ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Αυτόνομα και Ασφαλή Ασύρματα κατ΄ Απαίτηση Δίκτυα

Διδακτορική Διατριβή

Τσελίκης Χρήστος

Πειραιάς, Δεκέμβριος 2009

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΙΑΤΡΙΒΗ

για την απόκτηση Διδακτορικού

Διπλώματος του Τμήματος Πληροφορικής

Χρήστου Τσελίκη

ΑΥΤΟΝΟΜΑ ΚΑΙ ΑΣΦΑΛΗ ΑΣΥΡΜΑΤΑ ΚΑΤΑ ΑΠΑΙΤΗΣΗ ΔΙΚΤΥΑ

Τριμελής Συμβουλευτική Επιτροπή :
Επιβλέπων :
Χρήστος Δουληγέρης
Καθηγητής Πανεπιστημίου Πειραιώς

Μέλη :
Θεμιστοκλής Παναγιωτόπουλος
Καθηγητής Πανεπιστημίου Πειραιώς

Νικόλαος Αλεξανδρής
Καθηγητής Πανεπιστημίου Πειραιώς

Επταμελής Εξεταστική Επιτροπή :
Χρήστος Δουληγέρης
Καθηγητής Πανεπιστημίου Πειραιώς

Θεμιστοκλής Παναγιωτόπουλος
Καθηγητής Πανεπιστημίου Πειραιώς

Νικόλαος Αλεξανδρής
Καθηγητής Πανεπιστημίου Πειραιώς

Βασίλειος Χρυσικόπουλος
Καθηγητής Ιονίου Πανεπιστημίου

Δέσποινα Πολέμη
Επίκουρος Καθηγήτρια
Πανεπιστημίου Πειραιώς

Χαράλαμπος Κωνσταντόπουλος
Λέκτωρ Πανεπιστημίου Πειραιώς

Συμεών Παπαβασιλείου

Αναπληρωτής Καθηγητής Εθνικού Μετσόβιου Πολυτεχνείου

«Η μεν όρασις από του περιέχοντος αέρος λαμβάνει το φως, η δε ψυχή από των μαθημάτων» (Αριστοτέλης)

ΧΡΗΣΤΟΣ ΤΣΕΛΙΚΗΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΠΕΙΡΑΙΩΣ

ΜΕΤΡΟ 8.3, ΔΡΑΣΗ 8.3.1 – Γ' ΚΟΙΝΟΤΙΚΟ ΠΛΑΙΣΙΟ ΣΤΗΡΙΞΗΣ

Η Διδακτορική αυτή Διατριβή εκπονήθηκε στα πλαίσια του Προγράμματος ΠΕΝΕΔ
για το Συγχρηματοδοτούμενο Έργο «***Προηγμένα Συστήματα Ασφάλειας και Αντιμετώπισης Επιθέσεων***»
(80% της Δημόσιας Δαπάνης από το Ευρωπαϊκό Κοινωνικό Ταμείο, 20% της Δημόσιας Δαπάνης από τη ΓΓΕΤ και από τον Ιδιωτικό Τομέα)

ΚΩΔΙΚΟΣ ΕΡΓΟΥ 03ΕΔ/546

ΕΥΧΑΡΙΣΤΙΕΣ

Καθ' όλη τη διάρκεια της προσπάθειάς μου αυτής είχα σταθερό, πρόθυμο και έμπειρο συμπαραστάτη τον Καθηγητή κ. Χ. Δουληγέρη στον οποίο οφείλω πολλά. Τον ευχαριστώ πολύ.

Σημειώνω επίσης την άριστη και στενή συνεργασία μου με τον ακούραστο Επιστημονικό Συνεργάτη Δόκτορα κ. Σ. Μητρόπουλο και ακόμη την εποικοδομητική ανταλλαγή απόψεων πάνω σε ιδιαιτέρως ενδιαφέροντα ερευνητικά θέματα με τον Αν. Καθηγητή κ. Ν. Κομνηνό.

Ακόμη θέλω να εκφράσω τις θερμές ευχαριστίες μου στα μέλη της τριμελούς συμβουλευτικής επιτροπής Καθηγητή κ. Ν. Αλεξανδρή και Καθηγητή κ. Θ. Παναγιωτόπουλο, για την ενθαρρυντική τους στάση και τη συμβολή τους στην ολοκλήρωση της προσπάθειας αυτής.

Τέλος εκφράζω τις ευχαριστίες μας προς τη Γενική Γραμματεία Έρευνας και Τεχνολογίας για τους πόρους και τα μέσα που διέθεσε για την εκπόνηση της Διδακτορικής αυτής Διατριβής στα πλαίσια του Προγράμματος ΠΕΝΕΔ «Προηγμένα Συστήματα Ασφάλειας και Αντιμετώπισης Επιθέσεων».

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΕΚΤΕΤΑΜΕΝΗ ΠΕΡΙΛΗΨΗ

Τα ασύρματα κατ΄ απαίτηση δίκτυα (“wireless ad hoc networks”) διαθέτουν πολλές εγγενείς ιδιότητες που τα διαφοροποιούν από τα δίκτυα υποδομής και οι οποίες ιδιότητες αποτελούν προκλήσεις για την αποδοτική σχεδίαση και υλοποίηση των πρωτοκόλλων και των αλγορίθμων που ελέγχουν τα δίκτυα αυτά. Το κοινό χαρακτηριστικό όλων των κατηγοριών των δικτύων ad hoc είναι αυτό της αυθόρμητης ανακάλυψης των κόμβων όταν έρχονται σε κοντινή απόσταση και επίσης της μη υποβοήθησής τους από τη σταθερή δικτυακή υποδομή. Τα δύο αυτά βασικά χαρακτηριστικά αποτελούν την κοινή αφετηρία όλων των ερευνητικών προσπαθειών για την αποτελεσματική σχεδίαση και διαχείρισή των ασύρματων δικτύων ad hoc.

Σε αυτό το πλαίσιο η παρούσα διατριβή ακολουθεί μια σειρά από βήματα που οδηγούν στην εισαγωγή και την αναλυτική περιγραφή των προτεινόμενων λύσεων μετά από τον εντοπισμό των αδυναμιών και των ελλείψεων των υφιστάμενων λύσεων και των μοντέλων ανάπτυξης των ασυρμάτων δικτύων ad hoc. Τα βήματα που ακολουθεί η διατριβή είναι τα εξής.

- Αρχικά παρουσιάζονται με λεπτομέρεια οι μοντέρνες και διευρυμένες λειτουργικές απαιτήσεις καθώς και οι απαιτήσεις ασφάλειας που θα πρέπει να τηρούνται στα δίκτυα ad hoc. Αυτές οι απαιτήσεις θα πρέπει να διέπουν τις σύγχρονες και καινοτόμες προτεινόμενες λύσεις στην περιοχή των δικτύων ad hoc.
- Ακολουθεί το θεωρητικό υπόβαθρο της διατριβής το οποίο αναλύει τα ιδιαίτερα δυναμικά χαρακτηριστικά των δικτύων ad hoc και τους περιορισμούς στη λειτουργία τους λόγω των περιορισμένων πόρων των κόμβων. Ειδικότερα, οι περιορισμοί εντοπίζονται στη χαμηλή διαθέσιμη ενέργεια των ad hoc κόμβων, στη μικρή μνήμη, στη μικρή υπολογιστική ισχύ, στη χαμηλή ισχύ ασύρματης εκπομπής και, λόγω του περιορισμένου ασύρματου καναλιού μετάδοσης, στο μικρό διαθέσιμο εύρος ζώνης και στα σφάλματα μετάδοσης δεδομένων. Ταυτόχρονα, η αρχική αυτή ανάλυση υπογραμμίζει τα ανοιχτά προβλήματα που παραμένουν όσον αφορά την αποδοτικότερη και ασφαλέστερη λειτουργία των ήδη υφιστάμενων δικτυακών λύσεων.
- Στο πλαίσιο του θεωρητικού υπόβαθρου παρουσιάζεται ένα μικρό μόνο μέρος των πιο γνωστών υφιστάμενων ad hoc πρωτοκόλλων καθώς και των επεκτάσεων ασφάλειας αυτών στα πλαίσια μιας κατηγοριοποίησης των ad hoc πρωτοκόλλων που έχουν αναπτυχθεί μέχρι σήμερα. Αυτό είναι αναγκαίο ώστε λαμβάνοντας υπόψη τις ελλείψεις στις προδιαγραφές των υφιστάμενων τεχνολογιών (κυρίως όσον αφορά το επίπεδο του δικτύου) και των de facto ξεπερασμένων ad hoc προτύπων, να αναζητηθούν νέες μεθοδολογίες σχεδιασμού δικτύων ad hoc με έμφαση στα Κινητά Δίκτυα Ad Hoc (“Mobile Ad Hoc NETworks”) και τα Ασύρματα Δίκτυα Αισθητήρων (“Wireless Sensor Networks”).
- Στο επόμενο βήμα το ενδιαφέρον εστιάζεται στην έρευνα, στις λύσεις και τις προτάσεις που βρίσκονται ακόμη σε εξέλιξη, παρά στις παγιωμένες τεχνικές λύσεις. Οι απαιτήσεις που επιβάλλουν οι τελευταίες εφαρμογές ad hoc κάνουν φανερό ότι τα περισσότερα από τα υφιστάμενα πρωτόκολλα αδυνατούν να τα προστατέψουν ικανοποιητικά από τις απειλές και το μεγάλο αριθμό από επιθέσεις που διαρκώς προστίθενται. Οι καινοτόμες μεθοδολογίες σχεδιασμού λαμβάνουν σοβαρότερα υπόψη τα εγγενή χαρακτηριστικά των δικτύων ad hoc, τις εκτεταμένες αδυναμίες τους και τους νέους τύπους των πιθανών επιθέσεων που ανακύπτουν με έμφαση στην αντιμετώπιση των επιθέσεων κατά της δρομολόγησης των πακέτων στο επίπεδο του δικτύου και κατά του επιπέδου των εφαρμογών.
- Οι λύσεις που προτείνονται βελτιώνουν τις υπάρχουσες λύσεις και εισάγουν νέους ποιοτικούς στόχους με έμφαση στην επίτευξη του στόχου της *αυτονομίας* των δικτύων ad

hoc. Θεωρούμε ότι η αυτονομία είναι μια ισχυρή ιδιότητα που προϋποθέτει την ικανότητα για *αυτο-οργάνωση* των κόμβων του δικτύου και την ικανότητα της *αυτο-προστασίας* αυτών (δηλαδή δίχως εξωτερική παρέμβαση και υποβοήθηση) τόσο από τις τυχαίες βλάβες που μπορεί, για παράδειγμα, να οφείλονται στην έλλειψη ενέργειας των κόμβων ή/και στην ποιότητα του ασύρματου μέσου μετάδοσης όσο και από τις επιθέσεις που στοχεύουν τους σημαντικούς κόμβους μέσα στο δίκτυο. Για να επιτύχουμε αυτούς τους δύο στόχους ακολουθούμε σχεδίαση που είναι πολυστρωματική και κυρίως διαστρωματική. Ειδικότερα, κατά τη σχεδίαση και υλοποίηση ενσωματώνουμε στο δίκτυο λειτουργίες που σχετίζονται με την οργάνωση των κόμβων σε ιεραρχικές δομές και, επίσης, ενσωματώνουμε πρόσθετους μηχανισμούς προστασίας του δικτύου από κακόβουλες επιθέσεις.

- Στην προτεινόμενη λύση αυτο-οργάνωσης υποστηρίζονται τρόποι βελτίωσης και απλοποίησης των υφιστάμενων δικτυακών λύσεων που ασχολούνται με την αποδοτική ομαδοποίηση των κόμβων. Εισάγεται ένας κατάλληλα σταθμισμένος αλγόριθμος ομαδοποίησης των κόμβων και επιλογής αρχηγών των συστάδων που δημιουργούνται μέσα στο δίκτυο με δυναμικό τρόπο - ο αλγόριθμος που προτείνεται είναι ο “Robust Re-clustering Algorithm” (RRA). Ο αλγόριθμος RRA λαμβάνει υπόψη τις δυναμικές συνθήκες που επικρατούν στο ad hoc δίκτυο και σταθμίζει παραμέτρους όπως την κίνηση των κόμβων, τη διαθέσιμη ενέργεια και το βαθμό συνεκτικότητας των κόμβων και ως εκ τούτου λαμβάνει υπόψη την τοπολογία του δικτύου πριν αποφασίσει για το ποιοι κόμβοι είναι καταλληλότεροι να αναλάβουν το ρόλο και τα καθήκοντα του τοπικού αρχηγού. Συγκεκριμένα, ο αλγόριθμος RRA συγκρίνεται με άλλους δύο αλγόριθμους δημιουργίας συστάδων τον αλγόριθμο “Lower ID” (LID) και τον αλγόριθμο “Highest Degree” (HD). Ο RRA κατά τη διεξαγωγή πειραμάτων πετυχαίνει τη δημιουργία σταθερότερης δομής και συνεπώς επιφέρει μικρότερη επιβάρυνση στη λειτουργία του δικτύου επειδή ο ρυθμός μεταβολής των κόμβων-αρχηγών που επιλέγονται με τον RRA είναι μικρότερος από τον αντίστοιχο ρυθμό των δύο άλλων αλγορίθμων, ιδιαίτερα όταν οι δικτυακές συνθήκες είναι δύσκολες.
- Επίσης είναι επιτακτική η εισαγωγή αντιμέτρων κατά των επιθέσεων που απειλούν το ad hoc δίκτυο με την σχεδίαση και ενσωμάτωση στους κόμβους κατάλληλων κατανεμημένων αντιδραστικών μηχανισμών προστασίας. Είναι έκδηλο ότι οι υπάρχουσες λύσεις ανίχνευσης και αντιμετώπισης επιθέσεων που είναι ειδικά προσαρμοσμένες για τα δίκτυα ad hoc είναι λιγοστές, μη συστηματικές και ακόμη αποσπασματικές. Ειδικότερα, το τοπίο όσον αφορά τις αρχές, τις αρχιτεκτονικές και τα δυνατά μοντέλα των ad hoc συστημάτων ανίχνευσης εισβολών “Intrusion Detection Systems” (IDS) δεν έχει ακόμη ξεκαθαρίσει και συνεπώς αυτή η περιοχή είναι μια σημαντική κατεύθυνση έρευνας.
- Στην αρχιτεκτονική του συστήματος προστασίας που προτείνουμε η προστασία από τους κακόβουλους εισβολείς στο δίκτυο ad hoc διαπερνά τα τρία επίπεδα του δικτύου, του μεσισμικού και των ad hoc εφαρμογών. Η διαφοροποίηση με τις υφιστάμενες λύσεις έγκειται στο ότι οι μηχανισμοί προστασίας ενσωματώνονται και ολοκληρώνονται με τη λειτουργία της αυτο-οργάνωσης των ad hoc κόμβων. Έτσι η ιεραρχική δομή που προκύπτει με τον αλγόριθμο RRA στο προηγούμενο βήμα της αυτο-οργάνωσης προστατεύεται τώρα με βάση τον προτεινόμενο συνεργατικό μηχανισμό προστασίας. Ο μηχανισμός αυτός καθιστά *όλους* τους κόμβους του ad hoc δικτύου δυνητικούς ανιχνευτές των κακόβουλων κόμβων που προσπαθούν να βλάψουν την ορθή λειτουργία του δικτύου με το να μεταδίδουν παραπλανητικές πληροφορίες. Ακόμη είναι δυνατόν ο μηχανισμός προστασίας να εγκαθίσταται σε ένα περιορισμένο μόνο αριθμό κόμβων οι οποίοι θα λειτουργούν πλέον ως αφιερωμένοι πράκτορες ασφάλειας μέσα στο δίκτυο επιφορτισμένοι με το έργο της παρακολούθησης και της επεξεργασίας της δικτυακής κίνησης για τη λήψη ακέραιας και αμερόληπτης απόφασης ως προς το αν κάποιος κόμβος είναι κακόβουλος ή όχι.

  Ο συνεργατικός αυτός μηχανισμός στηρίζεται στη χρήση κατωφλίων για τη λήψη αποφάσεων από τους κόμβους που δρουν ως ανιχνευτές των ύποπτων εισβολέων.

Επιπλέον στο σύστημα ασφάλειας που προτείνουμε υιοθετούνται και κρυπτογραφικοί μηχανισμοί προληπτικής άμυνας. Εστιάζουμε στη δυνατότητα της δυναμικής δημιουργίας συμμετρικών κλειδιών κρυπτογράφησης που προέρχονται από τις ταυτότητες ή/και τις διευθύνσεις που ανταλλάσσουν οι κόμβοι μεταξύ τους. Επίσης, σύμφωνα με την αρχιτεκτονική που προτείνουμε, οι κρυπτογραφικοί έλεγχοι ενεργοποιούνται όταν κάποιος ανιχνευτής του συνεργατικού μηχανισμού προστασίας μεταδώσει συναγερμό για κάποιον ύποπτο κόμβο ο οποίος ύποπτος στη συνέχεια αυθεντικοποιείται περαιτέρω.

Οι προτεινόμενες λύσεις ολοκληρώνουν τα παραπάνω δίνοντας προστασία με πολλαπλές γραμμές άμυνας και, συνεπώς, δυνατότητες επιλογής του βαθμού ασφάλειας στο δίκτυο ανάλογα και με την ad hoc εφαρμογή που υποστηρίζει.

1. ΕΙΣΑΓΩΓΗ

Στην Κοινωνία της Πληροφορίας και των Επικοινωνιών διάφοροι παράγοντες απειλούν την ομαλή λειτουργία κάθε επικοινωνιακού ή πληροφοριακού συστήματος, καθώς οι κακόβουλοι χρήστες ποικίλουν και μπορεί να είναι ερασιτέχνες, βιομηχανικοί κατάσκοποι ακόμη και κυβερνήσεις. Επιπλέον, τυχαίοι παράγοντες όπως τα ανθρώπινα λάθη, οι περιβαλλοντικές συνθήκες και τα ατυχήματα που μπορεί να συμβούν προσθέτουν ένα ακόμη μεγαλύτερο επίπεδο κρισιμότητας στα εν λόγω συστήματα. Τα παραπάνω ισχύουν σε πολύ μεγαλύτερο βαθμό στα αυτόνομα δίκτυα ad hoc τα οποία δεν εξαρτώνται και δεν υποβοηθούνται από κάποια σταθερή υποδομή. Η ανάγκη για μηχανισμούς ασφάλειας που προλαμβάνουν, εντοπίζουν και αντιδρούν στις επιθέσεις κατά των δικτύων ad hoc είναι ολοφάνερη. Ακόμη περισσότερο, στην εποχή του ηλεκτρονικού εγκλήματος, τα όρια του οποίου δεν είναι καθόλου εύκολο να τεθούν, η ανάγκη για αξιόπιστη ανίχνευση των επιθέσεων, για άμεση αντιμετώπιση (response) και ανάκαμψη (recovery) από περιστατικά ασφάλειας γίνεται ολοένα και περισσότερο πιεστική.

1.1. ΤΑ ΑΝΟΙΧΤΑ ΠΡΟΒΛΗΜΑΤΑ ΩΣ ΚΙΝΗΤΡΑ

Παρακάτω συνοψίζουμε ποια είναι τα ανοιχτά προβλήματα που εντοπίσαμε όσον αφορά στα ασύρματα δίκτυα ad hoc και τα οποία λειτούργησαν ως κίνητρα για τις διερευνήσεις και τις λύσεις που προτείνουμε.

Οι ερευνητικές εργασίες στο σύνολό τους κατά τη διάρκεια του χρόνου μέχρι σήμερα έχουν αναδείξει πολλές διαφορετικές πλευρές των δικτύων ad hoc με τη μορφή ποιοτικών χαρακτηριστικών που οι δικτυακές λύσεις θα πρέπει να λαμβάνουν υπόψη, να υλοποιούν και να βελτιστοποιούν. Έτσι, όσον αφορά τα δίκτυα ad hoc οι υφιστάμενες τεχνικές λύσεις (πολύ συχνά αυτές ακολουθούν διαφορετικά μοντέλα επικοινωνιών, διαφορετικά υπολογιστικά παραδείγματα – “computational paradigms”– και διαφορετικές αρχιτεκτονικές) έχουν μελετήσει διεξοδικά ένα ευρύ φάσμα προβλημάτων όπως για παράδειγμα αυτό της αύξησης της χωρητικότητας των δικτύων ad hoc, της αύξησης του χρόνου ζωής των δικτύων και της διαθέσιμης ενέργειας των συσκευών ad hoc και της ικανότητας για προσαρμογή στη μεταβλητή τοπολογία με γρήγορη σύγκλιση των αλγορίθμων κάτω από τις έντονα μεταβαλλόμενες δικτυακές συνθήκες που κυρίως οφείλονται στην κίνηση των κόμβων. Δηλαδή είναι φανερό ότι το πρόβλημα της βελτιστοποίησης των αλγορίθμων στα δίκτυα ad hoc ήταν και είναι η σημαντικότερη συνιστώσα έρευνας στην περιοχή αυτή.

Οι τελευταίες ερευνητικές προσπάθειες πολλές φορές αποπειρώνται να εισάγουν νέες μεθόδους αντιμετώπισης του ίδιου προβλήματος και, για να αναφέρουμε ένα παράδειγμα μόνο, επιχειρούν να επιλύσουν αποδοτικά και αξιόπιστα το πρόβλημα της δρομολόγησης πάνω από μερικά συνδεδεμένες ad hoc τοπολογίες με καινοτόμες μεθόδους όπως η πιθανοκρατική δρομολόγηση - “opportunistic routing”- λύση που προσπαθεί να εκμεταλλευτεί την τυχαία κίνηση των κόμβων παρά να την αντιμετωπίσει ως εμπόδιο. Ένα άλλο σημαντικό και τρέχον πεδίο έρευνας για τα δίκτυα ad hoc είναι το πρόβλημα της διαφανούς διασύνδεσής τους με τα δίκτυα που διαθέτουν υποδομή, όπως το Διαδίκτυο, τα κινητά κυψελοειδή δίκτυα και τα Τοπικά Ασύρματα Δίκτυα WLAN (“Wireless Local Area Networks”). Περαιτέρω, η ασφάλεια στα αφύλακτα δίκτυα ad hoc είχε από την αρχή ελκύσει σημαντική ερευνητική προσπάθεια που έχει αποδώσει πολλά εμπειρικά και θεωρητικά αποτελέσματα στο συνδυασμό των οποίων βασίζονται πολλές τεχνολογικές λύσεις. Παραδείγματα πρόωρων εργασιών που εντόπισαν τις απειλές στα δίκτυα ad hoc (MANET και WSN) και πρότειναν αντίστοιχες λύσεις ασφαλείας είναι τα [1], [2], [3], [4], [5].

Κατά την άποψή μας η βελτίωση της επίδοσης και συμπεριφοράς των δικτύων ad hoc που έχουν υλοποιηθεί με τις τρέχουσες τεχνολογίες, η αντιμετώπιση των νέων απειλών που όλο και προστίθενται, όπως και η θεώρηση των απαιτήσεων των μοντέρνων εφαρμογών που σήμερα

αναδύονται αποδεικνύουν ότι απαιτείται να υπάρχει ακόμη μεγαλύτερη βελτιστοποίηση και ακόμη απαιτείται ***εναρμονισμός*** *μεταξύ του σχεδιασμού των δικτύων ad hoc και των συστημάτων αντιμετώπισης των επιθέσεων* που προστατεύουν τα δίκτυα από τις πιθανές απειλές τόσο στο τεχνικό όσο και στο διοικητικό επίπεδο.

Ειδικότερα, τα ποσοτικά χαρακτηριστικά της επίδοσης των δικτύων (ποιότητα ασύρματων ζεύξεων, δικτυακή διαπερατότητα, απώλεια πακέτων, μέση καθυστέρηση μηνυμάτων, αξιοπιστία μετάδοσης, διαθεσιμότητα κόμβων και υπηρεσιών, κ.α.) δε θα πρέπει να μελετώνται απομονωμένα, αντίθετα θα πρέπει να συναρτώνται και με το βαθμό ασφάλειας και προστασίας που προσφέρουν τα συστήματα αντιμετώπισης των επιθέσεων. Συνεπώς, η διαπίστωση για την *έλλειψη* ***μεθοδολογικά ολοκληρωμένων λύσεων*** λειτουργεί σαν ένα βασικό κίνητρο της διατριβής αυτής και διαμορφώνει τον πρωταρχικό στόχο της που είναι να προτείνει ολοκληρωμένες και αποδοτικότερες δικτυακές λύσεις που επιτυγχάνουν ταυτόχρονα ορθή, αξιόπιστη και αποδοτική δικτυακή λειτουργία αλλά και αποτελεσματική αυτο-προστασία έναντι των απειλών που ολοένα και διευρύνονται.

Σε αυτό το πλαίσιο, ένα πρόβλημα που παραμένει ανοιχτό για νέες λύσεις και προτάσεις είναι η επίτευξη της ***αυτο-οργάνωσης*** των ad hoc κόμβων. Η διατριβή αυτή εστιάζει στην εισαγωγή ιεραρχικών δομών σε ένα δίκτυο ad hoc με αποδοτικούς αλγορίθμους δυναμικής ομαδοποίησης των κόμβων οι οποίοι επιτυγχάνουν τα θετικά της ιεραρχικής δομής (οι ιεραρχικές δομές πολλών επιπέδων μπορεί να έχουν πολλαπλά πλεονεκτήματα όπως θα δούμε) ελαχιστοποιώντας τα αρνητικά, δηλαδή το διαχειριστικό κόστος υποστήριξης τέτοιων δομών.

Κατά πρώτον, οι ιεραρχίες δημιουργούν μια πολυ-επίπεδη δομή όπου τα ανώτερα επίπεδα δεν γνωρίζουν τις λεπτομέρειες της οργάνωσης και τις διαδικασίες λήψης αποφάσεων στα κατώτερα επίπεδα. Για παράδειγμα, σε ένα δίκτυο δύο επιπέδων οι πίνακες δρομολόγησης με τους οποίους προωθούνται τα πακέτα μεταξύ των κόμβων στο πρώτο (χαμηλότερο) επίπεδο παραμένουν άγνωστοι για το δεύτερο (ανώτερο) επίπεδο στην ιεραρχία των κόμβων. Έτσι ο αριθμός των κόμβων που τα κατώτερα ιεραρχικά επίπεδα μπορούν να υποστηρίξουν χωρίς να προκαλείται υπερφόρτωση στα ανώτερα επίπεδα είναι πολύ μεγαλύτερος σε ένα δίκτυο οργανωμένο ιεραρχικά. Συνεπώς, η κλιμάκωση των αλγορίθμων και των πρωτοκόλλων στα ιεραρχικά δίκτυα είναι πολύ μεγαλύτερη από ότι στα επίπεδα δίκτυα, ιδίως αν λάβουμε υπόψη και πόσο συχνά αλλάζουν οι συνθήκες σε ένα ad hoc δίκτυο.

Κατά δεύτερον, μια ιεραρχική δομή διαφυλάσσει τους ad hoc κόμβους από την ανεπιθύμητη κατανάλωση ενέργειας. Αυτό επιτυγχάνεται εφόσον μερικοί μόνο κόμβοι, οι οποίοι συνήθως είναι και οι πιο εύρωστοι μέσα στο ad hoc δίκτυο, αναλαμβάνουν το μεγαλύτερο βάρος της προώθησης των μηνυμάτων (ή/και άλλα βάρη όπως τη διαχείριση κλειδιών, τη διαχείριση του διαθέσιμου φάσματος, τη διαχείριση της συμμετοχής των κόμβων κ.α.). Έτσι οι απλοί (και πιο πολλοί) κόμβοι δεν αναλαμβάνουν να επιτελέσουν ενεργοβόρες εργασίες δηλαδή κυρίως την εκτέλεση υπολογιστικών πράξεων ή/και τις επαναλαμβανόμενες ασύρματες μεταδόσεις. Συνεπώς, εφόσον καταναλώνεται λιγότερη ενέργεια στους κόμβους, επιμηκύνεται ο συνολικός χρόνος ζωής του δικτύου.

Τα κύρια ανοιχτά προβλήματα όσον αφορά την αυτο-οργάνωση τα οποία αντιμετωπίζει η διατριβή αυτή είναι τα ακόλουθα.

1. Η επίτευξη ιεραρχικής αυτο-οργάνωσης με το μικρότερο δυνατό *διαχειριστικό κόστος*. Είναι γνωστό ότι οι αλγόριθμοι και τα σχήματα ομαδοποίησης των κόμβων επιφέρουν επιβάρυνση στις επικοινωνίες του δικτύου που εξαρτάται από την πολυπλοκότητά τους. Όλα τα σχήματα αυτό-οργάνωσης χρησιμοποιούν επιπλέον μηνύματα ελέγχου του που μεταδίδονται όταν απαιτείται ενημέρωση του δικτύου για τις αλλαγές των συνθηκών που συμβαίνουν, έτσι ώστε να αλλάξει και η δομή με την επιλογή καταλληλότερων κόμβων στην ιεραρχία μέσα στο δίκτυο. Η μείωση του αριθμού των μηνυμάτων ελέγχου αλλά και η μείωση της επεξεργαστικής

επιβάρυνσης των αλγορίθμων είναι βασικός στόχος στην αυτό-οργάνωση που επιδιώκεται ακόμη και σήμερα κατά τη φάση της σχεδίασης και επαλήθευσης των λύσεων.

2 Η διαφύλαξη της *συνέπειας* ("consistency") στις διαδικασίες της αυτο-οργάνωσης. Η αυτο-οργάνωση όσον αφορά τις διαδικασίες ομαδοποίησης συνήθως ασχολείται με την ελαχιστοποίηση του αριθμού των ομάδων μέσα στο δίκτυο. Ένας ποιοτικότερος όμως στόχος είναι η βέλτιστη, ακέραια και συνεπής επιλογή εκείνων των ομάδων (και αντίστοιχα κόμβων-αρχηγών) που τελικά θα καλύψουν όλους τους κόμβους του δικτύου. Διακρίναμε ότι η απαίτηση για λήψη ακέραιων αποφάσεων κατά τις διαδικασίες αυτο-οργάνωσης είναι ακόμη εντονότερη στις εχθρικές συνθήκες όπου πολλές φορές λειτουργεί το ad hoc δίκτυο. Ειδικότερα, η συνέπεια υπεισέρχεται έντονα και στα σχήματα εκλογής κόμβων-αρχηγών μέσα στο δίκτυο με τα οποία πετυχαίνουμε την αυτο-οργάνωση. Η ακεραιότητα ενός αποτελέσματος δικτυακής αυτο-οργάνωσης που επιτυγχάνεται με τεχνικά μέσα δεν είναι ένα τετριμμένο πρόβλημα, αντίθετα πολλές φορές φαίνεται δυσεπίλυτο. Εστιάζουμε σε αυτό το πρόβλημα χρησιμοποιώντας τη συνέπεια σαν ένα ποιοτικό χαρακτηριστικό που σαφώς σχετίζεται και με το επίπεδο προστασίας του συστήματος.

3 Η εύρεση της κατάλληλης *μεθόδου σχεδίασης* των αρχιτεκτονικών των δικτυακών πρωτοκόλλων και των αλγορίθμων αυτό-οργάνωσης. Δύο πιθανά μοντέλα είναι η αρθρωτή σχεδίαση των λειτουργικών στοιχείων που απαρτίζουν τα επίπεδα της δικτυακής αρχιτεκτονικής (modular design) και σε αντιπαράθεση η διαστρωματική σχεδίαση με αλληλεπιδράσεις μεταξύ των επιπέδων που διαθέτουν κοινή διεπαφή (cross layer design). Ποια μέθοδος είναι κατάλληλη εξαρτάται σαφώς από την ad hoc εφαρμογή, τις απαιτήσεις για εξασφάλιση της ποιότητας υπηρεσίας (QoS) και, εν τέλει, τις ίδιες τις υπηρεσίες που μια λύση στοχεύει να παρέχει, όπως θα εξηγήσουμε και αργότερα.

   Η προτεινόμενη λύση είναι μια πολυστρωματική και διαστρωματική λύση που περιλαμβάνει το επίπεδο του δικτύου, το επίπεδο του μεσισμικού και το επίπεδο των εφαρμογών. Ειδικότερα, στην αρχιτεκτονική που προτείνουμε οι διαδικασίες αυτο-οργάνωσης των κόμβων προς μια ιεραρχική δομή διατρέχουν τόσο το επίπεδο του δικτύου όσο και το υπερκείμενο επίπεδο του μεσισμικού. Επίσης, η ενέργεια λαμβάνεται υπόψη στους αλγορίθμους δρομολόγησης και αυτό-οργάνωσης, ενώ η γεωγραφική θέση είναι επίσης μια παράμετρος του φυσικού επιπέδου που χρησιμοποιείται από τους αλγορίθμους δρομολόγησης πακέτων, από τις διαδικασίες συντήρησης του δικτύου ("link maintenance") αλλά και από τις διαδικασίες της αυτό-οργάνωσης.

   Η προτεινόμενη λύση είναι μια *ολοκληρωμένη λύση αυτο-οργάνωσης και αυτο-προστασίας* του δικτύου ad hoc που σχεδιάστηκε με τη συγχώνευση του επιπέδου του δικτύου και του επιπέδου του μεσισμικού. Συγκεκριμένα, συγχωνεύσαμε το πρωτόκολλο δρομολόγησης με τη διαδικασία ομαδοποίησης των κόμβων ad hoc σε διακριτές ομάδες (στις οποίες θα αναφερόμαστε με τον όρο "clustering"). Έτσι στην υλοποίησή μας για το ad hoc δίκτυο σχεδιάσαμε πιο εύρωστο το επίπεδο του δικτύου και αυτό, όπως θα δούμε, είχε σαν αποτέλεσμα να παρέχεται βελτιωμένη δικτυακή απόδοση.

Ένα επίσης ανοιχτό πρόβλημα με το οποίο ασχοληθήκαμε είναι η *αξιοπιστία* στις ad hoc επικοινωνίες. Αυτό είναι ένα καυτό πρόβλημα που συναρτάται με την τοπολογία του ad hoc δικτύου που πολύ συχνά μπορεί να χάσει τη συνεκτικότητά της έτσι ώστε οι ροές των δεδομένων να διακόπτονται με μεγάλες απώλειες χρήσιμης πληροφορίας. Το πρόβλημα της αξιοπιστίας μπορεί να επιλυθεί σε πολλά επίπεδα, όπως για παράδειγμα στα χαμηλότερα επίπεδα της δικτυακής στοίβας πρωτοκόλλων (για παράδειγμα με τον έλεγχο των σφαλμάτων μετάδοσης στο φυσικό επίπεδο και με τον έλεγχο ροής στο επίπεδο διασύνδεσης των δεδομένων) αλλά και στο

επίπεδο του δικτύου όπου οι απώλειες των πακέτων απαιτούν κάποια προσαρμογή και αντίδραση των μηχανισμών προώθησης, όπως επίσης μπορεί η αξιοπιστία να επιλυθεί και στα ανώτερα επίπεδα του μεσισμικού (το επίπεδο μεταφοράς στην αρχιτεκτονική ISO/OSI) που αναλαμβάνουν την αξιόπιστη μετάδοση των μηνυμάτων από άκρη σε άκρη ("end-to-end"). Για εμάς η αξιοπιστία αποτιμάται με το ποσοστό των πακέτων που μεταδίδονται αξιόπιστα από άκρη σε άκρη για τις εγκατεστημένες ή/και τις χωρίς σύνδεση ροές δεδομένων και συναρτάται άμεσα με τη διαθεσιμότητα των ενδιάμεσων κόμβων, ή ισοδύναμα με το ποσοστό του χρόνου που οι κόμβοι είναι διαθέσιμοι, ή/και ισοδύναμα με την πιθανότητα κάποιος επιτιθέμενος να επιτύχει το στόχο του και να συμβιβάσει τους νόμιμους κόμβους του δικτύου. Η εναλλαγή των κόμβων που αναλαμβάνουν την προώθηση των πακέτων μέσα στο ad hoc δίκτυο είναι βασική συνιστώσα των λύσεων που προτείνουμε.

Επιπλέον, αν και η μεταβλητή και η μερική συνεκτικότητα της τοπολογίας όπως και η μικρή ακτίνα δράσης των ασύρματων κόμβων (ισοδύναμα η ισχύς εκπομπής τους) είναι τα βασικότερα προβλήματα των ad hoc δικτύων, η ασφάλεια των επικοινωνιών και της δικτυακής λειτουργίας είναι επίσης ένα βασικό πρόβλημα. Η ασφάλεια μπορεί να απειλείται περισσότερο στα δίκτυα ad hoc για λόγους που σχετίζονται τόσο με το μέσο μεταφοράς της επικοινωνίας (ασύρματη μετάδοση σε ένα ανοιχτό μέσο ευρείας εκπομπής που είναι πολύ εύκολο να παγιδευτεί) όσο και με τη φύση των ad hoc εφαρμογών (για παράδειγμα στρατιωτικές εφαρμογές όπου απαιτείται μεγάλος βαθμός εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας της πληροφορίας). Ο σχεδιασμός πρωτοκόλλων για ασφαλή και ανεκτική στις επιθέσεις ad hoc επικοινωνία και ad hoc δικτύωση είναι ακόμη ένα ανοικτό πρόβλημα, γεγονός που οφείλεται στη δυσκολία αντιμετωπίσεως των κακόβουλων επιθέσεων από θεωρητικά φιλικούς κόμβους.

Έτσι, η *αυτο-προστασία* των δικτύων ad hoc έναντι των πιθανών εισβολέων σε ένα πολύ περιορισμένο περιβάλλον καθώς και η αξιοπιστία έναντι των τυχαίων βλαβών είναι ένα ζήτημα που συνεχίζει να αποτελεί πόλο εντατικής έρευνας στα δίκτυα ad hoc. Αυτό το ανοιχτό θέμα αποτελεί έτερο σημαντικό μας κίνητρο. Πώς μπορεί να εννοηθεί η αυτο-προστασία σε μια ad hoc δομή που μεταβάλλεται τυχαία, ποιες είναι οι πρώτιστες απαιτήσεις ασφαλείας που θα πρέπει να υπηρετεί μια λύση ασφάλειας, σε ποιους κόμβους θα πρέπει να τοποθετηθεί η ασφάλεια και ιδίως πώς μπορεί μια τέτοια λύση να σχεδιαστεί με αποδοτικό τρόπο, δηλαδή στα πλαίσια ποιων αρχιτεκτονικών (κεντρικοποιημένο, κατανεμημένο, ιεραρχικό ή/και υβριδικό μοντέλο), ποιων μεθοδολογιών ασφάλειας (πολιτικές, κανόνες και επίπεδα ασφάλειας) και ποιών δικτυακών επιπέδων (στο επίπεδο του δικτύου ή/και στο επίπεδο του μεσισμικού ή/και στο επίπεδο της εφαρμογής) είναι ερωτήματα που αποτελούν βασικά μας κίνητρα και κατευθύνσεις έρευνας.

Κομβικό σημείο αδυναμίας σε μια ιεραρχική δομή που βασίζεται σε ένα κορμό δικτύου που αποτελείται από κόμβους-αρχηγούς (αυτοί οι κόμβοι απαρτίζουν το "forwarding set") είναι ακριβώς ο εύκολος συμβιβασμός των σημαντικών κόμβων από τους πιθανούς επιτιθέμενους. Ειδικότερα, η απειλή κατά της ακεραιότητας των πρωτοκόλλων και αλγορίθμων με στόχο το συμβιβασμό των σημαντικών/εύρωστων κόμβων (αυτοί μπορεί να είναι και ομότιμοι με όλους τους υπόλοιπους) που διεξάγουν την προώθηση των μηνυμάτων μέσα στο δίκτυο είναι το πεδίο που αφιερώνουμε σημαντική προσπάθεια. Οι λύσεις προστασίας που αναπτύσσουμε σκοπό έχουν να προστατέψουν τους κόμβους-αρχηγούς και κατ' επέκταση ολόκληρο το δίκτυο από κακόβουλους κόμβους που προσπαθούν να τους συμβιβάσουν.

Διαπιστώσαμε ότι η εισαγωγή των *Συστημάτων Ανίχνευσης Εισβολών (IDS)* στα δίκτυα ad hoc αποτελεί ένα εντατικό πεδίο προσπάθειας όπου η έρευνα για την (τις) κατάλληλη(ες) αρχιτεκτονικές των ad hoc IDS συστημάτων παραμένει ανοιχτή. Κατά τη γνώμη μας τα συστήματα IDS αποτελούν λύσεις που μπορούν να δώσουν μεθοδολογικές απαντήσεις στα προβλήματα της αυτό-προστασίας των δικτύων ad hoc εφόσον η ασφάλεια με το IDS από τις κακόβουλες επιθέσεις που έχουν καταφέρει να ξεπεράσουν τους κρυπτογραφικούς ελέγχους βασίζεται στο οργανωμένο σχήμα απώθηση - ανίχνευση εισβολέα – αντίδραση - ανάκαμψη του δικτύου από την επίθεση.

Επίσης διαπιστώσαμε ότι ένα τέτοιο σύστημα μπορεί να ακολουθεί τόσο κρυπτογραφικές όσο και μη κρυπτογραφικές μεθοδολογίες για την επίτευξη συγκεκριμένων επιπέδων ασφάλειας. Ειδικότερα, οι υποψήφιες μη κρυπτογραφικές μεθοδολογίες δεν είναι λίγες. Αντίθετα υπάρχουν πολλές διαφορετικές επιλογές όπως η εύρωστη στατιστική ανάλυση της δικτυακής κίνησης για ανίχνευση των ανωμαλιών, η μηχανική εκμάθηση, η εξόρυξη δεδομένων και ιδίως τα συνεργατικά σχήματα με εφαρμογή της θεωρίας παιγνίων, των συνεργατικών σχημάτων ψηφοφορίας, των συνεργατικών σχημάτων κατωφλίων και των μοντέλων/σχημάτων εμπιστοσύνης που για τα δίκτυα ad hoc βασίζονται στην αξιολόγηση της καλής συμπεριφοράς των κόμβων, για να αναφέρουμε λίγες μόνο από αυτές. Και μόνο μια συγκριτική μελέτη της αξιοπιστίας όλων των παραπάνω στο ad hoc περιβάλλον μπορεί να αποτελέσει αξιόλογη μελλοντική ερευνητική προσπάθεια.

Επίσης, διαπιστώσαμε ότι δεν επιβάλλεται κάποιος περιορισμός για την αρχιτεκτονική των συστημάτων αυτών, σίγουρα όμως θα πρέπει να γίνεται αποδοτική και αξιόπιστη σχεδίαση ανάλογα και με τα κατώτερα υφιστάμενα δικτυακά επίπεδα. Βασικός μας στόχος είναι η σχεδίαση λύσεων προστασίας που βασίζονται στην ανίχνευση και απομόνωση υπόπτων κόμβων με τη βοήθεια πλήρως κατανεμημένων και συνεργατικών σχημάτων προστασίας.

Ένα άλλο κίνητρο στη διατριβή αυτή ήταν η διερεύνηση της δυνατότητας εισαγωγής των *κατανεμημένων μοντέλων και των κατανεμημένων τεχνολογιών μεσισμικού* που έχουν εφαρμοστεί στο Διαδίκτυο στο επίπεδο του ad hoc μεσισμικού. Το ad hoc μεσισμικό είναι το στρώμα όπου μπορεί να υλοποιηθεί με ανοιχτό και διάφανο τρόπο η αυτό-οργάνωση των κόμβων, η ανακάλυψη και η διαχείριση των υπηρεσιών που είναι διαθέσιμες από τους ad hoc κόμβους (για παράδειγμα υπηρεσία αναφοράς θερμοκρασίας σε ένα δίκτυο αισθητήρων ή η κοινή χρήση αρχείων σε ένα δίκτυο MANET). Επάνω στο στρώμα μεσισμικού των δικτύων ad hoc μπορούν να βασιστούν και οι πολυάριθμες εφαρμογές των τελικών χρηστών. Με το στρώμα του μεσισμικού παρέχεται η δυνατότητα οι πόροι των δικτύων ad hoc να ανακαλύπτονται και να χρησιμοποιούνται με πολύ μεγαλύτερη κλίμακα διείσδυσης καθιστώντας έτσι τα δίκτυα ad hoc συνέχεια των δικτύων υποδομής όπως το Διαδίκτυο, τα κυψελοειδή δίκτυα, τα δορυφορικά συστήματα και τα WLAN.

Για το ad hoc περιβάλλον υποψήφια υπολογιστικά μοντέλα κατανεμημένων συστημάτων που ξεχωρίσαμε είναι το μοντέλο client/server, το μοντέλο Peer-to-Peer και το μοντέλο SOA. Επιλέξαμε αντιπροσωπευτικές κατανεμημένες πλατφόρμες/τεχνολογίες από κάθε ένα μοντέλο (αντίστοιχα sockets, RMI και XML Web Services) και τις συγκρίναμε με μέτρα την επίδοση και την ανθεκτικότητα σε συνθήκες πλημμύρας ερωτημάτων ανακάλυψης υπηρεσιών μέσα στο δίκτυο ad hoc. Στα πειράματά μας χειριστήκαμε τα κατώτερα στρώματα των ad hoc επικοινωνιών αφαιρετικά εφόσον εστιάζουμε στη μελέτη και την αξιολόγηση των εφαρμογών και του μεσισμικού. Έτσι πιστεύουμε ότι τα αποτελέσματα που συλλέξαμε και παρουσιάζουμε είναι αξιόπιστα όσον αφορά τη συμπεριφορά των εν λόγω κατανεμημένων πλαισίων. Ενδεικτικά αναφέρουμε εδώ ότι το κατανεμημένο μοντέλο Peer-to-Peer που περιλαμβάνει μητρώα υπηρεσιών, πάροχους και καταναλωτές υπηρεσίας ήταν αυτό που έδωσε τα βέλτιστα αποτελέσματα.

1.2. ΟΙ ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΛΥΣΕΙΣ

Η διατριβή αυτή συστηματικά εστιάζει στην ανεύρεση προσαρμοστικών μοντέλων και δικτυακών λύσεων κατάλληλων για το περιορισμένο ad hoc περιβάλλον. Λόγω ακριβώς της προσαρμοστικότητας των λύσεων που προτείνουμε, ένα δίκτυο ad hoc στο οποίο έχει εγκατασταθεί το προτεινόμενο λογισμικό θα μπορεί να υποστηρίζει ένα ευρύ φάσμα από ad hoc εφαρμογές, η κάθε μια με διαφορετικές απαιτήσεις.

Όπως έχουμε ήδη εξηγήσει εστιάζουμε σε μοντέλα και δικτυακές λύσεις που στοχεύουν στην ανάπτυξη ***αυτόνομων δικτύων*** που επιτυγχάνεται με μηχανισμούς ***δυναμικής αυτο-οργάνωσης*** και ***αντιδραστικής αυτο-προστασίας***. Οι επιμέρους στόχοι και τα αντίστοιχα αποτελέσματα που επιτεύχθηκαν εν συντομία είναι:

- Εντοπίσαμε, αναλύσαμε και διαχειριστήκαμε ως *δικτυακές συνθήκες* εκείνους τους παράγοντες που επηρεάζουν την επίδοση των κατανεμημένων αλγορίθμων και των πρωτοκόλλων στα κινητά ασύρματα δίκτυα ad hoc. Αυτό εξυπηρετεί τη σχεδίαση περισσότερο αποδοτικών αλγορίθμων, δηλαδή με τις κατάλληλες παραμετροποιήσεις και με την ανάλυση της ευαισθησίας των παραγόντων που χρησιμοποιούν οι δικτυακοί αλγόριθμοι και τα πρωτόκολλα (όπως για παράδειγμα οι αλγόριθμοι ομαδοποίησης) επιτυγχάνεται βελτιστοποίηση και συνεπώς αξιοσημείωτη μείωση του διαχειριστικού κόστους για την αυτο-οργάνωση των ad hoc κόμβων και συνεπώς επιτυγχάνεται βέλτιστη δικτυακή επίδοση.
- Όσον αφορά στο στόχο της αυτο-οργάνωσης ακολουθήσαμε τη σχεδίαση ενός *σταθμισμένου αλγορίθμου συσταδοποίησης/εκλογής αρχηγών* που λαμβάνει υπόψη τη διαθέσιμη ενέργεια στους ad hoc κόμβους. Προτείναμε το δυναμικό αλγόριθμο ομαδοποίησης και εκλογής αρχηγού “Robust Re-clustering Algorithm” (RRA). Επίσης η δρομολόγηση σχεδιάζεται και υλοποιείται με στόχο την αυτονομία, δηλαδή οι κόμβοι μόνοι τους ανακαλύπτουν τα μονοπάτια δρομολόγησης χωρίς εξωτερική διαχειριστική επέμβαση.
- Περαιτέρω, όσον αφορά το στόχο της αυτο-οργάνωσης, οι προτεινόμενοι αλγόριθμοι είναι *ολοκληρωμένοι αλγόριθμοι δρομολόγησης και δυναμικής ομαδοποίησης των κόμβων*. Διαγνώσαμε ότι πολύ σπάνια στις υπάρχουσες τεχνικές λύσεις ακολουθούνται ολοκληρωμένες λύσεις που να περιλαμβάνουν αν όχι όλα τα επίπεδα της δικτυακής αρχιτεκτονικής, τουλάχιστον τα βασικά από αυτά. Μια υποσχόμενη τάση σε αυτή την κατεύθυνση είναι η σχεδίαση διαστρωματικών πρωτοκόλλων και δικτυακών λύσεων. Ωστόσο, από την πλευρά μας ακολουθήσαμε μια ενοποιημένη σχεδίαση πρωτοκόλλου αυτό-οργάνωσης που λαμβάνει υπόψη το επίπεδο της ad hoc δρομολόγησης όπως επίσης και τη θέση των κόμβων. Ο προσαρμοστικός αυτός μηχανισμός της οργάνωσης των κόμβων σε διακριτές και αυτό-διαχειριζόμενες ομάδες (clusters) θεωρούμε ότι τυπικά ανήκει στο επίπεδο του ad hoc μεσισμικού, στο οποίο και τον εντάσσουμε τυπικά, ενώ παράλληλα σύμφωνα με τη σχεδίαση που ακολουθήσαμε διατρέχει και έχει διεπαφή με το επίπεδο της ad hoc δρομολόγησης.
- Όσον αφορά την ανακλαστική αυτο-προστασία προτείνουμε λύση που χρησιμοποιεί κρυπτογραφικές μεθόδους μόνο σε ότι αφορά την εγκατάσταση και την ανταλλαγή κρυπτογραφικών κλειδιών μεταξύ των κόμβων. Περισσότερο εστιάζουμε σε *συνεργατικά σχήματα προστασίας* που βασίζονται στην ανταλλαγή μηνυμάτων μεταξύ των κόμβων για τη διεξαγωγή συνεπών συμπερασμάτων και αποφάσεων ως προς την ανίχνευση επίθεσης από τους εισβολείς στο δίκτυο ad hoc. Τονίζουμε ότι αντιμετωπίζουμε το πρωτόκολλο της ad hoc δρομολόγησης ως βασικό μέρος του συστήματος προστασίας του δικτύου και όχι σαν ένα επίπεδο που λειτουργεί μεμονωμένα από τους μηχανισμούς προστασίας του δικτύου.

  Παρουσιάζουμε ένα *μοντέλο αναφοράς* για την αυτόνομη διαχείριση των δικτύων ad hoc. Κάνουμε την απόπειρα να εντάξουμε τα συνεργατικά σχήματα σε μια αρχιτεκτονική (μπορεί κατά περίσταση να είναι πλήρως κατανεμημένη ή ιεραρχική) για το ad hoc σύστημα ανίχνευσης εισβολών - Intrusion Detection System. Αυτό έχει σαν αποτέλεσμα η αντιμετώπιση των επιθέσεων από εισβολείς στο δίκτυο ad hoc να ακολουθεί το σχήμα: ανίχνευση κακόβουλου κόμβου (όπως θα δούμε τα πρωτόκολλα επεξεργάζονται πληροφορία μέχρι και τρία βήματα μακριά) – αντίδραση με μαρκάρισμα του κόμβου και ενημέρωση του υπόλοιπου δικτύου – ανάκαμψη με αλλαγή του μονοπατιού δρομολόγησης. Το προτεινόμενο σχήμα επεκτείνει ακόμη περισσότερο το σχήμα αυτο-οργάνωσης με χαρακτηριστικά προστασίας από κακόβουλους κόμβους. Το ολοκληρωμένο σχήμα αυτο-οργάνωσης και προστασίας που προτείνουμε καλείται “Secure CGPSR” (SC-GPSR).
- Επιπρόσθετα μελετήσαμε πιθανά *κατανεμημένα μοντέλα μεσισμικού* του Διαδικτύου που είναι δυνατόν να αξιοποιηθούν στα δίκτυα ad hoc κατά τη διαδικασία της ανακάλυψης των διαθέσιμων υπηρεσιών (“service discovery”) εσωτερικά από τους ομότιμους ad hoc

κόμβους ή/και εξωτερικά από κόμβους και χρήστες του Διαδικτύου. Προκειμένου να διαπιστώσουμε ποια τεχνολογία μεσισμικού μπορεί να είναι πιο κατάλληλη για το σκοπό αυτό, καθορίσαμε τις προδιαγραφές για την εφαρμογή δοκιμής και το κατανεμημένο πλαίσιο που μπορεί να χρησιμοποιηθεί στην αξιολόγηση της επίδοσης των υποψήφιων ad hoc κατανεμημένων τεχνολογιών μεσισμικού.

Πρέπει να σημειώσουμε σε αυτό το σημείο τις κύριες μεθοδολογίες που χρησιμοποιήσαμε κατά τη σχεδίαση και υλοποίηση των προτεινόμενων στη διατριβή λύσεων. Οι μέθοδοι που χρησιμοποιήσαμε όσον αφορά τις δικτυακές λύσεις είναι οι εξής:

1 *Εκτίμηση των προτεινόμενων λύσεων με εμπειρικές μεθόδους*. Ειδικότερα, στη διατριβή κάναμε χρήση τόσο πακέτων προσομοίωσης όσο και πακέτων εξομοίωσης. Τα πακέτα προσομοίωσης είναι αποκλειστικά πακέτα λογισμικού που προσομοιώνουν τις λειτουργίες στο επίπεδο του δικτύου και των εφαρμογών, ενώ κατά τη μέθοδο της εξομοίωσης (emulation) συμμετέχουν και πραγματικοί κόμβοι για την εκτίμηση των προτεινόμενων λύσεων.

- ΠΑΚΕΤΑ ΠΡΟΣΟΜΟΙΩΣΗΣ: J-SIM (δίκτυο ad hoc) και JNS(δίκτυο TCP/IP).
    - Στο Φυσικό επίπεδο: Κλιμάκωση των Κόμβων και της Ισχύος Εκπομπής.
    - Κλιμάκωση της ταχύτητας κόμβων και της δικτυακής κίνησης.
    - Κλιμάκωση του Αριθμού και Τύπων των Επιθέσεων.
    - Στο επίπεδο του Δικτύου: Εκτίμηση/Σύγκριση των προτεινόμενων Αλγόριθμων/Πρωτοκόλλων.
    - Στο επίπεδο της Εφαρμογής: Παραγωγή ροών TCP/SGN/UDP.
- ΠΑΚΕΤΟ ΕΞΟΜΟΙΩΣΗΣ Java-SIM. [Γεννήτρια Αιτημάτων] + [Πραγματικοί Κόμβοι].
    - Κλιμάκωση Ροών TCP/UDP/XML/HTTP.

2 *Μοντελοποίηση.*

- Με τα κατάλληλα εργαλεία της UML επιτυγχάνεται περιγραφή των αλληλεπιδράσεων μεταξύ των υπο-συστημάτων (χρησιμοποιήσαμε τα Διαγράμματα Ακολουθίας Μηνυμάτων), όπως και μεταξύ των χρηστών και των (υπο)συστημάτων (Περιπτώσεις Χρήσης).

3 *Σχεδίαση πρωτόκολλων και αλγορίθμων.*

- ΔΙΑΣΤΡΩΜΑΤΙΚΗ / ΠΟΛΥΣΤΡΩΜΑΤΙΚΗ /ΟΛΟΚΛΗΡΩΜΕΝΗ σχεδίαση. Τα επίπεδα της διαστρωματικής αρχιτεκτονικής ανταλλάσσουν τιμές των παραμέτρων επίδοσης όπως τις συντεταγμένες θέσης, τον αριθμό των γειτόνων, την ενέργεια των κόμβων (Εξαρτάται από τις Απαιτήσεις QoS της Ad Hoc Εφαρμογής).
- Η μέθοδος “piggyback” κατά τη σχεδίαση της λύσης αυτο-οργάνωσης κατά την οποία η πληροφορία την ομαδοποίηση των κόμβων και την εκλογή αρχηγών μεταφέρεται και ενσωματώνεται στα πακέτα που ανταλλάσσονται στο επίπεδο του δικτύου.

Οι μέθοδοι που χρησιμοποιήσαμε όσον αφορά τις λύσεις προστασίας είναι οι εξής:

1 *Προστασία με Συμπληρωματικές Λύσεις.*

- Κρυπτογραφικές Λύσεις. Συμμετρικές και Δυναμικές.
- Συνεργατικά Κατανεμημένα Σχήματα.
    - Παράδειγμα: N-Προγραμματισμός.
- Σχήματα ψηφοφορίας ανάμεσα σε ad hoc Κόμβους.
- Αναφορά θέσης.

- Γεωγραφικά Ad Hoc Πρωτόκολλα, GPS.

2 *Προστασία με Διακριτά Επίπεδα Ασφάλειας.*

- Έλεγχος Ακεραιότητας Πρωτοκόλλων και Δεδομένων.
- Εισαγωγή Διακριτών Κατωφλίων / Επιπέδων Αποφάσεων ($K_1 \geq K_2 \geq \ldots K_n$).
- Ανίχνευση και ταξινόμηση των κόμβων (καλός, ύποπτος, κακόβουλος) με βάση τη δικτυακή συμπεριφορά ως προς την τήρηση/παραβίαση των κατωφλίων.
- Σχήμα Προστασίας Πρόληψης, Ανίχνευσης / Πιστοποίησης, Αντίδρασης με αποφυγή των ύποπτων κόμβων στη δρομολόγηση και πληροφόρηση του δικτύου για τους ύποπτους κόμβους.

1.3. ΔΟΜΗ ΤΟΥ ΚΕΙΜΕΝΟΥ

Στο πρώτο Κεφάλαιο, το οποίο αποτελεί την Εισαγωγή της διατριβής, περιγράφονται πρώτα τα ανοιχτά προβλήματα στην περιοχή των ασύρματων δικτύων ad hoc τα οποία δρουν ως κίνητρα για τις περιοχές της έρευνας που εστιάζει η διατριβή καθώς και για τις λύσεις που προτείνονται. Ακολουθεί παρουσίαση των προτεινόμενων λύσεων οι οποίες εστιάζουν στην αποδοτική αυτό-οργάνωση και την αυτό-προστασία των ασύρματων δικτύων ad hoc από τους κακόβουλους κόμβους. Η Εισαγωγή κλείνει με τη δομή της διατριβής.

Στο δεύτερο Κεφάλαιο παρέχεται το θεωρητικό υπόβαθρο με ένα διευρυμένο σύνολο των απαιτήσεων λειτουργικότητας και ασφάλειας που σήμερα θα πρέπει να διέπουν την ανάπτυξη των καινοτόμων δικτύων ad hoc. Το πακέτο των απαιτήσεων που παρουσιάζεται αν και σίγουρα δεν μπορεί να θεωρηθεί πλήρες, είναι κατά το δυνατό επικαιροποιημένο γιατί προέρχεται από τη θεώρηση των υπό εξέλιξη και όχι των ξεπερασμένων προτύπων και, κυρίως, υπό το πρίσμα των μοντέρνων υπηρεσιών ad hoc που σήμερα αναδύονται.

Στο τρίτο Κεφάλαιο παρέχεται μια εκτεταμένη ανάλυση των ιδιαιτέρων χαρακτηριστικών των ασύρματων δικτύων ad hoc τα οποία διαφοροποιούν τα δίκτυα αυτά από τα υπόλοιπα δίκτυα. Επίσης, περιλαμβάνεται μια σύντομη περιγραφή των βασικών κατηγοριών των ασύρματων δικτύων ad hoc με βάση τις εφαρμογές που αυτά υποστηρίζουν (MANET, WSN, VANET, Mesh). Στο ίδιο Κεφάλαιο παρουσιάζεται μια μικρή και ενδεικτική κατηγοριοποίηση των γνωστότερων ad hoc πρωτοκόλλων δρομολόγησης. Σε αυτήν την κατηγοριοποίηση παρουσιάζεται ένα ad hoc πρωτόκολλο δρομολόγησης και, όπου υπάρχει, η αντίστοιχη ασφαλής επέκταση αυτού. Στο ίδιο Κεφάλαιο παρουσιάζεται μια ανάλυση των γνωστότερων ενεργητικών επιθέσεων κατά των δικτύων ad hoc. Η ανάλυση εστιάζει σε επιθέσεις κατά του επιπέδου του δικτύου τις οποίες διαχωρίζει σε επιθέσεις κατά της ακεραιότητας των πρωτοκόλλων και σε επιθέσεις κατά της προώθησης των μηνυμάτων και επίσης εστιάζει σε επιθέσεις κατά του επιπέδου των υπηρεσιών του τύπου Άρνησης Εξυπηρέτησης Υπηρεσιών.

Στο τέταρτο Κεφάλαιο εισάγονται οι αρχιτεκτονικές που προτείνονται με στόχο την αυτο-οργάνωση και την αυτό-προστασία των δικτύων ad hoc. Όσον αφορά την αρχιτεκτονική του συστήματος στόχος της διατριβής είναι να σχεδιαστεί και να υλοποιηθεί μια διαστρωματική λύση η οποία θα παρέχει την αυτο-οργάνωση των κόμβων ad hoc ως υπηρεσία. Στην προτεινόμενη αρχιτεκτονική τα επίπεδα που συμπεριλαμβάνονται είναι το επίπεδο δρομολόγησης, το επίπεδο του ad hoc μεσισμικού και το επίπεδο της ad hoc εφαρμογής. Οριοθετείται το επίπεδο του ad hoc μεσισμικού και εντάσσονται σε αυτό η υπηρεσία της αυτό-οργάνωσης των κόμβων, η ανακάλυψη, η παροχή και η διαχείριση των υπηρεσιών που διαθέτει το δίκτυο ad hoc τόσο στους κόμβους του όσο και προς τα εξωτερικά δίκτυα με τα οποία διασυνδέεται.

Επίσης, η προστασία σύμφωνα με την προτεινόμενη αρχιτεκτονική του συστήματος ασφάλειας

διατρέχει και τα τρία ad hoc επίπεδα (του δικτύου, του μεσισμικού και της αυτο-οργάνωσης). Ωστόσο, για λόγους που οφείλονται στους περιορισμούς του δικτύου ad hoc, προτείνεται σε κάθε επίπεδο η μέθοδος προστασίας να είναι διαφορετική. Έτσι προτείνεται το επίπεδο του δικτύου (όπως και τα κατώτερα επίπεδα) να προστατεύεται κρυπτογραφικά με τη χρήση κλειδιών. Η κατανεμημένη υπηρεσία της αυτο-οργάνωσης των ομότιμων κόμβων προτείνεται να προστατεύεται με συνεργατικές μεθόδους ανίχνευσης και αντιδραστικής αντιμετώπισης των εισβολέων και το επίπεδο της εφαρμογής προτείνεται να διασφαλίζεται με πρόσθετες αυθεντικοποιήσεις των κόμβων, εφόσον έχει προηγηθεί ανίχνευση μιας επίθεσης από το επίπεδο του μεσισμικού και έγερση συναγερμού. Συνεπώς το δίκτυο διασφαλίζεται από τις επιθέσεις κακόβουλων κόμβων με πολλαπλές γραμμές άμυνας που δρουν συμπληρωματικά.

Στο πέμπτο Κεφάλαιο παρουσιάζεται διεξοδικά η προτεινόμενη λύση αυτο-οργάνωσης που βασίζεται στην εισαγωγή ιεραρχικής δομής στο δίκτυο ad hoc. Οι πολυεπίπεδες ιεραρχίες προκύπτουν από τους αλγόριθμους ομαδοποίησης των κόμβων. Τις διακριτές ομάδες διαχειρίζονται οι επιλεγμένοι κόμβοι-αρχηγοί. Αρχικά αναλύονται οι πιθανοί παράγοντες που επηρεάζουν την επίδοση και εισάγονται νέα μέτρα εκτίμησης της αξιοπιστίας των αλγορίθμων ομαδοποίησης (όπως η διαθεσιμότητα των κόμβων-αρχηγών που επιλέγονται). Ο προτεινόμενος αλγόριθμος είναι ένας σταθμισμένος αλγόριθμος εκλογής αρχηγού πάνω σε τρεις παραμέτρους που αντανακλούν την ad hoc δυναμικότητα, με έμφαση στη μεταβλητή τοπολογία, την κίνηση και την ελαττούμενη κατά τη λειτουργία διαθέσιμη ενέργεια των κόμβων.

Στο ίδιο Κεφάλαιο παρουσιάζεται μια εκτίμηση της ευστάθειας του προτεινόμενου αλγόριθμου σε σύγκριση με άλλους δύο γενικούς αλγόριθμους συσταδοποίησης/ομαδοποίησης, ενώ έμφαση δίνεται στην βέλτιστη παραμετροποίηση της μεταβλητής απόφασης που χρησιμοποιεί ο αλγόριθμος σε σχέση με την ισχύ εκπομπής των ασύρματων κόμβων. Τα αποτελέσματα προσομοίωσης δείχνουν ότι ο αλγόριθμος επιφέρει μικρή επιβάρυνση στο δίκτυο και έχει τη βέλτιστη αξιοπιστία για μεσαία και μεγάλα επίπεδα της ασύρματης εκπομπής ισχύος.

Στο έκτο Κεφάλαιο παρουσιάζεται η προτεινόμενη λύση αυτό-προστασίας η οποία εμπεριέχει τον αλγόριθμο αυτό-οργάνωσης που παρουσιάστηκε στο έκτο Κεφάλαιο. Αρχικά δίνεται μια σύντομη περιγραφή των αρχιτεκτονικών των συστημάτων IDS που έχουν προταθεί στα δίκτυα ad hoc. Προτείνεται ένα μοντέλο αναφοράς για την αυτο-οργάνωση και αυτό-προστασία των αυτόνομων δικτύων ad hoc το οποίο βασίζεται στο σχήμα παρεμπόδιση – ανίχνευση – αντίδραση – ανάκαμψη μετά από την εκδήλωση επίθεσης. Το μοντέλο απαιτεί τη λήψη τοπικών αποφάσεων και στη συνέχεια την ανταλλαγή μηνυμάτων προκειμένου να παράγονται γνώμες / συμφωνίες / μαύρες λίστες / συναγερμοί με αντίκτυπο για την ολική δομή του δικτύου. Ειδικότερα, προτείνεται η αυτό-προστασία να παρέχεται με διακριτά κατώφλια ασφάλειας, η παραβίαση των οποίων ανιχνεύει και μαρκάρει κάποιο κόμβο ως ύποπτο. Το μοντέλο αναφοράς δεν αποκλείει τη χρήση κρυπτογραφικών μεθόδων προστασίας οι οποίες δρουν συμπληρωματικά ως προς τα συνεργατικά σχήματα προστασίας.

Ακολουθεί μία λεπτομερής περιγραφή της υλοποίησης του σχήματος αυτο-προστασίας που βασίζεται στο παραπάνω μοντέλο αναφοράς. Το προτεινόμενο σχήμα, το “Secure Clustered-Greedy Perimeter Stateless Routing” (SC-GPSR) υλοποιείται με μια σειρά από λειτουργικά τμήματα το καθένα από τα οποία αναλαμβάνει διαφορετικές λειτουργίες όπως τη γεωγραφική δρομολόγηση που βασίζεται στο ad hoc πρωτόκολλο GPSR, την ομαδοποίηση των κόμβων που βασίζεται στον προτεινόμενο αλγόριθμο εκλογής αρχηγών RRA, τη συνεργασία των κόμβων με κατανεμημένη διαδικασία ψηφοφορίας, την περιοδική παρακολούθηση του δικτύου και την ανίχνευση – αντίδραση στις εισβολές βάσει επιπέδων ασφαλείας και, τέλος, την ιδιωτικότητα/ακεραιότητα των επικοινωνιών και την αυθεντικότητα των κόμβων.

Η προτεινόμενη υλοποίηση ενοποιεί το στρώμα μεσισμικού και της δρομολόγησης των πακέτων και επίσης βασίζεται στην τεχνική μέθοδο “piggyback” ενσωμάτωσης της πληροφορίας ομαδοποίησης μέσα στα πακέτα που ανταλλάσουν οι κόμβοι στο επίπεδο του δικτύου. Αυτό

αποδεικνύεται με την περιγραφή του ρεπερτορίου των μηνυμάτων του σχήματος SC-GPSR το οποίο έχει ελαχιστοποιηθεί.

Στη συνέχεια του ίδιου Κεφαλαίου παρουσιάζεται η αξιολόγηση του προτεινόμενου σχήματος κάτω από μια σειρά από διαφορετικές δικτυακές συνθήκες (αριθμός κόμβων και αριθμός συνδέσεων TCP/UDP) και διαφορετικά σενάρια επιθέσεων, όπως έγχυση ψευδούς πληροφορίας, απόρριψη πακέτων, κλιμάκωση του αριθμού των επιθέσεων και τυχαία όπως και οργανωμένη τοποθέτηση των επιτιθεμένων που υλοποιούνται με το κατάλληλο εργαλείο δικτυακής προσομοίωσης. Τα πειραματικά αποτελέσματα που παρουσιάζονται δείχνουν πολύ καλή δικτυακή επίδοση (ρυθμο-απόδοση) του ενοποιημένου σχήματος και πολύ έγκαιρη ανίχνευση σχεδόν όλων των επιθέσεων που εκδηλώθηκαν σε διαφορετικούς χρόνους.

Στο έβδομο Κεφάλαιο διερευνάται η δυνατότητα μεταφοράς υπαρχόντων ενσύρματων κατανεμημένων συστημάτων και κατανεμημένων αρχιτεκτονικών σε ad hoc πλατφόρμες. Για το ad hoc περιβάλλον υποψήφια μοντέλα αντικειμενοστραφών κατανεμημένων συστημάτων που ξεχωρίσαμε για να χρησιμοποιηθούν στο στρώμα του μεσισμικού είναι το πελάτη/εξυπηρετητή, το SOA και το P2P. Γίνεται διερεύνηση και ανάλυση των χαρακτηριστικών των διαφορετικών μοντέλων επικοινωνιών και των κατάλληλων τεχνολογιών μεσισμικού για την ανάπτυξη εφαρμογών (για παράδειγμα ομαδοποίηση των κόμβων, ανακάλυψη ad hoc υπηρεσιών) βασισμένων στα υπό μελέτη πλαίσια. Ειδικότερα, εξετάζονται τρεις εναλλακτικές τεχνολογίες (sockets, XML, RMI) που αντιστοιχούν στα παραπάνω κατανεμημένα μοντέλα ως προς την ευκολία ανάπτυξης και ως προς τη συμπεριφορά τους σε συνθήκες κλιμάκωσης του αριθμού και του ρυθμού άφιξης των μηνυμάτων που δέχονται οι κόμβοι που τις φιλοξενούν. Οι τρεις υποψήφιες τεχνολογίες μεσισμικού δοκιμάστηκαν με συστηματικό τρόπο με κατάλληλο εργαλείο προσομοίωσης και με τρόπο ώστε οι περιπτώσεις δοκιμών που διεξήχθησαν να καλύπτουν ικανοποιητικά τους δυνατούς συνδυασμούς των παραμέτρων εισόδου. Τα αποτελέσματα των πειραμάτων έτυχαν στατιστικής επεξεργασίας που απέδειξε ότι το Peer-to-Peer μοντέλο είναι αυτό που κλιμακώνεται ικανοποιητικότερα, δηλαδή είναι αυτό που διατηρεί την καλύτερη επίδοση (ρυθμο-απόδοση και μέση καθυστέρηση) όταν τα αιτήματα αυξάνονται και άρα είναι πιο ανθεκτικό σε ένα εχθρικό ad hoc περιβάλλον. Επιπλέον, το Peer-to-Peer μοντέλο ταιριάζει με τη δομή του ad hoc δικτύου όπου οι νόμιμοι κόμβοι είναι ομότιμες οντότητες που συνεργάζονται για την προώθηση των μηνυμάτων.

Στο όγδοο Κεφάλαιο παρουσιάζονται τα γενικά συμπεράσματα της διατριβής και δίνονται οι κατευθύνσεις για μελλοντική έρευνα.

1.4. ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Asokan N. and Ginzboorg P. “Key-Agreement in Ad-hoc Networks”. In: Computer Communications. Special issue: advanced security techniques for network protection 2000, (vol. 23 no. 17), pp. 1627 - 1636.

[2] Stajano F. and Anderson R. “The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks”. In the 7th International Workshop on Security Protocols. Cambridge, UK, 1999.

[3] Yi S, Naldurg P, and Kravets R. “Security-Aware Ad-Hoc Routing for Wireless Networks”. Technical Report, University of Illinois, UIUCDCS-R-2001-2241, August 2001.

[4] Zhou L and Haas Z. “Securing Ad Hoc Networks”. IEEE Network, Vol. 13 (6), pp. 24—30, November, 1999.

[5] Zhang Y. and Lee W: “Intrusion Detection in Wireless Ad-Hoc Networks”. In: 6th ACM/IEEE Conference on Mobile Computing and Networking, Boston, USA, 2000.

2. ΑΠΑΙΤΗΣΕΙΣ ΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑΣ ΚΑΙ ΑΣΦΑΛΕΙΑΣ

Στο Κεφάλαιο που ακολουθεί παρουσιάζονται οι γενικές και οι ειδικές απαιτήσεις λειτουργικότητας και ασφαλείας που πρέπει να ικανοποιούν τα μοντέρνα ασύρματα δίκτυα ad hoc. Οι ειδικές απαιτήσεις λειτουργικότητας και ασφαλείας είναι άρρηκτα συνδεδεμένες και εξαρτώνται από τα χαρακτηριστικά των εφαρμογών αιχμής που αναπτύσσονται στα δίκτυα αυτά και καθορίζονται βάσει των πεδίων των εφαρμογών και των σεναρίων [2] που στοχεύει η ανάπτυξη ενός τέτοιου δικτύου. Για παράδειγμα, έχουμε τα πεδία των στρατιωτικών, περιβαλλοντικών, οικιακών, βιομηχανικών και πολυμεσικών ad hoc εφαρμογών για να αναφέρουμε ένα μικρό μόνο μέρος αυτών.

2.1. ΑΠΑΙΤΗΣΕΙΣ ΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑΣ

2.1.1. Επιβιωσιμότητα

Η επιβιωσιμότητα των δικτύων ad hoc χωρίς υποδομή συναρτάται με το χρόνο ζωής του δικτύου και το επίπεδο διαθεσιμότητας των εφαρμογών στον τελικό χρήστη παρουσία μειωμένης ισχύος, παρουσία τυχαίων σφαλμάτων (λόγω φυσικών καταστροφών, λόγω του καναλιού μετάδοσης, λόγω της κίνησης των κόμβων και άλλων τυχαίων παραγόντων που χαρακτηρίζουν την περιορισμένη ad hoc δικτυακή λειτουργία που αναλύσαμε πιο πάνω) και, επίσης, παρουσία στοχευμένων επιθέσεων. Το δίκτυο θα πρέπει να είναι έτσι σχεδιασμένο ώστε να μπορεί να παρακάμψει τα εμπόδια που προκύπτουν από τη μεγάλη δυναμικότητα στη συμπεριφορά των κόμβων, ιδίως σε συνθήκες απειλής από κακόβουλους κόμβους.

Μια άλλη σημαντική διάσταση της επιβιωσιμότητας είναι η αυτονομία των δικτύων. Η αυτονομία στα δίκτυα ad hoc εκτός από το προφανές της μακρόχρονης λειτουργίας των κόμβων δίχως ενεργειακή υποστήριξη από τη σταθερή υποδομή, σημαίνει και τη διαχείριση του δικτύου με μέσα αυτόνομα. Το πρώτο επιτυγχάνεται με τη σχεδίαση πρωτοκόλλων, αλγορίθμων και άλλων δικτυακών λύσεων που καταναλώνουν χαμηλό ποσό ενέργειας, δηλαδή λύσεων που λαμβάνουν υπόψη τη χαμηλή ενέργεια και ισχύ των κόμβων στο σχεδιασμό.

Το δεύτερο επιτυγχάνεται με τη λήψη αυτόνομων αποφάσεων από τους κόμβους που αφορούν στην οργάνωση του δικτύου αλλά και με αυτόνομες αποφάσεις που αφορούν στην αντίδραση στις μεταβολές της δομής του δικτύου ανάλογα με τις συνθήκες που επικρατούν, χωρίς να υπάρχει η δυνατότητα εξωτερικής διαχείρισης ή συντονισμού. Έτσι η αυτονομία των δικτύων ad hoc μπορεί να επεκταθεί με ικανοποιητικούς και αποδοτικούς τρόπους αυτό-οργάνωσης (εξοικονόμηση ενέργειας, προσαρμοστική αλλαγή δομής, εναλλαγή ρόλων και καθηκόντων μέσα στο δίκτυο, κ.α.) καθώς και με την αυτο-προστασία από τις απειλές. Το τελευταίο μπορεί να επιτευχθεί με την υιοθέτηση ενός σχήματος ανίχνευσης (“detection”) –αντίδρασης (“response”) –ανάκαμψης (“recovery”) από τις δυνατές επιθέσεις που όπως θα δούμε είναι πολλές και διαφορετικών τύπων.

Έτσι νέες αρχιτεκτονικές τόσο στο υλικό των κόμβων (όπως οι επαναπρογραμματιζόμενες αρχιτεκτονικές υλικού χαμηλής ενέργειας, π.χ. οι FPGA) όσο και στη διαχείριση του δικτύου (καινοτόμες αρχιτεκτονικές ασφαλούς αυτό-οργάνωσης) μπορούν να διασφαλίσουν την ορθή και αυτόνομη λειτουργία και να επεκτείνουν σε ένα μεγάλο βαθμό την επιβιωσιμότητα των δικτύων ad hoc.

2.1.2. Προσαρμοστικότητα

Οι αλγόριθμοι ελέγχου και διαχείρισης του δικτύου ad hoc πρέπει να είναι προσαρμοστικοί στις μεταβολές στις δικτυακές συνθήκες που προκύπτουν λόγω των ειδικών χαρακτηριστικών των

δικτύων αυτών και κυρίως λόγω της κινητικότητας των κόμβων που προκαλεί ραγδαίες αλλαγές στην τοπολογία του δικτύου. Αυτό σε ένα σχήμα αυτό-οργάνωσης των κόμβων με αυτόνομα μέσα μεταφράζεται στη δυνατότητα εναλλαγής μεταξύ ενός αριθμού από διακριτούς ρόλους τους οποίους οι κόμβοι θα πρέπει δυναμικά να αναλαμβάνουν προκειμένου να αντιμετωπίζουν τις αλλαγές στο δίκτυο πιο αποτελεσματικά. Η οργάνωση των κόμβων πρέπει να υποστηρίζει τους παρακάτω βασικούς διακριτούς ρόλους οι οποίοι καθορίζουν και τα διαφορετικά καθήκοντα των κόμβων μέσα στο δίκτυο:

- *Απλός Κόμβος*. Αυτοί είναι κόμβοι δίχως ιδιαίτερα καθήκοντα εκτός της προώθησης των μηνυμάτων δεδομένων. Σε ένα WSN είναι τα μικροσκοπικά motes ενώ σε ένα MANET είναι οι μικρές ομότιμες προσωπικές συσκευές, όπως τα Mobile Internet Devices, PDA, laptop και palmtop.

- *Κόμβος αρχηγός*. Είναι οι κόμβοι που συγκεντρώνουν, επεξεργάζονται και προστατεύουν τα δεδομένα πριν τα προωθήσουν προς τον τελικό προορισμό.

- *Κόμβος Σταθμός Βάσης*. Στα δίκτυα WSN είναι ο κόμβος που συλλέγει τα δεδομένα από όλους τους αισθητήρες για τους οποίους αποτελεί τον τελικό προορισμό.

- *Κόμβος Πύλη*. Είναι ο κόμβος που αποτελεί τη διεπαφή μεταξύ του δικτύου ad hoc και των εξωτερικών δικτύων όπως το Διαδίκτυο, το δίκτυο GSM, το δορυφορικό δίκτυο, το WLAN, το GPRS κ.α.). Για τα WSN ο υπολογιστής με το οποίο συνδέεται ο κόμβος σταθμός βάσης αποτελεί τον κόμβο πύλη προς το Διαδίκτυο.

- *Επιχειρησιακό Κέντρο*. Είναι συνδεδεμένο με το δίκτυο ad hoc μέσω του Διαδικτύου αποτελώντας το κέντρο ελέγχου της λειτουργίας ενός δικτύου ad hoc, π.χ. δίκτυο WSN στρατιωτικών εφαρμογών.

- *Εξωτερική Οντότητα*. Πρόκειται για το τρίτο μέρος που μπορεί να έχει πρόσβαση στα δεδομένα που συγκεντρώνονται είτε ενδο-δικτυακά σε ισχυρούς κόμβους του WSN είτε σε δεδομένα που φυλάσσονται σε εξωτερική βάση δεδομένων. Σε ένα τέτοιο μοντέλο ανάπτυξης υπάρχει προσανατολισμός στα δεδομένα (“data-centric”) και την ενδο-δικτυακή επεξεργασία (“in-network processing”). Παραδείγματα εφαρμογών αυτού του μοντέλου είναι η χρήση της γλώσσας επεξεργασίας δεδομένων που προέρχονται από μικροσκοπικούς αισθητήρες που ονομάζεται “tinySQL” (“SELECT max (value) FROM senors_id WHERE value > threshold, sample period 60msecs”) με ερωτήσεις προς τη βάση “tinyDB”.

Με τις κατάλληλες τεχνολογίες μεσισμικού, όπως την αναζήτηση και τη διαχείριση ad hoc υπηρεσιών και την κατάλληλη μετατροπή των πρωτοκόλλων μεταξύ των ad hoc δικτύων και του Διαδικτύου οι υπηρεσίες του Παγκόσμιου Ιστού μπορεί να θεωρηθούν σαν συνέχεια των αυτόνομων δικτύων ad hoc. Με αυτόν τον τρόπο μπορούμε να έχουμε ολοκλήρωση των ad hoc υπηρεσιών του μικρού κόσμου και των υπηρεσιών του Παγκόσμιου Ιστού.

2.1.3. Ετερογένεια

Το ad hoc δίκτυο θα πρέπει να μπορεί να λειτουργεί και με ετερογενείς κόμβους, δηλαδή να είναι δυνατόν οι κόμβοι να έχουν διαφορετικές δυνατότητες τόσο από την πλευρά του υλικού όσο και από την πλευρά του λογισμικού που διαθέτουν.

Ετερογενείς πλατφόρμες υλικού. Μια μοντέρνα απαίτηση για το δίκτυο ad hoc είναι η διαλειτουργικότητα έτσι ώστε να μπορούν να επικοινωνούν κόμβοι που διαθέτουν διαφορετικό υλικό. Έτσι μπορεί στο δίκτυο να συνυπάρχουν πολύ μικροί κόμβοι με μικρές δυνατότητες στην

επεξεργαστική ισχύ, στην αποθηκευτική ικανότητα και στη ραδιο-μετάδοση (για παράδειγμα ακτίνα κάλυψης όχι μεγαλύτερη από 150 μέτρα ή ρυθμός μετάδοσης όχι μεγαλύτερος από 200kbps) όπως και πιο ισχυροί κόμβοι της κλάσης laptop οι οποίοι μπορούν να εκτελέσουν τα καθήκοντα της ομαδοποίησης σε ομάδες, της προστασίας των υπολοίπων κόμβων, ή της τοπικής αποθήκευσης, του μοιράσματος και της επεξεργασίας δεδομένων που μπορούν να έχουν τη μορφή εικόνας ή ακόμη και video. Η ετερογένεια στο υλικό μπορεί να επιτευχθεί με πρωτόκολλα στο επίπεδο της ad hoc εφαρμογής που αφαιρούν λογικά το φυσικό επίπεδο των επιμέρους συσκευών, όπως το πρωτόκολλο ZigBee 802.15.4 με τις λογικές αναπαραστάσεις των συσκευών ZigBee Device Objects (ZDO).

Ετερογενή πεδία διαχείρισης. Επίσης καινοτόμα είναι τα ad hoc δίκτυα που μπορούν να αναπτυχθούν κατά μήκος πολλών και διαφορετικών διαχειριστικών πεδίων τα οποία διέπονται από διακριτές πολιτικές διαχείρισης και ελέγχου των υπηρεσιών και των δικτύων κυρίως όσον αφορά τους κανόνες ασφάλειας.

Ετερογενή πρωτόκολλα και αλγόριθμοι. Στο ίδιο πλαίσιο, είναι μια μοντέρνα απαίτηση το δίκτυο να μπορεί να υποστηρίξει πολλά διαφορετικά πρωτόκολλα και αλγορίθμους, για παράδειγμα να χρησιμοποιούνται διαφορετικοί αλγόριθμοι σε διαφορετικές γεωγραφικές περιοχές όπου επικρατούν διαφορετικές συνθήκες. Για παράδειγμα σε μια περιοχή η λειτουργία θα πρέπει να διασφαλίζεται περισσότερο από κάποια άλλη περιοχή που απειλείται σε λιγότερο βαθμό. Συνήθως η διαλειτουργικότητα επιτυγχάνεται με τη χρήση του πρωτόκολλου IP.

2.1.4. Ασφαλής Αναφορά Θέσης

Οι νέες εφαρμογές ad hoc απαιτούν τόσο την ταυτοποίηση των κόμβων όσο και την ακριβή αναφορά θέσης των κόμβων. Αυτή είναι μια ιδιαίτερη απαίτηση των δικτύων αισθητήρων τα οποία λειτουργούν χωρίς επίβλεψη, αλλά και των δικτύων MANET και των Vehicular Ad Hoc Nteworks (VANET), όπου η αυτόματη ανίχνευση της θέσης των κόμβων είναι εξίσου σημαντική. Ακόμη η ανίχνευση της θέσης θα πρέπει να είναι ασφαλής από σφάλματα και επιθέσεις ιδιαίτερα σε αυτού του είδους τα δίκτυα όπου πολλές φορές οι εισβολείς προκειμένου να παραπλανήσουν τους υπόλοιπους μεταδίδουν μη ακριβείς συντεταγμένες θέσης. Για παράδειγμα σε μια εφαρμογή έξυπνων δρόμων στην οποία τα αυτοκίνητα είναι εφοδιασμένα με αισθητήρες που μεταδίδουν τη θέση τους σε σταθμούς βάσης που τοποθετούνται κατά μήκος των πλευρών του δρόμου, πολύ εύκολα ένας κακόβουλος χρήστης μπορεί να προκαλέσει σύγχυση στο σύστημα με το να μεταδίδει ψευδή πληροφορία ως προς τη θέση του στο οδικό δίκτυο καθώς και λανθασμένες αναφορές για την κυκλοφοριακή κίνηση ή τις περιβαλλοντικές συνθήκες που επικρατούν σε αυτό. Έτσι προκύπτει η ανάγκη εκτός από τα συστήματα GPS οι εφαρμογές αυτές όπου η θέση παίζει σημαντικό ρόλο να προστατεύονται από αλγορίθμους που εξασφαλίζουν αυτόματα και με μεγάλη ακρίβεια (μέχρι και ένα μέτρο) ότι η θέση που ισχυρίζεται κάποιος κόμβος είναι αληθής, έτσι ώστε να είναι δυνατό να ανιχνεύεται ο εισβολέας. Οι τεχνικές μέθοδοι που επιτυγχάνουν το σκοπό αυτό είναι:

- Η προστασία των μηνυμάτων που περιέχουν αναφορές με τη θέση των κόμβων. Έτσι σε ένα δίκτυο που χρησιμοποιεί περιοδικά σήματα φάρων (πακέτα Beacon ή αλλιώς πακέτα Hello) για την ανακάλυψη των γειτονικών κόμβων με ένα πρωτόκολλο όπως το Neighborhood Discovery Protocol (NHDP, draft-ietf-manet-nhdp-05, [20]) θα πρέπει με τα κατάλληλα σχήματα κωδικοποίησης των δεδομένων και τα κατάλληλα σχήματα διαχείρισης κλειδιών αυτή η ευαίσθητη πληροφορία να μεταδίδεται με ασφαλή τρόπο.

- Το πρωτόκολλο δρομολόγησης να λαμβάνει υπόψη τη θέση των κόμβων (όπως για παράδειγμα κάνουν τα γεωγραφικά πρωτόκολλα δρομολόγησης).

- Η ύπαρξη ενός ικανοποιητικού αριθμού από κόμβους-άγκυρες (“anchors”) μέσα στο δίκτυο. Αυτοί είναι κόμβοι γνωστής θέσης με βάση τα εκπεμπόμενα σήματα των οποίων γίνεται η εκτίμηση αν η θέση που αναφέρει κάποιος κόμβος είναι αληθής ή ψευδής.

- Αλγόριθμους τριγωνοποίησης, αν πρόκειται για τον ασφαλή προσδιορισμό της θέσης στο επίπεδο, οι οποίοι με βάση τις διαθέσιμες μετρήσεις εξάγουν με δεδομένη ακρίβεια (μικρότερη και από ένα μέτρο, έως και μερικά cm καθώς οι τεχνολογίες εξελίσσονται) τη θέση ενός κόμβου μέσα στο δίκτυο. Αν προκύπτει ότι η θέση είναι εκτός των νόμιμων ορίων της επιφάνειας που καλύπτει το δίκτυο, τότε πρόκειται για μη νόμιμο κόμβο. Απαραίτητη προϋπόθεση είναι η ύπαρξη των κόμβων με γνωστές συντεταγμένες που λειτουργούν ως κόμβοι-αναφοράς (“anchors”) μέσα στο δίκτυο.

2.1.5. Ευρυζωνικό Ad Hoc

Οι τρέχουσες πολυμεσικές εφαρμογές που σήμερα αναπτύσσονται καθώς και η προστασία των δεδομένων στα ad hoc δίκτυα MANET, WSN και VANET απαιτούν τα δίκτυα ad hoc να υποστηρίζονται από τεχνολογίες ευρείας ζώνης. Αυτό σημαίνει ότι ονομαστικά σε ένα MANET θα υποστηρίζονται με τις κατάλληλες ασύρματες κάρτες δεδομένων ρυθμοί μέχρι και 200Mbps ενώ ένα WSN θα πρέπει να υποστηρίζει, με τους κατάλληλους πομπούς στους αισθητήρες (τεχνολογία CHIPCON RF) τουλάχιστον 250kbps για τη μετάδοση στατικής εικόνας. Ακόμη, οι απαιτήσεις για μεγαλύτερη ακτίνα κάλυψης αυξάνονται και φθάνουν μέχρι και τα 50km (802.11n). Περαιτέρω, είναι γνωστό ότι οι κρυπτογραφικές πράξεις επιβάλλουν επιπλέον bits σε ένα πακέτο που προστατεύεται. Αυτός είναι ένας ακόμη λόγος που θα πρέπει να μπορεί το δίκτυο να λειτουργεί σε υψηλότερους ρυθμούς μετάδοσης των δεδομένων στο ασύρματο κανάλι. Απαραίτητη προϋπόθεση των πιο πάνω είναι η αύξηση της ικανότητας επεξεργασίας του υλικού να συνοδεύεται και από τη διατήρηση της καταναλισκόμενης ενέργειας σε ανεκτά επίπεδα, διαφορετικά ο χρόνος ζωής των συσκευών θα είναι αρκετά μειωμένος.

2.1.6. Συγχρονισμός

Ο συγχρονισμός είναι μια απαίτηση αρκετών πρωτοκόλλων ad hoc τόσο στο επίπεδο ελέγχου της πρόσβασης (παράδειγμα το σχήμα πολυπλεξίας TDMA), όσο και στο επίπεδο του δικτύου και της δρομολόγησης των πακέτων. Με τον ασφαλή συγχρονισμό (δηλαδή την προστασία της ευαίσθητης πληροφορίας χρονισμού με κρυπτογραφικές μεθόδους, όπως για παράδειγμα τη χρήση και προστασία ενός πεδίου ακολουθίας αριθμών στα πακέτα που μεταδίδονται) επιτυγχάνεται η ορθή λήψη των δεδομένων των χρηστών αλλά, κυρίως, επιτυγχάνεται ανοχή σε επιθέσεις κατά του χρονισμού, όπως η επίθεση επανάληψης μηνυμάτων, η επίθεση αλλοίωση και καθυστέρησης των χρονοσφραγίδων οι οποίες μεταδίδονται μέσα στα πακέτα συγχρονισμού, η επίθεση καθυστέρησης παλμού (“pulse-delay attack”), ο χρονισμός με βάση ένα κακόβουλο κόμβο κ.α. Οι επιθέσεις χρονισμού θέτουν σε κίνδυνο την ασφάλεια των επικοινωνιών. Ο συγχρονισμός μπορεί να είναι ελαστικός και απαιτητικός και επίσης μπορεί να υλοποιηθεί με την εκπομπή των περιοδικών σημάτων φάρων (“beacons”). Για μια σύγκριση των σχημάτων συγχρονισμού στα δίκτυα με αισθητήρες δες [9], [10] και [11].

2.2. ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

Οι γενικές απαιτήσεις ασφαλείας για τα δίκτυα ad hoc έχουν καθοριστεί με ακρίβεια στις εργασίες [3], [4], [5]. Οι γενικές απαιτήσεις ασφαλείας αποτελούν το ελάχιστο πλαίσιο προστασίας που πρέπει να παρέχουν οι τεχνικές λύσεις προκειμένου να διασφαλίζεται η λειτουργία του δικτύου και να προστατεύονται οι νόμιμοι χρήστες των υπηρεσιών του από τα δυνατά σενάρια των κακόβουλων επιθέσεων.

Εν συντομία, αυτές οι βασικές απαιτήσεις ασφαλείας περιλαμβάνουν τα ακόλουθα. Η

εμπιστευτικότητα και η ακεραιότητα της πληροφορίας είναι δύο βασικές απαιτήσεις ασφαλείας που είναι δυνατό να επιτευχθούν με γνωστούς συμμετρικούς ή ασύμμετρους κρυπτογραφικούς μηχανισμούς, με την προϋπόθεση ότι οι κόμβοι του δικτύου μπορούν να αποδείξουν με ασφάλεια την ταυτότητά τους και να αυθεντικοποιηθούν στους υπόλοιπους κόμβους του δικτύου. Η διαθεσιμότητα του δικτύου μπορεί να υποστηριχθεί με τεχνικές πλεονασμού. Για να επικοινωνήσουν δύο κόμβοι και να εξασφαλίσουν τη διαθεσιμότητα των καναλιών επικοινωνίας έναντι κακόβουλων κόμβων που προσπαθούν να προκαλέσουν επιθέσεις άρνησης εξυπηρέτησης, είναι αναγκαία η χρήση διαφορετικών δρομολόγησης και με βάση αυτή την αρχή έχουν προταθεί διάφορα πρωτόκολλα δρομολόγησης [13], [14]. Όμως, τα πρωτόκολλα αυτά είναι επίσης ευάλωτα σε επιθέσεις συνεργασίας κακόβουλων κόμβων. Τέλος, για την επίτευξη του στόχου της επιβιωσιμότητας του δικτύου οι παραπάνω τεχνικές πρέπει να συνδυαστούν και να γενικευτούν ώστε να διατηρείται η συνεκτικότητα του δικτύου, ακόμα και σε περίπτωση γενικευμένων επιθέσεων. Ακολουθεί περιγραφή των απαιτήσεων αυτών με μεγαλύτερη λεπτομέρεια.

2.2.1. Αυθεντικοποίηση

Η αυθεντικοποίηση πρωτίστως αποκαλύπτει την ταυτότητα των συσκευών και των χρηστών που συμμετέχουν στις επικοινωνίες μέσα σε ένα δίκτυο ad hoc, δηλαδή επιτρέπει σε κάθε κόμβο να επιβεβαιώνει την ταυτότητα των υπολοίπων κόμβων. Στη συνέχεια, μπορεί πλέον να πιστοποιηθεί η γνησιότητα και η νομιμότητα των συσκευών/τερματικών/χρηστών. Η αυθεντικοποίηση είναι βασική απαίτηση ασφάλειας σε όλα τα δίκτυα γιατί είναι αναγκαίο να υπάρχει εμπιστοσύνη ότι τα δεδομένα του δικτύου ad hoc προέρχονται από νόμιμους κόμβους και όχι από κόμβους που έχουν διεισδύσει στο δίκτυο παράνομα χωρίς να ανήκουν σε αυτό. Συνεπώς, με τα ποικίλα πρωτόκολλα αυθεντικοποίησης επιτυγχάνεται η αναγνώριση της ταυτότητας του κόμβου που έστειλε τα μηνύματα και, συνεπώς, είναι δυνατόν κατόπιν να διαπιστωθεί η νομιμότητα ή όχι του κόμβου αυτού.

Με την αυθεντικοποίηση είναι εύλογο ότι μπορεί να διασφαλιστεί ότι οι πόροι του δικτύου δε θα κινδυνεύουν από χρήση από μη εξουσιοδοτημένους κόμβους. Έτσι, η αυθεντικοποίηση καθορίζει αν πράγματι έχει τα δικαιώματα κάποια συσκευή να κάνει χρήση των πόρων του δικτύου κάτι που είναι γνωστό και σαν διαδικασία εξουσιοδότησης (authorization), δηλαδή αναγνώριση του ποιος χρήστης έχει ποια δικαιώματα χρήσης και σε ποιους πόρους του δικτύου και των συστημάτων.

Η συνήθης πρακτική για αυθεντικοποίηση είναι η χρήση Υποδομής Δημοσίου Κλειδιού PKI (Public Key Infrastructure) σε συνδυασμό με κρυπτοσυστήματα δημοσίου κλειδιού. Για την εφαρμογή Υποδομής Δημοσίου Κλειδιού σε ad hoc περιβάλλον έχει προταθεί η χρήση μιας προωθημένης αρχής πιστοποίησης (forward area) [13], [14], η οποία κάνοντας χρήση κρυπτογραφικών μηχανισμών κατωφλίου και προληπτικών μηχανισμών άμυνας (“proactive”) [14, 15, 16, 17, 18, 19] επιτυγχάνει δυναμική αυθεντικοποίηση των κόμβων σε περιβάλλον κακόβουλων επιθέσεων. Όμως η τεχνική αυτή δεν επιτρέπει τη δυναμική ανάκληση κλειδιών σε περίπτωση συνεργασίας κακόβουλων κόμβων.

2.2.2. Εμπιστευτικότητα

Επίσης, πολύ βασική απαίτηση είναι η διασφάλιση του απορρήτου των επικοινωνιών. Τα δεδομένα θα πρέπει να προστατεύονται με διάφορους αλγορίθμους κρυπτογράφησης έτσι ώστε οι κόμβοι που έχουν τη δυνατότητα να ακούσουν και να συλλάβουν την ακολουθία των μηνυμάτων μέσα σε ένα δίκτυο να μην μπορούν να αποκρυπτογραφήσουν τη συνομιλία, εκτός αν είναι νόμιμοι κόμβοι που κατέχουν το κατάλληλο μυστικό υλικό. Το απαιτούμενο επίπεδο προστασίας των δεδομένων από τους ωτακουστές εξαρτάται από την εφαρμογή ad hoc που υποστηρίζεται από το δίκτυο. Για παράδειγμα, σε μια στρατιωτική εφαρμογή τα μηνύματα πρέπει να μεταδίδονται ισχυρώς κρυπτογραφημένα, ενώ σε μια περιβαλλοντική εφαρμογή οι απαιτήσεις για εμπιστευτικότητα των

δεδομένων που συλλέγονται από τους αισθητήρες είναι πολύ πιο χαλαρές. Η εμπιστευτικότητα των δεδομένων μπορεί να επιτευχθεί τεχνικώς με συμμετρικούς και με μη συμμετρικούς αλγορίθμους κρυπτογράφησης. Για το περιορισμένο περιβάλλον ad hoc οι τεχνικές κρυπτογράφησης που ενδείκνυνται ανήκουν συνήθως στην κατηγορία των συμμετρικών κρυπτοσυστημάτων.

2.2.3. Ακεραιότητα των Δεδομένων

Η ακεραιότητα των δεδομένων διασφαλίζει ότι τα μηνύματα δε μεταβάλλονται κατά τη διάδοσή τους μέσα στο δίκτυο. Έτσι με τη διασφάλιση της ορθότητας των δεδομένων που μεταδίδονται από μια πηγή σε ένα τελικό κόμβο, αντιμετωπίζονται εκείνες οι ενεργητικές επιθέσεις που έχουν να κάνουν με την αλλοίωση των μηνυμάτων από ενδιάμεσους κακόβουλους χρήστες που στοχεύουν στην πρόκληση συγχύσεως στα δύο επικοινωνούντα μέρη με την αποστολή μη αυθεντικών μηνυμάτων. Επιπλέον, η αλλοίωση των δεδομένων στο ασύρματο μέσο είναι πιθανό να οφείλεται και στην κακή ποιότητα των ασύρματων ζεύξεων μεταξύ των κόμβων, κάτι το οποίο αναγνωρίζεται με τη χρήση του πεδίου/σφραγίδας CRC (“Cyclic Redundancy Check”) που υπολογίζεται και προστίθεται ανά πακέτο που μεταδίδεται από τον πομπό.

Η συνηθέστερη λύση για τη διασφάλιση της ακεραιότητας των δεδομένων είναι οι ψηφιακές υπογραφές.

2.2.4. Ιδιωτικότητα

Η ιδιωτικότητα είναι μια πολύ σημαντική απαίτηση που συναντάμε ακόμη και στα δίκτυα ad hoc δίχως υποδομή. Η ιδιωτικότητα διασφαλίζει ότι η ευαίσθητη πληροφορία των κόμβων και των χρηστών του δικτύου ad hoc, όπως η ταυτότητα των κόμβων, η γεωγραφική τους θέση καθώς και κάθε άλλης ιδιωτικής φύσεως πληροφορία, όπως για παράδειγμα το ιατρικό ιστορικό χρηστών που κάνουν χρήση συσκευών ad hoc ιατρικής υποστήριξης, δεν γίνεται δημόσια γνωστή και προσβάσιμη από μη εξουσιοδοτημένους χρήστες που μπορούν να τη χρησιμοποιήσουν για δικούς τους σκοπούς.

2.2.5. Διαθεσιμότητα

Η διαθεσιμότητα είναι συγχρόνως μια λειτουργική απαίτηση όσο και μια απαίτηση που σχετίζεται με το βαθμό προστασίας που χαρακτηρίζει το σύστημα έναντι των τυχαίων σφαλμάτων που οφείλονται στα χαρακτηριστικά διάδοσης του ασύρματου μέσου αλλά και έναντι των επιθέσεων που στόχο έχουν την κατάρρευσή του. Είναι επιθυμητό να διατίθενται με υψηλό ποσοστό διαθεσιμότητας όχι μόνο οι υπηρεσίες στο επίπεδο του δικτύου αλλά και οι end-to-end υπηρεσίες και εφαρμογές θα πρέπει να είναι προσβάσιμες από τους τελικούς χρήστες κατά το μεγαλύτερο ποσοστό του χρόνου. Από την πλευρά της δικτυακής λειτουργικότητας η διαθεσιμότητα στο δίκτυο ad hoc είναι άρρηκτα συνδεδεμένη με την επιβιωσιμότητα, δηλαδή τελικά με τα ενεργειακά αποθέματα των κόμβων. Ο αποδοτικός σχεδιασμός των δικτυακών πρωτοκόλλων με τρόπο που να διασφαλίζεται μακρύς χρόνος ζωής για το σύστημα με χαμηλή κατανάλωση ενέργειας για τους κόμβους είναι πρωταρχικής σημασίας για τη διαθεσιμότητα του δικτύου.

Από την πλευρά της ασφάλειας η διαθεσιμότητα των υπηρεσιών απειλείται από επιθέσεις που στοχεύουν στην εξάντληση των αποθεμάτων των πόρων των κόμβων έτσι ώστε να προκαλούνται πτώσεις αυτών και άρα το δίκτυο να καθίσταται κατατμημένο με αποτέλεσμα να μην μπορεί να διεξάγει επιτυχώς τη διαβίβαση των μηνυμάτων. Τέτοιες επιθέσεις είναι η επίθεση άρνησης εξυπηρέτησης υπηρεσίας, η πλημμύρα πακέτων στο επίπεδο της δρομολόγησης και οι ισχυρές παρεμβολές στο φυσικό επίπεδο του ραδιοφάσματος που καταστρέφουν τις επικοινωνίες. Είναι εύλογο ότι το δίκτυο θα πρέπει να διαθέτει μηχανισμούς άμυνας σε επιθέσεις και διαδικασίες ανάκαμψης από τυχαία και ηθελημένα σφάλματα οι οποίοι θα πρέπει να σχεδιάζονται με στόχο τη

μικρή κατανάλωση των υπολογιστικών, ενεργειακών και αποθηκευτικών πόρων των κόμβων.

2.2.6. Αποποίηση Ευθύνης

Οι κακόβουλοι κόμβοι δεν μπορούν να κρύψουν ή να αρνηθούν τις δραστηριότητές τους και τα μηνύματα που μετέδωσαν μέσα στο δίκτυο.

Όπως ήδη διαπιστώσαμε τα δίκτυα ad hoc έχουν εγγενή χαρακτηριστικά (περιορισμούς στους κόμβους και ένα ανοιχτό κανάλι επικοινωνίας που μπορεί πολύ εύκολα να παγιδευτεί) που τα καθιστούν περισσότερο ευάλωτα στις επιθέσεις. Επιπλέον, δεδομένου ότι οι εφαρμογές των ad hoc δικτύων ολοένα διευρύνονται, είναι επόμενο οι απειλές που μπορεί να εμφανιστούν να αυξάνονται - τόσο στον αριθμό όσο και στους δυνατούς τύπους και τους σκοπούς των επιθέσεων που εκδηλώνουν οι κακόβουλοι κόμβοι. Είναι συνεπώς αναγκαίο να επεκτείνουμε τα μέτρα πρόληψης περιλαμβάνοντας και τις παρακάτω απαιτήσεις ασφαλείας όσον αφορά τα δίκτυα ad hoc.

2.2.7. Προστασία του Συστήματος Ασφάλειας

Ένας επιτιθέμενος εκτός από τους βασικούς μηχανισμούς της δικτυακής λειτουργίας (για παράδειγμα το πρωτόκολλο δρομολόγησης ή τη μεταφορά και την ανταλλαγή μηνυμάτων από άκρη σε άκρη στο επίπεδο της εφαρμογής) μπορεί να επιτεθεί και κατά του ιδίου του συστήματος ασφάλειας [5]. Έτσι είναι δυνατόν επίθεση να δεχθεί και το ίδιο το σύστημα ανίχνευσης και αντιμετώπισης εισβολών και συνεπώς σκοπός του επιτιθέμενου μπορεί να είναι να συμβιβάσει κάποιο κόμβο-πράκτορα του IDS με απώτερο στόχο αυτός ο IDS κόμβος να μεταδίδει ψευδείς συναγερμούς όσον αφορά τους ύποπτους κόμβους, ή να αποκρύπτει τους πραγματικούς εισβολείς στο δίκτυο. Επίσης, είναι πιθανόν ένας επιτιθέμενος να κρυφακούει και να αλλοιώνει τα μηνύματα και τους συναγερμούς που ανταλλάσσουν οι κόμβοι του συστήματος IDS. Συνεπώς είναι ανάγκη τα μηνύματα μεταξύ των πρακτόρων IDS να προστατεύονται ανάλογα.

Ένας άλλος τρόπος να χτυπηθεί το σύστημα ασφάλειας είναι για παράδειγμα μια επίθεση ωμής βίας ή όποια άλλη πιο έξυπνη επίθεση κατά του αλγορίθμου κρυπτογράφησης που χρησιμοποιείται από το σύστημα για την προστασία των δεδομένων του IDS. Επίσης, οι εξειδικευμένες επιθέσεις κατά του συστήματος διαχείρισης κλειδιών ή κατά των πρωτοκόλλων και σχημάτων δημιουργίας κλειδιών μέσα στο δίκτυο ad hoc αποτελούν επιθέσεις κατά του ίδιου του συστήματος ασφαλείας που θα πρέπει να λαμβάνονται εξίσου σοβαρά υπόψη [7], [8] κατά τη σχεδίαση. Έτσι είναι αναγκαίο τα κλειδιά να δημιουργούνται με δυναμικούς μηχανισμούς, θα πρέπει να παρέχεται η δυνατότητα να προστατεύουν τους κόμβους ανά ομάδες, να έχουν παροδική ισχύ και να κρυπτο-προστατεύονται.

Συνεπώς, είναι άκρως επιθυμητό στο δίκτυο ad hoc οι ίδιοι οι μηχανισμοί προστασίας του δικτύου, όποιοι κι αν είναι αυτοί, να παρουσιάζουν ανοχή στις επιθέσεις.

2.2.8. Προσαρμοζόμενα Επίπεδα Ασφαλείας

Είναι η ικανότητα το σύστημα προστασίας να υιοθετεί και να προσαρμόζεται σε διακριτά επίπεδα ασφαλείας ανάλογα με τους διαθέσιμους πόρους των κόμβων και ανάλογα και με το βαθμό απειλής που δέχεται από τους κακόβουλους κόμβους. Αυτό σημαίνει ότι τα αντίμετρα προστασίας είναι προσαρμοζόμενα στις συνθήκες των απειλών. Η σχεδίαση αλγορίθμων και πρωτοκόλλων ασφάλειας ειδικά για τα δίκτυα ad hoc πρέπει να έχει ως στόχο την προσαρμοστικότητα στο επίπεδο των απειλών οι οποίες θα πρέπει πρώτα να ανιχνευθούν με επαρκή ακρίβεια. Η απόφαση αν η προστασία θα είναι χαλαρή ή ισχυρή βασίζεται στην επεξεργασία των δεδομένων δικτυακής κίνησης που συλλέγονται από το σύστημα προστασίας του δικτύου.

2.2.9. Ανοχή σε Επιθέσεις

Είναι η ικανότητα του συστήματος ο αντίκτυπος μιας επιτυχούς επίθεσης εναντίον του να φέρνει μικρό κακό αποτέλεσμα. Για παράδειγμα ο κακόβουλος χρήστης δεν μπορεί να εκμεταλλευτεί την κατάληψη ενός αισθητήρα εφόσον το υλικό του αισθητήρα διασφαλίζεται επαρκώς με τις κατάλληλες μεθόδους προστασίας στο φυσικό επίπεδο. Ακόμη, η υποκλοπή κρυφών πιστοποιητικών ασφαλείας δε θα μπορεί να επιφέρει μεγάλη ζημιά στις επικοινωνίες εφόσον αυτό γίνεται έγκαιρα αντιληπτό και εφόσον το κρυφό υλικό ανανεώνεται καταλλήλως.

2.2.10. Αποδοτική Διαχείριση Κλειδιών

Σήμερα αναπόσπαστο κομμάτι του συστήματος ασφαλείας στα δίκτυα υποδομών αλλά και στα δίκτυα χωρίς υποδομή αποτελεί το σύστημα διαχείρισης των κλειδιών με το οποίο προστατεύονται τα δεδομένα από υποκλοπές και αυθεντικοποιούνται οι χρήστες, [7], [8]. Τα σχήματα διαχείρισης των κλειδιών προστατεύουν τις επικοινωνίες κυρίως στο επίπεδο της διασύνδεσης των δεδομένων. Ωστόσο η ανταλλαγή κλειδιών είναι επίσης συχνή στο επίπεδο του δικτύου και είναι απαραίτητη στο επίπεδο των από-άκρη-σε-άκρη ασφαλών εφαρμογών με αποτέλεσμα η διαχείριση των κλειδιών να αποτελεί μια πολυ-στρωματική διαδικασία. Στα δίκτυα MANET και WSN είναι πολύ σημαντική η διαδικασία της ασφαλούς διανομής και της ασφαλούς ανταλλαγής των πολλαπλών κλειδιών που δημιουργούνται δυναμικά ή εγκαθίστανται εξ αρχής στους κόμβους του δικτύου. Η διαχείριση των κλειδιών περιλαμβάνει τις παρακάτω λειτουργίες:

- *Εγκατάσταση των κλειδιών*. Τα κλειδιά είναι δυνατόν να είναι προφορτωμένα στους κόμβους ή να δημιουργούνται κατά την περίοδο της λειτουργίας του δικτύου. Σε κάθε περίπτωση θα πρέπει να είναι δυνατά κλειδιά των οποίων η δημιουργία περιλαμβάνει κάποια τυχαία συνιστώσα, όπως για παράδειγμα μια συνιστώσα χρόνου ή κάποια τυχαία ακολουθία δεδομένων (2 τυχαίων bytes για παράδειγμα) που παράγεται μία και μόνο φορά από το σύστημα γνωστή και ως “nonce”.

- *Διανομή - Ανταλλαγή των κλειδιών*. Ο τρόπος διανομής αλλά και ανταλλαγής των κλειδιών μεταξύ των κόμβων θα πρέπει να είναι ασφαλής.

- *Ανανέωση των κλειδιών*. Τα κλειδιά πρέπει να ανανεώνονται σε τακτά χρονικά διαστήματα ώστε η πρόβλεψή τους να είναι δύσκολη. Επίσης, νέα κλειδιά θα πρέπει να δημιουργούνται όταν νέοι κόμβοι εισέρχονται σε μια ομάδα του δικτύου ενώ τα κλειδιά κόμβων που απέρχονται από μια ομάδα (ή κόμβων των οποίων η ενέργεια έχει εξαντληθεί) πρέπει να διαγράφονται. Ταυτόχρονα τα υπόλοιπα κλειδιά της ομάδας θα πρέπει να ανανεώνονται. Οι διαδικασίες αυτές θα πρέπει να περιλαμβάνονται στη διαχείριση των κλειδιών κατά ομάδες.

Οι απαιτήσεις σε σχέση με τη διαχείριση των κλειδιών στο δίκτυο ad hoc περιλαμβάνουν:

- *Αποδοτικότητα*. Οι περιορισμοί στην επεξεργαστική ισχύ, την αποθηκευτική ικανότητα και την περιορισμένη μετάδοση δεδομένων στα δίκτυα ad hoc θέτουν τις αντίστοιχες απαιτήσεις κατά τη δημιουργία κλειδιών στα δίκτυα αυτά. Θα πρέπει η δημιουργία των κλειδιών να μην είναι ενεργοβόρα, να καταναλώνει δηλαδή μικρή επεξεργαστική ισχύ, το μέγεθος των κλειδιών να είναι ικανοποιητικά μικρό για τις περιορισμένες μεταδόσεις και την περιορισμένη μνήμη, τα απαιτούμενα μηνύματα που ανταλλάσσονται για την εγκατάσταση των κλειδιών πρέπει να είναι λίγα σε αριθμό και ταυτόχρονα θα πρέπει το επίπεδο ασφάλειας που επιτυγχάνεται με τα κλειδιά να είναι ικανοποιητικό.

- *Προσαρμοστικότητα στις δικτυακές συνθήκες*. Αφορά στο μηχανισμό ανανέωσης των κλειδιών όταν οι συνθήκες το απαιτούν, δηλαδή όταν κόμβοι προστίθενται ή αποχωρούν από το δίκτυο ή ακόμη όταν κόμβοι συμβιβάζονται από επιτιθέμενους.

- *Κλιμάκωση*. Είναι η ικανότητα του σχήματος κλειδιών να υποστηρίζει μεγάλα δίκτυα, αποτελούμενα από περισσότερους από 1000 κόμβους. Οι λειτουργίες του σχήματος διαχείρισης των κλειδιών που είδαμε πιο πάνω μπορεί να δίνουν ικανοποιητικά αποτελέσματα για ένα δίκτυο μερικών δεκάδων κόμβων, όμως σε ένα δίκτυο μερικών χιλιάδων κόμβων η απόδοση του σχήματος μπορεί να καταστεί προβληματική στο επίπεδο της επεξεργασίας, της αποθήκευσης και των απαιτούμενων επικοινωνιών για την εγκατάσταση παραδείγματος χάριν 1000 διαφορετικών κλειδιών από 20 bytes το καθένα σε ένα κόμβο. Με την αποδοτική σχεδίαση του σχήματος εγκατάστασης και ανταλλαγής των κλειδιών είναι δυνατόν τα δίκτυα μεγάλης κλίμακας να προστατεύονται χωρίς περιορισμούς στην απόδοση.

- *Προσβασιμότητα*. Είναι η ανάγκη τα δεδομένα ad hoc να είναι προσβάσιμα από πολλούς κόμβους, κάτι το οποίο επιτυγχάνεται με τη συγκέντρωση των δεδομένων και την ενδο-δικτυακή επεξεργασία στους κόμβους συνάθροισης των δεδομένων οι οποίοι επιπλέον επιφορτίζονται και με τη διαχείριση κλειδιών μέσα στο δίκτυο και την προστασία των δεδομένων.

- *Ανοχή*. Το σχήμα δημιουργίας κλειδιών δε θα πρέπει να θέτει σε κίνδυνο ολόκληρο το δίκτυο όταν ένας και μόνο κόμβος με το μυστικό του υλικό συμβιβάζεται από μία κακόβουλη ενέργεια.

- *Υψηλό επίπεδο ασφαλούς συνεκτικότητας*. Η εγκατάσταση αυθεντικοποιημένων ζεύξεων μεταξύ ζευγών κόμβων που μπορούν να μοιραστούν μεταξύ τους ένα κοινό κλειδί με μεγάλη πιθανότητα είναι βασική απαίτηση για τη διατήρηση της ασφαλούς λειτουργικότητας μέσα σ' ένα δίκτυο MANET, WSN ή VANET.

2.2.11. Ανανέωση Δεδομένων

Τα παλαιά δεδομένα δε θα πρέπει να θεωρούνται ότι είναι νέα δεδομένα. Η επανάληψη των πακέτων δεδομένων που δημιουργήθηκαν κάποια στιγμή στο παρελθόν από κακόβουλους χρήστες είναι μια επίθεση που μπορεί να δημιουργήσει μεγάλα προβλήματα σε ένα δίκτυο ad hoc.

Ένας κακόβουλος κόμβος μπορεί να επαναλάβει ένα νόμιμο πακέτο προηγούμενου χρόνου που έχει συλλάβει (μπορεί να είναι ένα πακέτο του πρωτοκόλλου αυθεντικοποίησης του συστήματος) και να προκαλέσει σύγχυση στους υπολοίπους κόμβους. Ακόμη και αν τα πακέτα κρυπτογραφούνται με κλειδιά είναι δυνατόν ο επιτιθέμενος να επαναλάβει το μήνυμα χωρίς καν να χρειαστεί να το αποκωδικοποιήσει, επίθεση που είναι δυσκολότερο να ανιχνευθεί. Έτσι, εκτός από τη χρήση κλειδιών που ανανεώνονται, τα αντίμετρα προστασίας περιλαμβάνουν τη χρήση αριθμών ακολουθιών, "Sequence Numbers" (SN) που αριθμούν μοναδικά κάθε πακέτο στο επίπεδο MAC ή εναλλακτικά στο επίπεδο του ad hoc πρωτοκόλλου δρομολόγησης, καθώς και τη χρήση χρονοσφραγίδων ("timestamps") που προστίθενται σε κάθε πακέτο και συγκρίνονται με το ρολόι του δέκτη.

2.3. ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] M. Graussglauser and D. N. C. Tse. "Mobiliy increases the capacity of ad hoc wireless networks."In: IEEE/ACM Transactions on Networking, Vol. 10, No. 4, August 2002.

[2] "Scenario Driven Security Analysis and Architecture Driven Requirement Specification", Deliverable D0.2, UbiSec&Sens, FP6-2004-IST-4 Project, 3 April 2007.

[3] Zhou, L. and Haas, Z. 1999. "Securing ad hoc networks". IEEE Network, Vol. 13 (6), pp. 24-30, November, 1999.

[4] Matt Welsh, Dan Myung, Mark Gaynor, and Steve Moulton. “Resuscitation monitoring with a wireless sensor network”. In Supplement to Circulation: Journal of the American Heart Association, October 2003.

[5] J-P Hubaux, L. Buttyan, S. Capkun. “The Quest for Security in Mobile Ad Hoc Networks”. MobiHOC 2001, Long Beach, CA, USA. Pp. 146-155.

[6] I. F. Akyildiz, X. Wang. “A Survey on Wireless Mesh Networks”. IEEE Communications Magazine, September 2005, Vol. 33, Issue 9, pp. S23-S30.

[7] S. A. Camtepe and B. U. Yener, “Key Distribution Mechanisms for Wireless Sensor Networks: a Survey”, TR-05-07, Department of Computer Science, Rensselaer Polytechnic Institute.

[8] Johnson C. Lee and Victor C. M. Leung, K. Wong, Cao. Jiannong, H. Chan. “Key Management Issues in Wireless Sensor Networks. Current Proposals and Future Developments”. IEEE Wireless Communications, October 2007, Vol. 14, Issue 5, pp. 76-83.

[9] Azzedine Boukerche, Damla Turgut, “Secure Time Synchronization Protocols For Wireless Sensor Networks”. In: IEEE Wireless Communications, October 2007.

[10] B. Sundararaman, U. Buy, and A. D. Kshemkalyani, “Clock Synchronization for Wireless Sensor Networks: A Survey”. In: Ad Hoc Networks, vol. 3, no. 3, May 2005, pp. 281–323.

[11] S. Chen et al. “Time Synchronization for Predictable and Secure Data Collection in WSN”. In: Procs of the 6th Annual MedhocNet WorkShop, Corfu, Greece, 12-15 June, 2007.

[12] Zhou L and Haas Z. Securing Ad Hoc Networks. IEEE Network, Vol. 13 (6), pp. 24—30, November, 1999.

[13] Papadimitratos P. and Haas Z., “Secure message transmission in mobile ad hoc networks”, Ad Hoc Networks, Volume 1, Issue 1, July 2003, pp. 193-209.

[14] Papadimitratos P. and Haas Z., “Secure routing for mobile ad hoc networks”. In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS) (TX, San Antonio), January 2002.

[15] Desmedt Y, and Frankel Y, Threshold Cryptosystems, In Advances in Cryptology – Crypto’89, Lecture Notes in Computer Science Vol. 435, Springer-Verlag, pp. 307 – 315, 1989.

[16] Desmedt Y, Threshold Cryptography. European Transactions on Tellecommunications, 5(4), pp. 449–57, 94.

[17] Jarecki S, Proactive Secret Sharing and Public Key Cryptosystems. Master Thesis, Dept. Elec. Eng. And Comp. Sci., MIT, September 1995.

[18] Herzberg A, Jarecki S, Krawczyk H, and Yung M. Proactive Secret Sharing or: How to Cope with Perpetual Leakage. In Proceedings of Advances in Cryptology – Crypto’95, Lecture Notes in Computer Science Vol. 963, Springer-Verlag, pp. 457 – 469, 1995.

[19] Herzberg A, Jakobsson M, Jarecki S, Krawczyk H, and Yung M. “Proactive Public key and Signature Schemes”. In Proceedings of 4th Annual Conference on Computer Communications Security, Zurich, Switzerland, pp. 100–110, 1997.

[20] https://datatracker.ietf.org/doc/draft-ietf-manet-nhdp/.

3. ΘΕΩΡΗΤΙΚΟ ΥΠΟΒΑΘΡΟ

Τα ασύρματα δίκτυα κατ΄ απαίτηση (ad hoc) αποτελούν ένα σχετικά πρόσφατο μοντέλο δικτύων, το οποίο δίχως να αποτελείται από κάποια στατική υποδομή για την υποστήριξη των δικτυακών υπηρεσιών, επιτυγχάνει την επικοινωνία μεταξύ προσωπικών ηλεκτρονικών συσκευών (όπως κινητά τηλέφωνα, φορητοί υπολογιστές, προσωπικοί ψηφιακοί βοηθοί – PDA) ακόμη και μεταξύ μικροσκοπικών αισθητήρων εστιάζοντας κυρίως στη φυσική των κόμβων καθώς και στην κίνηση αυτών. Είναι σημαντικό να ξεκαθαρίσουμε ότι τα δίκτυα ad hoc (κάθε κατηγορίας) δημιουργούνται δυναμικά όταν οι προσωπικές συσκευές των χρηστών μπαίνουν εντός της ακτίνας κάλυψης και ανιχνεύονται αμοιβαία, δηλαδή οι βασικές δικτυακές λειτουργίες που συναντάμε στα δίκτυα υποδομής όπως το Διαδίκτυο είναι κατ' ουσία απούσες στα δίκτυα ad hoc. Έτσι, δε θα συναντήσουμε αφιερωμένους κόμβους-δρομολογητές και επίσης στα δίκτυα ad hoc δε διατίθεται εγκατεστημένη η υπηρεσία DHCP που αποδίδει τις διευθύνσεις σε ένα δίκτυο IP, όπως επίσης και η υπηρεσία DNS (Domain Name Server) της αντιστοίχησης ονομάτων σε διευθύνσεις IP. Πολύ περισσότερο, τα δίκτυα ad hoc δε διαθέτουν εγκατεστημένες υπηρεσίες ασφάλειας όπως εξυπηρετητές αυθεντικοποίησης, αρχές πιστοποίησης CA ("Certification Authorities"), τείχη προστασίας ("firewalls") και άλλα συστήματα και υπηρεσίες που διασφαλίζουν τα σταθερά δίκτυα με υποδομή.

Σημαντικός παράγοντας για τα ασύρματα δίκτυα ad hoc είναι οι ιδιότητες του ασύρματου μέσου μετάδοσης και οι τεχνολογίες/πρότυπα ασύρματης διασύνδεσης που έχουν αναπτυχθεί. Τέτοιες ασύρματες τεχνολογίες που χρησιμοποιούνται στις ζεύξεις των ασυρμάτων δικτύων ad hoc είναι:

- Οι υπέρυθρες ακτίνες. Ο οργανισμός IrDA [73] ασχολείται με την προτυποποίηση των τεχνολογιών και πρωτοκόλλων (IrDA DATA και IrDA CONTROL) που βασίζονται στις υπέρυθρες ακτίνες. Με τις υπέρυθρες καλύπτονται πολύ μικρές αποστάσεις (ένα έως μερικά μόνο μέτρα) ενώ ο μέγιστος εφικτός ρυθμός μετάδοσης είναι 16Mbps.
- Το Bluetooth (ISM 2.5 GHz) που σε αντίθεση με τις υπέρυθρες δεν απαιτεί οπτική επαφή μεταξύ των συσκευών, αρκεί αυτές να είναι εντός της μέγιστης κάλυψης από 10m -100m. Το bluetooth μεταφέρει δεδομένα με ρυθμό μέχρι και 2Mbps. Χαρακτηριστικό της τεχνολογίας είναι η πολύ χαμηλή ισχύς λειτουργίας των συσκευών, μέχρι 1mW.
- Τα μικροκύματα στενής ζώνης (microwave narrowband).
- Το πρότυπο IEEE 802.11 (WiFi μικρής ως 500 mW και υψηλής ισχύος μερικών W). Το WiFi είναι μια ευρέως διαδεδομένη WLAN ad hoc τεχνολογία ασύρματης δικτύωσης στο φάσμα ISM των 2.4 και 5 GHz με πλεονεκτήματα την ευκολία ανάπτυξης, το χαμηλό κόστος, τον πολύ υψηλό βαθμό διαλειτουργικότητας μεταξύ των διαφόρων κατασκευαστών και το πλήθος των εφαρμογών που υποστηρίζει (χρήση ISP) αλλά και με πολλά μειονεκτήματα, ιδίως όσον αφορά στην ασφάλεια των χρησιμοποιούμενων πρωτοκόλλων.

  Το πρωτόκολλο πολλαπλής πρόσβασης MAC 802.11 των ασυρμάτων δικτύων στηρίζεται στο μηχανισμό CSMA/CD του ενσύρματου προτύπου IEEE 802.3. Ωστόσο τον επεκτείνει με το μηχανισμό αποφυγής των συγκρούσεων CSMA/CA κατά τρόπο τέτοιο ώστε να επιλύονται τα προβλήματα που οφείλονται στην ασύρματη μετάδοση (fading, κρυμμένα και εκτεθειμένα τερματικά, απόκρυψη των συγκρούσεων). Έτσι με βάση το πρότυπο 802.11 αναπτύχθηκαν και τα υπόλοιπα WLAN πρότυπα IEEE 802.11 b/g/a/n/i/e τα οποία έχουν κοινό το μηχανισμό CSMA/CA, διαφοροποιούνται ωστόσο στο φυσικό επίπεδο, δηλαδή ως προς τον τρόπο μετάδοσης και την ποιότητα του ραδιοσήματος (κάλυψη, ρυθμός μετάδοσης μέχρι και 300Mbps για το 802.11n έναντι των 11Mbps αρχικά, αντιμετώπιση των παρεμβολών), το βαθμό ασφάλειας (802.11i) και το QoS (802.11e) που επιτυγχάνουν. Με τις νέες αυτές ασύρματες τεχνολογίες καθίσταται δυνατή η ανάπτυξη εφαρμογών

πραγματικού χρόνου με ικανοποίηση απαιτήσεων QoS, όπως VOIP και πολυμεσικές εφαρμογές π.χ. τηλεδιάσκεψη πάνω από τα δίκτυα WLAN.

- Οι ποικίλες τεχνικές διασποράς του ραδιοφάσματος (spread spectrum), π.χ. Direct Sequence Spread Spectrum (DSSS).
- Το πρότυπο IEEE 802.15.4. Αυτό καθορίζει το φυσικό και το επίπεδο MAC για τη δικτύωση προσωπικών συσκευών PAN (Personal Area Networks) χαμηλής ισχύος μέχρι περίπου 250mW.

Στην παρούσα διατριβή το ενδιαφέρον επικεντρώνεται στη σχεδίαση και υλοποίηση ασφαλών αρχιτεκτονικών ασύρματων δικτύων ad hoc όπου οι ενδιάμεσοι κόμβοι είναι ομότιμοι και λειτουργούν ως δυνητικοί δρομολογητές και συγχρόνως ως δυνητικοί κόμβοι του συστήματος ασφαλείας του δικτύου έτσι ώστε να διασφαλίζουν την ορθή λειτουργία και να προστατεύουν τις επικοινωνίες του δικτύου από τους πιθανούς κακόβουλους κόμβους.

Επειδή στην κατηγορία των δικτύων ad hoc υπάρχουν διαφορετικά μοντέλα επικοινωνιών και, επιπλέον, επειδή είναι πολλές οι ad hoc εφαρμογές τελικού χρήστη οι οποίες και τελικά διαφοροποιούν το ένα δίκτυο ad hoc από το άλλο, κρίνεται σκόπιμο να διαχωρίσουμε τα ασύρματα δίκτυα ad hoc στις παρακάτω βασικές κατηγορίες (MANET, WSN, Mesh, VANET) που περιγράφονται με αφετηρία και την εφαρμογή που υποστηρίζουν κατά περίπτωση.

3.1. ΚΙΝΗΤΑ ΑΣΥΡΜΑΤΑ AD HOC ΔΙΚΤΥΑ (MANET)

Με τον όρο MANET (Mobile Ad Hoc Networks) περιγράφουμε τα δίκτυα ομότιμων κινητών υπολογιστών και κινητών μικρών συσκευών που μπορούν να συνδέονται μεταξύ τους μέσω ασύρματων τεχνολογιών. Τα δίκτυα MANET ερευνώνται από το IETF MANET WG [3].

Ο όρος MANET κατ' αρχήν χρησιμοποιείται σε εφαρμογές με προσωπικές συσκευές όπου το ενδιαφέρον εστιάζεται στην κίνηση των κόμβων. Στα κινητά ασύρματα δίκτυα MANET πολύ συχνά οι χρήστες/κόμβοι κινούνται με υψηλή ταχύτητα και είναι πολλά τα δυνατά μοντέλα κίνησης που μπορεί να χρησιμοποιηθούν όπως το τυχαίο μοντέλο ("Random Waypoint Model"), το μοντέλο της κίνησης κατά ομάδες ("group model"), το μοντέλο κίνησης εντός των πόλεων ("urban model") και το μοντέλο δρόμων ταχείας κυκλοφορίας ("motorway model").

Συνεπώς, στα MANET η δυναμικότητα λόγω της κίνησης των κόμβων είναι μεγάλης σημασίας και πρέπει να λαμβάνεται σοβαρά υπόψη κατά τη σχεδίασή τους διότι προκαλεί ραγδαίες και σημαντικές αλλαγές στην τοπολογία των δικτύων και άρα επηρεάζει ανάλογα την απόδοση των αλγορίθμων, των πρωτοκόλλων και των εφαρμογών που τρέχουν στο δίκτυο. Οι τελευταίες ερευνητικές εργασίες αποδεικνύουν ότι η κίνηση των κόμβων είναι ένας παράγοντας τον οποίο θα πρέπει να εκμεταλλευόμαστε στη σχεδίαση των πρωτοκόλλων στα δίκτυα ad hoc παρά να τον αντιμετωπίζουμε απλά σαν ένα εμπόδιο που μόνο μείωση της απόδοσης των δικτύων μπορεί να επιφέρει [4], [5].

Δύο κόμβοι MANET είναι γειτονικοί όταν ο ένας βρίσκεται εντός της ακτίνας εμβέλειας του άλλου – όπως θα δούμε σε επόμενα κεφάλαια. Ένα, δύο ή το πολύ τρία βήματα μακριά είναι η απόσταση που μπορούμε να εκμεταλλευτούμε για τον έλεγχο της τοπολογίας των δικτύων. Δύο γειτονικοί κόμβοι επικοινωνούν άμεσα μέσω ραδιοκυμάτων. Σε περίπτωση απομακρυσμένων κόμβων, δηλαδή κόμβων που δεν συνδέονται άμεσα μεταξύ τους, η επικοινωνία στηρίζεται σε ενδιάμεσους κόμβους για τη δρομολόγηση των πακέτων επικοινωνίας, οι οποίοι αναλαμβάνουν την απαραίτητη προώθηση των πακέτων. Συνεπώς, στα MANET κάθε κόμβος λειτουργεί ως δυνητικός δρομολογητής των δεδομένων των υπολοίπων κόμβων ενώ ταυτόχρονα διατηρεί την ιδιότητα του αυτόνομου συστήματος ή του τελικού κόμβου.

Η δρομολόγηση των πακέτων από την πηγή προς τον τελικό προορισμό, ανάλογα και με τη δυνατότητα των πομπών που διατίθενται στους κόμβους, μπορεί να γίνεται με πολλαπλά βήματα - δρομολόγηση “multi-hop” - ή είναι δυνατό η επικοινωνία να επιτυγχάνεται απευθείας με ένα και μόνο βήμα.

3.2. ΑΣΥΡΜΑΤΑ AD HOC ΔΙΚΤΥΑ ΜΙΚΡΟΣΚΟΠΙΚΩΝ ΑΙΣΘΗΤΗΡΩΝ

Μία άλλη κατηγορία δικτύου που εμπίπτει στα όρια της παρούσας διατριβής είναι τα ασύρματα δίκτυα αισθητήρων WSN (Wireless Sensors Networks) τα οποία κατά κύριο λόγο χρησιμοποιούνται σε εφαρμογές παρακολούθησης της θέσης ενός κινούμενου στόχου και της μεταβολής περιβαλλοντικών φαινομένων όπως σεισμοί, κλιματολογικές αλλαγές, θερμοκρασία, πίεση κ.α. Επίσης, πολύ συχνή είναι η χρήση των αισθητήρων σε οικιακές εφαρμογές, σε εφαρμογές παρακολούθησης εσωτερικών (όροφοι κτιρίων) και εξωτερικών χώρων, ακόμη και σε ολοκληρωμένες εφαρμογές βιομηχανικού ελέγχου. Στα δίκτυα αισθητήρων [1] η επικοινωνία διεξάγεται βήμα-βήμα μεταξύ μικροσκοπικών συσκευών (κόμβων του δικτύου) με μικρά αποθέματα ενέργειας, βασίζεται δε στο ραδιοφάσμα.

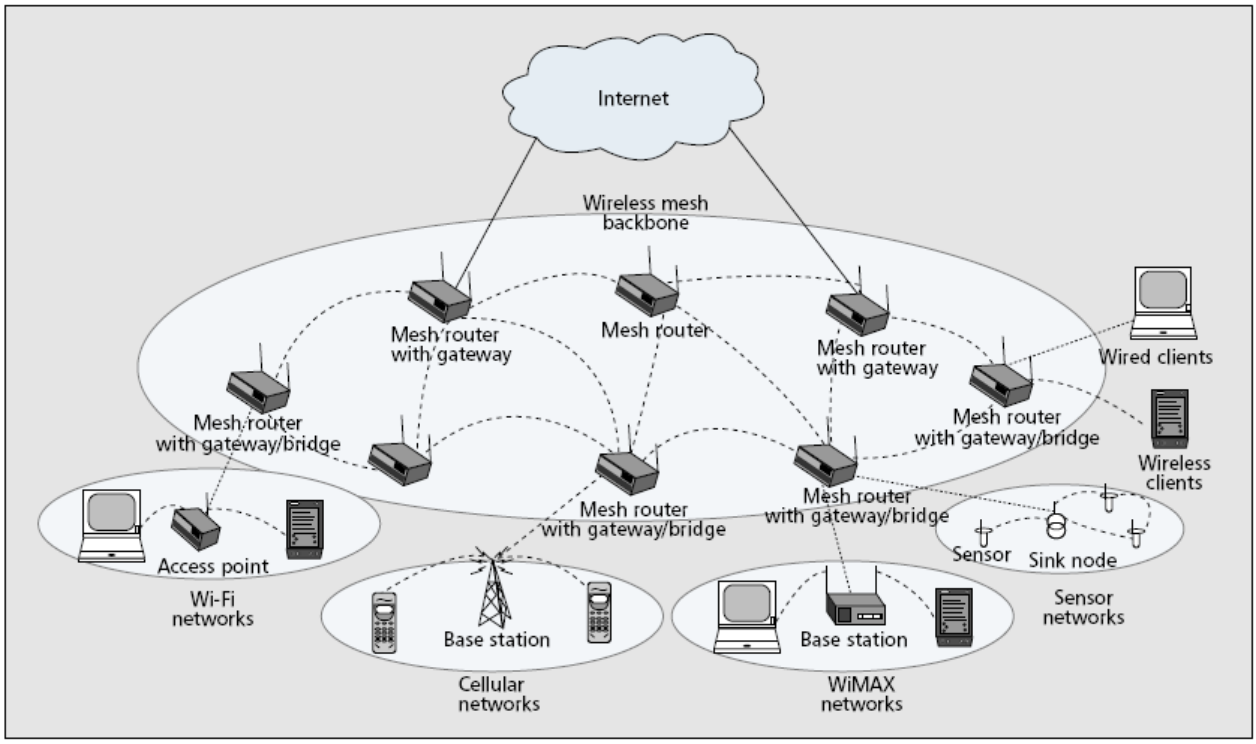
Οι κόμβοι του δικτύου ανταλλάσσουν μηνύματα με ένα ή και περισσότερους κεντρικούς σταθμούς βάσης (“sink”). Ο σταθμός μπορεί να είναι στατικός ή κινούμενος λειτουργεί δε σαν κόμβος συγκέντρωσης της κίνησης του δικτύου αλλά και ως πύλη (“gateway”) για την ανταλλαγή πληροφορίας με το Διαδίκτυο ή και με άλλα ασύρματα δίκτυα υποδομής. Το χαρακτηριστικό της απόδοσης των δικτύων αυτών είναι η μικρή διάρκεια ζωής τους η οποία πρωτίστως οφείλεται στην πολύ περιορισμένη διαθέσιμη ενέργεια ανά κόμβο. Κατά συνέπεια, ο σχεδιασμός των πρωτοκόλλων δικτύων αισθητήρων, όσον αφορά την επιβιωσιμότητα και την απόδοση, κατά κύριο λόγο θα πρέπει να λαμβάνει υπ’ όψη τη χαμηλή κατανάλωση ενέργειας κατά τη δρομολόγηση των πακέτων από τους συμμετέχοντες στην επικοινωνία κόμβους.

Για τα δίκτυα αισθητήρων η ταχύτητα κίνησης των κόμβων είναι ελάσσονος σημασίας. Ωστόσο, τα μοντέλα κίνησης που μπορούμε να χρησιμοποιήσουμε στα WSN για να εκτιμήσουμε την επίδοση των αλγορίθμων και πρωτοκόλλων ποικίλουν αναλόγως της εφαρμογής που υποστηρίζεται, όπως για παράδειγμα μπορεί να είναι η ομαδική κίνηση με κατεύθυνση ένα σημείο του πεδίου που μπορεί να είναι ένα ασύρματο σημείο πρόσβασης 802.11, ή η τυχαία κίνηση των κόμβων με χαμηλή μέση ταχύτητα.

3.3. ΑΣΥΡΜΑΤΑ AD HOC ΔΙΚΤΥΑ ΠΛΕΓΜΑΤΟΣ

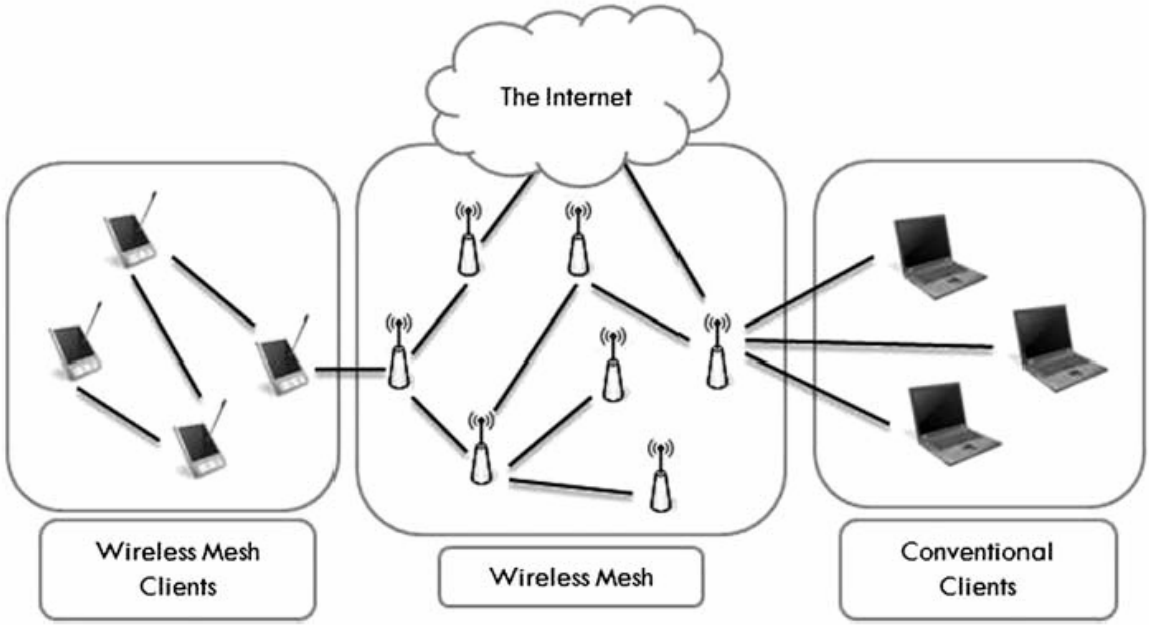
Τα WMN (Wireless Mesh Networks) -IEEE πρότυπο 802.11s- χαρακτηρίζονται από ένα αργά κινούμενο κορμό δικτύου που αποτελείται από σχετικά ισχυρούς κόμβους που λειτουργούν ως δρομολογητές που μπορούν να δρομολογήσουν τα πακέτα των υπολοίπων κόμβων με πολλαπλά βήματα (multi-hop) και οι οποίοι επικοινωνούν μεταξύ τους στην ελεύθερη ζώνη συχνοτήτων ISM (Industrial Scientific and Medical).

Ο κορμός του δικτύου WMN (Εικόνα 1) σκοπό έχει να παρέχει μία αξιόπιστη υπηρεσία πλήρως συνδεδεμένης υποδομής στους διάφορους κόμβους-πελάτες (clients), δηλαδή είναι μία υποδομή από δρομολογητές κορμού που συνδέονται με αυτο-προστατευόμενες ζεύξεις μεταξύ τους και οι οποίες με την ίδια ισχύ εκπομπής (P_t) μπορούν να προσφέρουν πολύ μεγαλύτερη κάλυψη στους τελικούς χρήστες. Επιπλέον οι δρομολογητές σύμφωνα με το πρότυπο 802.11s διατηρούν τις βασικές λειτουργικότητες πύλης και γέφυρας των συνηθισμένων δρομολογητών και πρόσθετα διαθέτουν δυνατότητες “multi-radio” (δηλαδή κάρτες πρόσβασης σε διαφορετικά ασύρματα δίκτυα) έτσι ώστε η κίνηση να μεταβιβάζεται τόσο στο Διαδίκτυο όσο και μεταξύ ετερογενών ασυρμάτων δικτύων (WiFi, WiMax, GPRS, 3G, WSN).



Εικόνα 1. Απεικόνιση δικτύου Wireless Mesh Network [2].

Έτσι όπως φαίνεται και στην Εικόνα 2, σε ένα δίκτυο από δρομολογητές πλέγματος μπορούν να συνδεθούν συμβατικοί τύποι ασύρματων συσκευών τους οποίους το δίκτυο θα εξυπηρετήσει με δρομολόγηση πολλαπλών βημάτων και με εξασφαλισμένη συνδεσιμότητα με το Διαδίκτυο.



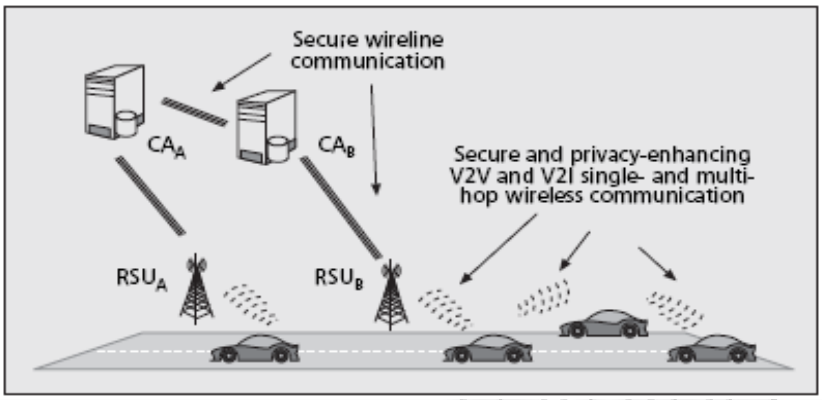
Εικόνα 2. Απεικόνιση των διαφορετικών τύπων των συσκευών-πελατών σ' ένα δίκτυο WMN.

Μπορούν ωστόσο να συνδεθούν και πελάτες πλέγματος, δηλαδή συσκευές (pda, laptops) που

μπορούν να χρησιμοποιήσουν τους δρομολογητές του πλέγματος και, επιπλέον, μπορούν να προωθήσουν τα πακέτα των άλλων πελατών, δυνατότητα που δεν έχουν οι συμβατικοί τύποι ασύρματων συσκευών.

Θα πρέπει ωστόσο να σημειωθεί ότι ο όρος “mesh” όσον αφορά τα ασύρματα ad hoc δίκτυα δεν αποδίδεται αποκλειστικά στα δίκτυα του προτύπου 802.11s. Αντίθετα, με τον όρο “mesh” αναφερόμαστε σε εκείνα τα δίκτυα που τρέχουν κάποιο πρωτόκολλο αυτο-οργάνωσης, αυτο-δρομολόγησης και αυτο-προστασίας, όπως για παράδειγμα τα δίκτυα που υλοποιούν την προτυποποιημένη στοίβα πρωτόκολλων 802.15.4 ZigBee που θα συναντήσουμε και παρακάτω ή/και άλλες εμπορικές λύσεις πλέγματος, όπως το πρωτόκολλο mcl (mesh connectivity layer) της Microsoft.

3.4. ΑΣΥΡΜΑΤΑ AD HOC ΔΙΚΤΥΑ ΟΧΗΜΑΤΩΝ



Εικόνα 3. Απεικόνιση ασφαλούς συστήματος VANET [6].

Τα ασύρματα ad hoc δίκτυα οχημάτων “Vehicular Adhoc NETworks” (VANET) επιτρέπουν τις επικοινωνίες ανάμεσα σε οχήματα (“Vehicular to Vehicular”, V2V) καθώς και μεταξύ των οχημάτων και της σταθερής υποδομής (Vehicular to Infrastructure, V2I) η οποία στην προκειμένη περίπτωση είναι σταθμοί βάσης που αναπτύσσονται κατά μήκος των πλευρών των δρόμων. Σε ένα δίκτυο VANET χρησιμοποιούνται ασύρματοι μικροσκοπικοί αισθητήρες που στέλνουν αναφορές στους σταθμούς βάσης, καθώς και συσκευές PC-based με τις οποίες είναι εφοδιασμένα τα οχήματα και τα οποία επεξεργάζονται περαιτέρω την πληροφορία. Επίσης στα δίκτυα VANET χρησιμοποιείται και η τεχνολογία WiFi.

Οι εφαρμογές των δικτύων VANET περιλαμβάνουν την παρακολούθηση περιβαλλοντικών συνθηκών, την παρακολούθηση της κυκλοφοριακής κίνησης και την έγκαιρη ειδοποίηση των οδηγών με κατάλληλα μηνύματα (έλεγχος πορείας). Πρόσφατα γίνεται και ανάπτυξη multi-hop πολυμεσικών εφαρμογών πάνω από τα δίκτυα αυτά (για παράδειγμα video on demand, κοινή χρήση αρχείων μεταξύ κινούμενων οχημάτων κ.α.).

Η ερευνητική προσπάθεια για την ασφάλεια στα δίκτυα VANET επικεντρώνεται στην προστασία των επικοινωνιών μεταξύ των οχημάτων, στην ανάπτυξη ασφαλών ad hoc πρωτοκόλλων και αρχιτεκτονικών που εγκαθιστούν εμπιστοσύνη για την αυθεντικότητα των μηνυμάτων, των οχημάτων και της ταυτότητας των οδηγών [6] καθώς και στην αντιμετώπιση επιθέσεων κυρίως στο επίπεδο της εφαρμογής, όπως οι επιθέσεις Denial of Service, η μετάδοση ψευδούς πληροφορίας από κακόβουλους κόμβους για παραπλάνηση του συστήματος κ.α.

3.5. ΠΡΟΒΛΗΜΑΤΑ ΕΠΙΒΙΩΣΗΣ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ AD HOC

Τα δίκτυα ad hoc παρουσιάζουν ένα ευρύ σύνολο από εγγενή χαρακτηριστικά τα οποία καθιστούν

την επιβίωσή τους αρκετά δύσκολη. Η επιβιωσιμότητα των δικτύων ad hoc επί το πλείστον σχετίζεται με τα αποθέματα ενέργειας των κόμβων καθώς και με τη διαθεσιμότητα ικανού αριθμού μονοπατιών επικοινωνίας μεταξύ των απομακρυσμένων κόμβων που συμμετέχουν στις επικοινωνίες.

Ενδεικτικά αναφέρεται ότι η ευρωστία, η διαθεσιμότητα και εν τέλει ο χρόνος ζωής του δικτύου κινδυνεύει στις περιπτώσεις πτώσης των κόμβων (για παράδειγμα λόγω έλλειψης ενέργειας σε έναν αισθητήρα-mote), ή πτώσης των δεσμών σε ένα δίκτυο MANET (για παράδειγμα λόγω πολύ κακής ποιότητας του ασύρματου καναλιού), ή για παράδειγμα στις περιπτώσεις αποσύνδεσης του δικτύου λόγω της κίνησης ενός (ή περισσοτέρων) κόμβου εκτός της εμβέλειας ενός άλλου γειτονικού κόμβου.

Παρακάτω περιγράφονται αναλυτικά οι ιδιότητες αυτές των δικτύων ad hoc οι οποίες οφείλονται κυρίως στους περιορισμένους πόρους τους οποίους διαθέτουν τόσο οι πλατφόρμες υλικού των κόμβων όσο και το ασύρματο κανάλι που αυτοί χρησιμοποιούν κατά την επικοινωνία τους.

Τα βασικά προβλήματα για την ασφάλεια της επικοινωνίας σε ad hoc δίκτυα επιβάλλουν λήψη μέτρων όπως την αυθεντικοποίηση των κόμβων, τη διαφύλαξη της εμπιστευτικότητας και της ακεραιότητας της πληροφορίας από ενεργούς και παθητικούς ωτακουστές, και τέλος την έγκαιρη και συντονισμένη ανάκαμψη του δικτύου από κακόβουλες ή εχθρικές ενέργειες. Οι κακόβουλες επιθέσεις ή ακόμη και η ύπαρξη παθητικών ωτακουστών θέτουν σε κίνδυνο την εμπιστευτικότητα και την ακεραιότητα της πληροφορίας. Ελάχιστες απαιτήσεις για την αποφυγή αυτών είναι η ασφαλής κωδικοποίηση των δεδομένων που μεταδίδονται στο ασύρματο μέσο καθώς και η αυθεντικοποίηση των κόμβων και των χρηστών.

Η συνεκτικότητα σε ένα δίκτυο ad hoc καθώς και η διαθεσιμότητα εναλλακτικών μονοπατιών επικοινωνίας μεταξύ απομακρυσμένων κόμβων που χωρίζονται από πολλά βήματα, μειώνεται μετά από μία ενδεχόμενη κακόβουλη επίθεση. Οι κακόβουλες επιθέσεις μπορούν να καταρρίψουν όχι μόνο ένα απομονωμένο κόμβο αλλά να μειώσουν τη συνεκτικότητα του δικτύου στο σύνολό του, μειώνοντας ή εξαφανίζοντας, κατά περίπτωση, τον αριθμό των εναλλακτικών μονοπατιών δρομολόγησης μεταξύ των ad hoc κόμβων.

Όσον αφορά τα δίκτυα αισθητήρων μία κακόβουλη επίθεση μπορεί να απομονώσει το σταθμό βάσης (sink) από τους ασύρματους κόμβους, με αποτέλεσμα τα δεδομένα που συγκεντρώνονται από τους αισθητήρες να μην φτάνουν στον τελικό χρήστη που τα επεξεργάζεται. Σε αυτές τις περιπτώσεις, τα δίκτυα καθίστανται μη συνδεδεμένα και κατά συνέπεια η λειτουργία τους είναι προβληματική. Κατ' επέκταση, η σχεδίαση του δικτύου θα πρέπει να είναι τέτοια ώστε να λαμβάνει εκ των προτέρων υπόψη της το ενδεχόμενο εχθρικών ενεργειών που στοχεύουν σε κατατμήσεις που έχουν ολικό αντίκτυπο για το δίκτυο. Για παράδειγμα το σχέδιο δράσης μπορεί να απαιτεί τη μετακίνηση ενός κόμβου σε μια συγκεκριμένη θέση ώστε να διατηρηθεί η συνδεσιμότητα άλλων απομακρυσμένων κόμβων [2].

3.5.1. Περιορισμοί Διαθέσιμης Ενέργειας

Η δυνατότητα αποθήκευσης ενέργειας στους κόμβους του δικτύου ad hoc είναι περιορισμένη. Η κατανάλωση όλης της διαθέσιμης ενέργειας οδηγεί πολύ συχνά σε πτώση των κόμβων. Αυτό εντείνεται ακόμη περισσότερο λόγω του γεγονότος ότι στα δίκτυα ad hoc χωρίς υποδομή είναι αναγκαίο οι κόμβοι να βρίσκονται διαρκώς σε κατάσταση ενεργή και ποτέ να μην είναι κλειστοί, εφόσον, όπως έχει ειπωθεί, λειτουργούν σαν δυνητικοί δρομολογητές της κίνησης που προέρχεται από τους λοιπούς ομότιμους κόμβους. Συνεπώς, η σχεδίαση των πρωτοκόλλων δρομολόγησης πρέπει να περιλαμβάνει, αν όχι να βασίζεται, στην ελαχιστοποίηση της κατανάλωσης της ενέργειας (P_c) από τους κόμβους κατά τη λειτουργία τους.

3.5.2. Περιορισμοί του Καναλιού Μετάδοσης

Στο ασύρματο μέσο μετάδοσης έχουμε τους γνωστούς περιορισμούς στο διαθέσιμο εύρος ζώνης του καναλιού και στην ποιότητα του σήματος που αποδίδεται στο χρήστη. Μια ριπή δεδομένων που μεταδίδεται σε απόσταση μεγαλύτερη από το διπλάσιο της ακτίνας κάλυψης θεωρείται χαμένη, δεδομένης σταθερής της ισχύος εκπομπής P_t ανά κόμβο. Η ισχύς εκπομπής P_t θα πρέπει να διατηρείται χαμηλή έτσι ώστε να μειώνεται η κατανάλωση ενέργειας P_c στον κόμβο και έτσι ώστε η μεταδιδόμενη πληροφορία να είναι λιγότερο εύκολο να υποκλαπεί. Πρέπει ωστόσο η ισχύς μετάδοσης P_t να μην είναι σε τέτοιο επίπεδο χαμηλή που να προκαλείται διάρρηξη της συνεκτικότητας μεταξύ των κόμβων του δικτύου.

3.5.3. Περιορισμοί λόγω της Κίνησης των Κόμβων

Η τυχαία κίνηση των ομότιμων ad hoc κόμβων οδηγεί σε συχνές αλλαγές της τοπολογίας και της συνεκτικότητας, ιδιαίτερα στα δίκτυα MANET. Οι σύνδεσμοι μεταξύ των κόμβων δημιουργούνται και καταστρέφονται δυναμικά, καθώς κάθε κόμβος εισέρχεται ή εξέρχεται από την ακτίνα εμβέλειας των υπολοίπων. Καθώς όμως κάθε κόμβος αποτελεί ένα δυνητικό ενδιάμεσο δρομολογητή των πακέτων πληροφορίας μεταξύ της πηγής και του τελικού αποδέκτη η συνεκτικότητα του δικτύου MANET, δηλαδή η διαθεσιμότητα μονοπατιών επικοινωνίας μεταξύ πηγών και τελικών κόμβων εξαρτάται από άκρως δυναμικούς και τυχαίους παράγοντες που μπορούμε όμως να μοντελοποιήσουμε και να εκμεταλλευτούμε [1] εφαρμόζοντας το κατάλληλο μοντέλο κίνησης των κόμβων και τους κατάλληλους μηχανισμούς ελέγχου της τοπολογίας του δικτύου.

Είναι αναγκαίο το πρωτόκολλο ad hoc να σχεδιάζεται έτσι ώστε να λαμβάνει υπ' όψιν τα ιδιαίτερα χαρακτηριστικά της τοπολογίας και της κίνησης των κόμβων που υφίστανται ανά περίπτωση της ad hoc εφαρμογής που αναπτύσσεται. Για παράδειγμα, προτιμούμε ένα ιεραρχικό πρωτόκολλο δρομολόγησης που βασίζεται σε σταθερές ή δυναμικές ομάδες που οργανώνονται σε πολλά διακριτά επίπεδα διαχείρισης έναντι ενός επίπεδου πρωτοκόλλου όταν αντίστοιχα και η κίνηση των πολλών κόμβων είναι ομαδική ή/και όταν η συμμετοχή των κόμβων σε μια ομάδα δεν μεταβάλλεται αισθητά κ.ο.κ. Με αυτό μόνο τον τρόπο θα μπορούμε να αξιολογήσουμε ορθά την επίδοση ενός προτεινόμενου ad hoc πρωτοκόλλου.

Επιπρόσθετα, μπορούμε να υποθέσουμε ότι η κίνηση των κόμβων επηρεάζεται και από ένα σχέδιο δράσης που προσπαθούν να εφαρμόσουν οι κόμβοι. Για παράδειγμα, το σχέδιο δράσης μπορεί να απαιτεί τη μετακίνηση ενός κόμβου σε μία συγκεκριμένη θέση ώστε να διατηρηθεί η συνεκτικότητα άλλων απομακρυσμένων κόμβων. Τέτοιοι αλγόριθμοι ελέγχου της τοπολογίας του δικτύου αποτελούν τρέχον ερευνητικό πεδίο και δίκτυα με τέτοια προηγμένα χαρακτηριστικά είναι τα WMN (Wireless Mesh Networks), δες §3.3 και [2].

3.5.4. Περιορισμοί Δικτυακής Λειτουργίας

Η έλλειψη σταθερής υποδομής στα δίκτυα ad hoc (MANET και WSN) έχει σαν φυσικό αποτέλεσμα την επαύξηση των προβλημάτων επιβίωσής τους σε σχέση με τα αντίστοιχα ενσύρματα ή ασύρματα κυψελοειδή δίκτυα (όπως τα δίκτυα GSM και UMTS). Τα τελευταία διαθέτουν σταθερή υποδομή ικανή να διατηρήσει αδιάλειπτη, ασφαλή και ορθή τη λειτουργία τους. Για παράδειγμα, στα ενσύρματα και στα κυψελοειδή δίκτυα εγκαθίστανται αποκλειστικοί ισχυροί δρομολογητές και ισχυρά υπολογιστικά συστήματα που λειτουργούν ως εξυπηρετητές αυθεντικοποίησης των χρηστών και των συσκευών του δικτύου, ως αρχές πιστοποίησης όταν απαιτούνται πιστοποιητικά για την αυθεντικοποίηση των χρηστών, ως κεντρικές βάσεις δεδομένων όπου αποθηκεύονται με ασφάλεια τα δεδομένα και διαχειρίζεται μυστικό υλικό όπως κλειδιά, passwords, pass phrases κ.α. Σε ένα δίκτυο ad hoc είναι πολλές φορές αδύνατον να εγκατασταθεί τέτοια υποδομή και, συνεπώς, είναι εφικτές μόνο εκείνες οι δικτυακές λύσεις που κατανέμουν παρόμοιες λειτουργίες στους

ομότιμους ad hoc κόμβους.

Μια ακόμη ιδιότητα του περιορισμένου της λειτουργίας του δικτύου ad hoc είναι ότι αυτό πολλές φορές, ιδιαίτερα όταν μιλάμε για τα WSN, παραμένει σε λειτουργία αφύλακτο δίχως να επιβλέπεται, με αποτέλεσμα οι κόμβοι του να καθίστανται ιδιαίτερα ευάλωτοι σε επιθέσεις που στοχεύουν να τους συμβιβάσουν, δηλαδή ουσιαστικά να ελέγξουν τη λειτουργία του δικτύου εκ των έσω.

3.5.5. Περιορισμοί Ασφάλειας

Ένας κρίσιμος παράγοντας που διαφοροποιεί τα δίκτυα ad hoc από τα ασύρματα δίκτυα που βασίζονται στην υποδομή είναι η ευπάθειά τους σε μια πολύ ευρύτερη σειρά από απειλές οι οποίες θέτουν σε κίνδυνο την ασφαλή τους λειτουργία. Η διευρυμένη τρωτότητα των δικτύων αυτών και η έκθεση των ασύρματων δικτύων ad hoc σε μια ευρύτερη σειρά απειλών αποδίδεται στους ακόλουθους βασικούς λόγους.

- ***Στο κοινό ασύρματο κανάλι επικοινωνίας***. Λόγω της φύσης της ραδιοφωνικής μετάδοσης στο ασύρματο μέσο τα κανάλια των επικοινωνιών μπορεί να παγιδευτούν εύκολα και τα μηνύματα να κρυφακουστούν και να αλλοιωθούν. Επίσης, το ασύρματο κανάλι είναι εγγενώς αναξιόπιστο με πολλά λάθη στη μετάδοση των μηνυμάτων από συσκευή σε συσκευή ή από τον αρχικό στον τελικό χρήστη. Τα λάθη αυτά οφείλονται στα χαρακτηριστικά μετάδοσης του ασύρματου μέσου όπως η εξασθένηση του σήματος που φέρει την χρήσιμη πληροφορία, οι ανακλάσεις και η διασπορά του σήματος, φαινόμενα που εξαρτώνται από τη συχνότητα μετάδοσης αλλά και την ταχύτητα των κόμβων.
- ***Στην αφύλακτη δικτυακή λειτουργία***. Πολλές φορές τα ad hoc δίκτυα αναπτύσσονται σε μια απομακρυσμένη περιοχή και αφήνονται δίχως επιτήρηση και δίχως φύλαξη, όπως για παράδειγμα σε μια στρατιωτική εφαρμογή, ή σε μια εφαρμογή που χρησιμοποιεί αισθητήρες για την παρακολούθηση ενός φαινομένου. Αυτή η ιδιότητα των ασύρματων δικτύων αισθητήρων εκθέτει τους κόμβους σε φυσικές καταστροφές αλλά και σε σκόπιμες επιθέσεις από κακόβουλους χρήστες που θα προσπαθήσουν να διαβάσουν τα δεδομένα, να αντιγράψουν το υλικό, να καταστρέψουν το υλικό ή τελικά να συμβιβάσουν τους κόμβους που βρίσκονται σε λειτουργία.
- ***Στην έλλειψη κεντρικής υποδομής***. Όπως έχουμε ήδη αναφέρει, στην πλειονότητά τους τα δίκτυα ad hoc χαρακτηρίζονται από την έλλειψη υποδομής. Αυτό καθιστά απαγορευτική την ανάπτυξη στα δίκτυα ad hoc λύσεων ασφάλειας που βασίζονται στην υποδομή δημόσιου κλειδιού (PKI). Η ταυτοποίηση των χρηστών και συσκευών με τη χρήση πιστοποιητικών, η κωδικοποίηση των δεδομένων με ασύμμετρους αλγορίθμους, οι ψηφιακές υπογραφές είναι διαδικασίες που απαιτούν επεξεργαστική ισχύ και συνεπώς καταναλώνουν σε σημαντικό βαθμό τα λιγοστά ενεργειακά αποθέματα που διαθέτουν οι κόμβοι ad hoc. Έτσι η έλλειψη πόρων για την υλοποίηση λύσεων ασφαλείας που χρησιμοποιούνται ευρέως στα ασύρματα και ενσύρματα δίκτυα υποδομής αποτελεί εξ αρχής ένα περιορισμό για την ασφάλεια του συστήματος.
- ***Στη δυναμικότητα***. Ένα δίκτυο ad hoc χαρακτηρίζεται από μεγάλη δυναμικότητα των συνθηκών που επικρατούν σε αυτό κατά τη διάρκεια της ζωής του. Οι συνθήκες αυτές σχετίζονται στενά με τη μεταβλητή τοπολογία του δικτύου, με τον αριθμό των κόμβων που συμμετέχουν στο δίκτυο την κάθε χρονική στιγμή – κόμβοι (φιλικοί ή εχθρικοί) εισέρχονται και απέρχονται – , με την αρχική πυκνότητα του δικτύου, με το αρχικό μέγεθος του δικτύου, με το μοντέλο κίνησης των κόμβων που είναι ο σημαντικότερος παράγοντας στον οποίο οφείλονται οι ραγδαίες αλλαγές στην τοπολογία, με την ποιότητα του καναλιού στην οποία οφείλονται οι (παροδικές ή μη) πτώσεις των δεσμών μεταξύ των κόμβων, στα μειούμενα ενεργειακά αποθέματα που προκαλούν πτώσεις των κόμβων. Είναι προφανές ότι όλοι

αυτοί οι παράγοντες απειλούν την ασφάλεια των δικτύων ad hoc σε πολύ μεγαλύτερο βαθμό από ότι απειλείται η ασφάλεια σε ένα δίκτυο με σταθερή υποδομή.

3.6. ΠΡΩΤΟΚΟΛΛΑ ΔΡΟΜΟΛΟΓΗΣΗΣ ΣΕ ΔΙΚΤΥΑ AD HOC

Έχουν προταθεί διάφορα πρωτόκολλα για τη δικτύωση ad hoc. Μια κατηγοριοποίηση των ad hoc πρωτοκόλλων δρομολόγησης που διεξήγαμε παρουσιάζεται στην Εικόνα 5. Είναι προφανές ότι στην υπάρχουσα βιβλιογραφία έχουν προταθεί πάρα πολλές τεχνικές λύσεις (αλγόριθμοι, πρωτόκολλα, σχήματα, αρχιτεκτονικές) που σκοπό έχουν να καταστήσουν τα ad hoc πρωτόκολλα δρομολόγησης κατά το δυνατόν αποδοτικότερα και κατά το δυνατόν ασφαλέστερα. Στις επόμενες παραγράφους αναλύονται μερικά από τα πιο αντιπροσωπευτικά πρωτόκολλα για κάθε μία από τις κατηγορίες της Εικόνας 5.

3.6.1. Πρωτόκολλα Καθολικών Πινάκων

Τα ad hoc πρωτόκολλα καθολικών πινάκων προσπαθούν να επιλύσουν το πρόβλημα της διαχείρισης και της ανανέωσης της πληροφορίας δρομολόγησης δημιουργώντας για κάθε κόμβο έναν αριθμό από πίνακες δρομολόγησης οι οποίοι ανανεώνονται εκ των προτέρων (δηλαδή πριν ζητηθεί κάποιο μονοπάτι από μία πηγή προς ένα προορισμό) και οι οποίοι περιέχουν τα μονοπάτια επικοινωνίας από ένα δεδομένο κόμβο προς όλους τους κόμβους του δικτύου. Πιθανά μειονεκτήματα πρωτοκόλλων καθολικών πινάκων είναι:

1. *Το πρόβλημα μέτρησης στο άπειρο ("count to infinity")*. Είναι το φαινόμενο κατά το οποίο δημιουργούνται βρόχοι όταν τα πακέτα δρομολογούνται μέσω ζεύξεων που πλέον δεν υπάρχουν με αποτέλεσμα αυτά να ανακυκλώνονται συνεχώς. Αυτός ο κίνδυνος είναι ιδιαίτερα πιθανός στα δίκτυα ad hoc όπου πολύ συχνά συμβαίνουν μεταβολές στην τοπολογία του δικτύου και επομένως υπάρχει η ανάγκη της γρήγορης ενημέρωσης των κόμβων με τα νέα δεδομένα της κατάστασης των ζεύξεων και της τοπολογίας του δικτύου.

2. *Αργή σύγκλιση.* Τα πρωτόκολλα που χρησιμοποιούν καθολικούς πίνακες δεν αντιδρούν έγκαιρα σε περίπτωση βλαβών που μπορεί να συμβούν σε κόμβους και ζεύξεις, ιδιαιτέρως όταν τα δίκτυα είναι μεγάλα σε μέγεθος. Αυτό κυρίως οφείλεται στο ότι τα πρωτοκόλλα αυτά βασίζονται στη μέθοδο δρομολόγησης Distance Vector (DV) όπου χρησιμοποιούνται πίνακες μεγάλου μεγέθους O(n) και κατανεμημένοι αλγόριθμοι δρομολόγησης -κυρίως ο αλγόριθμος Distributed Bellman Ford (DBF)- με τους οποίους οι κόμβοι δεν μπορούν να έχουν συνολική άποψη για την τοπολογία του δικτύου.

Παραδείγματα ad hoc πρωτοκόλλων πινάκων είναι τα ακόλουθα.

3.6.1.1. Destination-Sequenced Distance-Vector Routing (DSDV)

Το βασικό χαρακτηριστικό των πρωτοκόλλου DSDV [9] είναι ότι κάθε κόμβος διατηρεί πίνακα με εγγραφές για όλους τους πιθανούς κόμβους του δικτύου (αυτό είναι το "distance vector"). Κάθε εγγραφή περιέχει τον πιθανό προορισμό, το επόμενο βήμα (hop) και το κόστος του μονοπατιού για τον προορισμό αυτόν. Βασίζεται στον αλγόριθμο δρομολόγησης Distributed Bellman Ford για τον υπολογισμό του βέλτιστου μονοπατιού προς τον προορισμό. Οι καθολικοί πίνακες ανανεώνονται με την ανταλλαγή πακέτων που μπορεί να περιέχουν ολόκληρο τον πίνακα (full dump) ή μέρος αυτού (partial dump), περίπτωση όπου εξοικονομείται εύρος ζώνης. Για την αποφυγή βρόχων κατά τη δρομολόγηση των πακέτων καθώς και για την επιλογή των πιο φρέσκων μονοπατιών κατά τη δρομολόγηση χρησιμοποιείται ένας αριθμός ακολουθίας προορισμού σε κάθε πακέτο.

3.6.1.2. Wireless Routing Protocol (WRP)

Το WRP [37] βασίζεται στο βελτιωμένο αλγόριθμο δρομολόγησης Bellman Ford και επιλύει το πρόβλημα “μέτρησης στο άπειρο” ωστόσο η αποθήκευση, επεξεργασία και ανανέωση των διαφορετικών τύπων πινάκων δρομολόγησης που απαιτούνται από το πρωτόκολλο επιφέρει μεγάλη επιβάρυνση στους κόμβους, ιδίως όταν το δίκτυο ad hoc είναι μεγάλο.

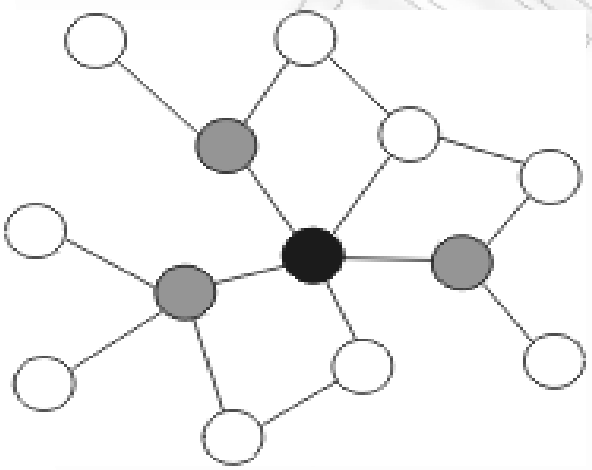
3.6.1.3. FisheyeStateRouting (FSR)

Το FSR [35] είναι ένα “link state” πρωτόκολλο το οποίο μπορεί επίσης να θεωρηθεί και ιεραρχικό. Το χαρακτηριστικό του είναι ότι βασίζει τη δρομολόγηση σε ακτίνες (“scopes” που μπορεί να είναι μέχρι και τρία βήματα μακριά από την πηγή), πέραν των οποίων η συχνότητα των πακέτων ενημέρωσης του δικτύου μειώνεται. Αποτέλεσμα είναι η επιβάρυνση στο δίκτυο να μειώνεται σε βάρος της ακρίβειας στη δρομολόγηση, τουλάχιστον όσον αφορά τους πολύ μακρινούς κόμβους. Ωστόσο καθώς το πακέτο πλησιάζει τον προορισμό η δρομολόγηση είναι και πάλι ακριβής.

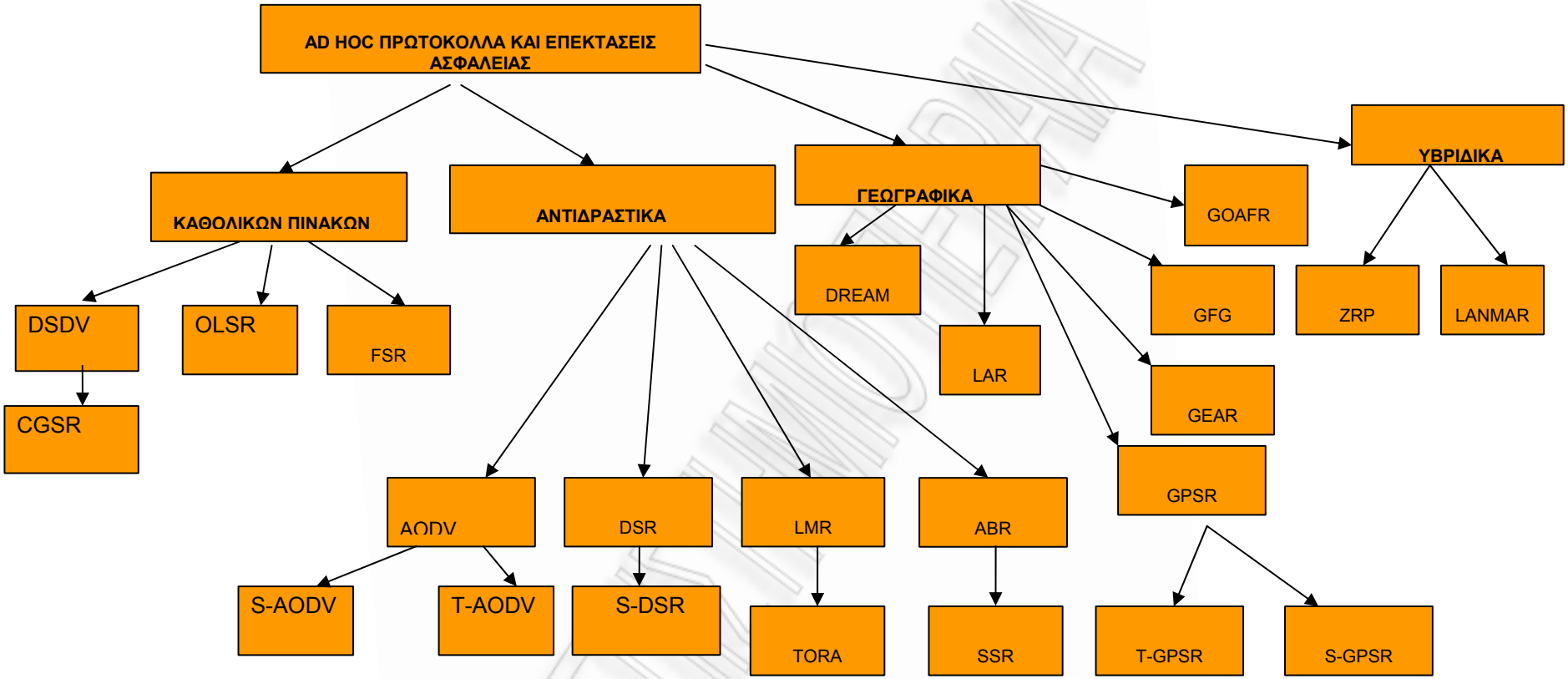
3.6.1.4. Optimized Link State Routing Protocol (OLSR)

Το OLSRv2 [RFC 3626] [36] είναι ένα πρωτόκολλο ειδικά σχεδιασμένο για τα δίκτυα ad hoc. Βασίζεται σε πίνακες δρομολόγησης που ανταλλάσσονται μεταξύ των κόμβων ανά περιοδικά διαστήματα καθώς και στην υπόθεση συμμετρικών ζεύξεων.

Το πρωτόκολλο OLSR βασίζεται σε ένα σύνολο από εκλεγμένους κόμβους, τους “Multi Point Relays” (MPR), που αναλαμβάνουν αυτοί (και μόνο αυτοί) να διαχέουν την πληροφορία ελέγχου, να διαφημίζουν μέσα στα πακέτα “Topology Control” (TC) τη σχέση γειτνίασης με τους κόμβους που τους εξέλεξαν (MPR “selectors”) και επιπλέον αυτοί να υπολογίζουν τα βέλτιστα μονοπάτια προς τον κάθε προορισμό. Με αυτούς τους τρόπους επιτυγχάνεται μείωση της επιβάρυνσης που οφείλεται στις αναμεταδόσεις της μη ελεγχόμενης διάχυσης, αφού μόνο οι MPR επιτρέπεται να αναμεταδώσουν την πληροφορία ελέγχου. Η μέθοδος δρομολόγησης βασίζεται σε λήψη απόφασης από βήμα σε βήμα, δηλαδή οι κόμβοι χρησιμοποιούν μόνο την τοπική πληροφορία για να αποφασίσουν το επόμενο βήμα στο οποίο θα σταλεί το πακέτο. Το OLSR είναι κατάλληλο για μεγάλα-πυκνά δίκτυα και με τυχαία κατανομή της κίνησης ανάμεσα στους κόμβους, εφόσον τότε οι βελτιστοποιήσεις που εισάγει είναι ακόμη πιο πολύ αποδοτικές.



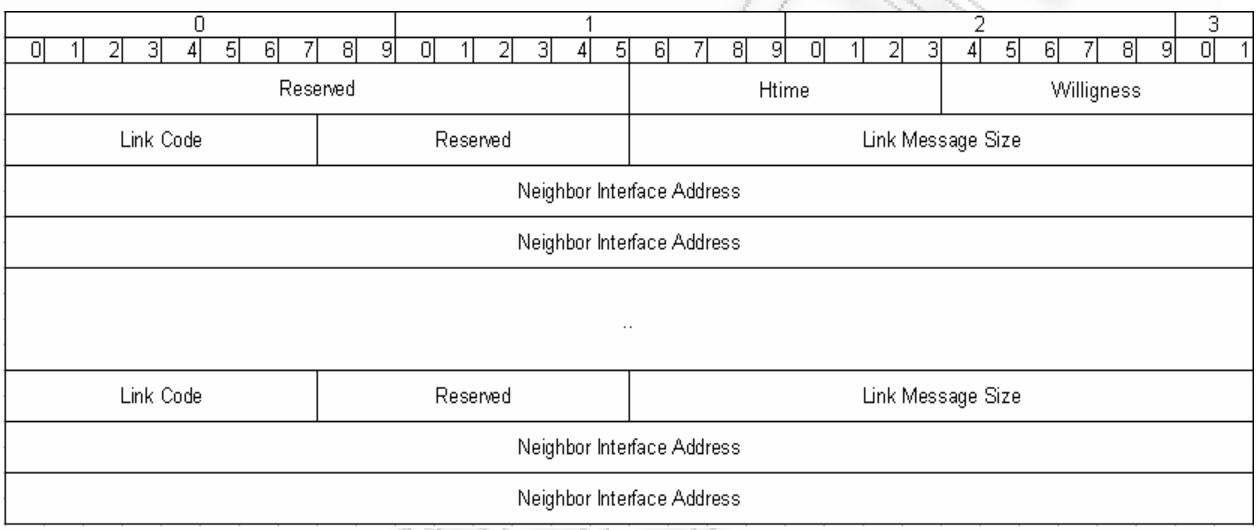
Εικόνα 4. Το σύνολο των “Multi-Point Relay” κόμβων (σε γκρι χρώμα) του κεντρικού κόμβου (σε μαύρο χρώμα) το οποίο καλύπτει όλους τους κόμβους σε απόσταση δύο βημάτων (σε λευκό χρώμα).



Εικόνα 5. Κατηγοριοποίηση των ad hoc πρωτοκόλλων δρομολόγησης.

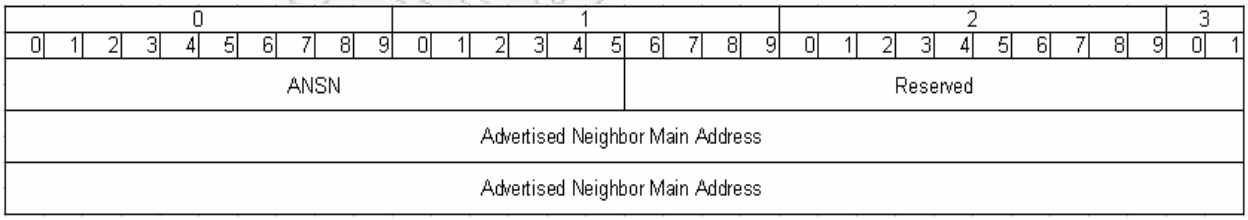
Εκλογή των MPR:

- Κάθε κόμβος εκλέγει τους MPR μεταξύ των κόμβων που βρίσκονται σε απόσταση ενός βήματος από αυτόν. Το σύνολο MPR του κόμβου N, MPR(N) αποτελείται από τους γείτονες που καλύπτουν με αναμετάδοση όλους τους κόμβους που βρίσκονται μέχρι και δύο βήματα μακριά από τον αρχικό κόμβο N. Οι κόμβοι MPR (και μόνο αυτοί) μπορούν να διαφημίζονται μέσα στα περιοδικά μηνύματα ελέγχου προκειμένου να εξοικονομείται το διαθέσιμο εύρος ζώνης.
- Πακέτα Hello, Εικόνα 6. Είναι τα πακέτα ελέγχου που μεταδίδονται περιοδικά (ως πακέτα broadcast) προκειμένου κάθε κόμβος να γνωρίζει ποιους κόμβους έχει εντός της ακτίνας κάλυψής του, τους οποίους ονομάζουμε και γειτονικούς κόμβους. Με τα πακέτα Hello μπορεί να γίνει δυνατή η εκλογή του συνόλου MPR του κάθε κόμβου.



Εικόνα 6. Το OLSR πακέτο Hello, [36].

- Πακέτα *Topology Control* (TC), Εικόνα 7. Είναι μηνύματα ελέγχου που μεταδίδονται περιοδικά ως πακέτα broadcast και τα οποία περιέχουν πληροφορία για την τοπολογία του δικτύου.



Εικόνα 7. Το OLSR πακέτο TC, [36].

- Με βάση τα πακέτα TC και Hello ο κάθε κόμβος δημιουργεί τους πίνακες δρομολόγησης και γίνεται δυνατός ο υπολογισμός των βέλτιστων μονοπατιών δρομολόγησης.

Χαρακτηριστικό της λειτουργίας του OLSRv2 είναι ότι διαθέτει μια βασική λειτουργικότητα (“core functionality”) που παρέχει την κύρια υπηρεσία δρομολόγησης στο δίκτυο MANET και η οποία περιλαμβάνει οντότητες/στοιχεία όπως το NHDP (“Neighborhood Discovery Protocol”), το “packet format”, την εκλογή των MPR και τα πακέτα Hello, ενώ υπάρχουν και επιμέρους στοιχεία που παρέχουν πρόσθετη και κατ’ επιλογή λειτουργικότητα (“auxiliary functions”).

3.6.2. Αντιδραστικά Πρωτόκολλα

Τα αντιδραστικά πρωτόκολλα κατασκευάζουν με αντιδραστικό τρόπο (“reactive”) τα μονοπάτια επικοινωνίας για τους κόμβους-προορισμούς όταν αυτό απαιτηθεί. Δηλαδή όταν υπάρχουν

δεδομένα προς μετάδοση και συγχρόνως δεν υπάρχει γνωστό διαθέσιμο μονοπάτι προς τον τελικό προορισμό τότε η πηγή ενεργοποιεί το μηχανισμό αναζήτησης του μονοπατιού. Τα αντιδραστικά πρωτόκολλα ως εκ τούτου δε συντηρούν καθολικούς πίνακες δρομολόγησης με τα μονοπάτια για όλους τους κόμβους του δικτύου. Η ανακάλυψη του μονοπατιού προς τον τελικό προορισμό επιτυγχάνεται με τη μέθοδο της πλημμύρας ("flooding") ειδικών πακέτων/ερωτημάτων που αναμεταδίδουν όλοι οι ενδιάμεσοι κόμβοι όταν δε διαθέτουν το ζητούμενο μονοπάτι.

Η διαδικασία της ανακάλυψης των μονοπατιών δρομολόγησης (route discovery) αποτελεί την πρώτη φάση στα αντιδραστικά πρωτόκολλα, ενώ σημαντική είναι και η δεύτερη φάση της συντήρησης των μονοπατιών δρομολόγησης (route maintenance) η οποία μπορεί να περιλαμβάνει την εκκίνηση μιας νέας αναζήτησης, όταν δεν υπάρχει κάποιο διαθέσιμο μονοπάτι από την πηγή προς τον προορισμό -εφόσον κάποια ενδιάμεση ζεύξη καθίσταται μη διαθέσιμη-, ή την επαναδρομολόγηση των πακέτων μέσα από εναλλακτικά διαθέσιμα μονοπάτια για το ίδιο ζεύγος πηγής και προορισμού.

Μειονεκτήματα είναι:

1. *Αναπόφευκτη καθυστέρηση* για την εύρεση και την εγκατάσταση του μονοπατιού δρομολόγησης. Αυτό πολλές φορές καθιστά απαγορευτικά τα αντιδραστικά πρωτόκολλα για εφαρμογές πραγματικού χρόνου.

2. *Συμφόρηση* που μπορεί εύκολα να προκληθεί από την πλημμύρα του δικτύου με ένα πολύ μεγάλο αριθμό από πακέτα/ερωτήματα κατά τη φάση της αναζήτησης μονοπατιού.

Μερικά από τα πιο αντιπροσωπευτικά ανακλαστικά πρωτόκολλα είναι τα παρακάτω:

3.6.2.1. Ad Hoc On Demand Distance Vector (AODV)

Το AODV RFC 3651 [7] είναι ένα από τα πρώτα ad hoc πρωτόκολλα το οποίο χρησιμοποιήθηκε τόσο σε εμπορικά προϊόντα όσο και σε ανοιχτού κώδικα λύσεις όπως το "LocusWorld" [72]. Το AODV υποθέτει συμμετρικούς δεσμούς μεταξύ των κόμβων. Σύμφωνα με το πρωτόκολλο αυτό οι κόμβοι δεν ανταλλάσσουν περιοδικά καμία πληροφορία δρομολόγησης ή πίνακες σχετικούς με την τοπολογία του δικτύου (ωστόσο, προκειμένου το επίπεδο του δικτύου να είναι ενήμερο για την τοπική -και μόνο- συνεκτικότητα των κόμβων το πρωτόκολλο προβλέπει την προαιρετική ανταλλαγή περιοδικών πακέτων Hello). Αντίθετα, το πρωτόκολλο καθορίζει ρητά ότι οι διαδικασίες εύρεσης και συντήρησης των μονοπατιών ενεργοποιούνται όταν υπάρχει η ανάγκη μετάδοσης δεδομένων και ταυτόχρονα δεν υπάρχει κάποιο διαθέσιμο μονοπάτι από την πηγή προς τον προορισμό.

Κατά τη διαδικασία εύρεσης μονοπατιού τα πακέτα RREQ αναμεταδίδονται από κόμβο σε κόμβο (διάχυση) μέχρι ο προορισμός να λάβει ένα πακέτο από την πηγή, οπότε και αποκρίνεται με το πακέτο RREP. Βασική παράμετρος του πρωτοκόλλου είναι ο αριθμός ακολουθίας (SN) που φέρει κάθε πακέτο προς ένα συγκεκριμένο προορισμό και ο οποίος αυξάνεται μονοτονικά με κάθε τέτοια νέα μετάδοση. Συγκεκριμένα σε κάθε πακέτο RREQ υπάρχει ο αριθμός ακολουθίας της πηγής και ο αριθμός ακολουθίας του προορισμού. Το SN στο AODV χρησιμοποιείται για να αποφεύγονται τα μη έγκυρα μονοπάτια που δεν έχουν ανανεωθεί (stale). Ακόμη, χρησιμοποιείται στη διαδικασία της επιλογής του βέλτιστου μονοπατιού που τρέχει μόνο στον προορισμό (ή σε κάποιο ενδιάμεσο κόμβο που έχει μονοπάτι προς τον προορισμό) και τέλος χρησιμοποιείται για την αποφυγή βρόχων κατά τη δρομολόγηση των πακέτων. Επίσης σημαντικές για το πρωτόκολλο είναι οι εγγραφές που κάθε κόμβος αποθηκεύει στον πίνακα δρομολόγησης στις οποίες καταγράφονται ο επόμενος και ο προηγούμενος κόμβος προκειμένου να γίνεται αντίστοιχα η εγκατάσταση του μονοπατιού από την πηγή προς τον προορισμό και αντίστροφα.

3.6.2.2. S-AODV

Το πρωτόκολλο S-AODV [10] [11] αποτελεί μία ασφαλή επέκταση του πρωτοκόλλου AODV. Βασίζεται στην προστασία με ψηφιακές υπογραφές των πακέτων RREQ, REPP και RERR. Τα πακέτα αυτά υπογράφονται με το ιδιωτικό κλειδί του κάθε κόμβου αποστολέα και αυθεντικοποιούνται στο δέκτη με το δημόσιο κλειδί του αποστολέα έτσι ώστε το πρωτόκολλο εγγυάται την ακεραιότητα και την αυθεντικότητα των μηνυμάτων δρομολόγησης. Σύμφωνα με το S-AODV οι κρυπτογραφικές αυτές πράξεις της υπογραφής των πακέτων και της επαλήθευσης εκτελούνται σε κάθε ένα κόμβο που συμμετέχει στο μονοπάτι δρομολόγησης από την πηγή προς τον τελικό αποδέκτη, γεγονός το οποίο επιφέρει αναπόφευκτη επεξεργαστική επιβάρυνση στους κόμβους και επιπλέον καθυστέρηση στην παράδοση των μηνυμάτων και σπατάλη του εύρους ζώνης καθώς το μέγεθος των πακέτων αυξάνεται σημαντικά. Ακόμη το S-AODV προβλέπει ότι υπογράφονται μόνο τα μη μεταβλητά πεδία των επικεφαλίδων των πακέτων, ενώ τα μεταβλητά πεδία όπως ο αριθμός βημάτων “hop count” προστατεύονται με τη χρήση αλυσίδων συναρτήσεων κατακερματισμού hash chains. Έτσι, εφόσον απαιτείται η πηγή να λάβει απάντηση RREP με υπογραφή από τον τελικό κόμβο-προορισμό, ένας κακόβουλος κόμβος που παρεμβάλλεται στις επικοινωνίες δεν μπορεί να μειώσει το “hop count” και να απαντήσει στο RREQ της πηγής με ένα αλλοιωμένο πακέτο RREP προκειμένου να επιτύχει να επιλεγεί αυτός σαν ενδιάμεσος κόμβος του μονοπατιού.

Τα ασφαλή ad hoc πρωτόκολλλα, όπως το S-AODV, επιχειρούν την προστασία των πακέτων που κυκλοφορούν στο δίκτυο με κρυπτογραφικές μεθόδους. Σύμφωνα με το S-AODV τα πεδία των πακέτων που μεταβάλλονται από βήμα σε βήμα στο μονοπάτι δρομολόγησης για λόγους υπολογιστικής οικονομίας κρυπτογραφούνται με συναρτήσεις κατακερματισμού, ενώ τα πεδία που παραμένουν αμετάβλητα μέχρι να φτάσουν τα πακέτα στον προορισμό προστατεύονται περισσότερο για παράδειγμα με τη χρήση υπογραφών. Αυτό αποτελεί σημαντική βελτίωση στο παρεχόμενο επίπεδο προστασίας, ωστόσο δεν μπορεί να αποφύγει τις επιθέσεις παραποίησης ταυτότητας, επανάληψης μηνυμάτων και της αντικατάστασης των μηνυμάτων σε μια επίθεση ενδιάμεσου κόμβου (“Man in the Middle”).

Η αιτιολογία είναι ότι στα περισσότερα από τα προστατευόμενα πρωτόκολλα ad hoc οι διευθύνσεις των μερών που επικοινωνούν (δηλαδή οι διευθύνσεις του πομπού και δέκτη ή ισοδύναμα η κεφαλίδα του πακέτου) κρυπτογραφούνται ξεχωριστά από το κυρίως σώμα που περιέχει τα δεδομένα του πακέτου. Έτσι στην περίπτωση που ο δέκτης δεν γνωρίζει τη διεύθυνση του πομπού, ακόμη και εάν χρησιμοποιούνται ψηφιακές υπογραφές, ένας ενδιάμεσος κόμβος μπορεί να συλλάβει τις κρυπτογραφημένες διευθύνσεις και να τις αντικαταστήσει εύκολα με τη δική του, χωρίς να γίνει αντιληπτός.

3.6.2.3. Trusted AODV

Μια διαφορετική επέκταση ασφάλειας του γνωστού πρωτοκόλλου AODV είναι και το Trusted-AODV [12]. Σύμφωνα με την παραλλαγή αυτή εισάγεται ένας μηχανισμός εγκατάστασης εμπιστοσύνης με ανταλλαγή γνωμών σχετικών με το βαθμό εμπιστοσύνης των κόμβων (“trust recommendations”). Επίσης, γίνεται ανανέωση των σχέσεων εμπιστοσύνης (“trust updates”) μεταξύ των γειτονικών κόμβων. Η γνώμη που σχηματίζει ένας κόμβος για κάποιον άλλον κόμβο βασίζεται σε κανόνες/πολιτικές που σχετίζονται με τον αριθμό των μηνυμάτων που έχουν ανταλλάξει μεταξύ τους οι δύο κόμβοι επιτυχώς.

3.6.2.4. Adaptive Secure AODV

Μια ακόμη επέκταση του AODV είναι το Adaptive S-AODV [13] που ουσιαστικά αποτελεί ένα τρόπο υλοποίησης του “Secure-AODV”. Σύμφωνα με την υλοποίηση του Adaptive S-AODV οι λειτουργίες της δρομολόγησης και της κρυπτογράφησης εκτελούνται από δύο διαφορετικά νήματα

έτσι ώστε να μην μπλοκάρει η μία την άλλη με αποτέλεσμα η επίδοση του S-AODV να είναι καλύτερη. Επίσης το A-SAODV εισάγει και προσαρμοστικό μηχανισμό απάντησης με χρήση των RREP από τους ενδιάμεσους κόμβους που λαμβάνουν το RREQ για προορισμό προς τον οποίο διαθέτουν μονοπάτι. Σύμφωνα με το “adaptive reply decision” του A-SAODV ένας ενδιάμεσος αποθηκεύει στην προσωρινή μνήμη του την υπογραφή της πηγής, υπογράφει με το δικό του κλειδί και απαντάει στέλνοντας επίσης και την υπογραφή της πηγής, μόνο αν διαθέτει τους απαραίτητους πόρους, αλλιώς προωθεί περαιτέρω το πακέτο αναζήτησης μονοπατιού.

3.6.2.5. Dynamic Sorce Routing (DSR)

Το DSR [8] είναι ένα ad hoc multi-hop πρωτόκολλο το οποίο είναι προσαρμοσμένο να λειτουργεί αποδοτικά κάτω από τις μεταβλητές συνθήκες που επικρατούν στα κινητά ασύρματα δίκτυα ad hoc. Πέραν του ότι τα μονοπάτια ανακαλύπτονται δυναμικά όποτε αυτό απαιτείται από μια πηγή, το βασικό χαρακτηριστικό του DSR είναι ότι κάθε πακέτο δεδομένων φέρει στην επικεφαλίδα μια λίστα στην οποία εγγράφονται όλοι οι κόμβοι και με διατεταγμένη σειρά από τους οποίους πρέπει να διέλθει το πακέτο αυτό. Η μέθοδος αυτή είναι γνωστή ως δρομολόγηση πηγής. Αποσκοπεί δε στη μείωση της επιβάρυνσης αναζήτησης μονοπατιών από τους ενδιάμεσους κόμβους οι οποίοι αποθηκεύουν σε προσωρινή μνήμη “cache” την πληροφορία με τη λίστα των κόμβων του μονοπατιού δρομολόγησης. Επεκτάσεις ασφάλειας του πρωτοκόλλου DSR είναι το Secure-DSR [17] και το Trusted-DSR [63].

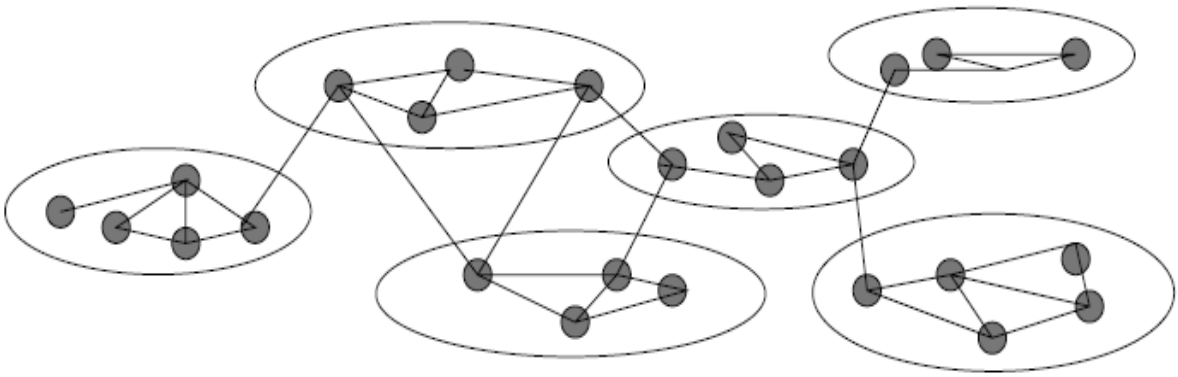
3.6.2.6. Associativity Based Routing (ABR)

Το πρωτόκολλο ABR [18] λαμβάνει υπόψη κατά τη δρομολόγηση τη σταθερότητα των ζεύξεων που συνθέτουν το μονοπάτι δρομολόγησης και όχι τον ελάχιστο αριθμό βημάτων από την πηγή προς τον προορισμό. Αυτό γίνεται εφόσον είναι δυνατό το μικρότερο μονοπάτι να μην είναι αυτό με την καλύτερη ποιότητα σήματος και άρα να υποφέρει από μεγαλύτερη απώλεια πακέτων και καθυστερήσεις. Το πρωτόκολλο ABR εισήγαγε ένα νέο μέτρο δρομολόγησης το οποίο υπολογίζει το βαθμό σταθερότητας της συνδετικότητας μεταξύ των γειτονικών κόμβων (“degree of association stability”) προκειμένου να επιλεγεί το μονοπάτι δρομολόγησης.

3.6.3. Ιεραρχικά Πρωτόκολλα

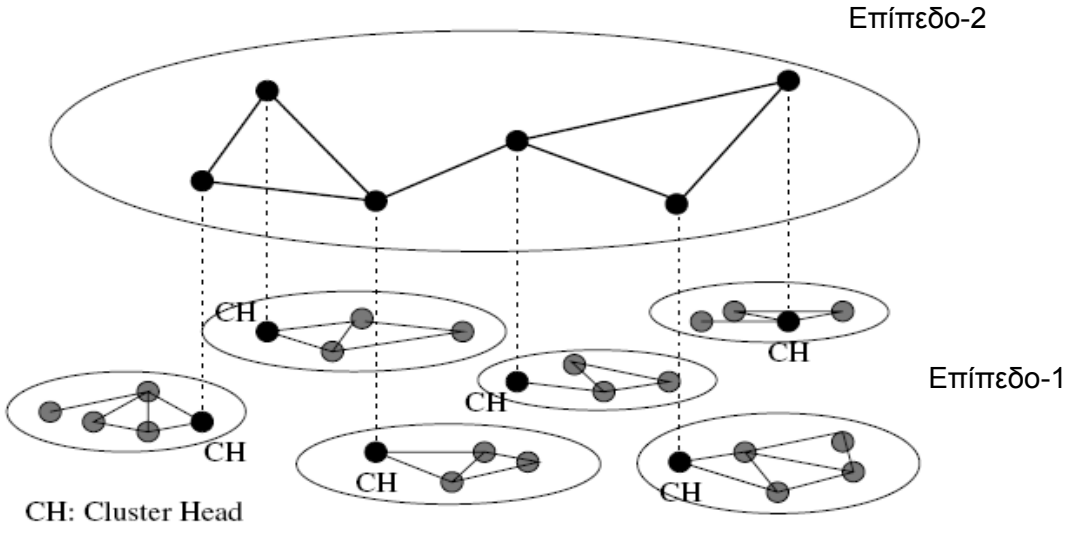
Μια άλλη κατηγορία ad hoc πρωτοκόλλων είναι τα ιεραρχικά ad hoc πρωτόκολλα τα οποία εισάγουν πολλαπλά επίπεδα ιεραρχίας και τα οποία χωρίζουν το δίκτυο σε διακριτές ή επικαλυπτόμενες ομάδες με σκοπό να μπορέσει να είναι πιο αποδοτική η δρομολόγηση των πακέτων ιδιαίτερα όταν το μέγεθος του δικτύου αυξάνεται. Ένα δεύτερο πλεονέκτημα των ιεραρχικών πρωτοκόλλων είναι ότι με αυτά ο χρόνος ζωής του δικτύου επιμηκύνεται, κάτι το οποίο μπορεί να είναι ιδιαίτερα επιθυμητό στην περίπτωση των δικτύων μικροσκοπικών αισθητήρων (WSN) όπου τα αποθέματα ενέργειας στους κόμβους είναι πολύ περιορισμένα.

Η κύρια ιδέα της χρήσης συστάδων (“clusters”) εντός των δικτύων ad hoc είναι να χωριστεί το δίκτυο σε ομάδες κόμβων που αποτελούνται από απλούς κόμβους-μέλη και από ισχυρότερους (συνήθως) κόμβους-αρχηγούς (“cluster heads”). Σε αντιπαράθεση με την απλή δομή που απεικονίζεται στην Εικόνα 8 η ομαδοποίηση των κόμβων σε clusters δίνει δομή σαν αυτή που απεικονίζεται στην Εικόνα 9. Δημιουργείται μια ιεραρχία όπου οι κόμβοι “cluster heads” αφού εκλεγούν στο Επίπεδο 1 γίνονται απλοί κόμβοι για το υψηλότερο Επίπεδο 2 στην ιεραρχία. Στο υψηλότερο επίπεδο δημιουργούνται υπερομάδες και η δομή αυτή μπορεί να συνεχιστεί επαναληπτικά με πολλά επίπεδα ιεραρχίας.



Εικόνα 8. Δίκτυο ad hoc με επίπεδη δομή.

Σε μια τέτοια δομή ένας κόμβος που πρέπει να επικοινωνήσει με κόμβο που δεν ανήκει στην ομάδα του θα προωθήσει το πακέτα του στον “cluster head” που ανήκει ο οποίος θα αναλάβει να το προωθήσει σε επόμενο “cluster head” έως ότου βρεθεί ένας “cluster head” που διαθέτει μονοπάτι δρομολόγησης για τον τελικό προορισμό.



Εικόνα 9. Δίκτυο ad hoc με ιεραρχική δομή δυο επιπέδων.

Οι κόμβοι-αρχηγοί των ομάδων είναι συνήθως κόμβοι με περισσότερους πόρους από τους απλούς κόμβους και, επομένως, είναι ικανοί να εκτελέσουν εργασίες όπως:

- ***Ενδοδικτυακή επεξεργασία των μηνυμάτων***. Οι αρχηγοί ομάδων πριν προωθήσουν (προς το σταθμό βάσης ή/και προς άλλες μακρινές ομάδες) τα μηνύματα που συγκεντρώνουν από τα απλά μέλη, τα επεξεργάζονται ενδο-δικτυακά υπολογίζοντας, για παράδειγμα, τη μέση τιμή, τη διάμεσο τιμή, τη συσχέτιση και άλλα χαρακτηριστικά των δεδομένων και των μετρήσεων που προέρχονται από τους κινητούς απλούς κόμβους δικτύων MANET και τους αισθητήρες δικτύων WSN.
- ***Προώθηση των μηνυμάτων των ομάδων***. Τα συναθροισμένα δεδομένα διαβιβάζονται από τους αρχηγούς προς τον τελικό προορισμό έτσι ώστε οι απλοί κόμβοι να απαλλάσσονται από το φόρτο αυτό. Η στρατηγική της δρομολόγησης μεταξύ των ομάδων εξαρτάται από το συγκεκριμένο ιεραρχικό πρωτόκολλο.

- ***Διαχείριση των πόρων του ραδιοφάσματος***. Διάφορα σχήματα πολλαπλής πρόσβασης στο ασύρματο μέσο (όπως TDMA ή CDMA) υιοθετούνται από τους κόμβους-αρχηγούς που καθορίζουν με αυτόν τον τρόπο την σειρά πρόσβασης των απλών κόμβων στο κανάλι με τη χρήση αποδοτικών αλγορίθμων διαχείρισης του ραδιοφάσματος.
- ***Επεξεργασία πολυμεσικών συνόδων και πολυμεσικών δεδομένων***. Οι πολυμεσικές διασκέψεις (videoconference) μεταξύ κόμβων δικτύων MANET αλλά και η μεταφορά κυρίως στατικών εικόνων στα δίκτυα WSN αποτελεί τρέχον πεδίο έρευνας και μπορεί αποδοτικότερα να επιτευχθεί με την ιεράρχηση της δομής των δικτύων αυτών σε συστάδες καθώς και με τη διαχείριση των πολυμεσικών εφαρμογών και των απαραίτητων συνδέσεων από τους ενισχυμένους σε πόρους κόμβους-αρχηγούς.

Επιπρόσθετες λειτουργίες που μπορούν να αναλάβουν οι κόμβοι-αρχηγοί σχετίζονται με την ασφάλεια των επικοινωνιών εντός της συστάδας και μεταξύ των συστάδων. Περιληπτικά οι λειτουργίες αυτές περιλαμβάνουν τα εξής.

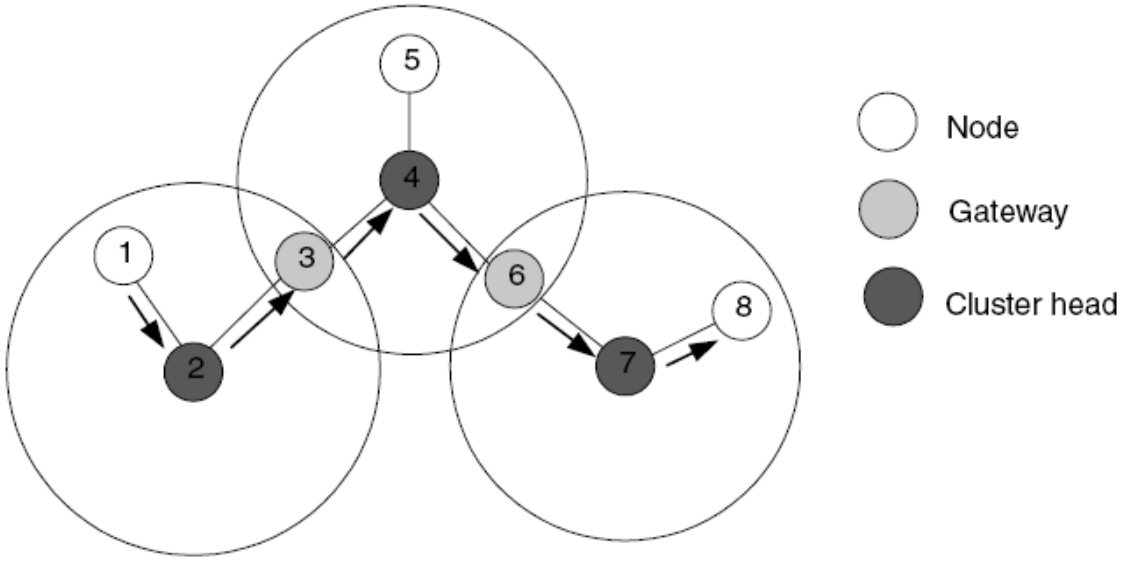
- ***Διαχείριση κλειδιών, κρυπτογράφηση μηνυμάτων και αυθεντικοποίηση των κόμβων***. Σε ένα δίκτυο ad hoc πολλές φορές οι αρχηγοί κόμβοι παίρνουν το ρόλο του τοπικού εξυπηρετητή πιστοποίησης. Έτσι λειτουργίες όπως η έκδοση και η διαμοίραση κλειδιών για την κρυπτογράφηση δεδομένων και την πιστοποίηση των απλών κόμβων μπορούν με κατανεμημένο τρόπο να εκτελούνται από τους κόμβους-αρχηγούς.
- ***Ανίχνευση και αντιμετώπιση εισβολών***. Αλγόριθμοι εντοπισμού και απομόνωσης των ύποπτων κόμβων καθώς και μηχανισμοί αντίδρασης και ανάκαμψης από μια επίθεση σε μία περιοχή του δικτύου είναι αποδοτικότερο να τρέχουν στους ισχυρότερους κόμβους-αρχηγούς, ιδιαίτερα σε ένα δίκτυο WSN μεγάλης κλίμακας. Σε αυτήν την περίπτωση η συνεργασία μεταξύ των κόμβων-αρχηγών μπορεί να προσφέρει ακόμη υψηλότερα επίπεδα ασφαλείας.

3.6.3.1. Cluster Based Routing Protocol (CBRP) και Clustered Gateway Switched Routing (CGSR)

Δύο από τα πιο γνωστά πρωτόκολλα δρομολόγησης βασισμένα σε ιεραρχίες είναι το “Clustered Based Routing Protocol” (CBRP) [16] και το “Clustered Gateway Switched Routing” (CGSR) [15]. Στο CBRP οι δεσμοί δεν είναι κατ’ ανάγκη συμμετρικοί το οποίο αποτελεί πλεονέκτημα για τη διατήρηση της συνεκτικότητας εντός και μεταξύ των clusters. Το πρωτόκολλο βασίζεται σε πίνακες και δημιουργεί clusters που εκτείνονται μέχρι και δύο βήματα. Στο CBRP οι κόμβοι-αρχηγοί, και μόνο αυτοί, προωθούν τα μηνύματα.

Στο πρωτόκολλο CGSR το οποίο είναι πρωτόκολλο που επίσης βασίζεται σε καθολικούς πίνακες δρομολόγησης η αποστολή των πακέτων από cluster σε cluster γίνεται μέσα από τους κόμβους-πύλες, όπως φαίνεται στην Εικόνα 10. Οι κόμβοι-πύλες (gateways) είναι ενδιάμεσοι δρομολογητές που βρίσκονται στην επικαλυπτόμενη περιοχή μεταξύ δύο γειτονικών clusters και οι οποίοι σκοπό έχουν να αυξήσουν τη συνεκτικότητα του δικτύου.

Οι κόμβοι-πύλες αναλαμβάνουν να προωθήσουν τα μηνύματα προς τους τοπικούς κόμβους-αρχηγούς οι οποίοι στη συνέχεια τα παραδίδουν στους απλούς κόμβους-προορισμούς που βρίσκονται στους πίνακές τους.



Εικόνα 10. Δρομολόγηση με το CGSR από τον κόμβο 1 στον κόμβο 8, [15].

3.6.3.2. LEACH

Το LEACH [38] ("Low-Energy Adaptative Clustering Hierarchy") είναι από τα πρώτα ιεραρχικά πρωτόκολλα που σχεδιάστηκαν ειδικά για τα δίκτυα αισθητήρων WSN. Το βασικό του χαρακτηριστικό είναι ότι η ενέργεια διατηρείται στους κόμβους με το να γίνεται εξισορρόπηση του χρόνου που οι κόμβοι αναλαμβάνουν το ρόλο του cluster head. Ουσιαστικά η επιλογή των κόμβων αρχικά γίνεται με τυχαίο τρόπο, ενώ η εναλλαγή των ρόλων από cluster head σε απλό μέλος γίνεται με τον αλγόριθμο "round robin".

3.6.4. Υβριδικά Πρωτόκολλα

Τα υβριδικά ad hoc πρωτόκολλα αποτελούν συνδυασμό των αντιδραστικών ("reactive") και των προληπτικών ("proactive") πρωτοκόλλων ad hoc που κάνουν χρήση καθολικών πινάκων. Η δρομολόγηση συνήθως γίνεται μεταξύ κόμβων που οργανώνονται σε ζώνες που βρίσκονται σε γεωγραφικά απομακρυσμένες περιοχές. Συνεπώς στην κατηγορία των υβριδικών πρωτοκόλλων, όπως θα δούμε και παρακάτω, εμπίπτουν αρκετά γεωγραφικά όπως και ιεραρχικά πρωτόκολλα. Σαν υβριδικό ξεχωρίζουμε το βασισμένο σε ζώνες πρωτόκολλο Zone Routing Protocol (ZRP) [34], στο οποίο εντός μιας ζώνης η δρομολόγηση γίνεται με διατήρηση καθολικών πινάκων, ενώ η δρομολόγηση μεταξύ των ζωνών γίνεται κατ' απαίτηση (on demand), δηλαδή με αντιδραστική εύρεση και εγκατάσταση των μονοπατιών. Επίσης σε αυτήν την κατηγορία ανήκει το ZHLS [30], ενώ εμπίπτει το LANMAR [31] και το Fisheye State Routing (FSR) [35].

3.6.5. Γεωγραφικά Πρωτόκολλα

Μια άλλη κατηγορία ad hoc πρωτοκόλλων είναι τα γεωγραφικά πρωτόκολλα, δηλαδή πρωτόκολλα δρομολόγησης κατάλληλα για δίκτυα MANET, WSN, VANET τα οποία βασίζονται στην υπόθεση της γνώσης της θέσης των κόμβων για τη λήψη απόφασης στη δρομολόγηση. Τα γεωγραφικά πρωτόκολλα δρομολόγησης είναι αυτά που στην απλούστερη περίπτωση σαν επόμενο βήμα προς τον τελικό προορισμό επιλέγουν εκείνο τον κόμβο που βρίσκεται σε κοντινότερη απόσταση από τον κόμβο-προορισμό. Τα γεωγραφικά πρωτόκολλα μπορεί να είναι προληπτικά όπως το GPSR [24] ή ιεραρχικά όπως το το υβριδικό Zone Routing Protocol-ZRP [34] (το ZRP χρησιμοποιεί ένα

προληπτικό και ένα αντιδραστικό πρωτόκολλο) και το ιεραρχικό ZHLSR [30]. Άλλα παραδείγματα γεωγραφικών πρωτοκόλλων είναι το TORA [19], ALARM [29], LAR [22], DREAM [20], το Landmark Routing Protocol (LANMAR) [31], το Gegraphic Location Service, GLS [21], GPSR [24], [29], GOAFR [32], GFG [33]), το OD-GPSR που είναι μια παραλλαγή του GPSR η οποία λαμβάνει υπόψη την ασυμμετρία των ζεύξεων [64] και τέλος το γεωγραφικό πρωτόκολλο της εργασίας [65].

3.6.5.1. Greedy Perimeter Stateless Routig (GPSR)

Το GPSR [24] είναι ένα γεωγραφικό πρωτόκολλο που λειτουργεί σε δύο “modes”: το “greedy forwarding mode” και το “perimeter forwarding mode”. Κατά τη greedy προώθηση των μηνυμάτων το επόμενο βήμα επιλέγεται από τη λίστα με όλους τους γείτονες που διαθέτουν οι κόμβοι και είναι αυτός ο γείτονας με τη μικρότερη απόσταση από τον τελικό κόμβο-προορισμό. Αν δεν υπάρχει κάποιος τέτοιος γείτονας και ο τελικός κόμβος είναι εκτός κάλυψης από τον τρέχοντα κόμβο τότε το πρωτόκολλο μπαίνει σε “perimeter mode” ώστε να αποφύγει αυτό το σημείο στην τοπολογία το οποίο ονομάζεται σημείο “void”. Το μονοπάτι τότε προς τον τελικό προορισμό καθορίζεται μέσα από τα “planar faces” τα οποία αποτελούν ένα συνδεδεμένο υποσύνολο της τοπολογίας του δικτύου που κατασκευάζεται με σκοπό να αποφεύγονται οι βρόχοι κατά τη δρομολόγηση πακέτων και να επιλύονται τα σημεία void με περιμετρική δρομολόγηση η οποία είναι συνήθως περισσότερων βημάτων από ότι απαιτεί η greedy δρομολόγηση. Ένα άλλο μειονέκτημα είναι ότι οι τοπολογίες “planar” κατασκευάζονται από το GPSR εκ των προτέρων (“proactively”) με την περιοδική μετάδοση ειδικών σημάτων “probes”.

3.6.5.2. Trusted GPSR

Το Trusted-GPSR [25] αποτελεί τη βασική επέκταση ασφάλειας του GPSR. Βασίζεται στην αξιολόγηση των κόμβων με τιμές/επίπεδα εμπιστοσύνης. Και σε αυτό το πρωτόκολλο η τιμή της εμπιστοσύνης ενός κόμβου για ένα γείτονά του μεταβάλλεται ανάλογα με τη συμπεριφορά που έχει ο γειτονικός κόμβος σε σχέση με το αν προωθεί ή όχι τα πακέτα που στέλνονται σε αυτόν. Απαραίτητος μηχανισμός επομένως για την βαθμολόγηση των κόμβων είναι ο μηχανισμός “passive ACK” κατά τον οποίο ο αρχικός κόμβος πρέπει να τεθεί σε “promiscuous mode”, δηλαδή κρυφακούει το κανάλι για να διαπιστώσει αν ο γείτονας (που επιθυμεί να αξιολογήσει) προώθησε περαιτέρω τα πακέτα που του μετέδωσε. Ο μηχανισμός “passive ACK” υιοθετήθηκε πρωταρχικά στις λύσεις “Watchdog” και “Pathrate” [69] όπου κάθε κόμβος παρακολουθεί τη συμπεριφορά των γειτόνων του ως προς την προώθηση των πακέτων που λαμβάνουν και τους βαθμολογεί είτε θετικά είτε αρνητικά, ωστόσο έχει το μειονέκτημα ότι καταναλώνει τη διαθέσιμη ενέργεια των περιορισμένων κόμβων. Οι τιμές εμπιστοσύνης για τον ίδιο γείτονα μπορεί να διαφέρουν από κόμβο σε κόμβο. Οι τιμές αυτές αποθηκεύονται στους πίνακες δρομολόγησης και λαμβάνονται υπόψη με σταθμισμένο τρόπο (δηλαδή σταθμίζεται το επίπεδο εμπιστοσύνης ενός υποψήφιου κόμβου και η απόστασή του από τον προορισμό) κατά τη διαδικασία της λήψης απόφασης για τη γεωγραφική δρομολόγηση των πακέτων.

Μια άλλη παραλλαγή του GPSR που εφαρμόζεται στα δίκτυα αισθητήρων [68] λαμβάνει υπόψη το επίπεδο εμπιστοσύνης των κόμβων όπου η απόφαση για τη δρομολόγηση εξαρτάται από τις εξής τρεις παραμέτρους: από την απόσταση, από το υπολογισμένο επίπεδο εμπιστοσύνης των κόμβων και από την κάλυψη των αισθητήρων. Ως επόμενο βήμα στο μονοπάτι δρομολόγησης προτιμώνται με αυτήν την τεχνική αισθητήρες που καλύπτουν μικρή επιφάνεια έτσι ώστε αν αυτοί μείνουν δίχως άλλη διαθέσιμη ενέργεια η περιοχή που θα μείνει δίχως παρακολούθηση να είναι η μικρότερη δυνατή.

3.6.5.3. Improved GPSR

Μια άλλη βελτιωμένη επέκταση του GPSR συναντάμε στο [66] όπου προτείνεται σχήμα GPSR που

αμύνεται στη επίθεση Sybil και στις επιθέσεις προώθησης μηνυμάτων. Κατά την επίθεση Sybil ένας κακόβλουλος κόμβος μπορεί να διαφημίσει ότι βρίσκεται σε πολλές θέσεις και επίσης να δηλώσει πολλές διαφορετικές ταυτότητες ή ακόμη να προκαλέσει βρόχους δρομολόγησης με το να αναφέρει ψευδείς θέσεις για τους γείτονες κόμβους. Το κατανεμημένο σχήμα αυθεντικοποίησης (κ, ν) που χρησιμοποείται στο [66] προφυλάσσει από τις ψευδείς ταυτότητες. Χρησιμοποιείται επίσης διαμέριση του δικτύου σε κόμβους-αρχηγούς οι οποίοι περιοδικά παρακολουθούν το δίκτυο.

3.6.6. Πρωτόκολλα Πολλαπλής Εκπομπής

Παραδείγματα ad hoc πρωτοκόλλων που χρησιμοποιούν την πολλαπλή εκπομπή μηνυμάτων ("multicasting") προς τα μέλη ομάδων είναι τα αναφερόμενα στις εγασίες [22], [27] και [28].

3.7. ΑΝΑΛΥΣΗ ΤΩΝ ΑΠΕΙΛΩΝ ΚΑΤΑ ΤΩΝ ΔΙΚΤΥΩΝ AD HOC

Στην παράγραφο αυτή θα αναλύσουμε τις πιο γνωστές κατηγορίες επιθέσεων που απειλούν τα δίκτυα ad hoc. Αρχικά θα ερευνήσουμε ποιες είναι οι γενικές αδυναμίες (οι οποίες είναι παρούσες στην πλειοψηφία των πρωτοκόλλων ad hoc) τις οποίες μπορεί να εκμεταλλευτεί ένας κακόβουλος κόμβος ως "ανοιχτές πόρτες" για να εισέλθει στο δίκτυο ad hoc. Στη συνέχεια, θα εξετάσουμε μία προς μία τις επιθέσεις κατά συγκεκριμένων πρωτοκόλλων δρομολόγησης, τη μέθοδο και τους στόχους του επιτιθέμενου, τα μέσα που χρησιμοποιεί και τις αδυναμίες που εκμεταλλεύεται κατά περίπτωση μελέτης του πρωτοκόλλου δρομολόγησης, ενώ στο τέλος θα περιγράψουμε το αποτέλεσμα που επιτυγχάνεται κατά των κόμβων που ο επιτιθέμενος καταφέρνει να συμβιβάσει και κατά του δικτύου συνολικά. Επίσης, για κάθε τύπο επίθεσης θα δοθούν και τα αντίστοιχα αντίμετρα που έχουν ήδη προταθεί καθώς και λύσεις αντιμετώπισης των επιθέσεων που θεωρούμε ότι είναι καινοτομίες.

3.7.1. Στόχοι του Επιτιθέμενου

Από ένα ευρύ φάσμα πιθανών στόχων κατά των δικτύων ad hoc, οι βασικότεροι στόχοι που έχουν ενδιαφέρον για τους επιτιθέμενους περιγράφονται πιο κάτω:

- ***Ο συμβιβασμός των επικοινωνιών του δικτύου***. Αυτό περιλαμβάνει τη σύλληψη και τη λαθραία ανάγνωση μηνυμάτων. Στην περίπτωση που οι επικοινωνίες διεξάγονται με ανοιχτό τρόπο, δηλαδή δίχως τη χρήση κάποιας προστασίας που να πειρλαμβάνει κωδικοποίηση των δεδομένων, ένας κακόβουλος χρήστης ("sniffer") μπορεί πολύ εύκολα να κρυφακούσει το ασύρματο μέσο και να υπεξαιρέσει την ευαίσθητη πληροφορία. Επίσης, το ίδιο μπορεί να επιτευχθεί σε συνθήκες αδύναμης προστασίας των δεδομένων όταν δηλαδή ο επιτιθέμενος έχει καταφέρει να σπάσει τον αλγόριθμο ή ακόμη χειρότερα να μαντέψει ή να υπολογίσει κρυφό υλικό όπως κλειδιά, passwords, pass phrases, οπότε σε αυτή την περίπτωση μπορεί να αποκωδικοποιήσει τα δεδομένα. Είναι αξιοσημείωτο ότι η σύλληψη και μόνο –χωρίς ανάγνωση– των μηνυμάτων μπορεί να αποβεί καταστροφική στην περίπτωση κρίσιμων εφαρμογών εφόσον δίνει την ευκαιρία στον επιτιθέμενο να προκαλέσει σύγχυση στο δίκτυο με μια απλή επανάληψη των μηνυμάτων που αναμένονται από τους αυθεντικούς χρήστες αυτού.

- ***Η επίδοση του δικτύου***. Στόχος εδώ είναι η αλλοίωση της ορθής λειτουργίας του δικτύου και άρα η μείωση δεικτών απόδοσης όπως η διαπερατότητα, η καθυστέρηση προώθησης/εξυπηρέτησης μηνυμάτων, η κατανάλωση της διαθέσιμης μνήμης στους κόμβους κ.α. (βλέπε και επίθεση Denial of Service).

- ***Η συνεκτικότητα*** μεταξύ των κόμβων ad hoc. Αυτό περιλαμβάνει τη διάρρηξη μέρους (ή και όλων) των δεσμών του δικτύου. Μπορεί δε να επιτευχθεί είτε με διείσδυση στο δίκτυο

και στη συνέχεια την άρνηση προώθησης των μηνυμάτων, είτε με ισχυρές ράδιο-εκπομπές και ράδιο-παρεμβολές.

- ***Το φυσικό επίπεδο των κόμβων***. Πολλές φορές οι επιθέσεις στοχεύουν το φυσικό επίπεδο των κόμβων, δηλαδή το υλικό τους. Έτσι στην περίπτωση ενός WSN, ένας επιτιθέμενος μπορεί να συλλάβει ένα αισθητήρα, να αντιγράψει το υλισμικό (hardware) του, ή ακόμη να προβεί σε στατιστική ανάλυση της ισχύος με την οποία εκπέμπει το θύμα στο ράδιο-φάσμα με απώτερο σκοπό να εξαγάγει το μυστικό κλειδί που χρησιμοποιεί ο κόμβος για τη μετάδοση των κρυφών μηνυμάτων. Τέτοιου είδους απειλές είναι εκτός των ορίων της παρούσης διατριβής.

3.7.2. Χαρακτήρας του Επιτιθέμενου

Διακρίνουμε το χαρακτήρα των επιτιθεμένων στις τέσσερις παρακάτω επιμέρους κατηγορίες.

- ***Παθητικός επιτιθέμενος***. Ο παθητικός επιτιθέμενος ανήκει στην κατηγορία των παραδοσιακών επιθέσεων και ενδιαφέρεται μόνο για τη συλλογή των ευαίσθητων στοιχείων από το δίκτυο ad hoc, το οποίο θέτει σε κίνδυνο την απαίτηση για την ιδιωτικότητα και την εμπιστευτικότητα των επικοινωνιών. Συνήθεις επιθέσεις αυτού του είδους περιλαμβάνουν τη λαθραία ανάγνωση μηνυμάτων μετά την αποκωδικοποίησή τους (όταν αυτά κωδικοποιούνται από τον αποστολέα), την επανάληψη των μηνυμάτων σε ύστερο χρόνο όπως για παράδειγμα την επανάληψη πακέτων επιβεβαιώσεων (ack) χωρίς δε ο επιτιθέμενος να χρειάζεται να αποκωδικοποιήσει τα μηνύματα που επαναλαμβάνει.

- ***Ενεργητικός επιτιθέμενος***. Ο ενεργός επιτιθέμενος ενδιαφέρεται να αποσαρθρωθεί η λειτουργία των δικτύων και να υποβιβαστεί η επίδοσή τους. Σε αυτήν την κατηγορία ανήκουν οι σύγχρονες, συνδυασμένες απειλές και επιθέσεις κατά των δικτύων τις οποίες θα προσπαθήσουμε να αντιμετωπίσουμε. Για παράδειγμα, ένας ενεργός επιτιθέμενος καταφέρνει να προσποιηθεί ότι είναι ένας νόμιμος κόμβος του δικτύου ad hoc και κατόπιν διαβάζει λαθραία, τροποποιεί επιλεκτικά, επαναλαμβάνει σε ύστερο χρόνο, ή και απορρίπτει τα μηνύματα που συλλαμβάνει. Σε αυτήν τη κατηγορία μπορούμε να εντάξουμε τις επιθέσεις που στόχο έχουν τη μείωση της επίδοσης (performance) του δικτύου και ιδιαίτερα τη διαθεσιμότητα των υπηρεσιών αυτού. Οι πιο γνωστές ενεργητικές επιθέσεις οι οποίες στοχεύουν τη διαθεσιμότητα των ad hoc υπηρεσιών είναι η επίθεση Denial of Service και η Man in the Middle attack οι οποίες θα εξεταστούν αναλυτικά αργότερα.

- ***Εσωτερικός επιτιθέμενος***. Ο εσωτερικός επιτιθέμενος έχει πρόσβαση στο δίκτυο WSN ή MANET καθώς και στη λειτουργία αυτού. Για παράδειγμα, μπορεί να αποκτήσει κάποιο από τα κλειδιά που διαμοιράζονται στους ad hoc κόμβους έτσι ώστε απρόσκοπτα στη συνέχεια να επιτεθεί όπως για να αποκωδικοποιήσει τα μηνύματα που θα προωθηθούν σε αυτόν ή αυτά που θα κρυφακούσει. Ακόμη, εφόσον μια πολύ βασική ιδιότητα του δικτύου ad hoc είναι ότι παραμένει αφύλακτο ο εσωτερικός επιτιθέμενος μπορεί εύκολα να καταλάβει τους κόμβους τόσο στο φυσικό τους επίπεδο όσο και με το να εγκαταστήσει και να εκτελέσει κακόβουλο κώδικα στους κόμβους του δικτύου. Κατά σύμβαση οι κόμβοι αυτοί καλούνται συμβιβασμένοι ("compromised"). Συνεπώς, στην περίπτωση αυτή οι επιθέσεις ξεκινούν από τους ίδιους τους κόμβους του δικτύου οι οποίοι (φαινομενικά μόνο) παρουσιάζονται ως νόμιμοι κόμβοι: αυτοί είναι οι κόμβοι που καλούμε εισβολείς (intruders) στο δίκτυο ad hoc.

- ***Εξωτερικός επιτιθέμενος***. Αντίθετα από τον εσωτερικό επιτιθέμενο, ένας εξωτερικός επιτιθέμενος δε διαθέτει πρόσβαση σε χρήσιμες πληροφορίες ή στους πόρους των κόμβων του συστήματος. Μπορεί όμως με τη χρήση ισχυρών μέσων, για παράδειγμα με ένα πολύ ισχυρό πομπό να καταστρέψει τις επικοινωνίες του ad hoc δικτύου και με RF παρεμβολές ("jamming") να σπάσει τη συνεκτικότητα μεταξύ των ad hoc κόμβων.

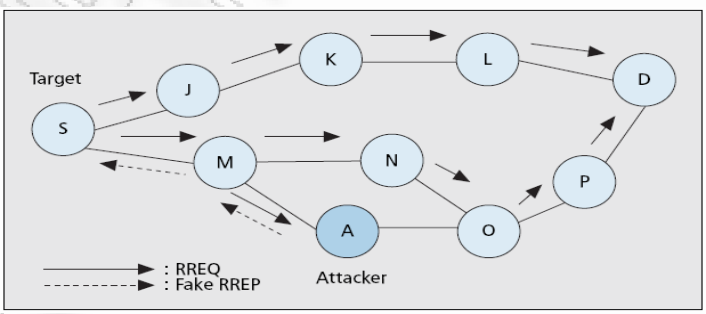
3.7.3. Ανάλυση Επιθέσεων Κατά της Προώθησης Μηνυμάτων

Όπως έχει αναφερθεί το κύριο χαρακτηριστικό των δικτύων ad hoc είναι ότι οι κόμβοι λειτουργούν ομότιμα ως δυνητικοί δρομολογητές των πακέτων δεδομένων που ανταλλάσσονται μεταξύ των πηγών και προορισμών. Ένας ενδιάμεσος κόμβος ad hoc που διαθέτει κάποιο αξιόπιστο μονοπάτι δρομολόγησης προς τον τελικό κόμβο-αποδέκτη αναλαμβάνει αυτός την προώθηση του πακέτου που έχει λάβει με το συγκεκριμένο προορισμό. Όπως θα δούμε σε αυτό το γεγονός στηρίζονται και εκμεταλλεύονται οι περισσότερες από τις επιθέσεις που έχουν στόχο το επίπεδο δρομολόγησης στα δίκτυα ad hoc. Παρακάτω παρουσιάζονται μερικές από τις πιο γνωστές έως τώρα επιθέσεις στο επίπεδο δικτύου, δηλαδή επιθέσεις που εξαπολύονται κατά της διαδικασίας εύρεσης του βέλτιστου μονοπατιού δρομολόγησης.

3.7.3.1. Επίθεση Μαύρης/Γκρι Τρύπας

Στην επίθεση μαύρης τρύπας ο κακόβουλος κόμβος διαφημίζει στο δίκτυο ελκυστική πλην πλαστή πληροφορία που έχει να κάνει με το μονοπάτι δρομολόγησης προς τον τελικό κόμβο-αποδέκτη των μηνυμάτων. Σε ένα δίκτυο MANET ο τελικός αποδέκτης μπορεί να είναι ένας κινητός χρήστης στον οποίο μεταβιβάζεται κάποιο αρχείο για παράδειγμα, ενώ στην περίπτωση ενός δικτύου WSN ο τελικός αποδέκτης των μηνυμάτων είναι ο συνήθως στατικός σταθμός βάσης. Χαρακτηριστικό παράδειγμα της επίθεσης αυτής είναι η επίθεση κατά των ad hoc πρωτοκόλλων που χρησιμοποιούν πλημμύρισμα με πακέτα αναζήτησης βέλτιστων διαδρομών και Αριθμούς Ακολουθίας (SN) που δείχνουν πόσο “φρέσκο” είναι ένα μονοπάτι δρομολόγησης. Στην περίπτωση του AODV αυτά τα πακέτα ονομάζονται Route Request Packets (RREQ) και σε κανονικές συνθήκες η πηγή θα επιλέξει ως ενδιάμεσο δρομολογητή εκείνο τον κόμβο που απαντά με ένα πακέτο Route Reply (RREP) που περιέχει το μεγαλύτερο SN για τον τελικό προορισμό. Έτσι είναι πολύ εύκολο ένας επιτιθέμενος να απαντήσει με ένα SN που είναι μεγαλύτερο από το SN που έλαβε στο RREQ, με αποτέλεσμα η πηγή να τον επιλέξει σαν ενδιάμεσο κόμβο. Στη συνέχεια, ο κόμβος μαύρη τρύπα δρα κακόβουλα με το να παραποιεί ή συνηθέστερα με το να απορρίπτει όλα τα πακέτα δεδομένων που προωθούνται προς αυτόν. Στην τελευταία περίπτωση το δίκτυο απειλείται με μεγάλη απώλεια πακέτων.

Η Εικόνα 11 παρουσιάζει μια επίθεση μαύρης τρύπας. Ο κόμβος (A) στέλνει πλαστό RREP στην πηγή (S), διαφημίζοντας ότι έχει μια αξιόπιστη διαδρομή προς τον κόμβο (D). Συγκεκριμένα, στέλνοντας ένα αρκούντως μεγάλο SN ο κόμβος (A) πείθει τον κόμβο (S) να στείλει τα δεδομένα μέσω αυτού [49].



Εικόνα 11. Παράδειγμα επίθεσης μαύρης τρύπας σε ad hoc δίκτυο AODV, [49].

Αντίμετρα:

Τα προτεινόμενα αντίμετρα στην επίθεση μαύρης τρύπας είναι πολλά. Εξαρτώνται δε από το συγκεκριμένο τρόπο με τον οποίο ο επιτιθέμενος προσπαθεί να ελκύσει την προώθηση των

πακέτων προς το μέρος του.

Ένα αντίμετρο που προτείνεται [53] βασίζεται σε στατιστικές μεθόδους δυναμικής εκμάθησης με την ανάλυση των αριθμών ακολουθίας των πακέτων RREP στο επίπεδο του δικτύου. Το ίδιο μέτρο εμφανίζεται και στην εργασία [71] όπου όμως εφαρμόζεται στην ανάλυση των αριθμών ακολουθίας των πλαισίων του επιπέδου MAC.

Σύμφωνα με το αντίμετρο της εργασίας [52] προτείνεται η τεχνική της "καθυστερημένης επεξεργασίας" των πακέτων RREP που λαμβάνονται από την πηγή που έστειλε τα πακέτα πλημμύρας RREQ. Σύμφωνα με αυτήν την τεχνική η πηγή δεν εγκαθιστά το μονοπάτι προς τον προορισμό, εκτός εάν λάβει παραπάνω από δύο πακέτα RREP. Ουσιαστικά αυτό γίνεται για να συγκριθούν τα αντίστροφα μονοπάτια που φθάνουν στην πηγή και ειδικότερα να διαπιστωθεί ότι υπάρχει κάποιο κοινό βήμα μεταξύ τους. Στην αντίθετη περίπτωση, δηλαδή όταν τα μονοπάτια είναι πλήρως διακριτά, θεωρείται ότι πρόκειται για μια συνεργατική επίθεση που προέρχεται από πάνω από δύο συνεργαζόμενους κόμβους.

Η εργασία [55] προτείνει τη χρήση των επιπλέον μηνυμάτων route confirmation request (CREQ) και route confirmation reply (CREP). Σύμφωνα με αυτή την τεχνική ένας ενδιάμεσος ad hoc κόμβος που λαμβάνει RREQ και διαθέτει μονοπάτι απαντάει με RREP προς την πηγή και επιπλέον μεταδίδει ένα πακέτο CREQ στον επόμενο κόμβο που διαθέτει στο μονοπάτι προς τον τελικό προορισμό. Ο επόμενος τότε κόμβος με τη λήψη του CREQ αναζητά τον τελικό προορισμό στη προσωρινή του μνήμη. Αν το αποτέλεσμα είναι θετικό, τότε αυτός μεταδίδει ένα πακέτο CREP προς την πηγή. Η πηγή συγκρίνει τα μονοπάτια που ακολούθησαν τα δύο πακέτα RREP και CREP και αν αυτά συμπίπτουν τότε αποφασίζει ότι το μονοπάτι είναι ορθό. Ο μηχανισμός αυτός ωστόσο δεν μπορεί να προστατέψει κατά την περίπτωση που ο επόμενος από τη μαύρη τρύπα κόμβος είναι και αυτός κακόβουλος και συνεργάζεται με τον προηγούμενο στην παρουσίαση του μονοπατιού που μεταδίδεται προς την πηγή ως ορθού και ασφαλούς.

3.7.3.2. Επίθεση Επιλεκτικής Προώθησης Μηνυμάτων

Η επίθεση αυτή διαφέρει από την επίθεση μαύρης τρύπας μόνο ως προς το ότι ο επιτιθέμενος αφού καταφέρει να ελκύσει τα πακέτα, στη συνέχεια εμφανίζει μια πιο επιλεκτική κακόβουλη συμπεριφορά με το να απορρίπτει μέρος των πακέτων που λαμβάνει για παράδειγμα κατά εντελώς τυχαίο τρόπο. Σε άλλες περιπτώσεις, ο επιτιθέμενος μπορεί να απορρίπτει τα πακέτα με βάση τον αποστολέα ή και με βάση τον παραλήπτη τους. Για παράδειγμα αν ο επιτιθέμενος καταλάβει ότι τα μηνύματα κάποιου συγκεκριμένου κόμβου είναι σημαντικά για το δίκτυο μπορεί επιλεκτικά να απορρίπτει όλα τα πακέτα που λαμβάνει από αυτόν τον κόμβο. Η επιλεκτική άρνηση προώθησης μηνυμάτων φαινομενικά έχει μικρότερο αντίκτυπο για το ad hoc δίκτυο, αφού η απώλεια πακέτων θα είναι μικρότερη από αυτήν της επίθεσης μαύρης τρύπας. Ωστόσο, η επιλεκτική προώθηση είναι πολύ πιο δύσκολο να ανιχνευθεί από τους μηχανισμούς αντιμετώπισης των επιθέσεων αφού είναι πιο δυναμικού χαρακτήρα με αποτέλεσμα η πότε καλή και πότε κακή συμπεριφορά του επιτιθέμενου να ξεγελά τους υπόλοιπους κόμβους.

3.7.3.3. Διαγραφή Πακέτων Επιβεβαίωσης

Στα περιορισμένα δίκτυα ad hoc αποφεύγονται οι επαναμεταδόσεις των χαμένων πακέτων με αποτέλεσμα τα πακέτα επιβεβαίωσης ACK να αποτελούν μια δεύτερη επιλογή για τα πρωτόκολλα δικτύου (όπως παράδειγμα το πρωτόκολλο AODV). Είναι επόμενο ένας κακόβουλος κόμβος να το εκμεταλλευτεί αυτό και να διαγράφει πακέτα χωρίς οι υπόλοιποι κόμβοι να μπορούν να το αντιληφθούν, εφόσον δεν περιμένουν επιβεβαίωση λήψης δεδομένων, και επομένως χωρίς να προσπαθήσουν να ανακτήσουν τα χαμένα πακέτα.

3.7.4. Ανάλυση Επιθέσεων κατά της Ακεραιότητας των Ad Hoc Πρωτοκόλλων

Οι περιορισμοί των δικτύων ad hoc που περιγράφησαν στην §3.5 αφήνουν όχι λίγες “ανοιχτές πόρτες” στον κακόβουλο χρήστη που επιθυμεί να βλάψει την ορθή λειτουργία του δικτύου ή απλά να υπεξαιρέσει ευαίσθητη πληροφορία που διακινείται μέσα στο δίκτυο. Αφήνοντας κατά μέρος τα χαρακτηριστικά της μετάδοσης στο φυσικό επίπεδο, οι βασικές αδυναμίες των ad hoc μηχανισμών δρομολόγησης που μπορούν να λειτουργήσουν ως “ανοιχτές πόρτες” παρουσιάζονται πιο κάτω.

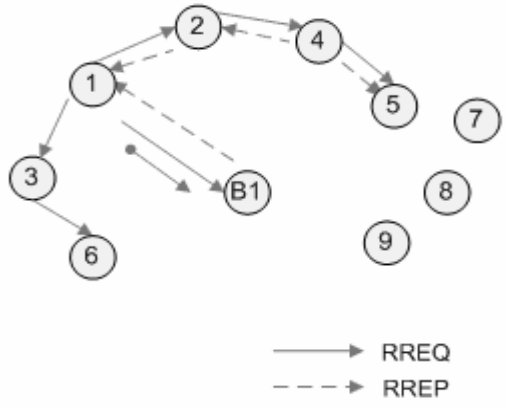
3.7.4.1. Αλλοίωση του Αριθμού Ακολουθίας

Η χρήση των αριθμών ακολουθίας λύνει πολλά προβλήματα στο επίπεδο του δικτύου όπως την αποφυγή των βρόχων κατά τη δρομολόγηση πακέτων, την ανίχνευση ζεύξεων που έχουν καταρρεύσει και την επιλογή μονοπατιών που είναι αξιόπιστα επειδή είναι φρέσκα με βάση την τιμή αρίθμησης των πακέτων από την πηγή προς κάποιο συγκεκριμένο κόμβο προορισμό. Από την άλλη μεριά όμως η ακολουθία αριθμών μπορεί να γίνει αντικείμενο εκμετάλλευσης από πληροφορημένους κακόβουλους κόμβους. Πολλά ad hoc πρωτόκολλα βασίζουν την ανεύρεση και εγκατάσταση των μονοπατιών δρομολόγησης από την πηγή στον προορισμό στα SN, για παράδειγμα το AODV (RFC-3561, [62]), το tinyAODV, το DSR (RFC-3728, [8]) κ.α. Ένας κακόβουλος κόμβος μπορεί να διαβάσει την τιμή SN και να τη μειώσει ή να την αυξήσει προκειμένου να προκαλέσει την κατάργηση ή την επιλογή αντίστοιχα ενός μονοπατιού από την πηγή προς τον προορισμό. Αυτό συμβαίνει διότι ως μονοπάτι στα παραπάνω πρωτόκολλα επιλέγεται αυτό με ενδιάμεσο κόμβο αυτόν που μετέδωσε το μεγαλύτερο αριθμό ακολουθίας. Έτσι, ένας επιτιθέμενος ενδιάμεσος μεταβάλλοντας κατάλληλα τον SN μπορεί να κατευθύνει τα πακέτα της πηγής στο μονοπάτι που αυτός επιθυμεί, ή ακόμη και να τα δρομολογήσει χωρίς προορισμό. Ακόμη εφόσον τα πρωτόκολλα αυτά προβλέπουν ένα μέγιστο αριθμό ακολουθίας που ένα πακέτο μπορεί να έχει, αν τεθεί ως SN πακέτου αριθμός μεγαλύτερος από το μέγιστο επιτρεπτό το πακέτο αυτό θα διαγραφεί από τον επόμενο στο μονοπάτι κόμβο.

Επίσης, η επίθεση spoofing μπορεί να βασιστεί στο γεγονός ότι το δίκτυο κάνει χρήση αριθμών ακολουθίας ιδιαίτερα στο επίπεδο διασύνδεσης δεδομένων με συνεχόμενη αρίθμηση των διαδοχικών πλαισίων που μεταδίδονται από τις ασύρματες κάρτες. Ο επιτιθέμενος πρώτα ανιχνεύει την ακολουθία των αριθμών που ένας κόμβος-στόχος μεταδίδει μέσα στα πλαίσια του. Αυτό είναι εύκολο να γίνει με κρυφάκουσμα του ασύρματου μέσου. Κατόπιν, ο επιτιθέμενος μεταδίδει πλαίσια που αριθμούνται ως συνέχεια των αριθμών που χρησιμοποιεί ο αυθεντικός κόμβος. Έτσι οι υπόλοιποι αδυνατούν να αντιληφθούν ότι τα πακέτα προέρχονται από κάποιον άλλο κόμβο και όχι από τον αυθεντικό, με αναμενόμενες δυσάρεστες συνέπειες αφού, για παράδειγμα, θα προωθήσουν τα πακέτα τους προς τον επιτιθέμενο και όχι προς τον νόμιμο κόμβο.

3.7.4.2. Αλλοίωση του Αριθμού των Βημάτων

Εκτός από τους αριθμούς ακολουθίας τα αντιδραστικά ad hoc πρωτόκολλα, όπως παράδειγμα το AODV και το DSR, στη λήψη απόφασης ως προς το βέλτιστο μονοπάτι δρομολόγησης από την πηγή προς τον προορισμό λαμβάνουν υπόψη και το συνολικό αριθμό των βημάτων ή ισοδύναμα το χρόνο απόκρισης των ενδιάμεσων κόμβων. Έτσι εκείνος ο ενδιάμεσος κόμβος που θα απαντήσει πρώτος με ένα πακέτο RREP στο πακέτο ευρείας εκπομπής RREQ που θα λάβει από την πηγή διαφημίζοντας ότι διαθέτει ένα μονοπάτι προς τον τελικό προορισμό, ή ο ενδιάμεσος κόμβος που θα απαντήσει RREP με το μικρότερο αριθμό βημάτων από τον προορισμό θα επιλεγεί ως το επόμενο βήμα στο μονοπάτι προς τον τελικό προορισμό. Αν ο κακόβουλος κόμβος επιτύχει κάτι τέτοιο τότε θα μπορεί να λαμβάνει τα πακέτα δεδομένων που προέρχονται από την πηγή και άρα είναι πολύ εύκολο να τα διαβάσει, να τα τροποποιήσει ή/και να τα διαγράψει. Το σενάριο μικρού αριθμού βημάτων (γνωστό και ως σενάριο χρονικής επίθεσης “rushing attack”) κατά του AODV απεικονίζεται στην Εικόνα 12.



Εικόνα 12. Επίθεση γρήγορης απόκρισης (“rushing attack”) κατά του πρωτοκόλλου AODV, [70].

Στο σενάριο αυτό η πηγή αντιστοιχεί στον κόμβο (1), ενώ προορισμός είναι ο κόμβος (5). Οι κόμβοι (2), (B1) και (3) βρίσκονται σε απόσταση ενός βήματος από την πηγή. Η πηγή εκπέμπει ευρέως ένα πακέτο RREQ με προορισμό τον (5) το οποίο σε πρώτη φάση λαμβάνεται από αυτούς τους τρεις κόμβους. Οι κόμβοι (3) και (6) θα μεταδώσουν περαιτέρω το πακέτο RREQ, ενώ ο κακόβουλος κόμβος (B1) θα απαντήσει πρώτος με ένα πακέτο RREP δίχως καν να έχει στους πίνακές του τον προορισμό. Ο κόμβος (1) βασιζόμενος στον αριθμό βημάτων (ένα) που ο (B1) επικαλείται πριν από τον προορισμό θα στείλει τελικά τα πακέτα του στον κόμβο (B1), δηλαδή ο σκοπός του επιτιθέμενου θα έχει επιτευχθεί εξαπατώντας την πηγή με ένα ανύπαρκτο μονοπάτι προς τον προορισμό.

Τα αντίμετρα προστασίας περιλαμβάνουν τη χρήση πεδίων χρονοσφραγίδων [60] και [61] και πεδίων με τη γεωγραφική θέση των κόμβων μέσα στα πακέτα έτσι ώστε (με βάση και με την ταχύτητα των κόμβων που θα πρέπει να θεωρείται κατά προσέγγιση γνωστή) να μπορεί να ελεγχθεί ότι πράγματι κάποιος κόμβος απέχει απόσταση ενός βήματος από το δέκτη. Ακόμη, συνιστάται η χρήση εναλλακτικών μονοπατιών δρομολόγησης και η σύγκριση του αριθμού των βημάτων προς τον τελικό προορισμό όπως και η εγκατάσταση συνεργατικών σχημάτων ανίχνευσης και αντιμετώπισης επιθέσεων στο επίπεδο του δικτύου.

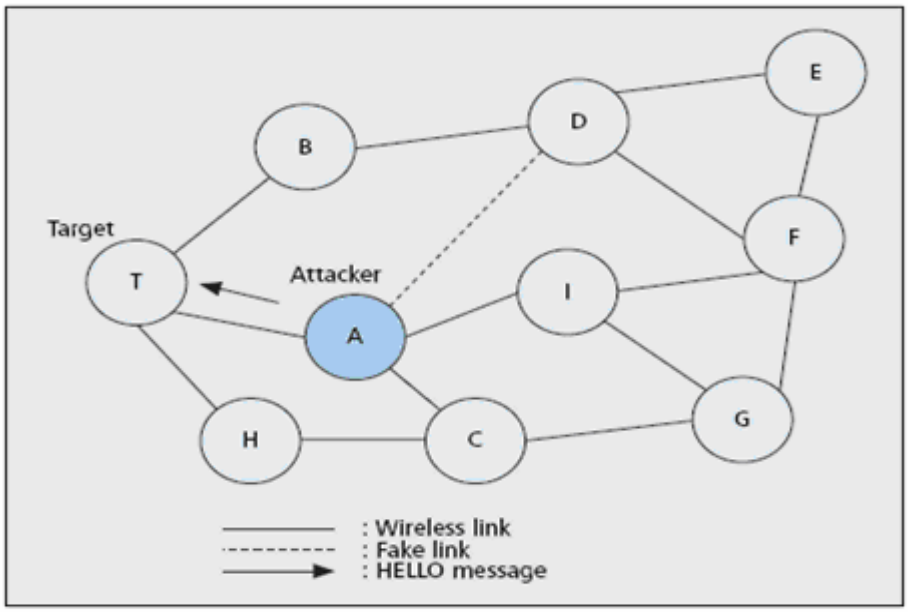
3.7.4.3. Επίθεση Παραποίησης των Δεσμών

Στις επιθέσεις αυτού του είδους (“link spoofing”) ο κακόβουλος κόμβος διαφημίζει πλαστές ζεύξεις με κόμβους του δικτύου που στην πραγματικότητα δεν διαθέτει ή αλλιώς αποκρύπτει κάποιες ενεργές ζεύξεις που έχει με γειτονικούς του κόμβους. Και στις δύο περιπτώσεις προκαλείται σύγχυση στους υπόλοιπους κόμβους αφού παρεμποδίζεται η ορθή λειτουργία των πρωτοκόλλων δρομολόγησης λόγω ψευδούς απεικόνισης της τοπολογίας του δικτύου.

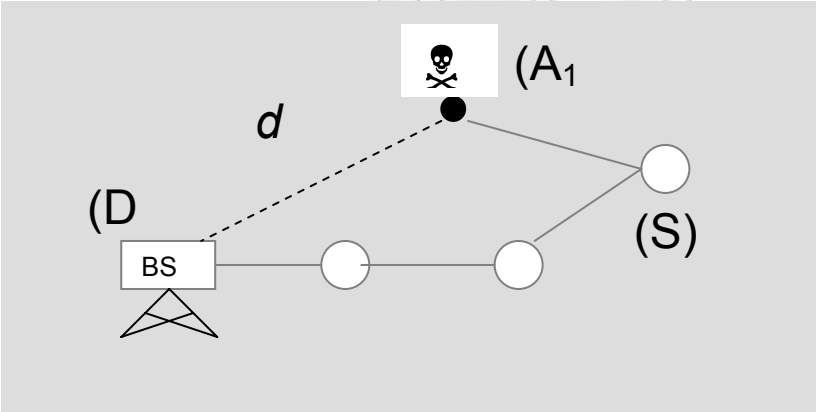
Η Εικόνα 13 παρουσιάζει τον αντίκτυπο της επίθεσης με παραποίηση των δεσμών στο πρωτόκολλο OLSR. Το OLSR είναι ένα ad hoc πρωτόκολλο που χρησιμοποιεί τους κόμβους “Mutli-Point Relay” (MPR) για την προώθηση των μηνυμάτων. Οι κόμβοι MPR είναι αυτοί που καλύπτουν όλους τους κόμβους που βρίσκονται μέχρι και δύο βήματα μακριά. Αν ο επιτιθέμενος καταφέρει να δείξει ότι πληρεί τις συνθήκες για να είναι ένας MPR κόμβος, τότε οι υπόλοιποι θα προωθήσουν σε αυτόν τα πακέτα, τα οποία όμως θα τα απορρίψει ή θα τα τροποποιήσει. Στην Εικόνα 13 ο κόμβος (A) ψευδώς διαφημίζει στους γείτονές του ότι έχει ενεργή ζεύξη με τον κόμβο (D). Ο κόμβος (T) θα επιλέξει συνεπώς τον κόμβο (A) ως έναν από τους MPR (μαζί με τον κόμβο B) αφού καταφέρνει να του δώσει κάλυψη μέχρι και δύο βήματα μακριά (κόμβοι D, I και C). Στη συνέχεια, ο επιτιθέμενος (A) δρα κακόβουλα κατά τους γνωστούς τρόπους που έχουν αναφερθεί.

Αντίμετρα:

Το βασικό αντίμετρο σε αυτήν την περίπτωση επίθεσης είναι η χρήση της πληροφορίας θέσης των κόμβων όπως αυτή παρέχεται από τους δέκτες GPS των κόμβων ή όπως υπολογίζεται με βάση τους κατάλληλους αλγορίθμους προσδιορισμού της θέσης των κόμβων στο επίπεδο. Με αυτόν τον τρόπο βάσει της απόστασης *d* που υπολογίζεται για δύο κόμβους (όπως απεικονίζεται στην Εικόνα 14, A_1 είναι ο κακόβουλος κόμβος που διαφημίζει απόσταση ενός βήματος *d*, S είναι η πηγή και D είναι ο προορισμός) μπορεί να ευρεθεί αν πράγματι η απόστασή τους είναι ίση με την απόσταση ενός βήματος του ασύρματου δικτύου.



Εικόνα 13. Παράδειγμα επίθεσης "link spoofing" σε ένα ad hoc δίκτυο OLSR, [49].



Εικόνα 14. Σενάριο ανίχνευσης επίθεσης παραποίησης δεσμού με βάση την πληροφορία θέσης.

3.7.4.4. Έγχυση Ψευδών Δεδομένων

Θεωρούμε ότι η έγχυση δεδομένων στο δίκτυο ad hoc από κακόβουλους κόμβους τα οποία δεν είναι αληθή είναι σχετικά εύκολη και συνιστά μια επίθεση που λιγοστά από τα υφιστάμενα ad hoc πρωτόκολλα έχουν προβλέψει να αντιμετωπίσουν. Οι κακόβουλοι κόμβοι είναι δυνατόν να παριστάνουν ότι είναι κόμβοι με την ταυτότητα κάποιου άλλου κόμβου (γνωστό ως επίθεση "spoofing" όπου γίνεται παραποίηση της ταυτότητας του κόμβου) και στη συνέχεια είναι δυνατόν να εισάγουν ψευδείς γεωγραφικές συντεταγμένες, ακόμη και να διαφημίζουν σε ένα πρωτόκολλο

δρομολόγησης που λαμβάνει υπόψη την ενέργεια των κόμβων ότι έχουν αρκετό απόθεμα ενέργειας -χωρίς στην πραγματικότητα να διαθέτουν αυτό το απόθεμα ενέργειας- και γενικά να προσπαθούν να διαχύσουν ψευδή πληροφορία. Ο απώτερος σκοπός παρόμοιων επιθέσεων είναι να βλάψουν περισσότερο την ορθή του λειτουργία παρά τα ίδια τα δεδομένα των χρηστών και να προκαλέσουν με αυτόν τον τρόπο σύγχυση ανάμεσα στους χρήστες του δικτύου.

3.7.4.5. Επίθεση Επανάληψης Μηνυμάτων

Η επίθεση επανάληψης είναι μια σοβαρή απειλή για τα ασύρματα δίκτυα ad hoc που μπορεί να πάρει πολλές μορφές. Ο επιτιθέμενος επαναλαμβάνει σε ύστερο χρόνο πακέτα που έχει προηγουμένως καταφέρει να συλλάβει, κάτι όχι και ιδιαίτερα δύσκολο σε ένα ασύρματο δίκτυο ευρείας εκπομπής. Τα μηνύματα που επαναλαμβάνονται μπορεί κατά πρώτον να είναι μηνύματα του ad hoc πρωτοκόλλου δρομολόγησης, για παράδειγμα πίνακες δρομολόγησης που σε κανονικές συνθήκες ενημερώνουν τους κόμβους για τις πιο πρόσφατες αλλαγές στην τοπολογία δικτύου ώστε οι αποφάσεις κατά τη δρομολόγηση των κόμβων να είναι σωστές. Η επανάληψη κάποιου μηνύματος το οποίο αντιστοιχεί σε μία τοπολογία που δεν υπάρχει πλέον (συνηθέστερα λόγω της κίνησης των κόμβων), προφανώς θα προκαλέσει διάρρηξη της ορθής λειτουργίας του πρωτοκόλλου, καθυστερήσεις, βρόχους, απορρίψεις πακέτων κ.ο.κ.

Χαρακτηριστική είναι η επίθεση επανάληψης του πακέτου επιβεβαίωσης ACK που αφορά στο επίπεδο ζεύξης Wireless Data Link Control (W-DLC), για παράδειγμα στο MAC επίπεδο του ad hoc πρωτοκόλλου IEEE 802.15.4. Το 802.15.4 σε πολλές περιπτώσεις αφήνει προαιρετική τη χρήση των ACK. Αν έχει συμφωνηθεί να γίνεται χρήση επιβεβαιώσεων τότε ο επιτιθέμενος μπορεί να στείλει ACK προσποιούμενος ότι είναι κάποιος άλλος γειτονικός κόμβος, ο οποίος όμως είναι ανενεργός ή έχει μικρή συνδεσιμότητα με τους υπόλοιπους. Οι κόμβοι που θα λάβουν αυτήν την επιβεβαίωση θα εκλάβουν ότι η αντίστοιχη ζεύξη με τον εν λόγω κόμβο είναι ενεργή και θα αποστείλουν πακέτα δεδομένων προς αυτόν. Αποτέλεσμα των ενεργειών αυτών είναι να χαθούν τα πακέτα αυτά.

Κατά δεύτερον, τα μηνύματα ACK που επαναλαμβάνονται μπορεί να αφορούν στο υψηλότερο επίπεδο της εφαρμογής. Σε αυτήν την περίπτωση, ο επιτιθέμενος που κρυφακούει καταφέρνει προσποιούμενος να δείξει ότι είναι κάποιος άλλος νόμιμος κόμβος που απαντά με τα προβλεπόμενα ACK από το πρωτόκολλο του επιπέδου της εφαρμογής. Σαν αποτέλεσμα, οι υπόλοιποι κόμβοι ξεγελώνται και συμπεριλαμβάνουν τον επιτιθέμενο στους αποδέκτες των μηνυμάτων που ανταλλάσσουν. Έτσι, ο κακόβουλος κόμβος έχει πρόσβαση στις επικοινωνίες των νόμιμων κόμβων και πράττει ανάλογα με το συμφέρον του. Σε αυτήν την περίπτωση δε, ο επιτιθέμενος μπορεί να ξεγελάσει με το να επαναλαμβάνει τα μηνύματα χωρίς να χρειάζεται να τα αποκωδικοποιήσει, οπότε η πιθανή προστασία, ακόμη και με ισχυρή κρυπτογράφηση, είναι αναποτελεσματική.

Αντίμετρα:

Ένα πρώτο μόνο μέτρο προστασίας είναι η χρήση των χρονο-σφραγίδων μέσα σε κάθε πακέτο. Η τεχνική αυτή απαιτεί κάποιο είδος συγχρονισμού μεταξύ των κόμβων. Με τη σύγκριση μεταξύ της χρονοσφραγίδας και του τρέχοντος χρόνου στο δέκτη μπορεί να διαπιστωθεί αν κάποιο πακέτο είναι επανάληψη ενός προηγούμενου. Ένας επιτιθέμενος ωστόσο μπορεί να υπολογίσει το χρόνο και να επαναλάβει μέρος του μηνύματος σε κατάλληλο χρόνο, χωρίς έτσι να γίνει αντιληπτός. Έτσι για περαιτέρω προστασία, το πεδίο της χρονο-σφραγίδας μπορεί να είναι προστατευμένο με συμμετρική κρυπτογράφηση ή με ψηφιακή υπογραφή [54].

3.7.5. Ανάλυση Επιθέσεων κατά της Διαθεσιμότητας των Υπηρεσιών

3.7.5.1. Η Επίθεση DoS

Οι επιθέσεις της Άρνησης Εξυπηρέτησης των Υπηρεσιών “Denial of Service” (DoS) είναι το αποτέλεσμα οποιασδήποτε κακόβουλης δράσης που τελικά απειλεί την ικανότητα του δικτύου ad hoc να διαθέτει τις υπηρεσίες του προς τους χρήστες, όποτε αυτοί τις απαιτούν. Με αφετηρία έναν ορισμό σαν και αυτό είναι εύλογο να περιμένουμε ότι οι επιθέσεις αυτές έχουν πολλούς πιθανούς στόχους και άρα μπορούν να κατηγοριοποιηθούν κατά πολλούς αντίστοιχους τρόπους όπως έχουμε διαπιστώσει στην υπάρχουσα βιβλιογραφία.

Έτσι, μια επίθεση DoS μπορεί να εκδηλωθεί κατά του λειτουργικού συστήματος (για παράδειγμα, στην επίθεση “Ping of Death” [51] στέλνονται στο στόχο υπερμεγέθη πακέτα ηχούς ICMP που θα πρέπει να τμηματοποιούνται στην πηγή και στη συνέχεια να επανενώνονται στον προορισμό στο επίπεδο του λειτουργικού, κάτι που μπορεί εύκολα να προκαλέσει υπερχείλιση της προσωρινής μνήμης -“buffers”).

Επίσης, μια επίθεση DoS μπορεί να εκδηλωθεί κατά του φυσικού επιπέδου (για παράδειγμα επίθεση με πολύ ισχυρό πομπό που παρεμβάλλεται στις νόμιμες επικοινωνίες) όπως και κατά του επιπέδου διασύνδεσης δεδομένων (για παράδειγμα με συνεχείς μεταδόσεις και πρόκληση μεγάλου αριθμού συγκρούσεων στο επίπεδο MAC), κυρίως όμως οι επιθέσεις DoS συνιστούν απειλές κατά του επιπέδου της εφαρμογής του τελικού χρήστη. Ένα παράδειγμα επίθεσης που βασίζεται στο επίπεδο εφαρμογής είναι η επίθεση “finger bomb”. Ένας κακόβουλος χρήστης μπορεί να προκαλέσει την επαναλαμβανόμενη εκτέλεση της ρουτίνας finger στον κόμβο-θύμα, οδηγώντας πιθανότατα στην εξάντληση των πόρων των δικτύων.

Σε όλες αυτές τις περιπτώσεις των επιθέσεων DoS η πιο συνήθης (και πιο απλή) τακτική του επιτιθέμενου είναι η μέθοδος της πλημμύρας (“flooding”) με δεδομένα ή με αιτήματα σύνδεσης εφόσον αναφερόμαστε στο επίπεδο της εφαρμογής και μεταφοράς αντίστοιχα. Έτσι, με τη μέθοδο της πλημμύρας στέλνονται πάρα πολλά αιτήματα σε έναν ευαίσθητο κόμβο ενός δικτύου MANET/WSN με αποτέλεσμα αυτός να μην μπορεί να ανταποκριθεί τόσο από πλευράς υπολογιστικών απαιτήσεων όσο και από πλευράς απαιτούμενης μνήμης. Τελικά οι υπηρεσίες θα καταστούν μη διαθέσιμες επειδή οι κόμβοι δε θα μπορούν να αφιερώσουν άλλους διαθέσιμους πόρους για τα νόμιμα αιτήματα που θα καταφθάνουν.

Από τη μεριά μας εντάσσουμε τις επιθέσεις DoS στην κατηγορία των επιθέσεων κατά της διαθεσιμότητας των υπηρεσιών που παρέχονται από το επίπεδο διασύνδεσης των δεδομένων (όπως πλαισιοποίηση και έλεγχος ροής), από το επίπεδο του δικτύου (υπηρεσίες από σημείο σε σημείο όπως διευθυνσιοδότηση, ανανέωση πινάκων δρομολόγησης, αποφυγή σπασμένων ζεύξεων, προώθηση πακέτων, ανα-δρομολόγηση πακέτων, έλεγχος συμφόρησης) και από το επίπεδο των εφαρμογών για τον τελικό χρήστη και για τη διαχείριση του δικτύου (υπηρεσίες από άκρη σε άκρη).

Σε αυτό το σημείο πρέπει επίσης να αναφέρουμε ότι κατά την άποψή μας η ανοχή του δικτύου στις επιθέσεις DoS έχει να κάνει και με την τεχνολογία μεσισμικού που είναι εγκατεστημένη στους κόμβους του. Η τεχνολογία μεσισμικού είναι αυτή που παρακολουθεί, διαχειρίζεται και συντονίζει τους πόρους των κόμβων του δικτύου ad hoc και επίσης το μεσισμικό είναι αυτό που καθορίζει το ανοιχτό και διάφανο μοντέλο των επικοινωνιών μεταξύ των κόμβων. Συνεπώς, η μελέτη των επιθέσεων DoS κατά του επιπέδου των υπηρεσιών θα πρέπει, πιστεύουμε, να λαμβάνει σοβαρά υπόψη και την ανθεκτικότητα που διαθέτουν τα στρώματα του μεσισμικού σε επιθέσεις τύπου πλημμύρας αιτημάτων και για το λόγο αυτό θα αφιερώσουμε μια ξεχωριστή μελέτη για την επίδοση των τεχνολογιών μεσισμικού σε συνθήκες πολλών αιτημάτων στο Κεφάλαιο 7.

3.7.5.2. Η Επίθεση DoS στην Ανακάλυψη Υπηρεσιών

Ένα εξειδικευμένο παράδειγμα της επίθεσης DoS που είναι ιδιαίτερα εφαρμόσιμο στα δίκτυα ad hoc είναι οι επιθέσεις που στοχεύουν να πλήξουν τη διαδικασία της αναζήτησης υπηρεσιών ("service discovery") μέσα σε ένα δίκτυο ad hoc. Σε μια επικοινωνία ανεύρεσης υπηρεσιών που ακολουθεί το μοντέλο "client-server" είναι δυνατόν ο κακόβουλος κόμβος να απειλήσει είτε τον κόμβο-πελάτη (μπορεί αυτός να βρίσκεται σε κάποιο σημείο του Διαδικτύου ή να βρίσκεται εντός του ad hoc δικτύου) που ψάχνει για υπηρεσίες όπως μια τιμή θερμοκρασίας ή πίεσης που διατίθεται σε κάποιον αισθητήρα, είτε είναι δυνατόν ο κακόβουλος κόμβος να απειλήσει τον κόμβο-εξυπηρετητή που δεν είναι άλλος από τον αισθητήρα που διαθέτει αυτές τις υπηρεσίες, εφόσον μιλάμε για ένα WSN.

Έτσι οι κόμβοι πελάτες που ψάχνουν για υπηρεσίες μπορεί να υπερφορτωθούν σε ένα δίκτυο ad hoc από τον κακόβουλο κόμβο που διαφημίζει με ευρεία εκπομπή ένα πολύ μεγάλο αριθμό μηνυμάτων με "διαθέσιμες" υπηρεσίες. Οι κόμβοι-πελάτες θα προσπαθήσουν να αποθηκεύσουν και να επεξεργαστούν αυτά τα κακόβουλα μηνύματα/διαφημίσεις με συνέπεια να σπαταλήσουν σε σημαντικό βαθμό τους πόρους τους, χωρίς ωστόσο να μπορούν να ανακαλύψουν κάποια αληθινή υπηρεσία. Ακόμη, ο επιτιθέμενος, εφόσον έχει καταφέρει να συμβιβάσει ένα ad hoc κόμβο, μπορεί να στείλει ψευδείς πληροφορίες προς τους κόμβους-πελάτες όσον αφορά την υπηρεσία που διαθέτει με απώτερο σκοπό να τους αποπροσανατολίσει. Έτσι για παράδειγμα, μπορεί να διαφημίσει ότι έχει μια υπηρεσία που στην πραγματικότητα δε διαθέτει, ή μπορεί να μεταδώσει ένα ψευδές URL ως σημείο διάθεσης της υπηρεσίας ή μια ψευδή διεύθυνση IP έτσι ώστε τελικά να αναγκάσει τον πελάτη σε επαναλαμβανόμενες αποτυχημένες προσπάθειες ανεύρεσης της επιθυμητής υπηρεσίας.

Ένας κόμβος εξυπηρετητής μπορεί να γίνει θύμα τις επίθεσης DoS από κακόβουλους πελάτες οι οποίοι μεταδίδουν ένα εξόχως μεγάλο αριθμό από ερωτήματα για τις διαθέσιμες υπηρεσίες. Έτσι ένας κόμβος ad hoc που διαθέτει κάποιες υπηρεσίες για τους υπολοίπους στο ad hoc δίκτυο, όπως μοίρασμα αρχείων, εκτυπωτικές υπηρεσίες ή υπηρεσίες ενός αισθητήρα, όπως τιμές πίεσης, θερμοκρασίας και άλλες μπορεί να υπερχειλιστεί με πολλά ερωτήματα που καταφθάνουν με υψηλό ρυθμό και συνεπώς δεν μπορεί να τα εξυπηρετήσει.

Επίσης, στην επικοινωνία του μοντέλου client-server ένας κακόβουλος επιτιθέμενος μπορεί να εξαπολύσει την επίθεση ενδιάμεσου κόμβου ("Man in the Middle") κατά την οποία παρεμβάλλεται ανάμεσα στα δύο νόμιμα μέρη που ανταλλάσσουν μηνύματα (κατά τη διαδικασία της ανακάλυψης υπηρεσίας) προσποιούμενος στον καθένα ότι είναι το άλλο μέρος της επικοινωνίας. Τα αποτέλεσμα είναι να λειτουργεί σαν ενδιάμεσος κόμβος ικανός να υποκλέπτει και να αλλοιώνει τη χρήσιμη πληροφορία χωρίς οι νόμιμοι κόμβοι να μπορούν να το αντιληφθούν.

Αντίμετρα Προστασίας σε Επιθέσεις κατά των Πελατών

Τα βασικό αντίμετρο στο πλημμύρισμα των πελατών είναι οι μηχανισμοί ελέγχου του ρυθμού με τον οποίο καταφθάνουν στους κόμβους-πελάτες οι διαφημίσεις των διαθέσιμων υπηρεσιών από τους εξυπηρετητές. Έτσι αν ο ρυθμός άφιξης πακέτων βρεθεί πολύ μεγάλος από τον έλεγχο, τα επιπλέον πακέτα απορρίπτονται για την αποφυγή της υπερφόρτωσης των κόμβων.

Μια δεύτερη τεχνική αντιμετώπισης είναι η αυθεντικοποίηση των κόμβων που ισχυρίζονται ότι διαθέτουν τις υπηρεσίες. Στο περιορισμένο ad hoc δίκτυο αυτό μπορεί να επιτευχθεί με τη χρήση κοινών μυστικών ή/και συμμετρικών κλειδιών ή/και πιστοποιητικών τα οποία θα πρέπει να είναι προ-φορτωμένα στους κόμβους από την αρχή της λειτουργίας του δικτύου (όπως συνηθίζεται στις στρατιωτικές εφαρμογές όπου η συμμετοχή των κόμβων είναι εκ των προτέρων γνωστή).

Αντίμετρα Προστασίας σε Επιθέσεις κατά των Εξυπηρετητών

Και εδώ οι τεχνικές αντιμετώπισης είναι ίδιες και είναι προτιμότερο αυτές να αποτελούν συνδυασμό των μέχρι τώρα μεθόδων προστασίας που έχουμε δει. Έτσι μπορεί να διαπιστωθεί η νομιμότητα ενός κόμβου που στέλνει πάρα πολλά ερωτήματα ανεύρεσης υπηρεσίας από την εγκυρότητα της θέσης του. Μπορεί ακόμη να εισαχθεί στον εξυπηρετητή κάποιο κατώφλι αποδοχής ερωτημάτων (με βάση το ρυθμό άφιξης) πάνω από το οποίο τα εξέχοντα πακέτα απορρίπτονται. Επιπλέον, μπορεί να γίνει περαιτέρω αυθεντικοποίηση της ταυτότητας του πελάτη με τη χρήση κάποιας από τις μεθόδους συμμετρικής κρυπτογράφησης ή προ-φορτωμένων πιστοποιητικών που μπορεί να χρησιμοποιούνται εντός των ορίων του δικτύου ad hoc.

3.7.5.3. Επίθεση Πλημμύρας Πακέτων Δεδομένων

Στις επιθέσεις πλημμύρας δεδομένων (“data flooding”), ο επιτιθέμενος προσπαθεί να χρησιμοποιήσει το διαθέσιμο εύρος ζώνης ενός κόμβου ή μιας συσκευής δικτύου στο μεγαλύτερο δυνατό βαθμό, στέλνοντας μαζικές ποσότητες δεδομένων και προκαλώντας την επεξεργασία και αποθήκευση ιδιαίτερα μεγάλων ποσοτήτων δεδομένων στους υπόλοιπους κόμβους. Κατά συνέπεια, η επίθεση data flooding αφορά κυρίως στα επίπεδα διασύνδεσης και δρομολόγησης.

Ιδιαίτερα επιτυχής η επίθεση πλημμύρας μπορεί να γίνει όταν συνδυάζεται με επίθεση-παραποίηση ταυτότητας, της οποίας η πιο απλή μορφή είναι η αλλαγή ταυτότητας (“address spoofing”). Σε μια τέτοια περίπτωση, ο επιτιθέμενος εύκολα υποκλέπτει την ταυτότητα ενός άλλου ασύρματου κόμβου σε ένα απροστάτευτο ασύρματο δίκτυο (“sniffer”) και στέλνει πακέτα-ερωτήματα στους υπόλοιπους θέτοντας στο πεδίο της πηγής την ταυτότητα του κόμβου-θύματος. Οι υπόλοιποι παραλήπτες απαντούν στο θύμα με αποτέλεσμα αυτό να μην μπορεί να δεχθεί (δηλαδή να αποθηκεύσει ή επεξεργαστεί) ένα τόσο μεγάλο αριθμό από δεδομένα, ιδίως όταν το δίκτυο είναι πολύ μεγάλο. Αυτή είναι γνωστή ως επίθεση “Internet Smurf” [48] και μπορεί εύκολα να εκδηλωθεί επιτυχώς και σε ένα δίκτυο MANET μεγάλης κλίμακας.

Θα πρέπει να τονίσουμε ότι ο επιτιθέμενος πρέπει να είναι κλάσης laptop/workstation προκειμένου να μπορεί να διεξάγει την επίθεση “data flooding” η οποία είναι αυξημένου κόστους.

Αντίμετρα:

Μια πρώτη αντιμετώπιση στην επίθεση πλημμύρας, για παράδειγμα πακέτων RREQ στο πρωτόκολλο AODV ή και δεδομένων, είναι να εξακριβώνεται πριν την περαιτέρω προώθηση των πακέτων από τους κόμβους η θέση του αποστολέα, για παράδειγμα ότι είναι εντός των νόμιμων χωρικών ορίων του δικτύου. Αν όχι, τότε ο κόμβος απομονώνεται και αποφεύγεται η πλημμύρα που μπορεί να προκαλέσει πτώση της εξυπηρετητικής ικανότητας των κόμβων. Ο έλεγχος της γεωγραφικής θέσης που μεταδίδεται μέσα στα πακέτα μπορεί να αποβεί πολύ χρήσιμος ακόμη και στην περίπτωση που ο επιτιθέμενος συνδυάζει την πλημμύρα με παραποίηση της ταυτότητάς του, δηλαδή όταν υποδύεται κάποιον άλλον κόμβο. Τότε πακέτα από τον ίδιο κόμβο θα λαμβάνονται ταυτόχρονα από δύο διαφορετικές θέσεις, γεγονός που αρκεί για το μαρκάρισμα ενός κόμβου σαν ύποπτου, απαιτείται όμως να γνωρίζουμε ότι το δίκτυο είναι στατικό.

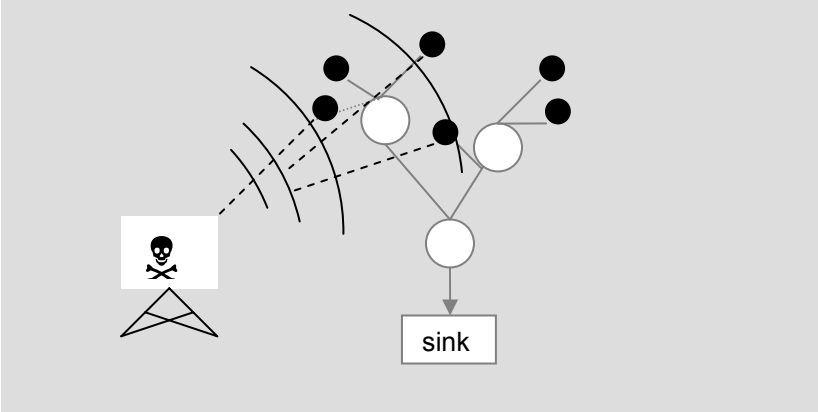
Επίσης σαν αντίμετρο μπορεί πολύ εύκολα να ελεγχθεί ο ενδιάμεσος χρόνος που μεσολαβεί ανάμεσα στις διαδοχικές αποστολές των πακέτων πλημμύρας (συνήθως πακέτα τύπου RREQ) και αν ο ρυθμός μετάδοσης που προκύπτει είναι εξόχως μεγάλος τότε μπορεί να διαγνωσθεί ύποπτη συμπεριφορά.

3.7.5.4. Επίθεση Πλημμύρας Πακέτων Hello

Μια επίθεση πλημμύρας που συνδυάζεται με ραδιο-παρεμβολές και που απειλεί ιδιαίτερα τη διάθεση των υπηρεσιών δικτύωσης όπως τη δρομολόγηση πακέτων είναι η ευρεία εκπομπή (broadcast) πακέτων Hello από έναν επιτιθέμενο της κλάσης *laptop/workstation* [50]. Σε αυτήν την επίθεση, ο κακόβουλος κόμβος πρέπει να διαθέτει τους αναγκαίους πόρους (δηλαδή ισχυρό

πομπό) ώστε να μεταδίδει περιοδικά ένα μεγάλο αριθμό από πακέτα Hello. Τα πακέτα Hello χρησιμοποιούνται σε πολλά δίκτυα ad hoc προκειμένου να αποδεικνύουν την ύπαρξη των γειτονικών κόμβων και μεταδίδονται κατά περιοδικό τρόπο ώστε να συντηρούν τους δεσμούς μεταξύ των γειτονικών κόμβων. Με αυτόν τον τρόπο οι κόμβοι μπορεί να είναι ενήμεροι για την τοπολογία του δικτύου μέχρι και δύο βήματα μακριά.

Ένας εξωτερικός κακόβουλος κόμβος μπορεί εύκολα να εκμεταλλευτεί τη χρήση των πακέτων Hello ώστε να καταρρίψει τη διαθεσιμότητα του δικτύου χωρίς καν να χρειαστεί να εισχωρήσει στο δίκτυο. Κατά πρώτον μεταδίδοντας τα πακέτα αυτά με εξόχως μεγάλη συχνότητα οπότε οι αποδέκτες κόμβοι τελικά υπερχειλίζουν και συνεπώς αδυνατούν να εκτελέσουν την απαραίτητη αποθήκευση και επεξεργασία των πακέτων αυτών. Κατά δεύτερον, ο κακόβουλος κόμβος μπορεί να χρησιμοποιήσει ένα πολύ ισχυρό πομπό και να μεταδώσει τα πακέτα Hello σε πολύ μακρινούς ad hoc κόμβους οι οποίοι θα πιστέψουν ότι πρόκειται για γειτονικό τους νόμιμο κόμβο που βρίσκεται σε απόσταση ενός βήματος, δες Εικόνα 15, με αποτέλεσμα το επίπεδο δρομολόγησης να ξεγελαστεί και τα πακέτα να χάνονται ή να περιφέρονται άσκοπα στο δίκτυο εφόσον δρομολογούνται προς ένα ανύπαρκτο κόμβο.



Εικόνα 15. Ισχυρή εκπομπή από κακόβουλο κόμβο και παραπλάνηση των κόμβων σε μαύρο χρώμα.

Αν επιπλέον ο επιτιθέμενος διαφημίζει ότι διαθέτει μονοπάτια μικρού κόστους προς κάποιο συγκεκριμένο κόμβο MANET ο οποίος για παράδειγμα διαθέτει για κοινή χρήση δεδομένα, video κ.α. ή διαφημίζει ότι βρίσκεται κοντά στο Base Station σε ένα δίκτυο WSN, τότε, σαν αποτέλεσμα, οι αποδέκτες των ψευδών πακέτων Hello θα επιχειρήσουν να προωθήσουν τα δεδομένα τους προς τον επιτιθέμενο κόμβο, ο οποίος όμως δε θα είναι δυνατό να βρεθεί αφού θα βρίσκεται σε πολύ μεγάλη απόσταση ή δεν θα περιλαμβάνεται στους πίνακες δρομολόγησης των ενδιάμεσων υπολοίπων κόμβων. Σαν αποτέλεσμα, θα προκληθούν πολυάριθμες αναμεταδόσεις πακέτων, βρόχοι δρομολόγησης και απώλεια των δεδομένων, στη χειρότερη δε των περιπτώσεων θα προκληθεί συμφόρηση σε όλο το δίκτυο και ίσως ολική διάρρηξη της συνεκτικότητάς του.

Αντίμετρα:

Μια πρώτη αντιμετώπιση στην επίθεση πλημμύρας πακέτων Hello είναι οι κόμβοι να αυθεντικοποιούν την ταυτότητα των γειτόνων από τους οποίους λαμβάνουν τα πακέτα. Αυτό μπορεί να επιτευχθεί με την υποστήριξη από μια εξωτερική αρχή πιστοποίησης ή με ίδια ad hoc μέσα αυθεντικοποίησης των κόμβων. Ένας άλλος τρόπος αντιμετώπισης είναι η πιστοποίηση της διπλής κατευθυντικότητας των ζεύξεων μεταξύ των κόμβων, δηλαδή πριν προωθηθούν τα πακέτα στον επόμενο ad hoc κόμβο πρέπει πρώτα να έχει εξακριβωθεί η συμμετρικότητα της ασύρματης αυτής ζεύξης [50]. Επίσης, είναι κοινή πρακτική οι κόμβοι να μην προωθούν περαιτέρω πακέτα που λαμβάνουν από κόμβους οι οποίοι βρίσκονται δύο βήματα μακριά.

3.8. ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. “A survey on sensor networks”. IEEE Communications Magazine, 40(8):102–114, August 2002.

[2] I. F. Akyildiz, X. Wang. “A Survey on Wireless Mesh Networks”. IEEE Communications Magazine, Vol. 33, Issue 9, September 2005, pp. S23-S30.

[3] IETF MANET WG, S. Corson and J. Macker. “Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations”, RFC 2501, January 1999, http://www.ietf.org/rfc/rfc2501.txt.

[4] M. Graussglauser and D. N. C. Tse: “Mobiliy increases the Capacity of Ad Hoc Wireless Networks”. IEEE/ACM Transactions on Networking, Vol. 10, No. 4, 2002.

[5] “Potentials of Opportunistic Routing in Energy-Constrained Wireless Sensor Networks”. Gunnar Schaefer, Fran´Ecois Ingelrest, and Martin Vetterli, Ecole Polytechnique F´ed´erale de Lausanne (EPFL), Switzerland, U. Roedig and C.J. Sreenan (Eds.): EWSN 2009, LNCS 5432, pp. 118–133, 2009. Springer-Verlag Berlin Heidelberg 2009.

[6] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, J.-P. Hubaux, “Secure vehicular communications: design and architecture”, IEEE Communications Magazine, vol. 46, no. 11, pp. 100-109, November 2008.

[7] C. Perkins, E. Royer, S. Das, “Ad hoc on demand distance vector (AODV) routing”, Available from: http://www.ietf.org/internet-drafts/draft-ieft-manetaodv-03.txt, 1999.

[8] D. B. Johnson and D.A. Maltz, “Dynamic source routing in ad hoc wireless networks”, Mobile Computing, T. Imielinski and H. Korth, Eds., Kluwer, 1996, pp. 153–81.

[9] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", Comp. Commun. Rev., Oct. 1994, pp.234-244.

[10] Manel Guerrero Zapata, “Secure Ad hoc On Demand Distance Vector (SAODV) Routing”, Technical University of Catalonia (UPC), Mobile Ad Hoc Networking Working Group, Internet Draft, 15 September 2005.

[11] Manel Guerrero Zapata, N. Asokan, “Securing Ad Hoc Routing Protocols”, WiSe’02,September 28, 2002, Atlanta, Georgia, USA, ACM 1-58113-585-8/02/0009 Copyright 2002.

[12] “A Trust Model Based Routing Protocol for Secure Ad Hoc Networks”. Xiaoqi Li, Michael R. Lyu, and Jiangchuan Liu Department of Computer Science and Engineering The Chinese University of Hong Kong Shatin, N.T., Hong Kong, IEEE2004.

[13] Davide Cerri and Alessandro Ghioni, “Securing AODV: The A-SAODV Secure Routing Prototype”, IEEE Communications Magazine, Vol. 46, Issue 2, February 2008, pp. 120-125.

[14] Tsu-Wei Chen and Mario Gerla, "Global State Routing: “A New Routing Scheme for Ad-hoc Wireless Networks" Proc. IEEE ICC '98, Atlanta, GA, USA, June 98, pp. 171-175, available at:

http://www.ics.uci.edu/~atm/adhoc/paper-collection/gerla-gsr-icc98.pdf.

[15] A. Iwata, C.-C. Chiang, G. Pei, M. Gerla, and T.-W. Chen, "Scalable Routing Strategies for Ad Hoc Wireless Networks" IEEE Journal on Selected Areas in Communications, Vol. 17, No 8, Special Issue on Ad-Hoc Networks, Aug. 1999, pp.1369-79, available at:

http://www.cs.ucla.edu/NRL/wireless/PAPER/jsac99.ps.gz.

[16] Mingliang Jiang, Jinyang Li, Y.C. Tay. "Cluster Based Routing Protocol". August 1999, IETF Draft, 27 pages. http://www.ietf.org/internet-drafts/draft-ietf-manet-cbrp-spec-01.txt.

[17] VD Park and MS Corson. "A highly adaptive distributed routing algorithm for mobile wireless networks", Proceedings INFOCOM'97, Apr. 1997, 9 pages.

http://www.ics.uci.edu/~atm/adhoc/paper-collection/corson-adaptive-routing-infocom97.pdf.

[18] Chai-Keong Toh. “A Novel Distributed Routing Protocol to Support Ad hoc Mobile Computing”. Proc. IEEE 15th Annual International Phoenix Conference on Computers and Communications, IEEE IPCCC 1996, 27 March-29, Phoenix, AZ, USA, pp. 480-486. http://www.ics.uci.edu/~atm/adhoc/paper-collection/toh-distributed-routing-ipccc96.pdf.

[19] V. Park, S. Corson: Temporally-Ordered Routing Algorithm (TORA) Version 1, Functional Specification, Internet Draft, IETF MANET Working Group, June 2001, [3]. A Link Reversal

Routing (LRR) algorithm. Z. J. Haas and M.R. Pearlman, "The Performance of Query Control Schemes for the Zone Routing Protocol," ACM SIGCOMM'98.

[20] Basagni S, Chlamtac I, Syrotiuk V, and Woodward B. “A Distance Routing Effect Algorithm for Mobility (DREAM)”. In Proceedings of ACM/IEEE MobiCom, pp. 76–84, 1998.

[21] Li J, Jannoti J, De Couto D, Krager D, and Morris R. “A Scalable Location Service for Geographic Ad Hoc Routing”. Proceedings of ACM/IEEE MobiCom, pp. 120–130, 2000.

[22] Lee S-J, Su W, and Gerla M. “Wireless Multicast Rooting with Mobility Prediction”. Mobile Networks and Applications, Kluwer Academic Publishers, Vol. No. 6 pp. 351-360, 2001.

[23] Bae Ko Y, and Vaidya N. Location-Aided Routing (LAR) in Mobile Ad Hoc Networks. In Proceedings of the ACM/IEEE MobiCom, pp. 66–75, 1998.

[24] B. Karp, H.T. Kung. “GPSR: greedy perimeter stateless routing for wireless networks”, in: Mobile Computing and Networking, 2000, pp. 243–254.

[25] Asad Amir Pirzada and Chris McDonald “Trusted Greedy Perimeter Stateless Routing”, IEEE, ICON2007.

[26] A. Iwata, C.-C. Chiang, G. Pei, M. Gerla, and T.-W. Chen, "Scalable Routing Strategies for Ad Hoc Wireless Networks" IEEE Journal on Selected Areas in Communications, Special Issue on Ad-Hoc Networks, Aug. 1999, pp.1369-79.

[27] Sung-Ju Lee, Mario Gerla, and Ching-Chuan Chiang: "On-Demand Multicast Routing Protocol", In Proc. of the Wireless Communications and Networking Conference (WCNC), pages 1298 - 1302, New Orleans, LA, September 1999. Available from: http://www.cs.ucla.edu/NRL/wireless/PAPER/odmrp-wcnc99.ps.gz.

[28] Elizabeth M. Royer and Charles E. Perkins: "Multicast Operation of the Ad-hoc On-Demand Distance Vector Routing Protocol", In Proc. of the 5th annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), pages 207 - 218, Seattle, WA, August 1999.

[29] Mines - J. Boleng and T. Camp, “Adaptive Location Aided Mobile Ad Hoc Network Routing”, Proceedings of the 23rd IEEE International Performance, Computing, and Communications Conference (IPCCC '04), pp. 423-432, 2004.

http://toilers.mines.edu/pub/Public/PublicationList/Boleng-PhD.pdf.

[30] MARIO JOA-NG, I-TAI-LU. “A Peer-to-Peer Zone-Based Two-Level Link State Routing for Mobile Ad Hoc Networks”. IEEE Journal on Selected Areas In Communication, Vol. 17, No. 8, pp. 1415-1425, August 1999.

[31] M. Gerla, X. Hong, L. Ma, G. Pei. “Landmark Routing Protocol (LANMAR)”, Internet Draft, draft-ietf-manet- lanmar-01.txt, work in progress, June 2001.

[32] Kuhn, R. Wattenhofer, Y. Zhang, and A. Zollinger, Geometric Ad-Hoc Routing: Of Theory and Practice. In Proc. of Symp. on Principles of Distributed Computing (PODC), 2003.

[33] Prosenjit Bose and Pat Morin and Ivan Stojmenovic and Jorge Urrutia: “Routing with guaranteed delivery in ad hoc wireless networks”, DIALM '99: Proceedings of the 3rd international workshop on Discrete algorithms and methods for mobile computing and communications, Seattle, Washington, US, pages 48-55, 1999, ISBN 1-58113-174-7.

[34] Z. J. Haas, M. R. Pearlman, P. Samar. “The Zone Routing Protocol (ZRP) for Ad Hoc Networks”, Internet Draft, http://www.ietf.org/proceedings/02nov/I-D/draft-ietf-manet-zone-zrp-04.txt.

[35] M. Gerla, G. Pei, X. Hong, T-W Chen. “Fisheye State Routing Protocol (FSR) for Ad Hoc Networks”, Internet Draft, draft-ietf-manet-fsr-00.txt, work in progress, June 2001. (http://wiki.uni.lu/secan-lab/Fisheye+State+Routing.html).

[36] P. Jacquet, P. Muhlethaler, A. Qayyum, A. Laouiti, L. Viennot, T. Clausen. “Optimized Link State Routing Protocol”, RFC 3626. http://www.olsr.net/, http://www.olsr.org/, http://qolsr.lri.fr/.

[37] S. Murthy and J. J. Garcia-Luna-Aceves, “An Efficient Routing Protocol for Wireless Networks,” ACM Mobile Networks and App. J., Special Issue on Routing in Mobile Communication Networks, Vol. 1, No. 2, Oct. 1996, pp. 183–97.

[38] W. Heinzelman, A. Chandrakasan and H. Balakrishnan “Energy-efficient communication protocol for wireless sensor networks“. Proceedings of the Hawaii International Conference System Sciences, Hawaii, January 2000.

[39] Asad Amir Pirzada, Amitava Dattaa and Chris McDonald, “Incorporating trust and reputation in the DSR protocol for dependable routing” Computer Communications Volume 29, Issue 15, 5 September 2006, Pages 2806-2821.

[40] Asad Amir Pirzada and Chris McDonald “Trusted Greedy Perimeter Stateless Routing”, IEEE, ICON2007.

[41] Asokan N, and Ginzboorg P. “Key-Agreement in Ad-hoc Networks”. In 4th Nordic Workshop on Secure Computer Systems, 1999.

[42] Stajano F, and Anderson R. “The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks”. In the 7th International Workshop on Security Protocols. Cambridge, UK, 1999.

[43] Yi S, Naldurg P, and Kravets R. Security-Aware Ad-Hoc Routing for Wireless Networks. Technical Report, University of Illinois, UIUCDCS-R-2001-2241, August 2001.

[44] Zhou L and Haas Z. Securing Ad Hoc Networks. IEEE Network, Vol. 13 (6), pp. 24—30, November, 1999.

[45] Zhang Y. and Lee W: “Intrusion Detection in Wireless Ad-Hoc Networks”. In: 6th ACM/IEEE Conference on Mobile Computing and Networking, Boston, USA, 2000.

[46] Yi, S., Naldurg, P., Kravets, R. “Secure Aware Ad Hoc Routing for Wireless Networks”. Proceedings of the 6th World Multi-Conference on Systemics, Cybernetics and Informatics (SCI) pp. 286-292, Orlando, FL, July 2002.

[47] Secure Routing Protocol (SRP) διαθέσιμο από: http://www.ietf.org/internet-drafts/draft-papadimitratos-secure-routing-protocol-00.txt

[48] CERT Coordination Center. Smurf IP denial-of-service attacks. Technical report, CERT Advisory CA-98:01, November, 1998.

[49] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour, A survey of routing attacks in mobile ad hoc networks, IEEE Wireless Communications, October 2007.

[50] Chris Karlof and David Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”, Proceedings of the IEEE International Workshop on Sensor Network Protocols and Applications, pp. 113-127, May 2003.

[51] Kenney, Malachi, “Ping of Death”, January 1997, Available from:
<http://www.insecure.org/sploits/ping-o-death.html>.

[52] M. Al-Shurman, S-M. Yoo, and S. Park, “Black Hole Attack in Mobile Ad Hoc Networks,” ACM Southeast Regional Conf. 2004.

[53] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, Y. Nemoto. “Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method”. International Journal of Network Security Vol.5, No.3, PP.338-346, Nov. 2007.

[54] C. Adjih, D. Raffo, and P. Muhlethaler, “Attacks Against OLSR: Distributed Key Management for Security,” 2nd OLSR Interop/Wksp., Palaiseau, France, July 28–29, 2005.

[55] S. Lee, B. Han, and M. Shin, “Robust Routing in Wireless Ad Hoc Networks,” 2002 Int’l. Conf. Parallel Processing Wksps, Vancouver, Canada, Aug. 18–21, 2002.

[56] Y.-C. Hu, A. Perrig, and D.B. Johnson. “Packet leashes: a defense against wormhole attacks in wireless networks”. In Proc. IEEE Infocom 2003, 3, 1976–1986, April 2003.

[57] Mauro Conti, Roberto Di Pietro, Luigi V. Mancini, and Alessandro Mei, “Requirements and Open Issues in Distributed Detection of Node Identity Replicas in WSN“, 2006 IEEE International Conference on Systems, Man, and Cybernetics, October 8-11, 2006, Taipei, Taiwan.

[58] Chakib Bekara and Maryline Laurent-Maknavicius, “A New Protocol for Securing Wireless Sensor Networks Against Nodes Replication Attacks”, Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2007).

[59] Bo Zhu and Venkata Gopala Krishna Addada, “Efficient Distributed Detection of Node Replication Attacks in Sensor Networks”, 23rd Annual Computer Security Applications Conference, Florida, 2007, pp. 257-267.

[60] A. Perring, Y-C Hu and D. B. Johnson. “Wormhole Protection in Wireless Ad Hoc Networks”. Technical Report TR01-384, Dept. of Computer Science, Rice University.

[61] Basagni S. et al. “Mobile Ad Hoc Networking”, Wiley Interscience, 2004.

[62] Charles E. Perkins, Elizabeth M. Royer, Samir R. Das, "Ad Hoc On-demand Distance Vector Routing", October 99 IETF Draft, 33 pages, http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-04.txt.

[63] Asad Amir Pirzada, Amitava Dattaa and Chris McDonald, “Incorporating trust and reputation in the DSR protocol for dependable routing” Computer Communications Volume 29, Issue 15, 5 September 2006, pp. 2806-2821.

[64] Jian Chen Yong Guan Udo Pooch, “Customizing GPSR for Wireless Sensor Networks”, 2004 IEEE International Conference on Mobile Ad-hoc and Sensor Systems. (OD-GPSR).

[65] A. Rao, C. Papadimitriou, S. Ratnasamy, S. Shenker, and I. Stoica. Geographic Routing without Location Information. In Proc. of Mobile Computing and Networking (MobiCom), 2003.

[66] Wu Hao, Cheng Chao Li, Cheng-shu, “Research on One Kind of Improved GPSR Secure Routing Protocol”, IEEE 2007 International Symposium on Microwave, Antenna, Propagation, and EMC Technologies For Wireless Communications, 14-17 August 2007 Hangzhou, China.

[67] Jian Chen Yong Guan Udo Pooch, “Customizing GPSR for Wireless Sensor Networks”, 2004 IEEE International Conference on Mobile Ad-hoc and Sensor Systems.

[68] Ka-Shun Hung, King-Shan Lui, and Yu-Kwong Kwok, “A Trust-Based Geographical Routing Scheme in Sensor Networks”, IEEE WCNC 2007.

[69] S. Marti et al. “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks”. ACM MOBICOM, 2000.

[70] Α. Μητροκώτσα, ΑΝΙΧΝΕΥΣΗ ΕΙΣΒΟΛΩΝ ΣΕ ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ ΜΕ ΑΛΓΟΡΙΘΜΟΥΣ ΜΗΧΑΝΙΚΗΣ ΜΑΘΗΣΗΣ. Διδακτορική Διατριβή, Τμήμα Πληροφορικής Πανεπιστημίου Πειραιώς, 2007.

[71] Kai Zimmermann et al. “Autonomic Wireless Network Management“. The Ambient Networks research project, supported by the EC under its Sixth Framework Program.

[72] http://locustworld.com.

[73] http://www.irda.org/.

4. ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ

4.1. ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ

Για τα ασύρματα δίκτυα ad hoc προτείνουμε λύσεις που διασφαλίζουν την ***αυτο-οργάνωση*** των δικτύων και ταυτόχρονα την ***αυτο-προστασία*** από τους κακόβουλους εισβολείς. Επιδιώκουμε λύση που είναι πολυστρωματική και διαστρωματική, δηλαδή λύση όπου τα ανώτερα επίπεδα στη δικτυακή αρχιτεκτονική αλληλεπιδρούν με τα κατώτερα επίπεδα λαμβάνοντας ενημερώσεις για τις τιμές των δικτυακών παραμέτρων που χαρακτηρίζουν την επίδοση στα χαμηλότερα επίπεδα. Στην αρχιτεκτονική αυτή οι διαστρωματικές ποιότητες που επιδιώκουμε να επιτύχουμε είναι η αποδοτική διαχείριση της διαθέσιμης ενέργειας στους κόμβους (προτείνουμε αλληλεπίδραση μεταξύ του φυσικού επιπέδου και του επιπέδου του δικτύου), η αποδοτική αυτό-οργάνωση των κόμβων (προτείνουμε αλληλεπίδραση ανάμεσα στο επίπεδο του δικτύου και στις διαδικασίες που τρέχουν στο στρώμα του μεσισμικού) και η προστασία του συστήματος από τις επιθέσεις. Το σύστημα προστασίας είναι ένα κάθετο στρώμα -“plane”- που διατρέχει και προστατεύει όλα τα λειτουργικά επίπεδα, όπως φαίνεται στην Εικόνα 16.

Η στοίβα των πρωτοκόλλων ad hoc από το επίπεδο του δικτύου και επάνω αποτελείται από τρία βασικά στρώματα που είναι το επίπεδο της ad hoc δρομολόγησης, το επίπεδο του ad hoc μεσισμικού και το επίπεδο της ad hoc εφαρμογής. Το επίπεδο της δρομολόγησης είναι πρωταρχικό στα δίκτυα ad hoc αφού η βασική λειτουργία του δικτύου ad hoc είναι να μπορούν οι κόμβοι μόνοι τους να βρίσκουν το μονοπάτι προς τον τελικό προορισμό, να αποκτούν αυτόματα μια διεύθυνση όταν εισέρχονται στο δίκτυο και επίσης να μπορούν να επαναδρομολογούν τα πακέτα σε περίπτωση τυχαίων βλαβών ή σε περίπτωση στοχευμένων επιθέσεων που καταφέρνουν να συμβιβάσουν κάποιους από τους κόμβους του δικτύου και άρα να ελέγξουν τα μονοπάτια δρομολόγησης. Στο επίπεδο των ad hoc εφαρμογών έχουμε τις ανώτερες εφαρμογές τελικού χρήστη όπως η κοινή χρήση αρχείων, οι πολυμεσικές εφαρμογές, οι περιβαλλοντικές εφαρμογές, οι εφαρμογές παρακολούθησης και άλλες που προϋποθέτουν την αξιόπιστη διάθεση των δικτυακών υπηρεσιών στα κατώτερα στρώματα της αρχιτεκτονικής.

Θεωρούμε ότι η επικοινωνία των ad hoc εφαρμογών πρέπει να βασίζεται στις *ανοιχτές και ομότιμες επικοινωνίες από άκρη σε άκρη* μέσα στο δίκτυο οι οποίες παρέχονται από τις υπηρεσίες του στρώματος του μεσισμικού. Το στρώμα του μεσισμικού βρίσκεται πάνω από το επίπεδο του δικτύου και κάτω από το επίπεδο της εφαρμογής. Στο ad hoc μεσισμικό εντάσσουμε τις παρακάτω διαδικασίες.

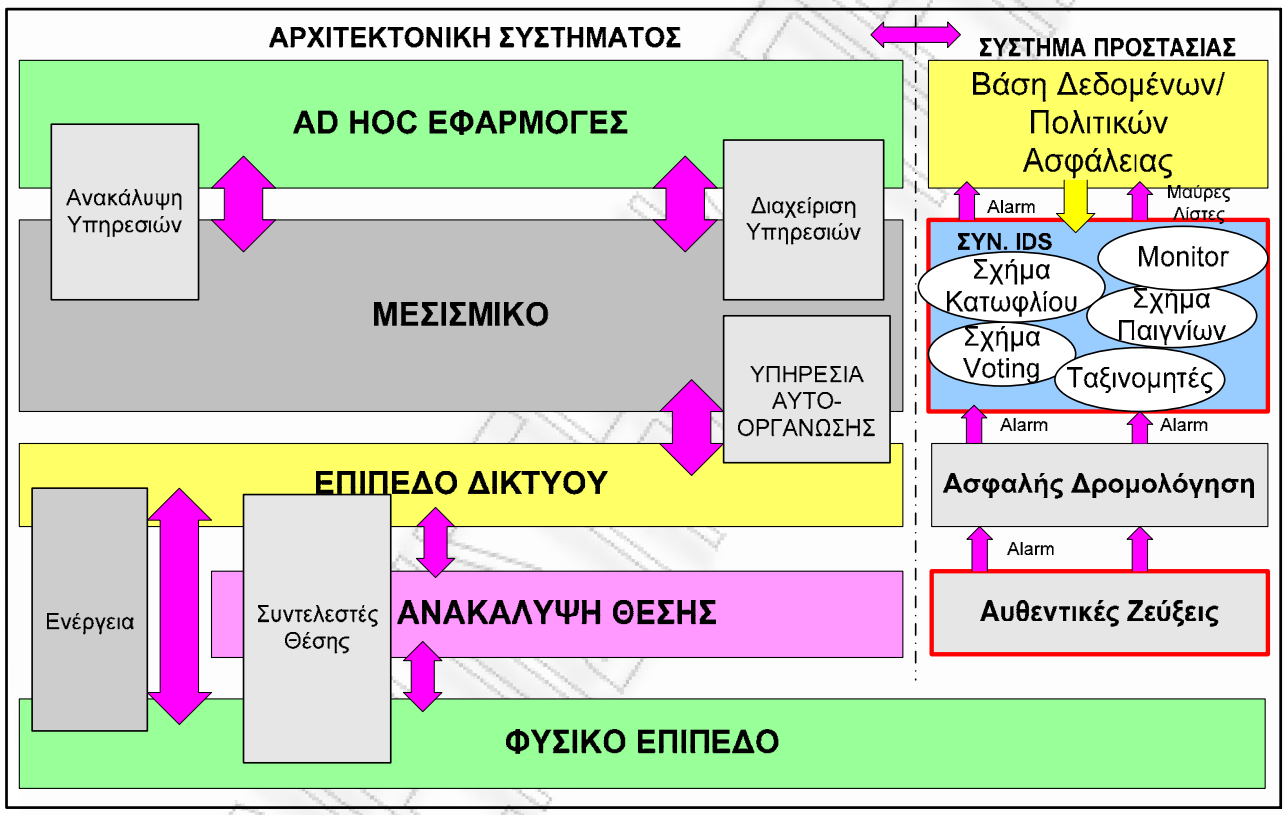
- Την ανακάλυψη και επίκληση των διαθέσιμων ad hoc υπηρεσιών (“service discovery and service invocation”) που εγγράφονται σε κατάλληλα μητρώα.
- Τη διαχείριση των ad hoc υπηρεσιών (ανάπτυξη, διάθεση και ανανέωση των υπηρεσιών).
- Τις υπηρεσίες παρακολούθησης της δικτυακής κίνησης και της συμπεριφοράς των κόμβων (“traffic monitoring”).
- Την υπηρεσία αυτο-οργάνωσης του δικτύου ad hoc (διαχείριση πόρων του δικτύου, ομαδοποίηση των κόμβων σε ιεραρχίες με κατάλληλους αλγορίθμους συσταδοποίησης και εκλογής αρχηγών).

Έτσι μια προτεινόμενη λύση είναι η εισαγωγή και διαχείριση των πολυ-επίπεδων ιεραρχιών όπως και η εκλογή των κόμβων-αρχηγών μέσα στο ad hoc δίκτυο να επιτυγχάνεται με αλγορίθμους, διαδικασίες και πρωτόκολλα που ανήκουν στο στρώμα του μεσισμικού. Συνεπώς, σε αυτή την περίπτωση το μεσισμικό είναι το στρώμα που αναλαμβάνει και διεκπεραιώνει την οργάνωση των

κόμβων σε ομάδες παρέχοντας ταυτόχρονα προσαρμοστικότητα, βελτιστοποίηση, ικανότητα κλιμάκωσης σε μεγάλα δίκτυα, αξιοπιστία και ευρωστία.

Μια άλλη πιθανή λύση όσον αφορά την αυτο-οργάνωση των κόμβων είναι αυτή να παρέχεται σαν υπηρεσία από το χαμηλότερο επίπεδο του δικτύου, δηλαδή κατά τη δρομολόγηση των μηνυμάτων από κόμβο σε κόμβο. Η καταλληλότητα των δύο λύσεων εξαρτάται από την πολυπλοκότητα της κάθε μιας σχεδίασης και υλοποίησης που προτείνεται καθώς επίσης και από τις απαιτήσεις των εφαρμογών που τρέχουν στα ανώτερα επίπεδα της στοίβας των ad hoc πρωτοκόλλων.

Όπως απεικονίζεται στην Εικόνα 16 προτείνεται συνδυασμός των παραπάνω λύσεων. Στην Εικόνα 16 η διαχείριση των υπηρεσιών και οι διαδικασίες οργάνωσης των κόμβων διατρέχουν γειτονικά επίπεδα στην αρχιτεκτονική του συστήματος.



Εικόνα 16. Προτεινόμενη αρχιτεκτονική συστήματος στο δίκτυο ad hoc.

Τέλος, όσο αφορά την αρχιτεκτονική του συστήματος που οργανώνεται σε μια ιεραρχική δομή πολλών επιπέδων πρέπει να ξεκαθαρίσουμε ότι οι κόμβοι-αρχηγοί είναι αυτοί που αναλαμβάνουν να εκτελέσουν πρόσθετες εργασίες όπως:

- Δρομολόγηση των πακέτων μέσα στη συστάδα και μεταξύ των απομακρυσμένων συστάδων.
- Διαχείριση της σειράς πρόσβασης των απλών κόμβων στο ασύρματο μέσο και διαχείριση των πόρων του ραδιοφάσματος.
- Διαχείριση κλειδιών για τα απλά μέλη.
- Διαχείριση της συμμετοχής των κόμβων στις ομάδες.
- Διαχείριση πολυμεσικών συνόδων σε ένα MANET.

- Συνεργατικές λειτουργίες ανίχνευσης εισβολέων, αντίδρασης και ανάκαμψης με ενημέρωση των υπολοίπων απλών κόμβων της συστάδας και των υπολοίπων αρχηγών σε μακρινές συστάδες σε περίπτωση επίθεσης.

Αυτές οι λειτουργίες είναι πρόσθετα λειτουργικές οντότητες/τμήματα που ενεργοποιούνται σε εκείνους τους κόμβους που επιλέγονται δυναμικά να είναι οι αρχηγοί μέσα στο δίκτυο. Σύμφωνα με αυτή την αρχιτεκτονική του συστήματος που προτείνουμε το *ομότιμο* στις επικοινωνίες όλων των κόμβων δεν καταργείται. Όλοι οι κόμβοι είναι κατ' αρχήν ομότιμοι ως προς τις δυνατότητές τους, τουλάχιστον ως προς το κατανεμημένο λογισμικό που διαθέτουν. Αυτό σημαίνει ότι αρχικά εγκαθίστανται σε όλους τους κόμβους τα ίδια λειτουργικά τμήματα λογισμικού. Κατά τη λειτουργία των πρωτοκόλλων στο δίκτυο, και καθώς οι δικτυακές συνθήκες μεταβάλλονται με δυναμικό τρόπο, το σχήμα οργάνωσης εκλέγει εκείνους τους κόμβους που είναι καταλληλότεροι να αναλάβουν το ρόλο του αρχηγού στη γειτονιά τους.

Σε αυτούς τους κόμβους-αρχηγούς ενεργοποιούνται επιλεκτικά τα πρόσθετα τμήματα λογισμικού έτσι ώστε να μπορούν οι κόμβοι αυτοί να παίξουν ισχυρότερο ρόλο μέσα στο δίκτυο εκτελώντας τις πιο πάνω εργασίες με αιχμή την προστασία του δικτύου που θα εξετάσουμε στην επόμενη παράγραφο. Στην Εικόνα 16 η προστασία από τις επιθέσεις δίνεται από συνεργατικά σχήματα Ανίχνευσης Εισβολέων ("Intrusion Detection Systems, IDS") όπως σχήματα κατωφλίου, σχήματα ψηφοφορίας, σχήματα στατιστικής ανάλυσης των δικτυακών δεδομένων και λήψης αποφάσεων κατά την ανίχνευση επιθέσεων, ταξινομητές και σχήματα εφαρμογής της θεωρίας παιγνίων για την από κοινού εκμετάλλευση των πόρων του δικτύου και των κόμβων από τις διεργασίες-ανταγωνιστές.

Σε μια άλλη περίπτωση ad hoc δικτύου είναι δυνατόν οι κόμβοι να είναι *ετερογενείς* κυρίως ως προς το υλικό τους. Δηλαδή μπορεί να έχουν διαφορετικές δυνατότητες επεξεργασίας, διαφορετικές δυνατότητες ασύρματης μετάδοσης όπως για παράδειγμα μεγαλύτερη ισχύ εκπομπής και άρα μεγαλύτερη κάλυψη, διαφορετικές δυνατότητες αποθήκευσης, διαφορετικές δυνατότητες αισθητήρων κ.α. Και στην περίπτωση ενός δικτύου που είναι ετερογενές το μοντέλο επικοινωνιών που υιοθετούμε είναι το μοντέλο ομότιμων κόμβων. Ωστόσο είναι προτιμότερο σε μια τέτοια περίπτωση οι αλγόριθμοι αυτο-οργάνωσης να είναι στατικοί, δηλαδή εκ των προτέρων να ορίζονται οι ισχυρότεροι κόμβοι ως εκείνοι οι κόμβοι που θα αναλάβουν το ρόλο του αρχηγού στην περιοχή τους.

4.2. ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ ΠΡΟΣΤΑΣΙΑΣ

Πολλές είναι οι υπάρχουσες τεχνικές λύσεις που προσφέρουν αντίμετρα για την αντιμετώπιση των επιθέσεων. Ωστόσο το επιτυγχάνουν αυτό για συγκεκριμένα ad hoc δίκτυα και για συγκεκριμένους τύπους επιθέσεων. Ενδεικτικά παραδείγματα τέτοιων μεμονωμένων λύσεων προστασίας είναι το πρωτόκολλο Trust-based DSR [9] το οποίο αποτελεί επέκταση ασφάλειας του DSR ή οι ιεραρχικές λύσεις των δικτύων MANET που τρέχουν το πρωτόκολλο δρομολόγησης AODV και που προστατεύουν το δίκτυο από την απειλή "wormhole" [3], ή από την απειλή της "μαύρης τρύπας" [4] ή ακόμη άλλες επεκτάσεις του πρωτοκόλλου AODV ([5] και [10]) που αντιμετωπίζουν τις επιθέσεις πλημμύρας με τεχνικές όπως η καθυστέρηση απάντησης και ακόμη λύσεις που επεκτείνουν το γεωγραφικό ad hoc πρωτόκολλο GPSR συνήθως με την εγκατάσταση εμπιστοσύνης μεταξύ των κόμβων όπως το πρωτόκολλο Trust-based GPSR [6] που προστατεύει το δίκτυο από επιθέσεις άρνησης προώθησης μηνυμάτων και μόνο ή ακόμη ad hoc λύσεις που προστατεύουν μόνο από την επίθεση Sybil [7].

Ωστόσο είναι επιθυμητό οι λύσεις προστασίας να σχεδιάζονται κατά τρόπο ώστε να αποτελούν ένα ολοκληρωμένο Σύστημα Ανίχνευσης και Αντιμετώπισης Εισβολών (IDS) και να εντάσσονται σε αρχιτεκτονικές που ικανοποιούν τις προδιαγραφές συστημάτων IDS που ήδη έχουμε αναφέρει και όπως φαίνεται στην Εικόνα 16. Ένα τέτοιο σύστημα θα πρέπει να αποτελεί μια τεχνική λύση που

είναι κατά το δυνατόν ανεξάρτητη και αποδεσμευμένη από ένα συγκεκριμένο πρωτόκολλο ad hoc. Η λύση προστασίας επιπλέον θα πρέπει να επιτυγχάνει την ανίχνευση και την αντιμετώπιση ενός αρκούντως μεγάλου αριθμού από δυνατές επιθέσεις κατά του δικτύου. Είναι προφανές ότι αυτή η κατεύθυνση στην αναζήτηση λύσης για την προστασία των δικτύων ad hoc δυσχεραίνεται από τους περιορισμούς στους διαθέσιμους πόρους που έχουμε επισημάνει. Η προσαρμογή όμως των τεχνικών λύσεων και των επιμέρους αντιμέτρων σε νέες αρχιτεκτονικές που διαθέτουν τα βασικά χαρακτηριστικά των συστημάτων IDS (πρόληψη, ανίχνευση, αντίδραση και ανάκαμψη) αν μη τι άλλο θα καταστήσει τον τρόπο αντιμετώπισης των επιθέσεων πιο συστηματικό. Στην Εικόνα 16 το συνεργατικό σύστημα IDS απεικονίζεται ως τμήμα του μεσισμικού στρώματος που εγκαθίσταται στο δίκτυο ad hoc.

Δεδομένου ότι έχουμε προτείνει η αυτο-οργάνωση και η προστασία των δικτύων ad hoc να σχεδιάζεται και να υλοποιείται με βάση κατάλληλους και αποδοτικούς αλγόριθμους clustering οι οποίοι εισάγουν και εκμεταλλεύονται τις πολύ-επίπεδες ιεραρχίες στο ad hoc δίκτυο, είναι επιθυμητό πρώτα να απαριθμήσουμε τις δυνατές υπάρχουσες αρχιτεκτονικές ενός συστήματος IDS και στη συνέχεια να διερευνήσουμε το εφικτό της χρήσης και της ενσωμάτωσης των διαφόρων παραλλαγών των σχημάτων clustering ως μέρος των συστημάτων ανίχνευσης εισβολών IDS στο περιβάλλον ad hoc.

Η πρωταρχική κατηγοριοποίηση των Συστημάτων Ανίχνευσης Εισβολών (IDS) που συναντάμε κυρίως στα ενσύρματα αλλά και στα ασύρματα δίκτυα γενικού σκοπού γίνεται με βάση τον τρόπο ανίχνευσης των επιθέσεων και τον τρόπο έγερσης και μετάδοσης συναγερμών, είναι δε η εξής:

- ***Ανίχνευση Κακόβουλης Χρήσης*** βασισμένη στις υπογραφές ("*signature-based misuse detection*"). Σε αυτήν την περίπτωση το IDS διαθέτει μια βάση δεδομένων με όλες τις γνωστές επιθέσεις που έχει καταγράψει ή είναι γνωστές εκ των προτέρων στο σύστημα. Στη διάθεση του συστήματος υπάρχουν δεδομένα ελέγχου (audit data) που έχουν συγκεντρωθεί κατά την κρίσιμη περίοδο λειτουργίας του δικτύου οπότε γίνεται σύγκριση της δικτυακής κίνησης με τις γνωστές υπογραφές των επιθέσεων που είναι διαθέσιμες στο σύστημα προκειμένου να ληφθεί απόφαση για συναγερμό ή όχι. Τα συστήματα αυτά είναι πλέον αρκετά τρωτά και, επιπρόσθετα, οι πόροι που απαιτούν τα καθιστούν συνήθως απαγορευτικά για τα δίκτυα ad hoc, ιδιαίτερα για τα δίκτυα αισθητήρων.

- ***Ανίχνευση Ανωμαλιών*** ("*anomaly detection*"). Σε αυτήν την περίπτωση αρχικά συλλέγονται ίχνη δικτυακής κίνησης χωρίς την παρουσία επιθέσεων. Αυτό αποτελεί για το IDS το προφίλ της κανονικής συμπεριφοράς για το δίκτυο (παράδειγμα μια Gaussian κατανομή των δεδομένων). Αν παρατηρηθεί κάποια συμπεριφορά-ενέργεια που αποκλίνει (συνήθως με βάση κάποια προκαθορισμένη τιμή κατωφλίου) από την κανονική συμπεριφορά που είναι καταγεγραμμένη στο σύστημα, τότε αυτό αποτελεί ανίχνευση εισβολής και ακολουθεί συναγερμός και η διαδικασία αντιμετώπισης και ανάκαμψης. Τα συστήματα αυτά έχουν το πλεονέκτημα ότι μπορούν να ανιχνεύσουν σωστά ακόμη και μη γνωστές επιθέσεις και να δώσουν πολλούς ορθούς συναγερμούς ("true positive, TP").

  Συνήθως στα δίκτυα ad hoc συστήνεται η μέθοδος της ανίχνευσης ανωμαλιών παρά της ανίχνευσης κακόβουλης χρήσης. Ωστόσο και τα συστήματα ανίχνευσης ανωμαλιών δεν είναι δίχως μειονεκτήματα. Απαιτούν μεθόδους μηχανικής εκπαίδευσης ("automated machine learning") ώστε να καταφέρουν να απομονώσουν την κανονική συμπεριφορά κάτι που συνήθως δεν είναι διαθέσιμο στα δίκτυα ad hoc. Επιπλέον είναι δυνατόν τα στατιστικά της δικτυακής κίνησης να μεταβάλλονται ακόμη και χωρίς την παρουσία επιτιθέμενων (για παράδειγμα λόγω της κίνησης των κόμβων ή λόγω του καναλιού μετάδοσης). Συνεπώς δεν μπορούμε να αποφανθούμε με ακρίβεια ποια είναι ακριβώς η

κανονική συμπεριφορά των κόμβων κατά τη διάρκεια ζωής του δικτύου [25]. Υπάρχει επομένως ο κίνδυνος το Σύστημα Ανίχνευσης Ανωμαλιών να σημάνει πολλούς λανθασμένους συναγερμούς ("false positive", FP – "false negative", FN).

Η υλοποίηση της μεθόδου της ανίχνευσης ανωμαλιών μπορεί να κατηγοριοποιηθεί στις ακόλουθες τρεις βασικές κατηγορίες [1] των οποίων η λεπτομερής ανάλυση είναι εκτός των πλαισίων της διατριβής αυτής.

- Ανίχνευση Ανωμαλιών με τη χρήση μηχανικής εκμάθησης.
- Ανίχνευση Ανωμαλιών με τη χρήση εξόρυξης δεδομένων.
- Ανίχνευση Ανωμαλιών με τη χρήση στατιστικών μεθόδων.

Η προστασία των δικτύων ad hoc έχει κατ' αρχήν σκοπό να διασφαλίσει τους ίδιους τους κόμβους από τη φυσική σύλληψη και την αντιγραφή του υλικού τους. Στη συνέχεια, θα πρέπει να διασφαλίζονται οι επικοινωνίες από τον κίνδυνο των υπεξαιρέσεων και της αλλοίωσης των μηνυμάτων (εμπιστευτικότητα και ακεραιότητα) και τελικά το σύστημα ασφάλειας θα πρέπει να προστατεύει από την προσπάθεια των κακόβουλων χρηστών να εισέλθουν στο δίκτυο χωρίς να είναι εξουσιοδοτημένοι για κάτι τέτοιο (αυθεντικοποίηση). Ωστόσο, οι κακόβουλοι κόμβοι μπορούν να ξεπεράσουν και τον έλεγχο της αυθεντικοποίησης, ιδιαίτερα όταν οι έλεγχοι αυτοί είναι ασθενείς, με αποτέλεσμα να παρεισφρέουν στο δίκτυο και να εξαπολύσουν επιθέσεις εκ των έσω. Θα πρέπει λοιπόν και αυτές οι απειλές από τους ενδεχόμενους εισβολείς να ανιχνεύονται και να αντιμετωπίζονται με αντιδραστικό τρόπο.

Η τελευταία απαίτηση οδήγησε στις σχετικά πρόσφατες ερευνητικές προσπάθειες που εισήγαγαν τα Συστήματα Ανίχνευσης Εισβολών (IDS) και στα κατ΄ απαίτηση δίκτυα σαν μια δεύτερη γραμμή άμυνας [23]. Ειδικά για τα δίκτυα ad hoc με τους περιορισμένους δικτυακούς και ενεργειακούς πόρους διακρίνουμε τις παρακάτω πρόσθετες απαιτήσεις όσον αφορά τη λειτουργία των ad hoc συστημάτων IDS:

- Το ίδιο το IDS πρέπει να είναι ασφαλές, θα πρέπει δηλαδή να είναι έτσι σχεδιασμένο ώστε να αντέχει σε επιθέσεις που απειλούν το ίδιο το σύστημα ασφαλείας του δικτύου ad hoc.
- Το IDS πρέπει να είναι αξιόπιστο δίνοντας μικρό ποσοστό ψευδών συναγερμών (FP και FN) και άρα υψηλό ρυθμό σωστών ανιχνεύσεων.
- Το IDS δε θα πρέπει να επιβαρύνει την επίδοση του δικτύου ad hoc: ο γνωστός συγκερασμός μεταξύ του επιπέδου ασφάλειας, της αποδοτικότητας των συστημάτων προστασίας από πλευράς της υπολογιστικής πολυπλοκότητας και της επιβάρυνσης που επιφέρουν στις ωφέλιμες επικοινωνίες (ανάλογα με τον αριθμό μηνυμάτων που απαιτούν) εντείνεται ακόμη περισσότερο στο περιορισμένο δίκτυο ad hoc.
- Η σχεδίαση του IDS θα πρέπει να λαμβάνει υπόψη τους περιορισμένους πόρους των κόμβων ιδιαίτερα τον ενεργειακό τους περιορισμό και το διαθέσιμο εύρος ζώνης.
- Το IDS θα πρέπει να είναι κατά το δυνατόν κρυφό και διάφανο στους χρήστες.
- Η σχεδίαση του IDS θα πρέπει να λαμβάνει υπόψη ότι η εμπιστοσύνη μεταξύ των κόμβων σε ένα δίκτυο ad hoc είναι πολύ περιορισμένη, εφόσον είναι απούσα η κατάλληλη υποδομή για την εγκατάσταση εμπιστοσύνης και εφόσον είναι σχετικά πολύ πιο εύκολο οι κόμβοι σε ένα μη επιβλεπόμενο δίκτυο να συμβιβαστούν.

- Το IDS που στηρίζεται σε ιεραρχική δομή θα πρέπει να εκλέγει με αποδοτικό για το δίκτυο τρόπο τους κόμβους-αρχηγούς.

- Το IDS θα πρέπει να είναι κατανεμημένο και συνεργατικό, εφόσον και η φύση των επικοινωνιών στα δίκτυα ad hoc είναι συνεργατική.

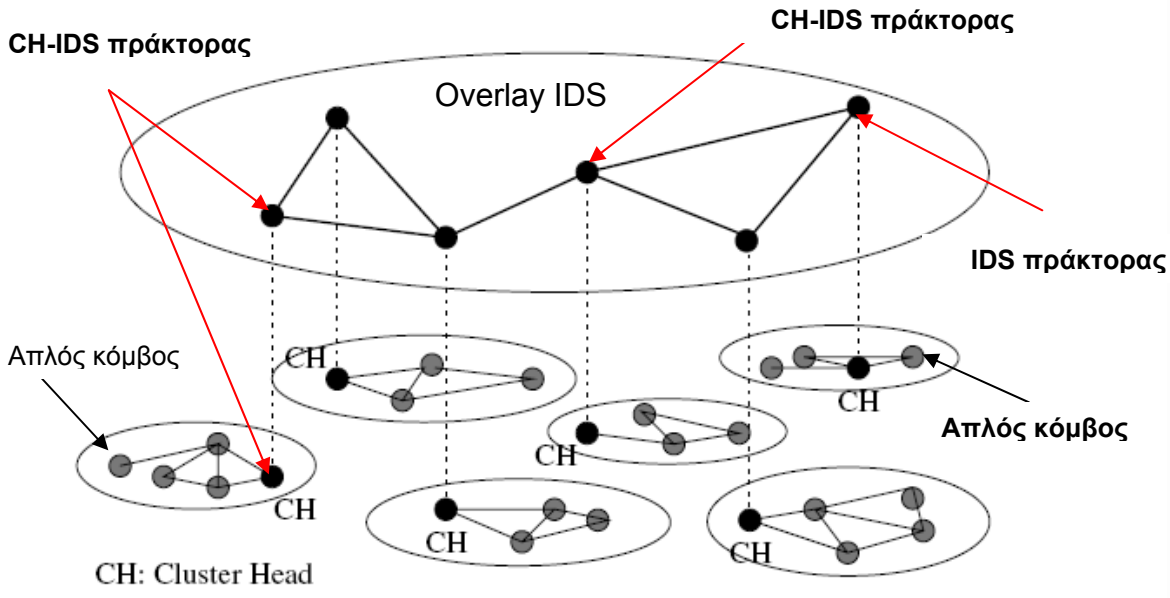
- Το IDS θα πρέπει να κάνει χρήση ανοιχτών προτύπων και προτάσεων (RFC) όπως αυτά δημοσιεύονται από το IETF Intrusion Detection Working Group (IDWG) [20].

Στη συνέχεια θα περιγράψουμε μερικές από τις βασικότερες αρχιτεκτονικές συστημάτων IDS που έχουν προταθεί και αναπτυχθεί για τα ασύρματα δίκτυα ad hoc.

4.2.1. Ιεραρχικό IDS

Το ιεραρχικό IDS για δίκτυο MANET [8] και το ιεραρχικό IDS για δίκτυο WSN [9] χαρακτηρίζεται από την απόδοση διαφορετικών ρόλων στους κόμβους. Σε ένα ad hoc δίκτυο όπου η δικτυακή λειτουργία βασίζεται στην αποδοτική ομαδοποίηση των κόμβων είναι φυσικό το ιεραρχικό μοντέλο να ταιριάζει περισσότερο για την οργάνωση του συστήματος ασφάλειας του δικτύου. Κατά τον ίδιο τρόπο που οργανώνεται το ad hoc δίκτυο σε επίπεδα, σε ένα ιεραρχικά δομημένο IDS την προστασία αναλαμβάνουν μερικοί μόνο κόμβοι-πράκτορες οι οποίοι παρακολουθούν τη δικτυακή κίνηση, συλλέγουν τα δεδομένα των υπολοίπων και αποφασίζουν με συνεργατικό [10] [11] [12] [13] ή με μη συνεργατικό τρόπο [14] για το αν το δίκτυο έχει δεχτεί επίθεση ή όχι.

Σε ένα πολύ-επίπεδο ιεραρχικό IDS το ρόλο του πράκτορα είναι δυνατόν να τον αναλάβουν αποκλειστικά οι κόμβοι-αρχηγοί που επιλέγονται για κάθε επίπεδο της ιεραρχίας, όπως απεικονίζεται στην Εικόνα 18. Φαίνεται στην Εικόνα 18 ότι οι κόμβοι αρχηγοί είναι οι αφιερωμένοι πράκτορες που απαρτίζουν ένα IDS δίκτυο επικάλυψης, δηλαδή ένα δίκτυο πρακτόρων ασφάλειας που λειτουργεί ανεξάρτητα από το εν λόγω ad hoc δίκτυο. Εναλλακτικά είναι δυνατόν και άλλοι κόμβοι εκτός των αρχηγών να λειτουργούν ως αφιερωμένοι πράκτορες στο δίκτυο IDS.



Εικόνα 17. Ιεραρχικό σύστημα προστασίας που βασίζεται σε πράκτορες IDS που εκλέγονται από τους απλούς ad hoc κόμβους.

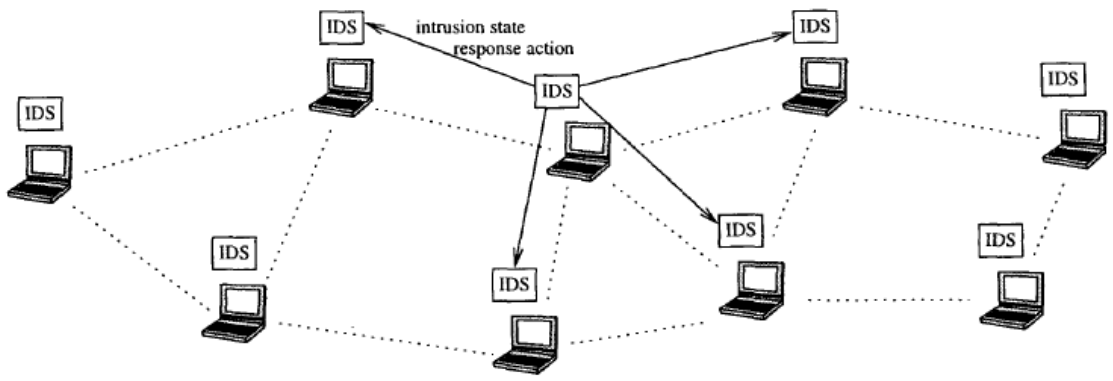
Κάθε επίπεδο της οργάνωσης του IDS σκοπό έχει να καταστήσει διαφανείς τις διαδικασίες οργάνωσης των κόμβων και τις διαδικασίες επεξεργασίας της πληροφορίας και να αποφορτίσει από αυτές τους IDS πράκτορες που βρίσκονται σε ένα ή και παραπάνω επίπεδα υψηλότερα στην ιεραρχία του συστήματος IDS. Μια έτσι οργανωμένη δομή πολλών επιπέδων μπορεί να αποσυμφορήσει την ανίχνευση εισβολέων σε δίκτυα ad hoc πολύ μεγάλης κλίμακας (για παράδειγμα σε ένα πολύ μεγάλο δίκτυο αισθητήρων) και να μειώσει για τους απλούς κόμβους τη ροή πληροφοριών ελέγχου (όπως μηνύματα συνεργασίας, μηνύματα alarms, μηνύματα ανανέωσης της ad hoc τοπολογίας και του πρωτοκόλλου δρομολόγησης). Επίσης, η ιεραρχική IDS αρχιτεκτονική μπορεί να μειώσει την επεξεργασία πολύ μεγάλου όγκου δεδομένων ελέγχου που απαιτείται για την έγκαιρη και έγκυρη ανίχνευση των εισβολέων.

Έτσι ουσιαστικά αποσυνδέεται το δίκτυο των κόμβων IDS από το δίκτυο των απλών ad hoc κόμβων οι οποίοι μπορούν να στέλνουν απρόσκοπτα τα δεδομένα που συλλέγουν όπως για παράδειγμα σε μια εφαρμογή περιβαλλοντικής παρακολούθησης, δηλαδή ανεξάρτητα από το σύστημα IDS όπου μόνο οι cluster heads αναλαμβάνουν τους μηχανισμούς παρακολούθησης, ανίχνευσης και αντίδρασης στις επιθέσεις.

Στην πλειονότητα των περιπτώσεων οι κόμβοι που αναλαμβάνουν τα επιπλέον καθήκοντα του κόμβου-πράκτορα IDS είναι οι πιο ισχυροί σε ένα ετερογενές ad hoc δίκτυο που αποτελείται από διαφορετικούς τύπους και πλατφόρμες κόμβων. Δεν αποκλείεται όμως οι IDS πράκτορες να επιλέγονται δυναμικά και σε ένα ομογενές δίκτυο, δηλαδή ανάμεσα σε εντελώς ισοδύναμους κόμβους τόσο από πλευράς του υλικού όσο και από πλευράς του λογισμικού που διαθέτουν εγκατεστημένο.

4.2.2. Κατανεμημένο IDS

Το πλήρως κατανεμημένο IDS [13], [15], [16] επιφορτίζει όλους τους κόμβους του δικτύου με τα ίδια καθήκοντα παρακολούθησης, ανταλλαγής, συλλογής και επεξεργασίας δεδομένων ελέγχου. Σε μια τέτοια περίπτωση όλοι οι κόμβοι δρουν ως IDS πράκτορες και είναι εύλογο ότι θα πρέπει να μοιράζονται τα δεδομένα τους έτσι ώστε τα αποτελέσματα των αποφάσεων να προκύπτουν μέσα από συνεργατική και συλλογική επεξεργασία. Σε ένα πλήρως κατανεμημένο σύστημα προστασίας είναι αναγκαίο οι ισοδύναμοι κόμβοι να έχουν τους απαραίτητους πόρους ώστε να μπορούν να λειτουργήσουν σαν κόμβοι-πράκτορες του συστήματος προστασίας οι οποίοι συγκεντρώνουν και επεξεργάζονται με περιοδικό ή/και ανακλαστικό τρόπο τα τοπικά δεδομένα με σκοπό να ανιχνεύσουν τους πιθανούς εισβολείς, πέρα από την επιβάρυνση για τη δρομολόγηση των μηνυμάτων που απαιτείται από την ad hoc εφαρμογή στην οποία συμμετέχουν.



Εικόνα 18. Πλήρως κατανεμημένη αρχιτεκτονική συστήματος IDS σε δίκτυο ad hoc.

Όπως φαίνεται στην Εικόνα 18 όλοι οι κόμβοι συμμετέχουν ομότιμα στη διαδικασία της ανίχνευσης ύποπτων κόμβων και στη συνέχεια της αντίδρασης ("response action"). Επίσης σε ένα πλήρως κατανεμημένο σύστημα προστασίας όλοι οι κόμβοι συμμετέχουν, όπως θα δούμε στο Κεφάλαιο 6 όπου παρουσιάζεται η προτεινόμενη λύση προστασίας, στην εκλογή των καταλληλότερων κόμβων-αρχηγών στη γειτονιά τους. Ειδικότερα, στην προτεινόμενη αρχιτεκτονική όλοι οι ad hoc κόμβοι συμμετέχουν στην προστασία από τους εισβολείς δρώντας ως IDS πράκτορες/ανιχνευτές εισβολέων ενώ οι εναλλασσόμενοι κόμβοι-αρχηγοί είναι αυτοί που δρομολογούν, συγκεντρώνουν και επεξεργάζονται ενδο-δικτυακά τα δεδομένα των υπολοίπων.

4.2.3. Συνεργατικό IDS

Όπως έχουμε ήδη περιγράψει προηγούμενα στο ιεραρχικό IDS, το χαρακτηριστικό ενός συνεργατικού IDS είναι ότι οι κόμβοι που συμμετέχουν σε αυτό αποτελούν ουσιαστικά ένα δίκτυο ασφαλείας όπου οι πράκτορες προστασίας ανταλλάσσουν δεδομένα (όπως δεδομένα που σχετίζονται με τη συμπεριφορά των υπόπτων κόμβων στο παρόν και το παρελθόν, συστάσεις για κόμβους, ψήφους, γνώμες, συναγερμούς, μαύρες λίστες κ.α.) με γειτονικούς ή και μακρινούς κόμβους που επίσης συμμετέχουν στην προστασία του δικτύου. Έτσι η τελική απόφαση ενός κόμβου-πράκτορα δεν λαμβάνει υπόψη μόνο τα τοπικά δεδομένα ελέγχου που ο ίδιος έχει συγκεντρώσει αλλά είναι αποτέλεσμα συνεργασίας με αποτέλεσμα να είναι πιο ασφαλής και πιο έγκυρη η απόφαση από την περίπτωση όπου ο κάθε κόμβος-πράκτορας παίρνει μια αυτόνομη απόφαση για μια πιθανή επίθεση. Στην τελευταία περίπτωση το IDS που βασίζεται αποκλειστικά στον κάθε κόμβο-πράκτορα είναι γνωστό ως host-based IDS το οποίο βασίζεται στα logs του λειτουργικού συστήματος για τη διάγνωση ή μη των επιθέσεων.

Τα συνεργατικά ad hoc IDS μπορεί να βασίζονται είτε σε αλγορίθμους/σχήματα εκλογής αρχηγών, είτε σε σχήματα εμπιστοσύνης που βασίζονται στη φήμη των κόμβων (reputation-based), είτε σε σχήματα κατωφλίου, είτε μπορεί να βασίζονται στη θεωρία παιγνίων για τη μοντελοποίηση της σχέσης μεταξύ επιτιθέμενου και νόμιμου ad hoc κόμβου ώστε τελικά να μπορέσουν να αποφασίσουν οι κόμβοι από κοινού για την ύπαρξη ενδεχόμενης επίθεσης και τα αντίμετρα κατά του κακόβουλου κόμβου.

Οι κόμβοι ενός IDS που δεν είναι συνεργατικό αποφασίζουν λαμβάνοντας υπόψη τα τοπικά δεδομένα που έχουν συγκεντρώσει χωρίς να μοιράζονται ή να ανταλλάσσουν δεδομένα με τους υπόλοιπους κόμβους. Στην περίπτωση που τα τοπικά δεδομένα χαρακτηρίζονται από ανεπαρκή ακρίβεια, λόγω της οποίας δεν μπορεί να εξαχθεί ασφαλές συμπέρασμα για μια πιθανή επίθεση, απαιτείται συνεργασία μεταξύ των κόμβων [13].

4.2.4. Υβριδικό IDS

Το υβριδικό σύστημα IDS συνδυάζει τα τοπικά δεδομένα ενός κόμβου-πράκτορα με τα δεδομένα που μπορούν να συγκεντρωθούν από όλο το δίκτυο. Ως αποτέλεσμα είναι δυνατή μια πιο έγκυρη άποψη για την κατάσταση του δικτύου.

4.2.5. IDS Βασισμένο σε Κινητούς Πράκτορες

Μια άλλη κατανεμημένη αρχιτεκτονική που βρίσκει εφαρμογή στα συστήματα IDS είναι αυτή που βασίζεται στο αυτόνομο υπολογιστικό υπόδειγμα των κινητών πρακτόρων. Πολλά από τα πλεονεκτήματα που προσφέρει το μοντέλο των κινητών πρακτόρων όπως η παράλληλη επεξεργασία, η απομακρυσμένη παρακολούθηση και ειδοποίηση, η κινητικότητα του κώδικα, οι αυτόνομες ενέργειες, η ανωνυμία κ.α. μπορούν να τα εκμεταλλευτούν οι ad hoc εφαρμογές που απαιτούν ασφάλεια.

Οι λύσεις που στηρίζονται στη μέθοδο αυτή διαφέρουν μεταξύ τους ως προς τον τρόπο που οι κινητοί πράκτορες χρησιμοποιούνται στην ανίχνευση των εισβολών. Ωστόσο, η βασική ιδέα είναι

ότι ένας πράκτορας του συστήματος IDS που δρα σαν κινητός πράκτορας μπορεί να αποσταλεί σε μια μακρινή περιοχή του δικτύου για να συγκεντρώσει και, κυρίως, για να αναλύσει τα δεδομένα και στη συνέχεια για να επιστρέψει το αποτέλεσμα στον αρχικό κόμβο ο οποίος ξεκίνησε τη διαδικασία ανίχνευσης.

Οι κινητοί πράκτορες είναι μία τεχνολογία απομακρυσμένης εκτέλεσης και υπολογισμού που είναι κατάλληλη για την επιδιόρθωση σφαλμάτων και την επιβεβαίωση της επιβιωσιμότητας και της συνεκτικότητας των κόμβων σε ένα ad hoc περιβάλλον. Ένας κινητός πράκτορας μεταφέρει μαζί με τον κώδικα και τα δεδομένα και την κατάσταση εκτέλεσης [26]. Συνεπώς μπορεί να συνεχίσει υπολογισμούς – όπως τον υπολογισμό εναλλακτικών μονοπατιών δρομολόγησης κατά τη μετανάστευσή του από κόμβο σε κόμβο. Η κινητικότητα και η αυτονομία των κινητών πρακτόρων τους καθιστούν κατάλληλους μηχανισμούς για την επιβολή μέτρων ασφάλειας σε ad hoc δίκτυα. Οι πράκτορες μπορούν ταχύτατα να προσαρμοστούν σε αλλαγές του δικτύου, όπως σε πιθανή αποσύνδεση και κατάτμηση του δικτύου, για να τροποποιήσουν τη δική τους δρομολόγηση. Συνεπώς μπορούν να προστατέψουν κρίσιμες εφαρμογές από μη αξιόπιστα δίκτυα. Η ασύγχρονη φύση τους καθιστά κατάλληλους για ανίχνευση λαθών δικτύου και για τροποποίηση της συμπεριφοράς των ίδιων των κόμβων. Συνεπώς οι κινητοί πράκτορες μπορούν να χρησιμοποιηθούν για τον έλεγχο της συμπεριφοράς του δικτύου, τη μεταφορά της συμπεριφοράς εκτέλεσης των ίδιων των κόμβων και για την αναζήτηση και επιδιόρθωση της κατάτμησης του δικτύου. Για αυτό το σκοπό όμως οι κινητοί πράκτορες θα πρέπει να είναι κατάλληλα εξοπλισμένοι με κρυπτογραφικούς μηχανισμούς όπως είναι οι κρυπτογραφημένες συναρτήσεις, οι μη αποσπώμενες υπογραφές και οι δυναμικές πολύ-υπογραφές που προστατεύουν τον ίδιο τον πράκτορα από κακόβουλες επιθέσεις [27], [28], [29], [30].

Ο κινητός πράκτορας ενός συστήματος IDS μπορεί να λαμβάνει αποφάσεις τελείως αυτόνομα [17] ή μπορεί να είναι επιφορτισμένος με την ανίχνευση ορισμένων μόνο τύπων επιθέσεων έτσι ώστε να επιτυγχάνεται εξισορρόπηση της επιβάρυνσης στους ad hoc κόμβους και το δίκτυο [18], ή ακόμη μπορεί να συλλέγει και να καταμετρά τις ψήφους που προέρχονται από τους κόμβους των διαφόρων ομάδων του δικτύου [19].

4.2.6. Προτεινόμενη Αρχιτεκτονική

Η προστασία και η ασφάλεια των τριών λειτουργικών στρωμάτων που περιγράψαμε στην αρχιτεκτονική του συστήματος (δηλαδή του δικτύου, του μεσισμικού και των εφαρμογών του χρήστη) είναι πρωταρχικής σημασίας. Σύμφωνα με τη πολυστρωματική και διαστρωματική αρχιτεκτονική του συστήματος προστασίας που προτείνουμε τα επίπεδα του δικτύου, του μεσισμικού και των εφαρμογών πρέπει να προστατεύονται με διαδικασίες ασφάλειας που θα λειτουργούν παράλληλα με το λειτουργικό επίπεδο του δικτύου. Έτσι οι διαχειριστές της ασφάλειας θα πρέπει να είναι πολυστρωματικές διαδικασίες που δε θα πρέπει να αφήνουν κενά στην προστασία της λειτουργίας του δικτύου. Ωστόσο, σύμφωνα με την πρότασή μας οι μεθοδολογίες ασφάλειας που μπορούν να εφαρμόζονται σε κάθε στρώμα μπορεί, και κάποτε επιβάλλεται, να είναι διαφορετικές.

Προτείνουμε το επίπεδο του δικτύου να προστατεύεται με αυθεντικοποίηση των ζεύξεων μεταξύ των γειτονικών κόμβων. Οι τεχνικές προστασίας των ασύρματων ζεύξεων με τη δημιουργία και τη διαχείριση συμμετρικών κλειδιών είναι πολλές [22], [23], [24]. Ενδεικτικά αναφέρουμε την τεχνική που είναι εφαρμόσιμη κυρίως σε στατικά δίκτυα και που βασίζει τη δημιουργία και την ανταλλαγή κλειδιών μεταξύ δύο όποιων κόμβων του δικτύου στις ταυτότητες (διευθύνσεις) αυτών. Με διαδικασίες όπως η κρυπτογράφηση και η αυθεντικοποίηση των μηνυμάτων που διακινούνται με ομότιμο τρόπο στο επίπεδο του δικτύου (τόσο δεδομένα όσο και πακέτα ελέγχου) είναι δυνατόν να προστατευθούν οι επικοινωνίες και έτσι να αντιμετωπιστούν επιθέσεις όπως η παρακολούθηση του καναλιού, η υπεξαίρεση δεδομένων, η αλλοίωση δεδομένων με στόχο την πρόκληση σύγχυσης στους τελικούς χρήστες, η έγχυση ψευδών δεδομένων που στοχεύει στην παραπλάνηση των πρωτοκόλλων/αλγορίθμων ελέγχου και στην πρόκληση σύγχυσης και μη ορθής λειτουργίας του

δικτύου και, τέλος, μπορεί να επαληθευθεί η αυθεντικότητα των κόμβων που συμμετέχουν στις ad hoc επικοινωνίες.

Στη συνέχεια, προτείνουμε το επίπεδο του μεσισμικού να προστατεύει το δίκτυο με συνεργατικές διαδικασίες και πρωτόκολλα, δηλαδή με κατανεμημένα σχήματα που βασίζονται στην ανταλλαγή μηνυμάτων (όπως ψήφους, γνώμες, συστάσεις, συναγερμούς, μαύρες λίστες, μερικά κλειδιά σε σχήματα κρυπτογράφησης κατωφλίου κ.α.). Έτσι η ανίχνευση και η απομόνωση των κακόβουλων κόμβων μπορεί να επιτευχθεί με λειτουργίες που τρέχουν στο στρώμα του μεσισμικού. Οι λόγοι για τους οποίους προτιμούμε μια τέτοια σχεδίαση δίνονται παρακάτω.

Κατά πρώτον, οι λειτουργίες και οι υπηρεσίες που παρέχονται στο στρώμα του ad hoc μεσισμικού είναι από άκρη σε άκρη. Αυτό πολλές φορές απαιτεί οι κόμβοι να διαθέτουν πληροφορία που αφορά την ασφάλεια του δικτύου συνολικά, δηλαδή να έχουν αντίληψη όχι μόνο για τη γειτονιά τους (δεδομένα κίνησης, τοπολογία, δικτυακή συμπεριφορά των γειτόνων) αλλά και για τους απομακρυσμένους κόμβους που δεν μπορούν να ελέγξουν άμεσα. Είναι σαφές ότι σε μια τέτοια περίπτωση η τοπική και μόνο πληροφορία είναι ανεπαρκής και άρα χρειάζεται και η γνώμη και συνεργασία των υπολοίπων κόμβων για τη διασφάλιση του δικτύου στο επίπεδο αυτό.

Κατά δεύτερον, τα κατανεμημένα συνεργατικά μοντέλα ταιριάζουν καλύτερα με την κατανεμημένη και ομότιμη αρχιτεκτονική των τεχνολογιών και πλαισίων που συναντάμε στο επίπεδο του ad hoc μεσισμικού.

Κατά τρίτον, είναι επιθυμητό η επιβάρυνση που προκαλούν οι διεργασίες ασφάλειας που τρέχουν στους κόμβους να είναι η ελάχιστη δυνατή προκειμένου να διαφυλάσσονται τα αποθέματα των περιορισμένων ad hoc πόρων (κυρίως η ενέργεια των κόμβων). Κατά τη γνώμη μας η σωστή σχεδίαση των κατανεμημένων σχημάτων που βασίζονται σε συνεργατικά σχήματα μπορεί να έχει βελτιωμένη επιβάρυνση σε σχέση με πολλά αποδεδειγμένα “βαριά” κρυπτοσυστήματα (όπως είναι οι ψηφιακές υπογραφές, οι ασύμμετροι αλγόριθμοι κρυπτογράφησης, η εγκατάσταση αρχών πιστοποίησης και γνωστών πιστοποιητικών κ.α.) τα οποία πολλές φορές έχουν αποδειχθεί απαγορευτικά για το ad hoc περιβάλλον.

Περαιτέρω, στη διαστρωματική σχεδίαση προτείνουμε η προστασία των εφαρμογών τελικού χρήστη να επιτυγχάνεται με βάση τις υπηρεσίες ασφάλειας που παρέχονται από το στρώμα του ad hoc μεσισμικού. Έτσι αν οι συνεργατικές διαδικασίες του μεσισμικού δώσουν ένα αρνητικό αποτέλεσμα/απόφαση όσον αφορά έναν ύποπτο κόμβο θα πρέπει οι διαδικασίες ασφάλειας στο ανώτερο επίπεδο των εφαρμογών να ενημερώνονται διαδραστικά με διαστρωματικό τρόπο και να λαμβάνουν τα απαραίτητα μέτρα. Έτσι σε μια τέτοια περίπτωση οι μηχανισμοί ασφάλειας στο ανώτερο επίπεδο πρέπει να προβαίνουν σε περαιτέρω ενέργειες, όπως για παράδειγμα την ισχυρότερη αυθεντικοποίηση του υπόπτου (με αποστολή αιτήματος αυθεντικοποίησης προς αυτόν και έλεγχο της απάντησής του), την αναγνώριση της ταυτότητάς του, την καταγραφή του σε κατάλληλες λίστες, την καταγραφή του τύπου και του χρόνου της επίθεσης που εξαπέλυσε και τον έγκαιρο αποκλεισμό του από τις επικοινωνίες της εφαρμογής.

4.3. ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] A. Patcha, J.-M. Park. “An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends”. In: Computer Networks 51 (2007), pp. 3448-3470.

[2] Asad Amir Pirzada and Chris McDonald. “Detecting and Evading Wormholes in Mobile Ad Hoc Wireless Networks”. In: International Journal of Network Security Vol.3, No.2, PP. 191-202, Sept. 2006.

[3] D. Roy, R. Chaki, N. Chaki. “A New Cluster-based Wormhole Intrusion Detection Algorithm for Mobile Ad Hoc Networks”. In: International Journal of Network Security and its Applications (IJNSA), Vol.1, No.1, April 2009.

[4] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, Y. Nemoto. “Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method”. International Journal of Network Security Vol.5, No.3, PP.338-346, Nov. 2007.

[5] D. Cerri, A. Ghioni. “Securing AODV: The A-SAODV Secure Routing Prototype”. IEEE Communications Magazine, Vol. 46, No 2, February 2008.

[6] A. Pirzada and Chris McDonald. “Trusted Greedy Perimeter Stateless Routing”, In: 15th IEEE International Conference on Networks (ICON2007), Adelaide, Australia, November 2007, pp. 206-211.

[7] J. Newsome, E. Shi, D. Song, A. Prrig. “The Sybil Attack in Sensor Networks: Analysis & Defences”. In: Proceedings of ISPN’04, April 2004, Berkeley, California, USA.

[8] A. Mishra, K. Nadkarni, and A. Patcha, “Intrusion detection in wireless ad hoc networks,” IEEE Wireless Communications, vol. 11, no. 1, pp. 48–60, February 2004.

[9] V. Bhuse and A. Gupta, “Anomaly intrusion detection in wireless sensor networks,” Journal of High Speed Networks, vol. 15, no. 1, pp. 33–51, 2006. Non-coop

[10] C. E. Loo, M. Y. Ng, C. Leckie, and M. Palaniswami, “Intrusion detection for routing attacks in sensor networks,” International Journal of Distributed Sensor Networks, 2005.

[11] Y. Huang, and W. Lee, “A Cooperative Intrusion Detection System for Ad Hoc Networks”, in Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN’03), October (2003), Fairfax, VA, USA, pp. 135-147.

[12] Fang Liu, Xiuzhen Cheng and Dechang Chen. “Insider Attacker Detection in Wireless Sensor Networks”, in INFOCOM 2007. 26th IEEE International Conference on Computer Communications.

[13] Y. Zhang, W. Lee. “Intrusion Detection in Wireless Ad Hoc Networks”. In: Proceedings of the MOBICOM 2000 Boston MA USA.

[14] O. Kachirski, R. Guha, D. Schwartz, S. Stoecklin, and E. Yilmaz, “Casebased agents for packet-level intrusion detection in ad hoc networks”. In: Proceedings of the 17th International Symposium on Computer and Information Sciences, Orlando, FL, October 2002, CRC Press, pp. 315–320.

[15] I. Krontiris, T. Dimitriou and F. C. Freiling, “Towards Intrusion Detection in Wireless Sensor Networks”. In: Proceedings of the 13th European Wireless Conference, Paris, France, April 2007.

[16] Ioanna Stamouli, “Real-time Intrusion Detection for Ad hoc Networks”, Master of Science dissertation, University of Dublin, 2003.

[17] Albers, P., Camp, O., Percher, J-M., Jouga, B., Mé, Ludovic, and Puttini, R. – Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches. In Proceedings of the First International Workshop on Wireless Information Systems (WIS-2002), April 2002.

[18] Y. Zhang, W. Lee, and Y. Huang, “Intrusion Detection Techniques for Mobile Wireless Networks," ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003.

[19] Xiao K., Zheng, J., Wang, X., Xue, X. “A Novel Peer-to-Peer Intrusion Detection System Using Mobile Agent in MANETs”. Sixth International Conference on Parallel and Distributed Computing Applications and Technologies (PDCAT'05).

[20] IETF IDS WG drafts, https://datatracker.ietf.org/drafts/wg/idwg/

[21] Abhijit Deodhar and Ritesh Gujarathi “A Cluster Based Intrusion Detection System for Mobile Ad Hoc Networks” Virginia Polytechnic Institute & State University.

[22] Johnson C. Lee and Victor C. M. Leung. “Key Management Issues in Wireless Sensor Networks. Current Proposals and Future Developments”. IEEE Wireless Communications, October 2007, Vol. 14, Issue 5, pp. 76-83.

[23] “Security in Mobile Ad Hoc Networks: Challenges and Solutions”. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, IEEE Wireless Communications, 2004, pp. 38-47.

[24] “A Design for Secure and Survivable Wireless Sensor Networks”. Y. Qian and K. Lu, IEEE Wireless Communications, 2007, pp. 30-37.

[25] N. Komninos and C. Douligeris. “LIDF: Layered Intrusion Detection Framework in Ad Hoc Networks”. In: Ad Hoc Networks Journal, Elsevier, Volume 7, Issue 1, January 2009, pp. 171-182.

[26] Wong D, N. Paciorek N and Moore D, “Java-based Mobile Agents”. Communications of the ACM, Vol. 42, (3), pp. 92 – 102, 1999.

[27] Vigna G. “Cryptographic Traces for Mobile Agents, Mobile Agent Security”. In Lecture Notes in Computer Science Vol. 1419, Springer-Verlag, pp. 137–153, 1998.

[28] Sander T and Tschudin CF. “Protecting Mobile Agents Against Malicious Hosts”. In: Mobile Agent Security, LNCS Vol.1419, Springer-Verlag, pp. 44–60, 1998.

[29] Kotzanikolaou P, Burmester M, and Chrissikopoulos V. “Secure Transactions with Mobile Agents in Hostile Environments”. In: Proceedings of ACISP 2000, Lecture Notes in Computer Science Vol. 1841, Springer-Verlag, pp. 289–297, 2000.

[30] Lee B, Kim H, and Kim K. “Secure Mobile Agent Using Strong Non-designated Proxy Signature”. In Proceedings of ACISP 2001, Lecture Notes in Computer Science Vol. 2119, Springer-Verlag, pp. 474–486, 2001.

5. ΛΥΣΗ ΟΡΓΑΝΩΣΗΣ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ AD HOC

Προτείνουμε μια *προσαρμοστική λύση αυτο-οργάνωσης* των ad hoc κόμβων στις τυχαία μεταβαλλόμενες συνθήκες του δικτύου. Οι κόμβοι ενός δικτύου ad hoc που δε διαθέτει υποδομή θα πρέπει με ίδια μέσα να αλλάζουν τη δομή τους όταν οι δικτυακές συνθήκες μεταβάλλονται προκειμένου η απόδοση, η διαθεσιμότητα και η προστασία του δικτύου να παραμένει σε υψηλά επίπεδα.

Οι δυναμικές μεταβολές περιλαμβάνουν τυχαία συμβάντα όπως αλλαγή της τοπολογίας λόγω κίνησης των κόμβων (αύξηση του αριθμού των κόμβων σε μια ομάδα λόγω εμφάνισης νέων κόμβων στην περιοχή και μείωση του αριθμού των κόμβων σε μια ομάδα λόγω πτώσης κάποιων κόμβων που δε διαθέτουν αρκετή ενέργεια για να λειτουργήσουν περαιτέρω ή λόγω κίνησης κάποιων κόμβων σε μακρινές περιοχές) ή λόγω της κακής ποιότητας του καναλιού μετάδοσης (πολλά σφάλματα μετάδοσης λόγω εξασθένησης και fading του σήματος) που μπορεί να επιφέρει πτώση δεσμών σε ένα τρέχον μονοπάτι δρομολόγησης.

Η οργάνωση σχετίζεται με πολλές δικτυακές λειτουργίες όπως με την αυτόματη εύρεση και απόδοση μιας διεύθυνσης σε ένα νέο νόμιμο κόμβο ad hoc, την έγκαιρη αλλαγή των πινάκων δρομολόγησης όταν η τοπολογία αλλάζει, τη διαχείριση της συμμετοχής των κόμβων στις συστάδες/ομάδες, την αντικατάσταση των κόμβων-αρχηγών με καταλληλότερους και πιο εύρωστους κόμβους για να επιτελέσουν την προώθηση των μηνυμάτων, τη δημιουργία, την ανταλλαγή, τη διαγραφή και την ανανέωση των κλειδιών κρυπτογράφησης για την ασφάλεια των επικοινωνιών (αυτές οι διαδικασίες απαιτούνται όταν κάποιος κόμβος εγκαταλείπει μια συστάδα/ομάδα), τον εντοπισμό και την παρακολούθηση της θέσης των κόμβων, κ.α.

Οι προσαρμοστικές και μικρού κόστους δικτυακές λύσεις δυναμικής αυτο-οργάνωσης μπορούν να περιορίσουν τις ανεπιθύμητες συνέπειες που μπορεί να έχουν μη αποδοτικοί αλγόριθμοι, όπως την αργή ενημέρωση των κόμβων για τη νέα τοπολογία, τη μη αξιόπιστη παράδοση δεδομένων με απώλεια δεδομένων και καθυστερήσεις, τις συγκρούσεις και τις επαναλήψεις στη μετάδοση δεδομένων και, γενικά, τις αστοχίες και την υποβάθμιση της επίδοσης του δικτύου και της ποιότητας των υπηρεσιών.

5.1. ΑΥΤΟ-ΟΡΓΑΝΩΣΗ ΜΕ ΑΛΓΟΡΙΘΜΟΥΣ ΕΚΛΟΓΗΣ ΑΡΧΗΓΩΝ

Αντικείμενο της έρευνας είναι η βελτίωση της απόδοσης πρωτοκόλλων δρομολόγησης σε δίκτυα ad hoc μεσαίας και μεγάλης κλίμακας με τη χρήση ιεραρχικών δομών (δες και παράγραφο 3.6.3 για μια σύντομη περιγραφή μερικών υφιστάμενων ιεραρχικών ad hoc πρωτοκόλλων).

5.2. ΠΡΟΚΛΗΣΕΙΣ ΣΤΗ ΣΧΕΔΙΑΣΗ ΚΑΙΝΟΤΟΜΩΝ ΑΛΓΟΡΙΘΜΩΝ

Μερικά από τα σημεία-κλειδιά τα οποία καθορίζουν τη σχεδίαση καινοτόμων σχημάτων αυτο-οργάνωσης τα οποία στηρίζονται σε αποδοτικούς αλγόριθμους συσταδοποίησης και εκλογής αρχηγών για το δίκτυο ad hoc δίνονται παρακάτω.

5.2.1. Κατανεμημένα Σχήματα έναντι Κεντρικών Σχημάτων

Σύμφωνα με τις αρχές των κατανεμημένων συστημάτων κατά τη διεργασία της δημιουργίας των ομάδων και της επιλογής των κόμβων-αρχηγών του δικτύου η πληροφορία που λαμβάνεται υπόψη πρωταρχικά είναι τοπικού χαρακτήρα. Δηλαδή, ως αρχηγός εκλέγεται ο καταλληλότερος κόμβος που πληρεί ορισμένες προϋποθέσεις (π.χ. περισσότερη διαθέσιμη ενέργεια από τους υπολοίπους γείτονες), όπως αυτό καθορίζεται από το χρησιμοποιούμενο σχήμα αυτο-οργάνωσης.

Η απαραίτητη πληροφορία για την λήψη απόφασης προκύπτει μετά από τη συλλογή και την επεξεργασία μηνυμάτων που ανταλλάσσουν μεταξύ τους οι γειτονικοί κόμβοι που βρίσκονται σε απόσταση ενός βήματος και το πολύ σε απόσταση δύο βημάτων (hops). Αντίθετα, σε ένα δίκτυο με κεντρικό έλεγχο οι κόμβοι-αρχηγοί επιλέγονται από ένα και μοναδικό κόμβο μετά από επεξεργασία της πληροφορίας που συλλέγεται από όλους τους κόμβους του δικτύου, μια τακτική που καταναλώνει προφανώς περισσότερους πόρους τόσο στους ίδιους τους κόμβους (εφόσον αυξάνεται η κλίμακα της επεξεργασίας) όσο και στο δίκτυο (εφόσον καταναλώνεται περισσότερο εύρος ζώνης για τις απαραίτητες επικοινωνίες με την ανταλλαγή μηνυμάτων, συναγερμών κ.λ.π. από άκρο σε άκρο στο δίκτυο).

Επιπλέον, δεύτερη βασική ιδιότητα των κατανεμημένων συστημάτων είναι ότι ο ίδιος κώδικας (δηλαδή ακριβώς ο ίδιος αλγόριθμος ή μέρος αυτού ανάλογα και με το ρόλο του κόμβου) τρέχει σε όλους τους κόμβους του δικτύου, γεγονός που εγγυάται και τη διεξαγωγή των επικοινωνιών με ομότιμο τρόπο ("peer-to-peer"). Αυτό είναι άλλωστε το βασικό χαρακτηριστικό που διακρίνει τα δίκτυα ad hoc που τείνουν να αυτο-οργανώνονται, δηλαδή η επεξεργασία και ανταλλαγή μηνυμάτων μεταξύ των κόμβων με ομότιμο και συνεργατικό τρόπο. Αντίθετα, σε ένα δίκτυο με κεντρικό έλεγχο ένας είναι ο βασικός κόμβος που διαχειρίζεται (συντονίζει, ερωτά, δίνει πρόσβαση στο ασύρματο κανάλι κ.α.) τους υπολοίπους κατά τρόπο που ομοιάζει με τα μοντέλα "master-slave" ή/και "polling" παρά σύμφωνα με το μοντέλο της αυτό-οργάνωσης και της ανοιχτής επικοινωνίας ομότιμων οντοτήτων.

Προφανώς σε ένα κεντρικό μοντέλο η εξάρτηση ολοκλήρου του δικτύου από ένα και μόνο σημείο αστοχίας ("single point of failure") είναι πολύ πιο έντονη και είναι επόμενο ότι η ανοχή είτε σε βλάβες είτε σε επιθέσεις κατά του κεντρικού αυτού σημείου ελέγχου είναι πολύ μικρή σε αυτά τα συστήματα.

Έτσι μια επίθεση που εκδηλώνεται κατά ενός συστήματος που λαμβάνει κεντρικά τις αποφάσεις έχει ολικό αντίκτυπο για το δίκτυο και, επιπλέον, το βάρος για το φιλτράρισμα της ασφαλούς πληροφορίας είναι πολύ μεγαλύτερο όταν εκτελείται κεντρικά σε έναν κόμβο παρά όταν αυτό κατανέμεται σε όλους τους κόμβους (ή σε μερικούς μόνο κόμβους) και αφορά μόνο το τοπικό επίπεδο.

Είναι εύλογο στην περίπτωση των δικτύων που προστατεύονται με κατανεμημένους αλγόριθμους ανίχνευσης εισβολέων ο χρόνος αντίδρασης στην επίθεση να είναι της τάξης των ολίγων δευτερολέπτων, ενώ αντίθετα στα κεντρικά συστήματα αντιμετώπισης επιθέσεων ο χρόνος αντίδρασης να είναι της τάξης των αρκετών λεπτών.

Ωστόσο, στα κατανεμημένα συστήματα ασφάλειας προκύπτει το πρόβλημα ποιοι από όλους θα πρέπει να είναι οι κόμβοι που θα πρέπει να αποτελούν μέρος του κατανεμημένου συστήματος αυτό-οργάνωσης και κυρίως ποιοι πρέπει να είναι οι κόμβοι του συστήματος που προστατεύει τους υπόλοιπους κόμβους, δηλαδή προκύπτει το ερώτημα πού να τοποθετήσουμε την ασφάλεια σ' ένα κατανεμημένο σύστημα.

Ένα άλλο μειονέκτημα της προσπάθειας αυτό-οργάνωσης με κατανεμημένους αλγορίθμους είναι ότι πιθανά το διαχειριστικό κόστος να αυξάνεται εφόσον απαιτείται επιπλέον ανταλλαγή μηνυμάτων ελέγχου μεταξύ των ομάδων των ομότιμων κόμβων ή μεταξύ των κόμβων μέσα στην ίδια την ομάδα προκειμένου αυτοί να ενημερωθούν για τις τυχόν αλλαγές στο δίκτυο ή/και για να εκλέξουν τους κόμβους αρχηγούς ή/και για να επιλύσουν ένα λάθος δρομολόγησης ή/και να αντιμετωπίσουν μια επίθεση κ.ο.κ.

Το κόστος αυτό θα πρέπει να μειώνει κατά περίσταση η προσεκτική ανάλυση των υποθέσεων που οριοθετούν τα εκάστοτε χαρακτηριστικά του δικτύου και ακόμη η αποδοτική σχεδίαση των πρωτοκόλλων η οποία πρέπει να εστιάζει στη βέλτιστη επιλογή των παραμέτρων και των μέτρων εκτίμησης της επίδοσης των αλγορίθμων και πρωτοκόλλων που προτείνονται, στην

ελαχιστοποίηση του αριθμού των μηνυμάτων ελέγχου που ανταλλάσσονται, στην ανάλυση της ευαισθησίας της επίδοσης του δικτύου σε όλους (κατά το δυνατόν) τους πιθανούς παράγοντες που μπορεί να την επηρεάζουν, κ.ο.κ.

5.2.2. Συγκερασμός μεταξύ Ευρωστίας και Ευστάθειας

Στο περιβάλλον των ασυρμάτων δικτύων ad hoc με περιορισμένους πόρους οι συγκερασμοί ("trade-offs") που μπορούμε να διακρίνουμε είναι πολύπλευροι. Για παράδειγμα, είναι γνωστός ο συγκερασμός μεταξύ της χωρητικότητας του δικτύου (δηλαδή του αριθμού των δυνατών ταυτόχρονων συνομιλιών) και των δυνατών ανεκτών παρεμβολών μεταξύ των χρηστών. Ο συμβιβασμός αυτός αντιμετωπίζεται στη σχεδίαση οποιουδήποτε ασύρματου συστήματος, ιδιαίτερα των κυψελοειδών ασύρματων δικτύων με υποδομή. Επίσης, ένας ακόμη γνωστός συγκερασμός είναι αυτός μεταξύ της ανάγκης για κατανάλωση μικρότερης ενέργειας σε ένα δίκτυο ad hoc και ταυτόχρονα της αυξήσεως του επιπέδου ασφαλείας που παρέχεται στους κόμβους του δικτύου.

Από τη μεριά μας επίσης εστιάζουμε και στο συγκερασμό μεταξύ της ευστάθειας του δικτύου (όπως αυτή προκύπτει από την ευστάθεια των αλγορίθμων ομαδοποίησης) και της ευρωστίας του δικτύου η οποία σχετίζεται ισχυρά με το βαθμό συνεκτικότητας των κόμβων. Η ευστάθεια των αλγορίθμων και των σχημάτων ομαδοποίησης σχετίζεται με το ρυθμό μεταβολής της δικτυακής δομής που οργανώνεται σε δυναμικές ομάδες επηρεάζοντας τη δικτυακή επίδοση. Η συνεκτικότητα του δικτύου αποτελεί κύριο μέτρο της ευρωστίας και της αξιοπιστίας των επικοινωνιών ενός ασυρμάτου δικτύου. Δεδομένου ότι η συνεκτικότητα σε ένα ασύρματο δίκτυο είναι απευθείας συνδεδεμένη με την ισχύ εκπομπής των κόμβων, μας ενδιαφέρει να δούμε τη σχέση ανάμεσα στο επίπεδο της ισχύος εκπομπής των κόμβων και στην ευστάθεια του δικτύου όταν αυτό αυτό-οργανώνεται με διαφορετικούς αλγόριθμους συσταδοποίησης, δηλαδή οργάνωσης των κόμβων σε συστάδες.

Περαιτέρω, μας ενδιαφέρει να συσχετίσουμε τυπικά μέτρα της δικτυακής απόδοσης (όπως είναι η μέση καθυστέρηση μηνυμάτων, η δικτυακή ρυθμοαπόδοση κ.α.) αλλά και εκτεταμένα μέτρα δικτυακής απόδοσης (όπως είναι η αξιόπιστη μετάδοση των μηνυμάτων στις επικοινωνίες εντός μιας συστάδας και μεταξύ των συστάδων του δικτύου, η εν σειρά και χωρίς απώλειες ή/και αλλοιώσεις παράδοση των μηνυμάτων στον τελικό προορισμό και η διαθεσιμότητα των κόμβων του δικτύου) τόσο με την ευστάθεια των σχημάτων ομαδοποίησης που χρησιμοποιούνται από το δίκτυο για την αυτόνομη οργάνωσή του όσο και με τη συνεκτικότητα των κόμβων του δικτύου.

Θα δείξουμε στο κεφάλαιο της αξιολόγησης και σύγκρισης των αλγορίθμων ομαδοποίησης ότι ο προτεινόμενος αλγόριθμος επιλέγει ως δρομολογητές του δικτύου ad hoc τους κόμβους με μεγαλύτερο βαθμό συνεκτικότητας και άρα επιτυγχάνει μεγαλύτερη ευρωστία στις επικοινωνίες (δηλαδή μικρότερες απώλειες πακέτων και μεγαλύτερο ποσοστό παράδοσης των πακέτων που φθάνουν στον τελικό προορισμό). Το τίμημα όμως είναι μια αύξηση του εύρους ζώνης που καταναλώνεται λόγω αύξησης του ρυθμού μεταβολής των κόμβων-αρχηγών που επιλέγονται από τον αλγόριθμο αυτόν. Η αύξηση αυτή όμως ισχύει για μια περιοχή μόνο των τιμών της ισχύος που εκπέμπεται από τους ασύρματους κόμβους οι οποίοι εφαρμόζουν τον προτεινόμενο αλγόριθμο.

5.2.3. Ανθεκτικότητα στις Επιθέσεις

Η προστασία από τις επιθέσεις θα πρέπει να είναι αναπόσπαστο στοιχείο των καινοτόμων αλγορίθμων clustering. Το ζήτημα της ασφάλειας στους αλγόριθμους clustering παραμένει ένα ανοιχτό πρόβλημα.

Το πώς όμως ικανοποιείται η απαίτηση της ασφάλειας έναντι των πιθανών επιθέσεων στα δίκτυα ad hoc όταν αυτά οργανώνονται με σχήματα clustering απαιτεί κάποια διευκρίνιση. Ένα σχήμα

clustering αρχικά χρησιμοποιείται για την οργάνωση του δικτύου ad hoc.Ωστόσο, είναι δυνατόν να χρησιμοποιηθεί και για την ασφάλεια και την προστασία του δικτύου από τις επιθέσεις λειτουργώντας σα σύστημα αντιμετώπισης των επιθέσεων (IDS) με το να δίνει στους εκλεγμένους κόμβους-αρχηγούς το ρόλο της ανίχνευσης των κακόβουλων κόμβων.

Επομένως, στην απλούστερη των περιπτώσεων, το σύστημα των εκλεγμένων αρχηγών θα πρέπει να ανιχνεύει τις επιθέσεις υπεξαίρεσης που εκδηλώνονται από κακόβουλους κόμβους (εσωτερικούς είτε εξωτερικούς, δες και §3.7.2) κατά των δεδομένων και των μηνυμάτων ελέγχων που διακινούνται στο δίκτυο. Ένα τέτοιο σχήμα θα πρέπει να μπορεί, αν είναι αναγκαίο, να κωδικοποιεί κατάλληλα τα μηνύματα που ανταλλάσσουν οι χρήστες εντός των cluster ή μεταξύ των clusters.

Ακόμη ένα τέτοιο σχήμα θα πρέπει να μπορεί να ανιχνεύει τους κακόβουλους χρήστες που παρεμβάλλονται σαν εσωτερικοί κόμβοι στα μονοπάτια δρομολόγησης και οι οποίοι επιτίθενται στο επίπεδο του δικτύου με το να απορρίπτουν τα πακέτα που λαμβάνουν από τους υπολοίπους κόμβους.

Κυρίως όμως ένα καινοτόμο σχήμα clustering που λειτουργεί σαν IDS σε ένα δίκτυο ad hoc θα πρέπει να αυτό-προστατεύεται έτσι ώστε να υπάρχει ανοχή σε επιθέσεις κατά των ίδιων των κόμβων-αρχηγών, δηλαδή τελικά να εξασφαλίζεται η προστασία του ίδιου του συστήματος ασφαλείας από τους κακόβουλους κόμβους οι οποίοι καμουφλαρισμένοι σαν νόμιμοι εσωτερικοί κόμβοι του δικτύου θα προσπαθήσουν να το συμβιβάσουν. Σε ένα σχήμα εκλογής αρχηγών είναι εύκολο να επιτευχθεί συμβιβασμός με την υπονόμευση της διαδικασίας εκλογής των αρχηγών. Είναι εύκολο στο ανοιχτό ασύρματο μέσο οι κακόβουλοι κόμβοι να διαφημίσουν στους γειτονικούς τους κόμβους ψευδείς τιμές των παραμέτρων που λαμβάνονται υπόψη στην επιλογή των κόμβων-αρχηγών, όπως ψευδή αριθμό γειτόνων, ή ψευδή γεωγραφική θέση μέσα στο δίκτυο, ή ψευδώς μεγάλο απόθεμα ενέργειας με αποτέλεσμα να αλλοιώνεται η σύνθεση της ιεραρχικής δομής μέσα στο δίκτυο.

Επομένως τονίζουμε την απαίτηση ο αλγόριθμος συσταδοποίησης να είναι ασφαλής έτσι ώστε να μην εκλέγεται σαν κόμβος-αρχηγός κάποιος συμβιβασμένος κόμβος γιατί τότε θα έχει υπονομευτεί σε μεγάλο βαθμό ολόκληρο το δίκτυο.

5.2.4. Εξειδικευμένα Σχήματα Εκλογής Αρχηγών στα Δίκτυα Ad Hoc

Κάθε αλγόριθμος εκλογής αρχηγών θα πρέπει να είναι ικανός να εκλέξει τελικά έναν αρχηγό ή ένα σύνολο από κόμβους-αρχηγούς, εφόσον μιλάμε για μια ιεραρχική δομή μέσα στο δίκτυο ad hoc. Για την εφαρμογή των αλγορίθμων αυτών στο δίκτυο ad hoc που έχει κόμβους περιορισμένης χωρητικότητας (capacity) απαιτούνται επιπλέον χαρακτηριστικά και περαιτέρω προσαρμογή στις επικρατούσες συνθήκες ώστε οι αλγόριθμοι οργάνωσης με την εκλογή αρχηγού να είναι πραγματικά αποδοτικοί.

Οι πρόσθετες προϋποθέσεις και απαιτήσεις που θα πρέπει να τηρούνται από τους αλγόριθμους εκλογής αρχηγών στα MANET, WSN, VANET και Mesh είναι οι εξής:

- Ο αλγόριθμος εκλογής αρχηγού *πρέπει να τερματίζει* δίνοντας μοναδικό αποτέλεσμα για τον προτεινόμενο αρχηγό/αρχηγούς.

- Ο αρχηγός που επιλέγεται θα πρέπει να ικανοποιεί ένα *κριτήριο ακροτάτου*, δηλαδή ανάμεσα στους υποψήφιους να είναι αυτός που έχει τη μέγιστη τιμή μιας μεταβλητής που χαρακτηρίζει την ευρωστία των κόμβων, για παράδειγμα να έχει μέγιστα υπολογιστικά και ενεργειακά αποθέματα, ή ελάχιστη απόσταση από τους υπολοίπους, ή μικρή σχετική ταχύτητα, ή κάποιο συνδυασμό αυτών, κ.α.

- Ο αλγόριθμος πρέπει να είναι *αποδοτικός*, τόσο από πλευράς της απαιτούμενης υπολογιστικής πολυπλοκότητας όσο και από πλευράς του αριθμού των μηνυμάτων ελέγχου που απαιτείται να στείλει προς το δίκτυο πριν φθάσει σε μια σταθερή κατάσταση.

- Οι αποφάσεις που λαμβάνονται πρέπει να είναι *τοπικού χαρακτήρα*. Το γνώρισμα αυτό το έχουμε αναλύσει επαρκώς μέχρι τώρα στην §5.2.1.

- Ο αλγόριθμος πρέπει να είναι *ανεκτικός σε τυχαία σφάλματα* ("fault tolerant"), όπως είδαμε στα χαρακτηριστικά των αυτόνομων δικτύων στην §2.2.5.

- Το σχήμα εκλογής αρχηγών πρέπει να είναι *ανεκτικό σε επιθέσεις* που εκδηλώνονται από κακόβουλους κόμβους. Η νέα πρόκληση είναι τα σχήματα αυτο-οργάνωσης να είναι ανθεκτικά στις επιθέσεις και ιδιαίτερα στις επιθέσεις από εσωτερικούς εισβολείς ("intruders"), γεγονός το οποίο οδηγεί σε πολλές περαιτέρω απαιτήσεις. Μια από αυτές είναι οι αλγόριθμοι εκλογής αρχηγών να είναι *συνεπείς ("consistent")* ως προς το τελικό τους αποτέλεσμα.

  Στα κατανεμημένα συστήματα η εκλογή μιας οντότητας-διεργασίας ως συντονιστή των υπολοίπων οντοτήτων διατηρεί την αρχή της ακεραιότητας ("integrity") και της συνέπειας όταν το τελικό αποτέλεσμα δεν αντιβαίνει με τη γνώμη της πλειοψηφίας. Το ίδιο μπορεί να βρει εφαρμογή και στα δίκτυα ad hoc όπου μπορούμε να υιοθετήσουμε κριτήρια πλειοψηφίας στους αλγορίθμους "clustering" για να αποφανθούμε αν κάποιος κόμβος μπορεί να επιλεγεί ως τοπικός κόμβος-αρχηγός, ή αν είναι εισβολέας ο οποίος προσπαθεί να συμβιβάσει τον κόμβο-αρχηγό.

  Το ζήτημα της ασφάλειας στους αλγόριθμους συσταδοποίησης θα αναλυθεί στο Κεφάλαιο 6. Σύμφωνα με το σχήμα που προτείνουμε στο Κεφάλαιο 6 η ακεραιότητα είναι μία πρωταρχικής σημασίας απαίτηση και κατηγοριοποιούμε με βάση αυτήν τους κόμβους σε νόμιμους και υπόπτους. Οι ύποπτοι υφίστανται περαιτέρω διαδοχικούς ελέγχους (για παράδειγμα δεύτερη αυθεντικοποίηση) μέχρι να αποφασιστεί ο πλήρης αποκλεισμός τους από τις επικοινωνίες του δικτύου ή όχι.

5.3. ΠΑΡΑΓΟΝΤΕΣ ΕΠΙΔΟΣΗΣ ΤΩΝ ΑΛΓΟΡΙΘΜΩΝ ΣΥΣΤΑΔΟΠΟΙΗΣΗΣ

Μας ενδιαφέρει αρχικά να εντοπίσουμε εκείνους τους παράγοντες που επιφέρουν σημαντικό αντίκτυπο στην επίδοση των αλγορίθμων ομαδοποίησης. Ονομάζουμε αυτούς τους παράγοντες παράγοντες επίδοσης. Οι παράγοντες επίδοσης διαμορφώνουν τις ad hoc δικτυακές συνθήκες τις οποίες θα εξομοιώσουμε στον προσομοιωτή δικτύων JNS [27]. Θεωρούμε ότι οι βασικότεροι παράγοντες που επηρεάζουν σε σημαντικό βαθμό την επίδοση των αλγορίθμων ομαδοποίησης και εκλογής αρχηγών είναι οι εξής:

- Η τοπολογία του δικτύου ad hoc και ο βαθμός συνεκτικότητας των κόμβων.

- Το μοντέλο κίνησης των κόμβων.

- Το μοντέλο κατανάλωσης ενέργειας στους κόμβους.

- Το μοντέλο εκπομπής ισχύος των ασύρματων κόμβων.

Το αποτέλεσμα της αυτο-οργάνωσης των κόμβων με ένα αλγόριθμο ομαδοποίησης πολλές φορές είναι μια δομή παροδική και η διαδικασία της οργάνωσης θα πρέπει να επαναλαμβάνεται επειδή τα δίκτυα ad hoc είναι πολύ δυναμικά. Αυτό επιβαρύνει τις ωφέλιμες επικοινωνίες του δικτύου. Με τον εντοπισμό, τον έλεγχο και τη βέλτιστη παραμετροποίηση των παραγόντων επίδοσης είναι δυνατόν

να σχεδιάσουμε καλύτερα τους προτεινόμενους αλγόριθμους και συνεπώς να μειώσουμε το διαχειριστικό κόστος που απαιτείται για την υποστήριξη των ιεραρχικών δομών που αλλάζουν μέσα στο δίκτυο ad hoc.

5.3.1. Το Μοντέλο Τοποθέτησης των Ασύρματων Κόμβων

Η μελέτη του παράγοντα επίδοσης της ad hoc τοπολογίας στην εργασία αυτή κατ' αρχήν αποσκοπεί στη διερεύνηση του ρόλου των γεννητριών τυχαίων τοπολογιών στα πειράματα προσομοίωσης για την εκτίμηση των νέων αλγορίθμων και πρωτοκόλλων στα ασύρματα δίκτυα ad hoc. Ειδικότερα, θα δοκιμαστούν νέα μοντέλα τοπολογιών που παράγονται από γεννήτριες τυχαίων γράφων και τα οποία προσομοιώνουν με μεγαλύτερη ακρίβεια τις τοπολογίες των νέων αρχιτεκτονικών των δικτύων ad hoc, όπως για παράδειγμα τις ιεραρχικές δομές δικτύων ad hoc μεγάλης κλίμακας και τα ασύρματα δίκτυα πλέγματος.

Από την πλευρά μας, επίσης εστιάζουμε σε δίκτυα μεγάλης κλίμακας επειδή αναπτύσσονται ραγδαία μοντέρνες ad hoc εφαρμογές όπως βιομηχανικές, στρατιωτικές κ.α. που απαιτούν τη συμμετοχή πολλών κόμβων με πολλαπλούς ρόλους και με μεγάλη πυκνότητα δικτύου.

Σαν δίκτυα μεγάλης κλίμακας θεωρούμε αυτά με πάνω από 1.000 (μέχρι και 5.000) συνδεδεμένους κόμβους. Είναι επομένως απαραίτητη η σχεδίαση αποδοτικών δικτυακών αλγορίθμων με ικανότητα κλιμάκωσης σε μεγάλο αριθμό κόμβων καθώς και η εξεύρεση τεχνικών, πρωτοκόλλων και κυρίως μοντέλων και αρχιτεκτονικών που να είναι περισσότερο συμβατές με τα ιδιαίτερα χαρακτηριστικά των κόμβων ad hoc οι οποίοι έχουν περιορισμένους ενεργειακούς, υπολογιστικούς και επικοινωνιακούς πόρους. Με αυτό τον τρόπο μπορούμε να επιτύχουμε τα δίκτυα ad hoc να είναι εύρωστα και με μεγάλο ποσοστό διαθεσιμότητας των υπηρεσιών που προσφέρουν.

Ειδικότερα, θα ερευνηθεί ο αντίκτυπος των τοπολογικών χαρακτηριστικών των δικτύων ad hoc μεγάλης κλίμακας στην απόδοση των αλγορίθμων συσταδοποίησης καθώς και η επίδραση των πιθανών μοντέλων τοποθέτησης των κόμβων στο χρόνο ζωής και στην επίδοση του δικτύου.

5.3.1.1. Το Πρόβλημα

Για τα δίκτυα ad hoc (MANET και ιδιαίτερα τα δίκτυα αισθητήρων WSN) η αυτο-οργάνωσή τους εξαρτάται άμεσα από τον τρόπο με τον οποίο αναπτύσσονται τα δίκτυα αυτά και ιδιαίτερα από τον τρόπο με τον οποίο διαμορφώνεται η τοπολογία τους στο επίπεδο/χώρο. Πολλές είναι οι εργασίες που μελετούν το βέλτιστο τρόπο τοποθέτησης και ανάπτυξης των κόμβων στο επίπεδο / χώρο και ακόμη περισσότερες είναι οι εργασίες που αφορούν τους αλγορίθμους ελέγχου της τοπολογίας των δικτύων ad hoc και ιδιαίτερα των δικτύων αισθητήρων [1], [2], [3]. Ενδεικτικά αναφέρουμε ότι η τοποθέτηση των κόμβων μπορεί να γίνεται με εντελώς τυχαίο τρόπο ή να εμφανίζει συγκεντρώσεις ομάδων είτε να σχηματίζει ένα εντελώς συμμετρικό πλέγμα ή ακόμη να γίνεται και με σπειροειδή ή κυκλικό τρόπο.

Σε μία από κάτω προς τα πάνω προσέγγιση της ad hoc αρχιτεκτονικής το πρώτο επίπεδο που συναντάμε προς διερεύνηση είναι αυτό των αλγορίθμων που λαμβάνουν υπόψη την τοπολογία των ad hoc δικτύων. Σε ένα ενσύρματο δίκτυο η τοπολογία καθορίζει την αρχιτεκτονική του. Στην περίπτωση όμως των ασύρματων δικτύων με κινούμενους κόμβους οι τοπολογίες είναι δυναμικές και η έγκαιρη σύγκλιση των αλγορίθμων με γρήγορη ανανέωση της πληροφορίας για τη δικτυακή τοπολογία θα πρέπει να παίζει ένα πολύ σημαντικό ρόλο στη σχεδίαση και την διαχείριση των δικτύων ad hoc. Από την πλευρά μας οι ad hoc τοπολογίες θα μας απασχολήσουν κατά δύο τρόπους.

Σε πρώτη φάση διερευνούμε το ρόλο του μοντέλου ανάπτυξης και τοποθέτησης των ad hoc κόμβων στα πρωτόκολλα ad hoc. Ειδικότερα, για τα ημι-στατικά δίκτυα Wireless Sensor Networks

μας ενδιαφέρει να μελετήσουμε τα χαρακτηριστικά των βέλτιστων μοντέλων τοποθέτησης των κόμβων στο πεδίο και την επίδραση των διαφορετικών μοντέλων ανάπτυξης των κόμβων στη δικτυακή απόδοση των αλγορίθμων. Τα χαρακτηριστικά αυτά περιγράφονται αναλυτικά από τα μοντέλα που περιγράφουν τις στατιστικές ιδιότητες των δικτυακών τοπολογιών που έχουν παρατηρηθεί μέχρι τώρα. Από όλα τα υπάρχοντα μοντέλα μερικά μόνο είναι κατάλληλα για την ορθή μοντελοποίηση των δικτύων ad hoc, ενώ άλλα είναι πιο κατάλληλα για τη μοντελοποίηση τοπολογιών που συναντάμε στο Διαδίκτυο, το οποίο χαρακτηρίζεται από πολύ μεγάλη κλίμακα, από ισχυρούς δρομολογητές συγκέντρωσης της κίνησης και από αυτόνομα διαχειριστικά συστήματα (“autonomous systems”).

Συνεπώς, πρωταρχικός μας στόχος είναι να εντοπίσουμε και να απομονώσουμε εκείνες τις παραμέτρους και μεταβλητές καθώς και εκείνα τα μοντέλα των τοπολογιών τα οποία μπορεί να αποδειχθούν ως τα πιο χρήσιμα στη αποδοτική σχεδίαση και τη διαχείριση των δικτύων ad hoc μεγάλης κλίμακας.

Από τη μεριά μας κάναμε χρήση των κατάλληλων μοντέλων τυχαίων γράφων για να μελετήσουμε αναλυτικά τα δυνατά χαρακτηριστικά της μορφολογίας ενός δικτύου ad hoc. Θα διαπιστώσουμε ότι χωρίς ακόμη να έχουμε κάνει αναφορά σε στοίβες πρωτοκόλλων, αλγόριθμους και μετρικά που σχετίζονται με την επίδοση ανώτερων επιπέδων στην αρχιτεκτονική των δικτύων, οι παράγοντες που σχετίζονται με την τοπολογία στο φυσικό επίπεδο είναι ικανοί από μόνοι τους να χαρακτηρίσουν το βαθμό συνεκτικότητας, το ποσοστό κάλυψης και άρα την ποιότητα των επικοινωνιών που μπορεί να επιτευχθεί για ένα σύνολο από δικτυακές οντότητες.

Μελετήσαμε με πειράματα προσομοίωσης ποια είναι η επίδραση δύο βασικών μοντέλων τοποθέτησης των κόμβων (“heavy tail” και “uniform”) στην επίδοση πρωτοκόλλων και αλγορίθμων που βρίσκονται σε ανώτερα επίπεδα της αρχιτεκτονικής του δικτύου ad hoc και ιδιαίτερα στο επίπεδο του δικτύου (όπου συναντάμε τα πρωτόκολλα δρομολόγησης) και στο επίπεδο της εφαρμογής (όπου συναντάμε τις πηγές της δικτυακής κίνησης, τις εφαρμογές οργάνωσης των κόμβων σε ομάδες με τους αλγορίθμους ομαδοποίησης και τις διαδικασίες ανακάλυψης και επίκλησης των υπηρεσιών των δικτύων). Ειδικότερα, μας ενδιαφέρει να ερευνήσουμε ποια είναι η επίδραση της θέσης των κόμβων στην επίδοση των αλγορίθμων ομαδοποίησης των κόμβων σε συστάδες-ομάδες (clusters), ποια είναι η επίδραση των ad hoc μορφολογιών στην κατανάλωση των πόρων των κόμβων και των πόρων του δικτύου – ισοδύναμα και στο χρόνο ζωής του δικτύου – και πώς οι δύο αυτοί διαφορετικοί τύποι τυχαίων τοπολογιών (“heavy tail” και “uniform”) μπορούν να επηρεάσουν την αξιόπιστη μεταφορά των δεδομένων από την πηγή προς τον προορισμό. Τα πειραματικά αποτελέσματα θα παρουσιαστούν στο επόμενο Κεφάλαιο.

Σε δεύτερη φάση, οι τοπολογίες των κόμβων θα μας απασχολήσουν στη σχεδίαση προσαρμοστικών και ασφαλών πρωτοκόλλων δρομολόγησης ad hoc. Ειδικότερα, θα διερευνήσουμε πρωτόκολλα δρομολόγησης που λαμβάνουν υπόψη τη θέση των κόμβων για τη λήψη της απόφασης δρομολόγησης πακέτων και επίσης λαμβάνουν υπόψη και την κίνηση των κόμβων στο χώρο. Ένα παράδειγμα τέτοιων πρωτοκόλλων είναι τα ad hoc γεωγραφικά πρωτόκολλα δρομολόγησης τα οποία θεωρήσαμε ότι με κατάλληλες προσαρμογές και επεκτάσεις μπορούν να ικανοποιήσουν πολλές από τις απαιτήσεις λειτουργικότητας και, κυρίως, ασφαλείας που θέσαμε στο Κεφάλαιο 2.

Έτσι σε ένα πρώτο στάδιο μας ενδιαφέρει να εντοπίσουμε ποια είναι τα μοντέλα των τοπολογιών που μπορούν να μοντελοποιήσουν καλύτερα τα δίκτυα ad hoc και ιδιαιτέρως αυτά τα δίκτυα που είναι μεγάλης κλίμακας (1.000-10.000 κόμβοι) και ακόμη και ποια είναι τα μέτρα που σχετίζονται με τις τοπολογίες των δικτύων και τα οποία επηρεάζουν την απόδοση των δικτύων έτσι ώστε να πρέπει να τα λάβουμε υπόψη στην εκτίμηση των προτεινόμενων δικτυακών λύσεων και στη διεξαγωγή των πειραμάτων με τα εργαλεία εξομοίωσης.

5.3.1.2. Τοπολογικές Παράμετροι

Ας περιγράψουμε όμως πρώτα τις πιο αντιπροσωπευτικές παραμέτρους (“affinity metrics”) που περιγράφουν με αναλυτικό τρόπο το βαθμό ομαδοποίησης των κόμβων σε μια τοπολογία από ακμές και κορυφές (σε ένα γράφο δηλαδή) τα οποία θα μας βοηθήσουν να μοντελοποιήσουμε με διαφορετικές κατανομές την τοποθέτηση και την ανάπτυξη των πραγματικών κόμβων μέσα στα δίκτυα ad hoc.

Οι παράμετροι/μέτρα με τις οποίες μπορούμε να χαρακτηρίσουμε μια τοπολογία κόμβων μπορούν να ανήκουν σε μια από τις παρακάτω περιγραφόμενες κατηγορίες.

5.3.1.2.1. Παράμετροι Μονοπατιού

Το χαρακτηριστικό μήκος μονοπατιού (*characteristic path length*, cpl_G) ενός συνδεδεμένου γραφήματος δικτύου *G* που αποτελείται από *N* κόμβους είναι το μέσο μήκος μονοπατιού για όλα τα ζεύγη κόμβων του δικτύου. Δηλαδή:

$$cpl_G = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} d_{ij}}{N(N-1)} \quad (1)$$

όπου d_{ij} είναι η απόσταση μεταξύ δύο κόμβων *i* και *j*.

Η διάμετρος D ενός δικτύου ορίζεται ως το μέσο μήκος των βραχύτερων μονοπατιών μεταξύ όλων των ζευγών των κόμβων του γράφου. Ένα πακέτο δεν επιτρέπεται να περιφέρεται στο δίκτυο για έναν αριθμό από βήματα μεγαλύτερο της διαμέτρου του δικτύου *D*. Αξίζει να σημειωθεί ότι η διάμετρος αποτελεί αξιόπιστο δείγμα της συνεκτικότητας του δικτύου και είναι μάλιστα ανεξάρτητη του μεγέθους του δικτύου. Έτσι έχει βρεθεί ότι πολύ μεγάλα κοινωνικά δίκτυα με πληθυσμό έξι δισεκατομμυρίων ατόμων έχουν διάμετρο κοντά στο έξι, ενώ η διάμετρος του WWW των 800 εκατομμυρίων κόμβων εμπειρικά βρέθηκε ίση με 19.

Το ελάχιστο μήκος μονοπατιού είναι το μήκος σε βήματα του βραχύτερου μονοπατιού από ένα κόμβο πηγή προς ένα κόμβο προορισμό.

5.3.1.2.2. Παράμετροι Ομαδοποίησης

Ο συντελεστής συγκέντρωσης λ μίας ομάδας S από M κόμβους ο οποίος ισούται με:

$$\lambda = \frac{cpl_S}{cpl_G} \quad (2)$$

Όπου cpl_G είναι το χαρακτηριστικό μήκος μονοπατιού του γράφου G και cpl_S είναι το χαρακτηριστικό μήκος μονοπατιού της ομάδας κόμβων S. Όταν μια ομάδα κόμβων S παρουσιάζει μεγάλο βαθμό συγκέντρωσης το λ είναι μικρό αφού και το cpl_S είναι μικρό. Όσο οι κόμβοι της ομάδας S απομακρύνονται τότε το λ αυξάνεται.

Ο συντελεστής *ρ*. Δεδομένης μιας ομάδας S από M κόμβους εντός του γραφήματος G, ο συντελεστής *ρ* ισούται με τον αριθμό L_s των μονοπατιών εντός της ομάδας S που έχουν μήκος μεγαλύτερο από το χαρακτηριστικό μήκος μονοπατιού του γράφου G (cpl_G), διαιρούμενο με το συνολικό αριθμό των μονοπατιών για όλα τα ζεύγη κόμβων της ομάδας S:

$$\rho = \frac{2L_S}{M(M-1)} \quad (3)$$

Η παράμετρος ομαδοποίησης β χαρακτηρίζει το βαθμό συγκέντρωσης μιας ομάδας S από M κόμβους. Εμπειρικά στο Διαδίκτυο έχουν βρεθεί τιμές του *β* οι οποίες κυμαίνονται μεταξύ -15 και +15. Η τιμή *β*=0 αντιστοιχεί στην ομοιόμορφη κατανομή των κόμβων στο επίπεδο, η τιμή *β*>0 αντιστοιχεί σε πυκνά συγκεντρωμένη ομάδα, ενώ τέλος ένα *β*<0 χαρακτηρίζει το βαθμό απομάκρυνσης μεταξύ των κόμβων της ομάδας στην έκταση του δικτύου. Η πιθανότητα p_i ένας κόμβος *i* να προσκολληθεί στην ομάδα S είναι σύμφωνα με το νόμο "Chuang-Sirbu" [6]:

$$p_i = \frac{a}{(d_{iS})^{\beta}} \quad (4)$$

όπου ο συντελεστής *α* βρίσκεται από τη συνθήκη $\sum_i p_i = 1$ και d_{iS} είναι η ελάχιστη ευκλείδεια απόσταση του κόμβου *i* από το cluster S. Όταν β>0 η πιθανότητα προσκόλλησης στην ομάδα S μεγιστοποιείται όταν η απόσταση d_{iS} είναι μικρή. Συνεπώς με μεγάλη πιθανότητα η υπάρχουσα ομάδα θα δεχτεί νέο μέλος. Αντίθετα, όταν β<0 η πιθανότητα p_i μεγιστοποιείται όταν η απόσταση d_{iS} είναι μεγάλη, περίπτωση κατά την οποία τα μέλη της ομάδας S απομακρύνονται το ένα από το άλλο.

Εναλλακτικά, η παράμετρος ομαδοποίησης *γ(u)* μπορεί να οριστεί σε μια γειτονιά Γ(u) γύρω από μια κορυφή *u* ως ο αριθμός των ακμών που περιλαμβάνουν την κορυφή u στη γειτονιά Γ(u) προς το συνολικό αριθμό των πιθανών ακμών που μπορεί να βρίσκονται στη γειτονιά Γ(u):

$$\gamma(u) = \frac{|E(\Gamma(u))|}{\binom{k_u}{2}} \quad (5)$$

όπου k_u είναι ο αριθμός των γειτόνων του κόμβου u. Ο βαθμός συνεκτικότητας *γ(G)* του γράφου G με κορυφές *u* είναι τότε:

$$\gamma(G) = |V^{-1}| \sum_u \gamma(u), \text{ δεδομένου ότι είναι } k_u \geq 2, \forall u \in V. \quad (6)$$

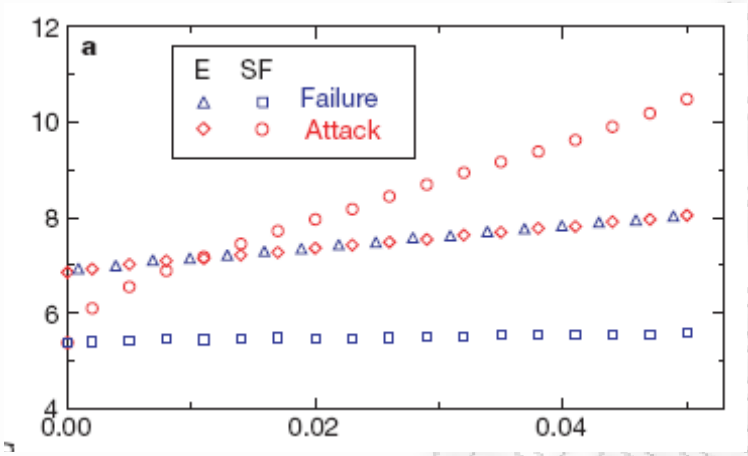
Η παράμετρος κάλυψης χ ισούται με το μέσο αριθμό βημάτων που χρειάζεται ένας κόμβος της ομάδας S για να φτάσει *p%* (κάλυψη για παράδειγμα 50%) από τους κόμβους της ομάδας S προς το μέσο αριθμό βημάτων που χρειάζεται ένας κόμβος του G για να φτάσει *p%* από όλους τους κόμβους του γραφήματος G.

$$\chi = \frac{E_S(50\%)}{E_G(50\%)} \quad (7)$$

Η παράμετρος *χ* αποτελεί ένα μέτρο της δυνατότητας κάλυψης των κόμβων με μικρό αριθμό βημάτων. Είναι γνωστό ότι αυτό στη περίπτωση της δρομολόγησης μηνυμάτων με πολλαπλά βήματα ("multi-hop routing") είναι ένα μέτρο της ποιότητας του μονοπατιού δρομολόγησης ("path optimality").

5.3.1.2.3. Παράμετροι Ευρωστίας

Οι παράμετροι ευρωστίας χαρακτηρίζουν την ανοχή μιας τυχαίας μορφολογίας τόσο στην περίπτωση τυχαίων βλαβών όσο και στις επιθέσεις που έχουν στόχο τους ισχυρούς κόμβους του δικτύου, δηλαδή τους κόμβους εκείνους οι οποίοι έχουν υψηλό βαθμό συνεκτικότητας *d*. Στις εργασίες [8] και [9] αναφέρεται ότι τα δίκτυα όπου η συνεκτικότητα έχει τα χαρακτηριστικά της (τυχαίας) ομοιόμορφης κατανομής έχουν καλό βαθμό ανοχής σε επιθέσεις εφόσον μια επίθεση σε έναν από τους σχεδόν ισοδύναμους κόμβους του δικτύου μπορεί να πλήξει το δίκτυο επιφέροντας το ίδιο σχεδόν (μικρό) αντίκτυπο. Αντίθετα, οι τυχαίες βλάβες των ισοδύναμων κόμβων έχουν καταστροφικό αποτέλεσμα στα ομοιόμορφα (εκθετικά) δίκτυα. Ειδικότερα, η διάμετρος του δικτύου D παρουσιάζει μονοτονική αύξηση με τον αριθμό των κόμβων που τίθενται εκτός λειτουργίας λόγω βλαβών.



Εικόνα 19. Μεταβολή της διαμέτρου *d* των δικτύων "Exponential" (E) και "Scale Free" (SF) ως συνάρτηση του αριθμού των σφαλμάτων στους κόμβους [8].

Η Εικόνα 19 παρουσιάζει τη μεταβολή της διαμέτρου *d* μεγάλων δικτύων όταν αφαιρεθεί ένα ποσοστό *f* κόμβων με τυχαίο τρόπο (μπλε χρώμα) και όταν επιλεκτικά αφαιρεθεί ποσοστό *f* κόμβων που έχουν τη μεγαλύτερη συνεκτικότητα μέσα στο δίκτυο (κόκκινο χρώμα). Συγκρίνονται οι δύο τύποι δικτύων, το εκθετικό δίκτυο (σύμβολα τρίγωνο και διαμάντι) και το ιεραρχικό δίκτυο ("scale free", σύμβολα τετράγωνο και κύκλος).

Για τα δίκτυα ομοιόμορφης (εκθετικής) κατανομής έχουν παρατηρηθεί τιμές κατωφλίων f_c^e (όπου c: "cut-off" και όπου e: "exponential") όσον αφορά το ποσοστό του αριθμού των κόμβων που πρέπει να τεθούν εκτός λειτουργίας πριν το ομοιόμορφο δίκτυο καταστεί μη συνδεδεμένο και καταρρεύσει. Στην περίπτωση κατάρρευσης το εκθετικό δίκτυο διασπάται σε διακριτές ομάδες με μεγάλο αριθμό κόμβων η καθεμιά χωρίς ωστόσο να υπάρχει κάποιο μονοπάτι επικοινωνίας μεταξύ τους.

Τα αντίθετα ισχύουν για την ευρωστία των δικτύων μεγάλης κλίμακας ("Scale Free networks") που χαρακτηρίζονται από την ύπαρξη ιεραρχικών δομών. Για αυτά τα δίκτυα οι τυχαίες βλάβες δεν έχουν σημαντικό αντίκτυπο εφόσον είναι εξίσου πιθανό να τύχουν σε κόμβους με μικρό βαθμό συνεκτικότητας μέσα στο δίκτυο. Συνεπώς δε θα επηρεαστεί σημαντικά και η διαθεσιμότητα του δικτύου, εφόσον πιθανώς κάποιοι μεμονωμένοι μόνο κόμβοι θα εγκαταλείψουν το δίκτυο. Μια μη τυχαία όμως επίθεση από ένα κακόβουλο χρήστη που γνωρίζει την τοπολογία σε ένα ιεραρχικό δίκτυο μεγάλης κλίμακας μπορεί πολύ εύκολα να αποσυνδέσει το δίκτυο, προκαλώντας για παράδειγμα τριπλασιασμό της διαμέτρου *D*, [8]. Ο τρόπος με τον οποίον καταρρέει το δίκτυο μεγάλης κλίμακας μετά από μια στοχευμένη επίθεση σε ένα ποσοστό *f* του συνολικού αριθμού των κόμβων και πάλι κρίνεται από ένα σημείο κατωφλίου f_c^{sf} (όπου c "cut-off" και sf "scale free") πάνω από το οποίο η αρχική τοπολογία θα αποσυνδεθεί σε ένα μεγάλο αριθμό από διακριτές ασύνδετες μεταξύ τους ομάδες και με αυξημένο αριθμό κόμβων η καθεμία.

5.3.1.3. Κατανομές Συνεκτικότητας

Βαθμός συνεκτικότητας *x* των ασύρματων κόμβων. Είναι ο αριθμός *x* των γειτόνων που βρίσκονται εντός της ακτίνας κάλυψης ενός ασύρματου κόμβου (σε απόσταση ενός βήματος).

Η πιο χαρακτηριστική ιδιότητα των τυχαίων τοπολογιών είναι η κατανομή του βαθμού συνεκτικότητας των κόμβων, *P(x)*. Σύμφωνα με θεωρητικά και εμπειρικά αποτελέσματα τα δίκτυα συνήθως ακολουθούν μία από τις παρακάτω κατανομές όσον αφορά το βαθμό συνεκτικότητας των κόμβων τους.

5.3.1.3.1. Κατανομές Εκθετικής Απόληξης

Αυτή είναι η κατανομή *Poisson* η οποία για μεγάλο αριθμό κόμβων τείνει προς την κατανομή ενός ομοιόμορφου δικτύου, δηλαδή όλοι οι κόμβοι τείνουν να έχουν τον ίδιο βαθμό x ≈ E{P(x)}. Παρόμοιες κατανομές ονομάζονται και κατανομές του μοντέλου του μικρού κόσμου ("small world models") οι οποίες ομοιάζουν με την κατανομή που απεικονίζεται στην Εικόνα 20(α). Η εκθετική κατανομή έχει χρησιμοποιηθεί ευρέως στην εξομοίωση της καθυστέρησης των μηνυμάτων σε ένα ad hoc δίκτυο.

5.3.1.3.2. Κατανομές Μακράς Απόληξης

Στην περίπτωση αυτή η κατανομή του βαθμού συνεκτικότητας *x* είναι της μορφής $P(x) \approx x^{-\gamma}$, όπου γ είναι ο συντελεστής σκέδασης της κατανομής, δηλαδή έχουμε μία "heavy tail" κατανομή που ακολουθεί "power laws" [4], [5], [6], [7], [8], [9]. Το κοινό χαρακτηριστικό των κατανομών αυτών είναι ότι η πιθανότητα ένας κόμβος να έχει πολύ μεγάλο βαθμό συνεκτικότητας, δηλαδή η πιθανότητα x >> E{P(x)} είναι μικρή, ενώ η διακύμανση *σ* μιας κατανομής "heavy tail" τείνει στο άπειρο. Αυτές είναι οι κατανομές εκθετικών νόμων του Διαδικτύου όπου ο εκθέτης γ έχει εμπειρικά βρεθεί ίσος με 2.8 [5], του WWW και άλλων μη ομογενών δικτύων πολύ μεγάλης κλίμακας.

Όπως φαίνεται και στην Εικόνα 20(β), σε μια κατανομή μεγάλης κλίμακας (scale free) με συνεκτικότητα που ακολουθεί κατανομή *power law heavy tail* υπάρχουν κόμβοι με μεγαλύτερη στατιστική σημασία από τους υπολοίπους, δηλαδή υπάρχουν κάποιοι κόμβοι στο δίκτυο που συγκεντρώνουν την κίνηση που προέρχεται από τους γειτονικούς κόμβους.

Μια τέτοια heavy tail κατανομή είναι και η κατανομή Pareto με pdf που χαρακτηρίζεται από τον εκθετικό συντελεστή σκέδασης α και την παράμετρο κ, όπως δείχνεται στα παρακάτω παραδείγματα:

$$p(x,k) = ak^{a}x^{-(a+1)} \quad x \geq k \quad a,k > 0. \tag{8}$$

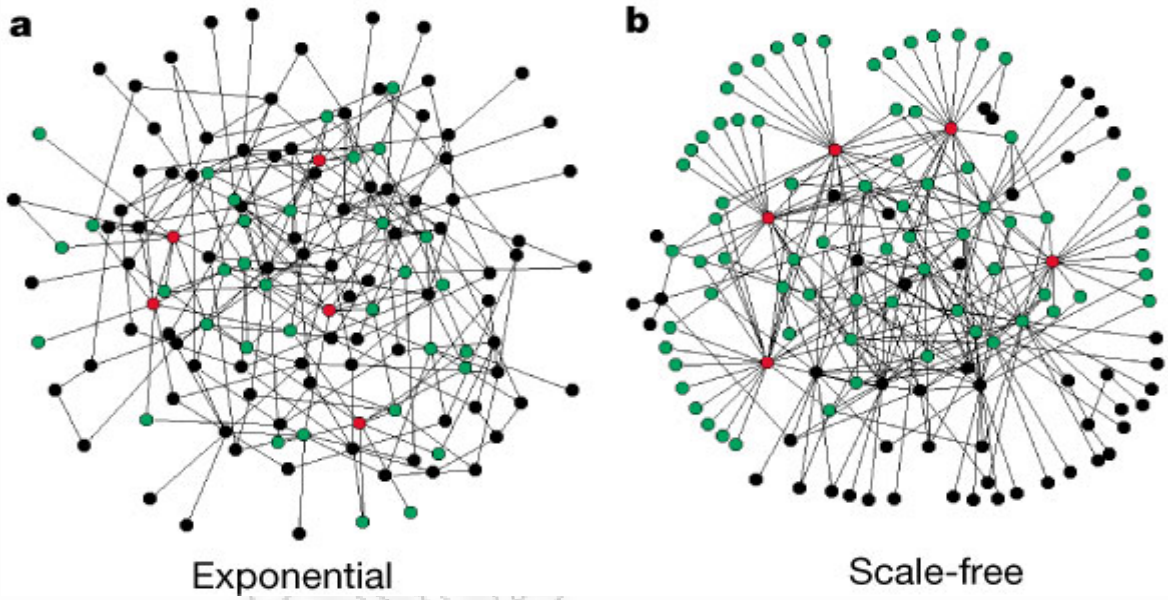
Μια άλλη κατανομή της κατηγορίας "heavy tail" είναι και οι κατανομές *Weibull*.
Παράδειγμα μιας Weibull pdf δείχνεται παρακάτω:

$$p(x) = \frac{bx^{b-1}}{a^{b}} e^{-(x/a)^{b}}. \tag{9}$$

Η συνάρτηση αθροιστικής πιθανότητας (cumulative distribution function, cdf) της κατανομής *Weibull* είναι της μορφής που δείχνεται παρακάτω:

$$F(x_e) = \begin{cases} 1 - e^{-e^{-k_1 x^{c_1}}} & if \quad F(x_e) \le 0.5, \\ 1 - e^{-e^{-k_2 x^{c_2}}} & if \quad F(x_e) \succ 0.5. \end{cases} \tag{10}$$

Μέσος βαθμός συνεκτικότητας d ενός γραφήματος G είναι η μέση τιμή E{P(x)} της κατανομής P(x) του βαθμού συνεκτικότητας x των κόμβων.



(α) (β)

Εικόνα 20. Δίκτυα με εκθετική ("exponential") συνεκτικότητα (α) και με συνεκτικότητα "power laws" (β) [8].

Όπως θα δούμε στη συνέχεια για τη μοντελοποίηση του βαθμού συνεκτικότητας σε δίκτυα ad hoc μεγάλης κλίμακας θα κάνουμε χρήση των κατανομών "heavy tail". Οι κατανομές αυτές έχουν χρησιμοποιηθεί επιτυχώς μέχρι σήμερα, ωστόσο περισσότερο στη θεωρία της τηλεπικοινωνιακής κίνησης και ιδιαίτερα στις εφαρμογές πολλαπλής εκπομπής. Πολυάριθμα παραδείγματα της μέχρι τώρα χρήσης των κατανομών heavy tail βρίσκονται στην παραγωγή κίνησης WWW, όπως είναι η υλοποίηση WWW workloads με ενδιάμεσο χρόνος άφιξης των ερωτημάτων που φθάνουν σε ένα WWW εξυπηρετητή και ενδιάμεσο χρόνος σκέψης των χρηστών που ακολουθούν την κατανομή *Pareto*. Επίσης, η κατανομή του μεγέθους των σελίδων και των αρχείων που συναντάμε στο WWW μοντελοποιείται με ακρίβεια από την κατανομή *Pareto*, ενώ η κατανομή *Weibull* μπορεί να χρησιμοποιηθεί ως μοντέλο για τη στατιστική περιγραφή της κίνησης μικρών μηνυμάτων της ηλεκτρονικής αλληλογραφίας.

5.3.1.4. Μοντέλα Ανάπτυξης Τυχαίων Τοπολογιών

Περιμένουμε ότι η επίδοση των δικτύων ad hoc, δηλαδή η επίδοση αλγορίθμων και πρωτοκόλλων που βρίσκονται σε υψηλότερα επίπεδα της στοίβας πρωτοκόλλων από το φυσικό επίπεδο να επηρεάζονται από τις ιδιότητες της τοπολογίας του δικτύου.

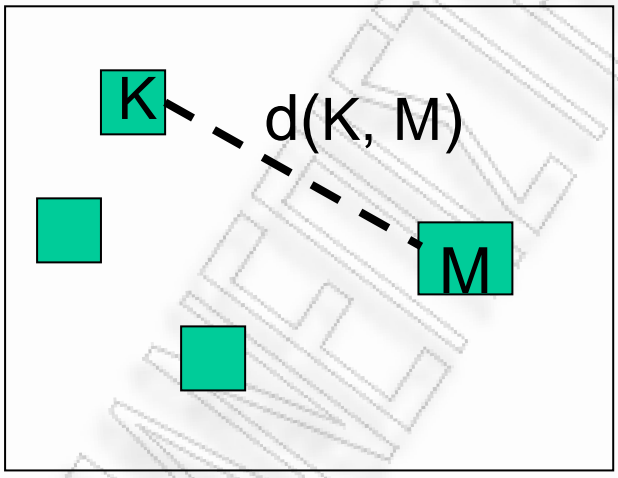
Ένα βασικό χαρακτηριστικό των τοπολογιών είναι ο μέσος βαθμός συνδεσιμότητας των ad hoc κόμβων, καθώς αυτός ο παράγοντας καθορίζει το μέσο αριθμό γειτόνων ανά κόμβο και άρα αποτελεί ένα στατιστικό δείκτη που παρουσιάζει αν ένα δίκτυο είναι συνδεδεμένο ή όχι. Ειδικότερα, θα εξετάσουμε αργότερα αλγόριθμους δημιουργίας συστάδων που ομαδοποιούν τους κόμβους κυρίως με βάση τη θέση τους μέσα στο δίκτυο αλλά και με άλλα χαρακτηριστικά όπως το βαθμό συνεκτικότητας των κόμβων, τη διαθέσιμη ενέργειά τους, την κίνησή τους κ.α. Συνεπώς, μας ενδιαφέρουν οι ιδιότητες των τοπολογιών με τις οποίες αναπτύσσονται τα δίκτυα ad hoc στο χώρο ως παράγοντες που μπορούν να επηρεάζουν τους αλγόριθμους ομαδοποίησης και την ευρωστία του δικτύου έναντι των περιπτώσεων διακοπής της συνεκτικότητας του δικτύου.

Προσεγγίζουμε τα μοντέλα τοπολογιών των δικτύων ad hoc μέσα από τη δημιουργία τυχαίων γράφων στο επίπεδο του δρομολογητή που αντιπροσωπεύει τον τυπικό ad hoc κόμβο. Οι γεννήτριες τυχαίων γράφων που κάνουν χρήση των αυτόνομων συστημάτων, των πεδίων (domain-levels) και των stubs-transits [10] αρμόζουν περισσότερο σε σχηματισμούς κόμβων, διαχειριστικές αρχές και διαχειριστικά πεδία που συχνότερα συναντάμε στο Διαδίκτυο παρά στα δίκτυα ad hoc.

Ειδικότερα, εστιάζουμε στους επαυξητικούς αλγόριθμους κατασκευής τυχαίων γράφων, δηλαδή στη διαδοχική προσθήκη νέων μελών σε ένα σύνολο από ήδη δημιουργημένους κόμβους κατά τρόπο ο οποίος κυρίως βασίζεται στο βαθμό συνεκτικότητας (“connectivity degree”) των κόμβων.

Συμβολίζουμε ένα τυχαίο γράφο ως G(u, v) όπου u είναι το σύνολο των κορυφών του γράφου και v είναι το σύνολο των ακμών του. Ακολουθεί μια σύντομη περιγραφή μερικών από τα πιο γνωστά μοντέλα γένεσης τυχαίων γράφων.

5.3.1.4.1. Το Μοντέλο Waxman



Εικόνα 21. Προσθήκη ζεύξης που συνδέει δύο κόμβους K, M σύμφωνα με το μοντέλο WaxMan.

Το μοντέλο Waxman είναι κατάλληλο για τη μοντελοποίηση σχετικά μικρών και δίχως δομή δικτύων και βασίζεται στις θέσεις των κόμβων για τη δημιουργία τυχαίων γράφων, δίχως την ύπαρξη ιεραρχιών. Όπως φαίνεται στην Εικόνα 21 το μοντέλο Waxman συνδέει δύο κορυφές K, M στο επίπεδο L με πιθανότητα p που εξαρτάται από την Ευκλείδεια απόσταση d αυτών και η οποία πιθανότητα παραμετροποιείται με τους συντελεστές α και b:

$$p = \alpha \times e^{-d/bL}, \qquad \text{όπου } 0<\alpha<1, \quad b>0. \tag{11}$$

5.3.1.4.2. Το Μοντέλο Barabasi-Albert

Το προτιμησιακό μοντέλο συνεκτικότητας ("linear preferential connectivity model") είναι ένας έμμεσος τρόπος να αποκτήσουμε μια τοπολογία όπου η κατανομή του βαθμού συνεκτικότητας των κόμβων ακολουθεί την κατανομή *power law heavy tail* με εκθετική παράμετρο α, όπως περιγράφηκε στην §5.3.1.3 :

$$P[X > x] \approx x^{-a}, x \to \infty, 0 \prec a \prec 2. \quad (12)$$

Σύμφωνα με το "preferential connectivity model" η πιθανότητα p_j ένας κόμβος *i* να ενωθεί με τον κόμβο *j* με βαθμό συνεκτικότητας d_j δίνεται ως:

$p_i = \frac{d_j}{\sum_k d_k}$, όπου d_k είναι ο βαθμός συνεκτικότητας του κάθε κόμβου *k* του γράφου.

Είναι προφανές ότι οι κόμβοι που έχουν αποκτήσει μεγάλο βαθμό συνεκτικότητας "έλκουν" όλο και πιο πολλούς νέους κόμβους στο γράφο, γι' αυτό το λόγο αποκαλούνται και "άπληστοι κόμβοι" και επομένως το μοντέλο της συνεκτικότητας "άπληστο" μοντέλο.

Το μοντέλο Barabasi/Albert [7] βασίζεται ακριβώς στο "preferential connectivity model" για να δημιουργήσει δίκτυα με κατανομές power laws. Θεωρούμε ότι μέσω του μοντέλου Barabasi/Albert οι κατανομές power laws εκτός από το Διαδίκτυο μπορεί επίσης επιτυχώς να εισαχθούν και στη μοντελοποίηση τοπολογιών μεγάλης κλίμακας που συναντάμε στα δίκτυα MANET και ιδιαίτερα στα δίκτυα αισθητήρων. Ειδικότερα, αν επιλέξουμε μικρές τιμές της εκθετικής παραμέτρου *a* της Εξίσωσης [12], τότε η κατανομή heavy tail θα διαμορφώσει ad hoc τοπολογίες που θα χαρακτηρίζονται από ομαδοποιήσεις (τοπικές συγκεντρώσεις) των κόμβων.

5.3.1.4.3. Το Μοντέλο Tiers

Το μοντέλο τυχαίων γράφων Tiers [12] εισάγει τρία διακριτά επίπεδα ιεραρχιών, ονομαστικά τα επίπεδα Wide Area Network (WAN), Metropolitan Area Network (MAN) και Local Area Network (LAN). Όπως φαίνεται στην Εικόνα 22 σε κάθε επίπεδο (ή αλλιώς διαχειριστικό πεδίο, "administrative domain") όλοι οι κόμβοι ανήκουν σε ένα MST (Minimum Spanning Tree) ενώ προστίθενται και ζεύξεις μεταξύ των διαφορετικών επιπέδων με τέτοιο τρόπο ώστε να ικανοποιούνται οι βαθμοί συνεκτικότητας των κόμβων.

5.3.1.4.4. Το Μοντέλο Transit-Stub

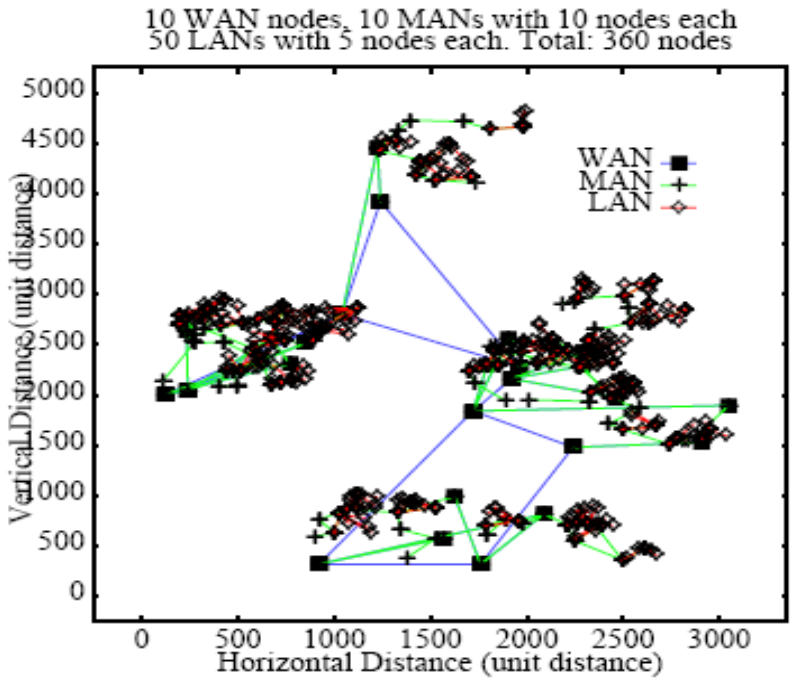
Περαιτέρω, το μοντέλο τυχαίων γράφων Tiers δημιουργεί δύο ιεραρχικά επίπεδα, ονομαστικά το επίπεδο "stub" και το επίπεδο "transit" [13].

5.3.1.4.5. Το Μοντέλο BRITE

Σύμφωνα με το μοντέλο BRITE [14] οι νέοι κόμβοι προστίθενται προσαυξητικά στο γράφο κατά δύο τρόπους:

- Με βάση την Ευκλείδεια απόσταση από τους ήδη υπάρχοντες κόμβους.
- Με βάση το βαθμό συνεκτικότητας των ήδη συνδεδεμένων κόμβων.

Στην πρώτη περίπτωση το μοντέλο BRITE ακολουθεί τις ιδιότητες του μοντέλου WaxMan με τυχαία διεσπαρμένους κόμβους ενώ στη δεύτερη περίπτωση ακολουθεί –και επεκτείνει– τις ιδιότητες του μοντέλου Barabasi/Albert που όπως είδαμε πιο πάνω είναι γνωστό και ως “linear preferential connectivity model” ή και αλλιώς άπληστο μοντέλο (“greedy model”) εφόσον οι ισχυροί κόμβοι με τους περισσότερους γείτονες “έλκουν” όλο και περισσότερα νέα μέλη που διαδοχικά εισέρχονται στο γράφο με αποτέλεσμα οι κόμβοι με μεγάλο βαθμό συνεκτικότητας να ενισχύονται όλο και περισσότερο.



Εικόνα 22. Παραγωγή τυχαίου γράφου τριών επιπέδων με το μοντέλο Tiers, [12].

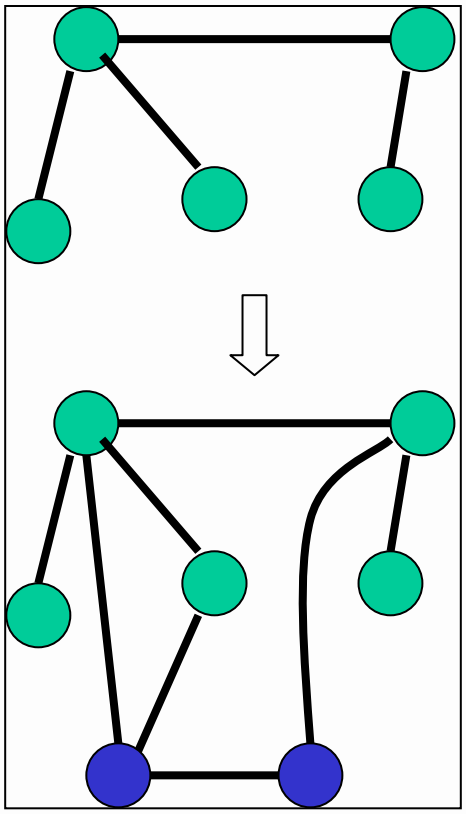
Η προκύπτουσα δομή στην περίπτωση του προτιμησιακού μοντέλου συνδεσιμότητας ακολουθεί την κατανομή των εκθετικών νόμων (“power laws”).

5.3.1.4.6. Η Γεννήτρια Τυχαίων Γράφων BRITE

Μπορούμε να συλλέξουμε τα στατιστικά αποτελέσματα και τα δεδομένα που αφορούν στην επίδοση και τη συμπεριφορά των καινοτόμων αλγορίθμων, πρωτοκόλλων και μηχανισμών κατά τρεις κύριους τρόπους.

- Πρώτον, με την ανάπτυξη των πρωτοκόλλων και των μοντέλων σε πραγματικά δίκτυα ad hoc, οπότε σε αυτήν την περίπτωση είναι πολύ αποτελεσματική η χρήση των κατάλληλα διαμορφωμένων test-beds.

- Δεύτερον, με τη διεξαγωγή πειραμάτων με εργαλεία προσομοίωσης. Σε αυτήν την περίπτωση επιζητούμε η εκτίμηση της απόδοσης των δικτυακών λύσεων να είναι άμεση και κατά το δυνατόν αξιόπιστη.



Εικόνα 23. Προσθήκη νέων κόμβων σύμφωνα με το μοντέλο παραγωγής γράφων BRITE.

- Τρίτον, με ένα συνδυασμό των δύο προηγούμενων, δηλαδή με το να χρησιμοποιούμε κατά ένα μέρος πραγματικούς κόμβους (υλικό) και κατά ένα άλλο μέρος να χρησιμοποιούμε εργαλεία προσομοίωσης (για παράδειγμα για την εισαγωγή δεδομένων και τη δημιουργία κίνησης μέσα σε ένα δίκτυο με πραγματικούς κόμβους). Η μέθοδος αυτή είναι γνωστή ως εξομοίωση ("emulation").

- Τέταρτον με την ανάλυση των δεδομένων που συγκεντρώνονται από τη μακρόχρονη λειτουργία μεγάλων δικτύων με υποδομή όπως το Διαδίκτυο.

Τα αποτελέσματα που θα παρουσιάσουμε αμέσως παρακάτω είναι αποτελέσματα προσομοίωσης, όπου όμως χρησιμοποιούμε δύο προσομοιωτές: τη γεννήτρια τυχαίων γραφημάτων BRITE που ακολουθεί το μοντέλο κατασκευής γράφων Medina/BRITE (2000) [14] και τον προσομοιωτή σε επίπεδο πακέτου Java Network Simulator (JNS) [16].

Παραμετροποιήσαμε κατάλληλα τη γεννήτρια BRITE ώστε να παίρνουμε ως έξοδο την ομοιόμορφη κατανομή και τη heavy tail κατανομή. Οι παράμετροι των δύο βασικών τοπολογιών που παρήγαμε είχαν το εξής εύρος τιμών:

Μέγιστος αριθμός κόμβων 1000 κόμβοι.
Μέγιστος αριθμός ακμών που δημιουργήθηκαν στο γράφο 2994.
Μέσος βαθμός συνεκτικότητας των κόμβων {3, 4, 5, 6}.

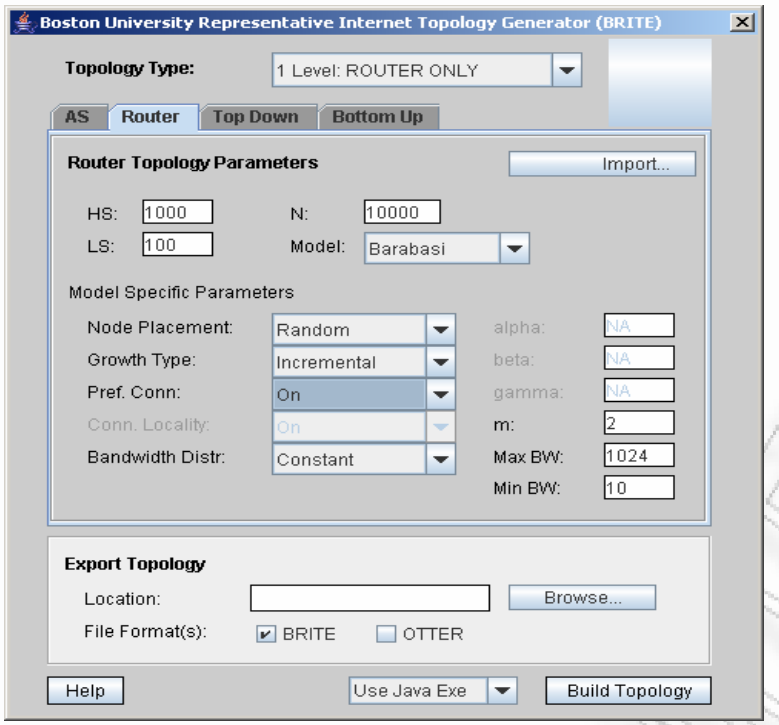
Ακολουθεί το αρχείο παραμετροποίησης BRITE στην περίπτωση του τοπολογικού μοντέλου WaxMan της Εξίσωσης (11) με παραμέτρους α και β.

```
BeginModel
Name =  1               #Router Waxman = 1, AS Waxman = 3
        N = 1000                #Number of nodes in graph
        HS = 1000               #Size of main plane (number of squares)
        LS = 100                #Size of inner planes (number of squares)
        NodePlacement = 1       #Random = 1, Heavy Tailed = 2
        GrowthType = 1                  #Incremental = 1, All = 2
        m = 4                   #Number of neighboring node each new node connects to.
        alpha = 0.15            #Waxman Parameter
        beta = 0.2              #Waxman Parameter
        BWDist = 1              #Constant = 1, Uniform =2, HeavyTailed = 3, Exponential =4
        BWMin = 10.0
        BWMax = 1024.0
End Model
```

Ακολουθεί το αρχείο παραμετροποίησης του μοντέλου Barabasi-Albert (BA) το οποίο παράγει τοποθέτηση των κόμβων-δρομολογητών κατά ομάδες.

```
BeginModel
        Name =  2               #Router Barabasi=2, AS Barabasi =4
        N = 1000                        #Number of nodes in graph
        HS = 1000               #Size of main plane (number of squares)
        LS = 100                #Size of inner planes (number of squares)
        NodePlacement = 2       #Random = 1, Heavy Tailed = 2
        m = 3                   #Number of neighboring node each new node connects to.
        BWDist = 1              #Constant = 1, Uniform =2, HeavyTailed = 3, Exponential =4
        BWMin = 10.0
        BWMax = 1024.0
EndModel
```

Ακολουθεί στιγμιότυπο του BRITE “Graphical User Interface” το οποίο έχει δεχθεί σαν είσοδο από το χρήστη τις απαραίτητες παραμέτρους για τη δημιουργία μιας ad hoc τοπολογίας μεγάλης κλίμακας που ακολουθεί το μοντέλο Barabasi-Albert. Φαίνεται ότι η ανάπτυξη 10000 κόμβων θα γίνει στο επίπεδο του δρομολογητή (επιλογή “1 Level: ROUTER ONLY”) με τυχαίο και αυξητικό τρόπο τοποθέτησης των κόμβων. Επίσης, φαίνεται ότι η επιλογή “Preferential Connectivity” είναι ενεργοποιημένη από το χρήστη.

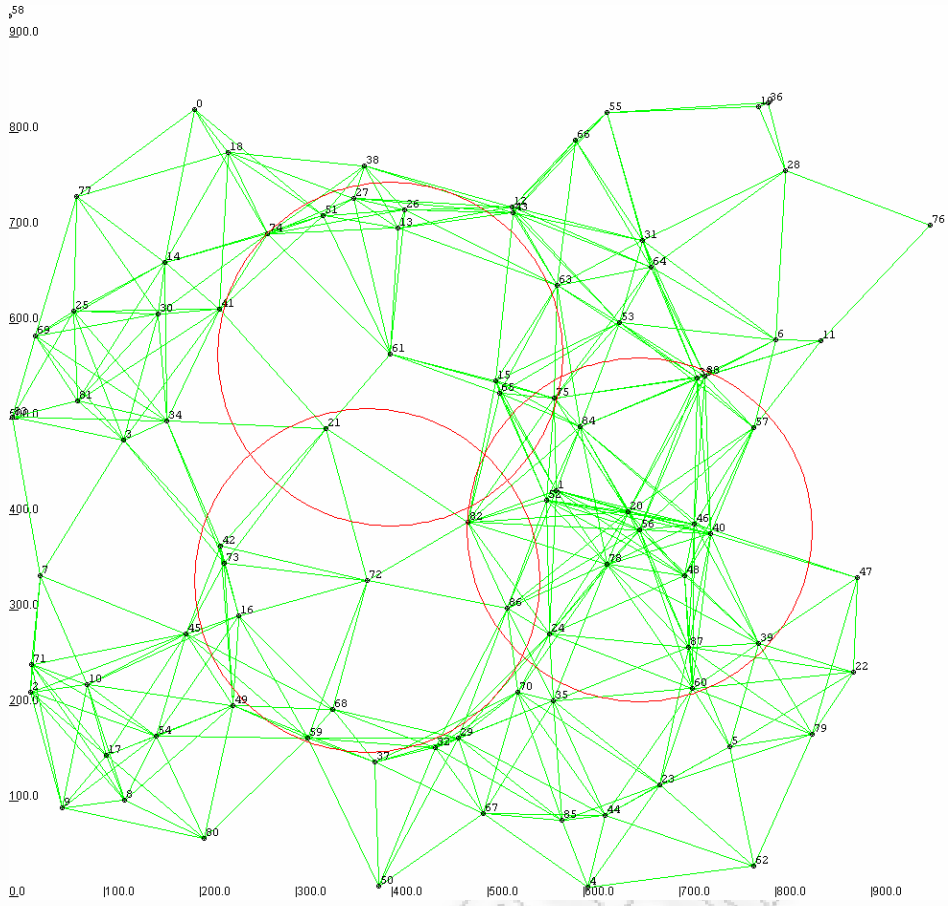


Εικόνα 24. Το Graphical User Interface της γεννήτριας τυχαίων γράφων BRITE.

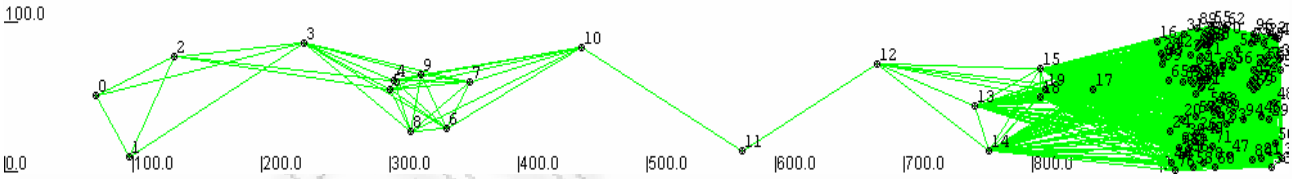
Ως αποτέλεσμα της παραμετροποίησης της γεννήτριας τυχαίων γράφων BRITE και στη συνέχεια της εκτέλεσης της γεννήτριας έχουμε την παραγωγή γράφων δύο από τους οποίους αναπαρίστανται με τη χρήση των κατάλληλων γραφικών εργαλείων και βιβλιοθηκών της Java2 στις Εικόνες 25 και 26. Οι Εικόνες 25 και 26 απεικονίζουν τους δύο βασικούς τύπους γράφων που δημιουργήθηκαν με τη γεννήτρια BRITE, δηλαδή την ασυμπτωτικά ομοιόμορφη τοπολογία (όπου η κατανομή του βαθμού συνεκτικότητας ακολουθεί την εκθετική κατανομή) και τη τοπολογία με ομαδοποίηση των κόμβων (όπου η κατανομή του βαθμού συνεκτικότητας ακολουθεί μια κατανομή “heavy tail”).

Αξίζει να σημειώσουμε ότι οι αποστάσεις που απεικονίζονται μεταξύ των κόμβων στους γράφους των Εικόνων 25 και 26 προκύπτουν από τις τιμές εισόδου και το μοντέλο συνδεσιμότητας που ο χρήστης επιλέγει όσον αφορά την κάθε μία τοπολογία. Κυρίως εξαρτώνται από το μέγεθος meter/pixel, δηλαδή την παράμετρο “number of inner squares” που επιλέγεται σαν παράμετρος της γεννήτριας BRITE. Έτσι, οι αποστάσεις αυτές είναι τελείως ανεξάρτητες από την ισχύ με την οποία θεωρούμε ότι εκπέμπουν οι κόμβοι και συνεπώς είναι ανεξάρτητες από την ακτίνα κάλυψης των ασύρματων ad hoc κόμβων οι οποίοι και τοποθετούνται στις κορυφές των γράφων με συντεταγμένες που παράγονται από τη γεννήτρια.

Οι δύο τοπολογίες 110 κόμβων που απεικονίζονται στην Εικόνα 25 και στην Εικόνα 26 είναι η γραφική αναπαράσταση στο επίπεδο 110 κορυφών και των δεσμών των γράφων που παρήγαγε η γεννήτρια BRITE. Η ακτίνα κάλυψης τέθηκε ίση με 180 μέτρα και στα δύο μοντέλα (ομοιόμορφο και heavy tail) και, όπως φαίνεται, οι δύο γράφοι είναι συνδεδεμένοι.



Εικόνα 25. Στιγμιότυπο τυχαίας τοπολογίας που παράγεται με την εκθετική (ομοιόμορφη) κατανομή.



Εικόνα 26. Στιγμιότυπο τυχαίας τοπολογίας που παράγεται με κατανομή heavy tail.

Ακολουθεί ένα ενδεικτικό απόσπασμα της εξόδου BRITE με τη μορφή αρχείου κειμένου που περιγράφει ένα γράφο που αποτελείται από 1000 κόμβους και 2994 ακμές.

Topology: (1000 Nodes, 2994 Edges)						
Nodes: (1000)						
0	338	546	9	9	-1	RT_NONE
1	306	80	7	7	-1	RT_NONE
2	145	786	4	4	-1	RT_NONE
3	20	510	3	3	-1	RT_NONE

4	985	438	3	3	-1	RT_NONE			
5	937	572	16	16	-1	RT_NONE			
6	43	461	7	7	-1	RT_NONE			
7	568	332	4	4	-1	RT_NONE			
8	940	654	3	3	-1	RT_NONE			
9	760	349	5	5	-1	RT_NONE			
10	947	105	4	4	-1	RT_NONE			
11	561	819	3	3	-1	RT_NONE			
12	852	981	3	3	-1	RT_NONE			
13	254	675	7	7	-1	RT_NONE			
Edges: (2994)									
0	607	928	769.54663	-1.0	10.0	-1	-1	E_AS_NONE	U
1	607	415	407.33893	-1.0	10.0	-1	-1	E_AS_NONE	U
2	607	863	573.6454	-1.0	10.0	-1	-1	E_AS_NONE	U
3	928	415	600.464	-1.0	10.0	-1	-1	E_AS_NONE	U
4	928	863	624.75995	-1.0	10.0	-1	-1	E_AS_NONE	U
5	415	863	167.52313	-1.0	10.0	-1	-1	E_AS_NONE	U
6	86	607	751.3787	0.0	10.0	-1	-1	E_RT_BACKBONE	U

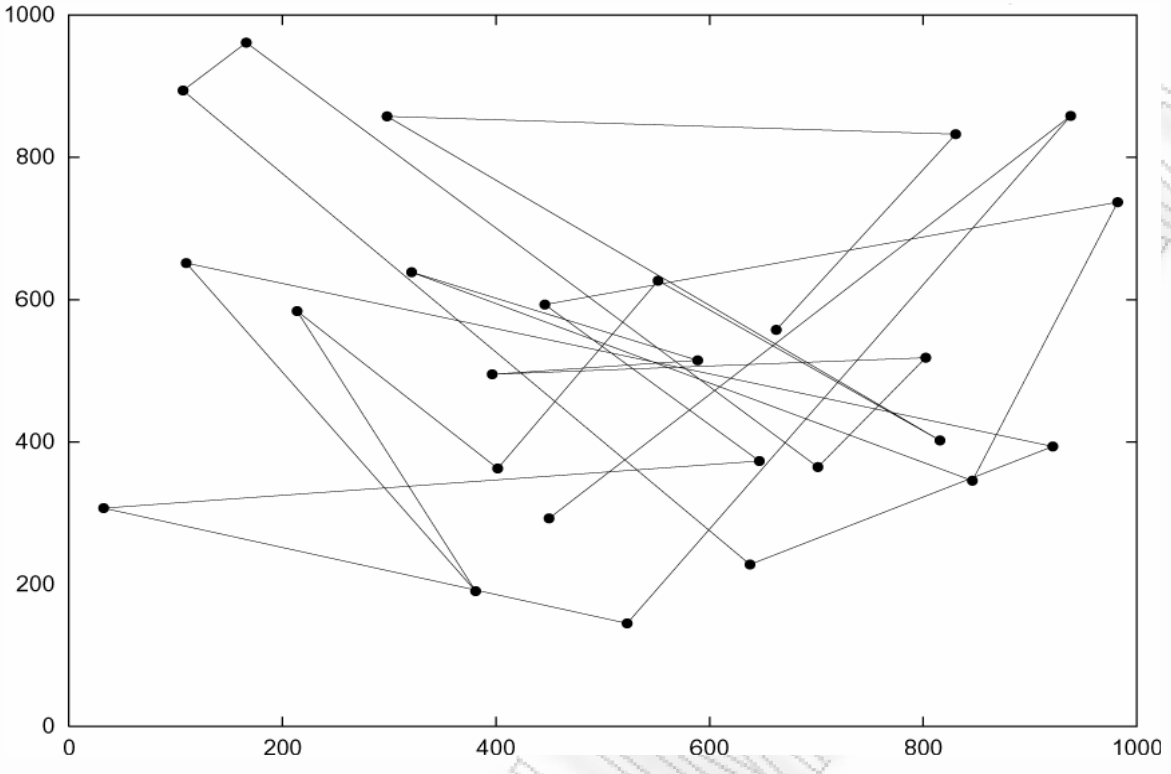
Όπως φαίνεται το αρχείο κειμένου περιέχει την ταυτότητα κάθε κόμβου, τη θέση (x, y) του κάθε κόμβου-κορυφή στο γράφο, τον τύπο των κόμβων (“RT_NONE”, δηλαδή κόμβος-δρομολογητής), την ταυτότητα (ID) των ακμών του γράφου, την πηγή και τον προορισμό της κάθε ακμής καθώς και το μήκος και τη φορά της (“U”, undirected, δηλαδή ακμή διπλής κατεύθυνσης).

5.3.2. Το Μοντέλο Κίνησης των Ασύρματων Κόμβων

Η κίνηση των κόμβων οδηγεί σε συχνές αλλαγές της τοπολογίας του δικτύου με συνέπεια οι σύνδεσμοι μεταξύ των κόμβων να δημιουργούνται και να καταστρέφονται δυναμικά, καθώς κάθε κόμβος εισέρχεται ή εξέρχεται από την ακτίνα εμβέλειας των υπολοίπων. Στο μοντέλο που εξετάζουμε θεωρούμε ότι η κίνηση των κόμβων επηρεάζεται τόσο από ένα σχέδιο δράσης που οι κόμβοι προσπαθούν να εφαρμόσουν, όσο και από τυχαίους παράγοντες.

Για παράδειγμα, το σχέδιο δράσης μπορεί να απαιτεί τη μετακίνηση ενός κόμβου σε μία συγκεκριμένη θέση ώστε να διατηρηθεί η συνεκτικότητα άλλων απομακρυσμένων κόμβων. Ωστόσο, στα πειράματα προσομοίωσης που διεξάγαμε με τον προσομοιωτή JNS υλοποιήσαμε το μοντέλο τυχαίας κίνησης των κόμβων “Random Waypoint Model” (RWP), στιγμιότυπο του οποίου

απεικονίζεται στην Εικόνα 27.



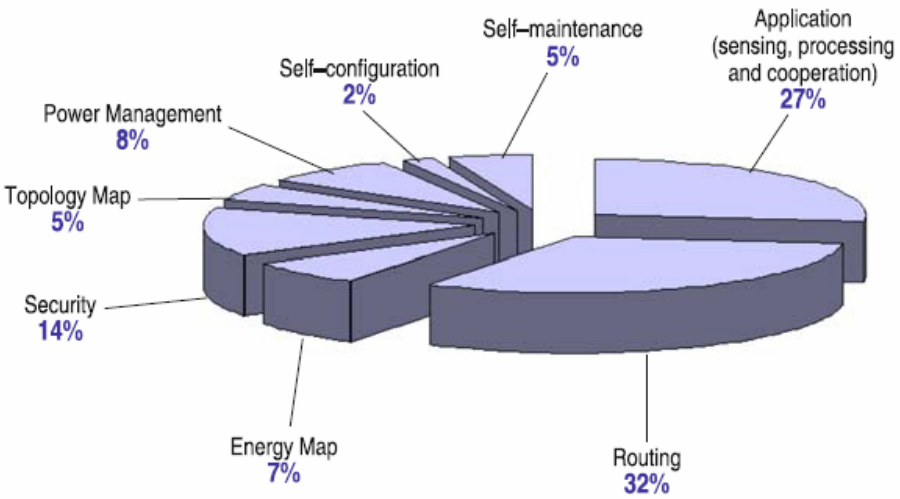
Εικόνα 27.Τυχαία κίνηση κόμβων σύμφωνα με το μοντέλο κίνησης Random Waypoint.

Η Εικόνα 27 παρουσιάζει τα ίχνη της τυχαίας κίνησης ad hoc κόμβων σε μία περιοχή 1000 x 1000 m^2 όταν η κίνηση είναι προσομοιωμένη σύμφωνα με το μοντέλο "κατεύθυνση τυχαίας οδού" ("Random Way Point", RWP). Στην αρχή της προσομοίωσης, κάθε κόμβος περιμένει για ένα διάστημα παύσης, στη συνέχεια επιλέγει ένα τυχαίο σημείο-προορισμό μέσα στο πεδίο και κινείται προς αυτή την κατεύθυνση με μία ταχύτητα που λαμβάνει τυχαίες τιμές ομοιόμορφα κατανεμημένες μεταξύ της μηδενικής και της μέγιστης ταχύτητας. Όταν φτάσει στον προορισμό του σταματά για χρόνο ίσο με το διάστημα παύσης (pause time) και πάλι επαναλαμβάνει την παραπάνω διαδικασία μέχρι το τέλος της προσομοίωσης. Η ελάχιστη ταχύτητα ισούται με 0 m/s ενώ η μέγιστη με 20 m/s.

Τα διαστήματα παύσης που χρησιμοποιήσαμε στα πειράματα προσομοίωσης προκειμένου να εξετάσουμε την συμπεριφορά των αλγόριθμων για ασύρματα δίκτυα ποικίλης κινητικότητας είναι 0, 200, 400 και 700 sec. Όταν το διάστημα παύσης είναι ίσο με 0 sec αυτό αντιστοιχεί σε συνεχή κίνηση του κόμβου, ενώ ένα διάστημα παύσης αρκούντως μεγάλο σε σχέση με τη συνολική διάρκεια της εξομοίωσης αντιστοιχεί σε ένα σταθερό δίκτυο.

Το τυχαίο μοντέλο κίνησης random way point θεωρείται ότι εξομοιώνει ικανοποιητικά την τυχαία κίνηση χρηστών σε δίκτυα MANET, χωρίς αυτό να σημαίνει ότι είναι ένα μοντέλο δίχως προβλήματα. Για παράδειγμα, με αυτό το μοντέλο κίνησης και μετά από ένα μεγάλο χρόνο εξομοίωσης οι κόμβοι τείνουν να συγκεντρώνονται στο κέντρο του πεδίου όπου εξελίσσεται η εξομοίωση της κίνησης, δίνοντας έτσι ψευδή εικόνα για τη συνεκτικότητα που επικρατεί στο δίκτυο. Εντούτοις, για μια πρώτη εκτίμηση της συμπεριφοράς των αλγορίθμων στα κινητά δίκτυα ad hoc για ταχύτητες που δεν ξεπερνούν τα 60km/h και κάτω από εντελώς τυχαίες συνθήκες μετατόπισης των κόμβων θεωρούμε ότι αυτό το μοντέλο είναι αξιόπιστο.

5.3.3. Το Ενεργειακό Μοντέλο των Ασύρματων Κόμβων



Εικόνα 28. Η κατανομή των ενεργοβόρων διαδικασιών στους κόμβους ad hoc [28].

Σύμφωνα με το ενεργειακό μας μοντέλο η διαθέσιμη ενέργεια των ασύρματων κόμβων μειώνεται τόσο όταν ο πομπός τους μεταδίδει όσο και όταν ο δέκτης τους λαμβάνει δεδομένα. Η Εικόνα 28 παρουσιάζει το ποσοστό ενέργειας που καταναλώνουν οι διάφορες διεργασίες στο δίκτυο ad hoc [28]. Φαίνεται στην Εικόνα 28 ότι οι τρείς περισσότερο ενεργοβόρες διαδικασίες είναι οι εφαρμογές που απαιτούν τη μετάδοση των μηνυμάτων στο ασύρματο μέσο, η δρομολόγηση και οι διαδικασίες ασφάλειας.

5.3.4. Το Μοντέλο Εκπομπής των Ασύρματων Κόμβων

Στα πειράματα προσομοίωσης που διεξήγαμε με τον JNS θέσαμε την ακτίνα μετάδοσης των ασύρματων κόμβων να κυμαίνεται μεταξύ των τιμών 0,5 μέτρα μέχρι 200 μέτρα. Η ρύθμιση αυτή είναι συμβατή με τα χαρακτηριστικά των περισσότερων 802.11b προϊόντων (ασύρματες κάρτες γνωστών κατασκευαστών). Ακόμη στην προσομοίωση με τον JNS υποθέσαμε ένα ιδεατό επίπεδο διασύνδεσης δεδομένων (“link layer”) δηλαδή υποθέσαμε ότι δεν υπάρχουν περιορισμοί στο διαθέσιμο εύρος ζώνης μετάδοσης, ότι οι συγκρούσεις είναι μηδενικές, όπως και ότι οι απορρίψεις πακέτων και ο ρυθμός σφαλμάτων στο δέκτη (“BER, bit error rate”) είναι επίσης μηδενικές. Αυτό διευκολύνει την εκτίμηση της απόδοσης των clustering αλγορίθμων, δηλαδή αποφεύγουμε το τελικό αποτέλεσμα να επηρεάζεται από εξωγενείς παράγοντες που σχετίζονται με τη λειτουργία και την επίδοση στα χαμηλότερα επίπεδα του δικτύου.

Στην περίπτωση που οι κόμβοι καλύπτουν μικρές μόνο αποστάσεις με τους πομπούς που διαθέτουν το ασύρματο δίκτυο είναι αραιό με μικρό βαθμό επικάλυψης μεταξύ των συστάδων (clusters) και μικρή συνδεσιμότητα μεταξύ των κόμβων χαμηλής ισχύος. Ως αποτέλεσμα, οι κόμβοι ομαδοποιούνται σε ένα μεγάλο αριθμό από διακριτές ομάδες. Σε αυτή την περίπτωση ο αριθμός των διακριτών ομάδων οι οποίες μπορούν να δημιουργηθούν από τους αλγορίθμους ομαδοποίησης τείνει να γίνει ίσος με τον αριθμό των κόμβων, όσο χαμηλότερη είναι η ισχύς εκπομπής. Αντίθετα, μεγάλες ακτίνες κάλυψης από εύρωστους κόμβους που διαθέτουν ισχυρούς πομπούς έχουν σαν αποτέλεσμα την ομαδοποίηση και τη δημιουργία πυκνών δικτύων με μεγάλο βαθμό συνεκτικότητας μεταξύ των κόμβων. Ως εκ τούτου, όταν οι ad hoc κόμβοι είναι ισχυροί ομαδοποιούνται σε λίγες μόνο συστάδες μεγάλης χωρητικότητας οι οποίες έχουν μεταξύ τους σημαντικό βαθμό επικάλυψης.

Έτσι φαίνεται ότι η ισχύς εκπομπής των κόμβων είναι ένας πολύ σημαντικός παράγοντας τον

οποίο θα πρέπει να μεταβάλλουμε κατά τιμή και εύρος στα πειράματά μας ώστε να αναλύσουμε ακόμη περισσότερο την επίδρασή του στη συμπεριφορά των αλγορίθμων και των πρωτοκόλλων του δικτύου.

5.4. Ο ΑΛΓΟΡΙΘΜΟΣ ΕΚΛΟΓΗΣ ΑΡΧΗΓΟΥ RRA

Υλοποιήσαμε τον προτεινόμενο αλγόριθμο “Robust Re-clustering Algorithm” (RRA) σαν ένα αλγόριθμο επιλογής κόμβων-αρχηγών και δυναμικής ομαδοποίησης του δικτύου σε συστάδες (clusters). Σε πρώτη φάση, ο αλγόριθμος “Robust Re-clustering Algorithm” βασίζεται σε τοπολογίες ασύρματων δικτύων ad hoc οι οποίες δημιουργούνται με γεννήτριες τυχαίων γράφων.

Η μεταβλητή απόφασης του αλγορίθμου είναι σταθμισμένη σε τρεις παραμέτρους απόφασης. Ο RRA εισάγει στο δίκτυο μια διεργασία λήψης απόφασης που βρίσκει τη μέγιστη τιμή της μεταβλητής απόφασης *V* προκειμένου να επιλέξει τον τοπικό αρχηγό μεταξύ των κόμβων μιας γειτονιάς. Ο αλγόριθμος RRA είναι εύρωστος εφόσον στοχεύει στην επιλογή κόμβων-αρχηγών οι οποίοι είναι πραγματικά διαθέσιμοι για να αναλάβουν αυτό το ρόλο. Οι τρεις παράμετροι που λαμβάνει υπόψη ο αλγόριθμος RRA και οι οποίοι παράγοντες δικαιολογούν την ευρωστία του αλγορίθμου είναι οι εξής.

- ***Η μέση τιμή d_i του βαθμού συνεκτικότητας*** των κόμβων του αρχικού γράφου, δες και §5.3.1.3. Η παράμετρος d_i ζυγίζεται με το συντελεστή *a* από τον RRA και καθορίζει τον αριθμό των γειτόνων σε απόσταση ενός και μόνο βήματος που κατά μέσο όρο έχουν οι κόμβοι στην τοπολογία που προκύπτει από τον τυχαίο γράφο. Συνεπώς για τους ασύρματους ad hoc κόμβους η παράμετρος μέσης συνεκτικότητας d_i είναι ο αριθμός των γειτόνων που βρίσκονται εντός της εμβελείας του ασύρματου κόμβου *i*.

- Η ***διαθέσιμη ενέργεια*** των κόμβων E_{ri}. Η διαθέσιμη ενέργεια των κόμβων είναι μια σημαντική παράμετρος για τη δημιουργία αυτόνομων και επιβιώσιμων δικτύων ad hoc η οποία σταθμίζεται από τον αλγόριθμο RRA με το συντελεστή *b*. Είναι επιθυμητό ο αλγόριθμος επιλογής κόμβων-αρχηγών να επιλέγει σαν αρχηγούς εκείνους τους κόμβους που διαθέτουν αρκούντως υψηλή στάθμη ενέργειας έτσι ώστε να μπορέσουν να επιτελέσουν τα καθήκοντα του αρχηγού για ικανοποιητικό χρονικό διάστημα.

- Η ***θέση των κόμβων*** μέσα στη συστάδα. Ο RRA λαμβάνει υπόψη την απόσταση των κόμβων από κάποιο σημείο αναφοράς που βρίσκεται μέσα σε μια περιοχή του δικτύου. Ως τέτοιο σημείο επιλέξαμε το μέσο σημείο της γειτονιάς, δηλαδή τη μέση τιμή των συντεταγμένων των κόμβων που συμμετέχουν σε μια συστάδα. Η απόσταση D_i ορίζεται ως η απόσταση κάθε κόμβου *i* από το μέσο της γειτονιάς του ($\underline{x}$, $\underline{y}$) και το αντίστροφο της απόστασης αυτής D_i^{-1} ζυγίζεται από τον RRA με το συντελεστή *c*. Η απόσταση D_i καθορίζει αν ο υποψήφιος κόμβος βρίσκεται στο κέντρο ή στην περιφέρεια ενός cluster που καθορίζεται από τους γειτονικούς κόμβους του. Είναι επιθυμητό ο αλγόριθμος εκλογής κόμβων-αρχηγών να επιλέγει σαν αρχηγούς εκείνους τους κόμβους που βρίσκονται κοντά στο κέντρο της συστάδας (cluster).

  Πρώτον, γιατί αυτό εξασφαλίζει ότι ένας τέτοιος κεντρικός κόμβος θα είναι συνδεδεμένος με περισσότερους γείτονες και άρα σαν cluster head θα μπορεί να εξυπηρετεί περισσότερα μέλη στην ομάδα του.

  Δεύτερον, γιατί ένας κόμβος στην περιφέρεια είναι πολύ πιθανό να περιφέρεται χωρίς να μπορεί να συσχετιστεί με κάποιο cluster head, εφόσον πολύ πιθανά θα χάνει την κάλυψή του. Επόμενο είναι τέτοιοι κόμβοι να προκαλούν πολλές συνεχόμενες προσπάθειες δημιουργίας ομάδας (re-clustering) κάτι το οποίο, όπως έχουμε εξηγήσει, προκαλεί επιβάρυνση στις επικοινωνίες του δικτύου. Επιπλέον, ως αποτέλεσμα των παραπάνω

τέτοιοι κόμβοι που βρίσκονται στην περιφέρεια αυξάνουν το συνολικό αριθμό των αρχηγών στο δίκτυο εφόσον αναπόφευκτα οι ίδιοι γίνονται κόμβοι-αρχηγοί.

Η μεταβλητή απόφασης V_i υπολογίζεται για κάθε κόμβο από τον RRA ως το σταθμισμένο άθροισμα των παραμέτρων d_i, E_{ri} και D_i^{-1}, όπως δίνεται στην Εξίσωση (13).

$$V_i = a \times d_i + b \times E_{ri} + c \times D_i^{-1}, \quad (13)$$

όπου τα βάρη *α*, *b* και *c* ικανοποιούν τη συνθήκη

$$\alpha + b + c = 1 \quad (14)$$

Η επιλογή των τιμών των συντελεστών α, b και c εξαρτάται από τις συνθήκες που επικρατούν σε κάθε δίκτυο ad hoc καθώς επίσης και από τις απαιτήσεις και τις προδιαγραφές της κάθε εφαρμογής ad hoc. Για παράδειγμα, αν δώσουμε μεγαλύτερο βάρος *α* στο βαθμό συνεκτικότητας d τότε με μεγαλύτερη πιθανότητα θα εκλέγονται ως αρχηγοί εκείνοι οι κόμβοι οι οποίοι διαθέτουν μεγάλο αριθμό γειτόνων, κάτι το οποίο είναι πράγματι επιθυμητό για πυκνά δίκτυα ad hoc, εφόσον τότε ένας κόμβος-αρχηγός θα μπορεί να εξυπηρετεί πολλούς γείτονες. Χαρακτηριστικά ανάπτυξης πυκνών δικτύων συναντάμε σε στρατιωτικές εφαρμογές.

Αντίθετα, σε μια αραιή κατανομή των κόμβων στο χώρο, για παράδειγμα σε μια εφαρμογή περιφρούρησης της περιμέτρου ενός σπιτιού, ή σε μια εφαρμογή διασποράς αισθητήρων για την παρακολούθηση της θερμοκρασίας του περιβάλλοντος είναι επιθυμητό οι κόμβοι-αρχηγοί να έχουν περισσότερη διαθέσιμη ενέργεια ώστε να μπορούν να στέλνουν τα δεδομένα τους προς το σταθμό βάσης, οπότε συνιστάται η ενίσχυση του συντελεστή *b* της ενέργειας E_{ri}.

Ο RRA αποτελείται από δύο φάσεις. Στην πρώτη φάση (PHASE I) εγκαθίσταται το ad hoc δίκτυο δηλαδή οι κόμβοι παίρνουν θέση στις κορυφές του τυχαίου γράφου G(u, v) βάσει της πληροφορίας η οποία λαμβάνεται ως έξοδος της γεννήτριας BRITE όπως εξηγήθηκε στην §5.3.1.4.6. Τα πρωτόκολλα, οι διεπαφές μεταξύ των και οι αλγόριθμοι που τρέχουν στους κόμβους εγκαθίστανται στη φάση αυτή. Ειδικότερα, στην πρώτη φάση υποθέτουμε ότι κάθε κόμβος γνωρίζει τις αρχικές συντεταγμένες του (x, y) και ενεργοποιεί το στοιχείο *ip_handler* που διαθέτει και το οποίο είναι το βασικό στοιχείο-χειριστής του πρωτοκόλλου IP με το οποίο δρομολογούνται τα πακέτα στον εξομοιωτή JNS, δες και Παραρτημα I :.

Επιπλέον, στην πρώτη φάση του αλγόριθμου RRA αρχικοποιούνται οι ταυτότητες των κόμβων, οι ρόλοι αυτών (ένας κόμβος μπορεί αποκλειστικά να έχει το ρόλο του απλού μέλους ή το ρόλο του αρχηγού (cluster head) ή μπορεί να είναι απομονωμένος (isolated), δηλαδή αρχικά να μην ανήκει σε κάποια συστάδα χωρίς να είναι αρχηγός ο ίδιος), οι δομές δεδομένων (οι πίνακες δρομολόγησης, οι λίστες με τα μέλη των ομάδων –cluster_member_Table –, οι λίστες με τους γείτονες του κάθε κόμβου –Neighbor_List –, οι λίστες με τους τρέχοντες αρχηγούς –CH_Table – καθώς και οι πόροι (ενέργεια και μετρητές) που χρησιμοποιούνται για κάθε ένα από τους κόμβους.

Επίσης, στην πρώτη φάση του αλγορίθμου RRA ενεργοποιείται η τυχαία κίνηση των κόμβων σύμφωνα με το μοντέλο “κατεύθυνση τυχαίας οδού” (“Random Waypoint”) όπου δίνονται τιμές στην ελάχιστη και τη μέγιστη ταχύτητα των κόμβων, δίνεται τιμή στο χρόνο παύσης των κόμβων, τιμές στα χωρικά όρια του πλέγματος μέσα στο οποίο κινούνται οι κόμβοι και τέλος καθορίζεται το μέγεθος του βήματος της τυχαίας κίνησης των κόμβων (ίση με 10 m/pixel).

Εγκατάσταση δικτύου ad hoc: RRA ΦΑΣΗ Ι

```
∀ node ∈ G{
            node.Role = Isolated;
            node.CH_counter , node.E_consumed = 0;
               node.E_residual = max;
               node.CH_Table = new Table;
               node.Members_Vector = new Vector;
               node.Neighbor_List = new List;
               node.Hellos_Vector= new Vector;
          }
```

Εικόνα 29. Η πρώτη φάση της εγκατάστασης του δικτύου με τον RRA.

Κατά τη δεύτερη φάση του αλγόριθμου RRA εκτελούνται συνεχόμενες και κεντρικά ελεγχόμενες επαναλήψεις ομαδοποίησης (“clustering runs”). Σε κάθε μία επανάληψη του αλγορίθμου εκτελείται η βασική διεργασία της εκλογής των κόμβων-αρχηγών κατά μήκος ολοκλήρου του δικτύου. Έτσι ο αλγόριθμος εξετάζει το σύνολο των κόμβων του γράφου σε κάθε μια επανάληψη. Κατά τη φάση αυτή επίσης εκτελείται η ομαδοποίηση των απλών κόμβων κάτω από τους νέους κόμβους-αρχηγούς. Είναι αξιοσημείωτο ότι σε κάθε επανάληψη κάθε κόμβος εξετάζεται μία και μόνο φορά από τον αλγόριθμο προκειμένου να μπορεί η ομαδοποίηση των κόμβων να είναι εφικτή (και αξιόπιστη) στη δεδομένη αυτή χρονική στιγμή.

Εκλογή αρχηγών ομάδων: RRA ΦΑΣΗ ΙΙ

```
∀ node ∈ G{
     //G is the deployed network graph
    if (node ∉ D) {
         //D is the set of all nodes already joined to a cluster
         build Neighbor_List;
         CH = node with Max w_i in Neighbor_List ;
         CH.setRole = cluster_head;
         CH.setCH(CH);
         CH_Table.add(CH);
         CH.E_res = CH.E_res - CH.E_consumed++;
         ∀ (neigh ∈ Neighbor_List and neigh != CH) {
                    neigh.setRole(Member);
                neigh.setCH(CH);
                Member_Table.add(neigh);
                D.add(neigh);
         }
          D.add(node);
          D.add(CH);
      }
}
```

Εικόνα 30. Η δεύτερη φάση της εκλογής αρχηγών - cluster heads - με τον RRA.

Προκειμένου να ληφθεί απόφαση για κάθε κόμβο του γράφου που εξετάζεται σε κάθε επανάληψη, ο αλγόριθμος εφαρμόζει την Εξίσωση (13) για τον εξεταζόμενο κόμβο και για κάθε έναν από τους γείτονές του. Ο βαθμός συνεκτικότητας του κάθε γειτονικού κόμβου υπολογίζεται με βάση την τάξη της λίστας που αυτός διαθέτει με τους γειτονικούς του κόμβους, δηλαδή με το μέγεθος της Neighboring_List. Η Neighboring_List για κάθε κόμβο συμπληρώνεται από εκείνους τους κόμβους που γεωγραφικά βρίσκονται σε θέση που καλύπτεται από την ακτίνα κάλυψης του εν λόγω κόμβου. Η ακτίνα κάλυψης των ασύρματων κόμβων εξαρτάται από την ισχύ εκπομπής.

Επιπλέον, για τη λήψη της απόφασης ως προς τον αρχηγό σε κάθε γειτονιά λαμβάνεται υπόψη το απόθεμα ενέργειας που διαθέτει κάθε κόμβος και ακόμη υπολογίζεται η απόσταση του κάθε κόμβου από το κέντρο της γειτονιάς του. Για την αξιοπιστία όλων των υπολογισμών που

περιλαμβάνουν τη θέση των κόμβων είναι απαραίτητο οι συντεταγμένες των κινούμενων κόμβων να ανανεώνονται. Αυτό επιτυγχάνεται με την έκδοση της κατάλληλης εντολής (“command”) από το στοιχείο (“element”) που υλοποιεί το τυχαίο μοντέλο κίνησης RWP στον εξομοιωτή JNS, έτσι ώστε οι θέσεις όλων των κινούμενων κόμβων να ενημερώνονται σε χρονικά διαστήματα ίσα με τη χρονική διάρκεια του βήματος κίνησης.

Επίσης, κατά τη δεύτερη αυτή φάση και σε κάθε επανάληψη πραγματοποιείται η αλλαγή των αρχικών ρόλων των κόμβων, διαδοχική μείωση της ενέργειας των αρχηγών σε κάθε μετάδοση και λήψη μηνύματος, κυρίως όμως πραγματοποιείται ενημέρωση των υπολοίπων αν χρειαστεί να πραγματοποιηθεί κάποια αλλαγή του ρόλου σε κάποιον από τους υπάρχοντες αρχηγούς (από αρχηγός σε απλό μέλος). Στην περίπτωση που κάποιος αρχηγός πρέπει να αλλάξει ρόλο και κάποιος άλλος κόμβος να γίνει αρχηγός στη γειτονιά χρειάζεται οι υπόλοιποι κόμβοι να ενημερωθούν για το νέο αρχηγό.

Η διαδικασία της ενημέρωσης του δικτύου για τη νέα δομή είναι η πιο κρίσιμη για την επίδοση κάθε αλγόριθμου ομαδοποίησης. Η διαδικασία αυτή η γνωστή ως επαναομαδοποίηση (“re-clustering procedure”). Έτσι, αν σύμφωνα με τις επιλογές του αλγορίθμου απαιτείται μεγάλος αριθμός μεταβολών των κόμβων-αρχηγών –“re-clustering”– κατά τη διάρκεια ενός συγκεκριμένου χρονικού διαστήματος, τότε η επιβάρυνση που επιβάλλει ο αλγόριθμος στις επικοινωνίες του δικτύου λόγω των πολλών μεταβολών κατάστασης των κόμβων και τη μετάδοση μεγάλου αριθμού μηνυμάτων ενημέρωσης αυξάνεται. Επίσης σε αυτή τη φάση κρίνεται και η ευρωστία του αλγορίθμου clustering (αν οι κόμβοι που επιλέγει για αρχηγούς είναι πράγματι διαθέσιμοι, δηλαδή αν έχουν το απαραίτητο επίπεδο ενέργειας).

5.5. ΕΚΤΙΜΗΣΗ ΤΗΣ ΕΠΙΔΟΣΗΣ ΤΩΝ ΑΛΓΟΡΙΘΜΩΝ ΣΥΣΤΑΔΟΠΟΙΗΣΗΣ

Σε αυτή την ενότητα θα εκτιμήσουμε και θα συγκρίνουμε την απόδοση τριών αλγορίθμων ομαδοποίησης, ονομαστικά του “Lower ID”, του “Highest Degree” και του προτεινόμενου RRA με το δικτυακό προσομοιωτή JNS, δες στο Παραρτημα Ι : για μια σύντομη περιγραφή του προσομοιωτή JNS.

5.5.1. Σχετικές Εργασίες

Στην υφιστάμενη βιβλιογραφία ([17] - [26]) συναντούμε πολλές διαφορετικές προσεγγίσεις του προβλήματος της αποδοτικής οργάνωσης των κόμβων των δικτύων ad hoc (κυρίως των δικτύων MANET) σε συστάδες με την επιλογή των βέλτιστων αρχηγών, το οποίο είναι ένα NP-hard πρόβλημα. Επικεντρώνουμε στους παρακάτω ευριστικούς αλγόριθμους.

Ο αλγόριθμος Lower ID (LID) [18] είναι από τους πιο δημοφιλείς στατικούς αλγορίθμους. Είναι στατικος εφόσον δεν λαμβάνει υπόψη την τοπολογία του δικτύου κατά την επιλογή των κόμβων-αρχηγών. Ο αλγόριθμος Lower ID έχει αρκετές παραλλαγές. Σε όλες όμως τις εκδοχές του ως αρχηγός επιλέγεται εκείνος ο κόμβος που έχει τη μικρότερη ταυτότητα στη γειτονιά του. Μειονέκτημα του αλγορίθμου LID είναι ότι στην περίπτωση που ένας κόμβος με μικρό αριθμό ταυτότητας εκτελεί περιαγωγή θα αναγκάσει το ad hoc δίκτυο σε πολλές αλλαγές αρχηγού εφόσον πάντα θα επικρατεί στις περιοχές που επισκέπτεται. Συνεπώς, ο κόμβος αυτός θα επιλεχθεί πολλές φορές ως αρχηγός και θα καταναλωθεί γρήγορα η ενέργειά του.

Επιπλέον, η επιβάρυνση στις επικοινωνίες του δικτύου με τον LID θα είναι αναπόφευκτα σημαντική.

Κατανεμημένα και πιο δυναμικά σχήματα που λαμβάνουν υπόψη την τοπολογία και την κίνηση των κόμβων στα δίκτυα MANET και τα οποία βελτιώνουν την επίδοση του αλγορίθμου LID είναι το σχήμα “Least Cluster Head Change” (LCC) [23]. Κατά τον αλγόριθμο LCC όταν δύο αρχηγοί

έρχονται σε κοντινή απόσταση κάλυψης ενεργοποιείται η διαδικασία επαναομαδοποίησης η οποία έχει σαν αποτέλεσμα ο ένας από τους δύο αρχηγούς να γίνει απλό μέλος της νέας συστάδας που προκύπτει από τη συγχώνευση των δύο προηγούμενων. Επίσης, κατά τον LCC επαναομαδοποίηση συμβαίνει όταν κάποιος κόμβος μένει "ακάλυπτος", δηλαδή τυχαίνει να μην είναι απλό μέλος καμιάς συστάδας.

Ο αλγόριθμος Highest Degree (HD) [19] είναι ένας απλός και δημοφιλής δυναμικός αλγόριθμος που λαμβάνει υπόψη του το βαθμό συνδεσιμότητας των κόμβων για την επιλογή των αρχηγών που θα δρομολογήσουν τα πακέτα. Κατά τον αλγόριθμο HD ως αρχηγός επιλέγεται εκείνος ο κόμβος που έχει το μεγαλύτερο βαθμό συνεκτικότητας στη γειτονιά του. Βελτιωμένα σχήματα του HD περιλαμβάνουν το σχήμα LCC [23] και μια σταθμισμένη εκδοχή του HD [24]. Στη σταθμισμένη εκδοχή του αλγόριθμου HD [24] ως αρχηγός εκλέγεται ο κόμβος που διαθέτει ένα μεγάλο αριθμό από γείτονες οι οποίοι έχουν μικρό βαθμό συνεκτικότητας.

Ο πιθανοκρατικός LEACH [15] ήταν μια από τις πρώτες σοβαρές απόπειρες να επιτευχθεί εξοικονόμηση ενέργειας κατά την ομαδοποίηση των κόμβων αισθητήρων με την εξισορρόπηση του φορτίου στο δίκτυο. Ο αλγόριθμος "Hybrid Energy-Efficient Distributed" (HEED) [16] διατηρεί μικρή την πιθανότητα να επιλεγούν δύο αρχηγοί που βρίσκονται ο ένας στην ακτίνα κάλυψης του άλλου και επίσης υπολογίζει την ελάχιστη απαραίτητη απόσταση μεταξύ των clusters η οποία διατηρεί το γράφο πολλπλών βημάτων με όλους τους αρχηγούς του δικτύου συνδεδεμένο. Ο σταθμισμένος Highest Degree [17] είναι μια τελευταία εκδοχή του αλγόριθμου Highest Degree στην οποία οι κόμβοι με μεγάλο αριθμό από γείτονες ενός βήματος μικρής συνεκτικότητας προτιμώνται να γίνουν αρχηγοί.

Στη διαδικασία της συσταδοποίησης των κόμβων μπορεί να ληφθούν υπόψη και παράμετροι που χαρακτηρίζουν το σύστημα, όπως τα σχήματα που παρουσιάζονται στις εργασίες [21], [22] όπου παρουσιάζεται ο αλγόριθμος MOBIC. Ο αλγόριθμος MOBIC λαμβάνει υπόψη του την κίνηση και θεωρείται αρκετά αποδοτικός ενώ άλλοι δύο αλγόριθμοι που λαμβάνουν υπόψη τους παραμέτρους του συστήματος είναι ο αλγόριθμος Distributed Clustering Algorithm (DCA) καθώς και η παραλλαγή αυτού για την περίπτωση κινούμενων κόμβων Distributed Mobility-Adaptive Clustering (DMAC) [20]. Επίσης ένα πολύ γνωστό σταθμισμένο σχήμα ομαδοποίησης που λαμβάνει υπόψη συστημικές παραμέτρους είναι ο Weighted Clustering Algorithm (WCA) [29]. Οι αλγόριθμοι αυτοί συνδυάζουν πολλές παραμέτρους όπως την ταχύτητα, το χρόνο που οι κόμβοι έχουν λειτουργήσει ως αρχηγοί, το βαθμό συνεκτικότητάς τους και τις σχετικές αποστάσεις μεταξύ των κόμβων. Επίσης, άλλες παράμετροι που υπολογίζονται από τους αλγόριθμους αυτούς είναι η ισχύς των κόμβων και η ενέργειά τους [21]. Η σχετική θέση και η σχετική ταχύτητα των κόμβων υπολογίζονται με βάση τη στάθμη ισχύος των σημάτων που λαμβάνονται από τους κόμβους οι οποίοι πρέπει να ανταλλάσσουν περιοδικά μηνύματα ([20], [22]).

Τα συμβατικά μέτρα αξιολόγησης της επίδοσης των αλγόριθμων συσταδοποίησης που συναντάμε εκτενώς στην υφιστάμενη βιβλιογραφία ([17] - [29]) και τα οποία θα χρησιμοποιήσουμε στην αξιολόγηση και σύγκριση των αλγορίθμων που θα επιχειρήσουμε είναι τα ακόλουθα:

- Η *ευστάθεια* των αλγορίθμων "clustering", δηλαδή ο ρυθμός αλλαγής των "cluster heads". Είναι επιθυμητό η δομή που προκύπτει σαν αποτελέσμα της εφαρμογής των αλγορίθμων clustering να είναι κατά το δυνατόν σταθερή, δηλαδή ο μέσος αριθμός αλλαγών των ρόλων των κόμβων μέσα στο δίκτυο να είναι ο ελάχιστος δυνατός σε ένα δεδομένο χρονικό διάστημα, έτσι ώστε και η επιβάρυνση που επιβάλλεται στις επικοινωνίες του δικτύου για την ενημέρωση των κόμβων να είναι η ελάχιστη δυνατή.

- Ο *αριθμός των διακριτών συστάδων* που παράγονται από τους αλγόριθμους. Κάθε αλγόριθμος ομαδοποιεί με διαφορετικό τρόπο τους κόμβους του ίδιου δικτύου και είναι γενικά επιθυμητό ο αριθμός των διακριτών συστάδων που δημιουργούνται από τους

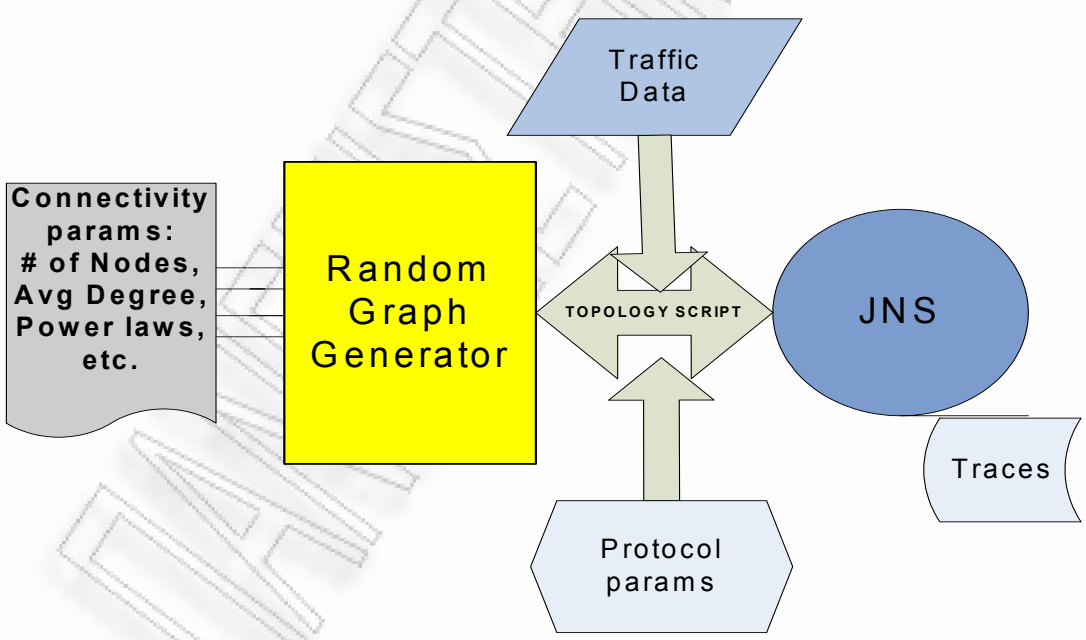
αλγόριθμους να είναι μικρός για λόγους κλιμάκωσης του δικτύου ώστε να διατηρείται μικρή η επιβάρυνση στη λειτουργία του δικτύου.

Επιπλέον, είναι θεμιτό η ευρωστία των συγκρινόμενων αλγορίθμων συσταδοποίησης να αξιολογείται με πρόσθετα μέτρα αξιοπιστίας και διαθεσιμότητας όπως είναι τα εξής.

- Το ποσοστό των μηνυμάτων που παραδίδονται επιτυχώς από άκρη σε άκρη ("packet delivery ratio, pdr").
- Το ποσοστό του χρόνου κατά το οποίο είναι διαθέσιμοι οι κόμβοι-αρχηγοί που εκλέγονται από τους αλγορίθμους.
- Ο βαθμός συνεκτικότητας του δικτύου ο οποίος αντιπροσωπεύεται από τη συνεκτικότητα μεταξύ των κόμβων-αρχηγών που εκλέγονται από τους αλγόριθμους.
- Η απώλεια πακέτων στο δίκτυο στις επικοινωνίες εντός και μεταξύ των συστάδων.

Στόχος μας είναι με βάση τα πειραματικά αποτελέσματα να εξαγάγουμε καθολικά συμπεράσματα που θα ισχύουν για τους γενικούς αλγορίθμους ομαδοποίησης και εκλογής αρχηγών και ακόμη να εξαγάγουμε ειδικά συμπεράσματα για τη συμπεριφορά του καθενός αλγορίθμου ξεχωριστά τα οποία θα έχουν ισχύ κάτω από τις παραδοχές που κάνουμε για τις δικτυακές συνθήκες που επικρατούν.

5.5.2. Ρύθμιση Παραμέτρων στον Προσομοιωτή JNS



Εικόνα 31. Οι παράμετροι εισόδου στον προσομοιωτή JNS.

Η Εικόνα 31 απεικονίζει τη μέθοδο με την οποία αξιολογούμε εμπειρικά τους αλγορίθμους συσταδοποίησης κάτω από διαφορετικές δικτυακές συνθήκες. Βασική είσοδος στο εμπειρικό σύστημα εκτίμησης της επίδοσης των αλγορίθμων συσταδοποίησης είναι οι τοπολογικές παράμετροι που περιγράψαμε παραπάνω, όπως για παράδειγμα ο βαθμός συνεκτικότητας, ο αριθμός των κόμβων, οι κατανομές του βαθμού συνεκτικότητας κ.α. .

Οι παράμετροι των διαφορετικών μοντέλων τοπολογιών που εξετάζονται αποτελούν την είσοδο της γεννήτριας τυχαίων γράφων. Η έξοδος της γεννήτριας είναι οι τυχαίες τοπολογίες οι οποίες διαθέτουν διαφορετικές στατιστικές ιδιότητες.

Στη συνέχεια η πληροφορία των τυχαίων γράφων αυτή συνδυάζεται με παραμέτρους που έχουν να κάνουν με τη σύνθεση της δικτυακής κίνησης (δηλαδή τις πηγές και τα πρωτόκολλα δικτυακής κίνησης, τον αριθμό ροών δεδομένων, την έγχυση δεδομένων και το ποσοστό έγχυσης παραπλανητικής πληροφορίας, το ρυθμό άφιξης μηνυμάτων, την κατανομή του μέγεθους των πακέτων κ.α.) και με τις ειδικές παραμέτρους των πρωτοκόλλων και των δικτυακών αλγορίθμων. Ο συνδυασμός αυτών αποτελεί την είσοδο στο δικτυακό προσομοιωτή JNS. Η εκτίμηση της επίδοσης των αλγορίθμων βασίζεται στα ίχνη της δικτυακής κίνησης τα οποία παράγονται στην έξοδο του δικτυακού προσομοιωτή JNS.

Οι παράμετροι εισόδου και το εύρος των τιμών τους που χρησιμοποιήσαμε στο δικτυακό προσομοιωτή JNS δίνονται στον Πίνακα 1.

ΠΑΡΑΜΕΤΡΟΣ	ΤΙΜΗ
Nodes	100 – 300
Area	1000pixel x1000pixel
Placement	Random, Heavy Tail
Hop distance	10 meters
Mobility	Static & Random Waypoint Μέση ταχύτητα 0 – 50km/h
Energy	1KJoule
Simulation time	4000 secs
Network PDU	1024 KBytes
Packet rate	100 packets / sec

Πίνακας 1: Ρύθμιση των τιμών των παραμέτρων στον προσομοιωτή JNS.

5.5.3. Αποτελέσματα Προσομοίωσης

Ακολουθούν τα αποτελέσματα της προσομοίωσης με τον JNS.

5.5.3.1. Σύγκριση του Ρυθμού Μεταβολής των Κόμβων-Αρχηγών

Η Εικόνα 32(α) απεικονίζει το ρυθμό μεταβολής των κόμβων-αρχηγών (“cluster head change rate”) στην περίπτωση που οι τρεις συγκρινόμενοι αλγόριθμοι οργανώνουν σε ομάδες ένα δίκτυο 100 κόμβων. Η κίνηση των κόμβων εξομοιώνεται σύμφωνα με το μοντέλο κίνησης Random Waypoint με μέση ταχύτητα σχετικά μεγάλη και ίση με 50km/h.

Ο συμβολισμός “–R, random” δείχνει ότι η αρχική τοποθέτηση των κόμβων στο επίπεδο ακολουθεί την εκθετική κατανομή (η οποία είναι ασυμπτωτικά ομοιόμορφη) ενώ ο συμβολισμός “–G, group” δηλώνει ότι η αρχική κατανομή των βαθμών συνεκτικότητας των κόμβων ακολουθεί κατανομή “pareto heavy tail” η οποία διακρίνεται από τοπικά αυξημένες συγκεντρώσεις των ad hoc κόμβων (συστάδες).

Στην Εικόνα 32(α) ο ρυθμός μεταβολής των κόμβων-αρχηγών παρουσιάζεται να μεταβάλλεται μη γραμμικά όταν μεταβάλλεται η ακτίνα κάλυψης των ad hoc κόμβων. Συγκεκριμένα, παρουσιάζεται ένα σημείο μη-ευστάθειας των αλγορίθμων ομαδοποίησης (δηλαδή ένα σημείο όπου ο ρυθμός μεταβολής στις καταστάσεις των κόμβων, από απλό μέλος σε αρχηγό και αντίστροφα, γίνεται μέγιστος) όταν οι κόμβοι έχουν ακτίνα κάλυψης ίση με ένα μέτρο.

Στην Εικόνα 32(α) παρατηρούμε ότι για μικρές τιμές της ακτίνας κάλυψης (και ισοδύναμα της ισχύος εκπομπής των ασύρματων κόμβων) η αρχική ad hoc τοπολογία που ευνοεί την απόδοση και των τριών αλγορίθμων είναι η τυχαία κατανομή, με συμβολισμό “-R”. Όπως φαίνεται στην περιοχή αυτή με χαμηλή ισχύ των κόμβων η βέλτιστη απόδοση επιτυγχάνεται από τον LID.

Αντίθετα, για κάλυψη μεγαλύτερη του σημείου μεγίστου ρυθμού (δηλαδή όταν η ακτίνα κάλυψης υπερβαίνει το ένα μέτρο) οι τρεις αλγόριθμοι επαναφέρουν την απόδοσή τους, και μάλιστα σε χαμηλότερο ρυθμό μεταβολής από αυτόν που πέτυχαν για μικρές τιμές της κάλυψης, ενώ η αρχική ad hoc τοπολογία που ευνοεί την απόδοση και των τριών αλγορίθμων στην περιοχή δεξιά του σημείου του ενός μέτρου, δηλαδή για μεγάλες τιμές της ισχύος εκπομπής, είναι η heavy tail κατανομή, συμβολισμός “-G”.

Στην περιοχή λειτουργίας όπου οι κόμβοι είναι ικανοί να εκπέμπουν με μεγαλύτερη ισχύ ο μικρότερος ρυθμός μεταβολής των κόμβων-αρχηγών επιτυγχάνεται από το σταθμισμένο RRA και από τον HD. Ο τελευταίος αλγόριθμος λαμβάνει υπόψη του το βαθμό συνεκτικότητας των κόμβων *d* και μόνο αυτόν στη λήψη απόφασης για τον τοπικό αρχηγό.

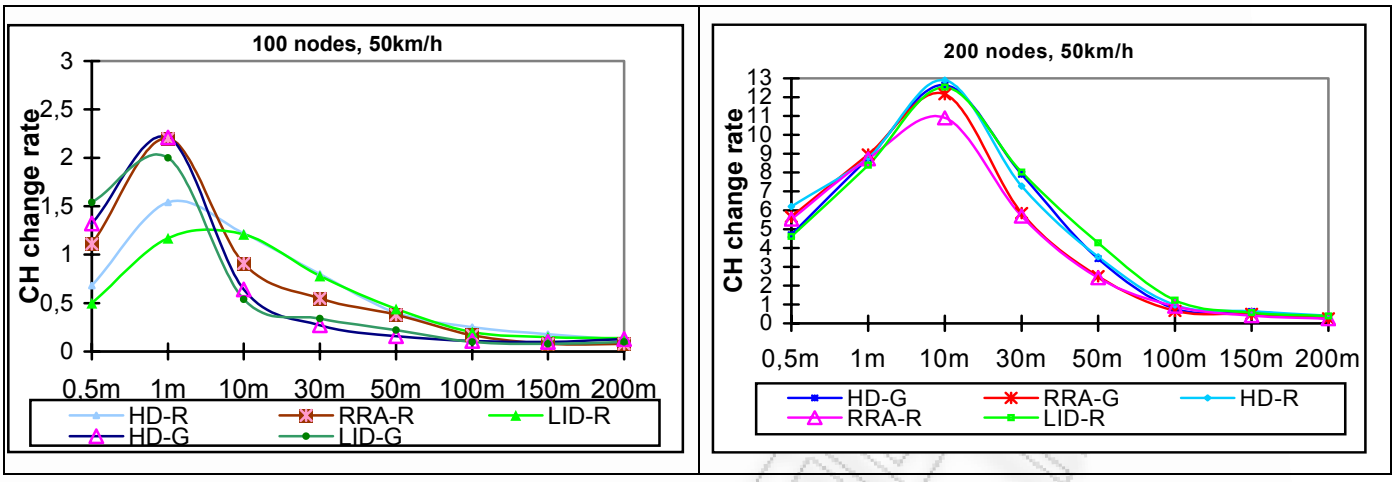
Στη συνέχεια διεξήγαμε μετρήσεις έχοντας αυξήσει τον αριθμό των κόμβων από 100 σε 200 κόμβους, τους οποίους τοποθετήσαμε στην ίδια επιφάνεια των 1000m x 1000m και διατηρώντας το βήμα στο πλέγμα σταθερό, εξομοιώνοντας έτσι ένα πυκνότερο ad hoc δίκτυο. Αρχικά θεωρήσαμε ότι η μέση ταχύτητα κίνησης παραμένει η ίδια όπως και στο αραιό δίκτυο, δηλαδή σχετικά μεγάλη ίση με 50km/h.

Στην Εικόνα 32(β) ο αριθμός των κόμβων έχει αυξηθεί στους 200 κόμβους ενώ η ταχύτητα παραμένει η ίδια -ίση με 50km/h. Παρατηρούμε ότι η μεταβολή του ρυθμού αλλαγής των κόμβων-αρχηγών με την ακτίνα κάλυψης διατηρεί τα ίδια χαρακτηριστικά με αυτά της Εικόνας 32(α) ωστόσο οι απόλυτες τιμές μέτρησης που φαίνονται στην Εικόνα 32 (α) αλλάζουν στην Εικόνα 32(β).

Έτσι, στο πυκνό δίκτυο με 200 κόμβους παρατηρούμε ότι και για τους τρεις αλγορίθμους έχουμε μεγαλύτερους ρυθμούς μεταβολής στις καταστάσεις των κόμβων, σε σχέση με αυτούς που επιτυγχάνουν οι αλγόριθμοι στο αραιό δίκτυο των 100 κόμβων. Αυτό είναι εύλογο αφού με περισσότερους κινούμενους κόμβους οι διελεύσεις νέων κόμβων μέσα στα υπάρχοντα clusters κατά μέσο όρο αυξάνουν με αποτέλεσμα οι αλγόριθμοι clustering να αλλάζουν πιο γρήγορα τους κόμβους-αρχηγούς (“churn rate”) και άρα η ευστάθεια του δικτύου να επηρεάζεται ανάλογα.

Ακόμη, στο πυκνό δίκτυο της Εικόνας 32(β) παρατηρούμε αλλαγή στη θέση όπου συμβαίνει το σημείου μη-ισορροπίας δηλαδή το σημείο όπου οι αλγόριθμοι clustering επιφέρουν τη μέγιστη επιβάρυνση στο δίκτυο. Στην Εικόνα 32 (β) το σημείο αυτό παρουσιάζεται για ακτίνα κάλυψης κατά προσέγγιση ίση με 10 μέτρα έναντι του ενός μέτρου που δείχνει η Εικόνα 32(α).

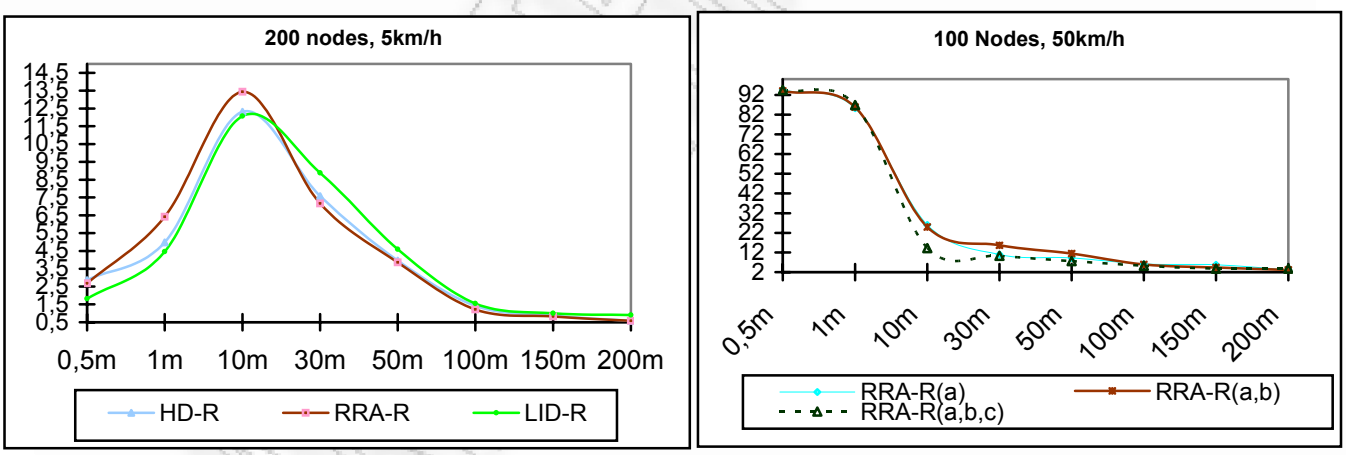
Έτσι σε ένα πυκνό δίκτυο οι κόμβοι θα πρέπει να αυξήσουν την ισχύ τους προκειμένου οι αλγόριθμοι οργάνωσης να διατηρήσουν σταθερή την ευστάθειά τους. Στο πυκνό δίκτυο παρατηρούμε ότι η απόδοση του LID μειώνεται σημαντικά. Αντίθετα η επίδοση του RRA είναι τώρα η βέλτιστη για ακτίνες κάλυψης μεγαλύτερες των 10 μέτρων (μέχρι τα 200 μέτρα).



(α) (β)

Εικόνα 32. Σύγκριση της ευστάθειας των αλγορίθμων σε ένα αραιό και σε ένα πυκνό δίκτυο.

Επιπλέον, παρατηρούμε στην Εικόνα 32(β) ότι η αρχική ad hoc τοπολογία που ευνοεί τον RRA είναι η ομοιόμορφη, "-R", ενώ, όπως και στο αραιό δίκτυο, η αρχική τοπολογία που ευνοεί τον Highest Degree για τις μεγάλες τιμές κάλυψης είναι η κατανομή "heavy tail", δηλαδή η τοποθέτηση των κόμβων κατά ομάδες, συμβολισμός "-G". Η βέλτιστη απόδοση του αλγόριθμου RRA επέφερε κατά 13.8% μικρότερο ρυθμό μεταβολής κόμβων-αρχηγών από ότι ο Highest Degree και κατά 13% μικρότερο ρυθμό μεταβολής στους αρχηγούς που εκλέγει από αυτόν που επέφερε ο αλγόριθμος LID.



(α) (β)

Εικόνα 33. Σύγκριση της ευστάθειας αλγορίθμων clustering σε ένα πυκνό δίκτυο, μέση ταχύτητα 5km/h.

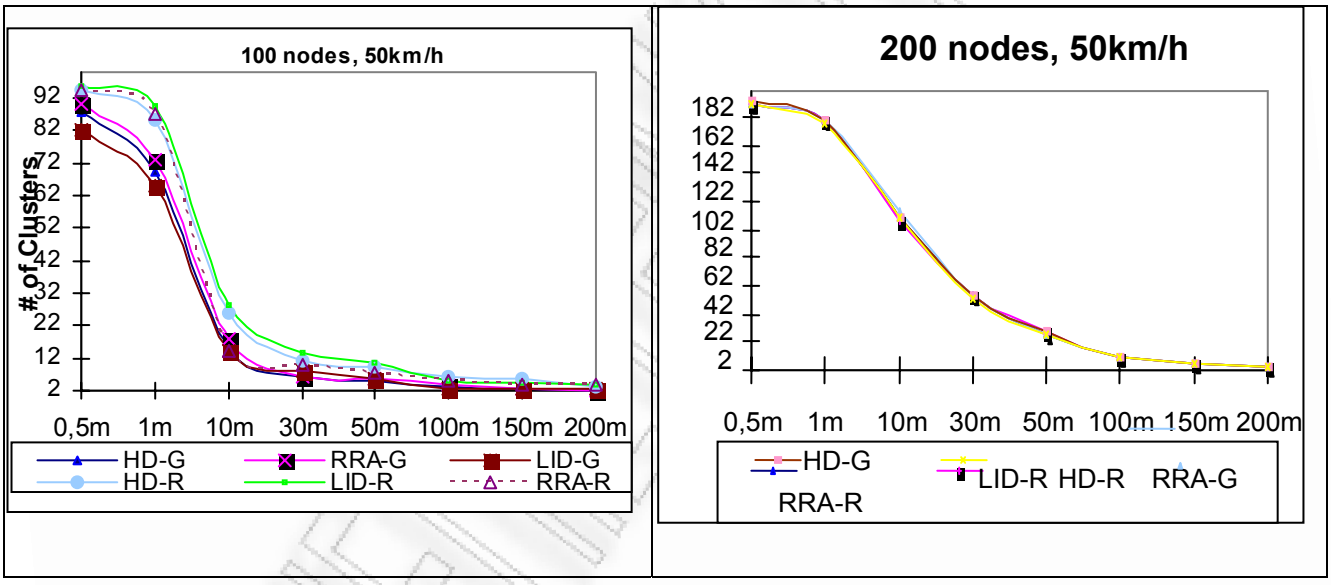
Στο Σχ. 33(α) συγκρίνουμε την ευστάθεια των τριών αλγορίθμων clustering σε ένα πυκνό δίκτυο με 200 κόμβους που έχουν αρχικά ομοιόμορφη κατανομή όταν η μέση ταχύτητα είναι ελαττωμένη και ισούται με 5km/h. Η Εικόνα 33(α) επιβεβαιώνει όσα αναφέραμε παραπάνω, δηλαδή την καλή ευστάθεια των αλγορίθμων RRA και HD για την περίπτωση κόμβων με ικανότητα ισχυρής ραδιο-εκπομπής.

Αν συγκρίνουμε τα αποτελέσματα του πυκνού δικτύου στο Σχ. 33(α), μέσης ταχύτητας 5km/h, με αυτά του πυκνού δικτύου στο Σχ. 32(β) μέσης ταχύτητας 50km/h, συμπεραίνουμε ότι η μείωση της ταχύτητας δεν επέφερε σημαντικές αλλαγές όσον αφορά την ευστάθεια των αλγορίθμων στο πυκνό δίκτυο.

Το Σχ. 33(β) συγκρίνει τον αριθμό των clusters που κατά μέσο όρο δημιουργήθηκαν από τον RRA όταν αυτός λαμβάνει υπόψη μία (το βαθμό συνεκτικότητας *d*), δύο (το βαθμό συνεκτικότητας *d* και τη διαθέσιμη ενέργεια E_{ri}) και τρεις παραμέτρους απόφασης (το βαθμό συνεκτικότητας *d*, τη διαθέσιμη ενέργεια E_{ri} και τη σχετική απόσταση των κόμβων από το μέσο γεωγραφικό κέντρο της γειτονιάς τους - παράμετρος D_i). Παρατηρούμε στο Σχ. 33(β) ότι ο RRA όταν σταθμίζει τρεις παραμέτρους δημιουργεί μικρότερο αριθμό συστάδων για ακτίνες κάλυψης μεγαλύτερες από τα 8 μέτρα. Αυτό δείχνει ότι η προσθήκη της τρίτης παραμέτρου D_i στη λήψη απόφασης κάνει την οργάνωση σε συστάδες πιο αποδοτική καθώς μια δομή που αποτελείται από λιγότερα clusters μπορεί να διατηρηθεί και να διαχειριστεί πιο αποδοτικά από τους ad hoc κόμβους. Αυτό ήταν αναμενόμενο αφού λόγω της τρίτης παραμέτρου που σταθμίζει ο RRA αποφεύγει να επιλέξει ως αρχηγούς τους περιφερειακούς, απομονωμένους και ακάλυπτους κόμβους, κάτι το οποίο θα αύξανε δραματικά τον αριθμό των συστάδων που δημιουργούνται.

5.5.3.2. Σύγκριση του Αριθμού των Παραγόμενων Ομάδων

Η Εικόνα 34(α) απεικονίζει τον αριθμό των συστάδων που κατά μέσο όρο δημιουργήθηκαν από τους συγκρινόμενους αλγόριθμους κατά τη διάρκεια των επαναλήψεων της διαδικασίας συσταδοποίησης στον JNS με σύνολο κόμβων 100 οι οποίοι κινούνται ταχέως.



(α) **(β)**

Εικόνα 34. Σύγκριση του αριθμού των παραγόμενων ομάδων από τους αλγορίθμους, μέση ταχύτητα 50km/h.

Παρατηρούμε στην Εικόνα 34(α) ότι για την περίπτωση που οι κόμβοι εκπέμπουν σε ακτίνα μεγαλύτερη των 30 μέτρων ο RRA είναι αποδοτικός εφόσον καταφέρνει να μειώσει στο ελάχιστο τον αριθμό των clusters που παράγει και τη βέλτιστη απόδοση την επιτυγχάνει όταν αρχικά οι κόμβοι είναι τοποθετημένοι σε ομάδες, συμβολισμός "-G". Έτσι για τον αλγόριθμο RRA ο αριθμός των clusters είναι μικρότερος με την τοποθέτηση "heavy tail" από τον αριθμό clusters που παράγονται με την ομοιόμορφη κατανομή των κόμβων, συμβολισμός "-R".

Για την περίπτωση που οι κόμβοι εκπέμπουν σε ακτίνα μικρότερη των 30 μέτρων, δηλαδή όταν ουσιαστικά δεν υπάρχουν ισχυροί δεσμοί μεταξύ των κόμβων ο LID είναι ο πιο αποδοτικός αλγόριθμος εφόσον παράγει το μικρότερο αριθμό από συστάδες, όπως φαίνεται στην Εικόνα 34(α). Αυτό οφείλεται στο γεγονός ότι ο LID δε λαμβάνει καθόλου υπόψη τα χαρακτηριστικά της συνεκτικότητας μεταξύ των κόμβων, ενώ οι RRA και LID εξαρτούν την απόφασή τους κατά την επιλογή αρχηγού από τη συνεκτικότητα των υποψήφιων κόμβων. 'Ετσι είναι εύλογο σε ένα χαλαρά συνδεδεμένο δίκτυο ο LID να υπερτερεί, γεγονός που οφείλεται στη σειρά με την οποία τα

δεδομένα του γράφου (δηλαδή οι ταυτότητες των κόμβων) εξετάζονται από τον αλγόριθμο.

Η Εικόνα 34(β) απεικονίζει τον αριθμό των συστάδων που κατά μέσο όρο δημιουργήθηκαν στην περίπτωση 200 κόμβων που κινούνται ταχέως. Παρατηρούμε ότι η διαφορά της επίδοσης των αλγορίθμων (ως προς το μέτρο του αριθμού των συστάδων) είναι πολύ μικρή καθώς αυξάνεται η ταχύτητα. Από την άλλη μεριά, όπως αναμένεται, ο αριθμός των διακριτών συστάδων που παράγονται στο πυκνό δίκτυο είναι μεγαλύτερος από τους αντίστοιχους στο αραιό δίκτυο.

5.5.3.3. Σύγκριση της Ευρωστίας των Αλγορίθμων Ομαδοποίησης

Εκτός από τα παραδοσιακά μέτρα εκτίμησης και σύγκρισης της επίδοσης των αλγορίθμων clustering οι εκτεταμένες προδιαγραφές λειτουργικότητας και ασφαλείας που είδαμε στο Κεφάλαιο 2 μας αναγκάζουν να μελετήσουμε και πρόσθετα μέτρα αξιολόγησης. Ιδιαίτερα θα πρέπει να εισάγουμε τέτοια μέτρα που να αξιολογούν την ευρωστία των αλγορίθμων, δηλαδή το βαθμό αξιοπιστίας στη μετάδοση των μηνυμάτων από άκρη σε άκρη και στο βαθμό της διαθεσιμότητας του δικτύου και των υπηρεσιών που προκύπτει μετά την εφαρμογή των αλγορίθμων αυτό-οργάνωσης.

5.5.3.3.1. Σύγκριση της Αξιόπιστης Παράδοσης Μηνυμάτων

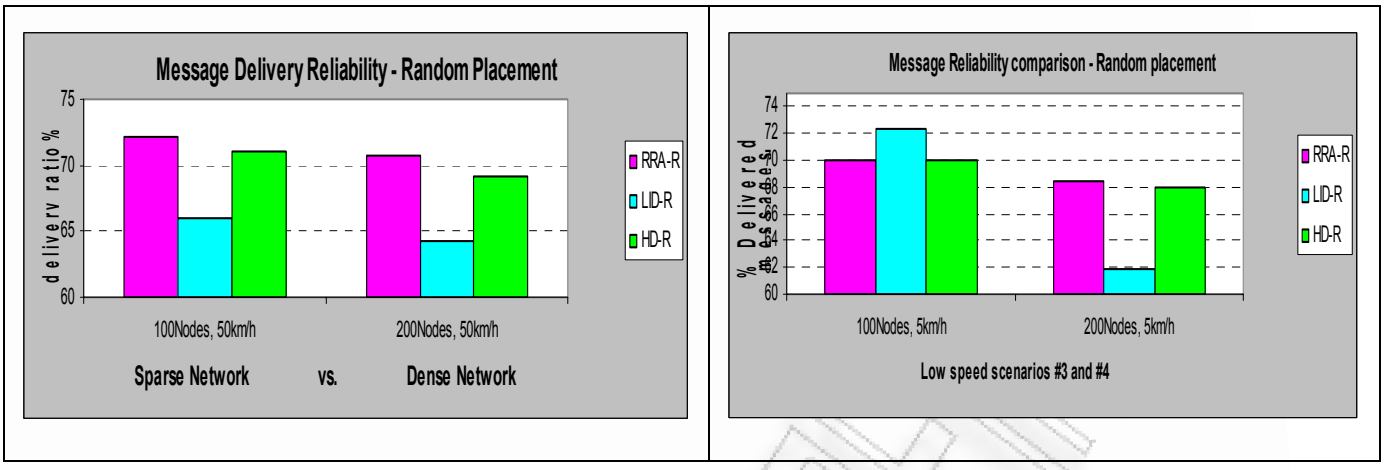
Μας ενδιαφέρει να αξιολογήσουμε την επίδραση των αλγορίθμων clustering στις ad hoc επικοινωνίες. Υπολογίσαμε το ποσοστό αξιόπιστης παράδοσης των μηνυμάτων με το να προσομοιώσουμε στον JNS μια μικτή κίνηση για κάθε ζεύγος πηγής - προορισμού η οποία προέρχεται από συνδέσεις με το πρωτόκολλο μεταφοράς Simple GoBackN (SGN) και από πακέτα datagram που φέρουν πληροφορία πακέτων UDP. Ο δείκτης αξιόπιστης μεταφοράς αυτών της μικτής κίνησης υπολογίστηκε σύμφωνα με την Εξίσωση (15):

$$\text{Αξιοπιστία} = 1 - \text{Mean}\left(\frac{\#\text{of dropped messages}}{\text{total}\#\text{of messages sent}}\right) \qquad (15)$$

Επιπλέον μας ενδιαφέρει να αξιολογήσουμε την επίδραση της ad hoc τοπολογίας στο ποσοστό των συνολικών μηνυμάτων που αξιόπιστα παραδίδονται στον τελικό προορισμό. Στο Σχ. 35(α) απεικονίζεται η απόδοση των τριων αλγορίθμων στην περίπτωση που η τοποθέτηση των κόμβων γίνεται με το εκθετικό μοντέλο. Παρατηρούμε ότι τόσο στο αραιό δίκτυο των 100 κόμβων όσο και στο πυκνό δίκτυο των 200 κόμβων ο RRA είναι ο πιο αξιόπιστος και αυτό ισχύει για μεγάλη μέση ταχύτητα ίση με 50km/h.

Στο Σχ. 35(β) οι αλγόριθμοι συγκρίνονται ως προς το ποσοστό των μηνυμάτων που παραδόθηκαν αξιόπιστα στον τελικό προορισμό για τις δύο βασικές διαφορετικές τοποθετήσεις των κόμβων για μικρότερη κινητικότητα των κόμβων. Στο Σχ. 35(α) η κινητικότητα των κόμβων είναι υψηλή ίση με 50km/h ενώ στο 35(β) κάτω από τις ίδιες συνθήκες μειώσαμε την ταχύτητα στα 5km/h.

Παρατηρήσαμε ότι ο LID επιτυγχάνει καλή απόδοση αξιοπιστίας στην περίπτωση που το δίκτυο είναι αραιό και η ταχύτητα μικρή, δηλαδή ο αλγόριθμος LID είναι αποδεκτός σε ομαλές συνθήκες. Επίσης παρατηρούμε στην Εικόνα 36(α) ότι σε ένα πυκνό δίκτυο με 200 κόμβους και κίνηση με μικρή ταχύτητα η αξιοπιστία στη μετάδοση αυξάνεται όταν οι κόμβοι τοποθετούνται κατά ομάδες παρά όταν αναπτύσσονται τυχαία στο πλέγμα.



Εικόνα 35. Σύγκριση της αξιοπιστίας των αλγορίθμων clustering.

Μεγαλύτερο ποσοστό αξιοπιστίας (περίπου πάνω από 70%) σε όλες αυτές τις περιπτώσεις επιτεύχθηκε από τον RRA, ακολουθούμενος από τον HD και τον LID. Στον Πίνακα 2 συνοψίζουμε τα πειραματικά αποτελέσματα σχετικά με την ευρωστία των αλγορίθμων για τις τέσσερις περιπτώσεις συνθηκών που μελετήσαμε στο ad hoc δίκτυο. Οι τιμές που παρουσιάζονται αποτελούν τους μέσους όρους που υπολογίστηκαν μετά από 100 επαναλήψεις για κάθε αλγόριθμο και για κάθε σενάριο δικτυακών συνθηκών. Το βέλτιστο ποσοστό επιτεύχθηκε από τον RRA (77.9%).

Σύγκριση Αξιοπιστίας **Δικτυακές Συνθήκες**	**Μοντέλο Τοποθέτησης Ad Hoc**	
	Random	**Heavy Tail**
#1(100 nodes, 50km/h)	$RRA^{72.2\%}$	$RRA^{77.9\%}$
#2(200 nodes, 50km/h)	$RRA^{70.75\%}$	$RRA^{73.2\%}$
#3(100 nodes, 5km/h)	$LID^{72.4\%}$	$RRA^{68.9\%}$
#4(200 nodes, 5km/h)	$RRA^{68.4\%}$	$RRA^{70..3\%}$

Πίνακας 2. Συγκριτικά αποτελέσματα της αξιοπιστίας των αλγορίθμων RRA, HD και LID.

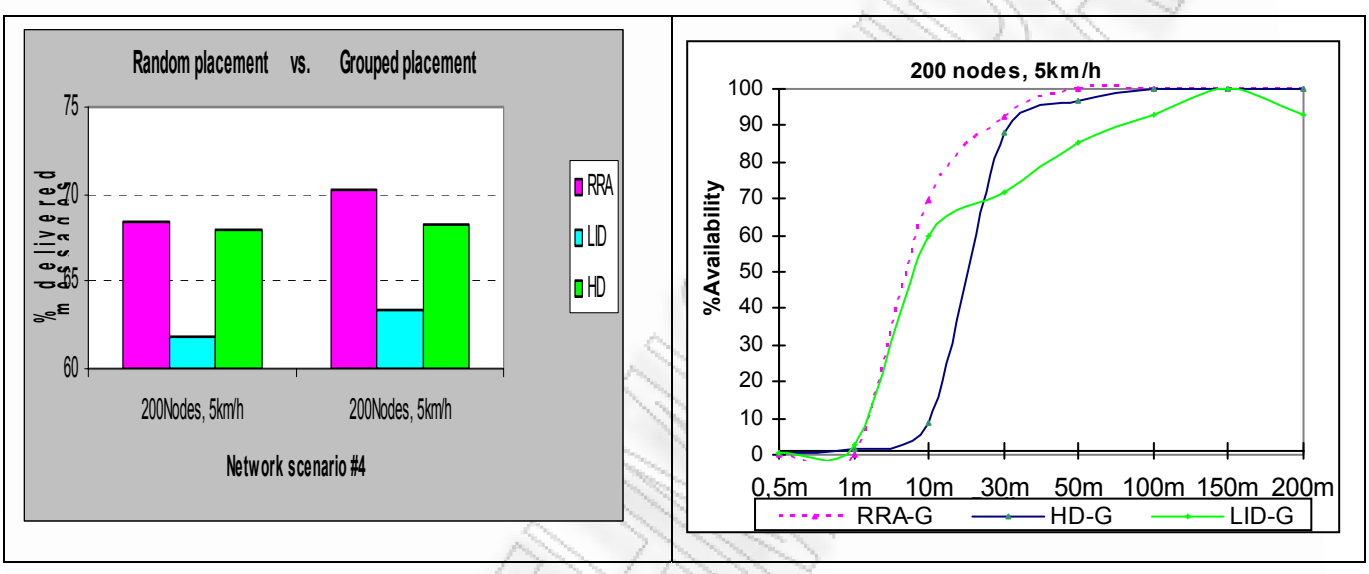
5.5.3.3.2. Σύγκριση της Διαθεσιμότητας των Αρχηγών

Στην Εικόνα 36(β) απεικονίζεται σύγκριση του ποσοστού διαθεσιμότητας των κόμβων-αρχηγών που εκλέγουν οι τρεις αλγόριθμοι. Είναι αναγκαίο οι υπηρεσίες-κόμβοι του δικτύου ad hoc να είναι πραγματικά διαθέσιμες όποτε κάτι τέτοιο είναι επιθυμητό. Έτσι, θα πρέπει ο κόμβος που εκλέγεται να έχει το απαραίτητο απόθεμα ενέργειας για να επιτελέσει τα καθήκοντα του ρόλου του αρχηγού. Αποτελεί η επιτυχία σε αυτό το μέτρο, δηλαδή οι κόμβοι-μέλη να έχουν στο περισσότερο ποσοστό του χρόνου διαθέσιμες τις υπηρεσίες του αρχηγού τους, ένδειξη της πολύ καλής αποδοτικότητας ενός αλγορίθμου ομαδοποίησης.

Παρατηρούμε στην Εικόνα 36(β) την μεταβολή του ποσοστού διαθεσιμότητας των cluster heads

σαν συνάρτηση της ακτίνας ραδιο-κάλυψης των κόμβων, όταν η αρχική τοποθέτηση των κόμβων είναι ομαδοποιημένη (“G”).

Όσο αυξάνεται η ισχύς εκπομπής η διαθεσιμότητα των κόμβων-αρχηγών και για τους τρείς αλγορίθμους αυξάνεται. Ωστόσο πιο γρήγορα ανέρχεται η καμπύλη RRA επιτυγχάνοντας μάλιστα και τα υψηλότερα ποσοστά διαθεσιμότητας. Αυτό δικαιολογείται από το γεγονός ότι μόνο ο RRA από τους τρεις αλγορίθμους υπολογίζει και τη διαθέσιμη ενέργεια των κόμβων στη λήψη απόφασης.



(α) **(β)**

Εικόνα 36. Σύγκριση του ποσοστού μετάδοσης μηνυμάτων και του ποσοστού της διαθεσιμότητας των αρχηγών που εκλέγονται από τους τρεις αλγορίθμους σε ένα πυκνό δίκτυο.

5.6. ΣΥΜΠΕΡΑΣΜΑΤΑ

Σε αυτό το Κεφάλαιο μελετήσαμε τους αλγόριθμους συσταδοποίησης ως μια λύση για την οργάνωση και τη διαχείριση του δικτύου ad hoc ιδιαίτερα αποδοτική όταν η πυκνότητα αυτού αυξάνεται. Προτείναμε ένα γενικό σταθμισμένο αλγόριθμο επιλογής αρχηγού (τον αλγόριθμο RRA) και συγκρίναμε την επίδοση του αλγορίθμου αυτού με άλλους δυο γενικούς αλγόριθμους συσταδοποίησης (τον LID και τον Highest Degree). Μελετήσαμε τη συμπεριφορά των τριών αλγορίθμων κάτω από διαφορετικές δικτυακές συνθήκες που σχετίζονται με πιθανοκρατικούς παράγοντες επίδοσης όπως η τοπολογία του δικτύου και η ταχύτητα των κόμβων. Δείξαμε ότι η αρχική τοποθέτηση των κόμβων με διαφορετικούς τρόπους είναι δυνατόν να επηρεάσει την επίδοση των αλγορίθμων.

Στα πειράματα που διεξήχθησαν ο RRA βρέθηκε πιο ευσταθής από τους δύο αλγόριθμους, LID και HD στην περίπτωση που η ισχύς εκπομπής και συνεπώς η κάλυψη των κόμβων ήταν μεγάλη. Αυτό διακαιλογείται από την επιλογή των παραμέτρων *a*, *b* και *c* που χρησιμοποιεί ο αλγόριθμος RRA για τη λήψη απόφασης. Ειδικότερα, στα πειράματα προσομοίωσης ευνοήσαμε την επιλογή των κόμβων που έχουν μεγάλο βαθμό συνεκτικότητας παρά εκείνους τους κόμβους που έχουν μεγαλύτερα αποθέματα ενέργειας δίνοντας μεγαλύτερο βάρος *a* σε σχέση με το βάρος *b* το οποίο σταθμίζει την ενέργεια των κόμβων. Αυτή η επιλογή των συντελεστών βάρους ευνόησε τους ισχυρούς κόμβους με πολλούς γείτονες και είχε ως αποτέλεσμα στην περίπτωση που το δίκτυο είναι πυκνό η ευστάθεια του RRA να είναι βέλτιστη, δηλαδή ο ρυθμός μεταβολής των κόμβων – αρχηγών να είναι ο μικρότερος με τον αλγόριθμο RRA. Μια τέτοια παραμετροποίηση ταιριάζει, για

παάδειγμα, σε μια στρατιωτική εφαρμογή με διακριτά επίπεδα ιεραρχιών μέσα σε ένα πυκνό πεδίο ad hoc κόμβων.

Στην περίπτωση όπου το δίκτυο είναι αραιό (για παράδειγμα σε μια οικιακή ad hoc εφαρμογή) η ενέργεια των κόμβων είναι μεγαλύτερης σημασίας για τη διατήρηση της συνεκτικότητας του δικτύου και την παράδοση των μηνυμάτων με αξιοπιστία. Συνεπώς, διατηρώντας την παραπάνω ρύθμιση των παραμέτρων *a*, *b* και *c* και για το αραιό δίκτυο ο RRA είχε χειρότερη επίδοση και αυτό έγινε φανερό στα πειράματα προσομοίωσης κατά την περίπτωση όπου η ισχύς εκπομπής των ασύρματων κόμβων κυμάνθηκε σε μικρό εύρος τιμών.

Ακόμη διαπιστώσαμε ότι η διαθεσιμότητα των αρχηγών που επιλέγει ο RRA σε σχέση με τους δύο αλγόριθμους είναι αισθητά μεγαλύτερη, εφόσον λαμβάνει υπόψη τόσο την τοπολογία όσο και την ενέργεια των κόμβων. Αυτό είναι σημαντικό για τη διαθεσιμότητα των δικτυακών υπηρεσιών εφόσον τα μηνύματα παραδίδονται αξιόπιστα μέσω των διαθέσιμων κόμβων-αρχηγών που επιλέγει ο εύρωστος στις τυχαίες μεταβολές των δικτυακών συνθηκών αλγόριθμος RRA.

5.7. ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Lucas, G., Ghose, A., Chuang, J. “On Characterizing Affinity and its Impact on Network Performance”. Proceedings of the ACM SIGCOMM 2003 Workshops, Karlsruhe, Germany, August 2003, pp 65-75.

[2] Tilak, S., Abu-Ghazaleh, N., B., and Heinzelman, W. “Infrastructure Tradeoffs for Sensor Networks”. WSNA’02, Atlanta, Georgia, USA, September 28, pp 49-58.

[3] Lao, L., Cui, J-H., and Gerla, M. “A framework for realistic and systematic multicast performance evaluation”. Elsevier, Computer Networks, Special Issue on Network Modelling and Simulation, vol. 50, Issue 12, 2006, pp. 2054-2069.

[4] Faloutsos, M., Faloutsos, P., and Faloutsos, C. “On power-law relationships of the Internet topology”. In Proceedings of the ACM SIGCOMM, Cambridge, MA, USA, 1999, pp 251-262.

[5] Tangmunarunkit, H., Govindan, R., Jamin, S. “Network topology generators: degree-based vs. structural”. In Proc of the ACM SIGCOMM, Pittsburgh, Pennsylvania, USA, August 2002, pp 147-159.

[6] J. C.-I. Chuang and M. Sirbu. “Pricing Multicast Communication: A Cost-Based Approach”. In: Proceedings of the Internet Society INET98 Conference, July 1998.

[7] Barabasi, A., L., Albert, R. “Emergence of scaling in random networks”. Science, 286(5439), Oct. 1999, pp. 509-512.

[8] Réka, A., Hawoong, J. & Albert-László, Barabasi. “Error and attack tolerance of complex networks”. Nature, vol. 406, 2000, pp. 378-381.

[9] Beygelzimer, A., Grinstein, G., Linsker, R., Rish, I. “Improving Network Robustness”. Proceedings of the International Conference on Automatic Computing (ICAC ‘04).

[10] Calvert, K., Doar, M., B., and Zegura, E., W. Modeling Internet Topology. IEEE Communications Magazine, June 1997, pp. 160-163.

[11] Waxman, B., M. “Routing of multipoint connections”. IEEE Journal on Selected Areas in Communications 6 (9), 1988.

[12] TIERS. http://www.isi.edu/haldar/topogen/tiers.

[13] K. Calvert, E. Zegura, S. Bhattacharjee. “How to Model and Internet work”. In: Proceedings of the IEEE INFOCOM, June 2002.

[14] Medina, A., Matta, I., and Byers, “J. BRITE: A flexible generator of internet topologies”. Technical Report 2000-005, CS Department, Boston University, Jan. 21, 2000.

[15] Feng Xue, P. R Kumar, “The number of neighbors needed for connectivity of wireless networks”. Wireless Networks, Vol. 10, Number 2, 2004, pp.169-181.

[16] Java Network Simulator (JNS), <http://jns.sourceforge.net>.

[17] Chandrakasan, A., Heinzelman, W., R., Balakrishnan, H. “Energy-efficient communication protocol for wireless micro sensor networks”. In the 33rd annual Hawaii International Conference on System Sciences, HICSS, page 30053014, 2000.

[18] Ephremides, A., Anthony, J., E., Baker, D., J. “A design concept for reliable mobile radio networks with frequency hopping signaling”. Proc. IEEE 1987, Vol. 75, no. 1, Jan. 1987, pp 56-73.

[19] Gerla, M., Tsai, JTC. “Multicluster, mobile, multimedia radio network”. ACM-Baltzer J Wireless Networks, 1995; Vol. 1, pp 255-265.

[20] Basagni, S. “Distributed clustering for ad hoc networks”. Proceedings of the International Symposium on Parallel Architectures, Algorithms and Networks, (I-SPAN’99), Perth/Fremantle. June 1999, pp. 310-315.

[21] El-Bazzal, Z., Kadoch, M., Agba, B. L., Gagnon, F., and Bennani, M. “An Efficient Management Algorithm for Clustering in Mobile Ad Hoc Network”. PM2HW2N’06 Torremolinos, Malaga, Spain, October 6, 2006.

[22] Basu, P., Kham N., Little, T. D. C. A. “Mobility Based Metric for Clustering in Mobile Ad Hoc Networks”. International Conference on Distributed Computing Systems Workshop, Apr. 2001.

[23] Chiang C. C., Wu, H. K., Liu, W., Gerla, M. “Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel”. Proc IEEE SICON, Singapore, 1996.

[24] Taniguchi, H., Inoue, M., Masuzawa, T., and Fujiwara, H. “Clustering Algorithms in Ad Hoc Networks”. Electronics and Communications in Japan, Part 2, Vol. 88, No. 1, 2005, pp 51-59.

[25] A. A. Abbasi, M. Younis. “A survey on clustering algorithms for wireless sensor networks”. In: Elsevier Computer Communications, Vol. 30, pp. 2826-2841, 2007.

[26] J. Y. Yu and P. H. J. Chong. “A Survey of Clustering Schemes for Mobile Ad Hoc Networks”. IEEE Communications Surveys and Tutorials, Vol. 7, No. 1, pp. 32-48, 2005.

[27] http://jns.sourceforge.net/

[28] Raquel A.F. Mini, Antonio A.F. Loureiro. “Energy in Wireless Sensor Networks”. In: Chapter 1, “Middleware for Network Eccentric and Mobile Applications”, Springer, Editors Benoît Garbinato, Hugo Miranda, Luís Rodrigues.

[29] M. Chatterjee, S. K. Das, D. Turgut. “WCA: A Weighted Clustering Algorithm for Mobile Ad Hoc Networks”, Cluster Computing Journal, Vol. 5, no. 2, Apr. 2002, pp. 193-204.

6. ΛΥΣΗ ΠΡΟΣΤΑΣΙΑΣ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ AD HOC

Σαν δεύτερη βασική ιδιότητα των αυτόνομων δικτύων καθορίζουμε την ικανότητα της *αυτο-προστασίας* που είναι θεμιτό να επιτυγχάνεται μέσα από μηχανισμούς πρόληψης ("prevention"), ανίχνευσης ("detection"), αντιμετώπισης ("response") και ανάκαμψης ("recovery") από τις πιθανές επιθέσεις και τις απειλές που προέρχονται από κακόβουλους κόμβους που εισβάλλουν στο δίκτυο.

Οι μηχανισμοί προστασίας πρέπει να αποτελούν γραμμές άμυνας για την αντιμετώπιση των στοχευμένων επιθέσεων οι οποίες απειλούν τα ευαίσθητα δεδομένα και επίσης απειλούν εκείνους τους κόμβους που αναλαμβάνουν σημαντικό ρόλο στη διεξαγωγή των επικοινωνιών του δικτύου ad hoc.

Η προστασία των κόμβων ad hoc με ίδια μέσα είναι απαραίτητη εφόσον το δίκτυο στις περισσότερες των περιπτώσεων δεν υποβοηθείται από κάποια "on line" κεντρική αρχή όπως οι Αρχές Πιστοποίησης (Certificate Authorities, CA) ή από κάποια κεντρική υπηρεσία ασφάλειας η οποία να διαχειρίζεται τα κλειδιά κρυπτογράφησης, ή εν τέλει από κάποιο εξωτερικό σύστημα ανίχνευσης επιθέσεων, έγερσης συναγερμών και προστασίας των κόμβων. Παρόμοιες λειτουργίες πρέπει να εισάγονται στο δίκτυο ad hoc με τρόπο που να είναι συμβατός με τις ιδιαιτερότητές του.

Η λύση αυτο-προστασίας που θα περιγραφεί στο παρόν Κεφάλαιο έχει ακριβώς σκοπό να προστατεύσει το αποτέλεσμα των μηχανισμών της αυτο-οργάνωσης που εισαγάγαμε στο προηγούμενο Κεφάλαιο με πρόσθετους μηχανισμούς ελέγχου οι οποίοι ενσωματώνονται στους κόμβους και οι οποίοι επιτυγχάνουν την προστασία από εισβολείς με βάση έναν αριθμό από διακριτά κατώφλια ασφάλειας.

Αρχικά παρουσιάζουμε ένα μοντέλο αναφοράς που παρέχει τα απαιτούμενα ποιοτικά χαρακτηριστικά για την επίτευξη της αυτονομίας στα δίκτυα ad hoc. Ειδικότερα, θεωρούμε ότι οι επιμέρους συνιστώσες που μπορούν να θεμελιώσουν την *ασφαλή αυτο-οργάνωση* των δικτύων ad hoc μπορούν να βασιστούν τόσο σε κρυπτογραφικές όσο και σε μη κρυπτογραφικές μεθόδους προστασίας. Οι κρυπτογραφικές μέθοδοι θα μας απασχολήσουν σε σχέση με την παραγωγή και με την ανταλλαγή δυναμικών κλειδιών κρυπτογράφησης και την αυθεντικοποίηση μεταξύ των κόμβων.

Οι μη κρυπτογραφικές μέθοδοι προστασίας θεωρούμε πως πρέπει να βασίζονται στις αρχές των κατανεμημένων αλγορίθμων ελέγχου των δικτύων, οι οποίες μπορούν να εφαρμοστούν στο περιβάλλον των ασύρματων κινητών δικτύων ad hoc με τις κατάλληλες προσαρμογές -όπου αυτό είναι σκόπιμο- και μπορεί να είναι μέθοδοι εύρωστης στατιστικής ανάλυσης των ανωμαλιών, συνεργατικές μέθοδοι όπως η θεωρία παιγνίων και τα σχήματα κατωφλίου καθώς και σχήματα υπολογισμού και αξιολόγησης του βαθμού (επιπέδων) εμπιστοσύνης των κόμβων. Ακόμη είναι σημαντικό οι μηχανισμοί προστασίας να μην αφήνουν χωρίς ασφάλεια τα κατώτερα επίπεδα της αρχιτεκτονικής των ad hoc δικτύων γιατί τότε οι κακόβουλοι κόμβοι μπορούν εύκολα να πλήξουν το σύστημα κατά τρόπο ανάλογο με τις επιθέσεις εναντίον των αδυναμιών των λειτουργικών συστημάτων.

Στη συνέχεια προτείνουμε μια ολοκληρωμένη δικτυακή λύση οργάνωσης και προστασίας για την ταυτόχρονη βελτιστοποίηση της δικτυακής απόδοσης αλλά και του βαθμού προστασίας από τις επιθέσεις έχοντας θέσει σα στόχο τη βελτίωση της επιβιωσιμότητας των δικτύων ad hoc και την ικανοποίηση των ποιοτικών χαρακτηριστικών του μοντέλου αναφοράς που θα περιγραφεί παρακάτω.

6.1. ΕΙΣΑΓΩΓΗ

Οι αλγόριθμοι συσταδοποίησης όταν εφαρμόζονται στα ασύρματα ad hoc δίκτυα έχουν σαν αποτέλεσμα τη δημιουργία ιεραρχικών δομών όπου οι κόμβοι αναλαμβάνουν διακριτούς ρόλους.

Για παράδειγμα, σε μια δομή δύο επιπέδων οι κόμβοι εναλλάσσουν την κατάστασή τους από απλά μέλη σε κόμβους-αρχηγούς και αντίστροφα. Οι κόμβοι-αρχηγοί διαχειρίζονται τη συμμετοχή στην ομάδα και διαχειρίζονται τους πόρους του ραδιοφάσματος, όπως τα διαθέσιμα κανάλια τα οποία μοιράζονται οι κόμβοι με μεθόδους πολυπλεξίας όπως TDMA ή/και CDMA. Με την εισαγωγή των επιπέδων ιεραρχίας στη δομή του δικτύου ad hoc είναι δυνατόν να αντιμετωπιστούν αποδοτικότερα πολλά προβλήματα όπως το πρόβλημα της κατανάλωσης των διαθέσιμων πόρων όπως μνήμη, επεξεργαστική ισχύς, ενέργεια, εύρος ζώνης, πρόβλημα το οποίο εντείνεται όταν ο αριθμός των κόμβων αυξάνεται.

Επιπλέον, με τους κόμβους-αρχηγούς και την ενδο-δικτυακή επεξεργασία και τη συγκέντρωση των δεδομένων που επιτελείται από αυτούς η διάρκεια ζωής του δικτύου και των κόμβων επιμηκύνεται εφόσον οι μεταδόσεις ενεργοποιούνται μόνο για εκείνα τα δεδομένα που είναι χρήσιμα. Περαιτέρω, λειτουργίες και διαδικασίες που σχετίζονται με την ασφάλεια του δικτύου ad hoc εμπίπτουν στη δικαιοδοσία των κόμβων-αρχηγών παρά στα απλά μέλη των ομάδων. Οι λειτουργίες προστασίας που εκτελούνται στους αρχηγούς περιλαμβάνουν την αυθεντικοποίηση των κόμβων, την αποκρυπτογράφηση των μηνυμάτων, τη διαχείριση των κλειδιών της ομάδας δηλαδή την ανανέωση με κλειδιά για νέους κόμβους και τη διαγραφή των κλειδιών των κόμβων που εγκαταλείπουν την ομάδα και, τέλος, την ανίχνευση των εισβολέων και την αντιμετώπιση των επιθέσεων [2].

Ωστόσο διάφοροι παράγοντες όπως η τυχαία κίνηση των κόμβων, τα χαρακτηριστικά μετάδοσης του ασύρματου καναλιού που πολλές φορές προκαλούν την πτώση και τη μείωση της ποιότητας των ασύρματων ζεύξεων, οι απρόβλεπτες πτώσεις των κόμβων λόγω έλλειψης ενέργειας και άλλοι τυχαίοι παράγοντες έχουν σαν αναπόφευκτο αποτέλεσμα τις συχνές αλλαγές των κόμβων-αρχηγών, μια διαδικασία που ονομάζεται επαναομαδοποίηση (“re-clustering”).

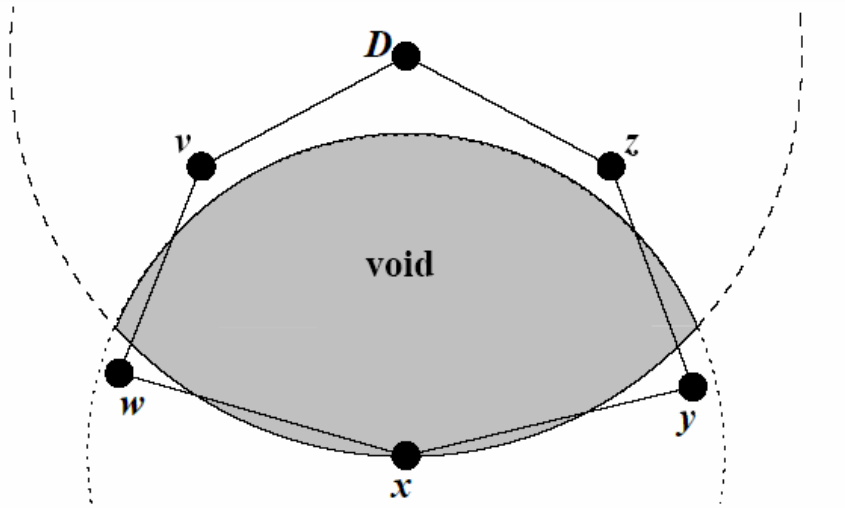
Η δυναμική επαναομαδοποίηση των κόμβων επιφέρει επιβάρυνση στις επικοινωνίες του δικτύου ad hoc. Αυτό συμβαίνει διότι απαιτεί την ανταλλαγή επιπλέον μηνυμάτων για την ενημέρωση των κόμβων κατά την εγκατάσταση της νέας ιεραρχικής δομής. Κατά συνέπεια, η επίδοση του δικτύου και η λειτουργία των εφαρμογών τελικού χρήστη επηρεάζεται από τις συχνές αλλαγές στους ρόλους των κόμβων. Έτσι πολλές φορές οι μεταβαλλόμενες ιεραρχικές δομές σε ένα δυναμικό περιβάλλον είναι δύσκολο να συντηρούνται, εκτός εάν οι αλγόριθμοι και τα πρωτόκολλα αυτο-οργάνωσης έχουν σχεδιαστεί με αποδοτικό τρόπο [1].

Στην πρόταση που θα περιγράψουμε αναλυτικά παρακάτω θα εστιάσουμε στην επίτευξη της αποδοτικής αυτο-οργάνωσης και αυτο-προστασίας των ad hoc δικτύων. Για αυτό το σκοπό θα σχεδιάσουμε και θα αναπτύξουμε ένα σχήμα ασφαλούς επαναομαδοποίησης των κόμβων που τρέχει πάνω από ένα γεωγραφικό ad hoc πρωτόκολλο. Επιλέξαμε ένα γεωγραφικό πρωτόκολλο για το ad hoc δίκτυο διότι με τα γεωγραφικά πρωτόκολλα η απόφαση δρομολόγησης στηρίζεται στη θέση των κόμβων και έτσι δεν απαιτείται πλημμύρα του δικτύου με μηνύματα εύρεσης του μονοπατιού προς τον τελικό προορισμό όπως γίνεται στα γνωστά ad hoc πρωτόκολλα πλημμύρας όπως είναι το AODV, το DSR κ.α.

Το προτεινόμενο σχήμα προστασίας επεκτείνει το γεωγραφικό πρωτόκολλο Greedy Perimeter Stateless Routing (GPSR) [3] με πολλά λειτουργικά τμήματα που προσφέρουν ασφάλεια. Το GPSR (δες και §3.6.5.1 για μια σύντομη περιγραφή του πρωτοκόλλου GPSR) έχει εκτενώς μελετηθεί στη βιβλιογραφία και έχει πολλά πλεονεκτήματα όπως τοπικές ανταλλαγές μηνυμάτων, λαμβάνει υπόψη την τοπολογία του δικτύου, είναι δυνατόν να υποστηρίξει μεγάλα δίκτυα και τέλος είναι ανεξάρτητο και ουδέτερο από τις εφαρμογές τελικού χρήστη.

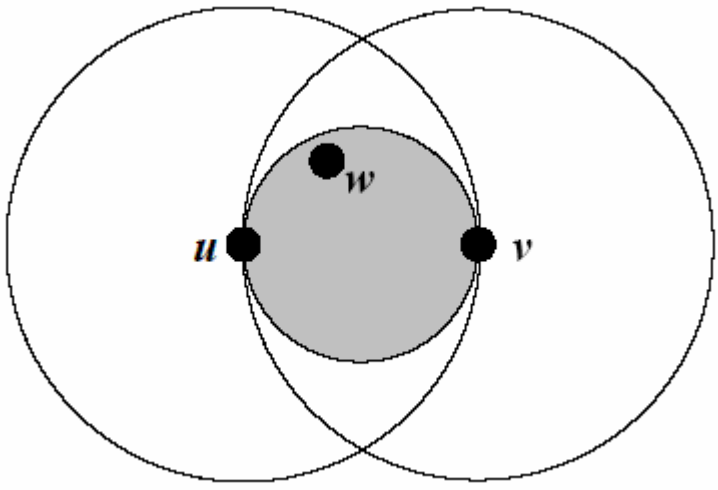
Επιπλέον το GPSR λειτουργεί σε δύο καταστάσεις (“modes”) την “*greedy*” και την “*perimeter*” δρομολόγηση. Με την “*perimeter*” δρομολόγηση το πρωτόκολλο επιλύει εκείνα τα σημεία όπου η “greedy” δρομολόγηση φτάνει σε αδιέξοδο μην μπορώντας οι κόμβοι να βρουν κάποιο μονοπάτι προς τον τελικό προορισμό. Τα σημεία αυτά καλούνται σημεία *void*. Μια τέτοια περίπτωση όπου η *greedy* δρομολόγηση προς τον προορισμό *D* αποτυγχάνει στον κόμβο *x* απεικονίζεται στην Εικόνα

37.



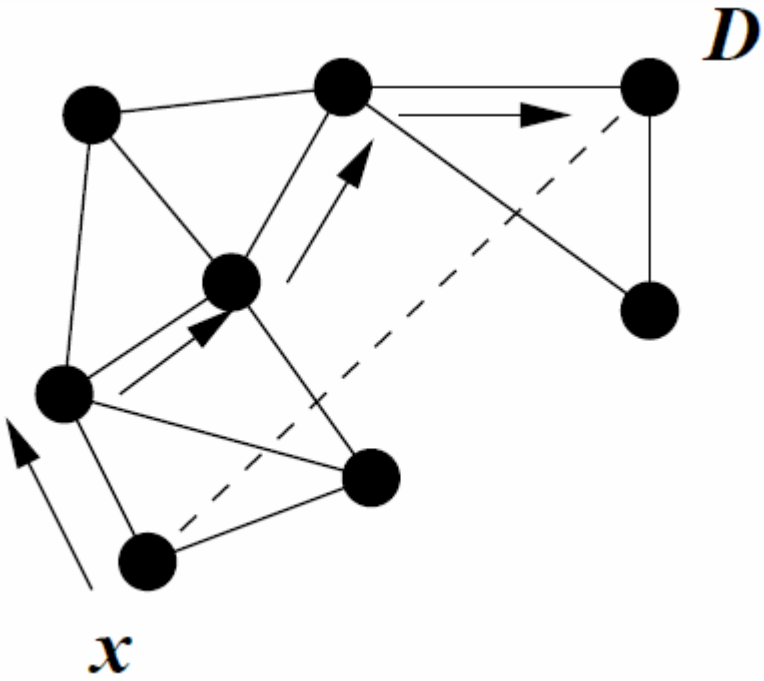
Εικόνα 37. Παράδειγμα σημείου void (x) κατά τη greedy δρομολόγηση με το πρωτόκολλο GPSR.

Σύμφωνα με τη *greedy* δρομολόγηση, το κριτήριο με το οποίο οι ενδιάμεσοι κόμβοι επιλέγουν το επόμενο βήμα σε ένα multi-hop μονοπάτι είναι η ευκλείδεια απόσταση των άμεσων γειτόνων τους από τον τελικό προορισμό. Για τον κόμβο **x** της Εικόνας 37 δεν υπάρχει κάποιος γειτονικός κόμβος εντός κάλυψης του **x** ο οποίος να βρίσκεται σε μικρότερη απόσταση από τον τελικό κόμβο D σε σύγκριση με την απόσταση του κόμβου **x** από τον κόμβο **D**. Το πρωτόκολλο GPSR προσπερνάει τα σημεία *void* (τοπικά μέγιστα) όπως το σημείο x αλλάζοντας το "mode" της δρομολόγησης από *greedy* σε *perimeter*.



Εικόνα 38. Ο κανόνας κατασκευής του Gabriel Graph (GG). Ο γράφος GG περιέχει μια ακμή uv όταν δεν υπάρχει κάποιος κόμβος w ("witness") εντός του κύκλου με διάμετρο uv.

Σύμφωνα με το *perimeter mode* του GPSR η δρομολόγηση επιτυγχάνεται δια μέσου συνδεδεμένων υπογράφων της τοπολογίας -τα οποία καλούνται "planar graphs"-, όπως το Gabriel Graph που κατασκευάζεται σύμφωνα με τον κανόνα της Εικόνας 38 - με τα οποία ένα πακέτο μπορεί να ξεπεράσει ένα σημείο "void" δρομολογούμενο ωστόσο κατά μήκος ενός περιμετρικού και συνεπώς μεγαλύτερου μονοπατιού προς τον τελικό κόμβο. Παράδειγμα GPSR δρομολόγησης σε "*perimeter mode*" απεικονίζεται στην Εικόνα 39. Τα βέλη δείχνουν το περιμετρικό μονοπάτι δρομολόγησης από το σημείο *void* (x) προς τον κόμβο-προορισμό (D).



Εικόνα 39. Παράδειγμα προσπεράσματος του σημείου void (x) με την περιμετρική δρομολόγηση του πρωτοκόλλου GPSR με το μονοπάτι που δείχνουν τα βέλη.

Ωστόσο, η ασφάλεια είναι μια ιδιότητα που δε συμπεριλαμβάνεται στον αρχικό σχεδιασμό του πρωτοκόλλου GPSR. Το GPSR είναι απροστάτευτο στις επιθέσεις που μπορούν να εκδηλωθούν στο επίπεδο του δικτύου. Αυτό οφείλεται στο ότι οι δρομολογητές GPSR μεταδίδουν τόσο τις συντεταγμένες όσο και την ταυτότητά τους ανοιχτά κατά τις μεταδόσεις στο ασύρματο μέσο. Κατά συνέπεια είναι πολύ εύκολο τα πακέτα GPSR και το δίκτυο GPSR να γίνει στόχος επιθέσεων. Το προτεινόμενο σχήμα προστασίας είναι το “Secured and Clustered GPSR” (SC-GPSR) το οποίο προσθέτει διακριτά επίπεδα ασφάλειας στο GPSR ενώ ταυτόχρονα επιτυγχάνει καλύτερη δικτυακή επίδοση από ότι το GPSR. Το SC-GPSR είναι ένα συνεργατικό και ευσταθές σχήμα επαναομαδοποίησης των κόμβων. Η ιδιότητα της ευστάθειας στα σχήματα “clustering”- δηλαδή η επίτευξη μικρού ρυθμού αλλαγών των κόμβων-αρχηγών - είναι ιδιαίτερα επιθυμητή στα ad hoc δίκτυα κινητών κόμβων.

Επιπλέον, το σχήμα SC-GPSR διαχειρίζεται την πληροφορία ομαδοποίησης των κόμβων σαν πληροφορία στο επίπεδο της εφαρμογής, ωστόσο με την τεχνική “piggyback” η πληροφορία αυτή ενσωματώνεται και μεταδίδεται στα περιοδικά μηνύματα “beacons” που χρησιμοποιεί το επίπεδο του δικτύου για τη συντήρηση των ασύρματων ζεύξεων και την ανακάλυψη των γειτονικών ad hoc κόμβων. Το αποτέλεσμα της τεχνικής “piggyback” είναι διπλό. Πρώτον, η επαναομαδοποίηση των κόμβων γίνεται αποδοτικότερα και, δεύτερον, η επίδοση του πρωτοκόλλου αυξάνεται εφόσον μειώνεται ο αριθμός των απαραίτητων μηνυμάτων για τη συντήρηση της ιεραρχικής δομής στο δίκτυο. Περαιτέρω, αυτή η βελτίωση της δικτυακής απόδοσης επιτρέπει την αποδέσμευση ενός μέρους των πόρων των κόμβων του συστήματος (μνήμη και επεξεργαστική ισχύ) για την χρήση τους από κατανεμημένα λειτουργικά τμήματα τα οποία υλοποιούν την ασφάλεια πολλαπλών γραμμών άμυνας.

Το προτεινόμενο σχήμα που θα περιγράψουμε στο Κεφάλαιο αυτό στοχεύει στην ανίχνευση και την αντιμετώπιση των επιθέσεων από κακόβουλους κόμβους που έχουν καταφέρει να παρεισφρύσουν εντός του δικτύου σαν εισβολείς (“intruders”). Ισχυριζόμαστε ότι το προτεινόμενο εκτεταμένο σχήμα προστατεύει το δίκτυο αποτελεσματικά δίχως να απαιτεί ενεργοβόρες διαδικασίες, όπως ψηφιακές υπογραφές και αρχές πιστοποίησης, ενώ ταυτόχρονα βασίζεται και

υλοποιεί τα χαρακτηριστικά και τις διαδικασίες ενός Συστήματος Ανίχνευσης και Αντιμετώπισης Επιθέσεων (Intrusion Detection System, IDS) για τη συστηματική αντιμετώπιση των επιθέσεων νέου τύπου στο δίκτυο ad hoc.

6.2. ΣΧΕΤΙΚΕΣ ΕΡΓΑΣΙΕΣ

Δύο εργασίες που πραγματοποιούν εκτενή επισκόπηση των αλγορίθμων clustering για δίκτυα αισθητήρων και για δίκτυα MANET είναι οι [4] και [5] αντίστοιχα. Όπως είδαμε στο προηγούμενο κεφάλαιο πολλές είναι οι εργασίες οι οποίες προτείνουν αλγορίθμους για την επιλογή των κόμβων-αρχηγών. Ο αλγόριθμος “Lower ID” (LID) στην πιο απλή του μορφή αποδίδει το ρόλο του αρχηγού στον κόμβο με το μικρότερο αριθμό ταυτότητας [6]. Στον αλγόριθμο “Highest Degree” (HD) ως αρχηγός επιλέγεται ο κόμβος που έχει το μεγαλύτερο αριθμό από γείτονες, δηλαδή κόμβους που βρίσκονται σε απόσταση ενός βήματος. Προφανώς η επιλογή που βασίζεται στο κριτήριο της συνεκτικότητας των κόμβων εξαρτάται σε μεγάλο βαθμό από την τοπολογία του δικτύου η οποία επηρεάζεται από την κίνηση των κόμβων. Εν συντομία αναφέρουμε μερικούς αντιπροσωπευτικούς αλγόριθμους clustering όπως ο LCC (Least ClusterHeadChange) [7], ο πιθανοκρατικός LEACH [15], ο αλγόριθμος “Hybrid Energy-Efficient Distributed” (HEED), ο Distributed Mobility-Adaptive Clustering (DMAC), ο αλγόριθμος MOBIC [13], ο Weighted Clustering Algorithm (WCA) [14] και ο σταθμισμένος Highest Degree [17].

Επίσης μέχρι σήμερα έχει αναπτυχθεί ένας μεγάλος αριθμός από πρωτόκολλα δρομολόγησης ad hoc που βασίζονται στη δημιουργία συστάδων (“clusters”). Μεταξύ αυτών ξεχωρίζουν το πρωτόκολλο δρομολόγησης με υποστήριξη ποιότητας υπηρεσίας για πολυμεσικές εφαρμογές [8], το προληπτικό Cluster Based Routing Protocol (CBRP) [9] και το ιεραρχικό Distance vector Cluster Head Gateway Switch Routing protocol (CGSR) [10]. Η τεχνική της παθητικής ομαδοποίησης (“passive clustering”) εισήχθη ως μια μέθοδος/μηχανισμός βελτιστοποίησης στα αντιδραστικά ad hoc πρωτόκολλα στην εργασία [11]. Σύμφωνα με το “passive clustering” τα δεδομένα ελέγχου μεταφέρονται μέσα στα πακέτα δεδομένων, σε αντιπαράθεση με τη δημιουργία των συστάδων κατά ρητό τρόπο (“explicit”).

Ωστόσο, έχει ήδη αναγνωρισθεί ότι η ασφάλεια θα πρέπει να είναι πρωταρχικής σημασίας στη διαδικασία της επιλογής αρχηγών [18], [22] έτσι ώστε οι σημαντικοί για το δίκτυο κόμβοι να προστατεύονται από πιθανό συμβιβασμό και εκμετάλλευση από κακόβουλους χρήστες. Είναι προφανές ότι η προστασία των αρχηγών μειώνει την πιθανότητα εμφάνισης μοναδικών σημείων αστοχίας μέσα στο δίκτυο (“single points of failure”). Προκειμένου να αποκαλυφθούν οι συμβιβασμένοι κόμβοι εντός του δικτύου είναι δυνατόν να εφαρμοστούν σχήματα που κάνουν χρήση παραγόντων εμπιστοσύνης για την επιλογή των αρχηγών [18], ή να εφαρμοστούν δυναμικά σχήματα ομαδικής διαχείρισης των κλειδιών [2].

Σύμφωνα με μια άλλη μεθοδολογία, οι εισβολείς μπορεί να ανιχνευθούν με την επίλυση της αβεβαιότητας των δεδομένων που συγκεντρώνονται στους κόμβους – αρχηγούς. Αυτές οι λύσεις εφαρμόζουν μεθόδους στατιστικής ανάλυσης στους ισχυρούς κόμβους του δικτύου. Η στατιστική ανάλυση περιλαμβάνει αλγόριθμους εκμάθησης (“learning algorithms”) όπως για παράδειγμα τον αλγόριθμο *Kullback-Leibler distance* καθώς και μη επιβλεπόμενους αλγορίθμους ταξινόμησης (“unsupervised classification algorithms”) που επίσης μπορούν να εκτελούνται στους αρχηγούς του δικτύου ad hoc [19]. Για παράδειγμα, ο αλγόριθμος καταμέρισης *K-Means* εφαρμόζεται στην εργασία [19] ώστε να επιτευχθεί η ταξινόμηση των τιμών των παραμέτρων εμπιστοσύνης που υπολογίζονται για αισθητήρες. Ο αλγόριθμος αρνητικής επιλογής (“negative selection algorithm”) είναι ένα άλλο παράδειγμα αλγορίθμου ταξινόμησης που χρησιμοποιήθηκε [20] για τον χαρακτηρισμό των ανωμαλιών της δικτυακής κίνησης. Ωστόσο, είναι ακόμη υπό διερεύνηση αν οι παραπάνω λύσεις μπορούν να αντιμετωπίσουν αξιόπιστα επιθέσεις σε ανώτερα επίπεδα όπως η επίθεση Denial of Service (DoS) ή/και οι επιθέσεις που απειλούν τη διαδικασία της προώθησης με απορρίψεις των πακέτων. Επιπρόσθετα, παραμένει το ερώτημα κατά πόσο αυτές οι τεχνικές είναι

εφαρμόσιμες στο περιορισμένο υπολογιστικά και ενεργειακά ad hoc περιβάλλον.

Μια εναλλακτική μέθοδος ανίχνευσης των κόμβων που έχουν καταφέρει να εισβάλουν στο δίκτυο και δεν συμπεριφέρονται ορθά είναι η ανάλυση της ορθότητας και η εύρεση των ασυνεπειών στη ορθή λειτουργία των πρωτοκόλλων τόσο στο επίπεδο του δικτύου όσο και στο επίπεδο των εφαρμογών τελικού χρήστη. Οι ασυνέπειες προκύπτουν στο επίπεδο του δικτύου όταν η απόφαση δρομολόγησης που λαμβάνεται στους ομότιμους κόμβους δεν αντανακλά την τρέχουσα τοπολογία του δικτύου, εφόσον έχει προηγηθεί πρόκληση σύγχυσης από τον κακόβουλο κόμβο. Σε αυτές τις περιπτώσεις επιθέσεων συστήνουμε την εφαρμογή κατανεμημένων και συνεργατικών μηχανισμών όπως για παράδειγμα τα σχήματα ψηφοφορίας. Στον αλγόριθμο “Voting Clustering Algorithm” (VCA) [21] οι κόμβοι ψηφίζουν για να εκλέξουν τον κόμβο-αρχηγό με αποτέλεσμα ο χρόνος ζωής του δικτύου να αυξάνεται, ωστόσο ο αλγόριθμος δεν προτείνεται και δεν εκτιμάται για την ασφάλεια που μπορεί να προσφέρει μια τέτοια συνεργατική λύση.

Κατά τη γνώμη μας οι διαδικασίες εκλογής όταν απαιτούν ακεραιότητα, συνέπεια και ομοφωνία μεταξύ των κόμβων είναι δυνατόν να αποτελέσουν μηχανισμούς αποκάλυψης των κακόβουλων κόμβων που μεταδίδουν ψευδή και παραπλανητική πληροφορία στο δίκτυο. Για παράδειγμα, οι εργασίες [22] και [23] εφαρμόζουν την αρχή της συμφωνίας (“agreement/consensus principle” όπως αυτή εισάγεται στην εργασία [24]) για λόγους ασφαλείας και ειδικότερα για να διατηρήσουν την εκλογή των κόμβων-αρχηγών ακέραια και δίχως διαστρεβλώσεις. Το πρωτόκολλο εκλογής αρχηγού στην εργασία [25] διαχειρίζεται επιτυχώς την πιθανή συγχώνευση και τον πιθανό διαμελισμό του κινητού δικτύου ad hoc (MANET) και επιτρέπει την διεξαγωγή παράλληλων εκλογών, ενώ παράλληλα διασφαλίζει ευστάθεια και σημαντικό ποσοστό διαθεσιμότητας για τον κόμβο που εκλέγεται ως αρχηγός. Παραμένει το ερώτημα αν το πρωτόκολλο της εργασίας [25] μπορεί να επιλέξει και να διαμοιράσει με ομοιόμορφο τρόπο έναν αριθμό από αρχηγούς ικανό να καλύψει ολόκληρο το δίκτυο αφού σύμφωνα με το προτεινόμενο σχήμα το αποτέλεσμα της εκλογής φαίνεται να είναι ένας μοναδικός αρχηγός που εκλέγεται για μια “multi-hop spanning tree” δομή η οποία επιλέγεται για να μοντελοποιήσει ολόκληρο το ad hoc δίκτυο.

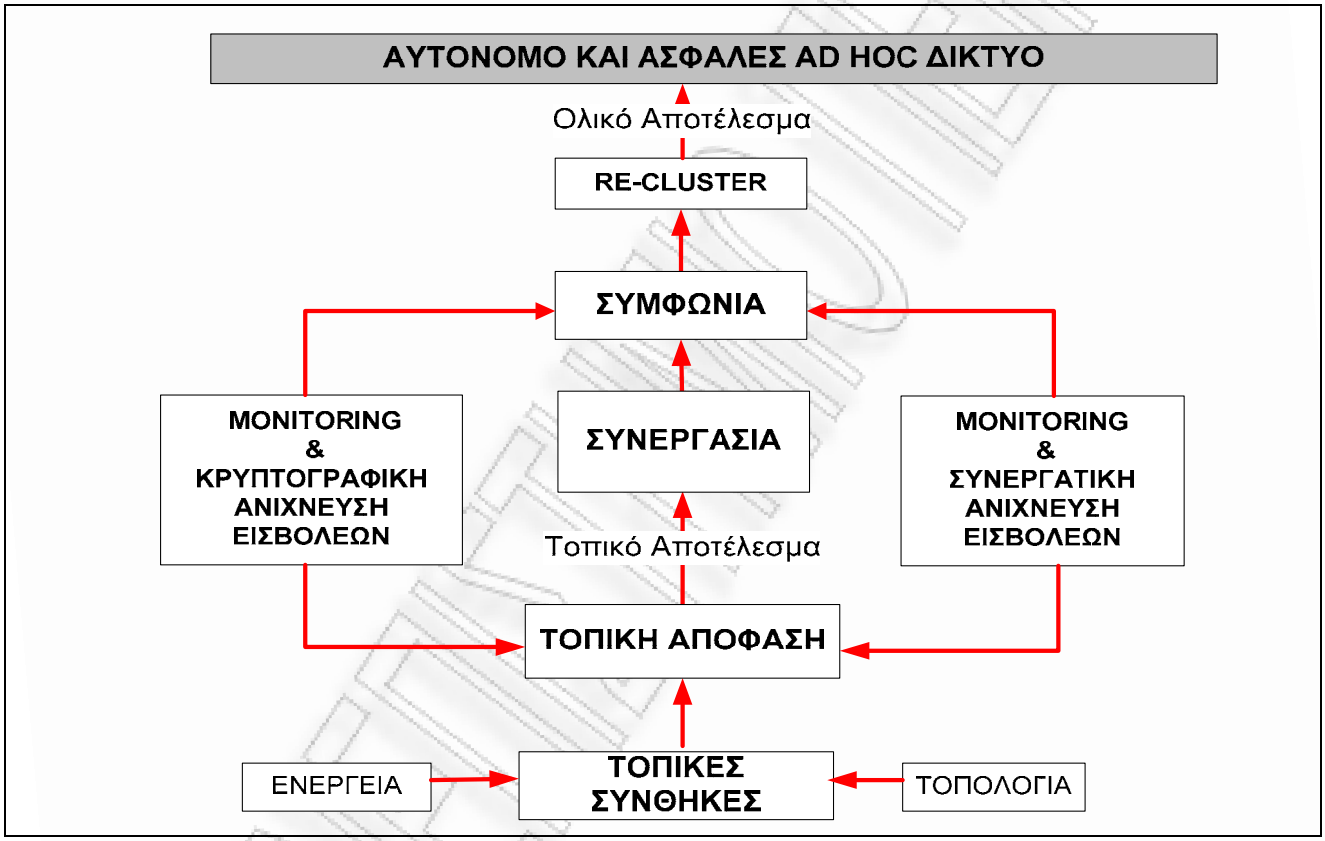
Τέλος, από όσο γνωρίζουμε υπάρχει μόνο ένα πολύ μικρό μέρος της υφιστάμενης βιβλιογραφίας που έχει αντιμετωπίσει την εισαγωγή των συνεργατικών σχημάτων ανίχνευσης κακόβουλων εισβολέων πάνω από γεωγραφικά πρωτόκολλα, όπως το GPSR. Ειδικότερα, υπάρχουν αρκετές επεκτάσεις ασφάλειας για το πρωτόκολλο GPSR ([26], [27], [28], [29], [30]) ωστόσο όλες βασίζονται στην εισαγωγή και τη διαχείριση εμπιστοσύνης μεταξύ των ad hoc κόμβων (που συνηθέστερα είναι αισθητήρες) η οποία υλοποιείται με τη μετάδοση των βαθμών εμπιστοσύνης που έχουν υπολογίσει οι κόμβοι για τους γείτονές τους. Στις εργασίες αυτές με πειράματα έχει δειχθεί ότι τα παραπάνω προτεινόμενα σχήματα βελτιώνουν το χρόνο ζωής των δικτύων αισθητήρων και προστατεύουν από επιθέσεις άρνησης προώθησης πακέτων. Η απόδοση αυτών των σχημάτων παραμένει καλή ακόμη και όταν αυξάνεται ο αριθμός των επιτιθέμενων, ωστόσο τα σχήματα δεν φαίνεται να μπορούν να αντιμετωπίσουν και άλλου τύπου επιθέσεις.

6.3. ΜΟΝΤΕΛΟ ΑΝΑΦΟΡΑΣ ΓΙΑ ΤΑ ΑΥΤΟΝΟΜΑ AD HOC ΔΙΚΤΥΑ

Ενώ συνήθως η αυτονομία συνδέεται με την παράταση του χρόνου ζωής του ad hoc δικτύου με κατάλληλες τεχνικές εξοικονόμησης ενέργειας, για παράδειγμα κατά τη μετάδοση και τη δρομολόγηση των δεδομένων, κατά την άποψή μας η αυτονομία στα δίκτυα ad hoc πρωτίστως εμπεριέχει τη διάσταση της ικανότητας για αυτόνομη λήψη αποφάσεων στα ανώτερα επίπεδα του δικτύου. Έτσι κατά τη γνώμη μας η αυτονομία προϋποθέτει την ικανότητα για αυτο-οργάνωση του δικτύου με αλγορίθμους, πρωτόκολλα και μηχανισμούς λήψης αποφάσεων που προσαρμόζονται στις μεταβλητές δικτυακές συνθήκες. Η αυτονομία επίσης εμπεριέχει τη διάσταση της αυτο-προστασίας. Έτσι αυτόνομο είναι το ad hoc δίκτυο που διαθέτει την ικανότητα της αυτο-οργάνωσης των κόμβων σε αποδοτικές δομές και ταυτόχρονα αυτόνομο είναι το δίκτυο που μπορεί με ίδια μέσα να προστατεύει αυτές τις δομές από τις στοχευμένες επιθέσεις αλλά και να ανακάμπτει από

τις τυχαίες βλάβες στις ασύρματες ζεύξεις και τους κόμβους.

Η ανίχνευση και αντιμετώπιση κακόβουλων κόμβων σε δίκτυα ad hoc με υποδομή έχει διερευνηθεί διεξοδικά σε πολλές εργασίες μέχρι σήμερα. Ωστόσο, αυτό που είναι σπάνιο στις μέχρι τώρα προσεγγίσεις είναι η πρόταση ολοκληρωμένων λύσεων που θα μπορούν να ικανοποιήσουν ταυτόχρονα πολλές απαιτήσεις και πολλά ποιοτικά χαρακτηριστικά, ιδιαίτερα σήμερα που οι εφαρμογές των ασφαλών δικτύων ad hoc ολοένα και αυξάνονται. Για τη *βελτιστοποίηση* και την *ολοκλήρωση* των λύσεων καθώς και για την αντιμετώπιση των προβλημάτων *προστασίας* και *οργάνωσης* σε πολλά διαφορετικά επίπεδα είναι πρωταρχική ανάγκη να θεμελιώσουμε πρώτα ένα μοντέλο αναφοράς που θα οριοθετεί τα υπό αυτούς τους όρους επιδιωκόμενα ποιοτικά χαρακτηριστικά και θα σκιαγραφεί τη γενική αρχιτεκτονική και τους πρόσθετους ***ενσωματωμένους μηχανισμούς*** των αυτόνομων δικτύων ad hoc.



Εικόνα 40. Μοντέλο αναφοράς για αυτόνομα και ασφαλή ασύρματα δίκτυα ad hoc.

Με βάση όσα έχουμε αναφέρει μέχρι τώρα είναι επόμενο το μοντέλο αναφοράς της Εικόνας 40 να μη βασίζεται σε λύσεις ασφαλείας που εξαρτώνται από την υποδομή (όπως ψηφιακές υπογραφές, πιστοποιητικά, εξυπηρετητές αυθεντικοποίησης κ.α.). Ως μη κρυπτογραφικές λύσεις που μπορούν να αξιοποιηθούν για την ανίχνευση και αντιμετώπιση των επιθέσεων στα δίκτυα ad hoc χωρίς υποδομή προτείνουμε και εξετάζουμε τις παρακάτω:

- Την ***ενδο-δικτυακή επεξεργασία*** της πληροφορίας η οποία διεξάγεται σε ειδικούς κόμβους μέσα στο δίκτυο. Αυτό περιλαμβάνει τη στατιστική επεξεργασία, τη συμπίεση και τη συγχώνευση (“fusion”) των δεδομένων με σκοπό τη μείωση της κατανάλωσης της ενέργειας ανά κόμβο, την αποφυγή των άσκοπων μεταδόσεων με δεδομένα που χαρακτηρίζονται από ομοιότητα και συνεπώς την αύξηση του χρόνου ζωής του δικτύου και την κλιμάκωση του αριθμού των κόμβων που μπορούν να συμμετέχουν ομότιμα στις επικοινωνίες. Σε αυτή την περίπτωση η χρήση κατανεμημένων αλγόριθμων ομαδοποίησης των ad hoc κόμβων (“clustering algorithms”) καθώς και κατανεμημένων αλγόριθμων εκλογής αρχηγών (“leader

election algorithms") είναι επιβεβλημένη.

- Τα ***συνεργατικά πρωτόκολλα επικοινωνιών*** και τα ***συνεργατικά συστήματα ανίχνευσης εισβολέων***. Τα συνεργατικά σχήματα περιλαμβάνουν σχήματα ψηφοφορίας, σχήματα κατωφλίων, σχήματα βασισμένα σε συμφωνία και σχήματα εμπιστοσύνης που βασίζονται στη φήμη των κόμβων.

- Τη ***διαχείριση των υπηρεσιών*** που διαθέτουν οι ad hoc κόμβοι με κατάλληλα προσαρμοσμένες κατανεμημένες τεχνολογίες μεσισμικού.

- Τη χρήση πρωτοκόλλων δρομολόγησης καθώς και σχημάτων παραγωγής, ανταλλαγής και εγκατάστασης κλειδιών που λαμβάνουν υπόψη την ταυτότητα και τη θέση των κόμβων. Σημαντικό ρόλο στη μελέτη μας παίζουν τα ***γεωγραφικά πρωτόκολλα ad hoc***.

Επιπλέον η κρυπτογραφική ασφάλεια δεν αποκλείεται από το μοντέλο μας. Αντίθετα θεωρείται ως μια επιπλέον γραμμή άμυνας που δρα προληπτικά και συμπληρωματικά ως προς τα μη κρυπτογραφικά σχήματα. Η μικρής επιβάρυνσης κρυπτογραφική ασφάλεια μπορεί να υλοποιηθεί με ένα από τους παρακάτω τρόπους:

- Συμμετρικούς αλγόριθμους κρυπτογράφησης δεδομένων (όπως AES, DES, Blowfish).
- Συναρτήσεις κατακερματισμού με κλειδί για την αυθεντικοποίηση των δεδομένων ("Hashed Message Authentication Codes") και την αυθεντικοποίηση των κόμβων.
- Συνεργατικά σχήματα κρυπτογραφίας κατωφλίου (κ, ν).

Στο μοντέλο αναφοράς που απεικονίζεται στην Εικόνα 40 βασίζονται οι υλοποιήσεις που θα ακολουθήσουν στο Κεφάλαιο αυτό. Το μοντέλο αυτό είναι ένα κατανεμημένο μοντέλο αυτο-οργάνωσης και αυτο-προστασίας ειδικά προσαρμοσμένο για τα περιορισμένα ασύρματα δίκτυα ad hoc.

Η κύρια ιδέα που κρύβεται πίσω από το μοντέλο αναφοράς είναι η συντήρηση μιας ιεραρχικής δομής στο δίκτυο με μηχανισμούς που βασίζονται στη συνεργασία και την ανταλλαγή πληροφορίας μεταξύ των κόμβων. Οι ίδιοι κατανεμημένοι αλγόριθμοι μπορούν να τρέχουν σε όλους τους ad hoc κόμβους και να λαμβάνουν υπόψη τις αυτόνομες ιδιότητες των κόμβων όπως τη στάθμη της ενέργειάς τους καθώς και τις τοπικές συνθήκες που επικρατούν στη γειτονιά τους, για παράδειγμα τη θέση των γειτόνων, τη σχετική ή την απόλυτη ταχύτητά τους και άλλες τοπικές πληροφορίες. Με αυτό τον τρόπο είναι δυνατόν να λαμβάνονται αυτόνομες αποφάσεις για την οργάνωση και την προστασία του δικτύου. Οι τοπικές αυτές παράμετροι απεικονίζονται στο χαμηλότερο επίπεδο της Εικόνας 40 ως ενέργεια των κόμβων και ως τοπολογία του δικτύου.

Ωστόσο, τα τοπικά αποτελέσματα που κάθε κόμβος εξάγει με βάση τις τοπικές πληροφορίες που διαθέτει πολλές φορές δεν είναι αρκετά για τη διεξαγωγή ασφαλών συμπερασμάτων, δηλαδή δεν είναι αποτελέσματα μεγάλης ακρίβειας. Έτσι με το μοντέλο εισάγουμε σε ένα υψηλότερο επίπεδο ένα συνεργατικό πρωτόκολλο το οποίο παίρνει σαν είσοδο τα αυτόνομα αποτελέσματα των κόμβων και σκοπό έχει, με την κατάλληλη επικοινωνία μεταξύ των κόμβων και την κατάλληλη επεξεργασία των δεδομένων, να οδηγήσει σε συμφωνία για την εκλογή των τοπικών αρχηγών μέσα σε ολόκληρο το δίκτυο. Το συνεργατικό αυτό επίπεδο βασίζεται σε ψηφοφορίες που διεξάγονται σε διαφορετικές περιοχές του δικτύου και σε διαφορετικές στιγμές ανάλογα με το ποιος τις ενεργοποιεί και πότε ξεκινάει η διαδικασία εκλογής.

Σε ιδανικές δικτυακές συνθήκες, δηλαδή στην περίπτωση που δεν έχουμε αστοχίες υλικού, δεν έχουμε τυχαία σφάλματα διεργασιών και όταν η ποιότητα του καναλιού είναι καλή, τα δεδομένα των κόμβων είναι ακριβή και η συνεργασία τους μπορεί να οδηγήσει σε συμφωνία.

Οι ιδανικές όμως συνθήκες είναι σπάνιες, ιδιαιτέρα όταν το ad hoc δίκτυο έχει αναπτυχθεί σε ένα

εχθρικό περιβάλλον. Έτσι το μοντέλο αναφοράς μας απαιτεί την ύπαρξη συμπληρωματικών πρωτοκόλλων προστασίας τα οποία θα μπορούν να αντιμετωπίσουν τόσο τους εξωτερικούς κακόβουλους κόμβους, δηλαδή τους κόμβους που απειλούν δίχως να έχουν πληροφορίες που σχετίζονται με την εσωτερική λειτουργία του δικτύου όσο και τους εσωτερικούς εισβολείς οι οποίοι έχοντας συλλάβει την ευαίσθητη δικτυακή πληροφορία (όπως κλειδιά, passwords, pass phrases και άλλο μυστικό υλικό) προσποιούνται ότι είναι νόμιμοι κόμβοι συμμετέχοντας ενεργά στις ροές των επικοινωνιών που διεξάγονται μεταξύ των νόμιμων κόμβων.

Όπως φαίνεται στην Εικόνα 40 το μοντέλο μας εισάγει δύο τείχη προστασίας διαφορετικών κατευθύνσεων τα οποία ωστόσο δρουν συμπληρωματικά το ένα με το άλλο έτσι ώστε το μοντέλο να δίνει πολλαπλές γραμμές άμυνας.

Το δεξιό τείχος προστασίας της Εικόνας 40 λειτουργεί ως πρώτη γραμμή άμυνας στο μοντέλο μας και είναι ένας μη κρυπτογραφικός μηχανισμός που βασίζεται στην παρακολούθηση των κόμβων και των δεδομένων που αυτοί μεταδίδουν για τη συνεργατική ανίχνευση της μη κανονικής συμπεριφοράς με βάση διακριτά επίπεδα ασφαλείας. Με βάση το μοντέλο αυτό θα εισάγουμε και θα υλοποιήσουμε διακριτά επίπεδα ασφαλείας βάσει των οποίων θα ανιχνεύονται οι κακόβουλοι κόμβοι. Αυτό είναι ένα πρώτο βήμα για τη διεξαγωγή ασφαλέστερων συμπερασμάτων όσον αφορά το χαρακτηρισμό της φυσιολογικής ή μη συμπεριφοράς των κόμβων, γεγονός το οποίο πηγάζει από την ανταλλαγή πληροφοριών με τη μορφή γνώμης ανάμεσα στους κόμβους (γειτονικούς ή/και μακρινούς).

Οι επιθέσεις που αντιμετωπίζει το συνεργατικό τείχος έχουν να κάνουν με εσωτερικούς εισβολείς που σκόπιμα εισάγουν στο δίκτυο λανθασμένα δεδομένα ελέγχου όπως για παράδειγμα ψευδή πληροφορία θέσης ή ταυτότητας που οδηγεί τους κόμβους στο να πάρουν λανθασμένη απόφαση δρομολόγησης ή ακόμη ψευδή πληροφορία στο επίπεδο της εφαρμογής όπως για παράδειγμα παραπλανητικές τιμές των παραμέτρων που χρησιμοποιεί το πρωτόκολλο εκλογής αρχηγών. Οι επιθέσεις αυτές υποβαθμίζουν πρωτίστως τη σωστή λειτουργία και την απόδοση του δικτύου και άρα το υπονομεύουν με ολιστικό αντίκτυπο εκ των έσω.

Το αριστερό τείχος της Εικόνας 40 λειτουργεί στην πρότασή μας ως δεύτερη γραμμή άμυνας. Βασίζεται σε πρότυπες κρυπτογραφικές διαδικασίες οι οποίες φροντίζουν για την ακεραιότητα τόσο των πακέτων δεδομένων όσο και των πακέτων ελέγχου που διακινούνται μέσα στο δίκτυο. Επίσης παρέχει την ακεραιότητα της ταυτότητας των κόμβων που μεταδίδεται μέσα στο δίκτυο (είναι δυνατή έτσι η καταπολέμηση επιθέσεων παραποίησης ταυτότητας, όπως οι επιθέσεις “spoofing” και “Sybil” για παράδειγμα). Κατά την άποψή μας, η ανίχνευση μιας αλλαγής στο περιεχόμενο των πακέτων με κρυπτογραφικές μεθόδους σηματοδοτεί με μεγάλη πιθανότητα την ύπαρξη ενός εξωτερικά επιτιθέμενου κόμβου, δηλαδή κατά την δεύτερη φάση της ανίχνευσης με κρυπτογραφικές μεθόδους είναι πολύ πιθανό να πρόκειται για κάποιον εξωτερικό κακόβουλο κόμβο που ακόμη δεν έχει καταφέρει να εισβάλουν στο δίκτυο. Τον εσωτερικό εισβολέα όπως είδαμε προηγουμένως αναλαμβάνει να ανιχνεύσει πιο αποτελεσματικά το συνεργατικό τείχος.

Αξίζει να σημειώσουμε ότι στις μέχρι τώρα προσεγγίσεις στην προστασία από τις εισβολές κακόβουλων κόμβων ως πρώτη γραμμή άμυνας τίθεται (η πολλές φορές “βαριά”) κρυπτογραφική προστασία (με μηχανισμούς όπως η ισχυρή συμμετρική κρυπτογράφηση, οι ψηφιακές υπογραφές, τα πιστοποιητικά κ.α.) και σα δεύτερη γραμμή άμυνας έπονται οι διάφοροι εναλλακτικοί μηχανισμοί προστασίας όπως η από κοινού λήψη αποφάσεων με ανταλλαγή γνωμών, με ανταλλαγή τιμών εμπιστοσύνης, με εκλογή κόμβων-αρχηγών, με στατιστική ανάλυση κ.ο.κ.

Θεωρούμε ότι η προσέγγισή μας ως προς την ιεράρχηση των γραμμών άμυνας και τη σειρά εφαρμογής των λύσεων προστασίας είναι καταλληλότερη για το περιορισμένο ad hoc δίκτυο.

Η συμφωνία μεταξύ των κόμβων είναι πιθανό να δώσει αποτέλεσμα που θα είναι διαφορετικό από την τρέχουσα δομή του δικτύου, συνθήκη που όπως έχουμε περιγράψει απαιτεί την αλλαγή των

ρόλων, την ενημέρωση των κόμβων για την αλλαγή του συνόλου των κόμβων-αρχηγών και τη συσχέτιση ("association") των απλών κόμβων με τους νέους αρχηγούς. Η διαδικασία αυτή της ενημέρωσης του δικτύου είναι η γνωστή επαναομαδοποίηση ("re-clustering").

Για ένα σχήμα που υποστηρίζει την ψηφοφορία μεταξύ των κόμβων επαναομαδοποίηση έχουμε όταν κάποιος κόμβος (απλό μέλος ή αρχηγός) ενεργοποιεί τη διαδικασία εκλογής με ψηφοφορία για το νέο αρχηγό στις περιπτώσεις εκείνες που το επιβάλλει η αλλαγή των τοπικών δικτυακών συνθηκών. Στο πλαίσιο της αυτο-οργάνωσης και αυτο-προστασίας των δικτύων ad hoc τα επιμέρους χαρακτηριστικά που προσφέρουν τα δύο τείχη προστασίας είναι τα εξής: ανοχή σε σφάλματα, αξιοπιστία επικοινωνιών, ακεραιότητα, συνέπεια, ανίχνευση και αντιμετώπιση απειλών, διαθεσιμότητα και καλή δικτυακή απόδοση. Οι σκοποί του μοντέλου αναφοράς εξυπηρετούνται από τον τρόπο υλοποίησης αυτών των επιμέρους ποιοτικών χαρακτηριστικών. Περιγράφουμε παρακάτω με ένα μεγαλύτερο βαθμό λεπτομέρειας τα επιμέρους ποιοτικά χαρακτηριστικά και τον τρόπο υλοποίησής τους:

- ***Μεγαλύτερος βαθμός αξιοπιστίας*** *με αύξηση της διαθεσιμότητας των ad hoc κόμβων και των υπηρεσιών*. Η αξιόπιστη μετάδοση μηνυμάτων στον τελικό προορισμό διασφαλίζεται με την ύπαρξη των κόμβων-αρχηγών και από το υψηλό ποσοστό διαθεσιμότητας αυτών. Με τη σειρά της η διαθεσιμότητα των κόμβων με το ρόλο του αρχηγού εξαρτάται από το απόθεμα ενέργειας που διαθέτουν, τη συνεκτικότητα ανάμεσα στα clusters όπως και μέσα σε κάθε cluster, και την ανοχή που οι αρχηγοί έχουν στις επιθέσεις από τους εισβολείς. Η διαθεσιμότητα των κόμβων-αρχηγών εγγυάται όχι μόνο αύξηση του χρόνου ζωής του δικτύου αλλά και την αξιόπιστη μετάδοση των μηνυμάτων σε ένα μονοπάτι πολλών βημάτων που διασχίζει πολλά clusters μέχρι να φτάσει τον τελικό μακρινό κόμβο, εφόσον οι κόμβοι-αρχηγοί είναι αυτοί που αναλαμβάνουν την προώθηση των μηνυμάτων από συστάδα σε συστάδα. Η λειτουργία του αλγορίθμου ομαδοποίησης στο δίκτυο θα πρέπει να διασφαλίζει τα ακόλουθα:

  - Ότι ο ρόλος του αρχηγού δεν αποδίδεται σε ένα κόμβο που έχει συμβιβαστεί. Αν συμβεί κάτι τέτοιο τότε η διαθεσιμότητα ολόκληρου του δικτύου κινδυνεύει αφού έτσι οι σημαντικοί κόμβοι μέσα στο δίκτυο θα αποτελούν τη βάση από όπου θα εκδηλώνονται οι επιθέσεις. Ουσιαστικά τότε όλα τα καθήκοντα και δικαιώματα του αρχηγού θα εκτελούνται σύμφωνα με τα ενδιαφέροντα του επιτιθέμενου.

  - Ότι ο εκλεγμένος κόμβος έχει αρκετούς πόρους για να εκτελεί τα καθήκοντα του αρχηγού για ένα αρκούντως μεγάλο διάστημα. Θα πρέπει δηλαδή ο αλγόριθμος εκλογής αρχηγού να επιλέγει εκείνους τους κόμβους που στο μεγαλύτερο ποσοστό του χρόνου είναι ικανοί να λειτουργήσουν ως κόμβοι αρχηγοί (για παράδειγμα έχουν αρκετή ενέργεια). Το ποσοστό του χρόνου που ένας εκλεγμένος κόμβος παραμένει διαθέσιμος είναι βασικό μέτρο της αποδοτικότητας και της διαθεσιμότητας που ο αλγόριθμος επιτυγχάνει.

- ***Ανίχνευση και αντιμετώπιση των επιθέσεων με συνεργασία***. Η συνεργασία μεταξύ των κόμβων μπορεί να κάνει την ανίχνευση των υπόπτων κόμβων πιο έγκαιρη και πιο ασφαλή ως προς την ακρίβεια της απόφασης καθώς εξαρτάται από μία συλλογική και όχι από μία ατομική δράση. Η συνεργασία μεταξύ των κόμβων μπορεί να αποκαλύψει στοιχεία μη κανονικής συμπεριφοράς με την ανάλυση των δεδομένων που ανταλλάσσουν οι κόμβοι. Ακόμη η αντίδραση στην επίθεση αφού αυτή ανιχνευθεί γίνεται πιο συντονισμένη και άρα πιο αποτελεσματική με τη συνεργασία των κόμβων, για παράδειγμα με την ανταλλαγή της γνώμης των κόμβων για κάποιο ύποπτο, με ανταλλαγή μαύρης λίστας από τους κόμβους που είναι επιφορτισμένοι με το έργο της προστασίας, με ανταλλαγή συναγερμών κ.α.

- ***Ακεραιότητα.*** Η ακεραιότητα είναι μια πολύ βασική απαίτηση ασφάλειας για τις επικοινωνίες στα ασύρματα δίκτυα ad hoc. Η ακεραιότητα των επικοινωνιών είναι

πρωταρχικής σημασίας για το μοντέλο αναφοράς μας. Η ακεραιότητα είναι πολυδιάστατη: ακεραιότητα των μηνυμάτων (από σφάλματα που οφείλονται στο κανάλι μετάδοσης και από σφάλματα που οφείλονται σε σκόπιμες μετατροπές του μηνύματος), ακεραιότητα των ταυτοτήτων των μερών που επικοινωνούν (μη παραποίηση της ταυτότητας των κόμβων), αλλά και ακεραιότητα της λειτουργίας των αλγορίθμων και των πρωτοκόλλων μέσα στο δίκτυο. Η παραβίαση της ορθής λειτουργίας του δικτύου είναι μια πολύ σημαντική απειλή η οποία μπορεί να καταστρέψει τις υπηρεσίες που προσφέρει το δίκτυο στους τελικούς χρήστες.

- ***Δικτυακή επίδοση με αποδοτική σχεδίαση και υλοποίηση των πρωτοκόλλων***. Τα παραπάνω ποιοτικά χαρακτηριστικά δε θα πρέπει να επιβαρύνουν την απόδοση του δικτύου που είναι αντιληπτή στον τελικό χρήστη με μεγέθη όπως η διαπερατότητα, η μέση καθυστέρηση μεταφοράς μηνύματος, η απώλεια πακέτων, η επιβάρυνση των μηνυμάτων ελέγχου, κ.α. Η σωστή σχεδίαση και η αναζήτηση και υλοποίηση αποδοτικών τεχνικών όσον αφορά τα πρωτόκολλα οργάνωσης και προστασίας του δικτύου ad hoc είναι μια λύση προς αυτήν την κατεύθυνση.

6.4. ΤΟ ΠΡΟΤΕΙΝΟΜΕΝΟ ΣΧΗΜΑ SC-GPSR

Το ολοκληρωμένο και κατανεμημένο σχήμα που υλοποιήσαμε είναι ένα συνεργατικό σχήμα αυτο-οργάνωσης, ανίχνευσης και αντιμετώπισης των επιθέσεων και ακολουθεί τη δομή του μοντέλου αναφοράς που παρουσιάσαμε παραπάνω. Προτείνουμε ένα νέο εκτεταμένο σχήμα του γεωγραφικού πρωτοκόλλου GPSR, ονομαστικά το σχήμα “Secured and Clustered GPSR” (SC-GPSR) το οποίο χρησιμοποιεί ως βασικές συνιστώσες του τον προτεινόμενο αλγόριθμο ομαδοποίησης RRA που παρουσιάστηκε στο Κεφάλαιο 5 (§5.4) και το γεωγραφικό πρωτόκολλο GPSR που αρχικά παρουσιάστηκε στο Κεφάλαιο (§3.6.5.1).

Ο αλγόριθμος RRA εδώ σχεδιάζεται και υλοποιείται ως βασικό λειτουργικό τμήμα του ολοκληρωμένου σχήματος SC-GPSR. Συνεπώς ο RRA υλοποιείται σαν ένας πλήρως κατανεμημένος αλγόριθμος ομαδοποίησης και εκλογής αρχηγών με συνεργατική λήψη αποφάσεων που στηρίζεται στη διεξαγωγή ψηφοφορίας για την επιλογή των αρχηγών (cluster heads). Αυτή είναι η πλήρως κατανεμημένη μορφή του αλγόριθμου που εισήχθη αρχικά στην §5.4 και ο οποίος βασιζόταν στον κεντρικό έλεγχο και την κεντρική επεξεργασία της πληροφορίας που προέρχεται από τους τυχαίους γράφους.

Επιπλέον, το εκτεταμένο σχήμα SC-GPSR εισάγει πρόσθετους τύπους μηνυμάτων και στηρίζεται στην υπόθεση ότι το ad hoc δίκτυο κάνει χρήση μηνυμάτων “φάρων” (“beacons”), δηλαδή μηνυμάτων ανοιχτής εκπομπής (“broadcasts”) τα οποία μεταδίδονται με περιοδικό τρόπο από όλους τους κόμβους. Οι περιοδικές αυτές εκπομπές είναι απαραίτητες για τη συντήρηση των δεσμών του δικτύου και την ανακάλυψη των γειτονικών κόμβων (του σταθμού βάσης συμπεριλαμβανομένου) και υποθέτουμε ότι πραγματοποιείται στο επίπεδο δικτύου (OSI επίπεδο 3). Εναλλακτικά τα πακέτα Beacons μπορεί να χρησιμοποιηθούν και στο επίπεδο MAC, όπως γίνεται για παράδειγμα στο πρότυπο IEEE 802.15.4 ZigBee MAC, αν η αντίστοιχη σημαία (flag) είναι ενεργοποιημένη μέσα στο πακέτο.

Το προτεινόμενο σχήμα SC-GPSR χρησιμοποιεί κατανεμημένους μηχανισμούς αυτο-προστασίας που σκοπό έχουν να ανιχνεύσουν επιθέσεις που προέρχονται από εισβολείς που έχουν εισέλθει στο δίκτυο (intruders). Το προτεινόμενο σχήμα αποτελείται από μια σειρά από λειτουργικά τμήματα το καθένα από τα οποία αναλαμβάνει μια από τις παραπάνω λειτουργίες, όπως την ομαδοποίηση των κόμβων, τη συνεργασία των κόμβων με διαδικασία ψηφοφορίας για την εκλογή αρχηγών, την παρακολούθηση του δικτύου και την ανίχνευση εισβολών που βασίζεται σε επίπεδα ασφαλείας. Το σχήμα SC-GPSR στην περίπτωση που πληρούνται οι συνθήκες για την ανίχνευση υπόπτου κόμβου, αντιδρά με το να απομονώσει τους ύποπτους κόμβους (*blacklisting*) και με το να

μεταδώσει την κατάλληλη πληροφορία της ταυτότητας των επιτιθέμενων στους υπολοίπους κόμβους για τον αποκλεισμό τους από τις διαδικασίες δρομολόγησης και ομαδοποίησης του δικτύου.

Τονίζουμε ότι στο προτεινόμενο σχήμα το επίπεδο του δικτύου παίζει σημαντικό ρόλο και ενισχύεται λειτουργικά αφού αντιμετωπίζεται σαν αναπόσπαστο μέρος του συστήματος ανίχνευσης και αντιμετώπισης των επιθέσεων. Αυτό γίνεται για να αυξηθεί η επίδοση αλλά και η ασφάλεια του δικτύου αφού είναι γνωστό ότι πολλές φορές οι επιτιθέμενοι προσπαθούν να εκμεταλλευτούν τις αδυναμίες ασφαλείας που υπάρχουν στα κατώτερα επίπεδα των συστημάτων.

Επίσης, το προτεινόμενο σχήμα χρησιμοποιεί και κρυπτογραφικά τμήματα για την διασφάλιση της ιδιωτικότητας και της ακεραιότητας των επικοινωνιών (μηνυμάτων) καθώς και την αυθεντικότητα των κόμβων. Ας περιγράψουμε όμως ένα προς ένα τα διάφορα λειτουργικά τμήματα από τα οποία απαρτίζεται το σχήμα SC-GPSR.

6.4.1. Το Λειτουργικό Τμήμα Ομαδοποίησης

Η εκλογή του κόμβου-αρχηγού στο σχήμα SC-GPSR βασίζεται στον υπολογισμό της μεταβλητής απόφασης V_i για κάθε κόμβο i, η οποία είναι η τιμή του παρακάτω σταθμισμένου αθροίσματος σύμφωνα με τον αλγόριθμο ομαδοποίησης RRA, §5.4:

$$V_i = a \times d_i + b \times E_{ri} + c \times D_i^{-1} \quad (1)$$

Στο προτεινόμενο σχήμα SC-GPSR όλοι οι κόμβοι υπολογίζουν την τιμή της μεταβλητής V_i για όλους τους γειτονικούς κόμβους i που ακούνε σε απόσταση ενός βήματος. Οι γείτονες στέλνουν την απαραίτητη πληροφορία - δηλαδή το βαθμό συνεκτικότητάς τους d_i, το απόθεμα ενέργειας E_{ri} και την απόστασή τους D_i από το κέντρο της γειτονιάς τους - μέσα στα πακέτα ευρείας εκπομπής (φάρους) που μεταδίδουν περιοδικά στο δίκτυο.

Στη συνέχεια, όλοι οι κόμβοι υπολογίζουν και εκπέμπουν την ψήφο τους υπέρ εκείνου του γειτονικού κόμβου που βρήκαν να έχει στη γειτονιά τη μέγιστη τιμή της μεταβλητής V_i. Οι κόμβοι τους οποίους ψηφίζουν οι υπόλοιποι μετά από την εύρεση της μεγίστης τιμής της μεταβλητής V_i αποτελούν για το σχήμα SC-GPSR το σύνολο των "πρωταρχικών υποψήφιων κόμβων-αρχηγών".

Η διαδικασία ομαδοποίησης των κόμβων κάτω από ένα κόμβο-αρχηγό μπορεί να ενεργοποιηθεί είτε από ένα απλό μέλος κάποιου cluster είτε από κάποιον κόμβο-αρχηγό. Συνήθως στους αλγορίθμους clustering οι συνθήκες αυτές είτε είναι απλά περιοδικές στο χρόνο είτε ενεργοποιούνται από τυχαία γεγονότα που έχουν να κάνουν με την αλλαγή της ad hoc τοπολογίας (χαρακτηριστικό παράδειγμα είναι η συνάντηση δύο cluster heads καθώς αυτοί κινούνται), ή με τη χαμηλή διαθεσιμότητα των υφιστάμενων αρχηγών, λόγω χαμηλής ενέργειας για παράδειγμα.

Στο προτεινόμενο σχήμα SC-GPSR οι συνθήκες υπό τις οποίες μπορεί να ενεργοποιηθεί η διαδικασία επαναομαδοποίησης για την εκλογή νέου αρχηγού ("re-clustering") είναι οι εξής:

- Όταν δύο cluster heads μπαίνουν ο ένας στην ακτίνα κάλυψης του άλλου, τότε ξεκινά μια νέα διαδικασία εκλογής αρχηγού προκειμένου να αποφασιστεί με ψηφοφορία ποιος από τους δύο αυτούς cluster heads ικανοποιεί καλύτερα τα κριτήρια που θέτει ο clustering αλγόριθμος RRA στην Εξίσωση (1). Το αποτέλεσμα είναι να έχουμε συγχώνευση των δύο προηγούμενων clusters σε ένα. Ο τελικός αρχηγός κοινοποιείται σε όλους τους υπόλοιπους κόμβους με την αποστολή κατάλληλου μηνύματος ευρείας εκπομπής, ενώ ο δεύτερος αρχηγός μετατρέπεται σε απλό μέλος του νέου cluster.

- Όταν η ενέργεια ενός υπάρχοντος cluster head πέφτει κάτω από κάποια τιμή

κατωφλίου. Σε αυτή την περίπτωση ο ίδιος ο αρχηγός σηκώνει τη σημαία της ψηφοφορίας οπότε ξεκινά και πάλι η διαδικασία του καθορισμού του νέου εύρωστου αρχηγού στην περιοχή και άρα της δημιουργίας νέας δομής μέσα στο ad hoc δίκτυο.

Στην πρότασή μας η διαδικασία επανεκλογής των κόμβων-αρχηγών περιλαμβάνει:

- Τον υπολογισμό της ψήφου (προτίμηση) σε κάθε κόμβο.
- Τη μετάδοση της ψήφου των κόμβων.
- Τη συγκέντρωση και την καταμέτρηση των ψήφων σε κάθε κόμβο, εφόσον η διαδικασία της ψηφοφορίας είναι ενεργοποιημένη.

Η διαδικασία αυτή ενεργοποιείται από ένα κόμβο-αρχηγό όταν πληρείται κάποια από τις συνθήκες "re-clustering" που περιγράψαμε προηγουμένως.

6.4.2. Το Λειτουργικό Τμήμα Συνεργατικής Ψηφοφορίας

Στην περίπτωση που ικανοποιείται μία από τις συνθήκες επανομαδοποίησης τότε οι κόμβοι συνεργάζονται με σκοπό να εκλέξουν με ψηφοφορία το νέο αρχηγό στη γειτονιά τους. Κάθε κόμβος πρέπει να συμμετέχει σε μία και μόνο ψηφοφορία κάθε στιγμή και κάθε ψηφοφορία παίρνει ένα μοναδικό αριθμό-ταυτότητα που παράγεται με τυχαίο τρόπο, ώστε να αποφευχθούν συγκρούσεις στα αποτελέσματα των εκλογών. Κάθε κόμβος μεταδίδει την προτίμησή του (ψήφο) ως προς τον κόμβο υποψήφιο (που είναι ένας από τους "πρωταρχικούς υποψήφιους κόμβους-αρχηγούς") που ικανοποιεί καλύτερα τα κριτήρια που θέτει ο αλγόριθμος ομαδοποίησης RRA.

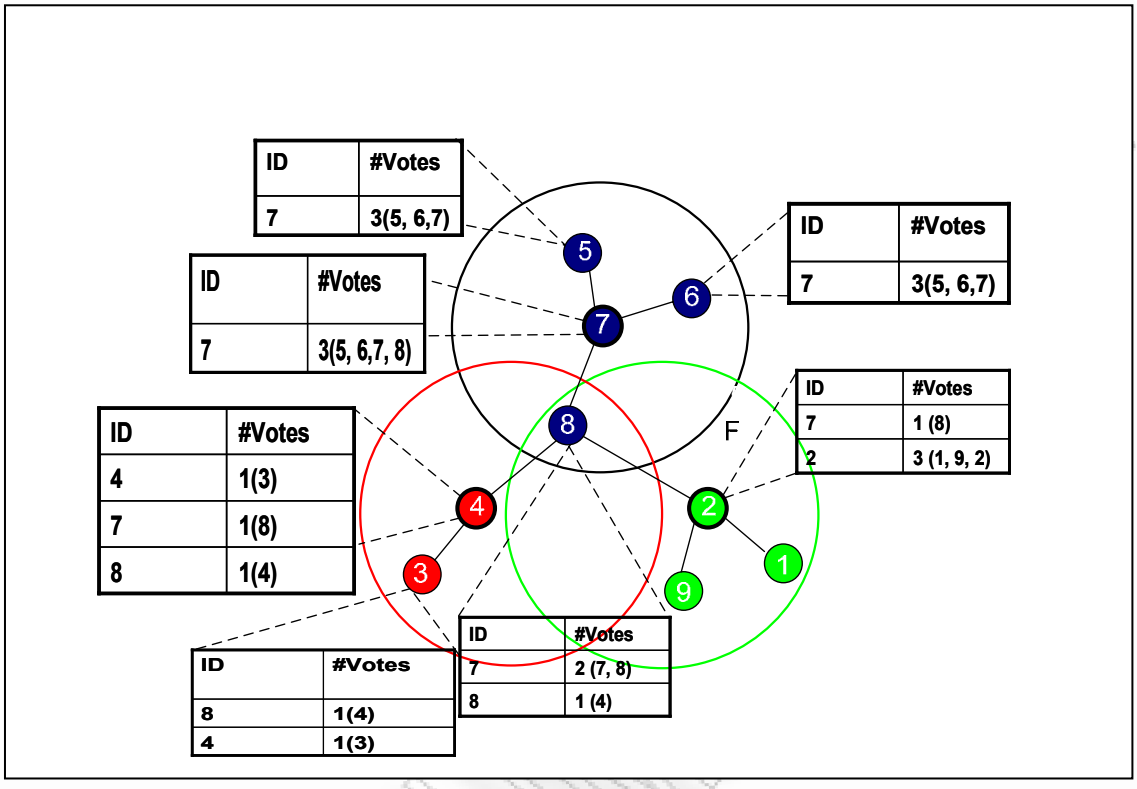
Κάθε κόμβος *i* επιτρέπεται να ψηφίσει ένα και μόνο κόμβο *j* σε μία ψηφοφορία. Η ψήφος κάθε κόμβου περιέχεται στο πεδίο "*My_Vote*" που μεταδίδεται με ευρεία εκπομπή μέσα στα πακέτα φάρους. Ο κόμβος για τον οποίο κάθε κόμβος *i* ψηφίζει μπορεί να είναι ο ίδιος ο κόμβος *i* αφού για την εύρεση του μεγίστου V_j εξετάζεται από τον κόμβο *i* τόσο η λίστα *Neighbor_List* (όπου αποθηκεύονται οι τιμές της μεταβλητής V_j που έχουν στείλει όλοι οι άμεσοι γείτονες $j \neq i$) όσο και η και η τιμή της μεταβλητής V_i που δίνει ο ίδιος ο κόμβος *i*.

Ακόμη, κάθε κόμβος κρατάει στη μνήμη ένα πίνακα *Votes_Table* με τις ψήφους που έχουν συγκεντρώσει οι κόμβοι της γειτονιάς του. Εκείνος ο "πρωταρχικός υποψήφιος κόμβος" που έχει συγκεντρώσει το μεγαλύτερο αριθμό ψήφων, όπως προκύπτει από τον πίνακα *Votes_Table*, είναι ο κόμβος που τελικά επιλέγεται ως τοπικός αρχηγός.

Η Εικόνα 41 απεικονίζει ένα στιγμιότυπο της τοπολογίας ad hoc που έχει ομαδοποιηθεί σε τρία clusters με το σχήμα SC-GPSR. Για χάρη απλότητας υποθέτουμε ότι ο αλγόριθμος ομαδοποίησης λαμβάνει υπόψη μόνο το βαθμό συνεκτικότητας *d* των κόμβων προκειμένου να αποφασίσει τον αρχηγό, ο οποίος για κάθε κόμβο ισούται με τον αριθμό των γειτόνων σε απόσταση ενός βήματος, δηλαδή τον αριθμό των κόμβων εντός της ακτίνας κάλυψης.

Οι εννέα κόμβοι του σχήματος αποφασίζουν για τους "πρωταρχικούς υποψήφιους κόμβους-αρχηγούς" με βάση το κριτήριο μέγιστου βαθμού συνεκτικότητας *d* και μεταδίδουν την ψήφο τους στους υπολοίπους.

Ο συμβολισμός (1) ⇒ (2) δηλώνει ότι ο κόμβος (1) ψηφίζει υπέρ του κόμβου (2).



Εικόνα 41. Συνεργατική ομαδοποίηση των κόμβων και συνεργατική εκλογή αρχηγού με ψηφοφορία μεταξύ γειτόνων.

(1) ⇒ **(2)**, **(3)** ⇒ **(4)**, **(4)** ⇒ **(8)**, **(5)** ⇒ **(7)**, **(6)** ⇒ **(7)**

(7) ⇒ **(7)** – μετά από εφαρμογή του κανόνα ελαχίστης ταυτότητας (“lower ID”)

(8) ⇒ **(7)** – μετά από εφαρμογή του κανόνα ελαχίστης ταυτότητας (“lower ID”).

(9) ⇒ **(2)**

Παρατηρούμε ότι ο κόμβος (7) πρέπει να αποφασίσει μεταξύ του κόμβου (8) και του ιδίου εφόσον και οι δυο κόμβοι (7) και (8) ισχυρίζονται βαθμό συνεκτικότητας *d* ίσο με τρία που είναι ο αριθμός των γειτόνων τους σε απόσταση ενός βήματος όπως φαίνεται στην Εικόνα 41. Ωστόσο, στην περίπτωση αυτή ο αλγόριθμος RRA αποφασίζει υπέρ του κόμβου με τη μικρότερη ταυτότητα (ID) και συνεπώς ο κόμβος (7) θα ψηφίσει τελικά υπέρ του κόμβου(8). Το ίδιο ισχύει και για τον τρόπο που ψηφίζει ο κόμβος (8), δηλαδή υπέρ του κόμβου (7). Οι κόμβοι (2), (7) και (4) συγκεντρώνουν τις περισσότερες ψήφους στη γειτονιά τους και είναι αυτοί που παίρνουν το ρόλο του cluster head στο συγκεκριμένο στιγμιότυπο.

6.4.3. Το Λειτουργικό Τμήμα Παρακολούθησης και Ανίχνευσης Εισβολών

Το τμήμα παρακολούθησης και ανίχνευσης στο σχήμα SC-GPSR (“monitoring block”) είναι ένα μη κρυπτογραφικό τείχος προστασίας το οποίο έχει σκοπό να προστατεύει τη διαδικασία της εκλογής κόμβων-αρχηγών στο αυτο-οργανωμένο δίκτυο ad hoc. Η διαδικασία εκλογής αρχηγού μπορεί να απειληθεί από κακόβουλους κόμβους που θα προσπαθήσουν να την υπονομεύσουν ώστε τελικά να συμβιβάσουν τους κόμβους-αρχηγούς και επομένως να ελέγξουν τις επικοινωνίες και την ομαλή λειτουργία του δικτύου.

Το τμήμα παρακολούθησης και ανίχνευσης του SC-GPSR, στην πλήρως κατανεμημένη του μορφή, εγκαθίσταται σε όλους τους ad hoc κόμβους. Συνεπώς όλοι οι κόμβοι είναι ικανοί να ανιχνεύσουν πιθανή μη φυσιολογική συμπεριφορά κοντινών κόμβων χωρίς να εξαρτώνται από άλλους κόμβους/πράκτορες. Με αυτόν τον τρόπο όλοι οι κόμβοι του δικτύου δυνητικά λειτουργούν σαν κόμβοι ενός πλήρως κατανεμημένου συστήματος ανίχνευσης εισβολών και προστασίας. Ωστόσο, δεν είναι απαγορευτική η επιλεκτική χρήση και εγκατάσταση του “monitoring block” σε ένα περιορισμένο αριθμό κόμβων του δικτύου οι οποίοι θα λειτουργούν ως αφιερωμένα σημεία παρακολούθησης της δικτυακής συμπεριφοράς. Έτσι, οι κόμβοι-ανιχνευτές μπορεί να είναι οι εκλεγμένοι κόμβοι-αρχηγοί [42] μπορεί όμως να είναι και κόμβοι διαφορετικοί από τους κόμβους-αρχηγούς, περίπτωση κατά την οποία οι κόμβοι αυτοί θα λειτουργούν αποκλειστικά ως κόμβοι-πράκτορες του συστήματος προστασίας IDS.

Τα πειραματικά αποτελέσματα εκτίμησης του προτεινόμενου σχήματος που θα παρουσιάσουμε στη συνέχεια αφορούν στην κατανεμημένη αρχιτεκτονική όπου όλοι οι κόμβοι περιοδικά συλλέγουν πληροφορία για τους γείτονές τους και όλοι οι κόμβοι είναι δυνατόν να εισέλθουν στην κατάσταση της ανίχνευσης των εισβολέων και να αντιδράσουν με ειδοποίηση των υπολοίπων κόμβων του δικτύου.

Σημειώνουμε ότι προκειμένου η ανίχνευση να μην είναι συνεχής, ούτως ώστε να μην σπαταλώνται οι περιορισμένοι πόροι του ad hoc δικτύου, η περίοδος ανίχνευσης μπορεί να ξεκινά όταν κάποιος κόμβος λάβει ένα κατάλληλο *voting_flag* από κάποιο γείτονά του. Δηλαδή η διαδικασία της ανίχνευσης εισβολέων και ακολούθως της αντίδρασης μπορεί να περιοριστεί μόνο κατά τις περιπτώσεις όταν οι κόμβοι πρέπει να συνεργαστούν για να εκλέξουν αρχηγό κατά τη χρονική διάρκεια μιας ψηφοφορίας που βρίσκεται σε εξέλιξη.

Η διαδικασία κατ’ αρχήν βασίζεται στην παρακολούθηση των δεδομένων που περιοδικά εκπέμπουν οι κόμβοι στη γειτονιά τους και τα οποία είναι απαραίτητα για να υπολογιστεί η μεταβλητή απόφασης V_i. Όπως είδαμε η μέγιστη τιμή της μεταβλητής απόφασης V_i κρίνει τον αρχηγό σε τοπικό επίπεδο. Ειδικότερα, το τμήμα παρακολούθησης αποθηκεύει σε κάθε κόμβο στη λίστα *Neighbor_Lists* (που αυτός διαθέτει) το βαθμό συνεκτικότητας που κάθε γείτονας κόμβος διαφημίζει ότι έχει. Ένας κακόβουλος κόμβος που προσπαθεί να μπει στο δίκτυο και να γίνει αυτός αρχηγός θα θελήσει να υπονομεύσει το αποτέλεσμα της εκλογής αρχηγού με το να διαφημίζει στους υπολοίπους ότι διαθέτει μεγάλο αριθμό γειτόνων, δηλαδή μεγάλο βαθμό συνεκτικότητας d_i, ή ότι έχει μεγάλο απόθεμα ενέργειας E_{ri}, ή ότι έχει καλή θέση στο δίκτυο (για παράδειγμα σε ένα δίκτυο WSN μεταδίδει ότι βρίσκεται κοντά στο σταθμό βάσης ώστε να έλκει τη δρομολόγηση των πακέτων προς το μέρος του) ή θα προσπαθήσει να αλλοιώσει οποιαδήποτε άλλη πληροφορία ελέγχου του δικτύου.

Είναι λοιπόν πολύ πιθανό το σενάριο ο επιτιθέμενος να εκλεγεί επειδή θα εμφανίσει μέγιστη τιμή της μεταβλητής V και άρα στη συνέχεια μπορεί να χρησιμοποιήσει προς όφελός του όλα τα μηνύματα που θα του στέλνουν οι κόμβοι-μέλη της περιοχής όπου θα είναι αρχηγός.

Η τεχνική της ανίχνευσης που υιοθετείται από το προτεινόμενο σχήμα SC-GPSR βασίζεται στην εύρεση εκείνων των δεδομένων που έχουν πρώτα συγκεντρωθεί από διαφορετικούς κόμβους κατά τη διάρκεια της διαδικασίας ομαδοποίησης και που παρουσιάζουν ασυνέπειες-αντιφάσεις μεταξύ τους. Η τεχνική πρώτα απαιτεί την προσωρινή αποθήκευση (“buffering”) σε κάθε κόμβο ενός ικανού αριθμού από πακέτα εκπομπής beacons τα οποία επεξεργάζεται η λειτουργική οντότητα της περιοδικής παρακολούθησης προκειμένου να αποκαλύψει τους ύποπτους κόμβους οι οποίοι διαχέουν ψευδή δεδομένα.

Ειδικότερα, σε κάθε κόμβο τα beacons αποθηκεύονται στον ενταμιευτή BEACON_buffer (μέχρι 64 πακέτα) και η χρήσιμη πληροφορία για την ανίχνευση βρίσκεται στο Neighbor_List που κάθε πακέτο beacon εμπεριέχει. Ως εκ τούτου, το “monitoring block” επεξεργάζεται πληροφορία σχετική με κόμβους που βρίσκονται μέχρι και δύο βήματα μακριά από τον κάθε κόμβο που βρίσκεται υπό

παρακολούθηση. Η ακτίνα των δύο βημάτων ορίζει την περιοχή που ανιχνεύεται γύρω από κάθε κόμβο για την ύπαρξη υπόπτων κόμβων από το πρωτόκολλο SC-GPSR ("suspicious_range").

Επιπρόσθετα, η προτεινόμενη τεχνική χρησιμοποιεί τη μέθοδο της ανίχνευσης υπόπτων κόμβων με βάση καθορισμένες τιμές κατωφλίου όταν αυτές υπερβαίνονται. Το σχήμα SC-GPSR απαιτεί να πληρούνται συγκεκριμένα επίπεδα συνέπειας καθώς και να υπάρχει συμφωνία για τον τοπικό αρχηγό. Ειδικότερα ο βαθμός d_i που ένας κόμβος *i* διαφημίζει συγκρίνεται με τα παρακάτω δύο κατώφλια από το monitoring block του SC-GPSR προκειμένου να ληφθεί απόφαση αν πρόκειται για ύποπτο ή όχι κόμβο. Έστω ότι ο κόμβος *n* είναι ανιχνευτής που παρακολουθεί τον κόμβο *i* κατά τη διάρκεια μιας ψηφοφορίας. Τότε τα δύο κατώφλια ανίχνευσης υπόπτου ορίζονται ως εξής:

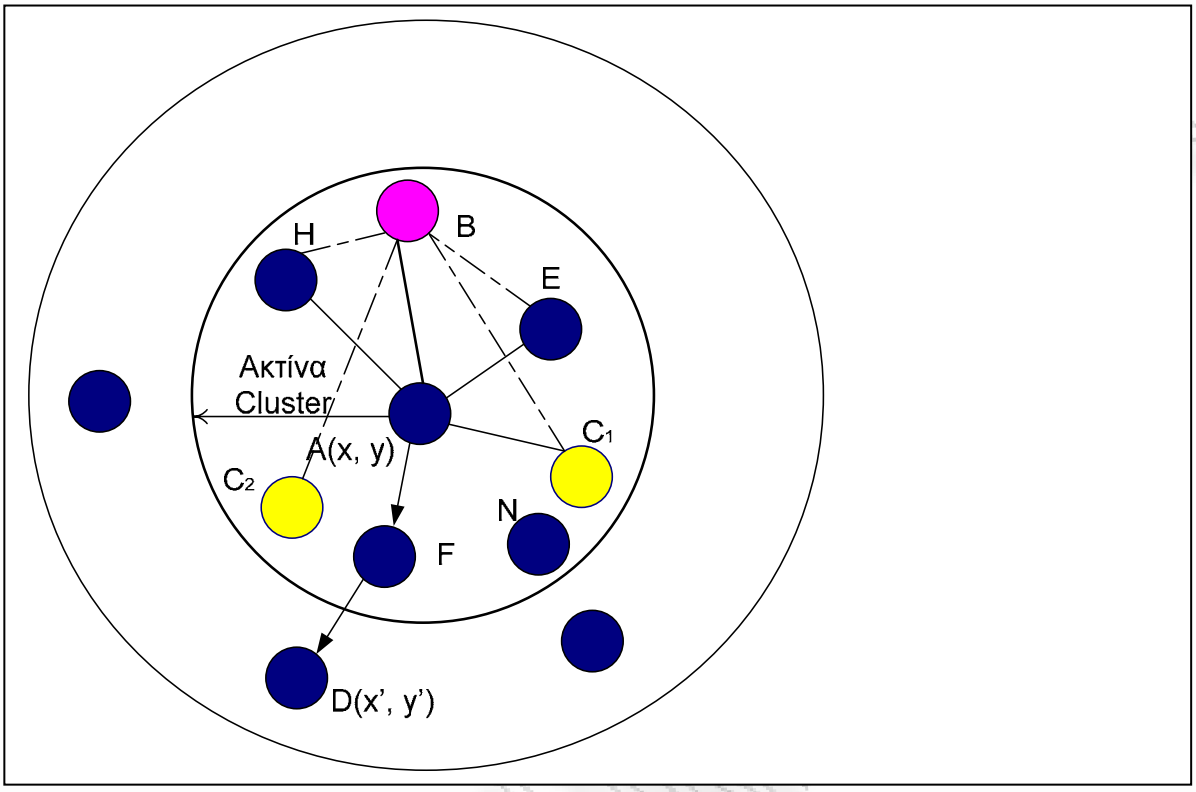
- ***Ανώτερο κατώφλι.*** Το σχήμα θέτει μια μέγιστη τιμή (προκαθορισμένη ή και δυναμικά καθοριζόμενη) στον αριθμό των γειτόνων που ένας κόμβος μπορεί να διαφημίσει ότι έχει. Δηλαδή ένας κόμβος για να γίνει αποδεκτός κατά τη διάρκεια της διαδικασίας της ψηφοφορίας θα πρέπει να έχει στείλει μια εύλογη τιμή του βαθμού συνεκτικότητας d_i η οποία, σύμφωνα με τη σχεδίασή μας, δε θα πρέπει να υπερβαίνει το μέγιστο επιτρεπτό μέγεθος του cluster. Απαραίτητη προϋπόθεση είναι το μέγεθος του cluster να είναι μια κρυφή παράμετρος του συστήματος την οποία θα πρέπει να γνωρίζουν μόνο οι νόμιμοι κόμβοι.

  Εκείνοι οι κόμβοι που δεν περνούν το πρώτο αυτό κατώφλι αποτυγχάνουν να ενταχθούν στη λίστα των "πρωταρχικών υποψήφιων κόμβων" εφόσον δεν υπολογίζονται από τον αλγόριθμο RRA και στη συνέχεια εντάσσονται στη λίστα των ύποπτων των κόμβων που τους ανίχνευσαν. Επιπρόσθετα, στη συνέχεια ούτε και η ψήφος που μπορεί να προέρχεται από κάποιο κόμβο που περιέχεται στη λίστα με τους ύποπτους θα καταμετρηθεί στην διαδικασία της ψηφοφορίας.

- ***Κατώτερο κατώφλι***. Στη συνέχεια, και εφόσον ο παρακολουθούμενος κόμβος *i* δεν έχει χαρακτηριστεί ύποπτος στο προηγούμενο βήμα, ο βαθμός d_i αυτού συγκρίνεται με τον αριθμό των γειτόνων του ανιχνεύοντος κόμβου *n* που συμπεριλαμβάνουν τον κόμβο *i* στις λίστες με τους γείτονες που έχουν διαφημίσει ότι διαθέτουν. Αυτό επιτυγχάνεται εξετάζοντας το BEACON_buffer ο οποίος περιέχει τις Neighbor_Lists των γειτόνων του κόμβου *n*. Ειδικότερα, αν σε αυτή τη λίστα βρεθούν περισσότεροι από $(2/3) * d_i$ γείτονες του ανιχνευτή *n* να έχουν τον κόμβο *i* στις λίστες τους τότε ο κόμβος *i* και η ψήφος του είναι αποδεκτά, οπότε η ψήφος θα προστεθεί στο *Votes_Table* του κόμβου-ανιχνευτή. Ως εκ τούτου, το τείχος παρακολούθησης δίνει εγγυήσεις συμφωνίας μεταξύ των δεδομένων ελέγχου που ανταλλάσσουν οι ad hoc κόμβοι στο τοπικό επίπεδο πριν καταλήξουν στην εκλογή του αρχηγού. Σύμφωνα με τα παραπάνω η ακτίνα που εξετάζει το σχήμα SC-GPSR για την εύρεση υπόπτων εισβολέων είναι ίση με δύο φορές την ακτίνα ραδιο-κάλυψης των ασύρματων κόμβων, δηλαδή ίση με δύο βήματα.

Η τιμή του κάτω κατωφλίου του σχήματος SC-GPSR προκύπτει από την αρχή των κατανεμημένων συστημάτων που ορίζει ότι συμφωνία για την εκλογή αρχηγού μπορεί να επιτευχθεί μόνο όταν περισσότερες από (2/3) * *N* οντότητες έχουν προτείνει τον ίδιο υποψήφιο [33]. Στο ad hoc δίκτυο, όταν παρακολουθούμε ένα κόμβο, κάνουμε τη συνθήκη αυτή πιο ελαστική απαιτώντας ο λόγος των κόμβων *N* που έχουν ακούσει τον κόμβο προς το βαθμό συνεκτικότητας που αυτός διαφημίζει *k* να είναι μεγαλύτερος από 2/3, δηλαδή θα πρέπει να ισχύει:

$$N \geq 3k + 1 \qquad (2)$$



Εικόνα 42. Ανίχνευση των υπόπτων γειτόνων με την οντότητα παρακολούθησης του σχήματος SC-GPSR.

Η Εικόνα 42 απεικονίζει ένα παράδειγμα ανίχνευσης εισβολέων που εισάγουν ψευδή δεδομένα στο δίκτυο για να παραπλανήσουν τους νόμιμους κόμβους. Το σχήμα SC-GPSR ελέγχει τα πακέτα που λαμβάνονται από τους γειτονικούς κόμβους. Στην Εικόνα 43 απεικονίζεται ένας ανιχνευτής αρχηγός, ο κόμβος A, και γύρω από αυτόν η συστάδα με ακτίνα ίση με την ακτίνα ραδιο-κάλυψης (απόσταση ενός βήματος). Αυτό εξηγείται από το γεγονός ότι ο αρχηγός εκλέγεται με υπολογισμό της RRA μεταβλητής απόφασης V_i η οποία αφορά τους κόμβους *i* που βρίσκονται σε απόσταση ενός βήματος από τον κόμβο A. Ακόμη στην ίδια εικόνα απεικονίζεται και η "ακτίνα των υπόπτων" ("suspicious range") η οποία εξετάζεται από το monitoring block και η οποία βρίσκεται σε απόσταση δυο βημάτων από τον κόμβο A. Ειδικότερα το ακόλουθο σενάριο παρουσιάζεται στην Εικόνα 42.

Ο κόμβος A ακούει τον κόμβο B ο οποίος έχει εισέλθει στην ακτίνα κάλυψης του A. Ο κόμβος B διαφημίζει ότι έχει τέσσερις γείτονες: τους κόμβους A, H, E and C_1. Ο ισχυρισμός του κόμβου B για γειτνίαση με τους κόμβους A, H and E είναι έγκυρος, ενώ ο κόμβος C_1 στην πραγματικότητα δεν είναι γείτονας του B εφόσον βρίσκεται πολύ μακρύτερα από την απόσταση του ενός βήματος από τον κόμβο A. Ο κόμβος A που βρίσκεται σε κατάσταση παρακολούθησης θα εξετάσει όλους τους γείτονες που βρίσκονται τόσο σε απόσταση ενός βήματος όσο και σε απόσταση δύο βημάτων από τον A για να βρει πόσοι κόμβοι έχουν δηλώσει τον κόμβο B ως γειτονικό τους κόμβο. Η ακτίνα των υπόπτων θα εξεταστεί με βάση τον ενταμιευτή *BEACON_buffer*. Στην περίπτωση όπου τρεις ή περισσότεροι κόμβοι περιέχουν στις λίστες των γειτόνων τους τον κόμβο B, τότε ο B θα περάσει τη δοκιμή του κάτω κατωφλίου. Στην Εικόνα 42 τρεις κόμβοι, με την υπόθεση ότι μόνο ο B λέει ψέματα, θα βρεθούν να έχουν τον κόμβο B στις λίστες των γειτόνων τους, δηλαδή οι κόμβοι H, A and E, ενώ ο C_1 δεν θα περιέχει τον κόμβο B σα γειτονικό του κόμβο. Συνεπώς θα έχουμε ανίχνευση ύποπτης κατάστασης όσον αφορά τον κόμβο B. Στην περίπτωση όπου ο κόμβος B είχε διαφημίσει βαθμό συνεκτικότητας κατά ένα μεγαλύτερο, δηλαδή (k=5) τότε η συνθήκη της ακεραιότητας της ψηφοφορίας δε θα είχε ικανοποιηθεί, το monitoring block θα το είχε ανιχνεύσει

και ο κόμβος B θα είχε μαρκαριστεί σαν ύποπτος και συνεπώς θα απαιτείτο περαιτέρω αυθεντικοποίηση του κόμβου B.

Επίσης, η Εικόνα 42 απεικονίζει τη *greedy* γεωγραφική δρομολόγηση που εφαρμόζει το σχήμα SC-GPSR για την προώθηση πακέτων από την πηγή στον προορισμό. Έστω ότι η πηγή είναι ο κόμβος A και έστω ότι ο τελικός προορισμός είναι εντός της ακτίνας κάλυψης του κόμβου, έστω ο κόμβος F. Σε μια τέτοια περίπτωση σύμφωνα με τη greedy τακτική ο κόμβος A θα στείλει όλα τα πακέτα του απευθείας στον κόμβο F. Αντίθετα, αν ο τελικός προορισμός βρίσκεται πολλά βήματα μακριά, για παράδειγμα είναι ο κόμβος D, τότε θα έχουμε multi-hop δρομολόγηση. Συγκεκριμένα ο κόμβος F θα επιλεγεί από τον κόμβο A ως ενδιάμεσος κόμβος για να προωθήσει τα πακέτα στον κόμβο D. Έτσι, όπως φαίνεται στην Εικόνα 42 ο γειτονικός κόμβος N δεν επιλέγεται από τον κόμβο A, εφόσον η απόστασή του από τον τελικό κόμβο D είναι μεγαλύτερη από την απόσταση που έχει ο γειτονικός κόμβος F από τον κόμβο D. Έτσι ενδιάμεσος κόμβος στο μονοπάτι A-D θα είναι ο F σύμφωνα με τον κανόνα της greedy γεωγραφικής δρομολόγησης.

Στην περίπτωση όπου κατά τη greedy δρομολόγηση πακέτων από την πηγή στον τελικό προορισμό συναντάται ένα σημείο *void* από τον αλγόριθμο δρομολόγησης, τότε το SC-GPSR λειτουργεί όπως το GPSR και εισέρχεται σε δρομολόγηση *perimeter*. Με το *perimeter mode* τα πακέτα από την πηγή φτάνουν στον τελικό κόμβο-προορισμό με την τεχνική προώθησης πακέτων μέσω των “planar graphs“. Έτσι στο σχήμα SC-GPSR είναι δυνατόν να έχουμε πολλές εναλλαγές ανάμεσα στα modes δρομολόγησης greedy και perimeter ανάλογα και με τις ιδιαιτερότητες των ad hoc τοπολογιών των δικτύων.

6.4.4. Το Τείχος Κρυπτογραφικής Προστασίας

Το τείχος του SC-GPSR που βασίζεται σε κρυπτογραφικές μεθόδους προστατεύει από τις επιθέσεις οι οποίες κατά κύριο λόγο απειλούν την εμπιστευτικότητα, την ακεραιότητα και την αυθεντικότητα των μηνυμάτων που ανταλλάσσονται και επιπλέον απειλούν την αυθεντικότητα των κόμβων. Όπως είδαμε το σχήμα SC-GPSR μεταδίδει τα δεδομένα της οργάνωσης σε συστάδες και όχι σε ξεχωριστά πακέτα ελέγχου αλλά περιλαμβάνει την πληροφορία της αυτο-οργάνωσης μέσα στα πακέτα φάρους (beacons) που μεταδίδονται με περιοδικό τρόπο από τους κόμβους.

Τέτοια πληροφορία η οποία εκπέμπεται εντός των beacon broadcasts είναι οι ψήφοι των κόμβων για τον τοπικό αρχηγό, η τιμή της μεταβλητής απόφασης V_i, η ταυτότητα των ενδιάμεσων κόμβων-δρομολογητών των μηνυμάτων και οι γεωγραφικές συντεταγμένες των ενδιάμεσων κόμβων. Αυτή η πληροφορία είναι πραγματικά ευαίσθητη και δε θα πρέπει να μεταδίδεται με ανοιχτό τρόπο μέσα στο δίκτυο. Η επιλογή μας για προστασία με κρυπτογραφικό τρόπο είναι η χρήση των Hashed Message Authentication Codes (HMAC) για την κωδικοποίηση των αντίστοιχων πεδίων μέσα στα πακέτα beacons. Αυτό προϋποθέτει την ύπαρξη ενός κοινού κλειδιού που υποθέτουμε ότι είναι φορτωμένο και διαθέσιμο στους κόμβους του δικτύου ad hoc από την αρχή της λειτουργίας του.

Το τείχος της κρυπτογραφικής προστασίας του SC-GPSR προστατεύει τα παραπάνω ευαίσθητα δεδομένα από μετατροπές και από λαθραία ανάγνωση που μπορούν να επιχειρήσουν οι κακόβουλοι κόμβοι. Η πρόσθετη προστασία που παρέχει ο συμμετρικός αλγόριθμος HMAC είναι ότι τα μηνύματα που λαμβάνονται σε ένα άκρο αυθεντικοποιούνται, δηλαδή μπορεί να διαπιστωθεί η αυθεντικότητα του αρχικού κόμβου που έστειλε κάποια πληροφορία μαζί με την υπογραφή της HMAC εντός του beacon με το να συγκριθεί η υπογραφή HMAC που φέρει το beacon με την υπογραφή που μπορεί να παράξει ο κόμβος-προορισμός με βάση το κοινό κλειδί και την πληροφορία που λαμβάνει από τον αποστολέα.

Υλοποιήσαμε τον πρότυπο αλγόριθμο HMAC με βάση τις συναρτήσεις κατακερματισμού MD-5 και SHA-1, από τις κατάλληλες βιβλιοθήκες ασφαλείας της πλατφόρμας Java2 SDK. Στην περίπτωση του HMAC με συνάρτηση κατακερματισμού την MD-5 το παραγόμενο συμμετρικό κλειδί είναι 64

bytes και το μέγεθος της υπογραφής HMAC είναι 16 bytes. Αυτό είναι ένα αποδεκτό μέγεθος για την το πεδίο της υπογραφής δεδομένου των περιορισμών για το μέγιστο επιτρεπτό συνολικό μήκος των πακέτων που μπορούν να διακινηθούν σε ένα ασύρματο δίκτυο ad hoc.

Υποθέσαμε ότι κανένας ενδιάμεσος κόμβος δεν πιστοποιεί τα μηνύματα που λαμβάνει και ότι μόνο ο κόμβος που βρίσκεται στον τελικό προορισμό ελέγχει την ακεραιότητα των μηνυμάτων που έστειλε ο κόμβος-πηγή. Έτσι αν κάποιο μήνυμα μετατράπηκε σκοπίμως από έναν επιτιθέμενο, ή αν ένας κόμβος παρεμβλήθηκε στις επικοινωνίες χωρίς να είναι αυθεντικός, θα διαπιστωθεί στον τελικό μόνο κόμβο με την επαλήθευση της υπογραφής HMAC. Ο τελικός κόμβος στην περίπτωση ενός WSN είναι ο Σταθμός Βάσης. Επιλέξαμε τη λύση της από άκρου εις άκρον αυθεντικοποίησης με βάση τον HMAC έτσι ώστε να διαφυλάξουμε την κατανάλωση των πόρων των κόμβων σε ανεκτά επίπεδα.

Το κρυπτογραφικό τείχος προστασίας λειτουργεί σαν μια δεύτερη γραμμή άμυνας και συμπληρώνει την ασφάλεια του μη κρυπτογραφικού τείχους παρακολούθησης που περιγράψαμε προηγούμενα. Έτσι ένας κόμβος που απέτυχε να περάσει ένα από τα δύο κατώφλια ανίχνευσης του SC-GPSR κατηγοριοποιείται σαν ύποπτος και αρχικά εγγράφεται στην λίστα “suspects_lists”. Στη συνέχεια, ένας ύποπτος κόμβος αυθεντικοποιείται περαιτέρω με το να πιστοποιείται η αυθεντικότητα των πληροφοριών που στέλνει μέσα στα πακέτα beacons σαν πεδία HMAC. Στην περίπτωση που η επαλήθευση HMAC δεν είναι επιτυχής, τότε ο ύποπτος κόμβος θεωρείται ότι είναι πραγματικά κακόβουλος και οι κόμβοι που τον ανίχνευσαν τον διαγράφουν αμέσως από τη λίστα Neighbor_Lists που περιέχει όλους τους γείτονές τους που βρίσκονται σε απόσταση ενός βήματος. Με αυτόν τον τρόπο το SC-GPSR routing block των κόμβων-ανιχνευτών δεν πρόκειται να προωθήσει άλλα πακέτα στον κακόβουλο κόμβο. Επιπρόσθετα, οι κόμβοι-ανιχνευτές είναι υποχρεωμένοι να μεταδώσουν ένα ειδικό πακέτο ευρείας εκπομπής BLACKLIST το οποίο περιέχει την ταυτότητα του κακόβουλου κόμβου που ανίχνευσαν.

Στην περίπτωση που απαιτούνται μεγαλύτερα επίπεδα ασφαλείας από την εφαρμογή ad hoc, συνιστάται η δυναμική δημιουργία και εγκατάσταση συμμετρικών κλειδιών μεταξύ των πιθανών ζευγών κόμβων που πρόκειται να εγκαταστήσουν μια ασφαλή ζεύξη μεταξύ τους. ‘Ενα τέτοιο σχήμα με δυναμικά συμμετρικά κλειδιά που δημιουργούνται ανά ζεύγη κόμβων αποφεύγει τη χρήση ενός μοναδικού κλειδιού τόσο στο επίπεδο του δικτύου (network key), όσο και στο επίπεδο της ομάδας κόμβων (group keys). Επιπλέον, προκειμένου ένα τέτοιο σχήμα κλειδιών να είναι ανθεκτικό σε επιθέσεις ταυτότητας που στοχεύουν στην παραποίηση της ταυτότητας των κόμβων συνιστούμε τα κλειδιά αυτά να δημιουργούνται με την τεχνική Address Based Keys (ABK) [32]. Βασιζόμενοι στην τεχνική ABK, προτείνουμε ένα κοινό κλειδί μεταξύ δύο κόμβων να δημιουργείται από το hashing των δύο προσωπικών κλειδιών των κόμβων που ο καθένας από αυτούς έχει δημιουργήσει με βάση την ταυτότητά του (κάποιο ID δηλαδή που μπορεί να είναι η MAC διεύθυνση, η IP διεύθυνση, ή ο αριθμός του κόμβου μέσα στο ad hoc δίκτυο) και με την προσθήκη των απαραίτητων και κατά τυχαίο τρόπο παραγόμενων nonces.

Έτσι αρχικά υποθέτουμε ότι οι δύο κόμβοι *i* και *j* έχουν παράξει τα προσωπικά τους κλειδιά K_i και K_j με βάση την ταυτότητά τους σύμφωνα με τον παρακάτω τρόπο:

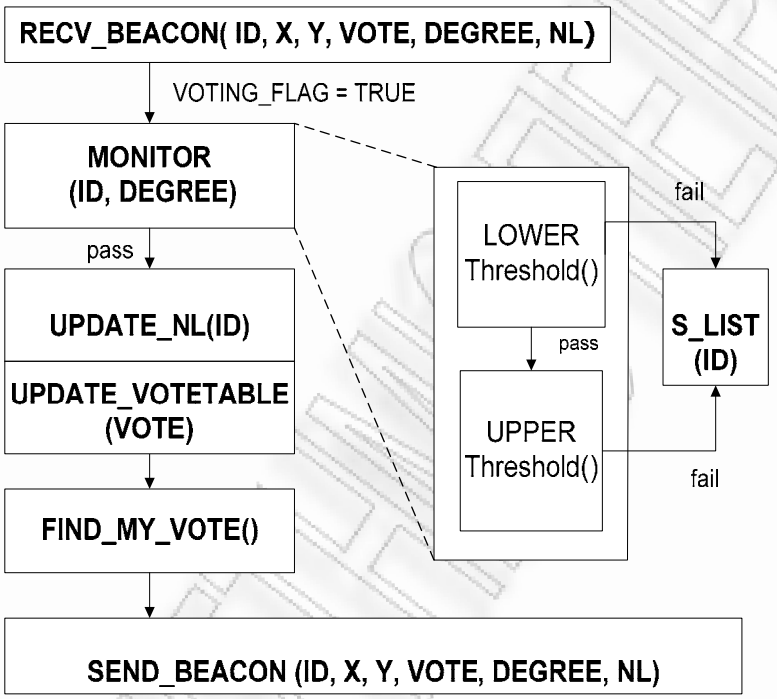
$K_i = Hash(ID_i, nonce_i)$.

$K_j = Hash(ID_j, nonce_j)$
Όπου $nonce_i$ δηλώνει τυχαίο αριθμό παραγόμενο στο χρόνο t_i. Στη συνέχεια οι δύο κόμβοι μπορούν να διασφαλίσουν τις μεταξύ τους επικοινωνίες παράγοντας το κοινό κλειδί κρυπτογράφησης K_c σύμφωνα με τον παρακάτω τρόπο:

$K_c = 2 * Hash(K_i, K_j, nonce_m, nonce_n)$.

Το παραπάνω δυναμικό σχήμα παραγωγής κλειδιών εκτός από την προστασία της ψηφοφορίας είναι κατάλληλο και για την εγκατάσταση ασφαλών ζεύξεων από cluster head σε cluster head στη δρομολόγηση πακέτων κατά μήκος μονοπατιών πολλαπλών βημάτων σε ένα δίκτυο MANET ή ακόμη και για την εγκατάσταση δυναμικών συμμετρικών κλειδιών κρυπτογράφησης μεταξύ των νέων κόμβων-αρχηγών και του Σταθμού Βάσης σε ένα ιεραρχικό δίκτυο αισθητήρων (WSN) ή/και σε ένα ad hoc δίκτυο οχημάτων (VANET).

6.4.5. Ρεπερτόριο Μηνυμάτων του Εκτεταμένου Σχήματος SC-GPSR



Εικόνα 43. Τα λειτουργικά τμήματα του SC-GPSR μεταξύ της λήψης και της εκπομπής ενός πακέτου beacon.

Τα λειτουργικά τμήματα της ομαδοποίησης, της παρακολούθησης και της ψηφοφορίας παρεμβάλλονται μεταξύ της μετάδοσης και της λήψης των μηνυμάτων beacon με τα πεδία (ID, X, Y, Vote_ID, connectivity_degree, Neighbor_List) με τον τρόπο που φαίνεται στην πιο πάνω Εικόνα 43. Ο Πίνακας 3 παρουσιάζει το σύνολο των μηνυμάτων που χρησιμοποιεί το σχήμα SC-GPSR για την αυτο-οργάνωση και την αυτο-προστασία ενός δικτύου ad hoc. Ο Πίνακας 3 παρουσιάζει τους τυπικούς τύπους πακέτων που ορίζει το πρωτόκολλο GPSR (PROBE, DATA_GREEDY και DATA_PERIMETER) καθώς και τα επιπλέον πακέτα με τα επιπλέον πεδία τους (δηλαδή εκτός της ταυτότητας και των συντεταγμένων των κόμβων) που χρησιμοποιεί το εκτεταμένο σχήμα SC-GPSR σε σχέση με το GPSR. Με το εκτεταμένο σχήμα ομαδοποίησης των κόμβων SC-GPSR τα επιπλέον πακέτα είναι τα CH_ANNOUNCEMENT, CH_ASSOCIATION και BLACKLIST.

Είναι προφανές ότι το μεγαλύτερο βάρος της πληροφορίας που είναι απαραίτητη για την οργάνωση των κόμβων σε ομάδες και την εκλογή μέσω ψηφοφορίας των αρχηγών μεταφέρεται από το πακέτο Beacon και η πληροφορία αυτή είναι η τιμή της μεταβλητής απόφασης *V*, η ψήφος των κόμβων *my_Vote* και οι λίστες των γειτόνων των κόμβων στο πεδίο *Neighbor_List* (NL) που διαφοροποιούν σε σημαντικό βαθμό το GPSR από το εκτεταμένο σχήμα SC-GPSR.

ΤΥΠΟΣ ΠΑΚΕΤΟΥ	ΠΕΔΙΑ ΠΑΚΕΤΟΥ
Εκτεταμένο BEACON	ID, *Role*, *NL*, *CH_ID* HMAC(X, Y), HMAC(V_i) HMAC(*my_Vote*)
CH_ ANNOUNCEMENT	CH_ID X_{CH_ID}, Y_{CH_ID} CHALLENGE
CH_ ASSOCIATION	CH_ID
BLACKLIST	ID
DATA_GREEDY	Application-level data
DATA_PERIMETER	GPSR πακέτο ελέγχου τοπολογίας
PROBE	GPSR πακέτο ελέγχου

Πίνακας 3: Το ρεπερτόριο μηνυμάτων του εκτεταμένου σχήματος SC-GPSR.

Με αυτόν τον τρόπο όλη η πληροφορία της αυτο-οργάνωσης γίνεται piggybacked στα πακέτα beacon και οι επιπρόσθετοι τύποι πακέτων που εισάγει το σχήμα SC-GPSR είναι μόνο τρεις. Αυτό πρόκειται να ελαττώσει σημαντικά την επιβάρυνση που προσθέτουν οι μηχανισμοί αυτο-οργάνωσης και αυτο-προστασίας στις επικοινωνίες του αυτόνομου ad hoc δικτύου. Αυτό θα γίνει εμφανές και στα πειραματικά αποτελέσματα όπου το εκτεταμένο σχήμα πέτυχε πολύ καλή δικτυακή απόδοση.

Ωστόσο, είναι αναπόφευκτο ένα υπολογιστικό κόστος που οφείλεται στον υπολογισμό των υπογραφών HMAC οι οποίες χρησιμοποιούνται από το SC-GPSR για την ασφάλεια και την προστασία της ιδιωτικότητας των κόμβων όσο και της ψήφου τους (τον κόμβο που προτιμούν για αρχηγό δηλαδή), των συντεταγμένων θέσης και της ταυτότητας των κόμβων.

Μετά από την εκλογή του τοπικού αρχηγού στη γειτονιά μιας ομάδας κόμβων, ο νέος αρχηγός εκπέμπει το μήνυμα CH_ANNOUNCEMENT για να γνωστοποιήσει στους γείτονές του την ταυτότητά του (CH_ID στον Πίνακα 3) και προαιρετικά τις συντεταγμένες του (X_{CH_ID}, Y_{CH_ID}, στον Πίνακα 3). Επιπλέον για λόγους ασφάλειας ο αρχηγός πρέπει να μεταδώσει ένα πεδίο “challenge” εντός του μηνύματος CH_ANNOUNCEMENT το οποίο υπολογίζεται ως το HMAC ενός κοινού μυστικού που όλοι οι κόμβοι γνωρίζουν, όπως φαίνεται παρακάτω:

challenge = HMAC(“common_secret”, broadcast_key). (3)

Για τον υπολογισμό του πεδίου challenge είναι απαραίτητο το κλειδί broadcast_key το οποίο προκύπτει από το κλειδί που είναι προ-φορτωμένο σε όλους τους αυθεντικούς κόμβους του δικτύου, όπως φαίνεται παρακάτω:

broadcast_key = Hash(global_key, nonce(t)) (4)

όπου nonce είναι ένας τυχαία παραγόμενος αριθμός σε μια δεδομένη χρονική στιγμή t και μόνο τότε.

Ακολουθεί το σχήμα “challenge-response” που εφαρμόζεται από το εκτεταμένο σχήμα SC-GPSR με σκοπό να διασφαλίσει τη διαδικασία της ανακοίνωσης του νέου αρχηγού από κόμβο που είναι πραγματικά ένας από τους αυθεντικούς κόμβους του δικτύου.

Ένας νέος εκλεγμένος κόμβος-αρχηγός ταυτότητας CH_ID:

Δημιουργεί το broadcast_key τη χρονική στιγμή t_1: broadcast_key = Hash (global_key, nonce(t_1)).
Δημιουργεί το πεδίο challenge = HMAC("common_secret", broadcast_key).

Εκπέμπει στους γείτονες το μήνυμα CH_ANNOUNCEMENT (CH_ID, X, Y, challenge, nonce(t_1))

Κάθε γείτονας ταυτότητας ID που λαμβάνει το μήνυμα CH_ANNOUNCEMENT:

Δημιουργεί το broadcast_key χρησιμοποιώντας το nonce(t_1):
broadcast_key = Hash (global_key, nonce(t_1))

Πιστοποιεί το κοινό μυστικό από το challenge που έλαβε και το broadcast_key που δημιούργησε verify ("secret", challenge, broadcast_key)

Αν (verify = true) τότε ο γείτονας στέλνει την ταυτότητά του στον αρχηγό στο μήνυμα ASSOCIATE(ID, CH_ID)

Αν (verify = false) τότε ο γείτονας:
Μεταδίδει μήνυμα BLACKLIST(CH_ID) στους γείτονες και
Διαγράφει τον ύποπτο CH_ID από τη λίστα των γειτόνων του (CH_ID, Neighbor_List)

Εικόνα 44. Η διαδικασία αυθεντικοποίησης του νέου κόμβου-αρχηγού στο εκτεταμένο σχήμα SC-GPSR.

Όπως φαίνεται στην Εικόνα 44, με το πεδίο challenge οι γείτονες δοκιμάζουν την αυθεντικότητα του κόμβου που ισχυρίζεται πως είναι ο νέος εκλεγμένος αρχηγός στη γειτονιά έτσι ώστε να αποφευχθεί η περίπτωση ένας μη νόμιμος κόμβος να προσποιηθεί τον αρχηγό και άρα να να επωφεληθεί και να διαβάσει τα μηνύματα που θα στείλουν οι κόμβοι που θα συσχετιστούν με αυτόν. Έτσι οι γείτονες θα συσχετιστούν (associate) με τον νέο αρχηγό μόνο αν το αποτέλεσμα της πιστοποίησης είναι επιτυχές. Σε διαφορετική περίπτωση οι γειτονικοί κόμβοι θα ακολουθήσουν τις παρακάτω ενέργειες:

- Διαγραφή του ύποπτου CH_ID από τη λίστα των γειτόνων.
- Προσθήκη του ύποπτου CH_ID στη λίστα των υπόπτων κόμβων.
- Μετάδοση του μηνύματος BLACKLIST(CH_ID).

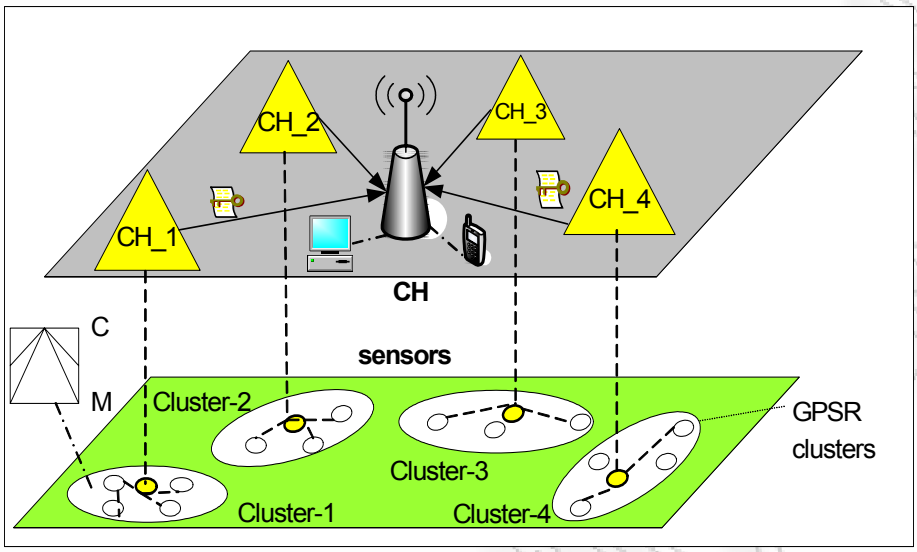
Στην περίπτωση εφαρμογών και σεναρίων ad hoc με ισχυρότερες απαιτήσεις ασφάλειας ο υπολογισμός των πεδίων HMAC μέσα στα πακέτα Beacon συνιστάται να κάνει χρήση των δυναμικά παραγόμενων συμμετρικών κλειδιών "Address Based Keys" όπως περιγράφηκε στην §6.4.4. Περαιτέρω, αν παρατηρηθεί ότι κάποιος κόμβος είναι ύποπτος κατά τη διαδικασία πιστοποίησης του κόμβου αρχηγού η πιο ασφαλής αντιμετώπιση είναι να γίνει επανάληψη της διαδικασίας της ψηφοφορίας.

6.5. ΕΠΙΔΟΣΗ ΤΟΥ ΣΧΗΜΑΤΟΣ SC-GPSR

Διεξαγάγαμε ένα εκτεταμένο αριθμό πειραμάτων στο επίπεδο του δικτύου με το εργαλείο προσομοίωσης J-Sim [43] με σκοπό να μελετήσουμε τη συμπεριφορά του προτεινόμενου εκτεταμένου σχήματος SC-GPSR και επίσης με σκοπό να συγκρίνουμε την επίδοση του SC-GPSR σε σχέση με το GPSR αλλά και με άλλα γνωστά ad hoc πρωτόκολλα όπως το AODV. Τα πειράματα συμπεριέλαβαν έναν αριθμό από κόμβους με κανονική συμπεριφορά και έναν αριθμό από κακόβουλους κόμβους που εξαπολύουν μια σειρά από διαφορετικές επιθέσεις. Κάθε πείραμα εξομοίωσης διαρκεί τουλάχιστον μια ώρα στον προσομοιωτή J-Sim. Προτού παρουσιάσουμε τα πειραματικά αποτελέσματα θα περιγράψουμε τις υποθέσεις που παραδεχθήκαμε για την εκτίμηση

της απόδοσης του προτεινόμενου σχήματος στην προσομοίωση.

6.5.1. Παραδοχές



Εικόνα 45. Σενάριο ιεραρχικής γεωγραφικής δρομολόγησης με το SC-GPSR.

- ***Τοποθέτηση των κόμβων***. Σε όλα τα πειράματα που διεξαγάγαμε με τον J-Sim η αρχική ad hoc τοπολογία ήταν ένα ομοιόμορφο πλέγμα κόμβων, όπως φαίνεται στην Εικόνα 45. Πειραματιστήκαμε με το μέγεθος του δικτύου μεταβάλλοντας τον αριθμό των κόμβων από 110 κόμβους μέχρι 1000 κόμβους κρατώντας σταθερό το βήμα του πλέγματος. Αντιθέτως, με τον ίδιο αριθμό κόμβων σε δύο διαφορετικά πειράματα μπορούμε να πετύχουμε διαφορετική πυκνότητα του δικτύου αν μεταβάλλουμε το βήμα του πλέγματος. Τα πειραματικά αποτελέσματα επικεντρώνονται στην περίπτωση των 110 κόμβων αρχικά τοποθετημένων σε ομοιόμορφο πλέγμα βήματος 20 μέτρων. Επίσης μετρήσαμε την επίδοση των αλγορίθμων τόσο με στατική τοπολογία (WSN) όσο και με κινούμενους κόμβους (MANET) με μέγιστη μέση ταχύτητα ίση με 50km/h. Κατά τη φάση της εγκατάστασης των κόμβων οι κόμβοι παίρνουν μοναδικό ID που τους διακρίνει στο δίκτυο και επίσης δημιουργούνται όλες οι δομές δεδομένων που προσομοιώνουν τα στοιχεία των πρωτοκόλλων που μελετώνται καθώς και τις δομές που είναι απαραίτητες για την δημιουργία των ad hoc κόμβων στον J-Sim. Αρχικά όλοι οι κόμβοι αποκτούν το ρόλο του αρχηγού. Κατά τη διάρκεια του πειράματος οι ρόλοι πολλών κόμβων μεταβάλλονται σε απλά μέλη ενώ ένα μέρος των κόμβων παίρνει εξ αρχής το ρόλο του επιτιθέμενου.
- ***Ομοιογένεια***. Υποθέτουμε ότι όλοι οι κόμβοι του συστήματος τρέχουν το ίδιο λογισμικό και ότι είναι ισοδύναμοι ως προς το υλικό που διαθέτουν, δηλαδή έχουν τα ίδια χαρακτηριστικά ασύρματης μετάδοσης (ρυθμός ασύρματης μετάδοσης και ακτίνα κάλυψης). Επίσης, η αποθηκευτική ικανότητα είναι ίδια για όλους τους κόμβους. Υποθέτουμε ότι οι κόμβοι διαθέτουν ικανή προσωρινή μνήμη για την αποθήκευση μέχρι και 64 πακέτων beacon το καθένα από τα οποία έχει μέγιστο μήκος 120 Bytes.
- ***Σενάριο δρομολόγησης***. Απεικονίζουμε το σενάριο δρομολόγησης που υποθέσαμε στην εξομοίωση ότι ακολουθούν οι κόμβοι για την προώθηση μηνυμάτων προς το Σταθμό Βάσης. Τα πειράματα προσομοίωσης εστίασαν σε δίκτυα ασύρματων αισθητήρων (WSN) που αυτό-οργανώνονται σε clusters δύο επιπέδων.

  Σύμφωνα με αυτό το σενάριο τα απλά μέλη των συστάδων (αισθητήρες) προωθούν τα πακέτα τους με την πληροφορία που έχουν διαβάσει από το περιβάλλον στους κόμβους-

αρχηγούς οι οποίοι μπορεί να βρίσκονται σε απόσταση πολλών βημάτων μακριά. Δηλαδή στα clusters που απεικονίζονται στην Εικόνα 45 υποθέτουμε ότι τρέχει το πρωτόκολλο SC-GPSR το οποίο χρησιμοποιούν οι απλοί κόμβοι για να προωθήσουν τα πακέτα τους κατά μήκος πολλών βημάτων, αν χρειαστεί, μέχρι να φτάσουν τα δεδομένα στον τελευταίο αρχηγό με τον οποίο έχουν συσχετιστεί. Στη συνέχεια, οι τοπικοί αρχηγοί επεξεργάζονται ενδοδικτυακά τα δεδομένα που λαμβάνουν από το cluster εκτελώντας πράξεις όπως εξαγωγή μέσης τιμής κ.α. και στη συνέχεια μεταδίδουν το επεξεργασμένο αποτέλεσμα στο Σταθμό Βάσης ο οποίος υποθέτουμε ότι βρίσκεται μόνο ένα βήμα μακριά από όλους τους αρχηγούς του δικτύου (συνολικά τέσσερις στο σχήμα). Κάτω από αυτές τις συνθήκες εκτιμήσαμε και συγκρίναμε την επίδοση του GPSR και του προτεινόμενου ασφαλούς σχήματος SC-GPSR.

- ***Μοντελοποίηση επιθέσεων***. Στα πειράματα που διεξαγάγαμε υποθέσαμε ότι στο επίπεδο του δικτύου το WSN απειλείται από ένα συγκεκριμένο ενεργητικό τύπο απειλών, αυτόν της άρνησης προώθησης μηνυμάτων από κακόβουλους κόμβους που έχουν εισέλθει στο δίκτυο. Σύμφωνα με αυτόν τον τύπο επιθέσεων ένας ενδιάμεσος κακόβουλος κόμβος μπορεί να απορρίπτει όσα πακέτα λαμβάνει χωρίς να τα προωθεί προς τον τελικό προορισμό, περίπτωση επίθεσης που είναι γνωστή ως επίθεση μαύρης τρύπας, ή μπορεί ο επιτιθέμενος να απορρίπτει επιλεκτικά ένα μόνο μέρος αυτών των πακέτων, για παράδειγμα αφού πρώτα εξετάσει ποιος είναι ο αρχικός κόμβος ή αφού εξετάσει το μέγεθος του πακέτου ή μπορεί να διαγράψει με εντελώς τυχαίο τρόπο τα πακέτα (επίθεση γκρι τρύπας). Ακόμη μια άλλη επίθεση σε αυτήν την κατηγορία είναι και η επίθεση των εγωιστικών κόμβων οι οποίοι αφού εξετάσουν τα αποθέματα των πόρων που διαθέτουν και τα βρουν ανεπαρκή βάσει υποκειμενικών κριτηρίων, όπως για παράδειγμα λόγω χαμηλής στάθμης ενέργειας, δεν προωθούν περαιτέρω τα πακέτα που λαμβάνουν.

  Ένα κοινό χαρακτηριστικό γνώρισμα αυτών των κακόβουλων κόμβων είναι ότι προσπαθούν να εξαπατήσουν το δίκτυο πρώτα ώστε να κάνουν τους υπόλοιπους να τους προτιμήσουν σαν το επόμενο βήμα στη δρομολόγηση των πακέτων. Έτσι σε πολλές περιπτώσεις οι επιθέσεις άρνησης προώθησης μηνυμάτων έπονται κακόβουλων ενεργειών που στοχεύουν να αλλοιώσουν την ορθή και συνεπή λειτουργία του δικτυακού πρωτοκόλλου και των δικτυακών εφαρμογών. Οι επιτιθέμενοι για να το επιτύχουν αυτό συνήθως διαφημίζουν στους υπολοίπους ότι βρίσκονται σε μικρή απόσταση από το Σταθμό Βάσης ο οποίος είναι ο τελικός προορισμός σε ένα δίκτυο WSN. Οι γειτονικοί κόμβοι σε περίπτωση που θα πειστούν θα προωθήσουν τα πακέτα τους στους κακόβουλους κόμβους οι οποίοι στη συνέχεια θα τα απορρίψουν με έναν από τους τρόπους που περιγράψαμε.

Στα πειράματά μας υποθέσαμε ότι οι κακόβουλοι κόμβοι αρχικά επιτίθενται στη διαδικασία της ομαδοποίησης και της εκλογής αρχηγών προσπαθώντας να αλλοιώσουν το αποτέλεσμα της εκλογής αρχηγού. Αυτό μπορούν να το επιτύχουν με το να διαφημίζουν στους γείτονες ψευδείς πληροφορίες όσον αφορά τις παραμέτρους που λαμβάνει υπόψη ο αλγόριθμος ομαδοποίησης RRA. Για παράδειγμα, αν κάποιος καλά πληροφορημένος κακόβουλος κόμβος στέλνει μέσα στα πακέτα Beacon μια μεγάλη τιμή της μεταβλητής απόφασης V_i, τότε είναι πολύ πιθανό οι κόμβοι να επιλέξουν τον επιτιθέμενο σαν ένα από τους “πρωταρχικούς υποψήφιους” και στη συνέχεια να τον εκλέξουν ως αρχηγό αφού θα ικανοποιεί καλύτερα το κριτήριο μέγιστου με βάση το οποίο λειτουργεί ο αλγόριθμος εκλογής αρχηγού. Με όμοιο τρόπο μπορεί να μεταδίδει ψευδώς ότι έχει μεγάλα αποθέματα ενέργειας ή ότι έχει μεγάλο αριθμό από γείτονες ή ότι έχει καλή θέση μέσα στο δίκτυο. Στη συνέχεια, είναι πολύ εύκολο για τον κακόβουλο κόμβο που έχει καταφέρει να εκλεγεί τοπικός αρχηγός να συγκεντρώνει όλα τα δεδομένα που προέρχονται από το cluster και να εξαπολύει ένα μεγάλο αριθμό από παθητικές ή από ενεργητικές επιθέσεις, όπως υπεξαιρέσεις ταυτότητας και θέσης των υπολοίπων, αλλοιώσεις των ευαίσθητων δεδομένων για παραπλάνηση, καθολικές και επιλεκτικές απορρίψεις πακέτων, παραποίηση ταυτότητας (spoofing), επίθεση sybil κατά την οποία ο επιτιθέμενος παρουσιάζει ταυτόχρονα πολλές ταυτότητες και σε διαφορετικές

θέσεις, μια επίθεση ιδιαίτερα δύσκολο να ανιχνευθεί σε συνθήκες κίνησης των κόμβων, κ.α.

Ο Πίνακας 4 παρουσιάζει τα στοιχεία προστασίας που εισάγει το εκτεταμένο σχήμα SC-GPSR και κατ'αντιστοιχία ποιες επιθέσεις αντιμετωπίζονται.

ΧΑΡΑΚΤΗΡΙΣΤΙΚΟ ΠΡΟΣΤΑΣΙΑΣ	ΕΠΙΘΕΣΗ ΠΟΥ ΑΝΤΙΜΕΤΩΠΙΖΕΙ
ΣΥΝΕΠΗΣ ΕΚΛΟΓΗ ΑΡΧΗΓΟΥ	ΨΕΥΔΗ ΔΕΔΟΜΕΝΑ
	ΑΡΝΗΣΗ ΠΡΟΩΘΗΣΗΣ ΠΑΚΕΤΩΝ (επιθέσεις black, gray, selfish)
ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ ΜΗΝΥΜΑΤΩΝ	ΥΠΕΞΑΙΡΕΣΗ-ΑΛΛΟΙΩΣΗ ΜΗΝΥΜΑΤΩΝ
ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ ΤΑΥΤΟΤΗΤΑΣ ΚΟΜΒΩΝ	ΕΠΙΘΕΣΕΙΣ ΤΑΥΤΟΤΗΤΑΣ (spoofing, sybil)

Πίνακας 4: Η ανοχή σε επιθέσεις του εκτεταμένου σχήματος SC-CGPSR.

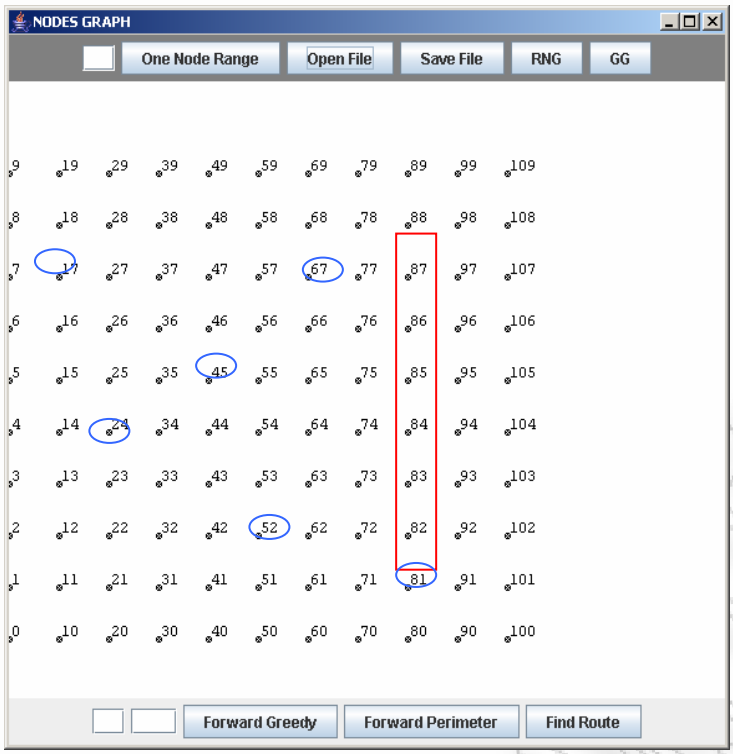
6.5.2. Ρύθμιση Παραμέτρων Προσομοίωσης στον J-Sim

Στις επόμενες παραγράφους θα παρουσιαστούν οι τιμές των μεταβλητών εισόδου στον προσομοιωτή J-Sim. Οι μεταβλητές αυτές περιγράφουν τον τρόπο ανάπτυξης των κόμβων του δικτύου WSN που προσομοιώνεται καθώς και τα χαρακτηριστικά της δικτυακής κίνησης που παράγεται στον προσομοιωτή.

6.5.2.1. Παράμετροι Ανάπτυξης των Κόμβων

Η αρχική θέση 110 κόμβων αισθητήρων στο ομοιόμορφο πλέγμα απεικονίζεται στην Εικόνα 46. Στα πειράματα το μέγεθος του δικτύου παραμετροποιήθηκε από τους 110 στους160, 220 και 1000 κόμβους. Επειδή τα ασύρματα δίκτυα αισθητήρων είναι συνήθως ημι-στατικά δεν αφήσαμε τη μέση ταχύτητα των κόμβων που εξομοιώθηκε με το μοντέλο Random Waypoint Model να υπερβεί τα 10m/sec, η οποία είναι αρκούντως υψηλή ταχύτητα για τις εφαρμογές που εξετάζουμε.

Οι επιμέρους παράμετροι ανάπτυξης του δικτύου ad hoc στο επίπεδο και οι τιμές αυτών που χρησιμοποιήθηκαν κατά τα πειράματα προσομοίωσης με τον J-Sim παρουσιάζονται στον Πίνακα 5. Όπως φαίνεται στον Πίνακα 5 η αρχική ενέργεια των κόμβων είναι 1KJoule και σύμφωνα με το ενεργειακό μοντέλο που υιοθετήσαμε στον προσομοιωτή J-Sim η ενέργεια μειώνεται τόσο όταν ο κόμβος εκπέμπει όσο και όταν ο δέκτης λαμβάνει μηνύματα κατά τρόπο που εξαρτάται από το μέγεθος του πακέτου που μεταδίδεται και το διαθέσιμο εύρος ζώνης στο ασύρματο κανάλι.



Εικόνα 46. Αρχική τοποθέτηση 110 ad hoc κόμβων σε τοπολογία πλέγματος. Οι κόμβοι 82-87 είναι έξι γραμμικά τοποθετημένοι επιτιθέμενοι και οι κόμβοι 17, 24, 45, 52, 67 και 81 είναι έξι τυχαία επιλεγμένοι κακόβουλοι κόμβοι.

ΠΑΡΑΜΕΤΡΟΣ	ΕΥΡΟΣ ΤΙΜΩΝ
Αριθμός Κόμβων	(110 – 1000)
Επιφάνεια	(80x80 - 800x800)m^2
Τοποθέτηση	Ομοιόμορφο πλέγμα
Βήμα Πλέγματος	20 meters
Μοντέλο Κίνησης	Static & Random Waypoint Μέση ταχύτητα: 0 - 10m/sec
Ενέργεια	1KJoule

Πίνακας 5: Οι παράμετροι τοποθέτησης αισθητήρων και οι τιμές τους στον J-Sim.

Η κίνηση των κόμβων εξομοιώθηκε σύμφωνα με το μοντέλο Random Waypoint Model (RWP) που περιγράφεται στην §5.3.2. Η μέγιστη επιφάνεια όπου κινήθηκαν οι κόμβοι είναι 800 x 800 m^2.

Όσον αφορά τους κακόβουλους κόμβους αυτοί είναι τοποθετημένοι κατά δύο διαφορετικούς τρόπους στα πειράματά μας. Στην πρώτη περίπτωση διασπείραμε τους επιτιθέμενους σε εντελώς τυχαίες θέσεις εντός του πλέγματος (έξι τυχαία τοποθετημένοι κύκλοι/κόμβοι στην Εικόνα 46). Στη δεύτερη περίπτωση οι κακόβουλοι κόμβοι τοποθετήθηκαν κατά μήκος μιας ευθείας γραμμής και όπως απεικονίζεται στην Εικόνα 46 είναι οι κόμβοι 82 έως και 87. Με αυτόν τον τρόπο τα δύο βασικά σενάρια επίθεσης που προσομοιώθηκαν είναι:

- ***Σενάριο #1 τυχαίων επιθέσεων***. Σε αυτό το σενάριο οι κόμβοι παίρνουν τυχαίες θέσεις μέσα στο πλέγμα και αφού κερδίσουν την εκλογή του αρχηγού μεταδίδοντας ψευδείς πληροφορίες, απορρίπτουν τα πακέτα με τυχαίο τρόπο (με τη ρίψη νομίσματος) (επίθεση "grey hole"). Επίσης σε αυτό το σενάριο εξομοιώνουμε και την εγωιστική συμπεριφορά των κόμβων, κατά την οποία οι κόμβοι δεν προωθούν τα πακέτα που λαμβάνουν αν η διαθέσιμη ενέργειά τους είναι κάτω από μια καθορισμένη τιμή κατωφλίου.

- ***Σενάριο #2 στοχευμένων επιθέσεων.*** Σε αυτό το σενάριο οι κόμβοι παίρνουν θέσεις κατά μήκος ενός τείχους μέσα στο πλέγμα, όπως εξηγήθηκε αμέσως πιο πάνω, και αφού κερδίσουν την εκλογή του αρχηγού μεταδίδοντας ψευδείς πληροφορίες, απορρίπτουν είτε όλα τα πακέτα που λαμβάνουν (επίθεση "black hole") είτε απορρίπτουν τα πακέτα που προέρχονται από συγκεκριμένους κόμβους του δικτύου.

6.5.2.2. Παράμετροι Δικτυακής Κίνησης

ΠΑΡΑΜΕΤΡΟΣ	ΤΙΜΗ
Propagation model	Free space
Transmission power	0.2818 W (240m)
MAC	802.11 DCF
Network PDU	100 bytes
Mean packet rate	10 packets/sec
UDP CBR flow	2KBps/flow
BEACON period	4 seconds
BEACON_buffer size	64 packets
BEACON expiration in BEACON_buffer	1 minute
Neighbor expiration in NL	2 x Beacon period

Πίνακας 6: Ρύθμιση παραμέτρων δικτυακής κίνησης στον J-Sim.

Η επόμενη κατηγορία παραμέτρων εισόδου στον J-Sim σχετίζεται με τα χαρακτηριστικά μετάδοσης στο φυσικό επίπεδο, στο επίπεδο διασύνδεσης, στο επίπεδο του δικτύου και στο επίπεδα μεταφοράς και εφαρμογής, όπως παρουσιάζει ο Πίνακας 6.

Όπως φαίνεται στον Πίνακα 6, το φυσικό επίπεδο στον J-Sim ακολουθεί το μοντέλο διάδοσης στον ελεύθερο χώρο (νόμος των αντίστροφων τετραγώνων) και το επίπεδο διασύνδεσης υλοποιείται με το WiFi MAC 802.11 Distributed Coordination Function (DCF) σε ad hoc mode. Σημαντικός παράγοντας για την εκτίμηση της επίδοσης των πρωτοκόλλων είναι η ισχύς μετάδοσης των ασύρματων κόμβων. Η ισχύς εκπομπής εξαρτάται από την ακτίνα κάλυψης R η οποία καθορίζει τον αριθμό των γειτόνων που μπορεί να έχει ένας κόμβος σε απόσταση ενός βήματος. Ο αριθμός των γειτόνων είναι $O(d * R^2)$ όπου d είναι η πυκνότητα του δικτύου. Ωστόσο, στα πειράματα που διεξαγάγαμε με τον J-Sim θέσαμε την ακτίνα κάλυψης σταθερή, ίση με 240 μέτρα, δεδομένου ότι το αντίκτυπο που έχει η μεταβολή της ακτίνας κάλυψης (και ισοδύναμα της ισχύος εκπομπής των κόμβων) έχει διεξοδικά μελετηθεί στα πειράματα που διεξήγαμε τον προσομοιωτή JNS, δες και §5.5.3.

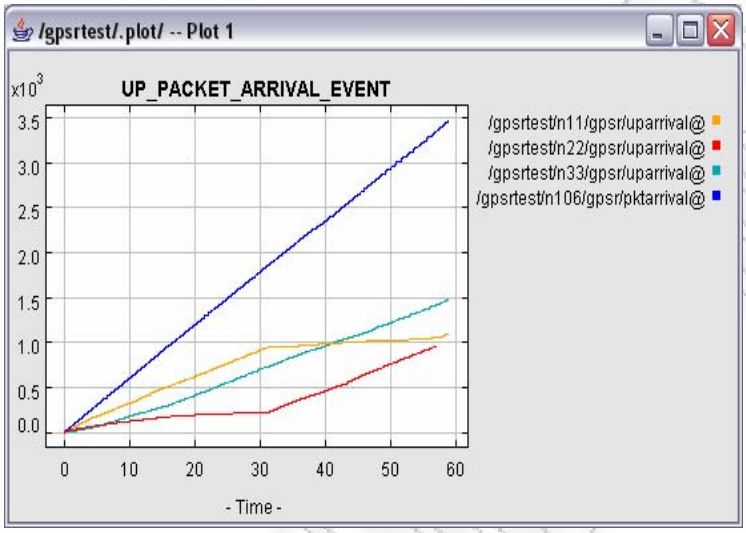
Έτσι η ισχύς σε όλα τα τρέχοντα πειράματα διατηρήθηκε σταθερή. Η τιμή που αντιστοιχεί στα 240 μέτρα σύμφωνα με το μοντέλο της ασύρματης κάρτας που εξομοιώνεται στον J-Sim είναι ίση με 0.2818 Watts.

Ακόμη, ο Πίνακας 6 παρουσιάζει τις παραμέτρους που σχετίζονται με τη μετάδοση ευρείας εκπομπής των πακέτων beacon. Αυτές οι παράμετροι είναι η περίοδος μετάδοσης των beacon, το

μέγεθος του προσωρινού ενταμιευτή των πακέτων beacon, ο χρόνος λήξης ενός πακέτου beacon στον ενταμιευτή και ο χρόνος λήξης ενός γείτονα στη λίστα με τους γείτονες Neighbor_List του κάθε κόμβου. Οι σχετικές τιμές που χρησιμοποιήθηκαν στα πειράματα δίνονται στον Πίνακα 6.

Στο επίπεδο της εφαρμογής εξομοιώσαμε ένα αυξανόμενο αριθμό από *Poisson* πηγές που μεταδίδουν με σταθερό ρυθμό UDP πακέτα σταθερού μήκους (ροή Constant Bit Rate, CBR) τα οποία ενθυλακώνονται σε πακέτα UDP (και επίσης TCP). Σε κάθε ροή δεδομένων ο μέσος ενδιάμεσος χρόνος που μεσολαβεί για τη μετάδοση δύο διαδοχικών πακέτων τέθηκε ίσος με 0.1 seconds, έτσι ώστε ο συνολικός ρυθμός μετάδοσης ανά ροή ήταν ίσος με 2KByte/sec.

Η Εικόνα 47 απεικονίζει τον αριθμό των TCP πακέτων που δημιουργούνται από κάθε μία πηγή κατά τη διάρκεια του πειράματος προσομοίωσης (συνολικά τρεις πηγές απεικονίζονται στην Εικόνα 47 που αντιστοιχούν στους κόμβους 11, 22 και 33) καθώς και το συνολικό αριθμό πακέτων SC-GPSR που ο Σταθμός Βάσης (κόμβος 106) λαμβάνει στην πόρτα που έχει οριστεί για το πρωτόκολλο SC-GPSR. Όπως φαίνεται στην Εικόνα 47, μετά από μία ώρα του χρόνου προσομοίωσης στον J-Sim οι τρεις πηγές παρέδωσαν στο Σταθμό Βάσης συνολικά 3.500 πακέτα.



Εικόνα 47. Προσομοίωση με τον J-Sim τριών ροών πακέτων TCP από τρεις διαφορετικές πηγές.

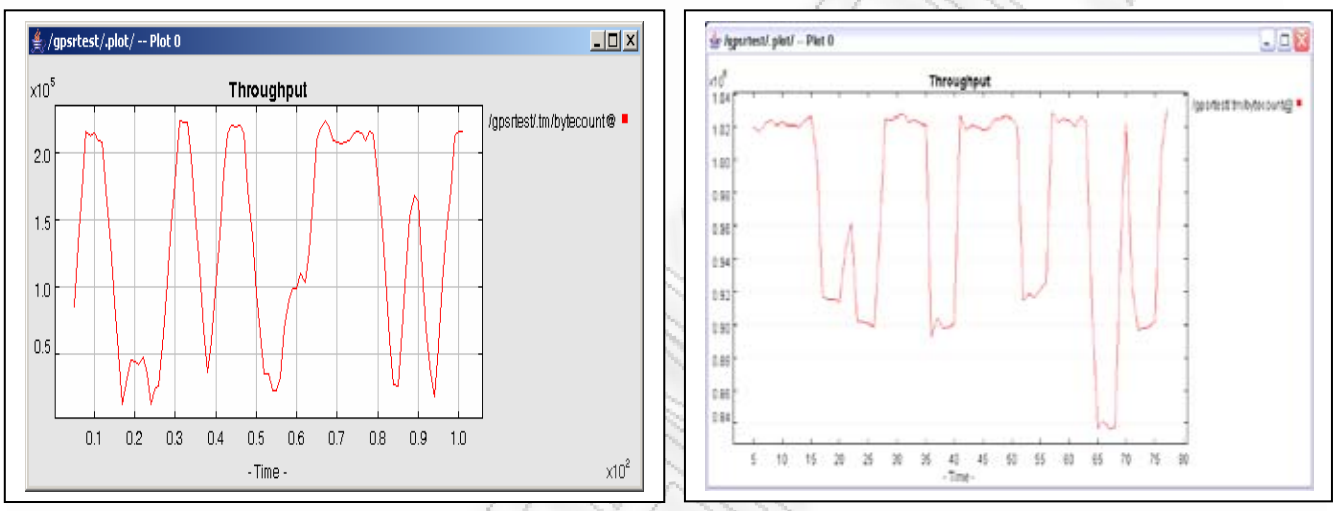
6.5.3. Αποτελέσματα Προσομοίωσης για τη Δικτυακή Απόδοση

Τα αποτελέσματα προσομοίωσης που θα παρουσιάσουμε σε αυτήν την παράγραφο αφορούν μέτρα της δικτυακής απόδοσης όπως είναι η μέση καθυστέρηση ανά πακέτο, η ρυθμοαπόδοση ("throughput") του δικτύου και η απώλεια πακέτων. Συγκρίνουμε την επίδοση για τρία πρωτόκολλα το AODV, το GPSR και το SC-GPSR. Αρχικά συγκρίνουμε και αναλύουμε την απόδοση των πρωτοκόλλων όταν το δίκτυο λειτουργεί χωρίς την παρουσία κακόβουλων κόμβων και έπειτα όταν διαφορετικού τύπου επιτιθέμενοι απειλούν ενεργητικά το δίκτυο. Για όλα τα πρωτόκολλα η αρχική τοποθέτηση των κόμβων ήταν το πλέγμα της Εικόνας 46.

6.5.3.1. Σύγκριση Αποτελεσμάτων Δικτυακής Απόδοσης χωρίς Επιθέσεις

Η ρυθμοαπόδοση του GPSR και του SC-GPSR στην περίπτωση που το αρχικό ομοιόμορφο πλέγμα με συνολικά 110 κόμβους διατηρείται στατικό απεικονίζεται στην Εικόνα 48(α) και 48(β) αντίστοιχα. Το μέγεθος του κάθε πακέτου στα πειράματα με το GPSR και το SC-GPSR ήταν 100 bytes. Τα αποτελέσματα αφορούν δύο ζεύγη κόμβων πηγής και τελικού προορισμού.

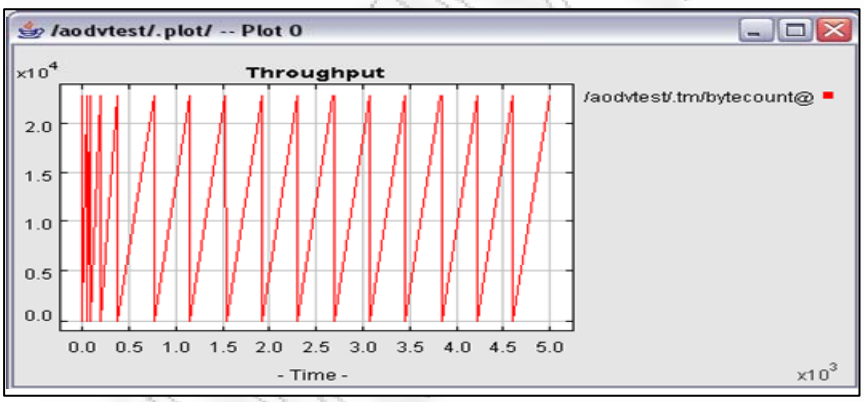
Η μέγιστη τιμή της ρυθμοαπόδοσης που επιτεύχθηκε από το GPSR ήταν κατά προσέγγιση 200 KBytes/second και η ελάχιστη τιμή ήταν 50KBytes/sec, όπως φαίνεται στην Εικόνα 48(α). Από την άλλη μεριά η μέγιστη τιμή της ρυθμοαπόδοσης που επιτεύχθηκε από το SC-GPSR με 110 στατικούς κόμβους ήταν κατά προσέγγιση 1MByte/second και η ελάχιστη τιμή ήταν κοντά στην τιμή των 840KBytes/sec, όπως φαίνεται στην Εικόνα 48(β). Αυτό αποτελεί μια αύξηση στη μέγιστη ρυθμοαπόδοση του GPSR κατά 4 φορές ενώ η ελάχιστη εφικτή ρυθμοαπόδοση του GPSR αυξήθηκε κατά 16 φορές στο προτεινόμενο σχήμα SC-GPSR. Το SC-GPSR πέτυχε αυτήν την απόδοση με όλα τα τμήματα που έχουμε περιγράψει σε λειτουργία, δηλαδή τα συνεργατικά τμήματα ψηφοφορίας, παρακολούθησης και ανίχνευσης και το κρυπτογραφικό τείχος προστασίας με τον αλγόριθμο HMAC που αυθεντικοποιεί τα μηνύματα που λαμβάνονται από τους κόμβους.



(α)
GPSR

(β)
SC-GPSR

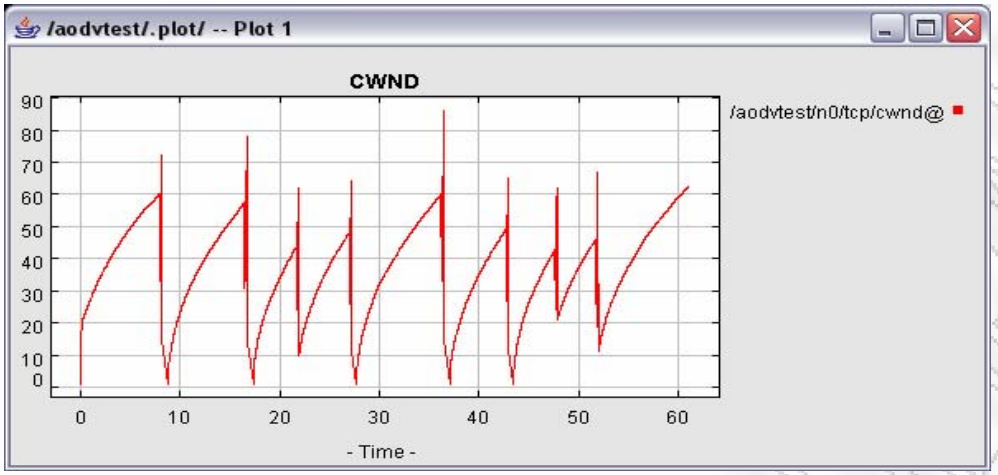
Εικόνα 48. GPSR vs. SC-GPSR, 110 κόμβοι, στατικό δίκτυο.



Εικόνα 49. Ρυθμοαπόδοση του AODV, 220 στατικοί κόμβοι, προσφερόμενη κίνηση 2KBps.

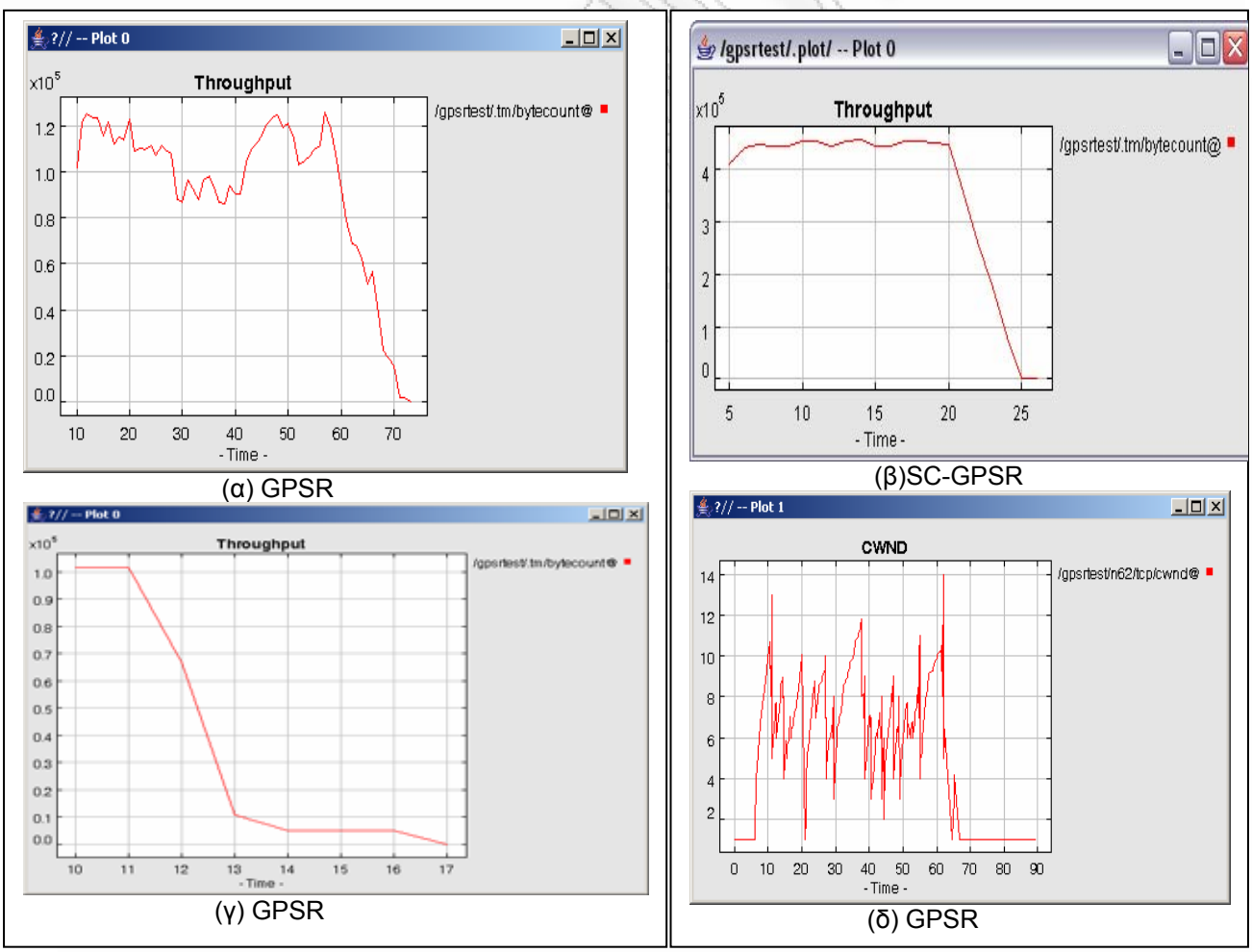
Ακόμη διεξήγαμε πειράματα για την εκτίμηση της δικτυακής απόδοσης του AODV κάτω από τις ίδιες συνθήκες (110 και 220 στατικοί κόμβοι και παραγωγή κίνησης TCP) που είχαμε στα πειράματα προσομοίωσης με τα πρωτόκολλα GPSR και SC-GPSR.

Η Εικόνα 49 απεικονίζει τη ρυθμοαπόδοση του AODV, μέγιστης τιμής 20 KBytes/sec. Η τιμή αυτή είναι μια τάξη μεγέθους μικρότερη από την επίδοση του GPSR και δύο τάξεις μεγέθους μικρότερη από τη ρυθμοαπόδοση του SC-GPSR.



Εικόνα 50. Το παράθυρο ελέγχου συμφόρησης στο TCP με ad hoc πρωτόκολλο το AODV.

Στην Εικόνα 50 απεικονίζεται η μεταβολή του παραθύρου συγκρούσεων στο πρωτόκολλο TCP ("collision window") κατά τη διάρκεια πειράματος προσομοίωσης με το πρωτόκολλο AODV.



(α) GPSR

(β)SC-GPSR

(γ) GPSR

(δ) GPSR

Εικόνα 51. Η επίδραση της κίνησης στην επίδοση των γεωγραφικών πρωτοκόλλων. (α) και (β): GPSR vs. SC-GPSR, 220 κόμβοι με ταχύτητα κόμβων 10m/sec. (γ), (δ): GPSR με ταχύτητα κόμβων 20m/sec.

Επιπλέον, πειραματιστήκαμε με περισσότερους κόμβους και με μεγαλύτερη κινητικότητα για να διαπιστώσουμε αν τα ad hoc πρωτόκολλα κλιμακώνονται ικανοποιητικά κάτω από συνθήκες κίνησης ενός αυξημένου αριθμού κόμβων-χρηστών. Στην περίπτωση που ο αριθμός των κόμβων είναι 220 και οι οποίοι κινούνται με μέση ταχύτητα των 10m/sec σύμφωνα με το μοντέλο Random Waypoint Model (RWP) πήραμε τα αποτελέσματα που απεικονίζονται στις Εικόνες 51(α) και 51(β) για την απόδοση του GPSR και του SC-GPSR αντίστοιχα. Τα δύο σχήματα απεικονίζουν έντονα το γεγονός ότι καθώς ο χρόνος του πειράματος εξαντλείται η απόδοση και για τα δύο πρωτόκολλα φθίνει, μάλιστα ο ρυθμός εξυπηρέτησης των πακέτων στο δίκτυο φθάνει μέχρι το μηδενικό σημείο.

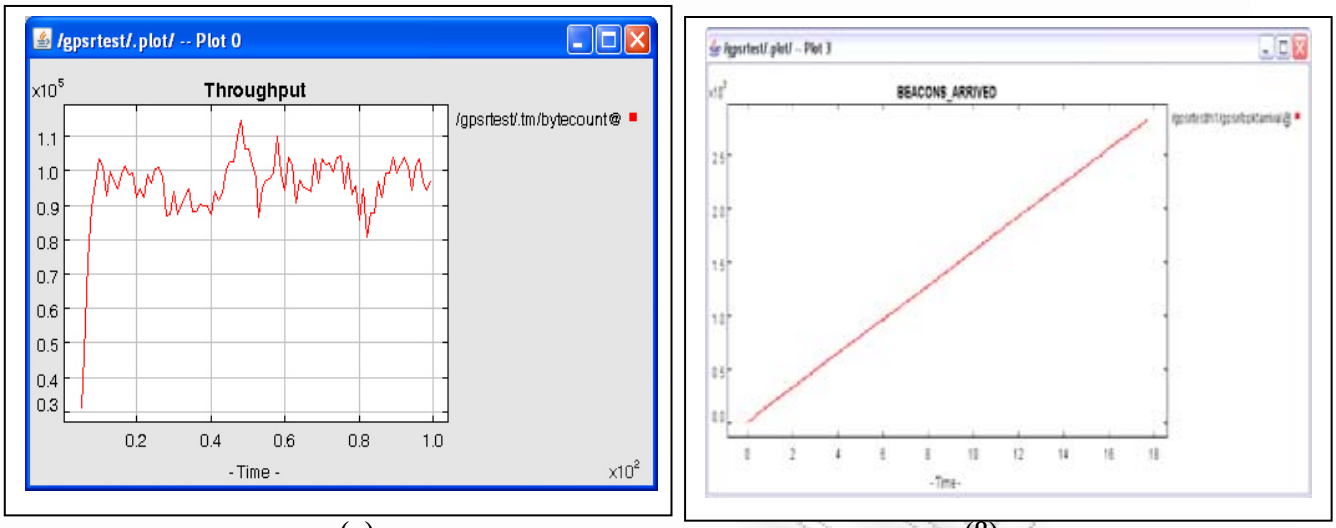
Τα Σχήματα 51(α) και 51(β) δείχνουν ότι η κίνηση των κόμβων διαδοχικά με το χρόνο προκαλεί σημαντική μείωση της ρυθμοαπόδοσης που επιτυγχάνεται με τα πρωτόκολλα GPSR και SC-GPSR. Ένας από τους βασικούς λόγους βρίσκεται στους κανόνες γεωγραφικής προώθησης των πακέτων οι οποίοι είναι οι ίδιοι και στα δύο πρωτόκολλα.

Σύμφωνα με το GPSR η προώθηση των πακέτων βασίζεται στη θέση των κόμβων. Ωστόσο η κίνηση προκαλεί σημαντικές αλλαγές στη δικτυακή τοπολογία και συνεπώς είναι πολύ πιθανό το πρωτόκολλο GPSR να βρεθεί σε ένα σημείο *void*, δηλαδή μπορεί ο τρέχων κόμβος-δρομολογητής να οδηγηθεί σε ένα σημείο μέσα στο δίκτυο όπου δεν μπορεί να βρεί κάποιο γειτονικό του κόμβο που να είναι πλησιέστερα στον τελικό προορισμό του πακέτου. Στην περίπτωση αυτή το GPSR (και το SC-GPSR) εγκαταλείπει τον *greedy* τρόπο δρομολόγησης και μπαίνει σε *perimeter mode*, όπου αναζητείται κάποιοι περιμετρικό μονοπάτι δρομολόγησης προς τον προορισμό. Ωστόσο, κατά το *perimeter mode* τα πακέτα ελέγχου για το πρωτόκολλο GPSR (και SC-GPSR) είναι περισσότερα από τα ωφέλιμα πακέτα δεδομένων και επιπλέον το μήκος του μονοπατιού που ακολουθούν τα δεδομένα αυξάνεται σε σχέση με τη *greedy* δρομολόγηση. Το γεγονός αυτό έχει σημαντική επίδραση στη ρυθμοαπόδοση του δικτύου την οποία ο τελικός χρήστης αντιλαμβάνεται αισθητά μειωμένη. Οι Εικόνες 51(γ) και 51(δ) απεικονίζουν την αισθητή μείωση στη διαπερατότητα του δικτύου GPSR και στην απόδοση των εφαρμογών όταν αυξήσαμε περαιτέρω τη μέση ταχύτητα κίνησης των κόμβων στα 20m/sec.

Επιπλέον, σε αυτή τη σειρά πειραμάτων δίχως επιθέσεις, προκειμένου να πιστοποιήσουμε περαιτέρω ότι η διαδοχική μείωση της δικτυακής απόδοσης των δύο πρωτοκόλλων οφείλεται περισσότερο στην κίνηση παρά στο μέγεθος του δικτύου πειραματιστήκαμε με ένα πολύ μεγάλο αριθμό κόμβων (πάνω από 1000 κόμβοι) τους οποίους υποθέσαμε στατικούς στο πλέγμα. Η Εικόνα 52(α) και η Εικόνα 52(β) απεικονίζει την ικανοποιητική μέση δικτυακή ρυθμοαπόδοση που επιτεύχθηκε από το GPSR στην περίπτωση των 1000 στατικών κόμβων.

Παρατηρούμε ότι με την υπόθεση στατικών κόμβων το πρωτόκολλο GPSR κλιμακώνεται πολύ καλά, δηλαδή η ρυθμοαπόδοσή του εμφανίζεται σταθερή καθόλη τη διάρκεια του πειράματος (100 λεπτά) κοντα στο σημείο των 100KB/sec, μια αρκετά καλή διαπερατότητα δεδομένου του μεγάλου μεγέθους του δικτύου στο συγκεκριμένο πείραμα.

Αυτό, σε σχέση και με τα προηγούμενα πειράματα της Εικόνας 51, επιβεβαιώνει ότι η κινητικότητα των GPSR κόμβων επιφέρει μεγαλύτερη επιβάρυνση στις επικοινωνίες από ότι επιφέρει η κλιμάκωση του αριθμού των GPSR κόμβων. Ωστόσο, η Εικόνα 52(β) παρουσιάζει και το γεγονός της αυξήσεως του αριθμού των πακέτων beacon που μεταδίδονται με ανοιχτή εκπομπή από το GPSR και τα οποία είναι εύλογο να αυξάνονται καθώς η κλίμακα του δικτύου αυξάνεται. Αυτό έχει σαν συνέπεια οι συγκρούσεις που συμβαίνουν κατά τη μετάδοση των πακέτων να είναι περισσότερες, γεγονός που μπορεί να επιδράσει στην επίδοση του δικτύου και των ad hoc εφαρμογών.

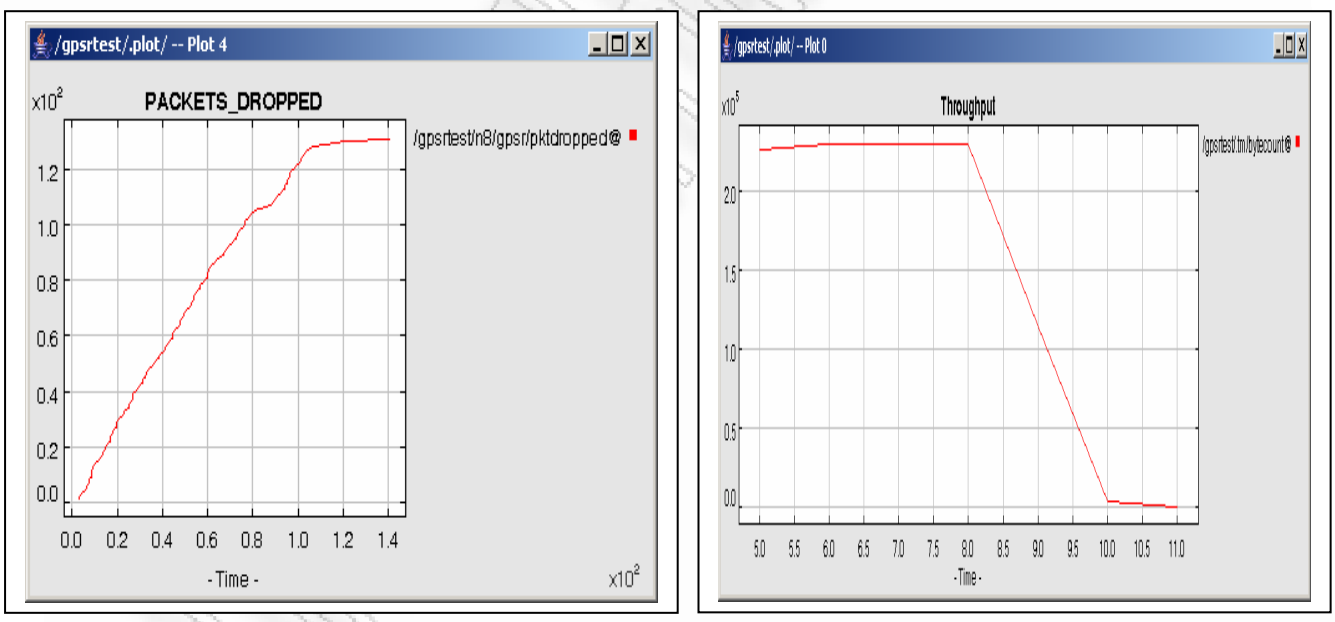


(α) (β)

Εικόνα 52. (α): GPSR ρυθμοαπόδοση με 1000 στατικούς κόμβους. (β): ο αριθμός των περιοδικά λαμβανομένων πακέτων beacon.

6.5.3.2. Σύγκριση Αποτελεσμάτων Δικτυακής Απόδοσης με Επιθέσεις

Το πρωτόκολλο GPSR είναι ανυπεράσπιστο σε κάθε είδους επίθεση που μπορεί να εκδηλωθεί κατά των κόμβων και της λειτουργίας του δικτύου.



(α) Απώλεια πακέτων. (β) Ρυθμοαπόδοση.

Εικόνα 53. Η αδυναμία του GPSR έναντι μοναδικού κόμβου γκρι τρύπας, 6 συνολικά στατικοί κόμβοι.

Ιδιαίτερα τρωτό είναι στις επιθέσεις που απειλούν την ιδιωτικότητα των κόμβων εφόσον σύμφωνα με το πρωτόκολλο GPSR ο κάθε ad hoc κόμβος που λειτουργεί σαν ενδιάμεσος δρομολογητής πρέπει να μεταδίδει τη θέση και την ταυτότητά του και άρα ένας κακόβουλος κόμβος που κρυφακούει μπορεί εύκολα να συλλάβει την ευαίσθητη αυτή πληροφορία.

Επίσης, τονίζεται ότι το GPSR απειλείται σημαντικά από τις επιθέσεις άρνησης προώθησης των

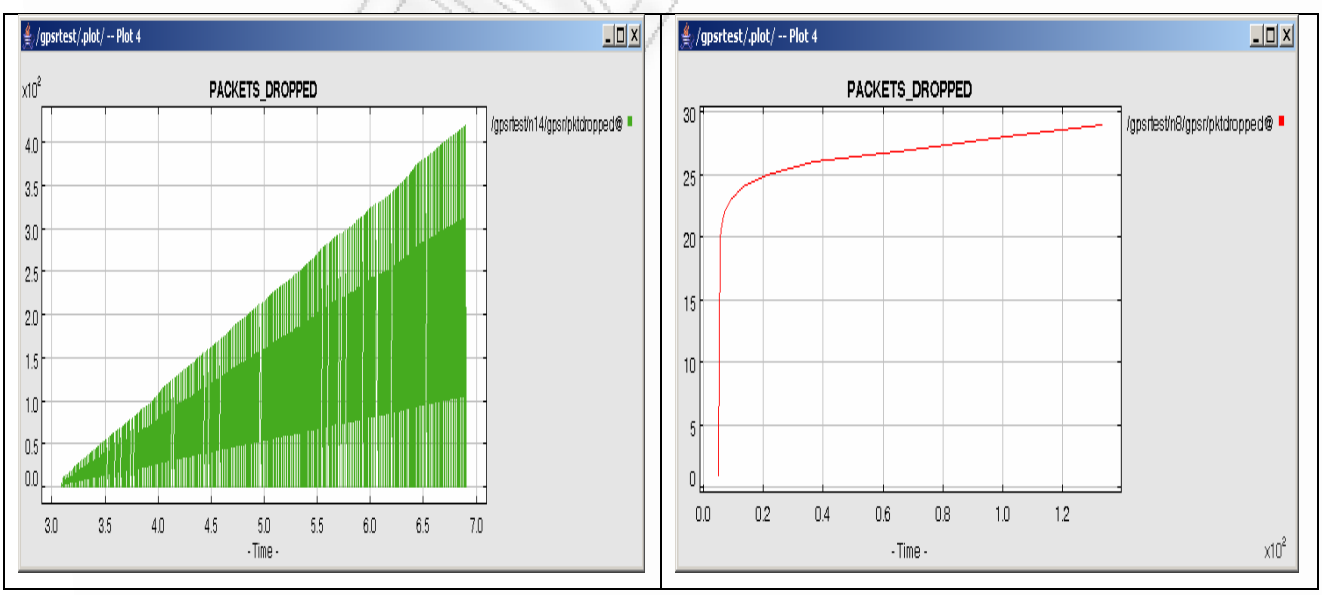
μηνυμάτων, δηλαδή από τους εισβολείς οι οποίοι δρουν σαν μαύρες τρύπες και απορρίπτουν ότι πακέτο λάβουν, ή σαν γκρι τρύπες που πότε απορρίπτουν και πότε προωθούν τα πακέτα ή δρούν εγωιστικά δίχως να προωθούν τα πακέτα για υποκειμενικούς λόγους όπως έχουμε αναλύσει προηγουμένως.

Η αδυναμία του GPSR να αντιμετωπίσει τέτοιου είδους επιθέσεις απεικονίζεται στις Εικόνες 53 και 54. Στην Εικόνα 53 το σενάριο επίθεσης είναι πολύ απλό. Σε μια γραμμική τοπολογία από 6 κόμβους ένας μόνο κόμβος παρεμβάλλεται μεταξύ μιας πηγής και ενός προορισμού και δρα σαν γκρι τρύπα, δηλαδή απορρίπτει τα πακέτα μετά από τη ρίψη νομίσματος. Ακόμη και για μια τόσο απλή επίθεση ο αντίκτυπος για το GPSR είναι ολέθριος εφόσον το GPSR δεν μπορεί να ανιχνεύσει τη γκρι τρύπα, όπως και καμία άλλη απειλή, και τελικά όπως βλέπουμε στην Εικόνα 53(β) μετά από 80 λεπτά το δίκτυο καθίσταται ανήμπορο να διεκπαιρεώσει την κίνηση από τους αισθητήρες προς το Σταθμό Βάσης. Το ίδιο πείραμα επαναλήφθηκε με μία επίθεση από κόμβο μαύρη τρύπα Εικόνα 54(α) και από κόμβο εγωιστή που παρεμβλήθηκε στη ροή TCP από την πηγή προς τον προορισμό Εικόνα 54(β).

Στις Εικόνες 54(α) και 54(β) απεικονίζεται ότι η απώλεια πακέτων είναι περισσότερο ολέθρια στην επίθεση μαύρης τρύπας εφόσον τότε απορρίφθησαν όλα τα πακέτα που έλαβε ο κακόβουλος κόμβος. Απώλεια πακέτων όμως είχαμε και με τον εγωιστή κόμβο ο οποίος αρνείται την περαιτέρω προώθηση πακέτων αν νομίζει ότι δεν έχει επαρκή διαθέσιμη ενέργεια.

Από την άλλη μεριά, στα πειράματα με το εκτεταμένο σχήμα SC-GPSR και για τα δύο σενάρια επίθεσης, ονομαστικά το επιλεκτικό #1 και το στοχευμένο σενάριο #2 (δες §6.5.1 για τον ορισμό τους) καμία απώλεια πακέτου δεν αναφέρθηκε. Το συνεργατικό τείχος του SC-GPSR κατάφερε να ανιχνεύσει έγκαιρα τους ύποπτους κόμβους και να τους απομονώσει με το να διαδώσει το κατάλληλο μήνυμα “BLACKLIST” σε όλο το δίκτυο έτσι ώστε οι όλοι οι υπόλοιποι κόμβοι να τους διαγράψουν.

Με αυτό τον τρόπο αποφεύγονται οι απώλειες πακέτων που οφείλονται σε κακόβουλους κόμβους που δρουν ως μαύρες τρύπες (δηλαδή αρνούνται τη προώθηση κάθε πακέτου που λαμβάνουν) σε πλήρη αντιπαράθεση με τη συμπεριφορά του GPSR που απέτυχε να αποφύγει ένα και μόνο κακόβουλο κόμβο.



(α) Επίθεση μαύρης τρύπας. **(β)** Επίθεση εγωιστικού κόμβου.

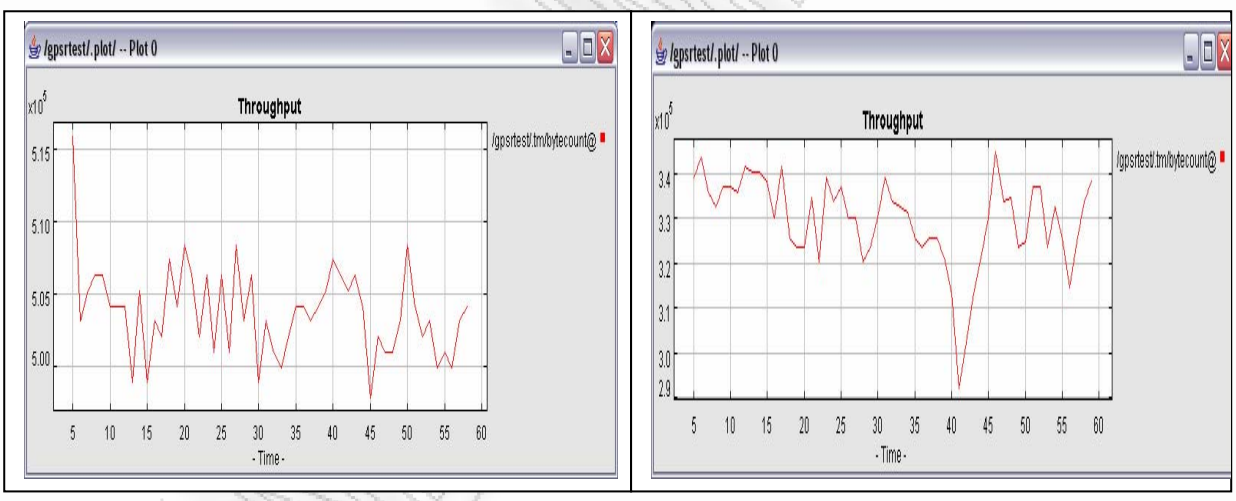
Εικόνα 54. Η απώλεια πακέτων του GPSRστην επίθεση μιας μαύρης τρύπας και ενός εγωιστικού κόμβου.

Η Εικόνα 55(α) παρουσιάζει τη δικτυακή απόδοση όταν πρωτόκολλο του δικτύου είναι το εκτεταμένο σχήμα SC-GPSR στην περίπτωση που οι επιτιθέμενοι απειλούν το δίκτυο σύμφωνα με το σενάριο τυχαίων επιθέσεων #1. Τοποθετήσαμε έξι συνολικά εγωιστικούς κόμβους σε τυχαίες θέσεις μέσα στο πλέγμα και αυτοί απείλησαν τους υπόλοιπους 104 κόμβους με απορρίψεις των πακέτων που λαμβάνουν. Η προσφερόμενη κίνηση από τους νόμιμους κόμβους σε αυτό το σενάριο ήταν 2KBytes/sec.

Η Εικόνα 55(α) δείχνει ότι υπό αυτές τις συνθήκες η διαπερατότητα του δικτύου με το SC-GPSR ήταν πολύ καλή και διατηρούμενη στα 500KBytes/sec. Ένα αρχικό μέγιστο που παρατηρείται στην απόδοση οφείλεται στο γεγονός ότι οι συγκρούσεις μεταξύ των κόμβων είναι λιγότερες από τις μεταδόσεις δεδομένων τουλάχιστον στην αρχική περίοδο λειτουργίας του δικτύου. Υπενθυμίζουμε ότι η ρυθμοαπόδοση του SC-GPSR στην περίπτωση των 110 κόμβων δίχως καθόλου επιθέσεις ήταν στο προηγούμενο Σχήμα 48(β) μεταξύ των τιμών 840KBytes/sec και 1000KBytes/sec.

Επιπλέον, η επίδοση του SC-GPSR υπό τις επιθέσεις του τυχαίου σεναρίου που απεικονίζεται στην Εικόνα 55(α) είναι καλύτερη από την απόδοση του GPSR δίχως επίθεση η οποία παρουσιάστηκε στο προηγούμενο Σχήμα 48(α) όπου ο μέγιστος ρυθμός που επιτεύχθηκε ήταν μεταξύ των τιμών 50KBytes/sec (ελάχιστο) και 200KBytes/sec (μέγιστο).

Συνεπώς η προσεκτική σχεδίαση, παραμετροποίηση και υλοποίηση των προτεινόμενων αλγορίθμων επέφερε καλύτερη απόδοση ακόμη και όταν το δίκτυο απειλήθηκε και μπήκαν σε λειτουργία οι διαδικασίες προστασίας από τις επιθέσεις που προβλέπει το εκτεταμένο σχήμα SC-GPSR.



(α) SC-GPSR, προσφερόμενη κίνηση 2KBps. **(β)** SC-GPSR, προσφερόμενη κίνηση 6KBps.

Εικόνα 55. Η επίδοση του SC-GPSR κάτω από το σενάριο τυχαίων επιθέσεων, 110 στατικοί κόμβοι.

Η Εικόνα 55(β) απεικονίζει την απόδοση που επιτεύχθηκε με το σχήμα SC-GPSR όταν το προσφερόμενο φορτίο ήταν τρεις φορές μεγαλύτερο από αυτό της Εικόνας 55(α). Παρατηρούμε ότι ο ρυθμός εξυπηρέτησης της τριπλάσιας προσφερόμενης κίνησης που απεικονίζεται στο 55(β) είναι της ίδιας τάξης μεγέθους με το ρυθμό που απεικονίζεται στην Εικόνα 55(α), δηλαδή το δίκτυο SC-GPSR δεν υπερφορτώθηκε.

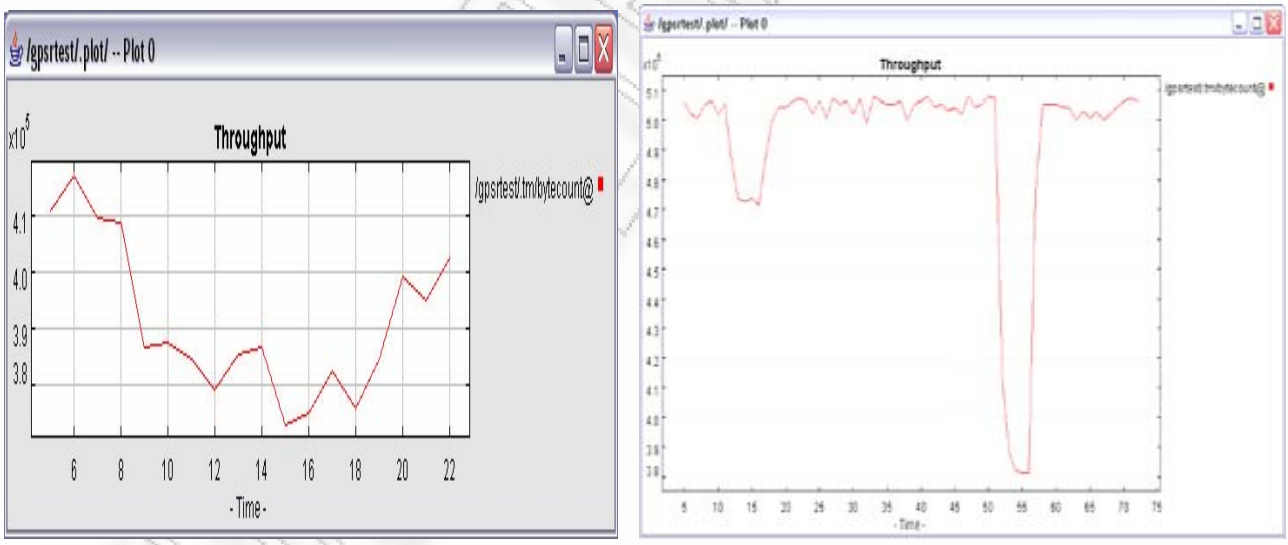
Στη συνέχεια αυξήσαμε τον αριθμό των κόμβων από 110 σε 220 κόμβους. Η επίδραση του διπλασιασμού του μεγέθους του στατικού δικτύου στην απόδοση του SC-GPSR όταν απειλείται από το ίδιο σενάριο #1 τυχαίων επιθέσεων από εγωιστικούς κόμβους φαίνεται στο Σχ. 56(α). Παρατηρούμε στο Σχ. 56(α) ότι για ροές συνολικού ρυθμού 4KB/sec η ρυθμοαπόδοση του SC-GPSR με 220 κόμβους δεν έπεσε κάτω από την τιμή ελαχίστου των 370 KBytes/sec και επομένως

η επίδοση διατηρήθηκε στην ίδια τάξη μεγέθους με αυτήν που απεικονίζεται στις Εικόνες 55(α) και 55(β).

Στη συνέχεια προσθέσαμε στα πειράματα κίνηση 10m/s στους κόμβους και μεταβάλαμε τη συμπεριφορά των κόμβων από εγωιστική σε συμπεριφορά κόμβων που εντελώς τυχαία απορρίπτουν πακέτα, δηλαδή οι επιτιθέμενοι δρουν τώρα ως κακόβουλοι γκρι κόμβοι. Το αποτέλεσμα παρουσιάζεται στην Εικόνα 56(β) όπου παρατηρούμε βυθίσματα στην απόδοση του δικτύου και τα οποία δικαιολογούνται από τους παρακάτω λόγους.

Ένας πρώτος λόγος είναι η κίνηση των κόμβων η οποία προκαλεί αλλαγές στην τοπολογία του δικτύου και άρα ένα μεγαλύτερο αριθμό από αλλαγές στους κόμβους-αρχηγούς που εκλέγονται από τον αλγόριθμο RRA. Πραγματικά η είσοδος νέων κόμβων στα υπάρχοντα clusters ή η μετακίνηση κάποιων άλλων εκτός του cluster στο οποίο ανήκουν αλλάζει τα δεδομένα ομαδοποίησης, όπως για παράδειγμα τους γείτονες που περιλαμβάνονται στις λίστες των γειτόνων *Neighbor_List*. Αυτό έχει ως πολύ πιθανό αποτέλεσμα οι τρέχοντες αρχηγοί να πρέπει να ξεκινήσουν νέες εκλογές.

Περαιτέρω, όπως έχουμε ήδη εξηγήσει, η διαδικασία επανεκλογής αρχηγών (reclustering) και κυρίως η διαδικασία της ενημέρωσης των κόμβων του δικτύου με τη πληροφορία για τη νέα δομή στο δίκτυο επιφέρει επιβάρυνση στις επικοινωνίες και επιπλέον χρειάζεται κάποιος χρόνος μέχρι το δίκτυο να ενημερωθεί για τις αλλαγές αυτές. Στη διάρκεια αυτού του διαστήματος και πριν το δίκτυο σταθεροποιηθεί ένας σημαντικός αριθμός από τα πακέτα δεδομένων των χρηστών είναι δυνατόν να χαθεί το γεγονός το οποίο απεικονίζεται ως απότομη μείωση στη ρυθμοαπόδοση του δικτύου. Συνεπώς, όσο πιο έντονη είναι η κινητικότητα των κόμβων, κατά μέσο όρο αλλά και σε συγκεκριμένες χρονικές στιγμές, τόσο πιο έντονη θα εμφανίζεται και η μείωση στην απόδοση του δικτύου λόγω της αυξήσεως του αριθμού των εκλογών τοπικών αρχηγών.



(α) 220 στατικοί SC-GPSR κόμβοι. **(β)** 110 SC-GPSR κινούμενοι κόμβοι, 10m/sec.

Εικόνα 56. Η επίδοση του SC-GPSR κάτω από σενάριο τυχαίων επιθέσεων σε συνθήκες κίνησης.

Επιπλέον, τα απότομα βυθίσματα της Εικόνας 56(β) οφείλονται στο γεγονός ότι με την κίνηση των κόμβων το SC-GPSR είναι πολύ πιο πιθανό να μεταβεί από τη δρομολόγηση *greedy mode* σε *perimeter mode* και αντίστροφα. Όπως έχουμε ήδη εξηγήσει, στο *perimeter mode* τα μηνύματα ελέγχου που απαιτούνται από το SC-GPSR είναι πολυάριθμα και το μονοπάτι προς το Σταθμό Βάσης είναι μεγαλύτερο συνεπώς είναι δυνατόν να προκληθεί μεγάλη επιβάρυνση στις ad hoc επικοινωνίες.

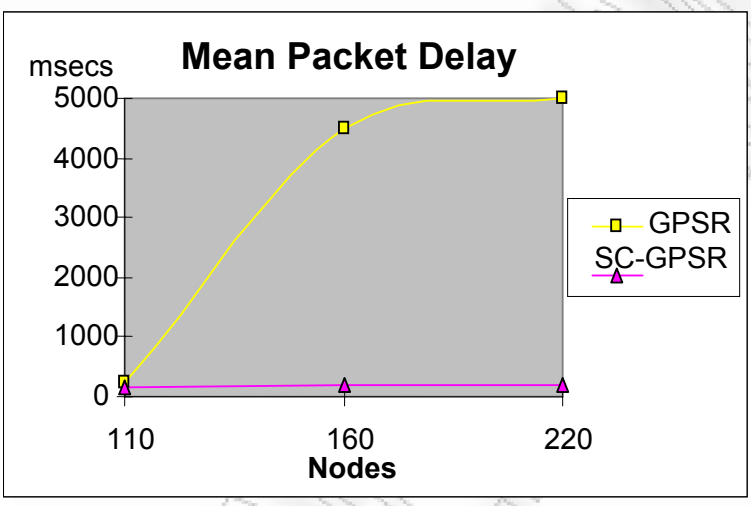
Ωστόσο, οι δύο Εικόνες 56(α) και 56(β) δείχνουν ότι η απόδοση του σχήματος SC-GPSR διατηρείται

σε πολύ καλά επίπεδα ακόμη και στις συνθήκες όπου το δίκτυο είναι διπλάσιο σε μέγεθος και ακόμη όταν οι κόμβοι κινούνται. Τόσο η Εικόνα 56(α) όσο και η Εικόνα 56(β) απεικονίζουν το γεγονός ότι το εκτεταμένο σχήμα SC-GPSR μπορεί να διατηρήσει την απόδοσή του στο πολύ καλό εύρος τιμών μεταξύ 370 KB/sec - 420 KB/sec, 56(α), και μεταξύ 150 KB/sec - 350 KB/sec, 56(β), ακόμη και όταν ένας αριθμός από τυχαία διεσπαρμένους κακόβουλους κόμβους παρεμβάλλεται στο μονοπάτι της επικοινωνίας των αισθητήρων με το Σταθμό Βάσης. Στις ίδιες συνθήκες το GPSR θα είχε καταστήσει το δίκτυο μη διαθέσιμο.

6.5.3.3. Σύγκριση Αποτελεσμάτων Μέσης Καθυστέρησης Πακέτου

Στη συνέχεια, παρουσιάζουμε συγκεντρωμένα τα αποτελέσματα που αφορούν τη μέση καθυστέρηση ανά πακέτο (“mean packet delay, MPD”) του σχήματος SC-GPSR έναντι του πρωτοκόλλου GPSR. Και για αυτή την παράμετρο της δικτυακής επίδοσης πειραματιστήκαμε με διαδοχικές μεταβολές στην προσφερόμενη κίνηση. Επίσης αυξήσαμε διαδοχικά το μέγεθος του δικτύου όπως και την κινητικότητα των κόμβων για να συγκρίνουμε και να μελετήσουμε πώς επιδρούν αυτοί οι παράγοντες στην επίδοση των δύο δικτυακών πρωτοκόλλων.

Τοποθετήσαμε έξι κακόβουλους κόμβους σύμφωνα με το στοχευμένο σενάριο επίθεσης #2 όπου οι επιτιθέμενοι σχηματίζουν ένα τείχος το οποίο παρεμβάλλεται στο μονοπάτι της επικοινωνίας των αισθητήρων με το Σταθμό Βάσης. Τα διαφορετικά δικτυακά προφίλ που περιγράφουν τις συνθήκες του δικτύου που προσομοιώσαμε είναι τα ακόλουθα.



Εικόνα 57. Σύγκριση της μέσης καθυστέρησης του SC-GPSR έναντι του GPSR για τρία διαφορετικά προφίλ των δικτυακών συνθηκών.

- *Το **πρώτο προφίλ** δικτύου* αποτελείται από 110 κόμβους, το προσφερόμενο φορτίο είναι ίσο με 2KBytes/sec και η τοπολογία είναι στατική ενώ το δίκτυο δεν απειλείται από κακόβουλους κόμβους.
- *Το **δεύτερο προφίλ** δικτύου* αποτελείται από 160 κόμβους, το προσφερόμενο φορτίο είναι ίσο με 4KBytes/sec και η τοπολογία είναι δυναμική με μέση ταχύτητα των κόμβων ίση με 3m/sec, ενώ παράλληλα έξι κόμβοι δρουν σαν μαύρες τρύπες μέσα στο δίκτυο.
- *Το **τρίτο προφίλ** δικτύου* αποτελείται από 220 κόμβους, το προσφερόμενο φορτίο είναι ίσο με 8KBytes/sec και η τοπολογία είναι δυναμική με μέση ταχύτητα των κόμβων ίση με 3m/sec, ενώ και πάλι έξι κόμβοι δρουν σαν μαύρες τρύπες μέσα στο δίκτυο.

Για την περίπτωση του πρώτου δικτυακού προφίλ μετρήσαμε ότι το SC-GPSR πέτυχε μέση καθυστέρηση κοντά στα 160 msec ενώ στην περίπτωση που το δίκτυο αποτελείται από 220

κινούμενους κόμβους (σύμφωνα με το τρίτο δικτυακό προφίλ) η καθυστέρηση ήταν όχι μεγαλύτερη από 300 msec. Από την άλλη μεριά, το GPSR στην περίπτωση του στατικού δικτύου και χωρίς επιθέσεις να το απειλούν πέτυχε μια σχετικά καλή απόδοση μέσης καθυστέρησης των 250 milliseconds, ωστόσο όταν το μέγεθος του δικτύου και των επιθέσεων μαύρης τρύπας κλιμακώθηκε η καθυστέρηση με κινητούς νόμιμους κόμβους αυξήθηκε αισθητά στα 5 seconds, όπως απεικονίζεται στην Εικόνα 57.

6.5.4. Αποτελέσματα Προσομοίωσης για την Ανίχνευση και την Αντιμετώπιση Επιθέσεων

Οι Εικόνες 58 και 59 απεικονίζουν την ικανότητα του εκτεταμένου σχήματος SC-GPSR να ανιχνεύει τους εισβολείς με βάση τον έλεγχο της ακεραιότητας και της συνέπειας των πληροφοριών που μεταδίδουν οι κόμβοι.

Υποθέτουμε ότι οι απειλές ακολουθούν τα σενάρια επίθεσης #1 (τυχαίο) και #2 (στοχευμένο) που ορίσαμε προηγουμένως και υλοποιούμε τα σενάρια αυτά μέσα στο ad hoc δίκτυο. Τα τείχη προστασίας του SC-GPSR κάνουν δυνατή την έγκαιρη ανίχνευση των εισβολέων έτσι ώστε το πρωτόκολλο κατά την προώθηση των πακέτων να μπορέσει να παρακάμψει τους κόμβους αυτούς και να παραδώσει τα πακέτα στον τελικό προορισμό. Ως αποτέλεσμα, με το SC-GPSR κανένα πακέτο δεδομένων δεν χάθηκε λόγω απόρριψης από τους κόμβους που απειλούν με επιθέσεις άρνησης προώθησης.

Ειδικότερα, η προστασία επιτυγχάνεται με το να εγκαταστήσουμε σε όλους τους ad hoc κόμβους το πρωτόκολλο SC-GPSR με όλα τα πρόσθετα λειτουργικά τμήματα που ορίσαμε έτσι ώστε να έχουμε μια πλήρως κατανεμημένη δομή του συστήματος ανιχνεύσεως εισβολών και προστασίας. Στη συνέχεια, κατά τη διαδικασία αυτό-οργάνωσης του δικτύου σε ομάδες (clusters) προσομοιώνουμε ένα αριθμό επιτιθέμενων κόμβων που μεταδίδουν ψευδή στοιχεία-παραμέτρους με σκοπό να αλλοιώσουν το αποτέλεσμα των τοπικών ψηφοφοριών. Είναι σημαντικό να ξεκαθαρίσουμε ότι το SC-GSPR σαν πρώτη γραμμή άμυνας χρησιμοποιεί μη κρυπτογραφικές μεθόδους προστασίας ώστε να αποφύγει την επιβάρυνση που επιφέρουν οι αναγκαίες διαδικασίες κρυπτογράφησης-αποκρυπτογράφησης και πιστοποίησης αυθεντικότητας στα περιορισμένα ad hoc δίκτυα. Έτσι, οι γειτονικοί κόμβοι των κακόβουλων κόμβων που έχουν εγκαταστημένα τα SC-GPSR blocks προστασίας ανιχνεύουν με συνεργατικό τρόπο τις ασυνέπειες που προκύπτουν μεταξύ των δεδομένων των επιτιθεμένων και των δεδομένων που μεταδίδουν οι υπόλοιποι γείτονες και με αυτόν τον τρόπο αρχικά μαρκάρουν τους υπόπτους κόμβους.

Έτσι με την εφαρμογή των κατωφλίων συνέπειας που ορίσαμε στην §6.4.3 γίνεται ένα πρώτο βήμα στην ανίχνευση της μη ορθής λειτουργίας του πρωτοκόλλου και ενεργοποιείται η διαδικασία της διασφάλισης της εκλογής των τοπικών αρχηγών. Ένας κόμβος είναι ύποπτος όταν δεν περνάει κάποιο (ή και τα δύο) από τα κατώφλια συνέπειας και τότε ανιχνεύεται από κάποιον από τους γείτονές του, ο οποίος καλείται κόμβος-ανιχνευτής (αυτοί μπορεί να είναι περισσότεροι του ενός).

Στη συνέχεια ο κόμβος-ανιχνευτής, απομονώνει τον ύποπτο κόμβο από τις λίστες που ο ίδιος διαθέτει με τους γειτονικούς κόμβους του έτσι ώστε να αποφύγει την προώθηση πακέτων προς τον ύποπτο κόμβο αλλά και για να αποκλείσει τον ύποπτο κόμβο από τις προτιμήσεις του για τον πιθανό κόμβο-αρχηγό κατά τη διαδικασία της ομαδοποίησης και συνεπώς να διαφυλάξει τους υπολοίπους κόμβους από ένα κακόβουλο και συμβιβασμένο αρχηγό.

Αν το απαιτούμενο επίπεδο ασφαλείας είναι υψηλό, τότε ο κόμβος-ανιχνευτής ενεργοποιεί έναν (ή και όλους) από τους τρεις παρακάτω κρυπτογραφικούς τρόπους άμυνας:

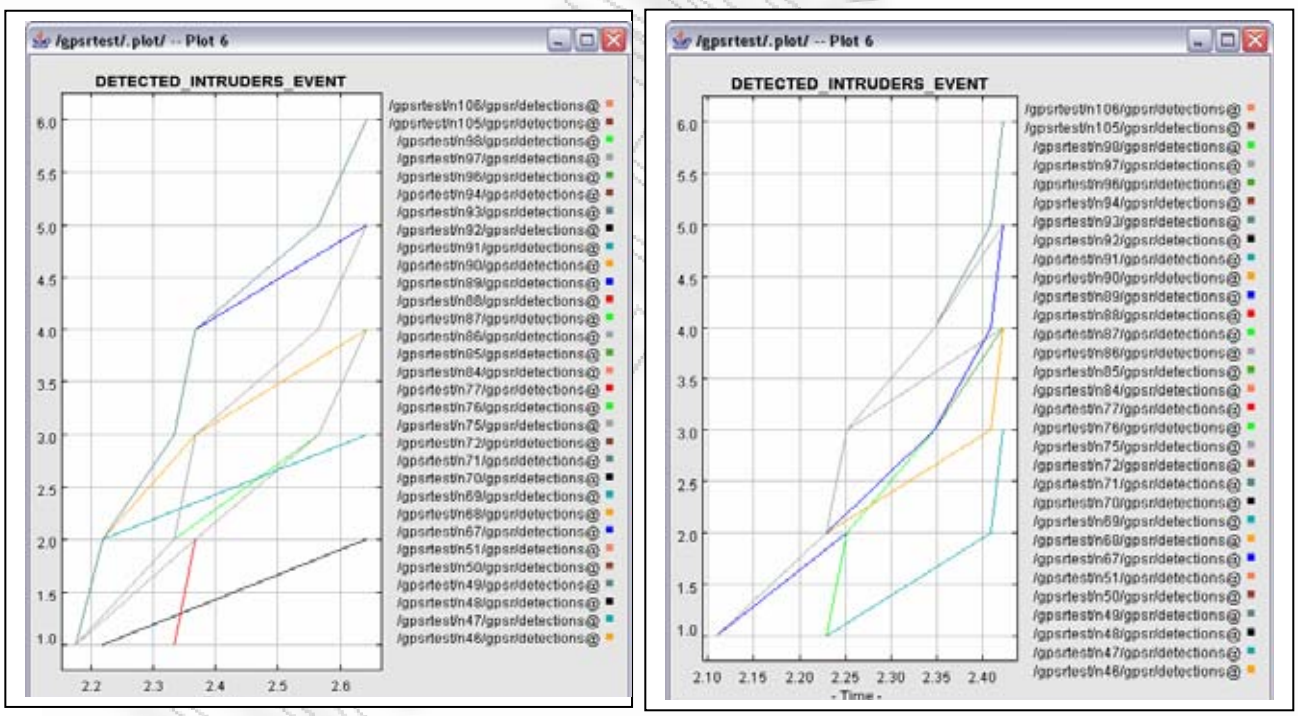
- Το σχήμα “challenge-response” με βάση το κοινό μυστικό του δικτύου SC-GPSR για την περαιτέρω αυθεντικοποίηση των ύποπτων μαρκαρισμένων κόμβων, δες §6.4.4.

- Τα δυναμικά παραγόμενα κλειδιά ταυτότητας ABK, δηλαδή συμμετρικά κλειδιά που παράγονται με βάση την ταυτότητα των κόμβων, δες §6.4.4.

- Την περαιτέρω αυθεντικοποίηση των μηνυμάτων Beacon που εκπέμπουν οι κόμβοι, έτσι ώστε να μπορέσει να πιστοποιηθεί τόσο η αυθεντικότητα των μηνυμάτων όσο και η αυθεντικότητα του κόμβου που τα εξέπεμψε.

Στην περίπτωση που ένας ύποπτος δεν είναι επιτυχής ως προς τους παραπάνω κρυπτογραφικούς ελέγχους, τότε μπαίνει στη μαύρη λίστα του δικτύου, η οποία είναι μια λίστα η οποία ανανεωμένη πρέπει να διαδίδεται σε όλο το δίκτυο ώστε οι κόμβοι να είναι ενημερωμένοι για το ποια είναι η ταυτότητα των εσωτερικών κόμβων του δικτύου που συνιστούν πραγματική απειλή. Οι κόμβοι-ανιχνευτές είναι αυτοί που ανανεώνουν τις μαύρες λίστες και τις εκπέμπουν πρώτοι στους γείτονές τους οι οποίοι σε ένα δίκτυο πολλαπλών βημάτων τις διαδίδουν περαιτέρω.

Η Εικόνα 58(α) απεικονίζει τους χρόνους ανίχνευσης που επιτεύχθηκαν από τους SC-GPSR κόμβους-ανιχνευτές. Για ένα σύνολο από 104 νόμιμους κόμβους και ένα τείχος από έξι κακόβουλους κόμβους (κάθετος άξονας στο γράφημα 58(α)) που δρουν σαν μαύρες τρύπες με τυχαία κινητικότητα των 10m/sec, οι κόμβοι-ανιχνευτές διέγνωσαν όλες τις επιθέσεις ψευδών μεταδόσεων σε χρόνο όχι μεγαλύτερο από 2.7 λεπτά (οριζόντιος άξονας στο γράφημα 58(α)). Δεδομένου ότι η διάρκεια του πειράματος ήταν 60 λεπτά και ότι ο χρόνος εκδήλωσης της πρώτης επίθεσης σε μία σειρά από έξι διαδοχικές επιθέσεις ήταν πολύ κοντά στην εκκίνηση του πειράματος οι χρόνοι ανίχνευσης που επιτεύχθηκαν είναι πολύ ικανοποιητικοί.



(α) Ανίχνευση με κίνηση, σενάριο επίθεσης #1. **(β)** Ανίχνευση χωρίς κίνηση, σενάριο επίθεσης #2.

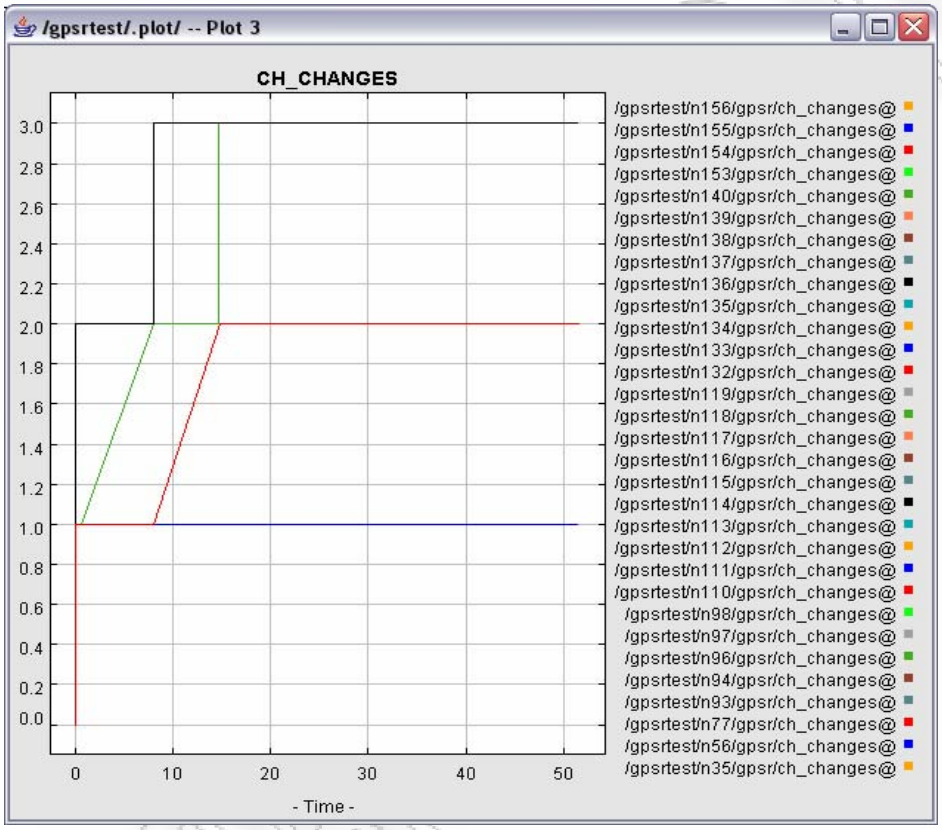
Εικόνα 58. Χρόνοι ανίχνευσης από το συνεργατικό σχήμα ανίχνευσης υπόπτων SC-GPSR.

Επίσης φαίνεται ότι οι πρώτες ανιχνεύσεις υπόπτων κόμβων έγιναν πολύ κοντά στο χρόνο εκκίνησης του πειράματος προσομοίωσης, δηλαδή η απόκριση του συνεργατικού τμήματος ανίχνευσης συνέβη πάρα πολύ κοντά στο χρόνο που η επίθεση εκδηλώθηκε από τον αντίστοιχο κακόβουλο κόμβο.

Η Εικόνα 58(β) δείχνει ότι στο σενάριο επίθεσης των έξι στατικών κόμβων με σταθερούς τους

υπόλοιπους κόμβους μέσα στο πλέγμα του δικτύου ο χρόνος απόκρισης των συστημάτων ανίχνευσης είναι μικρότερος από αυτόν της Εικόνας 58(α). Ονομαστικά ο μέγιστος χρόνος ανίχνευσης είναι τώρα μικρότερος των 2.5 λεπτών (οριζόντιος άξονας στο γράφημα 58(β)). Αυτό δείχνει ότι η κίνηση των κόμβων δυσχεραίνει την ανίχνευση των επιτιθέμενων με ύποπτη συμπεριφορά, ενώ αντίθετα οι στατικοί κακόβουλοι κόμβοι είναι δυνατόν να ανιχνευθούν και αντιμετωπιστούν συντομότερα.

Η Εικόνα 59 απεικονίζει τον αριθμό των αλλαγών στους ρόλους των κόμβων οι οποίες συνέβησαν κατά τη διάρκεια μιας ώρας πειράματος προσομοίωσης με το SC-GPSR. Στο συγκεκριμένο πείραμα συμμετείχαν 220 στατικοί κόμβοι και όπως φαίνεται στην Εικόνα 59 μόνο λίγοι κόμβοι πήραν το ρόλο του αρχηγού (συγκεκριμένα απεικονίζονται μόνο πέντε κόμβοι) οι οποίοι κατά τη διάρκεια του πειράματος προσομοίωσης άλλαξαν το ρόλο τους από αρχηγοί σε απλά μέλη και αντίστροφα. Ο αριθμός των αλλαγών ανά κόμβο δεν υπερέβη τον αριθμό των τριών αλλαγών. Αυτό είναι ένα ενδεικτικό αποτέλεσμα για την αποδοτικότητα του σχήματος επανεκλογής αρχηγών και ομαδοποίησης με τον αλγόριθμο RRA ο οποίος αποτελεί αναπόσπαστο μέρος του σχήματος ασφαλούς συσταδοποίησης και ad hoc δρομολόγησης SC-GPSR.



Εικόνα 59. Απεικόνιση του αριθμού των αλλαγών των κόμβων αρχηγών (cluster head changes) του δικτύου.

6.6. ΣΥΜΠΕΡΑΣΜΑΤΑ

Στο Κεφάλαιο αυτό ερευνήσαμε τη δυνατότητα ολοκλήρωσης της οργάνωσης και προστασίας των ασύρματων δικτύων ad hoc με τη χρήση ενός σχήματος που αποτελείται από κατανεμημένες λειτουργικές οντότητες. Το προτεινόμενο σχήμα σχεδιάστηκε και υλοποιήθηκε σαν επέκταση του γεωγραφικού πρωτοκόλλου GPSR. Κατά τη σχεδίαση δώσαμε έμφαση στα περιορισμένα δίκτυα αισθητήρων και στα ιδιαίτερα χαρακτηριστικά τους. Το βασικό τμήμα που διαφοροποιεί το προτεινόμενο σχήμα προστασίας είναι η χρήση του συνεργατικού μοντέλου ψηφοφορίας για την ανίχνευση εισβολέων με βάση διακριτά επίπεδα ασφάλειας.

Τα πειράματα προσομοίωσης που διεξαγάγαμε έδειξαν ότι τα πρόσθετα λειτουργικά τμήματα επιφέρουν αμελητέα επιβάρυνση στην δικτυακή επίδοση ενώ ταυτόχρονα επιτυγχάνουν προστασία από επιθέσεις που απειλούν να συμβιβάσουν τους ισχυρούς κόμβους του δικτύου. Οι επιθέσεις στις οποίες εστιάσαμε είναι οι επιθέσεις που απειλούν την συνεπή εκλογή των κόμβων-αρχηγών μέσα στο δίκτυο και επιθέσεις προώθησης επιθέσεων (επίθεση μαύρης/γκρι τρύπας) κατά τις οποίες οι κακόβουλοι κόμβοι απορρίπτουν τα πακέτα που λαμβάνουν από τους γείτονές τους.

Υπό την απειλή κόμβων που απέρριπταν πακέτα με το σχήμα SC-GPSR επιτεύχθηκε δικτυακή επίδοση που ήταν καλύτερη από τη δικτυακή επίδοση του GPSR. Επιπλέον, στα πειράματα προσομοίωσης η απόκριση και η ικανότητα ανίχνευσης υπόπτων κόμβων με το SC-GPSR ήταν ικανοποιητική. Είναι αξιοσημείωτο ότι το προτεινόμενο σχήμα SC-GPSR κατάφερε να ανιχνεύσει και να παρακάμψει τους κακόβουλους κόμβους που τοποθετήθηκαν στο πλέγμα δοκιμών ανάμεσα στους κόμβους με κανονική δικτυακή συμπεριφορά.

Ειδικότερα, ανιχνεύθηκαν όλοι οι κακόβουλοι κόμβοι που προσομοιώσαμε σε διαφορετικά σενάρια επιθέσεων, όπως τυχαία και καθορισμένη τοποθέτηση των επιτιθέμενων, μεταβλητό μέγεθος δικτύου και αυξανόμενη κινητικότητα των κόμβων. Το δίκτυο προστατεύεται έγκαιρα με το μαρκάρισμα των κόμβων που προσπαθούν να μεταδώσουν ψευδή δεδομένα ώστε να μπορέσουν να έλξουν και στη συνέχεια να απορρίψουν τα πακέτα που θα λάβουν. Οι κακόβουλοι κόμβοι με το SC-GPSR τοποθετούνται σε μαύρες λίστες που διαδίδονται στο δίκτυο με αποτέλεσμα να αποκλείονται από τις διαδικασίες της οργάνωσης, της εκλογής αρχηγών και της δρομολόγησης και επομένως η απώλεια δεδομένων αποφεύγεται.

Το σχήμα SC-GPSR πέτυχε καλή επίδοση όταν ο αριθμός των επιθέσεων αυξήθηκε.

6.7. ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] I. F. Akyildiz, X. Wang. “A Survey on Wireless Mesh Networks”. IEEE Communications Magazine, Vol. 33, Issue 9, September 2005, pp. S23-S30.

[2] K. Kifayat, M. Merabti, Q. Shi and D. Llewellyn-Jones, “Application Independent Dynamic Group-Based Key Establishment for Large-scale Wireless Sensor Networks”, China Communications, Vol. 4, No. 1, February 2007, pp. 14-27.

[3] B. Karp, H. Kung. “GPSR: Greedy Perimeter Stateless Routing for sensor networks”. In: Proceedings of the 6th Annual Int’l Conference on Mobile Computing and Networking, Boston: ACM Press, 2000, pp. 243-254.

[4] A. Abbasi, M. Younis. “A survey on clustering algorithms for wireless sensor networks”. In: Elsevier Computer Communications, Vol. 30, pp. 2826-2841, 2007.

[5] J. Y. Yu and P. H. J. Chong. “A Survey of Clustering Schemes for Mobile Ad Hoc Networks”. IEEE Communications Surveys and Tutorials, Vol. 7, No. 1, pp. 32-48, 2005.

[6] A. Ephremides, J. E. Anthony, D. J. Baker. A design concept for reliable mobile radio networks with frequency hopping signalling. Proc. IEEE 1987; Vol. 75, no. 1, pp. 56-73.

[7] Chiang C. C., Wu, H. K., Liu, W., Gerla, M. “Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel”. Proc. IEEE SICON, Singapore, 1996.

[8] C.R. Lin and M. Gerla. “Adaptive Clustering for Mobile Wireless Networks”. In: IEEE Journal on Selected Areas in Communications, Vol. 15, No. 7, Sep. 1997, pp. 1265-1275.

[9] M. Jiang, J. Li and Y. C. Tay, “Cluster Based Routing Protocol”, IETF Draft, August 1999. Work in Progress.

[10] A. Iwata, C.-C. Chiang, G. Pei, M. Gerla, and T.-W. Chen, “Scalable Routing Strategies for Ad Hoc Wireless Networks” IEEE Journal on Selected Areas in Communications, Special Issue on Ad-Hoc Networks, Aug. 1999, pp.1369-79.

[11] Yunjung Yi, Taek Jin Kwon and Mario Gerla “Passive Clustering (PC) in Ad Hoc Networks”, Internet Draft, draft-ietf-yi-manet-pac-00.txt, Nov. 2001.

[12] S. Basagni. “Distributed clustering for ad hoc networks”. Proceedings of the International Symposium on Parallel Architectures, Algorithms and Networks, (I-SPAN’99), Perth/Fremantle. June 1999, pp. 310-315.

[13] P. Basu, N. Kham, T. D. C. Little. “A Mobility Based Metric for Clustering in Mobile Ad Hoc Networks”. International Conference on Distributed Computing Systems Workshop, Apr. 2001.

[14] M. Chatterjee, S. K. Das, D. Turgut. “WCA: A Weighted Clustering Algorithm for Mobile Ad Hoc Networks”, Cluster Computing Journal, Vol. 5, no. 2, Apr. 2002, pp. 193-204.

[15] A. Chandrakasan, W. R. Heinzelman, H. Balakrishnan. “Energy-efficient communication protocol for wireless micro sensor networks”. In: 33rd Annual Hawaii International Conference on System Sciences, HICSS, 2000, pp. 3005-3014.

[16] O. Younis and S. Fahmy, “HEED: A Hybrid Energy-Efficient Distributed Clustering Approach for Ad Hoc Sensor Networks,” IEEE Transactions on Mobile Computing vol. 3, no. 4, Oct-Dec 2004.

[17] H. Taniguchi, M. Inoue, T. Masuzawa, and H. Fujiwara. “Clustering Algorithms in Ad Hoc Networks”. Electronics and Communications in Japan, Part 2, Vol. 88, No. 1, 2005, pp. 51-59.

[18] G. V. Crosby, N. Pissinou, J. Gadze. “A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks”, In: Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems (DSSNS 2006), Columbia MD, pp. 15-22.

[19] W. Zhang, S. K. Das, Y. Liu. “A Trust Based Framework for Secure Data Aggregation in Wireless Sensor Networks”. Proceedings of the IEEE SECON 2006, Vol. 1, pp. 60-69, Reston VA.

[20] D. Balachandran, D. Dasgupta, L. Wang. “A Hybrid Approach for Misbehavior Detection in Wireless Ad Hoc Networks”. In: Proceedings of the 9th Annual NYS Cyber Security Conference: Intrusion Detection and Prevention, 2006, New York.

[21] M. Qin , R. Zimmermann, “An Energy-Efficient Voting-Based Clustering Algorithm for Sensor Networks”, In: Proceedings of the Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing and First ACIS International Workshop on Self-Assembling Wireless Networks, May 23-25, 2005, pp. 444-451.

[22] C. Tselikis, C. Douligeris, S. Mitropoulos and N. Komninos. “Consistent re-clustering in Mobile Ad Hoc Networks”. In: Proceedings of the International Wireless Communications and Mobile Computing Conference (IWCMC’ 08), Crete Island, Greece, August 2008, pp. 825-830.

[23] M. Sirivianos, D. Westhoff, F. Armknecht, J. Girao. “Non-Manipulable Aggregator Node Election Protocols for Wireless Modelling and Optimization in Mobile Ad Hoc and Wireless Networks”, ICST WiOpt, 2007.

[24] M. Fischer, A. Lynch, M. S. Paterson. “Impossibility of Distributed Consensus with One Faulty Process”. Journal of the ACM, vol. 32, No 2, 1985, pp. 374-382.

[25] S. Vasudevan, J. Kurose and D. Towsley. “Design and Analysis of a Leader Election Algorithm for Mobile Ad Hoc Networks”. In: Proceedings of IEEE International Conference on Network Protocols (ICNP), Berlin, Germany, October 2004.

[26] K. D. Kang, K. Liu, and N. Abu-Ghazaleh, “Securing Geographic Routing in Wireless Sensor Networks”, 9th Annual NYS Cyber Security Conference: Intrusion Detection and Prevention.

[27] A. Pirzada and Chris McDonald. “Trusted Greedy Perimeter Stateless Routing”, In: 15th IEEE International Conference on Networks (ICON2007), Adelaide, Australia, November 2007, pp. 206-211.

[28] K. Huguenin, “Evaluating geographical routing for wireless sensor networks”. Available from: http://perso.eleves.bretagne.enscachan.fr/~huguenin/Stage06.pdf

[29] Wu Hao, Cheng Chao, Li Cheng-Shu. “Research on One Kind of Improved GPSR Secure Routing”, Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications, 2007 International Symposium.

[30] Tian He, Brian M. Blum, Qing Cao, John A. Stankovic, Sang H. Son, Tarek F. Abdelzaher. “Robust and timely communication over highly dynamic sensor networks”. Springer Real-Time Systems (2007), Vol. 37, pp. 261-289.

[31] [Huang, 2003a] Y. Huang, and W. Lee, *“A Cooperative Intrusion Detection System for Ad Hoc Networks”*, in Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN’03), October (2003), Fairfax, VA, USA, pp. 135-147.

[32] Kempf, J. et al. Internet Draft Document, draft-kempf-secure-nd-01.txt Securing IPv6 Neighbor Discovery Using Address Based Keys.

[33] M. Fischer, A. Lynch, M. S. Paterson. “Impossibility of Distributed Consensus with One Faulty Process”. Journal of the ACM, vol. 32, No 2, 1985, pp. 374-382.

[34] J-P Hubaux, L. Buttyan, S. Capkun. “The Quest for Security in Mobile Ad Hoc Networks”. MobiHOC 2001, Long Beach, CA, USA, pp. 146-155.

[35] Sirivianos, M., Westhoff, D., Armknecht, F., Girao, J. *Non-Manipulable Aggregator Node Election Protocols for Wireless Sensor Networks*. Proc of the. 5th Intl. Symposium on Modelling and Optimization in Mobile, Ad Hoc, and Wireless Networks, (ICST WiOpt), 2007.

[36] Komninos, N., Vergados, D., Douligeris, C. *Detecting unauthorized and compromised nodes in mobile ad hoc networks*. Ad Hoc Networks, vol. 5, 2007, pp. 289-298.

[37] C. Tselikis, C. Douligeris, S. Mitropoulos and N. Komninos. “Consistent re-clustering in Mobile Ad Hoc Networks”. In: Proceedings of the International Wireless Communications and Mobile Computing Conference (IWCMC’ 08), Crete Island, Greece, August 2008, pp. 825-830.

[38] S. Vasudevan, J. Kurose and D. Towsley. “Design and Analysis of a Leader Election Algorithm for Mobile Ad Hoc Networks”. In: Proceedings of IEEE International Conference on Network Protocols (ICNP), Berlin, Germany, October 2004.

[39] M. Qin , R. Zimmermann, “An Energy-Efficient Voting-Based Clustering Algorithm for Sensor Networks”, In: Proceedings of the Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing and First ACIS International Workshop on Self-Assembling Wireless Networks, May 23-25, 2005, pp. 444-451.

[40] A. A. Abbasi, M. Younis. “A survey on clustering algorithms for wireless sensor networks”. In: Elsevier Computer Communications, Vol. 30, pp. 2826-2841, 2007.

[41] J. Y. Yu and P. H. J. Chong. “A Survey of Clustering Schemes for Mobile Ad Hoc Networks”. IEEE Communications Surveys and Tutorials, Vol. 7, No. 1, pp. 32-48, 2005.

[42] O. Kachirski, R. Guha, D. Schwartz, S. Stoecklin, and E. Yilmaz, “Case-Based Agents for Packet-Level Intrusion Detection in Ad Hoc Networks,” in Proceedings of the 17th International Symposium on Computer and Information Sciences, October 28-30, 2002, Orlando, FL, USA, pp. 315–320.

[43] J-Sim. Available from: http://j-sim.cs.uiuc.edu

7. ΕΙΣΑΓΩΓΗ ΚΑΤΑΝΕΜΗΜΕΝΩΝ ΤΕΧΝΟΛΟΓΙΩΝ ΜΕΣΙΣΜΙΚΟΥ ΣΤΑ ΔΙΚΤΥΑ AD HOC

Στο Κεφάλαιο αυτό θα μας απασχολήσουν οι τεχνολογίες μεσισμικού και ιδιαίτερα η διερεύνηση της δυνατότητας εισαγωγής των κατανεμημένων τεχνολογιών ανακάλυψης υπηρεσιών στα περιορισμένα ασύρματα δίκτυα ad hoc. Για το σκοπό αυτό θα εκπονήσουμε μια συγκριτική μελέτη των υποψήφιων κατανεμημένων μοντέλων και τεχνολογιών μεσισμικού ("ad hoc middleware").

Μέχρι σήμερα, ο χώρος του ενσύρματου Διαδικτύου στεγάζει πλήθος εφαρμογών βασισμένων στην τεχνολογία των κατανεμημένων συστημάτων. Τα κατανεμημένα συστήματα διακρίνονται σε τρεις βασικές κατηγορίες ανάλογα με την αρχιτεκτονική στην οποία βασίζονται: Client – Server, 3 Tier και P2P. Κάθε μια κατηγορία περιλαμβάνει συστήματα που ικανοποιούν τις ιδιαίτερες απαιτήσεις των εφαρμογών που υποστηρίζουν. Σκοπός μας είναι να ερευνήσουμε κατά πόσο είναι δυνατή η ανάπτυξη κατανεμημένων συστημάτων και των τριών παραπάνω μοντέλων βασισμένα σε αρχιτεκτονικές ασυρμάτων ad hoc δικτύων. Στα πλαίσια της έρευνας αυτής, θα αναζητηθούν μεθοδολογίες και αρχιτεκτονικές ικανές να στηρίξουν την υλοποίηση θεμελιωδών υπηρεσιών κατανεμημένων συστημάτων, όπως αυτών της εγγραφής ("registration"), της πλοήγησης ("browsing") και της αναζήτησης ("searching") πληροφοριών και υπηρεσιών σε ασύρματα ad hoc δίκτυα [22]. Σε αυτό το πλαίσιο στις επόμενες παραγράφους θα μελετήσουμε τη δυνατότητα μεταφοράς υπαρχόντων ενσύρματων κατανεμημένων συστημάτων σε ad hoc πλατφόρμες. Τέλος, θα αναζητήσουμε και θα συγκρίνουμε τα απαραίτητα πρότυπα και τις κατάλληλες τεχνολογίες για την ανάπτυξη εφαρμογών βασισμένων στο υπό μελέτη περιβάλλον ad hoc (π.χ. XML, Web Services, RMI, EJB, JSP, Servlets, κλπ).

Οι τεχνολογίες ανακάλυψης υπηρεσιών έχουν γίνει αντικείμενο μεγάλης έρευνας όσον αφορά το Διαδίκτυο και τα ομότιμα δίκτυα (peer-to-peer) μεγάλης κλίμακας για τα οποία έχουν αναπτυχθεί διαφορετικά μοντέλα επικοινωνιών και αρχιτεκτονικών για την εγγραφή και την απομακρυσμένη ανακάλυψη των διαθέσιμων υπηρεσιών που βρίσκονται μέσα σε εξυπηρετητές. Μερικά από τα βασικά μοντέλα δημοσίευσης, ανακάλυψης και διαχείρισης υπηρεσιών που συναντάμε σε ένα δίκτυο με υποδομή είναι το σύγχρονο μοντέλο ερώτησης-απόκρισης, το ασύγχρονο μοντέλο "publish-subscribe" και το μοντέλο Services Oriented Architecture (SOA). Στην αρχιτεκτονική SOA οι απομακρυσμένοι κόμβοι δημοσιοποιούν τις υπηρεσίες/πόρους που διαθέτουν (συνήθως στη μορφή ενός URL) έτσι ώστε οι υπόλοιποι κόμβοι να μπορούν να ανακαλύπτουν και να καλούν τις υπηρεσίες αυτές απομακρυσμένα.

Τα πιθανά μοντέλα επικοινωνιών (σύγχρονο, ασύγχρονο, βασισμένο στη ροή –"stream oriented"– , βασισμένο στα μηνύματα –"message oriented"– κ.α.) και τα πιθανά υπολογιστικά παραδείγματα που είναι κατάλληλα για την ανακάλυψη των υπηρεσιών (client/server, peer-to-peer -όπως το publish/subscribe- και το publish/discover/invoke όπως το μοντέλο της αρχιτεκτονικής SOA) σε δίκτυα που τρέχουν ad hoc πρωτόκολλα δρομολόγησης παραμένει ένα ανοιχτό πεδίο έρευνας. Ειδικότερα, οι λύσεις που έχουν προσαρμοστεί ως υποσύνολα των λύσεων που υφίστανται στο Διαδίκτυο για τα περιορισμένα δίκτυα ad hoc είναι λιγοστές και είναι ακόμη υπό εξέλιξη και επομένως η περαιτέρω διερεύνηση του προβλήματος είναι επιβεβλημένη. Ενδεικτικά αναφέρουμε ότι μια τέτοια λύση που προσαρμόζει τα Web Services σε μικρές συσκευές είναι το πρότυπο "Devices Profile Web Services", DPWS, [1], όπως και η Java πλατφόρμα σχεδίασης, ανάπτυξης, ολοκλήρωσης και εύρεσης υπηρεσιών οι οποίες εγγράφονται σε μητρώα που αναπτύσσεται από την OSGi Alliance [23]. Ακόμη, το πρωτόκολλο 6lowPAN (RFC4944, [24]) προσαρμόζει το πρωτόκολλο IPv6 στο πρωτόκολλο δικτύωσης των προσωπικών συσκευών χαμηλής ισχύος IEEE 802.15.4.

Ιδιαίτερα τονίζουμε ότι οι λύσεις είναι αναγκαστικά διαφορετικές για τους διαφορετικούς τύπους των

ad hoc δικτύων και των ad hoc συσκευών αφού, για παράδειγμα, οι πόροι σε ένα ασύρματο δίκτυο αισθητήρων είναι λιγότεροι από τα δίκτυα MANET και συνεπώς η εισαγωγή διαλειτουργικών κατανεμημένων πλαισίων αν όχι αδύνατη είναι σίγουρα δυσχερής. Αυτή η δυσκολία της διαλειτουργικότητας των λύσεων στον κόσμο των μικρών και μικροσκοπικών συσκευών οφείλεται κυρίως στα διαφορετικών δυνατοτήτων και χαρακτηριστικών ενσωματωμένα λειτουργικά συστήματα. Έτσι, πολλά λειτουργικά συστήματα, όπως το tinyOS [25] που χρησιμοποιείται στα WSN, βασίζονται σε προγραμματισμό με “events” και δεν υποστηρίζουν προγραμματισμό πολλαπλών νημάτων. Ακόμη, η ασφάλεια που παρέχουν τα ενσωματωμένα λειτουργικά συστήματα πραγματικού χρόνου περιορίζεται μόνο στα χαμηλά δικτυακά επίπεδα (φυσικό επίπεδο και επίπεδο διασύνδεσης) ενώ η διαχείριση μνήμης που παρέχουν είναι υποτυπώδης. Ακόμη οι εφαρμογές που έχουν γραφτεί σε αυτά τα συστήματα είναι πολλές φορές λίγες και τα διαθέσιμα εργαλεία όχι εύχρηστα (ή/και ανύπαρκτα) με αποτέλεσμα να δυσχεραίνεται η περαιτέρω ανάπτυξη των εφαρμογών και η βελτιστοποίηση των τεχνολογιών.

Από την πλευρά μας ιδιαίτερη έμφαση θα δώσουμε στις βασικές αρχές που χαρακτηρίζουν και διαφοροποιούν τις τεχνολογίες ανακάλυψης υπηρεσιών και στα διαφορετικά μοντέλα ανοιχτών επικοινωνιών (μοντέλα μεσισμικού) στα οποία στηρίζονται οι διαφορετικές τεχνολογίες ανακάλυψης υπηρεσιών. Στη συνέχεια, θα ερευνήσουμε συστηματικούς και δομημένους τρόπους ελέγχου και εκτίμησης της επίδοσης των τεχνολογιών που διατίθενται με βάση τα διαφορετικά μοντέλα που αναλύονται.

Επίσης η εισαγωγή των τεχνολογιών ανακάλυψης υπηρεσιών στα δίκτυα ad hoc (ως υπηρεσίες θεωρούμε κοινούς πόρους, δηλαδή μνήμη, αρχεία, πολυμεσικό υλικό κ.α. που διαθέτουν για κοινή χρήση οι κόμβοι ενός δικτύου MANET ή υπηρεσίες όπως η ανάγνωση θερμοκρασίας, πίεσης και άλλων περιβαλλοντικών μεταβλητών καθώς και εικόνας που διαβάζουν οι αισθητήρες σε ένα δίκτυο WSN) θεωρούμε ότι υιοθετεί μια διεπαφή ανάμεσα στο ad hoc δίκτυο και το Διαδίκτυο και επομένως απαιτείται η υλοποίηση αυτής της διεπαφής με κατάλληλες πύλες ανακάλυψης υπηρεσιών (gateways) που προσαρμόζουν τα υφιστάμενα και τα νέα πρωτόκολλα που αναπτύσσονται ανάμεσα στα δίκτυα ad hoc και στα εξωτερικά δίκτυα, όπως είναι το Διαδίκτυο.

7.1. ΤΟ ΣΥΓΧΡΟΝΟ ΜΟΝΤΕΛΟ ΕΠΙΚΟΙΝΩΝΙΩΝ

Ένα σημαντικό τμήμα των κατανεμημένων υποδομών χαρακτηρίζεται από διαδράσεις με ανταλλαγή μηνυμάτων που στηρίζονται στο μοντέλο πελάτη-εξυπηρετητή το οποίο συνηθέστερα υλοποιείται μέσω του πρωτοκόλλου “αιτήματος-απαντήσεως”. Οι μοντέρνες κατανεμημένες εφαρμογές και τα συστήματα μπορούν να διαφοροποιηθούν με κριτήριο το αν τηρούν το συγχρονισμένο ή το μη συγχρονισμένο επικοινωνιακό μοντέλο για την εκτέλεση των αιτημάτων από τους κόμβους πελάτες και την αξιόπιστη παράδοση των μηνυμάτων-απαντήσεων από τους κόμβους εξυπηρετητές.

Μια συγκριτική μελέτη επιδόσεων [16] αναλύει το μη-συγχρονισμένο μοντέλο μεσισμικού το οποίο βασίζεται στη παράδοση και επεξεργασία μηνυμάτων κατά δεσμίδες (“batch processing”), έναντι του συγχρονισμένου μοντέλου επικοινωνιών που υλοποιείται με κλήσεις απομακρυσμένης διαδικασίας RPC (“Remote Procedure Calls”).

Εδώ επικεντρωνόμεθα στο συγχρονισμένο μοντέλο client-server τριών επιπέδων (three tier) που υλοποιούμε μέσω της πλατφόρμας Java2 Enterprise Edition (J2EE). Επιλέξαμε τούτο ως το πρώτο βήμα για την ανάπτυξη μιας πλατφόρμας δοκιμών και ελέγχου λογισμικού που θα είναι ικανή να δέχεται ποικίλες τεχνολογίες μεσισμικού ως είσοδο. Επιπλέον, όπως έχουμε ήδη αναφέρει στο παρόν ενδιαφερόμαστε για τον υπολογισμό και τη σύγκριση των επιδόσεων εφαρμογών με περιορισμούς στους χρόνους εκτέλεσης.

Τα τρία επίπεδα στο μοντέλο των τριών επιπέδων για την ανάκτηση πληροφοριών από ένα κεντρικό εξυπηρετητή είναι:

- Το στρώμα της βάσης δεδομένων όπου αποθηκεύονται οι πληροφορίες που είναι σχετικές με τις υπηρεσίες που παρέχονται από το δίκτυο.

- Το στρώμα των κόμβων-εξυπηρετητών που περιλαμβάνει τις διαθέσιμες πλατφόρμες μεσισμικού οι οποίες διασφαλίζουν την αποδοτική διαχείριση των διεργασιών στους εξυπηρετητές όπως τον επιμερισμό του φορτίου των εφαρμογών, το συγχρονισμό των διεργασιών αλλά και την αξιόπιστη επικοινωνία μεταξύ των απομακρυσμένων συστημάτων. Επίσης, σε αυτό το στρώμα ανήκουν και οι διαχειριστές και ελεγκτές των μηνυμάτων που ανταλλάσσονται ("monitors").

- Το στρώμα των εφαρμογών τελικού χρήστη, δηλαδή το λογισμικό μέσω του οποίου οι πελάτες υποβάλλουν ερωτήσεις στο στρώμα των εξυπηρετητών σχετικές με πληροφορίες των υπηρεσιών που οι τελευταίοι παρέχουν.

Διαλέξαμε τα εξής συγχρονισμένα μοντέλα μεσισμικού ως κοινούς υποψηφίους για ένα τέτοιο περιβάλλον με σκοπό να υπογραμμίσουμε τις διαφορετικές προσεγγίσεις και ιδέες που χαρακτηρίζουν κάθε ένα απ' αυτά:

- ***Μοντέλο επικοινωνιών προσανατολισμένο στη ροή*** ("stream-oriented"). Οι επεξεργασίες εισόδου και εξόδου επικοινωνούν μέσω συνδέσεων διπλής κατευθύνσεως με συγχρονισμένη ροή από bytes (π.χ. ανταλλαγή πληροφοριών μέσω απλών TCP sockets ή μέσω HTTP συνόδων μεταξύ φυλλομετρητών στην πλευρά του πελάτη και Servlets στην πλευρά του εξυπηρετητή στο Web.

- ***Αντικειμενοστρεφές κατανεμημένο μοντέλο*** ("Object Oriented distributed model"). Θεωρούμε την κλήση απομακρυσμένης μεθόδου RMI ("Remote Method Invokation") ως επαρκές δείγμα αυτού του μοντέλου. Τόσο ο πελάτης όσο και ο εξυπηρετητής ακολουθούν τη μοντελοποίηση με κλάσεις και το κατανεμημένο σύστημα υλοποιείται με ομότιμα (peer) αντικείμενα τα οποία ανταλλάσσουν τις πληροφορίες ως ορίσματα και ως τιμές επιστροφής συναρτήσεων που εγκαθίστανται και τρέχουν σε διαφορετικά και απομακρυσμένα μηχανήματα.

- ***Αρχιτεκτονική προσανατολισμένη στις υπηρεσίες*** (Services Oriented Architecture, SOA). Για το μοντέλο SOA όπου οι υπηρεσίες διατίθενται δημόσια με μηχανισμούς δημοσίευσης, ανακάλυψης και επίκλησης στο Web, επιλέξαμε τη Java διεπαφή προγράμματος εφαρμογής (Application Program Inteface, API) με βάση το XML, δηλαδή το Java XML-RPC (JAX-RPC) για συγχρονισμένη μεταφορά των δεδομένων των συναλλαγών μέσω του πρωτοκόλλου SOAP.

Ποικιλία πρωτοκόλλων μεσισμικού υποστηρίζει τα ως άνω μοντέλα. Μερικές Java τεχνολογίες που είναι υποψήφιες για το ad hoc περιβάλλον παρουσιάζονται στον Πίνακα 7.

Επίσης, πολύ μεγαλύτερη ποικιλία πακέτων μεσισμικού διαθεσίμων στο εμπόριο (ανοιχτού κώδικα ή με κατοχυρωμένη ιδιοκτησία) υλοποιεί και υποστηρίζει τα παραπάνω πρωτόκολλα. Έκαστο πακέτο λογισμικού που υλοποιεί τα παραπάνω μοντέλα διαθέτει τα ιδιαίτερα γνωρίσματά του.

Από την πλευρά μας εστιάσαμε σε τρία πακέτα J2EE (RMI, Servlets, JAX-RPC) των οποίων τα API θα παρουσιάσουμε διεξοδικά σε επόμενη ενότητα. Ωστόσο, πρέπει να υποδείξουμε εκ των προτέρων μερικές σημαντικές διαφορές των τριών αυτών τεχνολογιών. Αυτές είναι οι παρακάτω:

Java Τεχνολογία Μεσισμικού	Μοντέλο Μεσισμικού	Κωδικοποίηση	Επιστροφή Κλήσης
RMI	Κατανεμημένο Object Oriented μοντέλο	Δυαδικό	Java Object
Jini	Κεντρικοποιημένο Object Oriented μοντέλο	Δυαδικό	Java Object
WS-Discovery	SOA	Κείμενο XML	XML/SOAP
Sockets (6LowPan)	Byte Stream (TCP) / Datagram (UDP)	Δυαδικό	Java Object

Πίνακας 7: Τεχνολογίες αιχμής ανακάλυψης υπηρεσιών.

- Και το RMI και το JAX-RPC είναι υλοποιήσεις του μοντέλου πρόσβασης σε υπηρεσία μέσω απομακρυσμένης διεπαφής. Τα servlets και οι υπηρεσίες Web απαιτούν ένα περιβάλλον κόμβου-εξυπηρετητή εφαρμογών όπου θα διαχειρίζονται τα μηνύματα HTTP και SOAP και όπου θα εκτελούνται τα αιτήματα, ενώ το RMI μπορεί να εξυπηρετήσει τα αιτήματα που φθάνουν σε ομότιμη οντότητα βασιζόμενο μόνον επί των υπηρεσιών του Java "run-time system" το οποίο και εκτελεί τις κλήσεις απομακρυσμένης μεθόδου.

- Στο επίπεδο του προγραμματισμού οι υπηρεσίες Web και το JAX-RPC διαφέρουν απ' το μοντέλο κατανεμημένων αντικειμένων κατά το ότι θα – έπρεπε να – στερούνται κύριες μεθόδους ("main methods") και κατασκευαστές υπηρετών ("servants"). Πιστεύουμε ότι αυτό σχετίζεται στενά με την εκτέλεσή τους εντός του περιβάλλοντος των application servers.

Σκοπεύουμε να διερευνήσουμε με πειράματα πώς επιτυγχάνεται ο συγχρονισμός διαφορετικών πακέτων μεσισμικού και να τονίσουμε την επίδραση του μεσισμικού στο χρόνο απόκρισης (responsiveness) και στη διαπερατότητα των κατανεμημένων εφαρμογών που μπορούμε να συναντήσουμε ακόμη και στα δίκτυα ad hoc.

Επίσης, αξιοποιώντας πειράματα προσομοίωσης, σκοπεύουμε να συγκροτήσουμε κατάλληλα μοντέλα χρήσης και εμπειρικά να αποκαλύψουμε τα εγγενή γνωρίσματα των διαφορετικών μοντέλων μεσισμικού.

7.2. ΣΧΕΔΙΑΣΗ ΕΦΑΡΜΟΓΗΣ ΕΛΕΓΧΟΥ ΜΕΣΙΣΜΙΚΟΥ

Σχεδιάσαμε και υλοποιήσαμε με συστηματικό τρόπο μια κατανεμημένη εφαρμογή ελέγχου με σκοπό την εκτίμηση της απόδοσης των υποψηφίων για το ad hoc περιβάλλον τεχνολογιών μεσισμικού που διαλέξαμε να μελετήσουμε. Για τη συγκριτική μας μελέτη υποθέσαμε ότι οι πελάτες υποβάλλουν ένα φορτίο αιτημάτων ανακάλυψης και επίκλησης υπηρεσίας προς ένα κόμβο που διαθέτει υλοποιημένη τη δημόσια υπηρεσία με τις εν λόγω διαφορετικές τεχνολογίες μεσισμικού. Αυτός ο εξυπηρετητής στο ad hoc δίκτυο μπορεί να είναι ένας απλός εσωτερικός κόμβος ή/και μπορεί να είναι ο sink κόμβος ο οποίος συγκεντρώνει τα δεδομένα όλων των κόμβων-αισθητήρων σε ένα δίκτυο WSN.

Για λόγους επιδόσεων, κατά τη διάρκεια μίας συνεδρίας (session) μεταξύ ενός πελάτη και του εξυπηρετητή πολύ συχνά υιοθετείται το συγχρονισμένου μοντέλο επικοινωνιών RPC, δηλ. ο πελάτης σταματάει να επεξεργάζεται και περιμένει ώσπου να λάβει το αποτέλεσμα-απάντηση που μεταδίδεται από τον εξυπηρετητή. Από την άλλη μεριά, η επεξεργασία στον εξυπηρετητή μπορεί επίσης να μένει συγχρονισμένη με τα κατά σειρά λαμβανόμενα αιτήματα των πελατών, στην περίπτωση που η ad hoc εφαρμογή προσδιορίζει περισσότερες παράλληλες αλληλεπιδράσεις. Η επιλογή μιας εφαρμογής ελέγχου ανακάλυψης υπηρεσίας είναι κατάλληλη για τον έλεγχο και την εκτίμηση της απόδοσης συγχρονισμένων και ασύγχρονων τεχνολογιών μεσισμικού (εφόσον

αλλάξουμε το μοντέλο των τεχνολογιών που υλοποιείται και αξιολογείται).

Η εφαρμογή ελέγχου σχεδιάζεται ως μία σύνθετη εφαρμογή πελάτη-εξυπηρετητή, δηλαδή αποτελείται από δυο αυτοτελείς και μη περαιτέρω αναλυόμενες διαδικασίες οι οποίες είναι: (α) η διαδικασία της εξακρίβωσης της γνησιότητας (authentication) της ταυτότητας της συσκευής του πελάτη η οποία ταυτότητα μεταδίδεται από τον πελάτη στον εξυπηρετητή. Ο εξυπηρετητής στη συνέχεια διενεργεί αναζήτηση της ταυτότητας ταυτότητας της συσκευής του πελάτη στη βάση δεδομένων / μητρώο / ή στην προσωρινή μνήμη "cache" όπου είναι αποθηκευμένες οι ταυτότητες των νόμιμων συσκευών και χρηστών του δικτύου. Αν το αποτέλεσμα της αναζήτησης είναι θετικό για την ταυτότητα του πελάτη, μεταδίδεται ένα μήνυμα θετικής επιβεβαίωσης από τον εξυπηρετητή προς τον πελάτη, διαφορετικά η σύνθετη διαδικασία τερματίζεται στο πρώτο αυτό μέρος της. (β) μετά την επιτυχή ολοκλήρωση του (α), ο πελάτης εισάγει το δεύτερο αίτημά του το οποίο περιλαμβάνει την παράμετρο "τύπος υπηρεσίας" ("service_id") που επιθυμεί έτσι ώστε να λάβει την τιμή της συγκεκριμένης υπηρεσίας που διαθέτει ο κόμβος-εξυπηρετητής. Ο εξυπηρετητής στη συνέχεια διενεργεί αναζήτηση της ζητούμενης υπηρεσίας στο μητρώο υπηρεσιών που διαθέτει και αν η ζητούμενη υπηρεσία βρεθεί, ο εξυπηρετητής μεταδίδει ως απάντηση στον πελάτη την τιμή της συγκεκριμένης υπηρεσίας, για παράδειγμα μια τιμή θερμοκρασίας σε ένα δίκτυο WSN ή ένα αρχείο σε ένα δίκτυο MANET. Η Εικόνα 60 παρουσιάζει τα βασικά χαρακτηριστικά της εφαρμογής ελέγχου των τεχνολογιών μεσισμικού που σχεδιάσαμε και που χρησιμοποιήσαμε στις υλοποιήσεις και στα πειράματα εξομοίωσης που διεξήγαμε.

1. CLIENT sends his ID to SERVER
2. SERVER authenticates the CLIENT device:
3. if ID is valid
4. SERVER sends an ACK message to CLIENT
5. On ACK CLIENT sends a request for a SERVICE_ID
6. SERVER checks has available value for the SERVICE_ID
7. if YES
8. SERVER sends the available VALUE of the SERVICE_ID (examples: temperature, pressure, file, image, video)
9. else if NO SERVER notifies the CLIENT to try again with another SERVICE_ID

Εικόνα 60. Η ακολουθία μηνυμάτων εφαρμογής πάνω από το πρωτόκολλο ερώτησης-απόκρισης.

Κατά τη σχεδίαση της εφαρμογής ελέγχου, υιοθετήσαμε κάποια υποδείγματα σχεδιασμού λογισμικού που κρατήσαμε κοινά σε όλα τα πειράματα της εξομοίωσης που διεξήγαμε. Το πρότυπο σχεδίασης λογισμικού για τη δοκιμή μεσισμικού απεικονίζεται ως στοίβα στην Εικόνα 62 που ακολουθεί, ενώ τα επιμέρους χαρακτηριστικά περιγράφονται αμέσως παρακάτω.

- ***Ο χρόνος αντίδρασης του χρήστη***. Τον κρατάμε ελάχιστο διότι προσομοιώνουμε επικοινωνία από μηχανή-σε-μηχανή. Έτσι δεν αφήνουμε περιθώριο ώστε οι χρόνοι απόκρισης των συστημάτων να επηρεασθούν από ένα πιθανοκρατικό μοντέλο των σιωπηλών χρόνων του χρήστη.

- ***Ο εξυπηρετητής πολλαπλών νημάτων***. Μαζί με την άδεια για πρόσβαση στους πόρους του συστήματος ο έλεγχος συρροής για συμβατότητα, ολοκλήρωση και ακεραιότητα εξασφαλίζεται στο λογισμικό μέσω συγχρονισμού της πρόσβασης σε αντικείμενα κοινόχρηστης μνήμης με προκαταβολική χρονοδιάταξη. Άρα, δεν επιτρέπεται καθόλου σε δύο πελάτες να αποκτούν ταυτόχρονη πρόσβαση στα κοινά δεδομένα.

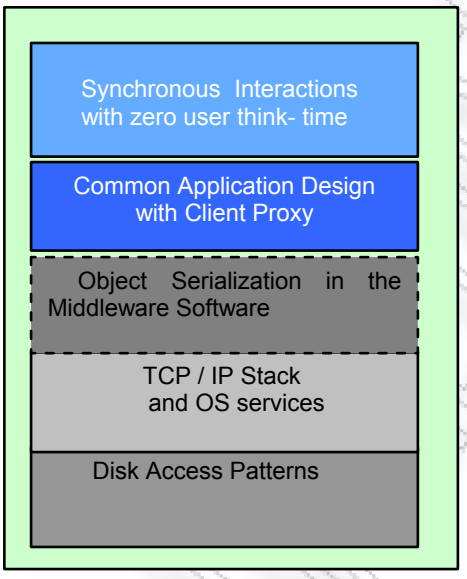
- ***Το υπόδειγμα σχεδιασμού λογισμικού*** με τη χρήση του μοντέλου στατικού μεσολαβητή ("static proxy pattern"). Πρόκειται για μια συνιστώσα λογισμικού που εγκαθίσταται στον πελάτη και η οποία μεσολαβεί στις επικοινωνίες μεταξύ του πελάτη και του εξυπηρετητή. Το λογισμικό client proxy αποφορτώνει την εφαρμογή του τελικού χρήστη αποστέλλοντας τα

μηνύματα του χρήστη σε δυαδική μορφή προς το απομακρυσμένο τελικό σημείο, σύμφωνα με τους κανόνες του σχετικού πρωτοκόλλου μεσισμικού.

- ***Ο μηχανισμός σειριοποίησης*** των αντικειμένων που χρησιμοποιείται σε Servlets, RMI και JAX-RPC για να περάσουν απομακρυσμένες αναφορές αντικειμένων στο δίκτυο. Τα δεδομένα που προέρχονται από μια σχεσιακή βάση δεδομένων ενθυλακώνονται μέσα σε πακέτα της δομής *JavaBeans valuetype*. Η σειριοποίηση αντικειμένων διευκολύνει την ανταλλαγή δομημένων και μεγάλου μεγέθους μηνυμάτων RPC, που αποστέλλονται μέσω του TCP. Το τελευταίο υλοποιεί το αναγκαίο μηχανισμό ελέγχου ροής για να εξυπηρετηθεί η λήψη του μηνύματος στο δέκτη.

- ***Το μοντέλο πρόσβασης στον δίσκο*** είναι κοινό σε όλα τα πειράματα προσομοίωσης. Ο εξυπηρετητής αποθηκεύει μόνιμα τα δεδομένα των υπηρεσιών του (service_id και τιμές σχετικές με την υπηρεσία που διαθέτει) και είναι ικανός να διαχειρίζεται μέσω συγχρονισμού των διαδικασιών ένα μεγάλο αριθμό από παράλληλα αιτήματα πρόσβασης σε εκείνα. Επίσης, ο εξυπηρετητής όντας πελάτης (client) των υπηρεσιών του Λειτουργικού Συστήματος, σχεδιάζεται έτσι ώστε να έχει μόνο μία φορά πρόσβαση στο δίσκο (ή flash memory) και με το ξεκίνημά του να φορτώνει όλα τα αναγκαία αντικείμενα και τα δεδομένα στη μνήμη του. Αυτός ο τύπος προσωρινής αποθήκευσης (caching) στη RAM υλοποιείται με ένα “Hash Table Container”. Πράγματι, μόλις εμφανισθούν τα παράλληλα αιτήματα των πελατών, η ανάγνωση των δεδομένων διενεργείται με τον ελάχιστο δυνατό αριθμό προσβάσεων στο δίσκο, διότι η συχνότητα πρόσβασης στο μόνιμο αποθηκευτικό χώρο είναι ένας κρίσιμος παράγων της επίδοσης σε συστήματα που είναι επικεντρωμένα σε δεδομένα.

- ***Οι στερούμενες δίσκου συσκευές*** του πελάτη (“disk-less clients”).



Εικόνα 61. Πρότυπο στοίβας ελέγχου πλατφόρμας μεσισμικού.

7.3. ΑΝΑΛΥΤΙΚΟ ΜΟΝΤΕΛΟ

Το κατανεμημένο σύστημά μας συνίσταται από πολλαπλούς πελάτες που σχηματίζουν μια *Poisson* ροή αιτημάτων του τύπου της εφαρμογής της Εικόνας 60 με ρυθμό άφιξης λ_s. Τα αιτήματα μοιράζονται ένα και μόνο κανάλι επικοινωνίας και ο CPU εξυπηρετητής υποτίθεται ότι αποκρίνεται με εκθετικούς χρόνους μέσου ρυθμού εξυπηρέτησης μ_s.

Επικεντρώνουμε στον χρόνο απόκρισης της εφαρμογής ελέγχου επειδή το εκλαμβάνουμε ως το πιο ενδεικτικό δεδομένο μέτρησης όσον αφορά την επίδοση και την επιβάρυνση που επιβάλλει το μεσισμικό στο χρόνο απόκρισης των εφαρμογών.

Ο χρόνος απόκρισης της κατανεμημένης εφαρμογής είναι ο χρόνος που μεσολαβεί από την υποβολή αιτήματος πελάτη για την τιμή μιας υπηρεσίας μέχρι το χρόνο όπου η απάντηση του εξυπηρετητή γίνεται δεκτή απ' τον πελάτη. Αυτό περιλαμβάνει ένα αμελητέο λανθάνοντα χρόνο καθυστέρησης για επεξεργασία στη μεριά του πελάτη, τον χρόνο μετάβασης-επιστροφής ("round-trip") επί του δικτύου T_N, συν ένα αξιόλογο χρόνο επεξεργασίας T_s που δαπανάται εντός του απομακρυσμένου τελικού σημείου εξυπηρέτησης.

Η εξίσωση (1) παριστάνει τα ανωτέρω στην περίπτωση όπου η επεξεργασία στον εξυπηρετητή είναι σύνθετη αποτελούμενη από δύο απομακρυσμένες ενέργειες-διεργασίες ("operations"):

$$T_{RT} = 2x\ (T_N+T_S). \qquad (1)$$

Ο χρόνος T_S είναι ο μέσος χρόνος αναμονής του αιτήματος: ο χρόνος δηλαδή που δαπανάται μέσα στον server εν αναμονή της εξυπηρέτησης συν το χρόνο εξυπηρέτησης που χρειάζονται οι κατανεμημένοι στο δίκτυο πόροι υλικού (κάρτα δικτύου και είσοδος-έξοδος στο δίσκο) και πόροι λογισμικού (μεσισμικό) για να εκτελέσουν τη διεργασία εξυπηρέτησης. Άρα ο συνολικός μέσος χρόνος εξυπηρέτησης μπορεί να γραφεί ως:

$$T_S = T_{(CPU + NIC + DISK IO)} + T_{middleware.} \qquad (2)$$

Αποδίδουμε την επιβάρυνση στο χρόνο εξυπηρέτησης λόγω του υλικού στις παρακάτω επιμέρους συνιστώσες: στην επεξεργαστική ισχύ της CPU, στους δίσκους και στις κάρτες δικτύου. Το $T_{middleware}$ της εξίσωσης (2) αναπαριστά τη μέση καθυστέρηση λόγω των επιμέρους στοιχείων του λογισμικού, όπως είναι τα στοιχεία που περιλαμβάνονται στο μεσισμικό που διαθέτει ο πελάτης και ο εξυπηρετητής (δηλαδή τα στοιχεία που χειρίζονται τα εισερχόμενα και εξερχόμενα μηνύματα, που συντονίζουν την ανταλλαγή μηνυμάτων, που παρακολουθούν και που ισοκατανέμουν το φορτίο στους εξυπηρετητές).

Αν δεχθούμε ότι η προσωρινή μνήμη του ενταμιευτή του εξυπηρετητή είναι απεριόριστη και ότι ο ρυθμός άφιξης λ_s είναι ανεξάρτητος από τον ήδη παρόντα στο σύστημα αριθμό αιτημάτων, μπορούμε να υιοθετήσουμε το μοντέλο ανοιχτής αναμονής M/M/1 ως ένα βασικό αναλυτικό μοντέλο για το σύστημά μας. Αυτό συνεπάγεται ότι, εφόσον παραμένει $\lambda_s<\mu_s$ ο μέσος χρόνος αναμονής είναι:

$$Ts = \frac{1}{\mu_s - \lambda_s}. \qquad (3)$$

Η εξίσωση (3) μπορεί να ξαναγραφεί ως εξής:

$$Ts = T_{s1} + T_Q, \qquad (4)$$

όπου $T_{s1} = 1/\mu_s$ είναι ο μέσος χρόνος εξυπηρέτησης που απαιτείται στη CPU για μια και μόνη συναλλαγή όταν δεν υπάρχει στο σύστημα κανένα άλλο αίτημα πελάτη και όπου T_Q:

$$T_Q = \frac{\rho}{\mu_s - \lambda_s}, \qquad (5)$$

είναι ο μέσος χρόνος καθυστέρησης, δηλ. ο μέσος χρόνος αναμονής που απαιτείται μέσα στον εξυπηρετητή πολλαπλών νημάτων δεδομένου ότι ο παράγοντας ρ της αξιοποίησης του συστήματος που δίνεται στην Εξίσωση (6) είναι μικρότερος από τη μονάδα:

$$\rho = \frac{\lambda_s}{\mu_s}. \qquad (6)$$

Το T_Q με αυτούς τους όρους αναλύει την επιβάρυνση του μεσισμικού για την κλήση και εκτέλεση της απομακρυσμένης υπηρεσίας. Η εξίσωση (5) προβλέπει ότι ο μέσος T_Q ανά αίτημα πελάτη μεταβάλλεται ασυμπτωτικά σε σχέση με το ρυθμό άφιξης αιτημάτων λ_s ή – ισοδύναμα – με τον παράγοντα χρήσης των πόρων του συστήματος ρ.

Επιπλέον, με εφαρμογή του νόμου του *Little* προκύπτει ότι σε σταθερές συνθήκες η μέση καθυστέρηση εξαρτάται απ' τον ολικό αριθμό των πελατών N που συνεμφανίζονται στο σύστημα και το ρυθμό αφίξεώς τους λ_s. Για το λόγο αυτό, αυτές οι δυο παράμετροι ήταν οι πρώτες από τις παραμέτρους χαρακτηρισμού των φορτίων αιτημάτων που επιλέχθηκαν για τα πειράματα εξομοίωσης.

Ωστόσο είναι προφανές ότι η Εξίσωση (3) αδυνατεί να αποτελέσει ένα επαρκές μοντέλο για την περιγραφή της δυναμικής συμπεριφορά των συνιστωσών του λογισμικού που αλληλεπιδρούν. Εξ άλλου, αδυνατεί φανερά να περιγράψει την εξάρτηση του μέσου χρόνου αναμονής T_Q των αιτημάτων από το μήκος του μηνύματος που ανταλλάσσεται μεταξύ των επικοινωνούντων μερών, αφού ο μέσος ρυθμός εξυπηρέτησης μ_s του κόμβου-εξυπηρετητή στην Εξίσωση (3) υποτίθεται ως σταθερός [5].

Οι μετρήσεις των προσομοιώσεων θα φανερώσουν την επίδραση που θα έχουν διαφορετικές πλατφόρμες μεσισμικού επί του χρόνου απόκρισης της εφαρμογής ελέγχου στο δίκτυο και επί της επίδοσης στη διαπερατότητα του κόμβου-εξυπηρετητή. Επιπλέον, τα πειράματα θα δείξουν ποιο είναι το επίπεδο των παράλληλων αιτημάτων για το οποίο η κάθε μια τεχνολογία μεσισμικού δίνει την καλύτερη επίδοση ως προς το χρόνο απόκρισης.

7.3.1. Περιβάλλον Εξομοίωσης

Οι Pooley και King [19] αλλά και ο Roper [20] διερεύνησαν την δυνητική χρήση των διαγραμμάτων ακολουθίας ("Message Sequence Diagrams") και των διαγραμμάτων καταστάσεως ("State Diagrams") της Ενοποιημένης Γλώσσας Μοντελοποίησης (UML, Unified Modelling Language), στην αποτίμηση της επίδοσης του κατανεμημένου λογισμικού. Συγκεκριμένα, εξέτασαν επαναλήψεις ακολουθιών μηνυμάτων και αξιοποίησαν τα προκύπτοντα ίχνη στα πειράματα προσομοίωσης. Κατέληξαν ότι η λογική διάταξη των γεγονότων καταρρέει στην περίπτωση που το λογισμικό του εξυπηρετητή κόμβου φορτώνεται με ένα πολύ μεγάλο αριθμό από παράλληλα αιτήματα. Επιπλέον, στις παραπάνω εργασίες η άμεση προσομοίωση των διαδραστικών και συνεργατικών διαγραμμάτων της UML προτείνονταν ως μια λύση για πρόβλεψη των επιδόσεων, καθώς και τα δύο προσφέρουν έγκυρα εργαλεία για την εκτίμηση και την ανάλυση της συμπεριφοράς ενός κατανεμημένου συστήματος σε λειτουργία κάτω από διαφορετικές συνθήκες φόρτωσης. Για το σκοπό αυτό στις εργασίες αυτές δημιουργήθηκαν κατάλληλες βιβλιοθήκες.

Στην δική μας μελέτη ενδιαφερόμαστε να πειραματισθούμε με πραγματικά συστήματα τόσο στην πλευρά της συσκευής και του λογισμικού του πελάτη όσο και στην πλευρά του κόμβου-εξυπηρετητή. Στόχος μας είναι η δημιουργία ενός πλαισίου ελέγχου των τεχνολογιών μεσισμικού με σημεία ελέγχου του όγκου των δεδομένων που ανταλλάσσονται μεταξύ των πελατών και των εξυπηρετητών του δικτύου. Το πλαίσιο δοκιμών θα μπορεί να δέχεται ως είσοδο τις παραμέτρους προσομοίωσης που χαρακτηρίζουν τις ποικίλες συνθήκες φορτίου και τα σενάρια χρήσης των διαθέσιμων πόρων μέσα σε ένα ζωντανό και κατανεμημένο δίκτυο. Το πλαίσιο δοκιμής θα αναπτύσσεται πάνω σε συστήματα που λειτουργούν πιλοτικά ως πρωτότυπα με σκοπό να δίνει έγκυρες και ταχείες προβλέψεις για τις επιδόσεις και τη συμπεριφορά των πραγματικών συστημάτων, προτού αυτά αναπτυχθούν σε μεγάλη κλίμακα.

Προς επίτευξη των ανωτέρω στόχων, επεκτείναμε το πακέτο προσομοίωσης Java Sim [13] το οποίο είναι κυρίως προσανατολισμένο στην προσομοίωση διεργασιών. Ακολουθώντας την λογική του Java Sim, θεωρήσαμε ότι τα παράλληλα αιτήματα για τις διαθέσιμες υπηρεσίες από τις

συσκευές πελατών προέρχονται από οντότητες που μοντελοποιούν/προσομοιώνουν τα χαρακτηριστικά των εκάστοτε πελατών και οι οποίες οντότητες επεκτείνουν τις βασικές λειτουργίες των αντικειμένων του πακέτου Java Sim. Οι οντότητες των πελατών ενεργοποιούνται στο πακέτο Java Sim από μια *Poisson* γεννήτρια αιτημάτων που υλοποιήσαμε και έρχονται σε επικοινωνία (δηλαδή ανταλλάσσουν μηνύματα) με την οντότητα του απομακρυσμένου εξυπηρετητή ως παράλληλες διαδικασίες-νήματα που καταναλώνουν τους πόρους του κόμβου-εξυπηρετητή. Σημειώνουμε ότι στα πειράματά μας ο εξυπηρετητής αναπτύχθηκε σε μια πραγματική μηχανή σε περιβάλλον Windows. Έτσι με αυτό τον τρόπο συνολικά αναπτύξαμε ένα κατανεμημένο περιβάλλον εξομοίωσης ("emulation") με δημιουργία των πελατών και με χρήση πραγματικού υλικού στην πλευρά του εξυπηρετητή ο οποίος ως προς το λογισμικό του υλοποιήθηκε σε τρείς διαφορετικές εκδοχές (Servlets, RMI, JAX-RPC).

Οι παράμετροι και οι αντίστοιχες τιμές τους που χρησιμοποιήσαμε στα πειράματα εξομοίωσης που διεξαγάγαμε για να συγκρίνουμε τις τεχνολογίες μεσισμικού διαφορετικών μοντέλων παρουσιάζονται στον Πίνακα 8. Εξομοιώσαμε τέσσερις διαφορετικές παραμέτρους (N, λ_s, L, f) και τέσσερις διαφορετικούς τύπους φορτίων-ερωτημάτων που καταφθάνουν στον κόμβο-εξυπηρετητή. Το αποτέλεσμα είναι οι τέσσερις κατακόρυφες στήλες του Πίνακα με τα αντίστοιχα "workloads" (WL_1, WL_2, WL_3 και WL_4) οι οποίες αποτελούν τις τέσσερις βασικές περιπτώσεις δοκιμών ("test cases") στα πειράματα που διεξαγάγαμε.

Όπως φαίνεται στον Πίνακα 8 στα τέσσερα διαφορετικά "workloads" που σχεδιάσαμε κλιμακώσαμε τον αριθμό των παράλληλων ερωτημάτων ανακάλυψης και επίκλησης υπηρεσίας από 10 έως 150 πελάτες οι οποίοι αναζητούν τις διαθέσιμες υπηρεσίες σε ένα δίκτυο ad hoc.

Η δεύτερη παράμετρος σε κάθε "workload" είναι ο ρυθμός άφιξης των αιτημάτων λ_s ο οποίος προσομοιώθηκε με *Poisson* ροή αιτημάτων που γεννώνται από κάθε μία πηγή (πελάτη).

Επίσης όπως έχει ήδη ειπωθεί το μέγεθος των μηνυμάτων είναι ένας παράγων που επηρεάζει το το ρυθμό εξυπηρέτησης των εξυπηρετητών μ_s. Τα μηνύματα μέσου μεγέθους αξιοποιούν αποδοτικά την διαθέσιμη ικανότητα-χωρητικότητα της CPU των κόμβων ενός MANET ή/και την υπολογιστική δυνατότητα του μικρο-επεξεργαστή ενός κόμβου αισθητήρα. Τα πιο βαριά μηνύματα επιφέρουν κορεσμό των δυνατοτήτων του υλικού σε σημείο ώστε να μην μπορούν να εξυπηρετηθούν παραπάνω μηνύματα, και να απορρίπτονται αλλεπάλληλα. Ως εμφαίνει ο Πίνακας 8 ελέγξαμε το μέγεθος του πακέτου L ως μια τρίτη παράμετρο στα πειράματα προσομοίωσης με τις τρεις διαφορετικές εκδοχές του μεσισμικού στην υλοποίηση του εξυπηρετητή στο εύρος μεταξύ 75KB-150KB.

Πέραν αυτών των κριτηρίων για το χαρακτηρισμό των φορτίων με τα αιτήματα των πελατών ενσωματώσαμε στον πειραματικό σχεδιασμό μας τον παράγοντα ασυμμετρίας *f* ως δείκτη της ασυμμετρίας μεταξύ του όγκου των δεδομένων που α) μεταβιβάζονται από τον πελάτη προς τον εξυπηρετητή και β) μεταβιβάζονται (downloaded) στην αντίστροφη κατεύθυνση, δηλαδή από το εξυπηρετητή προς τον πελάτη. Συνεπώς:

f = Όγκος δεδομένων από τον πελάτη προς τον εξυπηρετητή / Όγκος δεδομένων από τον εξυπηρετητή προς τον πελάτη. (7)

Ως γνωστό, στη διαδρομή προς τα επάνω σε ένα δίκτυο τα δεδομένα είναι αξιοσημείωτα λιγότερα σε σχέση με την ποσότητα των δεδομένων που συνήθως ο χρήστης λαμβάνει από τον εξυπηρετητή. Η ασυμμετρία εξαρτάται απ' το περιεχόμενο (ήχος, εικόνες, video) και την αντίστοιχη υπηρεσία που διατίθεται στον κόμβο-εξυπηρετητή. Με την παράμετρο *f* συνυπολογίζουμε ένα χαρακτηριστικό που κυμαίνεται από τη μια τυπική εφαρμογή στην άλλη τόσο στα δίκτυα δεδομένων όσο και στα ad hoc δίκτυα.

Μετρώντας το χρόνο απόκρισης του εξυπηρετητή όταν οι τιμές του *f* στην Εξίσωση (7)

μεταβάλλονται στο διάστημα [0,1] καλύπτουμε πολλούς δυνατούς συνδυασμούς μεγέθους μηνυμάτων που ανταλλάσσουν ο πελάτης και ο εξυπηρετητής.

Παράμετροι	WL_1	WL_2	WL_3	WL_4
Αριθμός Αιτημάτων N	*10*	*50*	*100*	*150*
Ρυθμός άφιξης αιτημάτων στον εξυπηρετητή λ_s	*2.0*	*2.25*	*2.50*	*2.75*
Μήκος Μηνύματος L	*75kB - 750kB*			
Παράγοντας Ασυμμετρίας f	*0.1 - 0.2*	*0.3 - 0.5*	*0.6 - 0.8*	*0.9 - 1*

Πίνακας 8: Παράμετροι και τιμές τεσσάρων φορτίων δοκιμής τεχνολογιών μεσισμικού.

7.4. ΑΠΟΤΕΛΕΣΜΑΤΑ ΕΞΟΜΟΙΩΣΗΣ

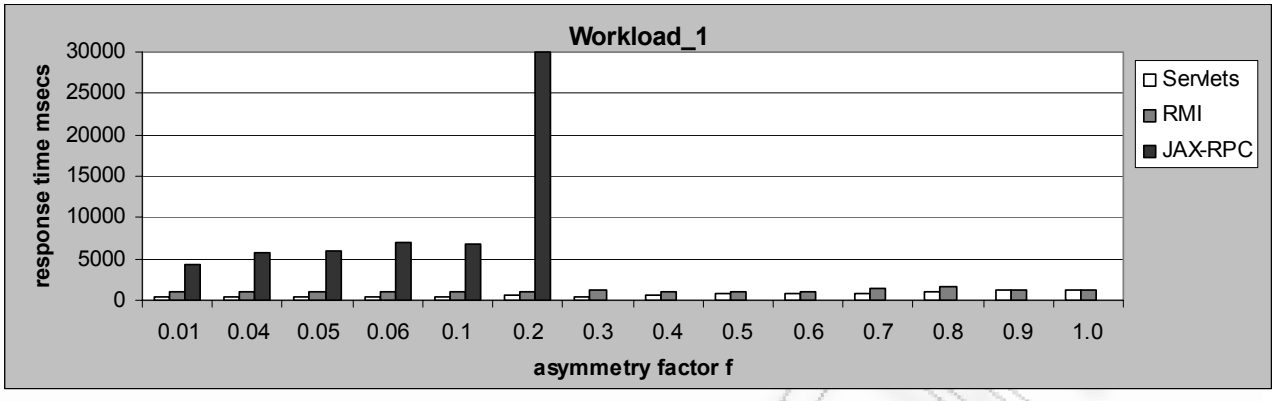
Οποιαδήποτε τιμή εικονιζόμενη ως χρόνος απόκρισης στα γραφήματα εκφράζει τον μέσο όρο των τιμών που ελήφθησαν από τρία πειράματα προσομοίωσης.

7.4.1. Περίπτωση Ελέγχου 1: WL_1

Σε περίπτωση του φορτίου Workload_1 με 10 πελάτες που μεταδίδουν αιτήματα ανακάλυψης και επίκλησης υπηρεσιών προς τον κόμβο-εξυπηρετητή η Εικόνα 62 επιδεικνύει ότι η υλοποίηση του λογισμικού εύρεσης υπηρεσιών με Servlets και επίμονες συνδέσεις διατηρεί τους χαμηλότερους χρόνους απόκρισης σε όλο το εύρος τιμών του παράγοντα *f*.

Αναλυτικότερα, για μικρού μεγέθους μηνύματα (75KB - 250KB) όπου αναμένεται οι καθυστερήσεις να εξαρτώνται από το χρόνο εγκατάστασης των συνδέσεων TCP, η εφαρμογή με τα Servlets αποκρίνεται γρηγορότερα απ' ότι το με το RMI σα μεσισμικό ανακάλυψης υπηρεσιών. Η επίδοση των δύο τεχνολογιών είναι ισοδύναμη για μεγαλύτερα μηνύματα (250KB-750KB). Στα Servlets παρατηρούμε μια μείωση της καθυστέρησης γύρω από την τιμή του *f* ίση με 0,3 και, μετά, μια μονότονη αύξηση στους χρόνους αποκρίσεως.

Οι χρόνοι RMI δείχνουν μια πρωιμότερη και μικρότερη βύθιση, συγκεκριμένα στην περιοχή τιμών του f μεταξύ [0.06 και 0.1] και ύστερα αρχίζουν και πάλι να αυξάνονται. Αξιοσημείωτο είναι ότι για υψηλές f τιμές στην περιοχή [0.9 ως 1] οι τιμές RMI δείχνουν μικρή πτώση έτσι ώστε για *f* = 1 οι χρόνοι απόκρισης των Servlets και των RMI σχεδόν συμπίπτουν για πρώτη φορά στο γράφημα.

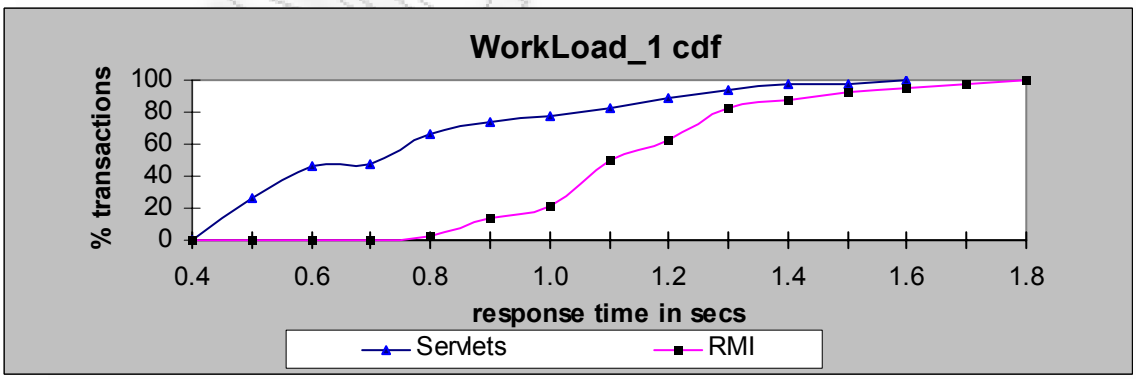


Εικόνα 62. Χρόνος απόκρισης εφαρμογής ελέγχου με χαμηλό φορτίο αιτημάτων WL_1.

Οι υπηρεσίες Web με JAX-RPC εξυπηρετούσαν στα πειράματα εξομοίωσης σχετικώς αργά το σχήμα WL_1 και έδιναν χρόνους απόκρισης δεκαπλάσιους των χρόνων των Servlets. Για μηνύματα > 150 KBytes, παρατηρήθηκε συμφόρηση στο CPU λόγω α) της επιβάρυνσης που οφείλεται στο ότι το πρωτοκόλλου SOAP δεν είναι δυαδικό αλλά αντιθέτως βασίζεται στη μετάδοση XML μηνυμάτων και β) στην επεξεργασία που αναλώνεται για την αναγκαία επεξεργασία των XML μηνυμάτων (parsing). Πράγματι, απορρίπτονταν τα επιπλέον αιτήματα, και οι χρόνοι απόκρισης ακόμη και γι' αυτό το ελαφρύ φορτίο WL_1 υπερέβαιναν τις αποδεκτές τιμές καθυστέρησης εντός των ορίων LAN (25sec -30sec).

Σημειωτέον ότι η Εικόνα 62 δείχνει ότι οι χρόνοι απόκρισης του JAX-RPC μεταβάλλονται ασυμπτωτικά σε σχέση με τον παράγοντα ασυμμετρίας *f*. Η μη γραμμική εξάρτηση του χρόνου αναμονής από το μήκος του μηνύματος συμπίπτει με την μη γραμμική εξάρτηση του χρόνου αναμονής T_s σε σχέση με το ρυθμό άφιξης λ_s, ως ήδη εξηγήσαμε περιγράφοντας το αναλυτικό μοντέλο. Στο JAX-RPC, το σημείο αστάθειας του server συνέβη γύρω στο f ίσο με 0.2.

Η Εικόνα 63 απεικονίζει την συνάρτηση συσωρευτικής κατανομής cdf ("cumulative distribution function") του χρόνου αποκρίσεως της εφαρμογής για το μεσισμικό πακέτο RMI και Servlets. Η καμπύλη JAX-RPC cdf δεν περιλαμβάνεται στην Εικόνα 63 αφού το JAX-RPC επέτυχε πολύ βραδύτερες αποκρίσεις στα αιτήματα των πελατών. Η Εικόνα 63 δείχνει ότι τα Servlets στατιστικώς είχαν καλύτερες επιδόσεις απ' το RMI στην περίπτωση ελέγχου με φορτίο , εφόσον για όλους τους χρόνους απόκρισης της εφαρμογής το ποσοστό των ερωτημάτων που εξυπηρετούνται από τα Servlets είναι μεγαλύτερο από το αντίστοιχο ποσοστό που εξυπηρετείται με το RMI σα μεσισμικό.



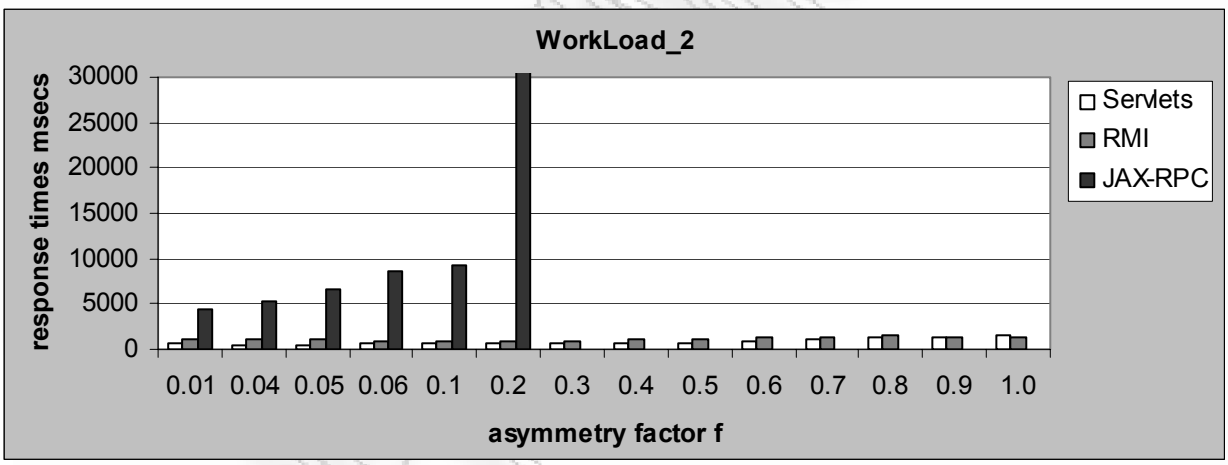
Εικόνα 63. Η cdf του χρόνου απόκρισης εφαρμογής με φορτίο WL_1.

7.4.2. Περίπτωση Ελέγχου 2: WL_2

Όπως δείχνει η παρακάτω εικόνα, το φορτίο αιτημάτων πελατών Workload_2 που δημιουργείται από 50 πελάτες-κόμβους προκαλεί μια αύξηση στους χρόνους αποκρίσεως σε όλες τις περιπτώσεις των πακέτων μεσισμικού που εξετάζουμε. Είναι αυτό μία σαφής ένδειξη ότι τα συστήματα εξυπηρέτησης πολλαπλών νημάτων που υποστηρίζονται απ' τις τεχνολογίες που εξετάζουμε αρχίζουν να υποφέρουν από την κλιμάκωση της παράλληλης φόρτωσης (στην προηγούμενη περίπτωση ελέγχου είχαμε φορτίο 10 ταυτόχρονων πελατών).

Και για τα Servlets και για τα RMI υπάρχει ένα σημείο του f (η τιμή 0.2) γύρω από το οποίο η καμπύλη χρόνων απόκρισης παίρνει κυρτό σχήμα, αποδεικνύοντας ότι, όταν αυξάνει ο όγκος των αιτημάτων και δεδομένων, οι χρόνοι αρχίζουν να υφίστανται περιορισμούς κυρίως λόγω της αύξησης στην καθυστέρηση μετάδοσης, και όχι από την καθυστέρηση για την εγκατάσταση των συνδέσεων. Παρατηρούμε ότι για συμμετρικά σενάρια χρήσης, το RMI έχει ελαφρώς καλύτερη επίδοση απ' τα Servlets, για πρώτη φορά σ' αυτά τα πειράματα.

Στην περίπτωση της XML κίνησης με το πρωτόκολλο SOAP στο σενάριο χρήσης Workload_2, η Εικόνα 64 δείχνει ότι για μικρά μεγέθη μηνύματος οι χρόνοι επίδοσης είναι πολύ κοντά στους χρόνους που επιτυγχάνει το JAX-RPC στην περίπτωση Workload_1 (Εικόνα 62). Το μέγιστο payload που η CPU μπόρεσε να εξυπηρετήσει είναι σχεδόν ίδιο με το αντίστοιχο της περίπτωσης WL_1. Στα πειράματα με αυτό το σενάριο χρήσης η CPU εξυπηρέτησε το 88% των εισερχόμενων συναλλαγών SOAP.

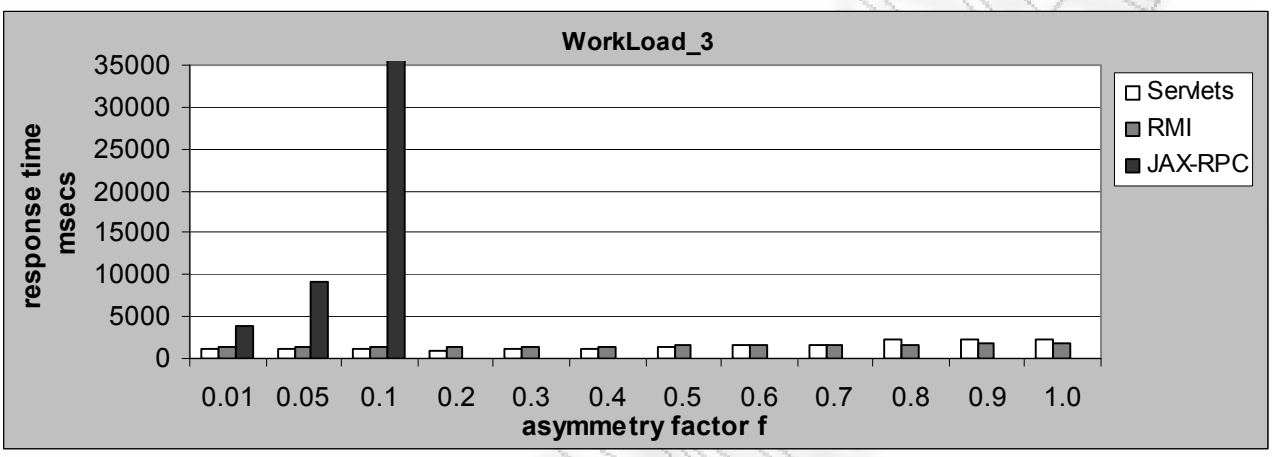


Εικόνα 64. Χρόνος απόκρισης εφαρμογής ελέγχου με φορτίο WL_2.

7.4.3. Περίπτωση Ελέγχου 3: WorkLoad_3

Προκειμένου για 100 παράλληλους πελάτες, WorkLoad_3, η Εικόνα 65 δείχνει ότι για f = 0,5 (αντιστοιχεί σε 375 KBytes προς τον κόμβο-εξυπηρετητή) οι χρόνοι των RMI και των Servlets είναι ίσοι. Για τιμές f<0,5, οι Servlets έχουν καλύτερο χρόνο από το RMI, κάτι που δείχνει ότι η προσωρινή αποθήκευση (buffering) των μηνυμάτων μικρο-μεσαίου μεγέθους παραμένει πιο αποδοτική από τους μηχανισμούς εγκατάστασης και ελέγχου των συνδέσεων που υποστηρίζονται από το RMI. Η επίδοση με Servlet υστερεί από την RMI στο β΄ μισό της περιοχής των τιμών του f. Αν και οι Servlets αυξάνουν τους χρόνους απόκρισης της εφαρμογής κατά μονοτονικό τρόπο, το RMI επιδεικνύει βελτιώσεις επιδόσεων. Οι συνδέσεις RMI φαίνονται να λειτουργούν καλύτερα στην ζώνη των μεγαλύτερων σε μέγεθος μηνυμάτων απ' ότι οι συνδέσεις HTTP. Άρα, όσα παρατηρήσαμε καταπονώντας την CPU με το φορτίο WorkLoad_1, τώρα στην περίπτωση της χρήσης του WorkLoad_3 αντιστρέφονται.

Αξιοσημείωτα, ο χρόνος απόκρισης του RMI για *f* = 1 είναι λίγο χαμηλότερος απ' ότι όταν f=0.9. Στην περίπτωση εφαρμογής με μεσισμικό JAX-RPC, στην ίδια εικόνα, η επίδοση μειώνεται βαθμιαία. Το μέγιστο εφικτό μέγεθος payload που μπορεί να φορτωθεί στον εξυπηρετητή είναι μόνο 75KB (δηλαδή έχουμε σημείο αστάθειας του server για f=0.1). Αυτό το μέγεθος μηνύματος είναι το μισό των μηνυμάτων που μπορούν να φορτώσουν οι πελάτες στα WorkLoad_1 και WorkLoad_2 σενάρια. Επίσης βλέπουμε ότι οι χρόνοι απόκρισης του JAX-RPC στις συνθήκες WorkLoad_3 πλησιάζουν αρκετά τους χρόνους που επιτεύχθηκαν κατά τα πειράματα με τις προηγούμενες συνθήκες.



Εικόνα 65. Χρόνος απόκρισης εφαρμογής ελέγχου με φορτίο αιτημάτων WorkLoad_3.

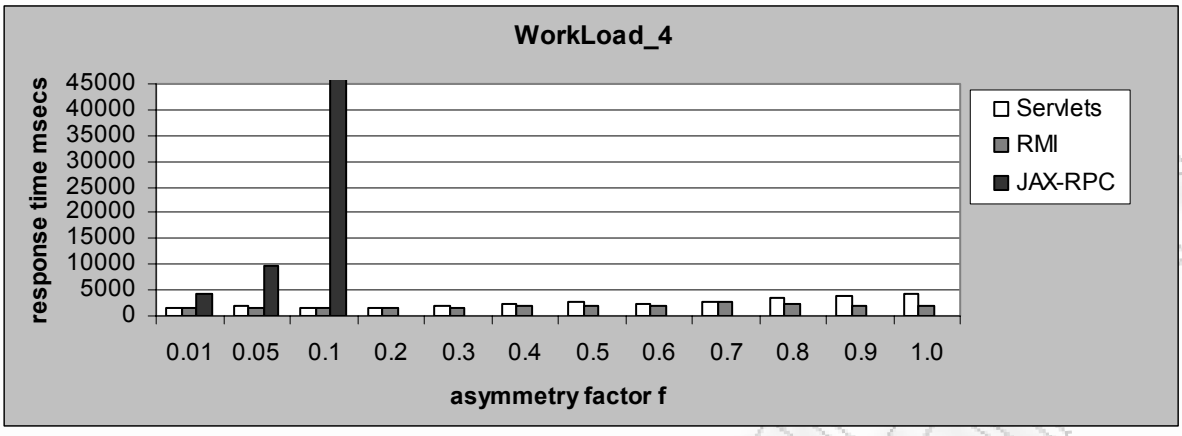
7.4.4. Περίπτωση Ελέγχου 4: WL_4

Βάσει της Εικόνας 66, όταν δοκιμάστηκε το σενάριο αιτημάτων 150 παράλληλων πελατών, WorkLoad_4, οι χρόνοι απόκρισης για Servlets και JAX-RPC είναι μεγαλύτεροι όταν συγκριθούν με τους αντίστοιχους χρόνους του φορτίου της προηγούμενης περίπτωσης WorkLoad_3.

Αξιοσημείωτο ότι, ξανά, για μικρές τιμές του συντελεστή ασυμμετρίας f<0.1, οι χρόνοι απόκρισης κυριαρχούνται από τον μηχανισμό εγκατάστασης και ελέγχου των συνδέσεων που υποστηρίζονται από την κάθε μία τεχνολογία μεισισμικού και τις καθυστερήσεις που αυτός επιφέρει. Η Εικόνα 67 δείχνει ότι με αύξηση των αιτημάτων από το σενάριο WorkLoad_3 στο WorkLoad_4 το RMI δεν εμφανίζει αισθητή μείωση στην επίδοση και εμφανώς αποδίδει καλύτερα από την υλοποίηση Servlet.

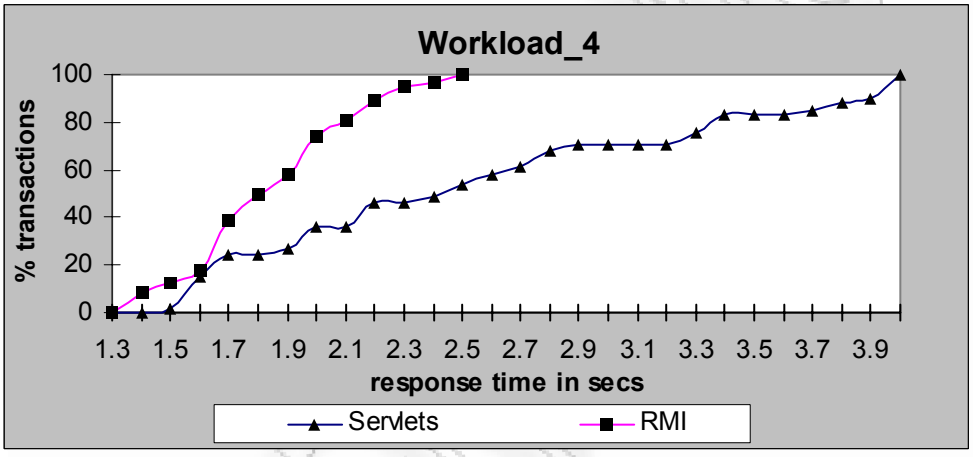
Αυτό πρωτίστως οφείλεται στο σύστημα πολλαπλών νημάτων του RMI που εξυπηρετεί ομοιόμορφα τα παράλληλα αιτήματα (το RMI κάνει χρήση "monitors" παθητικού κώδικα). Απεναντίας, οι άφθονες γεννήσεις νέων νημάτων από το σύστημα εξυπηρέτησης των Servlet δημιουργούν πρόσθετο φορτίο στο ρυθμό εξυπηρέτησης του server, ιδίως σε συνθήκες κλιμάκωσης του ανταγωνισμού για πόρους από ένα μεγάλο αριθμό από παράλληλα νήματα. Η Εικόνα 66 δείχνει ότι για μεγάλες τιμές του *f*, οπότε οι χρόνοι απόκρισης μοιραία αυξάνουν, η επιβάρυνση για την εγκατάσταση συνδέσεων αυξάνει σταθερά για το HTTP/Servlet.

Σημειωτέον ότι η χειρότερη επίδοση του RMI δεν εμφανίζεται όταν τα μεγέθη των μηνυμάτων βρίσκονται στη μέγιστη τιμή του *f*. Αυτή η τάση της τεχνολογίας RMI εκδηλώθηκε σ' όλα τα σενάρια μετάδοσης αιτημάτων που εξετάστηκαν στα πειράματα. Έτσι, συνάγουμε ότι το μεσισμικό RMI εκμεταλλεύεται το μηχανισμό διαχείρισης των συνδέσεων με διατήρηση της κατάστασης που υποστηρίζει (stateful connections), ιδίως στην περίπτωση μηνυμάτων μεγέθους άνω των 675 KB.



Εικόνα 66. Χρόνος απόκρισης εφαρμογής με φορτίο WL_4.

Η εικόνα 67 που ακολουθεί απεικονίζει τις καμπύλες των κατανομών cdf για τις δύο συγκρινόμενες τεχνολογίες, δηλαδή Servlets και RMI. Η καμπύλη των Servlets βρίσκεται τώρα κάτω απ' την καμπύλη του RMI. Επίσης, οι χρόνοι αποκρίσεως με τα Servlet δείχνουν υψηλότερη διακύμανση (χρόνοι μέχρι 4 seconds) σε σχέση με το RMI (μετρήθηκαν χρόνοι μέχρι 2.5 seconds).

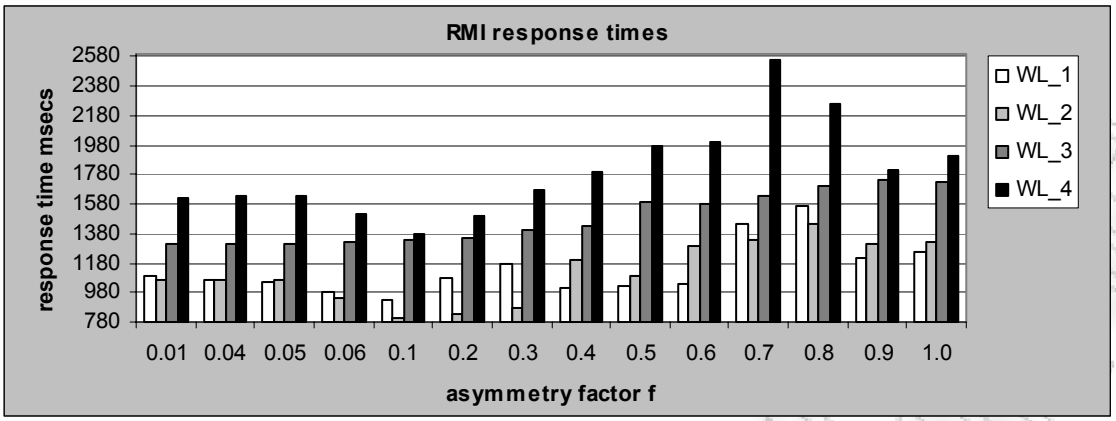


Εικόνα 67. Η cdf του χρόνου απόκρισης με φορτίο Workload_4.

Στα πειράματα, όσον αφορά τις επιδόσεις στο Workload_4, η επίδοση του JAX-RPC παρουσίασε βαθμιαία μείωση ακόμη εντονότερα σε σχέση με τα πειράματα της χρήσης WL_1. Σε αντίθεση με τα Servlets και την πλατφόρμα RMI ο JAX-RPC server υφίστατο πρόωρο κορεσμό.

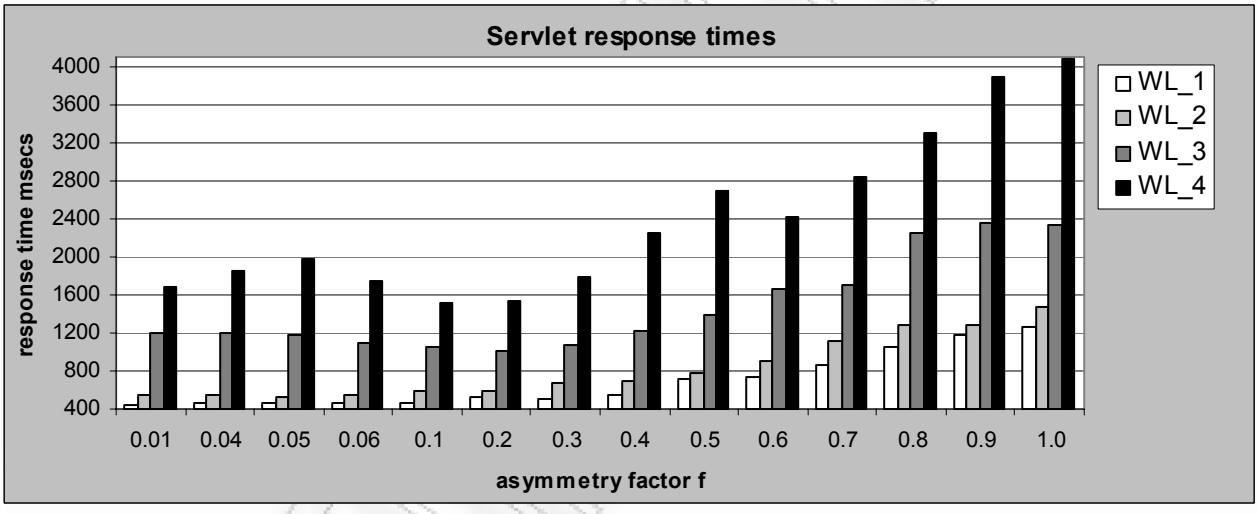
Οι Εικόνες 68 και 69 απεικονίζουν τους χρόνους RMI και των Servlets και για τα τέσσερα σενάρια άφιξης αιτημάτων στον κόμβο-εξυπηρετητή σε όλη την έκταση της περιοχής τιμών του συντελεστή *f*. Η Εικόνα 68 αποδεικνύει ότι όλα τα φορτία πελατών με την RMI υλοποίηση είχαν την εμπειρία μίας καλής επίδοσης με φραγμένο χρόνο απόκρισης ο οποίος απεικονίζεται να αυξομειώνεται με τη μεταβολή του μεγέθους των μηνυμάτων που ανταλλάχθηκαν.

Τα συγκεντρωτικά αποτελέσματα των Servlets δείχνουν ότι η υλοποίηση με τον Tomcat εξυπηρετούσε τον αύξοντα αριθμό των αιτημάτων των πελατών κατά τρόπο περισσότερο γραμμικό από ότι η υλοποίηση του εξυπηρετητή με το RMI.



Εικόνα 68. Συγκεντρωτικά αποτελέσματα του χρόνου απόκρισης με την τεχνολογία RMI.

Αναλυτικότερα, ο χρόνος απόκρισης με τα Servlet υπέστη μια βύθιση γύρω απ' την 0.2 τιμή της f και εφεξής στο πεδίο τιμών (0.2, 1) του f η απόκριση ήταν μία συνεχής αύξηση της καθυστέρησης (Εικόνα 69).



Εικόνα 69. Συγκεντρωτικά αποτελέσματα του χρόνου απόκρισης με Tomcat Servlets.

7.4.5. Συγκεντρωτικά Αποτελέσματα: Σύγκριση Διαπερατότητας

Οι κρίσιμοι πόροι που μπορούν να υποστούν συμφορήσεις - όπως ανέδειξαν τα πειράματα εξομοίωσης - ήταν η χρήση της CPU του εξυπηρετητή και η χρήση M_u της μνήμης buffer των sockets εντός της εικονικής μηχανής Java. Παρατηρήσαμε ότι για ένα δεδομένο επίπεδο παράλληλων αιτημάτων N, υπήρχε μια τιμή κατωφλίου του ρυθμού άφιξης λ_s πάνω απ' την οποία η επίδοση του εξυπηρετητή φθίνει με διαδοχικές αποτυχίες στην ολοκλήρωση των αιτημάτων για την τιμή της διαθέσιμης υπηρεσίας που καταφθάνουν. Σύμφωνα με τα σφάλματα του Java run – time system, τα αιτήματα απορρίπτονταν λόγω εξάντλησης των πόρων μνήμης του λειτουργικού συστήματος, δηλ. λόγω της υπερχείλισης του προσωρινού αποθηκευτικού χώρου ("buffering") των socket, ο οποίος είναι μεγέθους 1 MByte.

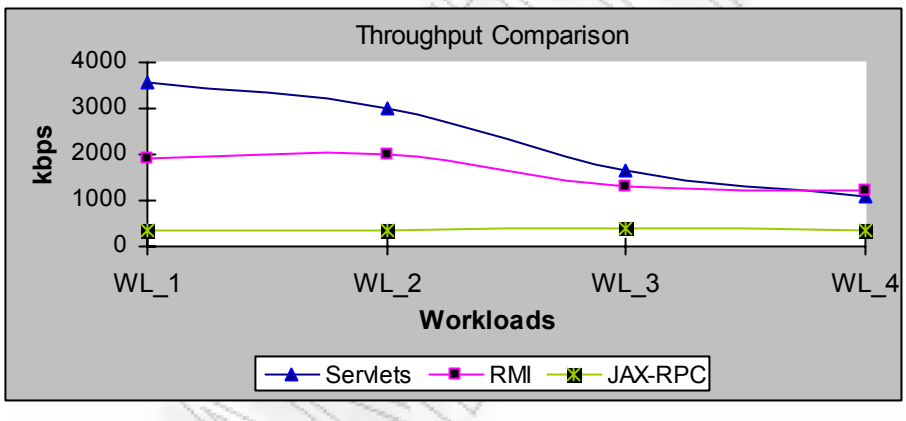
Με 2.75 εισερχόμενες συναλλαγές ανά δευτερόλεπτο, ο εξυπηρετητής μπορούσε επιτυχώς να επεξεργαστεί μηνύματα μήκους έως και 750 KB. Αυτό το μέγεθος αντιστοιχεί σε μια σελίδα HTML που περιέχει ένα ή δυο εικόνες μέσου μεγέθους. Η Εικόνα 70 απεικονίζει την επίδοση ως προς το ρυθμο-απόδοση του κόμβου εξυπηρετητή όταν αυτός υλοποιείται με τις τρείς τεχνολογίες

λογισμικού κάτω από τις συνθήκες τεσσάρων διαφορετικών φορτίων. Τα Servlets επιτύγχαναν το μέγιστο ρυθμό εξυπηρέτησης (δηλ. 3.56 Mbps) στην περίπτωση του φορτίου WL_1 και με f=0.3. Από την άλλη, το RMI έδωσε ένα μέγιστο ρυθμό 2 Mbps για την περίπτωση WL_2, για f=0.2. Άρα όπως απεικονίζεται στην Εικόνα 70 για τα τέσσερα φορτία του πειραματικού σχεδιασμού μας, επισυμβαίνει ένα μέγιστο ρυθμο-απόδοσης στον εξυπηρετητή για διαφορετικές τιμές του συντελεστή ασυμμετρίας f, ανάλογα με την εκάστοτε πλατφόρμα μεσισμικού που παρεμβάλλεται.

Ως προς τα δύο φορτία WL_3 και WL_4 η μέγιστη ικανότητα διαβίβασης των μηνυμάτων (διαπερατότητα) από το RMI εμφανίστηκε για την περίπτωση συμμετρικής ανταλλαγής μεγάλων μηνυμάτων από τον πελάτη προς τον εξυπηρετητή και αντίστροφα (f=0.9 για το WL_3 και f=1, για το WL_4).

Οι μηχανισμοί αναζήτησης υπηρεσίας μέσω της RMI απομακρυσμένης διεπαφής “Banking IF” είχε αρνητική επίπτωση επί της επιδόσης της διαπερατότητας του συστήματος για χαμηλά και μεσαία φορτία αιτημάτων. Αυτό έγινε ακόμα εμφανέστερο στην περίπτωση του μεσισμικού πακέτου JAX-RPC που χρησιμοποιούσε ένα αρχείο WDSL για να δώσει πρόσβαση στην απομακρυσμένη διεπαφή “Banking IF Port”.

Η επιβάρυνση που οφείλεται στο στρώμα της απομακρυσμένης αναφοράς (“remote reference”) που περιλαμβάνεται στις στοίβες των πρωτοκόλλων RMI και JAX-RPC δικαιολογεί γιατί τα Servlets αρχικά είχαν καλύτερες επιδόσεις από τις δύο αυτές τεχνολογίες RMI και JAX-RPC. Εντούτοις, στα υψηλά φορτία αιτημάτων ανακάλυψης υπηρεσιών, η διατήρηση κατάστασης που υποστηρίζουν τα RMI επιμέρους στρώματα (όπως το στρώμα διαχείρισης των συνδέσεων, το στρώμα χειρισμού των μηνυμάτων και το μοντέλο νημάτων του RMI) βελτίωσαν σημαντικά το χρόνο απόκρισης της εφαρμογής ελέγχου και την ικανότητα μεταβίβασης μηνυμάτων του συστήματος με το RMI. Έτσι, το σύστημα RMI έδωσε τελικά την καλύτερη επίδοση διαπερατότητας και μια τάση να υπερσκελίσει την επίδοση των Servlets, όπως απεικονίζεται στην Εικόνα 70.



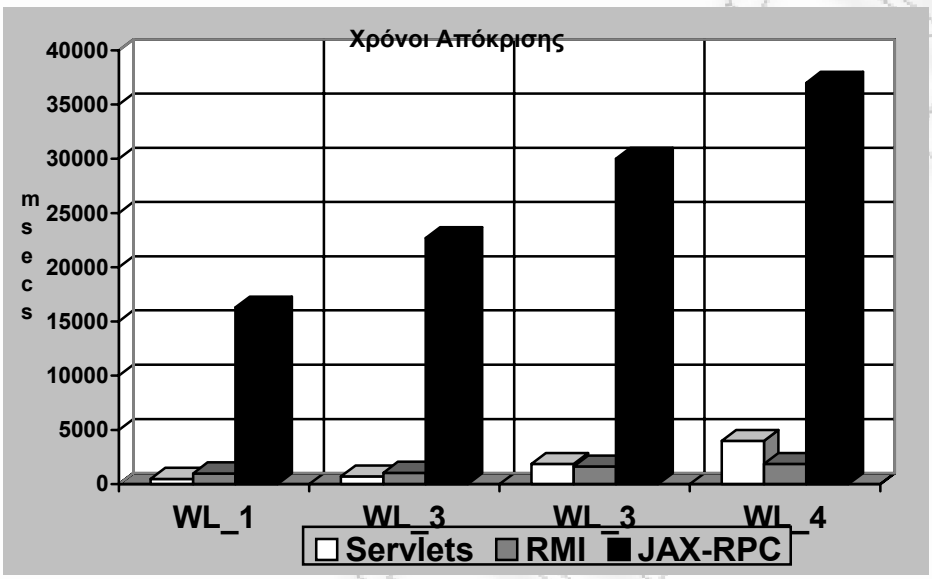
Εικόνα 70. Σύγκριση της διαπερατότητας του συστήματος με τρεις διαφορετικές τεχνολογίες μεσισμικού.

Η επίδοση της έκδοσης JAX-RPC όσον αφορά το μεσισμικό επηρεάστηκε σημαντικά από την επιβάρυνση που προέρχεται από το XML πρωτόκολλο SOAP. Η τιμή της διαπερατότητας του συστήματος με το JAX-RPC ήταν 1/10 της αντίστοιχης τιμής με τα Servlets και 5 φορές βραδύτερη από την τιμή με το RMI. Χρειάζεται λοιπόν βελτιστοποίηση των επιδόσεων του JAX-RPC και κατάλληλη προσαρμογή αυτού σε ένα δυαδικό πρωτόκολλο αντί της XML κωδικοποίησης.

7.4.6. Συγκεντρωτικά Αποτελέσματα: Σύγκριση Χρόνου Απόκρισης

Για να αναλύσουμε και να ερμηνεύσουμε ορθά τα αποτελέσματα των μετρήσεων, υπολογίσαμε το μέσο όρο των χρόνων αποκρίσεως του συστήματος σε υπο-περιοχές των τιμών του παράγοντα ασυμμετρίας *f* οι οποίες αντιστοιχούν στα παρακάτω τέσσερα φορτία αιτημάτων (workloads):

- **Workload_1**. Επιλέξαμε πειραματικά δεδομένα στην περιοχή του παράγοντα ασυμμετρίας *f* [0.1-0.2] και υπολογίσαμε τη μέση τιμή.
- **Workload_2**. Βρήκαμε τους μέσους όρους των χρόνων αποκρίσεως στην περιοχή [0.3.-0.5] του *f*.
- **Workload_3**. Εν προκειμένω, κάναμε δεκτό ότι το *f* κινείται στο διάστημα [0.6-0.8].
- **Workload_4**. Θεωρήσαμε ότι γι' αυτό το φορτίο αντιστοιχεί *f* μεταξύ των τιμών [0.9-0.10].



Εικόνα 71. Σύγκριση του χρόνου απόκρισης του συστήματος με τα τρία πακέτα μεσισμικού κάτω από τέσσερα διαφορετικά φορτία αιτημάτων.

Μια μεσοσταθμική σύγκριση των χρόνων αποκρίσεως φαίνεται στην Εικόνα 71 όπου φαίνεται ότι η υλοποίηση Servlets πέτυχε καλύτερες επιδόσεις στην περίπτωση αιτήσεων μεγέθους WL_1 και WL_2. Με βαθμιαία αύξηση των συνθηκών που επιβαρύνουν το σύστημα το πλεονέκτημα των Servlets φθίνει και οι επιδόσεις του RMI τελικά τείνουν να υπερέχουν.

Το πλεονέκτημα του RMI γίνεται εμφανέστερο σε βαρύτερα φορτία τύπου WL_4, όπου η επίδοσή του φθάνει χονδρικά στο μισό του χρόνου του Servlet.

Η Εικόνα 71 τεκμηριώνει ότι, ιδίως με όρους μεταβολής της κλίμακας του αριθμού των αιτημάτων που καταφθάνουν στον εξυπηρετητή, η RMI είναι η τεχνολογία με τα βέλτιστα αποτελέσματα μεταξύ και των τριών τεχνολογιών που ελέγχθηκαν. Το WL_3 και ιδίως το φορτίο WL_4 βρήκαν βέλτιστο χρόνο απόκρισης με το μεσισμικό RMI το οποίο είναι μια υλοποίηση του μοντέλου των κατανεμημένων και ομότιμων αντικειμένων.

Ομολογουμένως, η υλοποίηση του JAX-RPC χωρίς προσαρμογή του πρωτοκόλλου SOAP (όπως με ένα δυαδικό ή άλλης συμπίεσης / κωδικοποίησης σχήμα) στερείτο την αποδοτικότητα επίδοσης που απαιτεί το μοντέλο συγχρονιζόμενων επικοινωνιών κα κάτι τέτοιο είναι άκρως ανεπιθύμητο στο περιορισμένο δίκτυο ad hoc. Τα πειραματικά στοιχεία αποτρέπουν τις απλές ενεργοποιήσεις υπηρεσιών Web όταν ενδιαφέρει ο χρόνος (δηλ. η ταχύτητα), ιδίως αν παράγουν συμφόρηση σε συμμετρικά δεδομένα υψηλής προτεραιότητας. Έτσι, για να μην περιορίζουμε την εμβέλειά τους

μόνον σε μη-συγχρονιζόμενη μεταβίβαση πληροφοριών χαμηλής προτεραιότητας, πρέπει να επιφέρουμε κάποιου είδους προσαρμογή, π.χ. συμπίεση των δεδομένων σε συνδυασμό με ένα πρωτόκολλο μεταφοράς πολλαπλής μετάδοσης προσανατολισμένο στη ροή ("multicast streaming transport") [17] και σίγουρα θα πρέπει η υλοποίηση για τα δίκτυα ad hoc να βασίζεται στο κατάλληλο υποσύνολο του προτύπου των Web Services που έχει ειδικά αναπτυχθεί για τις συσκευές περιορισμένων δυνατοτήτων [1] καθώς και σε εργαλεία, λειτουργικές οντότητες και τεχνολογίες όπως η Java πλατφόρμα OSGi [23].

Οι υπηρεσίες του Παγκόσμιου Ιστού (Web Services) μπορούν να επιλεγούν λόγω α) της διευρυμένης δια-λειτουργικότητάς τους βάσει προδιαγραφών ("interoperability") και β) της ευελιξίας τους ως προς την ολοκλήρωση διαφορετικών συστημάτων.

7.5. ΣΥΜΠΕΡΑΣΜΑΤΑ

Τα εντατικά και εκτενή πειράματα εξομοίωσης που διεξήχθησαν έδειξαν ότι οι κατανεμημένες πλατφόρμες μεσισμικού αλλάζουν συμπεριφορά και επίδοση όταν λειτουργούν υπό διαφορετικές συνθήκες φορτίου με μεταβλητό αριθμό αιτημάτων που υποβάλλονται από τους πελάτες στους κόμβους-εξυπηρετητές. Διαπιστώσαμε ότι το αντικειμενοστρεφές κατανεμημένο μοντέλο, υπό την μορφή της τεχνολογίας Java RMI, απέδιδε ικανοποιητικά όταν κλιμακώναμε τον αριθμό και το ρυθμό άφιξης των αιτημάτων αναζήτησης των διαθέσιμων υπηρεσιών στο σύστημα με μια τάση οι χρόνοι απόκρισης που αντιλαμβάνονται οι πελάτες χρήστες/συσκευές να είναι άνω φραγμένοι.

Ερευνήσαμε τρόπους και μεθόδους με τις οποίες μπορούμε να αξιολογήσουμε "ζωντανά" κατανεμημένα συστήματα και πλατφόρμες μεσισμικού. Τα εγαλεία UML αποτελούν σημαντικό μέσο για τη συστηματική αντιμετώπιση των προβλημάτων που προκύπτουν στη μοντελοποίηση των κατανεμημένων συστημάτων αλλά και στην εκτίμηση της επίδοσής τους. Ειδικότερα, μπορούμε να εκμεταλλευτούμε τα διαγράμματα UML τόσο για την παραγωγή κώδικα με αυτόματο τρόπο όσο και για την ανάλυση των αλληλεπιδράσεων μέσα στο πραγματικό σύστημα.

Σε αυτό το πλαίσιο, μια θελκτική εναλλακτική πρόταση είναι να μεταχειρισθούμε τις διαφορετικές κατηγορίες (κλάσεις) ζήτησης υπηρεσιών ως δρώντες ("actors" στην UML) που μπορούν να κατέχουν πολλαπλούς ρόλους και να δημιουργούν χωριστές διαδρομές δραστηριοτήτων και αλληλεπιδράσεων κατά την επίκληση και την εκτέλεση της υπηρεσίας που παρέχεται από τους κόμβους του δικτύου.

7.6. ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Devices Profile for Web Services (DPWS) specification, http://schemas.xmlsoap.org/ws/2006/02/devprof/.

[2] Apache Tomcat Home Page, http://tomcat.apache.org/

[3] Bansal, V., Dalton, A., 2001. A Performance Analysis of Web Services on Wireless PDAs. CPS 214 Computer Networks, Duke University Computer Science, 2001.

[4] Chen, S., Liu, Y., Gorton, I., Liu, A., 2005. Performance prediction of component-based applications. In: The Journal of Systems and Software, pp. 35-43, vol 74, 2005.

[5] Dunlop, J., Smith, D. G., 1994. Telecommunications Engineering. Third Edition, Stanley Thornes (Publishers) Ltd, 1999, UK.

[6] European e-Business Market Watch, Europa, 2005. European Commission, Enterprise and Industry, http://ebusinesswatch.org/resources/by_sector.htm

[7] Franklin, M., Carey, J., Livny, M., 1997. Transactional Client-Server Cache Consistency: Alternatives and Performance. In: ACM Transactions on Database Systems, vol. 22(3), pp. 315-363, Sept. 1997.

[8] Gelenbe, E., (Eds.), 1999. System Performance Evaluation: Methologies and Applications. ICRC Press, Boca Raton, August 1999.

[9] Garcia-Sanchez, F., Garcia-Sanchez, A-J., Garcia-Haro, J., 2005. Performance Evaluation and Implementation Details for the CORBA A/V Stream Service for Video Communications. In: Proceeding (456) Distributed Computing and Networks, pp. 436-442, 2005.

[10] Haring, G. et al., 2000. Performance Evaluation: Origins and Directions. In: Lecture Notes in Computer Science, Volume 1769, Springer Verlag, 2000.

[11] Java WSDP download, http://java.sun.com/webservices/downloads/

[12] Java Sun's RMI page, http://java.sun.com/products/jdk/docs/guide/rmi

[13] Little, M. C., 1998. The JavaSim Home Page: http://javasim.ncl.ac.uk/.

[14] Liu, Z., Niclausse, N., Jalpa-Villanueva, C., 2001. "Traffic Model and performance evaluation of Web servers". In: Performance Evaluation Journal, pp. 77-100, 46 (2001).

[15] Menasce, D., Gomaa H., 2000. A Method for Design and Performance Modelling of Client Server Systems. In: IEEE Transactions on Software Engineering, Vol. 26, No. 11, pp. 1066-1085, November 2000.

[16] Menasce, D., 2005. "MOM vs. RPC Communication Models for Distributed Applications". In: IEEE Internet Computing Magazine, Vol. 9, No. 2, pp. 90 - 93, March/April 2005.

[17] Morse, J., Pullen, M., Tolk, A., 2004. "An Architecture for Web Services Based Interest Management in Real Time Distributed Simulation". In: Proceedings of the Eighth IEEE International Symposium on Distributed Simulation and Real-Time Applications (DS RT'04).

[18] Pancake, C. M., 1995. "The Promise and the Cost of Object Technology: A Five Year Forecast". In: Communications of the ACM, October 1995/Vol.38 No.10, pp. 33-49.

[19] Pooley, R., King, P., 1999. The Unified Modeling Language and Performance Engineering. In: IE Proceedings – Software, 146, 1, 1999.

[20] Roper, M., 2001. Testing Distributed Object Oriented Systems. Department of Computer Science, Strathclyde University, Technical Report EFoCS 40-2001.

[21] Villoldo, E. J., Serrat-Fernandez, J., 2005. "Evaluation of an Architecture Enabling Pluggable Web Services. In: Proceeding (456) Parallel and Distributed Computing and Networks, pp. 430-435, 2005.

[22] C. Tselikis, S. Mitropoulos, C. Douligeris. “An evaluation of the middleware's impact on the performance of object oriented distributed systems”, Journal of Systems and Software, Vol.80 No.7, July 2007, pp.1169-1181.

[23] OSGi Alliance, http://www.osgi.org.

[24] http://www.ietf.org/rfc/rfc4944.txt.

[25] http://www.tinyos.net.

8. ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΜΕΛΛΟΝΤΙΚΗ ΕΡΕΥΝΑ

Στη διατριβή αυτή ασχοληθήκαμε με τη μελέτη των ιδιαιτεροτήτων των δικτύων ad hoc και την εύρεση καινοτόμων μεθόδων, μοντέλων, αρχιτεκτονικών και τεχνικών λύσεων για την αποδοτική διαχείριση, οργάνωση και προστασία με ίδια μέσα από τις απειλές που εκδηλώνονται έναντι αυτών των δικτύων. Κίνητρο ήταν τα ανοιχτά προβλήματα που παραμένουν όσον αφορά την καλύτερη λειτουργία των δικτύων ad hoc αλλά και όσο αφορά την ολοκλήρωσή τους με τα δίκτυα υποδομής.

Οι συνεισφορές της διατριβής αυτής είναι οι εξής.

- Εντοπίσαμε, αναλύσαμε και διαχειριστήκαμε τους παράγοντες επίδοσης, δηλαδή εκείνους τους παράγοντες που επηρεάζουν την επίδοση των κατανεμημένων αλγορίθμων και των πρωτοκόλλων στα κινητά ασύρματα δίκτυα ad hoc και στα δίκτυα αισθητήρων. Είδαμε ότι σημαντικό ρόλο στη σχεδίαση των δικτύων ad hoc παίζουν η κίνηση των κόμβων, η ενέργειά τους, η ισχύς εκπομπής τους και τα χαρακτηριστικά της ad hoc τοπολογίας.
- Σχεδιάσαμε κατ' αρχήν ένα γενικό και σταθμισμένο αλγόριθμο συσταδοποίησης τον "Robust Re-clustering Algorithm" (RRA) που λαμβάνει υπόψη του τη διαθέσιμη ενέργεια στους ad hoc κόμβους καθώς και την τοπολογία. Εκτιμήσαμε τον αλγόριθμο αυτόν σε περιβάλλον κίνησης των κόμβων και με διαφορετικές τοποθετήσεις των κόμβων στο επίπεδο ακολουθώντας διαφορετικά μοντέλα τοπολογιών που προσομοιώσαμε με την κατάλληλη γεννήτρια τυχαίων γράφων. Διαπιστώσαμε ότι ο αλγόριθμος είναι πιο ευσταθής κάτω από δεδομένες δικτυακές συνθήκες (μεγάλη ισχύς εκπομπής), ωστόσο η συμπεριφορά του αλγορίθμου είναι διαφορετική όταν μεταβάλλονται οι τιμές των συντελεστών που χρησιμοποιεί.

  Σαν μελλοντική κατεύθυνση έρευνας θα εστιάσουμε στη βελτιστοποίηση των παραμέτρων συσταδοποίησης που χρησιμοποιούνται για τον υπολογισμό της μεταβλητής απόφασης κατά τη διαδικασία της επιλογής των κόμβων-αρχηγών. Αυτό μπορεί να επιτευχθεί με ανάλυση της ευαισθησίας των μέτρων της δικτυακής επίδοσης (όπως για παράδειγμα η ρυθμο-απόδοση του δικτύου, η διαθεσιμότητα των κόμβων και η αξιοπιστία στη μετάδοση μηνυμάτων) όταν μεταβάλλονται οι παράμετροι των αλγορίθμων και πρωτοκόλλων και ακόμη όταν μεταβάλλονται τα χαρακτηριστικά μετάδοσης στο ασύρματο μέσο όπως είναι η ισχύς εκπομπής των κόμβων.
- Ενσωματώσαμε τον αλγόριθμο RRA σε ένα σχήμα αυτο-οργάνωσης σε πλήρως κατανεμημένο ad hoc περιβάλλον. Προτείναμε ολοκληρωμένο σχήμα δρομολόγησης και δυναμικής οργάνωσης των κόμβων. Ακολουθήσαμε μια ενοποιημένη σχεδίαση πρωτοκόλλου αυτο-οργάνωσης που λαμβάνει σημαντικά υπόψη το επίπεδο της ad hoc δρομολόγησης όπως επίσης και τη θέση των κόμβων.
- Παρουσιάσαμε ένα μοντέλο αναφοράς για την αυτόνομη διαχείριση των δικτύων ad hoc. Εντάξαμε τα συνεργατικά σχήματα σε αυτό το μοντέλο ως συστήματα ανίχνευσης και αντιμετώπισης εισβολών. Το μοντέλο αναφοράς επεκτείνει ακόμη περισσότερο το σχήμα αυτο-οργάνωσης με χαρακτηριστικά πρόληψης, ανίχνευσης/πιστοποίησης και ανάκαμψης από τις επιθέσεις κόμβων που παρεισφρέουν στο ad hoc δίκτυο. Σύμφωνα με το μοντέλο αυτό υιοθετούνται συμπληρωματικές γραμμές άμυνας.
- Προτείναμε σχήμα αντιδραστικής αυτο-προστασίας που βασίζεται στην ανταλλαγή μηνυμάτων μεταξύ των κόμβων για τη λήψη ασφαλών αποφάσεων ως προς το αν κάποιος κόμβος είναι κακόβουλος ή όχι. Έτσι, στο προτεινόμενο αυτό σχήμα οι αρχηγοί εκλέγονται με συνεργατική ψηφοφορία από τους γειτονικούς κόμβους παρά απλά επιλέγονται όπως γίνεται στους συνηθισμένους αλγόριθμους ομαδοποίησης. Το ολοκληρωμένο σχήμα αυτο-οργάνωσης και προστασίας που προτείνουμε ακολουθεί τις προδιαγραφές και τις ποιότητες του μοντέλου αναφοράς (δηλαδή παρέχει ασφάλεια, ανοχή σε βλάβες, βελτιστοποίηση,

συμφωνία, αξιοπιστία, ολοκλήρωση λύσεων) και καλείται “Secure Clustered GPSR” (SC-GPSR). Το σχήμα SC-GPSR αποτελεί αναπόσπαστο μέρος του συστήματος ad hoc έτσι ώστε η ανοχή και η ασφάλεια δεν προσφέρονται από κάποια εξωτερική οντότητα αλλά ενσωματώνονται στους κόμβους του δικτύου. Το σχήμα κυρίως εστιάζει στην ανίχνευση και την αντιμετώπιση επιθέσεων που απειλούν να καταστήσουν τη λειτουργία των πρωτοκόλλων μη ορθή και μη συνεπή με σκοπό να βλάψουν το δίκτυο εκ των έσω και άρα να καταφέρουν σοβαρότερα πλήγματα. Το σχήμα αξιολογήθηκε με προσομοίωση διαφορετικών τύπων επιθέσεων και απέδειξε πολύ καλή επίδοση (ρυθμοαπόδοση και καθυστέρηση μηνύματος) ενώ ταυτόχρονα οι ανιχνευτές του κατάφεραν να ανακαλύψουν και να παρακάμψουν όλους τους επιτιθέμενους.

Το πρωτόκολλο SC-GPSR βασίζεται στο ad hoc γεωγραφικό πρωτόκολλο GPSR. Ωστόσο, η προτεινόμενη αρχιτεκτονική και οι προτεινόμενες μεθοδολογίες προστασίας από κακόβουλους κόμβους που εισβάλλουν στο δίκτυο δεν εξαρτώνται αποκλειστικά από το συγκεκριμένο πρωτόκολλο GPSR.

Το προτεινόμενο σχήμα οργάνωσης μπορεί να εφαρμοστεί πάνω από οποιοδήποτε ad hoc πρωτόκολλο -αρκεί αυτό το δίκτυο να χρησιμοποιεί περιοδικά beacons τα οποία είναι σημαντικά στη σχεδίαση που ακολουθούμε. Για παράδειγμα, το προτεινόμενο σχήμα εκλογής αρχηγών και συνεργατικής ανίχνευσης εισβολών με κατώφλια προστασίας μπορεί να εφαρμοστεί για την οργάνωση ενός δικτύου 802.15.4 ZigBee όταν αυτό χρησιμοποιεί τα σήματα beacon.

Με σωστή σχεδίαση και με διαστρωματική υλοποίηση των λύσεων που προτάθηκαν η επιβάρυνση στη μέση καθυστέρηση παράδοσης των πακέτων ήταν ελάχιστη. Περαιτέρω βελτιστοποιήσεις στα λειτουργικά τμήματα ασφάλειας του σχήματος για μικρότερη κατανάλωση των διαθέσιμων υπολογιστικών και ενεργειακών πόρων στο ad hoc δίκτυο είναι μια σημαντική κατεύθυνση της μελλοντικής εργασίας μας. Επίσης σημαντική μελλοντική έρευνα είναι η μεγαλύτερη κλιμάκωση του αριθμού και των τύπων των επιθέσεων με τις οποίες θα δοκιμαστεί το σχήμα SC-GPSR.

- Σημαντική μελλοντική κατεύθυνση έρευνας η εξέταση του πως μεταβάλλεται η επίδοση και η ευστάθεια των πρωτοκόλλων και αλγορίθμων όταν μεταβάλλονται οι εφαρμογές τελικού χρήστη και τα χαρακτηριστικά της παραγόμενης συνθετικής δικτυακής κίνησης.
- Μια άλλη σημαντική μελλοντική κατεύθυνση έρευνας είναι η διερεύνηση της δυνατότητας εφαρμογής των στατιστικών μεθόδων επεξεργασίας δεδομένων στην ασφαλή ενδο-δικτυακή επεξεργασία μέσα στους κόμβους του ad hoc δικτύου. Ενδιαφέρον παρουσιάζει να βρεθεί σε ποιες επιθέσεις οι στατιστικές μέθοδοι μπορούν να αποτελέσουν αξιόπιστο εργαλείο προστασίας και επιπλέον αξίζει να γίνει σύγκριση της επίδοσης αυτών με συνεργατικά σχήματα όπως και με υπάρχουσες (ή καινοτόμες) κρυπτογραφικές λύσεις.
- Μελετήσαμε πιθανά κατανεμημένα μοντέλα μεσισμικού του Διαδικτύου που είναι δυνατόν να αξιοποιηθούν στα δίκτυα ad hoc κατά τη διαδικασία της ανακάλυψης των διαθέσιμων υπηρεσιών από τους ομότιμους ad hoc κόμβους ή/και εξωτερικά από κόμβους και χρήστες του Διαδικτύου. Προκειμένου να διαπιστώσουμε ποια τεχνολογία μεσισμικού μπορεί να είναι πιο κατάλληλη για το σκοπό αυτό, καθορίσαμε τις προδιαγραφές για την εφαρμογή δοκιμής ως μια τυπική εφαρμογή ανεύρεσης υπηρεσίας και λήψης της τιμής αυτής που διαθέτει κόμβος εξυπηρετητή. Υλοποιήσαμε ένα κατανεμημένο πλαίσιο εξομοίωσης (“emulation”) που μπορεί να χρησιμοποιηθεί στην αξιολόγηση της επίδοσης των ad hoc κατανεμημένων και αντικειμενοστρεφών τεχνολογιών μεσισμικού.

  Παρά ταύτα, ο σκοπός της εργασίας μας δεν ήταν να κρίνει την μια εμπορική πλατφόρμα σε σχέση με τις άλλες, μια και εξαρτάται από την εφαρμογή το πόσο αξιοσύστατη είναι η μία ή η άλλη επιλογή μεσισμικού. Αντίθετα, αποβλέπουμε να δώσουμε ένα πλαίσιο ελέγχου των επιδόσεων του μεσισμικού ικανό να προσφέρει έγκυρα και αποτελεσματικά από άποψη χρόνου και κόστους, μία πρωταρχική αποτίμηση της επίδοσης των κατανεμημένων

μοντέλων και των συστημάτων και δη των αντικειμενοστραφών κατανεμημένων συστημάτων.

Η μελέτη μας όπως και οι υλοποιήσεις μας ήταν το πρώτο βήμα για την αποτίμηση των ιδιαίτερων χαρακτηριστικών των τεχνολογιών και των απαιτήσεων των δικτύων ad hoc ώστε οι μελλοντικές υλοποιήσεις να προσαρμοστούν και να βελτιωθούν ακόμη περισσότερο στο περιβάλλον των μικρών ad hoc συσκευών.

Με αυτό το δεδομένο, αποσκοπούμε να αναβαθμίσουμε περαιτέρω το πλαίσιο της εξομοίωσης που χρησιμοποιήσαμε με περαιτέρω ικανότητες όσον αφορά τη μοντελοποίηση της επίδοσης παρόμοιων συστημάτων και εφαρμογών. Σκοπεύουμε να εισάγουμε στα γνωρίσματα των αντικειμένων ιδιότητες που μπορούν να φέρουν πληροφορίες σχετικά με την επίδοση και το βαθμό αξιοποίησης των πόρων των επιμέρους συστημάτων, όπως και πληροφορίες σχετικές με την ποιότητα των υπηρεσιών (QoS) που διατίθενται.

ΠΑΡΑΡΤΗΜΑ Ι : ΠΡΟΣΟΜΟΙΩΤΗΣ JNS

Διαθέσιμος από το δεσμό http://jns.sourceforge.net/ ο Java Network Simulator (JNS) είναι ένας Discrete Event Simulator (DES) που χρησιμοποιείται στην έρευνα ρεαλιστικών δικτυακών εφαρμογών. Ουσιαστικά, πρόκειται για τη Java εκδοχή του προσομοιωτή ns-2 (διαθέσιμος από http://www.isi.edu/nsnam/ns/) η οποία ωστόσο περιέχει μικρότερο αριθμό προ-υλοποιημένων δικτυακών πρωτοκόλλων και εφαρμογών και λιγότερα χαρακτηριστικά. Για παράδειγμα, δεν περιέχεται κάποιο μοντέλο της κινητικότητας των κόμβων. Η στοίβα πρωτοκόλλων που προσομοιώνεται στον JNS περιλαμβάνει το φυσικό επίπεδο στη μετάδοση δεδομένων και τα χαρακτηριστικά διάδοσης του μέσου, το επίπεδο διασύνδεσης δεδομένων με εξομοίωση του δικτυακού προσαρμογέα και της προσωρινής μνήμης, το επίπεδο δικτύου το οποίο στέλνει πακέτα στην κατάλληλη διεπαφή, το επίπεδο μεταφοράς και τέλος το επίπεδο των εφαρμογών.

Η διαθέσιμη υλοποίηση δικτυακού πρωτοκόλλου στον JNS είναι το πρωτόκολλο IP για το οποίο η βασική υπηρεσία “datagram” παρέχεται από το στοιχείο “ip_handler”. Τα πρωτόκολλα που βρίσκονται πάνω από το επίπεδο δικτύου και τα οποία είναι υλοποιημένα στον JNS είναι τα εξής.

- Στο επίπεδο μεταφοράς (transport layer) το πρωτόκολλο TCP που βασίζεται στο πρωτόκολλο ομαδικής αναμετάδοσης SimpleGoBackN, ενώ προβλέπεται και το πρωτόκολλο UDP. Για τον JNS τα πρωτόκολλα των ανωτέρω επιπέδων ορίζονται ως πράκτορες (agents) οι οποίοι υλοποιούν τις κατάλληλες διεπαφές (interfaces) με ή και χωρίς εγκατάσταση σύνδεσης (πρωτόκολλα TCP/SGN και UDP αντίστοιχα).

- Στο επίπεδο της εφαρμογής οι πράκτορες (agents) RandomSource και RandomSink οι οποίοι τρέχουν πάνω από πρωτόκολλα με εγκατεστημένη σύνδεση (όπως τα TCP/SGN). Ο πράκτορας της πηγής RandomSource στέλνει πακέτα τυχαίου μεγέθους σε τυχαίες χρονικές στιγμές, ενώ η RandomSink στον κόμβο προορισμό ακούει σε κάποιο γνωστό αριθμό πόρτας.

Επίσης, για τον JNS υπάρχει ως επέκταση και το γραφικό εργαλείο javis 2.0, το οποίο είναι το ανάλογο του εργαλείου nam στον προσομοιωτή ns-2 και το οποίο μπορεί να χρησιμοποιηθεί για τη δυναμική αναπαράσταση των δικτύων και της δρομολόγησης των πακέτων. Τα ιδιαίτερα χαρακτηριστικά του JNS περιλαμβάνουν:

- *Πολλαπλή Εκπομπή (“multicasting”).* Υποστηρίζεται με τη JNS κλάση fake.net.MulticastSocket. Αυτή είναι μία κλάση socket που αντικαθιστά την κλάση java.net.multicast.socket του Java SDK και στέλνει μηνύματα πολλαπλής εκπομπής που χρονο-δρομολογούνται από τον προσομοιωτή JNS.

- *Επεξεργασία πολλαπλών νημάτων* (“multi-threading”). Στον προσομοιωτή JNS οι κλήσεις γίνονται με την τεχνολογία RMI η οποία υποστηρίζει τον προγραμματισμό και την επεξεργασία πολλαπλών νημάτων.

- *Δυναμικός χρονο-προγραμματισμός*. Ο δυναμικός προσομοιωτής JNS βασίζεται σε κλήσεις RMI και μετατρέπει τις δικτυακές κλήσεις που πραγματοποιούνται μέσα από προγράμματα Java σε *events* (γεγονότα) τα οποία και αποθηκεύονται σε κατάλληλη δομή δεδομένων προκειμένου να χρονο-προγραμματιστούν και να εκτελεστούν από τον προσομοιωτή JNS δυναμικά σε καθορισμένο ύστερο χρόνο. Προγραμματιστικά αυτό επιτυγχάνεται με τη χρήση και το χρονο-προγραμματισμό των κατάλληλων εντολών (“commands”) στον εξομοιωτή μέσα από τα στοιχεία (“elements”) των πρωτοκόλλων. Οι εντολές αυτές αποτελούν κλήσεις από ένα επικοινωνιακό στοιχείο που βρίσκεται υψηλότερα στη δικτυακή στοίβα πρωτοκόλλων προς ένα χαμηλότερο επικοινωνιακό στοιχείο. Αυτό διευκολύνει ώστε

να γίνονται ρεαλιστικές οι υλοποιήσεις των δικτυακών πρωτοκόλλων και των κλήσεων αυτών (“send, read, indicate, update”, κ.α.) οι οποίες διαχειρίζονται χρησιμοποιώντας τους χειριστές κλήσεων (handlers) του JNS και όχι απλά και μόνο scripts.

- *Εξομοίωση βασισμένη σε ίχνη* (“trace-driven simulation”).

```
# Trace file generated by JNS Version 1.6.
n -t * -a 0 -s 0 -S UP -v circle -c black
n -t * -a 1 -s 1 -S UP -v circle -c black
n -t * -a 2 -s 2 -S UP -v circle -c black
l -t * -s 0 -d 1 -S UP -r 10000000 -D 0.0050
l -t * -s 2 -d 1 -S UP -r 500000 -D 0.0080
+ -t 0.30000099999999996 -s 0 -d 1 -i 0 -e 36 -p sgn -a 0  -c 0
- -t 0.30100099999999996 -s 0 -d 1 -i 0 -e 36 -p sgn -a 0  -c 0
h -t 0.30100099999999996 -s 0 -d 1 -i 0 -e 36 -p sgn -a 0  -c 0
+ -t 0.30602979999999996 -s 0 -d 1 -i 0 -e 36 -p sgn -a 0  -c 0
- -t 0.30602979999999996 -s 0 -d 1 -i 0 -e 36 -p sgn -a 0  -c 0
r -t 0.30602979999999996 -s 0 -d 1 -i 0 -e 36 -p sgn -a 0  -c 0
+ -t 0.3060317999999999 -s 1 -d 2 -i 0 -e 36 -p sgn -a 0  -c 0
- -t 0.3070317999999999 -s 1 -d 2 -i 0 -e 36 -p sgn -a 0  -c 0
h -t 0.3070317999999999 -s 1 -d 2 -i 0 -e 36 -p sgn -a 0  -c 0
+ -t 0.3156077999999999 -s 1 -d 2 -i 0 -e 36 -p sgn -a 0  -c 0
- -t 0.3156077999999999 -s 1 -d 2 -i 0 -e 36 -p sgn -a 0  -c 0
r -t 0.3156077999999999 -s 1 -d 2 -i 0 -e 36 -p sgn -a 0  -c 0
+ -t 0.31560979999999983 -s 2 -d 1 -i 0 -e 36 -p sgn -a 0  -c 0
- -t 0.31660979999999983 -s 2 -d 1 -i 0 -e 36 -p sgn -a 0  -c 0
h -t 0.31660979999999983 -s 2 -d 1 -i 0 -e 36 -p sgn -a 0  -c 0
+ -t 0.32518579999999986 -s 2 -d 1 -i 0 -e 36 -p sgn -a 0  -c 0
- -t 0.32518579999999986 -s 2 -d 1 -i 0 -e 36 -p sgn -a 0  -c 0
```

Πληροφορίες σχετικές με τα “*events*” κατά τη διάρκεια της προσομοίωσης όσον αφορά το

επίπεδο διασύνδεσης και κυρίως όσον αφορά το επίπεδο πακέτου αποθηκεύονται σε αρχεία που περιέχουν τα αντίστοιχα ίχνη της δικτυακής κίνησης (traces). Όπως φαίνεται στο παραπάνω απόσπασμα αρχείου τα ίχνη δείχνουν ότι το πρωτόκολλο μεταφοράς (-p) είναι το πρωτόκολλο με σύνδεση SGN.

Για τον προσομοιωτή JNS τα αρχεία που περιέχουν τα ίχνη των πειραμάτων της προσομοίωσης είναι αντικείμενα ορισμένα σύμφωνα με το πρότυπο *javis jvs* το οποίο είναι παρεμφερές με τον τύπο αρχείων που χρησιμοποιείται στα ίχνη του εξομοιωτή *ns-2*.

Για παράδειγμα, σε ένα *jvs trace* όπως το παραπάνω ίχνος, μπορούμε να δούμε το χρόνο εξομοίωσης (“t”) κατά τον οποίον πέφτει μία ζεύξη (“l”) ή ένας κόμβος (“n”), πότε μπαίνει στην ουρά της δικτυακής κάρτας ένα πακέτο με ένα συγκεκριμένο *packet_id*, τους κόμβους πηγές (“s, sources”) και τους κόμβους προορισμούς (“d, destinations”), πότε ένα πακέτο δρομολογείται στο επόμενο βήμα (‘hop”) και άλλες δικτυακές πληροφορίες.

Επίσης, τα μηνύματα debug των εφαρμογών τελικού χρήστη μπορούν να αποθηκευτούν και αναλυθούν στα *jvs traces* ή να αποθηκευτούν σε αρχεία καταγραφής μετά από ανακατεύθυνση του *standard output*. Ενδεικτικά αναφέρουμε πώς περιγράφονται τα events μέσα στον εξομοιωτή JNS:

- *Με την Java κλάση κλάση Event*. Είναι η κλάση που αναπαριστά ένα συμβάν το οποίο χαρακτηρίζεται από ιδιότητες όπως το όνομα, το χρόνο και ένα σύνολο από παραμέτρους που περιγράφουν το συμβάν.

- *Με την Java κλάση κλάση Parameter*. Είναι η κλάση που αναπαριστά μία παράμετρο (*parameter*) της κλάσης Event. Με αυτήν συνδέουμε ένα αντικείμενο Parameter της μορφής (name, value) με ένα αντικείμενο της κλάσης *Event.*

Ο προσομοιωτής JNS χρησιμοποιήθηκε στα πειράματα που περιγράφονται στο Κεφάλαιο 5.

ΠΑΡΑΡΤΗΜΑ ΙΙ : ΠΡΟΣΟΜΟΙΩΤΗΣ J-SIM

Ο J-Sim είναι μία πλατφόρμα προσομοίωσης που βασίζεται στην αρχιτεκτονική ACA (Autonomous Component-based Architecture). Ο προσομοιωτής J-Sim είναι ένα πακέτο προσομοίωσης που κυρίως βασίζεται στις διεργασίες, δηλαδή είναι ένας process-based εξομοιωτής. Ωστόσο, υποστηρίζει και χαρακτηριστικά μοντελοποίησης και χειρισμού συμβάντων (events) οπότε πολύ εύκολα μπορεί να χρησιμοποιηθεί σαν ένας Discrete Event Simulator (DES).

Ο J-Sim διαθέτει υλοποιημένα πολλά πακέτα πρωτοκόλλων που ξεκινούν από το φυσικό επίπεδο και φτάνουν μέχρι το επίπεδο των εφαρμογών. Έτσι, κατ' αρχήν υλοποιείται η στοίβα πρωτοκόλλων του best-effort Internet με το J-Sim csl ("core service layer") που προσφέρει τις βασικές υπηρεσίες μεταγωγής πακέτου πάνω στην οποία έχουν υλοποιηθεί περαιτέρω αρχιτεκτονικές όπως η IETF differentiated services, η αρχιτεκτονική οπτικών δικτύων βασισμένη στην τεχνολογία WDM, η βασική αρχιτεκτονική των ασυρμάτων δικτύων αισθητήρων (WSN) όπως και μερικά από τα πιο γνωστά ad hoc πρωτόκολλα δρομολόγησης όπως το αντιδραστικό ad hoc AODV, το καθολικών πινάκων Routing Information Protocol DV (Distance Vector), το multicast πρωτόκολλο DVMRPv3, το IP multicast πρωτόκολλο CBT (Core Based Tree, RFC 2201), το link-state πρωτόκολλο OSPFv2 (RFC 2328), το ad hoc γεωγραφικό πρωτόκολλο GPSR (Greedy Perimeter Stateless Routing), κ.α.

Ο J-Sim έχει αναπτυχθεί σε Java ενώ ταυτόχρονα μπορεί και διαχειρίζεται τα αντικείμενα της Java μέσα από τη μεταγλώττιση scripts που μπορεί να είναι γραμμένα με Perl, Tcl, ή Python. Ο συνδυασμός αυτός (συνηθέστερα της java και των tcl scripts) είναι αρκετά ευέλικτος και αποδοτικός για τη παραμετροποίηση των μεταβλητών των πρωτοκόλλων και των αλγορίθμων καθώς και για την εξομοίωση των συνθηκών ανάπτυξης των δικτύων ad hoc (όπως το μοντέλο κίνησης, τον αριθμό κόμβων, το μοντέλο τοποθέτησης των κόμβων του δικτύου στο επίπεδο/χώρο, τα χαρακτηριστικά της ασύρματης μετάδοσης -όπως εμβέλεια, συχνότητα-, κ.α. συνθήκες). Έτσι, μπορεί να επιτευχθεί αξιόπιστη εκτίμηση της επίδοσης των προτεινόμενων δικτυακών λύσεων με πειράματα εξομοίωσης στην πλατφόρμα J-Sim.

Επιπλέον, μπορεί να χρησιμοποιηθεί για πιστοποίηση και την εκτίμηση της απόδοσης και λειτουργίας πραγματικών συστημάτων με κατάλληλες διεπαφές για "emulation". Εν συντομία, τα ιδιαίτερα χαρακτηριστικά του J-Sim είναι τα παρακάτω:

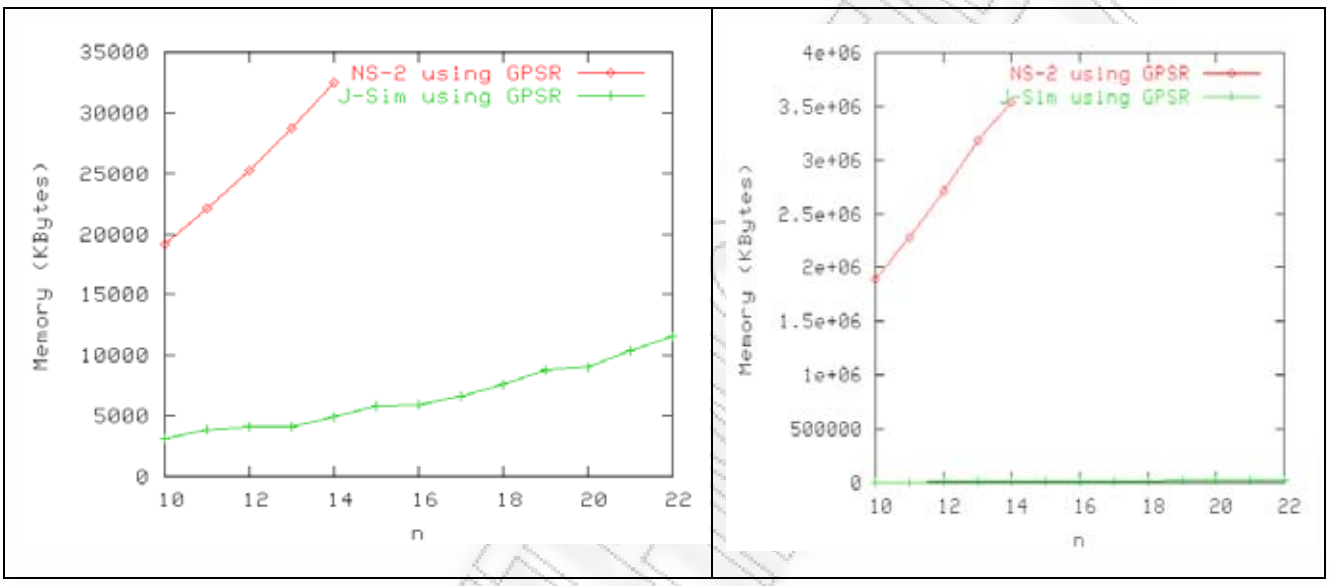
- Προγραμματιστικό μοντέλο που βασίζεται σε στοιχεία λογισμικού χαλαρώς εξαρτημένα.
- Εξομοίωση πραγματικού χρόνου βασισμένη τόσο σε διεργασίες όσο και σε γεγονότα.
- Υλοποίηση στοίβας πρωτοκόλλων του Διαδικτύου. Υποστηρίζονται πρωτόκολλα Ολοκληρωμένων, Διαφοροποιημένων και Βέλτιστης Προσπάθειας Υπηρεσιών.
- Περιβάλλον διπλής γλώσσας (Java και TCL).
- Υλοποίηση γενικευμένων κλάσεων διεπαφών.
- Μερικώς υλοποιημένη δυνατότητα για "emulation" με πραγματικά συστήματα.

Στο σχήμα (α) που ακολουθεί παρουσιάζεται μία σύγκριση της κατανάλωσης μνήμης μεταξύ του J-sim και του ns-2 όταν το πρωτόκολλο δρομολόγησης είναι το GPSR, και πριν από την εκκίνηση του πειράματος της εξομοίωσης.

Φαίνεται ότι αν συγκρίνουμε τη στατική μνήμη που δεσμεύει ο J-sim για τη δημιουργία των

απαραίτητων δομών δεδομένων που απαιτούν *n* GPSR οντότητες με την αντίστοιχη μνήμη που χρειάζεται ο ns-2, θα δούμε ότι ο J-sim χρειάζεται πολύ λιγότερη μνήμη για 10<*n*<22, ενώ επιπλέον ο ns-2 φθάνει το σημείο κορεσμού για *n*=15 κόμβους. Στο σχήμα (β) παρουσιάζεται μία σύγκριση της κατανάλωσης μνήμης μεταξύ του J-sim και του ns-2 όταν το πρωτόκολλο δρομολόγησης είναι το GPSR, μετά το τέλος του πειράματος της εξομοίωσης, δηλαδή συγκρίνεται η συνολική κατανάλωση μνήμης (στατικής και δυναμικής) κατά τη διάρκεια ενός πειράματος διάρκειας 1000 seconds.

Όπως φαίνεται στο σχήμα (β), το πλεονέκτημα του J-sim κατά τη διάρκεια του πειράματος της εξομοίωσης της δικτυακής λειτουργίας είναι ακόμη πιο έντονο.



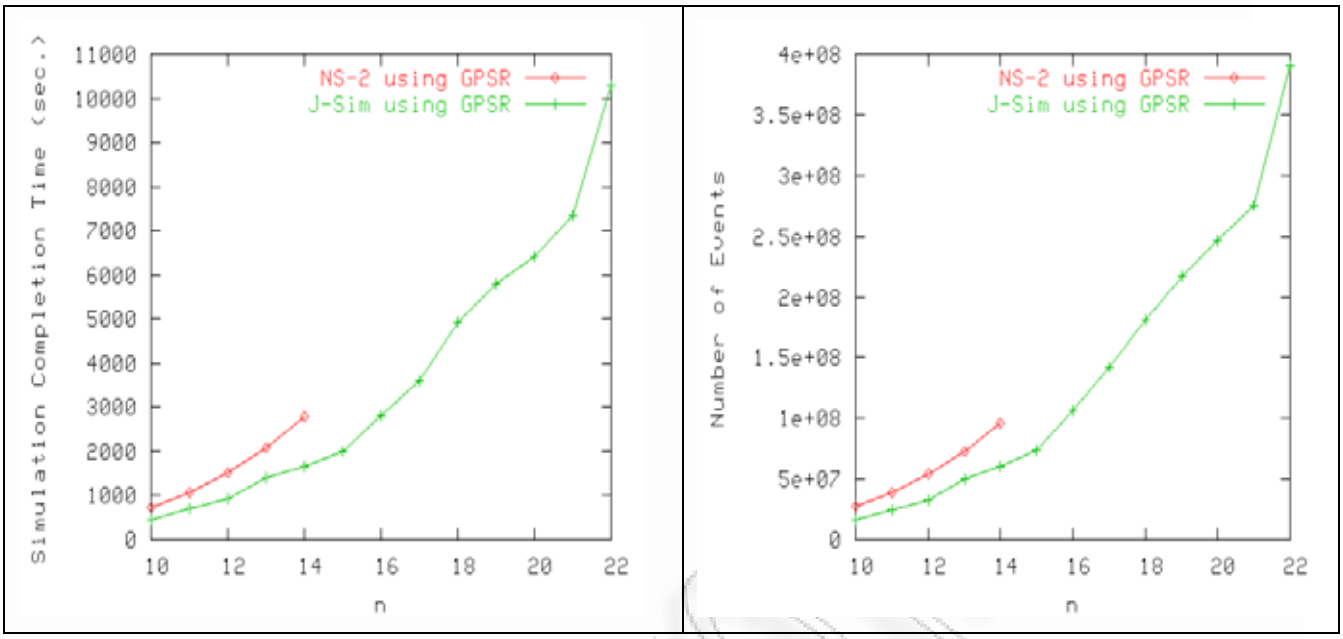
(α) **(β)**

Εικόνα 72. Σύγκριση της κατανάλωσης μνήμης από τους προσομοιωτές J-sim και ns-2.

Όσον αφορά το χρόνο εκτέλεσης του ίδιου πειράματος με το GPSR στους δύο προσομοιωτές αλλά και τον αριθμό των events που αυτοί παράγουν βλέπουμε ότι ο ns-2 αρχικά είναι πιο γρήγορος, όσον αφορά το χρόνο περάτωση του πειράματος, από τον J-sim. Αυτό όμως είναι αναμενόμενο αφού ο ns-2 είναι υλοποιημένος στην C/C++, ωστόσο το πλεονέκτημα αυτό ισχύει μόνο στις μικρές κλίμακες αφού για αριθμό κόμβων μεγαλύτερο από 14 ο ns-2 φτάνει στο σημείο κορεσμού της μνήμης. Αντίθετα, ο J-sim κλιμακώνεται πολύ ικανοποιητικά δίνοντας καλύτερη συμπεριφορά στο σύνολο.

Από τη δική μας πλευρά στα πειράματα που διεξήγαμε εκμεταλλευτήκαμε το γεγονός ότι ο J-Sim είναι κατάλληλα προσαρμοσμένος για την ανάπτυξη πλήρως κατανεμημένων αλγορίθμων που μπορούν να τρέχουν ομότιμα σε όλους τους κόμβους ενός δικτύου ad hoc. Αυτό μας διευκόλυνε στην υλοποίηση των προτεινόμενων μηχανισμών και επίσης πολύ βοηθητικό ήταν το γεγονός ότι ο J-Sim μπορεί και διατηρεί την επίδοσή του όταν ο αριθμός των κόμβων που εξομοιώνονται κλιμακώνεται. Δηλαδή, λόγω της αρχιτεκτονικής του προσομοιωτή αυτού όταν ο αριθμός των κόμβων του δικτύου αυξάνεται δεν παρατηρούνται διαρροές μνήμης και ο χρόνος των πειραμάτων δεν αυξάνεται όπως παρατηρήσαμε στις προηγούμενες Εικόνες.

Ως αποτέλεσμα αυτού του γεγονότος τα πειραματικά αποτελέσματα είναι αξιόπιστα ακόμη και για μεγάλες κλίμακες δικτύων (όπως είδαμε τα αποτελέσματα ήταν ικανοποιητικά ακόμη και για 1000 κόμβους) και για μεγάλες πυκνότητες (αριθμός κόμβων ανά μονάδα επιφανείας) δικτύων ad hoc. Κάτι τέτοιο θα ήταν πιθανώς αδύνατο με άλλους εξομοιωτές της κατηγορίας αυτής.



(α) **(β)**

Εικόνα 73. Σύγκριση του χρόνου εκτέλεσης των πειραμάτων προσομοίωσης μεταξύ των J-sim και ns-2.

Ο προσομοιωτής J-Sim χρησιμοποιήθηκε στα πειράματα που περιγράφονται στο Κεφάλαιο 6.

ΠΑΡΑΡΤΗΜΑ ΙΙΙ : ΟΡΟΛΟΓΙΑ

Παρακάτω δίνουμε μερικά από τα πιο συχνά ακρώνυμα που ο αναγνώστης θα συναντήσει στην έκταση ολοκλήρου του κειμένου.

ABK	Κλειδιά βασισμένα σε Διευθύνσεις – **A**ddress **B**ased **K**eys
AODV	**A**d-hoc **O**n-demand **D**istance **V**ector
CH	Κόμβος Αρχηγός Συστάδας – **C**luster **H**ead
CA	Αρχή Πιστοποίησης – **C**ertificate **A**uthority
DSR	**D**ynamic **S**ource **R**outing
GPSR	**G**reedy **P**erimeter **S**tateless **R**outing
IDS	Σύστημα Ανίχνευσης Εισβολών **- I**ntrusion **D**etection **S**ystem
MAC	Επίπεδο Ελέγχου Πρόσβασης στο Μέσο **- M**edium **A**ccess **C**ontrol
MANET	Κινητά Δίκτυα Ad Hoc - **M**obile **A**d Hoc **Net**works
OLSR	**O**ptimised **L**ink **S**tate **R**outing
PAN	Δίκτυα Προσωπικών Επικοινωνιών **- P**ersonal **A**rea **N**etworks
QoS	Ποιότητα Υπηρεσίας **- Q**uality **o**f **S**ervice
VANET	Ad Hoc Δίκτυα Οχημάτων **- V**ehicular **A**d Hoc **Net**works
W-DLC	Επίπεδο Ασύρματης Διασύνδεσης Δεδομένων **- W**ireless **D**ata **L**ink **C**ontrol
WLAN	Τοπικά Ασύρματα Δίκτυα – **W**ireless **L**ocal **A**rea **N**etworks
WSN	Ασύρματα Δίκτυα Αισθητήρων **- W**ireless **S**ensor **N**ode
XML	E**X**tensible **M**arkup **L**anguage