Μοντελοποίηση και Ανάλυση Επίδοσης Ασφαλών Αρχιτεκτονικών σε Περιβάλλοντα Ευφυών και Ασύρματων Δικτύων

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Ρόζα Α. Μαυροπόδη

Πανεπιστήμιο Πειραιά, Τμήμα Πληροφορικής

Πειραιάς, Ιούνιος 2009

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΙΑΤΡΙΒΗ

για την απόκτηση Διδακτορικού

Διπλώματος του Τμήματος Πληροφορικής

Ρόζας Α. Μαυροπόδη

ΜΟΝΤΕΛΟΠΟΙΗΣΗ ΚΑΙ ΑΝΑΛΥΣΗ ΕΠΙΔΟΣΗΣ ΑΣΦΑΛΩΝ ΑΡΧΙΤΕΚΤΟΝΙΚΩΝ ΣΕ ΠΕΡΙΒΑΛΛΟΝΤΑ ΕΥΦΥΩΝ ΚΑΙ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

Τριμελής Συμβουλευτική Επιτροπή :

Επιβλέπων :
Χρήστος Δουληγέρης
Καθηγητής Πανεπιστημίου Πειραιώς

Μέλη :
Θεμιστοκλής Παναγιωτόπουλος
Καθηγητής Πανεπιστημίου Πειραιώς

Δημήτριος Γκιζόπουλος
Αναπληρωτής Καθηγητής
Πανεπιστημίου Πειραιώς

Επταμελής Εξεταστική Επιτροπή :

Χρήστος Δουληγέρης
Καθηγητής Πανεπιστημίου Πειραιώς

Θεμιστοκλής Παναγιωτόπουλος
Καθηγητής Πανεπιστημίου Πειραιώς

Δημήτριος Γκιζόπουλος
Αναπληρωτής Καθηγητής
Πανεπιστημίου Πειραιώς

Ιάκωβος Βενιέρης
Καθηγητής Ε.Μ. Πολυτεχνείου

Συμεών Παπαβασιλείου
Επίκουρος Καθηγητής Ε.Μ. Πολυτεχνείου

Δέσποινα Πολέμη
Επίκουρος Καθηγήτρια
Πανεπιστημίου Πειραιώς

Δημήτριος Βέργαδος
Λέκτωρ Πανεπιστημίου Πειραιώς

ΡΟΖΑ Α. ΜΑΥΡΟΠΟΔΗ
Ειδικός Πληροφορικής τμήμα Πληροφορικής, Παν. Πειραιώς

Στον Αντώνη, που έπρεπε να ήταν εδώ.....

Περίληψη

Μια από τις σημαντικότερες προκλήσεις στη διαχείριση δικτύων μεγάλης κλίμακας αποτελεί η εισαγωγή νέων εφαρμογών. Η εισαγωγή νέων υπηρεσιών μπορεί να πραγματοποιηθεί με τη χρήση νέων ευφυών τεχνολογιών σε ήδη υπάρχουσα υποδομή, όπως τα Ευφυή Δίκτυα (Intelligent Networks) ή με τη δημιουργία μιας καθ' όλα νέας υποδομής, όπως τα Ασύρματα Κινητά Αυτο-οργανωμένα Δίκτυα (Mobile Ad Hoc). Τα δίκτυα μεγάλης κλίμακας αυτού του είδους παρουσιάζουν αυξημένες απαιτήσεις τόσο από άποψη υποστήριξης και υποδομής όσο και από άποψη ασφάλειας και αξιοπιστίας. Για να αντιμετωπιστούν τέτοιου είδους απαιτήσεις θα πρέπει να σχεδιαστούν και να εφαρμοστούν μηχανισμοί ασφάλειας που θα είναι προσαρμοσμένοι στο είδος του δικτύου που χρησιμοποιείται. Θα πρέπει να ελεγχθεί κατά πόσο οι προτεινόμενοι μηχανισμοί ασφάλειας επιβαρύνουν τη λειτουργία του δικτύου. Ανάλογα με τη φύση του υπό μελέτη συστήματος μπορούν να χρησιμοποιηθούν διάφορες τεχνικές εκτίμησης επίδοσης, όπως αναλυτικές και λιγότερο αναλυτικές.

Στην παρούσα διατριβή μελετάται, όσον αφορά τα Ευφυή Δίκτυα, μια αρχιτεκτονική ασφάλειας Ευφυών Δικτύων, η οποία εφαρμόζεται πάνω σε κατανεμημένα ευρυζωνικά Ευφυή Δίκτυα. Η εφαρμογή αποτελεί ένα συνδυασμό μηχανισμών ασφάλειας CORBA και μη - CORBA. Όσον αφορά τα κινητά δίκτυα Ad Hoc προτείνεται και παρουσιάζεται ένα ολοκληρωμένο κατ' αίτηση πρωτόκολλο δρομολόγησης πολλαπλών μονοπατιών το Secure Multipath Routing (SecMR), το οποίο παρέχει προστασία για τις επιθέσεις άρνησης υπηρεσίας ορισμένου αριθμού συνεργαζόμενων κακόβουλων κόμβων. Στη συνέχεια, πραγματοποιείται μελέτη του τρόπου με τον οποίο επηρεάζονται οι χαρακτηριστικοί παράμετροι του δικτύου, μετά την εφαρμογή αυτών των μηχανισμών ασφάλειας.

Abstract

One of the main challenges in network management of large scale networks is the introduction of new applications. This introduction may be performed with the use of new intelligent technologies applied on existing infrastructure, e.g. Intelligent Networks or with the use of totally new infrastructure, e.g. Wireless Mobile Ad Hoc Networks. Such large scale networks present increased requirements as regards their maintenance, infrastructure facilities, security and reliability. In order to meet such requirements new security mechanisms should be applied. These security mechanisms should be adjusted to the specific characteristics of the underline network. The relevant impact to the network's performance, should be taken into consideration. The performance could be evaluated with various techniques according to the nature of the underline network.

Throughout this thesis we present a secure IN architecture using application level and CORBA-based security mechanisms. Furthermore, through simulations we measure the efficiency burden imposed by the employment of the security mechanisms in the case of Interactive Multimedia Retrieval. More over, we identify several attacks that render multipath routing protocols vulnerable to collaborating malicious nodes. We propose an on-demand multipath routing protocol, the Secure Multipath Routing protocol (SecMR), and we analyze its security properties. Finally, through simulations, we evaluate the performance of the SecMR protocol in comparison with existing secure multipath routing protocols.

Ευχαριστίες

Κατά τη διάρκεια της εκπόνησης της διδακτορικής διατριβής μου ήταν πολλοί οι άνθρωποι που με στήριξαν και με βοήθησαν και προέρχονται τόσο από τον ακαδημαϊκό όσο και από το φιλικό και συγγενικό μου περιβάλλον.

Αρχικά, θα ήθελα να εκφράσω τις θερμές ευχαριστίες μου στον επιβλέποντα καθηγητή μου κ. Χρήστο Δουληγέρη, Καθηγητή Πανεπιστημίου Πειραιώς, για την ουσιαστική υποστήριξη που μου πρόσφερε τα χρόνια που διήρκεσε η προσπάθειά μου. Με τον άξιο σεβασμού χαρακτήρα του, όσο και με το επιστημονικό του υπόβαθρο έχει καταφέρει να οικοδομήσει σχέσεις εμπιστοσύνης και συνεργασίας ανάμεσα στα μέλη της επιστημονικής μας ομάδας.

Στη συνέχεια επιθυμώ να ευχαριστήσω τον κ. Θεμιστοκλή Παναγιωτόπουλο, Καθηγητή Πανεπιστημίου Πειραιώς, και τον κ. Δημήτριο Γκιζόπουλο, Αναπληρωτή Καθηγητή Πανεπιστημίου Πειραιώς, που ως μέλη της συμβουλευτικής μου επιτροπής με ενίσχυσαν καθ'όλη τη διάρκεια εκπόνησης της διατριβής μου και ήταν δίπλα μου κάθε φορά που ζήτησα τη συμβουλή τους. Ακόμα θα ήθελα να ευχαριστήσω τους κκ Ιάκωβο Βενιέρη, Καθηγητή Ε.Μ. Πολυτεχνείου, Συμεών Παπαβασιλείου, Επίκουρο Καθηγητής Ε.Μ. Πολυτεχνείου, Δημήτριο Βέργαδο, Λέκτωρ Πανεπιστημίου Πειραιώς και την κα Δέσποινα Πολέμη, Επίκουρο Καθηγήτρια Πανεπιστημίου Πειραιώς οι οποίοι με τίμησαν με τη παρουσία τους στην επταμελή εξεταστική επιτροπή της διατριβής μου.

Κατά τη διάρκεια εκπόνησης της ερευνητικής αυτής προσπάθειας είχα τη χαρά να συνεργαστώ με μια πλειάδα ανθρώπων από τους οποίους αποκόμισα πολλά οφέλη και εμπειρίες και τους θεωρώ περισσότερο φίλους παρά συνεργάτες. Έτσι επιθυμώ να ευχαριστήσω τους Γιάννη Παπαδάκη, Πάνο Κοντζανικολάου, Κατερίνα Μητροκώτσα, Αβραμίδη Αγάπιο, Δημήτρη Γλυνό, Γιάννη Ανδρέου, Έυη Κοπανάκη, Βοσινάκη Σπύρο, Βασίλη Μενεκλή, Δημήτρη Ζορμπά, Μάνο Μάγκο, Γιάννη Καλλιγάτση, Γιάννη Τασούλα, Εύη Κοπανάκη, Νίκο Αβραντινή, Γιώργο Ξενούλη και, αν με ακούει από κάπου, τον Αντώνη

Πετροπούλο. Θα ήθελα να ζητήσω προκαταβολικά από όποιον ξέχασα να συγχωρέσει την παράληψη μου.

Θέλω να ευχαριστήσω την οικογένεια μου για τη στήριξη που μου προσφέρει όλα αυτά τα χρόνια που πατάω στη γή και να εκφράσω τη λύπη μου που ο πατέρας μου, ο Αντώνης, δε ζεί αναμεσά μας ώστε να παραστεί στη χαρά μου. Τέλος ιδιαίτερες ευχαριστίες αρμόζουν στο Λευτέρη μου για την αγάπη και συμπαράσταση που έχει δείξει.

Ρόζα Μαυροπόδη

Ιούνιος 2009

Περιεχόμενα

1 Εισαγωγή **1**

1.1 Γενικά 2

1.1.1 Περιοχή Έρευνας 2

1.1.2 Ερευνητικός Στόχος 5

1.2 Αντικείμενο, Σπουδαιότητα και Προσφορά της Διατριβής 9

1.2.1 Δομή της Διατριβής 12

2 Τοπολογίες Δικτύων **13**

2.1 Ευφυή Δίκτυα 14

2.1.1 Τι είναι τα Ευφυή Δίκτυα 15

2.1.2 Κατανεμημένα Ευφυή Δίκτυα 22

2.1.3 Υπηρεσία Ανάκτησης Πολυμεσικών Δεδομένων κατά Απαίτηση 30

2.2 Δίκτυα Ad Hoc 43

2.2.1 Η Δρομολόγηση σε Δίκτυα MANET 43

2.2.2 Πρωτόκολλα Δρομολόγησης των Δικτύων MANET . . . 45

2.2.3 Επιθέσεις στα πρωτόκολλα δρομολόγησης των MANET 48

3 Μελέτη Επίδοσης και Ασφάλεια **56**

3.1 Μελέτη Επίδοσης 57

3.1.1 Μη Αναλυτικές τεχνικές μελέτης επίδοσης 60

3.1.2 Αναλυτικές τεχνικές μελέτης επίδοσης 66
3.2 Ασφάλεια 73
3.2.1 Απαιτήσεις Ασφάλειας 73
3.2.2 Είδη Επιθέσεων 77

4 Ασφαλής Κατανεμημένη Εφαρμογή σε περιβάλλοντα Ευφυών Δικτύων 86
4.1 Εισαγωγή 87
4.2 Σχετικές Ερευνητικές Εργασίες 89
4.3 Μια Ασφαλής Αρχιτεκτονική Ευφυούς Δικτύου 93
4.3.1 Επιθέσεις Ασφάλειας και Απαιτήσεις 93
4.3.2 Μηχανισμοί Ασφάλειας 95
4.3.3 Ένα μοντέλο ασφάλειας για τα DIN 101

5 Μελέτη Επίδοσης Ασφαλών Εφαρμογών σε περιβάλλοντα Ευφυών Δικτύων 112
5.1 Το μοντέλο Προσομοίωσης 113
5.1.1 Τα Σενάρια 113
5.1.2 Η Μοντελοποίηση 114
5.2 Παρουσίαση Αποτελεσμάτων 115
5.3 Σύγκριση Αποτελεσμάτων 123

6 Το Ασφαλές Πρωτόκολλο Δρομολόγησης SecMR 135
6.1 Εισαγωγή 136
6.2 Περιγραφή του πρωτοκόλλου SecMR 140
6.2.1 Πρώτη φάση - πιστοποίηση γειτονικών κόμβων 140
6.2.2 Εύρεση μονοπατιών και διαχείριση 142
6.3 Ανάλυση Ασφάλειας 153
6.3.1 Πιστοποίηση σε επίπεδο ακραίων κόμβων 153

6.3.2 Πιστοποίηση σε επίπεδο ζεύξεων 153
6.3.3 Ακεραιότητα από άκρο-σε-άκρο 155
6.3.4 Προστασία απέναντι σε συνεργαζόμενους κακόβουλους κόμβους 155

7 Μελέτη Επίδοσης Πρωτοκόλλων Δρομολόγησης στα Δίκτυα Ad Hoc **161**

7.1 Ανάλυση Επίδοσης Πρωτοκόλλων Δρομολόγησης 162
7.1.1 Μέγεθος μηνύματος 162
7.1.2 Μοντελοποίηση 167
7.1.3 Παρουσίαση Αποτελεσμάτων 172

8 Συμπεράσματα και Ανοικτά Θέματα προς Συζήτηση **182**

8.1 Συμπεράσματα και ερευνητικά Θέματα γύρω από τα DIN . . . 182
8.2 Συμπεράσματα και ερευνητικά Θέματα γύρω από τα Πρωτόκολλα Δρομολόγησης Δικτύων Ad Hoc 185

Κατάλογος Εικόνων

2.1 Εννοιολογική Ανάλυση των Υπηρεσιών ΕΔ 18
2.2 Αντιστοίχιση Φυσικών και Λειτουργικών Οντοτήτων σε ένα ΕΔ 23
2.3 Αντιστοίχιση Φυσικών και Λειτουργικών Οντοτήτων σε ένα παραδοσιακό ΕΔ 26
2.4 Αντιστοίχιση Φυσικών και Λειτουργικών Οντοτήτων σε ένα κατανεμημένο ΕΔ [4] 27
2.5 Οι Λειτουργικές Οντότητες σε ένα κατανεμημένο ΕΔ [4] 29
2.6 Γενικό διάγραμμα καταστάσεων για την υπηρεσία VoD [27] . 33
2.7 Διάγραμμα καταστάσεων επιλογής SP και video από τον χρήστη 34
2.8 Διάγραμμα καταστάσεων αναπαραγωγής video από τον χρήστη 35
2.9 Αρχιτεκτονική Κατανεμημένου Ευφυούς Δικτύου 37
2.10 Φάση 1, Βήμα 1 σηματοδοσίας [27] 39
2.11 Φάση 1, Βήμα 2 σηματοδοσίας [27] 39
2.12 Φάση 2, Βήμα 3 σηματοδοσίας [27] 40
2.13 Φάση 2, Βήμα 4 σηματοδοσίας [27] 41
2.14 Φάση 2, Βήμα 5 σηματοδοσίας [27] 41
2.15 Φάση 2, Βήμα 6 σηματοδοσίας [27] 42

3.1 Μέθοδος μελέτης επίδοσης της Παρατήρηση 61

4.1 Το DIN βασισμένο σε CORBA και MAT [4]. 91
4.2 Ασφαλής Λειτουργική Αρχιτεκτονική 102

4.3 Μια ασφαλής αρχιτεκτονική DIN [24]. 105

5.1 Το μοντέλο προσομοίωσης. 116
5.2 Ασφαλής ροή πληροφορίας (σύνδεση του χρήστη στην οντότητα B-SRF). 117
5.3 Μέση καθυστέρηση IMR. 118
5.4 Καθυστέρηση στον τερματικό κόμβο (TE). 119
5.5 Μέση καθυστέρηση στον κόμβο B-SSCP. 120
5.6 Μέση καθυστέρηση στον κόμβο B-SEN. 121
5.7 Σύγκριση των κόμβων B-SEN και B-SSCP αναφορικά με τη καθυστέρηση (έλεγχος στον B-SEN). 121
5.8 Σύγκριση των κόμβων B-SEN και B-SSCP αναφορικά με τη καθυστέρηση (έλεγχος στον B-SSCP). 122
5.9 Μέση καθυστέρηση IMR με μέγεθος πακέτου 10000 bit. 124
5.10 Μέση καθυστέρηση IMR με μέγεθος πακέτου 40000 bit. 124
5.11 Κατανομή Λειτουργικών οντοτήτων σε Φυσικούς κόμβους στο Ευφυές Δίκτυο. 125
5.12 Διαφορετικά σενάρια-θέσεις εκτέλεσης της λογικής της υπηρεσίας (SLP) (α- αρι.) Σενάριο 1: Ο Έλεγχος της Υπηρεσίας στον κόμβο B-SEN. (β-δεξιά) Σενάριο 2: Ο Έλεγχος της Υπηρεσίας στον κόμβο B-SSCP 126
5.13 Μέση καθυστέρηση IMR. 127
5.14 Μέση καθυστέρηση σε κάθε φυσικό κόμβο με μέσο μέγεθος πακέτου στα 40000 bit για το σενάριο α. 128
5.15 Μέση καθυστέρηση σε κάθε φυσικό κόμβο με μέσο μέγεθος πακέτου στα 40000 bit για το σενάριο β. 128
5.16 Μέση καθυστέρηση στο φυσικό κόμβο B-SSCP με μέσο μέγεθος πακέτου 40000 bit και για τα δύο σενάρια. 129

5.17 Μέση καθυστέρηση στο φυσικό κόμβο B-SEN με μέσο μέγεθος πακέτου 40000 bit και για τα δύο σενάρια. 129
5.18 Μέση καθυστέρηση της όλης υπηρεσάις IMR με μέσο μέγεθος πακέτου 40000 bit και για τα δύο σενάρια και ύπαρξη τηλεφωνικών κλήσεων. 130
5.19 Μέση καθυστέρηση στο φυσικό κόμβο B-SSCP με μέσο μέγεθος πακέτου 40000 bit και για τα δύο σενάρια και ύπαρξη τηλεφωνικών κλήσεων. 131
5.20 Μέση καθυστέρηση στο φυσικό κόμβο B-SEN με μέσο μέγεθος πακέτου 40000 bit και για τα δύο σενάρια και ύπαρξη τηλεφωνικών κλήσεων. 131
5.21 Μέση καθυστέρηση στους φυσικούς κόμβους B-SEN και B-SSCP με μέσο μέγεθος πακέτου 40000 bit, για το σενάριο β, σε σχέση με το ρυθμός μετάδοσης δεδομένων. 132

6.1 Ο αλγόριθμος εύρεσης νέων μονοπατιών στον αρχικό κόμβο . . 145
6.2 Ο αλγόριθμός εύρεσης νέων μονοπατιών στον ενδιάμεσο κόμβο 147
6.3 Διασπορά του μηνύματος εύρεσης νέων μονοπατιών 149

7.1 Δίκτυο που παράγει *ExcludeList* με μέγιστο μέγεθος 163
7.2 Μέση καθυστέρηση από άκρο-σε-άκρο πακέτων δεδομένων ανά μεσοδιάστημα παραγωγής πακέτων 172
7.3 Μέση καθυστέρηση από άκρο-σε-άκρο πακέτων δεδομένων ανά χρόνο στάθμευσης 173
7.4 Ποσοστό απόρριψης πακέτων δεδομένων ανά μεσοδιάστημα παραγωγής πακέτων 174
7.5 Ποσοστό απόρριψης πακέτων δεδομένων ανά χρόνο στάθμευσης 175
7.6 Ο αριθμός των πακέτων δεδομένων που έχουν παραδοθεί ορθά ανά μεσοδιάστημα παραγωγής πακέτων δεδομένων 176

7.7 Ο αριθμός των πακέτων δεδομένων που έχουν παραδοθεί ορθά ανά χρόνο στάσης 177
7.8 Χρόνος διάδοσης ανά χρόνο στάσης 178
7.9 Πρώτη εύρεση προορισμού ανά χρόνο στάσης 178
7.10 Παραγωγή πακέτων ελέγχου ανά χρόνο στάσης 180

Κατάλογος Πινάκων

3.1 Σύγκριση Τεχνικών Μελέτης Επίδοσης - Ιδιότητες ασφάλειας . . 57
3.2 Τυπικές Μέθοδοι Μελέτης Επίδοσης Πρωτοκόλλων[7] 72

4.1 Η δομή ενός PAC. 98
4.2 Πακέτα ασφάλειας CORBA, μηχανισμοί και οι εξαρτήσεις τους. . 99

6.1 Σύγκριση Πρωτοκόλλων 156

7.1 Σύγκριση Πρωτοκόλλων - Μέγεθος Λίστας 165
7.2 Σύγκριση Πρωτοκόλλων - Μέγεθος λίστας έως 5 μέλη 166

Κεφάλαιο 1

Εισαγωγή

Όλο και περισσότεροι άνθρωποι ανά τον κόσμο έχουν πρόσβαση σε κάποιον υπολογιστή και, μέσω αυτού, τη δυνατότητα πρόσβασης στην πληροφορία. Όσο αυξάνεται η χρήση αυτή, τόσο αυξάνονται και οι προκλήσεις ασφάλειας που θα πρέπει να αντιμετωπισθούν. Οι προκλήσεις αυτές δεν είναι απαραίτητο να προέρχονται από την κακόβουλη χρήση του μέσου αλλά και από το ασταθές περιβάλλον λειτουργίας. Παρά το γεγονός ότι το κόστος κτήσης μιας υπολογιστικής μηχανής έχει κατά πολύ μειωθεί, εντούτοις εξακολουθούν να παρουσιάζονται περιορισμοί στη λειτουργία εξυπηρέτησης εφαρμογών. Αυτό γίνεται κυρίως λόγω του γεγονότος ότι οι σύγχρονες εφαρμογές παρουσιάζουν όλο και μεγαλύτερες ανάγκες σε συστημικούς πόρους, όπως, π.χ. υπολογιστική ισχύ, αποθηκευτικό χώρο κ.α. Το πρόβλημα γίνεται εντονότερο όταν αυτές οι εφαρμογές απαιτούν τη χρήση κάποιου είδους δικτύου. Η ανάγκη της αγοράς για παροχή νέων, πολυπλοκότερων εφαρμογών, αλλά και για προσέγγιση νέων πελατών, αναγκάζει την επιστήμη να βρει τρόπους εξυπηρέτησης αυτών των απαιτήσεων. Μια λύση για την ικανοποίηση αυτών των απαιτήσεων, τουλάχιστον όσον αφορά το δίκτυο, είναι η χρήση νέων ευφυών τεχνολογιών (π.χ. κινητών πρακτόρων, CORBA)[1] σε ήδη υπάρχουσα

[1] Common Object Request Broker Architecture

υποδομή (π.χ. PSTN)[2], ή η δημιουργία μιας καθ' όλα νέας υποδομής (π.χ. ασύρματα, κινητά, ειδικά (ad hoc) δίκτυα). Σε αυτήν τη περίπτωση αυξάνονται οι προκλήσεις, πρώτον όσον αφορά τους περιορισμούς λειτουργίας ανάλογα με το είδος του δικτύου, και δεύτερον όσον αφορά τις απαιτήσεις ασφάλειας. Έτσι, θα πρέπει να αντιμετωπισθούν περιορισμοί όπως: το ασταθές κανάλι επικοινωνίας, η ύπαρξη τυχόν αδυναμιών στα σημεία εγκατάστασης νέων τεχνολογιών σε παλιά υποδομή, η ταχύτητα μετάδοσης δεδομένων, η κατανάλωση ενέργειας κ.α. Λαμβάνοντας υπόψη αυτούς τους περιορισμούς θα πρέπει να σχεδιαστούν και να εφαρμοστούν μηχανισμοί οι οποίοι μπορεί να βασίζονται σε ήδη υπάρχουσες τεχνικές ασφάλειας, αλλά θα είναι προσαρμοσμένοι στο είδος του δικτύου που χρησιμοποιείται. Θα πρέπει να ελεγχθεί κατά πόσο οι προτεινόμενοι μηχανισμοί ασφάλειας επιβαρύνουν τη λειτουργία του δικτύου. Ανάλογα με τη φύση του υπό μελέτη συστήματος μπορούν να χρησιμοποιηθούν διάφορες τεχνικές εκτίμησης επίδοσης, όπως αναλυτικές και λιγότερο αναλυτικές.

Το κεφάλαιο αυτό, παρουσιάζει τον επιστημονικό χώρο στον οποίο έχει κινηθεί η έρευνά μας και καταδεικνύει το ζητούμενο ερευνητικό στόχο. Στη συνέχεια γίνεται μια σύντομη επισήμανση στο αντικείμενο που πραγματεύεται αυτή η διατριβή, καθώς και στα οφέλη που προκύπτουν. Τέλος παρουσιάζονται η δομή και η οργάνωση των κεφαλαίων που ακολουθούν.

1.1 Γενικά

1.1.1 Περιοχή Έρευνας

Η συνεχώς αυξανόμενη ζήτηση που υπάρχει για υπηρεσίες πολυμεσικών δεδομένων έχει κυριαρχήσει και στην εξέλιξη της τεχνολογίας των δικτύων. Τα δίκτυα πρέπει να παρέχουν ικανοποιητικό εύρος ζώνης, αποδοτικούς μηχανι-

[2]Public Switched Telephone Network

σμούς ελέγχου, αξιόπιστη δρομολόγηση και όλα αυτά δεδομένων των περιορισμών που πάντα υπάρχουν στα τεχνικά χαρακτηριστικά των υπολογιστικών μηχανών, π.χ. σε ισχύ, ενέργεια. Για την ικανοποίηση αυτών των αναγκών στη διατριβή αυτή έχουν χρησιμοποιηθεί τα Ευφυή Δίκτυα (Intelligent Networks - IN)[3] και τα Ειδικά δίκτυα (Ad Hoc)[4]. Για να επιτευχθεί η γρήγορη και με χαμηλό κόστος παροχή νέων υπηρεσιών προς το χρήστη, τα μεν πρώτα εκμεταλλεύονται την ήδη υπάρχουσα υποδομή του δημόσιου τηλεφωνικού δικτύου (PSTN) σε συνδυασμό με πιο εξελιγμένες τεχνολογίες, όπως αυτή των κινητών πρακτόρων (Mobile Agent Technology - MAT) και της κατανεμημένης πλατφόρμας CORBA, τα δε δεύτερα, δηλαδή τα Ad Hoc, εκμεταλλεύονται την παντελή έλλειψη οποιασδήποτε υποδομής.

Η έννοια των Ευφυών δικτύων βασίζεται στην ιδέα της παροχής πολύπλοκων πολυμεσικών, συνήθως, εφαρμογών με τη χρήση ενός λιγότερο πολύπλοκου συστήματος σηματοδοσίας. Στα δίκτυα αυτά διαχωρίζεται η λογική της υπηρεσίας από τον έλεγχο της κλήσης, επιτρέποντας έτσι την ταχεία και με χαμηλό, σχετικά, κόστος εισαγωγή νέων υπηρεσιών. Η υλοποίηση της λογικής της υπηρεσίας (SLP - Service Logic Programs) σε κινητούς πράκτορες και η κατάλληλη τροποποίηση ορισμένων στοιχείων (B-SSCP- Broadband-Service Switching and Control Point) του δικτύου, έτσι ώστε να μπορούν να φιλοξενούν και να εκτελούν αυτά τα προγράμματα, έκανε την διαδικασία των νέων υπηρεσιών ανεξάρτητη από τον παροχέα της αλλά και από το ίδιο το δίκτυο. Η λογική της υπηρεσίας μπορεί να μεταναστεύει πλησιέστερα στο χρήστη ανάλογα με τη ζήτηση που υπάρχει, ώστε να αποφεύγεται τυχόν συμφόρηση στους κόμβους. Το ιδιαίτερο της τεχνικής αυτής είναι ότι αυτοί οι κόμβοι δεν αποτελούν απλώς κινητά τμήματα κώδικα αλλά όταν μεταναστεύουν, μεταφέρουν και τα δεδομένα που χρειάζονται. Η χρήση κατανεμημένων τεχνολογιών

[3]στη συνέχεια της διατριβής οι χρησιμοποιούμενοι όροι: Ευφυή Δίκτυα, ΕΔ και ο λατινικός όρος IN, θα θεωρούνται ισοδύναμοι

[4]καθ' ολη τη συνέχεια της διατριβής θα χρησιμοποιείται ο λατινικός όρος

όπως της CORBA έκανε δυνατή την εξυπηρέτηση τέτοιου είδους εφαρμογών ανεξαρτήτως της δικτυακής υποδομής. Μια δημοφιλής υπηρεσία των δικτύων αυτών που εκμεταλλεύεται πλήρως τα χαρακτηριστικά τους αποτελεί η Αλληλεπιδραστική Ανάκτηση Πολυμεσικών Δεδομένων (Interactive Multimedia Retrieval - IMR), η οποία παρέχει πολυμεσικά δεδομένα σε κατάλληλα εγγεγραμμένους χρήστες.

Αντίθετα, τα δίκτυα Ad Hoc αποτελούν ένα σύνολο από ασύρματους κινητούς κόμβους, καθένας από τους οποίους μπορεί να λειτουργεί ως πηγή παραγωγής δεδομένων, ως ενδιάμεσος κόμβος ή ως προορισμός. Οι κόμβοι σε ένα τέτοιο δίκτυο επικοινωνούν άμεσα μεταξύ τους όταν βρίσκονται εντός της περιοχής κάλυψης του ασύρματου σήματός τους. Για την επικοινωνία με κόμβους που βρίσκονται εκτός αυτής της περιοχής θα πρέπει ο κάθε κόμβος να βασιστεί στους γειτονικούς του για την προώθηση των μηνυμάτων του. Κατά τη διάρκεια αυτής της διαδικασίας ο κάθε κόμβος μπορεί να λειτουργήσει ως δρομολογητής εκτελώντας ένα κατάλληλο πρωτόκολλο δρομολόγησης. Τα δίκτυα Ad Hoc βρήκαν ιδιαίτερη απήχηση σε στρατιωτικές εφαρμογές και σε καταστάσεις εκτάκτου ανάγκης, όπου η έλλειψη υποδομής είναι δεδομένη.

Όπως γίνεται φανερό και οι δύο δικτυακές υποδομές τόσο λόγω του τρόπου λειτουργίας τους όσο και λόγω της φύσης των εφαρμογών που εξυπηρετούν, πρέπει να πληρούν ορισμένα χαρακτηριστικά ασφάλειας. Η έλλειψη αυτών των χαρακτηριστικών/ιδιοτήτων μπορεί να αποβεί ολέθρια για τη λειτουργία τους. Έτσι π.χ. στα Ευφυή δίκτυα είναι απαραίτητο ένας χρήστης να μην μπορεί να αρνηθεί τον καταλογισμό της χρέωσής του για κάποια υπηρεσία που έλαβε. Για παράδειγμα, θα πρέπει να μπορεί να χρεωθεί ο κάθε χρήστης, και ταυτόχρονα να μην μπορεί να το αρνηθεί, για τις ταινίες που μπορεί να παρακολούθησε (υπηρεσία video-on-demand). Καθώς κάθε κόμβος στα δίκτυα Ad Hoc βασίζεται στους γειτονικούς του για τη μεταφορά των μηνυμάτων του, η εισχώρηση ενός κακόβουλου κόμβου μπορεί να καταστρέ-

ψει/αλλοιώσει την επικοινωνία. Είναι σημαντικό, λοιπόν, να υπάρχει αμοιβαία εμπιστοσύνη μεταξύ των κόμβων του δικτύου.

Για να εξασφαλιστούν οι ιδιότητες ασφάλειας των δικτύων θα πρέπει να εφαρμοστούν κάποια σχήματα - πολιτικές ασφάλειας. Αυτά τα σχήματα θα πρέπει να είναι αποτελεσματικά την ασφάλεια, αλλά και ως προς τη γενικότερη διασφάλιση της αξιοπιστίας και των επιδόσεων του συστήματος. Είναι σημαντικό να κατανοηθούν οι διάφορες τεχνικές μελέτης επίδοσης ώστε να αναγνωρισθεί το είδος των αποτελεσμάτων που μπορεί να εξαχθεί από καθεμιά τους, καθώς επίσης και κάτω από ποιες συνθήκες είναι καθεμιά τους κατάλληλη για χρήση. Οι τεχνικές που χρησιμοποιούνται για τη μελέτη της επίδοσης ενός συστήματος διακρίνονται σε δύο μεγάλες κατηγορίες, τις *αναλυτικές* και τις *μη αναλυτικές*. Στις πρώτες γίνεται προσπάθεια ώστε το σύστημα να αναχθεί και να περιγραφεί με βάση κάποιο μαθηματικό μοντέλο. Στις δεύτερες το σύστημα μελετάται μέσα από την εφαρμογή του σε ένα δοκιμαστικό περιβάλλον.

1.1.2 Ερευνητικός Στόχος

Ερευνητικός στόχος αυτής της προσπάθειας είναι να μελετηθούν οι δύο δικτυακές δομές, δηλαδή οι δομές των Ευφυών δικτύων και των δικτύων Ad Hoc. Ως πρώτο βήμα, επιχειρείται η εύρεση σχημάτων - πολιτικών ασφάλειας που να καλύπτουν τα αιτήματα ασφάλειας. Ως δεύτερο βήμα, κρίνεται απαραίτητη η μελέτη της επίδοσης των συστημάτων αυτών.

Μελετώντας την αρχιτεκτονική των Ευφυών δικτύων διαπιστώθηκε ότι βασίζεται σχεδόν εξ ολοκλήρου στις κατανεμημένες τεχνολογίες. Επιπλέον, η επικοινωνία ανάμεσα στα στοιχεία του δικτύου πραγματοποιείται με τη χρήση ανοικτών και επισφαλών καναλιών. Αυτός ο τρόπος λειτουργίας υπόκειται σε πολλές επιθέσεις ασφάλειας όπως:

Πλαστοπροσωπία. Μη εξουσιοδοτημένοι χρήστες μπορούν να επιχειρήσουν

μέσω της επίθεσης της Πλαστοπροσωπίας (Impersonation) να αποκτήσουν πρόσβαση σε υπηρεσίες ΕΔ. Για παράδειγμα, στην περίπτωση της υπηρεσίας IMR ένας μη εγγεγραμμένος χρήστης μπορεί να επιχειρήσει να δει κάποια ταινία.

Μεταμφίεση. Ένας εγγεγραμμένος χρήστης μπορεί να επιχειρήσει μέσω της επίθεσης Μεταμφίεσης (Masquerading) να παρακάμψει την πολιτική ασφάλειας και παρανόμως να αποκτήσει πρόσβαση σε ευαίσθητες υπηρεσίες. Για παράδειγμα, ένας χρήστης που έχει δικαιώματα απλής πρόσβασης μπορεί να επιχειρήσει να λειτουργήσει σαν διαχειριστής ΕΔ.

Άρνηση Υπηρεσίας. Ένας κακόβουλος χρήστης μπορεί να επιχειρήσει να διακόψει νόμιμους χρήστες απο την πρόσβαση στις υπηρεσίες ΕΔ (Denial of Service - DoS), στέλνοντας, για παράδειγμα, ταυτόχρονα ένα μεγάλο αριθμό αιτημάτων στο σύστημα.

Υποκλοπή Επικοινωνίας και Τροποποιήση. Ένας κακόβουλος χρήστης μπορεί να επιχειρήσει να υποκλέψει και/ή να αλλάξει (communication eavesdropping and tampering) την επικοινωνία ανάμεσα σε έναν νόμιμο χρήστη και στα στοιχεία της υπηρεσίας IN.

Έλλειψη Ευθύνης. Εάν το ΕΔ δεν είναι ικανό να παρακολουθεί την επικοινωνία ανάμεσα στους χρήστες και τα στοιχεία της υπηρεσίας, τότε δεν θα είναι δυνατόν οι χρήστες να χρεωθούν για τις όποιες πράξεις τους (lack of accountability), π.χ. να χρεωθούν με το ανάλογο κόστος για τη χρήση της υπηρεσίας IMR.

Για το λόγο αυτό, η ασφαλής αρχιτεκτονική του ΕΔ θα πρέπει να επιβάλει κάποιες απαιτήσεις ασφάλειας. Μη εξουσιοδοτημένη χρήση μιας υπηρεσίας μπορεί να θεωρηθεί ως έλλειψη *πιστοποίησης* του χρήστη και δομικού στοιχείου του δικτύου, π.χ. κόμβου, παροχέα υπηρεσίας, κλπ. Με την εφαρμογή της

κατάλληλης πολιτικής ελέγχου πρόσβασης η *πιστοποίηση* του χρήστη μπορεί να επιτευχθεί, έχοντας ως αποτέλεσμα την αποφυγή απειλών μεταμφίεσης. Ο συνδυασμός της πολιτικής πρόσβασης και μιας πολιτικής παρακολούθησης (auditing) έχει ως αποτέλεσμα την αποφυγή ή και τον εντοπισμό της προέλευσης των επιθέσεων άρνησης υπηρεσίας, παρέχοντας έτσι *διαθεσιμότητα υπηρεσίας*. Επιπλέον, οι υπηρεσίες παρακολούθησης παρέχουν στο σύστημα τη δυνατότητα της *επίδοσης ευθύνης* στους χρήστες. Αυτό είναι απαραίτητο ώστε να κοστολογηθούν οι υπηρεσίες των δικτύων ΕΔ στους εκάστοτε χρήστες τους. Τέλος, υπηρεσίες *εμπιστευτικότητας* και *ακεραιότητας* είναι απαραίτητες για την αποφυγή υποκλοπών ή αλλαγών στην επικοινωνία ανάμεσα στους χρήστες και το δίκτυο.

Η διαδικασία ανεύρεσης δρομολογίων στα πρωτόκολλα δρομολόγησης πολλαπλών μονοπατιών παρουσιάζει πολλές αδυναμίες ασφάλειας επιτρέποντας έτσι είτε σε ένα μικρό σύνολο, είτε σε έναν και μόνο κακόβουλο κόμβο να ελέγξει το μονοπάτι επικοινωνίας ανάμεσα σε επιλεγμένους κόμβους. Αυτές οι αδυναμίες υποβιβάζουν την αξία των πρωτοκόλλων πολλαπλών μονοπατιών σαν να ήταν πρωτόκολλα ενός/μοναδικού μονοπατιού. Παρακάτω περιγράφονται μερικές από αυτές τις αδυναμίες.

Το φαινόμενο του ανταγωνισμού Σε πολλά πρωτόκολλα δρομολόγησης πολλαπλών μονοπατιών, κάθε ενδιάμεσος κόμβος επεξεργάζεται κάθε αίτηση για ανεύρεση μονοπατιού επικοινωνίας μόνον την πρώτη φορά που την λαμβάνει. Στη συνέχεια απορρίπτει κάθε επόμενο αντίγραφο αυτής ώστε να μειώσει την κίνηση περιτών δεδομένων στο δίκτυο. Αυτό συμβαίνει ακόμα και στην περίπτωση που το αντίγραφο της αίτησης έχει φτάσει στον ενδιάμεσο κόμβο ακολουθώντας ένα διαφορετικό μονοπάτι. Εάν τα πρωτόκολλα που λειτουργούν με αυτόν τον τρόπο καταφέρουν να ανακαλύψουν το σύνολο των μονοπατιών διακριτών/ μοναδικών κόμβων, εξαρτάται από τις συνθήκες ανταγωνισμού που υφίστανται στη μετάδο-

ση της αίτησης μέσα από διαφορετικά μονοπάτια. Εάν ένας ενδιάμεσος κόμβος τύχει να λάβει ένα αντίγραφο της αίτησης που έχει ταξιδέψει μέσα από ένα μονοπάτι Α, τότε εάν λάβει ένα άλλο αντίγραφο που έχει ταξιδέψει μέσα από ένα μονοπάτι Β θα το απορρίψει ακόμα και αν το μονοπάτι Β ανήκει σε ένα διαφορετικό σύνολο μονοπατιών μοναδικών/ διακριτών κόμβων. Έτσι, η διαδικασία εύρεσης μονοπατιών επικοινωνίας δεν θα έχει καταφέρει να ανακαλύψει όλα τα υπάρχοντα μονοπάτια διακριτών/ μοναδικών κόμβων που υπάρχουν ανάμεσα σε μια πηγή και έναν προορισμό.

Πλαστοπροσωπία και έλλειψη πιστοποίησης Εάν ένα πρωτόκολλο απαιτεί πιστοποίηση μόνο από άκρη σε άκρη και οι ενδιάμεσοι κόμβοι που συμμετέχουν στο μονοπάτι δεν είναι πιστοποιημένοι, τότε το πρωτόκολλο μπορεί να υποστεί επιθέσεις πλαστοπροσωπίας και επιθέσεις από κακόβουλος κόμβους οι οποίοι χρησιμοποιούν πολλαπλές ταυτότητες. Με αυτό τον τρόπο ένας κακόβουλος κόμβος μπορεί να συμμετέχει σε περισσότερα από ένα μονοπάτια, φαινομενικά μοναδικών κόμβων χρησιμοποιώντας μια διαφορετική ταυτότητα σε κάθε ένα από αυτά. Ο εχθρός μπορεί να καταλάβει μια μικρή ομάδα κόμβων σε μια περιορισμένη περιοχή του δικτύου ώστε να ελέγχει όλα τα μονοπάτια δρομολόγησης.

Αθέατος κόμβος Η μετάδοση του σήματος στα ασύρματα κινητά δίκτυα γίνεται μέσω ραδιοφωνικών κυμάτων. Σε αυτή την περίπτωση ένας κακόβουλος κόμβος δεν κάνει αισθητή την παρουσία του στο μονοπάτι. Αντιθέτως, ο κρυμμένος κόμβος σιωπηλά προωθεί την επικοινωνία ανάμεσα σε δύο κόμβους οι οποίοι, εσφαλμένα, νομίζουν ότι επικοινωνούν άμεσα μεταξύ τους. Με αυτό τον τρόπο ένας κόμβος μπορεί να συμμετέχει σε πολλά μονοπάτια επικοινωνίας, ακόμα και όταν το πρωτόκολλο απαιτεί πιστοποίηση των ενδιάμεσων κόμβων. Πράγματι, ένας κόμβος μπορεί νόμιμα να συμμετέχει σε ένα μονοπάτι και παράνομα, σιωπηρά,

να συμμετέχει και σε άλλα. Σε αυτή την περίπτωση η πιστοποίηση δεν μπορεί να προστατεύσει επιτυχώς την επικοινωνία καθώς ο κρυμμένος κόμβος αναμεταδίδει τα μηνύματα ασφάλειας ανάμεσα στην πηγή και τον προορισμό χωρίς να κάνει αισθητή την παρουσία του.

Για τους λόγους αυτούς η ασφαλής δρομολόγηση σε ένα δίκτυο Ad Hoc θα πρέπει να επιβάλλει κάποιες απαιτήσεις ασφάλειας. Ο κόμβος που αντιμετωπίζει το φαινόμενο του ανταγωνισμού θα συμπεριφερθεί σαν να δεχόταν μια επίθεση Ανταγωνισμού (Rushing attack), ενώ στην πραγματικότητα δεν υφίσταται τις ενέργειες ενός κακόβουλου χρήστη. Με την εφαρμογή της κατάλληλης στρατηγικής μπορεί να αποφευχθεί το φαινόμενο αυτό και να ανακαλυφθεί το σύνολο των μονοπατιών που υφίστανται ανάμεσα σε έναν κόμβο πηγή και σε έναν προορισμό. Το αποτέλεσμα της επίθεσης της πλαστοπροσωπίας και της έλλειψης πιστοποίησης μπορεί να μεγιστοποιηθεί εάν συνδυαστεί με επίθεση του είδους της 'Μαύρης Τρύπας' (''black-hole''), όπου ο επιτιθέμενος απαντά σε όλες τις αιτήσεις, με πλαστά (ανύπαρκτα) σύντομα μονοπάτια. Τότε ο κακόβουλος χρήστης μπορεί να παραποιήσει την επικοινωνία και, για παράδειγμα, να τη διακόψει σε κρίσιμες χρονικές στιγμές. Η μετάδοση μέσω ασύρματων καναλιών κάνει τα πρωτόκολλα δρομολόγησης πολλαπλών μονοπατιών ευπαθή σε επιθέσεις του τύπου Ενδιάμεσου (Man-In-the-Middle attack) και επιθέσεις Αθέατου Κόμβου (invisible node). Με την επιβολή της κατάλληλης πολιτικής ασφάλειας μπορεί να επιτευχθεί αμοιβαία εμπιστοσύνη μεταξύ των κόμβων που μετέχουν στη διαδικασία της δρομολόγησης.

1.2 Αντικείμενο, Σπουδαιότητα και Προσφορά της Διατριβής

Η διατριβή αυτή πραγματεύεται αρχικά τη μελέτη και παρουσίαση πολιτικών ασφάλειας για τα Ευφυή δίκτυα και τη δρομολόγηση στα κινητά δίκτυα Ad

hoc. Στη συνέχεια πραγματοποιείται μελέτη της επίδοσης των προτεινόμενων εφαρμογών, ώστε να διαπιστωθεί η επιβάρυνση που προσθέτει στο δίκτυο η εφαρμογή τους.

Προκειμένου να επιτευχθεί ο ερευνητικός στόχος της παρούσας διατριβής έχει μελετηθεί, όσον αφορά τα Ευφυή δίκτυα, η εφαρμογή ενός συνδυασμού μηχανισμών ασφάλειας CORBA και μη - CORBA. Μελετάται μια αρχιτεκτονική ασφάλειας Ευφυών δικτύων, η οποία εφαρμόζεται πάνω σε κατανεμημένα ευρυζωνικά Ευφυή Δίκτυα. Η αρχιτεκτονική των κατανεμημένων ευρυζωνικών Ευφυών δικτύων είναι βασισμένη στις τεχνολογίες CORBA και Grasshopper, ως πλατφόρμα πρακτόρων. Το μοντέλο ασφάλειας εξαρτάται από τα μοντέλα CORBA Security Service και το Grasshopper Security Service. Επιπλέον, χρησιμοποιούνται και άλλοι μηχανισμοί ασφάλειας μη-CORBA, όπως οι Trusted Third Party Services. Στη μελέτη αυτή έγινε ενδελεχής έρευνα της επίδοσης του δικτύου μετά την εφαρμογή των εν λόγω μηχανισμών.

Όσον αφορά τα κινητά δίκτυα Ad Hoc προτείνεται και παρουσιάζεται ένα ολοκληρωμένο κατ-αίτηση πρωτόκολλο δρομολόγησης πολλαπλών μονοπατιών το Secure Multipath Routing (SecMR), το οποίο παρέχει προστασία για τις επιθέσεις άρνησης υπηρεσίας ορισμένου αριθμού συνεργαζόμενων κακόβουλων κόμβων. Στη συνέχεια, πραγματοποιείται μελέτη του τρόπου με τον οποίο επηρεάζονται οι χαρακτηριστικοί παράμετροι του δικτύου, μετά την εφαρμογή του εν λόγω πρωτοκόλλου.

Στα πλαίσια της διδακτορικής διατριβής δημοσιεύτηκαν οι παρακάτω εργασίες σε διεθνή επιστημονικά βιβλία:

- Mavropodi R., Douligeris C.,"Multipath Routing protocols for Mobile Ad Hoc Networks: Security Issues and Performance Evaluation", WAC 2005, LNCS, 3854, Springer-Verlag, p 165-176, 2006
- Mavropodi R., Kotzanikolaou P., Douligeris C.,"Performance Analysis of Secure Multipath Routing Protocols for Mobile Ad Hoc Networks", WWIC 2005,

LNCS, 3510, Springer-Verlag, p 269-278, 2005

- Kotzanikolaou P., Douligeris C. Mavropodi R. and Chrissikopoulos V., "Mobile Agent Security", Invited chapter, Network Security: Current Status and Future Directions, Wiley-IEEE Press, p 257-269, 2007.

και σε έγκυρα διεθνή επιστημονικά περιοδικά:

- Mavropodi R., Kotzanikolaou P., Douligeris C., "SecMR - a SECure Multipath routing Protocol for ad hoc networks", Ad Hoc Networks, Elsevier, 5 (1), 87-99, 2007.

- Mavropodi R., Douligeris C., "Intelligent Networks - Security Issues and Performance Evaluation", Annual Review of Communications, IEC, 57, isbn:1-931695-28-8, 2004.

- Kotzanikolaou P., Mavropodi R., Douligeris C., and Chrissikopoulos V.,"Secure Intelligent Networks based on CORBA and Mobile Agents", Computer Communications, Elsevier, 29 (3), 325-336, 2006.

και σε διεθνή επιστημονικά συνέδρια:

- Kotzanikolaou P., Mavropodi R., Douligeris C., "Secure Multipath Routing for Mobile Ad Hoc Networks", WONS 2005, St. Moritz, Switzerland, January 19-21, 2005

- Mavropodi R., Douligeris C., "Performance Evaluation of Intelligent Network Topologies", SCI 2003, Orlando, USA, July 27-30, 2003

- R. Mavropodi and C. Douligeris, "Performance Evaluation of Interactive Multimedia Retrieval in Intelligent Networks", ComCon 8, 25-29, June 2001, Crete, Greece, 443 - 453.

- R. Mavropodi, P. Kotzanikolaou and C. Douligeris, "Secure Management of Intelligent Networks through Intelligent Agents", Workshop on Intelligent Agents and Virtual Reality, Athens, June 29, 2001, pp. 57-64.
- C. Douligeris, R. Mavropodi and P. Kotzanikolaou, "Agent - Based Security in Intelligent Multimedia Retrieval in Intelligent Networks", INFORMS Miami Annual Meeting, Miami Beach, FL, Nov. 2001.

1.2.1 Δομή της Διατριβής

Σκοπός αυτής της διατριβής είναι η μελέτη επίδοσης δύο διαφορετικών δικτυακών δομών όταν σε αυτές εφαρμόζονται προτεινόμενες πολιτικές ασφάλειας. Στο κεφάλαιο 2 παρουσιάζεται ο ερευνητικός χώρος στον οποίο πραγματοποιήθηκε η μελέτη, όπως αυτός ορίζεται από τις δικτυακές δομές των Ευφυών δικτύων και τα δίκτυα Ad Hoc. Στο κεφάλαιο 3 παρουσιάζονται μεθοδολογίες μελέτης επίδοσης καθώς και θέματα ασφάλειας που ανακύπτουν στα δίκτυα αυτά. Στο κεφάλαιο 4 προτείνεται μια πολιτική ασφάλειας ώστε να βελτιωθεί η λειτουργία του κατανεμημένου ευφυούς δικτύου. Στο κεφάλαιο 5 γίνεται παρουσίαση και ανάλυση των αποτελεσμάτων επίδοσης του κατανεμημένου ευφυούς δικτύου. Η παρουσίαση των αποτελεσμάτων γίνεται από δύο διαφορετικές οπτικές γωνίες. Στο κεφάλαιο 6 προτείνεται ένα πρωτόκολλο δρομολόγησης (SecMR) που μπορεί να εφαρμοστεί στα Ad Hoc δίκτυα. Το πρωτόκολλο εξασφαλίζει την ασφάλεια στην επικοινωνία με τη χρήση πολλαπλών μονοπατιών. Στο κεφάλαιο 7 γίνεται παρουσίαση και μελέτη των αποτελεσμάτων επίδοσης του πρωτοκόλλου SecMR. Το κεφάλαιο 8 παρουσιάζει συνοπτικά τα αποτελέσματα της διατριβής αυτής και προτείνει θέματα για μελλοντική μελέτη.

Κεφάλαιο 2

Τοπολογίες Δικτύων

Οι νέες τεχνολογίες και η ταχεία αυξανόμενη ανάγκη για επικοινωνία, καθώς και η εισαγωγή νέων εφαρμογών έχουν επιβάλλει τη δημιουργία πολλών επιλογών σε καθένα από τα τρία επίπεδα υποδομής ενός δικτύου. Αυτό το πολύπλευρο περιβάλλον θα πρέπει να παρέχει ομοιόμορφη πρόσβαση και μεταφορά πολυμεσικών δεδομένων, μέσω μιας ενοποιημένης υποδομής δικτύου. Η αυξανόμενη ανάγκη για περισσότερο εύρος ζώνης (bandwidth) και έγκαιρη παροχή υπηρεσιών, έχουν αναγκάσει το δίκτυο να προσαρμόζεται σε πραγματικό χρόνο.

Σήμερα, πολλές και διαφορετικές υπηρεσίες, όπως φωνή, δεδομένα και video αναπτύσσονται, παραδίδονται και προσπελαύνονται μέσω διαφορετικών υποδομών, όπως οι παρακάτω τεχνολογίες που αφορούν:

- τη μεταγωγή/δρομολόγηση: Public switched telephone network (PSTN), Mobile Ad hoc Networks (MANET), asynchronous transfer mode (ATM), Internet protocol (IP),
- τη μετάδοση (μεταφορά):Time division multiplexing (TDM) (plesiochronous digital hierarchy [PDH], synchronous optical network [SONET], synchronous digital hierarchy [SDH]), IP, A™ 'h wavelength division multiplexing [WDM]),

- την πρόσβαση Analog, digital loop carrier (DLC), integrated services digital network (ISDN), digital subscriber line (xDSL), cable, or passive optical networking (PON).

Μια υπηρεσία μπορεί να αναλυθεί σε τρεις κατηγορίες, τη μεταγωγή/δρομολόγηση, τη μεταφορά/μετάδοση και τέλος την πρόσβαση. Σε αυτή την ενότητα θα παρουσιαστούν δύο κύριες και καίριες προτάσεις μεταγωγής δρομολόγησης: τα ευφυή δίκτυα και τα ασύρματα κινητά ad hoc δίκτυα [22, 23, 24, 25].

Στο κεφάλαιο αυτό γίνεται παρουσίαση βασικών εννοιών των δικτυακών δομών των οποίων η μελέτη αποτελεί ερευνητικό αντικείμενο αυτής της διατριβής. Αρχικά παρουσιάζονται οι βασικές αρχές που διέπουν τα Ευφυή δίκτυα, περιγράφεται η δομή των κατανεμημένων Ευφυών δικτύων και γίνεται περιγραφή της υπηρεσίας παροχής πολυμεσικών πληροφοριών (IMR). Στη συνέχεια παρουσιάζονται οι βασικές έννοιες των δικτύων AD Hoc, γίνεται περιγραφή των πρωτοκόλλων δρομολόγησης που χρησιμοποιούν αυτού του είδους τα δίκτυα και αναφέρονται προβλήματα ασφάλειας που αντιμετωπίζουν τα πρωτόκολλα αυτά.

2.1 Ευφυή Δίκτυα

Αρχικά το τηλεφωνικό δίκτυο παρείχε μόνο βασικές υπηρεσίες (POTS), οι οποίες περιελάμβαναν κάποιο τερματικό εξοπλισμό, αναλογικές γραμμές και κάποιο μεταγωγέα (αστικό, υπεραστικό διεθνή). Η ολοκλήρωση μιας κλήσης περιελάμβανε τη συλλογή των ψηφίων, τη μεταγλώττιση και τη δρομολόγηση. Οι λειτουργίες αυτές πραγματοποιούνταν στον κεντρικό μεταγωγέα. Το σύστημα μεταγωγής υποστήριζε τον έλεγχο της κλήσης, τον έλεγχο της σύνδεσης και τον έλεγχο της υπηρεσίας. Η προσθήκη επιπλέον υπηρεσιών, όπως οι υπηρεσίες 800χχχ, η κλήση με τη χρήση κάρτας, τα ιδιωτικά δίκτυα και η προώθηση των κλήσεων απαιτούσαν τη πραγματοποίηση αλλαγών στο

τμήμα του δικτύου που έκανε τον έλεγχο της κλήσης (call-processing module). Οι προσθήκες αυτές ήταν χρονοβόρες, μεγάλες σε αριθμό και δαπανηρές, αφού έπρεπε να γίνουν παρεμβάσεις σε πολυάριθμα μέρη του δικτύου.

Το ευφυές δίκτυο εισήγαγε την έννοια της χρήσης ευφυών υπηρεσιών σε συστήματα μεταγωγής. Η ιδέα αυτή εμπεριείχε το λογικό διαχωρισμό της βασικής υπηρεσίας μεταγωγής (έλεγχος κλήσης/σύνδεσης) και των επιπλέον λειτουργιών συνθετότερων εφαρμογών (service control). Ο διαχωρισμός αυτός πραγματοποιείται μέσω ενός κατανεμημένου συστήματος/περιβάλλοντος, όπου σε κάποιο τμήμα του δικτύου δημιουργούνται οι υπηρεσίες, παρέχονται στον πελάτη από αλλού και τέλος κάποιο διαφορετικό τμήμα αναλαμβάνει την εκτέλεση και τη διαχείριση της όλης εφαρμογής [25]. Έτσι ο τελικός χρήστης μπορεί άμεσα να πραγματοποιήσει κλήσεις βασικών υπηρεσιών, αλλά και εκτελέσει συνθετότερες εφαρμογές.

Στα ευφυή δίκτυα η λογική της υπηρεσίας (δεδομένα και έλεγχος) έχει μεταφερθεί σε στοιχεία που καλούνται Service Control Points (SCP). Τα κεντρικά σημεία που πραγματοποιούν τον έλεγχο της κλήσης/σύνδεσης αναφέρονται σαν Service Switching Points (SSP). Ενώ ο έλεγχος των βασικών κλήσεων πραγματοποιείται στα σημεία του δικτύου που καλούνται SSP, ο έλεγχος των συνθετότερων υπηρεσιών πραγματοποιείται στα σημεία SCP. Γενικά, τα ευφυή δίκτυα έχουν ανεξαρτησία τόσο από τις ίδιες τις υπηρεσίες όσο και από το ίδιο το δίκτυο [25]. Παρακάτω αναλύεται σε βάθος η υποδομή δικτύων που ονομάζεται ¨Ευφυές Δίκτυο¨.

2.1.1 Τι είναι τα Ευφυή Δίκτυα

Τα Ευφυή Δίκτυα (ΕΔ, Intelligent Networks, IN), αποτελούν μια αρχιτεκτονική δικτύων που έχει ως σκοπό την παροχή εξειδικευμένων υπηρεσιών σε δίκτυα μεταγωγής (switched networks). Οι υπηρεσίες αυτές εφαρμόζονται γρηγορότερα, αποδοτικότερα και με έναν κατανεμημένο τρόπο ώστε η αρχιτεκτονική να

είναι ανεξάρτητη των κατασκευαστών και της υλοποίησης. Τα κύρια στοιχεία που αποτελούν την αρχιτεκτονική των ΕΔ είναι οι διάφορες λειτουργικές οντότητες, τα χρησιμοποιούμενα μοντέλα, οι μηχανές πεπερασμένων καταστάσεων (Finite State Machines, FSM) που ελέγχουν τη ροή των υπηρεσιών του καθώς και τα πρωτόκολλα με τα οποία επικοινωνούν τα διάφορα τμήματα του ΕΔ μεταξύ τους.

Το βασικό χαρακτηριστικό των ευφυών δικτύων είναι ο καταμερισμός της λογικής υπηρεσιών (service logic) σε διαφορετικά τμήματα του δικτύου, που ονομάζονται ευφυείς κόμβοι, τα οποία βρίσκονται εκτός του δικτύου μεταγωγής. Αυτό έρχεται σε αντίθεση με την μέχρι πρότινος πρακτική, η οποία επέβαλε η διαχείριση των κλήσεων να γίνεται από κοινού σε όλους τους κόμβους μεταγωγής του δικτύου. Το γεγονός αυτό ανέβαζε το λειτουργικό κόστος, κυρίως λόγω της διαφορετικότητας των κόμβων μεταγωγής, αλλά έκανε και την εισαγωγή νέων υπηρεσιών στο δίκτυο πολύ δύσκολη [27].

Προσπαθώντας να αντιμετωπίσει τα παραπάνω προβλήματα, η αρχιτεκτονική των ΕΔ διαχώρισε τη λογική διαχείρισης βασικών κλήσεων (basic call process logic) από τη λογική υπηρεσιών. Οι ευφυείς κόμβοι που είναι υπεύθυνοι για την λογική υπηρεσιών βρίσκονται εκτός του δικτύου μεταγωγής. Οι σχετικά λίγοι αυτοί κόμβοι, επικοινωνούν με τους κόμβους μεταγωγής του υπόλοιπου δικτύου για να παρέχουν τις υπηρεσίες στους πελάτες του ΕΔ. Το άμεσο αποτέλεσμα αυτής της αρχιτεκτονικής είναι ότι μπορούν να προστεθούν νέες υπηρεσίες ή να μεταβληθούν υπάρχουσες, κάνοντας αλλαγές μόνο στους ευφυείς κόμβους του δικτύου. Επειδή οι ευφυείς κόμβοι είναι σχετικά περιορισμένοι σε αριθμό, περιορισμένες είναι και οι επεμβάσεις που πρέπει να γίνουν στο δίκτυο. Η επικοινωνία μεταξύ των ευφυών κόμβων και των κόμβων μεταγωγής γίνεται με σηματοδοσία εκτός ζώνης (out of band signaling) η οποία υποστηρίζεται από το κοινό κανάλι του Συστήματος Σηματοδοσίας 7 (Signaling System 7, SS7) [27, 25].

Εννοιολογικό μοντέλο ευφυών δικτύων

Μέσα από τις προσπάθειες προτυποποίησης της αρχιτεκτονικής αυτής προέκυψε και το Εννοιολογικό Μοντέλο, σύμφωνα με το οποίο μπορούν να σχεδιαστούν αρχιτεκτονικές ΕΔ. Το μοντέλο αυτό διαχωρίζει τη φάση σχεδιασμού ενός ΕΔ σε τέσσερα επίπεδα, κάθε ένα από τα οποία αντιπροσωπεύει και ένα διαφορετικό επίπεδο αφαίρεσης στην μοντελοποίηση του δικτύου. Τα τέσσερα αυτά επίπεδα, τα οποία φαίνονται στην εικόνα 2.1, παρουσιάζονται παρακάτω [27].

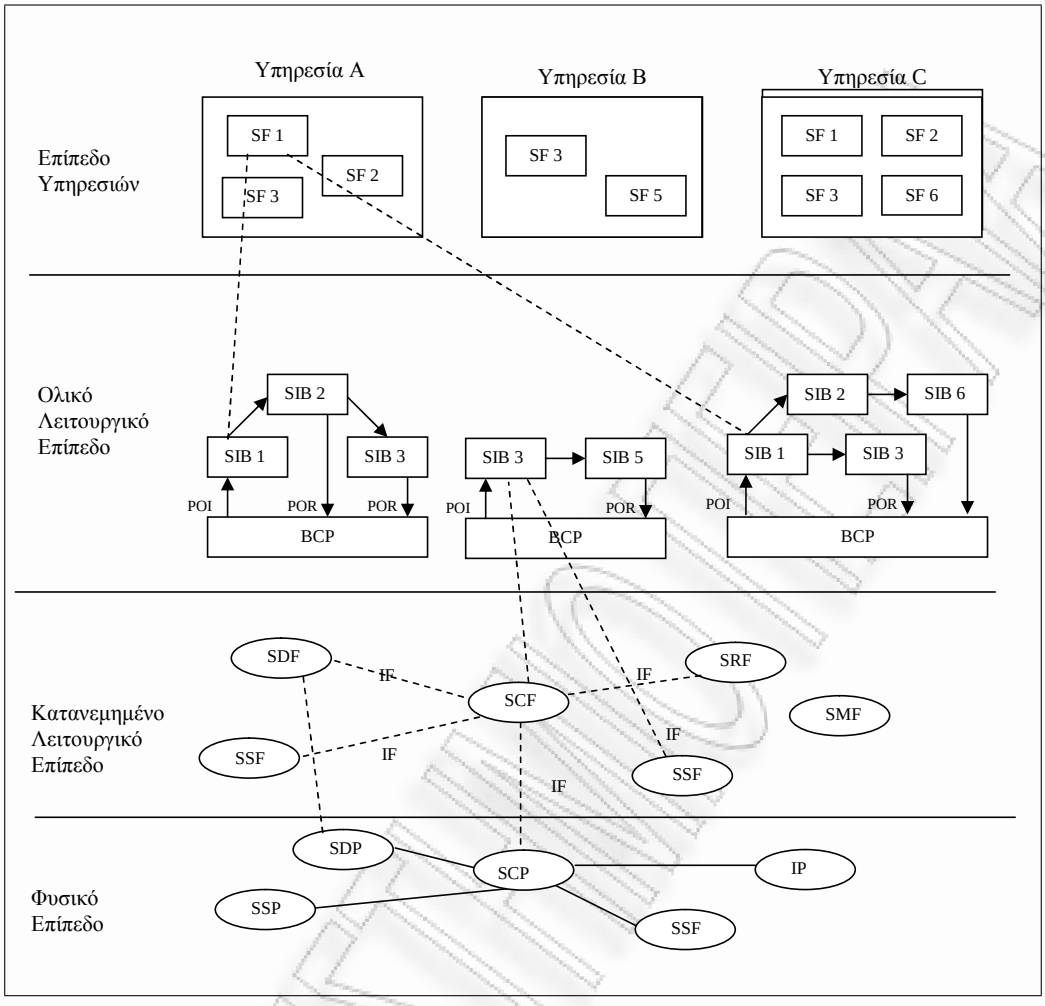
Επίπεδο Υπηρεσιών

Το επίπεδο αυτό αφορά την διεπαφή του χρήστη με το σύστημα του Ευφυούς Δικτύου και τις υπηρεσίες που προσφέρει αυτό. Κάθε υπηρεσία στο Επιπέδο Υπηρεσιών περιγράφεται από ένα ή περισσότερα Χαρακτηριστικά Υπηρεσίας (Service Features, SF) τα οποία αποτελούν τα βασικά λειτουργικά μέρη της.

Καθολικό Λειτουργικό Επίπεδο

Το επίπεδο αυτό αποτελείται από Στοιχεία Κατασκευής Ανεξάρτητα Υπηρεσιών (Service Independent Building Blocks, SIB) τα οποία αποτελούν ένα προς ένα αντιστοιχίες των SF του Επιπέδου Υπηρεσιών. Περιγράφεται επίσης η διασύνδεση μεταξύ των διαφόρων SIB ώστε αυτά να σχηματίζουν μια Ολική Λογική Υπηρεσιών (Global Service Logic, GSL) που χαρακτηρίζει κάθε υπηρεσία του δικτύου. Παράλληλα εμφανίζονται και οι τυχαίες αλληλεπιδράσεις μεταξύ των SIB και της Διαχείρισης Βασικών Κλήσεων (Basic Call Process, BCP). Η Διαχείριση Βασικών Κλήσεων δεν είναι τίποτα άλλο παρά από ένα SIB το οποίο αναλαμβάνει την έναρξη και τον έλεγχο ροής των υπηρεσιών του ΕΔ. Στο επίπεδο αυτό παρουσιάζεται ολόκληρη η μορφή του δικτύου χωρίς όμως να γίνεται αναφορά στον καταμερισμό των λειτουργιών του σε λειτουργικές οντότητες.

Κατανεμημένο Λειτουργικό Επίπεδο



Εικόνα 2.1: *Εννοιολογική Ανάλυση των Υπηρεσιών ΕΔ*

Το επίπεδο αυτό περιγράφει το δίκτυο ως ένα σύνολο Λειτουργικών Οντοτήτων (Functional Entities, FE) οι οποίες είναι ικανές να πραγματοποιήσουν μια ή περισσότερες υπηρεσίες του ΕΔ. Οι υπηρεσίες αυτές, στο επίπεδο αυτό, ονομάζονται Ενέργειες Λειτουργικής Οντότητας (Functional Entity Action, FEA). Κάθε FE μπορεί να πραγματοποιήσει περισσότερες από μια FEA, καθώς και μία FEA μπορεί να πραγματοποιηθεί από πολλές FE. Η σχέση μεταξύ των FE είναι μια σχέση πολλά προς πολλά. Όμως οι FEA είναι αρκούντως βασικές ώστε να μη μπορούν να διανεμηθούν σε δύο ή περισσότερα μέρη μεταξύ διαφορετικών FE. Ορισμένες FEA που επικοινωνούν κατά τη διάρκεια παρο-

χής μιας υπηρεσίας με άλλες FEA δημιουργούν κατά αυτό τον τρόπο Ροές Πληροφοριών (Information Flows, IF) οι οποίες αναπαρίστανται στο επίπεδο αυτό.

Φυσικό Επίπεδο

Στο Φυσικό Επίπεδο παρουσιάζεται το δίκτυο στην φυσική του υπόσταση. Οι Φυσικές Οντότητες (Physical Entities, PE) αποτελούν τα φυσικά εξαρτήματα του δικτύου και αντιπροσωπεύουν είτε μηχανήματα και δικτυακό εξοπλισμό, είτε άλλες οντότητες όπως τμήματα λογισμικού κλπ. Κάθε PE αυτού του επιπέδου αναλαμβάνει την εκπλήρωση των υπηρεσιών των FE του Κατανεμημένου Λειτουργικού Επιπέδου. Τέλος οι IF του προηγούμενου επιπέδου εμφανίζονται και εδώ και αναπαριστούν τα πρωτόκολλα με τα οποία πραγματοποιείται η επικοινωνία στο επίπεδο αυτό.

Λειτουργικές και Φυσικές οντότητες των ευφυών δικτύων

Παρακάτω περιγράφονται οι Λειτουργικές Οντότητες (FE) του Κατανεμημένου Λειτουργικού Επιπέδου και οι Φυσικές Οντότητες (PE) του Φυσικού Επιπέδου των ΕΔ.

Λειτουργικές Οντότητες

Οι FE που εμφανίζονται στο Κατανεμημένο Λειτουργικό Επίπεδο είναι οι παρακάτω:

- - *Λειτουργία Αντιπροσώπου Ελέγχου Κλήσεων (Call Control Agent Function, CCAF)*: Η λειτουργία αυτή αποτελεί την ενδιάμεση λειτουργική οντότητα μεταξύ των λειτουργιών ελέγχου κλήσεων του δικτύου και του χρήστη και παρέχει πρόσβαση των χρηστών στις υπηρεσίες του δικτύου.
- - *Λειτουργία Ελέγχου Κλήσεων (Call Control Function, CCF)*: Λειτουργία που ελέγχει τη ροή των κλήσεων από τους χρήστες.
- - *Λειτουργία Υπηρεσιών Χωρίς Κλήση (Call-Unrelated Service Function, CU-*

SF): Η λειτουργία η οποία αναλαμβάνει τις διαδικασίες που δεν σχετίζονται άμεσα με τις κλήσεις.

- - *Λειτουργία Μεταγωγής Υπηρεσιών (Service Switching Function, SSF)*: Λειτουργία που αναλαμβάνει τις διαδικασίες, οι οποίες είναι σχετικές με την επικοινωνία μεταξύ της CCF και της SCF.

- - *Λειτουργία Ελέγχου Υπηρεσιών (Service Control Function, SCF)*: Η λειτουργία που παρακολουθεί τη ροή παροχής υπηρεσιών του δικτύου στους χρήστες.

- - *Λειτουργία Πληροφοριών Υπηρεσιών (Service Data Function, SDF)*: Λειτουργία που αποθηκεύει λογιστικά στοιχεία για τους πελάτες καθώς και πληροφορίες για το δίκτυο. Τα δεδομένα αυτά χρησιμοποιούνται από την SCF.

- - *Λειτουργία Εξειδικευμένων Πόρων (Specialized Resource Function, SRF)*: Η λειτουργία αυτή παρέχει υπηρεσίες και αποθηκεύει πληροφορίες οι οποίες είναι εξειδικευμένες για το συγκεκριμένο δίκτυο.

- - *Λειτουργία Αντιπροσώπου για Έλεγχο Υπηρεσιών προς το Χρήστη (Service Control User Agent Function, SCUAF)*: Λειτουργία που είναι υπεύθυνη για αλληλεπιδράσεις με τις υπηρεσίες ΕΔ οι οποίες είναι ανεξάρτητες του χρήστη.

- - *Λειτουργία Περιβάλλοντος Δημιουργίας Υπηρεσιών (Service Creation Environment Function, SCEF)*: Η λειτουργία αυτή παράγει φόρμες λογικής υπηρεσιών και δεδομένων υπηρεσιών παρέχοντας ένα περιβάλλον ορισμού, δημιουργίας και δοκιμής νέων υπηρεσιών στο ΕΔ.

- - *Λειτουργία Αντιπροσώπου Διαχείρισης Υπηρεσιών (Service Management Agent Function, SMAF)*: Παρέχει μια διαπροσωπία μεταξύ των διαχειριστι-

κών λειτουργιών των υπηρεσιών του δικτύου και του διαχειριστή των υπηρεσιών αυτών (servive administrator).

- - *Λειτουργία Διαχείρισης Υπηρεσιών (Service Management Function, SMF)*: Λειτουργία υπεύθυνη για την επίβλεψη και τη χρέωση των υπηρεσιών που προσφέρονται από το ΕΔ.

Φυσικές Οντότητες

Οι ΡΕ που εμφανίζονται στο Φυσικό Επίπεδο είναι οι παρακάτω:

- - *Σημείο Μεταγωγής Υπηρεσιών (Service Switching Point, SSP)*: Παρέχει πρόσβαση των πελατών στο δίκτυο, λειτουργεί ως μεταγωγέας και επιτρέπει στους χρήστες πρόσβαση στις υπηρεσίες του δικτύου. Περιέχει τις λειτουργικές οντότητες SSF, CCF και, αν το δίκτυο υποστηρίζει επικοινωνία χωρίς κλήση, περιέχει και την CUSF.

- - *Σημείο Πρόσβασης Δικτύου (Network Access Point, NAP)*: Είναι ο κόμβος από τον οποίο οι χρήστες αποκτούν πρόσβαση στο δίκτυο. Περιέχει τις οντότητες CCAF και CCF.

- - *Σημείο Ελέγχου Υπηρεσιών (Service Control Point, SCP)*: Ο κόμβος που ελέγχει τη ροή των υπηρεσιών προς τον πελάτη. Περιέχει τα Προγράμματα Λογικής Υπηρεσιών (Service Logic Programs, SLPs) και ορισμένα δεδομένα για την παροχή υπηρεσιών. Είναι κόμβοι που χειρίζονται μεγάλο φόρτο δεδομένων, οπότε και υπάρχουν αρκετοί μέσα στο δίκτυο.

- - *Ευφυές Περιφερειακό (Intelligent Peripheral, IP)*: Βοηθητικά τμήματα που βρίσκονται στο τερματικό του πελάτη και προσφέρουν μια ευέλικτη αλληλεπίδραση με το δίκτυο, ενώ προσαρμόζονται ανάλογα με τις πληροφορίες που περιλαμβάνουν.

- - *Κόμβος Υπηρεσιών (Service Node, SN)*: Ελέγχει τις υπηρεσίες και αλληλεπιδρά με τον χρήστη για την ανταλλαγή πληροφοριών που είναι σχετικές

με τις υπηρεσίες αυτές. Το SN επικοινωνεί άμεσα με ένα ή περισσότερα SSP για σηματοδοσία και ανταλλαγή βασικών δεδομένων.

- - *Σημείο Πληροφοριών Υπηρεσιών (Service Data Point, SDP)*: Είναι ο κόμβος αποθήκευσης των δεδομένων των πελατών και του δικτύου τα οποία ανακτώνται αργότερα για τη σωστή παροχή των υπηρεσιών.

- - *Σημείο Ελέγχου και Μεταγωγής Υπηρεσιών (Service Switching and Control Point, SSCP)*: Περιέχει τις λειτουργικές οντότητες SSF και SCF και άρα παρέχει τις υπηρεσίες και των δύο, χωρίς να καθίσταται αναγκαία η εξωτερική επικοινωνία των δύο οντοτήτων.

- - *Εξοπλισμός Πελάτη ISDN (Enhanced ISDN Customer Premises Equipment, ISDN CPE)*: Παρέχει τις λειτουργίες που είναι απαραίτητες για την χρήση των πρωτοκόλλων πρόσβασης.

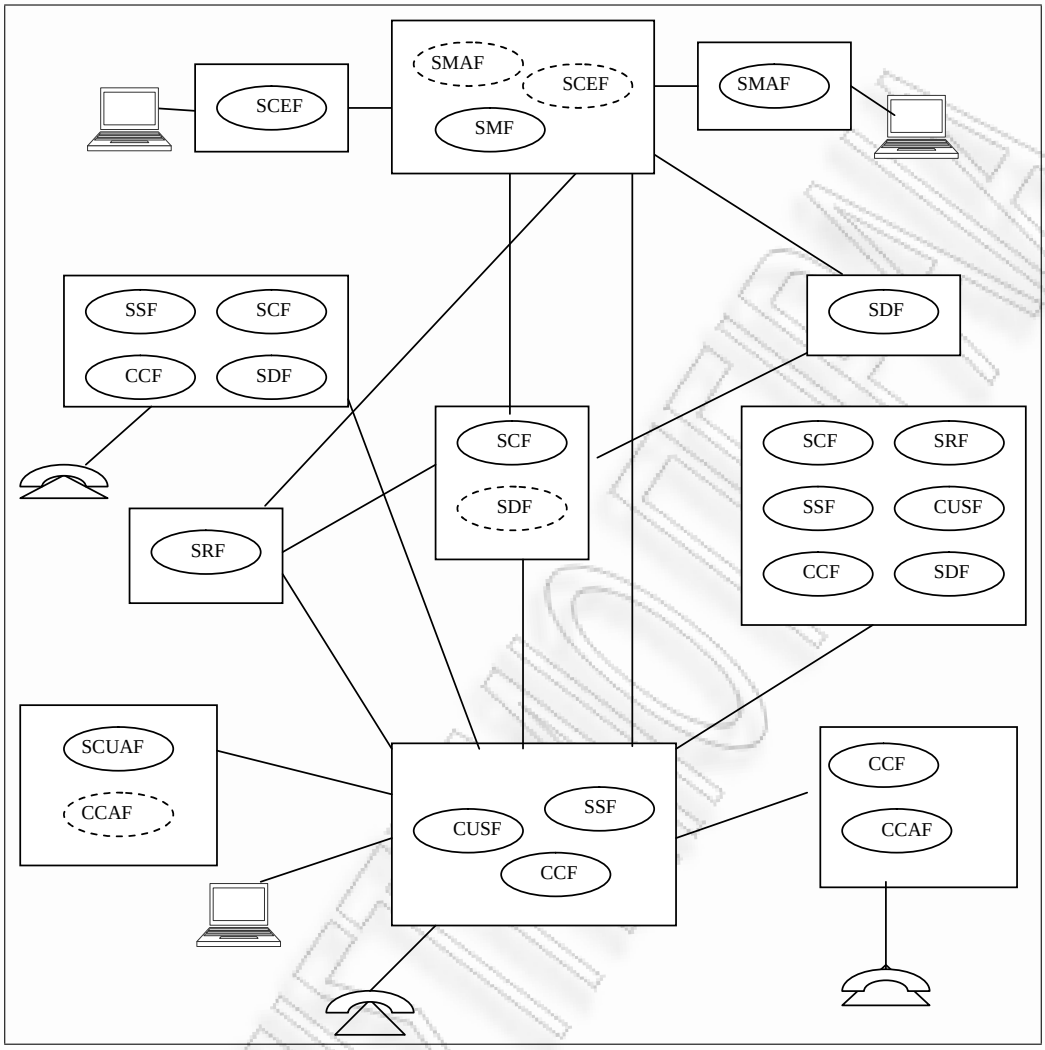
Ένα κάπως πολύπλοκο παράδειγμα μοντελοποίησης ενός δικτύου βασιζόμενο στις παραπάνω αρχές δίνεται στην εικόνα 2.2.

2.1.2 Κατανεμημένα Ευφυή Δίκτυα

Το παραδοσιακό μοντέλο των ευφυών δικτύων που παρουσιάστηκε ανωτέρω, είναι σχετικά συγκεντρωτικό αλλά μπορεί, με κατάλληλες αλλαγές, να γίνει πιο κανανεμημένο. Οι αλλαγές αυτές περιέχουν τη μετανάστευση της εκτέλεσης της υπηρεσίας πλησιέστερα στο χρήστη. Για να επιτευχθεί αυτό, μπορούν να χρησιμοποιηθούν ορισμένες νέες τεχνολογίες και τεχνικές. Δύο χρήσιμα τέτοια εργαλεία είναι οι τεχνολογίες των κατανεμημένων αντικειμένων και των κινητών αντιπροσώπων.

Τεχνολογία Κατανεμημένων Αντικειμένων (CORBA)

Η τεχνολογία των κατανεμημένων αντικειμένων βασίζεται στη δυνατότητα ύπαρξης οντοτήτων ενός συστήματος σε απομακρυσμένες μεταξύ τους τοπο-



Εικόνα 2.2: *Αντιστοίχιση Φυσικών και Λειτουργικών Οντοτήτων σε ένα ΕΔ*

θεσίες. Έτσι οι οντότητες αυτές επικοινωνούν μεταξύ τους αδιαφανώς, ούτως ώστε ούτε ο προγραμματιστής, ούτε ο παροχέας της υπηρεσίας να χρειάζεται να γνωρίζουν τον τρόπο που πραγματοποιείται η επικοινωνία αυτή. Με τον τρόπο αυτό γίνεται ευκολότερη η σχεδίαση μιας κατανεμημένης εφαρμογής, αφού ο προγραμματιστής έχει πρόσβαση σε υπηρεσίες και χαρακτηριστικά προγραμμάτων απομακρυσμένων αντικειμένων, μεταχειρίζοντάς τα σαν αυτά να βρίσκονται τοπικά και μάλιστα στο μέρος της ίδιας της εφαρμογής.

Μια τεχνολογία με την οποία υλοποιούνται μοντέλα κατανεμημένων αντι-

κειμένων είναι και η CORBA (Common Object Request Broker Architecture). Η αρχιτεκτονική αυτή χρησιμοποιεί μία υπηρεσία ονοματολογίας, παρόμοια με την υπηρεσία Domain Name System (DNS) του διαδικτύου, η οποία επιτρέπει τον εντοπισμό και τη χρησιμοποίηση απομακρυσμένων αντικειμένων, με τον ίδιο τρόπο που θα γίνονταν αν αυτά βρίσκονταν τοπικά. Ο ορισμός της διεπαφής μεταξύ των αντικειμένων στην CORBA ορίζεται με την γλώσσα IDL (Interface Definition Language) η οποία αποτελεί ένα πρωτόκολλο περιγραφής του συστήματος διεπαφής λογισμικών οντοτήτων. Υλοποιήσεις της εξαγόμενης αρχιτεκτονικής υπάρχουν σε πολλές γλώσσες προγραμματισμού και τεχνολογίες διαδικτύωσης [23].

Τεχνολογία Κινητών Αντιπροσώπων

Η τεχνολογία των κινητών αντιπροσώπων (Mobile Agent Technology (MAT)[1] μπορεί να περιγραφεί ως ένα σύστημα μέσα στο οποίο τμήματα μιας εφαρμογής μπορούν να μεταφέρονται από τον έναν κόμβο στον άλλο και να εκτελούνται τοπικά. Τα τμήματα αυτά, που ονομάζονται *κινητοί αντιπρόσωποι*, μπορούν να επικοινωνούν με άλλα τμήματα της εφαρμογής και με άλλους αντιπροσώπους, μέσω της αποστολής μηνυμάτων. Η λογική ύπαρξης κινητών αντιπροσώπων στηρίζεται στη μεταφορά της ίδιας της λειτουργίας ενός τμήματος μέσα στο δίκτυο, αλλά όχι και των δεδομένων που χρησιμοποιούνται. Επιπλέον, οι κινητοί αντιπρόσωποι μπορούν να χρησιμοποιηθούν για την κατανομή του φόρτου μέσα στο σύστημα.

Είναι προφανές ότι η τεχνολογία των κινητών αντιπροσώπων μπορεί να χρησιμοποιηθεί για την υλοποίηση μιας κατανεμημένης αρχιτεκτονικής αφού ουσιαστικά κάθε κόμβος του δικτύου θα μπορεί να χρησιμοποιηθεί για την επίτευξη μιας λειτουργίας. Επίσης, κινητοί αντιπρόσωποι μπορούν να χρησιμοποιηθούν σε περιπτώσεις κίνησης του χρήστη μέσα στο δίκτυο, καθώς και

[1] στη συνέχεια θα χρησιμοποιείται ο όρος MAT

σε λειτουργίες που απαιτούν μετακίνηση μεγάλου όγκου δεδομένων [23].

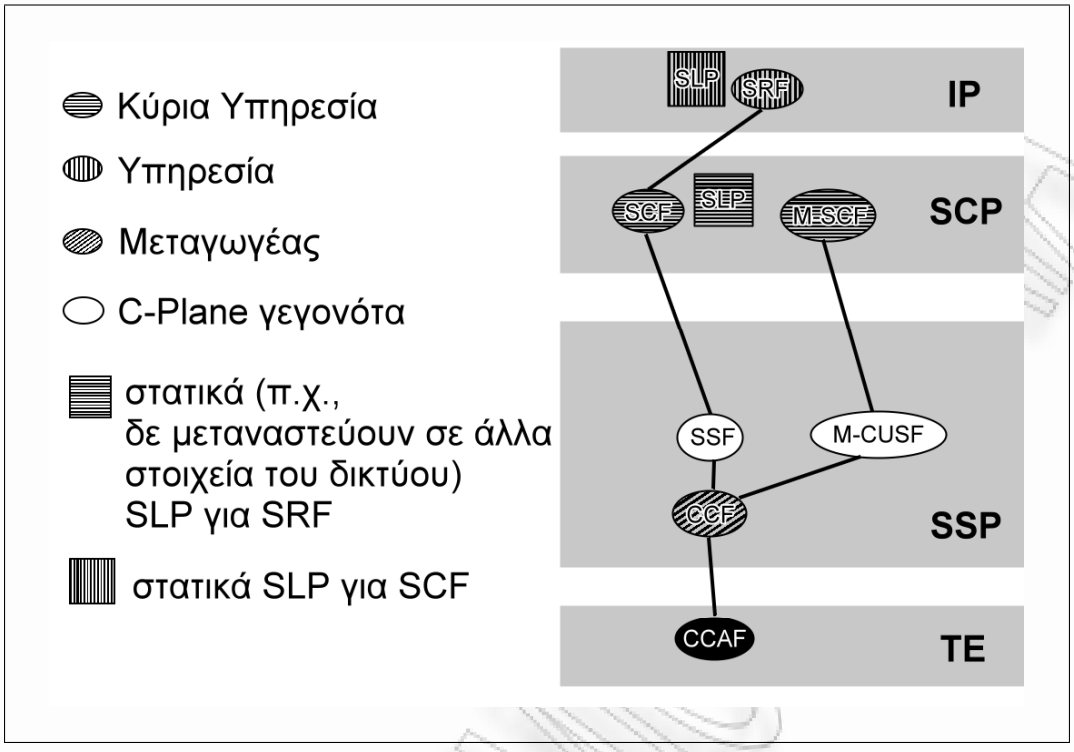
Αρχιτεκτονική Κατανεμημένων Ευφυών Δικτύων

Η χρήση των ανωτέρω τεχνολογιών στο σχεδιασμό ενός δικτύου, έχει ως αποτέλεσμα τη δημιουργία ενός ευφυούς δικτύου που χρησιμοποιεί κατανεμημένη αρχιτεκτονική, σε αντίθεση με την παραδοσιακή συγκεντρωτική αρχιτεκτονική. Η προτεινόμενη, κατανεμημένη αρχιτεκτονική είναι πιο ευέλικτη σε τυχόν αλλαγές κώδικα και, παράλληλα, αποδοτικότερη σε καταστάσεις μεγάλου φόρτου του δικτύου. Για τη δημιουργία της αρχιτεκτονικής αυτής έχει χρησιμοποιηθεί ένα επιπλέον επίπεδο, το οποίο και κάνει την αρχιτεκτονική αυτή κατανεμημένη. Το επίπεδο αυτό σχετίζεται με την αντιστοίχιση των Λειτουργικών Οντοτήτων (FE) στις Φυσικές Οντότητες (PE).

Στην εικόνα 2.3 φαίνεται η αντιστοίχιση μεταξύ FE και PE σε ένα τυπικό δίκτυο που χρησιμοποιεί την παραδοσιακή, συγκεντρωτική πολιτική των ΕΔ.

Στην αρχιτεκτονική των Κατανεμημένων Ευφυών δικτύων (D-IN, Distributed Intelligent Network) θεωρούνται ότι οι υπηρεσίες που προσφέρονται από το δίκτυο μπορούν να εκτελούνται και σε στατικά αλλά και σε μετακινούμενα μέρη του δικτύου, στο επίπεδο των λειτουργικών οντοτήτων. Έτσι κατά το σχεδιασμό του δικτύου και την αντιστοίχιση μεταξύ FE και PE, μπορεί να αποφασιστεί η τοποθέτηση ορισμένων FE σε ετερογενή συστήματα.

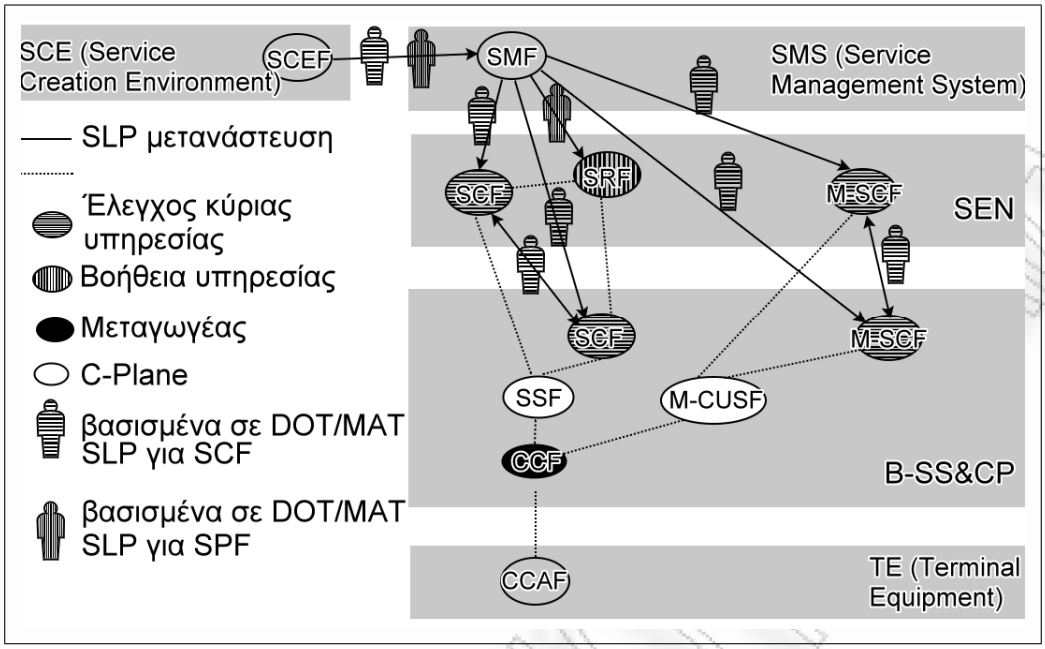
Αυτό έχει ως αποτέλεσμα οι λειτουργικές οντότητες όπως η SCF να υπάρχουν, συχνά, και σε κόμβους εξυπηρέτησης του ΕΔ αλλά και σε κόμβους του δικτύου μεταγωγής. Μερικές φορές, όμως, η οντότητα SCF τοποθετείται στις ίδιες φυσικές οντότητες με τη λειτουργική οντότητα SRF. Έτσι δημιουργούνται κόμβοι του δικτύου μεταγωγής με αναβαθμισμένο ρόλο. Οι κόμβοι αυτοί έχουν μέρος της λειτουργικότητας της φυσικής οντότητας SCP, που ονομάζονται, πλέον, B-SS&CP (Broadband-Service Switching and Control Point). Επίσης, υπάρχουν και κόμβοι εξυπηρέτησης που αποτελούνται από τμήματα των φυσικών ον-



Εικόνα 2.3: *Αντιστοίχιση Φυσικών και Λειτουργικών Οντοτήτων σε ένα παραδοσιακό ΕΔ*

τοτήτων SCP και IP οι οποίοι ονομάζονται SEN (Sevice Execution Node). Οι κόμβοι B-SS&CP και SEN φαίνονται στην εικόνα 2.4.

Η επικοινωνία μεταξύ των οντοτήτων για την ανταλλαγή πληροφοριών, οι οποίες είναι απαραίτητες για την παροχή των υπηρεσιών, γίνεται μέσω της τεχνολογίας CORBA. Για να πραγματοποιηθεί αυτή η επικοινωνία πρέπει να κατασκευαστούν αντικείμενα λογισμικού τα οποία θα αντιστοιχίζουν κάθε μία από τις οντότητες, που πρέπει να επικοινωνήσουν, με άλλες. Τα αντικείμενα αυτά περιγράφουν, μέσω της IDL, την αλληλεπίδραση των λειτουργικών αυτών οντοτήτων. Τα αντικείμενα αυτά, στη συνέχεια, κατανέμονται στο σύστημα και γίνονται προσβάσιμα από τις υπόλοιπες οντότητες μέσω της CORBA. Η λογική, αυτή, των κατανεμημένων αντικειμένων έρχεται να αντικαταστήσει τη μοντελοποίηση γύρω από τα SIB, προσφέροντας μεγαλύτερη ευελιξία καθώς και επαναχρησιμοποίηση κώδικα.



Εικόνα 2.4: *Αντιστοίχιση Φυσικών και Λειτουργικών Οντοτήτων σε ένα κατανεμημένο ΕΔ [4]*

Επιπρόσθετα, στο περιβάλλον των κατανεμημένων ευφυών δικτύων, η χρήση της τεχνολογίας MAT, επιτρέπει στα αντικείμενα να μετακινούνται μέσα στο δίκτυο, κατά τη λειτουργία του, εφαρμόζοντας έτσι μια δυναμική αντιστοίχιση μεταξύ Λειτουργικών και Φυσικών Οντοτήτων. Μεταφέροντας π.χ. έναν κινητό αντιπρόσωπο υπεύθυνο για την Λογική Υπηρεσιών στο SSP, μπορεί να αποφευχθεί η επικοινωνία μεταξύ δύο κόμβων, η οποία θα ήταν αναπόφευκτη αν αυτοί ήταν απομακρυσμένοι. Οι μετακινήσεις των κινητών αντιπροσώπων μπορεί να είναι αυτοματοποιημένες, παρέχοντας τη δυνατότητα στο δίκτυο να ενεργεί αυτόματα σε περιπτώσεις φόρτου. Για την απόκτηση αυτής της λειτουργικότητας θα πρέπει τα αντικείμενα να υλοποιούνται ως κινητοί αντιπρόσωποι στο περιβάλλον MAT που χρησιμοποιεί το σύστημα.

Φυσικές Οντότητες στα ΚΕΔ

Οι φυσικές οντότητες που βρίσκονται σε ένα κατανεμημένο ΕΔ διαφέρουν από αυτές που υπάρχουν στα παραδοσιακά συγκεντρωτικά ΕΔ, κυρίως λόγω της αναβαθμισμένης λειτουργικότητάς τους. Οι κυριότερες φυσικές οντότητες

σε ένα D-IN είναι οι παρακάτω:

- - *Σύστημα Διαχείρισης Υπηρεσιών (Service Management System, SMS)*: Η φυσική αυτή οντότητα περιέχει τη λειτουργική οντότητα SMF. Σκοπός της είναι, κυρίως, η ανεξαρτητοποίηση του τμήματος του ΕΔ που δεν έχει σχέση με τη λογική των υπηρεσιών του δικτύου, από το περιβάλλον εκτέλεσής του (π.χ. υλοποιήσεις CORBA και MAT).

- - *Κόμβος Εκτέλεσης Υπηρεσιών (Service Execution Node, SEN)*: περιέχει τις λειτουργικές οντότητες B-SCF και την B-SRF. Ο κόμβος αυτός έχει τη δυνατότητα λήψης και αποστολής κινητών αντιπροσώπων και επιτρέπει την εκτέλεση της λογικής της υπηρεσίας (SLP) με τη μορφή κινητών αντιπροσώπων.

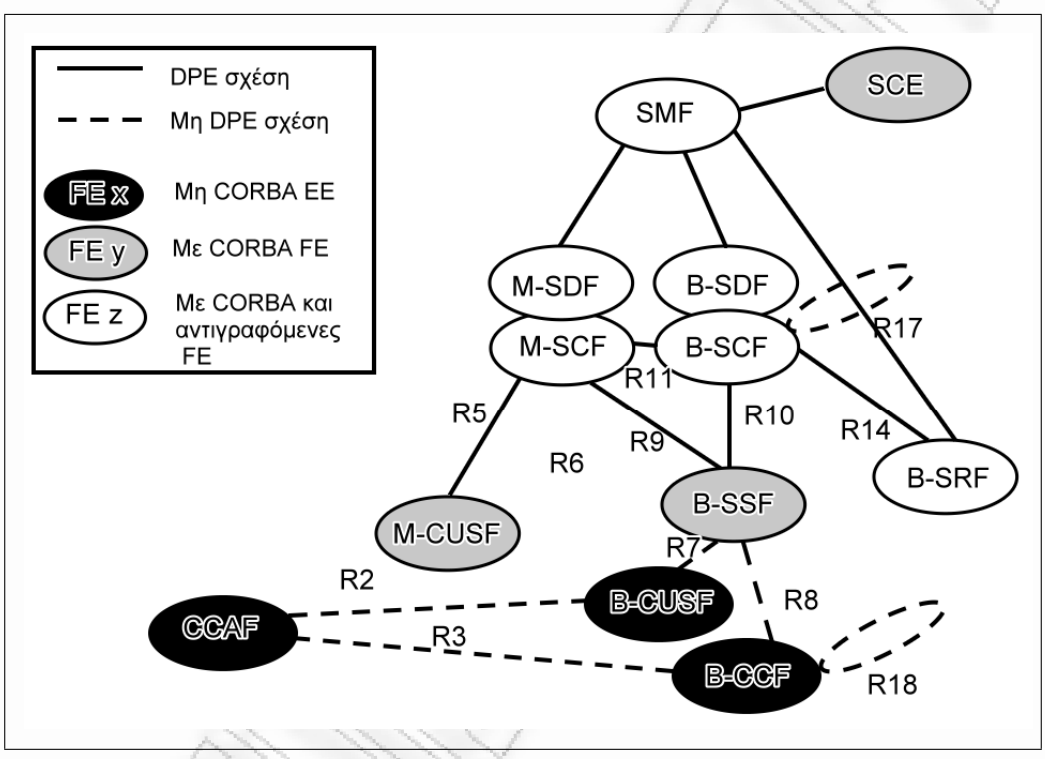
- - *Σημείο Μεταγωγής και Ελέγχου Υπηρεσιών Ευρείας Ζώνης (Broadband Service Switching and Control Point, B-SS&CP)*: Η φυσική αυτή οντότητα περιέχει τις λειτουργικές οντότητες B-SSF και B-SCF. Η λειτουργική οντότητα B-SCF, που βρίσκεται σε αυτόν τον κόμβο, περιέχει και αυτή ένα περιβάλλον εκτέλεσης κινητών αντιπροσώπων, όπως ακριβώς και η λειτουργική οντότητα SEN, που βρίσκεται στον ίδιο κόμβο. Υπάρχει η δυνατότητα ανταλλαγής αντιπροσώπων μεταξύ των κόμβων SEN και B-SS&CP. Έτσι, η ανταλλαγή πληροφοριών μεταξύ των λειτουργικών οντοτήτων SSF και SCF μπορεί να γίνεται εσωτερικά στον κόμβο B-SS&CP.

- - *Περιβάλλον Δημιουργίας Υπηρεσιών (Service Creation Environment, SCE)*: Συνήθως αυτός ο κόμβος συμπεριλαμβάνεται στον κόμβο SEN ώστε να απλοποιηθεί η αρχιτεκτονική. Στο SCE περιέχονται όλες οι δυνατότητες που είναι απαραίτητες για την επικοινωνία μεταξύ των κόμβων του δικτύου, με χρήση π.χ. της CORBA. Πιο συγκεκριμένα στο SCE δρα η υπηρεσία ονοματολογίας της CORBA, με την οποία θα μπορούν οι εφαρμογές να εντοπίζουν αντικείμενα, τα οποία διαμοιράζονται στο δίκτυο,

καθώς και άλλες υπηρεσίες που συνδέονται με την CORBA.

Λειτουργικές Οντότητες στα D-IN

Οι λειτουργικές οντότητες που συναντώνται στην κατανεμημένη αρχιτεκτονική είναι διαφοροποιημένες από αυτές που χρησιμοποιούνται στην παραδοσιακή συγκεντρωτική αρχιτεκτονική των ΕΔ και παρουσιάζονται στην εικόνα 2.5. Οι κυριότερες από αυτές αναφέρονται παρακάτω.



Εικόνα 2.5: *Οι Λειτουργικές Οντότητες σε ένα κατανεμημένο ΕΔ [4]*

- - *Λειτουργία Ελέγχου Κλήσεων Ευρείας Ζώνης (Broadband Call Control Function, B-CCF)*: Αυτή η λειτουργική οντότητα είναι υπεύθυνη για τη διαχείριση των κλήσεων και εκτελεί τις οδηγίες που δέχεται από τη λειτουργική οντότητα CCAF που βρίσκεται στον κόμβο CPE.

- - *Λειτουργία Μεταγωγής Υπηρεσιών Ευρείας Ζώνης (Broadband Service Switching Function, B-SSF)*: Η οντότητα B-SSF λειτουργεί ως ενδιάμεσο επίπεδο μεταξύ των μηχανών καταστάσεων της σηματοδοσίας, οι οποίες

βρίσκονται στα B-CCF και M-CUSF, και των αντικειμένων, τα οποία είναι υπεύθυνα για τις υπηρεσίες των SCF και SDF και κατανέμονται μέσω της CORBA.

- - *Λειτουργία Ελέγχου Υπηρεσιών Ευρείας Ζώνης (Broadband Service Control Function, B-SCF)*: Η οντότητα αυτή επικοινωνεί με την B-CCF στην οποία και δίνει εντολές. Επίσης, επικοινωνεί και με άλλες λειτουργικές οντότητες όπως οι SDF, SRF και SSF, διευρύνοντας έτσι τη λειτουργικότητά της. Σε γενικές γραμμές είναι υπεύθυνη για τη διατήρηση της Λογικής Υπηρεσιών, η οποία εκφράζεται μέσω των SLP (Service Logic Programs).

- - *Κινητή Λειτουργία Ελέγχου Υπηρεσιών (Mobile Service Control Function, M-SCF)*: Η οντότητα αυτή είναι μια κινούμενη έκδοση της οντότητας SCF και υλοποιείται χρησιμοποιώντας κινητούς αντιπροσώπους. Είναι ιδιαίτερα χρήσιμη για να ελέγχει την κινητικότητα του χρήστη στο δίκτυο, λειτουργία που διευκολύνεται πολύ με την τεχνολογία MAT.

- - *Λειτουργία Εξειδικευμένων Πόρων Ευρείας Ζώνης (Broadband Specialized Resource Function, B-SRF)*: Η οντότητα παρέχει εξειδικευμένους πόρους για κάθε εφαρμογή του δικτύου και επικοινωνεί με το SFF μέσω του CPE. Χρησιμοποιείται συνήθως για τη δημιουργία μιας φιλικής διεπαφής με την εφαρμογή του χρήστη (π.χ. σε μια εφαρμογή αναπαραγωγής video το SRF μπορεί να επιτρέπει στον χρήστη επιλογή συγκεκριμένης ταινίας).

2.1.3 Υπηρεσία Ανάκτησης Πολυμεσικών Δεδομένων κατά Απαίτηση

Αυτού του είδους οι αρχιτεκτονικές είναι αρκετά εξεζητημένες ώστε να υποστηρίζουν εφαρμογές που ικανοποιούν τις αυξημένες ανάγκες των χρηστών. Παραδείγματα αυτών των εφαρμογών αποτελούν και οι υπηρεσίες Multimedia Retrieval (IMR) και πιο συγκεκριμένα η Video-on-Demand (VoD) και News-

on-Demand (NoD). Η παροχή αλληλεπίδρασης μεταξύ των χρηστών και του δικτύου οδηγεί σε υπηρεσίες υψηλής ποιότητας.

Συγκεκριμένα η υπηρεσία ανάκτησης κινούμενης εικόνας κατά απαίτηση (Video On Demand, VoD) είναι μια διαδικασία που περιλαμβάνει τη παροχή ενός συγκεκριμένου video στον πελάτη, από μια απομακρυσμένη τοποθεσία, τη στιγμή που αυτός το ζητήσει. Η μεταφορά αυτή γίνεται μέσω ενός δικτύου δεδομένων, έπειτα από απαίτηση του πελάτη, του οποίου το λογισμικό έχει τη δυνατότητα αναπαραγωγής του. Μετά την έναρξη αποστολής των δεδομένων, ο πελάτης πρέπει να έχει πλήρη έλεγχο της προβολής του video, όπως π.χ. να παγώσει την εικόνα ή να προχωρήσει γρήγορα το video.

Τα video που είναι διαθέσιμα βρίσκονται σε διάφορους Παροχείς Περιεχομένου (Content Providers, CP). Οι CP δεν αποτελούν μέρος του δικτύου επικοινωνιών, αλλά παρέχουν το περιεχόμενό τους είτε ενοικιάζοντάς το, ή πουλώντας το σε Παροχείς Υπηρεσιών (Service Providers SP), οι οποίοι το διαμοιράζουν μεταξύ διάφορων Εξυπηρετητών Video (Video Servers, VS). Ο αποδέκτης του video είναι ένας απλός υπολογιστής με σύνδεση στο δίκτυο (Set Top Box, STB). Ο VS και το STB είναι ουσιαστικά τα τερματικά, όσον αφορά το δίκτυο μεταφοράς.

Το video που θα μεταφερθεί επιλέγεται από τον χρήστη αλληλεπιδραστικά. Αρχικά ο χρήστης επιλέγει έναν SP, ο οποίος έχει το επιθυμητό περιεχόμενο και στη συνέχεια, μέσω του SP επιλέγει το συγκεκριμένο video που θέλει να δει. Στην πρώτη φάση το STB πρέπει να πιστοποιηθεί στο δίκτυο και να εξακριβωθεί αν μπορεί να έχει πρόσβαση στον συγκεκριμένο SP. Έπειτα, ο χρήστης επιλέγει το video που τον ενδιαφέρει από τον SP και ένας VS αναλαμβάνει την αποστολή του.

Διαδικασίες Παροχής Υπηρεσιών

Για την παροχή της υπηρεσίας ανάκτησης video κατά απαίτηση ακολουθείται η παρακάτω διαδικασία:

Εγγραφή/Ενεργοποίηση Υπηρεσιών

Στην φάση αυτή ο χρήστης πρέπει να αποκτήσει πρόσβαση στο δίκτυο μέσω ενός Παροχέα Δικτύου (Network Provider, NP). Ο χρήστης επιλέγει σε ποιους SP επιθυμεί να έχει πρόσβαση και εγγράφεται στις υπηρεσίες που προσφέρουν. Κατά την εγγραφή ο χρήστης παραθέτει στοιχεία που τον αφορούν και τα οποία μπορεί να ενδιαφέρουν το δίκτυο (ταυτότητα, τύπος τερματικού, κτλ)

Εγκατάσταση Υπηρεσίας

Η φάση αυτή αποτελείται από τα παρακάτω βήματα:

1. Το λογισμικό του πελάτη του παρέχει τη δυνατότητα να περάσει στην φάση επιλογής.
2. Ανοίγει ένα κανάλι επικοινωνίας για ένα πρώτο επίπεδο επιλογής, μέσα από το οποίο ο χρήστης επιλέγει SP.
3. Ο χρήστης έχει επιλέξει SP και ακολουθεί μια διαδικασία πιστοποίησης κατά την οποία εξακριβώνεται αν ο χρήστης έχει δικαίωμα χρήσης της υπηρεσίας του συγκεκριμένου SP.
4. Αν επιτύχει η πιστοποίηση, ο χρήστης περνάει σε μια δεύτερη φάση επιλογής, αυτή την φορά με τον SP, ώστε να επιλεχθεί το video που αυτός επιθυμεί.
5. Ανοίγει ένα κανάλι πολυμέσων και ένα κανάλι επιλογής με τον VS που έχει το video μέσα από το οποίο (κανάλι) γίνεται η μεταφορά του και ο έλεγχος της προβολής του.

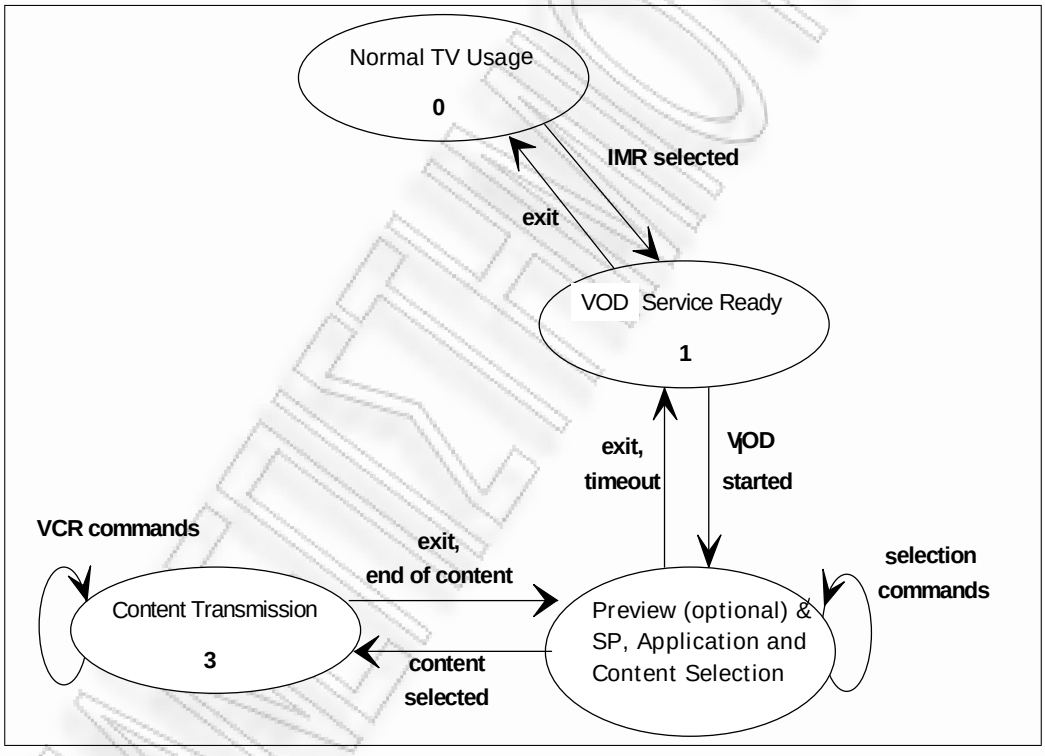
6. Αποδέσμευση Υπηρεσίας: Με την παύση του περιεχομένου ή την αντίστοιχη επιλογή του χρήστη, διακόπτεται η σύνδεση με το δίκτυο.

Διαγράμματα καταστάσεων

Η παραπάνω διαδικασία φαίνεται, με μεγαλύτερη λεπτομέρεια, στα διαγράμματα καταστάσεων που ακολουθούν.

Γενικό Διάγραμμα Καταστάσεων

Στην εικόνα 2.6 φαίνεται, από την αρχή ως το τέλος, η διαδικασία παροχής της υπηρεσίας αναπαραγωγής video κατά απαίτηση. Οι διάφορες καταστάσεις αναλύονται περαιτέρω σε μετέπειτα διαγράμματα.



Εικόνα 2.6: *Γενικό διάγραμμα καταστάσεων για την υπηρεσία VoD [27]*

Αναλυτικότερα υπάρχουν τις παρακάτω καταστάσεις:

0: Το STB είναι κλειστό. Η διαδικασία δεν έχει ακόμα αρχίσει.

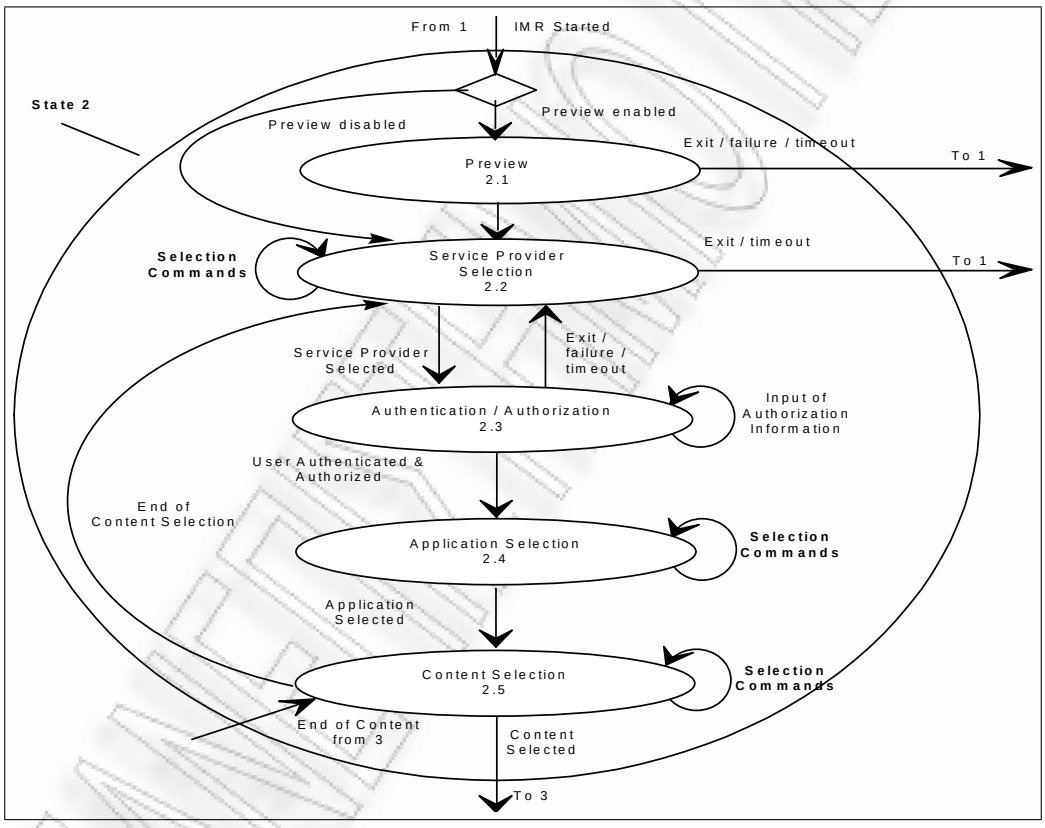
1: Αρχίζει η διαδικασία παροχής της υπηρεσίας.

2: Ο πελάτης επιλέγει τον SP και έπειτα το video που τον ενδιαφέρει από τον SP. Παράλληλα διενεργούνται διαδικασίες πιστοποίησης του πελάτη.

3: Γίνεται η μετάδοση του video που επέλεξε ο πελάτης. Ο πελάτης έχει τη δυνατότητα ελέγχου της ροής του (πάγωμα εικόνας, γρήγορη κίνηση, κλπ).

Διάγραμμα καταστάσεων επιλογής περιεχομένου

Στην εικόνα 2.7 φαίνονται αναλυτικότερα οι διαδικασίες που οδηγούν την επιλογή του video από τον χρήστη. Η εικόνα 2.7 αποτελεί ανάλυση της κατάστασης 1 του διαγράμματος της εικόνας 2.6.



Εικόνα 2.7: *Διάγραμμα καταστάσεων επιλογής SP και video από τον χρήστη*

Υπάρχουν οι παρακάτω διαδικασίες:

2.1: Ο χρήστης μπορεί (αν το επιτρέπει το δίκτυο) να παρακολουθήσει προεπισκοπήσεις των video χωρίς να συνδεθεί σε SP.

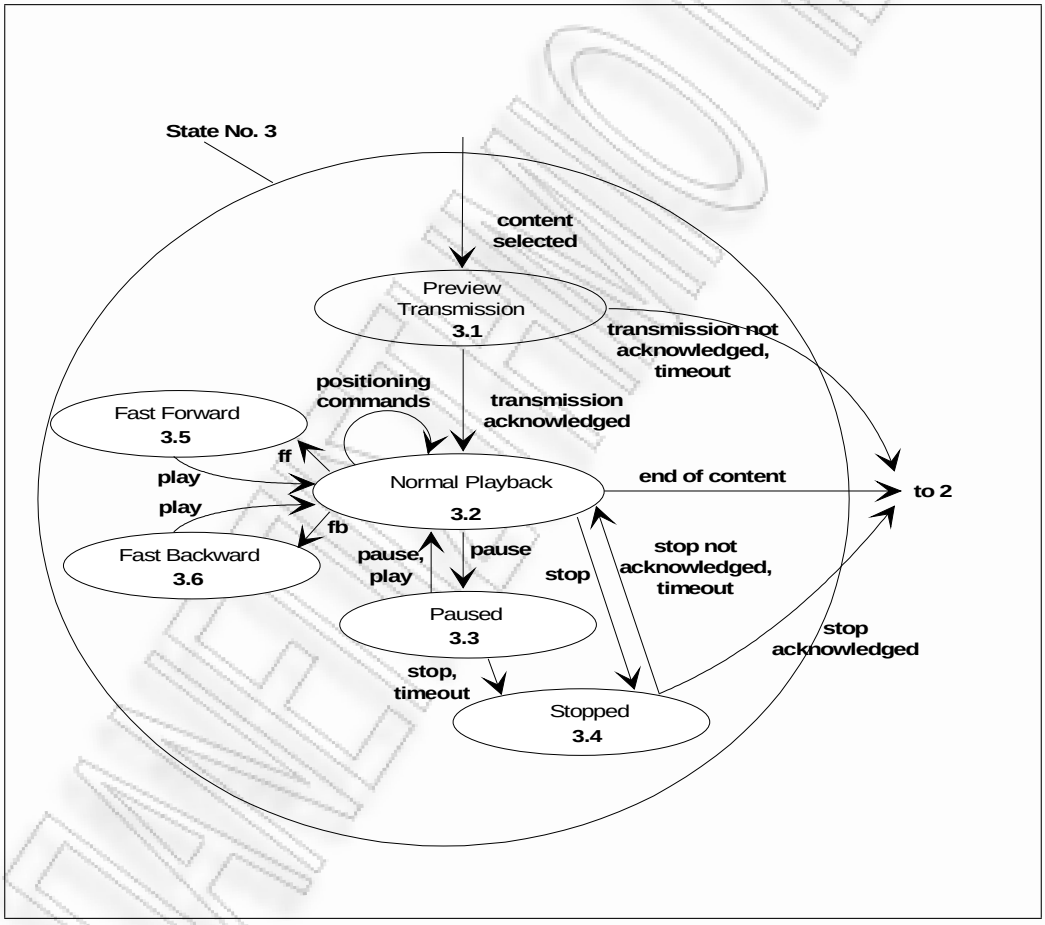
2.2: Λαμβάνεται μια λίστα με τους διαθέσιμους SP και ο χρήστης επιλέγει έναν από αυτούς.

2.3: Πιστοποιείται ο χρήστης από το δίκτυο και έπειτα ελέγχεται αν ο χρήστης έχει πρόσβαση στον επιλεγμένο SP.

2.5: Ο χρήστης επιλέγει το video από αυτά τα οποία έχει διαθέσιμα ο SP.

Διάγραμμα καταστάσεων μετάδοσης περιεχομένου

Στην εικόνα 2.8 φαίνεται αναλυτικότερα η διαδικασία κατά τη μετάδοση και την αναπαραγωγή του video από τον VS στο STB. Είναι η αναλυτικότερη περιγραφή της κατάστασης 3 της εικόνας 2.6.



Εικόνα 2.8: *Διάγραμμα καταστάσεων αναπαραγωγής video από τον χρήστη*

υπάρχουν οι παρακάτω καταστάσεις:

3.1: Το video μεταδίδεται για μικρό χρονικό διάστημα, περιμένοντας επι-

βεβαίωση από το χρήστη για συνέχεια.

3.2: Κανονική αναπαραγωγή του video.

3.3: Το video έχει παγώσει, μετά από εντολή του χρήστη, περιμένοντας εντολή για συνέχεια.

3.4: Έχει προηγηθεί η εντολή ¨stop¨. Η συνέχεια δίνεται ως εντολή από το χρήστη.

3.5: Έχει προηγηθεί η εντολή ¨fast forward¨ από το χρήστη. Το video παίζει σε γρήγορη ταχύτητα μέχρι κάποια νέα εντολή του χρήστη.

3.6: Έχει προηγηθεί η εντολή ¨fast backward¨ από το χρήστη. Το video παίζει σε γρήγορη ταχύτητα προς τα πίσω μέχρι κάποια νέα εντολή του χρήστη.

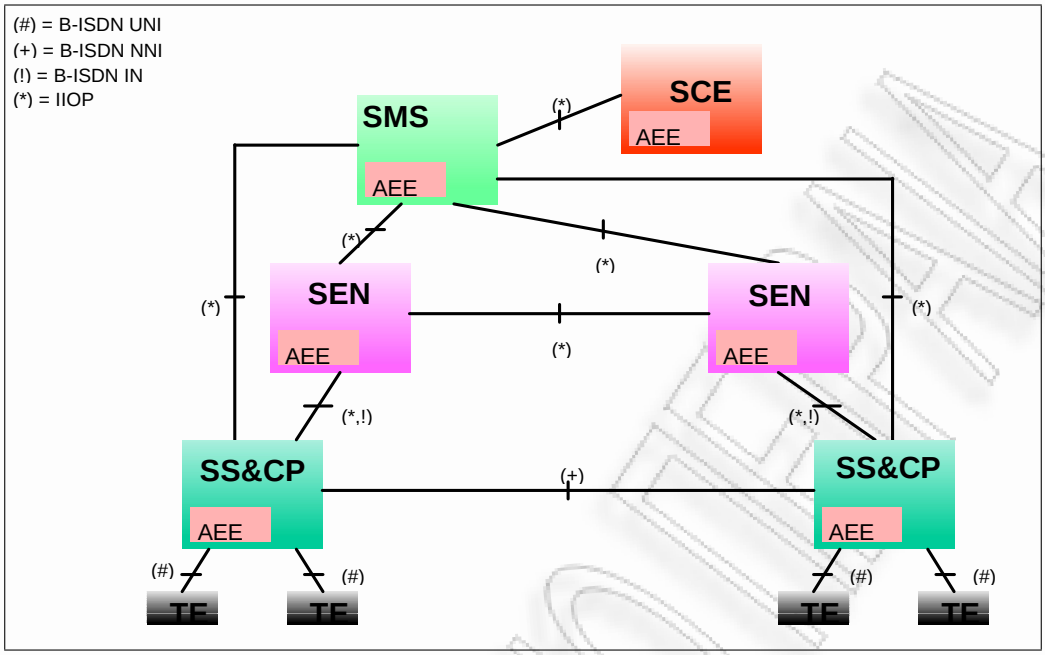
Περιγραφή Εφαρμογής

Το δίκτυο που χρησιμοποιήθηκε για την υπηρεσία αναπαραγωγής video κατά απαίτηση είναι σχεδιασμένο σύμφωνα με τις προδιαγραφές ενός Κατανεμημένου Ευφυούς συστήματος και περιγράφεται στην επόμενη ενότητα.

Περιγραφή του δικτύου

Το δίκτυο με το οποίο συνεργάζεται η όλη εφαρμογή είναι, όπως αναφέρθηκε, ένα Κατανεμημένο Ευφυές Δίκτυο. Το δίκτυο αυτό αποτελεί εξέλιξη του «Ευφυούς Δικτύου Ευρείας Ζώνης» σε ένα κατανεμημένο περιβάλλον, κάνοντας χρήση της αρχιτεκτονικής CORBA και την τεχνολογία των Κινητών Αντιπροσώπων. Η βασική αρχιτεκτονική του δικτύου φαίνεται στην εικόνα 2.9.

Όπως αναφέρθηκε, έχει γίνει χρήση των τεχνολογιών CORBA και MAT, σε μια προσπάθεια κατανομής των συστατικών του δικτύου. Με τον τρόπο αυτό τα τμήματα κώδικα των λειτουργικών οντοτήτων έχουν υλοποιηθεί ως προγραμματιστικά αντικείμενα και κατανέμονται μέσω της αρχιτεκτονικής CORBA σε ολόκληρο το δίκτυο. Η επικοινωνία μεταξύ τους, που αποτελεί ουσιαστικά



Εικόνα 2.9: *Αρχιτεκτονική Κατανεμημένου Ευφυούς Δικτύου*

την σηματοδοσία που υπάρχει μεταξύ των λειτουργικών οντοτήτων, γίνεται μέσω της CORBA. Με το σύστημα αυτό γίνεται ορατό στον προγραμματιστή σε ποια τοποθεσία βρίσκεται το κάθε αντικείμενο, είτε αυτό βρίσκεται τοπικά είτε σε κάποια απομακρυσμένη τοποθεσία.

Από την άλλη μεριά, ορισμένες λειτουργικές οντότητες έχουν υλοποιηθεί ως κινητοί αντιπρόσωποι. Ως αποτέλεσμα αυτού, τους δίνεται η δυνατότητα να αλλάζουν φυσική τοποθεσία αυτόματα όταν διαπιστωθεί φόρτος ή βλάβη στο δίκτυο, ενώ σε συνδυασμό με τη χρήση της CORBA ελαχιστοποιείται η μέριμνα του προγραμματιστή για τη νέα τοποθεσία της οντότητας.

Σηματοδοσία Εφαρμογής

Στην παρούσα εφαρμογή, το δίκτυο χρησιμοποιείται για την μετάδοση πολυμεσικών δεδομένων Multimedia Retrieval (IMR) και πιο συγκεκριμένα η βίντεο κατά απαίτηση (Video-on-Demand - VoD). Οι διαδικασίες που συμπεριλαμβάνει αυτή η υπηρεσία έχουν περιγραφεί στην ενότητα 2.1.3. Παρακάτω παρατίθενται οι απαραίτητες τροποποιήσεις για την ικανοποίηση των απαιτήσεων

που έχει μια τέτοια εφαρμογή.

Τα τερματικά του δικτύου έγιναν εκ των πραγμάτων ο δικτυακός υπολογιστής του πελάτη (Set Top Box, STB) και ο Παροχέας Video (Video Server, VS). Παράλληλα η λειτουργική οντότητα SRF ανέλαβε την καθοδήγηση του χρήστη στην επιλογή του Service Provider, ο οποίος για λόγους απλοποίησης ταυτίζεται με τον VS.

Επίσης, βασικό στοιχείο για την παροχή της υπηρεσίας αυτής σε ένα ΕΔ είναι η επικοινωνία μεταξύ των Λειτουργικών Οντοτήτων του δικτύου. Η επικοινωνία αυτή γίνεται μέσω μιας σηματοδοσίας, η οποία, στο δίκτυο, είναι υλοποιημένη ως κλήσεις CORBA εκτός ¨καναλιού¨ (out-of-band) μεταξύ των αντικειμένων που υλοποιούν τις λειτουργικές οντότητες. Η σηματοδοσία αυτή περιγράφεται αναλυτικότερα στο [27].

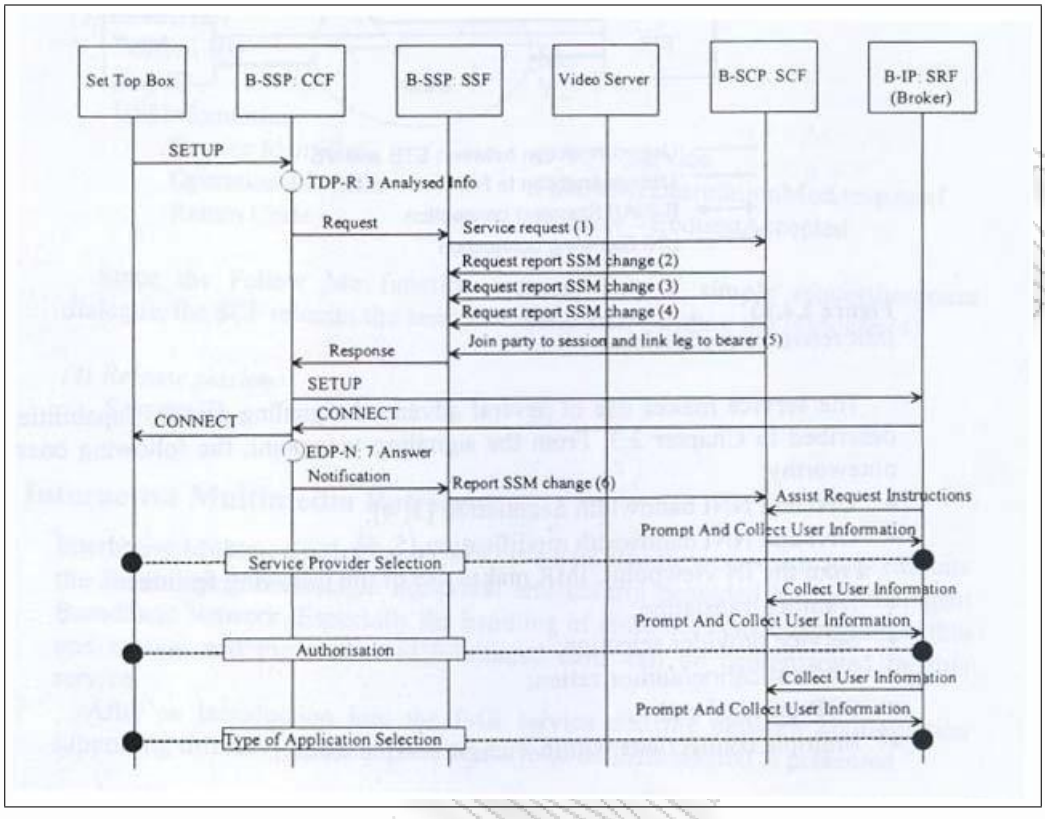
Παρακάτω περιγράφεται η σηματοδοσία μεταξύ των Λειτουργικών Οντοτήτων του δικτύου για την υλοποίηση της υπηρεσίας μετάδοσης video κατά απαίτηση.

Φάση 1, Βήμα 1

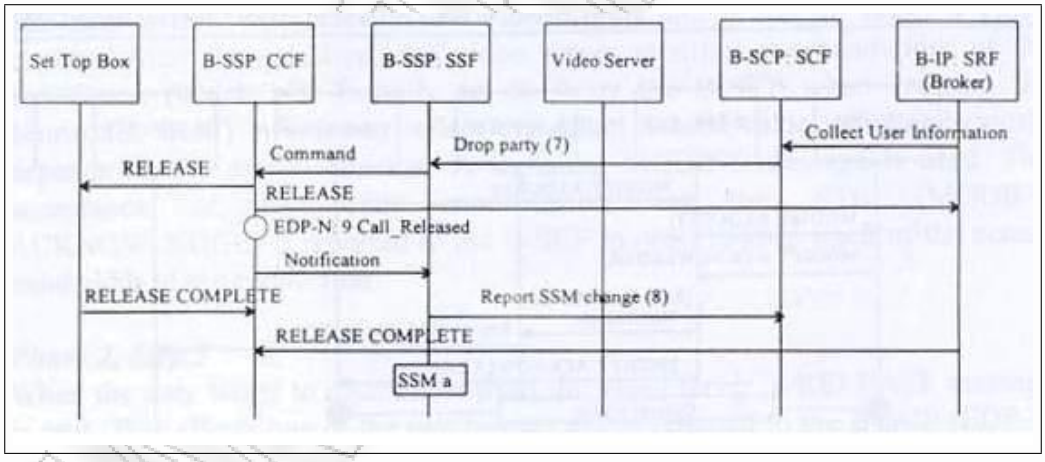
Το μήνυμα SETUP υποδηλώνει την επιθυμία του πελάτη για σύνδεση στο δίκτυο. Ως απάντηση, ο κόμβος B-SSP στέλνει ένα μήνυμα «Αίτησης Υπηρεσίας» στον κόμβο B-SCP και εγκαθιστά μια σύνοδο εκ μέρους του πελάτη. Αφού ενημερώνονται οι μηχανές καταστάσεων του SSM, ο κόμβος B-SSP δρομολογεί την κλήση στο B-IP (μήνυμα SETUP). Το B-IP απαντάει με CONNECT και ο B-SSP προωθεί το μήνυμα στο STB. Έπειτα ακολουθεί η επιλογή του VS και η πιστοποίηση του πελάτη (εικόνα 2.10).

Φάση 1, Βήμα 2

Η αποστολή του μηνύματος «Πληροφορίες Χρήστη» από το B-IP σημαίνει το τέλος της επιλογής VS και το μήνυμα RELEASE προωθείται στο STB. Αυτό απαντάει με RELEASE_COMPLETE και ολοκληρώνεται η αποδέσμευση της συνόδου (εικόνα 2.11).



Εικόνα 2.10: *Φάση 1, Βήμα 1 σηματοδοσίας [27]*

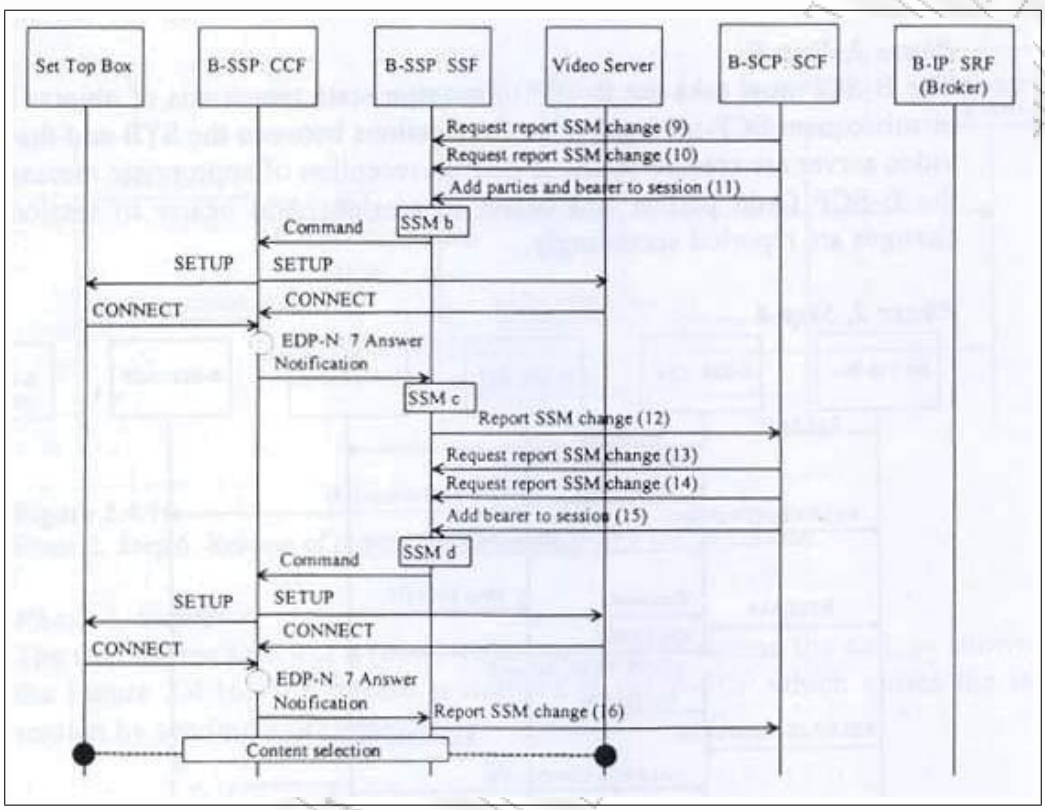


Εικόνα 2.11: *Φάση 1, Βήμα 2 σηματοδοσίας [27]*

Φάση 2, Βήμα 3

Το B-SCP ενημερώνεται για τις αλλαγές των καταστάσεων των αντικειμένων που συμμετέχουν στις επόμενες κλήσεις οι οποίες αρχικοποιούνται από

το SCP. Έπειτα με μια ακολουθία μηνυμάτων από το B-SCP δημιουργούνται οι ζεύξεις μεταξύ STB και VS και γίνεται η αναφορά αλλαγών καταστάσεων (εικόνα 2.12).



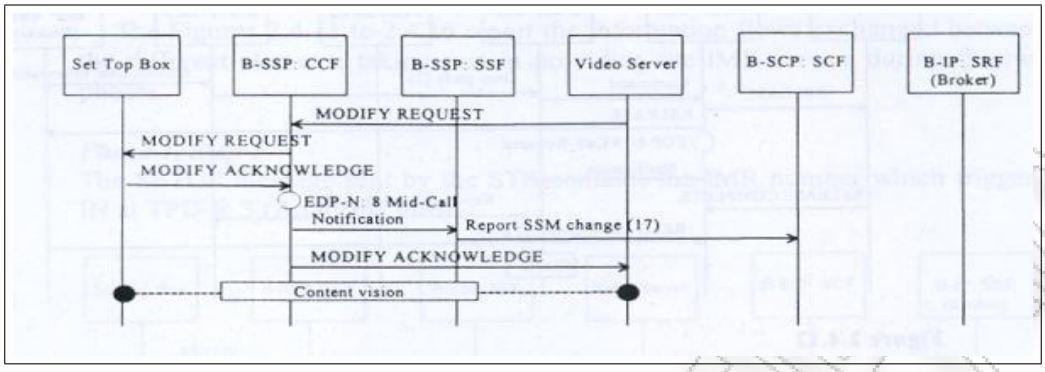
Εικόνα 2.12: *Φάση 2, Βήμα 3 σηματοδοσίας [27]*

Φάση 2, Βήμα 4

Ο χρήστης είναι συνδεδεμένος με τον VS και επιλέγει την ταινία που επιθυμεί να παρακολουθήσει, ενώ τροποποιείται το εύρος ζώνης που θα χρησιμοποιηθεί (εικόνα 2.13).

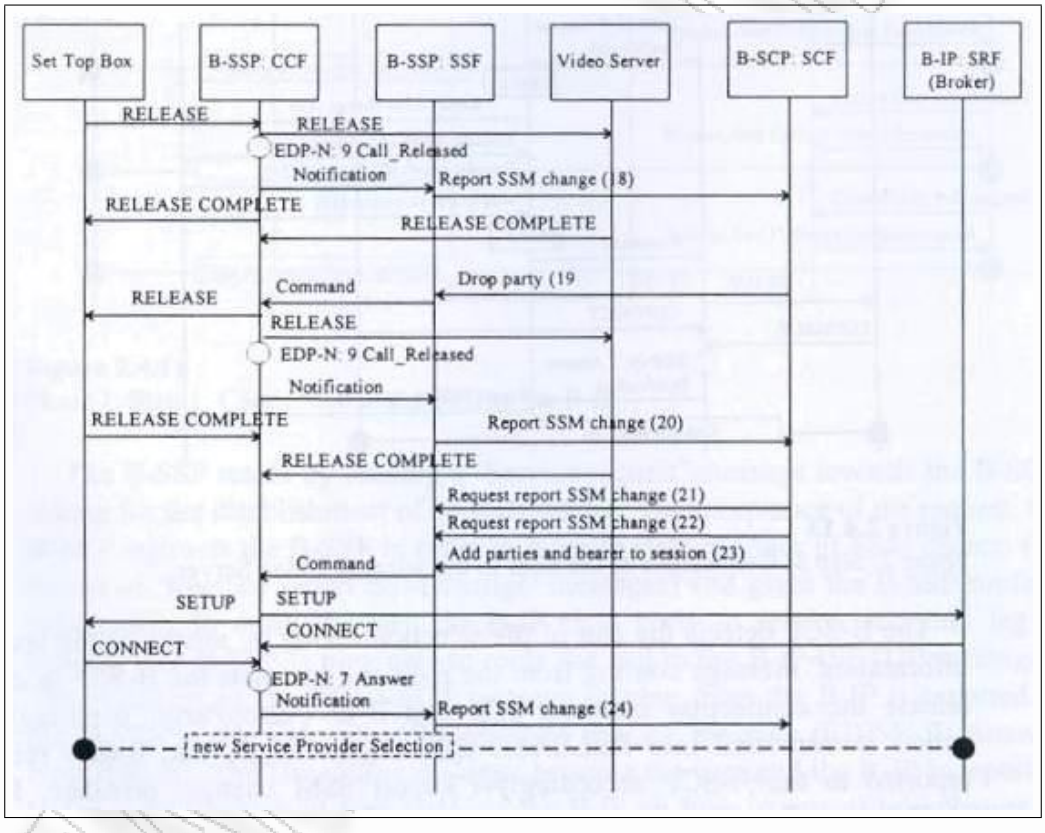
Φάση 2, Βήμα 5

Κατά την αποσύνδεση ο χρήστης αποστέλλει ένα μήνυμα RELEASE στο B-CCF. Η σύνδεση που απομένει αποδεσμεύεται μετά την αποστολή ενός μηνύματος ¨Αποδέσμευσε Μέλος¨ (Drop Party) από το B-SCP. Οι αλλαγές των καταστάσεων SSM αναφέρονται και το B-SCP είναι πλέον σε θέση να συνδέσει ξανά το χρήστη με το B-IP στέλνοντας ένα μήνυμα ¨Πρόσθεσε μέλη και φέρον



Εικόνα 2.13: *Φάση 2, Βήμα 4 σηματοδοσίας [27]*

στη σύνοδο¨ Add parties and bearer to session (εικόνα 2.14).

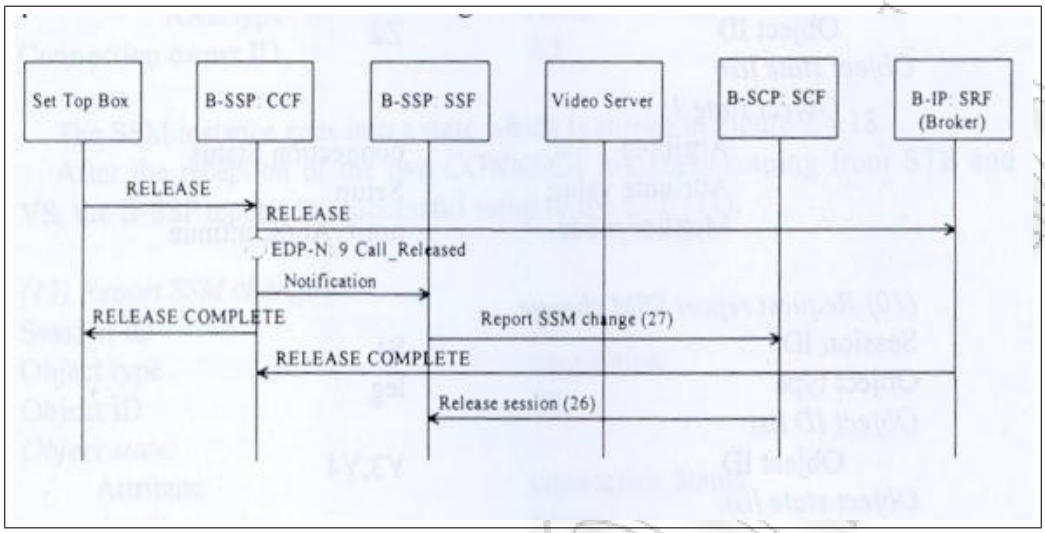


Εικόνα 2.14: *Φάση 2, Βήμα 5 σηματοδοσίας [27]*

Φάση 2, Βήμα 6

Ο χρήστης επιλέγει είτε σύνδεση σε άλλον VS ή αποδέσμευση της κλήσης. Η αποδέσμευση γίνεται με την αποστολή του ¨Αποδέσμευσε Σύνοδο¨ Release

session (εικόνα 2.15).



Εικόνα 2.15: *Φάση 2, Βήμα 6 σηματοδοσίας [27]*

2.2 Δίκτυα Ad Hoc

Ένα δίκτυο Ad Hoc δεν είναι τίποτα άλλο από μια συλλογή κινητών συσκευών που επικοινωνούν μεταξύ τους, χωρίς την ύπαρξη μιας προκαθορισμένης δομής και κάποιας κεντρικής διαχείρισης. Αν οι συσκευές που μετέχουν σε ένα τέτοιο δίκτυο έχουν πολύ περιορισμένες και ταυτόχρονα συγκεκριμένες *ικανότητες* τότε πρόκειται για ένα δίκτυο αισθητήρων (sensor). Αν μπορούν να κινούνται τότε πρόκειται για ένα κινητό δίκτυο Ad Hoc δηλαδή ένα Mobile Ad hoc NETwork (MANET).

Τα δίκτυα αυτού του είδους έχουν ενδιαφέρον καθώς αποτελούν πιθανές λύσεις χαμηλού κόστους σε μια πληθώρα εφαρμογών. Το χαμηλό, σχετικά, κόστος τους παρέχει τη δυνατότητα της δημιουργίας δικτύων ποικίλης μορφολογίας τα οποία μπορούν να εξυπηρετήσουν είτε στρατιωτικές είτε άλλου είδους εφαρμογές. Επιπλέον της ελεύθερης κινητικότητας, ένα δίκτυο τέτοιου είδους μπορεί να δημιουργηθεί γρήγορα, καθώς δεν στηρίζεται στην ύπαρξη σταθερής δομής.

Τα δίκτυα MANET εξαιτίας των χαρακτηριστικών τους είναι κατάλληλα για την υποστήριξη εφαρμογών όπως τα προσωπικά δίκτυα (π.χ. κινητά τηλέφωνα, laptops, πανεπιστημιακά δίκτυα κ.α.), στρατιωτικές εφαρμογές (π.χ. επικοινωνία στο πεδίο της μάχης μεταξύ στρατιωτών, αρμάτων, αεροπλάνων), εφαρμογές έκτακτης ανάγκης (π.χ. πυρόσβεση), καθώς και άλλες ιδιωτικές εφαρμογές (π.χ. επικοινωνία σε κάποιο στόλο ταξί, συνεδριάσεις, επικοινωνία σε θαλάσσιο περιβάλλον κ.α.).

2.2.1 Η Δρομολόγηση σε Δίκτυα MANET

Η δρομολόγηση αποτελεί τη διαδικασία εύρεσης κάποιου μονοπατιού/ δρόμου ανάμεσα σε δύο κόμβους και την ακόλουθη μεταβίβαση δεδομένων μεταξύ τους μέσω αυτού του δρόμου. Σε αντίθεση με τα συμβατικά δίκτυα, ένα κινητό

Ad Hoc δίκτυο χαρακτηρίζεται για τη δυναμική, και συνεχώς μεταβαλλόμενη τοπολογία του, λόγω της κινητικότητάς του [5]. Εξαιτίας αυτού του χαρακτηριστικού είναι δύσκολη η εύρεση μονοπατιών επικοινωνίας ανάμεσα σε δύο κόμβους του δικτύου.

Επιπλέον, στα δίκτυα αυτού του είδους υπάρχουν περιορισμοί όσον αφορά τους διαθέσιμους πόρους. Έτσι υπάρχουν περιορισμοί στο διαθέσιμο εύρος επικοινωνίας (bandwidth) και στην ενέργεια που διαθέτει ο κάθε κόμβος (η οποία προέρχεται συνήθως από κάποια μπαταρία). Τα πρωτόκολλα δρομολόγησης που εφαρμόζονται σε αυτό το δίκτυο πρέπει να έχουν ελάχιστες απαιτήσεις τόσο σε ενέργεια, όσο και σε εύρος επικοινωνίας.

Άλλη πρόκληση για τη δρομολόγηση αποτελεί και το γεγονός ότι είναι δυνατόν το δίκτυο να πρέπει να λειτουργήσει μέσα σε εχθρικό περιβάλλον. Η ασφάλεια στην επικοινωνία θα πρέπει να ληφθεί σοβαρά υπόψη για τα δίκτυα αυτού του είδους που δεν διαθέτουν κανενός είδους καλωδίωση.

Στα δίκτυα MANET ο δρόμος, το μονοπάτι επικοινωνίας, μεταξύ δύο κόμβων μπορεί να περιλαμβάνει πολλούς ενδιάμεσους κόμβους (multihop). Έτσι, για τη μεταβίβαση των δεδομένων από ένα κόμβο-πηγή σε ένα κόμβο-προορισμό, ο κόμβος-πηγή θα πρέπει να βασιστεί στους γειτονικούς του κόμβους για τη μεταφορά των πακέτων του. Από αυτούς τους γείτονές του, αυτοί που βρίσκονται εντός της εμβέλειας του σήματός του (wireless transmission range) θα του δώσουν πληροφορίες για την τοπολογία γύρω του. Ακόμα και αυτοί που δεν βρίσκονται εντός της εμβέλειας του σήματός του ίσως χρειαστεί να μεταβιβάσουν το σήμα του μακρύτερα. Ο τρόπος αυτός λειτουργίας δημιουργεί θέματα ¨εγωισμού¨ στους κόμβους. Δηλαδή γιατί ένας κόμβος να θελήσει να μεταβιβάσει το πακέτο ενός άλλου, ποιο όφελος έχει αυτός;

Είναι δυνατόν οι κόμβοι που μετέχουν σε ένα δίκτυο MANET να μην έχουν όλοι τις ίδιες ικανότητες και *υπευθυνότητες*. Αν υπάρχουν ασύμμετρες ικανότητες σημαίνει ότι δεν έχουν όλοι οι κόμβοι τις ίδιες ιδιότητες λειτουργίας. Έτσι,

μπορεί να υπάρχουν διαφορές όσον αφορά την ακτίνα ραδιοεκπομπής τους και κατά συνέπεια το εύρος της επικοινωνίας. Μπορεί ακόμα να υπάρχουν διαφορές στην ενέργεια που έχει ο καθένας και στην υπολογιστική ισχύ τους. Τέλος είναι δυνατόν να διαφέρει και η ταχύτητα με την οποία κινούνται στο περιβάλλον τους. Αν υπάρχουν ασυμμετρίες όσον αφορά τις υπευθυνότητες του καθενός (δηλαδή των ρόλων που καλούνται να παίξουν μέσα στο δίκτυο), τότε μπορεί μόνο μερικοί κόμβοι να προωθούν πακέτα, να συμμετέχουν δηλαδή στη δρομολόγηση, ενώ κάποιοι άλλοι, απλά να συνδέονται στο δίκτυο μόνο όταν έχουν οι ίδιοι ανάγκη για επικοινωνία. Τα χαρακτηριστικά αυτά κάνουν τη δρομολόγηση στα δίκτυα (MANET) μια δύσκολη υπόθεση.

Σύμφωνα με τα ανωτέρω, η δημιουργία ενός πρωτοκόλλου δρομολόγησης που θα εφαρμόζεται στα δίκτυα MANET αποτελεί συνάρτηση πολλών παραγόντων, όπως της διαφοροποίησης στις ικανότητες & υπευθυνότητες των κόμβων, της διαφοροποίησης στην ταχύτητα, στην παραγωγή δεδομένων κ.α., της διαφοροποίησης στα κριτήρια επίδοσης (π.χ. μεγιστοποίηση του ρυθμού μεταφοράς δεδομένων, μείωση της κατανάλωσης ενέργειας).

Σε ένα τόσο πολύπλοκο και μεταβαλλόμενο περιβάλλον είναι φανερό ότι δεν υπάρχει μια λύση, όσον αφορά τη δρομολόγηση, που να καλύπτει όλες τις ποικιλίες και τα χαρακτηριστικά του δικτύου. Αυτός είναι και ο λόγος που έχουν προταθεί στη βιβλιογραφία πολλά και διαφορετικά πρωτόκολλα δρομολόγησης (DSR, AODV, SECMR).

2.2.2 Πρωτόκολλα Δρομολόγησης των Δικτύων MANET

Τα πρωτόκολλα δρομολόγησης που εφαρμόζονται στα δίκτυα Ad Hoc κατηγοριοποιούνται σύμφωνα με τη στρατηγική που ακολουθούν στη διαδικασία ανακάλυψης μονοπατιών επικοινωνίας. Έτσι υπάρχουν τα πρωτόκολλα αντίδρασης (reactive), στα οποία η διαδικασία ανακάλυψης νέων μονοπατιών πυροδοτείται μόνο τη στιγμή που προκύπτει η ανάγκη επικοινωνίας ανά-

μεσα σε δύο κόμβους και όχι εκ των προτέρων. Τα πρωτόκολλα αυτά συχνά συναντώνται στη βιβλιογραφία είτε ως κατ' αίτηση (on demand) ή σαν πρωτόκολλα αρχικοποιούμενα από την πηγή (source initiated). Σε αντίθεση με τα πρωτόκολλα αντίδρασης υπάρχουν και τα προδραστικά πρωτόκολλα (proactive), κατά τα οποία ο κάθε κόμβος διατηρεί πληροφορίες για τη δρομολόγηση προς άλλους κόμβους ακόμα και πριν αυτή καταστεί αναγκαία. Τα πρωτόκολλα αυτά ονομάζονται και πρωτόκολλα οδηγούμενα από πίνακα (table driven) [1, 2, 3].

Το κάθε είδος παρουσιάζει τα δικά του πλεονεκτήματα και μειονεκτήματα. Τα προνοητικά παρουσιάζουν γενικά χαμηλότερη καθυστέρηση καθώς τα μονοπάτια διατηρούνται στον πίνακα δρομολόγησης. Τα πρωτόκολλα αντίδρασης καταναλώνουν (έστω και ελάχιστο) χρόνο ώστε να βρεθεί το μονοπάτι επικοινωνίας κάθε φορά που αυτό χρειάζεται. Τα προδραστικά μπορεί να προσθέτουν μεγαλύτερο βάρος στο δίκτυο, λόγω των μηνυμάτων δρομολόγησης (overhead) που πρέπει να ανταλλάξουν σε τακτά χρονικά διαστήματα, ενώ τα πρωτόκολλα αντίδρασης reactive φαίνεται να μη διατρέχουν αυτόν τον κίνδυνο.

Αν η στρατηγική του πρωτοκόλλου επιβάλλει την ύπαρξη των μονοπατιών δρομολόγησης πριν τη προώθηση των δεδομένων τότε τα πρωτόκολλα χαρακτηρίζονται ως *μονής φάσης*, ενώ σε αντίθετη περίπτωση ως *διπλής φάσης*. Τα πρωτόκολλα μονής φάσης περιλαμβάνουν δεδομένα στη διαδικασία δρομολόγησης. Τα πακέτα δεδομένων προκειμένου να φτάσουν στο προορισμό τους δεν ακολουθούν ένα προσυμφωνημένο/ προκαθορισμένο μονοπάτι. Το κάθε πακέτο δεδομένων μπορεί να έχει ακολουθήσει τελείως διαφορετικό δρόμο προς τον προορισμό. Τα πρωτόκολλα διπλής φάσης, λειτουργούν σε δύο φάσεις (εξ ου και το όνομά τους). Στη πρώτη φάση πραγματοποιείται η εύρεση /διαχείριση των μονοπατιών δρομολόγησης και στη δεύτερη φάση προωθούνται τα δεδομένα μέσα από κάποιο/α από τα ανακαλυφθέντα

μονοπάτια.

Ένα άλλο κριτήριο κατηγοριοποίησης των πρωτοκόλλων δρομολόγησης είναι ο αριθμός των μονοπατιών που ανακαλύπτονται κατά τη διάρκεια μιας αίτησης δρομολόγησης (route request). Έτσι μπορεί να χωριστούν σε πρωτόκολλα μονού μονοπατιού (*π.χ.* [6, 10]) και σε πρωτόκολλα πολλαπλών μονοπατιών (multipath) (*π.χ.* [11, 9]).

Τα τελευταία μπορούν να διακριθούν περαιτέρω με κριτήριο τον αριθμό των ανακαλυφθέντων μονοπατιών που χρησιμοποιούνται τελικά για την κυκλοφορία των δεδομένων. Έτσι, ενώ μερικά πρωτόκολλα πολλαπλών μονοπατιών χρησιμοποιούν ένα μοναδικό μονοπάτι από τα ανακαλυφθέντα για την επικοινωνία, κάποια άλλα χρησιμοποιούν πολλαπλά μονοπάτια. Έτσι η μεταφορά των δεδομένων γίνεται με κατανεμημένο τρόπο.

Ένα άλλο χαρακτηριστικό των πρωτοκόλλων δρομολόγησης πολλαπλών μονοπατιών είναι οι συνθήκες που πρέπει να πληρούνται έτσι ώστε να ξεκινήσει η διαδικασία αναζήτησης νέων μονοπατιών. Η διαδικασία αυτή μπορεί να ξεκινήσει είτε όταν καταρρεύσει μόνο το ενεργό μονοπάτι (σε αυτή την περίπτωση η επικοινωνία πραγματοποιείται με κάποιο από τα εναλλακτικά μονοπάτια) ή όταν καταρρεύσουν όλα τα γνωστά μονοπάτια από μια πηγή προς έναν προορισμό [7].

Η διαδικασία αναζήτησης μπορεί να ολοκληρωθεί είτε όταν έχει βρεθεί ένας ικανοποιητικός αριθμός μονοπατιών, ή όταν έχουν βρεθεί όλα τα υπάρχοντα μονοπάτια. Τα τελευταία αυτά πρωτόκολλα είναι γνωστά ως *ολοκληρωμένα* πρωτόκολλα δρομολόγησης πολλαπλών μονοπατιών.

Τέλος, τα πρωτόκολλα δρομολόγησης πολλαπλών μονοπατιών χωρίζονται σε *μοναδικών/διακριτών κόμβων* (node-disjoint) [12] ή *μοναδικών/διακριτών ζεύξεων* (link-disjoint) [8] Στα μεν πρώτα κάθε μονοπάτι περιέχει μοναδικούς κόμβους του Ad Hoc δικτύου (δηλαδή κάθε κόμβος δεν μπορεί να συμμετέχει σε περισσότερα από ένα μονοπάτια). Στα δε δευτέρα, ένας κόμβος μπορεί να

περιέχεται σε περισσότερα μονοπάτια αλλά οι ζεύξεις μεταξύ των κόμβων θα πρέπει να είναι μοναδικές μεταξύ των μονοπατιών.

Τα πρωτόκολλα χρησιμοποιούν ποικίλα χαρακτηριστικά ώστε να πάρουν πληροφορίες για τον κόσμο γύρω τους. Η επιλογή του εκάστοτε χαρακτηριστικού καθορίζει και τον τρόπο λειτουργίας του πρωτοκόλλου. Έτσι υπάρχουν πρωτόκολλα που χρησιμοποιούν γεωγραφικές πληροφορίες ή πληροφορίες για το επίπεδο ενέργειας του κάθε κόμβου κ.λ.π. Ενώ κάποια άλλα επιβάλλουν την ύπαρξη διαφορετικών ρόλων/υπευθυνοτήτων στους κόμβους του δικτύου (leader clusters). Ανάλογα με τη στρατηγική δράσης τους, τα πρωτόκολλα δρομολόγησης χωρίζονται σε *συμμετρικά* και *ασύμμετρα*. Αν όλοι οι κόμβοι έχουν τον ίδιο ρόλο στη διαδικασία δρομολόγησης, τότε πρόκειται για ένα συμμετρικό πρωτόκολλο, διαφορετικά ένα ασύμμετρο.

2.2.3 Επιθέσεις στα πρωτόκολλα δρομολόγησης των MANET

Στα δίκτυα MANET η επικοινωνία μεταξύ κόμβων πραγματοποιείται με τη χρήση ασύρματου μέσου και επιπλέον κάθε κόμβος βασίζεται στους γειτονικούς του κόμβους για τη μετάδοση των δεδομένων του. Τα χαρακτηριστικά αυτά αποτελούν και τις βασικές αιτίες που τα πρωτόκολλα δρομολόγησης των δικτύων MANET δέχονται πολλές επιθέσεις που θέτουν σε κίνδυνο την ασφαλή λειτουργία όλου του δικτύου. Παρακάτω παρουσιάζονται οι κυριότερες από αυτές τις αιτίες.

Πλημμύρα

Ο κύριος σκοπός της επίθεσης της *Πλημμύρας* (flooding attack) [16] είναι να εξαντλήσει τους πόρους του συστήματος (π.χ. το διαθέσιμο εύρος επικοινωνίας), να καταναλώσει τους διαθέσιμους πόρους ενός κόμβου (π.χ. υπολογιστική ισχύ, ενέργεια), ή να διακόψει τη λειτουργία δρομολόγησης ώστε να προκαλέσει ελάττωση της επίδοσης του δικτύου. Για παράδειγμα, στο πρωτόκολλο AODV [13], ένας κακόβουλος κόμβος μπορεί να στείλει ένα μεγάλο αριθμό

από μηνύματα αίτησης εύρεσης μονοπατιού δρομολόγησης (RREQ) μέσα σε μικρό χρονικό διάστημα. Προορισμός αυτών των μηνυμάτων είναι κάποιος ανύπαρκτος κόμβος. Επειδή κανένας κόμβος δε θα απαντήσει ποτέ σε αυτά τα μηνύματα, αυτά θα συνεχίσουν να κατακλύζουν ολόκληρο το δίκτυο. Σαν αποτέλεσμα, η ενέργεια καθώς και το εύρος επικοινωνίας θα καταναλωθούν και θα προκληθεί μια επίθεση άρνησης υπηρεσίας. Η πτώση της επίδοσης του δικτύου μπορεί να είναι μέχρι και 84% [17].

Μαύρη Τρύπα

Στην επίθεση της *Μαύρης Τρύπας* (blackhole), ένας κακόβουλος κόμβος αποστέλλει ψεύτικες πληροφορίες δρομολόγησης, ισχυριζόμενος ότι διαθέτει ένα βέλτιστο μονοπάτι, προκαλώντας έτσι τους καλούς κόμβους να δρομολογούν τα πακέτα τους διαμέσω κακόβουλων κόμβων. Για παράδειγμα, στο πρωτόκολλο AODV, ο επιτιθέμενος μπορεί να στείλει μηνύματα απάντησης δρομολόγησης (RREP) (περιλαμβάνοντας και έναν ψεύτικο αύξοντα αριθμό, ο οποίος παρουσιάζεται να είναι μεγαλύτερος ή ίσος με αυτόν που περιέχεται στο μήνυμα εύρεσης μονοπατιού) στον κόμβο-πηγή, ισχυριζόμενος ότι διαθέτει ένα πολύ πρόσφατο μονοπάτι δρομολόγησης προς τον κόμβο προορισμού. Η λειτουργία αυτή έχει ως αποτέλεσμα, ο κόμβος πηγής να επιλέγει να προωθεί τα πακέτα δεδομένων του μέσω αυτού του μονοπατιού, το οποίο και διέρχεται μέσω του κακόβουλου κόμβου. Αυτό δίνει τη δυνατότητα στον επιτιθέμενο να καταχραστεί, είτε να καταστρέψει την επικοινωνία, αφού όλα τα δεδομένα θα διέρχονται από αυτόν.

Απόκρυψη Ζεύξης - Ψεύτικη Ζεύξη

Με την επίθεση της *Απόκρυψης Ζεύξης* (link withholding), ένας κακόβουλος κόμβος αγνοεί την υποχρέωση να διαφημίζει την ύπαρξη ζεύξεων προς κάποιους (ή κάποιον) κόμβους του δικτύου. Η συμπεριφορά αυτή οδηγεί σε απώλεια σύνδεσης με αυτούς τους κόμβους. Αυτό το είδος της επίθεσης είναι ιδιαίτερα επικίνδυνο στα πρωτόκολλα δρομολόγησης όπως π.χ. στο OLSR

[14].

Μια παραλλαγή της επίθεσης αυτής αποτελεί και η ανακοίνωση της ύπαρξης ψεύτικων ζεύξεων προς κόμβους. Στην επίθεση, που ονομάζεται *Εξαπάτηση Ζεύξης* (link spoofing), ένας κακόβουλος κόμβος ανακοινώνει την ύπαρξη ψεύτικων ζεύξεων προς κόμβους, που στην πραγματικότητα δεν είναι γειτονές του. Για παράδειγμα, στο πρωτόκολλο δρομολόγησης OLSR, ένας επιτιθέμενος μπορεί να ανακοινώσει την ύπαρξη μιας ψεύτικης ζεύξης προς κάποιο κόμβο, ο οποίος βρίσκεται δυο βήματα μακριά από τον κόμβο-πηγή. Με τον τρόπο αυτό ο κακόβουλος κόμβος καταφέρνει να ξεγελάσει τον κόμβο-πηγή ώστε αυτός να χρησιμοποιεί μόνον αυτόν για την προώθηση των μηνυμάτων του. Ο κόμβος-πηγή νομίζει ότι ο κακόβουλος κόμβος αποτελεί τον μοναδικό άμεσο γείτονά του, ο οποίος έχει ζεύξεις προς τους περισσότερους κόμβους που απέχουν δυο βήματα από την πηγή. Με τη συμπεριφορά αυτή ο κακόβουλος κόμβος μπορεί να ελέγξει τα δεδομένα ή την γενικότερη κίνηση πακέτων, π.χ. με την αλλαγή ή απόρριψη πακέτων δρομολόγησης.

Επανάληψη

Στα δίκτυα MANET, η τοπολογία αλλάζει συχνά λόγω της κινητικότητας των κόμβων. Αυτό σημαίνει ότι η εικόνα που έχουν οι κόμβοι για την τοπολογία του περιβάλλοντός τους δεν διατηρείται σταθερή. Στην επίθεση της *Επανάληψης* (replay) [19], ένας κόμβος μπορεί να καταγράφει τα μηνύματα ελέγχου δρομολόγησης που εκπέμπει ένας νόμιμος κόμβος και να τα επανεκπέμπει κάποια άλλη χρονική στιγμή. Η συμπεριφορά αυτή αναγκάζει τους άλλους νόμιμους κόμβους να γεμίζουν τους πίνακες δρομολόγησης τους με άκυρα δρομολόγια. Η επίθεση αυτού του είδους μπορεί χρησιμοποιηθεί ώστε ο κακόβουλος κόμβος να πλαστογραφήσει την ταυτότητά του στο δίκτυο ή για να διαταράξει την όλη επικοινωνία.

Σκουλικότρυπα

Η επίθεση *Σκουλικότρυπας* (Wormhole) [21] αποτελεί ένα από τα σοβα-

ρότερα είδη επίθεσης στα δίκτυα MANET. Σε επιθέσεις τέτοιου είδους, ένα ζεύγος συνεργαζόμενων κακόβουλων κόμβων καταγράφουν τα πακέτα που ανταλλάσσονται σε κάποιο σημείο του δικτύου και στη συνέχεια τα επανεκπέμπουν σε άλλο σημείο του δικτύου, χρησιμοποιώντας κάποιο ιδιωτικό δίκτυο υψηλής ταχύτητας. Η σοβαρότητα αυτής της επίθεσης έγκειται στο γεγονός ότι μπορεί να εφαρμοστεί ενάντια σε όλες τις επικοινωνίες που παρέχουν αυθεντικότητα και εμπιστευτικότητα. Έστω, για παράδειγμα, ότι μηνύματα ελέγχου δρομολόγησης, που ανταλλάσσονται σε ένα σημείο του δικτύου, μεταφέρονται και επανεκπέμπονται σε άλλο σημείο πολύ μακρύτερα. Οι απομακρυσμένοι κόμβοι δημιουργούν εσφαλμένη εικόνα για τους γειτονικούς τους κόμβους.

Συνεργατική Παραποιημένη Μετάδοση

Στην επίθεση *Συνεργατική Παραποιημένη Μετάδοση* (colluding misrelay), πολλαπλοί επιτιθέμενοι κόμβοι συνεργάζονται ώστε να αλλάξουν ή να καταρρίψουν τη διαδικασία της δρομολόγησης στα δίκτυα MANET. Η επίθεση αυτή είναι δύσκολο να αναγνωριστεί με τις συνήθεις μεθόδους [15]. Έστω, για παράδειγμα, ότι υπάρχουν δύο κακόβουλοι κόμβοι, ο ένας ένα βήμα μακρυά και ο άλλος δυο βήματα (one and two hop away), τότε ο πλησιέστερος προς την πηγή κακόβουλος κόμβος προωθεί τα πακέτα κανόνικα (ώστε να μην γίνει αντιληπτός) προς τον άλλο κακόβουλο κόμβο, ο οποίος τα απορρίπτει. Η παρεμπόδιση της επικοινωνίας με αυτή τη συμπεριφορά μπορεί να φτάσει και σε ποσοστό 100% [18].

Βιβλιογραφία

[1] E. M. Royer and C. K. Toh, *A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks*, IEEE Pers. Commun., vol. 6, no. 2, 1999, pp. 46–55.

[2] P. G. Argyroudis and D. O''Mahony, *Secure Routing for Mobile Ad Hoc Networks*, IEEE Commun. Surveys Tutorials, vol. 7, no. 3, 2005, pp. 2–21.

[3] H. Deng, W. Li, and D. P. Agrawal, *Routing Security in Wireless Ad Hoc Networks*, IEEE Commun. Mag., vol. 40, no. 10, 2002, pp. 70–75.

[4] Mobile Agent enviRonments in Intelligent NEtworks ftp://ftp.cordis.europa.eu/pub/infowin/docs/fr-340.pdf

[5] S. Ci et al., *Self-Regulating Network Utilization in Mobile Ad-Hoc Wireless Networks*, IEEE Trans. Vehic. Tech., vol. 55, no. 4, July 2006, pp. 1302–10.

[6] D.B. Johnson and D.A. Maltz, *Mobile computing*, ch. Dynamic source routing in ad-hoc wireless networks, pp. 152–181, Kluwer Academic Publishers, 1996.

[7] S-J Lee and M. Gerla, *Split multipath routing with maximally disjoint paths in ad hoc networks*, Proc. of ICC'01, IEEE, Jun 2001, pp. 3201–3205.

[8] M. Marina and S. Das, *Ad hoc on-demand multipath distance vector routing*, ACM Mobile Computing and Communications Review 6 (2002), no. 3, 92–93.

[9] A. Nasipuri and S.R. Das, *On-demand multipath routing for mobile ad hoc networks*, Proc. of INFOCOM'99, IEEE, 1999, pp. 64–70.

[10] C. Perkins, E. Royer, and S. Das, *Ad hoc on-demand distance vector routing*, Proc. of the Workshop on Mobile Computing Systems and Applications, IEEE, Feb 1999, pp. 90–100.

[11] A-P Subramanian, A. J. Anto, J. Vasudevan, and P. Narayanasamy, *Multipath power sensitive routing protocol for mobile ad hoc networks*, Proc. of the 1st IFIP/TC6 Working Conference on Wireless On-Demand Network Systems, (WONS'2004), LNCS, vol. 2928, Springer-Verlag, Jan 2004, pp. 171–183.

[12] Jie Wu, *An extended dynamic source routing scheme in ad hoc wireless networks*, Telecommunication Systems 1 (2003), no. 4, 61–75.

[13] C. Perkins, E. Belding-Royer, and S. Das, *Ad Hoc Ondemand Distance Vector (AODV) Routing*, IETF RFC 3561, July 2003.

[14] Th. Clausen et al., *Optimized Link State Routing Protocol*, IETF Internet draft, draft-ietf-manet-olsr-11.txt, July 2003.

[15] S. Marti et al., *Mitigating Routing Misbehavior in Mobile Ad Hoc Networks*, 6th MobiCom, Boston, MA, Aug. 2000.

[16] P. Yi et al., *A New Routing Attack in Mobile Ad Hoc Networks*, Int''l. J. Info. Tech., vol. 11, no. 2, 2005, p.p. 83–94.

[17] S. Desilva, and R. V. Boppana, *Mitigating Malicious Control Packet Floods in Ad Hoc Networks*, Proc. IEEE Wireless Commun. and Networking Conf., New Orleans, LA, 2005.

[18] B. Kannhavong et al., *A Collusion Attack Against OLSR-Based Mobile Ad Hoc Networks*, IEEE GLOBECOM ''06.

[19] 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.

[20] Y-C. Hu, A. Perrig, and D. Johnson, *Wormhole Attacks in Wireless Networks*, IEEE JSAC, vol. 24, no. 2, Feb. 2006.

[21] Loay Abusalah, Ashfaq Khokhar and Mohsen Guizani, *A Survey of Secure Mobile Ad Hoc Routing Protocols*, IEEE Communications Surveys & Tutorials, vol. 10, no. 4, October 2008.

[22] R. Brennan, B. Jennings, C. McArdle, and T. Curran, *Evolutionary Trends in Intelligent Network*, IEEE Commun. Mag., 38:6 (2000), 86–93.

[23] F. G. Chatzipapadopoulos, M. K. Perdikeas, and I. S. Venieris, *Mobile Agent and CORBA Technologies in the Broadband intelligent Network*, IEEE Commun. Mag., 38:6 (2000), 116–124.

[24] T.-C. Chiang, J. Douglas, V. K. Gurbani, W. A. Montgomery, W. F. Opdyke, J. Reddy, and K. Vemuri, *IN Services for Converged (Internet) Telephony*, IEEE Commun. Mag., 38:6 (2000), 108–114.

[25] I. Faynberg, L. R. Gabuzda, M. P. Kaplan, and N. J. Shah, The intelligent Network Standards: Their Application to Services, McGraw-Hill, New York, 1997.

[26] M. K. Perdikeas, F. T. Chatzipapadopoulos, I. S. Venieris, and G. Marino, *Mobile Agent Standards and Available Platforms*, Computer Networks, 31:19 (1999), 1999–2016.

[27] Venieris I. Hussmann H., *Intelligent Broadband Networks*, John Wiley & Sons, West Sussex England (1998).

[28] Kevin H. Liu, *Intelligent network control middleware platform*, IEEE Communications Magazine, vol. 43, no. 5, May 2005, pp. 11 - 18.

[29] Olga Ormond, *John Murphy and Gabriel-Miro Muntean Utility-based intelligent network selection in beyond 3G systems*, ICC 2006 - IEEE International Conference on Communications, no. 1, June 2006, pp. 1816 - 1821.

[30] Masami Yabusaki, *Takatoshi Okagawa and Kazuo Imai Mobility management in all-IP mobile network: End-to-end intelligence or network intelligence*, IEEE Communications Magazine, vol. 43, no. 12, Dec 2005, pp. 16 - 24.

Κεφάλαιο 3

Μελέτη Επίδοσης και Ασφάλεια

Τα Ευφυή δίκτυα και τα δίκτυα Ad Hoc, που παρουσιάστηκαν στο προηγούμενο κεφάλαιο, επιτρέπουν την ταχεία ανάπτυξη εφαρμογών, καθώς τα μεν πρώτα δε βασίζονται σε κάποια σταθερή υποδομή και τα δεύτερα έχουν διαχωρίσει τη λογική εκτέλεσης της υπηρεσίας από τον ίδιο τον έλεγχο. Στα Ευφυή Δίκτυα η υποστήριξη των παρεχομένων υπηρεσιών τους, π.χ. της IMR, προϋποθέτει την ύπαρξη κατάλληλης διαδικασίας χρέωσης προς τον τελικό χρήστη. Το περιβάλλον των δικτύων Ad Hoc είναι ιδιαίτερα χρήσιμο στις στρατιωτικές εφαρμογές, όπου η έλλειψη σταθερής υποδομής θεωρείται βέβαιη.

Γίνεται φανερό ότι η ασφάλεια στα δίκτυα αυτά είναι πολύ σημαντική, καθώς η έλλειψή της μπορεί να οδηγήσει από εσφαλμένη λειτουργία του δικτύου (π.χ. χρέωση) έως και σε κατάρρευσή του. Ένα πρωτόκολλο- δίκτυο θεωρείται ασφαλές όταν μπορεί να εξασφαλίσει τη διατήρηση των χαρακτηριστικών ασφάλειας που ισχυρίζεται ότι διαθέτει ακόμα και όταν δέχεται επίθεση από κακόβουλους χρήστες.

Παρακάτω μελετώνται τα χαρακτηριστικά ασφάλειας που θα πρέπει να έχει ένα πρωτόκολλο, το οποίο εφαρμόζεται στα ανωτέρω δίκτυα. Επίσης, αναλύονται οι τεχνικές μελέτης επίδοσης της ασφάλειας ενός πρωτοκόλλου.

Είναι σημαντικό να κατανοηθούν οι διάφορες τεχνικές ώστε να αναγνωριστεί το είδος των αποτελεσμάτων που μπορεί να εξαχθεί από καθεμιά τους, καθώς επίσης και κάτω από ποιες συνθήκες είναι καθεμιά τους κατάλληλη για χρήση.

Σκοπός του κεφαλαίου αυτού είναι η παρουσίαση των τεχνικών μελέτης επίδοσης καθώς και θεμάτων ασφάλειας που προκύπτουν στον υπό μελέτη χώρο των δικτύων, δηλαδή τα Ευφυή Δίκτυα και τα δίκτυα Ad Hoc. Συγκεκριμένα γίνεται παρουσίαση αναλυτικών και μη αναλυτικών μεθόδων μελέτης επίδοσης καθώς και των πιο σημαντικών εκπροσώπων αυτών. Στη συνέχεια αναλύονται θέματα ασφάλειας του χώρου των συγκεκριμένων δικτύων. Συγκεκριμένα περιγράφονται οι απαιτήσεις ασφάλειας που πρέπει να ικανοποιούν τα δίκτυα αυτά και τα είδη των επιθέσεων που έχουν καταγραφεί.

3.1 Μελέτη Επίδοσης

Μια εκτενής μελέτη της επίδοσης ενός συστήματος ασφάλειας θα πρέπει τυπικά να αξιολογεί την ικανότητά του να παρέχει ακρίβεια και αξιοπιστία ακόμα και κάτω από κακόβουλες/εχθρικές επιθέσεις. Μέχρι στιγμής δεν υφίσταται κάποια κοινώς αποδεκτή και τυπική διαδικασία μελέτης της επίδοσης δικτύων MANET και των διαδικασιών ασφάλειας που χρησιμοποιούν. Στη βιβλιογραφία έχουν παρουσιαστεί πολλά πρωτόκολλα ασφάλειας τα οποία, πολλές φορές, δεν περιλαμβάνουν κανενός είδους μελέτη επίδοσης. Η όποια διαδικασία μελέτης της επίδοσης μιας επιστημονικής ιδέας αποτελεί εξειδικευμένη προσπάθεια και έχει απαιτήσεις από πολλαπλά γνωστικά αντικείμενα, όχι μόνο από το συγκεκριμένο επιστημονικό χώρο από όπου προέρχεται η βασική ιδέα.

Στον πίνακα 3.1 παρουσιάζονται οι ποικίλες προσεγγίσεις που έχουν χρησιμοποιηθεί κατά καιρούς στην αξιολόγηση της επίδοσης ασφάλειας.

Πίνακας 3.1: *Σύγκριση Τεχνικών Μελέτης Επίδοσης - Ιδιότητες ασφάλειας*

Τεχνικές Μελέτης		Αναλυτικές			Μη Αναλυτικές	
		Τυπικές Μέθοδοι	Αναγωγή σε αξιόπιστα μοντέλα	Μαθηματικές αποδείξεις	Προσομοίωση	Παρατήρηση
Στοιχεία	Άτυπες Επιθέσεις	Ναι	Ναι	Όχι	Όχι	Ναι
	Εγγύηση ιδιοτήτων	Ναι	Ναι	Ναι	Όχι	Όχι
	Ασφάλεια άνευ όρων	Ναι	Όχι	Ναι	Όχι	Όχι
Πρακτική εφαρμογή		Λιγότερο δαπανηρή, Λιγότερο χρονοβόρα, μπορεί λιγότερο αξιόπιστη και ακριβείας λόγω υπερβολικής απλοποίησης του συστήματος			Προγραμματιστικά Χρονοβόρα, Χρονοβόρα στην εκτέλεση	Ακριβέστερη, Χρονοβόρα, Δαπανηρή (το σύστημα θα πρέπει να υπάρχει ήδη)

Οι κατηγορίες αυτές διαφοροποιούνται μεταξύ τους ανάλογα με την εμπλεκόμενη διαδικασία και το ποσό αξιοπιστίας που φέρουν τα εξαγόμενα αποτελέσματά τους. Οι τεχνικές που δεν βασίζονται άμεσα σε μαθηματικά **(μη αναλυτικές)** δεν ακολουθούν τυπικές διαδικασίες- κανόνες. Το παραγόμενο αποτέλεσμα με τη χρήση αυτών των τεχνικών είναι στενά συνυφασμένο με το υπό μελέτη πρόβλημα και τις συγκεκριμένες συνθήκες. Για το λόγο αυτό τα αποτελέσματά τους ενδέχεται να μη μπορούν να χρησιμοποιηθούν μελλοντικά στη μελέτη άλλων παραπλήσιων προβλημάτων. Επίσης, μπορεί να παρουσιάζουν διαφορές στις τιμές κάτω από διαφορετικές συνθήκες (π.χ. διαφορετικά σενάρια κίνησης στα κινητά δίκτυα, είτε διαφορετικά αποτελέσματα από ερευνητή σε ερευνητή). Καθώς η εξαγωγή αποτελεσμάτων μέσω της μη αναλυτικής μεθόδους της *παρατήρησης*, αποτελεί την ακριβέστερη επιστημονικά μέθοδο, αποτελεί ταυτόχρονα και την ακριβότερη από άποψη κόστους, αφού το σύστημα θα πρέπει να υπάρχει ήδη για να μελετηθεί. Επίσης η μελέτη επίδοσης με τη χρήση της μη αναλυτικής μεθόδου της *προσομοίωσης* μπορεί να είναι χρονοβόρα και προγραμματιστικά, αλλά και κατά τη διάρκεια της εκτέλεσής της. Εντούτοις αποτελεί τον πιο κοινό τρόπο αξιολόγησης ενός

συστήματος που βρίσκεται ακόμα και στη φάση του σχεδιασμού.

Οι περισσότερο **αναλυτικές** τεχνικές (*Μαθηματικές αποδείξεις*, *Αναγωγή σε αξιόπιστα μοντέλα*, *Τυπικές Μέθοδοι*) ακολουθούν μια πιο τυπικά δομημένη προσέγγιση, και τα εξαγόμενα συμπεράσματά τους παρουσιάζουν μεγαλύτερο βαθμό αξιοπιστίας. Ωστόσο, οι τεχνικές αυτού του είδους απαιτούν υψηλό βαθμό εξειδίκευσης. Έτσι, ενώ οι τεχνικές αυτού του είδους αποτελούν τις λιγότερο δαπανηρές από άποψη κόστους και τις περισσότερο αποτελεσματικές από άποψη αξιοπιστίας, εντούτοις μπορεί να αποδειχθούν εύκολα λαθεμένες. Είναι δυνατόν να καταναλωθεί μεγάλη προσπάθεια να ενταχθεί το σύστημα σε κάποιο από τα γνωστά μαθηματικά μοντέλα και στην προσπάθεια αυτή να γίνει υπερβολικά απλό σε βάρος της αξιοπιστίας και της ακρίβειας των εξαγόμενων αποτελεσμάτων.

Είναι σημαντικό να κατανοηθούν οι διάφορες τεχνικές μελέτης επίδοσης ώστε να αναγνωριστεί το είδος των αποτελεσμάτων που μπορεί να εξαχθεί από καθεμιά τους, καθώς επίσης και κάτω από ποιες συνθήκες είναι καθεμιά τους κατάλληλη για χρήση. Το πρώτο στοιχείο στον πίνακα 3.1 που εξετάζεται είναι οι *άτυπες επιθέσεις*. Το στοιχείο αυτό προσδιορίζει το αν μια τεχνική μελέτης επίδοσης μπορεί να αντιμετωπίζει τις επιθέσεις που δεν έχουν ακόμα καταγραφεί στη βιβλιογραφία, είτε περιορίζεται μόνο στην αναφορά/ή και αντιμετώπιση των γνωστών (και καταγεγραμμένων) επιθέσεων. Το δεύτερο στοιχείο, η *εγγύηση ιδιοτήτων*, προσδιορίζει το κατά πόσο μια τεχνική μελέτης επίδοσης μπορεί να παρέχει εγγυήσεις για την ύπαρξη των ιδιοτήτων ασφάλειας. Για παράδειγμα με δεδομένη μια ιδιότητα ασφάλειας μπορεί η τεχνική μελέτης επίδοσης να εγγυηθεί ότι ισχύει ιδιότητα ή όχι; Το τελευταίο στοιχείο του πίνακα 3.1, *ασφάλεια άνευ όρων*, αποτελεί την παροχή ασφάλειας όχι μόνο κάτω από ορισμένες συνθήκες. Ενώ μερικές προσεγγίσεις μπορούν να εξασφαλίσουν κάποιες ιδιότητες της ασφάλειας κάτω από ορισμένες συνθήκες, δεν υπάρχει τρόπος να εξακριβωθεί εάν ένα πρωτόκολλο είναι

άτρωτο σε επιθέσεις άγνωστες σε ένα μη περιορισμένο περιβάλλον.

Στη συνέχεια αυτής της ενότητας εξετάζονται αναλυτικότερα τα στοιχεία του πίνακα 3.1, καθώς αυτά χρησιμοποιούνται στις τεχνικές για τη μελέτη επίδοσης διαφόρων πρωτοκόλλων.

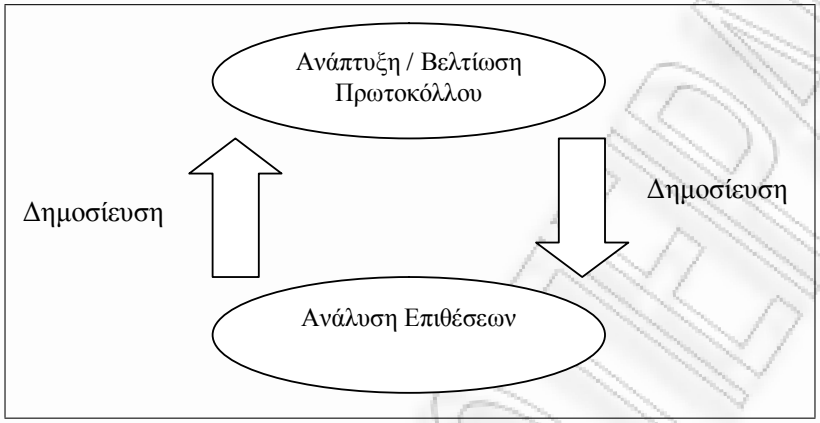
3.1.1 Μη Αναλυτικές τεχνικές μελέτης επίδοσης

Οι τεχνικές μελέτης επίδοσης που δεν χρησιμοποιούν αναλυτικές μεθόδους, τουλάχιστον όχι άμεσα, αποτελούν τις πιο χρονοβόρες από όλες τις μεθόδους και ίσως και τις πιο δαπανηρές. Εντούτοις προσφέρουν πολύτιμα συμπεράσματα. Η εξαγωγή συμπερασμάτων με τη μέθοδο της *οπτικής παρατήρησης* αποτελεί ίσως την ακριβέστερη από όλες τις μεθόδους αλλά και τη πιο δαπανηρή αφού για να παρατηρηθεί η συμπεριφορά ενός συστήματος, θα πρέπει πρώτα να υπάρχει ήδη αυτό το σύστημα. Τα αποτελέσματα της μελέτης επίδοσης με τη χρήση μοντέλων *προσομοίωσης* (διακριτών γεγονότων, είτε συνεχόμενων τιμών) μπορεί να αμφισβητούνται μερικές φορές, καθώς αυτά είναι συνδεδεμένα με τα χρησιμοποιούμενα σενάρια και το συγκεκριμένο ερευνητή που προγραμμάτισε το σύστημα. Εντούτοις παρέχουν πολύτιμα συμπεράσματα αφού μπορεί να χρησιμοποιηθούν από τη φάση του σχεδιασμού ακόμα και έτσι, να οδηγήσουν σε βελτιώσεις αδυναμιών που θα ήταν ορατές πολύ αργότερα, ίσως και κατά την εφαρμογή.

Παρατήρηση

Η τεχνική αυτή θεωρείται σαν συλλογή γενικών παρατηρήσεων/σχολίων (π.χ. οπτική παρατήρηση) της λειτουργίας ενός εφαρμοσμένου συστήματος. Η τεχνική αυτή αποτελεί τη λιγότερο κοπιαστική και την πιο παλαιά μέθοδο αξιολόγησης επίδοσης. Αποτελεί ίσως μια προσέγγιση δομημένης περιήγησης που έχει χρησιμοποιηθεί σε πρακτικές εφαρμογής λογισμικού [7]. Στην απλούστερή της μορφή, η οπτική παρατήρηση χρησιμοποιεί την ανθρώπινη ανάλυση και το ένστικτο ενός αναλυτή ή τα αποτελέσματα συζήτησης μεταξύ

των μελών μιας ομάδας ερευνητών. Παρά το γεγονός ότι δεν χρησιμοποιεί καμία εκτενή διαδικασία, εντούτοις αποτελεί μια ευρέως χρησιμοποιούμενη μέθοδο στην μελέτη επίδοσης ενός πρωτοκόλλου.



Εικόνα 3.1: *Μέθοδος μελέτης επίδοσης της Παρατήρηση*

Η οπτική παρατήρηση αποτελεί την επικρατέστερη μέθοδο για την έρευνα επιθέσεων ασφάλειας σε συστήματα/πρωτόκολλα που έχουν ήδη δημοσιευθεί στη βιβλιογραφία. Η εικόνα 3.1 παρουσιάζει τον επαναληπτικό τρόπο με τον οποίο λειτουργεί η μέθοδος αυτή. Υπάρχει μια συνεχής αλληλεπίδραση μεταξύ της ανάμεσα στη δημοσίευση ενός ασφαλούς πρωτοκόλλου, τη δημοσίευση ερευνών που τονίζουν τα σημεία αδυναμίας του πρωτοκόλλου, την αποδοχή και βελτίωση των σημείων αυτών και, τελικά, ξανά τη δημοσίευση του υπό κρίση πρωτοκόλλου. Η τεχνική αυτή έχει αξία και λογική ανάλογα με την αξία της αλληλεπίδρασης που υπάρχει. Βελτιώνεται συνεχώς όσο μεγαλύτερη ανάδραση λαμβάνει από την ερευνητική κοινότητα. Εντούτοις η οπτική παρατήρηση δεν μπορεί να παρέχει αξιοπιστία καθώς πολλά ευάλωτα πρωτόκολλα εμφανίζονται αρχικά ως άτρωτα. Η επιλογή αυτής της μεθόδου για την αξιολόγηση της επίδοσης ενός ασφαλούς πρωτοκόλλου μπορεί να έχει ολέθρια αποτελέσματα στην αξιοπιστία του ερευνητή καθώς η κατάρριψη των συμπερασμάτων της δεν είναι καθόλου απίθανη περίπτωση.

Ένα χαρατηριστικό παράδειγμα της μεθόδου αυτής αποτελεί η εξελικτι-

κή διαδικασία μεταξύ των πρωτοκόλλων DSR – > SRP –> Ariadne. Όταν δημοσιεύτηκε το πρωτόκολλο DSR [2] δε δόθηκε η ανάλογη σημασία στην ύπαρξη ασφάλειας, αλλά τονίστηκε περισσότερο η αποτελεσματικότητα του πρωτοκόλλου από την άποψη της δρομολόγησης. Τις αδυναμίες του πρωτοκόλλου DSR αναγνώρισε και αντιμετώπισε το πρωτόκολλο SRP [4]. Τέλος το πρωτόκολλο Ariadne [5] αποτελεί βελτίωση του SRP από άποψη ασφάλειας.

Προσομοίωση

Υπάρχουν διάφορα πακέτα προσομοίωσης δικτύων που χρησιμοποιούνται, όπως το NS-2 [28], το GloMoSIM [29], το OPNET [30], και το OMNET++ [32]. Το καθεστώς λειτουργίας τους ποικίλει. Μερικά από αυτά είναι λογισμικά ελευθέρου κώδικα, κάποια είναι εμπορικά πακέτα και κάποια ελεύθερα προς χρήση για ακαδημαϊκούς σκοπούς [31]. Τα διάφορα πακέτα προσομοίωσης ανάλογα με τον τρόπο που αντιμετωπίζουν τις αλλαγές στο εικονικό περιβάλλον τους διακρίνονται σε πακέτα διακριτών γεγονότων (discrete event), συνεχόμενων καταστάσεων (continuous) και υβριδικά (combined). Τα πρώτα μεταβάλλουν την κατάστασή τους μόνο στη περίπτωση όπου έχει πραγματοποιηθεί κάποιο γεγονός, σε αντίθεση με τα δεύτερα όπου η μεταβολή της κατάστασης τους γίνεται ακολουθώντας μια μεταβλητή που λαμβάνει συνεχιζόμενες τιμές. Το τρίτο είδος αποτελεί έναν συνδυασμό των δύο άλλων.

Η επιλογή της προσομοίωσης ως τεχνικής μελέτης της επίδοσης ενός δικτύου δεν αποτελεί μια εύκολη λύση, καθώς απαιτείται ένας συνδυασμός ικανοτήτων και γνώσεων. Έτσι χρειάζεται να υπάρχει καλή γνώση του επιστημονικού χώρου στον οποίο θα εφαρμοστεί η προσομοίωση ώστε να γίνει σωστή μοντελοποίηση. Στη συνέχεια θα πρέπει να γίνει η επιλογή του εργαλείου που θα χρησιμοποιηθεί, είτε αυτό αποτελεί κάποιο εργαλείο από τα ήδη υπάρχοντα, είτε να υλοποιηθεί ένα νέο. Στη φάση αυτή απαιτούνται προγραμματιστικές δεξιότητες. Αφού ολοκληρωθεί και η φάση της υλοποιήσης του μοντέλου, θα πρέπει να γίνει η αξιολόγηση των αποτελεσμάτων. Η φάση

αυτή αποτελεί ίσως και την πιο χρονοβόρα. Οι δεξιότητες που απαιτούνται εδώ προέρχονται κυρίως από το χώρο της στατιστικής. Χρειάζεται καλή γνώση των στατιστικών τεχνικών ώστε να επιλεγεί η κατάλληλη κάθε φορά, όπως για παράδειγμα το διάστημα εμπιστοσύνης (confidence intervals).

Η χρήση της προσομοίωσης ως τεχνικής μελέτης της επίδοσης ενός δικτύου παρουσιάζει και αδυναμίες στην ανακάλυψη νέων επιθέσεων και δεν μπορεί να εγγυηθεί τη διατήρηση των ιδιοτήτων ασφάλειας κάτω από οποιεσδήποτε συνθήκες. Οι επιθέσεις για τις οποίες θα εξετασθεί το εκάστοτε πρωτόκολλο θα πρέπει να είναι γνωστές εκ των προτέρων ώστε να προγραμματιστούν οι ενέργειες των επιτιθέμενου και να ενταχθούν στο πακέτο της προσομοίωσης. Επιπλέον, τα πακέτα προσομοίωσης αυτού του είδους χρησιμοποιούνται, κυρίως, για τη μελέτη της επίδοσης του δικτύου βασιζόμενα σε στατιστικές παρατηρήσεις μεμονωμένων εκτελέσεων (runs). Είναι επομένως δύσκολο να χρησιμοποιηθούν οι τεχνικές αυτές ώστε να απαντηθούν ερωτήματα (όπως: μια ιδιότητα ασφάλειας διατηρείται σε όλες τις συνθήκες ή όχι;) που δέχονται απόλυτες απαντήσεις, καθώς τέτοια ερωτήματα δεν ανέχονται στατιστικές αποκλίσεις ως απάντησή τους. Δηλαδή, επειδή μια επίθεση δεν είναι πιθανή δε σημαίνει ότι δε θα συμβεί στον πραγματικό κόσμο.

Τα πακέτα προσομοίωσης δικτύου δε χρησιμοποιούνται συνήθως για την μελέτη της επίδοσης αυτών καθαυτών ιδιοτήτων ασφάλειας, αλλά για τη γενικότερη μελέτη επίδοσης του συνόλου του δικτύου που επιδεικνύει ιδιότητες ασφάλειας. Για παράδειγμα το SEAD [6] έχει αναπτυχθεί ώστε να μελετηθεί το επιπλέον φορτίο (overhead) που παράγεται από την εφαρμογή κανόνων ασφάλειας στη διαδικασία δρομολόγησης σε σχέση με απλά πρωτόκολλα (π.χ. DSDV). Δηλαδή, η προσομοίωση δε δημιουργήθηκε ώστε να αξιολογήσει τις βελτιώσεις ασφάλειας που έχουν εφαρμοστεί στο SEAD, αλλά για να αξιολογήσει το πόσο αποδοτικό είναι το πρωτόκολλο στην εφαρμογή του.

Όταν χρησιμοποιούνται πακέτα προσομοίωσης για τη μελέτη της επίδο-

σης ενός πρωτοκόλλου ασφάλειας σε ένα δίκτυο συνήθως επικεντρώνονται στη μελέτη των επιπλέον διαδικασιών που εφαρμόζονται στη φάση της μετάδοσης των δεδομένων. Μετράται, δηλαδή, η επίδοση του πρωτοκόλλου σε σχέση με τις καθυστερήσεις που υφίστανται στη μετάδοση των δεδομένων, τις απώλειες πακέτων, και το ποσοστό των επιπλέον πακέτων ελέγχου που δημιουργούνται.

Η προσομοίωση ενός δικτύου μπορεί να μετρήσει την απόδοσή του ως προς το κόστος της επεξεργασίας των μηνυμάτων (overhead). Μπορεί, επίσης, να δώσει πολύτιμες πληροφορίες για το πώς αντιδρά το δίκτυο και οι μηχανισμοί ασφάλειας που χρησιμοποιεί, σε διάφορες κακόβουλες επιθέσεις. Η προσομοίωση ως μηχανισμός μελέτης της επίδοσης ενός ασφαλούς δικτύου παρέχει πληροφορίες για τον τρόπο που αντιδρά το δίκτυο όντας φορέας μηχανισμών ασφάλειας. Ωστόσο για να μετρηθεί το ποσοστό επιτυχημένης ή αποτυχημένης αντίδρασης του δικτύου κάτω από την πίεση κακόβουλων επιθέσεων, τότε η μέθοδος αυτή θα πρέπει να συνδυαστεί με κάποια άλλη (π.χ. της παρατήρησης). Μπορεί να χρησιμοποιηθεί σε συστήματα που βρίσκονται στο αρχικό στάδιο μελέτης τους, ακόμα και στον σχεδιασμό.

Η επιλογή των χαρακτηριστικών του δικτύου που επιλέγονται να μελετηθούν εξαρτάται από το υπό μελέτη σύστημα. Τα χαρακτηριστικά αυτά πρέπει να επιλεχθούν προσεκτικά καθώς μέσα από αυτά απεικονίζεται η συμπεριφορά του δικτύου. Έτσι π.χ. για τα πρωτόκολλα δρομολόγησης μελετώνται τα παρακάτω χαρακτηριστικά:

Μέση καθυστέρηση από άκρο σε άκρο (*Average end-to-end delay or mean overall packet latency*): Αποτελεί τη μέση καθυστέρηση που αντιλαμβάνεται ένα πακέτο από τη στιγμή που θα φύγει από τον αρχικό κόμβο έως την ορθή παραλαβή του από τον τερματικό κόμβο.

Χρόνος Εντοπισμού προορισμού (*Destination location time*): Είναι ο μέσος χρόνος που χρειάζεται ένα μήνυμα εύρεσης μονοπατιών να φτάσει στον

τερματικό κόμβο (προορισμό).

Χρόνος Διάδοσης αίτησης (*Request Propagation Time*): Αντιστοιχεί στον μέσο ολικό χρόνο που χρειάζεται ένα μήνυμα εύρεσης δρομολογίων ώστε να διαδοθεί σε όλο το δίκτυο. Αποτελεί ένα βασικό χαρακτηριστικό καθώς περιγράφει το φόρτο που επιβάλλει η διαδικασία εύρεσης δρομολογίων στη λειτουργία του δικτύου. Σε συσχέτιση με το χαρακτηριστικό *Χρόνος Εντοπισμού προορισμού*, περιγράφει το χρόνο που ένα μήνυμα εύρεσης δρομολογίων συνεχίζει να κυκλοφορεί/μεταναστεύει σε όλο το δίκτυο, και κατά συνέπεια, να καταναλώνει πόρους από το σύστημα, χωρίς αυτό να είναι απαραίτητο, αφού δεν προσθέτει κάτι στην εν γένει λειτουργία του πρωτοκόλλου δρομολόγησης.

Ποσοστό απόρριψης πακέτων (*Drop percentage*): Ορίζεται ως το ποσοστό των πακέτων που απορρίπτονται για διάφορους λόγους.

Φορτίο διαπερατότητας δρομολόγησης (*Routing throughput*): Περιγράφει την παραγωγή των πακέτων ελέγχου ολόκληρου του δικτύου ομαλοποιημένο ως προς τον αριθμό των κόμβων του δικτύου.

Γενικά ισχύει ότι τα αποτελέσματα της μελέτης της επίδοσης ενός δικτύου φαίνεται να παρουσιάζουν διαφορές κάτω από διαφορετικές συνθήκες (π.χ. διαφορετικά σενάρια κίνησης στα κινητά δίκτυα). Η επιλογή κάποιου από τα διαθέσιμα εργαλεία προσομοίωσης επηρεάζεται σε μεγάλο βαθμό από το πόσο δημοφιλής είναι στην επιστημονική κοινότητα. Καθώς η χρήση ενός γνωστού και κοινά αποδεκτού εργαλείου προσομοίωσης έχει το πλεονέκτημα ότι είναι γνωστές οι αδυναμίες του ίδιου του εργαλείου, οι οποίες μπορεί να έχουν κάποια επίδραση στην εκτιμώμενη συμπεριφορά του δικτύου. Επιπλέον παρέχεται η δυνατότητα ύπαρξης μιας κοινά (ακόμα και σιωπηρά) αποδεκτής πλατφόρμας σύγκρισης ανάμεσα στις διάφορες ερευνητικές εργασίες που παρουσιάζονται στη βιβλιογραφία. Ενώ αντίθετα η επιλογή ενός άγνωστου

εργαλείου αποδυναμώνει την αξιοπιστία των αποτελεσμάτων του. Ένα δημοφιλές εργαλείο έχει υποστεί κρίση και αξιολόγηση, επομένως έχει ενισχύσει, στις διάφορες εκδόσεις του, τα τυχόν τρωτά του σημεία. Επίσης σημαντικό κριτήριο επιλογής είναι και ο βαθμός υποστήριξης που διαθέτει το κάθε προσφερόμενο εργαλείο. Η υποστήριξη αυτή έχει να κάνει είτε με το πόσο λεπτομερές εγχειρίδιο χρήσης διαθέτει ή με την ύπαρξη κάποιου forum όπου μπορεί κάποιος να εκθέσει τις απορίες του και να βρει απαντήσεις. Τέλος, σημαντικά πλεονεκτήματα αποτελεί το εργαλείο να είναι ανοικτού κώδικα και να βρίσκεται σε καθεστώς ελεύθερης χρήσης. Όταν ο ερευνητής έχει πρόσβαση σε όλα τα τμήματα του κώδικα από τον οποίο είναι προγραμματισμένο το εργαλείο έχει τον έλεγχο του όλου συστήματος και μπορεί να εξάγει πολύτιμες γνώσεις όσον αφορά τον τρόπο αντίδρασης του υπό μελέτη δικτύου. Μπορεί να επέμβει και να πραγματοποιήσει βελτιώσεις σε όλα τα επίπεδα του δικτύου (π.χ. στο φυσικό επίπεδο) και όχι μόνο στο σημείο όπου έχουν εγκατασταθεί οι εφαρμογές ασφάλειας, π.χ. επίπεδο εφαρμογών.

3.1.2 Αναλυτικές τεχνικές μελέτης επίδοσης

Όπως αναφέρθηκε στον πίνακα 3.1 η χρήση των *μαθηματικών αποδείξεων*, της *αναγωγής σε αξιόπιστα μοντέλα* και των *τυπικών μεθόδων* μπορεί να αποδείξει την ύπαρξη η όχι μιας ιδιότητας ασφάλειας του δικτύου. Στην περίπτωση όπου η ιδιότητα ασφάλειας καταρρίπτεται (αναγωγής σε αξιόπιστα μοντέλα), μπορεί να εξαχθεί το συμπέρασμα ότι δεν ισχύει η συγκεκριμένη επίθεση, οπότε και να ανακαλυφθούν νέων ειδών επιθέσεις. Στην περίπτωση της χρήσης των τυπικών μεθόδων κάθε αποτυχία απόδειξης της ιδιότητας ασφάλειας θα οδηγήσει σε κατάρριψη όλου του πρωτοκόλλου και επίδειξη του τρόπου που λειτουργεί η συγκεκριμένη επίθεση.

Η χρήση των αναλυτικών μεθόδων, ως τεχνική μελέτης της επίδοσης ενός συστήματος, δεν αποκλείει τη χρήση και μη αναλυτικών μεθόδων, καθώς όταν

εξετάζεται ένα ζήτημα είναι καλύτερα να φωτίζεται από όλες του τις πλευρές. Η χρήση της προσομοίωσης, για παράδειγμα, ώστε να υπάρξουν ποικίλες τοπολογίες δικτύων και διαφορετικές επιθέσεις ενισχύει τα αποτελέσματα μιας έρευνας που έχει χρησιμοποιήσει αναλυτικές μεθόδους.

Μαθηματικές αποδείξεις

Η αναλυτική μέθοδος μελέτης της επίδοσης ενός δικτύου με τη χρήση μαθηματικών αποδείξεων, περιλαμβάνει τη χρησιμοποίηση θεωρημάτων, ιδιοτήτων και λημμάτων ώστε να αποδειχθεί (ή να καταρριφθεί) μια θεωρία για την ύπαρξη κάποιου είδους ασφάλειας στο σύστημα. Επιπλέον οι μαθηματικές αποδείξεις παρέχουν επαλήθευση για τις τυπικές μεθόδους που θα δούμε στη συνέχεια.

Για παράδειγμα οι Burmester, Le και Yasinsac [1] προτείνουν μια προσέγγιση πλέγματος-κυψέλης (cell-grid), όπου με τη χρήση μαθηματικών αποδεικνύουν την αποδοτικότητα και τις ιδιότητες ασφάλειας που έχουν πολλά συνεργαζόμενα (gossip) πρωτόκολλα. Τα πρωτόκολλα αυτού του είδους (gossip) ανήκουν στη κατηγορία των πρωτοκόλλων δρομολόγησης όπου το κάθε πακέτο δεδομένων βρίσκει το δικό του μονοπάτι προς τον προορισμό. Ο μηχανισμός αυτός βρίσκεται σε αντίθεση με τη δρομολόγηση κατά την οποία γίνεται διαχωρισμός της εύρεσης/διατήρησης του μονοπατιού επικοινωνίας προς κάποιο προορισμό και της προώθησης των πακέτων δεδομένων. Τα επιδημικά [1] (epidemic ή gossip) πρωτόκολλα εξασφαλίζουν την παράδοση των πακέτων των δεδομένων στον προορισμό τους, ακόμα και κάτω από την πίεση κακόβουλης επίθεσης, χρησιμοποιώντας τη τεχνική της πλημμύρας. Τα πακέτα των δεδομένων τα λαμβάνουν όλοι οι κόμβοι, ακόμα και αυτοί που ίσως δε θα έπρεπε (π.χ. κακόβουλοι), και όλοι οι κόμβοι τα προωθούν τουλάχιστον μια φορά έως ότου φτάσουν στον προορισμό τους. Με τη χρήση

[1] πρωτόκολλα κατά τα οποία ο κάθε κόμβος μεταδίδει τα πακέτα σε όλους ανεξαρτήτως τους γείτονές του. Κατά τρόπο ανάλογο με τη διάδοση κουτσομπολιών σε έναν εργασιακό χώρο.

τριγωνομετρικών συναρτήσεων αποδεικνύεται στο [1] ότι η μέγιστη ακτίνα ενός κελιού κάλυψης εκπομπής (transmission range) πρέπει να προσεγγίζει μια ορισμένη αριθμητική τιμή ώστε να μειώνεται στο ελάχιστο το φαινόμενο της πλημμύρας.

Παρά το γεγονός ότι η χρήση μαθηματικών στην υπηρεσία μελέτης της επίδοσης ενός δικτύου/εφαρμογής αποφέρει πολύτιμες πληροφορίες, υπάγεται, εντούτοις, σε κάποιους περιορισμούς. Κυρίως για το λόγο ότι για τη λειτουργία τους πραγματοποιούνται κάποιες υποθέσεις για το σύστημα, οι οποίες μπορεί να οδηγήσουν σε υπεραπλούστευση και στη συνέχεια σε έλλειψη ακριβείας. Επιπλέον, εξαρτώνται άμεσα από τις μαθηματικές ικανότητες του ερευνητή. Η χρήση μαθηματικών γίνεται πολυπλοκότερη όσο μεγαλύτερες είναι οι τοπολογίες που εξετάζονται και μπορεί πολύ εύκολα να μην αποδοθούν όλες οι αλληλεξαρτήσεις μεταξύ των οντοτήτων του συστήματος. Η έρευνα που γίνεται με τη χρήση μαθηματικών αποδείξεων δεν μπορεί εύκολα να μεταφερθεί και σε κάποιο άλλο επιστημονικό χώρο. Δηλαδή ό,τι έχει αποδειχθεί για ένα πρωτόκολλο (που λειτουργεί κάτω από συγκεκριμένες συνθήκες) δεν είναι υποχρεωτικό να ισχύει και για άλλο πρωτόκολλο. Όσο εξυπνότερη δε είναι μια απόδειξη τόσο μεγαλύτερος ο κίνδυνος παραπλάνησης.

Αναγωγή σε αξιόπιστα μοντέλα

Η αναλυτική μέθοδος της *αναγωγής σε αξιόπιστα μοντέλα* ακολουθεί μια γνωστή τεχνική που είχε χρησιμοποιηθεί στο παρελθόν για αποδείξεις σε κρυπτογραφικά συστήματα [9]. Κατά τη χρήση αυτής της μεθόδου ένα πρωτόκολλο αποδεικνύεται ασφαλές εάν μπορεί να αναχθεί σε κάποιο ιδεατό μοντέλο πρωτοκόλλου, ώστε εάν ένας κακόβουλος χρήστης δεν μπορέσει να επιδράσει στο ιδεατό πρωτόκολλο, δεν θα έχει επίδραση και στο πραγματικό. Το πλεονέκτημα αυτής της αναγωγής σε μοντέλα ιδεατού κόσμου είναι η προσθήκη ενός ¨σοφού¨ που έχει πλήρη γνώση του συστήματος (π.χ. της τοπολογίας του δικτύου). Η χρήση του ¨σοφού¨ καθιστά τον κάκοβουλο

χρήστη αδύναμο απέναντι στο ιδεατό πρωτόκολλο.

Οι Buttyan, Vajda και Acs προβάλλουν τη χρήση της αναγωγής σε ιδεατά-αξιόπιστα μοντέλα ώστε να αξιολογήσουν την ασφάλεια στη δρομολόγηση κατ' αίτηση πρωτοκόλλων (π.χ. DSR, SRP, Adriane) [3, 8] και επεκτείνουν τη μέθοδό τους σε κατ' αίτηση διανυσματικά πρωτόκολλα (π.χ. AODV, SAO-DV, ARAN) [10]. Ο πραγματικός και ο ιδεατός κόσμος έχουν αναχθεί με τη βοήθεια μιας βασικής-απλής μηχανής Turing σε μια στιγμή του χρόνου (π.χ. χωρίς την ύπαρξη κινητικότητας). Η μόνη διαφορά του πραγματικού και του ιδεατού κόσμου είναι ότι ο ιδεατός κόσμος ελέγχεται από ένα υψηλότερου επιπέδου μηχάνημα *T*. Το μηχάνημα *T* χρησιμοποιείται σαν ¨σοφός¨ και με τη γνώση που έχει για το σύστημα, ακυρώνει κάποια μονοπάτια. Η μηχανή που αναπαριστά τον ιδανικό κόσμο ¨μαθαίνει¨ το δίκτυο γύρω της παίρνοντας τα εξαγόμενα από τους κόμβους ως εισαγόμενα για τους γείτονές τους (π.χ. τα μηνύματα HELLO). Ένα μηχάνημα *H*, που αναπαριστά τα ανώτερα επίπεδα του πρωτοκόλλου, είναι υπεύθυνο για την εκκίνηση εύρεσης μονοπατιών και τη συλλογή των τελικών δρομολογίων επικοινωνίας. Τα δρομολόγια αυτά κατατάσσονται σε δύο σύνολα είτε Out_{real} είτε Out_{ideal}. Στον ιδεατό κόσμο χρησιμοποιείται η ολική γνώση του συστήματος ώστε να αποκλειστούν δρομολόγια από το σύνολο Out_{real}. Τελικώς το πρωτόκολλο είναι ασφαλές εάν ισχύει για τα δρομολόγια $Out_{real}=Out_{ideal}$.

Η χρήση της μεθόδου της αναγωγής σε ιδεατά/ αξιόπιστα μοντέλα για τη μελέτη της επίδοσης ενός δικτύου παρέχει πολύτιμες πληροφορίες. Δυστυχώς δεν παρέχει αποδείξεις για την ασφάλεια κάτω από όλες τις συνθήκες, καθώς περιορίζεται από περιβαλλοντικές υποθέσεις. Τονίζει τη διαφορά ανάμεσα στην αποδεδειγμένη ασφάλεια και στην ασφάλεια άνευ όρων. Καθώς ένα πρωτόκολλο θα παραμείνει ασφαλές όταν λειτουργεί σύμφωνα με κάποιες υποθέσεις, δεν είναι βέβαιο ότι το ίδιο θα ισχύει και όταν λειτουργήσει σε περιβάλλον χωρίς περιορισμούς (ανεξάρτητο από κάθε είδους σενάριο/έλεγχο).

Όταν τίθονται περιορισμοί/υποθέσεις για το σενάριο κάτω από το οποίο θα εφαρμοστεί ένα πρωτόκολλο τότε δεν υπάρχει ασφάλεια καθώς ένας κακόβουλος χρήστης μπορεί πολύ απλά να τις αγνοήσει.

Τυπικές μέθοδοι

Η χρήση των τυπικών μεθόδων αποτελεί άλλη μια αναλυτική τεχνική που, όμως, δεν έχει χρησιμοποιηθεί ευρέως στην ανάλυση των ιδιοτήτων ασφάλειας σε δίκτυα. Οι τυπικές μέθοδοι έχουν χρησιμοποιηθεί στα συστήματα ανάπτυξης λογισμικού, ως εργαλείο εξασφάλισης ακεραιότητας και αξιοπιστίας σε κρίσιμα συστήματα (π.χ. συστήματα ελέγχου πτήσεων, στρατιωτικά προγράμματα κ.α.) [11, 12]. Η χρήση των μεθόδων αυτών αποτελεί πολύτιμο εργαλείο στην αύξηση της αξιοπιστίας ενός συστήματος, ακόμα και αν δεν μπορούν να εγγυηθούν αυτήν την αξιοπιστία σε ποσοστό 100%.

Με τη χρήση της μεθόδου αυτής ένα σύστημα (π.χ. ένα πρωτόκολλο), καθώς και οι επιθυμητές ιδιότητές του (π.χ. ασφάλεια) ορίζονται με ακριβείς τυπικές μαθηματικές ή σημασιολογικές (semantic) έννοιες. Όταν έχει ολοκληρωθεί ο ορισμός αυτός τότε πραγματοποιείται η απόδειξη του παραγόμενου θεωρήματος (είτε ο έλεγχος του παραγόμενου μοντέλου) ώστε να μελετηθεί η λειτουργία του όλου συστήματος. Για την απόδειξη του παραγόμενου θεωρήματος περιλαμβάνονται τυπικές αποδείξεις που κάνουν χρήση τυπικών αξιωμάτων (ή κανόνων) και τυπικών σημασιολογικών εννοιών που έχουν οριστεί από την τυπική αυτή μέθοδο. Ωστόσο, όπως και στην περίπτωση των μαθηματικών αποδείξεων, η απόδειξη θεωρημάτων μπορεί να γίνει πολύπλοκη, ιδιαίτερα για μεγάλα συστήματα.

Στόχος του ελέγχου ενός παραγόμενου μοντέλου είναι η κατασκευή ενός τελικού συστήματος και διεξοδικά να αναζητηθούν όλες οι πιθανές καταστάσεις ώστε να καθοριστεί εάν η συγκεκριμένη (υπό μελέτη) ιδιότητα ικανοποιείται ή όχι [13]. Δυστυχώς, πολλά εργαλεία ελέγχου συστημάτων ενδέχεται να μην μπορούν να αντιμετωπίσουν μεγάλα ή πολύπλοκα συστήματα, αφού πάσχουν

από περιορισμούς τόσο σε χώρο όσο και σε ταχύτητα. Ανάλογα με τη συγκεκριμένη τυπική μέθοδο που εφαρμόζεται ο περιορισμός των δυνατών καταστάσεων αυξάνει τις αναλυτικές δυνατότητες του συστήματος (π.χ. το NRL Protocol Analyzer [14])

Όσον αφορά τη μελέτη επίδοσης σε θέματα ασφάλειας, οι τυπικές μέθοδοι έχουν χρησιμοποιηθεί στην αξιολόγηση πρωτοκόλλων πιστοποίησης, όπως το Needham- Schroeder Public Key (NSPK) και τα παρόμοια του [15, 16]. Ο πρωταρχικός στόχος της ασφάλειας είναι να μοιραστεί ένα ¨μυστικό¨ κλειδί ανάμεσα σε μια πιστοποιημένη πηγή και έναν πιστοποιημένο προορισμό ανεξάρτητα από τον κόμβο ή τους κόμβους που θα βρίσκονται ανάμεσα στο μονοπάτι επικοινωνίας. Η εκτίμηση της ασφάλειας ενός πρωτοκόλλου δρομολόγησης περιλαμβάνει την ασφαλή ανακάλυψη του/των μονοπατιού/ων επικοινωνίας και την εξασφάλιση της αξιοπιστίας στη μεταφορά των δεδομένων.

Στον πίνακα 4.2 περιλαμβάνονται τυπικές μέθοδοι που έχουν χρησιμοποιηθεί στην αξιολόγηση ιδιοτήτων ασφάλειας σε πρωτόκολλα δρομολόγησης, καθώς και ποιες από αυτές έχουν υιοθετηθεί/χρησιμοπιηθεί στη μελέτη της τοπολογίας των δικτύων MANET.

Πίνακας 3.2: *Τυπικές Μέθοδοι Μελέτης Επίδοσης Πρωτοκόλλων[7]*

Μέθοδοι	Περιγραφή	
Cryptographic Protocol Analysis Language Evaluation System (CPAL-ES) [17]	Χρησιμοποιεί αδύναμες υποθέσεις λογικής για να παράγει τις απαιτούμενες συνθήκες επαλήθευσης	[18]
Communicating Sequential Processes (CSP) [19]	Μοντελοποιεί τη διαδικασία αλληλεπίδρασης μεταξύ συγκλυνόντων κόμβων	A/N
Navy Research Lab (NRL) Protocol Analyzer [14]	Χρησιμοποιεί Prolog για να καθορίσει αν ανασφαλείς καταστάσεις είναι πιθανές	A/N
Petri Nets [20, 21]	Μοντελοποιεί γραφικά κατανεμημένες ροές πληροφορίας	[22]
Simple Promela Interpreter (SPIN) [23]	Μοντελοποιεί τη διαδικασία Prolog αλληλεπίδρασης με τη χρήση γραμμικής λογικής	N/A
Spi calculus [24]	Χρησιμοποιεί Αλγεβρικές διαδικασίες Prolog για τη μοντελοποίηση της αλληλεπίδρασης μεταξύ των καναλιών	[25]
Strand Spaces [26]	Μοντελοποιεί γραφικά κοινότυπες αλληλεπιδράσεις	[27]

3.2 Ασφάλεια

3.2.1 Απαιτήσεις Ασφάλειας

Παρακάτω θα εξετασθούν οι τυπικές απαιτήσεις ασφάλειας που θα πρέπει να ικανοποιεί ένα δίκτυο προκειμένου να χαρακτηριστεί ως ¨ασφαλές¨.

Εμπιστευτικότητα

Η *εμπιστευτικότητα* (Confidentiality) των δεδομένων αποτελεί, ίσως, τη σημαντικότερη απαίτηση ασφάλειας που θα πρέπει να επιδεικνύει ένα δίκτυο. Είναι η πρώτη ιδιότητα που προσπαθεί κάθε δίκτυο να κατακτήσει και έχει σχέση με τα παρακάτω:

- Ένα δίκτυο δεν θα πρέπει να διαρρέει δεδομένα στους γείτονές του, ιδιαίτερα αν πρόκειται για στρατιωτική εφαρμογή, όπου τα δεδομένα αυτά μπορεί να είναι εξαιρετικά σημαντικά.

- Σε πολλές εφαρμογές οι κόμβοι ανταλλάσσουν εξαιρετικά ευαίσθητα δεδομένα, π.χ. διανομή κλειδιών, και για το λόγο αυτό είναι σημαντική η ύπαρξη ενός ασφαλούς καναλιού επικοινωνίας, ιδιαίτερα για τα ασύρματα δίκτυα.

- Οι δημόσιες πληροφορίες που διαθέτει ο κάθε κόμβος, π.χ. δημόσιο κλειδί, ταυτότητα, θα πρέπει να κρυπτογραφούνται ώστε να προστατευτούν από επιθέσεις ανάλυσης κίνησης δεδομένων.

Η συνήθης διαδικασία ώστε να διατηρηθούν μυστικά τα ευαίσθητα δεδομένα είναι να κρυπτογραφούνται με τη χρήση ενός μυστικού κλειδιού, το οποίο μόνο διακεκριμένοι κόμβοι διαθέτουν, ώστε να εξασφαλιστεί η εμπιστευτικότητα.

Ακεραιότητα

Με την εξασφάλιση της εμπιστευτικότητας, ένας κακόβουλος χρήστης δεν θα μπορέσει να κλέψει πληροφορίες. Ωστόσο, αυτό δε σημαίνει ότι τα δεδο-

μένα είναι ασφαλή. Ο επιτιθέμενος μπορεί να αλλάξει τα δεδομένα, ώστε να αποπροσανατολίσει την επικοινωνία. Για παράδειγμα, ένας εχθρικός κόμβος μπορεί να προσθέσει κάποια κομμάτια, είτε να τροποποιήσει τα δεδομένα ενός πακέτου. Αυτό το νέο πακέτο μπορεί να αποσταλεί στον προορισμό σαν να πρόκειται για το αυθεντικό. Η απώλεια, ή η καταστροφή, δεδομένων μπορούν να καταστούν δυνατές και χωρίς την παρουσία κακόβουλου κόμβου, αλλά εξαιτίας του ασταθούς περιβάλλοντος επικοινωνίας. Η *ακεραιότητα* (Integrity) δεδομένων εξασφαλίζει ότι τα δεδομένα λαμβάνονται από τον προορισμό όπως τα έστειλε η πηγή, χωρίς αλλαγές ή τροποποιήσεις.

Νεότητα

Πλέον της εξασφάλισης της ακεραιότητας και της εμπιστευτικότητας των δεδομένων θα πρέπει να ισχύει και η *νεότητα* (freshness). Η νεότητα δηλώνει ότι τα δεδομένα είναι πρόσφατα και εξασφαλίζει ότι δεν έχει ανταλλαγεί κάποιο μήνυμα. Αυτή η απαίτηση ασφάλειας είναι ιδιαίτερα σημαντική όταν χρησιμοποιείται διαμοιρασμός δημόσιων-μυστικών κλειδιών. Συνήθως τα κλειδιά αυτά θα πρέπει να αλλάζουν σε τακτά χρονικά διαστήματα. Ωστόσο, χρειάζεται κάποιος χρόνος ώστε να πραγματοποιηθεί ο διαμοιρασμός σε όλο το δίκτυο. Σε αυτή την περίπτωση είναι εύκολο για τον εχθρό να χρησιμοποιήσει μια επίθεση επανάληψης. Επίσης, είναι εύκολο να καταστραφεί η επικοινωνία (ανταλλαγή δεδομένων) με τον κόμβο που δεν έχει καταλάβει ότι έχει αλλάξει το κλειδί της επικοινωνίας. Κατά τη διαδικασία εύρεσης νέων μονοπατιών δρομολόγησης στα κινητά δίκτυα είναι σημαντικό ο κάθε κόμβος να γνωρίζει αν έχει επεξεργαστεί την αίτηση στο παρελθόν, να γνωρίζει δηλαδή πόσο πρόσφατη είναι. Για τη λύση αυτού του προβλήματος εισάγεται σε κάθε πακέτο ένας χρονικός μετρητής ώστε να εξασφαλιστεί η ¨φρεσκάδα¨ των δεδομένων.

Διαθεσιμότητα

Η χρήση παραδοσιακών αλγορίθμων κρυπτογράφησης στα σύγχρονα δί-

κτυα, ιδιαίτερα τα ασύρματα, έχει σαν αποτέλεσμα την προσθήκη επιπλέον κόστους λειτουργίας και επιπρόσθετα θέτουν σε κίνδυνο τη διαθεσιμότητα του συστήματος. Μερικές προσεγγίσεις επιλέγουν να τροποποιήσουν τον ήδη υπάρχοντα κώδικα, ώστε να χρησιμοποιήσουν όσο το δυνατόν περισσότερα τμήματά του. Άλλες προσεγγίσεις χρησιμοποιούν επιπλέον επικοινωνία για να πετύχουν την κρυπτογράφηση που θέλουν. Επιπλέον, κάποιες εφαρμογές είτε περιορίζουν αυστηρά την πρόσβαση στα δεδομένα, ή προτείνουν κάποιο μη πρακτικό (κεντρικό) σχήμα ώστε να απλοποιηθούν οι διαδικασίες κρυπτογράφησης. Όλες αυτές οι προσεγγίσεις περιορίζουν τη *διαθεσιμότητα* (Availability) του συστήματος για τους παρακάτω λόγους:

- Η επιπρόσθετη υπολογιστική χρήση καταναλώνει περισσότερη ενέργεια. Εάν εξαντληθεί η ενέργεια αυτή τα δεδομένα δε θα είναι πλέον διαθέσιμα.
- Η αύξηση της ανάγκης για επικοινωνία καταναλώνει, επίσης, ενέργεια. Επιπλέον όσο περισσότερη κίνηση έχει το δίκτυο τόσο μεγαλύτερος είναι και ο κίνδυνος της συμφόρησης δεδομένων σε κάποιο κομβικό σημείο που παρουσιάζεται ενεργειακά αδύναμο.
- Εάν χρησιμοποιηθεί ένα κεντρικό σύστημα που θα πραγματοποιεί τη κρυπτογράφηση, τότε το δίκτυο κινδυνεύει να παρουσιάσει ένα ολικό σημείο αυτοκατάρρευσης, το οποίο θα είναι καταστροφικό για τη διαθεσιμότητα των δεδομένων.

Η απαίτηση της ασφάλειας δεν επηρεάζει μόνο τον τρόπο λειτουργίας του δικτύου αλλά αποτελεί παράγοντα σταθεροποίησης του συστήματος.

Αυτο-οργάνωση

Αυτή η απαίτηση ασφάλειας αφορά κυρίως τα κινητά ασύρματα δίκτυα που αποτελούν δίκτυα ad hoc, με ανεξαρτησία και ικανότητα να *αυτο-οργανώνονται* (Self-Organization) κατά περίπτωση. Τα δίκτυα αυτά δε διαθέτουν κάποια

σταθερή υποδομή διαχείρισης. Έτσι, για παράδειγμα, το μοίρασμα ενός κλειδιού θα πρέπει να έχει γίνει πριν την εγκατάσταση του όλου δικτύου. Στη βιβλιογραφία έχουν προταθεί πολλά σχήματα που καλύπτουν τη διαδικασία του μοιράσματος κλειδιών στα πλαίσια συμμετρικών τεχνικών κρυπτογράφησης [33, 34, 35, 36]. Για την εφαρμογή τεχνικών κρυπτογράφησης με τη χρήση δημόσιου κλειδιού θα πρέπει να έχει σχεδιαστεί και η διαδικασία διανομής του δημόσιου αυτού κλειδιού. Τα ασύρματα κινητά δίκτυα θα πρέπει να αυτο-οργανώνονται ώστε να μπορέσει να υπάρξει δρομολόγηση δεδομένων μεταξύ των κόμβων τους. Κατά τον ίδιο τρόπο θα πρέπει να αυτο-οργανώνονται ώστε να πραγματοποιείται διαμοιρασμός κλειδιών και να δημιουργούνται σχέσεις ασφάλειας μεταξύ τους. Εάν δεν υπάρχει η δυνατότητα της αυτο-οργάνωσης το αποτέλεσμα μιας εχθρικής επίθεσης, ή μιας ανωμαλίας του περιβάλλοντος, σε ένα τμήμα του δικτύου μπορεί να αποβεί καταστροφικό για τη λειτουργία του συνόλου.

Πιστοποίηση

Ένας εχθρικός κόμβος μπορεί να μην περιοριστεί στην αλλαγή μόνο των πακέτων δεδομένων. Μπορεί να τροποποιήσει όλη την επικοινωνία με την εισαγωγή επιπλέον πακέτων. Έτσι ο παραλήπτης θα πρέπει να πιστοποιήσει ότι κάθε πακέτο έχει προέλθει από το σωστό κόμβο. Αυτό περιλαμβάνει όχι μόνο πακέτα δεδομένων αλλά και πακέτα ελέγχου (π.χ. πακέτα αίτησης εύρεσης νέων δρομολογίων επικοινωνίας). Η *πιστοποίηση* (Authentication) των μηνυμάτων είναι σημαντική διαδικασία για πολλές δικτυακές εφαρμογές (π.χ. όταν υπάρχει η ανάγκη χρέωσης), καθώς επιτρέπει στον παραλήπτη να πιστοποιήσει ότι ο φερόμενος ως αποστολέας των δεδομένων είναι αυτός που δηλώνει και όχι κάποιος άλλος. Παραδοσιακά, η πιστοποίηση επιτυγχάνεται με καθαρά συμμετρικούς μηχανισμούς. Έτσι, ο αποστολέας και ο παραλήπτης κατέχουν από κοινού ένα μυστικό κλειδί και υπολογίζουν με αυτό τον κώδικα πιστοποίησης (Message Authentication Code-MAC) όλων των ανταλλασόμενων

μηνυμάτων.

Καταλογισμός Ευθύνης

Ο *καταλογισμός ευθύνης* (non-repudiation) αναφέρεται στη διαδικασία κατά την οποία ένας κόμβος δεν μπορεί να αρνηθεί ότι έχει υπογράψει ένα μήνυμα.

3.2.2 Είδη Επιθέσεων

Τα δίκτυα είναι ευαίσθητα σε πολλών ειδών επιθέσεις. Οι επιθέσεις αυτές μπορούν να πραγματοποιηθούν με πολλές μεθόδους, κυρίως με επιθέσεις άρνησης υπηρεσίας (Denial of Service), αλλά επίσης και με ανάλυση κίνησης, με παραβίαση της μυστικότητας (ιδιωτικότητας), ακόμα και με φυσικές επιθέσεις. Ειδικότερα οι επιθέσεις άρνησης υπηρεσίας στα ασύρματα δίκτυα ποικίλουν από απλές παρεμβολές της επικοινωνίας σε πιο εξειδικευμένες μορφές επιθέσεων που έχουν στόχο είτε το πρωτόκολλο 802.11 [37], ή κάποιο άλλο επίπεδο του δικτύου. Λόγω των περιορισμών που υπάρχουν τόσο σε ενέργεια όσο και σε υπολογιστική ισχύ η αντιμετώπιση μιας καλά οργανωμένης επίθεσης άρνησης υπηρεσίας μπορεί να είναι και αδύνατη. Ένας κακόβουλος κόμβος μπορεί εύκολα να παρεμποδίσει την επικοινωνία μέσα στο δίκτυο, ακόμα και με απλή παρεμβολή ραδιο-παρασίτων.

Άρνηση Υπηρεσίας

Οι επιθέσεις *άρνησης υπηρεσίας* (Denial of Service - DoS) δεν αποτελούν κάποιο νέο είδος επιθέσεων. Το γεγονός, όμως, της ύπαρξης περιορισμών στους πόρους του συστήματος, μπορεί να καταστήσει τις επιθέσεις αυτού του είδους πολύ επιζήμιες.

Οι επιθέσεις άρνησης υπηρεσίας μπορούν να επιτευχθούν είτε με τη συνεχή, ή με την περιοδική, εκπομπή ραδιο-παρασίτου παρεμβάλλοντας έτσι στην επικοινωνία. Αν η εκπομπή είναι συνεχής τότε κανένα μήνυμα δεν μπορεί να μεταδοθεί από τον κόμβο (ή το τμήμα του δικτύου) που είναι υπό επίθεση. Αν η εκπομπή είναι περιοδική τότε μπορεί να μεταδίδονται κάποια μηνύματα

αλλά όχι και όλη η ποσότητα της πληροφορίας.

Στόχος μιας τέτοιας επίθεσης μπορεί να είναι κάποιο πρωτόκολλο συγκεκριμένου επιπέδου (π.χ. του link layer) του δικτύου, π.χ. το πρωτόκολλο 802.11 (WiFi), οπότε και γίνεται μια συνεχής μετάδοση μηνυμάτων ώστε να δημιουργηθούν συνθήκες συμφόρησης. Η επανεκπομπή αυτών των συμφορηθέντων μηνυμάτων έχει ως αποτέλεσμα την κατανάλωση πόρων του συστήματος.

Στο επίπεδο δρομολόγησης μπορεί ένας κακόβουλος κόμβος να εμποδίσει την επικοινωνία απλά αρνούμενος τη μεταβίβαση μηνυμάτων. Τα μηνύματα αυτά μπορεί να είναι απλά πακέτα δεδομένων, μπορεί όμως να πρόκειται και για μηνύματα ελέγχου (π.χ. αίτησης εύρεσης μονοπατιού δρομολόγησης), οπότε και να υπάρξει ολική κατάλλειψη επικοινωνίας.

Το επίπεδο μεταφοράς μπορεί να δεχθεί επίθεση άρνησης υπηρεσίας με τη μορφή πλημμύρας μηνυμάτων. Κατά την τεχνική αυτή επιτυγχάνεται η εξάντληση των πόρων του συστήματος με τη συνεχή αποστολή πολλών μηνυμάτων αίτησης επικοινωνίας (connection requests) προς έναν κόμβο και την συνεπακόλουθη αντιμετώπιση (processing) αυτών των μηνυμάτων .

Πολλαπλές Ταυτότητες

Η επίθεση *πολλαπλών ταυτοτήτων* (Sybil attack) δεν είναι τίποτα άλλο παρά η παράνομη προσπάθεια ενός κόμβου να παρουσιαστεί στο δίκτυο με πολλαπλές ταυτότητες. Αυτού του είδους η επίθεση είχε αρχικά εμφανιστεί ώστε να αντικρούσει τους μηχανισμούς πλεονασμού (redundancy mechanisms) των κατανεμημένων συστημάτων αποθήκευσης σε ομόλογα δίκτυα (peer-to-peer). Οι αλγόριθμοι δρομολόγησης, οι μηχανισμοί συνάθροισης δεδομένων, οι μέθοδοι ψηφοφορίας, οι μηχανισμοί δίκαιης κατανομής πόρων και οι μηχανισμοί ανίχνευσης παράνομης συμπεριφοράς είναι όλοι ευαίσθητοι απέναντι σε αυτού του είδους την επίθεση. Ανεξάρτητα από το στόχο της επίθεσης (δρομολόγηση, ψηφοφορία, κλπ.) ο τρόπος άσκησης αυτής της επίθεσης είναι ο ίδιος. Ο κακόβουλος κόμβος/ χρήστης προσπαθεί να ενταχθεί στο δίκτυο με

πολλαπλές ταυτότητες. Για παράδειγμα, στην περίπτωση της δρομολόγησης μπορεί να εμφανίζεται με διαφορετικές ταυτότητες σε πολλαπλά μονοπάτια και έτσι να ελέγχει την επικοινωνία. Στην περίπτωση της ψηφοφορίας μπορεί ο εχθρός να έχει πολλαπλά δικαιώματα ψήφου ανάλογα με την ταυτότητα που χρησιμοποιεί.

Κατάργηση Ιδιωτικότητας

Η τεχνολογία των ασύρματων δικτύων υπόσχεται την εύκολη και γρήγορη επικοινωνία μεταξύ των κόμβων σε οποιοδήποτε περιβάλλον. Ενώ αυτή η προοπτική είναι πολύ συμφέρουσα για τον χρήστη, προβάλλει έντονος ο κίνδυνος της κατάχρησης (με την έννοια της κακής χρήσης). Ειδικότερα παρουσιάζονται προβλήματα που σχετίζονται με τη διατήρηση της μυστικότητας (ιδιωτικότητας) (Privacy) των δεδομένων του κάθε χρήστη, καθώς το περιβάλλον μέσα στο οποίο πραγματοποιείται η επικοινωνία μπορεί να είναι εχθρικό. Ένας κακόβουλος χρήστης μπορεί να χρησιμοποιήσει δεδομένα (φαινομενικά άσχετα, ασήμαντα) ώστε να εξάγει πολύτιμες πληροφορίες. Για παράδειγμα, ένας εχθρός μπορεί να λειτουργεί αθώα-κανονικά ενώ παρακολουθεί το κανάλι επικοινωνίας και να λειτουργήσει κακόβουλα μόνο όταν διαπιστώσει κίνηση δεδομένων. Μπορεί να καταστρέψει έτσι την επικοινωνία ανάμεσα σε κόμβους την κατάλληλη κρίσιμη στιγμή, χωρίς να έχει πρόσβαση στο πλήρες περιεχόμενο των πακέτων δεδομένων.

Οι πιο κοινές επιθέσεις που στόχο έχουν την καταπάτηση της ιδιωτικότητας της επικοινωνίας είναι:

- Παρακολούθηση (Monitor, Eavesdropping) Αποτελεί την πιο προφανή επίθεση. Αν ένας εχθρικός κόμβος παρακολουθεί το κανάλι μπορεί να ερμηνεύσει το περιεχόμενο της επικοινωνίας. Όταν τα πακέτα περιέχουν πληροφορίες π.χ. για την τοπολογία του δικτύου, ο εχθρικός κόμβος μπορεί να καταλάβει την επικοινωνία όλου του δικτύου και όχι μόνο ένος κόμβου.

- Ανάλυση κίνησης (Traffic Analysis) Η επίθεση αυτή συνήθως συνδυάζεται με την παρακολούθηση. Μια αύξηση στον αριθμό των μεταφερόμενων πακέτων μεταξύ δύο κόμβων μπορεί να πυροδοτήσει την έναρξη κατάληψης της επικοινωνίας. Μέσω της επίθεσης αυτής μπορεί να αποκαλυφθεί ο ειδικός ρόλος που ενδεχομένως έχει κάποιος κόμβος.
- Συγκάλυψη (Camouflage) Είναι δυνατόν να εισαχθεί ένας εχθρικός κόμβος στο δίκτυο και να λειτουργεί κανονικά-ομαλά έως τη στιγμή που κρίνει ότι είναι συμφέρουσα για αυτόν οπότε και λειτουργεί προς όφελός του.

Βιβλιογραφία

[1] M. Burmester, T. V. Le, and A. Yasinsac, *Adaptive gossip protocols: Managing security and redundancy in dense Ad Hoc Networks*, Ad Hoc Networks, vol. 5, no. 3, 2007, pp. 313–23.

[2] D. Johnson and D. Maltz, *Dynamic Source Routing in Ad Hoc Wireless Networks*, Mobile Computing, T. Imielinski and H. Korth, Eds. Kluwer, 1996, pp. 153–81.

[3] L. Buttyan and I. Vajda, *Towards Provable Security for Ad Hoc Routing Protocols*, Proc. 2nd ACM Wksp. Security of Ad Hoc and Sensor Networks, 2004, pp. 94–105.

[4] P. Papadimitratos and Z. J. Haas, *Secure Routing for Mobile Ad Hoc Networks*, Proc. SCS Commun. Networks and Distributed Systems Modeling and Simulation Conf., 2002.

[5] Y. C. Hu, A. Perrig, and D. B. Johnson, *Ariadne: α Secure On–Demand Routing Protocol for Ad Hoc Networks*, Proc. 8th Annual Int''l. Conf. Mobile Computing and Networking (Mobi– Com ''02), 2002, pp. 12–23.

[6] Y.–C. Hu, D. B. Johnson, and A. Perrig, *SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks*, Ad Hoc Networks, vol. 1, no. 1, 2003, pp. 175–92.

[7] T. R. Andel and A. Yasinsac, *Wireless Protocol Security to Simulate or not Simulate*, Proc. 2006 Spring Simulation Multi– Conf. (SpringSim''06), 2006, pp. 511–17.

[8] G. Acs, L. Buttyan, and I. Vajda, *Provably Secure On– Demand Source Routing in Mobile Ad Hoc Networks*, IEEE Trans. Mobile Computing, vol. 5, no. 11, 2006, pp. 33–46.

[9] D. Beaver, *Secure Multiparty Protocols and Zero–Knowledge Proof Systems Tolerating A Faulty Minority*, J. Cryptology, vol. 4, no. 2, 1991, pp. 75–122.

[10] G. Acs, L. Buttyan, and I. Vajda, *Provable Security of On– Demand Distance Vector Routing In Ad Hoc Networks*, Proc. European Wksp. Security and Privacy, 2005, pp. 113–27.

[11] J. P. Bowen and M. G. Hinchey, *Ten Commandments of Formal Methods*, IEEE Computer, vol. 28, no. 4, 1995, pp. 56–63.

[12] E. M. Clarke and J. M. Wing, *Formal Methods: State of the Art and Future Directions*, ACM Computing Surveys, vol. 28, no. 4, 1996, pp. 626–43.

[13] E. M. Clarke, O. Grumberg, and D. A. Peled, Model Checking, MIT Press, 1999.

[14] C. Meadows, *The NRL Protocol Analyzer: An Overview*, J. Logic Programming, vol. 26, no. 2, 1996, pp. 113–31.

[15] R. Needham and M. Schroeder, *Using Encryption for Authentication in Large Networks of Computers*, Commun. ACM, vol. 21, no. 12, 1978, pp. 993–99.

[16] G. Lowe, *Breaking and Fixing the Needham–Schroeder Public– Key Protocol using FDR*, Proc. Tools and Algorithms for the Construction and Analysis of Systems, 1996, pp. 147–66.

[17] A. Yasinsac and W. A. Wulf, *A Framework for A Cryptographic Protocol Evaluation Workbench*, The Int''l. J. Reliability, Quality and Safety Engineering (IJRQSE), vol. 8, no. 4, 2001, pp. 373–89.

[18] J. Marshall, *An Analysis of the Secure Routing Protocol for Mobile Ad Hoc Network Route Discovery: Using Intuitive Reasoning and Formal Verification to Identify Flaws*, M.S. thesis, Department of Computer Science, Florida State University, Tallahassee, FL, Apr. 2003.

[19] C. A. R. Hoare, Communicating Sequential Processes, Prentice–Hall, 1985.

[20] J. L. Peterson, *Petri Nets*, ACM Computing Surveys (CSUR), vol. 9, no. 3, 1977, pp. 223–52.

[21] J. L. Peterson, Petri Net Theory and the Modeling of Systems, Prentice–Hall, 1981.

[22] D. Djenouri and N. Badache, *A Novel Approach for Selfish Nodes Detection in MANETs: Proposal and Petri Nets Based Modeling*, Proc. 8th Int''l. Conf. Telecommun. (ConTEL ''05), 2005, pp. 569–74.

[23] G. J. Holzmann, *The Model Checker SPIN*, IEEE Trans. Software Engineering, vol. 23, no. 5, 1997, pp. 279–95.

[24] M. Abadi and A. D. Gordon, *A Calculus for Cryptographic Protocols: the SPI Calculus*, Proc. 4th ACM Conf. Comp. and Commun. Security, 1997, pp. 36–47.

[25] S. Nanz and C. Hankin, *A Framework for Security Analysis of Mobile Wireless Networks*, Theoretical Computer Science, vol. 367, no. 1–2, 2006, pp. 203–27.

[26] F. J. Thayer Fabrega, J. C. Herzog, and J. D. Guttman, *Strand Spaces: Proving Security Protocols Correct*, J. Computer Security, vol. 7, no. 2/3, 1999, pp. 191–230.

[27] S. Yang and J. S. Baras, *Modeling Vulnerabilities of Ad Hoc Routing Protocols*, Proc. 1st ACM Wksp. Security of Ad hoc and Sensor Networks, 2003, pp. 12–20.

[28] University of Southern California, *The Network Simulator*, http://nsnam.isi.edu/nsnam/index.php/Main_Page

[29] GloMoSim UCLA, *Global Mobile Information Systems Simulation Library*, http://pcl.cs.ucla.edu/projects/glomosim/

[30] OPNET Technologies, *Optimized Network Engineering Tools*, http://www.opnet.com/

[31] *simulation software development frameworks*, http://www.topology.org/soft/sim.html

[32] OMNeT++ Community Site, *OMNeT++*, http://www.omnetpp.org/

[33] H. Chan, A. Perrig, and D. Song. *Random key predistribution schemes for sensor networks* In Proceedings of the 2003 IEEE Symposium on Security and Privacy, page 197. IEEE Computer Society, 2003.

[34] L. Eschenauer and V. D. Gligor. *A key–management scheme for distributed sensor networks* In Proceedings of the 9th ACM conference on Computer and communications security, pages 41–47. ACM Press, 2002.

[35] J. Hwang and Y. Kim., *Revisiting random key pre–distribution schemes for wireless sensor networks*, In Proceedings of the 2nd ACM workshop on Security of Ad hoc and Sensor Networks (SASN ''04), pages 43–52, New York, NY, USA, 2004. ACM Press.

[36] D. Liu, P. Ning, and R. Li., *Establishing pairwise keys in distributed sensor networks*, ACM Trans. Inf. Syst. Secur., 8(1):41–77, 2005.

[37] A. Perrig, J. Stankovic, and D. Wagner., *Security in wireless sensor networks*, Commun. ACM, 47(6):53–57, 2004.

Κεφάλαιο 4

Ασφαλής Κατανεμημένη Εφαρμογή σε περιβάλλοντα Ευφυών Δικτύων

Τα Ευφυή Δίκτυα (ΕΔ) (Intelligent Networks - IN) διαχωρίζουν τον έλεγχο και την επεξεργασία της ίδιας της κλήσης από το μεταγωγέα (switch) του δικτύου, οδηγώντας έτσι σε υπηρεσίες που είναι ανεξάρτητες από την υποδομή του δικτύου αλλά και την εταιρεία παροχής τους. Με αυτό τον τρόπο οι παρεχόμενες υπηρεσίες έχουν μειωμένο κόστος ανάπτυξης αλλά και εφαρμογής. Η ενσωμάτωση νέων τεχνολογιών όπως η CORBA και οι κινητοί πράκτορες βελτιώνουν την επίδοση των ΕΔ.

Στο κεφάλαιο αυτό παρουσιάζεται μια αρχιτεκτονική με τη χρήση μηχανισμών ασφάλειας στο επίπεδο εφαρμογής και τεχνολογία CORBA που εφαρμόζεται στα κατανεμημένα Ευφυή δίκτυα. Συγκεκριμένες πολιτικές μπορούν να εφαρμοστούν τόσο σε επίπεδο δικτύου όσο και σε επίπεδο ασφάλειας, ώστε να επιτευχθούν ικανοποιητικά επίπεδα επίδοσης του δικτύου σύμφωνα, πάντα

με τις ιδιαίτερες ανάγκες που απαιτεί η κάθε εφαρμογή. Συγκεκριμένα γίνεται σύντομη παρουσίαση των σχετικών εργασιών που έχουν γίνει στο χώρο της ασφάλειας με εφαρμογή στα Ευφυή δίκτυα. Στη συνέχεια παρουσιάζονται οι επιθέσεις ασφάλειας καθώς και οι απαιτήσεις που έχουν καταγραφεί για τον υπό μελέτη χώρο. Αναλύονται οι μηχανισμοί ασφάλειας που μπορούν να χρησιμοποιηθούν προκειμένου να αντιμετωπιστούν αυτά τα θέματα ασφάλειας. Τέλος παρουσιάζεται η προτεινόμενη ασφαλής αρχιτεκτονική όπως αυτή εφαρμόζεται στα Κατανεμημένα Ευφυή δίκτυα.

4.1 Εισαγωγή

Κυρίαρχες τάσεις στο χώρο των τηλεπικοινωνιών επιβάλλουν τη γρήγορη ανάπτυξη υπηρεσιών ικανών να προσαρμόζονται στις απαιτήσεις των πελατών /χρηστών τους. Οι εφαρμογές αυτές θα πρέπει να παρέχουν τη δυνατότητα αυτόματης εγγραφής στην υπηρεσία, καθώς επίσης, και ευκολία στην εγκατάστασή τους στο υπάρχον δημόσιο τηλεπικοινωνιακό δίκτυο (PSTN). Σε αυτό το περιβάλλον τα ευφυή δίκτυα διαδραματίζουν σημαντικό ρόλο. Στο παραδοσιακό δημόσιο τηλεπικοινωνιακό δίκτυο τα λειτουργικά στοιχεία του δικτύου είχαν στατικό περιβάλλον διεπαφής, το οποίο ήταν προσαρμοσμένο στην εξυπηρέτηση συγκεκριμένων υπηρεσιών και αυτό είχε ως αποτέλεσμα τον περιορισμό των δυνατοτήτων λειτουργίας του δικτύου. Η εισαγωγή νέων υπηρεσιών αποτελούσε μια χρονοβόρα και δαπανηρή διαδικασία. Στα ΕΔ, ο έλεγχος καθώς και η επεξεργασία της κλήσης έχουν μεταφερθεί έξω από τον μεταγωγέα (switch) του δικτύου και τώρα εξυπηρετούνται από άλλες λειτουργικές μονάδες. Το ανωτέρω έχει ως αποτέλεσμα την ύπαρξη υπηρεσιών που είναι ανεξάρτητες από το δίκτυο, στο οποίο εφαρμόζονται, και από την εταιρεία ανάπτυξης τους ενώ ταυτόχρονα παρουσιάζουν χαμηλό κόστος και υψηλή ταχύτητα στην ενταξή τους στο δίκτυο [4]. Η αρχιτεκτονική των ΕΔ ενδυναμώνεται με τη χρήση τεχνολογιών όπως Common Object Request

Broker (CORBA) [17] and Mobile Agent Technologies (MAT). Με τη χρήση της CORBA ενισχύεται και επεκτείνεται η κατανεμημένη φύση της αρχιτεκτονικής των ΕΔ. Η χρήση των τεχνολογιών MAT παρέχει τη δυνατότητα ανάπτυξης εύρωστων και δυναμικά οργανωμένων εφαρμογών πάνω σε ΕΔ με ταυτόχρονα ελαττωμένο φόρτο σημασιοδοσίας (signalling traffic). Στα [3, 4] προτείνεται ένας τέτοιος συνδυασμός, όπου η αρχιτεκτονική του ΕΔ έχει βασιστεί στην CORBA και στην Grasshopper [10] ως πλατφόρμα πρακτόρων.

Αυτού του είδους οι αρχιτεκτονικές είναι αρκετά εξεζητημένες ώστε να υποστηρίζουν εφαρμογές που ικανοποιούν τις αυξημένες ανάγκες των χρηστών. Παραδείγματα αυτών των εφαρμογών αποτελούν και οι υπηρεσίες ανάκτησης πολυμεσικών δεδομένων κατ' απαίτηση (Multimedia Retrieval - IMR) και πιο συγκεκριμένα η ανάκτηση κινούμενης εικόνας κατ' απαίτηση (Video-on-Demand - VoD) και η ανάκτηση ειδήσεων κατ' απαίτηση News-on-Demand (NoD). Η παροχή αλληλεπίδρασης μεταξύ των χρηστών και του δικτύου οδηγεί σε υπηρεσίες υψηλής ποιότητας.

Η ανάπτυξη μιας αρχιτεκτονικής δικτύου με τη χρήση κατανεμημένων τεχνολογιών, εφαρμοσμένες πάνω σε ανασφαλή κανάλια επικοινωνίας, όπως το διαδίκτυο Internet, εγείρει πολλές απειλές ασφάλειας. Αυτές οι απειλές ασφάλειας μπορεί να περιέχουν επιθέσεις άρνησης υπηρεσίας Denial-of-Service (DoS), παράκαμψη του ελέγχου πρόσβασης ή αλλαγή της επικοινωνίας μεταξύ διαφόρων οντοτήτων του δικτύου.

Πολλές τεχνικές έχουν προταθεί ώστε να ξεπεραστούν τέτοιου είδους προβλήματα ασφάλειας που εμφανίζονται στα πλαίσια της αρχιτεκτονικής των ΕΔ. Ο Aura [2] προτείνει ένα σύστημα ελέγχου πρόσβασης βασισμένο στην εξουσιοδότηση. Το σύστημα αυτό εφαρμόζεται ανάμεσα στα στοιχεία του ΕΔ και των παρόχων της υπηρεσίας και χρησιμοποιείται για την πιστοποίηση των χρηστών. Η ανάπτυξη έγινε στην αρχιτεκτονική Calypso ΕΔ [13], η οποία αποτελεί μια ¨ελαφριά¨ πλατφόρμα ανάπτυξης υπηρεσιών και είναι

βασισμένη στη γλώσσα Java. Ο Breugst [3] προτείνει τη χρήση μιας έμπιστης οντότητας ώστε να ελεγχθεί η ακεραιότητα των κινητών πρακτόρων στην αρχιτεκτονική των ενεργών Ευφυών Δικτύων (Active Intelligent Networks).

Παρόλο που αρχιτεκτονικές που βασίζονται στην τεχνολογία CORBA έχουν προταθεί στο παρελθόν (π.χ., [14, 18]) και θέματα ασφάλειας συστημάτων που χρησιμοποιούν κινητούς πράκτορες έχουν αποτελέσει αντικείμενο μελέτης (π.χ., [5]), δεν έχει μελετηθεί αρκετά η ασφάλεια σε συστήματα που κάνουν συνδυασμό των ανωτέρω τεχνολογιών και οι οποίες εφαρμόζονται σε περιβάλλοντα ΕΔ.

Σε αυτό το κεφάλαιο, μελετάται μια αρχιτεκτονική ασφαλούς ΕΔ [24], η οποία εφαρμόζεται πάνω στα ευρυζωνικά ΕΔ των [4]. Από τη στιγμή που η προτεινόμενη αρχιτεκτονική είναι βασισμένη στις τεχνολογίες CORBA και Grasshopper ως πλατφόρμα πρακτόρων, το μοντέλο ασφάλειας εξαρτάται από τα μοντέλα CORBA Security Service [16] και το Grasshopper Security Service [12]. Επιπλέον, χρησιμοποιούνται και άλλοι μηχανισμοί ασφάλειας μη-CORBA, όπως οι Trusted Third Party Services.

4.2 Σχετικές Ερευνητικές Εργασίες

Η συγκεντρωτική αρχιτεκτονική των παραδοσιακών ΕΔ και η στατική φύση του πρωτοκόλλου SS7 έχει ως αποτέλεσμα τη μειωμένη επίδοση του δικτύου. Η αποτελεσματική ενσωμάτωση νέων κατανεμημένων τεχνολογιών όπως η CORBA και η MAT βελτιώνουν την επίδοση του δικτύου.

Η χρήση αυτών των τεχνολογιών πάνω σε ευρυζωνικά δίκτυα σηματοδοσίας έχει οδηγήσει στην έννοια των Κατανεμημένων (Ευρυζωνικών) Ευφυών Δικτύων (Distributed (broadband) Intelligent Network - DIN) [3, 4]. Αυτές οι αρχιτεκτονικές ξεχωρίζουν καθώς παρέχουν υπηρεσίες ευρείας ζώνης και έχουν κατανεμημένη δομή στο τμήμα ελέγχου που αφορά το ΕΔ και μπορούν να εφαρμοστούν σε ποικίλες εφαρμογές, όπως υπηρεσίες Interactive Multimedia

Retrieval -IMR.

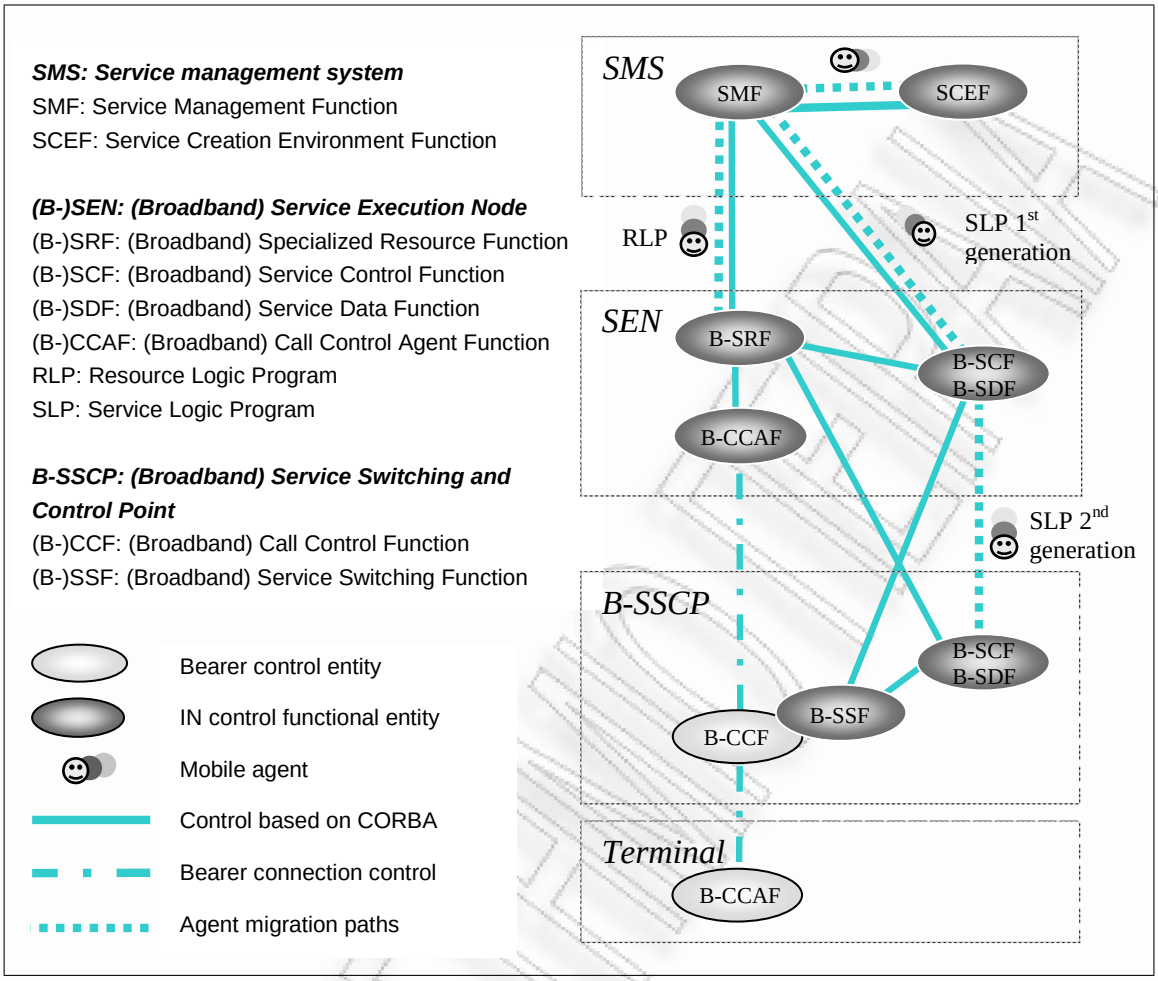
Όπως παρουσιάσθηκε και στο κεφάλαιο 2 τα DIN εκμεταλλεύονται την ευελιξία που τους προσδίδει η χρήση των τεχνολογιών CORBA και MAT (και συγκεκριμένα της πλατφόρμας πρακτόρων Grasshopper) ώστε να μειώσουν το φόρτο επικοινωνίας του δικτύου. Αυτό επιτυγχάνεται με την υλοποίηση καίριων λειτουργιών ελέγχου ως κινητοί πράκτορες. Η υλοποίηση αυτών των λειτουργικών οντοτήτων παρουσιάζει ενδιαφέρουσες βελτιώσεις σε σχέση με την υλοποίηση των παραδοσιακών ΕΔ. Αυτές οι βελτιώσεις επισημαίνονται στην εσωτερική δομή των οντοτήτων αυτών, στο σχέδιο επικοινωνίας που χρησιμοποιούν, καθώς και στις διαφορετικές ιδιότητες που παρουσιάζουν. Η εικόνα 4.1 παρουσιάζει την κατανομή των λειτουργικών οντοτήτων στον φυσικό κόμβο στην αρχιτεκτονική DIN.

Η αρχιτεκτονική που περιγράφεται στο [4] χρησιμοποιεί τρεις φυσικούς κόμβους οι οποίοι φιλοξενούν λειτουργικές οντότητες. Συγκεκριμένα φιλοξενούν τις: Broadband Service Switching and Control Point (B-SSCP), την Broadband Service Execution Node (B-SEN) και την Service Management Service (SMS).

Ο κόμβος SMS φιλοξενεί τις οντότητες που είναι υπεύθυνες για τη δημιουργία (SCEF) και τη διαχείριση των υπηρεσιών (SMF) που παρέχονται από το δίκτυο. Η χρήση των τεχνολογιών CORBA και MAT συνεπάγεται ότι ο σχεδιαστής της υπηρεσίας δε θα γνωρίζει τις λεπτομέρειες του δικτύου που δε σχετίζονται με τη λογική των υπηρεσιών ΕΔ.

Ο κόμβος B-SEN σχετίζεται κυρίως με την εκτέλεση των υπηρεσιών. Φιλοξενεί, μεταξύ άλλων, τις Broadband Service Control Function / Service Data Function (B-SCF/B-SDF) και τη Specialized Resource Function (B-SRF). Αυτές οι οντότητες είναι ικανές να εκτελούν τα Service Logic Programs (SLPs) και Resource Logic Programs (RLPs) ως κινητούς πράκτορες, οι οποίοι μεταναστεύουν με άμεσο/ απλό τρόπο από τον κόμβο SMS.

Ο B-SSCP κόμβος σχετίζεται κυρίως με τη διαδικασία της μεταγωγής στο



Εικόνα 4.1: *Το DIN βασισμένο σε CORBA και MAT [4].*

δίκτυο. Ωστόσο, φιλοξενεί και μια βασική/απλή έκδοση της οντότητας B-SCF/B-SDF. Η οντότητα αυτή μπορεί να εκτελεί τα προγράμματα SLP ως κινητούς πράκτορες, τα οποία μεταναστεύουν από την οντότητα B-SCF/B-SDF η οποία εδρεύει στον κόμβο B-SEN. Και οι δυο οντότητες (και αυτή που βρίσκεται στον κόμβο B-SEN και αυτή που βρίσκεται στο κόμβο B-SSCP) έχουν παρόμοια δομή. Ωστόσο, η B-SSCP που βρίσκεται στον B-SCF/B-SDF λαμβάνει και εξυπηρετεί αιτήσεις υπηρεσίας μόνο κάτω από ορισμένες προϋποθέσεις, συνήθως κάτω από βαρύ φόρτο κίνησης επικοινωνίας είτε κάτω από πολλαπλές αιτήσεις για την ίδια υπηρεσία. Ο ρόλος της Broadband Call Control Function (B-CCF) σχετίζεται με τον έλεγχο της μεταγωγής της

κλήσης/σύνδεσης και στη μετάβαση στο ΕΔ.

Τέλος, στον τερματικό κόμβο, η Broadband Call Control Agent Function (B-CCAF) αποτελεί την οντότητα διεπαφής ανάμεσα στο χρήστη και στο επίπεδο Access Signaling (AS). Η επικοινωνία ανάμεσα στα B-CCAF και το επίπεδο AS πετυχαίνεται με τη χρήση ενός εξειδικευμένου συστήματος διεπαφής Application Programmable Interface (API), το οποίο παρέχει τις κατάλληλες λειτουργίες ώστε ο χρήστης να έχει πρόσβαση στο δίκτυο [7].

Για την εξυπηρέτηση των αιτήσεων, το ΕΔ πραγματοποιεί την παρακάτω αλληλουχία επικοινωνίας μεταξύ των οντοτήτων: Όταν ο χρήστης αρχικοποιεί μια κλήση υπηρεσίας ΕΔ (μέσω της B-CCAF) αυτή προωθείται στο B-CCF, η οποία στέλνει ένα αίτημα στην B-SSF. Η τελευταία επιβεβαιώνει ότι η κλήση είναι κλήση υπηρεσίας ΕΔ και στέλνει ένα αίτημα στο διαχειριστή εκτέλεσης της υπηρεσίας (service logic manager), δηλαδή την οντότητα B-SCF/B-SDF (η οποία βρίσκεται στον κόμβο B-SEN). Ο διαχειριστής εκτέλεσης της υπηρεσίας είναι υπεύθυνος για την επιλογή του κατάλληλου πράκτορα που θα εξυπηρετήσει τελικά το αίτημα. Στη συνέχεια μετά την επιλογή του καταλληλότερου πράκτορα (ο οποίος καλείται ¨πρωτότυπο πρώτης γενιάς¨), αυτός ο πράκτορας αντιγράφεται σε ένα πράκτορα εργάτη δεύτερης γενιάς (worker) και μια απομακρυσμένη αναφορά σε αυτό το αντίγραφο επιστρέφεται στην οντότητα B-SSF. Μετά από τα παραπάνω, καθιερώνεται μια σύνδεση ανάμεσα στο χρήστη και στην οντότητα B-SRF, ώστε να πραγματοποιηθεί η επιλογή του παροχέα της υπηρεσίας, η πιστοποίηση του χρήστη και επιλογή του είδους της υπηρεσίας. Η οντότητα B-SRF εμπλουτίζεται, επίσης, με κινητούς πράκτορες που εκτελούν τα προγράμματα Resource Logic Programs και καλούνται RLP πράκτορες. Αυτοί οι πράκτορες αντιγράφονται (cloned) με τη χρήση ενός διαχειριστή αλληλεπίδρασης με το χρήστη και συνδέονται, κατά το χρόνο εκτέλεσης, με έναν πράκτορα εργάτη RLP. Οι πράκτορες RLP αποτελούν ειδικούς πόρους που χρησιμοποιούνται για συγκεκριμένες υπηρεσίες,

για παράδειγμα για προ-ηχογραφημένα μηνύματα, ώστε να παροτρύνουν το χρήστη στη πληκτρολόγηση και κατά συνέπεια τη συλλογή κάποιων αριθμών. Μετά την ολοκλήρωση αυτού του διαλόγου ανάμεσα στην οντότητα B-SRF και το χρήστη, η επικοινωνία ανάμεσά τους ελευθερώνεται. Για τις ανταλλασσόμενες πληροφορίες δίνεται αναφορά στην οντότητα B-SCF/B-SDF, η οποία στη συνέχεια πυροδοτεί τη σύνδεση με τον επιλεγμένο εξυπηρετητή. Όταν η υπηρεσία ολοκληρωθεί (π.χ. ολοκληρωθεί η εκπομπή ενός video) η σύνδεση με τον εξυπηρετητή ελευθερώνεται και δημιουργείται μια νέα σύνδεση με την οντότητα SRF, ώστε αν θέλει ο χρήστης να μπορεί να επιλέξει μια νέα υπηρεσία. Εάν ο χρήστης επιλέξει να τερματίσει τη σύνδεσή του τότε η σύνοδος (session) ελευθερώνεται εντελώς.

4.3 Μια Ασφαλής Αρχιτεκτονική Ευφυούς Δικτύου

4.3.1 Επιθέσεις Ασφάλειας και Απαιτήσεις

Όπως έχει προαναφερθεί η αρχιτεκτονική ΚΕΔ (Κατανεμημένα Ευφυή Δίκτυα) βασίζεται σχεδόν εξ ολοκλήρου στις κατανεμημένες τεχνολογίες. Επιπλέον, η επικοινωνία ανάμεσα στα στοιχεία του δικτύου πραγματοποιείται με τη χρήση ανοικτών και επισφαλών καναλιών. Αυτός ο τρόπος λειτουργίας υπόκειται σε πολλές επιθέσεις ασφάλειας όπως:

Πλαστοπροσωπία

Μη εξουσιοδοτημένοι χρήστες μπορούν να επιχειρήσουν μέσω της επίθεσης της Πλαστοπροσωπίας (Impersonation) να αποκτήσουν πρόσβαση σε υπηρεσίες ΕΔ. Για παράδειγμα, στην περίπτωση της υπηρεσίας IMR ένας μη εγγεγραμμένος χρήστης μπορεί να επιχειρήσει να δει κάποια ταινία.

Μεταμφίεση

Ένας εγγεγραμμένος χρήστης μπορεί να επιχειρήσει μέσω της επίθεσης Μεταμφίεσης (Masquerading) να παρακάμψει την πολιτική ασφάλειας και πα-

ρανόμως να αποκτήσει πρόσβαση σε ευαίσθητες υπηρεσίες. Για παράδειγμα, ένας χρήστης που έχει δικαιώματα απλής πρόσβασης μπορεί να επιχειρήσει να λειτουργήσει ως διαχειριστής ΕΔ.

Άρνηση Υπηρεσίας

Ένας κακόβουλος χρήστης μπορεί να επιχειρήσει να διακόψει νόμιμους χρήστες από την πρόσβαση στις υπηρεσίες ΕΔ (Denial of Service - DoS), για παράδειγμα στέλνοντας ταυτόχρονα ένα μεγάλο αριθμό αιτημάτων στο σύστημα.

Υποκλοπή Επικοινωνίας και Τροποποίηση

Ένας κακόβουλος χρήστης μπορεί να επιχειρήσει να υποκλέψει και/είτε να αλλάξει (communication eavesdropping and tampering) την επικοινωνία ανάμεσα σε έναν νόμιμο χρήστη και στα στοιχεία της υπηρεσίας IN.

Ανάληψη Ευθύνης

Εάν το ΕΔ δεν είναι ικανό να παρακολουθεί την επικοινωνία ανάμεσα στους χρήστες και τα στοιχεία της υπηρεσίας, τότε δεν θα είναι δυνατόν οι χρήστες να χρεωθούν για τις όποιες πράξεις τους (lack of accountability), π.χ. να χρεωθούν με το ανάλογο κόστος για τη χρήση της υπηρεσίας IMR.

Για το λόγο αυτό, η ασφαλής αρχιτεκτονική του ΕΔ θα πρέπει να επιβάλλει κάποιες απαιτήσεις ασφάλειας. Μη εξουσιοδοτημένη χρήση μιας υπηρεσίας μπορεί να θεωρηθεί ως έλλειψη *πιστοποίησης* ανάμεσα στο χρήστη και σε κάποιο κομβικό στοιχείο του δικτύου. Με την εφαρμογή της κατάλληλης πολιτικής ελέγχου πρόσβασης η *πιστοποίηση* του χρήστη μπορεί να επιτευχθεί, έχοντας ως αποτέλεσμα την αποφυγή απειλών μεταμφίεσης. Ο συνδυασμός της πολιτικής πρόσβασης και μιας πολιτικής παρακολούθησης (auditing) έχει ως αποτέλεσμα την αποφυγή ή και τον εντοπισμό της προέλευσης των επιθέσεων άρνησης υπηρεσίας, παρέχοντας έτσι *διαθεσιμότητα υπηρεσίας*. Επιπλέον, οι υπηρεσίες παρακολούθησης παρέχουν στο σύστημα τη δυνατότητα της *επίδοσης ευθύνης* στους χρήστες. Αυτό είναι απαραίτητο ώστε οι υπηρεσίες των δικτύων ΕΔ να κοστολογηθούν στους εκάστοτε χρήστες τους. Τέλος, υπηρε-

σίες *εμπιστευτικότητας* και *ακεραιότητας* είναι απαραίτητες για την αποφυγή των υποκλοπών ή αλλαγών στην επικοινωνία ανάμεσα στους χρήστες και το δίκτυο.

4.3.2 Μηχανισμοί Ασφάλειας

Για να εκπληρωθούν οι ανωτέρω περιορισμοί απαιτείται ένας συνδυασμός πολλών μηχανισμών ασφάλειας [24]. Οι μηχανισμοί έχουν διαιρεθεί σε αυτούς που είναι βασισμένοι στην τεχνολογία CORBA (*με-CORBA*) και σε όλους τους άλλους (*μη-CORBA*).

Οι με-CORBA μηχανισμοί ασφάλειας έχουν αναπτυχθεί στο ανώτερο επίπεδο της ήδη υπάρχουσας αρχιτεκτονικής των ΚΕΔ. Η ανάπτυξη έγινε με έναν απλό τρόπο, με την άμεση ένταξη και υλοποίηση των κατάλληλων συστατικών στοιχείων ασφάλειας της τεχνολογίας CORBA Security Service [16]. Στην ανάπτυξη αυτή έχει χρησιμοποιηθεί η αρχιτεκτονική CORBA τριών επιπέδων.

Στο χαμηλότερο επίπεδο, η ανταλλαγή μηνυμάτων ανάμεσα στα αντικείμενα CORBA πραγματοποιείται μέσω της δομής ORB Core Infrastructure. Η υπηρεσία ασφάλειας (CORBA Security Service) έχει αναπτυχθεί στο μεσαίο επίπεδο CORBA Services layer με τη χρήση των συστατικών στοιχείων (security components) CORBA. Η CORBA Security Service παρέχει ποικίλα συστήματα διεπαφής τα οποία μπορούν να χρησιμοποιηθούν ώστε να ενσωματωθούν οι απαιτούμενοι μηχανισμοί ασφάλειας CORBA στην εφαρμογή. Πολλές υπάρχουσες τεχνολογίες όπως οι GSS-API [8] μπορούν να χρησιμοποιηθούν ώστε να απομονωθεί/απεξαρτηθεί η ανάπτυξη των υπηρεσιών ασφάλειας από τις λεπτομέρειες κατασκευής των μηχανισμών λειτουργίας των κατωτέρων επιπέδων. Τέλος, στο ανώτερο επίπεδο, το επίπεδο εφαρμογής (Application layer) τα αντικείμενα επικοινωνούν χρησιμοποιώντας την Υπηρεσία Ασφάλειας, ενώ μπορεί και να μην έχουν επίγνωση του τρόπου με τον οποίον είναι υλοποιημένη αυτή η ασφάλεια.

Οι μη-CORBA μηχανισμοί ασφάλειας περιλαμβάνουν όλες τις μη-CORBA περιπτώσεις επικοινωνίας, όπως τη μετανάστευση των πρακτόρων, τις ζεύξεις του κομιστή (bearer connections) ή κάθε άλλου είδους μηχανισμό του επιπέδου εφαρμογής. Αυτοί οι μηχανισμοί μπορούν να εφαρμοστούν στο ανώτερο επίπεδο της αρχιτεκτονικής των υπαρχόντων ΚΕΔ και να συναλλάσσονται με τους μηχανισμούς ασφάλειας που είναι βασισμένοι στη CORBA. Αυτό μπορεί να επιτευχθεί με τη χρήση των ειδικών πακέτων (Replaceability packages of the CORBA Security Service). Η χρήση των χαρακτηριστικών πρότυπων (API) στην αλληλεπίδραση με τις εξωτερικές υπηρεσίες ασφάλειας, επιτρέπει, όχι μόνο την αμφίδρομη ανταλλαγή των μηχανισμών ασφάλειας, αλλά και την εφαρμογή/χρήση ήδη υπαρχόντων (και δοκιμασμένων) μηχανισμών ασφάλειας. Οι μηχανισμοί ασφάλειας πρέπει να είναι όσο το δυνατόν περισσότερο αδιαφανείς για τον τελικό χρήστη και δε θα πρέπει να επηρεάζουν τη λειτουργικότητα του όλου δικτύου.

Μηχανισμοί ασφάλειας με-CORBA

Η χρήση των μηχανισμών ασφάλειας με-CORBA απαιτεί τη συνεργασία των πακέτων CORBA Secure Interoperability (CSI), τα οποία είναι δομημένα σε πολλαπλά επίπεδα. Λεπτομερής περιγραφή των πακέτων ασφάλειας και των μηχανισμών μπορεί να βρεθεί στο CORBA Security Services Specification [16]. Σε αυτή την ενότητα παρουσιάζονται τα πακέτα ασφάλειας CORBA τα οποία είναι απαραίτητα για τη λειτουργία της προτεινόμενης αρχιτεκτονικής ΚΕΔ. Περιγράφεται, επίσης, και το είδος των μηχανισμών ασφάλειας οι οποίοι περιέχονται σε κάθε πακέτο. Η προτεινόμενη αρχιτεκτονική απαιτεί τη χρήση του πακέτου Main Security Functionality Package Level 2 το οποίο επιτρέπει στις εφαρμογές να ελέγχουν την ασφάλεια που παρέχεται κατά την κλήση των αντικειμένων. Παρέχει, επίσης, τη δυνατότητα η πολιτική διαχείρισης να είναι ευέλικτη και μεταφέρσιμη. Επιπλέον, χρησιμοποιούνται τα πακέτα

SECIOP Interoperability, τα οποία παρέχουν τη δυνατότητα στο πρωτόκολλο ORB πάνω από GIOP/IIOP να επικοινωνεί με ασφάλεια χρησιμοποιώντας το πρωτόκολλο TCP/IP.

Το πακέτο Common Secure Interoperability Feature (CSI Level 2) που χρησιμοποιείται παρέχει τη δυνατότητα δημιουργίας μιας ευέλικτης πολιτικής πρόσβασης. Σε μια εφαρμογή που βασίζεται στη τεχνολογία CORBA μια οντότητα - κάποιος χρήστης, κάποιο αντικείμενο - μπορεί να κατέχει κατάλληλα δικαιώματα πρόσβασης που κάνουν εφικτή τη πρόσβαση σε κάποια υπηρεσία. Αυτά τα δικαιώματα χωρίζονται σε *ταυτότητες* και *ιδιότητες/χαρακτηριστικά πρόσβασης*. Κάθε οντότητα μπορεί να έχει μια η περισσότερες ταυτότητες, οι οποίες μπορεί να χρησιμοποιηθούν ώστε να αναγνωριστεί/ταυτοποιηθεί ο δημιουργός ενός μηνύματος και να μπορέσει, έτσι, να χρεωθεί ο χρήστης για τις υπηρεσίες που έλαβε, είτε να του καταλογιστούν ευθύνες για άνομες πράξεις. Τα χαρακτηριστικά πρόσβασης κατηγοριοποιούν τους χρήστες σε διάφορες *ομάδες* ή *ρόλους*, καθένας από τους οποίους έχει διαφορετικά δικαιώματα πρόσβασης στις υπηρεσίες του δικτύου.

Το πακέτο CSI Level 2 επιτρέπει στα αντικείμενα CORBA να μοιράζουν/αποστέλλουν/μεταβιβάζουν (delegate) ταυτότητες και χαρακτηριστικά πρόσβασης σε άλλα αντικείμενα CORBA με τη χρήση της *ελεγχόμενης αποστολής*. Αυτό σημαίνει το αρχικά εξουσιοδοτημένο αντικείμενο ελέγχει την περαιτέρω αποστολή/παραχώρηση αυτών των χαρακτηριστικών.

Παρόλο που το ORB μπορεί να παρέχει άμεσα ασφάλεια με τη χρήση του πακέτου CSI Level 2, σε αυτή την περίπτωση ούτε η ορισμένη πολιτική ασφάλειας, ούτε η εφαρμογή των υπηρεσιών ασφάλειας μπορούν να αντικατασταθούν. Η ενσωμάτωση των υπηρεσιών ORB Services Replaceability και του πακέτου Security Replaceability επιτρέπει την αντικατάσταση των πρότυπων υπηρεσιών ασφάλειας CORBA [16] (CORBA Security Services), όπου αυτό είναι απαραίτητο. Αυτά τα πακέτα επιτρέπουν τη χρήση ζεύξεων, οι οποίοι επι-

τρέπουν τη μετάδοση των δικαιωμάτων πρόσβασης CORBA μέσω μη-CORBA εφαρμογών. Επιπλέον, αυτά τα πακέτα παρέχουν συστήματα διεπαφής για τη διαλειτουργικότητα με εξωτερικούς μηχανισμούς ασφάλειας μη-CORBA. Αυτό επιτρέπει την χρήση υπαρχόντων εφαρμογών τέτοιων μηχανισμών, μέσω πρότυπων Application Programming Interfaces (API).

Εκτός από τα πακέτα ασφάλειας CORBA, χρησιμοποιούνται, επίσης και οι μηχανισμοί ασφάλειας CORBA. Για την πιστοποίηση και την προστασία των διαπιστευτηρίων των χρηστών χρησιμοποιείται το πακέτο CORBA Privilege Attribute Certificates (PAC). Ένα PAC περιέχει τα διαπιστευτήρια ενός χρήστη, όπως φαίνεται και στον πίνακα 4.1. Με τη χρήση της μεθόδου εξουσιοδότησης Protection Value / Control Value (PV/CV), το PAC προστατεύεται από τους μη εξουσιοδοτημένους χρήστες. Επιπλέον, η μέθοδος PV/CV ελέγχει τους επιτρεπόμενους στόχους/προορισμούς της εξουσιοδότησης των PAC. Το PAC περιέχει επίσης την ημερομηνία λήξης του και είναι υπογεγραμμένο από μια έμπιστη οντότητα.

Σημειώνεται ότι τα PAC αποτελούν έναν αποτελεσματικό/ βολικό τρόπο για την ανάπτυξη δυναμικών και ευέλικτων πολιτικών με τη χρήση του Role Based Access Control (RBAC). Διαφορετικά PAC μπορούν να εφαρμοστούν για διαφορετικούς ρόλους στην εφαρμογή, (π.χ. το διαχειριστή της υπηρεσίας ΕΔ, το διαχειριστή του κόμβου ΕΔ, το τερματικό χρήστη). Αυτά τα PAC θα περιέχουν τα δικαιώματα πρόσβασης που έχουν ανατεθεί σε κάθε ρόλο.

Πίνακας 4.1: *Η δομή ενός PAC.*

Εκδότης	Σειριακός Αρ.	Ιδιοκτήτης	Εγκυρότητα	Χαρακτηριστικά	Ταυτότητες	Στόχοι	Υπογραφή
Η CA που εκδίδει και υπογράφει το PAC	Μια μοναδική ταυτότητα του PAC	Ο ιδιοκτήτης του PAC	Μια έγκυρη χρονική περίοδος για το PAC	Το χαρακτηριστικό προνόμιο και ο ρόλος του PAC	Οι ταυτότητες του PAC	ελέγχει τις τελικές εξουσιοδοτήσεις του PAC	Η υπογραφή του εκδότη στο PAC

Για την ασφαλή επικοινωνία των αντικειμένων CORBA, χρησιμοποιείται το πρωτόκολλο CSI-ECMA [14], το οποίο υποστηρίζει PAC για ελεγχόμενη ε-

ξουσιοδότηση και το πρωτόκολλο CSI-ECMA το οποίο επιτρέπει τη χρήση τεχνολογιών συμμετρικών και ασύμμετρων (δημόσιων) κλειδιών για την επικοινωνία ανάμεσα στις οντότητες CORBA.

Ο πίνακας 4.2 περιλαμβάνει τα πακέτα ασφάλειας CORBA και τους μηχανισμούς που χρησιμοποιούνται καθώς και τις εξαρτήσεις που έχουν με άλλα πακέτα ασφάλειας ή/και μηχανισμούς CORBA.

Πίνακας 4.2: *Πακέτα ασφάλειας CORBA, μηχανισμοί και οι εξαρτήσεις τους.*

Πακέτα (Μηχανισμοί)	Εξαρτήσεις σε πακέτα (Μηχανισμοί)
Main Security Functionality Level 2	Security, CORBA, TimeBase, Security Level 1, SecurityAdmin
SECIOP	Security, CORBA, TimeBase, IOP
ORB Service Replaceability	CORBA
Security Service Replaceability	Main Security Functionality Level 2
CSI-Level 2	Main Security Functionality Level 2 SECIOP
(CSI-ECMA)	Security Functionality Level 2, SECIOP,CSI-Level 2
(PAC)	(CSI-ECMA)
(PV/CV method)	(CSI-ECMA, PAC)

Μηχανισμοί ασφάλειας μη-CORBA

Όπως έχει αναφερθεί στην προηγούμενη ενότητα, το σύστημα διεπαφής των πακέτων αντικαταστασιμότητας CORBA (replaceability packages) επιτρέπει την ενσωμάτωση υπηρεσιών ασφάλειας με τη χρήση API. Αυτές οι υπηρεσίες μπορεί να περιλαμβάνουν πιστοποίηση, διαμοιρασμό κλειδιών, υπηρεσίες πιστοποίησης και ελέγχου (auditing) ή χαμηλού επιπέδου υπηρεσίες όπως δια-

δικασίες κρυπτογράφησης.

Για την ασφαλή επικοινωνία ανάμεσα στις οντότητες του συστήματος, χρησιμοποιείται συμμετρική και ασύμμετρη κρυπτογράφηση. Οι κρυπτογραφικές λειτουργίες μπορούν να υποστηριχθούν μέσω της υπηρεσίας Cryptographic Support Facility της CORBA, που μπορεί να χρησιμοποιήσει ήδη υπάρχοντες αλγόριθμους κρυπτογράφησης αποδεδειγμένης εγκυρότητας. Κάθε τερματικός χρήστης, όπως και κάθε κόμβος στο ΕΔ, καταλαμβάνει ένα ζεύγος δημόσιου/κρυφού κλειδιού προς κρυπτογραφική χρήση (π.χ., κλειδιά RSA [19]). Για λόγους αποτελεσματικότητας, οι οντότητες του συστήματος χρησιμοποιούν τα κλειδιά ασύμμετρης κρυπτογράφησης, ώστε να ανταλλάξουν τα κλειδιά συμμετρικής κρυπτογράφησης (π.χ., τα κλειδιά DES [15]). Αυτό γίνεται ώστε η διαδικασία να γίνει συντομότερη αφού η συμμετρική κρυπτογράφηση είναι σημαντικά γρηγορότερη.

Χρησιμοποιείται μια Αρχή Πιστοποίησης (Certifying Authority - CA) ώστε να παράγει πιστοποιητικά δημόσιων κλειδιών X.509 και με τον τρόπο αυτό να προστατευτεί η ακεραιότητα και η αυθεντικότητα των δημόσιων κλειδιών [11]. Για λόγους απλότητας υποτίθεται ότι η ίδια Αρχή (CA) πιστοποιεί και τα CORBA PAC που χρησιμοποιούνται για την πιστοποίηση των δικαιωμάτων πρόσβασης, παρόλο που μπορεί να χρησιμοποιηθεί διαφορετική Αρχή Πιστοποίησης.

Για την εμπιστευτικότητα και την ακεραιότητα της επικοινωνίας ανάμεσα στις μη-CORBA οντότητες χρησιμοποιείται το πρωτόκολλο TLS [6], το οποίο εγκαθιστά ασφαλή κανάλια για απομακρυσμένους κόμβους. Επιπλέον, με το συνδυασμό του πρωτοκόλλου TLS με τα πιστοποιητικά X.509 μπορεί να επιτευχθεί αμφίδρομη πιστοποίηση μεταξύ των απομακρυσμένων κόμβων.

Τέλος, για την ασφάλεια των μονοπατιών μετανάστευσης των πρακτόρων, χρησιμοποιείται το ασφαλές κανάλι Grasshopper migration channel [12]. Αυτό το πρωτόκολλο χρησιμοποιεί επίσης το συνδυασμό TLS με ψηφιακά πρωτόκολλα.

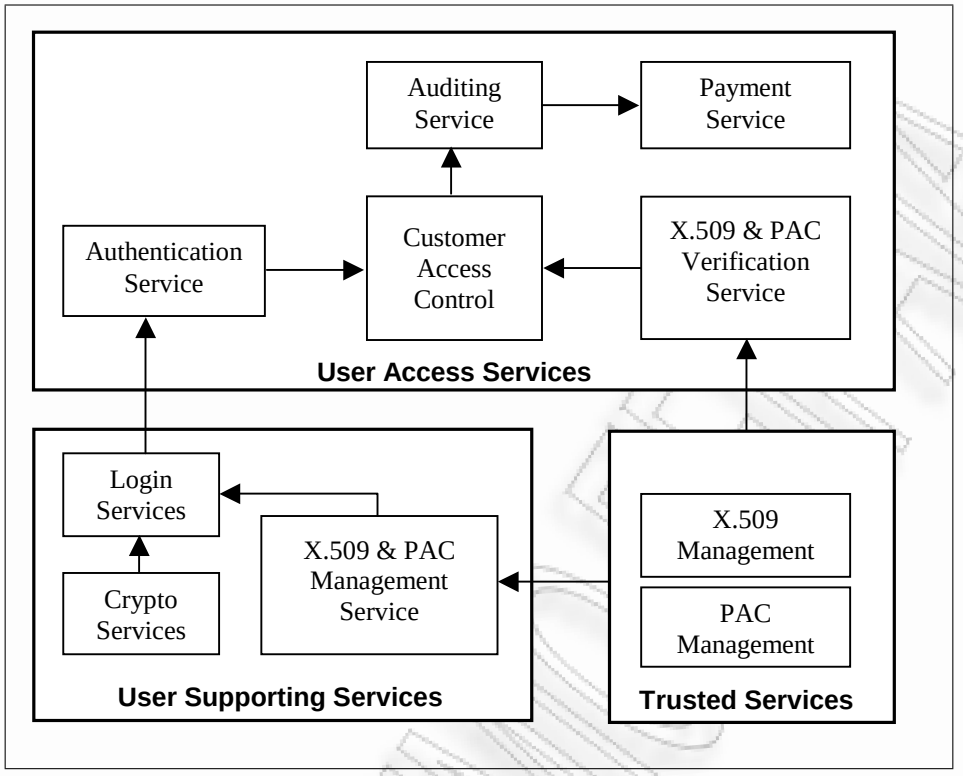
4.3.3 Ένα μοντέλο ασφάλειας για τα DIN

Όπως περιγράφεται και στο [24], οι υπηρεσίες ασφάλειας μπορεί να διαχωριστούν στις παρακάτω κατηγορίες: *Υπηρεσίες Υποστήριξης Χρήστη* (User Supporting Services), *Υπηρεσίες Πρόσβασης Χρήστη* (User Access Services), *Υπηρεσίες Διαχείρισης Πρόσβασης* (Management Access Services) και *Εμπιστευτικές Υπηρεσίες* (Trusted Services). Οι Υπηρεσίες Υποστήριξης Χρήστη εφαρμόζονται τοπικά από τους τερματικούς χρήστες του δικτύου ώστε να τους εξασφαλίσουν τη διαχείριση των ψηφιακών πιστοποιητικών και των PAC τους, τη διαδικασία σύνδεσης στο δίκτυο καθώς και τα πρωτόκολλα (και αλγόριθμους) κρυπτογράφησης.

Οι Υπηρεσίες Πρόσβασης Χρήστη περιλαμβάνουν τις υπηρεσίες ασφάλειας που εφαρμόζονται στα διάφορα επίπεδα της αρχιτεκτονικής των ΕΔ και ελέγχουν την πιστοποίηση του χρήστη. Οι ίδιες υπηρεσίες διαχειρίζονται, επίσης, και τους λογαριασμούς που υποδεικνύουν τα δικαιώματα πρόσβασης στο δίκτυο των χρηστών. Οι Υπηρεσίες Πρόσβασης Χρήστη περιλαμβάνουν επιπρόσθετα την υπηρεσία που είναι υπεύθυνη για την επαλήθευση των πιστοποιητικών και των PAC των χρηστών και του ελέγχου των συναλλαγών. Τέλος, μπορεί να περιλαμβάνουν μια υπηρεσία πληρωμής, η οποία μπορεί να χρησιμοποιεί την ανωτέρω υπηρεσία ελέγχου συναλλαγών ώστε να χρεώσει κατάλληλα τους χρήστες.

Οι Υπηρεσίες Διαχείρισης Πρόσβασης ελέγχουν τη πρόσβαση στο τμήμα διαχείρισης των υπηρεσιών. Το κεφάλαιο αυτό ασχολείται κατά κύριο λόγο με θέματα που σχετίζονται με τη πρόσβαση των χρηστών. Ωστόσο, η προτεινόμενη αρχιτεκτονική μπορεί να επεκταθεί ώστε να διαχειρίζεται και θέματα διαχείρισης υπηρεσιών.

Τέλος, οι Εμπιστευτικές Υπηρεσίες περιλαμβάνουν τη διαχείριση (δημοσίευση και ανάκληση) των πιστοποιητικών X.509 και των PAC των τερματικών χρηστών και των κόμβων του ΕΔ. Αυτές οι υπηρεσίες διαχειρίζονται από μια



Εικόνα 4.2: *Ασφαλής Λειτουργική Αρχιτεκτονική*

Αρχή Πιστοποίησης (Certifying Authority - ΆΑ), η οποία θεωρείται ότι αποτελεί μια Έμπιστη Τρίτη Οντότητα (Trusted Third Party). Η εικόνα 4.2 παρουσιάζει τις λειτουργικές οντότητες οι οποίες είναι απαραίτητες για την υλοποίηση της προτεινόμενης ασφαλούς αρχιτεκτονικής των ΕΔ.

Στην εικόνα 4.3 παρουσιάζεται η ολοκληρωμένη η ασφαλής αρχιτεκτονική του ΕΔ και ο τρόπος με τον οποίο αλληλεπιδρούν οι λειτουργικές οντότητες ασφάλειας με τις υπόλοιπες λειτουργικές οντότητες του ΕΔ. Θεωρείται απαραίτητο ότι κάθε τερματικός χρήστης που είναι εγγεγραμμένος σε μια υπηρεσία IMR πρέπει να πιστοποιηθεί με την CA χρησιμοποιώντας κάποιο διαφορετικό κανάλι/τρόπο επικοινωνίας από αυτόν που χρησιμοποιείται για την συνήθη επικοινωνία μεταξύ οντοτήτων ή χρηστών στο δίκτυο (out-of-band authentication). Επίσης, θεωρείται δεδομένο ότι η CA έχει δημοσιεύσει/εκδόσει ένα πιστοποιητικό X.509 για το δημόσιο κλειδί του χρήστη. Επιπλέον, η CA

έχει εκδόσει ένα PAC για κάθε εγγεγραμμένο χρήστη, το οποίο περιέχει τις ταυτότητες, τα δικαιώματα πρόσβασης και τους περιορισμούς εξουσιοδότησης (delegation) του συγκεκριμένου χρήστη.

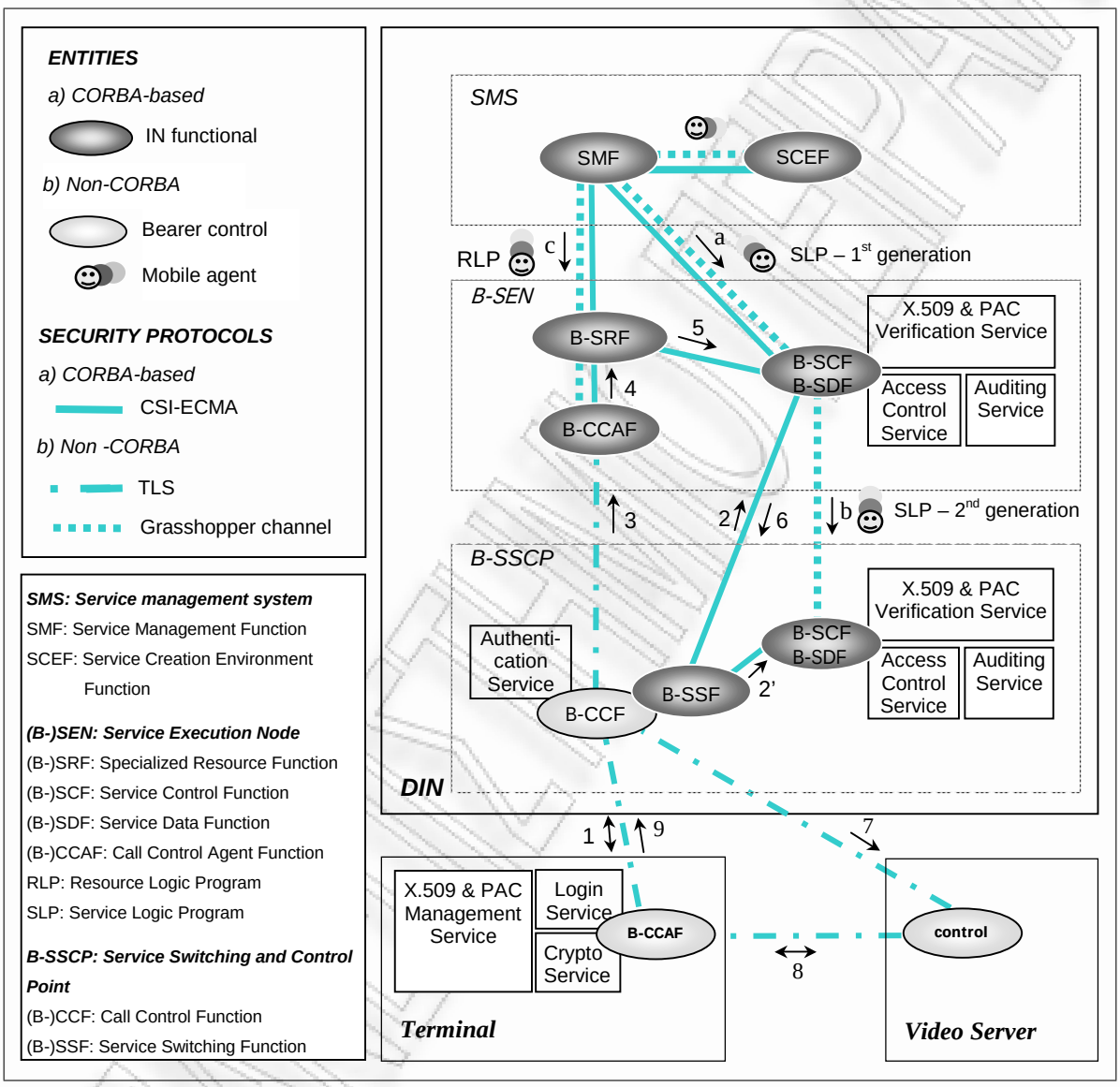
Ένας χρήστης που επιθυμεί να προσπελάσει μια υπηρεσία IMR, προετοιμάζει ένα μήνυμα αίτηση, το οποίο αποστέλλεται στην οντότητα B-CCF του κόμβου B-SSCP (βλέπε εικόνα 4.3). Η υπηρεσία σύνδεσης της οντότητας B-CCAF και η υπηρεσία πιστοποίησης της οντότητας B-CCF χρησιμοποιούν τα ψηφιακά πιστοποιητικά του τερματικού χρήστη και του κόμβου B-SSCP, αντιστοίχως. Τα ψηφιακά αυτά πιστοποιητικά χρησιμοποιούνται ώστε να εγκαθιδρυθεί μια ασφαλής σύνδεση μέσω του πρωτοκόλλου TLS (βήμα 1). Ο τερματικός χρήστης πιστοποιείται μέσω του πρωτοκόλλου TLS στον κόμβο B-SSCP και ανταλλάσσεται ένα κλειδί συμμετρικής κρυπτογράφησης. Αυτό το κλειδί θα χρησιμοποιηθεί για να εξασφαλιστεί η εμπιστευτικότητα της συνόδου. Η υπηρεσία πιστοποίησης της οντότητας B-CCF, η οποία ελέγχει την επικοινωνία των τερματικών χρηστών, επιτρέπει μόνο μια αίτηση ανά τερματικό χρήστη, ώστε να αποφευχθούν επιθέσεις άρνησης υπηρεσίας (DoS attacks).

Τότε, η υπηρεσία σύνδεσης της οντότητας B-CCAF χρησιμοποιεί την υπηρεσία διαχείρισης των PAC με σκοπό να μεταδώσει μέσω του καναλιού TLS το PAC του χρήστη μαζί με την αίτηση για χρήση της υπηρεσίας IMR, στην οντότητα B-CCF. Σημειώνεται ότι η B-CCF δεν αποτελεί οντότητα CORBA και δεν μπορεί, έτσι, να χρησιμοποιήσει τα διαπιστευτήρια που περιέχονται στο PAC. Ωστόσο, με τη χρήση των κατάλληλων διαβιβαστών, το PAC μπορεί να μεταβιβαστεί στην οντότητα B-SSF, η οποία αποτελεί αντικείμενο CORBA. Το ανωτέρω μπορεί να επιτευχθεί με εφαρμογή της προσέγγισης που προτείνεται στο [9] και χρησιμοποιεί GSS-APIs. Ενδιαφέρουσες εναλλακτικές προσεγγίσεις θα αποτελούσαν είτε η εξουσιοδότηση των PAC με τη χρήση μιας αλυσίδας πιστοποιητικών και υπογραφών όπως προτείνεται στο [2], είτε μια υβριδική

λύση όπως στο [1] στο οποίο προτείνεται η ενσωμάτωση των PAC μέσα στο πρωτόκολλο TLS.

Η μέθοδος PV/CV, που ελέγχει την εξουσιοδότηση των PAC, επιτρέπει την απλή εξουσιοδότηση του PAC. Επιπλέον, περιορίζει τον στόχο/προορισμό της εξουσιοδότησης σε μια από τις δύο οντότητες B-SCF/B-SDF, που βρίσκονται είτε στον κόμβο B-SSCP είτε στον B-SEN. Αυτό γίνεται καθώς σύμφωνα με τη λογική της λειτουργίας του ΕΔ, μια αίτηση θα εξυπηρετηθεί από μια από τις παρόμοιες αυτές οντότητες (εκτελείται είτε το βήμα 2 ή το βήμα 2'). Και στις δυο περιπτώσεις, η εξουσιοδότηση του PAC πραγματοποιείται με τη χρήση του πρωτοκόλλου CSI-ECMA. Ωστόσο, εάν η οντότητα B-SSF πρέπει να επικοινωνήσει με την οντότητα B-SCF/B-SDF του ανωτέρου επιπέδου (του κόμβου B-SEN), τότε χρησιμοποιείται ο μηχανισμός κρυπτογράφησης του πρωτοκόλλου CSI-ECMA. Ο μηχανισμός αυτός βασίζεται όχι μόνον στα βασικά κλειδιά αλλά και στα κλειδιά συνόδου. Σε αυτή τη περίπτωση χρησιμοποιείται το πιστοποιητικό X.509 των κόμβων B-SSCP και B-SEN για την ανταλλαγή ενός 'βασικού' κλειδιού, το οποίο χρησιμοποιείται στη συνέχεια για τη δημιουργία ενός (συμμετρικού) κλειδιού συνόδου. Το τελευταίο αυτό κλειδί χρησιμοποιείται για τη συμμετρική κρυπτογράφηση.

Η οντότητα B-SCF/B-SDF που θα εξυπηρετήσει την αίτηση χρησιμοποιεί την ενυπάρχουσα υπηρεσία επαλήθευσης του PAC, ώστε να ελεγχθεί η αυθεντικότητα/πιστότητα και η εγκυρότητα του PAC, πριν την εξυπηρέτηση της αίτησης. Ο τερματικός χρήστης επικοινωνεί επίσης και με την οντότητα B-SRF μέσω της οντότητας B-CCAF του κόμβου B-SEN (βήματα 3, 4). Το κανάλι αυτό χρησιμοποιείται ώστε να παρασχεθούν στο χρήστη οθόνες, περιέχουσες επιλογές και δείγματα video. Οι επιλογές αυτές είναι απαραίτητες ώστε ο χρήστης να μπορέσει να κάνει μια προσεκτική και έγκυρη επιλογή υπηρεσίας. Αυτή η επικοινωνία δεν απαιτεί κάποια κρυπτογράφηση, από τη στιγμή που αυτά τα δείγματα video είναι διαθέσιμα για τον κάθε χρήστη, είτε



Εικόνα 4.3: *Μια ασφαλής αρχιτεκτονική DIN [24].*

είναι εγγεγραμμένος είτε όχι. Αυτό γίνεται για εμπορικούς - διαφημιστικούς λόγους.

Η οντότητα B-SCF/B-SDF θα επικοινωνήσει με την οντότητα B-SRF του κόμβου B-SEN, ώστε να λάβει τις επιπλέον πληροφορίες για την αίτηση του χρήστη (βήμα 5). Τότε, η ενυπάρχουσα υπηρεσία ελέγχου πρόσβασης χρησιμοποιείται για να ελέγξει εάν τα διαπιστευτήρια του χρήστη είναι επαρκή για τη συγκεκριμένη υπηρεσία IMR. Εάν η επαλήθευση είναι επιτυχής, τότε η οντότητα B-SCF/B-SDF θα στείλει στην B-SSF (βήμα 6) τις κατάλληλες πληροφορίες για τις απαιτήσεις της υπηρεσίας π.χ., το IP του εξυπηρετητή που έχει αποθηκευμένα τα video. Εάν η επικοινωνία είναι ανάμεσα στην B-SCF/B-SDF οντότητα του κόμβου B-SEN και στην B-SSF του κόμβου B-SSCP τότε χρησιμοποιείται το πρωτόκολλο CSI-ECMA με δύο επίπεδα κρυπτογράφησης.

Αυτή τη στιγμή η οντότητα B-SSF έχει όλες τις πληροφορίες που της χρειάζονται για την ολοκλήρωση των απαιτήσεων της υπηρεσίας. Οι πληροφορίες αυτές έχουν διαβιβαστεί μαζί με τα πιστοποιητικά του χρήστη στην οντότητα B-CCF (βήμα 7). Ο εξυπηρετητής video χρησιμοποιεί αυτά τα πιστοποιητικά ώστε να εγκαθιδρύσει μια σύνδεση TLS με τον χρήστη (βήμα 8) και ολοκληρώνει την αίτηση. Ωστόσο, από τη στιγμή που η μετάδοση του video επιβαρύνει κατά πολύ το δίκτυο, ίσως να ήταν καταλληλότερη μια κρυπτογράφηση χαμηλότερου επιπέδου (π.χ. με τη χρήση κλειδιών 40 bit). Κάθε μετάδοση video μαρκάρεται με ένα μοναδικό αναγνωριστικό, ώστε να αποφευχθούν επιθέσεις επανάληψης. Η οντότητα B-CCF ενημερώνεται τελικά για την επιτυχή εξέλιξη της επικοινωνίας (βήμα 9) και στη συνέχεια πληροφορεί την υπηρεσία ελέγχου για τις λεπτομέρειες (όπως χρήστη, εξυπηρετητή video, χρόνος υπηρεσίας, κλπ.). Εάν χρησιμοποιείται κάποια υπηρεσία κοστολόγησης τότε η υπηρεσία ελέγχου μπορεί να παρέχει τις απαραίτητες πληροφορίες για τις συναλλαγές για κάθε χρήστη ξεχωριστά.

Οι οντότητες SMF και SCEF του κόμβου SMS ελέγχουν τη λειτουργία του

ΕΔ. Στην περίπτωση που έχουν πραγματοποιηθεί λειτουργικές αλλαγές (για παράδειγμα έχει γίνει προσθήκη ενός νέου video είτε ένας επανακαθορισμός υπηρεσιών ανάμεσα στις οντότητες B-SCF/B-SDF) τότε θα πρέπει να ενημερωθούν οι οντότητες B-SCF/B-SDF και των δύο κόμβων B-SEN και B-SSCP. Αυτό πραγματοποιείται με μετανάστευση των πρακτόρων. Πρώτα, η οντότητα SMF του κόμβου SMS εγκαθιδρύει ένα ασφαλές μονοπάτι μετανάστευσης με την οντότητα B-SCF/B-SDF του κόμβου B-SEN (βήμα α), για τη μετανάστευση του πράκτορα πρώτης γενιάς. Η αμφίδρομη πιστοποίηση και η εγκαθίδρυση ενός κρυπτογραφημένου καναλιού για την προστασία της εμπιστοσύνης πραγματοποιούνται με τη χρήση των πιστοποιητικών των κόμβων SMS και του B-SEN. Τέλος, οι οντότητες B-SCF/B-SDF των κόμβων B-SEN και B-SSCP προετοιμάζουν ένα ασφαλές μονοπάτι μετανάστευσης για τους πράκτορες δεύτερης γενιάς, ώστε να ολοκληρωθεί η ενημέρωση / εκσυγχρονισμός της λειτουργικότητας του ΕΔ (βήμα β). Η ίδια προσέγγιση ακολουθείται για τη μετανάστευση των RLP πρακτόρων στην οντότητα B-SRF (βήμα γ).

Βιβλιογραφία

[1] Ashley P., Vandenwauer M., and Claessens J.,*Using SESAME to secure web based applications on an Intranet*,Proceedings of the IFIP TC6/TC11, 303–317, CMS'99, Katholieke Universiteit Leuven, Belgium (1999).

[2] Aura T., Koponen P., and Rasanen J., *Delegation-based Access Control for Intelligent Network Services*, Proceedings of ECOOP Workshop on Distributed Object Security, Brussels, Belgium, July (1998).

[3] Breugst M., Magendaz T., *Mobile Agents - Enabling Technology for Active Intelligent Network Implementation*, IEEE Network, Vol. 12, no. 3, 53–60, May/June (1998).

[4] Chatzipapadopoulos F., Perdikeas M., and Venieris I., *Mobile Agent and CORBA Technologies in the Broadband Intelligent Network*, IEEE Communications Magazine, no 6, 116–124, June (2000).

[5] Chess D., *Security issues in Mobile Code Systems*, Modile Agents and Security, Lecture Notes in Computer Science, vol.1419, 1–14, Springer (1998).

[6] Dierks T., and Allen C., *The TLS Protocol Version 1.0*, RFC 2246, (1999), *http://www.faqs.org/rfcs/rfc2246.html*.

[7] Douligeris C. and Mavropodi R., *Performance Evaluation of Interactive Multimedia Retrieval in Intelligent Networks*, Procceedings of 8th International Con-

ference on Advances in Communications and Control, Rethymno Crete, Greece, 443-453 (June 25–29 /2001).

[8] European Computer Manufacturers Association, *ECMA-235, ECMA GSS API mechanism*. See also *ECMA-219, Authentication and Privilege Attribute Security Application with related key distribution functions*, http://www.ecma.ch/stand/ECMA-219.H™, (1996).

[9] Farrell S., *TLS Extensions for Attribute Certificate Based Authorization*, Internet Draft, August (1998).

[10] IKV++, *Grasshopper 2*, http://www.grasshopper.de/index.html

[11] ITU, Recomendation X.509, *The Directory: Abstract Service Definition*, International Telecommunications Union, Telecommunication Standardization Sector (ITU-T), (1993).

[12] IKV++, *Grasshopper security service*, http://www.grasshopper.de/ download/doc/pguide2.2.pdf

[13] Koponen P., Rasanen J., Martikainen O., *Calypso Service Architecture for Broadband Networks*, Proceedings of the 2nd IFIP Conference on Intelligent Networks and Intelligence in Networks, Paris, 73–82, (September 2–5/1997).

[14] Lang U., *CORBA security on the Web. An overview*, Future Generation Computer Systems, Vol. 16, No. 4, 417–421, (2000).

[15] National Bureau of Standards, *Data Encryption Standard - DES*, U.S. Department of Commerce, FIPS pub, 46, (1977).

[16] OMG, *CORBA security service, version 1.7*, http://www.omg.org/technology/documents/formal/security_service.htm, (1999).

[17] OMG, *CORBA 3*, http://www.omg.org/technology/CORBA/CORBA3releaseinfo.htm

[18] Papadakis I., Chrissikopoulos V., and Polemi D., *A Secure Web-based Medical Digital Library Architecture based on TTPs*, Proceedings of MIE2000, 610–616, Hanover Germany, (August 27 - September -1,2000).

[19] Rivest R. L., Shamir A. and Adleman, *A method for obtaining digital signatures and public key cryptosystems*, Communications of ACM, 294–299, vol. 21, no 2, (1978).

[20] Kevin H. Liu, *Intelligent network control middleware platform*, IEEE Communications Magazine, vol. 43, no. 5, May 2005, pp. 11 - 18.

[21] Olga Ormond, *John Murphy and Gabriel-Miro Muntean Utility-based intelligent network selection in beyond 3G systems*, ICC 2006 - IEEE International Conference on Communications, no. 1, June 2006, pp. 1816 - 1821.

[22] Masami Yabusaki, *Takatoshi Okagawa and Kazuo Imai Mobility management in all-IP mobile network: End-to-end intelligence or network intelligence*, IEEE Communications Magazine, vol. 43, no. 12, Dec 2005, pp. 16 - 24.

[23] Venieris I. Hussmann H., *Intelligent Broadband Networks*, John Wiley & Sons, West Sussex England (1998).

[24] Kotzanikolaou P., Mavropodi R., Douligeris C, Chrissikopoulos V, *Secure distributed intelligent networks*, Computer Communications, Vol 29, no 3, 325–336, 2006.

[25] Mavropodi R., Douligeris C., *Intelligent Networks - Security Issues and Performance Evaluation*, Annual Review of Communications, Volume 57, 2004.

[26] Kotzanikolaou P., Mavropodi R., Douligeris C, Chrissikopoulos V, *Secure distributed intelligent networks*, Computer Communications, Vol 29, no 3, 325–336, 2006.

[27] Mavropodi R., Douligeris C., *Performance Evaluation of Intelligent Network Topologies*, SCI 2003, Orlando, USA, July 27–30, 2003.

[28] Mavropodi R. and C. Douligeris, *Performance Evaluation of Interactive Multimedia Retrieval in Intelligent Networks*, ComCon 8,25–29, June 2001, Crete, Greece, 443–453.

[29] Mavropodi R., P. Kotzanikolaou and C. Douligeris, *Secure Management of Intelligent Networks through Intelligent Agents*, Workshop on Intelligent Agents and Virtual Reality, Athens, June 29, 2001, pp. 57–64.

[30] Douligeris C., R. Mavropodi and P. Kotzanikolaou, *Agent - Based Security in Intelligent Multimedia Retrieval in Intelligent Networks*, INFORMS Miami Annual Meeting, Miami Beach, FL, Nov. 2001.

Κεφάλαιο 5

Μελέτη Επίδοσης Ασφαλών Εφαρμογών σε περιβάλλοντα Ευφυών Δικτύων

Σε αυτό το κεφάλαιο μελετάται η επίδοση της κατανεμημένης εφαρμογής ευφυών δικτύων, που έχει περιγραφεί στο τέταρτο κεφάλαιο. Συγκεκριμένα θα μελετηθεί η συμπεριφορά του ευφυούς δικτύου όταν εφαρμόζονται επάνω του πολιτικές ασφάλειας στην εξυπηρέτηση υπηρεσιών αλληλεπιδραστικής παροχής πολυμεσικών δεδομένων. Θα παρουσιαστούν αποτελέσματα επίδοσης με τη χρήση της τεχνικής της προσομοίωσης. Θα αναλυθούν τα αποτελέσματα της μελέτης αυτής. Στη συνέχεια θα γίνει μια σύγκριση ανάμεσα σε δύο διαφορετικά εργαλεία προσομοίωσης, ώστε να γίνουν ορατές οι διαφορές που παρουσιάζονται ανάμεσα σε δύο διαφορετικές μελέτες προσομοίωσης.

5.1 Το μοντέλο Προσομοίωσης

Η μετακίνηση της πολιτικής της υπηρεσίας (SLPs) [2] πλησιέστερα στο χρήστη όπως και η ενοποίηση των μηχανισμών ασφάλειας έχουν ένα κόστος ιδιαίτερα στην επίδοση του δικτύου. Στη συνέχεια του κεφαλαίου αυτού μελεταται το κόστος αυτό με τη βοήθεια της τεχνικής της προσομοίωσης.

5.1.1 Τα Σενάρια

Εξετάζονται δύο διαφορετικές περιπτώσεις. Στην πρώτη περίπτωση η υπηρεσία εξυπηρετείται από την οντότητα B-SCF/B-SDF που εδρεύει στο κόμβο B-SEN (Εικόνα 5.1 περίπτωση a). Στη δεύτερη περίπτωση ο έλεγχος πραγματοποιείται ολοκληρωτικά στον κόμβο B-SSCF (Εικόνα 5.1 περίπτωση b). Στη δεύτερη περίπτωση ο έλεγχος της εκτέλεσης της υπηρεσίας πραγματοποιείται τοπικά και δεν υπάρχει ανάγκη για εξωτερική επικοινωνία. Το δίκτυο μπορεί να διαχειριστεί καλύτερα τους πόρους του από τη στιγμή που ο φόρτος σηματοδότησης έχει ελαττωθεί και έτσι το δίκτυο μπορεί να εξυπηρετήσει περισσότερες εφαρμογές. Για κάθε μια από τις ανωτέρω περιπτώσεις έχει μετρηθεί το επιπλέον βάρος στην επίδοση του δικτύου που δημιουργείται από την εφαρμογή των πολιτικών ασφάλειας.

Έχει χρησιμοποιηθεί ένα μοντέλο προσομοίωσης ώστε να αξιολογηθεί η επίδοση της προτεινομένης αρχιτεκτονικής. Το μοντέλο αυτό αποτελείται από ένα κόμβο B-SSCP, ένα κόμβο B-SEN, ένα τερματικό κόμβο και έναν εξυπηρετητή video για την παροχή των ζητούμενων video. Η ανωτέρω αρχιτεκτονική χρησιμοποιήθηκε καθώς η υπό μελέτη εφαρμογή είναι μια τυπική υπηρεσία IMR.

Η αλληλεπίδραση των κόμβων παρουσιάζεται στην Εικόνα 5.1. Αυτοί οι κόμβοι φιλοξενούν λειτουργικές οντότητες οι οποίες παρουσιάζονται ως ουρές. Στον τερματικό κόμβο έχει εφαρμοστεί ένας γεννήτορας μηνυμάτων που

ακολουθεί την ιδανική κατανομή Poisson. Αυτό έχει ως συνέπεια τα μεσοδιαστήματα ανάμεσα στα μηνύματα που ταξιδεύουν στο δίκτυο να ακολουθούν την εκθετική κατανομή. Ο γεννήτορας αυτός παράγει πακέτα-αιτήματα για χρήση της υπηρεσίας Video-on-Demand (VoD) τα οποία αιτήματα εξυπηρετούνται με τη σειρά με την οποία καταφτάνουν (FIFO). Θεωρείται δεδομένο ότι κάθε λειτουργική οντότητα χρησιμοποιεί αποκλειστικά έναν επεξεργαστή, ο οποίος χειρίζεται την εξυπηρέτηση των αφιχθέντων μηνυμάτων. Τα εναλλασσόμενα μηνύματα αναπαριστούν τη ροή πληροφορίας ανάμεσα στις οντότητες, όπως αυτή έχει περιγραφεί σε προηγούμενα κεφάλαια ή και στο [3].

5.1.2 Η Μοντελοποίηση

Η Εικόνα 5.2 παρουσιάζει τη ροή της πληροφορίας ανάμεσα στις οντότητες όταν έχει χρησιμοποιηθεί ο προτεινόμενος μηχανισμός ασφάλειας. Οι λειτουργικές οντότητες συνδέονται απευθείας μεταξύ τους και κατά συνέπεια οι καθυστερήσεις μετάδοσης θεωρούνται αμελητέες.

Οι κόμβοι του συστήματος θεωρείται ότι απέχουν 5 km μεταξύ τους, η ταχύτητα διάδοσης είναι 2×10^8 m/sec και ο ρυθμός μετάδοσης έχει οριστεί στα 10 Mbps. Το μέγεθος των πακέτων των μηνυμάτων ποικίλει, ακολουθεί δε την εκθετική κατανομή με μέσο μέγεθος πακέτου τα 1000 bit. Η έρευνα αυτή επικεντρώνεται στη μελέτη του τμήματος ελέγχου του δικτύου. Τα μηνύματα που μεταδίδονται σε αυτό το κανάλι επικοινωνίας (δηλ. τα μηνύματα ελέγχου) δεν απαιτούν μεγάλα πακέτα για τη μετάδοσή τους. Για λόγους συνέπειας έχουν πραγματοποιηθεί περαιτέρω πειράματα με μεγέθη πακέτων 10000 και 40000 bit.

Τα αποτελέσματα της προσομοίωσης έχουν εξαχθεί και υπολογιστεί με 10 βαθμούς ελευθερίας για ένα διάστημα εμπιστοσύνης 95%. Ο μέσος χρόνος καθυστέρησης έχει υπολογιστεί για 100 μηνύματα σε κάθε πείραμα. Οι χρόνοι καθυστέρησης λόγω εφαρμογής τεχνικών κρυπτογράφησης / αποκρυπτογρά-

φησης έχουν οριστεί ως εξής: 0.0085 msec για την εφαρμογή της τεχνικής RSA και 0.0027 msec για την τεχνική DES.

Οι χρόνοι καθυστέρησης έχουν υπολογιστεί σε έναν επεξεργαστή P3 1000 MHz μετά από 1000 κύκλους με κλειδιά RSA 1024-bit και κλειδιά DES 64-bit. Τα κλειδιά αυτά έχουν δημιουργηθεί με τη χρήση του PGP.

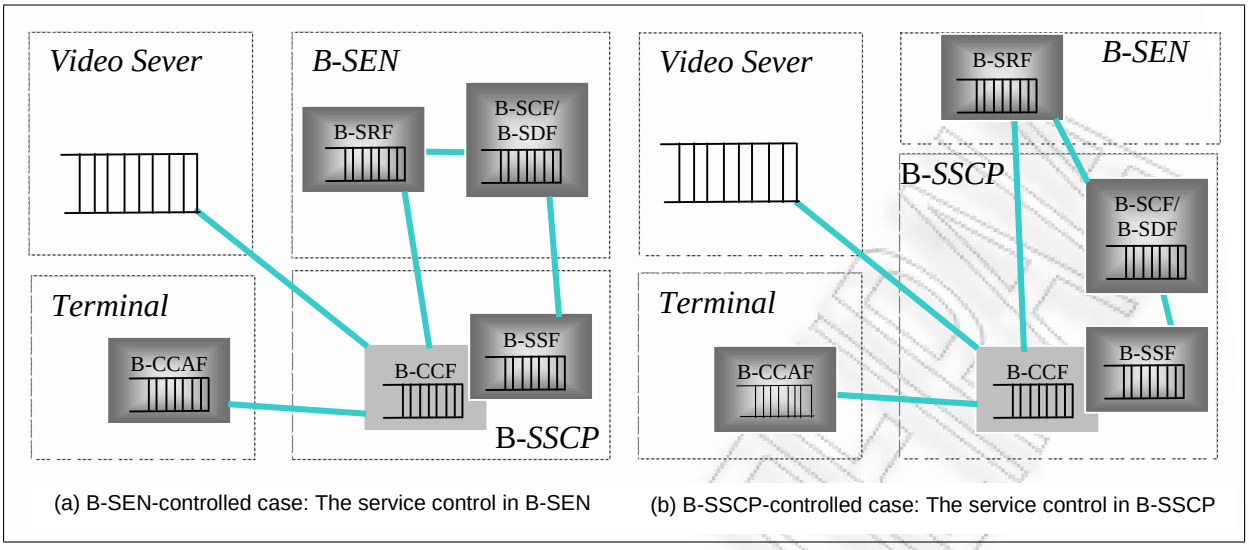
Στο μοντέλο της προτεινόμενης αρχιτεκτονικής πραγματοποιείται μετανάστευση μόνο του τμήματος του ελέγχου της υπηρεσίας. Για το λόγο αυτό στα πειράματα προσομοίωσης που έχουν πραγματοποιηθεί δεν έχουν ληφθεί υπόψη οι χρόνοι καθυστέρησης που εμφανίζονται στο κανάλι των δεδομένων. Η καθυστέρηση αυτών των πακέτων μπορεί να επηρεάσει μερικές παραμέτρους επίδοσης, όπως η καθυστέρηση λόγω αναμονής σε ουρά, αλλά δεν επηρεάζει το γενικότερο πρότυπο της επίδοσης των οντοτήτων σηματοδοσίας.

Κάθε φορά που ο χρήστης πραγματοποιεί μια κλήση για υπηρεσία IMR δημιουργείται μια αλληλουχία ανταλλαγής μηνυμάτων μεταξύ των οντοτήτων του δικτύου και κατ' επέκταση των κόμβων που αυτές φιλοξενούνται (Εικόνα 5.2). Θεωρείται ότι μια υπηρεσία ολοκληρώνεται όταν ο τερματικός κόμβος (Terminal Equipment (TE)) του χρήστη έχει στείλει ένα μήνυμα end_of_all. Η συνολική καθυστέρηση είναι το άθροισμα των καθυστερήσεων που εμφανίζουν αυτά τα μηνύματα κατά τη διάδοσή τους στους κόμβους του δικτύου.

Επειδή η προτεινόμενη αρχιτεκτονική δεν μπορούσε να προσεγγιστεί με κάποιο από τα γνωστά εργαλεία προσομοίωσης, κρίθηκε σκόπιμο να υλοποιηθεί εξ ολοκλήρου ως ένα νέο μοντέλο. Η γλώσσα που επιλέχθηκε να χρησιμοποιηθεί ήταν η C++, καθώς ο αντικειμενοστραφής (Object-Oriented) χαρακτήρας της βοηθούσε στην υλοποίηση των πακέτων του δικτύου ως γεγονότα.

5.2 Παρουσίαση Αποτελεσμάτων

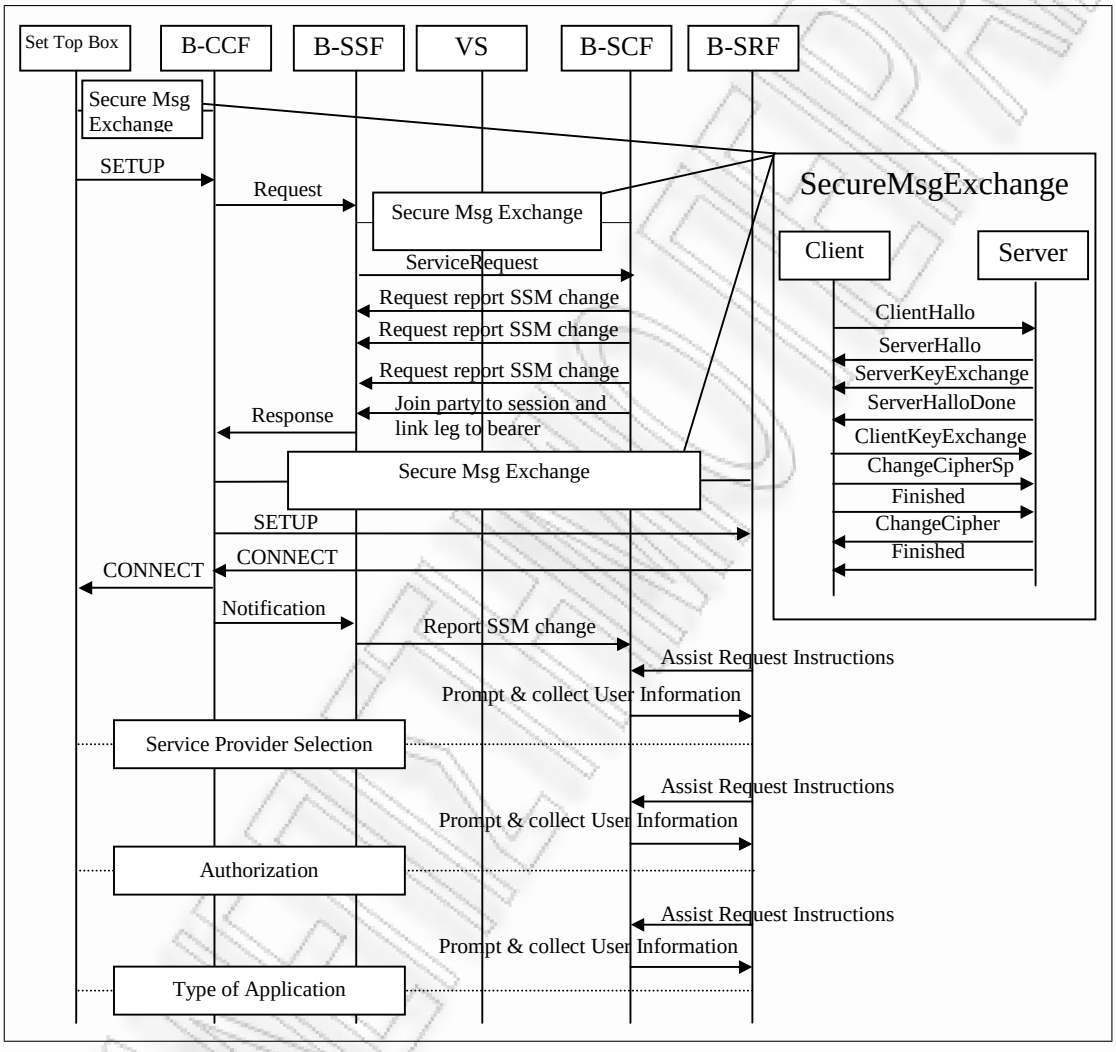
Η μετανάστευση του τμήματος ελέγχου της υπηρεσίας στον κόμβο B-SSCP, του κινητού πράκτορα SLP (δεύτερης γενιάς) προκαλεί μια σημαντική μείωση



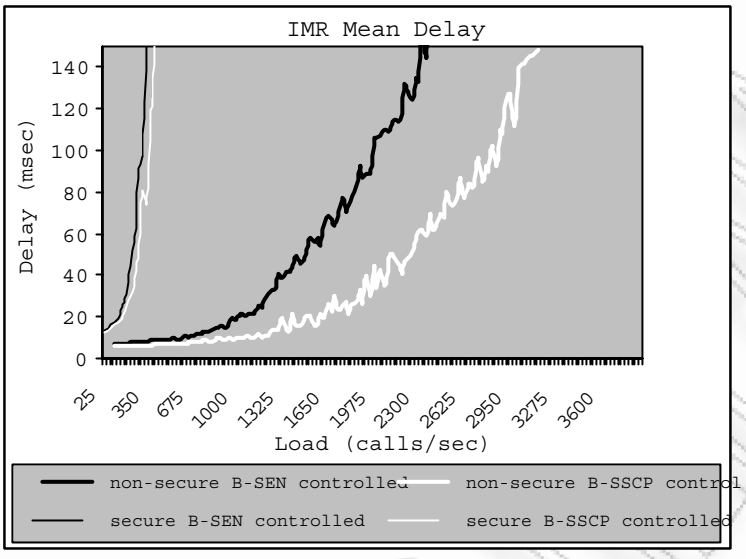
Εικόνα 5.1: *Το μοντέλο προσομοίωσης.*

στην καθυστέρηση ολοκλήρωσης της υπηρεσίας σε σύγκριση με την περίπτωση όπου το τμήμα ελέγχου της υπηρεσίας βρίσκεται/ εκτελείται από τον κόμβο B-SEN. Οι δύο αυτές περιπτώσεις, είτε έλεγχος από τον κόμβο B-SSCP ή έλεγχος από τον κόμβο B-SEN, παρουσιάζονται στις Εικόνες 5.1b και 5.1a, αντίστοιχα. Για καθεμιά από τις ανωτέρω περιπτώσεις εκτιμήθηκε η επιπλέον καθυστέρηση που προκαλείται από την εφαρμογή των μηχανισμών ασφάλειας. Η ενσωμάτωση των μηχανισμών ασφάλειας στην αρχιτεκτονική των ΕΔ προκαλεί μείωση της επίδοσης του συστήματος, κάτι το οποίο αναμενόταν αφού αυτοί οι μηχανισμοί καταναλώνουν / χρησιμοποιούν κρίσιμους πόρους από το σύστημα, όπως μνήμη και επεξεργαστική ισχύ. Η χρήση αυτών των μηχανισμών δεν επηρεάζει το πρότυπο επίδοσης των στοιχείων του δικτύου *π.χ.* το σύστημα αποδίδει καλύτερα στη περίπτωση που ο έλεγχος πραγματοποιείται από τον κόμβο B-SSCP ακόμα και κάτω από το βάρος των μηχανισμών ασφάλειας. Αυτή η διαφορά είναι περισσότερο έκδηλη στην περίπτωση όπου το φορτίο της διακινούμενης πληροφορίας γίνεται μεγαλύτερο.

Η εικόνα 5.3 παρουσιάζει τη συνολική καθυστέρηση της υπηρεσίας. Τα μηνύματα της εφαρμοσμένης πολιτικής ασφάλειας προκαλούν μια σημαντική



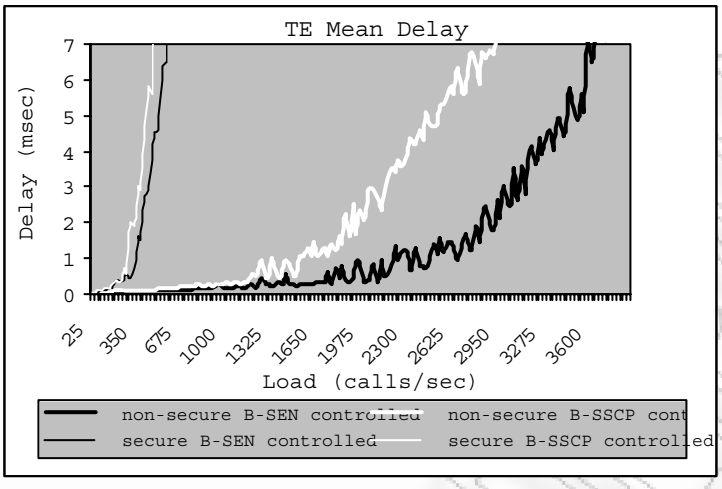
Εικόνα 5.2: *Ασφαλής ροή πληροφορίας (σύνδεση του χρήστη στην οντότητα B-SRF).*



Εικόνα 5.3: *Μέση καθυστέρηση IMR.*

μείωση στην επίδοση του συστήματος, αλλά η χρονική καθυστέρηση παραμένει σε χαμηλά, αποδεκτά όρια. Η ολοκλήρωση της υπηρεσίας είναι γρηγορότερη όταν το τμήμα ελέγχου της υπηρεσίας εκτελείται από τον κόμβο B-SSCP. Επιπλέον, η καθυστέρηση που παρουσιάζεται στον τερματικό κόμβο του τελικού χρήστη φαίνεται να αποδίδει καλύτερα στην περίπτωση που το τμήμα ελέγχου της υπηρεσίας βρίσκεται/ εκτελείται από τον κόμβο B-SEN (εικόνα 5.4). Αυτό αναμένεται καθώς στη δεύτερη περίπτωση το δίκτυο θα αντιδράσει/ απαντήσει γρηγορότερα στις απαιτήσεις του χρήστη, οι οποίες θα έχουν ως αποτέλεσμα την αύξηση του φόρτου επεξεργασίας της οντότητας. Το ίδιο ισχύει και όταν υπάρχουν εφαρμοσμένοι οι μηχανισμοί ασφάλειας.

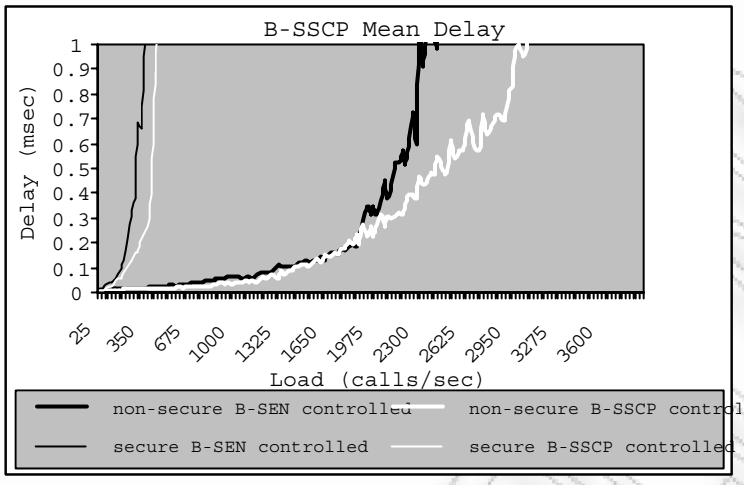
Η επίδοση των κόμβων B-SSCP και B-SEN φαίνεται να είναι καλύτερη στην περίπτωση όπου το τμήμα ελέγχου της υπηρεσίας εκτελείται από τον κόμβο B-SSCP (Εικόνες 5.5, 5.6). Παρόλο που η καθυστέρηση παραμένει σε πολύ χαμηλά επίπεδα η αύξησή της στην πρώτη περίπτωση είναι αξιοσημείωτη. Η αύξηση αυτή σχεδόν διπλασιάζεται ιδιαίτερα κάτω από υψηλό φόρτο κίνησης στο δίκτυο. Αυτό μερικώς αναμένεται καθώς στην περίπτωση όπου το τμήμα ελέγχου της υπηρεσίας εκτελείται από τον κόμβο B-SEN, ο κόμβος B-SSCP



Εικόνα 5.4: *Καθυστέρηση στον τερματικό κόμβο (TE).*

χρειάζεται να επικοινωνεί με τον κόμβο B-SEN ώστε να ελεγχθεί η ορθή εκτέλεση της υπηρεσίας. Αυτή η επικοινωνία έχει ως αποτέλεσμα ο κόμβος B-SSCP να υφίστανται καθυστέρηση καθώς αναμένει απόκριση από τον κόμβο B-SEN στις αιτήσεις του. Στην περίπτωση όπου το τμήμα ελέγχου της υπηρεσίας εκτελείται από τον κόμβο B-SSCP δεν υπάρχει αυτή η καθυστέρηση καθώς ο έλεγχος δεν απαιτεί την επικοινωνία με εξωτερικές του κόμβου οντότητες.

Η επεξεργασία των μηνυμάτων ασφάλειας επιβαρύνει το δίκτυο με επιπλέον καθυστέρηση. Όπως παρουσιάζεται στην Εικόνα 5.5 η επίδοση του κόμβου B-SSCP είναι η μικρότερη σε σχέση με τους B-SEN και TE. Είναι δόκιμο να παραχωρηθούν στον κόμβο επιπλέον πόροι από το σύστημα έτσι ώστε να αντιμετωπιστούν οι επιπλέον ανάγκες του κόμβου και να αποφευχθεί το φαινόμενο της συμφόρησης μηνυμάτων, το γνωστό ως πρόβλημα του στομίου μπουκάλας (bottleneck problem). Ο κόμβος B-SEN (Εικόνα 5.6), στην περίπτωση όπου το τμήμα ελέγχου της υπηρεσίας εκτελείται από τον κόμβο B-SEN, πρέπει να διαχειριστεί μεγαλύτερες ουρές μηνυμάτων καθώς φιλοξενεί τη λειτουργική οντότητα B-SCF/B-SDF, εξ ου και η αξιοσημείωτη διαφορά στην απόδοσή του. Η επεξεργασία των μηνυμάτων ασφάλειας δε δημιουργεί κάποιο φόρτο άξιο λόγου, καθώς η σηματοδοσία του κόμβου αυτού μειώνεται

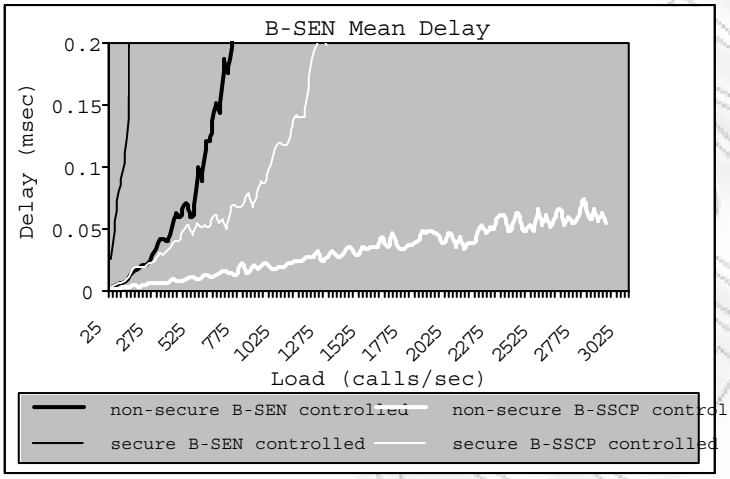


Εικόνα 5.5: *Μέση καθυστέρηση στον κόμβο B-SSCP.*

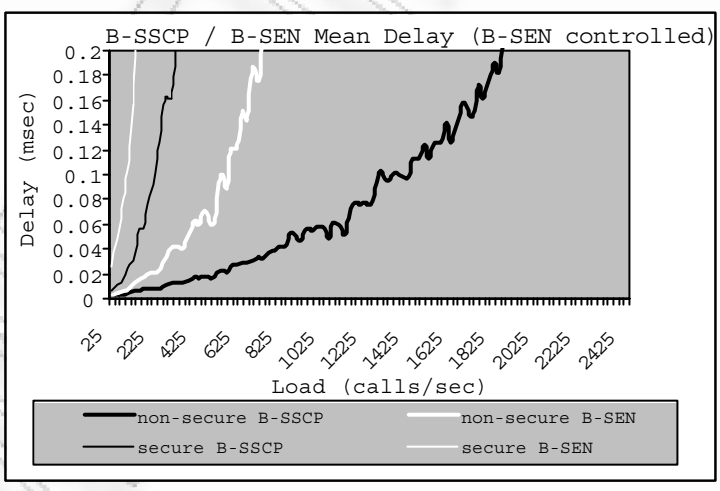
δραματικά μετά την μετανάστευση της λογικής της υπηρεσίας στον κόμβο B-SSCP.

Οι οντότητες οι οποίες προκαλούν σημαντική καθυστέρηση είναι οι B-SCF/B-SDF. Όπως φαίνεται και από τις εικόνες 5.7 και 5.8 η επίδοση του εκάστοτε κόμβου που φιλοξενεί τις λειτουργικές αυτές οντότητες, μειώνεται σημαντικά. Στην εικόνα 5.7 φαίνεται ότι ο κόμβος B-SSCP αποδίδει καλύτερα σε σχέση με τον κόμβο B-SEN αναφορικά με τις οντότητες B-SCF/B-SDF. Ωστόσο, στην περίπτωση όπου το τμήμα ελέγχου της υπηρεσίας εκτελείται από τον κόμβο B-SSCP το φορτίο σηματοδοσίας του B-SSCP είναι πολύ μεγαλύτερο και για το λόγο αυτό παρατηρείται η αύξηση της καθυστέρησης (εικόνα 5.8).

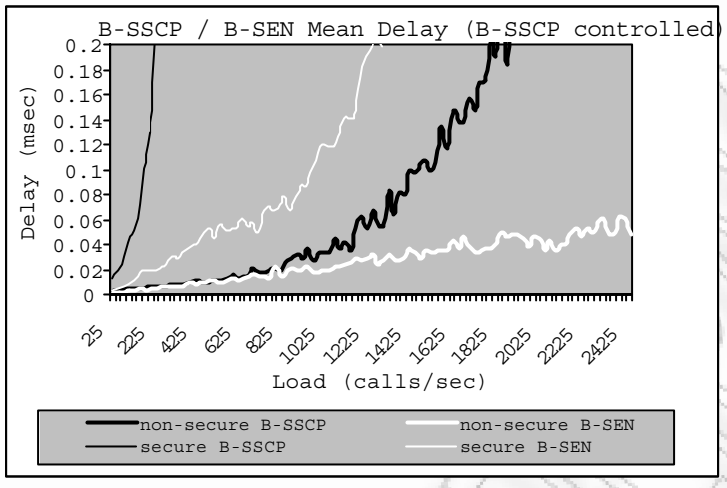
Η μετανάστευση της λογικής της υπηρεσίας στον κόμβο B-SSCP παρέχει στο σύστημα αποδοτικότερη λειτουργία. Η χρήση των μηχανισμών ασφάλειας προκαλεί μείωση στην απόδοσή του δικτύου, αλλά η καθυστέρηση παραμένει σε χαμηλά αποδεκτά όρια. Καθώς, μειώνεται η επίδοση του κόμβου στον οποίο φιλοξενείται, και κατά συνέπεια εκτελείται, η λογική ελέγχου της υπηρεσίας, θα πρέπει να παραχωρηθούν προς χρήση του επιπλέον πόροι συστήματος. Η παραχώρηση των επιπλέον πόρων μπορεί να αποτελέσει



Εικόνα 5.6: *Μέση καθυστέρηση στον κόμβο B-SEN.*



Εικόνα 5.7: *Σύγκριση των κόμβων B-SEN και B-SSCP αναφορικά με τη καθυστέρηση (έλεγχος στον B-SEN).*



Εικόνα 5.8: *Σύγκριση των κόμβων B-SEN και B-SSCP αναφορικά με τη καθυστέρηση (έλεγχος στον B-SSCP).*

πρόβλημα καθώς η μετανάστευση των πρακτόρων πλησιέστερα στον τελικό χρήστη προκαλεί την ανάγκη επεμβάσεων σε πολυάριθμα στοιχεία του δικτύου. Αυτό είναι αναμενόμενο καθώς τα δομικά στοιχεία του δικτύου είναι αυξημένα αριθμητικά στα άκρα του, άρα και στα κατώτερα επίπεδά του, σε σχέση με τα κεντρικά - ανώτερα επίπεδα του δικτύου.

Όπως διαπιστώνεται και από τα αποτελέσματα της προσομοίωσης, η επίδοση της ασφαλούς αρχιτεκτονικής έχει σημαντικά μειωθεί σε σύγκριση με τη μη ασφαλή, ίδια, αρχιτεκτονική. Το φαινόμενο αυτό μπορεί να αντιμετωπιστεί με τις κατάλληλες ρυθμίσεις των πολιτικών του δικτύου και της εφαρμοζόμενης ασφάλειάς του.

Μέσω της εφαρμοζόμενης πολιτικής του δικτύου θα πρέπει να διανέμονται αποδοτικά επιπρόσθετοι πόροι στους κόμβους που παρουσιάζουν χαμηλή επίδοση, συγκεκριμένα στους B-SEN και B-SSCP.

Επιπλέον, μέσω της εφαρμοζόμενης πολιτικής του δικτύου θα πρέπει να γίνεται επιλογή του κατάλληλου τύπου και του αριθμού των υπηρεσιών που θα εξυπηρετηθούν από κόμβους που παρουσιάζουν αδυναμία βέλτιστης επίδοσης, δηλαδή του B-SSCP. Οι εφαρμογές που θα εξυπηρετούνται από τον

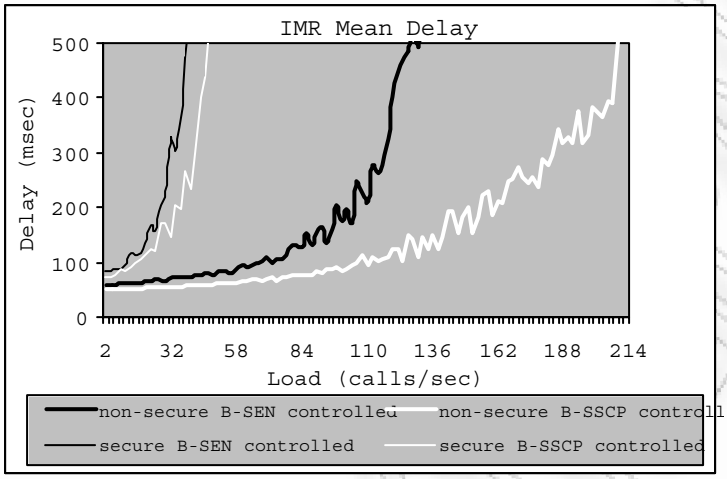
κόμβο B-SSCP θα πρέπει να είναι όσο το δυνατόν λιγότερες και η επιβάρυνση που θα επιφέρουν στον κόμβο και το δίκτυο να είναι η ελάχιστη δυνατή. Για παράδειγμα, θα μπορούσε να οριστεί ένας υψηλότερος αριθμός κλήσεων για υπηρεσία ΕΔ που θα εξυπηρετηθούν από τις οντότητες B-SCF/B-SDF, που είναι εγκατεστημένες στον B-SEN, και οι οποίες κλήσεις θα στέλνουν τις αιτήσεις για εξυπηρέτηση στον κόμβο B-SSCP.

Η κατάλληλη παραμετροποίηση της πολιτικής ασφάλειας μπορεί, επίσης, να οδηγήσει σε καλύτερη επίδοση του δικτύου. Σε συνθήκες επικοινωνίας αυξημένου φόρτου (μετάδοση video) όπως επίσης και σε κορεσμένους κόμβους (B-SSCP) μπορεί να εφαρμοστεί κρυπτογράφηση χαμηλότερου επιπέδου. Για παράδειγμα μπορεί να εφαρμοτεί η χρήση μικρότερου κλειδιού κρυπτογράφησης (π.χ. 40 bit κλειδί συμμετρικής κρυπτογράφησης και 512 bit κλειδί ασύμετρης κρυπτογράφησης), που ελαχιστοποιεί την καθυστέρηση που οφείλεται στα κανάλια ασφάλειας.

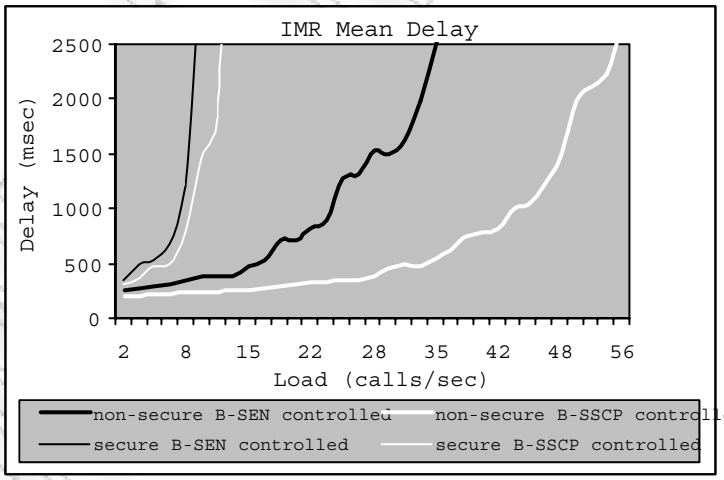
Ένα παράδειγμα παραμετροποίησης σε σχέση με το μέγεθος των πακέτων παρουσιάζεται στις εικόνες 5.9 και 5.10. Η μέση καθυστέρηση της IMR έχει υπολογιστεί για τις περιπτώσεις μεγέθους πακέτων ίσων με 10000 και 40000 bit. Είναι προφανές ότι παρόλο που η καθυστέρηση αυξάνεται αναλογικά με το μέγεθος του πακέτου, εξακολουθεί να παραμένει σε αποδεκτά, χαμηλά επίπεδα.

5.3 Σύγκριση Αποτελεσμάτων

Γενικά, φαίνεται να ισχύει ότι τα αποτελέσματα της μελέτης επίδοσης ενός δικτύου παρουσιάζουν διαφορές κάτω από διαφορετικές συνθήκες (π.χ. διαφορετικά σενάρια κίνησης στα κινητά δίκτυα). Η επιλογή κάποιου από αυτά, σε αντίθεση με άλλα, μπορεί να επηρεάσει τα αποτελέσματα της μελέτης. Για το λόγο αυτό έγινε προσπάθεια το ανωτέρω σενάριο να μοντελοποιηθεί χρησιμοποιώντας και κάποιο από τα γνωστά εργαλεία. Συγκεκριμένα χρησι-

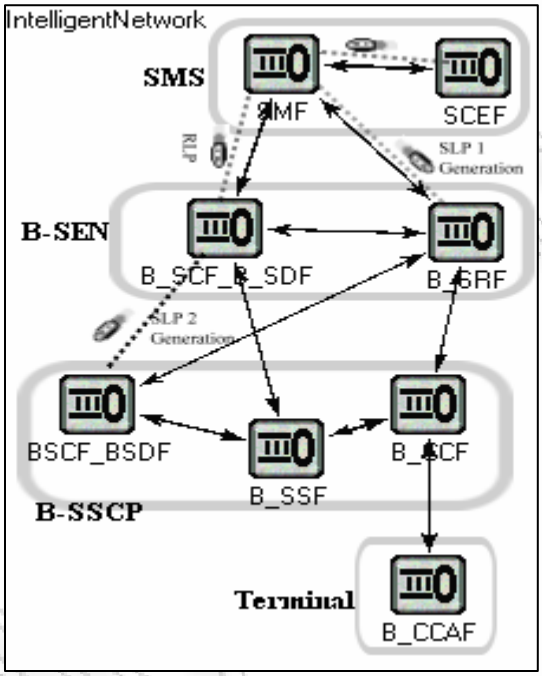


Εικόνα 5.9: *Μέση καθυστέρηση IMR με μέγεθος πακέτου 10000 bit.*



Εικόνα 5.10: *Μέση καθυστέρηση IMR με μέγεθος πακέτου 40000 bit.*

SMS: Service management system
SMF: Service Management Function
SCEF: Service Creation Environment Function
(B-)SEN: (Broadband) Service Execution Node
(B-)SRF: (Broadband) Specialized Resource Function
(B-)SCF: (Broadband) Service Control Function
(B-)SDF: (Broadband) Service Data Function
(B-)CCAF: (Broadband) Call Control Agent Function
RLP: Resource Logic Program
SLP: Service Logic Program
B-SSCP: (Broadband) Service Switching and Control Point
(B-)CCF: (Broadband) Call Control Function
(B-)SSF: (Broadband) Service Switching Function

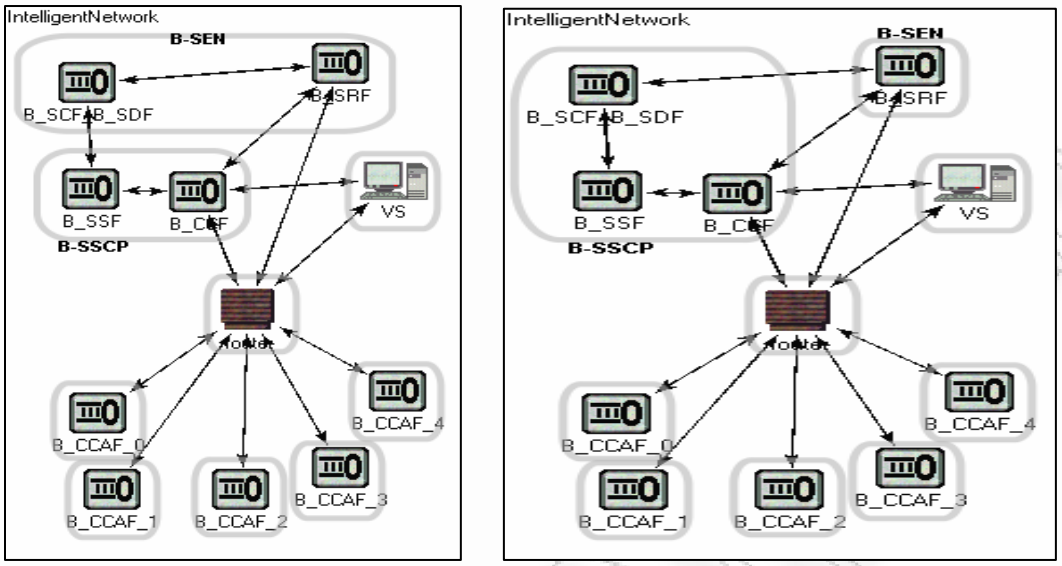


Εικόνα 5.11: *Κατανομή Λειτουργικών οντοτήτων σε Φυσικούς κόμβους στο Ευφυές Δίκτυο.*

μοποιήθηκε το OMNET++ [1]. Παρακάτω παρουσιάζονται τα αποτελέσματα αυτής της έρευνας, η οποία ακολουθεί το μοντέλο που έχει ήδη περιγραφεί στην παράγραφο 5.1.2. Τα αποτελέσματα σε αυτή την ενότητα δεν παρουσιάζουν διαφορές σε σχέση με τα αποτελέσματα της προηγούμενης παραγράφου. Εντούτοις κρίθηκε σκόπιμη η παρουσίασή τους καθώς πρόκειται για αποτελέσματα προσομοίωσης με τη χρήση ενός διαφορετικού εργαλείου.

Η εικόνα 5.11 παρουσιάζει την αντιστοιχία των λειτουργικών οντοτήτων (FE) στους φυσικούς κόμβους, παράγωντας, έτσι, ένα κατανεμημένο ευφυές δίκτυο. Βασιζόμενοι στο δίκτυο της εικόνας 5.12 δημιουργούνται τα δύο διαφορετικά σενάρια εκτέλεσης της λογικής της υπηρεσίας. Στο πρώτο (α αριστερά) ο έλεγχος της υπηρεσίας εκτελείται στο φυσικό κόμβο B-SEN, ενώ στο δεύτερο (β- δεξιά) εκτελείται στον φυσικό κόμβο B-SSCP.

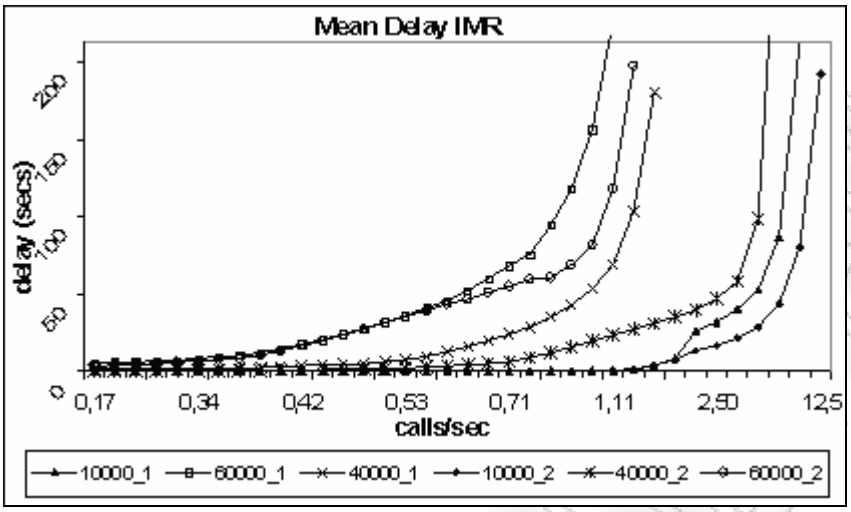
Η εικόνα 5.13 παρουσιάζει τη μέση καθυστέρηση ολοκλήρωσης της υπη-



Εικόνα 5.12: *Διαφορετικά σενάρια-θέσεις εκτέλεσης της λογικής της υπηρεσίας (SLP) (α- αρι.) Σενάριο 1: Ο Έλεγχος της Υπηρεσίας στον κόμβο B-SEN. (β-δεξιά) Σενάριο 2: Ο Έλεγχος της Υπηρεσίας στον κόμβο B-SSCP*

ρεσίας IMR, όταν δεν έχουν εφαρμοστεί μηχανισμοί ασφάλειας για διάφορα μεγέθη πακέτων μηνυμάτων. Όπως φαίνεται και από την εικόνα η εκτέλεση του ελέγχου της υπηρεσίας στο φυσικό κόμβο B-SSCP έχει ως αποτέλεσμα την εξυπηρέτηση περισσοτέρων κλήσεων μέχρι να εκδηλωθούν μεγάλοι χρόνοι καθυστέρησης. Όπως είναι φυσικό τα πακέτα με το μικρότερο μέγεθος παρουσιάζουν μικρότερες καθυστερήσεις. Αν δούμε την εικόνα 5.12 σε σχέση με την εικόνα 5.3 θα παρατηρείται ότι έχουν αλλάξει οι χρόνοι εκδήλωσης της συμπεριφοράς της γραφικής παράστασης, αλλά όχι και η γενικότερη τάση της. Και στις δύο περιπτώσεις το σενάριο β παρουσιάζει τους μικρότερους χρόνους καθυστέρησης.

Στις εικόνες 5.14 και 5.15 παρουσιάζονται οι καθυστερήσεις που εκδηλώνουν οι λειτουργικές οντότητες στο δίκτυο, όταν το μέσο μέγεθος του πακέτου είναι 40000 bit και στα δύο σενάρια και ο ρυθμός παραγωγής δεδομένων βρίσκεται στα 4 Mbps. Συγκρίνοντας τις καθυστερήσεις που εμφανίζονται στις δυο εικόνες φαίνεται ότι οι οντότητες B-SSF, B-SCF και B-CCF παρουσιάζουν

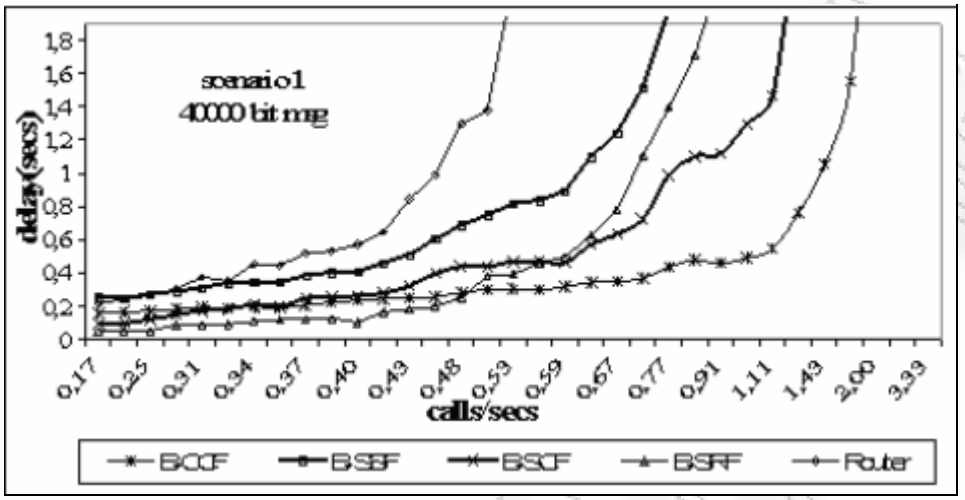


Εικόνα 5.13: *Μέση καθυστέρηση IMR.*

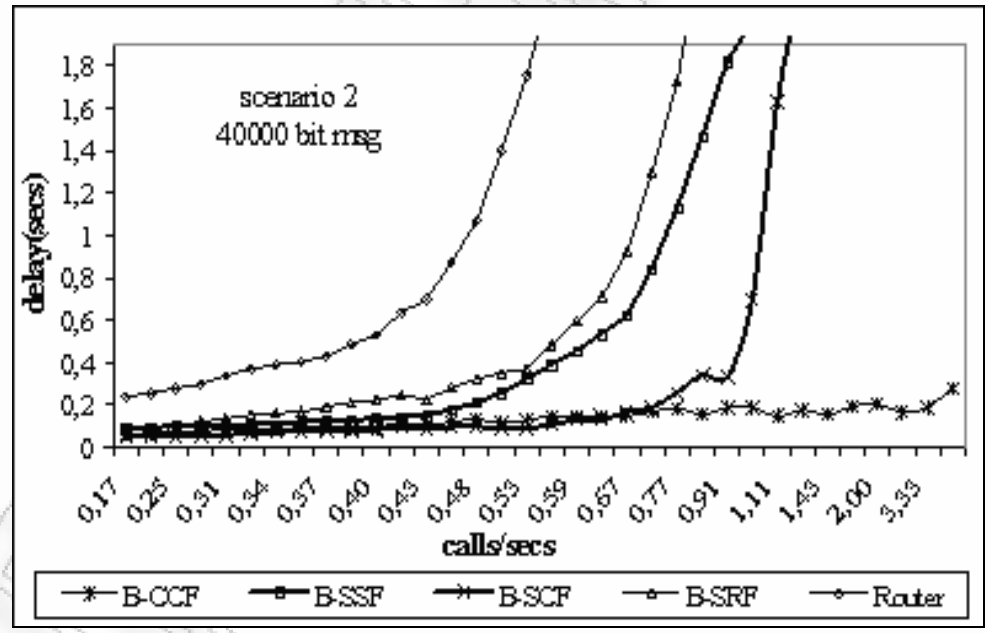
βελτίωση στη λειτουργία τους στο σενάριο β. Είναι εμφανές ότι η οντότητα B-SSF φέρει το μεγαλύτερο φόρτο επικοινωνίας (σενάριο α) ανάμεσα στους δύο φυσικούς κόμβους (B-SSCP και B-SEN). Η ανταλλαγή μηνυμάτων μεταξύ των οντοτήτων B-SSF και των B-SCF και B-CCF, είναι συνεχής. Οπότε η μετακίνηση της οντότητας B-SCF πλησιέστερα στην οντότητα B-SSF βελτιώνει την επίδοση του δικτύου (σενάριο β).

Στις εικόνες 5.16 και 5.17 παρουσιάζονται οι καθυστερήσεις που υφίστανται οι κόμβοι B-SSCP και B-SEN. Αρχικά, για το σενάριο α, ο κόμβος B-SEN παρουσιάζει μεγαλύτερες καθυστερήσεις σε σχέση με την επίδοσή του στο σενάριο β. Στο σενάριο α ο κόμβος αυτός καλείται να εξυπηρετήσει όλες τις κλήσεις για υπηρεσίες ευφυούς δικτύου, ενώ στο σενάριο β οι περισσότερες κλήσεις θα απαντηθούν από τον κόμβο B-SSCP, του οποίου και η επίδοση επιβαρύνεται (εικόνα 5.16).

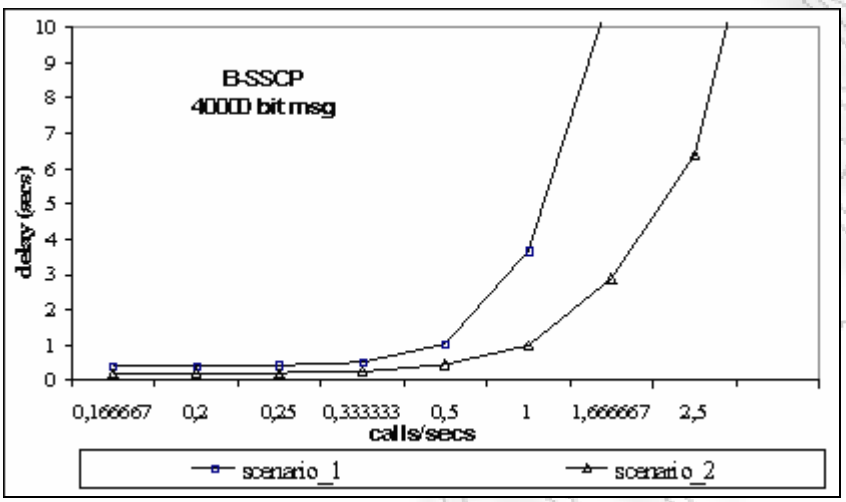
Εάν στο ανωτέρω δίκτυο εισαχθούν και κλήσεις για απλή τηλεφωνία (με αναλογία 3 προς 1), τότε, όπως φαίνεται και στην εικόνα 5.18, η μέση καθυστέρηση ολοκλήρωσης των υπηρεσιών ευφυούς δικτύου (IMR) έχει μειωθεί σημαντικά και το δίκτυο λειτουργεί καλύτερα στο σενάριο β. Το μέσο μέγεθος



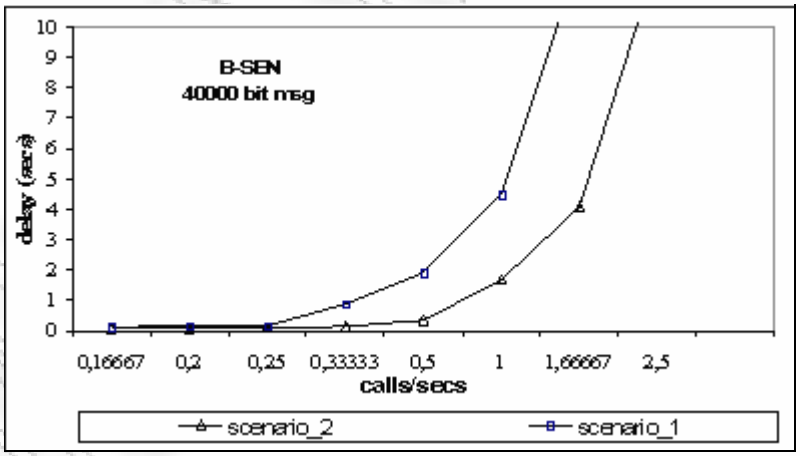
Εικόνα 5.14: *Μέση καθυστέρηση σε κάθε φυσικό κόμβο με μέσο μέγεθος πακέτου στα 40000 bit για το σενάριο α.*



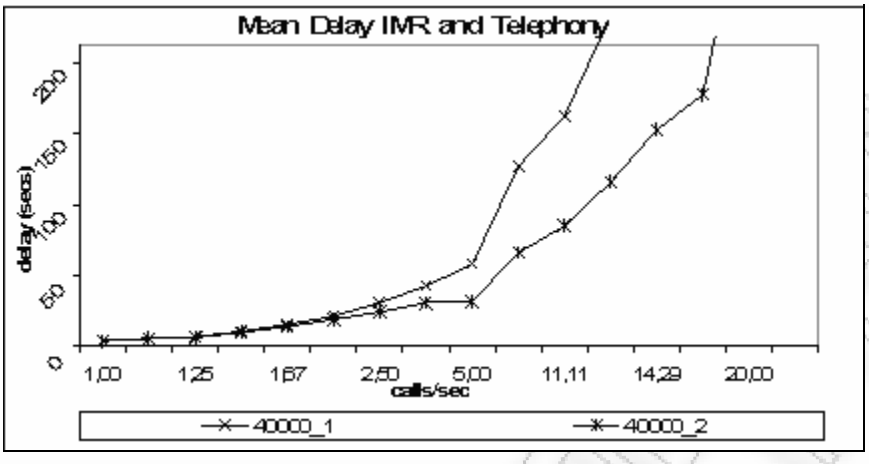
Εικόνα 5.15: *Μέση καθυστέρηση σε κάθε φυσικό κόμβο με μέσο μέγεθος πακέτου στα 40000 bit για το σενάριο β.*



Εικόνα 5.16: *Μέση καθυστέρηση στο φυσικό κόμβο B-SSCP με μέσο μέγεθος πακέτου 40000 bit και για τα δύο σενάρια.*



Εικόνα 5.17: *Μέση καθυστέρηση στο φυσικό κόμβο B-SEN με μέσο μέγεθος πακέτου 40000 bit και για τα δύο σενάρια.*

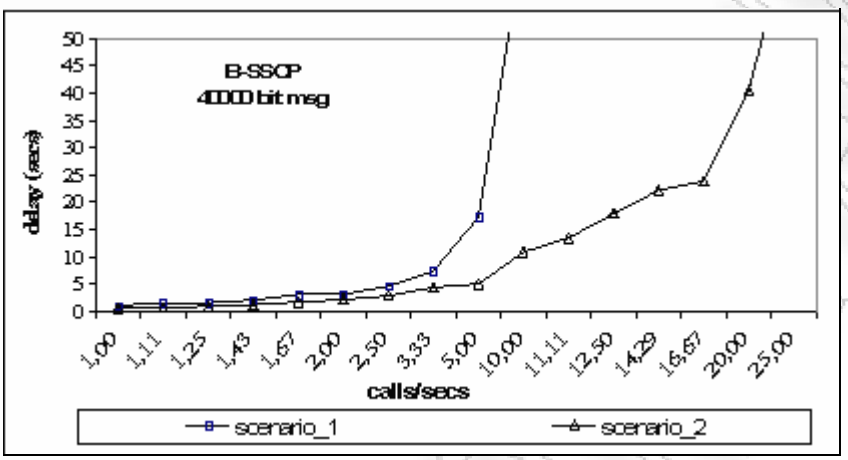


Εικόνα 5.18: *Μέση καθυστέρηση της όλης υπηρεσάις IMR με μέσο μέγεθος πακέτου 40000 bit και για τα δύο σενάρια και ύπαρξη τηλεφωνικών κλήσεων.*

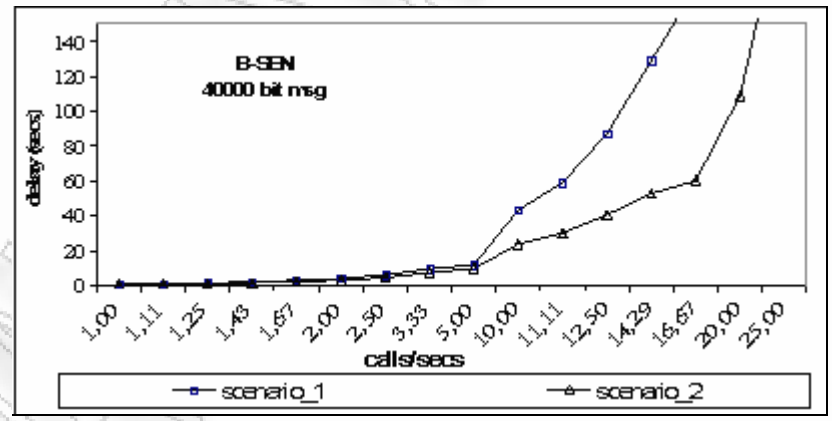
των πακέτων που έχει χρησιμοποιηθεί εδώ είναι 40000 bit, και οι χρόνοι εκπομπής δύο πακέτων/κλήσεων IMR αυξάνονται εκθετικά, ενώ οι τηλεφωνικές κλήσεις δημιουργούνται με μέσο το 1, το οποίο παριστά μια μέση κίνηση στο δίκτυο. Όπως φαίνεται από την εικόνα 5.18, το δίκτυο μπορεί να εξυπηρετήσει μηνύματα με μεγαλύτερη ταχύτητα, χωρίς πολλές καθυστερήσεις, σε αντίθεση με την περίπτωση όπου υπάρχει μόνο κλήση IMR (εικόνα 5.13).

Και οι δυο κόμβοι B-SSCP και B-SEN (εικόνες 5.19 και 5.20) λειτουργούν καλύτερα στο σενάριο β, ακόμα και κάτω από βαρύ φορτίο τηλεφωνικής κίνησης. Η μετακίνηση της λογικής της υπηρεσίας πλησιέστερα στον κόμβο B-SSCP προκαλεί την βελτίωση της επίδοσης του δικτύου. Καθώς η επίδοση του κόμβου στον οποίο βρίσκεται η λογική της υπηρεσίας, επιβαρύνεται, τότε θα πρέπει να αποδοθούν στον κόβμο επιπλέον πόροι του συστήματος. Αυτό αποτελεί, ίσως, πρόβλημα καθώς η μετανάστευση των πρακτόρων δεύτερης γενιάς, πλησιέστερα στο χρήστη, απαιτεί την απόδοση επιπλέον συστημικών πόρων σε πολυάριθμα στοιχεία του δικτύου, αφού οι χρήστες βρίσκονται στα χαμηλότερα επίπεδα του δικτύου, αρά και στα πολυπληθέστερα.

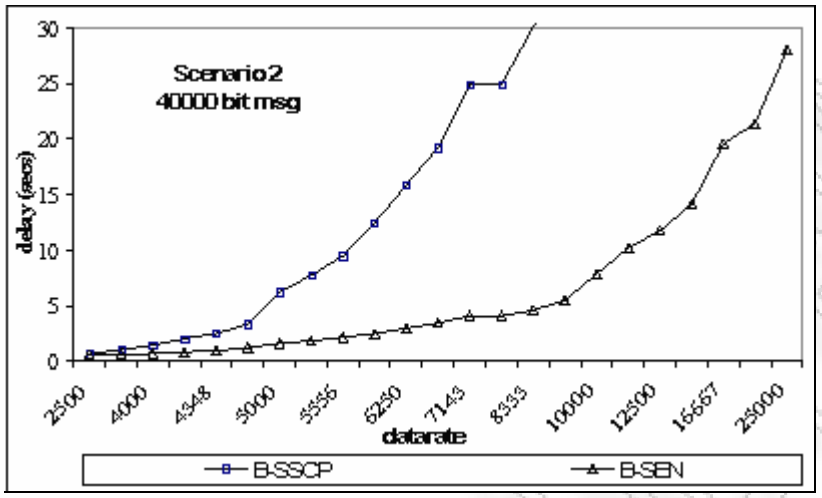
Η εικόνα 5.21 παρουσιάζει την επίδοση των κόμβων B-SSCP και B-SEN



Εικόνα 5.19: *Μέση καθυστέρηση στο φυσικό κόμβο B-SSCP με μέσο μέγεθος πακέτου 40000 bit και για τα δύο σενάρια και ύπαρξη τηλεφωνικών κλήσεων.*



Εικόνα 5.20: *Μέση καθυστέρηση στο φυσικό κόμβο B-SEN με μέσο μέγεθος πακέτου 40000 bit και για τα δύο σενάρια και ύπαρξη τηλεφωνικών κλήσεων.*



Εικόνα 5.21: *Μέση καθυστέρηση στους φυσικούς κόμβους B-SEN και B-SSCP με μέσο μέγεθος πακέτου 40000 bit, για το σενάριο β, σε σχέση με το ρυθμός μετάδοσης δεδομένων.*

σε σχέση με διαφορετικούς ρυθμούς παραγωγής δεδομένων. Στη μελέτη μας η επίδοση και των δύο κόμβων παραμένει σε ανεκτά επίπεδα όσον αφορά τις καθυστερήσεις που εκδηλώνουν, όταν ο ρυθμός παραγωγής είναι 2 MB ή μεγαλύτερος.

Βιβλιογραφία

[1] Mavropodi R., Douligeris C., *Intelligent Networks - Security Issues and Performance Evaluation*, Annual Review of Communications, Volume 57, 2004.

[2] Kotzanikolaou P., Mavropodi R., Douligeris C, Chrissikopoulos V, *Secure distributed intelligent networks*, Computer Communications, Vol 29, no 3, 325-336, 2006.

[3] Venieris I. Hussmann H., *Intelligent Broadband Networks*, John Wiley & Sons, West Sussex England (1998).

[4] Mavropodi R., Douligeris C., *Performance Evaluation of Intelligent Network Topologies*, SCI 2003, Orlando, USA, July 27-30, 2003.

[5] Mavropodi R. and C. Douligeris, *Performance Evaluation of Interactive Multimedia Retrieval in Intelligent Networks*, ComCon 8,25-29, June 2001, Crete, Greece, 443 - 453.

[6] Mavropodi R., P. Kotzanikolaou and C. Douligeris, *Secure Management of Intelligent Networks through Intelligent Agents*, Workshop on Intelligent Agents and Virtual Reality, Athens, June 29, 2001, pp. 57-64.

[7] Douligeris C., R. Mavropodi and P. Kotzanikolaou, *Agent - Based Security in Intelligent Multimedia Retrieval in Intelligent Networks*, INFORMS Miami Annual Meeting, Miami Beach, FL, Nov. 2001.

[8] Kotzanikolaou P., Douligeris C., Mavropodi R. and Chrissikopoulos V., *Mobile Agent Security*, Invited chapter, Network Security: Current Status and Future Directions, IEEE Press, (to appear) 2005.

Κεφάλαιο 6

Το Ασφαλές Πρωτόκολλο Δρομολόγησης SecMR

Η χρήση πολλαπλών μονοπατιών στα δίκτυα αυξάνει την ανθεκτικότητα ενάντια σε επιθέσεις συνεργαζόμενων κακόβουλων κόμβων καθώς μεγιστοποιεί τον αριθμό των κόμβων τους οποίους θα πρέπει να προσβάλει ένας εχθρός προκειμένου να αποκτήσει τον έλεγχο της επικοινωνίας. Σε αυτό το κεφάλαιο μελετούμε μερικά είδη επιθέσεων τα οποία καθιστούν τα πρωτόκολλα δρομολόγησης πολλαπλών μονοπατιών ευάλωτα σε συνεργαζόμενους κακόβουλους κόμβους. Προτείνεται ένα κατ' αίτηση πρωτόκολλο δρομολόγησης πολλαπλών μονοπατιών, το Secure Multipath Routing protocol (SecMR), και αναλύεται η ασφάλειά του. Συγκεκριμένα, αρχικά παρουσιάζονται οι αδυναμίες ασφάλειας των πρωτοκόλλων δρομολόγησης και στη συνέχεια παρουσιάζεται και αναλύεται το πρωτόκολλο SecMR. Τέλος πραγματοποιείται ανάλυση των χαρακτηριστικών ασφάλειας που επιδεικνύει το προτεινόμενο πρωτόκολλο.

6.1 Εισαγωγή

Στα κινητά δίκτυα, η δρομολόγηση είναι μια πρόκληση εξαιτίας της ίδιας της φύσης του δικτύου (mobility) καθώς επίσης και της εγγενούς δυναμικότητας της τοπολογίας. Επιπλέον, οι κόμβοι ενός τέτοιου δικτύου είναι συνήθως συσκευές περιορισμένων δυνατοτήτων όσον αφορά τους ενεργειακούς πόρους, την υπολογιστική τους ισχύ, και το εύρος της επικοινωνίας τους.

Όπως παρουσιάστηκε και στην παράγραφο 2.2.2 τα πρωτόκολλα δρομολόγησης τέτοιων δικτύων μπορούν κατά κανόνα να ταξινομηθούν σε διάφορες κατηγορίες: στα πρωτόκολλα με πίνακα (table driven - proactive) (*π.χ* ZRP [6]) και στα πρωτόκολλα αρχικοποίησης πηγής (source initiated) (*π.χ.* DSR [9]) είτε όπως λέγονται διαφορετικά κατ' αίτηση (on-demand). Υπάρχουν πρωτόκολλα μονής φάσης ή διπλής (ανάλογα αν περιλαμβάνουν δεδομένα κατά τη διαδικασία δρομολόγησης ή όχι), πρωτόκολλα πολλαπλών μονοπατιών (αν ανακαλύπτονται πολλαπλά μονοπάτια ή όχι), πρωτόκολλα διακριτών κόμβων ή διακριτών ζεύξεων κ.α. Η πληθώρα του είδους των πρωτοκόλλων που υπάρχουν δικαιολογείται από την ιδιομορφία που παρουσιάζει ο χώρος των ασύρματων κινητών δικτύων. Κάθε δίκτυο Ad Hoc παρουσιάζει τα δικά του χαρακτηριστικά γνωρίσματα και για το λόγο αυτό δεν μπορεί να εφαρμοστεί ένα πρωτόκολλο δρομολόγησης για όλες τις περιπτώσεις δικτύων. Τα γνωρίσματα που κάνουν κάθε δίκτυο Ad Hoc ιδιόμορφο προσδιορίζονται όχι μόνο στην κινητικότητα, την ακτίνα κάλυψης ή το διαφορετικό είδος εφαρμογών που καλείται να εξυπηρετήσει το δίκτυο (πολυμεσικά δεδομένα, στρατιωτικές εφαρμογές, εφαρμογές έκτακτης ανάγκης κ.α.) αλλά και στις ιδιότητες ασφάλειας που πρέπει να εξασφαλίζει.

Η διαδικασία ανεύρεσης δρομολογίων στα πρωτόκολλα δρομολόγησης πολλαπλών μονοπατιών παρουσιάζει πολλές αδυναμίες ασφάλειας επιτρέποντας έτσι είτε σε ένα μικρό σύνολο, είτε σε έναν και μόνο κακόβουλο κόμβο να ελέγξει το μονοπάτι επικοινωνίας ανάμεσα σε επιλεγμένους κόμβους. Τις κυ-

ριότερες από αυτές τις αδυναμίες αποτελούν το *φαινόμενο του ανταγωνισμού* [17, 16, 13], η *πλαστοπροσωπία* και η *έλλειψη πιστοποίησης* [5], η ύπαρξη επιθέσεων *Ενδιάμεσου κόμβου* Man-In-the-Middle attack [1] και επιθέσεις *αθέατου κόμβου* (invisible node) [14].

Μέχρι τώρα έχουν προταθεί αρκετές λύσεις για την ασφάλεια την δρομολόγησης δεδομένων. Μια λύση αποτελεί η παρακολούθηση της συμπεριφοράς δρομολόγησης που επιδεικνύει ο κάθε κόμβος (collaborative monitoring) [15], [22]. Σε αυτή τη λύση οι κόμβοι του δικτύου συνεργάζονται ώστε να καταγράφουν τη συμπεριφορά των γειτονικών τους κόμβων. Μια άλλη λύση αποτελεί και η προτροπή για σωστή συμπεριφορά με τη χρήση εικονικών νομισμάτων [4]. Σε αυτή τη λύση το δίκτυο παρέχει κίνητρα (εικονικά νομίσματα [4]) στους κόμβους του ώστε να συμπεριφέρονται νόμιμα (καλόβουλα). Τέλος υπάρχει η λύση κατά την οποία μπορούν οι κόμβοι να συμμετέχουν στα μονοπάτια δρομολόγησης αν και εφόσον πληρούν κάποια μετρήσιμα κριτήρια [23]. Σε αυτή τη λύση η αξιοπιστία ενός κόμβου αξιολογείται συλλέγοντας ενδείξεις (ποσοτικά χαρακτηριστικά) κατά τη διάρκεια της λειτουργίας-συμπεριφοράς του μέσα στο δίκτυο. Παρά την πρακτική τους εφαρμογή, όλες οι παραπάνω λύσεις είναι επιρρεπείς σε επιθέσεις άρνησης υπηρεσίας (Denial-of-Service (DoS)) καθώς έχουν σχεδιαστεί για πρωτόκολλα δρομολόγησης μοναδικών μονοπατιών. Πράγματι σε πρωτόκολλα τέτοιου είδους μια επίθεση άρνησης υπηρεσίας είναι συχνό φαινόμενο ακόμα και αν έχουν ληφθεί ειδικά μέτρα ασφάλειας. Ένας κακόβουλος κόμβος μπορεί να συμμετέχει παθητικά στη διαδικασία δρομολόγησης μεταξύ δύο τερματικών κόμβων ως νόμιμος ενδιάμεσος κόμβος. Στη συνέχεια αυτός ο κακόβουλος κόμβος μπορεί να αποδιοργανώσει ή ακόμα και ένα διακόψει εντελώς την επικοινωνία οποιαδήποτε στιγμή θεωρήσει ότι είναι πλεονεκτική για αυτόν. Ακόμα και στην περίπτωση που μια επικοινωνία είναι κρυπτογραφημένη, ένας κακόβουλος χρήστης μπορεί να βρει την κατάλληλη στιγμή για επίθεση εκμε-

ταλλευόμενος συγκεκριμένα χαρακτηριστικά του δικτύου, όπως τη συμφόρηση των πακέτων. Παρόλο που οι τερματικοί κόμβοι μπορούν να χρησιμοποιήσουν ένα νέο μονοπάτι για την επικοινωνία μετά την επίθεση, η καθυστέρηση που επέρχεται από την αναζήτηση αυτού του νέου μονοπατιού μπορεί να είναι κρίσιμη. Αυτήν ακριβώς την κρίσιμη καθυστέρηση μπορεί να εντοπίσει ένας επιδέξιος κακόβουλος χρήστης και να βρει ποια θα είναι η καταλληλότερη στιγμή για να επιτεθεί. Αυτό μπορεί να το πετύχει καταλαμβάνοντας συγκεκριμένους ζωτικούς κόμβους ενός μονοπατιού προκαλώντας τη μέγιστη δυνατή ζημιά στο δίκτυο.

Τα πρωτόκολλα δρομολόγησης πολλαπλών μονοπατιών είναι ανθεκτικά σε επιθέσεις άρνησης υπηρεσίας και μπορούν να προστατέψουν τη διαθεσιμότητα ενός δικτύου από κακόβουλους κόμβους [2]. Πράγματι εάν για την επικοινωνία ανάμεσα σε μια πηγή και έναν προορισμό χρησιμοποιούνται k μονοπάτια διακριτών/ μοναδικών κόμβων, ένας κακόβουλος κόμβος θα πρέπει να έχει στην κατοχή του τουλάχιστον k (κόμβους). Συγκεκριμένα πρέπει να κατέχει έναν κόμβο σε κάθε μονοπάτι, ώστε να ελέγχει την επικοινωνία. Ένα ασφαλές πρωτόκολλο πολλαπλών μονοπατιών θα πρέπει να χρησιμοποιεί k μονοπάτια μοναδικών/ διακριτών κόμβων. Σε αντίθετη περίπτωση, ένας κακόβουλος κόμβος μπορεί να διαβάλλει το πρωτόκολλο δρομολόγησης και με αυτό τον τρόπο να ελέγχει όλα τα πιθανά μονοπάτια ανάμεσα στην πηγή και τον προορισμό. Προφανώς, με τη χρήση μονοπατιών μοναδικών/ διακριτών κόμβων για την επικοινωνία, η ακεραιότητα και η διαθεσιμότητα της επικοινωνίας διασφαλίζεται από το γεγονός ότι το πρωτόκολλο δρομολόγησης γίνεται ανθεκτικό στις επιθέσεις άρνησης υπηρεσίας DoS από έναν εχθρό ο οποίος ελέγχει λιγότερους από k κακόβουλους κόμβους.

Παρακάτω θα δούμε τρία πρωτόκολλα αυτού του είδους. Συγκεκριμένα τα SRP[17] και το [3] και θα παρουσιαστεί αναλυτικά το Secure Multipath Routing (SecMR)[1].

Το SRP [17] είναι ένα πρωτόκολλο δρομολόγησης πολλαπλών μονοπατιών το οποίο στοχεύει στην προστασία από τέτοιου είδους επιθέσεις ασφάλειας. Το SRP χρησιμοποιεί συμμετρική κρυπτογράφηση από άκρο σε άκρο με σκοπό την προστασία της ακεραιότητας της διαδικασίας ανακάλυψης δρομολογίων. Έτσι λειτουργεί ικανοποιητικά προστατεύοντας από πολλές επιθέσεις κακόβουλων κόμβων. Εντούτοις η διαδικασία ανεύρεσης νέων μονοπατιών είναι εγγενώς αδύναμη στο φαινόμενο του ανταγωνισμού (racing) το οποίο μπορεί να αποτρέψει την ανακάλυψη υπαρχόντων μονοπατιών μοναδικών/ και διακριτών κόμβων. Επιπλέον, οι ενδιάμεσοι κόμβοι δεν πιστοποιούνται κάνοντας το πρωτόκολλο ευαίσθητο σε επιθέσεις *πλαστοπροσωπίας* και *πολλαπλών ταυτοτήτων* (sybil attacks) [5]. Έτσι ένας κακόβουλος κόμβος μπορεί να συμμετέχει με περισσότερες από μια πλαστές ταυτότητες σε πολλαπλά μονοπάτια διαβάλλοντας την επικοινωνία με τη χρήση πολλαπλών μονοπατιών.

Στο [3] παρουσιάζεται ένα πρωτόκολλο δρομολόγησης πολλαπλών μονοπατιών που βασίζεται στον αλγόριθμο Ford-Fulkerson MaxFlow. Αυτό το πρωτόκολλο ικανοποιεί τις απαιτήσεις ασφάλειας των πρωτοκόλλων πολλαπλών μονοπατιών. Επιπλέον, μπορεί να χαρακτηρισθεί σαν *ολοκληρωμένο* καθώς ανακαλύπτει όλα τα υπάρχοντα μονοπάτια περιορίζοντας το σύνολο αυτών χρησιμοποιώντας το πεδίο 'μέγιστος χρόνος ζωής'. Εν τούτοις η προώθηση της αίτησης ανεύρεσης νέων μονοπατιών είναι ασύμφορη τόσο σε υπολογιστικό χρόνο όσο και σε αποθηκευτικό χώρο. Κατά τη διάρκεια της διαδικασίας προώθησης της αίτησης αναίρεσης νέων μονοπατιών κάθε κόμβος που λαμβάνει την αίτηση επισυνάπτει πληροφορίες για τους γειτονικούς του κόμβους μαζί με μια υπογραφή και επανεκπέμπει το μήνυμα. Αυτό αυξάνει αισθητά το μέγεθος του μηνύματος. Επιπλέον, η χρήση ψηφιακών υπογραφών από τους ενδιάμεσους κόμβους κοστίζει τόσο σε υπολογιστική ισχύ όσο και σε καθυστέρηση. Γιά λόγους απλότητας στη συνέχεια το πρωτόκολλο [3] καλείται Multipath.

Σε αυτό το κεφάλαιο παρουσιάζεται ένα ολοκληρωμένο κατ-αίτηση πρωτόκολλο δρομολόγησης πολλαπλών μονοπατιών το Secure Multipath Routing (SecMR), το οποίο παρέχει προστασία για τις επιθέσεις άρνησης υπηρεσίας ενός ορισμένου αριθμού συνεργαζόμενων κακόβουλων κόμβων.

6.2 Περιγραφή του πρωτοκόλλου SecMR

Παρακάτω παρουσιάζεται το πρωτόκολλο SecMR [1] το οποίο ανήκει στην κατηγορία των κατ' αίτηση πρωτοκόλλων δρομολόγησης πολλαπλών μονοπατιών και το οποίο είναι ασφαλές για ένα ορισμένο αριθμό συνεργαζόμενων κακόβουλων χρηστών. Το SecMR ανακαλύπτει όλα τα υπάρχοντα μη κυκλικά, μοναδικών κόμβων μονοπάτια ανάμεσα σε έναν κόμβο-πηγή και σε έναν κόμβο-προορισμού. Το πρωτόκολλο λειτουργεί σε δύο φάσεις. Η πρώτη φάση, που ονομάζεται *πιστοποίηση γειτονικών κόμβων*, περιλαμβάνει την ασύγχρονη και αμοιβαία πιστοποίηση των κόμβων που είναι γείτονες μεταξύ τους. Η δεύτερη φάση, που ονομάζεται *εύρεση μονοπατιών και διατήρηση*, περιλαμβάνει την ανακάλυψη και διατήρηση των δρομολογίων/μονοπατιών μεταφοράς δεδομένων.

6.2.1 Πρώτη φάση - πιστοποίηση γειτονικών κόμβων

Έστω ότι n_i ένας κόμβος στο ασύρματο κινητό δικτύων. Υποθέτουμε ότι κάθε κόμβος n_i κατέχει ένα ζεύγος δημοσίου- μυστικού κλειδιού, (PK_i, SK_i) αντίστοιχα ενός Elliptic Curve Cryptosystem [11]. Επιπλέον, το δημόσιο κλειδί κάθε κόμβου n_i είναι εγγυημένο από ένα πιστοποιητικό $cert_i$, που έχει εκδοθεί από μια αρχη πιστοποίησης (Certifying Authority *CA*).

Επειδή η χρήση της αρχής πιστοποίησης και του δημόσιου κλειδιού PKI σε ένα ασύρματο κινητό περιβάλλον αποτελεί πρόκληση με πολλά αδύνατα σημεία, έχουν προταθεί πολλές προσεγγίσεις [24],[8],[26]. Η κύρια ιδέα πί-

σω από αυτές τις προσεγγίσεις είναι η εφαρμογή ενός κατανεμημένου PKI χρησιμοποιώντας *k-out-of-n* ως κατώτατο όριο στην κρυπτογράφηση και/ή κατανεμημένη τοπική εμπιστοσύνη ανάμεσα σε ένα ζεύγος κόμβων. Η πιστοποίηση και κατανομή του δημοσίου κλειδιού δεν θα αποτελέσει αντικείμενο μελέτης της παρούσης διατριβής. Υποθέτουμε ότι οι κόμβοι είναι ικανοί να χρησιμοποιήσουν τις υπηρεσίες μιας (κατανεμημένης) αρχής πιστοποίησης *CA*, η οποία μπορεί να πραγματοποιηθεί με κάποια κατάλληλη τεχνική. Στο πιστοποιητικό $cert_i$ περιέχεται, επίσης, ένας μοναδικός αριθμός ID_i ο οποίος αντιπροσωπεύει την ταυτότητα του κάθε κόμβου n_i και ο οποίος διανέμεται από την αρχή πιστοποίησης *CA*. Ανάλογα με το μέγεθος του δικτύου, η μοναδική αυτή ταυτότητα μπορεί να είναι ένας σχετικά μικρός αριθμός, π.χ. 1 ή 2 byte. Αν το δίκτυο είναι μεγάλο σε μέγεθος, προσαρμόζεται ανάλογα και το μέγεθος της ταυτότητας. Ωστόσο, η χρήση ενός αριθμού μεγέθους 2 byte καλύπτει μια ευρείας γκάμας δίκτυα καθώς το πλήθος των κόμβων που μπορεί να περιγράψει ανέρχεται στο 65,535. Καθώς η χρήση ενός αριθμού μεγέθους 3 byte μπορεί να περιγράψει δίκτυα το πλήθος των οποίων ανέρχεται στους 16 εκατομμύρια κόμβους. Η χρήση μικρών αριθμών ως ταυτότητες κόμβων οδηγεί σε μηνύματα ελέγχου μικρού μεγέθους.

Σε περιοδικές χρονικές στιγμές, κάθε κόμβος n_i εκπέμπει στους άμεσους γειτονικούς του κόμβους ένα υπογεγραμμένο μήνυμα $(sig_i(t, ID_i), cert_i)$ στο οποίο περιέχεται η τρέχουσα χρονική στιγμή (t) και η μοναδική του ταυτότητα (ID_i), π.χ.

$n_i \overset{t}{\Rightarrow} (t, ID_i, sig_i(t, ID_i), cert_i)$,

όπου $X \overset{t}{\Rightarrow} m$ δηλώνει ότι ο κόμβος X εκπέμπει ένα μήνυμα m τη χρονική στιγμή t. Έτσι, κάθε κόμβος θα παράγει μια υπογραφή και θα επαληθεύσει μια υπογραφή από κάθε άμεσο γειτονικό του κόμβο. Το μέσο κόστος αυτής της φάσης ισούται με το κόστος παραγωγής μιας υπογραφής αυξημένο με το κόστος επεξεργασίας $\overline{C}$ υπογραφών ανά κόμβο, όπου $\overline{C}$ αποτελεί το

μέσο πλήθος των άμεσα γειτονικών του κόμβων. Η συχνότητα της φάσης πιστοποίησης των γειτονικών κόμβων αποτελεί παράμετρο του συστήματος και εξαρτάται από τη μεταβλητότητα του περιβάλλοντος του δικτύου. Η συχνότητα εφαρμογής αυτής της φάσης προσαρμόζεται ανάλογα με τη συχνότητα των αλλαγών στη διασύνδεση των κόμβων.

Μετά τη φάση της επαλήθευσης, κάθε κόμβος n_i θα δημιουργήσει μια λίστα με τους γείτονες του για τη χρονική στιγμή t, η οποία δηλώνεται ως N_i^t, όπου για τη μοναδική ταυτότητα του κόμβου ισχύει $ID_j \in N_i^t, 1 \leq j \neq i \leq L$ εάν για τη χρονική στιγμή t, ο κόμβος n_i έλαβε ένα μήνυμα πιστοποίησης από τον κόμβο n_j, το οποίο είχε μια έγκυρη υπογραφή του n_j στο t, ID_j. Για λόγους απλότητας στη συνέχεια δεν αναφέρεται ο χρονικός δείκτης, εκτός εάν αυτό είναι απαραίτητο για λόγους κατανόησης. Έτσι, θα ισχύει $N_i^t = N_i$. Σημειώνεται ότι οι κόμβοι δεν επανεκπέμπουν τα μηνύματα πιστοποίησης τα οποία έχουν λάβει από τους γείτονές τους. Εφόσον η πιστοποίηση λαμβάνει χώρα σε τοπικό επίπεδο και δεν πραγματοποιείται ταυτόχρονα από όλους τους κόμβους του δικτύου, το κόστος της διαδικασίας αυτής διατηρείται σε ανεκτά επίπεδα και δεν οδηγεί σε υπερφόρτωση του δικτύου.

6.2.2 Εύρεση μονοπατιών και διαχείριση

Η φάση της εύρεσης νέων μονοπατιών καθώς και η διαχείρισή τους πραγματοποιείται με την εφαρμογή τριών αλγορίθμων.

- Ο αλγόριθμος *εύρεσης νέων μονοπατιών* (route request query) χρησιμοποιείται στην ανακάλυψη νέων μονοπατιών διακριτών κόμβων ανάμεσα σε μια πηγή S και έναν τελικό προορισμό T.
- Ο αλγόριθμος *απάντησης* (route reply) χρησιμοποιείται για να προωθήσει τα μονοπάτια που θα χρησιμοποιηθούν για την επικοινωνία ανάμεσα σε έναν κόμβο-πηγή και τον προορισμό.

- Τέλος, ο αλγόριθμος *λάθους δρομολόγησης* (route error) χρησιμοποιείται όταν απαιτείται η διόρθωση των πινάκων δρομολόγησης που διαθέτει ο κάθε κόμβος, π.χ. σε περιπτώσεις μετανάστευσης κόμβων οι οποίοι μετέχουν στη δημιουργία του μονοπατιού επικοινωνίας.

Αλγόριθμος Εύρεσης Νέων Μονοπατιών

Όταν ένας κόμβος-πηγή S θέλει να επικοινωνήσει με έναν κόμβο προορισμού T, πρώτα ελέγχει τον πίνακα δρομολόγησής του μήπως έχει ήδη καταχωρημένο κάποιο μονοπάτι προς τον κόμβο T. Εάν δεν υπάρχει κάποιο ενεργό μονοπάτι τότε δημιουργεί ένα μήνυμα/ αίτηση για εύρεση νέου μονοπατιού. Το μήνυμα έχει την παρακάτω μορφή:

$Q_{S,T}=[ID_S, ID_T, seq, hop_{cnt}, hop_{max}, E_{PK_T}(K_{S,T}), RouteList, ExcludeList, NextHop, hash_{K_{S,T}}(ID_S, ID_T, seq, hop_{max})]$, όπου:

- ID_S, ID_T, είναι οι ταυτότητες των κόμβων S και T αντίστοιχα·
- seq, είναι ένας μετρητής που χρησιμοποιείται από τον κόμβο-πηγή S για κάθε νέο αίτημα εύρεσης μονοπατιών·
- hop_{cnt}, είναι ένας μετρητής που κρατά τον αριθμό των κομβων που έχει ήδη επισκευθεί το μήνυμα εύρεσης μονοπατιών·
- hop_{max}, ο μέγιστος αριθμός των κόμβων που μπορεί να επισκευθεί το μήνυμα εύρεσης μονοπατιών·
- $E_{PK_T}(K_{S,T})$, η κρυπτογράφηση του κλειδιού $K_{S,T}$ με το δημόσιο κλειδί PK_T του κόμβου T·
- $RouteList$, μια δυναμικά δημιουργούμενη λίστα των ενδιάμεσων κόμβων που μετέχουν στο μονοπάτι επικοινωνίας μεταξύ των S και T·
- $ExcludeList$, μια δυναμικά δημιουργούμενη λίστα και περιέχει κόμβους που αν λάβουν το μήνυμα δε θα πρέπει να το επεξεργαστούν·

- *NextHop*, μια δυναμικά δημιουργούμενη λίστα και περιέχει κόμβους που αν λάβουν θα πρέπει να το επεξεργαστούν υποχρεωτικά, και

- $hash_{K_{S,T}}(ID_S, ID_T, seq, hop_{max})$, το αποτέλεσμα της κατακερματικής (hash) συνάρτησης με τη χρήση του κλειδιού $K_{S,T}$.

Στον αρχικό κόμβο S

Η πηγή S εκτελεί τον αλγόριθμο όπως αυτός παρουσιάζεται στην εικόνα 6.1. Ο αρχικός κόμβος S αρχικοποιεί τον μετρητή $hop_{cnt} = 0$ και επιλέγει τον μέγιστο αριθμό κόμβων hop_{max} που θα περιέχονται στο μονοπάτι, βασιζόμενος στις πληροφορίες που έχει για το δίκτυο όπως, π.χ. ο αριθμός των άμεσων γειτόνων του και η προσδοκώμενη/ αναμενόμενη πυκνότητα του δικτύου κ.ο.κ. Στη συνέχεια, αρχικοποιεί τις λίστες *RouteList* και την *ExcludeList* ενώ ταυτόχρονα τοποθετεί το σύνολο των άμεσων γειτόνων του στη λίστα $NextHop = N_S$, όπου N_S είναι η λίστα των άμεσων γειτονικών του κόμβων που έχει υπολογίσει από την προηγούμενη φάση του πρωτοκόλλου. Τέλος, ο αρχικός κόμβος S επιλέγει ένα τυχαίο κλειδί $K_{S,T}$, και υπολογίζει την κρυπτογράφηση αυτού του κλειδιού χρησιμοποιώντας το δημόσιο κλειδί PK_T του κόμβου τελικού προορισμού. Για λόγους ασφάλειας και ακεραιότητας, το μήνυμα περιέχει, επίσης, την τιμή της κατακερματικής συνάρτησης που έχει παραχθεί με τη χρήση του $K_{S,T}$, πάνω στα στατικά πεδία του μηνύματος αίτησης $Q_{S,T}$. Όταν ολοκληρωθεί αυτή η διαδικασία ο αρχικός κόμβος εκπέμπει το μήνυμα.

Στον ενδιάμεσο κόμβο n_i

Όταν ένας ενδιάμεσος κόμβος n_i λάβει ένα αντίγραφο του μηνύματος της εύρεσης νέων μονοπατιών $Q_{S,T}$, εκτελεί τον αλγόριθμο που περιγράφεται στην εικόνα 6.2. Κάθε ενδιάμεσος κόμβος n_i διατηρεί έναν πίνακα δρομολόγησης που περιέχει όλα τα ενεργά μονοπάτια προς τους άλλους κόμβους. Επιπλέον, διατηρεί μέσα στον πίνακα ένα δείκτη για τα πρόσφατα λαμβανόμενα

1) Set:
$hop_{cnt} = 0$, $hop_{max} = \text{MAX}$, $RouteList = \emptyset$, $ExcludeList = \emptyset$, $NextHops = N_S$
/* Initialize the route request query */

2) Select random $K_{S,T}$
/* The secret key (security association) to be shared between nodes *S* and *T* */

3) Compute $E_{PK_T}(K_{S,T})$ and $hash_{K_{S,T}}(ID_S, ID_T, seq, hop_{max})$

4) Construct and Broadcast
$Q_{S,T} = [ID_S, ID_T, seq, hop_{cnt}, hop_{\max}, RouteList, ExcludeList, NextHop,$
$E_{PK_T}(K_{S,T}),\ hash_{K_{S,T}}(ID_S, ID_T, seq, hop_{max})]$

Εικόνα 6.1: *Ο αλγόριθμος εύρεσης νέων μονοπατιών στον αρχικό κόμβο*

μηνύματα-αιτήσεις, για τα οποία δεν έχει λάβει απάντηση, έτσι ώστε να μην χρειαστεί να τα επεξεργαστεί ξανά. Για να αποφευχθεί η διατήρηση μεγάλων μηνυμάτων μέσα στον πίνακα δρομολόγησης, κάθε κόμβος που επεξεργάζεται ένα μήνυμα εύρεσης αποθηκεύει στον πίνακα δρομολόγησής του την τιμή της κατακερματικής συνάρτησης του μηνύματος για εύλογο χρονικό διάστημα. Πριν αρχίσει η επεξεργασία της λαμβανομένης αίτησης $Q_{S,T}$ ο κόμβος n_i δημιουργεί την τιμή κατακερματισμού του μηνύματος $Q_{S,T}$. Στη συνέχεια ελέγχει εάν αυτή η τιμή υπάρχει ήδη στον πίνακα δρομολόγησής του (*π.χ.* εάν το συγκεκριμένο αντίγραφο της αίτησης έχει ήδη επεξεργαστεί μια φορά) οπότε και δεν συνεχίζει την επεξεργασία του μηνύματος, αλλά αντιθέτως το διαγράφει. Σημειώνεται ότι αυτό δεν αποτρέπει τον κόμβο n_i να επεξεργαστεί ένα διαφορετικό αντίγραφο της αίτησης $Q'_{S,T}$ το οποίο περιέχει ίδιες τιμές στα πεδία ID_S, ID_T και *seq* αλλά το οποίο έχει φτάσει στον ενδιάμεσο κόμβο n_i μέσω ενός διαφορετικού δρόμου μετανάστευσης.

Πράγματι, εάν το αντίγραφο του μηνύματος $Q'_{S,T}$ φτάσει στον κόμβο n_i από ένα διαφορετικό δρόμο/μονοπάτι τότε το περιεχόμενο των λιστών *RouteList*, *ExcludeList* και *NextHop* που περιέχονται στο μήνυμα/αίτηση $Q'_{S,T}$ θα είναι διαφορετικό από αυτό που περιέχεται στο μήνυμα/αίτηση $Q_{S,T}$. Έτσι η τιμή

$hash(Q_{S,T}) \neq hash(Q'_{S,T})$ αυτού του αντίγραφου της αίτησης δεν θα έχει αποθηκευθεί στον πίνακα δρομολόγησης του κόμβου. Εξασφαλίζεται, έτσι, ότι όλα τα αντίγραφα της αίτησης θα επεξεργαστούν από κάθε ενδιάμεσο κόμβο για τουλάχιστον μια φορά ώστε να ανακαλυφθούν όλα τα υπάρχοντα μονοπάτια.

Ο αλγόριθμος αποτρέπει τη συμμετοχή ενός κόμβου σε περισσότερες από μια λίστες, όπως αυτές περιέχονται σε κάθε μήνυμα εύρεσης νέων μονοπατιών. Ωστόσο, ενώ αυτό μπορεί να συμβεί είτε από λάθος είτε από κακόβουλη χρήση, κάθε κόμβος n_i ελέγχει εάν στις λίστες τις οποίες έχει λάβει περιέχονται κοινές τιμές. Εάν διαπιστώσει ότι συμβαίνει κάτι τέτοιο διαγράφει το μήνυμα.

Σε αυτό το σημείο, ο κόμβος n_i ελέγχει εάν η ταυτότητά του περιέχεται στη λίστα *NextHop* του μηνύματος εύρεσης. Επίσης ελέγχει εάν ο αποστολέας της αίτησης *π.χ.* η τελευταία εισαγωγή στη λίστα *RouteList*, ανήκει στο σύνολο των πιστοποιημένων γειτονικών του κόμβων N_i. Εάν κάποιος από αυτούς τους ελέγχους αποτύχει τότε το μήνυμα διαγράφεται/απορρίπτεται. Η διαδικασία του βήματος αυτού παρέχει αμφίδρομη πιστοποίηση ανάμεσα σε οποιοδήποτε ζεύγος ενδιάμεσων κόμβων. Αυτό αποτελεί κρίσιμο σημείο για την προστασία από επιθέσεις πολλαπλής ταυτότητας.

Μετά από αυτούς τους ελέγχους, ο κόμβος n_i είναι πλέον βέβαιος για την εγκυρότητα του λαμβανομένου μηνύματος/αίτησης και προχωράει στην επεξεργασία του. Ο κόμβος n_i ενημερώνει τον πίνακα δρομολόγησής του έτσι ώστε να αποτραπεί η διπλή επεξεργασία μηνυμάτων. Στην περίπτωση όπου ο κόμβος n_i αποτελεί τον τελικό προορισμό του μηνύματος, τότε ο αλγόριθμος εύρεσης νέων μονοπατιών ολοκληρώνεται και χρησιμοποιείται ο αλγόριθμος απάντησης στην αίτηση.

Σε διαφορετική περίπτωση ο κόμβος n_i αυξάνει το μετρητή hop_{cnt} κατά ένα και ελέγχει τη νέα τιμή σε σχέση με το μέγιστο αποδεκτό μήκος μηνύματος hop_{max}, έτσι ώστε αν είναι δυνατόν να διαγράψει την αίτηση και να μην δημιουργούνται μεγάλα/μακριά μονοπάτια. Αυτό αποτρέπει την αίτηση από το

1) If ($hash(Q_{S,T}) \in RouteTable(n_i)$)
/* Drop the request query if the particular query thread has already been received by n_i */
OR (($RouteList \cap ExcludeList \neq \emptyset$)
OR ($RouteList \cap NextHop \neq \emptyset$)
OR ($ExcludeList \cap NextHop \neq \emptyset$))
/* Drop the query if the same node identifier belongs to more than one list */
OR (($ID_i \notin NextHop$) OR ($LastElement(RouteList) \notin N_i$)
/* Drop the query if the previous node is not an authenticated neighbor of n_i */
then
DROP($Q_{S,T}$)

else {
2) add($hash(Q_{S,T})$, $RouteTable(n_i)$)
/* The node n_i marks the specific route request query as processed */
3) If ($ID_i = ID_T$) then REPLY($Q_{S,T}$)
/* If n_i is the target, execute the route reply algorithm and exit */
else
{
4) $hop_{cnt} = hop_{cnt} + 1$
5) If ($hop_{cnt} > hop_{max}$)
/* Drop the query if it exceeds the maximum allowed hop-distance, to prevent propagation of the request query to long distance areas */
then
DROP($Q_{S,T}$)
else
{
6) $RouteList = RouteList + ID_i$
/*Node n_i adds itself to the *RouteList* */
7) $ExcludeList = ExcludeList + (NextHop - ID_i)$
/*Node n_i excludes the rest of the neighbors of the previous node, from this particular thread of the route request query */
8) $NextHop = N_i - (N_i \cap RouteList) - (N_i \cap ExcludeList)$
/*The neighbors of n_i are the allowed next hops of this thread of the query, unless they already belong to the routing path or have already been excluded from the routing path */
9) Update and Broadcast

$$Q_{S,T} = [ID_S, ID_T, seq, hop_{cnt}, hop_{max}, RouteList, ExcludeList, NextHop, Enc_{PK_T}(K_{S,T}), hash_{K_{S,T}}(ID_S, ID_T, seq, hop_{max})]$$

/* Update the query with the new values and broadcast it */
}
}
}

Εικόνα 6.2: *Ο αλγόριθμός εύρεσης νέων μονοπατιών στον ενδιάμεσο κόμβο*

να μεταδοθεί σε πολύ μακρινές αποστάσεις. Φυσικά, αυτός ο περιορισμός θα αποτρέψει την ανακάλυψη τυχόν υπαρχόντων μονοπατιών μοναδικών κόμβων τα οποία θα περιέχουν περισσότερους κόμβους από την δεδομένη αποδεκτή

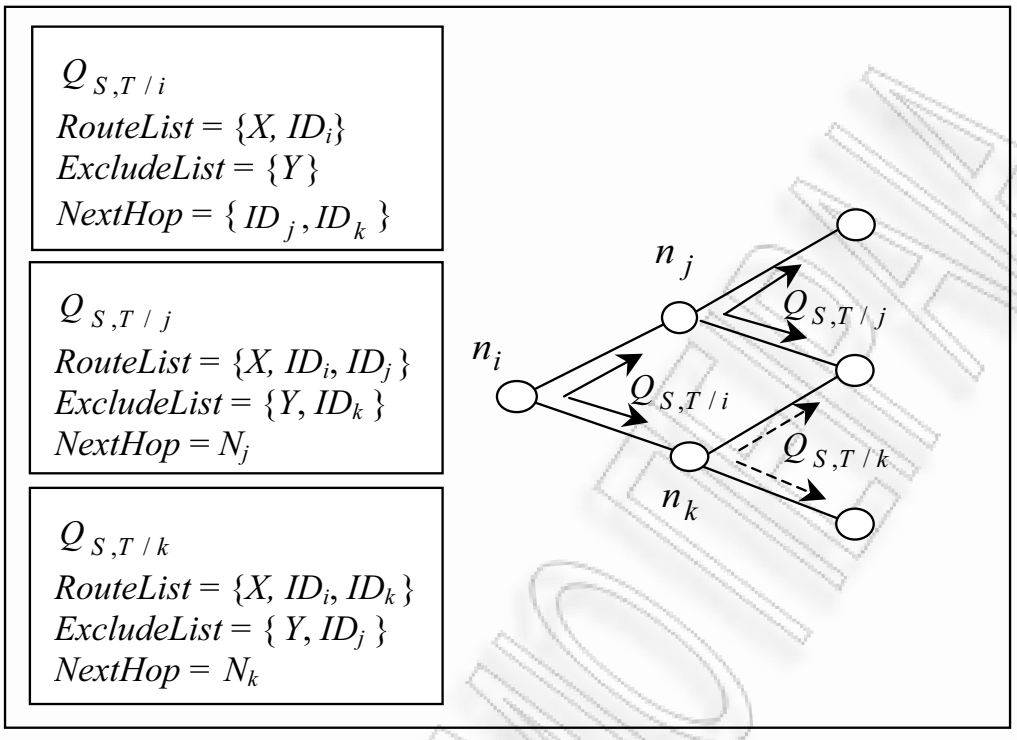
μέγιστη τιμή hop_{max}. Για το λόγο αυτό, αυτή η παράμετρος θα πρέπει να επιλέγεται με προσοχή, λαμβάνοντας υπόψη την υπάρχουσα τοπολογία του δικτύου, και την αποδεκτή καθυστέρηση, που υπεισέρχεται, στη μετάδοση του σήματος, κλπ.

Στη συνέχεια, ο κόμβος n_i επεξεργάζεται το μήνυμα/ αίτηση. Ενημερώνει τη λαμβανόμενη λίστα *RouteList* επισυνάπτοντας και τη δική του ταυτότητα ID_i. Ενημερώνει τη λίστα *ExcludeList*, ώστε να περιέχει τα μέλη της λαμβανομένης λίστας *NextHop*, διαγράφοντας παράλληλα τα τυχόν διπλά στοιχεία. Τέλος, δημιουργεί τη δική του έκδοση για τη λίστα *NextHop* εισάγοντας τους πιστοποιημένους άμεσους γείτονες του N_i τη χρονική εκείνη στιγμή, και διαγράφοντας τα, τυχόν, διπλά στοιχεία. Τελικά ο κόμβος n_i συμπληρώνει/κατασκευάζει το αντίγραφο της αίτησης και το εκπέμπει.

Η χρήση της λίστας *ExcludeList* αποτελεί βασικό στοιχείο για την επίδοση του πρωτοκόλλου και ιδιαίτερα για την αποδοτικότερη διάδοση του μηνύματος εύρεσης *νέων* μονοπατιών. Δημιουργώντας δυναμικά τα αντίγραφα της αίτησης ο αλγόριθμος καταλήγει στο να βρει όλα τα μονοπάτια μοναδικών/διακριτών κόμβων δεδομένου μέγιστου μήκος hop_{max}.

Για καλύτερη κατανόηση της όλης διαδικασίας ας θεωρηθεί το παρακάτω σενάριο. Έστω ότι n_i είναι ο κόμβος που εκπέμπει ένα μήνυμα $Q_{S,T}$ στους γείτονές του n_j και n_k (εικόνα 6.3). Για να διαχωρίστουν τα διαφορετικά αντίγραφα της αίτησης, δηλώνεται ως $Q_{S,T/x}$ το αντίγραφο που διέρχεται από τον κόμβο n_x. Με τον τρόπο αυτό, το αντίγραφο $Q_{S,T/i}$, που εκπέμπεται από τον κόμβο n_i θα περιέχει τις λίστες $RouteList = \{X, ID_i\}$, $ExcludeList = \{Y\}$ και $NextHop = \{ID_j, ID_k\}$, όπου τα X και Y δηλώνουν τη σειρά των μοναδικών ταυτοτήτων των κόμβων.

Και οι δυο κόμβοι n_j και n_k θα επεξεργαστούν την αίτηση εύρεσης μονοπατιών (θεωρείται ότι ισχύει $ID_j, ID_k \notin X, Y$). Ο κόμβος n_j θα προσθέσει τη μοναδική ταυτότητά του στη λίστα *RouteList*, τη μοναδική ταυτότητα του



Εικόνα 6.3: *Διασπορά του μηνύματος εύρεσης νέων μονοπατιών*

κόμβου n_k στη λίστα *ExcludeList* και θα ενημερώσει τη λίστα *NextHop* με το σύνολο των άμεσων γειτόνων του εκείνη τη χρονική στιγμή. Μετά τα βήματα αυτά, το αντίγραφο της αίτησης εύρεσης νέων μονοπατιών (request query) θα μεταμορφωθεί σε $Q_{S,T/j}$ και $Q_{S,T/k}$, περιέχοντας τις ενημερωμένες λίστες όπως αυτές παρουσιάζονται στην εικόνα 6.3. Καθένα απ' αυτά τα αντίγραφα της αίτησης θα προωθηθεί προς τον κόμβο προορισμού *T* με τον περιορισμό ότι σε αυτό το αντίγραφο $Q_{S,T/j}$ δεν θα επιτραπεί να ξαναπεράσει από τον κόμβο n_k και το αντίστροφο. Αυτό επιτρέπει στην αίτηση να προωθείται σε όλο και πιο απομακρυσμένους κόμβους ξεκινώντας από τον κόμβο-πηγή *S* προς τον κόμβο προορισμού *T*. Τα αντίγραφα της αίτησης που τυχόν κάνουν κύκλους και επιστρέφουν προς τα πίσω απορρίπτονται σε σύντομο χρονικό διάστημα όταν αυτά φτάσουν σε ένα κόμβο που βρίσκεται πλησιέστερα στην πηγή *S* και αυτός περιέχεται στη λίστα *ExcludeList*.

Αλγόριθμος Απάντησης

Όταν ο κόμβος προορισμού T λαμβάνει ένα αντίγραφο αίτησης εύρεσης νέων μονοπατιών $Q_{S,T/i}$ αποκρυπτογραφεί το $E_{PK_T}(K_{S,T})$, βρίσκει το κλειδί $K_{S,T}$ και ελέγχει την ορθότητα της παρεχόμενης τιμής της κατακερματικής συνάρτησης. Έπειτα, περιμένει για ένα ορισμένο χρονικό διάστημα έτσι ώστε να εξασφαλίσει ότι έχει λάβει οποιοδήποτε αντίγραφο της αίτησης που τυχόν ταξιδεύει/ μεταναστεύει από διαφορετικά μονοπάτια με τελικό προορισμό αυτόν. Η κρυπτογραφημένη τιμή hash για κάθε αντίγραφο αίτησης ελέγχεται επίσης. Τότε, ο κόμβος τελικού προορισμού T υπολογίζει το σύνολο M που περιέχει τα περισσότερα μονοπάτια μου μοναδικών κόμβων όπως αυτό εξηγείται παρακάτω:

Έστω ότι ο κόμβος προορισμού T λαμβάνει m αντίγραφα αίτησης $Q_{S,T/1}, ..., Q_{S,T/m}$. Από τις αντίστοιχες λίστες $RouteList_1$,..., $RouteList_m$, ο κόμβος προορισμού T υπολογίζει το μεγαλύτερο σύνολο λιστών που δεν έχουν κοινές τιμές μεταξύ τους. Θεωρείται ότι το μέγιστο σύνολο των λιστών που δεν έχουν κοινά στοιχεία μεταξύ τους είναι $\{RouteList_1, ..., RouteList_k : \bigcap_{i=1}^{k} RouteList_i = \oslash\}$, $1 \leq k \leq m$. Τότε, το μέγιστο σύνολο μονοπατιών μοναδικών κόμβων ανάμεσα στον αρχικό κόμβο S και στον κόμβο τελικού προορισμού T είναι $M = \{p_1, ..., p_k\} = \{(ID_S, RouteList_1, ID_T)$,..., $(ID_S, RouteList_k, ID_T)\}$. Για κάθε $RouteList_j \in M$, ο κόμβος T υπολογίζει και εκπέμπει ένα μήνυμα απάντησης: $R_{S,T/j}$= $[ID_S, ID_T, seq, RouteList_j, hash_{K_{S,T}}(ID_S, ID_T, seq, RouteList_j)]$.

Κάθε ενδιάμεσος κόμβος n_i που λαμβάνει το μήνυμα απάντησης $R_{S,T/j}$ ελέγχει εάν ισχύει: $n_i \in R_{S,T/i}$. Εάν δεν ισχύει, διαγράφει το μήνυμα. Διαφορετικά εάν ισχύει $ID_i \in RouteList_j$, τότε ο κόμβος n_i ελέγχει εάν οι κόμβοι που βρίσκονται μια θέση πριν και μια θέση μετά από αυτόν στη λίστα $RouteList_j$ ανήκουν στο σύνολο των γειτόνων του N_i. Σε αυτή την περίπτωση ο κόμβος n_i επανεκπέμπει το μήνυμα απάντησης, $R_{S,T/j}$, ως ορθό, διαφορετικά το διαγράφει. Τελικά, εάν η μοναδική ταυτότητα του κόμβου ταυτίζεται με

την μοναδική ταυτότητα της πηγής, δηλαδή ισχύει $ID_i = ID_S$ τότε ο κόμβος n_i είναι η πηγή. Σε αυτή την περίπτωση, ο κόμβος πηγή ελέγχει την τιμή $hash_{K_{S,T}}(ID_S, ID_T, seq, RouteList_j)$ και εάν είναι ορθή, αποθηκεύει το μονοπάτι $p_j = (ID_S, RouteList_j, ID_T)$ ως ενεργό και κατάλληλο για την επικοινωνία του με τον κόμβο προορισμό T.

Ο κόμβος-πηγή μπορεί να επικοινωνήσει με τον κόμβο προορισμού διαμέσου των μονοπατιών μοναδικών κόμβων με τρεις διαφορετικές μεθόδους.

- Στην πρώτη *απλή* μέθοδο, ο κόμβος πηγή S χρησιμοποιεί *ένα*, και μάλιστα το μικρότερο σε μήκος, μονοπάτι από το σύνολο M. Μπορεί να χρησιμοποιηθεί ένα εναλλακτικό μονοπάτι εάν αυτό που είναι ενεργό καταστραφεί.

- Με την *παράλληλη* μέθοδο ο κόμβος πηγή χρησιμοποιεί παράλληλα k ενεργά μονοπάτια μοναδικών κόμβων. Αυτή αποτελεί την πιο ακριβή μέθοδο και επίσης την πιο ασφαλή, αφού τουλάχιστον k κόμβοι θα πρέπει να είναι ταυτόχρονα κατειλημμένοι από κακόβουλους χρήστες έτσι ώστε να υπάρχει μια επιτυχής επίθεση άρνησης υπηρεσίας (DoS).

- Τέλος, με την *μικτή* μέθοδο, η επικοινωνία πραγματοποιείται όπως και με τη απλή μέθοδο. Είναι δυνατόν να συμβεί μια μεταπήδηση στην παράλληλη μέθοδο όταν ένας από τους δύο ακραίους κόμβους (είτε η πηγή είτε ο προορισμός) το απαιτήσει, *π.χ.* όταν κατά την επικοινωνία μεταφέρονται σημαντικά δεδομένα, σημαντικές πληροφορίες και υπάρχει υποψία ότι το κανάλι επικοινωνίας δέχεται επίθεση άρνησης υπηρεσίας.

Σημείωση πρώτη. Για να αποφευχθούν καθυστερήσεις που δημιουργούνται κατά τον υπολογισμό του μεγαλύτερου συνόλου από μονοπάτια μοναδικών κόμβων, ο κόμβος προορισμού T μπορεί να χρησιμοποιήσει το πρώτο μονοπάτι ως προσωρινό. Όταν το σύνολο M των μονοπατιών μοναδικών κόμβων έχει υπολογιστεί τότε ο κόμβος προορισμού T μπορεί να χρησιμοποιήσει κάποιο

από τα μονοπάτια του συνόλου.

Αλγόριθμος Λάθους

Εάν ένας κόμβος n_i διαπιστώσει κατά τη διάρκεια της πιστοποίησης των άμεσων γειτόνων του, τη χρονική στιγμή $t+1$, ότι κάποιος σύνδεσμός του προς κάποιο γειτονικό κόμβο n_j, κατά τη χρονική στιγμή t, έχει διακοπεί τότε ο κόμβος n_i εκπέμπει ένα μήνυμα ανίχνευσης λάθους διαδρομής για κάθε μονοπάτι που διέρχεται από τον κόμβο n_i, και το οποίο μονοπάτι επηρεάζεται από τον σύνδεσμο (n_i, n_j) που έχει διακοπεί. Το εκπεμπόμενο αυτό μήνυμα έχει υπογραφεί ψηφιακά από τον κόμβο n_i. Εάν το μήνυμα δεν έχει υπογραφεί, τότε κακόβουλοι κόμβοι μπορεί να πλημμυρίσουν το δίκτυο με εσφαλμένα/ κάλπικα μηνύματα ανίχνευσης λάθους ακόμα και για μονοπάτια στα οποία αυτοί δε συμμετέχουν και με αυτό τον τρόπο να διακόψουν την επικοινωνία. Το μήνυμα ανίχνευσης λάθους έχει την ακόλουθη μορφή:

$E_{S,T} = [ID_S, ID_T, seq, ID_i, RouteList, sig_i\ (ID_S, ID_T, seq\ , ID_i, RouteList)]$.

Κάθε κόμβος που συμμετέχει στο μονοπάτι το οποίο έχει διακοπεί, σημειώνει το συγκεκριμένο μονοπάτι ως μη διαθέσιμο και επανεκπέμπει το μήνυμα μέχρι να ενημερωθούν η πηγή S και ο προορισμός T. Ανάλογα με τη μέθοδο επικοινωνίας, ένας τελικός κόμβος μπορεί να επανεκκινεί τη διαδικασία εύρεσης νέων μονοπατιών όταν έχουν καταστραφεί

α) ένα μοναδικό μονοπάτι,

β) ένας κατώτερος αριθμός μονοπατιών, είτε

γ) όταν όλα τα ενεργά μονοπάτια

από τη πηγή S προς τον προορισμό T.

6.3 Ανάλυση Ασφάλειας

Αναλύονται οι ιδιότητες ασφάλειας του πρωτοκόλλου SecMR σε σχέση με άλλα πρωτόκολλα πολλαπλών μονοπατιών που εμφανίζουν παρόμοιες συγκρίσιμες ιδιότητες ασφάλειας.

6.3.1 Πιστοποίηση σε επίπεδο ακραίων κόμβων

Η διαδικασία εύρεσης *νέων* μονοπατιών περιέχει πιστοποίηση από άκρο σε άκρο με την σχέση ασφάλειας $K_{S,T}$ που οι ακραίοι κόμβοι έχουν κάποια στιγμή, στο παρελθόν, ανταλλάξει. Η τιμή $hash_{K_{S,T}}$ (ID_S, ID_T, seq, hop_{max}), που περιλαμβάνεται στο αρχικό μήνυμα-αίτηση εύρεσης μονοπατιών, επιτρέπει στον τελικό κόμβο προορισμού να επιβεβαιώσει την αυθεντικότητα της αίτησης. Σημειώνεται ότι για τη σύνδεση της σχέσης ασφάλειας $K_{S,T}$ με τον αρχικό κόμβο-πηγή S, ο κόμβος S μπορεί να χρειαστεί να υπογράψει το κλειδί $K_{S,T}$ πριν το κρυπτογραφήσει. Ωστόσο, το κόστος κρυπτογράφησης με δημόσιο κλειδί είναι ελάχιστο από τη στιγμή που χρησιμοποιείται η μέθοδος Κρυπτογράφησης Ελλιπτικών Καμπύλων (Elliptic Curve Cryptosystem) και μόνο από τους ακραίους κόμβους. Επιπλέον, εάν κάθε ζεύγος κόμβων μοιράζεται μια σχέση ασφάλειας πριν από τη επικοινωνία (το οποίο είναι δυνατό για δίκτυα μικρού μεγέθους), οι κόμβοι δεν χρειάζεται να ανταλλάξουν το κλειδί $K_{S,T}$ κατά τη διάρκεια της αίτησης εύρεσης *νέων* μονοπατιών.

6.3.2 Πιστοποίηση σε επίπεδο ζεύξεων

Οι ζεύξεις ενός μονοπατιού πιστοποιούνται κατά τη διάρκεια της πρώτης φάσης λειτουργίας του πρωτοκόλλου, την πιστοποίηση των γειτόνων. Από τη στιγμή που κάθε κόμβος n_i πιστοποιεί τους άμεσους γείτονές του περιοδικά, μπορεί να επιβεβαιώσει την αυθεντικότητα των ζεύξεων του, που περιέχονται σε οποιοδήποτε, μονοπάτι συμμετέχει και αυτός.

Κατά τη διάρκεια διάδοσης του μηνύματος-αίτησης ευρέσεως νέων μονοπατιών κάθε κόμβος n_i αποδέχεται/λαμβάνει μια αίτηση, μόνο εάν ο τελευταίος κόμβος n_i που έχει εισαχθεί στη λίστα *RouteList*, η οποία περιέχεται στο λαμβανόμενο μήνυμα, αποτελεί έναν πιστοποιημένο γείτονα του κόμβου n_i. Επιπλέον, κατά τη διάρκεια διάδοσης του μηνύματος απάντησης, κάθε κόμβος n_i αποδέχεται και προωθεί το μήνυμα απάντησης μόνο όταν οι δύο κόμβοι (και συγκεκριμένα οι μοναδικές τους ταυτότητες) που βρίσκονται πριν και μετά από το ID_i στο μονοπάτι δρομολόγησης $p_j = (ID_S, RouteList_j, ID_T)$ του μηνύματος απάντησης, είναι πιστοποιημένοι γείτονες του n_i. Σημειώστε ότι αυτοί οι έλεγχοι είναι αποτελεσματικοί χωρίς μεγάλο υπολογιστικό κόστος από τη στιγμή που δεν χρησιμοποιείται κάποιο είδος κρυπτογράφησης.

Κάθε κόμβος n_i ελέγχει μόνο εάν οι ταυτότητες ανήκουν στο τρέχον σύνολο των πιστοποιημένων γειτόνων του N_i^t. Η χρήση της πιστοποιημένης γειτονιάς είναι πολύ αποτελεσματική, καθώς οι ενέργειες κρυπτογράφησης πραγματοποιούνται μόνο μια φορά κατά τη διάρκεια μιας χρονικής περιόδου, ανεξάρτητα από τον αριθμό μηνυμάτων αίτησης ευρέσεως νέων μονοπατιών (route request query) και μηνυμάτων απάντησης που λαμβάνονται από έναν ενδιάμεσο κόμβο. Επιπλέον, αυτή η κοινόχρηστη επαλήθευση/πιστοποίηση ανάμεσα στους γειτονικούς κόμβους καταναλώνει λιγότερη ενέργεια και υπολογιστική ισχύ από τη συνεχή επικοινωνία με την αρχή πιστοποίησης *CA* ακόμα και για μια κοινή/τετριμμένη επαλήθευση. Αυτό το πλεονέκτημα μεγιστοποιείται για δίκτυα των οποίων η κινητικότητα είναι μικρή. Η εκάστοτε διάρκεια της χρονικής περιόδου κατά την οποία θα πραγματοποιείται η πιστοποίηση των άμεσων γειτόνων αποτελεί παράμετρο του συστήματος. Εξαρτάται, δε, από το πόσο συχνά αναμένεται να καταστραφούν οι ζεύξεις ανάμεσα στους κόμβους, δηλαδή οι κόμβοι να μεταναστεύσουν/μετακινηθούν έξω από την πιστοποιημένη γειτονιά ή όταν νέοι κόμβοι εισέλθουν στην πιστοποιημένη γειτονιά.

6.3.3 Ακεραιότητα από άκρο-σε-άκρο

Το μονοπάτι δρομολόγησης είναι, επίσης, προστατευμένο από την άποψη της ακεραιότητας κατά τη διάρκεια της διάδοσης των μηνυμάτων απάντησης σε επίπεδο ακραίων κόμβων. Πράγματι, κάθε μήνυμα απάντησης περιλαμβάνει μια τιμή $hash_{K_{S,T}}(ID_S, ID_T, seq, RouteList_j)$. Έτσι, εάν το μονοπάτι δρομολόγησης $p_j = (ID_S, RouteList_j, ID_T)$ έχει μετατραπεί/αλλαχθεί, τότε η επαλήθευση της τιμής κατακερματισμού θα αποτύχει στον αρχικό κόμβο και δεν θα χρησιμοποιηθεί το ψεύτικο/κάλπικο μονοπάτι.

6.3.4 Προστασία απέναντι σε συνεργαζόμενους κακόβουλους κόμβους

Η προστασία αποτελεί τη βασική ιδιότητα ασφάλειας για την οποία έχει σχεδιαστεί το πρωτόκολλο SecMR. Η προστασία αυτή επιτυγχάνεται με τη χρήση πολλαπλών μονοπατιών δρομολόγησης. Όταν χρησιμοποιούνται k μονοπάτια διακριτών κόμβων για την επικοινωνία, ένας κακός θα πρέπει να καταλάβει τουλάχιστον k κόμβους - και συγκεκριμένα τουλάχιστον έναν κόμβο σε κάθε μονοπάτι-, έτσι ώστε, να ελέγχει πλήρως την επικοινωνία ανάμεσα στον κόμβο-πηγή και τον τελικό προορισμό. Ανάλογα με τη μέθοδο επικοινωνίας, το SecMR προσφέρει διαφορετικά επίπεδα προστασίας. Αν χρησιμοποιηθεί η *παράλληλη* μέθοδος, το SecMR πρωτόκολλο είναι ανθεκτικό απέναντι σε $k-1$ συνεργαζόμενους κακόβουλους κόμβους. Εάν χρησιμοποιηθεί η *απλή* μέθοδος ο κακόβουλος χρήστης μπορεί να διακόψει την επικοινωνία καταλαμβάνοντας μόνο το μοναδικό ενεργό μονοπάτι. Ο χρόνος που χρειάζεται για να ενεργοποιήθεί ένα εναλλακτικό μονοπάτι εξακολουθεί να είναι πολύ μικρότερος από ό,τι στα πρωτόκολλα μοναδικού μονοπατιού. Η καθυστέρηση αυτή είναι σημαντική ιδιαίτερα σε περιπτώσεις όπου τέτοιες διακοπές επικοινωνίας μπορεί να είναι κρίσιμες. Το επίπεδο προστασίας, όταν χρησιμοποιείται η *μικτή* μέθοδος, κυμαίνεται ανάμεσα στο επίπεδο της απλής και της παράλληλης μεθόδου και μπορεί να αποδειχθεί αποτελεσματικότερο για απλές πρακτικές

εφαρμογές.

Σημείωση δεύτερη. Η προστασία της πραγματικής επικοινωνίας μπορεί να πραγματοποιηθεί μετά την εγκαθίδρυση των μονοπατιών δρομολόγησης με δοκιμασμένες τεχνικές κρυπτογράφησης και εφαρμογή ασφαλών πρωτοκόλλων μεταφοράς μηνυμάτων, *π.χ.* [19].

Στον πίνακα 6.1 παρουσιάζονται θέματα ασφάλειας που έχουν αναλυθεί σε αυτή την ενότητα σε σχέση με τα πρωτόκολλα που έχουν συζητηθεί παραπάνω.

Πίνακας 6.1: *Σύγκριση Πρωτοκόλλων*

Χαρακτηριστικά	Πρωτόκολλα			Αδυναμίες Ασφάλειας (λόγω της έλλειψης αυτού του χαρακτηριστικού)
	SecMR	Multipath	SRP	
πιστοποίηση από άκρο-σε-άκρο	ναι	ναι	ναι	έλλειψη ακεραιότητας δεδομένων
πιστοποίηση από σύνδεσμο-σε-σύνδεσμο	ναι	ναι	όχι	πλαστοπροσωπία, επιθέσεις πολλαπλών ταυτοτήτων
ολοκληρωμένο	ναι	ναι	όχι	λιγότερα μονοπάτια
μηνύματα αίτησης που επεξεργάζεται κάθε ενδιάμεσος κόμβος	όλα	όλα	μόνο το πρώτο	φαινόμενο του ανταγωνισμού

Βιβλιογραφία

[1] S. Bengio, G. Brassard, Y. Desmedt, C. Goutier, and J. Quisquater, *Secure implementation of identification systems*, Journ. of Cryptology, Springer-Verlag 4 (1991), no. 3, 175–184.

[2] M. Burmester and Y. Desmedt, *Secure communication in an unknown network using certificates*, Proc. of the Advances in Cryptography - ASIACRYPT'99, LNCS, vol. 1716, Springer-Verlag, 1999, pp. 274–287.

[3] M. Burmester and T. van Le, *Secure multipath communication in mobile ad hoc networks*, Proc. of ITCC'04 (Las Vegas, USA), IEEE, Apr 2004.

[4] L. Buttyan and J.P. Hubaux, *Enforcing service availability in mobile ad hoc* WANS, Proc. of the 1st MobiHoc Conference (BA, Massachusetts), ACM, Aug 2000.

[5] J. R. Douceur, *The sybil attack*, Proc. of the 1st International Workshop on Peer-to-Peer Systems (IPTPS'02), American Mathematical Society, Mar 2002.

[6] Z. Haas and M. Perlman, *The performance of query control schemes for zone routing protocol*, Proc. of SIGCOMM'98, ACM, 1998.

[7] Y-C. Hu, A. Perrig, and D.B. Johnson, *Rushing attacks and defense in wireless ad hoc routing protocols*, Proceedings of WiSe'03, 2003, pp. 30–40.

[8] J. Hubaux, L. Buttyan, and S. Capkun, *The quest for security in mobile ad hoc networks*, Proc. of the 2nd MobiHoc Conference, ACM, Aug 2001.

[9] D.B. Johnson and D.A. Maltz, *Mobile computing*, ch. Dynamic source routing in ad-hoc wireless networks, pp. 152–181, Kluwer Academic Publishers, 1996.

[10] N. Koblitz, *Elliptic curve cryptosystems*, Mathematics of Computation 48 (1997), 203–209.

[11] P. Kotzanikolaou, R. Mavropodi, and C. Douligeris, *Secure multi-path routing for mobile ad hoc networks*, Proc. of the 2nd Annual Conference on Wireless On-demand Network Systems and Services (WONS'2005) (St. Moritz, Switzerland), IEEE, Jan 2005, pp. 89–96.

[12] S-J Lee and M. Gerla, *Split multipath routing with maximally disjoint paths in ad hoc networks*, Proc. of ICC'01, IEEE, Jun 2001, pp. 3201–3205.

[13] M. Marina and S. Das, *Ad hoc on-demand multipath distance vector routing*, ACM Mobile Computing and Communications Review 6 (2002), no. 3, 92–93.

[14] J. Marshall, V. Thakur, and A. Yasinsac, *Identifying flaws in the secure routing protocol*, Proc. of the 22nd IPCC Conference, IEEE, Apr 2003, pp. 167–174.

[15] S. Marti, T.J. Giuli, K. Lai, and M. Baker, *Mitigating routing misbehavior in mobile ad hoc networks*, Proc. of the 6th MobiCom Conference, ACM, Aug 2000.

[16] R. Mavropodi, C. Douligeris, *Multipath Routing protocols for Mobile Ad Hoc Networks: Security Issues and Performance Evaluation*, Proc. of the Workshop on Autonomic Communication (WAC 2005), LNCS, vol. 3854/2006, Springer-Verlag, Oct. 2005, pp. 165–176.

[17] A. Nasipuri and S.R. Das, *On-demand multipath routing for mobile ad hoc networks*, Proc. of INFOCOM'99, IEEE, 1999, pp. 64–70.

[18] P. Papadimitratos and Z. Haas, *Secure routing for mobile ad hoc networks*, Proc. of he CNDS'02 (TX, San Antonio), jan 2002.

[19] P. Papadimitratos and Z. Haas, *Secure message transmission in mobile ad hoc networks*, Elsevier Ad Hoc Networks 1 (2003), 199–209.

[20] C. Perkins, E. Royer, and S. Das, *Ad hoc on-demand distance vector routing*, Proc. of the Workshop on Mobile Computing Systems and Applications, IEEE, Feb 1999, pp. 90–100.

[21] A-P Subramanian, A. J. Anto, J. Vasudevan, and P. Narayanasamy, *Multipath power sensitive routing protocol for mobile ad hoc networks*, Proc. of the 1st IFIP/TC6 Working Conference on Wireless On-Demand Network Systems, (WONS'2004), LNCS, vol. 2928, Springer-Verlag, Jan 2004, pp. 171–183.

[22] Jie Wu, *An extended dynamic source routing scheme in ad hoc wireless networks*, Telecommunication Systems 1 (2003), no. 4, 61–75.

[23] H. Yang, X. Meng, and S. Lu, *Self-organized network-layer security in mobile ad hoc networks*, Proc. of the ACM workshop on Wireless security (Atlanta, GA), ACM, Sep 2002, pp. 11–20.

[24] S. Yi, P. Naldurg, and R. Kravets, *Security-aware ad-hoc routing for wireless networks*, Proc. of the 2nd Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc'01) (Long Beach, CA), ACM, Oct 2001, pp. 299–302.

[25] S. Yi and R. Kravets, *MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks*, & The 2nd Annual PKI Research Workshop (PKI'03), Gaithersburg MD, USA, April 2003.

[26] L. Zhou and Z. Haas, *Securing ad hoc networks*, IEEE Network Magazine 13 (1999), no. 6, 24–30.

[27] Mavropodi R., Kotzanikolaou P., Douligeris C., *SecMR - α SECure Multipath routing Protocol for ad hoc networks*, Ad Hoc Networks, (Elsevier - In Press - Available online 28 June 2006).

[28] Mavropodi R., Douligeris C., *Multipath Routing protocols for Mobile Ad Hoc Networks: Security Issues and Performance Evaluation*, WAC 2005, LNCS, volume 3854, Springer-Verlag, p 165-176, 2006

[29] Kotzanikolaou P., Mavropodi R., Douligeris C., *Secure Multipath Routing for Mobile Ad Hoc Networks*, WONS 2005, St. Moritz, Switzerland, January 19-21, 2005

[30] Mavropodi R., Kotzanikolaou P., Douligeris C., *Performance Analysis of Secure Multipath Routing Protocols for Mobile Ad Hoc Networks*, WWIC 2005, LNCS, volume 3510, Springer-Verlag, p 269-278, 2005

Κεφάλαιο 7

Μελέτη Επίδοσης Πρωτοκόλλων Δρομολόγησης στα Δίκτυα Ad Hoc

Ένα κινητό δίκτυο Ad Hoc αποτελεί μια συλλογή από αυτόνομους κινητούς κόμβους που μπορούν να επικοινωνήσουν μεταξύ τους με τη χρήση ασύρματων καναλιών. Όπως παρουσιάστηκε αναλυτικότερα και σε προηγούμενα κεφάλαια, λόγω των περιορισμών που υπάρχουν στο εύρος κάλυψης του ασύρματου καναλιού, για να επικοινωνήσει ένας κόμβος με άλλους που βρίσκονται έξω από αυτή την περιοχή, θα πρέπει να βασιστεί (και να εμπιστευτεί) στους γειτονικούς του κόμβους ώστε να προωθήσουν τα δεδομένα του στον κατάλληλο προορισμό. Ωστόσο επειδή δεν υπάρχει κάποια σταθερή δομή, όπως ένας σταθμός βάσης (base station) ο κάθε κόμβος θα πρέπει να λειτουργεί ως δρομολογητής. Έτσι ένα πρωτόκολλο δρομολόγησης στα δίκτυα Ad Hoc εφαρμόζεται σε κάθε κόμβο και υπόκειται στους περιορισμούς που έχει ο κάθε κόμβος. Ένα αξιόπιστο ασφαλές πρωτόκολλο δρομολόγησης πρέπει να έχει ελάχιστο κόστος σε μέγεθος μηνυμάτων (άρα και σε υπολογιστική ισχύ), καθώς και σε φορτίο κίνησης στο δίκτυο.

Σκοπός του κεφαλαίου αυτού είναι η αξιολόγηση της αποδοτικότητας του πρωτοκόλλου SecMR, που παρουσιάστηκε στο προηγούμενο κεφάλαιο, σε σύγκριση με υπάρχοντα ασφαλή πρωτόκολλα δρομολόγησης πολλαπλών μονοπατιών και συγκεκριμένα το Multipath [3] και το SRP [18]. Η αξιολόγηση αυτή πραγματοποιείται σε δύο στάδια. Αρχικά συγκρίνονται τα πρωτόκολλα σε σχέση με το μέγεθος των μηνυμάτων που παράγουν. Στη συνέχεια, μέσω προσομοίωσης, μελετάται η επίδοση του δικτύου χρησιμοποιώντας ως δείκτες τα ποσοστά απόρριψης πακέτων και μέσης καθυστέρησης μετά από την εκτέλεση ποικίλων σεναρίων κίνησης και παραγωγής δεδομένων.

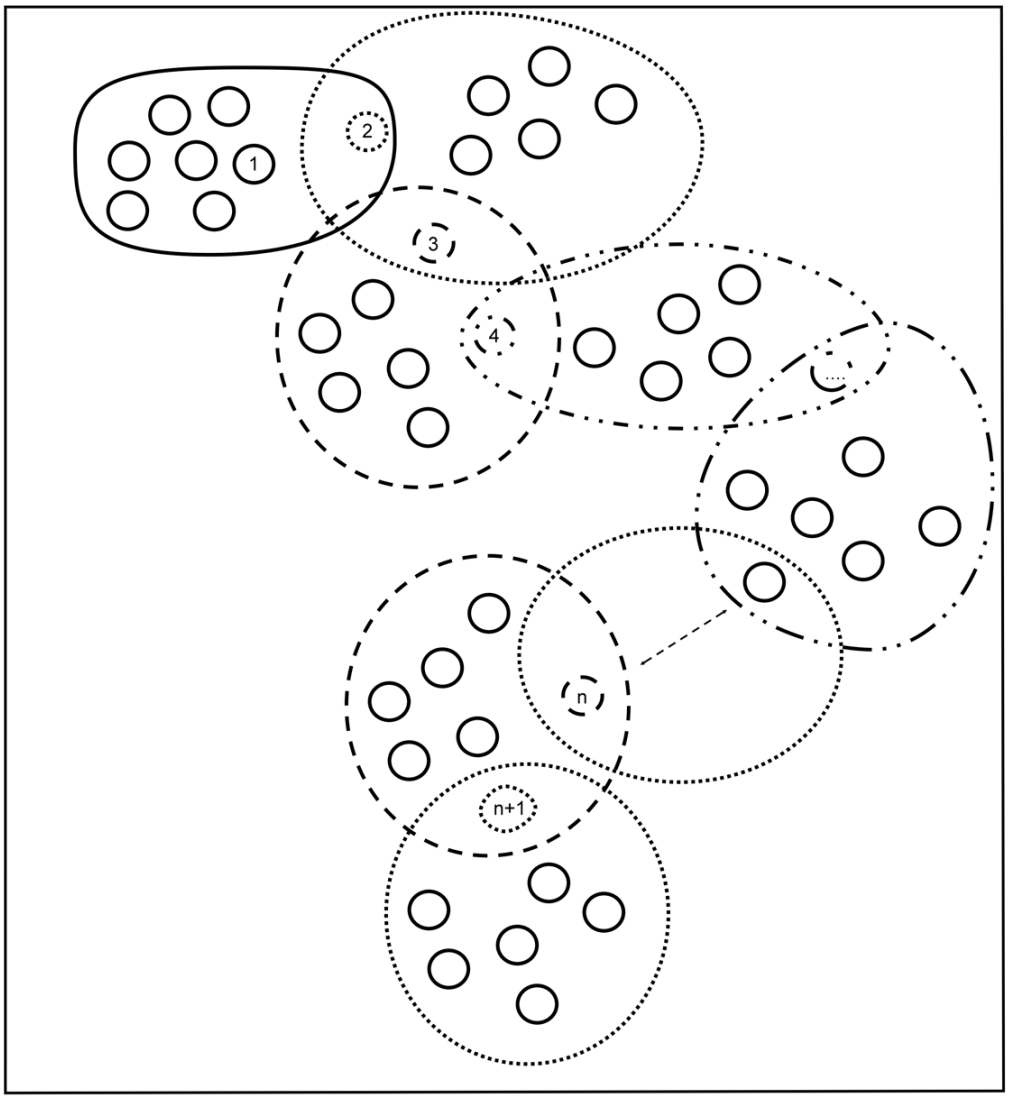
7.1 Ανάλυση Επίδοσης Πρωτοκόλλων Δρομολόγησης

Στην ενότητα αυτή αναλύονται τα χαρακτηριστικά επίδοσης και παρουσιάζονται αποτελέσματα μέσω προσομοίωσης του πρωτοκόλλου SecMR σε σύγκριση με άλλα πρωτόκολλα πολλαπλών μονοπατιών με παρόμοιες / συγκρίσιμες ιδιότητες ασφάλειας και συγκεκριμένα τα Multipath [3] και SRP [18].

7.1.1 Μέγεθος μηνύματος

Το μέγεθος των μηνυμάτων τα οποία ανταλλάσσονται κατά τη διάρκεια της φάσης εύρεσης μονοπατιών δρομολόγησης είναι κρίσιμο για την επίδοση των πρωτοκόλλων. Η κατάσταση γίνεται ακόμα πιο κρίσιμη στα πρωτόκολλα δρομολόγησης πολλαπλών μονοπατιών. Εάν μια αίτηση περιέχει πληροφορίες που αφορούν τους ενδιάμεσους κόμβους, τότε αντιμετωπίζει τον κίνδυνο να δημιουργεί μεγάλα σε μέγεθος μηνύματα. Το πρωτόκολλο SecMR δεν περιλαμβάνεται σε αυτή την κατηγορία καθώς το μέγεθος των λιστών *RouteList*, *NextHop* και *ExcludeList* που περιέχονται στα μηνύματά του μεγαλώνει με ελεγχόμενο και προβλεπόμενο τρόπο.

Συγκεκριμένα, το μέγιστο μέγεθος στοιχείων που μπορεί να περιέχει η



Εικόνα 7.1: *Δίκτυο που παράγει ExcludeList με μέγιστο μέγεθος*

λίστα *RouteList* είναι R_{max}, το οποίο αναπαριστά το μέγιστο επιτρεπτό μήκος που μπορούν να έχουν τα μονοπάτια δρομολόγησης στο συγκεκριμένο δίκτυο και ορίζεται από την τιμή της μεταβλητής hop_{max}. Η λίστα *NextHop* μπορεί να περιέχει μέχρι $N_{max} - 1$ μέλη, όπου N_{max} είναι ο μέγιστος αριθμός γειτόνων που μπορεί να έχει ένας κόμβος. Το μέγιστο μέγεθος της λίστας *ExcludeList*,

όσον αφορά τον αριθμό των μελών της, είναι:

$$1 + (N_{max} - 2) * (R_{max} - 1) \tag{7.1}$$

Έστω το σενάριο όπου ένα πρωτόκολλο δρομολόγησης εφαρμόζεται σε ένα δίκτυο του οποίου οι κόμβοι είναι διασκορπισμένοι σε συστάδες με μέγιστο αριθμό $N_{max}+1$ ανά ομάδα μελών. Για να είναι ένα πρωτόκολλο δρομολόγησης πρακτικό και να εφαρμόζεται σ' ένα δίκτυο αυτού του τύπου τότε οι συστάδες των κόμβων θα πρέπει να έχουν τουλάχιστον ένα κοινό κόμβο. Στη χειρότερη περίπτωση, κάθε ζεύγος αυτών των ομάδων θα έχει μόνο έναν κοινό κόμβο μεταξύ τους. Η εικόνα 7.1 παρουσιάζει ένα τυπικό ασύρματο κινητό δίκτυο που παρουσιάζει αυτού του είδους τις σχέσεις ανάμεσα στους κόμβους του. Εξ ορισμού, το πρωτόκολλο SecMR δεν επιτρέπει τη συμμετοχή των κόμβων σε παραπάνω από μια λίστα. Έτσι, στο σενάριο όπου οι συστάδες των κόμβων έχουν περισσότερους από έναν κοινούς κόμβους μεταξύ τους, το πρωτόκολλο SecMR θα εμποδίσει τη λίστα *ExcludeList* να φτάσει το μέγιστο μέγεθος της. Παρακάτω θα ασχοληθούμε με τη χειρότερη περίπτωση σεναρίου κατά την οποία η λίστα *ExcludeList* είναι δυνατόν να καταλήξει να περιέχει το μέγιστο αριθμό κόμβων.

Πίνακας 7.1: *Σύγκριση Πρωτοκόλλων - Μέγεθος Λίστας*

Πρωτόκολλο	Μέγιστο μέγεθος λίστας		
	RouteList	NextHop	ExcludeList
SecMR Multipath SRP	1	7 7 -	0 - -
SecMR Multipath SRP	2	6=(7-1) 13=7 + 6 -	6= 0 + (7-1)= 1+(7-2) - -
SecMR Multipath SRP	3	6=(7-1) 19=7+6+6 -	11= 0+1+(7-2)+(7-2) - -
.....	.....	.....	.....
SecMR Multipath SRP	v	$(N_{max}\text{-}1),\ v > 1$ $1 + v*(N_{max} - 1),\ v > 1$ -	$1+(v\text{-}1)*(N_{max} - 2),\ v > 1$ - -

Ο πίνακας 7.1 αναπαριστά την ανάπτυξη των λιστών του μηνύματος όσον αφορά τον αριθμό των μελών των λιστών που περιέχονται. Τα μηνύματα παράγονται από τα τρία πρωτόκολλα που συγκρίνονται δηλαδή το SecMR, το Multipath και το SRP.

Από τον ορισμό του αλγόριθμου, όπως αυτός περιγράφεται στην εικόνα 6.2 ισχύει ότι:

$$RouteList = RouteList + ID_i \tag{7.2}$$

$$NextHop = N_i - (N_i \cap RouteList) - (N_i \cap ExcludeList) \tag{7.3}$$

$$ExcludeList = ExcludeList + (NextHop - ID_i) \tag{7.4}$$

Εφαρμόζοντας τις 7.2, 7.3 και 7.4 στον πίνακα 7.1 για $R_{max} = n+1$ έχουμε:

$$RouteList \overset{7.2}{\Rightarrow} RouteList + ID_i = n + 1 = R_{max}$$

Πίνακας 7.2: *Σύγκριση Πρωτοκόλλων - Μέγεθος λίστας έως 5 μέλη*

Πρωτόκολλο	Μέγιστο μέγεθος λίστας		
	RouteList	NextHop	ExcludeList
SecMR	5	4	13
Multipath		21	-
SRP		-	-

$$
\begin{aligned}
NextHop &\overset{(7.3)}{\Rightarrow} N_i - (N_i \cap RouteList) - (N_i \cap ExcludeList) \\
&= N_{max} - (ID_i) - (N_{max} - ExcludeList) \\
&= N_{max} - 1 - \emptyset \\
&= N_{max} - 1 \qquad (7.5)
\end{aligned}
$$

$$
\begin{aligned}
ExcludeList &\overset{(7.4)}{\Rightarrow} ExcludeList + (NextHop - ID_i) \\
&\overset{(7.1)}{\Rightarrow} 1 + (n-1) * (N_{max} - 2) + (NextHop - ID_i) \\
&\overset{(7.5)}{\Rightarrow} 1 + (n-1) * (N_{max} - 2) + (N_{max} - 1 - ID_i) \\
&= 1 + (R_{max} - 1) * (N_{max} - 2)
\end{aligned}
$$

Ο πίνακας 7.2 παρουσιάζει την ανάπτυξη των μηνυμάτων σε σχέση με τον αριθμό των μελών που περιέχονται σε καθεμια από τις λίστες των τριών πρωτοκόλλων πολλαπλών μονοπατιών. Τα αποτελέσματα έχουν εξαχθεί για μέγιστο αριθμό κόμβων ίσο με πέντε ($R_{max} = 5$) και για μια μέση μέγιστη πυκνότητα σύνδεσης ανάμεσα στους κόμβους του δικτύου, επίσης ίση με 5 ($N_{max} = 5$).

Το πρωτόκολλο SecMR καταφέρνει να ελέγξει το μέγεθος των μηνυμάτων που δημιουργούνται κατά τη διάρκεια εφαρμογής του, αφού καταφέρνει να

υπολογίσει τη μέγιστη τιμή στην οποία μπορεί να φτάσουν οι λίστες οι οποίες μεταφέρονται. Το SRP παράγει μικρότερα μηνύματα αφού χρησιμοποιεί μόνο μια λίστα. Στην αντίθετη πλευρά βρίσκεται το πρωτόκολλο Multipath, το οποίο αντιμετωπίζει τον κίνδυνο τα μηνύματά του να γίνουν υπερβολικά μεγάλα σε μέγεθος, αφού οι λίστες αναπτύσσονται γραμμικά και με βαθμό μεγαλύτερο από ότι στο SecMR.

7.1.2 Μοντελοποίηση

Η μελέτη μας περιλαμβάνει τη σύγκριση ανάμεσα σε τρία πρωτόκολλα πολλαπλών μονοπατιών το SRP [18], το Multipath[3] και το SecMR. Το περιβάλλον της προσομοίωσης αναπτύχθηκε χρησιμοποιώντας τη βιβλιοθήκη NS. Το δίκτυο που προσομοιώθηκε περιλαμβάνει 50 κόμβους τοποθετημένους σε μια περιοχή $1500 \times 1000 m^2$ μέτρα. Κάθε κόμβος έχει ακτίνα διάδοσης 250 μέτρα και η χωρητικότητα του δικτύου είναι 2 Mb/s.

Στην μελέτη μας έχουν χρησιμοποιηθεί 10 πηγές παραγωγής δεδομένων που παράγουν CBR (constant bit rate) κίνηση. Κάθε πηγή παραγωγής δεδομένων εκπέμπει πακέτα δεδομένων συνεχώς μέχρι το τέλος της προσομοίωσης. Οι πηγές και οι προορισμοί έχουν επιλεχθεί τυχαία με βάση την ομοιόμορφη κατανομή.

Το μέγεθος των πακέτων δεδομένων έχει οριστεί στα 512 byte. Κάθε παράδειγμα που έχει προσομοιωθεί εκτελείται για χρόνο προσομοίωσης 350 sec. Χρησιμοποιήθηκε το IEEE 802.11 Distributed Coordination Function (DCF) ως πρωτόκολλο Πρόσβασης στο Μέσο (medium access control protocol).

Ο προορισμός των πακέτων δεδομένων, εάν είναι απαραίτητο, περιμένει για 5 δευτερόλεπτα. Ο χρόνος αυτός είναι απαραίτητος αφού πρέπει ο τελικός κόμβος πριν αρχίσει να υπολογίζει όλα τα μονοπάτια διακριτών κόμβων να βεβαιωθεί ότι έχουν φτάσει σε αυτόν όλα τα μηνύματα εύρεσης μονοπατιών, ανεξάρτητα από το δρόμο που έχουν ακολουθήσει. Στον κόμβο προορισμού

φτάνουν πακέτα των μηνυμάτων εύρεσης νέων μονοπατιών, τα οποία περιέχουν λίστες με κόμβους που μετέχουν, μοναδικά ο καθένας, σε κάθε μονοπάτι (μονοπάτια διακριτών κόμβων). Το γεγονός αυτό δεν εμποδίζει έναν κόμβο να μετέχει σε περισσότερα από ένα μονοπάτια, αρκεί να εμφανίζεται μόνο μια φορά ανά μονοπάτι. Στόχος ενός *ολοκληρωμένου* πρωτοκόλλου δρομολόγησης είναι να βρεθούν όλα τα υπάρχοντα μονοπάτια ανάμεσα σε έναν κόμβο-πηγή και σε έναν κόμβο-προορισμό. Για να το πετύχει αυτό ο κόμβος προορισμού θα πρέπει, αφενός μεν να περιμένει κάποιο χρονικό διάστημα πριν υπολογίσει το μέγιστο σύνολο μονοπατιών διακριτών κόμβων, αφετέρου δε να επιλέξει τα μονοπάτια με προσοχή ώστε να μην αποκλείσει άδικα κάποια από αυτά. Για την επιλογή των μονοπατιών αυτών λήφθηκε υπόψη το μέγεθος των μονοπατιών, καθώς και το ποσοστό της εμφάνισης ενός κόμβου στα μονοπάτια. Σε κάθε κόμβο αποδόθηκε ένας αριθμός που αντιπροσωπεύει τις εμφανίσεις του σε όλα τα μονοπάτια. Μετά σε κάθε μονοπάτι ορίστηκε, ως βάρος, το άθροισμα των εμφανίσεων όλων των κόμβων του. Με αυτό τον τρόπο τα μονοπάτια που είχαν λίγους κόμβους (hop count) βρέθηκαν να έχουν μικρό βάρος και να βρίσκονται στην κορυφή της λίστας με τα υποψήφια προς χρήση μονοπάτια. Στη συνέχεια επιλέχθηκαν τα μονοπάτια που διέθεταν κόμβους που δεν ήταν και τόσο ¨δημοφιλείς¨, μετείχαν δηλαδή σε ένα ή σε λίγα μονοπάτια κ.ο.κ. Με αυτό τον τρόπο ο προορισμός μπορεί γρήγορα και σχετικά απλά να υπολογίσει τα μονοπάτια που θα χρησιμοποιηθούν στην επικοινωνία. Είναι δυνατόν ο προορισμός, προκειμένου να επισπεύσει την επικοινωνία, να χρησιμοποιήσει το πρώτο μονοπάτι που θα φτάσει σε αυτόν και παράλληλα να κάνει τους παραπάνω υπολογισμούς, ώστε να υπάρξει όσο το δυνατόν μικρότερη καθυστέρηση.

Στη συνέχεια ο προορισμός δημιουργεί το μήνυμα απάντησης έτσι ώστε να ειδοποιήσει την πηγή για το ποιο μονοπάτι θα χρησιμοποιηθεί για τη μεταξύ τους επικοινωνία. Από αυτή τη μελέτη προέκυψε το φαινόμενο της αδικαιολό-

γητης απόρριψης των μηνυμάτων απάντησης από το εργαλείο προσομοίωσης (NS2). Ως αιτία απόρριψης ανακαλύφθηκε ότι ήταν ο τρόπος λειτουργίας του πρωτοκόλλου ARP (Address Resolution Protocol). Αυτή η παρατήρηση οδήγησε στο συμπέρασμα ότι ακόμα και αν λειτουργήσει άψογα ένα πρωτόκολλο δρομολόγησης, τουλάχιστο στη φάση της ανακάλυψης νέων μονοπατιών, κανείς δεν εξασφαλίζει ότι όλα τα μηνύματα απάντησης θα φτάσουν κάποτε στην πηγή. Το φαινόμενο αυτό είναι ανεξάρτητο από το πρωτόκολλο και εμφανίζεται στους αλγόριθμους εκείνους όπου ο προορισμός επιλέγει τα προς χρήση μονοπάτια επικοινωνίας και όχι ο κόμβος-πηγή, που εκπέμπει τα δεδομένα.

Το μήκος των χρησιμοποιηθέντων μονοπατιών καθορίζει και τον αριθμό των μηνυμάτων εύρεσης νέων μονοπατιών που επεξεργάζεται κάθε ενδιάμεσος κόμβος. Έτσι αν χρησιμοποιούνται μονοπάτια με μέγεθος όχι μεγαλύτερο από πέντε βήματα (hops), τότε κάθε ενδιάμεσος κόμβος θα πρέπει να επεξεργαστεί τουλάχιστον πέντε αντίτυπα του μηνύματος εύρεσης νέων μονοπατιών από ένα συγκεκριμένο κόμβο-πηγή προς ένα συγκεκριμένο κόμβο προορισμού. Τα αντίτυπα αυτά θα έχουν ταξιδέψει από διαφορετικούς δρόμους ώστε να φτάσουν στον ενδιάμεσο αυτό κόμβο, καθώς διαφορετικά δε θα είναι μονοπάτια διακριτών κόμβων.

Γεγονός, πάντως είναι πως σε δίκτυα με μεγάλη κινητικότητα η εύρεση μεγάλου αριθμού εναλλακτικών μονοπατιών επικοινωνίας δεν αποτελεί πρακτική λύση. Σε ένα δίκτυο με μεγάλη κινητικότητα αλλάζει γρήγορα η συσχέτιση μεταξύ των κόμβων, οπότε και τα δυνατά μονοπάτια επικοινωνίας. Ιδιαίτερα αν τα μονοπάτια αυτά πρέπει να διαθέτουν αυστηρά χαρακτηριστικά ασφάλειας, π.χ. ο άμεσα γειτονικός κόμβος που θα προωθήσει το μήνυμα εύρεσης νέων μονοπατιών να είναι ήδη πιστοποιημένος στον γειτονικό του ενδιάμεσο κόμβο.

Η συχνότητα πιστοποίησης των άμεσα γειτονικών κόμβων αποτελεί παράμετρο του συστήματος. Στα παρακάτω παραδείγματα ο χρόνος αυτός

έχει οριστεί ίσος με διάστημα 5 min και η συχνότητα δεν είναι ίδια για όλους κόμβους, καθώς διαφορετικά θα υπήρχαν στιγμές όπου όλοι οι κόμβοι του δικτύου θα προσπαθούσαν ταυτόχρονα να πιστοποιηθούν στους άμεσους γείτονές τους. Ως συνέπεια, εκείνες ακριβώς τις στιγμές όλα τα μηνύματα εύρεσης νέων μονοπατιών θα απορρίπτονταν μαζικά από όλους τους κόμβους. Η παράμετρος αυτή είναι αντιστρόφως ανάλογη με την κινητικότητα του δικτύου και ανάλογη με την αυστηρότητα των κανόνων ασφάλειας. Έτσι σε ένα δίκτυο με αυστηρούς κανόνες ασφάλειας και μεγάλη κινητικότητα η τιμή θα πρέπει να είναι μικρή, δηλαδή να πραγματοποιείται πιστοποίηση των γειτονικών κόμβων αρκετά συχνά.

Οι κόμβοι στην προσομοίωσή μας κινούνται σύμφωνα με το μοντέλο random way point. Στην αρχή της προσομοίωσης, κάθε κόμβος περιμένει ένα χρονικό διάστημα. Στη συνέχεια επιλέγει τυχαία και μετακινείται προς έναν προορισμό με ταχύτητα που κυμαίνεται ομοιόμορφα ανάμεσα στην τιμή 0 και σε μια μέγιστη τιμή. Όταν φτάσει στον προορισμό του ο κόμβος περιμένει για ένα χρονικό διάστημα και επαναλαμβάνει την παραπάνω περιγραφείσα διαδικασία μέχρι το τέλος της προσομοίωσης. Η ελάχιστη και η μέγιστη ταχύτητα είναι αντίστοιχα 0 και 20 μ/s και οι χρόνοι που ο κόμβος περιμένει στις θέσεις του είναι 0, 5, 10, 20, 30 και 40 sec. Το χρονικό διάστημα 0 sec ανταποκρίνεται σε συνεχή κίνηση του κόμβου και το χρονικό διάστημα των 40 sec ανταποκρίνεται στο χρόνο στον οποίο ο κόμβος μένει ακίνητος σε μια θέση.

Έχουν δημιουργηθεί ποικίλα σενάρια κίνησης με διαφορετικούς ρυθμούς παραγωγής δεδομένων. Για κάθε σενάριο κίνησης έχουν χρησιμοποιηθεί δέκα διαφορετικά μοντέλα κίνησης. Για την επιλογή των σεναρίων κίνησης λήφθηκε υπόψη η ταχύτητα καθώς και ο χρόνος στάσης που πραγματοποιεί ο κόμβος. Έτσι σε σενάρια κατά τα οποία οι κόμβοι κινούνται με μεγάλη ταχύτητα αλλά πραγματοποιούν και μεγάλα διαστήματα στάσης μεταξύ των κινήσεών

τους το δίκτυο αντιδρά σαν να ήταν στατικό και όχι κινητό. Αντίθετα σε σενάρια όπου οι κόμβοι κινούνταν με μικρή ταχύτητα, αλλά είχαν και μικρά διαστήματα παύσεων μεταξύ των κινήσεών τους το δίκτυο αντιδρά σαν υψηλά κινητικό, π.χ. το σύνολο των άμεσων γειτόνων ενός κόμβου αλλάζει πολύ συχνά. Οπότε για τη μελέτη ενός κινητού δικτύου δεν είναι σημαντική μόνο η ταχύτητα με την οποία κινούνται οι κόμβοι αλλά και ο χρόνος στάσης που πραγματοποιούν.

Έχει χρησιμοποιηθεί ένα μοντέλο διάδοσης ελεύθερης διάδοσης σήματος (free space) με ελάχιστη τιμή. Στο μοντέλο ραδιοκυμμάτων, υποτέθηκε ότι ο κόμβος μπορεί να κλειδώνει (radio capture) σ' ένα ικανοποιητικά δυνατό σήμα για την περίπτωση όπου υπάρχουν παρεμβολές στο σήμα.

Για να επιτευχθεί η βέλτιστη μελέτη της επίδοσης των ανωτέρω πρωτοκόλλων επιλέχθηκε η μελέτη να πραγματοποιηθεί με βάση τα παρακάτω χαρακτηριστικά:

Μέση καθυστέρηση από άκρο σε άκρο (*Average end-to-end delay or mean overall packet latency*): Αποτελεί τη μέση καθυστέρηση που αντιλαμβάνεται ένα πακέτο από τη στιγμή που θα φύγει από τον αρχικό κόμβο έως την ορθή παραλαβή του από τον τερματικό κόμβο.

Χρόνος Εντοπισμού προορισμού (*Destination location time*): Είναι ο μέσος χρόνος που χρειάζεται ένα μήνυμα εύρεσης μονοπατιών να φτάσει στον τερματικό κόμβο (προορισμό).

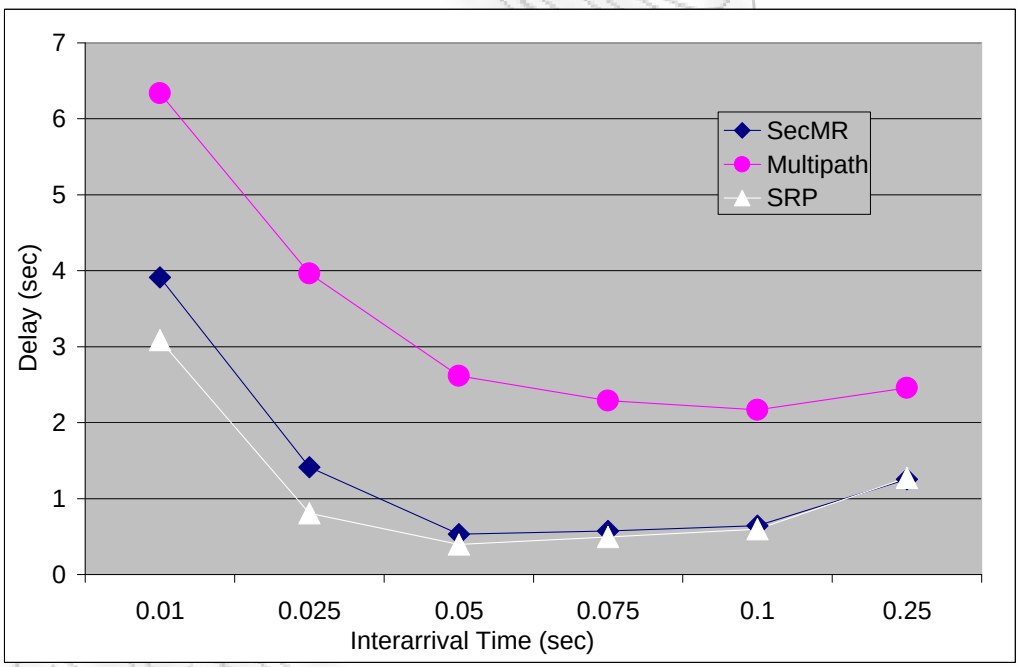
Χρόνος Διάδοσης αίτησης (*Request Propagation Time*): Αντιστοιχεί στον μέσο ολικό χρόνο που χρειάζεται ένα μήνυμα εύρεσης δρομολογίων ώστε να διαδοθεί σε όλο το δίκτυο. Αποτελεί ένα βασικό χαρακτηριστικό καθώς περιγράφει το φόρτο που επιβάλλει η διαδικασία εύρεσης δρομολογίων στη λειτουργία του δικτύου. Σε συσχέτιση με το χαρακτηριστικό *Χρόνος Εντοπισμού προορισμού*, περιγράφει το χρόνο που συνεχίζει να κυκλο-

φορεί/μεταναστεύει σε όλο το δίκτυο ένα μήνυμα εύρεσης δρομολογίων και άρα να καταναλώνει πόρους από το σύστημα, χωρίς αυτό να είναι απαραίτητο, αφού δεν προσθέτει κάτι στην εν γένει λειτουργία του πρωτοκόλλου δρομολόγησης.

Ποσοστό απόρριψης πακέτων (*Drop percentage*): Ορίζεται ως το ποσοστό των πακέτων που απορρίπτονται για διάφορους λόγους.

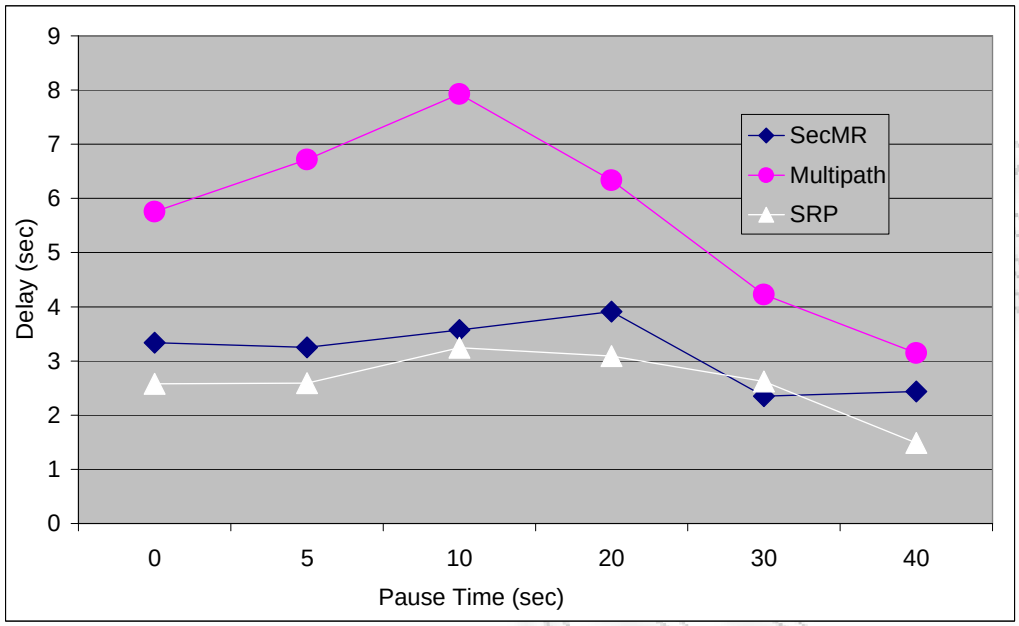
Φορτίο διαπερατότητας δρομολόγησης (*Routing throughput*): Περιγράφει την παραγωγή των πακέτων ελέγχου ολόκληρου του δικτύου ομαλοποιημένο ως προς τον αριθμό των κόμβων του δικτύου.

7.1.3 Παρουσίαση Αποτελεσμάτων



Εικόνα 7.2: *Μέση καθυστέρηση από άκρο-σε-άκρο πακέτων δεδομένων ανά μεσοδιάστημα παραγωγής πακέτων*

Η εικόνα 7.2 δείχνει το μέσο χρόνο καθυστέρησης των λαμβανομένων πακέτων δεδομένων σε σχέση με το χρόνο που μεσολαβεί ανάμεσα στην εκπομπή

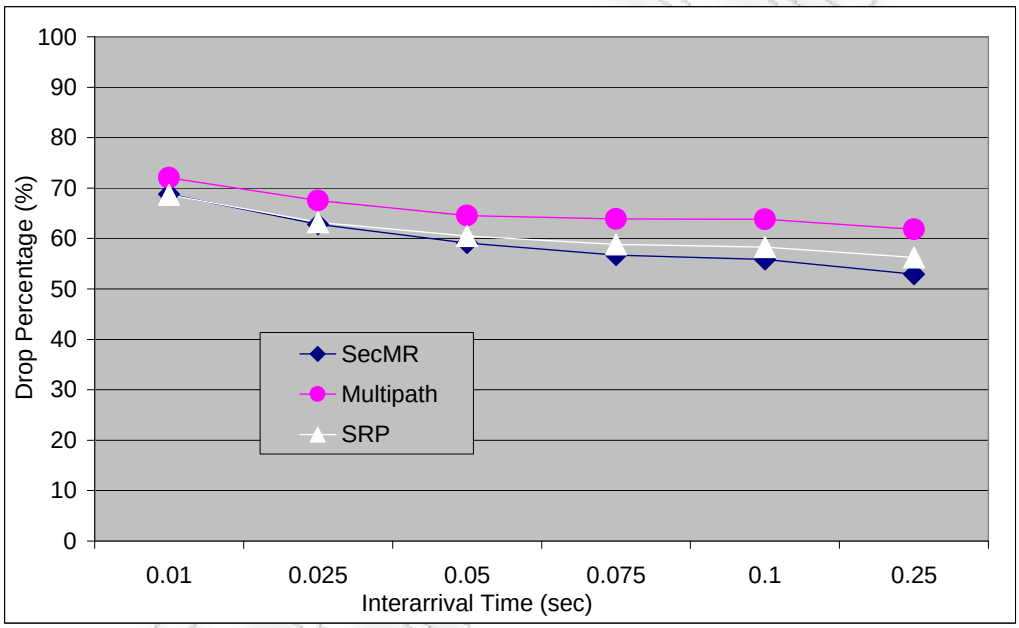


Εικόνα 7.3: *Μέση καθυστέρηση από άκρο-σε-άκρο πακέτων δεδομένων ανά χρόνο στάθμευσης*

δύο πακέτων, με χρόνο στάσης του κόμβου ίσο με 20 δευτερόλεπτα. Από τα αποτελέσματα μπορεί να παρατηρηθεί ότι τα πρωτόκολλα SRP και SecMR λειτουργούν καλύτερα από το πρωτόκολλο Multipath ακόμα και όταν ο ενδιάμεσος χρόνος είναι μικρός, το οποίο υποδηλώνει συνθήκες αυξημένης παραγωγής δεδομένων. Και στα δύο πρωτόκολλα, SRP και SecMR, ο αριθμός των νέων μηνυμάτων κατά τη διαδικασία ανακάλυψης νέων μονοπατιών έχει διατηρηθεί σε ικανοποιητικά χαμηλά επίπεδα ενώ στο πρωτόκολλο Multipath τείνει να πλημμυρίσει το δίκτυο. Αυτό συμβαίνει γιατί στο πρωτόκολλο Multipath, κάθε ενδιάμεσος κόμβος προωθεί όλα τα αντίγραφα της αίτησης εύρεσης νέων μονοπατιών που φτάνουν σε αυτόν από μια συγκεκριμένη πηγή προς ένα συγκεκριμένο προορισμό (της ίδιας ακολουθίας μηνυμάτων sequence number), ενώ το πρωτόκολλο SRP προωθεί μονάχα το πρώτο αντίγραφο που θα φτάσει στον κάθε ενδιάμεσο κόμβο και το SecMR επιχειρεί μια επιλεκτική προώθηση με τη χρήση της λίστας ExcludeList. Αυτή η πλημμύρα του

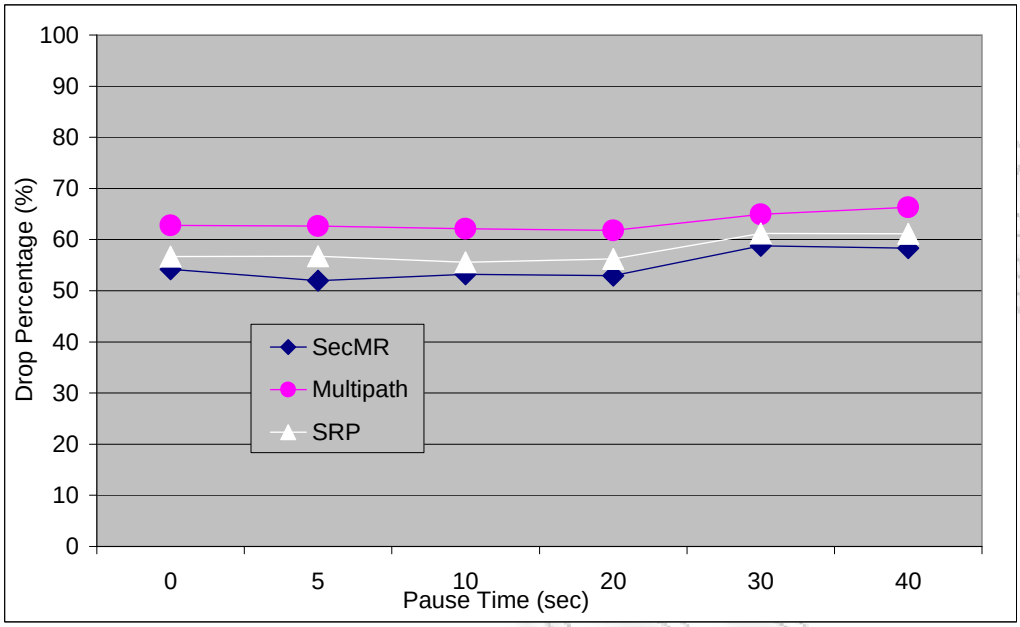
δικτύου έχει ως αποτέλεσμα τη δημιουργία μεγαλύτερης καθυστέρησης στην παράδοση των πακέτων δεδομένων.

Η Εικόνα 7.3 που παρουσιάζει τη μέση καθυστέρηση των λαμβανομένων πακέτων δεδομένων σε ένα δίκτυο που παράγει 100 πακέτα δεδομένων το δευτερόλεπτο ανά χρόνο στάθμευσης, ενισχύει την παραπάνω παρατήρηση. Πράγματι, όπως φαίνεται, τα πρωτόκολλα SRP και SecMR καταφέρνουν να αντιμετωπίσουν συνθήκες υψηλής κινητικότητας καλύτερα, παρ' όλο που με μεγαλύτερο χρόνο στάθμευσης η συμπεριφορά του πρωτοκόλλου Multipath τείνει να ανέλθει στα επίπεδα επίδοσης των δύο άλλων πρωτοκόλλων.



Εικόνα 7.4: *Ποσοστό απόρριψης πακέτων δεδομένων ανά μεσοδιάστημα παραγωγής πακέτων*

Η εικόνα 7.4 παρουσιάζει το ποσοστό απόρριψης πακέτων δεδομένων σε σχέση με το μεσοδιάστημα παραγωγής πακέτων και για χρόνο στάσης 20 δευτερολέπτων. Και τα τρία πρωτόκολλα παρουσιάζουν συγκρίσιμη επίδοση. Όλα τα πρωτόκολλα καταφέρνουν να απορρίπτουν λιγότερα πακέτα, ιδιαίτερα για όσο μεγαλώνει ο χρόνος μεσολάβησης. Το παρατηρούμενο υψηλό ποσοστό απόρριψης πακέτων που παρουσιάζουν και τα τρία πρωτόκολλα ο-



Εικόνα 7.5: *Ποσοστό απόρριψης πακέτων δεδομένων ανά χρόνο στάθμευσης*

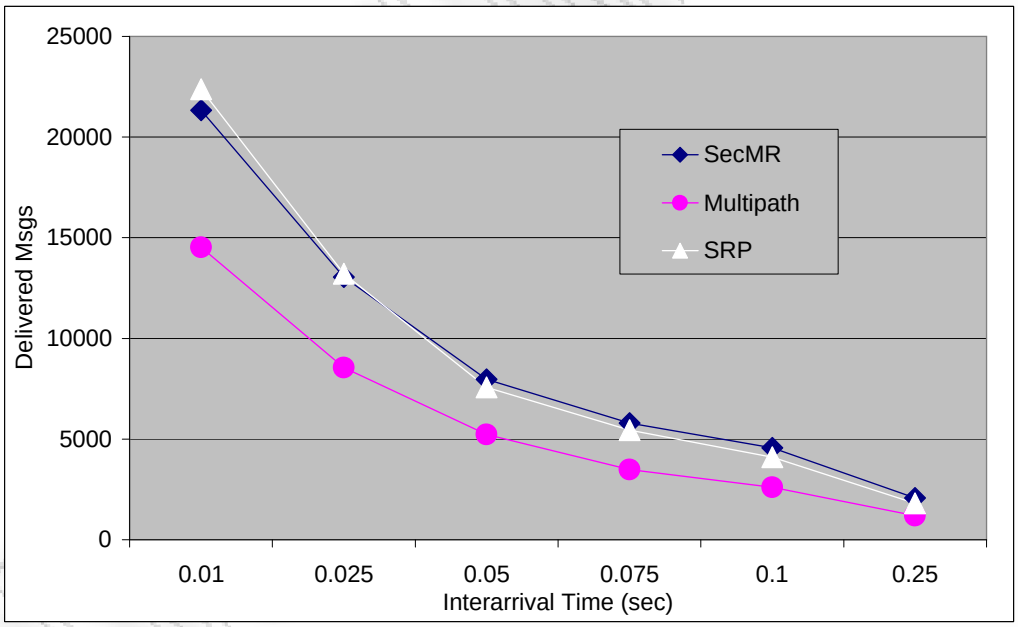
φείλεται κυρίως στην παραμετροποίηση/αρχικοποίηση της προσομοίωσης, και ιδιαίτερα στο χρονικό διάστημα κατά το οποίο τα μονοπάτια που περιέχονται στους πίνακες δρομολόγησης των κόμβων παραμένουν ενεργά. Εντούτοις το πρωτόκολλο Multipath παρουσιάζει το υψηλότερο ποσοστό σε σχέση με τα άλλα δύο. Το γεγονός αυτό αποτελεί ένδειξη ότι, ίσως, η εφαρμογή του σε μικρής κινητικότητας δίκτυο είναι αποτελεσματικότερη. Ωστόσο, για το SecMR και το SRP το μοτίβο επίδοσης είναι ενδεικτικό για την καλύτερη επίδοση των πρωτοκόλλων.

Η εικόνα 7.5 παρουσιάζει το ποσοστό απόρριψης πακέτων δεδομένων για διάφορους χρόνους στάσης και για χρόνο διαμεσολάβηση 0,25 δευτερολέπτων. Όπως φαίνεται στην εικόνα 7.5 και τα τρία πρωτόκολλα καταφέρνουν να διατηρήσουν το μοτίβο απόρριψης πακέτων ακόμα και κάτω από συνθήκες υψηλής κινητικότητας.

Ο αριθμός των πακέτων που λαμβάνονται ορθά από τον κόμβο προορισμού σε σχέση με τον χρόνο διαμεσολάβησης και για χρόνο στάσης 20

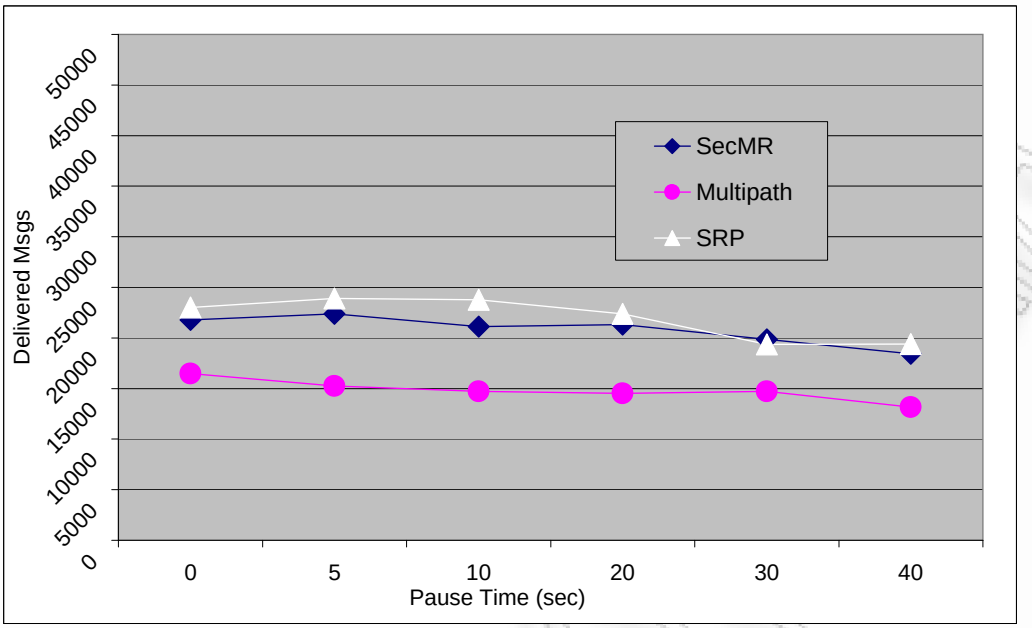
δευτερολέπτων παρουσιάζεται στην εικόνα 7.6. Η επίδοση και των τριών πρωτοκόλλων είναι ίδια όταν ο χρόνος διαμεσολάβησης μεγαλώνει, και αυτό ισχύει διότι σε αυτή την περίπτωση το δίκτυο αντιμετωπίζει συνθήκες χαμηλής κινητικότητας.

Όπως μπορεί κάποιος να δει τα πρωτόκολλα SecMR και SRP καταφέρνουν να εξυπηρετήσουν περισσότερα πακέτα σε σχέση με το πρωτόκολλο Multipath. Αυτό οφείλεται κυρίως στο γεγονός ότι τα πακέτα δεδομένων στο πρωτόκολλο Multipath αντιμετωπίζουν μεγαλύτερες καθυστερήσεις κατά τη διάρκεια διάδοσης της αίτησης εύρεσης νέων μονοπατιών και υψηλότερο βαθμό απόρριψης. Και τα τρία πρωτόκολλα καταφέρουν να διατηρήσουν τη συμπεριφορά τους σε σχέση με το βαθμό ορθής παράδοσης πακέτων κάτω από ποικίλες συνθήκες κινητικότητας όπως φαίνεται στην εικόνα 7.7, η οποία παρουσιάζει τη συμπεριφορά των πρωτοκόλλων με χρονικό μεσοδιάστημα 0,01 δευτερόλεπτα στην εκπομπή πακέτων δεδομένων.



Εικόνα 7.6: *Ο αριθμός των πακέτων δεδομένων που έχουν παραδοθεί ορθά ανά μεσοδιάστημα παραγωγής πακέτων δεδομένων*

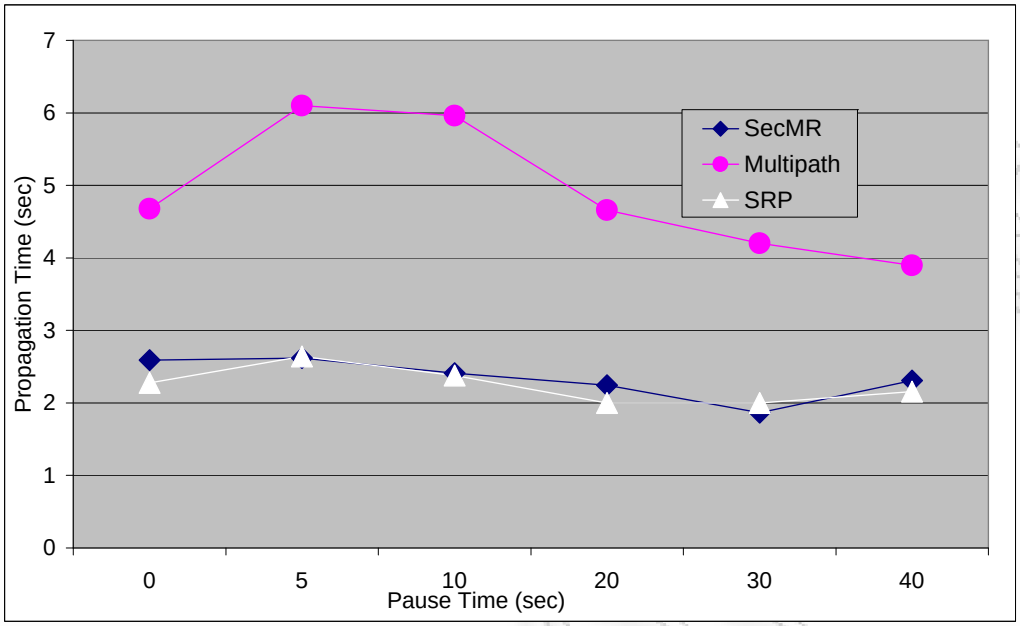
Η εικόνα 7.8 παρουσιάζει το μέσο συνολικό χρόνο κατά τον οποίο ένα



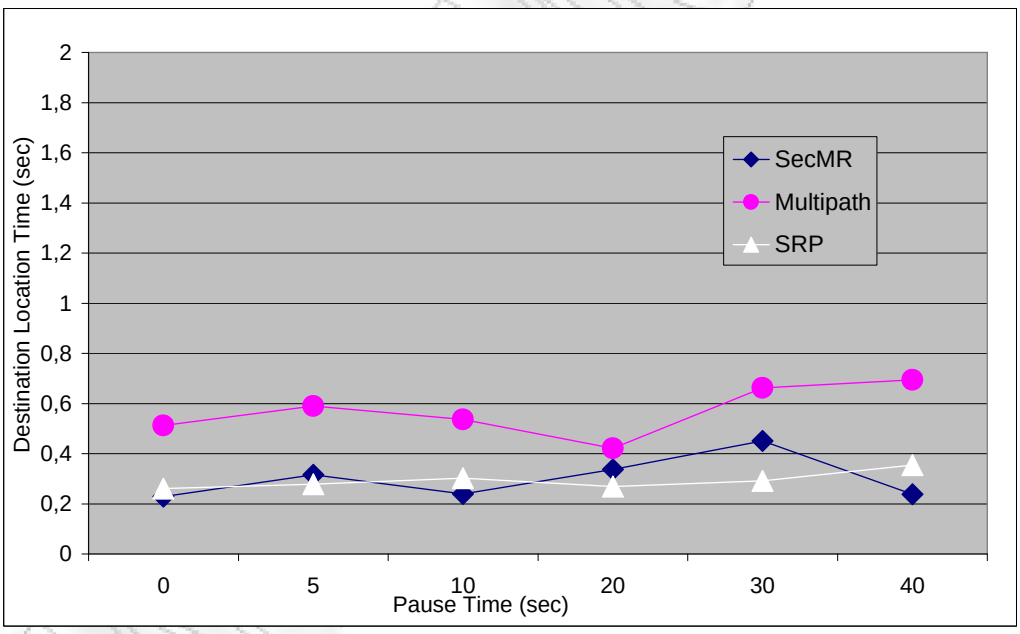
Εικόνα 7.7: *Ο αριθμός των πακέτων δεδομένων που έχουν παραδοθεί ορθά ανά χρόνο στάσης*

μήνυμα εύρεσης δρομολογίων συνεχίζει να διαδίδεται στους κόμβους του δικτύου. Στο Multipath όσο οι κόμβοι γίνονται όλο και πιο στάσιμοι τόσο και πιο πολύ ο χρόνος διάδοσης τείνει να γίνει συντομότερος, προσεγγίζοντας ένα κατώτερο όριο. Αυτό δε φαίνεται να ισχύει στο SecMR όπου η χρήση της λίστας *ExcludeList* αποτρέπει τη διάδοση των μηνυμάτων σε κόμβους που τα έχουν λάβει έστω και μια φορά στο παρελθόν. Στην περίπτωση του SRP το πρωτόκολλο εκμεταλλεύεται το γεγονός ότι κάθε ενδιάμεσος κόμβος προωθεί μόνον ένα μήνυμα της αλληλουχίας μηνυμάτων εύρεσης νέων μονοπατιών ανάμεσα σε μια πηγή και ένα προορισμό, παρουσιάζοντας έτσι χαμηλούς χρόνους καθυστέρησης.

Η εικόνα 7.9 παρουσιάζει το μέσο χρόνο που χρειάζεται ένα μήνυμα αίτησης να φτάσει στον κόμβο προορισμού του για πρώτη φορά. Εάν η εικόνα 7.9 συνδυαστεί με την εικόνα 7.8, είναι προφανές ότι στο πρωτόκολλο Multipath τα μηνύματα αίτησης συνεχίζουν να υπάρχουν μέσα στο δίκτυο μεγαλύτερο χρονικό διάστημα από ότι στα άλλα πρωτόκολλα, το οποίο προκαλεί μια



Εικόνα 7.8: *Χρόνος διάδοσης ανά χρόνο στάσης*



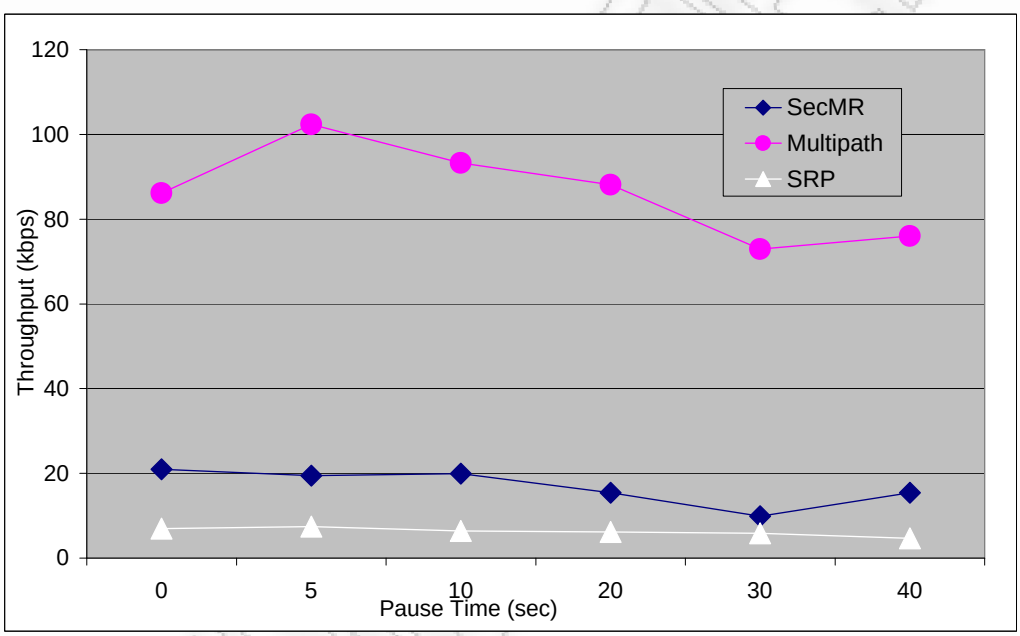
Εικόνα 7.9: *Πρώτη εύρεση προορισμού ανά χρόνο στάσης*

πτώση της επίδοσης του δικτύου. Στο ασφαλές πρωτόκολλο Multipath, ένα μήνυμα αίτησης ταξιδεύει για μεγαλύτερο χρονικό διάστημα από ό,τι στα άλλα δύο πρωτόκολλα, αφού το μήνυμα αίτησης προωθείται σε όλους τους

κόμβους του δικτύου, πολλοί από τους οποίους δεν θα περιλαμβάνονται στα μονοπάτια επικοινωνίας που θα χρησιμοποιηθούν τελικά.

Τα μηνύματα αίτησης του πρωτοκόλλου SRP διαδίδονται από τον κόμβο-πηγή στον κόμβο-προορισμού γρηγορότερα από ό,τι στα άλλα δύο πρωτόκολλα, αφού το πρωτόκολλο SRP απορρίπτει κάθε αντίγραφο αυτής της αίτησης. Η αίτηση ανεύρεσης *νέων* μονοπατιών του πρωτοκόλλου SecMR έχει ελαφρά μεγαλύτερο χρόνος ζωής έναντι του πρωτοκόλλου SRP. Αυτό είναι λογικό αφού το πρωτόκολλο SecMR επιχειρεί να ανακαλύψει όλα τα υπάρχοντα μονοπάτια μοναδικών κόμβων. Επιπλέον, το πρωτόκολλο SecMR έχει ως αποτέλεσμα, όλοι οι γειτονικοί κόμβοι να έχουν συνδεθεί/συνεισφέρει στην εύρεση μονοπατιών δρομολόγησης, είτε συμμετέχοντας στη λίστα (π.χ. στο μονοπάτι δρομολόγησης) είτε αποφεύγοντας να επεξεργαστούν το ίδιο αντίγραφο της αίτησης (π.χ. με τη συμμετοχή του στη λίστα). Το παραπάνω παρουσιάζεται στην εικόνα 7.10, η οποία παρουσιάζει το ολικό φορτίο δικτύου που δημιουργούν τα μηνύματα ελέγχου κανονικοποιημένο με τον ολικό αριθμό των κόμβων του δικτύου, για διαφορετικούς χρόνους στάσης και για χρόνο διαμεσολάβησης ίσο με 0,01 δευτερόλεπτα.

Το SRP φαίνεται να παράγει λιγότερα μηνύματα ελέγχου σε σχέση με τα άλλα δύο πρωτόκολλα, όπως φαίνεται στην εικόνα 7.10. Στο πρωτόκολλο SecMR το φορτίο που θα υποστεί το δίκτυο από τα μηνύματα ελέγχου είναι ελαφρώς αυξημένο, λόγω του ότι κάνει επιλεκτική προώθηση των μηνυμάτων αιτήσεων. Το πρωτόκολλο Multipath παρουσιάζει τη χειρότερη επίδοση σε σχέση με τα άλλα δύο, κάτι το οποίο σχετίζεται άμεσα με τον αριθμό των προωθήσεων που πραγματοποιεί.



Εικόνα 7.10: *Παραγωγή πακέτων ελέγχου ανά χρόνο στάσης*

Βιβλιογραφία

[1] Mavropodi R., Kotzanikolaou P., Douligeris C., *SecMR - a SECure Multipath routing Protocol for ad hoc networks*, Ad Hoc Networks, (Elsevier - In Press - Available online 28 June 2006).

[2] Mavropodi R., Douligeris C., *Multipath Routing protocols for Mobile Ad Hoc Networks: Security Issues and Performance Evaluation*, WAC 2005, LNCS, volume 3854, Springer-Verlag, p 165-176, 2006

[3] Kotzanikolaou P., Mavropodi R., Douligeris C., *Secure Multipath Routing for Mobile Ad Hoc Networks*, WONS 2005, St. Moritz, Switzerland, January 19-21, 2005

[4] Mavropodi R., Kotzanikolaou P., Douligeris C., *Performance Analysis of Secure Multipath Routing Protocols for Mobile Ad Hoc Networks*, WWIC 2005, LNCS, volume 3510, Springer-Verlag, p 269-278, 2005

Κεφάλαιο 8

Συμπεράσματα και Ανοικτά Θέματα προς Συζήτηση

Σε αυτό το κεφάλαιο παρουσιάζονται τα γενικά συμπεράσματα που προκύπτουν από τα θέματα που εξετάσθηκαν στην παρούσα διατριβή, ενώ επίσης παρουσιάζονται ορισμένα ανοικτά ερευνητικά προβλήματα.

8.1 Συμπεράσματα και ερευνητικά Θέματα γύρω από τα DIN

Η βασική ιδέα των κατανεμημένων ευρυζωνικών δικτύων είναι ο διαχωρισμός του ελέγχου της κλήσης από τη λογική εκτέλεσης της υπηρεσίας ευφυούς δικτύου και η μετατόπισή της εκτός του δρομολογητή. Η λογική της υπηρεσίας ευφυούς δικτύου υλοποιείται με τη μορφή κινητών αντιπροσώπων (SLP) και μπορεί να μεταναστεύει και να εκτελείται σε κόμβους του δικτύου που βρίσκονται πλησιέστερα στο χρήστη.

Στα πλαίσια αυτής της διατριβής προτάθηκε μια ασφαλή αρχιτεκτονική Ευφυών Δικτύων, η οποία εφαρμόζεται στο ανώτερο επίπεδο των κατανεμημένων ευρυζωνικών Ευφυών Δικτύων. Από τη στιγμή που η αρχιτεκτο-

νική των κατανεμημένων ευρυζωνικών Ευφυών δικτύων είναι βασισμένη στις τεχνολογίες CORBA και Grasshopper ως πλατφόρμα πρακτόρων, το μοντέλο ασφάλειας εξαρτάται από τα μοντέλα CORBA Security Service και το Grasshopper Security Service. Επιπλέον, στην παρούσα διατριβή χρησιμοποιήθηκαν και άλλοι μηχανισμοί ασφάλειας μη-CORBA, όπως Trusted Third Party Services. Τέλος μελετήθηκε η επίδοση της συγκεκριμένης αρχιτεκτονικής και πώς επηρεάζεται η συμπεριφορά του δικτύου με την εφαρμογή πρόσθετων μηχανισμών ασφάλειας.

Η συγκεκριμένη αρχιτεκτονική επικεντρώνεται στις εφαρμογές IMR. Ωστόσο, η προτεινόμενη αρχιτεκτονική του ΕΔ μπορεί, με σχετική ευκολία, να τροποποιηθεί και να εφαρμοστεί σε πολλές και διαφορετικές εφαρμογές. Για παράδειγμα, εάν η εφαρμογή απαιτεί μια πιο ευέλικτη πολιτική ασφάλειας, είναι δυνατόν να δημιουργηθεί μια ιεραρχία μεγαλύτερου βαθμού με τη χρήση των PAC, η οποία κατηγοριοποιεί περαιτέρω την εξουσιοδότηση σε υπηρεσίες και πόρους. Το ίδιο ισχύει και για την πολιτική εξουσιοδότησης. Εάν μια εφαρμογή απαιτεί ένα πιο πολύπλοκο σχήμα, η χρήση του πρωτοκόλλου CSI-ECMA σε συνδυασμό με τη χρήση της μεθόδου PC/VC μπορεί να δημιουργήσει αυτού του είδους την εξουσιοδότηση.

Σε αυτό το μοντέλο καμιά υπηρεσία δε χρησιμοποιείται για μη αποποίησης ευθύνης (non-repudiation). Εάν αυτό είναι απαραίτητο τότε μπορεί να χρησιμοποιηθεί η υπηρεσία non-repudiation της CORBA. Η υπηρεσία περιλαμβάνει ψηφιακές υπογραφές και/ή αξιόπιστη υπηρεσία παράδοσης. Ωστόσο, κάθε χρήστης θα πρέπει να πιστοποιεί ένα ζεύγος κλειδιών (δημόσιων και ιδιωτικών) για την κρυπτογράφηση και ένα διαφορετικό ζεύγος για τη χρήση του στις υπογραφές. Η χρήση διαφορετικού ζεύγους κλειδιών απαιτείται ώστε να προστατευτεί η ασφάλεια του κρυπτογραφικού συστήματος.

Η επικοινωνία μεταξύ των κόμβων του ιδίου επιπέδου αποτελεί άλλη μια επεκτάσιμη ιδιότητα. Ενώ στην υπάρχουσα ανάπτυξη η επικοινωνία μεταξύ

διαφορετικών κόμβων του ιδίου επιπέδου δεν απαιτείται, είναι σχετικά εύκολο να δημιουργηθούν ασφαλή μονοπάτια για την επικοινωνία αυτού του είδους. Για παράδειγμα, εάν η λειτουργική οντότητα B-SSF του κόμβου B-SSCP λειτουργεί κάτω από συνθήκες βαρέως φορτίου, τότε είναι δυνατόν να εξουσιοδοτήσει τα PAC ενός χρήστη στη λειτουργική οντότητα B-SSF ενός άλλου κόμβου B-SSCP μέσω μιας ελεγχόμενης εξουσιοδότησης. Η επικοινωνία ανάμεσα σε διαφορετικούς κόμβους B-SEN μπορεί να πραγματοποιηθεί μέσω της ασφαλούς μετανάστευσης πρακτόρων. Για παράδειγμα, ένας πράκτορας πρώτης γενιάς μεταναστεύει σε κάποιον κόμβο B-SEN μέσω ενός ασφαλούς Grasshopper μονοπατιού μετανάστευσης.

Όπως έχει αναφερθεί στο κεφάλαιο 4, παρόλο που η ύπαρξη υπηρεσιών ασφάλειας στο ανώτερο επίπεδο της αρχιτεκτονικής των κατανεμημένων ευφυών δικτύων έχει σαν αποτέλεσμα τη μείωση της επίδοσης του συστήματος, η αποτελεσματικότητα της προτεινόμενης αρχιτεκτονικής εξαρτάται από τις τιμές των ρυθμίσεων των πολιτικών του δικτύου και της ασφάλειας. Σύμφωνα με τα παραπάνω είναι υπό σκέψη η επέκταση της ανάλυσης της αποδοτικότητας της ασφαλούς αρχιτεκτονικής των κατανεμημένων ευφυών δικτύων σε δίκτυα με ρυθμίσεις όπως: κατανομή επιπρόσθετης επεξεργαστικής ισχύος σε κόμβους που στα γραφήματα επίδοσης παρουσιάζονται κορεσμένοι, εξέταση των κατάλληλων τύπων υπηρεσιών που θα εκτελεστούν στις οντότητες που φιλοξενούνται στον κόμβο B-SSCP. Επιπλέον, μελετάται η εφαρμογή ενός συνδυασμού των ανωτέρω ρυθμίσεων με πολιτικές ασφάλειας όπως, με τη μείωση του μεγέθους των κλειδιών κρυπτογράφησης που χρησιμοποιούνται στη προστασία των μηνυμάτων και τον έλεγχο των πιστοποιητικών. Για το σκοπό αυτό στην πολιτική του δικτύου θα πρέπει να επιλεγεί ο κατάλληλος αριθμός και τύπος των υπηρεσιών που θα εφαρμοστούν στους κόμβους χαμηλού επιπέδου (B-SSCP). Επιπρόσθετα, αφού η επίδοση του δικτύου στην ασφαλή αρχιτεκτονική δεν παρουσιάζει καμιά μεγάλη διαφορά ανάμεσα στην περί-

πτωση όπου η εξυπηρέτηση των εφαρμογών γίνεται από τον κόμβο B-SEN και την περίπτωση όπου η εξυπηρέτηση πραγματοποιείται από τον κόμβο B-SSCP, είναι προτιμότερο να πραγματοποιείται από τον κόμβο B-SEN. Οι εφαρμογές που θα εξυπηρετούνται από τον κόμβο B-SSCP θα πρέπει να είναι όσο το δυνατόν λιγότερες και η επιβάρυνση που θα επιφέρουν στον κόμβο και το δίκτυο να είναι η ελάχιστη δυνατή.

Η μετατόπιση και η εκτέλεση της λογικής της υπηρεσίας πλησιέστερα στο χρήστη, κάτω από συνθήκες αυξημένης ζήτησης, έχει ως αποτέλεσμα την αποσυμφόρηση τμημάτων του δικτύου και τη γρηγορότερη απόκριση στις αιτήσεις του χρήστη για εξυπηρέτηση. Παρόλα αυτά χρειάζεται προσοχή καθώς η μετανάστευση αυτή προκαλεί την επέμβαση και προσαρμογή σε πολυάριθμα τμήματα του δικτύου, ώστε να μπορεί να πραγματοποιηθεί η εκτέλεση της λογικής της υπηρεσίας.

Η επιλογή των κατάλληλων ρυθμίσεων τόσο για το δίκτυο όσο και για την εφαρμοζόμενη πολιτική θα πρέπει να γίνεται με σκοπό την εύρεση μιας χρυσής ισορροπίας ανάμεσα στην εφαρμογή ασφάλειας και την επίτευξή της αποτελεσματικότητας.

8.2 Συμπεράσματα και ερευνητικά Θέματα γύρω από τα Πρωτόκολλα Δρομολόγησης Δικτύων Ad Hoc

Ο χώρος των ασύρματων κινητών δικτύων έχει λάβει αυξημένη προσοχή α-πό τους ερευνητές τα τελευταία χρόνια, καθώς η ανάπτυξη της τεχνολογίας των ασύρματων δικτύων και των κινητών υπολογιστών έκαναν δυνατή την ανάπτυξη (και εισαγωγή αυτών στα ασύρματα κινητά δίκτυα) εφαρμογών υ-ψηλών απαιτήσεων. Η ασφάλεια σε τέτοια περιβάλλοντα αποτελεί ένα κρίσιμο χαρακτηριστικό. Οι τελευταίες έρευνες έχουν δημιουργήσει νέα πρωτόκολλα δρομολόγησης που στόχο έχουν να κάνουν τη δρομολόγηση σε ασύρματα

κινητά δίκτυα ασφαλέστερη. Ωστόσο δεν έχει ερευνηθεί αρκετά η επίδοση σε αυτά τα ασφαλή πρωτόκολλα δρομολόγησης πολλαπλών μονοπατιών.

Προτάθηκε ένα ασφαλές πρωτόκολλο πολλαπλών μονοπατιών το SecMR εφαρμόσιμο στα κινητά Ad Hoc δίκτυα. Αναλύθυηκαν αρκετά θέματα ασφάλειας που αφορούν τα πρωτόκολλα πολλαπλών μονοπατιών και ελέγχθηκαν τα χαρακτηριστικά ασφάλειας για το πρωτόκολλο SecMR.

Αναλύθηκαν τα χαρακτηριστικά επίδοσης και παρουσιάστηκαν αποτελέσματα μέσω προσομοίωσης του πρωτοκόλλου SecMR σε σχέση με άλλα πρωτόκολλα πολλαπλών μονοπατιών με παρόμοιες/συγκρίσιμες ιδιότητες ασφάλειας και συγκεκριμένα τα Multipath και SRP. Επιπλέον, μελετήθηκε η επίδοση των πρωτοκόλλων κάτω από διάφορες συνθήκες κινήσεις δεδομένων και κάτω από διαφορετικές συνθήκες κίνησης κόμβων. Τα αποτελέσματα της προσομοίωσης παρέχουν ικανοποιητικά αποτελέσματα για την επίδοση των υπό εξέταση πρωτοκόλλων δρομολόγησης πολλαπλών μονοπατιών. Η έρευνά μας έδειξε ότι το SRP έχει καλύτερη επίδοση σε σχέση με τα άλλα δύο πρωτόκολλα, το SecMR ακολουθεί σε μικρή απόσταση ενώ το Multipath φαίνεται να παρουσιάζει τη χειρότερη επίδοση για αλλά δύο.

Ωστόσο, όταν μελετάμε τα χαρακτηριστικά ασφάλειας των τριών αυτών πρωτοκόλλων η διαβάθμιση τους αλλάζει. Το Multipath πετυχαίνει τη μεγαλύτερη αντίσταση σε επιθέσεις άρνησης υπηρεσίας συνεργαζόμενων κακόβουλων κόμβων. Καταφέρνει να ανακαλύψει όλα τα υπάρχοντα μονοπάτια μοναδικών κόμβων που βρίσκονται ανάμεσα σε μια πηγή και έναν προορισμό και πιστοποιεί όλους τους ενδιάμεσους κόμβους σε κάθε μονοπάτι δρομολόγησης. Αυτά τα χαρακτηριστικά το κάνουν να βρίσκει εφαρμογή σε δίκτυα που έχουν ανάγκη ασφάλεια υψηλού επίπεδου, χαμηλής κινητικότητας, και η πυκνότητα αυτών των δικτύων διατηρείται σε χαμηλά ποσοστά. Σε τέτοια περιβάλλοντα το ρίσκο της υπερμεγέθους ανάπτυξης των μηνυμάτων αντισταθμίζεται με την κρισιμότητα που έχουν οι πληροφορίες που μεταφέρονται. Επιπλέον θα απο-

φευχθούν οι μεγάλες καθυστερήσεις, καθώς επίσης και η ανάπτυξη συνθηκών συμφόρησης δικτύων.

Το προτεινόμενο πρωτόκολλο SecMR πετυχαίνει να ανακαλύψει όλα τα μονοπάτια, ενός δεδομένου μήκους, μοναδικών κόμβων που υπάρχουν ανάμεσα σε μια πηγή και ένα προορισμό. Παρέχει, επίσης, ρητή πιστοποίηση των ενδιάμεσων κόμβων, από τη στιγμή που η πιστοποίηση πραγματοποιείται σε τακτά χρονικά διαστήματα. Σύμφωνα με αυτά τα χαρακτηριστικά βρίσκει εφαρμογή σε δίκτυα που απαιτούν υψηλή ασφάλεια στη δρομολόγηση των δεδομένων τους και των οποίων οι κόμβοι παρουσιάζουν μεσαία έως υψηλή πυκνότητα, καθώς και μεσαία κινητικότητα. Σε τέτοιες περιπτώσεις το πρωτόκολλο SecMR παρουσιάζει συγκρίσιμη επίδοση με το πρωτόκολλο SRP ενώ ταυτόχρονα παρέχει υψηλά επίπεδα ασφάλειας.

Τέλος το πρωτόκολλο SPR δεν καταφέρνει να βρει όλα τα μονοπάτια των κόμβων που υπάρχουν ανάμεσα σε μια πηγή και ένα προορισμό και παρέχει πιστοποίηση από άκρο σε άκρο. Η αυξημένη επίδοση του όσον αφορά την ικανότητα δρομολόγησης το κάνει εφαρμόσιμο σε δίκτυα με αυξημένη πυκνότητα κόμβων. Αυτό εξηγείται από το γεγονός ότι η διάδοση της αίτησης εύρεσης νέων μονοπατιών αποτυγχάνει να βρει όλα τα δυνατά μονοπάτια που υπάρχουν ανάμεσα στον κόμβο-πηγή και στον κόμβο προορισμού έτσι όμως η εκτέλεση του πρωτοκόλλου ολοκληρώνεται γρηγορότερα. Αυτό οδηγεί σε εύρεση ενός μέρους μόνο από το σύνολο υπαρχόντων μονοπατιών και μειώνει την αντίσταση του πρωτοκόλλου σε επιθέσεις άρνησης υπηρεσίας. Έτσι το πρωτόκολλο φαίνεται να βρίσκει εφαρμογή σε δίκτυα που έχουν ανάγκη μεσαία επίπεδα ασφάλειας.

Ενδιαφέρον παρουσιάζει η μελέτη της λειτουργίας του πρωτοκόλλου SecMR όταν η μεταφορά δεδομένων κατανέμεται σε περισσότερα μονοπάτια. Σε αυτήν την περίπτωση είναι σημαντικό να μελετηθεί η ανθεκτικότητα του πρωτοκόλλου σε αυξημένο αριθμό συνεργαζόμενων κόμβων. Βελτίωση της

επίδοσης του πρωτοκόλλου αποτελεί η επιλογή των/του μονοπατιών που θα χρησιμοποιηθούν (από το σύνολο των ανακαλυφθέντων) για τη μεταφορά των δεδομένων να πραγματοποιείται από τον κόμβο-πηγή και όχι από τον κόμβο-προορισμού. Η βελτίωση αυτή αναμένεται να επηρεάσει τη λειτουργία της δρομολόγησης και όχι τόσο τις ιδιότητες ασφάλειας που παρουσιάζει το πρωτόκολλο SecMR. Ένα άλλο θέμα ανοικτό προς συζήτηση, για το πρωτόκολλο SecMR, είναι η εξάρτησή του από τη διαθεσιμότητα της αρχής πιστοποίησης CA, κατά τη διάρκεια της φάσης της πιστοποίησης, του μηχανισμού δρομολόγησης. Παρόλο που η χρήση του κατανεμημένου PKI μπορεί να μειώσει αυτό το πρόβλημα, θα πρέπει να μελετηθεί η εφαρμογή του πρωτοκόλλου SecMR σε χρονικά διαστήματα όπου δε θα λειτουργεί η αρχή πιστοποίησης (CA). Καθώς τα ασύρματα κινητά δίκτυα παρουσιάζουν αδυναμία αντιμετώπισης του φαινομένου του αθέατου κόμβου και η χρήση της πιστοποίησης δεν αποτελεί δραστική λύση, η μελέτη της επίδοσης του πρωτοκόλλου SecMR σε αυτές τις περιπτώσεις αποτελεί αντικείμενο μελλοντικής έρευνας.

Γεγονός, πάντως είναι πως σε δίκτυα με μεγάλη κινητικότητα η εύρεση μεγάλου αριθμού εναλλακτικών μονοπατιών επικοινωνίας δεν αποτελεί πρακτική λύση. Σε ένα δίκτυο με μεγάλη κινητικότητα αλλάζει γρήγορα η συσχέτιση μεταξύ των κόμβων, οπότε και τα μονοπάτια επικοινωνίας. Ιδιαίτερα αν τα μονοπάτια αυτά πρέπει να διαθέτουν αυστηρά χαρακτηριστικά ασφάλειας, π.χ. ο άμεσα γειτονικός κόμβος που θα προωθήσει το μήνυμα εύρεσης νέων μονοπατιών να είναι ήδη πιστοποιημένος στον γειτονικό του ενδιάμεσο κόμβο.