Πανεπιστήμιο Πειραιώς
Τμήμα Διδακτικής της Τεχνολογίας και Ψηφιακών Συστημάτων

Ασφάλεια στα Ασύρματα Δίκτυα Αισθητήρων: Ανίχνευση Εισβολών με χρήση της Θεωρίας των Παιγνίων

Τζικόπουλος Παναγιώτης

Η εργασία υποβάλλεται για την μερική κάλυψη των απαιτήσεων με στόχο την απόκτηση του Μεταπτυχιακού Διπλώματος Σπουδών στα Δικτυοκεντρικά Συστήματα

Πειραιάς, Ιούνιος 2008

Αφιερώνεται στους γονείς μου

Ευχαριστίες

Εκφράζω θερμές ευχαριστίες στον Καθηγητή Σωκράτη Κάτσικα για την επίβλεψη και την αμέριστη και αδιάκοπη βοήθεια και συνεργασία που μου παρείχε, καθώς επίσης και στα μέλη της τριμελούς επιτροπής μου, Αναπληρωτή Καθηγητή Παναγιώτη Δεμέστιχα και Λέκτορα Χρήστο Ξενάκη, για τις παρατηρήσεις τους που αποτέλεσαν πολύτιμη συμβολή στην πτυχιακή αυτή εργασία. Τέλος, την Καθηγήτρια Εφαρμογών του ΤΕΙ Αθήνας Ιωάννα Καντζάβελου, για τις πολύτιμες οδηγίες και συμβουλές της.

Πρόλογος

Τα ασύρματα δίκτυα αισθητήρων (Wireless Sensor Networks - WSN) είναι μια σχετικά νέα τεχνολογία που διαφαίνεται ότι θα χρησιμοποιείται όλο και περισσότερο στο μέλλον λόγω των δυνατοτήτων που έχει στη συγκέντρωση στοιχείων και επεξεργασία δεδομένων. Η ασφάλεια των WSN είναι αναγκαίο να μελετηθεί περισσότερο, προκειμένου να προστατευθεί η λειτουργία αυτών των δικτύων. Είναι γεγονός πως τα πρότυπα & τα πρωτόκολλα ασφάλειας που χρησιμοποιούνται στα ενσύρματα και σε άλλα δίκτυα δεν ταιριάζουν στα WSN κυρίως λόγω των αυστηρά περιορισμένων πόρων τους.

Σε αυτή την εργασία, κατασκευάζουμε ένα μοντέλο ασφάλειας για τα ασύρματα δίκτυα αισθητήρων χρησιμοποιώντας τη θεωρία των παιγνίων. Συγκεκριμένα, ορίζουμε ένα παιχνίδι μεταξύ τριών παικτών, το οποίο και περιγράφουμε αναλυτικά. Στη συνέχεια, το επιλύουμε χρησιμοποιώντας τη μέθοδο της κυριαρχίας αλλά και ένα εργαλείο επίλυσης παιγνίων. Στο τέλος, δείχνουμε μέσα από μια μελέτη περίπτωσης, πως το μοντέλο μας βρίσκει εφαρμογή σε ένα πραγματικό σενάριο ασφάλειας ενός ασύρματου δικτύου αισθητήρων.

Κατάλογος Περιεχομένων

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Κατάλογος Συντομογραφιών

Συντομογραφία	*Επεξήγηση*
ACK	Acknowledgment Code
ADC	Analog to Digital Converter
CPU	Central Processing Unit
CTS	Clear To Send
DoS	Denial of Service
DSR	Dynamic Source Routing
EARS	Eavesdrop and Register
GoWiSeN	Game of Wireless Sensor Networks
GPS	Global Positioning System
IDS	Intrusion Detection System
LEACH	Low Energy Adaptive Clustering Hierarchy
MDP	Markov Decision Process
NE	Nash Equilibrium
RTS	Request To Send
RAM	Random Access Memory
SAR	Sequential Assignment Routing
SAR	Secure Auction based Routing
SMACS	Self-Organised Medium Access Control for Sensor Networks
SMECN	Small Minimum Energy Communication Network
SMP	Sensor Management Protocol
SPIN	Sensor Protocols for Information via Negotiation
SQDDP	Sensor Query and Data Dissemination Protocol
TADAP	Task Assignment and Data Advertisement Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UDSR	Utility based Dynamic Source Routing
WSN	Wireless Sensor Network

1 Εισαγωγή

1.1 Εισαγωγή

Οι πρόσφατες πρόοδοι στις ασύρματες επικοινωνίες και στην ανάπτυξη πολυσύνθετων αισθητήρων, οδήγησε στη γέννηση μιας νέας τεχνολογίας που ονομάζεται ασύρματα δίκτυα αισθητήρων. Το περιοδικό Business Week [Business, 1999] προχώρησε ακόμα περισσότερο έτσι ώστε να προσδιορίσει τη δικτύωση των ασύρματων αισθητήρων ως μια από τις 21 σημαντικότερες τεχνολογίες του 21ου αιώνα.

Ένα ασύρματο δίκτυο αισθητήρων ορίζεται απλά ως μια μεγάλη συλλογή κόμβων αισθητήρων που επικοινωνούν ασύρματα μεταξύ τους. Κάθε κόμβος εξοπλίζεται με τον αισθητήρα, τον επεξεργαστή και το ράδιο πομποδέκτη του. Τέτοια δίκτυα έχουν τις ικανότητες ανίχνευσης στοιχείων, συγκέντρωσης δεδομένων αλλά και επεξεργασίας δεδομένων. Για αυτόν το λόγο επεκτείνονται πυκνά σε μια περιοχή όπου επιθυμούμε να ελέγξουμε συγκεκριμένα φαινόμενα, όπως για παράδειγμα την ανίχνευση πυρκαγιάς.

Λόγω των περιορισμών σε πόρους που έχουν οι κόμβοι αισθητήρων, και τη μη ασφαλή φύση των ασύρματων καναλιών επικοινωνίας, αυτά τα δίκτυα είναι ευάλωτα στις εσωτερικές και εξωτερικές επιθέσεις. Έτσι για τους ερευνητές η παροχή ασφάλειας στα ασύρματα δίκτυα αισθητήρων αποτελεί μια μεγάλη πρόκληση. Οι συμβατικές μέθοδοι ασφάλειας, όπως οι κρυπτογραφικές τεχνικές που χρησιμοποιούνται σε άλλα δίκτυα, δε μπορούν να είναι επαρκείς για τα ασύρματα δίκτυα αισθητήρων.

Για την αντιμετώπιση του προβλήματος της ασφάλειας των ασύρματων δικτύων αισθητήρων, στη μελέτη αυτή θα ενσωματώσουμε στοιχεία από τη θεωρία των παιγνίων. Ειδικότερα, για το σκοπό αυτό θα κατασκευάσουμε ένα παίγνιο. Από την επίλυση του παιγνίου και τα συμπεράσματα που θα βγουν αναμένεται να αναδειχτούν προτάσεις που μπορούν να βελτιώσουν τα θέματα ασφάλειας ενός ασύρματου δικτύου αισθητήρων.

1.2 Διάρθρωση πτυχιακής

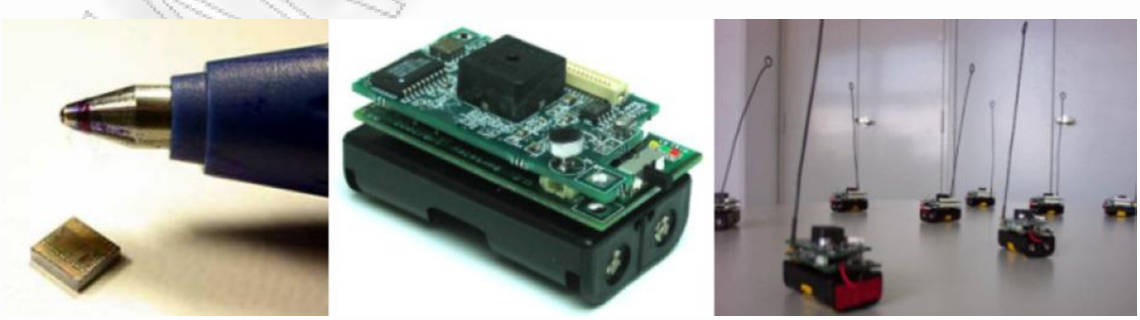
Η παρούσα εργασία είναι οργανωμένη σε οκτώ κεφάλαια, από τα οποία το πρώτο κεφάλαιο αποτελεί το εισαγωγικό κεφάλαιο της εργασίας, όπου περιγράφονται τα πεδία που καλύπτει αυτή η εργασία και η διάρθρωσης των περιεχομένων της. Στα επόμενα τρία κεφάλαια γίνεται η βιβλιογραφική επισκόπηση του θέματος. Το δεύτερο κεφαλαίο περιλαμβάνει μια επισκόπηση του θέματος των ασύρματων δικτύων αισθητήρων. Αναφέρεται δηλαδή σε θέματα όπως οι εφαρμογές, τα χαρακτηριστικά, τα πρωτόκολλα, η δομή, και η ασφάλεια των ασύρματων δικτύων αισθητήρων. Στο τρίτο κεφάλαιο παρουσιάζονται στοιχεία της θεωρίας των παιγνίων. Στο κεφάλαιο αυτό γίνεται μια ταξινόμηση των παιγνίων, παρουσιάζονται οι τρόποι περιγραφής των παιγνίων, ενώ στο τέλος υπάρχουν μεθοδολογίες για την επίλυση τους. Στο τέταρτο κεφάλαιο παρουσιάζονται τα συστήματα ανίχνευσης εισβολών και οι τεχνικές ανίχνευσης που χρησιμοποιούνται. Στο επόμενο κεφάλαιο γίνεται μια αναφορά σε όλες τις συναφείς με το θέμα εργασίες που έχουν γίνει μέχρι σήμερα, δηλαδή άλλες προσπάθειες προσέγγισης του θέματος ασφάλειας των WSN με χρήση της θεωρίας των παιγνίων. Το κεφάλαιο 6 περιλαμβάνει την κατασκευή ενός παιγνίου με σκοπό την ασφάλεια των δικτύων αισθητήρων. Γίνεται μια αναλυτική περιγραφή του παιγνίου, στη συνέχεια δημιουργούνται οι αποδόσεις για τον κάθε παίκτη και στο τέλος παρουσιάζεται η επίλυση του παιγνίου. Το κεφάλαιο 7 περιγράφει ένα case study για ένα πραγματικό σενάριο χρήσης των ασύρματων δικτύων αισθητήρων. Για την ασφάλεια του δικτύου ενσωματώνεται το παίγνιο που κατασκευάστηκε στο προηγούμενο κεφάλαιο. Στο τελευταίο κεφάλαιο, εκτίθενται τα συμπεράσματα της έρευνας μας. Αρχικά δίδεται η ανασκόπηση της εργασίας, στη συνέχεια συνάγονται τα συμπεράσματα και στο τέλος προτείνονται θέματα που χρήζουν περαιτέρω μελέτης.

2 Ασύρματα Δίκτυα Αισθητήρων

2.1 Εισαγωγή

Τα ασύρματα δίκτυα αισθητήρων, αποτελούνται από έναν μεγάλο αριθμό κόμβων αισθητήρων που αναπτύσσονται μέσα σε μια περιοχή, προκειμένου να ανιχνεύσουν κάποια σημαντικά γεγονότα (π.χ. έλεγχος άγριας φύσης, έλεγχος δασών για φωτιά, στρατιωτικές εντολές, έξυπνα κτήρια, ευφυείς επικοινωνίες, έλεγχος κυκλοφορίας). Αυτοί οι μικροσκοπικοί κόμβοι αισθητήρων, αποτελούνται από στοιχεία αισθητήρων, επεξεργασίας δεδομένων και επικοινωνίας [Akyildiz et al., 2002b]. Κάθε ένας από αυτούς τους κόμβους είναι σε θέση να συλλέγει και να στέλνει στοιχεία σε ένα σταθμό βάσης μέσω ενός multi-hop ασύρματου δικτύου.

Τα δίκτυα αισθητήρων έχουν ορισμένους περιορισμούς στην τοπική μνήμη, τη διάρκεια των μπαταριών, την ικανότητα υπολογισμών και επικοινωνίας, ενώ εύκολα μπορεί να συμβεί και το φαινόμενο αποτυχίας ενός κόμβου (node failure) [Hu και Sharma, 2005]. Λόγω αυτών των χαρακτηριστικών, το θέμα της ασφάλειας στα ασύρματα δίκτυα αισθητήρων αντιμετωπίζεται αρκετά διαφορετικά, σε σχέση με τους παραδοσιακούς τρόπους που χρησιμοποιούνται στα ασύρματα ad hoc δίκτυα. Είναι πολύ σημαντικό η ασφάλεια των δικτύων αισθητήρων να ελέγχεται με συστήματα ανίχνευσης εισβολών (Intrusion Detection Systems - IDS), για να εξασφαλιστεί η σωστή συμπεριφορά όλων των κόμβων του δικτύου. Αυτή είναι η πρόκληση σε ένα περιβάλλον όπου το δίκτυο έχει σχεδιαστεί για να είναι ευέλικτο.



Εικόνα 1: Ασύρματοι κόμβοι και δίκτυα αισθητήρων

2.2 Εφαρμογές και χαρακτηριστικά

Τα ασύρματα δίκτυα αισθητήρων σχεδιάστηκαν αρχικά για να μπορούν σε πραγματικό χρόνο να συλλέγουν και να αναλύουν στοιχεία από διαφορετικά περιβάλλοντα. Για αυτόν το λόγο ταιριάζουν καλά σε ένα πλήθος εφαρμογών ελέγχου και επίβλεψης. Οι δημοφιλείς εφαρμογές περιλαμβάνουν μεταξύ άλλων την παρακολούθηση άγριας φύσης, την ενημέρωση για πυρκαγιά, στρατιωτικές εντολές, τη ρομποτική, το βιομηχανικά ποιοτικό έλεγχο, την παρατήρηση κρίσιμων υποδομών, τα έξυπνα σπίτια, τις ευφυείς επικοινωνίες και τον έλεγχο της κυκλοφορίας.

Για μερικές εφαρμογές ασύρματων δικτύων αισθητήρων η ασφάλεια είναι κρίσιμη, δεδομένου ότι μπορούν να επεκταθούν σε εχθρικά περιβάλλοντα. Ένα προφανές παράδειγμα είναι εφαρμογές πεδίων μαχών, όπου υπάρχει μια επείγουσα ανάγκη για τη μυστικότητα της θέσης και της αντίστασης στην ανατροπή και την καταστροφή του δικτύου. Λιγότερο προφανείς αλλά επίσης σημαντικές εφαρμογές που απαιτούν αυξημένα επίπεδα ασφάλειας είναι [Wood και Stankovic, 2002]:

- *Καταστροφές:* Σε πολλά σενάρια καταστροφής, ειδικά σε εκείνα που προκαλούνται από τρομοκρατικές επιθέσεις, μπορεί να είναι απαραίτητο να προστατευθεί η θέση των θυμάτων από αυθαίρετη αποκάλυψη.
- *Δημόσια ασφάλεια:* Στις εφαρμογές όπου ελέγχονται οι χημικές, βιολογικές ή άλλες περιβαλλοντικές απειλές, είναι ζωτικής σημασίας η διαθεσιμότητα του δικτύου να μην απειλείται ποτέ. Οι επιθέσεις που προκαλούν ψεύτικους συναγερμούς μπορούν να οδηγήσουν σε απαντήσεις πανικού ή ακόμα χειρότερα στη συνολική αγνόηση των σημάτων.
- *Εφαρμογές υγείας:* Μερικές από τις εφαρμογές υγείας για τα δίκτυα αισθητήρων είναι η παροχή διεπαφών για άτομα με ειδικές ανάγκες, η ολοκληρωμένη παρακολούθηση ασθενών, τα διαγνωστικά, η διαχείριση φαρμάκων στα νοσοκομεία, η τηλε-παρακολούθηση της ψυχολογικής κατάστασης του ασθενούς, ο έλεγχος και η καταγραφή κινήσεων γιατρών και ασθενών μέσα σε ένα νοσοκομείο [Celler et al., 1994; Kahn et al., 1999; Noury et al., 2000; Rabaey et al., 2000; Warneke et al., 2001]. Σε τέτοιες εφαρμογές, η διασφάλιση της μυστικότητας είναι αναγκαία. Μόνο οι εξουσιοδοτημένοι χρήστες πρέπει να

είναι σε θέση να έχουν πρόσβαση στο δίκτυο και να διαχειρίζονται τους πόρους του μόνο με εξουσιοδοτημένο τρόπο.

Τα δίκτυα αισθητήρων συνήθως δημιουργούνται και στη συνέχεια αφήνονται στο φυσικό περιβάλλον χωρίς ιδιαίτερη συντήρηση, για ένα μικρό η μεγάλο χρονικό διάστημα που κυμαίνεται από μέρες έως χρόνια. Ανάλογα με τον σκοπό για τον οποίο έχει δημιουργηθεί το δίκτυο, υπάρχουν διαφορετικές απαιτήσεις σε θέματα αξιοπιστίας, απομακρυσμένου ελέγχου, ανοχής σε σφάλματα, ενώ η διάρκεια ζωής του δικτύου αισθητήρων μπορεί να είναι διαφορετική σε κάθε περίπτωση. Η διάρκεια ζωής των μεμονωμένων αισθητήρων καθορίζει τη διάρκεια ζωής ολόκληρου του δικτύου.

Μια σημαντική ερώτηση που γίνεται για οποιαδήποτε εφαρμογή δικτύων αισθητήρων είναι εάν οι κόμβοι είναι κινητοί, και αν αναμένεται να κινηθούν κατά τη διάρκεια ζωής του δικτύου. Στατική τοπολογία σημαίνει ότι το δίκτυο μπορεί να εκτελέσει τις αναζητήσεις για την εύρεση των διαδρομών κατά την αρχική ρύθμιση του δικτύου. Προφανώς, αυτό δε σημαίνει ότι η εφαρμογή μπορεί έπειτα να ξεχάσει τις αλλαγές των διαδρομών που θα γίνουν, επειδή το ηλεκτρομαγνητικό πεδίο μπορεί να αλλάξει (π.χ., ύπαρξη εξωτερικού θορύβου) και η εφαρμογή θα πρέπει ακόμα να χειριστεί τις αλλαγές στην αξιοπιστία και την απόδοση των συνδέσεων. Τέλος, στην ακραία περίπτωση, ένα στατικό σχέδιο δρομολόγησης μπορεί να προγραμματιστεί πριν γίνει η τοποθέτηση των κόμβων στο πεδίο, αλλά αυτό πρέπει να θεωρηθεί παράλογη προσέγγιση εκτός και αν γίνει σε ένα πολύ ελεγχόμενο περιβάλλον. Οι μεταβαλλόμενες τοπολογίες στις περισσότερες περιπτώσεις απαιτούν η εφαρμογή να εκτελεί αναζήτηση κόμβων ή να είναι σε θέση τουλάχιστον να καθορίσει ότι ένας κόμβος δεν είναι πλέον ικανός να στέλνει / λαμβάνει δεδομένα. Συναφής έννοια με την κινητικότητα είναι και ο εντοπισμός. Μερικές εφαρμογές απαιτούν τον εντοπισμό για να λειτουργήσουν αποτελεσματικά, το οποίο μπορεί πάλι να επηρεάσει το ποιες πλατφόρμες είναι κατάλληλες για την εφαρμογή.

Γενικά, οι κόμβοι μπορούν να αποτύχουν ή η επικοινωνία θα αποκαλύψει ότι ένας κόμβος έχει αποτύχει. Η πραγματική ερώτηση για την αποτυχία κόμβων είναι μέχρι ποιό σημείο η εφαρμογή μπορεί να την ανεχτεί. Μερικές εφαρμογές μπορούν να δεχτούν τις αποτυχίες κόμβων και να προσπαθήσουν απλά να εργαστούν με όσο το

δυνατόν περισσότερους κόμβους. Για άλλες εφαρμογές, μπορεί να είναι πολύ σημαντικό ότι ορισμένοι βασικοί κόμβοι δεν αποτυγχάνουν ποτέ.

Για μερικές εφαρμογές ελέγχου, μπορούμε να επιθυμούμε να συλλέγουμε τα στοιχεία πολύ συχνά. Παραδείγματος χάριν, μια ειδοποίηση κάθε φορά που περνούν τα αυτοκίνητα από ένα σημείο σε μια εθνική οδό. Σε άλλες περιπτώσεις, μπορούμε μόνο να επιθυμούμε ειδοποίηση για τον αριθμό αυτοκινήτων που πέρασε κατά τη διάρκεια μιας ώρας. Για μερικές εφαρμογές μπορούμε να συλλέξουμε τα στοιχεία πολύ σπάνια π.χ., ένας άνθρωπος μπαίνει σε ένα δωμάτιο, επειδή θέλουμε να λάβουμε μέτρα βασισμένα σε αυτές τις πληροφορίες.

2.3 Ένα γενικό μοντέλο για WSN

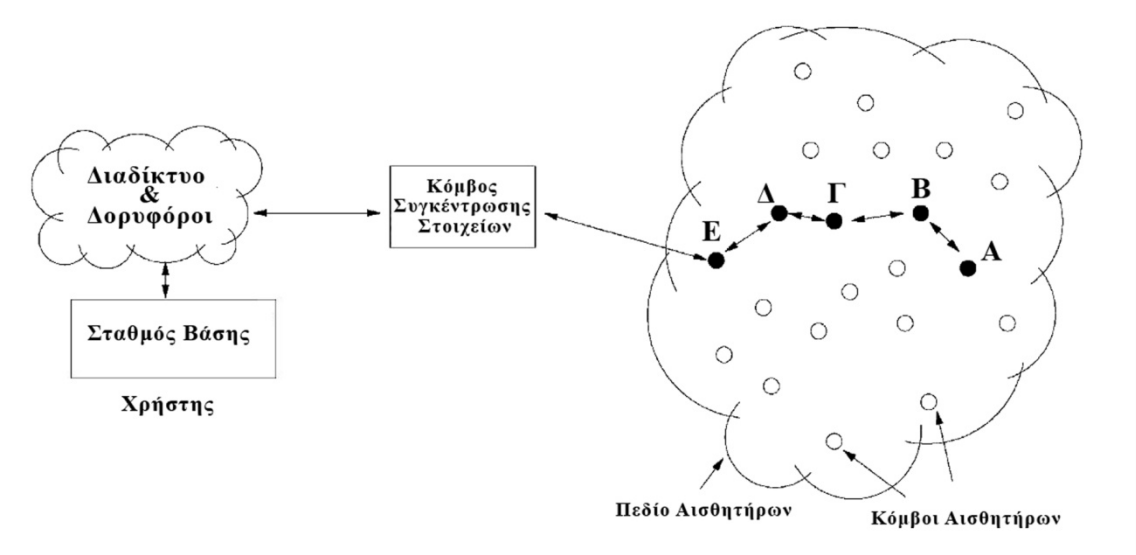
Πολλοί άνθρωποι συγχέουν τα ασύρματα δίκτυα αισθητήρων με τους πιο στενούς "προγόνους" τους τα ad hoc δίκτυα. Στην πραγματικότητα εντούτοις τα WSN είναι διαφορετικά από τα ad hoc δίκτυα. Συγκεκριμένα τα WSN έχουν περιορισμένους πόρους, αναπτύσσονται πυκνά, είναι επιρρεπή σε αποτυχίες, ο αριθμός κόμβων στα WSN είναι αρκετά υψηλότερος σε σχέση με αυτόν των ad hoc δικτύων, και η τοπολογία των WSN δικτύων αλλάζει συνεχώς. Επιπλέον τα WSN χρησιμοποιούν τα μέσα μιας ραδιοφωνικής μετάδοσης επικοινωνίας και οι κόμβοι αισθητήρων δεν έχουν έναν σφαιρικό προσδιορισμό με βάση κάποιο ID [Akyildiz et al., 2002].

Τα σημαντικότερα συστατικά ενός χαρακτηριστικού δικτύου αισθητήρων παρουσιάζονται στην εικόνα 2 και είναι: οι *κόμβοι αισθητήρων (sensor nodes)*, το *πεδίο αισθητήρων (sensor field)*, ο *κόμβος συγκέντρωσης στοιχείων (sink)* και ο *διαχειριστής εργασιών (task manager ή base station)*.

Το πεδίο αισθητήρων μπορεί να θεωρηθεί ως ένα πεδίο μέσα στο οποίο οι κόμβοι τοποθετούνται, δηλαδή η περιοχή στην οποία αναμένουμε ένα ιδιαίτερο φαινόμενο να εμφανιστεί.

Οι κόμβοι αισθητήρων είναι η καρδιά του δικτύου. Είναι υπεύθυνοι για τη συλλογή στοιχείων και τη δρομολόγηση αυτών των πληροφοριών πίσω στο sink.

Το sink είναι ένας κόμβος αισθητήρων με το συγκεκριμένο στόχο της λήψης, της επεξεργασίας και της αποθήκευσης στοιχείων από τους άλλους κόμβους αισθητήρων. Χρησιμεύει ώστε να μειωθεί ο συνολικός αριθμός μηνυμάτων που πρέπει να σταλούν μεταξύ των κόμβων, με αποτέλεσμα έτσι να μειώνονται και οι γενικές ανάγκες σε ενέργεια του δικτύου. Τέτοια σημεία ορίζονται συνήθως δυναμικά από το δίκτυο. Οι κανονικοί κόμβοι μπορούν επίσης να θεωρηθούν ως sink, εάν καθυστερούν τα εξερχόμενα μηνύματα, έως ότου έχουν συγκεντρώσει αρκετές πληροφορίες. Για αυτόν το λόγο, τα sink είναι επίσης γνωστά ως σημεία συγκέντρωσης στοιχείων.



Εικόνα 2: Δομή επικοινωνίας δικτύων αισθητήρων [Akyildiz et al., 2002a]

Ο διαχειριστής εργασιών ή σταθμός βάσης είναι ένα κεντρικό σημείο ελέγχου μέσα στο δίκτυο, το όποιο εξάγει τις πληροφορίες από το δίκτυο και διαδίδει τις πληροφορίες ελέγχου πίσω στο δίκτυο. Επίσης παρέχει μια πύλη στα άλλα δίκτυα, έναν ισχυρό επεξεργαστή δεδομένων, ένα κέντρο αποθήκευσης στοιχείων και ένα σημείο πρόσβασης για τους χρήστες. Ο σταθμός βάσεων είτε είναι ένας φορητός υπολογιστής είτε ένας τερματικός σταθμός. Τα δεδομένα κατευθύνονται από το sink προς αυτούς τους τερματικούς σταθμούς μέσω του Διαδικτύου, των ασύρματων καναλιών, των δορυφόρων κ.λπ.

Έτσι, εκατοντάδες σε ορισμένες περιπτώσεις και χιλιάδες κόμβοι επεκτείνονται σε όλο το πεδίο αισθητήρων, για να δημιουργήσουν ένα ασύρματο multi-hop δίκτυο. Οι κόμβοι μπορούν να είναι τοποθετημένοι πολύ πυκνά μεταξύ τους, όπως 20 κόμβοι/m^3.

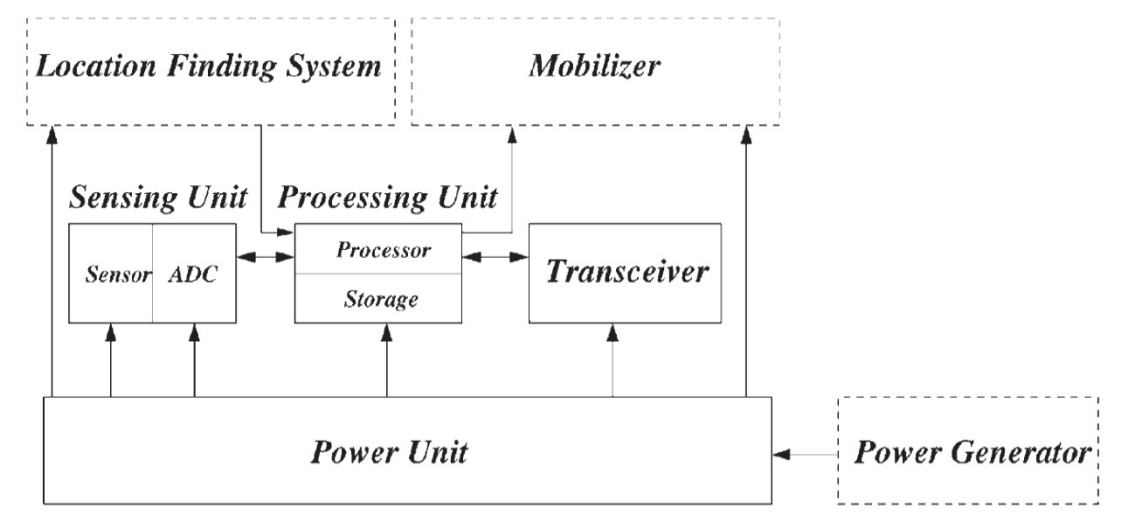
Οι κόμβοι μπορούν να χρησιμοποιήσουν τα ασύρματα μέσα επικοινωνίας όπως είναι οι υπέρυθρες, ράδιο, οπτικά μέσα ή bluetooth για τις επικοινωνίες τους. Η εμβέλεια μετάδοσης των κόμβων ποικίλλει ανάλογα με το πρωτόκολλο επικοινωνίας που χρησιμοποιείται.

Τέλος τα ασύρματα δίκτυα αισθητήρων μπορούν να περιγραφούν σε υψηλότερο επίπεδο, σαν ένα συνδυασμό δύο διαφορετικών δικτύων [Roman et al., 2005]:

- *Το δίκτυο απόκτησης δεδομένων:* Μια συλλογή από κόμβους αισθητήρων και του σταθμού βάσης. Τα δίκτυα αισθητήρων μετρούν τα φυσικά στοιχεία και ο σταθμός βάσης συλλέγει τις πληροφορίες από τους κόμβους και προωθεί στοιχεία ελέγχου στο περιβάλλον του δικτύου.
- *Το δίκτυο διάδοσης δεδομένων:* Διασυνδέει το δίκτυο απόκτησης δεδομένων σε έναν χρήστη και είναι μια συλλογή ενσύρματων και ασύρματων δικτύων.

2.4 Δομή κόμβου αισθητήρα

Οι κόμβοι αισθητήρων αποτελούνται συνήθως από τέσσερα βασικά στοιχεία όπως φαίνεται και στην εικόνα 3. Έναν *αισθητήρα (Sensing Unit)*, μια *μονάδα επεξεργασίας (Processing Unit)*, ένα *ράδιο πομποδέκτη (Transceiver)* και μια *μονάδα παροχής ενέργειας (Power Unit)*. Τα πρόσθετα στοιχεία μπορούν να περιλαμβάνουν συστήματα όπως το *GPS (Global Positioning System)*, το οποίο μπορεί να βρίσκει ανά πάσα στιγμή τη θέση του κόμβου, τα *mobilizers* τα οποία χρειάζονται για να μετακινηθεί ο κόμβος σε συγκεκριμένες εφαρμογές και τέλος οι *γεννήτριες ενέργειας (Power Generator)*.



Εικόνα 3: Sensor Node Hardware Components [Akyildiz et al., 2002a]

Παρακάτω δίνεται μια συνοπτική εξήγηση στο τι κάνει καθένα από αυτά τα στοιχεία που έχει ένας κόμβος αισθητήρων. Τα αναλογικά σήματα τα οποία μετριούνται από τους αισθητήρες, ψηφιοποιούνται μέσω ADC (Analog to Digital Converter) και τροφοδοτούνται στη συνέχεια προς την μονάδα επεξεργασίας. Η μονάδα επεξεργασίας διαχειρίζεται τις διαδικασίες που κάνουν τον κόμβο αισθητήρων να εκτελέσει τους ορισμένους στόχους της αντίληψης και της συνεργασίας. Ο ράδιο πομποδέκτης (radio transceiver) συνδέει τον κόμβο με το δίκτυο και χρησιμεύει ως το μέσο επικοινωνίας του κόμβου.

Η μονάδα παροχής ενέργειας (power unit) είναι το σημαντικότερο στοιχείο ενός κόμβου αισθητήρων, επειδή καθορίζει την διάρκεια ζωής ολόκληρου του δικτύου. Λόγω των περιορισμών μεγέθους, οι μπαταρίες AA ή τα quartz cells χρησιμοποιούνται ως αρχικές πηγές ενέργειας. Για να έχουμε μια ένδειξη της κατανάλωσης ενέργειας, ένας μέσος κόμβος αισθητήρων θα χρησιμοποιήσει περίπου 4.8mA για να λάβει ένα μήνυμα, 12mA για διαβιβάσει ένα πακέτο και 5mA για sleeping. Επιπλέον η CPU χρησιμοποιεί κατά μέσο όρο 5.5mA όταν το δίκτυο είναι ενεργό.

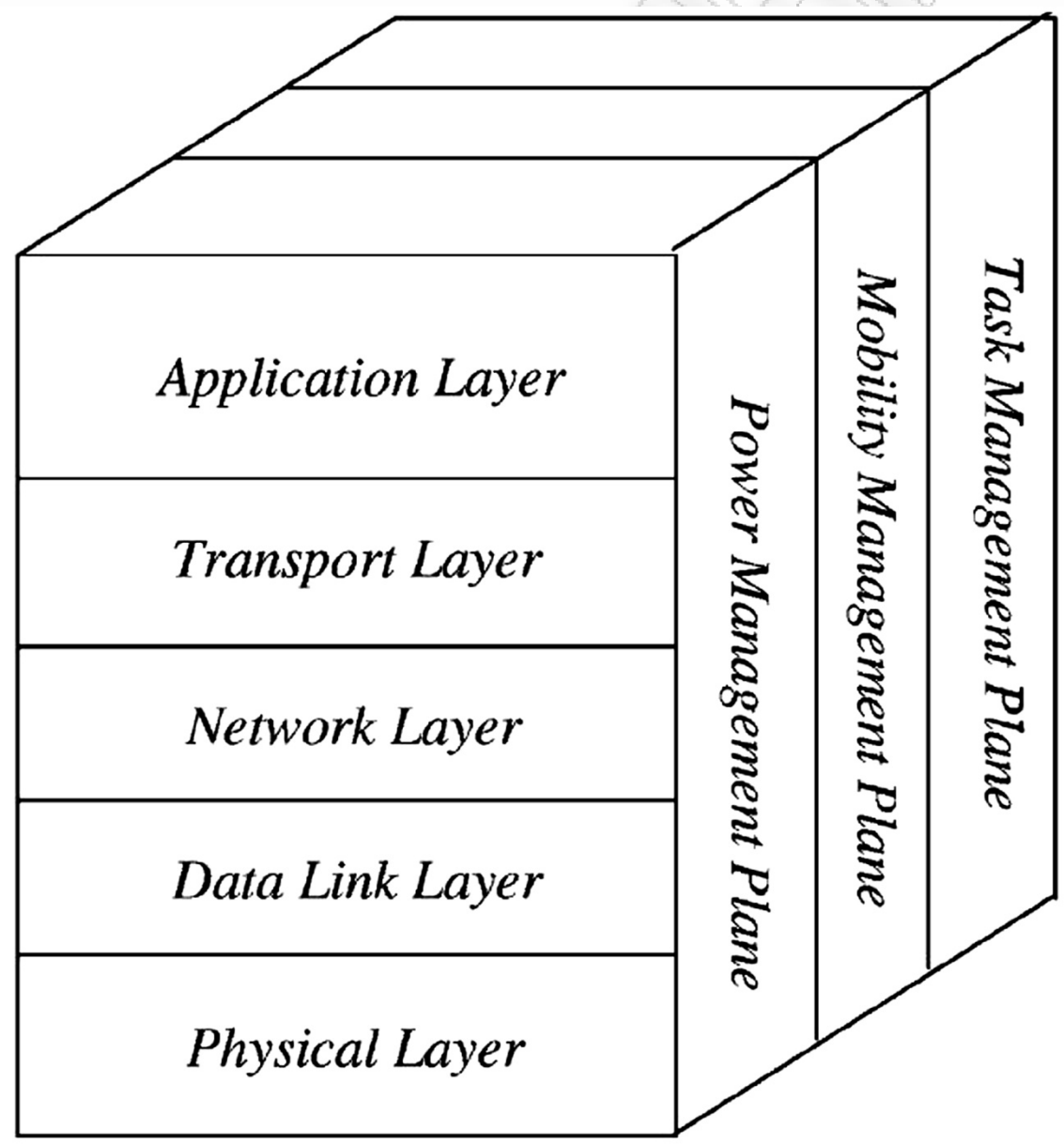
Η Xbow [Xbow, 2005] και η Ambient Systems [Ambient, 2006] είναι δύο επιχειρήσεις που παράγουν κόμβους αισθητήρων για εμπορική χρήση. Για να έχουμε μια ιδέα του περιορισμού των πόρων, ο πίνακας 1 παρουσιάζει λεπτομέρειες του καλύτερου σε πωλήσεις κόμβου της Xbow, τον Mica, και το κύριο προϊόν της Ambient Systems, τον μnode κόμβο. Ο κόμβος Mica έχει χρησιμοποιηθεί εκτενώς σε όλες τις μελέτες στο Πανεπιστήμιο του Berkeley, σε μία προσπάθεια να αναπτυχθεί ένα λειτουργικό σύστημα για WSN το TinyOS [TinyOS, www.tinyos.net].

	MICAz	μNODE
Processor	4MHz 8bit Atmel	16MHz 16bit TI MSP430
Memory	4KB RAM, 512KB flash	10KB RAM, 1MB flash
Radio	916MHz, 40Kbps, 35m range	868/917MHz, 50m range

Πίνακας 1 Mica και μnode στοιχεία

2.5 Πρωτόκολλα επικοινωνίας

Οι κόμβοι αισθητήρων, όπως οποιαδήποτε άλλη συσκευή τηλεπικοινωνιών, χρησιμοποιούν μια συγκεκριμένη στοίβα πρωτοκόλλων (protocol stack). Σε αυτή την ενότητα, διευκρινίζουμε το στόχο κάθε στρώματος (layer) και των πιο κοινών πρωτοκόλλων που συνδέονται με κάθε στρώμα. Στην εικόνα 4 αναπαριστούμε την στοίβα πρωτοκόλλων που χρησιμοποιείται από όλους τους κόμβους αισθητήρων.



Εικόνα 4: Στοίβα Πρωτοκόλλων Ασύρματου Κόμβου [Akyildiz et al., 2002a]

- Το φυσικό στρώμα (Physical Layer) είναι υπεύθυνο για τη δημιουργία του carrier frequency, την επιλογή συχνότητας, την ανίχνευση σήματος, τη διαμόρφωση (modulation) και την κρυπτογράφηση των δεδομένων. Τεχνικές, όπως είναι οι Ultra Wideband, Impulse Radio και Pulse Position modulation, έχουν χρησιμοποιηθεί ώστε να μειωθεί η πολυπλοκότητα και οι ενεργειακές απαιτήσεις.
- Το στρώμα ζεύξης δεδομένων (Data Link Layer) είναι υπεύθυνο για την πρόσβαση στο μέσο (medium access), τον έλεγχο σφαλμάτων, multiplexing of data streams, data frame detection. Εξασφαλίζει αξιόπιστες σημείο προς σημείο συνδέσεις μέσα στο δίκτυο. Λόγω των περιορισμών που υπάρχουν στο δίκτυο, τα συνηθισμένα MAC πρωτόκολλα δεν ταιριάζουν στα ασύρματα δίκτυα αισθητήρων. Κάποια διαδεδομένα πρωτόκολλα του επιπέδου ζεύξης δεδομένων είναι: SMACS (Self-Organised Medium Access Control for Sensor Networks) [Sohrabi, 2000], EARS (Eavesdrop and Register) [Sohrabi, 2000], CSMA-Based medium Access Protocols [Woo και Culler, 2001] και Hybrid TDMA/FDMA-Based protocols [Shih et al., 2001].
- Το στρώμα δικτύου (Network Layer) είναι αρμόδιο για τη δρομολόγηση των δεδομένων μέσα σε ένα ασύρματο δίκτυο αισθητήρων. Για παράδειγμα, να βρίσκει την αποδοτικότερη διαδρομή για ένα πακέτο μέχρι να φτάσει στον προορισμό του. Μερικά από τα πρωτόκολλα που χρησιμοποιούνται αναφέρονται παρακάτω: SMECN (Small Minimum Energy Communication Network) [Li και Halpern, 2001], SPIN (Sensor Protocols for Information via Negotiation) [Heinzelman et al., 1999], SAR (Sequential Assignment Routing) [Sohrabi, 2000], LEACH (Low Energy Adaptive Clustering Hierarchy) [Heinzelman et al., 2000] και Directed Diffusion [Intanagonwiwat et al., 2000].
- Το στρώμα μεταφοράς (Transport Layer) απαιτείται όταν το ασύρματο δίκτυο αισθητήρων χρειάζεται να έχει πρόσβαση στο Internet. Εντούτοις, κανένα σχέδιο δεν έχει επινοηθεί για να αντιμετωπίσει πλήρως αυτό το ζήτημα. Τα τροποποιημένα TCP/UDP πρωτόκολλα μπορεί να είναι μια κατάλληλη λύση, αλλά αυτό ακόμα δεν έχει καθιερωθεί.

- Το στρώμα εφαρμογής (Applications Layer) είναι αρμόδιο στο να παρουσιάζει όλες τις απαραίτητες πληροφορίες στην εφαρμογή και να μεταφέρει τα αιτήματα από την εφαρμογή στα κατώτερα στρώματα του πρωτοκόλλου. Κάποια πρωτόκολλα που χρησιμοποιούνται σε αυτό το επίπεδο είναι τα παρακάτω: SMP (Sensor Management Protocol) [Shen et al., 2001], TADAP (Task Assignment and Data Advertisement Protocol) [Shen et al., 2001], και SQDDP (Sensor Query and Data Dissemination Protocol) [Shen et al., 2001].

2.6 Ασφάλεια σε Ασύρματα Δίκτυα Αισθητήρων

Ένα ασύρματο δίκτυο αισθητήρων αποτελείται από διαφορετικά είδη αισθητήρων που ελέγχουν το περιβάλλον. Λόγω του χαμηλού κόστους και της ευελιξίας, τα δίκτυα αισθητήρων γρήγορα επεκτείνονται για ποικίλες εφαρμογές, όπως ο έλεγχος οικολογίας και περιβάλλοντος, στρατιωτικές εφαρμογές, περιοχές έκτακτης ανάγκης, έξυπνα σπίτια, υγεία, και εμπορικές περιοχές [Akyildiz et al., 2002b]. Εντούτοις, οι αισθητήρες έχουν πολύ περιορισμένους πόρους (CPU, μνήμη, εύρος ζώνης, ενέργεια). Κατά συνέπεια, ο σχεδιασμός αποδοτικών πρωτοκόλλων είναι μια σημαντική πρόκληση κατά το σχεδιασμό των δικτύων αισθητήρων. Άλλα ζητήματα περιλαμβάνουν την ασφάλεια, την ανοχή σε σφάλματα, την ικανότητα επιβίωσης κάτω από δύσκολες συνθήκες και την εξελιξιμότητα του δικτύου.

Δεδομένου ότι τα δίκτυα αισθητήρων λειτουργούν στον πραγματικό κόσμο, υπάρχει μια ανάγκη να προστατευθούν από τους διάφορους τύπους επιθέσεων. Αυτό είναι βεβαίως πρόκληση σε ένα περιβάλλον όπου το δίκτυο σχεδιάζεται για να είναι ευέλικτο. Οι σημαντικότερες προκλήσεις στην αντιμετώπιση της ασφάλειας δικτύων αισθητήρων, περιλαμβάνουν τη συντήρηση ενέργειας για τους κινητούς αισθητήρες, τη συνεργασία μεταξύ των ετερογενών αισθητήρων, την ευελιξία σε επίπεδο ασφάλειας, ώστε να ταιριάξουν οι ανάγκες των εφαρμογών και παράλληλα να συντηρηθούν οι κρίσιμοι πόροι του δικτύου, η εξελιξιμότητα του δικτύου, οι αποφάσεις εμπιστοσύνης και ασφάλειας για τις εφαρμογές, η διατήρηση της κινητικότητας, της μεταβλητότητας και της προστασίας του δικτύου από τις εξωτερικές και εσωτερικές εισβολές. Εν

συντομία, πρέπει να εξετάσουμε τρεις σημαντικούς παράγοντες για την ασφάλεια των δικτύων αισθητήρων οι οποίοι είναι: ενέργεια, επεξεργασία και επικοινωνία.

Λόγω της έλλειψης πόρων στους κόμβους αισθητήρων, το θέμα ασφάλεια σε ένα δίκτυο αισθητήρων είναι αρκετά διαφορετικό σε σχέση με τους παραδοσιακούς τρόπους που χρησιμοποιούνται και περιλαμβάνουν γενικά τη διαχείριση και την ασφαλή κράτηση ενός μικρού αριθμού ιδιωτικών και δημόσιων κλειδιών [Perrig et al., 2000]. Η αποκάλυψη ενός κλειδιού με κάθε πακέτο απαιτεί πάρα πολλή ενέργεια [Perrig et al., 2001]. Η αποθήκευση μιας μονόδρομης αλυσίδας μυστικών κλειδιών κατά μήκος μιας διαδρομής απαιτεί αρκετή μνήμη και πολλούς υπολογισμούς στους κόμβους στη συγκεκριμένη διαδρομή [Perrig και Tygar, 2003]. Η διαχείριση κλειδιών, που χρησιμοποιεί έναν εμπιστευμένο τρίτο πάροχο, απαιτεί πάλι μια κατασκευασμένη λύση που την καθιστά ακατάλληλη για τις εφαρμογές δικτύων αισθητήρων [Perrig et al., 2000]. Αν και το ασύμμετρο σύστημα κρυπτογραφίας δεν απαιτεί έναν εμπιστευμένο κεντρικό υπολογιστή, η ανάκληση κλειδιών δυσχεραίνει τη λειτουργία του δικτύου [Perrig et al., 2000], δεδομένου ότι περιλαμβάνει μια αρχή που διατηρεί έναν κατάλογο ανακλημένων κλειδιών σε έναν κεντρικό υπολογιστή ή που ζητά το δημόσιο κλειδί άμεσα από τον ιδιοκτήτη.

Υπάρχουν δύο τύποι επιτιθέμενων, οι εξωτερικοί και οι εσωτερικοί. Ένας επιτιθέμενος μπορεί να αναλάβει τον έλεγχο σε οποιοδήποτε κόμβο μέσα σε ένα δίκτυο. Η υπονόμευση ενός κόμβου σημαίνει, ότι όλοι οι κόμβοι που βρίσκονται μέσα στην ακτίνα επικοινωνίας εκείνου του κόμβου, μπορούν να αρνηθούν τη λήψη οποιωνδήποτε πληροφοριών. Επομένως, ο στόχος είναι να ελαχιστοποιηθεί ο αντίκτυπος ενός υπονομευμένου κόμβου στο υπόλοιπο του δικτύου. Ένας μόνο κόμβος δεν πρέπει να χορηγήσει στον επιτιθέμενο τη δυνατότητα να υπονομεύσει ολόκληρο το δίκτυο. Σε ένα δίκτυο με μια ενιαία πύλη (δηλαδή ένα σταθμό βάσης), ο επιτιθέμενος πρέπει να επιτεθεί σε εκείνο τον έναν κόμβο για να καταστήσει το δίκτυο ανενεργό. Προκειμένου να είναι σε θέση να εμπιστευθεί τα δεδομένα που στέλνουν οι αισθητήρες, η πηγή πρέπει να επικυρωθεί έτσι ώστε οι κακόβουλοι αισθητήρες να μην μπορούν να στείλουν ψεύτικα στοιχεία. Για τον έλεγχο της ακεραιότητας των στοιχείων, πρέπει να είμαστε σε θέση να ανιχνεύσουμε την τροποποίηση στοιχείων. Επιπλέον, τα στοιχεία πρέπει να είναι εμπιστευτικά έτσι κανένας να μην μπορεί αλλιώς να τα διαβάσει. Κατά συνέπεια οι απειλές που ένα δίκτυο αισθητήρων μπορεί να αντιμετωπίσει είναι: eavesdropping,

παρεμβολή μηνυμάτων (injection), επανάληψη μηνυμάτων, τροποποίηση μηνυμάτων (message modification) και άρνηση της υπηρεσίας (denial of service).

2.7 DoS Επιθέσεις σε ασύρματα δίκτυα αισθητήρων

Πολλές εγκαταστάσεις ασύρματων δικτύων αισθητήρων δεν είναι αρκετά ασφαλείς και οι επιθέσεις ενάντια σε αυτές μπορούν να δημιουργήσουν πραγματική ζημιά στην υγεία και την ασφάλεια των ανθρώπων. Αποτυχίες υλικού, ελαττώματα, η εξάντληση των πόρων, οι κακόβουλες επιθέσεις και οι περιβαλλοντικές συνθήκες μπορούν να επιφέρουν μείωση ή ακόμα και εξόντωση της λειτουργίας των δικτύων. Τέτοιες συνθήκες ορίζονται στη βιβλιογραφία σαν επιθέσεις άρνησης υπηρεσιών (Denial of Service – DoS). Σε αυτό το κεφάλαιο θα αναλύσουμε τις επιθέσεις που γίνονται σε κάθε στρώμα του πρωτοκόλλου των ασύρματα δικτύων αισθητήρων [Wood και Stankovic, 2002].

Επιθέσεις στο φυσικό επίπεδο

Οι κόμβοι σε ένα δίκτυο αισθητήρων χρησιμοποιούν ασύρματες τεχνολογίες για την επικοινωνία τους, λόγω του ότι η ad hoc αρχιτεκτονική του δικτύου καθιστά οτιδήποτε άλλο ανεπαρκές. Οι σταθμοί βάσης και οι κόμβοι συγκέντρωσης δεδομένων μπορούν να χρησιμοποιήσουν και ενσύρματες τεχνολογίες αλλά και δορυφορικές. Οι περιορισμοί τους όμως σε ενέργεια και η ανάγκη για κινητικότητα μερικές φορές κάνουν τις παραπάνω δύο επιλογές σπάνιες. Οι πιο συνηθισμένες επιθέσεις στο φυσικό επίπεδο ενός ασύρματου δικτύου αισθητήρων είναι οι παρεμβολές και οι πλαστογραφίες.

- Παρεμβολές (Jamming): Ένας πολύ συνηθισμένος τρόπος επίθεσης στις ασύρματες επικοινωνίες είναι η παρεμβολή στη συχνότητα που χρησιμοποιούν οι κόμβοι του δικτύου. Στα δίκτυα που εκπέμπουν σε μια μόνο συχνότητα, αυτός ο τρόπος επίθεσης είναι πολύ εύκολος, αλλά και πολύ αποδοτικός. Ένας κακόβουλος χρήστης μπορεί να διακόψει την ομαλή λειτουργία του δικτύου, παρεμβάλλοντας λίγους κόμβους αλλά βγάζοντας εκτός λειτουργίας ένα αρκετά μεγάλο μέρος των κόμβων του δικτύου. Ο συνηθισμένος τρόπος άμυνας

απέναντι σε τέτοιες επιθέσεις περιλαμβάνει διάφορες μορφές του λεγόμενου spread-spectrum communication [Anderson, 2001].

- Πλαστογραφίες: Οι κόμβοι μπορούν να πέσουν θύματα φυσικής παρέμβασης, ειδικά εάν είναι μέρος ενός δικτύου που καλύπτει μια απέραντη περιοχή. Τέτοια δίκτυα μπορούν να δεχτούν καταστροφικές brute force επιθέσεις αλλά και περιπλοκότερη ανάλυση (sophisticated analysis) [Anderson και Kuhn, 1996]. Ένας επιτιθέμενος μπορεί να βλάψει έναν αισθητήρα, να αντικαταστήσει ολόκληρο κόμβο ή μέρος του υλικού του, ή ακόμα και να παρέμβει ηλεκτρονικά στους κόμβους ώστε να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες, όπως τα κοινά κρυπτογραφικά κλειδιά και το πώς μπορεί να έχει πρόσβαση σε υψηλότερα στρώματα επικοινωνίας.

Επιθέσεις στο στρώμα ζεύξης δεδομένων

Το στρώμα ζεύξης δεδομένων, ή media access control (MAC) παρέχει «έλεγχο» καναλιού για επικοινωνίες που γίνονται μεταξύ γειτονικών κόμβων. Τα συνεργατικά σχήματα (cooperative schemes) που βασίζονται στο carrier sense, το οποίο δίνει τη δυνατότητα στους κόμβους να ανιχνεύουν εάν άλλοι κόμβοι μεταδίδουν δεδομένα, είναι ιδιαιτέρως ευάλωτα σε DoS επιθέσεις. Επιθέσεις που μπορούν να γίνουν ενάντια στο στρώμα ζεύξης ενός ασύρματου δικτύου αισθητήρων είναι οι συγκρούσεις, η εξάντληση των πόρων και η unfairness.

- Συγκρούσεις (collisions): Οι συγκρούσεις είναι ένας τύπος παρεμβολής αλλά αυτή τη φόρα γίνονται στο επίπεδο ζεύξης δεδομένων. Εάν ο επιτιθέμενος αλλάξει την αλληλουχία των bit στη μετάδοση, τότε δε θα προκύψει σωστό άθροισμα ελέγχου και το πακέτο θα απορριφτεί από το δέκτη. Αλλοιωμένα μηνύματα ACK συνήθως οδηγούν σε μεγάλη αύξηση του κόστους ενέργειας σε ορισμένα πρωτόκολλα MAC. Ένας κακόβουλος κόμβος, μπορεί επίσης σκόπιμα και επανειλημμένα να αρνηθεί την πρόσβαση σε ένα κανάλι, ταυτόχρονα χρησιμοποιώντας τη λιγότερη δυνατή ενέργεια που απαιτείται ώστε να μπλοκάρει το κανάλι.

- Εξάντληση πόρων (Exhaustion): Η εξάντληση των πόρων των μπαταριών μπορεί να εμφανιστεί όταν προσπαθούν οι εφαρμογές του στρώματος ζεύξης δεδομένων την επαναλαμβανόμενη αναμετάδοση ακόμα και μετά από τις κατά ασυνήθιστο τρόπο καθυστερημένες συγκρούσεις, όπως είναι αυτές που προκαλούνται στο τέλος ενός frame. Μια παραλλαγή αυτής της επίθεσης είναι όταν ένας κόμβος θυσιάζεται ζητώντας συνεχώς την πρόσβαση σε ένα κανάλι στέλνοντας RTS (Request To Send) μηνύματα, αναγκάζοντας τους γείτονές του να αποκριθούν με ένα CTS (Clear To Send) για να στείλει το μήνυμα.
- Unfairness: Αυτή η επίθεση μπορεί να δημιουργηθεί με κατάχρηση της προτεραιότητας των MAC schemes. Το αποτέλεσμα μιας τέτοιας επίθεσης είναι ότι μπορεί να υποβιβάσει την υπηρεσία, για παράδειγμα αναγκάζοντας τους χρήστες ενός σε πραγματικό χρόνο πρωτοκόλλου MAC να χάσουν τις προθεσμίες τους.

Επιθέσεις στο επίπεδο δικτύου

Τα υψηλότερα στρώματα του πρωτοκόλλου μπορούν να μην απαιτήσουν μια πλήρως αξιόπιστη μετάδοση των δεδομένων, αλλά το στρώμα δικτύων παρέχει πολύ κρίσιμες υπηρεσίες. Σε μια μεγάλης κλίμακας εγκατάσταση ασύρματου δικτύου αισθητήρων, τα μηνύματα μπορούν να περάσουν από πολλούς κόμβους πριν φθάσουν στον τελικό προορισμό τους. Δυστυχώς, καθώς το συνολικό κόστος αναμετάδοσης ενός πακέτου στο δίκτυο αυξάνεται, κάνει έτσι μεγαλύτερη και την πιθανότητα ότι το δίκτυο θα κόψει ή θα δώσει λανθασμένη κατεύθυνση στα πακέτα κατά μήκος της διαδρομής. Η απουσία προϋπάρχουσας υποδομής στα δίκτυα αισθητήρων, σημαίνει ότι, οι περισσότεροι εάν όχι όλοι οι κόμβοι, θα χρησιμεύσουν ως δρομολογητές για τη μεταφορά των πακέτων. Δεδομένου ότι κάθε κόμβος είναι ενδεχομένως ένας δρομολογητής, αυτό δημιουργεί νέα ευάλωτα σημεία στο στρώμα δικτύου, τα οποία είναι γνωστά και στο διαδίκτυο. Τα πρωτόκολλα δρομολόγησης πρέπει να είναι αρκετά απλά ώστε να χρησιμοποιούνται σε μεγάλα δίκτυα, αλλά να είναι και αρκετά γερά ώστε να αντιμετωπίσουν τις ενδεχόμενες αποτυχίες που εμφανίζονται μακριά από την πηγή.

- Neglect and greed: Μια πολύ συνηθισμένη επίθεση στους κόμβους είναι η αλλαγή των πακέτων πληροφορίας που αποστέλλονται. Ένας κακόβουλος

κόμβος μπορεί να συμμετέχει στο επίπεδο δικτύου και να στέλνει αλλαγμένα πακέτα, ή ακόμα και να απορρίπτει μηνύματα άλλων κόμβων. Το dynamic source routing (DSR) [Johnson και Maltz, 1996] είναι ευάλωτο σε αυτή την επίθεση. Επειδή το δίκτυο αποθηκεύει τις διαδρομές, οι επικοινωνίες από μια περιοχή μπορούν όλες να χρησιμοποιήσουν την ίδια διαδρομή για έναν προορισμό. Εάν ένας κόμβος κατά μήκος εκείνης της διαδρομής είναι κακόβουλος, μπορεί να μειώσει ή να εμποδίσει την κυκλοφορία δεδομένων από την περιοχή προς για παράδειγμα έναν σταθμό βάσης.

- Homing: Στα περισσότερα δίκτυα αισθητήρων ορισμένοι κόμβοι έχουν ειδικές ευθύνες, όπως το να είναι υπεύθυνοι για το συντονισμό μιας ομάδας κόμβων, διαχειριστές κρυπτογραφημένων κλειδιών, ελέγχουν τα σημεία πρόσβασης κ.α. Αυτοί οι κόμβοι γίνονται στόχος επίθεσης συχνότερα διότι παρέχουν κρίσιμες υπηρεσίες στο δίκτυο. Πρωτόκολλα δικτύων που βασίζονται στην τοποθεσία και στηρίζονται στη σωστή προώθηση των πακέτων, είναι εκτεθειμένα σε homing attacks. Εδώ ο κακόβουλος χρήστης παρατηρεί την κίνηση των δεδομένων, και μαθαίνει για την ύπαρξη και την τοποθεσία των κρίσιμων πόρων. Μόλις τα βρίσκει, αυτοί οι κόμβοι δέχονται επιθέσεις από συνεργάτες του επιτιθέμενου ή κινητούς εχθρούς.
- Misdirection: Ο σκοπός αυτής της επίθεσης είναι να παρασυρθεί όλη η κίνηση προς ένα κακόβουλο σημείο του δικτύου. Αυτό επιτυγχάνεται με το να κάνεις έναν κακόβουλο κόμβο ελκυστικό για το υπόλοιπο δίκτυο, διαφημίζοντας υψηλής ποιότητας διαδρομές με χαμηλή καθυστέρηση. Οι κόμβοι που έχουν παραπλανηθεί, θα στείλουν όλα τα δεδομένα που προορίζονται για το σταθμό βάσης, στον κόμβο που λέει ψέματα.
- Black holes: Τα distance vector πρωτόκολλα [Perkins και Bhagwat, 1994] παρέχουν άλλον έναν εύκολο δρόμο για αποτελεσματικές επιθέσεις. Οι κόμβοι διαφημίζουν διαδρομές μηδενικού κόστους σε οποιοδήποτε άλλο κόμβο, δημιουργώντας routing back holes μέσα στο δίκτυο [Cheung και Levitt, 1997]. Όσο η διαφήμιση συνεχίζεται, το δίκτυο δρομολογεί όλο και περισσότερη κίνηση προς την μεριά τους. Εκτός από τη διακοπή της παράδοσης των μηνυμάτων, αυτή η επίθεση προκαλεί έντονες διαμάχες για τους πόρους που

βρίσκονται γύρω από τον κακόβουλο κόμβο, καθώς οι γειτονικοί κόμβοι ανταγωνίζονται για το περιορισμένο εύρος ζώνης. Αυτοί οι γειτονικοί κόμβοι μπορούν να εξαντληθούν πρόωρα, προκαλώντας μια τρύπα ή ένα χώρισμα στο δίκτυο.

Επιθέσεις στο επίπεδο μεταφοράς

Το επίπεδο μεταφοράς διεκπεραιώνει τη μεταφορά των δεδομένων από χρήστη σε χρήστη. Τα δίκτυα αισθητήρων χρησιμοποιούν απλά πρωτόκολλα ώστε να ελαχιστοποιήσουν τα acknowledgements και τις επαναμεταδόσεις πακέτων.

- Flooding: Ο στόχος μια επίθεσης flooding είναι να εξαντλήσει τους πόρους σε μνήμη του συστήματος του θύματος. Όπως και στο συνηθισμένο TCP SYN flood [Schuba et al., 1997], ο επιτιθέμενος στέλνει πάρα πολλές αιτήσεις για συνδέσεις, αναγκάζοντας το θύμα να ελευθερώσει μνήμη του συστήματος, ώστε να διατηρήσει την κατάσταση της κάθε σύνδεσης.
- Desynchronization: Μια σύνδεση μεταξύ δύο σημείων μπορεί να αποσυγχρονιστεί. Ο επιτιθέμενος (hacker) μπορεί να πλαστογραφεί μεταξύ των δύο σημείων. Control flags και sequence numbers είναι αυτά που συνήθως τροποποιούνται. Εάν ο επιτιθέμενος μπορεί να δει το συγχρονισμό σωστά, τότε έχει την δυνατότητα να εμποδίσει τα δύο σημεία από το να ανταλλάξουν μηνύματα, αφού θα ζητούν συνεχώς την αναμετάδοση των προηγούμενων λανθασμένων μηνυμάτων.

2.8 Αντίμετρα

Στην ενότητα αυτή θα περιγράψουμε κάποια μέτρα αντιμετώπισης των επιθέσεων που αναφέρθηκαν στην προηγούμενη ενότητα. Αυτά τα αντίμετρα δεν έχουν αποδειχτεί πλήρως αποτελεσματικά μέχρι στιγμής και τα περισσότερα δεν έχουν υλοποιηθεί ακόμα σε επίπεδο λογισμικού, υλικού [Wood και Stankovic, 2002; Karlof και Wagner, 2003].

- Παρεμβολές: Υπάρχουν πολλές ελλιπείς λύσεις για το πρόβλημα των παρεμβολών. Η spread spectrum επικοινωνία μπορεί να είναι ένα προσωρινό αντίμετρο, ως ότου υπολογίσουν οι jammers πώς να ακολουθήσουν την ακριβή hopping ακολουθία ή πώς να φράξουν (jam) ένα ευρύτερο μέρος της ζώνης. Το code spreading, παρόμοιο με αυτό που χρησιμοποιείται στην κινητή τηλεφωνία, πιθανότατα μπορεί να λύσει το πρόβλημα, αλλά απαιτεί καλύτερες προσπάθειες σχεδίασης, μεγαλύτερες δαπάνες και περισσότερη ενέργεια.
- Πλαστογραφίες (Tampering): Ένας τρόπος άμυνας περιλαμβάνει το λεγόμενο tamper-proofing του κάθε κόμβου. Η επιτυχία αυτής της μεθόδου εξαρτάται από το πόσο καλά οι σχεδιαστές εξέτασαν τις πιθανές απειλές κατά τη διάρκεια σχεδίασης του δικτύου, τους πόρους που διατέθηκαν για το σχέδιο, την κατασκευή και τη δοκιμή, την ευφυΐα του επιτιθέμενου. Όταν είναι δυνατό, ο κόμβος πρέπει να αντιδράσει στο tampering κατά ένα fail-complete τρόπο. Θα μπορούσε, παραδείγματος χάριν, να σβήσει την μνήμη του προγράμματος. Άλλες παραδοσιακές φυσικές υπερασπίσεις περιλαμβάνουν το καμουφλάζ ή το κρύψιμο κόμβων.
- Συγκρούσεις (collision): Η ανίχνευση των συγκρούσεων είναι η προφανής λύση εδώ, εντούτοις δεν έχει αποδειχθεί ακόμα τίποτα απολύτως αποτελεσματικό. Κάποιος μπορεί να επιλέξει να χρησιμοποιήσει τους κώδικες διόρθωσης λαθών, εντούτοις αυτοί μπορούν να αλλοιωθούν εύκολα και να απαιτήσουν πρόσθετα overhead bits.
- Unfairness: Ένας τρόπος άμυνας είναι η χρήση μικρών πλαισίων, που σημαίνει ότι το κανάλι μπορεί να δεσμευτεί από έναν κόμβο μόνο για ένα μικρό χρονικό διάστημα. Ένας επιτιθέμενος εντούτοις μπορεί να εξαπατήσει αυτό τον τρόπο άμυνας, με το να αποκριθεί γρήγορα κατά την ανάγκη πρόσβασης, ενώ όλοι οι άλλοι κόμβοι καθυστερούν.
- Εξάντληση πόρων (Exhaustion): Οι τεχνική time division multiplexing μπορεί να λύσει το πρόβλημα των αόριστων αναβολών κατά την διάρκεια των συγκρούσεων. Ο περιορισμός του ρυθμού (rate limiting) του MAC admission control είναι ένα μέτρο με το οποίο το στρώμα διασύνδεσης δεδομένων μπορεί

να αγνοήσει υπερβολικά αιτήματα, χωρίς να χρειάζεται να στείλει ράδιο μηνύματα.

- Neglect and greed: Η χρησιμοποίηση πολλαπλών διαδρομών δρομολόγησης, ή η αποστολή περιττών μηνυμάτων, μπορεί να μειώσει την επίδραση αυτής της επίθεσης, με το να καταστήσει απαραίτητο για έναν επιτιθέμενο να υπονομεύσει περισσότερους κόμβους αισθητήρων. Η διαφοροποίηση ενός greedy κόμβου από έναν αποτυχημένο κόμβο μπορεί να είναι δύσκολη, εντούτοις, έτσι η πρόληψη είναι ασφαλέστερη από το να βασίζεται κάποιος στην ανίχνευση.
- Homing: Μια αμυντική προσέγγιση είναι να κρύψουμε τους σημαντικούς για το δίκτυο κόμβους. Αυτό μπορεί να γίνει με το να παρέχουμε εμπιστευτικότητα στις επικεφαλίδες και το κυρίως κείμενο των μηνυμάτων. Εάν όλοι οι γειτονικοί κόμβοι χρησιμοποιούν κρυπτογραφικά κλειδιά, τότε το δίκτυο μπορεί να κρυπτογραφήσει τις επικεφαλίδες σε κάθε hop. Αυτό θα απέτρεπε έναν παθητικά επιτιθέμενο από το να μάθει εύκολα για την πηγή ή τον προορισμό των overhead μηνυμάτων, υποθέτοντας πάντα ότι ο κόμβος δεν έχει υπονομευτεί και διατηρεί στην κατοχή του έγκυρα κλειδιά αποκρυπτογράφησης.
- Misdirection: Με την επαλήθευση της προέλευσης των διευθύνσεων, οι δρομολογητές γονέων (parent routers) μπορούν να ελέγξουν ότι όλα τα πακέτα που δρομολογούνται κάτω από αυτούς, θα μπορούσαν να έχουν δημιουργηθεί νόμιμα από τα παιδιά τους.
- Black holes: Παρότι οι κόμβοι μπορούν να ανιχνεύσουν μια black hole επίθεση ευκολότερα από ότι μπορούν να ανιχνεύσουν τις greed, neglect, ή misdirection επιθέσεις, μια επίθεση black hole είναι πιο διασπαστική. Άλλοι κόμβοι με γνώση της τοπολογίας του δικτύου μπορούν να υποψιαστούν τις ανακόλουθες διαφημίσεις διαδρομών.
- Flooding: Τα client puzzles είναι ένας τρόπος ώστε να μειωθεί η σφοδρότητα με την οποία γίνεται μια επίθεση flooding, ζητώντας από όλους τους κόμβους πελατών να περιγράψουν τις απαιτήσεις τους σε πόρους που χρειάζονται. Ο κεντρικός υπολογιστής (server) διανέμει έναν γρίφο με κάθε αίτημα σύνδεσης, το οποίο ο πελάτης πρέπει να λύσει προκειμένου να δημιουργηθεί μια σύνδεση. Ο επιτιθέμενος πρέπει τώρα να χρησιμοποιήσει περισσότερη ενέργεια για να

πλημμυρίσει το δίκτυο. Το μειονέκτημα τώρα είναι ότι νόμιμοι κόμβοι πρέπει να χρησιμοποιήσουν πρόσθετους πόρους για να συνδεθούν.

- Desynchronization: Ένας τρόπος αντιμετώπισης αυτού του είδους επιθέσεων είναι η αυθεντικοποίηση (authentication) όλων των πακέτων που ανταλλάσσονται μεταξύ των δύο σημείων, συμπεριλαμβανομένων όλων των control fields στο transport protocol header. Υποθέτοντας ότι ο επιτιθέμενος δε μπορεί να πλαστογραφήσει το μηχανισμό αυθεντικοποίησης, τα end points του δικτύου μπορούν να ανιχνεύσουν και να αγνοήσουν τα κακόβουλα πακέτα.

Network Layer	Επιθέσεις	Αντίμετρα
Φυσικό επίπεδο	Παρεμβολές	Χρήση spread spectrum
	Πλαστογραφίες (Tampering)	Δημιουργία κόμβων ανθεκτικών σε πλαστογραφίες, κρύψιμο κόμβων
Στρώμα ζεύξης δεδομένων	Συγκρούσεις (collisions)	Κώδικες διόρθωσης λαθών
	Εξάντληση πόρων	Rate limiting
	Unfairness	Small frames
Επίπεδο δικτύου	Neglect and greed	Redundancy, probing
	Homming	Encryption
	Misdirection	Egress filtering, authorization, monitoring
	Black holes	Authorization, monitoring, redundancy
Επίπεδο μεταφοράς	Flooding	Client puzzles
	Desynchronization	Authentication

Πίνακας 2: Επίπεδα ασύρματου δικτύου αισθητήρων και DoS επιθέσεις

Σε αυτό το κεφάλαιο παρουσιάσαμε τους πιθανούς τρόπους επίθεσης σε ένα ασύρματο δίκτυο αισθητήρων, βασισμένους στα εργαλεία που οι επιτιθέμενοι έχουν στη διάθεσή τους. Ένας επιτιθέμενος μπορεί να έχει πρόσβαση μόνο σε μερικούς κόμβους που έχει παραβιάσει. Ένας τέτοιος επιτιθέμενος μπορεί να ταξινομηθεί ως node attacker. Εναλλακτικά ένας επιτιθέμενος μπορεί να έχει πρόσβαση σε ισχυρότερες συσκευές όπως είναι τα laptops, ως εκ τούτου και ο καθορισμός του σαν laptop attacker. Τέτοιοι επιτιθέμενοι έχουν CPUs μεγάλης ισχύος, μεγάλης διάρκειας μπαταρίες, συσκευή αποστολής σημάτων υψηλής ισχύος και τις ευαίσθητες κεραίες στη διάθεσή τους και αποτελούν πολύ μεγαλύτερη απειλή για το δίκτυο. Παραδείγματος χάριν, μερικοί κόμβοι μπορούν να μπλοκάρουν μερικές ράδιο συνδέσεις, ενώ ένα laptop μπορεί να μπλοκάρει ολόκληρο το δίκτυο.

Τέλος, οι επιθέσεις που γίνονται σε ένα δίκτυο μπορούν να είναι εσωτερικές ή εξωτερικές επιθέσεις. Σε μια εξωτερική επίθεση ο επιτιθέμενος δεν έχει καμία ειδική πρόσβαση στο δίκτυο. Στις εσωτερικές επιθέσεις ο επιτιθέμενος θεωρείται εξουσιοδοτημένος συμμετέχων του δικτύου. Τέτοιες επιθέσεις είτε εκτελούνται από τους κόμβους αισθητήρων που έχουν παραβιαστεί και τρέχουν κακόβουλο λογισμικό είτε από υπολογιστές (laptop) χρησιμοποιώντας κλεμμένα στοιχεία (κρυπτογραφικά κλειδιά & κώδικα) από τους νόμιμους κόμβους.

2.9 Στόχοι ασφάλειας

Εξετάζοντας την ασφάλεια ενός ασύρματου δικτύου αισθητήρων, ο καθένας βρίσκεται αντιμέτωπος με την επίτευξη μερικών ή όλων από τους παρακάτω στόχους:

- Διαθεσιμότητα (Availability): Τα στοιχεία του δικτύου πρέπει να είναι διαθέσιμα στους εξουσιοδοτημένους χρήστες όποτε τα χρειάζονται και το δίκτυο αισθητήρων πρέπει να εξασφαλίσει τη διαθεσιμότητα των υπηρεσιών του δικτύου, παρά τις επιθέσεις άρνησης υπηρεσιών (Denial of service attack - DoS). Για να εξασφαλίσει τη διαθεσιμότητα της προστασίας των μηνυμάτων, το δίκτυο αισθητήρων πρέπει επίσης να προστατεύσει τους πόρους ώστε να ελαχιστοποιήσει την κατανάλωση ενέργειας [Hu και Sharma, 2005].

- Εμπιστευτικότητα (Confidentiality): Ένα δίκτυο αισθητήρων δεν πρέπει να διαρρεύσει τις πληροφορίες, που συλλέγονται από τους αισθητήρες, σε άλλα δίκτυα. Συνήθως οι κόμβοι ανταλλάσουν ευαίσθητα στοιχεία μεταξύ τους. Προκειμένου να προστατευθούν αυτά τα σημαντικά στοιχεία, κρυπτογραφούνται με ένα μυστικό κλειδί που μόνο οι παραλήπτες των μηνυμάτων το έχουν. Επιπλέον, δημιουργούνται ασφαλή κανάλια επικοινωνίας μεταξύ των κόμβων και των σταθμών βάσεων.
- Αυθεντικοποίηση (Authentication): Δεδομένου ότι ένας επιτιθέμενος μπορεί εύκολα να τροποποιήσει τα μηνύματα, πρέπει να υπάρξει ένας τρόπος που να βεβαιώνει το δέκτη για την προέλευση των δεδομένων. Με την αυθεντικοποίηση των στοιχείων επιτρέπουμε στο δέκτη, να ελέγξει ότι τα στοιχεία εστάλησαν από συγκεκριμένο αποστολέα. Σε περίπτωση επικοινωνίας δύο σημείων, ο αποστολέας και ο δέκτης μπορούν να μοιραστούν ένα μυστικό κλειδί. Αλλά αυτή η μέθοδος δε μπορεί να χρησιμοποιηθεί σε broadcast αναμετάδοση, όπου καθένας μπορεί να υποδυθεί τον αποστολέα και να στείλει τα μηνύματα σε άλλους δέκτες.
- Ακεραιότητα (Integrity): Εξασφαλίζεται ότι τα δεδομένα δεν έχουν τροποποιηθεί με μη εξουσιοδοτημένο τρόπο κατά τη μετάδοση τους.
- Πρόσφατα δεδομένα (Freshness): επιβεβαιώνει ότι τα δεδομένα είναι πρόσφατα και εξασφαλίζει ότι από κανέναν επιτιθέμενο δε θα επαναληφθούν παλιότερα μηνύματα.
- Εξελιξιμότητα (Scalability): τα δίκτυα αισθητήρων δε μπορούν να χρησιμοποιήσουν ένα σχέδιο διαμόρφωσης κλειδιών, το οποίο έχει μικρές δυνατότητες εξελιξιμότητας, με βάση το κόστος ενέργειας ή τη λανθάνουσα κατάσταση. Γενικά, ο αριθμός των γειτονικών κόμβων και της απόστασης, ή η δύναμη που απαιτείται για να σταλούν τα μηνύματα από τον έναν κόμβο στον άλλο, δε θα είναι γνωστά εκ των προτέρων.

Υπάρχει ένα αντικρουόμενο ενδιαφέρον στην ασφάλεια ενός δικτύου αισθητήρων, μεταξύ της ελαχιστοποίησης της κατανάλωσης πόρων των κόμβων αισθητήρων και της μεγιστοποίησης της ασφάλειας του δικτύου. Οι πόροι σε αυτό το περιβάλλον περιλαμβάνουν κυρίως την ενέργεια, καθώς επίσης και τους υπολογιστικούς πόρους, όπως είναι η μνήμη που έχει ο κάθε κόμβος. Οι δυνατότητες και οι περιορισμοί των κόμβων αισθητήρων επηρεάζουν σε μεγάλο βαθμό τους μηχανισμούς ασφάλειας, που μπορούν να φιλοξενηθούν σε μια πλατφόρμα κόμβων αισθητήρων. Η ενέργεια είναι ίσως ο μεγαλύτερος περιορισμός στις δυνατότητες των κόμβων αισθητήρων. Η πρόσθετη ενέργεια που θα χρησιμοποιηθεί από τους κόμβους αισθητήρων μπορεί να οφείλεται σε διάφορες λειτουργίες ασφάλειας, όπως η κρυπτογράφηση, η αποκρυπτογράφηση, η ταυτοποίηση δεδομένων, ή η αποθήκευση κλειδιού. Η προστασία από επιθέσεις πλαστογραφήσεων είναι ένα επιπλέον κόστος για κάθε κόμβο.

Κατά το σχεδιασμό της αρχιτεκτονικής ασφάλειας των δικτύων αισθητήρων πρέπει να υποθέσουμε, ότι ένας ή περισσότεροι κόμβοι αισθητήρων μέσα στο δίκτυο μπορούν να παραβιαστούν (compromised). Λόγω της έλλειψης προστασίας από τις πλαστογραφήσεις στους κόμβους αισθητήρων, ένας αρκετά ικανός αντίπαλος μπορεί να εξάγει τις κρυπτογραφικές πληροφορίες από έναν κόμβο αισθητήρων. Οι τεχνολογίες ανίχνευσης πλαστογραφήσεων, μπορούν να παρέχουν την ένδειξη ότι έγινε μια επίθεση πλαστογραφίας, αλλά έχουν περιορισμένη αξία σε μεγάλης διάρκειας και χωρίς συντήρηση λειτουργίες [Akyildiz et al., 2002b].

Η ad hoc τοπολογία δικτύωσης καθιστά ένα δίκτυο αισθητήρων ευάλωτο στις επιθέσεις συνδέσεων. Αντίθετα από τα ενσύρματα δίκτυα με τους μηχανισμούς άμυνας, όπως είναι τα firewalls και τα gateways, οι επιθέσεις στα δίκτυα αισθητήρων μπορούν να προέλθουν από όλες τις κατευθύνσεις και να στοχεύσουν σε οποιοδήποτε κόμβο. Δεδομένου ότι είναι δύσκολο να εντοπιστεί ένας συγκεκριμένος κινητός κόμβος σε ένα μεγάλης κλίμακας δίκτυο αισθητήρων, οι επιθέσεις από έναν παραβιασμένο κόμβο είναι πιο επικίνδυνες και πολύ πιο δύσκολο να ανιχνευτούν. Όλο αυτό δείχνει ότι οποιοσδήποτε κόμβος πρέπει να είναι προετοιμασμένος για να λειτουργήσει με έναν τρόπο σύμφωνα με τον οποίο δε θα εμπιστεύεται κανέναν άλλον κόμβο. Νέοι κόμβοι μπορούν να προστεθούν ή οι τρέχοντες κόμβοι μπορούν να αφαιρεθούν. Κατά συνέπεια ένα δίκτυο αισθητήρων έχει μια δυναμική δομή δρομολόγησης. Οι συχνές αλλαγές δρομολόγησης μπορούν να σημάνουν ότι οι ενδιάμεσοι κόμβοι που επεξεργάζονται τα

στοιχεία για μια σύνδεση σημείο προς σημείο μπορούν να αλλάξουν. Επίσης, δεδομένου ότι πολλές υπηρεσίες ασφάλειας θα λειτουργούν σε μια βάση «κόμβος με κόμβο», η διαδικασία κρυπτογράφησης θα εμφανιστεί ανάμεσα στους γειτονικούς κόμβους στην τοπολογία δρομολόγησης.

Εάν γίνουν αλλαγές δρομολόγησης, το σύνολο των τοπικών γειτονικών κόμβων μπορεί να αλλάξει και έτσι η διαδικασία κρυπτογράφησης μπορεί να πρέπει να επαναληφθεί. Εξετάζοντας έναν μεγάλο αριθμό κόμβων σε ένα χαρακτηριστικό δίκτυο αισθητήρων, δεν είναι πρακτικό να χρησιμοποιηθούν συγκεντρωτικά μέτρα ασφάλειας. Η εισαγωγή οποιασδήποτε κεντρικής οντότητας στην ασφάλεια των κόμβων, μπορεί να προκαλέσει μια επίθεση σε ολόκληρο δίκτυο, μόλις παραβιαστεί η κεντρική οντότητα. Γενικά, η λήψη αποφάσεων σε ένα δίκτυο αισθητήρων αποκεντρώνεται και πολλοί αλγόριθμοι ασφάλειας στηρίζονται στη συνεργασία όλων των κόμβων ή μερικών κόμβων. Η φύση της ad hoc δικτύωσης απαιτεί περιορισμένη αρχική διαμόρφωση, προκειμένου να υποστηριχθεί ένα ευέλικτο και εύκολα αναπτυσσόμενο δίκτυο. Έτσι περιορίζεται ο τύπος των κρυπτογραφικών σχεδίων που πρέπει να είναι απαραίτητα ώστε να δημιουργηθεί ένα ασφαλές δίκτυο αισθητήρων. Οι κόμβοι αισθητήρων μπορούν να είναι χωρίς συντήρηση για μεγάλες χρονικές περιόδους. Για παράδειγμα, οι μακρινές αποστολές αναγνώρισης πίσω από τις εχθρικές γραμμές, μπορούν να μην έχουν οποιαδήποτε φυσική επαφή με τις φιλικές δυνάμεις μόλις αναπτυχθούν. Αν και μπορούν να ρυθμιστούν από απόσταση, γενικά οι κόμβοι αισθητήρων δεν έρχονται σε φυσική επαφή με τα επίγεια στρατεύματα μόλις επεκταθούν. Αυτό καθιστά αδύνατη τη φυσική ανίχνευση της πλαστογραφίας και φυσικής συντήρησης (π.χ., αντικατάσταση μπαταριών). Άλλες λειτουργίες συντήρησης είναι δυνατές (π.χ., αναπροσαρμογές λογισμικού, ενημέρωση κλειδιού), αλλά πρέπει να γίνουν απομακρυσμένα. Το χρονικό διάστημα για το οποίο ένας αισθητήρας αφήνεται χωρίς συντήρηση, αυξάνει την πιθανότητα ένας αντίπαλος να τον έχει παραβιάσει [Hu και Sharma, 2005].

2.10 Περίληψη

Στο κεφάλαιο αυτό ορίσαμε την έννοια ασύρματο δίκτυο αισθητήρων. Αναλύσαμε τα κυριότερα χαρακτηριστικά τους και περιγράψαμε κάποιες εφαρμογές που απαιτούν αυστηρά επίπεδα ασφάλειας για τα ασύρματα δίκτυα αισθητήρων. Στη συνέχεια αναφερθήκαμε σε ένα γενικό μοντέλο WSN περιγράφοντας τα σημαντικότερα συστατικά ενός χαρακτηριστικού δικτύου αισθητήρων. Επιπλέον δείξαμε τη δομή λειτουργίας ενός τέτοιου δικτύου αλλά και τη δομή ενός μεμονωμένου κόμβου αισθητήρα. Σε μια ενότητα αναλύθηκαν τα πρωτόκολλα επικοινωνίας που χρησιμοποιούν οι κόμβοι αισθητήρων και ο στόχος του κάθε στρώματος (layer). Επιπλέον έγινε αναφορά στις σημαντικότερες προκλήσεις στην αντιμετώπιση της ασφάλειας των δικτύων αισθητήρων. Στην ενότητα 2.7 αναλύθηκαν οι επιθέσεις άρνησης υπηρεσιών που γίνονται σε κάθε στρώμα του πρωτοκόλλου των WSN, ενώ στην αμέσως επόμενη ενότητα αναφέρθηκαν κάποια μέτρα αντιμετώπισης αυτών των επιθέσεων. Στο τέλος του κεφαλαίου αναφέρθηκαν κάποιοι στόχοι που πρέπει να μελετηθούν κατά την εξέταση του θέματος ασφάλεια των ασύρματων δικτύων αισθητήρων. Στο κεφάλαιο που ακολουθεί θα ασχοληθούμε με την έννοια της θεωρίας των παιγνίων.

3 Θεωρία Παιγνίων

3.1 Εισαγωγή

Η Θεωρία των Παιγνίων (Game Theory) αποτελεί ένα παρακλάδι των εφαρμοσμένων μαθηματικών και των οικονομικών επιστημών, που μελετά καταστάσεις στις οποίες πολλοί παίκτες παίρνουν αποφάσεις, με σκοπό να βελτιώσει ο κάθε παίκτης τη θέση του σε σχέση με τους υπόλοιπους παίκτες [Dutta, 1999].

Η πρώτη αναφορά στη Θεωρία των Παιγνίων έγινε από τον John Von Neumann το 1928 και στη συνέχεια το 1944 στο βιβλίο του Theory of Games and Economic Behavior που συνέγραψε με τον Oskar Morgenstern. Αργότερα, το 1950, ο John Nash όρισε πρώτος την έννοια της «βέλτιστης» στρατηγικής για παίγνια πολλών παικτών, γνωστή ως Nash Equilibrium - NE (Nash Ισορροπία). Για την εργασία του αυτή ο αμερικάνος μαθηματικός τιμήθηκε με το βραβείο Nobel οικονομίας. Πολλά χρόνια μετά, το 1994, μοιράστηκε το βραβείο Nobel με τους John Harsanyi και Reinhard Selten, για τη συμβολή τους στη θεωρία των παιγνίων μη συνεργασίας (non-cooperative game theory), με την ανάλυση των σημείων ισορροπίας (equilibria).

Η θεωρία των παιγνίων έχει εφαρμογές σε κοινωνικές, πολιτικές, οικονομικές επιστήμες καθώς και στην τεχνητή νοημοσύνη. Μελέτες βασισμένες σε παίγνια έχουν γίνει από μια ποικιλία ανθρώπων, όπως για παράδειγμα από τους Myerson (1991) και Kreps (1990) στα οικονομικά, τους Ordeshook (1986), Shubik (1982), και Taylor (1995) στην πολιτική, τον Berne (1964) στην ψυχολογία, τον Smith (1982) στη στατιστική ή τους Girshick (1954) and Ferguson (1968) στην στατιστική.

Υπάρχουν ποικίλα παραδείγματα από την καθημερινή ζωή που δείχνουν την σημαντικότητα των παιγνίων. Τα παίγνια μπορούν να χρησιμοποιηθούν στους Ολυμπιακούς αγώνες είτε από τους αθλητές είτε από την Διεθνή Ολυμπιακή Επιτροπή (ΔΟΕ). Οι αθλητές θα πρέπει να αποφασίσουν εάν θα πάρουν αναβολικά προκειμένου να αυξήσουν τις πιθανότητες νίκης ή όχι για να μην αποκλειστούν από την διοργάνωση.

Αντίστοιχα η ΔΟΕ θα πρέπει να ελέγχει ποιοί αθλητές έχουν πάρει αναβολικά και να επιβάλλει τις ανάλογες ποινές. [Dutta, 1999]

Είναι γνωστή η χρησιμότητα των παιγνίων στα οικονομικά και στη βιολογία. Οι φαρμακευτικές εταιρείες χρησιμοποιούν τα παίγνια για να καθορίσουν την τιμή των προϊόντων τους αλλά και τις επιδράσεις των φαρμάκων στους ασθενείς. Οι δε βιολόγοι ορίζουν τα ζώα ως παίκτες για να δουν πως αλληλεπιδρούν μεταξύ τους και να αποφύγουν την εξαφάνιση των ειδών.

Πρέπει να σημειωθεί ότι, το ιδιαίτερο χαρακτηριστικό της Θεωρίας των Παιγνίων είναι ότι μελετά καταστάσεις στις οποίες οι παίκτες αλληλεπιδρούν μεταξύ τους. Τα παίγνια είναι καλά καθορισμένα μαθηματικά αντικείμενα στη θεωρία των παιγνίων. Ένα παίγνιο αποτελείται από ένα σύνολο παικτών που αλληλεπιδρούν μεταξύ τους, ένα σύνολο κανόνων, ένα σύνολο στρατηγικών και το όφελος ή την απώλεια για κάθε καθορισμένη στρατηγική.

3.2 Τρόποι περιγραφής των παιγνίων

Ένα παίγνιο μπορεί να αναπαρασταθεί είτε με στρατηγική / κανονική μορφή (normal / strategic form) ως πίνακας, είτε με εκτεταμένη μορφή ως δένδρο (extensive form) [Dutta, 1999]. Από μια εκτεταμένη μορφή ενός παιγνίου προκύπτει μόνο μια στρατηγική μορφή. Αντίθετα, σε μια στρατηγική μορφή ενός παιγνίου μπορεί να αντιστοιχούν περισσότερες από μια εκτεταμένες μορφές. Στη συνέχεια θα εξηγήσουμε αναλυτικά την εκτεταμένη και τη στρατηγική μορφή των παιγνίων.

Εκτεταμένη μορφή παιγνίου

Η εκτεταμένη ή αλλιώς δενδροειδής μορφή ενός παιγνίου θα πρέπει να μας δίνει κάποιες πληροφορίες σχετικά με τους παίκτες και τις επιλογές τους. Έτσι ένα δένδρο [Dutta, 1999]:

1. Περιγράφει τι διαθέσιμες επιλογές των παικτών που πρόκειται να κινηθούν (actions, moves).

2. Περιγράφει τη σειρά των κινήσεων (order of moves).
3. Περιγράφει το είδος της πληροφόρησης (information). Για παράδειγμα η εκτεταμένη μορφή καταδεικνύει αν οι παίκτες κινούνται διαδοχικά η ταυτόχρονα.

Ένα δένδρο παίγνιο αποτελείται από [Dutta, 1999]:

- Κόμβους Αποφάσεων (decision nodes)
- Κλαδιά (branches)
- Αποδόσεις (payoffs)

Υπάρχουν κάποιοι βασικοί κανόνες με βάση τους οποίους δημιουργείται ένα παίγνιο. Στην εκτεταμένη μορφή των παιγνίων θα πρέπει να ακολουθούνται οι παρακάτω κανόνες [Dutta, 1999]:

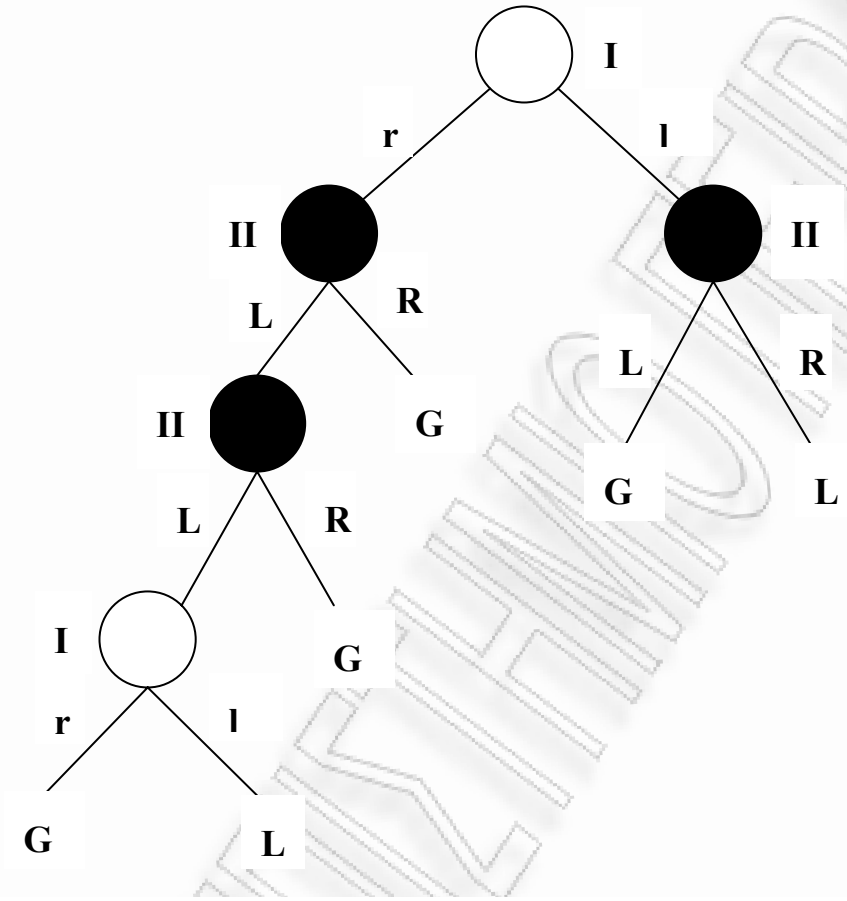
- Κάθε κόμβος προέρχεται από έναν μόνο κόμβο.
- Από κάθε κόμβο προσεγγίζεται ένας μόνο κόμβος.
- Απαγορεύονται οι κυκλικές δενδρομορφίες.
- Εάν κάποιος παίκτης γνωρίζει κάτι για την επιλογή του αντιπάλου του, τότε ο κόμβος απόφασης του αντιπάλου, θα πρέπει να προηγείται στο δένδρο παιγνίου, του κόμβου απόφασης του συγκεκριμένου παίκτη.

Παράδειγμα δένδρου – παιγνίου (game tree) [Carmichael, 2004]

Το πιο απλό παίγνιο που υπάρχει είναι το zero-sum game (παιχνίδι μηδενικού αθροίσματος). Παίγνιο μηδενικού αθροίσματος είναι το παίγνιο όπου ένα παίκτης κερδίζει και ο άλλος χάνει το αντίστοιχο του κέρδους του πρώτου. Πληρώνει δηλαδή ο ένας τον άλλο. Σε αυτά τα παίγνια, όπου το άθροισμα των αποτελεσμάτων είναι μηδέν, δε χρειάζεται να έχουμε δύο νούμερα, γιατί ό,τι κερδίζει ο ένας, το χάνει ο άλλος. Οπότε μπορούμε να το απλοποιήσουμε.

Ας υποθέσουμε ότι έχουμε δύο παίκτες τους (I) και (II). Ο παίκτης I παίζει πρώτος και έχει δύο επιλογές στη διάθεση του, l και r, κατόπιν ακολουθεί ο παίκτης II, όπου και

αυτός έχει δύο επιλογές, R και L. Τα αποτελέσματα του παιγνίου είναι G (Gain) και L (Lose). Το G (αφού μιλάμε για zero-sum game) σημαίνει ότι, ό,τι κερδίζει ο πρώτος παίκτης, το χάνει ο δεύτερος, ενώ το L σημαίνει ότι ο πρώτος παίκτης χάνει και κερδίζει ο δεύτερος.



Εικόνα 5: Παράδειγμα δένδρου – παιγνίου (game tree)

Αν το παιχνίδι συνεχίσει, αποφασίζει ο παίκτης ΙΙ μεταξύ L και R. Αν αποφασίσει R, χάνει αυτός και κερδίζει ο πρώτος παίκτης, ενώ αν αποφασίσει L, ξαναπαίζει ο παίκτης ΙΙ.

Στο συγκεκριμένο παράδειγμα που παρουσιάζουμε στην εικόνα 6, έχουμε δύο παίκτες τους Ι και ΙΙ. Πρώτα παίζει ο Ι, μετά ο ΙΙ, μετά ξαναπαίζει ο ΙΙ και στη συνέχεια τελειώνει το παιχνίδι ο Ι. Όπως βλέπουμε και οι δύο παίκτες έχουν από δύο επιλογές κάθε φορά που παίζουν. Θα μπορούσαμε για παράδειγμα να προσθέσουμε και μια τρίτη ενδιάμεση επιλογή.

Στρατηγική μορφή παιγνίου

Ένας δεύτερος τρόπος περιγραφής παιγνίου είναι η στρατηγική μορφή. Σε αυτή παρουσιάζονται όλες οι δυνατές στρατηγικές κάθε παίκτη και δηλώνονται οι αμοιβές ή απώλειες των παικτών, οι οποίες είναι αποτέλεσμα όλων των εναλλακτικών συνδυασμών των στρατηγικών που επιλέγουν. Στη στρατηγική μορφή δεν εμφανίζεται η χρονική στιγμή, δεν γνωρίζουμε δηλαδή ποιος παίκτης είναι πρώτος, ποιος είναι δεύτερος, αν παίζουν ταυτόχρονα ή διαδοχικά.

Η στρατηγική μορφή ενός παιγνίου αποτελείται από τα παρακάτω στοιχεία [Osborne, 2004]:

1. Ένα σύνολο παικτών (players).
2. Τις στρατηγικές (strategies) των παικτών, οι οποίες αποτελούν ένα πλήρες σχέδιο κάθε παίκτη για το παίγνιο, δηλαδή, ένα σύνολο οδηγιών για το τι θα κάνει κάθε παίκτης κάθε φορά που καλείται να κινηθεί.
3. Τα αποτελέσματα κάθε «παρτίδας» (payoffs). Κάτι που παίζεται και φτάνει σε ένα σημείο, τελειώνει και όταν τελειώνει παίρνει ο καθένας το μερίδιο του, δηλαδή, το τίμημα των επιλογών του στο παιχνίδι.

Η στρατηγική μορφή μπορεί να απεικονιστεί με έναν πίνακα, στον οποίο οι σειρές αντιστοιχούν στις στρατηγικές του ενός παίκτη, ενώ οι στήλες αντιστοιχούν στις στρατηγικές του άλλου παίκτη. Σε κάθε κελί του πίνακα γράφονται οι αποδόσεις που σχετίζονται με το αντίστοιχο ζευγάρι στρατηγικών.

Για παράδειγμα, ας υποθέσουμε ότι είμαστε σε ένα πολύ απλό παιχνίδι με δύο παίκτες: τους 1 και 2.

Ο παίκτης (1) έχει τις στρατηγικές Α και Β, ενώ ο παίκτης (2) τις C και D. Στον πίνακα μπαίνουν επίσης τα αποτελέσματα της κάθε στρατηγικής. Στο κάθε κελί του πίνακα χρειαζόμαστε δύο νούμερα-αποδόσεις: π.χ. το τι πετυχαίνει ο παίκτης (1) όταν ακολουθεί τη στρατηγική Α, τη στιγμή που ο παίκτης (2) ακολουθεί τη στρατηγική C. Το πρώτο παριστάνει το τι πετυχαίνει ο παίκτης (1), ενώ το δεύτερο το τι πετυχαίνει ο παίκτης (2). Έτσι για παράδειγμα, στη στρατηγική μορφή του παιγνίου που παρουσιάζεται στον πίνακα 3, το (7, 9) μας δίνει το αποτέλεσμα όταν οι στρατηγικές είναι Α και C.

		2	
		C	**D**
1	**A**	7 , 9	3 , 10
	B	9 , 20	0 , 7

Πίνακας 3: Στρατηγική μορφή παιγνίου με δύο παίκτες

Ένα από τα συχνότερα παραδείγματα που βρίσκουμε στην βιβλιογραφία παιγνίων είναι το λεγόμενο δίλημμα των φυλακισμένων (Prisoner's Dilemma). Αναλυτικά το παίγνιο έχει ως εξής [Binmore, 2007b]:

Δύο φυλακισμένοι, ο παίκτης 1 και ο παίκτης 2, έχουν συλληφθεί ως ύποπτοι για ένα έγκλημα. Ο εισαγγελέας μιλάει στον καθένα χωριστά και τους λέει ότι έχει στοιχεία για να τους καταδικάσει, αλλά μπορούν να κάνουν τη δουλειά του λίγο ευκολότερη (και να βοηθήσουν τους εαυτούς τους), εάν ομολογήσουν ότι έκαναν το έγκλημα. Προσφέρει λοιπόν και στους δύο την παρακάτω συμφωνία: «Ομολόγησε (c) το έγκλημα και ενοχοποίησε τον άλλο τύπο και δεν θα κάνεις φυλακή. Φυσικά, η ομολογία σου θα αξίζει αρκετά λιγότερο αν και ο άλλος τύπος ομολογήσει. Σε αυτή την περίπτωση, θα κάνετε και οι δύο 5 χρόνια φυλακή. Εάν δεν ομολογήσεις (n) όμως, ενώ ο άλλος ομολογήσει, θα σε καταδικάσουμε σε δεκαπέντε χρόνια φυλάκισης. Στην περίπτωση που δεν θα αποσπάσω ομολογία από κανέναν από τους δυο σας, θα έχω αρκετά στοιχεία ώστε να σας καταδικάσω και τους δυο σε ένα χρόνο φυλάκισης.

Στο παρακάτω πίνακα 4 οι αποδόσεις αντιστοιχούν σε έτη φυλάκισης. Οι αποδόσεις δείχνουν χρησιμότητα και άρα για τα έτη φυλάκισης βάζουμε αρνητικό πρόσημο. Όταν και οι δύο παίκτες ομολογούν (c, c) μοιράζονται την ποινή και φυλακίζονται για 5 χρόνια ο καθένας (-5, -5). Στην περίπτωση που μόνο ο ένας παίκτης ομολογήσει (c, n) ή (n, c), τότε αυτός θα αφεθεί ελεύθερος ενώ ο άλλος θα εκτίσει 15 έτη φυλάκισης (0, -15) (-15, 0). Τέλος εάν και οι δύο παίκτες αρνηθούν να ομολογήσουν (n, n) θα καταδικαστούν σε ένα χρόνο φυλάκισης (-1, -1).

		2	
		c	**n**
1	**c**	-5 , -5	0 , -15
	n	-15 , 0	-1 , -1

Πίνακας 4: Στρατηγική μορφή παιγνίου (Prisoner's Dilemma)

Αν και το καλύτερο αποτέλεσμα θα προέκυπτε στην ισορροπία (n, n), κάθε παίκτης θεωρεί πως είναι προς το συμφέρον του να ομολογήσει, σκεπτόμενος πως ο άλλος παίκτης δεν θα ομολογήσει. Έτσι κάθε παίκτης θα θέλει να βρεθεί στην ισορροπία (c, n) προκειμένου να μην φυλακιστεί καθόλου και να εκτίσει ο άλλος παίκτης όλα τα έτη φυλάκισης. Συνεπώς και οι δυο παίκτες τελικά θα ομολογήσουν και θα καταδικαστούν σε πέντε έτη φυλάκισης ο καθένας.

3.3 Ταξινόμηση των παιγνίων

Στην ενότητα αυτή θα ταξινομήσουμε τα παίγνια σε διάφορες κατηγορίες μέσω ποικίλων κριτηρίων. Καταρχήν μπορούμε να ταξινομήσουμε τα παίγνια σύμφωνα με το εάν η σειρά με την οποία λαμβάνονται οι αποφάσεις παίζει ρόλο ή όχι. Μια ταξινόμηση μπορεί επίσης να βασίζεται στο κατά πόσο οι παίκτες πριν παίξουν το παίγνιο μπορούν να επιτύχουν δεσμευτικές συμφωνίες για τις στρατηγικές. Ένας άλλος τρόπος ταξινόμησης των παιγνίων είναι ως προς το πόσες φορές επαναλαμβάνεται το παίγνιο. Με βάση αυτά και μερικά ακόμη κριτήρια θα καταλήξουμε στην παρακάτω ταξινόμηση παιγνίων [Carmichael, 2004]:

- *Συμμετρικό (symmetric) και ασύμμετρο (non-symmetric):* Σε ένα συμμετρικό παίγνιο, το όφελος εξαρτάται μόνο από τις στρατηγικές που χρησιμοποιούνται και όχι από το ποιος παίζει το παίγνιο. Τα ασύμμετρα παίγνια είναι παίγνια στα οποία οι στρατηγικές δεν είναι ίδιες για όλους τους παίκτες.

- *Zero sum and non-zero sum:* Στα zero sum παίγνια, το συνολικό όφελος σε όλους τους παίκτες στο παίγνιο είναι μηδέν. Όπως στο πόκερ, το κέρδος ενός ανθρώπου είναι η απώλεια κάποιου άλλου. Στα non-zero sum παίγνια, το αποτέλεσμα είναι μικρότερο η μεγαλύτερο από το μηδέν.

- *Ταυτόχρονα (simultaneous) και διαδοχικά (sequential):* Ένα ταυτόχρονο παίγνιο είναι εκείνο όπου οι παίκτες κινούνται συγχρόνως, ή εάν δεν κινούνται ταυτόχρονα, οι παίκτες που κινούνται αργότερα είναι απληροφόρητοι για τις προηγούμενες ενέργειες των άλλων παικτών. Σχηματικά, διαχωρίζουμε τα παίγνια ταυτόχρονων κινήσεων, τοποθετώντας μια διακεκομμένη γραμμή ανάμεσα στους κόμβους απόφασης των παικτών. Τότε λέμε ότι οι κόμβοι αυτοί ανήκουν στο ίδιο σύνολο πληροφόρησης (information set). Στα διαδοχικά παίγνια, οι τελευταίοι παίκτες έχουν κάποια γνώση για τις προηγούμενες ενέργειες των άλλων παικτών.

- *Τέλειας (perfect) και ατελούς (imperfect) πληροφόρησης:* Ένα παίγνιο τέλειας πληροφόρησης είναι αυτό στο οποίο όλοι οι παίκτες γνωρίζουν την ιστορία του παιγνίου, δηλαδή τις κινήσεις που έγιναν προηγουμένως από όλους τους άλλους παίκτες. Ως εκ τούτου, τα παίγνια τέλειας πληροφόρησης μπορούν εξ ορισμού να είναι μόνο διαδοχικά παίγνια. Η πλειοψηφία των παιγνίων παρόλα αυτά είναι παίγνια ατελούς πληροφόρησης. Στα παίγνια αυτά, ένας τουλάχιστον παίκτης δεν έχει τέλεια πληροφόρηση.

- *Πλήρους (complete) και ελλιπούς (incomplete) πληροφόρησης:* Ένα παίγνιο πλήρους πληροφόρησης είναι εκείνο στο οποίο κάθε παίκτης γνωρίζει όλα όσα προσδιορίζουν ένα παίγνιο, συμπεριλαμβανομένων των προτιμήσεων (preferences) και των πιστεύω (beliefs) των άλλων παικτών [Binmore, 2007a]. Ένα παίγνιο ελλιπούς πληροφόρησης, μπορεί να μετασχηματιστεί σε παίγνιο ατελούς πληροφόρησης (μετασχηματισμός Harsavy). Το αντίστροφο όμως δε μπορεί να συμβεί.

- *Στατικά (static) και δυναμικά (dynamic) παίγνια:* Στα στατικά παίγνια, κάθε απόφαση έχει επιπτώσεις μόνο στο παρόν (π.χ. στο παιχνίδι "κορώνα ή γράμματα" κάθε παίκτης κερδίζει ή χάνει την ίδια στιγμή). Στα δυναμικά παίγνια, κάθε απόφαση έχει επιπτώσεις στις μελλοντικές κινήσεις του ίδιου του

παίκτη, ή των αντιπάλων του (π.χ. στο σκάκι κάθε παίκτης πρέπει πριν από κάθε κίνηση του, να προβλέπει τις επόμενες κινήσεις του άλλου παίκτη). Ωστόσο δεν είναι απαραίτητο να υπάρχει χρονική απόκλιση.

- *Παίγνια συνεργασίας (cooperative) και μη συνεργασίας (non-cooperative):* Στα παίγνια συνεργασίας, οι παίκτες μπορούν να συνάπτουν συμβόλαια που έχουν νομική ισχύ, όπως είναι αυτά μεταξύ εργοδοτών και εργαζομένων. Αντίθετα στα παίγνια μη συνεργασίας, δεν επιτρέπεται η υπογραφή συμβολαίων. Αυτό συμβαίνει συχνά μεταξύ εταιριών που ανταγωνίζονται, παραδείγματος χάριν μεταξύ Microsoft και Google. Τα παίγνια που χρησιμοποιούνται είναι κυρίως μη συνεργατικά, όπου ο κάθε παίκτης είναι ένα άτομο που ορθολογικά αποφασίζει να μεγιστοποιήσει κάποια συνάρτηση χρησιμότητας / κέρδους.

  Στα μη συνεργατικά παίγνια, οι ενέργειες των απλών παικτών είναι σεβαστές. Αντιστοίχως, στα συνεργατικά παίγνια οι κοινές ενέργειες των ομάδων αναλύονται. Για παράδειγμα, ποιο θα είναι το αποτέλεσμα εάν μια ομάδα παικτών συνεργαστεί. Το ενδιαφέρον εδώ βρίσκεται στο είδος της συνεργασίας. Στις τηλεπικοινωνίες, το μεγαλύτερο ποσοστό έρευνας στη θεωρία των παιγνίων έχει γίνει χρησιμοποιώντας μη συνεργατικά παίγνια. Υπάρχουν όμως και κάποιες προσεγγίσεις που χρησιμοποιούν συνεργατικά παίγνια [Michiardi και Molva, 2002]. Τα συνεργατικά παίγνια μπορούν να χρησιμοποιηθούν για την ανάλυση ετερογενών ad hoc δικτύων. Εάν ένα δίκτυο αποτελείται από κόμβους με διαφορετικά επίπεδα εγωιστικής στάσης (selfishness), ίσως είναι ευεργετικό το να εμποδίσει κανείς τους πολύ selfish κόμβους από το δίκτυο, εφόσον στους εναπομείναντες κόμβους παρέχεται καλύτερη υπηρεσία με αυτόν τον τρόπο.

- *Επαναλαμβανόμενα (repeated) και απείρως μακροχρόνια (Infinitely repeated):* Όταν ένας παίκτης γνωρίζει κάτι (π.χ. την επιλογή του αντιπάλου), τότε ο κόμβος απόφασης του αντιπάλου πρέπει να προηγείται στο δέντρο παιγνίου. Οι καθαροί μαθηματικοί μελετούν παίγνια που διαρκούν άπειρα, με το νικητή να μην είναι γνωστός μέχρι όλες οι κινήσεις να έχουν γίνει. Οι οικονομολόγοι εντούτοις παίζουν παίγνια που τελειώνουν σε ένα πεπερασμένο σύνολο κινήσεων. Τα επαναλαμβανόμενα παίγνια δίνουν τη δυνατότητα για καλές συνεργατικές στρατηγικές, ενώ χωρίς επανάληψη δε θα υπήρχε συντονισμός.

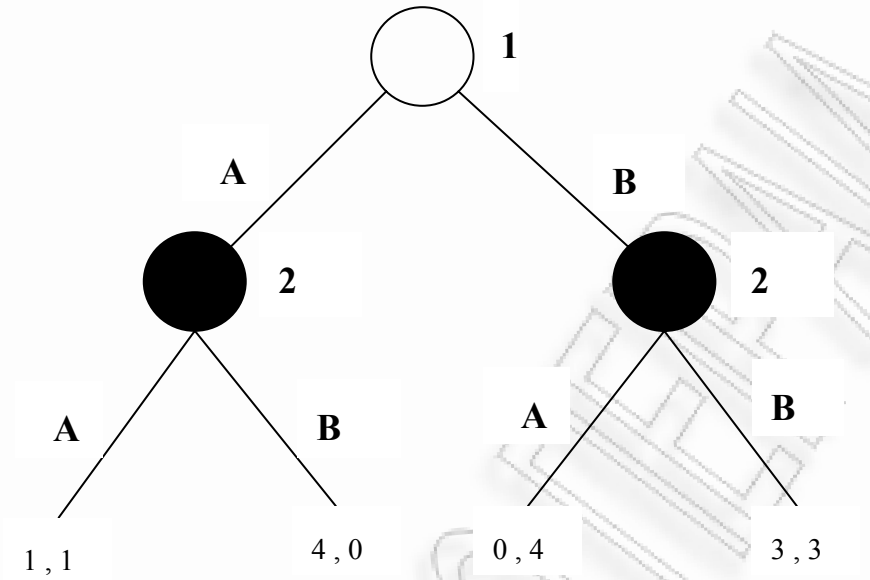
3.4 Σύνολα πληροφόρησης

Στη ενότητα αυτή θα εξηγήσουμε τι σημαίνει η έννοια σύνολο πληροφόρησης (information set). Σύνολο πληροφόρησης ενός παίκτη είναι αυτό που καταδεικνύει όλες τις πιθανές επιλογές του παίκτη, δεδομένου του τι γνωρίζει ο παίκτης μέχρι εκείνη τη στιγμή. Στην εκτεταμένη μορφή ενός παιγνίου, κάθε σύνολο πληροφόρησης αποτελείται από ένα σύνολο κόμβων. Έτσι:

- Όλοι οι κόμβοι απόφασης ενός παιγνίου, ανήκουν σε σύνολα πληροφόρησης μοναδιαία ή σε περισσότερα του ενός κόμβου.
- Όσο λιγότερους κόμβους έχει ένα σύνολο πληροφόρησης τόσο καλύτερη είναι η πληροφόρηση. Συνεπώς ένα μοναδιαίο σύνολο πληροφόρησης σημαίνει τέλεια πληροφόρηση.

Σε κάθε παίγνιο, όσο περισσότερους παίκτες έχουμε, τόσο περισσότερα σύνολα πληροφόρησης βρίσκουμε. Επίσης τα σύνολα πληροφόρησης σε ένα παίγνιο ταυτοχρόνων κινήσεων, είναι λιγότερα από αυτά ενός παιγνίου διαδοχικών κινήσεων. Για να κατανοήσουμε καλύτερα την έννοια των συνόλων πληροφόρησης, θα παρουσιάσουμε ένα παίγνιο τέλειας πληροφόρησης και θα εξηγήσουμε την εκτεταμένη μορφή του.

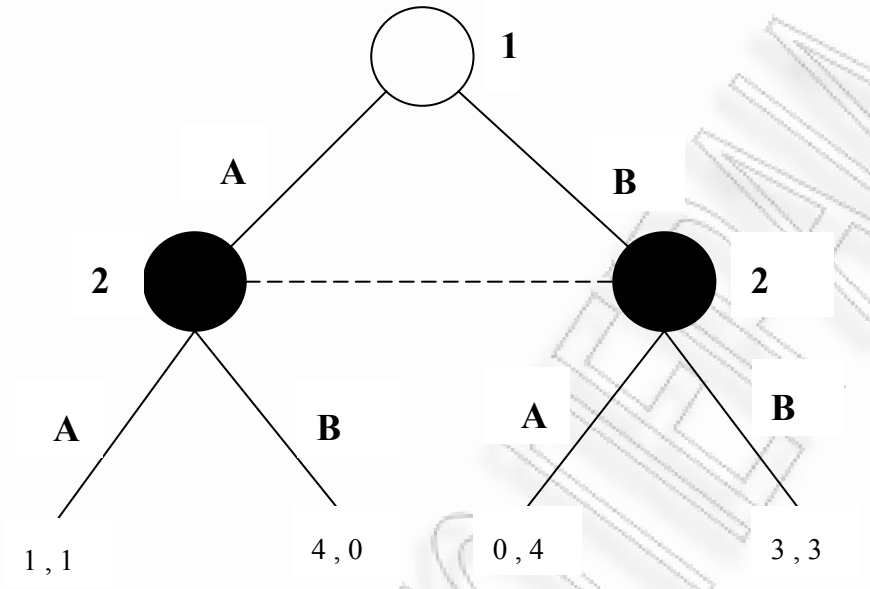
Έστω ένα παίγνιο στο οποίο υπάρχουν δύο παίκτες οι οποίοι κινούνται διαδοχικά. Πρώτα αποφασίζει ο παίκτης 1 εάν θα επιλέξει τη στρατηγική Α ή Β. Έπειτα, ο παίκτης 2, γνωρίζοντας το τι έχει επιλέξει ο παίκτης 1, αποφασίζει εάν θα επιλέξει τη στρατηγική Α ή Β. Έτσι έχουμε την παρακάτω εκτεταμένη μορφή όπως παρουσιάζεται στην εικόνα 6:



Εικόνα 6: Παράδειγμα σύνολα πληροφόρησης 1

Το παίγνιο αυτό αποτελείται από τρία μοναδιαία σύνολα πληροφόρησης. Ο παίκτης 1 έχει ένα μόνο σύνολο πληροφόρησης το οποίο ξεκινά από τον πρώτο κόμβο και στο οποίο έχει τις επιλογές Α, Β. Αντίθετα ο παίκτης 2 έχει δύο σύνολα πληροφόρησης. Εφόσον ο παίκτης 2 όταν θα κινηθεί θα γνωρίζει τι έχει προηγουμένως επιλέξει ο πρώτος παίκτης ,τότε θα γνωρίζει εάν θα βρίσκεται στον κόμβο κάτω αριστερά ή κάτω δεξιά. Το πρώτο λοιπόν σύνολο πληροφόρησης για τον παίκτη 2 αποτελείται από τον κόμβο κάτω αριστερά με τις στρατηγικές Α και Β. Έστω ότι ονομάζουμε το σύνολο αυτό 2Α. Το δεύτερο σύνολο πληροφόρησης για τον παίκτη 2 αποτελείται από τον κόμβο κάτω δεξιά, πάλι με τις στρατηγικές Α και Β. Έστω ότι ονομάζουμε το σύνολο αυτό 2Β.

Έστω τώρα το ίδιο παίγνιο, το οποίο όμως υποθέτουμε πως είναι ταυτοχρόνων κινήσεων. Δηλαδή κάθε παίκτης όταν καλείται να κινηθεί, δεν γνωρίζει τι έχει επιλέξει ο άλλος παίκτης. Έτσι έχουμε την παρακάτω εκτεταμένη μορφή στην εικόνα 7:



Εικόνα 7: Παράδειγμα σύνολα πληροφόρησης 2

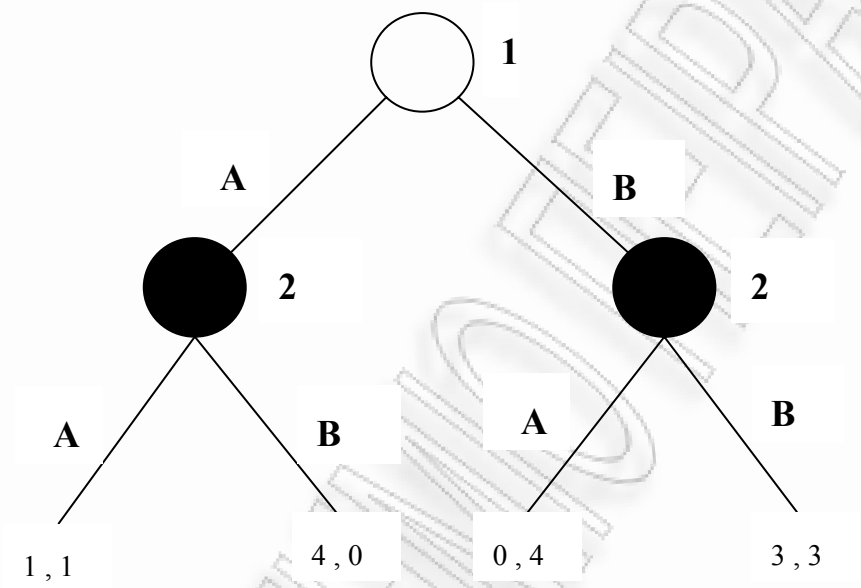
Εφόσον το παίγνιο αυτό είναι παίγνιο ταυτοχρόνων κινήσεων, αποτελείται από δύο μοναδιαία σύνολα πληροφόρησης. Ο παίκτης 1 έχει και πάλι ένα μοναδιαίο σύνολο πληροφόρησης, το οποίο ξεκινά από τον πρώτο κόμβο και στο οποίο έχει τις επιλογές A, B. Στην περίπτωση αυτή, ο παίκτης 2 έχει επίσης ένα σύνολο πληροφόρησης, αφού δεν γνωρίζει σε ποιον από τους δύο κάτω κόμβους θα βρίσκεται. Στο σύνολο πληροφόρησης αυτό θα ανήκουν οι δυο τελευταίοι κόμβοι, ενώ ο παίκτης 2 θα επιλέξει A ή B μη γνωρίζοντας την επιλογή του άλλου παίκτη.

- Για να κατανοήσουμε τις παραπάνω έννοιες θα επιλύσουμε το παρακάτω παίγνιο:

Έστω ότι ο παίκτης 1 κινείται πρώτος και έχει δυο επιλογές A και B. Ύστερα κινείται ο παίκτης 2, αφού παρατηρήσει τον παίκτη 1 και επιλέξει πάλι A ή B. Εάν και οι δυο παίκτες επιλέξουν A, καθένας κερδίζει 1 ευρώ. Εάν και οι δυο παίκτες επιλέξουν B, καθένας κερδίζει 3 ευρώ. Εάν ο παίκτης 1 επιλέξει A, ενώ ο παίκτης 2 επιλέξει B, τότε ο παίκτης 1 κερδίζει 4 ευρώ και ο παίκτης 2 κερδίζει μηδέν ευρώ. Αντίστοιχα, εάν ο

παίκτης 1 επιλέξει Β, ενώ ο παίκτης 2 επιλέξει Α, τότε ο παίκτης 2 κερδίζει 4 ευρώ και ο παίκτης 1 κερδίζει μηδέν ευρώ.

Στην εικόνα 8 απεικονίζεται το παίγνιο στην εκτεταμένη μορφή του και στον πίνακα 5 στην στρατηγική μορφή του.



Εικόνα 8: Εκτεταμένη μορφή παιγνίου διαδοχικών κινήσεων

		2			
		A A	**A B**	**B A**	**B B**
1	**A**	1 , 1	1 , 1	4 , 0	4 , 0
	B	0 , 4	3 , 3	0 , 4	3 , 3

Πίνακας 5: Στρατηγική μορφή παιγνίου διαδοχικών κινήσεων

Αυτό είναι ένα παίγνιο διαδοχικών κινήσεων αφού ο δεύτερος παίκτης γνωρίζει τις κινήσεις του πρώτου και ύστερα επιλέγει τι θα κάνει. Ενέργειες είναι οι επιλογές κάθε παίκτη σε κάποιο σύνολο πληροφόρησης. Παρακάτω συμβολίζουμε με Ai την ενέργεια (action) κάθε παίκτη.

- Ο πρώτος παίκτης έχει ένα σύνολο πληροφόρησης και άρα ισχύει:

  $A_1 = (A, B)$

- Ο δεύτερος παίκτης έχει δυο σύνολα πληροφόρησης, το 2Α και το 2Β. Άρα αφού έχει δύο σύνολα πληροφόρησης ισχύει:

  $A_2(2A) = (A, B)$

  $A_2(2B) = (A, B)$

- Το σύνολο των στρατηγικών του δεύτερου παίκτη είναι το καρτεσιανό γινόμενο:

ΑΑ: Α από το σύνολο 2Α και Α από το σύνολο 2Β

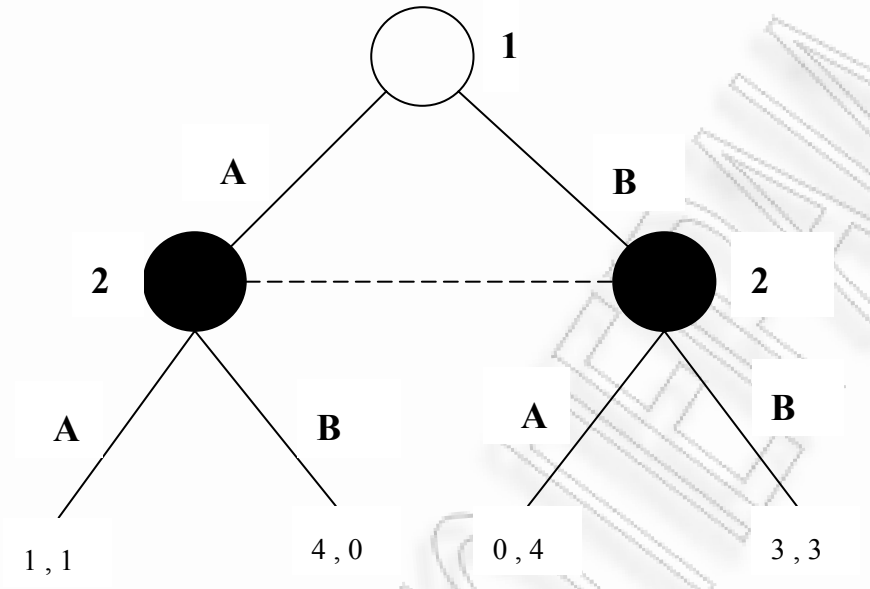
ΑΒ: Α από το σύνολο 2Α και Β από το σύνολο 2Β

ΒΑ: Β από το σύνολο 2Α και Α από το σύνολο 2Β

ΒΒ: Β από το σύνολο 2Α και Β από το σύνολο 2Β

Δηλαδή ο δεύτερος παίκτης έχει τέσσερις στρατηγικές

Ας υποθέσουμε τώρα πως κανένας παίκτης δεν παρατηρεί τον άλλο πριν πάρει την απόφασή του. Συνεπώς το παίγνιο γίνεται ταυτοχρόνων κινήσεων. Άρα στην εκτεταμένη απεικόνιση του παιγνίου δεν έχει σημασία ποιόν παίκτη θα βάλουμε πρώτο. Η στρατηγική και η εκτεταμένη μορφή του παιγνίου είναι:



Εικόνα 9: Εκτεταμένη μορφή παιγνίου ταυτοχρόνων κινήσεων

		2	
		A	**B**
1	**A**	1 , 1	4 , 0
	B	0 , 4	3 , 3

Πίνακας 6: Στρατηγική μορφή παιγνίου ταυτοχρόνων κινήσεων

Κάθε παίκτης έχει ένα σύνολο πληροφόρησης και οι ενέργειες για κάθε παίκτη είναι κοινές. Άρα:

- Για τον πρώτο παίκτη ισχύει πάλι $A_1 = (A, B)$
- Για τον δεύτερο παίκτη ισχύει επίσης $A_2 = (A, B)$ αφού έχει ένα σύνολο πληροφόρησης.

3.5 Επίλυση παιγνίων

Στην ενότητα αυτή θα αναλύσουμε διάφορες μεθόδους επίλυσης παιγνίων. Κάθε παίγνιο ανάλογα με τη μορφή με την οποία το απεικονίζουμε, μπορεί να λυθεί και με διαφορετικό τρόπο. Ο πιο εύκολος τρόπος για να λύσουμε ένα παίγνιο είναι να εξετάσουμε εάν υπάρχουν κυρίαρχες στρατηγικές για κάθε παίκτη. Εάν το παίγνιο που εξετάζουμε απεικονίζεται με δένδρο και είναι παίγνιο τέλειας πληροφόρησης, μπορούμε να το επιλύσουμε με την μέθοδο της οπισθογενούς επαγωγής. Βέβαια κάθε ισορροπία σε ένα παίγνιο είναι και ισορροπία Nash. Θα εξηγήσουμε πως χρησιμοποιείται κάθε μια από αυτές τις μεθόδους.

- Αυστηρή ή ισχυρή κυριαρχία στρατηγικής παίκτη (strict/strong dominance)

Μια στρατηγική s_i^* του παίκτη i, κυριαρχεί ισχυρά / αυστηρά μιας άλλης στρατηγικής του ίδιου παίκτη, αν οι αποδόσεις του παίκτη i όταν χρησιμοποιεί τη στρατηγική s_i είναι μεγαλύτερες των αντίστοιχων αποδόσεων όταν χρησιμοποιεί τη στρατηγική $s_{i'}$, για οποιονδήποτε συνδυασμό στρατηγικών των αντιπάλων του.

$\Pi_i (s_i^*, s_{-i}) > \Pi_i (s_{i'}, s_{-i})$ για κάθε s_{-i}

Δηλαδή, μια στρατηγική s_i^* είναι ισχυρά / αυστηρά κυρίαρχη για τον παίκτη ι, όταν κυριαρχεί επί όλων των άλλων στρατηγικών. Για να καταλάβουμε καλύτερα την έννοια της αυστηρής κυριαρχίας θα αναλύσουμε την παρακάτω στρατηγική μορφή (πίνακας 7) ενός παιγνίου.

		2	
		Γ	**Δ**
1	**Α**	1 , 1	4 , 0
	Β	0 , 4	3 , 3

Πίνακας 7: Στρατηγική μορφή παιγνίου (αυστηρή κυριαρχία)

Για τον παίκτη 1 η στρατηγική Α είναι αυστηρά κυρίαρχη στρατηγική αφού ισχύει:

$1 > 0$ και $4 > 3$

Αφού λοιπόν ο παίκτης 1 θα προτιμήσει την στρατηγική Α μπορούμε νοητά να διαγράψουμε τη δεύτερη γραμμή του πίνακα με την κυριαρχούμενη στρατηγική. Ο παίκτης 2 θα προτιμήσει έτσι τη στρατηγική Γ , εφόσον: $1 > 0$

Η ισορροπία θα είναι άρα η (Α, Γ) = (1, 1)

- Ασθενής κυριαρχία στρατηγικής παίκτη (weak dominance)

Μια στρατηγική s_i^* του παίκτη i, κυριαρχεί ασθενώς μιας άλλης στρατηγικής του ίδιου παίκτη, αν οι αποδόσεις του παίκτη i, όταν χρησιμοποιεί τη στρατηγική s_i είναι μεγαλύτερες ή ίσες για οποιουσδήποτε συνδυασμούς στρατηγικών των υπολοίπων παικτών και δίνει αυστηρά περισσότερες αποδόσεις, για τουλάχιστον κάποιο συνδυασμό στρατηγικών των υπολοίπων παικτών.

$\Pi_i (s_i^*, s_{-i}) \geq \Pi_i (s_{i'}, s_{-i})$ για κάθε s_{-i}

και

$\Pi_i (s_i^*, s_{-i}) > \Pi_i (s_{i'}, s_{-i})$ για μερικά s_{-i}

Δηλαδή, μια στρατηγική s_i^* είναι ασθενώς κυρίαρχη για τον παίκτη i, όταν κυριαρχεί ασθενώς επί όλων των άλλων στρατηγικών.

Όταν όλοι οι παίκτες έχουν κυρίαρχη στρατηγική σε ένα παίγνιο, τότε σίγουρα υπάρχει ισορροπία. Η ισορροπία μπορεί να βρεθεί με τη χρήση της διαδοχικής επαναληπτικής κυριαρχίας (iterated dominant equilibrium). Για να καταλάβουμε καλύτερα την έννοια της ασθενούς κυριαρχίας θα αναλύσουμε την παρακάτω στρατηγική μορφή (πίνακας 8) ενός παιγνίου.

		2			
		Γ	**Δ**	**E**	**Z**
1	**A**	1 , 1	1 , 1	4 , 0	4 , 0
	B	0 , 4	3 , 3	0 , 4	3 , 3

Πίνακας 8: Στρατηγική μορφή (ασθενής κυριαρχία)

Παρατηρούμε πως ο παίκτης 2 προτιμά τη στρατηγική Γ από την στρατηγική Δ αφού 1 = 1 αλλά 4 > 3. Ομοίως ο παίκτης 2 προτιμά τη στρατηγική Γ από την στρατηγική Ε αφού 1 > 0 και 4 = 4. Τέλος ο ίδιος παίκτης 2 προτιμά τη στρατηγική Γ από την στρατηγική Z αφού 1 > 0 και 4 > 3. Για τον παίκτη 2 η στρατηγική Γ είναι ασθενώς κυρίαρχη στρατηγική αφού οι αποδόσεις του παίκτη 2 είναι μεγαλύτερες ή ίσες των αποδόσεων του σε κάθε άλλη στρατηγική, είτε ο παίκτης 1 επιλέξει τη στρατηγική Α είτε επιλέξει τη στρατηγική Β.

Εφόσον λοιπόν οι αποδόσεις του παίκτη 2 είναι μεγαλύτερες ή ίσες από τις αποδόσεις του παίκτη σε κάθε άλλη στρατηγική, ο παίκτης 2 θα επιλέξει τη στρατηγική Γ. Συνεπώς δεδομένου ότι ο παίκτης 2 θα επιλέξει τη στρατηγική Γ, ο παίκτης 1 θα επιλέξει επίσης τη στρατηγική Α αφού 1 > 0.

Η ισορροπία θα είναι άρα η (Α, Γ) = (1, 1).

- Ισορροπία κατά Nash (Nash equilibrium)

Κάθε ισορροπία σε ένα παίγνιο θα είναι ισορροπία κατά Nash.

Η στρατηγική s_i^* αποτελεί βέλτιστη απόκριση (best response) του παίκτη i ως προς ένα συνδυασμό s_{-i} που αφορά στρατηγικές όλων των άλλων παικτών, εάν η απόδοση του i είναι μεγαλύτερη ή ίση με την απόκριση που θα είχε ο παίκτης i αν επέλεγε κάτι διαφορετικό.

$\Pi_i (s_i^*, s_{-i}) \geq \Pi_i (s_{i'}, s_{-i})$

Ένας συνδυασμός στρατηγικών $s_1, s_2, \ldots, s_n$ αποτελεί ισορροπία κατά Nash, εάν αυτό που κάνει κάθε παίκτης είναι βέλτιστη απόκριση σε αυτό που κάνουν οι υπόλοιποι. Με

άλλα λόγια, στην ισορροπία κατά Nash, κανένας παίκτης δεν έχει μονομερώς κίνητρο να βγει από την κατάσταση ισορροπίας.

Προκειμένου η ισορροπία κατά Nash να γίνει πιο κατανοητή, θα εξηγήσουμε πως προκύπτει ισορροπία κατά Nash στον παρακάτω πίνακα (πίνακας 9) παιγνίου.

		2	
		A	**B**
1	**A**	1 , 1	4 , 0
	B	0 , 4	3 , 3

Πίνακας 9: Στρατηγική μορφή παιγνίου (ισορροπία κατά Nash)

- Εάν ο παίκτης 1 επιλέξει τη στρατηγική A, ο παίκτης 2 θα επιλέξει τη στρατηγική A αφού 1 > 0. Ομοίως εάν ο παίκτης 2 επιλέξει τη στρατηγική A ο παίκτης 1 θα επιλέξει τη στρατηγική A αφού 1 > 0.

  Άρα η στρατηγική (A, A) = (1, 1) είναι ισορροπία κατά Nash, NE.

- Εάν ο παίκτης 1 επιλέξει τη στρατηγική B, ο παίκτης 2 θα επιλέξει τη στρατηγική A αφού 4 > 3. Όμως εάν ο παίκτης 2 επιλέξει τη στρατηγική A, ο παίκτης 1 θα επιλέξει τη στρατηγική A αφού 1 > 0.

Συνεπώς στο παίγνιο αυτό η στρατηγική (A, A) = (1, 1) είναι και η μοναδική ισορροπία κατά Nash.

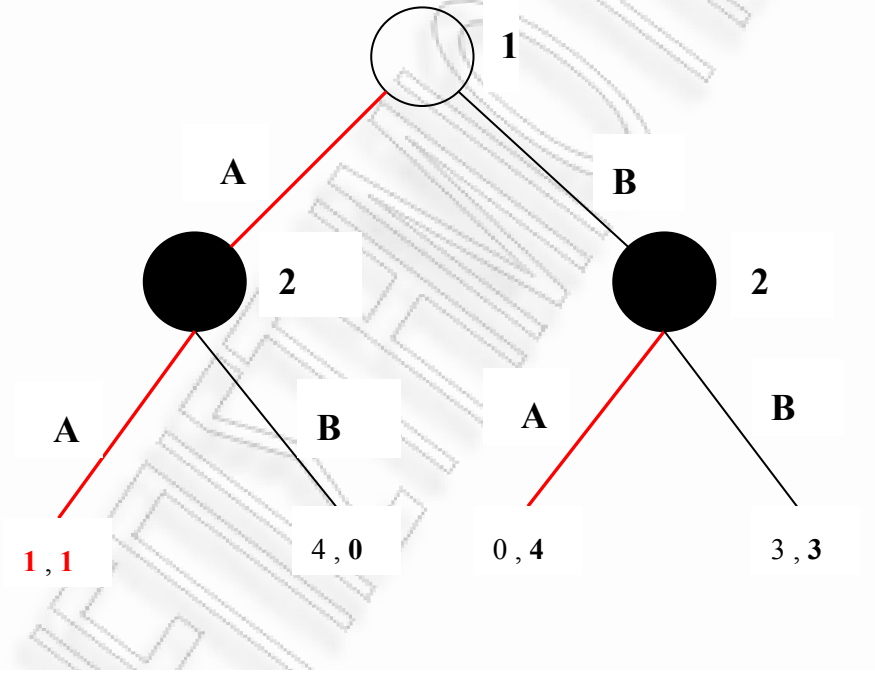
<u>Συμπεράσματα</u>

- Παρατηρούμε από τα παραδείγματα, ότι όταν σε ένα παίγνιο έχω ισορροπία δια της αυστηρής κυριαρχίας, τότε η ισορροπία στη οποία καταλήγω θα είναι και η μοναδική ισορροπία κατά Nash.
- Μια ισορροπία κατά Nash δεν είναι όμως απαραίτητα ισορροπία σε κυρίαρχες στρατηγικές.

- Οπισθογενής επαγωγή (backwards induction) [Gibbons, 1992]

Η προς τα πίσω επαγωγή χρησιμοποιείται στα παίγνια τέλειας πληροφόρησης και βασίζεται στη διαδοχική ορθολογικότητα (sequential rationality). Σύμφωνα με την τελευταία έννοια, ένας παίκτης που καλείται να κινηθεί θα επιλέξει την ενέργεια που θεωρεί καλύτερη για αυτόν, στη βάση του τι αναμένει να κάνουν οι αντίπαλοι που θα κινηθούν μετά από αυτόν.

Για να επιλύσουμε λοιπόν ένα τέτοιο παίγνιο, ξεκινάμε από τον τελευταίο παίκτη, βρίσκουμε τη βέλτιστη επιλογή του, συνεχίζουμε με τον προτελευταίο παίκτη και προχωράμε αντίστοιχα.



Εικόνα 10: Παράδειγμα οπισθογενής επαγωγής, εκτεταμένη μορφή παιγνίου

Συγκεκριμένα, θα προσπαθήσουμε να επιλύσουμε το παίγνιο που είχαμε εξηγήσει και παραπάνω, στο οποίο συμμετέχουν δυο παίκτες. Ξεκινάμε από το δεύτερο και τελευταίο παίκτη του παιγνίου. Ο παίκτης 2 θα επιλέξει τη στρατηγική Α είτε βρεθεί στο αριστερό είτε στο δεξί υποπαίγνιο του δένδρου. Στο συμπέρασμα αυτό καταλήγουμε συγκρίνοντας τις αποδόσεις του παίκτη σε κάθε υποπαίγνιο (subgame): 1 > 0 και 4 > 3.

Δεδομένου λοιπόν ότι ο παίκτης 2 θα επιλέξει τη στρατηγική Α, ο παίκτης 1 θα επιλέξει τη στρατηγική Α, αφού 1 > 0. Η ισορροπία στην οποία καταλήξαμε, είναι η ίδια με αυτή που έδωσαν η μέθοδος της κυριαρχίας και η ισορροπία κατά Nash, δηλαδή η (Α, ΑΑ) = (1, 1).

3.6 Περίληψη

Στο κεφάλαιο αυτό εξηγήσαμε τη χρησιμότητα των παιγνίων και αναφέραμε επιστήμες οι οποίες χρησιμοποιούν τα παίγνια ως βοηθητικά εργαλεία. Στη συνέχεια περιγράψαμε πως απεικονίζεται ένα παίγνιο με εκτεταμένη και στρατηγική μορφή ώστε να αντιλαμβανόμαστε τι πληροφορίες έχουν οι παίκτες. Κατηγοριοποιήσαμε τα παίγνια με βάση ποικίλα κριτήρια και επεξηγήσαμε την έννοια των συνόλων πληροφόρησης ώστε να διαχωρίζουμε τα παίγνια διαδοχικών και ταυτοχρόνων κινήσεων. Τέλος αναλύσαμε τους τρόπους επίλυσης των παιγνίων ώστε να μπορούμε να καταλήγουμε σε μία ή περισσότερες ισορροπίες. Στο επόμενο κεφάλαιο θα ασχοληθούμε με τα συστήματα ανίχνευσης εισβολών.

4 Συστήματα Ανίχνευσης Εισβολών

4.1 Εισαγωγή

Την έννοια του intrusion detection εισήγαγε για πρώτη φορά ο J.P. Anderson το 1980. Όρισε σαν εισβολή (intrusion) μια μη εξουσιοδοτημένη προσπάθεια να αποκτήσει κάποιος πρόσβαση ή να παραποιήσει πληροφορίες ή να καταστήσει ένα σύστημα αναξιόπιστο ή ασταθές [Anderson, 1980]. Ο στόχος των συστημάτων ανίχνευσης εισβολών (Intrusion Detection Systems - IDS) είναι να παρακολουθούν τους υπολογιστές που βρίσκονται σε ένα δίκτυο και το ίδιο το δίκτυο, και να ειδοποιούν τον υπεύθυνο ασφάλειας όταν ανιχνεύουν κάποια εισβολή, ενώ παράλληλα ενεργούν με αντίμετρα στην επίθεση [Bace, 2000].

4.2 IDS σε Ασύρματα Δίκτυα Αισθητήρων

Ένα ασύρματο δίκτυο αποτελείται από ένα σύνολο κόμβων που είναι σε θέση να διατηρήσουν ένα ασύρματο κανάλι επικοινωνίας ο ένας με τον άλλο, χωρίς να στηρίζονται σε κάποια σταθερή υποδομή. Αυτός και άλλοι παράγοντες καθιστούν τα ασύρματα δίκτυα ουσιαστικά διαφορετικά από τα συνδεμένα με καλώδιο δίκτυα. Σε ένα ασύρματο δίκτυο δεν υπάρχει ούτε ένα σημείο πρόσβασης, όλοι οι κόμβοι πρέπει να συνεργαστούν για να δημιουργήσουν το δίκτυο και να οργανώσουν την υποδομή του (π.χ. υποσύστημα δρομολόγησης) και τις υπηρεσίες (π.χ. συλλογή δεδομένων), και τελικά, οι περισσότερες διαδικασίες διενεργούνται με έναν διανεμημένο τρόπο.

Και τα ad hoc δίκτυα αλλά και τα δίκτυα αισθητήρων μπορούν να συμπεριληφθούν μέσα στην κατηγορία ασύρματων δικτύων. Παρόλα αυτά υπάρχουν ορισμένες σημαντικές διαφορές μεταξύ τους:

- Στα ad hoc δίκτυα, ο κάθε κόμβος συνήθως ρυθμίζεται και διαχειρίζεται από κάποιον άνθρωπο. Εντούτοις, σε ένα δίκτυο αισθητήρων, ο κάθε κόμβος είναι

συνολικά ανεξάρτητος, στέλνοντας στοιχεία και λαμβάνοντας τα πακέτα ελέγχου από ένα κεντρικό σύστημα που αποκαλείται σταθμός βάσης, ο οποίος συνήθως διαχειρίζεται από έναν ανθρώπινο χρήστη.

- Οι υπολογιστικοί πόροι και οι μπαταρίες είναι περισσότερο περιορισμένοι στους κόμβους αισθητήρων απ' ότι στους ad hoc κόμβους. Ένας χαρακτηριστικός κόμβος αισθητήρων όπως ο MICA2 έχει ένα μικροεπεξεργαστή 8Mhz με 128Kb flash memory και 512Kb serial flash memory.
- Ο σκοπός των δικτύων αισθητήρων είναι πολύ συγκεκριμένος. Για παράδειγμα, να μετρήσουν τις φυσικές πληροφορίες (όπως η θερμοκρασία, ο ήχος) από το περιβάλλον. Κατά συνέπεια, και το υλικό αλλά και τα πρωτόκολλα επικοινωνίας / διαμόρφωσης είναι ιδιαίτερα εξειδικευμένα.
- Η πυκνότητα τοποθέτησης κόμβων στα δίκτυα αισθητήρων είναι υψηλότερη απ' ότι στα ad hoc δίκτυα. Εντούτοις, οι κόμβοι αισθητήρων έχουν περισσότερες πιθανότητες αποτυχίας και εξαφάνισης από το δίκτυο, λόγω του περιορισμού τους σε μπαταρίες και της χαμηλής ασφάλειας τους.

Ως αποτέλεσμα αυτών των διαφορών, οι λύσεις IDS που έχουν αναπτυχθεί για τα ad hoc δίκτυα δε μπορούν να εφαρμοστούν άμεσα στα δίκτυα αισθητήρων. Κατ' αρχάς, δεν είναι δυνατό να υπάρξει ένας ενεργός πλήρης-τροφοδοτημένος πράκτορας μέσα σε κάθε κόμβο. Επίσης, ένα IDS σε δίκτυο αισθητήρων πρέπει να στέλνει μηνύματα συναγερμού στο σταθμό βάσης προκειμένου να προειδοποιηθεί ο ανθρώπινος χρήστης. Τέλος, το IDS πρέπει να είναι απλό και ιδιαίτερα εξειδικευμένο ώστε να μπορεί να αντιδράσει ενάντια στις συγκεκριμένες απειλές δικτύων αισθητήρων και στα συγκεκριμένα πρωτόκολλα που χρησιμοποιούνται μέσα σε ένα τέτοιο δίκτυο [Zhang και Lee, 2003; Kong et al., 2002; Albers et al., 2002; Karlof και Wagner, 2003].

Επί μέρους λύσεις υπάρχουν, που επιτρέπουν σε έναν κόμβο να ελέγξει την ασφάλεια του δικτύου αισθητήρων, με το να δοκιμάζει εάν μια ομάδα κόμβων είναι ζωντανή ή νεκρή [Hsin και Liu, 2002], με την ανάλυση των διακυμάνσεων στις αναγνώσεις αισθητήρων [Doumit και Agrawal, 2003], την επιβεβαίωση της ακεραιότητας του

κώδικα μέσα σε έναν κόμβο [Seshandri et al., 2004], ή την παρακολούθηση όλων των πληροφοριών που ανταλλάσσονται [Marti et al., 2000].

4.3 Τεχνικές Ανίχνευσης Εισβολών

Ένα σύστημα ανίχνευσης εισβολών ανιχνεύει γενικά τον ανεπιθύμητο χειρισμό στα συστήματα. Εφαρμόζονται για να παρακολουθούν διάφορα σημεία μέσα στο σύστημα τα οποία και προστατεύουν. Τα Passive IDSs ανιχνεύουν τις πιθανές παραβιάσεις ασφάλειας και καταγράφουν τις πληροφορίες αφού πρώτα ενεργοποιήσουν έναν συναγερμό, ενώ τα Reactive συστήματα αντιδρούν στις απειλές είτε αυτόνομα είτε έπειτα από εντολή ενός χειριστή.

Οι τρεις πιο δημοφιλείς τεχνικές ανίχνευσης εισβολών που χρησιμοποιούνται στην ασφάλεια δικτύων σήμερα είναι η misuse detection technique (pattern matching) η anomaly detection technique και η specification based technique.

- Το μοντέλο ανίχνευσης misuse detection είναι βασισμένο στην προϋπόθεση ότι όλες οι παρεισφρήσεις έχουν μια ξεχωριστή υπογραφή που μπορεί να ανιχνευθεί. Τα misuse detection συστήματα διατηρούν μια συλλογή με όλες τις υπογραφές επιθέσεων και ελέγχουν το σύστημα για επιθέσεις. Εάν η δραστηριότητα χρηστών ή συστημάτων ταιριάζει με μια υπογραφή, έπειτα το σύστημα ενημερώνει ότι γίνεται επίθεση. Τα οφέλη αυτής της τεχνικής είναι ότι οι υπογραφές είναι βασισμένες στην καλά γνωστή δραστηριότητα των εισβολέων και ως εκ τούτου οι επιθέσεις που ανιχνεύονται καθορίζονται καλά. Άλλα οφέλη περιλαμβάνουν την απλότητα αυτών των συστημάτων και τη δυνατότητα να ανιχνευθούν οι επιθέσεις αμέσως μετά από την εγκατάσταση. Αντίθετα, τα σημαντικότερα μειονεκτήματα των misuse detection συστημάτων, είναι η ανικανότητά τους στο να ανιχνεύουν τις καινούριες επιθέσεις και η μειωμένη δυνατότητα τους να παρακάμπτουν τους ψεύτικους αρνητικούς συναγερμούς.
- Το anomaly detection είναι βασισμένο στην προϋπόθεση ότι οι παρεισφρήσεις είναι ένα υποσύνολο της ανώμαλης δραστηριότητας. Ένα IDS στο μοντέλο anomaly detection παρακολουθεί τη δραστηριότητα των χρηστών και αναφέρει

τις σημαντικές αποκλίσεις από την κανονική δραστηριότητα ως παρεισφρήσεις. Ο έλεγχος μπορεί να είναι σε ένα σύστημα ή επίπεδο χρηστών και αποτελείται από τη σύγκριση της δραστηριότητας ενάντια σε κάποιο προφίλ χρήστη. Το προφίλ του χρήστη είναι μια συλλογή από μετρήσεις, όπως η μέση τιμή επιβάρυνσης της CPU, ο αριθμός διαδικασιών (processes), ο χρόνος σύνδεσης (login time), ή ο αριθμός δικτυακών συνδέσεων που χαρακτηρίζουν τη δραστηριότητα του χρήστη. Κατώτερα και ανώτερα όρια τίθενται για αυτά τα μεγέθη, και η δραστηριότητα έξω από αυτά τα αναμενόμενα όρια χαρακτηρίζεται ως παρείσφρηση. Το σημαντικότερο όφελος τέτοιων τεχνικών είναι ότι μπορούν να ανιχνεύσουν επιθέσεις που είναι αδημοσίευτες. Εντούτοις, τέτοια συστήματα είναι σύνθετα και απαιτούν πολλούς υπολογιστικούς πόρους, δεδομένου ότι παράγουν συνεχώς τεραστίου όγκου logs.

- Το μοντέλο ανίχνευσης specification-based βασίζεται στην αναμενόμενη συμπεριφορά του συστήματος αντί της δραστηριότητας των χρηστών. Η συμπεριφορά του συστήματος καθορίζεται για όλες τις περιπτώσεις και έτσι δημιουργείται ένα προφίλ. Το σύστημα παρακολουθείται στη συνέχεια και καταγράφονται όλες οι ενέργειές του οι οποίες και συγκρίνονται με το κανονικό του προφίλ. Ενέργειες και συμπεριφορές του συστήματος που δεν είναι διευκρινισμένες ως σωστές στο αρχικό προφίλ, χαρακτηρίζονται σαν εισβολές [Bishop et al., 1997].

  Ένα πλεονέκτημα του specification-based μοντέλου είναι ότι ο αριθμός των λανθασμένων αληθινών και ψεύτικων συναγερμών μπορεί να μειωθεί στο ελάχιστο, μέσω ενός ακριβούς και πλήρους προσδιορισμού της κατάστασης του συστήματος. Επιπλέον, όπως και στο anomaly based μοντέλο, οι επιθέσεις μπορούν να ανιχνευθούν ακόμα και αν δεν έχουν αντιμετωπιστεί προηγουμένως. Το κύριο μειονέκτημα είναι η θεμελιώδης απαίτηση να διευκρινιστεί ρητά η πολιτική ασφάλειας του συστήματος. Μια πλήρης προδιαγραφή ενός συστήματος θα απαιτούσε πολύ χρόνο και πείρα. Εάν το σύστημα ήταν δυναμικό, η διατήρηση μιας ακριβούς προδιαγραφής θα μπορούσε να είναι πολύ χρονοβόρα.

4.4 Περίληψη

Σε αυτό το κεφάλαιο είδαμε τι σημαίνει η έννοια του intrusion detection και το στόχο των συστημάτων ανίχνευσης εισβολών. Αναλύσαμε τις διαφορές μεταξύ ad hoc και ασύρματων δικτύων αισθητήρων που εξηγούν γιατί οι λύσεις IDS συστημάτων που έχουν αναπτυχθεί για τα ad hoc δίκτυα δεν μπορούν να εφαρμοστούν άμεσα στα ασύρματα δίκτυα αισθητήρων. Τέλος αναλύθηκαν οι τρεις δημοφιλείς τεχνικές ανίχνευσης εισβολών που χρησιμοποιούνται στην ασφάλεια δικτύων σήμερα. Στο επόμενο κεφάλαιο θα παρουσιάσουμε όλες τις συναφείς εργασίες που έχουν γίνει μέχρι στιγμής και περιλαμβάνουν τις έννοιες ασύρματα δίκτυα αισθητήρων, θεωρία των παιγνίων και συστήματα ανίχνευσης εισβολών.

5 Συναφείς έρευνες

Η χρήση της θεωρίας των παιγνίων στην ασφάλεια των ασύρματων δικτύων αισθητήρων έχει μελετηθεί σε έναν πολύ μικρό αριθμό δημοσιεύσεων τα τελευταία χρόνια. Διάφορα matrix games, συνήθως μεταξύ 2 παικτών (attacker, defending administrator), έχουν σχηματοποιηθεί και οι διάφορες ισορροπίες (equilibrium) τους έχουν εντοπισθεί και ερευνηθεί. Στη συνέχεια του κεφαλαίου θα παρουσιάσουμε συνοπτικά τις δημοσιεύσεις που έχουν γίνει και προσπαθούν να βρουν λύση στο πρόβλημα της ασφάλειας ασύρματων δικτύων αισθητήρων μέσω της θεωρίας των παιγνίων.

Οι Afrand Agah, Sajal K. Das και Kalyan Basu έκαναν για πρώτη φορά το 2004 μια έρευνα που συνδύαζε τη θεωρία παιγνίων με την ασφάλεια στα ασύρματα δίκτυα αισθητήρων. Σε αυτή τη δημοσίευση [Agah et al., 2004a] ορίζουν ένα παιχνίδι ανάμεσα σε κόμβους αισθητήρων και επικεντρώνονται σε τρείς θεμελιώδεις παράγοντες: τη συνεργασία, τη φήμη και την ποιότητα στην ασφάλεια. Η πολύ καλή συνεργασία ανάμεσα σε δύο κόμβους συνεπάγεται πιο αξιόπιστη επικοινωνία των δεδομένων ανάμεσα στους κόμβους. Επίσης, όσο περισσότερο συνεργάζεται ένας κόμβους με τους υπόλοιπους τόσο αυξάνεται η φήμη του. Αντίθετα, η φήμη μειώνεται όταν ανιχνεύεται κακή συμπεριφορά στους κόμβους.

Όταν η ασφάλεια του δικτύου παραβιάζεται, το ποσοστό των εκτεθειμένων σε κινδύνους δεδομένων μετράει την ποιότητα της ασφάλειας των κόμβων αισθητήρων. Ενσωματώνοντας και τους τρεις παράγοντες, τοποθέτησαν τους κόμβους αισθητήρων μέσα σε clusters. Οι συναρτήσεις απόδοσης (payoff functions) για τον κάθε κόμβο είναι παρόμοιες μεταξύ τους, όπου οι αποδόσεις δίνουν το μεγαλύτερο δυνατό κέρδος σε κάθε μεμονωμένο κόμβο, σύμφωνα με την καθορισμένη μέτρηση χρησιμότητας (utility metric). Στη συνέχεια ορίσανε μια στρατηγική για κάθε κόμβο, η οποία εξασφάλιζε μια κατάσταση ισορροπίας για κάθε συνάρτηση απόδοσης. Με τη χρησιμοποίηση της κατάλληλης φόρμουλας συνεργασίας, έδειξαν το πώς μπορείς να διατηρείς την ενέργεια των κόμβων αισθητήρων, έχοντας παράλληλα και συνεργασία ανάμεσα σε ετερογενείς

κόμβους αισθητήρων. Επιπλέον δημιούργησαν σχέσεις εμπιστοσύνης και αποφάσεις ασφάλειας ανάμεσα στους κόμβους, βασιζόμενοι στις συναρτήσεις απόδοσης, ενώ διατήρησαν την κινητικότητα και μεταβλητότητα των κόμβων.

Την ίδια χρονιά, οι Afrand Agah, Sajal K. Das και Kalyan Basu συνέχισαν την έρευνα τους πάνω στο θέμα, γράφοντας μια δημοσίευση με τίτλο Intrusion Detection in Sensor Networks: A Non-cooperative Game Approach [Agah et al., 2004b]. Σε αυτό το paper, προτείνουν ένα θεωρητικό πλαίσιο παιχνιδιών για την ανίχνευση εισβολών στα δίκτυα αισθητήρων. Διατυπώνουν το πρόβλημα ανίχνευσης εισβολών ως ένα παιχνίδι χωρίς συνεργασίες ανάμεσα σε δύο παίκτες, είναι ένα nonzero-sum game, μεταξύ του δικτύου αισθητήρων και του επιτιθέμενου. Δείχνουν ότι η ισορροπία Nash μπορεί να επιτευχθεί. Εξετάζουν πολλούς παράγοντες κινδύνου όπως είναι η αξιοπιστία ενός κόμβου αισθητήρων, διαφορετικοί τύποι επιθέσεων, και ενέργειες που έχουν γίνει στο παρελθόν από τον επιτιθέμενο. Επίσης, εφαρμόζουν μια προσέγγιση εκμάθησης (Markov Decision Process) MDP, προκειμένου να προβλέψουν τη μελλοντική συμπεριφορά του επιτιθέμενου. Με το MDP μπορούν να βρουν τον πιο ευάλωτο κόμβο του δικτύου, ο οποίος μπορεί να γίνει στόχος επιθέσεων στο μέλλον. Τα αποτελέσματα προσομοίωσης δείχνουν ότι με τη χρησιμοποίηση αυτού του θεωρητικού πλαισίου παιχνιδιών, μπορούμε σημαντικά να μεγαλώσουμε τα ποσοστά ανίχνευσης των εισβολών και επιτυχίας των αμυντικών στρατηγικών του δικτύου αισθητήρων.

Στο τέλος του 2004, οι Tansu Alpcan και Tamer Basar [Alpcan και Basar, 2004] παρουσιάζουν μια θεωρητική ανάλυση των συστημάτων ανίχνευσης εισβολών στα συστήματα ελέγχου πρόσβασης χρησιμοποιώντας τη θεωρία παιγνίων. Μελετούν την αλληλεπίδραση μεταξύ ενός επιτιθέμενου και ενός IDS σαν ένα παίγνιο μη συνεργασίας, non-zero sum. Εκτός από αυτούς του δύο παίκτες, προσθέτουν και το δίκτυο αισθητήρων σαν έναν «φανταστικό» παίκτη παρόμοιο με το «nature» παίκτη που συναντάμε συνήθως στη θεωρία παιγνίων. Η στρατηγική αυτού του παίκτη αποτελείται από μια σταθερή πιθανότητα δεδομένης μιας συγκεκριμένης επίθεσης, και αντιπροσωπεύει την απόδοση του δικτύου αισθητήρων κατά τη διάρκεια εκείνης της επίθεσης. Λύνοντας το παιχνίδι χρησιμοποιώντας το πρόγραμμα Gambit [Gambit] κατάφεραν να βρουν ένα NE στις μικτές στρατηγικές. Η αλληλεπίδραση μεταξύ των παικτών για μεγάλες περιόδους αναλύθηκε με χρήση επαναλαμβανόμενων παιγνίων και συγκεκριμένου δυναμικού μοντέλου για τα δίκτυα αισθητήρων.

Ένα χρόνο μετά και πάλι οι Afrand Agah, Sajal K. Das και Kalyan Basu δημοσιεύουν στο περιοδικό Elsevier μια έρευνα με τίτλο Security enforcement in wireless sensor networks: A framework based on non-cooperative games [Agah et al., 2005]. Σε αυτή τη δημοσίευση, προτείνουν δύο διαφορετικές προσεγγίσεις βασισμένες στη θεωρία των παιγνίων, για να αποτρέψουν την επίθεση άρνησης υπηρεσιών (DoS). Στην πρώτη προσέγγιση, που καλείται Secure Auction based Routing (SAR), προτείνουν ένα ασφαλές πρωτόκολλο δρομολόγησης δικτύων αισθητήρων, βασισμένο σε μια θεωρία δημοπρασίας, που απομονώνει τους κακόβουλους κόμβους. Οι κόμβοι που επιθυμούν να συμμετέχουν στην προώθηση των εισερχόμενων πακέτων και στην απόκτηση φήμης στο δίκτυο, πρέπει να ανταγωνιστούν ο ένας ενάντια στον άλλο συμμετέχοντας σε μια δημοπρασία. Το ποσό προσφοράς που κάθε κόμβος προσφέρει είναι η αξία χρησιμότητάς του και το τίμημα που ένας νικητής μιας δημοπρασίας πληρώνει είναι μια μείωση της αρχικής δύναμης των μπαταριών του. Η ειλικρινής προσφορά ενός κόμβου παραμένει μια κυρίαρχη στρατηγική. Έτσι, για να υπάρχει ένα ασφαλές πρωτόκολλο δρομολόγησης, οι κακόβουλοι κόμβοι που δεν προσφέρουν τίποτα πρέπει να απομονωθούν κατά τη διάρκεια του χρόνου.

Στη δεύτερη προσέγγιση, που καλείται Utility based Dynamic Source Routing (UDSR), εισάγεται ένα σχέδιο για την πρόληψη της επίθεσης άρνησης υπηρεσιών (DoS), που είναι βασισμένο στη θεωρία των παιγνίων. Εκεί έχουμε ένα παιχνίδι μεταξύ ενός επιτιθεμένου και του δικτύου αισθητήρων. Σε αυτό το παιχνίδι κάθε παίκτης μεγιστοποιεί τις αποδόσεις του. Ο επιτιθέμενος ως παίκτης προσπαθεί να αυξήσει την κακόβουλη συμπεριφορά του με την εκτέλεση δύο τύπων επιθέσεων άρνησης υπηρεσιών: (i) μη προωθώντας τα μηνύματα, ή (ii) διανέμοντας μηνύματα λάθους διαδρομών σε έναν κανονικό κόμβο, δίνοντας λανθασμένες κατευθύνσεις. Το δίκτυο επίσης σκοπεύει να ανιχνεύσει σωστά τις επιθέσεις. Έτσι, πρέπει να ελαχιστοποιήσει το συνολικό αριθμό ψεύτικων ανιχνεύσεων. Όσο λιγότερες λανθασμένες ανιχνεύσεις έχει, τόσο καλύτερη είναι η επίδοση που παίρνει, το οποίο οδηγεί σε υψηλότερες αποδόσεις. Δεδομένου ότι το δίκτυο αισθητήρων πρέπει να υπερασπίσει τους κόμβους από τέτοιες εισβολές, δημιουργήσανε ένα παιχνίδι δύο παικτών χωρίς συνεργασίες, non-zero-sum. Αυτό το παιχνίδι επιτυγχάνει την ισορροπία Nash, οδηγώντας κατά συνέπεια σε μια αμυντική στρατηγική για το δίκτυο. Προκειμένου να επιλεχτεί η πιο αξιόπιστη διαδρομή, δύο διαφορετικά σχέδια προτείνονται. Το πρώτο σχέδιο περιλαμβάνει τη

συνολική χρησιμότητα κάθε διαδρομής στα πακέτα δεδομένων, ενώ το δεύτερο σχέδιο ενσωματώνει έναν watch-list, όπου η κακή συμπεριφορά οδηγεί στην κακή φήμη και διαδίδεται σε άλλους κόμβους επίσης. Τα αποτελέσματα προσομοίωσης δείχνουν ότι η προτεινόμενη προσέγγιση κρατά τον αριθμό χαμένων πακέτων σταθερό, ανεξάρτητα από το μέγεθος του δικτύου. Αφού αναγνωρίσουν και στιγματίσουν ορισμένους κόμβους ως κακόβουλους, η κακή τους φήμη διαδίδεται σε ολόκληρο το δίκτυο. Οι υπόλοιποι κόμβοι του δικτύου μπορούν να αγνοήσουν αυτούς τους κακόβουλους κόμβους, για τις μελλοντικές αποστολές πακέτων δεδομένων.

Τα πειραματικά αποτελέσματα έδειξαν, ότι χρησιμοποιώντας την αξία χρησιμότητας της κάθε διαδρομής, που είναι βασισμένη στη συνεργασία και τη φήμη των κόμβων, μπορούμε να εγγυηθούμε πιο αξιόπιστη παράδοση δεδομένων. Επίσης, καθορίζοντας ένα αποδεχτό όριο για τη συνεργασία και φήμη των κόμβων, μπορούμε να παρατηρήσουμε ευκολότερα τη συμπεριφορά των κόμβων αισθητήρων και να απομονώσουμε τους ύποπτους κόμβους.

Τελευταία σχετική εργασία που βρίσκουμε δημοσιευμένη είναι από τους Afrand Agah και Sajal K. Das στο περιοδικό International Journal of Network Security τον Σεπτέμβριο του 2007 [Agah και Das, 2007]. Σε αυτό το paper προσπάθησαν να σχηματοποιήσουν την παρεμπόδιση των επιθέσεων άρνησης ασφάλειας (Denial of service - DoS) που γίνονται στα ασύρματα δίκτυα αισθητήρων. Δημιούργησαν ένα επαναλαμβανόμενο παιχνίδι ανάμεσα σε έναν intrusion detector και τους κόμβους ενός δικτύου αισθητήρων όπου μερικοί από τους κόμβους ενεργούν κακόβουλα. Πρότειναν ένα νέο πρωτόκολλο το οποίο βασίζεται στη θεωρία των παιγνίων και επιτυγχάνει το στόχο της ρεαλιστικής προσέγγισης των παιγνίων με το να αναγνωρίζει τους κόμβους οι οποίοι συμφωνούν στην προώθηση των πακέτων, αλλά αποτυγχάνουν να το κάνουν. Αυτή η προσέγγιση κατηγοριοποιεί διαφορετικούς κόμβους που βασίζονται στις μετρήσεις συμπεριφοράς που γίνονται δυναμικά. Μέσα από τη διαδικασία της προσομοίωσης, έγινε μια αποτίμηση του πρωτοκόλλου χρησιμοποιώντας την ταχύτητα διαμεταγωγής των πακέτων (throughput) και την ακρίβεια ανίχνευσης κακής συμπεριφοράς από τους κόμβους.

6 Το παίγνιο GoWiSeN

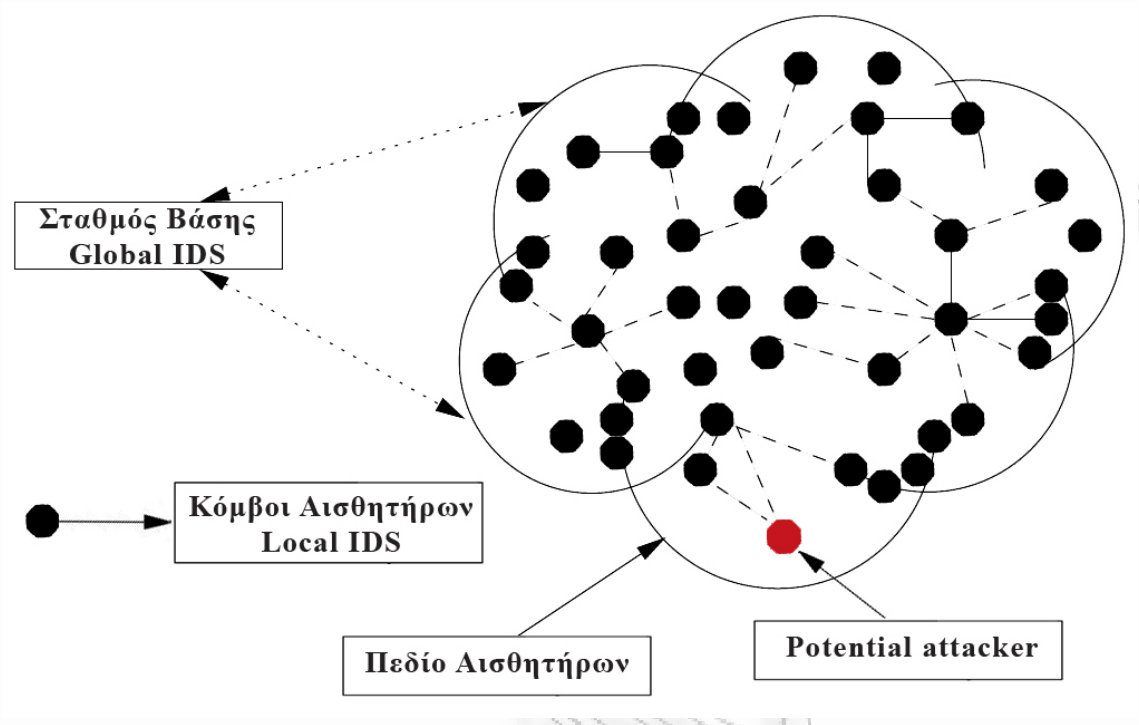
6.1 Εισαγωγή

Σε αυτό το κεφάλαιο κατασκευάζουμε ένα παιχνίδι ασφάλειας για ασύρματα δίκτυα αισθητήρων, το GoWiSeN (Game of Wireless Sensor Networks). Στην προσπάθεια μας να μοντελοποιήσουμε αυτό το σενάριο ασφάλειας χρησιμοποιώντας τη θεωρία των παιγνίων, θα ακολουθήσουμε συγκεκριμένα βήματα. Αρχικά θα ορίσουμε τους παίκτες του παιχνιδιού. Στη συνέχεια θα δημιουργήσουμε τις προτιμήσεις (preferences) του κάθε παίκτη, κατατάσσοντας τες σε μια κλίμακα προτεραιότητας. Αφού οριστούν συγκεκριμένες αποδόσεις (payoffs) για τον κάθε παίκτη, θα κατασκευαστεί η εκτεταμένη και η κανονική μορφή του παιχνιδιού. Τέλος, χρησιμοποιώντας την επίλυση παιγνίων με τη μέθοδο της κυριαρχίας, αλλά και το πρόγραμμα επίλυσης παιγνίων Gambit θα βρούμε όλα τα Nash equilibrium του παιχνιδιού.

6.2 Περιγραφή παιγνίου

Το ασύρματο δίκτυο αισθητήρων (εικόνα 11) μας αποτελείται από έναν μεγάλο αριθμό ασύρματων κόμβων, οι οποίοι είναι πυκνά διασκορπισμένοι σε μια περιοχή. Οι κόμβοι ομαδοποιούνται μέσα σε clusters. Οι κόμβοι μέσα στο κάθε cluster επικοινωνούν μεταξύ τους και φτάνουν μέχρι ένα σταθμό βάσης. Κάθε κόμβος σε ένα cluster τρέχει μια ελαφριά έκδοση IDS, την οποία ονομάζουμε Local IDS, που τον βοηθά να κάνει ανίχνευση κακής συμπεριφοράς άλλων κόμβων. Με τον όρο κακή συμπεριφορά εννοούμε κάθε είδους ενέργεια που μπορεί να βλάψει την ασφάλεια του δικτύου.

Ο σταθμός βάσης του δικτύου έχει και αυτός εγκατεστημένο ένα σύστημα ανίχνευσης εισβολών το οποίο ονομάζουμε Global IDS. Τα συστήματα ανίχνευσης εισβολών, όπως αναφερθήκαμε και παραπάνω, έχουν τη δυνατότητα παρακολούθησης των γεγονότων ενός συστήματος και ανάλυσης αυτών, ώστε να μπορούν να ανιχνεύσουν οποιοδήποτε σημάδι προβλήματος στην ασφάλεια του δικτύου.



Εικόνα 11: Αρχιτεκτονική του ασύρματου δικτύου αισθητήρων

Το παιχνίδι που θα μελετήσουμε αποτελείται από τρεις διαφορετικούς παίκτες. Αρχικά έχουμε έναν εν δυνάμει επιτιθέμενο (potential attacker) κόμβο του δικτύου. Ένας potential attacker μπορεί να κάνει φυσιολογικές κινήσεις ή επιθέσεις στο δίκτυο μας. Οι potential attackers ενεργούν τις περισσότερες φορές φυσιολογικά σαν να είναι κανονικοί κόμβοι του δικτύου.

Το δεύτερο παίκτη στο παιχνίδι μας τον έχουμε ονομάσει Local IDS. Ο Local IDS αποτελεί έναν απολύτως κανονικό κόμβο του δικτύου, με τη διαφορά ότι τρέχει μια Light έκδοση ενός IDS συστήματος. Με τον όρο light, θέλουμε να δηλώσουμε τις ελάχιστες απαιτήσεις σε πόρους (κυρίως ενέργειας), που χρειάζεται αυτή η IDS έκδοση για να λειτουργήσει. Ο Local IDS συνεργάζεται και επικοινωνεί με όλους τους άλλους φυσιολογικούς κόμβους του δικτύου και μαζί με αυτούς και με τους potential attackers. Τρέχοντας ένα τοπικό σύστημα ανίχνευσης (Local IDS) κακόβουλων ενεργειών έχει τη δυνατότητα να κάνει μια πρώτης μορφής ανίχνευση, παρακολουθώντας τη συμπεριφορά των υπόλοιπων κόμβων με τους οποίους επικοινωνεί. Μελετώντας αυτή τη συμπεριφορά και τις ενέργειες των γειτονικών κόμβων, του δίνεται η δυνατότητα να κάνει δύο κινήσεις στο παιχνίδι μας. Καταρχάς εφόσον αξιολογεί πως η κίνηση που

κάνει ο potential attacker του δικτύου είναι φυσιολογική, μπορεί να κάνει μια πρώτη πρόταση για εμπιστοσύνη (suggestion for trusting) στο Global IDS. Αν πάλι θεωρεί πως η ενέργεια του potential attacker είναι κακόβουλη, τότε κάνει πρόταση στο Global IDS για ύποπτο κόμβο (suggestion for suspicious).

Σαν τρίτο παίκτη, ορίζουμε το Global IDS. Το Global IDS δεν είναι τίποτα άλλο από τον σταθμό βάσης του δικτύου (base station), ο οποίος έχει εγκατεστημένο και ένα IDS σύστημα. Το Global IDS, εκτός από το να κάνει ανίχνευση για επιθέσεις, έχει τη δυνατότητα να κρατάει και ιστορικό για όλες τις επιθέσεις που έχουν γίνει στη διάρκεια ζωής του δικτύου. Αυτή του τη δυνατότητα την αξιοποιεί κρατώντας και μια λίστα ταξινόμησης (ranking) που δείχνει πόσες κακόβουλες ενέργειες έχει κάνει κάθε κόμβος του δικτύου. Η κλίμακα της λίστας κυμαίνεται από το 0 μέχρι το 5. Το 0 αντιστοιχεί στο ότι ένα κόμβος λειτουργεί κανονικά και δεν έχει υποπέσει ποτέ σε κακόβουλες ενέργειες, με σκοπό να βλάψει την λειτουργία του δικτύου. Η τιμή 5 δηλώνει πως ένας κόμβος έχει πιαστεί 5 φορές να κάνει επιθετικές / μη αποδεκτές κινήσεις στο δίκτυο. Για κάθε κακόβουλη ενέργεια δηλαδή που κάνει ένας κόμβος, το Global IDS προσθέτει 1 στη λίστα ταξινόμησης που κρατάει. Όταν ένας κόμβος φτάσει να έχει την τιμή 5 σε αυτή τη λίστα, αυτομάτως γίνεται blacklist από το δίκτυο, καθώς το Global IDS δίνει εντολή σε όλους τους άλλους κόμβους να τον αφαιρέσουν από τους πίνακες δρομολόγησης τους. Μπορούμε να πούμε ότι τη συγκεκριμένη στιγμή ο potential attacker γίνεται για το δίκτυο μας insider attacker.

Οι ενέργειες που μπορεί να κάνει το Global IDS στο παιχνίδι μας είναι δύο. Η πρώτη είναι admit, δηλαδή αποδοχή της ενέργειας που έκανε ο potential attacker του δικτύου, σαν απολύτως φυσιολογική. Η δεύτερη επιλογή είναι να κάνει exclude, δηλαδή να θεωρήσει πως η ενέργεια που έγινε από τον potential attacker είναι κακόβουλη. Αυτό έχει ως συνέπεια να χαρακτηρίσει το Global IDS το συγκεκριμένο κόμβο ως επιτιθέμενο για το δίκτυο. Επίσης, αυξάνει τη λίστα ταξινόμησης που κρατάει για το συγκεκριμένο κόμβο κατά 1 μονάδα και εφόσον με αυτή την αύξηση φτάσει στο 5, τον αποκλείει από τους πίνακες δρομολόγησης του δικτύου.

Για λόγους ευκολίας ονομάζουμε το παίγνιο που περιγράψαμε παραπάνω ως GoWiSeN (Game of Wireless Sensor Networks).

6.3 Δημιουργία συναρτήσεων χρησιμότητας των Von Neumann και Morgenstern

Στο κεφάλαιο αυτό θα δημιουργήσουμε τις προτιμήσεις (preferences) για κάθε παίκτη, ταξινομώντας τες από τη λιγότερο έως την περισσότερο προτιμώμενη. Για το σκοπό αυτό θα ακολουθήσουμε τα βήματα όπως παρουσιάζονται στην εργασία "Solving an Incomplete Information Intrusion Detection Game" [Kantzavelou και Katsikas, 2007].

Προτιμήσεις για τον Potential Attacker

A_1: Ο potential attacker του δικτύου κάνει μια ενέργεια επίθεσης. Το Local IDS κάνει suggestion for suspicious και το Global IDS κάνει exclude.

A_2: Ο potential attacker του δικτύου κάνει μια ενέργεια επίθεσης. Το Local IDS κάνει suggestion for suspicious και το Global IDS κάνει admit.

A_3: Ο potential attacker του δικτύου κάνει μια ενέργεια επίθεσης. Το Local IDS κάνει suggestion for trusting και το Global IDS κάνει exclude.

A_4: Ο potential attacker του δικτύου κάνει μια ενέργεια επίθεσης. Το Local IDS κάνει suggestion for trusting και το Global IDS κάνει admit.

A_5: Ο potential attacker του δικτύου κάνει μια κανονική ενέργεια. Το Local IDS κάνει suggestion for suspicious και το Global IDS κάνει exclude.

A_6: Ο potential attacker του δικτύου κάνει μια κανονική ενέργεια. Το Local IDS κάνει suggestion for suspicious και το Global IDS κάνει admit.

A_7: Ο potential attacker του δικτύου κάνει μια κανονική ενέργεια. Το Local IDS κάνει suggestion for trusting και το Global IDS κάνει exclude

A_8: Ο potential attacker του δικτύου κάνει μια ενέργεια επίθεσης. Το Local IDS κάνει suggestion for trusting και το Global IDS κάνει admit.

Έστω ότι A το σύνολο με τις προτιμήσεις του potential attacker. Με βάση όσα περιγράψαμε παραπάνω, ισχύει ότι το A περιλαμβάνει τα παρακάτω στοιχεία:

$A = \{A_1, A_2, A_3, A_4, A_5, A_6, A_7, A_8\}$

Τοποθετώντας αυτές τις προτιμήσεις σε μια σειρά κατάταξης από τη λιγότερο έως την περισσότερο επιθυμητή, παίρνουμε το παρακάτω:

$A_1 < A_3 < A_2 < A_5 < A_7 < A_6 < A_8 < A_4$

Από το σύνολο των προτιμήσεων και τις μεταξύ τους σχέσεις που αντικατοπτρίζονται στη σειρά κατάταξης, θα ορίσουμε την αντίστοιχη συνάρτηση χρησιμότητας για τον παίκτη potential attacker. Υποθέτουμε ότι $U_A : \{ A_1, A_2, A_3, A_4, A_5, A_6, A_7, A_8\} \rightarrow R$ είναι η συνάρτηση χρησιμότητας του potential attacker. Εκτιμώντας τις προτιμήσεις του δεν του αρέσει καθόλου να συμβαίνει το A_1. Δε θέλει δηλαδή καθόλου, όταν κάνει μια ενέργεια επίθεσης αυτή να ανιχνεύεται και από τα δύο IDS συστήματα του δικτύου Global και Local. Οπότε έχουμε $U_A(A_1) = 0$. Αντίθετα προτιμά περισσότερο από οτιδήποτε άλλο το A_4. Του αρέσει δηλαδή όταν κάνει επίθεση να μην τον ανιχνεύουν τα IDS συστήματα. Επομένως ισχύει ότι $U_A(A_4) = 1$. Επιλέγουμε ανάμεσα στα A_5 και A_7 τα οποία είναι ενδιάμεσες προτιμήσεις, αποφασίζουμε να ορίσουμε ως μέση το A_5, οπότε έχουμε $U_A(A_5) = ½$. Στη συνέχεια, επειδή το A_6 είναι ενδιάμεσος στα A_5 και A_4, ορίζουμε $U_A(A_6) = ¾$.

Αναλυτικά υπολογίζουμε όλες τις τιμές της συνάρτησης χρησιμότητας για τον παίκτη potential attacker:

$$U_A(A_6) = U_A(A_5) + \frac{U_A(A_4) - U_A(A_5)}{2} = \frac{1}{2} + \frac{1 - \frac{1}{2}}{2} = \frac{1}{2} + \frac{\frac{1}{2}}{2} = \frac{1}{2} + \frac{1}{4} = \frac{3}{4}$$

$$U_A(A_7) = U_A(A_5) + \frac{U_A(A_6) - U_A(A_5)}{2} = \frac{1}{2} + \frac{\frac{3}{4} - \frac{1}{2}}{2} = \frac{1}{2} + \frac{\frac{1}{4}}{2} = \frac{1}{2} + \frac{1}{8} = \frac{5}{8}$$

$$U_A(A_8) = U_A(A_6) + \frac{U_A(A_4) - U_A(A_6)}{2} = \frac{3}{4} + \frac{1 - \frac{3}{4}}{2} = \frac{3}{4} + \frac{\frac{1}{4}}{2} = \frac{3}{4} + \frac{1}{8} = \frac{7}{8}$$

$$U_A(A_3) = U_A(A_1) + \frac{U_A(A_5) - U_A(A_1)}{2} = 0 + \frac{\frac{1}{2} - 0}{2} = 0 + \frac{\frac{1}{2}}{2} = 0 + \frac{1}{4} = \frac{1}{4}$$

$$U_A(A_2) = U_A(A_3) + \frac{U_A(A_5) - U_A(A_3)}{2} = \frac{1}{4} + \frac{\frac{1}{2} - \frac{1}{4}}{2} = \frac{1}{4} + \frac{\frac{1}{4}}{2} = \frac{1}{4} + \frac{1}{8} = \frac{3}{8}$$

Με αυτό τον τρόπο αντί να έχουμε μια ταξινόμηση που θα περιλαμβάνει δεκαδικούς αριθμούς και κλάσματα, προτιμούμε τους ακέραιους αριθμούς για την αναπαράσταση των προτιμήσεων, οι οποίοι είναι και πολύ βολικοί στους υπολογισμούς μας.

Ο πίνακας 10 παρουσιάζει συνοπτικά στη δεύτερη γραμμή τα utilities που προκύπτουν για κάθε προτίμηση του παίκτη potential attacker. Η τρίτη γραμμή του πίνακα περιλαμβάνει τις αντίστοιχες utilities αφού έχουν μετατραπεί σε ακέραιους αριθμούς από κλάσματα πολλαπλασιάζοντας με το 24.

X	A_1	A_3	A_2	A_5	A_7	A_6	A_8	A_4
$U_A(x)$	0	1/4	3/8	1/2	5/8	3/4	7/8	1
$U'_A(x)$	0	6	9	12	15	18	21	24

Πίνακας 10: Προτιμήσεις του potential attacker

Προτιμήσεις για το Local IDS

L_1: Το Local IDS κάνει suggestion for suspicious σε μια ενέργεια επίθεσης του potential attacker και στη συνέχεια το Global IDS κάνει exclude.

L_2: Το Local IDS κάνει suggestion for suspicious σε μια ενέργεια επίθεσης του potential attacker και στη συνέχεια το Global IDS κάνει admit.

L_3: Το Local IDS κάνει suggestion for trusting σε μια ενέργεια επίθεσης του potential attacker και στη συνέχεια το Global IDS κάνει exclude.

L_4: Το Local IDS κάνει suggestion for trusting σε μια ενέργεια επίθεσης του potential attacker και στη συνέχεια το Global IDS κάνει admit.

L_5: Το Local IDS κάνει suggestion for suspicious σε μια κανονική ενέργεια του potential attacker και στη συνέχεια το Global IDS κάνει exclude.

L_6: Το Local IDS κάνει suggestion for suspicious σε μια κανονική ενέργεια του potential attacker και το Global IDS κάνει admit.

L_7: Το Local IDS κάνει suggestion for trusting σε μια κανονική ενέργεια του potential attacker και το Global IDS κάνει exclude.

L_8: Το Local IDS κάνει suggestion for trusting σε μια κανονική ενέργεια του potential attacker και το Global IDS κάνει admit.

Αντιστοίχως με πριν, έστω ότι L το σύνολο με τις προτιμήσεις του Local IDS. Με βάση όσα περιγράψαμε παραπάνω ισχύει ότι το L περιλαμβάνει τα παρακάτω στοιχεία:

$L = \{L_1, L_2, L_3, L_4, L_5, L_6, L_7, L_8\}$

Τοποθετώντας αυτές τις προτιμήσεις σε μια σειρά κατάταξης από τη λιγότερο έως την περισσότερο επιθυμητή, παίρνουμε το παρακάτω:

$L_4 < L_5 < L_3 < L_6 < L_7 < L_2 < L_8 < L_1$

Από το σύνολο των προτιμήσεων και τις μεταξύ τους σχέσεις, που αντικατοπτρίζονται στη σειρά κατάταξης, θα ορίσουμε την αντίστοιχη συνάρτηση χρησιμότητας για τον παίκτη Local IDS. Υποθέτοντας ότι $U_L : \{ L_1, L_2, L_3, L_4, L_5, L_6, L_7, L_8\} \rightarrow R$ είναι η συνάρτηση χρησιμότητας του Local IDS. Εκτιμώντας τις προτιμήσεις του δεν του αρέσει καθόλου να συμβαίνει το L_4. Δεν του αρέσει δηλαδή να κάνει suggestion for trusting μια ενέργεια επίθεσης, η οποία στη συνέχεια γίνεται και admit από το Global IDS. Οπότε έχουμε $U_L(L_4) = 0$. Αντίθετα προτιμά περισσότερο από οτιδήποτε άλλο το L_1. Θέλει να προτείνει ως ύποπτες, ενέργειες επίθεσης τις οποίες μετέπειτα το Global IDS θα κάνει exclude. Επομένως $U_L(L_1) = 1$. Επιλέγουμε ανάμεσα στα L_6 και L_7 τα οποία είναι ενδιάμεσες προτιμήσεις, αποφασίζουμε να ορίσουμε ως μέση το L_6, οπότε έχουμε $U_L(L_6) = ½$. Στη συνέχεια, επειδή το L_2 είναι ενδιάμεσος στα L_6 και L_1, ορίζουμε $U_L(L_2) = ¾$.

Αναλυτικά υπολογίζουμε όλες τις τιμές της συνάρτησης χρησιμότητας για τον παίκτη Local IDS:

$$U_L(L_2) = U_L(L_6) + \frac{U_L(L_1) - U_L(L_6)}{2} = \frac{1}{2} + \frac{1 - \frac{1}{2}}{2} = \frac{1}{2} + \frac{\frac{1}{2}}{2} = \frac{1}{2} + \frac{1}{4} = \frac{3}{4}$$

$$U_L(L_7) = U_L(L_6) + \frac{U_L(L_2) - U_L(L_6)}{2} = \frac{1}{2} + \frac{\frac{3}{4} - \frac{1}{2}}{2} = \frac{1}{2} + \frac{\frac{1}{4}}{2} = \frac{1}{2} + \frac{1}{8} = \frac{5}{8}$$

$$U_L(L_8) = U_L(L_2) + \frac{U_L(L_1) - U_L(L_2)}{2} = \frac{3}{4} + \frac{1 - \frac{3}{4}}{2} = \frac{3}{4} + \frac{\frac{1}{4}}{2} = \frac{3}{4} + \frac{1}{8} = \frac{7}{8}$$

$$U_L(L_5) = U_L(L_4) + \frac{U_L(L_6) - U_L(L_4)}{2} = 0 + \frac{\frac{1}{2} - 0}{2} = 0 + \frac{\frac{1}{2}}{2} = 0 + \frac{1}{4} = \frac{1}{4}$$

$$U_L(L_3) = U_L(L_5) + \frac{U_L(L_6) - U_L(L_5)}{2} = \frac{1}{4} + \frac{\frac{1}{2} - \frac{1}{4}}{2} = \frac{1}{4} + \frac{\frac{1}{4}}{2} = \frac{1}{4} + \frac{1}{8} = \frac{3}{8}$$

Ο πίνακας 11 παρουσιάζει συνοπτικά στη δεύτερη γραμμή τα utilities που προκύπτουν για κάθε προτίμηση του παίκτη Local IDS. Η τρίτη γραμμή του πίνακα περιλαμβάνει τις αντίστοιχες utilities, αφού έχουν μετατραπεί σε ακέραιους αριθμούς από κλάσματα πολλαπλασιάζοντας με 24.

X	L_4	L_5	L_3	L_6	L_7	L_2	L_8	L_1
$U_L(x)$	0	1/4	3/8	1/2	5/8	3/4	7/8	1
$U'_L(x)$	0	6	9	12	15	18	21	24

Πίνακας 11: Προτιμήσεις του Local IDS

Προτιμήσεις για το Global IDS

G_1: Ο potential attacker του δικτύου κάνει μια ενέργεια επίθεσης. Το Local IDS κάνει suggestion for suspicious και το Global IDS κάνει exclude.

G_2: Ο potential attacker του δικτύου κάνει μια ενέργεια επίθεσης. Το Local IDS κάνει suggestion for suspicious και το Global IDS κάνει admit.

G_3: Ο potential attacker του δικτύου κάνει μια ενέργεια επίθεσης. Το Local IDS κάνει suggestion for trusting και το Global IDS κάνει exclude.

G_4: Ο potential attacker του δικτύου κάνει μια ενέργεια επίθεσης. Το Local IDS κάνει suggestion for trusting και το Global IDS κάνει admit.

G_5: Ο potential attacker του δικτύου κάνει μια κανονική ενέργεια. Το Local IDS κάνει suggestion for suspicious και το Global IDS κάνει exclude.

G_6: Ο potential attacker του δικτύου κάνει μια κανονική ενέργεια. Το Local IDS κάνει suggestion for suspicious και το Global IDS κάνει admit.

G_7: Ο potential attacker του δικτύου κάνει μια κανονική ενέργεια. Το Local IDS κάνει suggestion for trusting και το Global IDS κάνει exclude

G_8: Ο potential attacker του δικτύου κάνει μια ενέργεια επίθεσης. Το Local IDS κάνει suggestion for trusting και το Global IDS κάνει admit.

Αντιστοίχως με τα προηγούμενα, έστω ότι G το σύνολο με τις προτιμήσεις του Global IDS. Με βάση όσα περιγράψαμε παραπάνω, ισχύει ότι το G περιλαμβάνει τα παρακάτω στοιχεία:

$G = \{G_1, G_2, G_3, G_4, G_5, G_6, G_7, G_8\}$

Τοποθετώντας αυτές τις προτιμήσεις σε μια σειρά κατάταξης, από τη λιγότερο έως την περισσότερο επιθυμητή, παίρνουμε το παρακάτω:

$G_2 < G_4 < G_5 < G_3 < G_6 < G_7 < G_8 < G_1$

Από το σύνολο των προτιμήσεων και τις μεταξύ τους σχέσεις, που αντικατοπτρίζονται στη σειρά κατάταξης, θα ορίσουμε μια αντίστοιχη συνάρτηση χρησιμότητας για τον παίκτη Global IDS. Θεωρούμε $U_G : \{ G_1, G_2, G_3, G_4, G_5, G_6, G_7, G_8\} \rightarrow R$ τη συνάρτηση

χρησιμότητας του Global IDS. Εκτιμώντας τις προτιμήσεις του, δεν του αρέσει καθόλου να συμβαίνει το G_2. Δεν του αρέσει δηλαδή, να κάνει admit ένα attacking action, το οποίο έχει γίνει suggestion for suspicious από το Local IDS. Οπότε έχουμε $U_G(G_2) = 0$. Αντίθετα, προτιμά περισσότερο από οτιδήποτε άλλο το G_1. Θέλει να κάνει exclude attacking actions, οι οποίες πρώτα έχουν γίνει και suggestion for suspicious από το Local IDS. Επομένως $U_G(G_1) = 1$. Επιλέγουμε ανάμεσα στα G_3 και G_5 τα οποία είναι ενδιάμεσες προτιμήσεις, αποφασίζουμε να ορίσουμε ως μέση το G_3, οπότε έχουμε $U_G(G_3) = ½$. Στη συνέχεια, επειδή το G_7 είναι ενδιάμεσος στα G_3 και G_1, ορίζουμε $U_G(G_7) = ¾$.

Αναλυτικά υπολογίζομε όλες τις συναρτήσεις χρησιμότητας για τον παίκτη Global IDS:

$$U_G(G_7) = U_G(G_3) + \frac{U_G(G_1) - U_G(G_3)}{2} = \frac{1}{2} + \frac{1 - \frac{1}{2}}{2} = \frac{1}{2} + \frac{\frac{1}{2}}{2} = \frac{1}{2} + \frac{1}{4} = \frac{3}{4}$$

$$U_G(G_6) = U_G(G_3) + \frac{U_G(G_7) - U_G(G_3)}{2} = \frac{1}{2} + \frac{\frac{3}{4} - \frac{1}{2}}{2} = \frac{1}{2} + \frac{\frac{1}{4}}{2} = \frac{1}{2} + \frac{1}{8} = \frac{5}{8}$$

$$U_G(G_8) = U_G(G_7) + \frac{U_G(G_1) - U_G(G_7)}{2} = \frac{3}{4} + \frac{1 - \frac{3}{4}}{2} = \frac{3}{4} + \frac{\frac{1}{4}}{2} = \frac{3}{4} + \frac{1}{8} = \frac{7}{8}$$

$$U_G(G_4) = U_G(G_2) + \frac{U_G(G_3) - U_G(G_2)}{2} = 0 + \frac{\frac{1}{2} - 0}{2} = 0 + \frac{\frac{1}{2}}{2} = 0 + \frac{1}{4} = \frac{1}{4}$$

$$U_G(G_5) = U_G(G_4) + \frac{U_G(G_3) - U_G(G_4)}{2} = \frac{1}{4} + \frac{\frac{1}{2} - \frac{1}{4}}{2} = \frac{1}{4} + \frac{\frac{1}{4}}{2} = \frac{1}{4} + \frac{1}{8} = \frac{3}{8}$$

Ο πίνακας 12 παρουσιάζει συνοπτικά στη δεύτερη γραμμή, τα utilities που προκύπτουν για κάθε προτίμηση του παίκτη Global IDS. Η τρίτη γραμμή του πίνακα, περιλαμβάνει τις αντίστοιχες utilities, αφού πρώτα έχουν μετατραπεί σε ακέραιους αριθμούς από κλάσματα μετά από πολλαπλασιασμό με το 24.

X	G_2	G_4	G_5	G_3	G_6	G_7	G_8	G_1
$U_G(x)$	0	1/4	3/8	1/2	5/8	3/4	7/8	1
$U'_G(x)$	0	6	9	12	15	18	21	24

Πίνακας 12: Προτιμήσεις του Global IDS

6.4 Δημιουργία Αποδόσεων

Οι συναρτήσεις χρησιμότητας U_A, U_L, και U_G που περιγράψαμε στην προηγούμενη ενότητα, καθορίζουν τα payoffs του κάθε κόμβου στην εκτεταμένη μορφή του παιγνίου μας.

Τα payoffs και των τριών παικτών κυμαίνονται μεταξύ του 0 και του 24. Ξεκινώντας από τον Potential Attacker, βλέπουμε πως έχει το μικρότερο κέρδος (0), όταν επιχειρεί attacking action, αλλά τα Local και Global IDS δεν τον αφήνουν να ολοκληρώσει την κακόβουλη ενέργεια του. Αντίθετα, κερδίζει 24 πόντους όταν κάνει επίθεση η οποία δεν ανιχνεύεται από κανένα από τα δύο IDS συστήματα του δικτύου. 21 πόντους κερδίζει όταν ενεργεί φυσιολογικά στο δίκτυο και τα δύο IDS τον εμπιστεύονται. 18 πόντους κερδίζει όταν κάνει φυσιολογική ενέργεια, το Local IDS κάνει suggestion for suspicious, αλλά το Global IDS τον αφήνει να συνεχίσει. Επιπλέον έχει όφελος 15 πόντους όταν ενεργεί κανονικά, το Local IDS τον εμπιστεύεται, αλλά το Global IDS τον αποκλείει, ενώ κερδίζει 12 πόντους σε normal action, αλλά με τα δύο IDS να τον εμποδίζουν τελικά. Ο potential attacker έχει μικρό κέρδος, 9 πόντους, όταν κάνει επίθεση, ενώ το Local IDS κάνει suggestion for suspicious και το Global IDS κάνει admit. Επίσης, σε επίθεση έχει απολαβή 6 πόντων, όταν τον εμπιστεύεται το Local IDS, αλλά τον εμποδίζει το Global IDS.

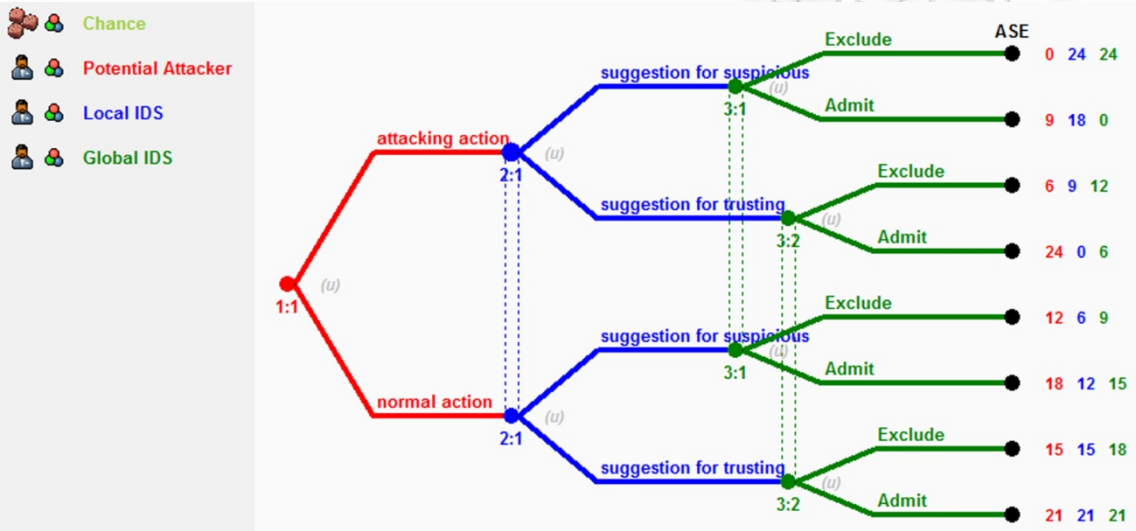
Το Local IDS έχει το μεγαλύτερο όφελος εκεί που είναι η χειρότερη επιλογή του attacker. Κερδίζει 24 πόντους όταν κάνει suggestion for suspicious μια ενέργεια επίθεσης και παράλληλα το Global IDS συμφωνεί μαζί του κάνοντας Exclude. Παίρνει το μικρότερο κέρδος (0), όταν γίνεται επίθεση στο δίκτυο αλλά τα Local και Global

IDS δεν την ανιχνεύουν. Το 2ο καλύτερο σενάριο με 21 πόντους είναι όταν και τα δύο IDS εμπιστεύονται μια φυσιολογική ενέργεια. Στη συνέχεια έχουμε 18 πόντους κέρδος για το Local IDS που κάνει suggestion for suspicious ένα attacking action, ενώ λανθασμένα το Global IDS παίζει Admit. 15 πόντους θα πάρει το Local IDS που σωστά εμπιστεύεται φυσιολογικές ενέργειες, αλλά το Global IDS τις αποκλείει. Επιπλέον κερδίζει 12 πόντους όταν κάνει suggestion for suspicious μια normal action, η οποία γίνεται όμως Admit από το Global IDS. Το Local IDS θα πάρει 9 πόντους όταν κάνει λανθασμένα πρόταση για εμπιστοσύνη σε ένα attacking action, το οποίο τελικά θα κοπεί από το Global IDS. Τέλος 6 πόντους όφελος για το Local IDS, όταν μια φυσιολογική ενέργεια την κόψουν και τα δύο IDS συστήματα.

Αντίστοιχα με του Local IDS είναι τα δύο μεγαλύτερα payoffs για το Global IDS 24 (attacking action - suggestion for suspicious - Exclude) και 21 (normal action - suggestion for trusting - Admit). Η χειρότερη επιλογή για το Global IDS είναι να κάνει Admit μια ενέργεια επίθεσης που την έχει πρώτα κάνει suggestion for suspicious το Local IDS. Όφελος 18 πόντων έχει το Global IDS, όταν κάνει Exclude μια κανονική ενέργεια, που πρώτα έχει γίνει suggestion for trusting από το Local IDS. Το 2ο μικρότερο κέρδος με 6 πόντους έχει το Global IDS, όταν κάνει Admit ένα attacking action το οποίο έχει κάνει suggestion for trusting το Local IDS. 9 πόντους κερδίζει το Global IDS, όταν κάνει Exclude μια φυσιολογική ενέργεια, την οποία έχει κάνει το Local IDS suggestion for suspicious. Επίσης, 12 πόντους όφελος θα έχει το Global IDS στην περίπτωση που γίνεται Exclude μια ενέργεια επίθεσης, την οποία πρώτα κακώς έχει κάνει suggestion for trusting το Local IDS. Τέλος, όταν έχουμε τον potential attacker να λειτουργεί φυσιολογικά, το Local IDS να κάνει λανθασμένα suggestion for suspicious την ενέργειά του, αλλά το Global IDS να παίζει Admit, το κέρδος είναι 15 πόντοι για τον τελευταίο παίκτη.

Στην εικόνα 12 παρουσιάζεται η εκτεταμένη μορφή του παιγνίου όπως προκύπτει μέσα από το πρόγραμμα Gambit. Με τρία διαφορετικά χρώματα παρουσιάζονται οι τρείς παίκτες. Κόκκινο για τον Potential Attacker, μπλε για το Local IDS και τέλος πράσινο για το Global IDS. Στη συγκεκριμένη μορφή δέντρου, όπου παρουσιάζεται το παιχνίδι, μπορούμε να δούμε βήμα βήμα την εξέλιξη του παιχνιδιού. Αρχικά ξεκινάει ο potential attacker, ο οποίος έχει τη δυνατότητα να κάνει δύο διαφορετικές ενέργειες attacking και normal action. Στη συνέχεια έχουμε τον παίκτη Local IDS, με διαθέσιμες κινήσεις

suggestion for suspicious και suggestion for trusting, για κάθε action του potential attacker. Ακολουθεί το Global IDS που παίρνει την τελική απόφαση για την ενέργεια του potential attacker. Το Global IDS μπορεί να επιλέξει να παίξει είτε Exclude, όταν θέλει να αποκλείσει την ενέργεια, είτε Admit, όταν δεν ανιχνεύει κάτι κακόβουλο και θεωρεί την ενέργεια απολύτως φυσιολογική.



Εικόνα 12: Η εκτεταμένη μορφή του παιγνίου GoWiSeN

Για κάθε μια σειρά κινήσεων μπορούμε να δημιουργήσουμε συντομογραφίες ώστε να αναφερόμαστε ευκολότερα σε αυτές. Για παράδειγμα μπορούμε να ορίσουμε ως ASE την περίπτωση που ο potential attacker κάνει attacking action, το Local IDS κάνει suggestion for suspicious και το Global IDS παίζει Exclude. Στον παρακάτω πίνακα παρουσιάζονται αναλυτικά όλες οι κινήσεις με τις συντομογραφίες τους.

Potential Attacker	Local IDS	Global IDS	Συντομογραφία
Attacking action	Suggestion for suspicious	Exclude	ASE
Attacking action	Suggestion for suspicious	Admit	ASA
Attacking action	Suggestion for trusting	Exclude	ATE
Attacking action	Suggestion for trusting	Admit	ATA

Normal action	Suggestion for suspicious	Exclude	NSE
Normal action	Suggestion for suspicious	Admit	NSA
Normal action	Suggestion for trusting	Exclude	NTE
Normal action	Suggestion for trusting	Admit	NTA

Πίνακας 13: Κινήσεις παικτών του παιγνίου GoWiSeN

6.5 Επίλυση Παιγνίου

Σε αυτή την ενότητα θα λύσουμε το παιχνίδι βασιζόμενοι σε τεχνικές από τη θεωρία των παιγνίων, αλλά χρησιμοποιώντας και το πρόγραμμα επίλυσης προβλημάτων θεωρίας παιγνίων Gambit. Στη συνέχεια θα εξηγήσουμε τα αποτελέσματα που βρήκαμε.

Μέχρι στιγμής στο κεφάλαιο 3 είδαμε ανάλυση και επίλυση παιχνιδιών που είχαν μέχρι 2 παίκτες. Στη περίπτωση μας το παιχνίδι που έχουμε δημιουργήσει αποτελείται από 3 διαφορετικούς παίκτες (potential attacker, Local IDS, Global IDS). Η προφανής διαφορά ανάμεσα σε παιχνίδια δύο και τριών παικτών είναι η πολυπλοκότητα που έχει το δέντρο του παιγνίου. Για κάθε παίκτη που έχει τη δυνατότητα να κινηθεί μια φορά, το δέντρο πρέπει να έχει τρία επίπεδα. Επίσης αυξάνεται και ο αριθμός των διαθέσιμων επιλογών για κάθε παίκτη ο οποίος αυξάνει το μέγεθος του δέντρου.

Όταν ένα παιχνίδι παίζεται ανάμεσα σε περισσότερους από δύο παίκτες, ο καθένας από τους οποίους έχει έναν σχετικά μικρό αριθμό από καθαρές (pure) στρατηγικές, η ανάλυση του μπορεί να γίνει μέσω πίνακα. Ο πίνακας χρειάζεται να είναι τριών διαστάσεων και οι στρατηγικές του τρίτου παίκτη θα αντιστοιχούν στην νέα διάσταση. Ο ευκολότερος τρόπος για να προστεθεί μια τρίτη διάσταση σε ένα πίνακα παιχνιδιού δύο διαστάσεων είναι με το να προστεθούν σελίδες (add pages). Η πρώτη σελίδα του πίνακα δείχνει τα payoffs για την πρώτη στρατηγική του τρίτου παίκτη. Η δεύτερη σελίδα δείχνει τα payoffs για τη δεύτερη στρατηγική του τρίτου παίκτη κ.λ.π.

Στους πίνακες 14 και 15 δείχνουμε τον πίνακα των τριών διαστάσεων για το παιχνίδι μας. Ο πίνακας έχει δυο γραμμές για τις στρατηγικές του Local IDS (suggestion for suspicious και suggestion for trusting), δύο στήλες για τις στρατηγικές του Global IDS (Exclude, Admit) και δύο σελίδες για τις στρατηγικές του potential attacker (attack ή normal action). Οι δύο σελίδες παρουσιάζονται η μια μετά την άλλη ώστε να φαίνονται όλα την ίδια στιγμή. Σε κάθε κελί υπάρχουν τα payoffs με την ακόλουθη σειρά potential attacker, Local IDS, Global IDS [Dixit και Skeath, 1999].

Ο potential attacker επιλέγει attacking action

		Global IDS	
		Exclude	Admit
Local IDS	Suggestion for suspicious	0 , 24 , 24	9 , 18 , 0
	Suggestion for trusting	6 , 9 , 12	24 , 0 , 6

Πίνακας 14: Ο potential attacker επιλέγει attacking action

Ο potential attacker επιλέγει normal action

		Global IDS	
		Exclude	Admit
Local IDS	Suggestion for suspicious	12 , 6 , 9	18 , 12 , 15
	Suggestion for trusting	15 , 15 , 18	21 , 21 , 21

Πίνακας 15: Ο potential attacker επιλέγει normal action

Η προσπάθεια μας θα πρέπει να επικεντρωθεί στο αν υπάρχουν κυρίαρχες στρατηγικές για οποιονδήποτε από τους παίκτες. Στον κάθε πίνακα ακολουθούμε την παρακάτω λογική. Συγκρίνουμε τα αποτελέσματα που συνδέονται με τις στρατηγικές ενός παίκτη με τα αποτελέσματα που συνδέονται με άλλες στρατηγικές του παίκτη.

Στο παίγνιο αυτό είναι πιθανό να υπάρχουν πολλαπλές ισορροπίες κατά Nash, αλλά εάν στο παίγνιο υπάρχουν κυρίαρχες στρατηγικές για κάθε παίκτη, τότε θα καταλήξουμε σε μια μόνο ισορροπία. Για αυτό θα επιλύσουμε το παίγνιο με τη μέθοδο των κυρίαρχων στρατηγικών, αλλά θα αποδείξουμε επίσης ότι η ισορροπία που βρίσκουμε είναι και ισορροπία κατά Nash. Έτσι θα επαληθευτεί το γνωστό ρητό "all is Nash", που σημαίνει ότι οποιαδήποτε ισορροπία σε ένα παίγνιο βρίσκεται με οποιαδήποτε μέθοδο επίλυσης θα είναι και ισορροπία Nash.

6.6 Επίλυση με τη μέθοδο της κυριαρχίας

Θα πρέπει να ελέγξουμε εάν υπάρχουν κυρίαρχες στρατηγικές για κάθε παίκτη ξεχωριστά. Αρκεί δύο από τους παίκτες να έχουν κυρίαρχη στρατηγική προκειμένου να καταλήξουμε σε κάποια ισορροπία. Εάν κανένας παίκτης δεν έχει κυρίαρχη στρατηγική, δε θα μπορέσουμε να καταλήξουμε σε κάποια ισορροπία και έτσι θα πρέπει να ελέγξουμε εάν υπάρχει ισορροπία σε μικτές στρατηγικές.

Για να βρούμε εάν υπάρχει κυριαρχία, θα πρέπει να συγκρίνουμε τις αποδόσεις κάθε παίκτη, κάθε φορά που επιλέγει μια στρατηγική, με τις αποδόσεις του ιδίου παίκτη, όταν αυτός επιλέγει μια δεύτερη στρατηγική. Για να γίνει αυτό, θα εργαστούμε με κάθε πίνακα ξεχωριστά. Κάθε φορά θα συγκρίνουμε για το Local IDS, τις αποδόσεις του μεταξύ των δυο σειρών για τις στρατηγικές suggestion for suspicious και suggestion for trusting. Αντίστοιχα, για το Global IDS θα συγκρίνουμε τις αποδόσεις του μεταξύ των δυο στηλών για τις στρατηγικές exclude και admit. Υπενθυμίζουμε ότι σε κάθε κελί του πίνακα οι αποδόσεις είναι κατά σειρά (potential attacker, Local IDS, Global IDS).

Έστω ότι ο potential attacker επιλέγει attacking action

Δεδομένου ότι το Global IDS προτιμά τη στρατηγική exclude, το Local IDS θα επιλέξει τη στρατηγική suggestion for suspicious που του δίνει μεγαλύτερη απόδοση (24 > 9). Ομοίως, δεδομένου ότι το Global IDS προτιμά τη στρατηγική admit, το Local IDS θα επιλέξει και πάλι τη στρατηγική suggestion for suspicious, αφού του δίνει επίσης

μεγαλύτερη απόδοση (18 > 0). Δηλαδή, η στρατηγική suggestion for trusting είναι κυριαρχούμενη από τη στρατηγική suggestion for suspicious. Με άλλα λόγια, το Local IDS θα προτιμήσει τη στρατηγική suggestion for suspicious, ανεξάρτητα από το τι θα κάνει το Global IDS. Συνεπώς, αφού η στρατηγική που κυριαρχεί για το Local IDS είναι αυτή του suggestion for suspicious, τότε στον πίνακα 16 θα διαγράψουμε τη δεύτερη σειρά.

Έστω τώρα ότι το Local IDS προτιμά τη στρατηγική suggestion for suspicious, το Global IDS θα επιλέξει τη στρατηγική exclude, δεδομένου ότι του δίνει μεγαλύτερη απόδοση (24 > 0). Ομοίως, δεδομένου ότι το Local IDS προτιμά τη στρατηγική suggestion for trusting, το Global IDS θα επιλέξει και πάλι τη στρατηγική exclude αφού του δίνει επίσης μεγαλύτερη απόδοση (12 > 6). Δηλαδή, η στρατηγική admit είναι κυριαρχούμενη από τη στρατηγική exclude. Με άλλα λόγια, το Global IDS θα προτιμήσει τη στρατηγική exclude, ανεξάρτητα από το τι θα κάνει το Local IDS. Συνεπώς, αφού η στρατηγική που κυριαρχεί για το Global IDS είναι αυτή του exclude, τότε στον πίνακα 16 θα διαγράψουμε τη δεύτερη στήλη.

Ο νέος πίνακας αποδόσεων (πίνακας 16), όταν ο potential attacker επιλέγει attacking action, θα έχει ως εξής:

		Global IDS	
		Exclude	Admit
Local IDS	Suggestion for suspicious	0 , 24 , 24	~~9 , 18 , 0~~
	Suggestion for trusting	~~6 , 9 , 12~~	~~24 , 0 , 6~~

Πίνακας 16: Πίνακας αποδόσεων όταν ο potential attacker επιλέγει attacking action

Παρατηρούμε ότι και οι δυο παίκτες Local IDS και Global IDS έχουν κυρίαρχη στρατηγική, προϋπόθεση απαραίτητη προκειμένου να καταλήξουμε σε κάποια ισορροπία, αφού απαιτείται να υπάρχει κυρίαρχη στρατηγική για τουλάχιστον δυο εκ των τριών παικτών. Στο συγκεκριμένο άρα υποπαίγνιο υπάρχει μία και μοναδική ισορροπία, η οποία προφανώς είναι η:

(attacking action, suggestion for suspicious, exclude) = (0, 24, 24) = (ASE)

Θα δείξουμε τέλος, ότι η παραπάνω ισορροπία (ASE) αποτελεί και ισορροπία κατά Nash. Αυτό θα ισχύει εάν αυτό που κάνει κάθε παίκτης, είναι για τον εαυτό του η βέλτιστη απόκριση. Δηλαδή, θα πρέπει κανένας από τους δυο παίκτες να μην έχει μονομερώς κίνητρο να ξεφύγει από την κατάσταση ισορροπίας. Ισχύει ότι εάν θεωρήσουμε δεδομένο ότι το Local IDS θα επιλέξει τη στρατηγική suggestion for suspicious, συμφέρει το Global IDS να επιλέξει τη στρατηγική exclude. Αυτό συμπεραίνεται από τη σύγκριση των δυο στηλών (24 > 0).

Αντιστρόφως , εάν θεωρήσουμε δεδομένο ότι το Global IDS θα επιλέξει τη στρατηγική exclude, συμφέρει το Local IDS να επιλέξει τη στρατηγική suggestion for suspicious. Είναι προφανές ότι κανένας από τους παίκτες δεν έχει κίνητρο να ξεφύγει από την ισορροπία (attacking action, suggestion for suspicious, exclude). Συνεπώς η ισορροπία αυτή αποτελεί και ισορροπία κατά Nash και έτσι επαληθεύεται το ρητό “all is Nash”.

Έστω ότι ο potential attacker επιλέγει normal action

Έστω ότι το Global IDS προτιμά τη στρατηγική exclude, το Local IDS θα επιλέξει τη στρατηγική suggestion for trusting που του δίνει μεγαλύτερη απόδοση (15 > 6). Ομοίως, δεδομένου ότι το Global IDS προτιμά τη στρατηγική admit, το Local IDS θα επιλέξει και πάλι τη στρατηγική suggestion for trusting, αφού του δίνει επίσης μεγαλύτερη απόδοση (21 > 12). Δηλαδή, η στρατηγική suggestion for suspicious είναι κυριαρχούμενη από τη στρατηγική suggestion for trusting. Με άλλα λόγια το Local IDS θα προτιμήσει τη στρατηγική suggestion for trusting, ανεξάρτητα από το τι θα κάνει το Global IDS. Συνεπώς, αφού η στρατηγική που κυριαρχεί για το Local IDS είναι αυτή του suggestion for trusting, στον πίνακα 17 θα διαγράψουμε την πρώτη σειρά.

Δεδομένου ότι το Local IDS προτιμά τη στρατηγική suggestion for suspicious, το Global IDS θα επιλέξει τη στρατηγική admit, επειδή του δίνει μεγαλύτερη απόδοση (15 > 9). Ομοίως, δεδομένου ότι το Local IDS προτιμά τη στρατηγική suggestion for trusting, το Global IDS θα επιλέξει και πάλι τη στρατηγική admit, αφού του δίνει επίσης μεγαλύτερη απόδοση (21 > 18). Δηλαδή, η στρατηγική exclude είναι κυριαρχούμενη από τη στρατηγική admit. Με άλλα λόγια, το Global IDS θα προτιμήσει τη στρατηγική admit, ανεξάρτητα από το τι θα κάνει το Local IDS. Συνεπώς, αφού η

στρατηγική που κυριαρχεί για το Global IDS είναι αυτή του admit, τότε στον πίνακα 17 θα διαγράψουμε την πρώτη στήλη.

Ο νέος πίνακας αποδόσεων (πίνακας 17), όταν ο potential attacker επιλέγει normal action, θα έχει ως εξής:

		Global IDS	
		Exclude	Admit
Local IDS	Suggestion for suspicious	~~12 , 6 , 9~~	~~18 , 12 , 15~~
	Suggestion for trusting	~~15 , 15 , 18~~	21 , 21 , 21

Πίνακας 17: Πίνακας αποδόσεων όταν ο potential attacker επιλέγει normal action

Παρατηρούμε ότι και πάλι και οι δυο παίκτες Local IDS και Global IDS έχουν κυρίαρχη στρατηγική. Στο συγκεκριμένο άρα υποπαίγνιο, υπάρχει μία και μοναδική ισορροπία, στην οποία όλοι οι παίκτες λαμβάνουν απόδοση 21. Η ισορροπία αυτή είναι συμφέρουσα και για τον potential attacker, αφού στην περίπτωση αυτή λαμβάνει την μεγαλύτερη απόδοση. Η ισορροπία που προκύπτει είναι η ακόλουθη:

(normal action, suggestion for trusting, admit) = (ATA) = (21, 21, 21)

Τέλος, θα δείξουμε ότι η παραπάνω ισορροπία αποτελεί και ισορροπία κατά Nash. Αυτό θα ισχύει εάν αυτό που κάνει κάθε παίκτης, είναι για τον εαυτό του η βέλτιστη απόκριση. Δηλαδή θα πρέπει κανένας από τους δυο παίκτες να μην έχει μονομερώς κίνητρο να ξεφύγει από την κατάσταση ισορροπίας. Ισχύει ότι εάν θεωρήσουμε δεδομένο ότι το Local IDS θα επιλέξει τη στρατηγική suggestion for trusting, συμφέρει το Global IDS να επιλέξει τη στρατηγική admit. Αυτό συμπεραίνεται από τη σύγκριση των δυο στηλών (21 > 18).

Αντιστρόφως, εάν θεωρήσουμε δεδομένο ότι το Global IDS θα επιλέξει τη στρατηγική admit, συμφέρει το Local IDS να επιλέξει τη στρατηγική suggestion for trusting. Είναι προφανές ότι κανένας από τους παίκτες δεν έχει κίνητρο να ξεφύγει από την ισορροπία (normal action, suggestion for trusting, admit). Συνεπώς με βάση το ρητό “all is Nash”, και αυτή η ισορροπία αποτελεί ισορροπία κατά Nash.

Αναλύοντας τους δυο πίνακες αποδόσεων που προκύπτουν από τα υποπαίγνια του παιγνίου, καταλήξαμε σε δυο ισορροπίες σε καθαρές στρατηγικές (pure strategies):

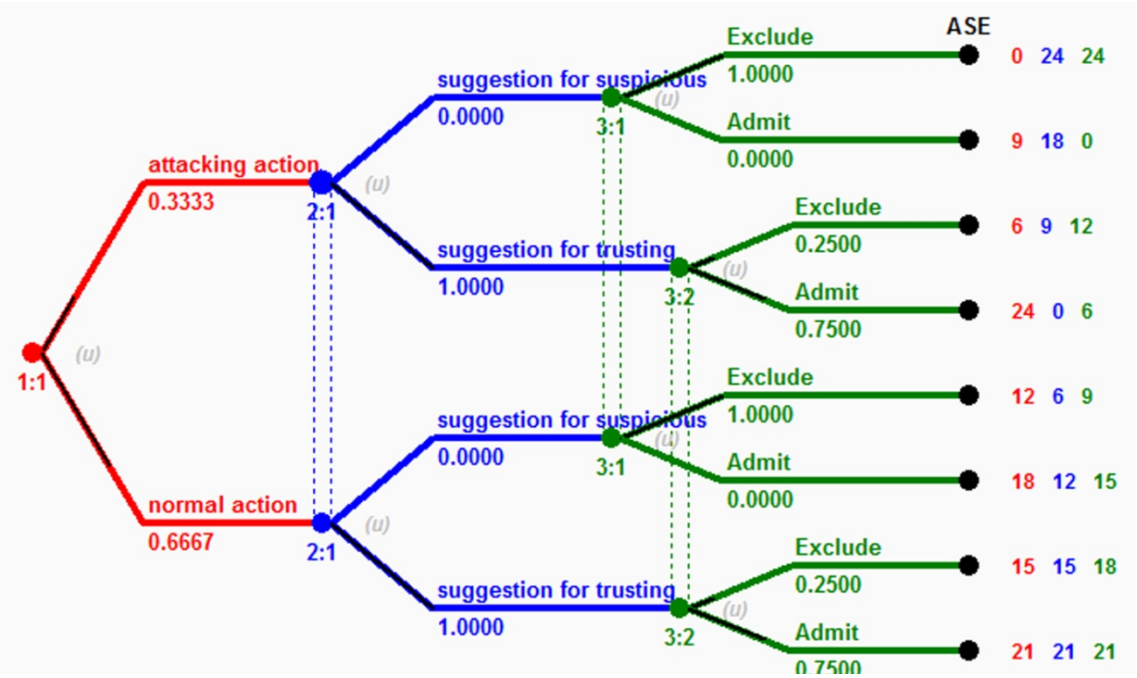
(attacking action, suggestion for suspicious, exclude) (ASE) = (0, 24, 24)

(normal action, suggestion for trusting, admit) (NTA) = (21, 21, 21)

Ερμηνεύοντας τις δύο ισορροπίες μπορούμε να πούμε ότι και οι δύο καταστάσεις είναι απολύτως επιθυμητές για το δίκτυο μας. Στη μεν πρώτη (ASE), ο potential attacker κάνει μια επίθεση, η οποία όμως ανιχνεύεται και αντιμετωπίζεται επιτυχώς και από τα δύο IDS συστήματα, τα οποία έχουμε εγκατεστημένα στο δίκτυο. Στη δεύτερη περίπτωση, ο potential attacker λειτουργεί σαν ένας κανονικός κόμβος του δικτύου, κάνοντας κανονικές ενέργειες. Το Local IDS εμπιστεύεται τις ενέργειες του και το Global IDS του επιτρέπει να συνεχίσει την ομαλή λειτουργία του.

6.7 Επίλυση με το πρόγραμμα Gambit

Στην προηγούμενη ενότητα βρήκαμε δύο ισορροπίες Nash στις καθαρές στρατηγικές. Το συγκεκριμένο παιχνίδι όμως παρουσιάζει λύση και στις μικτές στρατηγικές (mixed strategies) και θα την περιγράψουμε σε αυτή την ενότητα. Επιλύοντας το παιχνίδι με την εκτεταμένη του μορφή χρησιμοποιώντας το πρόγραμμα επίλυσης παιγνίων Gambit, αποκομίζουμε ένα Nash equilibrium. Αυτή η μοναδική ισορροπία κατά Nash στις μικτές στρατηγικές αντιστοιχεί ακόμα και σε μια μοναδική λύση στις στρατηγικές συμπεριφοράς (behavioral strategies). Στην εικόνα 13 απεικονίζεται το παιχνίδι σε εκτεταμένη μορφή με τις πιθανότητες (probability values) συσχετιζόμενες με τις αποδόσεις των παικτών ανάλογα με την στρατηγική που έχουν ακολουθήσει.



Εικόνα 13: Επίλυση στις μικτές στρατηγικές

Παρατηρούμε πως υπάρχουν δύο σύνολα πληροφόρησης για το Global IDS και ένα για το Local IDS. Ο potential attacker παίζει πρώτος και με πιθανότητες 1/3 να κάνει επίθεση και 2/3 να κάνει normal action. Στη συνέχεια παίζει το Local IDS το οποίο μπορεί να είναι είτε στο πάνω κλαδί είτε κάτω. Βλέπουμε ότι με πιθανότητα 1 και στις δύο περιπτώσεις προτιμάει να παίξει suggestion for trusting.

Τέλος έχουμε το Global IDS το οποίο στο πρώτο σύνολο πληροφόρησης δίνει πιθανότητες 1 να κάνει Exclude μια ενέργεια που πρώτα έχει γίνει suggestion for suspicious ενώ για το Admit η πιθανότητα είναι 0. Αντίστοιχα στο δεύτερο σύνολο πληροφόρησης βλέπουμε το Global IDS να επιλέγει με πιθανότητα 3/4 να κάνει Admit μια ενέργεια του potential attacker που πρώτα έχει γίνει suggestion for trusting από το Local IDS. Στη συγκεκριμένη περίπτωση βλέπουμε πως η πιθανότητα για να παίξει Exclude το Global IDS είναι 1/4.

6.8 Περίληψη

Σε αυτό το κεφάλαιο κατασκευάσαμε ένα παιχνίδι ασφάλειας για ασύρματα δίκτυα αισθητήρων. Το παιχνίδι αυτό το ονομάσαμε GoWiSeN (Game of Wireless Sensor Networks) και αποτελείται από τρεις παίκτες. Κατά την μοντελοποίηση αυτού του σεναρίου ασφάλειας χρησιμοποιήθηκαν τεχνικές ανίχνευσης εισβολών αλλά και η θεωρία των παιγνίων. Αναλυτικά τα βήματα που ακολουθήσαμε για την δημιουργία του παιγνίου είναι τα εξής. Στην ενότητα 6.2 έγινε μια πλήρης περιγραφή του παιγνίου αλλά και του ασύρματου δικτύου αισθητήρων. Στη συνέχεια δημιουργήθηκαν οι συναρτήσεις χρησιμότητας για κάθε παίκτη του και με βάση αυτές ορίστηκαν οι αποδόσεις των παικτών. Τέλος επιλύσαμε το παίγνιο χρησιμοποιώντας τη μέθοδο της κυριαρχίας για να βρούμε τις καθαρές στρατηγικές, αλλά και το πρόγραμμα Gambit με το οποίο βρήκαμε ένα Nash equilibrium στις μικτές στρατηγικές. Στο επόμενο κεφάλαιο θα περιγράψουμε ένα πραγματικό σενάριο χρήσης των ασύρματων δικτύων αισθητήρων στο οποίο θα ενσωματωθεί το παίγνιο GoWiSeN.

7 Μελέτη περίπτωσης

7.1 Εισαγωγή

Σε αυτό το κεφάλαιο, θα περιγράψουμε ένα πραγματικό σενάριο χρήσης των ασύρματων δικτύων αισθητήρων στο οποίο θα ενσωματώσουμε για την ασφάλεια του δικτύου, το παιχνίδι που κατασκευάστηκε και επιλύθηκε στο κεφάλαιο 6. Το case study έχει να κάνει με την πυρόσβεση και το πώς τα ασφαλή ασύρματα δίκτυα αισθητήρων μπορούν να μας βοηθήσουν για το σκοπό αυτό. Η πυρόσβεση είναι ένα από τα πιο επικίνδυνα επαγγέλματα στο οποίο απασχολούνται άνθρωποι. Οι κίνδυνοι που συνδέονται με αυτό το επάγγελμα είναι αποτέλεσμα διαφόρων παραγόντων, όπως η έλλειψη πληροφοριών σχετικά με τη θέση και το μέγεθος της πυρκαγιάς. Η χρήση των ασύρματων δικτύων αισθητήρων μπορεί να είναι ένας τρόπος ώστε να μειωθούν οι κίνδυνοι που αντιμετωπίζουν οι πυροσβέστες και επιπλέον μπορούν να βοηθήσουν στη γρήγορη κατάσβεση μιας πυρκαγιάς. Μπορούν επίσης να είναι σε θέση να παρέχουν στους ειδικούς που ερευνούν τα αίτια μιας πυρκαγιάς την πρόσθετη γνώση, που θα μπορούσε να βοηθήσει στον καθορισμό για το εάν μια πυρκαγιά δημιουργήθηκε κακόβουλα.

7.2 Τα ασύρματα δίκτυα αισθητήρων για την αντιμετώπιση των πυρκαγιών

Τα ασύρματα δίκτυα αισθητήρων μπορούν να ταξινομηθούν σε δύο τύπους: συλλογής δεδομένων ή σα δίκτυα ανίχνευσης γεγονότος. Σε πολλές εφαρμογές όπου η συλλογή δεδομένων είναι ο στόχος, οι αισθητήρες μπορούν να είναι αναγκαίοι για να συλλέξουν τα στοιχεία μικρών χρονικών περιόδων σε καθορισμένες στιγμές της ημέρας. Σε αυτήν την περίπτωση, τις περισσότερες φορές ο κόμβος αισθητήρων θα είναι αδρανής συντηρώντας έτσι ενέργεια. Εντούτοις, όπου ένα ασύρματο δίκτυο αισθητήρων πρόκειται να χρησιμοποιηθεί για την ανίχνευση γεγονότος, όπως η ανίχνευση μιας

πυρκαγιάς, θα πρέπει οι κόμβοι αισθητήρων να παραμείνουν άγρυπνοι καταναλώνοντας έτσι την πολύτιμη ενέργεια τους [Dutta, 2004].

Στο σχεδιασμό και την εφαρμογή ενός προ αναπτυγμένου ασύρματου δικτύου αισθητήρων για να βοηθήσει τους πυροσβέστες, υπάρχει ένας αριθμός απαιτήσεων που πρέπει να ικανοποιηθούν. Καταρχάς οποιοδήποτε σύστημα εφαρμόζεται, πρέπει να είναι αξιόπιστο και οικονομικός αποδοτικό. Ας υποθέσουμε ότι τα ζητήματα της αξιοπιστίας και των δαπανών μπορούν να ξεπεραστούν. Έχουμε της ακόλουθες προκλήσεις που πρέπει να εξεταστούν:

- Η πιθανότητα των λανθασμένων συναγερμών πρέπει να ελαχιστοποιηθεί. Είναι προφανές ότι τα περιστατικά των λανθασμένων συναγερμών πρέπει να ελαχιστοποιηθούν, δεδομένου ότι σπαταλούν το χρόνο και τους πόρους της πυροσβεστικής υπηρεσίας και μπορεί ενδεχομένως να οδηγήσουν τους πόρους της πυροσβεστικής να μην είναι διαθέσιμοι, για να παρευρεθούν αμέσως σε πραγματικά περιστατικά που χρήζουν αντιμετώπισης.
- Το ασύρματο δίκτυο αισθητήρων πρέπει να είναι ασφαλές προκειμένου να αποτραπούν κακόβουλες ενέργειες, που μπορούν να προκαλέσουν λανθασμένους συναγερμούς και αποστολή ψεύτικων στοιχείων. Για το σκοπό αυτό θα ενσωματώσουμε στο δίκτυο τα στοιχεία από το παιχνίδι που αναπτύξαμε στο κεφάλαιο 6.
- Λόγω της ταχύτητας με την οποία η πυρκαγιά μπορεί να εξαπλωθεί, είναι πολύ σημαντικό ο κόμβος αισθητήρων που ανιχνεύει το γεγονός να αρχίζει να στέλνει τα στοιχεία μόλις ανιχνεύσει την ύπαρξη πυρκαγιάς. Αν αποτύχει να το κάνει αυτό, μπορεί να μην ενεργοποιηθούν οι συναγερμοί και χρήσιμα δεδομένα που είναι να σταλούν στην πυροσβεστική υπηρεσία να χαθούν. Επιπλέον, ο κόμβος αισθητήρων που ανιχνεύει το γεγονός, πρέπει επίσης να ξυπνήσει άλλους κόμβους αισθητήρων κοντά στο γεγονός.
- Η πυροσβεστική υπηρεσία πρέπει να είναι σε θέση να συνδεθεί με το ασύρματο δίκτυο αισθητήρων στο κτίριο το οποίο θέλουμε να παρακολουθούμε. Ένα

σύστημα για ανίχνευση πυρκαγιάς είναι σημαντικό μόνο εάν η πυροσβεστική υπηρεσία μπορεί να συνδεθεί με το δίκτυο για να ανακτήσει πληροφορίες.

- Το δίκτυο πρέπει να μπορεί να τροποποιηθεί από μόνο του για να εξασφαλιστεί ότι τα στοιχεία μπορούν να μεταφερθούν ακόμα και όταν αποτυγχάνουν μεμονωμένοι αισθητήρες. Η ίδια η φύση μιας πυρκαγιάς θα οδηγήσει αναμφισβήτητα στην καταστροφή ή την αποτυχία κάποιων αισθητήρων. Συνεπώς, προκειμένου να εξασφαλιστεί ότι τα δεδομένα που είναι σχετικά με την κατάσταση της πυρκαγιάς συνεχίζουν να στέλνονται. το δίκτυο πρέπει να μπορεί να αλλάξει την δρομολόγηση των πακέτων από μόνο του.
- Πρέπει να υπάρχει γρήγορη μεταφορά των στοιχείων. Για να είναι σημαντικές οι πληροφορίες για τους πυροσβέστες, τα στοιχεία από τους διάφορους αισθητήρες που περιλαμβάνουν το δίκτυο πρέπει γρήγορα και σωστά να παραληφθούν.
- Οι θέσεις των αισθητήρων πρέπει να είναι γνωστές. Προκειμένου να παρασχεθεί μια ακριβής εικόνα της θέσης και διάδοσης της πυρκαγιάς, οι θέσεις των αισθητήρων μέσα στο κτίριο πρέπει να είναι γνωστές στην πυροσβεστική υπηρεσία.
- Πρέπει να υπάρξει μια οπτική επίδειξη (visualization) στην πυροσβεστική που να παρουσιάζει τη θέση και διάδοση της πυρκαγιάς και των θερμοκρασιών μέσα στο κτίριο.
- Οι αισθητήρες πρέπει να προστατευθούν όσο το δυνατόν περισσότερο από τη θερμότητα που παράγεται από την πυρκαγιά, προκειμένου να κρατηθούν λειτουργικοί καθ' όσο είναι δυνατό, χωρίς υποβάθμιση των δυνατοτήτων των αισθητήρων να ανιχνεύουν αλλαγές στη θερμοκρασία ή οποιεσδήποτε άλλες παραμέτρους που αισθάνονται.

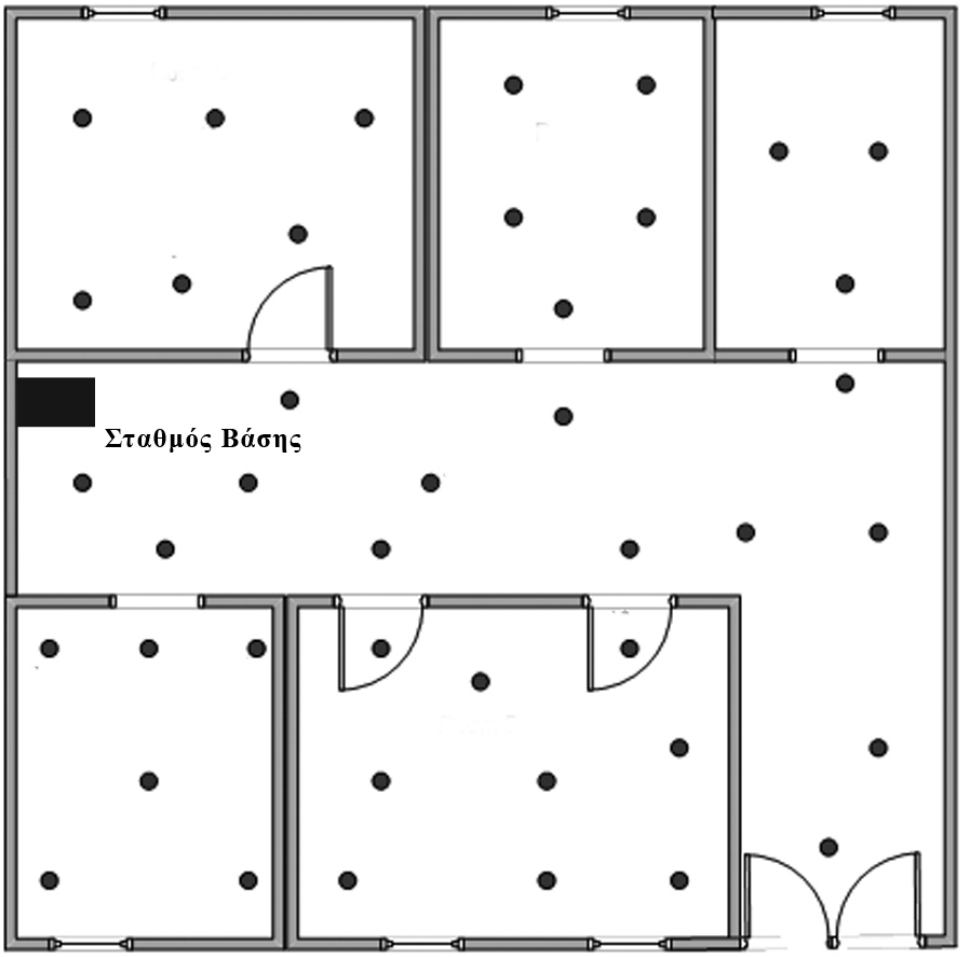
Κάποιοι από τους κινδύνους που αντιμετωπίζουν οι πυροσβέστες μπορούν αποφευχθούν με την εγκατάσταση ασύρματων δικτύων αισθητήρων. Ο παρακάτω πίνακας 18 παρουσιάζει συνοπτικά τα προβλήματα που υπάρχουν για να εξεταστεί και η πιθανή λύση των ασύρματων δικτύων αισθητήρων.

Πρόβλημα	WSN λύση
Έκθεση των πυροσβεστών στον κίνδυνο	Εγκατεστημένοι αισθητήρες ανίχνευσης θερμοκρασίας, καπνού, οξυγόνου.
Ανάφλεξη πυρκαγιάς, ξαφνική ανάφλεξη του περιεχομένου ενός δωματίου	Εγκατεστημένοι αισθητήρες ανίχνευσης θερμοκρασίας
Εκρήξεις που εμφανίζονται όταν μια πυρκαγιά ξαφνικά λαμβάνει οξυγόνο	Εγκατεστημένοι αισθητήρες ανίχνευσης οξυγόνου.
Κρυμμένες πυρκαγιές στους τοίχους, τις σοφίτες, και άλλες απαρατήρητες περιοχές	Εγκατεστημένοι αισθητήρες ανίχνευσης θερμοκρασίας και καπνού
Δομικοί κίνδυνοι, συμπεριλαμβανομένης της κατάρρευσης σημείων και των τοξικών αερίων από το κάψιμο των επικίνδυνων υλικών.	Εγκατεστημένοι αισθητήρες μέτρησης κίνησης και ανίχνευσης αεριών.

Πίνακας 18: Πιθανή χρησιμότητα των ασύρματων αισθητήρων [Kurata et al., 2004]

7.3 Εγκατάσταση ασύρματου δικτύου αισθητήρων μέσα σε κτίριο

Έστω ότι έχουμε δημιουργήσει ένα ασύρματο δίκτυο αισθητήρων μέσα στα γραφεία μιας μεγάλης εταιρείας, όπως παρουσιάζεται στην εικόνα 14. Το δίκτυο μας θα αποτελείται από διαφορετικούς τύπους ασύρματων αισθητήρων. Καταρχάς θα υπάρχουν αισθητήρες θερμοκρασίας, δεδομένου ότι είναι αυτοί που στις περισσότερες περιπτώσεις ανιχνεύουν την πυρκαγιά. Άλλοι αισθητήρες μπορούν να είναι αισθητήρες ανίχνευσης καπνού και κίνησης. Στο σχήμα μπορούμε να δούμε πως οι αισθητήρες καλύπτουν όλους τους χώρους του κτιρίου, ενώ σε ένα σημείο υπάρχει και ο σταθμός βάσης του δικτύου.



Εικόνα 14: Διάταξη δικτύου αισθητήρων μέσα στο κτίριο

Το ασύρματο δίκτυο αισθητήρων θα συνδέεται μέσω του διαδικτύου με την πυροσβεστική υπηρεσία. Κατά συνέπεια θα μπορεί να παρέχει μια στιγμιαία κλήση έκτακτης ανάγκης, εάν ανιχνεύσει μια πυρκαγιά. Με τη σύνδεση μέσω του διαδικτύου, μόλις ανιχνεύεται μια πυρκαγιά, οι ελεγκτές από το κέντρο της πυροσβεστικής θα είναι σε θέση να παρέχουν στους πυροσβέστες μια αρχική θέση της πυρκαγιάς μέσα στο κτίριο και επίσης αναπροσαρμογή ως προς τη διάδοση της πυρκαγιάς, κατά τη διάρκεια της πορείας τους προς το κτίριο που έχει εκδηλωθεί η πυρκαγιά. Κατά την άφιξη τους οι πυροσβέστες θα μπορούν να συνδεθούν ασύρματα στο δίκτυο αισθητήρων και θα ενημερώνονται με πληροφορίες για τη θέση και τη διάδοση της πυρκαγιάς. Είναι χρήσιμο ο ιδιοκτήτης κάθε κτιρίου με ένα ασύρματο δίκτυο αισθητήρων να παρέχει στην πυροσβεστική υπηρεσία τα λεπτομερή σχέδια ορόφων των εγκαταστάσεων. Αυτά θα επιδεικνύονται αυτόματα μαζί με τις θέσεις των αισθητήρων και της παρούσας κατάστασής τους.

Μόλις φτάσει η πυροσβεστική υπηρεσία στο συμβάν, θα μπορεί χρησιμοποιώντας έναν φορητό υπολογιστή να αναλάβει τη δουλειά που κάνει ο σταθμός βάσης του ασύρματου δικτύου αισθητήρων που υπάρχει μέσα στο κτίριο. Κατ' αυτό τον τρόπο, εάν ο σταθμός βάσης του δικτύου που βρίσκεται εντός κτιρίου έχει καταστραφεί από την πυρκαγιά, το ασύρματο δίκτυο αισθητήρων θα παραμείνει λειτουργικό, εφ' όσον οι αισθητήρες είναι λειτουργικοί μέσα στο κτίριο.

7.4 Σενάρια λειτουργίας δικτύου

Κακόβουλα άτομα μπορούν να προσπαθήσουν να αποκτήσουν πρόσβαση στο ασύρματο δίκτυο αισθητήρων, προκειμένου να προκληθεί ένας λανθασμένος συναγερμός, ή χειρότερα να τροποποιηθούν τα στοιχεία που συλλέγονται από τους αισθητήρες, με συνέπεια να διαβιβάζονται στο σταθμός βάσης λανθασμένα δεδομένα.

Για την ασφάλεια λοιπόν του δικτύου θα εφαρμόσουμε το μοντέλο που δημιουργήσαμε στο κεφάλαιο 6. Θα εγκαταστήσουμε σε κάθε κόμβο αισθητήρων ένα τοπικό σύστημα ανίχνευσης εισβολών, το οποίο θα ονομάσουμε Local IDS. Το Local IDS θα είναι μια ελαφριά έκδοση IDS, με ελάχιστες απαιτήσεις σε πόρους ενέργειας. Επίσης, στον κεντρικό σταθμό βάσης του δικτύου, θα υπάρχει ένα πλήρες IDS σύστημα το οποίο θα

ονομάσουμε Global IDS. Το Global IDS εκτός από ανίχνευση εισβολών θα έχει τη δυνατότητα να κρατάει και ιστορικό για όλες τις ενέργειες που έχουν γίνει από τους κόμβους, στη διάρκεια ζωής του δικτύου. Έτσι θα μπορεί να αποθηκεύει μια λίστα ταξινόμησης για κάθε κόμβο η οποία θα έχει μια κλίμακα από 0 έως 5 και θα δείχνει πόσες φορές έχει κάνει μη επιτρεπτές ενέργειες ο συγκεκριμένος κόμβος. Συγκεκριμένα, η τιμή 0 θα αντιστοιχεί σε ένα κόμβο που λειτουργεί φυσιολογικά και δεν έχει πιαστεί ποτέ να κάνει κακόβουλες ενέργειες. Αντιθέτως, η τιμή 5 υποδηλώνει ότι αυτός ο κόμβος έχει καταγραφεί 5 φορές για επιθετικές κινήσεις προς το δίκτυο. Ο κάθε κόμβος με εγκατεστημένο πλέον το Local IDS κατά την επικοινωνία του με γειτονικούς κόμβους, θα μπορεί να κάνει μια πρώτης μορφής ανίχνευση και αξιολόγηση των κινήσεων των γειτονικών κόμβων. Στη συνέχεια, θα στέλνει suggestion for suspicious ή suggestion for trusting στο Global IDS του δικτύου, το οποίο τελικά θα αποφασίζει αν η ενέργεια του κόμβου θα πρέπει να γίνει admit ή exclude.

Μια ανίχνευση γεγονότος πυρκαγιάς θα έχουμε όταν οι κόμβοι του δικτύου ανιχνεύουν θερμοκρασίες μεγαλύτερες από 40 ^{o}C για διάστημα μεγαλύτερο από 10 δευτερόλεπτα. Σε περίπτωση πυρκαγιάς το Local IDS θα κάνει suggestion for trusting στην πληροφορία για πυρκαγιά μόνο αν την ανιχνεύουν και άλλοι γειτονικοί κόμβοι. Σε περιπτώσεις όπου υπάρχει ανεβασμένη θερμοκρασία από φυσικά αίτια, όπως την καλοκαιρινή περίοδο οπού συμβαίνουν φαινόμενα καύσωνα, θα πρέπει να διαχειριστής του δικτύου να έχει ρυθμίσει διαφορετικά τα όρια θερμοκρασίας. Το Global IDS τώρα για να αποφασίσει αν θα κάνει Admit ή Exclude μια ενέργεια θα κοιτάζει τρεις συγκεκριμένες παραμέτρους. Αρχικά θα βλέπει τι του προτείνει το Local IDS, suggestion for trusting η suggestion for suspicious. Στη συνέχεια θα αξιοποιεί το ιστορικό και την λίστα ταξινόμησης του δικτύου τα οποία θα τον ενημερώνουν για τις έως τώρα ενέργειες του κόμβου που δημιούργησε το πρόβλημα. Τέλος θα μπορεί να χρησιμοποιήσει τις τεχνικές ανίχνευσης εισβολών που μελετήσαμε στο κεφάλαιο 4 misuse, anomaly και specification-based detection ώστε να μπορεί να ανιχνεύσεις τις πιθανές επιθέσεις.

Στη συνέχεια θα παρουσιάσουμε δύο σενάρια λειτουργίας του δικτύου. Στην πρώτη περίπτωση θα δείξουμε σε βήματα την αντιμετώπιση μιας πραγματικής εκδήλωσης

πυρκαγιάς. Στο δεύτερο σενάριο έχουμε μια ενέργεια επίθεσης από έναν παραβιασμένο κόμβο.

Σενάριο 1: Λειτουργία του δικτύου όταν έχουμε μια πραγματική εκδήλωση πυρκαγιάς

1. Ο κόμβος λειτουργεί φυσιολογικά στο δίκτυο μας έχοντας αισθητήρα ανίχνευσης θερμοκρασίας.
2. Δημιουργείται πυρκαγιά σε κάποιο χώρο του κτιρίου.
3. Ο κόμβος ανιχνεύει το γεγονός της ύπαρξης πυρκαγιάς στο σημείο που βρίσκεται.
4. Ο κόμβος ενημερώνει τους γειτονικούς κόμβους ότι ανίχνευσε θερμοκρασίες μεγαλύτερες των $40^{o}C$ για περισσότερο από 10 δευτερόλεπτα οπότε ενεργοποιείται ο συναγερμός.
5. Οι γειτονικοί κόμβοι ανιχνεύουν και αυτοί αυξημένη θερμοκρασία στο χώρο και αξιολογούν την πληροφορία που τους έχει έρθει θετικά ως αξιόπιστη, οπότε προτείνουν suggestion for trusting στο σταθμό βάσης.
6. Οι ανιχνεύσεις που κάνουν οι κόμβοι στέλνονται στο σταθμό βάσης του δικτύου.
7. Ο σταθμός βάσης (Global IDS) ενημερώνεται και εκτιμά τις πληροφορίες βλέποντας το ranking που έχει ο κόμβος που αρχικά εντόπισε το συμβάν, αλλά και τις προτάσεις που έστειλαν οι γειτονικοί κόμβοι.
8. Το Global IDS μετά από μια γρήγορη αποτίμηση της κατάστασης με βάση τα δεδομένα που έχει λάβει επιλέγει admit.
9. Ο σταθμός βάσης στέλνει όλα τα δεδομένα που έχει συλλέξει στο κέντρο της πυροσβεστικής υπηρεσίας, η οποία εκτιμά την κατάσταση και ανάλογα την αντιμετωπίζει.
10. Ενημέρωση του Global IDS από την πυροσβεστική για την εγκυρότητα τελικά της πληροφορίας.

Σενάριο 2: Λειτουργία του δικτύου όταν έχουμε μια ενέργεια επίθεσης:

1. Ένας επιτιθέμενος παραβιάζει έναν κόμβο του δικτύου με σκοπό να πραγματοποιεί επιθέσεις ανά τακτά χρονικά διαστήματα. Σκοπός του επιτιθέμενου, κάθε φορά που θα πραγματοποιεί μια επίθεση, είναι να βγάζει εκτός λειτουργίας ένα σημαντικό κομμάτι του δικτύου.

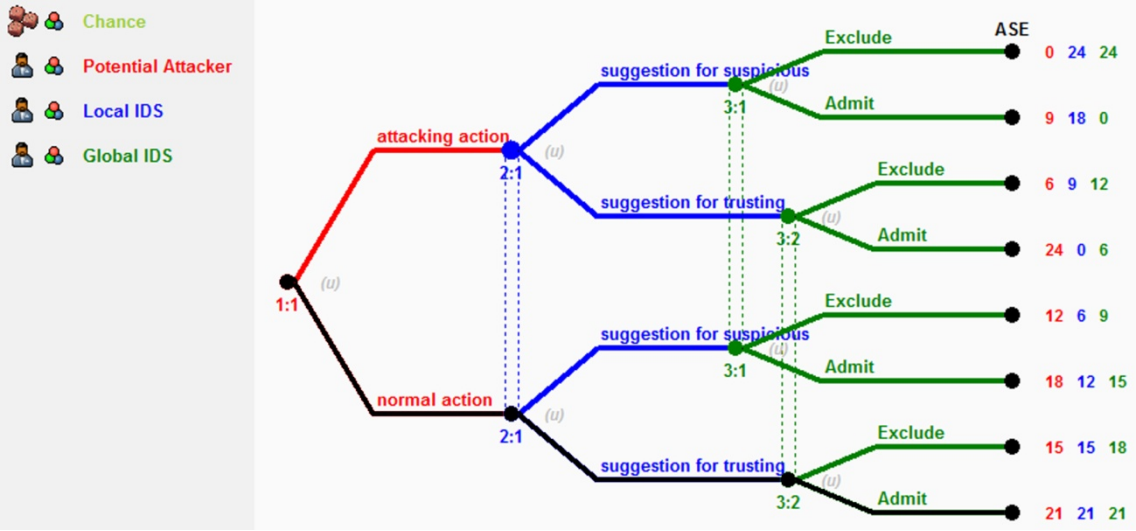
2. Ο κόμβος που έχει παραβιαστεί ξεκινά να κάνει μια ενέργεια επίθεσης. Η επίθεση θα γίνει στο επίπεδο μεταφοράς του δικτύου και θα είναι βασισμένη στην τεχνική flooding. Ο στόχος της επίθεσης flooding θα είναι να εξαντληθούν οι πόροι των γειτονικών κόμβων και να βγει μέρος του δικτύου εκτός λειτουργίας.
3. Ο γειτονικός κόμβος και το Local IDS του που δέχονται την επίθεση αξιολογούν την κίνηση αυτή. Το Local IDS ανιχνεύει περίεργη συμπεριφορά, καθώς ξαφνικά γίνονται από τον επιτιθέμενο πάρα πολλές αιτήσεις για συνδέσεις. Το Local IDS θα κάνει suggestion for suspicious, θεωρώντας την ενέργεια κακόβουλη και στέλνει τα δεδομένα στο σταθμό βάσης.
4. Ο σταθμός βάσης και το εγκατεστημένο Global IDS εξετάζουν την συγκεκριμένη ενέργεια και τη θεωρούν κακόβουλη, οπότε επιλέγουν Exclude, αποκλείοντας την από το να ολοκληρωθεί. Για την απόφαση του το Global IDS αξιοποιεί και την τεχνική anomaly detection η οποία αναφέρει τις σημαντικές αποκλίσεις από την κανονική δραστηριότητα ενός κόμβου ως επιθέσεις. Επίσης αξιοποιούν το ιστορικό και την λίστα ταξινόμησης του δικτύου προσθέτοντας συν 1 στον κόμβο που δημιούργησε το πρόβλημα. Αν ο κόμβος έχει φτάσει την τιμή 5 στη λίστα ταξινόμησης, τότε θα γίνει blacklist από όλους τους πίνακες δρομολόγησης του δικτύου.

7.5 Χρησιμοποιώντας το GoWiSeN στην ασφάλεια του δικτύου

Στην ενότητα αυτή θα δείξουμε το πώς μπορεί να χρησιμοποιηθεί το παιχνίδι που κατασκευάσαμε στο κεφάλαιο 6 έτσι ώστε να προστατέψει το δίκτυο που έχει δημιουργηθεί για την αντιμετώπιση των πυρκαγιών.

Μελετώντας ξανά το σενάριο 1 της προηγούμενης ενότητας (7.4) μπορούμε να το επιλύσουμε χρησιμοποιώντας το παιχνίδι GoWiSeN. Στην εικόνα 15 βλέπουμε σχηματοποιημένο το σενάριο 1 σαν εκτεταμένη μορφή παιγνίου. Στην αρχή του δέντρου υπάρχει ένας κόμβος του δικτύου τον οποίο εμείς έχουμε ονομάσει potential attacker θεωρώντας ότι μπορεί να λειτουργεί φυσιολογικά στη μεγαλύτερη διάρκεια της ζωής του αλλά είναι πιθανόν κάποια στιγμή να παραβιαστεί, από εξωτερική πηγή, και

να δημιουργήσει πρόβλημα στο δίκτυο. Με βάση το σενάριο ο κόμβος λειτουργεί φυσιολογικά έχοντας ενσωματωμένο έναν αισθητήρα ανίχνευσης θερμοκρασίας. Δημιουργείται μια πυρκαγιά σε κάποιο χώρο του κτιρίου όπου βρίσκεται εγκατεστημένος ο συγκεκριμένος αισθητήρας. Ο κόμβος ανιχνεύει την πυρκαγιά και κάνει μια προκαθορισμένη ενέργεια που είναι η αποστολή της πληροφορίας σε γειτονικούς κόμβους. Στο παιχνίδι στην εικόνα 15 η συγκεκριμένη ενέργεια είναι η κίνηση normal action μέσα στο δέντρο.



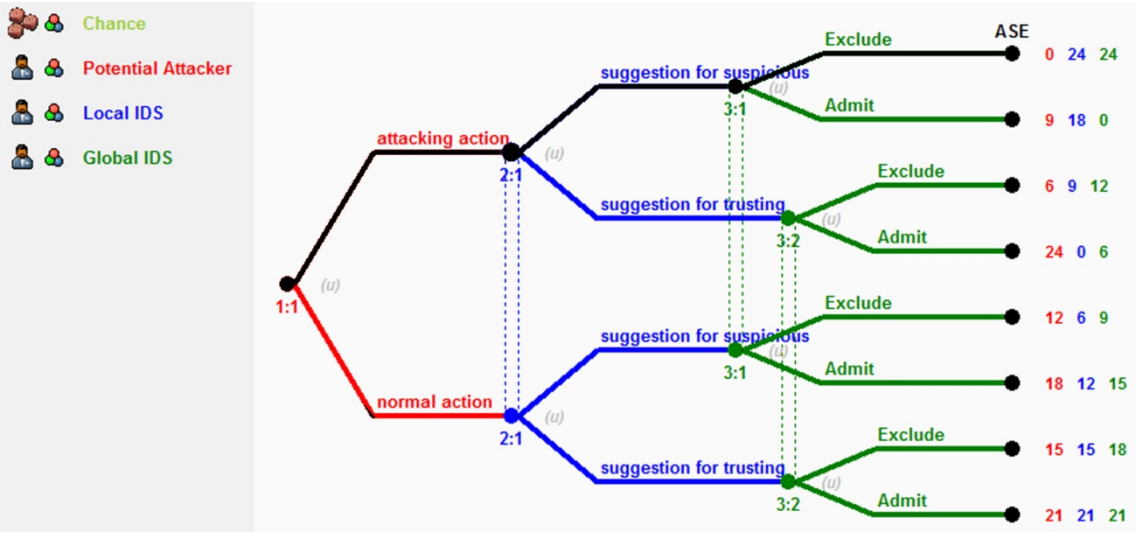
Εικόνα 15: Εκτεταμένη μορφή παιγνίου σεναρίου 1

Στη συνέχεια έχουμε την ανίχνευση του γεγονότος και από τους γειτονικούς κόμβους αλλά και την αξιολόγηση της πληροφορίας που στάλθηκε από τον κόμβο που έκανε πρώτος την ανίχνευση. Οι γειτονικοί κόμβοι αξιολογούν θετικά ως αξιόπιστη την πληροφορία οπότε προτείνουν suggestion for trusting στο σταθμό βάσης. Με βάση το παιχνίδι το Local IDS θα προτιμήσει στη συγκεκριμένη περίπτωση να παίξει suggestion for trusting αφού του δίνει μεγαλύτερη απόδοση ανεξάρτητα από το τι θα επιλέξει το Global IDS. Δηλαδή η στρατηγική suggestion for suspicious είναι κυριαρχούμενη από την στρατηγική suggestion for trusting.

Ο σταθμός βάσης εκτιμά τις πληροφορίες από τις ανιχνεύσεις και προσπαθεί να εκτιμήσει την κατάσταση. Βλέποντας το χαμηλό ranking του κόμβου με τιμή 0 που πρώτος εντόπισε το γεγονός αλλά και τις προτάσεις που στέλνουν γειτονικοί κόμβοι,

που κάνουν και αυτοί με τη σειρά τους ανίχνευση της πυρκαγιάς, επιλέγει admit. Με βάση το παιχνίδι το Global IDS θα προτιμήσει στη συγκεκριμένη περίπτωση να παίξει admit αφού του δίνει μεγαλύτερη απόδοση ανεξάρτητα από το τι θα επιλέξει το Local IDS. Δηλαδή η στρατηγική exclude είναι κυριαρχούμενη από την στρατηγική admit. Στο συγκεκριμένο άρα υποπαίγνιο, υπάρχει μία και μοναδική ισορροπία, στην οποία όλοι οι παίκτες λαμβάνουν απόδοση 21. Η ισορροπία αυτή είναι συμφέρουσα και για τον potential attacker, αφού στην περίπτωση αυτή λαμβάνει την μεγαλύτερη απόδοση. Η ισορροπία που προκύπτει είναι η ακόλουθη: (normal action, suggestion for trusting, admit) = (NTA) = (21, 21, 21) και στην εικόνα παρουσιάζεται με μια μαύρη γραμμή.

Μελετώντας τώρα ξανά το σενάριο 2 της προηγούμενης ενότητας (7.4) μπορούμε να το επιλύσουμε χρησιμοποιώντας και πάλι το παιχνίδι GoWiSeN. Στην εικόνα 16 βλέπουμε σχηματοποιημένο το σενάριο 2 σαν εκτεταμένη μορφή παιγνίου. Στην αρχή του δέντρου έχουμε όπως και πριν ένα κόμβο του δικτύου τον οποίο εμείς έχουμε ονομάσει potential attacker. Θεωρούμε ότι ο συγκεκριμένος κόμβος μπορεί να λειτουργεί φυσιολογικά στη μεγαλύτερη διάρκεια της ζωής του αλλά είναι πιθανόν κάποια στιγμή να παραβιαστεί, από εξωτερική πηγή, και να δημιουργήσει πρόβλημα στο δίκτυο. Με βάση το σενάριο ένας επιτιθέμενος παραβιάζει έναν κόμβο του δικτύου (τον potential attacker συγκεκριμένα) με σκοπό να πραγματοποιεί επιθέσεις ανά τακτά χρονικά διαστήματα. Σκοπός του επιτιθέμενου, κάθε φορά που θα πραγματοποιεί μια επίθεση, είναι να βγάζει εκτός λειτουργίας ένα σημαντικό κομμάτι του δικτύου. Ο κόμβος που έχει παραβιαστεί ξεκινά να κάνει μια ενέργεια επίθεσης. Η επίθεση θα γίνει στο επίπεδο μεταφοράς του δικτύου και θα είναι βασισμένη στην τεχνική flooding. Ο στόχος της επίθεσης flooding θα είναι να εξαντληθούν οι πόροι των γειτονικών κόμβων και να βγει μέρος του δικτύου εκτός λειτουργίας. Στο παιχνίδι στην εικόνα 16 η συγκεκριμένη ενέργεια είναι η κίνηση attacking action μέσα στο δέντρο.



Εικόνα 16: Εκτεταμένη μορφή παιγνίου σεναρίου 2

Στη συνέχεια ο γειτονικός κόμβος και το Local IDS του που δέχονται την επίθεση αξιολογούν την κίνηση αυτή. Το Local IDS ανιχνεύει περίεργη συμπεριφορά, καθώς ξαφνικά γίνονται από τον επιτιθέμενο πάρα πολλές αιτήσεις για συνδέσεις. Το Local IDS θα κάνει suggestion for suspicious, θεωρώντας την ενέργεια κακόβουλη και στέλνει τα δεδομένα στο σταθμό βάσης. Με βάση το παιχνίδι το Local IDS θα προτιμήσει στη συγκεκριμένη περίπτωση να παίξει suggestion for suspicious αφού του δίνει μεγαλύτερη απόδοση ανεξάρτητα από το τι θα επιλέξει το Global IDS. Δηλαδή η στρατηγική suggestion for trusting είναι κυριαρχούμενη από την στρατηγική suggestion for suspicious.

Ο σταθμός βάσης και το εγκατεστημένο Global IDS εξετάζουν την συγκεκριμένη ενέργεια και τη θεωρούν κακόβουλη, οπότε επιλέγουν Exclude, αποκλείοντας την από το να ολοκληρωθεί. Για την απόφαση του το Global IDS αξιοποιεί και την τεχνική anomaly detection η οποία αναφέρει τις σημαντικές αποκλίσεις από την κανονική δραστηριότητα ενός κόμβου ως επιθέσεις. Επίσης αξιοποιούν το ιστορικό και την λίστα ταξινόμησης του δικτύου προσθέτοντας συν 1 στον κόμβο που δημιούργησε το πρόβλημα. Αν ο κόμβος έχει φτάσει την τιμή 5 στη λίστα ταξινόμησης, τότε θα γίνει blacklist από όλους τους πίνακες δρομολόγησης του δικτύου. Με βάση το παιχνίδι το Global IDS θα προτιμήσει στη συγκεκριμένη περίπτωση να παίξει Exclude αφού του δίνει μεγαλύτερη απόδοση ανεξάρτητα από το τι θα επιλέξει το Local IDS. Δηλαδή η στρατηγική admit είναι κυριαρχούμενη από την στρατηγική exclude. Στο συγκεκριμένο

άρα υποπαίγνιο, υπάρχει μία και μοναδική ισορροπία, η οποία προφανώς είναι η ακόλουθη: (attacking action, suggestion for suspicious, exclude) = (ASE) = (0, 24, 24).

7.6 Περίληψη

Σε αυτό το κεφάλαιο παρουσιάσαμε ένα πραγματικό σενάριο χρήσης των ασύρματων δικτύων αισθητήρων. Περιγράψαμε αναλυτικά το πώς μπορούν να χρησιμοποιηθούν τα ασύρματα δίκτυα αισθητήρων για την αντιμετώπιση των πυρκαγιών. Είδαμε τους δύο τύπους που μπορούν να ταξινομηθούν τα WSN, αλλά και τις απαιτήσεις που πρέπει να ικανοποιηθούν στο σχεδιασμό και την εφαρμογή ενός τέτοιου δικτύου. Αναφέρθηκαν οι κίνδυνοι που αντιμετωπίζουν οι πυροσβέστες σε τέτοιες καταστάσεις και πως μπορούν να αποφευχθούν με την εγκατάσταση ασφαλών ασύρματων δικτύων αισθητήρων. Στη συνέχεια περιγράψαμε δύο σενάρια λειτουργίας ενός WSN που κάνει ανίχνευση πυρκαγιών και έχει εγκατασταθεί στα γραφεία μιας μεγάλης εταιρείας. Τέλος ενσωματώσαμε στο δίκτυο το παιχνίδι GoWiSeN που κατασκευάστηκε και επιλύθηκε στο κεφάλαιο 6. Στο επόμενο και τελευταίο κεφάλαιο, εκτίθενται τα συμπεράσματα της έρευνας αλλά και προτείνονται θέματα που χρήζουν περαιτέρω μελέτης.

8 Συμπεράσματα

Η ασφάλεια στα ασύρματα δίκτυα αισθητήρων είναι ένας τομέας έρευνας που αυξάνεται γρήγορα και έχει αποτελέσματα εφαρμόσιμα σε πραγματικά σενάρια της ζωής. Εντούτοις, υπάρχει ανάγκη για περισσότερες βελτιώσεις σε αυτήν την περιοχή. Ερευνητικά θέματα όπως η ανίχνευση εισβολών και η θεωρία παιγνίων στην ασφάλεια των δικτύων αισθητήρων είναι αρκετά καινούρια.

Σε αυτή την εργασία, αφού μελετήσαμε τα ιδιαίτερα χαρακτηριστικά των ασύρματων δικτύων αισθητήρων, τα συστήματα ανίχνευσης εισβολών και τη θεωρία των παιγνίων, δημιουργήσαμε ένα παιχνίδι ασφάλειας για τα WSN. Το παιχνίδι GoWiSen που δημιουργήσαμε έχει ως σκοπό την ασφάλεια των WSN χρησιμοποιώντας τεχνικές ανίχνευσης εισβολών αλλά και τη θεωρία των παιγνίων.

Ιδιαίτερα χαρακτηριστικά του παιγνίου μας όπως είδαμε είναι η ταυτόχρονη χρήση δύο συστημάτων ανίχνευσης εισβολών, Local και Global IDS με το πρώτο μάλιστα να βρίσκεται εγκατεστημένο σε κάθε κόμβο του δικτύου. Λαμβάνοντας υπόψη τους περιορισμούς σε πόρους που έχει ένας κόμβος αποφασίσαμε η Local IDS έκδοση να έχει περιορισμένες δυνατότητες, επομένως και ελάχιστες απαιτήσεις σε ενέργεια. Αντίθετα το Global IDS που είναι εγκατεστημένο στο σταθμό βάσης αποτελεί ένα πλήρες IDS σύστημα. Το Global IDS εκτός από ανίχνευση εισβολών κρατάει και μία λίστα με το ιστορικό του δικτύου. Έτσι γνωρίζει ποιοι κόμβοι είχαν δράσει κακόβουλα στο παρελθόν. Εάν ένας κόμβος λειτουργήσει επιθετικά πέντε φορές ο σταθμός βάσης δίνει εντολή για αποκλεισμό του από τους πίνακες δρομολόγησης του δικτύου.

Επιλύοντας το παιχνίδι με τη μέθοδο της κυριαρχίας καταλήξαμε σε δύο Nash ισορροπίες. Μελετώντας τις ισορροπίες αυτές καταλήξαμε ότι και οι δύο καταστάσεις είναι απολύτως επιθυμητές για το δίκτυο μας. Στη πρώτη (ASE) ο potential attacker κάνει μια ενέργεια επίθεσης η οποία όμως ανιχνεύεται και αντιμετωπίζεται επιτυχώς και από τα δύο IDS συστήματα. Στη δεύτερη περίπτωση, ο potential attacker λειτουργεί σαν ένας κανονικός κόμβος του δικτύου, και τα δύο IDS συστήματα του επιτρέπουν να συνεχίσει την ομαλή λειτουργία του.

Σε σχέση με τις συναφείς εργασίες που μελετήσαμε στο κεφάλαιο 5 το παιχνίδι που κατασκευάσαμε διαφοροποιήθηκε σε αρκετά σημεία. Καταρχάς το παιχνίδι μας αποτελείται από τρείς παίκτες, potential attacker, Local IDS, Global IDS. Στην βιβλιογραφία κυρίως είδαμε παίγνια ασφάλειας μεταξύ συνήθως δύο παικτών με εξαίρεση την εργασία των Tansu Alpcan και Tamer Basar [Alpcan και Basar, 2004] όπου είχαν όμως 2 chance players, σε ένα incomplete information game. Ένα άλλο ξεχωριστό σημείο του παιγνίου είναι η ταυτόχρονη χρήση δύο IDS συστημάτων μέσα στο δίκτυο. Τέλος, σημαντικό χαρακτηριστικό της εργασίας μας είναι η κατασκευή ενός παιγνίου από το μηδέν. Περιγράψαμε το παιχνίδι, δημιουργήσαμε τις αποδόσεις των παικτών με βάση συγκεκριμένη λογική και στο τέλος το επιλύσαμε με το πρόγραμμα Gambit αλλά και με το χέρι. Σε όλες τις περιπτώσεις στο κεφάλαιο 5 είδαμε πως όριζαν αυθαίρετα τις αποδόσεις των παικτών με βάση τα αποτελέσματα που επιθυμούσαν να βγάλει το Gambit. Αντίθετα εμείς δημιουργήσαμε τις προτιμήσεις του κάθε παίκτη χρησιμοποιώντας τη συνάρτηση χρησιμότητας Von Neumann και Morgenstern. Με βάση των συναρτήσεων χρησιμότητας του κάθε παίκτη καθορίστηκαν και οι αποδόσεις.

Στην παρούσα εργασία αντιμετωπίστηκαν τα σημαντικότερα (κατά την κρίση μας) ερευνητικά ερωτήματα με βάση τους διαθέσιμους πόρους. Πέρα όμως από αυτά, σημαντικό θα ήταν επίσης να γίνει και μια περαιτέρω μελέτη πάνω στο θέμα. Θα μπορούσε το παιχνίδι GoWiSeN που κατασκευάστηκε στο κεφάλαιο 6 να προσομοιωθεί χρησιμοποιώντας κάποιο λογισμικό προσομοίωσης όπως είναι το TOSSIM [TOSSIM]. Επίσης εξετάζοντας το θέμα από την πλευρά της θεωρίας των παιγνίων, θα μπορούσαμε να επεκτείνουμε λίγο το παίγνιο και να το κάνουμε επαναλαμβανόμενο (repeated). Θα είχε μεγάλο ενδιαφέρον να μελετήσουμε τις ισορροπίες που θα παρουσιάσει σε αυτή την περίπτωση.

9 Βιβλιογραφικές Αναφορές

Agah A., Basu K. and Das S. K., "A game theory based approach for security in sensor networks", International Performance Computing and Communications Conference (IPCCC), Phoenix, AZ, April 2004a.

Agah A., Basu K. and Das S. K., "Security enforcement in wireless sensor networks: A framework based on non-cooperative games", Pervasive and Mobile Computing Journal (PMC), Elsevier Publisher, 2005.

Agah A. and Das S. K., "Preventing DoS Attacks in Wireless Sensor Networks: A Repeated Game Theory Approach", International Journal of Network Security, 2007.

Agah A., Das S. K., Basu K. and Asadi M., "Intrusion detection in sensor networks: A non-cooperative game approach", 3rd IEEE International Symposium on Network Computing and Applications, NCA 2004, Boston, MA, August 2004b.

Akyildiz I., Su W., Sankarasubramaniam Y. and Cayirci E., "A survey on sensor networks", IEEE Communication Magazine, August 2002a.

Akyildiz I. F., Su W., Sankarasubramaniam Y. and Cayirci E., "Wireless sensor networks: a survey", Computer Networks, 2002b.

Albers P., Camp O., Percher J., Jouga B., Me L. and Puttini R., "Security in ad hoc Networks: A General Intrusion Detection Architecture Enhancing Trust Based Approaches", 1st International Workshop on Wireless Information Systems WIS'02, April 2002.

Alpcan T. and Basar T., "A game theoretic analysis of intrusion detection in access control systems", in Proc. of the 43rd IEEE Conference on Decision and Control, Paradise Island, Bahamas, December 2004.

Ambient systems, “Ambient systems - for low cost, low power, wireless mesh networking solutions”, http://www.ambient-systems.net, July 2006.

Anderson J.P., “Computer Security Threat Monitoring and Surveillance”, Tech. Rep. 79F296400, J.P Anderson Co., April 15, 1980.

Anderson R., “Security Engineering: A Guide to Building Dependable Distributed Systems”, Wiley Computer Publishing, New York, 2001.

Anderson R. and Kuhn M., “Tamper Resistance - a Cautionary Note”, Proc. 2nd Usenix Workshop Electronic Commerce, Usenix, Berkeley, Calif., 1996.

Bace R., “Intrusion Detection”, MacMillan Technical Publishing, 2000.

Binmore K., “Playing for Real - A text on game theory”, Oxford University Press, 2007a.

Binmore K., “Game Theory: A Very Short Introduction”, Oxford University Press, USA, 2007b.

Bishop M., Cheung S. and Wee C., “The Threat from the Net”, IEEE Spectrum, vol. 34 (8), 1997.

Business Week “21 ideas for the 21st century”, August 1999.

Carmichael F., “A Guide to Game Theory”, Financial Times Prentice Hall, 2004.

Celler B.G. et al., “An instrumentation system for the remote monitoring of changes in functional health status of the elderly”, International Conference IEEE-EMBS, New York, 1994.

Cheung S. and Levitt K.N., “Protecting Routing Infrastructures from Denial of Service Using Cooperative Intrusion Detection”, Proc. Workshop New Security Paradigms, ACM Press, New York, 1997.

Dixit A. and Skeath S., “Games of Strategy”, W.W. Norton & Company, 1999.

Doumit S. S. and Agrawal D. P., “Self-Organized Critically & Stochastic Learning Based Intrusion Detection System for Wireless Sensor Networks”, 2003 Military Communications Conference (MILCOM’03), October 2003.

Dutta P. K., “Strategies and Games: Theory and Practice”, Chapters 5-8. Cambridge, Massachusetts: The MIT Press, 1999.

Dutta P. K., “On Random Event Detection with Wireless Sensor Networks”, Masters Thesis, Ohio State University, 2004.

Gambit, http://gambit.sourceforge.net

Gibbons R., “A Primer in Game Theory”, Financial Times Prentice Hall, June 1992.

Heinzelman W., Kulik J. and Balakrishnan H., “Adaptive protocols for information dissemination in wireless sensor networks”, Proceedings of the ACM MobiCom'99, Seattle, Washington, 1999.

Heinzelman W. R., Chandrakasan A. and Balakrishnan H., “Energy-efficient communication protocol for wireless microsensor networks,” in The 33rd Annual Hawaii International Conference on System Sciences (HICSS-33), January 2000, Proceedings of the Hawaii International Conference on System Sciences, Maui, USA, IEEE, Los Alamitos, CA, USA, 2000.

Hsin C. and Liu M., “A Distributed Monitoring Mechanism for Wireless Sensor Networks”, 1st ACM Workshop on Wireless Security (WiSe’02), September 2002.

Hu F. and Sharma N. K., “Security considerations in ad hoc sensor networks”, Ad Hoc Networks”, Elsevier, August 2005.

Intanagonwiwat C., Govindan R. and Estrin D., “Directed diffusion: A scalable and robust communication paradigm for sensor networks”, Proceedings of the ACM MobiCom'00, Boston, MA, 2000.

Johnson D.B. and Maltz D.A., “Dynamic Source Routing in Ad Hoc Wireless Networks”, Mobile Computing, vol. 353, Imielinski and Korth, Eds. Kluwer Academic Publishers, Boston, 1996.

Kahn J.M., Katz R.H. and Pister K.S.J., “Next century challenges: mobile networking for smart dust”, Proceedings of the ACM MobiCom’99, Washington, USA, 1999.

Kantzavelou I. and Katsikas S., “Solving an Incomplete Information Intrusion Detection Game”, unpublished manuscript, 2007.

Karlof C. and Wagner D., “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”, 1st IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.

Kong J., Luo H., Xu K., Gu D. L., Gerla M. and Lu S., “Adaptive Security for Multi-Layer Ad-Hoc Networks”, Special Issue of Wireless Communications and Mobile Computing, 2002.

Kurata N., B. F. Spencer, Jr, and M. Ruiz-Sandoval, “Application of Wireless Sensor Mote for Building Risk Monitoring”, in Proceedings of INSS, 2004.

Li L. and Halpern J., “Minimum energy mobile wireless networks revisited”, in the Proceedings of IEEE International Conference on Communications (ICC’01), Helsinki, Finland, June 2001.

Marti S., Giuli T., Lai K. and Baker M., “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks”, 6th ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom’00), August 2000.

Michiardi P. and Molva R., “Game theoretic analysis of security in mobile ad hoc networks”, In Institute Eurecom, France, 2002.

Noury N., Herve T., Rialle V., Virone G., Mercier E., Morey G., Moro A. and Porcheron T., “Monitoring behavior in home using a smart fall sensor, IEEE-EMBS Special Topic Conference on Microtechnologies in Medicine and Biology”, October 2000.

Osborne M.J., “An Introduction to Game Theory”, Oxford University Press, 2004.

Perkins C.E. and Bhagwat P., “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers”, Proc. SIGCOMM, ACM Press, New York, 1994.

Perrig A., Canetti R., Tygar J. D. and Song D., “Efficient Authentication and Signing for Multicast Streams over lossy Channels”, In IEEE Symposium on Security and Privacy, May 2000.

Perrig A. and Tygar J. D., “Secure Broadcast Communication in Wired and Wireless Networks”, Kluwer Academic Publisher, 2003.

Perrig A., Szewczyk R., Wen V., Culler D. and Tygar J. D., “SPINS: Security Protocols for Sensor Networks”, MobiCom, July 2001.

Rabaey J.M., Ammer M.J., da Silva J.L. Jr., Patel D. and Roundy S., “PicoRadio supports ad hoc ultra-low power wireless networking”, IEEE Computer Magazine, 2000.

Roman R., Zhou J. and Lopez J., “On the security of wireless sensor networks”, in International Conference on Computational Science and Its Applications – ICCSA 2005, May 9-12 2005, vol. 3482 of Lecture Notes in Computer Science, (Singapore), Springer Verlag, Heidelberg, D-69121, Germany, 2005.

Schuba C.L. et al., “Analysis of a Denial of Service Attack on TCP”, Proc. IEEE Symp. Security and Privacy, IEEE Press, Piscataway, N.J., 1997.

Seshandri A., Perrig A., Van Doorn L. and Khosla P., “SWATT: SoftWarebased ATTestation for Embedded Devices”, 2004 IEEE Symposium on Security and Privacy, May 2004.

Shen C., Srisatjapornphat C. and Jaikaeo C., “Sensor information networking architecture and applications”, IEEE Pers. Communication, August 2001.

Shih E., Cho S., Ickes N., Min R., Sinha A., Wang A. and Chandrakasan A., “Physical layer driven protocol and algorithm design for energy efficient wireless sensor networks”, Proceedings of ACM MobiCom'01, Rome, Italy, July 2001.

Sohrabi E., Gao J., Ailawadhi V. and Pottie G.J., “Protocols for self-organization of a wireless sensor network”, IEEE Personal Communications, October 2000.

TOSSIM, www.cs.berkeley.edu/~pal/research/tossim.html

Warneke B., Liebowitz B. and Pister K.S.J., “Smart dust: communicating with a cubic-millimeter computer”, IEEE Computer, January 2001.

Woo A. and Culler D., “A transmission control scheme for media access in sensor networks”, Proc. 7th Ann. Int'l Conf. Mobile Computing and Networking (MobiCom 2001), ACM Press, New York, 2001.

Wood A. D. and Stankovic J. A., “Denial of service in sensor networks”, Computer vol. 35, no. 10, 2002.

Xbow, “Crossbow technology - wireless sensor networks, inertial & gyro systems, smart dust, advanced sensors”, http://www.xbow.com, July 2005.

Zhang Y. and Lee W., “Intrusion Detection Techniques for Mobile Wireless Networks”, ACM/Kluwer Wireless Networks Journal, September 2003.