Ατομική Διπλωματική Εργασία

ΑΣΦΑΛΕΙΑ ΣΕ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΑΙΣΘΗΤΗΡΩΝ

Ανδρέου Καλλιόπη

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μάιος 2015

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Ασφάλεια σε Ασύρματα Δίκτυα Αισθητήρων

Ανδρέου Καλλιόπη

Επιβλέπων Καθηγητής
Δρ. Βάσος Βασιλείου

Η Ατομική Διπλωματική Εργασία υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων απόκτησης του πτυχίου Πληροφορικής του Τμήματος Πληροφορικής του Πανεπιστημίου Κύπρου.

Μάιος 2015

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου, Δρ. Βάσο Βασιλείου για την καθοδήγηση και για την όλη άψογη συνεργασία κατά την διάρκεια της εκπόνησης της ατομικής αυτής, διπλωματικής εργασίας.

Επίσης θα ήθελα να ευχαριστήσω την διδακτορική φοιτήτρια του τμήματος Χριστιάνα Ιωάννου, για την υποστήριξη και την πολύτιμη βοήθεια που μου πρόσφερε μέσα σε αυτό το χρονικό διάστημα, για την ολοκλήρωση αυτής της εργασίας.

Τέλος, ήθελα να ευχαριστήσω την οικογένειά μου για την στήριξη και την συμπαράσταση καθ' όλη την διάρκεια των σπουδών μου.

Περίληψη

Με το πέρας των χρόνων, η ραγδαία ανάπτυξη της τεχνολογίας είναι πολύ αισθητή ανά το παγκόσμιο μιας και έχει αναπτυχθεί περισσότερο από οποιαδήποτε άλλη επιστήμη. Χρησιμοποιείται τόσο για ειρηνικούς σκοπούς προσφέροντας ανέσεις στην καθημερινή ζωή του ανθρώπου, όσο και για πολεμικούς σκοπούς μέσω της κατασκευής καταστροφικών όπλων και συστημάτων. Ένα είδος αυτών των συστημάτων, είναι οι διάφορες επιθέσεις που μπορούν να υπάρξουν μέσω του διαδικτύου και που βασικό σκοπό έχουν την εκμετάλλευση δεδομένων προκειμένου να προκαλέσουν σημαντικά προβλήματα σε ολόκληρα δίκτυα.

Όπως και τα παραδοσιακά δίκτυα, επιθέσεις είναι δυνατόν να δεχτούν και τα ασύρματα δίκτυα αισθητήρων, τα οποία λόγω της φύσεως τους είναι σαφώς και πιο ευάλωτα. Τα ασύρματα δίκτυα διαφοροποιούνται από τα υπόλοιπα, αφού αποτελούνται από πολλούς κόμβους, μικρού μεγέθους, οι οποίοι λειτουργούν μερικώς αυτόνομα και έχουν περιορισμένες υπολογιστικές δυνατότητες.

Στην παρούσα λοιπόν διπλωματική εργασία, στόχος είναι η δημιουργία και μελέτη μερικών επιθέσεων που είναι δυνατόν να δεχτούν τα δίκτυα αισθητήρων. Σκοπός της συγκεκριμένης εργασίας είναι η μελέτη της συμπεριφοράς ενός ασύρματου δικτύου αισθητήρων όταν αυτό δέχεται επιθέσεις που εστιάζουν στη δρομολόγηση (routing attack) και οι οποίες έχουν ως αποτέλεσμα την άρνηση παροχής υπηρεσιών από το δίκτυο (Denial-of-Services Attack). Συγκεκριμένα, για τον σκοπό αυτό, υλοποιήθηκε ένας ιός σε δύο μορφές, ο Sybil Attack-Stolen identities και ο Sybil Attack- Fabricated identities.

Περιεχόμενα

Contents

Κεφάλαιο 1

Εισαγωγή

1.1 Εισαγωγή

Στο κόσμο της πληροφορικής η χρήση όλο και πιο προχωρημένων τεχνικών και τεχνολογιών, όπως για παράδειγμα οι σύγχρονες βάσεις δεδομένων και τα σύγχρονα δίκτυα, προσφέρουν σημαντικά πλεονεκτήματα και δυνατότητες όπου κανένας δεν μπορεί να αμφισβητήσει. Παρόλα αυτά όμως αυξάνουν τα προβλήματα που αφορούν την προστασία και τη διαθεσιμότητα των πληροφοριών. Αναγκαία και απαραίτητη συνθήκη για την ομαλή λειτουργία ενός οργανισμού ή μιας επιχείρησης, είναι η ασφάλεια.

Η έννοια της ασφάλειας ενός Δικτύου Υπολογιστών σχετίζεται με την ικανότητα μιας επιχείρησης ή ενός οργανισμού, να προστατεύει τις πληροφορίες τους από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων από τρίτου. Για την επίτευξη των πιο πάνω, κρίνεται απαραίτητη η λήψη μέτρων τα οποία διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων.

Συγκεκριμένα, η ασφάλεια στα δίκτυα αφορά εκτός από την προστασία, την πρόληψη και την ανίχνευση τυχών επιθέσεων που μπορούν υπάρξουν στα δίκτυα. Έτσι, απαραίτητα συστατικά είναι τα πιο κάτω:

- **Πρόληψη (prevention)** : Λήψη μέτρων για να προληφθούν φθορές των μονάδων ενός δικτύου υπολογιστών.
- **Ανίχνευση (detection) :** Λήψη μέτρων για την ανίχνευση του πότε, πώς και από ποιον προκλήθηκε φθορά σε μία από τις παραπάνω μονάδες.
- **Αντίδραση (reaction)** : Λήψη μέτρων για την αποκατάσταση ή ανάκτηση των συστατικών ενός δικτύου

1.2 Κίνητρο και Σκοπός Εργασίας

Στη εποχή που διανύουμε, στις βασικές γνώσεις των πλείστων ανθρώπων, συμπεριλαμβάνεται και η χρήση του διαδικτύου. Έτσι, πολλά προσωπικά δεδομένα και πληροφορίες εκτίθενται στη κοινή χρήση με αποτέλεσμα να κινδυνεύει η ασφάλεια τους. Για την ασφάλεια τους όμως, πρέπει να καταπολεμηθούν ή έστω να μειωθούν οι επιθέσεις που τυχόν να υπάρχουν στα δίκτυα και γενικά στην διακίνηση πληροφοριών. Για την εύκολη αντιμετώπιση τους όμως, βασικό ρόλο έχει η ανίχνευση του κινδύνου.

Έτσι, με κίνητρο την ανίχνευση επιθέσεων, στην εργασία αυτή υλοποιήθηκε μια μορφή κάποιας επίθεσης σε ασύρματα δίκτυα αισθητήρων, με σκοπό την εξαγωγή συμπερασμάτων της συμπεριφοράς ενός δικτύου εν όψει κακόβουλου αισθητήρα, με σκοπό την ανίχνευση της και την δημιουργία συστήματος ανίχνευση της επίθεσης αυτής (Intrusion Detection System).

1.3 Μεθοδολογία

Η υλοποίηση της εργασίας αυτής, έγινε με βάση την ανάγνωση και κατανόηση διαφόρων άρθρων και κειμένων που αφορούσαν την ασφάλεια σε διάφορα δίκτυα υπολογιστών και ασύρματων δικτύων αισθητήρων. Έπειτα, μελετήθηκαν διάφορες επιθέσεις στις οποίες έρχεται αντιμέτωπο ένα είδους δίκτυο, λόγω της φύσης του καθώς και διάφορα τρόποι αντιμετώπισης τους. Στη συνέχεια, έγινε υλοποίηση μίας επίθεσης σε ασύρματα δίκτυα αισθητήρων και τέλος, μέσω πολλών προσημειώσεων, εξάχθηκαν αποτελέσματα για την αλλαγή της συμπεριφοράς του δικτύου και της δρομολόγησης.

1.4 Δομή

Η εργασία αυτή, αρχικά ασχολείται με τα Δίκτυα Υπολογιστών εξηγώντας το τι είναι και ποιες είναι η βασικές έννοιες ασφάλειας σε αυτά. Επίσης, αναφέρει τα εργαλεία μέσω των οποίων παρέχεται η ασφάλεια καθώς επίσης και τις επιθέσεις που τυχόν να υπάρξουν.

Το επόμενο κεφάλαιο, αναφέρεται στο κύριο μέρος της εργασίας το οποίο είναι τα Ασύρματα Δίκτυα Αισθητήρων. Γίνεται μια εισαγωγή για τον τομέα των δικτύων αυτών, την αρχιτεκτονική τους, τις επιθέσεις, τους περιορισμούς που υπάρχουν και τέλος προτείνονται κάποιες λύσεις για την ασφάλεια και περιπτώσεις εφαρμογής των ασύρματων δικτύων.

Ακολούθως, στο τέταρτο κεφάλαιο αναλύεται το περιβάλλον εργασίας που

χρησιμοποιήθηκε και είναι το πρόγραμμα Contiki OS 2.5, το οποίο είναι ένα ανοικτού τύπου λειτουργικό σύστημα για δικτυωμένες συσκευές περιορισμένης μνήμης και το εργαλείο Cooja. Δύο αυτά προγράμματα, χρησιμοποιήθηκαν για την υλοποίηση του ιού Sybil σε δύο μορφές των οποίων τα αποτελέσματα φαίνονται στο πέμπτο κεφάλαιο με διάφορες γραφικές.

Τέλος, στο έκτο και τελευταίο κεφάλαιο, γίνεται αναφορά στα συμπεράσματα από την όλη μελέτη και υλοποίηση της εργασίας.

Κεφάλαιο 2

Ασφάλεια Δικτύων

2.1 Δίκτυα Υπολογιστών

Ένα δίκτυο υπολογιστών είναι ένα σύστημα επικοινωνίας δεδομένων που συνδέει δύο ή περισσότερους αυτόνομους και ανεξάρτητους υπολογιστές και περιφερειακές συσκευές. Δύο υπολογιστές θεωρούνται διασυνδεδεμένοι όταν μπορούν να ανταλλάσσουν μεταξύ τους πληροφορίες.

Τα δίκτυα δημιουργήθηκαν για να εξυπηρετήσουν τις ανάγκες που προέκυψαν από την εξάπλωση της χρήσης των υπολογιστών. Βασικός σκοπός της ύπαρξης των δικτύων είναι ο διαμερισμός των πόρων του συστήματος και η ανταλλαγή πληροφοριών κάθε μορφής (προγράμματα, αρχεία, δεδομένα). Πόροι του συστήματος μπορούν να είναι είτε υλικό (hardware), π.χ. υπολογιστές, εκτυπωτές, σκληροί δίσκοι είτε λογισμικό (Software), π.χ. δεδομένα, προγράμματα εφαρμογών, υπηρεσίες. Τα προγράμματα, τα δεδομένα και οι συσκευές (σκληροί δίσκοι, εκτυπωτές, κλπ.) είναι διαθέσιμα σε οποιονδήποτε είναι συνδεδεμένος στο δίκτυο, ανεξάρτητα από τη φυσική του θέση. Με τον τρόπο αυτό επιτυγχάνεται εξοικονόμηση χρημάτων, αύξηση της απόδοσης του συστήματος, κεντρικός έλεγχος και εύκολη επεκτασιμότητα. Σε ένα δίκτυο μπορούμε να έχουμε ανταλλαγή δεδομένων, προγραμμάτων, χρήση κοινών βάσεων δεδομένων, αρχείων, αποστολή μηνυμάτων (electronic mail). Επιπλέον, ανεξάρτητα της τεχνολογίας, ένα δίκτυο είναι ένα πανίσχυρο μέσο επικοινωνίας ανθρώπων που βρίσκονται σε διαφορετικά μέρη.

Τα δομικά στοιχεία ενός δικτύου είναι:

- Υπολογιστικό σύστημα (host), όπως προσωπικοί υπολογιστές, σταθμοί εργασίας, εξυπηρετητές δικτύου (network servers).
- Κόμβοι (nodes), δηλαδή σημεία συνάντησης γραμμών επικοινωνίας (γραμμές μετάδοσης, κυκλώματα ζεύξης, κατανεμητές καλωδίων - hub, δρομολογητές).
- Περιφερειακές συσκευές δικτύου (network peripherals), όπως εκτυπωτές, modem, plotters κ.ά.
- Υποδίκτυο επικοινωνίας (communication subnet), που αφορά την καλωδίωση και τις γραμμές μετάδοσης.

2.2 Βασικές Έννοιες Ασφάλειας

Η χρησιμοποίηση όλο και πιο προχωρημένων τεχνολογιών όπως για παράδειγμα οι σύγχρονες βάσεις δεδομένων και τα σύγχρονα δίκτυα, προσφέρει αναμφισβήτητα σημαντικά πλεονεκτήματα και δυνατότητες, αυξάνει όμως ταυτόχρονα σημαντικά τα προβλήματα σχετικά με την προστασία και τη διαθεσιμότητα των πληροφοριών.

Η ασφάλεια αποτελεί αναγκαία συνθήκη και είναι απαραίτητη, σε συνδυασμό με τις άλλες βασικές προϋποθέσεις λειτουργίας- όπως η ποιότητα και η απόδοση- για την εξασφάλιση της εύρυθμης λειτουργίας μιας επιχείρησης ή ενός οργανισμού.

Η έννοια της ασφάλειας σήμερα, συνδέεται στενά με τέσσερις βασικές έννοιες που είναι η διαθεσιμότητα, η εμπιστευτικότητα, ο έλεγχος ακεραιότητας και η αυθεντικοποίηση.

2.2.1 Διαθεσιμότητα (Availability)

Διαθεσιμότητα ονομάζεται η ιδιότητα του να είναι διαθέσιμες και σε θέση να μπορούν να χρησιμοποιηθούν χωρίς καθυστέρηση οι υπηρεσίες ενός δικτύου, όταν κριθεί αναγκαίο. Για τους σκοπούς της ασφάλειας, αυτό σχετίζεται με την παρεμπόδιση κακόβουλων επιθέσεων που σκοπό έχουν να παρεμποδίσουν την είσοδο νόμιμων χρηστών. Αυτές οι επιθέσεις ονομάζονται επιθέσεις άρνησης παροχής υπηρεσιών (DoS) και σκοπό έχουν να θέσουν τους πόρους του συστήματος έκτος λειτουργίας είτε προσωρινά είτε μόνιμα [1].

2.2.2 Εμπιστευτικότητα (Confidentiality)

Σε πολλές περιπτώσεις της καθημερινής ζωής οι έννοιες της ασφάλειας και της

εμπιστευτικότητας σχεδόν ταυτίζονται, όπως για παράδειγμα στα στρατιωτικά περιβάλλοντα όπου η ασφάλεια έχει τη σημασία του να κρατούνται μυστικές οι πληροφορίες.

Η εμπιστευτικότητα σημαίνει πρόληψη μη εξουσιοδοτημένης αποκάλυψης πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη ανάγνωση. Επομένως, σημαίνει ότι τα δεδομένα που διακινούνται μεταξύ των υπολογιστών ενός δικτύου, αποκαλύπτονται μόνο σε εξουσιοδοτημένα άτομα. Αυτό αφορά όχι μόνο την προστασία από μη εξουσιοδοτημένη αποκάλυψη των δεδομένων αυτών καθαυτών αλλά ακόμη και από το γεγονός ότι τα δεδομένα απλώς υπάρχουν [2][3][5].

Άλλες εκφάνσεις της εμπιστευτικότητας είναι:

- Η ιδιωτικότητα : προστασία των δεδομένων προσωπικού χαρακτήρα, δηλαδή αυτών που αφορούν συγκεκριμένα πρόσωπα και
- Η μυστικότητα : προστασία των δεδομένων που ανήκουν σε έναν οργανισμό ή μια επιχείρηση.

2.2.3 Ακεραιότητα (Integrity)

Ακεραιότητα είναι η πρόληψη μη εξουσιοδοτημένης μεταβολής πληροφοριών, δηλαδή πρόληψη από μη εξουσιοδοτημένη εγγραφή ή διαγραφή, συμπεριλαμβανομένης και της μη εξουσιοδοτημένης δημιουργίας δεδομένων. Εκτός δηλαδή από την προστασία των δεδομένων έτσι ώστε να μην έχουν πρόσβαση μη εξουσιοδοτημένα άτομα, υπάρχει και η ανάγκη για προστασία της ακεραιότητας τους. Μπορεί να εμποδιστεί μια κακόβουλη ενέργεια, όπως το να "κλαπούν" πληροφορίες, όμως με την εμπιστευτικότητα αυτό δεν μπορεί να εμποδίσει ένα εισβολέα να προκαλέσει ζημιά στο δίκτυο, αλλάζοντας το περιεχόμενο των πακέτων που διακινούνται μεταξύ των κόμβων [3][4].

2.2.4 Αυθεντικοποίηση (Authentication)

Η αυθεντικοποίηση, είναι μια λειτουργία η οποία απαγορεύει μη εξουσιοδοτημένη πρόσβαση μέσα στο δίκτυο και που επιτρέπει στους υπόλοιπους κόμβους να ανιχνεύσουν αν τα πακέτα έρχονται από τον πραγματικό αποστολέα ή από κάποιον άλλο κακόβουλο κόμβο, οπότε και μπορούν σε αυτή την περίπτωση να τα απορρίψουν.

Στην περίπτωση της ασφάλειας των δικτύων λοιπόν, γίνεται ένας έλεγχος προκειμένου να εξακριβωθεί κατά πόσο η ταυτότητα του αποστολέα είναι όντως αυτή

που παρουσιάζει. Γίνεται λοιπόν μια επαλήθευση της ταυτότητας του αποστολέα και εγγυάται στον παραλήπτη πως ο αποστολέας δεν είναι κάποιος εισβολέας [2][3][5].

Με την έναρξη της επικοινωνίας δύο κόμβων, γίνεται αυθεντικοποίηση της ταυτότητας και των δύο συμμετεχόντων. Στην συνέχεια γίνεται ένας ακόμα έλεγχος προκειμένου να επιβεβαιωθεί ότι δεν υπάρχει τρίτος χρήστης ο οποίος προσπαθεί να υποκλέψει τα δεδομένα που ανταλλάσσουν οι δύο κόμβοι μεταξύ των οποίων έχει εγκαθιδρυθεί επικοινωνία [5].

Σύμφωνα με τα [4][6][7], η αυθεντικοποίηση λειτουργεί με ένα συμμετρικό μηχανισμό, όπου τόσο ο αποστολέας όσο και ο παραλήπτης μοιράζονται ένα μυστικό κλειδί για να υπολογίσουν το message authentication code (MAC). Το MAC είναι σαν μια ετικέτα που προκύπτει όταν δώσουμε στον αλγόριθμο το μυστικό κλειδί και το μήνυμα.

Η δομή του δικτύου από μόνη της, επιτρέπει την εκτέλεση επιθέσεων. Για την παρεμπόδιση τους, πρέπει αυτές να γνωστοποιηθούν και να ερευνηθούν, έτσι ώστε να μπορέσει να βρεθεί μια αποτελεσματική μέθοδος αντιμετώπισης τους [3][4][5].

2.3 Εργαλεία Ασφάλειας Δικτύων

Για την εξάλειψη ή έστω τη μείωση των επιθέσεων που δέχονται συνεχώς τα δίκτυα, διάφορες μέθοδοι, τεχνικές και μηχανισμοί έχουν αναπτυχθεί.

Για την προστασία λοιπόν κάποιων δεδομένων δεν πρέπει να λαμβάνεται υπόψη μόνο ένας τύπος ασφάλειας, όπως επίσης δεν πρέπει να γίνεται χρήση ενός μόνο εργαλείου. Μερικά τέτοια εργαλεία αναλύονται παρακάτω [8]:

- **Συστήματα Ανίχνευσης Εισβολής (Intrusion Detection Systems)**

Τα συστήματα αυτά αποτελούν συστήματα παρακολούθησης και ανάλυσης των συμβάντων που δημιουργούνται στα δίκτυα υπολογιστών καθώς και στους προσωπικούς υπολογιστές. Μπορούν να εντοπίζουν μη εξουσιοδοτημένη πρόσβαση σε ένα δίκτυο και να βοηθούν στην απομάκρυνση κινδύνων που μπορεί να υπάρξουν, μέσω της παρακολούθησης των ροών ανταλλαγής πακέτων μεταξύ των κόμβων. Οι προσπάθειες παράκαμψης των μηχανισμών ασφαλείας μπορεί να προέρχονται από εξωτερικούς μη εξουσιοδοτημένους χρήστες ή από εσωτερικούς χρήστες με περιορισμένα δικαιώματα πρόσβασης.

Οι λόγοι εγκατάστασης ενός συστήματος ανίχνευσης εισβολής ποικίλουν. Οι πιο σημαντικοί από αυτούς τους λόγους είναι η πρόληψη προβλημάτων, η ανίχνευση παραβιάσεων, η τεκμηρίωση υπαρκτών απειλών, ο έλεγχος ποιότητας για το σχεδιασμό ασφαλείας, καθώς και η θωράκιση παλαιών συστημάτων σε περίπτωση που κρίνεται αναγκαία η διατήρησή τους. Στην περίπτωση όμως όπου έχουμε ένα νόμιμο χρήστη ο οποίος μπορεί να έχει μια απαγορευμένη πρόσβαση σε πληροφορίες, τότε αυτός δεν μπορεί να ανιχνευθεί από το σύστημα ανίχνευσης εισβολής [8][9].

- **Κρυπτογραφικά Συστήματα (Cryptographic Systems)**

Κρυπτογράφηση είναι η διαδικασία μετατροπής δεδομένων με τρόπο ώστε μη εξουσιοδοτημένα άτομα να μην μπορούν να αναγνωρίσουν τη σημασία των δεδομένων αυτών και να τα διαβάσουν. Αποκρυπτογράφηση των δεδομένων μπορεί να γίνει με την ύπαρξη κατάλληλου κλειδιού που περιορισμένα άτομα το γνωρίζουν.

Έτσι, ο μηχανισμός όμως αυτός δεν μπορεί να ξεχωρίσει ένα νόμιμο χρήστη από ένα μη νόμιμο αν τα κλειδιά τα οποία χρησιμοποιούν είναι τα ίδια [8][10].

- **Τείχος Προστασίας (Firewall)**

Ο μηχανισμός αυτός είναι ο πρώτος ο οποίος αντιμετωπίζει οποιαδήποτε απειλή δεχτεί το δίκτυο. Παρεμποδίζει πακέτα τα οποία θεωρεί κακόβουλα, από το να περάσουν στο εσωτερικό του δικτύου ή να θεωρηθούν ως σημαντικές πληροφορίες. Με λίγα λόγια αυτό που κάνει είναι να ελέγχει την ροή της κίνησης των πακέτων, εμποδίζοντας πακέτα να εισέλθουν ή να εξέλθουν σύμφωνα κάποιους κανόνες.

Μια αδυναμία του Firewall όμως, είναι το ότι δεν μπορεί να προστατέψει το δίκτυο από κάποιον ο οποίος βρίσκεται ήδη μέσα στο ίδιο το δίκτυο [8][11].

2.4 Επιθέσεις στα δίκτυα

Χωρίς τη λήψη μέτρων ασφάλειας και ελέγχων τα δίκτυα γενικώς, είναι δυνατόν να αντιμετωπίζουν κακόβουλες επιθέσεις που θέτουν σε κίνδυνο τις υπηρεσίες που αυτά παρέχουν.

- **Identity Spoofing (IP Address Spoofing)**

Για τον εντοπισμό μιας έγκυρης οντότητας σε ένα δίκτυο, συνήθως χρησιμοποιείται η διεύθυνση IP του υπολογιστή. Κάποιες φορές όμως, η διεύθυνση αυτή μπορεί να πλαστογραφηθεί μέσω ειδικών προγραμμάτων και έτσι να μην είναι έγκυρη. Επίσης,

κάποιος εισβολέας, κατά την επίθεση αυτή, μπορεί να δημιουργήσει δικές του έγκυρες διευθύνσεις IP και μπαίνοντας νόμιμα στο δίκτυο να τροποποιήσει, αναδρομολογήσει, ή να διαγράψει δεδομένα.

- **Denial-Of -Service Attack**

Η επίθεση αυτή, μπορεί να προκαλέσει καθυστέρηση στην παροχή υπηρεσιών σε ένα εξουσιοδοτημένο χρήστη, μέχρι και πλήρη διακοπή της παροχής υπηρεσιών, κάτι το οποίο ουσιαστικά σημαίνει πως μπορεί να ρίξει σε κάποιο βαθμό την απόδοση του συστήματος μέχρι και πλήρη κατάρρευση του δικτύου. Αυτό εξαρτάται από το αν ο επιτιθέμενος στοχεύει σε ένα συγκεκριμένο κόμβο, ή το κανάλι επικοινωνίας.

Ο τρόπος με τον οποίο μπορεί να προκαλέσει μια τέτοια ζημιά στο δίκτυο κάποιος κακόβουλος κόμβος, είναι στέλνοντας συνεχώς αχρείαστα πακέτα μέσα στο δίκτυο. Οπότε με αυτό τον τρόπο προκαλούνται συγκρούσεις ή ακόμα και συμφόρηση μεταξύ των πακέτων και συνεπώς τα πακέτα από άλλους κόμβους δεν μπορούν να κινηθούν μέσα στο δίκτυο και να φτάσουν στον προορισμό τους [31][32].

- **Man-in-the-Middle Attack**

Σε αυτή την επίθεση, ο επιτιθέμενος παρεμποδίζει τη νόμιμη επικοινωνία μεταξύ των δύο άκρων που επικοινωνούν, τα οποία είναι φιλικά μεταξύ τους. Στη συνέχεια, ο κακόβουλος κόμβος ελέγχει τη ροή επικοινωνίας και μπορεί να αλλάξει πληροφορίες που στέλνονται από έναν από τους αρχικούς συμμετέχοντες [12].

Κεφάλαιο 3
Ασφάλεια στα Ασύρματα Δίκτυα Αισθητήρων

3.1 Εισαγωγή

Ένα ασύρματο δίκτυο αισθητήρων είναι μια συλλογή από οργανωμένους κόμβους σε ένα δίκτυο. Οι κόμβοι αυτοί, είναι μικρού μεγέθους αισθητήρες οι οποίοι λειτουργούν αυτόνομα και επικοινωνούν ασύρματα μεταξύ τους.

Ο κάθε κόμβος αποτελείται από ένα ή περισσότερους microcontrollers, CPUs ή DSP chips τα οποία του δίνουν την δυνατότητα να επεξεργάζεται τα δεδομένα, να προγραμματίζει διάφορες διεργασίες και να ελέγχει την λειτουργικότητα των άλλων συστατικών του υλικού και στην συνέχεια μπορεί να τα αποθηκεύει στην μνήμη του, η οποία όμως είναι περιορισμένη.

Επίσης διαθέτουν μια πηγή ενέργειας (μπαταρία ή πυκνωτής), η οποία χρησιμοποιείται για την συλλογή των δεδομένων, την επεξεργασία τους και για την ανταλλαγή των δεδομένων μεταξύ των κόμβων. Η περισσότερη κατανάλωση ενέργειας γίνεται κατά την επικοινωνία του ενός κόμβου με τους υπόλοιπους, παρά κατά την επεξεργασία των δεδομένων ή την συλλογή τους.

Οι αισθητήρες αυτοί, λόγω του εχθρικού αφύλακτου περιβάλλοντος στο οποίο ίσως να λειτουργούν, χρειάζονται οπωσδήποτε προστασία για την διατήρηση της ακεραιότητας των δεδομένων και των πληροφοριών. Οι τεχνικές ασφάλειας όμως που εφαρμόζονται στα κανονικά δίκτυα υπολογιστών, δεν μπορούν να εφαρμοστούν και στα ασύρματα δίκτυα αισθητήρων και αυτό οφείλεται στην περιορισμένη ενέργεια που έχουν οι αισθητήρες στην διάθεση τους, στους περιορισμένους υπολογισμούς που μπορούν να πραγματοποιήσουν, όπως επίσης και στην περιορισμένη χωρητικότητα μνήμης [5][6].

3.2 Χαρακτηριστικά Κόμβων Αισθητήρων

Συμπερασματικά από τα πιο πάνω, διακρίνουμε τα πιο βασικά χαρακτηριστικά των κόμβων αισθητήρων τα οποία είναι τα εξής:

- Μικρό μέγεθος πακέτων αποστολής
- Χαμηλή ενέργεια
- Χαμηλό εύρος ζώνης
- Χαμηλό κόστος
- Μικρό μέγεθος μνήμης

3.3 Εφαρμογές ασύρματων δικτύων αισθητήρων

Η ανάπτυξη των δικτύων αισθητήρων, ξεκίνησε από στρατιωτικές εφαρμογές για την επόπτευση του πεδίου μάχης. Σύντομα όμως βρήκαν χρήση τόσο σε εφαρμογές βιομηχανικής κλίμακας όσο και καταναλωτικές. Μπορούμε να διακρίνουμε τις εφαρμογές στα παρακάτω:

1. Παρακολούθηση περιοχής

Μια από τις πιο συνηθισμένες εφαρμογές των WSN είναι η παρακολούθηση περιοχής. Το δίκτυο υλοποιείται σε μια περιοχή όπου πρέπει να καταγραφεί κάποιο φαινόμενο. Οι στρατιωτικές εφαρμογές θα μπορούσαν να καταταχτούν σ' αυτή την κατηγορία. Οι αισθητήρες σε αυτή την περίπτωση χρησιμοποιούνται για να ανιχνεύσουν μια πιθανή εισβολή του εχθρού. Οι αισθητήρες θα μπορούσαν να ανιχνεύουν την κίνηση ή τη θερμοκρασία και σε περίπτωση μεταβολών να αναφέρουν σε ένα από τους σταθμούς βάσης το γεγονός, στέλνοντας ένα μήνυμα μέσω Internet ή δορυφόρου.

2. Παρακολούθηση έξυπνου σπιτιού

Παρακολούθηση των δραστηριοτήτων που εκτελούνται σε ένα έξυπνο σπίτι επιτυγχάνονται με τη χρήση ασύρματων αισθητήρων, ενσωματωμένων σε αντικείμενα καθημερινής χρήσης, σχηματίζοντας ένα WSN. Όταν η κατάσταση αλλάζει σε αντικείμενα που βασίζονται στην ανθρώπινη χειραγώγηση, συλλαμβάνεται από το ασύρματο δίκτυο αισθητήρων που επιτρέπουν τη δραστηριότητα σε Υπηρεσίες υποστήριξης.

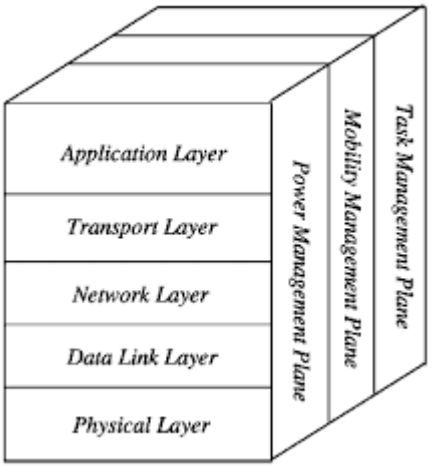
Άλλες πιθανές εφαρμογές

- Έλεγχος robot

- Παρακολούθηση στόλου οχημάτων
- Συστήματα ελέγχου για βιομηχανίες
- Παρακολούθηση κυκλοφορίας δρόμων
- Παρακολούθηση ιατρικών συσκευών
- Παρακολούθηση καταγραφή σεισμικής ή ηφαιστειακής δραστηριότητας.
- Έλεγχος εναέριας κυκλοφορίας

3.4 Αρχιτεκτονική Ασυρμάτων Δικτύων Αισθητήρων

Οι ασύρματοι κόμβοι διασπείρονται σε ένα πεδίο. Κάθε ένας από αυτούς συλλέγει δεδομένα, τα επεξεργάζεται και τα στέλνει πίσω σε ένα κεντρικό σημείο και από εκεί καταλήγουν στους ενδιαφερόμενους χρήστες.



Εικόνα 3.1: Στρώματα Ασύρματων Δικτύων Αισθητήρων [34]

Όπως φαίνεται από την παραπάνω εικόνα, τα ασύρματα δίκτυα αποτελούνται από πέντε επίπεδα. Το Application Layer, το Transport Layer, το Network Layer, το Data Link Layer και το Physical Layer.

Συνοπτικά, η λειτουργία του καθενός περιγράφεται παρακάτω:

- Φυσικό Επίπεδο (Physical Layer): Βασικός του σκοπός είναι μείωση της κατανάλωσης ισχύος, η επιλογή συχνότητας, η ανίχνευση σήματος και η διαμόρφωση και κρυπτογράφηση δεδομένων.
- Επίπεδο Διασύνδεσης Δεδομένων (Data-Link Layer): Είναι υπεύθυνο για την πολυπλεξία των δεδομένων, την εκπομπή και λήψη των 14 πλαισίων δεδομένων (data

frames), τον Έλεγχο Πρόσβασης Μέσου (Medium Access Control – MAC) και τον έλεγχο σφαλμάτων. Επίσης εξασφαλίζεται ο τρόπος με τον οποίο οι κόμβοι επικοινωνούν μεταξύ τους.

- Επίπεδο Δικτύου (Network Layer): Φροντίζει για τη διευθυνσιοδότηση και δρομολόγηση των πακέτων βρίσκοντας την καταλληλότερη διαδρομή για να φτάσει ένα πακέτο στον προορισμό του.
- Επίπεδο Μεταφοράς (Transport Layer): Είναι υπεύθυνο για τη ροή και τη μεταβίβαση των πακέτων δεδομένων όπως αυτό απαιτείται από το Επίπεδο Εφαρμογής.
- Επίπεδο Εφαρμογής (Application Layer): Το στρώμα αυτό, έχει ως αρμοδιότητα να εμφανίζει όλες τις πληροφορίες οι οποίες είναι απαραίτητες στην εφαρμογή, καθώς και να μεταφέρει τα αιτήματα από την εφαρμογή στα κατώτερα στρώματα του πρωτοκόλλου.

3.5 Επιθέσεις στα ασύρματα δίκτυα αισθητήρων

Τα δίκτυα αισθητήρων έχουν αυξηθεί σε μέγεθος και σπουδαιότητα σε πολύ σύντομο χρονικό διάστημα. Εάν όμως η ασφάλεια στα δίκτυα αυτά δεν είναι σταθερή μπορούν να υπάρξουν σοβαρές συνέπειες, αρχής γενομένης την κλοπή των πληροφοριών, την απώλεια της ιδιωτικής ζωής και την αλλοίωση των δεδομένων.

Οι τύποι των απειλών για το δίκτυο εξελίσσονται συνεχώς και πρέπει να υπάρχει τουλάχιστον θεωρητικά η γνώση για την αντιμετώπιση τους. Κάποιες από αυτές αναλύονται πιο κάτω.

3.5.1 Selective-Forwarding Attack

Στην επίθεση αυτή, κακόβουλοι κόμβοι προωθούν πακέτα επιλεκτικά με κύριο στόχο την διαταραχή των μονοπατιών δρομολόγησης. Ένας εισβολέας όταν καταστρέφει όλα τα πακέτα, προκειμένου αυτά να μην μεταδοθούν παρακάτω, συμπεριφέρεται ως black hole. Αυτό όμως είναι ένα ρίσκο αφού οι υπόλοιποι κόμβοι οι οποίοι προωθούν τα πακέτα τους στον συγκεκριμένο, υποψιάζονται πως αυτός αποτυγχάνει να μεταδώσει τα πακέτα παρακάτω, και έτσι αναζητούν ένα νέο κόμβο αντικαθιστώντας τον. Για να αποφευχθεί αυτό, ο κακόβουλος κόμβος δεν ‘πετά’ όλα τα πακέτα.

Για μεγαλύτερη αποτελεσματικότητα, ο εισβολέας επιλέγει να ‘μολύνει’ κάποιο κόμβο ο οποίος βρίσκεται κοντά ή ακόμα καλύτερα πάνω στο μονοπάτι της ροής των δεδομένων. Αυτό συμβαίνει γιατί μπορεί να έχει πιο εύκολη πρόσβαση στα πακέτα τα

οποία κινούνται στο δίκτυο και μπορεί να ελέγχει ακόμα περισσότερα πακέτα ιδίως όταν ο κόμβος είναι κοντά στην πηγή ή στον τελικό παραλήπτη [13][14].

3.5.2 Sinkhole Attack

Σε τέτοιου είδους επιθέσεις, οι κακόβουλοι αισθητήρες προσπαθούν μέσω διαφόρων ανακοινώσεων να επηρεάσουν την κυκλοφορία των μηνυμάτων σε ένα δίκτυο έτσι ώστε να γίνει η δρομολόγηση τους, μέσα από τους συγκεκριμένους κόμβους. Συγκεκριμένα, πλημυρίζουν το δίκτυο με εσφαλμένες χαμηλού κόστους διαδρομές με αποτέλεσμα οι κακόβουλοι αισθητήρες να φαίνονται ελκυστικοί. Εξασφαλίζοντας ότι όλη η κίνηση στην περιοχή ενδιαφέροντος κατευθύνεται μέσω ενός κακόβουλου αισθητήρα, μπορούν να απορριφθούν πακέτα που προέρχονται από οποιοδήποτε αισθητήρα του δικτύου. Σε κάποιες περιπτώσεις ένας κακόβουλος αισθητήρας διαφημίζει εσφαλμένα πως είναι ο αισθητήρας προορισμού με σκοπό την εξασφάλιση ότι όλα τα πακέτα θα φτάσουν κοντά του.

3.5.3 HELLO Flood Attack

Ένα HELLO μήνυμα, είναι το μήνυμα το οποίο στέλνεται πρώτο από ένα κόμβο κατά την ένταξη του στο δίκτυο. Υπάρχουν κάποια πρωτόκολλα τα οποία απαιτούν να γίνεται ένα broadcast από όλους τους κόμβους του δικτύου έτσι ώστε να γνωρίσει ο κάθε ένας τον γείτονα του. Ουσιαστικά μεταδίδονται hello πακέτα μεταξύ κόμβων. Κάθε κόμβος ο οποίος λαμβάνει από κάποιον άλλο ένα πακέτο, είναι σίγουρος πως αυτός είναι γείτονας του. Αυτό όμως δεν μπορεί να ισχύει πάντα, αφού ένας εισβολέας μπορεί να αρχίσει να μεταδίδει πληροφορίες δρομολόγησης ή άλλες πληροφορίες προς τους υπόλοιπους κόμβους, με μεγάλη ισχύ. Αφού λοιπόν μεταδίδονται πακέτα μέσα στο δίκτυο, αυτό θα έχει ως αποτέλεσμα πολλοί κόμβοι οι οποίοι είναι αρκετά hops μακριά, να τον αναγνωρίσουν ως γείτονα τους και να αρχίσουν να ανταλλάζουν δεδομένα με αυτόν.

Το αποτέλεσμα από αυτή την ανταλλαγή δεδομένων, όπου ίσως οι περισσότεροι κόμβοι είναι αρκετά μακριά από τον εισβολέα, είναι η ύπαρξη Multi-hop routed μηνυμάτων, μηνυμάτων δηλαδή που διανύουν μια απόσταση πολλών hop για να φτάσουν στον κακόβουλο κόμβο. Κατά συνέπεια έχουμε αύξηση της καθυστέρησης, χάσιμο δεδομένων, ακόμα και σπατάλη ενέργειας των κόμβων [15][16][17][18].

3.5.4 Wormhole Attack

Σε μια επίθεση τέτοιου είδους, ένας επιτιθέμενος λαμβάνει μηνύματα από ένα σημείο του δικτύου, τα διοχετεύει σε άλλο σημείο του δικτύου και στη συνέχεια τα επαναλαμβάνει στο δίκτυο από αυτό το σημείο. Μπορούν να χρησιμοποιηθούν για να πείσουν δύο απομακρυσμένους κόμβους ότι είναι γείτονες αναμεταδίδοντας πακέτα μεταξύ τους. Αν ο επιτιθέμενος εκτελεί αυτή τη διαδικασία άδολα και αξιόπιστα δεν δημιουργείται κακό. Στην πραγματικότητα, ο επιτιθέμενος παρέχει χρήσιμη υπηρεσία συνδέοντας το δίκτυο πιο αποτελεσματικά. Ωστόσο, η επίθεση αυτή, θέτει τον επιτιθέμενο σε πιο ισχυρή θέση από τους άλλους κόμβους του δικτύου και ο επιτιθέμενος μπορεί να το εκμεταλλευτεί με πολλούς τρόπους [19].

3.5.5 Blackhole Attack

Μια απλή μορφή της επίθεσης είναι όταν ένας κακόβουλος αισθητήρας συμπεριφέρεται σαν μαύρη τρύπα – Black Hole - και αρνείται να προωθήσει κάθε πακέτο που δέχεται. Σε αυτή τη μορφή επίθεσης, οι κακόβουλοι αισθητήρες διαφημίζουν ψευδώς καλές διαδρομές προς το κόμβο προορισμού (π.χ. τη συντομότερη διαδρομή). Απώτερος τους στόχος είναι είτε η παρεμπόδιση της διαδικασίας ανεύρεσης της διαδρομής μεταξύ αποστολέα και παραλήπτη είτε η υποκλοπή όλων των πακέτων δεδομένων που διαβιβάζονται στο ενδιαφερόμενο αισθητήρα προορισμού [20].

3.5.6 Sybil Attack

Η επίθεση Sybil ορίζεται ως μια κακόβουλη συσκευή η οποία παράνομα ¨κλέβει¨ ταυτότητες από γειτονικούς κόμβους ή τις δημιουργεί από μόνη της και τις παρουσιάζει ως δικές της. Οι ταυτότητες αυτές που παρουσιάζει ο Malicious node μπορεί να είναι είτε κατασκευασμένες είτε κλεμμένες από άλλους κόμβους που υπάρχουν μέσα στο δίκτυο και οι οποίοι σε αυτή την περίπτωση ονομάζονται Sybil nodes [22].

Η διαδικασία κατά την οποία ο κακόβουλος κόμβος αποκτά τις νέες ταυτότητας έχει ως εξής:

Στην περίπτωση όπου έχουμε κατασκευασμένες ταυτότητες (Sybil Attack-Fabricated identities), ο επιτιθέμενος δημιουργεί στην ουσία κάποιες αυθαίρετες Sybil ταυτότητες παράγοντας αυθαίρετους τυχαίους αριθμούς σαν αναγνωριστικά για τους Sybil κόμβους.

Στην περίπτωση όπου οι ταυτότητες είναι κλεμμένες (Sybil Attack-Stolen identities), ο επιτιθέμενος αναγνωρίζει τις ταυτότητες των γειτονικών του κόμβων μέσα στο δίκτυο και τις παρουσιάζει ως δικές του.

Ο κακόβουλος κόμβος λοιπόν μπορεί να παρουσιάζεται ως ένας Sybil node αποστολέας στους υπόλοιπους κόμβους, στους οποίους στέλνει κακόβουλα μηνύματα ή λανθασμένες πληροφορίες, όπως για παράδειγμα την διεύθυνση τoy αποστολέα αφού υποδύεται κάποιον άλλο κόμβο [33].

Κάτι παρόμοιο συμβαίνει και στην περίπτωση όπου οι άλλοι κόμβοι στην προσπάθεια τους να στείλουν πακέτα σε κάποιον Sybil node τα στέλνουν στην πραγματικότητα στον εισβολέα [17].

Το Sybil attack μπορεί να αποτελέσει μια σημαντική απειλή για το γεωγραφικό πρωτόκολλο δρομολόγησης. Σύμφωνα με το [18], κατά την ανταλλαγή πληροφοριών μεταξύ κόμβων προκειμένου να δρομολογηθεί σωστά ένα πακέτο, στην περίπτωση επίθεσης, ένας κόμβος μπορεί να εμφανίζεται πολλές φορές σε διαφορετικούς χώρους ταυτόχρονα προκαλώντας έτσι πρόβλημα στην δρομολόγηση του πακέτου, κάτι όμως που στην παρούσα διπλωματική εργασία δεν γίνεται.

Sybil Attack Taxonomy

- Διάσταση Ι: Άμεση εναντίον Έμμεσης Επικοινωνίας

Ένας τρόπος εκτέλεσης της Sybil επίθεσης είναι οι κόμβοι Sybil να επικοινωνούν άμεσα με τους νόμιμους κόμβους. Αυτή καλείται ως άμεση επικοινωνία. Δηλαδή, όταν ένας κόμβος στέλνει ένα μήνυμα σε έναν κόμβο Sybil, ή όταν ένας κόμβος Sybil στέλνει μήνυμα σε ένα νόμιμο κόμβο, μία από τις κακόβουλες συσκευές ακούει το μήνυμα αυτό.

Ο δεύτερος τρόπο εκτέλεσης της επίθεσης αυτής, είναι η έμμεση επικοινωνία, κατά την οποία οι νόμιμο κόμβοι δεν μπορούν να επικοινωνούν με τους Sybil κόμβους. Αντ' αυτού, η επικοινωνία τους γίνεται μέσω των κακόβουλων κόμβων. Μηνύματα που αποστέλλονται σε έναν κόμβο Sybil δρομολογούνται μέσω ενός από αυτούς τους κακόβουλους κόμβους, που προσποιούνται ότι θα περάσουν το μήνυμα σε ένα Sybil κόμβο.

- Διάσταση ΙΙ: Κατασκευασμένες εναντίον Κλεμμένων ταυτοτήτων

Ένας κόμβος Sybil να παίρνει μια ταυτότητα ακολουθώντας ένα από τους δύο τρόπους, οι οποίοι είναι η κατασκευή μιας νέας ταυτότητας, ή η κλοπή της από γειτονικούς νόμιμους κόμβους.

Σε ορισμένες περιπτώσεις, ο εισβολέας μπορεί να απλά δημιουργούν αυθαίρετες νέες ταυτότητες Sybil. Για παράδειγμα, εάν
κάθε κόμβος προσδιορίζεται από έναν ακέραιο αριθμό 32-bit, ο εισβολέας μπορεί απλά να ορίσει σε κάθε κόμβο Sybil μια τυχαία τιμή 32-bit. Αυτή είναι η περίπτωση κατασκευής ταυτότητας.

Στη περίπτωση κλοπής ταυτότητας ένας εισβολέας δεν μπορεί να κατασκευάσει νέες ταυτότητες, παρά μόνο να τις αντιγράψει από άλλους κόμβους.
Ένα ζήτημα που δημιουργείται με το Sybil attack, είναι το ότι η ίδια ταυτότητα χρησιμοποιείται πολλές φορές και υπάρχει σε πολλά σημεία στο δίκτυο, καταστρέφοντας την κανονική ροή του δικτύου.

- Διάσταση ΙΙΙ: Ταυτοχρονισμός εναντίων μη-ταυτοχρονισμού

Ο επιτιθέμενος μπορεί να προσπαθήσει να έχει όλες τις ¨εικονικές¨ του ταυτότητες να υπάρχουν ταυτόχρονα μέσα στο δίκτυο και αυτή είναι η περίπτωση συγχρονισμού.

Εναλλακτικά, ο εισβολέας μπορεί να παρουσιάσει μια ταυτότητα κατά τη διάρκεια μιας χρονικής περιόδου και αυτό γίνεται στην περίπτωση μη-ταυτοχρονισμού [23].

3.6 Περιορισμοί στα δίκτυα αισθητήρων

Κατά τον σχεδιασμό ασύρματων δικτύων αισθητήρων, υπάρχουν πολλοί περιορισμοί οι οποίοι πρέπει να ληφθούν υπόψη, ιδίως για την ύπαρξη ασφάλειας στα δίκτυα αυτά. Βασικότερο περιορισμό αποτελεί το μέγεθος των αισθητήρων, όμως υπάρχουν ακόμα πιο αυστηροί περιορισμοί για τους αισθητήριους κόμβους όπως:

- Ένας κανονικός κόμβος αποτελείται από ένα επεξεργαστή με συχνότητα 4-8 Mhz, έχει μέγεθος μνήμης RAM 4 KB, μια flash μνήμη 128 KB και radio frequency 916 Mhz.
- Πρέπει να καταναλώνουν εξαιρετικά χαμηλή ενέργεια.
- Πρέπει να λειτουργούν ακόμα και σε πολύ πυκνή χωρική τοποθέτηση.
- Πρέπει να έχουν χαμηλό κόστος παραγωγής και να είναι αναλώσιμοι.

- Πρέπει να είναι αυτόνομοι και να λειτουργούν χωρίς παρακολούθηση.
- Πρέπει να προσαρμόζονται στο περιβάλλον που θα λειτουργούν.

Επίσης, σημαντικό περιορισμό αποτελεί η υποδομή του δικτύου, αφού τα ασύρματα δίκτυα παρουσιάζουν μια έλλειψη φυσικής υποδομής και στηρίζονται σε ένα μη ασφαλισμένο μέσο, το οποίο είναι "ανοικτό", για να μεταφέρουν τα δεδομένα τους.

Τέλος, λόγω του ότι οι κόμβοι αυτοί πολλές φορές μπορεί να εγκαθίστανται σε περιβάλλοντα τα οποία δεν είναι φιλικά, κρίνονται ευαίσθητοι σε επιθέσεις από εξωτερικούς παράγοντες. Ένας τρόπος για την προστασία των κόμβων από τέτοιες επιθέσεις είναι η χρήση υλικού που να μπορεί να παρέχει προστασία στον κόμβο, κάτι το οποίο όμως αυξάνει το κόστος δημιουργίας των κόμβων [24][25].

3.7 Λύσεις για την ασφάλεια στα ασύρματα δίκτυα αισθητήρων

Λόγω της φύσης των ασύρματων δικτύων, δύσκολα μπορούν να ληφθούν μέτρα προστασίας για την ασφάλεια τους, Μερικές λύσεις για ασφάλεια στα δίκτυα αισθητήρων, είναι είτε η αλλαγή του τρόπου με τον οποίο οι κόμβοι είναι σχεδιασμένοι, είτε η δημιουργία κάποιων βελτιωμένων πρωτοκόλλων για τα ασύρματα δίκτυα αισθητήρων.

Η πλέον κατάλληλη και διαδεδομένη λύση, για την εξυπηρέτηση της ασφάλειας σε αυτού του είδους τα δίκτυα, θεωρείται η εφαρμογή των πρωτοκόλλων. Τα κυριότερα πρωτόκολλα είναι τα εξής:

- **SPINS (Security Protocols For Sensor Networks)**

Το SPIN είναι σχεδιασμένο έτσι ώστε να ακολουθεί δύο βασικές ιδέες οι οποίες είναι:

1. Να λειτουργεί σωστά και να διατηρεί την ενέργεια των κόμβων, στέλνοντας μονάχα τα δεδομένα, τα οποία χρειάζεται ο κόμβος, και όχι ολόκληρα τα δεδομένα τα οποία ήδη έχουν οι κόμβοι και
2. Οι κόμβοι πρέπει να γνωρίζουν για την κατάσταση της ενέργειας τους ανά πάσα στιγμή, έτσι ώστε να μπορούν να προσαρμοστούν με σκοπό να παρατείνουν όσο περισσότερο την λειτουργία τους.

Ο μηχανισμός αυτός, ο οποίος ουσιαστικά βασίζεται στην διαφήμιση των υπαρχόντων δεδομένων αλλά και των αναγκών σε δεδομένα, δεν μπορεί να εγγυηθεί την παράδοση των δεδομένων, αφού μεταξύ των κόμβων οι οποίοι ζητούν κάποια πληροφορία και των κόμβων που την διαθέτουν, είναι δυνατόν να παρεμβάλλονται κόμβοι οι οποίοι δεν ενδιαφέρονται στην ουσία για τα συγκεκριμένα δεδομένα.

Τα SPINS αποτελούνται από τα πρωτόκολλα SNEP (Secure Network Encryption Protocol) και τα μTESLA (the “micro” version of the Timed, Efficient,Streaming, Loss-tolerant Authentication Protocol).

- **SNEP (Secure Network Encryption Protocol)**

Το SNEP παρέχει την εμπιστευτικότητα, την ακεραιότητα των δεδομένων και την ασφάλεια από replay attack. Με την κρυπτογράφηση μπορεί να πετύχει την εμπιστευτικότητα, ενώ με τον Κώδικα Αυθεντικοποίησης Μηνύματος (Message Authentication Code-MAC), μπορεί να πετύχει αυθεντικοποίηση και ακεραιότητα, για τους δύο τελικούς κόμβους που επικοινωνούν. Πριν από την κρυπτογράφηση του μηνύματος με μια συνάρτηση κρυπτογράφησης, ο αποστολέας εισάγει στο μήνυμα με ένα τυχαίο αριθμό.

Εκτός από τις πιο πάνω βασικές υπηρεσίες που προσφέρει το συγκεκριμένο πρωτόκολλο, παρέχει και σημασιολογική ασφάλεια, κατά την οποία γίνεται μια τέτοια κρυπτογράφηση των δεδομένων, έτσι ώστε ένας εισβολέας να μην μπορεί να έχει καμία πληροφορία για τα δεδομένα αυτά, ακόμα και αν παρουσιάζεται κρυπτογράφηση του ίδιου κομματιού. Ο τρόπος με τον οποίο αυτό επιτυγχάνεται, είναι η τυχαία κρυπτογράφηση, κατά την οποία προκύπτουν διαφορετικές κωδικοποιήσεις του ίδιου κομματιού.

- μTESLA

Το μTESLA αποτελεί μια βελτιστοποιημένη μορφή του πρωτοκόλλου TESLA, η οποία λύνει κάποια προβλήματα που παρουσιάζει το δεύτερο, προκειμένου να μπορεί να εφαρμοστεί σε ασύρματα δίκτυα. Ο λόγος για τον οποίο το αρχικό πρωτόκολλο δεν εφαρμόζεται σε δίκτυα αισθητήρων, οφείλεται στις απαιτήσεις του για μεγάλη υπολογιστική δυνατότητα και την ύπαρξη ικανοποιητικών πόρων προς εκμετάλλευση. Τα δύο αυτά πρωτόκολλα διαφέρουν στα εξής σημεία:

- Το TESLA πιστοποιεί το αρχικό πακέτο με μια ψηφιακή υπογραφή, η οποία είναι πάρα πολύ ακριβή για τους κόμβους αισθητήρων, ενώ το μTESLA χρησιμοποιεί μόνο συμμετρικούς μηχανισμούς.
- Στο TESLA, χρειάζεται να γίνεται γνωστοποίηση του κλειδιού, για κάθε πακέτο, οπότε αυτό σημαίνει ότι θα χρειαζόταν πολλή περισσότερη ενέργεια για την αποστολή και λήψη των πακέτων. Αντιθέτως, στο μTESLA, γνωστοποιείται μόνο ένα κλειδί σε κάποιο χρονικό διάστημα.

- TinySec

Το TinySec είναι η αρχιτεκτονική στο link layer για τα ασύρματα δίκτυα αισθητήρων. Αυτό είναι ελαφρύ, γενικό πακέτο ασφαλείας που μπορεί να ενσωματωθεί σε ασύρματα δίκτυα αισθητήρων εφαρμογές. Είναι ένα γενικό πακέτο για ασφάλεια το οποίο μπορεί να ενσωματωθεί σε εφαρμογές δικτύων αισθητήρων.

Μοιάζει με το SNEP και κάπου το συμπληρώνει. Συγκεκριμένα, παρέχει εμπιστευτικότητα, αυθεντικοποίηση και ακεραιότητα των δεδομένων, όπως επίσης και εγγύηση όταν δεν θα υπάρχει αναμετάδοση παλαιότερων πακέτων.

Η βασική διαφορά του με το SNEP, είναι ότι σε αυτή την περίπτωση δεν παρουσιάζονται καθόλου μετρητές.

Η επεξεργασία των δεδομένων στα ασύρματα δίκτυα αισθητήρων, όπως είναι για παράδειγμα οι εξάλειψη αντιγράφων, γίνεται εντός του δικτύου, έτσι ώστε να γίνεται εξοικονόμηση ενέργειας, προτού τα πακέτα αυτά να μεταδοθούν προς τον τελικό προορισμό που βρίσκεται εκτός του δικτύου.

Όσον αφορά όμως τους μηχανισμούς για ασφάλεια στα άκρα του δικτύου, μεταξύ των εσωτερικών κόμβων και του τελικού προορισμού, δεν μπορούν να εγγυηθούν αυθεντικοποίηση, εμπιστευτικότητα και ακεραιότητα των μηνυμάτων, εφόσον οι μηχανισμοί αυτοί είναι εκτεθειμένοι σε άλλες εξωτερικές επιθέσεις [26][27].

Στην περίπτωση λοιπόν όπου ο έλεγχος της ακεραιότητας των μηνυμάτων γίνεται μόνο όταν φτάσουν στον τελικό τους προορισμό, τότε είναι πολύ πιθανόν τα πακέτα που λαμβάνονται από αυτόν, να είναι "μολυσμένα" από κάποιον εισβολέα. Στην περίπτωση αυτή, θα μπορούσε ο οποιοσδήποτε να αλλοιώσει τα πακέτα, μερικά hops προηγουμένως, χωρίς αυτό να γίνει αντιληπτό. Οι συνέπειες αυτής της ενέργειας θα ήταν η σπατάλη ακόμα περισσότερης ενέργειας και bandwidth.

Οπότε μια αρχιτεκτονική για ασφάλεια στο επίπεδο της σύνδεσης, θα πρέπει να μπορέσει να ανιχνεύσει πακέτα τα οποία έχει παρεμβάλει ή αλλοιώσει κάποιος άλλος. Το TinySec, παρέχει τις βασικές αρχές ασφάλειας για την αυθεντικοποίηση και ακεραιότητα των μηνυμάτων, όπως επίσης και εμπιστευτικότητα, σημασιολογική ασφάλεια και προστασία από την αναμετάδοση πακέτων.

- LEAP: Localized Encryption And Authentication Protocol

Το πρωτόκολλο αυτό, είναι ένα βασικό πρωτόκολλο διαχείρισης στα δίκτυα αισθητήρων, το οποίο είναι σχεδιασμένο για την υποστήριξη της ενδοδίκτυας

επεξεργασίας και παρέχει ασφαλισμένη επικοινωνία στα δίκτυα αισθητήρων. Παρέχει τις βασικές υπηρεσίες για ασφάλεια όπως η αυθεντικοποίηση και η εμπιστευτικότητα.

Τα μηνύματα που ανταλλάσσονται μεταξύ διαφορετικών κόμβων, έχουν και διαφορετικές απαιτήσεις σε θέμα ασφάλειας, γι ’αυτό και ο σχεδιασμός του πρωτοκόλλου αυτού, επηρεάζεται. Σύμφωνα με το πιο πάνω λοιπόν, ότι δηλαδή δεν μπορεί να υπάρξει ένας μόνο μηχανισμός ενιαίου κλειδιού ο οποίος να μπορέσει να προστατεύσει όλες τις επικοινωνίες μέσα στο δίκτυο, το πρωτόκολλο LEAP υποστηρίζει την εγκαθίδρυση τεσσάρων τύπων κλειδιών, για κάθε κόμβο αισθητήρα.

Υπάρχει λοιπόν ένα κλειδί το οποίο είναι κοινό με τον τελικό παραλήπτη (base station), ένα ζεύγος κλειδιών όπου παίρνει ο ένας κόμβος το ένα και δίνει το άλλο σε κάποιον άλλο αισθητήρα, ένα κλειδί που είναι κοινό για μια ολόκληρη ομάδα από πολλαπλούς κόμβους γείτονες και τέλος ένα κλειδί επίσης για μια ομάδα, το οποίο είναι κοινό για όλους τους κόμβους μέσα σε ολόκληρο το δίκτυο [26][27].

Κεφάλαιο 4

Περιβάλλον Εργασίας

4.1 Contiki OS

Στην παρούσα διπλωματική εργασία, για την υλοποίηση ασύρματων δικτύων με αισθητήρες και επιθέσεις σε αυτά, έγινε χρήση του Contiki 2.5 το οποίο είναι ένα ανοικτού τύπου λειτουργικό σύστημα για δικτυωμένες συσκευές περιορισμένης μνήμης.

Το εν λόγω σύστημα είναι γραμμένο σε C γλώσσα προγραμματισμού και τρέχει πάνω σε μια ποικιλία από πλατφόρμες που συμπεριλαμβάνουν μικροελεγκτές όπως είναι ο MSP430 και το AVR, μέχρι και κανονικούς προσωπικούς υπολογιστές σε περιβάλλον Ubuntu. Αξίζει να σημειωθεί πως ό,τι κώδικας γραφτεί για το Contiki μπορεί να χρησιμοποιηθεί ακριβώς ο ίδιος και στους αισθητήρες χωρίς οποιεσδήποτε αλλαγές.

Το Contiki μπορεί να χρησιμοποιηθεί σε ένα μεγάλο αριθμό συστημάτων όπως είναι η βιομηχανική παρακολούθηση, συστήματα συναγερμού, απομακρυσμένη παρακολούθηση ενός σπιτιού κτλ. Είναι σχεδιασμένο για μικρές συσκευές, οι οποίες λειτουργούν με χαμηλή κατανάλωση ενέργειας και έχουν μια μικρή ποσότητα μνήμης.

Οι τυπικοί αισθητήρες είναι εφοδιασμένοι με 8-bit μικροελεγκτές, με μνήμη κώδικα 100kilobytes και με μνήμη RAM, λιγότερη από 20kilobytes.

Το Contiki περιέχει 2 στοίβες επικοινωνίας οι οποίες είναι η uIP και Rime.
Η uIP TCP/IP στοίβα, παρέχει στο Contiki την δυνατότητα επικοινωνίας με το Διαδίκτυο, μέσω της TCP/IP στοίβας πρωτοκόλλων. Η uIP είναι μικρή και απλή, και της οποίας οι peers επίσης δεν έχουν πολύπλοκες στοίβες, μπορεί όμως να υπάρξει επικοινωνία με peers οι οποίοι τρέχουν μια παρόμοια "ελαφριά" στοίβα. Όσο αφορά το μέγεθος του κώδικα, είναι μερικά kilobytes, ενώ η χρήση της RAM είναι πολύ χαμηλή.

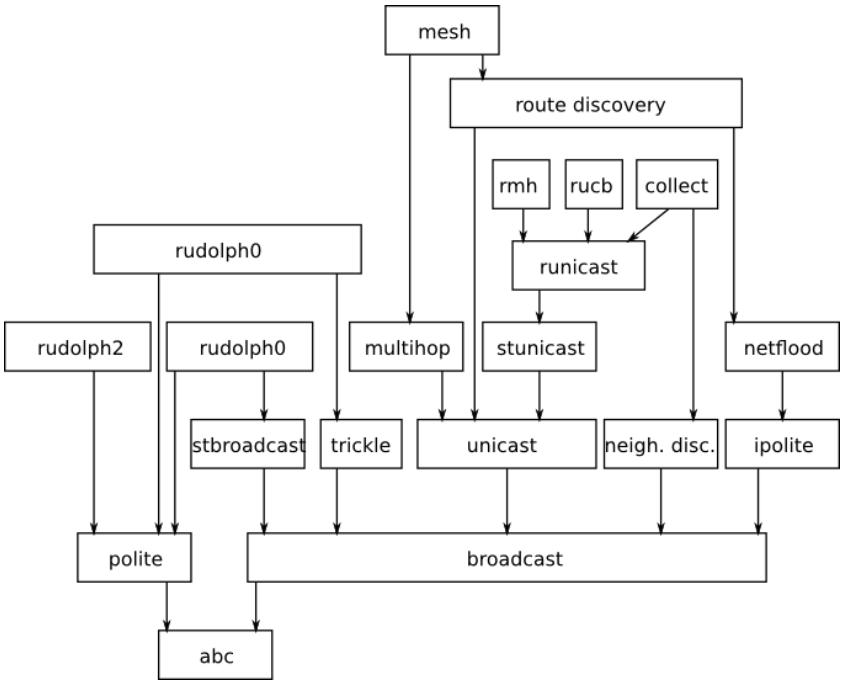
Η uIP είναι γραμμένη σε C γλώσσα προγραμματισμού, είναι υλοποιημένη για να έχει μόνο τα βασικά χαρακτηριστικά, τα οποία χρειάζονται για μια πλήρη TCP/IP στοίβα και περιέχει τα πρωτόκολλα IP, ICMP, UDP και TCP.

Μπορεί να τρέξει σαν μια διεργασία σε ένα σύστημα το οποίο μπορεί να εκτελεί πολλαπλές διεργασίες παράλληλα, ή σαν ένα βασικό πρόγραμμα σε ένα σύστημα το οποίο μπορεί να τρέξει μόνο μια διεργασία. Και στις δύο περιπτώσεις, ο βασικός σκοπός είναι να γίνεται έλεγχος αν ένα πακέτο έχει φτάσει από το δίκτυο και αν έχει προκύψει λήξη του χρόνου.

Η στοίβα Rime, είναι μια "ελαφριά" στοίβα επικοινωνίας σχεδιασμένη για να υποστηρίζει απλές λειτουργίες, όπως είναι η αποστολή ενός μηνύματος σε όλους τους γείτονες, ή σε ένα συγκεκριμένο γείτονα. Μπορεί επίσης να υποστηρίζει και πιο πολύπλοκους μηχανισμούς, όπως είναι η "πλημμύρα" του δικτύου (network flooding). Τα πρωτόκολλα στην στοίβα Rime, είναι διατεταγμένα με ένα πολυεπίπεδο τρόπο όπου τα περισσότερο πολύπλοκα πρωτόκολλα είναι υλοποιημένα με πρωτόκολλα λιγότερο πολύπλοκα.

Για την Rime στοίβα, έχουν επιλεχθεί αρχέτυποι τύποι επικοινωνίας, σύμφωνα με τα πρωτόκολλα που χρησιμοποιεί ένα δίκτυο αισθητήρων, οι οποίοι μπορεί να είναι ενός ή πολλαπλών hops.

Πρωτόκολλα ή εφαρμογές που τρέχουν πάνω από την Rime στοίβα, μπορούν να υλοποιήσουν επιπρόσθετα πρωτόκολλα τα οποία δεν βρίσκονται μέσα στην στοίβα [28][29].



Εικόνα 4.1: Στοίβα Rime [33]

Επεξηγηματικά με την πιο πάνω εικόνα, έχουμε τα εξής σημεία:

- ABC: η ανώνυμη εκπομπή, που απλά στέλνει ένα πακέτο μέσω του radio driver, παραλαμβάνει όλα τα πακέτα από αυτό και τα περνά στο ανώτερο στρώμα.
- Broadcast: μετάδοση με ταυτότητα, προσθέτει τη διεύθυνση αποστολέα προς τον εξερχόμενο πακέτο και περνά το πακέτο αυτό στο ABC.
- Unicast: Η ενότητα αυτή προσθέτει μια διεύθυνση προορισμού για τα πακέτα περνούν στο broadcast block. Από την πλευρά λήψης, αν η διεύθυνση προορισμού του πακέτου δεν ταιριάζει με τη διεύθυνση του κόμβου, το πακέτο απορρίπτεται.
- Stunicast: Όταν του ζητηθεί να στείλει ένα πακέτο σε κάποιο κόμβο, το στέλνει επανειλημμένα για ένα δεδομένο χρονικό διάστημα έως ότου ζήτηθει να σταματήσει. Η ενότητα αυτή συνήθως δεν χρησιμοποιείται ως έχει, αλλά χρησιμοποιείται από την πίο κάτω.
- Runicast: Η αξιόπιστη unicast, στέλνει ένα πακέτο χρησιμοποιώντας την ενότητα stunicast περιμένοντας για ένα πακέτο επιβεβαίωσης. Όταν το λάβει σταματά την συνεχή μετάδοση του πακέτου.Ο μέγιστος αριθμός αναμετάδοσης πρέπει να διευκρινίζεται, προκειμένου να αποφευχθεί η άπειρη αποστολή.
- Polite και ipolite: Οι δύο αυτές ενότητες είναι σχεδόν ταυτόσημες, όταν ένα πακέτο πρέπει να αποστέλλεται σε ένα συγκεκριμένο χρονικό διάστημα, η ενότητα περιμένει για το ήμισυ του χρόνου, ελέγχοντας εάν έχει λάβει το ίδιο πακέτο που πρεπει να στείλει. Αν είναι το ίδιο, το πακέτο δεν αποστέλλεται, ειδάλλως το αποστέλλει. Αυτό είναι χρήσιμο για τεχνικές πλημμύρες για να αποφεύγονται οι περιττές αναμεταδόσεις.
- Multihop: Η ενότητα αυτή απαιτεί μια λειτουργία πίνακα δρομολογιών, και όταν πρόκειται να στείλει ένα πακέτο ελέγχει τον πίνακα αυτό για να βρεί την σωστή διαδρομή για το επόμενο hop και στέλνει το πακέτο σε αυτό χρησιμοποιώντας unicast. Όταν λαμβάνει ένα πακέτο, αν ο κόμβος είναι ο προορισμός τότε το πακέτο περνά στο άνω στρώμα, διαφορετικά ζητά πάλι τον πίνακα διαδρομή για την επόμενη αναμετάδοση του πακέτου.

4.2 Εργαλείο προσομοίωσης Cooja

Η ρύθμιση μεγάλων δικτύων σε φυσικούς κόμβους, μπορεί να δημιουργήσει μια πρόκληση, ως εκ τούτου, η χρήση ενός προσομοιωτής για την ανάπτυξη και δοκιμή των συστημάτων μπορεί να είναι αρκετά χρήσιμη. Οι προσομοιωτές μπορούν να επιτρέπουν

τον έλεγχο σε μεγάλα δίκτυα, ενώ επίσης είναι σε θέση να εκτελούν τα καθήκοντά τους με μεγαλύτερες ταχύτητες από ό, τι σε πραγματικό χρόνο. Το Cooja**,** είναι ένας προσομοιωτής που παρέχεται από το Contiki, που αντίθετα με τους περισσότερους προσομοιωτές επιτρέπει την δημιουργία δικτύων οποιουδήποτε μεγέθους, από Contiki motes, και στην συνέχεια γίνεται μια προσομοίωση του δικτύου, σε επίπεδο υλικού.

Ο προσομοιωτής Cooja βρίσκεται στο μονοπάτι Contiki 2-5/ tools /Cooja. Χρησιμοποιεί ένα συνδυασμό κώδικα Java για το front-end interface και ειδικής πλατφόρμας εξομοιωτές για την εκτέλεση των προσομοιώσεων [30].

Η προσομοίωση σε επίπεδο υλικού είναι μεν πολύ πιο αργή, όμως επιτρέπει ακριβή έλεγχο της συμπεριφοράς του συστήματος.

Βέβαια υπάρχει και η δυνατότητα προσομοίωσης η οποία δίνει λιγότερες πληροφορίες με μεγαλύτερη ταχύτητα, επιτρέποντας έτσι προσομοιώσεις δικτύων μεγαλύτερου μεγέθους.

Οι προσομοιώσεις που γίνονται με το Cooja εξυπηρετούν στην αξιολόγηση του κώδικα πριν αυτός χρησιμοποιηθεί για τον τελικό σκοπό [29].

Κεφάλαιο 5
Υλοποίηση Επιθέσεων και Εξαγωγή Αποτελεσμάτων

5.1 Εισαγωγή

Μετά την μελέτη ορισμένων από τους πιο πάνω ιούς, στην εργασία αυτή υλοποιήθηκε ο Sybil ιός σε δύο διαφορετικές μορφές. Οι επιθέσεις αυτές υλοποιήθηκαν και προσομοιώθηκαν με την βοήθεια του λειτουργικού συστήματος Contiki χρησιμοποιώντας το εργαλείο Cooja.

Μέσω των πολλών προσομοιώσεων, απώτερος σκοπός ήταν η εξαγωγή αποτελεσμάτων όταν σε ένα δίκτυο υπάρχουν μολυσμένοι κόμβοι. Με αυτό τον τρόπο, είναι δυνατόν πλέον, να βρεθούν ευκολότερα τρόποι αντιμετώπισης των συγκεκριμένων ιών.

Έπειτα, παρουσιάζονται τα αποτελέσματα και τα συμπεράσματα που προέκυψαν κατά την προσομοίωση των ιών αυτών, με την δημιουργία κατάλληλων γραφικών παραστάσεων. Αρχικά παρουσιάζεται ο ιός Sybil-stolen identities ενώ στη συνέχεια ο ιός Sybil-fabricated identities.

Στο σημείο αυτό πρέπει να σημειωθεί πως για σκοπούς υλοποίησης του αλγορίθμου υποθέτουμε πως ο τελικός παραλήπτης είναι πάντα ο sink (αισθητήρας με rime address 1.0 και mac address 01:00:00:00:00:00:00:00). Επίσης θεωρούμε ως γείτονες τους κόμβους που καλύπτει στην περιοχή του. Τέλος, αξίζει να σημειωθεί ότι όλα τα σενάρια εκτελέστηκαν από 10 φορές το κάθε ένα για 15 λεπτά.

Όσον αφορά την δρομολόγηση των πακέτων, έγινε χρήση ενός αλγορίθμου προηγούμενης εργασίας, του Weighted Shortest Path, ο οποίος ήταν μια τροποποίηση του κώδικα του αρχείου example-multihop.c. Το αρχείο αυτό βρίσκεται στο φάκελο examples/rime του Contiki 2.5 και τροποποιήθηκε και για την δημιουργία των επιθέσεων.

Σύμφωνα τώρα με αυτό τον αλγόριθμο δρομολόγησης ένας αισθητήρας για να αποφασίσει σε ποιο γείτονα του θα προωθεί το πακέτο, θα λαμβάνει υπόψη την απόσταση του εκάστοτε γείτονα από τον τελικό παραλήπτη (αριθμός hops) καθώς και το RSSI μεταξύ του εκάστοτε γείτονα και του αισθητήρα.

Συγκεκριμένα, γίνεται έλεγχος του πίνακα γειτόνων κάθε αισθητήρα και από εκεί επιλέγεται η προώθηση του πακέτου στο γείτονα που βρίσκεται πιο κοντά στο sink, δηλαδή τον γείτονα με τον μικρότερο αριθμό hops. Στην περίπτωση εύρεσης γειτόνων με ίδιο αριθμό hops, ελέγχεται το RSSI και επιλέγεται αυτός με το μεγαλύτερο.

5.2 Βηματική περιγραφή

Sink Node

- Καθορισμός Rime Address και MAC Address
- Κλήση συναρτήσεων από αρχεία CSMA και Contiki Mac
- Έλεγχος συχνότητας κόμβου
- Δέσμευση χώρου για πίνακα γειτόνων
- Άνοιγμα Multi-hop connection
- Δέχεται ανακοινώσεις από γειτονικούς κόμβους και τους κατατάσσει στον πίνακα γειτόνων
- Λήψη πακέτων και αύξηση μετρητή

Benign Node

- Καθορισμός Rime Address και MAC Address
- Κλήση συναρτήσεων από αρχεία CSMA και Contiki Mac
- Έλεγχος συχνότητας κόμβου
- Δέσμευση χώρου για πίνακα γειτόνων
- Άνοιγμα Multi-hop connection
- Αποτυχημένες προσπάθειες αποστολής πακέτων μιας και δεν υπάρχουν ακόμη γείτονες στο πίνακα του
- Δέχεται ανακοινώσεις από γειτονικούς κόμβους και τους κατατάσσει στον πίνακα γειτόνων
- Αποστολή πακέτων με χρήση αλγορίθμου βάση μικρότερου αριθμού hops ή μεγαλύτερο RSSI

- Λήψη πακέτων και αύξηση μετρητή

Malicious Node

- Καθορισμός Rime Address και MAC Address
- Κλήση συναρτήσεων από αρχεία CSMA και Contiki Mac
- Έλεγχος συχνότητας κόμβου
- Δέσμευση χώρου για πίνακα γειτόνων
- Άνοιγμα Multi-hop connection
- Αποτυχημένες προσπάθειες αποστολής πακέτων μιας και δεν υπάρχουν ακόμη γείτονες στο πίνακα του
- Δέχεται ανακοινώσεις από γειτονικούς κόμβους και τους κατατάσσει στον πίνακα γειτόνων
- Κλοπή τυχαίας ταυτότητας από αυτούς ή δημιουργία μιας αυθαίρετης νέας ταυτότητας
- Λήψη πακέτων που προορίζονταν για τους κόμβους που τους έχει κλαπεί η ταυτότητα (Sybil Nodes) και αύξηση μετρητή
- Συμπεριφέρεται σαν τους Sybil Nodes

5.3 Sybil- Stolen ID

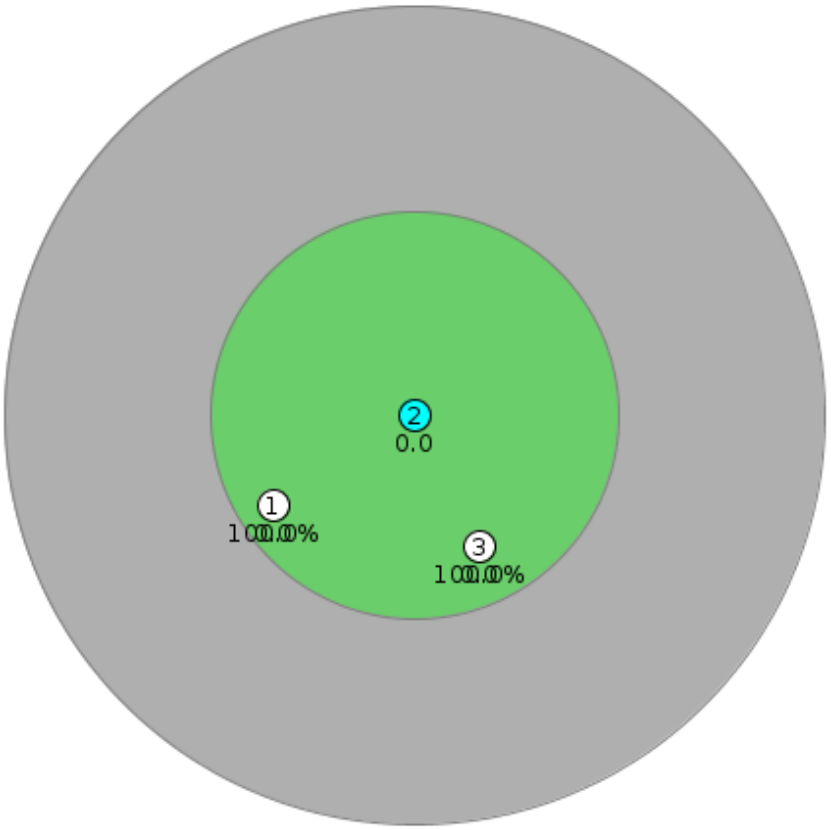
Η υλοποίηση του ιού αυτού, έγινε με βάση τον έτοιμο από προηγούμενη εργασία κώδικα, που υλοποιούσε τον ιό Sink Hole. Οι διαφοροποιήσεις που έγιναν, αφορούσαν τα κύρια χαρακτηριστικά του ιού, δηλαδή ότι έπρεπε να παίρνει πλαστές ταυτότητες και να προωθεί τα πακέτα αντί να τα πετά. Συγκεκριμένα, για τον ιό Sybil- Stolen ID, ετοιμαζόταν ο πίνακας γειτόνων του κακόβουλου κόμβου, στον οποίο κατατάσσονταν όσοι κόμβοι ήταν στην εμβέλεια του. Από τον πίνακα αυτό, ο κακόβουλος αισθητήρας, έπαιρνε μια τυχαία ταυτότητα και την παρουσίαζε σαν δική του. Αυτό έγινε με την χρήση της Random βιβλιοθήκης και της εντολής random_rand(). Έπειτα, χρησιμοποιήθηκε η συνάρτηση forward, μέσω της οποίας ο κακόβουλος κόμβος, προωθούσε τα πακέτα που παραλάμβανε, αλλά με την κλοπιμαία ταυτότητα.

Οι γραφικές οι οποίες εμφανίζονται παρακάτω, παρουσιάζουν τα αποτελέσματα τα οποία προκύπτουν από ένα δίκτυο, του οποίου οι κόμβοι μολύνονται από ένα ιό Sybil στη

μορφή του Stolen ID. Στην υλοποίηση που έγινε στην παρούσα διπλωματική εργασία, ανά πάσα στιγμή ο κάθε κακόβουλος κόμβος μπορεί να υποκλέψει μόνο μια ταυτότητα.

Σκοπός του ιού αυτού, είναι να ξεγελά τους υπόλοιπους νόμιμους κόμβους του δικτύου παρουσιάζοντας τους μια άλλη ταυτότητα από την πραγματική του, με σκοπό να αποστέλλουν σε αυτό πακέτα τα οποία θα έστελναν στον κόμβο με την πραγματική ταυτότητα που συνάδει με αυτή που έχει αντιγράψει.

Τοπολογία 5.3.1

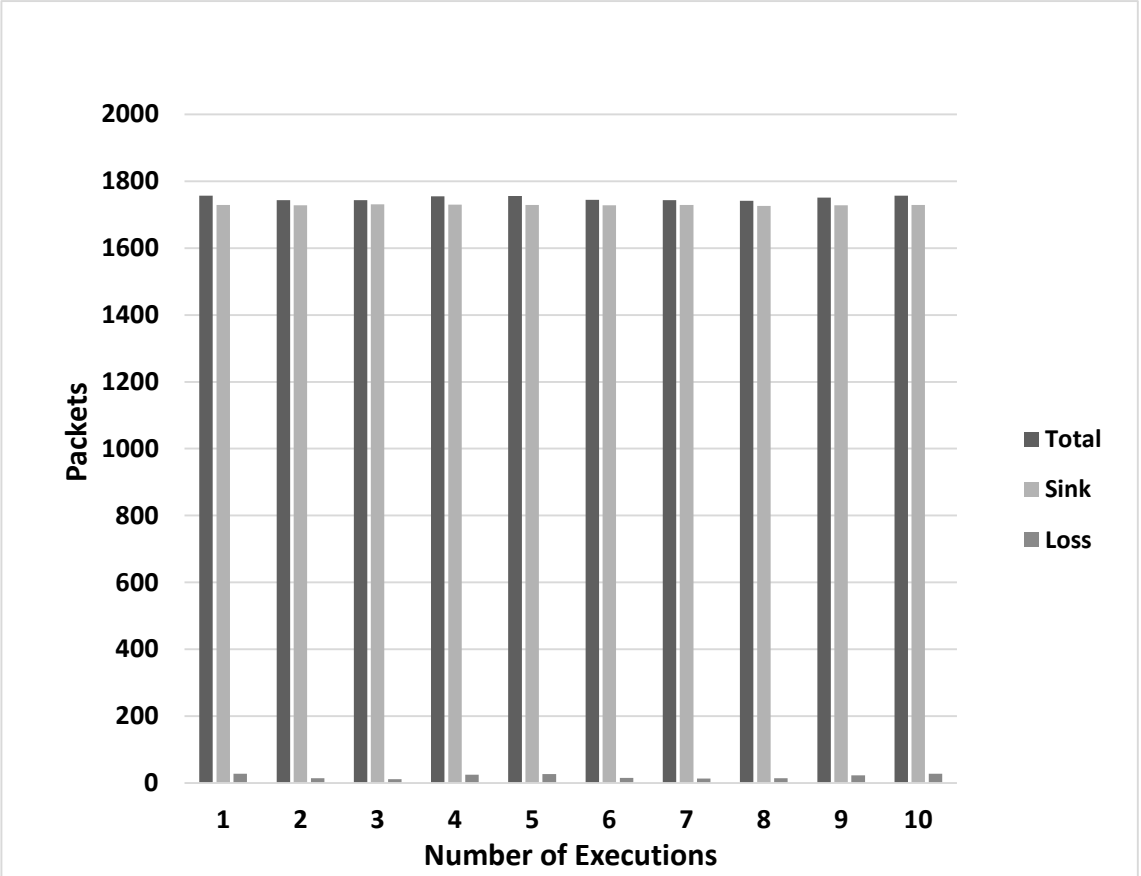


Σενάριο 5.3.1

3 Benign – 0 Malicious Nodes

Τοπολογία 5.3.1

Συνολικά πακέτα που στάλθηκαν	**Πακέτα που παραλήφθηκαν από Sink**	**Πακέτα που χάθηκαν**
1757	1729	28
1743	1728	15
1743	1731	12
1755	1730	25
1756	1729	27
1744	1728	16
1743	1729	14
1741	1726	15
1751	1728	23
1757	1729	28

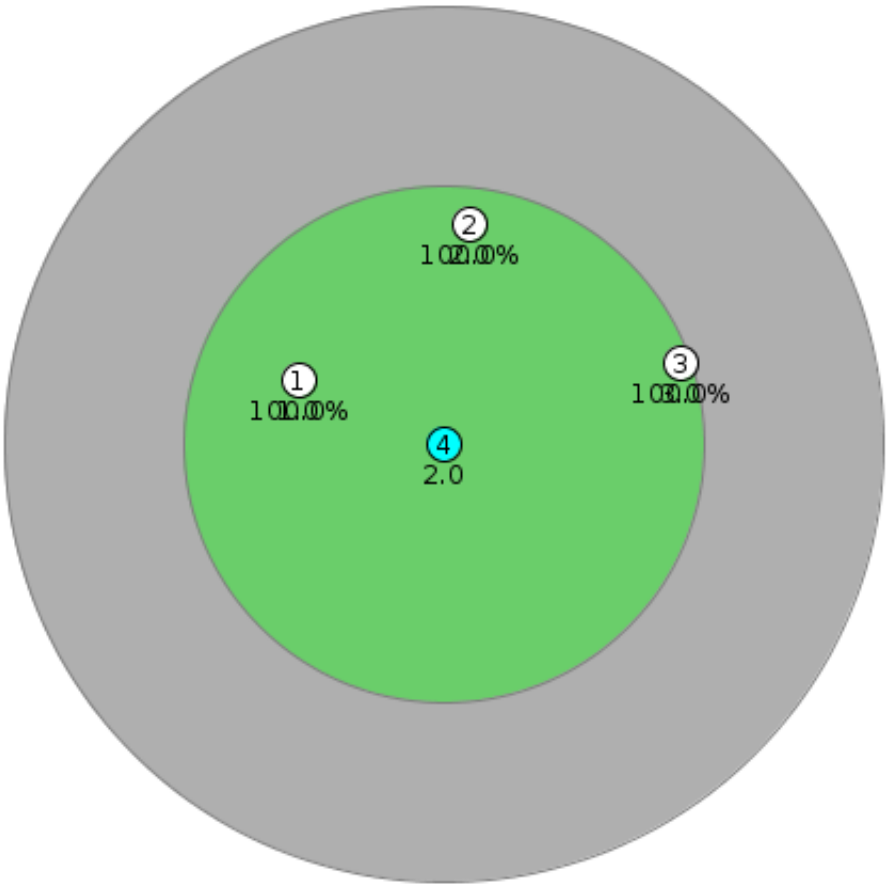


Σε αυτό το σενάριο όλοι οι κόμβοι είναι υγιείς. Από την γραφική παράσταση, παρατηρείται πως ο αριθμός των πακέτων που στέλνουν οι κόμβοι σε κάθε μια από τις 10 εκτελέσεις της προσομοίωσης κυμαίνεται στις ίδιες τιμές και είναι περίπου γύρω στα 1745 πακέτα.

Ο κόμβος με τον αριθμό 1, ο οποίος είναι και ο τελικός παραλήπτης(sink node), παραλαμβάνει τα πακέτα που φτάνουν σε αυτόν, αλλά δεν είναι σε θέση να στείλει.

Παρατηρούμε ότι, υπάρχουν κάποιες απώλειες πακέτων μέσα στο δίκτυο οι οποίες όμως είναι αμελητέες και έτσι, σχεδόν όσα πακέτα αποστέλνονται μέσα στο δίκτυο, τόσα περίπου παραλαμβάνονται και από τον τελικό παραλήπτη (sink node).

Τοπολογία 5.3.2

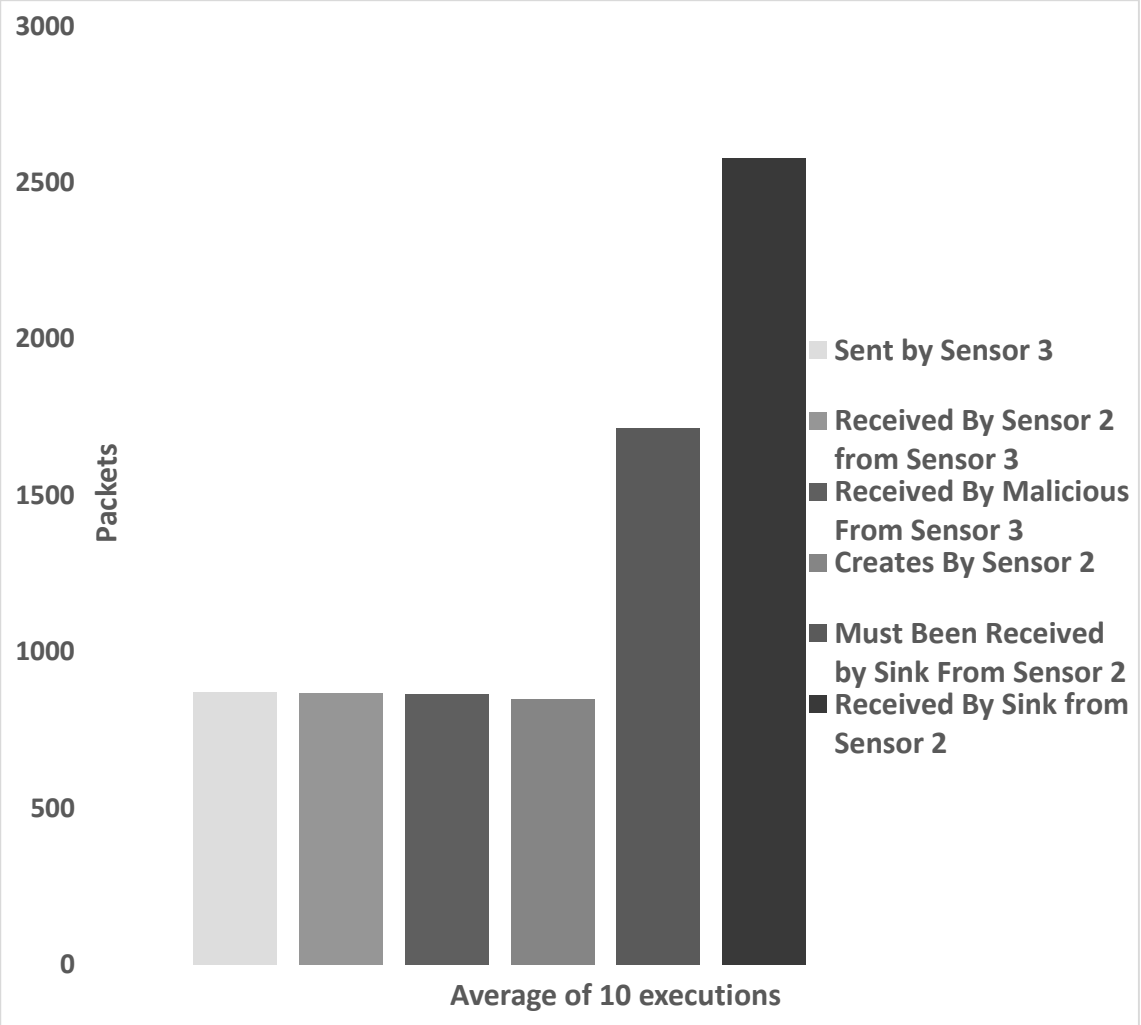


Τοπολογία 5.3.2

3 Benign – 1 Malicious Nodes

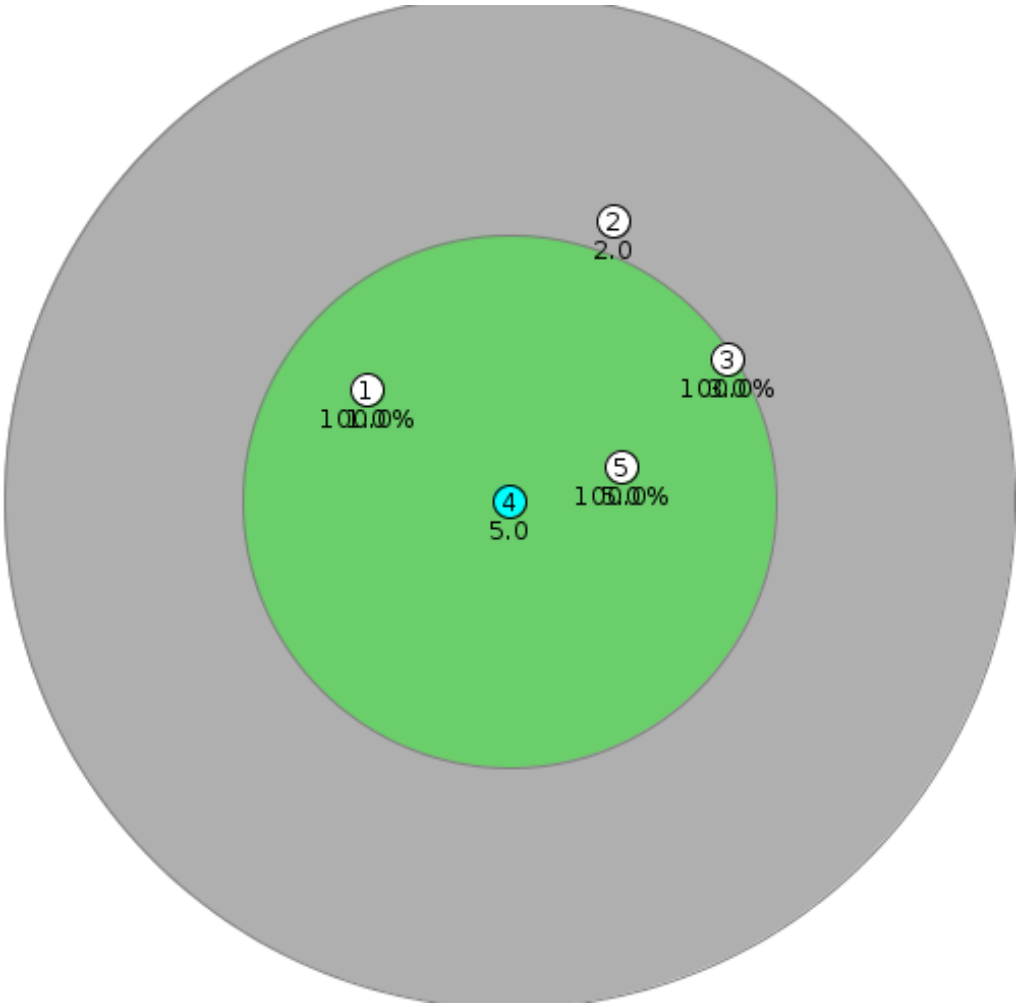
Σενάριο 5.3.2

	Packets sent by Sensor 3	Packets Received by Sensor 2 from Sensor 3	Packets Received By Malicious	Packets Created By Sensor 2	Total Packets must been received by sink from Sensor 2	Packets Received By Sink From Sensor 2
	872	870	870	858	1728	2578
	870	870	870	845	1715	2579
	868	868	848	847	1715	2580
	866	864	848	844	1708	2576
	870	870	870	845	1715	2578
	872	870	870	846	1716	2578
	868	866	865	844	1710	2578
	869	868	866	848	1716	2579
	868	865	864	848	1713	2578
	869	866	865	847	1713	2578
AVG	870	868	863	847	1715	2578



Παρατηρούμε ότι στην πιο πάνω τοπολογία, ο κακόβουλος αισθητήρας, κλέβει την ταυτότητα του αισθητήρα 2 και έτσι όσα πακέτα αποστέλνονταν στο αισθητήρα 2 από τον αισθητήρα 3, τα παραλάμβανε και ο κακόβουλος. Ο αισθητήρας 2 αποστέλλει στον sink και κάποια δικά του πέραν από αυτά που του έστειλε ο αισθητήρας 3, αλλά ταυτόχρονα, ο κακόβουλος στέλνει και αυτός στον sink όσα παρέλαβε από τον 3, με την ταυτότητα του αισθητήρα 2.Αποτέλεσμα αυτού, είναι να παραλαμβάνει ο sink διπλάσια ποσότητα πακέτων που στάλθηκαν από τον 2, νομίζοντας ότι όλα τα παραλαμβάνει από τον μη- μολυσμένο κόμβο 2.

Τοπολογία 5.3.3

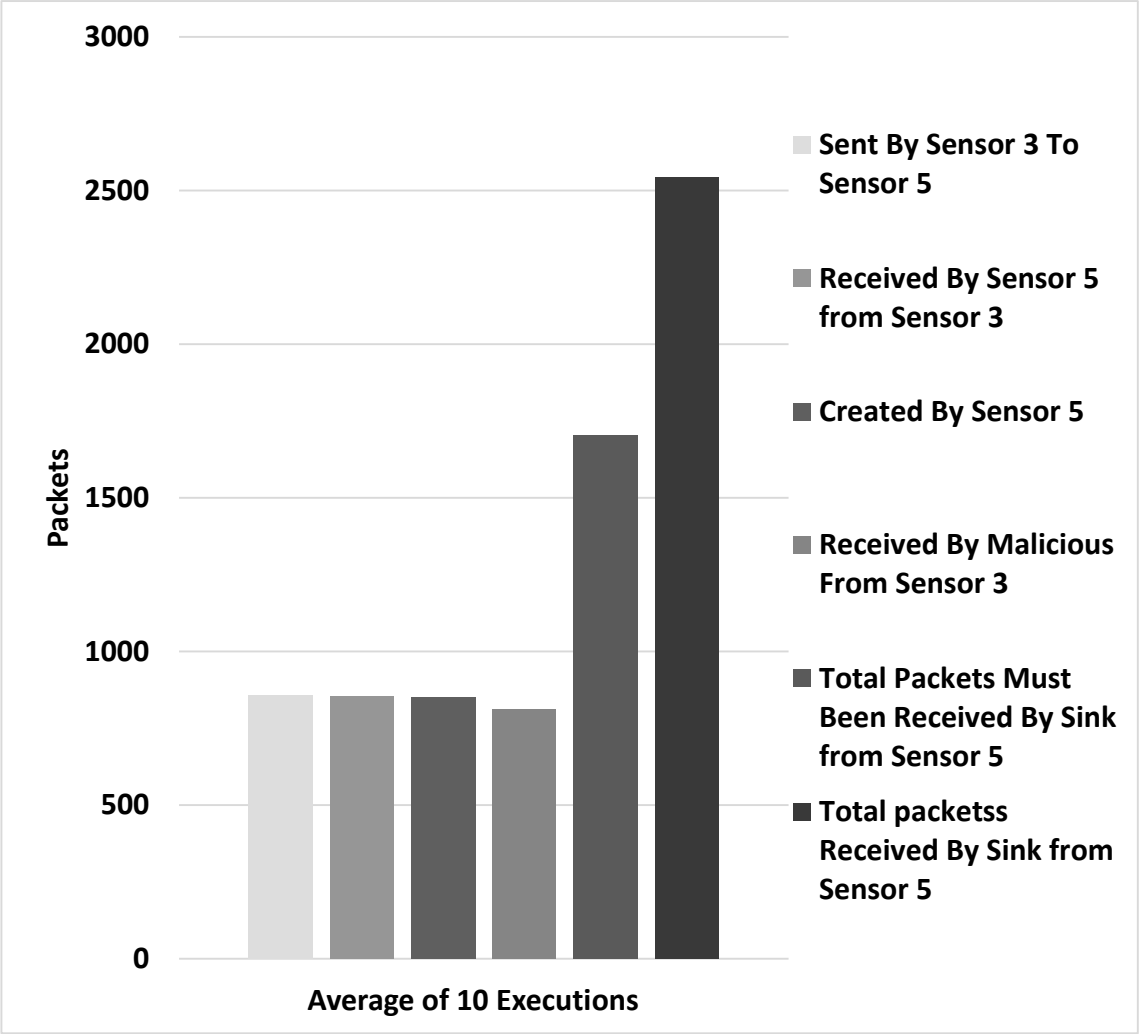


Σενάριο 5.3.3

2 Benign – 1 Malicious Nodes

Τοπολογία 5.3.3

	Packets sent by Sensor 3	Packets Received by Sensor 5 from Sensor 3	Packets Created By Sensor 5	Packets Received By Malicious	Total Packets must been received by sink from Sensor 5	Packets Received By Sink From Sensor 5
	858	848	846	843	1694	2530
	858	855	846	806	1701	2556
	857	856	850	805	1706	2543
	858	856	850	805	1706	2550
	857	856	846	806	1702	2555
	858	856	855	806	1711	2543
	858	848	846	803	1694	2536
	857	853	855	830	1708	2544
	856	855	846	808	1701	2545
	858	853	853	810	1706	2538
AVG	858	854	850	812	1703	2544



Σε αυτή τη γραφική, παρατηρούμε ότι και στην προηγούμενη, με την διαφορά ότι τώρα υπάρχουν περισσότεροι νόμιμοι κόμβοι στο δίκτυο και ότι ο κακόβουλος μπορούσε να παραλάβει πακέτα μόνο από τον αισθητήρα 3, αφού από τον αισθητήρα 5 δεν μπορούσε μιας και κανένας κόμβος δεν στέλνει πακέτα στον εαυτό του.

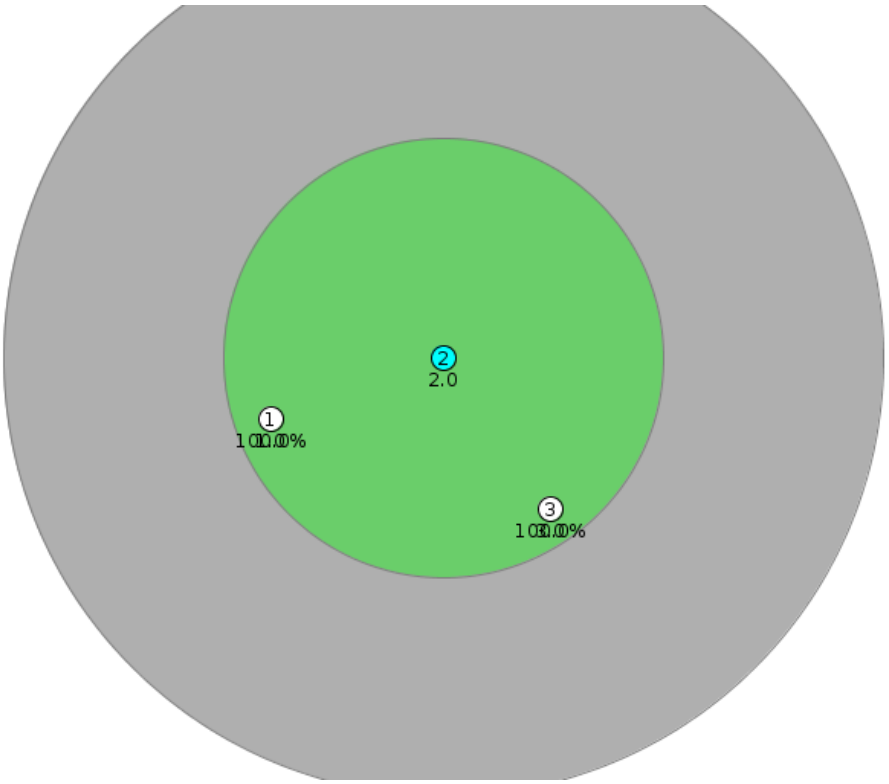
5.4 Sybil- Fabricated ID

Οι γραφικές οι οποίες εμφανίζονται παρακάτω, παρουσιάζουν τα αποτελέσματα τα οποία προκύπτουν από ένα δίκτυο, του οποίου οι κόμβοι μολύνονται από ένα ιό Sybil στη μορφή του Fabricates ID.

Οι κόμβοι οι οποίοι είναι μολυσμένοι από τον συγκεκριμένο ιό, δημιουργούν νέες τυχαίες ταυτότητες και τις παρουσιάζουν σαν δικές τους. Σκοπός του ιού αυτού, είναι να ξεγελά τους υπόλοιπους νόμιμους κόμβους του δικτύου παρουσιάζοντας τους μια άλλη ταυτότητα από την πραγματική του, με σκοπό να αποστέλλουν σε αυτό πακέτα τα οποία θα έστελναν στον κόμβο με την πραγματική ταυτότητα που συνάδει με αυτή που έχει αντιγράψει, όπως γίνεται και στη πιο πάνω μορφή του.

Η υλοποίηση του ιού αυτού, έγινε με βάση τον έτοιμο από προηγούμενη εργασία κώδικα, που υλοποιούσε τον ιό Sink Hole, όπως προαναφέρεται και για τον ιό. Sybil-Stolen ID. Οι διαφοροποιήσεις που έγιναν, αφορούσαν τα κύρια χαρακτηριστικά του ιού, δηλαδή ότι έπρεπε να παίρνει πλαστές ταυτότητες και να προωθεί τα πακέτα αντί να τα πετά. Συγκεκριμένα, για τον ιό, έγινε χρήση της Random βιβλιοθήκης και της εντολής random_rand(), μέσω της οποίας δημιουργείται κάθε φορά νέα ταυτότητα η οποία μπορεί να έχει μια αυθαίρετη τιμή, είτε ήδη υπάρχουσα σε κάποιο άλλο κόμβο, είτε εντελώς τυχαία, στο εύρος τω τιμών 1-10. Έπειτα, χρησιμοποιήθηκε η συνάρτηση forward, μέσω της οποίας ο κακόβουλος κόμβος, προωθούσε τα πακέτα που παραλάμβανε, αλλά με την κλοπιμαία ταυτότητα.

Τοπολογία 5.4.1

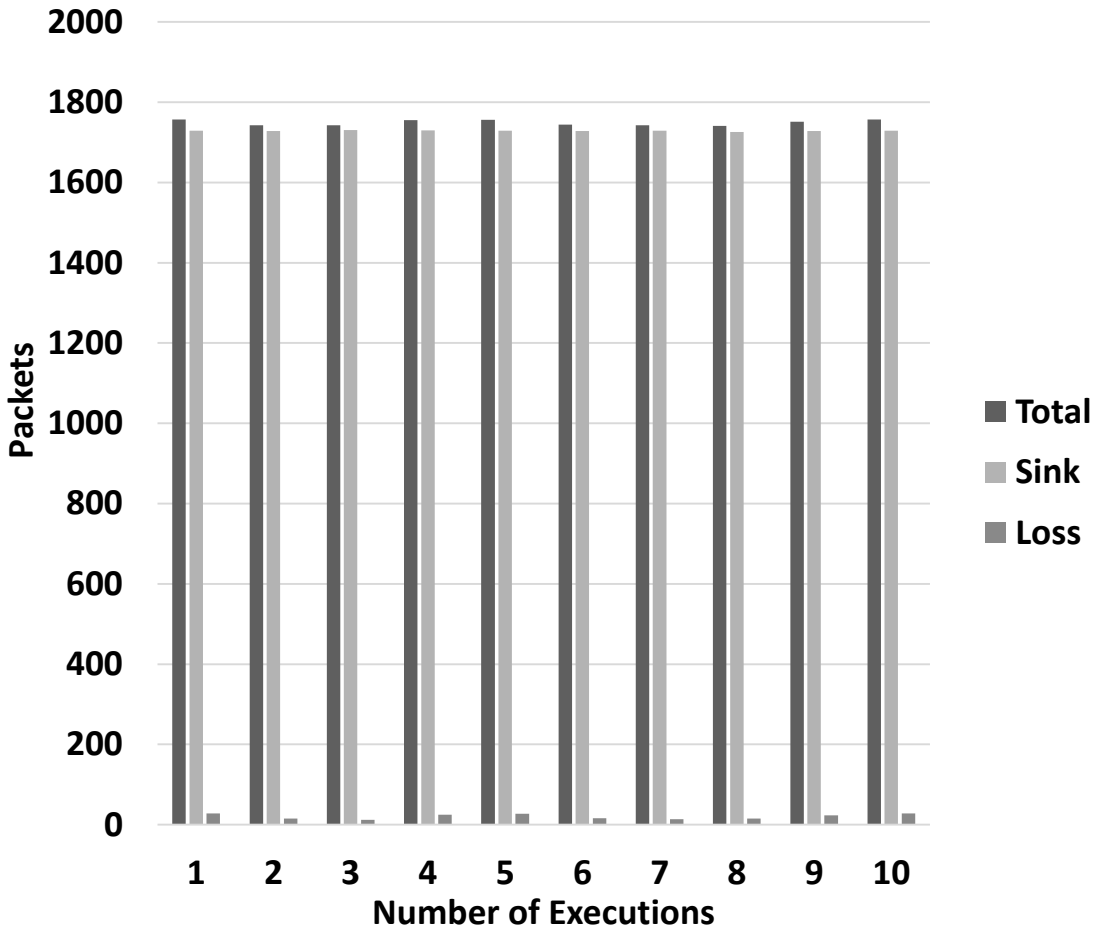


Σενάριο 5.4.1

3 Benign – 0 Malicious Nodes

Τοπολογία 5.4.1

Total Packets Sent	**Packets Received By Sink**	**Loss**
1744	1733	11
1742	1731	11
1744	1727	14
1744	1727	14
1740	1730	10
1745	1733	12
1745	1731	14
1744	1727	14
1740	1730	10
1744	1733	11



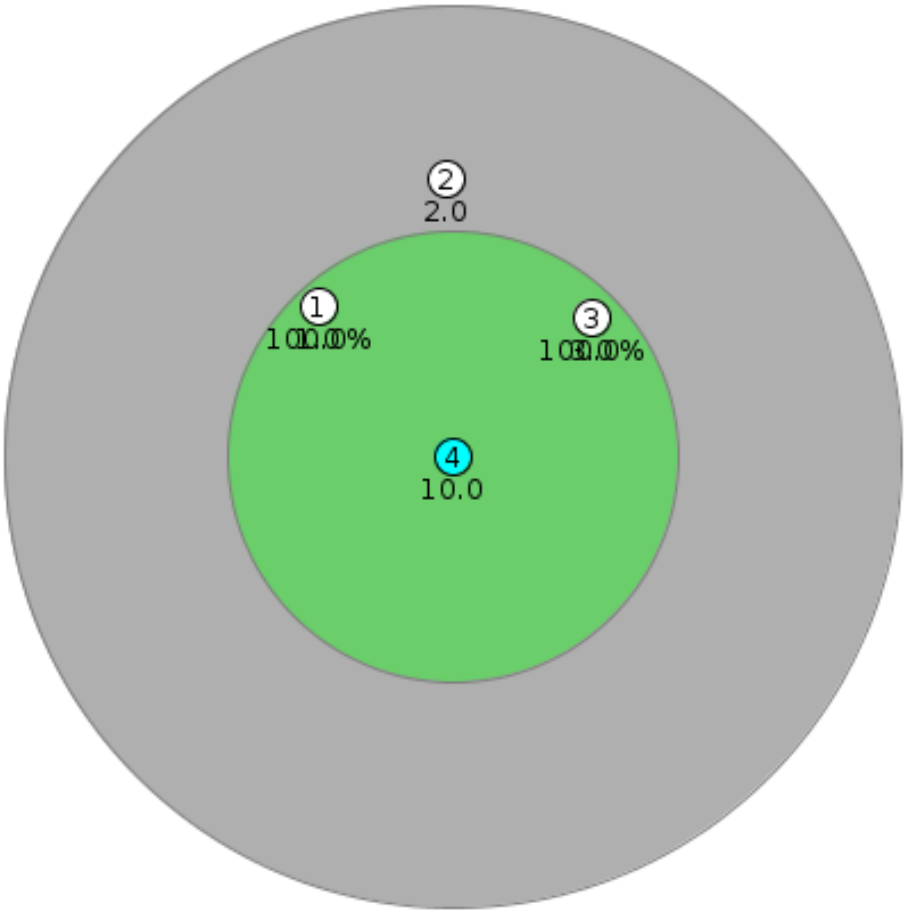
Σε αυτό το σενάριο όλοι οι κόμβοι είναι υγιείς. Από την γραφική παράσταση, φαίνεται ο αριθμός των πακέτων που αποστέλνονται συνολικά μέσα στο δίκτυο, ο αριθμός των πακέτων που παραλαμβάνονται από τον sink και ο αριθμός των πακέτων που χάνονται.

Παρατηρείται πως ο αριθμός των πακέτων που στέλνουν οι κόμβοι σε κάθε μια από τις 10 εκτελέσεις της προσομοίωσης κυμαίνεται στις ίδιες τιμές και είναι περίπου γύρω στα 1760 πακέτα.

Ο κόμβος με τον αριθμό 1, ο οποίος είναι και ο τελικός παραλήπτης (sink node), δεν συμπεριλαμβάνεται μέσα στην γραφική παράσταση αφού όλοι στέλνουν πακέτα σε αυτόν ενώ ο ίδιος είναι σε θέση μόνο να παραλαμβάνει τα πακέτα που φτάνουν σε αυτόν.

Παρατηρούμε ότι, υπάρχουν κάποιες απώλειες πακέτων μέσα στο δίκτυο οι οποίες όμως είναι αμελητέες και έτσι, σχεδόν όσα πακέτα αποστέλνονται μέσα στο δίκτυο, τόσα περίπου παραλαμβάνονται και από τον τελικό παραλήπτη (sink node).

Τοπολογία 5.4.2

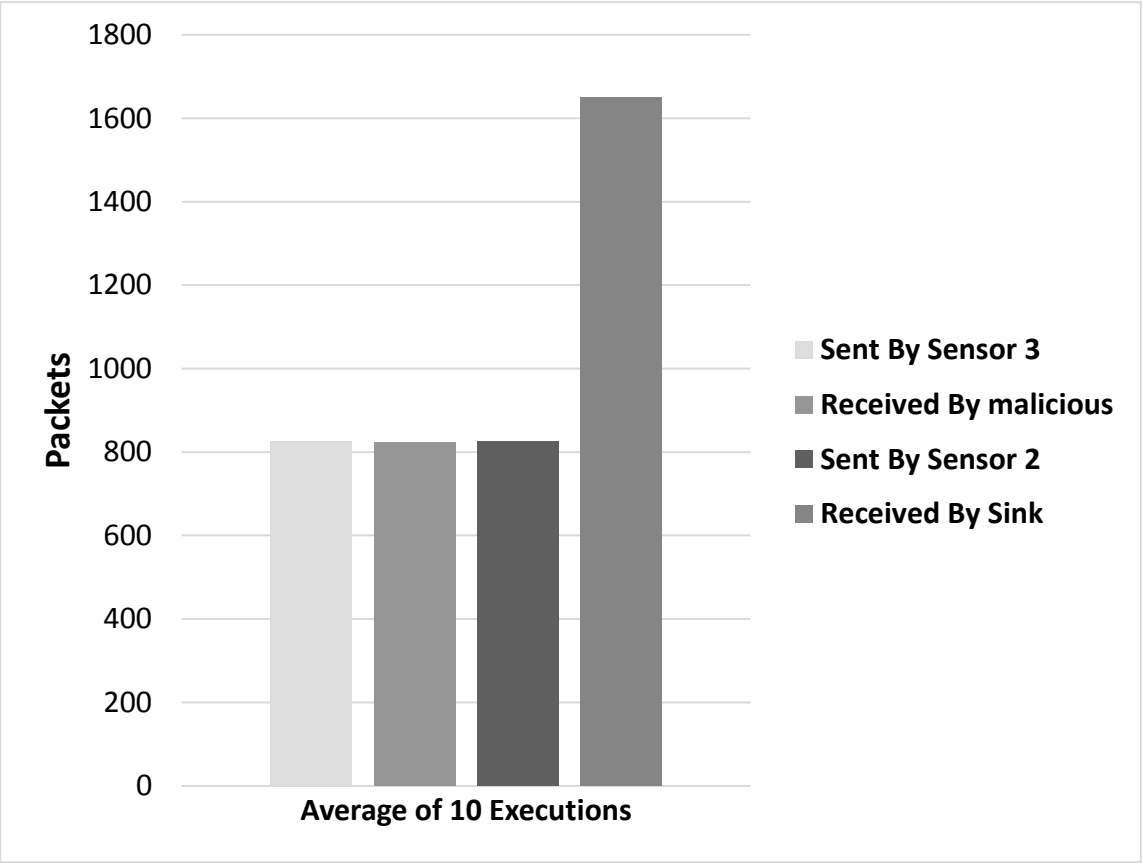


Σενάριο 5.4.2

3Benign – 1 Malicious Nodes

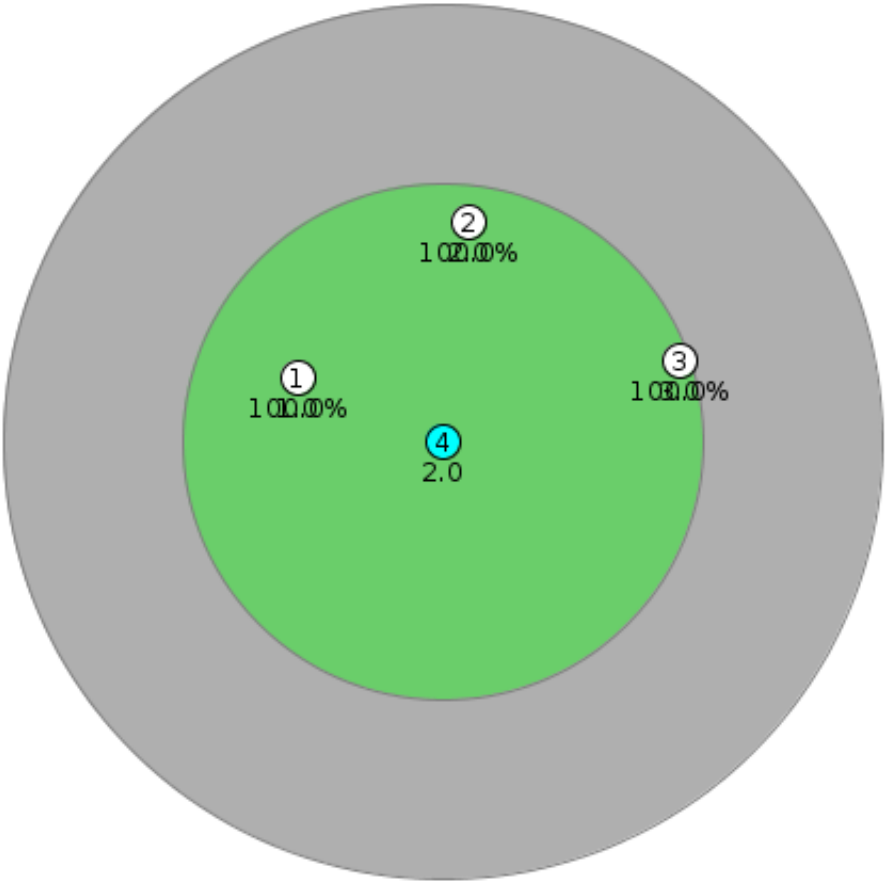
Τοπολογία 5.4.2

	Sent By Sensor 3	**Received By Malicious**	**Sent By Sensor 2**	**Received By Sink**
	825	824	825	1649
	825	825	825	1649
	824	824	824	1650
	826	823	826	1650
	825	824	825	1648
	824	824	824	1648
	826	823	826	1650
	826	824	826	1649
	825	824	825	1649
AVG	826	824	826	1648



Λόγω του ότι στην πιο πάνω τοπολογία, ο κακόβουλος αισθητήρας δημιούργησε τυχαία μια νέα ταυτότητα η οποία δεν ανήκε σε κανένα από τους υπόλοιπους κόμβους, η συμπεριφορά του στο δίκτυο δεν επηρεάζει την κανονική ροή του δικτύου. Έτσι βλέπουμε ότι, ως κανονικός κόμβος, παραλαμβάνει από τους υπόλοιπους κανονικά, αλλά δεν τα προωθεί.

Τοπολογία 5.4.3

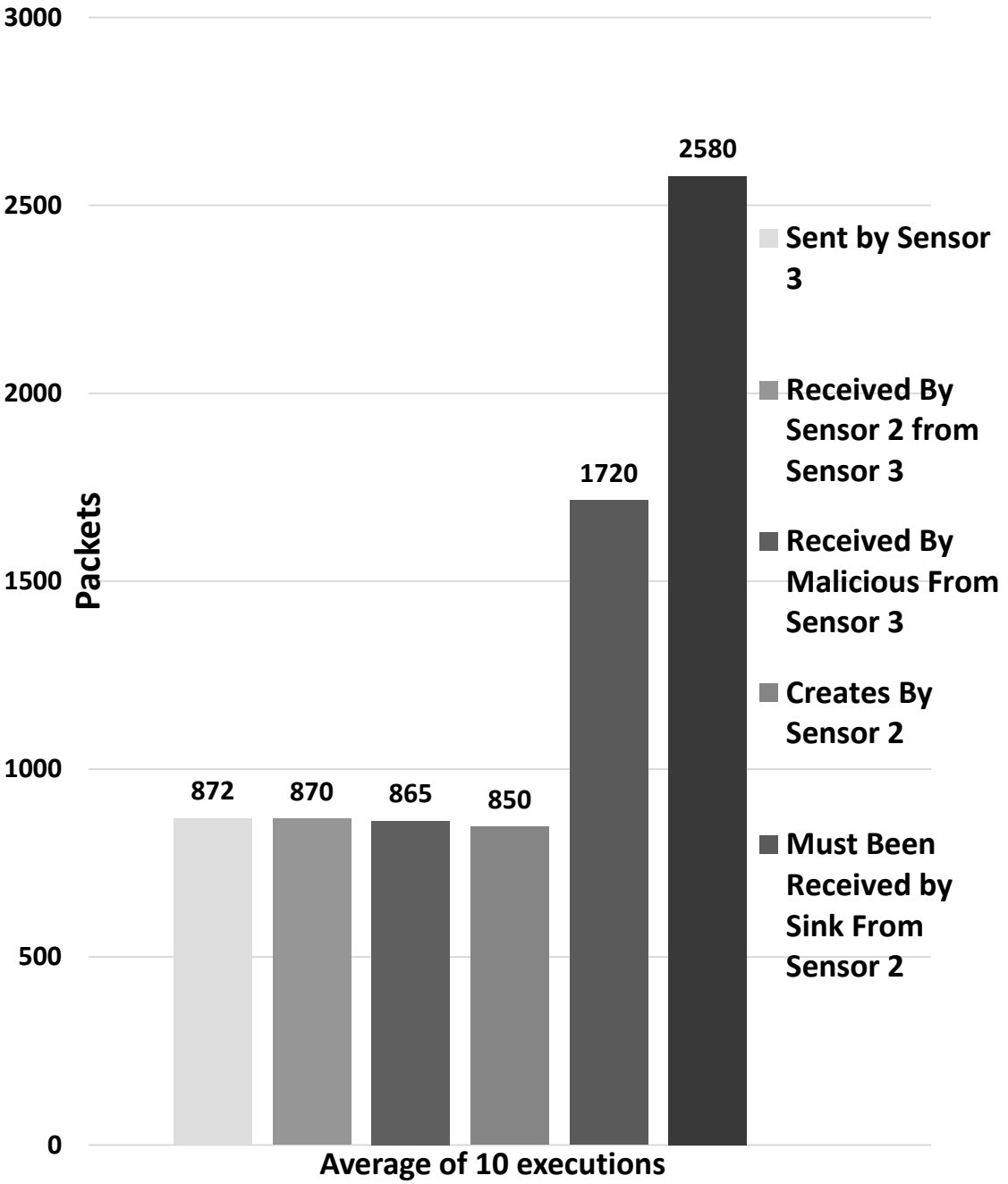


Σενάριο 5.4.3

3Benign- 1 Malicious

Τοπολογία 5.4.3

	Packets sent by Sensor 3	Packets Received by Sensor 2 from Sensor 3	Packets Received By Malicious	Packets Created By Sensor 2	Total Packets must been received by sink from Sensor 2	Packets Received By Sink From Sensor 2
	872	870	870	858	1728	2578
	870	870	870	845	1715	2580
	872	875	848	847	1715	25780
	875	872	848	844	1718	2580
	870	870	870	845	1720	2581
	872	870	870	846	1720	2580
	874	871	865	844	1718	2582
	872	870	866	848	1716	2580
	870	872	864	848	1723	2580
	872	870	865	847	1723	2581
AVG	872	870	865	850	1720	2580



Στην πιο πάνω τοπολογία, παρατηρούμε ότι ο κακόβουλος κόμβος δημιουργεί τυχαία μια ταυτότητα η οποία υπάρχει και στους γειτονικούς του κόμβους. Αυτό το σενάριο λοιπόν, βλέπουμε και στον πίνακα και στην γραφική, ότι είναι αντίστοιχο του σεναρίου 5.1.2 στο οποίο ο κακόβουλος κόμβος κλέβει ταυτότητες από γειτονικούς.

Κεφάλαιο 6

Συμπεράσματα

6.1 Συμπεράσματα

Σε αυτή τη διπλωματική εργασία, μελετήθηκαν διάφορα θέματα ασφάλειας τόσο σε δίκτυα υπολογιστών, όσο και σε ασύρματα δίκτυα αισθητήρων.

Με την υλοποίηση του ιού Sybil στις δύο πιο πάνω μορφές, μπορούμε να δούμε πως ένα κοινό δίκτυο αισθητήρων αντιδρά στην παρουσία κακόβουλων κόμβων οι οποίοι κλέβουν ή δημιουργούν νέες ταυτότητες.

Έτσι, συμπερασματικά, μπορούμε να κατανοήσουμε ότι, όταν ένας κακόβουλος κόμβος παρουσιαστεί ως ένας άλλος καθαρός κόμβος εν αγνοία των υπολοίπων, αυτοί στέλνουν και δέχονται πακέτα από το κακόβουλο, με αποτέλεσμα να υπάρχει σύγχυση μέσα στο δίκτυο και περισσότερη διανομή πακέτων.

Πιο συγκεκριμένα, διαβάζοντας αυτή την εργασία, είναι σε θέση κάποιος να κατανοήσει κάποια πράγματα όσο αφορά την ασφάλεια, αλλά κυρίως να μελετήσει την συμπεριφορά των μολυσμένων με Sybil attack κόμβων.

6.2 Μελλοντική εργασία

Στην παρούσα διπλωματική εργασία, η υλοποίηση του ιού Sybil, γίνεται στο πιο βασικό υπόβαθρο. Δηλαδή δεν υλοποιούνται περίπλοκα σενάρια και κυρίως δεν υπάρχει η έννοια του ταυτοχρονισμού. Μια μελλοντική εργασία που θα μπορούσε να γίνει με υπόβαθρο την παρούσα υλοποίηση, θα ήταν να συμπεριληφθεί ο ταυτοχρονισμός, όπου ένας κακόβουλος υποδύεται ταυτόχρονα με την δική του ταυτότητα και πολλές άλλες.

Επίσης, στην περίπτωση του Fabricated ID, θα μπορούσε να δοθεί πιο μεγάλη εμβέλεια στον αριθμό τυχαίων διευθύνσεων που μπορεί να δημιουργήσει ο κακόβουλος.

Τέλος, κάτι που δεν γίνεται σε αυτή την υλοποίηση και θα μπορούσε να γίνει, είναι να μπορεί ο κακόβουλος να προωθεί σε γειτονικούς του κόμβους και δικά του πακέτα ως ένας κανονικός νόμιμος κόμβος και όχι απλώς να προωθεί αυτά που παραλαμβάνει από τους άλλους.

Βιβλιογραφία

[1] *Ασφάλεια Δικτύων Υπολογιστών,* [online], http://el.wikipedia.org/wiki/%CE%91%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1_%CE%B4%CE%B9%CE%BA%CF%84%CF%8D%CF%89%CE%BD_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CF%8E%CE%BD [Accessed February 20, 2015]

[2] Mohammad O. Pervaiz, Mihaela Cardei, and Jie Wu, "Security in Wireless Local Area Networks", Florida Atlantic University

[3] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "*Wireless Sensor Network Security: A Survey",* in *Security in Distributed, Grid, and Pervasive Computing,* Yang Xiao, Auerbach Publications, CRC Press, 2006 [E-book]. Available: http://www.cs.wayne.edu/~weisong/papers/walters05-wsn-security-survey.pdf

[4] Dr. M. Kumar Jain, "Wireless Sensor Networks: Security Issues and Challenges*",* vol.02, no.01, 2011. [Online].Available:http://ijcit.uap-bd.edu/ijcit_papers/vol2no1/IJCIT-110746.pdf. [Accessed February 20, 2015].

[5] V. Rathod and M. Mehta, "Security in Wireless Sensor Network: A Survey", vol. 01, no.01, 2011. [Online].Available: http://academicpublishingplatforms.com/downloads/pdfs/gnujet/volume1/20110724173 1_18-58-1-PB.pdf. [Accessed March 02, 2015].

[6] J.A. Stankovic, "Wireless Sensor Networks", 2006. [Online]. Available: http://www.cs.virginia.edu/~stankovic/psfiles/wsn.pdf [Accessed March 02, 2015].

[7] L. Tobarra, D. Cazorla, and F. Cuartero, "Security in Wireless Sensor Networks: A Formal Approach". [Online].Available: https://investigacion.uclm.es/documentos/fi_1269424753-tobarra_book_security_wsn09.pdf . [Accessed March 02, 2015].

[8] B. Daya, "Network Security: History, Importance, and Future". [Online]. Available: http://web.mit.edu/~bdaya/www/Network%20Security.pdf. [Accessed March 02, 2015].

[9] Σύστημα Ανίχνευσης Εισβολής, [online], http://el.wikipedia.org/wiki/%CE%A3%CF%8D%CF%83%CF%84%CE%B7%CE%BC%CE%B1_%CE%91%CE%BD%CE%AF%CF%87%CE%BD%CE%B5%CF%85%CF%83%CE%B7%CF%82_%CE%95%CE%B9%CF%83%CE%B2%CE%BF%CE%BB%CE%AE%CF%82, [Accessed March 07, 2015].

[10] E. Maiwald, “Network Security A Beginner’s Guide to Network Security”, Cisco Systems, 2001. [Accessed March 07, 2015].

[11] Τι είναι Firewall [online], http://ti-einai.gr/firewall/, [Accessed March 07, 2015].

[12] Common Types of Network Attacks, [online], https://technet.microsoft.com/en-us/library/cc959354.aspx. [Accessed March 8, 2015]

[13] C. Karlof and D. Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”,

[14] L. Wallgren, S. Raza, T. Voigt, "Routing Attacks and Countermeasures in the RPL-Based", International Journal of Distributed Sensor Networks, vol.2013, 2013.[online].Available:http://www.hindawi.com/journals/ijdsn/2013/794326/. [Accessed March 10, 2015].

[15] H. K. Kalita and A. Kar, "WIRELESS SENSOR NETWORK SECURITY ANALYSIS",vol.1,no.1,2009,[online].Available: http://airccse.org/journal/ijngn/papers/1.pdf . [Accessed March 10, 2015].

[16] M. R. Ahmed, X. Huang, and D. Sharma, "A Taxonomy of

Internal Attacks in Wireless Sensor Network", vol.6, 2012.[online]. Available:http://waset.org/publications/11043/a-taxonomy-of-internal-attacks-in-wireless-sensor-network . [Accessed March 10, 2015].

[17] K. Sharma and M. K. Ghose, "Wireless Sensor Networks: An Overview on its SecurityThreats", 2010,[online].Available:http://dubairowing.com/admin/media/files/news-gallery/23_1374791231.PDF . [Accessed March 15, 2015].

[18] R. Tiwari and M. Kohli, "Security Aspects for Wireless Sensor Network", vol.1, no.8, 2012. [online]. Available: http://www.ijert.org/view-pdf/1472/security-aspects-for-wireless-sensor-network . [Accessed March 15, 2015].

[19] Y.C HU, A. Perrig, D. B. Johnson, "Wormhole attacks in wireless networks, IEEE Journal on selected areas in communication", vol.24, no.2, 2006. [online]. Available:http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1589115&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D1589115. [Accessed March 16, 2015].

[20] Z. A. Baig, *“Distributed Denial of Service Attack Detection in Wireless Sensor Networks”*, Phd Thesis, Monash University January, 2008

[21] A. Pandey and R.C. Tripathi, "A Survey on Wireless Sensor Networks Security", vol3, no.2,2010,[online].Available: http://www.ijcaonline.org/volume3/number2/pxc387989.pdf. [Accessed April 2015].

[22] J. Newsome, E. Shi, D.Song and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis&Defenses",2004,[online].Available: http://repository.cmu.edu/cgi/viewcontent.cgi?article=1041&context=ece.[Accessed April 2, 2015].

[23] A. S. Salehi., M.A. Razzaque, P. Naraei and A. Farrokhtala, "Security in Wireless Sensor Networks: Issues and Challenges", 2013, [online]. Available: http://eprints.qut.edu.au/74464/4/74464.pdf. [Accessed April 2, 2015].

[24] I. F. Akyildiz, W. Su, "Wireless sensor networks: a survey.", vol.1, no.1, 2002, [online].Available:http://www.academia.edu/10472071/Security_in_Wireless_Sensor_Network_A_survey. [Accessed April 22, 2015].

[25] T. H. Kim, C. H. Kim, C. P. Hong and H. Kim, "Comparison of Security Protocols for Wireless Sensor Networks",[online].Available: http://www.academia.edu/433773/Comparison_of_Security_Protocols_for_Wireless_Sensor_Networks. [Accessed May 2, 2015].

[26] R. Sharma, Y. Chaba and Y. Singh, "Analysis of Security Protocols in Wireless Sensor Network", 2010,[online].Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.419.4574. [Accessed May 2, 2015].

[27] Contiki, [online], http://en.wikipedia.org/wiki/Contiki. [Accessed May 2, 2015].

[28] Contiki: The Open Source Operating System for the Internet of Things, [online], Available at: http://www.contiki-os.org/. [Accessed May 3, 2015].

[29] A. Sehgal, "Using the Contiki Cooja Simulatr". [online]. Available: http://cnds.eecs.jacobs-university.de/courses/iotlab-2013/cooja.pdf. [Accessed May 20, 2015].

[30] Al. K. Pathan , H. Lee and C. S. Hong, "Security in Wireless Sensor Networks: Issues and Challenges", 2006, [online]. Available: http://arxiv.org/ftp/arxiv/papers/0712/0712.4169.pdf . [Accessed May 20,2015].

[31] W. Stallings, *Cryptography and Network Security Principles and Practise*, Published by Pearson, 5th Edition, 2011

[32] A. Vasudeva1 and M. Sood, “Sybil Attack on Lowest ID Clustering Algorithm in the mobile*”,* vol4. no.5, 2012, [online]. Available: http://airccse.org/journal/nsa/0912nsa11.pdf. [Accessed May 20, 2015].

[33] http://senstools.gforge.inria.fr/doku.php?id=os:contiki#rime_stack

[34] International Journal of Scientific & Engineering Research, Volume 3, Issue 3, March-2012