Ατομική Διπλωματική Εργασία

ΕΠΙΘΕΣΕΙΣ ΣΕ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΑΙΣΘΗΤΗΡΩΝ ΣΤΟ ΠΡΩΤΟΚΟΛΛΟ RPL

Χαράλαμπος Παντελή

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μάιος 2015

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Επιθέσεις σε Ασύρματα Δίκτυα Αισθητήρων
στο Πρωτόκολλο RPL

Χαράλαμπος Παντελή

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 θερμά τον επιβλέποντα καθηγητή μου κ. Βάσο Βασιλείου, για την υποστήριξη και καθοδήγηση που μου προσέφερε κατά την διάρκεια έρευνας και υλοποίησης της παρούσας εργασίας, καθώς και για την επίτευξη μιας άψογης συνεργασίας. Επίσης, να τον ευχαριστήσω για την κατανόηση και την βοήθεια στα όποια προβλήματα προέκυψαν στη πορεία.

Επίσης, ξεχωριστές ευχαριστίες πρέπει να δοθούν στη διδακτορική φοιτήτρια του τμήματος, Χριστιάνα Ιωάννου , η οποία βρισκόταν εκεί καθ' όλη της διάρκεια της χρονιάς για να με συμβουλεύει μέσα από εποικοδομητικές συζητήσεις για τα όποια αμφιλεγόμενα ή όχι σημεία της πτυχιακής μου εργασίας, αλλά και της καθοδήγησής μου για την εξέλιξή της.

Αξίζει να δοθούν ευχαριστίες και στους ερευνητές (Contiki developers) που συνεργαστήκαμε μέσω ηλεκτρονικών μηνυμάτων για επίλυση πολλών προβλημάτων που εμφανίστηκαν.

Εν τέλη, θα ήθελα να ευχαριστήσω την οικογένεια μου, τους φίλους μου και τη φίλη μου Μαρία, για τη στήριξη που μου έδιναν κατά τη διάρκεια εκπόνησης της πτυχιακής μου εργασίας, αλλά και καθ' όλη τη διάρκεια των σπουδών μου στο Πανεπιστήμιο Κύπρου.

Περίληψη

Είναι ευρέως γνωστό, ειδικότερα τα τελευταία χρόνια, η ακμή που επικρατεί στον τομέα της επιστήμης της πληροφορικής, καθότι είναι η επιστήμη η οποία μάλλον έχει αναπτυχθεί τόσο περισσότερο από οποιαδήποτε άλλη επιστήμη ανά το παγκόσμιο αλλά και σε πολύ μικρό χρονικό διάστημα.

Με αυτό το δεδομένο, όπως θα μπορούσε ένας ειδικός να πει ότι έχουν ενσωματωθεί διάφορες ανέσεις στην καθημερινή ζωή του ανθρώπου, θα μπορούσε κάλλιστα να πει ότι ενσωματώνεται και ένα διαφορετικό σύστημα, σύστημα το οποίο αποτελεί μέσο για να εκτελεσθούν διαφόρων ειδών επιθέσεις. Επιθέσεις οι οποίες έχουν συγκεκριμένο στόχο, ο οποίος στον τομέα εφαρμογής μας, δηλαδή της πληροφορικής, είναι η εκμετάλλευση των δεδομένων ή και η επεξεργασία αυτών, με απώτερο σκοπό την πρόκληση σημαντικών βλαβών στα δίκτυα.

Επιθέσεις μπορούν να δεχτούν όλα τα δίκτυα ανεξαρτήτως μορφής, και πιο συγκεκριμένα, τα ασύρματα δίκτυα αισθητήρων αφού μεγάλες ερευνητικές δραστηριότητες τα έχουν σαν κύρια βάση τους ανά το παγκόσμιο. Η μελέτη των ασύρματων δικτύων αισθητήρων, είναι από φύσης της πιο ιδιαίτερη, αφού τα ασύρματα δίκτυα αισθητήρων έχουν ένα ιδιόμορφο χαρακτήρα, καθότι αποτελούνται από κόμβους, είτε μικρού είτε μεγάλου μεγέθους, οι οποίοι λειτουργούν μερικώς αυτόνομα και έχουν περιορισμένες υπολογιστικές δυνατότητες, γεγονός το οποίο τα καθιστά πολύ πιο ευάλωτα.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

1.1 Γενικά

Είναι ευρέως γνωστό ότι πρώτιστη επιδίωξη της παρουσίας του διαδικτύου στην ζωή του ανθρώπου ήταν η ανταλλαγή δεδομένων μεταξύ δύο ή και περισσότερων χρηστών, καθώς επίσης και η επικοινωνία μεταξύ ανθρώπων. Βάση τούτου, υπάρχουν πολλά πλεονεκτήματα στα οποία μπορούμε να αναφερθούμε, και τα οποία είναι αναμφισβήτητα.
Σε αντίθεση όμως με τα πιο πάνω, το διαδίκτυο μπορεί να πει κανείς ότι έχει πληγεί, λόγω των συχνών επιθέσεων που μπορεί να δεχτεί, ένα γεγονός το οποίο μπορεί να κριθεί ιδιαίτερα σημαντικό, αφού χρειάζεται η άμεση ασφάλεια ως κύριος μοχλός προστασίας τόσο ενός οργανισμού, μιας επιχείρησης όσο και των πληροφοριών που μπορεί να βρίσκονται στις βάσεις δεδομένων τους. Η ασφάλεια των δεδομένων, είναι σημαντική σε χρήστη προσωπικού υπολογιστή αλλά και ως αναφέρεται ανωτέρω σε ολόκληρο οργανισμό ή και επιχείρησης.

Ένα απλό παράδειγμα, της έννοιας της ασφάλειας των δικτύων στην ακεραιότητα και εμπιστευτικότητα των δεδομένων, είναι η σωστή προσέγγιση προς προστασία μιας επιχείρησης ή του οργανισμού, στον τρόπο προστασίας πληροφοριών της, αλλά και η προστασία από τυχόν καταστροφές ή αλλοιώσεις. Περαιτέρω δε, η προστασία του οργανισμού από μη εξουσιοδοτημένη χρήση δεδομένων του από πρόσωπα μη έχοντα άδεια για μια τέτοια πράξη. Συγκεκριμένα, σε περιπτώσεις που αφορούν θέματα ασφάλειας όπως τα δεδομένα εθνικής φρουράς ή και θέματα πολιτικού επιπέδου, υπάρχει μία πολύ λεπτή γραμμή ευαισθησίας ως προς την προστασία αυτών, και η οποιαδήποτε υποκλοπή τους θα αποτελέσει πλήγμα.

Προκειμένου ένας οργανισμός να λειτουργήσει αξιόπιστα, χρειάζεται εκτός από ποιότητα και απόδοση, την σωστή ασφάλεια των δεδομένων. Βάση αυτού του γεγονότος, η ασφάλεια στα δίκτυα των υπολογιστών, αποτελεί ουσιαστικά τρόπο παρεμπόδισης ασυνήθιστων δραστηριοτήτων μέσα σε ένα δίκτυο καθώς και ορθοστάτη στην αντιμετώπιση αυτών, σύμφωνα πάντοτε με τα μέτρα τα οποία κρίνονται σωστά και κατάλληλα.

Τέλος δε, τρία από τα κύρια και απαραίτητα συστατικά της εφαρμογής της ασφάλειας στα δίκτυα των υπολογιστών τα οποία έχουν ως πρωταρχικό ρόλο την ασφάλεια από εξωτερικές απειλές απαριθμούνται κατωτέρω ως ακολούθως:

Α. Πρόληψη: η οποία αποσκοπεί στην λήψη μέτρων προτού καν προκύψει οποιοδήποτε πρόβλημα εις τα εντός του δικτύου.

Β. Ανίχνευση: πρώτιστος σκοπός της είναι η λήψη μέτρων ως προς το πότε πως και από ποιόν προκλήθηκε το οποιοδήποτε πρόβλημα εις τα εντός του δικτύου.

Γ. Αντίδραση: κύριος σκοπός της είναι η λήψη μέτρων αφότου επήλθε επίθεση ή και πρόβλημα στο δίκτυο. Συγκεκριμένα, η αντίδραση μεριμνά για την αποκατάσταση ή και την ανάκτηση των συστατικών μερών ενός δικτύου.

1.2 Σκοπός

Σκοπός της παρούσας διπλωματικής εργασίας είναι η δημιουργία επιθέσεων σε ασύρματα δίκτυα αισθητήρων. Επιχειρείται η μελέτη εισδοχής ενός κακόβουλου κόμβου σε ένα ασύρματο δίκτυο αισθητήρων με σκοπό την ανάπτυξη ενός αλγορίθμου για την ανίχνευση και τον εντοπισμό μιας απειλής που κινείται εντός της περιοχής του δικτύου. Ο κακόβουλος κόμβος κινείται εντός των ορίων του δικτύου και μπορεί να επικοινωνήσει ασύρματα με όλους τους κόμβους αυτού, μολύνοντας τους. Κάθε μολυσμένος κόμβος περιέχει λανθασμένη τιμή του μεγέθους το οποίο μετρά και εν δυνάμει, λόγω της επικοινωνίας του με άλλους κόμβους μπορεί να τη μεταδώσει.

Επειδή αυτά τα δίκτυα χρησιμοποιούνται σε σημαντικές εφαρμογές καθίσταται βασική απαίτηση η έγκαιρη ανίχνευση ενός σφάλματος – μόλυνση.

1.3 Μεθοδολογία

Κατά την εκπόνηση της παρούσας διπλωματικής εργασίας, έγινε εκτενής μελέτη διάφορων επιστημονικών και μη άρθρων, προς ορθή και καλύτερη κατανόηση των πρωτοκόλλων. Σκοπός της μελέτης των πρωτοκόλλων, ήταν η μέγιστη δυνατή υλοποίηση επιθέσεων σε αυτά.

Εν συνεχεία, υπήρξε μια πρώτη επαφή με το περιβάλλον εργασίας στο οποίο θα υλοποιούνταν οι ιοί, το λειτουργικό σύστημα Contiki καθώς και τον προσομοιωτή Cooja.

Πρωτίστως, έγιναν πειράματα σε απλά παραδείγματα ούτως ώστε να γίνει σωστή κατανόηση των προαναφερόμενων εργαλείων, με αποτέλεσμα την ορθή τους χρήση ως προς την υλοποίηση των ιών.

Συνεπακόλουθα των ανωτέρω και μετά από αποτελεσματική χρήση του περιβάλλοντος εργασίας αφού αυτό προήλθε μέσα από την κατανόηση του τρόπου λειτουργίας του, αλλά και με ορθή μελέτη συγκεκριμένων άρθρων, αμέσως επόμενο βήμα ήταν η υλοποίηση των ιών.

Τελικώς, μετά από πειράματα σε διάφορες τοπολογίες, διά μέσου χρήσεως γραφικών παραστάσεων, εξήχθησαν τα κατάλληλα αποτελέσματα.

1.4 Δομή

Η παρούσα πτυχιακή εργασία αποτελείται από οκτώ κεφάλαια. Στο Κεφάλαιο 2 γίνεται εισαγωγή για την ασφάλεια στα ασύρματα δίκτυα αισθητήρων. Επίσης, θα γίνει αναφορά για τα στρώματα δικτύου και για τα πρωτόκολλα με τα οποία θα ασχοληθούμε. Επιπλέον αναφέρονται οι σχεδιαστικοί περιορισμοί που έχουν τα ασύρματα δίκτυα αισθητήρων καθώς και για διάφορες εφαρμογές των ασύρματων δικτύων αισθητήρων.

Στο Κεφάλαιο 3 γίνεται αναφορά για τη ασφάλεια στα δίκτυα. Θα αναφερθούμε στους στόχους ασφαλείας των δικτύων, καθώς επίσης τα διάφορα εργαλεία ασφαλείας που μπορούμε να χρησιμοποιήσουμε για την ασφάλεια των δικτύων. Τέλος θα δούμε τις δύο κατηγορίες των επιθέσεων στα δίκτυα.

Στο Κεφάλαιο 4 γίνεται αναφορά για τις επιθέσεις στα ασύρματα δίκτυα αισθητήρων. Θα γίνει μια γενική αναφορά για τις επιθέσεις στα ασύρματα δίκτυα και θα αναλυθούν περισσότερο οι επιθέσεις στα δύο πρωτόκολλα που μας αφορούν, το RPL και το IPv6.

Στο Κεφάλαιο 5 γίνεται αναφορά στο λειτουργικό σύστημα Contiki και στο προσομοιωτή Cooja τα οποία θα χρησιμοποιήσουμε για να υλοποιήσουμε τους ιούς μας.

Στο Κεφάλαιο 6 γίνεται αναφορά στους ιούς που υλοποιήθηκαν καθώς και τα σενάρια προσομοιώσεων που υλοποιήθηκαν αναλύοντας τα εκτενέστερα. Επίσης γίνεται αναφορά σε μελλοντική εργασία που μπορεί να γίνει.

Στο Κεφάλαιο 7 γίνεται αναφορά στα γενικά συμπεράσματα που βγήκαν από την υλοποίηση.

Κεφάλαιο 2

Ασύρματα Δίκτυα Αισθητήρων

2.1 Εισαγωγή

Η τελευταία δεκαετία ήταν αρκετά καθοριστική στην ανάπτυξη και εξέλιξη της τεχνολογίας των ασύρματων επικοινωνιών καθότι έφεραν στο επίκεντρο τα ασύρματα δίκτυα αισθητήρων και κατ' επέκταση την ανάπτυξη κόμβων αισθητήρων. Οι κόμβοι αυτοί έχουν συγκεκριμένα χαρακτηριστικά μερικά εκ των οποίων είναι η χαμηλή δυνατότητα σε υπολογιστική ισχύ, αποθήκευση και μνήμη, χαρακτηριστικά τα οποία είχαν ως αποτέλεσμα οι κόμβοι να είναι χαμηλού κόστους, χαμηλής ισχύος και μικρού μεγέθους. Αν και το μέγεθος των συσκευών μπορεί να είναι μικρό, υπάρχει ωστόσο η δυνατότητα μέτρησης και συλλογής πληροφοριών από το περιβάλλον, χωρίς να είναι αναγκαίος ο οποιοσδήποτε έλεγχος.

Συγκεκριμένα τα ασύρματα δίκτυα αισθητήρων (wireless sensor network – WSN)[1][2] είναι δίκτυα που αποτελούνται από ποικιλία αισθητήρων καθώς και εκατοντάδες έως και χιλιάδες τέτοιους κόμβους που συνδέονται μεταξύ τους με ένα ασύρματο μέσο. Περαιτέρω αποτελούνται από ενεργειακά αυτόνομους κόμβους οι οποίοι αισθάνονται και παρατηρούν φυσικά μεγέθη, είναι δηλαδή ικανοί να συλλέγουν ποικιλία δεδομένων που αφορούν το περιβάλλον γύρω τους, όπως θερμοκρασία, πίεση, υγρασία, φωτισμό, επίπεδο θορύβου, κίνηση αντικειμένου κ.α. Προκειμένου να φτάσει η συλλογή πληροφοριών στον τελικό χρήστη, σημειωτέον ότι βρίσκεται σε μεγάλη απόσταση από τον χώρο εξέλιξης του φαινόμενου, χρειάζεται η συνεργασία των ενδιάμεσων κόμβων. Για να επιτύχει αυτό χρειάζεται η ορθή οργάνωση των κόμβων στο δίκτυο.

2.2 Στρώματα

Όπως κάθε άλλη συσκευή τηλεπικοινωνιών έτσι και οι κόμβοι αισθητήρων χρησιμοποιούν μία καθορισμένη στοίβα πρωτοκόλλων (protocol stack). Η στοίβα πρωτοκόλλων επιτρέπει τη συνεργασία μεταξύ των κόμβων, την επικοινωνία μεταξύ τους καθώς και την επικοινωνία πληροφοριών σχετικά με την κατάσταση των κόμβων. Η στοίβα πρωτοκόλλων αποτελείται από τα ακόλουθα στρώματα [1][2]:

Physical Layer

Το φυσικό στρώμα (Physical Layer): έχει ως βασικό του στόχο την ελαχιστοποίηση της κατανάλωσης ισχύος. Επίσης, είναι υπεύθυνο για την επιλογή της συχνότητας, την ανίχνευση σήματος, τη διαμόρφωση και την κρυπτογράφηση των δεδομένων.

Data Link Layer

Το στρώμα ζεύξης δεδομένων (Data Link Layer): έχει τις ακόλουθες αρμοδιότητες: την πολυπλεξία των ροών δεδομένων, την ανίχνευση πλαισίων δεδομένων, την πρόσβαση στο μέσο και τον έλεγχο σφαλμάτων. Εφόσον το περιβάλλον μπορεί να είναι αρκετά θορυβώδες και οι κόμβοι-αισθητήρες να είναι κινούμενοι, το πρωτόκολλο MAC πρέπει να φροντίζει για χαμηλή κατανάλωση ενέργειας και την ελαχιστοποίηση των συγκρούσεων μεταξύ μηνυμάτων γειτονικών κόμβων.

Network Layer

Το στρώμα δικτύου (Network Layer): ενώ στο Data Link Layer εξασφαλίζεται ο τρόπος με τον οποίο επικοινωνούν δύο κόμβοι μεταξύ τους, στο Network Layer έχουμε την επιλογή του κόμβου που θα επιχειρηθεί η επικοινωνία. Το στρώμα αυτό είναι αρμόδιο για την δρομολόγηση των δεδομένων μέσα σε ένα ασύρματο δίκτυο αισθητήρων, παραδείγματος χάριν να βρίσκει την αποδοτικότερη διαδρομή για ένα πακέτο μέχρι να φτάσει στον προορισμό του.

Transport Layer

Το στρώμα μεταφοράς (Transport Layer) : Χρησιμοποιείται για την φροντίδα διατήρησης της ροής των δεδομένων, σε περιπτώσεις επικοινωνίας με εξωτερικά συστήματα.

Applications Layer

Το στρώμα εφαρμογής (Applications Layer): 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 πρωτόκολλου. Πλήθος εφαρμογών μπορούν να αναπτυχθούν και να φιλοξενηθούν σε αυτό το στρώμα.

2.3 Πρωτόκολλα

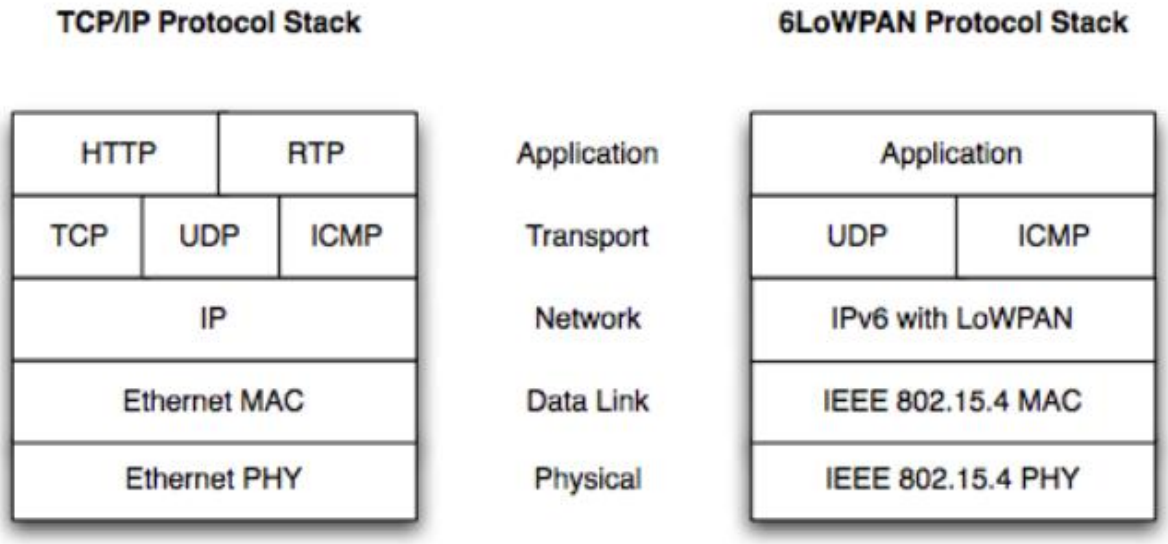
Πρωτόκολλο στην καθημερινή μας ζωή, θεωρείται ένα σύνολο από συμβάσεις που καθορίζουν πώς πρέπει κάποια διαδικασία να πραγματοποιηθεί. Τώρα, το πρωτόκολλο στη γλώσσα της Πληροφορικής είναι ένα σύνολο από συμβάσεις και καθορίζει το τρόπο ανταλλαγής δεδομένων μεταξύ των υπολογιστών που βρίσκονται στο δίκτυο. Το Internet δεν θεωρείται ένα απλό δίκτυο αλλά ένα διαδίκτυο. Επομένως, με την ύπαρξη υπολογιστών διαφορετικού τύπου που μπορεί να ανήκουν και σε διαφορετικά δίκτυα χρειάζεται ένα σύνολο πρωτοκόλλων για να καθοριστεί ο τρόπος επικοινωνίας μεταξύ τους.

2.3.1 6LoWPAN

Η IEFT στην προσπάθεια της για να εντάξει το Internet Protocol στα ασύρματα δίκτυα αισθητήρων έφτιαξε το 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Network) [3]. Με σκοπό την εκμετάλλευση των δυνατοτήτων και των πλεονεκτημάτων που παρέχει το IPv6 πρωτόκολλο πάνω στο IEEE 802.15.4.

Είναι εμφανής η διαφορά που υπάρχει μεταξύ της στοίβας 6LoWPAN **(Σχήμα 2.3.1.2**)[15]και της στοίβας TCP/IP **(Σχήμα 2.3.1.1)**[14]**.** Το 6LoWPAN πρωτόκολλο είναι ουσιαστικά ένα στρώμα προσαρμογής που μεσολαβεί μεταξύ του Network και

Link Layers και παρέχει όλες τις υπηρεσίες που χρειάζεται το Network Layer και δεν προσφέρονται από το Link Layer. Επιπλέον, το 6LoWPAN πρωτόκολλο υποστηρίζει μόνο IPv6 διευθύνσεις, σε αντίθεση με τη TCP/IP στοίβα που υποστηρίζει και IPv4 διευθύνσεις.

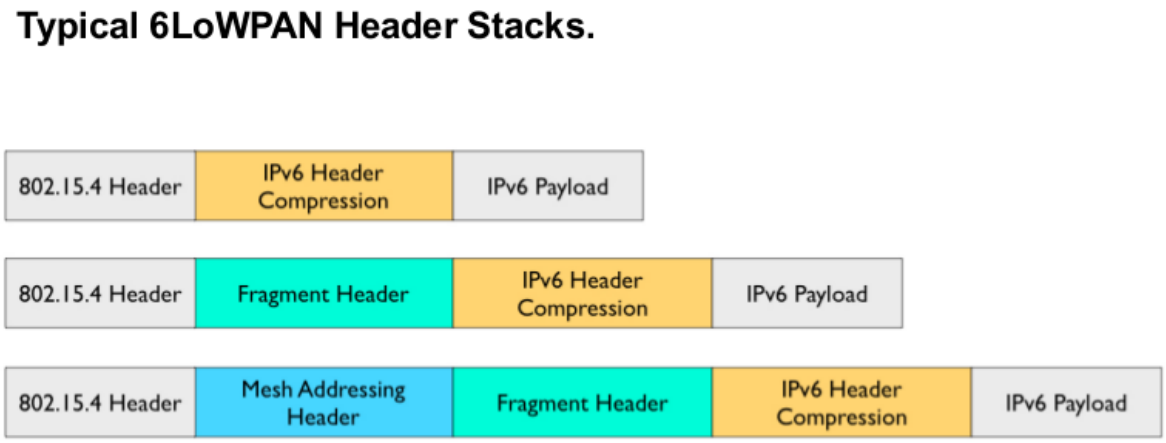


Σχήμα 2.3.1.1[32] **Σχήμα 2.3.1.2[32]**

Το IPv6 πρωτόκολλο χρειάζεται ελάχιστο maximum transmission unit (MTU) 1280 bytes για να προλαβαίνει τον συχνό κατακερματισμό της IP διεύθυνσης. Το IEEE 802.15.4 πρωτόκολλο, όπως παρουσιάστηκε, υποστηρίζει μέχρι 127 bytes ως μέγιστο μέγεθος πλαισίου. Συνεπώς, ο κατακερματισμός που προσφέρεται από το 6LoWPAN πρωτόκολλο δεν επιτρέπει την εκπομπή μεγάλων πακέτων στο δίκτυο. Στη περίπτωση που το πακέτο δεν χωράει μέσα σε ένα 802.15.4 πλαίσιο, κατακερματίζεται σε μικρότερα τμήματα. Ο παραλήπτης των τμημάτων χρησιμοποιεί την διεύθυνση του αποστολέα, τη διεύθυνση του παραλήπτη, το μέγεθος του πακέτου και την ετικέτα αναγνώρισης όλων των τμημάτων που ανήκουν στο συγκεκριμένο πακέτο για την ανακατασκευή του. Ο κατακερματισμός είναι ανεπιθύμητος στη περίπτωση των ασύρματων δικτύων αισθητήρων, αφού η περίπτωση που χαθεί κάποιο τμήμα χρειάζεται αναμετάδοση, καθώς επίσης και η ανακατασκευή του πακέτου κοστίζει σε πόρους.

Το 6LoWPAN πρωτόκολλο παρέχει τρείς μορφές κεφαλίδας (όπως παρουσιάζονται στο **Σχήμα 2.3.1.3**)[29]: αποστολής (dispatch), πλέγματος (mesh) και κατακερματισμού

(fragmentation). Η μορφή της κεφαλίδας προσδιορίζεται από το πεδίο 802.15.4 κεφαλίδας στην αρχή κάθε κεφαλίδας. Μειώνοντας το μέγεθος της κεφαλίδας, επιτυγχάνεται η εξοικονόμηση ενέργειας ανά πακέτο, η αύξηση της ωφέλιμης πληροφορίας και ο μέγιστος δυνατός περιορισμός του κόστους του κατακερματισμού.



Σχήμα 2.3.1.3 [33]

2.3.2 RPL

Η IETF λαμβάνοντας υπόψη τα ιδιαίτερα χαρακτηριστικά και απαιτήσεις των ασύρματων δικτύων αισθητήρων, οργάνωσε μια Ομάδα Εργασίας προκειμένου να προτυποποιήσει μια λύση δρομολόγησης βασισμένη στο IPv6, οδηγώντας στο σχηματισμό της Ομάδας Εργασίας «Δρομολόγηση πάνω από Χαμηλής Ισχύος και με Απώλειες Δίκτυα» (Routing Over Lowpower and Lossy – ROLL – networks) το 2008. Η συμβατότητα με το IPv6 χαρίζει στο πρωτόκολλο τη δυνατότητα διευθυνσιοδότησης, καθώς χαρακτηρίζεται από ευρεία κλίμακα διευθύνσεων, ενώ ενσωματώνει τη δυνατότητα αυτό-ρύθμισης. Το αποτέλεσμα των εργασιών της συγκεκριμένης ομάδας είναι το Πρωτόκολλο Δρομολόγησης για τα LLNs (RoutingProtocol for LLNs – RPL) [4]. Το RPL λειτουργεί στο επίπεδο IP σύμφωνα με την αρχιτεκτονική IP, επιτρέποντας τη δρομολόγηση πάνω από διάφορα επίπεδα ζεύξης.

Το RPL είναι ένα πρωτόκολλο δρομολόγησης IPv6 Διανύσματος Απόστασης σχεδιασμένο για LLNs, το οποίο καθορίζει τον τρόπο σχηματισμού ενός Άκυκλου Κατευθυνόμενου Γράφου Προσανατολισμένου στον Προορισμό (Destination Oriented

Directed Acyclic Graph – DODAG) με βάση την αντικειμενική συνάρτηση και ένα σύνολο μετρικών δρομολόγησης και περιορισμών. Οι μετρικές δρομολόγησης αντιστοιχούν σε βαθμωτά μεγέθη, που χρησιμοποιούνται για την επιλογή της καλύτερης διαδρομής. Οι περιορισμοί είναι πρόσθετα κριτήρια, με βάση τα οποία αποκλείονται ζεύξεις ή κόμβοι που δεν τα ικανοποιούν. Η αντικειμενική συνάρτηση συνίσταται από το συνδυασμό μετρικών δρομολόγησης και περιορισμών.

Ο DODAG αποτελείται από ένα σύνολο κορυφών που αντιστοιχούν σε κόμβους και ακμών που αντιστοιχούν σε ζεύξεις μεταξύ γειτονικών κόμβων, οι οποίες διαθέτουν προσανατολισμό ούτως, ώστε να μη δημιουργούνται βρόχοι, και οι οποίες είναι προσανατολισμένες προς έναν ή περισσότερους κόμβους-ρίζες (root nodes). Δεδομένου ότι ο γράφος είναι άκυκλος, εξ ορισμού θα πρέπει να υπάρχει ένας κόμβος-ρίζα, στον οποίο θα τερματίζονται όλες οι διαδρομές και ο οποίος δε διαθέτει εξερχόμενη ακμή.

Η δόμηση του DODAG ξεκινά από τον ή τους κόμβο(-ους)-ρίζα και προς τούτο το πρωτόκολλο καθορίζει τρία νέα μηνύματα ελέγχου ICMPv6:

- Το μήνυμα Αιτήματος Πληροφορίας DODAG (DODAG Information Solicitation– DIS)
- Το μήνυμα Αντικειμένου Πληροφοριών DODAG (DODAG Information Object –DIO)
- Το μήνυμα Αντικειμένου Διαφήμισης Προορισμού DODAG (DODAG Destination Advertisement Object – DAO)

Ο κόμβος-ρίζα ξεκινά τη διαφήμιση της πληροφορίας σχετικά με το γράφο εκπέμποντας ένα μήνυμα DIO. Οι γειτονικοί κόμβοι λαμβάνουν και επεξεργάζονται το μήνυμα DIO και αποφασίζουν αν θα συμμετέχουν στο γράφο ή όχι, με βάση την αντικειμενική συνάρτηση, τα χαρακτηριστικά του γράφου και πιθανώς την τοπική πολιτική. Εφόσον ένας κόμβος συμμετέχει στο γράφο, έχει διαδρομή προς τον κόμβο-ρίζα, ο οποίος είναι ο κόμβος-γονέας αυτού του κόμβου. Ο κόμβος υπολογίζει μια τιμή, που ονομάζεται «βαθμός» (rank) και αντιστοιχεί στις συντεταγμένες αυτού στην ιεραρχία του γράφου. Η αντικειμενική συνάρτηση ορίζει τον τρόπο κατά τον οποίο οι μετρικές δρομολόγησης, οι στόχοι βελτιστοποίησης και οι σχετικές συναρτήσεις χρησιμοποιούνται για τον υπολογισμό του «βαθμού». Ο «βαθμός» υπολογίζεται κατά

τρόπο, ώστε να αυξάνεται στην κατεύθυνση προς τα φύλλα και να μειώνεται προς τη ρίζα. Εάν ο κόμβος πρόκειται να λειτουργήσει ως δρομολογητής κίνησης, δηλαδή δεν είναι κόμβος-φύλλο που απλά συμμετέχει στο γράφο, ξεκινά να διαφημίζει το γράφο μέσω μηνυμάτων DIO στους γείτονές του, έχοντας ενσωματώσει τη νέα πληροφορία. Οι γείτονες επαναλαμβάνουν τη διαδικασία και επιλέγουν γονέα, προστίθενται στη διαδρομή και στέλνουν διαφημιστικά μηνύματα DIO. Η διαδικασία συνεχίζεται και ο γράφος συντίθεται σταδιακά με την προσθήκη ακμών από τη ρίζα μέχρι τα φύλλα, όπου ολοκληρώνεται η διαδικασία. Κατ' αυτόν τον τρόπο κάθε κόμβος του γράφου έχει σημείου εισόδου προς το γονέα του ακολουθώντας ένα σχήμα βήμα-βήμα (hop-by-hop), ενώ οι κόμβοι-φύλλα μπορούν να αποστείλουν ένα μήνυμα προς τον κόμβο-ρίζα, προωθώντας το στο γονέα τους.
Το μήνυμα DIS αποστέλλεται για την ανίχνευση γράφων. Συγκεκριμένα, ένας κόμβος που ενεργοποιείται σε περιβάλλον όπου υπάρχει ήδη γράφος αποστέλλει μήνυμα DIS προκειμένου να ζητήσει πληροφορία σχετικά με το γράφο από τους γείτονές του, οι οποίοι ενδεχομένως ανταποκριθούν με μηνύματα DIO.

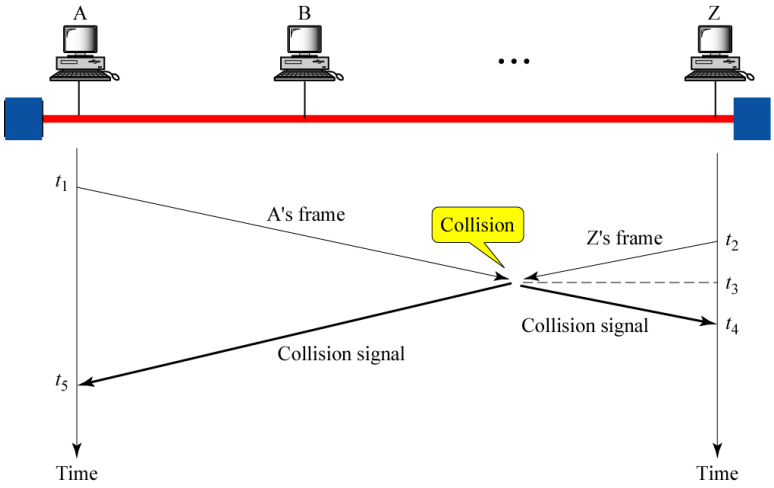
Τέλος, ο γράφος που δομεί το RPL αποτελεί μια λογική τοπολογία δρομολόγησης πάνω από το φυσικό δίκτυο, η οποία ικανοποιεί συγκεκριμένα κριτήρια, όπως αυτά ορίζονται στην αντικειμενική συνάρτηση. Ο διαχειριστής του δικτύου μπορεί να επιλέξει την ενεργοποίηση πολλαπλών γράφων ταυτοχρόνως, ώστε να δρομολογείται κίνηση με διαφορετικές απαιτήσεις. Σύμφωνα με αυτήν την προσέγγιση, κάθε κόμβος δύναται να συμμετέχει σε περισσότερους του ενός γράφους (ή στιγμιότυπα RPL) και να σηματοδοτεί την κίνηση σύμφωνα με τα χαρακτηριστικά του γράφου μέσω του οποίου μεταφέρεται, ώστε να ικανοποιούνται περιορισμοί και απαιτήσεις QoS και να εξυπηρετούνται ταυτόχρονα διαφορετικές υπηρεσίες.

2.3.3 CSMA

Σε όλα τα ασύρματα δίκτυα υπάρχουν περισσότεροι από έναν υπολογιστές που αναγκάζονται να μοιραστούν το ίδιο κανάλι για μεταφορά των δεδομένων τους. Επομένως αν δύο ή περισσότεροι υπολογιστές προσπαθήσουν ταυτόχρονα να στείλουν πακέτα στο ίδιο κανάλι, τα πακέτα τους θα συγκρουστούν με αποτέλεσμα την

καταστροφή των πακέτων. Ως αποτέλεσμα, πρέπει να βρεθεί ένας τρόπος αν δύο ή περισσότεροι υπολογιστές πρόκειται να στείλουν πακέτα στο ίδιο κανάλι.

Το CSMA (Carrier sense multiple access)[34] είναι ένα πρωτόκολλο ταυτόχρονης πρόσβασης στο ίδιο κανάλι. Το CSMA είναι μια βελτιωμένη έκδοση του πρωτόκολλου ALOHA. Ο κάθε υπολογιστής δεν στέλνει αμέσως μόλις έχει πακέτο για να στείλει. Πρώτα 'αισθάνεται' το κανάλι και στην συνέχεια ξεκίνα να στέλνει το πακέτο του (**Σχήμα 3.3.3.1**).



Σχήμα 2.3.3.1: CSMA [34]

Το πρωτόκολλο CSMA βασίζεται στο γεγονός ότι κάθε υπολογιστής στο δίκτυο μπορεί να ελέγχει την κατάσταση του καναλιού προτού μεταδώσει πληροφορίες. Συγκεκριμένα 'αισθάνεται' το κανάλι προτού μεταδώσει το πακέτο και αποφεύγει συγκρούσεις που θα μπορούσαν να αποφευχθούν. Έχει την δυνατότητα να μειώσει την πιθανότητα αποφυγής των συγκρούσεων, αλλά όχι να τις εξαλείψει.

Όσο αφορά το κανάλι μετάδοσης αυτό μπορεί να βρίσκεται σε δύο διαφορετικές καταστάσεις:

- Κατάσταση αργίας (idle state): στη κατάσταση αυτή κανένας υπολογιστής δεν επιχειρεί να στείλει κανένα πακέτο στο κανάλι, και το κανάλι είναι ελεύθερο για μετάδοση.

- Κατάσταση μετάδοσης (transmission state): στη κατάσταση αυτή κάποιος υπολογιστής έχει ξεκινήσει την αποστολή κάποιου αριθμού πακέτων και έτσι το κανάλι είναι κατειλημμένο.

Ο υπολογιστής όταν έχει πακέτο για αποστολή 'αισθάνεται' το κανάλι πρώτα. Εάν το κανάλι είναι κατειλημμένο, ο υπολογιστής περιμένει για τυχαίο χρόνο και μετά 'αισθάνεται' ξανά το κανάλι. Εάν το κανάλι είναι σε κατάσταση αργίας, ο υπολογιστής στέλνει τα πακέτα του αμέσως. Τέλος εάν προκύψει σύγκρουση στο πακέτο, ο υπολογιστής περιμένει για τυχαίο χρόνο προκειμένου να ξεκινήσει από την αρχή.

2.4 Σχεδιαστικοί περιορισμοί

Υπάρχουν συγκεκριμένοι περιορισμοί που προέρχονται από τις ευαίσθητα σημεία των ασύρματων δικτύων, οι οποίοι πρέπει πάντοτε να λαμβάνονται υπόψη, στο σχεδιασμό ασύρματων κόμβων. Τέτοιου είδους περιορισμοί, απαριθμούνται και αναλύονται κατωτέρω ως ακολούθως [6][7]:

- **Δυναμική τοπολογία και περιβάλλον λειτουργίας:** Καθότι κάποιοι κόμβοι ενός ασύρματου δικτύου μπορούν να χαρακτηριστούν ως αναξιόπιστοι, υπάρχουν πιθανότητες μεταβολής της τοπολογίας αυτού. Εξ' υπαιτιότητας της εξασθένησης της ενέργειας του κόμβου, ενδείκνυται να εμφανιστούν σφάλματα, όπως και τερματισμός της λειτουργίας, χωρίς οποιαδήποτε προειδοποίηση ως προς τους υπόλοιπους κόμβους. Ένας λόγος για τον οποίο μπορεί να επέλθει η δυσλειτουργία των κόμβων καθώς και η καταστροφή των συσσωρευμένων πληροφοριών τους, είναι το ευμετάβλητο περιβάλλον στο οποίο βρίσκονται είναι συγκεντρωμένοι. Προκειμένου να αντιμετωπιστεί το πρόβλημα, χρησιμοποιείται η υποστήριξη ευελιξίας και επεκτασιμότητας (flexibility scalability) μέσω της ομαδοποίησης (clustering) και της επικοινωνίας πολλαπλών αλμάτων (multi – hop).
- **Περιορισμένοι πόροι:** Η πηγή ενέργειας είναι δύσκολο να αντικατασταθεί για τον λόγο ότι οι κόμβοι εναποθέτονται σε περιοχές στις οποίες υπάρχει δύσκολη προσβασιμότητα. Αυτό έχει ως αποτέλεσμα, ο χρόνος ζωής του κόμβου να εξαρτάται αποκλειστικά από τον χρόνο εξασθένισης της μπαταρίας του. Προκειμένου να

εξασφαλιστεί η επέκταση ζωής του συστήματος, χρειάζεται να γίνεται χρήση των πρωτόκολλων εξοικονόμησης ενέργειας. Αυτό γίνεται καθότι, η δύναμη του κόμβου εξαντλείται κατά την αποστολή και την λήψη δεδομένων. Είναι θεμιτό, αλγόριθμοι οι οποίοι έχουν μειωμένη πολυπλοκότητα να πορεύονται στη μείωση του υπολογιστικού χρόνου και της καταναλισκόμενης ισχύος. Περαιτέρω, για να επέλθει η παράδοση των δεδομένων χρειάζονται τεχνικές οι οποίες αποδίδουν τον καθορισμό τους εύρους ζώνης.

- **Πυκνή και τυχαία τοποθέτηση των κόμβων:** Τα ασύρματα δίκτυα αισθητήρων ευρίσκονται σε αδιάβατες περιοχές σε τυχαία σειρά, αποτελούνται δε από μεγάλο αριθμό κόμβων. Προκειμένου να εξοικονομηθεί ενέργεια, ο κάθε κόμβος, αντί να βρίσκεται σε στάσιμη ενεργή κατάσταση, προβαίνει σε εναλλαγή της λειτουργίας του, εξαρτώμενος από τις απαιτήσεις που υπάρχουν μεταξύ των καταστάσεων off, sleep, idle, εκπομπής, λήψης και αστοχίας. Ανεξάρτητα της καταστάσεως στην οποία βρίσκονται οι κόμβοι, το δίκτυο επιβάλλεται όπως παράγει συνδέσεις από μόνο του. Για να είναι επιτυχής η συμμετρική εξασθένηση ενέργειας του δικτύου, πρέπει να χρησιμοποιηθεί η ανακατεύθυνση των πακέτων μέσω διαδρομών όπου οι κόμβοι διαθέτουν μεγαλύτερα αποθέματα ενέργειας. Η πράξη αυτή ονομάζεται αυτοπροσδιορισμός του δικτύου (self configuration).

- **Ανάγκη ειδικών μηχανισμών δρομολόγησης και μετάδοσης δεδομένων:** Απαιτούνται διαφορετικά πρωτόκολλα καθώς και κατάλληλος σχεδιασμός του δικτύου, ούτως ώστε να μπορέσουν να συνυπάρξουν διαφορετικές ανάγκες δρομολόγησης, από τα παραδοσιακά δίκτυα.

- **Ασύρματο μέσο επιρρεπές σε σφάλματα:** αποτελεί επακόλουθο η εμφάνιση φαινομένων εξασθένησης του σήματος, και περιορισμένης ασφάλειας, καθότι στο περιβάλλον στο οποίο μπορούμε να συναντήσουμε τους κόμβους επικρατεί υψηλός θόρυβος. Σε ένα τέτοιο περιβάλλον εφαρμογής θα ήταν θεμιτή η εξακρίβωση των δεδομένων σε όλα τα επίπεδα του δικτύου αλλά και τις λειτουργίες συντήρησης.

- **Πλεονασμός Δεδομένων:** Διά να εμφανιστεί ο πλεονασμός δεδομένων, χρειάζεται η πυκνή τοποθέτηση των κόμβων. Προκειμένου να αποφευχθεί η μεταφορά

περισσού όγκου δεδομένων από τους κόμβους, πρέπει να επιτευχθεί η συνεργατική επεξεργασία των πληροφοριών, συγχώνευση δεδομένων (data fusion) και υπολογισμοί εντός του δικτύου αισθητήρων. Ο κάθε κόμβος, επεξεργάζεται δεδομένα, και αποστέλλει μόνο τα αποτελέσματα σε αντίθεση με την άμεση αποστολή προς τον δέκτη δεδομένων.

2.5 Εφαρμογές ασύρματων δικτύων αισθητήρων

Χρησιμοποιώντας τα ασύρματα δίκτυα αισθητήρων, επιτυγχάνουμε την κάλυψη ευρέος φάσματος εφαρμογών, σε περισσότερο από ένα πεδίο. Για παράδειγμα, κάποια από τα πεδία όπου τα ασύρματα δίκτυα αισθητήρων εφαρμόζονται είναι σε μικρό – χειρουργικές επεμβάσεις, στην εκπαίδευση των νέων, σε πόλεμο, γενικότερα σε παρακολούθηση του περιβάλλοντος. Περαιτέρω δε, τεκμαίρεται ότι τα δίκτυα ασύρματων αισθητήρων θα εφαρμοστούν σε εξερεύνηση του διαστήματος.

Μπορεί να λεχθεί ότι τα ασύρματα δίκτυα αισθητήρων, θα χρησιμοποιούνται στο άμεσο μέλλον καθότι υποστηρίζουν καινούριες ευκαιρίες, στην μεταξύ των ανθρώπων και του φυσικού της κόσμου αλληλεπίδραση. Το ασύρματο δίκτυο αισθητήρων έχει καταφέρει να έχει υψηλή κλίμακα με χαμηλή ισχύ και χαμηλό κόστος, γεγονός το οποίο προέκυψε λόγω της πρόσφατης ανάπτυξης των ασύρματων επικοινωνιών.

Θεωρείται ότι υπάρχουν πολλά πλεονεκτήματα, μετά την ανάπτυξη η οποία επήλθε στα ασύρματα δίκτυα. Τέτοιες είναι η μεγάλη κλίμακα, η πυκνή ανάπτυξη, η οποία εξασφαλίζει καλύτερη κάλυψη του χώρου καθώς και πολύ καλύτερη ανάλυση. Επιπλέον αυξάνεται η αξιοπιστία και η ανθεκτικότητα του συστήματος.

Τέλος, αναλύονται κατωτέρω, κάποιες εφαρμογές των ασύρματων δικτύων. [3]

- Στρατιωτικές Εφαρμογές

Ο σκοπός των κόμβων, στις στρατιωτικές εφαρμογές, είναι η παρακολούθηση του περιβάλλοντος, κυρίως του εχθρού, όπου παρακολουθούν τις κινήσεις των μονάδων του

στρατού σε ξηρά και σε θάλασσα. Μπορούν επιπλέον να εντοπίζουν επιθέσεις από χημικά όπως επίσης να έχουνε πρόσβαση σε συνομιλίες των αντιπάλων και άλλα πολλά.

Η κύρια χρήση των κόμβων, είναι να ρίχνονται μέσα στο πεδίο εξερεύνησης. Ελέγχονται από χρήστη ο οποίος είναι απομακρυσμένος και συλλέγει τις πληροφορίες που του δίνει μαζεύοντας ο κόμβος.

Άλλη περίπτωση η οποία είναι αρκετά σημαντική στις εφαρμογές των αισθητήρων, είναι όταν κατηγοριοποιούνται αλγόριθμοι και δίνουν δεδομένα τα οποία συλλέγουν και τα οποία προέρχονται από σεισμικά και ακουστικά σήματα.

Μια τέτοια μέθοδος, έχει χρήση όταν αντικαθιστούνται νάρκες, οι οποίες ως γνωστό θεωρούνται πλέον απαρχαιωμένες. Δηλαδή, οι αισθητήρες θα εντοπίζουν την οποιαδήποτε εισβολή η οποία γίνεται από τον εχθρό και ενεργοποιεί σύστημα άμυνας το οποίο τον απωθεί και τον απομακρύνει. [3] .

- Περιβαλλοντική Παρακολούθηση

Λόγω των εξαιρετικών ικανοτήτων των ασύρματων δικτύων, μία άλλη ιδιαιτερότητα τους είναι να παρακολουθούν το περιβάλλον δηλαδή να προβαίνουν σε πρόβλεψη του καιρού, να ανιχνεύουν σεισμικές δραστηριότητες και πλημμύρες.

Καθότι οι κόμβοι έχουν την ιδιότητα να αισθάνονται, ‘βρίσκουν’ την θερμοκρασία η οποία υπάρχει σε ένα χώρο όπως επίσης τον φωτισμό, τα ρεύματα αέρα, την εσωτερική μόλυνση του αέρα. Όλα αυτά χρησιμοποιούνται για σωστό έλεγχο του εσωτερικού περιβάλλοντος.
Για παράδειγμα, με την απεριόριστη και συνήθως αχρείαστη χρήση της θέρμανσης, γίνεται αλόγιστη σπατάλη της θέρμανσης. Κάτι τέτοιο μπορεί να επιλυθεί με την χρήση των αισθητήριων κόμβων, κτίζοντας έτσι ένα υγιής και άνετο περιβάλλον.
Σε συνέχεια των ανωτέρω, άλλη περίπτωση όπου χρησιμοποιούνται τα ασύρματα δίκτυα αισθητήρων είναι όταν υπάρχει περίπτωση πρόκλησης πυρκαγιάς. Σε αυτή την περίπτωση, το δίκτυο συνδυάζεται με φωτεινά σήματα τα οποία δείχνουν εξόδους

διαφυγής, σε δίκτυο μαζί με τους αισθητήρες καπνού. Μόλις ανιχνευθεί πυρκαγιά, το δίκτυο βάση του σχεδιασμού του, δεικνύει το πιο ασφαλές μονοπάτι προς την έξοδο.
Άλλες εφαρμογές είναι η παρακολούθηση κάποιων ειδών ζώων τα οποία είναι προς εξαφάνιση. Μελετώντας με αισθητήρες ή ακόμα και με την χρήση ψηφιακής κάμερας στον κάθε κόμβο, το περιβάλλον στο οποίο ζουν διάφορα είδη μπορεί να επιφέρει πολλά θετικά αποτελέσματα [3]

- Εφαρμογές Υγείας

Άλλη ιδιότητα που παρέχουν τα δίκτυα αισθητήρων, είναι στον τομέα της υγείας, δηλαδή στην παρακολούθηση των ασθενών αλλά και σε κάποιες περιπτώσεις των ιατρών, εντός και εκτός του νοσοκομείου. Η χρήση ασύρματων αισθητήρων βοηθούν στην παρακολούθηση ασθενειών όπως το Alzheimer και να τις ελέγχει στο πρώιμο τους στάδιο. Οι κόμβοι έχουν τέτοιες ιδιότητες οι οποίες τους επιτρέπουν να καταγράφουν και να αποθηκεύουν συμπεριφορές ατόμων τα οποία αντιμετωπίζουν τις ασθένειες και να μελετούνται από ειδικούς.

Σε συνέχεια των πιο πάνω, τα ασύρματα δίκτυα αισθητήρων μπορούν να εφαρμοστούν και σε ότι αφορά την όραση των ατόμων. Η πρόσθεση ενός τεχνητού αμφιβληστροειδούς χιτώνα, ο οποίος αποτελείται από πολλούς μικροαισθητήρες, θα βοηθήσει στην επαναφορά όρασης κάποιου ατόμου, εφαρμογή, η οποία προέρχεται από τα ασύρματα δίκτυα αισθητήρων. Η δουλειά του συστήματος, είναι να επεξεργάζεται την εικόνα για αναγνώριση και επικύρωση, δίνοντας μια ανάδραση στον ασθενή για καλύτερο έλεγχο. Αυτό έχει ως αποτέλεσμα, την παροχή βοήθειας σε άτομα με περιορισμένη ή καθόλου όραση, ούτως ώστε να έχουν ικανοποιητικού επιπέδου όραση. Λόγω του περιορισμού της ενέργειας, δεν υπάρχει ακόμη η οποιαδήποτε δυνατότητα εφαρμογής της πιο πάνω ιδέας. [56][3].

Κεφάλαιο 3

Ασφάλεια Δικτύων

3.1 Στόχοι Ασφάλειας

Κατά την εξέταση της ασφάλειας των ασύρματων δικτύων αισθητήρων, είναι επιτακτική ανάγκη όπως ο καθένας ξεχωριστά διασφαλίσει τους παρακάτω στόχους είτε μερικώς είτε εξ' ολοκλήρου, και συγκεκριμένα:

3.1.1 Εμπιστευτικότητα

Το σημαντικότερο κομμάτι της ασφάλειας των δικτύων είναι ίσως η ασφάλεια των δεδομένων. Για αυτό το λόγο η διαφύλαξη των δεδομένων, δηλαδή η *εμπιστευτικότητα* (Confidentiality) [8][9][10] επιδιώκετε πρώτιστα από τον μηχανισμό ασφαλείας σε κάθε δίκτυο. Ένα δίκτυο αισθητήρων δεν πρέπει να διαρρεύσει σε άλλα δίκτυα, τις οποιεσδήποτε πληροφορίες που συλλέγονται από τους αισθητήρες. Οι κόμβοι ανταλλάσσουν ευαίσθητα στοιχεία μεταξύ τους, και προκειμένου να εξασφαλιστεί η προστασία τους, κρυπτογραφούνται με ένα μυστικό κλειδί που μόνο οι παραλήπτες των μηνυμάτων το γνωρίζουν. Πέραν τούτου, δημιουργούνται ασφαλή κανάλια επικοινωνίας μεταξύ των κόμβων και των σταθμών βάσεων. Επίσης είναι πολύ σημαντικό να διαφυλάσσονται ακόμα και οι δημόσιες πληροφορίες όπως είναι οι ταυτότητες των αισθητήρων ή τα δημόσια κλειδιά.

3.1.2 Αυθεντικοποίηση

Καθότι υπάρχει ο φόβος, ότι ένας επιτιθέμενος μπορεί να τροποποιήσει τα μηνύματα με σχετικά μεγάλη ευκολία, υπάρχει η ανάγκη για *αυθεντικοποίηση* (Authentication)

[8][9][10], δηλαδή για διαβεβαίωση του δέκτη για την προέλευση των δεδομένων, δηλαδή από ποιον αποστολέα έχουν σταλεί. Στην ασφάλεια των δικτύων γίνεται ένας έλεγχος για να εξακριβωθεί εάν η ταυτότητα του αποστολέα είναι όντως αυτή που πρέπει.

3.1.3 Διαθεσιμότητα

Τα στοιχεία του δικτύου οφείλουν να είναι διαθέσιμα ανά πάσα στιγμή, στους χρήστες οι οποίοι έχουν εξουσιοδότηση πρόσβασης και το δίκτυο αισθητήρων οφείλει να εξασφαλίσει την *διαθεσιμότητα* (Availability) [8][9][10] των υπηρεσιών του δικτύου. Το δίκτυο αισθητήρων οφείλει να προστατεύει τους πόρους, προκειμένου να μειώσει την κατανάλωση της ενέργειας στο ελάχιστο με σκοπό να εξασφαλίσει τη διαθεσιμότητα προστασίας των μηνυμάτων.

3.1.4 Ακεραιότητα

Επιπρόσθετα από τα μέτρα που λαμβάνονται για την αποφυγή πρόσβασης στα δεδομένα από χρήστες χωρίς εξουσιοδότηση, είναι σημαντικό να διατηρείται και η *ακεραιότητα* (Integrity) [8][9][10] των δεδομένων. Δηλαδή να εξασφαλίζει την ορθή μετάδοση των δεδομένων, ότι δηλαδή τα δεδομένα δεν έχουν τροποποιηθεί κατά τη μετάδοση τους, από οποιοδήποτε, χωρίς εξουσιοδότηση. Κάποιοι τρόποι με τους οποίους μπορεί να επηρεαστεί η ακεραιότητα ενός μηνύματος είναι από διαγραφή κάποιων πληροφοριών, προσθήκη κάποιων επιπλέον πληροφοριών στα δεδομένα ή την αλλοίωση του εσωτερικού των μηνυμάτων και την αποστολή του στον τελικό κόμβο , μπορεί να προκληθεί μεγάλη ζημία σε ολόκληρο το δίκτυο. Οπότε η διασφάλιση της ακεραιότητας των δεδομένων διαβεβαιώνει ότι τα δεδομένα παραδόθηκαν στον τελικό κόμβο χωρίς καμία αλλαγή.

3.2 Εργαλεία Ασφάλειας Δικτύων

Με την συνεχής ανάπτυξη του Διαδικτύου γίνονται όλο και περισσότερες επιθέσεις. Μέσα σε ένα δίκτυο υπάρχουν απεριόριστες προσβάσιμες πληροφορίες, για αυτό το λόγο απώτερος σκοπός θα πρέπει να είναι να μελετηθούν διάφορες τεχνικές οι οποίες θα μπορούν να μειώσουν τις επιθέσεις και αν είναι δυνατόν να τις εξαφανίσουν.

Για την ύπαρξη μίας πλήρης προστασίας ενός υπολογιστή ή οργανισμού θα πρέπει να λαμβάνονται υπόψη περισσότεροι από ένα τύποι ασφαλείας, καθώς επίσης και περισσότερων (πολλαπλών) εργαλείων ασφαλείας. Μερικά τέτοια εργαλεία είναι τα ακόλουθα[5]:

3.2.1 Συστήματα Ανίχνευσης Εισβολής

Τα Συστήματα Ανίχνευσης Εισβολής (Intrusion Detection Systems) [5] μπορούν να θεωρηθούν ως συστήματα παρακολούθησης και ανάλυσης των συμβάντων, που δημιουργούνται στα δίκτυα υπολογιστών. Τα συστήματα αυτά έχουν την δυνατότητα εντοπισμού μη εξουσιοδοτημένων ατόμων σε ένα δίκτυο και να προσπαθήσουν να απομακρύνουν τυχών κινδύνους που μπορεί να προκαλέσει. Αυτό μπορεί να επιτευχθεί μέσω παρακολούθησης των ροών ανταλλαγής πακέτων μεταξύ των κόμβων. 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. Υπάρχουν πολλοί και σημαντικοί λόγοι που θα ήταν καλό η εγκατάσταση ενός Συστήματος Ανίχνευσης Εισβολής. Οι πιο σημαντικοί από τους λόγους αυτούς 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.

3.2.2 Κρυπτογραφικά Συστήματα

Η σημασία της κρυπτογραφίας (Cryptographic Systems)[5] είναι τεράστια στους τομείς της ασφάλειας δικτύων. Ο κύριος στόχος της είναι να παρέχει μηχανισμούς ώστε 2 ή περισσότερα άκρα επικοινωνίας (π.χ. άνθρωποι, προγράμματα υπολογιστών κλπ.) να ανταλλάξουν μηνύματα, χωρίς κανένας τρίτος να είναι ικανός να διαβάζει την περιεχόμενη πληροφορία εκτός από τα δύο κύρια άκρα. Όταν το μήνυμα φτάσει στο δεύτερο άκρο τότε αυτό είναι υπεύθυνο να αποκρυπτογραφήσει το μήνυμα με την ύπαρξη του κατάλληλου κλειδιού. Το βασικότερο μειονέκτημα των Συστημάτων

Κρυπτογραφίας είναι ότι δεν μπορούν να διαχωρίσουν τον εξουσιοδοτημένο χρήστη από τον μη, αν έχουν τα ίδια κλειδιά στην κατοχή τους.

3.2.3 Τείχος Προστασίας

Το Τείχος Προστασίας (Firewall) [5] είναι από τους πρώτους μηχανισμούς ο οποίος θα αντιμετωπίσει κάποια απειλή την οποία θα δεχτεί το δίκτυο. Όποια πακέτα θα θεωρηθούν κακόβουλα για το δίκτυο θα απαγορευτούν να εισέλθουν σε αυτό. Εν συντομία αυτό που κάνει το Τείχος Προστασίας είναι να επιβλέπει την ροή κίνησης των πακέτων απαγορεύοντας τους να εισέλθουν ή να εξέλθουν από το δίκτυο με βάση κάποιων περιορισμών τους οποίους καθορίζει το κάθε δίκτυο ξεχωριστά. Αν κάποιος κακόβουλα, βρίσκεται ήδη μέσα στο δίκτυο, το Τείχος Προστασίας δεν μπορεί να σταθεί ασπίδα προστασίας και για αυτό αποτελεί το βασικό του μειονέκτημα.

3.3 Επιθέσεις στα δίκτυα

Λόγω του μέσου μετάδοσης τα ασύρματα δίκτυα είναι ευπαθή σε διάφορου τύπου επιθέσεις. Στα ασύρματα δίκτυα, επίθεση μπορεί να θεωρηθεί οποιαδήποτε ενέργεια που έχει την δυνατότητα να παραβιάσει την ασφάλεια της πληροφορίας. Μία επίθεση μπορεί να γίνει για διάφορους λόγους. Ο επιτιθέμενος ίσως να θέλει να αποκτήσει πρόσβαση στο δίκτυο για να ελέγξει την κίνηση του δικτύου ή να θέλει να κλέψει κάποιες πληροφορίες που υπάρχουν μέσα στο δίκτυο. Οι διάφορες επιθέσεις στα ασύρματα δίκτυα μπορούν να κατηγοριοποιηθούν σε δύο είδη επιθέσεων. Τις *ενεργητικές επιθέσεις* (active) και τις *παθητικές επιθέσεις* (passive). [24][30][31]

3.3.1 Ενεργητικές Επιθέσεις

Ως ενεργητικές επιθέσεις μπορούν να χαρακτηριστούν αυτές οι οποίες απαιτούν μεγάλου μεγέθους αλληλεπίδραση προς το στόχο από αυτό που επιτίθεται και εκτελεί ενέργειες. Συγκεκριμένα είναι όλες οι επιθέσεις που δεν ανήκουν στις παθητικές επιθέσεις.[30][31]

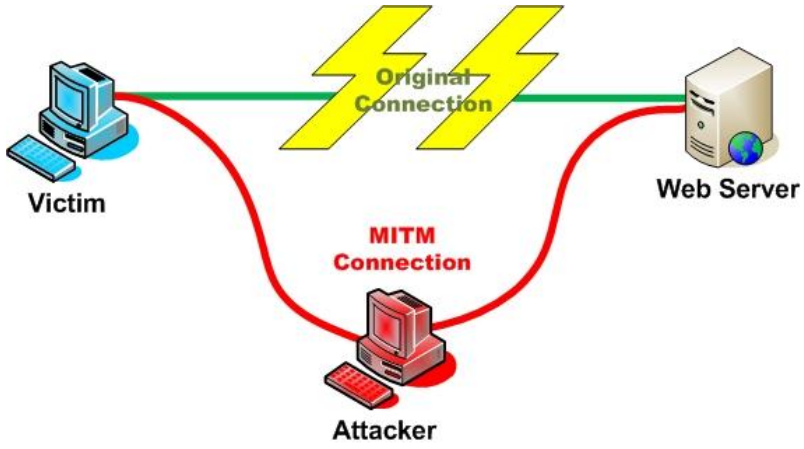
Υπάρχουν τρία είδη ενεργητικών επιθέσεων:

- Επιθέσεις άρνησης υπηρεσίας (Denial of Service)
- Μη εξουσιοδοτημένης πρόσβασης επιθέσεις (Unauthorized Access)
- Επιθέσεις τροποποίησης μηνυμάτων (Man in the Middle Attack)

Οι πιο διαδεδομένες επιθέσεις μπορούν να θεωρηθούν οι επιθέσεις άρνησης υπηρεσίας. Οι επιθέσεις αυτές έχουν την δυνατότητα να αχρηστεύουν το δίκτυο. Ένα είδος επίθεσης άρνησης υπηρεσίας είναι η επίθεση πλημμύρας (Flood Attack) όπου ο επιτιθέμενος αποστέλλει μεγάλο αριθμό πακέτων μέσα στο δίκτυο με σκοπό να καταναλώσει όλη την επεξεργαστική ισχύ του δικτύου.

Οι μη εξουσιοδοτημένης πρόσβασης επιθέσεις δεν στοχεύουν κάποιο συγκεκριμένο χρήστη, αλλά ολόκληρο το δίκτυο. Ανάλογα με την αρχιτεκτονική του δικτύου, ο επιτιθέμενος μπορεί να αποκτήσει μερικά ή όλα τα δικαιώματα του δικτύου. Ο επιτιθέμενος με αυτή την τεχνική έχει την δυνατότητα να αντιγράψει το όνομα του δικτύου και να δημιουργήσει ένα άλλο με πιο δυνατό σήμα έτσι ώστε οι χρήστες να συνδέονται στο ψεύτικο δίκτυο και να μεταδίδουν τα μηνύματά τους από αυτό.

Στις επιθέσεις τροποποίησης μηνυμάτων ο επιτιθέμενος με έμμεσο τρόπο αποκτά τα δεδομένα. Ο επιτιθέμενος στις επιθέσεις αυτές βρίσκεται στην μέση τις συνομιλίας και εμφανίζεται στον χρήστη ως το access point και στο access point ως ο χρήστης, με επακόλουθο ο επιτιθέμενος να διαβάζει πρώτος τα μηνύματα και να έχει την δυνατότητα μετατροπής τους. Δύο μηχανισμοί ασφαλείας που έχουν αναπτυχθεί για τέτοιου είδους επιθέσεις είναι το IPSec και το VPN (**Σχήμα 3.3.1**).



Σχήμα 3.3.1 : Man in the Middle Attack [35]

3.3.2 Παθητικές Επιθέσεις

Ως παθητικές επιθέσεις μπορούν να χαρακτηριστούν αυτές οι οποίες απαιτούν μικρού μεγέθους αλληλεπίδραση προς το στόχο από αυτό που επιτίθεται και εκτελεί ενέργειες. Ο στόχος των παθητικών επιθέσεων δεν είναι να βλάψουν άμεσα το θύμα αλλά ούτε να του προκαλέσουν οποιαδήποτε αλλαγή στην κατάσταση του. Ο επιτιθέμενος έχει σαν στόχο την παρακολούθηση αλλά και την συλλογή πληροφοριών από το θύμα. Οι παθητικές επιθέσεις, μπορούν να χαρακτηριστούν ως ενέργειες, οι οποίες γίνονται προτού επέλθει μια άλλη επίθεση. Περαιτέρω, για να φέρει εις πέρας μια κύρια επίθεση, ο επιτιθέμενος θα προβεί σε συλλογή πληροφοριών, τις οποίες θα εκμεταλλευτεί. [30][31]

Υπάρχουν δύο είδη παθητικών επιθέσεων:

- Συλλογή πακέτων (packet sniffing)
- Συλλογή πληροφοριών (traffic analysis)

Με τις επιθέσεις συλλογής πακέτων ο επιτιθέμενος έχει την ικανότητα να παρακολουθεί όλα τα πακέτα από την επικοινωνία που έχει το θύμα με το υπόλοιπο δίκτυο και ανήκουν στην δικτυακή κίνηση. Επίσης ο επιτιθέμενος έχει την ικανότητα να διαβάζει το περιεχόμενο των πακέτων, αν το μήνυμα είναι κρυπτογραφημένο πρέπει να το αποκρυπτογραφήσει πρώτα. Η συλλογή πακέτων μπορεί να υλοποιηθεί από ειδικά προγράμματα τα οποία ονομάζονται sniffers.

Με τις επιθέσεις συλλογής πληροφοριών ο επιτιθέμενος έχει την ικανότητα να αποκτήσει πληροφορίες που προέρχονται από ένα access point. Αυτό έχει ως αποτέλεσμα να γνωρίζει την μέθοδος κρυπτογράφησης , αν γίνεται , τις διευθύνσεις MAC, το όνομα του δικτύου και το κανάλι εκπομπής.

Κεφάλαιο 4

Επιθέσεις στα Ασύρματα Δίκτυα Αισθητήρων

4.1 Επιθέσεις στα ασύρματα δίκτυα

Γενικότερα τα δίκτυα αντιμετωπίζουν κακόβουλες επιθέσεις. Οι επιθέσεις αυτές στοχεύουν τις υπηρεσίες που παρέχονται από τα δίκτυα, καθώς επίσης τα δεδομένα που αποθηκεύονται στους κόμβους, αλλά και αυτά που μεταδίδονται μέσα στο δίκτυο. Κι αυτό γιατί, η επικοινωνία με τη χρήση ασύρματων μέσων είναι εύκολο να υποκλαπεί , εξίσου εύκολη με τη μεταφορά ψευδών πληροφοριών στο δίκτυο (Πίνακας 4.1.1). [11][24]

Είδος Επίθεσης	**Περιγραφή**
Επίθεση βρόχου δρομολόγησης (Routing loop attack)	Ατέρμονη δρομολόγηση, ώστε τα πακέτα να μη φτάσουν τον προορισμό τους
Επίθεση σκουληκότρυπας (Wormhole attack)	Ένας αριθμός κακόβουλων κόμβων προσποιούνται ότι συνδέουν δύο απομακρυσμένα σημεία του δικτύου, προκαλώντας επιπλοκές στο φόρτο και τη ροή της κίνησης
Επίθεση μαύρης τρύπας (Black-hole attack)	Αποδοχή όλων των αιτημάτων δρομολόγησης, ακόμα και με ελλιπή στοιχεία δρομολόγησης. Η μαύρη τρύπα απορρίπτει όλα τα πακέτα που φτάνουν σε αυτή
Επίθεση γκρίζας τρύπας (Grey-hole attack)	Επιλεκτική απόρριψη πακέτων
Επίθεση τρύπας προορισμού	Ο κακόβουλος κόμβος φροντίζει να

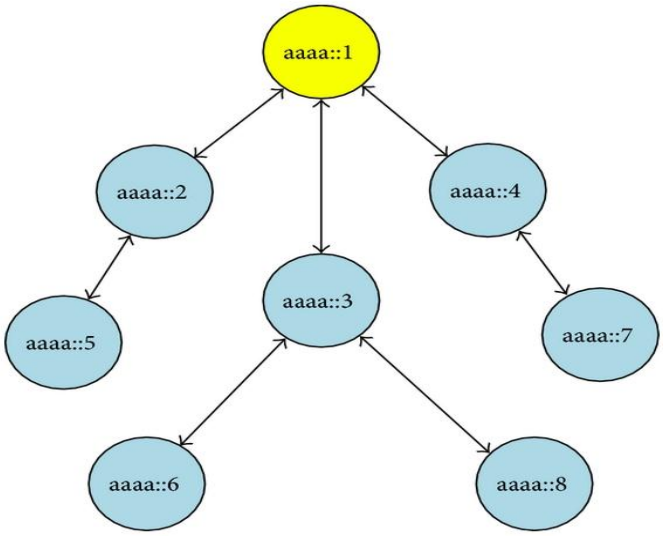
(Sink-hole attack)	φαίνεται ελκυστικός όσον αφορά τη δρομολόγηση πακέτων προς τον προορισμό, οπότε μετά εφαρμόζει επιθέσεις μαύρης ή γκρίζας τρύπας.
Επίθεση άρνησης υπηρεσίας (Denial-of-Service – DoS)	Μπλοκάρισμα της φυσιολογικής λειτουργίας ή διαχείρισης των πόρων επικοινωνιών (π.χ. προκαλώντας υπέρμετρη ενεργειακή κατανάλωση)
Παραποίηση/εισαγωγή πακέτου (Packet modification/insertion)	Παραποίηση της πληροφορίας που λαμβάνει ο κακόβουλος κόμβος και προώθηση του παραποιημένου πακέτου ή νέων ψευδών πακέτων
Επίθεση Sybil (Sybil attack)	Διαρροή πολλαπλών ταυτοτήτων στο δίκτυο επηρεάζοντας τη διατήρηση της τοπολογίας και τα σχήματα ανοχής σε σφάλματα
Επίθεση Αναμετάδοσης (Replay attack)	Αναμετάδοση προηγούμενων πακέτων στο δίκτυο
Επίθεση επιλεκτικής κακής συμπεριφοράς (Selective misbehaving attack)	Επιλεκτική παροχή ή άρνηση υπηρεσιών
Επίθεση πλημμύρα (Flood attack)	Αποστολή αιτημάτων σύνδεσης σε τακτά χρονικά διαστήματα.

(Πίνακας 4.1.1) : Επιθέσεις στα Ασύρματα Δίκτυα

4.2 Επιθέσεις στο RPL και IPv6

Το RPL χρησιμοποιείται κυρίως σε 6LoWPAN δίκτυα και δημιουργεί ένα κατευθυνόμενο άκυκλο γράφο (DAG) μεταξύ των κόμβων. Υποστηρίζει μονής κατεύθυνσης κυκλοφορίας προς μία ρίζα (sink) και αμφίδρομη κυκλοφορία μεταξύ των υπόλοιπων κόμβων. Κάθε κόμβος έχει ως αναγνωριστικό μία μοναδική IPv6 διεύθυνση (node ID) , μία λίστα με τους γείτονες του και ένα κόμβο γονέα. Επιπλέον κάθε κόμβος στο γράφο έχει ένα βαθμό (rank) ο οποίος δείχνει τη θέση του σε σχέση με τη ρίζα. Οι βαθμοί αυξάνονται από τη ρίζα προς τα κάτω (όπως παρουσιάζονται στο **Σχήμα 4.2.1**).

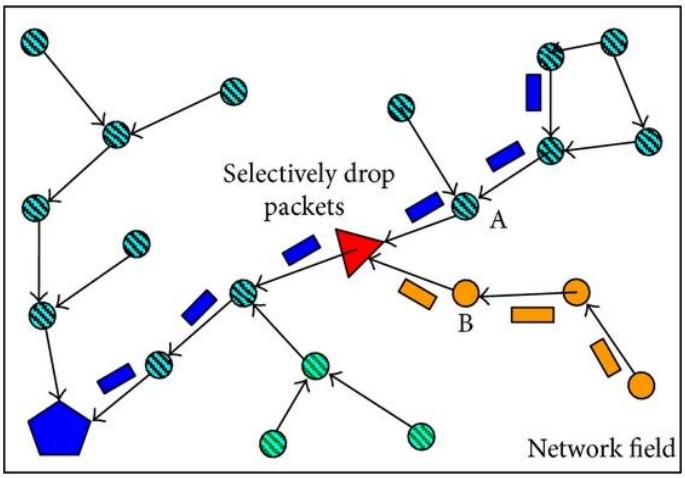
Στην συνέχεια αναλύονται διάφορες επιθέσεις που συναντούμε στα ασύρματα δίκτυα αισθητήρων στο πρωτόκολλο RPL [13] [12].



Σχήμα 4.2.1: Παράδειγμα RPL DODAG

4.2.1 Επίθεση Επιλεκτικής - Προώθησης

Μια επιλεκτική – προώθηση επίθεση (selective - forwarding attack) [13][26][27] έχει την δυνατότητα να αχρηστεύουν το δίκτυο (Denial of Service). Ένας κόμβος λαμβάνοντας ένα πακέτο από ένα γειτονικό του κόμβο, το προωθεί σε ένα άλλο γειτονικό του κόμβο , σύμφωνα με το πρωτόκολλο δρομολόγησης που έχει καθοριστεί. Στην επίθεση αυτή ένας κακόβουλος κόμβος ο οποίος εισέρχεται στο δίκτυο θα προωθήσει επιλεκτικά ορισμένα πακέτα, απορρίπτοντας τα υπόλοιπα, με σκοπό να διαταράξουν τα μονοπάτια δρομολόγησης (**Σχήμα 3.6.1.1**). Επέκταση της επίθεσης επιλεκτικής προώθησης θεωρείται η επίθεση μαύρης τρύπας (blackhole attack), στην οποία ο προσβεβλημένος κόμβος απορρίπτει κάθε πακέτο που λαμβάνει χωρίς να το προωθεί. Μια επίθεση selective – forwarding μπορεί να έχει καταστροφικές συνέπειες όταν συνδυαστεί με άλλες επιθέσεις, για παράδειγμα μια επίθεση sinkhole.



Σχήμα 4.2.1.1: Selective - Forwarding Attack

4.2.2 Επίθεση Καταβόθρας

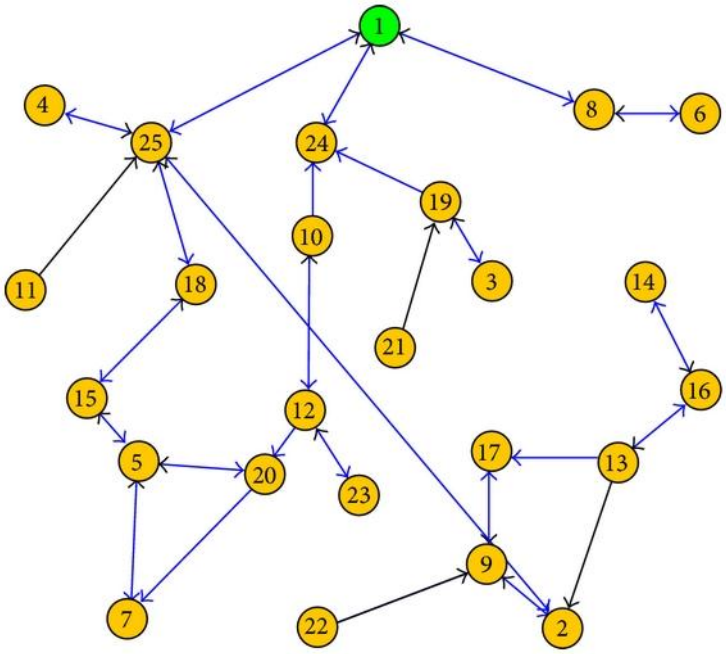
Σε μια επίθεση καταβόθρας (Sinkhole) [13] ο κακόβουλος κόμβος ο οποίος εισέρχεται στο δίκτυο, υποκλέπτει διάφορες πληροφορίες δρομολόγησης από το δίκτυο με σκοπό να τις διαχειριστεί για να γίνει ελκυστικός στους γειτονικούς κόμβους για λήψη πακέτων από αυτούς. Ως αποτέλεσμα αυτού οι γειτονικού κόμβοι επιλέγουν τον συγκεκριμένο κόμβο για την προώθηση των μηνυμάτων που λαμβάνουν. Με τον τρόπο αυτό ο επιτιθέμενος μπορεί να ελέγξει τη ροή πληροφοριών εντός του δικτύου μέσω του εισερχόμενου κακόβουλου κόμβου. Η επίθεση αυτή δεν διαταράζει από μόνη της την λειτουργία του δικτύου, ωστόσο όταν συνδυαστεί με άλλη επίθεση μπορεί να γίνει πολύ ισχυρή.

4.2.3 Επίθεση Πλημμύρας

Σε μια επίθεση πλημμύρας (flooding attack) [13][19][20][22] ο κακόβουλος κόμβος ο οποίος εισέρχεται στο δίκτυο στέλνει συνέχεια πακέτα στους άλλους κόμβους του δικτύου τα οποία είναι περισσότερα από όσα μπορεί να χειριστεί. Κύριος σκοπός της επίθεσης αυτής είναι να εξαντλήσει τους πόρους, τη μνήμη και την ενέργεια του κόμβου θύματος.

4.2.4 Επίθεση Σκουληκότρυπας

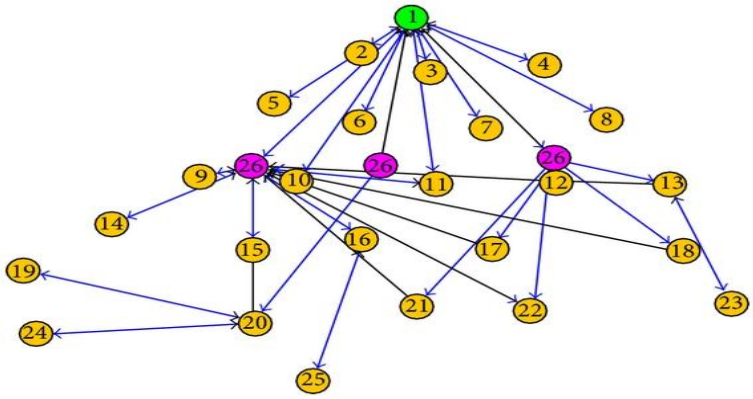
Σε μια επίθεση σκουληκότρυπας (Wormhole) [13][28] ο κακόβουλος κόμβος ο οποίος εισέρχεται στο δίκτυο έχει σκοπό την παραπλάνηση δύο απομακρυσμένων κόμβων ως προς την εγγύτητα τους, έτσι ώστε αυτοί να αναγνωρίζονται ως γειτονικοί (**Σχήμα 3.6.4.1**). Οι συγκεκριμένη επίθεση μπορεί να χρησιμοποιηθεί σε συνδυασμό με άλλες επιθέσεις, όπως την επιλεκτική προώθηση, την επίθεση καταβόθρας και τη σιβυλλική επίθεση.



Σχήμα 4.2.4.1: Επίθεση Wormhole

4.2.5 Σιβυλλική Επίθεση

Σε μια επίθεση σιβυλλική (Sybil) [13][25] ο κακόβουλος κόμβος ο οποίος εισέρχεται στο δίκτυο έχει σκοπό να δώσει πολλαπλές ταυτότητες σε ένα κόμβο. Ένας κακόβουλος κόμβος, με τον τρόπο αυτό έχει την δυνατότητα να μιμηθεί τις ταυτότητες άλλων κόμβων που βρίσκονται στο δίκτυο ή να αναπαράγει νέες ψεύτικες ταυτότητες. Οι κόμβοι οι οποίοι έχουν τις ψεύτικες ταυτότητες συμμετέχουν κανονικά στις λειτουργίες του δικτύου, αν και αποτελούν στην πραγματικότητα μόνο μια συσκευή.



Σχήμα 4.2.5.1: Sybil Attack

4.3 Ασφάλεια στα Ασύρματα Δίκτυα Αισθητήρων

Ενώ τα δίκτυα αισθητήρων έχουν ομοιότητες με πολλά άλλα κατανεμημένα συστήματα υπόκεινται σε μια πληθώρα περιορισμών. Αυτοί οι περιορισμοί επηρεάζουν τον σχεδιασμό των δικτύων και οδηγούν σε σχεδιασμό πρωτοκόλλων και αλγορίθμων που διαφέρουν από εκείνους στα υπόλοιπα κατανεμημένα συστήματα.

Τα σύρματα δίκτυα αισθητήρων πρέπει να είναι ικανά να κρατούν κρυφή, από μη εξουσιοδοτημένους χρήστες, την πληροφορία που συλλέγουν. Έτσι, για να μπορέσει να διατηρηθεί η μυστικότητα, το δίκτυο πρέπει να υποστηρίζει μηχανισμούς κρυπτογράφησης και αυθεντικότητα όπως αναλύθηκαν σε προηγούμενο κεφάλαιο.

Η χρήση τέτοιων τεχνικών επιδρούν αρνητικά τόσο στην κατανάλωση ισχύος όσο και στο διαθέσιμο εύρος ζώνης του δικτύου ενώ, η ενσωμάτωση επιπλέον bits στα μεταφερόμενα πακέτα, τα οποία περιέχουν τις πληροφορίες αυθεντικότητας, μειώνουν τον αριθμό των πραγματικών δειγμάτων που μπορούν να μεταφερθούν από ένα κόμβο.

Κεφάλαιο 5

Περιβάλλον Εργασίας

5.1 Contiki OS

5.2 Εργαλείο Προσομοίωσης Cooja

5.3 Χαρακτηριστικά Αισθητήρα

5.1 Contiki OS

Το Contiki [16][17] είναι λειτουργικό σύστημα ανοιχτού κώδικα. Αναπτύχθηκε από τον Adam Dunkels το 2002. Πλέον λαμβάνει υποστήριξη από πολλές μεγάλες εταιρείες του χώρου όπως η CISCO. Το Contiki χρησιμοποιείται για συστήματα τα οποία έχουν χαμηλή κατανάλωση και περιορισμό σε μνήμη και τα οποία θέλουμε να συνδέσουμε πάνω σε ένα δίκτυο. Η πιο διαδεδομένη χρήση του είναι για δικτυωμένες συσκευές οι οποίες έχουν μικρό κόστος και έχουν περιορισμό στη μνήμη. Παραδείγματα χρήσης του περιλαμβάνουν μετρήσεις σε έξυπνες πόλεις, όπως μέτρηση υγρασίας ή θερμοκρασίας.

Η χρήση του Contiki γίνεται όλο και πιο διαδεδομένη. Για αυτό υπάρχουν πολλοί λόγοι. Καταρχήν, είναι ανοικτού κώδικα. Εκτός αυτού, το Contiki παρέχει πλήρης διαδικτυακή υποστήριξη για τις συσκευές χαμηλής κατανάλωσης ή μικρής μνήμης. Συγκεκριμένα παρέχει υποστήριξη των IPv6 και IPv4 πρωτοκόλλων, καθώς και των standards ασύρματων πρωτοκόλλων για αυτά τα συστήματα, δηλαδή το 6lowpan, το RPL, το COAP αλλά υποστηρίζει και τα γνωστά πρωτόκολλα HTTP, UDP και TCP. Επίσης παρέχει το ContikiMAC radio duty cycling μηχανισμό, ο οποίος χρησιμοποίει ένα ισχυρό μηχανισμό για ξύπνημα των συσκευών όταν αυτές κάνουν sleep κατά τη διάρκεια μεταδόσεων μεταξύ τους, το οποίο είναι αναγκαστικό για να πετύχουν χαμηλή κατανάλωση ενέργειας. Επιπλέον, το Instant Contiki είναι μια έτοιμη πλατφόρμα στην οποία μπορεί να γίνει προσομοίωση της εφαρμογής. Οι εφαρμογές γράφονται σε γλώσσα C. Επιπλέον, η υποστήριξη είναι πολύ καλή καθώς η κοινότητα του Contiki είναι αρκετά ενεργή και το λειτουργικό σύστημα του Contiki μπορεί να τρέξει σε μια μεγάλη ποικιλία από κονσόλες, οι οποίες παρέχονται στο διαδίκτυο προς αγορά. Ο πιο εύκολος τρόπος για την εγκατάσταση του Contiki για την προσομοίωση των διαφόρων

εφαρμογών και παραδειγμάτων είναι σε περιβάλλον Ubuntu. Αξίζει να σημειωθεί πως ότι κώδικας γραφτεί για το Contiki μπορεί να χρησιμοποιηθεί ακριβώς ο ίδιος και στους αισθητήρες χωρίς οποιεσδήποτε αλλαγές.

5.2 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 [17] είναι ο προσομοιωτής δικτύου του Contiki. Χρησιμοποιείται για την οπτική αναπαράσταση των κόμβων στο Contiki και παρέχει πολλά παράθυρα και πολλές λειτουργίες στον χρήστη. Επιτρέπει την προσομοίωση μικρών ή μεγάλων δικτύων στο Contiki. Υπάρχει 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.

5.3 Χαρακτηριστικά Αισθητήρα

Οι αισθητήρες οι οποίοι θα χρησιμοποιηθούν στο προσομοιωτή Cooja είναι οι του τύπου Tmote-Sky. Αποτελεί εξέλιξη του Telosb και είναι το πιο πρόσφατο προϊόν σε μια σειρά από motes που αναπτύχθηκαν από το Πανεπιστήμιο της California, Berkeley με σκοπό τη χρήση τους σε ασύρματα δίκτυα αισθητήρων.Το Tmote-Sky είναι μια ασύρματη μονάδα (“mote”) πολύ χαμηλής κατανάλωσης ισχύος, για χρήση σε δίκτυα αισθητήρων και σε εφαρμογές καταγραφής και παρακολούθησης.

Τα χαρακτηριστικά του Tmote Sky φαίνονται περιληπτικά παρακάτω:

• Ασύρματος πομποδέκτης 250kbps 2.4 GHz IEEE 802.15.4 Chipcon

• Μικροελεγκτής 8MHz Texas Instruments MSP430 (10k RAM, 48k Flash)

• Ολοκληρωμένος ADC, DAC, Supply Voltage Supervisor και ελεγκτής DMA

• Onboard κεραία με εμβέλεια 50 m σε εσωτερικούς χώρους / 125 m σε εξωτερικούς.

• Ενσωματωμένοι αισθητήρες υγρασίας, θερμοκρασίας και φωτός.

• Χαμηλή κατανάλωση ρεύματος

• Γρήγορη αφύπνιση (<6μs)

• Κωδικοποίηση και πιστοποίηση αυθεντικότητας στο στρώμα ζεύξης υλικού

Κεφάλαιο 6

Υλοποίηση Επιθέσεων

6.1 Επίθεση Πλημμύρας

Η επίθεση πλημμύρας (flooding attack) [19][20][21][22][23]είναι μία επίθεση Άρνησης Υπηρεσίας (DoS). Η επίθεση αυτή έχει σχεδιαστεί με κύριο σκοπό να θέσει σε καταστολή ένα δίκτυο ή μια υπηρεσία. Ο κακόβουλος κόμβος ο οποίος εισέρχεται στο δίκτυο στέλνει συνέχεια πακέτα στους άλλους κόμβους του δικτύου τα οποία είναι περισσότερα από όσα μπορεί να χειριστεί. Κύριος σκοπός του επιτιθέμενου είναι να εξαντλήσει τους πόρους, τη μνήμη και την ενέργεια του δικτύου. Αυτό έχει ως αποτέλεσμα ο κακόβουλος κόμβος να γεμίζει το buffer του δικτύου και να μην μπορεί οποιοσδήποτε άλλος κόμβος να στείλει τα δικά του πακέτα.

6.2 Επίθεση επιλεκτικής προώθησης

Στη επίθεση επιλεκτικής προώθησης πακέτων (Selective – Forwarding Attack) [13][26][27], ο κακόβουλος κόμβος προωθεί τα πακέτα επιλεκτικά με κύριο στόχο την διατάραξη των μονοπατιών δρομολόγησης στα οποία συμμετέχει. Για να έχει ο επιτιθέμενος μεγαλύτερη αποτελεσματικότητα, επιλέγει κάποιο κόμβο ο οποίος βρίσκεται κοντά στον sink node. Αυτό γίνεται για να έχει την δυνατότητα εύκολης πρόσβασης στα πακέτα τα οποία κινούνται στο δίκτυο και να μπορεί να ελέγχει ακόμα περισσότερα πακέτα.

6.3 Εισαγωγή στην Υλοποίηση

Αρχικά, μελετήθηκαν ορισμένοι ιοί ως προς τον τρόπο με τον οποίο δρουν, και στη συνέχεια, προβήκαμε σε υλοποίηση ορισμένων από αυτούς. Με την βοήθεια του λειτουργικού συστήματος Contiki, και συγκεκριμένα χρησιμοποιώντας το εργαλείο Cooja, υλοποιήθηκαν και προσομοιώθηκαν οι επιθέσεις. Σε ότι αφορά το εργαλείο Cooja, έχει περιγραφεί και επεξηγηθεί ανωτέρω, ο τρόπος με τον οποίο λειτουργεί και το πως χρησιμοποιείται.

Συγκεκριμένα, πρωταρχικός σκοπός ήταν να τοποθετηθούν μερικοί κακόβουλοι κόμβοι, οι οποίοι ήταν μολυσμένοι με τους ιούς αυτούς, και στη συνέχεια να μελετηθεί ο τρόπος με τον οποίο οι ιοί, επηρεάζουν ολόκληρο το δίκτυο. Τοποθετώντας τις προσομοιώσεις των ιών, δηλαδή τους κακόβουλους κόμβους, αποτέλεσμα ήταν η λήψη ορισμένων μετρήσεων. Λαμβάνοντας τις πιο πάνω μετρήσεις, και έχοντας ουσιαστικά κάποια αποτελέσματα στην κατοχή μας, δύναται να βρεθούν τρόποι αντιμετώπισης των συγκεκριμένων ιών.

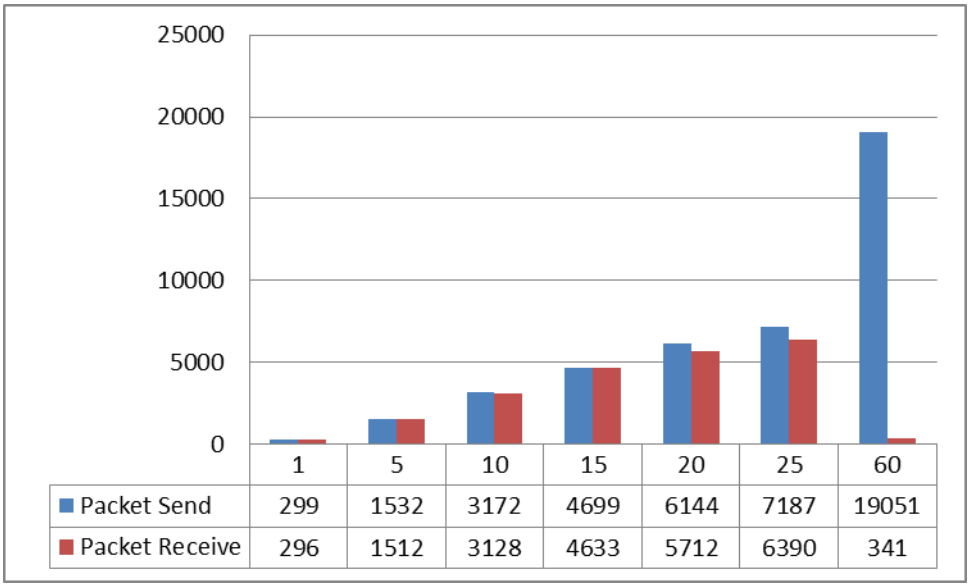
Στην συνέχεια της διπλωματικής αυτής εργασίας, παρουσιάζονται τα αποτελέσματα και τα συμπεράσματα που προέκυψαν κατά την προσομοίωση των ιών αυτών στο περιβάλλον Cooja, με την δημιουργία κατάλληλων γραφικών παραστάσεων.

6.4 Σενάρια

Αρχικά για την υλοποίηση της επίθεσης flooding πρέπει να βρούμε τη συχνότητα στην οποία ο κακόβουλος κόμβος ξεκινά να γεμίζει το buffer του, με αποτέλεσμα να απορρίπτει πακέτα και να μην καταλήγουν στο κόμβο sink. Αυτό κατέστη δυνατό ξεκινώντας με μικρή συχνότητα αποστολής πακέτων προς τον κόμβο sink αυξανόμενη συνεχώς μέχρι να βρεθεί η ζητούμενη συχνότητα.

Όπως παρατηρείται στην πιο κάτω γραφική παράσταση, η μεταβολή της συχνότητας είναι 1 πακέτο το δευτερόλεπτο σε 5,10,15,20,25 και 60. Ο κόμβος ξεκινά να χάνει πακέτα μετά όταν έχει περίοδο μεγαλύτερη από 20 πακέτα το δευτερόλεπτο. Τα πακέτα τα οποία χάνονται αρχικά από το κόμβο προς το κόμβο sink είναι τα πακέτα μέχρι να

ανακαλύψει μονοπάτι επικοινωνίας. Η συχνότητα που χρησιμοποιεί ο κακόβουλος κόμβος για να εκδηλώσει την επίθεση του είναι 60 πακέτα το δευτερόλεπτο και αυτό γίνεται για να φαίνονται τα αποτελέσματα σε πιο έντονο βαθμό.



	1	5	10	15	20	25	60
Packet Send	299	1532	3172	4699	6144	7187	19051
Packet Receive	296	1512	3128	4633	5712	6390	341

Σε όλα τα πιο κάτω σενάρια χρησιμοποιείται συχνότητα 60 πακέτα ανά δευτερόλεπτο για το κακόβουλο, 1 πακέτο ανά δευτερόλεπτο για το Benign node και η τοπολογία του δικτύου μεταβάλλεται αναλόγως του αποτελέσματος που επιθυμούμε να πετύχουμε.

Στις παρακάτω γραφικές παραστάσεις, ο άξονας y αναπαριστά τον αριθμό των πακέτων που κινούνται μέσα στο δίκτυο και ο άξονας x δείχνει τον κόμβο στον οποίο αντιστοιχεί ο αριθμός των πακέτων.

Στις τοπολογίες που παρουσιάζονται στα επόμενα σενάρια, οι κακόβουλοι κόμβοι διαφέρουν ως προς το χρώμα με τους υγιείς κόμβους. Συγκεκριμένα οι υγιείς κόμβοι ξεχωρίζουν με χρώμα κίτρινο ενώ οι μολυσμένοι παρουσιάζονται με λιλά χρώμα. Ο sink κόμβος είναι χρώμα πράσινο.

Ο λόγος που γίνεται αυτή η προσομοίωση του ιού, είναι για να χρησιμοποιηθούν οι γραφικές παραστάσεις οι οποίες προκύπτουν, ως ένα ορθό μέτρο σύγκρισης. Συγκρίνοντας δηλαδή τις γραφικές οι οποίες αντιπροσωπεύουν δίκτυα με κακόβουλους

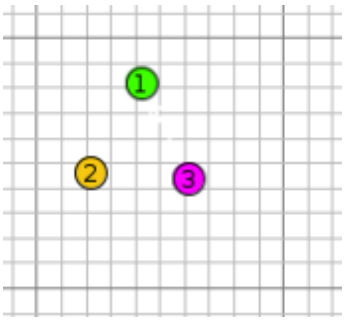
κόμβους με την γραφική ενός δικτύου με υγιείς κόμβους, μπορούν να διεξαχθούν ευκολότερα και ακριβέστερα τα συμπεράσματα.

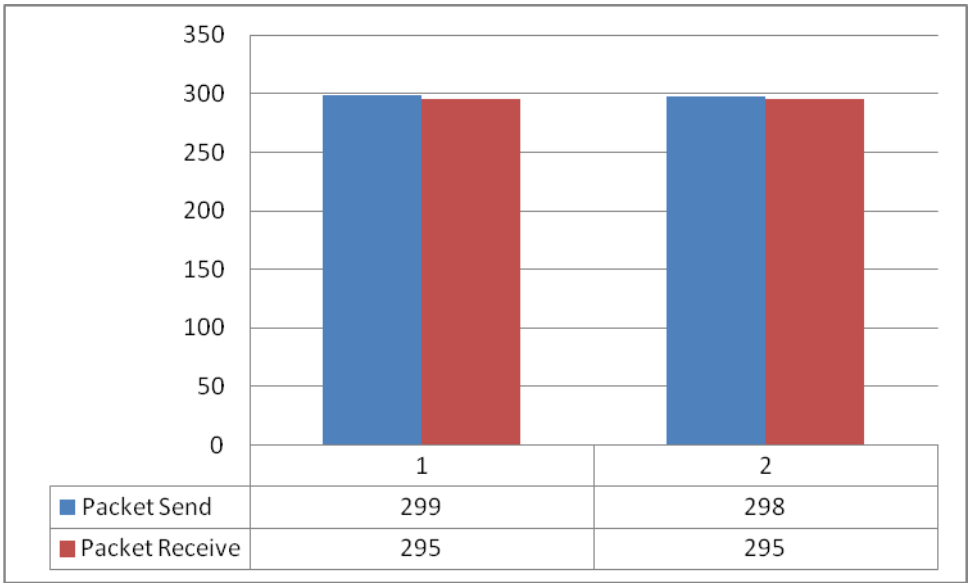
6.4.1 Sink node (1) – Benign node (1) – Malicious node (1)

Σε αυτό το σενάριο χρησιμοποιήσαμε ένας sink node στον οποίο καταλήγουν όλα τα πακέτα, ένας benign node και ένας malicious node. Κάναμε διάφορες τοπολογίες για να παρατηρήσουμε πώς ο malicious node επηρεάζει τους υπόλοιπους.

Τοπολογία 1

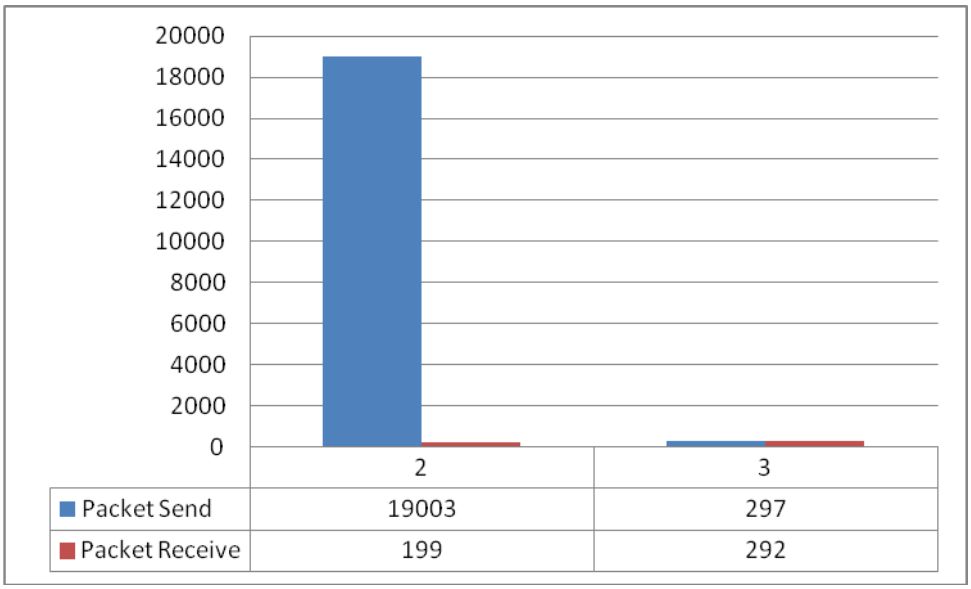
Στην πιο κάτω εικόνα φαίνεται η τοπολογία του δικτύου το οποίο χρησιμοποιώ για να πάρω τις μετρήσεις μου. Βασική προϋπόθεση είναι ο Malicious Node και ο Benign Node να βρίσκονται δίπλα – δίπλα. Ο λόγος που πρέπει να βρίσκονται δίπλα – δίπλα είναι γιατί με αυτό το τρόπο οι δύο κόμβοι είναι ανεξάρτητοι μεταξύ τους.





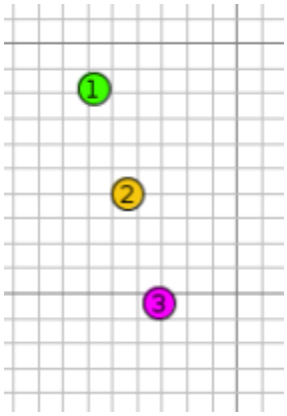
Στην πιο πάνω γραφική παράσταση με μπλε χρώμα παρατηρούμε τα πακέτα που στέλνουν οι κόμβοι 2 και 3 προς τον κόμβο sink. Οι δύο αυτοί κόμβοι δεν είναι ¨μολυσμένοι¨ και η συχνότητα αποστολής πακέτων είναι 1 πακέτο το δευτερόλεπτο. Με κόκκινο χρώμα παρατηρούμε τα πακέτα που παρέλαβε ο κόμβος sink από τους κόμβους 2 και 3. Από την γραφική παράσταση παρατηρούμε ότι όσα πακέτα στέλνουν οι κόμβοι μας ο κόμβος sink τα παραλαμβάνει. Τα 3-4 πακέτα που χάνονται είναι στα αρχικά στάδια επικοινωνίας όταν ο κόμβος εισέρχεται στο δίκτυο και προσπαθεί να δημιουργήσει σύνδεση προς το κόμβο sink.

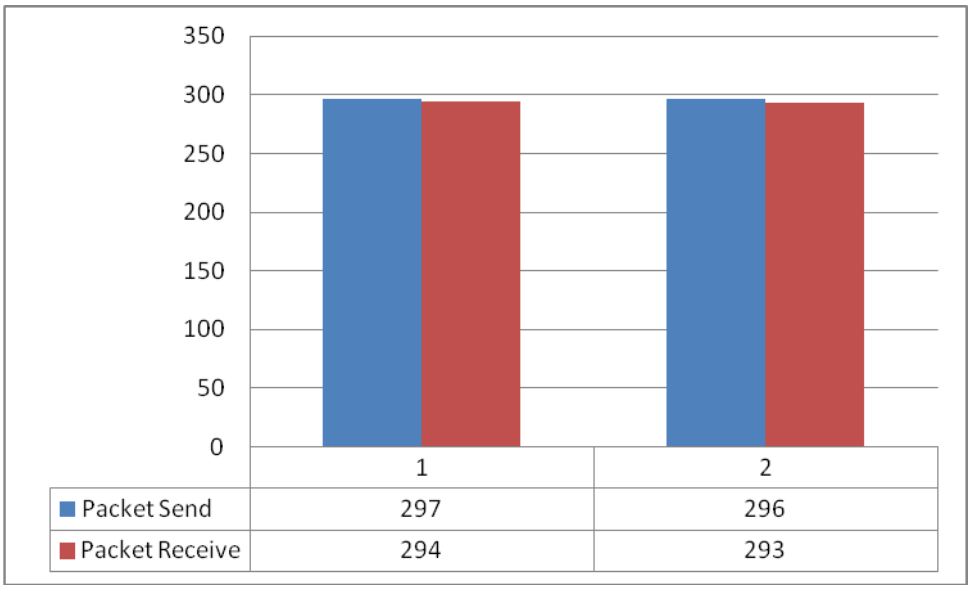
Στην πιο κάτω γραφική παράσταση με μπλε χρώμα παρατηρούμε τα πακέτα που στέλνουν οι κόμβοι 2 και 3 προς τον κόμβο sink. Ο κόμβος 2 τώρα, είναι ¨μολυσμένος¨ και η συχνότητα αποστολής πακέτων έγινε 60 πακέτα το δευτερόλεπτο, ενώ ο κόμβος 3 συνεχίζει να στέλνει με συχνότητα 1 πακέτο το δευτερόλεπτο. Με κόκκινο χρώμα παρατηρούμε τα πακέτα που παρέλαβε ο κόμβος sink από τους κόμβους 2 και 3. Από την γραφική παράσταση παρατηρούμε ότι ο ¨μολυσμένος¨ κόμβος 2 δεν επηρεάζει τον κόμβο 3 αλλά μόνο τον εαυτό του όσο αφορά την παραλαβή πακέτων από τον κόμβο sink. Αυτό συμβαίνει γιατί οι δύο κόμβοι είναι ανεξάρτητοι μεταξύ τους, ο κάθε κόμβος προωθεί τα πακέτα του μόνος του προς το κόμβο sink. Ο κόμβος 2 έχει μεγάλη απώλεια πακέτων για το λόγο ότι η συχνότητα αποστολής πακέτων (60 το δευτερόλεπτο) είναι πολύ μεγαλύτερη από αυτή που μπορεί το buffer το κόμβου να δεχτεί. Με αυτό το τρόπο ο κόμβος 2 βαρυφορτώνει το buffer του και τα πακέτα που δεν μπορούν να μπουν στο buffer για αποστολή απορρίπτονται.



Τοπολογία 2

Στην πιο κάτω εικόνα φαίνεται η τοπολογία του δικτύου το οποίο χρησιμοποιώ για να πάρω τις μετρήσεις μου. Βασική προϋπόθεση είναι ο Malicious Node να βρίσκεται πάνω από το Benign Node. Ο λόγος που πρέπει να βρίσκονται έτσι είναι γιατί με αυτό το τρόπο ο Malicious Node επηρεάζει άμεσα το Benign Node αφού τα πακέτα του Benign θα προωθηθούν μέσω του Malicious για να φτάσουν στο Sink.

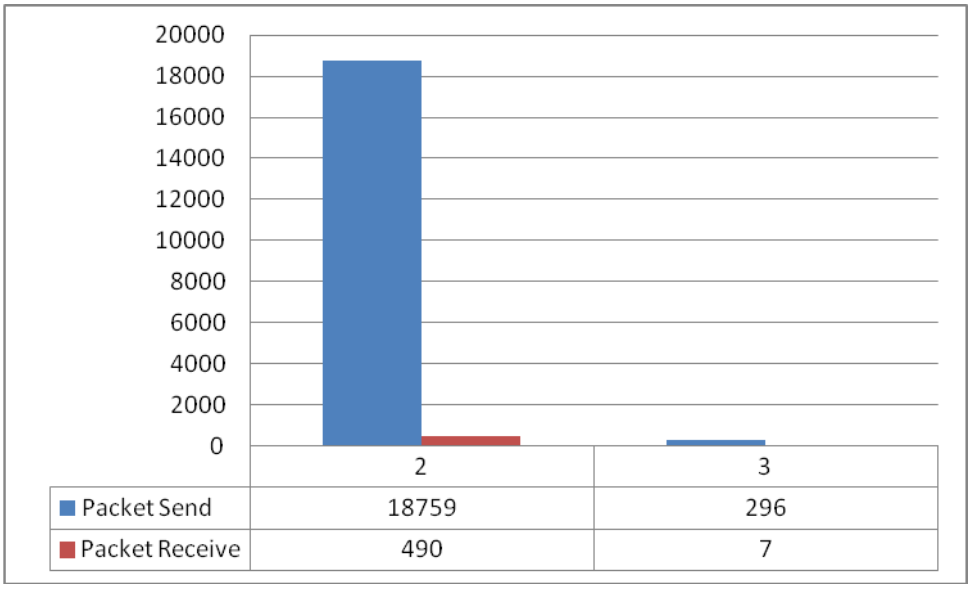




Στην πιο πάνω γραφική παράσταση με μπλε χρώμα παρατηρούμε τα πακέτα που στέλνουν οι κόμβοι 2 και 3 προς τον κόμβο sink. Οι δύο αυτοί κόμβοι δεν είναι ¨μολυσμένοι¨ και η συχνότητα αποστολής πακέτων είναι 1 πακέτο το δευτερόλεπτο. Με κόκκινο χρώμα παρατηρούμε τα πακέτα που παρέλαβε ο κόμβος sink από τους κόμβους 2 και 3 Από την γραφική παράσταση παρατηρούμε ότι όσα πακέτα στέλνουν οι κόμβοι μας ο κόμβος sink τα παραλαμβάνει. Τα 3-4 πακέτα που χάνονται είναι στα αρχικά στάδια επικοινωνίας όταν ο κόμβος εισέρχεται στο δίκτυο και προσπαθεί να δημιουργήσει σύνδεση προς το κόμβο sink.

Στην πιο κάτω γραφική παράσταση με μπλε χρώμα παρατηρούμε τα πακέτα που στέλνουν οι κόμβοι 2 και 3 προς τον κόμβο sink. Ο κόμβος 2 τώρα, είναι ¨μολυσμένος¨ και η συχνότητα αποστολής πακέτων έγινε 60 πακέτα το δευτερόλεπτο, ενώ ο κόμβος 3 συνεχίζει να στέλνει με συχνότητα 1 πακέτο το δευτερόλεπτο. Με κόκκινο χρώμα παρατηρούμε τα πακέτα που παρέλαβε ο κόμβος sink από τους κόμβους 2 και 3. Από την γραφική παράσταση παρατηρούμε ότι ο ¨μολυσμένος¨ κόμβος 2 επηρεάζει τον κόμβο 3 όσο αφορά την παραλαβή πακέτων από τον κόμβο sink. Αυτό συμβαίνει γιατί ο κόμβος 3 είναι άμεσα εξαρτημένος από τον κόμβο 2, ο κόμβος 3 για να αποστείλει πακέτα στο κόμβο sink πρέπει να προωθηθούν μέσω του κόμβου 2. Λόγο του ότι η συχνότητα αποστολής πακέτων του κόμβου 2 (60 το δευτερόλεπτο) είναι πολύ μεγαλύτερη από αυτή που μπορεί το buffer το κόμβου να δεχτεί, ο κόμβος 2 βαρυφορτώνει το buffer του και τα πακέτα που δεν μπορούν να μπουν στο buffer για

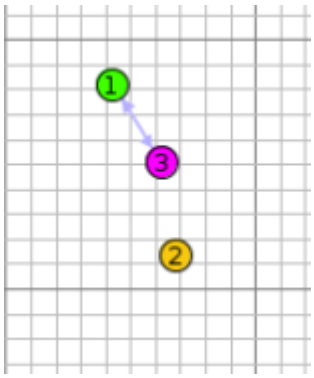
αποστολή απορρίπτονται. Εδώ εμφανίζεται και ένα είδος του ιού Selective-Forwarding. Ο κόμβος 2 τοποθετεί στο buffer για αποστολή πρώτα τα δικά του πακέτα και αν υπάρχει χώρος τότε τοποθετεί και τα πακέτα που πρόκειται να προωθήσει από άλλους κόμβους.

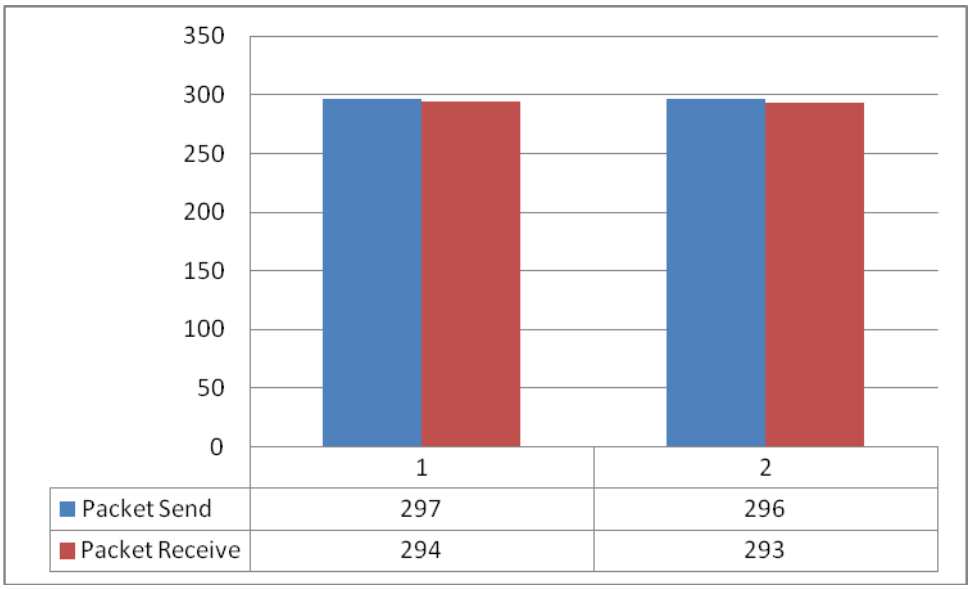


	2	3
Packet Send	18759	296
Packet Receive	490	7

Τοπολογία 3

Στην πιο κάτω εικόνα φαίνεται η τοπολογία του δικτύου το οποίο χρησιμοποιώ για να πάρω τις μετρήσεις μου. Βασική προϋπόθεση είναι ο Malicious Node να βρίσκεται κάτω από το Benign Node. Ο λόγος που πρέπει να βρίσκονται έτσι είναι γιατί με αυτό το τρόπο ο Malicious Node δεν επηρεάζει το Benign Node αφού τα πακέτα του Benign θα σταλούν απευθείας στο Sink.

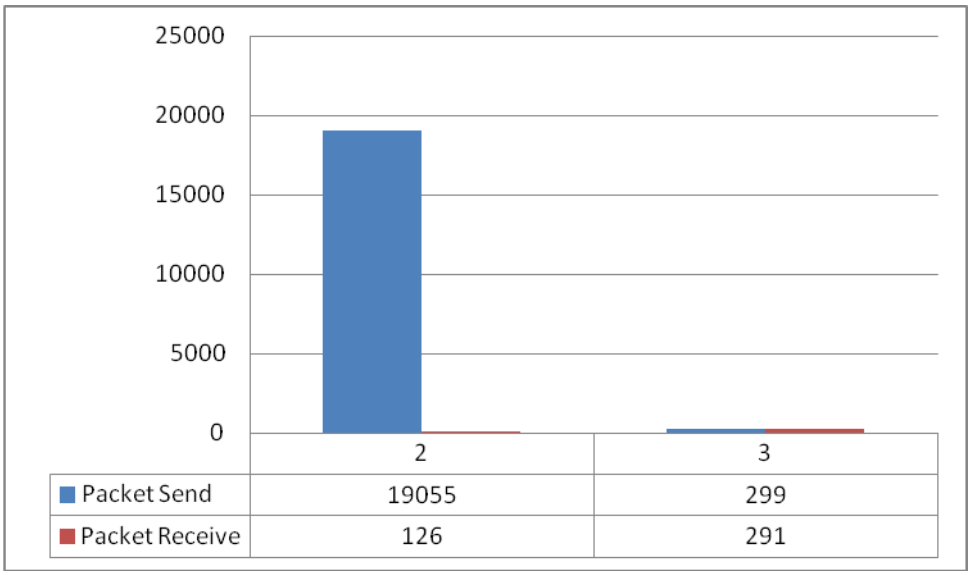




Στην πιο πάνω γραφική παράσταση με μπλε χρώμα παρατηρούμε τα πακέτα που στέλνουν οι κόμβοι 2 και 3 προς τον κόμβο sink. Οι δύο αυτοί κόμβοι δεν είναι ¨μολυσμένοι¨ και η συχνότητα αποστολής πακέτων είναι 1 πακέτο το δευτερόλεπτο. Με κόκκινο χρώμα παρατηρούμε τα πακέτα που παρέλαβε ο κόμβος sink από τους κόμβους 2 και 3. Από την γραφική παράσταση παρατηρούμε ότι όσα πακέτα στέλνουν οι κόμβοι μας ο κόμβος sink τα παραλαμβάνει. Τα 3-4 πακέτα που χάνονται είναι στα αρχικά στάδια επικοινωνίας όταν ο κόμβος εισέρχεται στο δίκτυο και προσπαθεί να δημιουργήσει σύνδεση προς το κόμβο sink.

Στην πιο κάτω γραφική παράσταση με μπλε χρώμα παρατηρούμε τα πακέτα που στέλνουν οι κόμβοι 2 και 3 προς τον κόμβο sink. Ο κόμβος 2 τώρα, είναι ¨μολυσμένος¨ και η συχνότητα αποστολής πακέτων έγινε 60 πακέτα το δευτερόλεπτο, ενώ ο κόμβος 3 συνεχίζει να στέλνει με συχνότητα 1 πακέτο το δευτερόλεπτο. Με κόκκινο χρώμα παρατηρούμε τα πακέτα που παρέλαβε ο κόμβος sink από τους κόμβους 2 και 3. Από την γραφική παράσταση παρατηρούμε ότι ο ¨μολυσμένος¨ κόμβος 2 δεν επηρεάζει τον κόμβο 3 αλλά μόνο τον εαυτό του όσο αφορά την παραλαβή πακέτων από τον κόμβο sink. Αυτό συμβαίνει γιατί ο κόμβος 3 βρίσκεται πάνω από τον κόμβο 2, , ο κόμβος 2 για να αποστείλει πακέτα στο κόμβο sink πρέπει να προωθηθούν μέσω του κόμβου 3. Ο κόμβος 2 έχει μεγάλη απώλεια πακέτων για το λόγο ότι η συχνότητα αποστολής πακέτων (60 το δευτερόλεπτο) είναι πολύ μεγαλύτερη από αυτή που μπορεί το buffer το

κόμβου να δεχτεί. Με αυτό το τρόπο ο κόμβος 2 βαρυφορτώνει το buffer του και τα πακέτα που δεν μπορούν να μπουν στο buffer για αποστολή απορρίπτονται.

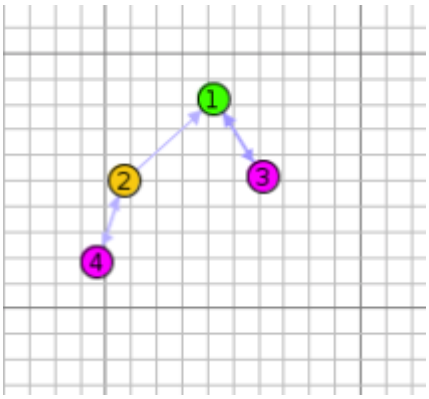


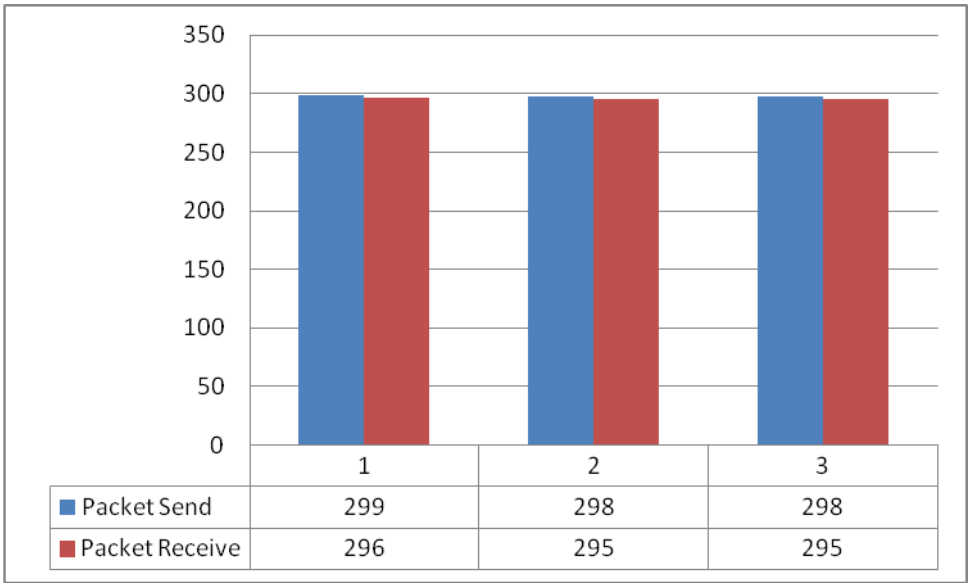
6.4.2 Sink node (1) – Benign node (2) – Malicious node (1)

Αυτό το σενάριο είναι συνδυασμός των προηγούμενων σεναρίων. Στο σενάριο χρησιμοποιήσαμε ένα sink node στον οποίο καταλήγουν όλα τα πακέτα, δύο benign node και ένα malicious node.

Τοπολογία 1

Στην πιο κάτω εικόνα φαίνεται η τοπολογία του δικτύου το οποίο χρησιμοποιώ για να πάρω τις μετρήσεις μου. Βασική προϋπόθεση είναι ο Malicious Node να βρίσκεται πάνω από ένα Benign Node και δίπλα από ένα Benign Node. Ο λόγος που πρέπει να βρίσκονται έτσι είναι για να παρατηρήσουμε πώς ο Malicious επηρεάζει τους δύο Benign Nodes.

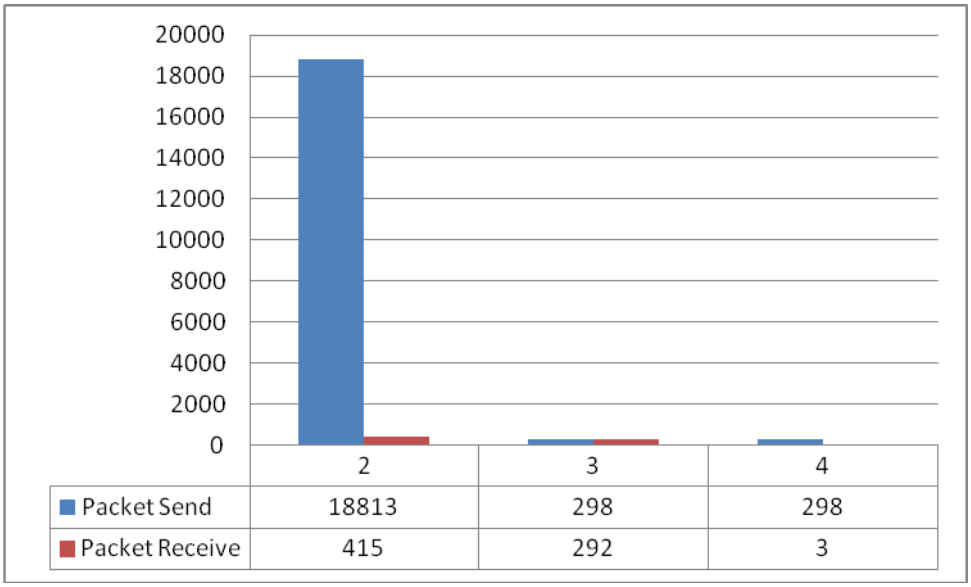




Στην πιο πάνω γραφική παράσταση με μπλε χρώμα παρατηρούμε τα πακέτα που στέλνουν οι κόμβοι 2 , 3 και 4 προς τον κόμβο sink. Οι δύο αυτοί κόμβοι δεν είναι ¨μολυσμένοι¨ και η συχνότητα αποστολής πακέτων είναι 1 πακέτο το δευτερόλεπτο. Με κόκκινο χρώμα παρατηρούμε τα πακέτα που παρέλαβε ο κόμβος sink από τους κόμβους 2 , 3 και 4. Από την γραφική παράσταση παρατηρούμε ότι όσα πακέτα στέλνουν οι κόμβοι μας ο κόμβος sink τα παραλαμβάνει. Τα 3-4 πακέτα που χάνονται είναι στα αρχικά στάδια επικοινωνίας όταν ο κόμβος εισέρχεται στο δίκτυο και προσπαθεί να δημιουργήσει σύνδεση προς το κόμβο sink.

Στην πιο κάτω γραφική παράσταση με μπλε χρώμα παρατηρούμε τα πακέτα που στέλνουν οι κόμβοι 2 , 3 και 4 προς τον κόμβο sink. Ο κόμβος 2 τώρα, είναι ¨μολυσμένος¨ και η συχνότητα αποστολής πακέτων έγινε 60 πακέτα το δευτερόλεπτο, ενώ οι κόμβοι 3 και 4 συνεχίζουν να στέλνουν με συχνότητα 1 πακέτο το δευτερόλεπτο. Με κόκκινο χρώμα παρατηρούμε τα πακέτα που παρέλαβε ο κόμβος sink από τους κόμβους 2 , 3 και 4. Από την γραφική παράσταση παρατηρούμε ότι ο ¨μολυσμένος¨ κόμβος 2 επηρεάζει μόνο τον κόμβο 4 και τον εαυτό του όσο αφορά την παραλαβή πακέτων από τον κόμβο sink. Αυτό συμβαίνει γιατί ο κόμβος 4 είναι άμεσα εξαρτημένος από τον κόμβο 2, ο κόμβος 4 για να αποστείλει πακέτα στο κόμβο sink πρέπει να προωθηθούν μέσω του κόμβου 2, εν αντιθέσει με τον κόμβο 3 ο οποίος είναι ανεξάρτητος από τον κόμβο 2 αφού βρίσκονται στο ίδιο επίπεδο. Λόγο του ότι η

συχνότητα αποστολής πακέτων του κόμβου 2 (60 το δευτερόλεπτο) είναι πολύ μεγαλύτερη από αυτή που μπορεί το buffer το κόμβου να δεχτεί, ο κόμβος 2 βαρυφορτώνει το buffer του και τα πακέτα που δεν μπορούν να μπουν στο buffer για αποστολή απορρίπτονται. Εδώ εμφανίζεται και ένα είδος του ιού Selective-Forwarding. Ο κόμβος 2 τοποθετεί στο buffer για αποστολή πρώτα τα δικά του πακέτα και αν υπάρχει χώρος τότε τοποθετεί και τα πακέτα που πρόκειται να προωθήσει από άλλους κόμβους.



Κεφάλαιο 7

Συμπεράσματα

7.1 Συμπεράσματα

Η επίθεση πλημμύρα εξ ορισμού είναι μια επίθεση Άρνησης Υπηρεσίας (DoS), οι επιθέσεις αυτές έχουν την δυνατότητα να αχρηστεύουν το δίκτυο. Ο επιτιθέμενος ο οποίος θα εισέλθει στο δίκτυο με σκοπό να καταστείλει την λειτουργία του ξεκινά να στέλνει μεγάλο αριθμό πακέτων, μεγαλύτερο από όσα μπορεί να χειριστεί, προς τον κόμβο sink. Αυτό έχει ως αποτέλεσμα ο κακόβουλος κόμβος να γεμίζει το buffer του δικτύου και να μην μπορεί οποιοσδήποτε άλλος κόμβος να στείλει τα δικά του πακέτα.

Στο σημείο αυτό έχουμε και την παρουσίαση του ιού selective – forwarding αφού ο κάθε κόμβος τοποθετεί στην αρχή του buffer τα δικά του πακέτα και μετά τα υπόλοιπα πακέτα που θα προωθήσει προς τον κόμβο sink από τους υπόλοιπους κόμβους. Αφού ο κακόβουλος κόμβος έχει συχνότητα αποστολής πακέτων μεγαλύτερη από αυτή που μπορεί να χειριστεί, υπερφορτώνει το buffer του με τα δικά του πακέτα και απορρίπτει τα πακέτα από τους άλλους κόμβους.

Μέσα στο ίδιο χρονικό διάστημα ένας κακόβουλος κόμβος μπορεί να στείλει πολύ μεγαλύτερο αριθμό πακέτων από ένα κανονικό κόμβο. Όσο περισσότερα πακέτα στείλει ένας κόμβος προς τον κόμβο sink τότε τόσο περισσότερα πακέτα θα χαθούν. Αυτό συμβαίνει λόγο του πρωτοκόλλου δρομολόγησης RPL, το οποίο χρησιμοποιεί τους κόμβους ως ενδιάμεσους κόμβους αποστολής πακέτων προς τον κόμβο sink, για τους κόμβους οι οποίοι δεν είναι στην εμβέλεια του κόμβου sink.

Όπως παρατηρήσαμε στις διάφορες τοπολογίες, ο τρόπος με τον οποίο ο επιτιθέμενος προσπαθεί να καταστρέψει το δίκτυο, είναι ότι στέλνοντας πολλά πακέτα προς τα πάνω, προς τον κόμβο sink, υπερφορτώνει το δικό του buffer. Αυτό έχει ως αποτέλεσμα να μην μπορεί να εξυπηρετήσει άλλους κόμβους, να προωθήσει τα πακέτα τους προς το

κόμβο sink, οι οποίοι βρίσκονται σε μεγαλύτερο βάθος από αυτόν και τα πακέτα τους να απορρίπτονται.

7.2 Μελλοντική Εργασία

Μια ενδιαφέρουσα πτυχή για προέκταση του υπάρχοντος ιού, είναι η υλοποίηση του ιού flooding ο οποίος θα στοχεύει στην αχρηστεύει ολόκληρου του δικτύου και όχι μόνο των κόμβων οι οποίοι βρίσκονται κάτω από τον κακόβουλο κόμβο. Αυτό μπορεί να επιτευχθεί στοχεύοντας την υπερφόρτωση του καναλιού του δικτύου και όχι του buffer του κάθε κόμβου.

Επιπρόσθετα, με την παρούσα εργασία προτείνεται η υλοποίηση περισσότερων επιθέσεων σε ασύρματα δίκτυα αισθητήρων και στο πρωτόκολλο RPL. Θα πρέπει να επιχειρείται η μελέτη της παρουσίας ενός κακόβουλου κόμβου σε ένα ασύρματο δίκτυο αισθητήρων με σκοπό την ανάπτυξη ενός αλγορίθμου για την ανίχνευση και τον εντοπισμό μιας απειλής που κινείται εντός της περιοχής του δικτύου.

Βιβλιογραφία

[1] https://learningnetwork.cisco.com/thread/5769

[2] http://en.wikipedia.org/wiki/OSI_model

[3] Z. Shelby and C. Bormann, *6LoWPAN: The Wireless Embedded Internet*. John Wiley & Sons, 1st edition, January 2010.

[4] J.P. Vasseur, N. Agarwal, J. Hui, Z. Shelby, P. Bertrand, C. Chauvenet, "RPL: The IP Routing Protocol Designed For Low Power and Lossy Networks", IPSO Alliance, April 2011.

[5] http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

[6] M. Ilyas, I.Mahgoud, Handbook of Sensor Networks : Compact Wireless and Wired Sensing Systems, CRC Press, 2004

[7] K. Sohraby, D. Minoli, T. Znati, Wireless sensor networks: Technology, Protocols, and Applications, Wiley, 2007

[8] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary *Wireless Sensor Network Security: A Survey* Wayne State University

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

[10] Vishal Rathod and Mrudang Mehta, *Security in Wireless Sensor Network: A survey*, Dharmsinh Desai University

[11] D. Meidanis, I. Papaefstathiou, "On the Power Consumption of Security Algorithms Employed in Wireless Networks", in Proc. of the IEEE Consumer

Communications & Networking Conference (CCNC09), Las Vegas, Nevada, 10-13 January, 2009.

[12] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” Ad Hoc Networks, vol. 1, no. 2, pp. 293–315, 2003. View at Publisher · View at Google Scholar · View at Scopus

[13] http://www.hindawi.com/journals/ijdsn/2013/794326/

[14] http://www.tamos.net/~rhay/overhead/ip-packet-overhead.htm

[15] http://orbigo.net/wp-content/uploads/2011/06/6LoWPAN_Stack.png

[16] http://www.contiki-os.org/

[17] http://en.wikipedia.org/wiki/Contiki

[18] https://github.com/contiki-os/contiki/wiki/An-Introduction-to-Cooja

[19] http://www.webopedia.com/DidYouKnow/Internet/DoS_attack.asp

[20] http://www.webopedia.com/TERM/F/Flooding.html

[21] https://www.paloaltonetworks.com/resources/learning-center/what-is-a-denial-of-service-attack-dos.html

[22] http://arxiv.org/ftp/arxiv/papers/1208/1208.5037.pdf

[23] http://users.ece.cmu.edu/~adrian/projects/tesla-ndss/node19.html

[24] Hemanta Kumar Kalita and Avijit Kar, WIRELESS SENSOR NETWORK SECURITY ANALYSIS, University, Kolkata, India, 2009

[25] Kalpana Sharma and M K Ghose, Wireless Sensor Networks: An Overview on its Security Threats, SMIT, Sikkim, India, 2010

[26] Chris Karlof and David Wagner, Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,University of California at Berkeley

[27] Linus Wallgren,Shahid Raza,Thiemo Voigt, Routing Attacks and Countermeasures in the RPL-Based

[28] Y.C HU, A. Perrig, D. B. Johnson, *Wormhole attacks in wireless networks*, IEEE Journal on selected areas in communication, 2006

[29] http://2.bp.blogspot.com/-_5ox6xoTMhU/T52Jm_9rGsI/AAAAAAAAAK0/VGeWDXaiGNE/s1600/Pantallazo12retallat.png

[30] https://www.cs.ucy.ac.cy/courses/EPL674/lectures/ch01GR.pdf

[31] http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/types-of-attack.html

[32] http://orbigo.net/wp-content/uploads/2011/06/6LoWPAN_Stack.png

[33] http://2.bp.blogspot.com/-_5ox6xoTMhU/T52Jm_9rGsI/AAAAAAAAAK0/VGeWDXaiGNE/s1600/Pantallazo12retallat.png

[34] http://www.cs.ucy.ac.cy/courses/EPL476/Lectures/2014F.EPL476.04-Multiple%20Access%20Techniques.pdf

[35]http://www.google.com.cy/imgres?imgurl=https://www.owasp.org/images/2/21/Main_the_middle.JPG&imgrefurl=https://www.owasp.org/index.php/Man-in-the-

middle_attack&h=316&w=569&tbnid=cSyLWUYoEFWtCM:&zoom=1&tbnh=102&tbnw=183&usg=__lxH-9Rli2Qx8t3bzdo2I0mo9oic=&docid=nz6mvjjNIlIiHM&itg=1