Ατομική Διπλωματική Εργασία

ΑΞΙΟΠΟΙΗΣΗ ΕΥΠΑΘΕΙΩΝ ΚΑΙ ΔΙΕΝΕΡΓΕΙΑ ΕΠΙΘΕΣΕΩΝ ΣΕ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΑΙΣΘΗΤΗΡΩΝ

Θωμά Γεώργιος

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μάιος 2016

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Αξιοποίηση Ευπαθειών και Διενέργεια Επιθέσεων σε Ασύρματα Δίκτυα Αισθητήρων

Θωμά Γεώργιος

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 2016

Ευχαριστίες

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

Επίσης, θα ήθελα να ευχαριστήσω την διδακτορική φοιτήτρια του τμήματος Χριστιάνα Ιωάννου, για την πολύτιμη βοήθεια που μου πρόσφερε για την ολοκλήρωση της εργασίας αυτής.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένεια μου και τους φίλους μου για την στήριξη και την συμπαράσταση τους καθ' όλη την διάρκεια των σπουδών μου.

Περίληψη

Τα ασύρματα δίκτυα αισθητήρων είναι μια νέα αναπτυσσόμενη τεχνολογία η οποία άρχισε να μπαίνει στην ζωή μας και αποτελεί σημαντικό πόλο έλξης στον ερευνητικό τομέα. Η ανάπτυξη των δικτύων αυτών και οι ποικίλες εφαρμογές τους, απαιτούν τη μελέτη και εύρεση νέων τρόπων για εξασφάλιση της βέλτιστης λειτουργίας τους, καθώς και εξασφάλιση της αξιοπιστίας και ασφάλειας στην χρήση τους.

Τα δίκτυα αισθητήρων έχουν διαφορετικά χαρακτηριστικά σε σχέση με τα κοινά ασύρματα δίκτυα. Οι αισθητήρες έχουν περιορισμένη υπολογιστική ισχύ, μνήμη και μπαταρία. Λόγω της διαφοροποίησης αυτής, είναι αδύνατη η χρησιμοποίηση υφιστάμενων μεθόδων για την εκτέλεση της λειτουργίας τους. Επιπρόσθετα, τα δίκτυα αυτά είναι από τη φύση τους πιο ευάλωτα σε κακόβουλες επιθέσεις και ενέργειες.

Στην παρούσα διπλωματική εργασία θα γίνει μια εισαγωγή στα ασύρματα δίκτυα αισθητήρων, τις εφαρμογές τους και τους περιορισμούς που τα διακατέχουν. Ακολούθως, θα παρουσιαστούν ορισμένα πρωτοκόλλα δρομολόγησης που σχεδιάστηκαν για τα δίκτυα αυτά εκ των οποίων ορισμένα πληρούν μερικές ανάγκες ασφάλειας. Στην συνέχεια, θα παρουσιαστεί το πρωτόκολλο δρομολόγησης RPL που χρησιμοποιείται ευρέως στα δίκτυα αισθητήρων και θα γίνει πειραματική αξιολόγησή του όσον αφορά την αντιμετώπιση συγκεκριμένων επιθέσεων. Τέλος, θα παρουσιαστούν τα συμπεράσματα που θα εξαχθούν από την μελέτη αυτή.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

1.1 Ορισμός του Προβλήματος

Τα τελευταία χρόνια έχει προχωρήσει σημαντικά η έρευνα σχετικά με τα ασύρματα δίκτυα αισθητήρων. Η νέα αυτή τεχνολογία έχει αρχίσει να εισχωρεί στην καθημερινότητά μας και το ερευνητικό ενδιαφέρον γίνεται όλο και πιο έντονο. Μέχρι σήμερα έχουν μελετηθεί αρκετά οι διάφορες πτυχές των ασύρματων δικτύων αισθητήρων. Για παράδειγμα, η ανάγκη που έχουν για αυτόνομη λειτουργία και η δημιουργία λειτουργικών συστημάτων που είναι προσαρμοσμένα στα χαρακτηριστικά των δικτύων αυτών. Όμως, ένα εξίσου σημαντικό θέμα αποτελεί η ανάγκη για ύπαρξη ασφάλειας.

Τα ασύρματα δίκτυα αισθητήρων χρησιμοποιούνται συχνά για μεταφορά ευαίσθητων πληροφοριών που δεν είναι επιτρεπτό να έλθουν εις γνώση μη εξουσιοδοτημένων ατόμων. Επομένως, επιβάλλεται η ανάπτυξη μεθόδων που εγγυόνται την ασφαλή μεταφορά των δεδομένων και την ομαλή λειτουργία του δικτύου παρά τις επιθέσεις που τυχόν να δεχθεί.

1.2 Σκοπός της Εργασίας

Στα πλαίσια της παρούσας εργασίας θα γίνει παρουσίαση ορισμένων πρωτοκόλλων δρομολόγησης που προτάθηκαν για τα ασύρματα δίκτυα αισθητήρων. Μερικά από τα πρωτόκολλα αυτά θεωρούνται ασφαλή και παρέχουν μηχανισμούς για προστασία ή αντιμετώπιση διάφορων τύπων επιθέσεων. Επίσης, θα παρουσιαστεί το πρωτόκολλο δρομολόγησης RPL, το οποίο είναι ένα διεθνές εγκεκριμένο πρωτόκολλο για χρήση σε δίκτυα χαμηλής ισχύος και με απώλειες (Low power and Lossy Networks) και θα αναλυθεί ο τρόπος λειτουργίας του.

Σκοπός της εργασίας αυτής είναι η υλοποίηση διάφορων επιθέσεων στο πρωτόκολλο RPL, η πειραματική αξιολόγησή του όσον αφορά την ασφάλεια και η εξαγωγή συμπερασμάτων μέσα από προσομοιώσεις σε ασύρματα δίκτυα αισθητήρων.

1.3 Δομή

Η παρούσα Διπλωματική Εργασία είναι χωρισμένη σε επτά κεφάλαια ως ακολούθως.
Στο πρώτο κεφάλαιο γίνεται η γενική εισαγωγή στο θέμα και αναφέρεται ο σκοπός της εργασίας.
Στο δεύτερο κεφάλαιο παρουσιάζονται τα ασύρματα δίκτυα αισθητήρων, τα πεδία εφαρμογής τους και οι περιορισμοί που έχουν.
Το κεφάλαιο τρία περιλαμβάνει βασικές έννοιες ασφάλειας που αφορούν τα ασύρματα δίκτυα αισθητήρων και περιγραφή ορισμένων τύπων επιθέσεων. Επίσης, γίνεται παρουσίαση διάφορων πρωτοκόλλων δρομολόγησης για τα δίκτυα αισθητήρων.
Στο τέταρτο κεφάλαιο γίνεται ανάλυση του πρωτοκόλλου RPL και αναφέρεται ο τρόπος λειτουργίας του.
Το κεφαλαίο πέντε παρουσιάζει το Contiki OS και εξηγείται ο τρόπος υλοποίησης των επιθέσεων σε αυτό.
Στο έκτο κεφάλαιο παρουσιάζονται τα σενάρια και οι προσομοιώσεις που έγιναν στον προσομοιωτή Cooja μαζί με τα σχετικά αποτελέσματα για τον κάθε τύπο επίθεσης.
Τέλος, στο έβδομο κεφάλαιο αναφέρονται τα συμπεράσματα που εξάχθηκαν με βάση τις προσομοιώσεις.

Κεφάλαιο 2

Ασύρματα Δίκτυα Αισθητήρων

2.1 Εισαγωγή

Τα ασύρματα δίκτυα αισθητήρων αποτελούνται από μια μεγάλη συλλογή οργανωμένων κόμβων οι οποίοι είναι ενωμένοι μεταξύ τους ασύρματα, σχηματίζοντας ένα δίκτυο. Οι κόμβοι αυτοί, είναι αισθητήρες μικρού μεγέθους και σχετικά χαμηλού κόστους. Οι αισθητήρες μπορούν να παρέχουν διάφορες πληροφορίες σχετικά με το περιβάλλον που βρίσκονται όπως θερμοκρασία, υγρασία, πίεση και κίνηση.
Ο κάθε αισθητήρας έχει ενσωματωμένο έναν πομποδέκτη, έναν μικροεπεξεργαστή, μνήμη και μια πηγή ενέργειας, συνήθως μια μπαταρία. Τα συστατικά αυτά επιτρέπουν την εκτέλεση των λειτουργιών του αισθητήρα. Ένας αισθητήρας μπορεί να συλλέγει, να αποστέλλει, να λαμβάνει και να επεξεργάζεται δεδομένα, όπως επίσης και να επικοινωνεί με άλλους αισθητήρες. Η επικοινωνία μεταξύ τους γίνεται αυτόνομα χρησιμοποιώντας διάφορα πρωτόκολλα επικοινωνίας. [1]

Σε ένα ασύρματο δίκτυο αισθητήρων τα δεδομένα που συλλέγονται από τους αισθητήρες προωθούνται σε έναν κόμβο τελικού προορισμού (sink node ή gateway). Ο κόμβος sink μπορεί να προσφέρει σύνδεση με κάποιον εξυπηρετητή (server) για λήψη και περεταίρω ανάλυση των δεδομένων. Η προώθηση των δεδομένων προς τον sink γίνεται με βάση το πρωτόκολλο δρομολόγησης που χρησιμοποιείται ανάλογα με την περίπτωση.

2.2 Εφαρμογές των Δικτύων Αισθητήρων

Τα ασύρματα δίκτυα αισθητήρων σήμερα έχουν διάφορες εφαρμογές σε πολλούς τομείς. Για παράδειγμα, οι αισθητήρες χρησιμοποιούνται στις στρατιωτικές δυνάμεις, σε βιομηχανίες, για περιβαλλοντική και ιατρική παρακολούθηση αλλά ακόμα και σε καταναλωτικό επίπεδο. [2]

Μια συνηθισμένη εφαρμογή των δικτύων αισθητήρων είναι η παρακολούθηση περιοχής. Σε στρατιωτικές επιχειρήσεις πολλοί αισθητήρες μπορούν να χρησιμοποιηθούν παρακολουθώντας μια περιοχή για ανίχνευση τυχόν εχθρικών δυνάμεων ή για παρακολούθηση οχημάτων. Επίσης, οι αισθητήρες μπορούν να χρησιμοποιηθούν σε συστήματα ελέγχου για παρακολούθηση βιομηχανικών μηχανημάτων και εξακρίβωση της σωστής λειτουργίας τους.

Τα δίκτυα αισθητήρων είναι ιδανικά για καταγραφή και παρακολούθηση περιβαλλοντικών φαινομένων. Καταγράφοντας τις μεταβολές στις περιβαλλοντικές συνθήκες μπορούν να χρησιμεύσουν για ανίχνευση πυρκαγιών, καταγραφή της ποιότητας του αέρα και νερού όπως επίσης και για πρόληψη φυσικών καταστροφών.

Επιπρόσθετα, έχουν δημιουργηθεί αισθητήρες που μπορούν να φορεθούν (wearable) ή να χρησιμοποιηθούν σαν εμφυτεύματα. Με την χρήση τους στον τομέα της ιατρικής, η παρακολούθηση ενός ασθενή γίνεται ευκολότερη. Οι αισθητήρες αυτοί είναι σχεδιασμένοι για να καταγράφουν δεδομένα σχετικά με την φυσική κατάσταση του ασθενή χωρίς ιατρική παρέμβαση.

Τα ασύρματα δίκτυα αισθητήρων αποτελούν αναγκαίο συστατικό για αναπτυσσόμενες τεχνολογίες όπως είναι τα έξυπνα σπίτια (smart homes) και το Internet of Things. Με την ενσωμάτωση διάφορων αισθητήρων σε αντικείμενα καθημερινής χρήσης και στους χώρους του σπιτιού, προσφέρεται στον καταναλωτή η διαδραστικότητα, η εξατομικευμένη εμπειρία και η χρήση νέων λειτουργιών.

2.3 Περιορισμοί στα Δίκτυα Αισθητήρων

Τα ασύρματα δίκτυα αισθητήρων έχουν ιδιαίτερα χαρακτηριστικά και έτσι διαφέρουν αρκετά από τα παραδοσιακά ενσύρματα ή ασύρματα δίκτυα. Οι ασύρματοι κόμβοι που σχηματίζουν το δίκτυο, όπως έχει αναφερθεί, έχουν μικρό μέγεθος και έτσι αποτελούνται από συγκεκριμένο υλικό (hardware) το οποίο περιορίζει τις δυνατότητες τους. Η μνήμη των ασύρματων αισθητήρων είναι περιορισμένη, έχουν μικρή υπολογιστική ισχύ και περιορισμένο ποσό ενέργειας το οποίο συνήθως είναι μη ανανεώσιμο. Επομένως, χρησιμοποιείται μεγάλος αριθμός κόμβων για να είναι το δίκτυο ανθεκτικό σε πιθανές απώλειες αισθητήρων. Οι απώλειες μπορεί να είναι είτε λόγω εξασθένησης των ενεργειακών πόρων των αισθητήρων είτε λόγω υιοθέτησης μη πρέπουσας συμπεριφοράς στο δίκτυο.

Επιπρόσθετα, οι κόμβοι ανάλογα με την απαιτούμενη εφαρμογή, μπορεί να τοποθετηθούν για λειτουργία σε σκληρές περιβαλλοντικές συνθήκες. Τα δίκτυα αισθητήρων είναι συνηθισμένο να έχουν τυχαίες τοπολογίες ή ακόμα και δυναμικές τοπολογίες στις οποίες υπάρχει κινητικότητα των κόμβων, γεγονός το οποίο δημιουργεί την ανάγκη για εξειδικευμένη μεταχείρισή τους σε σύγκριση με τα κοινά δίκτυα. Παράλληλα, παρουσιάζεται συχνά δυσκολία επικοινωνίας μεταξύ τους και λάθη στην μετάδοση των δεδομένων λόγω του περιβάλλοντος στο οποίο βρίσκονται καθώς επίσης και βλάβες των κόμβων (node failure).

Όλοι οι περιορισμοί αυτοί αποτελούν πρόκληση για τον τρόπο λειτουργίας και την βελτιστοποίηση των ασύρματων δικτύων αισθητήρων. [3]

Κεφάλαιο 3

Ασφάλεια στα Ασύρματα Δίκτυα Αισθητήρων

3.1 Εισαγωγή

Σε όλες τις μορφές δικτύων η ύπαρξη ασφάλειας είναι καίριας σημασίας. Κατά την λειτουργία των ασύρματων δικτύων αισθητήρων, μπορεί να μεταφέρονται προσωπικές, σημαντικές, ευαίσθητες ή απόρρητες πληροφορίες. Επομένως, είναι αναγκαία η ασφαλής μεταφορά των δεδομένων αυτών αλλά και η ομαλή λειτουργία του δικτύου παρά τις παρεμβολές που μπορεί να δεχθεί από κακόβουλους κόμβους. Οι τεχνικές που εφαρμόζονται για ασφάλεια στα παραδοσιακά δίκτυα είναι δύσκολο να εφαρμοστούν στα ασύρματα δίκτυα αισθητήρων λόγω των περιορισμών τους σε θέματα υπολογιστικής ισχύς, μνήμης και ενέργειας.

3.2 Βασικές Έννοιες Ασφάλειας

Για την επίτευξη του επίπεδου ασφάλειας που απαιτείται στα δίκτυα αισθητήρων είναι απαραίτητο να πληρούνται συγκεκριμένες προϋποθέσεις όπως η εμπιστευτικότητα, η ακεραιότητα και η πιστοποίηση. Στην συνέχεια δίνονται αναλυτικά οι έννοιες ασφάλειας που απαιτούνται για τα ασύρματα δίκτυα αισθητήρων. [4], [13]

Εμπιστευτικότητα (Confidentiality): Είναι απαραίτητο οι πληροφορίες που μεταφέρονται στο δίκτυο να μην είναι ορατές σε μη εξουσιοδοτημένα άτομα. Συνήθως, για να κρατηθούν κρυφά ορισμένα ευαίσθητα δεδομένα γίνεται χρήση κρυπτογράφησης.

Πιστοποίηση (Data Authentication): Η πιστοποίηση διασφαλίζει την ταυτότητα των κόμβων ξεχωρίζοντας τους νόμιμους από τους εισβολείς. Επομένως, αποτρέπει μη εξουσιοδοτημένα άτομα από το να συμμετέχουν στο δίκτυο. Οι κόμβοι πρέπει να έχουν την δυνατότητα να αναγνωρίζουν μηνύματα από μη εξουσιοδοτημένους κόμβους και να τα απορρίπτουν.

Ακεραιότητα (Integrity): Η ακεραιότητα διασφαλίζει ότι τα δεδομένα που έφτασαν στον παραλήπτη δεν έχουν τροποποιηθεί κατά την μεταφορά τους μέσα στο δίκτυο από κάποιο τρίτο άτομο.

Φρεσκάδα (Data freshness): Τα δεδομένα που διακινούνται στο δίκτυο πρέπει να είναι πρόσφατα. Έτσι, διασφαλίζεται ότι δεν θα ξανασταλεί ένα παλιό μήνυμα για κακόβουλο σκοπό.

Διαθεσιμότητα (Availability): Με την διαθεσιμότητα διασφαλίζεται ότι οι υπηρεσίες και οι πληροφορίες που παρέχει το δίκτυο είναι διαθέσιμες για χρήση, χωρίς καθυστέρηση, την στιγμή που είναι αναγκαίες. Αυτό σημαίνει ότι το δίκτυο πρέπει να είναι αξιόπιστο και να εγγυάται την παράδοση των δεδομένων στον προορισμό τους.

Έλεγχος Πρόσβασης (Access Control): Μη εξουσιοδοτημένοι κόμβοι δεν πρέπει να έχουν πρόσβαση στο δίκτυο και ούτε στις διαδικασίες που εκτελούνται σε αυτό. Οι εξουσιοδοτημένοι κόμβοι πρέπει να είναι σε θέση να εντοπίζουν τα πακέτα από μη εξουσιοδοτημένους κόμβους και να τα απορρίπτουν.

Ευρωστία / Επιβιωσιμότητα (Robustness / Survivability): Τα δίκτυα αισθητήρων πρέπει να είναι ανθεκτικά σε διάφορες επιθέσεις. Ακόμα και αν μια επίθεση πετύχει, τότε πρέπει οι επιπτώσεις της στο δίκτυο να είναι όσο το δυνατόν λιγότερες.

3.3 Επιθέσεις στα Ασύρματα Δίκτυα Αισθητήρων

Λόγω των χαρακτηριστικών των δικτύων αισθητήρων, των περιορισμών που έχουν, αλλά και έχοντας υπόψη ότι οι αισθητήρες ίσως να λειτουργούν σε εχθρικό και αφύλακτο περιβάλλον, τα ασύρματα δίκτυα αισθητήρων είναι σαφώς πιο ευάλωτα στην διενέργεια κακόβουλων επιθέσεων. Υπάρχουν διάφοροι τύποι επιθέσεων που μπορούν να επηρεάσουν τα δίκτυα αισθητήρων ή ακόμα και να τα θέσουν εκτός λειτουργίας. Οι επιθέσεις στα ασύρματα δίκτυα αισθητήρων διαχωρίζονται ανάλογα με το επίπεδο στο οποίο γίνονται οι κακόβουλες ενέργειες. [5]

3.3.1 Επιθέσεις στο Φυσικό Επίπεδο

Στο φυσικό επίπεδο (physical layer) αν ο εισβολέας έχει φυσική πρόσβαση στον κόμβο έχει την δυνατότητα να αλλοιώσει τα δεδομένα που στέλνονται και να εξάγει πληροφορίες από τον κόμβο όπως για παράδειγμα τα κρυπτογραφικά κλειδιά που χρησιμοποιεί. Επιπρόσθετα, επιθέσεις μπορούν να γίνουν χρησιμοποιώντας συσκευές που δημιουργούν παρεμβολές στις ραδιοσυχνότητες που χρησιμοποιεί το δίκτυο.

3.3.2 Επιθέσεις στο Επίπεδο Συνδέσμου

Στο επίπεδο του συνδέσμου (link layer) μπορούν να γίνουν κακόβουλα επιθέσεις που θα προκαλέσουν συγκρούσεις (collisions) σε πακέτα δεδομένων. Οι επαναλαμβανόμενες συγκρούσεις πακέτων μπορεί να προκαλέσουν εξάντληση (exhaustion) σε ένα κόμβο αφού θα προσπαθεί να στείλει δεδομένα χωρίς επιτυχία.

3.3.3 Επιθέσεις στο Επίπεδο Δρομολόγησης

Το επίπεδο δρομολόγησης (routing layer) είναι υπεύθυνο για την προώθηση – δρομολόγηση των πακέτων που στέλνονται στο δίκτυο από τον αποστολέα στον παραλήπτη. Για την υλοποίηση της δρομολόγησης χρησιμοποιούνται συγκεκριμένα πρωτόκολλα τα οποία καθορίζουν τον τρόπο που θα κινηθούν τα πακέτα στο δίκτυο για να φτάσουν στον προορισμό τους. Ακολουθεί μια περιγραφή των πιο συνηθισμένων επιθέσεων που μπορούν να γίνουν στο επίπεδο της δρομολόγησης.

3.3.3.1 Flooding

Ένας εισβολέας στο δίκτυο μπορεί να προκαλέσει την επίθεση της πλημμύρας (flooding) στέλνοντας ανά τακτά χρονικά διαστήματα πακέτα ζητώντας να γίνει μια νέα σύνδεση μέχρι οι πόροι που χρησιμοποιούνται για τις συνδέσεις να εξαντληθούν. Στην προκειμένη περίπτωση τα υπόλοιπα έγκυρα αιτήματα θα αγνοηθούν. Η συγκεκριμένη επίθεση εισάγει αχρείαστα πακέτα στο δίκτυο και μπορεί να προκαλέσει συμφόρηση.

3.3.3.2 Selective Forwarding

Η επίθεση της επιλεκτικής προώθησης (selective forwarding) μπορεί να επηρεάσει πρωτόκολλα δρομολόγησης που βασίζονται στην υπόθεση ότι οι συμμετέχοντες κόμβοι θα προωθήσουν τα πακέτα που λαμβάνουν. Κατά την επίθεση αυτή ο κακόβουλος κόμβος δεν προωθεί καθόλου μηνύματα ή προωθεί μόνο συγκεκριμένα μηνύματα και απορρίπτει (drop) τα υπόλοιπα. Με αυτό τον τρόπο επηρεάζεται η δρομολόγηση των πακέτων και η απόδοση του δικτύου. Για να επιτευχθεί μεγαλύτερη αποτελεσματικότητα της επίθεσης, ο εισβολέας μπορεί να επιλέξει να μολύνει κάποιον κόμβο ο οποίος βρίσκεται πάνω στο μονοπάτι της ροής των δεδομένων. Έτσι, θα έχει ευκολότερη πρόσβαση στα πακέτα τα οποία κινούνται στο δίκτυο.

3.3.3.3 Black Hole

Κατά την επίθεση μαύρης τρύπας (black hole) ο κακόβουλος κόμβος διαφημίζει ελκυστικά μονοπάτια προς τον κόμβο προορισμού (sink) με σκοπό να προσελκύσει όσο το δυνατό περισσότερα δεδομένα μπορεί. Ακολούθως, ο κόμβος - εισβολέας έχει την δυνατότητα τα πακέτα που θα λάβει να μην τα προωθήσει, να τα τροποποιήσει (alter) ή να παρακολουθεί την κίνηση των δεδομένων (eavesdropping).

3.3.3.4 Sinkhole

Ένας κακόβουλος κόμβος που υλοποιεί την επίθεση sinkhole διαφημίζει πολύ ελκυστικές πληροφορίες δρομολόγησης, συνήθως τόσο καλές όσο και του sink. Με αυτό τον τρόπο αναγκάζει τους γειτονικούς κόμβους να τον επιλέξουν ως προορισμό για τα πακέτα τους. Ουσιαστικά, στην επίθεση sinkhole ο εισβολέας διαφημίζει εσφαλμένα ότι είναι ο κόμβος προορισμού (sink) για να προσελκύσει όσο το δυνατόν περισσότερα πακέτα.

3.3.3.5 Wormhole

Στην επίθεση wormhole δύο απομακρυσμένοι κακόβουλοι κόμβοι δημιουργούν ένα κανάλι επικοινωνίας μεταξύ τους, μέσω του οποίου μεταφέρουν διάφορα δεδομένα και πληροφορίες που παίρνουν από άλλους κόμβους. Το κανάλι αυτό, μπορεί να χρησιμοποιηθεί από άλλους κόμβους για να στείλουν τα πακέτα τους, έχοντας την εντύπωση ότι τα πακέτα μεταφέρονται πολύ γρήγορα στον προορισμό τους. Η επίθεση wormhole μπορεί να έχει ως αποτέλεσμα δύο απομακρυσμένοι κόμβοι να θεωρήσουν ότι είναι γείτονες μέσω της χρήσης του καναλιού των κακόβουλων.

3.3.3.6 Sybil

Με την επίθεση sybil ένας κόμβος παρουσιάζει περισσότερες από μια ταυτότητες μέσα στο δίκτυο και μπορεί να εμφανιστεί σε διαφορετικές τοποθεσίες. Οι ταυτότητες που θα παρουσιάσει ο κακόβουλος κόμβος μπορεί να είναι είτε κλεμμένες από άλλους κόμβους είτε κατασκευασμένες από τον ίδιο. Η επίθεση sybil μπορεί να επηρεάσει γεωγραφικά πρωτόκολλα δρομολόγησης τα όποια βασίζονται στην τοποθεσία ενός κόμβου για να γίνει η δρομολόγηση των πακέτων. Επίσης, μπορεί να επηρεάσει πρωτόκολλα που βασίζονται στον πλεονασμό (redundancy) δεδομένων, αφού το πρωτόκολλο θα πιστεύει ότι τα δεδομένα είναι αποθηκευμένα σε κόμβους οι οποίοι στην ουσία δεν υπάρχουν.

3.4 Πρωτόκολλα Δρομολόγησης

Έχουν προταθεί πολλοί αλγόριθμοι και πρωτόκολλα για την λειτουργία και την επικοινωνία των αισθητήρων μεταξύ τους. Επίσης, έχουν σχεδιαστεί πολλές τεχνολογίες και πλατφόρμες για τον έλεγχο και την δοκιμή των δικτύων αυτών. Σε αυτή την ενότητα θα αναφερθούν ορισμένα πρωτόκολλα δρομολόγησης που μελετήθηκαν για ασύρματα δίκτυα αισθητήρων και οι κατηγορίες τους.

3.4.1 Location Based Protocols

Σε αυτή την κατηγορία οι κόμβοι γνωρίζουν την τοποθεσία τους στο δίκτυο. Η απόσταση μεταξύ γειτονικών κόμβων μπορεί να υπολογίζεται με βάση την λαμβανόμενη δύναμη του σήματος. Διαφορετικά, οι κόμβοι μπορεί να έχουν ενσωματωμένο πομπό GPS.
Ακολουθεί ένας πίνακας με ορισμένα location based πρωτόκολλα, μια σύντομη περιγραφή τους και την χρονολογία που προτάθηκε το καθένα.

Name/Year	Description
Geographic Adaptive Fidelity (GAF) [6,7]/2001	• Η τοπολογία χωρίζεται σε τετραγωνικό πλέγμα (grid) και κάθε κόμβος συσχετίζεται με ένα τετράγωνο • Οι κόμβοι σε ίδια τετράγωνα είναι ισοδύναμοι από άποψη κόστους δρομολόγησης • Υπάρχουν τρεις καταστάσεις για τους αισθητήρες: Sleeping, Discovery και Active • Μέσα σε ένα τετράγωνο, θα επιλεχθεί ένας αισθητήρας για να μείνει ενεργός και να στείλει δεδομένα στον sink • Χρησιμοποιούνται βαθμοί (rank) με βάση τα επίπεδα ενέργειας. Ψηλότερο rank συνεπάγεται μεγαλύτερη αναμενόμενη διάρκεια ζωής • Ένας αισθητήρας με ψηλό rank θα χειριστεί την δρομολόγηση στο grid του
Geographic and Energy-Aware Routing (GEAR) [6],[7]/2001	• Η τοπολογία χωρίζεται σε περιοχές • Οι αισθητήρες ξέρουν τα επίπεδα ενέργειάς τους, την τοποθεσία των γειτόνων τους και τα επίπεδα ενέργειάς τους • Χρησιμοποιούνται ευρετικά που έχουν επίγνωση της ενέργειας με βάση την γεωγραφική τοποθεσία για να γίνει δρομολόγηση πακέτων στην περιοχή του παραλήπτη • Χρησιμοποιείται αναδρομικός αλγόριθμος γεωγραφικής προώθησης για να παραδοθεί το πακέτο μέσα στην περιοχή

Coordination of Power Saving with Routing (SPAN) [6],[8]/2001	• Ο ασύρματος πομπός (wireless radio) απενεργοποιείται όταν οι αισθητήρες οι αδρανείς • Ένας αισθητήρας είτε «κοιμάται» είτε γίνεται συντονιστής (coordinator) • Οι συντονιστές προωθούν πακέτα εκ μέρους άλλων αισθητήρων και αλλάζουν με την πάροδο του χρόνου • Ο αισθητήρας διαφημίζει την κατάστασή του (συντονιστής ή όχι) στους γείτονες του και στους συντονιστές του • Κατά την άφιξη ενός πακέτου ο συντονιστής το προωθεί πιο κοντά στον προορισμό του (όχι απαραίτητα σε άλλον συντονιστή)
Trajectory-Based Forwarding (TBF) [6]/2003	• Απαιτεί μια πυκνή τοπολογία δικτύου και ένα σύστημα συντεταγμένων • Ορίζεται η τροχιά (trajectory) του πακέτου • Η πορεία δεν ορίζεται ρητά με βάση τα hops • Ο αισθητήρας που θα προωθήσει το πακέτο αποφασίζει με άπληστο τρόπο για να καθορίσει το επόμενο hop που είναι πιο κοντά στην τροχιά από τον αποστολέα • Είναι δυνατή η χρήση πολλαπλών διαδρομών για δρομολόγηση (multipath routing) χρησιμοποιώντας εναλλακτικές τροχιές

3.4.2 Data-centric Protocols

Στα Data-centric πρωτόκολλα ο sink μπορεί να ζητήσει δεδομένα από συγκεκριμένη περιοχή του δικτύου. Ο αποστολέας ακολούθως, θα στείλει τα δεδομένα του στον sink. Οι ενδιάμεσοι κόμβοι, μεταξύ αποστολέα και sink, μπορούν να ενσωματώσουν δεδομένα από πολλαπλές πηγές και έπειτα να γίνει η μετάδοση προς τον sink. Επομένως, γίνεται εξοικονόμηση ενέργειας αφού χρειάζονται λιγότερες μεταδόσεις δεδομένων για παραλαβή από τον sink.

Name/Year	Description
Sensor Protocols for Information via Negotiation (SPIN) [6],[7],[9]/1999	• Έχει γνώση των πόρων και μπορεί να προσαρμόζεται ανάλογα • Οι αισθητήρες μπορούν να υπολογίσουν την ενέργεια που χρειάζονται για να γίνει υπολογισμός, αποστολή και η λήψη δεδομένων. • Βασίζεται στους μηχανισμούς διαπραγμάτευσης και προσαρμογής των πόρων • Οι αισθητήρες μπορούν να διαπραγματευτούν μεταξύ τους πριν την αποστολή δεδομένων για αποφυγή της εισαγωγής μη χρήσιμων και περιττών πληροφοριών στο δίκτυο • Υπάρχει ένας διαχειριστής των πόρων που βοηθά τους αισθητήρες να παρακολουθούν και να προσαρμόζονται σε αλλαγές στους διαθέσιμους πόρους

Directed Diffusion [5],[6],[9]/2000	• Χρησιμοποιεί ονομασία δεδομένων (data naming), ενδιαφέροντα (interests), βαθμίδες (gradients), διάδοση δεδομένων (data propagation) και ενίσχυση (reinforcement) • Το ενδιαφέρον δηλώνει μια εργασία που πρέπει να γίνει στο δίκτυο και γίνεται broadcast από έναν κόμβο στους γείτονές του • Οι αισθητήρες δημιουργούν βαθμίδες πληροφοριών στις γειτονιές τους με την χρήση των ενδιαφερόντων • Αρχικά ο sink ορίζει χαμηλό data rate για τα εισερχόμενα δεδομένα • Ο sink μπορεί να ενισχύσει ένα συγκεκριμένο αισθητήρα για να στέλνει δεδομένα με ψηλότερο data rate στέλνοντας το αρχικό μήνυμα ενδιαφέροντος με μικρότερο χρονικό διάστημα • Αν ένας γειτονικός κόμβος λάβει αυτό το μήνυμα ενδιαφέροντος και ο αποστολέας έχει μεγαλύτερο data rate από πριν και αυτό είναι μεγαλύτερο από όλες τις βαθμίδες, τότε ο κόμβος θα ενισχύσει έναν ή περισσότερους από τους γείτονές του
Rumor Routing [6],[7],[9]/2002	• Χρησιμοποιείται η έννοια του πράκτορα • Ο πράκτορας είναι ένα πακέτο που κινείται στο δίκτυο και ενημερώνει κάθε αισθητήρα για τα γεγονότα που έμαθε κατά την κίνησή του • Ένας πράκτορας κινείται στο δίκτυο για συγκεκριμένο αριθμό hops και μετά καταστρέφεται • Κάθε αισθητήρας και ο πράκτορας έχουν μια λίστα γεγονότων με ζεύγη γεγονότος – απόστασης. Κάθε εγγραφή περιέχει το γεγονός και την απόσταση σε hops προς το γεγονός αυτό • Όταν ένας πράκτορας ληφθεί από έναν αισθητήρα, γίνεται συγχρονισμός της λίστας τους έτσι ώστε να έχουν το μικρότερο μονοπάτι προς τα γεγονότα που συμβαίνουν στο δίκτυο
Energy-Aware Data-Centric Routing (EAD) [6]/2003	• Δημιουργείται ένα εικονικό backbone που αποτελείται από τους ενεργούς αισθητήρες οι οποίοι είναι υπεύθυνοι για την επεξεργασία των δεδομένων και για την μετάδοση του traffic • Το δίκτυο αναπαρίσταται με ένα δέντρο που περιέχει όλους τους αισθητήρες και στην ρίζα του έχει τον sink. Οι κόμβοι στα φύλλα του δέντρου έχουν τους πομπούς τους απενεργοποιημένους. Όλοι οι υπόλοιποι κόμβοι σχηματίζουν το backbone, είναι ενεργοί και έχουν ενεργοποιημένους τους πομπούς τους. • Στόχος είναι να κτιστεί ένα βέλτιστο δέντρο, με τον ελάχιστο αριθμό φύλλων για να μειωθεί το μέγεθος του backbone • Μπορεί να βοηθήσει στην επέκταση της ζωής του δικτύου
Minimum Cost Forwarding Algorithm (MCFA) [7],[9]/2001	• Εκμεταλλεύεται το γεγονός ότι η κατεύθυνση της δρομολόγησης είναι πάντα προς τον sink • Ένας αισθητήρας δεν χρειάζεται μια μοναδική ταυτότητα ή πίνακες δρομολόγησης • Κάθε κόμβος διατηρεί μια εκτίμηση με το λιγότερο κόστος από αυτόν στον sink • Κάθε μήνυμα που πρέπει να προωθηθεί από έναν αισθητήρα γίνεται broadcast στους γείτονές του • Όταν ένας κόμβος λάβει ένα μήνυμα, ελέγχει αν είναι πάνω στο μονοπάτι με το ελάχιστο κόστος μεταξύ του αποστολέα και του

	sink. Αν είναι, τότε το μήνυμα γίνεται broadcast στους γείτονες του. Η διαδικασία επαναλαμβάνεται μέχρι να φτάσει το μήνυμα στον sink.

3.4.3 Hierarchical Protocols

Το δίκτυο είναι χωρισμένο σε επίπεδα συγκροτημάτων (clustered layers). Οι κόμβοι ανήκουν σε ένα cluster και για κάθε cluster ορίζεται ένας cluster head κόμβος ο οποίος έχει την ευθύνη για την δρομολόγηση από το cluster σε άλλα cluster heads. Τα δεδομένα κινούνται από μικρότερο σε μεγαλύτερο επίπεδο και κινούνται προς τον sink.

Name	Description
Low-energy adaptive clustering hierarchy (LEACH) [6],[7],[9]/2000	• Η εργασία του clustering γίνεται εναλλάξ από τους κόμβους με βάση την διάρκεια • Ο cluster head επικοινωνεί απευθείας με τον sink για να προωθήσει τα δεδομένα • Βασίζεται στην συσσωμάτωση η οποία συνδυάζει τα δεδομένα σε μικρότερο μέγεθος και μεταφέρονται μόνο οι πληροφορίες που έχουν νόημα για τους αισθητήρες • Χρησιμοποιεί τυχαία εναλλαγή για την επιλογή του cluster head έτσι ώστε όλοι οι αισθητήρες να οριστούν σαν cluster head και να αποφευχθεί εξάντληση της μπαταρίας • Η λειτουργία χωρίζεται σε δύο φάσεις: (α) Εγκατάσταση (οργάνωση του δικτύου σε clusters), Διαφήμιση του Cluster Head, Δημιουργία του προγράμματος μεταδόσεων (β) Φάση σταθεροποίησης για συσσωμάτωση δεδομένων, συμπίεση και μετάδοση στον sink • Δεν χρειάζεται καθολική γνώση του δικτύου • Δρομολόγηση singe hop (κάθε κόμβος στέλνει απευθείας στον cluster head και στον sink)
Power-Efficient Gathering in Sensor Information Systems (PEGASIS) [6],[7],[9]/2002	• Αποτελεί επέκταση του LEACH • Δημιουργεί αλυσίδες από αισθητήρες έτσι ώστε κάθε κόμβος να στέλνει και να λαμβάνει από ένα γείτονα • Μόνο ένας κόμβος στην αλυσίδα μεταδίδει δεδομένα στον sink. Ο κόμβος επιλέγεται τυχαία • Τα δεδομένα που μαζεύτηκαν κινούνται από κόμβο σε κόμβο, συσσωματώνονται και στέλνονται στον sink • Η φάση κατασκευής προϋποθέτει ότι όλοι οι αισθητήρες έχουν καθολική γνώση των θέσεων των αισθητήρων και χρησιμοποιεί άπληστη προσέγγιση • Όταν ένας αισθητήρας πεθάνει/έχει πρόβλημα η αλυσίδα κατασκευάζεται με την ίδια άπληστη προσέγγιση και ο συγκεκριμένος κόμβος θα παρακαμφθεί • Δεν δημιουργούνται clusters

Hybrid, Energy-Efficient Distributed Clustering (HEED) [6],[10]/2002	• Επεκτείνει την λογική του LEACH • Χρησιμοποιεί την ενέργεια και τον βαθμό ή την πυκνότητα ως μετρικά για την επιλογή των cluster, για να επιτευχθεί εξισορρόπηση της ενέργειας • Λειτουργεί σε δίκτυα multi-hop χρησιμοποιώντας προσαρμοστική ισχύ μετάδοσης κατά την επικοινωνία στο εσωτερικό του cluster • Έχει ως στόχο: (α) Την επέκταση του χρόνου ζωής του δικτύου κατανέμοντας την κατανάλωση ενέργειας (β) Τον τερματισμός της διαδικασίας του cluster μετά από έναν αριθμό επαναλήψεων (γ) Την ελαχιστοποίηση του control overhead (δ) Την παραγωγή καλά κατανεμημένων cluster heads και clusters • Χρησιμοποιεί ένα συνδυασμό παραμέτρων για την επιλογή των cluster heads. Κύρια παράμετρος: Υπόλοιπο ενέργειας του κάθε αισθητήρα • Δευτερεύουσα παράμετρος: Κόστος της επικοινωνίας μεταξύ των clusters ως συνάρτηση της πυκνότητας του cluster ή του βαθμού του κόμβου • Η κύρια παράμετρος χρησιμοποιείται για να υπολογιστεί το σύνολο των cluster heads και η δευτερεύουσα για να σπάσουν οι ισοπαλίες
Threshold Sensitive Energy Efficient Sensor Network Protocol (TEEN) [6], [9], [12] /2001	• Οι αισθητήρες ομαδοποιούνται σε clusters με επικεφαλής έναν cluster head(CH) • Οι αισθητήρες εντός ενός cluster στέλνουν τα δεδομένα τους στον CH τους • Ο CH στέλνει συσσωματωμένα δεδομένα στον CH του πιο πάνω επιπέδου, μέχρι τα δεδομένα φτάσουν στον sink • Οι κοντινοί κόμβοι σχηματίζουν clusters και η διαδικασία συνεχίζεται στο δεύτερο επίπεδο μέχρι να φτάσει στον sink • Χρησιμοποιεί data-centric μέθοδο με ιεραρχική προσέγγιση
Energy Efficient Homogenous Clustering Algorithm for Wireless Sensor Networks [6]/2010	• Γίνεται ομοιογενής κατανομή των κόμβων σε clusters • Το cluster head επιλέγεται με βάση το υπόλοιπο ενέργειας των υπαρχόντων cluster heads και την κοντινότερη απόσταση του κόμβου με βάση τα hops • Ο αλγόριθμος ομοιογένειας διασφαλίζει ότι κάθε κόμβος θα είναι είτε cluster head είτε μέλος ενός cluster • Τα μέλη ενός cluster είναι ομοιόμορφα κατανεμημένα και επομένως γίνεται επέκταση του χρόνου ζωής του δικτύου • Μόνο τα cluster heads κάνουν broadcast τα μηνύματα για δημιουργία του cluster και όχι κάθε κόμβος • Δίνεται έμφαση στην αύξηση της διάρκειας ζωής του δικτύου με την ομοιόμορφη κατανομή των κόμβων σε clusters έτσι ώστε να μην υπάρχει ψηλό overhead μετάδοσης

3.4.4 Mobility-based Protocols

Τα πρωτόκολλα αυτά, αφορούν δίκτυα στα οποία οι κόμβοι ή ο sink μπορεί να κινούνται και να μην έχουν σταθερή θέση.

Name	Description
Joint Mobility and Routing Protocol [6], [11]/2005	• Ο sink κινείται για να συλλέξει τα δεδομένα από τους αισθητήρες • Οι αισθητήρες που περιβάλλουν τον sink αλλάζουν με την πάροδο του χρόνου για να δοθεί η ευκαιρία σε όλους του αισθητήρες να προωθήσουν τα δεδομένα τους στον sink • Ο φόρτος της δρομολόγησης δεδομένων ισορροπείται σε όλους τους αισθητήρες
Data MULES Based Protocols [6]/2003	• Βασίζεται σε κινητές οντότητες που ονομάζονται Mobile Ubiquitous LAN Extensions (MULEs) • Χωρίζεται σε τρία κύρια επίπεδα: (1) Κάτω επίπεδο: Οι σταθεροί αισθητήρες που καταγράφουν δεδομένα από το περιβάλλον (2) Μέσο επίπεδο: MULEs που κινούνται στο πεδίο, συλλέγουν τα δεδομένα και τα παραδίδουν σε σημεία πρόσβασης όταν φτάσουν κοντά τους (3) Πάνω επίπεδο: Συσκευές συνδεδεμένες σε WAN ή σημεία πρόσβασης για την ανάλυση των δεδομένων. Είναι συνδεδεμένες με μια αποθήκη δεδομένων για συγχρονισμό των δεδομένων, αναγνωρίζουν πλεονασμούς και επιβεβαιώνουν την λήψη των δεδομένων από τα MULEs • Βοηθά στην εξοικονόμηση ενέργειας και στην επέκταση της διάρκειας ζωής του δικτύου • Λόγω της απευθείας σύνδεσης μεταξύ των αισθητήρων και των MULEs δεν υπάρχει overhead δρομολόγησης
Scalable Energy-Efficient Asynchronous Dissemination (SEAD) [6]/2003	• Οι αισθητήρες στέλνουν τα δεδομένα που συλλέγουν σε πολλαπλούς κινητούς sink • Αποτελείται από τρία κύρια συστατικά: Κατασκευή του δέντρου διάδοσης, διάδοση των δεδομένων, διατήρηση των συνδέσμων με τους κινητούς sinks • Υποθέτει ότι οι αισθητήρες γνωρίζουν την γεωγραφική τους τοποθεσία • Κάθε αισθητήρας κτίζει το δέντρο διάδοσης των δεδομένων με την ρίζα στον εαυτό του. Όλα τα δέντρα κτίζονται ξεχωριστά
Dynamic Proxy Tree-Based Data Dissemination [6]/2004	• Το δίκτυο αποτελείται από σταθερούς και μερικούς κινητούς κόμβους (sinks) • Οι αισθητήρες χρησιμοποιούνται για εντοπισμό και συνεχή παρακολούθηση ορισμένων κινητών στόχων • Οι sinks χρησιμοποιούνται για να συλλέγουν δεδομένα από συγκεκριμένους αισθητήρες – πηγές • Οι αισθητήρες – πηγές εντοπίζουν τους sinks και δημιουργούν ή συσσωματώνουν δεδομένα από ένα υποσύνολο αισθητήρων

	• Λόγω της κινητικότητας των στόχων, μια πηγή μπορεί να αλλάξει και ένας κοντινότερος αισθητήρας στον στόχο μπορεί να γίνει πηγή • Κάθε πηγή εκπροσωπείται από έναν σταθερό source proxy • Κάθε sink εκπροσωπείται από έναν σταθερό sink proxy • Οι proxies είναι προσωρινοί και αλλάζουν όσο οι πηγές αλλάζουν και οι sinks κινούνται • Μια πηγή θα έχει έναν νέο proxy μόνο όταν η απόσταση μεταξύ της πηγής και του παρόν proxy ξεπεράσει ένα threshold. Το ίδιο συμβαίνει και για τους sinks.

3.4.5 Multipath Based Protocols

Η συγκεκριμένη ομάδα πρωτοκόλλων δρομολόγησης χρησιμοποιεί πολλά μονοπάτια αντί ένα για δρομολόγηση των δεδομένων. Τα πρωτόκολλα αυτά, προσφέρουν ελαστικότητα και αξιοπιστία στο δίκτυο.

Name	Description
Sensor-disjoint multipath routing [6]/2001	• Βοηθά στην εύρεση ενός μικρού αριθμού εναλλακτικών μονοπατιών που δεν έχουν κοινό αισθητήρα μεταξύ τους και με το πρωτεύον μονοπάτι • Το πρωτεύον μονοπάτι είναι το καλύτερο μονοπάτι που είναι διαθέσιμο • Τα εναλλακτικά μονοπάτια είναι λιγότερο επιθυμητά διότι έχουν μεγαλύτερη καθυστέρηση • Τα εναλλακτικά μονοπάτια είναι ανεξάρτητα από το πρωτεύον μονοπάτι • Μια βλάβη στο πρωτεύον μονοπάτι είναι τοπική και δεν επηρεάζει κανένα από τα εναλλακτικά μονοπάτια • Το δίκτυο πλημμυρίζεται με μερικά low-rate δείγματα • Ακολούθως ο sink μπορεί να καθορίσει ποιοι από τους γείτονες μπορούν να παρέχουν την υψηλότερη ποιότητα δεδομένων η οποία χαρακτηρίζεται από τις χαμηλότερες απώλειες ή από την λιγότερη καθυστέρηση
Braided Paths [6]/2001	• Δημιουργούνται μονοπάτια που είναι μερικώς ξένα από το πρωτεύον μονοπάτι • Για την κατασκευή του πλεγμένου (braided) μονοπατιού, υπολογίζεται πρώτα το πρωτεύον μονοπάτι • Ακολούθως για κάθε κόμβο στο πρωτεύον μονοπάτι, υπολογίζεται το καλύτερο μονοπάτι από τον αποστολέα στον sink το οποίο δεν περιλαμβάνει τον συγκεκριμένο κόμβο • Τα εναλλακτικά μονοπάτια δεν είναι απαραίτητα ξένα (disjoint) από το πρωτεύον μονοπάτι • Οι σύνδεσμοι των εναλλακτικών μονοπατιών είναι πάνω ή κοντά στο πρωτεύον μονοπάτι

N-to-1 Multipath Discovery [6]/2002	• Γίνεται απλή πλημμύρα από τον sink • Έχει δύο φάσεις: Branch aware flooding, Multipath extension of flooding • Και οι δύο φάσεις χρησιμοποιούν τα ίδια μηνύματα δρομολόγησης • Δημιουργεί πολλαπλά disjoint μονοπάτια για κάθε αισθητήρα

3.4.6 Heterogeneity-Based Protocols

Μπορούν να εφαρμοστούν σε δίκτυα που έχουν δύο τύπους αισθητήρων, τους line-powered οι οποίοι δεν έχουν περιορισμούς όσον αφορά την ενέργεια και τους battery-powered οι οποίοι έχουν περιορισμένο χρόνο ζωής.

Name	Description
Information - Driven Sensor Query (IDSQ) [6],[7],[9]/2002	• Για εξοικονόμηση ενέργειας, μόνο ένα υποσύνολο αισθητήρων παραμένει ενεργό όταν υπάρχουν δεδομένα που πρέπει να αναφερθούν σε μερικά κομμάτια του δικτύου • Επιλέγει έναν αισθητήρα ως ηγέτη (leader) από ένα cluster από αισθητήρες • Ο ηγέτης είναι υπεύθυνος για να επιλέξει το βέλτιστο σύνολο αισθητήρων με βάση μετρήσεις για την χρησιμότητα των πληροφοριών • Η επιλογή του υποσυνόλου των ενεργών αισθητήρων που έχουν τις πιο χρήσιμες πληροφορίες ισορροπείται με το κόστος επικοινωνίας μεταξύ των αισθητήρων αυτών • Αναζητούνται χρήσιμες πληροφορίες προβλέποντας τον χώρο και τον χρόνο που θα συμβούν ενδιαφέροντα γεγονότα
Cluster-Head Relay Routing (CHR) [6]/2005	• Το δίκτυο απαρτίζεται από ένα sink και δύο είδη αισθητήρων • Έχει μεγάλο αριθμό από low-end αισθητήρες (L-sensors) και μικρό αριθμό από ισχυρούς high-end αισθητήρες (H-sensors) • Οι αισθητήρες είναι στατικοί και έχουν γνώση της τοποθεσίας τους • Και οι δύο τύποι αισθητήρων κατανέμονται ομοιόμορφα και τυχαία στον χώρο • Το δίκτυο χωρίζεται σε clusters, που το καθένα έχει L-sensors και ένα H-sensor ως ηγέτη • Οι L-sensors προωθούν τα δεδομένα στον H-sensor • Οι H-sensors προωθούν συσσωματωμένα δεδομένα από άλλους H-sensor με δρομολόγηση multihop μέχρι να φτάσουν στον sink

3.4.7 Quality of Service Based Protocols

Τα συγκεκριμένα πρωτόκολλα αφορούν δίκτυα με απαιτήσεις για συγκεκριμένη ποιότητα υπηρεσίας, αξιοπιστία και χαμηλές καθυστερήσεις.

Name	Description
Sequential Assignment Routing (SAR) [6], [7], [9]/2002	• Για να αποφασιστεί πως θα γίνει η δρομολόγηση βασίζεται σε: ποσοστό ενέργειας, QoS σε κάθε μονοπάτι και την προτεραιότητα του κάθε πακέτου • Δημιουργεί δέντρα με ρίζα τους κόμβους που είναι ένα hop από τον sink(λαμβάνοντας υπόψη το QoS μετρικό, την ενέργεια και την προτεραιότητα) • Με την χρήση δέντρων, δημιουργούνται πολλαπλά μονοπάτια από τον sink στους αισθητήρες • Ένα από αυτά τα μονοπάτια επιλέγεται ανάλογα με την ποσότητα ενέργειας και το QoS στο μονοπάτι • Οποιαδήποτε τοπική βλάβη ή αλλαγή στην τοπολογία προκαλεί μια αυτόματα διαδικασία επαναφοράς του μονοπατιού • Για προληπτικούς λόγους γίνεται ένας περιοδικό επανυπολογισμός των μονοπατιών. Η διαδικασία ενεργοποιείται από τον sink • Η επαναφορά από βλάβες επιτυγχάνεται, με την επιβολή της συνέπειας των πινάκων δρομολόγησης μεταξύ των κόμβων
SPEED [6], [7]/2003	• Απαιτεί κάθε κόμβος να διατηρεί πληροφορίες για τους γείτονές του • Χρησιμοποιεί γεωγραφική προώθηση για να βρει μονοπάτια • Παρέχει αποφυγή συμφόρησης • Χρησιμοποιεί την μονάδα δρομολόγησης που ονομάζεται Stateless Geographic Non-Deterministic Forwarding (SNFG) • Υπολογίζει την εκτίμηση της καθυστέρησης σε κάθε κόμβο, μετρώντας τον χρόνο που πέρασε όταν ένα ACK ληφθεί από ένα γείτονα • Υπολογίζει την αναλογία μετάδοσης ενός κόμβου χρησιμοποιώντας το miss ratio των γειτόνων • Κοιτάζει την καθυστέρηση και επιλέγει τον κόμβο που ικανοποιεί της απαιτήσεις ταχύτητας • Αν αυτό αποτύχει χρησιμοποιείται το η αναλογία μετάδοσης
Energy-Aware QoS Routing Protocol [6], [9]/2003	• Χρησιμοποιεί μια επέκταση του αλγόριθμου του Dijkstra και βρίσκει το μονοπάτι με το λιγότερο κόστος και την λιγότερη απαίτηση ενέργειας το οποίο ικανοποιεί συγκεκριμένες τιμές για την καθυστέρηση • Το link cost είναι μια συνάρτηση που καταγράφει την ενέργεια του κόμβου, την ενέργεια για μετάδοση, το error rate και άλλες παραμέτρους επικοινωνίας • Για να υποστηρίξει δεδομένα πραγματικού χρόνου χρησιμοποιείται ένα μοντέλο class-based queuing

	• Το μοντέλο αυτό επιτρέπει το μοίρασμα των υπηρεσιών για δεδομένα πραγματικού χρόνου και για δεδομένα διαφορετικού τύπου

3.5 Ασφαλή Πρωτόκολλα Δρομολόγησης

Υπάρχουν επίσης προτάσεις για πρωτόκολλα δρομολόγησης τα οποία παρέχουν ασφάλεια στα ασύρματα δίκτυα αισθητήρων. Τα πρωτόκολλα αυτά έχουν την δυνατότητα είτε να εντοπίζουν επιθέσεις στο δίκτυο και να τις μετριάζουν, είτε είναι ανθεκτικά σε συγκεκριμένους τύπους επιθέσεων. Ένα πρωτόκολλο δρομολόγησης σε δίκτυα αισθητήρων για να θεωρηθεί ασφαλές πρέπει να ικανοποιεί μερικές ή όλες από τις έννοιες ασφάλειας που αναφέρθηκαν στο υποκεφάλαιο 3.2. Για την επίτευξη της ασφάλειας, τα πρωτόκολλα που ακολουθούν κάνουν χρήση διάφορων μηχανισμών όπως η κρυπτογράφηση των πακέτων, τα Message Authentication Codes (MACs) και των κατανεμημένων κλειδιών για ασφαλή επικοινωνία.

Στον πίνακα που ακολουθεί φαίνονται τα ασφαλή πρωτόκολλα που έχουν μελετηθεί, ορισμένα από τα χαρακτηριστικά τους, η χρονολογία που προτάθηκαν καθώς επίσης και τυχόν ευπάθειες που έχουν.

Name / Year	Description	Vulnerabilities
Secure and Efficient Intrusion Fault Tolerant Protocol (SEIF) [14] / 2008	• Κατασκευάζει disjoint μονοπάτια χρησιμοποιώντας μια παραλλαγή της branch-aware πλημμύρας • Επιτρέπει την κατασκευή εναλλακτικών μονοπατιών ξεκινώντας από του κόμβου που είναι 2 hops μακριά από τον sink, αντί από τους άμεσους γείτονες του sink • Κάθε κόμβος εξετάζει τα disjoint μονοπάτια που προέρχονται από κόμβους σε διαφορετικά υπο-κλαδιά (sub-branches) • Οι πίνακες δρομολόγησης δημιουργούνται τοπικά από τον κάθε αισθητήρα, χωρίς να εξαρτούνται από τον sink • Ένα μονοπάτι επιλέγεται τυχαία από τον κόμβο για να προωθήσει δεδομένα. Έτσι, αποφεύγεται η επαναχρησιμοποίηση του ίδιου μονοπατιού, αν αυτό έχει παραβιαστεί	• Αν ένας κόμβος κλαπεί, ο εισβολέας μπορεί να μάθει τα κρυπτογραφικά δεδομένα που είναι αποθηκευμένα στον αισθητήρα και να τα χρησιμοποιήσει για να παραβιάσει την εμπιστευτικότητα του δικτύου • Η επίθεση selective forwarding μπορεί να επηρεάσει την κατασκευή της τοπολογίας • Επιθέσεις του τύπου DoS, wormhole και sinkhole μπορούν να επηρεάσουν την κατασκευή των μονοπατιών κάνοντας αισθητήρες που είναι απομακρυσμένοι να

	• Χρησιμοποιείται ένα σύνολο από one-way hash chains για την αυθεντικοποίηση των μηνυμάτων από τον sink και της επικοινωνίας σε ένα sub-branch • Κάθε κόμβος εγκαθιστά ένα broadcasting key για να επικοινωνεί με ασφάλεια με τους γειτονικούς κόμβους	πιστεύουν ότι είναι γείτονες
Multi-version multi-path (MVMP) [14] / 2007	• Αποτελείται από τέσσερις φάσεις • Αρχικά, τα πακέτα δεδομένων χωρίζονται σε ομάδες • Κάθε ομάδα πακέτων κρυπτογραφείται χρησιμοποιώντας διαφορετικούς ασυμμετρικούς και συμμετρικούς αλγόριθμους κρυπτογράφησης • Τα κρυπτογραφημένα πακέτα αναδιοργανώνονται σε μπλοκ κ-πακέτων και γίνεται εφαρμογή της RS(n,k) κωδικοποίησης η οποία παράγει μια κωδική λέξη για κάθε μπλοκ • Κάθε κωδική λέξη στέλνεται στον προορισμός χρησιμοποιώντας πολλαπλά μονοπάτια. Τα πακέτα με την ίδια κωδική λέξη στέλνονται μέσω διαφορετικών μονοπατιών για αύξηση της ασφάλειας • Ο παραλήπτης, θα ανακατασκευάσει το κρυπτογραφημένο μπλοκ αν ληφθούν τουλάχιστον κ πακέτα • Ακολούθως, γίνονται έλεγχοι για αυθεντικοποίηση και ακεραιότητα και αυτοί επιτύχουν ο παραλήπτης θα αποκρυπτογραφήσει το πακέτο	• Ευάλωτο σε επίθεση DoS και σε φυσική κλοπή κόμβων • Αν ένας εισβολέας κλέψει έναν κόμβο, μπορεί να εφαρμόσει την επίθεση selective forwarding ή να κλέψει το κρυπτογραφικό υλικό που είναι αποθηκευμένο στον κόμβο και να εισάγει πλαστά πακέτα στο δίκτυο
Intrusion-tolerant routing protocol for wireless sensor networks (INSENS) [14] / 2002	• Μόνο ο sink μπορεί να κάνει broadcast στο δίκτυο και οι αισθητήρες κάνουν drop τα ίδια μηνύματα (προστασία από DoS flooding) • Χρησιμοποιεί συμμετρική κρυπτογραφία για να παρέχει εμπιστευτικότητα, ακεραιότητα και αυθεντικοποίηση • Κάθε κόμβος μοιράζεται ένα μυστικό κλειδί με τον sink και όχι με άλλους κόμβους	• Κατά την φάση εξεύρεσης μονοπατιών, ένας εισβολέας μπορεί να χρησιμοποιήσει μια επίθεση rushing με ένα τροποποιημένο μήνυμα request ή μπορεί να κάνει επιλεκτικά drop πακέτα. Ωστόσο, η ζημιά από αυτές τις επιθέσεις είναι περιορισμένη σε μια τοπική περιοχή του δικτύου

	• Οι πίνακες δρομολόγησης υπολογίζονται από τον sink και διανέμονται στους αισθητήρες • Κατασκευάζονται εναλλακτικά disjoint μονοπάτια μεταξύ του κάθε αισθητήρα και του sink • Κάθε μήνυμα στέλνεται πολλές φορές από το κάθε εναλλακτικό μονοπάτι • Χρησιμοποιείται one-way hash chain για την αυθεντικόποιηση των μηνυμάτων που στέλνονται από τον sink και υλοποιούνται μηχανισμοί MAC για να πιστοποιηθεί η ακεραιότητα των πακέτων • Αποτελείται από τρεις φάσεις • Αρχικά, ο sink κάνει broadcast ένα μήνυμα request • Ακολούθως, συλλέγει πληροφορίες για την τοπολογία από τους αισθητήρες • Μετά υπολογίζει και προωθεί τους πίνακες δρομολόγησης σε κάθε κόμβο	• Η δεύτερη φάση είναι ευάλωτη σε DoS, σε selective forwarding feedback μηνύματα και τροποποιημένες πληφορίες γειτόνων. Αυτές οι επιθέσει είναι επίσης τοπικές και δεν μπορούν να επηρεάσουν ολόκληρο το δίκτυο • Αν η τοπολογία που υλοποιήθηκε έχει μόνο ένα μονοπάτι από έναν κόμβο στον sink, τότε έρχεται σε αντίθεση με την φιλοσοφία του πρωτοκόλλου για δημιουργία πολλαπλών μονοπατιών
RLEACH [15] / 2008	• Για την εγγύηση ασφαλούς επικοινωνίας χρησιμοποιείται ο μηχανισμός random pair keys (RPK) • Η λειτουργία του δικτύου γίνεται σε πέντε φάσεις • Φάση προ-κατανομής: Τα ID και τα original keys προ-κατανέμονται σε κάθε κόμβο • Φάση share-key discovery: Γίνονται broadcast τα IDs στους γείτονες των κόμβων • Φάση cluster set-up: Κάθε κόμβος αποφασίζει αν θα είναι cluster head για την παρόν φάση. Αν ο κόμβος είναι cluster head θα το διαφημίσει στο δίκτυο • Φάση δημιουργίας χρονοδιαγράμματος: Τα cluster heads δημιουργούν ένα Time Division Multiple Access (TDMA) χρονοδιάγραμμα και το κάνουν broadcast στα μέλη του cluster • Φάση μετάδοσης δεδομένων: Οι κόμβοι στέλνουν δεδομένα στο	• Παρέχει προστασία από επιθέσεις sybil, sinkhole, wormhole, selective forwarding και HELLO flood

	cluster head και αυτό τα προωθεί στον sink	
Secure and Energy-Efficient Multipath routing protocol (SEEM) [15] / 2007	• Ο sink υπολογίζει εναλλακτικά μονοπάτια για να φτάσει στον κάθε κόμβο • Επιλέγει περιοδικά ένα νέο μονοπάτι το οποίο καταναλώνει την ελάχιστη ενέργεια για την δρομολόγηση του πακέτου από τον αποστολέα στον παραλήπτη • Το πρωτόκολλο κατασκευάζει disjoint και braided μονοπάτια χρησιμοποιώντας μια τροποποίηση του αλγορίθμου BFS • Το πρωτόκολλα αντιμετωπίζει την επίθεση replayed ορίζοντας ένα sequence number σε κάθε πακέτο, το οποίο μπορεί να σταλεί μόνο μια φορά • Αφού ο sink αποφασίζει το μονοπάτι δρομολόγησης δεν μπορούν να εφαρμοστούν οι επιθέσεις wormhole και sinkhole	• Ένας εισβολέας μπορεί να κρυφακούσει και να αλλάξει πακέτα, επηρεάζοντας την κατασκευή των μονοπατιών δρομολόγησης και προσθέτοντας ψεύτικους κόμβους στο δίκτυο • Αν κλαπεί ένα σύνολο κόμβων, αυξάνεται η πιθανότητα να είναι πάνω στο μονοπάτι που επέλεξε ο sink και μπορούν να γίνουν drop πακέτα • Το πρωτόκολλα δεν λαμβάνει μέτρα για να απομονώσει κακόβουλους κόμβους ακόμα και αν εντοπιστούν
H-SPREAD [15] / 2006	• Επεκτείνει το SPREAD • Χρησιμοποιεί ένα threshold secret sharing scheme (T,N) το οποίο χωρίζει ένα μήνυμα σε N κομμάτια, που ονομάζονται shares • Κάθε share προωθείται από έναν κόμβο μέσω διαφορετικού μονοπατιού προς τον sink • Στον sink ανακατασκευάζεται το πακέτο αν ληφθούν τουλάχιστον T shares • Κατασκευάζει πολλαπλά disjoint μονοπάτια σε δύο φάσεις • Κατά την πρώτη φάση, χρησιμοποιείται το branch-aware flooding πρωτόκολλο για να βρεθεί ένα σύνολο disjoint μονοπατιών. Με βάση την τοποθεσία οι κόμβοι κάνουν tag τους γείτονες τους ως παιδί, αδελφό ή ξάδερφο (child, sibling, cousin) • Στην φάση δύο, χρησιμοποιείται μια επέκταση της πλημμύρας. Για την μεγιστοποίηση των μονοπατιών, κάθε κόμβος στέλνει τα μονοπάτια	• Ένας εισβολέας μπορεί να εφαρμόσει την επίθεση DoS για να αποτρέψει τους κόμβους να βρουν εναλλακτικά μονοπάτια • Μπορούν να εισαχθούν κακόβουλοι κόμβοι ή να κλαπούν νόμιμοι κόμβοι και να εφαρμοστεί ή επίθεση selective forwarding ή συνδυασμός επιθέσεων wormhole/sinkhole/rushing • Δεν χρησιμοποιούνται μηχανισμοί αυθεντικοποίησης και έτσι ένας εισβολέας μπορεί να υποδηθεί τον sink και να προσελκύσει δεδομένα

	που εντόπισε στον γονέα, στα αδέρφια και ξαδέλφια του • Αν ένας κόμβος εντοπίσει ότι ένα πακέτο δεν μεταδόθηκε επιτυχώς στον sink, αυτό προωθείται από άλλο μονοπάτι αντί να γίνει drop	
Secure Multipath Routing Protocol (SecMR) [15] / 2007	• Βασίζεται σε αυθεντικοποίηση των γειτονικών κόμβων χρησιμοποιώντας ένα Elliptic Curve Cryptosystem (ECC) • Οι κόμβοι υπογράφουν (sign) ψηφιακά τα μηνύματα κατά την φάση αυθεντικοποίησης για να επιτραπεί στους γείτονες τους να επιβεβαιώσουν την ταυτότητα τους • Χρησιμοποιείται η λίστα next hop που περιέχει πιθανά next hops για ένα συγκεκριμένο query δρομολόγησης • Η λίστα δρομολόγησης περιέχει κόμβους που συμμετέχουν στο μονοπάτι δρομολόγησης • Η λίστα εξαίρεσης περιέχει τους κόμβους που δεν επιτρέπεται να συμμετέχουν στο παρόν query δρομολόγησης • Κατά την διάρκεια της φάσης εύρεσης μονοπατιών, ένας κόμβος θα επεξεργαστεί ένα request query αν ο αποστολέας: (α) Ανήκει στην λίστα next hop (β) Αν δεν ανήκει στην λίστα δρομολόγησης (γ) Αν δεν ανήκει στην λίστα εξαίρεσης • Οι λίστες ενημερώνονται από κάθε κόμβο • Ο κόμβος που κάνει το query προσθέτει στο πακέτο τα κλειδιά που θα λάβει ο sink για να επιβεβαιώσει την ακεραιότητα του πακέτου • Ο sink υπολογίζει το μέγιστο σύνολο με τα disjoint μονοπάτια μέχρι ένα αριθμό hops και κάνει broadcast ένα μήνυμα με τα μονοπάτια και την τιμή hash στον αποστολέα • Ο αποστολέας χρησιμοποιεί διάφορες τεχνικές multipath δρομολόγησης	• Είναι ευάλωτο στην επίθεση selective forwarding η οποία μπορεί να αποτρέψει τον εντοπισμό όλων των γειτονικών κόμβων • Αν κλαπούν μερικοί κόμβοι, μπορεί να εφαρμοστεί ένας συνδυασμός των επιθέσεων wormhole και sinkhole για να τροποποιηθούν οι λίστες δρομολόγησης και ο sink να υπολογίσει λανθασμένα μονοπάτια • Ένας εισβολέας μπορεί να παραποιήσει τον έλεγχο ακεραιότητας αλλάζοντας έναν αριθμό μηνυμάτων, τα οποία θα πρέπει να φτάσουν στον προορισμό τους για να εντοπιστεί ότι αλλάχθηκαν

Secure alternate path Routing IN Sensor networks (SeRINS) [14], [15] /2006	• Εντοπίζει και απομονώνει τους κακόβουλους κόμβους που διαφημίζουν λανθασμένες πληροφορίες δρομολόγησης, χρησιμοποιώντας ένα σύστημα αναφοράς γειτόνων • Όταν ένας γείτονας διαφημίσει λανθασμένες πληροφορίες, οι γείτονες του αναφέρουν την ταυτότητά του στον sink. Ο sink ενημερώνει το δίκτυο έτσι ώστε οι κόμβοι να ανακαλέσουν τα σχετικά κλειδιά και να αφαιρέσουν τον κακόβουλο από το δίκτυο • Χρησιμοποιεί συνδεσιμότητα με δέντρα, όπου κάθε κόμβος έχει πολλαπλούς κόμβους – γονείς και προωθεί πακέτα εκ περιτροπής μέσω εναλλακτικών μονοπατιών σε έναν από τους γονείς του • Το δίκτυο εδραιώνει μια νέα τοπολογία δρομολόγησης σε κάθε γύρο • Η επικοινωνία γίνεται χρησιμοποιώντας συμμετρική κρυπτογραφία. Για την επιβεβαίωση ότι τα requests έγιναν από τον sink χρησιμοποιείται one-way hash chain	• Με την χρήση εναλλακτικών μονοπατιών το πρωτόκολλο αντιμετωπίζει την επίθεση selective forwarding αλλά όχι πλήρως. Τα προτεινόμενα εναλλακτικά μονοπάτια δεν εντοπίζουν κακόβουλους κόμβους που εφαρμόζουν επιθέσεις selective forwarding • Κακόβουλοι κόμβοι μπορούν να υλοποιήσουν επιθέσεις DoS, Sybil, wormhole και rushing και να επηρεάσουν την κατασκευή μονοπατιών
Concept of Neighbor Watch System (NWS) designed by Lee and Choi [14], [16] /2006	• Ελέγχει αν ο γείτονας ενός κόμβου έχει προωθήσει πραγματικά ένα πακέτο που έλαβε στους γείτονες του • Αρχίζει εντοπίζοντας single-path μονοπάτια και τα μετατρέπει σε multipath όπου εντοπίστει ασυνήθιστη συμπεριφορά • Για την προστασία της επικοινωνίας χρησιμοποιείται μια επέκταση του LEAP • Κατά τον εντοπισμό γειτόνων, οι κόμβοι αναγνωρίζουν τους γείτονες τους και τους γείτονες των γειτόνων τους • Οι γειτονικοί κόμβοι παράγουν ένα MAC για να πιστοποιήσουν ο ένας τον άλλον μέσα σε ένα χρονικό διάστημα (Tmin) • Αν ένας κόμβος στείλει την λίστα γειτόνων του μέσα σε Tmin, κάθε	• A DoS attack can enforce packet dropping at different nodes so that it manipulates the NWS and multipath is established over single path, consuming nodes resources. • Η αναπαραγωγή παλιών πακέτων μπορεί να οδηγήσει σε κατανάλωση ενέργειας • Παρ’ όλο που ένας κακόβουλος κόμβος εντοπίζεται και παρακάμπτεται μέσω multipath μονοπατιών, δεν λαμβάνονται μέτρα για απαγόρευση της επικοινωνίας του με άλλους κόμβους

	παραλήπτης αποδέχεται την λίστα ως έγκυρη • Κάθε κόμβος αποθηκεύει πιστοποιητικά των γειτόνων του και την σχετική λίστα σε έναν πίνακα γειτόνων • Ένα πακέτο κρυπτογραφείται με ένα cluster key του κόμβου – διαβιβαστή για αποφυγή eavesdropping και επίσης κάθε κόμβος χρησιμοποιεί one-way key chain για αυθεντικοποίηση	• Αν κλαπούν αισθητήρες, μπορούν να ανακτηθούν πληροφορίες όπως κλειδιά κρυπτογράφησης, πιστοποιητικά, λίστες γειτόνων) • Ένας εισβολέας μπορεί να χρησιμοποιήσει παραβιασμένους κόμβους για να ξεκινήσει μια επίθεση man-in-the-middle και να εξαπατήσει το NWS
Security of geographic routing (Abu-Ghazaleh et al.) [14], [17] /2005	• Χρησιμοποιεί κρυπτογραφία δημόσιου κλειδιού για να αποτρέψει εισβολείς από το να υποδυθούν έναν έγκυρο κόμβο ή να έχουν πρόσβαση στα περιεχόμενα ενός πακέτου • Όταν έχει εδραιωθεί ένα μονοπάτι μεταξύ του αποστολέα και του παραλήπτη, οι δύο συμφωνούν για ένα session key • Προτείνεται ένα σχέδιο επιβεβαίωσης τοποθεσίας για να αντιμετωπιστούν οι επιθέσεις Sybil και sinkhole • Χρησιμοποιεί multipath για να αυξήσει την αναλογία παράδοσης πακέτων και διαχείριση εμπιστοσύνης για να εντοπιστούν κακόβουλοι κόμβοι και να αφαιρεθούν από το δίκτυο • Κάθε κόμβος έχει έναν πίνακα δρομολόγησης με τους γείτονες του και τιμές εμπιστοσύνης για τον καθένα • Κάθε φορά που ένας γείτονας προωθεί ένα πακέτο στον προορισμό του, αυξάνεται η τιμή εμπιστοσύνης, αλλιώς μειώνεται • Αν ένας κόμβος έχει τιμή εμπιστοσύνης κάτω από ένα threshold, αφαιρείται από τους πίνακες δρομολόγησης • Για να προωθηθεί ένα πακέτο, ένας κόμβος επιλέγει κ γείτονες με επίπεδο εμπιστοσύνης μεγαλύτερο ή ίσο με το threshold	• Αν ένας εισβολέας εφαρμόσει συχνά μια επίθεση DoS επηρεάζοντας ACK πακέτα ή δεδομένα, το επίπεδο εμπιστοσύνης μερικών κόμβων θα μειωθεί κάτω από το threshold • Ένας εισβολέας μπορεί να αναπαράγει πακέτα δημιουργώντας συμφόρηση και εξαντλώντας την μπαταρία των κόμβων • Αν κλαπούν κόμβοι, είναι προσβάσιμες οι κρυπτογραφικές πληροφορίες σε αυτούς

Secure sensor protocol for information via negotiation (SPINS) [15] / 2001	• Παρέχει δύο ομάδες πρωτοκόλλων ασφάλειας: Sensor Network Encryption Protocol (SNEP) και το μTESLA • Το SNEP παρέχει εμπιστευτικότητα, ακεραιότητα, αυθεντικοποίηση, προστασία από αναπαραγωγή (replay) και φρεσκάδα • Το μTESLA παρέχει authenticated broadcast • Η δομή του δικτύου είναι επίπεδη, ο sink βρίσκεται στην κορυφή • Οι κόμβοι πρέπει να είναι στην εμβέλεια του sink • Ο sink είναι έμπιστος και κάθε κόμβος εμπιστεύεται τον εαυτό του • Για να προστεθούν νέοι κόμβοι πρέπει να έχουν ένα αυθεντικοποιημένο κλειδί • Τα κλειδιά είναι προ-εγκατεστημένα και χρησιμοποιήται η μέθοδος του συμμετρικού κλειδιού • Χρησιμοιποιείται MAC για την πιστοποίηση της αυθεντικότητας	• Οι επιθέσεις wormhole, sinkhole, Sybil και selective forwarding δεν μπορούν να εφαρμοστούν επειδή τα πακέτα γίνονται broadcast • Αντιμετωπίζεται η επίθεση HELLO flood
Efficient secure relay scheme (ESRS) [14] / 2008	• Περιλαμβάνει δύο φάσεις • Η πρώτη φάση εδραιώνει ένα ασφαλές μονοπάτι για να προστατέψει τα δεδομένα που προωθούνται. Κάθε κόμβος μοιράζεται ένα κλειδί με τον sink το οποίο χρησιμοποιείται για αυθεντικοποίηση και για κρυπτογράφηση των πακέτων • Κατά την εύρεση μονοπατιών εντοπίζεται ένα έμπιστο και power-aware μονοπάτι, αποφεύγοντας τους κόμβους που υπάρχουν στην μη έμπιστων κόμβων και χρησιμοποιώντας έναν power-aware αλγόριθμο • Στην δεύτερη φάση παρακολουθείται η συμπεριφορά των κόμβων κατά την μεταφορά των δεδομένων. Οι κόμβοι παρακολουθούν αν οι γείτονες τους προώθησαν τα δεδομένα στον προορισμό και αποφασίζουν αν έγινε μια επίθεση	• Η φάση εύρεσης μονοπατιών είναι ευάλωτη αφού τα πακέτα δεν κρυπτογραφούνται • Μπορεί να εφαρμοστούν οι επιθέσεις hello, wormhole, sinkhole και οι κόμβοι να πειστούν ότι βρίσκονται μακριά • Ένας κακόβουλος κόμβος μπορεί να αναφέρει λανθασμένα επίπεδα μπαταρίας και να επηρεάσει τον power-aware αλγόριθμο • Μπορεί να χρησιμοποιηθεί μια επίθεση man-in-the-middle για να αλλάξει το κόστος των πακέτων που στέλνονται μεταξύ των κόμβων και να επηρεαστεί η επιλογή μονοπατιών • Αν μια επίθεση DoS εφαρμοστεί σε

	• Αν επιβεβαιωθεί ότι έγινε μια επίθεση, οι κόμβοι ειδοποιούνται, ο ύποπτος κόμβος προστίθεται στην λίστα μη έμπιστων κόμβων και η μεταφορά δεδομένων τερματίζεται • Ακολούθως, οι κόμβοι βρίσκουν εναλλακτικά μονοπάτια για να προωθήσουν τα πακέτα τους στον προορισμό	διαφορετικούς κόμβους, το πρωτόκολλο αναγκάζεται να αντιληφθεί τους κόμβους ως κακόβουλους και να τους προσθέσει ως μη έμπιστους. Έτσι, επηρεάζεται η συνδεσιμότητα του δικτύου.
Secure and robust multipath routing protocol (SAODV-MAP) [14] / 2007	• Εντοπίζει disjoint και braided μονοπάτια • Η φάση εντοπισμού γειτόνων προστατεύεται από κρυπτογραφία δημόσιου κλειδιού • Κάθε κόμβος επικυρώνει το πιστοποιητικό του γείτονα του και αν η πιστοποίηση είναι επιτυχής, τότε και οι δύο κόμβοι προσθέτουν ο ένας τον άλλον στο πίνακα γειτόνων τους • Ο εντοπισμός μονοπατιών προστατεύεται από ένα HMAC shared key μεταξύ του αποστολέα και του sink για να πιστοποιηθεί η ακεραιότητα του πακέτου • Κάθε κόμβος ελέγχει αν ο αποστολέας είναι στον πίνακα γειτόνων του και το πεδίο του πακέτου για κύκλους. Αν εντοπιστεί ασυνήθιστη συμπεριφορά το πακέτο γίνεται drop • Κάθε κόμβος κρυφακούει τις μεταδόσεις των γειτόνων του και πιστοποιεί ότι το πακέτο προωθήθηκε με την σωστή πληροφορία δρομολόγησης. Αν η μετάδοση πιστοποιηθεί τότε ο κόμβος προσθέτει τον γείτονα σε μια λίστα προώθησης. • Όταν ληφθεί μια απάντηση σε route request, προωθείται στο επόμενο hop μόνο αν αποστολέας είναι στην λίστα προώθησης • Χρησιμοποιείται ένα timestamp και μια ψηφιακή υπογραφή για την αυθεντικοποίηση του route request error πακέτου και για την επιβεβαίωση της φρεσκάδας	• Επιθέσεις όπως sinkhole και wormhole μπορούν να επηρεάσουν την εδραίωση του μονοπατιού δρομολόγησης όταν γίνει ένα route request • Η ύπαρξη κακόβουλων γειτονικών κόμβων μπορεί να ξεγελάσει έναν ενδιάμεσο κόμβο ότι οι γείτονες του όντως έχουν προωθήσει το πακέτο του χρησιμοποιώντας το σωστό μονοπάτι

Secure SPIN [15] / 2006	• Επεκτείνει το SPIN • Χρησιμοποιεί Message Authentication Code (MAC) για να εγγυηθεί την ορθότητα και την ακεραιότητα των μηνυμάτων • Βασίζεται σε clusters • Δεν μπορούν να προστεθούν νέοι κόμβοι • Αναξιόπιστη επικοινωνία (δεν στέλνονται ACKs) • Χρησιμοποιείται συμμετρικό κλειδί για να κωδικοποιηθούν τα μηνύματα • Τρεις φάσεις: Διαφήμιση των δεδομένων που συλλέχθηκαν, αίτηση δεδομένων από τους κόμβους και μετάδοση των δεδομένων	• Οι επιθέσεις Sybil, sinkhole και wormhole δεν μπορούν να εφαρμοστούν • Αν κλαπεί ένας κόμβος που είναι cluster head μπορεί να γίνει επίθεση selective forwarding
Just Enough Redundancy Transmission (JERT) [14] / 2008	• Χρησιμοποιεί Maximum Distance Separable codes (MDS). • Αφού τελειώσει η διαδικασία της προκατανομής των κλειδιών, το μυστικό κλειδί κωδικοποιείται σε MDS κωδικό από τον αποστολέα και προωθείται μέσω πολλαπλών multihop μονοπατιών στον προορισμό • Λειτουργεί με braided ή disjoing μονοπάτια και με διάφορα μήκη μονοπατιών • Το πρωτόκολλο μπορεί να χρησιμοποιήσει ένα ήδη υπάρχον σύστημα για υπολογισμό των εναλλακτικών μονοπατιών • Όταν υπάρξει σφάλμα στην μετάδοση, παρέχονται στον παραλήπτη τα αναγκαία symbols για την διόρθωση των λαθών	• Αν κλαπούν αισθητήρες μπορεί να χρησιμοποιηθούν τα κλειδιά τους για να κρυπτογραφηθούν/ αποκρυπτογραφηθούν/ τροποποιηθούν μηνύματα ή να γίνει επίθεση selective forwarding • Μια επίθεση DoS μπορεί να εφαρμοστεί αναγκάζοντας τον κόμβο – προορισμό να ζητήσει επαναμετάδοση των πακέτων λόγω σφαλμάτων, προκαλώντας συμφόρηση και εξάντληση ενέργειας
Path redundancy based security algorithm (PRSA) [14], [18] /2007	• Υπολογίζει disjoint και braided multipath μονοπάτια, χρησιμοποιώντας τον αλγόριθμο του Dijkstra και χρησιμοποιεί ένα συνδυασμό τεχνικών μετάδοσης για παράδοση των πακέτων (round-robin, redundant και selective) • Ορίζεται ένα σύνολο παραμέτρων (ενέργεια του κόμβου, μηνύματα HELLO, hops μέχρι τον προορισμό) για εντοπισμό των κακόβουλων κόμβων	• Δεν προσφέρει μηχανισμούς πρόληψης και είναι ευάλωτο σε επιθέσεις DoS, Sybil, wormhole, sinkhole και replayed • Η επικοινωνία μπορεί να υποκλαπεί και ο εισβολέας μπορεί να διαβάσει και να αλλάξει δεδομένα ή να επηρεάσει την κατασκευή μονοπατιών έτσι ώστε να

	• Αν ένας κόμβος αναγνωριστεί ως κακόβουλος, ο κόμβος αυτός και τα μονοπάτια του εξαιρούνται από την διαδικασία υπολογισμού μονοπατιού	συμπεριλαμβάνεται σε αυτά
Certainty Based Secure Routing Protocol (CBSRP) [15] / 2006	• Χρησιμοποιεί clusters • Το επίπεδο ασφάλειας αλλάζει δυναμικά ανάλογα με τις ανάγκες της εφαρμογής και τα επίπεδα ενέργειας • Εφαρμόζει Advanced Encryption Standard (AES) για να παρέχει μυστικότητα των δεδομένων και αυθεντικοποίηση • Χρησιμοποιεί μια τιμή βεβαιότητας για να παράγει νέα κλειδιά για την μεταφορά των μηνυμάτων. Η τιμή αυτή ορίζει πόσο έμπιστο είναι το περιεχόμενο του πακέτου • Αρχικά ένα κλειδί και μια συνάρτηση χρησιμοποιούνται για παραγωγή νέων κλειδιών. Τα νέα κλειδιά υπολογίζονται δυναμικά • Για αποκωδικοποίηση του πακέτου, χρησιμοποιείται η μέθοδος συμμετρικού κλειδιού • Το δίκτυο μπορεί να αναδιοργανωθεί όταν ζητηθεί από τον sink	• Μπορεί να εφαρμοστεί η επίθεση wormhole στον cluster head. Με βάση το πρωτόκολλο, τα cluster heads διαγράφουν από την μνήμη τους το κλειδί και την συνάρτηση που χρησιμοποιήθηκε για παραγωγή κλειδιών. Επομένως, δεν μπορούν να αποκρυπτογραφήσουν τα πακέτα που λαμβάνονται και τα προωθούν στον προορισμό τους.
Secure Directed Diffusion (SDD) [15] / 2011	• Απαιτεί την ύπαρξη ενός sink ο οποίος μοιράζεται ένα μυστικό κλειδί με κάθε κόμβο • Χρησιμοποιείται συμμετρική κρυπτογραφία και μια one-way hash συνάρτηση για ασύμμετρη κρυπτογραφία • Σε όλους τους κόμβους παρέχεται η πρώτη τιμή της one-way key συνάρτησης. Ο sink γνωρίζει όλα τα κλειδιά για να πιστοποιεί τα μηνύματα του. • Έχει τις ίδιες φάσεις με το Directed Diffusion αλλά σε κάθε φάση προστατεύεται η ακεραιότητα και η αυθεντικότητα	• Ανθεκτικό σε σχεδόν όλες τις γνωστές επιθέσεις

Τα πιο πάνω πρωτόκολλα δρομολόγησης μπορούν να διαχωριστούν με βάση τις επιθέσεις που έχουν την ικανότητα να αντιμετωπίσουν όπως φαίνεται πιο κάτω.

Attack Type	Protocols which address the attack
Selective Forwarding	RLEACH, SEEM, SeRINS, Lee and Choi, Abu-Ghazaleh, SPINS, ESRS, SAODM-MAP, Secure SPIN, SDD
Sinkhole	RLEACH, SEEM, SeRINS, Lee and Choi, Abu-Ghazaleh, SPINS, Secure SPIN, CBSRP, SDD
Sybil	SEIF, INSENS, RLEACH, SecMR, Abu-Ghazaleh, SPINS, ESRS, SAODV-MAP, Secure SPIN, CBSRP, SDD
Wormhole	RLEACH, Lee and Choi, Abu-Ghazaleh, SPINS, Secure SPIN, SDD
HELLO Flood	SEIF, INSESNS, RLEACH, Lee and Choi, Abu-Ghazaleh, SPINS, Secure SPIN, SDD
Replayed	SEIF, INSENS, SEEM, H-SPREAD, SecMR, SeRINS, ESRS, SAODV-MAP
Denial of Service	INSENS, ESRS, SAODV-MAP

Κεφάλαιο 4

Το Πρωτόκολλο Δρομολόγησης RPL

4.1 Εισαγωγή

Τα περισσότερα πρωτόκολλα δρομολόγησης για ασύρματα δίκτυα αισθητήρων αποτελούν θεωρητικές προτάσεις και δεν έχουν υλοποιηθεί. Για τους σκοπούς αυτής της εργασίας επιλέχθηκε το πρωτόκολλο δρομολόγησης για δίκτυα χαμηλής ισχύος και με απώλειες (Routing Protocol for Low-power and lossy networks – RPL). Το RPL έχει προταθεί από την ομάδα εργασίας ROLL (Routing Over Low power and Lossy) για χρήση σε δίκτυα χαμηλής ισχύος (Low power and Lossy Networks - LLN) όπως τα δίκτυα αισθητήρων. Σήμερα, το RPL αποτελεί ένα διεθνές αναγνωρισμένο και εγκεκριμένο πρότυπο που χρησιμοποιείται ευρέως για διάφορες εφαρμογές των ασύρματων δικτύων αισθητήρων. Για τον λόγο αυτό, θελήσαμε να το αξιολογήσουμε πειραματικά ως προς την ασφάλεια που παρέχει εναντίον συγκεκριμένων τύπων επιθέσεων.

Το RPL υποστηρίζει την τελευταία έκδοση του Internet Protocol, το IPv6. Ο κυρίως στόχος του συγκεκριμένου πρωτοκόλλου είναι να παρέχει αποδοτικά μονοπάτια δρομολόγησης για Point to Multipoint (P2MP) και Multipoint to Point (MP2P) ροές δεδομένων. [19], [20]

4.2 Περιγραφή Λειτουργίας

Το RPL είναι ένα distance vector πρωτόκολλο δρομολόγησης το οποίο χρησιμοποιεί το IPv6 για την λειτουργία του. Οι συσκευές που κάνουν χρήση του πρωτοκόλλου είναι συνδεδεμένες έτσι ώστε να μην υπάρχουν κύκλοι στην τοπολογία. Γι' αυτόν τον λόγο, κτίζεται ένας προσανατολισμένος άκυκλος κατευθυνόμενος γράφος (Destination Oriented Directed Acyclic Graph - DODAG). Ο γράφος είναι προσανατολισμένος προς μια ρίζα, η οποία συνήθως είναι ο κόμβος sink. Η δημιουργία του DODAG γίνεται χρησιμοποιώντας μια συνάρτηση στόχου (Objective Function – OF), η οποία καθορίζει τα μετρικά (metrics) και τους περιορισμούς (constraints) που θα ληφθούν υπόψη για τον υπολογισμό του καλύτερου μονοπατιού. Το Objective Function μπορεί να αλλάξει ανάλογα με την εφαρμογή και τις απαιτήσεις του δικτύου.

Ο γράφος που κτίζεται αποτελεί μια λογική τοπολογία δρομολόγησης πάνω στο φυσικό δίκτυο. Στο ίδιο δίκτυο μπορούν να υπάρξουν πολλοί γράφοι για εξυπηρέτηση διαφορετικών απαιτήσεων. Ένας κόμβος του δικτύου έχει την δυνατότητα να συμμετέχει σε έναν ή περισσότερους γράφους, οι οποίοι αναφέρονται ως RPL παρουσίες (RPL instances). [21]

4.2.1 Μηνύματα Ελέγχου στο RPL

Το RPL καθορίζει ένα σύνολο από νέα ICMPv6 (Internet Control Message Protocol version 6) μηνύματα ελέγχου για να γίνεται η ανταλλαγή πληροφοριών του γράφου στο δίκτυο. Αυτά τα μηνύματα ελέγχου περιγράφονται πιο κάτω.

DODAG Information Object (DIO): Είναι η κύρια πηγή των πληροφοριών δρομολόγησης. Χρησιμοποιείται κατά την κατασκευή του DODAG και για διαφήμιση διάφορων πληροφοριών σχετικά με τον γράφο. Περιέχει μεταξύ άλλων τον βαθμό ενός κόμβου (rank), το RPL instance και την διεύθυνση της ρίζας.

DODAG Destination Advertisement Object (DAO): Στέλνεται από τους κόμβους στο κάτω μέρος του γράφου, προς την πάνω κατεύθυνση του γράφου (προς τον sink) μεταφέροντας πληροφορίες δρομολόγησης. Κάθε κόμβος στέλνει μήνυμα DAO στον γονέα (parent) του. Με αυτόν τον τρόπο, υποστηρίζεται η δρομολόγηση προς την κάτω

κατεύθυνση του γράφου (Point to Multipoint). Ο κόμβος που λαμβάνει ένα μήνυμα DAO, το χρησιμοποιεί για να ενημερώσει τον πίνακα δρομολόγησης του.

DAO-ACK: Στέλνεται ως απάντηση σε ένα μήνυμα τύπου DAO επιβεβαιώνοντας την παραλαβή του.

DODAG Information Solicitation (DIS): Στέλνεται στους γείτονες ενός κόμβου ως αίτημα για πληροφορίες δρομολόγησης. Όταν ένας κόμβος λάβει μήνυμα DIS θα απαντήσει στον αποστολέα με ένα μήνυμα τύπου DIO.

4.2.2 Trickle timers

Αφού οι περισσότερες συσκευές που σχηματίζουν το δίκτυο κάνουν χρήση μπαταριών ως πηγή ενέργειας, είναι ζωτικής σημασίας να περιοριστεί ο αριθμός των μηνυμάτων ελέγχου στο δίκτυο. Όσον αφορά την συντήρηση (maintenance) του δικτύου, το πρωτόκολλο RPL χρησιμοποιεί τα χρονόμετρα trickle (trickle timers). Τα χρονόμετρα αυτά ελέγχουν την συχνότητα των μηνυμάτων DIO. Το χρονικό διάστημα που στέλνονται τα μηνύματα DIO ξεκινά από μια αρχική τιμή Tmin και αυξάνεται όσο το δίκτυο σταθεροποιείται. Επομένως, μειώνεται ο αριθμός των μηνυμάτων DIO που στέλνονται στο δίκτυο. Το χρονικό διάστημα μπορεί να αυξηθεί μέχρι μια σταθερή τιμή Tmax.

Όταν εντοπιστεί μια ασυνέπεια (inconsistency) στο δίκτυο τότε το χρονόμετρο επαναφέρεται (reset) στην αρχική τιμή Tmin για να σταλούν πιο συχνά τα μηνύματα DIO και να διορθωθεί η ασυνέπεια. Ως ασυνέπεια θεωρείται ο εντοπισμός κύκλου (loop) στον γράφο, η είσοδος ενός νέου κόμβου στον γράφο και η μετακίνησή ενός κόμβου στο δίκτυο. Επίσης, το χρονόμετρο γίνεται reset όταν παραληφθεί ένα μήνυμα τύπου DIS.

4.2.3 Κατασκευή Γράφου DODAG

Η κατασκευή του γράφου αρχίζει από τον sink (ρίζα του γράφου). Ο sink αρχικά θα στείλει μήνυμα τύπου DIO σε όσους κόμβους βρίσκονται στην εμβέλειά του. Ένας κόμβος που θα λάβει το DIO, θα αποφασίσει με βάση το objective function αν θα ενταχθεί στον γράφο ή όχι. Όταν ο κόμβος ενταχθεί στον γράφο, τότε θα έχει ένα μονοπάτι προς τον sink, ο οποίος αποτελεί τον γονέα του. Ακολούθως, ο κόμβος θα υπολογίσει τον βαθμό (rank) που έχει στον γράφο ο οποίος αντιπροσωπεύει την θέση του σε σχέση με

τον sink. Η τιμή του rank είναι ακέραια και αυξάνεται όσο πιο μακριά από τον sink είναι ένας κόμβος. Αντίστοιχα, μειώνεται όσο πιο κοντά στον sink βρίσκεται ένας κόμβος. Ο sink έχει rank ίσο με ένα. Αφού γίνει ο υπολογισμός του rank, ο κόμβος θα στείλει μήνυμα DIO σε όσους κόμβους βρίσκονται στην εμβέλειά του διαφημίζοντας τον γράφο.

Η διαδικασία αυτή επαναλαμβάνεται από όλους τους κόμβους μέχρι να κατασκευαστεί ολόκληρος ο γράφος για την τοπολογία. Όταν η κατασκευή του γράφου ολοκληρωθεί, κάθε κόμβος θα έχει ορισμένο έναν γονέα και έτσι θα μπορεί να στείλει πακέτα στον sink προωθώντας τα στον γονέα του. Αυτό το μοντέλο αναπαριστά την προώθηση Multipoint to Point αφού κάθε κόμβος έχει την δυνατότητα να στείλει πακέτα στον sink. Η προώθηση αυτή αναφέρεται και ως δρομολόγηση προς τα πάνω.

Εκτός από Multipoint to Point δρομολόγηση δεδομένων (προς τον sink), είναι απαραίτητη και η δρομολόγηση Point to Multipoint δεδομένων που έχουν σαν προορισμό διάφορους κόμβους στο δίκτυο. Επομένως, είναι αναγκαία η ύπαρξη ενός πίνακα δρομολόγησης (routing table) σε κάθε κόμβο. Αυτό επιτυγχάνεται με τα μηνύματα DAO τα οποία χρησιμοποιούνται για να διαφημιστεί η προσβασιμότητα προς τους κόμβους - φύλλα. Όταν ένας κόμβος εισαχθεί στον γράφο θα στείλει ένα DAO μήνυμα στον γονέα του με πληροφορίες για την προσβασιμότητα που έχει προς άλλους κόμβους. Κάθε κόμβος που θα λάβει ένα DAO μήνυμα θα ενημερώσει σχετικά τον πίνακα δρομολόγησης του και θα το προωθήσει στον γονέα του. Το μήνυμα συνεχίζει να κινείται προς το πάνω μέρος του γράφου μέχρι να φτάσει στον sink.

Το πρωτόκολλο RPL υποστηρίζει επίσης και Point to Point (P2P) επικοινωνία από έναν κόμβο σε έναν άλλο στον γράφο. Για να επιτευχθεί η P2P επικοινωνία το πακέτο του αποστολέα κινείται προς τα πάνω στον γράφο μέχρι να φτάσει σε έναν κοινό «πρόγονο» του αποστολέα και του παραλήπτη. Ακολούθως, το πακέτο προωθείται προς τα κάτω, μέχρι να φτάσει στον παραλήπτη.

4.2.4 Μηχανισμός Διόρθωσης

Το RPL υποστηρίζει μηχανισμούς για διόρθωση του γράφου όταν παρουσιαστούν ασυνέπειες. Οι μηχανισμοί αυτοί ονομάζονται τοπική διόρθωση (local repair) και καθολική διόρθωση (global repair).
Η τοπική διόρθωση μπορεί να ενεργοποιηθεί όταν για παράδειγμα ένας κόμβος μείνει χωρίς γονέα (λόγω βλάβης στον κόμβο - γονέα) και συνεπώς δεν έχει μονοπάτι προς τον sink. Η διόρθωση του είδους αυτού δεν επηρεάζει ολόκληρο τον γράφο. Όμως, μετά από ορισμένες τοπικές διορθώσεις ο γράφος μπορεί να αρχίσει να αποκλίνει από την βέλτιστη μορφή του και να είναι απαραίτητη η χρήση της καθολικής διόρθωσης.
Η καθολική διόρθωση κατασκευάζει ξανά ολόκληρο τον γράφο από την αρχή. Η διαδικασία αυτή μπορεί να επαναφέρει τον γράφο στην βέλτιστή του μορφή αλλά έχει μεγάλο κόστος λόγω των επιπλέον μηνυμάτων ελέγχου στο δίκτυο. Μόνο η ρίζα του γράφου (sink) μπορεί να ενεργοποιήσει την καθολική διόρθωση. Ακολούθως, ο κάθε κόμβος θα τρέξει ξανά την συνάρτηση στόχου (objective function) και θα γίνει επιλογή γονέων.

4.2.5 Αποφυγή Κύκλων – Εντοπισμός Κύκλων (Loop Avoidance – Loop Detection)

Στο RPL καθορίζονται δύο κανόνες για αποφυγή δημιουργίας κύκλων στον γράφο (loop avoidance). Οι κανόνες αυτοί βασίζονται στον βαθμό (rank) των κόμβων. Αρχικά, ένας κόμβος δεν επιτρέπεται να διαλέξει ως γονέα του έναν κόμβο με μεγαλύτερο rank από το δικό του. Επίσης, ένας κόμβος δεν επιτρέπεται να είναι άπληστος και να προσπαθήσει να μετακινηθεί πιο κάτω στον γράφο έτσι ώστε να αυξήσει των αριθμό των γονέων του.
Επιπρόσθετα, το RPL μπορεί να εντοπίσει τους κύκλους στον γράφο (loop detection) χρησιμοποιώντας πεδία ελέγχου στα πακέτα. Σε ένα πακέτο που κινείται στο δίκτυο εξετάζεται αν το rank του αποστολέα (που είναι αποθηκευμένο στο πακέτο) είναι μικρότερο από το rank του παραλήπτη. Σε αυτή την περίπτωση το πακέτο πρέπει να γίνει drop, να γίνει reset το χρονόμετρο για τα DIO και να ενεργοποιηθεί ο μηχανισμός τοπικής διόρθωσης.

Κεφάλαιο 5

Υλοποίηση στο Contiki OS

5.1 Λειτουργικό Σύστημα Contiki

Για την μελέτη του πρωτοκόλλου δρομολόγησης RPL, την διενέργεια επιθέσεων σε αυτό και για την διεξαγωγή προσομοιώσεων, χρησιμοποιήθηκε το λειτουργικό σύστημα Contiki 2.5. Το Contiki OS είναι ένα λειτουργικό σύστημα ανοικτού κώδικα για δικτυωμένες συσκευές. Το σύστημα αυτό, είναι γραμμένο σε γλώσσα προγραμματισμού C και μπορεί να τρέξει σε μια ποικιλία από πλατφόρμες συμπεριλαμβανομένου και προσωπικών υπολογιστών μέσω του περιβάλλοντος Ubuntu. Επιπρόσθετα, ο κώδικας που γράφεται στο Contiki μπορεί να χρησιμοποιηθεί ως έχει στους ασύρματους αισθητήρες. [22]

Το Contiki χρησιμοποιείται σήμερα σε συστήματα συναγερμού, ανίχνευσης υγρασίας, εντοπισμού ακτινοβολίας, βιομηχανικής παρακολούθησης και διάφορα άλλα. Είναι σχεδιασμένο για χρήση σε συσκευές μικρού μεγέθους, οι οποίες έχουν περιορισμένη μνήμη και ενέργεια.

Στο Contiki OS υπάρχουν δύο στοίβες επικοινωνίας οι οποίες είναι η uIP και η Rime.

Η στοίβα uIP παρέχει την δυνατότητα επικοινωνίας μέσω των πρωτοκόλλων που ορίζει η στοίβα TCP/IP. Η uIP είναι μικρή, απλή και περιέχει πρωτόκολλα όπως το IP, IPv6, UDP, TCP και ICMP. Το IPv6 στο Contiki OS αποτελεί συνεισφορά της Cisco και περιέχει το πρωτόκολλο RPL το οποίο χρησιμοποιείται για την παρούσα εργασία.

Η στοίβα Rime είναι μια μικρή στοίβα επικοινωνίας η οποία υποστηρίζει απλές λειτουργίες όπως η αποστολή ενός μηνύματος σε όλους τους γείτονες ή σε ένα συγκεκριμένο γείτονα. Επίσης, υποστηρίζει και πιο πολύπλοκες λειτουργίες όπως η πλημμύρα του δικτύου (network flooding) και η συλλογή δεδομένων χωρίς χρήση διευθύνσεων (address-free data collection). Οι αρχέγονοι τύποι επικοινωνίας που έχει υλοποιημένους η Rime, μπορούν να χρησιμοποιηθούν από μόνοι τους ή να συνδυαστούν για να δημιουργήσουν πιο πολύπλοκα πρωτόκολλα και μηχανισμούς. [23]

5.2 Εργαλείο Προσομοίωσης Cooja

Το λειτουργικό σύστημα Contiki περιλαμβάνει το εργαλείο προσομοίωσης Cooja το οποίο έχει την δυνατότητα να προσομοιώσει την λειτουργία δικτύων από κόμβους που τρέχουν το Contiki OS. Το Cooja μπορεί να προσομοιώσει την λειτουργία των κόμβων με την χρήση μόνο ενός υπολογιστή, χωρίς την ύπαρξη οποιουδήποτε επιπλέον υλικού. Οι προσομοιώσεις μπορούν να γίνουν σε δίκτυα μεγάλου μεγέθους, βοηθώντας έτσι στην αξιολόγηση και στην απασφαλμάτωση του κώδικα. Ακόμα, υπάρχουν έτοιμα παραδείγματα στο Contiki OS τα οποία μπορούν να τρέξουν στο Cooja. Ο προσομοιωτής βρίσκεται κάτω από τον φάκελο /tools/cooja και είναι γραμμένος σε γλώσσα προγραμματισμού Java.

5.3 Flooding

Για την υλοποίηση της επίθεσης πλημμύρας (flooding) έγιναν αλλαγές στο αρχείο core/net/rpl/rpl-timers.c το οποίο περιέχει τον κώδικα που είναι υπεύθυνος για την διαχείριση των διάφορων χρονομέτρων που χρησιμοποιεί το RPL. Οι αλλαγές έγιναν στις συναρτήσεις new_dio_interval και handle_dio_timer. Η πρώτη συνάρτηση, καλείται για να υπολογιστεί το χρονικό διάστημα (interval) με το οποίο θα στέλνονται τα μηνύματα DIO του κόμβου. Η δεύτερη συνάρτηση, υλοποιεί την λειτουργία της αύξησης του χρονομέτρου για τα μηνύματα DIO.

Η συνάρτηση new_dio_interval τροποποιήθηκε έτσι ώστε το χρονικό διάστημα που επιστρέφει να είναι πάντα σταθερό (έγιναν προσομοιώσεις για interval ίσο με 1024, 4096 και 16384 milliseconds). Επιπρόσθετα, η συνάρτηση handle_dio_timer αλλάχθηκε έτσι

ώστε να μην αυξάνεται καθόλου το χρονόμετρο του κακόβουλου κόμβου κατά την διάρκεια της προσομοίωσης.
Με την επίθεση flooding ο κακόβουλος κόμβος θα στέλνει μηνύματα DIO με σταθερό χρονικό διάστημα, πλημμυρίζοντας το δίκτυο. Επίσης, ενώ τα χρονόμετρα των υπόλοιπων κόμβων θα αυξάνονται κατά την διάρκεια της λειτουργίας του δικτύου, το χρονόμετρο του κακόβουλου δεν θα αυξηθεί καθόλου. [24]

5.4 Selective Forwarding

Η προώθηση και η αποστολή των πακέτων δεδομένων στο πρωτόκολλο RPL γίνεται με την χρήση της στοίβας επικοινωνίας uIP. Για να πραγματοποιηθεί η επίθεση επιλεκτικής προώθησης (selective forwarding) έγιναν μετατροπές στο αρχείο /core/uip6.c. Το συγκεκριμένο αρχείο αποτελεί ένα κομμάτι της στοίβας επικοινωνίας uIP για IPv6 δίκτυα και υλοποιεί τον κώδικα για την προώθηση των πακέτων δεδομένων.
Αρχικά, δηλώθηκε μια σταθερά ratio ακέραιου τύπου η οποία αντιπροσωπεύει την πιθανότητα με την οποία ο κακόβουλος κόμβος θα απορρίψει (θα κάνει drop) ένα πακέτο. Ακολούθως, στην συνάρτηση uip_process υπολογίζεται ένας τυχαίος αριθμός από μηδέν μέχρι εκατό. Αν ο αριθμός αυτός είναι μεγαλύτερος από το ratio, τότε το πακέτο προωθείται κανονικά, διαφορετικά γίνεται drop. Για παράδειγμα, αν το ratio έχει τιμή πενήντα, τότε ο κακόβουλος κόμβος θα κάνει drop τα εισερχόμενα πακέτα δεδομένων με πιθανότητα 50%. Έγιναν προσομοιώσεις με τιμές ratio από δέκα μέχρι εκατό, αυξάνοντας κατά δέκα κάθε φορά.

5.5 Black Hole

Η προεπιλεγμένη συνάρτηση στόχου στην υλοποίηση του RPL στο Contiki OS χρησιμοποιεί ως μετρικό το ETX (estimated number of transmissions). Η τιμή του ETX αντιπροσωπεύει τον αναμενόμενο αριθμό μεταδόσεων που θα γίνουν στον σύνδεσμο (link) για να σταλεί ένα πακέτο. Η συγκεκριμένη συνάρτηση έχει ως στόχο την επιλογή του κόμβου που έχει την μικρότερη τιμή ETX. Ο κόμβος αυτός θα οριστεί ως γονέας για να προωθούνται τα πακέτα σε αυτόν. [25]
Όσον αφορά την επίθεση μαύρης τρύπας (black hole) έγιναν αλλαγές στο αρχείο /core/net/rpl/rpl-of-etx.c, το οποίο περιέχει τις λειτουργίες σχετικά με την συνάρτηση

στόχου. Για την υλοποίηση της επίθεσης τροποποιήθηκε η συνάρτηση update_metric_container έτσι ώστε ο κακόβουλος κόμβος να δηλώνει ότι έχει ETX ίσο με ένα. Με αυτόν τον τρόπο, ο κακόβουλος κόμβος θα διαφημίζει ότι ο αναμενόμενος αριθμός μεταδόσεων για να φτάσει ένα πακέτο στον sink, αν περάσει από αυτόν, θα είναι ίσος με ένα. Δηλαδή, δηλώνει ότι έχει τον sink γείτονα του. Επομένως, με την ελκυστική αυτή διαφήμιση, υπάρχει πιθανότητα ο κακόβουλος κόμβος να προσελκύσει περισσότερα πακέτα που κινούνται στο δίκτυο. [26]

5.6 Sinkhole

Για την υλοποίηση της επίθεσης sinkhole έγινε τροποποίηση του αρχείου /core/net/rpl/rpl-of-etx.c με παρόμοιο τρόπο όπως και για την επίθεση black hole, με την διαφορά ότι η τιμή ETX που θα διαφημίσει ο κακόβουλος κόμβος είναι ίση με μηδέν. Επιπρόσθετα, τροποποιήθηκε το αρχείο /core/net/rpl/rpl-icmp6.c, το οποίο διαχειρίζεται τα διάφορα μηνύματα ελέγχου (DIO, DAO, DIS) του RPL. Αλλάχθηκε η συνάρτηση dio_output, έτσι ώστε τα μηνύματα DIO που θα σταλούν να περιέχουν την εσφαλμένη πληροφορία ότι ο κόμβος έχει rank ίσο με ένα. Με αυτόν τον τρόπο, ο κακόβουλος κόμβος θα διαφημίσει τιμές rank και ETX ίσες με αυτές που έχει ο sink.
Επίσης, ο κόμβος που υλοποιεί την επίθεση sinkhole δεν θα στέλνει πακέτα δεδομένων, ούτε θα προωθεί αυτά που λαμβάνει από τους κόμβους – παιδιά του. Αυτό επιτεύχθηκε με την τροποποίηση του αρχείου /core/uip6.c. [27]

Κεφάλαιο 6

Πειραματισμός και Εξαγωγή Αποτελεσμάτων

6.1 Στοιχεία των Προσομοιώσεων

Στο κεφάλαιο αυτό θα παρουσιαστούν τα σενάρια που χρησιμοποιήθηκαν για τις προσομοιώσεις των επιθέσεων που υλοποιήθηκαν και επίσης τα αποτελέσματα που προέκυψαν από αυτά.

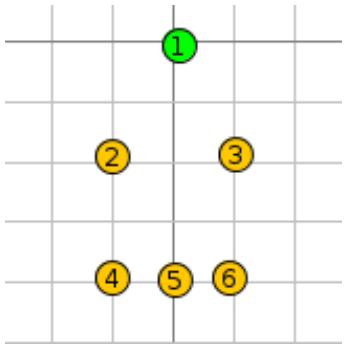
Η υλοποίηση του πρωτοκόλλου δρομολόγησης RPL που χρησιμοποιήθηκε στο Contiki OS μπορεί να βρεθεί κάτω από τον φάκελο /core/net/rpl.

Ως εφαρμογή (application) για τις προσομοιώσεις που εκτελέστηκαν χρησιμοποιήθηκε το παράδειγμα που υπάρχει στο /examples/ipv6/rpl-udp. Το παράδειγμα αυτό, αποτελεί μια απλή εφαρμογή αποστολής δεδομένων μέσω μιας σύνδεσης UDP από τους clients (ασύρματοι αισθητήρες) στον server (sink). [28] Για τους σκοπούς της πειραματικής αξιολόγησης, τα δεδομένα των αισθητήρων στέλνονται κάθε ένα δευτερόλεπτο. Επίσης, τα δεδομένα που στέλνουν όλοι οι αισθητήρες είναι η συμβολοσειρά “Hello from me” και το συνολικό μέγεθος του πακέτου των δεδομένων είναι 48 bytes.

Ο χρόνος που προσομοιώθηκαν όλα τα σενάρια που υλοποιήθηκαν είναι δέκα λεπτά.

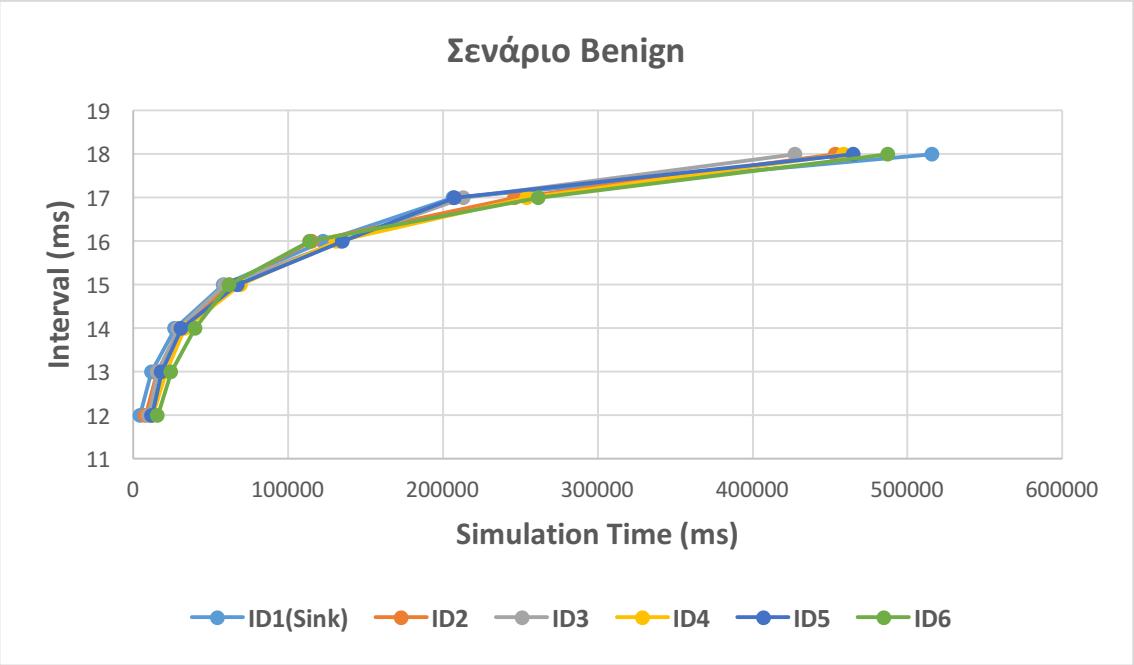
6.2 Flooding

6.2.1 Σενάριο 1 – Benign



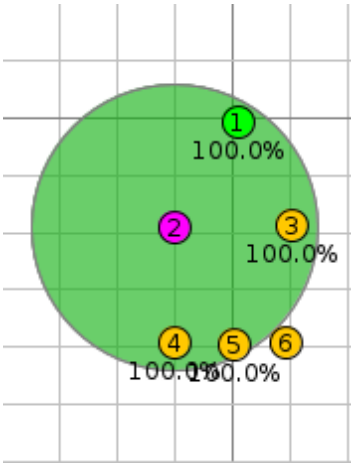
Στην πιο πάνω τοπολογία ο κόμβος 1 είναι ο sink και οι υπόλοιποι κόμβοι είναι benign. Στο τέλος της προσομοίωσης καταγράφηκαν οι συνολικοί αριθμοί μηνυμάτων τύπου DODAG Information Object (DIO) που έστειλε ο κάθε κόμβος και ο συνολικός αριθμός DIOs που αποστάλθηκαν στο δίκτυο, όπως φαίνεται πιο κάτω. Επίσης, καταγράφηκε ο χρόνος που σταθεροποιήθηκε το δίκτυο.

Node ID	DIOs Sent
1 (Sink)	7
2	7
3	7
4	7
5	7
6	7
Total DIOs	42
Stable Time	16210 ms



Η πιο πάνω γραφική παράσταση παρουσιάζει τον χρόνο προσομοίωσης σε σχέση με το interval που είχε ο κάθε κόμβος για το DIO timer του. Οι τιμές στον άξονα των ψ αναπαριστούν τον εκθέτη για τον υπολογισμό του interval με βάση το δύο. Παρατηρείται ότι τα interval όλων των κόμβων είχαν την ίδια ανοδική πορεία αρχίζοντας από 2^{12} milliseconds και φτάνοντας μέχρι 2^{18} milliseconds.

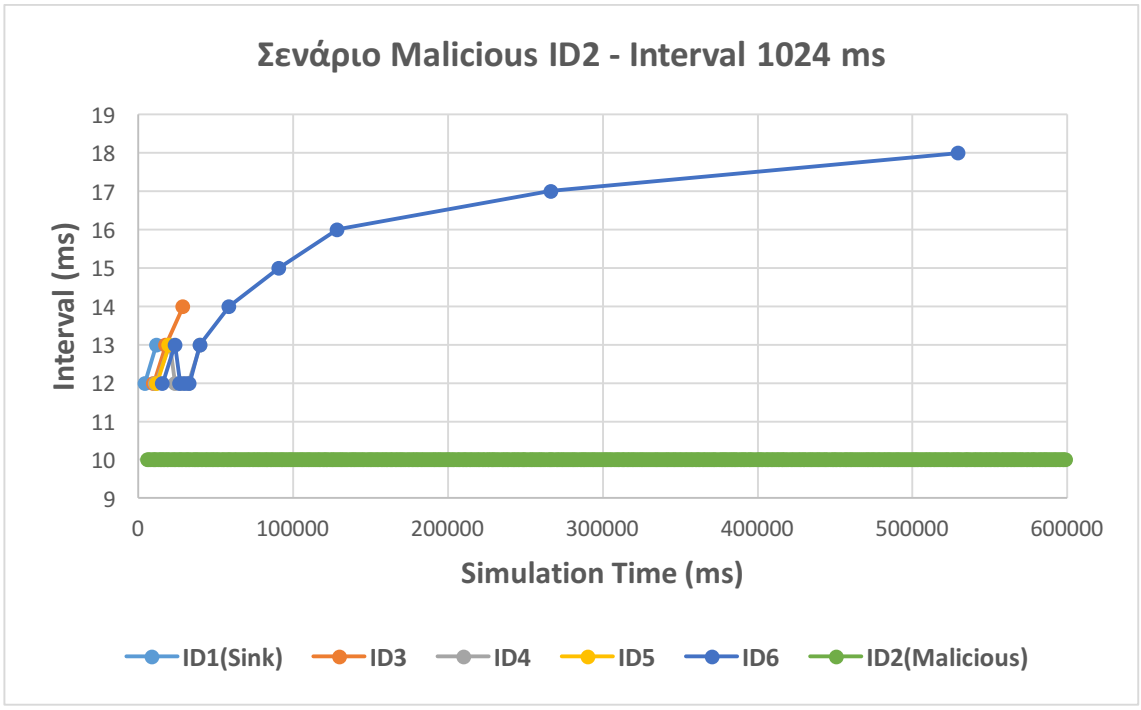
6.2.2 Σενάριο 2 – Malicious ID2

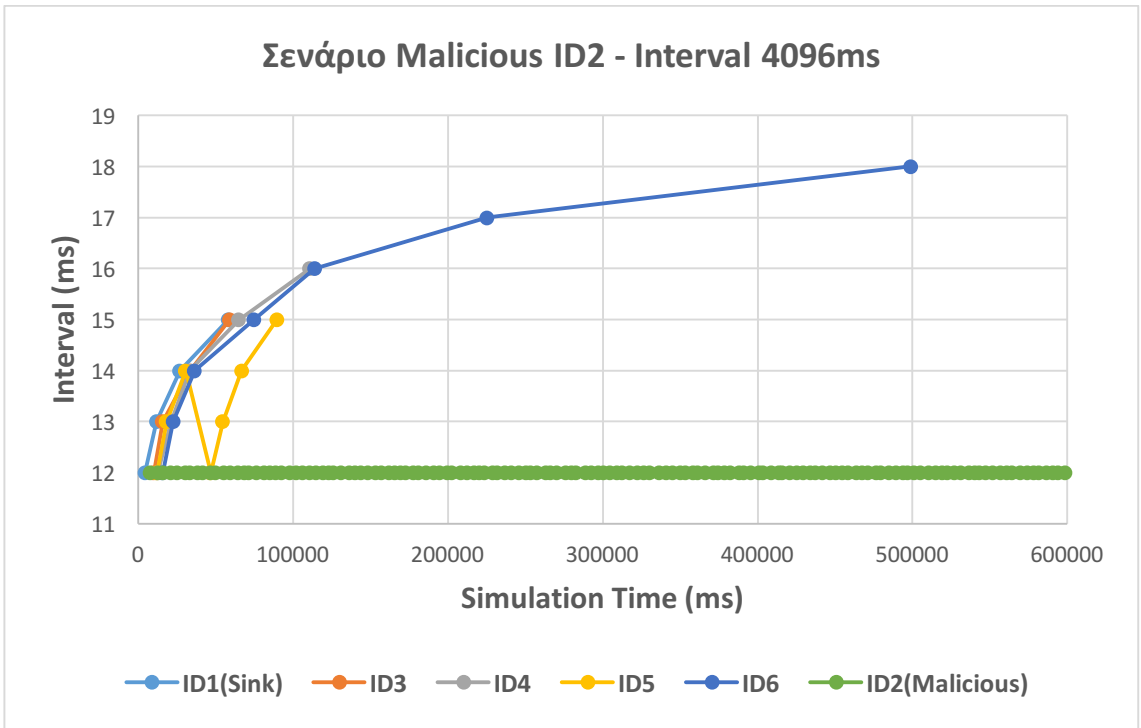


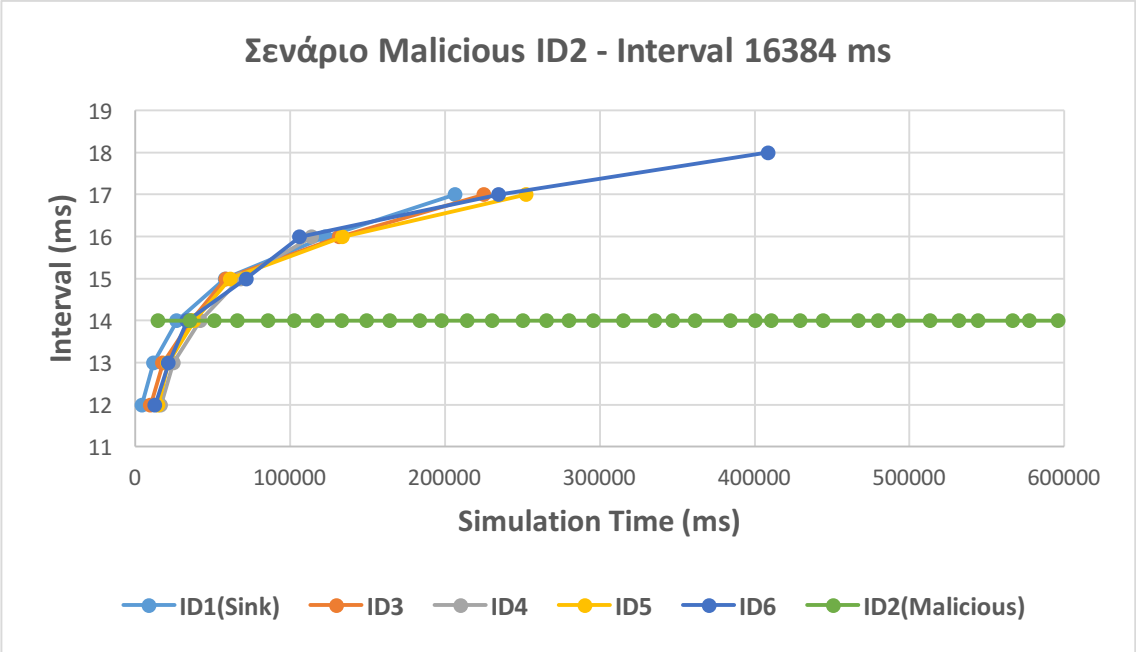
Στο σενάριο αυτό ο κόμβος 2 είναι κακόβουλος υλοποιώντας την επίθεση πλημμύρας (flooding). Έγιναν προσομοιώσεις αλλάζοντας τις τιμές του interval με το οποίο θα στέλνει μηνύματα DIO ο κόμβος 2. Τα αποτελέσματα φαίνονται πιο κάτω.

Interval	**2^{10}=1024ms**	**2^{12}=4096ms**	**2^{14}=16384ms**
Node ID	**DIOs Sent**	**DIOs Sent**	**DIOs Sent**
1 (Sink)	2	4	6
2 (Malicious)	509	140	36
3	3	4	6
4	6	5	5
5	2	7	6
6	11	7	7
Total DIOs	533	167	66
Stable Time	15859 ms	16210 ms	16722 ms

Ακολουθούν γραφικές παραστάσεις του χρόνου προσομοίωσης σε σχέση με το interval που είχε το timer κάθε κόμβου. Παρατηρείται ότι το interval του κακόβουλου κόμβου παραμένει πάντα σταθερό. Ακόμα, μπορούμε να δούμε ότι όσο πιο μεγάλο interval έχει ο κακόβουλος κόμβος, τόσο περισσότερα μηνύματα DIO καταφέρνουν να στείλουν οι benign κόμβοι.


Σενάριο Malicious ID2 - Interval 1024 ms
Interval (ms)
19
18
17
16
15
14
13
12
11
10
9
0
100000
200000
300000
400000
500000
600000
Simulation Time (ms)
ID1(Sink)
ID3
ID4
ID5
ID6
ID2(Malicious)


Σενάριο Malicious ID2 - Interval 4096ms
Interval (ms)
19
18
17
16
15
14
13
12
11
0
100000
200000
300000
400000
500000
600000
Simulation Time (ms)
ID1(Sink)
ID3
ID4
ID5
ID6
ID2(Malicious)



6.2.3 Σχολιασμός Αποτελεσμάτων

Παρατηρείται μεγάλη αύξηση στον αριθμό των DIOs που αποστάλθηκαν στο δίκτυο και τα περισσότερα προήλθαν από τον κόμβο 2 ο οποίος είναι κακόβουλος. Επίσης, φαίνεται μείωση στα DIO που έστειλαν οι benign κόμβοι. Αυτό συμβαίνει διότι ο κόμβος 2 πλημμύρισε την σύνδεση (link) με πακέτα και όταν προσπάθησαν άλλοι κόμβοι να στείλουν, δημιουργήθηκαν συγκρούσεις πακέτων (collisions). Επιπρόσθετα, χρησιμοποιείται το πρωτόκολλο Carrier Sense Multiple Access (CSMA) για έλεγχο πρόσβασης στο μέσο (Medium Access Control – MAC). Το CSMA διαισθάνεται το μέσο (medium) όταν θέλει ένας κόμβος να στείλει κάτι και αν αυτό δεν είναι διαθέσιμο (κάποιος άλλος στέλνει πακέτα) τότε θα περιμένει για ένα τυχαίο χρονικό διάστημα και θα προσπαθήσει ξανά. Ο κόμβος 2 στέλνοντας συνεχώς πακέτα απασχολεί το μέσο και ουσιαστικά το CSMA δεν επιτρέπει στους υπόλοιπους κόμβους να στείλουν αφού αυτό είναι απασχολημένο.

Επιπρόσθετα, όπως φαίνεται στις γραφικές παραστάσεις σε ορισμένους κόμβους γίνεται reset το timer τους. Αυτό συμβαίνει λόγω των μηνυμάτων DODAG Information Solicitation (DIS) που στέλνονται στο δίκτυο και λόγω ορισμένων parent switches που προκαλούνται από τα πολλά μηνύματα DIO που κινούνται στο δίκτυο.

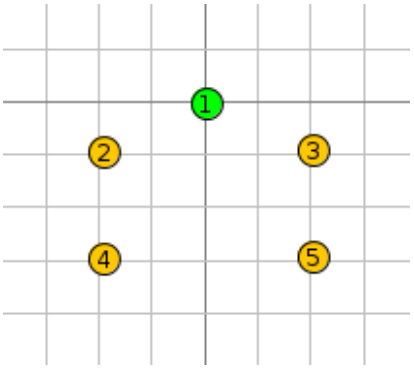
Από το πιο πάνω σενάριο φαίνεται ότι το πρωτόκολλο RPL δεν έλαβε κανένα μέτρο για να επαναφέρει ή να προστατέψει το δίκτυο από την επίθεση flooding. Η επίθεση αυτή

εισάγει επιπλέον αχρείαστα πακέτα στο δίκτυο και μπορεί να προκαλέσει συμφόρηση και συγκρούσεις πακέτων στο δίκτυο.

Τα μηνύματα DIO λαμβάνονται από όλους τους αισθητήρες που βρίσκονται στην εμβέλεια του αποστολέα. Επομένως, όσο περισσότεροι αισθητήρες υπάρχουν στην εμβέλειά του κακόβουλου αισθητήρα, τόσο περισσότερο αντίκτυπο μπορεί να έχει η επίθεση flooding στο δίκτυο.

6.3 Selective Forwarding

6.3.1 Σενάριο 1 – Benign



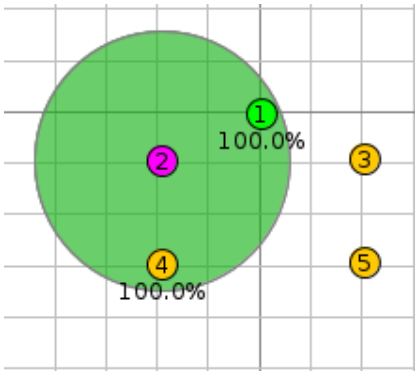
Στην πιο πάνω τοπολογία όλοι οι κόμβοι είναι benign. Ο κόμβος 1 είναι ο sink και στην εμβέλειά του βρίσκονται οι κόμβοι 2 και 3. Στην εμβέλεια του 2 και του 3 βρίσκονται οι κόμβοι 4 και 5 αντίστοιχα.

Στον πιο κάτω πίνακα φαίνεται ο αριθμός των πακέτων δεδομένων που προώθησε και που έστειλε ο κάθε κόμβος όπως επίσης και ο αριθμός των πακέτων που έλαβε ο sink. Ο αριθμός των πακέτων που προωθήθηκαν (forwarded) αντιπροσωπεύει όσα πακέτα φτάνουν στον αισθητήρα από άλλους αισθητήρες και πρέπει να προωθηθούν στον sink. Στον αριθμό των πακέτων που στάλθηκαν (sent) συμπεριλαμβάνεται ο αριθμός των πακέτων που προωθήθηκαν και ο αριθμός των πακέτων δεδομένων του συγκεκριμένου κόμβου.

Οι κόμβοι 4 και 5 δεν προωθούν πακέτα αφού δεν αποτελούν γονείς για κανένα κόμβο.

Node ID	**F/W**	**Sent**
1 (Sink)	-	-
2	590	1187
3	590	1187
4	0	597
5	0	597
Sink Received	2364	

6.3.2 Σενάριο 2 – Malicious ID2

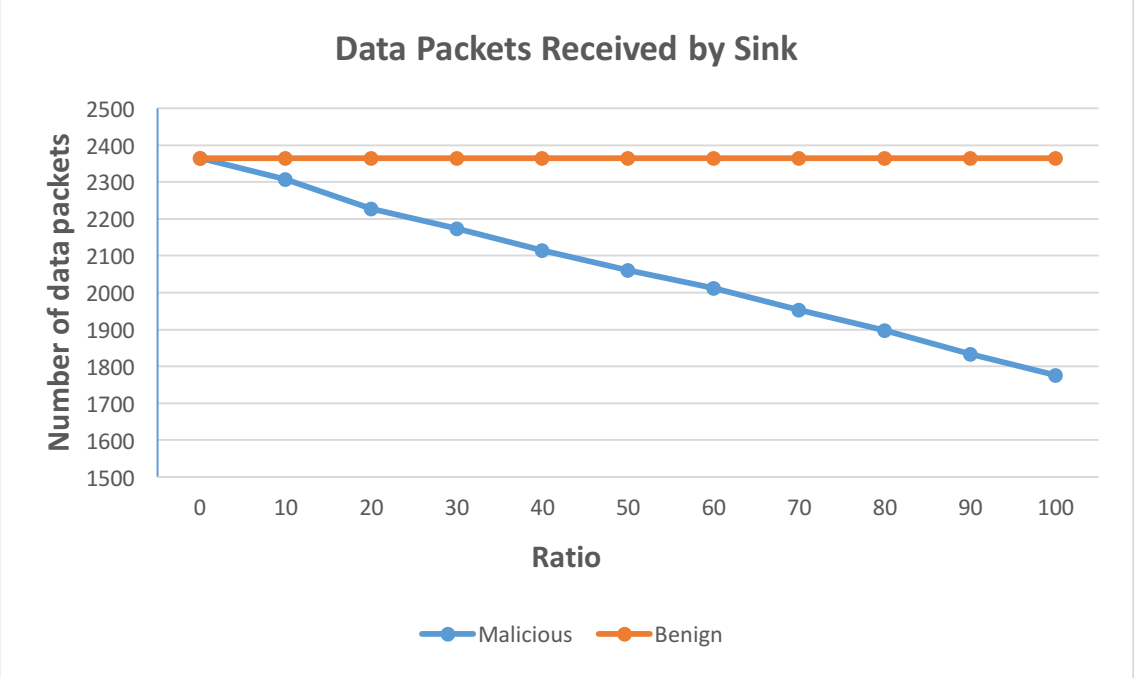


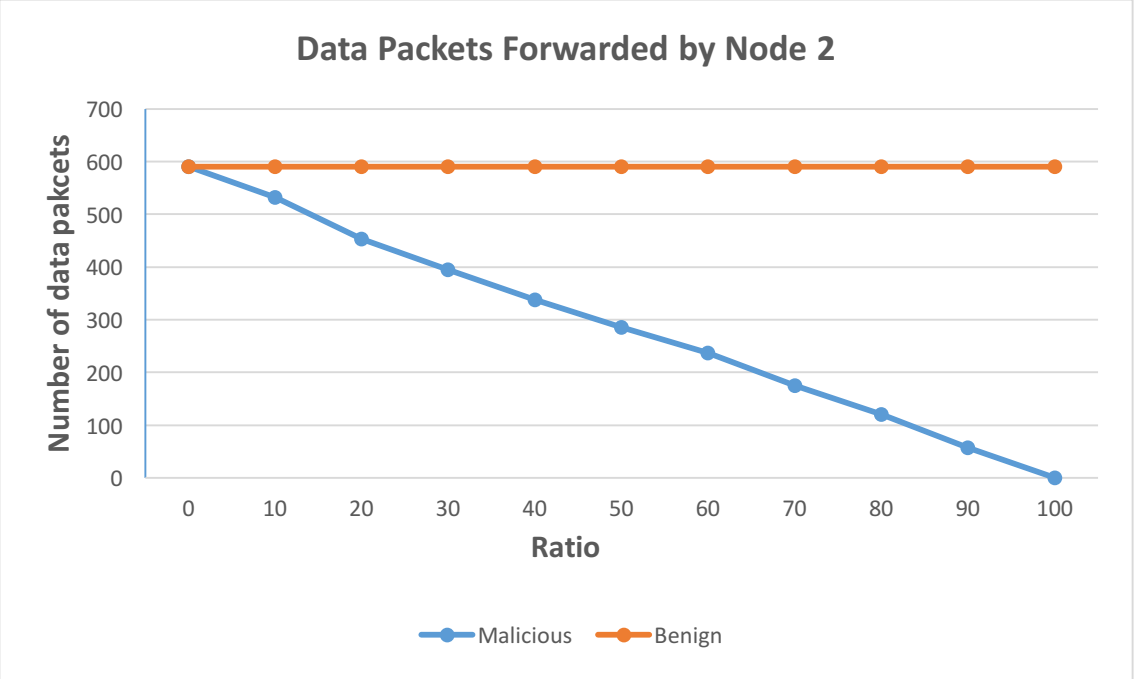
Στο σενάριο αυτό ο κόμβος 2 υλοποιεί την επίθεση της επιλεκτικής προώθησης (selective forwarding). Ο κακόβουλος κόμβος 2 θα κάνει drop τα πακέτα που λαμβάνει για προώθηση, με βάση ένα ακέραιο ratio που ορίστηκε. Έγιναν προσομοιώσεις για τιμές του ratio από δέκα μέχρι εκατό, αυξάνοντας δέκα κάθε φορά. Στον πιο κάτω πίνακα παρουσιάζονται τα αποτελέσματα όλων των προσομοιώσεων.

Στον πίνακα φαίνονται τα πακέτα που προωθήθηκαν και που στάλθηκαν από τον κάθε κόμβο. Παρατηρείται ότι όσο αυξάνεται η τιμή του ratio τα πακέτα που προωθούνται από τον κακόβουλο κόμβο 2 μειώνονται. Επίσης, μειώνεται και ο συνολικός αριθμός πακέτων δεδομένων που λαμβάνει ο sink. Στο σενάριο που τέθηκε η τιμή του ratio ίση με εκατό, δεν προωθήθηκε κανένα από τα πακέτα του κόμβου 4.

	Ratio=10		**Ratio=20**		**Ratio=30**		**Ratio=40**		**Ratio=50**	
Node ID	**F/W**	**Sent**	**F/W**	**Sent**	**F/W**	**Sent**	**F/W**	**Sent**	**F/W**	**Sent**
1 (Sink)	-	-	-	-	-	-	-	-	-	-
2 (Malicious)	532	1130	453	1050	395	993	338	936	286	884
3	590	1188	590	1188	590	1188	590	1187	590	1187
4	0	597	0	596	0	597	0	597	0	597
5	0	597	0	596	0	597	0	598	0	598
Sink Received	2308		2228		2173		2115		2061	
	Ratio=60		**Ratio=70**		**Ratio=80**		**Ratio=90**		**Ratio=100**	
Node ID	**F/W**	**Sent**	**F/W**	**Sent**	**F/W**	**Sent**	**F/W**	**Sent**	**F/W**	**Sent**
1 (Sink)	-	-	-	-	-	-	-	-	-	-
2 (Malicious)	237	835	175	773	120	719	57	656	0	599
3	589	1187	590	1188	590	1187	590	1188	589	1187
4	0	596	0	597	0	597	0	597	0	597
5	0	597	0	597	0	598	0	598	0	597
Sink Received	2012		1954		1898		1833		1776	

Στις πιο κάτω γραφικές παραστάσεις φαίνεται ο αριθμός των πακέτων που έλαβε ο sink και τα πακέτα που προώθησε ο κόμβος δύο σε σχέση με το κάθε ratio που ορίστηκε, για τα σενάρια Benign και Malicious ID2.





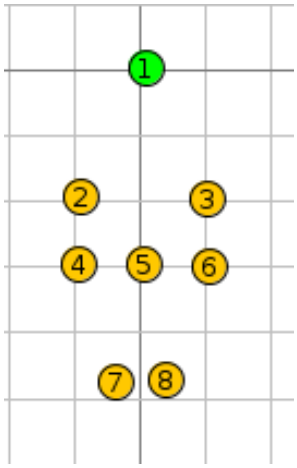
6.3.3 Σχολιασμός Αποτελεσμάτων

Με βάση το σενάριο 2 μπορούμε να δούμε ότι η προώθηση των πακέτων από τον κακόβουλο κόμβο γίνεται ανάλογα με το ratio που έχει οριστεί. Συγκρίνοντας το σενάριο benign με το σενάριο malicious, παρατηρείται ότι ακόμα και για μικρές τιμές του ratio υπάρχει απώλεια αρκετών πακέτων. Επίσης, φαίνεται ότι το πρωτόκολλο RPL δεν κατάφερε να προστατέψει το δίκτυο από την επίθεση τύπου selective forwarding, ούτε έλαβε μέτρα για τον μετριασμό της. Η επίθεση αυτή μπορεί να προκαλέσει ζημιά στο δίκτυο αφού ορισμένα ή ακόμα και όλα τα πακέτα των αισθητήρων που θα φτάσουν στον κακόβουλο θα χαθούν και δεν θα φτάσουν στον sink.

Η επίδραση της επίθεσης επιλεκτικής προώθησης μπορεί να μεγιστοποιηθεί όταν ο κακόβουλος κόμβος έχει στην εμβέλεια του πολλούς κόμβους – παιδιά του. Οι κόμβοι αυτοί θα στέλνουν τα πακέτα τους στον κακόβουλο για να προωθηθούν στον sink. Όμως, ο κακόβουλος κόμβος υπάρχει περίπτωση να μην τα προωθήσει και να χαθεί μεγάλος αριθμός πακέτων.

6.4 Black Hole

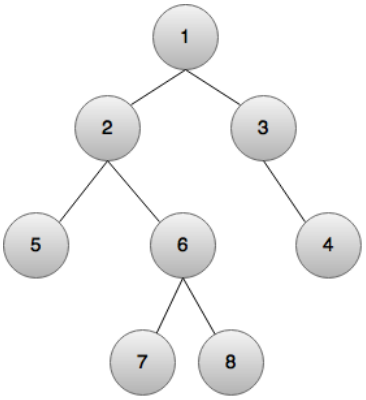
6.4.1 Σενάριο 1 – Benign



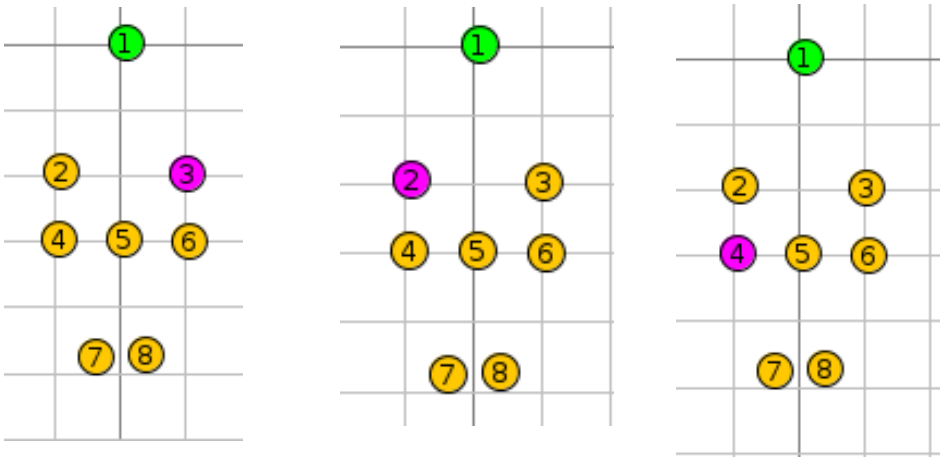
Στην πιο πάνω τοπολογία ο κόμβος 1 είναι ο sink και οι υπόλοιποι κόμβοι είναι benign. Ο sink έχει στην εμβέλειά του τους κόμβους 2 και 3. Οι κόμβοι 2,3,4,5 και 6 είναι όλοι γείτονες μεταξύ τους. Επίσης, οι κόμβοι 7 και 8 έχουν στην εμβέλειά τούς κόμβους 4, 5 και 6.

Ο πιο κάτω πίνακας παρουσιάζει τους γονείς (parents) που επέλεξε ο κάθε κόμβος και την τιμή ETX που διαφημίζει. Στο σχήμα φαίνεται το δέντρο που δημιουργείται με την επιλογή των γονέων για κάθε κόμβο.

Node ID	Preferred Parent	Advertised ETX
1 (Sink)	-	0
2	1	1
3	1	1
4	3	2
5	2	2
6	2	2
7	6	3
8	6	3



6.4.2 Σενάριο 2 – Malicious



Για το σενάριο αυτό έγιναν προσομοιώσεις με έναν κακόβουλο κόμβο που υλοποιεί την επίθεση black hole. Έγιναν τρεις διαφορετικές προσομοιώσεις με τον κακόβουλο να είναι ο κόμβος 2, ο κόμβος 3 και ο κόμβος 4. Στον πιο κάτω πίνακα παρουσιάζονται για την κάθε προσομοίωση οι γονείς (parents) που έχει επιλέξει ο κάθε κόμβος και η τιμή ETX που διαφημίζει.

Για την υλοποίηση της επίθεσης black hole ο κόμβος 3 διαφημίζει μέσω των DIO μηνυμάτων ότι ο αναμενόμενος αριθμός μεταδόσεων του (estimated number of transmissions – ETX) είναι ίσος με 1. Παρατηρείται ότι ο κόμβος 4 τώρα επέλεξε ως γονέα του τον κακόβουλο κόμβο 3 αντί τον 2 όπως στο benign σενάριο, αφού διαφημίζει πιο ελκυστικό μετρικό.

Malicious ID3			**Malicious ID2**			**Malicious ID4**		
Node ID	**Parent**	**ETX**	**Node ID**	**Parent**	**ETX**	**Node ID**	**Parent**	**ETX**
1 (Sink)	-	0	**1 (Sink)**	-	0	**1 (Sink)**	-	0
2	1	1	**2(Mal.)**	1	1	**2**	1	1
3(Mal.)	1	1	**3**	1	1	**3**	1	1
4	2	2	**4**	2	2	**4(Mal.)**	2	1
5	2	2	**5**	2	2	**5**	5	2
6	3	2	**6**	3	2	**6**	3	2
7	6	3	**7**	6	3	**7**	6	3
8	6	3	**8**	6	3	**8**	4	2

6.4.3 Σχολιασμός Αποτελεσμάτων

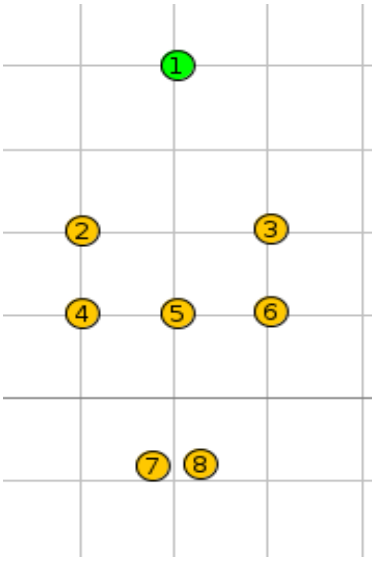
Στην περίπτωση που ο κακόβουλος κόμβος ήταν ο 3, παρατηρείται ότι κατάφερε να προσελκύσει τον κόμβο 6 να τον θέσει ως γονέα του, ενώ στο benign σενάριο είχε ως γονέα τον κόμβο 2. Όμοιο φαινόμενο παρατηρείται και με τους κόμβους 4 και 8 στις προσομοιώσεις με κακόβουλο τον 2 και τον 4 αντίστοιχα.

Κατά την προσομοίωση που έγινε με κακόβουλο τον κόμβο 4, φαίνεται επίσης ότι ο κόμβος 8, ο οποίος επέλεξε ως γονέα του τον κακόβουλο, διαφημίζει τιμή ETX μικρότερη σε σύγκριση με το benign σενάριο. Αυτό συμβαίνει διότι ο υπολογισμός του ETX ενός κόμβου, γίνεται με βάση την τιμή ETX του γονέα του. Επομένως, όσοι κόμβοι έχουν σαν γονέα τον κακόβουλο που διαφημίζει λανθασμένο ETX και αυτοί με την σειρά τους θα κάνουν το ίδιο.

Με βάση τις πιο πάνω προσομοιώσεις, προκύπτει ότι το πρωτόκολλο RPL δεν αντιλαμβάνεται την εσφαλμένη διαφήμιση ελκυστικού μετρικού που μπορεί να κάνει ένας κακόβουλος κόμβος. Με την επίθεση black hole ένας εισβολέας στο δίκτυο μπορεί να προσελκύσει πακέτα δεδομένων και ακολούθως έχει την ευκαιρία να τα τροποποιήσει (alter) ή να τα κάνει drop. Επίσης, η επίθεση μπορεί να εξαπλωθεί αφού και οι κόμβοι – παιδιά του κακόβουλου θα διαφημίσουν και αυτοί πιο ελκυστικό μετρικό. Η συγκεκριμένη επίθεση θα έχει την μεγαλύτερη επίδραση στο δίκτυο όταν ο κακόβουλος κόμβος έχει όσο το δυνατόν περισσότερους κόμβους – παιδιά του.

6.5 Sinkhole

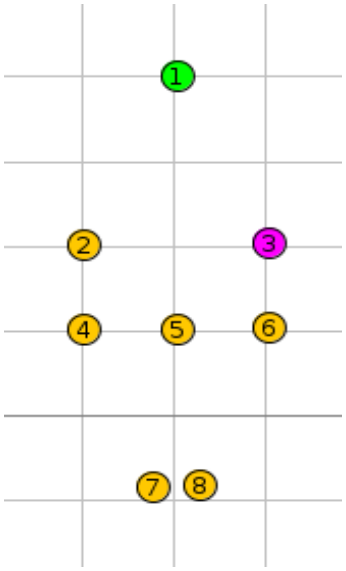
6.5.1 Σενάριο 1 – Benign



Στην πιο πάνω τοπολογία ο κόμβος 1 είναι ο sink και όλοι οι κόμβοι είναι benign. Η τοπολογία είναι χωρισμένη σε τρία επίπεδα με τους κόμβους 2 και 3 να βρίσκονται στην εμβέλεια του sink. Στον πιο κάτω πίνακα φαίνονται οι γονείς (parents) που επέλεξε ο κάθε κόμβος, η τιμή ETX που διαφημίζει και ο αριθμός των πακέτων που παρέλαβε ο sink. Το σενάριο προσομοιώθηκε τρεις φορές αλλάζοντας κάθε φορά το random seed στον προσομοιωτή.

Node ID	Preferred Parent	Advertised ETX	Preferred Parent	Advertised ETX	Preferred Parent	Advertised ETX
1 (Sink)	-	0	-	0	-	0
2	1	1	1	1	1	1
3	1	1	1	1	1	1
4	2	2	3	2	2	2
5	2	2	2	2	3	2
6	3	2	2	2	3	2
7	6	3	4	3	4	3
8	6	3	4	3	4	3
Sink Received	3907		3909		3877	

6.5.2 Σενάριο 2 – Malicious ID3

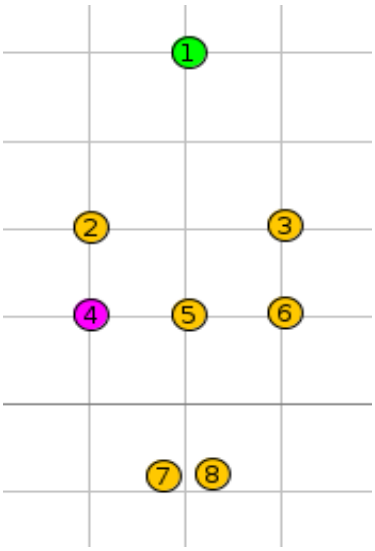


Στο παρόν σενάριο ο κόμβος 3 είναι κακόβουλος υλοποιώντας επίθεση τύπου sinkhole. Ο κόμβος 3 για την υλοποίηση της επίθεσης διαφημίζει μέσω των DIO μηνυμάτων ότι έχει ETX ίσο με μηδέν και rank ίσο με 1. Δηλαδή, διαφημίζει ότι έχει το ίδιο ETX και rank με τον sink. Στον πιο κάτω πίνακα φαίνονται οι γονείς (parents) που επέλεξε ο κάθε κόμβος, η τιμή ETX που διαφημίζει, ο αριθμός των πακέτων που έλαβε ο sink και ο αριθμός των πακέτων που έλαβε ο κακόβουλος κόμβος. Το σενάριο προσομοιώθηκε τρεις φορές αλλάζοντας κάθε φορά το random seed στον προσομοιωτή.

Παρατηρείται ότι ο κακόβουλος κόμβος 3 κατάφερε πάντα να προσελκύσει τους κόμβους 4,5 και 6 να το ορίσουν ως γονέα τους. Επίσης, η τιμή ETX που διαφημίζουν οι συγκεκριμένοι κόμβοι μειώνεται σε σχέση με το benign σενάριο.

Node ID	**Parent**	**ETX**	**Parent**	**ETX**	**Parent**	**ETX**
1 (Sink)	-	0	-	0	-	0
2	1	1	1	1	1	1
3(Mal.)	1	0	1	0	1	0
4	3	1	3	1	3	1
5	3	1	3	1	3	1
6	3	1	3	1	3	1
7	4	2	6	2	5	2
8	4	2	6	2	5	2
Sink Received	595		594		594	
Malicious Received	2890		2787		2889	

6.5.3 Σενάριο 3 – Malicious ID4

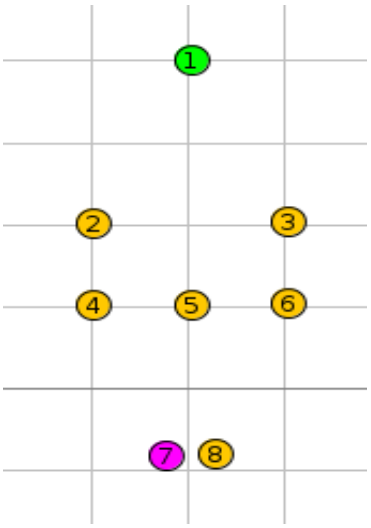


Για το σενάριο αυτό ο κόμβος 4 είναι κακόβουλος υλοποιώντας την επίθεση sinkhole. Στον πιο κάτω πίνακα φαίνονται οι γονείς (parents) που επέλεξε ο κάθε κόμβος, η τιμή ETX που διαφημίζει, ο αριθμός των πακέτων που έλαβε ο sink και ο αριθμός των πακέτων που έλαβε ο κακόβουλος.

Παρατηρείται ότι ο κακόβουλος κόμβος στην πρώτη και τρίτη περίπτωση, καταφέρνει να προσελκύσει του κόμβους 7 και 8. Στην δεύτερη περίπτωση οι κόμβοι 5 και 6 επέλεξαν τον κακόβουλο ως γονέα τους. Επίσης, η τιμή ETX που διαφημίζουν οι κόμβοι – παιδιά του κακόβουλου είναι μικρότερη σε σχέση με το benign σενάριο.

Node ID	**Parent**	**ETX**	**Parent**	**ETX**	**Parent**	**ETX**
1 (Sink)	-	0	-	0	-	0
2	1	1	1	1	1	1
3	1	1	1	1	1	1
4(Mal.)	2	0	2	0	3	0
5	2	2	4	1	3	2
6	2	2	4	1	3	2
7	4	1	6	2	4	1
8	4	1	6	2	4	1
Sink Received	2361		1245		2361	
Malicious Received	1176		2252		1170	

6.5.4 Σενάριο 4 – Malicious ID7



Στο συγκεκριμένο σενάριο ο κόμβος 7 είναι κακόβουλος υλοποιώντας την επίθεση sinkhole. Στον πιο κάτω πίνακα φαίνονται οι γονείς (parents) που επέλεξε ο κάθε κόμβος, η τιμή ETX που διαφημίζει, ο αριθμός των πακέτων που έλαβε ο sink και ο αριθμός των πακέτων που έλαβε ο κακόβουλος.

Εδώ φαίνεται ότι ο κακόβουλος κόμβος υπάρχει περίπτωση να προσελκύσει ακόμα και κόμβους που βρίσκονται σε ανώτερο επίπεδο από αυτόν. Στην πρώτη περίπτωση ο κόμβος 5 και στην τρίτη περίπτωση οι κόμβοι 4 και 6 επέλεξαν τον κακόβουλο ως γονέα τους.

Node ID	**Parent**	**ETX**	**Parent**	**ETX**	**Parent**	**ETX**
1 (Sink)	-	0	-	0	-	0
2	1	1	1	1	1	1
3	1	1	1	1	1	1
4	2	2	2	2	7	1
5	7	1	2	2	3	2
6	2	2	2	2	7	1
7(Mal.)	6	0	4	0	4	0
8	6	3	4	3	4	2
Sink Received	2977		3147		2434	
Malicious Received	317		0		832	

6.5.5 Σχολιασμός Αποτελεσμάτων

Από το σενάριο 2 προκύπτει ότι αν ο κακόβουλος κόμβος βρίσκεται στην εμβέλεια του sink μπορεί εύκολα να ξεγελάσει του κόμβους στο πιο κάτω επίπεδο ότι είναι ο sink. Επιπρόσθετα, στο Σενάριο 2 ο κακόβουλος κατάφερε να προσελκύσει τον μεγαλύτερο αριθμό πακέτων δεδομένων.

Παρατηρώντας τα σενάρια 3 και 4 μπορούμε να δούμε ότι με την επίθεση sinkhole είναι εφικτό να προσελκύσουμε κόμβους που βρίσκονται στο ίδιο επίπεδο με τον κακόβουλο ή ακόμα και από ανώτερο επίπεδο. Επίσης, στο σενάριο 4 μπορούμε να δούμε ότι η επίθεση sinkhole υπάρχει περίπτωση να μην πετύχει. Αυτό συμβαίνει διότι ο κακόβουλος κόμβος θα διαφημίσει ότι είναι ο sink μετά την εισαγωγή του στον γράφο. Επομένως, όταν ο κακόβουλος κόμβος τοποθετηθεί χαμηλά στην τοπολογία, θα καθυστερήσει να διαφημίσει ότι είναι ο sink με αποτέλεσμα οι γείτονες του να υπάρχει πιθανότητα να έχουν ήδη επιλέξει κάποιον άλλο κόμβο ως γονέα τους.

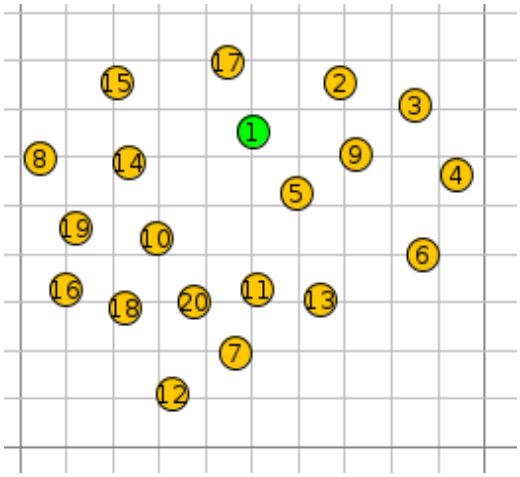
Ακόμα, οι κόμβοι που επηρεάζονται από την επίθεση διαφημίζουν λανθασμένο ETX αφού ο υπολογισμός του γίνεται με βάση το ETX του γονέα. Έτσι, ακόμα και οι κόμβοι – παιδιά του κακόβουλου μπορούν να προσελκύσουν άλλους κόμβους.

Κατά την διάρκεια των προσομοιώσεων του Σεναρίου 4 παρατηρήθηκε ότι σε ορισμένους κόμβους ενεργοποιήθηκε ο μηχανισμός loop detection του RPL, κατά την αποστολή των μηνυμάτων DAO. Οι κόμβοι αυτοί ακολούθως αφαιρούσαν τον κακόβουλο κόμβο από γονέα τους και όριζαν ως γονέα τους έναν από τους κόμβους που είχαν ως υποψήφιους γονείς (candidate parents). Όμως, με την άφιξη του επόμενου DIO μηνύματος από τον κακόβουλο, ο κόμβος όριζε ξανά ως γονέα του τον κακόβουλο. Επομένως, παρ' όλο που το πρωτόκολλο RPL έχει υλοποιημένο τον μηχανισμό για εντοπισμό κύκλων (loop detection), αυτός δεν ήταν αποτελεσματικός για την αντιμετώπιση της επίθεσης sinkhole.

Η επίθεση sinkhole είναι αρκετά ισχυρή και αν ο κακόβουλος κόμβος τοποθετηθεί κοντά στον sink τότε η επίθεση θα έχει την μεγαλύτερη επίδραση στο δίκτυο. Όπως φαίνεται και στο Σενάριο 3 η επίθεση αυτή έχει την λιγότερη επίδραση όταν ο κακόβουλος είναι χαμηλά στην τοπολογία.

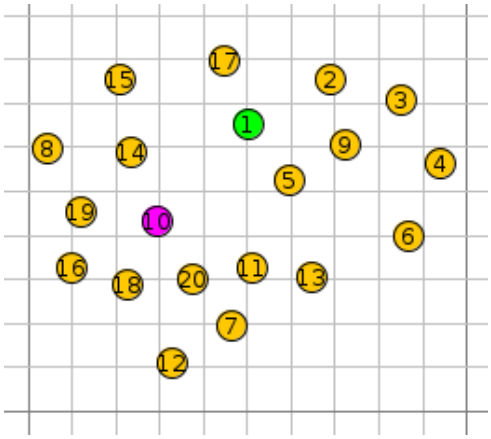
6.6 Συνδυασμός Black Hole και Selective Forwarding

6.6.1 Σενάριο 1 – Benign



Η πιο πάνω τοπολογία αποτελείται από είκοσι κόμβους. Οι θέσεις των κόμβων, καθορίστηκαν τυχαία με την βοήθεια του εργαλείου Cooja. Ο κόμβος 1 είναι ο sink και όλοι οι κόμβοι είναι benign. Στο τέλος της προσομοίωσης, ο αριθμός των πακέτων που παραλήφθηκαν από τον sink ήταν 8233.

6.6.2 Σενάριο 2 – Malicious ID10



Στο σενάριο αυτό η τοπολογία παραμένει η ίδια αλλά ο κόμβος 10 είναι κακόβουλος υλοποιώντας τις επιθέσεις black hole και selective forwarding. Για την επίθεση black hole ο κακόβουλος διαφημίζει ότι έχει ETX ίσο με ένα και για την επίθεση selective forwarding ορίστηκε ratio ίσο με πενήντα.

Το σενάριο προσομοιώθηκε δέκα φορές αλλάζοντας κάθε φορά το random seed στον προσομοιωτή. Στον πιο κάτω πίνακα παρουσιάζεται ο αριθμός των πακέτων που παρέλαβε ο sink και τα πακέτα που χάθηκαν σε σύγκριση με το benign σενάριο.

	Run 1	**Run 2**	**Run 3**	**Run 4**	**Run 5**
Sink Received	7671	7956	7877	7225	7650
Packets Lost	562	277	356	1008	583
	Run 6	**Run 7**	**Run 8**	**Run 9**	**Run 10**
Sink Received	6947	7779	6856	6676	7480
Packets Lost	1286	454	1377	1557	753
Average Packets Received: 7411					
Average Packets Lost: 821					

6.6.3 Σχολιασμός Αποτελεσμάτων

Παρατηρείται ότι στις διάφορες περιπτώσεις που εξετάστηκαν ανάλογα με το random seed, ο αριθμός των πακέτων που χάθηκαν και δεν παρέλαβε ο sink ήταν αρκετά μεγάλος. Κατά μέσο όρο στις δέκα προσομοιώσεις που έγιναν, παραλήφθηκαν από τον sink 7411 πακέτα και χάθηκαν 821 πακέτα. Τα αποτελέσματα ήταν αναμενόμενα αφού ο κακόβουλος κόμβος προσπαθεί να προσελκύσει άλλους κόμβους για να του προωθήσουν τα πακέτα τους. Επίσης, ο κακόβουλος κόμβος προωθεί επιλεκτικά όσα πακέτα λαμβάνει με πιθανότητα 50%.

Μέσα από τις προσομοιώσεις που έγιναν φαίνεται ότι ο συνδυασμός των επιθέσεων black hole και selective forwarding μπορεί να έχει μεγάλο αντίκτυπο όσον αφορά την παράδοση πακέτων στον sink.

Κεφάλαιο 7

Συμπεράσματα – Μελλοντική Εργασία

7.1 Γενικά Συμπεράσματα

Με βάση τις προσομοιώσεις που έγιναν για τις επιθέσεις που υλοποιήθηκαν στο πρωτόκολλο δρομολόγησης RPL, φαίνεται ότι η θέση που έχει ο κακόβουλος αισθητήρας στην τοπολογία του δικτύου, παίζει σημαντικό ρόλο στην επίδραση που θα έχει η επίθεση στο δίκτυο. Οι επιθέσεις αυτές μπορούν να προκαλέσουν αρκετή ζημιά σε ένα ασύρματο δίκτυο αισθητήρων, αν τοποθετηθεί ο κακόβουλος κόμβος σε στρατηγικό σημείο. Επίσης, υπάρχουν επιθέσεις που οι συνέπειες τους εξαρτώνται και από τον αριθμό των γειτονικών κόμβων που έχει ο κακόβουλος αισθητήρας.

Επιπρόσθετα, με την παρακολούθηση και καταγραφή συγκεκριμένων παραμέτρων κατά την λειτουργία του δικτύου, μπορεί να εντοπιστεί κατά πόσο το δίκτυο δέχεται κάποιο είδος επίθεσης. Συγκεκριμένα, οι παράμετροι αυτοί μπορούν να περιλαμβάνουν: τον αριθμό των μηνυμάτων DIO που στέλνονται, πόσα resets έγιναν στο timer ενός κόμβου, τον αριθμό πακέτων που χάνονται στο δίκτυο, την ποσότητα συγκρούσεων (collisions) πακέτων καθώς επίσης το ETX που διαφημίζουν οι κόμβοι.

Αναλύοντας την συμπεριφορά του πρωτοκόλλου RPL όταν δέχεται συγκεκριμένου τύπου επιθέσεις, προέκυψε ότι δεν λαμβάνονται μέτρα ούτε για την πρόληψη, αλλά ούτε για την αντιμετώπιση των επιθέσεων. Με τις προσομοιώσεις διάφορων σεναρίων, επιβεβαιώθηκε ότι το RPL είναι ευάλωτο σε επιθέσεις τύπου flooding, selective forwarding, black hole και sinkhole. Το πρωτόκολλο δρομολόγησης RPL είναι εγκεκριμένο για χρήση σε ασύρματα δίκτυα αισθητήρων και χρησιμοποιείται ευρέως σε διάφορες εφαρμογές. Επομένως, είναι αναγκαία η ενσωμάτωση μηχανισμών οι οποίοι θα παρέχουν ασφάλεια στην επικοινωνία με την χρήση του RPL.

Για την επίτευξη του επιπέδου ασφάλειας που είναι αναγκαίο κατά την επικοινωνία σε δίκτυα που χρησιμοποιούν το RPL θα μπορούσε να χρησιμοποιηθεί κρυπτογράφηση συμμετρικού κλειδιού (symmetric key cryptography) και one-way hash function για ασύμμετρη κρυπτογράφηση. Επίσης, θα μπορούσαν να εφαρμόζονται Message Authentication Codes (MACs) κατά την αποστολή πακέτων έτσι ώστε να γίνεται αυθεντικοποίηση των αισθητήρων.

7.2 Μελλοντική Εργασία

Τα αποτελέσματα από την παρούσα διπλωματική εργασία μπορούν να προσαρμοστούν ανάλογα και να ενσωματωθούν σε ένα σύστημα εντοπισμού εισβολής (Intrusion Detection System - IDS). Σαν είσοδο στο IDS θα μπορούσαν να δοθούν οι παράμετροι που αναφέρονται στο 7.1. Με αυτόν τον τρόπο, θα μπορούν να εντοπιστούν οι συγκεκριμένες επιθέσεις από το σύστημα, σε ασύρματα δίκτυα αισθητήρων που χρησιμοποιούν το πρωτόκολλο RPL.
Επιπρόσθετα, ως μελλοντική εργασία θα μπορούσε να γίνει μελέτη της επίδρασης των επιθέσεων σε δίκτυα με αστάθειες, τα οποία αποτελούν πιο ρεαλιστικό σενάριο. Για παράδειγμα, μπορούν να γίνουν οι προσομοιώσεις των επιθέσεων και μελέτη της συμπεριφοράς του δικτύου σε τοπολογίες όπου θα υπάρξει βλάβη ενός ή περισσότερων αισθητήρων.

Βιβλιογραφία

[1] Wireless Sensor Network [Online]. Available: https://en.wikipedia.org/wiki/Wireless_sensor_network

[2] Akyildiz, Ian F., Weilian Su, et al. "Wireless sensor networks: a survey." *Computer networks* 38, no. 4 (2002): 393-422.

[3] Jain, Manoj Kumar. "Wireless sensor networks: Security issues and challenges." *International Journal of Computer and Information Technology* 2, no. 1 (2011): 62-67.

[4] Walters, John Paul, Zhengqiang Liang et al. "Wireless sensor network security: A survey." *Security in distributed, grid, mobile, and pervasive computing* 1 (2007): 367.

[5] Wang, Yong, Garhan Attebury, et al. "A survey of security issues in wireless sensor networks." (2006).

[6] Singh, Shio Kumar, M. P. Singh, et al. "Routing protocols in wireless sensor networks–A survey." *International Journal of Computer Science & Engineering Survey (IJCSES) Vol* 1 (2010): 63-83.

[7] Al-Karaki, Jamal N., and Ahmed E. Kamal. "Routing techniques in wireless sensor networks: a survey." Wireless communications, IEEE 11.6 (2004): 6-28.

[8] Chen, Benjie, et al. "Span: An Energy-Efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks."

[9] Akkaya, Kemal, and Mohamed Younis. "A survey on routing protocols for wireless sensor networks." Ad hoc networks 3.3 (2005): 325-349.

[10] Younis, Ossama, and Sonia Fahmy. "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks." Mobile Computing, IEEE Transactions on 3.4 (2004): 366-379.

[11] Luo, Jun, and Jean-Pierre Hubaux. "Joint mobility and routing for lifetime elongation in wireless sensor networks." INFOCOM 2005. 24th annual joint conference of the IEEE computer and communications societies. Proceedings IEEE. Vol. 3. IEEE, 2005.

[12] García Villalba, Luis Javier, et al. "Routing protocols in wireless sensor networks." Sensors 9.11 (2009): 8399-8421.

[13] Kim, T., et al. "Comparison of Security Protocols for Wireless Sensor Networks."

[14] Stavrou, Eliana, and Andreas Pitsillides. "A survey on secure multipath routing protocols in WSNs." Computer Networks 54.13 (2010): 2215-2238.

[15] Khan, Imran A., et al. "Application-based Classification and Comparison of Secure Routing Protocols in Wireless sensor Networks." SmartCR 5.3 (2015): 209-223.

[16] Zhu, Sencun, Sanjeev Setia, et al. "LEAP: efficient security mechanisms for large-scale distributed sensor networks-10th ACM Conference on Computer and Communications Security (CCS'03)." Washington DC, October (2003).

[17] Abu-Ghazaleh, Nael, Kyoung-Don Kang, et al. "Towards resilient geographic routing in WSNs." Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks. ACM, 2005.

[18] Sami, S., Eng Saad, and A. Al-Swailem. "PRSA: a path redundancy based security algorithm for wireless sensor networks." (2007).

[19] Vasseur, J., Navneet Agarwal, Jonathan Hui, Zach Shelby, Paul Bertrand, and Cedric Chauvenet. "RPL: The IP routing protocol designed for low power and lossy networks." Internet Protocol for Smart Objects (IPSO) Alliance 36 (2011).

[20] Winter, Tim. "RPL: IPv6 routing protocol for low-power and lossy networks." (2012).

[21] Tsvetkov, Tsvetko. "RPL: IPv6 Routing Protocol for Low Power and Lossy Networks." Sensor Nodes–Operation, Network and Application (SN) 59 (2011):2.

[22] Contiki: The Open Source OS [Online]. Available: http://www.contiki-os.org

[23] Contiki [Online]. Available: https://en.wikipedia.org/wiki/Contiki

[24] Pongle, Pavan, and Gurunath Chavan. "A survey: Attacks on RPL and 6LoWPAN in IoT." In Pervasive Computing (ICPC), 2015 International Conference on, pp. 1-6. IEEE, 2015.

[25] Ali, Hazrat. "A Performance Evaluation of RPL in Contiki." (2012).

[26] Chugh, Karishma, L. Aboubaker, and Jonathan Loo. "Case study of a black hole attack on LoWPAN-RPL." In Proc. of the Sixth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), Rome, Italy (August 2012), pp. 157-162. 2012.

[27] Wallgren, Linus, Shahid Raza, and Thiemo Voigt. "Routing Attacks and Countermeasures in the RPL-based Internet of Things." International Journal of Distributed Sensor Networks 2013 (2013).

[28] RPL UDP [Online]. Available: http://anrg.usc.edu/contiki/index.php/RPL_UDP