Πανεπιστημιο Πατρων
Πολυτεχνικη Σχολη
Τμημα Μηχανικων Η/Υ & Πληροφορικης

Διπλωματικη Εργασια

Κατανεμημένοι Αλγόριθμοι για Ασύρματα Αδόμητα Δίκτυα

Φοιτητής:
Κωνσταντίνος
Μπαϊρακταρης
ΑΜ:3167

Επιβλέπων Καθηγητής:
Χρήστος
Ζαρολιαγκης

Συν-επιβλέπων Καθηγητής:
Ιωάννης Χατζηγιαννακης

Πάτρα, 21 Απριλίου 2009

Πρόλογος

Το παρόν κείμενο αποτελεί το αποτέλεσμα της εκπόνησης της διπλωματικής εργασίας που ανέλαβα στην αρχή της ακαδημαϊκής χρονιάς 2007-08. Το θέμα της ήταν 'Κατανεμημένοι Αλγόριθμοι σε Αδόμητα Δίκτυα'. Κατά τη διάρκεια της ενασχόλησής μου με την εργασία, η μελέτη ειδικεύτηκε στα Ασύρματα Δίκτυα Αισθητήρων, ένα θέμα με πάρα πολύ ενδιαφέρον και με έρευνα που βρίσκεται ακόμα σε σχετικά εμβρυακό στάδιο, αλλά που αντιμετωπίζεται με ενθουσιασμό και πρωτοτυπία από τη διεθνή επιστημονική κοινότητα.

Έπειτα από μια αρχική μελέτη γύρω από τα Ασύρματα Δίκτυα Αισθητήρων πάνω σε υλικό που μου δόθηκε από τους επιβλέποντες καθηγητές, αρχίσαμε να καταπιανόμαστε με τον σχεδιασμό και ορισμό ενός καινούριου πρωτοκόλλου δρομολόγησης. Το πρωτόκολλο αυτό αρχικά εμπεριείχε το στοιχείο της πιθανοτικής επιλογής στη δρομολόγηση και την ύπαρξη κινητικότητας των συσκευών, ενώ αργότερα εισάχθηκε και το στοιχείο της ασφάλειας.

Στα πλαίσια της μελέτης σχεδιάστηκε ένα καινούριο πρωτόκολλο δρομολόγησης με υποστήριξη κρυπτογραφίας και ασφάλειας. Η συγκεκριμένη προσέγγιση επιστρατεύει ένα σύνολο από μηχανισμούς, κάποιοι από τους οποίους είναι δανεισμένοι από άλλες προσεγγίσεις ενώ κάποιοι είναι καινούριοι. Το αποτέλεσμα είναι ένα πρωτόκολλο το οποίο υποστηρίζει δρομολόγηση προς κάθε προορισμό εντός του δικύου, με βελτιωμένη απόδοση όταν ο προορισμός είναι η απόληξη (sink), πιθανοτικούς μηχανισμούς μείωσης και *δίκαιης* κατανομής κατανάλωσης ενέργειας, αντιμετώπιση κίνησης της απόληξης, αντιμετώπιση κίνησης των αισθητήρων, ασφάλεια και κρυπτογραφία σε όλη τη διάρκεια λειτουργίας του πρωτοκόλλου. Η δουλειά μας παρουσιάζεται στην εργασία [3].

Στα κεφάλαια 1 μέχρι 3 παρουσιάζονται όλα τα θέματα που χρειάζεται κάποιος σχετικά άπειρος με τα Ασύρματα Δίκτυα Αισθητήρων αναγνώστης για να είναι σε θέση να καταλάβει και να μελετήσει το βασικό περιεχόμενο της δουλειάς που έγινε φέτος. Στην εισαγωγή περιγράφονται τα Ασύρματα Δίκτυα Αισθητήρων, δίνονται βασικοί ορισμοί, αναλύονται οι κατευθύνσεις που ακολουθεί η έρευνα και οι βασικοί παράγοντες που επηρρεάζουν το σχεδιασμό όσον αφορά την κατασκευή των αισθητήριων συσκευών, τα πρωτόκολλα δρομολόγησης και τους μηχανισμούς ασφαλείας. Στο δεύτερο κεφάλαιο περιγράφεται το πρόβλημα της δρομολόγησης και παρουσιάζονται κάποια πρωτόκολλα τα οποία αναδεικνύουν συγκεκριμένες προσεγγίσεις στο ζήτημα της δρομολόγησης. Στο τρίτο κεφάλαιο μελετάται το θέμα της ασφάλειας, παρουσιάζονται κάποιες βασικές προσεγγίσεις στην παραδοσιακή κρυπτογραφία, εξειδικεύεται η ασφάλεια στα Ασύρματα Δίκτυα Αισθητήρων και παρουσιάζονται κάποιες πρακτικές τεχνικές ασφάλειας οι οποίες χρησιμοποιούνται και στο καινούριο πρωτόκολλο που παρουσιάζουμε στο τέταρτο κεφάλαιο.

Ευχαριστίες

Ευχαριστώ πολύ τον επιβλέποντα καθηγητή μου Χρήστο Ζαρολιάγκη ο οποίος μου έκανε την τιμή να με επιλέξει αναθέτοντάς μου τη συγκεκριμένη διπλωματική εργασία και μου έδωσε την ευκαιρία να ασχοληθώ με ένα τόσο ενδιαφέρον θέμα.

Ευχαριστώ πολύ τον συνεπιβλέποντα καθηγητή μου Ιωάννη Χατζηγιαννάκη, ο οποίος μου αφιέρωσε πάρα πολύ χρόνο από το φορτωμένο του πρόγραμμα, με καθοδήγησε στη μελέτη μου, με ενθάρρυνε να κάνω ερευνητική δουλειά αντί βιβλιογραφικής στα πλαίσια της διπλωματικής εργασίας, δίνοντας μου έτσι την ευκαιρία να βιώσω την εμπειρία του να συνεισφέρω, έστω και σε πολύ μικρό βαθμό, στην επιστημονική κοινότητα, σχεδίασε μαζί μου το πρωτόκολλο που παρουσιάζουμε, ανέλαβε μεγάλο ποσοστό της συγγραφής των κειμένων προς δημοσίευση και με συμβούλευσε στη συγγραφή του τελικού κειμένου της διπλωματικής εργασίας.

Ευχαριστώ πολύ την Βάσια Λιάγκου που αφιέρωσε και αυτή χρόνο από το φορτωμένο της πρόγραμμα για να συνεισφέρει καθοριστικά στην ερευνητική δουλειά στο ζήτημα της ασφάλειας στο οποίο διαθέτει εξαιρετικές γνώσεις.

Ευχαριστώ πολύ τον Κο Παύλο Σπυράκη για την τιμή που μου έκανε να συνεισφέρει και να συμμετάσχει στις εργασίες που εστάλησαν προς δημοσίευση.

Ευχαριστώ πολύ όλους τους φίλους μου που αμέλησα προκειμένου να πραγματοποιήσω αυτήν την εργασία και που με ενθάρρυναν σε όλη τη διάρκεια της φετινής χρονιάς.

Περιεχόμενα

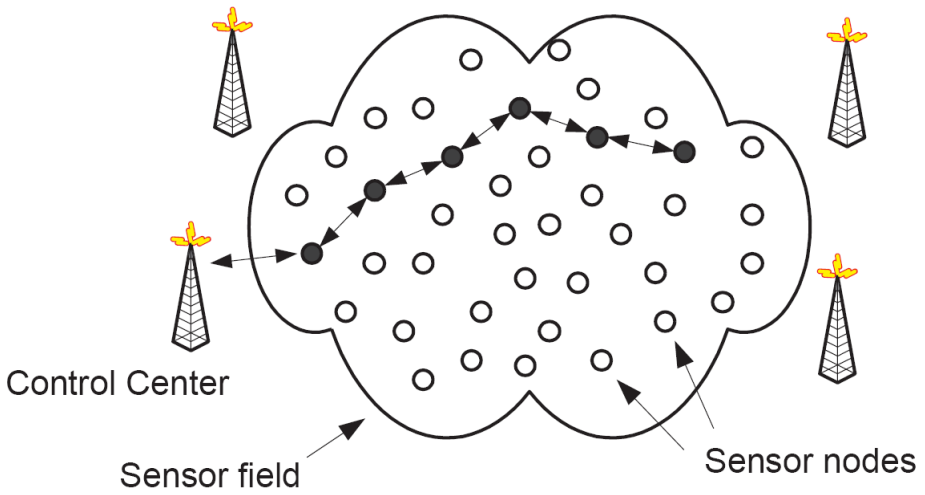
Κεφάλαιο 1

Εισαγωγή

1.1 Δίκτυα Αισθητήρων: Δρομολόγηση και Ασφάλεια

1.1.1 Δίκτυα Αισθητήρων και Προβλήματα Μελέτης

Ένα δίκτυο αισθητήρων είναι μια υποδομή που αποτελείται από αισθητήρια, υπολογιστικά και επικοινωνιακά στοιχεία που δίνουν την δυνατότητα σε μια εξωτερική οντότητα, δηλαδή εναν διαχειριστή, να παρατηρεί και να αντιδρά σε δυναμικές συνθήκες ενός συγκεκριμένου περιβάλλοντος. Πιο συγκεκριμένα, ένα ασύρματο δίκτυο αισθητήρων (Wireless Sensor Network, WSN) είναι ένα ασύρματο δίκτυο το οποίο αποτελείται από αυτόνομες συσκευές τοποθετημένες σε ένα περιβάλλον οι οποίες χρησιμοποιούν αισθητήρια όργανα για να μπορέσουν έπειτα και από συνεργασία μεταξύ τους να επιβλέψουν περιβαλλοντικές συνθήκες, όπως θερμοκρασία, κίνηση, φωτεινότητα, ήχο, δονήσεις, πίεση, υγρασία, κ.α. Ο διαχειριστής/παρατηρητής είναι μια εξωτερική οντότητα, συνήθως κάποιος από κυβερνητικό, εμπορικό, βιομηχανικό, κ.α. περιβάλλον, ο οποίος χρησιμιοποιεί το ασύρματο δίκτυο αισθητήρων για να παρακολουθεί τις αλλαγές στις συνθήκες του περιβάλλοντος. Το περιβάλλον μπορεί να είναι ένα φυσικό περιβάλλον, ένας βιολογικός οργανισμός, ένας βιότοπος, μια κτιριακή



υποδομή, μια ολόκληρη πόλη κ.α.

Η έρευνα που σχετίζεται γύρω από τα Ασύρματα Δίκτυα Αισθητήρων είναι πολυεπίπεδη καθώς και η ίδια η λειτουργία των ασύρματων δικτύων αισθητήρων. Πολλά από τα πεδία έρευνας γύρω από τα Ασύρματα Δίκτυα Αισθητήρων είναι 'εισαγόμενα' από άλλους τομείς της επιστήμης των υπολογιστών, όπως ο σχεδιασμός συστημάτων υλικού και τα ολοκληρωμένα κυκλώματα, οι ψηφιακές τηλεπικοινωνίες, η αρχιτεκτονική υπολογιστών, τα τηλεπικοινωνιακά δίκτυα, ο προγραμματισμός χαμηλού επιπέδου, τα λειτουργικά συστήματα, οι κατανεμημένοι αλγόριθμοι, τα αδόμητα (ad-hoc) δίκτυα, η κρυπτογραφία κ.α. Η βασική στοχοθεσία στα Ασύρματα Δίκτυα Αισθητήρων όμως είναι να χρησιμοποιούνται συσκευές πολύ μικρού κόστους προκειμένου να είμαστε σε θέση να επιστρατεύουμε περισσότερες τέτοιες συσκευές. Αυτό έχει σαν αποτέλεσμα μέχρι στιγμής να μην επαληθεύεται ο νόμος του Moore και οριακά να αντιστρέφεται. Συνεπώς, η εφαρμογή των Ασύρματων Δικτύων Αισθητήρων απαιτεί τουλάχιστον ειδίκευση των παραπάνω, αλλά και περαιτέρω εισαγωγή καινούριων πεδίων έρευνας. Αυτό συμβαίνει επειδή συνήθως απαιτείται από ένα ασύρματο δίκτυο αισθητήρων και τα συστατικά μέρη του να πληρεί κάποιες προϋποθέσεις, όπως χαμηλή κατανάλωση ενέργειας, βασική ροή πληροφοριών προς το κέντρο ελέγχου, κ.α.

Ένα πεδίο έρευνας που σχετίζεται έντονα με τα Ασύρματα Δίκτυα Αισθητήρων είναι τα Αδόμητα Δίκτυα (ad-hoc Networks) και τα Κινητά Αδόμητα Δίκτυα (MANETs, Mobile Ad-hoc Networks). Τα Αδόμητα Δίκτυα είναι δίκτυα ομέγενων συσκευών τα οποία δεν έχουν αρχικά επίγνωση της τοπολογίας του δικτύου. Συνήθως χρησιμοποιούν ασύρματη επικοινωνία και χρησιμοποιούν επικοινωνία μέσω πολλαπλών ενδιάμεσων κόμβων, δηλαδή δύο απομακρυσμένες συσκευές δεν επικοινωνούν απ΄ ευθείας αλλά εκμεταλλεύονται την ύπαρξη ενδιάμεσων συσκευών. Οι αλγόριθμοι δρομολόγησης βρίσκουν διαδρομές μεταξύ οποιονδήποτε συσκευών και άλλα προβλήματα που επιχειρούνται να λυθούν μέσω των αδόμητων δικτύων είναι η κατανεμημένη μνήμη μέσω τεχνικών Pastry [23], κατανεμημένες υπολογιστικές διεργασίες, κ.α. Πολλοι αλγόριθμοι των αδόμητων δικτύων χρησιμοποιούνται και στο διαδίκτυο, όπως για παράδειγμα ο Κατανεμημένος Πίνακας Κατακερματισμού (Distributed Hash Table, DHT) το οποίο είναι μια υλοποίηση τεχνικής Pastry. Τα Κινητά Αδόμητα Δίκτυα είναι μια ειδίκευση των αδόμητων δικτύων τα οποία είναι έχουν το στοιχείο της κίνησης, δηλαδή κατά στο σχεδιασμό των πρωτοκόλλων και των αλγορίθμων περιλλαμβάνεται η υπόθεση ότι οι συνδέσεις επικοινωνίας μεταξύ των συσκευών μπορεί να καταργηθούν ή να δημιουργηθούν νέες.

Αν και τα δύο πεδία έρευνας (τα Αδόμητα Δίκτυα και τα Ασύραματα Δίκτυα Αισθητήρων) έχουν πολλές ομοιότητες, όπως το γεγονός ότι και στα δύο χρησιμοποιείται επικοινωνία μέσω πολλαπλών ενδιάμεσων κόμβων ως επί το πλήστον, και ίσως κάποιος θα μπορούσε να πει πως τα ασύρματα δίκτυα αισθητήρων αποτελούν ειδίκευση των αδόμητων δικτύων, υπάρχουν τεράστιες διαφορές που καθιστούν το πεδίο των ασύρματων δικτύων αισθητήρων σχετικά αυτόνομο. Οι βασικές διαφορές είναι:

- Οι συσκευές που χρησιμοποιούντα στα Αδόμητα Δίκτυα έχουν δυνατότητες που δεν περιγράφονται γενικά αλλά διευκρινίζονται συνήθως στο μοντέλο πάνω στο οποίο εφαρμόζεται ένας αλγόριθμος ή ένα πρωτόκολλο. Γενικά πάντως, οι δυνατότητες των συσκευών σε ένα Αδόμητο Δίκτυο θεωρούνται πολύ καλύτερες απ΄ ότι στα Ασύρματα Δίκτυα Αισθητήρων, καθώς κάθε συσκευή μπορεί να έχει τακτική ή συνεχή επίβλεψη από έναν χρήστη του δικτύου, οπότε και η πηγή ενέργειας να ανανεώνεται, οι συσκευές οι ίδιες επιλέγονται ώστε να είναι σε θέση να ανταπεξέλθουν στις απαιτήσεις του δικτύου, για παράδειγμα θα μπορούσαν να είναι φορητοί υπολογιστές, κ.α. Στα Ασύρματα

Δίκτυα Αισθητήρων αντίθετα, οι συσκευές λειτουργούν για μεγάλα χρονικά διαστήματα χωρίς ανθρώπινη αλληλεπίδραση και η ανάγκη για μεγάλο πλήθως αισθητήριων συσκευών πιέζει για συσκευές μικρού κόστους και άρα χαμηλών δυνατοτήτων.

- Στα Αδόμητα Δίκτυα οι συσκευές συνήθως είναι ομότιμες, ενώ στα Ασύρματα Δίκτυα Αισθητήρων υπάρχουν οι διακριτοί ρόλοι της απόληξης (sink) και των αισθητήρων (sensors).

- Οι στόχοι των Αδόμητων Δικτύων διαφέρουν σημαντικά από αυτούς των Ασύρματων Δικτύων Αισθητήρων με το κύριο παράδειγμα να είναι η δρόμολόγηση. Στα Αδόμητα Δίκτυα η δρομολόγηση συνεπάγεται την αναζήτηση διαύλων επικοινωνίας μεταξύ δύο οποιονδήποτε συσκευών ενώ στα Ασύρματα Δίκτυα Αισθητήρων η βασική ροή πληροφορίας είναι από τις αισθητήριες συσκευές στην απόληξη ενώ πολλές φορές επιθυμείται και το αντίθετο προκειμένου να μπορεί να αναθέτει εργασίες ο διαχειριστής στις αισθητήριες συσκευές αλλά και να συντονίζει τη λειτουργία του δικτύου.

- Το μέγεθος ενός Ασύρματου Δικτύου Αισθητήρων συνήθως είναι μερικές τάξεις μεγέθους μεγαλύτερο απ΄ ότι ενός Αδόμητου Δικτύου με αποτέλεσμα οι αλγόριθμοι και τα πρωτόκολλα να πρέπει να προσαρμόζονται σε αυτήν την κατάσταση. Για παράδειγμα, σε ένα Αδόμητο Δίκτυο μπορεί να υπάρχουν τόσες καταχωρήσεις στον πίνακα δρομολόγησης όσες και οι συσκευές που συμμετέχουν στο δίκτυο, ενώ στα Ασύρματα Δίκτυα Αισθητήρων απαιτείται ο πίνακας δρομολόγησης να καταλαμβάνει σταθερό χώρο. Επίσης, η μεγάλη πυκνότητα των συσκευών και συνεπώς η μικρή απόσταση μεταξύ τους καθιστά την επικοινωνία μέσω πολλαπλών ενδιάμεσων κόμβων πιο αποτελεσματική απ΄ ότι στα Αδόμητα Δίκτυα.

- Οι συσκευές που συμμετέχουν σε ένα Ασύρματο Δίκτυο Αισθητήρων είναι πολύ πιθανόν να σταματήσουν να λειτουργούν με αποτέλεσμα οι αλγόριθμοι και τα πρωτόκολλα να πρέπει να προσαρμόζονται σε αυτήν την κατάσταση.

Έχουν εμφανιστεί ειδικεύσεις στα Ασύρματα Δίκτυα Αισθητήρων που περιλαμβάνουν:

- Κινητά Ασύρματα Δίκτυα Αισθητήρων, όπου οι αισθητήρες, η απόληξη ή και τα δύο είναι κινητά.

- Παρουσία πολλών απολήξεων, όπου συνήθως επικοινωνούν μεταξύ τους αυτόνομα χωρίς να επηρρεάζουν τη λειτουργία του υπόλοιπου δικτιού, οπότε η παραλαβή ενός μηνύματος από μια απόληξη είναι ισοδύναμη με την παραλαβή του ίδιου μηνύματος από οποιοδήποτε άλλη απόληξη.

- Ύπαρξη ενδιάμεσων συσκευών ελέγχου πέραν από τις απολήξεις τα οποία μπορεί να καθορίζονται από την κατασκευή τους ως τέτοια και να τοποθετούνται με ανάλογο τρόπο στο περιβάλλον ή να είναι απλές αισθητήριες συσκευές που σύμφωνα με το πρωτόκολλο που εκτελείται αναλαμβάνουν αυτόν τον ρόλο.

1.1.2 Συστατικά/Αρχιτεκτονική των Συσκευών - Σχεδιασμός

Κάνουμε μια αφαίρεση σύμφωνα με την οποία οι συσκευές που συμμετέχουν σε ένα Ασύρματο Δίκτυο Αισθητήρων χωρίζονται σε δύο κατηγορίες. Οι αισθητήριες συσκευές (sensor motes), στα οποία στα πλαίσια περιγραφής ενός πρωτοκόλλου θα αναφερόμαστε ως αισθητήρες, και τις απολήξεις στις οποίες θα αναφερόμαστε ως κέντρα ελέγχου (control centers), σταθμούς βάσης (base stations) ή απολήξεις (sinks). Οι αισθητήριες συσκευές διαθέτουν αισθητήρες, προκειμένου να ανιχνεύουν περιβαλλοντικές συνθήκες, ένα υπολογιστικό σύστημα με επεξεργαστή και μνήμη, προκειμένου να ελέγχουν όλες τις λειτουργίες της συσκευής και να εκτελούν υπολογισμούς, ένα ασύρματο σύστημα μετάδοσης πληροφορίας, προκειμένου να μπορούν να επικοινωνούν με τους υπόλοιπους αισθητήρες και της απόληξης, και μια (συνήθως αναλώσημη) πηγή ενέργειας. Η απόληξη θεωρείται ως η σύνδεση του Ασύρματου Δικτύου Αισθητήρων με τον παρατηρητή/χρήστη. Είναι οι συσκευές οι οποίες συλλέγουν τις πληροφορίες που παράγει το δίκτυο και πολλές φορές συντονίζουν τη λειτουργία του δικτύου. Μέσω αυτών πραγματοποιείται όλη η αλληλεπίδραση με τον έξω κόσμο, διευκρινίζοντας σε αυτό το σημείο ότι έξω κόσμος δεν θεωρείται το περιβάλλον, αλλά ο διαχειριστής/χρήστης ο οποίος μπορεί να θέσει ένα συγκεκριμένο ερώτημα στο δίκτυο, να αναθέσει μια συγκεκριμένη εργασία ή να πραγματοποιήσει κάποια ενέργεια σχετική με τα πρωτόκολλα που υλοποιεί το δίκτυο και, προφανώς, να συλλέξει τις πληροφορίες που παράγει το δίκτυο. Στα πλαίσια περιγραφής των μοντέλων πάνω στα οποία ορίζεται ένα πρωτόκολλο, αλλά και στην εφαρμογή των Ασύρματων Δικτύων Αισθητήρων στην πράξη, οι απολήξεις διαθέτουν σαφώς περισσότερους πόρους όσον αφορά την υπολογιστική δυνατότητα, την αυτονομία σε ενέργεια, την επικοινωνική δυνατότητα και την αξιοπιστία λειτουργίας και μετάδοσης πληροφοριών.

Το ζήτημα του σχεδιασμού μιας αισθητήριας συσκευής είναι αρκετά πολύπλοκο καθώς συνδυάζει πολλούς τομείς έρευνας. Οι παράμετροι του σχεδιασμού εξαρτώνται τόσο από την εφαρμογή στην οποία καλείται να ανταπεξέλθει η αισθητήρια συσκευή αλλά και από το περιβάλλον στο οποίο καλείται να λειτουργήσει. Για παράδειγμα, ανάλογα με το τι περιβαλλοντικές πληροφορίες πρέπει να μετρήσει, πρέπει να εξοπλισθεί με τα ανάλογα αισθητήρια όργανα (μετρητές μαγνητικού πεδίου, φωτόμετρα, μετρητές ραδιενέργιας, υγρόμετρα, θερμόμετρα, μετρητές ατμοσφαιρικής πίεσης, μετρητές ήχου, επιταχυνσιόμετρα, συστήματα εντοπισμού τοποθεσίας κλπ), ενώ ανάλογα με το περιβάλλον πρέπει να προσδιορίζονται οι κατάλληλες παράμετροι ώστε να εξασφαλίζεται η εύρυθμη λειτουργία τους (αντοχή σε κρούσεις, στην ύπαρξη υγρασίας, διάρκεια ενεργειακής αυτονομίας, κλπ). Συγκεκριμένα, οι βασικοί παράγοντες που επηρρεάζουν το σχεδιασμό των Ασύρματων Δικτύων Αισθητήρων είναι οι εξής:

- **Αντοχή σε Σφάλματα:** Σε ένα Ασύρματο Δίκτυο Αισθητήρων, κάποιες συσκευές είναι πιθανό να σταματήσουν τη λειτουργία τους εξαιτίας έλλειψης αποθεμάτων ενέργειας ή περιβαλλοντικών συνθηκών. Ο σχεδιασμός πρέπει να λαμβάνει υπόψιν του αυτήν την κατάσταση και να εξασφαλίζει ότι οι λειτουργικοί στόχοι ενός δικτύου θα συνεχίζουν να εκπληρώνονται παρά την παρουσία αυτού του προβλήματος. Αξίζει να παρατηρήσουμε ότι η βαρύτητα του συγκεκριμένου παράγοντα μπορεί να μεταβάλλεται ανάλογα με την εφαρμογή του δικτύου. Για παράδειγμα, η επίβλεψη ενός νοσοκομειακού χώρου δεν παρέχει ένα ¨επικίνδυνο' περιβάλλον για αισθητήριες συσκευές οπότε ο σχεδιασμός σε αυτήν την περίπτωση μπορεί να είναι πιο χαλαρός όσον αφορά τον συγκεκριμένο

παράγοντα, σε αντίθεση με εφαρμογές επίβλεψης ενός βιότοπου (πχ μια δασική περιοχή) ή ενός πεδίου μάχης.

- **Επεκτασιμότητα:** Οι εφαρμογές στις οποίες καλούνται να ανταπεξέλθουν τα Ασύρματα Δίκτυα Αισθητήρων μπορούν να επιστρατεύουν εκατοντάδες χιλιάδες αισθητήριες συσκευές. Κατά το σχεδιασμό, αυτός ο παράγοντας πρέπει να λαμβάνεται σοβαρά υπόψιν, σε αντιστοιχία πάντα και με την εκάστοτε εφαρμογή.

- **Κόστος Παραγωγής:** Το κόστος ανάπτυξης ενός Ασύρματου Δικτύου Αισθητήρων πρέπει να είναι τέτοιο ώστε να δικαιολογεί την επιλογή του έναντι παραδοσιακών αισθητήρων. Λόγω και της μεγάλης πυκνότητας και ποσότητας των αισθητήριων συσκευών, ο συγκεκριμένος παράγοντας αποκτάει ιδιαίτερα μεγάλη σημασία. Ένας επιθυμητός στόχος για το άμεσο μέλλον θα ήταν πχ να κοστίζει μια αισθητήρια συσκευή 1$.

- **Περιορισμοί υλικού:** Το γεγονός ότι ένα πλήρες ολοκληρωμένο υπολογιστικό σύστημα εξοπλισμένο με παροχή ενέργειας, αισθητήριες συσκευές, μετατροπείς αναλογικού σε ψηφιακού σήματος, τηλεπικοινωνιακό σύστημα και κάποιες ακόμα προαιρετικές μονάδες το οποίο πρέπει να έχει το μέγεθος ιδανικά ενός σπιρτόκουτου με πολύ μικρό επιθυμητό κόστος επιβάλλει μια πολύ συγκεκριμένη πραγματικότητα. Ο συνδυασμός μικρού μεγέθους - μικρού κόστους για τις αισθητήριες συσκευές επιβάλλει σοβαρούς περιορισμούς δυνατοτήτων υλικού. Αυτό πρέπει να λαμβάνεται σοβαρά υπόψιν κατά το σχεδιασμό αλγορίθμων και πρωτοκόλλων για τα Ασύρματα Δίκτυα Αισθητήρων και πρέπει να επιδιώκεται πάντα η βελτιστοποίηση σε υπολογισμούς και ασύρματες μεταδόσεις, τόσο προκειμένου να έχει το δίκτυο μεγάλη διάρκεια ζωής, όσο και να πραγματοποιεί τις απαιτούμενες λειτουργίες σε ικανοποιητικό χρόνο. Για παράδειγμα, δύσκολοι υπολογισμοί πρέπει να αποφεύγονται ή να πραγματοποιούνται με κατανεμημένο τρόπο στο δίκτυο, όπως στις εφαρμογές κρυπτογραφίας, αλλά και εξαγωγής στατιστικών συμπερασμάτων όσον αφορά τις περιβαλλοντικές συνθήκες που καλείται να καταγράψει το δίκτυο.

- **Λειτουργικό Περιβάλλον:** Τα Ασύρματα Δίκτυα Αισθητήρων τοποθετούνται είτε μέσα είτε πολύ κοντά στο φαινόμενο που καλούνται να παρατηρήσουν, οπότε πιθανά περιβάλλοντα μπορεί να είναι εσωτερικό κτιρίων, το βάθος της θάλασσας, στο εσωτερικό μιας μηχανής, στην επιφάνεια ενός ωκεανού κατά τη διάρκεια ενός ανεμοστρόβιλου, σε μια περιοχή με παρουσία βιοχημικών στοιχείων, σε ένα πεδίο μάχης, σε ένα ποτάμι καθώς καταγράφουν τη ροή του νερού, κλπ. Αυτά μας δίνουν μια εικόνα για το τι πρέπει να είναι σε θέση να αντιμετωπίσουν τα Ασύρματα Δίκτυα Αισθητήρων, τόσο όσον αφορά τους αλγόριθμους και τα πρωτόκολλα, όσο και τις ίδιες τις συσκευές, οι οποίες πρέπει να είναι σχεδιασμένες έτσι ώστε να μπορούν να επιβιώσουν και να ανταπεξέλθουν στις συνθήκες που επιβάλλει το περιβάλλον.

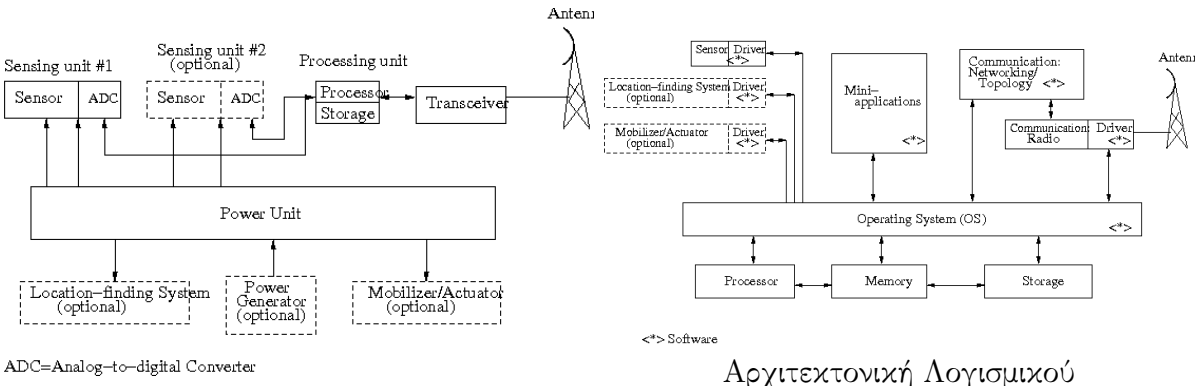
- **Τοπολογία Δικτύου Αισθητήρων:** Ο τρόπος με τον οποίον τοποθετούνται οι αισθητήριες συσκευές σε ένα Ασύρματο Δίκτυο Αισθητήρων εισάγει μια σημαντική παράμετρο σχεδιασμού των Ασύρματων Δικτύων Αισθητήρων. Το μεγάλο πλήθος αισθητήριων συσκευών καθιστά απαγορευτική την εισαγωγή των συσκευών 'με το χέρι', καθώς κάτι τέτοιο θα ήταν πολύ χρονοβόρο και θα απαιτούσε προσεχτικό σχεδιασμό της διαδικασίας τοποθέτησης εκ των προτέρων παρ'ολο που αυτό θα είχε σαν

αποτέλεσμα τη βέλτιστη τοπολογία για τη λειτουργία του δικτύου. Αντί αυτού πρέπει να σκεφτόμαστε τρόπους που οι συσκευές τοποθετούνται τυχαία στο περιβάλλον, πχ με ρίψη από αεροπλάνο. Το δίκτυο πρέπει λοιπόν να προσαρμόζεται στην τυχαία αυτή τοπολογία. Επιπλέον, πρέπει να έχουμε υπόψιν μας ότι η τοπολογία ενός δικτύου μπορεί να αλλάζει κατά τη διάρκεια της λειτουργίας για διάφορους λόγους. Τέλος, πολλές φορές πρέπει οι αλγόριθμοι και τα πρωτόκολλα να είναι σχεδιασμένοι έτσι ώστε να υποστηρίζουν την προσθήκη επιπλέον συσκευών στο δίκτυο, επίσης με τυχαίο τρόπο, κατά τη διάρκεια της λειτουργίας του.

- **Τηλεπικοινωνιακά μέσα:** Όσον αφορά τα τηλεπικοινωνιακά μέσα, το ζήτημα του σχεδιασμού αφορά των εντοπισμό της κατάλληλης τεχνολογίας που να συνδυάζει αποτελεσματικότητα, χαμηλή κατανάλωση και την εύρεση συχνοτήτων που να μην είναι σε χρήση. Στην περίπτωση των Ασύρματων Δικτύων Αισθητήρων δεν μας ενδιαφέρει η μεγάλη εμβέλεια εκπομπής καθώς η μεγάλη πυκνότητα συσκευών στο περιβάλλον ευνοεί την επικοινωνία μέσω πολλαπλών ενδιάμεσων κόμβων. Όσον αφορά τους παράγοντες κατανάλωσης και εύρεσης κατάλληλων συχνοτήτων, η βέλτιστη λύση μέχρι στιγμής είναι οι συχνότητες UHF. Μια άλλη ενδιαφέρουσα προτεινόμενη λύση είναι οι υπέρυθρες ακτίνες με βασικό πλεονέκτημα την χαμηλή κατανάλωση και με βασικό μειονέκτημα την ανάγκη για οπτική επαφή μεταξύ των συσκευών.

- **Κατανάλωση Ενέργειας:** Κατά τη διάρκεια λειτουργίας μιας αισθητήριας συσκευής, ενέργεια καταναλώνεται όταν καταγράφονται οι συνθήκες του περιβάλλοντος μέσω των αισθητήριων οργάνων, όταν πραγματοποιείται ασύρματη επικοινωνία και όταν πραγματοποιούνται υπολογισμοί. Όσον αφορά την καταγραφή των συνθηκών του περιβάλλοντος, δεν μπορεί να αντιμετωπιστεί κατά το σχεδιασμό καθώς εξαρτάται από το περιβάλλον και το πόσο συχνά αλλάζουν οι συνθήκες του. Όσον αφορά την ασύρματη επικοινωνία, έχει παρατηρηθεί ότι η ενεργοποίηση και απενεργοποίηση της τηλεπικοινωνιακής μονάδας κοστίζει πολλές φορές περισσότερο από τη μετάδοση αυτή καθ΄ εαυτή, οπότε για έναν αλγόριθμο είναι θεμιτό να μπορεί να εντοπίζει πότε υπάρχει έντονη κινητικότητα όσον αφορά τις μεταδόσεις και να διατηρει το τηλεπικοινωνιακό σύστημα μονίμως αναμένο και πότε δεν υπάρχει καθόλου κινητικότητα και να διατηρεί το τηλεπικοινωνιακό σύστημα μονίμως σβηστό. Όσον αφορά τους υπολογισμούς, πρέπει να προσπαθούμε να αποφεύγουμε πολύπλοκες διαδικασίες και να κρατάμε τους επιμέρους υπολογισμούς σε κάθε συσκευή σε χαμηλό επίπεδο, μεταφέροντας το βάρος είτε σε κατανεμημένους υπολογιστικούς αλγόριθμους ή στην απόληξη. Μια επιπλέον παρατήρηση είναι ότι η ενέργεια που καταναλώνεται για τις μεταδόσεις είναι κάποιες τάξεις μεγέθους μεγαλύτερη από την ενέργεια που καταναλώνεται για τους υπολογισμούς, οπότε πολλές φορές είναι προτιμότερο να συμπιέζονται δεδομένα και να μεταδίδονται παρά να μεταδίδονται απ΄ ευθείας.

Τα σύστατικά μιας αισθητήριας συσκευής όσον αφορά το υλικό εμφανίζουνται στο σχήμα 1.1. Η πηγή ενέργειας συνδέεται με όλες τις λειτουργικές μονάδες της συσκευής. Η μονάδα επεξεργασίας συνδέεται με τα αισθητήρια όργανα και με τη τηλεπικοινωνιακή μονάδα προκειμένου να λαμβάνει δεδομένα και να ελέγχει τη λειτουργία τους. Όπως βλέπουμε, υπάρχουν και προαιρετικές μονάδες όπως σύστημα εντοπισμού τοποθεσίας (GPS), μια παροχή ενέργειας και/ή ένα mobilizer/actuator, τα οποία συνδέονται επίσης με την πηγή ενέργειας και την μονάδα επεξεργασίας. Όσον αφορά το λογισμικό, η δομή είναι πιο περίπλοκη. Το



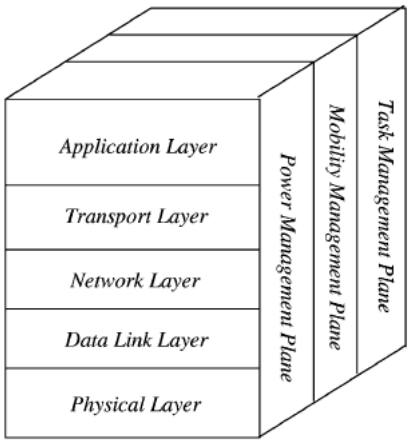
Αρχιτεκτονική Υλικού

Αρχιτεκτονική Λογισμικού

Σχήμα 1.1: Αρχιτεκτονική μιας αισθητήριας συσκευής

κεντρικό στοιχείο εδώ είναι το λειτουργικό σύστημα το οποίο αναλαμβάνει τη διεπαφή με τα αισθητήρια όργανα, την κατανομή των επεξεργαστικών πόρων, την εκτέλεση των εφαρμογών, την υλοποίηση των πρωτοκόλλον που υλοποιούνται και τη διεπαφή με τα υπόλοιπα περιφερειακά (σύστημα τηλεπικοινωνίας, σύστημα εντοπισμού τοποθεσίας, mobilizer, κλπ).

Τα επίπεδα λειτουργίας των Ασύρματων Δικτύων Αισθητήρων διακρίνονται σε επίπεδο υλικού, επίπεδο συνδέσμου μετάδοσης δεδομένων, επίπεδο δικτύου, επίπεδο μεταφοράς και επίπεδο εφαρμογών. Το φυσικό επίπεδο είναι υπεύθυνο για την επιλογή συχνότητας, δημιουργία συχνότητας φέροντος, ανίχνευση σήματος και διαμόρφωση. Το επίπεδο συνδέσμου μετάδοσης δεδομένων είναι υπεύθυνο για την πολύπλεξη ροών πληροφορίας, ανίχνευση πακέτων πληροφοριών, πρόσβαση μέσου (Medium Access Control, MAC) και έλεγχο σφαλμάτων. Το επίπεδο δικτύου στα Ασύρματα Δίκτυα Αισθητήρων διαφέρει σημαντικά από τα συνηθισμένα δίκτυα και τα Αδόμητα δίκτυα και πρέπει να σχεδιάζεται έτσι ώστε να εξοικονομείται ενέργεια, να επικεντρωνουν στα δεδομένα και να διευθυνσιοδητούν με βάση περιβαλλοντικά χαρακτηριστικά και τοποθεσία. Το επίπεδο μεταφοράς χρησιμεύει στα Ασύρματα Δίκτυα Αισθητήρων όταν έχουμε σκοπό να παρακολουθούμε το περιβάλλον εξωτερικά μέσω κάποιου άλλου δικτύου όπως το διαδίκτυο. Συνήθως πραγματοποιείται ένα κλασσικό TCP ή UDP επίπεδο μεταφοράς μεταξύ των απομακρυσμένων χρηστών και της απόληξης και μεταξύ της απόληξης και των αισθητήρων χρησιμοποιείται κάποιο πρωτόκολλο μεταφοράς που μοιάζει περισσότερο με UDP εξαιτίας της περιορισμένης μνήμης των αισθητήρων. Υπενθυμίζουμε ότι η διευθυνσιοδότηση σε αυτό το επίπεδο δύσκολα μπορεί να βασίζεται σε καθολικές και μοναδικές ταυτότητες αλλά πρέπει να βασίζεται σε γνωρίσματα του περιβάλλοντος. Στο επίπεδο εφαρμογών πάλι έχουμε να κάνουμε με την αλληλεπίδραση των απομακρυσμένων χρηστών και του δικτύου μέσω της απόληξης. Εφαρμογές που μπορούν να αναπτυχθούν παρέχουν στους χρήστες εύκολους τρόπους να θέσουν ερωτήματα στους αισθητήρες του δικτύου, να συλλέξουν πληροφορίες και να διαχειριστούν τη λειτουργία των αισθητήρων γενικότερα.



Σχήμα 1.2: Τα Επίπεδα Πρωτοκόλλων των Ασύρματων Δικτύων Αισθητήρων

1.2 Προβλήματα που Πραγματεύεται η Διπλωματική Εργασία - Υπάρχουσες Προσεγγίσεις

1.2.1 Η Δρομολόγηση

Το πρόβλημα της δρομολόγησης στα Ασύρματα Δίκτυα Αισθητήρων παρουσιάζει ιδιαίτερο ενδιαφέρον σε σχέση τόσο με τα παραδοσιακά δίκτυα όσο και με τα Αδόμητα Δίκτυα. Ειδικά για την περίπτωση των Αδόμητων Δίκτυων, θα μπορούσε κάποιος να υποθέσει ότι μια απλή προσαρμογή ή μεταφορά ενός αλγόριθμου δρομολόγησης από τα Αδόμητα Δίκτυα θα αρκούσε για να έχει πετυχημένη και αποδοτική εφαρμογή στα Ασύρματα Δίκτυα Αισθητήρων. Αυτό συμβαίνει για αρκετούς λόγους, κάποιους από τους οποίους του είδαμε στις προηγούμενες ενότητες. Εδώ θα τους παραθέσουμε ολοκληρωμένα:

- Περιορισμοί υλικού στις συσκευές αισθητήρων
- Πλήθος των κόμβων του Δικτύου
- Ύπαρξη μη Ομότιμων Συσκευών (Αισθητήρες - Απόληξη)
- Μη αξιοπιστία των συσκευών
- Διασύνδεση του Διαχειριστή με το Δίκτυο Μόνο Μέσω της Απόληξης, Ανεξάρτητη Λειτουργία των Αισθητήρων
- Διαφορετικά Ζεύγη Αφετηρίασ-Προορισμού Πακέτων (Αισθητήρες - Απόληξη ή Απόληξη - Αισθητήρες, όχι Αισθητήρας - Αισθητήρας)
- Ανάγκη για Χαμηλή Κατανάλωση Ενέργειας

Στην παρούσα διπλωματική εργασία εξετάζονται κάποιοι αντιπροσωπευτικοί προτεινόμενοι αλγόριθμοι δρομολόγησης για τα Ασύρματα Δίκτυα Αισθητήρων. Κάθε αλγόριθμος προσπαθεί να βελτιστοποιήσει τη συμπεριφορά του δικτύου ως προς ένα κριτήριο κάθε φορά. Ο

σχεδιαστής ενός αλγόριθμου δρομολόγησης πρέπει ανάλογα με τις απαιτήσεις της εφαρμογής του Ασύρματου Δικτύου Αισθητήρων να καταλαβαίνει ποιο είναι το κριτήριο ως προς το οποίο πρέπει να βελτιστοποιήσει τη συμπεριφορά του αλγόριθμου. Τα κριτήρια αυτά είναι τα εξής:

1. **Διευθυνσιοδότηση:** Ένα ζήτημα το οποίο εξετάσαμε ήδη είναι ότι μερικές φορές το πλήθος των συσκευών σε ένα Ασύρματο Δίκτυο Αισθητήρων μπορεί να καταστήσει απαγορευτική το να υπάρχει διαθέσιμη μία μοναδική διεύθυνση για κάθε συσκευή. Αυτό όμως δεν είναι το μόνο πρόβλημα. Στα Ασύρματα Δίκτυα Αισθητήρων η απόληξη ανήκει πάντα στο ζεύγος αφετηρία-προορισμός. Στην περίπτωση που οι αισθητήρες δρομολογούν προς την απόληξη, που είναι και η πιο συνηθισμένη περίπτωση, εφόσον ο προορισμός είναι πάντα ο ίδιος δεν έχει νόημα να του δώσουμε μια 'διεύθυνση'. Αλλά ακόμα και στην περίπτωση πολλών απολήξεων, θα πρέπει να αποφύγουμε οι αισθητήρες να διευθυνσιοδοτούν την κάθε απόληξη, αλλά πρέπει να σχεδιάσουμε τον αλγόριθμό μας να δρομολογεί 'αυτόματα' προς την πλησιέστερη απόληξη κάθε φορά. Το ζήτημα της διευθυνσιοδότησης αποκτάει ενδιαφέρον στην αντίστροφη περίπτωση, δηλαδή όταν δρομολογούμε από την/τις απόληξη/απολήξεις προς τους αισθητήρες. Αυτό συμβαίνει όταν ο διαχειριστής του δικτύου θέλει να θέσει ένα *ερώτημα* προς τους αισθητήρες. Επειδή λοιπόν οι αισθητήρες ενδέχεται να είναι πάρα πολλοί ή επειδή ενδέχεται η τοποθέτησή τους να έγινε τυχαία με αποτέλεσμα να μην γνωρίζει ο διαχειριστής πού βρίσκεται η κάθε συσκευή, δεν έχει νόημα η διευθυνσιοδότηση των πακέτων να αντιστοιχεί στις μοναδικές διευθύνσεις των αισθητήρων (οι οποίες ενδέχεται και να μην υπάρχουν). Αντίθετα, πρέπει να προτιμήσουμε να στείλουμε τα ερωτήματα χρησιμοποιώντας για *διεύθυνση* μια παράμετρο του περιβάλλοντος (θερμοκρασία, υγρασία, τοποθεσία κλπ).

2. **Επιλογή Μοντέλου Επικοινωνίας:** Στα Ασύρματα Δίκτυα Αισθητήρων διακρίνουμε δύο μοντέλα επικοινωνίας, την Απευθείας Επικοινωνία (Direct Communication) και την Επικοινωνία Μέσω Πολλαπλών Ενδιάμεσων Κόμβων. Στο πρώτο μοντέλο μια συσκευή μπορεί να επιλέξει πόση ισχύ θα επιστρατεύσει για την εκπομπή ενός μηνύματος, άρα μπορεί ιδανικά να πετύχει οποιαδήποτε εμβέλεια εκπομπής. Στο δεύτερο μοντέλο οι συσκευές επιστρατεύουν πάντα την ίδια ισχύ, άρα έχουν ιδανικά την ίδια σταθερή εμβέλεια εκπομπής. Τα πλεονεκτήματα της Απευθείας Επικοινωνίας είναι ότι δεν χρειάζεται να βρούμε ένα μονοπάτι από την αφετηρία ενός πακέτου προς τον προορισμό, μπορούμε να προσαρμόσουμε την κατανάλωση ενέργειας σε κάθε εκπομπή προσπαθώντας να πετύχουμε την ελάχιστη και δίνει τη δυνατότητα σε μια συσκευή να μετρήσει την ισχύ μιας εισερχόμενης εκπομπής ενώ η αρχική ισχύς αναγράφεται στην ίδια την εκπομπή και έτσι να αποκτήσει μια εκτίμηση της απόστασης από τη συσκευή-αφετηρία. Τα μειονεκτήματα της Απευθείας Επικοινωνίας είναι ότι παρουσιάζει γενικά μεγάλη κατανάλωση ενέργειας καθώς η κατανάλωση ενέργειας αυξάνεται ανάλογα με το τετράγωνο της αύξησης της εμβέλειας εκπομπής και η παράλληλη εκπομπή διαφορετικών πακέτων και με μεγάλη εμβέλεια είναι πολύ πιθανό να οδηγήσει σε σύγκρουση η οποία επιλύεται με επανάληψη των εκπομπών, κάτι που οδηγεί σε αύξηση της κατανάλωσης και καθυστέρηση. Τα πλεονεκτήματα της Επικοινωνίας Μέσω Πολλαπλών Ενδιάμεσων Κόμβων είναι ότι αποφεύγονται οι συγκρούσεις και έχει σε γενικές γραμμές καλή κατανάλωση ενέργειας. Τα μειονεκτήματα της Επικοινωνίας Μέσω Πολλαπλών Ενδιάμεσων Κόμβων είναι ότι για να επικοινωνήσουν δύο απομακρυσμένες

συσκευές πρέπει να συνεισφέρουν πολλές ενδιάμεσες και έτσι η επικοινωνία στο δίκτυο είναι περισσότερο ευάλωτη σε αποτυχίες κόμβων, καθώς και η δημιουργία της απαραίτητης υποδομής για να δρομολογούνται πακέτα έχει το δικό της κόστος σε ενέργεια και χρόνο.

3. **Τρόπος Συλλογής Δεδομένων από τους Αισθητήρες :**Το Ασύρματο Δίκτυο Αισθητήρων παρέχει πληροφορίες σε έναν διαχειριστή σχετικά με ένα περιβάλλον. Η συλλογή της πληροφορίας μπορεί να γίνεται με τρεις τρόπους. Πρώτον, μπορεί να είναι οδηγούμενη από γεγονότα (event based), δηλαδή όταν μια αισθητήρια συσκευή αντιληφθεί κάποια αλλαγή στο περιβάλλον μπορεί να αναλάβει την πρωτοβουλία να συλλέξει την αντίστοιχη πληροφορία και να προσπαθήσει να την προωθήσει στην απόληξη. Δεύτερον, μπορεί να γίνεται περιοδικά, δηλαδή σε τακτά χρονικά διαστήματα κάθε αισθητήρια συκευή να αναλαμβάνει να συλλέξει πληροφορίες σχετικές με το περιβάλλον και να τις προωθήσει στην απόληξη.

4. **Τοπικά/Ολικά Κριτήρια για Εύρεση Διαδρομών:** Κάθε αλγόριθμος που χρησιμοποιεί Επικοινωνία Μέσω Πολλαπλών Ενδιάμεσων Κόμβων έχει μια συγκεκριμένη στρατηγική με την οποία βρίσκει μονοπάτια από την αφετηρία προς τον προορισμό ενός πακέτου, στην περίπτωσή μας από τους αισθητήρες στην απόληξη ή το αντίστροφο. Αυτή η στρατηγική εκτελείται κατανεμημένα από όλους τους κόμβους του δικτύου οι οποίοι προσπαθούν να 'στήσουν' έναν *πίνακα δρομολόγησης* (routing table) ή κάτι αντίστοιχο αξιοποιόντας τις πληροφορίες που έχουν για όλο το δίκτυο. Ένα ερώτημα που τίθεται εδώ είναι το αν αυτές οι πληροφορίες θα αφορούν το σύνολο του δικτύου ή μόνο τη γειτονιά της κάθε συσκευής. Στην πρώτη περίπτωση οι πληροφορίες που θα αξιοποιηθούν θα είναι πιο χρήσιμες οδηγόντας σε αποδοτικότερους πίνακες δρομολόγησης αλλά θα είναι πιο ακριβό σε ενέργεια και χρόνο να μαζευτούν. Στη δεύτερη περίπτωση έχουμε το αντίστροφο, δηλαδή λιγότερο αξιόπιστο πίνακα δρομολόγησης αλλά είναι πιο φτηνό σε ενέργεια και χρόνο. Το ιδανικό για έναν αλγόριθμο δρομολόγησης μάλλον είναι να αξιοποιούνται τοπικά κριτήρια, τέτοια ώστε να είναι όσο το δυνατό πιο αποδοτικά.

5. **Διαθέσιμες 'Τεχνολογίες ' - Επιλογή Μοντέλου:** Ο σχεδιαστής του αλγορίθμου δρομολόγησης έχει τη δυνατότητα να επιστρατέψει κάθε διαθέσιμη τεχνολογία για τις συσκευές του δικτύου, τουλάχιστον στη σημερινή φάση ανάπτυξης των Ασύρματων Δικτύων Αισθητήρων που δεν είναι διαδεδομένες πρακτικές εφαρμογές και όλα περιγράφονται σε θεωρητική βάση. Οι διαθέσιμες τεχνολογίες περιλαμβάνουν GPS, επιταχυνσιόμετρα, κεραίες που μπορούν να εκτιμούν την κατεύθυνση των εισερχόμενων εκπομπών (direction-sensing antennae), δυνατότητα κίνησης των συσκευών κατά βούληση και μπορούν γενικώς να κάνουν τη ζωή του σχεδιαστή πολύ πιο εύκολη, καθώς δίνουν πολύ χρήσιμες ιδιότητες στις συσκευές που μπορεί να εκμεταλλευτεί ο αλγόριθμος. Στην ανάλυση ενός πρωτοκόλλου οι διαθέσιμες τεχνολογίες περιλαμβάνονται στην περιγραφή του *μοντέλου*. Συνεπώς ο σχεδιαστής καλείται να επιλέξει το μοντέλο πάνω στο οποίο θα υλοποιήσει τον αλγόριθμό του. Ένα ελαστικό μοντέλο, δηλαδή ένα μοντέλο που επιτρέπει τη συνδρομή πολλών από τις παραπάνω τεχνολογίες, μπορεί να οδηγήσει σε εντυπωσιακά πειραματικά αποτελέσματα ενός αλγόριθμου, ωστόσο πιθανόν να είναι μη ρεαλιστικό οπότε να μειώνει την πρακτική αξία του αλγόριθμου, ακόμα και μακροπρόθεσμα. Παρ΄ όλα αυτά οι κεντρικές ιδέες αλγορίθμων που

υλοποιούνται σε ελαστικά μοντέλα μπορούν να έχουν μεγάλη συνεισφορά στην έρευνα των Ασύρματων Δικτύων Αισθητήρων.

6. **Αξιοποίηση Μερικών Γνωστών Τεχνικών Επικαλυπτικά Δέντρα Έκτασης, Κατακερματισμός, Τυχαιότητα):** Οι τεχνικές που θα περιγράψουμε έχουν ευρεία χρήση και έτσι αξίζει να τις περιγράψουμε σύντομα, καθώς θα τις δούμε και παρακάτω.

   - Τα Επικαλυπτικά Δέντρα Εκτασης (spanning trees) ανακαλύπτουν τη συντομότερη διαδρομή προς την απόληξη σε ένα ακίνητο και αξιόπιστο δίκτυο. Η απόληξη 'πλημμυρίζει' (τεχνική flood) το δίκτυο με ένα πακέτο πάνω στο οποίο αναγράφεται η απόσταση από την απόληξη. Κάθε κόμβος του δικτύου αναθέτει ως *πατέρα* του στο δίκτυο τη συσκευή από την οποία έλαβε το πακέτο, θέτει ως απόστασή του από την απόληξή του την απόσταση που αναγράφεται στο πακέτο και προωθεί το πακέτω περεταίρω αυξάνοντας την απόσταση κατά 1. Ο χρόνος που χρειάζεται αυτή η τεχνική είναι $O(\delta)$ όπου δ η διάμετρος του δικτύου. Ακριβώς επειδή τα Ασύρματα Δίκτυα Αισθητήρων δεν είναι αξιόπιστα, και κάποιες φορές δεν είναι ακίνητα, η τεχνική αυτή δεν αρκεί για να λύσει εν γένει το πρόβλημα της δρομολόγησης, αλλά χρησιμοποιείται συχνά ως μέρος ενός γενικότερου αλγόριθμου.
   - Ο κατακερματισμός ενός δικτύου σε υποομάδες αισθητήρων μπορεί να έχει πολύ θετικά αποτελέσματα για έναν αλγόριθμο δρομολόγησης. Πρώτον, μπορεί να απλόποιήσει σημαντικά τη διαδιακασία. Δεύτερον, μπορεί να επιφέρει μείωση της κατανάλωσης ενέργειας καθώς μπορούμε να οδηγήσουμε όλα τα δεδομένα της υποομάδας σε έναν κόμβο ο οποίος να τα συμπιέσει πριν τα στείλει στην απόληξη. Δεδομένου ότι οι εκπομπές καταναλώνουν δεκαπλάσιες ποσότητες ενέργειας από τους υπολογισμούς, η συμπίεση των δεδομένων μπορεί να μειώσει την κατανάλωση.
   - Η χρήση πιθανοτήτων μας επιτρέπει να δρομολογούμε με μια σχετική αξιοπιστία έχοντας άγνοια της πραγματικής τοπολογίας του δικτύου, κάτι που μπορεί να μας γλιτώσει από εκτενείς φάσεις αρχικοποίησης ή επισκευής μονοπατιών.

7. **Κίνηση Συσκευών:** Το στοιχείο της κίνησης στο μοντέλο ενός αλγόριθμου σε γενικές γραμμές εμφανίζεται ως ένα πρόβλημα το οποίο καλούμαστε να αντιμετωπίσουμε. Η επίδραση της κίνησης των συσκευών σε έναν αλγόριθμο δρομολόγησης είναι η δημιουργία καινούριων και η κατάργηση παλιών συνδέσμων ανάμεσα σε συσκευές. Αυτό έχει σαν αποτέλεσμα να πρέπει να 'επισκευαστούν' μονοπάτια τα οποία δεν ισχύουν πλέον, κατάσταση παρόμοια με το σενάριο αποτυχίας κάποιων συσκευών. Επιπλέον, η κίνηση των συσκευών επηρρεάζει όργανα όπως τα GPS και τα επιταχυνσιόμετρα, οι μετρήσεις των οποίων μπορούν να αξιοποιηθούν από τον σχεδιαστή. Μπορούμε όμως να ακολουθήσουμε και άλλες προσεγγίσεις που αντί να βλέπουν την κίνηση ως ένα πρόβλημα προς αντιμετώπιση, την βλέπουν ως ευκαιρία για εξοικονόμηση ενέργειας. Η βασική ιδέα είναι ότι, στην περίπτωση που δεν μας ενδιαφέρει αν η παράδοση των πακέτων έχει καθυστέρηση, αντί να γίνονται πολλές μεταδόσεις κατά μήκος ενός μεγάλου μονοπατιού από την αφετηρία στον προορισμό, να περιμένουμε να έρθουν πιο κοντά η αφετηρία με τον προορισμό λόγω της κίνησης και άρα να χρειάζονται λιγότερες μεταδόσεις εξοικονομώντας ενέργεια.

Σε αυτό το σημείο, και αφού έχουμε αναλύσει τα βασικά κριτήρια γύρω από τα οποία πραγματοποιείται ο σχεδιασμός ενός αλγορίθμου δρομολόγησης, θα παρουσιάσουμε μια περίληψη των πρωτοκόλλων που πραγματεύεται η παρούσα διπλωματική εργασία:

Δέντρα BFS και DFS

Τα Δέντρα Αναζήτησης Προτεραιότητας κατά Πλάτος (BFS Trees) και τα Δέντρα Αναζήτησης Προτεραιότητας κατά Βάθος (DFS Trees) είναι απλοί αλγόριθμοι οι οποίοι δεν αρκούν για να λύσουν εξ ολοκλήρου το πρόβλημα της δρομολόγησης. Μπορούν, λόγω της απλότητάς τους να περιλαμβάνονται ως μέρη ενός γενικότερου αλγόριθμου. Για παράδειγμα, θα μπορούσε ένα πρωτόκολλο δρομολόγησης να δημιουργεί ένα επικαλυπτικό δέντρο αναζήτησης προτεραιότητας κατά πλάτος και έπειτα να προσπαθεί να προσαρμόζεται στις αλλαγές του δικτύου (αποτυχίες κόμβων, κίνηση, κλπ). Επειδή είναι απλές τεχνικές και όχι ολοκληρωμένα πρωτόκολλα, δεν γίνονται πειραματικές αξιολογήσεις.

LEACH

Το LEACH είναι ένα πρωτόκολλο αντιπροσωπευτικό για τα Ασύρματα Δίκτυα Αισθητήρων με την έννοια ότι αναδεικνύει τις διαφορές που υπάρχουν μεταξύ δρομολόγησης στα Αδόμητα Δίκτυα και δρομολόγησης στα Ασύρματα Δίκτυα Αισθητήρων. Επιπλέον, είναι αντιπροσωπευτικό με την έννοια ότι παρ΄ όλο που χρησιμοποιεί ένα ελαστικό μοντέλο, η συνεισφορά του στην έρευνα είναι πολύ σημαντική καθώς η βασική του προσέγγιση μπορεί να εφαρμοστεί και σε πραγματικές συνθήκες. Το LEACH χρησιμοποιεί το μονέλο της απευθείας επικοινωνίας και η εκτέλεσή του γίνεται σε γύρους. Σε κάθε γύρο το δίκτυο χωρίζεται σε συστάδες οι οποίες συγκεντρώνουν τα δεδομένα στους επικεφαλής των συστάδων οι οποίοι με τη σειρά τους τα στέλνουν στην/στις απόληξη/απολήξεις. Στον επόμενο γύρο επαναπροσδιορίζονται οι συστάδες κοκ. Ο προσδιορισμός των συστάδων γίνεται με πιθανοτικό τρόπο, δηλαδή στην αρχή κάθε γύρου, κάθε αισθητήρας 'αυτοεκλέγεται' ως επικεφαλής συστάδας χρησιμοποιόντας κάποια πιθανότητα (στον πρώτο γύρο η πιθανότητα αυτή είναι $\frac{1}{\vartheta}$ όπου ϑ είναι το ιδανικό πλήθος των αισθητήρων για μια συστάδα). Κατόπιν, οι αισθητήρες επιλέγουν να ενταχθούν στη συστάδα της οποίας ο επικεφαλής βρίσκεται πιο κοντά. Σε κάθε συστάδα καθορίζεται η χρονική περίοδος κατά την οποία κάθε αισθητήρας θα εκπέμψει προκειμένου να αποφευχθούν οι συγκρούσεις και, τέλος, γίνεται η μετάδοση των δεδομένων από τους αισθητήρες στους επικεφαλής των συστάδων και από τους τελευταίους στην/στις απόληξη/απολήξεις. Η πειραματική αξιολόγησης του LEACH δείχνει εντυπωσιακή μείωση της κατανάλωσης ενέργειας και καλύτερη κατανομή της κατανάλωσης σε σχέση με άλλους πιο απλούς αλγόριθμους.

Directed Diffusion

Το Directed Diffusion είναι ένα ακόμα αντιπροσωπευτικό πρωτόκολλο καθώς επίσης αναδεικνύει τις διαφορές της δρομολόγησης στα Ασύρματα Δίκτυα Αισθητήρων από τα Αδόμητα Δίκτυα. Το μοντέλο εδώ είναι πιο ρεαλιστικό και περιλαμβάνει επικοινωνία μέσω πολλαπλών ενδιάμεσων κόμβων. Η βασική λειτουργία περιλαμβάνει την αποστολή ενός ερωτήματος μέσω της απόληξης το οποίο διαχέεται στο δίκτυο και έπειτα οι αισθητήρες τους οποίους αφορά το ερώτημα δρομολογούν τα δεδομένα πίσω στην απόληξη. Το κριτήριο για την επιλογή του επόμενου κόμβου στη διαδρομή προς την απόληξη είναι η ποιότητα των συνδέσμων.

Χρησιμοποιόντας τον βασικό μηχανισμό εισάγονται τεχνικές οι οποίες εμπλέκουν όσο το δυνατόν λιγότερες συσκευές στη δρομολόγηση για να μειωθεί η κατανάλωση της ενέργειας και βρίσκουν εναλλακτικές διαδρομές σε περιπτώσεις αποτυχίας κόμβων. Η πειραματική αξιολόγηση του Directed Diffusion δείχνει σημαντική βελτίωση της κατανάλωσης σε σχέση με άλλους πιο απλούς αλγόριθμους.

Probabilistic Forwarding Routing (PFR)

Το συγκεκριμένο πρωτόκολλο χρησιμοποιεί ένα ελαστικό μοντέλο και έχει σκοπό να δείξει ότι υπάρχει η δυνατότητα για αποτελεσματική δρομολόγηση με κριτήρια πιθανότητας. Η βασική ιδέα έχει ως εξής: όταν ένας αισθητήρας καλείται να προωθήσει ένα πακέτο, εξετάζει την γωνία από την οποία έλαβε το πακέτο και τη γωνία που βρίσκεται η απόληξη και έτσι ξέρει πόσο κοντά βρίσκεται στην γραμμή που ενώνει την πηγή του μηνύματος με την απόληξη. Μετά αποφασίζει αν θα το προωθήσει περεταίρω με βάση κάποια πιθανότητα η οποία είναι μεγαλύτερη όσο πιο κοντά είναι ο αισθητήρας σε αυτήν την γραμμή.

Πρωτόκολλα με Παρουσία Πολλαπλών Κινητών Απολήξεων

Τα συγκεκριμένα πρωτόκολλα καλούνται να αποδείξουν αυτό που αναφέραμε παραπάνω, ότι δηλαδή η κίνηση αντί να αποτελεί πρόβλημα, μπορεί να αξιοποιθεί προκειμένου να μειωθεί η κατανάλωση. Παρουσιάζονται τρία πρωτόκολλα: Στο πρώτο υποθέτουμε ότι οι απολήξεις πραγματοποιούν μια επαναλαμβανόμενη διαδρομή έτσι ώστε περιοδικά όλοι οι αισθητήρες να βρίσκονται εντός εμβέλειας της απόληξης για ένα χρονικό διάστημα στο οποίο στέλνουν τα δεδομένα τους με απλές εκπομπές χαμηλής ενέργειας. Στο δεύτερο, οι απολήξεις κινούνται τυχαία αλλά έχουν τη δυνατότητα να αλλάξουν τη διαδρομή τους. Όταν επισκευτούν έναν αισθητήρα τον οποίον έχει επισκευτεί πρόσφατα μια άλλη απόληξη, τότε αλλάζει κατεύθυνση. Στο τρίτο, οι αισθητήρες χωρίζονται σε συστάδες με παρόμοιο τρόπο όπως και στο LEACH προσπαθώντας οι συστάδες να έχουν το ίδιο *βάρος* (ποσότητα η οποία αναπαριστά την αναμενόμενη ποσότητα παραγόμενων δεδομένων). Κατόπιν οι απολήξεις ανατίθενται στις συστάδες μία προς μία και κινούνται εντός των συστάδων τους (και σε αυτό το πρωτόκολλο έχουν ελευθερία κίνησης) συλλέγοντας τα δεδομένα. Έπειτα από πειραματικές αξιολογήσεις αποδεικνύεται το ζητούμενο, ότι δηλαδή το πρωτόκολλο λειτουργεί και ότι υπάρχει ένα *παζάρι* (trade-off) μεταξύ μείωσης κατανάλωσης και καθυστέρησης.

1.2.2 Η Ασφάλεια

Στα διάφορα σενάρια εφαρμογών των Ασύρματων Δικτύων Αισθητήρων, ένας παράγοντας που εισάγεται είναι η ασφάλεια. Τα δεδομένα που διακινούνται εντός του δικτύου μπορεί να ενδιαφέρουν και κάποιον άλλον πέρα από τον διαχειριστή του δικτύου ή μπορεί κάποιος να έχει όφελος αν ένα Ασύρματο Δίκτυο Αισθητήρων δεν μπορεί να λειτουργεί. Μας ενδιαφέρει λοιπόν να μπορέσουμε να προφυλάξουμε το δίκτυό μας από κακόβουλες εξωτερικές παρεμβολές που στόχο έχουν να υποκλέψουν πληροφορίες ή να εμποδίσουν τη λειτουργία του δικτύου.

Σε ένα παραδοσιακό δίκτυο, ο παράγοντας της Ασφάλειας στα πρωτόκολλα δρομολόγησης εξαντλείται στο να είναι μονίμως εφικτή η επικοινωνία μεταξύ δύο συσκευών του δικτύου ενώ η κρυπτογράφηση, η αυθεντικότητα και η ακεραιότητα των πληροφοριών εξασφαλίζεται από ανώτερα επίπεδα, πχ μέσω εφαρμογών SSH ή SSL. Στα Ασύρματα Δίκτυα Αισθητήρων

τα πράγματα είναι πολύ διαφορετικά. Όπως αναλύσαμε, δεν συνηθίζεται να πραγματοποιούνται συνεδρίες μεταξύ συσκευών αλλά όλοι οι αισθητήρες στέλνουν πληροφορίες στην απόληξη, οπότε οι ίδιες συσκευές που παίζουν το ρόλο του δρομολογητή είναι και αυτές που παράγουν πληροφορία. Συνεπώς η ασφάλεια πρέπει να υλοποιείται στο πρωτόκολλο δρομολόγησης.

Το ζήτημα της Ασφάλειας αποκτάει ιδιαίτερο ενδιαφέρον στα Ασύρματα Δίκτυα Αισθητήρων αν αναλογιστούμε τις ιδιαίτερες συνθήκες που επικρατούν. Το γεγονός ότι η επικοινωνία γίνεται ασύρματα και ότι τα δίκτυα αυτά συνήθως πρέπει να λειτουργούν για μεγάλα χρονικά διαστήματα χωρίς ανθρώπινη αλληλεπίδραση παρέχει ευνοϊκό περιβάλλον έτσι ώστε μια συσκευή να εισέλθει στο χώρο που είναι τοποθετημένο το δίκτυο και να αλληλεπιδράσει με αυτό. Επιπλέον, οι περιορισμένοι υπολογιστικοί και τηλεπικοινωνιακοί πόροι των συσκευών ενός Ασύρματου Δικτύου Αισθητήρων καθιστούν πολύ δύσκολο να εφαρμοστούν συνηθισμένοι αλγόριθμοι κρυπτογραφίας και πιστοποίησης αυθεντικότητας, ειδικά αν αναλογιστούμε ότι η συσκευή που επιτίθεται ενδεχομένως να είναι και αρκετές τάξεις μεγέθους ισχυρότερη όσον αφορά τους πόρους.

Συγκεντρωμένα, τα κριτήρια γύρω από τα οποία κινείται η σχεδίαση της ασφάλειας στα Ασύρματα Δίκτυα Αισθητήρων είναι τα εξής:

1. **Τύποι Επιθέσεων:** Δεν θα επεκταθούμε με λεπτομέρεια στους τύπους των επιθέσεων καθώς αφιερώνουμε ολόκληρο κεφάλαιο στη συνέχεια. Σε αυτό το σημείο θα αναφερθούμε στους στόχους που μπορεί να έχουν οι επιτιθέμενοι και σε κάποιες κατηγοριοποιήσεις των επιθέσεων. Ο στόχος ενός επιτιθέμενου μπορεί να είναι η υποκλοπή δεδομένων, η εισαγωγή ψεύτικων δεδομένων έτσι ώστε ο διαχειριστής να τα εισπράξει σαν 'νόμιμα' ή η παρεμπόδιση της λειτουργίας του δικτύου. Οι επιτιθέμενοι διακρίνονται αφενός σε χαμηλών πόρων (mote-class attackers) και υψηλών πόρων (laptop-class attackers) και αφετέρου σε εξωτερικούς και εσωτερικούς επιτιθέμενους. Οι εξωτερικοί επιτιθέμενοι είναι συσκευές που είναι στον χώρο του δικτύου χωρίς να γνωρίζουν το περιεχόμενο των μνημών των αισθητήρων ενώ οι εσωτερικοί επιτιθέμενοι έχουν *καταλάβει* κάποια συσκευή του δικτύου και έχουν αντιγράψει το περιεχόμενο της μνήμης της. Ο σχεδιαστής κάποιου ασφαλούς αλγόριθμοι πρέπει να εξετάζει τη λειτουργία του δικτύου και από τη σκοπιά του επιτιθέμενου προκειμένου να εξασφαλίσει την ασφάλειά του σε κάθε περίπτωση.

2. **Μαθηματικά Εργαλεία:** Η παρούσα Διπλωματική εργασία δεν αναλύει σε βάθος τα διαθέσιμα μαθηματικά εργαλεία κρυπτογραφίας και ασφάλειας, ωστόσο τον σχεδιαστή και υλοποιητή ενός ασφαλούς αλγόριθμου πρέπει να τον απασχολήσουν. Ειδικά για τα Ασύρματα Δίκτυα Αισθητήρων, όπου οι συσκευές είναι χαμηλών υπολογιστικών πόρων, η επιλογή μαθηματικών εργαλείων χαμηλών υπολογιστικών απαιτήσεων είναι καθοριστικής σημασίας. Για αυτόν τον λόγο στην παρούσα μελέτη χρησιμοποιούνται οι Ελλειπτικές Καμπύλες οι οποίες είναι πειραματικά αποδεδειγμένο ότι απαιτούν λίγους υπολογιστικούς πόρους.

3. **Συνδυασμός Ασφάλειας - Δρομολόγησης:** Όπως εξηγήσαμε, στα Ασύρματα Δίκτυα Αισθητήρων οι μηχανισμοί της ασφάλειας δεν μπορούν να υλοποιηθούν σε ανώτερα επίπεδα αλλά μόνο στο επίπεδο δικτύου, οπότε ο σχεδιαστής ενός ασφαλούς αλγόριθμου πρέπει να επικεντρώσει την προσπάθειά του να υλοποιήσει με ασφαλή

τρόπο τον μηχανισμό της δρομολόγησης. Επιπλέον, η δρομολόγηση είναι το πιο ευάλωτο σημείο σε έναν επιτιθέμενο να παρεμποδίσει τη λειτουργία του δικτύου αν όχι και να υποκλέψει δεδομένα.

4. **Κίνηση:** Η κίνηση παίζει πολύ σημαντικό ρόλο στα Ασύρματα Δίκτυα Αισθητήρων καθώς, αν επιθυμούμε δύο νόμιμες συσκευές του δικτύου να μπορούν ανά πάσα στιγμή να δημιουργήσουν ένα ασφαλές κανάλι μεταξύ τους, αυτό αφήνει *παράθυρα* για έναν επιτιθέμενο να δημιουργήσει και αυτός κανάλι επικοινωνίας και έτσι να ενταχθεί στο δίκτυο ως 'νόμιμο μέλος '. Η κατάσταση γίνεται ακόμα πιο δύσκολη στην περίπτωση των εσωτερικών επιτιθέμενων καθώς δεν υπάρχει τρόπος να εξακριβώσουμε εαν μια πρωτοεμφανιζόμενη συσκευή στη γειτονά ενός αισθητήρα είναι νόμιμος αισθητήρας η ξένη συσκευή.

Στα πλαίσια της ανάλυσης του ζητήματος της ασφάλειας στα Ασύρματα Δίκτυα Αισθητήρων, στην παρούσα διπλωματική εργασία εξετάζουμε τα παρακάτω θέματα:

Βασικά Μοντέλα Κρυπτογραφίας

Εξετάζουμε μερικές βασικές και ευρέως διαδεδομένες τεχνικές κρυπτογραφίας σε γενικό πλαίσιο, δηλαδή όχι για Ασύρματα Δίκτυα Αισθητήρων ή Αδόμητα Δίκτυα. Το περιβάλλον συνήθως περιγράφεται αφηρημένα ως ένας *χώρος* με *χρήστες* οι οποίοι επικοινωνούν μεταξύ τους. Σε ένα τέτοιο περιβάλλον εξετάζουμε τα πρωτόκολλα Δημοσίου Κλειδιού, Ιδιωτικού Κλειδιού, Ψηφιακές Υπογραφές και το Πρόβλημα Diffie-Hellman.

Τύποι Επιθέσεων

Εξετάζουμε ζητήματα ασφάλειας που ειδικεύονται στα Ασύρματα Δίκτυα Αισθητήρων, κατηγοριοποιούμε τους επιτιθέμενους ανάλογα με τις ιδιότητές τους και κάνουμε αναλυτική παρουσίαση γνωστών επιθέσεων σε Ασύρματα Δίκτυα Αισθητήρων

Ελλειπτικές Καμπύλες

Παρουσιάζουμε το μαθηματικό μοντέλω των Ελλειπτικών Καμπύλων και κάποιες εφαρμογές του. Αρχικά παραθέτουμε κάποια εισαγωγικά στοιχεία σχετικά με το μαθηματικό σκέλος και έπειτα την εφαρμογή των Ελλειπτικών Καμπύλων στη λύση του προβλήματος Diffie-Hellman, του GDH (Diffie-Hellman Group Key Establishment) στην περίπτωση εικονικού δακτυλίου και του GDH στην περίπτωση γενικού δικτύου. Οι εφαρμογές των Ελλειπτικών Καμπύλων που παρουσιάζουμε χρησιμοποιούνται και στην δική μας προσέγγιση για τη δρομολόγηση και την ασφάλεια.

Δημιουργία Ασφαλούς Δέντρου Επικοινωνίας

Τέλος, ως παράδειγμα ολοκληρωμένης αλγοριθμικής πρότασης παρουσιάζουμε ένα ολοκληρωμένο πρωτόκολλο ασφάλειας. Στόχος του πρωτοκόλλου είναι η δημιουργία ενός Δέντρου Αναζήτησης Προτεραιότητας κατά Πλάτος με τέτοιον τρόπο ώστε να μην είναι δυνατό να εκδηλωθούν επιθέσεις ή στην περίπτωση των εσωτερικών επιθέσεων (που δεν μπορούν να αποφευχθούν πλήρως) να έχουν πολύ περιορισμένη επίδραση. Στο μοντέλο του πρωτόκολλου δεν περιλαμβάνεται κίνηση. Αρχικά οι συσκευές δημιουργούν ασφαλή κανάλια επικοινωνίας μεταξύ

τους με μια τεχνική με την οποία καμία νεοφερμένη συσκευή να μην μπορεί να συμμετάσχει. Αυτό προϋποθέτει μια χρονική περίοδο στην έναρξη του πρωτοκόλλου όπου θεωρούμε ότι το δίκτυο δεν απειλείται από επιθέσεις. Κατόπιν παρουσιάζει τον τρόπο με τον οποίον δημιουργείται το Δέντρο αποτρέποντας κάθε επίθεση. Τέλος, προτείνονται τρόποι για την ένταξη στο δίκτυο νεοφερμένων *νόμιμων* συσκευών αποκλείοντας παράλληλα την ένταξη νεοφερμένων *παράνομων* συσκευών.

1.3 Συνεισφορά της Διπλωματικής Εργασίας

Η παρούσα διπλωματική εργασία έγινε με στόχο να παρουσιάσει ένα καινούριο προτινόμενο πρωτόκολλο το οποίο ονομάζεται APSR (Adaptive Probabilistic Secure Routing Protocol, Προσαρμοστικό Πιθανοτικό Ασφαλές Πρωτόκολλο Δρομολόγησης). Η παρουσίαση άλλων προσεγγίσεων στα προβλήματα της δρομολόγησης και ασφάλειας έγινε με στόχο την εξοικείωση του αναγνώστη με βασικά προβλήματα που αντιμετωπίζει ο σχεδιαστής καθώς και με κάποιες τεχνικές που χρησιμοποιούνται.

Το πρωτόκολλο υποστηρίζει κίνηση τόσο των αισθητήρων όσο και της απόληξης. Υποστηρίζει βέλτιστη δρομολόγηση προς την απόληξη αλλά διαθέτει την υποδομή και για κάθε άλλου είδους δρομολόγηση. Η συντήρηση των πληροφοριών που διατηρούν οι κόμβοι για τη δρομολόγηση και ασφάλεια συλλέγονται σε τοπικό επίπεδο και απαιτούν χαμηλούς πόρους. Η εκτέλεσή του διακρίνεται σε τρεις φάσεις: τη φάση αρχικοποίησης, τη φάση δρομολόγησης και τεχνικές προσαρμογής σε μεταβαλλόμενες συνθήκες:

- Η φάση αρχικοποίησης περιλαμβάνει με τη σειρά της τέσσερις φάσεις. Αρχικά, το δίκτυο οργανώνεται σε κυκλικές περιοχές γύρω από την απόληξη τις οποίες ονομάζουμε στρωματώσεις (layers) τα οποία χαρακτηρίζονται από την απόσταση των αισθητήρων από την απόληξη. Κατόπιν, κάθε στρωμάτωση χωρίζεται σε τομείς και σε κάθε τομέα δημιουργείται ένα ομαδικό κλειδί κρυπτογραφίας. Έπειτα, οι γειτονικοί τομείς δημιουργούν διατομεακά κλειδιά και, τέλος, οι διάφοροι τομείς αποκτούν μια κοινή αίσθηση προσανατολισμού προκειμένου να μπορούν να δρομολογούν 'δεξιόστροφα' ή 'αριστερόστροφα'.

- Έχοντας υλοποιήσει όλη αυτή την υποδομή είμαστε σε θέση να δρομολογήσουμε πακέτα από και προς κάθε κατεύθυνση αρκεί να γνωρίζουμε την στρωμάτωση και τον τομέα όπου βρίσκεται ο προορισμός. Η περίπτωση είναι ξεκάθαρη στην περίπτωση της απόληξης η οποία βρίσκεται στην '*κατώτερη*' στρωμάτωση. η λογική είναι ότι το πακέτο ταξιδεύει πρώτα 'προς τα μέσα' ή 'προς τα έξω' μέχρι να φτάσει την κατάλληλη στρωμάτωση και έπειτα 'δεξιόστροφα' ή 'αριστερόστροφα' μέχρι να βρει τον προορισμό. Οι υποψήφιες συσκευές για προώθηση είναι καθορισμένες από τη φάση αρχικοποίησης. Επιπλέον, περιγράφεται και ένας πιθανοτικός μηχανισμός με τον οποίον ενεργοποιείται για την προώθηση μόνο μία συσκευή (ιδανικά) με τέτοιον τρόπο ώστε να έχουμε την ελάχιστη δυνατή κατανάλωση, να έχουμε την καλύτερη δυνατή κατανομή κατανάλωσης και να μειώνουμε την εμπιστοσύνη σε κινούμενες συσκευές.

- Οι διορθωτικές κινήσεις για την περίπτωση μετακίνησης της απόληξης περιλαμβάνουν αρχικά τον επαναπροσανατολισμό του μηχανισμού δρομολόγησης προς την απόληξη, όταν η απόληξη μετακινηθεί αρκετά κάνοντας την προηγούμενη διαδικασία ασύμφορη τον ορισμό ενός τομέα ως *προσωρινή απόληξη* ο οποίος αποθηκεύει τα δεδομένα

που κανονικά προορίζονται προς την απόληξη και, τέλος, όταν ολοκληρωθεί η κίνηση της απόληξης την επαναναρχικοποίηση του πρωτόκολλου. Για την περίπτωση όπου μετακινείται ένας αισθητήρας έχουμε τους κατάλληλους μηχανισμούς έτσι ώστε να αποκτά τα απαραίτητα κλειδιά του καινούριου τομέα στον οποίον έχει μετακινηθεί.

Κεφάλαιο 2

Το Πρόβλημα της Δρομολόγησης

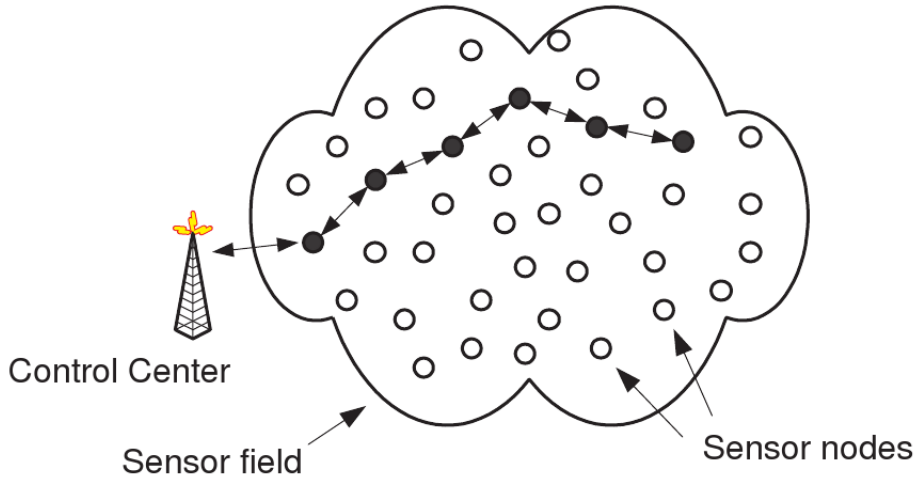
Στο παρόν κεφάλαιο εξετάζουμε κάποια πρωτόκολλα που θεωρούμε ότι είναι αντιπροσωπευτικά ως προς τη δρομολόγηση στα Ασύρματα Δίκτυα Αισθητήρων. Αρχικά παρουσιάζουμε δύο τεχνικές δημιουργίας επικαλλυπτικών δέντρων, έπειτα παρουσιάζουμε το LEACH, ένα πρωτόκολλο που χωρίζει το δίκτυο σε συστάδες και συλλέγει τις πληροφορίες από τις συστάδες μέσω απευθείας μεταδόσεων, στη συνέχεια παρουσιάζουμε το Directed Diffusion, ένα πρωτόκολλο που θέτει ερωτήματα στο δίκτυο και κατόπιν επιλέγεται η καλύτερη διαδρομή για δρομολόγηση προς την απόληξη με βάση την ποιότητα των συνδέσμων και με βάση μόνο τοπικά κριτήρια, κατόπιν παρουσιάζουμε το PFR ένα πρωτόκολλο που κάθε συσκευή που καλείται να προωθήσει ένα πακέτο κάνει την επιλογή του βάσει πιθανότητας και βάσει γεωγραφικών παραμέτρων και, τέλος, παρουσιάζουμε τρια πρωτόκολλα που αξιοποιούν την κίνηση των απολήξεων προκειμένου να μειώσουν την κατανάλωση ενέργειας.

2.1 Αλόριθμοι Διάτρεξης Δέντρου - Η Εφαρμογή στα Ασύρματα Δίκτυα Αισθητήρων

2.1.1 Οι Αλγόριθμοι Διάτρεξης BFS και DFS σε Δέντρα

Θα μας απασχολήσουν δύο αλγόριθμοι διάτρεξης δέντρου, η αναζήτηση προτεραιότητας κατά πλάτος (BFS, Breadth-First Search) και η αναζήτηση προτεραιότητας κατά βάθος (DFS, Depth-First Search). Το πρόβλημα της διάτρεξης δέντρου έγκειται στην καταγραφή σε μια λίστα όλων των κόμβων ενός δέντρου με σειρά που βασίζεται σε κάποια λογική. Η αναζήτηση προτεραιότητας κατά πλάτος δημιουργεί μια λίστα με πρώτο στοιχείο τη ρίζα του δέντρου, στη συνέχεια όλους τους κόμβους που έχουν ύψος 1 με οποιανδήποτε σειρά, στη συνέχεια όλους τους κόμβους που έχουν ύψος 2 με οποιαδήποτε σειρά, κ.ο.κ. Η αναζήτηση προτεραιότητας κατά βάθος επιτυγχάνεται από τον ακόλουθο αναδρομικό αλγόριθμο:

```
Search(x) {
1. Add x to the output list
2. Create a list l=[l1,l2,...,ln] containing the children of x
3. Until l is empty {
4.       a=pop(l)
5.       Search(a)
6. } return
```



Σχήμα 2.1: Δρομολόγηση στα Ασύρματα Δίκτυα Αισθητήρων

```
}

DFS(tree) {
1. Search(root of tree)
}
```

2.1.2 Δημιουργία Επικαλλυπτικών BFS και DFS Δέντρων

Οι παραπάνω αλγόριθμοι διάτρεξης (ή οι παραπάνω λογικές) μπορούν να εφαρμοστούν σε ένα Ασύρματο Δίκτυο Αισθητήρων προκειμένου να δημιουργηθεί ένα δέντρο με ρίζα την απόληξη το οποίο θα μπορεί να χρησιμοποιηθεί έτσι ώστε να δρομολογούνται πακέτα πληροφορίας από τους αισθητήρες προς την απόληξη. Ο στόχος μας είναι να ορίσει κάθε αισθητήρας μια μεταβλητή *parent* η οποία θα αντιστοιχεί στην ταυτότητα του επόμενου κόμβου στην διαδρομή προς την απόληξη.

Δημιουργία BFS δέντρου:

Κάθε αισθητήρας έχει μια μεταβλητή *parent* η οποία αρχικά δεν έχει τιμή και μια μεταβλητή *distance* η οποία αρχικά έχει τιμή ∞. Όταν ξεκινάει ο αλγόριθμος η απόληξη εκπέμπει ένα μήνυμα $SEARCH < sinkID, 0 >$. Από εκεί και πέρα κάθε αισθητήρας εκτελεί τον εξής αλγόριθμο:

```
1. While(true) {
2.       Wait for a SEARCH message
3.       Read the message: SEARCH<ID,d>
4.       If d < distance-1 then {
5.         Set parent = ID
6.         Set distance = d+1
7.         Transmit a SEARCH<myID, distance> message
         }
   }
```

Με αυτόν τον τρόπο κάθε αισθητήρας θα έχει θέσει μια τιμή στην μεταβλητή *parent* που θα αντιστοιχεί στον σταθμό όπου θα απευθύνεται ένα πακέτο όταν ο αισθητήρας θα

προσπαθεί να δρομολογήσει προς την απόληξη. Κάθε διαδρομή που θα ακολουθείται με αυτόν τον τρόπο θα είναι και ελάχιστου μήκους.

Δημιουγία DFS Δέντρου:

Ο στόχος εδώ είναι πάλι να ανατεθεί μια τιμή στη μεταβλητή *parent* σε κάθε αισθητήρα. Η λογική είναι ότι κυκλοφορεί ένα token σε όλους του κόμβους του δικτύου. Τα μηνύματα που χρησιμοποιούμε είναι τα $SEARCH$, $PARENT$, $BEACON$ και $BEACON\_REPLY$. Όταν ένας αισθητήρας ή η απόληξη στέλνει το μήνυμα $BEACON$, όλες οι συσκευές που το ακούνε απαντάνε με το $BEACON\_REPLY < ID, joined >$ όπου ID είναι η ταυτότητά τους και $joined$ μια boolean μεταβλητή που υποδηλώνει εαν έχουν θέσει τιμή στη μεταβλητή *parent* και συνεπώς εαν συμμετέχουν στο δέντρο. Ο αλγόριθμος για τους αισθητήρες είναι ο εξής:

```
1.Wait for a SEARCH message
2.Read the message: SEARCH<ID>
3.Set parent = ID
4.Send a BEACON message and wait for the replies
5.While there is at least one BEACON_REPLY with joined=false {
6. Choose a node with joined=false and send a SEARCH<myID> message
7. Wait for a PARENT message
8. Send a BEACON message and wait for the replies
9.} Send a PARENT message to the node with ID = parent
```

Η απόληξη απλώς διαλέγει ένα γειτονικό του κόμβο και του στέλνει το μήνυμα $SEARCH < sinkID >$.

Αυτοί οι αλγόριθμοι είναι αρκετά απλοί και εύκολοι στην υλοποίηση και σε ένα ευνοϊκό περιβάλλον υλοποιούν τους στόχους της δρομολόγησης, δηλαδή χρησιμοποιώντας τα δέντρα που προκύπτουν, κάθε αισθητήρας μπορεί να δρομολογήσει πακέτα πληροφορίας προς την απόληξη. Παρ' όλα αυτά, τα Ασύρματα Δίκτυα Αισθητήρων όπως έχουμε πει συνήθως δεν παρέχουν ένα ευνοϊκό περιβάλλον. Αν ένας αισθητήρας σβήσει για οποιονδήποτε λόγο, τότε όλα το υπόδεντρο αυτού του αισθητήρα δεν θα είναι σε θέση να δρομολογήσει πακέτα. Παρ' όλα αυτά, οι παραπάνω αλγόριθμοι έχουν μεγάλη αξία καθώς χρησιμοποιούνται ως κομμάτια άλλων αλγορίθμων.

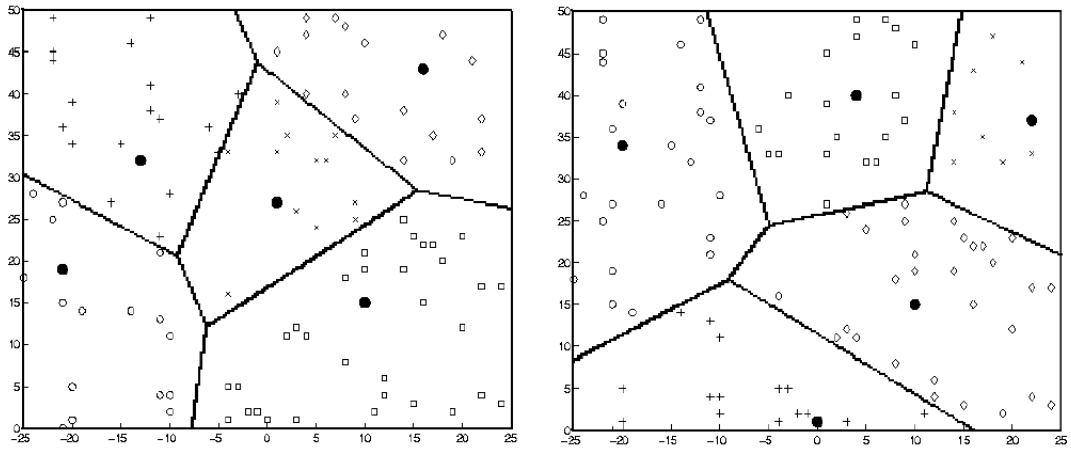
2.2 Ένα Ιεραρχικό Πρωτόκολλο Δρομολόγησης

Ένα πολύ βασικό και αντιπροσωπευτικό πρωτόκολλο για Ασύρματα Δίκτυα Αισθητήρων είναι το LEACH [14]. Ο λόγος για τον οποίον θεωρούμε ότι αυτό το πρωτόκολλο είναι αντιπροσωπευτικό είναι ότι αναδεικνύει τους ιδιαίτερους στόχους που πρέπει να έχει και τις συνθήκες που έχει να αντιμετωπίσει ένα πρωτόκολλο δρομολόγησης σε Ασύρματα Δίκτυα Αισθητήρων.

Όταν στο εξής θα περιγράφουμε το μοντέλο ενός πρωτοκόλλου θα εννοούμε ότι θα εξηγούμε τις συνθήκες που θα επικρατούν στο περιβάλλον, ποιες υποθέσεις δεχόμαστε ότι θα ισχύουν στο δίκτυο και ποιες υποθέσεις δεχόμαστε όσον αφορά το πώς περιμένει ο διαχειριστής του δικτύου να ανταπεξέλθει το πρωτόκολλο.

2.2.1 Το Μοντέλο Λειτουργίας

Το μοντέλο του LEACH, λοιπόν, περιλαμβάνει τα εξής:



Σχήμα 2.2: Δυναμική Ρύθμιση των συστάδων στο LEACH

- Το μοντέλο επικοινωνίας είναι η απευθείας επικοινωνία και όχι την επικοινωνία μέσω πολλαπλών ενδιάμεσων κόμβων, δηλαδή η εμβέλεια εκπομής δεν είναι σταθερή αλλά κάθε αισθητήρας μπορεί να επιλέξει με τι ισχύ θα εκπέμψει ένα πακέτο και η εμβέλεια εκπομπής είναι συνάρτηση της ισχύος αυτής.

- Οι αισθητήρες είναι σε θέση να μετρήσουν την ισχύ μιας εισερχόμενης εκπομπής οπότε και να έχουν μια εκτίμηση για την σχετική απόσταση της συσκευής που πραγματοποίησε την εκπομπή. Μετρώντας την ισχύ ενός εισερχόμενου πακέτου, ένας αισθητήρας είναι σε θέση να εκτιμήσει την ισχύ που πρέπει να επιστρατέψει το ίδιο προκειμένου να στείλει ένα πακέτο πίσω στον αρχικό αποστολέα. Αυτό μπορεί να επιτευχθεί αν στα πακέτα αναγράφεται η αρχική ισχύς εκπομπής οπότε ο αισθητήρας/παραλήπτης μπρορεί να την συγκρίνει με την ισχύ της εκπομπής στο σημείο του παραλήπτη και να εκτιμήσει την απαραίτητη ισχύ για μια απάντηση.

- Η συλλογή πληροφοριών από τους αισθητήρες γίνεται περιοδικά, δηλαδή ανά τακτά χρονικά διαστήματα κάθε αισθητήρας συλλέγει πληροφορίες για το περιβάλλον τις οποίες επιθυμεί να προωθήσει στην απόληξη.

- Ενδεχομένως να υπάρχουν πολλές απολήξεις στο δίκτυο. Για ένα πακέτο δε μας ενδιαφέρει σε ποια απόληξη θα καταλήξει αλλά θα θεωρήσουμε ότι μέσω κάθε απόληξης η πληροφορία θα φτάσει στον διαχειριστή ισοδύναμα. Επιπλέον, κάθε αισθητήρας στο δίκτυο είναι σε θέση να γνωρίζει την ισχύ που πρέπει να επιστρατέψει προκειμένου να στείλει ένα πακέτο στην πλησιέστερη απόληξη.

2.2.2 Το Πρωτόκολλο

Η βασική ιδέα είναι ότι το δίκτυο χωρίζεται σε συστάδες (clusters), με κάθε συστάδα να διαθέτει ένας αισθητήρας που θα έχει αναλάβει το ρόλο του επικεφαλής συστάδας. Κατόπιν κάθε επικεφαλής συστάδας συλλέγει της πληροφορίες από κάθε αισθητήρα που βρίσκεται

εντός της συστάδας, τις συμπιέζει και τις στέλνει απ΄ ευθείας στην απόληξη. Αυτή η διαδικασία επαναλαμβάνεται ανά γύρους προκειμένου να εναλάσσονται οι επικεφαλής συστάδας οι οποίοι καταναλώνουν περισσότερη ενέργεια σε σχέση με τους υπόλοιπους αισθητήρες.

Ο κάθε γύρος περιλαμβάνει τρεις φάσεις:

α)Καθορισμός επικεφαλής συστάδων - φάση διαφήμησης

β)Ρύθμιση των συστάδων

γ)συλλογή μηνυμάτων και αποστολή στην/στις απόληξη/απολήξεις

Κατά την πρώτη φάση κάθε αισθητήρας επιλέγει να αυτοεκλεχθεί ως επικεφαλής συστάδας χρησιμοποιώντας μια πιθανότητα:

$$T(n) = \begin{cases} \frac{P}{1-p\cdot(r\cdot mod\frac{1}{P})} & , \quad if\ n \in G \\ 0 & , \quad otherwise \end{cases}$$

όπου

P: το επιθυμητό ποσοστό των επικεφαλής συστάδων

r: ο τρέχων γύρος

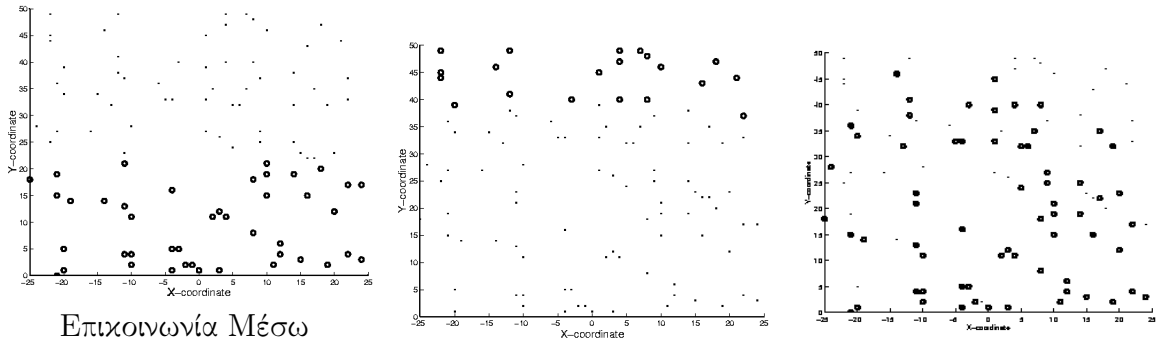
G: το σύνολο των αισθητήρων που δεν έχουν γίνει επικεφαλής συστάδων στους τελευταίους $\frac{1}{P}$ γύρους

Αποδεικνύεται ότι η χρήση της παραπάνω πολύπλοκης πιθανότητας μας εξασφαλίζει ότι σε κάθε γύρο το ποσοστό P των επικεφαλής συστάδων θα μένει σταθερό. Επιπλέον η χρήση πιθανότητας μας εξασφαλίζει σε πρακτικό επίπεδο ότι οι επικεφαλής συστάδων θα έχουν μια ομοιόμορφη κατανομή στο δίκτυο. Στη συνέχεια κάθε επικεφαλής συστάδας εκπέμπει ένα μήνυμα διαφήμησης με μια προκαθορισμένη ισχύ και την ταυτότητά του. Οι υπόλοιποι αισθητήρες λαμβάνουν αυτά τα μηνύματα διαφήμησης και επιλέγουν τον επικεφαλής συστάδας του οποίου το μήνυμα έχει τη μεγαλύτερη ισχύ. Με αυτόν τον τρόπο καθορίζονται οι συστάδες.

Κατά τη δεύτερη φάση κάθε συστάδα κάνει ορισμένες ρυθμίσεις προκειμένου να είναι σε θέση να εκτελέσει τις λειτουργίες της. Το βασικό πρόβλημα είναι ότι επειδή το μοντέλο επικοινωνίας είναι η απευθείας επικοινωνία, αν δύο συσκευές εκπέμψουν ταυτόχρονα με τα σήματα να επικαλύπτονται, η υλοποίηση του επιπέδου MAC δεν μπορεί να διαχειριστεί τις συγκρούσεις. Οπότε είναι απαραίτητο σε κάθε συστάδα να έχει ο κάθε αισθητήρας τη δική του χρονική περίοδο (time slot) κατά την οποία στέλνει τις πληροφορίες που έχει συλλέξει στον επικεφαλής συστάδας.

Μετά την αποστολή του μηνύματος διαφήμησης και τον καθορισμό των συστάδων, κάθε αισθητήρας ενημερώνει τον επικεφαλής συστάδας του με την ταυτότητά του. Ο επικεφαλής συστάδας συλλέγει αυτές τις ταυτότητες και ορίζει ένα χρονοδιάγραμμα σύμφωνα με το οποίο κάθε αισθητήρας που ανήκει στησυστάδα θα έχει τη δική του χρονική περίοδο (time slot) για να εκπέμψει και το στέλνει στους αισθητήρες της συστάδας.

Κατά την τελευταία φάση οι αισθητήρες που δεν είναι επικεφαλής συστάδας στέλνουν στους επικεφαλής συστάδας τις πληροφορίες που έχουν συλλέξει από την τελευταία φορά που τις στείλανε, οι επικεφαλής συστάδων λαμβάνουν αυτές τις πληροφορίες, τις συνδυάζουν με αυτές που συλλέγουν τα ίδια, τις συμπιέζουν (προκειμένου να εξοικονομήσουν ενέργεια) και τις στέλνουν στην/στις απόληξη/απολήξεις.



Επικοινωνία Μέσω Πολλαπλών Ενδιάμεσων Κόμβων

Απευθείας Επικοινωνία

Σχήμα 2.3: Πειραματική Αξιολόγηση του Πρωτοκόλλου με Επίδειξη 'Νεκρών Κόμβων' μετά από μια Χρονική Περίοδο

2.2.3 Συμπεράσματα

Σε πειραματικά αποτελέσματα που έχουν γίνει σε εξομοιώσεις, το LEACH έχει εντυπωσιακά αποτελέσματα όσον αφορά την κατανάλωση ενέργειας. Η σύγκριση κατά βάση γίνεται με δύο άλλες βασικές προσεγγίσεις, ένα απλό πρωτόκολλο που χρησιμοποιεί επικοινωνία μέσω πολλαπλών ενδιάμεσων κόμβων (πχ ένα BFS δέντρο που συζητήσαμε παραπάνω) και ένα απλό πρωτόκολλο που χρησιμοποιεί απευθείας επικοινωνία σύμφωνα με το οποίο κάθε αισθητήρας εκπέμπει απ΄ ευθείας στην πλησιέστερη απόληξη. Όπως φαίνεται στο σχήμα 2.3, αν υποθέσουμε ότι έχουμε μόνο μια απόληξη και αυτό βρίσκεται στην άκρη της περιοχής στην οποία είναι τοποθετημένο το Ασύρματο Δίκτυο Αισθητήρων, τότε πρωτόκολλο που χρησιμοποιεί επικοινωνία μέσω πολλαπλών ενδιάμεσων κόμβων θα έχει σαν αποτέλεσμα οι αισθητήρες που βρίσκονται κοντά στην απόληξη να καταναλώνουν περισσότερη ενέργεια και συνεπώς να κλείνουν μετά από κάποιο χρόνο. Αυτό συμβαίνει επειδή οι συγκεκριμένοι αισθητήρες αναλαμβάνουν να προωθήσουν εκτός από τις πληροφορίες που τα ίδια συλλέγουν από το περιβάλλον και όλα τα πακέτα που παράγει το υπόλοιπο δίκτυο. Το πρωτόκολλο που χρησιμοποιεί απευθείας επικοινωνία αντίστοιχα θα έχει σαν αποτέλεσμα οι αισθητήρες που βρίσκονται μακριά από την απόληξη να καταναλώνουν περισσότερη ενέργεια και συνεπώς να κλείνουν μετά από κάποιο χρόνο. Αυτό συμβαίνει επειδή οι συγκεκριμένα αισθητήρες αναγκάζονται να επιστρατεύσουν περισσότερη ισχύ στις εκπομπές τους.

Στο LEACH αντίθετα σε κάθε γύρο οι περισσότεροι αισθητήρες κάνουν μικρές εκπομπές ενώ μόνο οι επικεφαλής συστάδων κάνουν εκπομπές μεγάλης εμβέλειας. Επιπλέον οι επικεφαλής συστάδων εναλάσσονται σε κάθε γύρο προκειμένου να μην κλείσουν από την μεγάλη κατανάλωση που έχουν. Τέλος, η χρήση συμπίεσης δεδομένων, όπως συζητήσαμε και στην προηγούμενη ενότητα έχει σαν αποτέλεσμα περαιτέρω εξοικονόμηση ενέργειας. Παρ΄ όλα αυτά, το μοντέλο που χρησιμοποιεί απευθείας επικοινωνία δεν χρησιμοποιείται ποτέ στην πράξη πρώτον διότι μπορεί εύκολα να έχει σαν αποτέλεσμα συγκρούσεις στις εκπομπές οι αντιμετωπίζονται πολύ δύσκολα και δεύτερον διότι στην πράξη δεν είναι εφικτό να προσδιοριστεί η ελάχιστη ενέργεια για να φτάσει μια εκπομπή στον επιθυμητό παραλείπτη. Ωστόσο σαν θεωρητικό εργαλείο το LEACH είναι πολύ ισχυρό πρωτόκολλο και παραλλαγές του είναι σε θέση να εφαρμοστούν στην πράξη, αλλά κυρίως απαντάει πολύ καλά στις ιδιαιτερότητες που έχει να αντιμετωπίσει ένα πρωτόκολλο δρομολόγησης στα Ασύρματα Δίκτυα

Αισθητήρων.

2.3 Ένα Κλιμακωτό και Ανθεκτικό σε Σφάλματα Πρωτόκολλο

2.3.1 Εισαγωγή - Βασικές Έννοιες

Το Directed Diffusion[16] είναι άλλο ένα πρωτόκολλο που ανταποκρίνεται αρκετά καλά στις συνθήκες που επικρατούν στα Ασύρματα Δίκτυα Αισθητήρων. Το σενάριο εφαρμογής περιλαμβάνει ειδικά ερωτήματα που εισέρχονται από τον διαχειριστή του δικτύου μέσω της απόληξης, η προώθηση των μηνυμάτων μέσω του δικτύου προς τους αισθητήρες που μπορούν να συλλέξουν την κατάλληλη πληροφορία, την συλλογή πληροφορίας και τη δρομολόγηση πίσω προς την απόληξη με βασικό κριτήριο την ποιότητα των συνδέσμων. Όλες οι επιλογές όσον αφορά τη δρομολόγηση γίνονται σε τοπικό επίπεδο, δηλαδή έπειτα από αλληλεπίδραση μεταξύ γειτονικών αισθητήρων.

Το μοντέλο λειτουργίας του Directed Diffusion περιλαμβάνει τα εξής:

- Το μοντέλο επικοινωνίας είναι η επικοινωνία μέσω πολλαπλών ενδιάμεσων κόμβων, δηλαδή όλες οι συσκευές εκπέμπουν με την ίδια εμβέλεια εκπομπής και οι διαδρομές από έναν κόμβο του δικτύου σε έναν άλλον συνήθως περιλαμβάνουν ενδιάμεσους κόμβους

- Οι αισθητήρες σε γενικές γραμμές είναι ακίνητα αλλά οι συνθήκες του δικτύου είναι δυναμικές με την έννοια ότι οι σύνδεσμοι (links) μεταξύ των αισθητήρων θεωρούμε ότι μπορούν να καταργηθούν ή να μειωθεί η χωρητικότητά τους κατά την εκτέλεση του πρωτοκόλλου

- Ένας αισθητήρας μπορεί να καταλάβει αν είναι σε θέση να συλλέξει την πληροφορία από το περιβάλλον που σχετίζεται με ένα ερώτημα. Για παράδειγμα, μπορεί το ερώτημα να περιλαμβάνει κάποια γεωγραφική περιοχή από την οποία στοχεύει ο διαχειριστής να συλλέξει πληροφορίες και οι αισθητήρες να διαθέτουν συσκευή GPS οπότε και να γνωρίζουν αν βρίσκονται εντός αυτής της περιοχής

Η βασική ιδέα είναι ότι ένα ερώτημα εισέρχεται στο δίκτυο μέσω της απόληξης και διοχετεύεται στο δίκτυο μέσω των αισθητήρων. Κάθε αισθητήρας που λαμβάνει ένα μήνυμα με την περιγραφή του ερωτήματος δημιουργεί μια καταχώρηση με τα στοιχεία του ερωτήματος και μια ειδική δομή για κάθε συσκευή από την οποία δέχτηκε το μήνυμα που αντιπροσωπεύει το ρυθμό δεδομένων με τον οποίον θα της προωθήσει τα δεδομένα που κάποια στιγμή θα αποκτήσει. Με αυτόν τον τρόπο, οι συσκευές που είναι σε θέση να συλλέξουν από το περιβάλλον τις πληροφορίες που σχετίζονται με το ερώτημα θα προωθήσουν τα δεδομένα στις συσκευές από τις οποίες έλαβαν το ερώτημα ενώ οι υπόλοιπες συσκευές θα συνεχίσουν να προωθούν τα δεδομένα με ανάλογο τρόπο μέχρι να φτάσουν στην απόληξη. Κατόπιν εφαρμόζονται τεχνικές οι οποίες επιλέγουν συγκεκριμένους γειτονικούς αισθητήρες για τον καθορισμό των διαδρομών, οι οποίες έχουν σαν αποτέλεσμα τη μείωση των εκπομπών και συνεπώς της κατανάλωσης ενέργειας και το δίκτυο να προσαρμόζεται σε τυχόν αλλαγές όσον αφορά την κατάσταση των συνδέσμων.

Οι βασικές έννοιες που θα μας απασχολήσουν είναι οι εξής:

- **Μηνύματα Ενδιαφέροντος Interest Messages) :** Τα μηνύματα που μεταφέρουν τα ερωτήματα που τίθενται στους αισθητήρες
- **Μηνύματα Δεδομένων Data Messages) :** Τα μηνύματα που περιλαμβάνουν τις πληροφορίες που στέλνουν οι αισθητήρες πίσω στην απόληξη
- **Βαθμίδες Gradients) :** Η δομή που αποθηκεύει κάθε αισθητήρας σε σχέση με κάποια γειτονική του συσκευή και αναπαριστά το ρυθμό δεδομένων με τον οποίο θα προωθήσει ή θα λάβει τα μηνυματα δεδομένων στο/από τον συγκεκριμένο γείτονα για κάθε ερώτημα
- **Ενίσχυση Βαθμίδων Reinforcement of Gradients) :** Η τεχνική που χρησιμοποιείται για να επιλεγεί μια υποομάδα των γειτονικών συσκευών ενός αισθητήρα για την προώθηση των δεδομένων

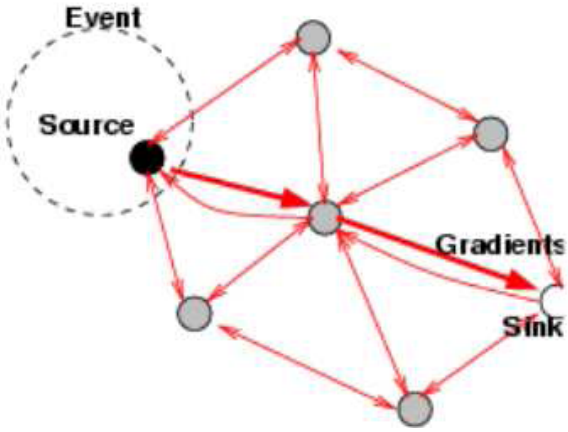
2.3.2 Το Πρωτόκολλο - Βασική Λειτουργία

Ο διαχειριστής όταν θέλει να μετρήσει μια συγκεκριμένη παράμετρο του περιβάλλοντος, δημιουργεί ένα *ενδιαφέρον* (interest) και το διαχέει (diffuses) στο δίκτυο μέσω της απόληξης. Σε κάθε αισθητήρα για κάθε *ενδιαφέρον* που λαμβάνεται δημιουργείται μια εργασία στην προσωρινή μνήμη του. Ένα ενδιαφέρον περιλαμβάνει την περιγραφή μιας εργασίας. Για παράδειγμα, ένα ενδιαφέρον θα μπορούσε να είναι το εξής:

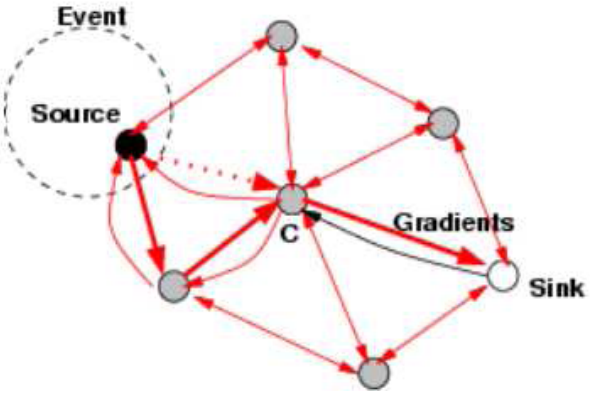
```
type = wheeled vehicle // detect vehicle location
interval = 100 ms // send events every 100 ms
duration = 10 seconds // for the next 10 seconds
rect = [-100, 100, 200, 400] // from nodes within rectangle
```

Το ενδιαφέρον διαχέεται στο δίκτυο βάσει κάποιας στρατηγικής. Η πιο απλή στρατηγική είναι η 'τεχνική πλημμύρας' flooding, δηλαδή κάθε αισθητήρας που λαμβάνει το ενδιαφέρον, αφού δημιουργήσει την ανάλογη εργασία στην προσωρινή μνήμη του, το προωθεί στους γείτονές του. Υπάρχουν και άλλες δυνατές στρατηγικές, όπως για παράδειγμα κάποια που βασίζεται σε γεωγραφική πληροφορία, στην περίπτωση που οι αισθητήρες διαθέτουν GPS. Στις εργασίες που δημιουργούνται στην προσωρινή μνήμη περιλαμβάνονται και βαθμίδες, μέχρι μία βαθμίδα για κάθε γείτονα. Οι βαθμίδες αντιπροσωπεύουν τον ρυθμό με τον οποίον θα προωθήσουν ή θα 'τραβήξουν' δεδομένα από τον κάθε γείτονα όσον αφορά τη συγκεκριμένη εργασία. Δηλαδή περιλαμβάνουν μια τιμή (μετρημένη σε $\frac{events}{sec}$) και μια κατεύθυνση. Όταν λοιπόν δέχεται ένα ενδιαφέρον, ένας αισθητήρας δημιουργεί μια καταχώρηση του ενδιαφέροντος στην προσωρινή μνήμη του που περιλαμβάνει μία χρονοσφραγίδα (timestamp) του τελευταίου ενδιαφέροντος που έλαβε και κάποιες βαθμίδες, όπου κάθε βαθμίδα περιλαμβάνει τον ρυθμό δεδομένων (data rate) και την διάρκεια του. Παρατηρούμε ότι αν ένας αισθητήρας λάβει ένα ενδιαφέρον το οποίο έχει ήδη λάβει στο παρελθόν τότε απλώς το ενημερώνει προσθέτωντας μία βαθμίδα ενώ ένα ενδιαφέρον σβήνεται από την προσωρινή μνήμη όταν όλες οι βαθμίδες λήξουν.

Αν ληφθεί ένα ενδιαφέρον από έναν αισθητήρα που μπορεί να το εξυπηρετήσει, τότε ο αισθητήρας αυτός ξεκινάει να συλλέγει πληροφορίες από το περιβάλλον. Έπειτα υπολογίζει τον μέγιστο ρυθμό δεδομένων από όλες τις βαθμίδες που διαθέτει σχετικά με αυτό το ενδιαφέρον και παράγει *δείγματα γεγονότων* (event samples) σε αυτόν τον ρυθμό. Τέλος προωθεί τα μηνύματα δεδομένων στους αισθητήρες τα οποία αναλογούν στις βαθμίδες.



Ενίσχυση των βαθμίδων



Επισκευή Διαδρομών με Ενίσχυση των Βαθμίδων

Κάθε αισθητήρας διατηρεί μια προσωρινή μνήμη με τα μηνύματα που είναι προς προώθηση. Όταν λοιπόν λαμβάνουν ένα μήνυμα δεδομένων, οι αισθητήρες ελέγχουν άν διαθέτουν ένα αντίστοιχο ενδιαφέρον στην προσωρινή μνήμη ενδιαφέροντων (interest cache) και αν το ίδιο μήνυμα δεδομένων δεν υπάρχει ήδη στην προσωρινή μνήμη δεδομένων. Σε αυτήν την περίπτωση, οι αισθητήρες αποθηκεύουν το μήνυμα στην προσωρινή μνήμη δεδομένων και κάποια στιγμή το προωθούν, ενώ σε διαφορετική περίπτωση το αγνοούν. Για να προωθήσουν τα μηνύματα, οι αισθητήρες υπολογίζουν τον ρυθμό δεδομένων των εισερχόμενων μηνυμάτων ελέγχοντας την προσωρινή μνήμη δεδομένων. Αν ο ρυθμός δεδομένων των εισερχόμενων μηνυμάτων είναι μικρότερος ή ίσος με τον ρθυμό δεδομένων των βαθμίδων, τότε προωθεί τα μηνύματα δεδομένων στους προορισμούς που υποδεικνύουν τις βαθμίδες, ενώ στην αντίθετη περίπτωση, τα δεδομένα μετατρέπονται 'προς τα κάτω' (down-converted) για να φτάσουν στον ανάλογο ρυθμό δεδομένων.

2.3.3 Το Πρωτόκολλο - Διορθωτικές Κινήσεις

Προκειμένου να επιλέγεται μια βασική διαδρομή για την δρομολόγηση των δεδομένων έτσι ώστε να μην καταναλώνεται περισσότερη ενέργεια σε μεταδόσεις ακολουθείται μια παραλλαγή της βασικής διαδικασίας. Για κάθε εργασία η απόληξη δημιουργεί ένα ενδιαφέρον με χαμηλό ρυθμό δεδομένων (exploratory interest) και το διαχέει στο δίκτυο μέχρι να λάβει τα αντίστοιχα χαμηλού ρυθμού δεδομένα (exploratory events). Οι βαθμίδες που δημιουργούνται σε αυτή τη διαδικασία ονομάζονται *εξερευνητικές βαθμίδες* (exploratory gradients). Κατόπιν η απόληξη επιλέγει να 'ενισχύσει' έναν από τους γείτονές του από τους οποίους λαμβάνει τα δεδομένα αυτά. Αυτό το καταφέρνει στέλνοντας ένα πανομοιότυπο ενδιαφέρον με μεγαλύτερο ρυθμό δεδομένων σε αυτόν τον γείτονα. Ο γείτονας αυτός προκειμένου να ανταπεξέλθει στον μεγαλύτερο ρυθμό δεδομένων επιλέγει με τη σειρά του να 'ενισχύσει' έναν από τους δικούς του γείτονες. Έτσι δημιουργείται μια διαδρομή από τους αισθητήρες που συλλέγουν πληροφορία μέχρι την απόληξη που περιλαμβάνει τις βαθμίδες που έχουν 'ενισχυθεί'. Αυτές οι βαθμίδες ονομάζονται βαθμίδες δεδομένων (data gradients). Η επιλογή των προς ενίσχυση βαθμίδων γίνεται εξόλοκλήρου με τοπικά κριτήρια όπως για παράδειγμα ενισχύεται ο γείτονας που ανέφερε πρώτος το καινούριο (όχι *εξερευνητικό*) ενδιαφέρον.

Με αυτή τη διαδικασία, το πρωτόκολλο μπορεί να προσαρμόζεται σε αλλαγές, για παράδειγμα, αν ενισχύεται η βαθμίδα που αντιστοιχεί στον σύνδεσμο με τη μεγαλύτερη χωρητικότητα σε

ρυθμό δεδομένων, το πρωτόκολλο θα μπορεί να προσαρμοστεί στην καταστροφή ή μειωμένη απόδοση ενός συνδέσμου. Επιπλέον, με αυτήν την διαδιακασία, το πρωτόκολλο μπορεί να ανταπεξέλθει στην παρουσία πολλών απολήξεων που διαχέουν διαφορετικά ενδιαφέροντα στο δίκτυο.

Χρησιμοποιώντας αυτήν την προσθήκη, μπορεί για το ίδιο ενδιαφέρον να ενισχυθούν περισσότερες της μιας διαδρομές από τα γεγονότα προς μέτρηση (events) στην απόληξη. Για παράδειγμα, αν ένας κόμβος ενισχύσει αρχικά έναν γείτονά του και στη συνέχεια διαπιστώσει πως ένας άλλος γείτονάς του μπορεί να εξυπηρετήσει πιο αποτελεσματικά τη δρομολόγηση των δεδομένων, θα ενισχύσει και τον δεύτερο γείτονα. Σε αυτήν την περίπτωση πρέπει ο πρώτος γείτονας να ενισχυθεί αρνητικά. Αυτό μπορεί να επιτευχθεί με δύο τρόπους:

- Ο πρώτος τρόπος είναι να σταματήσουμε να στέλνουμε ενδιαφέροντα στον γείτονα που θέλουμε να ενισχύσουμε αρντητικά μέχρι η βαθμίδα δεδομένων να εκλείψει λόγω της πεπερασμένης διάρκειας και να παραμείνει ως εξερευνητική βαθμίδα.

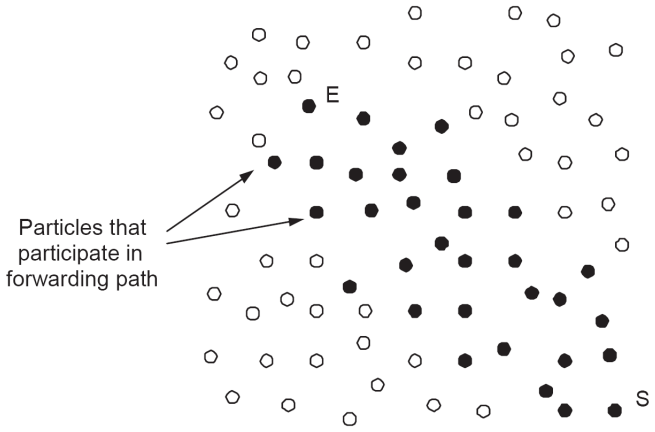
- Ο δεύτερος τρόπος είναι περισσότερο ενεργητικός και περιλαμβάνει την αποστολή στον γείτονα που θέλουμε να ενισχύσουμε αρνητικά ενός πανομοιότυπου ενδιαφέροντος με χαμηλό ρυθμό δεδομένων (δηλαδή ένα εξερευνητικό ενδιαφέρον). Ένας αισθητήρας που λαμβάνει ένα εξερευνητικό ενδιαφέρον από ένα κόμβο του δικτύου στον οποίο αντιστοιχεί βαθμίδα δεδομένων θα ενημερώσει την προσωρινή μνήμη ενδιαφέροντων του αντικαθιστώντας τη βαθμίδα δεδομένων με μία εξερευνητική βαθμίδα.

Η χρήση της αρνητικής ενίσχυσης μπορεί να έχει σαν αποτέλεσμα την προσαρμογή και εύρεση εναλλακτικής διαδρομής στην περίπτωση που καταστροφεί κάποιον σύνδεσμο του δικτύου και την αφαίρεση κύκλων loops στις διαδρομές των δεδομένων.

2.3.4 Συμπεράσματα

Όπως και το LEACH, το Directed Diffusion ανταπεξέρχεται πολύ καλά στις ιδιαίτερες απαιτήσεις που παρουσιάζει ένα πρωτόκολλο δρομολήγησης για Ασύρματα Δίκτυα Αισθητήρων. Η εύρεση διαδρομών και οι προσαρμογές στις διαδρομές γίνονται από τους αισθητήρες με εξ ολοκλήρου τοπικά κριτήρια. Η 'διευθυνσιοδότηση', δηλαδή τα χαρακτηριστικά που δίνει ο διαχειριστής του δικτύου όσον αφορά σε ποια συσκευή αναφέρεται μια εργασία, δεν γίνεται με τις μοναδικές ταυτότητες των αισθητήρων, αλλά με το ίδιο το ερώτημα που τίθεται στο δίκτυο. Το γεγονός ότι οι αισθητήριες συσκευές είναι ευάλωτες σε σφάλματα και αποτυχίας αντιμετωπίζεται με τη δυνατότητα να προσαρμόζονται οι διαδρομές. Τέλος, εφαρμόζονται ρυθμίσεις που καταφέρνουν να κρατήσουν στο ελάχιστο την παραπανήσια κατανάλωση ενέργειας.

Οι πειραματικές μετρήσεις πάνω στο Directed Diffusion σε σύγκριση με απλά πρωτόκολλα που χρησιμοποιούν επικοινωνία μέσω πολλαπλών ενδιάμεσων κόμβων όπως το flooding και το Omniscient Multicast δείχνουν ότι μπορεί να επιτύχει σοβαρή αποτελεσματικότητα στην κατανάλωση ενέργειας, ειδικά με χρήση των τεχνικών ενίσχυσης, μπορεί να ανταπεξέλθει πολύ καλά σε δυναμικές συνθήκες του δικτύου και η απόδοσή του επηρεάζεται σημαντικά από την υλοποίηση του επιπέδου MAC.



Σχήμα 2.4: Η ζώνη των Συσκευών που Προωθούν το πακέτο πληροφοριών

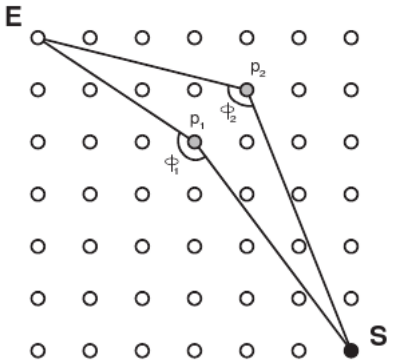
2.4 Ένα Πιθανοτικό πρωτόκολλο

Η χρήση πιθανότητας στη δρομολόγηση στα Ασύρματα Δίκτυα Αισθητήρων μπορεί να έχει αρκετά πλεοντεκτήματα. Η βασική πιθανοτική επιλογή γίνεται στην επιλογή του επόμενου κόμβου ή των επόμενων κόμβων στη διαδρομή ενός πακέτου προς την απόληξη. Συνεπώς, με τη χρήση πιθανότητας σε αυτήν την επιλογή, μπορεί να απλοποιηθεί η διαδικασία δημιουργίας υποδομής δρομολόγησης και μπορεί να υποστηρίζεται η δυνατότητα να δημιουργείται ένας σχετικά μικρός αριμός αντιγράφων του πακέτου που προωθούνται προς την απόληξη έτσι ώστε το δίκτυο να έχει περισσότερη αντοχή σε σφάλαματα συσκευών ή συνδέσμων. Όλα αυτά χωρίς να πλήττεται επί της ουσίας η αποτελεσματικότητα του πρωτοκόλλου. Θα περίμενε κανείς ότι η χρήση πιθανότητας μπορεί να οδηγήσει σε αποτυχίες δρομολόγησης ή σε ιδιαίτερα ιδιόμορφες καταστάσεις, αλλά όπως προκύπτει από προσεκτική μελέτη και πειραματισμούς, είναι πρακτικά αδύνατο η χρήση πιθανότητας να έχει αυτά τα αποτελέσματα. Ένα παράδειγμα το είδαμε ήδη στο LEACH, όπου η επιλογή των επικεφαλής συστάδων βασίζεται σε πιθανοτική επιλογή. Θεωρητικά θα μπορούσαν να επιλεγούν επικεφαλής συστάδων οι οποίοι να είναι πολύ κοντά μεταξύ τους αχρηστεύοντας σε μεγάλο βαθμό τη λογική που δημιουργούνται οι συστάδες, αλλά σε πρακτικό επίπεδο αυτό δε συμβαίνει ποτέ.

Οι υποθέσεις του Πρωτόκολλου Πιθανοτικής Προώθησης (Probabilistic Forwarding Routing (PFR)[8]) που θα περιγράψουμε παρακάτω είναι οι εξής :

- Κάθε αισθητήρας μπορεί να εκτιμήσει την κατεύθυνση μιας εισερχόμενης εκπομπής, πιθανόν μέσω μιας direction-sensing antenna
- Κάθε αισθητήρας μπορεί να εκτιμήσει την απόσταση μιας εισερχόμενης εκπομπής, πιθανόν μετρώντας την ισχύ της
- Κάθε αισθητήρας γνωρίζει επιπλέον την κατεύθυνση προς την απόληξη, πιθανώς μέσω μιας φάσης αρχικοποίησης κατά την οποία η απόληξη 'διαφημίζει' την ύπαρξη και τοποθεσία του
- Όλοι οι αισθητήρες έχουν μια κοινή αίσθηση συστήματος συντεταγμένων

Αξίζει να παρατηρήσουμε ότι δεν χρειάζεται κάποιο υλικό GPS για αυτό το πρωτόκολλο.



Σχήμα 2.5: Η γωνία που σχηματίζεται από την ευθεία που συνδέει το γεγονός προς μέτρηση (event) με τη συσκευή και τη συσκευή με την απόληξη

Επιπλέον, δεν χρειάζεται οι αισθητήρες να γνωρίζουν κάτι σχετικά με την τοπολογία του δικτύου.

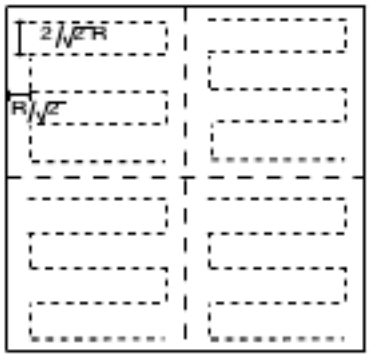
Η βασική ιδέα του πρωτοκόλλου είναι ότι με πιθανοτικό τρόπο επιλέγεται μια μικρής περιοχής ζώνη γύρω από τη γραμμή που ενώνει ένα γεγονός προς μέτρηση με την απόληξη στην οποία οι αισθητήρες αναλαμβάνουν να προωθήσουν το πακέτο δεδομένων που περιγράφει το γεγονός προς μέτρηση. Για κάθε αισθητήρα δημιουργείται μια γωνία από τις γραμμές που ενώνουν τον αισθητήρα με το γεγονός προς μέτρηση και τον αισθητήρα με την απόληξη (βλέπε fig.2.5). Χάρη στις υποθέσεις που έγιναν στο μοντέλο του πρωτοκόλλου, οι αισθητήρες είναι σε θέση να υπολογίσουν αυτή τη γωνία. Κάθε αισθητήρας κάνει την επιλογή αν θα προωθήσει το πακέτο ή όχι σύμφωνα με τον κανόνα:

$$P_{fwd} = \begin{cases} 1 & , \quad \phi \geq \phi_{threshold} = 134^{\circ} \\ \frac{\phi}{\pi} & , \quad otherwise \end{cases}$$

Αποδεικνύεται ότι για σχετικά μεγάλη πυκνότητα αισθητήρων στο περιβάλλον, το PFR επιτυγχάνει πάντα να δρομολογήσει πακέτα από τα γεγονότα προς μέτρηση στην απόληξη. Επιπλέον, οι στόχοι που τέθηκαν στο σχεδιασμό του πρωτοκόλλου, όπως η ανοχή σε σφάλματα, η σχετικά μικρή απόσταση από το γεγονός προς μέτρηση μέχρι την απόληξη και η σχετικά μικρή κατανάλωση ενέργειας επιβεβαιώνονται από τα πειραματικά αποτελέσματα

2.5 Πρωτόκολλα με Παρουσία Πολλαπλών Κινητών Απολήξεων

Ο παράγοντας της κίνησης όταν εισάγεται στα Ασύρματα Δίκτυα Αισθητήρων έχει πολλά αποτελέσματα. Είναι προφανές ότι μια παραδοσιακή προσέγγιση στο πρόβλημα της δρομολόγησης η οποία βασίζεται στην εύρεση διαδρομών από τους αισθητήρες προς την απόληξη δεν θα είχε καλά αποτελέσματα σε συνθήκες κίνητικότητας. Προσεγγίσεις επίσης που υπάρχουν στα Κινητά Αδόμητα Δίκτυα οι οποίες βασίζονται στην επιδιόρθωση είτε περιοδικά, είτε έπειτα από εντοπισμό λάθους, αφενός προκαλούν μεγάλη επιβάρυνση (overhead), αφετέρου μπορούν να αποφευχθούν στα Ασύρματα Δίκτυα Αισθητήρων αν λάβουμε υπόψιν τα ιδιαίτερα χαρακτηριστικά τους.



Σχήμα 2.6: Παράδειγμα Κατάτμησης σε Ίσους Χώρους και Κίνησης των απολήξεων εντός Αυτών όταν $k = 4$

Παρακάτω θα περιγράψουμε κάποια προτεινόμενα πρωτόκολλα συλλογής δεδομένων [7] τα οποία προσπαθούν, βασιζόμενα στην ιδιαίτερη φύση των Ασύρματων Δικτύων Αισθητήρων, να εκμεταλλευτούν τον παράγοντα της κίνησης έτσι ώστε να εξοικονομήσουν ενέργεια από εκπομπές. Το βασικό χαρακτηριστικό των Ασύρματων Δικτύων Αισθητήρων που ευνοεί μια τέτοια προσέγγιση είναι ότι δεν μας ενδιαφέρει να ανταλάσσεται πληροφορία μεταξύ δύο οποιονδήποτε συσκευών του δικτύου, αλλά μόνο να προωθείται πληροφορία από τους αισθητήρες στην απόληξη. Επιπλέον, στην περίπτωση που έχουμε περισσότερα της μιας απόληξης, μας ενδιαφέρει να καταλήξει η πληροφορία σε οποιοδήποτε απόληξη χωρίς να μας ενδιαφέρει σε ποιο.

Στις υποθέσεις των παρακάτω πρωτοκόλλων θα συμπεριλάβουμε το ότι οι απολήξεις του δικτύου έχουν τη δυνατότητα να μετακινούνται κατά βούληση, ορίζοντας ακριβώς σε ποια κατεύθυνση θα κινούνται και μπορούν να έχουν επίγνωση της ακριβούς τοποθεσίας τους.

2.5.1 Πρώτο Πρωτόκολλο: Κεντρική Χωροταξική Διαμέρι-ση (Centralized Spatial Partitioning)

Σε αυτήν την προσέγγιση θεωρούμε ότι ο διαχειριστής του δικτύου μπορεί να οργανώσει την τοποθέτηση των αισθητήρων με μεγάλη ακρίβεια. Υποθέτουμε ότι το δίκτυο καλύπτει μια τετραγωνική περιοχή A και k κινητές απολήξεις όπου $\sqrt{k} \in N$ οπότε χωρίζουμε το δίκτυου σε k τετραγωνικές περιοχές μεγέθους $D/\sqrt{k} \times D/\sqrt{k}$ (όπου D η διάσταση της τετραγωνικής περιοχής, δηλαδή $A = D \times D$). Από εκεί και πέρα, αναθέτουμε κάθε απόληξη σε μια περιοχή όπου πραγματοποιούν μια 'φιδίσια' (snakelike) κίνηση συλλέγοντας τα δεδομένα από τους αισθητήρες, όπως φαίνεται στο φιγ. 2.6. Η επικοινωνία των απολήξεων με τους αισθητήρες πραγματοποιείται ως εξής: οι απολήξεις εκπέμπουν περιοδικά ένα beacon μήνυμα ανακοινώνοντας την παρουσία τους στους γειτονικούς αισθητήρες και οι αισθητήρες απαντάνε με τις πληροφορίες που έχουν συλλέξει μέχρι στιγμής. Η συγκεκριμένη προσέγγιση έχει σημαντικά πλεονεκτήματα όσον αφορά την κατανάλωση καθώς τα πακέτα πληροφορίας μεταδίδονται στις απολήξεις πραγματοποιώντας μόλις μια εκπομπή.

2.5.2 Δεύτερο Πρωτόκολλο: Αμοιβαία Αποφυγή Απολήξεων (Sink Mutual Avoidance)

Σε αυτήν την προσέγγιση οι απολήξεις δεν περιφέρονται βάσει κάποιας προκαθορισμένης διαδρομής, αλλά τυχαία. Καθώς έρχονται σε εμβέλεια εκπομπής με τους αισθητήρες, πέρα από την ανταλαγή πληροφορίας αφήνουν και ένα ίχνος. Οι αισθητήρες έπειτα από κάθε αλληλεπίδραση με κάποια απόληξη, αποθηκεύουν την ταυτότητά του και έναν μετρητή χρόνου με αρχική τιμή $t_c = t_{exp}$ η οποία είναι παράμετρος του πρωτοκόλλου. Ο μετρητής αυτός μειώνεται σταδιακά εκτός και αν ο αισθητήρας ξαναέρθει σε επαφή με την ίδια απόληξη οπότε και αρχικοποιείται. Από εκεί και πέρα, σε κάθε αλληλεπίδραση με κάποια άλλη απόληξη, οι αισθητήρες στέλνουν τις πληροφορίες που έχουν να κάνουν με το πόσο πρόσφατα έχουν αλληλεπιδράσει με κάποια απόληξη, οπότε και οι απολήξεις έτσι μπορούν να έχουν επίγνωση των διαδρομών που έχουν πραγματοποιήσει τις υπόλοιπες απολήξεις. Έτσι, όταν ένα απόληξη πέσει πάνω στο ίχνος κάποιας άλλης απόληξης, τότε αλλάζει κατεύθυνση προκειμένου να επισκευτεί αισθητήρες που έχουν περισσότερο καιρό να δώσουν πληροφορίες.

2.5.3 Τρίτο Πρωτόκολλο: Διαμέριση με Βάση το Φορτίο (Load Based Network Partitioning)

Στην τρίτη προσέγγιση ο στόχος είναι να δημιουργήσουμε τόσες ομάδες (groups) μέσα στο δίκτυο όσα και οι απολήξεις και να αναθέσουμε κάθε ομάδα σε μια απόληξη, προσπαθώντας οι ομάδες να έχουν όσο το δυνατόν ίσο *βάρος*, ποσότητα την οποία θα αναλύσουμε στη συνέχεια. Αρχικά χωρίζουμε το δίκτυο σε συστάδες (clusters) με έναν παρόμοιο τρόπο με αυτόν που παρουσιάζεται στην εργασία [14], εντός ενός προκαθορισμένου χρονικού διαστήματος T_{init}. Αρχικά κάθε αισθητήρας αποφασίζει να γίνει επικεφαλής συστάδας με μια προκαθορισμένη πιθανότητα p_C και εκπέμπει ένα *beacon* μήνυμα σε όλους τους γείτονές του σε μια τυχαία χρονική στιγμή εντός του $T_{init}/3$ (η τυχαία χρονική στιγμή χρησιμεύει στο να αποφευχθούν οι συγκρούσεις μεταδόσεων). Οι αισθητήρες οι οποίοι δεν είναι επικεφαλής συστάδων όταν δεχθούν αυτά τα beacon μηνύματα απαντάνε στον επικεφαλής συστάδας του οποίου η εκπομπή ήταν η ισχυρότερη με ένα *join* μήνυμα, σε μια τυχαία χρονική στιγμή εντός του $T_{init}/2$. Επειδή το μοντέλο επικοινωνίας εδώ είναι η επικοινωνία μέσω πολλαπλών ενδιάμεσων κόμβων και όχι η απευθείας επικοινωνία, είναι πιθανό κάποιοι επικεφαλής συστάδας να μην δεχτούν κανένα *join* μήνυμα ή κάποιοι αισθητήρες να μην δεχτούν κανένα *beacon* μήνυμα. Στην πρώτη περίπτωση, ένας επικεφαλής συστάδας είτε επιλέγει να ενταχθεί ως απλός αισθητήρας σε κάποιον γειτονικό επικεφαλής συστάδας εαν υπάρχει τέτοιο, είτε να συμπεριφέρεται στο εξής ως συστάδα με μοναδικό μέλος τον εαυτό του. Στη δεύτερη περίπτωση, ένας αισθητήρας που δεν δέχεται κανένα beacon μήνυμα αυτοεκλέγεται ως επικεφαλής συστάδας. Οι εκπομπές σε αυτές τις διορθωτικές κινήσεις γίνονται σε κάποια τυχαία χρονική στιγμή εντός του υπόλοιπου $T_{init}/6$.

Κατόπιν εκτελείται σε κάθε συστάδα ένα υποπρωτόκολλο το οποίο έχει στόχο να καθορίσει το *βάρος* της συστάδας. Ο επικεφαλής συστάδας εκπέμπει περιοδικά ένα *status* μήνυμα και οι υπόλοιποι αισθητήρες απαντάνε με ένα *statusreply* μήνυμα που περιέχει τις τιμές λ_i που είναι ο ρυθμός παραγωγής μηνυμάτων του αισθητήρα και ε_i που είναι μια εκτίμηση του ρυθμού κατανάλωσης ενέργειας. Η απόληξη όταν συλλέξει αυτά τα μηνύματα, υπολογίζει το βάρος της συστάδας ως

$$W_C = \alpha \cdot N_C + \beta \cdot \Lambda_C + \gamma \cdot E_C,$$

όπου N_C είναι ο αριθμός των αισθητήρων που απαρτίζουν τη συστάδα, Λ_C είναι ο μέσος ρυθμός παραγωγής μηνυμάτων της συστάδας, E_C είναι ο μέσος ρυθμός κατανάλωσης της συστάδας και τα α, β και γ παράμετροι του πρωτοκόλλου.

Στη συνέχεια, οι συστάδες συμπεριφέρονται σαν κόμβοι ενός δικτύου οι οποίοι επικοινωνούν μεταξύ τους. Κάθε απόληξη διαλέγει μια συστάδα με την οποία έχει επαφή και την αναγάγει σε επικεφαλής ομάδας μέσω ενός μηνύματος $group - init$ (σε αυτό το σημείο σημειώνουμε ότι το πρωτόκολλο θα λειτουργεί καλύτερα εαν οι απολήξεις είναι ομοιόμορφα κατανεμημένα στο δίκτυο, αν και θα δουλέψει και σε διαφορετικές περιπτώσεις). Οι επικεφαλής ομάδων ξεκινούν τη δημιουργία δέντρων έκτασης τα οποία θα αποτελέσουν αργότερα τις ίδιες τις ομάδες. Αυτή η φάση εκτελείται σε γύρους. Σε κάθε γύρο, προστίθενται κάποιες συστάδες στην ομάδα τα οποία έχουν απόσταση μιας εκπομπής περισσότερο από τις συστάδες που είναι ήδη στην ομάδα μέσω ενός μηνύματος $group - join$. Κατόπιν, όλα τα μέλη ττης ομάδας στέλνουν στον επικεφαλής ομάδας τα *βάρη* τους, μέσω του δέντρου, ο επικεφαλής ομάδας υπολογίζει τη μέση τιμή και το στέλνει πίσω σε όλα τα μέλη της ομάδας. Καθώς οι ομάδες επεκτείνονται, κάποιες συστάδες οι οποίες αποτελούν 'φύλλα' του δέντρου έκτασης, ενδέχεται να δεχτούν ένα μήνυμα $group - join$ από κάποια άλλη ομάδα. Σε αυτήν την περίπτωση αποφασίζουν να ενταχθούν στην καινούρια ομάδα στην περίπτωση όπου το μέσο *βάρος* του είναι μικρότερο από το παλιό, προκειμένου να μοιράζεται καλύτερα η κατανάλωση ανάμεσα στις ομάδες.

Οι απολήξεις, τα οποία έχουν ελευθερία κίνησης και σε αυτό το μοντέλο, επιλέγουν μια τυχαία κατεύθυνση και ταξιδεύουν μια απόσταση ίση με το εκτιμώμενο μέγεθος της ομάδας (υπολογίζεται βάσει του μεγέθους του δικτύου και του αριθμού των απολήξεων), συλλέγοντας τα δεδομένα που παράγουν οι αισθητήρες μέσω απλών επικοινωνιών μίας εκπομπής. Στην περίπτωση που έρθουν σε επαφή με μια συστάδα που ανήκει σε διαφορετική ομάδα, αλλάζουν την κατεύθυνσή τους. Επειδή τα μέσα *βάρη* των ομάδων μπορεί να αλλάξουν κατά τη διάρκεια εκτέλεσης του πρωτοκόλλου, προβλέπεται η διαδικασία κατασκευής εκ νέου ομάδων η οποία ξεκινάει με την αποστολή μηνυμάτων $group - init$.

Κεφάλαιο 3

Ασφάλεια και Κρυπτογραφία

Σε αυτό το κεφάλαιο αναλύουμε το ζήτημα της ασφάλειας γύρω από τα Ασύρματα Δίκτυα Αισθητήρων. Αρχικά παρουσιάζουμε κάποιες τεχνικές παραδοσιακής κρυπτοργραφίας (πρωτόκολλα δημοσίου κλειδιού, πρωτόκολλα ιδιωτικού κλειδιού, ψηφιακές υπογραφές, πρόβλημα Diffie-Hellman), στη συνέχεια αναλύουμε το πώς ειδικεύεται το ζήτημα της ασφάλειας στα Ασύρματα Δίκτυα Αισθητήρω κατηγοριοποιώντας τους επιτιθέμενους και παραθέτοντας τις βασικές επιθέσεις, κατόπιν παρουσιάζουμε το μαθηματικό μοντέλο των ελλειπτικών καμπύλων ως κατάλληλο για Ασύρματα Δίκτυα Αισθητήρων λόγω των χαμηλών απαιτήσεών τους σε υπολογιστικούς πορους και παρουσιάζουμε κάποιες χρήσεις των ελλειπτικών καμπύλων στην κρυπτογραφία (Diffie-Hellman, GDH σε τοπολογία εικονικού δακτυλίου, GDH σε γενικό δίκτυο) και τέλος παρουσιάζουμε ένα ολοκληρωμένο πρωτόκολλο που δημιουργεί μια υποδομή δρομολόγησης με απόλυτα ασφαλή τρόπο.

3.1 Βασικά Μοντέλα Κρυπτογραφίας

Προκειμένου να μελετήσουμε κάποιες βασικές προσεγγίσεις στο ζήτημα της ασφάλειας των Ασύρματων Δικτύων Αισθητήρων, στη συνέχεια θα αναλύσουμε τη λογική πίσω από κάποιους αλγορίθμους κρυπτογράφησης και πιστοποίησης αυθεντικότητας γενικών προβλημάτων κρυπτογραφίας χωρίς να εισέλθουμε σε λεπτομέρειες υλοποίησης.

Το πρόβλημα που καλούμαστε να αντιμετωπίσουμε περιγράφεται αφηρημένα ως εξής. Σε ένα χώρο βρίσκεται μια ομάδα από χρήστες και ό,τι μήνυμα στέλνει κάποιος είναι σε θέση να το διαβάσουν όλοι. Έστω δύο χρήστες A και B (συνήθως λόγω αυτών των αρχικών τους ονομάζουμε Alice και Bob). Οι δύο στόχοι που πρέπει να πετύχουμε είναι:

- Πώς μπορεί κάποιος να στείλει ένα μήνυμα το οποίο θα είναι σε θέση να διαβάσει μόνο ο B·
- Πώς μπορεί να στείλει ο A ένα μήνυμα με τέτοιον τρόπο έτσι ωστε κάποιος που θα το λάβει να μπορεί να πιστοποιήσει ότι όντως προέρχεται από τον A·

Αν βρούμε δύο μεθόδους για να πετύχουμε αυτούς τους δύο στόχους, τότε συνδυάζοντάς τες μπορούμε να επιτύχουμε ασφαλή επικοινωνία μεταξύ των A και B, δηλαδή να στέλνει ο A μηνύματα στον B τα οποία ο B θα μπορεί αφενός να καταλάβει και αφετέρου να πιστοποιήσει ότι όντως προέρχονται από τον A.

3.1.1 Πρωτόκολλα Δημοσίου Κλειδιού

Έστω ότι έχουμε τα παρακάτω μαθηματικά εργαλεία. Πρώτον μια συνάρτηση $M' = E_K(M)$ η οποία μετασχηματίζει ένα μήνυμα M σε ένα μήνυμα M' ίδιου μεγέθους με βάση τον αριθμό K. Όταν πραγματοποιούμε αυτόν τον μετασχηματισμό θα λέμε ότι κρυπτογραφούμε (ή αποκρυπτογραφούμε) το μήνυμα M με το κλειδί K. Δεύτερον τη συνάρτηση $f(r) =< P, S >$ όπου r μια τυχαία ποσότητα και οι P και S έχουν την συγκεκριμένη ιδιότητα: $E_P(E_S(M)) = M$ και $E_S(E_P(M)) = M$. Η συνάρτηση που παράγει τα P και S είναι υπολογιστικά υλοποιήσημη και χρειάζεται σχετικά λίγο χρόνο για να εκτελεστεί, ενώ το να έχουμε στη διάθεσή μας το P και να βρούμε το S, ή το αντίστροφο, αν και συνήθως είναι μαθηματικά εφικτό, είναι υπολογιστικά πολύ δύσκολο με την έννοια ότι οι ισχυρότεροι υπολογογιστές σήμερα θα χρειάζονταν κάποια χρόνια να το επιτύχουν. Τέτοια μαθηματικά εργαλεία υπάρχουν και χρησιμοποιούνται σήμερα σε ένα πλήθος εφαρμογών, αλλά στην παρούσα μελέτη δεν θα τα αναλύσουμε περεταίρω.

Χρησιμοποιώντας αυτά τα εργαλεία μπορούμε να επιτύχουμε τους στόχους που είχαμε θέσει. Οι A και B χρησιμοποιούν την f για να παράγουν δύο ζευγάρια κλειδιών $< P_A, S_A >$ και $< P_B, S_B >$. Στα κλειδιά P θα αναφερόμαστε ως δημόσια κλειδιά (public) και στα κλειδιά S θα ανφερόμαστε ως μυστικά κλειδιά (secret). Οι A και B δημοσιοποιούν σε όλους τους χρήστες τα δημόσια κλειδιά τους. Από εκεί και πέρα, αν κάποιος θέλει να στείλει ένα μήνυμα το οποίο θα είναι σε θέση να διαβάσει μόνο ο B, το κρυπτογραφεί με το δημόσιο κλειδί του B, δηλαδή παράγει το $M' = E_{P_B}(M)$. Ο B για να ανακτήσει το αρχικό μήνυμα αποκρυπτογραφεί με το μυστικό του κλειδί, δηλαδή παράγει το $E_{S_B}(M') = E_{S_B}(E_{P_B}(M)) = M$ που είναι το αρχικό μήνυμα. Εφόσον μόνο ο B κατέχει το S_B είναι ο μόνος που είναι σε θέση να ανακτήσει το M, έτσι έχουμε πετύχει τον πρώτο στόχο μας.

Αν τώρα ο A θέλει να στείλει ένα μήνυμα M το οποίο κάποιος λαμβάνοντάς το να μπορεί να πιστοποιήσει ότι όντως προέρχεται από αυτόν, τότε παράγει το πακέτο $< M, M' = E_{S_A}(M) >$ και το στέλνει στους υπόλοιπους χρήστες. Κάποιος λαμβάνοντάς το μπορεί να αποκρυπτογραφήσει το M' με το δημόσιο κλειδί του A, να συγκρίνει το αποτέλεσμα με το M και να επαληθεύσει ότι όντως προέρχεται από τον A. Εφόσον μόνο ο A κατέχει το S_A είναι ο μόνος που μπορούσε να παράγει το ζευγάρι $< M, M' >$, οπότε έτσι έχουμε πετύχει τον δεύτερο στόχο μας.

Ο συνδυασμός των δύο μεθόδων που εξασφαλίζει την ασφαλή επικοινωνία μεταξύ των A και B είναι ο εξής, έστω ότι το μήνυμα που επιθυμεί να στείλει ο A στον B είναι το M, τότε ο A παράγει το εξής πακέτο : $< E_{P_B}(M), E_{S_A}(E_{P_B}(M)) >$ και το στέλνει. Ο B μπορεί να εφαρμόσει το P_A για να αποκρυπτογραφήσει το δεύτερο μέρος του πακέτου, να το συγκρίνει με το πρώτο και να πιστοποιήσει την προέλευση του πακέτου. Κατόπιν χρησιμοποιεί το S_B προκειμένου να ανακτήσει το M.

3.1.2 Πρωτόκολλα Ιδιωτικού Κλειδιού - Ψηφιακές Υπογραφές

Τα πρωτόκολλα ιδιωτικού κλειδιού είναι αρκετά πιο απλά στην περιγραφή της βασικής ιδέας, πάλι χωρίς να μπούμε σε λεπτομέρειες υλοποίησης. Το μαθηματικό εργαλείο που χρησιμοποιούμε σε αυτήν την περίπτωση είναι μια συνάρτηση $M' = E_K(M)$ η οποία έχει την ιδιότητα: $E_K(E_K(M)) = M$. Το K σε αυτήν την περίπτωση είναι το ιδιωτικό κλειδί που ήδη μοιράζονται οι χρήστες A και B, γνωρίζουν μόνο αυτοί και χρησιμοποιούν για να έχουν ασφαλή και πιστοποιημένη επικοινωνία μεταξύ τους. Προκειμένου να επικοινωνήσουν οι A και B κρυπτογραφεί ο A το μήνυμα M με το K και ο B το αποκρυτογραφεί πάλι με το K.

Το ιδιωτικό κλειδί οι A και B μπορεί να το έχουν αποφασίσει πριν μπουν στο δίκτυο μέσω του οποίου θέλουν να συνομιλήσουν, να το αποφασίσουν μέσω ενός πρωτοκόλλου δημοσίου κλειδιού ή χρησιμοποιώντας κάποια λύση στο πρόβλημα Diffie Hellman που θα συζητήσουμε παρακάτω.

Οι Ψηφιακές Υπογραφές είναι ένας υπολογιστικά πιο εύκολος τρόπος να λειτουργήσει ένα πρωτόκολλο δημοσίου κλειδιού. Παρατηρούμε ότι για μια ασφαλή μετάδοση χρειάζονται δύο κρυπτογραφήσεις (η $E_{P_B}(M)$ και η $E_{S_A}(E_{P_B}(M))$ ενώ μπορούμε εύκολα να αποφύγουμε τη μια. Οι χρήστες A και B αρχικά συμφωνούν με ασφαλή τρόπο σε έναν αριθμό s ο οποίος θα καλείται η Ψηφιακή Υπογραφή του A. Έπειτα, όποτε θέλει ο A να στείλει ένα μήνυμα M στον B, θα παράγει το πακέτο $< M, s >$ και θα το κρυπτογραφεί μια φορά με το δημόσιο κλειδί του B. Ο B θα αποκρυπτογραφεί το πακέτο και θα πιστοποιεί την προέλευσή του απλά ελέγχοντας την ψηφιακή υπογραφή.

3.1.3 Το Πρόβλημα Diffie-Hellman

Δύο χρήστες A και B επικοινωνούν μέσω ενός μη-ασφαλούς καναλιού, που σημαίνει ότι κάποιος εξωτερικός παράγοντας μπορεί να 'ακούσει' τη συνομιλία τους. Το πρόβλημα Diffie-Hellman[10] είναι το πώς οι A και B θα μπορέσουν να καταλήξουν σε έναν κοινό αριθμό χωρίς να έχουν κάποια πληροφορία στη μνήμη τους εκ των προτέρον και χωρίς να μπορεί κάποιος που παρακολουθεί αυτή τη συνομιλία να αποσπάσει αυτόν τον αριθμό. Ιδανικά θα πρέπει οι A και B να παράγουν εσωτερικά κάποια τυχαία πληροφορία, να μοιραστούν μεταξύ τους μέρος της και μέσω κάποιου μαθηματικού εργαλείου να καταλήξουν στον ίδιο αριθμό.

Μια σχετικά προφανής λύση θα ήταν να εκκινήσουν και οι δύο ένα πρωτόκολλο δημοσίου κλειδιού μέσω του οποίου θα εμπιστευτεί ο ένας στον άλλον τον κοινό αριθμό. Μπορούμε ωστόσο να βρούμε αλγορίθμους που λύνουν το πρόβλημα πιο απλά και, κυρίως, χρησιμοποιώντας λιγότερους υπολογιστικούς πόρους. Στη συνέχεια θα παρουσιάσουμε μια λύση στο πρόβλημα Diffie-Hellman η οποία βασίζεται στο μαθηματικό μοντέλο των Ελλειπτικών Καμπύλων.

Μια επέκταση του προβλήματος Diffie-Hellman είναι το GDH (Diffie-Hellman Group Key Establishment). Σε αυτό το πρόβλημα έχουμε μια ομάδα χρηστών οι οποίοι θέλουν όλοι από κοινού να αποφασίσουν έναν κοινό αριθμό. Οι χρήστες μπορούν να επικοινωνούν όλοι απ΄ ευθείας μεταξύ τους ή τα κανάλια επικοινωνίας να περιγράφονται από κάποιο γράφημα, μοντέλο που είναι πιο κοντά στα Ασύρματα Δίκτυα Αισθητήρων. Θα παρουσιάσουμε μια λύση για αυτό το πρόβλημα η οποία βασίζεται επίσης στις Ελλειπτικές Καμπύλες και προϋποθέτει δύο πράγματα: πρώτον, υπάρχει ένας χρήστης σε αυτήν την ομάδα ο οποίος εκ των προτέρων είναι καθορισμένο ότι θα εκκινήσει αυτήν την διαδικασία και, δεύτερον, κάποιος εξωτερικός παράγοντας θα έχει ως στόχο μόνο να υποκλέψει την κοινή πληροφορία στην οποία καταλήγει αυτός ο αλγόριθμος και όχι να συμμετάσχει στην διαδικασία.

3.2 Ασφάλεια-Κρυπτογραφία στα Ασύρματα Δίκτυα Αισθητήρων - Τύποι Επιθέσεων

Διακρίνουμε τους εξωτερικούς παράγοντες που έχουν σκοπό να βλάψουν ένα Ασύρματο Δίκτυο Αισθητήρων σε *χαμηλών πόρων επιτιθέμενους* (mote-class attackers) και *υψηλών πόρων επιτιθέμενους* (laptop-class attackers) με βάση τους υπολογιστικούς και τηλεπικοιν-

ωνιακούς πόρους που διαθέτουν. Οι χαμηλών πόρων επιτιθέμενοι διαθέτουν τους ίδιους ή ανάλογους υπολογιστικούς πόρους με τους αισθητήρες του δικτύου. Ένας υψηλών πόρων επιτιθέμενος αντίθετα μπορεί να κάνει υπολογισμούς πολύ πιο γρήγορα από τους αισθητήρες του δικτύου (όχι κατ΄ ανάγκη και από την απόληξη) και μπορεί να πραγματοποιεί εκπομπές πολύ μεγαλύτερης εμβέλειας από τους αισθητήρες. Για παράδειγμα, μια επίθεση απέναντι στην οποία δεν υπάρχει άμυνα είναι η *denial-of-service attack* κατά την οποία μια συσκευή εκπέμπει συνεχώς με μεγάλη εμβέλεια στην ίδια συχνότητα που λειτουργούν οι αισθητήρες με αποτέλεσμα να μην μπορεί κανένας αισθητήρας να λάβει πληροφορία. Όταν θα σχεδιάζουμε ένα ασφαλές πρωτόκολλο θα θεωρούμε ότι πρέπει να ανταπεξέρχεται σε επιθέσεις από υψηλών πόρων επιτιθέμενους.

Θεωρούμε πάντα ότι η εξωτερική οντότητα που επιτίθεται έχει πλήρη επίγνωση του ορισμού και της λειτουργίας του πρωτοκόλλου που τρέχει στο δίκτυο, και με βάση αυτό προσπαθεί να επηρρεάσει τη λειτουργία του. Για παράδειγμα, μια αποτελεσματική επίθεση σε ένα απλό πρωτόκολλο που δημιουργεί ένα επικαλλυπτικό BFS δεντρο είναι να εκπέμψει ένας υψηλών πόρων επιτιθέμενος ένα $SEARCH$ μήνυμα με μεγάλη εμβέλεια και τιμή $dist = 0$ υποδυόμενος την απόληξη. Με αυτόν τον τρόπο, όλοι οι αισθητήρες θα θέσουν για πατέρα τους την απόληξη, άσχετα με το αν γειτονεύουν μαζί του ή όχι. Αν δεν γειτονεύουν (που είναι και η πιο συνηθισμένη περίπτωση), δεν θα είναι σε θέση να δρομολογήσουν πακέτα προς την απόληξη. Συγκεκριμένα, απέναντι σε εκπομπές μεγάλης εμβέλειας υπάρχει ένας απλός τρόπος άμυνας ο οποίος μπορεί να υλοποιηθεί και στο επίπεδο MAC. Κάθε εισερχόμενο μήνυμα για να γίνει αποδεκτό θα πρέπει να υπόκειται σε μία *τριπλή χειραψία* (three-way acknowledgment). Όταν μια (νόμιμη) συσκευή του δικτύου λάβει ένα μήνυμα από μια άλλη, απαντάει μέ μία επιβεβαίωση που περιέχει και έναν τυχαίο αριθμό. Κατόπιν, η πρώτη συσκευή πρέπει να απαντήσει και αυτή στην επιβεβαίωση με μία δική της επιβεβαίωση που περιέχει τον ίδιο τυχαίο αριθμό. Αν η πρώτη συσκευή ήταν νόμιμη αυτό σημαίνει ότι η απόσταση μεταξύ των δύο συσκευών είναι μικρότερη της εμβέλειας εκπομπής τους άρα θα είναι σε θέση να λάβει την πρώτη επιβεβαίωση και να απαντήσει. Αν όμως η πρώτη συσκευή είναι ένας υψηλών πόρων επιτιθέμενος ο οποίος πραγματοποιεί εκπομπή μεγάλης εμβέλειας, τότε δεν θα είναι σε θέση να λάβει την πρώτη επιβεβαίωση και έτσι δεν θα ξέρει τον τυχαίο αριθμό ωστε να είναι σε θέση να απαντήσει. Έτσι μια συσκευή μπορεί να γνωρίζει αν μια εκπομπή έχει έρθει από συσκευή που βρίσκεται εντός της εμβέλειας εκπομπής της οπότε και να τη δεχτεί ή από συσκευή που πραγματοποιεί εκπομπή μεγάλης εμβέλειας οπότε και να την απορρίψει.

Η επόμενη βασική διάκριση που κάνουμε είναι ανάμεσα στους *εσωτερικούς επιτιθέμενους* (inside-attackers) και στους *εξωτερικούς επιτιθέμενους* (outside-attackers. Οι εξωτερικοί επιτιθέμενοι δεν έχουν πρόσβαση στη μνήμη κανενός αισθητήρα και έτσι αν υιοθετούμε κάποια μέθοδο κρυπτογραφίας και πιστοποίησης τότε είναι πολύ δύσκολο να προκαλέσουν σοβαρό πρόβλημα. Οι εσωτερικοί επιτιθέμενοι αντίθετα θεωρούμε ότι έχουν πάρει υπό την κατοχή τους έναν (ή περισσότερους) αισθητήρες του δικτύου και έχουν αντιγράψει τη μνήμη του. Έτσι ο επιτιθέμενος θα είναι σε θέση να συμμετέχει στο δίκτυο σαν 'νόμιμο' μέλος ό,τι μέθοδο κρυπτογραφίας και πιστοποίησης χρησιμοποιούμε. Οι άμυνες που μπορούμε να εφαρμόσουμε έχουν σαν αποτέλεσμα μόνο τον περιορισμό της αρνητικής επίδρασης που μπορεί να επιφέρει ο επιτιθέμενος στο δίκτυο. Πρέπει να έχουμε υπόψιν μας ότι αυτός ο περιορισμός πρέπει επί της ουσίας να επιβάλλεται σε συσκευές του δικτύου που θεωρούνται 'νόμιμες ', άρα και στους αισθητήρες που έχουμε εμείς τοποθετήσει στο περιβάλλον. Αυτό δημιουργεί περίπλοκες καταστάσεις, για παράδειγμα, σε σενάρια εφαρμογών όπου υπάρχει κίνηση των

αισθητήρων, οπότε επιθυμούμε οποιαδήποτε δύο αισθητήρες να μπορούν να δημιουργούν ασφαλές κανάλι επικοινωνίας μεταξύ τους. Αυτό συνεπάγεται ότι θα αναγκαζόμαστε να επιτρέπουμε σε τυχόν εσωτερικούς επιτιθέμενους τη δυνατότητα να μετακινηθούν και να ανακτήσουν **όλα** τα κλειδιά κρυπτογράφησης του δικτύου.

Στην εργασία [17] βρίσκουμε έναν κατάλογο από πιθανές επιθέσεις που μπορεί κάποιος εξωτερικός παράγοντας να πραγματοποιήσει σε ένα Ασύρματο Δίκτυο Αισθητήρων:

1. **Spoofed, Altered, or Replayed Routing Information :** Η πιο άμεση επίθεση σε ένα πρωτόκολλο δρομολόγησης είναι να στοχοποιήσει κάποιος τις πληροφορίες δρομολόγησης που ανταλλάσονται μεταξύ των συσκευών. Κάποιος μπορεί αντιγράφοντας, αλλάζοντας ή επαναλαμβάνοντας πληροφορίες δρομολόγησης που ανταλλάσονται μεταξύ των συσκευών, να δημουργήσει κύκλους στις διαδρομές των πακέτων, να προσελκύει πάνω του ή να απωθεί πακέτα δεδομένων, να επιμηκύνει τις διαδρομές των πακέτων, να παράγει πλαστά μηνύματα σφαλμάτων παράδοσης, να διχοτομήσει το δίκτυο, να αυξήσει την καθυστέρηση παράδοσης των πακέτων, κλπ.

2. **Selective Forwarding :** Τα πρωτόκολλα που χρησιμοποιούν επικοινωνία μέσω πολλαπλών ενδιάμεσων κόμβων βασίζονται στη συνθήκη ότι κάθε συμμετέχον θα προωθεί όλα τα πακέτα που δέχεται στον προορισμό τους. Κάποιος επιτιθέμενος που συμμετέχει στο δίκτυο μπορεί να αρνείται να προωθήσει πακέτα δημιουργώντας ένα είδος 'μαύρης τρύπας ' στο δίκτυο. Ωστόσο αν κάποιος πραγματοποιήσει αυτήν την επίθεση είναι δυνατό οι γειτονικοί κόμβοι του δικτύου να αντιληφθούν αυτήν την κατάσταση και να σταματήσουν να τον εμπιστεύονται. Μια παραλλαγή της επίθεσης αυτής είναι ο επιτιθέμενος να προωθεί επιλεκτικά τα μηνύματα που δέχεται. Αν ο επιτιθέμενος έχει σαν στόχο να εκμηδενήσει ή να μεταβάλλει συγκεκριμένο μέρος της πληροφορίας που διακινείται στο δίκτυο, τότε μπορεί να προωθεί τα υπόλοιπα κανονικά μειώνοντας έτσι τις υποψίες που μπορεί να εγείρει στους γειτονικούς αισθητήρες.

3. **Sinkhole Attack :** Αυτή η επίθεση συμβαίνει όταν ο επιτιθέμενος προσπαθεί να προσελκύσει πάνω του όλη την πληροφορία που διακινείται σε ένα μέρος του δικτύου. Αν είναι σε θέση να το καταφέρει αυτό θα μπορεί να πραγματοποιήσει στη συνέχεια ένα πλήθος άλλων επιθέσεων που βλάπτουν τη λειτουργία του δικτύου, όπως για παράδειγμα την selective forwarding. Προκειμένου να το καταφέρει αυτό, ο επιτιθέμενος πρέπει να πείσει τους αισθητήρες αυτής της περιοχής ότι παρέχει ένα πολύ *ελκυστικό* μονοπάτι προς την απόληξη δημιουργώντας έτσι ένα μεταφορικό "sinkhole". Για παράδειγμα, ο επιτιθέμενος μπορεί να στέλνει μια διαφήμηση για μια πολύ υψηλής ποιότητας διαδρομής προς την απόληξη. Κάποια πρωτόκολλα ίσως να προσπαθήσουν να επαληθεύσουν την πολύ καλής ποιότητας διαδρομή προς την απόληξη. Σε αυτήν την περίπτωση, ένας υψηλών πόρων επιτιθέμενος ίσως όντως να μπορεί να παρέχει αυτό το υψηλής ποιότητας μονοπάτι πραγματοποιώντας μια εκπομπή μεγάλης εμβέλειας ή χρησιμοποιώντας ένα wormhole attack που θα αναλύσουμε στη συνέχεια. Αν ο επιτιθέμενος καταφέρει τον στόχο του, τότε οι γειτονικοί αισθητήρες θα τον εμπιστευτούν για να προωθούν τα μηνύματά τους και επιπλέον θα διαφημήσουν αυτό το υψηλής ποιότητας μονοπάτι και στο υπόλοιπο δίκτυο.

4. **Sybil Attack :** Σε αυτήν την επίθεση, ο επιτιθέμενος μπορεί να παρουσιάζει πολλαπλές ταυτότητες του εαυτού το στο δίκτυο. Έτσι μπορούν να επηρρεαστούν αρνητικά αλγοριθμικές προσεγγίσεις ανεκτικές σε σφάλματα όπως η δρομολόγηση σε

πολλαπλούς προορισμούς (multipath routing). Κάτι που οι αισθητήρες του δικτύου πιστεύουν πως είναι εναλλακτικές διαδρομές μπορεί να είναι η ίδια εξωτερική οντότητα. Αυτή η επίθεση μπορεί να προκαλέσει αρκετή ζημιά και σε πρωτόκολλα γεωγραφικής δρομολόγησης. Σε αυτά τα πρωτόκολλα, οι συσκευές δέχονται τις συντεταγμένες των γειτόνων τους με απλές μεταδόσεις και έτσι αποφασίζουν σε ποιον θα προωθήσουν κάθε πακέτο. Κάποιος επιτιθέμενος όμως με αυτήν την επίθεση μπορεί να βρίσκεται *σε πολλά σημεία ταυτόχρονα* και έτσι να προσελκύει μεγάλο μέρος πληροφορίας.

5. **Wormhole Attack :** Σε αυτήν την επίθεση ένας υψηλών πόρων επιτιθέμενος μπορεί να προωθεί όλα τα πακέτα πληροφορίας που λαμβάνει σε έναν άλλον υψηλών πόρων επιτιθέμενο μέσω μιας εκπομπής μεγάλης εμβέλειας σε ένα άλλο σημείο του δικτύου. Αν ο ένας από τους δύο επιτιθέμενους βρίσκεται κοντά στην απόληξη αυτό θα δημιουργήσει ένα sinkhole καθώς ο απομακρυσμένος επιτιθέμενος θα είναι σε θέση να διαφημίσει ένα τεχνητό μονοπάτι πολύ υψηλής ποιότητας προς την απόληξη. Η συγκεκριμένη επίθεση είναι σε θέση να επηρεάσει αρνητικά το δίκτυο ακόμα και αν χρησιμοποιούμε κρυπτογραφία και πιστοποίηση καθώς οι επιτιθέμενοι δεν χρειάζεται να αποκρυπτογραφούν τα μηνύματα αλλά προκαλούν ζημιά ακόμα και αν τα προωθούν ο ένας στον άλλον ως έχουν.

6. *HELLO* **Flood Attack :** Πολλά πρωτόκολλα βασίζονται σε πληροφορίες που ανταλάσσονται σε τοπικό επίπεδο για να προσδιορίσουν τον επόμενο γειτονικό κόμβο στη διαδρομή προς τον προορισμό ενός πακέτου δεδομένων, συνήθως την απόληξη. Ένας υψηλών πόρων επιτιθέμενος μπορεί να κάνει σε αυτές τις περιπτώσεις μια εκπομπή μεγάλης εμβέλειας διαφημίζοντας μια διαδρομή υψηλής ποιότητας προς την απόληξη. Αν οι αισθητήρες του δικτύου υιοθετήσουν για γείτονά τους τον επιτιθέμενο τότε το δίκτυο θα έχει μείνει σε κατάσταση σύγχησης. Ένα παράδειγμα τέτοιας επίθεσης το αναλύσαμε στην εισαγωγή αυτής της υποενότητας κατά τη δημιουργία ενός BFS επικαλυπτικού δέντρου. Παρόμοιες επιθέσεις γίνονται και σε πρωτόκολλα που βασίζονται στην περιοδική ανταλλαγή πληροφορίας δρομολόγησης. Παρατηρούμε ότι ακόμα και με χρήση απλής κρυπτογραφίας και πιστοποίησης στο πρωτόκολλο, ο επιτιθέμενος μπορεί ακόμα να προκαλέσει ζημιά στη λειτουργία του δικτύου επαναεκπέποντας με μεγάλη εμβέλεια κάποιο πακέτο πληροφορίας δρομολόγησης που έχει λάβει 'κοντά' στην απόληξη.

7. **Acknowledgment Spoofing :** Κάποια πρωτόκολλα δρομολόγησης βασίζονται στην παροχή επιβεβαίωσης πακέτων για κάθε εκπομπή πληροφορίας προκειμένου ο αποστολέας να διαπιστώσει εάν ένας σύνδεσμος είναι ενεργός ή αν είναι υψηλής ποιότητας. Σε αυτές τις περιπτώσεις, ένας επιτιθέμενος μπορεί να στέλνει ψεύτικες επιβεβαιώσεις κάνοντας έναν αισθητήρα να πιστεύει πως κάποιος σύνδεσμος ή κάποιος αισθητήρας είναι ενεργός τη στιγμή που δεν είναι. Κατόπιν, από τη στιγμή που ο επιτιθέμενος θα είναι σε θέση να διαφημίσει έναν ψεύτικο ς ως υψηλής ποιότητας, θα μπορεί να τραβήξει μεγάλο μέρος πληροφορίας προς αυτό και να πραγματοποιήσει ένα selective forwardink attack.

3.3 Ελλειπτικές Καμπύλες

3.3.1 Εισαγωγικές Γνώσεις

Σε αυτήν την ενότητα θα δούμε κάποιες βασικές ιδέες που σχετίζεται με τις Ελλειπτικές Καμπύλες και τον ορισμό τους πάνω σε πεπερασμένα πεδία. Ο ενδιαφερόμενος αναγνώστης μπορεί να βρει περισσότερες πληροφορίες στα [4, 24]. Υποθέτουμε επίσης ένα βαθμό εξοικείωσης με βασική θεωρία αριθμών (βλ. [6]). Οι ελλειπτικές καμπλύλες συνήθως ορίζονται πάνω σε δυαδικά πεδία $F_{2^m}(m \geq 1)$, ή πάνω σε πεδία πρώτων αριθμών $F_p(p > 3)$. Συνήθως στις εφαρμογές κρυπτογραφίας χρησιμοποιούνται ελλειπτικές καμπύλες που ορίζονται πάνω σε πεδία πρώτων αριθμών.

Μια *ελλειπτική καμπύλη* $E(F_p)$ πάνω σε ένα πεπερασμένο πεδίο F_p. όπου $p > 3$ και πρώτος, είναι το σύνολο των σημείων $(x, y) \in F_p$ τα οποία ικανοποιούν την εξήσωση:

$$y^2 = x^3 + ax + b$$

όπου $a, b \in F_p$ είναι τέτοια ώστε $4a^3 + 27b^2 \neq 0$. Το σύνολο των λύσεων (x, y) της εξίσωσης μαζί με ένα σημείο $\mathcal{O}$, το οποίο ονομάζεται σημείο απειρίας, και έναν ειδικό τελεστή πρόσθεσης ορίζουν μια Αβελιανή ομάδα, η οποία ονομάζεται *ομάδα Ελλειπτικής Καμπύλης*. Το σημείο $\mathcal{O}$ λειτουργεί ως το στοιχείο ταυτότητας (για τον ορισμό της πρόσθεσης βλ. [4, 24]).

Η τάξη m μιας ελλειπτικής καμπύλης είναι ο αριθμός των σημείων στην $E(F_p)$. Η τάξη ενός σημείου P είναι ο μικρότερος θετικός ακέραιος n έτσι ώστε $nP = \mathcal{O}$. Η εφαρμογή του θεωρήματος του Langrange (βλ [6]) στην $E(F_p)$, αποδεικνύει ότι η τάξη ενός σημείου $P \in E(F_p)$ πάντα διαιρεί την τάξη της ομάδας ελλειπτικής καμπύλης, άρα $mP = \mathcal{O}$ για κάθε σημείο $P \in E(F_p)$, το οποίο δείχνει επίσης ότι η τάξη ενός σημείου δεν μπορεί να ξεπεράσει την τάξη της ελλειπτικής καμπύλης.

Η ασφάλεια των συστημάτων που βασίζονται στις ελλειπτικές καμπύλες βασίζεται στη δυσκολία επίλυσης του προβλήματος διακριτού λογαρίθμου (discrete logarithm problem, DLP) στις ομάδες ελλειπτικής καμπύλης. Το πρόβλημα διακριτού λογαρίθμου στις ελλειπτικές καμπύλες (ECDLP) είναι να προσδιοριστεί ο ελάχιστος θετικός ακέραιος k ο οποίος ικανοποιεί την εξίσωση $Q = kP$ για δύο γνωστά σημεία Q και P σε μια ομάδα ελλειπτικής καμπύλης. Ένας χρήστης A σε συστήματα κρυπτογραφίας μπορεί να διαλέξει έναν τυχαίο ακέραιο $0 < k < p - i$ και να στείλει το Q σε έναν χρήστη B με τον οποίο θέλει να επικοινωνήσει με ασφαλή τρόπο. Το δημόσιο κλειδί του A είναι το Q και το ιδιωτικό κλειδί του είναι το k. Έπειτα μπορεί να εφαρμοστεί ένας αλγόριθμος κρυπτογράφησης (βλ. ElGamal encryption [12]) έτσι ώστε ο B να μπορεί να κρυπτογραφεί το μήνυμα που θέλει να στείλει στον A με το δημόσιο κλειδί Q και ο A να το αποκρυπτογραφεί χρησιμοποιόωντας το ιδιωτικό κλειδί του k.

3.3.2 Λύση του Προβλήματος Diffie-Hellman με χρήση Ελλειπτικών Καμπύλων

Τώρα είμαστε σε θέση να λύσουμε το πρόβλημα Diffie-Hellman χρησιμοποιώντας τις ελλειπτικές καμπύλες. Η λύση που παρουσιάζουμε βασίζεται στο γεγονός ότι δεδομένων δύο σημείων σε ελλειπτική καμπύλη P_1 και P_2, είναι υπολογιστικά πολύ δύσκολο να υπολογιστεί το $\frac{P_1}{P_2}$. Έστω λοιπόν δύο χρήστες A και B οι οποίοι θέλουν να καταλήξουν σε ένα

κοινό σημείο μέσω ενός μη-ασφαλούς καναλιού. Οι χρήστες παράγουν με τυχαίο τρόπο τις πληροφορίες $< c_A, P_A >$ και $< c_B, P_B >$ αντίστοιχα όπου c_A και c_B ακέραιοι και P_A και P_B σημεία σε ελλειπτική καμπύλη. Ο A υπολογίζει το σημείο $\frac{P_A}{c_A}$ και το στέλνει στον B ενώ ο B υπολογίζει το $\frac{P_B}{c_B}$ και το στέλνει στον B. Κατόπιν, ο A παράγει το $\frac{P_A P_B}{c_B}$ και το στέλνει στον B ενώ ο B παράγει το $\frac{P_A P_B}{c_A}$ και το στέλνει στον A. Στο τέλος, ο A πολλαπλασιάζει την ποσότητα που μόλις έλαβε από τον B με το c_A και ανακτάει το $S = P_A P_B$ ενώ ο B πολλαπλασιάζει την ποσότητα που μόλις έλαβε από τον A με το c_B και ανακτάει επίσης το $S = P_A P_B$. Παρατηρούμε ότι οι δύο χρήστες καταλήξανε στο ίδιο σημείο S χωρίς αυτό να εξαρτάται από τους c_A και c_B. Αυτό είναι πολύ βολικό σε περιπτώσεις που οι A και B ανήκουν αρχικά σε δύο διαφορετικές ομάδες με τα P_A και P_B να έχουν αποφασιστεί από κοινού σε κάθε ομάδα και θέλουν να καταλήξουν σε ένα κοινό κλειδί μεταξύ των δύο ομάδων διότι κάθε ζευγαρι χρηστών από τις δύο ομάδες αν ακολουθήσει αυτόν τον αλγόριθμο θα καταλήξει στο ίδιο σημείο S.

3.3.3 Λύση του GDH με χρήση Ελλειπτικών Καμπύλων - Περίπτωση (Εικονικού) Δακτυλίου

Έστω ότι έχουμε n συσκευές $M_1, M_2, \cdots, M_n$ συνδεδεμένες σε ένα δίκτυο δακτυλίου (για την ακρίβεια δεν μας ενδιαφέρει να συνδέεται το M_n με το M_1). Χρησιμοποιώντας τις ελλειπτικές καμπύλες μπορούμε να εφαρμόσουμε έναν αλγόριθμο προκειμένου όλες οι συσκευές να καταλήξουν στο ίδιο σημείο ελλειπτικής καμπύλης. Θα περιγράψουμε ένα πρωτόκολλο που παρουσιάζεται στην εργασία [9] και που αποτελεί βελτίωση ενός πρωτοκόλλου που παρουσιάζεται στην εργασία [26]:

1. Στην πρώτη φάση κάθε συσκευή M_i του δικτύου δημιουργεί μια τυχαία μυστική ακέραια ποσότητα k_i. Η συσκευή M_1 επιλέγει ένα σημείο P και στέλνει στην M_2 το σημείο $Q_1 = k_1 P$ το οποίο είναι το δημόσιο κλειδί του και μπορεί να χρησιμοποιηθεί από την M_2. Έπειτα, η M_2 στέλνει στην M_3 το σημείο $Q_2 = k_1 k_2 P$ (το οποίο είναι το δημόσιο κλειδί της M_2) και συνεχίζουμε με αυτόν τον τρόπο μέχρις ότου το πρωτόκολλο να φτάσει την συσκευή M_n.

2. Στη δεύτερη φάση η συσκευή M_n κρυπτογραφεί το Q_n με το δημόσιο κλειδί της M_{n-1} : Q_{n-1} και το στέλνει στην M_{n-1}. Η συσκευή M_{n-1} μπορεί να αποκρυπτογραφήσει το μήνυμα με το ιδιωτικό της κλειδί k_{n-1}, να ανακτήσει τη μυστική τιμή Q_n, να την κρυπτογραφήσει με το δημόσιο κλειδί της M_{n-2} και να στείλει το αποτέλεσμα στην M_{n-2}. Η ίδια διαδικασία συνεχίζεται μέχρις ότου το πρωτόκολλο να φτάσει στη συσκευή M_1.

Με αυτή τη διαδικασία κάθε συσκευή θα ενεργοποιηθεί ακριβώς δύο φορές και θα πραγματοποιήσει ακριβώς δύο μεταδόσεις. Στο τέλος όλες οι συσκευές του δακτυλίου θα κατέχουν το Q_n που θα είναι το διαμοιρασμένο κλειδί όλων των συσκευών. Παρατηρούμε ότι αυτό το πρωτόκολλο λειτουργεί για τοπολογία δακτυλίου αλλά μπορεί πολύ εύκολα να λειτουργήσει και στην περίπτωση όπου κάθε συσκευή έχει απ΄ ευθείας επικοινωνία με όλες τις άλλες.

3.3.4 Λύση του GDH με χρήση Ελλειπτικών Καμπύλων - Περίπτωση Γενικού Δικτύου

Τώρα θα εξετάσουμε την περίπτωση του γενικού δικτύου, δηλαδή την περίπτωση όπου ο τρόπος με τον οποίον συνδέονται οι συσκευές περιγράφεται από ένα γράφημα. Η γενική ιδέα είναι ότι μέσω ενός αλγόριθμου διάτρεξης DFS που περιγράψαμε στο 2.1 θα ενεργοποιηθεί μια φορά κάθε συσκευή και θα συνεισφέρει στη δημιουργία του διαμοιρασμένου κοινού κλειδιού όπως και στην περίπτωση του δακτυλίου. Έπειτα, χρησιμοποιώντας τα δημόσια κλειδιά κάθε συσκευής που θα έχουν προκύψει, θα ενημερωθούν όλες οι συσκευές για το τελικό κλειδί. Η διαδικασία επί της ουσίας είναι η μεταφορά του αλγόριθμου για τα δίκτυα δακτυλίου στα γενικά δίκτυα.

Κάθε συσκευή $M_1, M_2, \cdots, M_n$ στο δίκτυο υπολογίζει μια τυχαία μυστική ποσότητα k_i ενώ η συσκευή M_1 επιλέγει ένα σημείο P και υπολογίζει το σημείο $Q_1 = k_1 P$ το οποίο είναι το δημόσιο κλειδί της. Κατόπιν, με βάση κάποιον κατανεμημένο αλγόριθμο διάτρεξης που επισκέπτεται όλους τους συμμετέχοντες του δικτύου τουλάχιστον μια φορά, και συγκεκριμένα έναν κατανεμημένο αλγόριθμο διάτρεξης προτεραιότητας *κατά βάθος* (δηλαδή ένα DFS traversal) στέλνει το Q_1 στη συσκευή M_2 η οποία είναι γειτονική συσκευή μέσω ενός ειδικού $SEARCH < M_2, Q_1 >$ μηνύματος. Όταν η συσκευή M_2 λάβει το μήνυμα, ενεργοποιείται για πρώτη φορά, θεωρεί ότι την έχει επισκευτεί ο αλγόριθμος και θέτει τη συσκευή M_1 ως τον πατέρα της (θα λέμε ότι η συσκευή M_2 συμμετέχει στον αλγόριθμο διάτρεξης). Επιπλέον, όταν η συσκευή M_2 είναι ενεργή, υπολογίζει το σημείο $Q_2 = k_1 k_2 P$ (το οποίο είναι το δημόσιο κλειδί της συσκευής M_2) και μεταφέρει τον έλεγχο σε μια συσκευή M_3 την οποία δεν έχει επισκεφτεί ακόμα ο αλγόριθμος, μέσω ενός ειδικού $SEARCH < M_3, Q_2 >$ μηνύματος.

Όταν το πρωτόκολλο φτάσει τη συσκευή M_u ενώ έχει ήδη επισκευτεί όλους τους γείτονές της, τότε η συσκευή M_u κρυπτογραφεί το Q_u με το δημόσιο κλειδί της συσκευής M_{u-1}, δηλαδή το Q_{u-1}, και το στέλνει στη συσκευή M_{u-1} χρησιμοποιώντας ένα ειδικό $PARENT < M_{u-1}, E_{Q_{u-1}}(Q_u) >$ μήνυμα [1]. Η συσκευή M_{u-1} μπορεί να αποκρυπτογραφήσει το μήνυμα με το ιδιωτικό κλειδί της k_{u-1}, να ανακτήσει τη μυστική τιμή M_u και είτε να συνεχίσει τον κατανεμημένο αλγόριθμο διάτρεξης μεταφέροντας τον έλεγχο στην επόμενη γειτονική συσκευή που δεν έχει ακόμα επισκευτεί ο αλγόριθμος (εαν υπάρχει), πάλι μέσω ενός ειδικού $SEARCH < M_{u+1}, Q_u >$ μηνύματος ή αν ο αλγόριθμος έχει επισκευτεί όλους τις γειτονικές συσκευές, να στείλει ένα $PARENT < M_{u-2}, E_{Q_{u-2}}(Q_u) >$ μηνύματος στον πατέρα της. Αυτή η διαδικασία συνεχίζεται μέχρις ότου το πρωτόκολλο να φτάσει την τελευταία συσκευή του δικτύου M_n η οποία υπολογίζει το σημείο Q_n που είναι το διαμοιρασμένο μυστικό κλειδί του δικτύου. Με τρόπο παρόμοιο με τη συσκευή M_u, η M_n κρυπτογραφεί το Q_n με το δημόσιο κλειδί της M_{n-1}, δηλαδή το Q_{N-1}, και το στέλνει στη συσκευή M_{n-1} (τον πατέρα της) χρησιμοποιώντας ένα ειδικό $PARENT < M_{n-1}, E_{Q_{n-1}}(Q_n) >$ μήνυμα.

Στην περίπτωση που η συσκευή M_u έχει περισσότερα του ενός παιδιών (στο DFS δέντρο), αφού λάβει το $PARENT$ μήνυμα από το τελευταίο παιδί που κατέχει το διαμοιραζόμενο κλειδί, πρώτα στέλνει το $PARENT < M_{u-1}, E_{Q_{u-1}}(Q_n) >$ μήνυμα στον πατέρα της και μετά ενημερώνει τα παιδιά της στέλνοντας ένα ειδικό $UPDATE < M_i, E_{Q_u}(Q_n) >$ μήνυμα. Το παιδί M_i που λαμβάνει ένα $UPDATE$ μήνυμα, το αποκρυπτογαφεί για να ανακτήσει το διαμοιραζόμενο κλειδί και το προωθεί στα παιδιά του στέλνοντας ένα $UPDATE <$

[1] Όπως και στις προηγούμενες υποενότητες, το $E_K(M)$ σημαίνει ότι κρυπτογραφούμε το μήνυμα M με το κλειδί K

$M_{i+1}, E_{Q_i}(Q_n) >$ μήνυμα. Αυτό διασφαλίζει ότι το διαμοιραζόμενο κλειδί θα διατρέξει το DFS δέντρο μέχρι τη συσκευή M_1 αλλά θα φτάσει επίσης όλους τους κόμβους που ανήκουν στο δέντρο, άρα και στο δίκτυο.

Η υλοποίηση αυτής της τεχνικής διάτρεξης απαιτεί από την ενεργή συσκευή να γνωρίζει ακριβώς ποιες από τις γειτονικές συσκευές έχει επισκευτεί ο αλγόριθμος. Προκειμένου να το επιτύχουμε αυτό, ο κατανεμημένος αλγόριθμος εκτός από τα $SEARCH$ και $PARENT$ μηνύματα, χρησιμοποιεί ένα ειδικό $VISITED$ μήνυμα που επιτρέπει σε κάθε συσκευή να ενημερώσει τους γείτονές της (εκπέμπωτας το μήνυμα) ότι έχει συμμετάσχει στη διάτρεξη.

3.4 Δημιουργία Ασφαλούς Δέντρου Επικοινωνιών σε Ασύρματα Δίκτυα Αισθητήρων

Το πρωτόκολλο που θα περιγράψουμε [11] δημιουργεί μια δομή επικαλυπτικού δέντρου σε ένα Ασύρματο Δίκτυο Αισθητήρων με τέτοιον τρόπο ώστε να μην μπορεί κάποια εξωτερική οντότητα να παρέμβει με βλαβερό τρόπο κατά τη δημιουργία του δικτύου και να υπάρχει η δυνατότητα για ασφαλή επικοινωνία προς την απόληξη με τον τρόπο που αναλύσαμε στο 2.1. Ο αλγόριθμος αποτελεί μια επέκταση πάνω στον 'αφελή' αλγόριθμο δημιουργίας DFS επικαλυπτικού δέντρου. Χρησιμοποιείται μια σειρά από μαθηματικά εργαλεία κρυπτογραφίας που και πάλι δεν αναλύονται όσον αφορά στην υλοποίηση. Στη συνέχεια θα παρουσιάσουμε τον τρόπο που αυτή η προσέγγιση αντιμετωπίζει τις βασικές επιθέσεις που αναλύσαμε παραπάνω στο 3.2.

3.4.1 Το Μοντέλο

Το μοντέλο αυτού του αλγορίθμου περιλαμβάνει τα εξής:

- Το μοντέλο επικοινωνίας είναι η επικοινωνία μέσω πολλαπλών ενδιάμεσων κόμβων, δηλαδή οι συσκευές κάνουν εκπομπές με μια προκαθορισμένη εμβέλεια r.
- Οι συσκευές παραμένουν ακίνητες σε όλη τη διάρκεια λειτουργίας του δικτύου και οι συνδέσεις μεταξύ των συσκευών δεν χαλάνε.
- Υπάρχει μια μοναδική απόληξη η οποία έχει σημαντικά περισσότερες υπολογιστικές δυνατότητες από τους αισθητήρες.
- Για μια (σύντομη) χρονική περίοδο στην έναρξη λειτουργίας του πρωτοκόλλου δεν υπάρχει κίνδυνος επίθεσης του δικτύου από εξωτερικές οντότητες.

3.4.2 Συμβολισμοί

Από εδώ και στο εξής θα χρησιμοποιούμε τους εξής συμβολισμούς:

M_1, M_2 : Συνένωση των μηνυμάτων M_1 και M_2

$E_K(M)$: Κρυπτογράφηση του μηνύματος M χρησιμοποιώντας το κλειδί K

$MAC_K(M)$: Κωδικός Ταυτοποίησης Μηνύματος (Message Authentication Code) του μηνύματος M χρησιμοποιώντας το κλειδί K

N_i : Τυχαίος Αριθμός που χρησιμοποιείται μόνο από τη συσκευή i

K_{ij} : Συμμετρικό (pairwise) κλειδί το οποίο μοιράζονται οι συσκευές i και j

K_i^G : Ένα κλειδί ομάδας (group key) το οποίο χρησιμοποιεί η συσκευή i για να εκπέμψει με ασφαλή τρόπο ένα μήνυμα σε όλους τους γείτονές της

3.4.3 Προσδιορισμός Κλειδιών

Θεωρούμε ότι υπάρχει ένα Master Key το οποίο έχουμε φορτώσει στη μνήμη όλων των αισθητήρων πριν από την τοποθέτησή τους στο δίκτυο. Υπενθυμίζουμε ότι για ένα χρονικό διάστημα, το δίκτυό μας θεωρείται ασφαλές από εξωτερικές παρεμβάσεις οπότε δεν φοβόμαστε μήπως κάποιος εξωτερικός παράγοντας αποκτήσει το Master Key, το οποίο οι αισθητήρες είναι προγραμματισμένοι να το σβήσουν από τη μνήμη τους αφού το χρησιμοποιήσουν. Μια συσκευή που κατέχει το Master Key μπορεί να κατασκευάσει όλα τα κλειδιά που θα χρησιμοποιηθούν στο δίκτυο, δηλαδή και τα K_{ij} και τα K_i^G αρκεί να ξέρει τις ταυτότητες των συσκευών που εμπλέκονται. Δηλαδή υπάρχει μια συνάρτηση $F(K_m, i, j) = K_{ij}$ που παράγει το διαμοιρασμένο (pairwise) κλειδί δύο συσκευών i και j. Επίσης υπάρχει μια συνάρτηση $F(K_m, i) = K_i^G$ που παράγει το κλειδί γειτονιάς (group key) της συσκευής i.

Σε πρώτη φάση κάθε συσκευή i ανιχνεύει τους γείτονές της μέσω απλών Beacon και Beacon_Reply μηνυμάτων. Κατόπιν, για κάθε γείτονα παράγει μονομερώς ένα διαμοιρασμένο κλειδί (αξίζει να παρατηρήσουμε ότι τόσο η συσκευή i όσο και η συσκευή j θα καταλήξουν στο ίδιο διαμοιρασμένο κλειδί K_{ij} σε περίπτωση που γειτονεύουν) καθώς και το κλειδί γειτονιάς : K_i^G. Από τη στιγμή που έχουν δημιουργηθεί τα κλειδιά που θα απασχολήσουν τους αισθητήρες του δικτύου, το K_m δεν χρειάζεται πλέον (για την ακρίβεια είναι επικίνδυνο να διατηρηθεί στη μνήμη) οπότε και σβήνεται από τη μνήμη των αισθητήρων. Από αυτήν την στιγμή το δίκτυό μας θεωρείται ότι δεν είναι ασφαλές, δηλαδή πρέπει να περιμένουμε ότι κάποιος θα προσπαθεί να υποκλέψει πληροφορίες που ανταλάσσονται στο δίκτυο, να επηρρεάσει τη λειτουργία του δικτύου εκπέμποντας ο ίδιος, στη χειρότερη περίπτωση να καταφέρει να αποσπάσει κάποιο κλειδί και έτσι να συμμετέχει στο δίκτυο ή να καταλάβει μια συσκευή και να αντιγράψει τη μνήμη της και όλα τα κλειδιά και έτσι να προσπαθήσει να επηρρεάσει το δίκτυο. Σε δεύτερη φάση, κάθε αισθητήρας χρησιμοποιεί τα διαμοιρασμένα κλειδιά για να εκμυστηρευτεί στους γείτονές του το κλειδί γειτονιάς του. Συγκεκριμένα, στέλνει το εξής μήνυμα σε όλους τους γείτονες του:

$$Sensor_i : c = E_{K_{ij}}(\text{“}Groupkey\text{''}, K_i^G),$$

$$\tau = MAC_{K_{ij}}(ID_i, ID_j, c)$$

$$Sensor_i \rightarrow Sensor_j : ID_i, ID_j, c, \tau$$

Με αυτόν τον τρόπο παρέχονται σε κάθε γείτονα ενός αισθητήρα i με κρυπτογράφηση και πιστοποίηση το κλειδί γειτονιάς K_i^G. Άρα από εδώ και στο εξής θα μπορούν οι αισθητήρες να πραγματοποιούν ασφαλείς εκπομπές στους γειτονικούς αισθητήρες.

3.4.4 Δημιουργία του Ασφαλούς Δέντρου Επικοινωνιών

Η πιο απλή λύση σε αυτό το σημείο για να δημιουργηθεί με ασφαλή τρόπο ένα BFS δέντρο στο δίκτυο ξεκινώντας από την απόληξη θα ήταν να παρέχεται πιστοποίηση για κάθε

$SEARCH$ μήνυμα και κατά τα άλλα να λειτουργήσει ακριβώς ο ίδιος αλγόριθμος. Χρειαζόμαστε μόνο πιστοποίηση και όχι κρυπτογράφηση διότι ο κίνδυνος δεν είναι να υποκλαπούν πληροφορίες, αλλά να παραπλανηθούν κάποιοι αισθητήρες σχετικά με τα μηνύματα που λαμβάνουν. Δηλαδή η απόληξη να στείλει το παρακάτω μήνυμα:

$$sink \rightarrow Neighbors : N_{sink}, (ID_{sink}, dist_{sink} = 0), MAC_{K^G_{sink}}(N_{sink}, ID_{sink}, dist_{sink} = 0).$$

Οι γείτονες της απόληξης λαμβάνοντας αυτό το μήνυμα θα μπορούν όντως να πιστοποιήσουν ότι προέρχεται από την απόληξη και έτσι θα το θέσουν ως πατέρα τους στο επικαλυπτικό δέντρο και θα θέσουν $dist = 1$. Κατόπιν, οι αισθητήρες στέλνουν τα $SEARCH$ μηνύματά τους με ανάλογο τρόπο:

$$Sensor_i \rightarrow Neighbors : N_i, (ID_i, dist_i), MAC_{K^G_i}(N_i, ID_i, dist_i).$$

Η διαδικασία συνεχίζεται όπως και στο 2.1.

Κάποιος εξωτερικός παράγοντας δεν μπορεί να στείλει ένα πιστοποιημένο μήνυμα μπερδεύοντας έτσι τους υπόλοιπους αισθητήρες, αλλά αν ένας αισθητήρας έχει καταληφθεί από εξωτερικό παράγοντα ο οποίος έχει αντιγράψει τα περιεχόμενα της μνήμης του μπορεί να στείλει πιστοποιημένα $SEARCH$ μηνύματα με τιμή $dist$ κατά πολύ μικρότερη από την πραγματική, προσανατολίζοντας ένα μεγάλο μέρος του δικτύου να δρομολογεί στη συνέχεια πακέτα προς αυτόν. Προκειμένου να αμυνθούμε απέναντι σε αυτήν την επίθεση υιοθετούμε την εξής τεχνική η οποία παρουσιάζεται στο πρωτόκολλο μ-TESLA [22]:

Επιστρατεύουμε μια μονής κατεύθυνσης αλυσίδα κλειδιών η οποία είναι μια λίστα $k_0, k_1, \cdots, k_n$ τέτοια ώστε:

$$\forall l, 0 < l < n, k_{l-1} = f(k_l),$$

όπου η f είναι μια ασφαλής ψευδοτυχαία συνάρτηση η οποία είναι υπολογιστικά δύσκολο να αντιστραφεί. Κάθε αισθητήρας έχει στη μνήμη του το k_0 από πριν την τοποθέτηση ενώ ολόκληρη η λίστα είναι γνωστή μόνο στην απόληξη. Έτσι μια συσκευή που γνωρίζει το k_i μπορεί να επαληθεύσει ότι το k_j είναι στοιχείο της αλυσίδας για $i < j$ εφαρμόζοντας τη συνάρτηση $f()$ $j - i$ φορές, αλλα δεν μπορεί να παράγει το k_j από μόνη της.

Η δημιουργία του δέντρου λοιπόν γίνεται σε φάσεις οι οποίες διαρκούν μια συγκεκριμένη χρονική περίοδο (time interval) η οποία αρκεί για να φτάσει ένα πακέτο στον πιο απομακρυσμένο αισθητήρα του δικτύου. Ένας αισθητήρας θα δεχτεί ένα μήνυμα $SEARCH$ ως έγκυρο μόνο αν η τιμή της $dist$ που θα θέσει συμπίμπτει με την αντίστοιχη χρονική περίοδο. Κατά την πρώτη χρονική περίοδο, η απόληξη στέλνει στους γείτονές της το $SEARCH$ μήνυμα μαζί με το στοιχείο k_1. Οι γείτονές της απόληξης αποκρυπτογραφούν το μήνυμα με το K^G_{sink} ελέγχουν την εγκυρότητα του k_1 και θέτουν για πατέρα τους την απόληξη. Από εκεί και πέρα, κατά την i-οστή χρονική περίοδο, η απόληξη δημιουργεί ένα μήνυμα με το k_i, όσοι αισθητήρες έχουν θέσει πατέρα απλώς προωθούν το μήνυμα προς τους γείτονές τους και οι πρώτοι που λαμβάνουν αυτό το μήνυμα χωρίς να έχουν θέσει πατέρα (εκείνοι που έχουν απόσταση i από την απόληξη) ελέγχουν την εγκυρότητα του μηνύματος (εφαρμόζοντας i φορές την f στο k_i) και θέτουν για πατέρα τους τον αισθητήρα από το οποίο έλαβαν το μήνυμα.

Αυτή η τεχνική μας προστατεύει από εσωτερικές επιθέσεις καθώς κάποιος που έχει ήδη καταλάβει μια συσκευή η οποία βρίσκεται σε απόσταση i από την απόληξη και συνεπώς κάποια

στιγμή μαθαίνει το k_i δεν μπορεί να στείλει ένα $SEARCH$ μήνυμα με τιμή $dist$ μεγαλύτερη i καθώς δεν μπορεί να παράγει το $k_j, j > i$ και δεν μπορεί να στείλει μήνυμα $SEARCH$ με τιμή μικρότερη του i το οποίο να γίνει αποδεκτό καθώς τη στιγμή που θα ανακτήσει το k_i θα έχουν ήδη περάσει τις αντίστοιχες χρονικές περιόδους για τους αισθητήρες των μικρότερων αποστάσεων από την απόληξη

3.4.5 Ανάλυση Ασφάλειας

Τώρα θα αναλύσουμε πώς το πρωτόκολλο ανταποκρίνεται στις επιθέσεις που περιγράψαμε στο 3.2:

- **Spoofed, Altered, Replayed Routing Information :** Αυτή η επίθεση στοχεύει στην ανταλλαγή πληροφορίας μεταξύ των συσκευών του δικτύου. Απο τη στιγμή που χρησιμοποιείται κρυπτογραφία και πιστοποίηση τότε δεν θα υπάρχει κάποιο πρόβλημα.

- **Spoofed, Altered, Replayed Routing Information :** Αυτού του είδους η επίθεση είναι πολύ δύσκολο να αντιμετωπιστεί καθώς πρέπει να περιμένουμε ότι μια συσκευή η οποία έχει καταληφθεί από κάποιον επιτιθέμενο θα έχει τη δυνατότητα να συμμετέχει στο δίκτυο. Θα ήταν χρήσιμο εάν ο αμέσως επόμενος παραλήπτης στη διαδρομή ενός πακέτου επιλεγόταν πιθανοτικά, αλλά η δομή δέντρου που χρησιμοποιείται δεν επιτρέπει κάτι τέτοιο. Μια λύση θα ήταν η δημιουργία πολλών δέντρων με ρίζα την απόληξη οπότε και θα μπορούσαν να υπάρχουν περισσότερες της μιας διαδρομής προς την απόληξη.

- **Sinkhole and Wormhole Attacks :** Οι συγκεκριμένες επιθέσεις απειλούν το δίκτυο μόνο κατά τη φάση προσδιορισμού των κλειδιών η οποία έχει πολύ μικρή διάρκεια και κατά την οποία έχουμε ήδη αποσαφηνίσει ότι δεν περιμένουμε να δεχτούμε επίθεση. Από εκεί και πέρα κάθε αισθητήρας απλώς προωθεί τα πακέτα του στον *πατέρα* του στο BFS δέντρο και δεν μπορεί να παραπλανηθεί από ψεύτικες διαφημίσεις διαδρομών υψηλής ποιότητας προς την απόληξη.

- **Sybil Attacks :** Και πάλι το γεγονός ότι μετά τη φάση αρχικοποίησης οι αισθητήρες εμπιστεύονται μόνο έναν κόμβο του δικτύου για να προωθήσουν τα πακέτα τους μας προστατεύει από αυτήν την επίθεση. Ακόμα και εαν ο επιτιθέμενος έχει καταλάβει κάποιον αισθητήρα, παρουσιάζοντας πολλαπλές ταυτότητες δεν θα έχει μεγαλύτερο πλεονέκτημα να βλάψει τη λειτουργία του δικτύου.

- **Hello Flood Attacks and Acknowledgment Spoofing :** Αυτή η επίθεση εφαρμόζεται κατά τη δημιουργία ενός BFS δέντρου αλλά στην περίπτωση αυτού του πρωτόκολλου χρησιμοποιείται πιστοποίηση, άρα και δεν είναι σε θέση να βλάψει τη λειτουργία του δικτύου.

Κεφάλαιο 4

Ένα Καινούριο Προσαρμοστικό, Πιθανοτικό, Ασφαλές Πρωτόκολλο Δρομολόγησης

Σε αυτό το κεφάλαιο παρουσιάζουμε την καινούρια μας δουλειά. Πρόκειται περί ενός πρωτόκολλου δρομολόγησης το οποίο είναι ασφαλές σε όλη τη διάρκεια της εκτέλεσής του και ανταποκρίνεται ακόμα και σε σενάρια κίνησης των συσκευών. Έπειτα από μια σύντομη εισαγωγή προχωράμε στην περιγραφή του μοντέλου, στη συνέχεια σε μια υψηλού επιπέδου ανάλυση του πρωτοκόλλου, έπειτα στην ανάλυση της φάσης αρχικοποίησης η οποία χωρίζεται με τη σειρά της σε τέσσερις επιπλέον φάσεις, κατόπιν περιγράφουμε το βασικό μηχανισμό δρομολόγησης, επιπλέον παρουσιάζουμε τους μηχανισμούς προσαρμογής στις περιπτώσεις όπου μετακινείται η απόληξη ή οι αισθητήρες και τέλος εξάγουμε κάποια συμπεράσματα.

4.1 Εισαγωγή

Το πρωτόκολλο που παρουσιάζουμε στοχεύει σε δίκτυα όπου οι αισθητήρες και η απόληξη μπορούν να μετακινηθούν κατά τη διάρκεια της εκτέλεσης και όπου η κατεύθυνση των πακέτων πληροφορίας δέν είναι κατ΄ ανάγκη η απόληξη. Το πρωτόκολλο επιστρατεύει μια συλλογή από μηχανισμούς έτσι ώστε η ακεραιότητα και εμπιστευτικότητα της πληροφορίας που δρομολογείται να είναι εξασφαλισμένη. Οι μηχανισμοί αυτοί είναι απλοί στην υλοποίηση, απαιτούν χρήση μόνο τοπικής πληροφορίας και χρειάζονται $O(1)$ αποθηκευτικό χώρο ανά αισθητήρα. Το πρωτόκολλο αυτό προσαρμόζεται σε προκλήσεις κινητικότητας και ασφάλειας που μπορεί να εμφανιστούν κατά τη διάρκεια εκτέλεσης του πρωτοκόλλου. Δείχνουμε ιδιαίτερη μέριμνα για δίκτυα που παρακολουθούν δυναμικά περιβάλλοντα και για εφαρμογές που απαιτείται η εκτέλεσή τους για μεγάλα χρονικά διαστήματα. Το APSR (Adaptive Probabilistic Secure Routing Protocol) μπορεί να εντοπίσει πότε οι τρέχουσες συνθήκες του δικτύου αναμένεται να αλλάξουν και προετοιμάζεται για να προσαρμοστεί σε αυτές τις αλλαγές. Επιδεικνύουμε επίσης πώς αντιμετωπίζονται οι *εσωτερικές επιθέσεις* και οι *εξωτερικές επιθέσεις* ακόμα και όταν το δίκτυο προσαρμόζεται σε εσωτερικά ή/και εξωτερικά γεγονότα.

4.2 Το Μοντέλο

Το μοντέλο του πρωτοκόλλου περιλαμβάνει τα εξής:

- Το μοντέλο επικοινωνίας είναι η επικοινωνία μέσω πολλαπλών ενδιάμεσων κόμβων, δηλαδή όλες οι συσκευές εκπέμπουν με την ίδια εμβέλεια εκπομπής και οι διαδρομές από έναν κόμβο του δικτύου σε έναν άλλον συνήθως περιλαμβάνουν ενδιάμεσους κόμβους.

- Υπάρχει ένας μοναδικός κόμβος στο δίκτυο ο οποίος αναπαριστά τον συνδετικό κρίκο ανάμεσα στο δίκτυο και στον διαχειριστή του τον οποίον ονομάζουμε απόληξη και θεωρούμε ότι αποτελεί τον προορισμό των περισσότερων μηνυμάτων του δικτύου. Η απόληξη εκπέμπει με την ίδια εμβέλεια με τους αισθητήρες, έχει σημαντικά περισσότερους υπολογιστικούς, επικοινωνιακούς και αποθεματικούς πόρους από τους αισθητήρες και θεωρούμε ότι δεν υπόκειται σε επιθέσεις.

- Οι αισθητήρες διαθέτουν κάποιες αισθητήριες συσκευές με τις οποίες μπορούν να μετρήσουν τις συνθήκες του περιβάλλοντος. Ανάμεσα σε αυτές τις αισθητήριες συσκευές περιλαμβάνεται ένα επιταχυνσιόμετρο με το οποίο οι αισθητήρες είναι σε θέση να αντιλαμβάνονται πότε ξεκινούν και πότε ολοκληρώνουν μια κίνηση, αλλά και να υπολογίσουν το βαθμό κινητικότητας που παρουσιάζουν σε ένα χρονικό διάστημα. Επιπλέον, μέσω του υλικού τους, οι αισθητήρες μπορούν να έχουν μια εκτίμηση για το υπολειπόμενο επίπεδο διαθέσιμης ενέργειας.

- Οι αισθητήρες μπορεί να είναι ετερογενή ως προς το υλικό τους. Ειδικότερα, μπορεί κάποιες συσκευές να παραμένουν μονίμως ακίνητες ενώ άλλες να βρίσκονται πάνω σε κινούμενα αντικείμενα.

- Οι αισθητήρες, η απόληξη ή και τα δύο έχουν τη δυνατότητα να κινηθούν. Η κίνηση αυτή δεν γίνεται ποτέ από επιλογή των ίδιων των συσκευών αλλά προκαλλείται από εξωτερικούς παράγοντες. Παρ΄ όλα αυτά, η ταχύτητα κίνησης είναι σημαντικά μικρότερη από την ταχύτητα μεταδόσεων οπότε και μια συνεδρία μερικών πακέτων πληροφορίας μπορεί πάντα να πραγματοποιείται μεταξύ δύο συσκευών που επικοινωνούν. Τα παραπάνω συνιστούν την υπόθεση ότι πάντοτε είναι δυνατή η παροχή επιβεβαίωσης για την επιτυχή παραλαβή ενός πακέτου.

- Η συλλογή της πληροφορίας από το περιβάλλον είναι βασισμένη σε γεγονότα (event-based), δηλαδή σε χρονικά σημεία τα οποία δεν είναι γνωστά εκ των προτέρων, οι αισθητήρες αναλαμβάνουν πρωτοβουλιακά να συλλέξουν πληροφορίες από το περιβάλλον και να προσπαθήσουν να τα στείλουν στην απόληξη. Συνεπώς δεν υποστηρίζεται η δυνατότητα ο διαχειριστής μέσω της απόληξη να θέσει ένα συγκεκριμένο *ερώτημα* (query) στο δίκτυο.

- Σε όλη τη διάρκεια λειτουργίας του πρωτοκόλλου περιμένουμε ότι μπορούν να συμβούν επιθέσεις οι οποίες έχουν σκοπό να βλάψουν τη λειτουργία του δικτύου ή να αποσπάσουν πληροφορίες. Θεωρούμε ότι ένας επιτιθέμενος έχει καλή επίγνωση του ορισμού και της λειτουργίας του πρωτοκόλλου και με αυτήν την γνώση προσπαθεί να πετύχει τους στόχους του. Οι επιθέσεις αυτές διακρίνονται σε παθητικούς (passive) και ενεργητικούς (active). Ένας παθητικός επιτιθέμενος απλώς 'κρυφακούει' για εκπομπές

μηνυμάτων ενώ ένας ενεργητικός επιτιθέμενος επιπλέον εκπέμπει μηνύματα προκειμένου να πετύχει τους στόχους του. Το πρωτόκολλό μας θα το σχεδιάσουμε έτσι ώστε να είναι ασφαλές από ενεργητικές επιθέσεις. Επιπλέον διακρίνουμε τις επιθέσεις σε εσωτερικούς και εξωτερικούς επιτιθέμενους. Ένας εξωτερικός επιτιθέμενος δεν έχει επίγνωση του περιεχόμενου καμίας συσκευής ενώ ένας εσωτερικός επιτιθέμενος θεωρούμε ότι έχει καταλάβει μια συσκευή, έχει αντιγράψει τη μνήμη του και χρησιμοποιεί αυτήν την πληροφορία για να επηρρεάσει τη λειτουργία του δικτύου. Θεωρούμε ότι το δίκτυο υπόκειται τόσο σε εξωτερικές όσο και σε εσωτερικές επιθέσεις. Περιγράφουμε όμως και ότι σε πραγματικές εφαρμογές μπορούμε να εκμηδενίσουμε την πιθανότητα να συμβεί εσωτερική επίθεση κατά τη φάση της αρχικοποίησης.

4.3 Υψηλού Επιπέδου Ανάλυση του πρωτοκόλλου

Προτείνουμε ένα καινούριο πρωτόκολλο δρομολόγησης το οποίο ονομάζουμε **APSR**. Το πρωτόκολλο οργανώνει το δίκτυο σε ομόκεντρες κυκλικές περιοχές (τις οποίες θα ονομάσουμε στρωματώσεις (layers) γύρω από την απόληξη τα οποία χωρίζονται περεταίρω σε τομείς (sectors). Οι στρωματώσεις δημιουργούνται σταδιακά ανάλογα με την απόσταση (hop-distance) τους από την απόληξη με ασφαλή τρόπο χρησιμοποιώντας μια αλυσίδα κλειδιών. Έπειτα, κάθε στρωμάτωση χωρίζεται σε τομείς οι οποίοι ακολουθούν το μαθηματικό μοντέλο των ελλειπτικών καμπύλων προκειμένου να ορίσουν ομαδικά κλειδιά κρυπτογράφησης για κάθε τομέα. Οι τομείς ορίζονται με κατανεμημένο τρόπο παράλληλα, μειώνοντας έτσι σημαντικά την πολυπλοκότητα χρόνου της φάσης αρχικοποίησης (παρ'ολο που η κρυπτογραφία με ελλειπτικές καμπύλες είναι υλοποιήσημη σε συσκευές με περιορισμένους πόρους, χρειάζεται μη-αμελητέο χρόνο για να εκτελεστεί). Έτσι κλειδιά κρυπτογράφησης δημιουργούνται για κάθε τομέα και διατομεακά κλειδιά δημιουργούνται μεταξύ γειτονικών τομέων.

Το **APSR** χρησημοποιεί έναν κατανεμημένο μηχανισμό, που είναι εύκολο να υλοποιηθεί, ο οποίος προσανατολίζει τις στρωματώσεις του δικτύου και τους τομείς έτσι ώστε οι συσκευές να έχουν μια κοινή αίσθηση κατεύθυνσης (προς τα μέσα, προς τα έξω, αριστερόστροφα, δεξιόστροφα). Αυτή η διαδικασία έχει απαιτήσεις χώρου τάξης $O(1)$. Προκειμένου ένα μήνυμα να φτάσει στον προορισμό του, κρυπτογραφείται και αποκρυπτογραφείται κάποιες φορές καθώς μετακινείται ανάμεσα σε διαφορετικούς τομείς και στρωματώσεις.

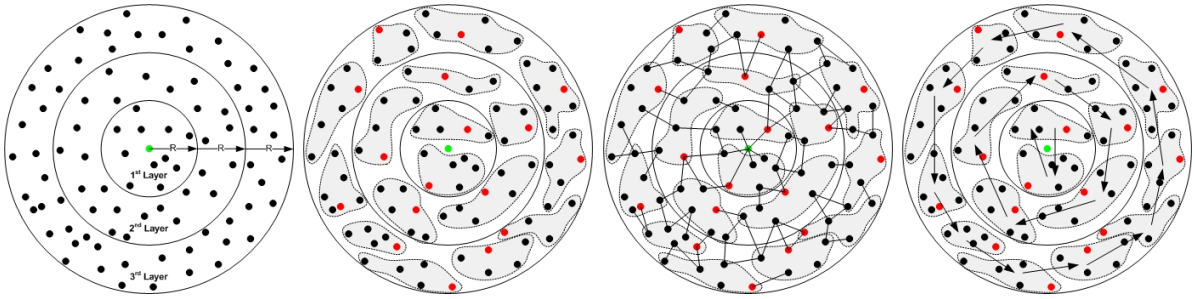
Ένας αισθητήρας δημιουργεί ένα πακέτο δεδομένων και προσπαθεί να το δρομολογήσει στον προορισμό του σε χρονικά σημεία που δεν είναι γνωστά εκ των προτέρων. Οι ενδιάμεσοι παραλήπτες του πακέτου αποφασίζουν αν θα το προωθήσουν περαιτέρω βασιζόμενοι σε μια συγκεκριμένη πιθανότητα. Αυτή η πιθανότητα εξαρτάται από τον αριθμό των αισθητήρων που είναι υποψήφιοι να προωθήσουν το ίδιο πακέτο και σε τοπικές πληροφορίες όπως η διαθέσιμη ενέργεια, ασφάλεια και κατάσταση κινητικότητας των αισθητήρων και των γειτονιών τους. Με αυτόν τον τρόπο, το πακέτο μπορεί να ακολουθήσει εναλλακτικές διαδρομές, όλες από τις οποίες προσπαθούν να ελαχιστοποιήσουν την απαιτούμενη απόσταση. Κάθε πακέτο κρυπτογραφείται χρησιμοποιώντας τα διατομεακά κλειδιά. Ανάλογα με την επιλογή του κάθε αισθητήρα αν θα προωθήσει ή όχι ένα πακέτο, μπορούμε να επιτρέψουμε προώθηση προς πολλαπλούς παραλήπτες (multi-path) των πακέτων προκειμένου να αυξήσουμε την αντοχή του δικτύου σε σφάλματα όπως αποτυχίες των αισθητήρων ή απώλεια δεδομένων.

Το **APSR** είναι ρυθμισμένο έτσι ώστε να επιτυγχάνει μεγαλύτερη αποτελεσματικότητα (σε χρόνο, αριθμό μεταδόσεων) όταν δρομολογεί μηνύματα προς την απόληξη. Έχει επιπλέον τη δυνατότητα να δρομολογεί πακέτα προς κάθε άλλα προορισμό στο δίκτυο αλλά με λιγότερη αποτελεσματικότητα. 'Παζαρεύουμε' την αποτελεσματικότητα προς τους άλλους προορισμούς προκειμένου το δίκτυο να μπορεί να προσαρμόζεται σε προκλήσεις κινητικότητας και ασφάλειας. Ένας επιτιθέμενος μπορεί να επικοινωνήσει με αισθητήρες σε ένα συγκεκριμένο μέρος του δικτύου παριστάνοντας πως έχει μόλις ταξιδέψει από ένα άλλο. Το πρωτόκολλό μας προσπαθεί να προσαρμόζεται σε δυνακιμές συθήκες περιβάλλοντος με τέτοιον τρόπο έτσι ώστε τόσο η δρομολόγηση δεδομένων και η ασφάλεια να είναι εφικτές ανά πάσα στιγμή. Όταν ένας αισθητήρας διαπιστώσει ότι έχει μετακινηθεί από την αρχική του θέση (χρησιμοποιώντας το επιταχυνσιόμετρο που διαθέτει), μπορεί να ξεκινήσει δράσεις που θα επανεντάξουν τη θέση και χρησιμότητα στο δίκτυο. Ανάλογα με το μέγεθος της κίνησης το πρωτόκολλο εφαρμόζει διαφορετικές στρατηγικές για να προσαρμοστεί στις εξωτερικές αλλαγές. Δείχνουμε ιδιαίτερη προσοχή στην περίπτωση που κινείται η απόληξη. Για μικρή κίνηση (σε χρόνο, απόσταση), η απόληξη μεταδίδει ειδικά μηνύματα ελέγχου έτσι ώστε η υποδομή του δικτύου να επαναπροσανατολίζεται προς τη νέα θέση. Όσο η κίνηση γίνεται μεγαλύτερη και με μεγαλύτερη ταχύτητα, ο επαναπροσανατολισμός αποφεύγεται και όταν σταματήσει την κίνησή του η απόληξη στη νέα του θέση, επανεκινεί τη φάση αρχικοποίησης της υποδομής του δικτύου.

Όσον αφορά την ασφάλεια, ο στόχος μας είναι να ασφαλίσουμε το δίκτυό μας από διάφορα είδη επιθέσεων που έχουν σκοπό να επηρρεάσουν αρνητικά τη λειτουργία του δικτύου ή να αποσπάσουν πληροφορίες. Για παράδειγμα, θα μπορούσε εύκολα ένας επιτιθέμενος να πραγματοποιήσει μια εκπομπή μεγάλης εμβέλειας προσποιούμενο την απόληξη προσπαθώντας να κάνει τις πληροφορίες δρομολόγησης στους αισθητήρες τελείως άχρηστη. Έτσι, αν έχουμε τρόπους να να δημιουργεούμε κλειδιά ασφαλούς επικοινωνίας στο δίκτυό μας, θα είμαστε ασφαλείς από τέτοιες επιθέσεις. Όσον αφορά τη φάση αρχικοποίησης του πρωτοκόλλου μας, το μόνο που υποθέτουμε είναι ότι δεν μπορεί ο επιτιθέμενος να καταλάβει μια συσκευή του δικτύου, να αντιγράψει τη μνήμη του και όλα τα κλειδιά κρυπτογράφησης και να προσπαθήσει να χρησιμοποιήσει αυτήν την πληροφορία για να εμποδίσει τη λειτουργία του δικτύου · κάθε άλλου τύπου επίθεση αντιμετωπίζεται. Τέλος, κατά τη φάση αρχικοποίησης υποθέτουμε ότι το δίκτυο είναι στατικό, δηλαδή δεν υπάρχει κίνηση των συσκευών.

4.4 Αρχικοποίηση του Πρωτοκόλλου και Ρύθμιση του Δικτύου

Η αρχικοποίηση του πρωτοκόλλου είναι οργανωμένη σε τέσσερεις διαδοχικές φάσεις. Στην πρώτη φάση δημιουργούμε μια σειρά από ομόκεντρους κύκλους, με κέντρο την απόληξη, με βάση την απόσταση των συσκευών από την απόληξη (παρατηρούμε ότι επειδή αυτοί οι κύκλοι δεν ανταποκρίνονται κατ' ανάγκη στην ευκλείδια απόσταση των συσκευών από την απόληξη αλλά στην απόσταση σε αριθμό ενδιάμεσων κόμβων, δεν είναι κύκλοι με την γεωμετρική έννοια, αλλά αυτό δεν επηρρεάζει τη λειτουργία του πρωτοκόλλου). Ονομάζουμε αυτούς τους ομόκεντρους κύκλους **στρωματώσεις** (layers). Χρησιμοποιούμε τις στρωματώσεις προκειμενου να προωθούμε πακέτα πληροφορίας είτε *προς τα μέσα* (δηλαδή προς την απόληξη) είτε *προς τα έξω* (δηλαδή μακριά από την απόληξη). Ο μέγιστος αριθμός των στρωματώσεων είναι δ, η διάμετρος του δικτύου (για την ακρίβεια θα είναι μεταξύ των



Phase 1 Phase 2 Phase 3 Phase 4

Σχήμα 4.1: Ρύθμιση Δικτύου και Αρχικοποίηση του APSR

$\frac{\delta}{2}$ και δ). Έπειτα, στην δεύτερη φάση, χωρίζουμε κάθε στρωμάτωση σε τομείς περίπου ίδιου μεγέθους και εντός κάθε τομέα υπολογίζουμε ένα *Τομεακό Διαμοιρασμένο Μυστικό Κλειδί* **Sector Shared Secret Key**. Κατά τη διάρκεια αυτών των φάσεων, οι αισθητήρες λαμβάνουν μεταδόσεις από γειτονικούς κόμβους του δικτύου που ανήκουν και σε γειτονικούς τομείς.

Δεδομένου ότι όλες οι στρωματώσεις έχουν χωριστεί σε τομείς, κατά την τρίτη φάση όλες οι συσκευές που έχουν γείτονες από άλλους τομείς δημιουργούν Τομεακά Διαμοιρασμένα Μυστικά Κλειδιά. Αυτό μας επιτρέπει να δρομολογούμε πακέτα πληροφορίας μεταξύ των τομέων με ασφαλή τρόπο. Στην τελική φάση, οι τομείς που ανήκουν στην ίδια στρωμάτωση συμφωνούν σε έναν κοινό προσανατολισμό εντός της στρωμάτωσης: συμφωνούν σε έναν κοινό δεξιόστροφο και αριστερόστροφο προσανατολισμό. Για μια γραφική αναπαράσταση της ρύθμισης του δικτύου και των τεσσάρων φάσεων αρχικοποίησης δείτε την εικόνα 4.1.

Με βάση αυτήν την υποδομή, ένας κόμβος του δικτύου μπορεί να δρομολογήσει μηνύματα σε έναν προορισμό δηλώνοντας το $LayerID$ και το $SectorID$ του προορισμού στην επικεφαλίδα του μηνύματος. Τα μηνύματα πρώτα προωθούνται είτε προς τα μέσα ή προς τα έξω μέχρι ανάλογα με το $LayerID$ του προορισμού. Όταν φτάσει στην επιθυμητή στρωμάτωση, το μήνυμα προωθείται είτε προς τα δεξιά είτε προς τα αριστερά μέχρι να φτάσει τον τομέα του προορισμού. Το πρωτόκολλο δρομολόγησης περιγράφεται στην ενότητα 4.5.

4.4.1 Πρώτη Φάση: Ασφαλής Δημιουργία των Στρωματώσεων (Hop-Distance Layers, HDL)

Ο απλούστερος τρόπος να δημιουργηθούν οι στρωματώσεις είναι η απόληξη να πλημμυρίσει (τεχνική flood) το δίκτυο με ένα μήνυμα που περιέχει έναν μετρητή. Κάθε συσκευή η οποία λαμβάνει αυτό το μήνυμα, πρέπει να θέσει τον αριθμό της στρωμάτωσης του (το οποίο ονομάζουμε HDL) στην τιμή του μετρητή του μηνύματος, να αυξήσει τον μετρητή κατά ένα και να προωθήσει το μήνυμα στους γείτονές του. Επαναλαμβάνοντας αυτήν την διαδικασία το πολύ για δ γύρους, το μήνυμα θα φτάσει τελικά όλους τους κόμβους του δικτύου. Παρ' όλα αυτά, αυτή η απλή προσέγγιση έχει μια βασική παράλειψη όσον αφορά την ασφάλεια: ένας επιτιθέμενος ο οποίος βρίσκεται στην στρωμάτωση j, μόλις λάβει το μετρητή του μηνύματος μπορεί να αλλάξει την τιμή του και να στείλει ψεύτικες τιμές του μετρητή στους γείτονές του. Επιπλέον, η απόληξη χρειάζεται να παρέχει μια επιβεβαίωση ότι η προέλευση του μηνύματος και συνεπώς του μετρητή δεν είναι ένας επιτιθέμενος ο οποίος θέλει να φανεί πως είναι η απόληξη του δικτύου.

Προκειμένου να αντιμετωπίσουμε αυτά τα ζητήματα ασφαλείας και να δημιουργήσουμε με ασφαλή τρόπο τις στρωματώσεις του δικτύου, επιστρατεύουμε μια μονής κατεύθυνσης αλυσίδα κλειδιών η οποία είναι μια λίστα $k_0, k_1, \cdots, k_\delta$, όπου δ είναι ο μέγιστος αριθμός των στρωματώσεων που περιμένουμε να δημιουργηθούν στο δίκτυο, τέτοια ώστε: $\forall l, 0 < l < \delta, k_{l-1} = f(k_l)$, όπου η f είναι μια ασφαλής ψευδοτυχαία συνάρτηση η οποία είναι υπολογιστικά δύσκολο να αντιστραφεί. Κάποιος που γνωρίζει το k_i μπορεί να επαληθεύσει ότι το $k_j, j > i$ είναι μέρος της μονής κατεύθυνσης αλυσίδας κλειδιών χρησιμοποιώντας το k_i. Συνεπώς μια συσκευή που γνωρίζει το k_i μπορεί να επαληθεύσει ότι το k_j είναι στοιχείο της αλυσίδας για $i < j$ εφαρμόζοντας τη συνάρτηση $f()$ $j - i$ φορές στο k_j, αλλα δεν μπορεί να παράγει το k_j από μόνη της. Το k_0 το βάζουμε στη μνήμη των αισθητήρων πριν από την τοποθέτηση τους στο περιβάλλον. Ολόκληρη η αλυσίδα κλειδιών είναι γνωστή μόνο στην απόληξη. Όλα τα μηνύματα που ανταλλάσσονται σε αυτήν την φάση κρυπτογραφούνται με το k_0 προκειμένου να εμποδίσουν τυχόν επιτιθέμενοι από το να αποσπάσουν κρίσιμες πληροφορίες ή να πραγματοποιήσουν 'επικίνδυνες ' μεταδόσεις.

Η πρώτη φάση λοιπόν εκτελείται σε γύρους οι οποίοι διαρκούν μια συγκεκριμένη χρονική περίοδο (time interval) η οποία αρκεί για να φτάσει ένα πακέτο στον πιο απομακρυσμένο αισθητήρα του δικτύου. Κατά τον πρώτο γύρο δημιουργείται η πρώτη στρωμάτωση. Η απόληξη δημιουργεί ένα πακέτο αρχικοποίησης ($IPKT_1$), το κρυπτογραφεί με το k_0 και το μεταδίδει στους γειτονικούς αισθητήρες χρησιμποιώντας την ίδια εμβέλεια εκπομπής με τους αισθητήρες. Όλα οι αισθητήρες που βρίσκονται εντός απόστασης μίας εκπομπής από την απόληξη, αφού λάβουν το μήνυμα αυτό, το αποκρυπτογραφούνε με το k_0, επαληθεύουν ότι το μήνυμα προέρχεται από την απόληξη και θέτουν την τοπική μεταβλητή HDL ίση με 1.

Για κάθε στρωμάτωση l μετά το πρώτο, η απόληξη δημιουργεί ένα νέο $IPKT_l$ το οποίο περιέχει το $k_l, HDL = l$ και ένα $sessionID$, κρυπτογραφημένο με το k_0. Οι αισθητήρες οι οποίοι έχουνε ήδη θέσει ότι ανήκουν σε στρωματώσεις μικρότερες του l απλώς προωθούν το $IPKT_l$ στους γείτονές τους. Το μήνυμα φτάνει κάποια στιγμή τους αισθητήρες στην στρωμάτωση j τα οποία ελέγχουν την εγκυρότητα του k_l εφαρμόζοντας την f, 'μπαίνουν' στην στρωμάτωση l και αποθηκεύουν το k_l στη μνήμη τους. Η διαδικασία αυτή συνεχίζεται μέχρι να δημιουργηθούν όλες τις στρωματώσεις. Κατά τη διάρκεια αυτής της φάσης, όλοι οι αισθητήρες αποθηκεύουν στη μνήμη τους το στοιχείο της αλυσίδας κλειδιών που αντιστοιχεί στην στρωμάτωση που ανήκουν (πχ το k_3 για την στρωμάτωση 3) και σβήνουν όλα τα άλλα από τη μνήμη τους.

Αυτή η τεχνική μας επιτρέπει να ασφαλίσουμε την φάση δημιουργίας των στρωματώσεων από επιθέσεις. Ένας εσωτερικός επιτιθέμενος που βρίσκεται στην στρωμάτωση j δεν μπορεί να στείλει ένα $IPKT$ με τιμή HDL $i > j$ καθώς δεν μπορεί να παράγει το k_i και δεν μπορεί να στείλει ένα $IPKT$ με τιμή HDL $i < j$ καθώς οι παραλήπτες αυτού του μηνύματος θα περίμεναν να το έχουν λάβει σε κάποιον προηγούμενο γύρο. Η χρονική περίοδος που χρησιμοποιοείται από την απόληξη είναι ίσο με τον χρόνο που χρειάζεται ένα μήνυμα να φτάσει τον πλέον απομακρυσμένο κάμβο του δικτύου, δηλαδή είναι ανάλογος της διάμετρου του δικτύου ($t \propto \delta$). Από τη στιγμή που αυτή η φάση χρειάζεται δ γύρους για να φτάσει όλες τις συσκευές, ο χρονική πολυπλοκότητα είναι $O(\delta)$.

Προκειμένου να υπολογίσουμε την πολυπλοκότητα μεταδόσεων υποθέτουμε ότι οι συσκευές είναι τοποθετημένες με τυχαίο και ομοιόμορφο τρόπο στην περιοχή, ο αριθμός των συσκευών εντός απόστασης μίας εκπομπής από την απόληξη μπορούν να υπολογιστούν σύμφωνα με την εργασία [5] ως $\mu(1) = \frac{n\pi R^2}{A}$, όπου R είναι η εμβέλεια εκπομπής των συσκευών και A το μέγεθος την περιοχής του δικτύου. Επομένως, ο αρθιμός των συσκευών στην στρωμάτωση $l > 0$

είναι $\mu(l) = \frac{(2l-1)n\pi R^2}{A}$. Προκειμένου ένα μήνυμα να φτάσει την στρωμάτωση l. πρέπει να προωθηθεί από όλες τις συσκευές που βρίσκονται σε προηγούμενες στρωματώσεις, δηλαδή από όλες τις συκευές που έχουν απόσταση $(l-1)\cdot R$ από την απόληξη (προσμετρώντας και την εκπομπή της απόληξης). Έτσι, αυτή η φάση χρειάζεται $\delta + \sum_{i=0}^{\delta} \frac{n\pi(i-1)^2R^2}{A}$ μεταδόσεις.

4.4.2 Δεύτερη Φάση: Καθορισμός των τομέων και Δημιουργία των Τομεακών Διαμοιρασμένων Μυστικών Κλειδιών

Συνεχίζουμε χωρίζοντας κάθε στρωμάτωση σε τομείς ίδιου περίπου μεγέθους (σε αριθμό αισθητήρων). Ακολουθούμε μια παρόμοια προσέγγιση με την εργασία [15]. Χρησιμοποιούμε το ϑ (μια παράμετρος του πρωτοκόλλου που έχουμε ήδη εισάγει στη μνήμη των συσκευών) που αντιπροσωπεύει το ιδανικό μέγεθος ενός τομέα. Μετά την ολοκλήρωση της πρώτης φάσης, όλοι οι αισθητήρες χρησιμοποιούν το ϑ για να αποφασίσουν μονομερώς εάν θα γίνουνε επικεφαλής τομέα (sector heads) με πιθανότητα $\frac{1}{\vartheta}$. Με αυτόν τον τρόπο δεν διασφαλίζουμε μόνο ότι όλοι οι τομείς θα περιέχουν περίπου ϑ αισθητήρες, αλλά και ότι οι τομείς θα είναι ομοιόμορφα κατανεμημένοι σε κάθε στρωμάτωση.

Κατόπιν, κάθε επικεφαλής τομέα ξεκινάει τον αλγόριθμο επιλογής Τομεακού Διαμοιρασμένου Μυστικού Κλειδιού που χρησιμοποιεί το μαθηματικό μοντέλο των ελλειπτικών καμπύλων και που περιγράψαμε στο 3.3.4 την οποία δεν θα επαναλάβουμε εδώ. Η βασική διαφορά σε αυτήν την περίπτωση είναι ότι όλα τα μηνύματα που ανταλλάσσονται σε αυτήν την διαδικασία κρυπτογραφούνται με το αντίστοιχο στοιχείο της αλυσίδας κλειδιών που αντιστοιχεί στην στρωμάτωση στην οποία ανήκει ο κάθε τομέας προκειμένου να διασφαλίσουμε ότι δεν θα συμμετέχουν τυχόν επιτιθέμενοι οι οποίοι διαφορετικά θα μπορούσαν να αποκτήσουν το Τομεακό Μυστικό Κλειδί. Επιπλέον, εκτός από το ειδικό $VISITED$ μήνυμα που χρησιμοποιούν οι αισθητήρες για να δηλώσουν στους γείτονές τους ότι έχουν ήδη 'επισκευτεί' από τον αλγόριθμο, προκειμένου τα κλειδιά να υπολογιστούν από αισθητήρες μόνο του ίδιου τομέα, εαν κάποιος αισθητήρας το έχει ήδη επισκευτεί ο αλγόριθμος που έχει εκκινήσει ένας επικεφαλής τομέα και κατόπιν του έρθει μια αίτηση να συμμετάσχει στον αντίστοιχο αγόριθμο που έχει εκκινήσει ένας άλλος επικεφαλής τομέα απαντάει με ένα ειδικό $DIFF\_SECTOR$ μήνυμα.

Το γεγονός ότι χρησιμοποιήσαμε το ϑ για να προσδιορίσουμε τους τομείς έχει σαν αποτέλεσμα αυτή η φάση να χρειάζεται $O(\vartheta)$ χρόνο καθώς όλοι οι τομείς δημιουργούνται παράλληλα. Αυτό είναι πολύ σημαντικό όσον αφορά την ασφάλεια καθώς σε μια πραγματική εφαρμογή θα είμαστε σε θέση να επιβλέπουμε το δίκτυο και να εξασφαλίσουμε ότι καμία επίθεση δεν θα συμβεί στο δίκτυο για μια χρονική περίοδο που είναι ανεξάρτητη από τον αριθμό των συσκευών που έχουμε τοποθετήσει.

4.4.3 Τρίτη Φάση: Δημιουργία Διατομεακών Διαμοιρασμένων Μυστικών Κλειδιών (Cross-Sector Shared Key Creation)

Σε αυτήν την φάση θα αξιοποιήσουμε τη λύση στο πρόβλημα Diffie-Dellman που παρουσιάσαμε στο 3.3.2 την οποία δεν θα επαναλάβουμε εδώ. Αυτό που πρέπει να παρατηρήσουμε είναι ότι το σημείο ελλειπτικής καμπύλης που χρησιμοποιούν δύο αισθητήρες a και b οι οποίοι

ανήκουν στους τομείς A και B αντίστοιχα, θα είναι τα Τομεακά Διαμοιρασμένα Μυστικά Κλειδιά που δημιουργήθηκαν στην προηγούμενη φάση. Έτσι, το Διατομεακό Διαμοιρασμένο Μυστικό Κλειδί μεταξύ δύο τομέων θα είναι το ίδιο για κάθε ζευγάρι αισθητήρων των δύο αυτών τομέων. Η βασική ιδέα είναι ότι οι αισθητήρες που γνωρίζουν ότι 'συνορεύουν' με αισθητήρες από γειτονικούς τομείς, εκκινούν αυτήν την διαδικασία με τους γείτονές τους προκειμένου να καθορίσουν τα επιθυμητά Διατομεακά Διαμοιρασμένα Μυστικά Κλειδιά.

Κατά τη διάρκεια αυτής της διαδικασίας (είτε μεταξύ τομέων της ίδιας στρωμάτωσης είτε μεταξύ διαφορετικών στρωματώσεων) είναι πιθανό ότι ένας επιτιθέμενος θα προσπαθήσει να εμφανιστεί ως μέλος ενός φανταστικού γειτονικού τομέα και θα προσπαθήσει να δημιουργήσει ένα Διατομεακό Διαμοιρασμένο Μυστικό Κλειδί. Έστω a και b δύο αισθητήρες από γειτονικούς τομείς. Αν και οι δύο αισθητήρες ανήκουν (ή δηλώνουν ότι ανήκουν) στην ίδια στρωμάτωση τότε δεν υπάρχει πρόβλημα καθώς κρυπτογραφούμε όλα τα μηνύματα αυτής της φάσης με το στοιχείο της αλυσίδας κλειδιών που αντιστοιχεί στη συγκεκριμένη στρωμάτωση οπότε και κάποιος επιτιθέμενος δεν θα μπορεί να συμμετέχει. Έστω τώρα ότι τα a και b ανήκουν (ή δηλώνουν ότι ανήκουν) στις στρωματώσεις j και $j-1$ αντίστοιχα. Κάθε αισθητήρας δημιουργεί ένα Discovery Packet ($DPKT$) το οποίο περιέχει τα $ID, sectorID, layerID$ τους και έναν τυχαίο αριθμό. Έπειτα δημιουργεί ένα EncodDiscoveryery Packet ($EDPKT$) από το $DPKT$ κρυπτογραφώντας με το στοιχείο της αλυσίδας κλειδιών που διαθέτουν. Με αυτόν τον τρόπο το a μπορεί να παράγει το κλειδί του b, το $k_{-1}j = f(k_j)$, να αποκρυπτογραφήσει το $EDPKT$ του b και έτσι να πιστοποιήσει ότι το b είναι 'νόμιμο' μέλος του δικτύου. Κατόπιν απαντάει στο b χρησιμοποιώντας το k_{j-1} και τον τυχαίο αριθμό που περιλαμβανόταν στο $EDPKT$ του b, οπότε και το b πείθεται ότι το a είναι και αυτό 'νόμιμο' μέλος του δικτύου. Σε αυτό το σημείο αξίζει να παρατηρήσουμε ότι η απόληξη συμπεριφέρεται σαν να ήταν μια στρωμάτωση και τομέας από μόνη της.

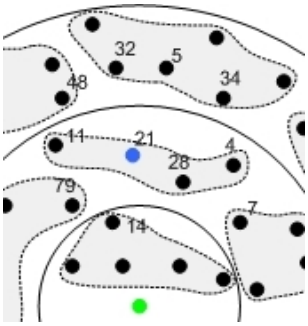
4.4.4 Τέταρτη Φάση: Επίτευξη Προσανατολισμού των τομέων στις Στρωματώσεις

Στην τελική φάση της αρχικοποίησης του δικτύου οι τομείς της κάθε στρωμάτωσης συντονίζονται μεταξύ τους έτσι ώστε να συμφωνήσουν σε μια κοινή αίσθηση προσανατολισμού. Όταν τελειώσει αυτή η φάση, όλοι οι τομείς μίας συγκεκριμένης στρωμάτωσης θα έχουν συμφωνήσει μια κοινή αίσθηση 'αριστερόστροφης ' και 'δεξιόστροφης ' κατεύθυνσης. Παρατηρούμε ότι αυτός ο προσανατολισμός δεν ανταναικλά κατ΄ ανάγκη τον αντίστοιχο προσανατολισμό στις πραγματικές θέσεις των τομέων και ότι διαφορετικές στρωματώσεις μπορεί να έχουν διαφορετικό προσανατολισμό.

Η δημιουργία προσανατολισμού επιτυγχάνεται καταφέρνοντας όλοι οι τομείς σε μία στρωμάτωση να συμφωνήσουν στην ίδια λίστα που περιλαμβάνει τους αριθμούς $0, 1, 2, \cdots, \sigma-1$ όπου κάθε αριθμός της λίστας αντιστοιχεί σε έναν διαφορετικό τομέα, γειτονικοί τομείς αντιστοιχούν σε 'γειτονικούς αριθμούς ' (θεωρούμε ότι ο αριθμός 0 γειτονεύει με τον αριθμό $\sigma-1$) και το σ είναι ο αριθμός των τομέων εντός της στρωμάτωσης. Σε αυτό το σημείο δεχόμαστε την υπόθεση ότι λόγω της πυκνότητας των αισθητήρων, οι στρωματώσεις δεν είναι ποτέ κατατμημένα οπότε και, όσον αφορά τους τομείς, πάντα θα είναι παρούσα μια τοπολογία εικονικού δακτυλίου εντός των στρωματώσεων. Προκειμένου να επιτύχουμε τον στόχο μας εφαρμόζουμε την ακόλουθη διαδικασία:

Κάθε επικεφαλής τομέα θέτει μονομερώς στον εαυτό του τον αριθμό 0, δημιουργεί ένα πακέτο το οποίο περιλαμβάνει τη λίστα [0] και το $sectorID$ του (το $sectorID$ αρχικά είναι

Variable	Type
Neighbor ID	numerical
Layer ID	numerical
Sector ID	numerical
in-bound	bit
out-bound	bit
left-bound	bit
right-bound	bit
flood	bit



ID	Layer	Sector	IOLRF
5	3	2	01000
34	3	2	01000
32	3	2	01000
48	3	3	01000
79	2	4	00010
14	1	1	10000
7	2	2	00100
11	2	1	00001
28	2	1	00001
4	2	1	00001

Σχήμα 4.2: Πληροφορία που Διατηρείται για κάθε Γειτονική Συσκευή και ένα Παράδειγμα για τον Κόμβο 21

το ίδιο με το ID του επικεφαλής τομέα) και επιλέγει έναν από τους γειτονικούς τομείς για να προωθήσει το πακέτο αυτό. Τα πακέτα αυτά προωθούνται μεταξύ των τομέων με απλά μηνύματα 'πλημμύρας' (flooding) τα οποία είναι κρυπτογραφημένα με το στοιχείο της αλυσίδας κλειδιών που αντιστοιχεί στη συγκεκριμένη στρωμάτωση. Έπειτα, ο επικεφαλής τομέα είναι σε αναμονή να λάβει τέτοια πακέτα από άλλους τομείς. Αν ληφθεί ένα πακέτο με αφετηρία έναν άλλον τομέα με μεγαλύτερο $sectorID$, αγνοείται. Αντίθετα, αν ληφθεί ένα πακέτο με αφετηρία έναν τομέα με μικρότερο $sectorID$, τότε επικεφαλής τομέα αναθέτει στον εαυτό του τον επόμενο αχρησιμοποίητο αριθμό της λίστας, επεκτείνει τη λίστα με αυτόν τον αριθμό και την προωθεί στον επόμενο τομέα (δηλαδή τον γειτονικό τομέα από τον οποίον **δεν** έλαβε το πακέτο). Είναι προφανές ότι η λίστα με αφετηρία τον τομέα με το μικρότερο $sectorID$ δεν θα αγνοηθεί και θα κάνει έναν πλήρη κύκλο στην στρωμάτωση καταφθάνοντας τελικά στον τομέα από τον οποίον ξεκίνησε. Σε αυτό το σημείο η λίστα θα είναι πλήρης. Μετά από αυτό πρέπει να κάνει άλλον έναν πλήρη κύκλο στην στρωμάτωση έτσι ώστε όλοι οι τομείς της στρωμάτωσης να την αποκτήσουν. Τέλος, όλα τα $sectorIDs$ μετονομάζονται ως $< L, S >$ όπου L είναι η τιμή της μεταβλητής HDL και S ο αριθμός της λίστας που αντιστοιχεί στον κάθε τομέα.

Μετά από αυτήν την διαδικασία, το μόνο που χρειάζεται να έχουν στη μνήμη τους οι αισθητήρες σχετικά με τον προσανατολισμό είναι το $sectorID$ και το σ. Έστω δύο αισθητήρες a και b που ανήκουν στους τομείς i και j της ίδιας στρωμάτωσης αντίστοιχα. Προκειμένου το a να προσδιορίσει αν το b βρίσκεται 'προς τα αριστερά' ή 'προς τα δεξιά' κάνει τον εξής απλο υπολογισμό: Αν $i - j \otimes \sigma \leq \frac{\sigma}{2}$ [1] τότε θα λέμε ότι το b βρίσκεται 'προς τα αριστερά' του a, ενώ αν $i - j \otimes \sigma > \frac{\sigma}{2}$ θα λέμε ότι το b βρίσκεται 'προς τα δεξιά' του a.

4.5 Φάση Δρομολόγησης

Δεδομένης της υποδομής του δκτύου που περιγράψαμε στην προηγούμενη ενότητα, θα περιγράψουμε το μηχανισμό δρομολόγησης του **APSR**. Επισυνάπτουμε σε κάθε πακέτο μια επικεφαλίδα που περιλαμβάνει: το ID, το $layerID$ και το $sectorID$ (SID) του παραλήπτη και μια *κατεύθυνση προώθησης*. Θεωρούμε ότι η απόληξη βρίσκεται στο $HDL = 0$ και

[1] το σύμβολο '$\otimes$' συμβολίζει τον υπολογισμό του υπόλοιπου ευκλείδιας διαίρεσης

$SID = 0$. Όταν ένας αισθητήρας λαμβάνει ένα πακέτο, ελέγχει την επικεφαλίδα του για να αποφασίσει αν πρέπει να το προωθήσει περεταίρω. Αυτό γίνεται ελέγχοντας το εσωτερικό πίνακα γειτόνων (neighborhood table, βλ. εικόνα 4.2)· αν ο αισθητήρας από το οποίο έλαβε το πακέτο βρίσκεται στην *αντίθετη κατεύθυνση* από την κατεύθυνση που αναγράφεται στην επικεφαλίδα του πακέτου, τότε ο αισθητήρας αναλαμβάνει να προωθήσει το πακέτο. Στο παράδειγμα της εικόνας 4.2, αν ο κόμβος 21 λάβει ένα μήνυμα από τον κόμβο 7 με μια 'δεξιόστροφη' κατεύθυνση, τότε θα δεχτεί να συμμετάσχει στην προώθηση, αλλιώς θα αγνοήσει τη μετάδοση.

Οι αισθητήρες που αποφασίζουν να προωθήσουν περεταίρω ένα πακέτο εφαρμόζουν την συνάρτηση δρομολόγησης f_{route} (με είσοδο τα HDL και SID της επικεφαλίδας του μηνύματος) η οποία ορίζεται ως εξής:

$$f_{route}(HDL, SID) = \begin{cases} down & , \ if\ HDL < my(HDL) \\ up & , \ if\ HDL > my(HDL) \\ left & , \ if\ HDL == my(HDL) \wedge SID - my(SID)\ \otimes\ \sigma > \frac{\sigma}{2} \\ right & , \ if\ HDL == my(HDL) \wedge SID - my(SID)\ \otimes\ \sigma \leq \frac{\sigma}{2} \\ flood & , \ if\ HDL == my(HDL) \wedge SID == my(SID) \end{cases}$$

Ανάλογα με την έξοδο της f_{route}, ο αισθητήρας ενημερώνει την επικεφαλίδα του πακέτου με τη νέα *κατεύθυνση προώθησης* (forwarding direction) και εκπέμπει το πακέτο. Έπειτα στέλνει μια επιβεβαίωση στον αισθητήρα από το οποίο έλαβε το πακέτο. Τα πακέτα πρώτα προωθούνται προς την στρωμάτωση στην οποία βρίσκεται ο προορισμός του πακέτου (δηλαδή προς τα μέσα ή προς τα έξω). Μετά, όταν το πακέτο φτάσει στην στρωμάτωση, προωθείται προς τον τομέα όπου βρίσκεται ο προορισμός του πακέτου (δηλαδή αριστερόστροφα ή δεξιόστροφα). Καθώς το πακέτο δρομολογείται προς τον προορισμό του, κρυπτογραφείται και αποκρυπτογραφείται σε κάθε μετάδοση χρησιμοποιώντας είτε τα Τομεακά Διαμοιρασμένα Μυστικά Κλειδιά ή τα Διατομεακά Διαμοιρασμένα Μυστικά Κλειδιά.

Δεδομένου ότι οι τομείς διαθέτουν έναν κοινό προσανατολισμό και ότι το δίκτυο δεν είναι κατατμημένο, και βασιζόμενοι στις υποθέσεις που κάναμε στο μοντέλο μας ότι είναι πάντα δυνατό να παρέχονται επιβεβαιώσεις, αυτός ο μηχανισμός εγγυάται ότι τα πακέτα θα φτάνουν στον προορισμό τους. Όμως, καθώς τα πακέτα δρομολογούνται προς τον προορισμό τους, ο μηχανισμός αυτός ενεργοποιεί ένα μεγάλο αριθμό από γειτονικές συσκευές. Όταν ένας κόμβος του δικτύου αποφασίζει να προωθήσει ένα πακέτο σε έναν γειτονικό τομέα, είναι πιθανό ότι περισσότεροι του ενός αισθητήρες θα το δεχτούνε. Έτσι, κάθε ένας από τους κόμβους που θα λάβουν το πακέτο θα εφαρμόσουν την f_{route} και θα επαναμεταδόσουν το πακέτο προς τον προορισμό του. Απο το παράδειγμα της εικόνας 4.2, όταν ο κόμβος 21 θέλει να προωθήσει ένα μήνυμα 'προς τα έξω' ένα σύνολο τεσσάρων αισθητήρων θα απαντήσουν και θα προωθήσουν το μήνυμα περεταίρω. Αν και αυτό αυξάνει την αντοχή σε σφάλματα του πρωτοκόλλου, σίγουρα αυξάνει και την κατανάλωση ενέργειας. Στις επόμενες υποενότητες προσπαθούμε να ελαχιστοποιήσουμε την επιβάρυνση (overhead) των μεταδόσεων εφαρμόζοντας μια τεχνική αναστολής μεταδόσεων (emission inhibition) εμπνευσμένη από την εργασία [18].

4.5.1 Ελαχιστοποίηση της Επιβάρνσης Δρομολόγησης με Αναστολή Μεταδόσεων

Αφού έχει εφαρμοστεί η συνάρτηση f_{route}, ο κόμβος συμβουλεύεται τον πίνακα γειτονιάς για να μετρήσει τον αριθμό των αισθητήρων που ενδεχομένως να συμμετέχουν στην προώθηση του πακέτου προς τον προορισμό του. Ορίζουμε με αυτόν τον αριθμό τη μεταβλητή Sensor Number (Αριθμός Αισθητήρων, SN) και την επισυνάπτουμε στην επικεφαλίδα του πακέτου. Όταν το πακέτο λαμβάνεται από τους υπόλοιπους κόμβους, και αφού αυτοί αποφασίσουν αν θα το προωθήσουν περεταίρω ή όχι (βασισμένοι στον κανόνα που περιγράψαμε παραπάνω), οι κόμβοι πραγματοποιούν έναν ακόμα έλεγχο πριν ολοκληρώσουν την απόφασή τους. Κάθε αισθητήρας θα προωθήσει το πακέτο με πιθανότητα $\frac{1}{SN}$, όπου SN είναι η τιμή της μεταβλητής που υποδηλώνεται στην επικεφαλίδα του πακέτου. Αυτός ο κανόνας χρησιμοποιείται για να ενεργοποιηθεί ένα μικρό μέρος των αισθητήρων στην προώθηση των πακέτων, μειώνοντας έτσι την κατανάλωση από εκπομπές.

Ιδανικά, η χρήση αυτού του απλού πιθανοτικού κανόνα χρησιμοποιείται για να ενεργοποιηθεί ακριβώς ένας αισθητήρας στην περεταίρω προώθηση του πακέτου. Θα υπάρχουν ωστόσο περιπτώσεις όπου είτε κανένας αισθητήρας δεν θα αναλάβει να προωθήσει, είτε περισσότερα του ενός αισθητήρα θα αναλάβουν να προωθήσουν το πακέτο. Η πρώτη περίπτωση συνεπάγεται την είσοδο κάποιας καθυστέρησης στο πρωτόκολλο καθώς η εκπομπή του πακέτου θα πρέπει να επαναληφθεί (καθώς ο αποστολέας δεν θα λάβει επιβεβαίωση ότι το πακέτο προωθήθηκε) ενώ η δεύτερη περίπτωση συνεπάγεται ότι θα δημιουργηθούν στο δίκτυο αντίγραφα του πακέτου αυξάνοντας την επιβάρυνση.

Παρατηρούμε ότι στην περίπτωση που η έξοδος της f_{route} είναι $flood$ ή η έξοδος της f_{route} είναι $left$ ή $right$ αλλά δεν υπάρχει κατάλληλος αισθητήρας στον πίνακα γειτονιάς, τότε ο αποστολέας πρέπει είτε να 'πλημμυρίσει' το πακέτο εντός του τομέα οπότε και η μεταβλητή SN δεν μπορεί να εφαρμοστεί, είτε να μεταδόσει απ΄ ευθείας το πακέτο στον τελικό προορισμό, εφόσον ο τελευταίος βρίσκεται στον πίνακα δρομολόγησης. Αυτή η κατάσταση καθιστά σαφές τον λόγο για τον οποίον το **APSR** είναι λιγότερο αποτελεσματικό όταν δρομολογεί '*οριζόντια*' απ΄ ότι όταν δρομολογεί '*κάθετα*'.

4.5.2 Προσαρμογή σε Τοπικές Συνθήκες Δικτύου

Ο μηχανισμός που υπολογίζει τη μεταβλητή Sensor Number αποδίδει καλά όταν το δίκτυο παραμένει στατικό και όλοι οι αισθητήρες λειτουργούν κανονικά. Παρ΄ όλα αυτά, σε περιπτώσεις όπου οι αισθητήρες λειτουργούν με μπαταρίες, είναι πιθανό ότι οι κόμβοι του δικτύου θα χρησιμοποιούν μια τακτική εξοικονόμησης ενέργειας η οποία θα τα θέσει σε sleep mode για ορισμένες χρονικές περιόδους. Σε άλλες περιπτώσεις, είναι πιθανό ότι κόμβοι θα υπόκεινται σε προσωρινές ή ακόμα και μόνιμες αποτυχίες λειτουργίας. Τελος, οι κόμβοι μπορούν να αλλάξουν την τοποθεσία τους (αν για παράδειγμα βρίσκονται πάνω σε κινούμενες οντότητες). Σε τέτοιες περιπτώσεις, η χρήση της μεταβλητής SN θα είναι ανακριβής οδηγώντας σε καταστάσεις όπου τα πακέτα δεν θα προωθούνται σχεδόν ποτέ (οδηγώντας έτσι σε συνεχείς επαναμεταδόσεις) ή σε καταστάσεις όπου πολλοί αισθητήρες θα ανταποκρίνονται στην προώθηση (αυξάνοντας έτσι την επιβάρυνση δρομολόγησης).

Για αυτούς τους λόγους, το **APSR** προσπαθεί ενεργητικά να εντοπίζει αλλαγές στις συνθήκες του περιβάλλοντας χρησιμοποιώντας περιορισμένες τοπικές πληροφορίες. Κάθε αισθητήρας εκπέμπει περιοδικά δύο beacon messages τα οποία περιλαμβάνουν: το $ID, layerID$

και $sectorID$ του αισθητήρα, το μ (μια εκτίμηση της κατάστασης κινητικότητας του αισθητήρα με χρήση του επιταχυνσιόμετρου) και το ϵ (μια εκτίμηση για το επίπεδο της διαθέσιμης ενέργειας της μπαταρίας). Το ένα beacon κρυπτογραφείται με το k_l (έτσι ώστε οι αισθητήρες από την ίδια και τις ψηλότερες στρωματώσεις να μπορούν να αποκρυπτογραφήσουν και να πιστοποιήσουν την προέλευσή τους) και το δεύτερο beacon με το k_{l-1} (έτσι ώστε οι αισθητήρες από χαμηλότερες στρωματώσεις να μπορούν να αποκρυπτογραφήσουν και να πιστοποιήσουν την προέλευσή τους). Βασιζόμενα σε αυτά τα beacon messages, οι αισθητήρες μπορούν να προσαρμόσουν τους πίνακες δρομολόγησης έτσι ώστε να ανταποκρίνονται στις τρέχουσες συνθήκες περιβάλλοντος. Επιπλέον, μπορούνε να εκτιμήσουν τη μέση κατάσταση κινητικότητας ($\bar{\mu}$) και τα αποθέματα ενέργειας ($\bar{\epsilon}$) της γειτονιάς τους.

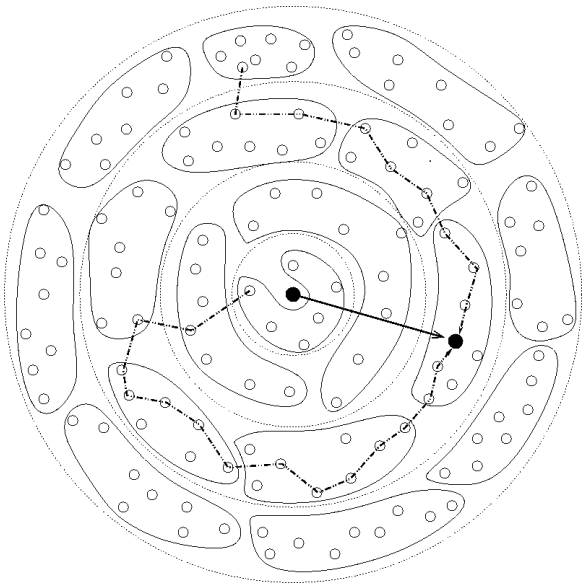
Οι αισθητήρες χρησιμοποιούν μια τοπική μεταβλητή $\beta = \frac{\bar{\mu}}{\mu} \times \frac{\epsilon}{\bar{\epsilon}}$ και πραγματοποιούν την πιθανοτική επιλογή τους (για να αποφασίσουν αν θα προωθήσουν ένα πακέτο ή όχι) με πιθανότητα $\frac{\beta}{SN}$. Έτσι, όσο αυξάνει η κινητικότητα των αισθητήρων, σε σχέση με τη μέση κατάσταση κινητικότητας της γειτονιάς, ή όσο η διαθέσιμη ενέργεια του αισθητήρα μειώνεται σε σχέση με τη μέση διαθέσιμη ενέργεια της γειτονιάς, το β μειώνεται. Με αυτόν τον τρόπο, η πιθανότητα να αναλάβει ο αισθητήρας την προώθηση ενός πακέτου μειώνεται και αυτή. Ιδανικά με αυτόν τον τρόπο δίνουμε προτεραιότητα σε αισθητήρες χαμηλής κινητικότητας καθώς θεωρούμε ότι είναι περισσότερο αξιόπιστοι για να δρομολογούν πακέτα, και σε αισθητήρες με περισσότερη διαθέσιμη ενέργεια προκειμένου να διανείμουμε καλύτερα την κατανάλωση ενέργειας και να επιμηκύνουμε τη διάρκεια ζωής του δικτύου. Επιπλέον, αυτός ο μηχανισμός εντοπίζει αλλαγές στην πυκνότητα της γειτονιάς επαναυπολογίζοντας την τιμή της μεταβλητής SN.

Αυτό το δυναμικό χαρακτηριστικό του πρωτοκόλλου είναι ιδιαίτερα ωφέλιμο σε ετερογενείς καταστάσεις και σε περιπτώσεις όπου οι αισθητήρες είναι κινητοί εντός της περιοχής του δικτύου. Παρατηρούμε ότι το beacon message και ο υπολογισμός του β μπορεί να επεκταθεί ώστε να περιλαμβάνει και άλλες μετρικές του δικτύου όπως τον υπολογιστικό φόρτο των συκευών, την διαθέσιμη μνήμη ή ακόμα το βαθμό υποψίας εχθρικής συμπεριφοράς απέναντι στο δίκτυο εφόσον υπάρχει ένας ανάλογος μηχανισμός [2].

4.6 Κινητικότητα της Απόληξης

Όταν η απόληξη αλλάζει την τοποθεσία της, είναι προφανές ότι σχεδόν όλες οι μεταβλητές δρομολόγησης του δικτύου θα έχουν μη έγκυρες τιμές. Δεν μπορούμε να βασιστούμε σε τοπικές διορθωτικές μεθόδους για να λύσουμε αυτό το πρόβλημα καθώς αυτό θα προκαλέσει μεγάλη επιβάρυνση δρομολόγησης αυξάνοντας έτσι την κατανάλωση ενέργειας. Ένας τρόπος να χειριστούμε αυτό το πρόβλημα θα ήταν να εκκινήσουμε ακόμα μια φάση αρχικοποίησης. Παρ' όλα αυτά, δεν μπορούμε να καταφεύγουμε σε αυτήν την επιλογή συχνά καθώς αυτό θα οδηγήσει επίσης σε πολύ μεγάλεπιβάρυνση καθώς και καθυστέρηση. Το **APSR** προσπαθεί να προσαρμόζεται στην μεταβαλλόμενη τοποθεσία της απόληξης χρησιμοποιώντας μια λιγότερο αποτελεσματική μέθοδο δρομολόγησης μέχρι ένα σημείο όπου αυτό είναι ακόμα πρακτικό· έπειτα επαναναρχικοποιεί το δίκτυο.

Υποθέτουμε ότι η απόληξη παραμένει στατική στο μεγαλύτερο μέρος της λειτουργίας του δικτύου και έχει επίγνωση της χρονικής περιόδου κατά την οποία κινείται (πιθανόν μέσω ενός επιταχυνσιόμετρου). Όταν ξεκινάει την κίνηση, 'πλημμυρίζει' με ασφαλή τρόπο (χρησιμοποιώντας τα Τομεακά και Διατομεακά Διαμοιρασμένα Μυστικά Κλειδιά με ένα



Σχήμα 4.3: Πώς Δρομολογούνται τα Πακέτα Πληροφορίας όταν έχει Αλλάξει η Τοποθεσία της απόληξης

καιρνούριο σημείο ελλειπτικής καμπύλης P και μια καινούρια τιμή k_0 που είναι το πρώτο στοιχείο μιας κανούριας μονής κατεύθυνσης αλυσίδας κλειδιών. Οι αισθητήρες του δικτύου αποθηκεύουν αυτές τις πληροφορίες προκειμένου να είναι σε θέση να συμμετάσχουν στην επικείμενη φάση αρχικοποίησης.

Προκειμένου τα πακέτα που δρομολογούνται στην απόληξη να φτάσουν τον προορισμό τους, η έξοδος της f_{route} στους αισθητήρες που βρίσκονται στην ίδια στρωμάτωση όπου βρίσκεται η απόληξη και 'παρακάτω' πρέπει να είναι κάτι διαφορετικό από $down$. Ας υποθέσουμε ότι η απόληξη μετακινείται από την στρωμάτωση i στην στρωμάτωση j, όπου $j = i+1$. Η απόληξη πρέπει να 'πλήμμυρίσει' ένα μήνυμα σε όλα τους αισθητήρες της στρωμάτωσης i για να τα ενημερώσει ότι η f_{route} πρέπει να δίνει έξοδο up όταν η δρομολόγηση είναι προς την απόληξη και ένα μήνυμα σε όλα τους αισθητήρες της στρωμάτωσης j ενημερώνοντάς τα για το σε ποιον τομέα βρίσκεται έτσι ώστε να αποφασίσουν ανάλογα αν η έξοδος της f_{route} θα είναι $left, right$ ή $flood$ όταν η δρομολόγηση είναι προς την απόληξη.Όταν η απόληξη μετακινείται από την στρωμάτωση i στην στρωμάτωση j, όπου $i = j + 1$, οι αισθητήρες στην στρωμάτωση j ενημερόντονται όπως παραπάνω, ενώ οι αισθητήρες στην στρωμάτωση i ενημερώνονται ότι η f_{route} πρέπει να δίνει έξοδο $down$ όταν η δρομολόγηση είναι προς την απόληξη.

Ο συνεχής επαναπροσανατολιστός της υποδομής του δικτύου αναπόφευκτα διαταράσσει την αποτελεσματικότητα της δρομολόγησης. Για αυτόν τον λόγο η απόληξη χρησιμοποιεί μια τοπική μεταβλητή λ η οποία μετράει τον αριθμό των διαφορετικών τομέων που έχει επισκευτεί. Όταν το λ ξεπεράσει μια προκαθορισμένη τιμή (η οποία αποτελέι παράμετρο του πρωτοκόλλου και ορίζεται από τον διαχειριστή του δικτύου), η απόληξη ενημερώνει τον τομέα στον οποίον βρίσκεται ότι πρέπει να γίνει η 'εικονική απόληξη' του δικτύου και σταματάει να εκπέμπει περεταίρω ενημερώσεις. Οι αισθητήρες που χαρακτηρίζονται ως 'εικονικές απολήξεισ' θα αποθηκεύσουν όλα τα εισερχόμενα πακέτα μέχρι να επανεμφανιστεί η απόληξη. Τελικά, όταν η κίνηση της απόληξης ολοκληρωθεί, η απόληξη επανεκκινεί την φάση αρχικοποίησης του δικτύου. Μόλις ολοκληρωθεί η φάση αρχικοποίησης και η υποδομή

του δικτύου είναι επαναπροσανατολισμένη στη νέα τοποθεσία της απόληξης, Οι αισθητήρες τα οποία είχαν προηγουμένως χαρακτηριστεί ως 'εικονικές απολήξεισ' προωθούν όλα τα αποθηκευμένα πακέτα προς τη νέα τοποθεσία της απόληξης.

4.7 Κινητικότητα των Αισθητήρων

Ο τρόπος με τον οποίο έχουμε υλοποιήσει την υποδομή δρομολόγησης και ασφάλειας κάνει το πρωτόκολλό μας ικανό να προσαρμόζεται στην κινητικότητα των αισθητήρων. Παρ΄ όλα αυτά, αυτό το γεγονές παρέχει επίσης ένα ευνοϊκό περιβάλλον για επιθέσεις. Μια συσκευή που εισέρχεται σε έναν τομέα δεν θα κατέχει τα Τομεακά Διαμοιρασμένα Μυστικά Κλειδιά είτε είναι 'νόμιμο' μέλος του δικτύου, είτε είναι επιτιθέμενος. Συνεπως, ένας επιτιθέμενος θα μπορούσε να εισέλθει στο δίκτυο και να προσπαθήσει να πείσει τους γειτονικούς του αισθητήρες ότι είναι έγκυρο μέλος του δικτύου και ότι έχει ταξιδέψει από κάποιον άλλον τομέα. Έτσι, προκειμένου να αναγνωριστεί μια νεοφερμένη συσκευή, να ενταχθεί στον τομέα και να του εμπιστευτούν τα Τομεακά Διαμοιρασμένα Μυστικά Κλειδιά, πρέπει να πείσει τους καινούριους του γείτονες ότι άνηκε προηγουμένως σε κάποιον άλλον τομέα χρησιμοποιώντας τα παλιά του Τομεακά Διαμοιρασμένα Μυστικά Κλειδιά. Σε αυτή τη φάση πρέπει να είμαστε προσεχτικοί για δύο πράγματα: Οι αισθητήρες δεν θα πρέπει να εκπέμψουν χωρίς ασφάλεια κάποιο κλειδί κρυπτογράφησης καθώς ένας επιτιθέμενος ο οποίος κρυφακούει θα μπορεί εύκολα να τα αποκτήσει και επιπλέον πρέπει να ορίσουμε αυτήν την διαδικασία προσαρμογής σε κίνηση με τετοιον τρόπο έτσι ώστε ένας επιτιθέμενος να μην μπορεί επανεκπέμποντας αντίγραφα μεταδόσεων που έχει ακούσει (ακόμα και αν είναι κρυπτογραφημένες) να αναγνωριστεί και να ενταχθεί στον τομέα.

Όταν ένας αισθητήρας (ή το αντικείμενο πάνω στο οποίο βρίσκεται) ξεκινάει να κινείται, έχει επίγνωση αυτού του γεγονότος χρησιμοποιώντας το επιταχυνσιόμετρό του. Σε αυτό το σημείο σταματάει να συμμετέχει ενεργά στο πρωτόκολλο. Σε αυτήν την κατεύθυνση σταματάει να δρομολογεί πακέτα και σταματάει να εκπέμπει περιοδικά τα beacon messages που χρησιμοποιούνται για να ορίζεται δυναμικά το β. Μόλις ολοκληρωθεί η κίνηση, ο αισθητήρας έχει και πάλι επίγνωση του γεγονότος αυτού χρησιμοποιώντας το επιταχυνσιόμετρό του. Στις παρακάτω υποενότητες περιγράφουμε τον τρόπο με τον οποίο θα επαναπροσδιορίσει τη θέση του και τη λειτουργικότητά του στο δίκτυο.

4.7.1 Χαμηλή Κινητικότητα (ο Αισθητήρας έχει Σταματήσει Εντός του Ίδιου Τομέα από τον οποίο Ξεκίνησε)

Μόλις ο αισθητήρας σταματήσει την κίνησή του, περιμένει να ακούσει εκπομπές από τους γείτονές του. Έτσι λαμβάνει τα περιοδικά beacon messages που χρησιμοποιούνται για να οριστεί δυναμικά το β τα οποία είναι κρυπτογραφημένα με τα στοιχεία της μονής κατεύθυνσης αλυσίδας κλειδιών οπότε μπορεί να τα αποκρυπτογραφήσει και μετά απλά ενημερώνει τον πίνακα δρομολόγησης του και συνεχίζει να συμμετέχει στο δίκτυου όπως πριν.

4.7.2 Μέση Κινητικότητα (ο Αισθητήρας έχει Ταξιδέψει σε έναν Γειτονικό Τομέα)

Αν ο αισθητήρας μπορεί ακόμα να αποκρυπτογραφήσει τα beacon messages, συνειδητοποιεί ότι έχει ταξιδέψει σε έναν τομέα της ίδιας ή γειτονικής στρωμάτωσης. Προκειμένου να αναγνωριστεί στον καινούριο τομέα, επιλέγει τυχαία έναν γείτονα και του ζητάει να τον εντάξει στον τομέα. Έστω a ο νεοφερμένος αισθητήρας και b ο αισθητήρας που έχει αναλάβει να το αναγνωρίσει.

Προκειμένου να εμποδίσουμε έναν επιτιθέμενο να αναγνωριστεί από το b, κρυπτογραφούμε όλα τα μηνύματα με τα Διατομεακά Διαμοιρασμένα Μυστικά Κλειδιά που διαθέτει το b. Ο αισθητήρας b δημιουργεί ένα Discovery Packet (DPKT βλέπε 4.4.3) το οποίο περιέχει έναν τυχαίο αριθμό. Μετά δημιουργεί ορισμένα Encoded Discovery Packets (EDPKT) χρησιμοποιώντας τα Διατομεακά Διαμοιρασμένα Μυστικά Κλειδιά που διαθέτει. Κάποια στιγμή, αν τα a και b μοιράζονται κάποιο τέτοιο κλειδί, το a θα είναι σε θέση να αποκρυπτογραφήσει κάποιο από τα EDPKTs και να απαντήσει στο b με τον τυχαίο αριθμό που περιέχεται στο DPKT κρυπτογραφημένο με το ίδιο Διατομεακά Διαμοιρασμένα Μυστικά Κλειδιά. Έτσι το b πείθεται ότι το a είναι όντως 'νόμιμο' μέλος του δικτύου οπότε και του εμπιστεύεται με ασφαλή τρόπο το Τομεακό Διαμοιρασμένο Μυστικό Κλειδί.

Αν δεν βρεθούν κοινά Διατομεακά Διαμοιρασμένα Μυστικά Κλειδιά, αυτή η διαδικασία επαναλαμβάνεται μέχρι να βρεθεί ένας τέτοιος αισθητήρας b με το οποίο το a να μοιράζεται κάποιο κλειδί. Αν δεν υπάρχει τέτοιος αισθητήρας, τότε ακολουθείται η διαδικασία που περιγράφουμε παρακάτω.

4.7.3 Υψηλή Κινητικότητα (ο Αισθητήρας έχει Ταξιδέψει σε έναν Απομακρυσμένο Τομέα)

Από τη στιγμή που τα IDPKTs και τα EDPKTs απέτυχαν να αναγνωρίσουν τον αισθητήρα a, τα a και b χρησιμοποιούν τα στοιχεία της αλυσίδας κλειδιών για να επικοινωνήσουν. Ο αισθητήρας που κατέχει την υψηλότερη τιμή της αλυσίδας κλειδιών χρησιμοποιεί την $f()$ μερικές φορές για να υπολογίσει την χαμηλότερη τιμή. Μετά από αυτό, ο αισθητήρας b μπορεί με ασφαλή τρόπο να εμπιστευτεί το Τομεακό Διαμοιρασμένο Μυστικο Κλειδί στο a. Με αυτόν τον τρόπο, κάποιος εξωτερικός επιτιθέμενος ο οποίος δεν κατέχει κάποιο στοιχείο της αλυσίδας κλειδιών δεν μπορεί να συμμετάσχει σε αυτήν την διαδικασία και να αναγνωριστεί ως 'νόμιμο' μέλος τους δικτύου.

4.8 Ανάλυση Ασφάλειας

Σε αυτό το σημείο θα περιγράψουμε το επίπεδο ασφάλειας που έχουμε πετύχει στο πρωτόκολλό μας δείχνοντας πώς ανταποκρίνεται στις επιθέσεις που περιγράψαμε στο 3.2:

1. **Spoofed, Altered, Replayed Routing Information :** Από τη στιγμή που όλα τα μεταδιδόμενα πακέτα είναι κρυπτογραφημένα και πιστοποιημένα, αυτού του είδους η επίθεση δεν θέτει κάποιο πρόβλημα για το πρωτόκολλό μας. Επιπλέον, με τη χρήση των χρονικών περιόδων κατά τη δημιουργία των hop-distance layers (διαστρωματώσεων), ένας εσωτερικός επιτιθέμενος δεν μπορεί να επαναλάβει πληροφορίες δρομολόγησης και να κάνει τους αισθητήρες να πιστέψουν ότι έχουν διαφορε-

τική απόσταση από την απόληξη από την πραγματική. Κατά τη φάση όπου ένας αισθητήρας έχει μετακινηθεί σε κάποιον άλλον τομέα και ζητάει τα Τομεακά Διαμοιρασμένα Μυστικά Κλειδιά, τα EDPKTs που χρησιμοποιούνται περιέχουν τυχαίες τιμές έτσι ώστε κάποιος επιτιθέμενος να μην μπορεί να επαναλάβει κάποια μετάδοση και να του εμπισευτούν τα Τομεακά Διαμοιρασμένα Μυστικά Κλειδιά.

2. **Selective Forwarding :** Αυτού του είδους η επίθεση είναι εκ των πραγμάτων δύσκολο να αντιμετωπιστεί καθώς πρέπει να αποδεχτούμε ότι αν ένας αισθητήρας έχει καταληφθεί από έναν επιτιθέμενο, ο επιτιθέμενος θα είναι σε θέση να συμμετέχει κανονικά στο δίκτυο. Παρ΄ όλα αυτά, το γεγονός ότι η δρομολόγηση στο **APSR** βασίζεται σε πιθανότητα ελαχιστοποιεί τη δυνατότητα του επιτιθέμενου να προκαλέσει ζημιά στο δίκτυο. Επιπλέον, θα μπορούσαμε να προσθέσουμε έναν μηχανισμό ο οποίος υπολογίζει το βαθμό υποψίας εχθρικής συμπεριφοράς και να τον εντάσσει στη μεταβλητή β απομονώνοντας έτσι τον κατελλημένο αισθητήρα.

3. **Sinkhole and Wormhole Attacks :** Αυτή η επίθεση δεν μπορεί πάντα να αντιμετωπιστεί από κρυπτογραφία και πιστοποίηση καθώς οι επιτιθέμενοι μπορούν να μεταδίδουν τις εκπομπές όπως ακριβώς τις ακούνε χωρίς να είναι ανάγκη να τις 'καταλαβαίνουν'. Η καλύτερη άμυνα που διαθέτουμε απέναντι σε αυτήν την επίθεση, καθώς και σε κάποιες άλλες, είναι ότι το **APSR** μας παρέχει με μέσα έτσι ώστε να μπορούμε να εκτιμήσουμε τη διάρκεια της φάσης αρχικοποίησης του δικτύου εκ των προτέρων, διάρκεια η οποία δεν εξαρτάται από το μέγεθος του δικτύου, οπότε στα περισσότερα σενάρια εφαρμογών, ο διαχειριστής του δικτύου μπορεί να επιβλέπει το δίκτυο και να εξασφαλίσει ότι δεν πραγματοποιείται καμία επίθεση. Όταν τελειώσει η φάση αρχικοποίησης, η τοπολογία που έχουν υπόψιν τους οι αισθητήρες είναι καθορισμένη και δεν μπορούν να παραπλανηθούν έτσι ώστε να πιστέψουν ότι υπάρχουν περεταίρω κανάλια επικοινωνίας από τα πραγματικά.

4. **Sybil Attacks :** Αυτή η επίθεση μπορεί να βλάψει το πρωτόκολλό μας μόνο κατά τη φάση αρχικοποίησης κατά την οποία έχουμε εξηγήσει ότι δεν έχουμε κάποιον σοβαρό φόβο επίθεσης. Κατά τη φάση δρομολόγησης, τα περισσότερα πακέτα ταξιδεύουν μόνο μια φορά από κάθε στρωμάτωση και διαφορετικά κλειδιά κρυπτογραφίας χρησιμοποιούνται σε κάθε μετάδοση, οπότε κάποιος επιτιθέμενος ο οποίος κατέχει τα κλειδιά ενός μόνο τομέα δεν αποκτάει κάποιο ιδιαίτερο πλεονέκτημα μέσω αυτής της επίθεσης περισσότερο από αυτό που ήδη έχει έχοντας καταλάβει έναν αισθητήρα.

5. **Hello and Acknowledgment Spoofing Attacks :** Αυτή η επίθεση θα μπορούσε να εφαρμοστεί στοχεύοντας στα beacon messages που χρησιμοποιούνται για τη δημιουργία του b. Μια επίθεση κατά την οποία μεταδίδονται πολλά τέτοια μηνύματα μπορεί να 'πείσει' τους περισσότερους αισθητήρες του δικτύου να χρησιμοποιούν υπερβολικά χαμηλές πιθανότητες στην προώθηση των πακέτων. Παρ΄ όλα αυτά, η χρήση κρυπτογραφίας και πιστοποίησης στα beacon messages μας προστατεύει από αυτού του είδους την επίθεση καθώς και από το acknowledgment spoofing.

4.9 Συμπεράσματα

Παρουσιάσαμε ένα πρωτόκολλο δρομολόγησης για Ασύρματα Δίκτυα Αισθητήρων το οποίο ονομάζουμε APSR . Το πρωτόκολλό μας βασίζεται σε μια συλλογή από μηχανισμούς τέτοιους ώστε η ακεραιτότητα και εμπιστευτικότητα των πληροφοριών που παραδίδονται στους διαχειριστές του δικτύου να διασφαλίζονται σε κάθε περίπτωση. Το πρωτόκολλό μας είναι κατάλληλο ειδικά για καταστάσεις όπου το δίκτυο είναι ευάλλωτο σε επιθέσεις (είτε ενεργητικές, είτε παθητικές), για παράδειγμα από 'κακόβουλες ' συσκευές οι οποίες είναι αρκετά ισχυρές (σε επίπεδο ταχύτητας υπολογισμών, επικοινωνίας και μνήμης) και γνωρίζουν καλά τους εσωτερικούς μηχανισμούς του APSR . Παρ' όλο που θεωρούμε ότι η προστασία του δικτύου από εσωτερικές επιθέσεις (για παράδειγμα, από συσκευές που μπορούν να αποσπάσουν το περιεχόμενο της μνήμης κάποιων αισθητήρων) είναι πολύ δύσκολη (αν όχι και αδύνατη), χρησιμοποιούμε μηχανισμούς οι οποίοι παράγουν αρκετά κλειδιά κρυπτογραφίας αναγκάζοντας την εξωτερική επιτιθέμενη συσκευή σε περισσότερο επίπονες διαδικασίες προκειμένου να μπορέσει να επηρεάσει τη λειτουργία του δικτύου.

Οι μηχανισμοί που επιστρατεύουμε είναι απλοί στην υλοποίηση και βασίζονται μόνο σε τοπικές πληροφορίες. Μεριμνούμε ιδιαίτερα για περιπτώσεις όπου το Ασύρματο Δίκτυο Αισθητήρων χρησιμοποιείται για να παρακολουθήσει ένα δυναμικά μεταβαλλόμενο περιβάλλον και για εφαρμογές που απαιτούν τη λειτουργία του για μεγάλες χρονικές περιόδους. Το APSR μπορεί να εντοπίσει τις αλλαγές στις συνθήκες περιβάλλοντος και ετοιμάζεται να προσαρμοστεί στις νέες συνθήκες. Όταν οι αλλαγές (εσωτερικές ή εξωτερικές) ολοκληρωθούν, το πρωτόκολλο επαναρυθμίζεται έτσι ώστε οι ασφαλείς υπηρεσίες δρομολόγησης να συνεχίσουν να υφίστανται.

Κεφάλαιο 5

Συμπεράσματα και Προοπτική

Ύστερα από όλη την ενασχόλησή μας με τα Ασύρματα Δίκτυα Αισθητήρων το πιο σημαντικό που έχουμε να πούμε, το οποίο όμως είναι ταυτόχρονα και το πιο απλό, είναι ότι παρουσιάζουν εξαιρετικό ενδιαφέρον. Αξίζει να δούμε τους λόγους για τους οποίους συμβαίνει αυτό: Πρώτον, συνδυάζουν πολύ καλά πάρα πολούς τομείς της επιστήμης των υπολογιστών. Δεύτερον, τα προβλήματα τα οποία καλούμαστε να λύσουμε περιλαμβάνουν εκτός από τεχνικούς περιορισμούς και φυσικά εμπόδια (κίνηση, αντικείμενα μεταξύ των συσκευών κλπ), έτσι καλούμαστε να επιστρατεύσουμε αρκετή δημιουργικότητα προκειμένου να τα λύσουμε.

Υπάρχει και ένας παράγοντας εδώ που παίζει πολύ σημαντικό ρόλο αν και, ευτυχώς ή δυστυχώς, δεν θα συνεχίσει να παίζει ρόλο στο μέλλον. Αυτός είναι ότι το περιβάλλον λειτουργίας ενός Ασύρματου Δικτύου Αισθητήρων, οι θεωρητικοί ορισμοί, τα τεχνικά μέρη των συσκευών, οι απαιτήσεις μιας εφαρμογής, κλπ δεν είναι σαφώς ορισμένα διότι η έρευνα γύρω από τα Ασύρματα Δίκτυα Αισθητήρων βρίσκεται σε σχετικά εμβρυακό στάδιο. Είδαμε ήδη πόσο πολύ μεγάλο ρόλο παίζει η περιγραφή του μοντέλου σε ένα πρωτόκολλο ή έναν αλγόριθμο για αυτόν το λόγο. Αυτή η πραγματικότητα δίνει τη δυνατότητα μερικές φορές σε έναν σχεδιαστή αντί να προσαρμόζει τις ιδέες του και τον αλγόριθμό του στο μοντέλο λειτουργίας, να προσαρμόζει το μοντέλο στις ιδέες του. Δηλαδή, έχοντας κάποια βασική ιδέα, ο σχεδιαστής μπορεί να επιλέξει σε ποιο μοντέλο λειτουργίας θα την εφαρμόσει. Αυτό κάνει συνήθως αρκετά πιο εύκολη τη δουλειά ενός σχεδιαστή. Αν και πολλές φορές το μοντέλο μπορεί να είναι μη ρεαλιστικό ή να ισχύει σε εξαιρετικά περιορισμένες περιπτώσεις, η συνεισφορά του αλγορίθμου δεν αποκλείεται να είναι πολύ σημαντική καθώς οι βασικές του ιδέες ίσως να μπορούν να προσαρμοστούν σε άλλα πιο ρεαλιστικά μοντέλα, ή οι ευνοϊκές συνθήκες ενός μοντέλου που υιοθετούμε να μπορούν να υλοποιούνται σε κάποιο υποπρωτόκολλο. Στα πλαίσια της μελέτης μας είδαμε πολλά τέτοια παραδείγματα. Κατά τη γνώμη μου, η ισορροπία ευκολίας και δυνατότητας ουσιαστικής συνεισφοράς στην έρευνα που παρέχουν τα Ασύρματα Δίκτυα Αισθητήρων τους προσδίδουν ένα μοναδικό ενδιαφέρον.

Η έλλειψη θεωρητικής και τεχνικής τεκμηρίωσης στα Ασύρματα Δίκτυα Αισθητήρων αντανακλάται έντονα στις πλατφόρμες υλοποίησης και στα περιβάλλοντα εξομοίωσης, όπου η επιστημονική κοινότητα ταλαντεύεται ανάμεσα σε κάποιες πλατφόρμες ανάπτυξης και εξομοίωσης εφαρμογών. Καθώς στα πλαίσια της παρούσας μελέτης δεν προχωρήσαμε στην υλοποίηση του βασικού πρωτοκόλλου που παρουσιάζουμε, δεν θεωρείται σκόπιμο να γίνει μια αναλυτική περιγραφή των υπάρχοντων πλατφόρμων ανάπτυξης εφαρμογών. Η υλοποίηση του APSR , η δοκιμή του σε εξομοίωση και σε πραγματικές συσκευές αποτελούν το αντικεί-

μενο της μελλοντικής μας εργασίας.

Κλείνοντας αυτήν την μελέτη, και αφού έχουμε ήδη δει κάποιες βασικές αλγοριθμικές προσεγγίσεις, αξίζει να παρατηρήσουμε την ιδιαιτερότητα που παρουσιάζει το ζήτημα της ασφάλειας στα Ασύρματα Δίκτυα Αισθητήρων. Σε αντίθεση με την 'παραδοσιακή' ασφάλεια και κρυπτογραφία, εδώ έχουμε συσκευές χαμηλού κόστους οι οποίες προσπαθούν να συνεργαστούν προκειμένου να επιτύχουν το επιθυμητό επίπεδο ασφάλειας. Δίνουμε επομένως λιγότερη βαρύτητα στα μαθηματικά εργαλεία κρυπτογραφίας και προσπαθούμε να εισάγουμε λογικές των κατανεμημένων αλγορίθμων στην ασφάλεια. Προσπαθούμε δε να προσαρμοστούμε, ή ακόμα και να εκμεταλλευτούμε τις ιδιαίτερες συνθήκες που επικρατούν στο περιβάλλον, όπως την κινητικότητα. Καταθέτοντας και την προσωπική μου εμπειρία, μπορώ να πω ότι αυτή η προσέγγιση δίνει μια τελείως διαφορετική οπτική γωνία στο θέμα της ασφάλειας ενώ ταυτόχρονα συνδυάζεται με τους μηχανισμούς δρομολόγησης δίνοντας και σε αυτόν τον τομέα ξεχωριστό ενδιαφέρον.

Bibliography

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: a survey. *Journal of Computer Networks*, 38:393–422, 2002.

[2] F. Anjum, D. Subhadrabandhu, S. Sarkar, and R. Shetty. On optimal placement of intrusion detection modules in sensor networks. In *1st International Conference on Broadband Networks (BROADNETS)*, 2004.

[3] K. Bairaktaris, I. Chatzigiannakis, V. Liagkou, and P.G. Spirakis. Adaptive probabilistic secure routing in mobile wireless sensor networks. In *Software, Telecommunications and Computer Networks, 2008. SoftCOM 2008. 16th International Conference on*, pages 208–212, 2008.

[4] I. Blake, G. Seroussi, and N. Smart. Elliptic curves in cryptography. Technical report, Cambridge University Press, 1999. London Mathematical Society Lecture Note Series 265.

[5] N. Bulusu, D. Estrin, L. Girod, and J. Heidemann. Scalable coordination for wireless sensor networks: self-configuring localization systems. In *International Symposium on Communication Theory and Applications (ISCTA 2001)*, 2001.

[6] D. Burton. *Elementary Number Theory*. McGraw-Hill Publishing Company, 4th edition, 1998.

[7] I. Chatzigiannakis, A. Kinalis, S. Nikoletseas, and J. Rolim. Fast and energy efficient sensor data collection by multiple mobile sinks. *Proceedings of the 5th ACM international workshop on Mobility management and wireless access*, pages 25–32, 2007.

[8] Ioannis Chatzigiannakis, T. Dimitriou, Sotiris Nikoletseas, and Paul Spirakis. A probabilistic forwarding protocol for efficient data propagation in sensor networks. In *5th European Wireless Conference on Mobile and Wireless Systems beyond 3G (EW 2004)*, pages 344–350, 2004.

[9] Ioannis Chatzigiannakis, E. Konstantinou, V. Liagkou, and Paul Spirakis. Design, analysis and performance evaluation of group key establishment in wireless sensor networks. In *2nd Workshop on Cryptography for Ad hoc Networks*. Springer-Verlag, 2006. ICALP 2006 Workshop, Electronic Notes in Theoretical Computer Science.

[10] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22:644–654, 1976.

[11] T. Dimitriou. Securing communication trees in sensor networks. In *2nd International Workshop on Algorithmic Aspects of Wireless Sensor Networks (ALGOSENSORS 2006)*. Springer-Verlag, 2006. Lecture Notes in Computer Science.

[12] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31:469–472, 1985.

[13] G. Gaubatz, J. Kaps, and B. Sunar. Public key cryptography in sensor networks – revisited. In *1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004)*, pages 2–18. Springer-Verlag, 2004. Lecture Notes in Computer Science, LNCS 3313.

[14] Wendi R. Heinzelman, Anantha P. Chandrakasan, and Hari Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. In *33rd IEEE Hawaii International Conference on System Sciences (HICSS 2000)*, page 8020, 2000.

[15] Wendi R. Heinzelman, Anantha P. Chandrakasan, and Hari Balakrishnan. An application-specific protocol architecture for wireless microsensor networks. *IEEE Transactions on Wireless Communications*, 1(4):660–670, October 2002.

[16] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva. Directed diffusion for wireless sensor networking. Technical report, University of Southern California, 2002. Extended version.

[17] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. In *1st IEEE International Workshop on Sensor Network Protocols and Applications*, 2003.

[18] P. Leone, L. Moraru, O. Powell, and J. Rolim. A localization algorithm for wireless ad-hoc sensor networks with traffic overhead minimization by emission inhibition. In *2nd International Workshop on Algorithmic Aspects of Wireless Sensor Networks (ALGOSENSORS 2006)*. Springer-Verlag, 2006. Lecture Notes in Computer Science.

[19] N. A. Lynch. *Distributed Algorithms*. Morgan Kaufmann Publishers Inc, 1996.

[20] U. Maurer. Modelling a public-key infrastructure. *Proceedings of the 1996 European Symposium on Research in Computer Security*, pages 325–350, 1996.

[21] P. Naik and K.M. Sivalingam. A survey of MAC protocols for sensor networks. *Wireless sensor networks*, pages 93–107, 2004.

[22] Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen, and David E. Culler. Spins: security protocols for sensor networks. *Wireless Networks*, 8(5):521–534, 2002.

[23] Antony I. T. Rowstron and Peter Druschel. Pastry: Scalable, decentralized object location, and routing for large-scale peer-to-peer systems. In *IFIP/ACM International Conference on Distributed Systems Platforms Middleware 2001*, pages 329–350. Springer-Verlag, 2001. Lecture Notes in Computer Science, LNCS 2218.

[24] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer Verlag, 1986.

[25] K. Sohraby, D. Minoli, and T. Znati. *Wireless Sensor Networks: Technology, Protocols, and Applications*. Wiley-Interscience, 2007.

[26] M. Steiner, G. Tsudik, and M. Waidner. Diffie-Hellman key distribution extended to group communication. In *3rd ACM Conference on Computer and Communications Security (CCS 1996)*, pages 31–37. ACM Press, 1996.