ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ
ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

Ασφάλεια σε δίκτυα ad hoc και δίκτυα αισθητήρων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Δημήτριος Κ. Κουτσουβέλας
Ηλίας Δ. Κωστούδης

Επιβλέπων: Θεολόγου Μιχαήλ
Καθηγητής Ε.Μ.Π.

Αθήνα, Νοέμβριος 2008

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ
ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

Ασφάλεια σε δίκτυα ad hoc και δίκτυα αισθητήρων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Δημήτριος Κ. Κουτσουβέλας
Ηλίας Δ. Κωστούδης

Επιβλέπων: Θεολόγου Μιχαήλ
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 24η Νοεμβρίου 2008.

.....	.....	.....
Θεολόγου Μιχαήλ	Βέργαδος Δημήτριος	Συκάς Ευστάθιος
Καθηγητής Ε.Μ.Π	Λέκτορας Παν. Πειραιώς	Καθηγητής Ε.Μ.Π

Αθήνα, Νοέμβριος 2008

.....
Δημήτριος Κ. Κουτσουβέλας
Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

…..……..
Ηλίας Δ. Κωστούδης
Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Θα θέλαμε, στο σημείο αυτό, να ευχαριστήσουμε θερμά τον επιβλέποντα καθηγητή κ. Μιχαήλ Θεολόγου για τη δυνατότητα που μας έδωσε να εκπονήσουμε την παρούσα διπλωματική εργασία. Επίσης, ευχαριστούμε τον κ. Δημήτριο Βέργαδο, λέκτορα Πανεπιστημίου Πειραιώς, για τη βοήθεια και την καθοδήγησή του σε όλη τη διάρκεια της προσπάθειας και τον κ. Νικόλαο Πανταζή, επίκουρο καθηγητή ΤΕΙ Αθήνας, για τις πολύτιμες παρατηρήσεις του κατά τη συγγραφή της διπλωματικής εργασίας και την παραχώρηση χρησιμοποίησης κατάλληλων αισθητήρων για την πειραματική εφαρμογή του ασύρματου ad hoc δικτύου.

Δημήτριος Κουτσουβέλας
Ηλίας Κωστούδης

Νοέμβριος 2008

ΠΕΡΙΛΗΨΗ

Η εξέλιξη των ασύρματων επικοινωνιών και των ηλεκτρονικών έχει οδηγήσει στη δημιουργία δικτύων χαμηλού κόστους, χωρίς συγκεκριμένη δομή. Τα δίκτυα αυτά, (όπως είναι τα ad hoc δίκτυα και μία περίπτωσή τους, τα δίκτυα αισθητήρων) αποτελούνται από μικρού μεγέθους κόμβους, οι οποίοι δεν έχουν μια συγκεντρωτική διαχείριση. Καθώς τα συγκεκριμένα δίκτυα γίνονται κομμάτι της καθημερινής ζωής, η ασφάλειά τους αποτελεί ένα γόνιμο πεδίο έρευνας.

Τα θέματα ασφαλείας στα ad hoc δίκτυα και στα δίκτυα αισθητήρων είναι διαφορετικά απ' ότι στα σταθερά δίκτυα. Αυτό οφείλεται στο γεγονός ότι οι απαιτήσεις και οι ιδιαιτερότητες αυτών των δικτύων (όπως είναι η περιορισμένη ενέργεια και η κινητικότητα), διαφέρουν από αυτές των σταθερών.

Στην εργασία αυτή αναφερόμαστε γενικά στα ad hoc δίκτυα και στα δίκτυα αισθητήρων. Συγκεκριμένα αναφέρουμε τα χαρακτηριστικά των δυο δικτύων, τα πρωτόκολλα δρομολόγησης που χρησιμοποιούνται, καθώς επίσης και την πιστοποίηση (authentication). Επίσης παρουσιάζουμε θέματα ασφαλείας στα δύο είδη δικτύων και προτεινόμενα μέτρα αντιμετώπισης απειλών. Στη συνέχεια γίνεται μία ταξινόμηση (classification) των δεδομένων σε θέματα ασφαλείας, σύμφωνα με τα κοινά τους χαρακτηριστικά. Έπειτα παρουσιάζεται ένα κεφάλαιο που ασχολείται αποκλειστικά με τα στρατιωτικά δίκτυα (military networks).

Τέλος, μετά τα συμπεράσματά μας, εξετάζεται σε παράρτημα πειραματικά ένα δίκτυο αισθητήρων, λαμβάνονται κάποιες μετρήσεις και επισημαίνονται δυνατότητες και προοπτικές.

ABSTRACT

The evolution of wireless communications and electronic devices has lead in the creation of low-cost infrastructureless networks. Those networks (such as ad hoc networks and their special category, sensor networks) consist of small in size nodes with no centralized administration. As ad hoc and sensor networks are becoming part of our everyday life, their security represents a fertile field of research.

The security issues in ad hoc and sensor networks are different than those for the fixed networks. This is due to the requirements and the features of those networks (such as energy efficiency and mobility).

This work deals with ad hoc and sensor networks in general. In particular, we mention the features of the networks, the routing protocols and the authentication. Moreover we introduce security issues and intended techniques of defending against threats. Thereafter a classification of security items takes place. Next, a chapter referring exclusively to military networks is viewed.

Finally, after our conclusions, a particular sensor network is examined in an appendix**,** some measurements are taken and capabilities and perspectives are highlighted.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 4^{Ο}
ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ AD HOC ΚΑΙ ΔΙΚΤΥΩΝ ΑΙΣΘΗΤΗΡΩΝ

ΚΕΦΑΛΑΙΟ 5^{Ο}
CLASSIFICATION ΑΣΦΑΛΕΙΑΣ

Κατάλογος Σχημάτων

ΚΕΦΑΛΑΙΟ 1^{Ο}

ΕΙΣΑΓΩΓΗ

1.1 Γενικά για ασύρματες επικοινωνίες

Η ανάγκη του ανθρώπου για επικοινωνία, έχει παρατηρηθεί από αρχαιοτάτων χρόνων. Η ανταλλαγή πληροφορίας, κυρίως για οικονομικούς και εμπορικούς λόγους, ήταν αυτή που ώθησε την επιστήμη στην προσπάθεια ανακάλυψης νέων τεχνολογιών.

Αρχικά η πληροφορία μεταδιδόταν μέσω της υποδομής που υπήρχε για τις φυσικές μεταφορές και κατά συνέπεια, μεταφερόταν μεταξύ τόπων όπου υπήρχαν εμπορικές δραστηριότητες, όπως λ.χ. μεταξύ πόλεων. Με την ανάπτυξη των επικοινωνιών, η μετάδοση της πληροφορίας δεν χρειαζόταν να ακολουθήσει φυσικά δρομολόγια. Επιπλέον, η ανακάλυψη νέων τεχνολογιών βελτίωσε την απόδοση της μεταφοράς της πληροφορίας. Αρχικά ο τηλέγραφος, στη συνέχεια το τηλέφωνο και τέλος οι ασύρματες επικοινωνίες ήταν αυτές που έδωσαν ώθηση στην τεχνολογία της επικοινωνίας.

Η μετάδοση τηλεπικοινωνιακών σημάτων γίνεται κατά δύο τρόπους, είτε με χρήση ενσύρματων μέσων (σταθερή τηλεφωνία), είτε με ασύρματη μετάδοση. Η ενσύρματη επικοινωνία (γραμμές μεταφοράς, κυματοδηγοί και οπτικές ίνες) προτιμάται κυρίως για την τηλεπικοινωνιακή διασύνδεση σημείων που είναι σταθερά και σε μικρή γεωγραφική έκταση. Αντίθετα, η ασύρματη επικοινωνία στηρίζεται στην ηλεκτρομαγνητική ακτινοβολία και χρησιμοποιεί κεραίες για την εκπομπή και λήψη σημάτων. Στα τέλη του 19^{ου} αιώνα, ο G. Marconi υλοποίησε για πρώτη φορά ένα σύστημα ασύρματης μετάδοσης, βασιζόμενος στην θεωρία που είχε διατυπώσει ο Maxwell. Μέχρι το 1940 χρησιμοποιούνταν συνήθως συχνότητες UHF. Από την δεκαετία του ’40 και έπειτα, η αλματώδης ανάπτυξη της πληροφορικής και της ηλεκτρονικής σε συνδυασμό με την αύξηση του όγκου πληροφορίας, έχουν οδηγήσει στην ανάπτυξη νέων τεχνολογιών.

Η προτίμηση των ασύρματων ως προς τις ενσύρματες επικοινωνίες οφείλεται σε ορισμένα προτερήματα που έχουν. Έτσι, ως συγκριτικά πλεονεκτήματα αναφέρονται τα παρακάτω:

- Η αλγεβρική απόσβεση του ηλεκτρομαγνητικού κύματος καθώς αυξάνεται η απόσταση από την πηγή. Αντίστοιχα, στα ενσύρματα μέσα, παρατηρείται εκθετική απόσβεση του ηλεκτρομαγνητικού κύματος.
- Το σχετικά μικρό κόστος εγκατάστασης και λειτουργίας ενός δικτύου, σε αντίθεση με το μεγάλο κόστος στο ενσύρματο δίκτυο.
- Η δυνατότητα κινητών επικοινωνιών.

Με τον καιρό αναπτύχθηκε ένας μεγάλος αριθμός ασύρματων δικτύων ανάλογα με το σκοπό και τα αντίστοιχα μέσα που διατίθενται για τη δημιουργία τους.

1.2 Γενικά περί Ad hoc και Sensor δικτύων. Ομοιότητες και διαφορές

Ένα ad hoc δίκτυο είναι μία συλλογή αυτόνομων κόμβων που δεν στηρίζονται σε μία προκαθορισμένη δομή για να κρατάει το δίκτυο σε συνοχή. Οι κόμβοι επικοινωνούν μεταξύ τους χρησιμοποιώντας ασύρματη επικοινωνία και λειτουργούν ακολουθώντας ένα μοντέλο ομότιμων οντοτήτων (peer-to-peer). Αυτά τα δίκτυα είναι γνωστά και ως MANET (mobile ad hoc networks) [1]. Η βασική αρχή πίσω από την δικτύωση ad hoc είναι η αναμετάδοση με πολλαπλά άλματα (multi-hop networking). Έτσι οι κόμβοι σ' ένα δίκτυο MANET στηρίζονται ο ένας στον άλλον για να φέρουν σε πέρας βασικές λειτουργίες δικτύων (όπως προώθηση και δρομολόγηση πακέτων).

Οι βασικές διαφορές οι οποίες υπάρχουν μεταξύ ενός ad hoc δικτύου και ενός δικτύου με σταθερή υποδομή αναφέρονται παρακάτω [2]:

- *Μεταβλητή τοπολογία*: Η τοπολογία του δικτύου σ' ένα ad hoc δίκτυο είναι δυναμική λόγω της κινητικότητας των κόμβων. Μπορούν να κινούνται μέσα και έξω από την εμβέλεια των κόμβων. Αυτό δυσκολεύει τη διαχείριση του δικτύου.
- *Περιορισμένη ενέργεια*: Οι κινητές συσκευές χρησιμοποιούν γενικά ισχύ μπαταρίας, η οποία δεν είναι ανεξάντλητη. Για να εξοικονομήσουν ενέργεια μπορούν να πέσουν σε λειτουργία αδράνειας. Κατά τη διάρκεια αυτή, μπορεί να μην είναι προσβάσιμες ή να μην προωθούν την κυκλοφορία ή να επανέρχονται σε κανονική κατάσταση με αργοπορία.
- *Περιορισμός επεξεργαστή*: Ορισμένες κινητές συσκευές έχουν φθηνούς και αργούς επεξεργαστές, διότι οι γρήγοροι επεξεργαστές είναι ακριβοί. Γι' αυτό χρειάζεται περισσότερος χρόνος να εκτελέσουν πολύπλοκους υπολογισμούς.
- *Περιορισμένη ικανότητα αποθήκευσης και περιορισμός άλλων πηγών*: Λόγω του μεγέθους και των περιορισμών κόστους, οι περισσότερες κινητές συσκευές έχουν περιορισμένη ικανότητα αποθήκευσης.
- *Εφήμερη σύνδεση και διαθεσιμότητα*: Ορισμένοι κόμβοι μπορεί να μην είναι διαθέσιμοι για κάποια περίοδο, ώστε να μπορούν να εξοικονομούν ενέργεια.
- *Κάθε κόμβος είναι και δρομολογητής*: Οι κόμβοι που βρίσκονται εκτός εμβέλειας ενός σταθερού κόμβου δεν μπορούν να ανιχνευθούν απ' ευθείας απ' αυτόν τον κόμβο αλλά πρέπει να ανιχνευθούν μέσω άλλων κόμβων.
- *Διαμοιρασμένο φυσικό μέσο*: Αντίθετα προς τα ενσύρματα δίκτυα, κάθε συσκευή μπορεί να χρησιμοποιήσει το μέσο μετάδοσης μέσα στο όριο εμβέλειάς της.
- *Έλλειψη κεντρικής διοίκησης*: Τα ad hoc δίκτυα μπορούν να δημιουργηθούν οπουδήποτε. Γενικά, δεν υπάρχει κεντρική διοίκηση και έτσι μπορούμε να υποθέσουμε ότι δεν διαμοιράζεται οποιαδήποτε πληροφορία μεταξύ των κόμβων.

Λόγω των παραπάνω διαφορών, είναι πολύπλοκο να εφαρμόσουμε και να προσαρμόσουμε πρωτόκολλα και άλλες τεχνολογίες των δικτύων με σταθερή υποδομή σε πρωτόκολλα ad hoc.

Ένα συγκεκριμένο είδος ad hoc δικτύου είναι τα δίκτυα αισθητήρων (sensor networks). Τα δίκτυα αισθητήρων αποτελούνται από ένα μεγάλο αριθμό συσκευών με ικανότητες ευαισθησίας, που μπορούν να εκτελέσουν απλά θέματα προώθησης πληροφοριών και να επικοινωνήσουν ασύρματα με άλλες παρόμοιες συσκευές. Αυτά τα δίκτυα αναπτύσσονται σε οποιοδήποτε μέσο διασκορπίζοντας τους κόμβους σε μία περιοχή ενδιαφέροντος. Μετά την ανάπτυξή τους, οι κόμβοι ξεκινούν έναν αλγόριθμο για να δημιουργήσουν ομάδες, κανάλια επικοινωνίας, ιεραρχία κ.ά. Με την

εγκατάστασή του, το δίκτυο αναμένεται να λειτουργήσει για μεγάλο χρονικό διάστημα χωρίς ανθρώπινη επιτήρηση ή ανάγκη αναπλήρωσης και αντικατάστασης των κόμβων λόγω έλλειψης ενέργειας [3].

Η ανάπτυξη αυτών των δικτύων χρειάζεται τεχνικές ad hoc δικτύων. Παρακάτω παρατίθενται οι κυριότερες ομοιότητες μεταξύ των ad hoc δικτύων και των δικτύων αισθητήρων [4]:

- *Κατάσταση ad hoc*: Δεν υπάρχει συγκεκριμένη υποδομή. Οι οντότητες του δικτύου επικοινωνούν μεταξύ τους με πολλαπλές ασύρματες συνδέσεις.
- *Περιορισμοί πόρων:* Οι κόμβοι και των δύο δικτύων είναι περιορισμένων πόρων. Οι κόμβοι στο ad hoc δίκτυο έχουν μικρή δυναμικότητα ισχύος. Οι κόμβοι-αισθητήρες ακόμα μικρότερη.
- *Θέματα ισχύος:* Οι κόμβοι έχουν συνήθως μπαταρίες (επαναφορτιζόμενες ή μη). Αλγόριθμοι που χρησιμοποιούν αποτελεσματικά την ενέργεια βελτιώνουν την απόδοση του συστήματος.
- *Ασύρματη επικοινωνία:* Και τα δύο δίκτυα στηρίζονται σε ασύρματη επικοινωνία.

Παρόλο ότι υπάρχουν πολλά πρωτόκολλα που εφαρμόζονται άριστα σε ad hoc δίκτυα, δεν είναι ικανά να εξυπηρετήσουν τα ιδιαίτερα χαρακτηριστικά των δικτύων αισθητήρων. Για να κατανοήσουμε αυτό το σημείο θα αναφέρουμε τις διαφορές μεταξύ δικτύων ad hoc και δικτύων αισθητήρων [4,5].

- Ο αριθμός των κόμβων σ' ένα δίκτυο αισθητήρων είναι πολύ μεγαλύτερος απ' ότι σ' ένα ad hoc δίκτυο.
- Οι κόμβοι αισθητήρων αναπτύσσονται πυκνά.
- Οι κόμβοι αισθητήρων έχουν προδιάθεση στην αποτυχία και έτσι κάθε φορά τα κανάλια επικοινωνίας εκπέμπουν χωρίς μηχανισμό επιβεβαίωσης.
- Η τοπολογία ενός δικτύου αισθητήρων αλλάζει πολύ συχνά. Η αποτυχία των κυκλωμάτων αισθητήρων και η εξάντληση της μπαταρίας οδηγούν στη συνεχή εναλλαγή της τοπολογίας. Στα ad hoc δίκτυα, αντίθετα, οι κόμβοι έχουν την ικανότητα να κινούνται, ενώ σ' ένα δίκτυο αισθητήρων μόνο η δεξαμενή (sink) και η προέλευση των δεδομένων κινούνται.
- Οι κόμβοι αισθητήρων χρησιμοποιούν μία επικοινωνία ευρείας εκπομπής, ενώ τα περισσότερα ad hoc δίκτυα χρησιμοποιούν επικοινωνία σημείου-προς-σημείο.
- Οι κόμβοι αισθητήρων έχουν μεγαλύτερο περιορισμό σε ισχύ, ικανότητες υπολογισμών και μνήμης. Έτσι, ενώ τα ad hoc δίκτυα έχουν επεξεργαστές εκατοντάδων MHz, οι επεξεργαστές των αισθητήρων είναι πολύ μικρότεροι.
- Οι κόμβοι αισθητήρων πιθανόν να μην έχουν μια κοινή ταυτότητα για όλο το δίκτυο λόγω του μεγάλου αριθμού κόμβων. Αντίθετα, στα ad hoc δίκτυα οι οντότητες έχουν ένα μοναδικό ID (π.χ. διεύθυνση MAC ή IP).
- Στη σχεδίαση των ad hoc δικτύων εφαρμόζεται η αρχή της διαστρωμάτωσης. Αντίθετα στα δίκτυα αισθητήρων εφαρμόζεται η αρχή "όλα σε ένα" που είναι πιο κατάλληλη.

1.3 Ο ρόλος και η σημασία της ασφάλειας στα ad hoc και sensor δίκτυα

Η ασφάλεια στα ασύρματα δίκτυα και κυρίως στα ad hoc δίκτυα, είναι ένα πολύ σημαντικό κομμάτι της ευρωστίας των δικτύων και της λειτουργίας τους. Ένα δίκτυο, εκτός από τις λειτουργίες της δημιουργίας και μετάδοσης μηνυμάτων, για να μπορέσει να εκτελέσει την αποστολή του ομαλά, πρέπει να μπορεί να είναι ασφαλές κατά την διάρκεια της λειτουργίας του. Και όταν λέμε ασφαλές, πρέπει να μπορεί κάθε κομμάτι του δικτύου να στέλνει και να δέχεται ασφαλή μηνύματα.

Η ασφάλεια στα ad hoc και τα sensor δίκτυα είναι δύσκολο να επιτευχθεί, λόγω της αδυναμίας των ασύρματων ζεύξεων, της περιορισμένης φυσικής προστασίας των κόμβων του δικτύου, της δυναμικά μεταβαλλόμενης τοπολογίας, της έλλειψης μιας αρχής πιστοποίησης και της έλλειψης ενός κεντρικού σημείου ελέγχου και διαχείρισης [6]. Για να μπορέσουμε να εξασφαλίσουμε ότι ένα δίκτυο είναι ασφαλές, πρέπει να διασφαλίσουμε ότι το κάθε κομμάτι που αποτελεί το δίκτυο είναι ασφαλές. Όπως αναφέραμε στο προηγούμενο κεφάλαιο, τα ad hoc και sensor δίκτυα αποτελούνται από ένα μεγάλο αριθμό κόμβων. Η ασφάλεια του δικτύου επιβάλλει να είναι κάθε κόμβος ασφαλής ώστε να μπορεί να ανταλλάσει μηνύματα με τους γειτονικούς κόμβους και με τον σταθμό βάσης.

Παρόλο που η ασφάλεια στα sensor δίκτυα φαίνεται να είναι ίδια με αυτή των ad hoc δικτύων (λόγω των παρόμοιων μοντέλων συστημάτων και για τα δύο είδη δικτύων), υπάρχουν εμφανείς διαφορές στις απαιτήσεις ασφαλείας των δύο δικτύων. Αυτό οφείλεται στις διαφορετικές εφαρμογές για τις οποίες χρησιμοποιούνται τα δύο δίκτυα και στις διαφορές που υπάρχουν μεταξύ των δύο δικτύων, όπως αναφέρθηκαν στο προηγούμενο κεφάλαιο [4]. Έτσι, λόγω των ιδιαίτερων χαρακτηριστικών των αισθητήρων (μεγαλύτερη πυκνότητα δικτύων, μεγαλύτερη πιθανότητα αποτυχίας, περιορισμοί ισχύος-υπολογισμών-μνήμης), πρέπει να λαμβάνεται πιο σοβαρά υπ' όψιν η ασφάλεια για την εύρυθμη λειτουργία του δικτύου.

1.4 Σύντομη περιγραφή των θεμάτων που θα διαπραγματευθεί η παρούσα εργασία

Στην παρακάτω εργασία, αναπτύσσονται αναλυτικά θέματα που αφορούν τα ad hoc και τα sensor δίκτυα. Έτσι, στο 2^{ο} κεφάλαιο περιγράφονται τα ad hoc δίκτυα, τα χαρακτηριστικά τους, οι εφαρμογές τους και τα πρωτόκολλα δρομολόγησης που χρησιμοποιούνται. Γίνεται μια ιδιαίτερη αναφορά στα ασύρματα ad hoc δίκτυα (τα γνωστά MANET) και καταλήγουμε με τους τρόπους βελτίωσης της QoS (ποιότητας υπηρεσίας) στα εν λόγω δίκτυα.

Αντίστοιχα, στο 3^{ο} κεφάλαιο αναπτύσσονται τα δίκτυα αισθητήρων (sensor). Παρόμοια με τα ad hoc δίκτυα, αναφέρονται τα χαρακτηριστικά των δικτύων αισθητήρων, οι παράγοντες σχεδίασής τους και η αρχιτεκτονική ενός τέτοιου είδους δικτύου. Τέλος, καταλήγουμε με ένα κεφάλαιο για τις εφαρμογές των δικτύων αισθητήρων.

Στο 4^{ο} κεφάλαιο αναλύεται η ασφάλεια των δύο δικτύων. Έτσι περιγράφονται αναλυτικά οι απαιτήσεις ασφαλείας, οι περιορισμοί ενός συστήματος και τα είδη των απειλών-επιθέσεων που δέχονται τα δύο δίκτυα. Αναλύεται η ασφάλεια στα επίπεδα

κατά το σύστημα OSI και τα μέτρα αντιμετώπισης των απειλών. Τέλος καταλήγουμε με μία σύντομη περιγραφή των υπαρχόντων πρωτοκόλλων ασφαλείας.

Στο 5^{ο} κεφάλαιο παρουσιάζεται μια ταξινόμηση των θεμάτων ασφαλείας των δικτύων που μας αφορούν. Έτσι εξετάζονται αναλυτικά τέσσερα βασικά θέματα: Η ασφάλεια των κόμβων, οι αλγόριθμοι που χρησιμοποιούνται για την επικοινωνία μεταξύ κόμβων, η πιστοποίηση που εκτελείται για την ασφάλεια της επικοινωνίας και τέλος η εργασία της δρομολόγησης και η εύρεση πολλαπλών δρομολογίων.

Στο 6^{ο} κεφάλαιο παρουσιάζεται μία μελέτη που ασχολείται με στρατιωτικά δίκτυα. Μια σύντομη ιστορική αναδρομή γίνεται αρχικά για τα δίκτυα αυτά. Αναφέρονται επιγραμματικά τα πρωτόκολλα που χρησιμοποιούν, καθώς επίσης και οι ιδιαιτερότητες που παρουσιάζουν. Τέλος γίνεται μια ταξινόμηση των δικτύων, όπου παρουσιάζονται οι δυσχέρειες και οι περιορισμοί της λειτουργίας τους.

Στο 7^{ο} κεφάλαιο παραθέτουμε τα συμπεράσματα από την εργασία μας.

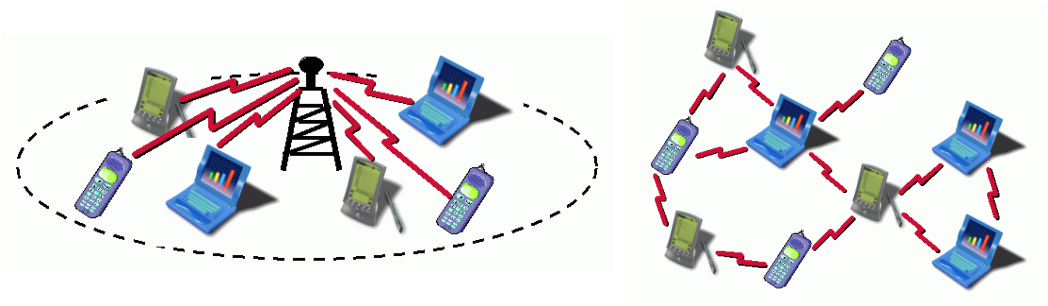
Καταλήγουμε με ένα παράρτημα όπου περιγράφονται τα χαρακτηριστικά των δομικών στοιχείων που χρησιμοποιούνται σε ένα δίκτυο αισθητήρων καθώς και τα πρωτόκολλα επικοινωνίας. Έπειτα γίνεται αναφορά στον τρόπο εγκατάστασης του λογισμικού, στον προγραμματισμό κάθε δομικού στοιχείου και στα προβλήματα που παρουσιάστηκαν κατά τις ενέργειες αυτές. Λαμβάνονται μετρήσεις δεδομένων που είναι διαθέσιμα στους συγκεκριμένους αισθητήρες καθώς και απεικονίσεις της τοπολογίας του δικτύου και της ποιότητας των ζεύξεων μεταξύ των κόμβων. Τέλος, περιγράφεται ο τρόπος πρόσβασης στους αισθητήρες μέσω Ethernet με την χρήση του διαθέσιμου software.

ΚΕΦΑΛΑΙΟ 2^{Ο}

ΔΙΚΤΥΑ AD HOC

2.1 Δίκτυα ad hoc (Γενικά και εφαρμογές)

Η ασύρματη επικοινωνία επιτρέπει τη μεταφορά πληροφοριών μεταξύ ενός δικτύου αποσυνδεδεμένων και συχνά κινητών χρηστών. Τα δημοφιλή ασύρματα δίκτυα, όπως τα δίκτυα κινητής τηλεφωνίας και τα ασύρματα LANs είναι παραδοσιακά βασισμένα σε υποδομή, δηλ. οι σταθμοί βάσεως, τα σημεία πρόσβασης και οι κεντρικοί υπολογιστές (servers) αναπτύσσονται (παίρνουν συγκεκριμένες θέσεις) προτού να μπορέσει να χρησιμοποιηθεί το δίκτυο. Αντίθετα, τα δίκτυα ad hoc, διαμορφώνονται δυναμικά μεταξύ μιας ομάδας ασύρματων χρηστών και δεν απαιτούν καμία υπάρχουσα υποδομή ή προ-διαμόρφωση, όπως φαίνεται στο Σχήμα 1:



Ασύρματο δίκτυο με υποδομή **Ad hoc δίκτυο**

Σχήμα 1. Ασύρματο δίκτυο με υποδομή και ad hoc δίκτυο

Η δυναμική και αυτό-οργανωτική φύση των δικτύων ad hoc τα καθιστά ιδιαίτερα χρήσιμα σε καταστάσεις όπου απαιτούνται γρήγορες επεκτάσεις δικτύων ή η επέκταση και διαχείριση της υποδομής των δικτύων είναι απαγορευτικά δαπανηρές. Μερικά παραδείγματα εφαρμογών περιλαμβάνουν:

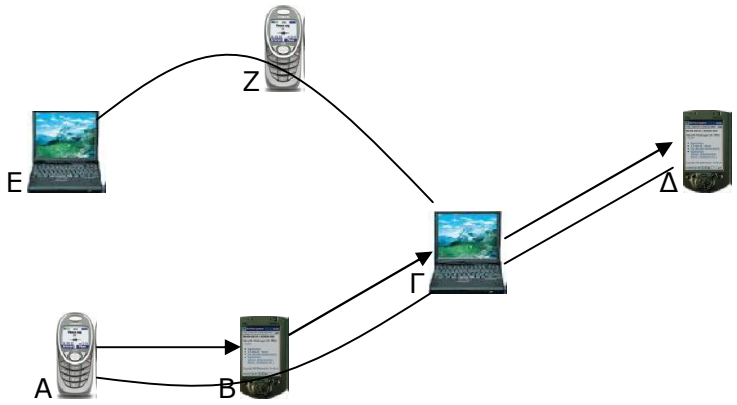
- Τους συμμετέχοντες σε διάσκεψη σε ένα δωμάτιο, που μοιράζονται έγγραφα και άλλες πληροφορίες μέσω των φορητών υπολογιστών.
- Τις ένοπλες δυνάμεις, που δημιουργούν σε άγνωστο έδαφος ένα τακτικό δίκτυο για τις επικοινωνίες και τη διανομή των περιστασιακών πληροφοριών.
- Την τοποθέτηση μικρών συσκευών αισθητήρων σε ζώα και σε άλλες θέσεις που ελέγχουν και παρακολουθούν βιοτόπους και περιβαλλοντικές συνθήκες.
- Τις υπηρεσίες έκτακτης ανάγκης, που επικοινωνούν μεταξύ τους σε μια περιοχή που έχει πληγεί από φυσική ή άλλη καταστροφή και που μοιράζονται video συγκεκριμένων περιοχών με την προϊστάμενη αρχή.

Δυστυχώς, η φύση των δικτύων ad hoc που τα καθιστά ελκυστικά εισάγει επίσης πολλά σύνθετα προβλήματα επικοινωνίας. Αν και μερικά από τα πρώτα ad hoc δίκτυα αναπτύχθηκαν στις αρχές της δεκαετίας του ’70, τα σημαντικά ερευνητικά προβλήματα παραμένουν αναπάντητα.

2.1.1 Χαρακτηριστικά ad hoc δικτύων

Αν και δεν υπάρχει ακόμα ακριβής καθορισμός των γενικών ιδιοτήτων των ad hoc δικτύων, μετά από σύγκριση μερικών από τους ορισμούς, επιλέγουμε αυτόν κατά NIST [7]: " Ένα ασύρματο ad hoc δίκτυο είναι μια συλλογή αυτόνομων κόμβων ή τερματικών που επικοινωνούν ο ένας με τον άλλον με τη διαμόρφωση ενός ραδιοδικτύου πολλαπλών αλμάτων (multi-hop) και διατηρούν τη συνεκτικότητα με έναν αποκεντρωμένο τρόπο''.

Η αρχή πίσω από την ad hoc δικτύωση είναι η αναμετάδοση πολλαπλών αλμάτων, το οποίο σημαίνει ότι τα μηνύματα διαβιβάζονται από τους άλλους κόμβους εάν ο κόμβος-στόχος δεν είναι άμεσα προσπελάσιμος [8]. Η απουσία οποιουδήποτε κεντρικού σταθμού βάσεως καθιστά δύσκολη τη διαχείριση του δικτύου. Το σχήμα 2 επεξηγεί ένα παράδειγμα ενός ειδικού δικτύου που περιέχει δύο φορητούς υπολογιστές, δύο κινητά τηλέφωνα και δύο PDAs. Η τεθλασμένη γραμμή δείχνει την ασύρματη σύνδεση. Από τη στιγμή που ο κόμβος Α δεν μπορεί να φθάσει στον κόμβο Δ άμεσα, τα δεδομένα από το Α στο Δ πρέπει να διαβιβαστούν μέσω των κόμβων Β και Γ.



Σχήμα 2: Ένα δίκτυο ad hoc

Οι κόμβοι ή τερματικά μπορεί να είναι έξυπνοι αισθητήρες, κινητά τηλέφωνα, PDAs και φορητοί υπολογιστές. Οι ασύρματες τεχνολογίες μετάδοσης δεδομένων όπως το Bluetooth [9] και το 802.11 [10], επιτρέπουν την αποδοτική επικοινωνία και χρησιμοποιούνται ευρέως σε στρατιωτικό, εμπορικό και ιδιωτικό περιβάλλον. Οι A.Khalili et al. [2] έχουν απαριθμήσει ένα σύνολο διαφορών μεταξύ των ad hoc δικτύων και των αντίστοιχων που είναι βασισμένα σε υποδομή:

- *Καμία σταθερή τοπολογία:* Η τοπολογία δικτύου σε ένα ad-hoc ασύρματο δίκτυο είναι ιδιαίτερα δυναμική λόγω της κινητικότητας των κόμβων. Μπορεί ο κάθε κόμβος να κινείται μέσα και έξω από την εμβέλεια του άλλου. Η τοπολογία αλλάζει εάν ένα από αυτά τα γεγονότα συμβεί, ενώ ο πίνακας δρομολόγησης και ο πίνακας πολύ-εκπομπής πρέπει να αλλάξουν αναλόγως. Αυτό αυξάνει τη δυσκολία στη διαχείριση του δικτύου.

- *Περιορισμένη ενέργεια:* Οι κινητές συσκευές χρησιμοποιούν γενικά την ενέργεια μπαταριών, η οποία είναι περιορισμένη. Προκειμένου να εξοικονομηθεί ενέργεια, μερικές συσκευές μπορούν να λειτουργούν με έναν αντίστοιχο τρόπο. Κατά τη διάρκεια αυτής της περιόδου, δεν είναι ενδεχομένως προσπελάσιμοι, ή δεν επεξεργάζονται την κίνηση που περνά από αυτούς , ή μεταπίπτουν στον κανονικό τρόπο λειτουργίας με καθυστέρηση. Από τη μια μεριά, οι περισσότερες ασύρματες συσκευές χρησιμοποιούν τις επικοινωνίες εξάπλωσης φάσματος, οι οποίες χρειάζονται τη λήψη και την αποκωδικοποίηση του σήματος. Αυτές είναι ακριβές διαδικασίες που καταναλώνουν πολλή ενέργεια. Αφ' ετέρου, μερικοί σύνθετοι υπολογισμοί είναι επίσης πολύ ακριβοί και καθιστούν δύσκολη την εφαρμογή των συστημάτων δημόσιων κλειδιών στα ad-hoc δίκτυα.
- *Περιορισμένος επεξεργαστής*: Οι περισσότερες κινητές συσκευές έχουν τους φτηνούς και αργούς επεξεργαστές, επειδή οι γρήγοροι επεξεργαστές κοστίζουν πολύ περισσότερο. Ως εκ τούτου παίρνει πολύ χρόνο να εκτελεστούν μερικοί σύνθετοι υπολογισμοί.
- *Περιορισμένη ικανότητα αποθήκευσης και άλλων πόρων*: Λόγω των περιορισμών μεγέθους και δαπανών, οι περισσότερες κινητές συσκευές είναι εξοπλισμένες με περιορισμένη ικανότητα αποθήκευσης. Λόγω των ασύρματων τεχνολογιών, το εύρος ζώνης δικτύων είναι επίσης περιορισμένο.
- *Παροδική συνεκτικότητα και διαθεσιμότητα*: Πολλοί κόμβοι μπορεί να μην είναι προσπελάσιμοι για κάποιο χρόνο ώστε μπορούν να εξοικονομούν ενέργεια.
- *Κάθε κόμβος είναι ένας δρομολογητής*: Οι κόμβοι που είναι εκτός εμβέλειας ενός σταθερού κόμβου, δεν μπορούν να προσπελασθούν άμεσα από αυτόν τον κόμβο. Μπορούν μόνο να προσπελασθούν με την αποστολή πακέτων άλλων κόμβων.
- *Κοινό φυσικό μέσο:* Αντίθετα με τα συνδεδεμένα με καλώδιο δίκτυα, κάθε συσκευή εντός εμβέλειας μπορεί να έχει πρόσβαση στο μέσο μετάδοσης.
- *Έλλειψη κεντρικής διαχείρισης*: Τα ειδικά δίκτυα μπορούν να συσταθούν παντού και κάθε στιγμή. Γενικά δεν υπάρχει διαθέσιμη καμία κεντρική διαχείριση και δεν μπορούμε επίσης να υποθέσουμε ότι όλες οι πληροφορίες μοιράζονται.

Λόγω της έλλειψης σταθερής υποδομής και των περιορισμένων πόρων, θα είναι πιο σύνθετο εδώ να υιοθετηθούν πρωτόκολλα και άλλες τεχνολογίες από ότι στα βασισμένα σε υποδομή δίκτυα.

2.1.2 Υποδομή ad hoc δικτύων

Δεδομένου ότι καμία σταθερή κατηγορία ad-hoc δικτύων δεν είναι διαθέσιμη, χρησιμοποιούμε τις συνήθεις περιπτώσεις, δηλαδή τα κινητά ad-hoc δίκτυα (MANETs) και τα έξυπνα δίκτυα αισθητήρων.

Μαζί με την ανάπτυξη της επόμενης γενιάς των ασύρματων συστημάτων επικοινωνιών, θα υπάρξει ανάγκη για τη γρήγορη επέκταση των ανεξάρτητων

κινητών χρηστών. Μερικά παραδείγματα των πιθανών χρήσεων περιλαμβάνουν τους σπουδαστές που χρησιμοποιούν τους φορητούς υπολογιστές για να συμμετέχουν σε μια διαλογική διάλεξη, τους επιχειρησιακούς συνεταίρους που μοιράζονται τις πληροφορίες κατά τη διάρκεια μιας συνεδρίασης και τον συντονισμό των προσπαθειών του προσωπικού έκτακτης ανάγκης για την ανακούφιση του πληθυσμού έπειτα από μία φυσική καταστροφή. Τέτοια σενάρια δικτύων δεν μπορούν να στηριχθούν στη συγκεντρωμένη και οργανωμένη συνεκτικότητα και μπορούν να εκληφθούν ως εφαρμογές των κινητών ad-hoc δικτύων (MANETs). Ένα MANET είναι μια αυτόνομη συλλογή κινητών χρηστών που επικοινωνούν πέρα από τις - σχετικά περιορισμένες σε εύρος ζώνης - ασύρματες συνδέσεις. Λόγω της κινητικότητας των κόμβων, η τοπολογία δικτύων μπορεί να αλλάξει γρήγορα και απρόβλεπτα.

Ένα ασύρματο ad-hoc δίκτυο αισθητήρων αποτελείται από διάφορους αισθητήρες που εξαπλώνονται πέρα από μια γεωγραφική περιοχή. Κάθε αισθητήρας έχει την ασύρματη ικανότητα επικοινωνίας και κάποιο επίπεδο νοημοσύνης για την επεξεργασία σήματος και τη δικτύωση των δεδομένων. Μερικά παραδείγματα περιλαμβάνουν μια ομάδα στρατιωτών που εγκαθιστούν επικοινωνία ή μια μέτρηση της ατμοσφαιρικής ρύπανσης. Υπάρχουν δύο τρόποι να ταξινομηθούν τα έξυπνα δίκτυα αισθητήρων, με το εάν οι κόμβοι είναι χωριστά προσπελάσιμοι και με το εάν τα δεδομένα στο δίκτυο σωρεύονται. Οι κόμβοι αισθητήρων σε ένα ταχείας κυκλοφορίας δίκτυο πρέπει να είναι χωριστά προσπελάσιμοι, έτσι ώστε ένας να μπορεί να καθορίσει τη θέση των αισθητήρων. Ακόμα η δυνατότητα προσπέλασης των αισθητήρων που χρησιμοποιούνται για να μετρήσουν τη θερμοκρασία και τον αέρα δεν είναι τόσο σημαντική, επειδή αυτοί ποικίλλουν μόνο λίγο όταν βρίσκονται στην ίδια θέση.

Τόσο τα δίκτυα MANETs όσο και τα δίκτυα αισθητήρων μπορούν να ταξινομηθούν περαιτέρω σε δύο ευρείς τύπους: ομοιογενή και ετερογενή δίκτυα. Στα ομοιογενή δίκτυα όλοι οι κόμβοι είναι ίδιοι από την άποψη της ενέργειας μπαταριών και της πολυπλοκότητας του υλικού. Σε ένα ετερογενές δίκτυο αισθητήρων χρησιμοποιούνται δύο ή περισσότεροι διαφορετικοί τύποι κόμβων με διαφορετική ενέργεια μπαταρίας και διαφορετική λειτουργικότητα. Το κίνητρο είναι ότι το πιο σύνθετο υλικό και η πρόσθετη ενέργεια μπαταριών μπορούν να ενσωματωθούν σε μερικούς κόμβους, μειώνοντας με αυτόν τον τρόπο το κόστος υλικού του υπόλοιπου δικτύου.

2.2 Πρωτόκολλα δρομολόγησης

Ένα ad hoc ασύρματο δίκτυο αποτελείται από ένα σύνολο κινητών κόμβων που συνδέονται με ασύρματες ζεύξεις. Όπως έχουμε δει, η τοπολογία δικτύων αλλάζει τυχαία ενώ οι κόμβοι κινούνται. Λόγω της ιδιαίτερα δυναμικής τοπολογίας και της έλλειψης κεντρικής διαχείρισης, τα πρωτόκολλα που χρησιμοποιούνται σε ένα παραδοσιακό δίκτυο για να καθορίσουν μία διαδρομή από έναν κόμβο πηγής σε έναν κόμβο προορισμού δεν μπορούν να χρησιμοποιηθούν άμεσα στα ασύρματα ad hoc δίκτυα. Έτσι, πολλά πρωτόκολλα δρομολόγησης για τα ad hoc δίκτυα έχουν αναπτυχθεί στο πρόσφατο παρελθόν.

2.2.1 Απαιτήσεις (requirements) των πρωτοκόλλων δρομολόγησης

Λόγω των ζητημάτων που προκύπτουν και που συζητήθηκαν παραπάνω, ένα πρωτόκολλο δρομολόγησης για τα ασύρματα ad hoc δίκτυα πρέπει να ικανοποιεί τις ακόλουθες απαιτήσεις:

- Να είναι πλήρως κατανεμημένο.
- Να είναι προσαρμοστικό στις συχνές αλλαγές τοπολογίας.
- Ο καθορισμός των διαδρομών (μέσω υπολογισμών) και η συντήρησή τους να περιλαμβάνουν έναν ελάχιστο αριθμό κόμβων.
- Να υπάρχει ελάχιστος αριθμός σύγκρουσης πακέτων.
- Να παρέχεται ένα ορισμένο επίπεδο ποιότητας της υπηρεσίας (QoS).
- Να χρησιμοποιούνται προσεκτικά οι περιορισμένοι πόροι, όπως το εύρος ζώνης.

2.2.2 Ταξινόμηση των πρωτοκόλλων δρομολόγησης

Μπορούμε να ταξινομήσουμε τα πρωτόκολλα δρομολόγησης για τα ad hoc δίκτυα σύμφωνα με διαφορετικά κριτήρια:

(1). Μηχανισμός πληροφοριών δρομολόγησης με αναπροσαρμογή ή ενημέρωση (update). Αυτά τα πρωτόκολλα μπορούν να ενεργοποιηθούν είτε από έναν πίνακα δρομολόγησης είτε μετά από αίτηση. Στη πρώτη περίπτωση, κάθε κόμβος αποθηκεύει τις πληροφορίες δικτύων σε έναν πίνακα δρομολόγησης, ο οποίος ενημερώνεται περιοδικά. Προκειμένου να φτάσουμε στον προορισμό, ο κόμβος χρησιμοποιεί έναν κατάλληλο αλγόριθμο εύρεσης πορείας για να βρει την πιο σύντομη διαδρομή. Τα χαρακτηριστικά πρωτόκολλα αυτής της περίπτωσης είναι τα εξής: DSDV, WRP, CGSR, STAR, OLSR, FSR, HSR και GSR. Στη δεύτερη περίπτωση οι κόμβοι δεν χρειάζεται να διατηρήσουν την τοπολογία του δικτύου. Η διαδρομή τούς γνωστοποιείται όταν την χρειάζονται, με τη χρησιμοποίηση μιας διαδικασίας σύνδεσης. Το πλεονέκτημα είναι ότι οι κόμβοι δεν χρειάζεται να ανταλλάσουν πληροφορίες δρομολόγησης περιοδικά. Τα χαρακτηριστικά πρωτόκολλα αυτής της περίπτωσης είναι τα: DSR, AODV, ABR, SSA, FORP και PLBR. Μερικά πρωτόκολλα, όπως τα CEDAR, ZRP, ZHLS, συνδυάζουν και τα δύο χαρακτηριστικά γνωρίσματα και ονομάζονται υβριδικά πρωτόκολλα δρομολόγησης.

(2). Χρήση των χρονικών πληροφοριών για τη δρομολόγηση. Αυτή η ταξινόμηση είναι βασισμένη στη χρήση των χρονικών πληροφοριών που χρησιμοποιείται για τη διαδικασία δρομολόγησης. Δεδομένου ότι τα ad hoc δίκτυα είναι ιδιαίτερα δυναμικά, είναι πολύ σημαντικό να χρησιμοποιηθούν οι χρονικές πληροφορίες για τη δρομολόγηση.

Σύμφωνα με το χρόνο των πληροφοριών, παίρνουμε δύο περαιτέρω ταξινομήσεις σε αυτήν την κατηγορία:

a) Πρωτόκολλα δρομολόγησης που χρησιμοποιούν τις πρότερες χρονικές πληροφορίες, δηλ. κάνουν χρήση πληροφόρησης για την προηγούμενη θέση των συνδέσεων ή τη θέση των συνδέσεων κατά τη διάρκεια της δρομολόγησης, ώστε να λάβουν τις αποφάσεις δρομολόγησης. Τέτοια πρωτόκολλα είναι τα DSDV, WRP, STAR, AODV, FSR, HSR, GSR.

b) Πρωτόκολλα δρομολόγησης που χρησιμοποιούν τις μελλοντικές χρονικές πληροφορίες, δηλ. κάνουν χρήση πληροφόρησης για την αναμενόμενη μελλοντική θέση των ασύρματων συνδέσεων προκειμένου να λάβουν τις αποφάσεις δρομολόγησης. Τέτοια πρωτόκολλα είναι τα FORP, RABR, LBR.

(3). Οργάνωση πληροφοριών τοπολογίας. Δεδομένου ότι ο αριθμός κόμβων στα ad hoc δίκτυα είναι γενικά μικρός, είναι πιθανό να χρησιμοποιηθεί είτε μια επίπεδη τοπολογία, είτε μια ιεραρχική τοπολογία για τη δρομολόγηση. Στην πρώτη περίπτωση, πρέπει να υποτεθεί η διαθεσιμότητα ενός μοναδικού μηχανισμού διευθυνσιοδότησης για τους κόμβους στα ad hoc ασύρματα δίκτυα. Πρωτόκολλα όπως τα DSR, AODV, ABR, SSA, FORP, PLBR ανήκουν σε αυτήν την περίπτωση. Τα πρωτόκολλα της δεύτερης περίπτωσης κάνουν χρήση μιας λογικής ιεραρχίας στο δίκτυο και ενός σχετικού σχεδίου διευθυνσιοδότησης. Τα πρωτόκολλα CGSR, FSR, HSR είναι αυτής της περίπτωσης.

(4). Χρησιμοποίηση συγκεκριμένων πόρων. Τα πρωτόκολλα αυτής της κατηγορίας μπορούν να ταξινομηθούν περαιτέρω σε δύο τύπους:

a) Πρωτόκολλα δρομολόγησης ενήμερα για την ενέργεια (*power aware*): Πρωτόκολλα που ανήκουν σε αυτήν την κατηγορία προσπαθούν να ελαχιστοποιήσουν την κατανάλωση ενέργειας από τη μπαταρία. Ένα χαρακτηριστικό πρωτόκολλο είναι το PAR.

b) Πρωτόκολλα δρομολόγησης που υποβοηθούνται από γεωγραφικές πληροφορίες: Τα πρωτόκολλα που ανήκουν σε αυτήν την κατηγορία προσπαθούν να βελτιώσουν την απόδοση της δρομολόγησης και να μειώσουν την επιβάρυνση ελέγχου με αποτελεσματική χρήση των γεωγραφικών πληροφοριών. Ένα χαρακτηριστικό πρωτόκολλο είναι το LAR. Αρκετά από τα πρωτόκολλα που αναφέρονται ανωτέρω περιγράφονται στο [11].

2.3 Δρομολόγηση πολύ-εκπομπής

Λόγω της δυναμικής τοπολογίας, του περιορισμένου εύρους ζώνης και άλλων περιορισμένων πόρων των ad hoc δικτύων, αποτελεί πρόκληση η υιοθέτηση των υπαρχόντων πρωτοκόλλων δρομολόγησης πολλαπλής διανομής των ενσύρματων δικτύων ή η ανάπτυξη νέων πρωτοκόλλων για τα ad hoc δίκτυα.

2.3.1 Απαιτήσεις (requirements) των πρωτοκόλλων πολύ-εκπομπής

Ένα καλό πρωτόκολλο δρομολόγησης πολλαπλής διανομής για τα ad hoc δίκτυα πρέπει να ικανοποιεί τις ακόλουθες απαιτήσεις:

- *Ευρωστία*: Πρέπει να είναι αρκετά σταθερό για να στηρίξει την κινητικότητα των κόμβων και να επιτύχει έναν υψηλό ρυθμό μετάδοσης πακέτων.
- *Αποδοτικότητα:* Η πολλαπλής διανομής αποδοτικότητα ορίζεται ως η αναλογία του αριθμού πακέτων δεδομένων που παραλαμβάνονται από τους δέκτες και του συνολικού αριθμού πακέτων που διαβιβάζονται στα δίκτυα.
- *Επιβάρυνση ελέγχου*: Προκειμένου να ρυθμιστούν οι κόμβοι σε ένα ad hoc δίκτυο, είναι απαραίτητο να ανταλλαχθούν πακέτα ελέγχου. Λόγω του περιορισμένου εύρους ζώνης στα ad hoc δίκτυα, ο αριθμός των πακέτων ελέγχου πρέπει να είναι ο ελάχιστος δυνατός.
- *Ποιότητα υπηρεσίας (QoS):* Οι κύριες παράμετροι για την QoS είναι η ρυθμό-απόδοση, η καθυστέρηση, η παραμόρφωση και η αξιοπιστία.
- *Ανεξαρτησία του πρωτοκόλλου δρομολόγησης απλής (μονής) διανομής:* Ένα πρωτόκολλο δρομολόγησης πολλαπλής διανομής πρέπει να είναι ανεξάρτητο από οποιοδήποτε συγκεκριμένο πρωτόκολλο δρομολόγησης απλής διανομής.
- *Διαχείριση πόρων*: Ένα πρωτόκολλο δρομολόγησης πολλαπλής διανομής πρέπει να χρησιμοποιεί την ελάχιστη ενέργεια και μνήμη.

2.3.2 Ταξινόμηση των πρωτοκόλλων πολύ-εκπομπής

Σύμφωνα με την εξάρτηση από τις εφαρμογές, μπορούμε να ταξινομήσουμε τα πρωτόκολλα δρομολόγησης πολλαπλής διανομής σε δύο τύπους:

1. Ανεξάρτητα από εφαρμογή/γενικά πρωτόκολλα πολλαπλής διανομής. Τα πιο πολλά πρωτόκολλα δρομολόγησης πολλαπλής διανομής είναι αυτής της κατηγορίας. Μπορούν να ταξινομηθούν περαιτέρω ως εξής:
    a) Με βάση την τοπολογία
        i. Βασισμένα σε μορφή δέντρου: Μόνο μια διαδρομή υπάρχει μεταξύ ενός ζεύγους πηγής-δεκτών. Έναντι των βασισμένων σε πλέγμα πρωτοκόλλων, αυτά είναι αποδοτικότερα. Πρωτόκολλα αυτής της τάξης είναι τα MCEDAR, BEMRP, MZRP, ABAM, DDM, WBM.
        ii. Βασισμένα σε μορφή πλέγματος: Μπορούν να υπάρξουν περισσότερες από μία διαδρομές μεταξύ ενός ζεύγους πηγής-δεκτών και ως εκ τούτου τα πρωτόκολλα αυτού του τύπου είναι σταθερότερα από τα βασισμένα σε μορφή δέντρου. Πρωτόκολλα αυτής της τάξης είναι τα AM Route, MAODV, AMRIS.
    b) Με βάση την έναρξη της συνόδου πολλαπλής διανομής

i. Με έναρξη από την πηγή : Στα πρωτόκολλα αυτής της κατηγορίας, η πηγή αρχικοποιεί τον σχηματισμό πολλαπλής διανομής. Πρωτόκολλα αυτής της τάξης είναι τα MZRP, ABAM, AMRIS, ODMRP, DCMP, NSMP.
ii. Με έναρξη από τον δέκτη: Στα πρωτόκολλα αυτής της κατηγορίας, ο δέκτης αρχικοποιεί τον σχηματισμό πολλαπλής διανομής. Πρωτόκολλα αυτής της τάξης είναι τα BEMRP, DDM, WBM, PLBM, FGMP-RA, NSMP.

c) Με βάση το μηχανισμό διατήρησης της τοπολογίας
i. Μαλακή προσέγγιση: Τα πρωτόκολλα που ανήκουν σε αυτήν την κατηγορία στέλνουν πακέτα ελέγχου περιοδικά για να ανανεώσουν τη διαδρομή. Πρωτόκολλα αυτής της τάξης είναι τα MZRP, DDM, ODMRP, DCMP, FGMP-RA, NSMP.
ii. Σκληρή προσέγγιση: Τα πρωτόκολλα που ανήκουν σε αυτήν την κατηγορία στέλνουν πακέτα ελέγχου για να ανανεώσουν τη διαδρομή μόνο όταν ‘σπάζει’ μια σύνδεση. Πρωτόκολλα αυτής της τάξης είναι τα BEMRP, ABAM, WBM, PLBM, AMRIS, CAMP.

2. Εξαρτώμενα από εφαρμογή πρωτόκολλα πολλαπλής διανομής. Τα πρωτόκολλα αυτής της τάξης χρησιμοποιούνται για τη συγκεκριμένη εφαρμογή για την οποία σχεδιάζονται. Μόνο λίγα πρωτόκολλα έχουν αναπτυχθεί, όπως τα RBM, CBM, LBM.

Αρκετά από τα πρωτόκολλα που αναφέρονται ανωτέρω περιγράφονται στο (11).

2.4 CMMP: Ένα αποτελεσματικό πρωτόκολλο διαχείρισης για ασύρματα ad hoc δίκτυα

Μία από τις επιτυχείς και ευρέως επεκταμένες ασύρματες τεχνολογίες τοπικού LAN είναι το πρωτόκολλο IEEE 802.11. Τα πλεονεκτήματα των πρωτοκόλλων 802.11 περιλαμβάνουν την υψηλή ρυθμό-απόδοση, την απρόσκοπτη πρόσβαση καναλιών και το μηχανισμό εξοικονόμησης ενέργειας. Εντούτοις, εάν τα πρωτόκολλα 802.11 εφαρμόζονται στο βασισμένο σε ομάδες (cluster-based) πολύ-διαυλικό περιβάλλον, μπορούν να εμφανιστούν τα ακόλουθα προβλήματα. Κατ' αρχάς, για να εφαρμοστούν στο πολύ-διαυλικό περιβάλλον, απαιτείται ένας αποδοτικός μηχανισμός ανάθεσης καναλιών έτσι ώστε κάθε μία συσκευή να ξέρει σε ποιο κανάλι πρέπει να συντονιστεί. Δεύτερον, εάν ένας κόμβος πυλών δεν μπορεί να συμμετέχει ομαλά σε δύο γειτονικές ομάδες, μπορεί να εμφανιστούν προβλήματα είτε υψηλής καθυστέρησης είτε χαμηλής ρυθμό-απόδοσης. Τρίτον, πρέπει να κανονιστεί ο κατάλληλος αριθμός ζευγαριών επικοινωνίας για να επικοινωνήσει σε ένα κανάλι επικοινωνίας. Εάν πάρα πολλά ζευγάρια προσπαθήσουν να έχουν πρόσβαση σε ένα κανάλι, το πρόβλημα σύγκρουσης οδηγεί σε περιττή κατανάλωση ισχύος. Αφ' ετέρου, εάν πολύ λίγα ζευγάρια επιτρέπεται να διαβιβάσουν πακέτα, η χρησιμοποίηση καναλιών είναι μικρή.

Έτσι, οι απαιτήσεις ενός αποτελεσματικού κατανεμημένου πρωτοκόλλου λειτουργίας συντονισμού (DCF) στα πολύ-διαυλικά cluster-based δίκτυα μπορούν να συνοψιστούν ως εξής:

- αποδοτική χρησιμοποίηση του εύρους ζώνης,
- καλή κατάσταση ανταγωνισμού καναλιών,
- ευφυής μηχανισμός διαχείρισης ισχύος για να μειωθεί ο ανταγωνισμός, και
- αποδοτικός μηχανισμός μετατροπής πυλών.

Παρακάτω προτείνεται ένα αποδοτικό MAC πρωτόκολλο διαχείρισης [12], το οποίο μπορεί να λειτουργήσει στα ακόλουθα cluster-based δίκτυα και έχει τα παρακάτω δύο πλεονεκτήματα:

1. Για την intra-cluster επικοινωνία, μπορούν να επιτευχθούν μία καλύτερη κατάσταση ανταγωνισμού και μία καλή χρησιμοποίηση καναλιών.
2. Για την inter-cluster επικοινωνία, μπορεί να μειωθεί ο χρόνος καθυστέρησης της κυκλοφορίας.

Κάνοντας μια επισκόπηση του πρωτόκολλου CMMP (*cluster-based multi-channel management protocol*) μπορούμε να πούμε ότι το CMMP περιλαμβάνει το ATIM (*announcement traffic indication message*), την ανάθεση καναλιών και τις τρεις φάσεις μετάδοσης δεδομένων.

Στην πολύ-διαυλική cluster-based δικτυακή αρχιτεκτονική, το πρωτόκολλο 802.11 DCF χρειάζεται μερικές τροποποιήσεις για να επιτύχει τους στόχους της απρόσκοπτης πρόσβασης καναλιών, της ενεργειακής αποδοτικότητας και της καλής χρησιμοποίησης καναλιών. Ο καθορισμός ενός αναγνωριστικού διαστήματος που χρησιμοποιείται από το CMMP είναι συμβατός με το 802.11 DCF με μια μικρή επέκταση. Ένα αναγνωριστικό διάστημα διαιρείται σε παράθυρα ATIM και δεδομένων όπως στο 802.11 DCF. Το παράθυρο δεδομένων χωρίζεται περαιτέρω στα υπό-παράθυρα ανάθεσης καναλιών και μετάδοσης δεδομένων. Με βάση τον καθορισμό ενός αναγνωριστικού διαστήματος, το πρωτόκολλο CMMP περιλαμβάνει τις ακόλουθες τρεις φάσεις:

- *Φάση ATIM*. Το χρονικό διάστημα αυτής της φάσης περιλαμβάνει το πακέτο αναγνωριστικών σημάτων και το παράθυρο ATIM. Σε αυτήν την φάση, ο επικεφαλής ομάδας παραδίδει αρχικά τις παραμέτρους συγχρονισμού ενός διαστήματος αναγνωριστικών σημάτων σε όλα τα μέλη της ομάδας μέσω ενός εκπεμπόμενου πακέτου αναγνωριστικών σημάτων. Εκείνες οι συσκευές που προτίθενται να μεταδώσουν δεδομένα διαβιβάζουν τα πακέτα ATIM στο παράθυρο ATIM για να ενημερώσουν το δέκτη να παραμείνει ενεργός και απαιτούν το απαραίτητο εύρος ζώνης από τον επικεφαλής ομάδας. Ο δέκτης απαντά έπειτα με ένα πακέτο ATIM ack στον αποστολέα για να επιβεβαιώσει αμέσως την επικοινωνία. Ο επικεφαλής ομάδας 'κρυφακούει' το απαιτούμενο εύρος ζώνης που συνδέεται με κάθε πακέτο ATIM και καταγράφει την απαίτηση εύρους ζώνης στον εσωτερικό πίνακά του. Σύμφωνα με τους ρόλους των μελών σε μια ομάδα, ο επικεφαλής ομάδας ορίζει επίσης διαφορετικά βάρη στις συσκευές για να δείξει την προτεραιότητα επικοινωνίας.
- *Φάση ανάθεσης καναλιών*. Ο στόχος αυτής της φάσης περιλαμβάνει τρεις πτυχές. Κατ' αρχάς, ο επικεφαλής ομάδας επιλέγει τα ζευγάρια συσκευών με την αποδοχή επικοινωνίας. Δεύτερον, ο επικεφαλής ομάδας ορίζει τα ζευγάρια συσκευών στα κατάλληλα κανάλια σύμφωνα με τις απαιτήσεις εύρους ζώνης και τους στόχους επικοινωνίας. Τρίτον, οι επικεφαλής ομάδας θέτουν σε κατάσταση εξοικονόμησης ενέργειας όσες συσκευές είναι άεργες ή ανάρμοστες. Όλες οι πληροφορίες διαχείρισης κωδικοποιούνται σε ένα πακέτο και μεταδίδονται σε

όλα τα μέλη ομάδων. Όταν όλες οι συσκευές λάβουν αυτό το πακέτο, αρχίζει η φάση μετάδοσης δεδομένων.

- *Φάση μετάδοσης δεδομένων*. Σε αυτήν την φάση, εκείνες οι συσκευές που έχουν αποδοχή επικοινωνίας μεταβαίνουν στο ορισμένο κανάλι και διαβιβάζουν τα δεδομένα. Εκείνες οι συσκευές που δεν επιτρέπεται να επικοινωνήσουν θα μεταβούν στην κατάσταση εξοικονόμησης ενέργειας, ακόμα κι αν έχουν ανταλλάξει ήδη πακέτα ATIM και ATIM ack επιτυχώς στη φάση ATIM. Αυτή η κατάσταση μπορεί να συμβεί όταν ο επικεφαλής ομάδας ανιχνεύσει ότι ο αριθμός ζευγαριών συσκευών που απαιτούν επικοινωνία σε αυτήν την ομάδα είναι πάρα πολύ μεγάλος. Ο περιορισμός του αριθμού ζευγαριών επικοινωνίας δεν θα μειώσει μόνο την κατανάλωση ισχύος των συσκευών, αλλά και θα καθιερώσει καλύτερους όρους ανταγωνισμού για να μειωθεί η σύγκρουση μηνυμάτων.

Στο CMMP, η καλή χρησιμοποίηση καναλιών μπορεί να επιτευχθεί μέσω της κατάλληλης ανάθεσης καναλιών. Με βάση την απαίτηση εύρους ζώνης που συνδέεται με κάθε ζευγάρι συσκευών, ο επικεφαλής ομάδας μπορεί να ορίσει τα ζευγάρια συσκευών στα κανάλια επικοινωνίας με έναν τρόπο ισορροπημένου φορτίου. Όλες οι συσκευές μπορούν έτσι είτε να μεταπηδήσουν σε ένα κατάλληλο κανάλι είτε να γυρίσουν στην κατάσταση εξοικονόμησης ενέργειας, έτσι ώστε η απόδοση συστημάτων να μπορεί να βελτιωθεί.

2.5 Βελτίωση στην QoS στα ασύρματα ad hoc δίκτυα

Δεδομένου ότι πολλές εφαρμογές έχουν απαιτήσεις (QoS) όπως η καθυστέρηση και η ρυθμό-απόδοση, είναι επιτακτικό το ασύρματο μέρος της επικοινωνίας να μπορεί να είναι σε θέση να υποστηρίξει ποιότητα υπηρεσίας παρόμοια με αυτή των συνδεμένων με καλώδιο δικτύων [13]. Για να επιτύχει τέτοιους στόχους, το πρωτόκολλο ελέγχου πρόσβασης μέσου (MAC) πρέπει να παρέχει έναν αποδοτικό μηχανισμό για να μοιράσει το περιορισμένο φάσμα μεταξύ όλων των κινητών κόμβων, μαζί με την απλότητα της λειτουργίας, την υψηλή ρυθμό-απόδοση συστήματος και την καλή διαφοροποίηση υπηρεσιών για ροές με διαφορετικές προτεραιότητες [4].

Το IEEE 802.11 [14] για τα ασύρματα δίκτυα τοπικής περιοχής (WLANs) είναι μια από τις ευρύτατα επεκταμένες ασύρματες τεχνικές. Επιτρέπει να εφαρμοστεί ένα ασύρματο δίκτυο με τη μια από τις δύο πιθανές διαμορφώσεις: τον τρόπο με υποδομή ή τον ad hoc τρόπο. Με τον ad hoc τρόπο, όλοι οι κόμβοι μπορούν να διαμορφώσουν ένα ειδικό δίκτυο αυθόρμητα, χωρίς οποιοδήποτε συγκεντρωμένο έλεγχο. Ακόμα κι αν ένας κόμβος χάσει τις άμεσες συνδέσεις με μερικούς κόμβους, είναι ακόμα δυνατό για τον κόμβο να επικοινωνήσει με άλλους μέσω των συνδέσεων πολλαπλών αλμάτων.

Το πρότυπο IEEE 802.11 περιλαμβάνει ένα σύνολο πρωτοκόλλων που είναι αρμόδια για τον έλεγχο πρόσβασης μέσου. Ο βασικός μηχανισμός πρόσβασης για τα ad hoc δίκτυα είναι η κατανεμημένη λειτουργία συντονισμού (DCF), η οποία χρησιμοποιεί την πολλαπλή πρόσβαση με την αποφυγή σύγκρουσης (CSMA/CA). Εντούτοις, στο DCF η καθυστέρηση πακέτων αυξάνεται εκθετικά δεδομένου ότι αυξάνει το ποσό κυκλοφορίας που ανταγωνίζεται το κανάλι, και έτσι το DCF δεν

υποστηρίζει ικανοποιητικά τις σε πραγματικό χρόνο εφαρμογές, όπως το home networking, το video on demand και η voice over IP. Για να αντιμετωπίσουν αυτό το ζήτημα, πολλά πρωτόκολλα πρόσβασης μέσου έχουν προταθεί για να ενισχύσουν τις παροχές QoS κάτω από DCF.

Το βελτιωμένο DCF (EDCF) πρωτόκολλο, που είναι μια επέκταση του DCF και είναι εντελώς κατανεμημένο, προσθέτει πολλά νέα και απαραίτητα χαρακτηριστικά γνωρίσματα στα τρέχοντα IEEE 802.11 πρότυπα. Το EDCF παρέχει μια εύκαμπτη και διανεμημένη λύση στη διαφοροποίηση υπηρεσιών με την εισαγωγή της έννοιας των πλέον σημαντικών κατηγοριών κυκλοφορίας. Με την ανάθεση διαφορετικών προτεραιοτήτων στα διαφορετικά διαστήματα εντός πλαισίου και στα μεγέθη παραθύρων ανταγωνισμού, η ροή υψηλής προτεραιότητας αποκτά γρηγορότερη πρόσβαση στο μέσο από τη ροή χαμηλής προτεραιότητας. Παρόμοιο με το DCF, το EDCF είναι ένα MAC πρωτόκολλο βασισμένο στον ανταγωνισμό.

Το τυποποιημένο πρωτόκολλο DCF απαιτεί ότι κάθε κόμβος πρέπει να ανιχνεύσει το μέσο πριν στείλει πακέτα. Το DCF υποστηρίζει επίσης έναν μηχανισμό αποφυγής σύγκρουσης για να μειώσει την πιθανότητα των συγκρούσεων που προκαλούνται από τους πολλαπλούς κόμβους οι οποίοι ανιχνεύουν ταυτόχρονα πως το κανάλι είναι ελεύθερο. Ειδικότερα, αφού ένας κόμβος μετάδοσης ανιχνεύσει ένα μη απασχολημένο κανάλι για ένα χρονικό διάστημα διανεμημένου interframe διαστήματος (DIFS), αυτό υπαναχωρεί για ένα χρονικό διάστημα που επιλέγεται ομοιόμορφα από το 0 έως το μέγεθος του παραθύρου ανταγωνισμού του (CW). Μόνο εάν το κανάλι παραμείνει μη απασχολημένο για τη περίοδο backoff, ο κόμβος επιτρέπεται να αρχίσει τη μετάδοση. Μετά από κάθε επιτυχή μετάδοση δεδομένων, το μέγεθος παραθύρων τίθεται στο *CW*, το οποίο δείχνει το ελάχιστο παράθυρο ανταγωνισμού.

Δεδομένου ότι το αρχικό 802.11 DCF δεν υποστηρίζει κάποιους μηχανισμούς προτεραιότητας και όλοι οι κόμβοι έχουν την ίδια προτεραιότητα πρόσβασης στο κοινό κανάλι με έναν τρόπο ανταγωνισμού, οι απαιτήσεις QoS (π.χ. ρυθμό-απόδοση και καθυστέρηση) των σε πραγματικό χρόνο εφαρμογών δεν μπορούν να ικανοποιηθούν όταν ο αριθμός ανταγωνιστικών κόμβων είναι μεγάλος.

Το EDCF είναι ένα βασισμένο σε ανταγωνισμό πρωτόκολλο πρόσβασης καναλιών. Το προτεινόμενο σχέδιο παρέχει τη δυνατότητα σε μέχρι και οκτώ τύπους κατηγοριών κυκλοφορίας (TC). Εκχωρεί τα μικρότερα μεγέθη CW για τις κατηγορίες υψηλής προτεραιότητας και τα μεγαλύτερα μεγέθη στις κατηγορίες χαμηλής προτεραιότητας. Αντί για DIFS που χρησιμοποιείται στο DCF, ένα AIFS θα χρησιμοποιείται για κάθε TC. Το TC με το μικρότερο AIFS θα έχει την πιο υψηλή προτεραιότητα. Κάθε AIFS είναι ίσο με το χρόνο DIFS συν μερικές (ενδεχομένως μηδέν) χρονικές σχισμές. Μια μεγάλη διαφορά μεταξύ DCF και EDCF είναι ότι όταν ανιχνεύεται ότι το μέσο είναι μη απασχολημένο για μια περίοδο AIFS, στο EDCF ο μετρητής backoff μειώνεται κατά ένα στην αρχή της τελευταίας χρονικής σχισμής της περιόδου AIFS, ενώ στο DCF ο μετρητής backoff μειώνεται κατά ένα στην αρχή της πρώτης χρονικής σχισμής μετά από τη περίοδο DIFS [15].

Κάθε TC μέσα σε κάθε κόμβο συμπεριφέρεται σαν ένας εικονικός κόμβος και ανταγωνίζεται ανεξάρτητα για την πρόσβαση στο μέσο. Η διαδικασία backoff πραγματοποιείται επίσης χωριστά μετά από την ανίχνευση εάν το μέσο είναι μη απασχολημένο για ένα χρόνο ίσο με το AIFS του. Κατά συνέπεια κάθε *TCi* παραμετροποιείται χωριστά ως εξής: $AIFSi$,$CWi_{\min}$,CWi_{max} και PFi , όπου PFi είναι ο παράγοντας εμμονής του *TCi* . Οι συγκρούσεις μεταξύ των εικονικών κόμβων μέσα σε κάθε κόμβο επιλύονται με τη χορήγηση της πρόσβασης στη μετάδοση υψηλής προτεραιότητας. Με το EDCF, μετά από κάθε επιτυχή μετάδοση *TCi* , η αντιστοιχία

CWi θα τεθεί στο *CWi* min. Μόλις αποτύχει μια μετάδοση, το *CWi* θα υπολογιστεί ως εξής:

$$\boldsymbol{CW_i = \min\left\{CW_i, \max\{CW_i \times PF_i\}\right\}}$$

Για να μειωθεί η καθυστέρηση, η παραμόρφωση και να επιτευχθεί υψηλότερη χρησιμοποίηση μέσου, προτείνεται η εκρηκτικότητα πακέτου. Κατά συνέπεια, όταν ένας κόμβος παίρνει την πρόσβαση στο κανάλι, ο κόμβος επιτρέπεται να στείλει τόσα πλαίσια όσα επιθυμεί εφ' όσον ο συνολικός χρόνος πρόσβασης καναλιού δεν υπερβαίνει ένα ορισμένο όριο μετάδοσης και καμία σύγκρουση δεν εμφανίζεται. Αυτό επιτυγχάνεται μέσω ενός χαρακτηριστικού γνωρίσματος αποκαλούμενου ευκαιρία μετάδοσης (TXOP), η οποία ορίζεται ως ένα διάστημα του χρόνου όπου ένας κόμβος έχει το δικαίωμα να αρχίσει τις μεταδόσεις.

Λαμβάνοντας υπόψη την κατάσταση δικτύου και την κυκλοφορία για την υιοθέτηση παραθύρου ανταγωνισμού, κάνουμε ένα σχέδιο διπλής μέτρησης για να πάρουμε τις σχετικές online πληροφορίες.

Με τις μετρήσεις της κατάστασης δικτύου και της κυκλοφορίας, προτείνουμε ένα νέο πρωτόκολλο EDCF βασισμένο στη διπλή μέτρηση, αποκαλούμενο EDCF-DM. Η βασική ιδέα του EDCF-DM είναι ότι με βάση τα αποτελέσματα μέτρησης προσαρμόζεται ανάλογα και η έκταση της αλλαγής του CWi. Όταν ο φόρτος εργασίας του συστήματος είναι υψηλός, το *CWi* αλλάζει αργά για να αποφύγει τις περαιτέρω συγκρούσεις. Για TCi, εάν άλλα υψηλής προτεραιότητας TCs έχουν χαμηλή πυκνότητα κυκλοφορίας, το CWi μπορεί να μειωθεί ταχύτερα για να μειώσει τον αριθμό των σπαταλημένων μη απασχολούμενων σχισμών. Η ταχύτητα ελέγχεται από τον παράγοντα ελέγχου του *TCi*, που συμβολίζεται με *σi*, στο οποίο εκχωρούνται δυναμικά διαφορετικές τιμές σύμφωνα με τα αποτελέσματα μέτρησης. Ειδικότερα, όταν δεν υπάρχει καμία σύγκρουση κατά τη διάρκεια του τελευταίου παραθύρου μέτρησης και κανένα υψηλότερο TC δεν έχει πακέτα για μετάδοση ή λήψη, το σi υπολογίζεται ως

$$\boldsymbol{\sigma_i = \min\{(1 + (i \times 2)) \times a_{avg}, \sigma_{min}\}}$$

όπου το σ_i είναι η διευκρινισμένη παράμετρος συστήματος.

Διαφορετικά, το σi υπολογίζεται ως:

$$\boldsymbol{\sigma_i = \min\{(1 + (i \times 2)) \times a_{avg}, \sigma_{max}\}}$$

όπου το σ_{max} είναι η διευκρινισμένη παράμετρος συστήματος.

Μετά από μια επιτυχή μετάδοση, σύμφωνα με το σ_i, το *CWi* αλλάζει ως εξής:

$$\boldsymbol{CW_i = \max\left\{CW_i, \min\{CW_i \times \sigma_i\}\right\}}$$

Όταν μια μετάδοση αποτυγχάνει λόγω σύγκρουσης, το *CWi* υπολογίζεται σύμφωνα με τη σχέση:

$$\boldsymbol{CW_i = \min\left\{CW_i, \max\{CW_i \times PF_i\}\right\}}$$

ΚΕΦΑΛΑΙΟ 3^{Ο}

ΔΙΚΤΥΑ ΑΙΣΘΗΤΗΡΩΝ

3.1 Δίκτυα αισθητήρων

Μέσα από την ανάπτυξη των ασύρματων επικοινωνιών και των ηλεκτρονικών, έχει γίνει εύκολη η δημιουργία δικτύων αισθητήρων χαμηλού κόστους, χαμηλής κατανάλωσης ισχύος, με πολλαπλές λειτουργίες. Τα δίκτυα αισθητήρων αποτελούνται από κόμβους αισθητήρων οι οποίοι είναι ικανοί να αισθάνονται, να επεξεργάζονται δεδομένα και να επικοινωνούν μεταξύ τους συνήθως σ' ένα RF κανάλι. Ένα δίκτυο αισθητήρων έχει σχεδιαστεί για: (α) να ανιχνεύει γεγονότα ή φαινόμενα, (β) να συλλέγει και να προωθεί πληροφορίες και (γ) να μεταδίδει ανιχνευμένες πληροφορίες σε άλλους ενδιαφερόμενους. Συνήθως, τα βασικά χαρακτηριστικά των δικτύων αισθητήρων είναι τα παρακάτω [16]:

- Ικανότητες αυτό-οργάνωσης.
- Επικοινωνία με εκπομπή μικρής εμβέλειας και δρομολόγηση με πολλαπλούς κόμβους (multi-hop communication).
- Πυκνή ανάπτυξη και συνεργατική προσπάθεια των κόμβων αισθητήρων.
- Συχνή αλλαγή τοπολογίας λόγω της εξαφάνισης κόμβων.
- Περιορισμοί στην ενέργεια, στη μεταδιδόμενη ισχύ, στη μνήμη και στην υπολογιστική ισχύ.

Αυτά τα χαρακτηριστικά και κυρίως τα τρία τελευταία, διαφοροποιούν τα δίκτυα αισθητήρων από άλλα ασύρματα ad hoc δίκτυα.

Όπως αναφέραμε, ένα χαρακτηριστικό των δικτύων αισθητήρων είναι η πυκνή ανάπτυξη των κόμβων μέσα σε μια προκαθορισμένη περιοχή γεγονότων. Η πυκνή ανάπτυξη μαζί με τη δρομολόγηση πολλαπλών κόμβων, αποτελούν ένα πλεονέκτημα εν συγκρίσει με την παραδοσιακή επικοινωνία, καθόσον οι γειτονικοί κόμβοι βρίσκονται πολύ κοντά ο ένας στον άλλο. Αυτή η διάταξη απαιτεί λιγότερη ενέργεια για την επικοινωνία και μπορεί να αντιμετωπίσει αποτελεσματικά κάποια προβλήματα διάδοσης του σήματος σε μακρινές αποστάσεις.

Στα δίκτυα αισθητήρων η κατανάλωση ενέργειας οφείλεται κυρίως σε τρεις αιτίες: μετάδοση δεδομένων, επεξεργασία σήματος και λειτουργία λογισμικού [17]. Είναι λοιπόν επιθυμητό να δημιουργηθούν τεχνικές αποδοτικές σε κατανάλωση ενέργειας που ελαχιστοποιούν την ανάγκη για ισχύ και ταυτόχρονα ελαχιστοποιούν την αποστολή μηνυμάτων για τον έλεγχο και τη συνεργασία του δικτύου.

Ένα ασύρματο δίκτυο αισθητήρων (Wireless Sensor Network, WSN) είναι ένα δίκτυο αισθητήρων που αποτελείται από μεγάλο αριθμό κόμβων με ικανότητες ανίχνευσης, οι οποίοι επικοινωνούν ασύρματα μεταξύ τους. Μετά την ανάπτυξη του δικτύου, οι κόμβοι ξεκινούν μία διαδικασία δημιουργίας ομάδων (clusters), εγκατάστασης καναλιών επικοινωνίας, δημιουργίας ιεραρχίας κ.ά. Με την ολοκλήρωση των εργασιών αυτών, αναμένεται το δίκτυο να λειτουργήσει για μεγάλο

χρονικό διάστημα χωρίς ανθρώπινη παρέμβαση και επίβλεψη ή ανάγκη αντικατάστασης κόμβων λόγω ελάττωσης της ενέργειας [3].

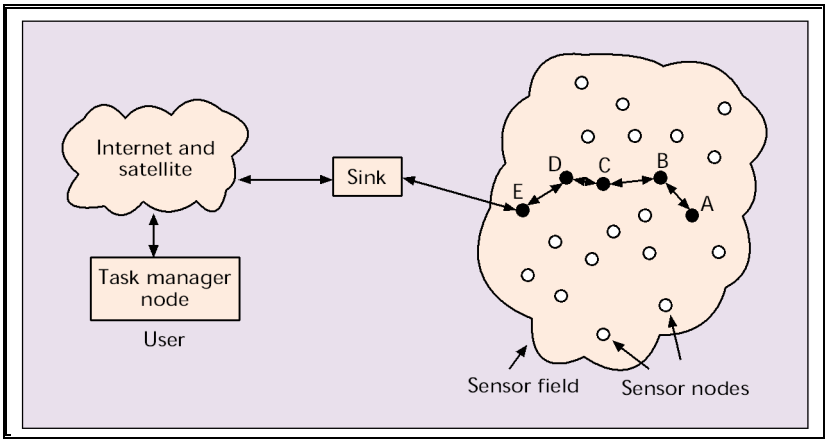
3.1.1 Χαρακτηριστικά δικτύων αισθητήρων

Όπως έχουμε αναφέρει, ένα δίκτυο αισθητήρων αποτελεί μια ιδιαίτερη κατηγορία δικτύων ad hoc. Οι κόμβοι που αποτελούν το δίκτυο είναι πολύ μικρές συσκευές μικρού κόστους, οι οποίες συνεργάζονται μεταξύ τους χωρίς εξωτερική καθοδήγηση για την επίτευξη ενός κοινού σκοπού. Τα κυριότερα χαρακτηριστικά ενός δικτύου αισθητήρων αναφέρονται παρακάτω:

- *Περιορισμοί:* Οι συσκευές (κόμβοι) είναι φθηνού κόστους και έτσι περιορίζονται από υπολογιστική ικανότητα (4 ή 8 bit CPU).
- *Ασύρματες Συνδέσεις*: Για λόγους αλληλεπίδρασης, οι κόμβοι εφοδιάζονται με ικανότητες ασύρματης μετάδοσης.
- *Μέγεθος Πακέτου*: Το μέγεθος πακέτου είναι περιορισμένο (της τάξης των 100 Byte ή λιγότερο)
- *Ενέργεια Μπαταρίας*: Οι συσκευές λειτουργούν με μπαταρία ή με ηλιακή ενέργεια ή άλλο αυτόνομο μέσο. Όταν η μπαταρία εξαντληθεί, οι κόμβοι μπορούν να αντικατασταθούν αφού η μπαταρία είναι το σημαντικότερο κομμάτι της συσκευής.
- *Κινητικότητα:* Ενώ η τοποθεσία του δικτύου είναι σταθερή, η τοπολογία του συνεχώς μεταβάλλεται λόγω της αντικατάστασης αισθητήρων ή την επέκταση του δικτύου.
- *Μη Σταθερή Υποδομή*: Όταν το δίκτυο αναπτυχθεί δεν υπάρχει εξωτερική καθοδήγηση. Οι αισθητήρες συνεργάζονται για να πετύχουν το σκοπό τους.
- *Τοπολογία Δικτύου*: Το δίκτυο αισθητήρων μπορεί να επικοινωνεί με multi-hop τρόπο με οποιοδήποτε κόμβο του δικτύου ή μπορεί να επικοινωνεί άμεσα με τον γειτονικό κόμβο με single-hop. Ο πρώτος τρόπος ονομάζεται global approach ενώ ο δεύτερος local neighborhood approach.
- *Ομοιογένεια:* Συνήθως όλοι οι αισθητήρες είναι ίσοι (δεν υπάρχει ιεραρχία και δεν απαιτείται εξωτερική επίβλεψη). Όμως, οι αισθητήρες μπορούν να διαιρεθούν σε ομάδες. Επιπλέον, συνήθως υπάρχει ένας σταθμός βάσης που συλλέγει και αξιολογεί τα συγκεντρωμένα στοιχεία. Ο σταθμός βάσης είναι πιο ισχυρός και περισσότερο ασφαλής από τα άλλα τμήματα του δικτύου. Οι υπόλοιποι κόμβοι δημιουργούν κανάλια επικοινωνίας με τον σταθμό βάσης.
- *Ασφάλεια:* Η ασφάλεια πρέπει να λαμβάνεται υπόψη πριν την ανάπτυξη του δικτύου. Η αρχιτεκτονική της ασφάλειας απαιτεί ελαφρούς κρυπτογραφικούς αλγόριθμους των οποίων ο χρόνος εφαρμογής δεν πρέπει να διαταράσσει τον βασικό σκοπό των αισθητήρων. Εφόσον η ενέργεια είναι περιορισμένη, τα μεταδιδόμενα μηνύματα για την ασφάλιση του δικτύου δεν πρέπει να είναι μεγάλα σε μέγεθος.

3.1.2 Παράγοντες σχεδίασης δικτύων αισθητήρων

Οι κόμβοι ενός δικτύου αισθητήρων είναι συνήθως διασκορπισμένοι σ' έναν πεδίο ανίχνευσης (sensor field), όπως φαίνεται στο Σχήμα 3. Κάθε ένας από αυτούς τους κόμβους έχει τη δυνατότητα να συλλέγει δεδομένα και να τα προωθεί σε μία δεξαμενή (sink). Τα δεδομένα, όπως φαίνεται στο σχήμα, προωθούνται στη δεξαμενή (sink) μέσω μιας αρχιτεκτονικής χωρίς υποδομή. Η δεξαμενή επικοινωνεί με τον κόμβο διαχείρισης (task management node) μέσω του διαδικτύου ή μέσω δορυφόρου.



Σχήμα 3. Δίκτυο αισθητήρων

Οι κυριότεροι παράγοντες σχεδίασης ενός δικτύου αισθητήρων αναφέρονται παρακάτω. Οι παράγοντες αυτοί είναι σημαντικοί διότι χρησιμοποιούνται σαν κατευθυντήριες οδηγίες για την δημιουργία ενός πρωτοκόλλου ή ενός αλγόριθμου για τα δίκτυα αισθητήρων. Επιπλέον, αυτοί οι παράγοντες μπορούν να χρησιμοποιηθούν για σύγκριση διαφορετικών σχημάτων.

α. Αντοχή σε σφάλματα

Ορισμένοι αισθητήριοι κόμβοι είναι δυνατόν κατά την διάρκεια της εργασίας τους να αποτύχουν ή να μπλοκαριστούν λόγω έλλειψης ενέργειας ή λόγω φυσικής καταστροφής ή εξαιτίας περιβαλλοντικών παρεμβολών. Η αποτυχία των κόμβων δεν πρέπει να επηρεάσει την όλη εργασία του δικτύου αισθητήρων. Η αντοχή σε σφάλματα είναι η ικανότητα που έχει το δίκτυο να διατηρεί τη λειτουργικότητά του χωρίς διακοπή λόγω αποτυχίας ορισμένων από τους κόμβους που το απαρτίζουν [18]. Η αξιοπιστία ή αντοχή σε σφάλματα συμβολίζεται με $R_k(t)$ και μοντελοποιείται στο [19], χρησιμοποιώντας διασπορά Poisson για να υπολογιστεί η πιθανότητα να μην υπάρξει αποτυχία σ' ένα μικρό χρονικό διάστημα (0,t). Η πιθανότητα αυτή δίνεται από τον τύπο:

$$\boldsymbol{R_k(t) = e_k^{-\lambda_t}}$$

όπου λ είναι ο ρυθμός αποτυχίας ενός τυχαίου κόμβου k και t είναι η χρονική περίοδος.

β. Κλιμάκωση

Όπως έχουμε αναφέρει, ένα δίκτυο αισθητήρων αποτελείται από μεγάλο αριθμό κόμβων αισθητήρων. Ανάλογα με την εφαρμογή, ο αριθμός αυτός μπορεί να αυξάνεται. Οι αλγόριθμοι και τα πρωτόκολλα που σχεδιάζονται πρέπει να μπορούν να χειρίζονται αυτόν το μεγάλο αριθμό. Πρέπει επίσης να εκμεταλλευτούν τη μεγάλη πυκνότητα των δικτύων. Η πυκνότητα κυμαίνεται από λίγους κόμβους έως μερικές εκατοντάδες κόμβους σε μία περιοχή η οποία δεν ξεπερνάει τα 10 μ. σε διάμετρο. Η πυκνότητα μ υπολογίζεται ως εξής [20]:

$$\mu(R) = \frac{(N \times \pi \times R^2)}{A}$$

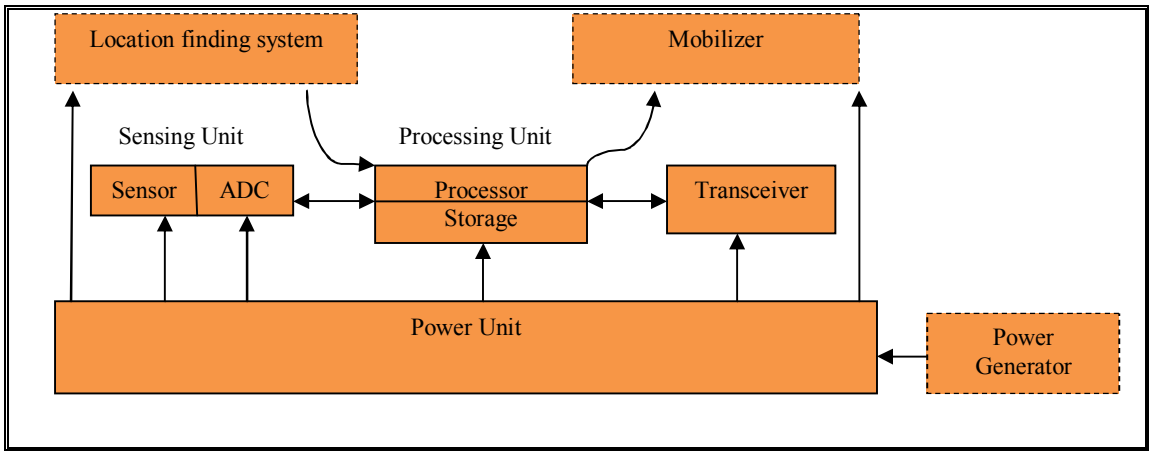
όπου N είναι ο αριθμός των κόμβων σε μία περιοχή εμβαδού A και R η εμβέλεια της ασύρματης μετάδοσης. Ο παραπάνω τύπος δίνει τον αριθμό των κόμβων μέσα στην εμβέλεια της ασύρματης μετάδοσης του κάθε κόμβου που ανήκει στην περιοχή Α.

γ. Κόστος παραγωγής

Εφόσον το δίκτυο αισθητήρων αποτελείται από μεγάλο αριθμό κόμβων, το κόστος κάθε κόμβου πρέπει να είναι σημαντικά μικρό ώστε να δικαιολογείται το συνολικό κόστος του δικτύου. Εάν το κόστος του δικτύου είναι μεγαλύτερο από ένα συνηθισμένο δίκτυο, τότε δεν είναι αναγκαία η ανάπτυξή του. Έτσι πρέπει να διατηρηθεί το κόστος κάθε κόμβου χαμηλό.

δ. Περιορισμοί του υλικού

Ένας συνηθισμένος κόμβος αποτελείται από τέσσερα βασικά στοιχεία, όπως φαίνεται στο Σχήμα 4:



Σχήμα 4. Αισθητήριος Κόμβος

Τα στοιχεία αυτά είναι: *Αισθητήρια μονάδα (Sensing Unit), επεξεργαστής (Processing Unit), πομποδέκτης (Transceiver Unit)* και μία *μονάδα ισχύος (Power Unit)*. Πιθανό να έχουν επιπλέον κομμάτια όπως: *Μονάδα εντοπισμού θέσης (location finding system), γεννήτρια (power generator), αποθηκευτική μονάδα (storage)* και *μονάδα κίνησης (mobiliser)*. Οι αισθητήριες μονάδες αποτελούνται από δύο υπό-στοιχεία: αισθητήρα (sensor) και αναλογικούς-ψηφιακούς μετατροπείς (ADCs). Τα αναλογικά σήματα που παράγονται από τους αισθητήρες μετατρέπονται σε ψηφιακά μέσω του ADC και στην συνέχεια προωθούνται στη μονάδα επεξεργασίας. Η μονάδα επεξεργασίας που συνδέεται με μια αποθηκευτική μονάδα, διαχειρίζεται τις διαδικασίες που επιτρέπουν στον αισθητήρα να συνεργάζεται με άλλους κόμβους. Ο πομποδέκτης συνδέει των αισθητήρα με το δίκτυο. Ίσως το πιο σημαντικό κομμάτι του αισθητήρα είναι η μονάδα ισχύος. Η μονάδα ισχύος τροφοδοτείται από μονάδες συλλογής ενέργειας, όπως είναι ηλιακές κυψέλες κ.ά. Υπάρχουν και άλλες υπό-μονάδες στους αισθητήρες που μπορούν να χρησιμοποιηθούν, ανάλογα με την εφαρμογή. Οι περισσότερες από τις τεχνικές δρομολόγησης και πολλά θέματα ανίχνευσης απαιτούν γνώση της περιοχής ανάπτυξης του δικτύου αισθητήρων με μεγάλη ακρίβεια. Γι' αυτό πρέπει ο αισθητήρας να έχει μια μονάδα εντοπισμού θέσης. Η μονάδα κίνησης χρησιμοποιείται γιατί μπορεί να χρειαστεί η μετακίνηση του αισθητήρα για να φέρει σε πέρας την αποστολή του.

Τα παραπάνω κομμάτια πρέπει να μπορούν να χωρέσουν σε πολύ μικρό χώρο ακόμα και λίγων κυβικών εκατοστών [21]. Εκτός του μεγέθους, υπάρχουν και άλλα αυστηρά κριτήρια για τους αισθητήρες. Αυτά είναι [22]:

- Ελάχιστη κατανάλωση ενέργειας.
- Λειτουργία σε μεγάλη ογκομετρική πυκνότητα.
- Μικρό κόστος παραγωγής.
- Να είναι αναλώσιμοι και αυτόνομοι.
- Λειτουργία χωρίς επιτήρηση.
- Προσαρμοστικότητα στο περιβάλλον.

ε. Τοπολογία δικτύων αισθητήρων

Το δίκτυο αισθητήρων αποτελείται από εκατοντάδες έως μερικές χιλιάδες κόμβους που αναπτύσσονται στην περιοχή ενδιαφέροντος. Βάσει της πυκνότητας του δικτύου, τα δίκτυα αισθητήρων μπορούν να ταξινομηθούν σε δύο μεγάλες κατηγορίες:

- Στα πυκνά δίκτυα, όπου ανάλογα με την περιοχή κάλυψης του δικτύου υπάρχει πυκνή κατανομή κόμβων στην περιοχή. Η μέγιστη πυκνότητα μπορεί να φτάσει μέχρι και τους 20 κόμβους/m^3. Η ανάπτυξη ενός τόσο πυκνού δικτύου απαιτεί προσεκτικό χειρισμό της διατήρησης της τοπολογίας και
- Στα αραιά δίκτυα, όπου αντίθετα με τα πυκνά δίκτυα έχουμε αραιή κατανομή κόμβων. Φυσικά η αραιή κατανομή δεν σημαίνει έλλειψη πλήρους κάλυψης της περιοχής που θα ελέγξουμε. Οι κόμβοι σε αυτήν την κατηγορία θα έχουν κατάλληλη εμβέλεια αίσθησης ώστε να καλύπτουν την περιοχή ελέγχου.

Μια περαιτέρω ταξινόμηση των δικτύων μπορεί να γίνει ανάλογα με την κινητικότητά τους. Η ύπαρξη κινητικότητας οφείλεται καθαυτού στην εκτέλεση της αποστολής του δικτύου. Έτσι μπορούμε να διακρίνουμε σταθερά δίκτυα, στα οποία έχουμε έλλειψη κινητικότητας και κινητά δίκτυα, όπου οι κόμβοι είναι εφοδιασμένοι με μια συσκευή κίνησης. Ένας κινητός κόμβος θα μπορέσει να καταλάβει μια καλύτερη θέση προς το στόχο και να έχει καλύτερα αποτελέσματα αίσθησης από έναν ακίνητο κόμβο.

Εξετάζουμε τη διατήρηση της τοπολογίας σε τρεις φάσεις:

- *Φάση πριν την ανάπτυξη και κατά την ανάπτυξη*: Οι αισθητήρες μπορούν να αναπτυχθούν είτε μαζικά είτε τοποθετώντας έναν προς έναν τους κόμβους στο πεδίο ανίχνευσης. Μπορούν να αναπτυχθούν είτε με ρίψη από αεροπλάνο είτε με βολή πυροβολικού, πυραύλου ή ρουκέτας και να τοποθετηθούν ένας προς έναν από άνθρωπο ή από ρομπότ.
- *Φάση μετά την ανάπτυξη*: Μετά την ανάπτυξη του δικτύου, η τοπολογία αλλάζει λόγω των αλλαγών της θέσης ενός κόμβου, της μη επικοινωνίας (λόγω θορύβου, κινούμενων εμποδίων κ.ά.), της διαθέσιμης ενέργειας, της κακής λειτουργίας και άλλων θεμάτων.
- *Φάση ανάπτυξης επιπλέον κόμβων:* Επιπλέον κόμβοι μπορούν να προστεθούν στο υπάρχον δίκτυο λόγω κακής λειτουργίας των υπαρχόντων κόμβων ή λόγω αλλαγής στο σκοπό της εγκατάστασης του δικτύου.

στ. Περιβάλλον

Οι αισθητήρες αναπτύσσονται πυκνά, είτε πολύ κοντά στην περιοχή ανίχνευσης είτε μέσα στην περιοχή. Γι' αυτό συνήθως δουλεύουν χωρίς επιτήρηση σε απόμακρες γεωγραφικές περιοχές. Μπορούν να λειτουργούν στο εσωτερικό μιας μεγάλης μηχανής, στο βάθος ενός ωκεανού, σε μια μολυσμένη με βιολογικά ή χημικά περιοχή, σε ένα πεδίο μάχης πίσω από τις γραμμές του εχθρού και σε άλλα μέρη.

ζ. Μέσα Μετάδοσης

Σ' ένα δίκτυο αισθητήρων, οι κόμβοι επικοινωνούν ασύρματα μεταξύ τους. Αυτές οι συνδέσεις μπορούν να δημιουργηθούν με ραδιοσυχνότητες, υπέρυθρες ή οπτικά μέσα. Για να καταστήσουμε δυνατή παγκόσμια λειτουργία των δικτύων, το επιλεχθέν μέσο μετάδοσης πρέπει να είναι διαθέσιμο παντού στον κόσμο.

Οι περισσότερες διαθέσιμες εφαρμογές για αισθητήρες βασίζονται σε επικοινωνία με ραδιοσυχνότητες. Ο βασικός λόγος χρησιμοποίησης ραδιοσυχνοτήτων είναι ότι δεν χρειάζεται οπτική επαφή και επιτρέπει μη κατευθυντικές συνδέσεις [23]. Σε ορισμένες εφαρμογές, όπως η παρακολούθηση κέρδους ή ο έλεγχος αλυσίδας εφοδιασμού στις οποίες οι κόμβοι μπορεί να είναι εσώκλειστοι σε μεγάλα μηχανήματα, αυτά τα προνόμια είναι αναγκαία. Παρόλα αυτά, οι ραδιοσυχνότητες έχουν και περιορισμούς που αποτελούν μειονεκτήματα για τις μικρές συσκευές, όπως οι αισθητήρες:

- Οι αποτελεσματικές κεραίες πρέπει να έχουν μεγάλο μήκος κύματος και συνεπώς σημαντικό φυσικό μήκος για να έχουμε αποτελεσματική μετάδοση.
- Μικρότερες κεραίες έχουν μικρότερο κέρδος κεραίας γιατί η απόκλιση της δέσμης περιορίζεται από τη διάθλαση, που εξαρτάται από το μήκος κύματος. Για να πετύχουμε διόρθωση στην ευθυγράμμιση πρέπει να έχουμε μεγάλη σε μέγεθος παραβολική κεραία.
- Οι πομποδέκτες ραδιοσυχνοτήτων έχουν μικρή αποτελεσματικότητα.
- Η λαμβανόμενη ισχύς κυμαίνεται, όσο η απόσταση μειώνεται, από τη δεύτερη στην έβδομη δύναμη λόγω της πολύ-διαδρομικής λήψης.

Ένας άλλος τρόπος επικοινωνίας μεταξύ των αισθητήρων είναι με υπέρυθρες. Η επικοινωνία με υπέρυθρες είναι ελεύθερη χωρίς άδεια χρήσης και είναι ανθεκτική σε

παρεμβολές από άλλες ηλεκτρικές συσκευές. Οι πομποδέκτες που χρησιμοποιούν υπέρυθρες είναι φθηνότεροι και πιο εύκολοι στην κατασκευή. Το μειονέκτημα των υπερύθρων είναι η απαίτηση για οπτική επαφή των επικοινωνούντων συσκευών. Αυτό περιορίζει την επιλογή τους στην περίπτωση των δικτύων ασυρμάτων αισθητήρων (WSN).

Τέλος, μία άλλη μορφή επικοινωνίας είναι με οπτικά μέσα. Η επικοινωνία με οπτικά μέσα έχει πολλά πλεονεκτήματα για τους μικροσκοπικούς αισθητήρες [23]:

- Οι οπτικές κεραίες εκπομπής (καθρέπτες, δίοδοι λέιζερ) είναι πολύ μικρές σε μέγεθος.
- Η μετάδοση με οπτικά μέσα εξασφαλίζει μεγάλο κέρδος κεραίας, που έχει ως επακόλουθο μεγάλη αποδοτικότητα στη μετάδοση.
- Η λαμβανόμενη ισχύς εξασθενεί μόνο κατά τη δεύτερη δύναμη της απόστασης, αν υποθέσουμε οπτική ευθεία.
- Η μεγάλη κατευθυντικότητα της οπτικής επικοινωνίας επιτρέπει τη χρησιμοποίηση τεχνικής SDMA ή οποία είναι πιο αποτελεσματική από τις τεχνικές μετάδοσης των ραδιοσυχνοτήτων (FDMA, TDMA, CDMA).
- Είναι πολύ δύσκολο να 'κρυφακούσει' κανείς σε μία ευθυγραμμισμένη οπτική επικοινωνία (μικρή πιθανότητα ανίχνευσης και μικρή πιθανότητα αναχαίτισης), που είναι μεγάλο πλεονέκτημα ασφάλειας.

Τα κυριότερα μειονεκτήματα της οπτικής επικοινωνίας είναι η απαραίτητη οπτική επαφή για όλες τις συνδέσεις μεταξύ των αισθητήρων. Επίσης, οι μικρότερες αποστάσεις και η στενή δέσμη συνεπάγονται την ανάγκη για ακριβή σκόπευση.

Δύο κύριες μέθοδοι οπτικής επικοινωνίας που υπάρχουν είναι η παθητική και η ενεργητική. Στην πρώτη περίπτωση δεν είναι απαραίτητη η ύπαρξη κάποιας ενσωματωμένης πηγής φωτός. Αντίθετα, στη δεύτερη περίπτωση, χρησιμοποιείται μία ενσωματωμένη δίοδος λέιζερ και ένα ανάλογο σύστημα επικοινωνίας προκειμένου να σταλεί μια δέσμη φωτός προς το στοχευόμενο δέκτη.

Η επιλογή του μέσου μετάδοσης είναι ένα θέμα που εξετάζεται πριν την εγκατάσταση του δικτύου. Η εφαρμογή που θα χρησιμοποιεί το δίκτυο είναι αυτή που καθορίζει κατά κύριο λόγο το μέσο μετάδοσης.

η. Κατανάλωση Ενέργειας

Ο αισθητήρας, ως μικροηλεκτρονική συσκευή, μπορεί να έχει μια περιορισμένη πηγή ενέργειας (<0.5 Ah, 1,2 V). Σε ορισμένες εφαρμογές, η αναπλήρωση της ενέργειας μπορεί να είναι αδύνατη. Ο χρόνος ζωής ενός αισθητήρα εξαρτάται άμεσα από τη διάρκεια ζωής της μπαταρίας. Μια καλή μπαταρία πρέπει να έχει τα παρακάτω χαρακτηριστικά [23]:

- Μεγάλη πυκνότητα ενέργειας.
- Μεγάλη αναλογία ενεργού όγκου προς τον όγκο πακέτου.
- Μικρό δυναμικό κελιού (0.5-1.0 V) ώστε τα ψηφιακά κυκλώματα να εκμεταλλεύονται τη δευτέρου βαθμού ελάττωση στην κατανάλωση ενέργειας με την προσφερόμενη τάση.
- Ικανότητα να χωρίζεται σε σειρές κελιών ώστε να παρέχει διαφορετικό δυναμικό σε κάθε κομμάτι του αισθητήρα.

- Να είναι επαναφορτιζόμενη, σε περίπτωση που το σύστημα έχει δυνατότητα απόκτησης ενέργειας.

Σ' ένα δίκτυο αισθητήρων, κάθε κόμβος παίζει τον διπλό ρόλο του δημιουργού δεδομένων και του δρομολογητή δεδομένων. Η κακή λειτουργία μερικών κόμβων μπορεί να επιφέρει σημαντικές αλλαγές στην τοπολογία του δικτύου και μπορεί να οδηγήσει σε αναδρομολόγηση των πακέτων και αναδιοργάνωση του δικτύου. Γι' αυτό, η σωστή διαχείριση της ενέργειας παίζει μεγάλο ρόλο. Ο σημαντικότερος ρόλος των αισθητήρων είναι να ανιχνεύουν γεγονότα, να εκτελούν γρήγορη επεξεργασία δεδομένων και να μεταδίδουν τα δεδομένα, οπότε η κατανάλωση ενέργειας μπορεί να χωριστεί σε τρεις κατηγορίες: ανίχνευσης, επικοινωνίας και επεξεργασίας δεδομένων.

3.2 Σχεδίαση δικτύων αισθητήρων

Στο επόμενο κεφάλαιο παρουσιάζονται κάποια θέματα που αφορούν στη σχεδίαση των δικτύων αισθητήρων. Δίδονται οι κατασκευαστικές απαιτήσεις καθώς επίσης και οι δυσχέρειες σχεδιασμού. Στη συνέχεια παρουσιάζονται τα σημαντικότερα στοιχεία ενός κόμβου αισθητήρα και τέλος, αναπτύσσεται μια παράγραφος που αφορά στην αρχιτεκτονική των κόμβων.

3.2.1 Γενική άποψη - Απαιτήσεις και δυσχέρειες σχεδιασμού

Όπως είδαμε, τα δίκτυα αισθητήρων αποτελούνται από ένα μεγάλο αριθμό κόμβων-αισθητήρων, με συγκεκριμένες ικανότητες επικοινωνίας, υπολογισμών, αποθήκευσης, ανίχνευσης και κίνησης. Τα δίκτυα αισθητήρων σκοπεύουν να παράσχουν αποτελεσματική και ικανή σύνδεση μεταξύ φυσικού και υπολογιστικού κόσμου. Επιπλέον, έχουν υψηλή οικονομική επίδραση σε πολλά πεδία, όπως ο στρατός, η εκπαίδευση, το εμπόριο κ.ά. Ταυτόχρονα, τα δίκτυα αισθητήρων προσφέρουν νέα πεδία έρευνας και ανάπτυξης, όπως η ανάγκη για δημιουργία αισθητήρων μικρότερου κόστους με μικρή κατανάλωση ισχύος, πιο εύκαμπτων, με μεγαλύτερη ανθεκτικότητα σε λάθη και επιθέσεις. Παρόλα αυτά, πριν αναπτυχθούν οποιεσδήποτε απ' όλες αυτές τις καινοτομίες, το δίκτυο πρέπει να σχεδιαστεί και να εκτελεστεί σωστά. Έτσι, η αρχιτεκτονική τόσο σε υλικό όσο και σε πρόγραμμα, θα δώσει μια μεγαλύτερη αποτελεσματικότητα στο δίκτυο. Επίσης, η σχεδίαση των δικτύων θα έχει βασική επίδραση στο κόστος και στην απόδοσή τους.

Οι εφαρμογές των δικτύων αισθητήρων καθορίζονται άμεσα από τα χαρακτηριστικά των υπολογιστικών και επικοινωνιακών ικανοτήτων ενός συστήματος. Η απόφαση για την αρχιτεκτονική και τη σχεδίαση ενός δικτύου καθορίζεται από έναν αριθμό χαρακτηριστικών. Τα χαρακτηριστικά αυτά είναι το χαμηλό κόστος, το μικρό μέγεθος, η μικρή κατανάλωση ενέργειας, η ευρωστία του δικτύου, η αντοχή σε σφάλματα και λάθη και η ασφάλεια με τη μυστικότητα.

Όπως αναφέραμε παραπάνω, οι αισθητήρες αποτελούνται από τέσσερα βασικά στοιχεία (μονάδα ισχύος, πομποδέκτης, επεξεργαστής, αισθητήρια μονάδα) και πολλά δευτερεύοντα. Εδώ πρέπει να εξεταστεί ένας αριθμός σχετικών τεχνολογιών. Για

παράδειγμα, πρέπει να ληφθεί υπόψη μια μεγάλη ποικιλία από πανίσχυρους, μικρής ισχύος και κόστους επεξεργαστές και μνήμες χαμηλού κόστους. Επίσης, οι τεχνολογίες της μνήμης και των επεξεργαστών αναπτύσσονται ραγδαία τα τελευταία χρόνια.

Λόγω των παραπάνω απαιτήσεων και των εμποδίων που παρουσιάζονται, δίδονται παρακάτω τα σημαντικότερα αρχιτεκτονικά και σχεδιαστικά αντικείμενα [23]:

α. Μικρό φυσικό μέγεθος

Ένα από τα σημαντικότερα σχεδιαστικά θέματα είναι η μείωση του φυσικού μεγέθους. Γι' αυτό, σκοπός είναι η παροχή ισχυρών επεξεργαστών, μεγάλης μνήμης πομποδέκτη και άλλων στοιχείων, ενώ κρατείται ένα λογικά μικρό μέγεθος που υπαγορεύεται από την εφαρμογή.

β. Μικρή κατανάλωση ισχύος

Η ικανότητα, ο χρόνος ζωής και η απόδοση των αισθητήρων περιορίζονται από την ενέργεια. Οι αισθητήρες πρέπει να είναι ενεργοί για ένα μεγάλο χρονικό διάστημα χωρίς να επαναφορτίζουν την μπαταρία τους διότι η συντήρησή τους είναι πανάκριβη.

γ. Συνεργασία-Εντατική λειτουργία

Με σκοπό την επίτευξη της συνολικής προσπάθειας, τα δεδομένα πρέπει να συλλέγονται από τον αισθητήρα, να επεξεργάζονται, να συμπιέζονται και στη συνέχεια να στέλνονται στο δίκτυο ταυτόχρονα σε ένα άμεσο κανάλι πληροφόρησης, αντίθετα από τον σειριακό τρόπο. Οι δύο επακόλουθες προσεγγίσεις σχετίζονται με αυτήν την απαίτηση:

1. Διαμέλιση του επεξεργαστή σε πολλαπλά κομμάτια, κάθε ένα από τα οποία έχει την ευθύνη για έναν συγκεκριμένο σκοπό και
2. Ελάττωση του χρόνου αλλαγής των διεργασιών.

δ. Ποικιλία στο σχεδιασμό και στη χρήση

Αφού ο κάθε κόμβος πρέπει να είναι μικρός στο μέγεθος, να έχει μικρή κατανάλωση ισχύος και να έχει μικρές φυσικές ομοιότητες με κάποιον άλλο, οι κόμβοι τείνουν να είναι ειδικής εφαρμογής. Παρόλα αυτά, διαφορετικοί κόμβοι έχουν διαφορετικές απαιτήσεις. Για παράδειγμα, οι κάμερες και τα απλά θερμόμετρα είναι ακραία από άποψη λειτουργικότητας και πολυπλοκότητας. Γι' αυτό, ο σχεδιασμός πρέπει να διευκολύνει την ανταλλαγή μεταξύ επαναχρησιμοποίησης, κόστους και απόδοσης.

ε. Εύρωστες λειτουργίες

Επειδή οι αισθητήρες αναπτύσσονται σε μεγάλα και πολλές φορές εχθρικά περιβάλλοντα (δάση, στρατιωτική χρήση, ανθρώπινο σώμα κ.ά.), πρέπει να είναι ανεκτικοί σε σφάλματα και λάθη. Έτσι οι αισθητήρες χρειάζονται ικανότητες αυτοελέγχου, αυτορρύθμισης και αυτό-επισκευής [24].

στ. Ασφάλεια και μυστικότητα

Κάθε αισθητήρας πρέπει να έχει ικανά μέσα ασφαλείας ώστε να αποτρέπει μη εξουσιοδοτημένη πρόσβαση, επιθέσεις και σκόπιμες καταστροφές της πληροφορίας στο εσωτερικό του κόμβου. Επίσης, χρειάζονται επιπλέον μηχανισμοί μυστικότητας.

ζ. Συμβατότητα

Το κόστος της ανάπτυξης λογισμικού υπερτερεί των υπολοίπων συστημάτων. Συγκεκριμένα, είναι σημαντικό να μπορείς να επαναχρησιμοποιείς το λογισμικό μέσω της δυαδικής συμβατότητας ή της δυαδικής μετάφρασης.

η. Ευκαμψία

Είναι απαραίτητο να εξομαλύνεται η λειτουργικότητα και οι χρονικές αλλαγές. Η ευκαμψία μπορεί να επιτευχθεί με δύο μέσα:

1. Ικανότητα προγραμματισμού (αναπτύσσοντας επεξεργαστές όπως μικροεπεξεργαστές, επεξεργαστές DSP, και μικροελεγκτές).
2. Επαναβεβαίωση (χρησιμοποιώντας FPGA πλατφόρμες)

Η ευκαμψία μπορεί να επιτευχθεί με τον προγραμματισμό και την χρήση συνεπεξεργαστών λόγω της χαμηλής κατανάλωσης ισχύος.

3.2.2 Στοιχεία κόμβων αισθητήρων

Όπως αναφέραμε παραπάνω, ο αισθητήρας αποτελείται από τέσσερα βασικά στοιχεία (μονάδα ισχύος, πομποδέκτης, επεξεργαστής, αισθητήρια μονάδα) και πολλά δευτερεύοντα ανάλογα με την αποστολή που πρέπει να φέρει σε πέρας. Παρακάτω παρουσιάζονται χαρακτηριστικά των στοιχείων ενός κόμβου αισθητήρα:

α. Επεξεργαστής

Έχουν αναπτυχθεί πολλοί επεξεργαστές για αισθητήριους κόμβους. Στο [25] αναπτύσσεται ο επεξεργαστής Maia. Ο βασικός στόχος είναι η παροχή παραλληλισμού σε χαμηλά επίπεδα ενέργειας.

Ένα κομμάτι που συνδέεται με τον επεξεργαστή είναι η μονάδα αποθήκευσης. Ανάλογα με τη συνολική δομή του δικτύου, οι απαιτήσεις για αποθήκευση σε σχέση με την γρήγορη και μόνιμη μνήμη σε κάθε κόμβο διαφέρουν. Για παράδειγμα, αν ακολουθείται η αρχιτεκτονική της άμεσης αποστολής των πληροφοριών στον κεντρικό κόμβο, υπάρχει μικρή ανάγκη για τοπική αποθήκευση σε κάθε κόμβο. Σε ένα διαφορετικό σενάριο, όπου ο στόχος είναι η ελάττωση της επικοινωνίας και η διεξαγωγή μεγάλου κομματιού των υπολογισμών σε κάθε κόμβο, θα υπάρχει μεγάλη ανάγκη για τοπική αποθήκευση. Οποιαδήποτε τεχνική ακολουθηθεί είναι αναπόφευκτο ότι θα χρησιμοποιηθεί συμπίεση δεδομένων για να μειωθεί το ποσό των δεδομένων που θα αποθηκευτούν ή θα μεταδοθούν.

β. Μονάδα ισχύος

Υπάρχει απόλυτη σιγουριά ότι η ενέργεια θα είναι ένα από τα μεγαλύτερα τεχνολογικά εμπόδια για τους αισθητήρες [26]. Η παροχή ενέργειας μπορεί να επιλυθεί με δύο τουλάχιστον διαφορετικούς τρόπους. Η πρώτη είναι να εφοδιαστεί κάθε κόμβος με μια επαναφορτιζόμενη πηγή ενέργειας. Έτσι έχουμε δύο επιλογές: είτε να χρησιμοποιήσουμε κυψέλες μπαταρίας υψηλής πυκνότητας, είτε κυψέλες καυσίμων. Οι κυψέλες καυσίμων παρέχουν εξαιρετικά υψηλή πυκνότητα και καθαρή μορφή ενέργειας. Παρόλα αυτά, δεν είναι διαθέσιμες σε κατάλληλη μορφή για κόμβους-αισθητήρες.

Ο δεύτερος τρόπος είναι η συγκέντρωση ενέργειας από το περιβάλλον [27]. Χαρακτηριστικό παράδειγμα είναι η χρήση ηλιακών κυψελών και η μετατροπή των δονήσεων σε ηλεκτρική ενέργεια.

γ. Αισθητήρια Μονάδα

Ο σκοπός των αισθητήρων δεν είναι ούτε ο υπολογισμός ούτε η επικοινωνία, αλλά η ανίχνευση γεγονότων. Το στοιχείο της ανίχνευσης στους αισθητήρες είναι η κύρια τεχνολογική καθυστέρηση και αυτό γιατί οι τεχνολογίες αυτές δεν αναπτύσσονται όπως η ημιαγωγοί. Επακόλουθο είναι οι περιορισμοί να είναι πιο αυστηροί για την αισθητήρια μονάδα παρά για τα υπόλοιπα στοιχεία του κόμβου.

Μία από τις κύριες προκλήσεις για τους αισθητήρες είναι η επιλογή του τύπου και της ποσότητας των κόμβων και ο καθορισμός του χώρου τοποθέτησης. Αυτό το θέμα είναι δύσκολο λόγω των πολλών διαφορετικών τύπων αισθητήρων με διαφορετικές ιδιότητες όπως αναλυτικότητα, κόστος, ακρίβεια, μέγεθος και κατανάλωση ισχύος. Επιπλέον, συχνά χρησιμοποιούνται περισσότεροι του ενός τύπου αισθητήρες για να εξακριβώσουν την ορθότητα της λειτουργίας και των δεδομένων.

Μια άλλη πρόκληση είναι η επιλογή του σωστού τύπου αισθητήρα και ο τρόπος να τους λειτουργήσουμε. Ο βαθμός δυσκολίας έγκειται στην αλληλεπίδραση των αισθητήρων. Για παράδειγμα, εάν θέλουμε να υπολογίσουμε την απόσταση χρησιμοποιώντας ακουστικούς αισθητήρες, θα λαμβάναμε υπόψη τη θερμοκρασία και την υγρασία του περιβάλλοντος τα οποία επηρεάζουν την ταχύτητα του ήχου.

Για τον σχεδιασμό των αισθητήρων λαμβάνονται υπόψη και άλλοι παράγοντες όπως είναι η ανοχή σε σφάλματα, ο έλεγχος λαθών, η βαθμονόμηση και ο συγχρονισμός.

δ. Πομποδέκτης

Οι πομποδέκτες, ως στοιχεία επικοινωνίας, είναι πολύ σημαντικοί, γιατί το ποσό της ενέργειας που αφιερώνεται στη λήψη και αποστολή μηνυμάτων υπερκαλύπτει τις υπόλοιπες λειτουργίες του αισθητήρα [27]. Κατά τη διάρκεια της σχεδίασης και επιλογής του πομποδέκτη πρέπει να ληφθούν υπόψη τρία επίπεδα: φυσικό, MAC και δικτύου. Στο φυσικό επίπεδο, το βασικό θέμα είναι η διαμόρφωση του σήματος και η κωδικοποίηση των δεδομένων με σκοπό τη διατήρηση της επικοινωνίας σε περιβάλλον θορύβου και παρεμβολών. Για να χρησιμοποιηθεί πιο αποτελεσματικά το εύρος ζώνης και για να μειωθεί το κόστος ανάπτυξης, η τυπική τεχνική είναι να μοιράζονται πολλοί πομποδέκτες το ίδιο μέσο σύνδεσης. Η παραπάνω διεργασία επιλύεται στο επίπεδο MAC. Τέλος, το επίπεδο δικτύου είναι υπεύθυνο για την

εγκατάσταση διαδρομών μέσω των οποίων το μήνυμα θα μεταφερθεί από την πηγή στον προορισμό του.

Ο σχεδιασμός ενός πομποδέκτη αποτελεσματικού σε εύρος ζώνης και σε κατανάλωση ισχύος είναι ένα μεγάλο θέμα έρευνας. Η αρχιτεκτονική του πομποδέκτη είναι μια λειτουργία της δομής του δικτύου και των πρωτοκόλλων. Η κύρια ανταλλαγή είναι μεταξύ του σχετικού ενεργειακού κόστους της μετάδοσης και της λήψης και αυτό γιατί το να 'ακούς' το κανάλι είναι ακριβό. Έτσι, είναι αναγκαίο να αναπτυχθούν σχήματα που θα καθιστούν ικανές μεγάλες περιόδους σιγής για τους δέκτες. Μια επιλογή είναι η χρησιμοποίηση συνεργατικής πολιτικής για την επιλογή του κόμβου που θα σιγήσει ενώ η συνδεσιμότητα στον κόμβο θα διατηρηθεί. Η άλλη επιλογή είναι η χρησιμοποίηση δύο πομποδεκτών, ενός υπεύθυνου για τη λήψη δεδομένων που δαπανά πολύ ισχύ και ενός πολύ χαμηλής ισχύος που χρησιμοποιείται μόνο για να ανιχνεύσει αν κάποιος θέλει να στείλει δεδομένα στον αισθητήρα.

3.2.3 Αρχιτεκτονική κόμβου-αισθητήρα

Τα θέματα αρχιτεκτονικής των κόμβων αισθητήρων προσανατολίζονται προς τρεις κατευθύνσεις: *hardware, software και middleware*. Επιπλέον, τα θέματα σχεδιασμού παρουσιάζονται από την πλευρά της σύνθεσης και της ανάλυσης.

Στον πρώτο τομέα, οι αρχικές προσπάθειες περιλαμβάνουν έναν αριθμό σχεδιασμών από ανεξάρτητους κόμβους και σήματα. Η έμφαση σ' αυτόν τον τομέα έχει κατευθυνθεί στην επιβεβαίωση της δημιουργίας πρωτοτύπων και σε ορισμένες περιπτώσεις, στην προώθηση της τεχνολογίας των ανεξάρτητων συστατικών των κόμβων. Στον δεύτερο τομέα, έγινε προσπάθεια να διευθετηθούν οι ανταλλαγές μεταξύ των διάφορων συστατικών ενός κόμβου, δημιουργώντας μια νέα αρχιτεκτονική και ένα λειτουργικό σύστημα (OS). Το κύριο χαρακτηριστικό της τελευταίας προσπάθειας επικεντρώνεται στον αισθητήρα. Η έμφαση είναι στην εκμετάλλευση σχετικά ετοιμοπαράδοτων, ακριβών στοιχείων του κόμβου σε σχέση με το κόστος και την ενέργεια, ως βάση στην εξερεύνηση ποιοτικών και ποσοτικών ανταλλαγών μεταξύ των στοιχείων των κόμβων και των αισθητήρων.

Είναι δύσκολο να προβλεφθούν οι τεχνολογικές τάσεις, αλλά μπορούν να αναγνωριστούν ορισμένες τάσεις επιρροής και οι απαραίτητες λύσεις. Για παράδειγμα, είναι φανερό ότι χρειάζονται αρχιτεκτονικές ισορροπημένες σε κατανάλωση ενέργειας. Ένα άλλο θέμα έρευνας αφορά στην οργάνωση και στην ανάπτυξη της αλληλεπίδρασης μεταξύ των στοιχείων. Τέλος, λόγω των αναγκών σε ασφάλεια, μυστικότητα και αυθεντικότητα υπάρχει απαίτηση σε τεχνικές, όπως ο μοναδικός ID για τους υπολογιστές και για τα άλλα στοιχεία που διευκολύνουν την ασφάλεια.

Στον τομέα του *software,* η κύρια προσπάθεια γίνεται στον πραγματικό χρόνο λειτουργίας των συστημάτων (RTOS) [28]. Υπάρχει ανάγκη για διαχείριση του συστήματος με πολύ χαμηλή ενέργεια λόγω των εμποδίων στην ισχύ. Επιπλέον, χρειάζεται υποστήριξη του λογισμικού για κινητές υπηρεσίες (π.χ. εύρεση τοποθεσίας).

Το *middleware* θα είναι σε μεγαλύτερη ζήτηση για να γίνει δυνατή η ταχεία ανάπτυξη και αξιοποίηση νέων εφαρμογών. Θέματα όπως φιλτράρισμα δεδομένων, συμπίεση, ένωση δεδομένων, αναζήτηση δεδομένων και αποκάλυψη ασφάλειας, θα είναι πάντα επίκαιρα.

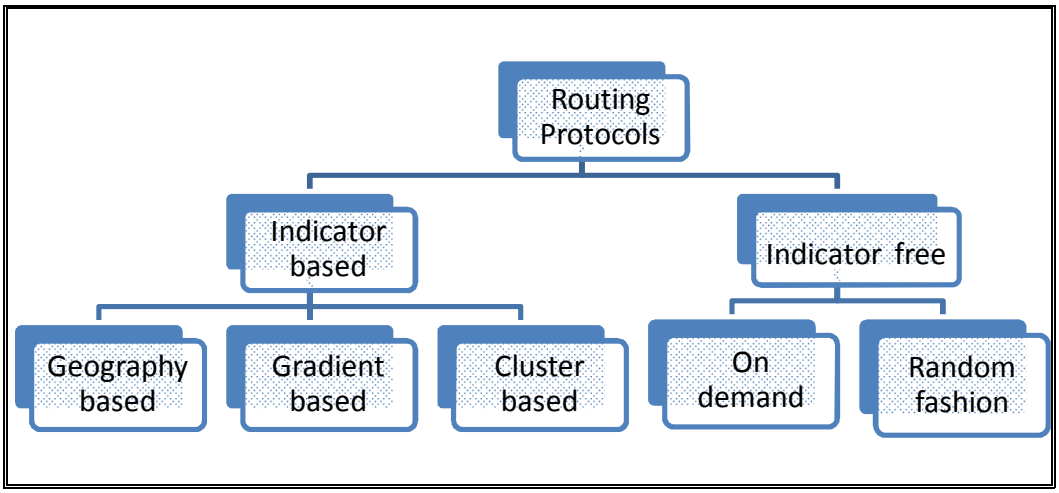
Η σύνθεση των αισθητήρων θα δημιουργήσει καινούργια προβλήματα. Είναι φανερό ότι καινούργια μοντέλα θα δημιουργούνται αλλά και νέα προβλήματα θα

προκύπτουν και τελικά θα επιλύονται. Η ανάπτυξη απλών και φθηνών μοντέλων είναι πρωταρχικής σημασίας, σαν ένα αρχικό σημείο για τη σύνθεση. Είναι γνωστό ότι τα πιο χρονοβόρα συστατικά είναι αυτά που ασχολούνται με τη δημιουργία μοντέρνων μοντέλων, με λιγότερα λάθη και μεγαλύτερη ασφάλεια. Τα παραπάνω κομμάτια, λόγω της ανομοιομορφίας και της πολυπλοκότητας των στοιχείων, θα αποτελέσουν πρόβλημα και κατά τη δημιουργία των αισθητήρων.

3.3 Πρωτόκολλα δρομολόγησης σε δίκτυα αισθητήρων

Ένα από τα σημαντικότερα θέματα στα δίκτυα αισθητήρων είναι η μεταφορά δεδομένων μεταξύ αισθητήρων αλλά και με την μονάδα συλλογής δεδομένων (sink). Παρόλο που τα δίκτυα αισθητήρων και τα δίκτυα ad hoc είναι όμοια ως ένα βαθμό, διαφέρουν σε πολλά σημεία. Τα δίκτυα αισθητήρων έχουν ορισμένα μοναδικά χαρακτηριστικά, τα οποία δημιουργούν καινούργιες ευκαιρίες για περαιτέρω εξέλιξη. Συνήθως τα ad hoc δίκτυα, έχουν ενεργή την ιδιότητα της διαστρωμάτωσης στη σχεδίαση τους (την οποία ουσιαστικά κληρονομούν από τα κλασικά ενσύρματα δίκτυα). Αντίστοιχα, τα πρωτόκολλά τους προσαρμόζονται και αναπτύσσονται σε επίπεδα. Αντίθετα, στα WSN είναι πιο κατάλληλη η σχεδίαση των πρωτοκόλλων όλα σε ένα.

Γενικά, τα υπάρχοντα πρωτόκολλα δρομολόγησης μπορούν να χωρισθούν σε δύο κατηγορίες: πρωτόκολλα βάσει ενδείκτη και πρωτόκολλα χωρίς ενδείκτη. Μια περαιτέρω ταξινόμηση φαίνεται στο Σχήμα 5 [4]:



Σχήμα 5. Ταξινόμηση πρωτοκόλλων δρομολόγησης

Στα πρωτόκολλα βάσει ενδείκτη υπάρχει πάντα μια αρχική φάση όπου εφαρμόζεται ένας αλγόριθμος παραγωγής ενδείκτη. Σύμφωνα με τον αλγόριθμο, κάθε κόμβος παράγει έναν ενδείκτη που βοηθάει στον καθορισμό του δρομολογίου. Στην κατηγορία πρωτοκόλλων χωρίς ενδείκτη, τα δρομολόγια δημιουργούνται αυθαίρετα.

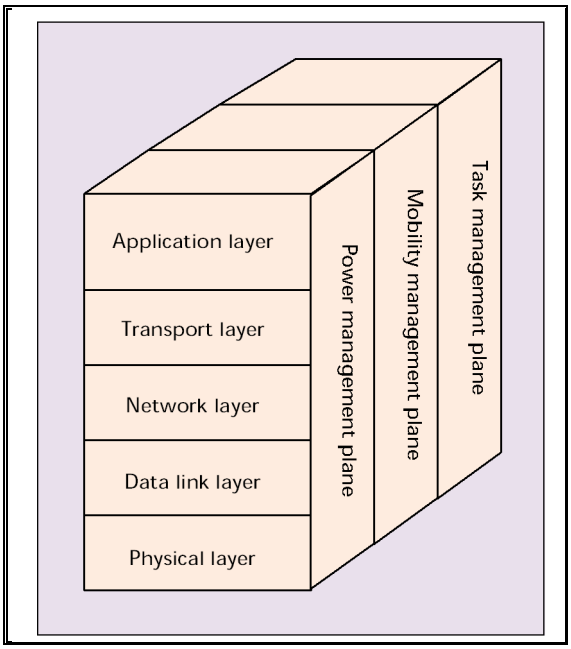
Παρατηρούμε ότι στα πρωτόκολλα δρομολόγησης το σημαντικότερο θέμα είναι η συντήρηση της ενέργειας. Η ενέργεια είναι σημαντικότερη ακόμα και από την απόδοση του δικτύου. Όσο η ενέργεια εξαντλείται, το δίκτυο μπορεί να ελαττώσει την ποιότητα των δεδομένων για να μειώσει την απώλεια της ενέργειας και έτσι να αυξήσει τον χρόνο ζωής του δικτύου. Παρόλα αυτά πρέπει να ελέγχονται και οι

υπόλοιποι παράμετροι για την εύρυθμη λειτουργία του δικτύου. Έτσι τα πρωτόκολλα δρομολόγησης σ' ένα δίκτυο αισθητήρων πρέπει να ικανοποιούν τις παρακάτω απαιτήσεις (ταυτόσημες με τις αντίστοιχες των ad hoc δικτύων):

- Πλήρως κατανεμημένα.
- Προσαρμοστικότητα στις συχνές αλλαγές τοπολογίας του ασύρματου δικτύου.
- Ο υπολογισμός δρομολογίων και η διαχείριση πρέπει να εμπλέκει τον ελάχιστο αριθμό κόμβων.
- Ελάχιστος αριθμός συγκρούσεων πακέτων.
- Παροχή ικανοποιητικής ποιότητας υπηρεσιών (QoS).
- Χρήση των ελάχιστων πόρων (όπως το εύρος ζώνης).

3.3.1 Sensor Network Protocol Stack

Η στοίβα πρωτοκόλλων που χρησιμοποιείται στη δεξαμενή (sink) και στους κόμβους φαίνεται στο Σχήμα 6 [5].



Σχήμα 6. Η στοίβα πρωτοκόλλων των δικτύων αισθητήρων

Η στοίβα πρωτοκόλλων συνδυάζει ενημερότητα ισχύος και δρομολόγησης, ενοποιεί τα δεδομένα με τα πρωτόκολλα δικτύωσης, επικοινωνεί αποτελεσματικά διά μέσου του ασύρματου μέσου και προάγει τις συνεργατικές προσπάθειες των αισθητήρων. Η στοίβα πρωτοκόλλων αποτελείται από το φυσικό επίπεδο (*physical layer*), το επίπεδο ζεύξης δεδομένων (*data link layer*), το επίπεδο δικτύου (*network layer*), το επίπεδο μεταφοράς (transport layer) και το επίπεδο εφαρμογής (*application layer*). Στις κάθετες στήλες υπάρχουν τα επίπεδα διαχείρισης ισχύος (*power management plane*), διαχείρισης κινητικότητας (*mobility management plane*) και διαχείρισης στόχου (*task management plane*). Το φυσικό επίπεδο διευθύνει τις

ανάγκες της διαμόρφωσης, της μετάδοσης και τις τεχνικές λήψης δεδομένων. Μιας και το περιβάλλον είναι θορυβώδες και οι αισθητήρες μπορούν να είναι κινητοί, το πρωτόκολλο medium access control (MAC) πρέπει να είναι ενήμερο για θέματα ισχύος και ελαχιστοποιεί τις συγκρούσεις μεταξύ γειτονικών εκπομπών. Το επίπεδο δικτύου φροντίζει για τη δρομολόγηση των δεδομένων που παρέχονται από το επίπεδο μεταφοράς. Το επίπεδο μεταφοράς βοηθάει στη διατήρηση της ροής των δεδομένων, εάν οι εφαρμογές το απαιτούν. Ανάλογα με τις αποστολές ανίχνευσης, διαφορετικές μορφές λογισμικού μπορούν να κατασκευαστούν και να χρησιμοποιηθούν από το επίπεδο εφαρμογής. Επιπλέον, τα επίπεδα διαχείρισης ισχύος, κινητικότητας και αποστολών, ελέγχουν την ισχύ, την κίνηση και τη διανομή της αποστολής μεταξύ των αισθητήρων. Αυτά τα επίπεδα, βοηθούν τους αισθητήριους κόμβους να συντονίζουν την αποστολή τους και να μειώνουν την συνολική κατανάλωση ενέργειας.

Το επίπεδο διαχείρισης ισχύος, διευθύνει την κατανάλωση ισχύος σε έναν αισθητήρα. Για παράδειγμα, ο αισθητήρας μπορεί να κλείσει τους δέκτες του αφού λάβει ένα μήνυμα από έναν γείτονά του. Αυτό μπορεί να γίνει για να αποφύγει την λήψη αντιγραμμένου μηνύματος. Επίσης, όταν το επίπεδο ισχύος του αισθητήρα είναι χαμηλό, εκπέμπει ένα μήνυμα στους γείτονές του ότι έχει χαμηλή ισχύ και δεν μπορεί να συμμετάσχει στη δρομολόγηση μηνυμάτων. Η υπόλοιπη ισχύς φυλάσσεται για ανίχνευση. Το επίπεδο διαχείρισης δικτύου εντοπίζει και καταγράφει τις κινήσεις του αισθητήρα ώστε να διατηρείται μια διαδρομή επιστροφής στον χρήστη. Επίσης, οι αισθητήρες μπορούν να κρατούν στοιχεία για τους γειτονικούς τους κόμβους και έτσι μπορούν να εξισορροπήσουν την ισχύ τους. Το επίπεδο διαχείρισης στόχου σχεδιάζει τις αποστολές ανίχνευσης που δίνονται σε μια συγκεκριμένη γεωγραφική περιοχή. Δεν χρειάζονται όλοι οι αισθητήρες για να επιτελέσουν την αποστολή ανίχνευσης την ίδια χρονική στιγμή. Ορισμένοι κόμβοι χρειάζονται περισσότερο, ενώ άλλοι δεν χρειάζονται, ανάλογα και με το επίπεδο της ισχύος τους.

Ο παραπάνω διαχωρισμός σε επίπεδα χρειάζεται ώστε οι αισθητήρες να μπορούν να εργάζονται μεταξύ τους σε πιο αποδοτική μορφή, να δρομολογούν τα δεδομένα σ' ένα ασύρματο δίκτυο αισθητήρων και να μοιράζονται πληροφορίες μεταξύ τους.

3.3.2 Πρωτόκολλα με ενδείκτη

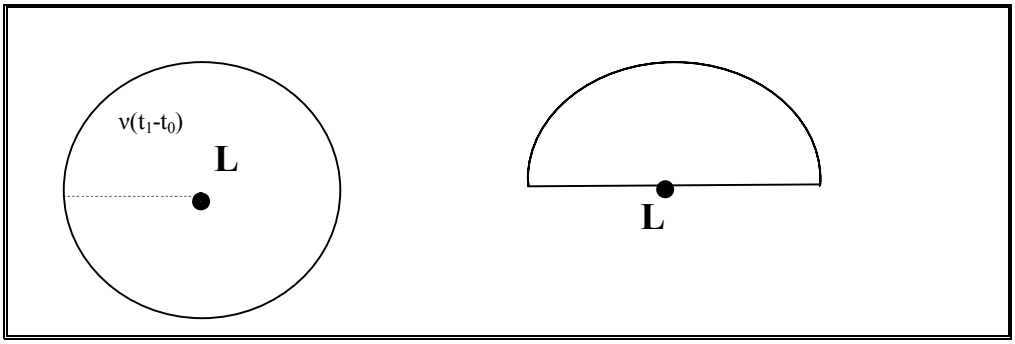
Σ' αυτήν την κατηγορία, οι ενδείκτες δημιουργούνται για τους αισθητήρες σε μια φάση προετοιμασίας. Στη συνέχεια, οι αισθητήρες χρησιμοποιούν αυτούς τους ενδείκτες για να αποφασίσουν για τη δρομολόγηση. Ανάλογα με τους διάφορους τύπους ενδεικτών, κατηγοριοποιούμε περαιτέρω τα πρωτόκολλα, όπως φαίνεται στο σχήμα 3, σε geography-, gradient- και cluster-based.

α. Geography based

Ορισμένα πρωτόκολλα υποθέτουν ότι είναι διαθέσιμες οι ακριβείς τοποθεσίες των αισθητήρων. Τα πακέτα μεταφέρουν την τοποθεσία της πηγής και του προορισμού, βοηθώντας τους ενδιάμεσους κόμβους να τα προωθήσουν στο κατάλληλο δρομολόγιο. Γενικά, ο αποστολέας επιλέγει το επόμενο βήμα ως αυτό που είναι πιο κοντά στον προορισμό. Αυτή η πολιτική χρησιμοποιείται μέχρι τελικά το πακέτο να φτάσει στον προορισμό του.

(1). Το *Location-Aided Routing (LAR)* είναι ένα πρωτόκολλο που αντί να πλημμυρίζει όλο το δίκτυο, επιλέγει μία μικρή περιοχή για να διασπείρει τα δεδομένα. Το LAR χρησιμοποιεί πληροφορία θέσης (η οποία μπορεί να είναι ξεπερασμένη την ώρα που χρησιμοποιείται) για να μειώσει το χώρο έρευνας για ένα δρομολόγιο. Ελαχιστοποίηση του χώρου έρευνας σημαίνει λιγότερα μηνύματα εύρεσης δρομολογίου. Συνήθως η πληροφορία θέσης που χρησιμοποιείται στο LAR παρέχεται από ένα σύστημα GPS.

Ο αλγόριθμος λειτουργεί όπως παρακάτω: Καθορίζονται η *αναμενόμενη ζώνη (expected zone)* και η *ζώνη αίτησης (request zone)*. Ως *αναμενόμενη ζώνη* θεωρείται μια γεωγραφική περιοχή όπου αναμένεται να περιέχει τον κόμβο προορισμού *D* σε κάποιο μελλοντικό χρόνο. Έτσι, εάν στον χρόνο t_0 ο *D* βρίσκεται σε κάποιο σημείο και σε χρόνο t_1 κινείται με μέση ταχύτητα u τότε μπορούμε να υπολογίσουμε μια τοποθεσία *L* στην οποία αναμένουμε να βρίσκεται ο *D*. Εάν ο αρχικός κόμβος *S* δεν ξέρει την προηγούμενη θέση του *D,* τότε ως αναμενόμενη ζώνη θεωρείται ολόκληρη η περιοχή που ελέγχουμε. Σε αυτήν την περίπτωση, ο αλγόριθμος *LAR* μεταπίπτει σε απλό αλγόριθμο πλημύρας μηνυμάτων.

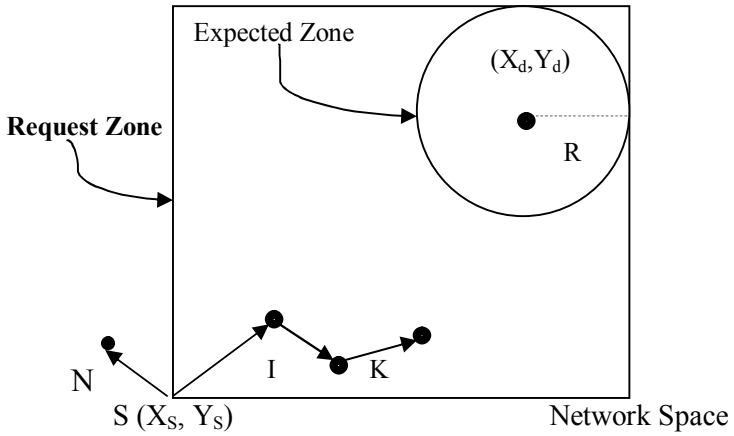


Σχήμα 7. Παράδειγμα αναμενόμενης ζώνης

Εάν τώρα έχουμε περισσότερες πληροφορίες σχετικά με την κίνηση του κόμβου *D,* μπορεί να οδηγήσει σε μικρότερη αναμενόμενη ζώνη. Παράδειγμα στο Σχήμα 7, αν γνωρίζουμε ότι ο *D* κινείται βόρεια, τότε η αναμενόμενη ζώνη μειώνεται στο ημικύκλιο της δεύτερης περίπτωσης. Η *ζώνη αίτησης* καθορίζεται ώστε να περιλαμβάνει την αναμενόμενη ζώνη αλλά και άλλες περιοχές που θα μπορέσουν να γειτνιάσουν με την αναμενόμενη ζώνη. Ένα πακέτο προωθείται μόνο αν ο επόμενος κόμβος βρίσκεται μέσα στην ζώνη αίτησης. Οπότε κάθε κόμβος, όταν δέχεται μια route request, πρέπει να καθορίσει αν βρίσκεται μέσα στην ζώνη αίτησης για αυτήν την αίτηση.

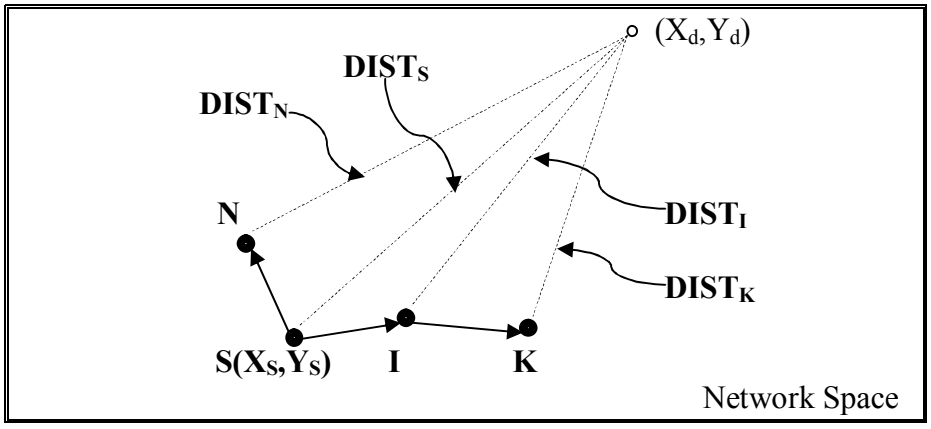
Έχουν αναπτυχθεί δύο σχήματα για την εύρεση δρομολογίου βάσει του πρωτοκόλλου *LAR*.

I. Στην πρώτη περίπτωση, η έκταση της ζώνης αίτησης εξαρτάται από την μέση ταχύτητα κίνησης αλλά και από τον χρόνο που πέρασε από την τελευταία καταγεγραμμένη πληροφορία θέσης του κόμβου. Έτσι η ζώνη αίτησης καθορίζεται ως η μικρότερη ορθογώνια περιοχή που περιέχει τωρινή θέση του *S* και την αναμενόμενη ζώνη, έτσι ώστε οι πλευρές του ορθογωνίου να είναι παράλληλες προς τους άξονες X, Y (Σχήμα 8).



Σχήμα 8. Σχήμα LAR-1

II. Στο πρώτο σχήμα, ο *S* καθορίζει τη ζώνη αίτησης στο μήνυμα route request. Αντίθετα, στο δεύτερο σχήμα, ο *S* περιέχει την απόσταση DIST από τον *D* και τις συντεταγμένες (X_d, Y_d). Σε αυτή τη περίπτωση, ο κάθε ενδιάμεσος κόμβος προωθεί το πακέτο προς τον γειτονικό κόμβο μόνο αν αυτός είναι πλησιέστερα ή όχι μακρύτερα από (X_d, Y_d) από ότι ο γείτονάς του (Σχήμα 9).

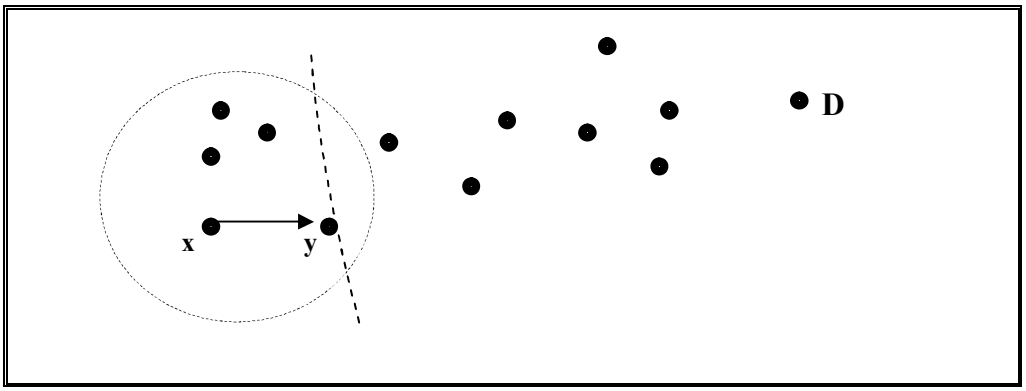


Σχήμα 9. Σχήμα LAR-2

Από την χρήση του πρωτοκόλλου παρατηρούμε ότι η χρήση πληροφορίας θέσης οδηγεί στην μείωση της επιβάρυνσης δρομολόγησης από τα πρωτόκολλα που δεν χρησιμοποιούν αυτήν την πληροφορία. Με περαιτέρω βελτίωση των βασικών σχημάτων του πρωτοκόλλου πετυχαίνουμε καλυτέρα αποτελέσματα.

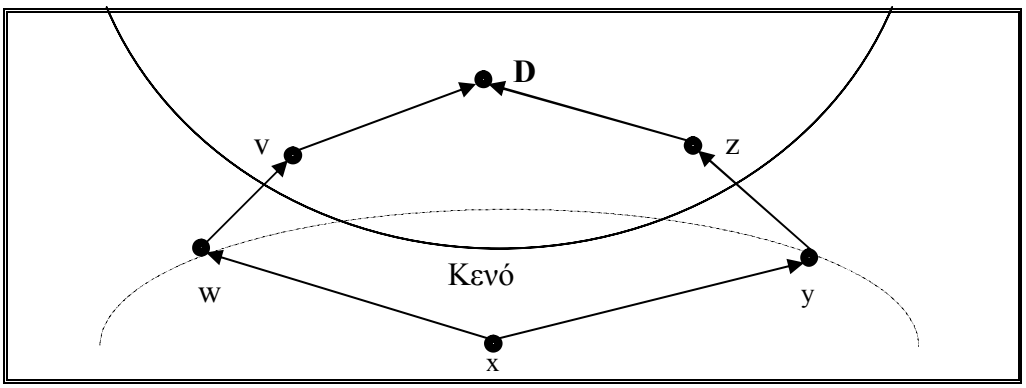
(2). Το πρωτόκολλο *Greedy Perimeter Stateless Routing (GPSR)* είναι ένας αλγόριθμος μοναδικής διαδρομής που αποφεύγει την πλημμύρα πληροφοριών στο δίκτυο. Το πρωτόκολλο χρησιμοποιεί τη θέση των κόμβων και την κατεύθυνση των πακέτων για να πάρει απόφαση για το που θα προωθήσει τα πακέτα. Επίσης, σε περιπτώσεις έντονης κινητικότητας, χρησιμοποιεί την τοπική πληροφορία τοπολογίας για να βρίσκει γρηγορότερα διαδρομές.

Το GPSR αποτελείται από δύο μεθόδους για να καθορίσει ένα δρομολόγιο: *greedy forwarding* και *perimeter forwarding*. Με τη μέθοδο *greedy forwarding (άπληστη προώθηση)* κάθε πακέτο μαρκάρεται από τον κατασκευαστή του με την τοποθεσία προορισμού του. Έτσι, κάθε ενδιάμεσος κόμβος μπορεί να κάνει μια τοπική βέλτιστη επιλογή για τον επόμενο κόμβο προορισμού του πακέτου. Ειδικότερα, εάν ο κόμβος ξέρει την τοποθεσία του γειτονικού κόμβου, η πιο βέλτιστη λύση είναι να προωθήσει τα πακέτα στον πλησιέστερα γεωγραφικά κόμβο προς τον προορισμό του πακέτου (Σχήμα 10). Η τακτική αυτή συνεχίζεται μέχρι τέλους. Σε περίπτωση που κάποιος κόμβος δεν λάβει ένα σήμα για κάποιο χρονικό διάστημα από γειτονικό κόμβο, υποθέτει ότι αυτός ο κόμβος έχει μετακινηθεί ή απορριφθεί και διαγράφει αυτόν τον κόμβο από τη λίστα του. Το μεγαλύτερο πλεονέκτημα αυτής της μεθόδου είναι η στήριξη μόνο στην γνώση των άμεσα γειτονικών κόμβων. Έτσι, δεν χρειάζεται πολύ πυκνά κατανεμημένα δίκτυα για να επιτύχει την αποστολή του. Το κύριο μειονέκτημα αυτής της τεχνικής είναι ότι υπάρχουν τοπολογίες όπου εάν χρειάζεται μόνο ένα άλμα για να φτάσει το πακέτο στον προορισμό του, πιθανόν να χρειαστούν περισσότερα εγγύτερα άλματα μέχρι την ολοκλήρωση.



Σχήμα 10. Παράδειγμα τεχνικής *άπληστης προώθησης*

Με την μέθοδο *perimeter forwarding (περιμετρική προώθηση),* προσπαθούμε να προωθήσουμε πακέτα περιμετρικά των κενών που δημιουργούνται κατά την έλλειψη ενδιάμεσων κόμβων που παρουσιάζονται μεταξύ δύο κόμβων (Σχήμα 11).



Σχήμα 11. Παράδειγμα τεχνικής περιμετρικής προώθησης

Τα πλεονεκτήματα του GPSR πηγάζουν από την χρήση της άμεσης πληροφορίας των γειτονικών κόμβων στην απόφαση προώθησης. Τα πρωτόκολλα δρομολόγησης που στηρίζουν την από άκρη σε άκρη δρομολόγηση στην εύρεση του δρομολογίου μεταξύ των κόμβων προορισμού και αποστολής (όπως είναι οι αλγόριθμοι Distance Vector και Link State), αντιμετωπίζουν προβλήματα όσο η διάμετρος του δικτύου και η κινητικότητα αυξάνονται καθόσον αυτοί οι δύο παράγοντες καθορίζουν τον ρυθμό που αλλάζουν τα δρομολόγια. Η ιεραρχία και η χρήση μνήμης έχει αποδειχθεί αποτελεσματική σε αυτές τις περιπτώσεις. Η γεωγραφία, όπως χρησιμοποιείται στο GPRS, παρουσιάζει ένα σημαντικό πλεονέκτημα στην κλιμάκωση της δρομολόγησης.

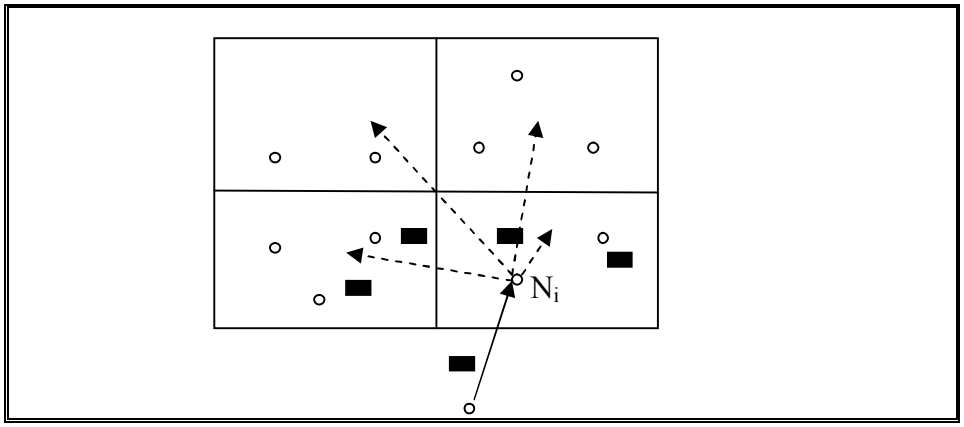
(3). Το πρωτόκολλο *Geographical and Energy Aware Routing (GEAR)* προσπαθεί να λύσει το πρόβλημα του κενού που δημιουργείται στο GPSR. Η διαφορά από τα υπόλοιπα γεωγραφικά πρωτόκολλα έγκειται στους παρακάτω τομείς:

- Σε αντίθεση με την απλή επικοινωνία, ελέγχεται το πρόβλημα της προώθησης ενός πακέτου σε όλους τους κόμβους μέσα σε μια περιοχή η οποία είναι κοινή σε επικοινωνία που στηρίζεται στα δεδομένα.
- Το πρωτόκολλο *GEAR* δεν προϋποθέτει την ανάγκη μιας βάσης δεδομένων τοποθεσίας που αντιστοιχίζει τα αναγνωριστικά των κόμβων με την τοποθεσία των κόμβων.
- Το πρωτόκολλο απευθύνεται σε στατικούς κόμβους.
- Υποτίθεται η ύπαρξη ενός συστήματος εντοπισμού που βοηθάει κάθε κόμβο να γνωρίζει τη θέση του.
- Στο πρωτόκολλο *GEAR* χρησιμοποιούνται παράμετροι που αφορούν στην κατανάλωση ενέργειας μαζί με γεωγραφική πληροφορία για να ληφθούν αποφάσεις δρομολόγησης με αποτελεσματική κατανάλωση ενέργειας.

Η διαδικασία της προώθησης ενός πακέτου σε όλους τους κόμβους στην περιοχή ενδιαφέροντος αποτελείται από δύο φάσεις:

I. Προώθηση των πακέτων προς την περιοχή ενδιαφέροντος. Το *GEAR* χρησιμοποιεί επιλογή του γειτονικού κόμβου βάσει γνώσης της γεωγραφικής και ενεργειακής κατάστασής του. Πρέπει να σκεφτούμε δύο περιπτώσεις: όταν ο επόμενος κόμβος υπάρχει, το *GEAR* επιλέγει το επόμενο βήμα ως τον πλησιέστερο προς τον προορισμό κόμβο. Επίσης, όταν όλοι οι κόμβοι είναι μακριά, το *GEAR* επιλέγει τον επόμενο κόμβο ως τον κόμβο που μειώνει κάποιο ενεργειακό κόστος.

II. Διασπορά των πακέτων μέσα στην περιοχή ενδιαφέροντος. Στις περισσότερες περιπτώσεις χρησιμοποιείται η Αναδρομική Γεωγραφική Δρομολόγηση (Recursive Geographic Routing) για τη διασπορά των πακέτων (Σχήμα 12). Σε περιπτώσεις αραιής ανάπτυξης δικτύων χρησιμοποιείται περιορισμένη πλημμύρα δεδομένων.



Σχήμα 12. Αναδρομική Γεωγραφική Δρομολόγηση.

Η ιδέα είναι η εξής: για κάθε εκπεμπόμενο πακέτο, ο αποστολέας N δημιουργεί ένα *αποκτηθέν κόστος h(N,R)* προς μια περιοχή R. Εάν ένας κόμβος δεν έχει μια τιμή *h(N,R)* για κάποιο γείτονα, τότε υπολογίζει ένα *εκτιμώμενο κόστος c(N,R)* όπως παρακάτω:

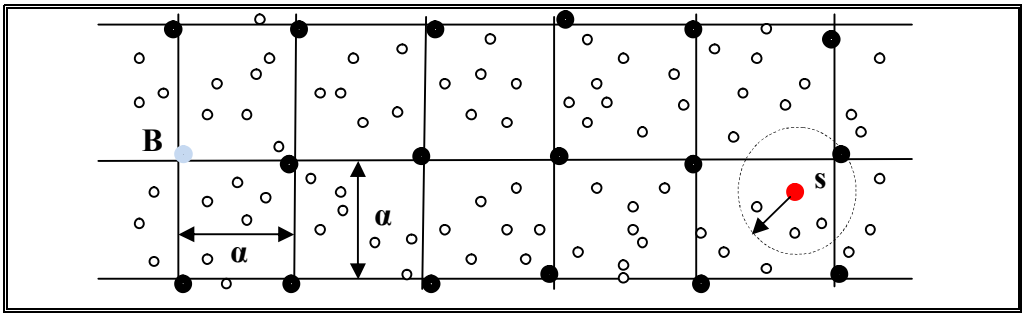
$$\boldsymbol{c(N_i, R) = \alpha \times d(N_i, R) + (1 - \alpha) \times e(N_i)}$$

όπου *α* είναι ένα μεταβλητό βάρος, $d(N_i,R)$ είναι η απόσταση από τον κόμβο N_i προς την κεντρική περιοχή *D* της περιοχής *R*, και $e(N_i)$ είναι η καταναλωθείσα ενέργεια στον κόμβο N_i κανονικοποιημένη στην μεγαλύτερη καταναλωθείσα ενέργεια από τους γείτονες του N_i. Όταν ένας κόμβος λαμβάνει ένα μήνυμα από τον άμεσα γειτονικό του καθορίζει το δικό του *αποκτηθέν κόστος h(N,R)* ως $h(N_{min},R)+C(N, N_{min})$, όπου ο τελευταίος όρος είναι το κόστος μετάδοσης ενός πακέτου από τον κόμβο N προς τον N_{min}. Τώρα που έχει τις δύο τιμές, ο κόμβος θα διαλέξει το επόμενο άλμα μεταξύ των κόμβων που είναι πιο κοντά στον προορισμό ελαχιστοποιώντας το κόστος *h(N,R)*. Όταν όλοι οι γειτονικοί κόμβοι είναι μακριά, τότε δημιουργείται μια τρύπα. Σε περίπτωση ύπαρξης τρύπας, το αποκτηθέν κόστος συνδυάζεται με πληροφορίες ανανέωσης για να παρακαμφθεί η τρύπα.

Όταν το πακέτο βρίσκεται μέσα στην περιοχή ενδιαφέροντος με απλή πλημμύρα δεδομένων, μπορούμε να φτάσουμε στον κόμβο προορισμού. Όμως η πλημμύρα δεδομένων είναι ακριβή από άποψη ενέργειας, καθόσον κάθε κόμβος πρέπει να μεταδώσει προς όλες τις κατευθύνσεις και όλοι οι γείτονες θα λάβουν τα δεδομένα. Σε αυτήν την περίπτωση χρησιμοποιείται η τεχνική της αναδρομικής δρομολόγησης (Recursive Geographic Routing), κατά την οποία χωρίζεται η περιοχή ενδιαφέροντος σε 4 υπό-περιοχές και μεταδίδεται το μήνυμα σε 4 αντίγραφα, ένα για κάθε μία υπό-περιοχή. Η διάσπαση αυτή επαναλαμβάνεται μέχρις ότου βρεθεί ο κόμβος προορισμού μέσα σε κάποια υπό-περιοχή. Παρατηρούμε ότι δημιουργείται ένα πρόβλημα για το ποια τεχνική να διαλέξουμε για την μετάδοση μέσα στην περιοχή ενδιαφέροντος (αναδρομική δρομολόγηση ή επιλεκτική πλημμύρα δεδομένων). Η τεχνική εξαρτάται από την πυκνότητα του δικτύου. Έτσι σε αραιά δίκτυα είναι προτιμότερο να χρησιμοποιείται επιλεκτική δρομολόγηση ενώ αντίθετα σε πυκνά δίκτυα χρησιμοποιείται η αναδρομική δρομολόγηση.

Σε σύγκριση που γίνεται με το προηγούμενο πρωτόκολλο (GPSR) επιτυγχάνεται καλύτερη παράδοση πακέτων (25% έως 35% περισσότερα πακέτα). Επίσης, επιτυγχάνεται μικρότερη κατανάλωση ενέργειας αναλογικά με τα πακέτα που παραδίδονται.

(4). Το πρωτόκολλο *Two-Tier Data Dissemination (TTDD)* [29], δημιουργήθηκε για εφαρμογές πολλών κινητών δεξαμενών (sink). Μια δεξαμενή είναι μια συσκευή που συλλέγει δεδομένα και αναφορές από τους κόμβους του δικτύου. Όταν ένας κόμβος παράγει δεδομένα, ετοιμάζει τη διάδοσή τους δημιουργώντας μια δικτυωτή κατασκευή. Η πηγή ορίζει τη δική της θέση ως σημείο διασταύρωσης του πλέγματος και το ανακοινώνει και στα τέσσερα άλλα σημεία του πλέγματος. Κάθε ανακοίνωση σταματάει τελικά σε έναν κόμβο που βρίσκεται εγγύτερα στο σημείο διασταύρωσης που αναφέρεται στο μήνυμα. Ο κόμβος αποθηκεύει την πληροφορία θέσης της πηγής και προωθεί το μήνυμα στο επόμενο σημείο διασταύρωσης, πλην αυτού που έχει λάβει το μήνυμα (Σχήμα 13).



Σχήμα 13. Πλέγμα στο πρωτόκολλο TTDD.

Όταν δημιουργηθεί το πλέγμα, η δεξαμενή μπορεί να πλημμυρίσει τις αιτήσεις της σε ένα συγκεκριμένο κελί του πλέγματος για να λάβει δεδομένα. Η αίτηση θα φτάσει στον πλησιέστερο κόμβο του πλέγματος ο οποίος στην συνέχεια θα την μεταδώσει στους υπόλοιπους κόμβους του πλέγματος. Τα ληφθέντα δεδομένα θα ακολουθήσουν την αντίθετη κατεύθυνση προς τη δεξαμενή.

Το πλέγμα - όπως φαίνεται και στο παραπάνω σχήμα - είναι χωρισμένο σε κελιά μεγέθους $\alpha \times \alpha$. Στα ακραία σημεία των κελιών βρίσκονται οι *κόμβοι διάδοσης*. Η θέση των κόμβων αυτών δεν είναι ακριβώς πάνω στις άκρες των κελιών. Αυτό δεν επηρεάζει την ορθή λειτουργία του *TTDD*. Ο λόγος που δεν επηρεάζεται είναι ότι κάθε *κόμβος διάδοσης* περιλαμβάνει στα μηνύματα του τη θέση του (και όχι τη θέση του σημείου διάδοσης). Η επιλογή της παραμέτρου α επηρεάζει την κατανάλωση ενέργειας και την πολυπλοκότητα του δικτύου. Το πρωτόκολλο χρησιμοποιεί δύο επίπεδα για την εκτέλεσή του. Ένα επίπεδο επικοινωνίας μεταξύ των κόμβων διάδοσης που βρίσκονται στις γωνίες των κελιών του πλέγματος και ένα επίπεδο επικοινωνίας των κόμβων διάδοσης με τους εσωτερικούς κόμβους του δικτύου και τους κόμβους-δεξαμενές.

Υπάρχουν επίσης και άλλα πρωτόκολλα με βάσει την γεωγραφική εύρεση του επόμενου βήματος δρομολόγησης όπως το SPAN, το GHT κ.ά. Τα πρωτόκολλα με βάσει την γεωγραφία είναι πολύ καλά στην εύρεση του προορισμού, στην περίπτωση

που ο προορισμός υπάρχει. Όταν δεν υπάρχει, ο αλγόριθμος τελειώνει στον πλησιέστερο προς τον προορισμό κόμβο. Επίσης παρέχει μη κατευθυντική παράδοση πληροφορίας με την οποία τα μηνύματα μπορούν να σταλούν σε οποιοδήποτε ζεύγος κόμβων. Όμως αυτές οι εφαρμογές χρειάζονται πληροφορία γεωγραφικής θέσης, η οποία είναι χρονοβόρα και καταναλώνει ενέργεια σε απλούς αισθητήριους κόμβους.

β. Gradient based

Στην κατηγορία αυτή ανήκουν πρωτόκολλα που δεν χρησιμοποιούν την γεωμετρική απόσταση για να δρομολογήσουν τα πακέτα προς τον προορισμό, αλλά μία σχετική απόσταση μεταξύ των κόμβων. Τέτοια σχετική απόσταση είναι το άνυσμα (gradient) που δηλώνει την κατεύθυνση προς τον δημιουργό του πακέτου.

(1). Στο πρωτόκολλο *Minimum Cost Forwarding for Large Scale Sensor Networks (MCFN),* εξετάζεται το πρόβλημα της παράδοσης των πακέτων από τον κόμβο στη δεξαμενή (sink). Κάθε κόμβος περιέχει ένα πεδίο κόστους ως το ελάχιστο κόστος από τον κόμβο προς τη δεξαμενή. Με τη δημιουργία του πεδίου κόστους, τα πακέτα οδηγούνται προς την δεξαμενή κατά μήκος του πεδίου κόστους προς την κατεύθυνση μειούμενου κόστους. Κάθε ενδιάμεσος κόμβος, με την λήψη του πακέτου, ελέγχει αν βρίσκεται στην διαδρομή μικρότερου κόστους. Αν βρίσκεται, τότε εκπέμπει το πακέτο στους γειτονικούς κόμβους. Αυτή η διαδικασία συνεχίζεται μέχρι το πακέτο να φτάσει στον προορισμό του.

(2). Το πρωτόκολλο *ARRIVE* θεωρεί τον αριθμό των αλμάτων ως το άνυσμα. Έτσι οι κόμβοι διατηρούν μια λίστα με τους αμέσως γειτονικούς κόμβους και βάσει αυτής της λίστας εκτελούν την επόμενη κίνηση.

(3). Στο πρωτόκολλο *Direct Diffusion (D.D.),* ακολουθείται ένας αλγόριθμος με κέντρο τα δεδομένα [30]. Αποτελείται από τέσσερα κομμάτια: *ενδιαφέροντα (interests), μηνύματα δεδομένων (data messages), ανύσματα (gradients) και ενισχύσεις (reinforcements).* Αρχικά, μία ερώτηση μετατρέπεται σε 'ενδιαφέρον' και διαχέεται προς την περιοχή ενδιαφέροντος. Για παράδειγμα, όταν η αποστολή μας είναι η ανίχνευση κάποιου ζώου, η μορφή του ερωτήματος-ενδιαφέροντος είναι η παρακάτω:

```
Type = four-legged animal          // detect animal location
Interval = 20 ms                   // send back events every 20 ms
Duration = 10 seconds              // .. for the next 10 seconds
Rect=[-100, 100, 200,400]          // from sensors within rectangle
```

Παρατηρούμε ότι το ερώτημά μας περιλαμβάνει το όνομα των δεδομένων που θα ανιχνευθούν (type), τον χρόνο που θα διαρκέσει η ανίχνευση (duration), τον χρόνο που θα στέλνει ο κόμβος τα δεδομένα (interval) και τέλος την περιοχή που θα ελεγχθεί (rect). Κατά τη δημιουργία ενός ερωτήματος μπορούν να δημιουργηθούν και άλλοι τύποι ερωτημάτων. Όταν ένας κόμβος λάβει το 'ενδιαφέρον', ενεργοποιεί τον αισθητήρα και αρχίζει την καταγραφή τον γεγονότων. Τα ανιχνευμένα δεδομένα - στη συνέχεια - επιστρέφουν στο αντίθετο δρομολόγιο από αυτό που αρχικά εκπέμφθηκε το 'ενδιαφέρον'. Έτσι, στο προηγούμενο παράδειγμα, η απάντηση από τους υπολοίπους κόμβους θα είναι της παρακάτω μορφής:

Type = four-legged animal	**// type of animal seen**
Instance = elephant	**// instance of this type**
Location = [125, 220]	**// node location**
Intensity = 0.6	**// signal amplitude measure**
Confidence = 0.85	**// confidence in the match**
Timestamp = 01:20:40	**// event generation time**

Οι ενδιάμεσοι κόμβοι μπορεί να συγκεντρώσουν τα δεδομένα ανάλογα με το περιεχόμενό τους. Κάθε ενδιάμεσος κόμβος περιέχει μια κρυφή μνήμη από ενδιαφέροντα. Κάθε αντικείμενο στην μνήμη αντιστοιχεί σε διαφορετικό ενδιαφέρον. Οι είσοδοι ενδιαφερόντων στην μνήμη δεν περιέχουν πληροφορίες για τον αρχικό κόμβο. Κάθε ενδιαφέρον αποτελείται από διάφορα πεδία ('timestamp', 'gradient', 'rate', 'duration', 'expires at' fields). Όταν ένας κόμβος λάβει ένα ενδιαφέρον, ελέγχει να δει μήπως υπάρχει ένα αντίγραφό του στην μνήμη του. Εάν όχι, τότε δημιουργεί ένα νέο αντίγραφο το οποίο περιέχει μια αναφορά στον κόμβο από τον οποίο προήλθε. Εάν υπάρχει ήδη στην μνήμη του, τότε απλώς ανανεώνει τα πεδία που έχει το ενδιαφέρον. Ένας κόμβος που ελέγχει έναν συγκεκριμένο στόχο, ελέγχει τη μνήμη του για μια παρόμοια είσοδο ενδιαφέροντος. Αν βρει, επιφορτίζει τα συστήματά του να ελέγξουν την περιοχή με μέγιστο ρυθμό αναφοράς. Ένας ενδιάμεσος κόμβος που λαμβάνει μηνύματα από τους γείτονες προσπαθεί να βρει μια παρόμοια είσοδο ενδιαφέροντος στη μνήμη του. Εάν δεν υπάρχει, τότε τα δεδομένα απορρίπτονται. Αν υπάρχει, τότε κρατάει αντίγραφο των πρόσφατα ελεγχθέντων δεδομένων και στη συνέχεια αποστέλλει το μήνυμα στους γειτονικούς κόμβους. Όταν τα δεδομένα φτάσουν στον προορισμό τους, η δεξαμενή ενισχύει τη διαδρομή ανακοινώνοντας στους ενδιάμεσους κόμβους ότι βρίσκονται στην κατάλληλη διαδρομή. Συνήθως αυτή η ενίσχυση γίνεται μικραίνοντας τον χρόνο αποστολής των δεδομένων (interval) ενός κόμβου ώστε να λαμβάνει δεδομένα υψηλότερης ποιότητας. Κάθε ενδιάμεσος κόμβος το ανακοινώνει στον γειτονικό του, από τον οποίο παρέλαβε τα δεδομένα. Αυτή η προώθηση σταματάει όταν φτάσει στον κόμβο προέλευσης των δεδομένων. Παρατηρούμε ότι το πρωτόκολλο έχει ορισμένα χαρακτηριστικά. Πρώτον, όπως αναφέραμε και αρχικά, έχει ως κέντρο τα δεδομένα. Όλα τα δίκτυα που χρησιμοποιούν το πρωτόκολλο χρησιμοποιούν ενδιαφέροντα (interests) για να καθορίσουν τα δεδομένα. Δεύτερον, δεν υπάρχουν δρομολογητές σε ένα δίκτυο αισθητήρων. Κάθε κόμβος μπορεί να ερμηνεύσει τα δεδομένα και τα μηνύματα και έτσι τα δίκτυά μας έχουν συγκεκριμένες αποστολές. Τρίτον, οι αισθητήρες δεν χρειάζεται να έχουν μοναδικές ταυτότητες ή μοναδικές διευθύνσεις. Οι κόμβοι όμως χρειάζεται να ξεχωρίζουν από τους γειτονικούς τους. Τέλος, τα δίκτυα WSN μπορούν να εκτελούν συντονισμένες ενέργειες όταν βρίσκονται στην περιοχή ενδιαφέροντος.

Το πρωτόκολλο D.D. διαφέρει από τις άλλες τεχνικές δρομολόγησης των δικτύων ad hoc σε πολλά σημεία. Πρώτον, χρησιμοποιείται η μέθοδος της πλημμύρας των δεδομένων στο δίκτυο για να βρεθούν πολλαπλές διαδρομές. Δεύτερον, οι ενισχύσεις προσπαθούν να μειώσουν τις πολλαπλές διαδρομές ώστε να επιτυγχάνεται καλύτερο αποτέλεσμα. Τέλος, χρησιμοποιείται μια μνήμη μηνυμάτων για να αποφευχθεί η δημιουργία βρόχων. Από την αξιολόγηση του πρωτοκόλλου ως προς δύο εξιδανικευμένα σχήματα διασποράς δεδομένων (σχήμα πλημμύρας και

σχήμα πολύ-εκπομπής), προέκυψε ότι επιτυγχάνεται μικρότερη κατανάλωση ενέργειας καθώς επίσης και μικρότερη καθυστέρηση.

Υπάρχουν και άλλα πρωτόκολλα που μπορούν να ενταχθούν σ' αυτή την ομάδα, όπως είναι το *GRAD*. Τα πρωτόκολλα αυτής της ομάδας δεν χρειάζονται πληροφορίες τοποθεσίας αλλά συμμετρικές συνδέσεις μεταξύ των κόμβων. Το κύριο πρόβλημα είναι ότι παρέχουν ένα μικρό μερίδιο των υπηρεσιών παράδοσης των δεδομένων μόνο για τη μετάδοση από άλλους προς τους κόμβους με μηδενικό άνυσμα.

γ. Cluster based

Σ' αυτή την κατηγορία πρωτοκόλλων δημιουργούνται ομάδες (clusters) κόμβων και εκλέγονται αρχηγοί ομάδων (cluster-heads). Κατά τη δρομολόγηση, τα πακέτα στέλνονται πρώτα προς τον αρχηγό της ομάδας και οι αρχηγοί αναλαμβάνουν την ευθύνη να προωθήσουν τα πακέτα προς τη δεξαμενή.

(1). Στο πρωτόκολλο *Cluster-head Gateway Switch Protocol (CGSR),* ο αρχηγός ομάδας επιλέγεται από τον ελάχιστο αριθμό ID ή από την μεγαλύτερη συνδεσιμότητα. Κάθε ομάδα περιέχει έναν αρχηγό ομάδας και όλους τους άμεσους γείτονές του. Έτσι, δύο γειτονικοί αρχηγοί έχουν δύο άλματα απόσταση μεταξύ τους.

(2). Στο πρωτόκολλο *Low Energy Adaptive Clustering Hierarchy (LEACH)* [31], χρησιμοποιείται μια τυχαία αλλαγή των αρχηγών ομάδων (cluster-heads) για να διανείμει το φορτίο ενέργειας μεταξύ των κόμβων του δικτύου. Τα βασικά χαρακτηριστικά του *LEACH* είναι τα παρακάτω:

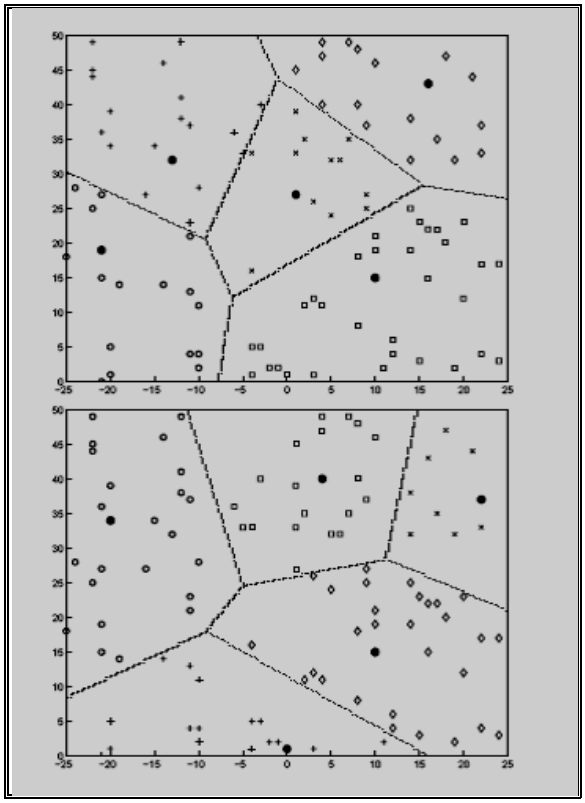
- Τοπική συνεργασία και έλεγχος για τη δημιουργία και λειτουργία ομάδων.
- Τυχαία εναλλαγή των σταθμών βάσεων των ομάδων ή των αρχηγών ομάδων και
- Τοπική συμπίεση δεδομένων για να μειωθεί η επιβάρυνση στην επικοινωνία.

Η χρήση ομάδων για την μετάδοση δεδομένων προς τον σταθμό βάσης δίνει ένα πλεονέκτημα στους κόμβους αισθητήρες, καθώς απαιτούνται μόνο λίγοι κόμβοι που θα μεταδώσουν σε μεγάλες αποστάσεις. Επιπλέον, το *LEACH* ανακατανέμει την ενέργεια που καταναλώνεται από τους αρχηγούς ομάδων και μπορεί να εκτελέσει τοπικούς υπολογισμούς σε κάθε ομάδα για να μειώσει τα δεδομένα που μεταδίδονται προς τον σταθμό βάσης.

Το *LEACH* υποθέτει ότι ο σταθμός βάσης είναι μακριά από τους κόμβους και ότι όλοι οι κόμβοι είναι ομοιογενείς και περιορισμένοι ενεργειακά. Η κύρια εξοικονόμηση ενέργειας προέρχεται από τον συνδυασμό της συμπίεσης δεδομένων και της δρομολόγησης. Έτσι εφαρμόζει περιορισμένες συνεργασίες για να βελτιώσει την κλιμάκωση και την ευρωστία του δικτύου. Επιπλέον, χρησιμοποιεί συγχώνευση δεδομένων για να μειώσει το ποσό της πληροφορίας που μεταδίδεται μεταξύ ενός κόμβου και της δεξαμενής και τέλος, χρησιμοποιεί δυναμικούς μηχανισμούς επιλογής αρχηγών ομάδας για να αποφύγει την μείωση της ενέργειας των κόμβων.

Η τυχαία επιλογή αρχηγών ομάδας γίνεται για να αποφευχθεί ο ενεργειακός θάνατος προκαθορισμένων κόμβων που θα οδηγήσει στην

ανάλωση του χρόνου ζωής των κόμβων που βρίσκονται σε αυτήν την ομάδα (Σχήμα 14).



Σχήμα 14. Δυναμικές ομάδες (clusters)

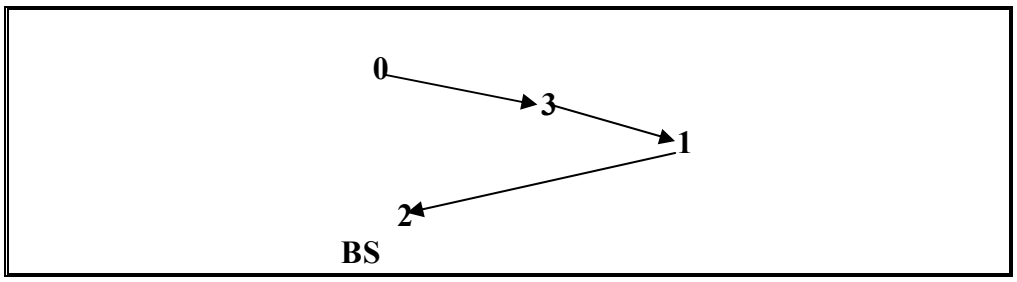
Η επιλογή των αρχηγών ανακοινώνεται σε όλους τους κόμβους της ομάδας. Κάθε κόμβος καθορίζει σε ποια ομάδα θέλει να ανήκει ανάλογα με την ελάχιστη ενέργεια επικοινωνίας. Όταν όλοι οι κόμβοι οργανωθούν σε ομάδες, κάθε αρχηγός ομάδας δημιουργεί ένα σχέδιο με τους κόμβους του δικτύου. Όταν ο αρχηγός ομάδας έχει όλα τα δεδομένα των κόμβων της ομάδας, τα συμπιέζει και τα μεταδίδει στον σταθμό βάσης. Η μετάδοση από λίγους μόνο κόμβους του δικτύου επηρεάζει ενεργειακά μόνο αυτούς τους κόμβους και όχι όλο το δίκτυο.

Το πρωτόκολλο *LEACH* πετυχαίνει σημαντική μείωση στην κατανάλωση ενέργειας σε σχέση με την απευθείας επικοινωνία του κάθε κόμβου με τον σταθμό βάσης. Η παραπάνω εξοικονόμηση ενέργειας οφείλεται στον συνδυασμό της συμπίεσης δεδομένων και της δρομολόγησης. Ένα άλλο πλεονέκτημα του *LEACH* είναι η σχεδόν ταυτόχρονη μείωση του χρόνου ζωής των κόμβων.

(3). Μια βελτιωμένη εκδοχή του *LEACH* είναι το *Power-Efficient Gathering in Sensor Information System (PEGASIS)* [32]. Η βασική ιδέα του πρωτοκόλλου είναι ότι, για να παραταθεί ο χρόνος ζωής του δικτύου, οι κόμβοι χρειάζεται να επικοινωνούν μόνο με τους αμέσως γειτονικούς τους και να εναλλάσσονται στην επικοινωνία τους με τον σταθμό βάσης. Όταν ο γύρος της επικοινωνίας όλων των κόμβων με τον σταθμό βάσης τελειώσει, ξεκινάει ένας νέος γύρος επικοινωνίας και ούτω καθεξής. Αυτή η τεχνική μειώνει την ενέργεια που χρειάζεται για να μεταδοθούν δεδομένα σε κάθε

γύρο, γιατί η εξάντληση ενέργειας διαμοιράζεται εξίσου σε όλους τους κόμβους.

Αρχικά τοποθετούμε τους κόμβους τυχαία στο χώρο. Οι κόμβοι θα οργανωθούν για να δημιουργήσουν αλυσίδες, οι οποίες θα εκτελούνται από τους κόμβους χρησιμοποιώντας έναν «άπληστο» αλγόριθμο (greedy algorithm). Εναλλακτικά, ο σταθμός βάσης μπορεί να υπολογίσει την αλυσίδα και να την μεταδώσει σε όλους τους κόμβους. Σε περίπτωση που ένας κόμβος πεθαίνει, η αλυσίδα αναδιοργανώνεται για να παρακάμψει αυτόν τον νεκρό κόμβο. Για τον σχηματισμό της αλυσίδας, υποθέτουμε ότι όλοι οι κόμβοι γνωρίζουν το δίκτυο και εφαρμόζουν τον αλγόριθμο (Σχήμα 15).



Σχήμα 15. Δημιουργία αλυσίδας.

Για τη συλλογή των δεδομένων σε κάθε γύρο, κάθε κόμβος συλλέγει τα δεδομένα από έναν γείτονά του, τα επεξεργάζεται με τα δικά του και τα μεταδίδει στον επόμενο γείτονα της αλυσίδας. Με την λογική της συγκέντρωσης και επεξεργασίας των δεδομένων σε έναν κόμβο, πετυχαίνουμε την καλύτερη κατανάλωση ενέργειας από το δίκτυό μας. Κάθε κόμβος σε έναν γύρο θα συλλέγει τα δεδομένα από τον προηγούμενό του, θα τα επεξεργάζεται και θα τα στέλνει στον επόμενο μέχρις ότου φτάσουν στον τελευταίο κόμβο πριν τον σταθμό βάσης. Στον επόμενο γύρο επιλέγεται ο επόμενος κόμβος που θα στείλει τα δεδομένα στον σταθμό βάσης. Έτσι, στο πρωτόκολλο *PEGASIS,* κάθε κόμβος θα λάβει και θα μεταδώσει ένα πακέτο σε κάθε γύρο και θα είναι αυτός που θα μεταδώσει προς το σταθμό βάσης μια φορά στους N γύρους (όπου N ο αριθμός των κόμβων του δικτύου).

Το *PEGASIS* είναι βελτιωμένο ως προς το *LEACH* σε πολλούς τομείς. Πρώτα, εξοικονομεί ενέργεια στην τοπική συλλογή δεδομένων και οι αποστάσεις που οι περισσότεροι κόμβοι μεταδίδουν είναι μικρότερες σε σύγκριση με την μετάδοση των αρχηγών ομάδων του *LEACH.* Δεύτερον, το ποσό των δεδομένων που μπορεί να λάβει ο αρχηγός είναι το πολύ δύο μηνύματα σε σχέση με των αριθμό των κόμβων που μπορεί να υπάρχει σε κάθε κόμβο στο *LEACH.* Τέλος, μόνο ο κόμβος μεταδίδει προς τον σταθμό βάσης σε κάθε γύρο επικοινωνίας.

Συμπερασματικά, το *PEGASIS* έχει δύο σκοπούς: (1) να αυξήσει το χρόνο ζωής κάθε κόμβου και επακόλουθα τον χρόνο ζωής του δικτύου και (2) να επιτρέψει μόνο τοπικές συνεργασίες μεταξύ κόμβων, ώστε να μειωθεί η κατανάλωση του εύρους ζώνης.

Υπάρχουν και άλλα πρωτόκολλα σ' αυτή την κατηγορία, όπως είναι τα *Cluster-based topology control (CLTC), DIMENSION, MECN, SMECN.* Τα παραπάνω

πρωτόκολλα είναι ανεξάρτητα από προηγούμενους αλγόριθμους δρομολόγησης. Παρόλα αυτά χρειάζεται επιπλέον προσπάθεια στην επικοινωνία για να διατηρηθεί η αρχιτεκτονική των ομάδων.

3.3.3 Πρωτόκολλα χωρίς ενδείκτη

Στους αλγόριθμους χωρίς ενδείκτη δεν υπάρχει αρχική φάση και τα πακέτα μεταδίδονται με ζήτηση (*on-demand*), ή με τυχαίο τρόπο.

α. On-Demand Μέθοδος

Σ' αυτή την κατηγορία, στέλνονται αιτήσεις για ανεύρεση του δρομολογίου. Το μήνυμα αίτησης περιέχει την πληροφορία του δρομολογίου.

(1). Στο πρωτόκολλο *Ad hoc On-Demand Vector Routing (AODV)* [33], για να σταλεί ένα μήνυμα, ο κόμβος αποστολής των δεδομένων ξεκινά μια διαδικασία εξεύρεσης διαδρομής για να βρει το κατάλληλο δρομολόγιο.

Το *AODV* χρησιμοποιεί συμμετρικές συνδέσεις μεταξύ γειτονικών κόμβων. Δεν προσπαθεί να ακολουθήσει διαδρομές μεταξύ κόμβων που δεν μπορούν να 'ακούσουν' ο ένας τον άλλον. Η βασική ιδέα του πρωτοκόλλου καλείται *σύστημα απόκτησης δρομολογίων με ζήτηση (on-demand route acquisition system)* και αφορά κόμβους που δεν ανήκουν σε ενεργές διαδρομές ή δεν έχουν πληροφορία δρομολόγησης ή δεν συμμετέχουν σε περιοδικές ανταλλαγές πινάκων δρομολόγησης. Επιπλέον, ο κόμβος δεν χρειάζεται να ανακαλύψει ή να διατηρήσει μια διαδρομή προς έναν άλλον κόμβο μέχρι οι δυο τους να χρειαστούν να επικοινωνήσουν, εκτός και αν ένας από τους δύο λειτουργεί σαν ενδιάμεσος κόμβος για την προώθηση ενός μηνύματος. Όταν ένας κόμβος θέλει να επικοινωνήσει ή να κάνει γνωστή την παρουσία του στους γείτονες, μεταδίδει ένα μήνυμα γνωστό ως *hello message*. Οι πίνακες δρομολόγησης των γειτονικών κόμβων οργανώνονται έτσι ώστε να βελτιστοποιήσουν τον χρόνο απάντησης. Οι βασικοί αντικειμενικοί στόχοι του αλγορίθμου είναι οι εξής:

- Η μετάδοση πακέτων ανακάλυψης δρομολογίων μόνο όταν χρειάζεται.
- Ο διαχωρισμός μεταξύ διαχείρισης τοπικής συνδεσιμότητας και διαχείρισης γενικής τοπολογίας.
- Η διασπορά πληροφορίας για τις αλλαγές στην τοπική συνδεσιμότητα σε αυτούς τους γειτονικούς κόμβους που την χρειάζονται.

Το *AODV* χρησιμοποιεί ένα μηχανισμό ανακάλυψης δρομολογίων παρόμοιο με αυτόν που χρησιμοποιείται στο DSR. Όμως το *AODV* στηρίζεται στη δυναμική εγκατάσταση-ανανέωση πινάκων δρομολογίων στους ενδιάμεσους κόμβους. Για να διατηρήσουμε τις πρόσφατες πληροφορίες δρομολόγησης, το *AODV* χρησιμοποιεί την ιδέα τον αριθμών ακολουθίας κόμβου κατεύθυνσης καθώς επίσης και έναν μονοτονικό αύξοντα αριθμό ακολουθίας που χρησιμοποιείται για να αντικαταστήσει παλαιές μνήμες διαδρομών. Ο συνδυασμός αυτών των τεχνικών παράγει έναν αλγόριθμο που χρησιμοποιεί το εύρος ζώνης αποτελεσματικά (ελαχιστοποιώντας το φορτίο του δικτύου για έλεγχο και κίνηση), είναι

υπεύθυνος για τις αλλαγές στην τοπολογία και εξασφαλίζει δρομολόγηση χωρίς τη δημιουργία βρόχων.

Κατά την ανακάλυψη δρομολογίων, ο κόμβος-πηγή μεταδίδει ένα μήνυμα *RREQ* στους γείτονές του. Το μήνυμα περιέχει τα ακόλουθα πεδία:

<source_addr, source_sequence_#, broadcast_id, dest_addr, dest_sequence_#, hop_cnt >

Το ζευγάρι < *source_addr, broadcast_id*> προσδιορίζει μοναδικά το *RREQ.* Κάθε γείτονας ή ικανοποιεί το μήνυμα *RREQ* στέλνοντας μια απάντηση (*RREP)* στην πηγή ή προωθεί το μήνυμα στον γειτονικό κόμβο αυξάνοντας την τιμή *hop_cnt.* Εάν ένας κόμβος δεν μπορεί να ικανοποιήσει το *RREQ,* τότε κρατάει ίχνη των παρακάτω πληροφοριών ώστε να μπορέσει να χρησιμοποιηθεί κατά την αντίθετη διαδρομή:

- Η IP διεύθυνση του προορισμού.
- Η IP διεύθυνση της πηγής.
- Το πεδίο *broadcast _id.*
- Ο χρόνος λήξης της εγγραφής του αντίστροφου δρομολογίου και
- Ο αριθμός ακολουθίας του κόμβου πηγής.

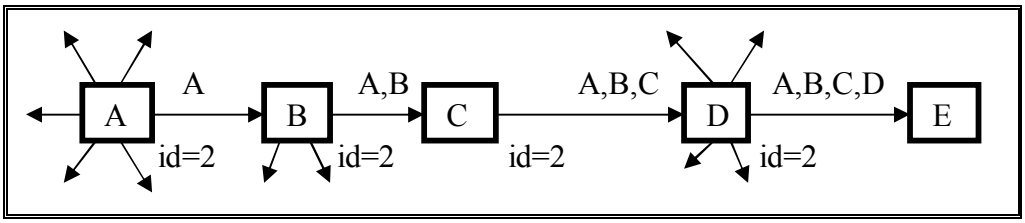
Για τη διατήρηση της πληροφορίας δρομολόγησης στους πίνακες δρομολόγησης, ο κάθε κόμβος διατηρεί διάφορες πληροφορίες από τους ενεργούς κόμβους (ως ενεργός λογίζεται ένας κόμβος για μια διαδρομή εάν έχει δημιουργήσει τουλάχιστον ένα πακέτο μέσα στον πιο πρόσφατο χρόνο *active_timeout)*. Επίσης, για τη διατήρηση των δρομολογίων, ο κάθε κόμβος μπορεί να επανεκκινήσει τη διαδικασία εύρεσης δρομολογίου. Η παραπάνω διαδικασία εκτελείται όταν έχουμε κίνηση ενδιάμεσων κόμβων και σπάσιμο ζεύξεων που δημιουργούν προβλήματα στη δρομολόγηση. Όταν το επόμενο άλμα γίνει απρόσιτο, ο κόμβος που βρίσκεται αντίθετα από την φορά της κίνησης μεταδίδει ένα αυθαίρετο μήνυμα *RREP* με καινούριο αριθμό ακολουθίας (έναν αριθμό ακολουθίας που είναι κατά μία μονάδα μεγαλύτερος από το προηγούμενο γνωστό αριθμό ακολουθίας) προς τους γειτονικούς κόμβους. Οι κόμβοι μεταδίδουν στους γειτονικούς τους και ούτω καθεξής. Αυτή η διαδικασία συνεχίζεται μέχρις ότου όλοι οι ενεργοί κόμβοι επισημανθούν.

Το σύνηθες πρόβλημα που εμφανίζεται στο *AODV* είναι το πρόβλημα του κρυμμένου τερματικού (*hidden terminal problem*). Όταν ο κόμβος *A* μεταδίδει προς τον κόμβο *B* και ο κόμβος *C,* που δεν μπορεί να ακούσει τον *A,* ταυτόχρονα εκπέμψει στον κόμβο *B,* τότε υποθέτουμε ότι τα πακέτα συγκρούονται στον *B* και απορρίπτονται.

(2). Το *Dynamic Source Routing (DSR)*, εξαλείφει την ανάγκη για ύπαρξη συμμετρικών συνδέσεων που υπάρχει στο AODV. Το *DSR* αποτελείται βασικά από δύο μηχανισμούς. Την *ανακάλυψη δρομολογίων (Route Discovery)* και τη *διατήρηση δρομολογίων (Route Maintenance)*. Αυτοί οι δύο μηχανισμοί συνεργάζονται μεταξύ τους για να δημιουργήσουν και να διατηρήσουν δρομολόγια προς τυχαίες κατευθύνσεις σε ένα δίκτυο.

Κατά την *ανακάλυψη δρομολογίων (Route Discovery)* οι κόμβοι δεν γνωρίζουν μια διαδρομή προς έναν κόμβο και θέλουν να στείλουν σε αυτόν ένα πακέτο. Η επικεφαλίδα ενός πακέτου που δημιουργείται από έναν κόμβο *S* και κατευθύνεται προς τον κόμβο *D* περιέχει το δρομολόγιο της πηγής, που δίνει την ακολουθία των αλμάτων την οποία το πακέτο πρέπει

να διασχίσει. Έτσι για παράδειγμα ο κόμβος *A* μεταδίδει ένα μήνυμα *ROUTE REQUEST* που λαμβάνεται από όλους τους κόμβους στην εμβέλειά του (Σχήμα 16).



Σχήμα 16. Ανακάλυψη δρομολογίων στο DSR.

Κάθε μήνυμα *ROUTE REQUEST* καθορίζει τον κόμβο έναρξης και τον κόμβο αποστολής και περιέχει έναν μοναδικό ID αίτησης. Επίσης, περιέχει μια εγγραφή που καταγράφει τη διεύθυνση κάθε ενδιάμεσου κόμβου που πέρασε το μήνυμα. Όταν ο στόχος λαμβάνει το μήνυμα, τότε επιστρέφει ένα μήνυμα *ROUTE REPLY* με ένα αντίγραφο της λίστας των ενδιάμεσων κόμβων που ελήφθει από το *ROUTE REQUEST*. Αυτή η διαδρομή αποθηκεύεται στην μνήμη του κόμβου και χρησιμοποιείται όταν θα σταλούν άλλα πακέτα προς αυτόν τον προορισμό.

Η *διατήρηση δρομολογίων (Route Maintenance)* εκτελείται όταν η διαδρομή έχει σπάσει ή δεν μπορεί να εκτελεστεί ξανά η *ανακάλυψη δρομολογίου* για να βρεθεί νέα διαδρομή. Όταν ένα πακέτο προωθείται από οποιονδήποτε κόμβο, ο κόμβος βεβαιώνεται ότι το πακέτο έχει ληφθεί από τον επόμενο κόμβο στη διαδρομή. Η επιβεβαίωση θα έρθει μόνο αν επανεκπέμψει το πακέτο για κάποιο χρονικό διάστημα. Η επιβεβαίωση γίνεται συνήθως με παθητική επιβεβαίωση ή με την βοήθεια μηχανισμών του επιπέδου ζεύξης. Ο κόμβος, λαμβάνοντας το πακέτο, μπορεί να επιστρέψει μια συγκεκριμένη επιβεβαίωση λογισμικού. Αυτό γίνεται δημιουργώντας ένα bit στην επικεφαλίδα του πακέτου και στη συνέχεια ζητείται μια συγκεκριμένη επιβεβαίωση λογισμικού από τον κόμβο που στέλνει το πακέτο. Όταν ο κόμβος δεν μπορεί να στείλει το πακέτο στον επόμενο, στέλνει ένα μήνυμα *ROUTE ERROR* προς τον αρχικό αποστολέα. Η σπασμένη ζεύξη - στη συνέχεια - απομακρύνεται από την μνήμη του αποστολέα και γίνονται νέες μεταδόσεις του πακέτου μέσω πρωτοκόλλων ανώτερων επιπέδων, όπως το TCP.

Οι σημαντικότερες διαφορές του πρωτοκόλλου *DSR* από το *AODV* αναλύονται παρακάτω. Το πρωτόκολλο *DSR* γνωρίζει την ακριβή διαδρομή άλμα προς άλμα προς τον προορισμό, η οποία και αποθηκεύεται σε μία μνήμη στον κόμβο που δημιουργεί το μήνυμα. Το *AODV* χρησιμοποιεί πίνακες δρομολόγησης και μία είσοδο για κάθε προορισμό για τη διατήρηση της πληροφορίας δρομολόγησης. Τα μηνύματα *ROUTE ERROR* στο *AODV* ενημερώνουν όλους τους κόμβους του δικτύου και όχι τον κόμβο που δημιουργεί ένα συγκεκριμένο δρομολόγιο. Το *DSR* έχει μεγαλύτερη πρόσβαση σε πληροφορία δρομολόγησης από το *AODV* γιατί απαντάει σε όλες τις αιτήσεις που πλησιάζουν έναν προορισμό ενώ το *AODV* απαντάει μόνο σε μια αίτηση. Το βασικότερο μειονέκτημα του *DSR* είναι η υπερβολική κατανάλωση ενέργειας και η χρήση μεγάλου εύρους ζώνης για τη διενέργεια της επικοινωνίας.

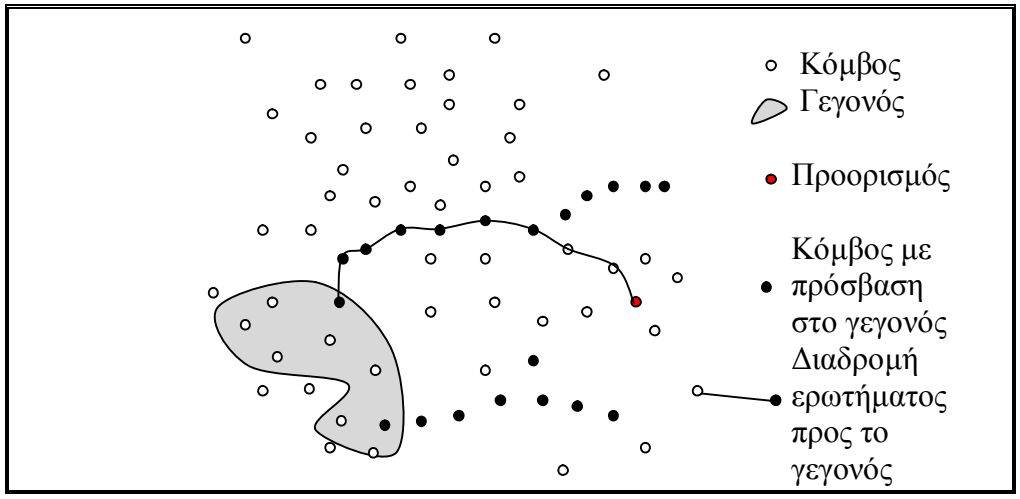
(3). Μια πολύ-διαδρομική έκδοση του AODV είναι το Multipath On-Demand Routing (MOR). Η κύρια συνεισφορά του MOR είναι ότι πολλά μηνύματα REP στέλνονται πίσω αντί ενός. Επομένως, δημιουργούνται πολλαπλές διαδρομές από την πηγή προς τον προορισμό.

Τα πρωτόκολλα αυτής της κατηγορίας είναι αξιόπιστα και ανθεκτικά. Παρόλα αυτά, καταναλώνουν πολύ ενέργεια στις διάφορες διαδρομές.

β. Random Μέθοδος

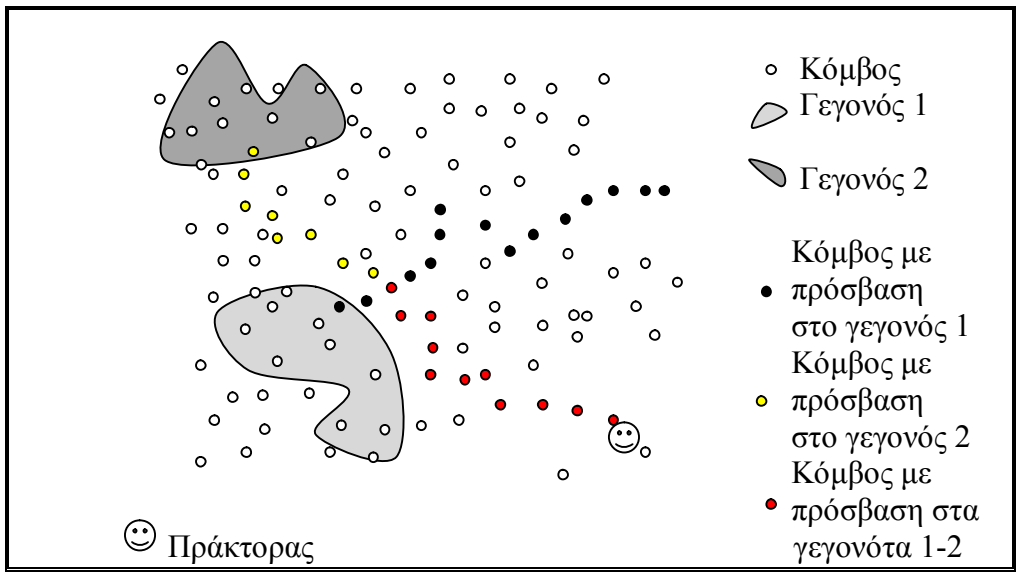
Για μια πιο ευνοϊκή επιλογή διαδρομής, οι αλγόριθμοι αυτής της κατηγορίας χρησιμοποιούν τυχαίους παράγοντες όταν αποφασίζουν για τη διαδρομή που θα ακολουθηθεί.

(1). Στην τεχνική *Rumor routing* [34], η βασική ιδέα είναι να δημιουργηθούν δρομολόγια που οδηγούν σε κάθε γεγονός που λαμβάνει χώρα. Έτσι, όταν ένα ερώτημα παράγεται, μπορεί να σταλεί με τυχαίο τρόπο μέχρι να βρει το δρομολόγιο του γεγονότος, αντί να πλημμυρίσει το ερώτημα σε όλο το δίκτυο (Σχήμα 17).



Σχήμα 17. Ανακάλυψη δρομολογίων στο Rumor Routing.

Μόλις το ερώτημα βρει το δρομολόγιο προς το γεγονός, μπορεί να δρομολογηθεί κατευθείαν σε αυτό. Εάν η διαδρομή δεν βρεθεί, η εφαρμογή μπορεί να προσπαθήσει να ξανά-υποβάλλει το ερώτημα, ή σαν τελευταία λύση να πλημμυρήσει το δίκτυο. Ο αλγόριθμος χρησιμοποιεί ομάδες μακρόβιων πρακτόρων (agents) που δημιουργούν δρομολόγια (σε μορφή κατάστασης στους κόμβους) που κατευθύνονται προς το γεγονός που ελέγχεται. Έτσι, ένας πράκτορας μπορεί να δημιουργήσει δρομολόγια για πολλαπλά γεγονότα σε έναν κόμβο (Σχήμα 18). Επίσης, μπορεί να βελτιστοποιήσει τα δρομολόγια στο δίκτυο αν βρει συντομότερα. Επιπλέον, μπορεί να ανανεώσει τον πίνακα δρομολόγησης ενός κόμβου προς το πιο αποτελεσματικό δρομολόγιο.



Σχήμα 18. Λειτουργία πρακτόρων στο Rumor Routing.

Τα βασικά χαρακτηριστικά του πρωτοκόλλου είναι τα παρακάτω:

- Κάθε κόμβος διατηρεί μια λίστα με τους γείτονές του, όπως επίσης έναν πίνακα γεγονότων, με πληροφορίες προώθησης όλων των γεγονότων που ξέρει.
- Όταν ένας κόμβος παρατηρήσει ένα γεγονός, το προσθέτει στον πίνακα γεγονότων με μηδενική απόσταση. Επίσης δημιουργεί έναν πράκτορα.
- Ο πράκτορας είναι ένα μακρόβιο πακέτο που ταξιδεύει στο δίκτυο, μεταδίδοντας πληροφορίες σχετικά με ένα γεγονός. Αποτελείται από έναν πίνακα γεγονότων, τον οποίο συγχρονίζει με κάθε κόμβο που επισκέπτεται.
- Κάθε κόμβος μπορεί να δημιουργήσει ένα ερώτημα, το οποίο πρέπει να δρομολογηθεί προς ένα γεγονός. Εάν ο κόμβος έχει δρομολόγιο προς το γεγονός, θα μεταδώσει το ερώτημα. Εάν δεν έχει, θα προωθήσει το ερώτημα προς τυχαία κατεύθυνση.
- Εάν ο κόμβος που δημιούργησε το ερώτημα καθορίσει ότι το ερώτημα δεν έφτασε στον στόχο του τότε μπορεί να αναμεταδώσει, εγκαταλείψει ή να πλημμυρήσει το ερώτημα στο δίκτυο.

Η συνολική ενέργεια που καταναλώνεται σε κάθε ερώτημα μπορεί να χρησιμοποιηθεί για να βρεθεί η ολική ενέργεια που χρειάζεται το δίκτυο για να προωθήσει Q ερωτήματα.

$$\boldsymbol{E_t = E_s + Q \times \left(E_q + N \times \frac{1000 - Q_f}{1000} \right)}$$

Παραπάνω, Q_f είναι ο αριθμός των παραδοτέων ερωτημάτων, N ο αριθμός των κόμβων του δικτύου, E_q είναι η ενέργεια που καταναλώνεται για να δρομολογηθούν τα ερωτήματα, Q ο αριθμός των ερωτημάτων και E_s η ενέργεια εγκατάστασης. Συγκρίνοντας την παραπάνω ενέργεια με την ενέργεια που καταναλώνεται σε περίπτωση πλημμύρας μηνυμάτων, παρατηρούμε ότι πετυχαίνουμε καλύτερα αποτελέσματα όταν ο αριθμός των πρακτόρων είναι μικρός και έχουν μεγάλο TTL. Το βασικό

μειονέκτημα το πρωτοκόλλου είναι η αστάθειά του όταν απενεργοποιηθεί μεγάλος αριθμός κόμβων.

(2). Το πρωτόκολλο *ReInForM* αποδεικνύει ότι ο μέσος αριθμός των μη επιτυχημένων διαδρομών μεταξύ δύο κόμβων είναι περίπου ίσος με τον μέσο αριθμό των γειτονικών κόμβων σε ένα δίκτυο αισθητήρων μεγάλης κλίμακας. Όταν η διαδρομή είναι μεγάλη, η διαφορά μεταξύ της κατάλληλης και της χειρότερης είναι μικρή. Έτσι το πρωτόκολλο τυχαία επιλέγει μερικές από τις διαδρομές για να παραδώσει τα δεδομένα ώστε να αυξήσει την πιθανότητα της μετάδοσης.

Το πρωτόκολλο χρησιμοποιεί τοπική γνώση του ρυθμού λαθών και των γειτονικών κόμβων. Αυτό επιτυγχάνεται με μια τεχνική ανάλογη της δυναμικής κατάστασης πακέτων. Τα πακέτα έχουν μικρή συνεισφορά στην λήψη απόφασης της προώθησης σε έναν κόμβο ώστε να παρέχουν την κατάλληλη αξιοπιστία στο δίκτυο. Το πρωτόκολλο δεν χρειάζεται οποιαδήποτε αποθήκευση σε κάποιο κόμβο του δικτύου, γεγονός το οποίο είναι σημαντικό καθόσον οι κόμβοι έχουν περιορισμένη μνήμη.

Το πρωτόκολλο παρέχει αξιοπιστία στην παράδοση πακέτων με οποιοδήποτε ρυθμό λαθών στέλνοντας πολλαπλά αντίγραφα του πακέτου κατά μήκος πολλαπλών διαδρομών. Έτσι στηρίζεται στην ύπαρξη πολλαπλών διαδρομών από την πηγή προς τον κόμβο-δεξαμενή (sink). Μόνο εάν υπάρχει ένας ικανοποιητικός αριθμός διαδρομών από τη πηγή προς τη δεξαμενή, χωρίς μεγάλη απόκλιση των αριθμών των αλμάτων από την βέλτιστη διαδρομή, θα πετύχει η πολύ-διαδρομική προσέγγιση. Όταν ο αριθμός των διαδρομών μεταξύ δύο κόμβων δεν είναι αρκετός για να παρέχει την απαιτούμενη αξιοπιστία, τότε θα υπάρξουν περισσότερα από ένα αντίγραφα σε μια διαδρομή. Η βασική ιδέα είναι να κρατάει το πακέτο μια πληροφορία κατάστασης στην επικεφαλίδα επιτρέποντας το δίκτυο να υπηρετεί το πακέτο με έναν ικανοποιητικό τρόπο ακόμα και αν οι ενδιάμεσοι κόμβοι δεν διατηρούν πληροφορίες κατάστασης του πακέτου.

Με τη δημιουργία ενός πακέτου, η πηγή καθορίζει τη σημαντικότητα της πληροφορίας που περιέχει και καθορίζει μια επιθυμητή αξιοπιστία r_s. Γνωρίζει επίσης τον ρυθμό λαθών e_s του καναλιού και την απόσταση αλμάτων h_s από τη δεξαμενή. Χρησιμοποιώντας αυτές τις τιμές, η πηγή υπολογίζει των αριθμό των διαδρομών P που απαιτούνται για να μεταδώσουμε το πακέτο με την επιθυμητή αξιοπιστία ως εξής:

$$\boldsymbol{P(r_s, e_s, h_s) = \frac{\log(1 - r_s)}{log(1 - (1 - e_s)^{h_s})}}$$

Η πηγή εκπέμπει το πακέτο και προσθέτει ένα πεδίο στην επικεφαλίδα που καλείται DPC (*Dynamic Packet State* field). Οι ενδιάμεσοι κόμβοι του δικτύου, βάσει του παραπάνω πεδίου, μπορούν να λάβουν εύκολα αποφάσεις για την προώθηση των πακέτων. Βάσει επίσης του παραπάνω πεδίου καθορίζεται ποιος κόμβος θα είναι ο επόμενος που θα προωθήσει το πακέτο προς τον κόμβο-δεξαμενή. Τα πακέτα μπορούν να προωθηθούν σε τρεις υποομάδες κόμβων, αυτούς που βρίσκονται σε αποστάσεις h_s*-1,* h_s*,* h_s*+1* πάντα προς την πλευρά της δεξαμενής. Η προώθηση γίνεται πάντα βάσει του παραπάνω τύπου και του επιθυμητού ρυθμού λαθών. Η εργασία της προώθησης των πακέτων κατανέμεται εξίσου στο δίκτυο και δεν συγκεντρώνεται σε μια διαδρομή.

Τα πρωτόκολλα αυτής της κατηγορίας έχουν έλλειψη της σταθερότητας της δρομολόγησης.

3.4 Εφαρμογές δικτύων αισθητήρων

Η ραγδαία ανάπτυξη των μικροηλεκτρονικών συστημάτων και της ασύρματης επικοινωνίας έχει δημιουργήσει φθηνούς αισθητήρες χαμηλής κατανάλωσης. Αυτοί οι αισθητήρες είναι ικανοί να ανιχνεύσουν διάφορες φυσικές πληροφορίες, όπως θερμοκρασία, πίεση, κίνηση κ.ά.. Ένα τυπικό δίκτυο αισθητήρων αποτελείται από εκατοντάδες ως χιλιάδες τέτοιους κόμβους που συνδέονται είτε με ενσύρματο είτε με ασύρματο μέσο (WSN).

Τα δίκτυα αισθητήρων έχουν δημιουργήσει καινούργια παραδείγματα αξιόπιστων παρακολουθήσεων. Τα ασύρματα δίκτυα (WSN) υπερτερούν των ενσύρματων στην χρησιμοποίηση πιο φθηνών αισθητήρων και στην έλλειψη καλωδίωσης. Ορισμένα από τα πλεονεκτήματα των (WSN) παρουσιάζονται παρακάτω:

- *Ανάπτυξη οπουδήποτε και οποτεδήποτε*. Τα ασύρματα δίκτυα περιέχουν κόμβους που δεν χρειάζονται ανθρώπινη παρακολούθηση για τη σωστή λειτουργία τους. Η τοποθέτηση των κόμβων μπορεί να γίνει και στις πιο επικίνδυνες περιοχές, ενώ η αποστολή τους μπορεί να επιτευχθεί σε οποιοδήποτε χρόνο.
- *Μεγαλύτερη αντοχή στα σφάλματα*. Αυτό επιτυγχάνεται με την πυκνή ανάπτυξη του δικτύου WSN. Αν ένα μικρό ποσοστό κόμβων σταματήσει να λειτουργεί, τότε το δίκτυο μπορεί ακόμα να παράγει ικανοποιητικά αποτελέσματα.
- *Βελτιωμένη ακρίβεια*. Ένας μικρός αριθμός μικροσκοπικών κόμβων μπορεί να έχει μεγαλύτερη ακρίβεια από έναν μεγαλύτερο κόμβο.
- *Μικρότερο κόστος*. Λόγω του μικρότερου μεγέθους και της χαμηλότερης τιμής, ένα δίκτυο WSN είναι πιο οικονομικό από τα ενσύρματα δίκτυα αισθητήρων. Ένας άλλος παράγοντας που επηρεάζει την τιμή του δικτύου είναι η ευκολία ανάπτυξής τους.

Τα δίκτυα αισθητήρων μπορούν να ελέγχουν μια μεγάλη ποικιλία φυσικών χαρακτηριστικών, όπως είναι [35]:

- Θερμοκρασία
- Υγρασία
- Φωτεινότητα
- Πίεση
- Κίνηση αντικειμένου
- Σύσταση εδάφους
- Επίπεδο θορύβου
- Παρουσία συγκεκριμένου αντικειμένου
- Χαρακτηριστικά αντικειμένου όπως βάρος, μέγεθος, ταχύτητα, κατεύθυνση κίνησης και την τελευταία θέση.

Οι εφαρμογές των δικτύων αισθητήρων ποικίλουν λόγω των διαφοροποιημένων χαρακτηριστικών που έχουν σε σχέση με τα συμβατά ad hoc δίκτυα. Παρακάτω θα δοθούν χαρακτηριστικά παραδείγματα εφαρμογών δικτύων αισθητήρων.

α. Στρατιωτικές εφαρμογές

Τα δίκτυα αισθητήρων έχουν γίνει αναπόσπαστο κομμάτι των στρατιωτικών επιχειρήσεων στα συστήματα διαταγών, ελέγχου, επικοινωνιών, υπολογισμών, πληροφοριών, επίβλεψης, αναγνώρισης και στόχευσης. Στο πεδίο της μάχης, δημιουργείται μια τάση οι στόχοι να γίνονται μικρότεροι σε μέγεθος, λιγότερο αναγνωρίσιμοι, με μεγαλύτερη ταχύτητα και να κινούνται συνήθως σε πολύ εχθρικό περιβάλλον. Για να μπορέσουμε να γνωρίζουμε την θέση και τη δύναμη των εχθρικών δυνάμεων, μπορούμε να τοποθετήσουμε πυκνές παρατάξεις αισθητήρων κοντά στον υποτιθέμενο στόχο. Λόγω των ικανοτήτων τους να είναι μη ελεγχόμενα από ανθρώπους, της εύκολης ανάπτυξης, της αυτό-οργάνωσης και της αντοχής σε σφάλματα, τα δίκτυα αισθητήρων μπορούν να παρέχουν άφθονα και διασταυρωμένα δεδομένα χωρίς την υποστήριξη φίλιων δυνάμεων. Επίσης, οι αισθητήρες μπορούν να διασπαρθούν με αεροπορικά μέσα, με πυραύλους και τορπίλες ώστε να ξεπεράσουν κάποια εμπόδια και να οδηγηθούν στο ακριβές σημείο ανίχνευσης για την πιο αποτελεσματική εκπλήρωση της αποστολής τους. Η καταστροφή ορισμένων από τους αισθητήρες δεν επηρεάζει τη στρατιωτική επιχείρηση σε τέτοιο βαθμό, λόγω της πυκνής ανάπτυξης και της δυνατότητας αυτό-οργάνωσης. Ορισμένες χαρακτηριστικές εφαρμογές των δικτύων αισθητήρων είναι οι παρακάτω:

- Παρακολούθηση εξοπλισμού και πυρομαχικών των φίλιων δυνάμεων.
- Παρακολούθηση του πεδίου της μάχης.
- Αναγνώριση των εχθρικών δυνάμεων και του εδάφους.
- Κατάδειξη στόχων.
- Εκτίμηση ζημιών.
- Ανίχνευση και αναγνώριση μολυσμένης περιοχής.

β. Περιβαλλοντολογικές εφαρμογές.

Με τη διασπορά χιλιάδων μικροσκοπικών αισθητήρων σε μια γεωγραφική περιοχή, μπορούμε να παρακολουθούμε ή να ελέγχουμε το περιβάλλον. Έτσι μπορούμε να ανιχνεύουμε πλημμύρες, να επιβλέπουμε τον αέρα και την παροχή νερού, να ελέγχουμε τοπικά το κλίμα, να επιβλέπουμε τις καλλιέργειες για πιθανό κίνδυνο καταστροφών, να ανιχνεύουμε πυρκαγιές, να εξερευνούμε για αποθέματα μεταλλευμάτων κ.ά. [36]. Ορισμένα αντιπροσωπευτικά παραδείγματα είναι τα παρακάτω:

- *Έλεγχος οικοσυστήματος*. Τα ιδιαίτερα χαρακτηριστικά των δικτύων αισθητήρων (αυτό-οργάνωση, έλλειψη ελέγχου από τον άνθρωπο, πυκνή ανάπτυξη) επιτρέπουν την χρησιμοποίησή τους στον έλεγχο των οικοσυστημάτων γιατί παρέχουν πληροφορίες σε πολλές περιβαλλοντολογικές καταστάσεις. Εξασφαλίζεται η μακροχρόνια αναγνώριση, καταγραφή και ανάλυση των ενδιαφερόμενων γεγονότων. Η μακροχρόνια συλλογή δεδομένων μπορεί να βοηθήσει τους επιστήμονες να αναγνωρίσουν, εντοπίσουν και ανιχνεύσουν φαινόμενα σε περιοχές ενδιαφέροντος.

- *Έλεγχος κλίματος σε μεγάλα κτηριακά συγκροτήματα.* Η συνεχής δημιουργία όλο και μεγαλύτερων κτηρίων και εγκαταστάσεων (όπως εμπορικών κέντρων, ουρανοξυστών κ.ά.), έχει δημιουργήσει την ανάγκη για καλύτερο έλεγχο του κλίματος στο εσωτερικό τους. Έτσι, μία περιήγηση σε ένα μεγάλο εμπορικό κέντρο μας δείχνει ότι η θερμοκρασία δεν είναι παντού ιδανική, π.χ. αλλού είναι χαμηλή και αλλού υψηλή, αλλού έχει υψηλότερη υγρασία και αλλού όχι. Για αυτούς και για άλλους λόγους υγιεινής πρέπει να εξασφαλίσουμε ένα ευχάριστο χώρο. Η δημιουργία τόσο ενσύρματων όσο και ασύρματων δικτύων σε αυτούς τους χώρους είναι ένας τρόπος ανίχνευσης και αντιμετώπισης των προβλημάτων που αναφέραμε. Συνήθως προτιμάται η ανάπτυξη WSN διότι είναι πιο εύκαμπτα από τα ενσύρματα.
- *Ανίχνευση φωτιάς σε ακαλλιέργητο έδαφος.* Παρόλα τα σημαντικά μέτρα που λαμβάνονται για την ανίχνευση φωτιάς, οι φωτιές σε ακαλλιέργητες και δασικές περιοχές δημιουργούν μεγάλες καταστροφές κάθε χρόνο, τόσο σε άψυχο όσο και έμψυχο υλικό. Επειδή οι καιρικές συνθήκες κατά τη διάρκεια μιας φωτιάς είναι προβλέψιμες, μπορούμε εύκολα να προβλέψουμε την ύπαρξη μιας πυρκαγιάς κατά την περίοδο επικινδυνότητας για φωτιά. Λόγω της τυχαίας και της πυκνής ανάπτυξής τους, τα δίκτυα αισθητήρων είναι μια καλή επιλογή για την ανίχνευση και αναφορά για φωτιά. Διασκορπίζοντας μαζικά δίκτυα αισθητήρων σε επικίνδυνες περιοχές μπορεί να γίνει πιο αποδοτική η ειδοποίηση για φωτιά και η προέλευσή της.

γ. Πρόληψη καταστροφών και παροχή βοήθειας

Τα δίκτυα αισθητήρων μπορούν να είναι αποτελεσματικά σε επείγουσες καταστάσεις και περιοχές καταστροφής [17]. Η ακριβής ανίχνευση μιας περιοχής που εκτελείται από τα δίκτυα αισθητήρων μπορεί να είναι κρίσιμη σε επιχειρήσεις διάσωσης, όπως ανεύρεση θυμάτων, εκτίμηση κινδύνου και αναγνώριση ή εντοπισμός παγιδευμένου προσωπικού. Για παράδειγμα, τα δίκτυα αισθητήρων μπορούν να αναπτυχθούν σε μεγάλα κτίρια κατά την κατασκευή των κτιρίων, να ριχτούν στην περιοχή διάσωσης, ή να χρησιμοποιηθούν ήδη τοποθετημένοι αισθητήρες σε μια περιοχή καταστροφής. Είναι επίσης χρήσιμο να αναπτυχθούν δίκτυα αισθητήρων για αποστολές ανίχνευσης μακράς διάρκειας, όπως ανίχνευση και παρακολούθηση αστοχίας υλικού, ώστε να παρθούν κατάλληλα μέτρα για την αποφυγή ατυχημάτων. Ένα άλλο παράδειγμα είναι η υδατοστεγής υποβρύχιοι αισθητήρες (underwater sensors), οι οποίοι μπορούν να ανιχνεύσουν την τοποθεσία βυθισμένων σκαφών και μπορούν να δώσουν σημαντικές πληροφορίες για τη διάσωση πληρωμάτων. Επίσης οι υποβρύχιοι αισθητήρες μπορούν να αναφέρουν διαρροή πετρελαίου η άλλων τοξικών ουσιών στην θάλασσα από κάποιο παρακείμενο ναυάγιο.

δ. Ιατρική φροντίδα

Τα δίκτυα αισθητήρων είναι χρήσιμα στην παροχή άμεσης και αποτελεσματικής ιατρικής βοήθειας και θα οδηγήσουν σε ένα πιο υγιές περιβάλλον για τον άνθρωπο. Ορισμένες από τις χρήσεις σ' αυτό το πεδίο περιλαμβάνουν:

- *Απομακρυσμένη ανίχνευση ιών*. Πολλές περιοχές, βασανιζόμενες από ασθένειες, είναι φτωχές σε αξιόπιστες τηλεπικοινωνίες. Η ανάπτυξη μεγάλου αριθμού ασύρματων αισθητήρων σε τέτοιες περιοχές, μπορεί να βοηθήσει στη

συλλογή και μετάδοση σημαντικών πληροφοριών, όπως μια ασθένεια και τα χαρακτηριστικά του μολυσμένου πληθυσμού, η αναγνώριση χαρακτηριστικών της περιοχής, ο έλεγχος περιβαλλοντολογικών συνθηκών όπως η υγρασία και το ύψος της βροχής που επιτρέπουν την εξάπλωση ιών και νοσογόνων οργανισμών. Τα δίκτυα αισθητήρων μπορούν να χρησιμοποιηθούν για την πρόβλεψη ξεσπάσματος πολλών μεταδοτικών ασθενειών, όπως είναι η ελονοσία.

- *Ολοκληρωμένη παρακολούθηση ασθενών.* Η χρήση συσκευών αισθητήρων για την ανίχνευση πιθανών μολυσμένων ατόμων μπορεί να είναι μια αποτελεσματική μέθοδος για την αποφυγή εξάπλωσης μεταδοτικών ασθενειών. Επιπλέον, οι γηραιότεροι πολίτες μπορούν να φέρουν ασύρματους αισθητήρες οι οποίοι παρακολουθούν συνεχώς τους χτύπους της καρδιάς, την πίεση κ.ά. Σε αντικανονικές καταστάσεις, ένας προειδοποιητικός ήχος υπενθυμίζει τον ασθενή να ειδοποιήσει τον γιατρό του ή μία αυτόματη υπενθύμιση στέλνεται στο κέντρο υγείας. Επιπλέον τα δίκτυα αισθητήρων μπορούν να χρησιμοποιηθούν για την παρακολούθηση της εύρυθμης λειτουργίας ενός νοσοκομείου ή ενός κέντρου υγείας. Έτσι, αισθητήρες τοποθετούνται σε καίρια σημεία των κτιρίων ώστε να ελέγχουν την παροχή ρεύματος, την παροχή οξυγόνου, την θερμοκρασία δωματίων κ.ά.

ε. Οικιακές εφαρμογές

Τα δίκτυα αισθητήρων μπορούν να παίξουν σημαντικό ρόλο στη δημιουργία ενός πιο βολικού και έξυπνου χώρου διαμονής για τον άνθρωπο. Ορισμένες χρήσιμες εφαρμογές δίδονται παρακάτω:

- *Καταμέτρηση αγαθών από απόσταση*: Τα δίκτυα αισθητήρων μπορούν να χρησιμοποιηθούν στην καταμέτρηση εξ' αποστάσεως των αγαθών γενικής χρήσης (όπως το νερό, ο ηλεκτρισμός κ.ά.) και στη συνέχεια να μεταδώσουν τα αποτελέσματα μέσω ασύρματων συνδέσεων [17]. Ένα απλό παράδειγμα αυτής της χρήσης είναι η τοποθέτηση ασύρματων αισθητήρων στα παρκόμετρα που θα ειδοποιούν τους χρήστες τους για την λήξη του χρόνου παρκαρίσματος.
- *Έξυπνος χώρος*: Με τις σύγχρονες τεχνολογικές ανακαλύψεις, γίνεται δυνατή η ενσωμάτωση διάφορων ασύρματων αισθητήρων σε έπιπλα και οικιακές συσκευές, οι οποίοι να συνεργάζονται μεταξύ τους και να δημιουργούν ένα αυτόνομο δίκτυο. Για παράδειγμα, ένα έξυπνο ψυγείο μπορεί δημιουργήσει ένα μενού ανάλογα με τα υπάρχοντα αγαθά που υπάρχουν και να μεταδώσει τις σχετικές παραμέτρους ψησίματος σε ένα έξυπνο φούρνο ο οποίος θα επιλέξει την κατάλληλη θερμοκρασία και τον χρόνο ψησίματος.

στ. Επιστημονικές εξερευνήσεις

Η αποτελεσματική ανάπτυξη και λειτουργία των αυτορρυθμιζόμενων δικτύων αισθητήρων ανοίγει νέους ορίζοντες στην εξερεύνηση σε ψηλότερα αλλά και χαμηλότερα περιβάλλοντα όπως το διάστημα και οι αβαθείς ωκεανοί. Έτσι η εξερεύνηση των ωκεανών μπορεί να γίνει εύκολη με διασπορά αισθητήρων σε μεγάλα βάθη οι οποίοι θα συλλέγουν πληροφορίες και θα τις μεταδίδουν στον απομακρυσμένο σταθμό βάσης.

ζ. Αλληλεπίδραση με το περιβάλλον

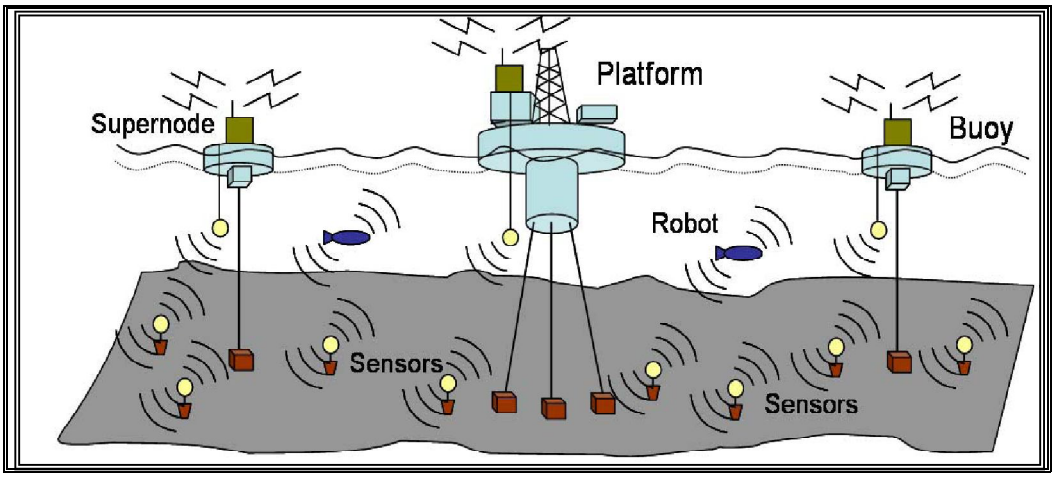
Τα δίκτυα αισθητήρων μπορούν να δώσουν χρήσιμες πληροφορίες για μεταλλεύματα που βρίσκονται σε μεγάλα βάθη του γήινου φλοιού και να τις μεταδώσει στον φυσικό κόσμο. Αναπτύσσοντας φθηνές και μικροσκοπικές συσκευές αισθητήρων, ελεγκτών κίνησης σε παιχνίδια και άλλα παιδικά αντικείμενα μπορούμε να δημιουργήσουμε έξυπνα νηπιαγωγεία για να προάγουμε την παιδική ανάπτυξη. Αυτά τα συστήματα παρέχουν ένα περιβάλλον με αλληλεπίδραση ατόμου-φυσικού κόσμου και όχι των κλασικών ατόμου-ατόμου ή ατόμου-υπολογιστή. Αυτό γιατί επιτρέπει προσωπική αντίληψη για κάθε παιδί, προσαρμογή στη δυναμική για τις δραστηριότητες των παιδιών και μόνιμη και διακριτική συλλογή πληροφοριών για τις ενέργειες των παιδιών. Επίσης, τα δίκτυα αισθητήρων μπορούν να χρησιμοποιηθούν για τη δημιουργία αλληλεπιδρώντων μουσείων. Τα παιδιά μπορούν να συμμετέχουν ενεργά στα πειράματα και να λαμβάνουν απαντήσεις με το άγγιγμα ενός αντικειμένου που είναι εφοδιασμένο με αισθητήρες. Τέλος, μία ακόμα εφαρμογή των δικτύων αισθητήρων είναι η χρήση τους ως πλατφόρμες ψηφοφορίας [37].

η. Επίβλεψη

Η άμεση και από απόσταση επίβλεψη αποτελεί έναν σημαντικό τομέα όπου έχουν εφαρμογή τα συστήματα αισθητήρων. Για παράδειγμα, ένας μεγάλος αριθμός ακουστικών αισθητήρων μπορεί να χρησιμοποιηθεί για να ανιχνευθούν και να ανακαλυφθούν στόχοι και εισβολείς σ' έναν ορισμένο χώρο ασφαλείας. Τα δίκτυα αισθητήρων μπορούν να αναπτυχθούν σε μεγάλα κτίρια, κατοικημένες περιοχές, αεροδρόμια, σιδηροδρομικούς σταθμούς κ.α. για να ανιχνεύουν εισβολείς και να αναφέρουν στο κέντρο ελέγχου άμεσα ώστε η ανακάλυψη τους να γίνει γρήγορα. Παρόμοια, η ανάπτυξη αισθητήρων καπνού σε στρατηγικά επιλεγμένες θέσεις των σπιτιών, γραφείων ή εργοστασίων είναι σημαντική στην πρόληψη κατά των πυρκαγιών και στην ανίχνευση της εξάπλωσης μιας πυρκαγιάς.

θ. Underwater sensors networks

Τα υποβρύχια δίκτυα αισθητήρων (Σχήμα 19) είναι μια νέα εφαρμογή των δικτύων αισθητήρων τα οποία χρήζουν ιδιαίτερης μελέτης. Συνήθως χρησιμοποιούνται για στρατιωτικές και επιστημονικές εφαρμογές. Αποτελούνται από μεταβλητό αριθμό αισθητήρων και οχημάτων που αναπτύσσονται για να εκτελέσουν αποστολές ανίχνευσης κίνησης σε μια δεδομένη περιοχή του βυθού [38]. Ο master node είναι υπεύθυνος για τη συλλογή των δεδομένων, μεταφορά τους στο κέντρο ελέγχου στην ακτή και για τον έλεγχο των υπολοίπων κόμβων. Η κίνηση του δικτύου αποτελείται από ασύγχρονη μεταφορά δεδομένων, απομακρυσμένη εποπτεία του δικτύου και έλεγχο ωκεανογραφικών αισθητήρων.



Σχήμα 19. Ένα υποθαλάσσιο δίκτυο αισθητήρων

Το κύριο κίνητρο για τη δημιουργία υποβρύχιων δικτύων αισθητήρων είναι η σχετικά εύκολη ανάπτυξη τους λόγω της έλλειψης καλωδίων και της μη παρέμβασης πλοίων στην επίτευξη των στόχων. Υπάρχουν πολλές εφαρμογές των υποβρύχιων συστημάτων, όπως η ανάπτυξη κατάλληλων συστημάτων επιτήρησης, η ανίχνευση υποβρύχιων στόχων και η προώθηση κρίσιμων πληροφοριών. Οι περιβαλλοντολογικές εφαρμογές περιλαμβάνουν ανίχνευση φυσικών ενδείξεων (όπως περιεκτικότητα σε αλάτι, πίεση και θερμοκρασία) και χημικών-βιολογικών ενδείξεων (όπως επίπεδα βακτηρίων, επίπεδα μόλυνσης και επικίνδυνοι βιολογικοί ή χημικοί παράγοντες σε πηγάδια και δεξαμενές). Τα υποβρύχια δίκτυα βρίσκουν επίσης εφαρμογή και στη συλλογή ωκεανογραφικών δεδομένων, στην παρακολούθηση πληθυσμών, στην εκμετάλλευση υπογείων κοιτασμάτων και στην παρεμπόδιση καταστροφών από σεισμική δραστηριότητα ή την εμφάνιση τσουνάμι.

Σε σύγκριση με τα ραδιοφωνικά κύματα, ο ήχος έχει καλύτερα χαρακτηριστικά διάδοσης στο νερό. Έτσι, η χρήση του ήχου είναι πιο βολική για την υποβρύχια επικοινωνία. Γι' αυτό οι υποβρύχιοι αισθητήρες χρησιμοποιούν ακουστικά μόντεμ για την επικοινωνία τους. Μειονεκτήματα αυτής της τεχνολογίας είναι η μεγάλη χρονική καθυστέρηση, η μικρή ταχύτητα μετάδοσης και ο μεγάλος θόρυβος λόγω της υποβρύχιας επικοινωνίας.

ι. Άλλες εφαρμογές

Τα αυτό-οργανωμένα δίκτυα αισθητήρων μπορούν να χρησιμοποιηθούν και σε άλλες εφαρμογές, όπως είναι έλεγχος αυτομάτων μηχανισμών, εγκατάσταση μηχανισμών, αυτόματη ανίχνευση αποθέματος αποθήκης, έλεγχος χημικής διαδικασίας, έλεγχος κυκλοφορίας κ.ά.

ΚΕΦΑΛΑΙΟ 4^{Ο}

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ AD HOC ΚΑΙ ΔΙΚΤΥΩΝ ΑΙΣΘΗΤΗΡΩΝ

4.1 Απαιτήσεις ασφαλείας

Αφού εξετάσαμε αναλυτικά τα δίκτυα ad hoc και sensor στα προηγούμενα κεφάλαια, στη συνέχεια θα αναλύσουμε όλα τα θέματα ασφαλείας που διέπουν τα παραπάνω δίκτυα. Στα παρακάτω κεφάλαια αναπτύσσονται όλα τα θέματα ασφαλείας των δικτύων, όπως είναι οι απαιτήσεις ασφαλείας, τα είδη απειλών και επιθέσεων, η ασφάλεια που παρέχεται στα επίπεδα των συστημάτων, τα μέτρα αντιμετώπισης των απειλών κ.ά. Η ασφάλεια είναι ίσως το σημαντικότερο κομμάτι κατά τη δημιουργία και ανάπτυξη ενός ασύρματου δικτύου. Οι σημαντικότερες απαιτήσεις ασφαλείας αναφέρονται παρακάτω.

4.1.1 Διαθεσιμότητα

Η διαθεσιμότητα εξασφαλίζει την βιωσιμότητα των υπηρεσιών του δικτύου, παρά τις επιθέσεις denial of services (DoS) που δέχεται. Μια DoS επίθεση μπορεί να εκκινήσει σε οποιοδήποτε επίπεδο ενός ad hoc δικτύου. Επίσης, τα συστήματα που εξασφαλίζουν τη διαθεσιμότητα προσπαθούν να καταπολεμήσουν τις επιθέσεις κατανάλωσης ενέργειας, καθώς επίσης την παρεκτροπή των κόμβων και την εγωιστική συμπεριφορά τους κατά την προώθηση μηνυμάτων. Οι παραπάνω απειλές θα παρουσιαστούν στη συνέχεια [6].

Στο φυσικό επίπεδο, ένας αντίπαλος μπορεί να προκαλέσει συνωστισμό (jamming) για να παρέμβει στις επικοινωνίες. Στο επίπεδο δικτύου, μπορεί να διαταραχτεί το πρωτόκολλο προώθησης και να διακοπεί το δίκτυο. Σε ανώτερα επίπεδα μπορούν να ανατραπούν οι αντίστοιχες υπηρεσίες, όπως είναι η υπηρεσία διαχείρισης κλειδιού [39].

4.1.2 Εμπιστευτικότητα

Η εμπιστευτικότητα εξασφαλίζει ότι ορισμένη πληροφορία δεν εκτίθεται σε μη εξουσιοδοτημένες οντότητες. Η μετάδοση ευαίσθητων πληροφοριών, όπως είναι στρατηγικές ή τακτικές στρατιωτικές πληροφορίες, απαιτεί εμπιστευτικότητα. Η διαρροή τέτοιων πληροφοριών σε εχθρούς μπορεί να έχει καταστροφικές συνέπειες. Η πληροφορία δρομολόγησης πρέπει επίσης να μείνει εμπιστευτική σε ορισμένες περιπτώσεις γιατί αυτή μπορεί να είναι πολύτιμη για τον εχθρό ώστε να εξακριβώσει και να προσδιορίσει τους στόχους του στο πεδίο της μάχης.

Η συνήθης τακτική για να κρατηθούν ευαίσθητα δεδομένα ασφαλή είναι η κρυπτογράφηση των δεδομένων με ένα μυστικό κλειδί, το οποίο μόνο οι επίδοξοι λήπτες κατέχουν. Επειδή η κρυπτογράφηση δημόσιου κλειδιού είναι πολύ ενεργοβόρα στα δίκτυα αισθητήρων, τα περισσότερα από τα προτεινόμενα πρωτόκολλα χρησιμοποιούν μεθόδους κρυπτογράφησης συμμετρικού κλειδιού.

4.1.3 Αυθεντικότητα

Η αυθεντικότητα επιτρέπει σ' ένα κόμβο να διασφαλίσει την ταυτότητα του επικοινωνούντα κόμβου. Χωρίς την αυθεντικότητα, ένας αντίπαλος μπορεί να μεταμφιέσει έναν κόμβο και έτσι να κερδίσει μη εξουσιοδοτημένη πρόσβαση σε πηγές του δικτύου, σε ευαίσθητες πληροφορίες και να παρέμβει στις λειτουργίες άλλων κόμβων. Έτσι, η αυθεντικότητα είναι απαραίτητη για πολλούς εκτελεστικούς σκοπούς του προγράμματος, όπως εκ νέου προγραμματισμός του δικτύου, έλεγχος κύκλου ασφαλείας σ' ένα κόμβο κ.ά. Η αυθεντικότητα πληροφορίας επιτρέπει στον δέκτη να επιβεβαιώσει ότι η πληροφορία στάλθηκε τοπικά από τον πραγματικό αποστολέα.

Σε επικοινωνία δύο μερών, η αυθεντικότητα μπορεί να επιτευχθεί με έναν καθαρά συμμετρικό μηχανισμό: Ο αποστολέας και ο λήπτης μοιράζονται ένα μυστικό κλειδί με το οποίο υπολογίζουν έναν κώδικα αυθεντικότητας μηνύματος (message authentication code-MAC) για όλα τα αποστελλόμενα δεδομένα. Όταν ένα μήνυμα με τον σωστό MAC φτάσει, ο λήπτης ξέρει ότι στάλθηκε από τον αποστολέα.

Όμως, κατά την εκπομπή μηνύματος προς πολλούς αποδέκτες, χρειάζονται ισχυρότεροι δεσμοί εμπιστοσύνης. Σε αυτή την περίπτωση, μπορούν να χρησιμοποιηθούν άλλες τεχνικές όπως είναι τα πρωτόκολλα SPINS [40] και LEAP [42].

4.1.4 Μη αποποίηση

Η απαίτηση της μη αποποίησης εξασφαλίζει ότι ο αποστολέας ενός μηνύματος δεν μπορεί να αρνηθεί ότι έχει στείλει το μήνυμα. Η μη αποποίηση είναι χρήσιμη στην επισήμανση και απομόνωση εκτεθειμένων κόμβων. Έτσι, όταν ένας κόμβος Α δέχεται ένα λανθασμένο μήνυμα από έναν κόμβο Β, η μη αποποίηση επιτρέπει στον Α να κατηγορήσει τον Β ότι αυτός έστειλε το μήνυμα και να πείσει τους υπόλοιπους κόμβους του δικτύου ότι ο Β είναι εκτεθειμένος. Οι ψηφιακές υπογραφές μπορεί να είναι μία λύση για την παραπάνω περίπτωση [41].

4.1.5 Ανανέωση-Φρεσκάδα

Η απαίτηση για ανανέωση και φρεσκάδα των δεδομένων δηλώνει ότι οι πληροφορίες και τα μηνύματα που ανταλλάσσονται είναι πρόσφατα και διαβεβαιώνει ότι δεν επαναλαμβάνεται αναμετάδοση παλαιών μηνυμάτων. Σε όλα τα μηνύματα, συνήθως, παρέχεται ένας καταμετρητής χρόνου. Βάσει αυτού του μετρητή μπορούμε

να διασφαλίσουμε ότι ένα μήνυμα είναι φρέσκο. Όταν ανανεώνουμε την πληροφορία, διασφαλίζουμε ότι η πληροφορία αυτή είναι πρόσφατη και έτσι αποτρέπουμε κάποιον εχθρό να ξαναγράψει παλαιά μηνύματα. Ένας κοινός τρόπος αντιμετώπισης απειλών είναι να περιλάβουμε έναν μονοτονικά αυξανόμενο μετρητή με κάθε αποστελλόμενο μήνυμα και να απορρίψουμε μηνύματα με παλαιές τιμές του μετρητή.

Επίσης η ανανέωση μπορεί να αφορά στην ανανέωση του κλειδιού που χρησιμοποιείται για την κρυπτογράφηση των δεδομένων. Στην περίπτωση αυτή, κάθε κλειδί βεβαιωμένης μεθόδου μπορεί να βεβαιώσει ότι το διαμοιραζόμενο κλειδί ανάμεσα στους εμπλεκόμενους είναι καινούργιο (δηλαδή δεν έχει ξαναχρησιμοποιηθεί από τους εμπλεκομένους).

4.1.6 Ακεραιότητα πληροφορίας

Η ακεραιότητα πληροφορίας δηλώνει την γνησιότητα των δεδομένων που στέλνονται μεταξύ εμπλεκομένων. Έτσι, ένα μήνυμα που στέλνεται από έναν κόμβο Α σ' ένα κόμβο Β δεν έχει τροποποιηθεί από έναν κακόβουλο κόμβο Γ κατά τη διάρκεια της μετάδοσης. Ένα μήνυμα μπορεί επίσης να τροποποιηθεί ή να καταστραφεί λόγω εξασθένησης του σήματος. Η υπηρεσία της ακεραιότητας πληροφορίας παρέχεται συχνά από την υπηρεσία της αυθεντικότητας ώστε να εξασφαλιστεί η ασφάλεια του δικτύου. Ένα καλό και ασφαλές σύστημα θα ήταν ικανό να ανιχνεύσει οποιοδήποτε πρόβλημα ακεραιότητας ώστε αν μια παράβαση διαπιστωθεί, τότε άμεσα η υπηρεσία να αναφέρει αυτό το πρόβλημα. Εάν έχει εφαρμοσθεί ένας εύρωστος μηχανισμός εμπιστευτικότητας, η ακεραιότητα πληροφορίας είναι τόσο απλή, όπως η προσθήκη κατατεμαχισμών πριν την κρυπτογράφηση των μηνυμάτων [41].

4.1.7 Επεκτασιμότητα και αυτό-οργάνωση

Συνήθως τα δίκτυα που εξετάζουμε χρειάζονται επέκταση με προσθήκη μεγάλου αριθμού νέων κόμβων. Η ανάγκη αυτή απαιτεί δίκτυα τα οποία να μπορούν να έχουν ιδιότητες επέκτασης, είτε ως προς το ενεργειακό μέρος είτε ως προς το θέμα αναδιοργάνωσης του δικτύου. Ο αριθμός των γειτόνων, οι αποστάσεις μεταξύ τους και η απαιτούμενη ισχύς για την αποστολή μηνυμάτων από έναν κόμβο στον άλλο, πιθανόν να μην είναι γνωστά κατά τη διάρκεια ζωής ενός δικτύου. Έτσι οι κόμβοι στα υπό εξέταση δίκτυα πρέπει να είναι ικανοί να αυτό-οργανώνονται και να επιλέγουν τους κατάλληλους μηχανισμούς που ταιριάζουν σε κάθε περίσταση.

4.1.8 Υποκίνηση συνεργασίας

Εκτός από την ασφαλή αποστολή και λήψη μηνυμάτων, η υποκίνηση της συνεργασίας είναι ένα σημαντικό θέμα ασφαλείας. Λόγω του περιορισμένου αριθμού πηγών του δικτύου, οι συσκευές του δικτύου τείνουν να γίνουν «εγωιστές». Έτσι χρειάζεται ένα είδος υποκίνησης για να παρακινηθεί η συνεργασία στο δίκτυο.

Πολλές μέθοδοι δουλεύουν δίνοντας κίνητρο για επιτυχή συνεργασία, ενώ άλλες τιμωρούν την εγωιστική συμπεριφορά. Αυτό το σχήμα πρέπει να είναι ασφαλές από κακόβουλες επιθέσεις. Διαφορετικά, οι συσκευές του δικτύου θα είναι αρκετά εγωιστικές ώστε να σπαταλούν την ενέργεια του δικτύου.

4.2 Περιορισμοί (limitations) από τις απαιτήσεις ασφαλείας του συστήματος

Τα χαρακτηριστικά των δικτύων που εξετάζουμε, όπως η χαμηλή μνήμη, η χαμηλή ενέργεια και ο μεγάλος αριθμός κόμβων, κάνουν μη πρακτική την χρήση των περισσότερων αλγορίθμων ασφαλείας. Για παράδειγμα, η μνήμη ενός αισθητήρα είναι ανεπαρκής στην αποθήκευση των απαραίτητων μεταβλητών (με μεγάλο μέγεθος για τη διασφάλιση της ασφάλειας) που χρειάζονται στους αλγόριθμους ασύμμετρης κρυπτογράφησης [40].

Υπάρχουν ορισμένα χαρακτηριστικά των δικτύων τα οποία έχουν συγκεκριμένες επιπτώσεις. Παρακάτω παρουσιάζονται αναλυτικά αυτά τα χαρακτηριστικά και οι επιπτώσεις τους στην ασφάλεια.

4.2.1 Έλλειψη υποδομής

Κεντρικοί επεξεργαστές, ειδικευμένο λογισμικό και σταθεροί δρομολογητές είναι αναγκαστικά απόντες. Η έλλειψη τέτοιας υποδομής αποκλείει την ανάπτυξη κεντρικής διοίκησης. Αντίθετα, οι κόμβοι υποστηρίζουν ισόνομες σχέσεις και έτσι οποιοδήποτε σχήμα ασφαλείας στηρίζεται σε κατανεμημένα συνεργατικά σχήματα σε σχέση με τα κεντρικά σχήματα ασφαλείας.

4.2.2 Χρήση ασύρματων συνδέσεων

Η χρήση ασύρματων συνδέσεων καθιστά τα δίκτυα ad hoc και sensor ευαίσθητα σε επιθέσεις. Σε αντίθεση με τα ενσύρματα δίκτυα στα οποία ένας αντίπαλος πρέπει να κερδίσει φυσική πρόσβαση στα καλώδια των δικτύων ή να περάσει διαμέσου αρκετών γραμμών άμυνας στα firewalls και στις πύλες εξόδου (gate-ways), οι επιθέσεις στα ασύρματα δίκτυα μπορούν να έρθουν από όλες τις κατευθύνσεις και να στοχεύσουν οποιοδήποτε κόμβο. Γι' αυτό, τα δίκτυα αυτά δεν θα έχουν μια καθαρή γραμμή άμυνας και κάθε κόμβος πρέπει να είναι προετοιμασμένος για να αμυνθεί στις επιθέσεις. Επιπλέον, το πρωτόκολλο MAC που χρησιμοποιείται στα ad hoc δίκτυα όπως είναι το IEEE 802.11, στηρίζεται σε εμπιστευτική συνεργασία με τους γειτονικούς κόμβους για να εξασφαλίσουν πρόσβαση σε κάποιο κανάλι επικοινωνίας, γεγονός το οποίο οδηγεί σε υψηλό ποσοστό προσβολής.

4.2.3 Πολλαπλά άλματα

Λόγω της έλλειψης κεντρικών δρομολογητών και πυλών εξόδου (gate-ways), οι κόμβοι είναι από μόνοι τους δρομολογητές. Έτσι, τα πακέτα ακολουθούν πολλούς δρομολογητές πριν φτάσουν στον τελικό προορισμό. Λόγω της πιθανής αναξιοπιστίας αυτών των κόμβων, το χαρακτηριστικό αυτό αποτελεί ένα σοβαρό σημείο τρωτότητας των δικτύων.

4.2.4 Αυτονομία κινήσεων κόμβων

Οι ασύρματοι κόμβοι είναι γενικά αυτόνομες μονάδες που είναι ικανές να περιφέρονται ανεξάρτητα. Αυτό σημαίνει ότι η ανίχνευση ενός συγκεκριμένου κόμβου σ' ένα δίκτυο ευρείας κλίμακας δεν μπορεί να γίνει εύκολα.

4.2.5 Αμορφία

Η κινητικότητα των κόμβων και η ασύρματη διασύνδεση επιτρέπει τους κόμβους να εισέρχονται και να φεύγουν από ένα δίκτυο αυθόρμητα και να δημιουργούν συνδέσεις αθέλητα. Έτσι, η τοπολογία του δικτύου δεν είναι σταθερή ως προς το σχήμα και το μέγεθος, αλλά αλλάζει συνεχώς. Για να δημιουργηθεί ένα καλό σύστημα ασφαλείας πρέπει να ληφθεί υπ' όψιν αυτό το χαρακτηριστικό των δικτύων ώστε να επιτραπεί η δημιουργία ασφαλούς σύνδεσης με οποιοδήποτε κόμβο ή άλλη συσκευή εισέρχεται κατά καιρούς στο δίκτυο.

4.2.6 Περιορισμοί ισχύος

Η ενέργεια είναι το μεγαλύτερο εμπόδιο για τις ικανότητες των ad hoc και sensor δικτύων. Όταν ένα ασύρματο δίκτυο αναπτυχθεί, δεν μπορεί εύκολα να αντικατασταθεί (λόγω λειτουργικού κόστους) ή να επαναφορτιστεί (λόγω υψηλού κόστους των συσκευών). Έτσι, η μπαταρία ή οι συσκευές παροχής ενέργειας που έχουν μαζί τους οι κόμβοι πρέπει να προφυλάσσονται για να παρατείνουν τον χρόνο ζωής των κόμβων αλλά και του δικτύου. Όταν εφαρμόζεται μια κρυπτογραφική λειτουργία ή ένα πρωτόκολλο σε έναν κόμβο, πρέπει να λαμβάνεται υπ' όψιν η επιπλέον ενεργειακή επιβάρυνση από τον κώδικα ασφαλείας. Όταν θέλουμε να εφαρμόσουμε ένα σύστημα ασφαλείας, μας ενδιαφέρει να μην μειώνεται ο μέγιστος χρόνος ζωής των κόμβων (η ζωή της μπαταρίας) από το σύστημα.

Η επιπλέον ενέργεια που καταναλώνεται από τον κόμβο για την ασφάλεια, συνδέεται με τις επεξεργασίες που χρειάζονται για συγκεκριμένες λειτουργίες ασφαλείας (κρυπτογράφηση, αποκρυπτογράφηση, υπογραφή δεδομένων, επαλήθευση υπογραφών), με την αποστολή δεδομένων ασφαλείας (απαιτείται αποστολή αρχικών διανυσμάτων για την κρυπτο- και αποκρυπτο-γράφηση) και με την αποθήκευση των

παραμέτρων ασφαλείας σε ένα ασφαλές μέσο (αποθήκευση κλειδιού κρυπτογράφησης).

4.2.7 Περιορισμός μνήμης και αποθηκευτικού χώρου

Συνήθως οι κόμβοι των δικτύων ad hoc και sensor είναι μικρές συσκευές με μικρό ποσοστό της αποθηκευτικής μνήμης να καταναλώνεται για κώδικα. Έτσι, για να δημιουργηθεί ένας αποτελεσματικός μηχανισμός ασφαλείας, είναι αναγκαίο να περιοριστεί ο κώδικας του αλγόριθμου ασφαλείας. Για παράδειγμα, ένας κοινός αισθητήριος κόμβος (TelosB) έχει μια 16-bit, 8 MHz RISC CPU με μόνο 10K RAM, 48K μνήμη προγράμματος και 1024K αποθηκευτική μνήμη [43]. Με τέτοιους περιορισμούς, το λογισμικό που δημιουργείται για τους κόμβους πρέπει να είναι μικρό σε μέγεθος. Επίσης, το συνολικό μέγεθος κώδικα TinyOS είναι περίπου 4K και ο προγραμματιστής πυρήνα κατέχει μόνο 178 bytes. Επομένως, το μέγεθος του κώδικα για όλες τις εργασίες ασφαλείας πρέπει να είναι μικρό.

4.2.8 Ασφαλές πρωτόκολλο δρομολόγησης

Η δρομολόγηση και η προώθηση των δεδομένων είναι βασικές λειτουργίες ενός δικτύου για την επικοινωνία. Σε αντίθεση με τα παραδοσιακά δίκτυα όπου η λειτουργία της δρομολόγησης εκτελείται από συγκεκριμένους κόμβους και δρομολογητές, στα εξεταζόμενα δίκτυα η δρομολόγηση εκτελείται από όλους τους κόμβους. Επιπλέον, οι κοινοί μηχανισμοί ασφάλειας κατά τη δρομολόγηση που αποτελείται από την αυθεντικότητα του κόμβου και του μηνύματος, αναφέρονται σε ένα a priori μοντέλο εμπιστοσύνης στο οποίο νόμιμοι δρομολογητές πιστεύεται ότι εκτελούν τις σωστές εργασίες. Όμως η αυθεντικότητα του κόμβου ή των μηνυμάτων του δεν εγγυάται τη σωστή εκτέλεση της δρομολόγησης σε ανοιχτά περιβάλλοντα με έλλειψη εμπιστοσύνης.

Στα περισσότερα πρωτόκολλα δρομολόγησης, οι δρομολογητές ανταλλάσουν πληροφορίες για την τοπολογία του δικτύου για να μπορέσουν να δημιουργήσουν διαδρομές μεταξύ των κόμβων.

Υπάρχουν δύο κύριες απειλές για τα πρωτόκολλα δρομολόγησης. Η πρώτη έρχεται από εξωτερικές επιθέσεις [39]. Εισάγοντας εσφαλμένες πληροφορίες δρομολόγησης, επαναλαμβάνοντας παλιές πληροφορίες δρομολόγησης ή διαστρεβλώνοντας τις πληροφορίες δρομολόγησης, ένας επιτιθέμενος μπορεί άνετα να διχοτομήσει ένα δίκτυο ή να προκαλέσει υπερβολική κίνηση στο δίκτυο που οδηγεί σε αναγκαστική αναμετάδοση ή ανεπαρκή δρομολόγηση. Η δεύτερη και περισσότερο επιβλαβής απειλή έρχεται από εκτεθειμένο κόμβο, ο οποίος μπορεί να προβάλλει λανθασμένες πληροφορίες δρομολόγησης σε άλλους κόμβους. Η ανακάλυψη αυτής της λάθος πληροφόρησης είναι πολύ δύσκολη: η υπογραφή της πληροφορίας δρομολόγησης από κάθε κόμβο δεν είναι αρκετή διότι οι εκτεθειμένοι κόμβοι είναι ικανοί να δημιουργήσουν έγκυρες υπογραφές με τα ιδιωτικά τους κλειδιά.

Για να αμυνθούν κατά του πρώτου είδους απειλών, οι κόμβοι μπορούν να προστατεύσουν την πληροφορία δρομολόγησης με τον ίδιο τρόπο που προστατεύουν τα δεδομένα: μέσω της χρήσης κρυπτογραφικών σχημάτων όπως οι ψηφιακές

υπογραφές. Όμως, αυτή η άμυνα είναι αναποτελεσματική εναντίον επιθέσεων από εκτεθειμένους κόμβους. Η αποκάλυψη εκτεθειμένων κόμβων μέσω της πληροφορίας δρομολόγησης είναι επίσης δύσκολη λόγω της μη σταθερής τοπολογίας του δικτύου: Όταν ένα κομμάτι πληροφορίας είναι άκυρο, η πληροφορία μπορεί να δημιουργήθηκε από έναν εκτεθειμένο κόμβο ή μπορεί να έγινε άκυρη λόγω της αλλαγής της τοπολογίας. Είναι πολύ δύσκολο να ξεχωρίσουμε μεταξύ των δύο περιπτώσεων.

Μπορούμε να χρησιμοποιήσουμε ορισμένες από τις ιδιότητες των δικτύων για να πετύχουμε ασφαλή δρομολόγηση. Είναι γνωστό ότι τα πρωτόκολλα δρομολόγησης πρέπει να χειρίζονται τη ξεπερασμένη (outdated) πληροφόρηση δρομολόγησης για να προσαρμόζουν τη συνεχώς μεταβαλλόμενη τοπολογία. Έτσι, η λάθος πληροφορία δρομολόγησης που παράγεται από εκτεθειμένους κόμβους μπορεί να θεωρηθεί πληροφορία ξεπερασμένη.

Μία άλλη λύση είναι η εύρεση πολλαπλών δρομολογίων ώστε να μην χρειάζεται η δρομολόγηση από τους εκτεθειμένους κόμβους. Αν τα πρωτόκολλα δρομολόγησης μπορούν να βρουν πολλαπλά δρομολόγια, οι κόμβοι μπορούν να προωθήσουν τα δεδομένα τους προς ένα εναλλακτικό δρομολόγιο όταν το βασικό δρομολόγιο έχει αχρηστευτεί.

Μπορεί επίσης να υπάρχει ένα είδος εμπιστευτικής ιεραρχίας μεταξύ των κόμβων [44], ώστε ένα γκρουπ από κακόβουλους κόμβους να μην μπορεί να εκκινήσει μια επίθεση εκβιασμού εναντίον ενός νόμιμου κόμβου, προωθώντας εσφαλμένες πληροφορίες κακής συμπεριφοράς του κόμβου.

Επιπλέον, το ασφαλές πρωτόκολλο πρέπει να είναι προετοιμασμένο να αντιμετωπίσει καταστάσεις στις οποίες ένας κακόβουλος κόμβος εισέρχεται σε ένα μη εκτεθειμένο δρομολόγιο ή καταφέρνει να υπονομεύσει έναν κόμβο σε ένα τέτοιο δρομολόγιο. Σε μια τέτοια περίπτωση, το πρωτόκολλο πρέπει να ξεχωρίσει τους εκτεθειμένους κόμβους και να τους αποκλείει από τους υπάρχοντες ασφαλείς δρόμους.

Τέλος, το πρωτόκολλο πρέπει να μπορεί να διατηρήσει την εμπιστευτικότητα της τοπολογίας δικτύου. Πρέπει να αποτρέπει έναν επιτιθέμενο από το να γνωρίσει ποιοι κόμβοι είναι κρίσιμοι λόγω συνωστισμού ή ποιοι κόμβοι είναι σημαντικοί για την επιτυχή μετάδοση στα υπάρχοντα ασφαλή δρομολόγια. Σε αντίθετη περίπτωση μπορεί να πετύχει μια επίθεση DoS υπονομεύοντας τους σημαντικούς κόμβους του δικτύου.

4.3 Είδη απειλών-επιθέσεων

Αφού εξετάσαμε τα χαρακτηριστικά και τις απαιτήσεις ασφαλείας ενός ασφαλούς δικτύου, είναι καιρός να γνωρίσουμε και τον εχθρό. Η προηγούμενη έρευνα για τα δίκτυα ad hoc και sensor έγινε σε ένα περιβάλλον εμπιστοσύνης. Ωστόσο, τα δίκτυα αυτά τις περισσότερες φορές αναπτύσσονται σε εχθρικά περιβάλλοντα, στα οποία δεν μπορεί να γίνει εύκολα η συντήρηση του δικτύου. Έτσι, πρέπει το δίκτυο να γνωρίζει τις πιθανές απειλές καθώς επίσης και τα αντίμετρα που μπορεί να πάρει για να αποφύγει αυτές τις επιθέσεις, αλλά και αν ένα τμήμα του δικτύου προσβληθεί, να μπορέσει να απομονωθεί από το υπόλοιπο υγειές δίκτυο. Οι απειλές που δέχεται ένας κόμβος του δικτύου μπορούν να χωριστούν σε δύο κλάσεις, στις επιθέσεις και στην κακή συμπεριφορά [6].

Σαν επίθεση λογίζεται οποιαδήποτε πράξη που σκόπιμα προσπαθεί να προκαλέσει οποιαδήποτε ζημιά στο δίκτυο. Μπορούν να χωριστούν ανάλογα με την προέλευση

τους και την φύση τους. Μια κατηγοριοποίηση με βάση την προέλευση χωρίζει τις επιθέσεις σε εξωτερικές και εσωτερικές. Ως εξωτερικές επιθέσεις λογίζονται οι επιθέσεις που ξεκινάνε από κόμβους που δεν ανήκουν στο δίκτυο ή δεν επιτρέπεται η πρόσβαση τους στο δίκτυο. Ως εσωτερικές επιθέσεις θεωρούνται επιθέσεις που ξεκινάνε από εσωτερικούς εκτεθειμένους ή κακόβουλους κόμβους. Αυτή είναι μια πιο σοβαρή απειλή, αφού η προτεινόμενη άμυνα για τις εξωτερικές επιθέσεις είναι άχρηστη εναντίον εσωτερικών εχθρών.

Οι επιθέσεις, όπως είπαμε, ταξινομούνται και ανάλογα με την φύση τους. Έτσι χωρίζονται σε παθητικές και ενεργητικές επιθέσεις. Οι παθητικές επιθέσεις είναι μια συνεχής ροή πληροφοριών από το δίκτυο, η οποία μπορεί να χρησιμοποιηθεί αργότερα σε κάποια ενεργητική επίθεση. Έτσι ο επιτιθέμενος «κρυφακούει» τα πακέτα που στέλνονται και τα αναλύει για να πάρει χρήσιμες πληροφορίες. Λόγω της φύσης του μέσου διάδοσης των ασύρματων επικοινωνιών που είναι ευρέως διαμοιραζόμενο, είναι εύκολο για έναν επιτιθέμενο να εκκινήσει μια τέτοια επίθεση σε αυτό το περιβάλλον, παρά σε ένα κλασικό ενσύρματο περιβάλλον. Το χαρακτηριστικό ασφαλείας που χρειάζεται σε αυτές τις περιπτώσεις είναι η εμπιστευτικότητα πληροφορίας. Οι ενεργητικές επιθέσεις περιλαμβάνουν σχεδόν όλες τις υπόλοιπες επιθέσεις που ξεκινάνε με ενεργή αλληλεπίδραση με το θύμα, όπως είναι: 'βασανιστήριο απώλειας ύπνου' (sleep deprivation torture) το οποίο στοχεύει τις μπαταρίες, 'πειρατεία' (hijacking) στην οποία ο επιτιθέμενος ελέγχει την επικοινωνία μεταξύ δύο οντοτήτων και «μεταμφιέζεται» σε έναν από τους δύο, 'συμφόρηση' (jamming) που προκαλεί μη διαθεσιμότητα του καναλιού λόγω υπερβολικής χρήσης κ.ά. Οι περισσότερες από αυτές τις επιθέσεις προκαλούν μια κατάσταση που είναι γνωστή ως άρνηση υπηρεσίας (Denial of Service-DoS), η οποία είναι ένας υποβιβασμός ή μια ολική απώλεια επικοινωνίας μεταξύ κόμβων.

Ως απειλές κακής συμπεριφοράς ορίζονται αυθαίρετες συμπεριφορές εσωτερικών κόμβων που μπορούν να οδηγήσουν αθέλητα σε καταστροφή άλλων κόμβων. Ο στόχος του κόμβου δεν είναι να επιτεθεί σε έναν άλλο κόμβο, αλλά μπορεί να έχει άλλους στόχους, όπως να αποκτήσει ένα άδικο πλεονέκτημα σε σύγκριση με άλλους κόμβους. Για παράδειγμα, ένας κόμβος μπορεί να μην εκτελέσει σωστά το πρωτόκολλο MAC με σκοπό να λάβει μεγαλύτερο εύρος ζώνης ή μπορεί να αρνηθεί να προωθήσει πακέτα για άλλους για να μην καταναλώσει κομμάτι της ενέργειάς του, ενώ χρησιμοποιεί την ενέργειά του και ζητά από άλλους κόμβους να προωθούν τα δικά του πακέτα.

Κατά την εκτέλεση μιας επίθεσης, οι επιτιθέμενοι έχουν μεγαλύτερη ενέργεια από τους κόμβους του δικτύου. Συνήθως αναγκάζουν τα θύματα να χρησιμοποιούν όλη τους την ενέργεια και τελικά να πεθαίνουν. Έτσι, είναι αναγκαία η άμεση πρόληψη και γνώση μιας απειλής. Παρακάτω περιγράφουμε αναλυτικά τις απειλές που δέχεται ένα δίκτυο. Οι επιθέσεις σε ένα ασύρματο δίκτυο δεν περιορίζονται σε επιθέσεις άρνησης υπηρεσίας αλλά περιλαμβάνουν μια ποικιλία τεχνικών όπως κατάληψη κόμβου, επιθέσεις εναντίον του πρωτόκολλου δρομολόγησης και επιθέσεις στην φυσική ασφάλεια ενός κόμβου.

4.3.1 Επιθέσεις άρνησης υπηρεσίας. (Denial of Service-DoS)

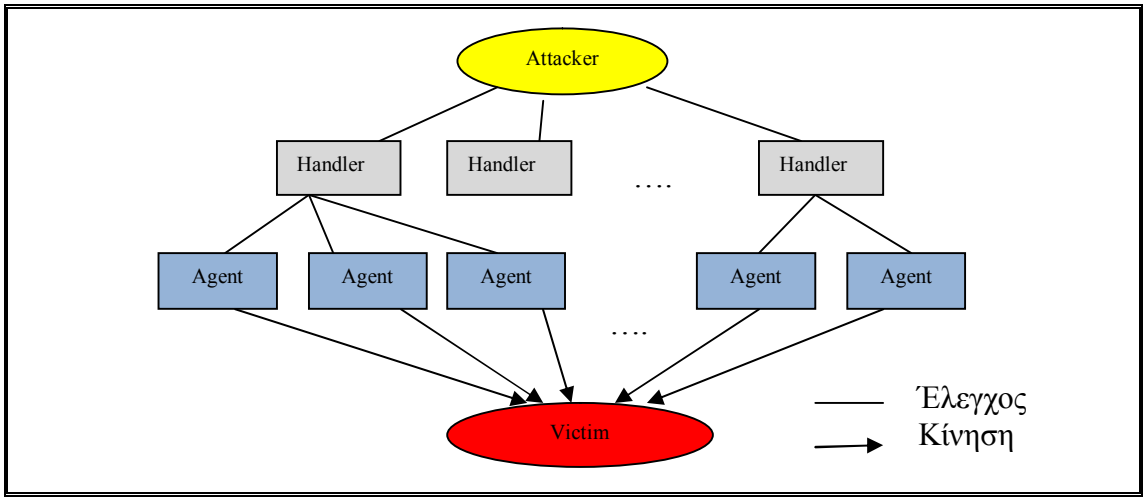
Μια επίθεση άρνησης υπηρεσίας (Denial of Service-DoS) ορίζεται ως οποιοδήποτε γεγονός που μειώνει ή εξαλείφει την ικανότητα ενός δικτύου να εκτελέσει τις αναμενόμενες λειτουργίες [45]. Οι επιθέσεις DoS δεν είναι νέο φαινόμενο. Υπάρχουν

πολλές τεχνικές που χρησιμοποιούνται στην κλασική υπολογιστική και ανταπεξέρχονται σε κάποιες μορφές άρνησης υπηρεσίας. Το πρόβλημα είναι ότι οι περιορισμοί ενέργειας, αποθηκευτικού χώρου και υπολογιστικών ενεργειών των εξεταζόμενων δικτύων εμποδίζουν την εφαρμογή των συνήθων τεχνικών άμυνας.

Ένα μεγαλύτερο μειονέκτημα αυτών των δικτύων είναι η χρήση τους για συγκεκριμένες κρίσιμες και ευαίσθητες εφαρμογές. Για παράδειγμα, ένα δίκτυο αισθητήρων που χρησιμοποιείται για να ειδοποιήσει τους ενοίκους ενός κτηρίου από πυρκαγιά, μπορεί να χτυπηθεί από μια DoS επίθεση, η οποία είναι σε θέση να οδηγήσει σε ανθρώπινες απώλειες λόγω της μη λειτουργίας του δικτύου εντοπισμού πυρκαγιάς. Για αυτούς τους λόγους πρέπει να αναγνωρίσουμε τις διάφορες μορφές DoS επιθέσεων και να βρούμε στρατηγικές για την αντιμετώπισή τους. Οι συνήθεις τακτικές των επιθέσεων DoS είναι οι παρακάτω:

- Προσπάθεια δημιουργίας πλημμύρας στο δίκτυο.
- Προσπάθεια διακοπής σύνδεσης μεταξύ δύο οντοτήτων του δικτύου.
- Προσπάθεια εμποδισμού ενός νέου στο δίκτυο να χρησιμοποιήσει μια υπηρεσία.
- Προσπάθεια διάλυσης μιας υπηρεσίας.

Συνήθως μια επίθεση DoS αποτελείται από τέσσερα κομμάτια (Σχήμα 20): το θύμα, τον υπαίτιο της επίθεσης (attack daemon agent), το πρόγραμμα συντονισμού επίθεσης (control master program) και τον εγκέφαλο της επίθεσης (real attacker).



Σχήμα 20. Αρχιτεκτονική μιας DDOS επίθεσης.

Μια συνήθης επίθεση σε ένα δίκτυο είναι η συμφόρηση (jamming) ενός κόμβου ή μιας ομάδας κόμβων. Η συμφόρηση, σ' αυτή την περίπτωση, είναι η μετάδοση ενός σήματος που παρεμβάλλεται στις συχνότητες που χρησιμοποιούνται από το δίκτυο [45]. Η συμφόρηση σ' ένα δίκτυο μπορεί να έρθει με δύο μορφές: συνεχής και διακοπτόμενη. Η συνεχής συμφόρηση επιφέρει την ολική συμφόρηση του δικτύου. Κανένα μήνυμα δεν μπορεί να σταλεί ή να ληφθεί. Εάν η συμφόρηση είναι μόνο διακοπτόμενη, τότε οι κόμβοι είναι ικανοί να ανταλλάσουν μηνύματα περιοδικά, αλλά όχι μόνιμα. Αυτό μπορεί να έχει μια επιβλαβή επίπτωση στο δίκτυο, καθώς τα μηνύματα που ανταλλάσσονται μεταξύ των κόμβων μπορεί να είναι ευαίσθητα.

Η επίθεση της συμφόρησης, όπως και η επίθεση της πλαστογράφησης *(tampering*), είναι επιθέσεις που εκδηλώνονται στο φυσικό επίπεδο των δικτύων. Η πλαστογράφηση μπορεί να οδηγήσει σε εκτεθειμένους κόμβους οι οποίοι μπορούν να εξάγουν ευαίσθητα δεδομένα (όπως κρυπτογραφικά κλειδιά κ.ά.) για να κερδίσουν μη απεριόριστη πρόσβαση σε υψηλότερα επίπεδα επικοινωνίας.

Οι επιθέσεις μπορούν να κατευθυνθούν και προς το επίπεδο ζεύξης. Έτσι, μια πιθανότητα είναι ο επιτιθέμενος να προσπαθήσει να παραβιάσει το πρωτόκολλο επικοινωνίας και να μεταδίδει συνεχώς μηνύματα σε μια προσπάθεια να προκαλέσει συγκρούσεις (*collisions*). Τέτοιες συγκρούσεις απαιτούν την αναμετάδοση οποιουδήποτε πακέτου επηρεάζεται από αυτές. Ένα αποτέλεσμα των συγκρούσεων είναι η εξάντληση (exhaust) των κόμβων του δικτύου από την ισχύ τους.

Στο επίπεδο δικτύου, οι συνηθέστερες επιθέσεις που μπορούν να δημιουργηθούν είναι η αμέλεια (*neglect),* η επίθεση αποστολής σε λάθος διεύθυνση (misdirection) και οι μαύρες τρύπες (*black holes*) [45]. Στις επιθέσεις αμέλειας ένας κόμβος αυθαίρετα αμελεί να δρομολογήσει ορισμένα μηνύματα. Ο υπονομευμένος ή κακόβουλος κόμβος μπορεί να συμμετέχει σε χαμηλών επιπέδων πρωτόκολλα και μπορεί να γνωρίζει ότι λαμβάνει δεδομένα από έναν άλλο κόμβο αλλά δεν τα αποστέλλει σε τυχαία ή αυθαίρετη βάση. Μια πιο ενεργή μορφή επίθεσης, η αποστολή μηνυμάτων σε λάθος διεύθυνση, προωθεί τα μηνύματα σε λάθος διαδρομές, πιθανόν δημιουργώντας λάθος πληροφορίες δρομολόγησης. Αυτή η επίθεση στοχεύει τον αποστολέα. Σε μια παραλλαγή αυτής της επίθεσης, στις επιθέσεις *smurf* [46], πλαστογραφείται η διεύθυνση του θύματος, ως την πηγή πολλών ICMP μηνυμάτων ηχούς. Στις επιθέσεις μαύρης τρύπας, οι κόμβοι διαφημίζουν μηδενικού κόστους δρομολόγια σε κάθε άλλο κόμβο, δημιουργώντας δρομολόγηση μαύρης τρύπας στο δίκτυο. Όσο η διαφήμισή τους διαδίδεται, το δίκτυο δρομολογεί περισσότερη κίνηση προς την κατεύθυνσή τους. Αυτό προκαλεί έντονη διαμάχη πηγών γύρω από τους κακόβουλους κόμβους, καθώς οι γείτονες συναγωνίζονται για περιορισμένο εύρος ζώνης. Οι γείτονες μπορούν να εξαντληθούν δημιουργώντας μια τρύπα ή ένα χώρισμα στο δίκτυο.

Τέλος, το επίπεδο μεταφοράς είναι ευάλωτο σε επιθέσεις όπως είναι οι πλημμύρες (*flooding*) και ο αποσυγχρονισμός (*desynchronization*). Η πλημμύρα είναι τόσο απλή όσο το να στέλνεις πολλές αιτήσεις σύνδεσης σε έναν ευάλωτο κόμβο [47]. Κάθε αίτηση προκαλεί το θύμα να δεσμεύσει πηγές που διατηρεί γι' αυτήν τη σύνδεση και τελικά την εξάντλησή του από άποψη πηγών. Κατά την επίθεση του αποσυγχρονισμού, ο επιτιθέμενος επανειλημμένα πλαστογραφεί τα μηνύματα των σημείων τερματισμού. Αυτά τα μηνύματα έχουν νούμερα ακολουθίας ή σημαίες ελέγχου που αναγκάζουν τα σημεία τερματισμού να αιτηθούν αναμετάδοση των χαμένων κομματιών.

4.3.2 Η Σιβυλλική επίθεση (Sybil attack)

Η Σιβυλλική επίθεση ορίζεται ως 'μια κακόβουλη συσκευή η οποία προσλαμβάνει πολλαπλές ταυτότητες' [48]. Οι επιπλέον ταυτότητες που προσλαμβάνει η συσκευή ονομάζονται Σιβυλλικοί κόμβοι. Έτσι, ένας κακόβουλος κόμβος συμπεριφέρεται σαν να είναι ένας μεγάλος αριθμός κόμβων, για παράδειγμα μιμούμενος άλλους κόμβους ή παρουσιάζοντας λάθος ταυτότητες. Στην χειρότερη περίπτωση, ο επιτιθέμενος μπορεί να παράγει έναν αυθαίρετο αριθμό επιπλέον κόμβων, χρησιμοποιώντας μόνο μια φυσική συσκευή.

Αρχικά περιγράφηκε ως μια επίθεση που ήταν ικανή να νικήσει τους μηχανισμούς πλεονασμού των κατανεμημένων συστημάτων αποθήκευσης δεδομένων στα peer-to-peer δίκτυα [49]. Επιπλέον της επιβολής έναντι των συστημάτων αποθήκευσης, η Σιβυλλική επίθεση είναι αποτελεσματική έναντι των πρωτόκολλων δρομολόγησης, της συγκέντρωσης δεδομένων, της ψηφοφορίας, της δίκαιης κατανομής πόρων και της αποτροπής εντοπισμού κακής συμπεριφοράς. Ανάλογα με τον στόχο, ο αλγόριθμος της επίθεσης λειτουργεί παρόμοια. Όλες οι τεχνικές προϋποθέτουν χρήση πολλαπλών ταυτοτήτων. Παρακάτω παρουσιάζεται μια ταξινόμηση των Σιβυλλικών επιθέσεων.

- *Άμεση και έμμεση επικοινωνία*: Κατά την άμεση επικοινωνία, οι Σιβυλλικοί κόμβοι επικοινωνούν άμεσα με μια νόμιμη συσκευή. Αντίθετα, κατά την έμμεση επικοινωνία, οι νόμιμοι κόμβοι δεν μπορούν να επικοινωνήσουν άμεσα με τις πολλαπλές οντότητες, αλλά τα μηνύματα στέλνονται μέσω των κακόβουλων συσκευών.
- *Παραγόμενες ή κλεμμένες ταυτότητες*: Οι Σιβυλλικοί κόμβοι μπορούν να πάρουν μία ταυτότητα με δύο τρόπους. Μπορούν να παράγουν μία καινούργια ταυτότητα ή να κλέψουν μία από έναν νόμιμο κόμβο. Μια παραπλήσια επίθεση είναι η αναπαραγωγή ταυτότητας, κατά την οποία η ίδια ταυτότητα χρησιμοποιείται πολλές φορές και υπάρχει σε διαφορετικά σημεία στο δίκτυο.
- *Συγχρονισμός*: Ο επιτιθέμενος μπορεί να προσπαθήσει να συμμετέχουν όλες οι Σιβυλλικές ταυτότητες στο δίκτυο ταυτόχρονα. Εναλλακτικά, ο επιτιθέμενος μπορεί να παρουσιάζει ένα μεγάλο αριθμό ταυτοτήτων για μια περίοδο χρόνου, ενώ ενεργεί με ένα μικρότερο αριθμό ταυτοτήτων σε συγκεκριμένο χρονικό διάστημα. Μια άλλη πιθανότητα είναι ο επιτιθέμενος να έχει πολλές φυσικές συσκευές στο δίκτυο και να ανταλλάσουν μεταξύ τους ταυτότητες.

Τέλος, εξετάζεται πώς η επίθεση χρησιμοποιείται για την προσβολή διάφορων μορφών των πρωτοκόλλων.

- *Κατανεμημένα συστήματα αποθήκευσης*. Η Σιβυλλική επίθεση μπορεί να νικήσει την αναπαραγωγή και τους μηχανισμούς κατακερματισμού στα συστήματα αποθήκευσης peer-to-peer [49]. Το ίδιο πρόβλημα μπορεί να δημιουργηθεί και στα ad hoc και sensor δίκτυα. Ενώ το σύστημα έχει σχεδιασθεί να αναπαράγει και να κατακερματίζει δεδομένα σε διάφορους κόμβους, στην πραγματικότητα αποθηκεύει τα δεδομένα σε Σιβυλλικές οντότητες που παράγονται από κακόβουλους κόμβους.
- *Δρομολόγηση*. Κατά τη δρομολόγηση υπάρχουν πολλά σημεία αδυναμίας ενός πρωτοκόλλου από μία Σιβυλλική επίθεση [50]. Μια αδυναμία είναι η πολύ-διαδρομή ή η δρομολόγηση διασποράς, όπου φαινομενικά μη συνδεόμενες διαδρομές μπορούν να περάσουν από έναν και μόνο κακόβουλο κόμβο που παρουσιάζει πολλές Σιβυλλικές ταυτότητες. Μια άλλη αδυναμία είναι η γεωγραφική δρομολόγηση, όπου αντί να έχει μία ομάδα συντεταγμένων, ένας Σιβυλλικός κόμβος εμφανίζεται σε περισσότερα από ένα σημεία ταυτόχρονα.
- *Συγκέντρωση δεδομένων*. Συνήθως τα αποτελεσματικά πρωτόκολλα συγκεντρώνουν τα διάφορα δεδομένα στο δίκτυο για εξοικονόμηση ενέργειας αντί να κυκλοφορούν διαμοιρασμένα σε όλους τους κόμβους του δικτύου [51]. Χρησιμοποιώντας τη Σιβυλλική επίθεση, ένας κακόβουλος κόμβος μπορεί να συνεισφέρει στη συγκέντρωση πολλές φορές. Με αρκετούς Σιβυλλικούς κόμβους, ένας επιτιθέμενος μπορεί να αλλάξει τα συγκεντρωμένα δεδομένα.

- *Ψηφοφορία*. Η ψηφοφορία χρησιμοποιείται στα δίκτυα σε πολλές περιπτώσεις. Η Σιβυλλική επίθεση μπορεί να χρησιμοποιηθεί για να γεμίσει την κάλπη με τις δικές της «ψήφους». Ανάλογα με τον αριθμό των ταυτοτήτων που έχει ο επιτιθέμενος, μπορεί να καθορίσει το αποτέλεσμα τέτοιων ψηφοφοριών. Για παράδειγμα αυτό μπορεί να χρησιμοποιηθεί για την εκτέλεση επιθέσεων εκβιασμού (*blackmail attacks*), κατά την οποία ο επιτιθέμενος μπορεί να ισχυριστεί ότι ένας κόμβος έχει κακόβουλη συμπεριφορά. Επίσης, εάν υπάρχει ψηφοφορία για την νόμιμη ταυτότητα ενός επιτιθέμενου, ο επιτιθέμενος μπορεί να χρησιμοποιήσει τη Σιβυλλική επίθεση για να επιβεβαιώσει τις ταυτότητές του.
- *Δίκαιη κατανομή πόρων*. Ορισμένες πηγές του δικτύου μπορούν να κατανεμηθούν με βάση τον αριθμό των κόμβων. Για παράδειγμα, γειτονικοί κόμβοι που μοιράζονται ένα μόνο κανάλι συχνότητας, μπορούν να καταλάβουν ένα τμήμα χρόνου στο οποίο μπορούν να μεταδίδουν. Η Σιβυλλική επίθεση μπορεί να χρησιμοποιηθεί για να επιτρέψει σε ένα κακόβουλο κόμβο να αποκτήσει άνιση μοιρασιά, που δίδεται με αυτό τον τρόπο. Αυτό επιτρέπει στον επιτιθέμενο να αποκτήσει επιπλέον πηγές για να εκτελέσει άλλες επιθέσεις.
- *Εντοπισμός κακής συμπεριφοράς*. Ας υποθέσουμε ότι ένα δίκτυο έχει πιθανότητα να ανακαλύψει μια συγκεκριμένη μορφή κακής συμπεριφοράς. Είναι πιθανό να υπάρχουν ορισμένες πιθανότητες αποτυχίας εντοπισμού. Κατά συνέπεια, πιθανόν να μην ληφθούν μέτρα μέχρι να παρατηρηθούν επανειλημμένες προσπάθειες άμυνας από τον ίδιο κόμβο. Ένας επιτιθέμενος με πολλούς Σιβυλλικούς κόμβους μπορεί να εξαπλώσει την αιτία, χωρίς να έχει καμία Σιβυλλική ταυτότητα με κακή συμπεριφορά ικανή να κάνει το δίκτυο να λάβει μέτρα άμυνας. Επιπλέον, αν η δράση που λαμβάνεται είναι για να ανακαλύψει τον επιτιθέμενο κόμβο, ο επιτιθέμενος μπορεί απλά να χρησιμοποιεί Σιβυλλικές ταυτότητες για να μην αποκαλυφθεί ο ίδιος.

Για την αντιμετώπιση των παραπάνω επιθέσεων, πρέπει να τεκμηριώσουμε ότι η ταυτότητα κάθε κόμβου είναι η μοναδική η οποία παρουσιάζεται από τον φυσικό κόμβο.

4.3.3 Επιθέσεις ανάλυσης κίνησης

Τα δίκτυα ad hoc και sensor αποτελούνται από συσκευές μικρής ισχύος που επικοινωνούν με λίγους, εύρωστους και δυνατούς σταθμούς βάσης. Δεν είναι ασυνήθιστο λοιπόν, τα δεδομένα να συγκεντρώνονται από τους ξεχωριστούς κόμβους και να δρομολογούνται στον σταθμό βάσης. Συχνά, ένας επιτιθέμενος για να καταστήσει το δίκτυο άχρηστο, μπορεί να απενεργοποιήσει το σταθμό βάσης. Υπάρχουν δύο μορφές επιθέσεων που μπορούν να «τακτοποιήσουν» το σταθμό βάσης στο δίκτυο με μεγάλη πιθανότητα, χωρίς να χρειάζεται να καταλάβουν το περιεχόμενο των πακέτων [52].

Μια επίθεση καταγραφής του ρυθμού απλά χρησιμοποιεί την ιδέα ότι οι κόμβοι πλησίον των σταθμών βάσεων τείνουν να προωθούν περισσότερα πακέτα από αυτούς που βρίσκονται μακρύτερα από τους σταθμούς βάσης. Ένας επιτιθέμενος χρειάζεται να παρακολουθεί ποιος κόμβος στέλνει πακέτα και να ακολουθήσει αυτούς τους κόμβους που στέλνουν τα περισσότερα πακέτα. Σε μια επίθεση συσχέτισης χρόνου, ένας επιτιθέμενος απλά παράγει γεγονότα και παρακολουθεί σε ποιόν τα στέλνει ένας

οποιοδήποτε κόμβος. Για να δημιουργήσει ένα γεγονός, ο επιτιθέμενος απλά παράγει ένα φυσικό γεγονός που μπορεί να καταγραφεί από τους κόμβους του δικτύου.

4.3.4 Επιθέσεις αναπαραγωγής κόμβου

Μια επίθεση αναπαραγωγής κόμβου είναι πολύ απλή ως έννοια: ένας επιτιθέμενος προσπαθεί να προσθέσει έναν κόμβο στο υπάρχον δίκτυο αντιγράφοντας (αναπαράγοντας) το ID ενός υπάρχοντος κόμβου [53]. Ένας κόμβος που παράγεται με αυτόν τον τρόπο μπορεί να διαταράξει την ομαλή λειτουργία του δικτύου: τα πακέτα μπορεί να αλλοιώνονται ή να οδηγούνται σε λάθος διαδρομή. Αυτό μπορεί να οδηγήσει ένα δίκτυο που δεν συνδέεται ομαλά, να παρέχει λάθος δεδομένα.

Αν ένας επιτιθέμενος κερδίσει φυσική πρόσβαση στο δίκτυο, μπορεί να αντιγράψει τα κρυπτογραφικά κλειδιά και μπορεί να εισάγει αναπαραγόμενους κόμβους σε στρατηγικά σημεία του δικτύου. Εισάγοντας νέους κόμβους σε συγκεκριμένα σημεία, ο επιτιθέμενος μπορεί να ελέγχει ένα συγκεκριμένο κομμάτι του δικτύου και να εκτελεί επιθέσεις στο υπόλοιπο υγιές δίκτυο.

4.3.5 Επιθέσεις εναντίον του απορρήτου

Τα δίκτυα που εξετάζουμε υπόσχονται μια μεγάλη αύξηση στις ικανότητες αυτόματης συλλογής δεδομένων μέσω αποτελεσματικής ανάπτυξης μικρών σε μέγεθος συσκευών. Ενόσω αυτές οι τεχνολογίες προσφέρουν πολλά πλεονεκτήματα στους χρήστες, επιδεικνύουν σημαντικές δυνατότητες για παρενόχληση. Ιδιαίτερα σχετικό ενδιαφέρον παρουσιάζουν τα προβλήματα απορρήτου, εφόσον τα δίκτυα αυτά παρέχουν σημαντικές ικανότητες συλλογής δεδομένων [54]. Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν φαινομενικά ακίνδυνα δεδομένα για να αποκομίσουν ευαίσθητα δεδομένα αν ξέρουν πώς να συσχετίσουν πολλαπλά μηνύματα που καταφθάνουν στους κόμβους.

Το κύριο πρόβλημα απορρήτου δεν είναι ότι τα δίκτυα επιτρέπουν τη συγκέντρωση δεδομένων. Στην πραγματικότητα, πολλές πληροφορίες του δικτύου πιθανόν να συγκεντρώνονται μέσω άμεσης παρακολούθησης ενός γεγονότος. Μάλλον τα δίκτυα επιδεινώνουν το πρόβλημα γιατί κάνουν εύκολα διαθέσιμο μεγάλο όγκο δεδομένων μέσω απομακρυσμένης πρόσβασης. Συνεπώς, οι επιτιθέμενοι δεν χρειάζεται να είναι παρόντες για να διατηρήσουν επαφή. Μπορούν να συγκεντρώνουν δεδομένα με έναν χαμηλού κινδύνου ανώνυμο τρόπο. Η απομακρυσμένη πρόσβαση επιτρέπει σε έναν επιτιθέμενο να παρακολουθεί πολλαπλά σημεία του δικτύου ταυτόχρονα [55]. Οι συνηθέστερες επιθέσεις εναντίον του απορρήτου είναι οι παρακάτω:

- *Παρακολούθηση και κρυφάκουσμα.* Αυτή είναι η πιο προφανής επίθεση κατά του απορρήτου. «Ακούγοντας» τα δεδομένα ο επιτιθέμενος μπορεί εύκολα να ανακαλύψει το περιεχόμενο της επικοινωνίας. Όταν η πληροφορία διαβιβάζει την πληροφορία ελέγχου για τη διάρθρωση του δικτύου (που περιέχει πιο αναλυτικές πληροφορίες από την πρόσβαση στον τοπικό σταθμό βάσης), το κρυφάκουσμα μπορεί να επιδράσει αποτελεσματικά εναντίον του απορρήτου του δικτύου.

- *Ανάλυση κίνησης*. Η ανάλυση κίνησης τυπικά συνδυάζεται με την παραπάνω κατηγορία επίθεσης. Μια αύξηση στον αριθμό των πακέτων που στέλνονται από συγκεκριμένους κόμβους μπορεί να σηματοδοτήσει ότι ένας συγκεκριμένος κόμβος έχει καταχωρημένη δραστηριότητα. Μέσω της ανάλυσης στη κίνηση, ορισμένοι κόμβοι με ειδικό ρόλο ή δραστηριότητα μπορούν να εξακριβωθούν.
- *Παραλλαγή (camouflage)*. Οι επιτιθέμενοι μπορούν να εισάγουν το κόμβο τους ή να «κρύψουν» τους ήδη εκτεθειμένους κόμβους τους μέσα στο δίκτυο. Μετά από αυτό, αυτοί οι κόμβοι μπορούν να μασκαρευτούν σαν κανονικοί κόμβοι για να προσελκύουν πακέτα και στη συνέχεια να τα κατευθύνουν σε λάθος δρόμο ή να προωθήσουν τα πακέτα στους κόμβους που εκτελούν την ανάλυση του απορρήτου.

4.3.6 Φυσικές επιθέσεις

Τα δίκτυα που εξετάζουμε συχνά λειτουργούν σε εχθρικά περιβάλλοντα. Σε τέτοια περιβάλλοντα, το μικρό μέγεθος των κόμβων μαζί με την έλλειψη επιτήρησης και την κατανεμημένη ανάπτυξη του δικτύου, τα κάνουν ευάλωτα σε φυσικές επιθέσεις. Ως φυσικές επιθέσεις θεωρούνται απειλές που επιφέρουν την φυσική καταστροφή των κόμβων [56]. Σε αντίθεση με τις επιθέσεις που αναφέρθηκαν παραπάνω, οι φυσικές επιθέσεις καταστρέφουν τον κόμβο μόνιμα και οι απώλειες είναι μη αναστρέψιμες. Για παράδειγμα, οι επιτιθέμενοι μπορούν να εξάγουν κρυπτογραφικά μυστικά, να σκαλίσουν τη διάταξη των κυκλωμάτων των κόμβων, να τροποποιήσουν τον προγραμματισμό των κόμβων ή να αντικαταστήσουν κόμβους με άλλους κακόβουλους υπό την επίβλεψη του επιτιθέμενου.

Η πρόσφατη έρευνα έχει δείξει ότι οι συνήθεις κόμβοι των κυκλωμάτων μπορούν να καταλειφθούν σε λιγότερο από ένα λεπτό [57]. Μολονότι αυτά τα αποτελέσματα δεν είναι εντυπωσιακά, παρέχουν μια προειδοποίηση για την ταχύτητα καλά εκπαιδευμένων επιτιθέμενων. Εάν ένας επιτιθέμενος καταλάβει έναν κόμβο, τότε ο κώδικας στο εσωτερικό του κόμβου μπορεί να τροποποιηθεί.

4.3.7 Επιθέσεις ‘καταβόθρας’ (Sinkhole attacks)

Σε μια επίθεση ‘καταβόθρας’ ο στόχος του επιτιθέμενου είναι να παρασύρει όλη την κίνηση μιας συγκεκριμένης περιοχής του δικτύου μέσω ενός εκτεθειμένου κόμβου, δημιουργώντας μια μεταφορική καταβόθρα με τον επιτιθέμενο στο κέντρο [50]. Επειδή οι κόμβοι δίπλα ή πάνω στη διαδρομή που ακολουθούν τα πακέτα έχουν μεγάλες δυνατότητες να απασχολούνται με δεδομένα εφαρμογών, οι επιθέσεις καταβόθρας μπορούν να ενεργοποιήσουν και άλλες επιθέσεις (για παράδειγμα επιλεκτική προώθηση).

Οι επιθέσεις καταβόθρας συνήθως δουλεύουν κάνοντας έναν εκτεθειμένο κόμβο να φαίνεται ελκυστικός στους γειτονικούς κόμβους ως προς τον αλγόριθμο δρομολόγησης. Για παράδειγμα, ένας επιτιθέμενος μπορεί να παραπλανήσει ή να επαναλάβει μια ανακοίνωση για ένα εξαιρετικά ποιοτικό δρομολόγιο σε έναν σταθμό βάσης. Ορισμένα πρωτόκολλα πιθανόν να προσπαθήσουν να επιβεβαιώσουν την ποιότητα του δρομολογίου με μια ανταπόδοση από άκρη σε άκρη που να περιέχει

πληροφορία αξιοπιστίας και χρόνου. Σ' αυτή την περίπτωση, ένας επιτιθέμενος με μια ισχυρή κεραία μπορεί να παρέχει υψηλής ποιότητας δρομολόγηση μεταδίδοντας με αρκετή ισχύ για να φτάσει στο σταθμό βάσης με ένα άλμα. Λόγω της αληθινής ή φανταστικής υψηλής ποιότητας της διαδρομής μέσω του εκτεθειμένου κόμβου, είναι πιθανό κάθε γειτονικός κόμβος να προωθεί τα πακέτα που κατευθύνονται στο σταθμό βάσης μέσω του επιτιθέμενου κόμβου και επίσης να διαδίδει την ελκυστικότητα της διαδρομής στους γείτονες. Συνοπτικά, ο επιτιθέμενος δημιουργεί μια σφαίρα επιρροής, ελκύοντας όλη την κυκλοφορία που κατευθύνεται σε έναν σταθμό βάσης, από κόμβους που βρίσκονται πολλά άλματα μακριά από τον εκτεθειμένο κόμβο.

Ένα κίνητρο για τη δημιουργία μιας επίθεσης 'καταβόθρας' είναι ότι κάνει την επιλεκτική προώθηση ασήμαντη. Εξασφαλίζοντας ότι όλη η κίνηση στην περιοχή ενδιαφέροντος ρέει μέσω ενός εκτεθειμένου κόμβου, ένας επιτιθέμενος μπορεί επιλεκτικά να τροποποιήσει ή να απορρίψει πακέτα που προέρχονται από οποιοδήποτε κόμβο του δικτύου.

Πρέπει να επισημανθεί ότι ο λόγος για τον οποίο τα δίκτυα που εξετάζουμε είναι ιδιαίτερα ευάλωτα σε επιθέσεις καταβόθρας είναι η ειδική μορφή επικοινωνίας που έχουν. Επειδή όλα τα πακέτα μοιράζονται τον ίδιο απώτερο προορισμό (σε δίκτυα με έναν σταθμό βάσης), ένας εκτεθειμένος κόμβος χρειάζεται μόνο να παρέχει μία υψηλής ποιότητας διαδρομή στον σταθμό βάσης για να επηρεάσει έναν μεγάλο αριθμό κόμβων.

4.3.8 Σκουληκότρυπες (wormholes)

Σε μια επίθεση 'σκουληκότρυπας' ένας επιτιθέμενος λαμβάνει μηνύματα από ένα σημείο του δικτύου, τα διοχετεύει σε άλλο σημείο του δικτύου και στη συνέχεια τα επαναλαμβάνει στο δίκτυο από αυτό το σημείο [58]. Για αποστάσεις διοχέτευσης μεγαλύτερες από την φυσιολογική εμβέλεια ασύρματης μετάδοσης ενός απλού άλματος, είναι εύκολο για τον επιτιθέμενο να κάνει τα πακέτα να φτάσουν με καλύτερες παραμέτρους από ότι σε μια φυσιολογική δρομολόγηση. Είναι επίσης δυνατό για τον επιτιθέμενο να προωθήσει κάθε bit στη 'σκουληκότρυπα' απευθείας, χωρίς να περιμένει ένα ολόκληρο πακέτο να ληφθεί για να μειώσει τον χρόνο καθυστέρησης που δημιουργείται από τη 'σκουληκότρυπα'. Λόγω της φύσης της ασύρματης μετάδοσης, ο επιτιθέμενος μπορεί να δημιουργήσει μια 'σκουληκότρυπα' ακόμα και για πακέτα που δεν απευθύνονται σ' αυτόν, αφού μπορεί να τα ακούσει κατά την ασύρματη μετάδοση και να τα διοχετεύσει στον συνεργαζόμενο επιτιθέμενο στην άλλη πλευρά της 'σκουληκότρυπας'.

Αν ο επιτιθέμενος εκτελεί αυτήν τη διαδικασία άδολα και αξιόπιστα δεν δημιουργείται κακό. Στην πραγματικότητα, ο επιτιθέμενος παρέχει χρήσιμη υπηρεσία συνδέοντας το δίκτυο πιο αποτελεσματικά. Ωστόσο, η 'σκουληκότρυπα' θέτει τον επιτιθέμενο σε πιο ισχυρή θέση σε σχέση με τους άλλους κόμβους του δικτύου και ο επιτιθέμενος μπορεί να το εκμεταλλευτεί με πολλούς τρόπους. Η επίθεση μπορεί να διαδραματίζεται ακόμα και αν το δίκτυο παρέχει εμπιστευτικότητα και αυθεντικότητα και ακόμα και αν ο επιτιθέμενος δεν έχει κρυπτογραφικά κλειδιά. Επιπλέον, ο επιτιθέμενος είναι «αόρατος» σε υψηλότερα επίπεδα. Αντίθετα με έναν κακόβουλο κόμβο σε ένα πρωτόκολλο δρομολόγησης που μπορεί άνετα να κατονομαστεί, η παρουσία της 'σκουληκότρυπας' και των δύο συνεργαζόμενων επιτιθέμενων σε οποιοδήποτε σημείο αυτής δεν είναι ορατή στη δρομολόγηση.

Ένας επιτιθέμενος που βρίσκεται πλησίον ενός σταθμού βάσης μπορεί να διαταράξει πλήρως τη δρομολόγηση δημιουργώντας μια καλά τοποθετημένη ‘σκουληκότρυπα’. Ο επιτιθέμενος μπορεί να πείσει τους κόμβους που βρίσκονται σε μεγάλη απόσταση από τον σταθμό βάσης ότι βρίσκονται μόνο μερικά άλματα μακριά του. Αυτό μπορεί να δημιουργήσει μια ‘καταβόθρα’: εφόσον ο επιτιθέμενος στην άλλη πλευρά της ‘σκουληκότρυπας’ μπορεί να παρέχει τεχνητά μία υψηλής ποιότητας δρομολόγηση προς τον σταθμό βάσης, όλη η κίνηση της γειτονικής περιοχής θα διεξάγεται αν τα διαφορετικά δρομολόγια δεν είναι τόσο ελκυστικά.

Οι ‘σκουληκότρυπες’ μπορούν να χρησιμοποιηθούν για να πείσουν δύο απομακρυσμένους κόμβους ότι είναι γείτονες αναμεταδίδοντας πακέτα μεταξύ τους. Οι ‘σκουληκότρυπες’ μπορούν να χρησιμοποιηθούν σε συνδυασμό με την επιλεκτική προώθηση και το κρυφάκουσμα. Ο εντοπισμός είναι πολύ δύσκολος αν συνδυαστεί με τη Σιβυλλική επίθεση.

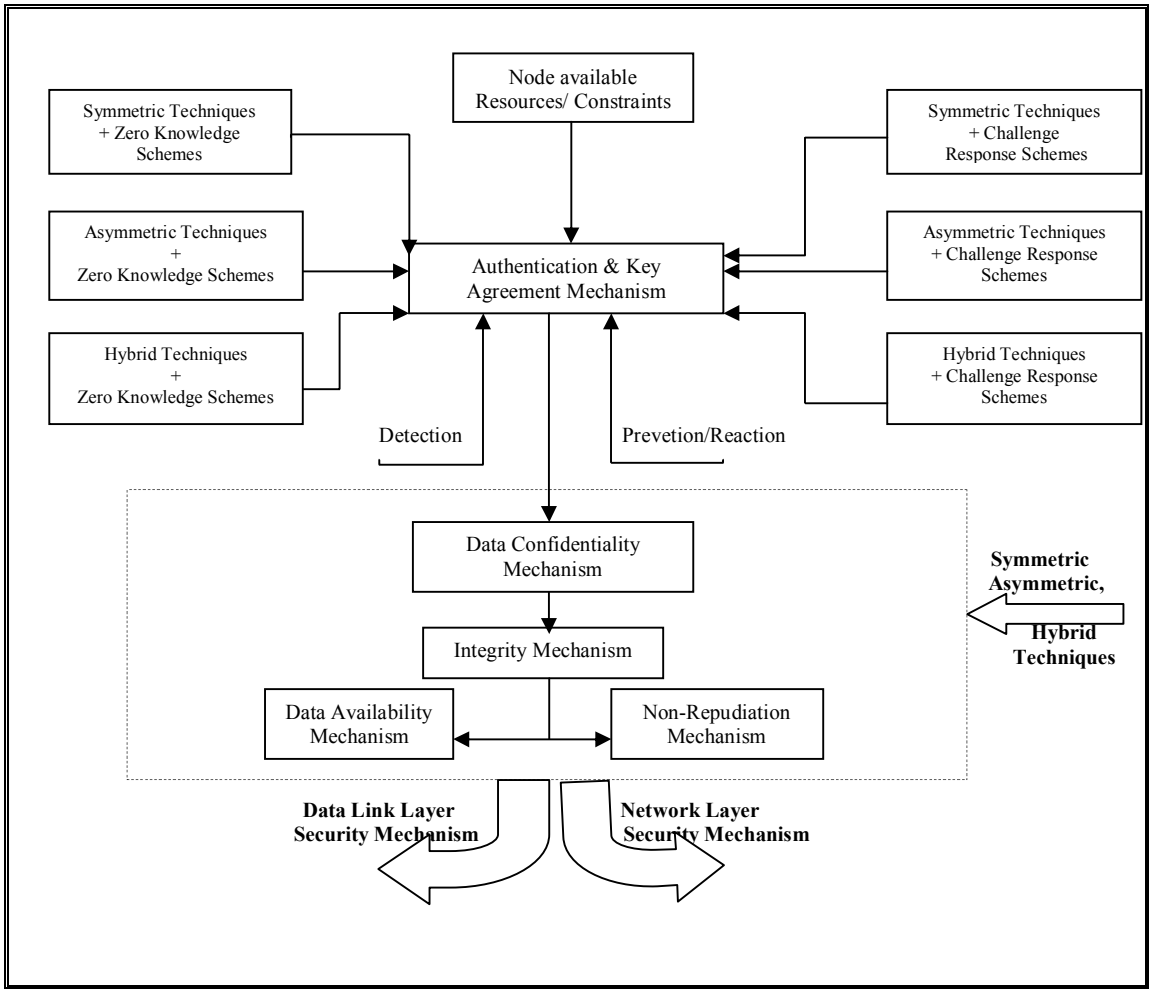
4.3.9 Επιλεκτική προώθηση

Συνήθως τα δίκτυα πολλαπλών αλμάτων στηρίζονται στην υπόθεση ότι οι συμμετέχοντες κόμβοι θα προωθήσουν με συνέπεια τα λαμβανόμενα μηνύματα. Σε μια επίθεση επιλεκτικής προώθησης, κακόβουλοι κόμβοι μπορεί να αρνηθούν να προωθήσουν ορισμένα μηνύματα και απλά να τα αφήσουν, εξασφαλίζοντας ότι δεν θα διαδοθούν παραπέρα [50].

Μια απλή μορφή της επίθεσης είναι όταν ένας κακόβουλος κόμβος συμπεριφέρεται σαν μαύρη τρύπα και αρνείται να προωθήσει κάθε πακέτο που δέχεται. Όμως, ένας τέτοιος επιτιθέμενος, κινδυνεύει να αποκλειστεί από τους γειτονικούς κόμβους και να επιλεγεί κάποια εναλλακτική διαδρομή. Μια πιο επιδέξια μορφή επίθεσης είναι όταν ο επιτιθέμενος επιλεκτικά προωθεί πακέτα. Ένας επιτιθέμενος που ενδιαφέρεται στην μείωση ή την τροποποίηση της κίνησης που δημιουργείται από μια ομάδα κόμβων μπορεί να προωθήσει την υπολειπόμενη κίνηση για να μειώσει την υποψία της επίθεσης.

4.4 Ασφάλεια σε επίπεδα

Οι επιθέσεις που περιγράφηκαν αναλυτικά στο προηγούμενο κεφάλαιο (κεφ. 4.3), προσδιορίζουν τις κρίσιμες απειλές ασφάλειας στα ad-hoc δίκτυα. Οι προκλήσεις ασφάλειας που προκύπτουν στις κύριες διαδικασίες - τις σχετικές με τη δικτύωση ad hoc - βρίσκονται στα επίπεδα ζεύξης δεδομένων και δικτύου [59], και ένα σχετικό πλαίσιο διαδικασιών φαίνεται στο Σχήμα 21.



Σχήμα 21. Πλαίσιο διαδικασιών για την ασφάλεια σε επίπεδα.

4.4.1 Ασφάλεια στο επίπεδο ζεύξης δεδομένων

Το πρότυπο αναφοράς διασύνδεσης ανοικτών συστημάτων (γνωστό ως πρότυπο αναφοράς OSI) αποτελεί μια συνοπτική θεωρητική περιγραφή για τις τηλεπικοινωνίες και το σχεδιασμό πρωτοκόλλου δικτύων υπολογιστών. Το στρώμα ζεύξης δεδομένων είναι το δεύτερο από τα επτά επίπεδα του πρότυπου OSI και είναι εκείνο που εξασφαλίζει ότι τα δεδομένα μεταφέρονται σωστά μεταξύ των παρακείμενων κόμβων δικτύων. Το στρώμα ζεύξης δεδομένων παρέχει τα λειτουργικά και διαδικαστικά μέσα για την μεταφορά των δεδομένων μεταξύ των οντοτήτων δικτύων ενώ παράλληλα ανιχνεύει και ενδεχομένως διορθώνει τα λάθη που μπορεί να εμφανιστούν στο φυσικό στρώμα [60]. Εντούτοις, οι κύριες λειτουργίες του επιπέδου αυτού που σχετίζονται με την ad hoc δικτύωση είναι η συνδεσιμότητα μονού άλματος (one-hop) και η μετάδοση πλαισίων [61]. Τα πρωτόκολλα του επιπέδου ζεύξης δεδομένων διατηρούν τη συνδεσιμότητα μεταξύ γειτονικών κόμβων και εξασφαλίζουν την ορθότητα των πλαισίων που μεταφέρονται.

Είναι ουσιαστικό να διακριθεί η σχέση των μηχανισμών ασφάλειας που εφαρμόζονται στο στρώμα ζεύξης δεδομένων, όσον αφορά στις απαιτήσεις MANET.

Στην περίπτωση των κινητών ad hoc δικτύων, υπάρχουν αξιόπιστα και μη αξιόπιστα περιβάλλοντα. Σε ένα αξιόπιστο περιβάλλον, οι κόμβοι του ad hoc δικτύου ελέγχονται από ένα τρίτο μέρος και μπορούν να καταστούν αξιόπιστοι με βάση την πιστοποίηση (authentication). Η ασφάλεια του στρώματος ζεύξης δεδομένων δικαιολογείται σε αυτήν την περίπτωση από την ανάγκη να καθιερωθεί μια αξιόπιστη υποδομή βασισμένη σε λογικά μέσα ασφάλειας. Εάν μπορεί να εξασφαλισθεί η ακεραιότητα των λειτουργιών υψηλότερων επιπέδων που εφαρμόζονται από τους αξιόπιστους κόμβους, τότε η ασφάλεια του στρώματος ζεύξης δεδομένων μπορεί ακόμη και να καλύψει τις απαιτήσεις ασφάλειας που εγείρονται από υψηλότερα στρώματα συμπεριλαμβανομένων των πρωτοκόλλων δρομολόγησης και εφαρμογής.

Στα μη-αξιόπιστα περιβάλλοντα, η εμπιστοσύνη στα υψηλότερα στρώματα όπως τα πρωτόκολλα δρομολόγησης ή εφαρμογής, δεν μπορεί να βασιστεί στους μηχανισμούς ασφάλειας του στρώματος ζεύξης δεδομένων. Η μόνη σχετική χρήση των τελευταίων εμφανίζεται να είναι η πιστοποίηση κόμβου προς κόμβο και η ακεραιότητα των δεδομένων, όπως απαιτείται από το στρώμα δρομολόγησης. Επιπλέον, ο κύριος περιορισμός στην επέκταση των υπαρχουσών λύσεων ασφάλειας στρώματος ζεύξης δεδομένων είναι η έλλειψη υποστήριξης για την αυτοματοποιημένη διαχείριση κλειδιών, που είναι επιβεβλημένη στα ανοικτά περιβάλλοντα όπου η χειροκίνητη εγκατάσταση κλειδιών δεν είναι κατάλληλη.

Η κύρια απαίτηση για τους μηχανισμούς ασφάλειας του στρώματος ζεύξης δεδομένων είναι η ανάγκη να αντιμετωπιστεί η έλλειψη φυσικής ασφάλειας στα ασύρματα τμήματα της επικοινωνιακής υποδομής. Οι μηχανισμοί στρώματος ζεύξης δεδομένων, όπως αυτοί που παρέχονται από το 802.11 και το *Bluetooth*, χρησιμεύουν βασικά για τις ενισχύσεις ελέγχου και ατομικότητας πρόσβασης ώστε να αντιμετωπιστούν οι ευπάθειες των ράδιο-τηλεπικοινωνιακών ζεύξεων. Εντούτοις, η ασφάλεια ζεύξης δεδομένων που εκτελείται σε κάθε άλμα δεν μπορεί να καλύψει τις από άκρο σε άκρο απαιτήσεις ασφάλειας των εφαρμογών, ούτε στις ασύρματες συνδέσεις που προστατεύονται από το IEEE 802.11 ή το Bluetooth, ούτε στις φυσικά προστατευμένες ενσύρματες συνδέσεις.

Οι πρόσφατες ερευνητικές προσπάθειες έχουν προσδιορίσει τις ευπάθειες στο WEP και υπάρχουν διάφοροι τύποι κρυπτογραφικών επιθέσεων λόγω της κακής χρήσης των αρχών κρυπτογράφησης [62]. Το πρωτόκολλο IEEE 802.11 είναι επίσης ευάλωτο στις επιθέσεις DoS όπου ο αντίπαλος μπορεί να εκμεταλλευτεί το δυαδικό εκθετικό back-off σχήμα του και να αρνηθεί την πρόσβαση στο ασύρματο κανάλι από τους τοπικούς γείτονές του. Επιπλέον, ένας συνεχώς μεταδίδων κόμβος μπορεί πάντα να 'συλλάβει' το κανάλι και να θέσει τους άλλους κόμβους σε μια ατέρμονη back-off κατάσταση, έτσι ώστε να προκαλέσει μια αλυσιδωτή αντίδραση από τα πρωτόκολλα ανωτέρων επιπέδων (π.χ. διαχείριση παραθύρων TCP) [62,63].

Μια άλλη επίθεση DoS ισχύει επίσης στο IEEE 802.11 με τη χρήση του πεδίου NAV, το οποίο δείχνει τη δέσμευση καναλιών και μεταφέρεται στο αίτημα να σταλούν (send) ή να χαθούν (clear) τα πλαίσια RTS/CTS. Ο αντίπαλος μπορεί να 'κρυφακούσει' τις πληροφορίες NAV και έπειτα σκόπιμα να εισάγει ένα λάθος ενός bit στο πλαίσιο του στρώματος ζεύξης του θύματος μέσω ασύρματης παρεμβολής [62,63].

Τα πρωτόκολλα ασφάλειας του στρώματος ζεύξης πρέπει να παρέχουν ασφάλεια μεταξύ ομότιμων (peer to peer), όπου οι ομότιμοι είναι οι άμεσα συνδεδεμένοι κόμβοι και να εξασφαλίσουν τις μεταδόσεις πλαισίων με την αυτοματοποίηση των κρίσιμων διαδικασιών ασφάλειας συμπεριλαμβανομένων της πιστοποίησης κόμβων, της κρυπτογράφησης πλαισίων, της επαλήθευσης ακεραιότητας δεδομένων και της διαθεσιμότητας κόμβων.

4.4.2 Ασφάλεια στο επίπεδο δικτύου

Το στρώμα δικτύου είναι το τρίτο επίπεδο του προτύπου OSI, το οποίο δίνει την κατάλληλη διεύθυνση στα μηνύματα και μεταφράζει τις λογικές διευθύνσεις και τα ονόματα στις φυσικές διευθύνσεις. Καθορίζει επίσης τη διαδρομή από την πηγή στον υπολογιστή προορισμού και διαχειρίζεται τα προβλήματα κυκλοφορίας, όπως η μεταγωγή, η δρομολόγηση και ο έλεγχος συμφόρησης των πακέτων δεδομένων [59].

Οι κύριες λειτουργίες δικτύων, οι σχετικές με την ad hoc δικτύωση, είναι η δρομολόγηση και η αποστολή πακέτων δεδομένων [64,65]. Τα πρωτόκολλα δρομολόγησης ανταλλάσσουν τα δεδομένα δρομολόγησης μεταξύ των κόμβων και διατηρούν τις καταστάσεις δρομολόγησης σε κάθε κόμβο αναλόγως. Με βάση τις καταστάσεις δρομολόγησης, τα πακέτα δεδομένων διαβιβάζονται από τον ενδιάμεσο κόμβο κατά μήκος μιας ορισμένης διαδρομής προς τον προορισμό.

Οι επιτιθέμενοι στα πρωτόκολλα δρομολόγησης μπορούν να εξαγάγουν την κυκλοφορία προς ορισμένους προορισμούς στους συμβιβασμένους (compromised) κόμβους και να προωθήσουν τα πακέτα κατά μήκος μιας διαδρομής που δεν είναι βέλτιστη. Οι αντίπαλοι μπορούν επίσης να δημιουργήσουν βρόχους δρομολόγησης στο δίκτυο και να εισάγουν συμφόρηση δικτύων και ανταγωνισμό καναλιού σε ορισμένες περιοχές.

Εκτός από τις επιθέσεις δρομολόγησης, ο αντίπαλος μπορεί να εκτελέσει επιθέσεις ενάντια στις λειτουργίες προώθησης πακέτου. Τέτοιες επιθέσεις αναγκάζουν τα πακέτα δεδομένων να παραδοθούν με έναν τρόπο που είναι ασυμβίβαστος με τις καταστάσεις δρομολόγησης. Παραδείγματος χάριν, ο επιτιθέμενος κατά μήκος μιας ορισμένης διαδρομής μπορεί να απορρίψει τα πακέτα, να τροποποιήσει το περιεχόμενό τους, ή να αναπαράγει πακέτα που έχουν ήδη προωθηθεί [39]. Το DoS είναι ένας άλλος τύπος επίθεσης που στοχεύει στα πρωτόκολλα προώθησης πακέτων και εισάγει ανταγωνισμό ασύρματου καναλιού και ανταγωνισμό δικτύου στα ad hoc δίκτυα [66].

Τα πρωτόκολλα δρομολόγησης μπορούν να διαιρεθούν σε δυναμικά (*proactive*), αντιδραστικά (*reactive*) και υβριδικά (*hybrid*) ανάλογα με την τοπολογία δρομολόγησης [67]. Τα δυναμικά πρωτόκολλα είναι είτε οδηγούμενα-από-πίνακα είτε διανυσματικά πρωτόκολλα απόστασης. Σε τέτοια πρωτόκολλα, οι κόμβοι ανανεώνουν περιοδικά τις υπάρχουσες πληροφορίες δρομολόγησης έτσι ώστε κάθε κόμβος να μπορεί αμέσως να θέσει σε ισχύ συνεπείς και ενημερωμένους πίνακες δρομολόγησης.

Σε αντίθεση, τα αντιδραστικά ή εναρκτώμενα από πηγή μετά από αίτηση πρωτόκολλα δεν ανανεώνουν περιοδικά τις πληροφορίες δρομολόγησης [68]. Κατά συνέπεια, δημιουργούν μεγάλη επιβάρυνση όταν καθορίζεται η διαδρομή, δεδομένου ότι οι διαδρομές δεν είναι απαραιτήτως ενημερωμένες σε περίπτωση ανάγκης. Τα υβριδικά πρωτόκολλα χρησιμοποιούν τόσο την αντιδραστική όσο και τη δυναμική προσέγγιση. Προσφέρουν τα μέσα για δυναμική μετάπτωση μεταξύ της αντιδραστικής και δυναμικής μορφής του πρωτοκόλλου.

Οι τρέχουσες προσπάθειες για τον σχεδιασμό ασφαλών πρωτοκόλλων δρομολόγησης στρέφονται κυρίως στα αντιδραστικά πρωτόκολλα, όπως η δυναμική δρομολόγηση πηγής (DSR) ή το ad hoc κατόπιν παραγγελίας διάνυσμα απόστασης (AODV) [33], που προτυποποιήθηκαν για να αποδώσουν καλύτερα από τα δυναμικά, με τη σημαντικά χαμηλότερη επιβάρυνση, δεδομένου ότι είναι σε θέση να αντιδρούν γρήγορα στις αλλαγές τοπολογίας κρατώντας την επιβάρυνση δρομολόγησης χαμηλή

σε περιόδους ή περιοχές του δικτύου όπου οι αλλαγές είναι λιγότερο συχνές. Μερικές από αυτές τις τεχνικές περιγράφονται εν συντομία στις επόμενες παραγράφους.

Τα υφιστάμενα ασφαλή πρωτόκολλα δρομολόγησης λαμβάνουν υπόψη τις ενεργές επιθέσεις που πραγματοποιούνται από τους συμβιβασμένους κόμβους και που αποσκοπούν να διαστρεβλώσουν την εκτέλεση των πρωτοκόλλων δρομολόγησης, ενώ οι ενεργητικές επιθέσεις και τα προβλήματα ιδιοτέλειας κόμβων δεν εξετάζονται. Παραδείγματος χάριν, το πρωτόκολλο ασφαλούς δρομολόγησης (SRP) [64,65], που είναι ένα αντιδραστικό πρωτόκολλο, εγγυάται την απόκτηση των σωστών τοπολογικών πληροφοριών. Χρησιμοποιεί μια υβριδική κατανομή βασισμένη στα δημόσια κλειδιά των επικοινωνούντων μερών. Πάσχει, εντούτοις, από την έλλειψη ενός μηχανισμού επικύρωσης για τα μηνύματα συντήρησης διαδρομών [39].

Ένα άλλο αντιδραστικό ασφαλές ad hoc πρωτόκολλο δρομολόγησης, το ARIADNE, που είναι βασισμένο σε DSR, εγγυάται την από σημείο σε σημείο πιστοποίηση με τη χρησιμοποίηση ενός κώδικα επικύρωσης μηνυμάτων (MAC) και ενός κοινού μυστικού μεταξύ των δύο συμβαλλόμενων μερών [69]. Το ασφαλές πρωτόκολλο δρομολόγησης ARAN [65] ανιχνεύει και προστατεύει από τις κακόβουλες ενέργειες που εκτελούνται από τρίτους και από ομότιμους στο ad hoc περιβάλλον. Προστατεύει από επιτήδειους χρησιμοποιώντας την τροποποίηση, την επεξεργασία και την προσωποποίηση, αλλά η χρήση ασύμμετρης κρυπτογραφίας το καθιστά ένα πολύ δαπανηρό πρωτόκολλο από την άποψη της χρήσης ΚΜΕ (CPU) και της κατανάλωσης ισχύος.

Το πρωτόκολλο SEAD, αφ' ετέρου, είναι ένα δυναμικό πρωτόκολλο βασισμένο στο DSDV (*destination sequenced distance vector protocol*) [70], που εξετάζει τους επιτιθεμένους που τροποποιούν τις πληροφορίες δρομολόγησης. Προτιμά να χρησιμοποιεί τις αποδοτικές μονόδρομες συναρτήσεις κατατεμαχισμού (*hash functions*) παρά τη στήριξη στις ακριβές ασύμμετρες διαδικασίες κρυπτογραφίας. Το SEAD δεν αντιμετωπίζει την επίθεση *wormhole* και οι συντάκτες προτείνουν, όπως στο πρωτόκολλο ARIADNE, να χρησιμοποιήσουν ένα διαφορετικό πρωτόκολλο για να ανιχνεύσουν αυτήν την ιδιαίτερη απειλή [65,70].

4.5 Μέτρα αντιμετώπισης απειλών

Όπως κάθε επίθεση χρειάζεται μια ανάλογη άμυνα για να υπάρξει αντίσταση, έτσι και στα δίκτυά μας, κάθε τύπος εισβολής χρειάζεται μια αντίστοιχη ηλεκτρονική άμυνα ώστε να αποτρέψουμε κάθε επίδοξο εισβολέα-επιτιθέμενο να καταφέρει να καταλάβει το δίκτυό μας.

4.5.1 Συστήματα ανίχνευσης εισβολών (IDSs)

Μια εισβολή μπορεί να οριστεί ως "ένα σύνολο ενεργειών που προσπαθούν να θέσουν σε κίνδυνο την ακεραιότητα, την εμπιστευτικότητα, ή τη διαθεσιμότητα ενός πόρου" [71], ή "οποιαδήποτε αναρμόδια ή ανεπιθύμητη δραστηριότητα σε ένα σύστημα ή ένα δίκτυο" [72]. Ένα IDS μπορεί να οριστεί ως "ένα σύστημα που

προσπαθεί να ανιχνεύσει και να προειδοποιήσει για αποπειραθείσες παρεισφρήσεις σε ένα σύστημα ή ένα δίκτυο" [72].

Η εμπειρία από την έρευνα σε θέματα ασφάλειας έχει δείξει ότι ανεξάρτητα από το πόσα μέτρα πρόληψης εισβολών παρεμβάλλονται στα δίκτυα, υπάρχουν πάντα μερικές αδυναμίες στα συστήματα που κάποιος εισβολέας θα μπορούσε να εκμεταλλευτεί για να παρεισφρήσει [73]. Αυτές οι αδυναμίες περιλαμβάνουν κυρίως τα λάθη σχεδιασμού και προγραμματισμού. Ως εκ τούτου, τα μέτρα πρόληψης εισβολών (δυναμικές λύσεις) δεν μπορούν να αποτρέψουν τις επιθέσεις και πρέπει να ενισχυθούν με IDS's. Ένα IDS παρουσιάζει έναν δεύτερο τοίχο άμυνας και είναι ζωτικό για οποιοδήποτε δίκτυο υψηλής ικανότητας επιβίωσης.

Οι αρχικές παραδοχές της ανίχνευσης εισβολής είναι:

- Οι δραστηριότητες χρηστών και προγράμματος είναι παρατηρήσιμες, παραδείγματος χάριν μέσω των μηχανισμών ελέγχου συστημάτων.
- Το πιο σημαντικό, οι κανονικές (normal) δραστηριότητες και οι δραστηριότητες που προέρχονται από εισβολή έχουν διακριτή συμπεριφορά.

Επομένως, η ανίχνευση εισβολής περιλαμβάνει τη σύλληψη των στοιχείων ελεγκτικής παρακολούθησης και την εύρεση ενδείξεων στα στοιχεία για να καθοριστεί εάν το σύστημα είναι υπό επίθεση. Ένα πρότυπο ανίχνευσης εισβολής έχει δύο συστατικά: *τα χαρακτηριστικά γνωρίσματα* (ιδιότητες ή μέτρα) και *τον αλγόριθμο διαμόρφωσης*.

Το σημαντικότερο βήμα στην οικοδόμηση ενός αποτελεσματικού προτύπου ανίχνευσης εισβολής είναι ο καθορισμός ενός συνόλου χαρακτηριστικών πρόγνωσης που συλλαμβάνουν με ακρίβεια τις αντιπροσωπευτικές συμπεριφορές των παρεισφρητικών ή κανονικών δραστηριοτήτων και μπορεί να είναι ανεξάρτητο από τον σχεδιασμό του αλγόριθμου διαμόρφωσης.

Πρόσφατα, μερικά IDSs έχουν προταθεί για τα MANETs. Είναι όλα κατανεμημένα, host-based, anomaly-based, και συνεργάσιμα. Η συνεργασία, εντούτοις, μπορεί να διανεμηθεί πλήρως και εξίσου μεταξύ των κόμβων, ή μπορεί να βασιστεί στην ιεραρχική οργάνωση των κόμβων. Κάθε σχέδιο IDS διαφέρει από τη μία λύση στην άλλη.

4.5.2 Αντιμετώπιση εισβολών

Η προσέγγιση για ανθεκτικά στις εισβολές ασύρματα δίκτυα ad hoc που γίνεται στο [74] βασίζεται σε τρεις ιδέες-κλειδιά:

- Ένας πλήρως αποκεντρωμένος και δυναμικά διευθετούμενος μηχανισμός προστασίας (firewall) που περιορίζει την επίδραση μιας επίθεσης πλημμυρίδας πακέτων στο άμεσο γειτονικό περιβάλλον του κόμβου-εισβολέα.
- Μία αμερόληπτη τεχνική αλγορίθμου δρομολόγησης για ανίχνευση και ανάκτηση από αποτυχημένη δρομολόγηση που προκλήθηκε από εισβολή.
- Μία αρχιτεκτονική ασύρματης επέκτασης δρομολογητή (WRE) που επιτρέπει στους μηχανισμούς επιβίωσης από επιθέσεις DoS να ενσωματωθούν με μικρή προσπάθεια στις υπάρχουσες ασύρματες υλοποιήσεις συστημάτων.

Το ασύρματο περιβάλλον δικτύωσης χαρακτηρίζεται από τις ακόλουθες τρεις ιδιότητες:

- Υφίσταται μία προϋπάρχουσα σχέση εμπιστοσύνης μεταξύ όλων των κόμβων στο ad hoc δίκτυο. Αυτή είναι μία εύλογη παραδοχή για τα είδη των εφαρμογών που υλοποιούνται από τέτοια δίκτυα. Κάθε κόμβος πρέπει να είναι διευθετημένος με τα δημόσια κλειδιά όλων των άλλων κόμβων του δικτύου.
- Χρησιμοποίηση της πιστοποίησης πακέτων βασισμένη στο IPSEC για την προστασία της ακεραιότητας όλων των πακέτων δεδομένων που μεταδίδονται στο δίκτυο.
- Όλες οι ασύρματες συνδέσεις στο δίκτυο είναι διπλής κατεύθυνσης και έτσι το δίκτυο χαρακτηρίζεται συμμετρικό.

Παρακάτω θα περιγραφούν σε συντομία οι τρεις ιδέες-κλειδιά για την ανθεκτικότητα σε εισβολές των ad hoc ασύρματων δικτύων:

α. Κατανεμημένη ασύρματη αντιπυρική ζώνη (firewall)

Σε ένα παραδοσιακό ενσύρματο περιβάλλον δικτύου, το firewall εγκαθίσταται στο σημείο εισόδου/εξόδου του δικτύου ώστε να φιλτράρεται η μη επιτρεπτή κυκλοφορία που προέρχεται από έξω από το όριο του προστατευόμενου δικτύου.

Σε ένα ad hoc ασύρματο περιβάλλον όπου οι κόμβοι μπορούν ενδεχομένως να είναι κινητοί, η τοπολογία δικτύων είναι δυναμική και δεν έχει επομένως κανένα νόημα ένα καλά καθορισμένο σημείο εισόδου/εξόδου για το δίκτυο. Επίσης, οποιοσδήποτε κόμβος μέσα στο δίκτυο θα μπορούσε να είναι ο εισβολέας και έτσι η κυκλοφορία επίθεσης θα μπορούσε να δημιουργηθεί από μέσα από το ίδιο το δίκτυο. Επιπλέον, οι παραδοσιακές αντιπυρικές ζώνες δεν σχεδιάζονται για να προστατεύσουν από επιθέσεις πλημμυρίδας πακέτων όπου η κυκλοφορία επίθεσης μεταμφιέζεται σε νόμιμα πακέτα που περνούν από τους κανόνες ελέγχου πρόσβασης του firewall.

Εννοιολογικά, η λειτουργία αντιπυρικών ζωνών διανέμεται πλήρως σε όλους τους κόμβους (δηλ. στους ασύρματους δρομολογητές IP) μέσα στο δίκτυο. Κάθε κόμβος στο δίκτυο διατηρεί έναν πίνακα αντιπυρικών ζωνών που περιέχει έναν κατάλογο από τις επιτρεπόμενες ροές πακέτων που μπορούν να περάσουν μέσω αυτού του κόμβου-δρομολογητή. Μια ροή πακέτων είναι ένα ρεύμα πακέτων από έναν κόμβο πηγής σε έναν προορισμό και προσδιορίζεται μονοσήμαντα από τις IP διευθύνσεις της πηγής και του προορισμού των πακέτων.

Το κατανεμημένο ασύρματο firewall σχεδιάζεται για να είναι δυναμικά ρυθμιζόμενο, δηλαδή οι καταχωρήσεις του πίνακα δημιουργούνται και διατηρούνται στο χρόνο εκτέλεσης και δεν είναι στατικά προ-διαμορφωμένες πριν από τη λειτουργία του δικτύου. Οι καταχωρήσεις των πινάκων των αντιπυρικών ζωνών είναι αυτόματα επαναδιαμορφώσιμες σε απάντηση στις αλλαγές της τοπολογίας του δικτύου, καθώς επίσης και στις ανιχνευμένες επιθέσεις πλημμυρίδας.

Επιπλέον, η διαμόρφωση και ο έλεγχος του firewall ολοκληρώνεται με ένα συνολικά αποκεντρωμένο τρόπο. Δεν υπάρχει κανένας κεντρικός ελεγκτής ή διαχειριστής αντιπυρικών ζωνών του δικτύου για την εκτέλεση αυτής της λειτουργίας.

Η τελική επίδραση της διανεμημένης αντιπυρικής ζώνης είναι ότι όταν ο κόμβος-εισβολέας παράγει μια πλημμύρα της πλαστής κυκλοφορίας (παραπλανητικά και επαναλαμβανόμενα πακέτα), οι ασύρματοι μηχανισμοί αντιπυρικών ζωνών στους άμεσους one-hop γείτονες του εισβολέα φιλτράρουν την κυκλοφορία επίθεσης.

Η δυναμική διαμόρφωση και η συντήρηση των καταχωρήσεων του πίνακα του firewall μέσα στο δίκτυο ενεργοποιείται με το πρωτόκολλο χειραψίας που εκτελείται μεταξύ του αποστολέα και του δέκτη μιας ροής.

β. Επικαλυπτόμενη δρομολόγηση

Για την ανίχνευση μιας προκληθείσης από εισβολέα αποτυχίας της τρέχουσας διαδρομής μιας ροής, ο αποστολέας της ροής επικαλείται το μηχανισμό δρομολόγησης επικαλύψεων για να ανακαλύψει μια διαδρομή προς τον δέκτη που παρακάμπτει τον εισβολέα. Αυτός ο μηχανισμός σχεδιάζεται ώστε να είναι ανεξάρτητος από τον αλγόριθμο δρομολόγησης.

Η νέα διαδρομή μεταξύ της πηγής και του προορισμού είναι μια διαδρομή επικαλύψεων που διαμορφώνεται από μια αλληλουχία δύο tunnel στον φίλιο κόμβο. Εάν ο φίλιος κόμβος δεν παράκαμψε τον εισβολέα και τον περιέλαβε στη διαδρομή, η πρόσφατα επιλεγμένη διαδρομή θα αποτύχει πάλι. Ο αποστολέας επιλέγει έπειτα έναν νέο φίλιο κόμβο και προσπαθεί πάλι έως ότου πετύχει τον σκοπό του ή εξαντλήσει όλους τους φίλιους κόμβους.

γ. Ανίχνευση αποτυχημένης δρομολόγησης

Αυτός ο μηχανισμός όχι μόνο επιτρέπει τον ανασχηματισμό της κατανεμημένης ασύρματης αντιπυρικής ζώνης αλλά και ενεργοποιεί τον μηχανισμό επικαλυπτόμενης δρομολόγησης που είναι ανθεκτικός σε εισβολές.

Η προσέγγιση ανίχνευσης αποτυχημένης δρομολόγησης χρησιμοποιεί ένα μηχανισμό βασισμένο στον δέκτη για να ανιχνεύσει μια επίθεση πλημμυρίδας ή διακοπής της ροής που αρχίζει από ένα εισβολέα στη διαδρομή. Ο αποστολέας τοποθετεί έναν υπογεγραμμένο κώδικα επικύρωσης μηνυμάτων (MAC) στο πεδίο επικεφαλίδας πιστοποίησης ενός πακέτου IP. Ο δέκτης ελέγχει τη MAC του πακέτου ώστε να πιστοποιηθεί η ακεραιότητά του. Η επικεφαλίδα IPSEC περιέχει επίσης ένα πεδίο αριθμού ακολουθίας πακέτων που χρησιμοποιείται από το δέκτη για να ανιχνεύσει τη διπλή παραλαβή πακέτων καθώς επίσης και για να ανιχνεύσει τις απώλειες πακέτων.

Ο δέκτης ελέγχει τρεις παραμέτρους κάθε ροής που καταλήγει σε αυτόν: (1) ποσοστό απώλειας πακέτων, (2) ποσοστό παραλαβών διπλών πακέτων και (3) ποσοστό αποτυχίας επικύρωσης πακέτων, για να ανιχνεύσει τις ανωμαλίες στη συμπεριφορά της ροής που συνιστούν μια επίθεση.

4.5.3 Αντίσταση σε επιθέσεις υπερχείλισης (πλημμύρας)

Μία επίθεση DoS που ονομάζεται Ad Hoc Flooding Attack, έχει ως αποτέλεσμα την άρνηση παροχής υπηρεσίας (denial of service) όταν χρησιμοποιείται εναντίον όλων των κατόπιν απαίτησης (*on-demand*) πρωτοκόλλων δρομολόγησης των ad hoc δικτύων [75]. Σε αυτού του τύπου την επίθεση, ο επιτιθέμενος είτε μεταδίδει πάρα πολλά πακέτα Route Request είτε στέλνει πολλά πακέτα δεδομένων ώστε να καταναλώσει (ουσιαστικά σπαταλήσει) το εύρος ζώνης και έτσι να δημιουργήσει συμφόρηση στις ζεύξεις. Για την άμυνα των πρωτοκόλλων δρομολόγησης ενάντια στην Ad Hoc Flooding Attack έχει αναπτυχθεί μία γενική συνιστώσα ασφάλειας που

ονομάζεται Flooding Attack Prevention (FAP), η οποία μπορεί να εφαρμοστεί στο πρωτόκολλο δρομολόγησης AODV και να επιτρέπει στο πρωτόκολλο να ανθίσταται στην επίθεση συμφόρησης.

Θα αναπτυχθεί η επίδραση της Ad Hoc Flooding Attack στην λειτουργία του AODV αφού και τα υπόλοιπα πρωτόκολλα (όπως τα DSR, ARIADNE, SAODV και ARAN) είναι ευάλωτα κατά τον ίδιο τρόπο.

Στο AODV η ανακάλυψη της διαδρομής (path discovery) γίνεται εξ' ολοκλήρου on demand. Η λειτουργία του γίνεται με τα πακέτα RREQ, RREP και RERR (ως γνωστόν δεν απαιτείται να εξηγηθεί περαιτέρω), ενώ στη συνέχεια θα αναλυθούν περισσότερο οι επιθέσεις πλημμυρίδας RREQ και DATA.

Τα πακέτα RREQ που πλημμυρίζουν το δίκτυο θα καταναλώσουν μεγάλο μέρος των πόρων του δικτύου. Για να μειωθεί η συμφόρηση στο δίκτυο, το πρωτόκολλο AODV υιοθετεί κάποιες μεθόδους, όπου απαντώνται όροι όπως RREQ_RATELIMIT (ο max αριθμός των RREQ μηνυμάτων ανά sec που μπορεί να δημιουργήσει ένας κόμβος), το RREP που αναμένει ένας κόμβος που έχει αποστείλει ένα RREQ, η max τιμή TTL (οι max φορές εκ νέου προσπάθειας ενός κόμβου να βρει διαδρομή προς τον προορισμό στέλνοντας RREQ), ο προσαυξανόμενος δακτύλιος στον οποίο μεταδίδονται τα πακέτα RREQ ώστε να μειωθεί η επιβάρυνση που προκαλείται από την πλημμύρα σε όλο το δίκτυο, ο RING TRAVERSAL TIME πέραν του οποίου - αν δεν έχει ληφθεί κανένα RREP – η πλημμυρισμένη περιοχή μεγεθύνεται μεγαλώνοντας το TTL κατά μία δεδομένη τιμή και, τέλος, η επανάληψη της διαδικασίας μέχρι να ληφθεί ένα RREP από τον δημιουργό του RREQ.

Στην Ad Hoc Flooding Attack, ο επιτιθέμενος κόμβος καταστρατηγεί τους παραπάνω κανόνες για να εξαντλήσει τους πόρους του δικτύου. Αρχικά, ο επιτιθέμενος επιλέγει πολλές IP διευθύνσεις που δεν ανήκουν στα δίκτυα. Επειδή κανείς κόμβος δεν μπορεί να απαντήσει RREP πακέτα για αυτά τα RREQ, η ανάστροφη διαδρομή στον πίνακα δρομολόγησης του κόμβου θα διατηρηθεί περισσότερο. Ο επιτιθέμενος μπορεί να επιλέξει τυχαίες διευθύνσεις IP. Έπειτα, ο επιτιθέμενος δημιουργεί επιτυχώς μαζικά RREQ μηνύματα για αυτές τις άκυρες IP διευθύνσεις και προσπαθεί να στείλει υπερβολικά RREQ χωρίς να λαμβάνει υπ' όψιν το RREQ_RATELIMIT ανά sec. Ο ίδιος θα ξαναστείλει τα πακέτα RREQ χωρίς να περιμένει για το RREP ή για τον round-trip χρόνο. Ο TTL των RREQ έχει τεθεί στο max. Στις Flooding Attacks, ολόκληρο το δίκτυο θα είναι γεμάτο με πακέτα RREQ τα οποία στέλνει ο επιτιθέμενος. Το εύρος ζώνης επικοινωνίας εξαντλείται από τα πακέτα RREQ που πλημμυρίζουν το δίκτυο και το ίδιο συμβαίνει ταυτόχρονα και με τους πόρους των κόμβων. Εάν μαζικά πακέτα RREQ καταφθάνουν στον κόμβο σε μικρό χρόνο, η αποθηκευτική ικανότητα του πίνακα δρομολόγησης εξαντλείται έτσι που ο κόμβος δεν μπορεί να λάβει νέα RREQ πακέτα. Σαν αποτέλεσμα, οι νόμιμοι κόμβοι δεν μπορούν να δημιουργήσουν διαδρομές για να στείλουν δεδομένα.

Στην DATA Flooding Attack, αρχικά, ο επιτιθέμενος κόμβος δημιουργεί διαδρομές σε όλους τους κόμβους στα δίκτυα. Έπειτα, ο επιτιθέμενος κατευθύνει μεγάλους όγκους άχρηστων πακέτων δεδομένων προς όλους τους κόμβους κατά μήκος αυτών των διαδρομών. Τα υπερβολικά πακέτα δεδομένων φράσσουν το δίκτυο και μειώνουν το διαθέσιμο εύρος ζώνης του δικτύου για επικοινωνία μεταξύ των άλλων κόμβων στο δίκτυο. Ο κόμβος-προορισμός θα είναι απασχολημένος με την λήψη των υπερβολικών πακέτων από τον επιτιθέμενο και δεν θα λειτουργεί κανονικά. Εάν ο επιτιθέμενος συνδυάσει τα δύο είδη των Flooding Attack, αυτό θα έχει ως αποτέλεσμα την κατάρρευση ολόκληρου του δικτύου.

Στη συνέχεια θα περιγραφεί ένα σετ γενικών μηχανισμών οι οποίοι από κοινού αντιστέκονται ενάντια στις Ad Hoc Flooding Attacks: Η κατάπνιξη από γειτονικούς κόμβους (*neighbour suppression*) και η διακοπή της διαδρομής (*path cut-off*).

Η μέθοδος της κατάπνιξης από τους γειτονικούς κόμβους χρησιμοποιείται για να εμποδίσει την RREQ επίθεση πλημμυρίδας. Τα κινητά δίκτυα ad hoc είναι ασύρματα δίκτυα πολλαπλών αλμάτων και συνεπώς ο κάθε κόμβος στέλνει και λαμβάνει πακέτα μέσω των γειτονικών του κόμβων. Εάν όλοι οι γειτονικοί κόμβοι γύρω από τον συγκεκριμένο κόμβο αρνηθούν να προωθήσουν τα πακέτα του, ο κόμβος αυτός δεν μπορεί να επικοινωνήσει με τους άλλους κόμβους στο δίκτυο. Στην πράξη, ο κόμβος έχει απομονωθεί από το δίκτυο έστω και αν η θέση του είναι ακόμη εντός του δικτύου.

Όταν ο επιτιθέμενος εξαπολύει μία DATA επίθεση πλημμυρίδας, οι γειτονικοί κόμβοι είναι δύσκολο να το αναγνωρίσουν διότι ο γειτονικός κόμβος δεν μπορεί να κρίνει εάν ένα πακέτο DATA είναι άχρηστο στο επίπεδο δικτύου. Ο κόμβος προορισμού μπορεί εύκολα να πάρει την απόφαση στο επίπεδο εφαρμογών όταν έχει λάβει αυτά τα άχρηστα DATA πακέτα. Ο επιτιθέμενος θέτει μία διαδρομή από τον εαυτό του προς τον κόμβο-θύμα για να εξαπολύσει την επίθεση. Όταν το θύμα ανακαλύπτει την DATA Flooding Attack, μπορεί να διακόψει τη διαδρομή από τον επιτιθέμενο και έτσι να τον εμποδίσει από την συνέχιση της επίθεσης. Ο κόμβος-θύμα στέλνει ένα RRER μήνυμα στον επιτιθέμενο. Το μήνυμα αυτό εμφανίζει την IP διεύθυνση του θύματος απρόσιτη. Οι ενδιάμεσοι κόμβοι από τους οποίους περνάει το μήνυμα RRER θα διαγράψουν τη διαδρομή από τον επιτιθέμενο στο θύμα. Έτσι, με την αποκοπή όλων των σχετικών διαδρομών, η DATA Flooding Attack προοδευτικά τερματίζεται. Όταν αυτές οι διαδρομές επίθεσης τελειώσουν, ο επιτιθέμενος μπορεί να δημιουργήσει RREQ προκειμένου να φτιάξει ξανά νέες διαδρομές προς άλλους κόμβους. Οι άλλοι κόμβοι μπορούν να αρνηθούν να ιδρύσουν αυτές τις διαδρομές μέσω μη απάντησης με κάποιο RREP στα συγκεκριμένα RREQ. Στο πρωτόκολλο AODV, οι ενδιάμεσοι κόμβοι μπορούν να απαντήσουν στο RREQ αντί των τελικών κόμβων, εάν αυτοί έχουν μια ενεργό διαδρομή προς τον προορισμό. Για αυτόν τον λόγο, ο επιτιθέμενος μπορεί να ιδρύσει τις διαδρομές προς το θύμα αν και ο κόμβος-θύμα αρνείται να το κάνει. Για να αποφευχθεί αυτό, η λειτουργία κατά την οποία οι ενδιάμεσοι κόμβοι έχουν τη δυνατότητα να απαντούν στα RREQ πρέπει να ανασταλεί. Μόνο ο προορισμός πρέπει να μπορεί να αποκρίνεται σε τέτοια RREQ.

4.5.4 Λύσεις σε θέματα ασφάλειας δρομολόγησης

Παρακάτω παρουσιάζονται λύσεις που αφορούν στην ασφαλή δρομολόγηση και στην εφαρμογή ενός πρωτοκόλλου δρομολόγησης. Οι τεχνικές που προτείνονται είναι τέσσερις:

a) *Πιστοποίηση κατά τη διάρκεια όλων των φάσεων δρομολόγησης:* Αυτή η λύση έγκειται στη χρησιμοποίηση τεχνικών πιστοποίησης κατά τη διάρκεια όλων των φάσεων δρομολόγησης για να αποκλειστούν οι επιτιθέμενοι και μη πιστοποιημένοι κόμβοι από τη συμμετοχή στη δρομολόγηση. Δεδομένου ότι χρησιμοποιεί ψηφιακές υπογραφές, αυτή η λύση στηρίζεται σε μια αρχή πιστοποίησης (CA) η οποία απαιτεί τη χρήση ενός αξιόπιστου server πιστοποίησης του οποίου το δημόσιο κλειδί είναι εκ των προτέρων γνωστό σε όλους τους έγκυρους κόμβους. Αυτή η εμπιστοσύνη σε έναν σταθερό server

καθιστά τη λύση συγκεντρωτική και λιγότερο εύκαμπτη. Το σημαντικότερο πλεονέκτημα αυτής της προσέγγισης είναι ότι αποκλείει τους εξωτερικούς αναρμόδιους κόμβους από το να συμμετάσχουν στη δρομολόγηση και επομένως όλες οι επιθέσεις αποτρέπονται όταν δημιουργούνται από έναν εξωτερικό κόμβο. Επιπλέον, μερικές από τις επιθέσεις που προωθούνται από έναν εξουσιοδοτημένο κόμβο μπορούν να κατατροπωθούν.

b) *Μετρικό σύστημα με επίπεδα αξιοπιστίας*: Στο [76] ορίζεται ένα νέο μετρικό σύστημα το οποίο διέπει τη συμπεριφορά των πρωτοκόλλων δρομολόγησης. Αυτό το μετρικό σύστημα πρόκειται να ενσωματωθεί στα πακέτα ελέγχου για να αντανακλαστεί η ελάχιστη τιμή αξιοπιστίας που απαιτείται από τον αποστολέα. Κατά συνέπεια, ένας κόμβος που λαμβάνει οποιοδήποτε πακέτο δεν θα μπορεί ούτε να το επεξεργαστεί ούτε να το προωθήσει εκτός αν παρέχει το απαιτούμενο επίπεδο αξιοπιστίας που παρουσιάζεται στο πακέτο. Με αυτόν τον τρόπο, σχεδιάστηκε το SAR (Security-Aware Routing), ένα πρωτόκολλο προερχόμενο από το AODV και βασισμένο στο ιεραρχικό μετρικό σύστημα τιμών αξιοπιστίας. Στο SAR, αυτό το μετρικό χρησιμοποιείται ακόμη για την επιλογή συγκεκριμένης διαδρομής, όταν είναι διαθέσιμες περισσότερες από μία που ικανοποιούν το απαιτούμενο επίπεδο αξιοπιστίας. Στο γενικό πλαίσιο εφαρμογής, όπου δεν υπάρχει καμία ιεραρχία στο δίκτυο, ο καθορισμός των τιμών αξιοπιστίας των κόμβων είναι προβληματικός. Το πλεονέκτημα αυτής της λύσης συγκρινόμενης με την προηγούμενη είναι ότι αποτρέπει τις επιθέσεις από έναν εσωτερικό κόμβο σε ένα πιο υψηλό επίπεδο αξιοπιστίας.

c) *Επιβεβαίωση ασφαλούς γειτονικού κόμβου*: Αυτή η λύση έγκειται σε μία τριών γύρων ανταλλαγή μηνύματος αξιοπιστίας ανάμεσα σε δύο κόμβους, πριν επιβεβαιώσει ο ένας τον άλλο ως γείτονα. Από την στιγμή που ο αποστολέας χρησιμοποιεί υψηλότερη ισχύ, δεν μπορεί να λάβει το πακέτο από τους υπόλοιπους κόμβους, με συνέπεια αυτός να μην είναι σε θέση να εκτελέσει τη διαδικασία ανίχνευσης γειτόνων και να αγνοηθεί. Το σπουδαιότερο μειονέκτημα αυτής της λύσης είναι η σημαντική επιβάρυνση όταν αυξάνεται η κινητικότητα.

d) *Τυχαία κατανομή προώθησης μηνύματος:* Αυτή η τεχνική που προτείνεται στο [77] ελαχιστοποιεί την πιθανότητα ένας ορμητικός αντίπαλος να μπορέσει να διακατέχει όλες τις επιστρέφουσες διαδρομές. Κάνοντας χρήση αυτής της τεχνικής, ένας κόμβος πρώτα συλλέγει έναν αριθμό από RREQ's και έπειτα επιλέγει τυχαία ένα RREQ για προώθηση. Υπάρχουν έτσι δύο παράμετροι σχετικές με αυτήν την τεχνική: κατ' αρχάς, ο αριθμός πακέτων RREQ που συλλέγονται και δεύτερον, ο αλγόριθμος σύμφωνα με τον οποίο επιλέγονται οι λήξεις χρόνου. Το μειονέκτημα αυτής της λύσης είναι ότι αυξάνει την καθυστέρηση ανακάλυψης της διαδρομής, δεδομένου ότι κάθε κόμβος πρέπει να περιμένει μία λήξη χρόνου ή να λάβει έναν δεδομένο αριθμό πακέτων πριν προωθήσει την RREQ. Επιπλέον, η τυχαία επιλογή αποτρέπει την ανακάλυψη βέλτιστων διαδρομών.

4.5.5 Λύσεις ενάντια στην ιδιοτέλεια (selfishness) των κόμβων κατά την προώθηση δεδομένων

Για την περίπτωση των εγωιστικών κόμβων (κόμβων που προτιμούν την μη επίτευξη της αποστολής του δικτύου από την έλλειψη ενέργειας) έχουν προταθεί λύσεις πρόληψης , ανίχνευσης και λύσεις που βασίζονται στην φήμη.

Στις λύσεις ανίχνευσης ανήκει η από άκρο σε άκρο ανατροφοδότηση, η παρακολούθηση λειτουργίας χωρίς διάκριση, παρακολούθηση βασισμένη σε δραστηριότητα και η αμοιβαία χορήγηση εισόδου στην γειτονιά:

(1). *Από άκρο σε άκρο ανατροφοδοτήσεις*. Ο μηχανισμός αυτός έγκειται στην αναγνώριση πακέτων στο επίπεδο δικτύου με έναν από άκρου εις άκρον τρόπο, ώστε να καταστήσει αξιόπιστο το πρωτόκολλο δρομολόγησης (όπως το TCP). Αυτό σημαίνει ότι ο κόμβος προορισμού βεβαιώνει την επιτυχή λήψη πακέτων στέλνοντας ανατροφοδοτήσεις (ACK's) στην πηγή. Μια επιτυχής λήψη υπονοεί ότι η αντίστοιχη διαδρομή είναι λειτουργική, ενώ μία αποτυχία στη λήψη ack μετά από τη λήξη χρόνου (timeout) μπορεί να εκληφθεί σαν ένδειξη ότι η διαδρομή είναι σπασμένη, συμβιβασμένη ή περιλαμβάνει ιδιοτελείς κόμβους. Τα πρωτόκολλα δρομολόγησης που είναι βασισμένα σε αυτή την προσέγγιση διατηρούν μια διαβάθμιση για κάθε διαδρομή που απεικονίζει την αξιοπιστία της διαδρομής και ενημερώνεται κάθε φορά που ένα σύνολο πακέτων δεδομένων διαβιβάζεται κατά μήκος της διαδρομής. Όταν η διαβάθμιση ενός δρομολογίου μιας δεδομένης διαδρομής μειωθεί κάτω από ένα καθορισμένο κατώτατο όριο, το οποίο είναι αρκετά υψηλό ώστε να υπερνικήσει τις απώλειες λόγω των συγκρούσεων, αυτή η διαδρομή δεν θα χρησιμοποιηθεί άλλο. Το σημαντικότερο πρόβλημα με αυτήν την τεχνική είναι η έλλειψη μηχανισμού ανίχνευσης κόμβων που δεν συμπεριφέρονται σωστά. Αυτή η τεχνική μπορεί να ανιχνεύσει τόσο διαδρομές που περιέχουν κακόβουλους κόμβους όσο και αυτές που είναι κομμένες, αλλά χωρίς να κάνει οποιαδήποτε διάκριση μεταξύ αυτών των δύο περιπτώσεων και χωρίς συμπληρωματικές πληροφορίες σχετικά με τον κόμβο που προκαλεί την απώλεια πακέτων. Εντούτοις, αυτή η τεχνική βοηθά για να αποφευχθεί η μετάδοση άχρηστων πακέτων μέσω αναξιόπιστων διαδρομών και μπορεί να συνδυαστεί με άλλες περιπλοκότερες τεχνικές.

(2). *Παρακολούθηση λειτουργίας χωρίς διάκριση (Watchdog)*. Η μέθοδος watchdog που ορίζεται στο [78], αποτελεί μία βασική τεχνική πάνω στην οποία στηρίζονται πολλές περαιτέρω λύσεις. Στόχος της είναι να ανιχνεύει δυσλειτουργικούς κόμβους που δεν προωθούν πακέτα (ή βεβλαμένους κόμβους που απορρίπτουν πακέτα) όταν χρησιμοποιείται ένα πρωτόκολλο δρομολόγησης πηγής, με το να παρακολουθεί τους γειτονικούς κόμβους χωρίς διάκριση. Η watchdog είναι σε θέση να ανιχνεύει δυσλειτουργικούς κόμβους σε πολλές περιπτώσεις και δεν προσθέτει καμία επιβάρυνση όταν κανείς κόμβος δεν δυσλειτουργεί. Αποτυγχάνει ωστόσο να ανιχνεύσει τη συνεργατική δυσλειτουργία που, ούτως ή άλλως, είναι δύσκολα ανιχνεύσιμη και μπορεί να προκαλέσει λανθασμένες ανιχνεύσεις, ιδιαίτερα όταν ο υπό παρακολούθηση κόμβος χρησιμοποιεί την τεχνική ελέγχου ισχύος για να διατηρήσει την ισχύ του.

(3). *Παρακολούθηση βασισμένη σε δραστηριότητα*. Πρόκειται για μια γενίκευση της τεχνικής watchdog. Στην τεχνική αυτή, ένας κόμβος συνεχώς παρακολουθεί αδιάκριτα την κυκλοφορία όλων των γειτόνων για τα κανονικά πακέτα δεδομένων, και επιβλέπει την προώθηση κάθε πακέτου του οποίου ο επόμενος προωθητής βρίσκεται επίσης στην γειτονιά του. Αυτό μπορεί να μεγαλώσει τον αριθμό των παρατηρήσεων και να βελτιώσει την αποτελεσματικότητα της μεθόδου watchdog.

(4). *Αμοιβαία χορήγηση εισόδου στη 'γειτονιά'*. Πρόκειται για μία ενοποιημένη λύση στο επίπεδο δικτύου που περιγράφεται στο [79]. Αυτή η τεχνική σκοπεύει στην προστασία τόσο της δρομολόγησης όσο και της προώθησης δεδομένων. Μία υπογραφή κατωφλίου βασισμένη σε κρυπτογραφία και η τεχνική watchdog αποτελούν τον πυρήνα αυτής της λύσης.

Η δεύτερη κατηγορία είναι οι λύσεις πρόληψης που περιλαμβάνει τον ορισμό ενός εικονικού νομίσματος (*nuglets*) και τη διασπορά δεδομένων:

(1). *Nuglets*. Η κύρια ιδέα αυτής της τεχνικής που προτείνεται στο [82] είναι ότι οι κόμβοι που κάνουν χρήση μιας υπηρεσίας πρέπει να πληρώνουν για αυτή (σε nuglets) στους κόμβους που παρέχουν την υπηρεσία αυτή. Έτσι κινητοποιούνται οι κόμβοι στο να αυξήσουν το απόθεμα σε nuglets παρέχοντας υπηρεσίες σε άλλους κόμβους. Κάθε κόμβος έχει έναν μετρητή μέσω του οποίου αναπαρίστανται τα nuglets και ο οποίος διαχειρίζεται από ένα αξιόπιστο και ανθεκτικό hardware σχήμα ασφαλείας. Με αυτό τον τρόπο εμποδίζεται ο κάθε κόμβος από το να αυξάνει παράτυπα την τιμή του μετρητή του, αν και καθιστά πιο σύνθετη την υλοποίησή του. Εάν ένας κόμβος συμπεριφέρεται εγωιστικά, δεν μπορεί να κερδίζει nuglets και συνεπώς είναι αδύνατο να στέλνει τα πακέτα του.

(2). *Διασπορά δεδομένων*. Αυτή η προσέγγιση είναι βασισμένη στον αλγόριθμο *Rabin* [65], ο οποίος παίρνει ως πλεονέκτημα την ύπαρξη των πολλαπλάσιων διαδρομών από μια πηγή σε έναν προορισμό για να αυξήσει την αξιοπιστία κατά την μετάδοση των πακέτων. Πρόκειται για προσθήκη πλεοναζόντων bit στο προς αποστολή μήνυμα με παράλληλη κωδικοποίηση και τεμαχισμό σε έναν αριθμό κομματιών και τέλος διάδοση στις διαθέσιμες διαδρομές, έτσι ώστε ακόμη και μία τμηματική λήψη να είναι σε θέση να οδηγήσει σε επιτυχή ανασύνθεση του μηνύματος στον παραλήπτη. Ακόμα κι αν αυτός ο μηχανισμός δεν αποτρέπει τους κόμβους από αθέμιτη συμπεριφορά και δεν παρακινεί τους κόμβους να συνεργαστούν, αντίθετα από την προηγούμενη προσέγγιση, είναι χρήσιμος και μπορεί να μειώσει την εγωιστική συμπεριφορά και τις επιπτώσεις των επιθέσεων στην αξιοπιστία της επικοινωνίας.

Μια άλλη κατηγορία είναι οι λύσεις που βασίζονται στην φήμη. Η φήμη ενός κόμβου είναι το ποσό της αξιοπιστίας που του αποδίδουν οι άλλοι κόμβοι σε σχέση με τη συνεργασιμότητα και τη συμμετοχή του στην προώθηση πακέτων. Η πληροφορία της φήμης πρέπει να ανταλλάσσεται μεταξύ των κόμβων ώστε ο καθένας να συμπεραίνει τις ακριβείς τιμές. Υπάρχει μια δοσοληψία ανάμεσα στην αποτελεσματικότητα της χρήσης της διαθέσιμης πληροφορίας και στη σθεναρότητα (ανοχή σε σφάλματα) ενάντια στην παραπληροφόρηση. Δύο λύσεις αυτής της κατηγορίας υπάρχουν και ονομάζονται CORE και CONFIDANT. Στην πρώτη [80], μεταδίδονται οι θετικές παρατηρήσεις (από κόμβους που συμπεριφέρονται σωστά) αλλά όχι οι αρνητικές παρατηρήσεις, γεγονός που μειώνει το ενδεχόμενο της πληροφόρησης από παρατηρήσεις άλλων και μπορεί να μειώσει την αποτελεσματικότητα ανίχνευσης δυσλειτουργιών στο δίκτυο. Στη δεύτερη λύση [81], το σύστημα CONFIDANT είναι βασισμένο σε αρνητικές εμπειρίες.

Τέλος, υπάρχει και ο μηχανισμός της διερεύνησης. Αυτός ο μηχανισμός έγκειται στο να ενσωματώνει απλά τις εντολές στα πακέτα δεδομένων για να τα αναγνωρίζει. Αυτές οι εντολές είναι οι αποκαλούμενοι ‘έλεγχοι’ (probes) και προορίζονται για τους επιλεγμένους κόμβους. Οι έλεγχοι, γενικά, εφαρμόζονται όταν ανιχνεύεται μια διαδρομή που περιέχει έναν εγωιστικό ή κακόβουλο κόμβο.

4.5.6 Λύσεις σε παρεκτροπές κατά την πρόσβαση καναλιού

Λόγω της τυχαίας επιλογής του backoff, είναι δύσκολο να γίνει διάκριση μεταξύ της θεμιτής επιλογής των μικρών τιμών backoff και της επιλογής μιας αθέμιτης συμπεριφοράς. Ως εκ τούτου, η ανίχνευση μιας αθέμιτης συμπεριφοράς MAC στρώματος είναι ένα περίπλοκο πρόβλημα. Στο [61] προτείνεται ένα σχήμα προς επίλυση αυτού του προβλήματος, το οποίο αποτελείται από τροποποιήσεις στο πρωτόκολλο IEEE 802.11 που επιτρέπει στο δέκτη να προσδιορίσει την κακή συμπεριφορά των αποστολέων μέσα σε ένα μικρό διάστημα παρατήρησης. Αντί του αποστολέα, ο δέκτης επιλέγει μία τυχαία τιμή backoff και την επισυνάπτει στα CTS και στα ACK πακέτα που διαβιβάζει στον αποστολέα. Ο αποστολέας χρησιμοποιεί αυτήν την ορισμένη τιμή backoff στην επόμενη μετάδοση προς τον δέκτη.

Με αυτές τις τροποποιήσεις, ένας δέκτης μπορεί να προσδιορίσει την παρέκκλιση αποστολέων από το πρωτόκολλο με την παρατήρηση του αριθμού μη απασχολούμενων χρονοθυρίδων μεταξύ των διαδοχικών μεταδόσεων από τον αποστολέα. Το μέγεθος των παρατηρούμενων αποκλίσεων χρησιμοποιείται για να εντοπίσει την κακή συμπεριφορά αποστολέων με υψηλή πιθανότητα. Το προτεινόμενο σχέδιο προσπαθεί επίσης να αρνηθεί οποιοδήποτε πλεονέκτημα ρυθμοαπόδοσης που οι κόμβοι αθέμιτης συμπεριφοράς μπορούν να λάβουν. Για να επιτευχθεί αυτό και να αποθαρρυνθεί η λανθάνουσα συμπεριφορά, οι παρεκκλίνοντες αποστολείς τιμωρούνται με προσθήκη ποινής στο επόμενο backoff που εκχωρείται σε αυτούς.

4.5.7 Εγκατάσταση και διαχείριση κλειδιού

Ένα θέμα ασφαλείας που χρήζει μεγάλης προσοχής στα ασύρματα δίκτυα είναι ο τομέας της διαχείρισης κλειδιού. Τα ad hoc δίκτυα είναι μοναδικά, σε σχέση με τα υπόλοιπα δίκτυα σ' αυτό το θέμα, λόγω του μεγέθους, της κινητικότητας και των περιορισμών σε υπολογισμούς και σε ισχύ που έχουν συζητηθεί σε προηγούμενες παραγράφους. Έτσι, οι παραπάνω περιορισμοί σε συνδυασμό με τα λειτουργικά εμπόδια, κάνουν τη διαχείριση κλειδιού μια απόλυτη αναγκαιότητα στα περισσότερα ad hoc και sensor δίκτυα.

Παραδοσιακά, η εγκατάσταση κλειδιού γίνεται με χρήση ενός από τα πολλά πρωτόκολλα δημόσιου κλειδιού. Ένα από τα πιο κοινά είναι το πρωτόκολλο δημόσιου κλειδιού των *Diffie-Hellman*. Όμως, οι περισσότερες παραδοσιακές τεχνικές είναι ακατάλληλες για συσκευές χαμηλής ισχύος, όπως είναι τα δίκτυά μας. Αυτό οφείλεται κυρίως στο γεγονός ότι μια τυπική ανταλλαγή κλειδιού χρησιμοποιεί ασύμμετρη κρυπτογραφία, που ονομάζεται κρυπτογραφία δημόσιου κλειδιού. Σ' αυτή την περίπτωση, είναι αναγκαία η διατήρηση δύο μαθηματικά σχετιζόμενων κλειδιών, ένα εκ των οποίων θα είναι δημόσια γνωστό ενώ το δεύτερο θα διατηρείται μυστικό. Αυτό επιτρέπει στα δεδομένα να κρυπτογραφούνται με το δημόσιο κλειδί και να αποκρυπτογραφούνται με το ιδιωτικό. Αυτό δημιουργεί μεγάλο υπολογιστικό κόστος σε κάθε κόμβο του δικτύου.

Έτσι η συμμετρική κρυπτογραφία είναι η τυπική επιλογή για εφαρμογές που δεν μπορούν να αντέξουν την υπολογιστική πολυπλοκότητα της ασύμμετρης κρυπτογραφίας. Τα συμμετρικά σχήματα χρησιμοποιούν ένα μονό διαμοιραζόμενο

κλειδί που είναι γνωστό σε δύο επικοινωνούντα τμήματα. Αυτό το κοινό κλειδί χρησιμοποιείται τόσο για κρυπτογράφηση όσο και αποκρυπτογράφηση. Το πιο χαρακτηριστικό παράδειγμα συμμετρικής κρυπτογραφίας είναι το DES (Data Encryption System), το οποίο εγκαταλείφθηκε γρήγορα.

Ένα μεγάλο μειονέκτημα της συμμετρικής κρυπτογραφίας είναι το πρόβλημα ανταλλαγής κλειδιού. Το πρόβλημα αυτό παρουσιάζεται στο γεγονός ότι τα δύο επικοινωνούντα τμήματα πρέπει να ξέρουν το κλειδί πριν επικοινωνήσουν. Έτσι, πρέπει να εξασφαλίσουμε ότι το κλειδί ανταλλάσσεται μεταξύ των δύο τμημάτων που θέλουν να επικοινωνήσουν και όχι μεταξύ αντιπάλων.

Κατά καιρούς έχουν παρουσιαστεί πολλές τεχνικές εγκατάστασης και διαχείρισης κλειδιού. Και όταν αναφέρουμε τον όρο διαχείριση κλειδιού δεν εννοούμε μόνο την εγκατάσταση κλειδιού σε δύο επικοινωνούντες κόμβους αλλά και την ανάκληση, την επανεγκατάσταση κλειδιού και την προσθήκη και αφαίρεση κόμβων.

Ένα ενδιαφέρον σχήμα στο οποίο στηρίχθηκαν και άλλες τεχνικές είναι το πρωτόκολλο LEAP (*Localized Encryption and Authentication Protocol*) [42]. Σ' αυτό το σχήμα χρησιμοποιούνται τέσσερα διαφορετικά είδη κλειδιών ανάλογα με ποιόν επικοινωνεί ο κάθε κόμβος. Οι κόμβοι φορτώνονται αρχικά με κλειδιά τα οποία στη συνέχεια σβήνονται (μετά τη χρήση τους). Επίσης, στο πρωτόκολλο PIKE [83] περιγράφεται ένας μηχανισμός για την εγκατάσταση κλειδιού μεταξύ δύο κόμβων που στηρίζεται στην κοινή εμπιστοσύνη ενός τρίτου κόμβου μέσα στο δίκτυο. Έτσι, το πρωτόκολλο εγκατάστασης κλειδιού μπορεί να δρομολογηθεί μέσω του τρίτου κόμβου.

Μια ενδιαφέρουσα τεχνική είναι η χρήση υβριδικών τεχνικών για την εγκατάσταση κλειδιού [84,85]. Οι υβριδικές τεχνικές στηρίζονται στο γεγονός ότι υπάρχουν μέσα στο δίκτυο κόμβοι που έχουν μεγαλύτερες υπολογιστικές και ενεργειακές δυνατότητες από τους υπολοίπους. Έτσι είναι πιθανόν, κατά την εγκατάσταση κλειδιού μεταξύ κόμβων με αυξημένες δυνατότητες, να χρησιμοποιείται ένα πιο «βαρύ» πρωτόκολλο από πλευράς ασφάλειας και υπολογιστικών αναγκών, ενώ για την εγκατάσταση κλειδιού με απλούς κόμβους να χρησιμοποιείται άλλο πρωτόκολλο.

Κατά την εγκατάσταση κλειδιού υποτίθεται ότι οι κόμβοι δεν μπορούν να δεχθούν επίθεση. Αυτή είναι μια ασθενής υπόθεση καθόσον οι κόμβοι δεν είναι ανθεκτικοί λόγω των φυσικών περιορισμών τους. Επιπλέον, εάν ένας κόμβος εκτεθεί κατά την αρχική φάση, τότε μπορεί να χρησιμοποιηθεί το δημόσιο κλειδί του για να εκθέσει οποιοδήποτε άλλο κόμβο. Τέλος, επειδή εφαρμόζεται μόνο συμμετρική κρυπτογράφηση, οι κόμβοι δεν μπορούν να αποδείξουν τη συμμετοχή τους σε μία εισερχόμενη γενιά κόμβων. Έτσι, ορισμένοι κακόβουλοι κόμβοι μπορούν να προσποιηθούν ότι ανήκουν σε μια άλλη γενιά.

Παρόλο που η κρυπτογραφία δημόσιου κλειδιού είναι πολύ ενεργοβόρα για τους κόμβους ενός δικτύου, πρόσφατες έρευνες απέδειξαν ότι είναι πιθανό να δημιουργηθούν κόμβοι ικανοί να εκτελέσουν περιορισμένα πρωτόκολλα δημόσιου κλειδιού (κυρίως μέσω Κρυπτογραφίας Ελλειπτικών Καμπύλων) [86]. Για να μειωθεί ο αριθμός των «ακριβών» πολλαπλασιασμών, προτείνεται σε πολλές περιπτώσεις η ανάπτυξη ορισμένων πλήρως λειτουργικών συσκευών στο δίκτυο που θα εκτελούν το μεγαλύτερο μέρος των κρυπτογραφικών πράξεων [84].

Τελικά, η εγκατάσταση κλειδιού αποτελείται σχεδόν σε όλα τα πρωτόκολλα από δύο κύριες φάσεις. Την φάση πριν την ανάπτυξη του δικτύου, κατά την οποία φορτώνονται όλοι οι κόμβοι του δικτύου με τις απαραίτητες πληροφορίες του κλειδιού κρυπτογράφησης οι οποίες μετά την εγκατάσταση του κλειδιού σβήνονται για να αποφευχθεί ενδεχόμενη απόκτησή τους από κάποιον εισβολέα και την φάση εγκατάστασης του κλειδιού, κατά την οποία δύο κόμβοι θα χρησιμοποιήσουν τις

αρχικές πληροφορίες (της προηγούμενης φάσης) για να εγκαταστήσουν ένα πιστοποιημένο κλειδί κρυπτογράφησης. Με την εγκατάσταση του κλειδιού γίνεται δυνατή και η διαχείρισή του. Έτσι οι εργασίες της ανάκλησης, της επανεγκατάστασης κλειδιού και της προσθήκης και αφαίρεσης κόμβων εκτελούνται ανάλογα με την ανάγκη.

Η εγκατάσταση και διαχείριση κλειδιού είναι μια βασική εργασία για τους κόμβους γιατί εξασφαλίζουν τη σταθερότητα των εργασιών τους από άποψη ασφαλείας. Με την ορθή ανταλλαγή των κλειδιών κρυπτογράφησης εξασφαλίζεται ότι τα μηνύματα που θα ανταλλάσουν δύο κόμβοι θα είναι κρυπτογραφημένα χωρίς την πιθανότητα απόκτησής τους από τρίτο κακόβουλο κόμβο.

4.5.8 Κρυπτογραφία ελλειπτικών καμπυλών (Elliptic Curve Cryptography), πρωτόκολλο ECDH (Elliptic Curve Diffie Hellmann) και αλγόριθμος ECDSA (Elliptic Curve Digital Signature Algorithm)

Οι Ελλειπτικές Καμπύλες παριστάνονται γενικά με μία από τις ακόλουθες εξισώσεις:

$$y^2 + xy = x^3 + a_2x^2 + a_6 \text{ και } y^2 + y = x^3 + a_4x + a_6$$

με τις σταθερές να είναι πολυώνυμα ή φυσικοί αριθμοί [87]. Τα σημεία των ελλειπτικών καμπυλών αναγνωρίζονται από τις συντεταγμένες τους [P(x,y)]. Η πρόσθεση και ο διπλασιασμός των σημείων είναι απαραίτητα στην αριθμητική των ελλειπτικών καμπυλών και παράγουν ένα τρίτο σημείο: $P(x_3,y_3)=P(x_1,y_1)+P(x_2,y_2)$ και $P(x_3,y_3)=2P(x_1,y_1)$.

Μία ελλειπτική καμπύλη ορίζεται με τις παραμέτρους $(a_2,a_6,P(x,y),n)$ όπου P(x,y) είναι ένα σημείο της καμπύλης (σημείο βάσης) και n ένας πρώτος αριθμός που αναφέρεται στη διάταξη του σημείου. Στην κρυπτογραφία ελλειπτικών καμπυλών (*Elliptic Curve Cryptography*), τα επικοινωνούντα μέρη χρησιμοποιούν ένα ζεύγος δημόσιου-ιδιωτικού κλειδιού, όπου το ιδιωτικό κλειδί k είναι μυστικό και το δημόσιο κλειδί είναι το σημείο K=kP(x,y). Κατά την αποστολή ενός μηνύματος, ο αξιόπιστος κόμβος A θέτει μία τυχαία τιμή r και ζητά το δημόσιο σημείο του B, B=bP. Έπειτα ο A υπολογίζει το τυχαίο σημείο R=rP και το μυστικό κλειδί S=rB. Η x-συνιστώσα του S χρησιμεύει για να παραχθεί ένα κλειδί εφαρμόζοντας μία παράγωγο συνάρτηση κλειδιού και στο αποτέλεσμα εφαρμόζουμε XOR με το μήνυμα που θα κρυπτογραφηθεί. Το μήνυμα στέλνεται στον B με το τυχαίο σημείο R. Ο B αποκρυπτογραφεί το μήνυμα υπολογίζοντας το ίδιο διαμοιραζόμενο μυστικό κλειδί S=bR.

Το πρωτόκολλο Diffie Hellmann μπορεί να χρησιμοποιηθεί για να δημιουργήσει και να εγκαταστήσει ένα διαμοιραζόμενο κοινό μυστικό μεταξύ δύο επικοινωνούντων μερών. Η εκδοχή του συγκεκριμένου πρωτοκόλλου με τη χρήση των ελλειπτικών καμπυλών θεωρεί μία δημόσια γνωστή ελλειπτική καμπύλη της οποίας οι παράμετροι $(a_2,a_6,P(x,y),n)$ είναι γνωστές σε έναν επιτιθέμενο. Δύο αξιόπιστοι κόμβοι A και B παράγουν τους αντίστοιχους μυστικούς αριθμούς w_A και w_B και υπολογίζουν τα δημόσια κλειδιά ως εξής:

$$\textbf{A: } W_A = w_A\,P(x,y) \quad \text{και} \quad \textbf{B: } W_B = w_B\,P(x,y)$$

Οι δύο κόμβοι ανταλλάσουν τα δημόσια κλειδιά και μπορούν να υπολογίσουν το ίδιο κοινό διαμοιραζόμενο μυστικό από το οποίο μπορεί να παραχθεί μια μάσκα ενός bit, χρησιμοποιώντας μία παράγωγο συνάρτηση κλειδιού:

$$\mathbf{A:}\ S_{AB} = w_A W_B = w_A w_B P(x, y) = w_B w_A P(x,y)$$
$$\mathbf{B:}\ S_{BA} = w_B W_A = w_B w_A P(x, y) = w_A w_B P(x,y)$$

Κάθε επιτιθέμενος βλέπει μόνο τις τιμές w_A και w_B αλλά δεν μπορεί να υπολογίσει το μυστικό κλειδί $S_{AB} = S_{BA}$ εξ' αιτίας του προβλήματος του διακριτού λογαρίθμου των ελλειπτικών καμπυλών.

Ο αλγόριθμος ψηφιακής υπογραφής με τη χρήση ελλειπτικών καμπυλών (*Elliptic Curve Digital Signature Algorithm*) χρησιμεύει για την επαλήθευση της γνησιότητας ενός μηνύματος που μεταφέρεται μεταξύ δύο επικοινωνούντων μερών. Σ' αυτόν τον αλγόριθμο, το δημόσιο κλειδί του υπογράφοντος χρησιμοποιείται από τον παραλήπτη για να επαληθεύσει ότι το μήνυμα που μεταφέρθηκε στάλθηκε από τον ίδιο τον υπογράφοντα που κατέχει το αντίστοιχο μυστικό κλειδί. Η παραγωγή της ψηφιακής υπογραφής για έναν κόμβο Α με το ζεύγος δημόσιου-ιδιωτικού κλειδιού (W_A,w_A) προϋποθέτει την εκτέλεση των ακόλουθων τεσσάρων βημάτων χρησιμοποιώντας τις παραμέτρους των ελλειπτικών καμπυλών $(a_2,a_6,P(x,y),n)$:

1. Παράγεται μία τυχαία τιμή r modulo n και υπολογίζεται το τυχαίο σημείο $R(x_R,y_R) = r\,P(x,y)$.
2. Η πρώτη συνιστώσα της υπογραφής είναι: $s_1 = x_R \pmod n$.
3. Υπολογίζεται η συνάρτηση κατατεμαχισμού (hash function) του μηνύματος: h=Hash(message).
4. Η δεύτερη συνιστώσα της υπογραφής είναι: $s_2 = (h+s_1 w_A)/r \pmod n$

Οι υπογραφές μεταφέρονται με το μήνυμα στον κόμβο Β, ο οποίος έχει ήδη στην κατοχή του το δημόσιο κλειδί του Α. Ο Β μπορεί έπειτα να επαληθεύσει ότι το μήνυμα έχει όντως σταλεί από τον Α ως εξής:

1. Υπολογίζεται η συνάρτηση κατατεμαχισμού (hash function) του μηνύματος: h΄=Hash(message).
2. Υπολογίζονται τα: $u=h'/s_2 \pmod n$ και $\upsilon=s_1/s_2 \pmod n$.
3. Υπολογίζεται το σημείο στην ελλειπτική καμπύλη: $N(x_N,y_N) = uP + \upsilon W_A$
4. Εάν $x_N \pmod n = s_1$ τότε η υπογραφή έχει επαληθευτεί και έχει πιστοποιηθεί η γνησιότητα του μηνύματος.

4.5.9 Υβριδική εγκατάσταση κλειδιού για πολλαπλών-φάσεων αυτό-οργανωμένα (χωρίς υποδομή) δίκτυα αισθητήρων

Είναι σήμερα εφικτό να εφαρμόσουμε περιορισμένη κρυπτογραφία ελλειπτικών καμπυλών στα δίκτυα αισθητήρων με τη χρήση υβριδικών πρωτοκόλλων. Το προτεινόμενο πρωτόκολλο που αναπτύσσεται στο [85] συνδυάζει την εγκατάσταση κλειδιού *Elliptic Curve Diffie Hellmann* με αφανή πιστοποιητικά (*implicit certificates*) και κρυπτογραφικές τεχνικές συμμετρικού κλειδιού. Το συγκεκριμένο πρωτόκολλο μπορεί να εφαρμοστεί σε ομοιόμορφα δίκτυα που συνίστανται

αποκλειστικά από συσκευές περιορισμένης λειτουργίας, σε αντίθεση με τα μη-ομοιόμορφα δίκτυα όπου υπάρχουν και συσκευές πλήρους λειτουργίας (υψηλής ενέργειας, ισχύος και δυνατοτήτων αποθήκευσης). Λόγω της φύσεως του δημοσίου κλειδιού του πρωτοκόλλου, αυτό είναι ευπροσάρμοστο σε μια ευρεία γκάμα παθητικών και ενεργητικών επιθέσεων όπως επιθέσεις 'γνωστού-κλειδιού' και επιθέσεις ενάντια στην εμπιστευτικότητα, την ακεραιότητα και την αυθεντικότητα της επικοινωνίας. Το πρωτόκολλο είναι προσαρμόσιμο και αποτελεσματικό για συσκευές χαμηλών δυνατοτήτων σε θέματα αποθήκευσης, επικοινωνίας και υπολογιστικής πολυπλοκότητας. Το κόστος ανά κόμβο για μία εγκατάσταση κλειδιού περιορίζεται σε έναν βαθμωτό-μονόμετρο πολλαπλασιασμό με ένα τυχαίο σημείο συν έναν με ένα σταθερό σημείο.

Κάθε ομάδα από εισερχόμενους στο δίκτυο κόμβους σε κάποια μελλοντική στιγμή αποτελεί μία γενιά κόμβων (node generation). Αυτό συμβαίνει όταν πρόκειται να επεκταθεί το δίκτυο ή να αντικατασταθούν εσφαλμένοι κόμβοι. Τα πρωτόκολλα που επιτρέπουν πολλαπλές φάσεις επανεκκίνησης κλειδιού (*key bootstrapping*) μεταξύ κόμβων διαφορετικών γενεών, είναι γνωστά ως πρωτόκολλα ανάπτυξης πολλαπλών φάσεων (*multiphase deployment protocols*). Η κρυπτογραφία συμμετρικού κλειδιού φαίνεται να είναι η πιο αποτελεσματική επιλογή για την εγκατάσταση κλειδιού πολλαπλών φάσεων στα DSN. Σε διάφορα σχήματα που έχουν προταθεί, όλοι οι κόμβοι που ανήκουν σε μία συγκεκριμένη γενιά i είναι προ-εγκατεστημένοι με ένα συμμετρικό κλειδί K_i, το οποίο θα χρησιμοποιήσουν κατά τη διάρκεια της i-οστής περιόδου επανεκκίνησης κλειδιού μεταξύ τους. Κάθε κόμβος A που ανήκει στην i-οστή γενιά είναι επίσης προ-εγκατεστημένος με ένα διαφορετικό 'στιγμιότυπο' των κλειδιών μελλοντικής γενιάς, που συνδέεται με την μοναδική ταυτότητά του ID_A,

$$\boldsymbol{K_{i+1}(ID_A) = f_{K_{i+1}}[ID_A] \ldots\ldots K_m(ID_A) = f_{K_m}[ID_A]}$$

όπου f είναι μία μονόδρομα 'κλειδωμένη' συνάρτηση κατατεμαχισμού (hash function) και m είναι ο συνολικός αριθμός των γενεών. Κάθε ένα από αυτά τα κλειδιά χρησιμοποιείται από τον κόμβο για να συμμετάσχει στη μελλοντική φάση επανεκκίνησης και στο τέλος κάθε τέτοιας περιόδου όλοι οι κόμβοι διαγράφουν τα κλειδιά της γενιάς τους. Σε όλα αυτά τα σχήματα προϋποτίθεται ότι οι κόμβοι δεν θα δεχθούν επίθεση κατά τη διάρκεια των φάσεων επανεκκίνησης. Αυτή είναι μια ισχυρή παραδοχή λόγω και των φυσικών περιορισμών των κόμβων. Εάν ένας κόμβος ενδώσει κατά τη διάρκεια της περιόδου επανεκκίνησης, τότε μπορεί να χρησιμοποιήσει το χαρακτηριστικό κλειδί της γενιάς για να υποδυθεί οποιονδήποτε άλλο κόμβο, μια επίθεση γνωστή ως σιβυλλική.

Κατά παρόμοιο τρόπο, οι κόμβοι δεν μπορούν να αποδείξουν τη συμμετοχή τους σε μία συγκεκριμένη γενιά από τη στιγμή που εφαρμόζονται μόνο συμμετρικές τεχνικές κρυπτογράφησης. Έτσι, τα πρωτόκολλα αυτά γίνονται αντικείμενα σε επιθέσεις πλαστογράφησης της γενιάς (fake generation): διεφθαρμένοι κόμβοι προσποιούνται ότι ανήκουν σε διαφορετική γενιά από την πραγματική.

Το προτεινόμενο πρωτόκολλο βελτιώνει τα ήδη προταθέντα επί του θέματος σχήματα, αφού δεν επιτρέπει ένα συμβιβασμένο κόμβο να υποδυθεί άλλους κόμβους που ανήκουν στην ίδια ή σε διαφορετική γενιά. Επιπλέον παρέχει πρόσθετη μυστικότητα σε έναν μοναδικό κόμβο όσο και σε μία γενιά από κόμβους. Δεν απαιτεί την παραδοχή μιας προστατευμένης περιόδου επανεκκίνησης, αν και εφόσον υπάρχει μία τέτοιου είδους προστασία, η ασφάλεια του πρωτοκόλλου αυξάνεται περισσότερο. Τέλος, το συγκεκριμένο πρωτόκολλο υποστηρίζει την ανάπτυξη σε πολλές φάσεις και δεν απαιτεί την ύπαρξη συσκευών πλήρους λειτουργίας.

4.5.9.1 Συμβολισμοί και φάση προ-ανάπτυξης

Πριν την αρχικοποίηση του δικτύου, μία αξιόπιστη αρχή CA προ-εγκαθιστά σε κάθε κόμβο-αισθητήρα τα κατάλληλα EC και συμμετρικά κλειδιά. Οι κόμβοι αναπτύσσονται τυχαία (π.χ. με εναέρια διασπορά) και δεν είναι γνώστες των γειτόνων τους μέχρι την ανάπτυξή τους. Έπειτα οι κόμβοι συμμετέχουν σε μια φάση επανεκκίνησης κλειδιού ώστε να αλλάξουν κλειδιά με τους γειτονικούς κόμβους. Μετά την αρχικοποίηση του δικτύου είναι δυνατόν στο μέλλον νέοι κόμβοι να εισέλθουν στο δίκτυο με την προϋπόθεση ότι είναι εφοδιασμένοι (από την CA) με τα αντίστοιχα κλειδιά της γενιάς.

Ας θεωρήσουμε q την τάξη του υποκείμενου πεπερασμένου επιπέδου F_q και E μία κατάλληλα επιλεγμένη ελλειπτική καμπύλη που ορίζεται στο F_q. Το P είναι ένα σημείο βάσης στην E, το σημείο-γεννήτρια, και n είναι η τάξη του P, όπου n είναι πρώτος αριθμός. Έτσι nP=O και P≠O, όπου O είναι το σημείο στο άπειρο. Θεωρούμε $q_{CA} \in [2,n-2]$ έναν τυχαίο ακέραιο που επιλέχθηκε από την CA και $Q_{CA} = q_{CA} \times P$. Το ζεύγος των στατικών κλειδιών (κρυφό/δημόσιο) της CA είναι τα q_{CA} και Q_{CA}.

Η αρχή πιστοποίησης (CA) παράγει ένα συμμετρικό κλειδί K για όλο το δίκτυο το οποίο θα χρησιμοποιηθεί από όλους τους κόμβους σαν ένας αρχικός αυθεντικοποιητής (επαληθευτής ταυτότητας), ώστε να αποφευχθεί η επεξεργασία πλαστών 'hello' μηνυμάτων και να αποτραπούν ασήμαντες επιθέσεις DoS. Η CA παράγει επίσης έναν αριθμό από ανεξάρτητα συμμετρικά κλειδιά κρυπτογράφησης $K_1, K_2, \ldots, K_m$, ένα κλειδί για κάθε γενιά κόμβων.

Η CA παράγει και εφοδιάζει κάθε κόμβο με την κατάλληλη πληροφορία κλειδιών. Έστω ο κόμβος X της γενιάς i που συμβολίζεται με $X^{(i)}$ ή πιο απλά X. Η CA επιλέγει ένα τυχαίο αριθμό $g_x \in [2,n-2]$ και υπολογίζει το $G_x = g_x \times P$. Έπειτα η CA υπολογίζει το αφανές πιστοποιητικό (Implicit Certificate) για τον κόμβο X ως εξής: $IC_x=(G_x,M)$, με το M να είναι $M=\{i, ID_x, t_x\}$, όπου i είναι η γενιά του κόμβου, ID_x ένα μοναδικό αναγνωριστικό για τον κόμβο X και t_x είναι ο χρόνος λήξης του πιστοποιητικού. Η CA εφαρμόζει μία κρυπτογραφική hash function (h) στο IC_x και από την τιμή $h(IC_x)$ παίρνει έναν ακέραιο e_x. Μετά η CA υπολογίζει το στατικό μυστικό κλειδί $q_x = g_x + e_x \cdot q_{CA}$. Η τιμή g_x δεν δίνεται στον κόμβο X και διαγράφεται με το πέρας της όλης διαδικασίας παραγωγής κλειδιού. Διαφορετικά, ένας συμβιβασμένος κόμβος θα ήταν σε θέση να εξάγει το μυστικό κλειδί του CA από τις τιμές q_x και g_x. Το αντίστοιχο δημόσιο κλειδί Q_x δεν αποθηκεύεται στη μνήμη του κόμβου X. Οποιοσδήποτε άλλος κόμβος θα είναι σε θέση να αντλήσει το Q_x από το IC_x και το δημόσιο κλειδί Q_{CA} από την CA.

Συνολικά, η CA προ-εφοδιάζει τον κόμβο X με τα εξής:

- Το μυστικό κλειδί q_x
- Το implicit certificate IC_x
- Το δημόσιο κλειδί της CA, Q_{CA}
- Το σημείο P
- Το αρχικό κλειδί αυθεντικοποίησης K
- Το κλειδί της i-οστής γενιάς K_i
- Τα στιγμιαία κλειδιά K_{i+1} (ID_X), K_{i+2} (ID_X), …, K_m (ID_X), τα οποία υπολογίζονται με την χρήση της συναρτήσεως κατατεμαχισμού f, όπως αναφέρθηκε στο προηγούμενο κεφάλαιο.

4.5.9.2 Φάση εγκατάστασης κλειδιού (Key establishment phase)

Σ' αυτή τη φάση, δύο κόμβοι θα χρησιμοποιήσουν τα ήδη εγκατεστημένα σε αυτούς κλειδιά για να εκτελέσουν μεταξύ τους μια πιστοποιημένη εγκατάσταση κλειδιού. Ας θεωρήσουμε $A^{(j)}$ και $B^{(i)}$ δύο κόμβους που ανήκουν στις γενιές j και i αντίστοιχα, με $1 \leq j \leq i \leq m$. Έτσι οι κόμβοι μπορούν να ανήκουν στην ίδια (j=i) ή διαφορετική γενιά (j<i).

Κατά την φάση εγκατάστασης κλειδιού της i-οστής περιόδου και οι δύο κόμβοι θα κατέχουν αρχικά το i-οστής γενιάς κλειδί ή ένα στιγμιότυπο αυτού. Αν j=i, τότε και οι δύο κόμβοι κατέχουν το κλειδί K_i, ή διαφορετικά, αν j<i, τότε ο κόμβος $A^{(j)}$ θα έχει εφοδιαστεί με το στιγμιότυπο $K_i(ID_A)$ του i-οστής γενιάς κλειδιού K_i.

Ο κόμβος $B^{(i)}$ αρχικοποιεί την όλη διαδικασία επιλέγοντας έναν τυχαίο για την περίσταση αριθμό N_B και τον μεταδίδει με το IC_B. Επίσης εκπέμπει έναν MAC (*Message Authentication Code*) των παραπάνω τιμών που παράγεται με το αρχικό κλειδί K. Ο κόμβος Α λαμβάνει και επαληθεύει τον MAC και εάν η επαλήθευση είναι επιτυχής, επιλέγει έναν τυχαίο αριθμό r_A.

Για να προστατευθεί η τυχαία αυτή τιμή από πιθανή υποκλοπή, ο κόμβος Α παράγει ένα προσωρινό κλειδί $\bar{K}_{AB}$ με το οποίο κρυπτογραφεί τον r_A ως εξής: $\bar{K}_{AB} = f_{Ki(IDA)}[ID_B]$. Έπειτα ο Α στέλνει την κρυπτογραφία $E_{\bar{K}_{AB}}[r_A]$ στον Β μαζί με το IC_A και έναν MAC ως συνάρτηση των IC_A, r_A, N_B που παράγεται με το κλειδί $K_i(ID_A)$.

Λαμβάνοντας αυτό το μήνυμα, ο κόμβος Β υπολογίζει το κλειδί $K_i(ID_A)$ χρησιμοποιώντας το κλειδί K_i. Εάν έπειτα επαληθεύσει ορθά τον ληφθέντα MAC, υπολογίζει το προσωρινό κλειδί $\bar{K}_{AB}$ χρησιμοποιώντας αυτή τη φορά το ήδη υπολογισμένο κλειδί $K_i(ID_A)$. Ο Β αποκρυπτογραφεί το $E_{\bar{K}_{AB}}[r_A]$ και ανακτά τον r_A. Επιλέγει επίσης μία τυχαία τιμή r_B και την κρυπτογραφεί με το προσωρινό κλειδί $\bar{K}_{AB}$.

Τώρα ο κόμβος Β θα χρησιμοποιήσει το ληφθέν IC_A και το δημόσιο κλειδί Q_{CA} για να υπολογίσει το δημόσιο κλειδί του Α ως εξής: $Q_A = G_A + e_A \times Q_{CA}$. Σ' αυτό το σημείο ο Β δεν είναι ακόμη σε θέση να επιβεβαιώσει ότι το Q_A είναι γνήσιο.

Ο Β υπολογίζει το στατικό κλειδί του ζεύγους $Z_{AB} = q_B \times Q_A$. Το τελικό κλειδί K_{AB} υπολογίζεται εφαρμόζοντας μία παράγωγο συνάρτηση κλειδιού στο Z_{AB} και στο SharedInfo, όπου SharedInfo= r_A, r_B δηλ. $K_{AB}=kdf(Z_{AB},SharedInfo)$. Έπειτα ο Β υπολογίζει έναν MAC (ως συνάρτηση των r_A, r_B) με το κλειδί K_{AB} και στέλνει στον Α τα $E_{\bar{K}_{AB}}[r_B]$, $MAC_{KAB}[r_A, r_B]$. Ο MAC θα παρέχει επιβεβαίωση κλειδιού στον Α από τη στιγμή που θα αποδείξει ότι χρησιμοποιήθηκε το αντίστοιχο μυστικό κλειδί q_B.

Ο Α αποκρυπτογραφεί το $E_{\bar{K}_{AB}}[r_B]$ και ανακτά τον r_B. Έπειτα χρησιμοποιεί το K_B και το δημόσιο κλειδί Q_{CA} για να υπολογίσει το δημόσιο κλειδί του Β ως εξής: $Q_B = G_B + e_B \times Q_{CA}$. Σ' αυτό το σημείο ο Α δεν είναι βέβαιος για την γνησιότητα του Q_B. Η γνησιότητα αυτού του κλειδιού θα επιβεβαιωθεί μόνο όταν ο Α επιβεβαιώσει τη γνώση του Β για το αντίστοιχο μυστικό κλειδί q_B.

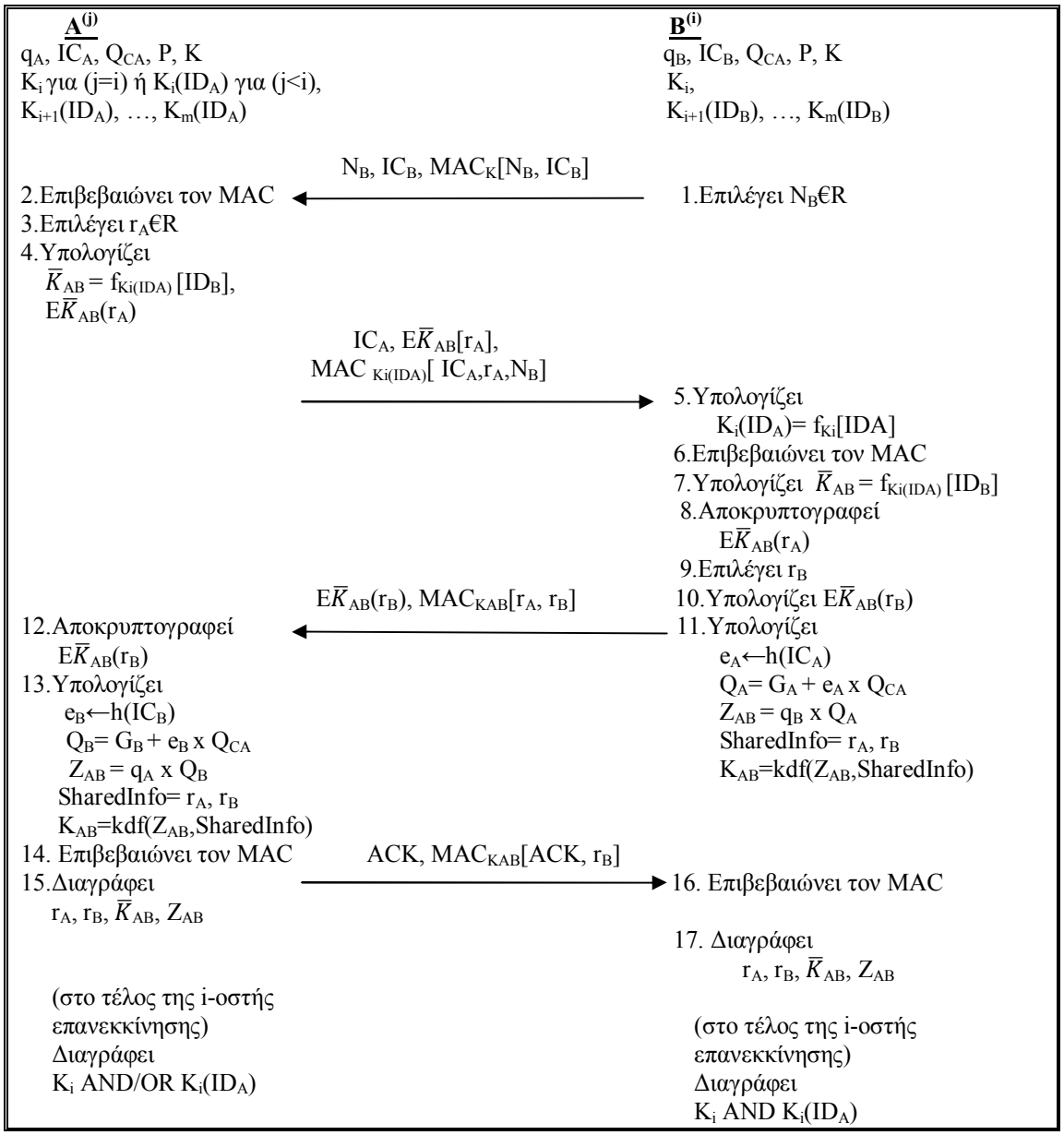
Ο κόμβος Α υπολογίζει το στατικό κλειδί του ζεύγους $Z_{AB} = q_A \times Q_B$ και το $K_{AB}=kdf(Z_{AB},SharedInfo)$, όπου SharedInfo= r_A, r_B. Τώρα ο Α θα επαληθεύσει τον ληφθέντα MAC ώστε να επιβεβαιώσει ότι στον υπολογισμό του K_{AB} χρησιμοποιήθηκε το κατάλληλο μυστικό κλειδί του κόμβου Β.

Για να παρέχει ο Α επιβεβαίωση κλειδιού ως αναφορά στο δικό του μυστικό κλειδί q_A, θα υπολογίσει έναν MAC με το κλειδί K_{AB} και θα το στείλει στον Β. Μετά την επαλήθευση, και οι δύο κόμβοι θα διαγράψουν τις τυχαίες τιμές r_A, r_B και το προσωρινό κλειδί $\bar{K}_{AB}$ και θα χρησιμοποιούν το K_{AB} για την επικοινωνία. Επίσης, οι

κόμβοι μπορούν περιοδικά να ανανεώνουν το κοινό κλειδί με μία μονόδρομη συνάρτηση κατατεμαχισμού και με τον χρόνο μεταξύ διαδοχικών ανανεώσεων να εξαρτάται από τον όγκο των δεδομένων που κυκλοφορούν και από την αντοχή των υποκείμενων κρυπτογραφικών αρχών.

Στο τέλος της i-οστής φάσης επανεκκίνησης και αφού οι κόμβοι έχουν εκτελέσει την εγκατάσταση κλειδιού με καθένα από τους γείτονές τους, θα διαγράψουν το κλειδί της γενιάς K_i και/ή τα κλειδιά $K_i(ID_A)$, $K_i(ID_B)$ που κατέχουν. Στην επόμενη φάση επανεκκίνησης ο Α (αντ. Β) θα χρησιμοποιήσει το μυστικό στατικό κλειδί q_A (αντ. q_B) όπως επίσης το στιγμιότυπό του από το κλειδί της επόμενης γενιάς K_{i+1} (ID_A) (αντ. K_{i+1} (ID_B)) για να συμμετάσχει στη φάση επανεκκίνησης με τους κόμβους της γενιάς i+1.

Ο αλγόριθμος για την εγκατάσταση κλειδιού δίνεται καλύτερα παρακάτω στο Σχήμα 22.



Σχήμα 22. Η φάση εγκατάστασης κλειδιού.

4.5.9.3 Ανάλυση ασφάλειας

Το προτεινόμενο πρωτόκολλο επεκτείνει την σύμβαση ECDH κατανέμοντας κατά τυχαίο τρόπο την γενιά κλειδιού ώστε να παρέχει προστασία από επιθέσεις ασφαλείας γνωστού κλειδιού. Πρόκειται για ένα υβριδικό πρωτόκολλο με το 'συμμετρικό' μέρος του να είναι μία τεσσάρων τμημάτων συνδιαλλαγή με αναγνώριση ταυτότητας, όπου γίνεται χρήση τυχαίων στιγμιαίων τιμών για το 'φρεσκάρισμα' μηνύματος, συμμετρική κρυπτογράφηση για αξιοπιστία δεδομένων και των MAC (κωδικών) για ακεραιότητα δεδομένων.

Το 'δημόσιο' μέρος του πρωτοκόλλου περιέχει τη σύμβαση ECDH σε συνδυασμό με αφανή πιστοποιητικά (IC) για αμοιβαία πιστοποίηση. Το μοντέλο αντιμετωπίζει τόσο παθητικούς όσο και ενεργητικούς επιτιθέμενους. Οι μεν πρώτοι παρακολουθούν ολόκληρο το δίκτυο και επιτελούν κρυπταναλυτικές επιθέσεις με στόχο την υποκλοπή επικοινωνίας, οι δε δεύτεροι μπορούν να εισάγουν ψευδή μηνύματα και να συμβιβάσουν έναν κόμβο για να συλλέξουν όλα τα αποθηκευμένα κλειδιά και την εντοπισμένη πληροφορία.

Χρησιμοποιώντας μία ιδιωτική διεπαφή χωρίς σύνδεση ανάμεσα σε κάθε κόμβο αισθητήρα και την CA, ματαιώνεται κάθε ενεργητική ή παθητική επίθεση ενάντια στη διαδικασία παραγωγής κλειδιού, με την προϋπόθεση ότι η CA είναι αξιόπιστη και λαμβάνει όλα τα απαραίτητα μέτρα. Μόνο εάν τόσο το κλειδί της γενιάς K_i (ή το στιγμιότυπο $K_i(ID_A)$) όσο και το μυστικό κλειδί q_A του κόμβου A ενδώσουν, τότε και μόνο τότε το παραγόμενο κλειδί του ζεύγους K_{AB} συμβιβάζεται. Με το παρόν πρωτόκολλο παρέχεται ασφάλεια ενάντια στον συμβιβασμό του κλειδιού K_i και του μυστικού κλειδιού q_A, ώστε να μην υπάρξει καμία περίπτωση να ενδώσουν και τα δύο ταυτόχρονα.

Στην πρώτη περίπτωση, εάν ένα κλειδί K_i συμβιβαστεί, τότε όλα τα προσωρινά κλειδιά $\overline{K}_{AB}$ θα συμβιβαστούν και κατά συνέπεια θα αποκαλυφθούν οι τυχαίες τιμές r_A και r_B. Το ζητούμενο όμως κλειδί K_{AB} βασίζεται και στο στατικό ECDH κλειδί Z_{AB}, το οποίο παράγεται μόνο μία φορά κατά τη φάση εγκατάστασης κλειδιού και αμέσως μετά διαγράφεται. Επίσης το Z_{AB} δεν χρησιμοποιείται ποτέ για κρυπτογράφηση ώστε να μπορεί να ανακτηθεί από τον αντίπαλο, ο οποίος το καλύτερο που μπορεί να κάνει είναι να προσπαθήσει να αποκτήσει το κλειδί $K_{AB}=kdf(Z, r_A,r_B)$ για τυχαίες τιμές του Z. Συνεπώς, ο αντίπαλος δεν είναι σε θέση να ανακτήσει το K_{AB} αφού το μήκος του Z_{AB} είναι αρκετά μεγάλο και τα στατικά μυστικά EC κλειδιά των δύο κόμβων δεν έχουν συμβιβαστεί.

Στη δεύτερη περίπτωση, εάν μόνο το κλειδί q_A έχει ενδώσει και το K_i είναι ασφαλές, τότε ο αντίπαλος θα είναι σε θέση να αποκτήσει κάθε στατικό κλειδί ζεύγους αυτού του κόμβου, για παράδειγμα το Z_{AB}. Όμως, δεν θα έχει στη διάθεσή του τις τυχαίες τιμές r_A, r_B (που είναι και επαρκώς μεγάλες), άρα ούτε και το ζητούμενο κλειδί $K_{AB}=kdf(Z_{AB}, r_A,r_B)$.

Για να αποτραπούν οι επιθέσεις μίμησης κόμβου (ασφάλεια ενάντια στην πλαστοπροσωπία), γίνεται χρήση των αφανών πιστοποιητικών (IC). Στο τέλος της φάσης επανεκκίνησης, ο κόμβος A έχει αφανή διαβεβαίωση ότι μιλάει με τον κόμβο B και ότι όλη η πληροφορία που περιλαμβάνεται στο πιστοποιητικό είναι γνήσια (υπογεγραμμένη από την CA). Επίσης, ένας συμβιβασμένος κόμβος δεν μπορεί να παρουσιάσει τον εαυτό του σαν ένα κόμβο μιας προηγούμενης ή μελλοντικής γενιάς αφού – αν συμβεί αυτό – στο βήμα 11 του Σχήματος 22, ο κόμβος B θα κατασκευάσει ένα λανθασμένο δημόσιο κλειδί Q_A και η επιβεβαίωση κλειδιού θα αποτύχει στο βήμα 16 (ασφάλεια ενάντια στις επιθέσεις πλαστογράφησης της γενιάς).

Πρόκειται – γενικά – για ένα πρωτόκολλο που βελτιώνει τα σχήματα που προτείνονται στα [88] και [42], αφού δεν επιτρέπει σε έναν συμβιβασμένο κόμβο να υποδυθεί άλλους κόμβους της ίδιας ή διαφορετικής γενιάς. Επίσης, παρέχει ασφάλεια προς τα εμπρός και δεν προϋποθέτει την παραδοχή μίας προστατευμένης περιόδου επανεκκίνησης (αν και εφόσον υπάρχει, αυξάνεται και η ασφάλεια του πρωτοκόλλου). Τέλος, βελτιώνει και το υβριδικό σχήμα του [84], από τη στιγμή που υποστηρίζει πολυφασική ανάπτυξη και δεν απαιτεί την ύπαρξη πλήρως λειτουργικών συσκευών.

4.5.9.4 Αξιολόγηση επίδοσης

Η αξιολόγηση της επίδοσης του προτεινόμενου πρωτοκόλλου θα γίνει σε σχέση με το υπολογιστικό και επικοινωνιακό κόστος, καθώς και τις απαιτήσεις αποθήκευσης σε σχέση με τα συνολικά κλειδιά που απαιτούνται [85]:

- *Υπολογιστική πολυπλοκότητα*: Για την παραγωγή συγκρίσιμων αποτελεσμάτων με σχετικές προγενέστερες εργασίες, χρησιμοποιούνται τα μετρικά του [84] αναφορικά με το κόστος κάθε κρυπτογραφικής ενέργειας. Η αποτίμηση (evaluation) του τρόπου υπολογισμού του πρωτοκόλλου δείχνει ένα συνολικό κόστος ανά κόμβο περί τα 645 msec το οποίο είναι κατά 20% χαμηλότερο από το κόστος του υβριδικού πρωτοκόλλου του [84] (760 msec). Οι κρυπτογραφικές ενέργειες που αξιολογούνται και ο τρόπος άθροισης ώστε να καταλήξουμε στο τελικό αποτέλεσμα γίνεται ως εξής:

$$\sum_{i=1}^{7} (\text{κόστος ανά ενέργεια (msec) x αριθμό ενεργειών ανά κόμβο})$$

  όπου i είναι η κρυπτογραφική ενέργεια (βαθμωτός πολλαπλασιασμός για τυχαίο και σταθερό σημείο με κόστος 480 και 130 msec αντίστοιχα και μία ενέργεια ανά κόμβο για τον καθένα, συμμετρική κρυπτογράφηση-αποκρυπτογράφηση με 3msec κόστος και 2 ενέργειες ανά κόμβο κ.τ.λ.).
- *Επικοινωνιακή πολυπλοκότητα*: Το προτεινόμενο πρωτόκολλο απαιτεί 4 ανταλλαγές μηνυμάτων για εγκατάσταση κλειδιού με συνολικό κόστος επικοινωνίας τα 1488 bits ή 186 bytes, σχεδόν ίσο με τα 180 bytes που απαιτούνται στο [84].
- *Απαιτήσεις αποθήκευσης*: Θεωρώντας ότι οι κόμβοι είναι προ-εγκατεστημένοι με κλειδιά που επιτρέπουν την επικοινωνία με κόμβους K γενιών, οι συνολικές απαιτήσεις αποθήκευσης είναι $1032 + K \cdot 128$ bits (συγκρίσιμες με το [84]). Για έναν σταθερό αριθμό γενιών, οι ανά κόμβο πηγές αποθήκευσης και ενέργειες δεν περιορίζουν το μέγεθος του δικτύου (μεταβλητού μεγέθους / κλιμακούμενο πρωτόκολλο).

4.5.10 Εγκατάσταση κλειδιού σε πολλαπλά επίπεδα για δίκτυα αισθητήρων μεγάλης κλίμακας με κρυπτογραφία ελλειπτικών καμπυλών

Αν και τα πιο αποτελεσματικά πρωτόκολλα για την εγκατάσταση κλειδιού βασίζονται στην κρυπτογράφηση συμμετρικού κλειδιού, αυτά τα πρωτόκολλα δεν είναι σε θέση να παρέχουν επαρκή ασφάλεια ενάντια σε επιθέσεις όπως η απομίμηση κόμβου ή η πλαστογράφηση της γενιάς του κόμβου. Έτσι αναπτύχθηκαν κάποια υβριδικά πρωτόκολλα εγκατάστασης κλειδιού, τα οποία κάνουν περιορισμένη χρήση της κρυπτογραφίας δημοσίου κλειδιού και πιο συγκεκριμένα της κρυπτογραφίας των Ελλειπτικών Καμπυλών, της οποίας μία περιληπτική περιγραφή έγινε στο προηγούμενο κεφάλαιο. Παρόλο που αυτά τα πρωτόκολλα φαίνεται να είναι αποτελεσματικά για κόμβους-αισθητήρες, μειώνουν την απόδοση, ειδικά σε δίκτυα μεγάλης κλίμακας. Το προτεινόμενο πρωτόκολλο στο [89] συνδυάζει τεχνικές υβριδικής και συμμετρικής εγκατάστασης κλειδιού. Η ανάλυση της επίδοσης δείχνει μία εύλογη μείωσή της που οφείλεται στη βέλτιστη χρήση των ακριβών κρυπτογραφικών λειτουργιών δημοσίου κλειδιού. Το σχήμα αυτό έχει τρία επίπεδα εγκατάστασης κλειδιού. Οι κόμβοι ομαδοποιούνται σε γεωγραφικές περιοχές και όσοι ανήκουν στην ίδια ομάδα χρησιμοποιούν ένα συμμετρικό πρωτόκολλο εγκατάστασης κλειδιού ώστε να ανταλλάσουν τα ανά ζεύγος κλειδιά. Ένας κόμβος ανά ομάδα έχει διευρυμένες δυνατότητες και είναι σε θέση να επικοινωνεί με άλλους κόμβους της κατηγορίας του που βρίσκονται σε γειτονικές ομάδες. Αυτοί οι κόμβοι ανταλλάσουν κλειδιά χρησιμοποιώντας το υβριδικό πρωτόκολλο εγκατάστασης κλειδιού που αναλύθηκε στο προηγούμενο κεφάλαιο. Έτσι, οι συνηθισμένοι κόμβοι που βρίσκονται πολύ μακριά ο ένας από τον άλλον βοηθούνται να αλλάξουν κλειδιά μεταξύ τους με ασφάλεια. Επίσης, η χρήση του υβριδικού πρωτοκόλλου επιτρέπει την ασφαλή πολύ-φασική ανάπτυξη των κόμβων-αισθητήρων.

Με σκοπό τη διατήρηση των πλεονεκτημάτων των υβριδικών πρωτοκόλλων και μία πιο ανεκτή μείωση της επίδοσης, προτάθηκε το σχήμα εγκατάστασης κλειδιού σε πολλά επίπεδα που θα αναλυθεί παρακάτω και όπου γίνεται χρήση τόσο των υβριδικών όσο και των συμμετρικών πρωτοκόλλων (το συμμετρικό από την πλειοψηφία των κόμβων και το υβριδικό από μερικούς επιλεγμένους κόμβους που διαθέτουν μεγαλύτερη ισχύ, υπολογιστική ικανότητα και περισσότερους επικοινωνιακούς πόρους από τους υπολοίπους (clusterheads)).

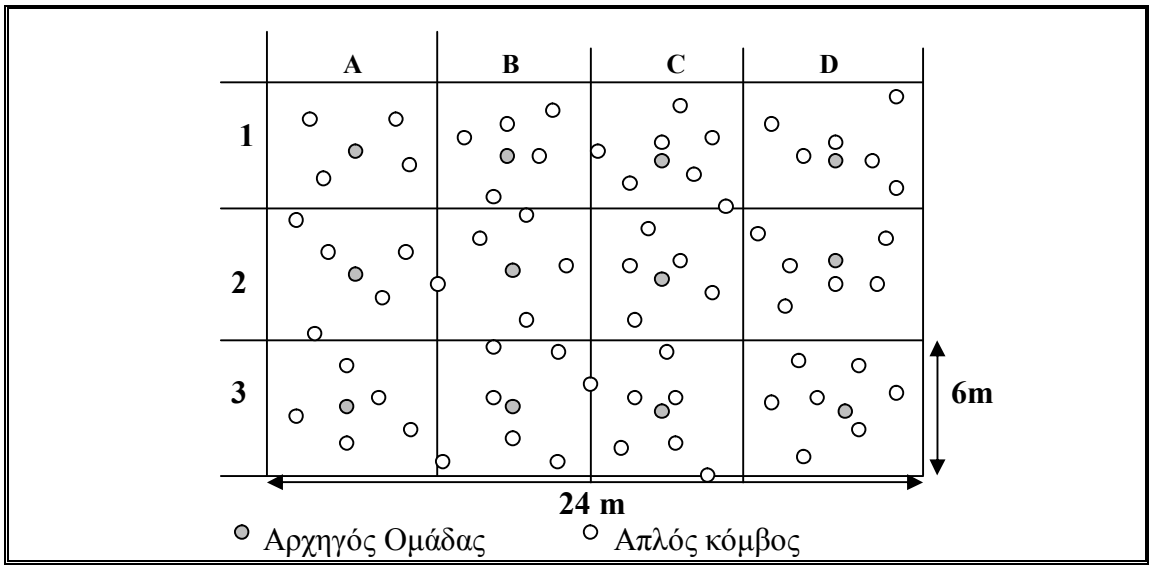
Η εγκατάσταση κλειδιού πραγματοποιείται σε 3 φάσεις που εκτελούνται διαδοχικά η μία μετά την άλλη. Το πρωτόκολλο θεωρεί ότι οι επικεφαλείς των ομάδων (clusterheads) είναι προ-εγκατεστημένοι με τα κατάλληλα κλειδιά (συμμετρικό και ελλειπτικής καμπύλης) και τα πιστοποιητικά ταυτότητας, ενώ οι απλοί κόμβοι μόνο με τα συμμετρικά κλειδιά.

Θεωρούμε ότι το δίκτυο διαιρείται σε ομάδες-συμπλέγματα, π.χ. τετραγωνικές περιοχές με περιορισμένη έκταση, και αποτελείται από επικεφαλείς ομάδων και απλούς κόμβους. Κάθε clusterhead τοποθετείται κατά προσέγγιση στο κέντρο της ομάδας και έχει τη δυνατότητα να επικοινωνεί με τους αρχηγούς ομάδων όλων των γειτονικών κόμβων. Κάθε ομάδα-σύμπλεγμα περιέχει επίσης έναν αριθμό απλών συνηθισμένων κόμβων-αισθητήρων με περιορισμένες δυνατότητες και με εμβέλεια επικοινωνίας περιορισμένη εντός των γεωγραφικών ορίων της ομάδας στην οποία ανήκουν. Επίσης, πριν την αρχικοποίηση της όλης διαδικασίας, όλοι οι κόμβοι έχουν εγκαταστήσει ένα κατάλληλο πρωτόκολλο δρομολόγησης.

Ένα στιγμιότυπο ενός δικτύου με 16 ομάδες φαίνεται στο Σχήμα 23. Θεωρείται ότι κάθε απλός κόμβος ανήκει σε μία και μόνη ομάδα και ότι απαντά μόνο στο πρώτο 'hello' μήνυμα που λαμβάνει από κάποιον clusterhead.

Το προτεινόμενο σχήμα μπορεί να χρησιμοποιηθεί για ανάπτυξη πολλαπλών φάσεων όπου οι κόμβοι ομαδοποιούνται σε γενιές και κάθε γενιά μπορεί να εισέλθει στο δίκτυο σε μια μελλοντική περίοδο (υποστήριξη bootstrapping μεταξύ κόμβων που ανήκουν σε διαφορετικές γενιές).

Μετά την ανάπτυξη των κόμβων και την εγκατάσταση του πρωτοκόλλου δρομολόγησης, η διαδικασία εγκατάστασης κλειδιού ξεκινά σε τρεις διαδοχικές φάσεις.



Σχήμα 23. Δίκτυο 16 ομάδων σε περιοχές των 6x6 (m^2).

4.5.10.1 Φάση $1^{η}$: Εγκατάσταση κλειδιού μεταξύ των επικεφαλής των ομάδων

Στην $1^{η}$ φάση, κάθε clusterhead εγκαθιστά ένα κλειδί με όλους τους γειτονικούς (ενός άλματος) αρχηγούς ομάδων χρησιμοποιώντας το υβριδικό πρωτόκολλο που προτάθηκε στο [85] και αναλύθηκε παραπάνω. Το πρωτόκολλο αυτό εκτελείται για ένα χρονικό διάστημα μόνο από τους αρχηγούς ομάδων, διάστημα κατά το οποίο οι απλοί κόμβοι είναι προγραμματισμένοι να παραμένουν ανενεργοί.

4.5.10.2 Φάση $2^{η}$: Εγκατάσταση κλειδιού στο εσωτερικό των ομάδων

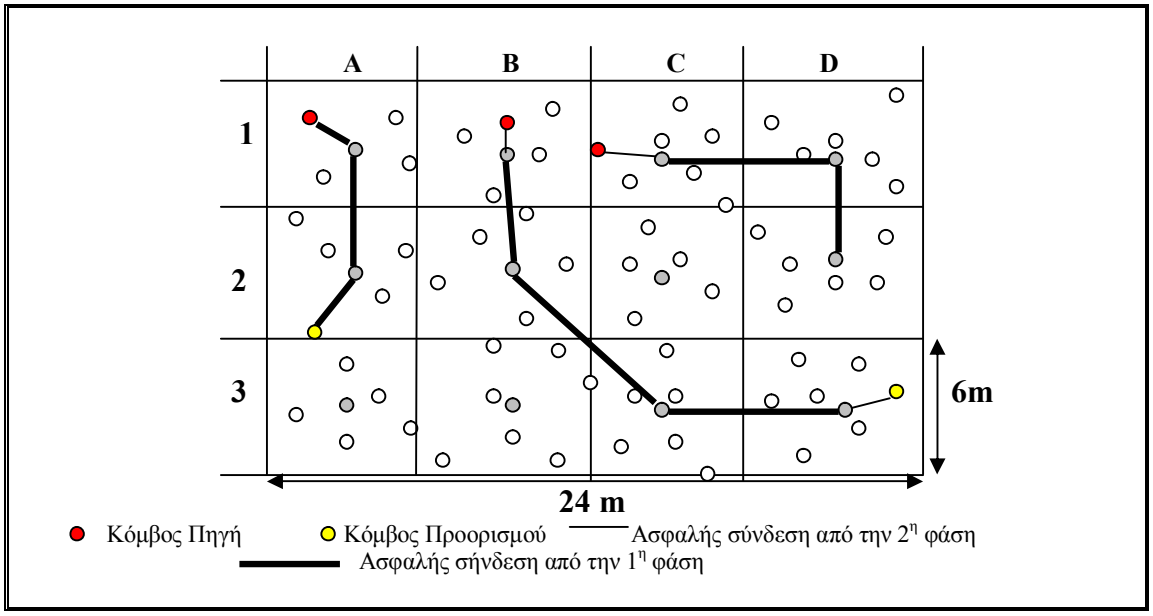
Στην $2^{η}$ φάση, όλοι οι κόμβοι που ανήκουν σε μία ομάδα εγκαθιστούν ένα κλειδί ζεύγους με τους υπόλοιπους κόμβους της ίδιας ομάδας (τόσο με τον clusterhead όσο και με τους απλούς) σύμφωνα με το πρωτόκολλο που περιγράφεται στο [42].

Κατά τη φάση αυτή γίνεται χρήση του κλειδιού γενιάς K_i το οποίο συνδέεται με έναν συγκεκριμένο κόμβο X με αναγνωριστικό ID_X, π.χ. το κλειδί $K_i(ID_X)$. Το κόστος

(χρόνος) κάθε εγκατάστασης κλειδιού είναι το κόστος που προσδίδει το συμμετρικό πρωτόκολλο και περιορίζεται από τον αριθμό των ζευγαριών των κόμβων σε κάθε ομάδα. Στην περίπτωση όπου ένας απλός κόμβος είναι στην εμβέλεια περισσοτέρων του ενός αρχηγού ομάδας, αυτός προγραμματίζεται να απάντα μόνο στον πρώτο που θα τον καλέσει.

4.5.10.3 Φάση 3η : Εγκατάσταση κλειδιού εξωτερικά των ομάδων

Στην 3η φάση, απλοί κόμβοι μιας ομάδας είναι σε θέση να εγκαταστήσουν κλειδί με έναν clusterhead ή με έναν απλό κόμβο μιας άλλης ομάδας. Γίνεται κι εδώ χρήση του συμμετρικού πρωτοκόλλου της δεύτερης φάσης και τα μηνύματα μεταφέρονται μέσω των διαδρομών των ενδιάμεσων αρχηγών ομάδων, όπως φαίνεται στο Σχήμα 24. Οι καταληκτικοί κόμβοι (πηγή και προορισμός) θα πιστοποιηθούν αμοιβαία κατά μήκος της διαδρομής με έναν τρόπο σημείου προς σημείο μέχρι τον κόμβο προορισμό. Ασφάλεια παρέχεται με τη χρήση των ασφαλών συνδέσεων που έχουν εγκατασταθεί στις προηγούμενες φάσεις. Όσο αυξάνεται ο αριθμός των ενδιάμεσων κόμβων, το κόστος της κρυπτογράφησης σημείου προς σημείο αυξάνεται επίσης. Έτσι πρέπει να υπάρχει μία ισορρόπηση στον αριθμό των ενδιάμεσων κόμβων ώστε να είναι εφικτή η ανάπτυξη σε μεγάλη κλίμακα. Με το πέρας της 3ης φάσης, όλοι οι κόμβοι της γενιάς i θα διαγράψουν τα κλειδιά γενιάς K_i και όλα τα στιγμιότυπά τους.



Σχήμα 24. Εγκατάσταση κλειδιού μεταξύ κόμβων διαφορετικών ομάδων.

4.5.10.4 Ασφάλεια του σχήματος ανά φάση

Και στις δύο πρώτες φάσεις κληρονομούνται οι ιδιότητες ασφαλείας καθενός από τα χρησιμοποιούμενα πρωτόκολλα. Έτσι, στην $1^{η}$ φάση η αυθεντικοποίηση βασίζεται στα Implicit Certificates και η επιβεβαίωση κλειδιού στην απόδειξη κάθε κόμβου ότι γνωρίζει το αντίστοιχο μυστικό κλειδί ελλειπτικής καμπύλης. Επιπλέον, η χρήση του υβριδικού πρωτοκόλλου αποτρέπει τις επιθέσεις μίμησης κόμβου και πλαστογράφησης γενιάς. Στην $2^{η}$ φάση επιτελείται αυθεντικοποίηση κόμβου κατά τη διάρκεια της εγκατάστασης κλειδιού, ενώ δεν είναι δυνατόν να εμποδιστούν επιθέσεις πλαστογράφησης γενιάς ή πλαστοπροσωπίας. Η $3^{η}$ φάση συνδυάζει μερικά χαρακτηριστικά ασφαλείας των προηγούμενων δύο φάσεων:

Πρώτον, στη σημείο προς σημείο πιστοποίηση (*point to point authentication*), η ανταλλαγή μηνυμάτων βασίζεται στις συσχετίσεις ασφαλείας που έχουν ήδη εγκατασταθεί στις προηγούμενες φάσεις. Έτσι, δεν υπάρχει τρωτότητα σε επιθέσεις πλαστοπροσωπίας και πλαστογράφησης γενιάς που προκαλούνται από ενδιάμεσους κακόβουλους κόμβους, ενώ ταυτόχρονα υπάρχει ανθεκτικότητα σε εσωτερικές επιθέσεις από διεφθαρμένους κόμβους.

Δεύτερον, στην από άκρο σε άκρο πιστοποίηση (*end to end authentication*), οι καταληκτικοί κόμβοι πιστοποιούνται ακολουθώντας τον τρόπο που περιγράφεται στο πρωτόκολλο του Zhu [42] (αναγνωριστικό κόμβου και κλειδί γενιάς).

Τρίτον, στη σημείο προς σημείο κρυπτογράφηση (point to point encryption), τα μηνύματα κρυπτογραφούνται και αποκρυπτογραφούνται με έναν τρόπο σημείου προς σημείο χρησιμοποιώντας τα κλειδιά που εγκαταστάθηκαν μεταξύ των κόμβων στις προηγούμενες φάσεις. Έτσι, καθίσταται αδύνατο να αντιγραφούν και να συσχετιστούν τα μηνύματα από κάποιον παρείσακτο εισβολέα.

Και τέλος, στην από άκρο σε άκρο κρυπτογράφηση (end to end encryption), η από απόσταση εγκατάσταση κλειδιού μεταξύ κόμβων είναι ασφαλής απέναντι σε ενδιάμεσους κόμβους που προσπαθούν να κατασκευάσουν το κλειδί ζεύγους που έχει εγκατασταθεί μεταξύ καταληκτικών κόμβων.

4.5.10.5 Μοντέλο συστήματος - Ανάλυση επίδοσης

Σύμφωνα με το πρωτόκολλο [89], σε ένα σενάριο εξομοίωσης του δικτύου, οι κόμβοι αναπτύσσονται σε τετραγωνικές περιοχές , όπως στο Σχήμα 23 (8 απλοί κόμβοι ανά τετράγωνο και 1 *clusterhead* στο κέντρο). Θέτουμε την εμβέλεια μετάδοσης των απλών κόμβων στα 5m και των αρχηγών ομάδων στα 9m (για λόγους εξοικονόμησης ενέργειας).

Το προτεινόμενο σχήμα αξιολογείται με την πλατφόρμα εξομοίωσης Network Simulator (NS-2) και το MAC πρωτόκολλο είναι το IEEE 802.11 με DCF (*Distributed Coordination Function*). Η ουρά αναμονής της διεπαφής είναι μία FIFO ουρά, όπου τα πακέτα δρομολόγησης έχουν μεγαλύτερη προτεραιότητα από τα πακέτα δεδομένων.

Από γνωστή σχέση της θεωρίας κεραιών [ομοιοκατευθυντική (omni-directional) κεραία και διαδρομή οπτικής επαφής (line of sight (LoS)) μεταξύ πομπού και δέκτη], παίρνουμε την λαμβανόμενη ισχύ σε απόσταση d.

Για την αξιολόγηση του υβριδικού πρωτοκόλλου του [89] τρέχουμε κάποια σενάρια (εκτίμηση απαιτούμενου χρόνου για εγκατάσταση κλειδιού μεταξύ δύο κόμβων σε πραγματικές συνθήκες, αξιολόγηση απαιτούμενου χρόνου από έναν κόμβο για εγκατάσταση κλειδιών με 8 γειτονικούς κόμβους και αξιολόγηση του πρωτοκόλλου όταν συμβαίνουν περισσότερες από μία αρχικοποιήσεις εγκατάστασης κλειδιού). Όλα τα σενάρια τρέχουν χρησιμοποιώντας δύο διαφορετικά πρωτόκολλα δρομολόγησης, το AODV και το DSDV.

Στην αρχή της εξομοίωσης, οι πίνακες δρομολόγησης κάθε κόμβου δημιουργούνται με την χρήση του DSDV, αφού οι ασύρματοι κόμβοι έχουν αναπτυχθεί εντός των 16 ομάδων.

Έπειτα λαμβάνουν χώρα διαδοχικά οι 3 φάσεις του πρωτοκόλλου που περιγράφηκαν προηγουμένως. Κάθε clusterhead εγκαθιστά κλειδί με όλους τους 8 γειτονικούς clusterheads (στην περίπτωσή μας μόνο οι 4 κεντρικοί), κάθε απλός κόμβος εγκαθιστά κλειδί με τον clusterhead της ομάδος του (και παράλληλα αποκτά δυνατότητα εγκατάστασης με κάποιον απλό κόμβο άλλης ομάδας), και τέλος ένας απλός κόμβος πρώτα εγκαθιστά κλειδί με άλλο απλό κόμβο γειτονικής ομάδας, έπειτα με απλό κόμβο 2 ομάδες μακριά και τέλος με απλό κόμβο 3 ομάδες μακριά. Στον Πίνακα 1 παρουσιάζονται οι θεωρητικοί χρόνοι και οι χρόνοι εξομοίωσης (πραγματικοί) για κάθε φάση.

	Υβριδικό (μεταξύ clusterheads)	Συμμετρικό (εντός των ομάδων)	1 ομάδα μακριά	2 ομάδες μακριά	3 ομάδες μακριά
Θεωρητικός χρόνος (sec)	< 5.424	0.025	0.088	0.102	0.136
Πραγματικός χρόνος(sec)	4.9404	1.5787	0.0899	0.1252	0.3784

Πίνακας 1. Τα αποτελέσματα της θεωρητικής εγκατάστασης κλειδιού και των 3 σεναρίων εξομοίωσης κατά Κοτζανικολάου.

Αθροιστικά μπορούμε να πάρουμε τον συνολικό πραγματικό απαιτούμενο χρόνο (κόστος) για εγκατάσταση κλειδιού για κόμβους σε διαφορετικές αποστάσεις. Από την μελέτη του πίνακα συμπεραίνουμε τα παρακάτω:

Κατά την εκτέλεση του υβριδικού πρωτοκόλλου μεταξύ γειτονικών αρχηγών ομάδων και επειδή μόνο οι αρχηγών ομάδων που είναι εγκατεστημένοι σε κεντρικές ομάδες εκκινούν εγκατάσταση κλειδιού, έχουμε διαφορετικό αριθμό εγκαταστάσεων κλειδιού ανά κόμβο (κάποιες εγκαταστάσεις θα έχουν ήδη ολοκληρωθεί προς τη μία κατεύθυνση). Έτσι, ο πραγματικός χρόνος που απαιτείται γι' αυτή τη φάση ελαττώνεται σε σχέση με τον θεωρητικό.

Αντίθετα, ο χρόνος της συμμετρικής εγκατάστασης κλειδιού είναι μεγαλύτερος συγκρινόμενος με τον θεωρητικό. Αυτό οφείλεται στο γεγονός ότι στην εξομοίωση λαμβάνουμε την χειρότερη περίπτωση (πολλές συγκρούσεις και αναμεταδόσεις μετά από ένα τυχαίο χρόνο που ορίζεται από τον αλγόριθμο back off / οι απλοί κόμβοι εκκινούν την εγκατάσταση).

Για το τρίτο σενάριο, όταν αυξάνεται ο αριθμός των αρχηγών ομάδων που μεσολαβούν για την μεταφορά των πακέτων μεταξύ δύο απλών κόμβων, τότε αυξάνεται και η διαφορά μεταξύ πραγματικού και θεωρητικού χρόνου (καθυστέρηση

λόγω αναμονής από άλλες σε εξέλιξη μεταδόσεις στους κόμβους που παρεμβάλλονται).

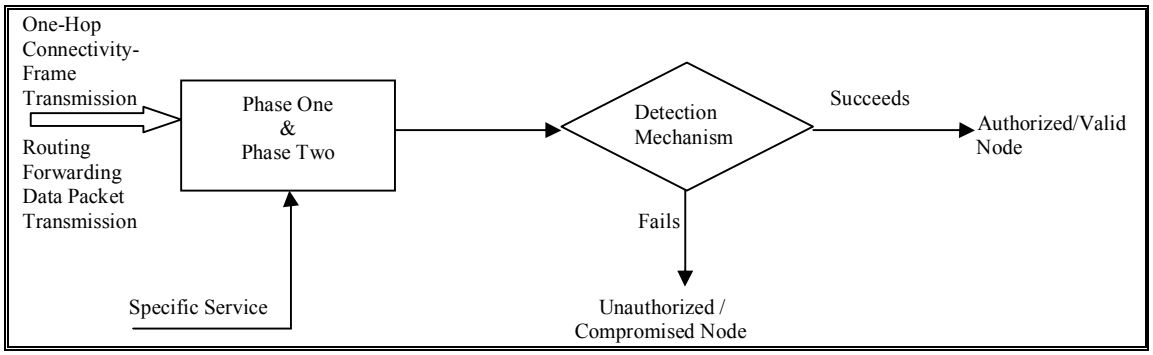
4.5.11 Ανιχνεύοντας μη εξουσιοδοτημένους και ήδη εκτεθειμένους σε κίνδυνο κόμβους

Σε αντίθεση με τα υπόλοιπα δίκτυα που χρησιμοποιούν συγκεκριμένους κόμβους για την υποστήριξη βασικών λειτουργιών όπως είναι η προώθηση πακέτων, η δρομολόγηση και η διαχείριση δικτύου, στα εξεταζόμενα δίκτυα οι παραπάνω λειτουργίες διεκπεραιώνονται από όλους τους διαθέσιμους κόμβους. Η ασύρματη και κινητή φύση των δικτύων κάνει τα δίκτυα πιο ευπαθή σε κακόβουλες ενέργειες. Όπως αναφέραμε, αυτά τα δίκτυα είναι ευάλωτα σε επιθέσεις που κυμαίνονται από απλό κρυφάκουσμα μέχρι και ενεργή παρέμβαση στην λειτουργία του δικτύου.

Αντίθετα με τα ενσύρματα δίκτυα όπου ένας επιτιθέμενος πρέπει να αποκτήσει φυσική πρόσβαση στο δίκτυο, σε ένα ασύρματο δίκτυο οι επιθέσεις μπορούν να έρθουν από οποιαδήποτε κατεύθυνση και να στοχεύουν κάθε κόμβο του δικτύου. Στα δίκτυα, οι κόμβοι είναι δυνατόν να καταληφθούν, να εκτεθούν ή να «αιχμαλωτιστούν», αφού είναι μονάδες που μπορούν να περιφέρονται ανεξάρτητες. Έτσι, οι κόμβοι πρέπει να είναι προετοιμασμένοι να λειτουργήσουν με μία μη εμπιστευτική κατάσταση λειτουργίας. Επιπλέον, η έλλειψη μίας κεντρικής αρχής, δίνει ευκαιρίες στους αντίπαλους να εκτελέσουν νέες επιθέσεις και να σπάσουν τον απαραίτητο αλγόριθμο.

Όταν παρατηρηθούν ένα σύνολο από ενέργειες που προσπαθούν να διαταράξουν την ακεραιότητα, την εμπιστευτικότητα ή τη διαθεσιμότητα ενός κόμβου, τότε λαμβάνουν χώρα τεχνικές εντοπισμού παρέμβασης (*intrusion detection*), όπως είναι η κρυπτογράφηση και η πιστοποίηση. Παρόλα αυτά, η πρόληψη της παρέμβασης από μόνη της δεν είναι δυνατή όταν τα συστήματα γίνονται ολοένα και πιο πολύπλοκα. Έτσι, ο εντοπισμός της παρέμβασης μπορεί να χρησιμοποιηθεί ως ένα δεύτερο τοίχος για να προστατέψει το δίκτυο, γιατί όταν μία παρέμβαση επισημανθεί, μία αντίδραση πρέπει να λάβει χώρα για να ελαχιστοποιηθούν οι ζημιές. Εξ' ορισμού, ο εντοπισμός παρέμβασης περιλαμβάνει έλεγχο δεδομένων και αιτιολόγηση των στοιχείων στα δεδομένα για να καθοριστεί αν το δίκτυο δέχεται επίθεση [90].

Η σημαντικότερη διαφορά μεταξύ συμβατικών δικτύων και των υπό εξέταση δικτύων είναι η έλλειψη από τα τελευταία μιας σταθερής υποδομής. Για την ανίχνευση μη εξουσιοδοτημένων και ήδη εκτεθειμένων κόμβων χρησιμοποιείται γενικά η παραγωγή και διαχείριση κλειδιού για να εξασφαλίσει την αυθεντικότητα και την ακεραιότητα της πληροφορίας δρομολόγησης [91]. Μια τακτική που χρησιμοποιείται για ανίχνευση μη εξουσιοδοτημένων κόμβων περιλαμβάνει δύο φάσεις (Σχήμα 25). Κατά την πρώτη φάση, ο μηχανισμός ανίχνευσης προσπαθεί να καθορίσει την πραγματική ταυτότητα των επικοινωνούντων κόμβων και έτσι να αποκαλύψει μη εξουσιοδοτημένους κόμβους χρησιμοποιώντας ένα μη αλληλεπιδραστικό μηδενικής γνώσης πρωτόκολλο (*non-interactive zero knowledge protocol*) [92]. Στη δεύτερη φάση, ο μηχανισμός ανίχνευσης καθορίζει αν οι επικοινωνούντες κόμβοι έχουν εκτεθεί ή όχι, μέσω ενός ίδιου πρωτοκόλλου.



Σχήμα 25. Διαδικασία ανίχνευσης.

Η δεύτερη φάση, λαμβάνει χώρα μόλις τα δεδομένα είναι έτοιμα να μεταφερθούν. Η διαδικασία ανίχνευσης για εκτεθειμένους κόμβους διεξάγεται στους διαθέσιμους κόμβους ξεκινώντας βήμα προς βήμα από την πηγή μέχρι τον κόμβο προορισμού. Η χρήση του πρωτοκόλλου μηδενικής γνώσης είναι επιτακτική σε δίκτυα τέτοιου είδους γιατί είναι χαμηλής πολυπλοκότητας πρωτόκολλο που δεν θα δημιουργήσει επιπλέον υπολογιστικό κόστος στο δίκτυο. Τα αλληλεπιδραστικά πρωτόκολλα μηδενικής γνώσης δεν είναι κατάλληλα για ασύρματα περιβάλλοντα καθόσον ανταλλάσουν πολλαπλά μηνύματα και έτσι επιφέρουν μείωση της απόδοσης του δικτύου.

Οι δυσκολίες που δημιουργούνται κατά τη διαδικασία ανίχνευσης είναι σημαντικές για την εύρυθμη λειτουργία του δικτύου. Έτσι, η κρυπτογράφηση είναι σχετικά ακριβή στους κόμβους των δικτύων, όπου η ικανότητα υπολογισμών είναι περιορισμένη. Επίσης, επειδή δεν υπάρχει μια κεντρική αρχή διαχείρισης, η πιστοποίηση είναι πολύ δύσκολο να εφαρμοστεί. Τέλος, τα προϋπάρχοντα σχήματα ανίχνευσης παρουσίαζαν ικανοποιητικά αποτελέσματα μόνο για παρείσακτους από εξωτερικές επιθέσεις και όχι για ήδη εκτεθειμένους κόμβους που είναι εσωτερικά στο δίκτυο. Λόγω της περιορισμένης ενέργειας των κόμβων είναι απαραίτητη η δημιουργία αποτελεσματικών σχημάτων για την ανίχνευση μη εξουσιοδοτημένων και ήδη εκτεθειμένων κόμβων.

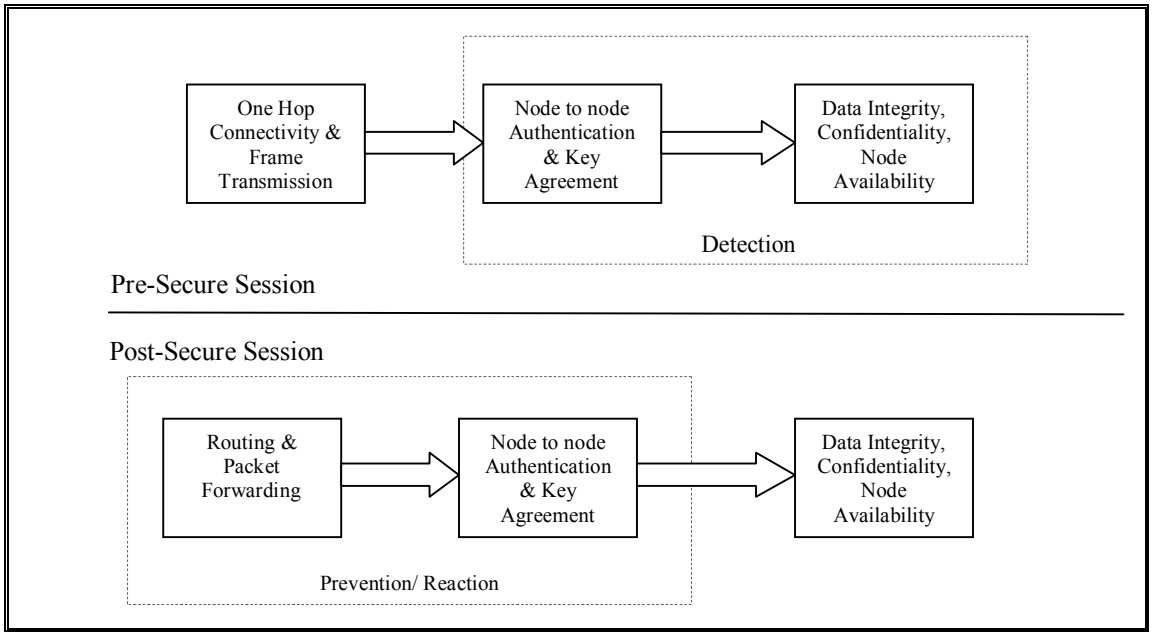
4.6 Σχεδιασμός ασφαλείας σε επίπεδα

Το μοντέλο OSI είναι μια διαστρωματωμένη περιγραφή για σχεδίαση δικτύων και για τις επικοινωνίες. Σ' αυτό το μοντέλο, από τα επτά συνολικά επίπεδα, μας ενδιαφέρουν το επίπεδο ζεύξης (*data link layer*) και το επίπεδο δικτύου (*network layer*). Στο επίπεδο ζεύξης, οι βασικές λειτουργίες που εκτελούνται είναι η σύνδεση μονού άλματος (one hop connectivity) και αναμετάδοση πλαισίων (*frame transmission*) [61]. Αντίστοιχα, στο επίπεδο δικτύου, οι βασικές λειτουργίες είναι η δρομολόγηση και η προώθηση πακέτων δεδομένων [64].

Κατά τη λειτουργία ενός δικτύου, η εργασία που γίνεται είναι η αναγνώριση κάποιων απειλών και στη συνέχεια η ενεργοποίηση ή η βελτίωση του υπάρχοντος πρωτοκόλλου ασφαλείας για την αντιμετώπιση των απειλών. Αυτή η εργασία είναι αποτελεσματική για την περίπτωση που οι απειλές είναι γνωστές, αλλά μπορεί να καταρρεύσει όταν εμφανιστούν νέες απειλές. Έτσι, είναι απαραίτητο να σχεδιάσουμε

τα δίκτυά μας με πολλαπλές γραμμές άμυνας ώστε να μπορούν να ανταπεξέλθουν τόσο σε γνωστές όσο και σε άγνωστες απειλές. Αυτή η σχεδίαση καλείται σχεδίαση ασφαλείας σε επίπεδα.

Στη σχεδίαση ασφαλείας σε επίπεδα, λαμβάνονται επίσης υπόψη σφάλματα του δικτύου λόγω κακής διάρθρωσης, υπερφόρτωσης του δικτύου ή λειτουργικών αστοχιών. Τα παραπάνω σφάλματα πρέπει να αντιμετωπίζονται από τους μηχανισμούς ασφαλείας του δικτύου. Τα δύο επίπεδα του μοντέλου OSI που μας ενδιαφέρουν, περιλαμβάνουν μηχανισμούς ασφαλείας που ενοποιούν μια διαδικασία ασφάλισης πρωτοκόλλου (Σχήμα 26). Η διαδικασία αυτή αποτελείται από τις pre-secure και post-secure φάσεις. Κατά την pre-secure φάση επιχειρείται η ανακάλυψη απειλών μέσω διάφορων κρυπτογραφικών μηχανισμών ενώ η post-secure φάση προσπαθεί να αποτρέψει τέτοιες απειλές και να αντιδράσει ανάλογα.



Σχήμα 26. Διαδικασία ασφάλισης πρωτοκόλλου.

Οι μηχανισμοί ασφαλείας σε επίπεδα πρέπει να περιλαμβάνουν πρόληψη, ανακάλυψη και λειτουργίες αντίδρασης για να αποτρέψουν τους επιτιθέμενους να εισέλθουν στο δίκτυο. Έτσι, η πρόληψη μπορεί να εφαρμοστεί στην ασφαλή προώθηση πακέτων ώστε να αποτρέψει έναν επιτιθέμενο να εγκαταστήσει λάθος πληροφορία δρομολόγησης στους κόμβους. Η διαδικασία της ανακάλυψης ερευνά την αντικανονική συμπεριφορά κακόβουλων ή εγωιστικών κόμβων. Τέλος, όταν ανακαλυφθεί ένας επιτιθέμενος, λαμβάνονται μέτρα αντίδρασης για την αντιμετώπισή του.

4.6.1 Pre-secure session

Κατά την φάση αυτή, η σχεδίαση ασφαλείας σε επίπεδα προσαρμόζει κρυπτογραφικές μεθόδους για να προσφέρει πολλαπλές γραμμές προστασίας στους επικοινωνούντες κόμβους. Όταν ένας ή περισσότεροι κόμβοι συνδέονται σε ένα δίκτυο, λαμβάνουν χώρα μία αρχική πιστοποίηση κόμβο προς κόμβο και μία

συμφωνία κλειδιού (*key agreement*). Σ' αυτήν τη φάση, είναι απαραίτητο να μπορεί κάθε κόμβος να αναγνωρίσει την πραγματική ταυτότητα των γειτόνων του, οι οποίοι θα αποκτήσουν πρόσβαση σε κάποιο μυστικό κλειδί αργότερα.

Λόγω των περιορισμών ισχύος που υπάρχουν στα δίκτυά μας, η πιστοποίηση και η συμφωνία κλειδιού μπορούν να επιτευχθούν με ένα πρωτόκολλο μηδενικής γνώσης. Η βασική ιδέα για τη χρησιμοποίηση τέτοιων κρυπτογραφικών πρωτοκόλλων είναι ότι επιτρέπουν σε έναν κόμβο να επιδείξει γνώση ενός μυστικού, ενώ δεν αποκαλύπτουν καμία πληροφορία χρήσης στον κόμβο επαλήθευσης ακόμα και αν ο κόμβος έχει κακή συμπεριφορά.

Η πιστοποίηση κόμβου προς κόμβο και η συμφωνία κλειδιού (που βρίσκονται στην pre-secure φάση) μπορούν να ανακαλύψουν αν ένας πιστοποιημένος κόμβος έχει εκτεθεί. Αυτό μπορεί να γίνει όταν ένας τυχαίος μυστικός αριθμός έχει μοιραστεί μεταξύ δύο επικοινωνούντων κόμβων. Ο αριθμός αυτός μπορεί να ελεγχθεί και να εξακριβωθεί από τους δύο κόμβους. Η ενέργεια αυτή θα ενεργοποιήσει ή θα σταματήσει την κυκλοφορία σε κόμβους που έχουν ή δεν έχουν πιστοποιηθεί.

Ο τυχαίος αυτός αριθμός μπορεί να πάρει μέρος στην παραγωγή του κλειδιού κρυπτογράφησης που λαμβάνει χώρα στην post-secure φάση. Επίσης, τέτοια τυχαία πληροφορία μπορεί να χρησιμοποιηθεί για να καθορίσει τη διαθεσιμότητα ενός κόμβου. Όταν οι παραπάνω εργασίες τελειώσουν, τα πλαίσια μπορούν να κρυπτογραφηθούν και η ακεραιότητα των πληροφοριών μπορεί να αποκτηθεί χρησιμοποιώντας τα υπάρχοντα κρυπτογραφικά πρωτόκολλα.

4.6.2 Post-secure session

Όταν η πληροφορία δρομολόγησης είναι έτοιμη να μεταδοθεί, λαμβάνει χώρα η δεύτερη φάση της πιστοποίησης και της συμφωνίας κλειδιού. Η πιστοποίηση συνεχίζεται στους διαθέσιμους κόμβους βήμα προς βήμα από την πηγή προς τον κόμβο προορισμού. Καθόσον οι κόμβοι στη διαδρομή πιστοποιούνται, μπορούν παράλληλα να συμφωνήσουν σε ένα κρυπτογραφικό κλειδί, που καλείται κλειδί συνεδρίας και θα χρησιμοποιηθεί για να κρυπτογραφήσει την κίνησή τους. Παρόμοια με την προηγούμενη φάση, μπορεί να επιτευχθεί η εμπιστευτικότητα και η ακεραιότητα δεδομένων χρησιμοποιώντας γνωστούς κρυπτογραφικούς αλγόριθμους. Επίσης, μπορεί να αποκτηθεί η μη αποκήρυξη με κρυπτογραφικές τεχνικές, όπως είναι οι ψηφιακές υπογραφές, οι συναρτήσεις κατακερματισμού κ.ά.

Σε αυτή τη δεύτερη φάση, είναι απαραίτητη η ισχυρή πιστοποίηση γιατί τα δεδομένα είναι έτοιμα να αποσταλούν. Τα πρωτόκολλα πρόκλησης-απόκρισης (*challenge-response protocols*) μπορούν να χρησιμοποιηθούν για να εξακριβώσουν την ταυτότητα των επικοινωνούντων κόμβων χρησιμοποιώντας την επαλήθευση της γνώσης ενός κοινού μυστικού.

Οι διαδικασίες πιστοποίησης και συμφωνίας κλειδιού που λαμβάνουν χώρα στην post-secure φάση μπορούν να αντιδράσουν και να αποτρέψουν εκτεθειμένους κόμβους. Αυτό γίνεται χρησιμοποιώντας την τυχαία πληροφορία που έχει εισαχθεί και συμφωνηθεί στην pre-secure φάση.

Τελικά, παρατηρήσαμε ότι οι απαιτήσεις ασφαλείας (πιστοποίηση, εμπιστευτικότητα, ακεραιότητα και μη αποκήρυξη) πρέπει να εστιάζονται στο επίπεδο ζεύξης και στο επίπεδο δικτύου. Και αυτό γιατί τα δίκτυά μας μπορούν να λειτουργούν μέσα σε μη εμπιστευτικά περιβάλλοντα, όπου πρέπει να

χρησιμοποιούνται εξεζητημένοι μηχανισμοί ασφαλείας. Έτσι, τα δίκτυα πρέπει να είναι ικανά να ανακαλύπτουν και να αντιδρούν σε ενδεχόμενες ενέργειες κακόβουλων κόμβων. Η παραπάνω εργασία μπορεί να γίνει εύκολα με τη σχεδίαση της ασφάλειας σε επίπεδα ασφαλείας και με πολλαπλές γραμμές άμυνας ώστε να προστατεύεται κάθε κόμβος από αντίστοιχους εχθρικούς.

4.7 Σύντομη περιγραφή των υπαρχόντων πρωτοκόλλων

Η προσπάθεια που γίνεται για τον σχεδιασμό ασφαλών πρωτοκόλλων δρομολόγησης προσανατολίζεται προς τα ενεργά πρωτόκολλα δρομολόγησης με ζήτηση (*on-demand routing protocols*) όπως το DSR ή το AODV, όπου ένας κόμβος προσπαθεί να ανακαλύψει ένα δρομολόγιο προς μία ορισμένη κατεύθυνση μόνο όταν έχει να στείλει ένα πακέτο προς αυτήν την κατεύθυνση. Τα πρωτόκολλα αυτής της κατηγορίας έχει αποδειχθεί ότι αποδίδουν καλύτερα με μικρότερη επιβάρυνση από τα προ-ενεργά πρωτόκολλα, εφόσον είναι δυνατόν να αντιδράσουν άμεσα στην αλλαγή τοπολογίας, ενώ διατηρούν την επιβάρυνση δρομολόγησης χαμηλή σε περιόδους ή περιοχές του δικτύου που οι αλλαγές είναι λιγότερο συχνές.

Τα σύγχρονα πρωτόκολλα δρομολόγησης, λαμβάνουν υπ' όψιν τις ενεργές επιθέσεις που εκτελούνται από κακόβουλους κόμβους που σκοπεύουν στο συνεχές 'ανακάτεμα' στην εκτέλεση των πρωτοκόλλων δρομολόγησης, ενώ οι παθητικές επιθέσεις δεν εξετάζονται. Επιπλέον, η προϋπόθεση για όλες τις υπάρχουσες λύσεις είναι ένα ελεγχόμενο περιβάλλον που χαρακτηρίζεται από μία υποδομή ασφάλειας που εγκαθίσταται πριν από την εκτέλεση του ασφαλούς πρωτόκολλου δρομολόγησης. Οι πλέον αξιόπιστες προτάσεις για ασφαλή δρομολόγηση στα εξεταζόμενα δίκτυα περιγράφονται παρακάτω.

4.7.1 Secure Routing Protocol (SRP)

Το πρωτόκολλο SRP [67] σχεδιάστηκε ως επέκταση συμβατή με μία ποικιλία από υπάρχοντα πρωτόκολλα δρομολόγησης. Το SRP μάχεται με επιθέσεις που διαταράσσουν τη διαδικασία ανακάλυψης δρομολογίου και εγγυάται την απόκτηση της σωστής πληροφορίας τοπολογίας. Το SRP επιτρέπει στον εκκινητή μιας διαδικασίας εύρεσης δρομολογίου να ανιχνεύσει και να απορρίψει πλαστές απαντήσεις. Το SRP στηρίζεται στη διαθεσιμότητα μιας *σχέσης ασφάλειας* (ΣΑ) μεταξύ του κόμβου *πηγής* (Π) και του κόμβου *προορισμού* (Ρ). Η ΣΑ μπορεί να παγιωθεί χρησιμοποιώντας κατανομή ενός υβριδικού κλειδιού που στηρίζεται στα δημόσια κλειδιά των συμμετεχόντων. Ο Π και ο Ρ μπορούν να ανταλλάξουν το συμμετρικό τους κλειδί χρησιμοποιώντας τα δημόσια κλειδιά τους για να εγκαταστήσουν ένα ασφαλές κανάλι. Στη συνέχεια, μπορούν να προχωρήσουν σε αμοιβαία επαλήθευση ταυτότητας και πιστοποίηση των μηνυμάτων δρομολόγησης.

Το SRP ανταπεξέρχεται με κακόβουλους κόμβους που είναι ικανοί να τροποποιήσουν, αναπαράγουν και πλαστογραφήσουν πακέτα δρομολόγησης. Επίσης, ενσωματώνει μηχανισμούς που διασφαλίζουν τη λειτουργικότητα του δικτύου από επιθέσεις που εκμεταλλεύονται το πρωτόκολλο, με σκοπό να υποβαθμίσουν την απόδοση του δικτύου και πιθανόν να οδηγήσουν σε μια άρνηση υπηρεσίας.

Ο κόμβος πηγής Π αρχίζει την εύρεση δρομολογίου, δημιουργώντας ένα πακέτο ζήτησης δρομολογίου (RREQ), που χαρακτηρίζεται από ένα ζεύγος από αναγνωριστικά: μία ερώτηση με αύξοντα αριθμό και μία τυχαία αναγνωριστική ερώτηση. Η πηγή, ο προορισμός και οι μοναδικοί αναγνωριστικοί αριθμοί των ερωτήσεων είναι οι είσοδοι για τον υπολογισμό του κώδικα πιστοποίησης μηνύματος (*Message Authentication Code-MAC*) μαζί με το συμμετρικό κλειδί Κ. Επιπλέον, οι ταυτότητες (IP διευθύνσεις) των ενδιάμεσων κόμβων συγκεντρώνονται στο RREQ.

Οι ενδιάμεσοι κόμβοι αναμεταδίδουν τις αιτήσεις, ώστε ένα ή περισσότερα πακέτα να φθάσουν στον προορισμό και να διατηρούν ένα ελάχιστο ποσό της πληροφορίας κατάστασης που αφορά στα μεταδιδόμενα πακέτα, ώστε πακέτα που έχουν αναμεταδοθεί να απορρίπτονται.

Η αίτηση RREQ φθάνει στον προορισμό Ρ και κατασκευάζεται μια απόκριση δρομολογίου (RREP). Υπολογίζει έναν MAC που περιλαμβάνει τα περιεχόμενα του RREP και επιστρέφει το πακέτο στον Π πάνω ακριβώς στην αντίθετη διαδρομή που περιλαμβάνεται στο RREQ.

Η βασική έκδοση του SRP υποφέρει από την επίθεση 'δηλητηριασμού' κρυφού δρομολογίου: οι πληροφορίες δρομολόγησης που μαζεύονται από τους κόμβους που λειτουργούν με ανομοιογενή τρόπο για να καλυτερέψουν την αποτελεσματικότητα του πρωτοκόλλου DSR μπορεί να τεθούν εκτός υπηρεσίας, λόγω ενδεχόμενης πλαστογράφησης από κακόβουλους κόμβους. Το SRP πάσχει επίσης από έλλειψη μηχανισμών επικύρωσης για μηνύματα διατήρησης δρομολογίου: τα λανθασμένα πακέτα δρομολόγησης δεν επαληθεύονται. Τέλος, το SRP είναι ευάλωτο στην επίθεση 'σκουληκότρυπας' (*wormhole attack*): δύο συνωμοτούντες κακόβουλοι κόμβοι μπορούν να αλλάξουν κατεύθυνση στα πακέτα δρομολόγησης σ' ένα ιδιωτικό δίκτυο και να αλλάξουν την αντίληψη της τοπολογίας του δικτύου στους νόμιμους κόμβους.

4.7.2 Πρωτόκολλο ARIADNE

Το πρωτόκολλο ARIADNE είναι ένα πρωτόκολλο δρομολόγησης με ζήτηση που στηρίζεται στο DSR, αντέχει στην έκθεση των κόμβων και στηρίζεται μόνο σε υψηλής απόδοσης συμμετρική κρυπτογραφία [69]. Το πρωτόκολλο εγγυάται ότι ο κόμβος-στόχος μπορεί να τακτοποιήσει οποιοδήποτε ενδιάμεσο κόμβο στη διαδρομή προς τον προορισμό που υπάρχει στο μήνυμα RREP και ότι κανένας ενδιάμεσος κόμβος δεν μπορεί να αποσύρει οποιοδήποτε κόμβο από την λίστα των μηνυμάτων RREQ και RREP.

Το ARIADNE χρειάζεται ορισμένους μηχανισμούς για να εκκινήσει τα κλειδιά αυθεντικότητας που απαιτούνται. Συγκεκριμένα, κάθε κόμβος χρειάζεται ένα μοιραζόμενο μυστικό κλειδί με κάθε κόμβο που επικοινωνεί σε υψηλότερο επίπεδο, ένα αυθεντικό κλειδί TESLA (ένα αποτελεσματικό σχήμα μετάδοσης πιστοποίησης που χρειάζεται χαλαρό χρονικό συγχρονισμό) για κάθε κόμβο στο δίκτυο και ένα αυθεντικό στοιχείο 'αλυσίδας ανακάλυψης δρομολογίου' (Route Discovery Chain) για κάθε κόμβο που θα προωθήσει τα μηνύματα RREQ.

Το ARIADNE παρέχει πιστοποίηση σημείου προς σημείο χρησιμοποιώντας ένα MAC και ένα μοιραζόμενο κλειδί μεταξύ δύο τμημάτων. Παρόλα αυτά, για την πιστοποίηση ενός εκπεμπόμενου προς όλους τους κόμβους μηνύματος, το ARIADNE χρησιμοποιεί το πρωτόκολλο TESLA. Επίσης, τα καταφέρνει με επιθέσεις που εκτελούνται από κακόβουλους κόμβους που τροποποιούν και πλαστογραφούν την

πληροφορία δρομολόγησης, με επιθέσεις που χρησιμοποιούν μίμηση και - σε μία προχωρημένη έκδοση - με την επίθεση ‘σκουληκότρυπας’. Οι «εγωιστές» κόμβοι δεν λαμβάνονται υπ’ όψιν.

Για να αποτρέψει την εισαγωγή άκυρων λαθών δρομολόγησης στο δίκτυο που παράγεται από οποιοδήποτε κόμβο εκτός από αυτόν που αναφέρεται στο μήνυμα λάθους, το ARIADNE προσθέτει μια πληροφορία πιστοποίησης TESLA στο μήνυμα λάθους δρομολόγησης, τέτοιο ώστε όλοι οι κόμβοι στη διαδρομή επιστροφής να ταυτοποιήσουν το λάθος.

Το ARIADNE προστατεύεται από την πλημμύρα RREQ πακέτων που μπορούν να οδηγήσουν στην επίθεση ‘δηλητηριασμού’ cache. Οι νόμιμοι κόμβοι μπορούν να φιλτράρουν πλαστά ή υπέρμετρα πακέτα RREQ χρησιμοποιώντας αλυσίδες ανακάλυψης δρομολογίου (Route Discovery Chains), έναν μηχανισμό για να ταυτοποιήσουν την ανακάλυψη δρομολογίων επιτρέποντας κάθε κόμβο να εκτιμήσει (περιορίσει) τις ανακαλύψεις από άλλους κόμβους.

Το ARIADNE είναι απρόσβλητο στην επίθεση ‘σκουληκότρυπας’ μόνο στην προηγμένη του έκδοση: χρησιμοποιώντας μία επέκταση που χρειάζεται σκληρό χρονικό συγχρονισμό μεταξύ κόμβων, μπορεί να ανακαλύψει ανωμαλίες που προκαλούνται από ‘σκουληκότρυπες’ που στηρίζονται σε χρονικές ανακολουθίες.

4.7.3 Πρωτόκολλο ARAN

Το πρωτόκολλο ARAN θεωρείται ως ένα πρωτόκολλο δρομολόγησης με ζήτηση που ανακαλύπτει και προστατεύει από κακόβουλες ενέργειες που εκτελούνται από τρίτους και εισβάλουν στο ad hoc περιβάλλον [93]. Το ARAN εισάγει την πιστοποίηση, την ακεραιότητα μηνύματος και τη μη αποκήρυξη ως κομμάτι μιας ελάχιστης πολιτικής ασφαλείας για το ad hoc περιβάλλον και αποτελείται από μια προκαταρκτική διαδικασία πιστοποίησης, μια υποχρεωτική από άκρο σε άκρο πιστοποίηση και μία προαιρετική δεύτερη φάση που παρέχει ασφαλείς σύντομες διαδρομές.

Το ARAN απαιτεί την χρήση ενός εμπιστευτικού κέντρου πιστοποίησης: πριν την είσοδο στο περιβάλλον ad hoc, κάθε κόμβος πρέπει να ζητήσει ένα πιστοποιητικό που υπογράφεται από το κέντρο. Το πιστοποιητικό περιέχει τη διεύθυνση IP κάθε κόμβου, το δημόσιο κλειδί του, μια χρονοσφραγίδα τού πότε δημιουργήθηκε το πιστοποιητικό και τον χρόνο λήξης του πιστοποιητικού, μαζί με την υπογραφή του κέντρου. Όλοι οι κόμβοι υποτίθεται ότι έχουν φρέσκα πιστοποιητικά με το εμπιστευτικό κέντρο και πρέπει να ξέρουν το δημόσιο κλειδί του κέντρου.

Στη δεύτερη φάση του ARAN, το πρωτόκολλο εγγυάται με ένα ασφαλές τρόπο ότι το δρομολόγιο που δημιουργήθηκε από έναν κόμβο είναι το πιο σύντομο. Σε αυτή τη φάση, όσο και κατά τη φάση της διατήρησης δρομολογίου, το πρωτόκολλο ασφαλίζεται με ψηφιακή υπογραφή των πακέτων λάθους δρομολογίου. Όμως, είναι πολύ δύσκολο να ανακαλύψει πότε τα λάθος μηνύματα παράγονται από συνδέσεις που είναι ενεργές και όχι σπασμένες. Παρόλα αυτά, επειδή τα μηνύματα υπογράφονται, οι κακόβουλοι κόμβοι δεν μπορούν να παράγουν λάθος μηνύματα για άλλους κόμβους. Η μη αποκήρυξη, που παρέχεται από την υπογραφή των λανθασμένων μηνυμάτων, επιτρέπει σε έναν κόμβο να εξακριβώσει την πηγή του λάθους μηνύματος.

Όπως σε κάθε ασφαλές σύστημα που στηρίζεται σε κρυπτογραφικές υπογραφές, η ανάκληση κλειδιού πρέπει να επιληφθεί ώστε να γίνει σίγουρο ότι ληγμένα ή άκυρα πιστοποιητικά δεν επιτρέπουν στον κάτοχο να εισέλθει στο δίκτυο.

Το πρωτόκολλο ARAN προστατεύει από επιθέσεις που χρησιμοποιούν τροποποίηση, πλαστογράφηση και μίμηση αλλά η χρήση ασύμμετρης κρυπτογραφίας το κάνει πολύ δαπανηρό πρωτόκολλο σε σχέση με την CPU και την χρήση ενέργειας. Επιπλέον το ARAN δεν είναι άτρωτο από την επίθεση 'σκουληκότρυπας'.

4.7.4 Πρωτόκολλο SEAD

Το πρωτόκολλο SEAD είναι ένα υπέρ ενεργό πρωτόκολλο δρομολόγησης που στηρίζεται στο πρωτόκολλο DSDV [70]. Σε ένα υπέρ ενεργό πρωτόκολλο, οι κόμβοι περιοδικά ανταλλάσουν πληροφορία δρομολόγησης με άλλους κόμβους με σκοπό κάθε κόμβος να γνωρίζει ένα δρομολόγιο προς όλες τις κατευθύνσεις [94].

Το SEAD αντιμετωπίζει επιτιθέμενους που τροποποιούν την πληροφορία δρομολόγησης που μεταδίδεται κατά την φάση αναβάθμισης του πρωτοκόλλου DSDV: συγκεκριμένα, η δρομολόγηση μπορεί να διαταραχθεί εάν ο επιτιθέμενος τροποποιήσει το νούμερο ακολουθίας και το μετρικό πεδίο του μηνύματος ανανέωσης του πίνακα δρομολόγησης. Λαμβάνονται υπ' όψιν και οι επιθέσεις επανάληψης.

Για να ασφαλίσει το πρωτόκολλο DSDV, το SEAD κάνει χρήση αλυσίδων (συναρτήσεων) κατατεμαχισμού ενός δρόμου (one-way hash functions) και δεν στηρίζεται σε πανάκριβες λειτουργίες ασύμμετρης κρυπτογραφίας. Όπως και τα υπόλοιπα πρωτόκολλα που παρουσιάστηκαν, το SEAD υποθέτει έναν μηχανισμό για κάθε κόμβο που διανέμει ένα αυθεντικό κομμάτι της αλυσίδας κατατεμαχισμού που χρησιμοποιείται για την πιστοποίηση των υπόλοιπων κομματιών της αλυσίδας.

Η βασική ιδέα του SEAD είναι η πιστοποίηση του αριθμού ακολουθίας και του μετρικού του μηνύματος ανανέωσης του πίνακα δρομολόγησης χρησιμοποιώντας κομμάτια από αλυσίδες κατατεμαχισμού. Επιπλέον, ο παραλήπτης της πληροφορίας δρομολόγησης του SEAD πιστοποιεί τον αποστολέα, εξασφαλίζοντας ότι η πληροφορία δρομολόγησης προέρχεται από τον σωστό κόμβο.

Η πηγή κάθε μηνύματος ανανέωσης πληροφορίας πρέπει να πιστοποιείται, γιατί διαφορετικά ένας επιτιθέμενος μπορεί να δημιουργήσει βρόχους μέσω της επίθεσης μίμησης. Τέλος, το SEAD δεν ανταπεξέρχεται στις επιθέσεις 'σκουληκότρυπας'.

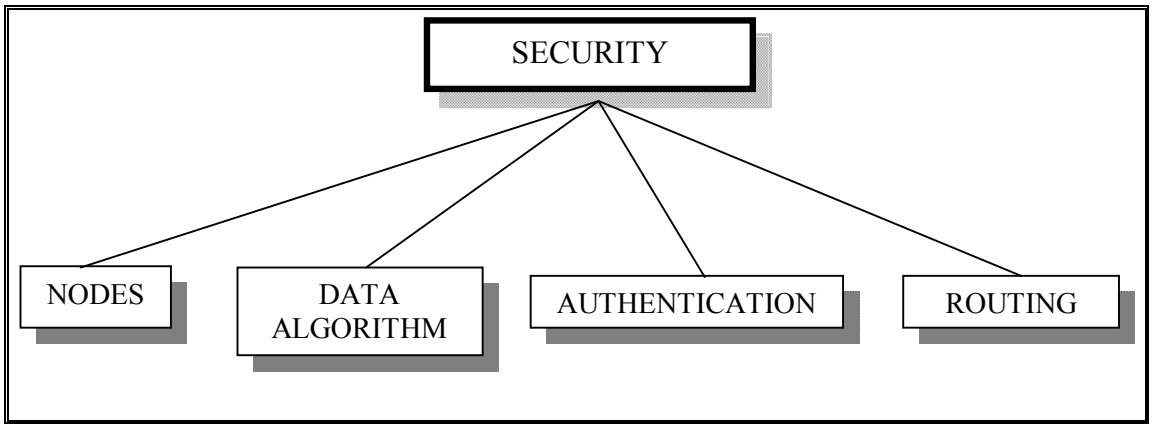
ΚΕΦΑΛΑΙΟ 5^{Ο}

CLASSIFICATION ΑΣΦΑΛΕΙΑΣ

5.1 Ταξινόμηση (classification) μέτρων ασφαλείας

Στα προηγούμενα κεφάλαια αναφερθήκαμε διεξοδικά στα δίκτυα ad hoc και στα δίκτυα αισθητήρων (*sensor networks*), όπως επίσης και στα θέματα ασφαλείας που διέπουν τα παραπάνω δίκτυα.

Σ' αυτό το κεφάλαιο θα προσπαθήσουμε να ταξινομήσουμε την ασφάλεια των δικτύων. Ουσιαστικά, όταν αναφερόμαστε σε ασφάλεια δικτύων, εννοούμε οποιαδήποτε μέτρα λαμβάνονται ώστε ένα μήνυμα που παράγεται από έναν κόμβο να μπορέσει να φτάσει στον προορισμό του χωρίς να αλλοιωθεί ή καταστραφεί ή «εξαφανιστεί» από κάποιον κακόβουλο τρίτο. Τα μέτρα ασφαλείας που λαμβάνονται μπορούν να ταξινομηθούν σε τέσσερις κατηγορίες (Σχήμα 27): Στην αυτασφάλιση των κόμβων, στους αλγόριθμους με τους οποίους πρέπει να κρυπτογραφούνται τα δεδομένα, στην εργασία της πιστοποίησης (*authentication*) και τέλος στην εργασία της δρομολόγησης.



Σχήμα 27. Ταξινόμηση των μέτρων ασφαλείας.

Οι κόμβοι, ως μονάδες ασφαλείας, είναι αυτοί που θα εφαρμόσουν όλα τα ληπτέα μέτρα. Οι αλγόριθμοι που θα χρησιμοποιηθούν πρέπει να είναι δυνατοί ώστε να κρατήσουν τα δεδομένα μας κρυφά από επιτιθέμενους. Η πιστοποίηση μάς επιτρέπει να γνωρίζουμε από που στάλθηκαν τα δεδομένα. Τέλος, η εργασία της δρομολόγησης είναι αυτή που θα επιτρέψει την επικοινωνία από ασφαλείς δρόμους του δικτύου.

Στο υπόλοιπο του κεφαλαίου θα αναλύσουμε διεξοδικά τα τέσσερα αυτά βασικά κομμάτια για την ασφάλιση του δικτύου.

5.2 Ο κόμβος

Τα ad hoc δίκτυα είναι ασύρματα δίκτυα που αποτελούνται από μεγάλο αριθμό μικροσκοπικών συσκευών οι οποίες με τη σειρά τους απαρτίζονται από κυκλώματα

επεξεργασίας, ασύρματο πομποδέκτη και συσκευές ανίχνευσης (αν πρόκειται για κυκλώματα αισθητήρων). Αυτές οι συσκευές ονομάζονται κόμβοι (ή αισθητήρες αντίστοιχα). Όπως αναφέρθηκε σε προηγούμενο κεφάλαιο, κάθε κόμβος αποτελείται από διάφορα στοιχεία εκ των οποίων τα σημαντικότερα είναι ο επεξεργαστής, ο πομποδέκτης, μια μονάδα ισχύος και η αισθητήρια μονάδα (σε περίπτωση που πρόκειται για κόμβο ad hoc δικτύου αυτή η μονάδα δεν υφίσταται). Όταν αναπτύσσονται οι κόμβοι, οργανώνουν ένα δίκτυο ώστε να συνδυάσουν τις παρατηρήσεις τους και να παρέχουν μια σφαιρική άποψη της επιτηρούμενης περιοχής.

Το πρόβλημα με τους συγκεκριμένους κόμβους είναι οι περιορισμένες δυνατότητες απόδοσης λόγω της μικρής ισχύος του επεξεργαστή (CPU clocks) και της χωρητικότητας της μνήμης τους. Επιπλέον είναι ενεργοί για περιορισμένο χρονικό διάστημα λόγω της μικρής παροχής από την μπαταρία τους (95). Επίσης, η κινητικότητα των κόμβων οδηγεί στο συχνό ‘σπάσιμο’ των δρομολογίων επικοινωνίας προκαλώντας αποτυχίες στο δίκτυο [95].

Κλασικά παραδείγματα κόμβων είναι τα παρακάτω:

- Ο κόμβος Mica Motes που αναπτύχθηκε από το US Berkeley και διανεμήθηκε από την Crossbow Technology [43] αποτελεί το πρότυπο για τις έρευνες σε δίκτυα αισθητήρων. Αποτελείται από έναν 8-bit χαμηλής ισχύος μικροεπεξεργαστή που τρέχει στα 4 MHz, 128 KB εσωτερικής FLASH μνήμης προγράμματος, 4KB εσωτερικής SRAM μνήμης δεδομένων, 512KB εξωτερικής FLASH μνήμης δεδομένων, αρκετούς αισθητήρες και ασύρματο περιβάλλον επικοινωνίας.
- Το TmoteSky (ή Telos B), που αναπτύχθηκε από την Moteiv και διανεμήθηκε από την Crossbow, αποτελεί ένα παράδειγμα πιο περιορισμένης συσκευής από άποψη προγραμματιστικής μνήμης. Αποτελείται από έναν εξαιρετικά χαμηλής ισχύος 16-bit μικροεπεξεργαστή που τρέχει στα 8 MHz, 48 KB εσωτερικής FLASH μνήμης προγράμματος, 10 KB εσωτερικής SRAM μνήμης δεδομένων, 1024KB εξωτερικής FLASH μνήμης δεδομένων, αρκετούς αισθητήρες και ασύρματο περιβάλλον επικοινωνίας.

Οι κόμβοι λειτουργούν βάσει πέντε βασικών περιορισμών [96]:

- Οι κόμβοι είναι ανώνυμοι, δηλαδή δεν έχουν χρόνο παραγωγής ή ιδιότητες στον χρόνο εκτέλεσης.
- Κάθε κόμβος, και ιδιαίτερα οι αισθητήρες που δουλεύουν σε ασύρματο περιβάλλον χωρίς την ανθρώπινη παρέμβαση, έχει ένα μη ανανεώσιμο προϋπολογισμό ενέργειας.
- Οι κόμβοι βρίσκονται σε μια κατάσταση ‘ύπνου’ τον περισσότερο χρόνο, ξυπνώντας σε άτακτα χρονικά διαστήματα για περιορισμένο χρόνο για να επιτελέσουν την αποστολή τους.
- Με την ανάπτυξη του δικτύου, οι κόμβοι πρέπει να εργάζονται χωρίς επιτήρηση καθώς η ανθρώπινη παρέμβαση είναι μη πρακτική και ανεπιθύμητη.
- Τέλος, οι κόμβοι έχουν μια μέση εμβέλεια μετάδοσης, συνήθως λίγα μέτρα όπου μπορούν να στέλνουν και να δέχονται ένα ευρύ φάσμα συχνοτήτων.

Ουσιαστικά τα σενάρια ανάπτυξης των δικτύων μπορούν να χωριστούν σε δύο φάσεις: στην φάση εκκίνησης (bootstrapping phase) και στην φάση ομαλής

λειτουργίας. Κατά την φάση έναρξης, λαμβάνουν χώρα πολλές διαδικασίες ασφαλείας που είναι απαραίτητες, όπως είναι ένα σχήμα διανομής κλειδιού που εξασφαλίζει την κωδικοποίηση από άκρο σε άκρο, μια αρχική κατάστρωση της τοπολογίας του περιβάλλοντος και άλλα θέματα, όπως καλυμμένη συνάθροιση δεδομένων (concealed data aggregation). Κατά την ομαλή λειτουργία, για την ασφάλεια των δεδομένων, λαμβάνουν χώρα άλλες τεχνικές όπως κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων, ανίχνευση εισβολέων κ.ά.

Εμείς παρακάτω θα εξετάσουμε τέσσερα θέματα που αφορούν στην ασφάλεια των κόμβων σε ένα εχθρικό περιβάλλον. Τα θέματα αυτά είναι η *διανομή κλειδιού (key distribution)*, *ο εντοπισμός* (*localization*), *η αυτό-διάρθρωση διεύθυνσης (address auto configuration)* και η *ανίχνευση εισβολέων* (*intrusion detection)*.

5.2.1 Διανομή κλειδιού (Key distribution)

Τα κλειδιά είναι βασικά κομμάτια της ασφάλειας των δικτύων γιατί μας επιτρέπουν να διαβάζουμε μηνύματα που υπό άλλες συνθήκες θα ήταν ακατάληπτα και να υπογράψουμε με ψηφιακές υπογραφές έγγραφα και άλλα αρχεία. Τα πρωτόκολλα κρυπτογράφησης χρησιμοποιούν κλειδιά για να αναγνωρίσουν οντότητες και να αποκτήσουν πρόσβαση σε φυλασσόμενες πληροφορίες [97]. Γι' αυτό είναι αναγκαίο τα κλειδιά να παράγονται και να διανέμονται με ασφάλεια σε κατάλληλες οντότητες.

Τα μυστικά κλειδιά μοιράζονται μεταξύ επικοινωνούντων κόμβων. Ένα μυστικό κλειδί μπορεί να παραχθεί από μια οντότητα και να διανεμηθεί σε μια άλλη είτε μέσω απευθείας επικοινωνίας είτε μέσω ενός ασφαλούς καναλιού. Στην κρυπτογραφία δημόσιου κλειδιού, το δημόσιο κλειδί είναι γνωστό σε όλους, ενώ το ιδιωτικό κλειδί κρατείται μυστικό.

Υπάρχουν δύο τρόποι να διανεμηθούν μυστικά κλειδιά: μέσω προ-εγκατεστημένου ασφαλούς καναλιού ή μέσω ενός ανοιχτού καναλιού [97]. Τα δημόσια κλειδιά διανέμονται μέσω πιστοποιητικών (*certificates*). Τα πιστοποιητικά 'δένουν' ένα δημόσιο κλειδί με μία οντότητα. Ένα πιστοποιητικό μπορεί να περιγραφεί συμβολικά ως:

$$\boldsymbol{C_A = Sig_{KS}(T_S, L, A, K_A, V_A)}$$

όπου T_s είναι η ημερομηνία και η ώρα έναρξης του πιστοποιητικού, L είναι το χρονικό διάστημα κατά το οποίο είναι έγκυρο, A είναι το όνομα του χρήστη, K_A είναι το δημόσιο κλειδί και V_A είναι το κλειδί επαλήθευσης υπογραφής (*public signature verification key*). Σε μια συγκεντρωτική προσέγγιση υπάρχει ένα εμπιστευτικό τρίτο κομμάτι επικοινωνίας που ονομάζεται αρχή πιστοποίησης (*certification authority, CA*).

Ένα από τα πρώτα πρωτόκολλα διανομής δημόσιου κλειδιού δημιουργήθηκε από τους Dorothy Denning και Giovanni Sacco, οι οποίοι το 1981 πρότειναν ότι δύο χρήστες (που τους ονόμασαν *Alice* και *Bob*) εγκατέστησαν ένα μυστικό κλειδί K_{AB} ως εξής: Όταν η Alice αρχικά θέλει να επικοινωνήσει με τον Bob, πάει στην CA και παίρνει τρέχοντα αντίγραφα πιστοποιητικών δημοσίου κλειδιού γι' αυτήν και τον Bob. Στη συνέχεια δημιουργεί ένα πακέτο που περιέχει μια αποτύπωση χρόνου T_A (timestamp), ένα κλειδί συνέλευσης K_{AB} και μια υπογραφή την οποία υπολογίζει σε αυτά τα αντικείμενα χρησιμοποιώντας το ιδιωτικό της κλειδί υπογραφής.

Κρυπτογραφεί όλο αυτό το πακέτο υπό το δημόσιο κλειδί του Bob και στη συνέχεια του το αποστέλλει. Συμβολικά η όλη ενέργεια παριστάνεται ως εξής:

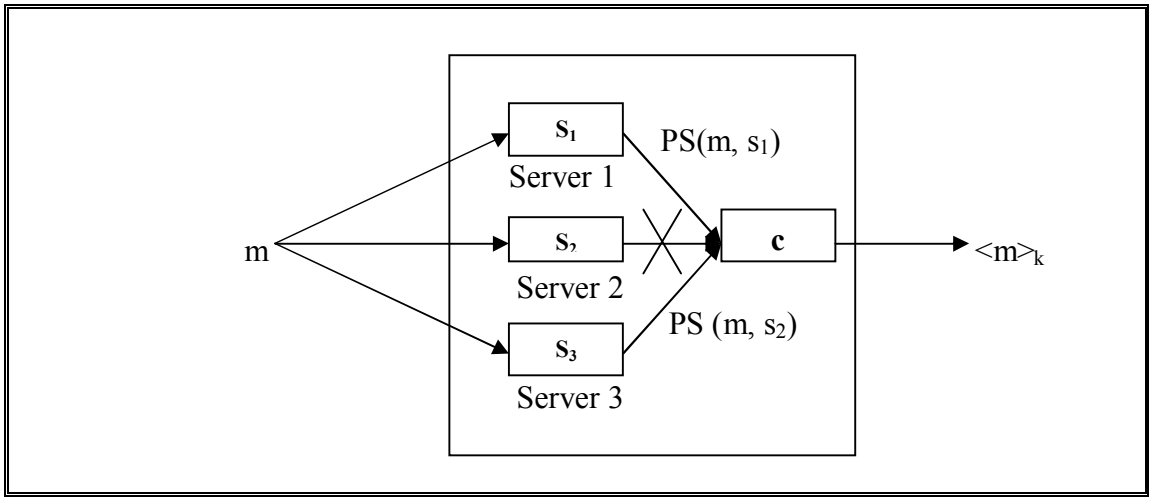
$$\boldsymbol{A \rightarrow B: C_A, C_B, \{T_A, K_{AB}, Sig_{KA}(T_A, K_{AB})\}_{KB}}$$

Αντίθετα, κατά τη μη συγκεντρωτική προσέγγιση, υπάρχουν δύο τύποι διανομής δημόσιου κλειδιού [98]:

- Μέσω ενός αποκεντρωμένου κέντρου διανομής κλειδιού.
- Μέσω ιδιαίτερων κόμβων που αποτελούν το δίκτυο.

α. Αποκεντρωμένο κέντρο διανομής κλειδιού

Στην περίπτωση αυτή ανήκει το αποκεντρωμένο Κέντρο Διανομής Κλειδιού (*Key Distribution Center, KDC*) το οποίο πρότειναν οι Zhou και Haas (39). Το κέντρο αυτό διαχωρίζει τις ευθύνες των πιστοποιητικών και του διαχωρισμού κλειδιών σε ένα γκρουπ κόμβων (Σχήμα 28). Οποιαδήποτε υποομάδα του γκρουπ με μέγεθος μεγαλύτερο από ένα κατώφλι μπορεί να χορηγήσει πιστοποιητικά. Η λειτουργία του σχήματος στηρίζεται στην κρυπτογραφία κατωφλίου (*threshold cryptography*) [99].



Σχήμα 28. Αποκεντρωμένη διανομή κλειδιού.

Βάσει αυτού του σχήματος, ας θεωρήσουμε ότι το KDC έχει ένα δημόσιο κλειδί K_{CA} και ένα ιδιωτικό κλειδί K_{CA}^{-1}. Κάθε κόμβος έχει ένα κομμάτι του ιδιωτικού κλειδιού K_{CA}^{-1}. Αν υποθέσουμε ότι το κατώφλι των κόμβων που μπορούν να παρέχουν πιστοποίηση είναι 4, τότε οποιοιδήποτε 4 κόμβοι του δικτύου μπορούν να παρέχουν πιστοποίηση και διανομή κλειδιού σε οποιοδήποτε άλλο. Κάθε κόμβος αποθηκεύει τα δημόσια κλειδιά όλων των κόμβων του δικτύου.

β. Δημοκρατική διανομή κλειδιού

Όπως σε μια δημοκρατική κοινωνία κάθε πολίτης συμμετέχει στα κοινά, έτσι και οι Hubaux, Buttyan και Capkun πρότειναν μία αυτό-οργανωμένη υποδομή δημοσίου κλειδιού για δίκτυα ad hoc, στην οποία κάθε κόμβος συμμετέχει στη διαδικασία διανομής κλειδιού [68]. Τα πιστοποιητικά εκδίδονται από ανεξάρτητους κόμβους του δικτύου. Οι κόμβοι θεωρούνται ότι είναι έντιμοι, δηλαδή δεν εκδίδουν ψεύτικα

πιστοποιητικά. Κάθε κόμβος διατηρεί το δικό του απόθεμα από πιστοποιητικά που εκδίδονται από αυτόν και από άλλους κόμβους, αποφεύγοντας έτσι οποιαδήποτε αποτυχία.

Η όλη διαδικασία ακολουθεί την εξής λογική: όταν δύο κόμβοι θέλουν να έχουν μια ασφαλή επικοινωνία, υπολογίζουν το δημόσιο κλειδί μέσω μιας αλυσίδας πιστοποιητικών (που εκτελείται από τον έναν κόμβο στον άλλο), συνδυάζοντας τα προσωπικά τους αποθέματα σε πιστοποιητικά.

Ένα μειονέκτημα στη δημοκρατική διανομή κλειδιού είναι η πολυπλοκότητα στην εμπιστοσύνη. Στη συγκεντρωτική διανομή κλειδιού, έχουμε ένα ορισμένο επίπεδο εμπιστοσύνης στα πιστοποιητικά, αφού αφήνουμε την εμπιστοσύνη στο KDC. Στη δημοκρατική διανομή, η εμπιστοσύνη είναι μια συνάρτηση από την εμπιστοσύνη που έχουμε σε κάθε κόμβο κατά μήκος της αλυσίδας που χρησιμοποιούμε.

Ένας άλλος τρόπος για να πετύχουμε διανομή κλειδιού είναι η συμμετρική κρυπτογραφία. Η κρυπτογραφία δημόσιου κλειδιού έχει μεγαλύτερο υπολογιστικό κόστος από την συμμετρική κρυπτογραφία. Χρειάζεται μεγαλύτερο κλειδί για την ίδια μορφή ασφάλειας και επακόλουθα μεγαλύτερη μνήμη και εύρος ζώνης επικοινωνίας. Το μεγάλο υπολογιστικό κόστος δεν μπορεί να καλυφθεί από τους κόμβους των ad hoc δικτύων. Έτσι τα ad hoc δίκτυα χρησιμοποιούν κυρίως συμμετρικά κλειδιά και όχι δημόσια κλειδιά [100]. Φυσικά αυτά τα σχήματα έχουν το μειονέκτημα ότι δεν είναι τόσο ευέλικτα όσο τα σχήματα δημόσιου κλειδιού.

Υπάρχουν φυσικά και άλλοι μέθοδοι διανομής κλειδιού εκτός της συμμετρικής και ασύμμετρης (δημοσίου κλειδιού) προσέγγισης. Αυτά τα σχήματα ονομάζονται υβριδικά σχήματα τα οποία στηρίζονται σε τεχνικές ελλειπτικής κρυπτογραφίας (*Elliptic Curve Cryptography*). Οι τεχνικές αυτές συνδυάζουν τα πλεονεκτήματα και των δύο μεθόδων κρυπτογραφίας. Έτσι, είναι πιο εύκαμπτες σε επιθέσεις μίμησης από ότι αυτές που χρησιμοποιούν συμμετρικές τεχνικές, αφού επιτρέπουν σε κάθε κόμβο να αναγνωρίζεται μοναδικά. Επιπλέον, επιτρέπουν την πολυφασική διανομή κλειδιού όταν κάποιος κόμβος ή κάποια γενιά κόμβων εισέρχεται στο δίκτυο. Επιπρόσθετα, αυτές οι τεχνικές αποτρέπουν κάποιους κόμβους που ανήκουν σε μία γενιά κόμβου να μιμηθούν έναν κόμβο που βρίσκεται σε άλλη γενιά (μια επίθεση που είναι γνωστή ως επίθεση ψεύτικης γενιάς - fake generation attack). Δυστυχώς, παρόλο που αυτά τα σχήματα είναι πιο αποτελεσματικά για τα δίκτυα ad hoc και ιδιαίτερα για τα δίκτυα αισθητήρων, είναι πιο ενεργοβόρα από τα συμμετρικά πρωτόκολλα.

Ένα παράδειγμα τέτοιου σχήματος είναι το [85], όπου συνδυάζεται η τεχνική εγκατάστασης κλειδιού Elliptic Curve Diffie-Hellmann (*ECDH*) με τεχνικές συμμετρικής κρυπτογράφησης και αναλύθηκε στο προηγούμενο κεφάλαιο. Τα πλεονεκτήματα αυτής της μεθόδου μπορούμε να τα δούμε σε όρους υπολογιστικούς, επικοινωνίας και απαιτήσεις αποθήκευσης. Έτσι, από υπολογιστικής πλευράς, υπάρχει μια μείωση 20% από ότι σε άλλα υβριδικά σχήματα όταν υπολογίζονται με τα ίδια μετρικά μεγέθη. Από άποψη επικοινωνίας, το πρωτόκολλο χρειάζεται 4 μηνύματα για να διανεμηθεί-εγκατασταθεί το κλειδί, που ισούται με 186 bytes (περίπου ίδιο μέγεθος με άλλες τεχνικές).

5.2.2 Εντοπισμός (Localization)

Στα δίκτυα αισθητήρων, οι κόμβοι αναπτύσσονται σε μια απροσχεδίαστη υποδομή όπου δεν υπάρχει εκ των προτέρων γνώση της θέσης. Το πρόβλημα του υπολογισμού των συντεταγμένων των κόμβων αναφέρεται ως *εντοπισμός (localization)*. Μία λύση στο πρόβλημά μας είναι η χρήση του GPS (Global Positioning System). Όμως

υπάρχουν ορισμένα προβλήματα με την χρήση του [101]. Οι πομποί του GPS είναι πολύ ακριβοί και ανάρμοστοι για δημιουργία φθηνών και μικρών κόμβων αισθητήρων. Επιπλέον, το GPS δεν μπορεί να δουλέψει υπό την παρουσία οποιουδήποτε εμποδίου, όπως πυκνής φυλλωσιάς κ.ά. Συνεπώς, οι κόμβοι ενός δικτύου πρέπει να χρησιμοποιούν άλλα μέσα για να εδραιώσουν την θέση τους και να οργανώσουν το δίκτυο σε ένα σύστημα συντεταγμένων, χωρίς να στηρίζονται σε κάποια υπάρχουσα υποδομή.

Η διαδικασία του εντοπισμού και του προσδιορισμού της θέσης έχει διάφορες ιδιότητες, οι σημαντικότερες από τις οποίες είναι οι παρακάτω [102]:

- *Φυσική τοποθέτηση έναντι συμβολικής θέσης*. Η τάση είναι να χρησιμοποιούμε την τοποθεσία ως έναν γενικό όρο. Πρέπει να ταιριάξουμε όσο το δυνατόν την φυσική θέση του κόμβου με τη συμβολική τοποθεσία μέσα στο δίκτυο.
- *Απόλυτες έναντι σχετικών συντεταγμένων*. Ένα απόλυτο σύστημα συντεταγμένων είναι έγκυρο για όλα τα αντικείμενα του δικτύου με κάποιο βαθμό αναφοράς. Οι σχετικές συντεταγμένες, από την άλλη μεριά, διαφέρουν για οποιοδήποτε τοποθετημένο αντικείμενο του δικτύου. Για να παρέχουμε απόλυτες συντεταγμένες στο δίκτυο χρησιμοποιούμε ορισμένα σταθερά σημεία (τουλάχιστον τρία σε ένα 2D σύστημα). Αυτά τα σημεία είναι κόμβοι οι οποίοι γνωρίζουν τη θέση τους στο απόλυτο σύστημα συντεταγμένων.
- *Τοπικοί έναντι κεντρικών υπολογισμών*. Οι τοπικοί υπολογισμοί είναι υπολογισμοί που εκτελούνται τοπικά στους συμμετέχοντες κόμβους, ενώ αντίθετα οι κεντρικοί υπολογισμοί είναι υπολογισμοί που εκτελούνται σε έναν κεντρικό σταθμό, ο οποίος υπολογίζει τη θέση ή την τοποθεσία και τις διανέμει πίσω στους συμμετέχοντες κόμβους.
- *Ακρίβεια και ορθότητα (accuracy and precision)*. Είναι τα σημαντικότερα στοιχεία ενός συστήματος εντοπισμού θέσης. Η ορθότητα της θέσης είναι η μεγαλύτερη απόσταση μεταξύ της εκτιμώμενης και της πραγματικής θέσης. Η ακρίβεια είναι το ποσοστό της ορθότητας που πετυχαίνεται κατά μέσο όρο σε διαδοχικές προσπάθειες εντοπισμού μιας θέσης.
- *Κλιμάκωση*. Ένα σύστημα μπορεί να προορίζεται για διαφορετικές κλίμακες, για παράδειγμα εσωτερική ή εξωτερική ανάπτυξη. Δύο σημαντικές παράμετροι είναι η έκταση την οποία μπορεί να καλύψει ένα σύστημα και ο αριθμός των προσδιοριζόμενων αντικειμένων.
- *Περιορισμοί*. Για κάποιες τεχνικές υπάρχουν περιορισμοί κατά την ανάπτυξη, όπως περιορισμοί λειτουργίας, περιορισμοί εύρους στο οποίο μπορούν να λειτουργήσουν κ.ά.
- *Κόστος*. Τα συστήματα προσδιορισμού θέσης δημιουργούν κόστος σε χρόνο (εγκατάσταση υποδομής, διαχείρισης), χώρο (μέγεθος συσκευής, χώρο για την υποδομή), ενέργεια (κατά τη διάρκεια της λειτουργίας) και κεφάλαια (κόστος κόμβου, εγκατάσταση δικτύου).

Υπάρχουν τρείς κύριες τεχνικές για τον καθορισμό της θέσης ενός κόμβου [103]: χρησιμοποιώντας πληροφορίες για την γειτονιά του κόμβου (εγγύτητα), εκμεταλλευόμενοι γεωμετρικές ιδιότητες (τριγωνισμός ή τριμερισμός) και

αναλύοντας χαρακτηριστικές ιδιότητες μίας θέσης του κόμβου σε σχέση με κάποιες προ-μετρημένες ιδιότητες (ανάλυση σκηνής). Παρακάτω παρουσιάζεται μια επισκόπηση αυτών των τεχνικών:

α. Εγγύτητα

Είναι η πιο απλή από τις τεχνικές εντοπισμού θέσης και στηρίζεται στην εκμετάλλευση του πεπερασμένου βεληνεκούς των ασύρματων επικοινωνιών. Μπορεί να χρησιμοποιηθεί για να αποφασιστεί αν ένας κόμβος που θέλει να προσδιορίσει την θέση του βρίσκεται στη γειτονιά ενός σταθερού σημείου (*anchor*). Ένα παράδειγμα είναι ο φυσικός περιορισμός των υπέρυθρων επικοινωνιών από τοίχους, που χρησιμοποιούνται για να παρέχουν σε ένα κόμβο μια απλή πληροφορία τοποθεσίας.

β. Τριγωνισμός και τριμερισμός

Σε αντίθεση με την εγγύτητα, η επικοινωνία μεταξύ δύο κόμβων επιτρέπει την εξαγωγή πληροφορίας για την γεωμετρική σχέση τους. Για παράδειγμα, μπορεί να υπολογιστεί η απόσταση μεταξύ δύο κόμβων ή η γωνία σε ένα τρίγωνο. Όταν χρησιμοποιείται η απόσταση μεταξύ δύο οντοτήτων, η τεχνική καλείται *τριμερισμός*, ενώ όταν χρησιμοποιούνται οι γωνίες μεταξύ κόμβων, τότε μιλάμε για *τριγωνισμό*.

Για τον *τριμερισμό* σε ένα επίπεδο, το απλούστερο σενάριο για έναν κόμβο είναι να διαθέτει ακριβείς μετρήσεις απόστασης από τρία μη συγγραμμικά σταθερά σημεία. Σε έναν 3D χώρο χρειάζονται τέσσερα σταθερά σημεία. Χρησιμοποιώντας αποστάσεις ή γωνίες, η θέση του κόμβου πρέπει να βρίσκεται στην τομή τριών κύκλων γύρω από τα σταθερά σημεία.

γ. Ανάλυση σκηνής

Μία τελείως διαφορετική τεχνική είναι η ανάλυση σκηνής. Η πιο εμφανής πρακτική είναι να αναλυθούν φωτογραφίες που λαμβάνονται από μία κάμερα και να προσπαθήσουμε να προσδιορίσουμε τη θέση από αυτές τις φωτογραφίες. Αυτό απαιτεί επιπλέον υπολογιστικό έργο και είναι απαγορευτικό για τους κόμβους των ad hoc και sensor δικτύων.

Εκτός όμως της παραπάνω πρακτικής, υπάρχουν και άλλα χαρακτηριστικά αποτυπώματα που μπορούν να χρησιμοποιηθούν για την εύρεση της θέσης, για παράδειγμα το μοτίβο διάδοσης των ραδιοκυμάτων. Μια μέθοδος είναι να χρησιμοποιήσουμε τις μετρήσεις των σημάτων κατά την εκπομπή ενός γνωστού σήματος και να τα συγκρίνουμε με πραγματικές τιμές που είναι αποθηκευμένες σε μια βάση δεδομένων. Έτσι, το σύστημα RADAR [104] είναι ένα παράδειγμα που χρησιμοποιεί αυτήν την προσέγγιση για να καθορίσει θέσεις σε ένα κτήριο.

Εδώ πρέπει να ξεχωρίσουμε τον εντοπισμό θέσεως σε εντοπισμό ενός άλματος και σε αντίστοιχο πολλαπλών αλμάτων. Βάσει αυτού του διαχωρισμού, προέκυψαν πολλά συστήματα εντοπισμού θέσεως. Κατά τον εντοπισμό ενός άλματος, ένας οποιοσδήποτε κόμβος με άγνωστες συντεταγμένες μπορεί να επικοινωνήσει απευθείας με κάποιο σταθερό σημείο (anchor). Σε αυτήν την κατηγορία υπάρχουν τα παρακάτω συστήματα [105]:

- Το σύστημα Active Badge Location System [106] που χρησιμοποιεί διαχεόμενη υπέρυθρη ακτινοβολία ως μέσο μετάδοσης και εκμεταλλεύεται τον φυσικό

περιορισμό των υπέρυθρων κυμάτων από τους τοίχους ως οριοθέτηση για την αναλυτικότητα της τοποθεσίας.

- Το σύστημα Active Office [107], όπου χρησιμοποιείται υπέρηχος, με τους πομπούς τοποθετημένους σε καλά γνωστά σημεία του χώρου. Οι συσκευές που θα εντοπιστούν λειτουργούν σαν πομποί των υπερήχων.
- Το σύστημα RADAR [104] που χρησιμοποιεί τεχνικές ανάλυσης σκηνής, συγκρίνοντας τα χαρακτηριστικά του λαμβανόμενου συστήματος από πολλαπλούς anchors με προηγούμενες μετρημένες και αποθηκευμένες τιμές.
- Στο σύστημα Cricket [108] οι ίδιοι οι κόμβοι υπολογίζουν την θέση τους στηριζόμενοι σε συνδυασμό ραδιοφωνικών παλμών και υπέρηχων.
- Στην επικοινωνία επικάλυψης [109] το σύστημα δεν χρησιμοποιεί αριθμητικές μετρήσεις. Αντίθετα, προσπαθεί να χρησιμοποιήσει μόνο την παρατήρηση της συνδεσιμότητας με μία ομάδα anchors για να καθοριστεί η θέση του κόμβου.

Κατά τον εντοπισμό πολλαπλών αλμάτων στηριζόμαστε σε πληροφορίες συνδεσιμότητας και θεωρούμε την εύρεση της θέσης ενός κόμβου ως ένα πρόβλημα πιθανοτήτων. Έτσι, αν θεωρήσουμε ότι οι θέσεις *n* anchors είναι γνωστές και απαιτούνται οι θέσεις *m* κόμβων, η σύνδεση μεταξύ οποιοδήποτε δύο κόμβων είναι πιθανή μόνο εάν οι δύο αυτοί κόμβοι βρίσκονται εντός μιας γνωστής εμβέλειας R [110]. Μια άλλη τεχνική που χρησιμοποιείται είναι να πλημυρίσουμε το δίκτυο με πληροφορία, η οποία θα ξεκινάει ανεξάρτητα από κάθε anchor. Είναι μια παρόμοια τεχνική με τα πρωτόκολλα απομακρυσμένου διανύσματος (*Distance Vector Protocol*). Έτσι, βάσει αυτής της τεχνικής, μπορούμε να μετρήσουμε τον αριθμό των αλμάτων (στη συντομότερη διαδρομή) μεταξύ δύο anchors και να την χρησιμοποιήσουμε για να υπολογίσουμε το μήκος ενός άλματος διαιρώντας το άθροισμα των αποστάσεων από τους anchors προς το άθροισμα των αλμάτων. Μία διαφορετική τεχνική είναι να χρησιμοποιήσουμε την θέση κανονικών κόμβων, όταν αυτοί την έχουν υπολογίσει. Κατά αυτήν την τεχνική, όταν ένας κόμβος ξέρει τις συντεταγμένες του μπορεί να χρησιμοποιηθεί ως σταθερό σημείο μαζί με άλλους δύο anchors για να υπολογίσει τη θέση ένας τρίτος κόμβος. Η παραπάνω τεχνική καλείται *επαναληπτικός πολυμερισμός* [111]. Μια παραλλαγή της προηγούμενης τεχνικής είναι να θέσουμε βάρη σε όσες θέσεις έχουν υπολογιστεί και να λύσουμε ένα τροποποιημένο πρόβλημα βελτιστοποίησης που επακολουθεί στη σύγκλιση όλων των σεναρίων. Η τεχνική αυτή καλείται *συνεργατικός πολυμερισμός* [111]. Τέλος, στην *πιθανολογική περιγραφή θέσης* [112], περιγράφεται η θέση ενός κόμβου από μια συνάρτηση πιθανότητας της τυχαίας θέσης του κόμβου, δίνοντας ένα μεγάλο μέρος πληροφορίας που είναι απαραίτητη για την τοποθεσία που βρίσκεται ο κόμβος.

Όπως είδαμε, ο εντοπισμός της θέσης ενός κόμβου σε ένα δίκτυο επιβαρύνει τους ήδη περιορισμένους σε πηγές κόμβους με επιπλέον φόρτο εργασίας και τον κίνδυνο της ανακρίβειας. Η συνηθέστερη τεχνική για την εύρεση της θέσης ενός κόμβου είναι η χρήση σταθερών σημείων (anchors), είτε αυτά είναι οι σταθμοί βάσης των δικτύων είτε κάποιοι άλλοι κόμβοι του δικτύου. Η τεχνική του εντοπισμού θέσης είναι σημαντική για την ασφάλεια του δικτύου καθόσον πρέπει ο κάθε κόμβος να γνωρίζει το άμεσο περιβάλλον του και τι χαρακτηριστικά έχει αυτό. Επιπλέον, ο χρόνος και το κόστος που δημιουργείται από την εκπομπή μηνυμάτων σε μια έμμεση επικοινωνία δεν πρέπει να αμεληθεί.

5.2.3 Αυτό-διάρθρωση διεύθυνσης (Address auto configuration)

Στα δίκτυα που εξετάζουμε, οι κόμβοι πρέπει να εισέρχονται και να εξέρχονται κατά βούληση. Έτσι, οι κόμβοι πρέπει να εναρμονίζονται δυναμικά με το δίκτυο κατά την είσοδο τους σ' αυτό. Μια λύση στο πρόβλημα είναι η μέθοδος DHCP [113]. Απαιτείται όμως η ύπαρξη ενός κεντρικού DHCP server που διατηρεί την διάρθρωση όλων των κόμβων του δικτύου. Εφόσον όμως τα δίκτυά μας δεν έχουν μια σταθερή υποδομή ή κεντρική διαχείριση, αυτή η λύση δεν είναι η κατάλληλη.

Υπάρχουν και εναλλακτικές λύσεις για την αυτό-διάρθρωση διεύθυνσης [114], όπου ο κόμβος αρχικά δημιουργεί μια προσωρινή διεύθυνση. Αυτή μπορεί να δοθεί χρησιμοποιώντας ένα δεσμευμένο πρόθεμα που δεν ανήκει στο τοπικό δίκτυο (όπως το *MANET_INITIAL_PREFIX*), με σκοπό να εκτελέσουμε επικοινωνία πολλαπλών αλμάτων [115]. Με αυτήν την τεχνική πρέπει να εκτελεστεί η ενέργεια DAD (*duplicate address detection*) για να επιβεβαιωθεί ότι η διεύθυνση που δόθηκε είναι μοναδική. Χρησιμοποιώντας αυτήν την προσωρινή διεύθυνση, ο κόμβος μπορεί να επικοινωνεί με άλλους στο δίκτυο. Επιπλέον, μπορεί να χρησιμοποιηθεί για να βρεθεί η πλησιέστερη πύλη διαφυγής (gateway). Αυτό είναι απαραίτητο για να αποκτηθεί ένα συνολικό πρόθεμα (διεύθυνση) και μπορεί να γίνει με δύο τρόπους [116]:

- Ενεργά, όπου ο κόμβος μεταδίδει ένα τροποποιημένο μήνυμα route request AODV καταδεικνύοντας στην πύλη (μέσω μιας σημαίας) να περιλάβει το πρόθεμά του στο RREP μήνυμα.
- Παθητικά, όπου ο κόμβος δέχεται τροποποιημένη πληροφορία από την πύλη σύμφωνα με το πρωτόκολλο NDP (Neighbor Discovery Protocol) που περιλαμβάνει το πρόθεμά του.

Είναι πιθανό ο κόμβος να λαμβάνει πολλαπλές απαντήσεις από πολλές πύλες . Σ' αυτήν την περίπτωση, ο κόμβος επιλέγει με συγκεκριμένα κριτήρια, όπως το μήκος αλμάτων, το φορτίο που δέχεται η πύλη, η χωρητικότητα κ.ά. Αφού ο κόμβος διαλέξει μία πύλη, χρησιμοποιεί το πρόθεμα για να καθορίσει μια συνολική IP διεύθυνση, ενώ την ίδια στιγμή η προσωρινή διεύθυνση σβήνεται χρησιμοποιώντας τα μηνύματα RERR.

5.2.4 Ανίχνευση εισβολέων (Intrusion detection)

Τυπικά, ένα ad hoc δίκτυο χρησιμοποιεί κρυπτογραφία για να ασφαλιστεί από κακόβουλους εξωτερικούς κόμβους που προσπαθούν να κερδίσουν πρόσβαση στο δίκτυο. Όμως η κρυπτογραφία δεν κάνει πολλά πράγματα για να καταπολεμήσει κακόβουλους κόμβους που έχουν στην κατοχή τους ένα ή περισσότερα κλειδιά. Εξ ορισμού, η ανίχνευση εισβολέων περιλαμβάνει την «αιχμαλώτιση» δεδομένων και την εξακρίβωση της ένδειξης στα δεδομένα ότι το δίκτυο δέχεται επίθεση [90]. Η πιο σημαντική διαφορά μεταξύ των σταθερών δικτύων και των δικτύων ad hoc είναι ότι τα τελευταία δεν έχουν σταθερή υποδομή. Σε σύγκριση με ενσύρματα δίκτυα όπου ο έλεγχος της κίνησης γίνεται με διακόπτες, δρομολογητές και πύλες, το ασύρματο περιβάλλον των ad hoc δικτύων δεν έχει τέτοια σημεία συγκεντρώσεων.

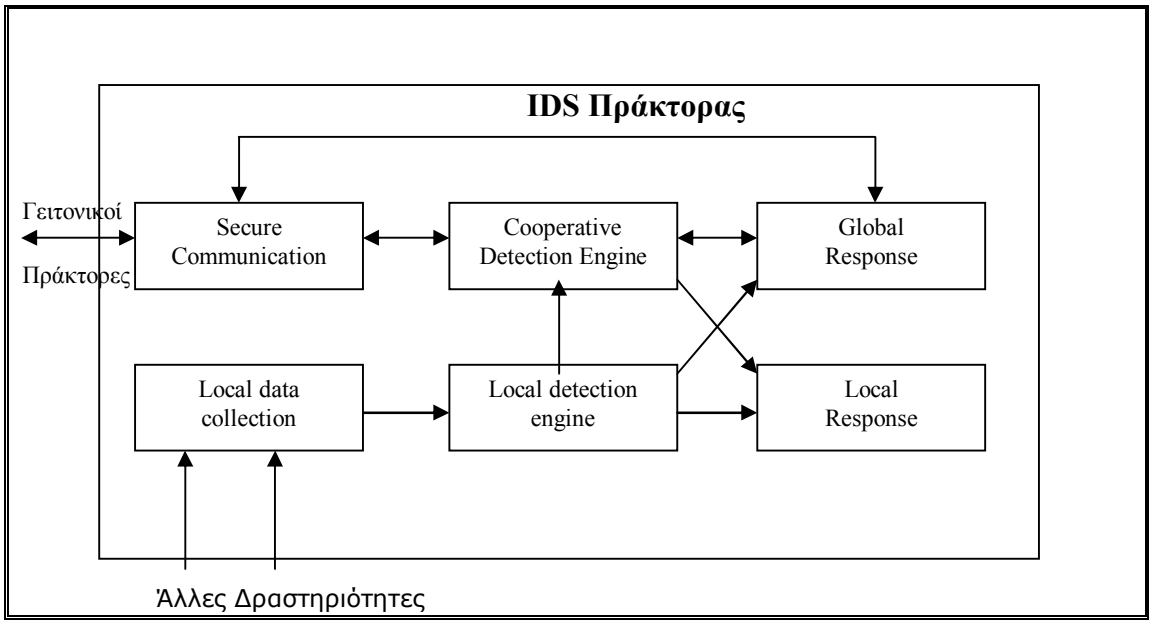
Τα συστήματα ανίχνευσης εισβολέων (*Intrusion Detection Systems-IDS*) μπορούν να χωρισθούν σε δύο κατηγορίες: host-based και network-based [117]. Στα host-based συστήματα, η λειτουργία επικεντρώνεται στην κίνηση που λαμβάνει χώρα σε κάθε κόμβο. Τα συστήματα αυτά είναι ικανά να ανιχνεύσουν ενέργειες όπως επαναλαμβανόμενες αποτυχίες πρόσβασης ή αλλαγές σε κρίσιμα αρχεία του συστήματος και λειτουργούν προσπελάζοντας log files ή ελέγχοντας την χρήση του συστήματος σε πραγματικό χρόνο. Αντίθετα, τα συστήματα network-based λειτουργούν αποκλειστικά με πακέτα που έχουν ανιχνευθεί σε όλο το δίκτυο. Επιπλέον ταξινόμηση των συστημάτων μπορεί να γίνει σε signature-based (ελέγχει το δίκτυο για προκαθορισμένες υπογραφές, χαρακτηριστικές για κάποιον εισβολέα), anomaly-based (καθορίζεται μια σταθερή συμπεριφορά και οποιαδήποτε εκτροπή από αυτήν αποκαλύπτει την εισβολή) και τα specification-based (καθορίζονται μια σειρά από εμπόδια που είναι χαρακτηριστικά για την ομαλή λειτουργία ενός προγράμματος ή πρωτοκόλλου).

Γενικά, η αρχιτεκτονική των IDS εξαρτάται από την υποδομή των δικτύων. Σε ένα επίπεδο δίκτυο, όλοι οι κόμβοι θεωρούνται ίσοι μεταξύ τους ενώ σε ένα πολύ-επίπεδο δίκτυο οι κόμβοι χωρίζονται σε ομάδες (*clusters*) με έναν επικεφαλή (*clusterhead*) σε κάθε ομάδα. Ανάλογα με την υποδομή του δικτύου, οι αρχιτεκτονικές των IDS χωρίζονται ως εξής [117]:

- Στην *Stand- Alone architecture,* όπως λέει και το όνομά της, κάθε κόμβος ενεργεί σαν ένα ανεξάρτητο σύστημα ανίχνευσης και είναι υπεύθυνος για ανίχνευση επιθέσεων που κατευθύνονται σε αυτόν. Σε καμία περίπτωση οι κόμβοι δεν συνεργάζονται μεταξύ τους. Είναι κατάλληλη τεχνική για επίπεδα δίκτυα.
- Η τεχνική *Distributed and Cooperative architecture*. Σε αυτήν την περίπτωση, ένας πράκτορας ανίχνευσης υπάρχει σε κάθε κόμβο (όπως στην προηγούμενη περίπτωση) και οι κόμβοι είναι και πάλι υπεύθυνοι για να ανιχνεύουν τοπικές επιθέσεις, αλλά συνεργάζονται με τους υπόλοιπους κόμβους ανταλλάσοντας πληροφορίες για να ανιχνεύσουν καθολικές προσπάθειες εισβολής.
- Η τελευταία τεχνική που καλείται ιεραρχική αρχιτεκτονική (*hierarchical architecture)* είναι κατάλληλη για πολύ-επίπεδα δίκτυα. Σε αυτήν την τεχνική το δίκτυο διαιρείται σε ομάδες. Κάθε ομάδα έχει τον επικεφαλή της, ο οποίος κατά μία έννοια λειτουργεί σαν σημείο ελέγχου. Κάθε πράκτορας ανίχνευσης ενεργεί μέσα σε μια ομάδα και είναι υπεύθυνος τοπικά να ελέγξει τους κόμβους της ομάδας. Ο επικεφαλής της ομάδας είναι υπεύθυνος τοπικά για τους κόμβους της ομάδας και καθολικά, ελέγχοντας τα πακέτα που κυκλοφορούν στο δίκτυο, αρχίζοντας μια ολική απάντηση όταν ανιχνεύεται μια προσπάθεια εισβολής.

Συνήθως ένας «πράκτορας» IDS αποτελείται από 6 βασικά στοιχεία [73]: Το *local data collection* (συλλέγει τα στοιχεία επιθεώρησης σε πραγματικό χρόνο, τα οποία περιλαμβάνουν τις δραστηριότητες των κόμβων στην εμβέλειά τους), το *local detection engine* (αναλύει τα συγκεντρωμένα δεδομένα για απόδειξη ανωμαλιών), το *local response και το global response* (ενεργοποιούνται σε περίπτωση που έχει ανιχνευτεί με μεγάλη σιγουριά μια ανωμαλία, ανάλογα με το είδος της εισβολής), το *cooperative detection engine* (ενεργοποιείται όταν μια ανωμαλία ανιχνεύεται με

μικρή πιθανότητα) και το *secure communication* (εκτελεί επικοινωνία μεταξύ των διαφόρων πρακτόρων του δικτύου) (Σχήμα 29).



Σχήμα 29. Μοντέλο ενός IDS πράκτορα

Μια καλή αρχιτεκτονική είναι αυτή που προτάθηκε από τον Albers [118] και ανήκει στη δεύτερη κατηγορία (*Distributed and Cooperative architecture*). Ονομάζεται Local Intrusion Detection System (*LIDS*) και αναπτύσσεται σε κάθε κόμβο με σκοπό την εγγύς ασφάλεια, όμως μπορεί να επεκταθεί και σε όλο το δίκτυο. Δύο ειδών πληροφορίες ανταλλάσσονται στο LIDS: πληροφορία ασφάλειας (για να αποκτηθεί συμπληρωματική πληροφορία από συνεργαζόμενους κόμβους) και συναγερμοί εισβολής (για να πληροφορήσει άλλους κόμβους για τοπική ανίχνευση εισβολής). Για τη μεθοδολογία της ανίχνευσης, το LIDS χρησιμοποιεί την ανίχνευση ανωμαλίας και κακομεταχείρισης για καλύτερα αποτελέσματα. Όταν μια τοπική εισβολή ανιχνευθεί, το LIDS εκκινεί μια αντίδραση ενημερώνοντας παράλληλα και τους άλλους κόμβους του δικτύου. Με την λήψη ενός συναγερμού, το LIDS προστατεύει τον εαυτό του από οποιαδήποτε εισβολή.

Το σύστημα ανίχνευσης εισβολέων στοχεύει στην προστασία του δικτύου και των κόμβων από οποιαδήποτε προσπάθεια εισβολής. Παρόλα αυτά, οι επιτιθέμενοι πιθανόν να προσπαθήσουν να επιτεθούν στο ίδιο το σύστημα ανίχνευσης. Οι κόμβοι των δικτύων, λόγω των περιορισμένων πηγών που έχουν, πρέπει να αποφασίσουν αν θα συνεργαστούν με άλλους κόμβους του δικτύου για την καλύτερη ασφάλεια του δικτύου. Τα τελευταία χρόνια έχουν αναπτυχθεί διάφορες τεχνικές και πρωτόκολλα για τη συνεργασία των κόμβων σε ένα δίκτυο ad hoc. Η συνεργασία μεταξύ των κόμβων επιφέρει την ανακάλυψη των κόμβων που παρεκτρέπονται, η οποία παρεκτροπή μπορεί να οδηγήσει σε υποβάθμιση της απόδοσης του συστήματος. Οι κυριότερες τεχνικές και πρωτόκολλα είναι:

- Τεχνικές Watchdog και Pathrater [78]
- Πρωτόκολλο CONFIDANT [119]
- Τεχνική CORE [80]

- Πρωτόκολλο OCEAN [120]

Κατά την τεχνική watchdog ανιχνεύονται παρεκτροπές στη συμπεριφορά ενός κόμβου 'κρυφακούοντας' στην μετάδοση του επόμενου κόμβου. Στη συνέχεια, ένα pathrater βοηθάει στην εύρεση των δρομολογίων που δεν περιέχουν αυτούς τους κόμβους. Το πρωτόκολλο CONFIDANT είναι παρόμοιο με το watchdog και επιπλέον, όταν ένας κόμβος ανακαλύπτει έναν άλλο κόμβο που έχει παρεκτραπεί, στέλνει μηνύματα προειδοποίησης σε άλλους κόμβους του δικτύου. Στην τεχνική CORE ανιχνεύεται ένα συγκεκριμένο είδος κόμβων - οι 'εγωιστές' - και τους αναγκάζει να συνεργαστούν, ενώ το OCEAN στηρίζεται αποκλειστικά σε δικές του παρατηρήσεις για να αποφύγει την αδυναμία της κακής πληροφόρησης από την ανταλλαγή πληροφορίας με άλλους κόμβους. Παρακάτω παρατίθεται σχηματικά (Σχήμα 30) μια σύγκριση των συστημάτων ανίχνευσης [121]:

Techniques		**Watchdog/ Pathrater**	**CONFIDANT**	**CORE**	**OCEAN**	**Cooperative IDS**
Architecture		Distributed and cooperative			Stand alone	Hierarchical
Type of Data collection		Reputation				Statistics
Data Distribution		Negative to source node	Negative to friends	Positive from RREP	no	To clusterhead
Observation	**Self to neighbor**	yes	yes	yes	yes	yes
	Neighbor to neighbor	no	yes	no	yes	yes
Misbehavior detection	**Selfish-routing**	no	yes	yes	yes	yes
	Selfish- packet forwarding	yes	yes	yes	yes	yes
	Malicious-routing	no	yes	no	no	yes
	Malicious-packet forwarding	yes	yes	no	no	yes
Punishment		no	yes	yes	yes	n/a
Avoid misbehaving node in route discovery		no	no	no	yes	n/a

Σχήμα 30. Σύγκριση των IDS για συνεργασία κόμβων.

Μελετώντας το θέμα της ανίχνευσης εισβολής, ολοκληρώσαμε τα ζητήματα ασφαλείας που αφορούν στον κόμβο. Στη συνέχεια εξετάζουμε τους αλγόριθμους που καθορίζουν την επικοινωνία μεταξύ κόμβων.

5.3 Αλγόριθμοι

Ο μεγάλος αριθμός κόμβων σε ένα δίκτυο ad hoc και ακόμη χειρότερα σε ένα δίκτυο αισθητήρων, καθιστά μεγάλη πρόκληση τη σχεδίαση των δικτύων. Για να γίνει καλύτερη η επικοινωνία μεταξύ των κόμβων του δικτύου έχουν δημιουργηθεί διάφοροι αλγόριθμοι. Υπάρχουν σημαντικά πλεονεκτήματα ασφαλείας κατά τη χρησιμοποίηση ενός καλά δομημένου αλγόριθμου.

Συνήθως τα δίκτυα που εξετάζουμε έχουν τρεις βασικές εργασίες να επιτελέσουν [122]:

- *Ανίχνευση.* Το πακέτο ανίχνευσης για έναν πραγματικό κόμβο-αισθητήρα θα εξαρτηθεί από την εφαρμογή που πρέπει να εκτελέσει. Έτσι, ένας αισθητήρας ανίχνευσης βιοχημικών ουσιών θα χρειαστεί μια 'οσφρητική' είσοδο, ενώ ένας

ανιχνευτής τρωκτικών θα χρησιμοποιήσει θερμικά, κινητικά ή ακουστικά πρότυπα.

- *Επεξεργασία.* Ένα σύστημα που αποτελείται από μεγάλο αριθμό υπολογιστικών στοιχείων μπορεί να επεξεργαστεί πληροφορία σε δύο διαφορετικούς δρόμους. Είτε μέσα στον ίδιο τον κόμβο, είτε μέσω δια-επικοινωνίας με άλλους κόμβους. Οι παραδοσιακοί αλγόριθμοι χρησιμοποιούν τον πρώτο τρόπο. Κάθε κόμβος αναλύει τα δεδομένα εισόδου και δημιουργεί ένα συμπέρασμα ανεξάρτητα από τους γείτονές του. Αυτή η τακτική χρησιμοποιεί τους κλασικούς αλγόριθμους, αλλά δεν λαμβάνει υπόψη τις πληροφορίες που ανιχνεύονται από τους γειτονικούς κόμβους. Σε ένα κατανεμημένο υπολογιστικό μοντέλο, κάθε κόμβος είναι υπεύθυνος να εκτελεί την αρχική επεξεργασία για τις δικές του ανιχνευμένες πληροφορίες αλλά η έξοδος του αλγόριθμου εξάγεται ως αποτέλεσμα της επικοινωνίας με τους γείτονές του. Αυτό επιτρέπει στο δίκτυο να εξάγει συμπεράσματα που ένας μόνο κόμβος δεν θα μπορούσε.
- *Ενέργεια.* Όταν η διεργασία της ανίχνευσης έχει τελειώσει, το δίκτυο πρέπει να ενεργήσει. Το δίκτυό μας μπορεί να ενεργήσει είτε επικοινωνώντας με τον χρήστη ή ανακατανέμοντας τις πηγές του. Η αποτελεσματικότητα και η ευαισθησία μπορούν να ρυθμιστούν για να βελτιστοποιηθεί η απόδοση του δικτύου.

Υπάρχει πληθώρα αλγόριθμων που αφορούν στα δίκτυά μας και συνήθως οι αλγόριθμοι αυτοί αφορούν θέματα ανάπτυξης κόμβων, κάλυψης, δικτύου, δρομολόγησης και συγχώνευσης δεδομένων ανίχνευσης (*sensing fusion*). Σαν μια πρώτη ταξινόμηση των αλγορίθμων μπορούμε να τα κατανέμουμε σε *συγκεντρωτικούς* και σε *κατανεμημένους* [123]. Συνήθως τα δίκτυα αισθητήρων λόγω περιορισμών σε μνήμη, υπολογιστικά μέσα και επικοινωνιακές ικανότητες εστιάζονται σε τοπικούς κατανεμημένους αλγόριθμους, αλγόριθμους δηλαδή που χρειάζονται μόνο τοπική πληροφορία.

5.3.1 Ανάπτυξη και κάλυψη δικτύου

Σε μια τυπική εφαρμογή δικτύου, οι κόμβοι κατανέμονται έτσι ώστε να ελέγχουν μια περιοχή ή μια ομάδα σημείων. Όταν η επιλογή της τοποθεσίας είναι πιθανή, τότε χρησιμοποιούμε την *ντετερμινιστική ανάπτυξη* ενώ όταν δεν μπορούμε να επιλέξουμε τοποθεσία, η ανάπτυξη είναι *μη ντετερμινιστική*. Σε οποιαδήποτε μορφή ανάπτυξης απαιτούμε τη δημιουργία ενός συνεκτικού δικτύου, όπου κάθε κόμβος θα μπορεί να επικοινωνεί με κάθε άλλον κόμβο του δικτύου. Για μια ορισμένη τοποθέτηση των κόμβων, είναι εύκολο να ελέγξουμε αν η συγκέντρωση των κόμβων καλύπτει την περιοχή που ενδιαφερόμαστε και αν η συγκέντρωση διατηρείται. Για την ιδιότητα της κάλυψης, πρέπει να ξέρουμε την εμβέλεια της ανίχνευσης κάθε κόμβου, ενώ για την ιδιότητα της επικοινωνίας, πρέπει να ξέρουμε την εμβέλεια επικοινωνίας ενός κόμβου.

α. Ντετερμινιστική ανάπτυξη

Το κυριότερο πρόβλημα που μας απασχολεί στην κάλυψη περιοχής είναι η ανάπτυξη όσο το δυνατόν μικρότερου αριθμού κόμβων ώστε να καλύψουμε τον χώρο με ένα δίκτυο. Το πρόβλημα αυτό εξετάστηκε από τους Kar και Banerjee οι οποίοι υπέθεσαν ότι η εμβέλεια ανίχνευσης είναι ίση με την εμβέλεια επικοινωνίας. Ο αλγόριθμος (Σχήμα 31) που περιγράφει τη διαδικασία δίδεται παρακάτω [124]:

Step 1: [Achieve Coverage]

Let $\delta = (\sqrt{3}/2 + 1)\, r$. Place a sensor at $(i, j\delta)$, i even and j integer as well as one at $(i + r/2, j\delta)$, i odd and j integer.

Step 2: [Achieve Connectivity]

Let $\beta = \sqrt{3}/2\, r$. Place a sensor at $(0, j\delta \pm \beta)$, j odd.

Σχήμα 31. Ο αλγόριθμος των Kar και Banerjee για την ανάπτυξη των δικτύων.

Με αυτόν το αλγόριθμο επιτυγχάνεται μια πυκνότητα δικτύου με απόκλιση 2,6% από τη βέλτιστη. Ο αλγόριθμος αυτός μπορεί να επεκταθεί για να πετύχει καλύτερη πυκνότητα δικτύου. Παρακάτω δίδεται ένας αλγόριθμος [124] για την ανάπτυξη του δικτύου ώστε να καλύψει μια ομάδα σημείων στον Ευκλείδειο Χώρο (Σχήμα 32).

Step 1: [Initialize]

Let s be any leaf of the Euclidean minimum-cost spanning tree of the point set.

Candidate Set = {s}

Step 2: [Deploy Sensors]

While (*candidate Set* $\neq \varnothing$) {

Remove any point p from *candidate Set*.

Place a sensor at p.

Remove from *candidateSet* all points covered by the sensor at p.

Add to *candidateSet* all points (not necessarily vertices) q on the spanning tree T that satisfy the conditions:

(1) q is distance r from p.

(2) q is not covered by an already placed sensor.

(3) The spanning tree path from s to q is completely covered by already placed sensors.

}

Σχήμα 32. Ο «αχόρταγος» αλγόριθμος των Kar και Banerjee.

Και σε αυτόν τον αλγόριθμο υποτίθεται ότι η εμβέλεια επικοινωνίας είναι ίση με την εμβέλεια ανίχνευσης. Ο παραπάνω αλγόριθμος χρησιμοποιεί 7.256 φορές τον

ελάχιστο αριθμό των κόμβων που χρειάζεται για να καλυφθεί το δεδομένο σημείο. Το δικτύωμα που δημιουργείται καλύπτει όλα τα σημεία και είναι ένα συνεκτικό δίκτυο.

β. Μεγιστοποίηση χρόνου ζωής κάλυψης

Όταν ένα δίκτυο αναπτύσσεται σε περιβάλλοντα με δυσκολία πρόσβασης, όπως είναι πολλές στρατιωτικές εφαρμογές, ένας μεγάλος αριθμός κόμβων μπορεί να χρειαστεί να ριφθούν από αέρος στην περιοχή-στόχος. Υποθέτουμε ότι οι κόμβοι που επιζούν από την ρίψη καλύπτουν όλη την περιοχή. Η ενέργεια του κόμβου δεν μπορεί να αναπληρωθεί καθόσον θα αχρηστευτεί. Ως ζωή του κάθε κόμβου είναι ο συντομότερος χρόνος στον οποίο το δίκτυο καταφέρνει να καλύψει όλους τους στόχους. Ο χρόνος ζωής ενός δικτύου μπορεί να παραταθεί εάν τοποθετήσουμε πλεονάζοντες κόμβους οι οποίοι θα «κοιμούνται» και θα «ξυπνάνε» όταν χρειάζεται να ανακτηθεί η κάλυψη του δικτύου. Οι κόμβοι αυτοί καταναλώνουν σημαντικά λιγότερη ενέργεια από τους ενεργούς.

Χρησιμοποιώντας μια τεχνική που προτάθηκε από τους Cardei και Du [125] μπορούμε να αυξήσουμε τον χρόνο ζωής διαμερίζοντας τους υπάρχοντες κόμβους έτσι ώστε κάθε ομάδα κόμβων να καλύπτει όλους τους στόχους. Έτσι, δημιουργώντας αποσπασματικές ομάδες κόμβων οι οποίοι θα εναλλάσσονται σε καταστάσεις ύπνου-λειτουργίας μπορούμε να ελέγχουμε όλους τους στόχους και να αυξήσουμε τη διάρκεια ζωής του δικτύου .

Έχουν δημιουργηθεί και άλλες τεχνικές και αλγόριθμοι που ελέγχουν την κατάσταση ύπνου-λειτουργίας για να αυξήσουμε τον χρόνο λειτουργίας του δικτύου. Έτσι, οι Ye, Zhong, Lu και Zhang [126] πρότειναν ένα πρωτόκολλο όπου μόνο οι ενεργοί κόμβοι παρέχουν την επιθυμητή κάλυψη. Οι 'κοιμώμενοι' κόμβοι, επανέρχονται όταν ο χρόνος 'ύπνου' λήξει και στέλνουν ένα διερευνητικό σήμα σε απόσταση d. Εάν στην απόσταση αυτή δεν υπάρχει κανένας ενεργός κόμβος, τότε μεταπίπτει σε ενεργή κατάσταση. Αντίθετα, αν βρεθούν ενεργοί κόμβοι, τότε ο κόμβος καθορίζει για πόσο χρόνο θα βρίσκεται σε κατάσταση 'ύπνου'. Άλλοι αλγόριθμοι που έχουν αναπτυχτεί είναι οι Optimal Geographical Density Control (OGDC) [127], PEAS [128], GAF [129] και Coverage Configuration Protocol [130].

5.3.2 Δρομολόγηση

Οι συνήθεις αλγόριθμοι δρομολόγησης επικεντρώνονται στα δεδομένα. Λόγω της περίεργης φύσης των δικτύων που εξετάζουμε (έλλειψη υποδομής, έλλειψη κεντρικής διαχείρισης, περιορισμοί ενέργειας κ.ά.), η δρομολόγηση πρέπει να είναι συνεργατική και να διαφυλάσσει ενέργεια για κάθε κόμβο. Η συνεργασία μεταξύ των κόμβων μπορεί να αποδειχθεί πάρα πολύ αποτελεσματική. Για παράδειγμα, σε έναν αλγόριθμο επικεντρωμένο στον κόμβο, οι κόμβοι συνεργάζονται μεταξύ τους για να επιτύχουν κοινούς σκοπούς για το δίκτυο, όπως αξιοπιστία δρομολογίων και εκτίμηση μήκους δρομολογίου, ενώ παράλληλα μειώνουν το κόστος λειτουργίας του δικτύου [131].

Επιπλέον της συνεργασίας μεταξύ κόμβων, σημαντικό ρόλο στην λειτουργία ενός δικτύου παίζει και η κατανάλωση ενέργειας. Και αυτό γιατί συνήθως τα δίκτυά μας βρίσκονται σε τέτοιες τοποθεσίες που δεν μπορούν να αναπληρώσουν την ενέργειά τους. Συνήθως εξετάζονται τρεις μορφές για το θέμα της δρομολόγησης: απλή εκπομπή, εκπομπή σε όλους τους κόμβους του δικτύου και πολύ-εκπομπή. Το τελικό αποτέλεσμα αυτόν των αλγορίθμων είναι να μεγιστοποιήσουν τόσο το χρόνο ζωής

του δικτύου όσο και τη χωρητικότητα του δικτύου (το ποσό των δεδομένων που μπορεί να μεταφερθεί από το δίκτυο σε ορισμένο χρόνο).

α. Απλή εκπομπή (unicast)

Κατά την απλή εκπομπή, θέλουμε να στείλουμε ένα μήνυμα από έναν κόμβο-πηγή σε έναν κόμβο-προορισμό. Οι Singh, Woo και Raghavendra προτείνουν πέντε στρατηγικές για την επιλογή ενός δρομολογίου [132]. Η πρώτη είναι να χρησιμοποιήσουν ένα δρομολόγιο ελαχίστης ενέργειας. Το δρομολόγιο μπορεί να βρεθεί χρησιμοποιώντας τον αλγόριθμου ελαχίστου δρομολογίου Diijkstra. Αυτή η στρατηγική παρουσιάζει ένα μειονέκτημα, εφόσον πολλά μηνύματα πρέπει να μεταδοθούν διαδοχικά. Χρησιμοποιώντας τη διαδρομή ελάχιστης ενέργειας μπορεί να ανατραπεί η επιτυχής αποστολή τους.

Οι υπόλοιπες τέσσερις στρατηγικές προσπαθούν να ξεπεράσουν τη μυωπική φύση της προηγούμενης στρατηγικής. Παρόλα αυτά δεν μπορούμε να βρούμε έναν on-line αλγόριθμο (κάθε αποστολή ενός μηνύματος θα πρέπει να γνωρίζει την πηγή και τον προορισμό του μηνύματος) με συγκεκριμένο ανταγωνιστικό λόγο. Για να μεγιστοποιήσουμε τον χρόνο ζωής και την χωρητικότητα πρέπει να έχουμε μια ισορροπία μεταξύ της ενέργειας που καταναλώνεται σε κάθε δρομολόγιο και της ελάχιστης απομένουσας ενέργειας σε κάθε κόμβο. Στο Σχήμα 33 παρουσιάζεται ο αλγόριθμος max-min zP_{min}-path που επιλέγει δρομολόγια απλής εκπομπής για να πετύχει αυτήν την ισορροπία [133]:

Step 1: [Initialize]

Eliminate from G every edge (u, v) for which ce(u) < w(u, v) * I.

Let L be the list of possible values for the minimum residual-energy fraction.

Step 2: [Binary Search]

Do a binary search in L to find the maximum value max of the minimum residual-energy fraction for which there is a path P from source to destination that uses at most $z * P_{min}$ energy.

For this, when testing a value q from L, we find a shortest source to destination path that does not use edges (u, v) that make the residual-energy fraction at u less than q.

Step 3: [Wrap Up]

If no path is found in Step 2, the unicast isn't possible.

Otherwise, use the path P corresponding to max.

Σχήμα 33. Ο αλγόριθμος max-min zP_{min}-path.

Ο παραπάνω αλγόριθμος επιλέγει ένα δρομολόγιο που χρησιμοποιεί τουλάχιστον $z*P_{min}$ ενέργεια, όπου z είναι η παράμετρος του αλγόριθμου και P_{min} είναι η ενέργεια που χρειάζεται από το δρομολόγιο ελαχίστης ενέργειας. Το επιλεγμένο δρομολόγιο μεγιστοποιεί το κλάσμα υπόλοιπης ενέργειας (ενέργεια που μένει μετά την εκπομπή προς την αρχική ενέργεια).

Έχουν δημιουργηθεί πολλές προσαρμογές στον παραπάνω αλγόριθμο καθώς επίσης και μια κατανεμημένη εκδοχή του [133]. Έτσι ο CMAX [134] χρησιμοποιεί λογαριθμικό λόγο κάνοντας επιπλέον ελέγχους. Στον αλγόριθμο MRPC [135], ο χρόνος ζωής ενός δρομολογίου καθορίζεται ως η ελάχιστη χωρητικότητα στο δρομολόγιο.

β. Πολλαπλή εκπομπή και πολύ-εκπομπή (broadcasting και multicasting)

Χρησιμοποιώντας μία όμοιο-κατευθυντική κεραία, ένας κόμβος μπορεί να μεταδώσει το ίδιο μήνυμα σε διάφορούς κόμβους χρησιμοποιώντας λιγότερη ενέργεια από ότι σε ένα ενσύρματο δίκτυο. Η παραπάνω ιδιότητα καλείται *wireless broadcast advantage* [136].

Κατά την πολύ-εκπομπή χρησιμοποιούμε δέντρο-εκπομπής που είναι μια διευρυμένη μορφή του δέντρου των δρομολογίων που καταλήγουν στον κόμβο-πηγή. Εδώ δημιουργείται το πρόβλημα εύρεσης δέντρου ελαχίστης ενέργειας (*Minimum-energy broadcast tree-MEBT*). Η λύση σε αυτό το πρόβλημα δίδεται με τέσσερις διαφορετικούς αλγόριθμους. Ο DSA (Dijkstra Shortest path Algorithm) κατασκευάζει ελάχιστο δρομολόγιο από την πηγή προς οποιοδήποτε κάθετο δρομολόγιο.

Το MST (*Minimum Spanning Tree*) χρησιμοποιεί τον αλγόριθμο του Pim [137] για να κατασκευάσει ένα διευρυμένο δέντρο ελαχίστου κόστους. Το κατασκευασμένο δέντρο ανακατασκευάζεται εκτελώντας ένα σάρωμα πάνω από τους κόμβους για να ελαττώσει την ενέργεια που χρειάζεται το δένδρο.

Ο αλγόριθμος BIP (*Broadcast Incremental Power*) ξεκινάει με ένα δέντρο που περιέχει μόνο τον κόμβο πηγής. Οι υπόλοιποι κόμβοι προστίθενται, ένας κάθε φορά. Ο επόμενος κόμβος που θα προστεθεί επιλέγεται ώστε να είναι γειτονικός των προηγούμενων και η ενέργεια που απαιτείται για επικοινωνία είναι η ελάχιστη. Όταν έχει κατασκευαστεί το δέντρο, γίνεται ένα σάρωμα ώστε να μειωθεί η απαιτούμενη ενέργεια.

Τέλος, ο BIPPN (*Broadcast Incremental Power Per Node*) ξεκινάει με ένα δέντρο που αποτελείται από την πηγή και χρησιμοποιεί πολλούς κύκλους για να δημιουργήσει ένα ολοκληρωμένο δέντρο. Έτσι καθορίζεται ο αντίστροφος λόγος της αυξητικής ενέργειας που χρειάζεται κάθε κόμβος για να εισέλθει στο δέντρο μας. Σε κάθε κύκλο, ο κάθε λόγος πρέπει να είναι μέγιστος για να εισέλθει κάποιος κόμβος.

Σε πραγματικές εφαρμογές δικτύων, υπάρχει πιθανότητα να χρειαστεί μια ακολουθία πολύ-εκπομπών. Σε αυτήν την περίπτωση, η πρώτη πολύ-εκπομπή μπορεί να καταναλώσει όλη την υπάρχουσα ενέργεια. Γι' αυτό καθορίζεται η κρίσιμη ενέργεια της πολύ-εκπομπής. Βάσει αυτής της ενέργειας δημιουργούνται δέντρα πολύ-εκπομπής που μεγιστοποιούν την ενέργεια.

γ. Συγκέντρωση και διανομή δεδομένων.

Τα προβλήματα της συγκέντρωσης και διανομής δεδομένων δημιουργούνται όταν ένας σταθμός βάσης πρέπει να συγκεντρώσει ή να διανείμει δεδομένα από και προς τους κόμβους του δικτύου αντίστοιχα, στο μικρότερο χρονικό διάστημα. Τα δύο αυτά προβλήματα είναι συμμετρικά και κάποιος μπορεί να βγάλει έναν αλγόριθμο για τη συλλογή δεδομένων από έναν αντίστοιχο αλγόριθμο διανομής δεδομένων και αντίστροφα.

Στην εξέτασή μας διακρίνουμε την περίπτωση της όμοιο-κατευθυντικής και της μη όμοιο-κατευθυντικής κεραίας. Στην πρώτη περίπτωση, ένα πακέτο που μεταδίδεται από έναν πομπό λαμβάνεται από όλους τους δέκτες που βρίσκονται στην εμβέλεια

της κεραίας. Ο σκοπός και τα εμπόδια που παρουσιάζονται είναι ίδια με τη μη όμοιο-κατευθυντική κεραία, μόνο που στη δεύτερη περίπτωση υπεισέρχεται και ο παράγοντας της κατεύθυνσης.

Στην μη όμοιο-κατευθυντική κεραία έχει δημιουργηθεί ένας αποτελεσματικός αλγόριθμος από τους Florens-McEliece [138] για τη διανομή δεδομένων σε ένα δίκτυο σε μορφή δέντρου, χρησιμοποιώντας τον ελάχιστο αριθμό χρονικών σχισμών. Ο αλγόριθμος παρουσιάζεται παρακάτω (Σχήμα 34):

Step 1: [Transmit the packets for $S_n, \dots, S_2$]

Transmit the packets for $S_n, \dots, S_2$, in this order.

For this transmission, use slots $2j - 1$, $1 \le j \le t$, where $t = \sum_{i=2}^{n} p_i$.

The base station makes no transmission in slots $2j$, $1 \le j \le t$.

Step 2: [Transmit S_1's packets]

The packets destined for S_1 are transmitted in slots $2t < j \le 2t + p_1$.

Σχήμα 34. Ο αλγόριθμος των Florens-McEliece για τη διανομή δεδομένων.

Στον παραπάνω αλγόριθμο, μόνο ο σταθμός βάσης είναι αυτός που πρέπει να λάβει απόφαση για κάθε χρονοσχισμή. Εάν ένας κόμβος λάβει ένα πακέτο το οποίο πρέπει να προωθηθεί σε επόμενο κόμβο, απλά αναμεταδίδει αυτό το πακέτο στην επόμενη χρονοσχισμή.

Ο παραπάνω αλγόριθμος μπορεί να τροποποιηθεί ώστε να περιλάβει έναν αλγόριθμο που θα εφαρμοστεί στις όμοιο-κατευθυντικές κεραίες ή και σε οποιοδήποτε μορφή δέντρου [139]. Ο αλγόριθμος αυτός παρουσιάζεται παρακάτω (Σχήμα 35):

Step 1: [Transmit the packets for $S_n, \dots, S_3$]

Transmit the packets for $S_n, \dots, S_3$, in this order.

For this transmission, use slots $3j - 2$, $1 \le j \le t$, where $t = \sum_{i=3}^{n} p_i$.

The base station makes no transmission in slots $3j$ and $3j - 1$, $1 \le j \le t$.

Step 2: [Transmit S_2's packets]

The packets destined for S_2 are transmitted in slots $3t + 2j - 1$, $1 \le j \le p_2$.

The base station makes no transmission in slots $3t + 2j$, $1 \le j \le p_2$.

Step 3: [Transmit S_1's packets]

The packets destined for S_1 are transmitted in slots $3t + 2p_2 < j \le 3t + 2p_2 + p_1$.

Σχήμα 35. Ο αλγόριθμος των Florens-McEliece για όμοιο-κατευθυντικές κεραίες.

Κάθε κόμβος αποστέλλει στην επόμενη χρονοσχισμή κάθε πακέτο που λαμβάνει και που κατευθύνεται σε άλλο κόμβο. Μόνο ο σταθμός βάσης έχει ευελιξία. Έτσι το

μόνο που χρειαζόμαστε είναι να δημιουργήσουμε έναν αλγόριθμο που καθορίζει την χρονοσχισμή στην οποία θα μεταδοθεί κάθε πακέτο, ανάλογα με τον προορισμό του. Λόγω της όμοιο-κατευθυντικής παρεμβολής, βλέπουμε ότι ένα πακέτο που προορίζεται για τον επόμενο κόμβο (κόμβο πρώτου άλματος) μπορεί να μεταδοθεί σε διαδοχικές σχισμές, ενώ τα πακέτα που μεταδίδονται στους επόμενους κόμβους μπορούν να σταλούν σε διαφορετικές σχισμές.

5.3.3 Συγχώνευση δεδομένων (Fusion)

Το τελευταίο θέμα που εξετάζουμε από πλευράς αλγορίθμων είναι η συγχώνευση των συγκεντρωμένων δεδομένων. Η αξιοπιστία ενός δικτύου αυξάνεται μέσω της χρήσης του πλεονασμού. Έτσι κάθε περιοχή ή σημείο ελέγχεται από πολλούς κόμβους-αισθητήρες. Σε ένα πλεονάζον σύστημα αισθητήρων, αντιμετωπίζουμε το πρόβλημα της συγχώνευσης ή συνδυασμού των δεδομένων που στέλνονται από όλους τους κόμβους που ελέγχουν μια περιοχή-στόχο.

Η βασική επιδίωξη είναι η δημιουργία ενός διανύσματος *V* που περιλαμβάνει τις μετρήσεις των κόμβων για την περιοχή μας. Μια λύση σε αυτό το πρόβλημα δόθηκε από τον παρακάτω αλγόριθμο (Σχήμα 36). Είναι ένας υβριδικός κατανεμημένος αλγόριθμος, όπου κάθε κόμβος χρειάζεται να υπολογίσει ένα εύρος μέσα στο οποίο βρίσκεται η πραγματική τιμή για τον στόχο, όπως επίσης και η αναμενόμενη τιμή. Για αυτόν τον υπολογισμό, κάθε κόμβος στέλνει στους υπολοίπους κόμβους τις μετρήσεις για τον στόχο και την ακρίβεια με την οποία γίνονται οι μετρήσεις. Κάθε κόμβος που δεν είναι ελαττωματικός λαμβάνει και επεξεργάζεται σωστές μετρήσεις από τους υπολοίπους. Οι ελαττωματικοί κόμβοι λαμβάνουν λανθασμένα δεδομένα [140].

Step 1: [Determine range for real value V]

Let $[l_i, u_i, n_i]$, $1 \le i \le q$ be such that

1. $l_i \le u_i \le l_{i+1}$, $1 \le i < q$ and $l_q \le u_q$. The $[l_i, u_i]$'s define disjoint measurement intervals.

2. $n_i \ge k - \tau$ gives the number of sensors whose measurement range includes $[l_i, u_i]$.

3. If x is a measurement value not included in one of the $[l_i, u_i]$ intervals, x is included in the measurement interval of fewer than $k - \tau$ sensors.

V is estimated to lie in the range $[l_1, u_q]$.

Step 2: [Estimate V]

V is estimated to be the weighted average $\sum_{i=1}^{q}[(li + ui) * ni]/[2 * \sum_{i=1}^{q} ni]$

Σχήμα 36. Ο υβριδικός αλγόριθμος για τον υπολογισμό του διανύσματος *V*.

Στο παραπάνω κεφάλαιο εξετάσαμε τους αλγόριθμους που διέπουν τα ασύρματα ad hoc και sensor δίκτυα. Τα παραπάνω δίκτυα λόγω των ιδιαίτερων χαρακτηριστικών τους δημιουργούν επιπλέον ανάγκες κατά την ανάπτυξη τους και κατά την εύρεση κατάλληλων αλγορίθμων. Επικεντρωθήκαμε στην ανάπτυξη και

κάλυψη δικτύων, στη δρομολόγηση και στη συγχώνευση δεδομένων. Παρακάτω εξετάζουμε θέματα πιστοποίησης δικτύων.

5.4 Πιστοποίηση (Authentication)

Η πιστοποίηση είναι μια γενική έννοια που χρησιμοποιείται ευρέως. Η σημασία της λέξης είναι να αποδώσει την ιδέα ότι έχουν προσφερθεί ορισμένα μέσα για να εγγυηθούμε ότι κάποιες οντότητες είναι αυτές που ισχυρίζονται ότι είναι ή ότι καμία πληροφορία δεν έχει παραποιηθεί από μη εξουσιοδοτημένες ομάδες.

Υπάρχει πιστοποίηση οντότητας, πιστοποίηση προέλευσης δεδομένων και πιστοποίηση μηνύματος [97]. Η *πιστοποίηση προέλευσης δεδομένων (data origin authentication)* είναι ένας τύπος πιστοποίησης όπου μια ομάδα επιβεβαιώνεται ότι είναι η πρωτογενής πηγή μιας συγκεκριμένης πληροφορίας που δημιουργήθηκε σε μια συγκεκριμένη χρονική περίοδο στο παρελθόν. Η *πιστοποίηση μηνύματος* είναι ανάλογη με την πιστοποίηση προέλευσης δεδομένων και παρέχει πιστοποίηση στον πρωταρχικό δημιουργό ενός μηνύματος. Η *πιστοποίηση οντότητας* είναι η διαδικασία κατά την οποία μία ομάδα επιβεβαιώνει την ταυτότητα μιας δεύτερης ομάδας που εμπλέκεται σε ένα πρωτόκολλο και ότι η δεύτερη ομάδα ήταν ενεργή όταν το «πειστήριο» έλαβε χώρα. Η τεχνική αυτή καλείται επίσης εξακρίβωση ταυτότητας (identification).

Η πιστοποίηση είναι μια διαδικασία που περιλαμβάνει μια *αρχή πιστοποίησης (authenticator)* που επικοινωνεί με μία οντότητα που ζητάει πιστοποίηση (*supplicant*) χρησιμοποιώντας ένα *πρωτόκολλο πιστοποίησης (authentication protocol)* για να εξακριβώσει τα *πιστοποιητικά (credentials)* του supplicant και να καθοριστεί το δικαίωμα προσπέλασής του [141].

5.4.1 Στοιχεία μιας διαδικασίας πιστοποίησης

Μια γενική διαδικασία πιστοποίησης έχει έξι μεγάλες φάσεις:

- Η *εκκίνηση (bootstrapping)* είναι η πρώτη φάση, όπου μια οντότητα που ζητάει πιστοποίηση υπάρχει είτε εκτός είτε εντός του δικτύου μας. Η οντότητα έχει κάποια χαρακτηριστικά τα οποία η πιστοποιούσα αρχή θα λάβει ως απόδειξη για να παρέχει πρόσβαση στο δίκτυο. Έτσι, η εκκίνηση μπορεί να γίνει εκχωρώντας ένα ολικό κλειδί στο δίκτυο για κάθε νεοεισελθόντα κόμβο του δικτύου ή όταν παρέχεται μια λίστα με εμπιστευτικούς κόμβους του δικτύου.
- Εφόσον η φάση της εκκίνησης έχει ολοκληρωθεί, η οντότητα μπορεί να λάβει μέρος στο δίκτυο. Τώρα λαμβάνει χώρα η φάση της *προ-πιστοποίησης (pre-authentication)*. Κατά τη διάρκεια αυτής της φάσης, η οντότητα παρουσιάζει τα κατάλληλα πιστοποιητικά στον authenticator για να λάβει πρόσβαση στο δίκτυο. Παράδειγμα, ένας νέος κόμβος πρέπει να παρουσιάσει ότι γνωρίζει το ολικό κλειδί του δικτύου (χρησιμοποιώντας απάντηση πρόσκλησης).
- Όταν επαληθευτούν τα πιστοποιητικά λαμβάνει χώρα η διαδικασία της *εγκατάστασης πιστοποιητικών (credential establishment),* τα οποία θα λειτουργήσουν σαν απόδειξη της ταυτότητας της οντότητας και επαλήθευση

της πιστοποιημένης κατάστασής του. Ένα πιστοποιητικό μπορεί να είναι ένα συμμετρικό κλειδί, ένα ζεύγος ιδιωτικού/δημόσιου κλειδιού ή κάποια άλλη συμφραζόμενη πληροφορία.

- Με την επιτυχία των προηγούμενων φάσεων, μία οντότητα θεωρείται πιστοποιημένη. Κατά την φάση της *πιστοποίησης (authentication),* η επικοινωνία μεταξύ της οντότητας και του authenticator είναι πιστοποιημένη από την πηγή και επικυρώνεται στον προορισμό χρησιμοποιώντας τα εγκατεστημένα πιστοποιητικά. Όσο πιστοποιείται, η οντότητα ελέγχεται για την περίπτωση που εκτεθεί (έλεγχος συμπεριφοράς (monitor behavior)). Σε μια εκτεθειμένη οντότητα μπορεί να *ακυρωθούν (revoked)* τα πιστοποιητικά τους ή να απαγορευτούν οι αιτήσεις για επανεγκατάσταση των πιστοποιητικών (φάση ανάκλησης/απομόνωσης (revocation/isolation)). Και στις δυο περιπτώσεις η οντότητα απομονώνεται από το δίκτυο.

Συνοψίζοντας τα στοιχεία μιας διαδικασίας πιστοποίησης, έχουμε τις εξής φάσεις: Εκκίνηση (bootstrapping), προ-πιστοποίηση (*pre-authentication*), εγκατάσταση πιστοποιητικών (credential establishment), πιστοποίηση (*authentication*), έλεγχο συμπεριφοράς (monitor behavior) και τέλος, φάση ανάκλησης/απομόνωσης (revocation/isolation).

5.4.2 Βασικά σχήματα πιστοποίησης

Κατά την πιστοποίηση οντότητας και μηνύματος, ο κάθε κόμβος εφοδιάζεται με ψηφιακή υπογραφή (σε σχήματα δημόσιου κλειδιού) και με τον MAC (*Message Authentication Code*) (σε σχήματα συμμετρικού κλειδιού).

α. Ασύμμετρη πιστοποίηση

Σε ένα σενάριο δημοσίου κλειδιού κάθε οντότητα έχει ένα πιστοποιητικό (certificate-PK) που διανέμεται από μία αρχή πιστοποίησης (certificate authority-CA) και ένα ζευγάρι ιδιωτικού/δημόσιου κλειδιού. Παρακάτω παρουσιάζεται ένας αλγόριθμος πιστοποίησης μηνύματος δημοσίου κλειδιού (Σχήμα 37). Ας θεωρήσουμε ότι SIG(m,SK) είναι η υπογραφή του μηνύματος m από το ιδιωτικό κλειδί SK και ότι VER(S,m,PK) είναι η επιβεβαίωση της υπογραφής S του μηνύματος m από το δημόσιο κλειδί PK. Η VER(S,m,PK) είναι έγκυρη εάν η S είναι η υπογραφή του m από το αντίστοιχο μυστικό κλειδί PK και είναι άκυρη σε κάθε διαφορετική περίπτωση.

1: *A* signs a message *m* as *S: = SIG* (*m; SK*) and sends *m; S; <PK> to B*.
2: *B* verifies whether *<PK>? = valid* and whether *V ER*(*S; m; PK*)? *= valid*.

Σχήμα 37. Πιστοποίηση μηνύματος δημόσιου κλειδιού.

β. Συμμετρική πιστοποίηση

Σε ένα σχήμα συμμετρικού κλειδιού υπάρχει ένας κοινά αποδεκτός εμπιστευτικός server *S* που εγκαθιστά τη σχέση εμπιστοσύνης μεταξύ δύο πλευρών. Κάθε οντότητα μοιράζεται ένα μυστικό κλειδί με τον server. Έτσι, μια οντότητα *A* ζητάει να εγκαταστήσει ο *S* μια σχέση με την οντότητα *B*. Ο *S* στέλνει στους Α και *B* ένα κλειδί συνόδου *K* το οποίο μπορούν να χρησιμοποιήσουν για την πιστοποίηση. Η διαδικασία φαίνεται παρακάτω στο Σχήμα 38.

1: *A* sends a *hello* message to *S*.
2: *S* sends *E* (*K; K_A*) to *A*.
3: *S* sends *E* (*K; K_B*) to *B*.
For each authentication, do the following:
4: *A* computes *M: = MAC* (*m; K*) and sends *m; M* to *B*.
5: *B* checks whether *M? = MAC* (*m; K*).

Σχήμα 38. Πιστοποίηση μηνύματος συμμετρικού διακομιστή.

Εδώ *E(m, K)* είναι η κρυπτογράφηση του μηνύματος m από το κλειδί *K*, *MAC(m, K)* είναι ο κώδικας πιστοποίησης μηνύματος του m από το κλειδί *K* και K_A είναι το κλειδί που μοιράζεται από τους *S* και *A*.

Τα σχήματα δημοσίου κλειδιού παρέχουν υπογραφές, ενώ τα σχήματα συμμετρικού κλειδιού παρέχουν μία συμφωνία κλειδιού από έναν κεντρικό server και στη συνέχεια μία διαδικασία πιστοποίησης.

γ. Υβριδική πιστοποίηση

Σε ένα σενάριο δημοσίου κλειδιού, μια ισοδύναμη προσέγγιση είναι η χρήση μιας συμφωνίας κλειδιού ανάλογη με αυτής του Diffie-Hellman ακολουθούμενη από ένα συμμετρικό σχήμα MAC για κάθε διαδικασία πιστοποίησης. Μια τέτοια μορφή πιστοποίησης παρουσιάζεται στον παρακάτω αλγόριθμο (Σχήμα 39).

1: *A* sends *B* its public key *KA*.
2: *B* sends *A* its public key *KB*.
3: *A* computes *K: = a * KB*.
4: *B* computes *K: = b * KA*.
For each authentication, do the following:
5: *A* computes *M: = MAC* (*m, K*) and sends *m, M* to *B*.
6: *B* checks whether *M? = MAC* (*m, K*).

Σχήμα 39. Υβριδική πιστοποίηση μηνύματος.

Εδώ οι *α* και *b* δηλώνουν τα ιδιωτικά κλειδιά τους , όπου $K_A = \alpha * G$ και $K_B = b * G$ και το *G* δηλώνει τα δημόσια κλειδιά των *A* και *B*.

δ. Πιστοποίηση αποτύπωσης χρόνου

Για να πετύχουμε πιστοποίηση οντότητας, απαιτείται αλληλεπίδραση όπως αποδεικνύεται από πολλές εργασίες. Αυτό μπορεί να γίνει χρησιμοποιώντας μια χρονική αποτύπωση, όπως παρουσιάζεται στον παρακάτω αλγόριθμο (Σχήμα 40).

1: *A* computes $M: = E(t||B, K)$ and sends *M* to *B*.
2: *B* verifies that the time-stamp *t* is acceptable and that the received identifier is its own.

Σχήμα 40. Πιστοποίηση οντότητας με χρονικό αποτύπωμα.

Παρατηρούμε ότι είναι επιβεβλημένο να συμπεριλάβουμε την ταυτότητα του δέκτη στο πιστοποιημένο μήνυμα για να αποφευχθούν επιθέσεις επανάληψης. Ο χρόνος *t* είναι μέρος της ετικέτας πιστοποίησης.

ε. Αποδείξεις μηδενικής γνώσης (zero-knowledge proofs)

Μια άλλη μέθοδος παροχής πιστοποίησης είναι οι αποδείξεις μηδενικής γνώσης. Τα πρωτόκολλα μηδενικής γνώσης επιτρέπουν σε έναν κόμβο του δικτύου να αποδείξει τη γνώση του σε ένα μυστικό, ενώ δεν αποκαλύπτει καμία πληροφορία στον κόμβο επαλήθευσης ακόμα και αν ο κόμβος παρεκτρέπεται στο πρωτόκολλο. Σε τέτοια πρωτόκολλα, οι κόμβοι πρέπει να ανταλλάσσουν πολλαπλά μηνύματα που αναφέρονται ως επαναληπτικά, στα οποία η απόδειξη είναι πιθανολογική και όχι απόλυτη. Στην περίπτωση των ασύρματων δικτύων είναι προτιμότερη η χρήση μη επαναληπτικών πρωτοκόλλων μηδενικής γνώσης, όπου οι κόμβοι δεν θα ανταλλάσουν πολλά μηνύματα για να αποδείξουν την ταυτότητά τους.

Μια καλή προσέγγιση αυτού του σχήματος πιστοποίησης δίδεται στην πιστοποίηση Fiat-Shamir [142]. Μια άλλη τεχνική που χρησιμοποιεί πρωτόκολλα μηδενικής γνώσης δίδεται στο πρωτόκολλο που αναπτύχθηκε από τους Κομνηνό, Βέργαδο και Δουλιγέρη [143]. Στο σχήμα αυτό, η πιστοποίηση εκτελείται σε δύο φάσεις, όπου κατά την πρώτη φάση γίνεται πιστοποίηση κόμβο προς κόμβο χρησιμοποιώντας τα πρωτόκολλα μηδενικής γνώσης ενώ κατά τη δεύτερη φάση εφαρμόζονται τεχνικές ασύμμετρης κρυπτογραφίας, ώστε η πληροφορία να μεταδοθεί μεταξύ των κόμβων.

στ. Αμοιβαία πιστοποίηση

Τα μέχρι τώρα σχήματα πιστοποίησης ακολουθούσαν την μονόδρομη πιστοποίηση. Δηλαδή ο κόμβος έπρεπε να πιστοποιηθεί για την ταυτότητά του άλλα δεν έπρεπε να πιστοποιήσει τον έτερο κόμβο της επικοινωνίας. Η αμοιβαία πιστοποίηση μπορεί να αποκτηθεί εκτελώντας μονόδρομη πιστοποίηση δύο φορές. Σ' αυτήν την περίπτωση δεν υπάρχει λογική σύνδεση μεταξύ των ενεργειών. Έτσι, η αμοιβαία πιστοποίηση μπορεί να επιτύχει βάσει του παρακάτω αλγόριθμου (Σχήμα 41).

1: *B* sends random r_B to *A*.
2: *A* computes $M_A: = MAC(r_B||r_A, K)$ and sends *MA*, r_A to *B*.
3: *B* checks whether *MA*? $=MAC(r_B||r_A, K)$, computes
$M_{B:=} MAC(r_A||r_B, K)$ and sends M_B to *A*.
A checks whether $M_{B:=} MAC(r_A||r_B, K)$.

Σχήμα 41. Αμοιβαία πιστοποίηση οντότητας.

Ο αριθμός των ανταλλασσόμενων μηνυμάτων μειώνεται εν συγκρίσει με τη μονόδρομη πιστοποίηση κατά δύο φορές. Η αμοιβαία πιστοποίηση μπορεί να γίνει χρησιμοποιώντας και ψηφιακές υπογραφές αντί για MAC.

ζ. Πιστοποίηση εκπομπής

Η πιστοποίηση εκπομπής είναι η διαδικασία κατά την οποία μία οντότητα πιστοποιεί μηνύματα από διαφορετικούς κόμβους. Ένα συμμετρικό σχήμα απαιτεί τα κλειδιά να έχουν διανεμηθεί, ενώ σε ένα ασύμμετρο σχήμα κάθε οντότητα έχει ένα ζευγάρι ιδιωτικού/δημόσιου κλειδιού. Έτσι, ένα MAC μπορεί να παρέχει αμοιβαία πιστοποίηση, ενώ οι ψηφιακές υπογραφές παρέχουν και πιστοποίηση εκπομπής. Για παράδειγμα, μια οντότητα μπορεί να υπογράψει ένα μήνυμα το οποίο στη συνέχεια επιβεβαιώνεται από πολλούς παραλήπτες. Η πιστοποίηση εκπομπής συνήθως συνδέεται με την μη αποκήρυξη γιατί ένα πιστοποιημένο μήνυμα μπορεί να εξακριβωθεί από ένα τρίτο μέρος.

η. Άλλα σχήματα πιστοποίησης

Ως επιπλέον σχήματα πιστοποίησης μπορούν να θεωρηθούν τα παρακάτω:

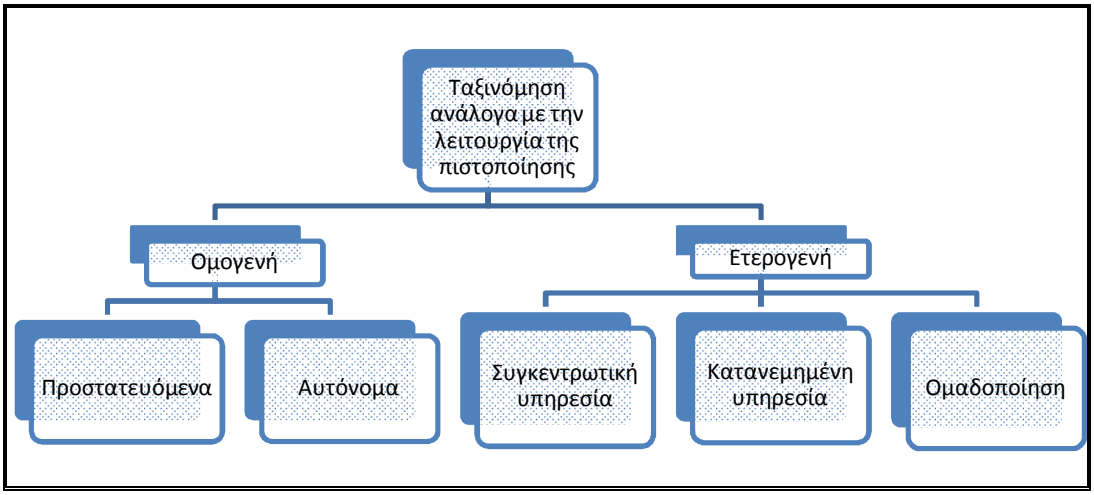
- Το σχήμα του *Lamport* [*97*]. Στηρίζεται σε συναρτήσεις κατακερματισμού. Δεν παρέχει πιστοποίηση οντότητας καθόσον δεν υπάρχει απόδειξη μιας ενεργής επικοινωνίας. Επίσης δεν μπορεί να κατανικήσει την ανάγκη για πιστοποιημένη αρχική ανταλλαγή κλειδιού.
- Το *TESLA* [144] είναι ένα πρωτόκολλο για πιστοποίηση εκπομπής. Το πρωτόκολλο αυτό ακολουθεί μια διαφορετική τακτική εισάγοντας ένα ρολόι. Κάθε μήνυμα m_i που πιστοποιείται από ένα κλειδί k_i γίνεται δεκτό μόνο σε συγκεκριμένη χρονική στιγμή t_i. Σ' αυτήν την περίπτωση, ο κόμβος πρέπει να αποθηκεύει μηνύματα πριν τα επιβεβαιώσει. Επιπλέον, πρέπει να υπάρχει συγχρονισμός μεταξύ αποστολέα και δέκτη. Διαφορετικά, όταν ένα κλειδί ανοιχθεί, ένας επιτιθέμενος μπορεί να το χρησιμοποιήσει για να πλαστογραφήσει μηνύματα.
- Το πρωτόκολλο *Guy Fawkes* [145] χρησιμοποιεί δεσμεύσεις κλειδιών από μια συνάρτηση κατακερματισμού για να παρέχει πιστοποίηση μηνύματος. Το μειονέκτημα του πρωτοκόλλου είναι ότι η δέσμευση αυτή πρέπει να γίνει δημόσια γνωστή.

5.4.3 Ταξινόμηση πρωτοκόλλων πιστοποίησης

Τα πρωτόκολλα πιστοποίησης παρουσιάζουν διάφορους τρόπους με τους οποίους εκτελούν την πιστοποίηση. Κάποια πρωτόκολλα προϋποθέτουν εμπιστοσύνη σε ένα τρίτο μέρος, το οποίο είναι έμπιστο τμήμα του δικτύου από όλους τους κόμβους. Αντίθετα, άλλα πρωτόκολλα δεν ακολουθούν αυτή τη διαδικασία. Παρακάτω παρουσιάζουμε ταξινόμηση των πρωτοκόλλων ανάλογα με την λειτουργία της πιστοποίησης, ανάλογα με τους τύπους των πιστοποιητικών που χρησιμοποιούνται και ανάλογα με την εγκατάσταση των πιστοποιητικών.

α. Ταξινόμηση ανάλογα με την λειτουργία της πιστοποίησης

Η κατηγορία αυτή ταξινομεί τα πρωτόκολλα, ανάλογα με τον ρόλο που παίζουν οι κόμβοι στο δίκτυο για την εκτέλεση της πιστοποίησης. Βάσει αυτού, τα πρωτόκολλα διακρίνονται σε *ομογενή* και *ετερογενή* (Σχήμα 42).



Σχήμα 42. Ταξινόμηση ανάλογα με τον ρόλο των κόμβων.

Τα *ομογενή* πρωτόκολλα θεωρούνται αυτά στα οποία όλοι οι κόμβοι του δικτύου έχουν τον ίδιο ρόλο ως προς τη λειτουργία της πιστοποίησης. Έτσι, σε αυτήν την κατηγορία υποτίθεται ότι οι κόμβοι είτε εκτελούν την πιστοποίηση αυτόνομα είτε στηρίζονται σε πληροφορία που προσφέρεται από άλλους κόμβους του δικτύου [141]. Έτσι έχουμε μια περαιτέρω κατηγοριοποίηση σε αυτόνομα (οι κόμβοι δεν στηρίζονται σε πληροφορία από τους υπολοίπους) και σε προστατευόμενα (οι κόμβοι στηρίζονται σε έμπιστους ομότιμους κόμβους). Τα πρωτόκολλα LHAP [146], LEAP [42], SPINS [40] και τα zero-knowledge proofs [147] είναι ορισμένα που ανήκουν σε αυτήν την κατηγορία.

Αντίθετα, στα *ετερογενή* πρωτόκολλα, οι κόμβοι του δικτύου έχουν διαφορετικούς ρόλους κατά την εκτέλεση της πιστοποίησης. Αυτό σημαίνει ότι υπάρχει μια υποκείμενη υπηρεσία στο δίκτυο που βοηθάει τους κόμβους να πάρουν αποφάσεις πιστοποίησης. Η υποκείμενη υπηρεσία μπορεί να είναι συγκεντρωτική (ένας ειδικός κόμβος είναι υπεύθυνος για αυτήν την λειτουργία), κατανεμημένη (οι ειδικοί κόμβοι μπορεί να βρίσκονται παντού στο δίκτυο) ή σε συγκροτήματα (όπου κάθε ομάδα έχει τον δικό της πάροχο της υπηρεσίας πιστοποίησης). Τα πρωτόκολλα Kerberos [148] και το πρωτόκολλο που αναπτύχθηκε από τους Zhou και Haas [39] είναι κλασικά παραδείγματα ετερογενούς συμπεριφοράς.

β. Ταξινόμηση ανάλογα με τους τύπους των πιστοποιητικών

Ανάλογα με τους τύπους των πιστοποιητικών τα πρωτόκολλα διακρίνονται σε αυτά που βασίζονται στην *ταυτότητα* ή στο *πλαίσιο εφαρμογής (context-based)*.

Στα πρωτόκολλα που βασίζονται στην *ταυτότητα* αναγνωρίζεται ένα ιδιαίτερο χαρακτηριστικό που κατέχει ο κόμβος που θέλει να πιστοποιηθεί και ταυτοποιείται με υψηλή εμπιστοσύνη. Αυτήν την κατηγορία μπορούμε να τη διαχωρίσουμε επιπλέον σε πρωτόκολλα που στηρίζονται σε κρυπτογράφηση (παράγεται πληροφορία με

κρυπτογράφηση και υπογράφεται από το κλειδί που κατέχει ο κόμβος για να αποδείξει την κατοχή του κλειδιού. Αν ο κόμβος που θα πιστοποιήσει έχει το ίδιο κλειδί μιλάμε για συμμετρική κρυπτογραφία ενώ αν έχει το ζεύγος δημόσιο/ιδιωτικό κλειδί μιλάμε για ασύμμετρη κρυπτογραφία) και σε αυτήν που στηρίζεται σε μη κρυπτογραφημένα μηνύματα (μια μορφή αυτής της κατηγορίας είναι αυτή που στηρίζεται στον κατακερματισμό του μηνύματος χρησιμοποιώντας μια μονόδρομη συνάρτηση κατακερματισμού).

Στα πρωτόκολλα που *στηρίζονται στο πλαίσιο εφαρμογής* αναγνωρίζεται ένα χαρακτηριστικό γνώρισμα των συμφραζόμενων και χρησιμοποιείται για την πιστοποίηση. Επιπλέον μπορούν να κατηγοριοποιηθούν με βάση τη συμπεριφορά τους (προσπάθεια πιστοποίησης βάσει του μοτίβου της συμπεριφοράς του κόμβου) και με βάση τα φυσικά χαρακτηριστικά τους (η πιστοποίηση γίνεται βάσει ενός ιδιαίτερου χαρακτηριστικού όπως η θέση GPS, το RSSI (Received Signal Strength Indication) ή το SNR (Signal to Noise Ratio)).

γ. Ταξινόμηση ανάλογα με την εγκατάσταση των πιστοποιητικών

Η κατηγοριοποίηση αυτή διακρίνει τα πρωτόκολλα ανάλογα με τον τρόπο με τον οποίο εγκαθίστανται τα πιστοποιητικά στο προς πιστοποίηση δίκτυο. Έτσι, στην πρώτη κατηγορία ανήκουν πρωτόκολλα στα οποία έχουν διανεμηθεί τα πιστοποιητικά πριν την ανάπτυξη του δικτύου. Παράδειγμα αυτής της κατηγορίας είναι τα ζεύγη κλειδιών που διανέμονται πριν την ανάπτυξη των δικτύων σε όλους τους κόμβους για να χρησιμοποιηθούν για πιστοποίηση κόμβο προς κόμβο. Η κατηγορία αυτή βρίσκει εφαρμογή σε πρωτόκολλα που στηρίζονται σε συμμετρικά κλειδιά. Στη δεύτερη κατηγορία αναφέρονται πρωτόκολλα στα οποία τα πιστοποιητικά διανέμονται μετά την ανάπτυξη του δικτύου. Στην τρίτη κατηγορία, υποτίθεται διανομή των αρχικών πιστοποιητικών όπως στην πρώτη κατηγορία. Όμως τα πραγματικά πιστοποιητικά που θα χρησιμοποιηθούν για την πιστοποίηση παράγονται από τα αρχικά πιστοποιητικά.

5.4.4 Ασθενής πιστοποίηση

Με τον όρο ασθενής πιστοποίηση εννοούμε σχήματα πιστοποίησης που χρησιμοποιούν *συνθήματα (password)*. Η ιδέα που ακολουθείται είναι η εξής: Ένα σύνθημα που σχετίζεται με έναν κόμβο, είναι μια γραμμή 6 έως 10 ή περισσοτέρων χαρακτήρων. Το σύνθημα λειτουργεί ως ένα μυστικό μεταξύ του χρήστη και του συστήματος. Για να αποκτήσει πρόσβαση στο σύστημα, ο χρήστης εισάγει το σύνθημα. Το σύστημα ελέγχει το σύνθημα να ταιριάζει με τα δεδομένα που κατέχει και ότι η οντότητα είναι εξουσιοδοτημένη να εισέλθει στο σύστημα.

Μια απλή τεχνική που μπορεί να χρησιμοποιηθεί είναι το σύστημα να αποθηκεύει ένα σύνθημα σε ένα φάκελο συνθημάτων του συστήματος, το οποίο προστατεύεται από ανάγνωση και γραφή. Με την είσοδο του συνθήματος, το σύστημα συγκρίνει το σύνθημα με το σύνθημα που βρίσκεται στον φάκελο συνθημάτων. Αφού δεν εφαρμόζονται μέθοδοι μυστικού κλειδιού ή κρυπτογραφικές τεχνικές, η τεχνική αυτή αναφέρεται ως μη κρυπτογραφική. Ένα βασικό μειονέκτημα είναι ότι δεν παρέχει προστασία σε «υπέρ-χρήστες» που έχουν πλήρη πρόσβαση σε αρχεία του συστήματος.

Μία καλύτερη τεχνική από την αποθήκευση ενός απλού συνθήματος, είναι η αποθήκευση μιας μονόδρομης συνάρτησης. Για να εξακριβώσουμε ένα σύνθημα, το

σύστημα υπολογίζει την μονόδρομη συνάρτηση του συνθήματος και το συγκρίνει με την αποθηκευμένη τιμή. Η χρήση αυτής της μεθόδου είναι προτιμότερη από τη μη κρυπτογραφική, καθόσον πετυχαίνουμε καλύτερη ασφάλεια του χρήστη.

Λόγω της ύπαρξης αποτελεσματικών επιθέσεων κατά προβλέψιμων συνθημάτων, ορισμένα συστήματα έχουν επιβάλλει κανόνες συνθημάτων για να αποθαρρύνουν τους χρήστες να χρησιμοποιήσουν ασθενή συστήματα. Τυπικοί κανόνες περιλαμβάνουν τα παρακάτω:

- Κατώτατο όριο στο μήκος του συνθήματος (συνήθως 8 ή 12 χαρακτήρες).
- Κάθε σύνθημα πρέπει να περιέχει τουλάχιστον ένα χαρακτήρα από μια ομάδα κατηγοριών (π.χ. κεφαλαία, αριθμητικά, μη αλφαριθμητικά κ.ά.).
- Ελέγχονται τα υποψήφια συνθήματα ώστε να μην περιέχονται σε on-line ή διαθέσιμα λεξικά.
- Δεν αποτελούνται από πληροφορίες που σχετίζονται με λογαριασμούς, όπως υπό-αλφαριθμητικά ή userid.

Ένας επιτιθέμενος, γνωρίζοντας ποιοι κανόνες είναι ενεργοί, μπορεί να εκτελέσει μια επίθεση τροποποιημένου λεξικού λαμβάνοντας υπόψη τους κανόνες και στοχεύοντας τις πιο αδύναμες μορφές συνθημάτων που παρόλα αυτά ικανοποιούν τους κανόνες. Οι συνηθέστερες επιθέσεις που μπορούν να δεχθούν συστήματα που χρησιμοποιούν συνθήματα αναπτύσσονται παρακάτω.

Η επανάληψη σταθερών συνθημάτων αυξάνει την πιθανότητα ένας επιτιθέμενος να μάθει το σύνθημα απλώς παρατηρώντας όπως τυπώνεται. Μια δεύτερη ανησυχία είναι ότι τα συνθήματα μεταφέρονται σε απλά μηνύματα στην γραμμή επικοινωνίας και χρησιμοποιούνται στην ίδια μορφή κατά την εξακρίβωσή τους από το σύστημα. Ένας επιτιθέμενος, απλά κρυφακούοντας, μπορεί να αντιγράψει τα δεδομένα, επιτρέποντας την μίμηση. Μια άλλη κοινή επίθεση είναι να δοκιμάσει συνθήματα ο επιτιθέμενος στον πραγματικό εξακριβωτή, με την ελπίδα ότι θα βρεθεί το αληθινό σύνθημα. Αυτό μπορεί να μετρηθεί, εξασφαλίζοντας ότι τα συνθήματα διαλέγονται από έναν μεγάλο χώρο, περιορίζοντας έτσι την αποτυχημένες προσπάθειες. Οι *off-line* επιθέσεις, προϋποθέτουν υπολογισμούς που δεν απαιτούν την αλληλεπίδραση με τον εξακριβωτή μέχρι μια τελική φάση.

Μια αναβάθμιση της υπηρεσίας των σταθερών συνθημάτων είναι η χρησιμοποίηση συνθημάτων μίας χρήσης. Πρόκειται για συνθήματα που χρησιμοποιούνται μόνο μία φορά. Αυτά τα συστήματα είναι αποτελεσματικά εναντίον παθητικών επιθέσεων που κρυφακούν και αργότερα μιμούνται τους κόμβους. Χαρακτηριστικό παράδειγμα είναι το πρωτόκολλο του Lamport, όπου χρησιμοποιείται μια μονόδρομη συνάρτηση για να παραχθεί κάθε φορά η ακολουθία συνθημάτων.

5.4.5 Ισχυρή πιστοποίηση

Κατά την ισχυρή πιστοποίηση (ή ταυτοποίηση πρόκλησης-απάντησης / challenge-response identification), μια οντότητα αποκαλύπτει την ταυτότητά της σε μια άλλη, αποδεικνύοντας τη γνώση ενός μυστικού που είναι συσχετισμένο με αυτήν την οντότητα, χωρίς να αποκαλύπτει το μυστικό του στην άλλη οντότητα. Αυτό γίνεται παρέχοντας μια απάντηση σε μια πρόκληση, όπου η απάντηση εξαρτάται από το

μυστικό της οντότητας και την πρόκληση. Η πρόκληση είναι ένα νούμερο και η αρχή ενός πρωτόκολλου. Εάν η επικοινωνία παρακολουθείται, το αποτέλεσμα μιας πράξης του πρωτοκόλλου πιστοποίησης δεν πρέπει να παρέχει σε έναν επιτιθέμενο χρήσιμη πληροφορία.

Συνήθως, κατά την ισχυρή πιστοποίηση χρησιμοποιούνται παράμετροι για να εξουδετερώσουν τις επιθέσεις και να παρέχουν μοναδικότητα σε κάθε τεχνική. Οι πιο συνήθεις παράμετροι είναι οι *εξειδικευμένες τιμές (nonce), τα τυχαία νούμερα (random numbers), οι αύξοντες αριθμοί (sequence numbers)* και *οι χρονοσφραγίδες (timestamps)*.

Τα πρωτόκολλα ισχυρής πιστοποίησης είναι πρωτόκολλα που χρησιμοποιούν συμμετρικές και ασύμμετρες τεχνικές. Έτσι, όπως έχουμε αναφέρει παραπάνω, οι συμμετρικές τεχνικές προϋποθέτουν την ύπαρξη ενός συμμετρικού κλειδιού και από τις δύο οντότητες πιστοποίησης. Παράδειγμα τέτοιων πρωτοκόλλων είναι τα πρωτόκολλα *Kerberos* [148] και το *Needham-Schroeder*. Αντίστοιχα, στις τεχνικές δημοσίου κλειδιού, η οντότητα που θέλει να πιστοποιηθεί παρουσιάζει την γνώση του ιδιωτικού κλειδιού της με έναν από τους παρακάτω δύο τρόπους:

(1) Αποκρυπτογραφεί μια πρόκληση την οποία κρυπτογράφησε με το δημόσιο κλειδί της.
(2) Υπογράφει ψηφιακά μια πρόκληση.

Παράδειγμα των τεχνικών αυτών είναι το τροποποιημένο πρωτόκολλο των *Needham-Schroeder,* ο μηχανισμός *X.509* που χρησιμοποιεί ψηφιακές υπογραφές κ.ά.

5.4.6 Επιθέσεις στα πρωτόκολλα πιστοποίησης

Οι επιθέσεις που δέχονται τα πρωτόκολλα πιστοποίησης δεν διαφέρουν από τις αντίστοιχες των υπόλοιπων πρωτοκόλλων, όπως αυτά της εγκατάστασης κλειδιού, και οι τύποι τους μπορούν ανάλογα να κατηγοριοποιηθούν. Παρόλα αυτά, στα πρωτόκολλα πιστοποίησης δεν είναι τόσο περίπλοκα τα πράγματα. Οι επιθέσεις που δέχονται τα πρωτόκολλα πιστοποίησης αναπτύσσονται παρακάτω:

- *Απομίμηση*: μία εξαπάτηση όπου μια οντότητα παριστάνει κάποια άλλη.
- *Επιθέσεις αναπαραγωγής:* μία απομίμηση ή άλλη εξαπάτηση που περιλαμβάνει χρήση πληροφορίας από ένα προηγούμενο πρωτόκολλο στον ίδιο ή άλλο πιστοποιητή.
- *Επιθέσεις διεμπλοκής:* μία απομίμηση ή άλλη εξαπάτηση που περιλαμβάνει επιλεκτικό συνδυασμό πληροφορίας από έναν ή περισσότερα προηγούμενα ταυτόχρονα εξελισσόμενα πρωτόκολλα.
- *Επιθέσεις ανάκλησης:* μία επίθεση διεμπλοκής που περιλαμβάνει αποστολή πληροφορίας από ένα εξελισσόμενο πρωτόκολλο πίσω στον αποστολέα της αρχικής πληροφορίας.
- *Εξαναγκασμένη καθυστέρηση:* μία εξαναγκασμένη καθυστέρηση διαδραματίζεται όταν ένας επιτιθέμενος καθυστερεί ένα μήνυμα και το αναμεταδίδει αργότερα.

- *Επίθεση επιλεγμένου κειμένου:* μία επίθεση σε ένα πρωτόκολλο πρόκλησης απάντησης, όπου ο επιτιθέμενος επιλέγει απαντήσεις σε μια προσπάθεια να αποσπάσει πληροφορία.

Σε περίπτωση ενεργών επιθέσεων, οι επιθέσεις μπορεί να περιλαμβάνουν την έναρξη ενός ή περισσοτέρων πρωτοκόλλων από πλευράς του επιτιθέμενου και τη δημιουργία, εισαγωγή ή τροποποίηση προηγουμένων μηνυμάτων. Παρακάτω συνοψίζονται τα αντίμετρα [97] για τις παραπάνω απειλές (Σχήμα 43).

Τύποι επιθέσεων	Αντίμετρα
Επανάληψη	Χρήση τεχνικών πρόκλησης-απάντησης, εξειδικευμένων τιμών και ενσωμάτωση ταυτότητας στόχου στην απάντηση.
Διεμπλοκή	Σύνδεση μηνυμάτων ενός πρωτοκόλλου (χρησιμοποιώντας αλυσίδες αριθμών).
Ανάκληση	Ενσωμάτωση του στόχου στις απαντήσεις, δημιουργία πρωτοκόλλων με διαφορετική δομή μηνυμάτων σε κάθε αποστολή, χρήση κλειδιών μιας κατεύθυνσης.
Επιλογή κειμένου	Χρήση τεχνικών μηδενικής γνώσης, ενσωμάτωση σε κάθε απάντηση ενός τυχαίου αριθμού.
Εξαναγκασμένη καθυστέρηση	Συνδυασμένη χρήση τυχαίων μηνυμάτων με μικρές απαντήσεις με χρονικό όριο, χρονοσφραγίδες μαζί με κατάλληλες επιπρόσθετες τεχνικές.

Σχήμα 43. Επιθέσεις και αντίμετρα στα πρωτόκολλα πιστοποίησης.

Σε περίπτωση που η πιστοποίηση εκτελείται στην αρχή μιας περιόδου επικοινωνίας, για να επιτύχουμε πρόσβαση στην επικοινωνία, μια βασική απειλή είναι η διατήρηση της πιστοποίησης και κατά τη διάρκεια της λειτουργίας του δικτύου. Ένας επιτιθέμενος μπορεί να αποκτήσει πρόσβαση αμέσως μετά την παροχή πιστοποίησης σε έναν κόμβο και να μπορεί στη συνέχεια να διαβάλλει ολόκληρο το δίκτυο. Για να αποφύγουμε αυτήν την απειλή μπορούμε να εκτελούμε πιστοποίηση στο δίκτυο περιοδικά κατά τη διάρκεια της λειτουργίας του, με την προϋπόθεση να έχουμε τη διαθέσιμη ενέργεια. Μια άλλη τακτική είναι να ‘δέσουμε’ την πιστοποίηση με μια ήδη εξελισσόμενη έμπιστη υπηρεσία. Σε αυτήν την περίπτωση, η πιστοποίηση μπορεί να ολοκληρωθεί με έναν μηχανισμό εγκατάστασης κλειδιού.

Το τελευταίο θέμα που θα μας απασχολήσει είναι η δρομολόγηση μέσα στο δίκτυο.

5.5 Δρομολόγηση (Routing)

Ένα πρωτόκολλο στα δίκτυα ad hoc και sensor βρίσκει δρομολόγια μεταξύ κόμβων προωθώντας τα πακέτα προς τον τελικό προορισμό. Σε αντίθεση με τα παραδοσιακά πρωτόκολλα δρομολόγησης, τα πρωτόκολλα αυτά πρέπει να είναι προσαρμοστικά στη συνεργασία τους με τα δίκτυα και τα ιδιαίτερα χαρακτηριστικά που παρουσιάζουν αυτά (έλλειψη υποδομής, ασύρματη μετάδοση, συχνή αλλαγή

θέσης, περιορισμοί ισχύος και μνήμης κ.ά.). Έχουν αναπτυχθεί πολλά πρωτόκολλα δρομολόγησης, τα οποία έχουν αναφερθεί σε προηγούμενα κεφάλαια της εργασίας.

Είναι πολύ σημαντικό να ασφαλίσουμε το πρωτόκολλο δρομολόγησης. Εάν το πρωτόκολλο υπονομευτεί και τα μηνύματα μπορούν να τροποποιηθούν κατά την μετάδοση, τότε καμία ασφάλεια δεν θα υπάρχει στα πακέτα πληροφορίας στα ανώτερα επίπεδα [6].

5.5.1 Επιθέσεις στα πρωτόκολλα δρομολόγησης

Τα πρωτόκολλα δρομολόγησης των δικτύων εκτίθενται σε πολλών τύπων απειλές και επιθέσεις. Ανάλογες επιθέσεις υπάρχουν και στα απλά ασύρματα δίκτυα, αλλά μπορούν πιο εύκολα να υπερνικηθούν από την υπάρχουσα ισχυρή υποδομή τους. Παρακάτω παρουσιάζονται οι κλάσεις επιθέσεων που απαντώνται στα πρωτόκολλα δρομολόγησης.

α. Επιθέσεις που χρησιμοποιούν τροποποίηση

Η κίνηση στο δίκτυο μπορεί να ανακατευθυνθεί και επιθέσεις DoS μπορούν να εκτελεστούν τροποποιώντας την πληροφορία δρομολόγησης [64], όπως η αλλαγή του πεδίου μηνύματος ελέγχου των δεδομένων ή η προώθηση μηνυμάτων με πλαστές τιμές. Οι σημαντικότερες επιθέσεις αυτής της μορφής αναπτύσσονται παρακάτω:

- *Ανακατεύθυνση, τροποποιώντας τον αριθμό ακολουθίας δρομολογίου.* Ορισμένα πρωτόκολλα δρομολόγησης όπως το AODV [33], συγκεκριμενοποιούν και διατηρούν τα δρομολόγια αναθέτοντας μονότονα αυξανόμενους αριθμούς ακολουθίας. Έτσι, οποιοσδήποτε κόμβος μπορεί να κατευθύνει την κίνηση μέσω του εαυτού του ανακοινώνοντας διαδρομή με υψηλότερο αριθμό ακολουθίας από τον πραγματικό.
- *Ανακατεύθυνση, τροποποιώντας τον αριθμό άλματος.* Πολλά πρωτόκολλα χρησιμοποιούν το πεδίο αριθμού άλματος για να καθορίσουν τη βέλτιστη διαδρομή. Επακόλουθα, ένας κακόβουλος κόμβος μπορεί να αυξήσει τις πιθανότητες να περιληφθεί στη διαδρομή, επαναφέροντας το πεδίο αριθμού άλματος του μηνύματος RREP που προωθούν στο μηδέν. Η ανακατεύθυνση είναι πιθανή και στην περίπτωση που το πρωτόκολλο χρησιμοποιεί μετρικά διαφορετικά από τον αριθμό άλματος. Σε αυτήν την περίπτωση, ο επιτιθέμενος πρέπει να τροποποιήσει το πεδίο που χρησιμοποιείται για να υπολογίσει τα μετρικά.
- *Τροποποίηση δρομολογίου προορισμού.* Σε ορισμένα πρωτόκολλα, ο κόμβος προορισμού δηλώνει το δρομολόγιο στα πακέτα. Αυτά τα δρομολόγια στερούνται ελέγχου ακεραιότητας, έτσι η αλλαγή του δρομολογίου προορισμού στην επικεφαλίδα του πακέτου μπορεί να οδηγήσει σε επιθέσεις DoS.
- *Δημιουργία τούνελ.* Δύο απομακρυσμένοι κόμβοι μπορούν να συνεργαστούν για να ανταλλάσσουν μηνύματα μεταξύ τους, μέσω υπαρχόντων δρομολογίων. Έτσι, μπορούν να συνεργαστούν για να παρουσιάσουν λάθος το μήκος του δρομολογίου, μεταδίδοντας μεταξύ τους νόμιμα μηνύματα δρομολόγησης τα

οποία παράγονται από άλλους κόμβους, εμποδίζοντας τους ενδιάμεσους κόμβους να αυξάνουν τα μετρικά που χρησιμοποιούνται για να μετρήσουν το μήκος του δρομολογίου.

β. Επιθέσεις παραπλάνησης

Η παραπλάνηση υπάρχει όταν ένας κόμβος παραποιεί την ταυτότητα του στο δίκτυο, όπως αλλάζοντας τη διεύθυνση MAC ή IP στα πακέτα που προωθεί. Η επίθεση αυτή μπορεί να συνδυαστεί με τις επιθέσεις τροποποίησης και να οδηγήσουν σε κακή πληροφόρηση που θα δημιουργήσουν βρόχους δρομολογίων [64].

γ. Επιθέσεις που χρησιμοποιούν πλαστογραφία

Οι επιθέσεις αυτές είναι πολύ δύσκολο να ανιχνευθούν. Περιλαμβάνουν επιθέσεις που στηρίζονται σε παραγωγή λαθεμένης πληροφορίας δρομολόγησης.

- *Παραποίηση της λάθος διαδρομής.* Σε περίπτωση διακοπής ενός δρομολογίου, ο τελευταίος κόμβος της διαδρομής στέλνει πίσω στον αποστολέα ένα πακέτο RERR. Οι επιθέσεις αυτές μπορούν να εκτελεστούν παραποιώντας τα μηνύματα RERR, καταλήγοντας στην καταστροφή των έγκυρων δρομολογίων και δημιουργώντας επιπλέον επιβάρυνση, η οποία μπορεί να προκαλέσει επιθέσεις DoS και σπατάλη πόρων.
- *Μετάδοση σε λάθος δρομολόγιο.* Ένας κόμβος κατά τακτά χρονικά διαστήματα ανανεώνει την πληροφορία δρομολόγησής του από τα μηνύματα που προωθεί και από αδιάφορα πακέτα. Έτσι, ένας επιτιθέμενος μπορεί να εκμεταλλευτεί αυτή την αδυναμία και να δηλητηριάσει της μνήμες δρομολογίου των γειτόνων του μεταδίδοντας πακέτα που περιέχουν λάθος δρομολόγια.

δ. Επιθέσεις βιασύνης

Σε όλα τα πρωτόκολλα on-demand, για να μειώσουμε την επιβάρυνση από την ανακάλυψη δρομολογίου, κάθε κόμβος προωθεί μόνο ένα μήνυμα RREQ που δημιουργείται από οποιαδήποτε διαδρομή και συνήθως το πρώτο που λαμβάνεται. Αυτήν την ιδιότητα μπορεί να εκμεταλλευτεί ένας επιτιθέμενος για να επισπεύσει την προώθηση των μηνυμάτων RREQ [77]. Ο επιτιθέμενος μπορεί να χρησιμοποιήσει μια από τις τρεις παρακάτω τεχνικές για να εκτελέσει τις επιθέσεις βιασύνης:

- Αφαίρεση των καθυστερήσεων MAC, όταν προωθούνται πακέτα.
- Μετάδοση μηνυμάτων RREQ με μεγαλύτερη ισχύ και
- Εφαρμογή της τεχνικής της σκουληκότρυπας [149].

5.5.2 Αντίμετρα και λύσεις

Παρακάτω αναλύονται κάποιες λύσεις στις επιθέσεις που εκτελούνται κατά των πρωτοκόλλων δρομολόγησης.

α. Πιστοποίηση σε όλες τις φάσεις της δρομολόγησης

Σε αυτήν την λύση χρησιμοποιούνται τεχνικές πιστοποίησης σε όλες τις φάσεις της δρομολόγησης, προσπαθώντας να αποκλειστούν οι επιτιθέμενοι και οι μη πιστοποιημένοι κόμβοι από τη δρομολόγηση. Οι περισσότερες από τις λύσεις τροποποιούν το υπάρχον πρωτόκολλο δρομολόγησης για να δημιουργήσουν λύσεις που στηρίζονται στην πιστοποίηση (π.χ. το Ariadne, SRP κ.ά.). Βασικό μειονέκτημα αυτής της λύσης είναι ότι στηρίζονται σε μια αρχή πιστοποίησης και έτσι γίνεται συγκεντρωτική και λιγότερο ευέλικτη. Το κύριο πλεονέκτημα είναι ότι εμποδίζονται εξωτερικοί μη πιστοποιημένοι κόμβοι να συμμετάσχουν στη δρομολόγηση και μ' αυτό τον τρόπο αποτρέπεται οποιαδήποτε απειλή εκτελείται από τέτοιους κόμβους.

β. Παραμετροποίηση εμπιστοσύνης

Αυτή η μέθοδος εισάγει ένα καινούργιο μετρικό που καλείται τιμή εμπιστοσύνης και εξουσιάζει τη συμπεριφορά του πρωτοκόλλου δρομολόγησης [76]. Αυτή η τιμή εφαρμόζεται στα πακέτα ελέγχου και καθρεφτίζει την ελάχιστη τιμή εμπιστοσύνης που απαιτείται από τον αποστολέα. Έτσι, ένας κόμβος που δέχεται ένα πακέτο μπορεί να μην το προωθήσει ή να μην το επεξεργαστεί, αν το πακέτο δεν έχει την απαραίτητη τιμή εμπιστοσύνης. Η τεχνική αυτή στηρίζεται στην πιστοποίηση και απαιτεί ιεραρχική διαμοίραση κλειδιού. Ως πλεονέκτημα λογίζεται ότι εμποδίζεται επίθεση από εσωτερικό κόμβο που βρίσκεται σε υψηλότερο επίπεδο εμπιστοσύνης.

γ. Διακρίβωση ασφαλούς γειτονίας

Η μέθοδος αυτή αποτελείται από μια ανταλλαγή μηνυμάτων τριών βημάτων μεταξύ δύο κόμβων οι οποίοι λογίζονται ως γείτονες. Εάν αυτή η ανταλλαγή αποτύχει, τότε ο κόμβος που συμπεριφέρεται νόμιμα αγνοεί τον δεύτερο και δεν διακινεί πακέτα που προέρχονται από αυτόν. Αυτή η λύση υπερνικά τη χρήση υψηλής ισχύος για να εκτελεστούν επιθέσεις βιασύνης. Εφόσον ο αποστολέας που χρησιμοποιεί υψηλή ισχύ δεν μπορεί να δεχτεί πακέτα από μακρινούς κόμβους, δεν μπορεί να εκτελέσει τη διαδικασία εντοπισμού γειτόνων και επακόλουθα θα αγνοηθεί. Το κυριότερο μειονέκτημα είναι η μεγάλη επιβάρυνση που δημιουργείται στο δίκτυο όταν η κινητικότητα αυξάνεται.

δ. Τυχαία προώθηση μηνυμάτων

Η τεχνική αυτή προτάθηκε για να ελαχιστοποιηθεί η πιθανότητα ένας βιαστικός επιτιθέμενος να επικρατήσει σε όλες τις διαδρομές. Κατά την προώθηση των μηνυμάτων RREQ, ο κόμβος προωθεί αμέσως το πρώτο RREQ και απορρίπτει όλα τα επακόλουθα. Βάσει αυτού του σχήματος, ένας κόμβος πρώτα συγκεντρώνει έναν αριθμό μηνυμάτων RREQ και επιλέγει τυχαία κάποια από αυτά. Λαμβάνονται υπόψη δυο παράμετροι: πόσα πακέτα RREQ πρέπει να συλλεχθούν και ο αλγόριθμους που επιλέγεται για την λήξη των χρονικών διαστημάτων αποστολής μηνυμάτων. Το μειονέκτημα αυτής της τεχνικής είναι ότι αυξάνεται η καθυστέρηση της ανακάλυψης δρομολογίων, καθόσον κάθε κόμβος πρέπει να περιμένει κάποιο χρόνο για να λάβει το μήνυμα RREQ που προορίζεται γι' αυτόν. Επίσης, αποτρέπεται η ανακάλυψη των βέλτιστων δρομολογίων.

ε. Δρομολόγηση «κρεμμυδιού»

Η τακτική αυτή προτείνει μια αποτελεσματική στρατηγική ασύμμετρης κρυπτογράφησης για να προστατευτεί και να διασφαλιστεί η ανωνυμία των προορισμών των δρομολογίων εφαρμόζοντας ένα πρωτόκολλο δρομολόγησης πηγής [150]. Αυτή η τεχνική περιλαμβάνει κρυπτογράφηση ενός δρομολογίου σε μια μορφή κρεμμυδιού και μετάδοση των πακέτων με αυτή τη μορφή. Κατά την φάση απάντησης, κάθε κόμβος προσθέτει τη διεύθυνση στο επόμενο κομμάτι του αποκαλυπτόμενου δρομολογίου και κρυπτογραφεί το αποτέλεσμα χρησιμοποιώντας το δημόσιο κλειδί του προηγούμενου κόμβου. Έτσι, κάθε κόμβος θα μπορεί να διαβάζει το αμέσως επόμενο άλμα - όταν τα δεδομένα μεταδίδονται - και όχι κάποιο άλλο.

Αυτός ο μηχανισμός εξασφαλίζει ότι κάθε κόμβος θα μπορέσει να ταυτοποιήσει τον επόμενο, όταν το υπόλοιπο του δρομολογίου μείνει ανώνυμο. Μπορούμε να αποφύγουμε τις επιθέσεις DoS με τροποποίηση δρομολογίου πηγής. Όταν συνδυαστεί με πιστοποίηση, αυτός ο μηχανισμός είναι ισχυρός και αποτελεσματικός αλλά υποφέρει από υψηλό υπολογιστικό κόστος. Παρακάτω παρουσιάζεται ένας συγκεντρωτικός πίνακας με τις λύσεις που προτείνονται, τις επιθέσεις που αποτρέπονται και τα μειονεκτήματά τους (Σχήμα 44).

Λύσεις	**Επιθέσεις που αποτρέπονται**	**Μειονεκτήματα**
Πιστοποίηση σε όλες τις φάσεις	Όλες οι εξωτερικές επιθέσεις, παραπλάνηση, ανακατεύθυνση τροποποιώντας το νούμερο ακολουθίας δρομολογίου.	Απαιτεί αρχή πιστοποίησης ή μηχανισμό διαμοίρασης κλειδιού.
Παραμετροποίηση εμπιστοσύνης	Όλες οι επιθέσεις αποτρέπονται από την πιστοποίηση καθώς και οι επιθέσεις σε κόμβους υψηλότερης εμπιστοσύνης.	Απαιτεί αρχή πιστοποίησης ή μηχανισμό διαμοίρασης κλειδιού. Δυσκολία στον ορισμό του επιπέδου εμπιστοσύνης.
Διακρίβωση ασφαλούς γειτονίας	Όλες οι επιθέσεις αποτρέπονται από την πιστοποίηση καθώς επίσης και οι επιθέσεις βιασύνης.	Απαιτεί αρχή πιστοποίησης ή μηχανισμό διαμοίρασης κλειδιού. Σημαντική επιβάρυνση όταν αυξηθεί η κινητικότητα.
Τυχαία προώθηση μηνυμάτων	Επιθέσεις βιασύνης.	Καθυστέρηση.
Κρυπτογράφηση κρεμμυδιού.	Όλες οι εξωτερικές επιθέσεις και οι επιθέσεις παραπλάνησης και τροποποίησης δρομολογίου προορισμού.	Απαιτεί αρχή πιστοποίησης ή μηχανισμό διαμοίρασης κλειδιού. Υψηλό υπολογιστικό κόστος.

Σχήμα 44. Λύσεις στα πρωτόκολλα δρομολόγησης.

5.5.3 Σχεδιαστικά ζητήματα κατά τη δρομολόγηση

Παρά τις πολλές εφαρμογές των δικτύων που εξετάζουμε, όπως έχουμε αναφέρει, τα δίκτυα έχουν και πολλούς περιορισμούς (περιορισμένη παροχή ενέργειας, ισχύ υπολογισμών, περιορισμό στο εύρος ζώνης κ.ά.). Ο κυριότερος στόχος ενός πρωτοκόλλου δρομολόγησης είναι να βγάλει σε πέρας την επικοινωνία, ενώ ταυτόχρονα να προσπαθήσει, με τα διαθέσιμα μέσα, να παρατείνει τον χρόνο ζωής του κόμβου. Ο σχεδιασμός ενός πρωτοκόλλου δρομολόγησης επηρεάζεται από πολλούς παράγοντες. Αυτοί οι παράγοντες πρέπει να εκτιμηθούν κατάλληλα ώστε να επιτύχουμε αποτελεσματική επικοινωνία στο δίκτυο. Παρακάτω αναλύονται κάποια από τα σχεδιαστικά ζητήματα που επηρεάζουν τη διαδικασία δρομολόγησης.

α. Ανάπτυξη κόμβων

Η ανάπτυξη των κόμβων σε ένα δίκτυο εξαρτάται από την εφαρμογή που θα εκτελέσουμε και επηρεάζει την απόδοση του πρωτοκόλλου δρομολόγησης. Η ανάπτυξη μπορεί να είναι είτε προκαθορισμένη είτε τυχαία. Στην προκαθορισμένη ανάπτυξη, οι κόμβοι τοποθετούνται χειροκίνητα και τα δεδομένα δρομολογούνται σε προκαθορισμένες διαδρομές. Αντίθετα, στην τυχαία ανάπτυξη, οι κόμβοι σκορπίζονται τυχαία δημιουργώντας μια ad hoc υποδομή. Εάν η επακόλουθη κατανομή των κόμβων δεν είναι ομοιόμορφη, χρειάζεται ομαδοποίηση των κόμβων για να δημιουργηθεί η συνδεσιμότητα και να εφαρμοστεί η αποτελεσματική λειτουργία του δικτύου. Ένα δρομολόγιο, για την αποτελεσματική χρήση της ενέργειας και του εύρους ζώνης, θα αποτελείται από πολλαπλά άλματα.

β. Κατανάλωση ενέργειας χωρίς απώλεια ακρίβειας

Οι κόμβοι ενός δικτύου θα χρησιμοποιήσουν την περιορισμένη ενέργειά τους για να εκτελέσουν υπολογισμούς και να μεταδώσουν πληροφορία σε ένα ασύρματο περιβάλλον. Οπότε είναι αναγκαία η ύπαρξη μορφών επικοινωνίας και υπολογισμών που προφυλάσσουν την ενέργεια. Σε ένα δίκτυο, κάθε κόμβος παίζει διπλό ρόλο, τον παραλήπτη και τον αποστολέα δεδομένων. Η κακή λειτουργία ορισμένων κόμβων λόγω έλλειψης ισχύος, μπορεί να προκαλέσει σημαντικές αλλαγές στην τοπολογία του δικτύου και να χρειαστεί η ανά-δρομολόγηση των πακέτων και η αναδιοργάνωση του δικτύου.

γ. Μοντέλο αναφοράς δεδομένων

Η αναφορά των δεδομένων στα δίκτυα εξαρτώνται από την εφαρμογή και την κρισιμότητα των δεδομένων. Η αναφορά των δεδομένων μπορεί να κατηγοριοποιηθεί σε αυτά που οδηγούνται από τον χρόνο, το γεγονός, το ερώτημα και στα υβριδικά. Η αναφορά που εξαρτάται από τον χρόνο είναι κατάλληλη για εφαρμογές που απαιτούν περιοδικό έλεγχο δεδομένων. Σε αυτά που οδηγούνται από το γεγονός και το ερώτημα, οι κόμβοι αντιδρούν ακαριαία κατά την εμφάνιση ενός γεγονότος ή ενός ερωτήματος. Ο συνδυασμός των παραπάνω μοντέλων είναι πιθανός και δημιουργεί το υβριδικό μοντέλο. Το πρωτόκολλο δρομολόγησης επηρεάζεται άμεσα από την αναφορά των δεδομένων καθόσον από αυτήν εξαρτάται η κατανάλωση της ενέργειας και η σταθερότητα των διαδρομών.

δ. Ετερογένεια κόμβων-συνδέσεων

Σε πολλά δίκτυα υποθέτουμε ότι οι κόμβοι είναι ομογενείς (έχουν δηλαδή ίση ικανότητα σε όρους υπολογισμών, επικοινωνίας και ισχύος). Ανάλογα με την εφαρμογή του δικτύου, κάθε κόμβος μπορεί να έχει διαφορετικές ικανότητες. Η ύπαρξη ετερογένειας στους κόμβους δημιουργεί πολλά τεχνικά ζητήματα στη δρομολόγηση δεδομένων. Έτσι, για παράδειγμα, τα ιεραρχικά πρωτόκολλα καθορίζουν έναν επικεφαλή ομάδας διαφορετικό από τους υπολοίπους κόμβους. Αυτοί οι επικεφαλής μπορούν να επιλεγούν τυχαία ή να είναι οι πιο ισχυροί κόμβοι από όλους τους υπολοίπους. Σε αυτήν την περίπτωση το βάρος της μετάδοσης των δεδομένων προς τον σταθμό βάσης μετατοπίζεται προς τους επικεφαλείς κόμβους.

ε. Ανοχή σφαλμάτων

Ορισμένοι κόμβοι μπορεί να αποτύχουν στην αποστολή τους λόγω της έλλειψης ισχύος, φυσικής καταστροφής ή περιβαλλοντικής παρεμβολής. Η αποτυχία ενός κόμβου δεν πρέπει να επηρεάσει την όλη αποστολή του δικτύου. Εάν πολλοί κόμβοι αποτύχουν, τα πρωτόκολλα δρομολόγησης πρέπει να προσαρμόσουν την μορφή του δικτύου δημιουργώντας νέες συνδέσεις και δρομολόγια προς τον σταθμό βάσης. Αυτό μπορεί να απαιτήσει προσαρμογή της μετάδοσης στα νέα δεδομένα και ενημέρωση των υπαρχόντων συνδέσεων για μείωση κατανάλωσης ενέργειας ή ανά-δρομολόγηση των πακέτων μέσω περιοχών του δικτύου όπου υπάρχει περισσότερη ενέργεια.

στ. Κλιμάκωση

Ο αριθμός των κόμβων που αναπτύσσονται σε μια περιοχή μπορεί να είναι χιλιάδες. Οποιοδήποτε πρωτόκολλο δρομολόγησης πρέπει να μπορεί να τα βγάζει πέρα με αυτό το μεγάλο αριθμό κόμβων. Επιπλέον, το πρωτόκολλο δρομολόγησης πρέπει να είναι κλιμακωτό για να αντιδρά στα γεγονότα του περιβάλλοντος. Μέχρι να λάβει χώρα κάποιο γεγονός, πολλοί από τους κόμβους μπορούν να παραμείνουν στην κατάσταση ύπνωσης, με τα δεδομένα από τους υπόλοιπους κόμβους να παρέχουν ικανοποιητική ποιότητα επικοινωνίας.

ζ. Δυναμική δικτύου

Πολλές αρχιτεκτονικές δικτύων υποθέτουν ότι οι κόμβοι είναι στάσιμοι. Παρόλα αυτά, η κινητικότητα τόσο των κόμβων όσο και των σταθμών βάσεων είναι απαραίτητη σε πολλές εφαρμογές. Η δρομολόγηση προς και από κινούμενους κόμβους γίνεται σημαντικό θέμα καθόσον τα δρομολόγια πρέπει να αναπροσαρμόζονται. Επιπλέον, το φαινόμενο που ελέγχεται μπορεί να είναι κινούμενο ανάλογα με την εφαρμογή. Σε κινούμενα γεγονότα απαιτείται περιοδική αναφορά και επακόλουθα δημιουργείται σημαντική κίνηση προς τον σταθμό βάσης.

η. Μέσο μετάδοσης

Σε ένα δίκτυο πολλαπλών αλμάτων, οι επικοινωνούντες κόμβοι συνδέονται με ένα ασύρματο μέσο. Τα παραδοσιακά προβλήματα που συνδέονται με το ασύρματο μέσο μπορούν να επηρεάσουν την λειτουργία του δικτύου. Γενικά, το απαιτούμενο εύρος ζώνης των δεδομένων ανίχνευσης είναι χαμηλό, περίπου 1-100 kb/s. Ανάλογη με το μέσο μετάδοσης είναι και η σχεδίαση του Medium Access Control (MAC), μία

σχεδίαση που χρησιμοποιεί TDMA πρωτόκολλα τα οποία καταναλώνουν περισσότερη ενέργεια σε σχέση με τα πρωτόκολλα που στηρίζονται σε ανταγωνισμό, όπως το CSMA.

θ. Συνδεσιμότητα

Η υψηλή πυκνότητα των κόμβων σε ένα δίκτυο καθιστά αδύνατη την απομόνωση των κόμβων. Γι' αυτό οι κόμβοι αναμένεται να έχουν καλή σύνδεση μεταξύ τους. Αυτό όμως δεν αποτρέπει την τοπολογία του δικτύου να είναι μεταβλητή και το μέγεθος του δικτύου να συρρικνώνεται λόγω της αποτυχίας των δικτύων. Επιπλέον, η συνδεσιμότητα εξαρτάται από την πιθανόν τυχαία κατανομή των κόμβων.

ι. Κάλυψη

Στα δίκτυα ad hoc και sensor κάθε κόμβος ελέγχει μια ορισμένη περιοχή του περιβάλλοντος. Η περιοχή αυτή περιορίζεται από την εμβέλεια και από την ακρίβεια και έτσι μπορεί να καλύψει μόνο μια περιορισμένη φυσική περιοχή του περιβάλλοντος. Έτσι, η κάλυψη αποτελεί ένα σημαντικό μέρος για τη δημιουργία ενός πρωτοκόλλου δρομολόγησης.

ια. Συγκέντρωση δεδομένων

Επειδή οι κόμβοι παράγουν περιττή κίνηση, όμοια πακέτα από διάφορους κόμβους συγκεντρώνονται ώστε να μειωθεί ο αριθμός των μεταδόσεων. Η συγκέντρωση δεδομένων είναι ο συνδυασμός δεδομένων από διαφορετικές πηγές, σύμφωνα με μια συνάρτηση συγκέντρωσης. Αυτή η τεχνική χρησιμοποιείται για να επιτύχουμε αποδοτικότητα στην κατανάλωση ενέργειας και βέλτιστη μεταφορά δεδομένων σε ένα μεγάλο αριθμό πρωτοκόλλων. Μέθοδοι επεξεργασίας σήματος μπορούν να χρησιμοποιηθούν για τη συγκέντρωση δεδομένων. Αυτή η περίπτωση αναφέρεται ως συγχώνευση δεδομένων (*data fusion*), όπου ένας κόμβος είναι ικανός να παράγει καλύτερο σήμα εξόδου χρησιμοποιώντας ορισμένες τεχνικές όπως διαμόρφωση δέσμης (beam forming) για να συνδυάσει τα εισερχόμενα σήματα και να μειώσει το θόρυβό τους.

ιβ. Ποιότητα υπηρεσιών

Σε ορισμένες εφαρμογές, τα δεδομένα πρέπει να παραδίδονται εντός ενός ορισμένου χρονικού διαστήματος, διαφορετικά τα δεδομένα θεωρούνται άχρηστα. Άρα, μια περιορισμένη καθυστέρηση στην παράδοση δεδομένων είναι μια συνθήκη που πρέπει να ικανοποιείται στις εφαρμογές που περιορίζονται από τον χρόνο. Όμως, σε πολλές εφαρμογές, η κατανάλωση ενέργειας που συνδέεται άμεσα με τον χρόνο ζωής του δικτύου θεωρείται πιο σημαντική από την ποιότητα των δεδομένων. Όσο η ενέργεια μειώνεται, το δίκτυο θα προσπαθήσει να μειώσει την ποιότητα των αποτελεσμάτων ώστε να αυξήσει το χρόνο ζωής του. Για να επιτευχθεί αυτή η απαίτηση χρειάζονται πρωτόκολλα που αντιλαμβάνονται το επίπεδο ενέργειας του δικτύου (*energy aware protocols*).

5.5.4 Πολύ-διαδρομική δρομολόγηση

Σύμφωνα με τον αριθμό των διαδρομών που ανακαλύπτονται από την αίτηση για εύρεση δρομολογίου, τα πρωτόκολλα δρομολόγησης διακρίνονται σε απλής διαδρομής και πολλαπλών διαδρομών. Στα πρωτόκολλα δρομολόγησης απλής διαδρομής, ένας επιτιθέμενος μπορεί να εκτελέσει μια DoS επίθεση ακόμα και αν ληφθούν μέτρα ασφαλείας. Στην πολυδιαδρομική δρομολόγηση τα πρωτόκολλα προσαρμόζονται εύκολα στις επιθέσεις DoS και μπορούν να προστατεύσουν τη διαθεσιμότητα του δικτύου από «ελαττωματικούς», ή ακόμα χειρότερα, κακόβουλους κόμβους [151]. Έτσι, εάν υπάρχουν *k* διαδρομές μεταξύ δύο κόμβων, ο επιτιθέμενος πρέπει να καταλάβει τουλάχιστο *k* κόμβους και συγκεκριμένα έναν κόμβο από κάθε διαδρομή για να μπορέσει να ελέγχει την επικοινωνία.

α. Ελαττώματα πολυδιαδρομικής δρομολόγησης

Τα πρωτόκολλα πολλών διαδρομών μπορούν να δεχθούν διάφορες επιθέσεις που θα επηρεάσουν την εύρεση διαδρομών. Έτσι, η ασφάλεια των πολυδιαδρομικών πρωτοκόλλων ανάγεται στην ασφάλεια ενός πρωτοκόλλου απλής διαδρομής. Παρακάτω παρουσιάζονται κάποια από τα ελαττώματα και τις επιθέσεις που δέχονται τα πρωτόκολλα:

- *Το ανταγωνιστικό φαινόμενο*. Σε πολλά πολυδιαδρομικά πρωτόκολλα, κάθε ενδιάμεσος κόμβος επεξεργάζεται την κάθε αίτηση διαδρομής μόνο την πρώτη φορά που τη λαμβάνει. Αυτό συμβαίνει ανεξάρτητα εάν μια επιτυχημένη επεξεργασία έχει μεταδοθεί μέσω ενός διαφορετικού δρομολογίου. Σε περίπτωση που ένας ενδιάμεσος κόμβος τύχει να λάβει πρώτος μια αίτηση που αποτρέπει την εύρεση άλλου δρομολογίου (που ανήκει σε μία ομάδα από δρομολόγια), τότε η αίτηση εύρεσης δρομολογίου θα σταματήσει χωρίς να βρει όλα τα υπάρχοντα δρομολόγια. Ένας κόμβος ο οποίος θα δοκιμαστεί από το ανταγωνιστικό φαινόμενο θα συμπεριφέρεται σαν να δέχεται την επίθεση βιασύνης [77], παρόλο που καμία κακόβουλη ενέργεια δεν λαμβάνει χώρα.
- *Απομίμηση και έλλειψη πιστοποίησης*. Εάν ένα πρωτόκολλο απαιτεί την πιστοποίηση από την αρχή ως το τέλος και οι ενδιάμεσοι κόμβοι δεν είναι πιστοποιημένοι, τότε οι κόμβοι εκτίθενται σε σιβυλλικές επιθέσεις απομίμησης, κατά την οποία ένας κόμβος μπορεί να παρουσιάσει πολλαπλές ταυτότητες [49]. Έτσι, ένας κακόβουλος κόμβος μπορεί να συμμετάσχει σε περισσότερες από μία διαδρομές, παρουσιάζοντας διαφορετική ταυτότητα σε κάθε διαδρομή. Τα αποτελέσματα αυτής της επίθεσης μπορούν να μεγιστοποιηθούν εάν συνδυαστεί με την επίθεση μαύρης τρύπας, όπου ο επιτιθέμενος απαντάει σε όλες τις αιτήσεις με ψεύτικες συνδέσεις ελάχιστης διαδρομής.
- *Αόρατος κόμβος* [152]. Σε αυτήν την κατάσταση ένας κακόβουλος κόμβος δεν αποκαλύπτει την παρουσία του στη διαδρομή. Αντίθετα, ο αόρατος κόμβος επαναλαμβάνει αθόρυβα την επικοινωνία μεταξύ δύο κόμβων που βρίσκονται δύο άλματα μακριά, οι οποίοι υποθέτουν ότι επικοινωνούν απευθείας. Με αυτή την τεχνική, ο κόμβος μπορεί να συμμετέχει σε πολλές διαδρομές, ακόμα και αν

το πρωτόκολλο απαιτεί πιστοποίηση των ενδιάμεσων κόμβων. Η πιστοποίηση δεν μπορεί να βοηθήσει καθόσον ο αόρατος κόμβος αναμεταδίδει τα μηνύματα πιστοποίησης.

β. Πλεονεκτήματα πολυδιαδρομικής δρομολόγησης

Η πολυδιαδρομική δρομολόγηση παρέχει ισορροπία φορτίου και μειώνει τη συχνότητα της ανακάλυψης δρομολογίων κατόπιν αίτησης. Αυτά τα πλεονεκτήματα μετατρέπουν την πολυδιαδρομική δρομολόγηση ως μια ιδανική δρομολόγηση για τα δίκτυα ad hoc και sensor. Παρόλα αυτά, τα παραπάνω πλεονεκτήματα δεν αποκτώνται εύκολα καθόσον οι πολλαπλές διαδρομές παρεμβαίνουν στην μεταδόσεις των υπολοίπων κόμβων και το κόστος για την εύρεση των κατάλληλων διαδρομών είναι συνήθως μεγαλύτερο από ότι σε μία απλή διαδρομή. Τα συνήθη πλεονεκτήματα των πολλαπλών διαδρομών παρατίθενται παρακάτω [153]:

- Η συχνότητα εύρεσης ενός δρομολογίου στην πολυδιαδρομική δρομολόγηση είναι μικρότερη από την εύρεση σε ένα δρομολόγιο απλής διαδρομής.
- Στην πολυδιαδρομική δρομολόγηση επιτυγχάνεται βελτίωση της καθυστέρησης από άκρο σε άκρο.
- Το φορτίο που παράγεται μπορεί να κατανεμηθεί πιο ομαλά στην πολυδιαδρομική δρομολόγηση. Η κινητικότητα μπορεί να συνεισφέρει στην εξισορρόπηση του φορτίου. Η εξισορρόπηση του φορτίου είναι σημαντική καθόσον μπορεί να προστατέψει έναν κόμβο από την κατασπατάληση της ενέργειας.
- Η αρχική επιλογή των πολλαπλών διαδρομών μπορεί να επηρεάσει τη μέση καθυστέρηση όταν η ταχύτητα είναι χαμηλή.

γ. Παρουσίαση πολυδιαδρομικών πρωτοκόλλων

Σε αυτή την παράγραφο εξετάζουμε πρωτόκολλα δρομολόγησης που χρησιμοποιούν πολλαπλές διαδρομές για να βελτιώσουν την απόδοση του δικτύου. Η προσαρμοστικότητα ενός πρωτοκόλλου μετριέται από την πιθανότητα της ύπαρξης εναλλακτικής διαδρομής, όταν η υπάρχουσα διαδρομή μεταξύ πηγής και προορισμού καταρρεύσει. Η πιθανότητα μπορεί να αυξηθεί, διατηρώντας πολλαπλές διαδρομές μεταξύ των κόμβων με αύξηση φυσικά της κατανάλωσης ενέργειας και της παραγωγής κίνησης. Αυτές οι διαδρομές διατηρούνται ζωντανές στέλνοντας περιοδικά μηνύματα. Γι' αυτούς τους λόγους, η αξιοπιστία του δικτύου μπορεί να αυξηθεί με κόστος την αύξηση της επιβάρυνσης για τη διατήρηση των εναλλακτικών διαδρομών.

Παρόλα αυτά, για να μειώσουν την επιβάρυνση που δημιουργείται σε πολλά πρωτόκολλα δρομολόγησης, κάθε ενδιάμεσος κόμβος επεξεργάζεται και προωθεί μόνο το πρώτο μήνυμα που δέχεται από μία αίτηση και απορρίπτει οποιοδήποτε αντίγραφο [154]. Αυτό οδηγεί στη δημιουργία λιγότερο επικαλυπτόμενων διαδρομών καθόσον τα αντίγραφα απορρίπτονται εάν έχουν μεταδοθεί σε κάποια διαφορετική γειτονιά κόμβων.

Το πρωτόκολλο SRP [67] είναι ένα πρωτόκολλο που καταφέρνει να βρίσκει μη επικαλυπτόμενες διαδρομές. Χρησιμοποιεί συμμετρική κρυπτογραφία από άκρη σε άκρη, για να προστατέψει την ακεραιότητα της ανακάλυψης δρομολόγιου. Το μήνυμα

αίτησης δρομολόγιου αποτελείται από διαφορετικές οντότητες, που ανατίθενται από την πηγή για να αποφευχθούν οι επιθέσεις επανάληψης. Κάθε ενδιάμεσος κόμβος προωθεί μόνο το πρώτο μήνυμα που δέχεται και όχι τα αντίγραφά του. Μόλις ένας ενδιάμεσος κόμβος λάβει μία αίτηση, ελέγχει εάν έχει λάβει το μήνυμα πρόσφατα και αν όχι, προσθέτει τον εαυτό του στον πίνακα δρομολογίου και το προωθεί, διαφορετικά το απορρίπτει. Όταν ο προορισμός δέχεται μια αίτηση, ελέγχει την πιστοποίησή της χρησιμοποιώντας κρυπτογράφηση συμμετρικού κλειδιού, την οποία οι δύο κόμβοι υποτίθεται ότι έχουν μοιραστεί πριν την έναρξη της ανταλλαγής μηνυμάτων επικοινωνίας. Το μήνυμα απάντησης προστατεύεται με τον ίδιο τρόπο (συμμετρικό κλειδί), με σκοπό να προστατευτεί η ακεραιότητα των δρομολογίων. Παρόλα αυτά, η διάδοση αιτήσεων είναι αδύναμη στο φαινόμενο βιασύνης (racing phenomenon) που μπορεί να αποτρέψει την ανακάλυψη μη επικαλυπτόμενων διαδρομών. Επιπλέον, οι ενδιάμεσοι κόμβοι δεν πιστοποιούνται και έτσι καθιστούν το πρωτόκολλο αδύναμο σε επιθέσεις απομίμησης και στη Σιβυλλική επίθεση [49]. Κατά την επίθεση αυτή, ένας κακόβουλος κόμβος μπορεί να συμμετάσχει με ψεύτικες οντότητες σε πολλές διαδρομές, καθιστώντας ανασφαλή την πολλαπλή δρομολόγηση.

Το πρωτόκολλο Multipath [155] στηρίζεται στον αλγόριθμο Ford-Fulkerson MaxFlow. Σε αυτό το πρωτόκολλο, όταν ένας ενδιάμεσος κόμβος δέχεται μια αίτηση, πρώτα ελέγχει εάν το πεδίο 'μέγιστη απόσταση άλματος' (maximum hop distance) έχει πάρει την μέγιστη τιμή του. Εάν όχι, προσθέτει τα στοιχεία του γείτονά του μαζί με μια υπογραφή και προωθεί το πακέτο, διαφορετικά το απορρίπτει. Όταν ο κόμβος προορισμού δέχεται την αίτηση, χρησιμοποιεί την πληροφορία για να υπολογίσει την τωρινή συνδεσιμότητα του δικτύου και για να κατασκευάσει πλήρεις ομάδες υπαρχόντων, μη επικαλυπτόμενων διαδρομών. Το πρωτόκολλο παρουσιάζει χαρακτηριστικά υψηλής ασφάλειας, καθόσον όλοι οι συμμετέχοντες κόμβοι πιστοποιούνται και η ακεραιότητα του δρομολογίου προστατεύεται. Καταφέρνει να βρει όλες τις μη επικαλυπτόμενες διαδρομές. Όμως, η μετάδοση των αιτήσεων δεν είναι αποτελεσματική καθόσον έχει μεγάλο υπολογιστικό κόστος. Η συσσωρευτική πληροφορία από τα μηνύματα των γειτονικών κόμβων μπορεί να γίνει μεγαλύτερη από το μέγεθος του μηνύματος. Επιπλέον, η χρήση ψηφιακών υπογραφών από τους ενδιάμεσους κόμβους σε κάθε μήνυμα αίτησης δημιουργεί κόστος καθυστέρησης και επιπλέον υπολογιστική ισχύ και μπορεί να γίνει απρόσιτη σε τυπικούς εξοπλισμούς.

Το πρωτόκολλο SecMR [156] είναι ένα πλήρες πολυδιαδρομικό πρωτόκολλο που παρουσιάζει πιστοποίηση από άκρο σε άκρο και μεταξύ επιπέδων ζεύξεων και καταφέρνει να προστατεύσει την ακεραιότητα των δρομολογίων. Το πρωτόκολλο εργάζεται σε δύο φάσεις. Στην πρώτη φάση, εκτελείται πιστοποίηση μεταξύ γειτονικών κόμβων η οποία επαναλαμβάνεται σε τακτά χρονικά διαστήματα και εξασφαλίζει την πιστοποίηση μεταξύ των επιπέδων ζεύξης. Κατά τη δεύτερη φάση, η πηγή παράγει μια υπογεγραμμένη αίτηση, που παρέχει στο δίκτυο πιστοποίηση από άκρη σε άκρη. Κάθε ενδιάμεσος κόμβος επεξεργάζεται όλες τις ληφθείσες αιτήσεις, εξασφαλίζοντας με αυτόν τον τρόπο την ανακάλυψη όλων των μη επικαλυπτόμενων διαδρομών. Όταν ένας ενδιάμεσος κόμβος λάβει μια αίτηση μέσω ενός κόμβου που ανήκει στη λίστα με τους πιστοποιημένους γειτονικούς κόμβους, αρχικά προσθέτει τον εαυτό του στο δρομολόγιο και στη συνέχεια κατασκευάζει την πληροφορία γειτονίας και την πληροφορία αποκλειόμενων κόμβων που υπάρχει στο μήνυμα. Η πληροφορία γειτονίας περιέχει όλους τους πιστοποιημένους γειτονικούς κόμβους που δεν έχουν ακόμα λάβει την αίτηση, ενώ η πληροφορία αποκλειόμενων κόμβων περιέχει όλους τους κόμβους που έχουν λάβει την πληροφορία κάποια στιγμή στο παρελθόν. Όταν ο κόμβος προορισμού λάβει την αίτηση, ελέγχει την πιστοποίηση βάσει της υπογραφής του, κατασκευάζει τα μη επικαλυπτόμενα δρομολόγια και

παράγει ένα υπογεγραμμένο μήνυμα απάντησης, προστατεύοντας έτσι την ακεραιότητα της χρησιμοποιημένης διαδρομής.

Βασισμένο στην τεχνική της άμεσης εξάπλωσης (*directed diffusion*) [157], δημιουργήθηκε ένα σχήμα πολλαπλών διαδρομών που βρίσκει μερικώς μη επικαλυπτόμενες διαδρομές [158]. Στην ουσία παρουσιάζονται δύο σχήματα, ένα με μη επικαλυπτόμενα δρομολόγια και ένα με διαδρομές σε μορφή πλεξούδας. Στην πρώτη περίπτωση, κατασκευάζεται μια κύρια διαδρομή και ένας μικρός αριθμός εναλλακτικών διαδρομών που είναι μη επικαλυπτόμενες με την κύρια διαδρομή αλλά και μεταξύ τους. Οι εναλλακτικές διαδρομές είναι ανεπηρέαστες από τις αποτυχίες που παρατηρούνται στην κύρια διαδρομή. Παρόλα αυτά οι εναλλακτικές διαδρομές είναι πιο επιθυμητές από την κύρια διαδρομή, κυρίως λόγω μεγαλύτερης διαδρομής. Επίσης, επειδή οι κόμβοι έχουν μόνο τοπική γνώση των εναλλακτικών διαδρομών, η διαδικασία αναζήτησης μπορεί να ανακαλύψει μεγαλύτερες διαδρομές. Στο δεύτερο σχήμα προσπαθούμε να αποφύγουμε την κατανάλωση ενέργειας από τις μεγαλύτερες διαδρομές και κατασκευάζουμε μερικώς επικαλυπτόμενες διαδρομές. Οι επικαλυπτόμενες διαδρομές κατασκευάζονται με τη λογική της εύρεσης μιας εναλλακτικής διαδρομής από τους κόμβους της κύριας διαδρομής, χωρίς να περιέχεται ο συγκεκριμένος κόμβος.

Μια επέκταση του πρωτοκόλλου DSR έχει προταθεί για τη δημιουργία δύο μη επικαλυπτόμενων διαδρομών. Το πρωτόκολλο EDSR [159] διατηρεί δύο μη επικαλυπτόμενες διαδρομές μετά τη διαδικασία ανακάλυψης διαδρομής. Το βασικό πλεονέκτημα της τεχνικής είναι ότι δεν παρουσιάζει επιπλέον επιβάρυνση. Επιτρέπει τη δημιουργία επικαλυπτόμενων διαδρομών με την ύπαρξη όμως ενός επιπλέον bit που ονομάζεται "dirty bit" για να μπορέσει να υποδείξει σε ποια από τις δύο διαδρομές κινείται το πακέτο.

Μια ακόμα επέκταση ενός απλού πρωτοκόλλου είναι το πρωτόκολλο Ad Hoc On-demand Multipath Distance Vector (AOMDV) [160]. Ο βασικός σκοπός του πρωτοκόλλου είναι να παρέχει αποτελεσματικότητα στην αποτυχία δρομολογίων σε δυναμικά δίκτυα. Για να το πετύχουμε, το AOMDV υπολογίζει πολλαπλά δρομολόγια μη επικαλυπτόμενα που δεν δημιουργούν βρόχους. Η ιδέα ενός διαφημιζόμενου άλματος χρησιμοποιείται για τη δημιουργία αυτών των διαδρομών. Το πρωτόκολλο παρέχει μια σημαντική μείωση στην καθυστέρηση παράδοσης πακέτων από ότι το απλό πρωτόκολλο. Επίσης παρέχει 20% μείωση στο φορτίο και στη συχνότητα ανακάλυψης δρομολογίων.

Με την παρουσίαση των πιο σημαντικών πρωτοκόλλων πολλαπλών διαδρομών τελειώνει η κατηγοριοποίηση για την ασφάλεια σε δίκτυα ad hoc και sensor. Στο επόμενο κεφάλαιο δίδεται μια περιγραφή των στρατιωτικών δικτύων (military networks), των πρωτοκόλλων που χρησιμοποιούν και των ιδιαιτεροτήτων που τα διέπουν.

ΚΕΦΑΛΑΙΟ 6ο

MILITARY NETWORKS

6.1 Στρατιωτικά δίκτυα (Γενικά)

Σχήμα 45. Επίγειες, θαλάσσιες και εναέριες δυνάμεις στηρίζονται στην αποτελεσματική δικτύωση για τακτικές κινήσεις και συνδυασμένες ενέργειες.

Τα δίκτυα - γενικότερα - καθίστανται ολοένα και πιο κρίσιμο σημείο επιτυχίας ή αποτυχίας για τις σύγχρονες ένοπλες δυνάμεις (Σχήμα 45). Αυτό συμβαίνει διότι όλο και περισσότερα συστήματα δικτυώνονται μεταξύ τους και εξαρτώνται –κατόπιν τούτου– από το δίκτυο για να εκπληρώσουν την αποστολή τους. Η απουσία του δικτύου σηματοδοτεί και την απουσία εναλλακτικών διόδων για τη συγκέντρωση και τη διανομή των πληροφοριών. Πιο συγκεκριμένα, τα δίκτυα ad hoc, σχεδιασμένα να διαμορφώνονται από μόνα τους, να 'αυτό-θεραπεύονται' σε περίπτωση προσβολής, κατανεμημένα εκ φύσεως και με έλλειψη κάθε κεντρικού ελέγχου, αποτελούν μία αναδυόμενη τεχνολογία που θεμελιώνουν τα συστήματα Joint Tactical Radio System (JTRS), Wideband Networking Waveform (WNW), Tactical Targeting Network Technology (TTNT), αντικαθιστώντας τα συμβατικά συστήματα JTIDS/MIDS. Η αξιοσημείωτη προσαρμοστικότητα των δικτύων ad hoc, τα καθιστά ισχυρότατα όπλα στην στρατιωτική δικτύωση (military networking).

6.2 Σύντομη αναδρομή στην εξέλιξη των στρατιωτικών δικτύων

Μία σύντομη αναδρομή στην εξέλιξη της ad hoc δικτύωσης στο στρατιωτικό τομέα γίνεται στο [161], όπου αναφέρεται ότι η αρχική ιδέα διατυπώθηκε στην δεκαετία του ’70 και οδήγησε σχετικά γρήγορα στο δίκτυο Packet Radio Network (PRnet) στα 1972, και αργότερα στα Survivable Radio Network (SURAN) και Lowcost Packet Radio (LPR) κατά τη διάρκεια της δεκαετίας του 1980. Τη δεκαετία του ’90, τα ad hoc δίκτυα εισήλθαν και στον εμπορικό τομέα ως ένα παραπροϊόν φθηνών ασύρματων διεπαφών ραδιοσυχνοτήτων.

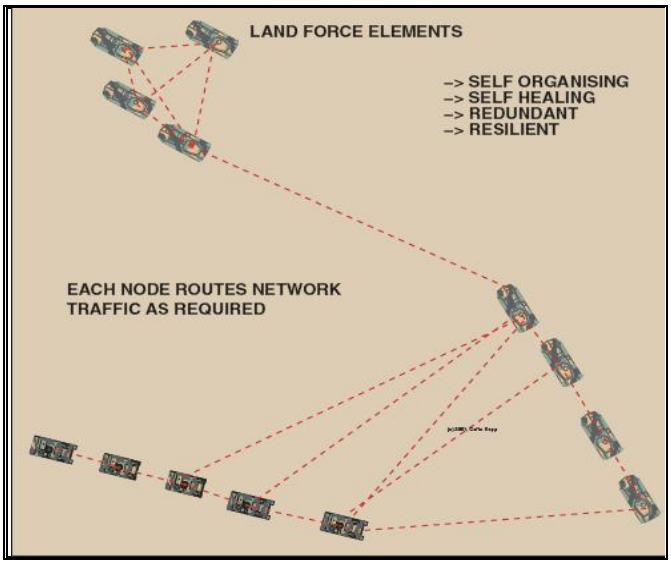
Το ήδη προϋπάρχον σύστημα JTIDS/MIDS στηρίζονταν σε ένα ελεγχόμενο σύστημα χρονικών σχισμών που απαιτεί συγχρονισμό. Επίσης, το παγκόσμιο Internet έχει πρωτόκολλα που βασίζονται σε μία ιεραρχική δενδροειδή τοπολογία συνδέσεων, στην οποία κρίσιμες υπηρεσίες όπως η αντιστοίχηση ονόματος σε διεύθυνση είναι αναγκαστικά συγκεντρωτικές.

Όμως, σε ασύρματα δίκτυα υψηλής κινητικότητας - όπως αυτά που απαιτούνται στη στρατιωτική δικτύωση – η ακαταλληλότητα του ιεραρχικού μοντέλου διαπιστώνεται από το πρόβλημα της δυσκολίας προσαρμογής ενός πανίσχυρου μέσου δικτύωσης (π.χ. δρομολογητής) σ’ ένα περιβάλλον όπου η συνδεσιμότητα στο δίκτυο, και κατά συνέπεια η ίδια η τοπολογία του, μεταβάλλονται με ταχύτατους ρυθμούς.

Η τρέχουσα κατάσταση της σύγχρονης ad hoc δικτύωσης εξελίχθηκε αξιόλογα στα μέσα της δεκαετίας του ’90. Στον στρατιωτικό τομέα, το JTRS εξακολουθεί να ηγείται των πρωτοκόλλων της ad hoc δικτύωσης και μεθοδεύει την ανάπτυξη και επιχειρησιακή αξιολόγηση των τερματικών δικτύωσης. Το πειραματικό πρόγραμμα NTDR (Near Term Digital Radio) επινοήθηκε για να προπορευθεί του JTRS και να συμπληρώσει το κενό των δυνατοτήτων του.

6.3 Ιδιαιτερότητες των στρατιωτικών δικτύων και χρησιμοποιούμενα πρωτόκολλα

Η κεντρική ιδέα πίσω από όλα τα δίκτυα ad hoc και ειδικότερα από τα military networks είναι ότι δεν υφίσταται σταθερή τοπολογία ή ότι αυτή η τελευταία είναι δυναμική και ταχέως μεταβαλλόμενη. Αυτό είναι και το κατ’ εξοχήν κατάλληλο μοντέλο για τα military networks, όπως φαίνεται και στο Σχήμα 46.



Σχήμα 46. Παράδειγμα ενός ad hoc στρατιωτικού δικτύου.

Κάθε υπολογιστής έχει έναν router προσαρτημένο σε αυτόν, είτε ενσωματωμένο στο software είτε ως ένα modem ραδιοσυχνοτήτων (‘κόμβος’), ο οποίος δρομολογεί κίνηση από και προς τους ομότιμους στο δίκτυο. Μία από τις πιο δημοφιλείς τεχνικές που χρησιμοποιούνται είναι το πρωτόκολλο DSR (Dynamic Source Routing), χωρίς να αποκλείονται πρωτόκολλα όπως τα ZRP (Zone Routing Protocol), DSDV (Destination Sequenced Distance Vector), TORA (Temporally Ordered Routing Algorithm), AODV (Ad hoc On demand Distance Vector) και άλλα, κυρίως υβριδικά πρωτόκολλα. Αυτή η πλειάδα επιλογών στα πρωτόκολλα αντανακλά τη δυσάρεστη πραγματικότητα ότι τα ad hoc δίκτυα βασίζονται στις πραγματικά απαραίτητες προσωρινές συνδέσεις μεταξύ των κόμβων που αποτελούν το δίκτυο. Από τη στιγμή που τίποτα δεν είναι μόνιμο και σταθερό στα στρατιωτικά δίκτυα, αυτά πρέπει να σχεδιάζονται εξ’ αρχής ώστε να ανταπεξέρχονται στις συνεχείς αλλαγές των πιθανών συνδέσεων. Δεν παρέχεται επίσης καμία εγγύηση ότι κάθε κόμβος του δικτύου θα είναι συνδεδεμένος στο δίκτυο ανά πάσα στιγμή ή ότι κάθε δίκτυο σε κάποια χρονική στιγμή δεν θα έχει εισχωρήσει σε περισσότερα από ένα μικρότερα δίκτυα.

Όλα τα παραπάνω αποτελούν συνέπειες της ασύρματης διάδοσης διαμέσου της ατμόσφαιρας και της συμπεριφοράς της διάδοσης σχετικά κοντά στην επιφάνεια της γης, όπου η πολυπλοκότητα του εδάφους διαδραματίζει σημαντικό ρόλο (επιφάνεια θάλασσας, βουνά, δάση, τραχύ ή σχετικά ομαλό έδαφος).

6.4 Είδη στρατιωτικών ad hoc δικτύων, δυσχέρειες-περιορισμοί κατά τη λειτουργία τους και τρόποι αντιμετώπισής τους

Γενικά, τα στρατιωτικά ad hoc δίκτυα μπορούν να διαιρεθούν σε εναέρια – μεταξύ κόμβων που βρίσκονται στον αέρα – και επιφανειακά, για περιπτώσεις μεταξύ στρατιωτικών οχημάτων ή πολεμικών πλοίων.

Στα εναέρια δίκτυα, οι πιθανές συνδέσεις μεταξύ κόμβων – καθένας από τους οποίους μεταφέρεται σε ένα αεροσκάφος – περιορίζονται από την εμβέλεια της

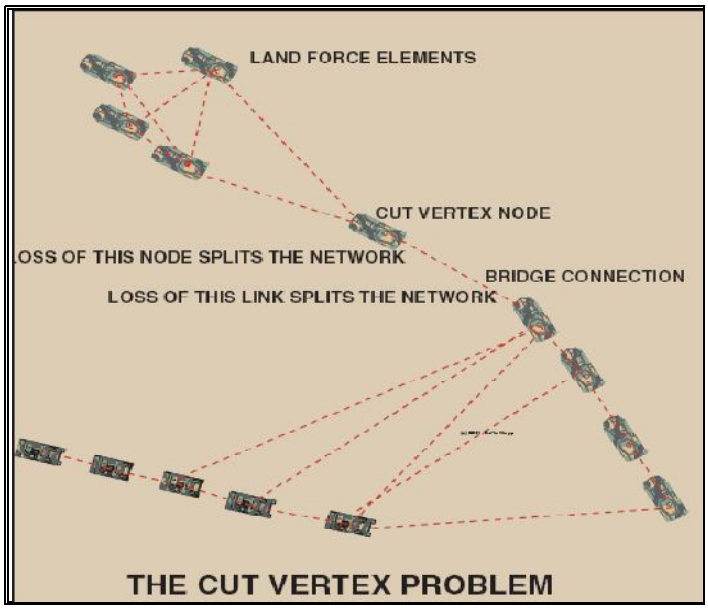
ράδιο-ζεύξης (ή ζεύξης laser) που χρησιμοποιείται, την διάδοση των ραδιοκυμάτων με το συγκεκριμένο χρησιμοποιούμενο μήκος κύματος διαμέσου των καιρικών συνθηκών (πυκνότητα ατμόσφαιρας, ατμοσφαιρικά κατακρημνίσματα) και την καμπυλότητα της γης. Για αεροσκάφη στην τροπόπαυση, η εμβέλεια μπορεί να φτάσει και εκατοντάδες χιλιόμετρα.

Αυτά όμως – όπως γίνεται εύκολα κατανοητό – δεν ισχύουν στα δίκτυα επιφανείας και κυρίως σε όσα αναπτύσσονται στην επιφάνεια του εδάφους. Από τη στιγμή που οι ράδιο- ή laser- ζεύξεις, κατά κανόνα, δεν λειτουργούν όταν χαθεί η οπτική επαφή μεταξύ των επικοινωνούντων συστημάτων, ο ρυθμός αλλαγής της τοπολογίας είναι αρκετά μεγαλύτερος από τα αντίστοιχα εναέρια δίκτυα.

Η ράδιο-διάδοση για επίγειες ή χαμηλού ύψους εναέριες ζεύξεις είναι πλήρης δυσχερειών που οφείλονται στις ανακλάσεις και σκεδάσεις του σήματος λόγω του εδάφους και έχουν ως αποτέλεσμα φαινόμενα εξασθένισης. Σ' αυτή την περίπτωση, ένα ad hoc δίκτυο υφίσταται τους ίδιους περιορισμούς με τα άλλα δίκτυα και μια μορφή αντίστασης στην πολύ-διαδρομική εξασθένιση είναι η χρήση κατάλληλης διαμόρφωσης στο σήμα και του κατάλληλου μήκους κύματος που θα εφαρμοστεί στη ράδιο-ζεύξη.

Σ' αυτό το περιβάλλον, εάν η εξασθένιση του σήματος προκαλέσει τη διακοπή μιας συγκεκριμένης σύνδεσης και εάν υπάρχει μία άλλη διαδρομή προς τον κόμβο-προορισμό, το δίκτυο θα την ανακαλύψει (με το χρησιμοποιούμενο πρωτόκολλο) και θα προσπαθήσει να αποκαταστήσει την επικοινωνία. Υπό αυτή την έννοια, τα δίκτυα ad hoc προσφέρουν δυνητικά πολύ μεγαλύτερη προσαρμοστικότητα και ευκαμψία σε σχέση με άλλα παραδοσιακά, συμβατικά σχήματα και εναλλακτικές.

Τα ad hoc δίκτυα, και συνεπώς τα military networks, υπόκεινται σε περιορισμούς, όπως εξάλλου όλα τα δίκτυα. Το σημαντικότερο πρόβλημα – κυρίως στα εμπορικά δίκτυα όπου δεν ελέγχεται εύκολα η θέση των κόμβων – παρατηρείται όταν ένας κόμβος ή μια σύνδεση είναι η μόνη διαδρομή ανάμεσα σε δύο μέρη του δικτύου (the cut vertex problem) (Σχήμα 47).



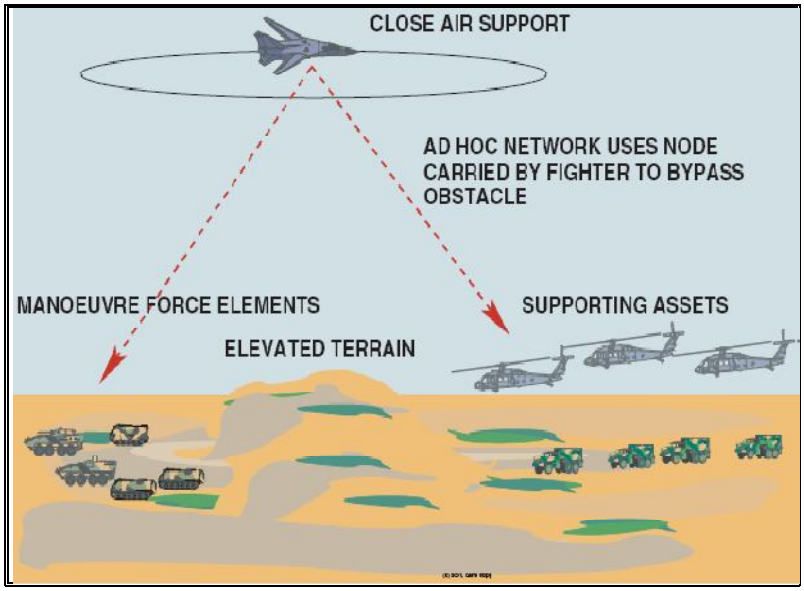
Σχήμα 47. Το πρόβλημα cut vertex.

Εάν ο κόμβος χαθεί ή η σύνδεση διακοπεί, το δίκτυο διαχωρίζεται σε δύο μικρότερα δίκτυα. Στα στρατιωτικά δίκτυα η κατάσταση είναι κάπως διαφορετική αφού υπάρχει η δυνατότητα να διαταχθούν συγκεκριμένες μονάδες στρατού να ανακόψουν ταχύτητα, εάν είναι εφικτό, ώστε να διατηρηθεί η συνδεσιμότητα του δικτύου, π.χ. η εύστοχη χάραξη της τροχιάς ενός αεροσκάφους ανεφοδιασμού για να χρησιμοποιηθεί σαν γέφυρα σύνδεσης ή η κατάλληλη αραίωση μεταξύ φαλάγγων από οχήματα εδάφους.

Τα σοβαρότερα ωστόσο προβλήματα ανακύπτουν με επίγειες δυνάμεις, λόγω των δυσχερειών στη διάδοση, ειδικά για ταχέως προωθούμενες δυνάμεις ελιγμού. Πίσω από αυτές τις δυνάμεις υπάρχουν περιοχές που είναι κυριολεκτικά κορεσμένες από φάλαγγες οχημάτων, οι οποίες παρέχουν υποστήριξη και ανεφοδιασμό σε καύσιμα, πυρομαχικά και άλλα αναλώσιμα. Οι φάλαγγες αυτές παρέχουν δυνατότητες για συνδεσιμότητα στα δίκτυα, εάν μερικά από τα οχήματα φέρουν τον απαραίτητο εξοπλισμό για να λειτουργούν ως κόμβοι δικτύωσης. Στην πράξη, οι φάλαγγες καθίστανται μια προοδευτική αλυσίδα κόμβων δρομολόγησης.

Ο μεγαλύτερος ‘πονοκέφαλος’ προκύπτει από στοιχεία δυνάμεων ελιγμού αποτελούμενα από ταχέως προελαύνοντα τεθωρακισμένα οχήματα και επιθετικά ελικόπτερα, αφού αυτά δύνανται να προωθηθούν αρκετά εμπρός από τα υποστηρίζοντα τμήματα ώστε να έχει χαθεί η οπτική επαφή, ιδιαίτερα εάν το έδαφος είτε έχει εξάρσεις είτε η διάδοση των ραδιοκυμάτων πάνω από αυτό δεν έχει ικανοποιητικό βαθμό.

Η λύση σε αυτό το φαινομενικό αδιέξοδο δίνεται με τη χρήση κοινού και συμβατού εξοπλισμού στην Αεροπορία, στο Στρατό Ξηράς και στο Ναυτικό. Ως εκ τούτου, όταν μία απευθείας σύνδεση διακοπεί, το δίκτυο μπορεί να βρει εναλλακτικές διαδρομές μέσω εναέριων μέσων που υπερίπτανται εκείνη τη στιγμή. Έτσι, κάποιο μαχητικό φίλιο αεροσκάφος σχεδιάζει την τροχιά της πτήσης του κατά τέτοιο τρόπο, ώστε να βρίσκεται κοντά πάνω από τις προωθημένες επίγειες δυνάμεις και να παρέχει μία διαδρομή δρομολόγησης κίνησης πάνω από τα εδαφικά εμπόδια, υπερπηδώντας τους περιορισμούς της ράδιο-διάδοσης (Σχήμα 48).



Σχήμα 48. Αξιοποίηση εναέριου μέσου προς αποφυγή των περιορισμών του εδάφους.

6.5 Προκλήσεις στα δίκτυα αισθητήρων για στρατιωτικές εφαρμογές

Οι μελλοντικές επικοινωνίες, σε τακτικό επίπεδο, των ενόπλων δυνάμεων θα περιλαμβάνουν την ανάπτυξη ευρείας κλίμακας δικτύων αισθητήρων, στα οποία εκατοντάδες μέχρι και χιλιάδες μικρό-αισθητήρες – σχετικά φθηνές και ελαφριές συσκευές με ολοκληρωμένες δυνατότητες αίσθησης, υπολογισμών, επικοινωνίας και δραστηριοποίησης – θα συνεργάζονται για να εκπληρώσουν έναν κοινό ειδικό αντικειμενικό σκοπό [3]. Οι κόμβοι μπορεί να είναι ετερογενείς με ποικίλους ενεργειακούς πόρους, διαφορετικές δυνατότητες και κινητικότητα (π.χ. σταθεροί μη επανδρωμένοι αισθητήρες εδάφους και αισθητήρες-robot). Το δίκτυο οφείλει να λειτουργεί κάτω από σοβαρούς περιορισμούς σε ενέργεια και εύρος ζώνης, πάνω από κανάλια επικοινωνίας με έντονες παρεμβολές και με συχνές αλλαγές στην τοπολογία και τη συνδεσιμότητα. Οι απαιτήσεις σε QoS θα διαφέρουν, κυμαινόμενες – σε σχέση πάντα με τα δεδομένα – από εκείνα που είναι κρίσιμα στο χρόνο (time critical) για υποστήριξη τηλεϊατρικής, ρομποτικής ή στον έλεγχο του πυρός, έως εκείνα που ‘τρέχουν’ στο παρασκήνιο και είναι χαμηλής προτεραιότητας (background data) [162].

Οι συνδυασμοί μεταξύ της τοπικής ή κατανεμημένης επεξεργασίας δεδομένων και της μετάδοσης των μη επεξεργασμένων δεδομένων σ’ ένα κέντρο μίξης (κέντρο επεξεργασίας δεδομένων), πρέπει να εξεταστούν υπό τους περιορισμούς ενέργειας, εύρους ζώνης και καθυστέρησης. Το σχετικό μέτρο που χρησιμοποιείται πρέπει να είναι ανάλογο με την εφαρμογή (π.χ. η ακρίβεια ανίχνευσης και παρακολούθησης του στόχου, η ακρίβεια εκτίμησης της πυκνότητας μιας διασποράς χημικών όπλων, τα χρονικά όρια ανίχνευσης της εξάπλωσης μιας επιδημίας ή την ποιότητα και χρησιμότητα των συλλεγόμενων πληροφοριών) και πάντα σύμφωνο με τα τακτικά δεδομένα και το σενάριο δράσης. Επίσης, το γεγονός ότι οι κόμβοι-αισθητήρες επικοινωνούν με το κέντρο μίξης μέσω μιας ασύρματης ζεύξης και ότι χρησιμοποιείται ένα μεγάλης κλίμακας ad hoc δίκτυο πολλαπλών αλμάτων, οδηγεί στο συμπέρασμα ότι τα χαρακτηριστικά του καναλιού επικοινωνίας και των πρωτοκόλλων MAC και δρομολόγησης επιδρούν επιπλέον στον προαναφερθέντα συνδυασμό.

Τα χρησιμοποιούμενα στις μέρες μας προγράμματα είναι κατατοπιστικά στη χάραξη της εξέλιξης των εφαρμογών των δικτύων αισθητήρων (AWACS, δικτυωμένα συστήματα radar, υποθαλάσσια ακουστικά δίκτυα αισθητήρων για παρακολούθηση υποβρυχίων και πρόγραμμα της DARPA/Defense Advanced Research Projects Agency) [163].

Η παρακολούθηση του περιβάλλοντος του πεδίου της μάχης, όπως η ανίχνευση βιολογικών, ραδιενεργών, πυρηνικών, χημικών και εκρηκτικών υλικών και όπλων καθίσταται ολοένα και πιο σημαντική στον ασύμμετρο πόλεμο. Το περιβάλλον λειτουργίας των αισθητήρων (έδαφος) πιθανόν να είναι τραχύ και δεν επιδέχεται προ-αναπτύξεις πιο ‘μόνιμων’ – πιθανώς και ενσύρματων δικτύων – ή το δίκτυο μπορεί να χρειαστεί να λειτουργήσει σε εχθρική περιοχή. Έτσι υφίσταται μια αυξανόμενη πίεση για ανάπτυξη αναλώσιμων, χαμηλού κόστους και πρόσκαιρης χρησιμότητας ασύρματων αισθητήρων. Οι αισθητήρες αυτοί πρέπει να τοποθετηθούν χειροκίνητα ή να διασπαρθούν από πυροβόλα ή κινούμενα εναέρια και επίγεια μέσα. Το πρόβλημα ισχυροποιείται από ενεργειακούς, υπολογιστικούς και επικοινωνιακούς περιορισμούς και καθώς μεγαλώνει η κλίμακα του δικτύου, η δικτύωση και η επεξεργασία σήματος γίνονται ολοένα και πιο κρίσιμες.

Χαρακτηριστικό παράδειγμα τέτοιου δικτύου αποτελεί η ανανέωση ενός ναρκοπεδίου, όπου το δίκτυο παρακολουθεί συνεχώς τον εαυτό του και, όταν κάποιοι κόμβοι καταστραφούν, κάποιοι άλλοι οφείλουν να μετακινηθούν ανάλογα, ώστε να διατηρηθεί η έκταση της περιοχής κάλυψης. Σε ένα περιορισμένο ενεργειακά δίκτυο όπως το παραπάνω, δεν μπορούν να αγνοηθούν οι επιβαρύνσεις σε θέματα επικοινωνίας. Έτσι, υπάρχουν δοσοληψίες και συνδυασμοί στην επιβάρυνση της συλλογής των πληροφοριών και στα πλεονεκτήματα που θα προκύψουν μιας τέτοιας – συχνά ανακριβούς και μη πλήρους – πληροφόρησης.

Αισθητήρες εξειδικευμένοι ανάλογα της εφαρμογής είναι κατάλληλοι και για στρατιωτικές επιχειρήσεις σε αστικό περιβάλλον (έξυπνα συστήματα για εκκαθάριση και ασφάλεια αστικών κέντρων). Ως παράδειγμα αναφέρεται ένα σύστημα ανίχνευσης της θέσης ενός ελεύθερου σκοπευτή που αποτελείται από αισθητήρες-ανιχνευτές ακουστικών κυμάτων και ένα ad hoc δίκτυο πολλαπλών αλμάτων. Ο χρόνος άφιξης των ηχητικών κυμάτων από τον πυροβολισμό οδηγεί προοδευτικά στον εντοπισμό της ακριβούς θέσης του σκοπευτή [164].

6.6 Χρήση UAVs και δίκτυα UAV-MBN

Τα UAVs (*unmanned aerial vehicles/μη επανδρωμένα αεροσκάφη*) είναι επίσης καλοί υποψήφιοι για επέκταση της περιοχής κάλυψης με τον σημαντικό περιοριστικό όρο ότι ο εξοπλισμός της δικτύωσης και οι σχετιζόμενες με αυτόν κεραίες πρέπει να αντικαταστήσουν αρκετό από το ήδη υπάρχον φορτίο ενός UAV (απαιτήσεις για αυξημένο μέγεθος του UAV). Έτσι, ο εξοπλισμός αυτός τοποθετείται εμβόλιμα σε μεγαλύτερα UAVs ώστε, τόσο να αυξηθούν οι δυνατότητές τους ως εναέριοι επαναλήπτες, όσο και παράλληλα η έξοδος των αισθητήρων τους να γίνεται περισσότερο προσιτή και καλύτερα αναγνώσιμη από τις επίγειες δυνάμεις.

Επίσης, επειδή η ασφαλής επικοινωνία είναι ένας κρίσιμος παράγοντας στα στρατιωτικά περιβάλλοντα, όπου η υποδομή δικτύου είναι ευάλωτη σε επιθέσεις, είναι απαραίτητη η δημιουργία ενός πλαισίου εργασίας με χρήση UAVs που θα εναρμονίζεται με τις ενδεχόμενες αλλαγές ή καταστροφές της υποδομής του δικτύου.

Το ασύρματο ad hoc δίκτυο είναι μία ιδανική τεχνολογία για να εγκατασταθεί μία υποδομή άμεσης επικοινωνίας για στρατιωτικές εφαρμογές, σε περιβάλλοντα τακτικών επιχειρήσεων [163]. Τα χρησιμοποιούμενα πρωτόκολλα δρομολόγησης όμως, δεν ανταποκρίνονται επαρκώς καθώς αυξάνεται το μέγεθος του δικτύου (αύξηση του φορτίου κίνησης λόγω του μεγάλου αριθμού κόμβων προκαλεί αύξηση της επιβάρυνσης δρομολόγησης, δηλ. σπαταλιούνται πόροι και κυρίως χρόνος για την λειτουργία του συστήματος παρά για την ίδια την εφαρμογή).

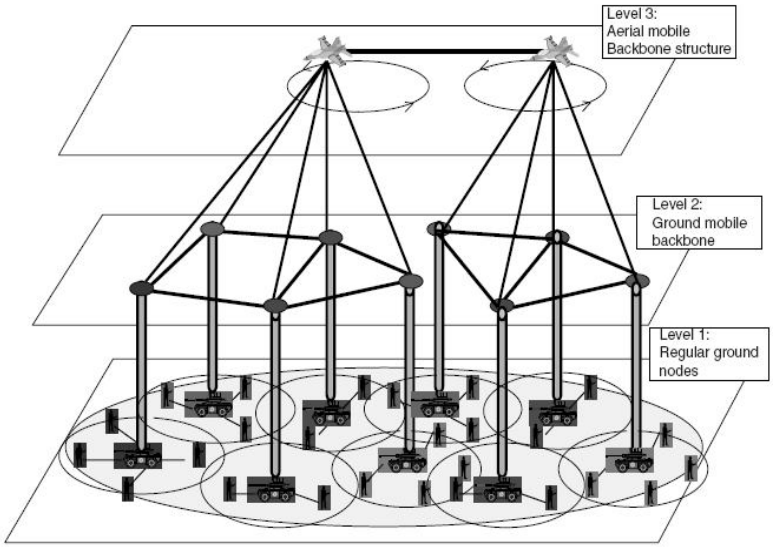
Για να παρακαμφθούν αυτοί οι περιορισμοί, προτάθηκαν ετερογενή πολύ-επίπεδα ad hoc δίκτυα με UAVs, τα επονομαζόμενα UAV-MBN δίκτυα [165], που λειτουργούν με δύο τρόπους, με ή χωρίς υποδομή δικτύου.

Σε ένα τέτοιο δίκτυο (Σχήμα 49), υπάρχουν τρία επίπεδα που αποτελούνται από τρία είδη μονάδων δικτύωσης:

- Οι κανονικοί κινητοί κόμβοι στο έδαφος (1ο επίπεδο), που είναι στρατιώτες εξοπλισμένοι με συσκευές περιορισμένων δυνατοτήτων επικοινωνίας και υπολογιστικής ισχύος.
- Οι κινητοί κόμβοι εδάφους του δικτύου κορμού (*MBN/Mobile Backbone Nodes*) (2ο επίπεδο), που είναι ειδικές μαχόμενες μονάδες (φορτηγά, tanks κτλ.) και που

φέρουν αρκετά καλύτερο εξοπλισμό για μεγαλύτερη επικοινωνιακή και υπολογιστική ισχύ. Με τη χρήση κατάλληλων κεραιών εγκαθίστανται ασύρματες ζεύξεις σημείου προς σημείο μεγάλου εύρους ζώνης μεταξύ των MBN κόμβων, που δρουν ως αρχηγοί ομάδων.

- Οι κόμβοι UAV που σχηματίζουν μία εναέρια κατασκευή από UAVs τα οποία ίπτανται σε ένα ύψος 10 περίπου μιλίων και σε ένα κύκλο με διάμετρο άλλων 10 μιλίων. Κάθε UAV βρίσκεται στην κορυφή ενός θεάτρου επιχειρήσεων, ακριβώς από κάτω του, και επιτυγχάνει επικοινωνία οπτικής επαφής με όλους τους υποκείμενους MBN κόμβους. Όλα τα UAVs που αποτελούν το εναέριο MBN δίκτυο επικοινωνούν μεταξύ τους.



Σχήμα 49. Ιεραρχικά τριών-επιπέδων ασύρματα ad hoc δίκτυα με MBN και UAVs.

6.7 Ασφάλεια UAV-MBN δικτύων

Η υποστήριξη ασφάλειας είναι επιβεβλημένη για δίκτυα που αναπτύσσονται σε περιβάλλοντα στρατιωτικών επιχειρήσεων. Στα υπάρχοντα δίκτυα εφαρμόζονται γενικά κρυπτό-συστήματα και πρωτόκολλα πιστοποίησης για να επιτευχθούν το απόρρητο και η ακεραιότητα μηνυμάτων, η μη-απόρριψη, η πιστοποίηση-αυθεντικοποίηση και η διαθεσιμότητα της υπηρεσίας ασφαλείας. Οι συσκευές επικοινωνίας στα πεδία των μαχών είναι ικανές να λειτουργούν με κρυπτό-συστήματα τόσο συμμετρικού όσο και δημοσίου κλειδιού. Για την πιστοποίηση προϋποτίθεται κεντρική διαχείριση, είτε από κέντρα κατανομής κλειδιού (KDC) είτε από αρχές πιστοποίησης (CA). Για τα UAV-MBN δίκτυα, τα όσα αφορούν στις υπηρεσίες πιστοποίησης εφαρμόζονται στο $3^{ο}$ επίπεδο και παρέχονται από κάθε UAV για το δικό του θέατρο επιχειρήσεων και συνολικά για όλο το εναέριο MBN δίκτυο. Όμως, με μια πιθανή καταστροφή των UAVs από πυραύλους ή εχθρικά αεροσκάφη, το όλο

σύστημα ασφαλείας θα καταρρεύσει, εκτός εάν αναπτυχθούν κάποιοι servers πιστοποίησης σε επίγειες μονάδες ($2^{ου}$ επιπέδου MBN κόμβοι), δημιουργώντας έτσι ένα σχήμα backup. Χωρίς να θυσιαστεί μέρος της αποτελεσματικότητας και της ευελιξίας της κεντρικοποιημένης προσέγγισης, μετά την απώλεια του UAV, οι επίγειες μονάδες μεταπίπτουν στον χωρίς υποδομή τρόπο λειτουργίας, έως ότου ένα νέο UAV γίνει διαθέσιμο.

ΚΕΦΑΛΑΙΟ 7^{Ο}

ΣΥΜΠΕΡΑΣΜΑΤΑ

Η ασφάλεια είναι η σημαντικότερη παράμετρος για τα δίκτυα που εξετάστηκαν στην παρούσα εργασία. Η έλλειψη ασφάλειας οδηγεί σε μη εκπλήρωση της αποστολής του εκάστοτε δικτύου ή σε παραποίησή της προς όφελος του κάθε επιτιθέμενου.

Στην εργασία μας εξετάστηκαν διάφορα θέματα ασφαλείας που διέπουν τα δίκτυα αισθητήρων και τα δίκτυα ad hoc. Επισημάνθηκαν τα χαρακτηριστικά που έχουν τα δύο αυτά είδη δικτύων τα οποία, αν και ανήκουν στην ίδια κατηγορία δικτύων χωρίς υποδομή, έχουν κάποιες διαφορές μεταξύ τους, οι οποίες οφείλονται στην ιδιαίτερη αποστολή για την οποία προορίζεται καθένα από αυτά.

Μελετήθηκαν τα πρωτόκολλα δρομολόγησης που μεταφέρουν δεδομένα μέσα σε ένα δίκτυο. Είδαμε ότι οι ιδιαιτερότητες των δικτύων αισθητήρων - ως προς τα δίκτυα ad hoc - έχουν οδηγήσει στην δημιουργία νέων πρωτοκόλλων. Το κάθε πρωτόκολλο δρομολόγησης παρουσιάζει ξεχωριστά χαρακτηριστικά, τέτοια που να μπορούν να ανταπεξέρχονται στην αποστολή που ανατίθεται σε κάθε δίκτυο. Έτσι, η κινητικότητα, τα πολλαπλά άλματα και η αλλαγή τοπολογίας είναι ορισμένα από τα χαρακτηριστικά που διαφοροποιούν τα πρωτόκολλα δρομολόγησης. Περαιτέρω μελέτη πρέπει να γίνει στη δημιουργία πρωτοκόλλων δρομολόγησης, ώστε να αρθούν οι αδυναμίες που παρουσιάζει κάθε πρωτόκολλο και η δρομολόγηση να γίνεται με πιο αποτελεσματικό τρόπο.

Στη συνέχεια, έγινε αναφορά σε όλα τα θέματα ασφαλείας που αφορούν στα δίκτυά μας. Έτσι μελετήθηκαν οι απαιτήσεις ασφαλείας και οι περιορισμοί που απορρέουν από αυτές τις απαιτήσεις. Έπειτα αναφέρθηκαν οι επιθέσεις που δέχονται τα δίκτυα και τα κυριότερα αντίμετρα και μέτρα αντιμετώπισης των απειλών. Σε αυτό το θέμα, της αντιμετώπισης των απειλών, πρέπει να γίνεται διαρκής μελέτη, καθόσον συνεχώς νέες επιθέσεις και νέοι ιοί δημιουργούνται. Η μελέτη πρέπει να κατευθυνθεί προς την δημιουργία ασφαλέστερων δικτύων.

Η ασφάλεια των δικτύων – ουσιαστικά - μπορεί να κατηγοριοποιηθεί σε τέσσερις βασικές κατευθύνσεις: Στην ασφάλεια του κόμβου, στους αλγόριθμους με τους οποίους κρυπτογραφούνται τα δεδομένα, στην διαδικασία της πιστοποίησης και τέλος στην ασφάλεια κατά την δρομολόγηση. Οποιοδήποτε τμήμα από τα τέσσερα προαναφερθέντα δεν ασφαλιστεί επαρκώς, θα θέσει το δίκτυο σε άμεσο κίνδυνο με αποτέλεσμα – πιθανώς - την αδυναμία εκπλήρωσης της ίδιας της αποστολής του.

Πρέπει να δοθεί ιδιαίτερη βαρύτητα στην έρευνα για τη δημιουργία όλο και ασφαλέστερων πρωτοκόλλων, στην ανάπτυξη ισχυρών αλγόριθμων κρυπτογράφησης αλλά και στην κατασκευή πιο ανθεκτικών κόμβων, ώστε να αποτρέπεται και οποιαδήποτε προσπάθεια φυσικής παραβίασής τους.

ΠΑΡΑΡΤΗΜΑ

ΕΦΑΡΜΟΓΗ ΑΣΥΡΜΑΤΟΥ ΔΙΚΤΥΟΥ ΑΙΣΘΗΤΗΡΩΝ

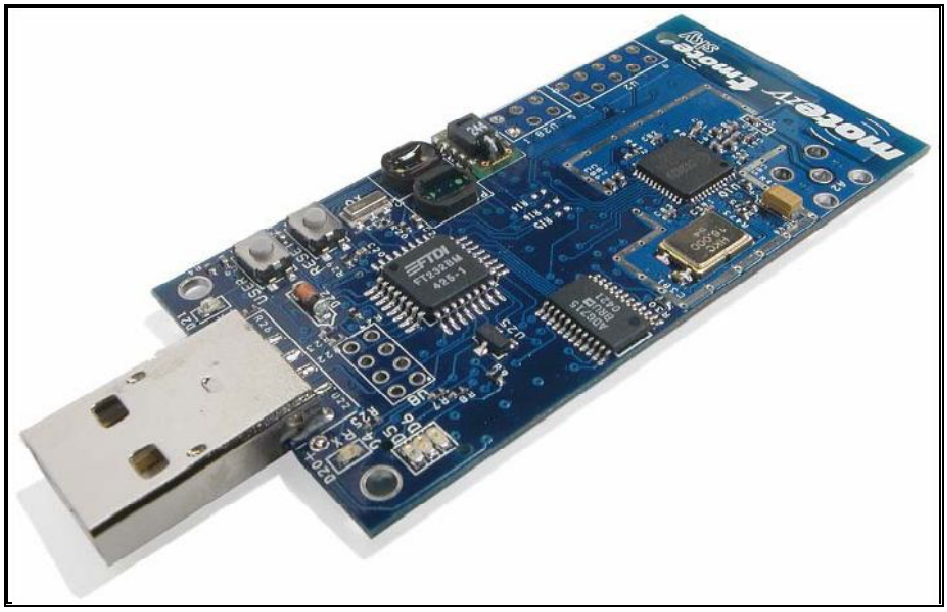
Π.1 Γενική περιγραφή των tmote sky της Moteiv Corporation

Το tmote sky είναι ένα ασύρματο δομικό στοιχείο εξαιρετικά χαμηλής ισχύος για χρήση στα δίκτυα αισθητήρων, στην απεικόνιση εφαρμογών και στην ταχεία προτυποποίηση μιας εφαρμογής. Χρησιμοποιεί πρότυπα όπως το USB και το IEEE 802.15.4 για να διαλειτουργεί απρόσκοπτα με άλλες συσκευές (επικοινωνεί, εκτελεί προγράμματα και μεταφέρει δεδομένα μεταξύ διάφορων λειτουργικών μονάδων). Χρησιμοποιώντας πρότυπα, ενοποιώντας αισθητήρες υγρασίας, θερμοκρασίας και φωτός και παρέχοντας ευέλικτη διασύνδεση με τα περιφερειακά, το tmote sky καθιστά εφικτό ένα μεγάλο εύρος εφαρμογών ασυρμάτων δικτύων και επιτυγχάνει αύξηση της ευρωστίας και της ανοχής σε σφάλματα με παράλληλη μείωση του κόστους και του μεγέθους.

Τα χαρακτηριστικά των tmote sky είναι τα εξής:

- 250kbps, 2.4GHz, IEEE 802.15.4 Ασύρματος Πομποδέκτης
- Διαλειτουργικότητα με άλλες συσκευές IEEE 802.15.4
- 8MHz Μικροελεγκτής (10k RAM, 48k Flash)
- Ολοκληρωμένοι ADC, DAC, Επόπτης Παροχής Τάσης και Ελεγκτής DMA
- Ολοκληρωμένη ενσωματωμένη κεραία με 50m εμβέλεια indoors και 125m outdoors
- Ολοκληρωμένοι αισθητήρες υγρασίας, θερμοκρασίας και φωτός
- Εξαιρετικά χαμηλή κατανάλωση ρεύματος
- Γρήγορη αφύπνιση από την νάρκη (<6μs)
- Κρυπτογράφηση και αυθεντικοποίηση hardware στο επίπεδο ζεύξης δεδομένων
- Προγραμματισμός και συλλογή δεδομένων μέσω USB
- 16-pin υποστήριξη επέκτασης και προαιρετικός σύνδεσμος SMA κεραίας
- Υποστήριξη TinyOS: mesh δικτύωση και υλοποίηση επικοινωνίας
- Φιλικότητα με το περιβάλλον – συμβατότητα με τους κανονισμούς RoHS

Το tmote sky είναι ένα ‘μόριο’ (mote) με ολοκληρωμένους αισθητήρες, ράδιο, κεραία, μικροεπεξεργαστή και δυνατότητες προγραμματισμού και φαίνεται στο Σχήμα 50.



Σχήμα 50. Ο αισθητήρας tmote sky.

Π.2 Εγκατάσταση των Tmote Tools και προκύπτοντα προβλήματα

Πριν ξεκινήσουμε με την εγκατάσταση, κρίνεται απαραίτητο να σβήσουμε όλες τις προηγούμενες εγκαταστάσεις του TinyOS και του Cygwin. Το Cygwin δεν παρέχει κάποια κατάλληλη μέθοδο για την απεγκατάσταση. Αυτή πρέπει να γίνει κλείνοντας όλες τις εφαρμογές και τις υπηρεσίες του Cygwin, σβήνοντας ή μετονομάζοντας κάποια συγκεκριμένα κλειδιά στο registry (κλειδιά μητρώου) μέσω του επεξεργαστή μητρώου (registry editor) και διαγράφοντας ή μετονομάζοντας το directory εγκατάστασης του Cygwin. Για το TinyOS απλά τρέχουμε τον σχετικό απεγκαταστάτη (uninstaller) ή χειροκίνητα απεγκαθιστούμε όλα τα 'tinyos', 'nesc' και 'msp430' RPMs. Κατά τη διαδικασία τώρα της εγκατάστασης, επιλέγουμε την 'τυπική' δυνατότητα εγκατάστασης και, αφού εμφανιστεί το παράθυρο του Cygwin Setup, θα χρειαστεί να περιμένουμε λίγα λεπτά για να εγκατασταθούν όλα τα απαραίτητα packages. Έπειτα γίνεται εγκατάσταση της πλατφόρμας Java και στη συνέχεια το Moteiv Tmote Tools Setup Wizard θα εγκαταστήσει και θα ρυθμίσει τις παραμέτρους των απαραίτητων εργαλείων για την ανάπτυξη και το 'τρέξιμο' των εφαρμογών, χρησιμοποιώντας το open source λειτουργικό σύστημα TinyOS, πράγμα που θα απαιτήσει αρκετό χρόνο.

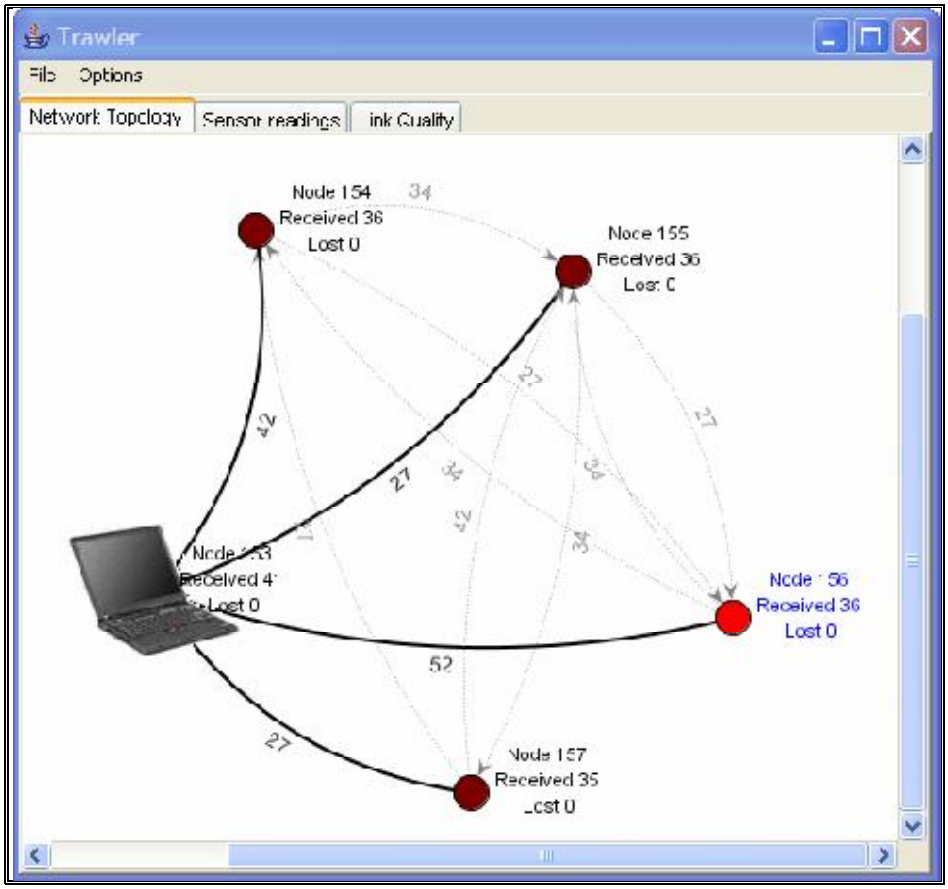
Με την ολοκλήρωση της εγκατάστασης μεταβαίνουμε στην επόμενη ενότητα της δημιουργίας εφαρμογών με τις διαθέσιμες συσκευές. Το πρώτο βήμα είναι να συνδέσουμε έναν αισθητήρα Tmote στην USB θύρα του υπολογιστή μας. Αν δεν βρεθούν τα drivers, θα ανοίξει αμέσως ο wizard για την εγκατάστασή τους. Ήταν αδύνατο να συμβεί αυτό εάν προηγουμένως δεν απεγκαθιστούσαμε από το σύστημά μας όλα τα άλλα 'USB Serial' drivers συσκευών. Τα windows εγκαθιστούν τα αρχεία των driver, ολοκληρώνοντας την εγκατάσταση για το Tmote σαν μία 'USB Serial Port'.

Το Cygwin χρησιμοποιείται για την μεταγλώττιση (compile) και τον επαναπρογραμματισμό των εφαρμογών για το Tmote. Ανοίγουμε ένα shell από το

shortcut του Cygwin που βρίσκεται στο desktop. Μέσα από μια διαδικασία - που δεν κρίνεται σκόπιμο να αναφερθεί – μεταγλωττίζουμε την Delta, μια εφαρμογή της Moteiv για ασύρματους αισθητήρες και mesh δικτύωση. Για το κάθε δομικό στοιχείο (αισθητήρα) πρέπει να συγκεκριμενοποιήσουμε την αντίστοιχη serial port. Εγκαθιστώντας τη Delta σε μερικούς από τους αισθητήρες Tmote Sky, πρέπει να είμαστε σίγουροι ότι κάθε κόμβος έχει μια διαφορετική διεύθυνση δικτύου.

Π.3 Εκτελώντας τον Trawler

Αφού έχουμε εγκαταστήσει την εφαρμογή Delta στα δομικά μας στοιχεία, μπορούμε να παρουσιάσουμε οπτικά το mesh (πλεγματοειδές) δίκτυο, χρησιμοποιώντας την εφαρμογή Moteiv's Trawler (Σχήμα 51). Με εκτέλεση της εντολής MOTECOM=serial@COM4:tmote java com.moteiv.trawler.Trawler, η μεταβλητή 'serial@COM4:tmote' λέει στα εργαλεία της Java να επικοινωνήσουν με τον προσαρτημένο Tmote αισθητήρα, κάνοντας χρήση του σειριακού πρωτοκόλλου στην COM4.



Σχήμα 51. Το πλεγματοειδές (mesh) δίκτυο της εφαρμογής μας.

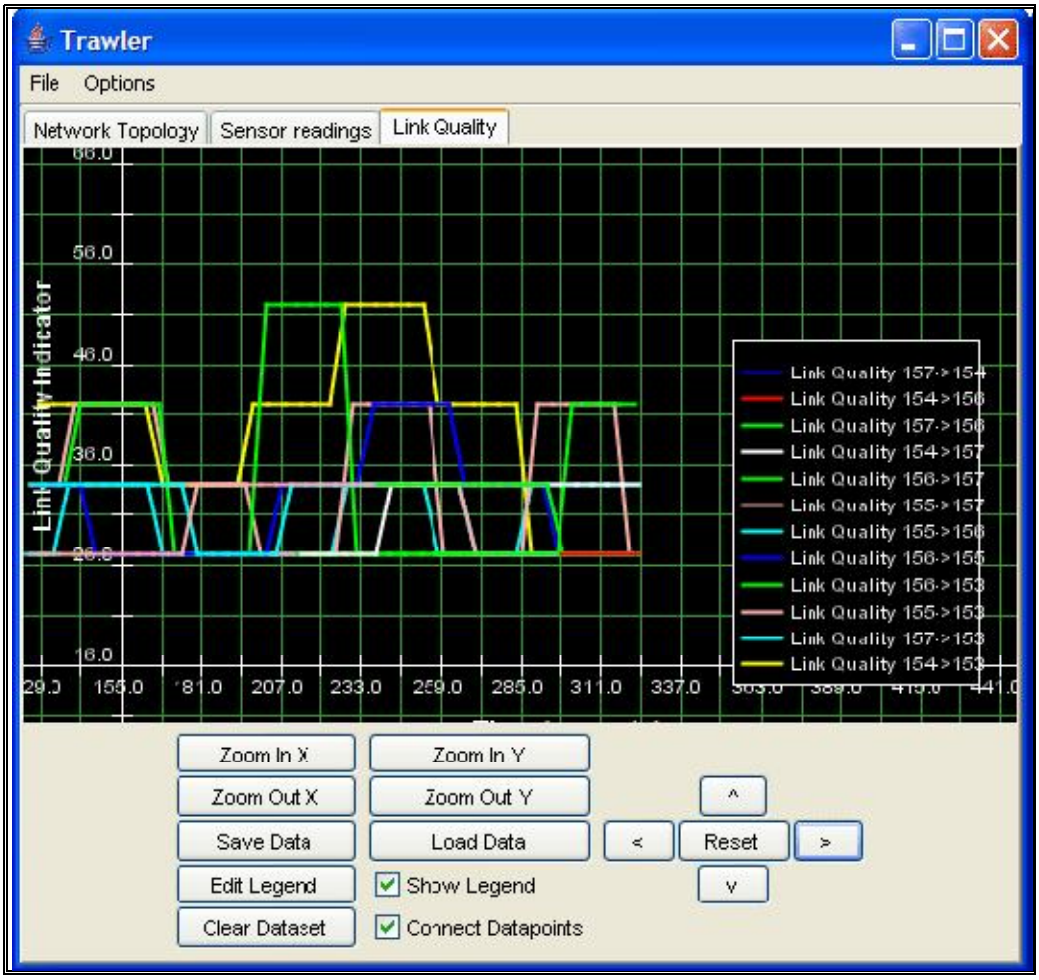
Όταν εκκινήσει ο Trawler, ξεκινά η διαδικασία δημιουργίας ενός ad-hoc mesh δικτύου του οποίου η τοπολογία παρουσιάζεται στην οθόνη. Πρέπει να περιμένουμε μερικά λεπτά για να εμφανιστεί ολόκληρο το δίκτυο και να εγκατασταθούν σταθερές

και αξιόπιστες διαδρομές από τους αισθητήρες προς τη συσκευή-αισθητήρα που είναι συνδεδεμένη στο PC.

Κάνοντας κλικ στο tab ‘Sensor readings’, ο Trawler μάς παρουσιάζει τις τιμές θερμοκρασίας που λαμβάνει από τους κόμβους του δικτύου (Σχήμα 52). Μπορούμε να κάνουμε zoom στα δεδομένα πιέζοντας τα αντίστοιχα πλήκτρα ή, χρησιμοποιώντας τα πλήκτρα κύλισης στο κάτω δεξιό μέρος της οθόνης, να μεταβούμε με κύλιση σε οποιοδήποτε σημείο. Ακόμη, με το ποντίκι μπορούμε να επιλέξουμε μία περιοχή στο γράφημα και μετά ο Trawler θα κάνει zoom στα επιλεγμένα δεδομένα.

Σχήμα 52. Δεδομένα των αισθητήρων.

Κάνοντας κλικ στο ‘Link Quality’ tab, μπορούμε να προσδιορίσουμε αν η ποιότητα της ζεύξης μεταξύ κόμβων είναι εξαιρετικά χαμηλή ώστε να χρειαστεί να μετακινήσουμε τον κόμβο ή να προσθέσουμε επιπλέον κόμβους στο δίκτυο που να συμμετάσχουν στο πλέγμα (Σχήμα 53).



Σχήμα 53. Επιπλέον εφαρμογές των αισθητήρων.

Μπορούμε, τέλος, να καταγράψουμε τις αναγνώσεις των δεδομένων σε ένα αρχείο κάνοντας απλά κλικ στο ‘Log Packets’ που θα το βρούμε στο sidebar ‘Visualization Controls’ και που είναι ανοιχτό, παράλληλα με τον Trawler.

Π.4 Tmote Sky Software

Το σύστημα επικοινωνίας της Moteiv περιλαμβάνει 3 μέρη: ένα multihop mesh πρωτόκολλο δικτύωσης, ένα κυκλικό πρωτόκολλο εργασιών δικτύωσης (μεταξύ καταστάσεων wake up και sleep) και το πρόσφατα προταθέν ‘Sensornet Protocol’ (SP), μία προσέγγιση για αποστολή και λήψη μηνυμάτων. Όλα τα προαναφερθέντα πρωτόκολλα χρησιμοποιούνται στην εφαρμογή πλεγματοειδούς δικτύωσης της Moteiv, τη Delta.

- Multihop δικτύωση

Η - κατόπιν αιτήσεως - ad-hoc δικτύωση της Moteiv χρησιμοποιεί τον χωρικό και χρονικό πλεονασμό για την αξιόπιστη μεταφορά μηνυμάτων διαμέσου ενός δικτύου προς τον προορισμό τους. Πρώτα πρέπει να συμπεριλάβουμε το multihop στις ρυθμίσεις των παραμέτρων:

components Multihop;

Κατόπιν συνδέουμε την εφαρμογή με τους κατάλληλους χειριστές για τον τύπο του μηνύματος. Για παράδειγμα:

AppM.Send -> Multihop.Send[APP_ID];
AppM.Receive -> Multihop.Receive[APP_ID];

όπου το APP_ID είναι ένα μοναδικό 8-bit αναγνωριστικό για τη συγκεκριμένη υπηρεσία ή εφαρμογή. Τα μηνύματα αποστέλλονται στη multihop υπηρεσία και μπαίνουν σε ουρά αναμονής μέχρι να υπάρξει η δυνατότητα δρομολόγησής τους προς τον προορισμό.

- Λειτουργία low power

Το software της Moteiv περιλαμβάνει ένα πρωτόκολλο συγχρονισμού για ασύρματη δικτύωση χαμηλής ισχύος. Δημιουργείται και συντηρείται μία προδιαγραφή, όπου ολόκληρο το δίκτυο 'αφυπνίζεται' μαζί και έπειτα επιστρέφει στη 'νάρκη'. Μπορούμε, με την εισαγωγή μιας μόνο παραμέτρου, να μεταπέσουμε σ' αυτή την κατάσταση και συγκεκριμένα χρησιμοποιώντας και την εφαρμογή Delta:

cd /opt/moteiv/apps/Delta
make tmoteinvent lowpower

Το εύρος ζώνης περιορίζεται κατά πολύ με αυτόν τον τρόπο λειτουργίας (κάθε κόμβος είναι ενεργός για λίγα μόνο milliseconds κάθε δύο seconds). Ο αρχικός συγχρονισμός του δικτύου μπορεί να χρειαστεί έως και 15 λεπτά για να σταθεροποιηθεί, αλλά θα μπορεί αξιόπιστα να διαχειριστεί δεδομένα μετά την αρχική αυτή φάση.

- Πρωτόκολλο Sensornet (SP)

Το SP είναι μια ενοποιημένη προσέγγιση για το 'τρέξιμο' πρωτοκόλλων δικτύου πάνω σε μια ποικιλία τεχνολογιών επιπέδου ζεύξης δεδομένων και φυσικού επιπέδου, χωρίς να απαιτείται αλλαγή στην υλοποίηση του πρωτοκόλλου δικτύου.

Π.5 Tmote Connect: Wireless Gateway Appliance Software

Με το Moteiv's Tmote Connect gateway software έχουμε πρόσβαση στους ασύρματους αισθητήρες μέσω του Ethernet. Το λογισμικό αυτό επιτρέπει σε ένα εξάρτημα (Linksys NSLU2 Network Attached Storage) να λειτουργεί σαν μια συσκευή-πύλη δικτύων (Σχήμα 54), συνδέοντας τους ασύρματους αισθητήρες Tmote με ένα ενσύρματο τοπικό δίκτυο περιοχής (LAN). Σε κάθε αισθητήρα που είναι συνδεδεμένος σε μια τέτοια συσκευή-πύλη, μπορεί να γίνει η διαχείρισή του εξ αποστάσεως μέσω ενός περιβάλλοντος επικοινωνίας χρήστη από τον ιστό (web-based). Το Tmote Connect συνεργάζεται γρήγορα και κατάλληλα με το TinyOS και παρέχει έλεγχο στους συνδεδεμένους από απόσταση αισθητήρες.

Σχήμα 54. Το Linksys NSLU2 της Tmote.

Το λογισμικό Tmote Connect περιλαμβάνει:

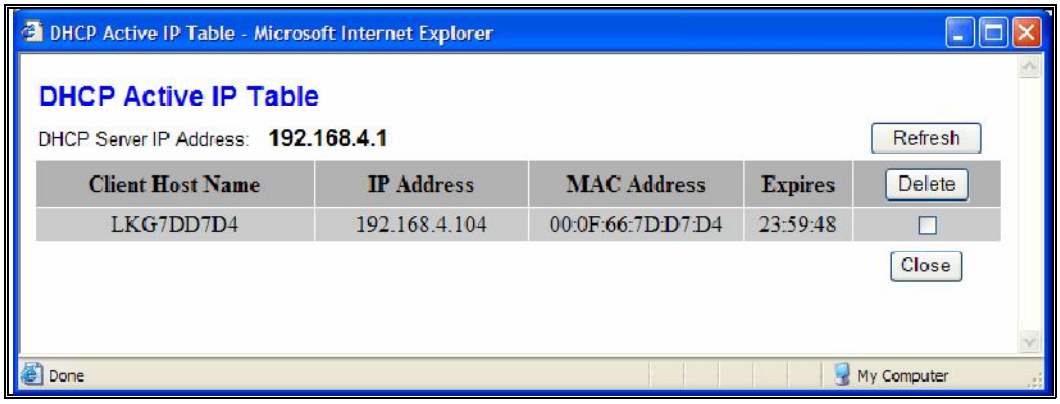
- Γεφύρωση (bridging) μεταξύ των ασύρματων δικτύων Tmote και της υποδομής Ethernet.
- Υποστήριξη μέχρι και σε δύο αισθητήρες ανά πύλη.

- Συνεκτικότητα διπλής κατεύθυνσης για μεταφορά δεδομένων από και προς τους αισθητήρες πάνω σε TCP/IP sockets.
- Άμεσος εκ νέου προγραμματισμός των αισθητήρων από απόσταση με χρήση standard in-system πρωτόκολλα προγραμματισμού.
- Συνεργασία με το TinyOS και τα εργαλεία του.
- Web-based περιβάλλον επικοινωνίας με αναγνώριση αισθητήρα, δυνατότητα reset και μετρητές επίδοσης.
- Λειτουργία σε δίκτυα με ή χωρίς υποστήριξη DHCP.
- Δυνατότητα ανανέωσης με νέες εκδόσεις λογισμικού από την Moteiv.

Στη συνέχεια θα δούμε πως εντάσσεται το Tmote Connect στο τοπικό μας δίκτυο. Το Tmote Connect είναι σχεδιασμένο να λειτουργεί τόσο με το DHCP, όσο και χωρίς αυτό. Το DHCP προτιμάται για όλες τις εγκαταστάσεις Tmote Connect, ενώ η λειτουργία χωρίς το DHCP είναι κατάλληλη για 'μικρές' εγκαταστάσεις σε ιδιωτικά δίκτυα.

Στη βάση της μονάδος υπάρχει η MAC address του Tmote Connect, που στη δική μας περίπτωση είναι η 00:0F:66:7D:D7:D4 και έτσι το αντίστοιχο hostname προκύπτει LKG7DD7D4. Συνδέουμε τη θύρα Ethernet του Tmote Connect με την έξοδο Ethernet, τον μεταγωγέα ή το hub, χρησιμοποιώντας το καλώδιο Ethernet που περικλείεται. Έπειτα συνδέουμε τους αισθητήρες Tmote Sky στις θύρες USB και όλη τη συσκευή με το ηλεκτρικό ρεύμα. Όταν συνδεθεί το καλώδιο, το Tmote Connect ενεργοποιείται αυτόματα, τρέχει ένα self test, μία διαδικασία εκκίνησης και βγάζει έναν ήχο όταν είναι έτοιμο για προσπέλαση. Τα αντίστοιχα LEDS των θυρών ανάβουν όταν είναι συνδεδεμένοι σε αυτές οι αισθητήρες.

Οι περισσότεροι DHCP servers, όπως και αυτή η συσκευή της Linksys, παρέχουν ένα mapping table με τη διεύθυνση IP και το hostname της συνδεδεμένης συσκευής Tmote Connect χρησιμοποιώντας τις MAC διευθύνσεις, όπως αυτός που φαίνεται στο Σχήμα 55:



Σχήμα 55. Ο πίνακας Διευθύνσεων IP της συνδεμένης συσκευής.

Το Tmote Connect μπορεί να προσπελαθεί μέσω ενός αριθμού διαδραστικών ή μη διαδραστικών διεπαφών. Μία webpage διεπαφή που τρέχει στην θύρα 80, επιτρέπει στον χρήστη να κάνει reset μεμονωμένα σε κάθε αισθητήρα, χωρίς να διακόψει ήδη εγκαταστημένες σειριακές συνδέσεις, να κάνει restart στα προγράμματα του server ή reboot στο Tmote Connect.

Ο κώδικας προγραμματισμού των motes εξαρτάται από το βοηθητικό πρόγραμμα netcat (nc), που είναι ευρέως διαθέσιμο στο σύστημα UNIX. Αφού έχουν εγκατασταθεί οι κανόνες προγραμματισμού, το Tmote Connect είναι έτοιμο για χρήση. Για να κάνουμε compile και εγκατάσταση μιας εφαρμογής σε ένα mote, πληκτρολογούμε:

make tmote reinstall,2 netbsl,192.168.4.104:10002

και έτσι θα εγκατασταθεί το πρόγραμμα που προορίζεται για τον mote με id 2 στο Tmote Connect στη διεύθυνση 192.168.4.104 στην USB θύρα 2. Οι αριθμοί θυρών 1 και 2 αντιστοιχούν στις θύρες 10001 και 10002 που χρησιμοποιούνται για να προγραμματίσουμε κάθε USB θύρα του Tmote Connect.

Όλες οι TinyOS εφαρμογές java ανακτούν τις πληροφορίες της σύνδεσης από μια μεταβλητή (environmental variable) που ονομάζεται MOTECOM. Για να συνδεθούμε και να ακούσουμε τα πακέτα που δημιουργήθηκαν από την εφαρμογή, πληκτρολογούμε:

MOTECOM=sf@192.168.4.104:9002 java net.tinyos.tools.Listen

Με αυτή τη σύνταξη μπορούμε γρήγορα να κάνουμε εναλλαγές μεταξύ διαφορετικών servers που χρησιμοποιούν το πρωτόκολλο Serial Forwarder.

Παραπομπές

[1] Perkins C. *Ad Hoc Networking.* Addilson-Wesley Reading, MA, 2000

[2] A Khalili and W.A. Arbaugh. *Security of Wireless Ad Hoc Networks*

[3] Chee-Yee Chong, S. P. Kumar *Sensor Networks: Evolution, Opportunities and Challenges,* Proceedings of IEEE, Vol. 91, No 8, August 2003.

[4] Shin-Lin Wu,Yu-Chee Tseng, *Wireless Ad-Hoc Networking,* Auerbach Publ.

[5] F. Akyildiz, W. Su, Y. Sankarasubramanian, and E. Cayirci *A Survey on Sensor Networks,* IEEE Communications Magazine,2002

[6] D. Djenouri, L. Khelladi. *A Survey of security issues in mobile ad hoc and sensor networks,* IEEE Communication Surveys*, 2005.*

[7] National Institute of Standards and Technology (NIST). *Wireless Ad Hoc Network Projects.* URL: http://w3.antd.nist.gov/wahn home.shtml.

[8] Lijun Liao. *Master Thesis: Group Key Agreement for Ad Hoc Networks.* Ruhr-University Bochum, Germany

[9] *The Official BlueTooth R Webseite*. URL: http://www.bluetooth.com/.

[10] IEEE 802.11. *The Working Group Setting the Standards for Wireless.* URL: http://grouper.ieee.org/groups/802/11/.

[11] C. R. Murthy and B. S. Manoj. *Ad Hoc Wireless Networks - Architectures and Protocols*. Person Education, 2004.

[12] Gwo-Jong Yu, Chih-Yung Chang. *An efficient cluster-based multi-channel management protocol for wireless Ad Hoc networks*. Department of Computer and Information Science, Aletheia University, Taiwan, Department of Computer Science and Information Engineering, Tamkang University, Taiwan, 2007 Elsevier

[13] Ada and C. Castelluccia. *Differentiation Mechanisms for IEEE 802.11.*IEEE INFOCOM'01, 2001.

[14] IEEE. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Spec.* IEEE 802.11 Standards, 1999.

[15] S. Mangold, S. Choi, P. May, O. Klein, G. Hiertz and L. Stibor. *IEEE 802.11e Wireless LAN for Quality of Service.* Proceedings of European Wireless, February 2002.

[16] *Sensor Networks and applications*, IEEE Proc., 8, Aug. 2003.

[17] A.J. Goldsmith and S.B. Wicker, *Design challenges for energy-constrained ad-hoc wireless networks,* IEEE Wireless Commun., 9, 8-27, Aug. 2002.

[18] C. Shen, C. Srisathapornphat, and C. Jaikaeo, *Sensor Information Networking Architecture and Applications,* IEEE Pers. Commun., Aug. 2001.

[19] G. Hoblos, M. Staroswiecki, and A. Aitouche, *Optimal Design of Fault Tolerant Sensor Networks,* IEEE Int'l Conf. Cont. Apps., Anchorage, AK, Sept. 2000.

[20] Bulusu et al., *Scalable Coordination for Wireless Sensor Networks: Self-Configuring Localization Systems,* ISCTA 2001, Ambleside, U.K., July 2001.

[21] G. J. Pottie and W. J. Kaiser, *Wireless Integrated Network Sensors,* Commun. ACM, vol. 43, no. 5, May 2000.

[22] J. M. Kahn, R. H. Katz and K. S. J. Pister, *Next Century Challenges: Mobile Networking for Smart Dust,* Proc. ACM MobiCom '99, Washington, DC, 1999.

[23] M. Ilyas and I. Mahgoub, *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*. 2005.

[24] Koushanfar F., Potkonjak M., and Sangiovanni-Vincentelli A. *Fault-tolerance techniques for sensor networks,* in Proc. IEEE Sensors, 49, 2002.

[25] Zhang H., et al., *A 1-V Heterogeneous reconfigurable processor IC for base band wireless applications,* in IEEE Int. Solid-State Circuits Conf. 2000.

[26] Slijepcevic S. and Potkonjak M. *Power efficient organization of wireless sensor networks,* in Proc. IEEE Int. Conf. Commun., 2001.

[27] Rabaey J.M. et al. *Pico Radio supports ad hoc ultra low power wireless networking,* Computer, 2000.

[28] Li Y., Potkonjak M. and Wolf M., *Real-time operating systems for embedded computing,* in Proc. Int. Conf. Computer Design, 1997.

[29] F. Ye, H. Luo, J. Cheng, S. Lu, and L. Zhang, *A Two-tier Data Dissemination Model for Large-scale Wireless Sensor Networks,* in Proc. of 8th Annual International Conf. on Mobile computing and networking. Atlanta, Georgia, USA: ACM Press, Sept. 2002.

[30] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, *Directed Diffusion for Wireless Sensor Networking,* IEEE/ACM Transactions on Networking, vol. 11, Feb. 2003.

[31] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, *LEACH: Energy-Efficient Communication Protocol for Wireless Microsensor Networks,* In Proceedings of Hawaii International Conference on System sciences, 2000.

[32] S. Lindsey and C. Raghavendra: *PEGASIS: Power-Efficient Gathering in Sensor Information Systems,* in International Conf. on Communications, 2001.

[33] C. E. Perkins and E. M. Royer, *Ad hoc On-Demand Distance Vector Routing,* In Proceedings of IEEE Workshop on Mobile Computing Systems and Applications, 1999.

[34] D. Braginsky and D. Estrin, *Rumor Routing Algorithm for Sensor Networks,* In Proceedings of ACM MobiCom, 2002.

[35] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, *Wireless sensor network: A survey,* Computer Networks, March 2002.

[36] A. Mainwaring, J Polastre, R. Szewczyk, D. Culler, and J. Anderson, *Wireless sensor networks for habitat monitoring,* ACM WSNA'02, Atlanta, Sept. 2002.

[37] M. D. Yarvis et al. *Real world experience with an interactive ad hoc sensor network,* Int. Conf. Parallel Processing Workshops (ICPPW'02),2002.

[38] D. Makhija, P. Kumaraswamy, R. Rajarshi, *Challenges and design of MAC protocol for underwater acoustic sensor networks,* IEEE, 2006.

[39] L. Zhou and Z. J. Haas*, Securing ad hoc networks.* IEEE Network, Nov/Dec 1999.

[40] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. Tygar. *SPINS: Security Protocols for Sensor Networks.* In 7th Annual ACM International Conference on Mobile Computing and Networks (Mobicom 2001) Rome, Italy, July 2001.

[41] W. Stallings, *Cryptography and Network Security Principles and Practices,* 3rd ed., Pearson Education Inc., 2003.

[42] S. Zhu, S. Setia and S. Jajodia, *LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks.* In the proceedings of the 10th ACM conference on computer communications security, 2003.
[43] http://www.xbow.com/wireless home.aspx, 2006.
[44] S. Gupte, M. Singhal, *Secure Routing in Mobile Wireless Ad Hoc Networks,* Ad Hoc Networks 1, 2003.
[45] A.D. Wood and J.A. Stankovic, *Denial of service in sensor networks,* Computer 35, 2002.
[46] CERT Coordination Center, *Smurf IP Denial-of-Service Attacks*, CERT Advisory CA-98, Jan. 1998.
[47] C.L. Schuba et. al., *Analysis of a Denial of Service Attack on TCP*, Proc. IEEE Symp. Security and Privacy, IEEE Press, 1997.
[48] J. Newsome, E. Shi, D. Shong and A. Perrig. *The Sybil attack in sensor networks: analysis & defenses.* In Proceedings of the third international symposium on Information processing in sensor networks, ACM Press, 2004.
[49] J. Douceur. *The Sybil attack.* In Proc. of the 1st International Workshop on Peer-to-Peer Systems (IPTPS'02) February 2002.
[50] C. Karlof and D. Wagner. *Secure routing in wireless sensor networks: Attacks and countermeasures.* In First IEEE International Workshop on Sensor Networks Protocols and Applications, May 2003.
[51] S. Madden, M. J. Franklin, J. M. Hellerstein and W. Hong. *TAG: A tiny aggregation service for ad hoc sensor networks.* In Symposium on Operating Systems Design and Implementation, Nov. 2002.
[52] J. Deng, R. Han and S. Mishra. *Countermeasures against traffic analysis in wireless sensor networks.* Technical Report CU-CS-987-04, University of Colorado at Boulder, 2004.
[53] B. Parno, A. Perrig and V. Gligor. *Distributed detection of node replication attacks in sensor network.* In Proceedings of IEEE Symposium on Security and Privacy, May 2005.
[54] M. Gruteser, G. Schelle, A. Jain, R. Han and D. Grunwald. *Privacy-aware location sensor networks.* In 9th USENIX Workshop on Hot Topics in Operating Systems (HotOS IX), 2003.
[55] H. Chan and A. Perrig. *Security and privacy in sensor networks.* IEEE Computer Magazine, 2003.
[56] X. Wang, W. Gu, K. Schosek, S. Chellappan and D. Xuan. *Sensor network configuration under physical attacks.* Technical Report (OSU-CISRC-7/04-TR45) Dept. of Computer Science and Engineering, the Ohio-State University, July 2004.
[57] S. Duri, M. Gruteser, X. Liu, P. Moskowitz, R. Perez, M. Singh and J. Tang. *Framework for security and privacy in automotive telematics.* In 2nd ACM International Workshop on Mobile Commerce, 2000.
[58] Yih-Chun Hu, A. Perrig and D. B. Johnson. *Wormhole attacks in wireless networks.* 2002.
[59] Nikos Komninos, Dimitris Vergados, Christos Douligeris. *Layered security design for mobile ad hoc networks*, 2005, p.123-124
[60] Komninos N. *Security architecture for future communication systems*. PhD thesis, Lancaster University, 2003

[61] Kyasanur P, Vaidya N. *Detection and handling of MAC layer misbehavior in wireless networks.* In: International conference on dependable systems and networks (DSN'03). San Francisco, California, 2003.
[62] Borisov N, Goldberg I, Wagner D. *Intercepting mobile communications: the insecurity of 802.11.* In: ACM MOBICON, 2001.
[63] Stubblefield A, Ioannidis J, Rubin A. *Using the Fluhrer, Martin, and Shamir attack to break WEP*. In: NDSS, 2002.
[64] Dahill B, Sanzgiri K, Levine BN, Shields C, Belding-Royer EM. *A secure routing protocol for ad hoc networks*. In: IEEE ICNP, 2002.
[65] Royer EM, Toh C-K. *A review of current routing protocols for adhoc mobile wireless networks,* IEEE Personal Communications Magazine 1999.
[66] Schneier B. *Secret and lies, digital security in a networked world*. Wiley, 2000.
[67] Papadimitratos P, Haas ZJ. *Secure routing for mobile ad hoc networks*. In SCS communication networks and distributed systems modelling and simulation conference (CNDS 2002). San Antonio, 2002.
[68] Hubaux J, Buttya´n L, Capkun S. *The quest for security in mobile ad hoc networks.* In Proceedings of the second ACM international symposium on mobile ad hoc networking and computing. USA, 2001.
[69] Hu Y, Perrig A, Johnson D. *Ariadne: a secure on-demand routing protocol for ad hoc networks.* In ACM WiSe, 2002a
[70] Hu Y, Johnson D, Perrig A. *Sead: secure efficient distance vector routing for mobile wireless ad hoc networks.* In IEEE WMCSA, 2002c
[71] R. Heady et al. *The Architecture of a Network Level Intrusion Detection System.* Computer Science Department, University of New Mexico, Tech. Rep., Aug. 1990.
[72] Y. H. W. Lee. *A Cooperative Intrusion Detection System for Ad Hoc Networks.* 1st ACM Wksp. Security of Ad Hoc and Sensor Networks, Fairfax, Virginia, USA, 2003.
[73] Y. Zhang, W. Lee, and Y. Huang. *Intrusion Detection Techniques for Mobile Wireless Networks.* ACM Wireless Networks, vol. 9, no. 5, Sept. 2003.
[74] Ramanujan, Kudige, Takkella, Nguyen, Adelstein, *Intrusion-Resistant Ad Hoc Wireless Networks* .Architecture Technology Corporation, Minneapolis, Minnesota.
[75] Ping Yi, Zhoulin Dai, Yiping Zhong, Shiyong Zhang. *Resisting Flooding Attacks in Ad Hoc Networks,* Department of Computing and Information Technology, Fudan University, Shanghai, China.
[76] S. Yi, R Naldurg, and R. Kravets. *Security-aware Ad-hoc routing for Wireless Networks.* ACM Wksp. Mobile Ad Hoc Networks, Mobihoc, 2001.
[77] Y.-C. Hu, A. Perrig, and D. B. Johnson. *Rushing Attacks and Defences in Wireless Ad Hoc Network Routing Protocols.* ACM Wksp. Wireless Security WiSe 2003, San Diego, CA, USA, Sept. 2003.
[78] S. Marti *et al. Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks.* ACM Mobile Comp. and Net. MOBICOM 2000.
[79] H. Yang, X. Meng, and S. Lu. *Self-organized Network Layer Security in Mobile Ad Hoc Networks.* ACM MOBICOM Wireless Security Wksp (WiSe'02), Sept. 2002.

[80] P. Michiardi and R. Molva. *Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks.* Commun. and Multimedia Security 2002 Conf., Portoroz, Slovenia, Sept. 26–27 2002.

[81] S. Buchegger and J.-Y. Le-Boudec. *A Robust Reputation System for p2p and Mobile Ad-hoc Networks.* 2nd Wksp. Economics of Peer-to-Peer Systems, June 2004.

[82] L. Buttyan and J. Hubaux. *Stimulating Cooperation in Selforganizing Mobile Ad Hoc Networks.* ACM/Kluwer Mobile Networks and Applications, vol. 8, no. 5, Oct. 2003.

[83] H. Chan and A. Perrig. *Pike: Peer intermediaries for key establishment in sensor networks.* In IEEE Infocom 2005.

[84] Q. Huang, J. Cukier, H. Kobayashi, B. Liu and J. Shang. *Fast authenticated key establishment protocols for self-organizing sensor networks.* In Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications, ACM Press, 2003.

[85] P. Kotzanikolaou, E. Magkos, C. Douligeris and V. Chrissikopoulos. *Hybrid Key Establishment for Multiphase Self-Organized Sensor Networks.* In Proceedings of the first IEEE international workshop on trust, security and privacy for ubiquitous computing, 2005.

[86] Certicom Research. *Standard for efficient cryptography, SEC1: EC Cryptography.* Ver. 1.0, 2000.

[87] Roshan Duraisamy, Zoran Salcic, Miguel Morales-Sandoval and Claudia Feregrino-Uribe. *A fast elliptic curve based key agreement protocol-on-chip (PoC) for securing networked embedded systems.*

[88] Dutertre, B., Cheung, S., and Levy, J. *Lightweight Key Management in Wireless Sensor Networks by Leveraging Initial Trust.* TR SRI-SDL-04-02, April 2004.

[89] Kotzanikolaou, P., Vergados D., Stergiou G., and Magkos E. *Multi-Layer Key Establishment for Large Scale Sensor Networks.* Int. J. Security and Networks, Vol. 1, Nos. 1/2/3. 2005.

[90] A. Mishra, K. Nadkarni and A. Patcha. *Intrusion detection in wireless ad hoc networks.* IEEE Personal Communications 11, 2004.

[91] D. Watkins and C. Scott. *Methodology for evaluating the effectiveness of intrusion detection in tactical mobile ad hoc networks.* In IEEE Wireless Communications and Networking Conference (WCNC). March 2004.

[92] N. Komninos, D Vergados and C. Douligeris. *Detecting unauthorized and compromised nodes in mobile ad hoc networks.* Ad Hoc Networks 5. 2007.

[93] B. Dahill, B. N. Levine, E. Royer, C. Shields. *ARAN: A secure routing protocol for ad hoc networks.* UMass Tech Report, 2002.

[94] C. E. Perkins, P. Bhagwat. *Highly Dynamic Destination Sequence Distance Vector Routing (DSDV) for Mobile Computers.* In proceedings of SIGCOMM 1994.

[95] L. Liao and M. Manulis. *Tree-based Group Key Agreement Framework for Mobile Ad-Hoc Networks.* In Proceedings of the 20th IEEE International Conference on Advanced Information Networking and Applications (AINA 2006) Vienna Austria.

[96] S. Olariu and Q. Xu, *Information Assurance in Wireless Sensor Networks.* In Proceedings of the 19th IEEE IPDPS' 05.

[97] A. J. Menezes, P.C. van Oorschot and S.A. Vanstone. *Handbook of Applied Cryptography,* CRC Press, Boca Raton, FL, 1997.

[98] C. Kaufman, R. Perlman and M. Speciner. *Network Security: Private Communication in a Public World.* Prentice Hall, Englewood Cliffs, NJ, 1995.

[99] Y. Desmedt. *Threshold Cryptography.* European Transactions on Telecommunications. July-August, 1994.

[100] A. S. Wander, N. Gura and H. Eberle. *Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks.* In Proc. Of the 3rd IEEE International Conference on Pervasive Computing and Communication (PERCOM), 2005.

[101] A. Bharathidasan and V. A. S. Ponduru. *Sensor Networks: An Overview.*

[102] J. Hightower and G. Borriello. *Location Systems for Ubiquitous Computing.* IEEE Computer, 2001.

[103] J. Hightower and G. Borriello. *A Survey and Taxonomy of Location Systems for Ubiquitous Computing.* Technical Report UW-CSE 01-08-03. University of Washington. Computer Science and Engineering Seattle. WA. August 2001.

[104] P. Bahl and V. N. Padmanabhan. *RADAR: An In-Building RF-Based User Location and Tracking System.* In Proceedings of the IEEE INFOCOM, Tel-Aviv, Israel, April 2000.

[105] H. Karl and A. Willig, *Protocols and Architectures for Wireless Sensor Networks.* 2005.

[106] R. Want, A. Hopper, V. Falao and J. Gibbons. *The Active Badge Location System.* ACM Transactions on Information Systems. 1992.

[107] A. Ward, A. Jones and A. Hopper. *A New Location Technique for the Active Office.* IEEE Personal Communications. 1997.

[108] N. B. Priyantha, A. Chakraborty and H. Balakrishnan. *The Cricket Location-Support System.* In Proceedings of the 6th International Conference on Mobile Computing and Networking (ACM Mobicom) Boston, MA, 2000.

[109] N. Bulusu, J. Heidemann and D. Estrin. *GPS-Less Low Cost Outdoor Localization for very small devices.* IEEE Personal Communications Magazine, 2000.

[110] L. Doherty, L. El. Ghaoui and K. S. J. Pister. *Convex Position Estimation in Wireless Sensor Networks.* In Proceedings of the IEEE INFOCOM, Anchorage, AK, 2001.

[111]A. Savvides, C.-C. Han and M. Srivastava. *Dynamic Fine-Grained Localization in Ad-Hoc Networks of Sensors.* Proceedings of the 7th Annual International Conference on Mobile Computing and Networking. ACM press, Rome, July 2001.

[112] V. Ramadurai and M. L. Sichitiu. *Localization in Wireless Sensor Networks: A Probabilistic Approach.* In Proceedings of 2003 International Conference on Wireless Networks (ICWN 2003), Law Vegas, June 2003.

[113] J. Bound, M. Carney, C. Perkins and R. Droms. *Dynamic host configuration protocol for IPv6 (DHCPv6).* Internet draft, June 2001.

[114] C. E. Perkins, J. T. Malinen, R. Wakikawa, E. M. Belding-Royer and Y. Sun. *IP address auto configuration for ad hoc networks.* Internet draft, Nov. 2001.

[115] G. Andreadis. *Providing internet access to mobile ad hoc networks.*

[116] R. Wakikawa, J.T. Malinen, C. E. Perkins, A. Nilsson and A. J. Tuominen. *Global connectivity for IPv6 mobile ad hoc networks.* Internet Draft, Nov. 2001.
[117] P. Brutch and C. Ko. *Challenges in intrusion detection for wireless ad-hoc networks.* In 2003 Symposium in Applications and Internet Workshops (SAINT'03), 2003.
[118] P. Albers, O. Camp, J. Pecher, B. Jouga, L.M. and R. Puttini. *Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches.* Proceedings of the 1st International Workshop on Wireless Information Systems (WIS-2002), April 2002.
[119] S. Buchegger and j. Le Boudec. *Performance Analysis of the CONFIDANT (Cooperation Of Nodes-Fairness In Dynamic Ad-hoc NeTworks).* Proceedings of the 3rd ACM International Symposium on MANET and Computing (MobiHoc'02), June 2002.
[120] S. Bansal and M. Baker *Observation-Based Cooperation Enforcement in Ad hoc Networks.* Research Report cs.NI/0307012, Stanford University, 2003.
[121] Y. Xiao, X. Shen and D.-Z. Du. *Wireless/Mobile Network Security.* Chapter 7. 2006.
[122] J. D. McLurkin. *Algorithms for distributed sensor networks.* 1999.
[123] S. Sahni and X. Xu. *Algorithms for wireless sensor networks.* September 2004.
[124] K. Kar and S. Banerjee. *Node placement for connected coverage in sensor networks.* Proc WiOpt 2003: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks. 2003.
[125] M. Carei and D. Du, *Improving wireless sensor network lifetime through power aware organization.* ACM Wireless Networks.
[126] F. Ye, G. Zhong, S. Lu and L. Zhang. *Energy efficient robust sensing coverage in large sensor networks.* Technical Report, UCLA, 2002.
[127] H. Zhang and J. Hou. *Maintaining sensing coverage and connectivity in large sensor networks.* Technical Report UIUC, UIUCDCS-R-2003-2351. 2003
[128] F. Ye, G. Zhong, S. Lu and L. *A Robust energy conserving protocol for long-lived sensor networks.* 23rd ICDCS. 2003.
[129] Y. Xu, J. Heidemann and E. Estrin. *Geography-informed energy conservation for ad hoc routing.* MOBICOM. 2001.
[130] X. Wang. *Integrated coverage and connectivity configuration in wireless sensor networks.* SenSys. 2003.
[131] R. Kannan and S. S. Iyengar. *Game-theoretic models for reliable, path-length and energy-constrained routing in wireless sensor networks.* IEEE Journal on Selected Areas in Communications. 2004.
[132] S. Singh, M. Woo and C. Raghavendra. *Power-aware routing in mobile ad hoc networks.* ACM/IEEE MOBICOM. 1998.
[133] J. Aslam, Q. Li and R. Rus. *Three power-aware routing algorithms for sensor networks.* Wireless Communications and Mobile Computing. 2003.
[134] K. Kar, M. Kodialam, T. Lakshman and L. Tassiulas. *Routing for network capacity maximization in energy-constrained ad hoc networks.* IEEE INFOCOM. 2003.

[135] A. Misra and S. Banerjee. *MRPC: Maximizing network lifetime for reliable routing in wireless.* IEEE Wireless Communications and Networking Conference (WCNC). 2002.

[136] J. Wieselthier, G. Nguyen and A. Ephremides. *On the construction of energy-efficient broadcasting and multicast trees in wireless networks.* IEEE INFOCOM. 2000.

[137] S. Sahni. *Data structures, algorithms and applications in Java.*2nd Edition, Silicon Press, NJ, 2005.

[138] C. Florens and R. McEliece. *Scheduling algorithms for wireless ad-hoc sensor networks.* IEEE GLOBECOM. 2002.

[139] C. Florens and R. McEliece. *Packets distribution algorithms for sensor networks.* INFOCOM 2003.

[140] R. Brooks and S. Iyengar. *Robust distributed computing and sensing algorithm.* IEEE Computer, June. 1996.

[141] N. Aboudagga, M. T. Refai, M. Eltoweissy, L.A. DaSilva and J.Quisquater. *Authentication Protocols for Ad Hoc Networks: Taxonomy and Research Issues.* MSWiM'05, October 2005.

[142] A. Fiat and A. Shamir. *How to prove yourself: Practical solutions to identification and signature problems.* In Proceedings on Advances in Cryptology-CRYPTO'86. 1986.

[143] N. Komninos, D. D. Vergados and C. Douligeris. *Multifold node authentication in mobile ad hoc networks.* Int. J. Commun. Syst. December 2005.

[144] A. Perrig, R. Canneti, D. Tygar and D. Song. *The TESLA Broadcast Authentication Protocol.* Technical Report 2, RSA Laboratories, 2002.

[145] R. Anderson, F. Bergadano, B. Crispo, J.-H. Lee, C. Manifavas and R. Needham. *A new family of authentication protocols.* In ACM Operating Systems Review, 1998.

[146] S. Zhu, S. Xu, S. Setia and S. Jajodia. *LHAP: A lightweight hop-by-hop authentication protocol for ad hoc networks.* In Proc. Of ICDS 2003 International Workshop on Mobile and Wireless Network (MWN), May 2003.

[147] J. Binder and H-P. Bischof. *Zero knowledge proofs of identity for ad hoc wireless networks.* 2003.

[148] A. A. Pirzada and C. McDonald. *Kerberos Assisted Authentication in Mobile Ad Hoc Networks.* Proceedings of the 27th conference on Australasian computer science.

[149] Y.-C. Hu, A. Perrig and D. B. Johnson. *Packet Leashes: A defense against wormhole attacks in wireless ad hoc networks.* 22nd Annual Joint Conf. IEEE Comp. and Commun. Societies (INFOCOM 2003), Apr. 2003.

[150] B. Awerbuch. *An On Demand Secure Routing Protocol Resilient to Byzantine Failures.* ACM Wrksp. Wireless Security (WiSe) Atlanta, 2002.

[151] M. Burmester and Y. Desmedt. *Secure communication in an unknown network using certificates.* In Advances in Cryptography-Asiacrypt '99. LNCS 1999.

[152] J. Marshall, V. Thakur and A. Yasinsac. *Identifying flaws in the secure routing protocol.* In Proceedings of the 22nd International Performance, Computing and Communications Conference, Apr. 2003.

[153] K. Wu and J. Harms. *On-Demand multipath routing for mobile ad hoc networks.* EPMCC'01, Vienna Feb. 2001.

[154] R. Mavropodi and C. Douligeris. *Multipath Routing Protocols for Mobile Ad Hoc Networks: Security Issues and Performance Evaluation.* IST FET Coordination Action ACCA. 2006.

[155] M. Burmester and T. van Lee. *Secure multipath communication in mobile ad hoc networks.* Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC 2004), IEEE, April 2004.

[156] P. Kotzanikolaou, R. Mavropodi and C. Douligeris. *Secure multipath routing for mobile ad hoc networks.* Proceedings of the WONSS'05 Conference (St. Moritz, Switzerland), IEEE, January 2005.

[157] C. Intanagonwiwat, R. Gonvindan and D. Estrin. *Directed Diffusion: a Scalable and Robust Communication Paradigm for Sensor Networks.* Proc. ACM Mobicom 2000.

[158] D. Ganesan. *Highly Resilient, Energy-Efficient Multipath Routing in Wireless Sensor Networks.* ACM SIGMOBILE Mobile Comp. Commun. Rev. 2001.

[159] J. Wu. *An extended dynamic source routing scheme in ad hoc wireless networks.* In Proceedings of the 35th Hawaii International Conference on System Sciences.

[160] M. K. Marina and S. R. Das. *On-demand Multipath Distance Vector Routing in Ad Hoc Networks.* IEEE 2001.

[161] Dr Carlo Kopp. *Ad Hoc Networking NCW101 part 4*.

[162] Q. Zhao, A. Swami and L. Tong, *The interplay between signal processing and networking in sensor networks,* IEEE Signal Processing Magazine, July 2006.

[163] J. Kong et al., *Wirel. Commun. Mob. Comput. 2002; **2**:533–547*, John Wiley & Sons, Ltd.

[164] G. Simon, A. Ledeczi, and M. Maroti, "*Sensor network-based countersniper system,"* in *Proc. SenSys*, Nov. 2004.

[165] Gu DL, Pei G, Ly H, Gerla M, Hong X. *Hierarchical routing for multi-layer ad-hoc wireless networks with UAVs.* In *IEEE MILCOM*, 2000.