ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών
Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών

Ειδίκευση Δικτύων Επικοινωνιών και Κατανεμημένων Συστημάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ζητήματα Ασφάλειας στα Ασύρματα Δίκτυα Αισθητήρων

Διονύσιος Π. Κυριακάκης
Α.Μ. 18040

Εισηγητής: Βασίλειος Μάμαλης, Καθηγητής

Vasileios Mamalis
Digitally signed by Vasileios Mamalis
Date: 2021.03.30 12:00:57 +03'00'

Ζητήματα Ασφάλειας στα Ασύρματα Δίκτυα Αισθητήρων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ζητήματα Ασφάλειας στα Ασύρματα Δίκτυα Αισθητήρων

Διονύσιος Π. Κυριακάκης
Α.Μ. 18040

Εισηγητής:

Βασίλειος Μάμαλης, Καθηγητής

Εξεταστική Επιτροπή:

Βασίλειος Μάμαλης, Καθηγητής

Γραμματή Πάντζιου, Καθηγήτρια

Ιωάννα Καντζάβελου, Επίκουρη Καθηγήτρια

Ημερομηνία εξέτασης 17/3/2021

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Κυριακάκης Διονύσιος του Παναγιώτη, με αριθμό μητρώου 18040 φοιτητής του Προγράμματος Μεταπτυχιακών Σπουδών Επιστήμη και τεχνολογία της πληροφορικής και των υπολογιστών του Τμήματος Μηχανικών πληροφορικής και υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

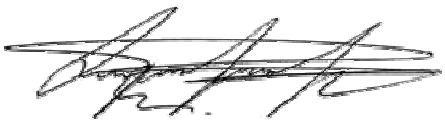
«Είμαι συγγραφέας αυτής της μεταπτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Επιθυμώ την απαγόρευση πρόσβασης στο πλήρες κείμενο της εργασίας μου μέχρι και έπειτα από αίτηση μου στη Βιβλιοθήκη και έγκριση του επιβλέποντα καθηγητή.

-Ο- Δηλών

Κυριακάκης Διονύσιος



ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να εκφράσω τις ευχαριστίες μου, πρωτίστως στον επιβλέποντα της εργασίας, καθηγητή κύριο Βασίλειο Μάμαλη, για τη δυνατότητα που μου έδωσε προκειμένου να ασχοληθώ με το συγκεκριμένο αντικείμενο ώστε να ανακαλύψω το επιστημονικό ενδιαφέρον που παρουσιάζει όπως επίσης για την υποστήριξη και καθοδήγησή του.

Επίσης θα ήθελα να ευχαριστήσω την οικογένειά μου, η οποία με στήριξε και μου συμπαραστάθηκε με τον καλύτερο δυνατό τρόπο και ειδικά την γυναίκα μου για την παρότρυνση, την υπομονή και την κατανόηση που έδειξε καθ' όλη τη διάρκειά εκπόνησης της εργασίας.

ΠΕΡΙΛΗΨΗ

Τα ασύρματα δίκτυα αισθητήρων (Wireless Sensor Networks – WSN's) αποτελούν δικτυακές υποδομές συγκροτούμενες από έναν μεγάλο αριθμό και χαμηλού κόστους αισθητήριους κόμβους. Ανάλογα με το περιβάλλον εφαρμογής αυτοί οι κόμβοι αναπτύσσονται στη περιοχή ενδιαφέροντος έχοντας αποστολή την ανίχνευση, παρακολούθηση και καταγραφή των συμβάντων στην εν λόγω περιοχή. Οι κόμβοι διοχετεύουν τη συλλεγόμενη από τους αισθητήρες πληροφορία και την δρομολογούν με τεχνική πολλαπλών αλμάτων μέσω των κόμβων που συνθέτουν το δίκτυο, προς το σταθμό βάσης όπου γίνεται η συλλογή, η επεξεργασία, η ανάλυση και η παρουσίαση των δεδομένων μέτρησης.

Οι κόμβοι σε ένα δίκτυο WSN έχουν σοβαρούς περιορισμούς σε ζητήματα υπολογιστικών, αποθηκευτικών και ενεργειακών πόρων. Αυτοί οι περιορισμοί σε συνδυασμό με το ασύρματο μέσο μετάδοσης και την απομακρυσμένη και χωρίς δυνατότητα επιτήρησης λειτουργία του δικτύου, καθιστούν τα WSN's ευάλωτα σε επιθέσεις. Οι επιθέσεις αυτές θέτουν υπο αμφισβήτηση τις απαιτήσεις ασφάλειας, στοχεύοντας στις λειτουργίες του δικτύου βάσει της πολυεπίπεδης αρχιτεκτονικής των WSN's. Οι πιο κρίσιμες επιθέσεις είναι οι άρνησης εξυπηρέτησης (DoS), επιθέσεις ανάλυσης κίνησης, κατά του απορρήτου, φυσικές και επιθέσεις αναπαραγωγής κόμβου. Για τον λόγο αυτό έχουν αναπτυχθεί μηχανισμοί ασφάλειας, πρωτόκολλα ασφαλούς δρομολόγησης καθώς και μηχανισμοί κρυπτογράφησης για την ανίχνευση και καταστολή των επιθέσεων, την ασφαλή δρομολόγηση και την προστασία του απορρήτου.

Λέξεις κλειδιά: << αισθητήριοι κόμβοι, σταθμός βάσης, αρχιτεκτονική WSN, απαιτήσεις ασφάλειας, επιθέσεις ασφάλειας, κρυπτογράφηση, ασφαλής δρομολόγηση, μηχανισμός ασφάλειας >>

ABSTRACT

Wireless sensor networks (WSN's) are network structures composed of a large number of low cost sensor nodes. Depending on the application environment, these nodes are deployed in the area of interest with the mission of detecting, monitoring and recording events in that area. The nodes delever the information collected by the sensors with multi-hop routing technique through the nodes that compose the network to the base station where the measurement data can be collected, processed, analyzed and presented.

Nodes in a WSN network have severe limitations on computing, storage, and energy resources. These limitations, combined with wireless transmission medium and the remote function without human surveillance of network operation, make WSN's vulnerable to attacks. These attacks dispute security requirements, targeting network operations based on WSN's multilevel architecture. The most crucial attacks are DoS (Denial of Service) attacks, traffic analysis, against privacy, physical and node replication attacks. Therefore, security mechanisms, secure routing protocols and encryption mechanisms have been developed for detecting and suppressing attacks, secure routing and protection of privacy.

Key words: << sensor nodes, base station, WSN architecture, security requirements, security attacks, cryptography, secure routing, security mechanism >>

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

WSNs Wireless Sensor Networks

ΚΕΦΑΛΑΙΟ 1

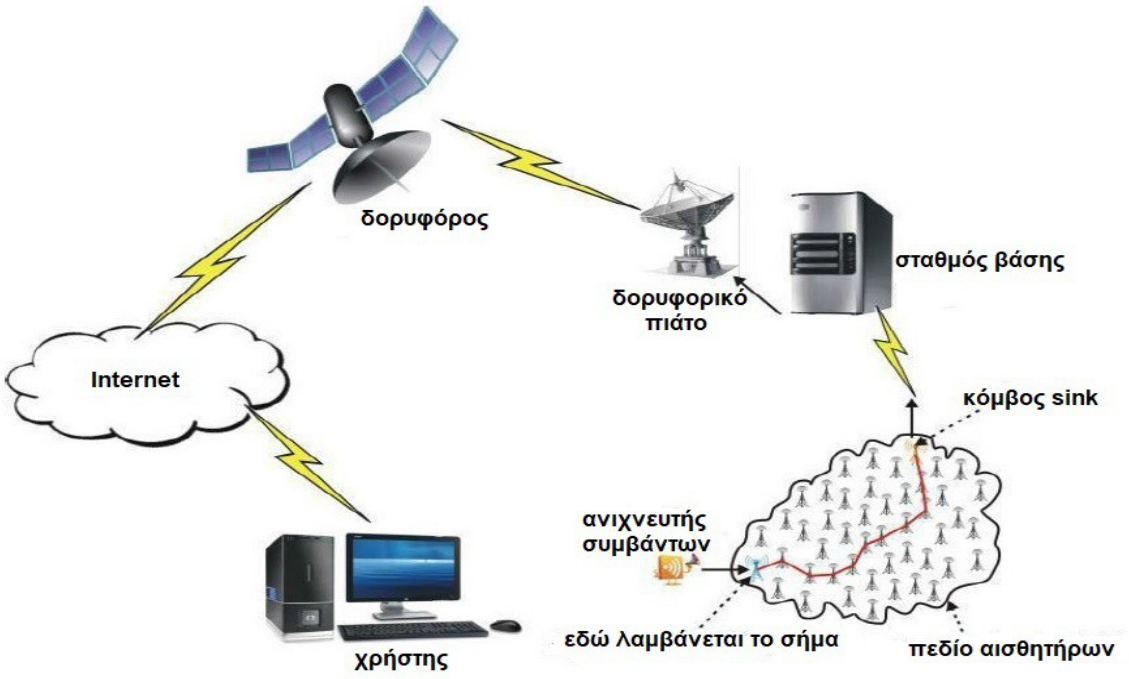
1.1 Εισαγωγή

Ένα Ασύρματο Δίκτυο Αισθητήρων (WSN) είναι το σύνολο από μερικές εκατοντάδες έως μερικές χιλιάδες κατανεμημένους στο χώρο αισθητήριους κόμβους (nodes) οι οποίοι συνδέονται με αισθητήρες που ποικίλουν ανάλογα με τη κύμανση του φυσικού μεγεθους που θέλουν ν' ανιχνεύσουν και συνεργατικά μέσω του δικτύου μεταφέρουν τα αποτελέσματα των μετρήσεων σε μια συγκεκριμένη τοποθεσία χωρίς τη χρήση καλωδίων.

Το ερώτημα που γενιέται είναι γιατί να έχουμε ένα δίκτυο αισθητήρων; Γιατι να μην αφήσουμε μεμονωμένους τους αισθητήρες; Η απάντηση είναι ότι έχουμε πολλά ωφέλη με τους αισθητήρες διασυνδεδεμένους σε ένα δίκτυο. Τα πιο *σημαντικά ωφέλη* είναι ότι μπορούν να καλύψουν περισσότερες περιοχές, πιο ευρείας κλίμακας περιοχές ενδιαφέροντος. Επίσης παρέχουν μεγαλύτερη ακρίβεια καθώς συνδυάζουν τα αποτελέσματα των μετρήσεων τους αλλά παρέχουν και μεγαλύτερη αξιοπιστία καθώς είναι εύκολα ανιχνεύσιμος ο εντοπισμός και η απομόνωση του ελαττωματικού κόμβου. Τέλος, δεν αποτελούν απλά ένα παθητικό σύστημα δηλαδή μόνο να ανιχνεύει και να στέλνει κάποιες τιμές. Μπορεί παράλληλα να εντολοδοτείται, να έχει διαδραστικότητα προκειμένου να επικοινωνούν οι κόμβοι μεταξύ τους, σχηματίζοντας έτσι μια αναπτυγμένη μορφή ευφυΐας [17].

Ένα Ασύρματο Δίκτυο Αισθητήρων (Wireless Sensor Network - WSN) αποτελείται λοιπόν από διασκορπισμένες αυτόνομες συσκευές που χρησιμοποιούν αισθητήρες για την παρακολούθηση φυσικών ή περιβαλλοντικών συνθηκών. Αυτές οι αυτόνομες συσκευές ή κόμβοι όπως αλλιώς ονομάζονται, συνδυάζονται με δρομολογητές για τη δημιουργία ενός τυπικού συστήματος WSN.

Οι κόμβοι επικοινωνούν ασύρματα με μία προεπιλεγμένη πύλη η οποία παρέχει σύνδεση με τον ενσύρματο κόσμο όπου μπορεί να γίνει η συλλογή, η επεξεργασία, η ανάλυση και η παρουσίαση των δεδομένων μέτρησης [22]. Στην εικόνα 1.1 απεικονίζεται ένα κλασσικό παράδειγμα Ασύρματου Δικτύου Αισθητήρων [23].



Εικόνα 1.1: Ένα κλασικό παράδειγμα Ασύρματου Δικτύου Αισθητήρων

- *Πεδίο αισθητήρων:* Μπορεί να θεωρηθεί ως η περιοχή στην οποία είναι τοποθετημένοι οι κόμβοι
- *Αισθητήριοι κόμβοι:* Αποτελούν την καρδιά του δικτύου. Είναι υπεύθυνοι για τη συλλογή και τη δρομολόγηση των δεδομένων προς τον sink κόμβο. Οι αισθητήριοι κόμβοι είναι έξυπνοι για να παρατηρήσουν μια εκτεταμένη ποικιλομορφία περιπτώσεων που περιλαμβάνουν ροή, θερμοκρασία, πίεση, υγρασία, επίπεδα θορύβου, μηχανική πίεση, ταχύτητα κ.ά.

- *Sink κόμβος:* Είναι ένας αισθητήριος κόμβος ο οποίος αναλαμβάνει να φέρει εις πέρας την διαδικασία της λήψης, επεξεργασίας και αποθήκευσης των δεδομένων απο τους υπόλοιπους αισθητήριους κόμβους του πεδίου. Χρησιμεύουν στη μείωση του συνολικού αριθμού μηνυμάτων που πρέπει να σταλούν μειώνοντας μ αυτό τον τρόπο την κατανάλωση ενέργειας στο δίκτυο. Ο κόμβος που θα αναλάβει να υποδυθεί τον ρόλο του sink κόμβου επιλέγεται δυναμικά από το δίκτυο.
- *Σταθμός Βάσης:* Είναι ένα κεντρικό σημείο ελέγχου εντός του ασύρματου δικτύου αισθητήρων, το οποίο εξάγει πληροφορίες από το δίκτυο και διαδίδει τις πληροφορίες ελέγχου πίσω σε αυτό. Χρησιμεύει επίσης ως πύλη προς άλλα δίκτυα, ένα ισχυρό κέντρο επεξεργασίας και αποθήκευσης δεδομένων καθώς και ένα σημείο πρόσβασης για ανθρώπινη διεπαφή. Ο σταθμός βάσης μπορεί να είναι είτε φορητός υπολογιστής είτε σταθμός εργασίας. Τα μέσα που χρησιμοποιούνται για τη διάδοση των πληροφοριών από και προς τον σταθμό βάσης είναι το Internet, τα ασύρματα κανάλια, δορυφόροι κ.ά. Έτσι λοιπόν εκατοντάδες έως αρκετές χιλιάδες αισθητήριοι κόμβοι αναπτύσονται εντός πεδίου για να δημιουργήσουν ένα ασύρματο δίκτυο πολλαπλών κόμβων. Οι κόμβοι μπορεί να χρησιμοποιήσουν ασύρματα μέσα επικοινωνίας όπως υπέρυθρες, ραδιοκύματα, οπτικά μέσα ή Bluetooth για την επικοινωνία τους, με το εύρος μετάδοσής τους να ποικίλλει ανάλογα με το πρωτόκολλο επικοινωνίας που χρησιμοποιούν κάθε φορά.

1.2 Ιστορική αναδρομή

Για την ιστορία, τα πρώτα ασύρματα δίκτυα αισθητήρων προορίζονταν για στρατιωτικές εφαρμογές και είχαν υψηλό κόστος. Οι πρώτες κινήσεις σε αυτή τη θεματική περιοχή βασίστηκαν σε κάποια **προγράμματα DARPA** (Defence Advance Research Projects Agency) [70]. Πρόκειται για έναν οργανισμό του Υπουργείου Εθνικής Άμυνας των ΗΠΑ υπεύθυνο για την ανάπτυξη των αναδυόμενων τεχνολογιών για χρήση από τον στρατό. Στα μέσα λοιπόν της δεκαετίας του 1990 χρηματοδοτήθηκε το πρόγραμμα SmartDust (“έξυπνη σκόνη”)

και αντικείμενο ήταν να δημιουργηθούν κόμβοι πολύ μικροί σε μέγεθος προκειμένου να χρησιμοποιηθούν για κατασκοπεία, να μπορούν δηλαδή οι κόμβοι να ανιχνεύουν τι γίνεται στον χώρο ενδιαφέροντος χωρίς να γίνονται αντιληπτοί απ' τον εχθρό και δρώντας διαδραστικά μεταξύ τους [17] [65]. Με την εξέλιξη της τεχνολογίας, τα WSN έχουν βρεί χρήσιμες εφαρμογές στον τομέα της υγείας, της βιομηχανίας, του εμπορίου και των υπολογιστικών συστημάτων καθώς και σε ένα πλήθος άλλων εφαρμογών.

1.3 Δομή κόμβων δικτύων WSN

Ένα ασύρματο δίκτυο αισθητήρων μπορεί να αποτελείται από μερικές δεκάδες έως και αρκετές χιλιάδες βαθμίδες αισθητήριων κόμβων. Το μικρό μέγεθος των αισθητήριων κόμβων έχει αντίκτυπο στους περιορισμούς πόρων όπως η ενέργεια, η μνήμη και η υπολογιστική ισχύς. Τα βασικά δομικά στοιχεία (σχήμα 1.1) ενός αισθητήριου κόμβου είναι [17] [24]:

- **Μονάδα αίσθησης** που έχει έναν ή περισσότερους αισθητήρες και έναν αναλογικό σε ψηφιακό μετατροπέα (A/D converter).
- **Μονάδα επεξεργασίας** για την επεξεργασία των δεδομένων που οι ίδιοι ανιχνεύουν
- **Πομποδέκτης** για την ασύρματη επικοινωνία
- **Μονάδα ενέργειας** συνήθως μια μπαταρία η μια ενσωματωμένη μορφή συγκομιδής ενέργειας
- Προαιρετικά ενα **συστημα ανίχνευσης θέσης** και ενα **κινητήριο σύστημα** για να δώσουμε κινητικότητα στους κόμβους μας

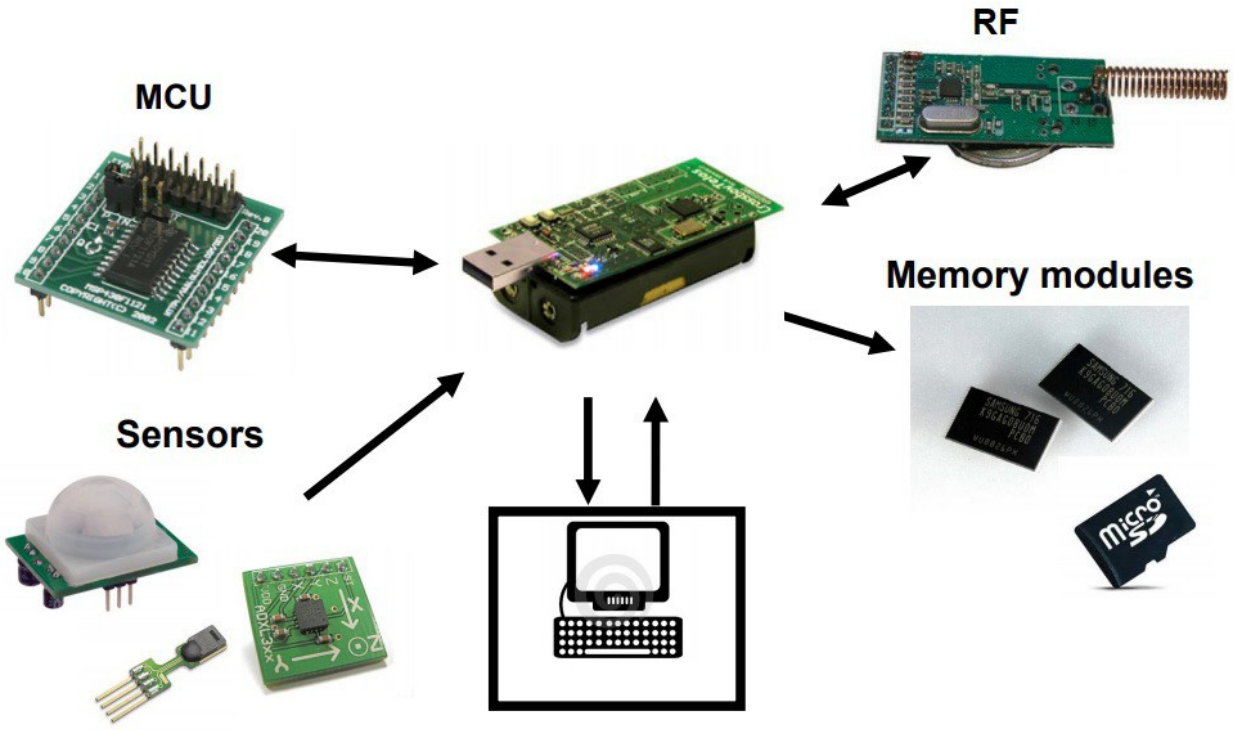
Σχήμα 1.1: Διάγραμμα τυπικής δομής κόμβου σε δικτύου WSN

Ειδικότερα...

- Η **μονάδα αίσθησης (sensing unit)** ανιχνεύει και καταγράφει το τι υπάρχει γύρω απο τον αισθητήρα. Συνήθως είναι μια αναλογική τάση γ' αυτο και χρησιμοποιουμε τον a/d μεταροπέα
- Η **μονάδα επεξεργασίας (processing unit)** συγκεντρώνει, επεξεργάζεται και αποθηκεύει τα δεδομένα που καταγράφονται από τους αισθητήρες και διαχειρίζεται τη πληροφορία από και προς τη μονάδα επικοινωνίας. Είναι αρμόδια ώστε κάθε κόμβος να μπορεί να επικοινωνεί με τους υπολοίπους και επίσης να μπορεί να καθοδηγήσει το σύστημα κίνησης που θα πρέπει να οδηγήσει με τη σερά του τους κόμβους στη σωστή θέση. Μπορεί να χρησιμοποιεί μικροελεγκτή ή μικροεπεξεργαστή ή συστοιχία επιτόπια προγραμματιζόμενων πυλών (FPGA). Πραγματοποιεί συχνή αναδιάταξη των δεδομένων που περιέχονται στη μνήμη της ώστε να εξοικονομεί αποθηκευτικό χώρο με διαδικασίες όπως η συσσωμάτωση δεδομένων (data aggregation) ενώ συνήθως χρησιμοποιεί flash memory.
- Η **μονάδα επικοινωνίας (transeiver unit)** συνήθως χρησιμοποιεί ένα ασύρματο πομποδέκτη ραδιοσυχνότητας (RF) ο οποίος υπόκεινται σε

αυστηρούς περιορισμούς. Εναλλακτικά χρησιμοποιούνται και άλλα μέσα μετάδοσης όπως Wi-Fi, Bluetooth, υπέρυθρες.

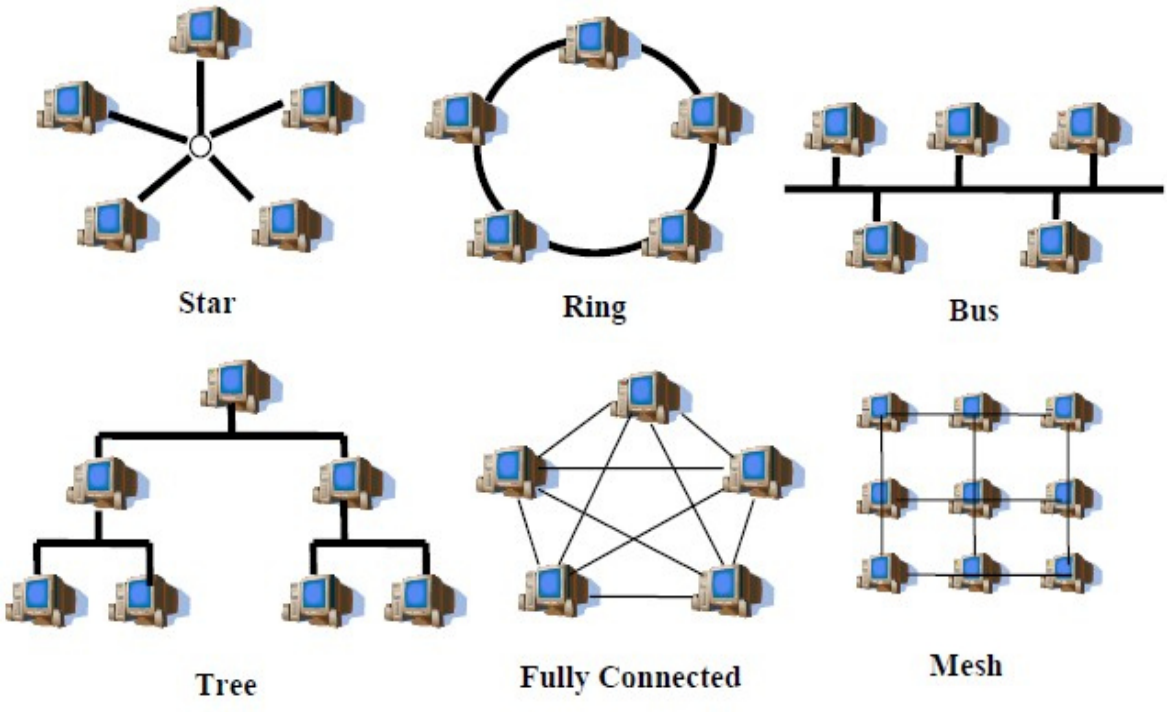
- Η **μονάδα ενέργειας (power unit)** συνήθως είναι μια μπαταρία επαναφορτιζόμενη ή μη επαναφορτιζόμενη. Στα δύσκολα περιβάλλοντα είναι δύσκολο να αντικαταστήσεις ή να επαναφορτίσεις τις μπαταρίες, γ αυτό και αποτελεί το μεγαλύτερο πρόβλημα-αδυναμία στα WSN's.
- Το **σύστημα ανίχνευσης θέσης (location finding system)** όπως είναι το GPS. Η λειτουργία του είναι ικανοποιητική μόνο σε συγκεκριμένα πεδία εφαρμογής.
- Το **κινητήριο σύστημα (mobilizer)** που συνήθως αποτελείται από μικρά κινούμενα ρομπότ αυτόματης ή τηλεκατευθυνόμενης οδήγησης



Εικόνα 1.2: Δομικά στοιχεία αισθητήριου κόμβου

1.4 Βασικές τοπολογίες

Ένα ασύρματο δίκτυο αισθητήρων αποτελείται από κόμβους, οι οποίοι μπορεί να επιτελούν λειτουργίες ελέγχου, αποστολής και λήψης μηνυμάτων, μέσω του ασύρματου διαύλου. Οι κόμβοι αυτοί συνθέτουν την τοπολογία του δικτύου. Οι βασικές τοπολογίες, οι οποίες απεικονίζονται στην εικόνα 1.3 είναι:



Εικόνα 1.3: Βασικές τοπολογίες

1.5 Βασικά χαρακτηριστικά των κόμβων

Για την αξιολόγηση της απόδοσης ενός ασύρματου δικτύου αισθητήρων θα πρέπει να εξετασθούν τα παρακάτω κύρια χαρακτηριστικά για κάθε αισθητήριο κόμβο [17].

- *Ανοχή σφαλμάτων*: Κάθε κόμβος στο δίκτυο είναι επιρρεπής σε απρόσμενη αποτυχία. Η ανοχή σφαλμάτων αφορά τη δυνατότητα αδιάλειπτης λειτουργίας του δικτύου σε περίπτωση αστοχίας στον κόμβο.
- *Κινητικότητα κόμβων*: Προκειμένου να αυξηθεί η αποτελεσματικότητα στην επικοινωνία, οι κόμβοι μπορούν να κινηθούν οπουδήποτε μέσα στο πεδίο εφαρμογής τους ανάλογα πάντα με τον τύπο εφαρμογής.

- *Δυναμική τοπολογία δικτύου*: Η διασύνδεση μεταξύ των κόμβων βασίζεται σε κάποια βασική τοπολογία. Τα WSN's πρέπει να έχουν τη δυνατότητα λειτουργίας σε δυναμικές τοπολογίες.
- *Αποτυχίες διασύνδεσης*: Εάν κάποιος κόμβος εντός δικτύου αποτύχει να ανταλλάξει δεδομένα με άλλους κόμβους τότε θα πρέπει να αναφερθεί αμέσως στον σταθμό βάσης.
- *Ετερογένεια των κόμβων*: Οι αισθητήριοι κόμβοι διαφορετικών χαρακτηριστικών-τύπων θα πρέπει να συνεργάζονται εντός του δικτύου.
- *Επεκτασιμότητα*: Οι κόμβοι σε ένα WSN μπορεί να είναι εκατοντάδες έως μερικές χιλιάδες. Για τον λόγο αυτό ο σχεδιασμός του δικτύου θα πρέπει να γίνεται με το σκεπτικό της επεκτασιμότητας.
- *Ανεξαρτησία*: Τα WSN's θα πρέπει να είναι ικανά να δουλέψουν χωρίς να εξαρτώνται απο κάποιο κεντρικό σημείο ελέγχου.
- *Προγραμματισμός*: Οι έννοιες του επαναπρογραμματισμού και της αναδιάρθρωσης θα πρέπει να είναι υπαρκτές σε τέτοια δίκτυα έτσι ώστε να μπορούν να ανταποκριθούν σε ενδεχόμενες δυναμικές αλλαγές εντός του δικτύου.
- *Αξιοποίηση αισθητήρων*: Οι αισθητήρες πρέπει να χρησιμοποιούνται με τέτοιο τρόπο ώστε να παράγουν τη μέγιστη απόδοση, καταναλώνοντας λιγότερη ενέργεια.
- *Αποτελεσματικότητα των κρυπτοσυστημάτων δημοσίου κλειδιού*: Ο περιορισμός στην υπολογιστική δύναμη και την ενέργεια των κόμβων καθιστούν συχνά ανεπιθύμητη τη χρήση αλγορίθμων κρυπτογράφησης δημοσίου κλειδιού.

1.6 Κατηγορίες Ασύρματων Δικτύων Αισθητήρων

Η αρχιτεκτονική των ασύρματων δικτύων αισθητήρων δεν είναι σταθερή. Διαφέρει από εφαρμογή σε εφαρμογή. Επομένως, οι προκλήσεις και οι

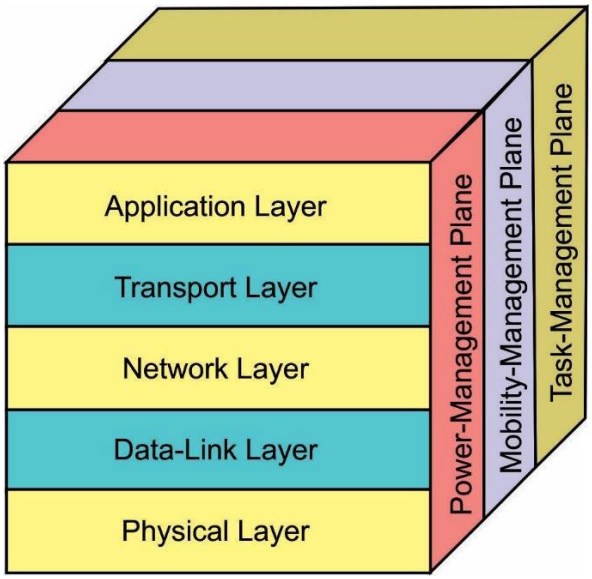
περιορισμοί είναι συγκεκριμένοι, αντίστοιχοι με τα περιβάλλοντα που εφαρμόζονται σε αυτά τα δίκτυα. Στη σύγχρονη επιστημονική βιβλιογραφία [28] [11] αναφέρονται διαφορετικές κατηγορίες Ασύρματων Δικτύων Αισθητήρων ανάλογα με το περιβάλλον εφαρμογής, οι οποίες ονομαστικά ταξινομούνται σε:

- Επίγεια (terrestrial WSNs): Οι αισθητήριοι κόμβοι είναι διατεταγμένοι όπως ένα ασύρματο ad-hoc δίκτυο είτε με προκαθορισμένο τρόπο στο έδαφος.
- Υπόγεια (Underground WSNs): Η συγκεκριμένη αρχιτεκτονική είναι ακριβή λόγω των περιορισμών που υπάρχουν σε συνθήκες υπόγειου εδάφους.
- Υποβρύχια (Underwater WSNs): Σε τέτοιου είδους αρχιτεκτονικές η επικοινωνία επιτυγχάνεται μέσω μετάδοσης ακουστικών κυμμάτων κάτω από το νερό.
- Πολυμέσων (Wireless Multimedia Sensor Networks WMSNs): Τέτοιου είδους αρχιτεκτονικές διαμόρφωσης μπορούν να υλοποιηθούν με χαμηλού κόστους αισθητήριους κόμβους χρησιμοποιώντας κάμερες και μικρόφωνα και επιτυγχάνοντας επικοινωνία μέσω ασύρματης σύνδεσης για σκοπούς ανάκτησης δεδομένων, επεξεργασίας, συσχέτισης και συμπίεσης.
- Κινητά (Mobile WSNs): Αυτή η αρχιτεκτονική περιλαμβάνει την κινητικότητα των κόμβων, την ανατοποθέτησή τους και την ικανότητα αυτο-οργάνωσης. Οι πληροφορίες που συλλέγονται μέσω ενός κινητού δικτύου WSN, γνωστοποιούνται εντός του εύρους μεταξύ των. Οι βασικοί στόχοι αυτής της αρχιτεκτονικής είναι η ανάπτυξη, η τοπικοποίηση των κόμβων, η αυτο-οργάνωσή τους, ο έλεγχος στη πλοήγηση, η κάλυψη, η ενέργεια κ.ά.

1.7 Αρχιτεκτονική Ασύρματων Δικτύων Αισθητήρων

Σε ένα ασύρματο δίκτυο αισθητήρων οι κόμβοι συνήθως χρησιμοποιούν τη μονάδα επικοινωνίας για να μεταδώσουν τα δεδομένα από τις μετρήσεις τους προς μια κεντρική βαθμίδα συγκέντρωσης δεδομένων που ονομάζεται σταθμός βάσης (base station). Ο σταθμός βάσης ουσιαστικά είναι ένα κεντρικό σημείο συγκέντρωσης δεδομένων που επιτελεί τον εποπτικό έλεγχο του WSN ενώ επιπρόσθετα, αποτελεί μέσω ενσύρματων ή ασύρματων μέσων, το σημείο διασύνδεσης του δικτύου με τον τελικό χρήστη ή ακόμα και με ένα άλλο δίκτυο. Τόσο οι αισθητήριοι κόμβοι όσο και οι σταθμοί βάσης χρησιμοποιούν τη παρακάτω στοίβα πρωτοκόλλου (σχήμα 1.2). Αυτή η στοίβα συνδυάζει την ισχύ και την γνώση στη δρομολόγηση, ενσωματώνει τα δεδομένα με πρωτόκολλα δικτύωσης, επικοινωνεί αποτελεσματικά μέσω του ασύρματου μέσου ενώ παράλληλα προωθεί συνεργατικές προσπάθειες αισθητήριων κόμβων [18]. Η προαναφερθείσα στοίβα αποτελείται από τα παρακάτω επίπεδα:

- Φυσικό επίπεδο (Physical)
- Επίπεδο ζεύξης δεδομένων (Data-Link)
- Επίπεδο δικτύου (Network)
- Επίπεδο μεταφοράς (Transport)
- Επίπεδο εφαρμογής (Application) καθώς επίσης και από τρία επίπεδα διαχείρισης (management planes), α] ενέργειας (power), β] κινητικότητας (mobility) και γ] εργασιών (task).



Σχήμα 1.2: Στοίβα πρωτοκόλλου

Το φυσικό επίπεδο θα πρέπει να πληροί τις απαιτήσεις όπως η παραγωγή φορέα συχνότητας, η επιλογή συχνότητας, η ανίχνευση σήματος, η διαμόρφωση και η κρυπτογράφηση των δεδομένων, μηχανισμοί αποστολής και λήψης.

Το επίπεδο ζεύξης δεδομένων θα πρέπει να πληροί τις απαιτήσεις για πρόσβαση στο μέσο, έλεγχο σφαλμάτων, διαμόρφωση ροής δεδομένων και ανίχνευση ροών δεδομένων. Το MAC επίπεδο στο επίπεδο ζεύξης δεδομένων θα πρέπει να είναι ικανό να ανιχνεύει τυχόν συγκρούσεις χρησιμοποιώντας πάντα την ελάχιστη ισχύ.

Το επίπεδο δικτύου είναι αρμόδιο για την δρομολόγηση των πακέτων προς το επίπεδο μεταφοράς. Θα πρέπει για παράδειγμα να βρεί το πιο αποδοτικό μονοπάτι για τα πακέτα που κατευθύνονται προς κάποιον προορισμό.

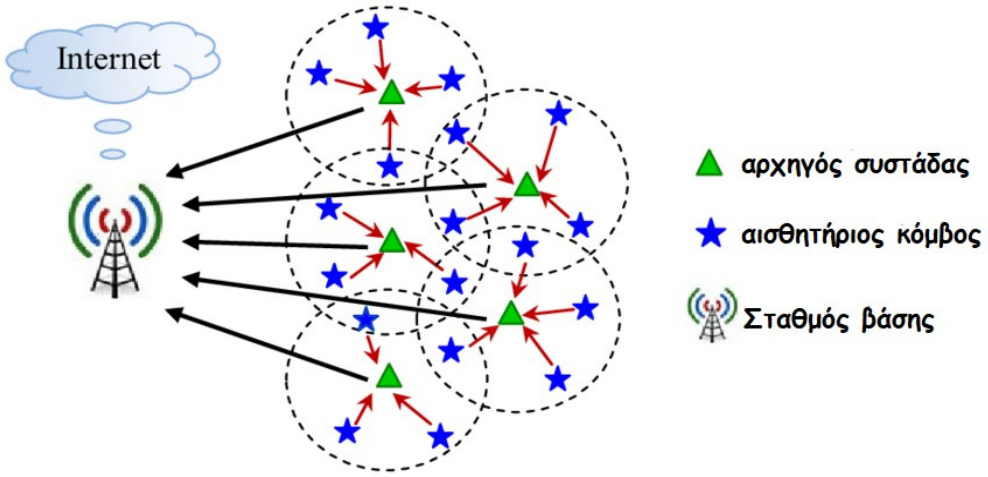
Το επίπεδο μεταφοράς είναι αναγκαίο όταν το ασύρματο δίκτυο αισθητήρων χρειαστεί να είναι προσβάσιμο μέσω διαδικτύου. Βοηθάει στη διατήρηση της ροής των δεδομένων όποτε αυτό απαιτείται από την εκάστοτε εφαρμογή. Το επίπεδο εφαρμογής είναι υπεύθυνο να παρουσιάζει όλη την απαιτούμενη πληροφορία στην τρέχουσα κάθε φορά εφαρμογή και να μεταδίδει μηνύματα από το επίπεδο εφαρμογής πιο χαμηλά στα υπόλοιπα επίπεδα.

Το επίπεδο διαχείρισης ισχύος διαχειρίζεται την αξιοποίηση ισχύος από τους κόμβους ενώ το επίπεδο διαχείρισης κινητικότητας είναι υπεύθυνο για το μοτίβο κίνησης των αισθητήριων κόμβων. Επίσης το επίπεδο διαχείρισης εργασιών προγραμματίζει τα καθήκοντα ανίχνευσης και αποστολής από τους αισθητήριους κόμβους. Τα επίπεδα διαχείρισης (management planes) γενικά, βοηθούν τους αισθητήριους κόμβους να συνεργάζονται αποτελεσματικότερα μεταξύ τους μέχρις ότου φθάσουν στον επιθυμητό στόχο, καταναλώνοντας όσο το δυνατόν λιγότερη ενέργεια.

Ο σχεδιασμός ενός πρωτοκόλλου δικτύου που προορίζεται για ασύρματα δίκτυα αισθητήρων θα πρέπει να πληροί κάποιους περιορισμούς όπως περιορισμένο εύρος ζώνης καναλιού, περιορισμένη ενέργεια, διάδοση ηλεκτρομαγνητικών κυμάτων, κανάλι επιρρεπές σε σφάλματα, χρονικές συνθήκες και κινητικότητα.

Υπάρχουν γενικές ιδέες που μπορούν να χρησιμοποιηθούν για την υπέρβαση αυτών των περιορισμών. Τα πρωτόκολλα χαμηλής ενέργειας βοηθούν στην επιμήκυνση της περιορισμένης ενέργειας του κόμβου. Ο έλεγχος ισχύος για παράδειγμα μπορεί να χρησιμοποιηθεί για την καταπολέμηση της εξασθένησης των ραδιοκυμάτων. Ένας πομπός μπορεί να ρυθμίσει την ισχύ του ραδιοκυμάτων με τέτοιο τρόπο ώστε να γινόνταν αποδεκτό μόνο με συγκεκριμένο επίπεδο ισχύος. Πρωτόκολλα επιπέδου ζεύξης καθώς και MAC πρωτόκολλα μπορούν να χρησιμοποιηθούν για την καταπολέμηση των σφαλμάτων στα κανάλια. Προσαρμοστική δρομολόγηση καθώς επίσης πρωτόκολλα MAC και επιπέδου ζεύξης μπορούν να χρησιμοποιηθούν για να ξεπεραστούν οι χρονικά μεταβαλλόμενες συνθήκες που προκύπτουν από το ασύρματο κανάλι και τη κινητικότητα των κόμβων. Όλα τα παραπάνω αποτελούν ιδέες που θα μπορούσαν να υλοποιηθούν προς εξάλειψη των άνω περιορισμών.

Οι κόμβοι σε ένα ασύρματο δίκτυο αισθητήρων οργανώνονται κατά συστοιχίες (clusters), κατά επίπεδα (layers), είτε κατα συνδυασμούς αυτών [21]. Στην εικόνα 1.4 απεικονίζεται η οργάνωση των κόμμβων κατά συστοιχίες (clusters).



Εικόνα 1.4: Μοντέλο WSN βασισμένο σε συστοιχίες (clusters) κόμβων

1.8 Απαιτήσεις Ασύρματων Δικτύων Αισθητήρων

Τα χαρακτηριστικά που απαιτούνται και καθιστούν τα ασύρματα δίκτυα αισθητήρων δημοφιλή και ελκυστικά για χρήση σε νέες καινοτόμες εφαρμογές είναι [70]:

1. **Ευελιξία.** Η αρχιτεκτονική των WSNs δεν είναι σταθερή αλλά ποικίλλει από εφαρμογή σε εφαρμογή γεγονός που δικαιολογεί ότι τα πρωτόκολλα και οι αλγόριθμοι διέπονται από χαρακτηριστικά αυτοοργάνωσης.
2. **Ανοχή σφαλμάτων.** Οι κόμβοι έχουν τη δυνατότητα να διατηρούν τις λειτουργίες που διενεργούνται στο δίκτυο ακόμη και σε δυσμενείς καταστάσεις όπως είναι η περιορισμένη ισχύς μπαταρίας, οι παρεμβολές από εξωτερικές πηγές, ποσοστά σφάλματος των κόμβων και οι σκληρές περιβαλλοντικές συνθήκες.

3. **Διάρκεια ζωής.** Οι δύο κύριοι παράγοντες που πρέπει να ληφθούν υπόψιν είναι η εξισορρόπηση φορτίου και η εξοικονόμηση ενέργειας. Αυτοί οι δύο παράγοντες μπορούν να βελτιώσουν τη διάρκεια ζωής σε δίκτυο WSN όσο το δυνατόν περισσότερο.
4. **Επεκτασιμότητα.** Ο αριθμός των κόμβων σε ένα ασύρματο δίκτυο αισθητήρων μπορεί να είναι πολύ μεγάλος. Ως εκ τούτου, ο σχεδιασμός στην αρχιτεκτονική και τα πρωτόκολλα θα πρέπει να ανάλογος του αριθμού αυτού.
5. **Σε πραγματικό χρόνο.** Διάφορες δυνατότητες όπως η ανίχνευση, η επεξεργασία και η επικοινωνία των WSNs, αξιοποιούνται σε διάφορα προβλήματα στον πραγματικό κόσμο, οπότε θα πρέπει να ακολουθείται σχολαστικά ο συντονισμός τους σε παρόμοια προβλήματα
6. **Ασφάλεια.** Τα δεδομένα που προσφέρονται ενδέχεται να είναι υψίστης διαβάθμισης, όπως για παράδειγμα δεδομένα που πηγάζουν απ' τον χώρο της υγειονομικής περίθαλψης όπως επίσης και αυτά που διακινούνται στις ένοπλες δυνάμεις. Έτσι λοιπόν η ασφάλεια θα πρέπει να θεωρείται δεδομένη σε ανάλογες αρχιτεκτονικές.
7. **Κόστος παραγωγής.** Το κόστος των αισθητήριων κόμβων θα πρέπει να είναι χαμηλό έτσι ώστε μόλις εξαντληθούν τα ενεργειακά τους αποθέματα να μπορούν να αντικατασταθούν από άλλους κόμβους.
8. **Ανάπτυξη.** Σε WSN συστήματα μεγάλης κλίμακας ανάπτυξης, οι κόμβοι που χρίζουν αντικατάστασης και συντήρησης γίνεται με τυχαία σειρά. Υπάρχει λοιπόν μια τεράστια απαίτηση για αναδιαμόρφωση και επαναπρογραμματισμό.
9. **Αξιοπιστία.** Οποιοσδήποτε μπορεί να βασιστεί στα ασύρματα δίκτυα αισθητήρων, καθώς ο αρχιτεκτονικός σχεδιασμός τους είναι στιβαρός οδηγώντας σε ασφαλή συλλογή δεδομένων και αξιόπιστη παράδοση χωρίς απώλειες.

1.9 Περιορισμοί Ασύρματων Δικτύων Αισθητήρων

Τα WSNs υποφέρουν από πολλούς περιορισμούς λόγω των ιδιαίτερων χαρακτηριστικών τους. Αποτελούνται από μεγάλο αριθμό αισθητήριων κόμβων με περιορισμένη ικανότητα επεξεργασίας, πολύ χαμηλή χωρητικότητα αποθήκευσης και περιορισμένο εύρος ζώνης επικοινωνίας [17] [18]. Αυτοί οι περιορισμοί οφείλονται στη περιορισμένη ενέργεια και στο φυσικό τους μέγεθος. Λόγω αυτών των περιορισμών, είναι δύσκολο να χρησιμοποιηθούν άμεσα οι συμβατικοί μηχανισμοί ασφάλειας. Για τη βελτιστοποίηση των συμβατικών αλγορίθμων ασφάλειας, είναι απαραίτητο να γνωρίζουμε σχετικά με τους περιορισμούς των αισθητήριων κόμβων. Μερικοί από τους σημαντικότερους περιορισμούς είναι [20]:

1. **Περιορισμοί πόρων.** Περιορισμένο εύρος ζώνης, ενέργεια, δυνατότητες μνήμης και επεξεργασίας, multi-hop, μη ασφαλή ραδιοκύματα και μικρό εύρος επικοινωνίας.
2. **Περιορισμοί σχεδίασης.** Οι διάφοροι περιορισμοί σχεδίασης περιλαμβάνουν την αποτυχία κόμβων, το γεγονός ότι είναι κινούμενοι, συγκεκριμένη τοπολογία δικτύου ανά εφαρμογή, ετερογενές δίκτυο, φυσικό μέγεθος, συνολικός αριθμός κόμβων κ.ά.

Παρακάτω θα αναλύσουμε δύο από τους πιο σημαντικούς περιορισμούς στα ασύρματα δίκτυα αισθητήρων:

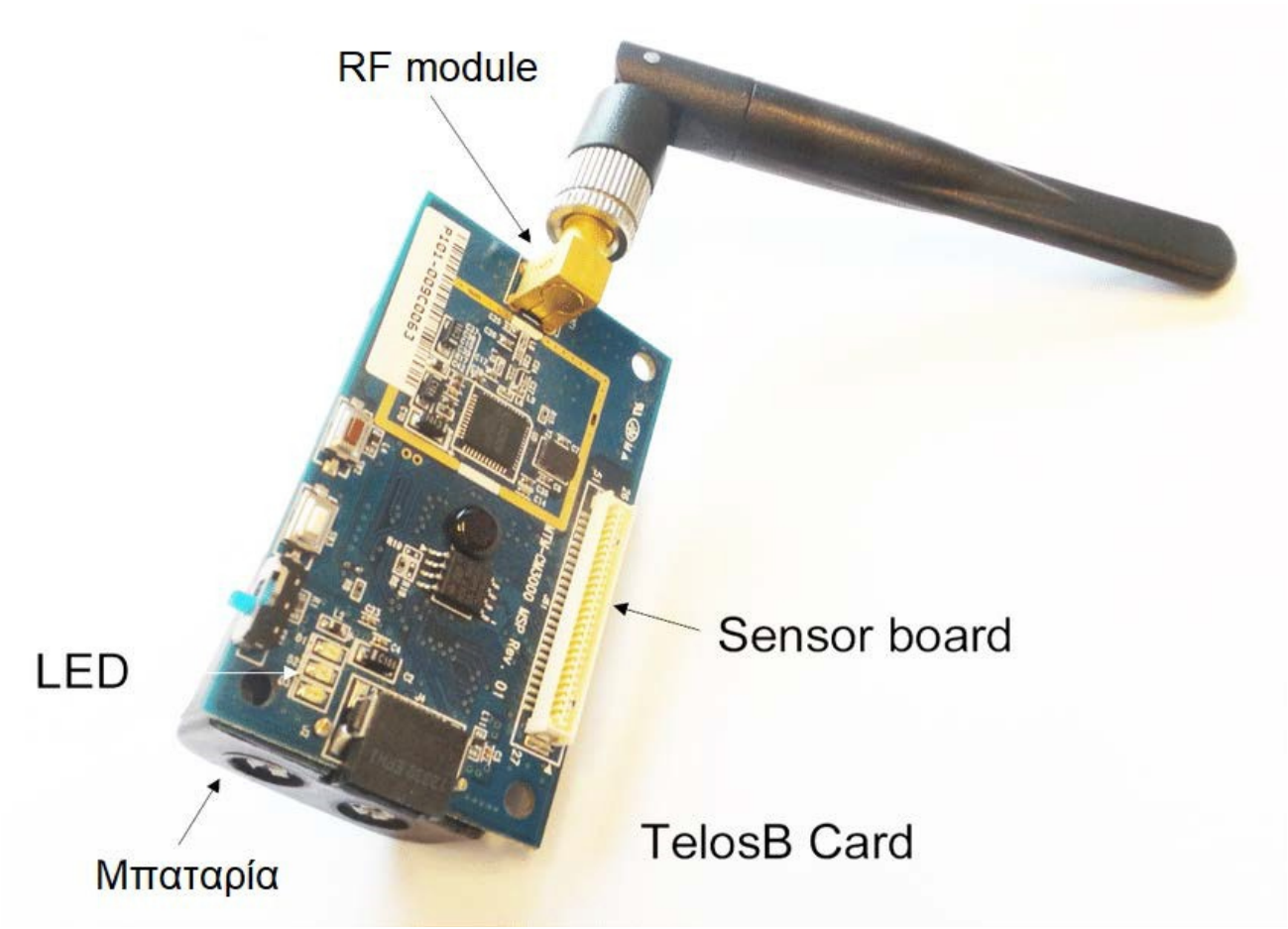
Περιορισμός ενέργειας: Η ενέργεια είναι ο μεγαλύτερος περιορισμός στα WSNs. Γενικά, η κατανάλωση ενέργειας στους αισθητήριους κόμβους μπορεί να κατηγοριοποιηθεί σε τρία μέρη:

- ενέργεια για τον αισθητήρα
- ενέργεια για την επικοινωνία μεταξύ αισθητήριων κόμβων, και
- ενέργεια για τον υπολογισμό στον μικροεπεξεργαστή.

Στα συστήματα αυτά κάθε bit που μεταδίδεται καταναλώνει περίπου τόσο μεγάλη ισχύ όσο απαιτεται για την εκτέλεση 800 έως 1000 εντολών, μεταρέποντας

την επικοινωνία πιο δαπανηρή από τον υπολογισμό. Τα υψηλότερα επίπεδα ασφάλειας στα WSN συστήματα συνήθως αντιστοιχούν σε περισσότερη κατανάλωση ενέργειας για λειτουργίες κρυπτογράφησης. Ως εκ' τούτου θα μπορούσαν να χωριστούν σε διαφορετικά επίπεδα ασφάλειας ανάλογα με το ενεργειακό τους κόστος.

Περιορισμός μνήμης: Ο αισθητήριος κόμβος είναι μια μικροσκοπική συσκευή με μικρή μνήμη και ελάχιστο χώρο αποθήκευσης. Η μνήμη αποτελείται συνήθως από μνήμη flash και RAM. Η μνήμη Flash χρησιμοποιείται για την αποθήκευση του ληφθέντος κώδικα εφαρμογής και η μνήμη RAM χρησιμοποιείται για την αποθήκευση προγραμμάτων εφαρμογών, δεδομένων αισθητήρα και ενδιάμεσων αποτελεσμάτων υπολογισμού. Συνήθως δεν υπάρχει αρκετός χώρος για την εκτέλεση πολύπλοκων αλγορίθμων ασφάλειας μετά τη φόρτωση του λειτουργικού συστήματος και του κώδικα εφαρμογής. Στο project Smart Dust, για παράδειγμα, το Tiny OS καταναλώνει περίπου 4Kbytes οδηγιών, αφήνοντας μόνο 4500bytes για την εκτέλεση εφαρμογών και αλγορίθμων ασφάλειας. Ένας κοινός τύπος αισθητήριου κόμβου - Telos B - (εικόνα 1.5) διαθέτει CPU 16-bit, 8 MHz RISC με μόνο 10Kbyte RAM, μνήμη προγράμματος 48Kbytes και μνήμη flash 1024Kbytes [71]. Επομένως, οι αλγόριθμοι ασφάλειας δυσκολεύονται να ενσωματωθούν σε αυτούς τους αισθητήρες.

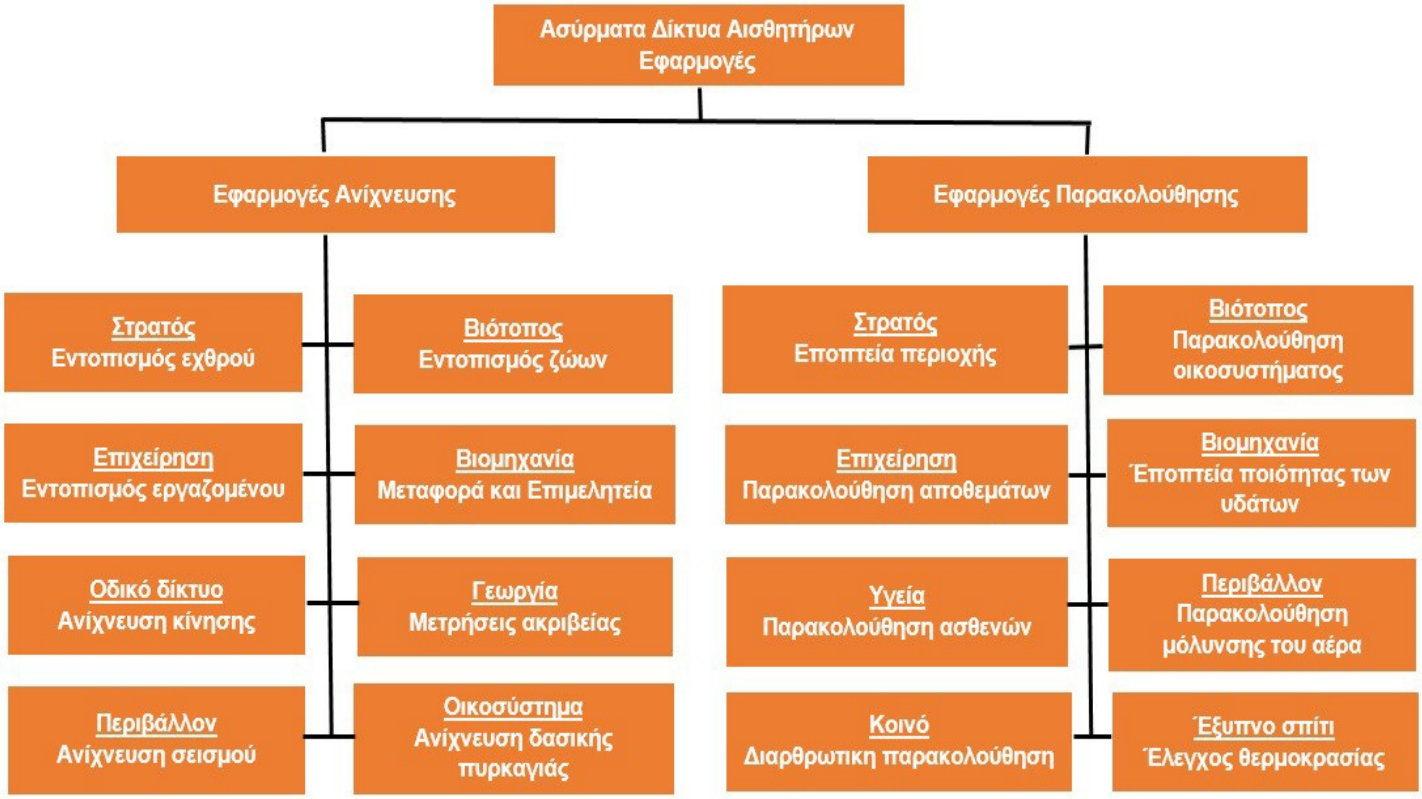


Εικόνα 1.5: (MTM-CM5000-MSP) TelosB αισθητήριος κόμβος

1.10 Πεδία εφαρμογής Ασύρματων Δικτύων Αισθητήρων

Τα Ασύρματα δίκτυα Αισθητήρων αξιοποιήθηκαν αρχικώς σε συλλογή δεδομένων απο περιβάλλοντα που ο άνθρωπος δεν δύναται να παραστεί και εν συνέχεια χρησιμοποιήθηκαν στον εντοπισμό κινούμενων αντικειμένων ή σεισμικών δραστηριοτήτων. Επίσης χρησιμοποιήθηκαν με επιτυχία στη καταγραφή συγκεκριμένων συμβάντων και τιμών στο χώρο, από την παρακολούθηση των οποίων αξιολογούνται οι τιμές και προσδιορίζονται καταστάσεις. Στη σημερινή εποχή οι εφαρμογές των Ασύρματων Δικτύων Αισθητήρων είναι αναρίθμητες, καθώς οι τρεις βασικές υπηρεσίες της ανίχνευσης, επεξεργασίας και επικοινωνίας, συγκεντρώνονται σε μία μόνο συσκευή που

ονομάζεται αισθητήριος κόμβος και είναι ικανή να παρακολουθεί τη θερμοκρασία, την υγρασία, την πίεση και τα επίπεδα θορύβου. Οι αισθητήρες έχουν πολυδιάστατο πεδίο εφαρμογής και ελάχιστες είναι πλέον οι συσκευές που δεν απαρτίζονται τουλάχιστον απο ένα.Οι εφαρμογές των ασύρματων δικτύων αισθητήρων [24] [70] μπορούν γενικά να ταξινομηθούν σε δύο κατηγορίες: *παρακολούθησης* και *ανίχνευσης* (σχήμα 1.3).



Σχήμα 1.3: Ταξινόμηση εφαρμογών Ασύρματων Δικτύων Αισθητήρων

ΚΕΦΑΛΑΙΟ 2

2.1 Εισαγωγή

Ενώ ποικίλες υλοποιήσεις σε θέματα ασφάλειας επικρατούν για διαφορετικά είδη δικτύων, τα ασύρματα δίκτυα αισθητήρων διέπονται απο ορισμένες ιδιότητες που τα κάνουν ευάλωτα σε επιθέσεις σε σύγκριση με τα παραδοσιακά δίκτυα υπολογιστών (πχ ενσύρματα δίκτυα). Παρακάτω θα περιγράψουμε τους λόγους που κάνουν τα WSN να είναι ευάλωτα σε επιθέσεις, τις κατηγορίες επίθεσης καθώς επίσης και τις απαιτήσεις ασφάλειας.

2.2 Κενά ασφάλειας

Τα ιδιαίτερα χαρακτηριστικά των ασύρματων δικτύων αισθητήρων όπως αυτά που περιγράφονται παρακάτω είναι οι λόγοι που καθιστούν τα Ασύρματα Δίκτυα Αισθητήρων ευάλωτα σε επιθέσεις [17] [18] [25].

1. **Περιορισμοί πόρων:** Οι περισσότεροι μηχανισμοί ασφάλειας που χρησιμοποιούνται στα δίκτυα υπολογιστών βασίζονται σε κάποια μορφή κρυπτογραφίας. Ενώ η κρυπτογράφηση με χρήση δημοσίου κλειδιού είναι ένα πολύ πιο ευέλικτο και αποτελεσματικό σχήμα μηχανισμού ασφάλειας σε σχέση με αυτό που χρησιμοποιεί ιδιωτικό κλειδί, οι περιορισμοί ωστόσο σε μνήμη και επεξεργαστική ισχύς των αισθητήριων κόμβων, καθιστούν έναν τέτοιο μηχανισμό αποδοτικό μόνο υπό την προϋπόθεση πολύ προσεκτικής βελτιστοποίησης των αλγορίθμων τόσο σε επίπεδο σχεδιασμού όσο και σε επίπεδο εφαρμογής. Κάτι τέτοιο δεν ισχύει με τα παραδοσιακά δίκτυα υπολογιστών (Ad-Hoc δίκτυα).

2. **Υλοποίηση σε ανοιχτό περιβάλλον:** Επειδή οι αισθητήριοι κόμβοι συνήθως αναπτύσονται σε εξωτερικά περιβάλλοντα χωρίς δυνατότητα επιτήρησης, κάποιος εισβολέας θα μπορούσε εύκολα να έχει πρόσβαση σ' αυτούς και να υποκλέψει ευαίσθητες πληροφορίες (π.χ. κλειδιά ασφάλειας). Αυτό έρχεται σε αντίθεση με τα παραδοιακά δίκτυα υπολογιστών τα οποία ως επι το πλέιστον θα περιορίσουν στο ελάχιστο μια τέτοια απειλή στηριζόμενα σε συστήματα ανίχνευσης εισβολών και ειδικά μοντέλα ασφάλειας.

3. **Μεγάλης κλίμακας ανάπτυξη:** Τα ασύρματα δίκτυα αισθητήρων περιέχουν συνήθως χιλιάδες κόμβους οι οποίοι συνεργάζονται μεταξύ τους για να επιτύχουν αποτελεσματικά τον στόχο τους. Τέτοιες διμερείς συνεργασίες μεταξύ των κόμβων απαιτούν την χρήση πρωτοκόλλων ασφάλειας, όχι πάντοτε κατάλληλων για τα WSN. Επίσης όλοι οι κόμβοι που διακινούν ευαίσθητες πληροφορίες θα πρέπει να πλαισιώνονται από κατάλληλους μηχανισμούς έτσι ώστε όταν ένας κακαντρεχής κόμβος εισέλθει στο δίκτυο με σκοπό να αποσπάσει ευαίσθητες πληροφορίες, να μπορούν να τον ανιχνεύσουν και να τον περιορίσουν.

4. **Ασύρματη συνδεσιμότητα:** Επειδή στα ασύρματα δίκτυα αισθητήρων η επικοινωνία επιτυγχάνεται ασύρματα, αρκεί για κάποιον εισβολέα να συντονιστεί στις συχνότητες λειτουργίας τους για να μπορέσει να παρακολουθήσει την ανταλλαγή κίνησης μεταξύ των κόμβων. Επομένως οι μηχανισμοί ασφάλειας στα ασύρματα δίκτυα αισθητήρων θα πρέπει να λάβουν σοβαρά υπόψιν το ενδεχόμενο να εκδηλωθούν τέτοιου είδους επιθέσεις

2.3 Σχεδιασμός μηχανισμού ασφάλειας

Ο σχεδιασμός του μηχανισμού ασφάλειας σε ένα ασύρματο δίκτυο αισθητήρων θα πρέπει να είναι ευέλικτος και αποτελεσματικός και θα πρέπει να εναρμονίζεται

πλήρως με τις απαιτήσεις ασφάλειας, τις απειλές και τις κατηγορίες των επιθέσεων που υφίστανται σε αυτό [18].

2.3.1 Απειλή

Καλείται το συμβάν που δύναται να παραβιάσει την ασφάλεια ενός συστήματος και έχει τη δυνατότητα να επηρεάσει τη λειτουργία του. Με άλλα λόγια, η απειλή είναι ο πιθανός κίνδυνος να εκμεταλλευτεί κάποιος μια ευπάθεια του συστήματος.

2.3.2 Επίθεση

Καλείται η προσβολή της ασφάλειας του συστήματος που προέρχεται απο μία έξυπνη απειλή. Με άλλα λόγια είναι μια ευφυής πράξη που δύναται σκόπιμα να παρακάμψει τις υπηρεσίες ασφάλειας και να παραβιάσει εν τέλει το σύστημα μας. Στη βιβλιογραφία συχνά οι επιθέσεις αναφέρονται και ως απειλές.

2.3.3 Κατηγορίες απειλών

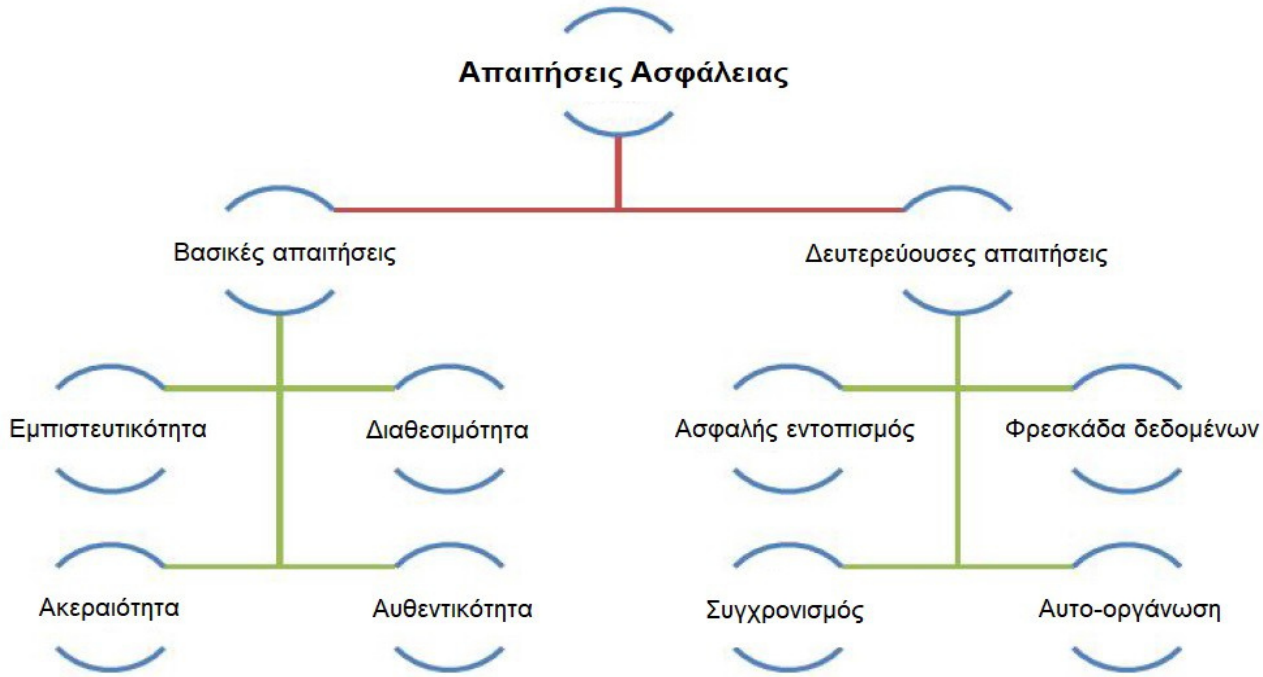
Όπως αναφέρεται στο [29] υπάρχουν τέσσερις κατηγορίες απειλών στα ασύρματα δίκτυα αισθητήρων:

- **Παρέμβαση**. Ένας τύπος επίθεσης που μπορεί να βλάψει την εμπιστευτικόηττα προσπαθώντας να έχει μη εξουσιοδοτημένη πρόσβαση στον αισθητήριο κόμβο και στα αποθηκευμένα δεδομένα/κλειδιά του.
- **Διακοπή**. Ένας τύπος επίθεσης που εμποδίζει τη νόμιμη επικοινωνία μεταξύ των μονάδων επικοινωνίας του συστήματος. Η διακοπή μπορεί να βλάψει τη διαθεσιμότητα του δικτύου, καταστρέφοντας μηνύματα, εγχύοντας κακόβουλο κώδικα ή καταγράφοντας φυσικά τους κόμβους
- **Τροποποίηση**. Ένας τύπος επίθεσης που βλάπτει την ακεραιότητα του δικτύου. Σε αυτή την επίθεση ο αντίπαλος προσπαθεί όχι μόνο να έχει πρόσβαση στα δεδομένα αλλά προσπαθεί επίσης να τα πειράξει. Για παράδειγμα ο αντίπαλος μπορεί να τροποποιήσει τα δεδομένα που βρίσκονται σε μεταφορά μέσα στο δίκτυο.

- **Παρασκεύασμα**. Αυτός ο τύπος επίθεσης μπορεί να βλάψει την αυθεντικότητα των δεδομένων που διακινούνται στο δίκτυο καθώς ο αντίπαλος εγχύει ψευδή πακέτα δεδομένων μέσα σ' αυτό.

2.3.4 Απαιτήσεις ασφάλειας

Πριν αναφερθούμε στους διάφορους τύπους επιθέσεων στα ασύρματα δίκτυα αισθητήρων είναι πολύ σημαντικό να γνωρίζουμε τις απαιτήσεις ασφάλειας πουαναγκαίουν σε αυτά. Οι υπηρεσίες ασφάλειας θα πρέπει να προστατεύουν τις πληροφορίες που κοινοποιούνται μέσω του δικτύου και τους πόρους, από επιθέσεις και κακή συμπεριφορά των κόμβων όπως ακριβώς και σε ένα αυτοοργανωμένο (ad hoc) δίκτυο. Υπάρχουν δύο είδη απαιτήσεων-στόχων στα ασύρματα δίκτυα αισθητήρων: *Πρωταρχικές* και *δευτερεύουσες* απαιτήσεις (σχήμα 2.1) [56] [42] [34]. Οι πρωταρχικές απαιτήσεις είναι αυτές που θα πρέπει να υπάρχουν σε κάθε περίπτωση. Είναι επίσης γνωστές ως οι βασικές απαιτήσεις ασφάλειας. Σε αυτές ανήκουν η εμπιστευτικότητα, η ακεραιότητα, η αυθεντικότητα και η διαθεσιμότητα. Στις δευτερεύουσες απαιτήσεις ανήκουν η φρεσκάδα δεδομένων, ο ασφαλής εντοπισμός, η οργάνωση, ο συγχρονισμός χρόνου και η βέλτιστη κατανάλωση ισχύος.



Σχήμα 2.1: Απαιτήσεις ασφάλειας στα WSN's

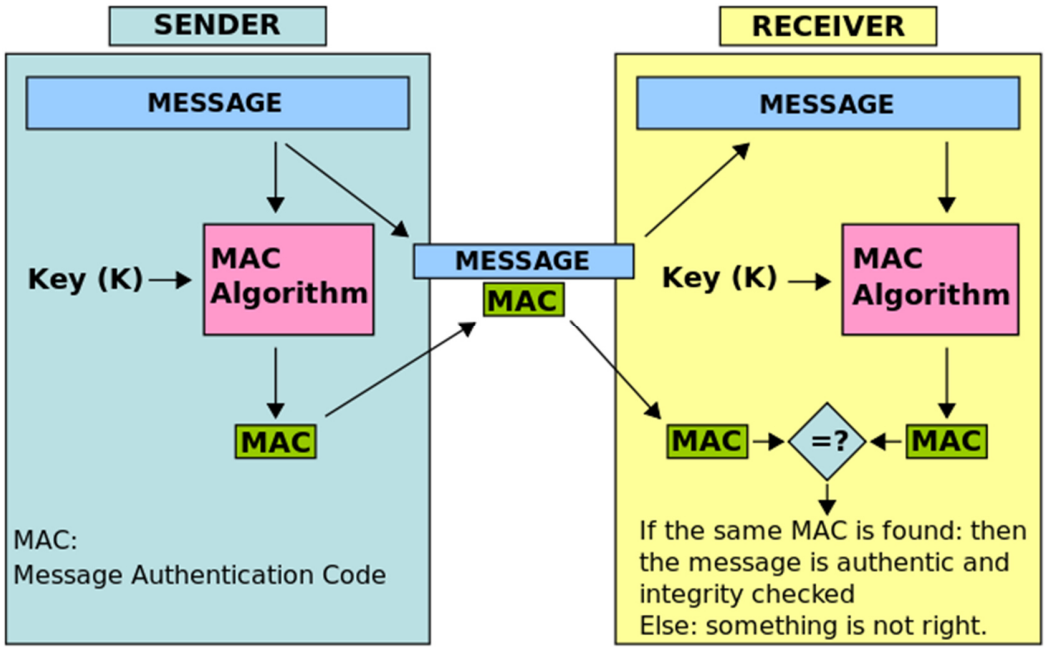
2.4 Βασικές απαιτήσεις ασφάλειας

Οι *βασικές απαιτήσεις* ασφάλειας ενός ασύρματου δικτύου αισθητήρων είναι οι εξής:

1. **Αυθεντικότητα:** Ο έλεγχος ταυτότητας επιτρέπει σε έναν κόμβο να επιβεβαιώσει ότι η ταυτότητα του κόμβου με τον οποίο επικοινωνεί είναι αυτή που αξιώνεται. Αυτό βοηθά έναν κόμβο να επαληθεύσει την προέλευση των πακέτων που αποστέλλονται σ' αυτόν, αποκλείωντας έτσι την πιθανότητα ότι κακεντρεχή πακέτα έχουν εισέλθει στο κανάλι ασύρματης επικοινωνίας με σκοπό να παραπλανήσουν με υποτιθέμενα γνήσια πακέτα. Ένας ακόμη μηχανισμός ελέγχου ταυτότητας είναι ο κωδικός επαλήθευσης μηνυμάτων (MAC) που χρησιμοποιείται για να επαλήθευσει τη προέλευση ενός μηνύματος.

2. **Εμπιστευτικότητα:** Η εμπιστευτικότητα ορίζει ότι στη πληροφορία θα έχουν πρόσβαση μονο οι κόμβοι που επιτρέπεται να έχουν πρόσβαση σ' αυτήν. Εξασφαλίζεται με την κρυπτογράφηση των πακέτων που στέλνονται απ' τον αρχικό κόμβο και την αποκρυπτογράφησή τους απ' τον κόμβο παραλήπτη. Ανάλογα με τον τομέα εφαρμογής των WSN, η κρυπτογράφηση γίνεται είτε στο τμήμα δεδομένων του πακέτου είτε σε ολόκληρο το πακέτο (συμπεριλαμβανομένης της κεφαλίδας). Η κρυπτογράφηση του πλήρους πακέτου με την οποία αντιπαραβάλονται οι ταυτότητες των κόμβων απ την κεφαλίδα του πακέτου, βοηθά στην ελαχιστοποίηση των πιθανοτήτων κάποιος κόμβος να έχει πέσει θύμα επίθεσης και έτσι να εξασφαλίζεται η εμπιστευτικότητα στη διακίνηση της πληροφορίας μέσα στο δίκτυο.

3. **Ακεραιότητα:** Η ακεραιότητα εξασφαλίζει ότι ένα μήνυμα που ανταλλάχθηκε μεταξύ δύο κόμβων δεν τροποποιήθηκε απο κάποιον κακόβουλο χρήστη. Εάν πακέτα δρομολόγησης ή συγχρονισμού μεταξύ κόμβων τροποποιούνταν από κάποιον κακεντρεχή κόμβο τότε ολόκληρο το WSN θα μπορούσε να έρθει σε διακοπή. Ένας μηχανισμός ελέγχου δεδομένων για σφάλματα όπως είναι ο MAC (Message Authentication Code) μπορεί να χρησιμοποιηθεί για τυχόν τροποποιημένα δεδομένα. Στο σχήμα 2.2 παρουσιάζεται ο τρόπος με τον οποίο ελέγχεται η ακεραιότητα του μηνύματος από ένα κόμβο αποστολέα (SENDER) σε έναν κόμβο παραλήπτη (RECEIVER) με χρήση του κώδικα αυθεντικότητας μηνύματος (MAC) [69].



Σχήμα 2.2: Επαλήθευση ακεραιότητας μηνύματος με χρήση MAC

4. **Διαθεσιμότητα:** Η διαθεσιμότητα υποδεικνύει ότι το WSN θα πρέπει να λειτουργεί αδιάλειπτα και να παρέχει υπηρεσίες όταν απαιτείται. Η διαθεσιμότητα ελέγχεται μόνο όταν πρέπει να εξασφαλισθεί η αξιοπιστία τόσο στους κόμβους όσο και στο επιπέδο δικτύου και αυτό επιτυγχάνεται με την οικοδόμηση ανοχής σφαλμάτων τόσο στους μεμονωμένους κόμβους όσο και στο δίκτυο. Σχεδιάζοντας ένα σύστημα ενάντια στα διάφορα είδη επιθέσεων άρνησης υπηρεσιών (DoS attack) είναι επίσης ζωτικής σημασίας για την εγγυημένη διαθεσιμότητα σε ένα τέτοιο δίκτυο.

5. **Έλεγχος πρόσβασης:** Έλεγχος πρόσβασης σημαίνει ότι μονάχα οι νόμιμα εξουσιοδοτημένοι χρήστες έχουν δικαίωμα πρόσβασης στις υπηρεσίες του κόμβου.

2.5 Δευτερεύουσες απαιτήσεις ασφάλειας

Οι *δευτερεύουσες απαιτήσεις* ασφάλειας ενός ασύρματου δικτύου αισθητήρων είναι οι εξής:

1. **Φρεσκάδα δεδομένων:** Τα συστήματα WSN ως επί το πλείστον είτε καταγράφουν τις μετρήσεις που αντιλαμβάνονται (αισθάνονται) από το περιβάλλον τους και προωθούν τα δεδομένα-μετρήσεις είτε προωθούν κάποια δεδομένα σαν απάντηση σε κάποια συμβάντα. Και στις δύο περιπτώσεις είναι ζωτικής σημασίας τα δεδομένα

   να φθάσουν στον σταθμό βάσης όσο το συντομότερο δυνατόν (όσο τα δεδομένα δλδ είναι φρέσκα). Αυτό όχι μόνο μειώνει τη πιθανότητα τα επαναλαμβανόμενα πακέτα που στέλνονται από κάποιον κακόβουλο να παραπλανούν και να γίνονται δεκτά ως νόμιμα πακέτα αλλά διασφαλίζει επίσης ότι θα παρθούν οι σωστές αποφάσεις αντίδρασης στα συμβάντα που ανιχνεύονται από το ίδιο το δίκτυο. Για παράδειγμα σε μια εφαρμογή εντοπισμού θέσης, η θέση μπορεί να εντοπιστεί εφόσον τα τρέχοντα δεδομένα προωθούνται στον σταθμό βάσης. Η φρεσκάδα δεδομένων γενικά επιτυγχάνεται μέσα από αξιόπιστα συστήματα μεταφοράς και κανόνων δρομολόγησης που ελαχιστοποιούν τις απώλειες πακέτων και τις καθυστερήσεις.

2. **Διαχείριση Ισχύος:** Η κατανάλωση ισχύος αποτελεί την βασική ανησυχία λόγω των εγγενών ενεργειακών περιορισμών στους αισθητήριους κόμβους, καθώς λειτουργούν γενικά με μπαταρίες και μπορεί να μην είναι πρακτικό να αντικαθίστανται οι εξαντλημένες μπαταρίες στην περιοχή που αυτοί αναπτύσονται. Είναι σημαντικό λοιπόν να αναφέρουμε ότι οι επιθέσεις που ξεκίνησαν με στόχο να εξαντλήσουν την ισχύ των μπαταριών στους αισθητήριους κόμβους, έχουν την ικανότητα να επηρεάσουν αρνητικά την απόδοση ολόκληρου

του δικτύου, εάν ο εισβολέας ξεκινήσει την επίθεση απ' τον «κρίσιμο κόμβο», τον κόμβο δηλαδή που συνδέονται διαφορετικοί κόμβοι και που χρησιμεύει ως πύλη (sink κόμβος) προς άλλους κόμβους ή άλλα δίκτυα. Ο επιτιθέμενος μπορεί να θέσει στον κρίσιμο κόμβο ανεπιθύμητες ενημερώσεις δρομολόγησης, άσχετους υπολογισμούς ή ακόμη και να του αποστείλλει περιττά μηνύματα ελέγχου. Αυτό έχει σαν αποτέλεσμα την εξάντληση της μπαταρίας του «κρίσιμου κόμβου» και ως εκ τούτου μια πιθανή DoS επίθεση.

3. **Αυτο-Οργάνωση:** Το WSN έχει την τυπική μορφή ενός αυτοοργανωμένου (ad-hoc) δικτύου που δεν διαθέτει σταθερή ή κεντρική υποδομή για λόγους διαχείρισης δικτύου. Αυτός ο εγγενής περιορισμός στην αρχιτεκτονική του, θέτει μια τεράστια πρόκληση για την ασφάλειά του. Για να αντιμετωπιστεί επιτυχώς αυτός ο περιορισμός στην υποδομή (peer to peer), κάθε αισθητήριος κόμβος θα πρέπει να αυτο-οργανωθεί και να αυτοθεραπευτεί, ανεξάρτητα και ευέλικτα όπως επιτάσσει η εκάστοτε περίσταση. Εάν οι κόμβοι δεν διαθέτουν ικανότητα αυτο-οργάνωσης και αυτοθεραπείας, τότε η ζημιά που θα προέκυπτε από μια επίθεση ή φυσικά φαινόμενα, θα μπορούσε να αποβεί καταστροφική.

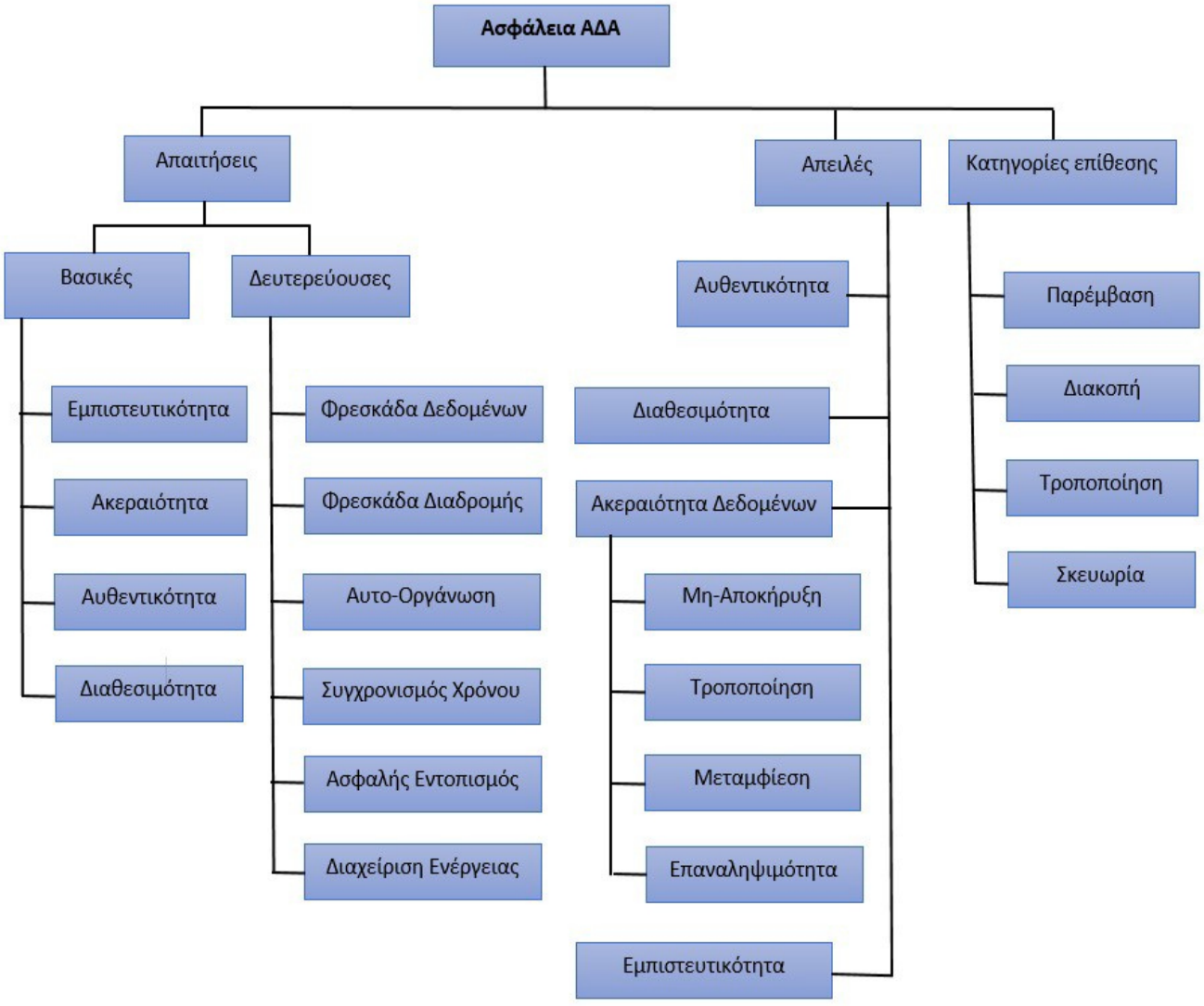
4. **Ασφαλής εντοπισμός:** Ο εντοπισμός είναι η διαδικασία καθορισμού των φυσικών συντεταγμένων των αισθητήριων κόμβων (ή μιας ομάδας κόμβων) ή της χωρικής σχέσης μεταξύ των αντικειμένων. Η ωφέλεια απ' τη χρήση ενός ασύρματου δικτύου αισθητήρων έγγειται στην ικανότητα των αισθητήριων κόμβων να προσδιορίζουν και να εντοπίζουν με ακρίβεια την τρέχουσα θέση των αισθητήριων κόμβων με τους οποίους θέλουν να επικοινωνήσουν. Ο άμεσος και με ακρίβεια εντοπισμός είναι υψίστης σημασίας εάν το δίκτυο αισθητήρων προορίζεται για λόγους επιτήρησης- παρακολούθησης. Ένα σημαντικό μειονέκτημα είναι ότι η θέση του αισθητήριου κόμβου μπορεί να προσδιοριστεί αβίαστα από τον

αντίπαλο μέσω αναφοράς ψευδών σημάτων ή επαναλήψης μηνυμάτων. Εάν υπάρξει όμως έστω και ένας προβληματικός κόμβος τότε το δίκτυο θα στείλει μια αναφορά προς όλους τους κόμβους του δικτύου, εξασφαλίζοντας έτσι την ασφάλεια.

5. **Συγχρονισμός χρόνου:** Τα ασύρματα δίκτυα αισθητήρων είναι κατανεμημένα συστήματα στα οποία κάθε κόμβος έχει το δικό του ρολόι και τον δικό του τομέα χρόνου. Τα περισσότερα χρησιμοποιούν έναν μετρητή χρόνου καθώς υπάρχουν καθυστερήσεις στο δίκτυο κυρίως καθυστερήσεις στην ανταλλαγή δεδομένων μεταξύ των κόμβων. Αυτές οι καθυστερήσεις μπορεί να αποβούν επικίνδυνες στην λειτουργία του δικτύου και αυτό γιατί ο επιτιθέμενος μπορεί να γεμίσει το δίκτυο με ψεύτικα πακέτα δεδομένων και να τα στείλει πολύ πιο γρήγορα απ' τα γνήσια πακέτα στον αποδέκτη, εκμεταλλευόμενος αυτές τις χρονικές καθυστερήσεις. Σε εφαρμογές παρακολούθησης, υπάρχει περισσότερο η ανάγκη για επίτευξη συγχρονισμού χρόνου στις συστοιχίες κόμβων.

6. **Φρεσκάδα διαδρομής:** Ακόμα κι αν εξασφαλίσουμε την ανανέωση των δεδομένων, υπάρχει ανάγκη να εξασφαλιστεί και η φρεσκάδα στη διαδρομή δικτύου. Καθώς οι κόμβοι αντιμετωπίζουν εγγενώς το πρόβλημα στην έλλειψη πόρων λόγω της περιορισμένης ικανότητας επεξεργασίας, αποθήκευσης και διαθεσιμότητας ενέργειας, ένας εισβολέας θα μπορούσε να υποδύονταν κάποιον κόμβο και να τον απέτρεπε απ' το να ενημερώσει τους πίνακες δρομολόγησής του. Επομένως, τα πρωτόκολλα δρομολόγησης θα πρέπει να είναι ευέλικτα και προσαρμοστικά σε κάθε αλλαγή στη τοπολογία δικτύου, διασφαλίζοντας έτσι τη φρεσκάδα διαδρομής.

Στο σχήμα 2.3 απεικονίζεται η δομή ασφάλειας στα ασύρματα δίκτυα αισθητήρων αποτελούμενη απο τις απειλές (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα, αυθεντικότητα), τις κατηγορίες επίθεσης (παρέμβαση, διακοπή, τροποποίηση, σκευωρία) και τους στόχους ασφάλειας [23].



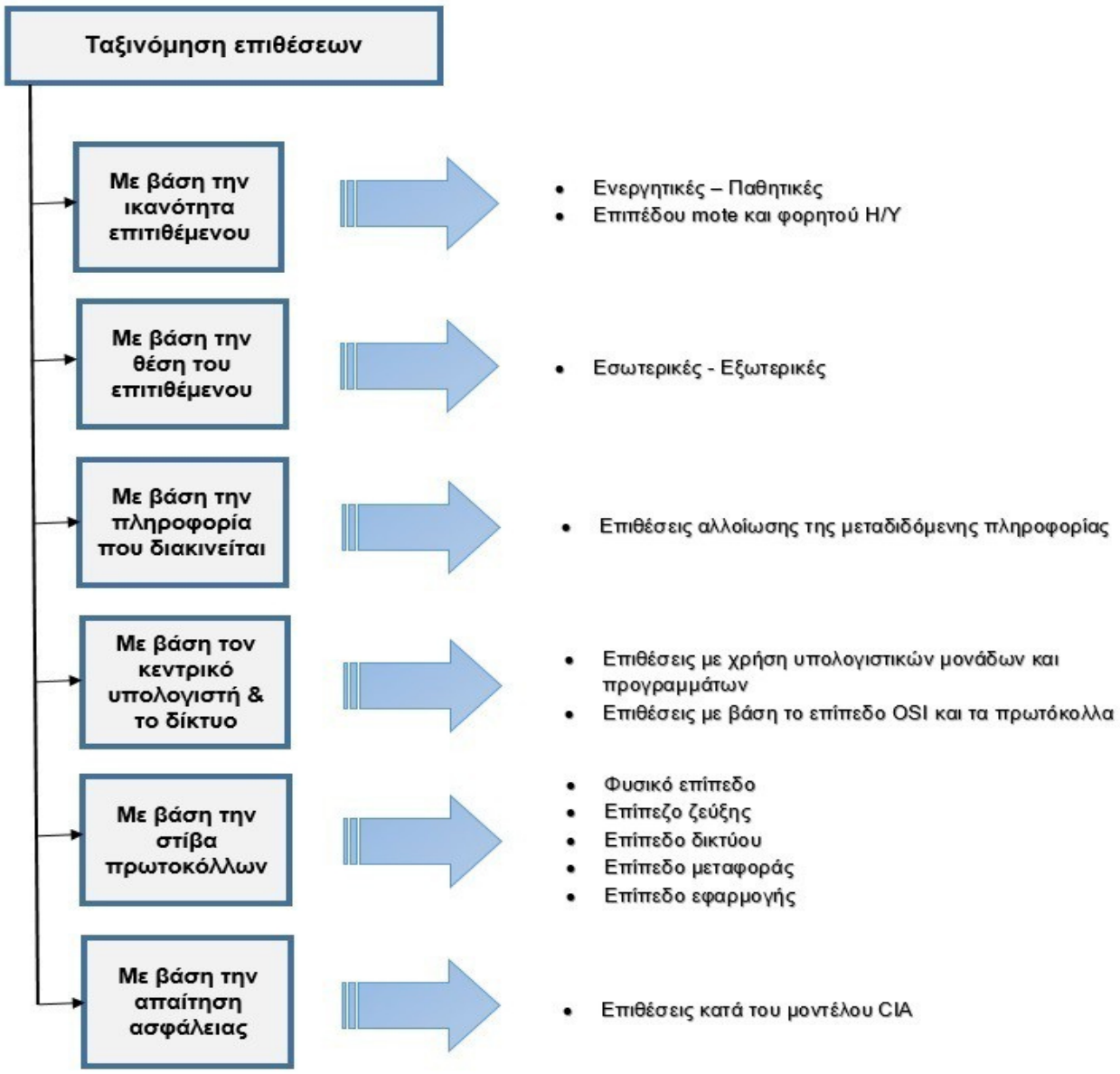
Σχήμα 2.3: Δομή ασφάλειας στα Ασύρματα Δίκτυα Αισθητήρων

ΚΕΦΑΛΑΙΟ 3

3.1 Ταξινόμηση επιθέσεων

Επιθέσεις ασφάλειας ορίζονται ως οι κακόβουλες ενέργειες “εξωτερικών” οντοτήτων με σκοπό τη πρόκληση δυσμενών συνεπειών (υποκλοπή, τροποποίηση, εισαγωγή ή διαγραφή μηνυμάτων) στη λειτουργία ενός WSN συστήματος. Οι επιθέσεις που λαμβάνουν χώρα στα Ασύρματα Δίκτυα Αισθητήρων κατηγοριοποιούνται (σχήμα 3.1) σε [72]:

- Ενεργές και Παθητικές
- Εσωτερικές και Εξωτερικές
- Επιπέδου φορητού υπολογιστή και mote επιπέδου
- Με βάση την πληροφορία που διακινείται στο δίκτυο
- Με βάση τον κεντρικό υπολογιστή και το δίκτυο
- Με βάση τα πακέτα δεδομένων
- Με βάση τη στίβα πρωτοκόλλων
- Με βάση την απαίτηση ασφάλειας



Σχήμα 3.1: Ταξινόμηση επιθέσεων στα WSN's

3.1.1 Ενεργές και Παθητικές επιθέσεις

Οι πιο σημαντικοί τύποι επιθέσεων είναι αυτοί που ταξινομούνται, ανάλογα με την ικανότητά τους να επηρεάζουν τη λειτουργικότητα ή όχι του δικτύου, σε Ενεργές και Παθητικές.

Επιθέσεις που μπορούν να επηρεάσουν τη λειτουργικότητα του δικτύου ονομάζονται *Ενεργές* επιθέσεις ενω αυτές που δεν μπορούν να επηρεάσουν τη λειτουργικότητα του δικτύου ονομάζοντα *Παθητικές* επιθέσεις.

α) *Παθητικές επιθέσεις*: Ένας κακόβουλος, μη εξουσιοδοτημένος κόμβος παρακολουθεί και ακούει το κανάλι επικοινωνίας. Αυτός ο τύπος επίθεσης είναι δύσκολο να εντοπιστεί αφού ο εισβολέας δεν συνεισφέρει δεδομένα στο κανάλι επικοινωνίας. Ο στόχος του επιτιθέμενου είναι να συγκεντρώσει εμπιστευτικής διαβάθμισης πληροφορίες και να προετοιμαστεί για μια ενεργή επίθεση.

β) *Ενεργές Επιθέσεις:* Ένας κακόβουλος, μη εξουσιοδοτημένος κόμβος παρακολουθεί, ακούει και τροποποιεί τη ροή δεδομένων στο κανάλι επικοινωνίας. Σε αυτόν τον τύπο επίθεσης, ο εισβολέας παίζει ενεργό ρόλο και προσποιείται στους υπόλοιπους ως ένας έγκυρος κόμβος. Μπορεί να τροποποιείσει τα μηνύματα μετάδοσης όπως επίσης και να προκαλέσει άρνηση παροχής υπηρεσιών

3.1.2 Εσωτερικές και Εξωτερικές επιθέσεις

Οι επιθέσεις σε ένα WSN δίκτυο μπορούν επίσης να κατηγοριοποιηθούν με βάση την θέση του επιτιθέμενου απέναντι στον υποψήφιο στόχο του που δεν είναι άλλος από το δίκτυο. Τις διακρίνουμε λοιπόν σε *Εσωτερικές* έαν η επίθεση πηγάζει από κάποιον κόμβο που αποτελεί κομμάτι του ίδιου του δικτύου ή *Εξωτερικές* εάν η επίθεση πηγάζει από κάποιον κόμβο/συσκευή που δεν αποτελούν όμως κομμάτι του δικτύου. Αξίζει να σημειωθεί ότι μια επίθεση που λαμβάνει χώρα απο μια εξωτερική οντότητα (κόμβος/συσκευή) η οποία μετέπειτα εξουσιοδοτείται να εισέλθει στο δίκτυο και κατόπιν τούτου να εκμεταλλευτεί τα δικαιώματα που κέρδισε ξεκινώντας επιθέσεις στο WSN, ταξινομείται τελικά σε εσωτερική επίθεση.

3.1.3 Επίθεση επιπέδου φορητού υπολογιστή και mote

Σε μια επίθεση επιπέδου φορητού υπολογιστή, ο επιτιθέμενος χρησιμοποιεί δυναμικές συσκευές για να γίνει περισσότερο πειστικός στο ΑΔΑ. Αυτές οι συσκευές έχουν αυξημένη ικανότητα μεταφοράς μέσα στο δίκτυο.

Σε μια επίθεση mote επιπέδου, ο επιτιθέμενος χρησιμοποιεί μερικούς κόμβους παρόμοιων δυνατοτήτων με αυτές των κόμβων του δικτύου.

3.1.4 Με βάση τη πληροφορία που διακινείται στο δίκτυο

Οποιαδήποτε αλλαγή υπάρξει στο δίκτυο ανιχνεύεται από τους αισθητήριους κόμβους αναφέροντας σχετικά στον σταθμό βάσης ή στους γείτονες κόμβους. Κατά την αποστολή αυτής της ενημέρωσης, η πληροφορία που διακινείται στο δίκτυο μπορεί να υποκλαπεί από κάποιον επιτιθέμενο με στόχο την αλλοίωση της και κατ' επέκταση την λανθασμένη ενημέρωση του σταθμού βάσης και των γείτονων κόμβων. Τέτοιες επιθέσεις αποτελούν οι DoS, καταγραφή κόμβου, υπερχείλισης, επανάληψης, υποκλοπής.

3.1.5 Με βάση τον κεντρικό υπολογιστή και το δίκτυο

Είναι οι επιθέσεις στις οποίες γίνεται χρήση υπολογιστικών μονάδων και εφαρμογών προκειμένου να υποκλέψουν τους κωδικούς και τα κλειδιά από τους αισθητήριους κόμβους. Σε αυτές ανήκουν οι επιθέσεις της υποκλοπής, υπερχείλιση μνήμης.

Οι επιθέσεις βάσει δικτύου διενεργούνται άλλοτε με βάση το επίπεδο και άλλοτε βάσει του πρωτοκόλλου. Ο επιτιθέμενος δημιουργεί συνθήκες παραβίασης της εμπιστευτικότητας των δεδομένων, απόριψης των πακέτων, λανθασμένης δρομολόγησης κ.ά.

3.1.6 Επίθεση με βάση τα πακέτα δεδομένων

Ο επιτιθέμενος μπορεί να τροποποιήσει τμήμα ή ολόκληρο το πακέτο και στη συνέχεια να το προωθήσει σε διαφορετική κατεύθυνση απ' αυτή που αρχικώς προορίζονταν, ανιχνεύοντας (sniffing), επαναλαμβανοντας, ή απορίπτοντας πακέτα.

3.1.7 Επίθεση με βάση τη στίβα πρωτοκόλλων

Εδώ οι επιθέσεις που εκδηλώνονται βασίζονται στα επίπεδα του μοντέλου OSI. Κάθε επίπεδο μπορεί να διακόψει τη λειτουργία του εξαιτίας αυτών των επιθέσεων. Υπάρχουν αρκετά πρωτόκολλα που χρησιμοποιούνται στα WSN συστήματα για να τα προστατέψουν από κακεντρεχής κόμβους. Σε αυτές τις επιθέσεις ανήκουν οι jamming, wormhole, παραβίασης, σύγκρουσης, βασισμένη σε μονοπάτι DoS κ.ά.

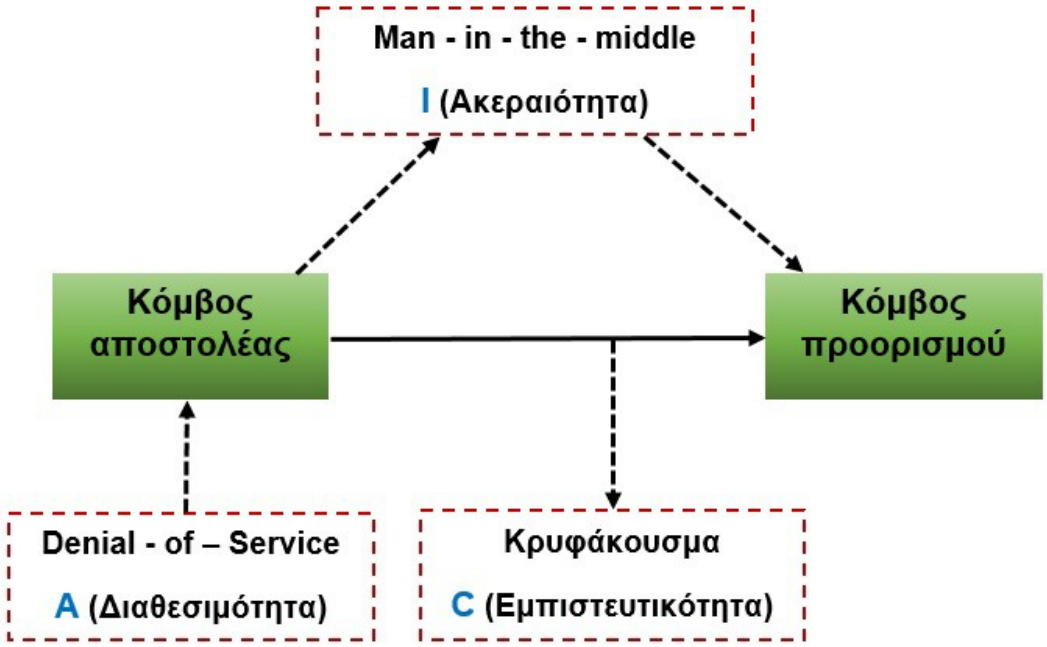
3.1.8 Επίθεση με βάση την απαίτηση ασφάλειας

Οι επιθέσεις μπορούν επίσης να ταξινομηθούν με βάση την απαίτηση ασφάλειας (σχήμα 3.2), στην οποία στοχεύουν. Με τον τρόπο αυτό προκύπτουν οι επιθέσεις ασφαλείας κατά:

(α) της εμπιστευτικότητας και αυθεντικότητας ενός ΑΔΑ συστήματος: Στοχεύουν σε υποκλοπή ή τροποποίηση δεδομένων και αντιμετωπίζονται με τεχνικές κρυπτογράφησης προστατεύοντας το απόρρητο μεταξύ των καναλιών απέναντι σε εξωτερικές επιθέσεις.

(β) της διαθεσιμότητας με επιθέσεις άρνησης εξυπηρέτησης (DoS) ή

(γ) της ακεραιότητας των υπηρεσιών εκχωρώντας εσφαλμένες τιμές στο δίκτυο μέσω κρυφών επιθέσεων.

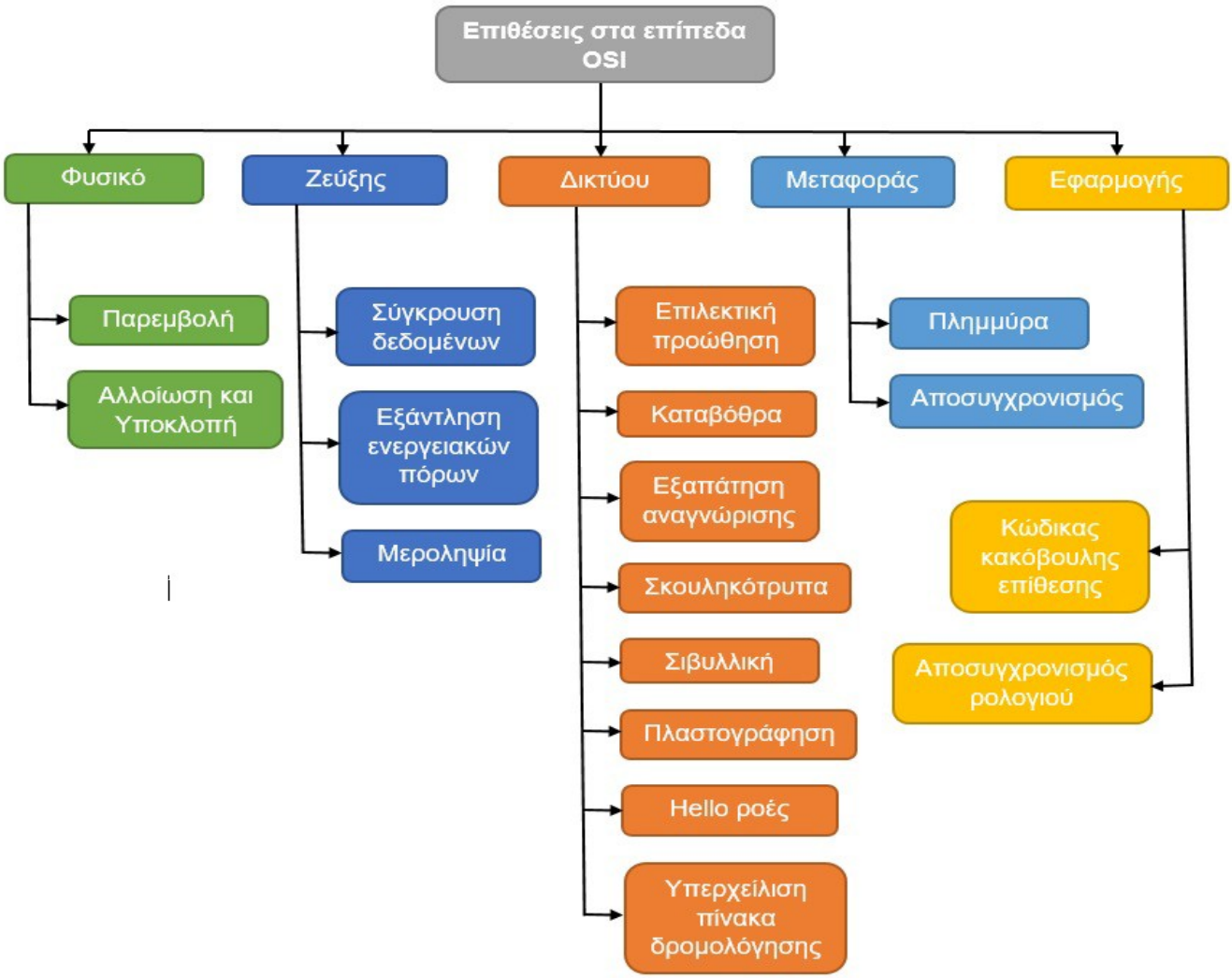


Σχήμα 3.2: Παράδειγμα επίθεσης κατά την επικοινωνία αποστολέα κόμβου και κόμβου παραλήπτη και παραβίαση μοντέλου ασφάλειας CIA

Για την επίτευξη των σκοπών του, ο επιτιθέμενος στοχεύει στις λειτουργίες του δικτύου, οι οποίες δεν υλοποιούνται μεμονωμένα αλλά σύμφωνα με την πολυεπίπεδη αρχιτεκτονική στα ασύρματα δίκτυα αισθητήρων, όπως αυτή περιγράφηκε στο Κεφάλαιο 1. Άλλωστε είναι και ο λόγος που οι επιθέσεις αναλύονται στη βιβλιογραφία ξεχωριστά ανά επίπεδο σχεδίασης, στο οποίο ανήκει και η λειτουργία που προσβάλλεται.

3.2 Επιθέσεις άρνησης εξυπηρέτησης (Denial Of Service DoS)

Οι επιθέσεις άρνησης εξυπηρέτησης ορίζονται ως οι επιθέσεις κατά της διαθεσιμότητας του δικτύου με στόχο να διαταράξουν τις λειτουργίες του, μειώνοντας ή εξαλείφοντας την ικανότητά του να εκτελεί τις αναμενόμενες λειτουργίες του, όπως επίσης και να διακόψουν, υπονομεύσουν και να καταστρέψουν το ίδιο το δίκτυο. Οι συγκεκριμένες επιθέσεις δύναται να προκαλέσουν σφάλματα υλικού και λογισμικού, εξάντληση πόρων ή συνδυασμό αυτών. Στη βιβλιογραφία υπάρχουν αρκετές τεχνικές αντιμετώπισης των συγκεκριμένων επιθέσεων ωστόσο ο σχεδιασμός των μηχανισμών άμυνας απαιτεί υψηλή υπολογιστική ισχύ και αυτό είναι δύσκολο να επιτευχθεί λόγω των περιορισμών σε πόρους. Από τη στιγμή που οι DoS επιθέσεις μπορεί να αποβούν μοιραίες για την λειτουργία του δικτύου με το αντίστοιχο κόστος που έχει κάθε φορά, οι ερευνητές έχουν καταβάλει μεγάλη προσπάθεια στον εντοπισμό τους αλλά και στον σχεδιασμό κατάλληλων στρατηγικών αντιμετώπισης σε ανάλογες επιθέσεις. Μερικές από τις πιο σημαντικές επιθέσεις ανά επίπεδο σχεδίασης (σχήμα 3.3) περιγράφονται παρακάτω [18] [23] [25] [27] [29] [34] [38].



Σχήμα 3.3: Επιθέσεις με βάση τη στίβα πρωτοκόλλων (μοντέλο OSI)

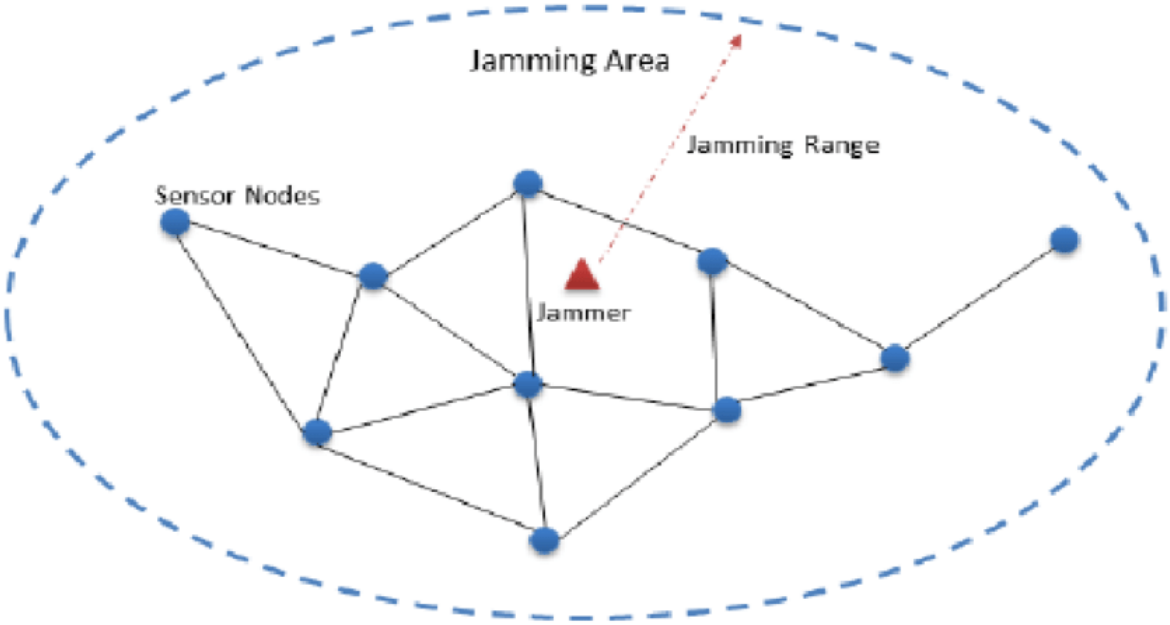
3.2.1 Φυσικό επίπεδο

Το φυσικό επίπεδο καθορίζει την επιλογή στη συχνότητα λειτουργίας, τη παραγωγή της φέρουσας συχνότητας, την ανίχνευση και διαμόρφωση σήματος καθώς και την κρυπτογράφηση των δεδομένων [31]. Το γεγονός ότι το χρησιμοποιούμενο μέσο μετάδοσης είναι ασύρματο, σημαίνει ότι ο επιτιθέμενος

ενδέχεται να έχει πρόσβαση σε αυτό και ως εκ τούτου το καθιστά αυτομάτως ευάλωτο σε επιθέσεις παρεμβολής και τροποποίησης δεδομένων. Οι επιθέσεις στο φυσικό επίπεδο στοχεύουν στο υλικό και ενώ από τη μια έχουν την ικανότητα να εκτελεστούν με απλό τρόπο, από την άλλη χρειάζονται πρόσβαση σε κάποιο σημείο του υλικού για να είναι σε θέση να επηρεάσουν την ευρύτερη λειτουργία του δικτύου. Ας δούμε λοιπόν τις επιθέσεις αυτές και τον τρόπο που αποκτούν πρόσβαση στις λειτουργίες του φυσικού επιπέδου με σκοπό να βλάψουν το υλικό.

- Επίθεση παρεμβολής (jamming attack)

  Η επίθεση παρεμβολής μπορεί να ξεκινήσει από κάποιον επιτιθέμενο τόσο εξωτερικά όσο και εσωτερικά του δικτύου. Για να ξεκινήσει μια επίθεση παρεμβολής χρησιμοποιείται ένας πομπός υψηλής ισχύος, δημιουργώντας ένα σήμα (θόρυβο) αρκετά ισχυρό ώστε να παρεμποδίσει την ορθή λειτουργία στην ασύρματη επικοινωνία. Το αποτέλεσμα αυτής της παρεμβολής είναι είτε να αποτραπεί η μετάδοση του πακέτου από μια πραγματική πηγή, είτε να παρεμποδιστεί η λήψη νόμιμων πακέτων από κάποιον αποδέκτη. Για τον αντίπαλο, η επίθεση παρεμβολής έχει μεγάλο βαθμό δυσκολίας, λόγω της δυναμικής τοπολογίας του ασύρματου δικτύου και της συχνής αλλαγής στις θέσεις των αισθητήριων κόμβων. Στο σχήμα 3.4 απεικονίζεται η περιοχή επίθεσης εντός της οποίας ο επιτιθέμενος έχει τοποθετήσει μια συσκευή παραμβολής παρεμποδίζοντας έτσι την επικοινωνία μεταξύ των αισθητήριων κόμβων.



Σχήμα 3.4: Επίθεση παρεμβολής (jamming)

- Επίθεση αλλοίωσης και υποκλοπής (tampering attack)

  Τα WSNs λειτουργούν συνήθως σε εχθρικές και απομακρυσμένες περιβαλλοντικές συνθήκες. Εκτεθιμένα και χωρίς επίβλεψη σε αυτά τα περιβάλλοντα, καθίστανται ευάλωτα σε φυσικές επιθέσεις. Ο επιτιθέμενος μπορεί να καταστρέψει τον κόμβο με φυσική παρουσία, να παρεμποδίσει το σχετικό κύκλωμα, να εκβιάσει τη συλλογή κρυπτογραφημένων στοιχείων, να τροποποιήσει την κωδικοποίηση στους αισθητήριους κόμβους, να αντικαταστήσει τους κωδικούς με αυτούς των αισθητήρων που βρίσκονται εντός του εύρους και του ελέγχου του επιτιθέμενου ή ακόμη και να αντικαταστήσει τους κόμβους με κεκεντρεχής κόμβους.

3.2.2 Επίπεδο ζεύξης

Το επίπεδο ζεύξης είναι υπεύθυνο για την πολυπλεξία και την ανίχνευση των δεδομένων, τον έλεγχο σφαλμάτων και τη πρόσβαση στο μέσο μετάδοσης [31]. Οι επιθέσεις που λαμβάνουν χώρα σε αυτό το επίπεδο δημιουργούν συσγκρούσεις δεδομένων, εξάντληση ενεργειακών πόρων καθώς και μεροληψία στη κατανομή αυτών.

- Σύγκρουση δεδομένων (Collision)
  Σύγκρουση των δεδομένων μπορεί να συμβεί μεταξύ δύο κόμβων όταν μεταφέρουν ταυτόχρονα πακέτα χρησιμοποιώντας το ίδιο κανάλι επικοινωνίας. Τα πρωτόκολλα MAC γενικότερα βοηθούν έτσι ώστε να διασφαλιστεί ότι οι αισθητήριοι κόμβοι χρησιμοποιούν αποτελεσματικά το διαμοιραζόμενο κανάλι επικοινωνίας. Όταν ένας κόμβος του δικτύου όμως παραβιάζει τους μηχανισμούς του πρωτοκόλλου MAC (πχ στέλνοντας ταυτόχρονα δεδομένα με έναν άλλο κόμβο που βρισκόνταν ήδη σε διαδικασία αποστολής πακέτων) προκαλούνται συγκρούσεις δεδομένων. Ανάλογα με το βαθμό παραβίασης του πρωτοκόλου MAC, οι συγκρούσεις μπορεί να προκαλέσουν ένα ευρύ φάσμα προβλημάτων όπως:
  - Ολική καταστροφή-απώλεια των πακέτων δεδομένων
  - Αλόγιστη - αθέμιτη χρήση εύρους ζώνης του δικτύου
  - Σφάλματα στο δίκτυο
  - Όλική άρνηση υπηρεσιών (DoS) εάν ο κακόβουλος αποστολέας καταλαμβάνει διαρκώς το κανάλι και (ή) οι κακεντρεχής κόμβοι συνεχώς επανεκπέμπουν κατεστραμμένα πακέτα

- Εξάντληση ενεργειακών πόρων (Exhaustion)
  Όταν έχει παραβιαστεί το πρωτόκολο MAC και επανεκπέμπονται συνεχώς τα κατεστραμμένα πακέτα λόγω των συνεχή συγκρούσεων, οι κόμβοι κατασπαταλούν τα ενεργειακά τους αποθέματα μέχρι ότου φτάσουν στην ολική τους εξάντληση.

- Μεροληψία (Unfairness)

  Η μεροληψία είναι μια αδύναμη μορφή επίθεσης DoS. Ο επιτιθέμενος μπορεί να προκαλέσει μεροληψία χρησιμοποιώντας κατα διαστήματα μία από τις επιθέσεις επιπέδου ζεύξης που αναλύσαμε πιο πάνω. Σε αυτή τη περίπτωση ο επιτιθέμενος προκαλεί την υποβάθμιση των προγραμματισμένων εργασιών των μη μολυσμένων κόμβων που εκτελούνται σε πραγματικό χρόνο, διακόπτωντας ανα διαστήματα τις αποστολές των πακέτων

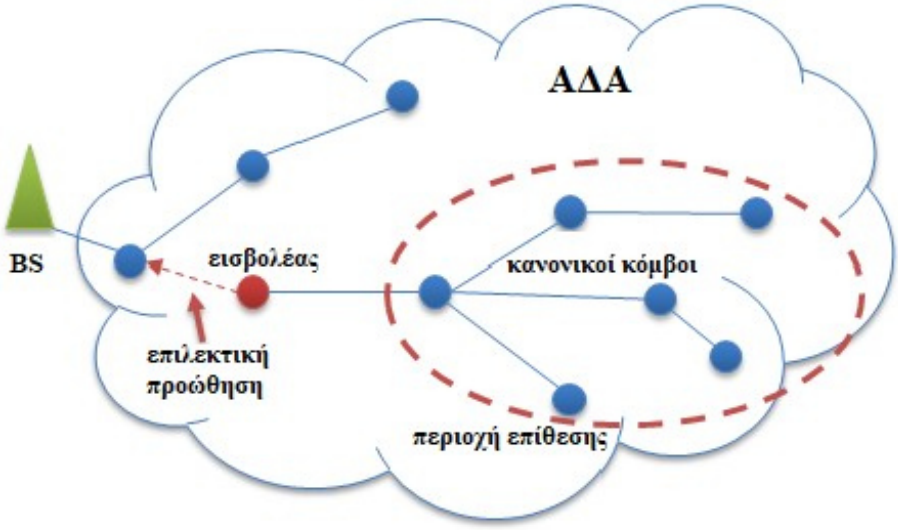
3.2.3 Επίπεδο δικτύου

Το επίπεδο δικτύου είναι υπεύθυνο για τη δρομολόγηση των πακέτων στο δίκτυο διαμέσου των αισθητήριων κόμβων. Ως εκ τούτου, οποιαδήποτε επίθεση που λαμβάνει χώρα σε αυτό το επίπεδο, έχει ως αποτέλεσμα τις δυσλειτουργίες στη δρομολόγηση αυτών των πακέτων [31]. Οι πιο σημαντικές επιθέσεις που συντάμε σε αυτό το επίπεδο αναφέρονται και αναλύονται παρακάτω:

- Επιλεκτική προώθηση (Selective forwarding)

  Σε ένα ασύρματο δίκτυο αισθητήρων κάθε κόμβος που λαμβάνει ένα μήνυμα, έχει την υποχρέωση να το προωθήσει στον γειτονικό του κόμβο και αυτή η διαδικασία επαναλαμβάνεται συνεχώς μέχρις ότου το μήνυμα παραληφθεί απο όλους τους κόμβους του δικτύου. Στη περίπτωση όμως που το δίκτυο έχει προσβληθεί απο κάποιον κακόβουλο, ο κακεντρεχής κόμβος θα επιλέξει να προωθήσει μερικά από τα μηνύματα ενώ τα υπόλοιπα τα απορρίπτει (σχήμα 3.5). Έτσι λοιπόν τα πακέτα δεδομένων ακολουθούν τη διαδρομή στο δίκτυο σύμφωνα με την επιλογή του εισβολέα και όχι με βάση αυτό που ορίζει το εκάστοτε πρωτόκολο δρομολόγησης. Η επίθεση επιλεκτικής προώθησης αντιπαραβάλεται κατα κάποιον τρόπο με την επίθεση “μαύρης τρύπας”

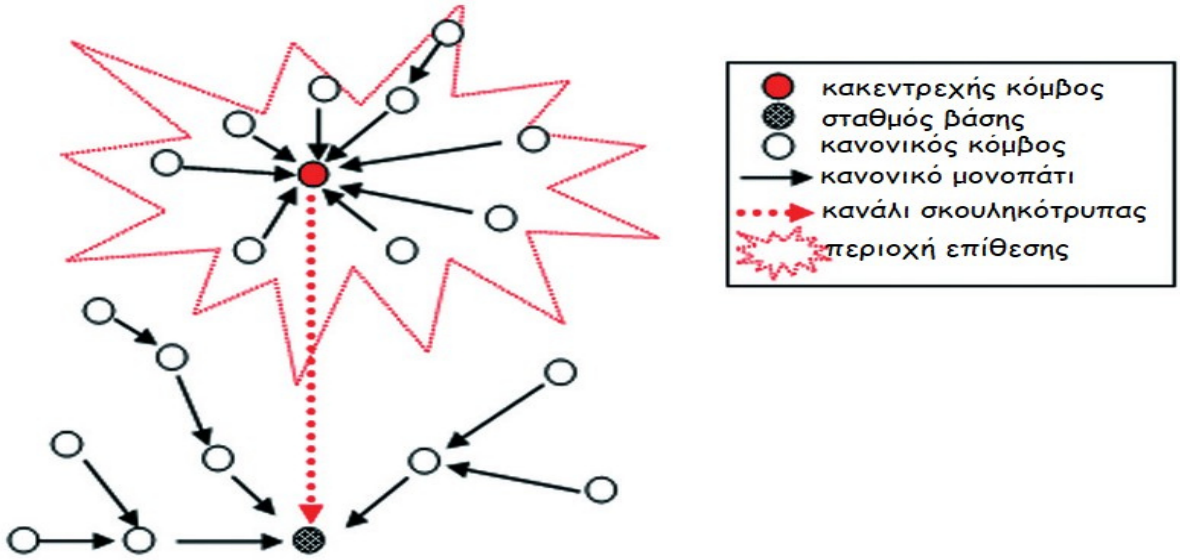
(blackhole attack) κατα την διάρκεια της οποίας, ο προσβεβλημένος κόμβος απορίπτει όλα τα πακέτα που λαμβάνει χωρίς καν να τα προωθεί [33].



Σχήμα 3.5: Παράδειγμα επίθεσης επιλεκτικής προώθησης (selective forwarding)

- Επίθεση καταβόθρας (Sinkhole attack)

  Είναι είδος επίθεσης κατα την οποία ο κακεντρεχής κόμβος μοιάζει να είναι ο περισσότερο ελκυστικός κόμβος μιας ιδιαίτερης περιοχής του δικτύου με αποτέλεσμα οι γειτονικοί κόμβοι να προωθούν τα δεδομένα σε αυτόν βλέποντάς τον σαν το επόμενο hop. Η επίθεση καταβόθρας [60] είναι υπεύθυνη για την εμφάνιση της επίθεσης επιλεκτικής προώθησης και αυτό γιατί προσπαθεί μέσω του κακεντρεχή κόμβου να προσελκύσει όλη τη κίνηση των πακέτων μιας μεγάλης περιοχής του δικτύου, προωθώντας συγκεκριμένα - επιλεκτικά πακέτα. Στο σχήμα 3.6, εντός της κόκκινης περιοχής εκδηλώνεται μια sinkhole επίθεση. Ο κόκκινος κόμβος (κακεντρεχής κόμβος) προσπαθεί να προσελκύσει όλη τη κίνηση των πακέτων από τους γειτονικούς του κόμβους, για να την δρομολογήσει στη συνέχεια μέσω τεχνητού καναλιού στον σταθμό βάσης



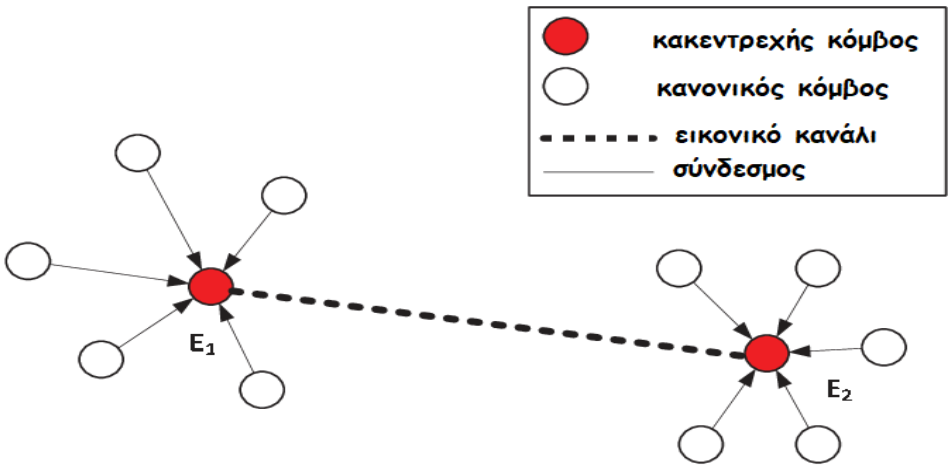
Σχήμα 3.6: Sinkhole επίθεση σε WSN δίκτυο με χρήση τεχνητού καναλιού δρομολόγησης

- Εξαπάτηση αναγνώρισης (Acknowledgment spoofing)

  Όταν ένας κόμβος Α στέλνει δεδομένα σε έναν κόμβο Β, οι αλγόριθμοι δρομολόγησης στο WSN δίκτυο απαιτούν από τον Β (ρητά ή σιωπηρά) να στείλει κάποιο αναγνωριστικό στον Α, σαν επιβεβαίωση της ορθής λήψης των πακέτων δεδομένων. Ωστόσο ένας κακόβουλος κόμβος Γ, γνωρίζοντας τα δεδομένα που ανταλλάχθησαν μεταξύ Α και Β και υποδυόμενος τον κόμβο Β, μπορεί να στείλει πληροφορίες επιβεβαίωσης προς τον Α, ο οποίος θα πίστευε ότι η αναγνώριση προέρχεται από τον Β. Μία τέτοια επίθεση θα μπορούσε να ξεγελάσει τον κόμβο Α, προκαλώντας αστάθεια στους κανόνες δρομολόγησης μέσα στο WSN δίκτυο μεταδίδοντας ψευδής πληροφορίες.

- Επίθεση σκουληκότρυπας (Wormhole attack)

  Με την επίθεση σκουληκότρυπας προκαλείται η ψευδαίσθηση σε δύο απομακρυσμένους κόμβους, μιας διαδρομής μικρότερης απ' όσο θα απείχαν στη πραγματικότητα, δημιουργώντας παράλληλα ένα εικονικό κανάλι σκουληκότρυπας μεταξύ τους. Αυτό μπορεί να μπερδέψει τους μηχανισμούς δρομολόγησης που στηρίζονται στη πληροφορία της απόστασης μεταξύ των κόμβων [12] [13] [59]. Οι επιθέσεις wormhole μπορούν να χρησιμοποιηθούν σε συνδυασμό με τις επιθέσεις επιλεκτικής προώθησης ή τροποποίησης δεδομένων. Όταν δε συνδυαστεί με την σιβυλλική επίθεση, η ανίχνευσή της μοιάζει πολύ δύσκολη. Στο σχήμα 3.7 παρουσιάζεται μια επίθεση σκουληκότρυπας μεταξύ δύο απομακρυσμένων κόμβων.

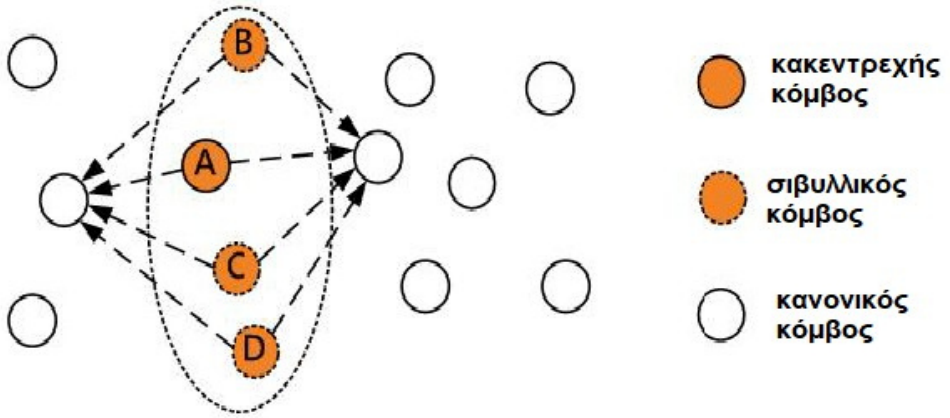


Σχήμα 3.7: Παράδειγμα wormhole επίθεσης σε WSN δίκτυο με χρήση τεχνητού καναλιού

- Σιβυλλική επίθεση (Sybil attack)

  Κατα τη διάρκεια μιας σιβυλλικής επίθεσης ο επιτιθέμενος παρουσιάζεται με πολλές ταυτότητες μέσα στο δίκτυο. Ομοίως στα πρωτόκολλα δρομολόγησης βασισμένα σε γεωγραφική περιοχή, ένας εισβολέας

ισχυρίζεται ότι βρίσκεται ταυτόχρονα σε πολλές γεωγραφικές περιοχές. Εάν οι περισσότεροι κόμβοι του δικτύου πιστέψουν ότι αυτός ο κακεντρεχής κόμβος είναι ο γείτονάς τους, υπάρχει μεγάλη πιθανότητα ότι θα τον επιλέξουν ως τον next hop κόμβο για να προωθήσουν τα δεδομένα τους με αποτέλεσμα την ταχύτερη ενεργειακή τους απόσβεση. Αυτός είναι άλλωστε και ο στόχος της συγκεκριμένης επίθεσης, να εξαντλήσουν δλδ την ενέργεια των κόμβων σε ένα WSN δίκτυο μέσω των πολλαπλών εικονικών κόμβων (σιβυλλικών κόμβων) αν και αποτελούν στη πραγματικότητα μόνο μία συσκευή (σχήμα 3.8).



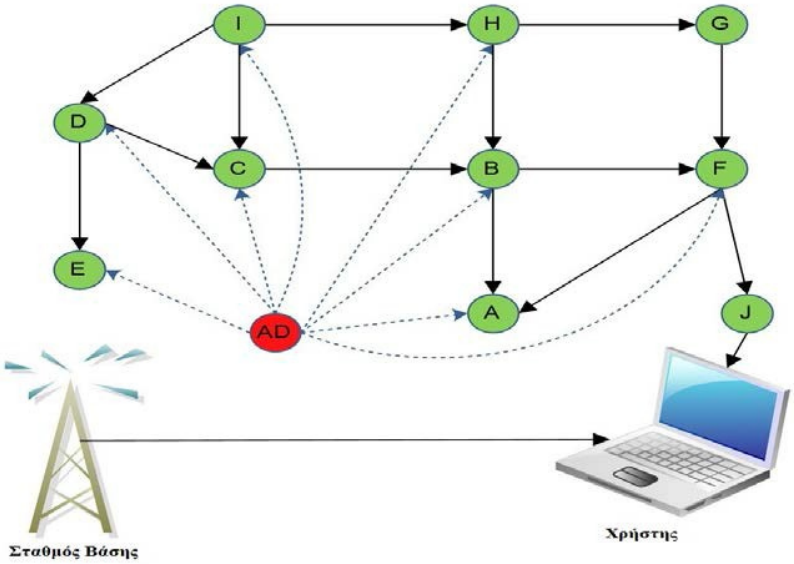
Σχήμα 3.8: Παράδειγμα Σιβυλλικής επίθεσης

- Πλαστογράφηση, τροποποίηση ή αντικατάσταση πληροφοριών δρομολόγησης

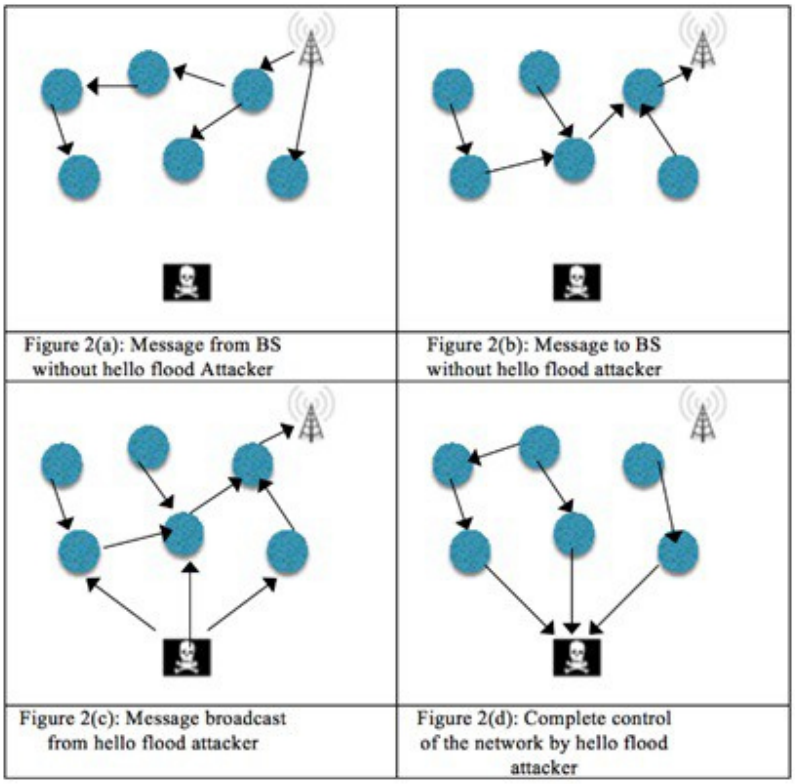
  Η πιο άμεση επίθεση ενάντια κάποιου πρωτοκόλλου δρομολόγησης είναι να στοχεύσει στις πληροφορίες δρομολόγησης του δικτύου. Ο εισβολέας μπορεί να πλαστογραφήσει, να τροποποιήσει ή να επαναλάβει τις πληροφορίες δρονολόγησης με στόχο την διακοπή στην ανταλλαγή πληροφοριών δρομολόγησης. Οι τεχνικές που χρησιμοποιούνται απο τον εισβολέα είναι η δημιουργία βρόχων δρομολόγησης, η απώθηση ή

προσέλκυση του δικτύου απ' τους κακεντρεχής κόμβους, η επέκταση ή συντόμευση πηγαίων διαδρομών, η δημιουργία ψευδών μηνυμάτων σφάλματος, προκαλώντας έτσι διαμερισμό του δικτύου και αύξηση απο άκρη σε άκρη της αδράνειάς του.

- Επίθεση Hello ροών (Hello flood)
  Ο εισβολέας χρησιμοποιώντας ένα υπολογιστικό μέσο (πχ laptop) μπορεί να στείλει δρομολογήσεις ή άλλες πληροφορίες (πακέτα Hello) με αρκετά μεγάλη ισχύ μετάδοσης σε όλους τους κόμβους του δικτύου, με απώτερο σκοπό να πείσει κάθε κόμβο ότι δεν αποτελεί περίπτωση εισβολέα. Μόλις οι γειτονικοί κόμβοι πειστούν ότι δεν υπάρχει καμία απειλή, θα αναγνωρίσουν τον εισβολέα ως γείτονα, ανταλλάσοντας πληροφορίες μεταξύ τους [35]. Οι επιθέσεις Hello ροών επηρεάζουν τα πρωτόκολλα που εξαρτώνται από τις τοπικές πληροφορίες που ανταλλάσονται μεταξύ των γειτονικών κόμβων. Στα σχήματα 3.9 και 3.10 παρουσιάζεται ο τρόπος εκδήλωσης μια επίθεσης Hello ροών.



Σχήμα 3.9: Παράδειγμα επίθεσης Hello ροών με χρήση υπολογιστή



Σχήμα 3.10: Επικοινωνία με τον σταθμό βάσης προ και μετά επίθεσης Hello ροών

- Υπερχείλιση πίνακα δρομολόγησης (Routing table overflow)

  Η δηλητηρίαση μιας διαδρομής μπορεί επίσης να προκληθεί από υπερχείλιση δεδομένων στους πίνακες δρομολόγησης των κόμβων. Συγκεκριμένα, στέλνοντας συνέχεια “κενή” πληροφορία δρομολόγησης στο δίκτυο, ένας επιτιθέμενος θα μπορούσε να εξασφαλίσει ότι οι κόμβοι θα έχουν συνεχώς ψευδής πληροφορίες στους πίνακες δρομολόγησής τους, με ελάχιστο ή καθόλου διαθέσιμο χώρο στο buffer για καταχώρηση μιας αληθούς πληροφορίας δρομολόγησης.

3.2.4 Επίπεδο Μεταφοράς

Οι επιθέσεις που λαμβάνουν χώρα στο επίπεδο μεταφοράς είναι η πλημμύρα και ο αποσυγχρονισμός [31]

- Επίθεση πλημμύρας (Flooding)

  Όταν απαιτείται να επέμβει κάποιο πρωτόκολλο δρομολόγησης για την απο άκρη σε άκρη διατήρηση της κατάστασης μιας σύνδεσης, γίνεται ευάλωτο στο ενδεχόμενο εξάντλησης της μνήμης διαμέσου μιας επίθεσης πλημμυρίσματος. Ένας επιτιθέμενος μπορεί επανειλημμένα να στέλνει αιτήματα για νέα σύνδεση μέχρις ότου οι πόροι που απαιτούνται για αυτη τη σύνδεση είτε εξαντληθούν είτε φθάσουν στο μέγιστο όριο διαθεσιμότητας. Για οποιαδήποτε άλλη περίπτωση, τυχόν αιτήματα απορίπτονται.

- Επίθεση αποσυγχρονισμού (Desynchronization)

  Ο αποσυγχρονισμός αναφέρεται σε διακοπή μιας υπάρχουσας σύνδεσης. Ένας επιτιθέμενος για παράδειγμα μπορεί επανηλειμμένα να υποκλέπτει τα μηνύματα απο έναν αισθητήριο κόμβο υποχρεώνοντάς τον να ζητήσει την αναμετάδοση των χαμένων πακέτων. Η προσπάθεια επαναφοράς από τα

συνεχή σφάλματα, έχει ως αποτέλεσμα τον αποσυγχρονισμό των κόμβων και ως εκ τούτου την εξάντληση των ενεργειακών τους αποθεμάτων.

3.2.5 Επίπεδο Εφαρμογής

Το επίπεδο εφαρμογής παρουσιάζεται αρκετά ευάλωτο σε θέματα παραβίασης ασφάλειας συγκριτικά με τα υπόλοιπα επίπεδα της στοίβας πρωτοκόλλου επικοινωνίας [31] [23]. Σε αυτό το επίπεδο συναντάμε πρωτόκολλα όπως τα FTP, TELNET, HTTP και SMTP ανταλλάσοντας δεδομένα και όντας επιρρεπή σε επιθέσεις όπως αυτές που αναφέρονται παρακάτω.

- Κώδικας κακόβουλης επίθεσης (Malicious code)
  Κακόβουλοι κώδικες όπως τα σκουλήκια, οι ιοί, οι δούρειοι ίπποι, λογισμικό κατασκοπίας είναι ικανά να επιτεθούν τόσο στο λογισμικό του χρήστη όσο και στο λειτουργικό σύστημα της συσκευής. Τέτοιου είδους κακόβουλα προγράμματα συνήθως καταστρέφουν ή προκαλούν καθυστερήσεις στους υπολογισμούς και τα δίκτυα τους.

- Επίθεση αποσυγχρονισμού ρολογιού (Clock desynchronization)
  Η υπηρεσία συγχρονισμού ρολογιού που παρέχεται απο το επίπεδο εφαρμογής πρέπει να εκτελείται με πολύ υψηλή ακρίβεια. Μια επίθεση αποσυγχρονισμού ρολογιού μπορεί να ξεκινήσει μοιράζοντας πακέτα παραπλανητικά εντός δικτύου, αναγκάζοντας μερικούς κόμβους να προσαρμόσουν τα ρολόγια τους σε αυτά, χάνοντας τον συγχρονισμό τους με τους υπόλοιπους κόμβους του δικτύου και την σχετική υπηρεσία. Σε εφαρμογές για παράδειγμα ασύρματων δικτύων αισθητήρων όπου η καταγραφή του χρόνου χρησιμεύει για την εκτίμηση της ταχύτητας, τυχόν προβλήματα στον συγχρονισμό ρολογιού θα δημιουργούσε λάθος υπολογισμούς της μετρήσιμης ταχύτητας. Επίσης η αποφυγή καταγραφής τυχόν διπλών μετρήσεων από διαφορετικούς κόμβους βασίζεται στη σωστή λειτουργία της υπηρεσίας συγχρονισμού ρολογιού.

3.3 Επιθέσεις κατά της εμπιστευτικότητας και της αυθεντικότητας

Αυτές οι επιθέσεις στοχεύουν σε υποκλοπή ή τροποποίηση δεδομένων και αντιμετωπίζονται με τεχνικές κρυπτογράφησης προστατεύοντας το απόρρητο μεταξύ των καναλιών απέναντι σε εξωτερικές επιθέσεις [31] [23] [25] [29]. Διακρίνονται στις εξής κατηγορίες

3.3.1 Τεχνική αναπαραγωγής κόμβου (Node replication) - Φυσική επίθεση

Τα ασύρματα δίκτυα αισθητήρων όπως ήδη έχουμε αναφέρει, αναπτύσσονται πολλές φορές σε απομακρυσμένες γεωγραφικά περιοχές (σε «εχθρικά» περιβάλλοντα) και η έλλειψη επιτήρησης τα καθιστουν αυτομάτως επιρρεπή σε φυσικές επιθέσεις. Η διαφορά των φυσικών επιθέσεων με αυτές που αναφέρθηκαν παραπάνω είναι το γεγονός ότι οι βλάβες στους κόμβους και στο ευρύτερο δίκτυο θα είναι μόνιμες και οι απώλεις μη αναστρέψιμες [39]. Ο επιτιθέμενος μπορεί να αποκρυπτογραφήσει διάφορες πληροφορίες, να αναλύσει τη διάταξη των κόμβων στον χώρο του δικτύου, να επέμβει στη λειτουργία τους παραμετροποιώντας τον κώδικα λειτουργίας τους ή ακόμη και να αντικαταστήσει κόμβους με άλλους κακόβουλους που είναι προγραμματισμένοι απ' αυτόν και βρίσκονται υπό τον πλήρη έλεγχό του (τεχνική αναπραγωγής κόμβου)

3.3.2 Επιθέσεις κατά του απορρήτου

Η αχίλλειος πτέρνα στη λειτουργία των ασύρματων δικτύων αισθητήρων αποτελούν οι πληροφορίες που συλλέγονται απ τους κόμβους και διακινούνται εντός του δικτύου. Αν και φαινομενικά είναι ακίνδυνες και κρυπτογραφημένες, υπάρχει δυνατότητα κατόπιν σχετικής συσχέτισης των δεδομένων και παράλληλης αποκρυπτογράφησή τους, να εξαχθούν χρήσιμες πληροφορίες για κάποιον που σκοπεύει να επιτεθεί. Η εργασία απομακρυσμένης πρόσβασης επιδεινώνει τη κατάσταση αφού δινεται η δυνατότητα στον επιτιθέμενο να διαχειρίζεται

απομακρυσμένα τις πληροφορίες χωρίς να απαιτείται φυσική παρουσία στον χώρο επιτήρησης. Οι πιο συνηθισμένες επιθέσεις κατά του απορρήτου είναι οι παρακάτω

- Παρακολούθηση και κρυφάκουσμα (monitoring and eavesdropping)
  Αποτελεί τη συνηθέστερη μορφή επίθεσης στο απόρρητο των δεδομένων [40]. Εαν τα μηνύματα δεν είναι προστατευμένα με τους κατάλληλους μηχανισμούς κρυπτογράφησης, ο αντίπαλος μπορεί πολύ εύκολα να κατανοήσει το περιεχόμενό τους. Τα πακέτα που περιέχουν πληροφορίες ελέγχου για το ασύρματο δίκτυο διακινούμενες μέσω ενός εξυπηρετητή τοποθεσίας, αποδεικνύονται περισσότερο ελκυστικά για έναν επιτιθέμενο προκειμένου να τα υποκλέψει.

- Ανάλυση κίνησης (traffic analysis)
  Προκειμένου να γίνει πιο αποτελεσματική η επίθεση κατά του απορρήτου, το κρυφάκουσμα θα μπορούσε να συνδυαστεί με την ανάλυση της κίνησης. Η ανάλυση της
  κίνησης του δικτύου έχει ως στόχο τον εντοπισμό και την αδρανοποίηση του σταθμού βάσης. Η ανάλυση της κίνησης μπορεί να επιτευχθεί με δύο τρόπους. Με την επίθεση καταγραφής ρυθμού (rate monitoring attack) ο επιτιθέμενος εντοπίζει τους κόμβους που στέλνουν τα περισσότερα πακέτα. Όπως είναι γνωστό οι κόμβοι που βρίσκονται πιο κοντά σ' ένα σταθμό βάσης διαχειρίζονται περισσότερες πληροφορίες, επομένως με την άνω επίθεση μπορεί να εντοπιστεί ο σταθμός βάσης. Στην επίθεση συσχέτισης χρόνου (time correlation attack) ο επιτιθέμενος παράγει ένα φυσικό γεγονός παρακολουθώντας κάθε φορά την κατεύθυνση μέχρι τον παραλήπτη [29].

- Παραλλαγή (camouflage)
  Ο επιτιθέμενος εκχωρεί στο δίκτυο κόμβους . Ο καμουφλαρισμένος κόμβος προσποιούμενος τον κανονικό, ανταλλάσει πληροφορίες δρομολόγησης με τους άλλους κόμβους και τις συγκεντρώνει εκεί που τον έχει ορίσει ο επιτιθέμενος. Αφού έχει συγκεντρωθεί ικανός αριθμός δεδομένων, στη συνέχεια γίνεται ανάλυση για την εκμαίευση απόρρητων πληροφοριών [29].

3.4 Σύνοψη

Στον πίνακα 3.1 παρουσιάζονται συνοπτικά οι τύποι των επιθέσεων που λαμβάνουν χώρα σε ένα ασύρματο δίκτυο αισθητήρων, με βάση την πολυεπίπεδη αρχιτεκτονική τους και το μοντέλο ασφάλειας CIA, με σχετική αναφορά στους στόχους της κάθε επίθεσης καθώς επίσης και το μοντέλο επίθεσης και τις προδιαγραφές που θέτουν κάθε φορά υπό αμφισβήτηση.

Πίνακας 3.1: Επιθέσεις στα ασύρματα δίκτυα αισθητήρων WSN's

Επίθεση	**Επίπεδο**	**Προδιαγραφή**	**Μοντέλο επίθεσης**		**Στόχος επίθεσης**
			Ενεργητική/ Παθητική	**Εσωτερική/ Εξωτερική**	
Παρεμβολή (jamming)	Φυσικό	Διαθεσιμότητα Ακεραιότητα	Ενεργητική	Εσωτερική Εξωτερική	Πλημμύρισμα τμήματος του δικτύου με θόρυβο
Αλλοίωση (tampering)		Εμπιστευτικότητα Ακεραιότητα Αυθεντικότητα	Ενεργητική	Εσωτερική Εξωτερική	Καταστροφή κόμβων και υποκλοπή ευαίσθητων δεδομένων
Φυσική επίθεση		Διαθεσιμότητα Ακεραιότητα	Ενεργητική	Εξωτερική	Καταστροφή κόμβου
Αναπαραγωγή κόμβου (node replication)		Διαθεσιμότητα Ακεραιότητα	Ενεργητική	Εσωτερική Εξωτερική	Αντικατάσταση κόμβου με κόμβο υπό τον έλεγχο του επιτιθέμενου
Σύγκρουση δεδομένων (collision)	Ζεύξης	Διαθεσιμότητα	Ενεργητική	Εσωτερική	Απώλεια δεδομένων
Εξάντληση ενεργειακών πόρων (exhaustion)			Ενεργητική	Εσωτερική Εξωτερική	Εξάντληση ενεργειακών πόρων

Μεροληψία (unfairness)			Ενεργητική	Εσωτερική	Απώλεια δεδομένων
Επιλεκτική προώθηση (selective forwarding)	Δικτύου	Εμπιστευτικότητα Διαθεσιμότητα	Ενεργητική	Εσωτερική	Απώλεια δεδομένων
Επίθεση καταβόθρας (sinkhole)		Εμπιστευτικότητα Ακεραιότητα Αυθεντικότητα	Ενεργητική	Εσωτερική Εξωτερική	Έλεγχος δρομολόγησης
Εξαπάτηση αναγνώρισης (acknowledgment spoofing)		Αυθεντικότητα Διαθεσιμότητα	Ενεργητική	Εσωτερική	Διακίνηση ψευδών μηνυμάτων
Σκουληκότρυπα (wormhole)		Εμπιστευτικότητα Αυθεντικότητα	Ενεργητική	Εσωτερική	Έλεγχος δρομολόγησης
Σιβυλλική (sybil)		Αυθεντικότητα Διαθεσιμότητα	Ενεργητική	Εσωτερική	Δυσλειτουργία στη ταυτοποίηση κόμβου και έλεγχος δρομολόγησης
Hello ροών (Hello flood)		Αυθεντικότητα Διαθεσιμότητα	Ενεργητική	Εσωτερική Εξωτερική	Έλεγχος δρομολόγησης & απώλεια πακέτων
Υπερχείλιση πίνακα δρομολόγησης (Routing table overflow)		Διαθεσιμότητα	Ενεργητική	Εξωτερική Εσωτερική	Έλεγχος δρομολόγησης
Παρακολούθηση και κρυφάκουσμα (monitoring and eavesdropping)		Εμπιστευτικότητα	Παθητική	Εσωτερική Εξωτερική	Υποκλοπή κρίσιμων πληροφοριών
Ανάλυση κίνησης (traffic analysis)		Εμπιστευτικότητα	Παθητική	Εσωτερική Εξωτερική	Ανίχνευση κόμβων κρίσιμης σημασίας
Παραλλαγή (camouflage)		Εμπιστευτικότητα Διαθεσιμότητα	Παθητική	Εσωτερική Εξωτερική	Απώλεια-καταστροφή πακέτων, ψευδή μηνύματα
Πλημμύρα (flooding)	Μεταφοράς	Διαθεσιμότητα	Ενεργητική	Εσωτερική	Εξάντληση πόρων
Αποσυγχρονισμός (desynchronization)		Αυθεντικότητα Διαθεσιμότητα	Ενεργητική	Εσωτερική Εξωτερική	Δυσλειτουργίες σύνδεσης
Κώδικας κακόβουλης επίθεσης (malicious code)	Εφαρμογής	Διαθεσιμότητα	Ενεργητική	Εσωτερική Εξωτερική	Δυσλειτουργία κόμβων - καθυστερήσεις δικτύου
Αποσυγχρονισμός ρολογιού (clock desynchronization)		Διαθεσιμότητα	Ενεργητική	Εσωτερική Εξωτερική	Λανθασμένες μετρήσεις

ΚΕΦΑΛΑΙΟ 4

4.1 Εισαγωγή

Στο προηγούμενο κεφάλαιο αναφερθήκαμε στις επιθέσεις που λαμβάνουν χώρα στα ασύρματα δίκτυα αισθητήρων θέτοντας υπο αμφισβήτηση τις απαιτήσεις ασφάλειας και παραβιάζοντας εν συνεχεία τις προδιαγραφές που έχουν οριστεί για την ορθή λειτουργία του δικτύου. Αυτές οι παραβιάσεις θίγουν τόσο την ασφάλεια όσο και την αξιοπιστία, έννοιες που έχουν καθοριστική σημασία σε τέτοιας μορφής ασύρματα δίκτυα. Για την εξάλειψη αυτής της απειλής έχουν σχεδιασθεί μηχανισμοί ασφάλειας που λειτουργούν ως αντίμετρα εναντίον αυτών των επιθέσεων. Οι μηχανισμοί ασφάλειας έχουν ως βασικό συστατικό την χρήση περισσότερων του ενός αλγορίθμου και συγκεκριμένων πρωτοκόλλων δρομολόγησης που αυξάνουν την πολυπλοκότητα στη λειτουργία ενός δικτύου WSN. Επίσης γίνεται χρήση μυστικών κλειδιών κρυπτογράφησης που αυξανουν την προστασία της πληροφορίας που διακινείται.

4.2 Χαρακτηριστικά Μηχανισμών Ασφάλειας

Ένας μηχανισμός ασφάλειας θα πρέπει να σχεδιάζεται λαμβάνοντας υπόψιν τα παρακάτω χαρακτηριστικά, προκειμένου να μπορεί να αποκρούσει με επιτυχία τυχόν εκδήλωση απειλής για το σύστημα που έχει προγραμματιστεί να προστατεύει [18].

- Ασφάλεια: Ο μηχανισμός ασφάλειας θα πρέπει να προσαρμόζεται στις απαιτήσεις αφάλειας ππου διέπουν τα ασύρματα δίκτυα αισθητήρων
- Ανθεκτικότητα: Ο μηχανισμός ασφάλειας δεν θα πρέπει να επηρεάζεται στη περίπτωση που προσβληθεί ένας κόμβος έτσι ώστε να μπορεί να συνεχίσει αδιάλειπτα τη λειτουργία του.

- Εξοικονόμηση ενέργειας: Μια βασική απαίτηση στον σχεδιασμό ενός δικτύου WSN είναι τα υψηλά αποθέματα ενέργειας στους κόμβους. Ο μηχανισμός ασφάλειας θα πρέπει να εναρμονίζεται με αυτή τη προδιαγραφή και όχι να καταναλώνει επιπλέον ενέργεια.
- Ευελιξία: Ο μηχανισμός ασφάλειας και οι αλγόριθμοι κρυπτογράφησης θα πρέπει να είναι ευέλικτοι στον τρόπο που προσαρμόζονται στις ανάγκες του κάθε δικτύου.
- Δυνατότητα κλιμάκωσης: Εφόσον ένα ασύρματο δίκτυο αισθητήρων έχει τη δυνατότητα κλιμάκωσης , θα πρέπει απαραίτητα και ο μηχανισμός ασφάλειας να συμμετέχει σ' αυτό.
- Ανοχή σφαλμάτων: Ο μηχανισμός ασφάλειας θα πρέπει να παρέχει αξιοπιστία στο δίκτυο προσπερνώντας τα σφάλματα που προέρχονται από κακόβουλες ενέργειες (π.χ στη καταστροφή κόμβων)

4.3 Ανίχνευση παρείσφρησης (intrusion detection)

Το ενδεχόμενο εισαγωγής εσφαλμένων πληροφοριών στο δίκτυο δημιουργεί την ανάγκη ανάπτυξης μηχανισμών ανίχνευσης παρεισφρήσεων και αντιδράσεις σε αυτές. Ένα σύστημα ανίχνευσης παρεισφρησης (Intrusion Detection System – IDS) παρακολουθεί το δίκτυο και συγκρίνει τυχόν διαφορές μεταξύ των παρατηρήσεων που εντοπίζονται και του φυσιολογικού πλαισίου συμπεριφορών. Διακρίνονται σε δύο κατηγορίες [73]:

α) Βασισμένα σε κανόνες (rule based) να ανιχνεύουν γνωστά πρότυπα παρεισφρήσεων

β) Βασισμένα στην ανίχνευση στατιστικών ανωμαλιών (anomaly based) να ανιχνεύουν αγνώστης μορφής ανωμαλιών στο δίκτυο

Τα συστήματα αυτά εκπέμπουν συναγερμό στο δίκτυο μόλις εντοπίσουν κάποια παρείσφρηση με στόχο την άμεση αντίδραση και εξουδετέρωση του

προβλήματος. Αξίζει να σημειωθεί ότι τα anomaly based συστήματα έχουν μεγαλύτερη αποτελεσματικότητα ανίχνευσης γιατί χαρακτηρίζονται απο υψηλότερο ποσοστό ψευδών συναγερμών συγκρινόμενα με αυτά που είναι βασισμένα σε κανόνες.

4.4 Αντιμετώπιση επιθέσεων – Αντίμετρα

Κατά τη σχεδίαση κάποιου μηχανισμού ασφάλειας θα πρέπει να γνωρίζουμε ότι υπάρχει ειδοποιός διαφορά στον τρόπο αντιμετώπισης μιας παθητικής επίθεσης από μια επίθεση ενεργητικής μορφής. Ο ρόλος του μηχανισμού ασφάλειας σε μια επίθεση παθητικής μορφής είναι περισσότερο «αποτρεπτικός». Αυτό συμβαίνει για τον λόγο ότι σε μια τέτοια επίθεση ο επιτιθέμενος δεν σκοπεύει να τροποποιήσει τα δεδομένα παρά μόνο να συλλέξει χρήσιμα γ αυτόν δεδομένα μέσω της συλλογής πληροφοριών (traffic analysis) και συλλογής πακέτων (packet sniffing). Η αντιμετώπιση των επιθέσεων παθητικής μορφής πραγματοποιείται κυρίως με αλγόριθμους κρυπτογράφησης. Αντίθετα, σε μια επίθεση ενεργητικής μορφής όπου τα δεδομένα τροποποιούνται και οι υπηρεσίες του δικτύου αναστέλλονται ή διακόπτονται επ’ αορίστου, ο ρόλος του μηχανισμού ασφάλειας πρέπει να έχει χαρακτήρα ανίχνευσης, με σκοπό την άμεση αποτροπή των δυσμενών συνεπειών που θα έχει μια τέτοια επίθεση για τη λειτουργία του δικτύου και την ταχύτερη ανάκαμψή του.

4.4.1 Αντιμετώπιση επιθέσεων DoS

Παρακάτω θα αναφερθούμε στους τρόπους άμυνας απέναντι σε επιθέσεις άρνησης εξυπηρέτησης με βάση την πολυεπίπεδη αρχιτεκτονική των ασύρματων δικτύων αισθητήρων [18] [25] [29] [43].

4.4.1.1 Φυσικό επίπεδο

Η *επίθεση παρεμβολής (jamming)* μπορεί να αντιμετωπιστεί χρησιμοποιώντας τις τεχνικές εξάπλωσης του φάσματος FHSS και DSSS. Η τεχνική DSSS (Direct Sequence Spread Spectrum) χρησιμοποιεί κώδικες εξάπλωσης (code spreading) για να εξαπλώσει το σήμα στο διαθέσιμο φάσμα συχνοτήτων. Επειδή όμως έχει υψηλές απαιτήσεις σε ενεργειακά αποθέματα και υπολογιστικούς πόρους, δεν βρίσκει απόλυτη εφαρμογή σε ασύρματα δίκτυα αισθητήρων. Από την άλλη πλευρά η τεχνική μεταπήδησης συχνότητας FHSS (Frequency-Hopping Spread Spectrum) χρησιμοποιεί ένα στενό φασματικά φέρον σήμα το οποίο μεταδίδεται σε κάποια συχνότητα για συγκεκριμένο χρόνο μέχρις ότου να μεταπηδήσει σε άλλη συχνότητα βάσει μιας τυχαίας ακολουθίας. Ο αλγόριθμος για τη μεταπήδηση της συχνότητας γνωστοποιείται τόσο στον πομπό όσο και στον δέκτη. Εάν αυτό το σήμα φτάσει στα χέρια του επιτιθέμενου, τότε αγνοείται γιατί το θεωρεί θόρυβο μικρής διάρκειας. Έτσι λοιπόν μη γνωρίζοντας την ακολουθία μεταπήδης συχνοτήτων δεν μπορεί να δημιουργήσει παρεμβολή στο δίκτυο που να συμβαδίζει με αυτή την ακολουθία. Άλλες τεχνικές αντιμετώπισης της ιδίας επίθεσης είναι το σερφάρισμα καναλιού, η μείωση του κύκλου λειτουργίας των αισθητήριων κόμβων καθώς επίσης και ο αποκλεισμός της προσβεβλημένης περιοχής (τα πακέτα δρομολογούνται πέριξ αυτής της περιοχής).

Απέναντι στις επιθέσεις *αλλοίωσης (tampering)* ή *υποκλοπής* χρησιμοποιούνται οι άμυνες της φυσικής απόκρυψης των κόμβων ή το «καμουφλάρισμά» τους καθώς επίσης και η άμεση διαγραφή στοιχείων κώδικα αλλα και μνήμης που περιέχει κρυπτογραφημένα δεδομένα ως αποτέλεσμα άμεσης αντίδρασης σε απόπειρα επίθεσης αλλοίωσης.

4.4.1.2 Επίπεδο ζεύξης

Μια τυπική άμυνα απέναντι στην επίθεση *σύγκρουσης δεδομένων (collisions)* είναι με τη χρήση κωδικών διόρθωσης σφαλμάτων (error-correcting codes) [29]. Οι περισσότεροι κώδικες λειτουργούν καλύτερα με χαμηλού επιπέδου συγκρούσεις όπως αυτές που προκαλούνται από περιβαλλοντικά ή πιθανολογικά σφάλματα. Ωστόσο αυτοί οι κώδικες προκαλούν μεγάλο ενεργειακό κόστος σε υπολογισμούς και στην επικοινωνία. Κάθε φορά που σχεδιάζεται ένας μηχανισμός ασφάλειας έναντι συγκρούσεων, θα πρέπει να λαμβάνεται υπόψιν ότι ο επιτιθέμενος θα βρίσκεται πάντα σε θέση να καταστρέψει περισσότερα απο όσα μπορούμε να διορθώσουμε. Αν και με τη χρήση κωδικών διόρθωσης σφαλμάτων μπορούμε να εντοπίσουμε τις κακόβουλες συγκρούσεις, δεν υπάρχει κάποιος μηχανισμός ωστόσο να μας προστατεύει εξολοκλήρου από ανάλογες επιθέσεις μέχρι και σήμερα.

Μια πιθανή λύση για την επίθεση *εξάντλησης ενέργειας (exhaustion)* είναι ο περιορισμένος ρυθμός ελέγχου εισαγωγής MAC. Κάτι τέτοιο θα επέτρεπε στο δίκτυο να αγνοήσει τυχόν αιτήματα που στόχο έχουν την εξάντλση των ενεργειακών αποθέματα των κόμβων. Μια δεύτερη τεχνική άμυνας είναι η χρήση της πολλαπλής πρόσβασης διαίρεσης χρόνου (TDMA). Σύμφωνα με αυτή, οι κόμβοι διαχωρίζονται στο πεδίο του χρόνου με εκχώρηση σε κάθε έναν εξ' αυτών χρονοθυρίδων (timeslots).

Η επίδραση της *μεροληψίας (unfairness)* που προκαλείται απο έναν εισβολέα ξεκινώντας απο μία επίθεση επιπέδου ζεύξης μπορεί να περιοριστεί με τη χρήση μικρών πλαισίων δεδομένων καθώς μπορεί να μειώσει τον χρόνο που ένας επιτιθέμενος παίρνει στη διάθεσή του μέχρι να καταγράψει το κανάλι επικοινωνίας αφού κάθε κόμβος προσπελαύνει το κανάλι για σύντομο χρονικό διάστημα. Ωστόσο αυτή η τεχνική μειώνει την αποδοτικότητα και είναι ευάλωτη σε περαιτέρω επίθεση μεροληψίας καθώς ο επιτιθέμενος ενδέχεται να προσπαθήσει την γρήγορη επανεκπομπή αντί να περιμένει για ένα τυχαίο χρονικό διάστημα.

4.4.1.3 Επίπεδο δικτύου

Το πρωτόκολλο δρομολόγησης που εφαρμόζεται κάθε φορά, είναι αυτό που παίζει τον πιο καθοριστικό ρόλο στην αντιμετώπιση επιθέσεων στο επίπεδο δικτύου. Ένα αντίμετρο κατά της πλαστογράφησης και τροποποίησης είναι η χρήση κωδικού ελέγχου ταυτότητας μηνύματος (MAC) ακριβώς μετά το μήνυμα. Προσθέτοντας ένα MAC στο μήνυμα οι αποδέκτες μπορούν κάθε φορά να επιβεβαιώσουν εάν τα μηνύματα έχουν πλαστογραφηθεί ή τροποποιηθεί [29].

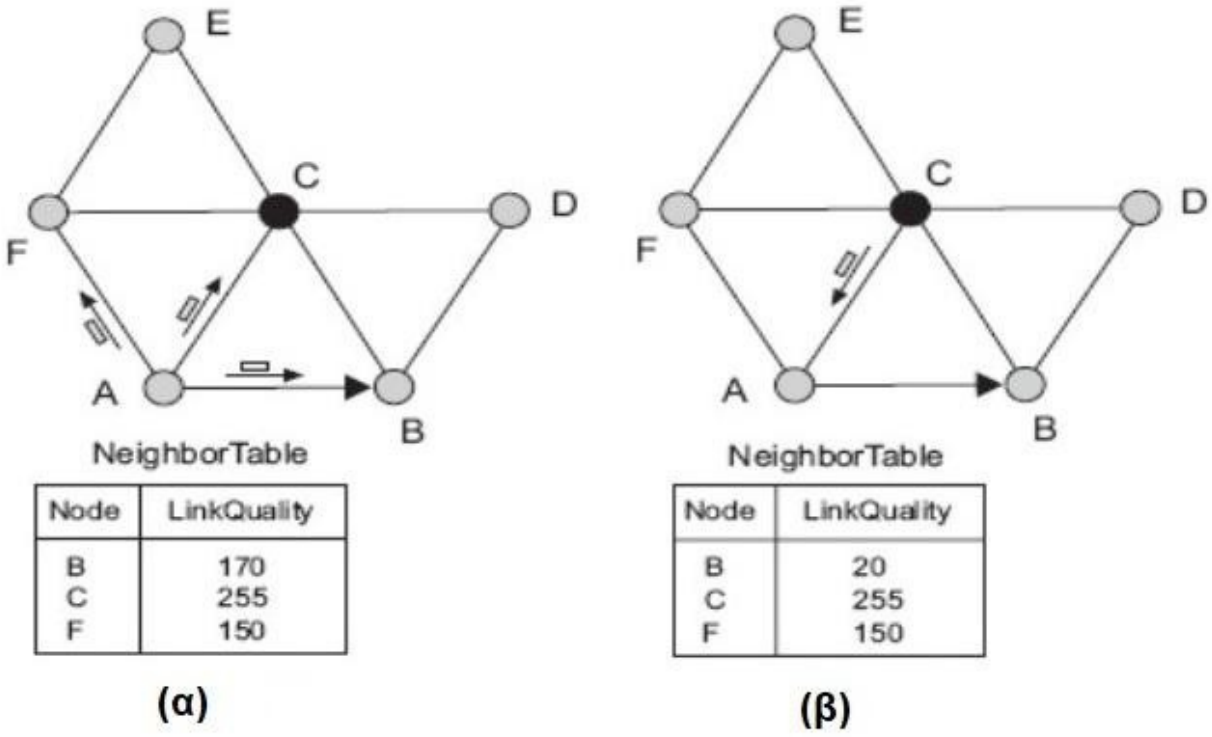
Η επίθεση *επιλεκτικής προώθησης (selective forwarding)* αντιμετωπίζεται από το εκάστοτε πρωτόκολλο δρομολόγησης, με τον εντοπισμό μη φυσιολογικών συμπεριφορών στο δίκτυο και την απομόνωση των κόμβων που τις προκαλούν [33]. Η χρήση εναλλακτικών μονοπατιών δρομολόγησης είναι μια τεχνική απομόνωσης των κόμβων. Επίσης η κρυπτογράφηση και αυθεντικοποίηση με χρήση δημοσίου κλειδιού είναι ένας ακόμη τρόπος άμυνας απέναντι σε ανάλογες επιθέσεις. Ένας ακόμη αμυντικός μηχανισμός είναι αυτός που γίνεται χρήση τοπολογίας ροής πολλαπλών δεδομένων (MultiDataflow Topologies) MDT. Χρησιμοποιώντας MDT χωρίζουμε τους αισθητήριους κόμβους σε δύο τοπολογίες διαφορετικής ροής δεδομένων ικανές να καλύψουν το εύρος της εποπτευόμενης περιοχής. Επομένως ο σταθμός βάσης απαιτεί μόνο μία ενημέρωση από οποιαδήποτε τοπολογία για τον έλεγχο του συνόλου του δικτύου. Μέσα από αυτές τις τοπολογίες ο σταθμός βάσης μπορεί να αμυνθεί στο ενδεχόμενο εκδήλωσης ανάλογης επίθεσης. Εάν εντοπισθεί κάποιος κακεντρεχής κόμβος, ο σταθμός βάσης αποκλείει από τη λειτουργία του δικτύου την τοπολογία μέσα στην οποία εντοπίστηκε, εξακολουθώντας όμως να δέχεται πακέτα από την δεύτερη τοπολογία. Εν συνεχεία ακολουθείται διαδικασία γεωγραφικού εντοπισμού του επιτιθέμενου κόμβου από τον σταθμό βάσης.

Για την αντιμετώπιση της *σιβυλλικής επίθεσης (sybil attack)* χρησιμοποιείται η τεχνική της αυθεντικοποίησης της ταυτότητας των κόμβων που συμμετέχουν στο δίκτυο με χρήση ισχυρών αλγορίθμων κρυπτογράφησης. Ο αλγόριθμος συμμετρικής κρυπτογράφησης (με χρήση δημοσίου κλειδιού) αποτελεί μια καλή επιλογή. Υπάρχουν κάποιες προσεγγίσεις που συμβάλλουν στην αντιμετώπιση της σιβυλλικής επίθεσης όπως αυτή της αξιόπιστης πιστοποίησης που εξουδετερώνει πλήρως την επίθεση διότι εξασφαλίζει ότι κάθε οντότητα στο δίκτυο έχει αυθεντικοποιημένη ταυτότητα και αυτό δύναται να συμβεί, ανιχνεύοντας τις κλεμμένες ή χαμένες ταυτότητες και κατόπιν ανακκλώντας τις από το δίκτυο. Μία δεύτερη προσέγγιση αποτρεπτικού κυρίως χαρακτήρα, είναι ο έλεγχος πόρων έτσι ώστε να εντοπισθούν οι κόμβοι που έχουν λιγότερους από τους αναμενούμενους. Απέναντι στις επιθέσεις Hello ροών χρησιμοποιούνται πρωτόκολλα δρομολόγησης γεωγραφικού προσανατολισμού τα οποία χρησιμοποιούν ως δεδομένο την πληροφορία της γεωγραφικής θέσης του κάθε κόμβου ως πρόσθετης πληροφορίας για να αποφασίσουν εάν η πηγή του κάθε πακέτου είναι ύποπτη ή όχι.

Προκειμένου να καταπολεμήσουμε την επίθεση *σκουληκότρυπας (wormhole)* χρησιμοποιούμε το DAWWSEN (Defense mechanism Against Wormhole attacks in Wireless Sensor Networks), ένα προληπτικό πρωτόκολλο δρομολόγησης που λειτουργεί όπως και η δομή ενός ιεραρχικού δέντρου όπου ο σταθμός βάσης είναι ο αρχικός (root) κόμβος και οι αισθητήριοι κόμβοι είναι το φύλλωμα του δέντρου. Η δομή του δέντρου ξεκινάει από το σταθμό βάσης που εκπέμπει ένα πακέτο δεδομένων για να ανακαλύψει τους κόμβους που βρίσκονται απο κάτω του στην ιεραρχία του δέντρου [59].

Ενδεχόμενη επίθεση *καταβόθρας (sinkhole)* καταστέλλεται με χρήση δύο κρυπτογραφικών πρωτοκόλλων δρομολόγησης RESIlient and Simple Topology-based reconfiguration protocols: RESIST-1 και RESIST-0 με κόστος όμως την αύξηση πολυπλοκότητας για το ίδιο το δίκτυο [60]. Επίσης χρησιμοποιείται το πρωτόκολλο δρομολόγησης Mint-Route το οποίο όμως έχει χαρακτήρα

περισσότερο ανίχνευσης και αποτροπής παρά αντιμετώπισης της επίθεσης. Με το συγκεκριμένο πρωτόκολλο κάθε κόμβος υπολογίζει την ποιότητα της σύνδεσης με τον γειτονικό του κόμβο και βάσει των απωλεσθέντων πακέτων «χτίζει» το δένδρο δρομολόγησης προς τον σταθμό βάσης. Οσο λιγότερα πακέτα χάνονται, τόσο ποιοτικότερη η ζεύξη. Μέχρις ότου υλοποιηθεί το δένδρο δρομολόγησης οι κόμβοι ενημερώνουν τον σταθμό βάσης εκπέμποντας περιοδικά πακέτα ενημέρωσης (update packets) που περιέχουν τέτοιες πληροφορίες. Επίσης κάθε κόμβος αποθηκεύει στον πίνακα γειτνίασης (neighbor table) πληροφορίες σχετικά με το κόστος (ταχύτητα σύνδεσης, απόσταση) μεταξύ των κόμβων (για την επιλογή κάθε φορά του κόμβου με την μεγαλύτερη ποιότητα ζεύξης). Στο σχήμα 4.1 απεικονίζεται το σενάριο μιας επίθεσης καταβόθρας και πως το πρωτόκολλο MINT-ROUTE [74] δρα αποτρεπτικά για λογαριασμό του δικτύου. Στο σενάριο αυτό λαμβάνουν χώρα δύο συνθήκες. Στην (α) ο επιτιθέμενος C λαμβάνει ένα πακέτο ενημέρωσης από τον A. Στην (β) συνθήκη ο επιτιθέμενος C παραπλανά τον A προσποιούμενος τον B. Ωστόσο το πρωτόκολλο MINT-ROUTE συγκρίνοντας περιοδικά τα περιεχόμενα των πινάκων γειτνίασης (neighbor table) μπορεί να ανιχνεύσει την αλλαγή κόστους του κόμβου B και εν τέλει να αποτρέψει το ενδεχόμενο μιας τέτοιας επίθεσης.



Σχήμα 4.1: Επίθεση καταβόθρας και πρωτόκολλο Mint-Route

Οι επιθέσεις *εξαπάτησης αναγνώρισης (acknowledgment spoofing)* μπορούν να αποφευχθούν με σωστό έλεγχο ταυτότητας για εξασφάλιση μιας έγκυρης και σωστά διαπιστευμένης επικοινωνίας μεταξύ των κόμβων και χρήση αποτελεσματικών τεχνικών κρυπτογράφησης [36]

Στα [15] [16] [37] αναφέρεται ότι οι επιθέσεις *Hello ροών* μπορούν να αντιμετωπιστούν με χρήση «πρωτοκόλλου επαλήθευσης ταυτότητας». Με το συγκεκριμένο πρωτόκολλο εξασφαλίζεται η αμφίδρομη επικοινωνία μιας σύνδεσης δικτύου με τον κρυπτογραφημένο μηχανισμό echoback προτού προβεί σε οποιαδήποτε ενέργεια στηριζόμενο σε μηνύματα που λαμβάνει μέσα από αυτή τη σύνδεση. Αυτή η άμυνα μοιάζει λιγότερο αποτελεσματική όταν ο επιτιθέμενος κάνει χρήση ενός ισχυρού πομπού. Όταν ο επιτιθέμενος «μολύνει» κάποιον κόμβο πριν

την αποστολή του μηνύματος ανατροφοδότησης τότε μπορεί πολύ εύκολα να αποκλείσει όλους τους παράπλευρους κόμβους απλά ρίχνοντας μηνύματα ανατροφοδότησης. Ως εκ τούτου ο επιτιθέμενος βρίσκεται σε θέση να δημιουργήσει ένα κανάλι σκουληκότρυπας για κάθε κομβο που βρίσκεται εντός εμβέλειας του πομπού του. Από την στιγμή που η επικοινωνία αυτών των κόμβων με τον επιτιθέμενο είναι αμφίδρομη τότε η παραπάνω προσέγγιση είναι απίθανο να εντοπίσει και να αποτρέψει μια επίθεση Hello ροών. Για να αποτρέψουμε μια τέτοια επίθεση κάθε αίτημα (REC) που προωθείται από έναν κόμβο θα πρέπει να είναι κρυπτογραφημένο με χρήση κλειδιού. Όταν δύο αισθητήριοι κόμβοι ανταλλάσουν κοινά μυστικά τότε ένα νέο κλειδί κρυπτογράφησης δημιουργείται στη μεταξύ τους επικοινωνία. Με αυτό τον τρόπο κάποιος γειτονικός κόμβος γνωρίζοντας το κλειδί μπορεί να αποκρυπτογραφήσει και να επαληθεύσει το αίτημα (REC) ενώ ο επιτιθέμενος μη γνωρίζοντας το κλειδί δεν μπορεί να εκδηλώσει επίθεση

4.4.1.4 Επίπεδο μεταφοράς

Η επίθεση *πλημμύρας (flooding attack)* αντιμετωπίζεται χρησιμοποιώντας τον αμυντικό μηχανισμό client puzzles [37]. Ο σταθμός βάσης κάθε φορά που υπάρχει αίτημα για μια νέα σύνδεση, στέλνει client puzzles με σκοπό την επίλυσή τους από τους κόμβους έτσι ώστε να διασφαλιστεί η έγκυρη διασύνδεσή τους. Όσοι κόμβοι δεν επιστρέψουν την λύση, απορρίπτονται από τη συνολική λειτουργία του δικτύου. Αυτό πρακτικά για τον επιτιθέμενο σημαίνει ότι χρειάζεται περισσότερους πόρους για να επιλύσει τα client puzzles και ταυτόχρονα

να αποτρέψει την εδραίωση σύνδεσης για μεγάλο αριθμό κόμβων μέσα σε σύντομο χρονικό διάστημα. Επιπλέον μέτρα αποτελούν τα κρυπτογραφικά puzzles, μηχανισμοί αυθεντικοποίησης και μέτρα περιορισμού αριθμού συνδέσεων ανα κόμβο.

Η λύση απέναντι στην επίθεση *αποσυγχρονισμού (desynchronization)* είναι η αυθεντικοποίηση όλων των πακέτων που ανταλλάσονται μεταξύ των αισθητήριων κόμβων, συμπεριλαμβανομένων των πεδίων ελέγχου της κεφαλίδας του πακέτου.

4.4.1.5 Επίπεδο εφαρμογής

Η επίθεση του κακόβουλου κώδικα αντιμετωπίζεται με τη χρήση ειδικών προγραμμάτων ανίχνευσης απειλής και καταστολής συμβάντων. Στον σταθμό βάσης εγκαθίσταται ένα λογισμικό το οποίο αποστέλλει σε όλους κόμβους του δικτύου απο ένα μοναδικό κομμάτι κώδικα κρυπτογραφημένο το οποίο ανα τακτά χρονικά διαστήματα ελέγχεται και αντιπαραβάλλεται με το αντίστοιχο είδωλό του που είναι αποθηκευμένο στον σταθμό βάσης. Εάν το αποτέλεσμα της σύγκρισης είναι θετικό ως προς την ακεραιότητά του κώδικα τότε ο εκάστοτε κόμβος συνεχίζει να υπάρχει και να συμμετέχει στις λειτουργίες του δικτύου. Υποθέτοντας ότι ο αντίπαλος δεν μπορεί να παρακάμψει τον αλγόριθμο κρυπτογράφησης, με αυτόν τον τρόπο εξασφαλίζεται η ακεραιότητα τόσο του λογισμικού του χρήστη όσο και του λειτουργικού συστήματος της συσκευής

Οι επιθέσεις αποσυγχρονισμού ρολογιού (clock desynchronization) είναι ουσιαστικά επιθέσεις που βάλλονται κατά της ακεραιότητας των δεδομένων που ανταλλάσονται μεταξύ των αισθητήριων κόμβων. Αυτό σημαίνει ότι θα πρέπει να ελέγχονται μέσα από μηχανισμούς αυθεντικοποίησης.

4.4.2 Αντιμετώπιση επιθέσεων κατά της εμπιστευτικότητας και της Αυθεντικότητας

Παρακάτω θα αναφερθούμε στους τρόπους άμυνας απέναντι σε επιθέσεις που στοχεύουν σε υποκλοπή ή τροποποίηση δεδομένων που ανταλλάσονται μεταξύ των αισθητήριων κόμβων.

4.4.2.1 Αντίμετρα αναπαραγωγής κόμβου - Φυσική επίθεση

Οι μηχανισμοί αντιμετώπισης παρεμβολών (μηχανισμοί FHSS και διαμόρφωσης φάσματος) προσφέρουν μερική προστασία ως προς τον εντοπισμό της θέσης των κόμβων από έναν επιτιθέμενο. Ο εξοπλισμός των κόμβων με υλικό, το οποίο θα τους προστατεύει από τους επιτιθέμενους όπως επίσης και ο αυτό-τερματισμός της συσκευής (self-termination) είναι ακόμη δύο τεχνικές άμυνας απέναντι σε τέτοιες επιθέσεις. Οι πιο σημαντικοί όμως μηχανισμοί στην αντιμετώπιση επιθέσεων αναπαραγωγής κόμβου αποτελούν τα πρωτόκολλα τυχαιοποιημένης πολυεκπομπής RM (Random Multicast), line selected πολυεκπομπής LSM (Line Selected Multicast) καθώς επίσης και το πρωτόκολλο τυχαιοποιημένης αποδοτικά κατανεμημένης ανίχνευσης RED (Randomized Efficient Distributed detection). Αξίζει να σημειωθεί ότι το πρωτόκολλο RED έχει αποδοτικότερο βαθμό στον εντοπισμό της επίθεσης συγκριτικά με τα πρωτόκολλα RM και LSM [39].

4.4.2.2 Αντίμετρα σε επιθέσεις κατά του απορρήτου

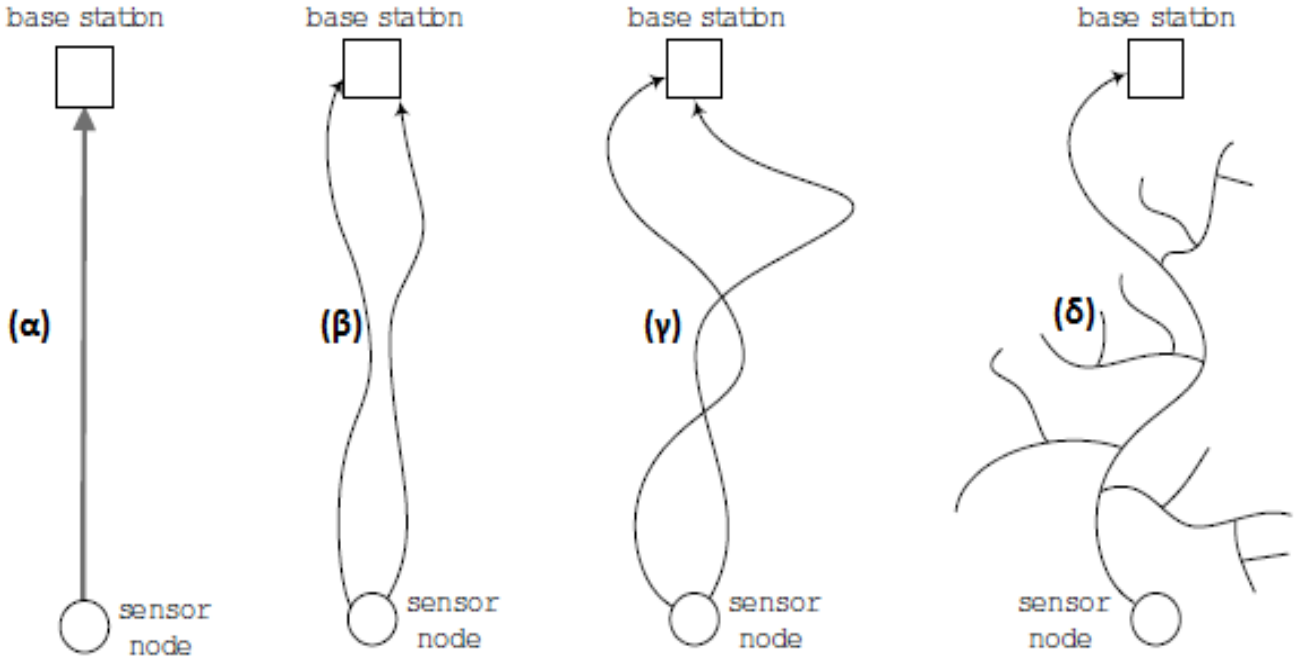
Στο [44] αναφέρονται οι τεχνικές που χρησιμοποιούνται ως άμυνα απέναντι σε επιθέσεις *κατά του απορρήτου*. Η πρώτη τεχνική που χρησιμοποιείται είναι με χρήση μηχανισμών ανωνυμίας. Οι μηχανισμοί ανωνυμίας μπορούν να υλοποιηθουν με: α) την αποκέντρωση των αποθηκευμένων ευαίσθητων πληροφοριών (διαμοιρασμός της πληροφορίας σε γειτονικούς κόμβους και όχι εξ ολοκλήρου σε έναν κόμβο), β) την εξασφάλιση ασφαλούς καναλιού επικοινωνίας (με χρήση ασφαλών πρωτοκόλλων επικοινωνίας πχ SPINS), γ) την τροποποίηση στο μονοπάτι δρομολόγησης των δεδομένων (με χρήση τεχνικών MPR, RW, Fractal Propagation) και δ) αξιοποιώντας την κινητικότητα των κόμβων. Η δεύτερη τεχνική που χρησιμοποιείται αφορά στη προσέγγιση με χρήση κάποια πολιτικής (policy-based approaches). Πρόκειται για αμυντικό μηχανισμό στον οποίο οι αποφάσεις για τον έλεγχο πρόσβασης και αυθεντικοποίησης λαμβάνονται βάσει του συνόλου των εφαρμοζόμενων πολιτικών. Τέλος χρησιμοποιείται και μια τρίτη

τεχνική που αποσκοπεί στη παραπλάνηση του επιτιθέμενου ως προς τη κίνηση των πακέτων στο δίκτυο, διασφαλίζοντας το απόρρητο. Αυτή η τεχνική κάνει χρήση των παρακάτω πρωτοκόλλων δρομολόγησης στηριζόμενα σε πλημμυρίσματα: α) πλημμύρισμα αρχικής τιμής (baseline flooding), β) πιθανολογικό πλημμύρισμα (propabilistic flooding), γ) πλημμύρισμα με ψεύτικα μηνύματα (flooding with fake messages και δ) πλημμύρισμα φαντάσματος (phantom flooding).

Αλγόριθμοι κρυπτογράφησης [40] μπορούν να χρησιμοποιηθούν για τον έλεγχο της *παρακολούθησης και κρυφακούσματος (monitoring and eavesdropping)*. Επίσης μπορούν να χρησιμοποιηθούν κατευθυντικές κεραίες (directional antennas) [68] που έχουν την ικανότητα να εκπέμπουν μεγαλύτερης ισχύς σήματα σε συγκεκριμένες κατευθύνσεις, μειώνοντας κατα πολύ την παρεμβολή και εν τέλει την υποκλοπή των δεδομένων απο κάποιον επιτιθέμενο.

Σύμφωνα με το [41] προτείνεται η στρατηγική χρήσης τριών μεθόδων για την αντιμετώπιση της επίθεσης *ανάλυσης κίνησης*. Στόχος τους είναι η παραπλάνηση του επιτιθέμενου ως προς τον εντοπισμό της θέσης του σταθμού βάσης και αυτό επιτυγχάνεται με δημιουργία κίνησης σε τυχαίες κατευθύνσεις εντός του δικτύου. Σύμφωνα με την πρώτη τεχνική για να μειώσουμε τον εύκολο εντοπισμό των προφανών διαδρομών τροποποιούμε το σχήμα δρομολόγησης συντομότερου μονοπατιού SP (Shortest Path σχήμα 4.2(α)) έχοντας κάθε κόμβο να επιλέγει έναν από τους πολλαπλούς γειτονικούς κόμβους για να μεταφέρει τα δεδομένα προς τον σταθμό βάσης. Ως εκ τούτου τα πακέτα που μεταφέρονται από τον αισθητήριο κόμβο προς τον σταθμό βάσης διέρχονται όχι μέσω του συντομότερου μονοπατιού SP αλλά μέσω εναλλακτικών διαδρομών MPR (Multiparent Routing (σχήμα 4.2 (β)). Η δεύτερη τεχνική είναι η RW (Random Walk σχήμα 2.2 (γ)). Σε αυτή τη μέθοδο γίνεται χρήση κάποιου αλγορίθμου δρομολόγησης που επιλέγει τυχαία το μονοπάτι μέσα από το οποίο θα διακινηθούν τα δεδομένα. Κάθε κόμβος που λαμβάνει ένα πακέτο το προωθεί ισοπίθανα σε κάποιον γειτονικό του κόμβο. Μπορεί η μέθοδος RW να είναι αποτελεσματικότερη από την MPR γιατί μπορεί πολύ εύκολα να παραπλανήσει

τον εισβολέα μέσα από την τυχαιότητα επιλογής των κόμβων και των μονοπατιών, ωστόσο δεν συνίσταται στις περιπτώσεις που η άμεση εξάντληση ενεργειακών πόρων δεν είναι επιθυμητή. Αυτό συμβαίνει διότι δημιουργούνται μεγάλα μονοπάτια δρομολόγησης που απαιτούν υψηλά αποθέματα ενέργειας. Μπορεί οι τεχνικές MPR και RW να δημιουργούν εναλλακτικές διαδρομές και να καθιστούν δύσκολη την εκδήλωση μιας επίθεσης παρακολούθησης του δικτύου, ωστόσο παραμένουν ευάλωτες σε επιθέσεις συσχέτισης χρόνου. Για την αντιμετώπιση των μειονεκτημάτων των μεθόδων PR και RW δημιουργήθηκε μια τρίτη μέθοδος που ονομάζεται κλασματική διάδοση (Fractal Propagation σχήμα 4.2(δ)). Σύμφωνα με αυτή τη τεχνική δημιουργούνται ψευδή πακέτα και εικονικά μονοπάτια δρομολόγησης στο δίκτυο. Πιο συγκεκριμένα κάθε φορά που κάποιος κόμβος λάβει ένα πακέτο τότε με μια καθορισμένη πιθανότητα δημιουργείται ένα ψευδές πακέτο και το προωθεί σε κάποιον γείτονά του. Αυτή η μέθοδος έχει το μειονέκτημα της αυξημένης κυκλοφορίας γύρω από τον σταθμό βάσης με αποτέλεσμα τις επαναλαμβανόμενες συγκρούσεις και το ενδεχόμενο απώλειας πακέτων δεδομένων.



Σχήμα 4.2: Τεχνικές αντιμετώπισης επίθεσης κίνησης: **α)** Συντομότερο μονοπάτι SP, **β)** Τεχνική MPR, **γ)** Τεχνική RW **δ)** Τεχνική Κλασματικής διάδοσης

4.5 Σύνοψη

Οι περισσότερες επιθέσεις στα WSNs ξεκινούν με την εισαγωγή ψευδών πληροφοριών στο δίκτυο. Για τον εντοπισμό αυτών των μηνυμάτων απαιτείται η υλοποίηση ενός μηχανισμού ανίχνευσης-άμυνας. Όπως είδαμε παραπάνω, όλες οι απειλές κατά της ασφάλειας, δλδ όλες οι προαναφερθείσες επιθέσεις έχουν στόχο να θέσουν σε κίνδυνο την λειτουργικότητα του δικτύου καθώς επίσης και το μοντέλο CIA της διακινούμενης πληροφορίας. Η κρυπτογράφηση, η αυθεντικοποίηση, η πολυδιαδρομική δρομολόγηση, η επιβεβαίωση ταυτότητας, η αμφίδρομη επιβεβαίωση ζεύξης και η αυθεντικοποίηση εκπομπών είναι μερικές από τις τεχνικές που χρησιμοποιούνται προκειμένου να διασφαλιστεί η εμπιστευτικότητα της διακινούμενης πληροφορίας. Στον πίνακα 4.1 παρουσιάζονται συνοπτικά οι αμυντικοί μηχανισμοί ανά τύπο επίθεσης που λαμβάνουν χώρα σε ένα ασύρματο δίκτυο αισθητήρων.

Πίνακας 4.1: Μηχανισμοί αντιμετώπισης επιθέσεων στα WSN's

Επίθεση	Μηχανισμοί αντιμετώπισης επίθεσης
Παρεμβολή (jamming)	Τεχνική μεταπήδησης συχνότητας FHSS, τεχνική διαμόρφωσης φάσματος DSSS (Code spreading), PDR, RSSI, αλγόριθμοι κρυπτογράφησης
Αλλοίωση (tampering)	Μηχανισμοί προστασίας παραβίασης, φυσική απόκρυψη, μηχανισμοί απενεργοποίησης, AODV
Φυσική επίθεση	Φυσική απόκρυψη, παρακολούθηση, συμμετρικοί αλγόριθμοι κρυπτογράφησης
Αναπαραγωγή κόμβου (node replication)	Φυσική απόκρυψη, κρυπτογράφηση, συγχρονισμός
Σύγκρουση δεδομένων (collision)	Κώδικας διόρθωσης σφαλμάτων ECC (error-correcting code), αποφυγή χρήσης πρωτοκόλλων MAC που λειτουργούν με το σχήμα RTS/CTS, MCC, CSMA/CA, RSSI
Εξάντληση ενεργειακών πόρων (exhaustion)	TDMA, δρομολόγηση πακέτων μόνο μετά από αυθεντικοποίηση του αποστολέα, περιορισμός πακέτων, λύση ασαφούς λογικής
Μεροληψία (unfairness)	Χρήση μικρών σε μήκος πακέτων
Επιλεκτική προώθηση (selective forwarding)	Τεχνικές πλεονασμού, συνεργατική ανίχνευση hop by hop, πρόκληση/απόκριση
Επίθεση καταβόθρας (sinkhole)	Πρωτόκολλο δρομολόγησης MintRoute, AODV, κρυπτογραφικά πρωτόκολλα RESIST-0/RESIST-1, IDS με βάση την υπογραφή

Εξαπάτηση αναγνώρισης (acknowledgment spoofing)	Τεχνικές αυθεντικοποίησης
Σκουληκότρυπα (wormhole)	DAWWSEN, χρήση πληροφοριών θέσης και χρόνου, AES, AODV, Distance Vector πρωτόκολλα
Σιβυλλική (sybil)	Πιστοποίηση ταυτότητας
Hello ροών (Hello flood)	Κατανεμημένα IDS, τεχνικές αυθεντικοποίησης δύο δρόμων, τριών δρόμων χειραψία, LEACH, CSMA/CA, Client puzzle
Παρακολούθηση και κρυφάκουσμα (monitoring and eavesdropping)	Αλγόριθμοι κρυπτογράφησης, FHSS, κατευθυντικές κεραίες (directional antennas)
Ανάλυση κίνησης (traffic analysis)	Τεχνικές MPR, RW, κλασματικής διάδοσης
Παραλλαγή (camouflage)	Τεχνικές αυθεντικοποίησης
Πλημμύρα (flooding)	Client puzzle, cryptographic pazzle, περιορισμός συνδέσεων, τεχνικές αυθεντικοποίησης
Αποσυγχρονισμός (desynchronization)	Τεχνικές υδατογράφησης με βάση το περιεχόμενο και κομμάτια κώδικα
Κώδικας κακόβουλης επίθεσης (malicious code)	Τεχνικές αυθεντικοποίησης
Συγχρονισμός ρολογιού (clock synchronization)	Τεχνικές αυθεντικοποίησης
Επίθεση κατά του απορρήτου	Μηχανισμοί ανωνυμίας, policy-based approaches, πλημμύρισμα αρχικής τιμής, πιθανολογικό πλημμύρισμα, πλημμύρισμα με ψεύτικα μηνύματα

4.6 Κρυπτογράφηση

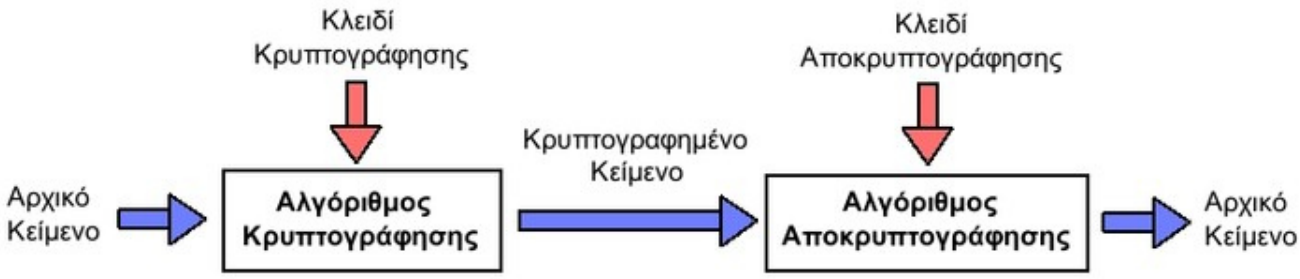
Η κρυπτογράφηση είναι ένας μηχανισμός άμυνας απέναντι στην υποκλοπή-διαρροή της πληροφορίας και στόχος της είναι η αποτελεσματική προστασία των ροών δεδομένων (data streams) μέσα από μετασχηματισμό των δεδομένων σε τέτοια μορφή που θα γίνεται κατανοητή μόνο από τους εξουσιοδοτημένους κόμβους που συμμετέχουν στην επικοινωνία χωρίς κάποιος τρίτος να μπορεί να τα κατανοήσει. Με άλλα λόγια η τροποποιημένη (κρυπτογραφημένη) πληροφορία μπορεί να διαβαστεί μόνο απο αυτόν που διαθέτει το κατάλληλο κλειδί. Η διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης παρουσιάζεται στο σχήμα 4.3. Στα ασύρματα δίκτυα αισθητήρων λόγω των περιορισμών που

υφίστανται σε ζητήματα επεξεργασίας δεδομένων και κατανάλωσης ενέργειας δεν είναι δυνατόν να γίνει χρήση όλων των τύπων κρυπτογράφησης. Εμείς θα σχολιάσουμε δύο βασικές κατηγορίες κρυπτογράφησης α) Συμμετρική κρυπτογράφηση και β) Ασύμμετρη κρυπτογράφηση. Οι αρχές λειτουργίας της κρυπτογράφησης είναι οι εξής [25]:

- Ακεραιότητα: Τα δεδομένα μπορούν να αλλοιωθούν μόνο από εξουσιοδοτημένους κόμβους
- Εμπιστευτικότητα: Η κρυπτογραφημένη πληροφορία είναι κατανοητή μόνο από εξουσιοδοτημένους κόμβους
- Πιστοποίηση: Οι κόμβοι (αποστολείς και παραλήπτες) που συμμετέχουν σε συνεδρία ανταλλαγής μηνυμάτων μπορεί να εξακριβώνουν τη γνησιότητα των ταυτοτήτων τους
- Μη απάρνηση: Οι κόμβοι (αποστολείς και παραλήπτες) δεν μπορούν να αρνηθούν την αυθεντικότητα της μεταδιδόμενης πληροφορίας

Παρακάτω θα αναφερθούμε στους βασικούς ορισμούς που συναντούμε στη κρυπτογραφία προκειμένου να κατανοήσουμε καλύτερα αυτά τα συστήματα.

- Αρχικό κείμενο (plaintext): Είναι το αρχικό μήνυμα που πρόκειται να κρυπτογραφθεί
- Κλειδί (key): Ένας αριθμός αρκετών bit που χρησιμοποείται στην είσοδο της συνάρτησης κρυπτογράφησης.
- Κρυπτογραφημένο κείμενο (chiphertext): Είναι το μήνυμα που προκύπτει από την εφαρμογή κάποιου αλγορίθμου κρυπτογράφησης πάνω στο απλό μήνυμα.



Σχήμα 4.3: Ένα τυπικό σύστημα κρυπτογράφησης - αποκρυπτογράφησης

4.6.1 Μέθοδοι κρυπτογράφησης

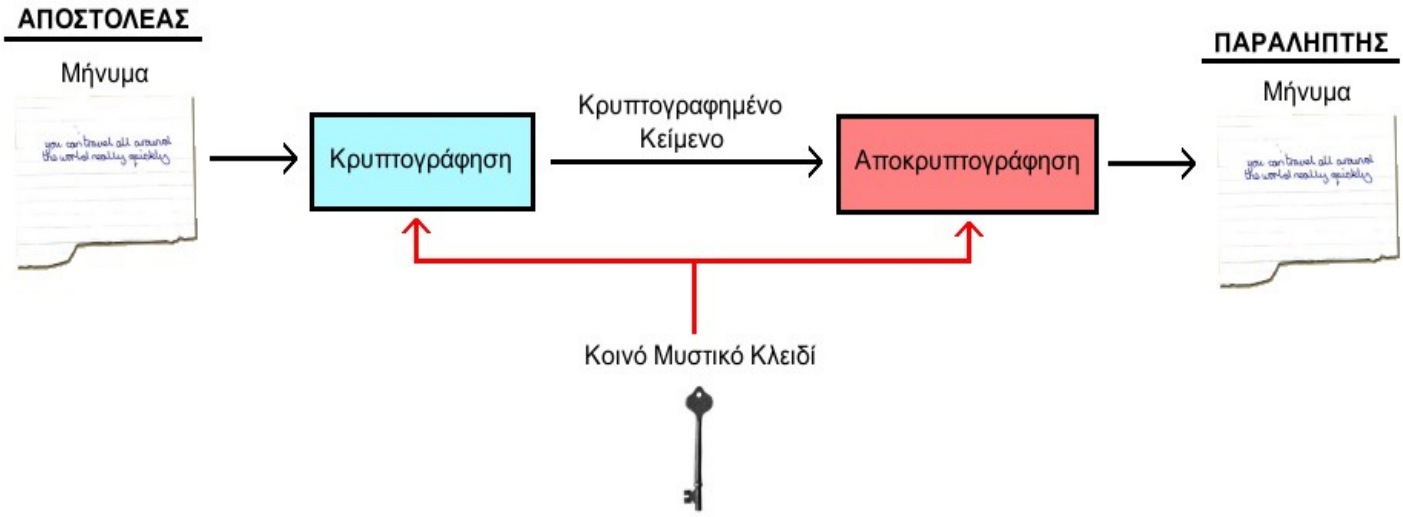
Στα ασύρματα δίκτυα αισθητήρων συναντάμαι δύο τρόπους κρυπτογράφησης της διακινούμενης πληροφορίας α) κρυπτογράφηση ζεύξης (link encryption) και β) κρυπτογράφηση απο άκρο σε άκρο (end-to-end encryption) [18]. Σύμφωνα με την πρώτη, η πληροφορία που διακινείται στο δίκτυο κρυπτογραφείται και αποκρυπτογραφείται σε κάθε συσκευή (κόμβο) του δικτύου. Αυτό συμβαίνει γιατι πρέπει να γνωστοποιηθεί ο αποδέκτης στους υπόλοιπους κόμβους έτσι ώστε να συνεχιστεί η δρομολόγηση του πακέτου προκειμένου να φθάσει στον παραλήπτη. Ενα μειονέκτημα εδώ είναι ότι κάθε συσκευή του δικτύου γνωρίζει το κλειδί κρυπτογράφησης-αποκρυπτογράφησης. Στη δεύτερη μέθοδο απο άκρο σε άκρο, το πακέτο μετάδοσης κρυπτογραφείται (πλην της κεφαλίδας που αφορά τον παραλήπτη) από τον αποστολέα και δρομολογείται αυτούσιο προς τον τελικό αποδέκτη στον οποίο θα γίνει η διαδικασία της αποκρυπτογράφησης. Σε αυτή τη μέθοδο, οι μόνοι που γνωρίζουν το κλειδί είναι ο κόμβος αποστολέας και ο κόμβος παραλήπτης. Ένα αρνητικό της κρυπτογράφησης απο άκρο σε άκρο αποτελεί το γεγονός ότι η κεφαλίδα του πακέτου που προσδιορίζει τον παραλήπτη είναι αναγνώσιμη και κατανοητή απο όλους στο δίκτυο ακόμη και απο κάποιον εισβολέα, γεγονός που καθιστά το δίκτυο ευάλωτο σε επιθέσεις ανάλυσης κίνησης.

4.6.2 Αλγόριθμοι κρυπτογράφησης

Οι αλγόριθμοι κρυπτογράφησης διακρίνονται σε τρείς μεγάλες κατηγορίες α) Συμμετρικοί β) Ασύμμετροι και γ) Υβριδικοί. Οι συμμετρικοί αλγόριθμοι (κρυπτογράφηση με χρήση ιδιωτικού κλειδιού) χρησιμοποιούν ένα κοινό κλειδί για την κρυπτογράφηση και αποκρυπτογράφηση. Οι ασύμμετροι αλγόριθμοι (κρυπτογράφηση με χρήση δημοσίου κλειδιού) χρησιμοποιούν ένα δημόσιο κλειδί για την κρυπτογράφηση και το αντίστοιχο ιδιωτικό κλειδί που έχει μόνο ο κόμβος παραλήπτης για την αποκρυπτογράφησή του. Οι υβριδικοί αλγόριθμοι είναι συνδυασμός των δύο προαναφερθέντων. Συμμετρικοί αλγόριθμοι κρυπτογράφησης αποτελούν οι DES, AES, CRYPTON, RC4, SERPENT, TWOFISH, IDEA, SHA-1, MD5. Στην κατηγορία των ασύμμετρων αλγορίθμων συναντάμε τους αλγορίθμους RSA, Diffie-Hellman, ELGAMAL, ελλειπτικη καμπύλη κρυπτογράφησης ECC, ελλειπτική καμπύλη ψηφιακής υπογραφής ECDSA, ελλειπτική καμπύλη Diffie-Hellman ECDH. Αξίζει να σημειωθεί ότι τα τελευταία έτη προτάθηκε στην ακαδημαϊκή κοινότητα ο ασύμμετρος αλγόριθμος δημοσίου κλειδιού MQQ (Multivariate Quadratic Almost Group) [49]. Σε μελέτές που υλοποιήθηκαν στις πλατφόρμες FPGA και PC, έδειξαν ότι είναι πολύ πιο γρήγορος από τους RSA και ECC

4.6.3 Συμμετρική κρυπτογράφηση

Στα συστήματα συμμετρικής κρυπτογράφησης χρησιμοποιείται ένα και μόνο κλειδί για την κρυπτογράφηση και αποκρυπτογράφηση του μηνύματος (σχήμα 4.4). Το βασικό πρόβλημα είναι ότι το κλειδί δεν ανταλλάσεται με ασφαλή τρόπο μεταξύ δύο κόμβων όταν αυτοί αποφασίσουν να ανταλλάξουν δεδομένα και καταλήξουν ποιο θα είναι το κοινό κλειδί τους [18] [67]. Από την άλλη το σημαντικότερο πλεονέκτημα με τους αλγορίθμους συμμετρικής κρυπτογράφησης αποτελεί η ανάγκη για μικρή υπολογιστική ισχύ και αυτό διότι η όλη διαδικασία κρυπτογράφησης-αποκρυπτογράφησης εξελίσσεται πάρα πολυ γρήγορα.



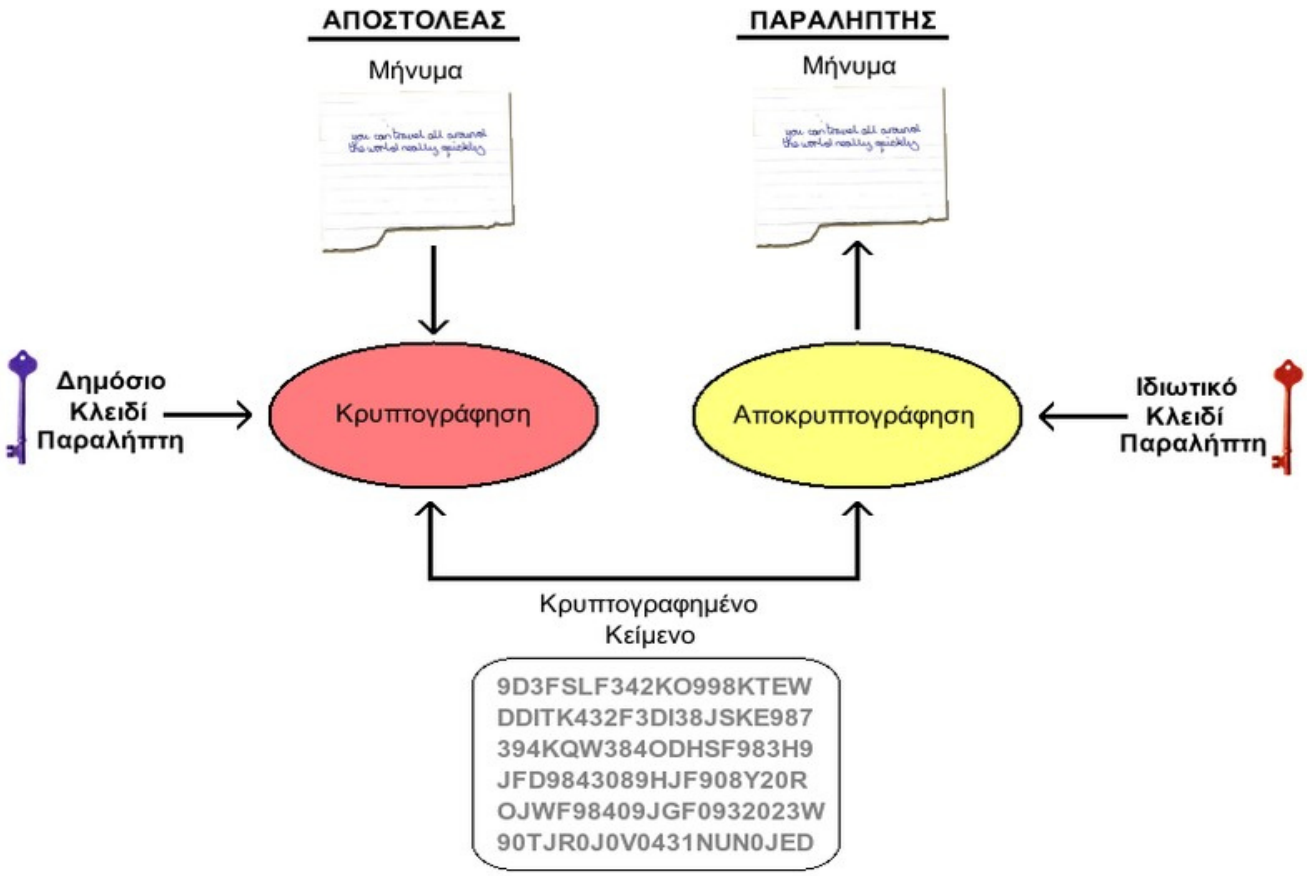
Σχήμα 4.4: Αλγόριθμος συμμετρικής κρυπτογράφησης

Πέραν όμως του προβλήματος της ασφάλειας κλειδιών υπάρχει και το πρόβλημα της αποτελεσματικής διανομής των κλειδιών μεταξύ των αισθητήριων κόμβων σε μεγάλα δίκτυα αφού ο αριθμός των ζεύγων-κλειδιών (key-pairs) είναι μεγάλος. Για την επίλυση των άνω προβλημάτων (ασφάλεια κλειδιών, αποτελεσματική διανομή κλειδιών) χρησιμοποιείται ένα ευρύ φάσμα από τεχνικές-σχήματα διαχείρισης κλειδιών που θα αναλύσουμε πιο κάτω.

4.6.4 Ασύμμετρη κρυπτογράφηση

Στα συστήματα ασύμμετρης κρυπτογράφησης, ο αποστολέας χρησιμοποιεί το δημόσιο κλειδί του παραλήπτη για την κρυπτογράφηση του μηνύματος ενώ ο παραλήπτης χρησιμοποιεί το δικό του ιδιωτικό κλειδί για την αποκρυπτογράφηση (σχήμα 4.5). Το ιδιωτικό κλειδί είναι γνωστό μόνο στον παραλήπτη ενώ το δημόσιο κλειδί είναι γνωστό σε όλους τους κόμβους που θέλουν να ανταλλάξουν μήνυμα [66] [45]. Η ασύμμετρη κρυπτογράφηση έχει απαιτήσεις σε κατανάλωση ενέργειας χάριν της υπολογιστικής

πολυπλοκότητας στους μεγάλους αριθμούς. Υπάρχουν ορισμένες εφαρμογές για τις οποίες η αποκρυπτογράφηση εξελίσσεται στον σταθμό βάσης (εξαιτίας της μεγαλύτερης διαθεσιμότητας πόρων) ενώ η κρυπτογράφηση εξελίσσεται στους κόμβους οι οποίοι είναι εγγενώς περιορισμένοι σε πόρους. Η ασύμμετρη κρυπτογράφηση ωστόσο έχει αρκετά πλεονεκτήματα που την καθιστούν ελκυστική. Ένα απο αυτά αποτελεί η άμυνά της έναντι επιθέσεων καταγραφής -παρακολούθησης κόμβων δεδομένου ότι ο κόμβος που θα παραδοθεί σε κάποιον εισβολέα δεν μπορεί να δώσει παραπάνω πληροφορία πλην του ιδιωτικού του κλειδιού. Η επεκτασιμότητά τους και η ευκολία στην ανάκτηση απολεσθέντων κλειδιών είναι ακόμη δύο βασικά πλεονεκτήματα των ασύμμετρων συστημάτων.

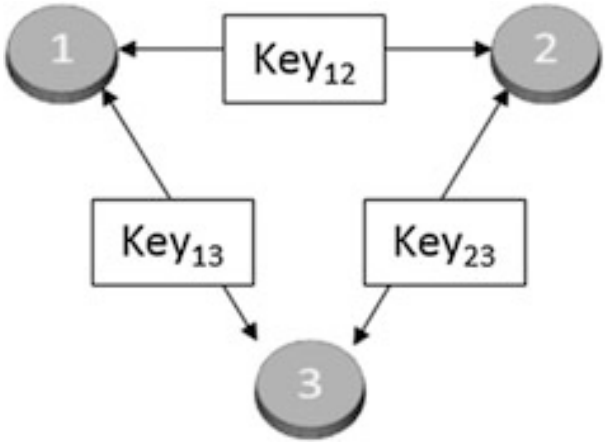


Σχήμα 4.5: Αλγόριθμος ασύμμετρης κρυπτογράφησης

4.6.5 Μηχανισμοί διαχείρισης κρυπτογραφικών κλειδιών

Η πιο εύκολη προσέγγιση στα ασύρματα δίκτυα θα ήταν η χρησιμοποίηση ενός μόνο κλειδιού που θα γνώριζαν όλοι οι κόμβοι του δικτύου και έτσι κάθε φορά που απαιτούνταν θα χρησιμοποιούσαν το ίδιο κοινό κλειδί για την κρυπτογράφηση και αποκρυπτογράφηση. Το ρίσκο όμως για όποιον ακολουθήσει αυτή τη προσέγγιση είναι ότι εάν παραβιαθεί ένας κόμβος απο κάποιον εισβολέα, θα παραβιασθεί και το υπόλοιπο δίκτυο. Η δεύτερη προσέγγιση αφορά στη συγκεντρωτική κατανομή κλειδιών (Centralized key distribution) που αποτελεί την πιο ασφαλή εναλλακτική λύση αφού κάθε κόμβος ανταλλάσει το κλειδί του μόνον με το σταθμό βάσης. Άρα λοιπόν κάθε φορά που δύο αισθητήριοι κόμβοι θέλουν να επικοινωνήσουν, θα πρέπει πρώτα να ζητήσουν από το σταθμό βάσης το κλειδί. Η βασική αδυναμία αυτού του σχήματος έγκειται στο υψηλό φόρτο εργασιών γύρω από το σταθμό βάσης αφού δυο αισθητήριοι κόμβοι θα πρέπει πρώτα να επικοινωνήσουν με τον απομακρυσμένο σταθμό βάσης και ύστερα μεταξύ τους οι γειτονικοί κόμβοι. Η πιο σημαντική ευπάθεια αυτού του σχήματος είναι οτι ο σταθμός βάσης εκθέτει όλα τα κλειδιά για κάθε ζεύγος αισθητήριων κόμβων στον επίδοξο εισβολέα.

Τα προβλήματα που προκύπτουν απο τις δύο παραπάνω προσεγγίσεις [18], μπορούν να αντιμετωπιστούν με την προ-διανομή των κλειδιών (key pre-distribution), αντιστοιχίζοντας για κάθε ζευγάρι κόμβων ένα μοναδικό κλειδί (σχήμα 4.6)

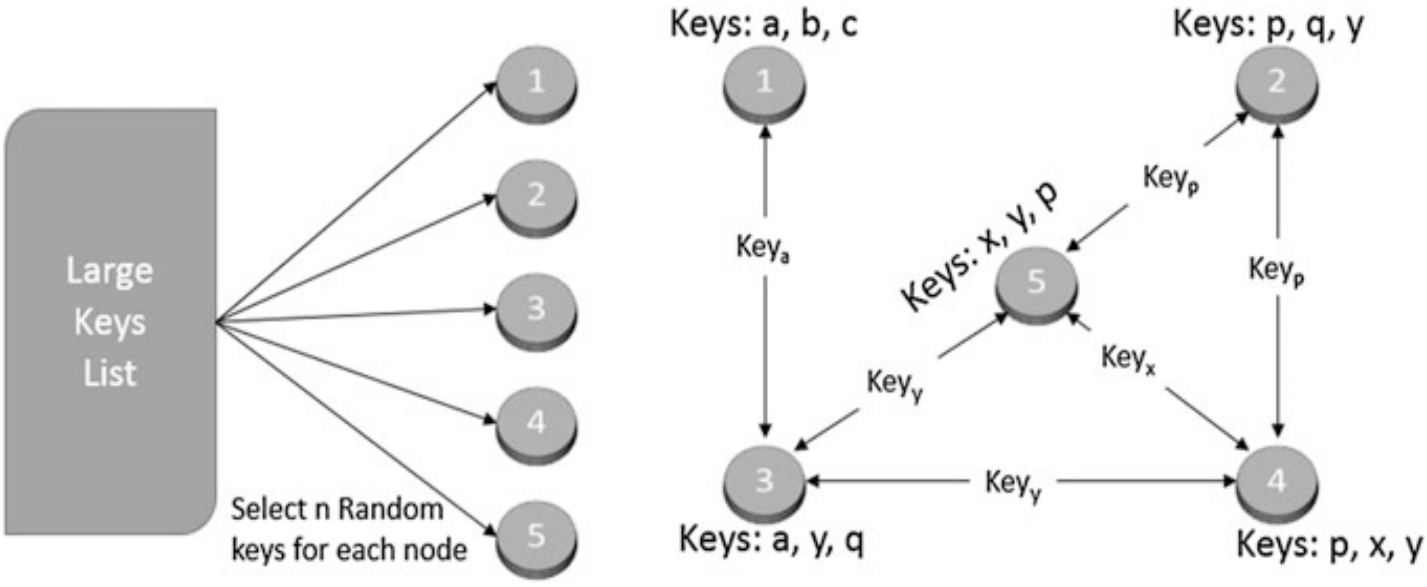


Σχήμα 4.6: Κατανομή ζεύγους κλειδιών για κάθε ζευγάρι αισθητήριων κόμβων

Ας υποθέσουμε ότι ένα ασύρματο δίκτυο αισθητήρων αποτελείται από *N* κόμβους. Αυτό σημαίνει ότι κάθε κόμβος θα πρέπει να αποθηκεύσει *N-1* κλειδιά ενώ συνολικά σε όλο το δίκτυο θα αποθηκευτούν *0.5N(N-1)* κλειδιά. Όσο το *N* αυξάνεται, ο αριθμός των αποθηκευμένων κλειδιών στο δίκτυο συνεχώς θα μεγαλώνει και αυτό ενδέχεται κάποια στιγμή να προκαλέσει σημαντικό περιορισμό στη μνήμη όλου του δικτύου. Ακολουθούν κάποια βασικά σχήματα κατανομής κλειδιών με τα οποία μπορούμε να εκμεταλλευτούμε τα οφέλη από την προ-διανομή των κλειδιών.

- Τυχαία προ-διανομή κλειδιών (Random Key Pre-Distribution RKP): Η ιδέα της τυχαίας ανάθεσης ασφαλών κλειδιών σε αισθητήριους κόμβους εισήχθη για πρώτη φορά από τους Eschenauer και Gligor [46] [47]. Σε αυτό το σχήμα κάθε κόμβος του δικτύου πριν την ανάπτυξή του στη περιοχή επιτήρησης, εξοπλίζεται με ένα σετ απο κλειδιά, τυχαία επελεγμένα και προερχόμενα από μία μεγάλη δεξαμενή κλειδιών. Έτσι λοιπόν δύο κόμβοι που θα θελήσουν να επικοινωνήσουν μεταξύ τους θα έχουν πρωτίστως ανταλλάξει κάποιο κοινό κλειδί που θα προέρχεται από το σετ. Στο σχήμα 4.7 παρουσιάζεται ο τρόπος που λειτουργεί η τεχνική RKP. Πιο συγκεκριμένα οι κόμβοι 1, 2, 3, 4 και 5 τυχαία επιλέγουν από τη δεξαμενή κλειδιών ένα σετ απο κλειδιά. Ο κόμβος 1 στο σετ κλειδιών που έλαβε περιλαμβάνονται τα κλειδιά a, b και c. Στους κόμβους 2, 3, 4 και 5 αντίστοιχα τα σετ αποτελούνται από τα κλειδιά p, q και y: a, y και q: p, x και y και x, y και p. Οι κόμβοι 1 και 3 έχουν κοινό κλειδί το a και μπορούν να το χρησιμοποιήσουν ως κλειδί για τη μεταξύ τους επικοινωνία. Αντίστοιχα οι κόμβοι 3 και 4 μπορούν να χρησιμοποιήσουν το y ως κλειδί. Με ανάλογο τρόπο οι υπόλοιποι κόμβοι θα χρησιμοποιήσουν τα κοινά κλειδιά για την επικοινωνία με άλλους κόμβους. Αξίζει να σημειώσουμε ότι και οι πέντε κόμβοι του δικτύου μπορούν να επικοινωνήσουν μεταξύ τους αρκεί να υπάρχει το κατάλληλο μονοπάτι. Για παράδειγμα ο κόμβος 1 μπορεί να επικοινωνήσει με τον 4 μέσω του κόμβου 3 αρκεί να υπάρχει ο κατάλληλος

συνδυασμός κλειδιών μεταξύ των άμεσα συνδεδεμένων κόμβων. Σε ένα δίκτυο αποτελούμενο απο 10.000 κόμβους και εφαρμόζοντας την τεχνική της προ-διανομής κλειδιών, ο αριθμός των κλειδιών που θα χρειάζονταν για τη λειτουργία του δικτύου ειναι 50 εκατ (*0,5N(N-1)*) θέτοντας σοβαρά προβλήματα περιορισμού μνήμης. Ο αριθμός αυτός μειώνεται εντυπωσιακά στα 2,5 εκατ κλειδιά εάν επιλεγεί σχήμα τυχαίας προ-διανομής κλειδιών RKP. Ελάχιστες απαιτήσεις σε κατανάλωση ενέργειας και αποθηκευτικό χώρο (λιγότεροι υπολογισμοί και ανταλλαγές μηνυμάτων) καθώς και εξασφάλιση ασφαλούς διανομής (τα κρυπτογραφικά κλειδιά είναι ήδη υπολογισμένα και διανεμημένα) είναι κάποια απο τα κύρια πλεονεκτήματα του RKP σχήματος. Το βασικό μειονέκτημα είναι ότι ενώ υποστηρίζει ανάκληση κλειδιών σε περιπτώσεις προσβολής κόμβων από κάποιον εισβολέα, δεν μπορεί να προβλέψει μεθόδους για την ανανέωση τους.



Σχήμα 4.7: Παράδειγμα τεχνικής τυχαίας προ-διανομής κλειδιών RKP

Q - Τυχαία προ-διανομή κλειδιών (Q-Random Key Pre-Distribution Q-RKP): Το σχήμα q-RKP είναι παρόμοιο με το RKP Σε αυτόν το μηχανισμό οι κόμβοι διαμοιράζονται τουλάχιστον q κρυπτογραφικά κλειδιά (*q>1*) και κάθε φορά που ανανεώνουν τα κλειδιά τους με τυχαία σειρά, χρησιμοποιούν διαφορετικές διαδρομές. Σε περίπτωση προσβολής και αποκάλυψης ενός κλειδιού, αυτό απορρίπτεται και οι κόμβοι επικοινωνούν με τα υπόλοιπα κλειδιά. Ωστόσο, ο μηχανισμός είναι ευάλωτος όταν ο εισβολέας επιτίθεται σε περισσότερους από έναν κόμβους, οπότε και δεν είναι πλέον αποτελεσματικός.

ΚΕΦΑΛΑΙΟ 5

5.1 Εισαγωγή

Σε προηγούμενο κεφάλαιο έγινε αναφορά και ανάλυση στις επιθέσεις που λαμβάνουν χώρα σε ένα ασύρματο δίκτυο αισθητήρων και βάλλονται ενάντια της πολυεπίπεδης αρχιτεκτονικής του. Το επίπεδο όμως που στοχεύει να πλήξει περισσότερο ένας επιτιθέμενος είναι αυτό του Δικτύου γιατί πάνω σε αυτό στεγάζονται οι μηχανισμοί ασφάλειας και δρομολόγησης του δικτύου. Το επίπεδο δικτύου έχει να αντιμετωπίσει διάφορες επιθέσεις με συνήθεις αυτές της επιλεκτικής προώθησης, εξαπάτησης αναγνώρισης, σκουληκότρυπας, Hello ροών, σιβυλλικής μορφής, καταβόθρας. Όλες αυτές οι επιθέσεις εκδηλώνονται έναντι των τυπικών πρωτοκόλλων δρομολόγησης που δίνουν βαρύτητα στην εξιόπιστη ανταλλαγή μηνυμάτων, στην εξοικονόμηση ενέργειας, στην απλότητα των υπολογισμών και καθόλου στην ασφαλή δρομολόγηση. Για την εξασφάλιση των απαιτήσεων ασφάλειας σε ένα ασύρματο δίκτυο αισθητήρων απαιτείται κάποιος ασφαλής μηχανισμός δρομολόγησης ο οποίος θα έχει να αντιμετωπίσει τέσσερις βασικές προκλήσεις [21]:

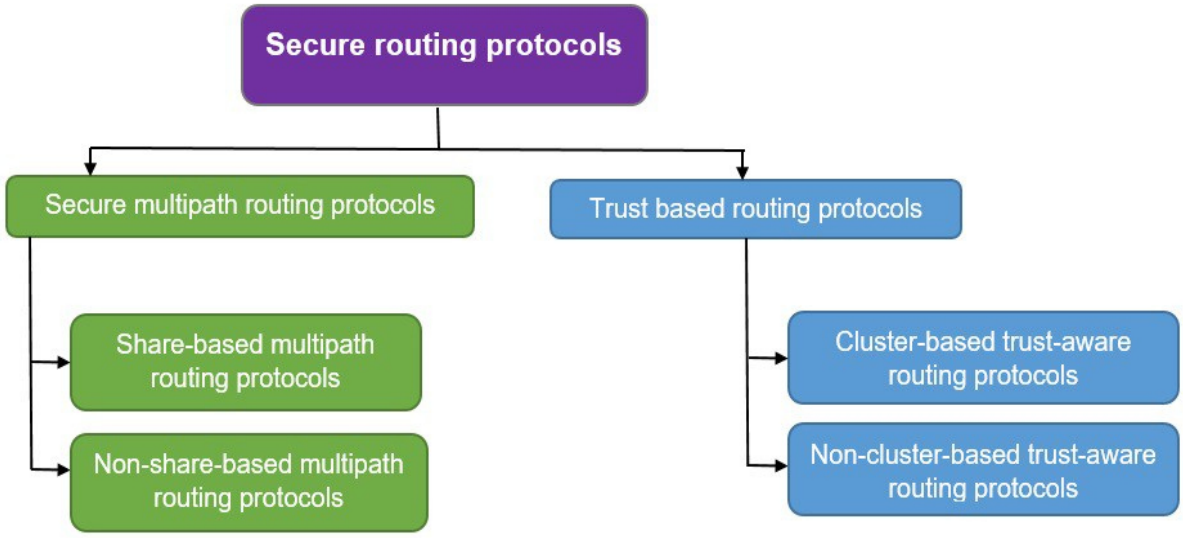
- Πρόληψη
- Ανίχνευση επίθεσης
- Αποκατάσταση λειτουργιών
- Ανοχή σε επιθέσεις

Για να μπορέσει λοιπόν ένα δίκτυο να αντέξει στις ανω προκλήσεις θα πρέπει κατά τον σχεδιασμό του να ληφθούν υπόψιν τεχνικές δρομολόγησης και ελέγχου ταυτότητας (αυθεντικοποίησης) των κόμβων και να χρησιμοποιηθούν

ισχυροί αλγόριθμοι κρυπτογράφησης της μεταδιδόμενης πληροφορίας έτσι ώστε να διασφαλίσουμε ότι όλοι οι κόμβοι επικοινωνίας είναι αξιόπιστοι.

Η δρομολόγηση μίας διαδρομής (Single-path routing) είναι ένα απλό πρωτόκολλο δρομολόγησης αλλά εύκολα μπορεί να μπλοκαριστεί από κάποιον εισβολέα. Επομένως, η πιο λογική προσέγγιση είναι μέσω δρομολόγησης πολλαπλών διαδρομών (multipath routing). Σε αυτήν την περίπτωση, ακόμη και αν εξελίσσεται επίθεση σε μερικές από αυτές τις πολλαπλές διαδρομές, τα δεδομένα μπορούν να φτάσουν με ασφάλεια στον προορισμό τους. Τα *ασφαλή πρωτόκολλα δρομολόγησης πολλαπλών διαδρομών* (Secure multipath routing protocols) μπορούν να διακριθούν περαιτέρω ανάλογα με το εάν τα αρχικά πακέτα δεδομένων διαιρούνται σε μικρά κομμάτια διαμοιρασμού,

Μια άλλη δημοφιλής μέθοδος για την αποφυγή επιθέσεων και τη πιθανότητα μιας επιτυχούς δρομολόγησης αποτελεί η *δρομολόγηση αξιοπιστίας* (trust routing). Σε αυτή τη μέθοδο δρομολόγησης διατηρείται μια τιμή εμπιστοσύνης για κάθε κόμβο, βασισμένη κυρίως στο ιστορικό των προωθήσεων του κάθε κόμβου. Μόνο οι κόμβοι με πολύ υψηλές τιμές εμπιστοσύνης επιλέγονται για να συμμετάσχουν στη διαδρομή δρομολόγησης. Οι τεχνικές διαχείρισης εμπιστοσύνης στη δρομολόγηση των αυτοοργανωμένων και των peer-to-peer δικτύων δεν είναι η βέλτιστη επιλογή για τα WSNs λόγω της αυξημένης κατανάλωσης πόρων σε ενέργεια και μνήμη στους κόμβους. Παρόλα αυτά, τα τελευταία χρόνια έχουν προταθεί πολλές νέες τεχνικές διαχείρισης εμπιστοσύνης με τα αντίστοιχα πρωτόκολλα δρομολόγησης. Επιπλέον, προκειμένου να εξοικονομήσουμε ενέργεια και να βελτιώσουμε την ασφάλεια στα WSNs, επιλέγεται τα περισσότερα από αυτά να είναι οργανωμένα σε ομάδες (clusters). Βάσει των προαναφερθέντων στη παρούσα εργασία θα αναφερθούμε α) στα ασφαλή πρωτόκολλα δρομολόγησης πολλαπλών διαδρομών με τις αντίστοιχες υποκατηγορίες τους και β) στα πρωτόκολλα δρομολόγησης αξιοπιστίας με τις αντίστοιχες κατηγορίες τους [1] όπως αυτά φαίνονται και διαχωρίζονται στο σχήμα 5.1



Σχήμα 5.1: Ταξινόμηση πρωτοκόλλων ασφαλούς δρομολόγησης στα WSNs

5.2 Ασφαλή πρωτόκολλα δρομολόγησης πολλαπλών διαδρομών (Secure multipath routing protocols)

Η δρομολόγηση μίας διαδρομής (single-path) είναι η πιο κοινή προσέγγιση στη δρομολόγηση. Ωστόσο στα WSNs για λόγους εξοικονόμησης πόρων στο δίκτυο, οι κόμβοι δεν είναι ανθεκτικοί σε παραβιάσεις και πιθανόν να τεθούν σε κίνδυνο. Επιπλέον, λόγω της ασύρματης επικοινωνίας πολλά είδη επιθέσεων μπορούν να διεξεχθούν και συνεπώς η μεταφορά δεδομένων μέσω ενός μονοπατιού μπορεί πολύ εύκολα να παραβιαστεί. Γ' αυτό το λόγο έχει προταθεί ένας αριθμός πρωτοκόλλων που μειώνουν τη πιθανότητα παραβίασης της ασφάλειας χρησιμοποιώντας πολλαπλές διαδρομές για δρομολόγηση πακέτων. Παρακάτω θα αναφερθούμε στα δύο βασικά σχήματα δρομολόγησς με χρήση πολλαπλών διαδρομών. Στα *διαμοιραζόμενα πρωτόκολλα δρομολόγησης πολλαπλών διαδρομών (Share-based multipath routing)* και στα *μη διαμοιραζόμενα πρωτόκολλα δρομολόγησης πολλαπλών διαδρομών (non-share-based multipath routing).*

5.2.1 Πρωτόκολλα δρομολόγησης πολλαπλών διαδρομών που δεν βασίζονται στον διαμοιρασμό (non-share-based multipath routing)

Το πρωτόκολλο δρομολόγησης ανεκτικής παρείσφρησης για τα ασύρματα δίκτυα αισθητήρων INSENS (Inrusion Tolerant Routing protocol for Wireless Sensor Networks) είναι ένα πρωτόκολλο που χρησιμοποιεί τη τεχνική των πολλαπλών διαδρομών και συμβάλλει με ασφάλεια και αποτελεσματικότητα στην ασφαλή δρομολόγηση βασισμένη σε δομή δένδρου [26] [51]. Βασικός του στόχος είναι η ανοχή του δικτύου σε ζημιά που προκλήθηκε απο κάποιον εισβολέα που έχει θέσει σε κίνδυνο τους αναπτυσσόμενους κόμβους και σκοπεύει στη τροποποίηση ή τον αποκλεισμό των πακέτων. Για τον περιορισμό ή τον εντοπισμό της πάσχουσας περιοχής, το πρωτόκολλο ενσωματώνει κατανεμημένους μηχανισμούς ασφάλειας, συμπεριλαμβανομένων της μεθόδου παραγωγής μιας χρήσης κλειδιών (one-way hash chain) και κωδικούς ελέγχου ταυτότητας ένθετων κλειδιών που προστατεύουν απο επιθέσεις τύπου σκουληκότρυπας καθώς και δρομολόγησεις πολλαπλών διαδρομών. Ο κύριος υπολογισμός των μετρήσεων διαδραματίζεται στον σταθμό βάσης ενώ η υπόλοιπη διαδικασία επεξεργασίας ολοκληρώνεται από τους αισθητήριους κόμβους. Ο σταθμός βάσης είναι ο κατεξοχήν υπεύθυνος για την κατασκευή και διανομή των πινάκων δρομολόγησης στους υπόλοιπους κόμβους του δικτύου. Το INSENS χρησιμοποιεί τρείς φάσεις λειτουργίας: α) πλημμύρα β) προώθηση περιεχομένων πινάκων δρομολόγησης γ) προώθηση δεδομένων. Η απόδοση ασφάλειας με χρήση του συγκεκριμένου πρωτοκόλλου είναι ανάλογη του κόστους απόδοσης ενέργειας. Για την διανομή των πινάκων δρομολόγησης από τον σταθμό βάσης στους αισθητήριους κόμβους απαιτούνται υψηλά ποσοστά ενέργειας κυρίως σε ευρείας κλίμακας εφαρμογές. Αυτό σημαίνει ότι απαιτούνται ικανά ποσοστό ενέργειας για να πετύχουμε υψηλά στάνταρ ασφάλειας και αυτό είναι το βασικό μειονέκτημά του. Ένα δεύτερο μειονέκτημα είναι ότι δεν βελτιώνει την εμπιστευτικότητα των δεδομένων γιατί δεν χρησιμοποιεί κάποιον αλγόριθμο κρυπτογράφησης (υπάρχει μόνο ένα κοινό κλειδί κατά την διαδικασία ανακάλυψης των γείτονων κόμβων) γεγονός που διευκολύνει τη τροποποίησή τους. Τέλος αξίζει να σημειώσουμε ότι χρησιμοποιείται ο

αλγόριθμος Dijkstra για την επιλογή της συντομότερης διαδρομής ενώ εν συνεχεία χρησιμοποιείται σετ κόμβων για τη δημιουργία πολλαπλών διαδρομών.

Το ασφαλές και ενεργειακής απόδοσης πολλαπλών διαδρομών πρωτόκολλο δρομολόγησης SEEM (Secure and Energy-Efficient Multipath routing protocol) εστιάζει στη μεγιστοποίηση της διάρκειας ζωής του δικτύου και στην αύξηση του ασφάλειάς του. Κάθε κόμβος διατηρεί μια λίστα από κόμβους που χρησιμοποιούνται ως μεταφορείς για την προώθηση των πακέτων προς τον σταθμό βάσης. Ο υπολογισμός των διαδρομών δρομολόγησης μεταφέρεται στις αρμοδιότητες του σταθμού βάσης και αυτό καθιστά το πρωτόκολλο ισχυρό ενάντια στις επιθέσεις που προσελκύουν δεδομένα από άλλους αισθητήριους κόμβους διαφημίζοντας μια υψηλής ποιότητας διαδρομή προς τον σταθμό βάσης. Ο σταθμός βάσης χρησιμοποιείται ως εξυπηρετητής και οι κόμβοι ως πελάτες. Χρησιμοποιεί δλδ το ίδιο μοντέλο με αυτό της αρχιτεκτονικής των προγραμμάτων πελάτη/εξυπηρετητή [51]. Ο σταθμός βάσης αναλαμβάνει την ευθύνη της ανακάλυψης διαδρομών, της συντήρησης και της επιλογής της καταάλληλης διαδρομής. Επίσης με βάση το τρέχον ενεργειακό επίπεδο των κόμβων επιλέγει περιοδικά μια νέα διαδρομή. Το SEEM εξετάζει ταυτόχρονα την εξασφάλιση ενεργειακής απόδοσης και την παροχή ασφάλειας στο δίκτυο. Γενικότερα έχει αποδειχθεί ότι συμβάλει στην γενικότερη απόδοση του δικτύου, στην αποτελεσματική επικοινωνία μεταξύ των κόμβων και στην μακρά διάρκεια ζωής του δικτύου. Είναι επίσης ανθεκτικό σε επιθέσεις καταβόθρας, σκουληκότρυπας και επιλεκτικής προώθησης. Η κατασκευή πολλαπλών διαδρομών δρομολόγησης λαμβάνει υπόψιν τα επιτρεπόμενα επίπεδα κατανάλωσης ενέργειας του δικτύου, ωστόσο τα δεδομένα που διακινούνται με χρήση του SEEM μπορούν να τροποποιηθούν κατα τη μεταφορά τους καθότι το πρωτόκολλο δεν χρησιμοποιεί αλγόριθμο κρυπτογράφησης ούτε μηχανισμούς ελέγχου ταυτότητας με χρήση κλειδιών.

Το πρωτόκολλο ESARS (Energy and Security Aware Route Selection) έχει στόχο την εύρεση της βέλτιστης διαδρομής μεταξύ δύο αισθητήριων κόμβων και όχι της βέλτιστης διαδρομής από τους κόμβους προς τον σταθμό βάσης όπως

κάνουν άλλωστε τα περισσότερα στη κατηγορία αυτή πρωτόκολλα δρομολόγησης. Εφαρμόζοντας έναν αλγόριθμο δρομολόγησης πολλαπλών διαδρομών, το ESARS βρίσκει εναλλακτικές διαδρομές μεταξύ κόμβου πηγής και κόμβου προορισμού. Διαδρομές που περιλαμβάνουν κόμβους με ελάχιστα αποθέματα ενέργειας, εξαιρούνται της διαδικασίας εύρεσης διαδρομής από το ίδιο το πρωτόκολλο. Εν συνεχεία το πρωτόκολλο επιλέγει ως τελική διαδρομή δρομολόγησης, μια διαδρομή που είναι σχετικά μικρή και δεν περιέχει κόμβους με μεγάλο αριθμός γειτόνων. Το σκεπτικό επιλογής της βέλτιστης διαδρομής βάσει του ελάχιστου μήκους της είναι ότι οι μεγαλύτερες διαδρομές έχουν μεγαλύτερη πιθανότητα να παραβιαστούν. Επίσης, ένας κόμβος με μεγάλο αριθμό γειτόνων είναι πιθανό να συμπεριληφθεί σε περισσότερες διαδρομές δρομολόγησης και ως εκ τούτου η ενέργειά του να εξαντληθεί γρήγορα. Μετά το πέρας εύρεσης της βέλτιστης (μικρότερης) διαδρομής δρομολόγησης θα πρέπει να καθοριστεί το επίπεδο ασφάλειας αυτής της διαδρομής. Διαδρομές που περιέχουν κόμβους χαμηλής εμπιστοσύνης ή είναι σχετικά μεγάλες, διατρέχουν μεγαλύτερο κίνδυνο παραβίασης. Σε αυτή τη περίπτωση προτείνεται η λύση μεγάλων κλειδιών κρυπτογράφησης καθώς και μεγάλων κωδικών αυθεντικοποίησης μηνυμάτων. Ένα μειονέκτημα του ESARS είναι ότι περιοδικά ο κόμβος πηγής πρέπει να μαθαίνει το επίπεδο ενέργειας όλων των κόμβων στις εναλλακτικές διαδρομές με αποτέλεσμα τη συνολική επιβάρυνση του δικτύου.

Ένα ακόμη πρωτόκολλο που συναντάμε σε αυτή τη κατηγορία είναι το BEARP (Balanced Energy-Aware Routing Protocol) το οποίο περιλαμβάνει τρείς φάσεις: α) την αναζήτηση του γείτονα, β) την αναζήτηση της διαδρομής δρομολόγησης και γ) τη φάση συντήρησης της δρομολόγησης. Η πρώτη φάση εκτελείται στον σταθμό βάσης που κατασκευάζει την τοπολογία του δικτύου. Η χαρτογράφηση του δικτύου εξαρτάται από τα αποθέματα ενέργειας του κόμβου κεφαλής. Στη δεύτερη φάση εύρεσης της διαδρομής, ο σταθμός βάσης στέλνει ένα αίτημα ενδιαφέροντος και όποιοι κόμβοι ικανοποιούνται σχετικά, τότε απαντούν. Στη συνέχεια ο σταθμός βάσης υπολογίζει τη συντομότερη διαδρομή μεταξύ του ιδίου και του αντίστοιχου κόμβου στη τοπολογία, στέλνοντάς την στον κόμβο, απαντώντας με τη σειρά του

με ένα αναγνωριστικό επιβεβαίωσης προς τον σταθμό βάσης. Η ανταλλαγή των δεδομένων διασφαλίζεται με κρυπτογράφηση και με χρήση κατάλληλων μηχανισμών ελέγχου ταυτότητας. Στη φάση της συντήρησης διαδρομής στόχος είναι ο εντοπισμός των μολυσμένων κόμβων. Αυτό επιτυγχάνεται με αποστολή ερώτησης (εάν ο ύποπτος κόμβος έχει προωθήσει το πακέτο που ερευνάται) προς τους κανονικούς κόμβους εντός γειτονιάς του υποτιθέμενου μολυσμένου κόμβου. Σε περίπτωση που επιβεβαιωθεί συμβάν παραβίασης κόμβου, ο σταθμός βάσης επιλέγει εναλλακτική διαδρομή δρομολόγησης παρακάπτοντας τον μολυσμένο κόμβο. Το πρωτόκολλο BEARP μπορεί να αντιμετωπίσει τις επιθέσεις σκουληκότρυπας, επιλεκτικής προώθησης και τρύπας νεροχύτη.

5.2.2 Πρωτόκολλα δρομολόγησης πολλαπλών διαδρομών που βασίζονται στον διαμοιρασμό (share-based multipath routing protocols)

Το H-SPREAD είναι ένα υβριδικό πρωτόκολλο δρομολόγησης που συμβάλλει στην αξιοπιστία και ασφάλεια της ανταλλαγής μηνυμάτων σε WSN δίκτυα. Το H-SPREAD χρησιμοποιεί ένα κατανεμημένο N σε 1 πρωτόκολλο εύρεσης πολλαπλών διαδρομών που είναι ικανό να βρεί πολλαπλές διαδρομές κόμβου-αποσύνδεσης μεταξύ αισθητήριων κόμβων και σταθμού βάσης. Αυτή η τεχνική διασποράς δεδομένων πολλαπλών διαδρομών συνδυάζεται με ένα διαμοιραζόμενο σχήμα και έτσι το πρωτόκολλο μπορεί να μεταφέρει επιτυχώς τα δεδομένα απο τους κόμβους στον σταθμό βάσης όταν ο αριθμός των κόμβων που έχουν παραβιαστεί στο δίκτυο είναι μικρός. Συγκεκριμένα σε ένα μυστικό διαμοιραζόμενο σχήμα, τα προς αποστολή πακέτα είναι διαχωρισμένα σε M τμήματα χρησιμοποιώντας έναν (T,M) μυστικό μηχανισμό διαμοιρασμού με αποτέλεσμα τα τμήματα αυτά να αποστέλλονται μεμονωμένα στον σταθμό βάσης. Για να μπορεί το πακέτο να αναγνωσθεί και να ανακτηθεί θα πρέπει να φθάσουν στον σταθμό βάσης τουλάχιστον T τμήματα. Το πρωτόκολλο εύρεσης πολλαπλών διαδρομών περιλαμβάνει δύο φάσεις. Στην πρώτη φάση ανάλογα με την πυκνότητα του δικτύου ανακαλύπτεται συγκεκριμένος αριθμός διαδρομών

κόμβου-αποσύνδεσης. Στη δεύτερη φάση ανταλλάσονται μεταξύ των κόμβων οι διαδρομές κόμβου-αποσύνδεσης που αποφασίστηκαν κατά την πρώτη φάση με αποτέλεσμα ο αριθμός των κόμβων που γνωρίζει αυτές τις διαδρομές να είναι μεγαλύτερος στο τέλος της δεύτερης φάσης.

Στη βιβλιογραφία προτείνεται ένα σχήμα βασισμένο σε ένα μυστικό σχήμα κοινής χρήσης και ένα πρωτόκολλο δρομολόγησης διασποράς. Η διαδρομή που θα ακολουθήσει κάθε διαμοιραζόμενο πακέτο αποφασίζεται στον “αέρα” σε κάθε άλμα, με τυχαία επιλογή του επόμενου κόμβο. Με την τυχαιοποιημένη επιλογή του επόμενο κόμβου σχεδόν εκμηδενίοζνται οι διαδρομές κόμβου-αποσύνδεσης. Το βασικό πλεονέκτημα του πρωτοκόλλου τυχαίας παραγωγής διαδρομής του επόμενου άλματος αποτελεί το γεγονός ότι κάθε κόμβος που προωθεί τα δεδομένα στον επόμενο κόμβο μέχρις ότου φθάσουν στον κόμβο προορισμού, δεν μπορεί να γνωρίζει τις διαδρομές δρομολόγησης εκ των προτέρων γιατί πολύ απλά δεν ξέρει κάθε φορά ποιός θα είναι ο επόμενος κόμβος που θα συναντήσει. Αυτομάτως δημιουργείται ένα καθεστώς προστασίας έναντι επιθέσεων που είναι σχεδόν ακατόρθωτο να παραβιαστεί.

Ένα ακόμη πρωτόκολλο δρομολόγησης διασποράς είναι το SEDR (Secure and Energy-efficient Disjoint Route). Βασικός στόχος του SEDR είναι η αύξηση διάρκειας ζωής του δικτύου και η προστασία από τις επιθέσεις «μαύρης τρύπας». Η λειτουργία του βασίζεται σε τρείς φάσεις. Στη πρώτη φάση τμήματα του αρχικού πακέτου αποστέλλονται σε τυχαία επιλεγμένους αισθητήριους κόμβους στην τοπική περιοχή του κόμβου προέλευσης. Στη δεύτερη φάση τα τμήματα διαμοιρασμού από τους κόμβους που επιλέχθηκαν στο πρώτο στάδιο μεταφέρονται σε άλλους κόμβους με την προϋπόθεση ότι ο προορισμός θα πρέπει να απέχει τον ίδιο αριθμό αλμάτων από τον σταθμό βάσης όσο και ο αρχικός κόμβος της διαδρομής. Τέλος, στη τρίτη φάση κάθε τμήμα διαμοιρασμού αποστέλλεται στον σταθμό βάσης ακολουθώντας το συντομότερο μονοπάτι. Με την διασπορά των πακέτων στο δίκτυο το πρωτόκολλο επιτυγχάνει καλύτερη διαχείριση ενέργειας στους κόμβους και επίσης αμύνεται αποτελεσματικά έναντι επιθέσεων «μαύρης τρύπας».

Ένα ακόμη πρωτόκολλο διαμοιρασμού πολλαπλών διαδρομών που αποτελεί βελτίωση του πρωτοκόλλου H-SPREAD προσφέροντας περισσότερες εναλλακτικές διαδρομές και μεγαλύτερη ασφάλεια στη φάση κατασκευής της διαδρομής δρομολόγησης αποτελεί το SMRP (Sub-branch Multipath Routing Protocol). Το συγκεκριμένο πρωτόκολλο δημιουργεί εναλλακτικές διαδρομές από τον κάθε κόμβο προς τον σταθμό βάσης αλλά με την προϋπόθεση ότι κάθε μία από αυτές τις διαδρομές θα πρέπει να περνά από διαφορετικούς κόμβους του δέντρου που ξεκινάει από τον σταθμό βάσης για τον λόγο ότι οι κόμβοι κοντά στον σταθμό βάσης επιτηρούνται καλά και αυτό συνεπάγεται μικρή πιθανότητα παραβίασης. Στη βιβλιογραφία αναφέρεται και το SEIF (Secure and Efficient Intrusion-Fault tolerant) πρωτόκολλο δρομολόγησης το οποίο είναι μια ασφαλής έκδοση του SMRP. Το SEIF στηρίζεται στη τεχνική των συναρτήσεων μονόδρομου κατακερματισμού για να παρέχει αυθεντικοποίηση των κόμβων που αποστέλλουν μηνύματα ελέγχου. Έτσι λοιπόν ένας εισβολέας δεν μπορεί να πλαστογραφήσει έναν κόμβο γονέα στο δένδρο δρομολόγησης. Το SEIF δεν μπορεί να ανιχνεύσει επιθέσεις σκουληκότρυπας.

5.3 Πρωτόκολλα δρομολόγησης που βασίζονται στην αξιοπιστία (trust based routing protocols)

Τα πρώτα πρωτόκολλα δρομολόγησης που συναντάμε στη βιβλιογραφία με γνώμονα την εμπιστοσύνη, είναι τα T-RGR και EMPIRE τα οποία και στηρίχθηκαν στους προκατόχους τους προσδίδοντας στη παράμετρο εμπιστοσύνη μια καλύτερη προσέγγιση. Αρκετά ακόμη σχήματα δρομολόγησης εμπιστοσύνης (πχ ERRM, TCLM, TARF, SETM) αναπτύχθηκαν στη συνέχεια, ενσωματώνοντας πολλαπλά χαρακτηριστικά / μετρήσεις σε μια πιο ολοκληρωμένη μορφή. Παρακάτω θα εστιάσουμε στα πιο πρόσφατα (και σημαντικά) πρωτόκολλα δρομολόγησης εμπιστοσύνης δίνοντας έμφαση στα καινοτόμα χαρακτηριστικά τους όπως επίσης στα πλεονεκτήματα και μειονεκτήματά τους.

5.3.1 Αξιόπιστα πρωτόκολλα δρομολόγησης χωρίς να βασίζονται σε ομάδες (Non-cluster-based trust-aware routing protocols)

Σύμφωνα με το [1] προτείνεται ένα ενεργειακά αποδοτικό ασφαλές μοντέλο δρομολόγησης (Active Trust) βασισμένο στο Active trust το οποίο λειτουργεί αποδοτικό στην ανίχνευση επίθεσης μαύρης τρύπας. Το Active Trust είναι το πρώτο σχήμα δρομολόγησης που χρησιμοποιεί ενεργή ανίχνευση δρομολόγησης για την αντιμετώπιση επιθέσεων μαύρης τρύπας. Διενεργεί πολλαπλούς ελέγχους σε διαδρομές υψηλής εμπιστοσύνης αξιοποιώντας την ενέργεια από το πεδίο του sink κόμβου. Κατα συνέπεια , η τρέχουσα εμπιστοσύνη των κόμβων μπορεί να υπολογισθεί πριν τη δρομολόγηση των δεδομένων και αφού έχει επιτευχθεί επίθεση μαύρης τρύπας. Οι βασικοί ενδείκτες απόδοσης στου Active Trust (ενεργειακή απόδοση, διάρκεια ζωής δικτύου, επιτυχία και αποτελεσματικότητα δρομολόγησης) αποδεικνύονται ισχυρότεροι συγκριτικά με άλλα σχήματα. Ωστόσο το μοντέλο λαμβάνει υπόψιν μόνο τις επιθέσεις μαύρης τρύπας κατα τη διαδικασία αξιολόγησης της εμπιστοσύνης χωρίς να μπορεί να αντιμετωπίσει κάποια άλλη επίθεση. Το Active Trust χρησιμοποιείται μονο για δρομολογήσεις προς τον σταθμό βάσης και όχι για την επικοινωνία μεταξύ των αισθητήριων κόμβων.

Ένα ακόμη σχήμα δρομολόγησης όπως είναι το TAIV (Trust with Abstract Information Verified) χρησιμοποιείται για την ασφαλή δρομολόγηση μεταξύ των αισθητήριων κόμβων. Η βασική διαφορά μεταξύ του TAIV και του προηγούμενου σχήματος είναι ότι διαθέτει δύο μεμονωμένες διαδρομές δρομολόγησης: τη διαδρομή δικτύου κορμού (χρησιμοποιείται για την αποστολή πακέτων) και τη βοηθητική διαδρομή (χρησιμοποιείται για την μεταφορά επαληθευμένων μηνυμάτων). Το TAIV σε συδυασμό με τη σύνδεση κυρίαρχης δομής set, όχι μόνο αυξάνει την ασφάλεια σε μια διαδρομή δικτύου με ελάχιστο κόστος αλλά προσδιορίζει επίσης και τη θέση των κακόβουλων κόμβων. Ωστόσο παραμένει μία πολύ καλή λύση μόνο για επιθέσεις «μάυρης τρύπας». Επίσης λόγω της εσωτερικής του διάρθρωσης (διαδρομή δρομολόγησης δικτύου κορμού) είναι δύσκολο να προσαρμοστεί σε WSNs που στηρίζονται σε ομάδες.

Στη συνέχεια θα αναλύσουμε ένα δυναμικό πρωτόκολλο δρομολόγησης που βασίζεται στην εμπιστοσύνη και δεν είναι άλλο απο το TERP (Trust and Energy Aware Routing Protocol). Το TERP είναι ικανό να ανιχνεύει δυναμικά και να απομονώνει δυσλειτουργικούς/λανθασμένους κόμβους στο στάδιο αξιολόγησης εμπιστοσύνης καθώς τα χαρακτηριστικά της ενεργειακής απόδοσης ενσωματώνονται στο στάδιο ρύθμισης της δρομολόγησης βοηθώντας μ αυτόν τον τρόπο στην εξισορρόπηση μεταξύ αξιόπιστων κόμβων. Το TERP κάνει χρήση μιας σύνθετης λειτουργίας δρομολόγησης όπου οι αποφάσεις λαμβάνονται βάσει της αξιοπιστίας, της ενέργειας και του αριθμού αλμάτων. Επίσης υποθέτει ότι δεν δύναται να συγκρουσθούν μεταξύ τους οι κακόβουλοι κόμβοι καθώς και ότι δεν επιτρέπεται η προσθήκη ή η κατάργηση αισθητήριων κόμβων μετά τη σύγκληση του δικτύου.

Για την εδραίωση ενός μοντέλου αξιοπιστίας που θα έχει την ικανότητα αντιμετώπισης διαφόρων κακόβουλων επιθέσεων, προτείνεται η λύση ενός ολοκληρωμένου πλαισίου αξιοπιστίας με την ονομασία TSRF (Trust-aware Security Routing Framework). Αρχικά αναλύει τις επιθέσεις που εκδηλώνονται απέναντι σε αξιόπιστα πρωτόκολλα δρομολόγησης προτείνοντας παράλληλα συγκεκριμένο υπολογισμό της αξιοπιστίας καθώς και σχήματα που συμβάλλουν στην αξιοπιστία με απώτερο στόχο την αντιμετώπιση επιθέσεων. Επιπλέον, έχει σχεδιαστεί ένας βελτιστοποιημένος αλγόριθμος δρομολόγησης που λαμβάνει υπόψιν όχι μόνο τα χαρακτηριστικά της μέτρησης αξιοπιστίας, αλλά και κάποιες QoS απαιτήσεις στην επιλογή της διαδρομής. εν τω μεταξύ το σύνολο το δρομολόγιο γενικά διατηρείται χαμηλό. Παρά την εγκυρότητα των παραπάνω βημάτων στη βελτίωση της ασφάλειας, η ενέργεια των κόμβων δεν λαμβάνεται υπόψιν στη λήψη των αποφάσεων δρομολόγησης.

Στο [1] προτείνεται ένα αποδοτικό κατ’ απαίτηση αξιοπιστίας πρωτόκολλο TSR (Time Switching-based Relaying) δρομολόγησης λαμβάνοντας υπόψιν το ποσοστό ακρίβειας πακέτου ως κριτήριο αξιολόγησης και χρησιμοποιώντας τη μέθοδο πρόβλεψης κανόνων συγκεγχυμένης λογικής για την αξιολόγηση της αξιοπιστίας των κόμβων. Μια πηγή μπορεί να δημιουργήσει πολλαπλές διαδρομές

χωρίς βρόχους προς έναν προορισμό και κάθε διαδρομή να έχει ένα διάνυσμα αξιολόγησης που αποτελείται από τον αριθμό των αλμάτων και τη τιμή αξιοπιστίας της διαδρομής. Ένας προορισμός θα απαντήσει με εξειδικευμένες διαδρομές ως υποψήφιοι που πληρούν τις απαιτήσεις αξιοπιστίας της μεταδιδόμενης πληροφορίας. Το πιο σύντομο μονοπάτι θα επιλεγεί ως η διαδρομή μετάδοσης. Σε σύγκριση με τα περισσότερα πρωτόκολλα δρομολόγησης που βασίζονται στην αξιοπιστία, το TSR αγνοεί τις προτάσεις από τρίτους κόμβους καθ όλη τη διαδικασία υπολογισμού της αξιοπιστίας. Εξάλλου, η διεργασία επιλογής της βέλτιστης διαδρομής εκτελείται από τον κόμβο νεροχύτη, ο οποίος θα μπορούσε να οδηγήσει στην ταχύτερη εξάντληση της ενέργειας του.

Τέλος, στη κατηγορία των αξιόπιστων πρωτοκόλλων δρομολόγησης χωρίς να βασίζεται σε ομάδες ανήκει και το πρωτόκολλο κλιμακούμενης προσέγγισης γεωγραφικής δρομολόγησης ATSR (Ambient Trust Sensor Routing) το οποίο υιοθετεί την αρχή της γεωγραφικής δρομολόγησης που προσφέρει υψηλή επεκτασιμότητα λόγω της λειτουργίας σε τοπικό επίπεδο [51]. Ένα κατανεμημένης εμπιστοσύνης μοντέλο έχει σχεδιασθεί για να προστατεύει αποτελεσματικά από τις επιθέσεις δρομολόγησης. Η δρομολόγηση βασίζεται σε μεταβλητές γεωγραφικής θέσης και εμπιστοσύνης. Αξίζει να σημειώσουμε ότι το ATSR αποδίδει καλύτερα όσον αφορά στο χρόνο παράδοσης, τη χρονοκαθυστέρηση και τη βελτιστοποίηση της διαδρομής. Το συγκεκριμένο πρωτόκολλο κάνει χρήση σχήματος συστάδας για τη μείωση κατανάλωσης ενέργειας και τη δημιουργία ενός μοντέλου εμπιστοσύνης στην ασφάλεια.

Πίνακας 5.1: Αξιόπιστα πρωτόκολλα δρομολόγησης χωρίς να βασίζονται σε ομάδες

Πρωτόκολλο	Μεθοδολογία	Τιμές αξιοπιστίας	Πλεονεκτήματα	Περιορισμοί	Επιθέσεις
ACTIVE TRUST	Δρομολόγηση ενεργού εντοπισμού (εκκίνηση πολλαπλών διερευνητικών διαδρομών)	Υπολογίζονται βάσει συστάσεων των γείτονων κόμβων και του πρόσφατου ιστορικού των κόμβων	Υψηλής απόδοσης αισθητήρες (απόδοση ενέργειας, διάρκεια ζωής δικτύου, επιτυχής δρομολόγηση)	Επικεντρώνεται σε επιθέσεις μαύρης τρύπας. Δρομολογεί με βασικό γνώμονα προορισμού τον σταθμό βάσης	Μαύρης τρύπας, αλλοίωσης
TAIV	Χρήση δύο ξεχωριστών μονοπατιών δρομολόγησης (μονοπάτι δικτύοθ κορμού για αποστολή πακέτων και βοηθητικής διαδρομής για αποστολή επαληθευμένων πακέτων)	Αυξάνονται ή μειόνονται για όλους τους κόμβους ανάλογα με την επιτυχία στην αποστολή των πακέτων	Αυξημένο ποσοστό επιτυχίας στη δρομολόγηση. Αποτελεσματική στον γεωγραφικό προσδιορισμό των κακόβουλων κόμβων	Επικεντρώνεται μόνο σε επιθέσεις μαύρης τρύπας. Δεν μπορεί να ενσωματωθεί σε σχήματ WSNs που βασίζονται σε ομάδες	Μαύρης τρύπας, αλλοίωσης
TERP	Ισορροπημένη λειτουργία δρομολόγησης όπου οι αποφάσεις λαμβάνονται βάσει της αξιοπιστίας, ενέργειας και του αριθμό αλμάτων	Ισορροπημένος συνδυασμός άμεσων / έμμεσων τιμών αξιοπιστίας και μελλοντική εκτίμηση συμπεριφοράς.	Υψηλή απόδοση ενέργειας. Βελτιωμένος μηχανισμός συντήρησης διαδρομής.	Επικεντρώνεται μόνο σε επιθέσεις μαύρης τρύπας.Δεν επιτρέπει την προσθήκη ή διαγραφή κόμβων.	Μαύρης τρύπας, αλλοίωσης
TSRF	Μαθηματικές μέθοδοι (εύρεση της βέλτιστης διαδρομής σε ένα σταθμισμένο γράφημα χρησιμοποιώντας μεταβλητή δρομολόγησης πολλαπλών χαρακτηριστικών)	Ισορροπημένος συνδυασμός άμεσων /έμμεσων τιμών αξιπιστίας (με βάση το κλάσμα προώθησης).	Αποτελεσματικότητα απέναντι στις περισσότερες επιθέσεις. Αποτρέπει επιθέσεις διαχείρισης των τιμών αξιοπιστίας.	Η ενέργεια των κόμβων δεν λαμβάνεται υπόψη. Αυξημένο φόρτο στην επικοινωνία.	Μαύρης τρύπας, αλλοίωσης, καταβόθρας
TSR	Εκκίνηση διαδικασίας εύρεσης διαδρομής (πολλαπλές διαδρομές), επιλέγοντας τελικά τη συντομότερη διαδρομή που πληροί τις απαιτήσεις αξιοπιστίας.	Οι άμεσες τιμές αξιοπιστίας ενισχύονται από τη μελλοντική εκτίμηση συμπεριφοράς (βάσει μοντέλου πρόβλεψης ασαφούς λογικής)	Αποτελεσματικότητα απέναντι στις περισσότερες επιθέσεις. Ελάχιστο φόρτο στην επικοινωνία.	Η σύσταση αξιοπιστίας και η ενέργεια των κόμβων δεν λαμβάνονται υπόψιν	Μαύρης τρύπας, αλλοίωσης, καταβόθρας

5.3.2 Αξιόπιστα πρωτόκολλα δρομολόγησης που βασίζονται σε ομάδες (cluster-based trust-aware routing protocols)

Η εκλογή ενός κακόβουλου ή παραβιασμένου κόμβου ως αρχηγός συστάδας (Cluster Head) είναι μία από τις πιο σημαντικές παραβιάσεις στα ασύρματα δίκτυα αισθητήρων που βασίζονται στην αξιοπιστία και το μηχανισμό εκλογής των πιο αξιόπιστων κόμβων ως αρχηγούς ομάδας (CH). Σε αυτά τα σχήματα χρησιμοποιείται ένας μηχανισμός που βασίζεται στην αξιοπιστία για την εκλογή αξιόπιστων κόμβων ως αρχηγοί ομάδας με χρήση αλγορίθμου που χρησιμοποιεί μια τιμη πιθανότητας γι αυτή την εκλογή. Οι αιθητήριο κόμβοι προσεγγίζουν την ομάδα που βασίζεται στην τιμή αξιοπιστίας του εκάστοτε κόμβου ομαδάρχη. Αυτή η διαδικασία επαναλαμβάνεται μέχρις ότου όλοι οι κόμβοι προσεγγίσουν μία ομάδα υποχρεώνοντας τον αλγόριθμο να καταναλώνει πολύ ενέργεια. Το πρωτόκολλο TLEACH που βασίζεται στην αξιοπιστία (Trust-based LEACH) προτάθηκε για να παρέχει ασφάλεια στον αλγόριθμο LEACH. Το TLEACH εμποδίζει τους κακεντρεχής κόμβους να γίνουν ομαδάρχες (cluster heads). Απαρτίζεται από:

α) το τμήμα διαχείρισης αξιοπιστίας χρησιμοποιώντας άμεσες παρατηρήσεις όπως ακριβώς ένας μηχανισμός ανταλλαγής αξιόπιστων πληροφοριών που δημιουργεί και διατηρεί αξιόπιστη πληροφορία μεταξύ γείτονων κόμβων και

β) το τμήμα δρομολόγησης που βασίζεται στην αξιοπιστία που είναι μια τροποποιημένη έκδοση του LEACH σε συνδυασμό με το τμήμα λήψης αποφάσεων που βασίζεται στην αξιοπιστία .

Αν και το πρωτόκολλο είναι ανθεκτικό απέναντι σε κακόβουλες επιθέσεις, είναι αρκετά ευάλωτο σε επιθέσεις σκευωρίας.

Ένα ακόμη πρωτόκολλο δρομολόγησης που βασίζεται σε έναν εξιόπιστο πυρήνα δέντρου, στοχεύοντας στην οικοδόμηση μιας ασφαλούς δομής αξιοπιστίας και στην παράταση της διάρκειας ζωής του δικτύου είναι το RATCT (Routing Algorithm base on Trustworthy Core Tree). Οι κόμβοι με υψηλότερα επίπεδα αξιοπιστίας και αποθέματα ενέργειας εκλέγονται ως ομαδάρχες. Όλοι οι κόμβοι ομαδάρχες είναι οργανωμένοι σε έναν αξιόπιστο πυρήνα δέντρου με τον σταθμό βάσης να αποτελεί τη ρίζα του δέντρου. Ένα μοντέλο αξιοπιστίας χρησιμοποιείται για την αξιολόγηση της αξιοπιστίας των κόμβων και τον εντοπισμό κόμβων με κακόβουλη συμπεριφορά. Κάθε κόμβος διατηρεί ένα ζευγάρι δημόσιου και ιδιωτικού κλειδιού για την κρυπτογράφηση και την ψηφιακή υπογραφή των προς αποστολή δεδομένων. Ο σταθμός βάσης εντοπίζει κακόβουλες συμπεριφορές αναλύοντας τα κρυπτογραφημένα και με ψηφιακή υπογραφή δεδομένα. Το RATCT εντοπίζει αποτελεσματικά μια κακόβουλη συμπεριφορά ωστόσο η οικοδόμηση του πυρήνα δέντρου και ο υπολογισμός των τιμών αξιοπιστίας απαιτούν υψηλά ποσοστά ενέργειας.

Το πρωτόκολλο ασφαλούς δρομολόγησης που βασίζεται σε αξιοπιστία TEESR (Trust-based Energy Efficient Secure Routing protocol) χρησιμοποιεί τους κατάλληλους μηχανσιμούς ελέγχου ταυτότητας και πλημμύρας για τον περιορισμό ανάπτυξης των κακόβουλων γείτονων κόμβων. Ένα δίκτυο επικάλυψης είναι κατασκευασμένο να χρησιμοποιεί τιμές αξιοπιστίας για ασφαλής δρομολογήσεις πολλαπλών διαδρομών. Οι ασφαλής διαδρομές επιλέγονται από τους ομαδάρχες και τον σταθμό βάσης. Αν και το πρωτόκολλο είναι ανθεκτικό απέναντι σε επιθέσεις σκουληκότρυπας και καταβόθρας, δεν παρέχει καμία άμυνα απέναντι σε εσωτερικές επιθέσεις.

Στο [1] προτείνεται ο αλγόριθμος δρομολόγησης εξοικονόμησης ενέργειας αξιόπιστων πολλαπλών διαδρομών ECTMRA (Energy Conserving Trustworthy Multipath Routing Algorithm). Συνδυάζει ομαδοποίηση κόμβων, αξιοπιστία και δρομολόγηση πολλαπλών διαδρομών για να παρατείνει τη διάρκεια ζωής του

δικτύου. Οι ομαδάρχες είναι υπέυθυνοι για τον υπολογισμό των τιμών αξιοπιστίας των κόμβων που ανήκουν στην ομάδα τους ενώ ο βαθμός αξιοπιστίας των ομαδαρχών υπολογίζεται απο τον σταθμό βάσης ή απο γείτονες ομαδάρχες άλλης ομάδας κόμβων. Ο υπολογισμός του βαθμού αξιοπιστίας βασίζεται σε παραμέτρους όπως είναι ο ρυθμός προώθησης των δεδομένων, η συνοχή του πακέτου και η εφεδρική πηγή ενέργειας. Ο αλγόριθμος δρομολόγησης εξετάζει μόνο διαδρομές που ικανοποιούν ένα αναμενόμενο σκορ αξιοπιστίας.

Πρόσφατα προτάθηκε από τους ερευνητές το πρωτόκολλο δρομολόγσης που βασίζεται στην αξιοπιστία έχοντας πολλαπλά γνωρίσματα TRPM (Trust-aware Routing Protocol with Multiattributes). Το μοντέλο διαχείρισης αξιοπιστίας του TRPM ενσωματώνει την επικοινωνία, τα δεδομένα, την ενέργεια και τα προτεινόμενα χαρακτηριστικά αξιολόγησης της αξιοπιστίας μαζί με μια συνάρτηση χαρακτηριστικών που αφορά τη συχνότητα εκδήλωσης μιας επίθεσης. Το TRPM έχει καλή απόδοση απέναντι σε επιθέσεις που στοχεύουν στη δρομολόγηση και στην αζιοπιστία του δικτύου. Επίσης δεν ενσωματώνει κάποιο σχήμα εκλογής ενός αξιόπιστου ομαδάρχη.

Πίνακας 5.2: Αξιόπιστα πρωτόκολλα δρομολόγησης που βασίζονται σε ομάδες

Πρωτόκολλο	Μεθοδολογία	Τιμές αξιοπιστίας	Πλεονεκτήματα	Περιορισμοί	Επιθέσεις
TLEACH	Το τμήμα διαχείρισης αξιοπιστίας διατηρεί πληροφορίες αξιοπιστίας μεταξύ των κόμβων	Συνδυασμός άμεσων / έμμεσων τιμών αξιοπιστίας	Ισχυρό έναντι κακόβουλων κόμβων.	Ευπάθεια σε σκευωρία κόμβων	Μαύρης τρύπας, αλλοίωσης
RATCT	Δημιουργείται ένα αξιόπιστο δέντρο και το μοντέλο αξιοπιστίας χρησιμοποιεί τη δομή του δέντρου για την ανίχνευση κακόβουλης συμπεριφοράς	Η αξιολόγηση του επιπέδου αξιοπιστίας βασίζεται στην ανάλυση των κρυπτογραφημένων και με ψηφιακή υπογραφή πακέτων	Ανιχνεύει αποτελεσματικά κακόβουλη συμπεριφορά.	Επιπλέον κατανάλωση ενέργειας για τη δημιουργία του δένδρου πηρύνα	Μαύρης τρύπας, αλλοίωσης
TEESR	Ασφαλής δρομολόγηση πολλαπλών διαδρομών που βασίζεται στην αξιοπιστία των κόμβων.	Ο υπολογισμός τους εξελίσσεται στον σταθμό βάσης	Ανθεκτικό απέναντι στις επιθέσεις καταβόθρας και σκλουληκότρυπας	Κανένας αμυντικός μηχανισμός απέναντι στις εσωτερικές επιθέσεις.	Καταβόθρας, σιβυλλικής, επιλεκτικής προώθησης
ECTMRA	Η προσέγγιση της ομαδοποίησης σε συνδυασμό με την αξιόπιστη και πολλαπλών διαδρομών δρομολόγηση εξετάζει μόνο αυτές τις διαδρομές που καλύπτουν το σκορ της αξιοπιστίας	Ο υπολογισμός βασίζεται στον ρυθμό προώθησης των δεδομένων, στη συνοχή του πακέτου και στην εφεδρική πηγή ενέργειας	Αποτελεσματικότητα απέναντι στις περισσότερες επιθέσεις. Αποτρέπει επιθέσεις διαχείρισης των τιμών αξιοπιστίας.	Ποιότητα στη διαδικασία δρομολόγησης που παρατείνει τη διάρκεια ζωής του δικτύου και μειώνει τις καθυστερήαεις end-to-end.	Μαύρης τρύπας, αλλοίωσης
TRPM	Δημιουργία πραγματικών δρομολογήσεων που βασίζονται στην επικοινωνία, την ενέργεια,τα δεδομένα και τα προτεινόμενα χαρακτηριστικά αξιολόγησης σύστασης αξιοπιστίας	Το μοντέλο αξιοπιστίας ενσωματώνει την επικοινωνία, τα δεδομένα, την ενέργεια, τα χαρακτηριστικά σύστασης αξιολόγησης	Καλή απόδοση στην αντιμετώπιση διάφορων επιθέσεων δρομολόγησης και αμφισβήτησης αξιοπιστίας.	Δεν ενσωματώνει κάποιο σχήμα εκλογής ενός αξιόπιστου ομαδάρχη	Μαύρης τρύπας, αλλοίωσης, καταβόθρας, καταβόθρας, σιβυλλικής, σκευωρίας

5.4 Ασφαλή πρωτόκολλα δρομολόγησης (secure routing protocols)

Πέραν των σχημάτων/μοντέλων δρομολόγησης πολλαπλών διαδρομών και αυτών που βασίζονται σε τιμές αξιπιστίας, αναφέρονται στη βιβλιογραφία και κάποια πρωτόκολλα δρομολόγησης που στοχεύουν αποκλειστικά και μόνο στην ασφαλή λειτουργία του δικτύου εξασφαλίζοντας την ακεραιότητα, την αυθεντικότητα και την διαθεσιμότητα των μηνυμάτων που ανταλλάσονται, αντιμετωπίζοντας τις διάφορες μορφές επίθεσης [25]. Κάποια από τα ασφαλή πρωτόκολλα δρομολόγησης που θα παρουσιασθούν παρακάτω είναι το SPINS, το SIGF, το DAWWSEN, το AODV, το OLSR, το DSR, το SEEM, το MPH, το ZTR και το LEAP.

5.4.1 SPINS (Security Protocols for Sensor Networks)

Το πρωτόκολλο SPINS (Security Protocols for Sensor Networks) είναι ένα προληπτικό πρωτόκολλο ασφαλούς δρομολόγησης, η λειτουργία του οποίου βασίζεται σε δύο δομές: το πρωτόκολλο SNEP (Sensor Network Encryption Protocol) και το πρωτόκολλο μTESLA (micro version of Timed, Efficient, Streaming, Loss – tolerant Authentication Protocol) [57]. Το SNEP παρέχει στην ανταλλαγή μηνυμάτων μεταξύ των αισθητήριων κόμβων εμπιστευτικότητα, ακεραιότητα, αυθεντικοποίηση δύο μερών (two-party data authentication) και φρεσκάδα δεδομένων. Από την άλλη μεριά το μTesla παρέχει αυθεντικοποίηση ευρυεκπομπής (broadcast authentication). Ένα σύνηθες πρόβλημα στα ασύρματα δίκτυα αισθητήρων είναι η παροχή αποτελεσματικού ελέγχου ταυτότητας στα πακέτα μετάδοσης λόγω των απαιτήσεων που υπάρχουν σε πόρους. Το μTESLA είναι ικανό να παρέχει αποτελεσματικό έλεγχο ταυτότητας και ταυτόχρονα να εξοικονομεί πόρους του δικτύου γεγονός που το καθιστά χρήσιμο ακόμη και σε περιβάλλοντα με περιορισμένους πόρους. Το πρωτόκολλο SPINS είναι αποτελεσματικό ως πρωτόκολλο πρόληψης των επιθέσεων, όχι όμως και το καταλληλότερο για την αντιμετώπιση τους.

5.4.2 SIGF (Secure Implicit Geographic Forwarding)

Το ασφαλές πρωτόκολλο IGF ή αλλιώς το πρωτόκολλο SIGF (Secure Implicit Geographic Forwarding) ανήκει στην οικογένεια των πρωτοκόλλων ασφαλούς δρομολόγησης [55]. Πρόκειται για ένα προληπτικό πρωτόκολλο δρομολόγησης που βασίζεται στη θέση των αισθητήριων κόμβων που συμμετέχουν στη δρομολόγηση. Κάθε φορά που πρέπει να σταλεί ένα μήνυμα από τον κόμβο προέλευσης στον κόμβο προορισμού, το SIGF επιλέγει δυναμικά το επόμενο άλμα και ύστερα απο πολλαπλά άλματα φθάνει το πακέτο στον προορισμό του. Το συγκεκριμένο πρωτόκολλο με χρήση μεθόδων και αλγορίθμων αυθεντικοποίησης και κρυπτογράφησης, παρέχει προστασία από επιθέσεις σκουληκότρυπας, HELLO ροών, μαύρης τρύπας, ψευδών μηνυμάτων, σιβυλλικής μορφής. Απαρτίζεται απο τρία πρωτόκολλα (SIGF-0, SIGF-1, SIGF-2) τα οποία συνεργατικά παρέχουν στο πρωτόκολλο την ιδιότητα της πρόληψης. Το SIGF-0 είναι ένα ακαταστατικό (stateless) πρωτόκολλο που δεν διατηρεί πληροφορίες δρομολόγησης, αλλά παρέχει μόνο τους πιθανούς τρόπους άμυνας κατά της επίθεσης. Το SIGF-1 είναι ένα καταστατικό πρωτόκολλο (stateful) διατηρώντας συγκεκριμένες πληροφορίες που αντλήθηκαν από ανταλλαγές μηνυμάτων με τους γείτονες κόμβους. Το SIGF-2 χρησιμοποιεί κλειδιά και αριθμούς ακολουθίας που ανταλλάσονται μεταξύ των κόμβων για την εξασφάλιση της κρυπτογραφικής ακολουθίας κατά τη δρομολόγηση. Κάθε πρωτόκολλο είναι ένα υποσύνολο του επόμενου, χρησιμοποιώντας το ένα τους μηχανισμούς του άλλου προκειμένου να λειτουργήσει σαν ένα ενιαίο και αυτόνομο SIGF πρωτόκολλο παρέχοντας αυξημένη ασφάλεια στη δρομολόγηση και υψηλή απόδοση για το ευρύτερο δίκτυο.

5.4.3 DAWWSEN (Defense Mechanism Against Wormhole attacks in Wireless Sensor Networks)

Προκειμένου να καταπολεμήσουμε την επίθεση σκουληκότρυπας χρησιμοποιούμε το πρωτόκολλο δρομολόγησης DAWWSEN (Defense Mechanism Against Wormhole attacks in Wireless Sensor Networks) [54].

Πρόκειται για ένα προληπτικό πρωτόκολλο δρομολόγησης, το οποίο βασίζεται στην ιεραρχική δρομολόγηση όπου ο σταθμός βάσης είναι η ρίζα του δέντρου και οι υπόλοιποι αισθητήριοι κόμβοι τα φυλλώματα του δέντρου. Η κατασκευή του δέντρου ξεκινά από τον σταθμό βάσης που εκπέμπει μια ερώτηση προκειμένου να ανακαλύψει τους κόμβους παιδιά του. Το εν λόγω πρωτόκολλο προσδίδει επιπλέον δυνατότητα ανίχνευσης της συγκεκριμένης επίθεσης. Τα βασικά πλεονεκτήματα του πρωτοκόλλου που συμβάλλουν στην εξασφάλιση ενεργειακών αποθεμάτων στους κόμβους είναι:

- Η μη αναγκαιότητα διάθεσης πληροφορίας θέσης από τους κόμβους
- Η απλότητα στη μέθοδο ανίχνευσης της επίθεσης, τα οποία κρίνονται σημαντικά σε ένα δίκτυο WSN, όπου οι περιορισμοί σε πόρους είναι υπαρκτοί.

5.4.4 AODV (Ad hoc On-Demand Distance Vector)

Το πρωτόκολλο δρομολόγησης AODV (Ad hoc On-Demand Distance Vector) βασίζεται στη λειτουργία του σε κινούμενους/στατικούς αισθητήριους κόμβους με στόχο την έγκαιρη αναγνώριση των διαδρομών και τον επαναϋπολογισμό μιας νέας [50],[52],[53]. Ελαχιστοποιεί το πακέτο εκπομπής δημιουργώντας διαδρομή μόνο όταν απαιτείται. Κάθε κόμβος στο δίκτυο πρέπει να διατηρεί τον πίνακα πληροφοριών διαδρομής και να συμμετέχει στην ανταλλαγή πινάκων δρομολόγησης. Όταν ο κόμβος προέλευσης θέλει να στείλει δεδομένα στον κόμβο προορισμού, ξεκινά πρώτα τη διαδικασία εύρεσης διαδρομής. Σε αυτήν τη διαδικασία, ο κόμβος προέλευσης εκπέμπει ένα πακέτο αιτήματος διαδρομής (RREQ) στους γείτονές του. Οι γειτονικοί κόμβοι που λαμβάνουν αυτό το αίτημα, το προωθούν αντιστοίχως στους γείτονές τους και ούτω καθεξής. Αυτή η διαδικασία συνεχίζεται μέχρις ότου το RREQ να φθάσει στον προορισμό του ή στον κόμβο που γνωρίζει τη διαδρομή μέχρι τον παραλήπτη. Οι ενδιάμεσοι κόμβοι που λαμβάνουν το RREQ καταγράφουν στους πίνακές τους τη διεύθυνση των

γειτόνων, δημιουργώντας έτσι την αντίστροφη σε κατεύθυνση διαδρομή. Όταν ο κόμβος που γνωρίζει τη διαδρομή προορισμού ή ο ίδιος ο κόμβος προορισμού, λάβουν το RREQ, θα απαντήσουν στέλνοντας ένα πακέτο απάντησης διαδρομής (RREP) στον κόμβο προέλευσης. Το πακέτο RREP θα μεταδοθεί μέσω της αντίστροφης διαδρομής που βρίσκεται στον πίνακα δρομολόγησης κάθε ενδιάμεσου κόμβου. Μόλις λάβει το RREP ο αρχικός κόμβος που έστειλε το RREQ, τότε θα είναι σ θέση να γνωρίζει την ακριβής διαδρομή μέχρι τον κόμβο προορισμού, αποθηκεύοντας στον πίνακα δρομολόγησης τις πληροφορίες των διαδρομών που ανακαλύφθησαν. Αυτό είναι και το τέλος της διαδικασίας εύρεσης διαδρομής. Στη συνέχεια το πρωτόκολλο επιτελεί μια διαδικασία συντήρησης των διαδρομών κατα την οποία κάθε κόμβος περιοδικά εκπέμπει HELLO μήνυμα για τον έλεγχο τυχόν προβληματικής διαδρομής. Η δομή του αλγορίθμου AODV συνίσταται από χαρακτηριστικά όπως αυτόνομη, δυναμική, πολλαπλών αλμάτων δρομολόγηση μεταξύ των κόμβων για τη δημιουργία και συντήρηση της διαδρομής σ' ένα αυτοοργανωμένο (ad-hoc) δίκτυο. Το συγκεκριμένο πρωτόκολλο μπορεί να αντιμετώπισει σε σύντομο χρονικό διάστημα διάφορα ζητήματα που απορούν σε διακοπές στη δρομολόγηση και σε γενικότερες διακυμάνσεις στην τοπολογία δικτύου. Επίσης αποτρέπει τη δημιουργία βρόχων ενώ παράλληλα αποκλείει το πρόβλημα Bellman-Ford (μέτρηση στο άπειρο) προκειμένου να παρέχει ταχύτατο ρυθμό σύγκλισης σε ενδεχόμενο ύπαρξης αλλαγών σε ένα Ad-Hoc δίκτυο. Οι προκλήσεις που προκύπτουν κατα την ανάπτυξη ασύρματων δικτύων Ad-Hoc αφορούν α) στη διαχείριση ενέργειας, β) στην εξασφάλιση ποιότητας υπηρεσιών (QoS) και γ) στο πρωτόκολλο MAC. Το πρωτόκολλο AODV είναι ικανό να δημιουργήσει με υπευθυνότητα κατ' απαίτηση προσεγγίσεις με βάση τις συνθήκες και τις προύποθέσεις επικοινωνίας που να ανταποκρίνονται στις παραπάνω προκλήσεις.

5.4.5 OLSR (Optimized Link State Routing)

Το πρωτόκολλο βελτιστοποιημένης διαδρομής κατάστασης συνδέσμου OLSR (Optimized Link State Routing) είναι ένα πρωτόκολλο δρομολόγησης που παρέχει το πλεονέκτημα να υπάρχουν άμεσα διαθέσιμες διαδρομές για κάθε κόμβο σε όλους τους προορισμούς του δικτύου [52]. Πρόκειται για μια βελτιωμένη διαδικασία βελτιστοποίησης του κλασσικού αλγορίθμου κατάστασης σύνδεσης. Η βελτιστοποίηση βασίζεται στην έννοια των πολλαπλών ρελέ MPRs (MultiPoint Relays). Αρχικά η χρήση πολλαπλών ρελέ μειώνει το μέγεθος του μηνύματος ελέγχου: αντί να δηλώνει όλους τους συνδέσμους, κάθε κόμβος δηλώνει μόνο εκείνους τους συνδέσμους με τους γείτονες που αποτελούν τα πολλαπλά σημεία ρελέ. Η χρήση MPRs ελαχιστοποιεί επίσης την πλημμύρα στη κυκλοφορία ελέγχου και πράγματι μόνο τα πολλαπλά ρελέ προωθούν μηνύματα ελέγχου. Αυτή η τεχνική μειώνει σημαντικά τον αριθμό στις αναμεταδόσεις των μηνυμάτων ελέγχου εκπομπής. Το OLSR απαρτίζεται από δύο τύπους μηνυμάτων ελέγχου: μηνύματα γειτνίασης (HELLO μηνύματα) και μηνύματα τοπολογίας (μηνύματα ελέγχου τοπολογίας TC). Πιο αναλυτικά ο μεμονωμένος κόμβος αναγνωρίζει κάθε νέα ζεύξη στους γειτονικούς κόμβους και περιστασιακά πλημμυρίζει το δίκτυο με ένα μήνυμα που περιέχει όλες τις συνδέσεις συνδέσμου όπως είναι για παράδειγμα το μήνυμα κατάστασης σύνδεσης. Επιπλέον κάθε μεμονωμένος κόμβος αναπτύσει έναν χάρτη τοπολογίας για το δίκτυο και εντοπίζει μέσω του αλγορίθμου βραχύτερης διαδρομής την βέλτιστη διαδρομή μέχρι τον προορισμό. Εν συντομία λοιπόν, στο OLSR συναντάμε δύο κύριες λειτουργίες: τον εντοπισμό του γείτονα κόμβου και την διάδοση της τοπολογίας δικτύου.

5.4.6 DSR (Dynamic Source Routing)

Το πρωτόκολλο πηγαίας δυναμικής δρομολόγησης DSR (Dynamic Source Routing) είναι ένα πρωτόκολλο αντίδρασης που δρομολογεί βάσει του κόμβου προέλευσης συμπεριλαμβανομένου και μιάς κεφαλίδας στα πακέτα [50],[53]. Αυτή η κεφαλίδα υποδεικνύει στον κόμβο προέλευσης με ποιούς άλλους κόμβους θα

διασταυρωθεί προκειμένου να “χτίσει” την διαδρομή που θα διανύσει μέχρι τον κόμβο προορισμού. Αυτή η διαδικασία ονομάζεται πηγαία δρομολόγηση αφού ο κόμβος προέλευσης είναι ο υπεύθυνος για τον υπολογισμό της πλήρους διαδρομής. Το DSR δεν απαιτεί την ανταλλαγή περιοδικών μηνυμάτων μειώνοντας κατ’ αυτό τον τρόπο την υπερφόρτωση στο δίκτυο. Κάθε φορά που αλλάζει η τοπολογία στο δίκτυο ή ο κόμβος προέλευσης μετακινηθεί, ο αλγόριθμος προσαρμόζεται ανάλογα. Το πρωτόκολλο διαχειρίζεται μονοκατευθυντήριους συνδέσμους και ασύμμετρες διαδρομές. Κάθε κόμβος στο δίκτυο διαθέτει προσωρινή μνήμη για να αποθηκεύει όλες τις διαδρομές που μαθαίνει μέσω της διαδικασίας εύρεσης διαδρομών και αυτό ενδέχεται να αυξήσει την επεξεργαστική ισχύ για τον ίδιο τον κόμβο. Εάν δεν βρίσκεται στη προσωρινή μνήμη κάποιο μονοπάτι για τον εκάστοτε κόμβο προορισμού τότε ο κόμβος ξεκινά την αντιδραστική εύρεση διαδρομής όπως ακριβώς και στο πρωτόκολλο AODV. Ο πίνακας δρομολόγησης και η προσωρινή μνήμη κάθε κόμβου ελέγχονται συνεχώς από το πρωτόκολλο έτσι ώστε εάν βρεθούν μη έγκυρες διαδρομές να ενημερώνονται με νέες όσο η τοπολογία δικτύου μεταβάλλεται. Αυτή η διαδικασία ονομάζεται συντήρηση διαδρομής. Το DSR διαθέτει τα εξής πλεονεκτήματα:

- Στη προσωρινή μνήμη των κόμβων περιλαμβάνονται περισσότερες της μιας διαδρομές μέχρι τον κόμβο προορισμού ωστόσο μόνο μία μπορούν να ζητήσουν από τους γείτονές τους
- Επιτρέπεται στο δίκτυο να είναι πλήρως αυτορυθμιζόμενο χωρίς κάποια συγκεκριμένη αρχιτεκτονική ή τοπολογία
- Κατάλληλο για δίκτυα στα οποία ο αριθμός των κινούμενων κόμβων συνεχώς μειώνεται
- Προσαρμόζεται γρήγορα στις αλλαγές που προκύπτουν στη δρομολόγηση από τη συνεχή κίνηση των κόμβων, μειώνοντας έτσι την υπερφόρτωση δικτύου.

5.4.7 MPH (Multi-Parent Hierarchical)

Το MPH (Multi-Parent Hierarchical) αποτελεί ένα υβριδικό (πρόληψης και αντίδρασης) πρωτόκολλο δρομολόγησης που δημιουργεί μια ιεραρχική λογική τοπολογία δικτύου στην οποία η ιεραρχία στους κόμβους δίνεται από την εκάστοτε θέση τους στο ιεραρχικό δέντρο [62]. Ο sink κόμβος έχει την υψηλότερη θέση στην ιεραρχία. Αυτή η ιεραρχική δομή στη τοπολογία ελαχιστοποιεί τον αριθμό των αλμάτων ενισχύοντας παράλληλα τις διαδρομές προς τον κόμβο συντονισμού. Το βασικό πλεονέκτημα του πρωτοκόλλου είναι ότι συνδυάζει χαρακτηριστικά τόσο προληπτικού όσο και αντιδραστικού μηχανισμού και παρουσιάζει πλεονασμό στο δίκτυο χωρίς απώλεια στην απλότητα προγραμματισμού του αλγορίθμου. Το MPH εκμεταλλεύεται την προληπτικά ελεγχόμενη διαδρομή συντήρησης, έχει την ικανότητα να προσαρμόζεται σε διάφορες τοπολογίες ενώ παράλληλα συνδυάζει την ευελιξία που παρέχει με τις περισσότερες από μία διαδρομές μέχρι τον κόμβο προορισμού.

5.4.8 ZTR (ZigBee Tree Routing)

Το ZTR (ZigBee Tree Routing) είναι ένα απλό πρωτόκολλο δρομολόγησης που δημιουργεί συνδέσμους γονέα-παιδιού με τους κόμβους που μεταφέρουν πληροφορία στους κόμβους-γονείς τους [53]. Πρόκειται για ένα πρωτόκολλο που διαθέτει τοπολογία δέντρου, εύκολο στην εφαρμογή, γρήγορο στη λειτουργία με βασική δομή πρόληψης. Τα δίκτυα ZigBee προύποθέτουν την ύπαρξη μιας τουλάχιστον ισχυρής συσκευής με καθήκοντα συντονιστή δικτύου με τους υπόλοιπους κόμβους να χρίζουν χαμηλών προδιαγραφών για μείωση του συνολικού κόστους υλοποίησης δικτύου. Μερικά από τα πλεονεκτήματα του ZTR είναι:

- Ισορροπία ανάμεσα στο κόστος ανα συσκευή
- Χαμηλή δαπάνη σε μπαταρίες

- Πολυπλοκότητα στην υλοποίηση της εφαρμογής για την επίτευξη κατάλληλης αναλογίας κόστους - απόδοσης

5.4.9 LEAP (Localized Encryption and Authentication Protocol)

Το πρωτόκολλο LEAP (Localized Encryption and Authentication Protocol) είναι πολύ δημοφιλές στην ασφάλεια των ασύρματων δικτύων αισθητήρων και παρουσιάσθηκε από τον Zhu το 2004 [48] [64]. Το LEAP είναι ένα πρωτόκολλο διαχείρισης κρυπτογραφικών κλειδιών παρέχοντας ασφάλεια και υποστήριξη στα ασύρματα δίκτυα αισθητήρων. Χρησιμοποιεί το πρωτόκολλο μTESLA για να παρέχει μέσω του σταθμού βάσης έλεγχο ταυτότητας για όλους τους κόμβους του δικτύου. Το LEAP βασίζεται στην ιδέα ότι κάθε μεταδιδόμενη μεταξύ αισθητήριων κόμβων πληροφορία, είναι διαφορετική από τις υπόλοιπες και χρήζει διαφορετικής αντιμετώπισης εφαρμοζόμενης ασφάλειας. Γ' αυτόν τον λόγο χρησιμοποιεί τέσσερις τύπους κλειδιών σε κάθε κόμβο μεμονωμένα. Οι τύποι αυτοί είναι:

α) *ένα ατομικό κλειδί (individual key)* για την επικοινωνία μεταξύ κόμβου και σταθμού βάσης προκειμένου να εξασφαλισθεί η ασφάλεια στη μεταξύ τους επικοιωνία

β) *ένα ομαδικό κλειδί (group key)* δημόσιο κλειδί που το γνωρίζουν όλοι οι κόμβοι του δικτύου και αυτό που χρησιμοποιεί ο σταθμός βάσης για την κρυπτογράφηση των μηνυμάτων που θα σταλούν στους κόμβους εντός ιδίου γκρουπ

γ) *κλειδιά ζεύξης (pair-wise keys)* για την ασφαλή επικοινωνία μεταξύ γειτονικών κόμβων

δ) *ένα κλειδί συστάδας (cluster key)* για την ασφαλή επικοινωνία με τον κόμβο αρχηγό της συστάδας

Το βασικό πλεονέκτημα απ' την χρήση του LEAP είναι ότι μειώνει τη συμμετοχή του σταθμού βάσης στη διαχείριση των κρυπτογραφικών κλειδιών και συνδράμει αποτελεσμτικά στην επικοινωνία και στη κατανάλωση ενέργειας.

Επίσης παρέχει ασφάλεια σ ένα τοπικό δίκτυο όπως οι πληροφορίες που πηγάζουν από τους πίνακες δρομολόγησης και τα μηνύματα που ανταλλάσονται μεταξύ των κόμβων αντιμετωπίζοντας επιθέσεις όπως είναι οι Hello ροές, σκουληκότρυπας και σιβυλλικής μορφής. Ωστόσο το βασικό μειονέκτημα είναι ότι τίθεται ζήτημα περιορισμού μνήμης από την αποθήκευση των τεσσάρων τύπων κλειδιών στους κόμβους. Στον πίνακα 5.3 παρουσιάζονται συνοπτικά όλα τα πρωτόκολλα δρομολόγησης που αναλύθηκαν στον παρόν κεφάλαιο καθώς επίσης και η δράση τους στην εξασφάλιση του μοντέλου CIA και της αυθεντικοποίησης ανάλογα με τον αλγόριθμο κρυπτογράφησης που διαθέτουν, τις επιθέσεις που καταπολεμούν, τον ρόλο που επιτελούν έναντι αυτών των επιθέσεων, τα επίπεδα ενέργειας που καταναλίσκουν καθώς επίσης και την δομή των κόμβων τους εντός του δικτύου και τον μηχανισμό διαχείρισης κλειδιών.

Πίνακας 5.3: Συγκριτικός πίνακας πρωτοκόλλων ασφαλούς δρομολόγησης

Πρωτόκολλλο	Βασικές απαιτήσεις ασφάλειας				Επιθέσεις								Ρόλος έναντι επιθέσεων			Εξοικονόμηση ενέργειας	Δομή στο δίκτυο			Πρωτόκολλο διαχείρισης κλειδιών
	Εμπιστευτικότητα	Ακεραιότητα	Διαθεσιμότητα	Αυθεντικοποίηση	Επιλεκτική προώθηση	Σκουληκότρυπαα	Καταβόθρα	Κρυφάκουσμα	Σιβυλλική	Hello ροές	Αναπαραγωγή κόμβου	Αλλοίωση & Υποκλοπή	Πρόληψη	Δραστικό	Υβριδικό		Ιεραρχική	Επίπεδη	Γεωγραφικής θέσης	
SPINS																				
SIGF																				
INSENS																				
DAWWSEN																				
AODV																				
OLSR																				
DSR																				
SEEM																				
ATSR																				
MPH																				
ZTR																				
LEAP																				

Με πράσινο χρώμα φαίνονται οι στήλες που αντιστοιχίζονται στα χαρακτηριστικά του εκάστοτε πρωτοκόλλου
Με κόκκινο χρώμα δεν αντιστοιχίζονται οι στήλες με τα πρωτόκολλα

5.5 Σύνοψη

Τα ασύρματα δίκτυα αισθητήρων εφαρμόζονται ολοένα και περισσότερο σε διαφορετικά πεδία εφαρμογών. Ανάλογα με τα πεδία εφαρμογής τους θα πρέπει να επιτυγχάνεται και ο αντίστοιχος βαθμός ασφάλειας. Για να εξασφαλιστεί η αδιάλειπτη λειτουργία του δικτύου καθώς επίσης η εμπιστευτικότητα, αυθεντικότητα και ακεραιότητα της πληροφορίας θα πρέπει να χρησιμοποιηθεί κάποιο ασφαλές πρωτόκολλο δρομολόγησης. Στο παρόν κεφάλαιο παρουσιάσθηκαν τα ασφαλή και βασιζόμενα στην αξιοπιστία πρωτόκολλα δρομολόγησης όπως επίσης και η κατηγοριοποίησή τους με βάσει τα κύρια χαρακτηριστικά τους. Επίσης αναλύθηκαν τα ασφαλή πρωτόκολλα πολλαπλών διαδρομών. Ωστόσο οι περιορισμοί των ασύρματων δικτύων αισθητήρων στη κατανομή των πόρων, οδήγησαν την τελευταία δεκαετία στην εξέλιξη πρωτοκόλλων που βασίζονται στην αξιοπιστία. Επιπλέον τα τελευταία πέντε χρόνια οι ερευνητές εργάζονται σε συγκεκριμένες καυτευθύνσεις με σκοπό τη βελτίωση: α) στα αξιόπιστα πρωτόκολλα δρομολόγησης που να μπορούν αποτελεσματικά να ενσωματώνουν τη δομή των WSNs που βασίζονται σε ομάδες και β) στο κατάλληλο και αποτελεσματικό συνδυασμό των διαφόρων σχημάτων (τιμές αξιοπιστίας σε συνδυασμό με πολλαπλές διαδρομές). Η επιλογή του κατάλληλου ασφαλούς πρωτοκόλλου δρομολόγησης ποικίλει κάθε φορά και εξαρτάται από παράγοντες όπως είναι η δομή του δικτύου, το πεδίο εφαρμογής, ο αριθμός των κόμβων, το είδος της επίθεσης, η κατανάλωση ενέργειας, οι περιορισμοί πόρων, η πληροφορία που διακινείται, ο επιθυμητός αλγόριθμος κρυπτογράφησης, οι μηχανισμοί διαχείρισης κλειδιών και ο ρόλος που θα έχει (πρόληψη-αντίδραση) απέναντι σε κάθε είδους επίθεση. Η ασφάλεια στα αναπτυσσόμενα ασύρματα δίκτυα αισθητήρων αποτελεί μια πράξη εξισορρόπησης που θα αναζητά συνεχώς το υψηλότερο επίπεδο προστασίας.

ΚΕΦΑΛΑΙΟ 6

Βιβλιογραφία

[1] C. Konstantopoulos, B. Mamalis, and G. Pantziou, “Secure and Trust-Aware Routing in Wireless Sensor Networks”, 2018, https://doi.org/10.1145/3291533.3291544

[2] Sahabul Alam, Debashis De, “ANALYSIS OF SECURITY THREATS IN WIRELESS SENSOR NETWORK, International Journal of Wireless & Mobile Networks (IJWMN) Vol. 6, No. 2, April 2014

[3] Jasmin Ilyani Ahmad, Roshidi Din, Mazida Ahmad, “Analysis Review on Public Key Cryptography Algorithms”, Indonesian Journal of Electrical Engineering and Computer ScienceVol. 12, No. 2, November 2018, pp. 447~454, ISSN: 2502-4752, DOI: 10.11591/ijeecs.v12.i2.pp447-454

[4] Waleed .K, Shaimaa .H, “Methods of Secure Routing Protocol in Wireless Sensor Networks”, Journal of AL-Qadisiyah for computer science and mathematics, Vol.10, No.3, Year 2018, ISSN (Print): 2074 – 0204, ISSN (Online): 2521 – 3504, Comp Page 38 – 55

[5] Tao Yang, Leonard Barolli, Makoto Ikeda, Fatos Xhafa, Arjan Durresi, “Performance Analysis of OLSR Protocol forWireless Sensor Networks and Comparison Evaluation with AODV Protocol, 2009 International Conference on Network-Based Information Systems

[6] Rouba El Kaissi, Ayman Kayssi, Ali Chehab and Zaher Dawy, “DAWWSEN: A DEFENSE MECHANISM AGAINST WORMHOLE ATTACKS IN

WIRELESS SENSOR NETWORKS", The Second International Conference on Innovations in Information Technology (IIT'05)

[7] Jaydip Sen, "Security in Wireless Sensor Networks", Department of Computer Science & Engineering, National Institute of Science & Technology, INDIA

[8] Riaz A. Shaikh, Young Jae Song, Sungyoung Lee, "Securing Distributed Wireless sensor Networks: Issues and Guidelines", February 2006, DOI: 10.1109/SUTC.2006.120 Source IEEEXplore Conference: Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference on Volume: 2

[9] Edited By Biju Issac, Nauman Israr, "Case St,udies in Secure Computing, Achievements and Trends", ISBN 9781138034136

[10] Shayan Zamani & Mojtaba Jafari, Mazanadaran University of Science and Technology, Distributed Systems Class Seminar, Supervisor: Hadi Salimi, "Security Issues in Wireless Sensor Networks (WSNs)", https://slideplayer.com/slide/1505722/

[11] Opeyemi Osanaiye, Attahiru S. Alfa, Gerhard P. "Hancke, Denial of Service (DoS) Defence for Resource Availability in Wireless Sensor Networks", January 2018 IEEE Access PP(99):1-1

[12] Majid Meghdadi, Suat Ozdemir and Inan Güler, "A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks", March 2011 IETE Technical Review 28(2):89

[13] Harsh Kishore Mishra, "WORMHOLE ATTACK", slide presentation, https://www.slideshare.net/HarshMishra3/wormhole-attack

[14] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", PowerPoint PPT Presentation,

https://www.slideserve.com/abdul-conrad/secure-routing-in-wireless-sensor-networks-attacks-and-countermeasures-chris-karlof-david-wagner

[15] Mohammad Abdus Salam and Nayana Halemani, "PERFORMANCE EVALUATION OF WIRELESS SENSOR NETWORK UNDER HELLO FLOOD ATTACK", https://ijcnc.com/8216cnc07-pdf/

[16]https://www.youtube.com/watch?v=ROltFe0HXBw&ab_channel=KarinaHleuka, HELLO FLOOD ATTACK

[17]https://www.youtube.com/watch?v=hZbtQtIxDM&ab_channel=anastasiaveloni, ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΑΙΣΘΗΤΗΡΩΝ ΔΡ. ΔΙΟΝ. ΚΑΝΔΡΗΣ

[18] Rastko R. Selmic, Abdul Serwadda , Vir V. Phoha ,"Wireless Sensor Networks, Security, Coverage, and Localization", Springer, ISBN 978-3-319-46769-6 (eBook), DOI 10.1007/978-3-319-46769-6

[19] Boyuan Sun, "A Comprehensive Trust-Aware Routing Protocol With Multi-Attributes for WSNs" December 2017, Digital Object Identifier 10.1109/ACCESS.2017.2786944

[20] Waltenegus Dargie, Christian Poellabauer, "FUNDAMENTALS OF WIRELESS SENSOR NETWORKS, THEORY AND PRACTICE", This edition first published 2010 by John Wiley & Sons Ltd., ISBN 978-0-470-99765-9 (H/B)

[21] ΒΟΥΡΟΣ ΑΝΔΡΕΑΣ, ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ "ΑΣΦΑΛΕΙΑ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ ΑΙΣΘΗΤΗΡΩΝ (WSN) ΣΕ ΕΦΑΡΜΟΓΕΣ ΕΠΙΤΗΡΗΣΗΣ ΚΑΙ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ ΠΕΡΙΟΧΗΣ", Μάρτιος 2015

[22] S.Prasanna, Srinivasa Rao, "An Overview of Wireless Sensor Networks Applications and Security", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-2, Issue-2, May 2012

[23] Muhammad Noman Riaza, Attaullah Burirob, Athar Mahboobb, "Classification of Attacks on Wireless Sensor Networks: A Survey", Published

Online November 2018 in MECS (http://www.mecs-press.net), DOI: 10.5815/ijwmt.2018.06.02

[24] Chandrakant Mallick, Suneeta Satpathy, "Challenges and Design Goals of Wireless Sensor Networks: A Sate-of-the-art Review", International Journal of Computer Applications (0975 – 8887) Volume 179 – No.28, March 2018

[25] Jaydip Sen, "A Survey on Wireless Sensor Network Security", International Journal of Communication Networks and Information Security (IJCNIS) Vol. 1, No. 2, August 2009

[26] Eliana Stavrou, Andreas Pitsillides, "A survey on secure multipath routing protocols in WSNs", March 2010

[27] Gurmukh Singh, "Security Attacks and Defense Mechanisms in Wireless Sensor Network: A Survey", IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 4, April 2016, ISSN 2348 – 7968

[28] Ms. Sheffy Jindal, Mr. Pinaki Ghosh, "An Assessment on Attacks on Routing Protocols in Wireless Sensor Networks", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-018, Vol. 5 Issue 11, November-2016

[29] Nusrat Fatema, Remus Brad, "ATTACKS AND COUNTERATTACKS ON WIRELESS SENSOR NETWORKS", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.4, No.6, December 2013

[30] Suman Bala, "SECURE ROUTING IN WIRELESS SENSOR NETWORKS", COMPUTER SCIENCE AND ENGINEERING DEPARTMENT THAPAR UNIVERSITY PATIALA – 147004, MAY 2009

[31] Hector Kaschel, Jose Mardones, Gustavo GUEZADA, "Safety In Wireless Sensor Networks:Types of Attacks and Solutions", Studies in Informatics and Control, Vol.22, No.3, September 2013

[32] Mohammad A. Matin, "Wireless Sensor Networks – Technology and Protocols", ISBN 978-953-51-0735-4

[33] Wazir Zada Khan, Yang Xiang, Mohammed Y Aalsalem, "Comprehensive Study of Selective Forwarding Attack in Wireless Sensor Networks", I.J. Computer Network and Information Security, 2011, 1, 1-10, Published Online February 2011 in MECS (http://www.mecs-press.org/)

[34] Shio Kumar Singh, M P Singh, and D K Singh, "A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks", January 2011, ISSN: 2231-2803

[35] Virendra Pal Singh, Aishwarya S. Anand Ukey, Sweta Jain, "Signal Strength based Hello Flood Attack Detection and Prevention in Wireless Sensor Networks", International Journal of Computer Applications (0975 – 8887) Volume 62– No.15, January 2013

[36] Sahabul Alam, Debashis De, "ANALYSIS OF SECURITY THREATS IN WIRELESS SENSOR NETWORK", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 6, No. 2, April 2014

[37] Virendra Pal Singh, Sweta Jain, Jyoti Singhai, "Hello Flood Attack and its Countermeasures in Wireless Sensor Networks", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 11, May 2010, ISSN (Online): 1694-0784

[38] M. Premkumar, Dr. TVP. Sundararajan , Dr. K. Vinoth Kumar, "Various Defense Countermeasures against DoS Attacks in Wireless Sensor Networks", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 8, ISSUE 10, OCTOBER 2019, ISSN 2277-8616

[39] V. Manjula, C. Chellappan, "The Replication Attack in Wireless Sensor Networks: Analysis and Defenses", January 2011, DOI: 10.1007/978-3-642-17878-8_18

[40] V. E. Ekong1, U. O. Ekong, "A SURVEY OF SECURITY VULNERABILITIES IN WIRELESS SENSOR NETWORKS", Nigerian Journal of

Technology (NIJOTECH) Vol. 35, No. 2, April 2016, pp. 392 – 397, Electronic ISSN: 2467-8821

[41] Jing Deng, Richard Han, Shivakant Mishra, "Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks", October 2005, Source: IEEE Xplore, DOI: 10.1109/SECURECOMM.2005.16

[42] Deepali Virmani, Ankita Soni, Shringarica Chandel, Manas Hemrajani, "Routing Attacks in Wireless Sensor Networks: A Survey", May 2014, https://arxiv.org/abs/1407.3987

[43] Vikhyath K, Dr. Brahmanand S, "Wireless sensor networks security issues and challenges: A survey", International Journal of Engineering & Technology, 7 (2.33) (2018) 89-94

[44] Jaydip Sen, "Security in Wireless Sensor Networks", International Journal of Engineering & Technology, August 2017

[45] Jasmin Ilyani Ahmad, Roshidi Din, Mazida Ahmad, "Analysis Review on Public Key Cryptography Algorithms", Indonesian Journal of Electrical Engineering and Computer Science, Vol. 12, No. 2, November 2018, pp. 447~454, ISSN: 2502-4752, DOI: 10.11591/ijeecs.v12.i2.pp447-454

[46] Atsuko Miyaji, Kazumasa Omote, "Self-healing wireless sensor networks", April 2015 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/cpe.3434

[47] Osman Yagan, "Performance of the Eschenauer-Gligor key distribution scheme under an ON/OFF channel", IEEE Transactions on Information Theory, June 2012, DOI: 10.1109/TIT.2012.2189353

[48] Delan Alsoufi, Khaled Elleithy, Tariq Abuzaghleh, Ahmad Nassar, "SECURITY IN WIRELESS SENSOR NETWORKS –IMPROVING THE LEAP PROTOCOL", International Journal of Computer Science & Engineering Survey · July 2012, DOI: 10.5121/ijcses.2012.3301

[49] Jean-Charles Faugere, Rune Steinsmo Odegard, Ludovic Perret, and Danilo Gligoroski, “Analysis of the MQQ Public Key Cryptosystem”, December 2010, DOI: 10.1007/978-3-642-17619-7_13 · Source: DBLP

[50] Waleed Kh. Alzubaidi, Shaimaa H. Shaker, “Methods of Secure Routing Protocol in Wireless Sensor Networks”, Journal of AL-Qadisiyah for computer science and mathematics Vol.10 No.3 Year 2018, ISSN (Online): 2521 – 3504

[51] Ayan Kumar, Rituparna CHAKI, Kashi Nath, “SECURE ENERGY EFFICIENT ROUTING PROTOCOL FOR WIRELESS SENSOR NETWORK”, FOUNDATIONS OF COMPUTING AND DECISION SCIENCES Vol. 41 (2016), DOI: 10.1515/fcds-2016-0001, e-ISSN 2300-3405

[52] Tao Yang, Leonard Barolli, Makoto Ikeda, Fatos Xhafa, Arjan Durresi, “Performance Analysis of OLSR Protocol forWireless Sensor Networks and Comparison Evaluation with AODV Protocol”, 2009 International Conference on Network-Based Information Systems

[53] Carolina Del-Valle-Soto, Carlos Mex-Perera, Juan Arturo Nolazco-Flores, Ramiro Velázquez, Alberto Rossa-Sierra, “Wireless Sensor Network Energy Model and Its Use in the Optimization of Routing Protocols”, February 2020, doi:10.3390/en13030728

[54] Rouba El Kaissi, Ayman Kayssi, Ali Chehab and Zaher Dawy, “DAWWSEN: A DEFENSE MECHANISM AGAINST WORMHOLE ATTACKS IN WIRELESS SENSOR NETWORKS”, The Second International Conference on Innovations in Information Technology (IIT’05)

[55] Anthony D. Wood, Lei Fang, John A. Stankovic, Tian He, “SIGF: A Family of Configurable, Secure Routing Protocols for Wireless Sensor Networks”

[56] Shipra Suman, Shubhangi, “A Survey On Comparison Of Secure Routing Protocols in Wireless Sensor Networks”, International Journal of Wireless

Communications and Networking Technologies, Volume 5, No.3, April – May 2016, ISSN 2319 – 6629

[57] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar, “SPINS: Security Protocols for Sensor Networks”

[58] Harmanpreet Singh, Damanpreet Singh, “Taxonomy of Routing Protocols in Wireless Sensor Networks: A Survey”, May 2017, DOI: 10.1109/IC3I.2016.7918796

[59] Umashankar Ghugar, Jayaram Pradhan, “A Review on Wormhole Attacks in Wireless Sensor Networks”, International Journal of Information Communication Technology and Digital Convergence Vol. 4, No. 1, June 2019, pp. 32-45

[60] Junaid Ahsenali Chaudhry, Usman Tariq, Mohammed Arif Amin, Robert G. Rittenhouse, “Dealing with Sinkhole Attacks in Wireless Sensor Networks”, Advanced Science and Technology Letters Vol.29 (SecTech November 2013), pp.7-12, DOI: 10.14257/astl.2013.29.02

[61] Ali Modirkhazeni, Norafida Ithnin, Mohammadjavad Abbasi, “Secure Hierarchal Routing Protocols in Wireless Sensor Networks; Security Survey Analysis”, International Journal of Computer Communications and Networks, Volume 2, Issue 1, February 2012

[62] Carolina Del Valle Soto, Carlos Mex-Perera, “An efficient Multi-Parent Hierarchical Routing Protocol for WSNs”, April 2014, DOI: 10.1109/WTS.2014.6834993

[63] Fasee Ullah, Tahir Mehmood, Masood Habib, Muhammad Ibrahim, “SPINS: Security Protocols for Sensor Networks”, International Conference on Machine Learning and Computing IPCSIT vol.3, July 2009

[64] Maleh Yassine, Abdellah Ezzati, “LEAP Enhanced: A Lightweight Symmetric Cryptography Scheme for Identifying Compromised Node in WSN”,

International Journal of Mobile Computing and Multimedia Communications, Volume 7 • Issue 3 • July-September 2016 DOI: 10.4018/IJMCMC.2016070104

[65] https://el.wikipedia.org/wiki/DARPA

[66] https://en.wikipedia.org/wiki/Public-key_cryptography

[67] https://en.wikipedia.org/wiki/Symmetric-key_algorithm

[68] https://en.wikipedia.org/wiki/Directional_antenna

[69] https://en.wikipedia.org/wiki/Message_authentication_code

[70] Waltenegus Dargie, Christian Poellabauer, "FUNDAMENTALS OF WIRELESS SENSOR NETWORKS THEORY AND PRACTICE", @2010 John Wiley & Sons Ltd., ISBN 978-0-470-99765-9 (H/B),

[71] Feriel Bouakkaz, Mawloud Omar, Ahcene Bounceur, Abdelkamel Tari, "Secure and Efficient Sharing Aggregation Scheme for Data Protection in WSNs", December 2015, DOI: 10.1109/ISSPIT.2015.7394374

[72] Ulya Sabeel, Saima Maqbool, Nidhi Chandra, "Categorized Security Threats in the Wireless Sensor Networks: Countermeasures and Security Management Schemes", International Journal of Computer Applications (0975 – 8887), Volume 64– No.16, February 2013

[73] Ashfaq Hussain Farooqi, Farrukh Aslam Khan, "Intrusion Detection Systems for Wireless Sensor Networks: A Survey", January 2009, International Journal of Ad Hoc and Ubiquitous Computing 9(2):234-241, DOI: 10.1504/IJAHUC.2012.045549