ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

ΑΣΦΑΛΕΙΑ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ ΑΙΣΘΗΤΗΡΩΝ (WSN) ΣΕ ΕΦΑΡΜΟΓΕΣ ΕΠΙΤΗΡΗΣΗΣ ΚΑΙ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ ΠΕΡΙΟΧΗΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΒΟΥΡΟΣ ΑΝΔΡΕΑΣ

Επιβλέπων: Παναγιώτης Κωττής
Καθηγητής ΕΜΠ

Αθήνα, Μάρτιος 2015

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

ΑΣΦΑΛΕΙΑ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ ΑΙΣΘΗΤΗΡΩΝ (WSN) ΣΕ ΕΦΑΡΜΟΓΕΣ ΕΠΙΤΗΡΗΣΗΣ ΚΑΙ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ ΠΕΡΙΟΧΗΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΒΟΥΡΟΣ ΑΝΔΡΕΑΣ

Επιβλέπων: Παναγιώτης Κωττής
Καθηγητής ΕΜΠ

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την

.....	.....	.....
Π. Κωττής Καθηγητής ΕΜΠ	Χ. Καψάλης Καθηγητής ΕΜΠ	Γ. Φικιώρης Αν. Καθηγητής ΕΜΠ

Αθήνα, Μάρτιος 2015

(Υπογραφή)

.....

Ανδρέας Ι. Βούρος

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

ΠΕΡΙΛΗΨΗ

Τα ασύρματα δίκτυα αισθητήρων (Wireless Sensor Networks) αποτελούν δικτυακές υποδομές με μεγάλο αριθμό συσκευών – κόμβων χαμηλού κόστους, οι οποίες αναπτύσσονται στην περιοχή ενδιαφέροντος. Αποστολή τους είναι η ανίχνευση, παρακολούθηση και καταγραφή συμβάντων στην περιοχή αυτή. Ένα δίκτυο WSN διοχετεύει τη συλλεγόμενη πληροφορία και τα μηνύματα διαχείρισης με πολλαπλά άλματα μέσω των κόμβων που το συνθέτουν προς το σταθμό βάσης. Οι κόμβοι που συμμετέχουν σε ένα δίκτυο WSN έχουν σοβαρούς περιορισμούς σε ζητήματα υπολογιστικών, αποθηκευτικών και ενεργειακών πόρων, εξαιτίας των απαιτήσεων συγκράτησης του κόστους του δικτύου σε αποδεκτά επίπεδα και εξοικονόμησης ενέργειας (αύξηση ορίου λειτουργίας δικτύου). Σύμφωνα με αυτούς τους περιορισμούς, έχουν αναπτυχθεί πρωτόκολλα επικοινωνίας, με βάση την αρχιτεκτονική του δικτύου, η οποία στηρίζεται στο μοντέλο OSI. Τα πρωτόκολλα αυτά υλοποιούν στοίβες πρωτοκόλλων με βάση αυτή την αρχιτεκτονική και αποτελούν τη βάση για την ανάπτυξη προτύπων επικοινωνίας, με κυριότερες την τεχνολογία ZigBee και το πρότυπο Bluetooth LE.

Η παρουσία των περιοριστικών παραγόντων σε ένα δίκτυο WSN, σε συνδυασμό με το ασύρματο μέσο μετάδοσης και την απομακρυσμένη και χωρίς ανθρώπινη επίβλεψη λειτουργία, καθιστούν το δίκτυο αυτό σε κίνδυνο, ως προς την εκδήλωση επιθέσεων. Οι επιθέσεις αυτές θέτουν υπό αμφισβήτηση τις απαιτήσεις ασφαλείας, οι οποίες είναι η διαθεσιμότητα, η εμπιστευτικότητα, η αυθεντικότητα, η ακεραιότητα, η ιδιωτικότητα, η μη αποποίηση, η φρεσκάδα δεδομένων, η ευρωστία, η αυτό-οργάνωση και ο συγχρονισμός συσκευών. Οι εν λόγω επιθέσεις στοχεύουν στις λειτουργίες του δικτύου, με βάση την αρχιτεκτονική του, με σημαντικότερες τις επιθέσεις άρνησης εξυπηρέτησης (DoS) και τις επιθέσεις καταβόθρας, σιβυλλικής μορφής, σκουληκότρυπας, ανάλυσης κίνησης, κατά του απορρήτου, φυσικές και αναπαραγωγής κόμβου. Τα πρωτόκολλα που έχουν αναπτυχθεί για συνήθεις εφαρμογές δεν προσφέρουν προστασία έναντι των επιθέσεων αυτών, καθώς είναι σχεδιασμένα με γνώμονα την απλότητα και την εξοικονόμηση ενέργειας. Για το λόγο αυτό έχουν αναπτυχθεί μηχανισμοί και πρωτόκολλα, τα οποία προσφέρουν δικλείδες ασφαλείας σε θέματα ανίχνευσης επιθέσεων, δρομολόγησης και συνάθροισης δεδομένων. Επιπλέον, η κρυπτογράφηση και οι μηχανισμοί αυθεντικοποίησης και

προστασίας απορρήτου κινούνται προς αυτή την κατεύθυνση. Ωστόσο, οι παραπάνω μηχανισμοί προσφέρουν ασφάλεια στο δίκτυο, με αντίκρισμα την αύξηση της πολυπλοκότητας και της κατανάλωσης ενέργειας σε αυτό.

Λέξεις κλειδιά: << αισθητήριοι κόμβοι, σταθμός βάσης, πρωτόκολλα επικοινωνίας, αρχιτεκτονική WSN, απαιτήσεις ασφαλείας, επιθέσεις – απειλές ασφαλείας, άρνηση εξυπηρέτησης, κρυπτογράφηση, ασφαλής δρομολόγηση, ασφαλής συνάθροιση δεδομένων >>

ABSTRACT

Wireless sensor networks (WSN) are network structures with a large number of low cost devices – nodes, which are located in the surveillance area. Their operation includes the detection, observation and record of events in this area. A WSN drains the collected information and the management messages through nodes, which compose it, to the base station, using multiple – hop routing technique. The nodes, which compose a WSN, are characterized by critical constraints on processing, storage and energy issues, due to the requirement of a low cost service and low energy consumption. According to these constraints, communication protocols have been developed based on OSI model. These protocols implement protocol stacks, according to WSN architecture and constitute the base of the development of communication standards, like ZigBee technology and BluetoothLE.

The constraints of a WSN, in the combination with the wireless transmission medium and the remote function without human supervision, make the network prone to attacks. These attacks challenge the security requirements, like availability, confidentiality, authentication, integrity, privacy, non – reputation, freshness, robustness, self – organization and device synchronization. The attacks are planned to affect the network functions, according to its architecture. The most crucial attacks are DoS (Denial of Service) attacks and the sinkhole, Sybil, wormhole, traffic analysis, against privacy, physical and node replication attacks. The protocols, which are developed for common services, are not appropriate to provide protection against these attacks, as are designed to be simple and energy – saving. Therefore, secure mechanisms and protocols have been developed, in order to offer security measures in intrusion detection, routing and data aggregation issues. In addition, cryptography, authentication and privacy protection techniques focus on these security issues. Nevertheless, the above mechanisms offer security services, increasing the complexity and the energy consumption.

Key words: << sensor nodes, base station, communication protocols, WSN architecture, security requirements, security attacks - threats, denial of service, cryptography, secure routing, secure data aggregation >>

ΕΥΧΑΡΙΣΤΗΡΙΟ ΣΗΜΕΙΩΜΑ

Η παρούσα διπλωματική εργασία συντάχθηκε στα πλαίσια του προπτυχιακού προγράμματος σπουδών του τμήματος Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου. Θα ήθελα να εκφράσω τις ευχαριστίες μου, πρωτίστως στο καθηγητή κύριο Παναγιώτη Κωττή, ο οποίος ανέλαβε την επίβλεψη της εργασίας, για την υποστήριξη και καθοδήγηση του. Επιπλέον, θα ήθελα να ευχαριστήσω τους καθηγητές και τους συμφοιτητές μου, με τους οποίους θεωρώ ότι είχα μία εποικοδομητική συνεργασία κατά τη διάρκεια των σπουδών μου και την οικογένεια μου, η οποία με στήριξε με τον καλύτερο δυνατό τρόπο.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Κεφάλαιο 3: Προδιαγραφές Ασφαλείας και Μοντέλο Επιθέσεων

Κεφάλαιο 4: Μηχανισμοί Ασφαλείας Ασύρματων Δικτύων Αισθητήρων

Εισαγωγή

1. Πρόλογος

Τα ασύρματα δίκτυα αισθητήρων (WSN) αποτελούν μια δικτυακή υποδομή, η οποία γεφυρώνει το χάσμα μεταξύ φυσικού και ψηφιακού κόσμου, συλλέγοντας πληροφορίες από το περιβάλλον ενδιαφέροντος. Οι πληροφορίες αυτές προωθούνται μέσω των κόμβων του δικτύου σε μία υπολογιστικά ισχυρή οντότητα, η οποία τις διαχειρίζεται με κατάλληλη επεξεργασίας, αποδίδοντας την στον τελικό χρήστη. Τα δίκτυα WSN είναι εφικτό να λειτουργούν για μεγάλο χρονικό διάστημα, χωρίς την ανθρώπινη επίβλεψη. Για το λόγο αυτό, η εξέλιξη τους είναι ραγδαία, ειδικά σε περιβάλλοντα δυσπρόσιτα για τον άνθρωπο, στα οποία όμως είναι η συλλογή πληροφοριών (ανίχνευση, παρακολούθηση ή καταγραφή συμβάντων), κρίνεται σημαντική.

2. Σκοπός

Σκοπός της παρούσας εργασίας είναι να διερευνήσει ζητήματα ασφαλείας σε δίκτυα WSN και ειδικότερα σε εφαρμογή επιτήρησης περιοχής (στρατιωτική εφαρμογή). Η διερεύνηση αυτή γίνεται υπό το πρίσμα των ιδιαιτεροτήτων της φύσης ενός δικτύου WSN, ως προς θέματα δομής, δυνατοτήτων συσκευών – κόμβων, μεθόδων δρομολόγησης κλπ. Συγκεκριμένα, επιδιώκεται η εξέταση των απειλών, οι οποίες είναι πιθανό να θέσουν υπό αμφισβήτηση την ασφάλεια ενός δικτύου WSN καθώς και η διερεύνηση μηχανισμών αντιμετώπισης τους, οι οποίοι αποσκοπούν στην εξασφάλιση των καθοριζόμενων απαιτήσεων. Τέλος, εξετάζεται η εφαρμογή των ζητημάτων διαχείρισης και ασφάλειας δικτύου σε ένα δίκτυο WSN επιτήρησης περιοχής, στην οποία οι απαιτήσεις ασφαλείας κρίνονται αυστηρές,

3. Δομή εργασίας

Στο Κεφάλαιο 1 γίνεται αναφορά στα ασύρματα δίκτυα αισθητήρων (WSN), με έμφαση τα χαρακτηριστικά που τα διέπουν, τη δομή τους, τη διαχείριση λειτουργιών τους και τη διάδραση τους με έτερα δίκτυα.

Στο Κεφάλαιο 2 γίνεται αναφορά στην αρχιτεκτονική ενός δικτύου WSN, η οποία κρίνεται αναγκαία για την κατανόηση των ζητημάτων ασφαλείας. Επιπλέον, γίνεται αναφορά πρωτοκόλλων επικοινωνίας, τα οποία βρίσκουν εφαρμογή σε

συνήθεις εφαρμογές WSN, με βάση τη συγκεκριμένη αρχιτεκτονική. Τέλος, γίνεται συνοπτική αναφορά και σύγκριση των προτύπων, τα οποία έχουν σχεδιαστεί για τέτοια δίκτυα.

Στο Κεφάλαιο 3 παρουσιάζονται οι απαιτήσεις ασφαλείας ενός δικτύου WSN, η επίτευξη των οποίων αποτελεί πρόκληση, εξαιτίας των ιδιαιτεροτήτων ενός τέτοιου δικτύου. Οι ιδιαιτερότητες αυτές προσδίδουν στα συγκεκριμένα δίκτυα ευπάθεια έναντι κακόβουλων ενεργειών (επιθέσεων). Επιπλέον, εξετάζονται οι πιθανές επιθέσεις σε ένα δίκτυο WSN, υπό το πρίσμα της αρχιτεκτονικής του δικτύου και των λειτουργιών που θίγονται.

Στο Κεφάλαιο 4 παρουσιάζονται οι μηχανισμοί ασφαλείας για την αντιμετώπιση επιθέσεων σε ένα δίκτυο WSN. Συγκεκριμένα, εξετάζεται αρχικά το ζήτημα ανίχνευσης μιας κακόβουλης ενέργειας και εν συνεχεία τα αντίμετρα των επιθέσεων που έχουν παρατεθεί στο προηγούμενο κεφάλαιο. Επιπλέον, εξετάζονται ζητήματα ασφαλούς δρομολόγησης και συνάθροισης δεδομένων, κρυπτογράφησης, αυθεντικοποίησης και προστασίας απορρήτου.

Στο Κεφάλαιο 5 εξετάζεται ένα σενάριο εφαρμογής επιτήρησης περιοχής, στο οποίο καθορίζονται οι απαιτήσεις και οι πιθανές επιθέσεις και εξετάζονται λύσεις για την ικανοποίηση ασφαλούς και αξιόπιστης λειτουργίας.

Κεφάλαιο 1

Ασύρματα Δίκτυα Αισθητήρων (Wireless Sensor Networks)

1. 1 Εισαγωγή

Ένα ασύρματο δίκτυο αισθητήρων (Wireless Sensor Network – WSN) είναι μια δικτυακή υποδομή αποτελούμενη από μονάδες ικανές να δέχονται εξωτερικά ερεθίσματα (αισθητήριοι κόμβοι), να επεξεργάζονται τα δεδομένα που συλλέγουν και να επικοινωνούν τόσο μεταξύ τους, όσο και με το διαχειριστή του δικτύου. Ο διαχειριστής δικτύου έχει τη δυνατότητα να παρατηρεί και να αλληλεπιδρά με το δίκτυο αναλόγως των απαιτήσεων της εφαρμογής. Τα δίκτυα WSN ερμηνεύονται ως μια ιδιαίτερη μορφή ad hoc δικτύων. Τα ad hoc δίκτυα αναπτύσσονται με μη προσχεδιασμένο και τυχαίο τρόπο στο πεδίο ενδιαφέροντος, χωρίς να απαιτείται προϋπάρχουσα υποδομή. Με παρόμοιο τρόπο, τα δίκτυα WSN σχεδιάζονται έτσι ώστε να απαιτείται η ελάχιστη ή μηδενική υποδομή για την ανάπτυξή τους. Υπάρχουν δύο τύποι δικτύων WSN: (α) τα δομημένα (structured), όπου το δίκτυο των κόμβων αναπτύσσεται σε προεπιλεγμένες θέσεις και (β) τα μη δομημένα (unstructured) ή τυχαία, όπου οι κόμβοι αναπτύσσονται κατά τυχαίο και μη προσχεδιασμένο (ad hoc) τρόπο.

Η υλοποίηση μη δομημένων δικτύων WSN προσδίδει μεγαλύτερη ευελιξία, ωστόσο εμφανίζει δυσχέρειες σε ζητήματα συντήρησης και διαχείρισης σε σύγκριση με τα αντίστοιχα δομημένα. Επιπλέον, η ανάπτυξη με τυχαίο τρόπο δεν εγγυάται την επαρκή κάλυψη της περιοχής ενδιαφέροντος. Τα δίκτυα WSN διακρίνονται περαιτέρω ανάλογα με το περιβάλλον ανάπτυξης και τα αισθητήρια μέσα σε υπέργεια, υπόγεια, υποθαλάσσια, κινητά και πολυμέσων. Η διάκριση αυτή γίνεται εξαιτίας των διαφορετικών απαιτήσεων που προκύπτουν από κάθε εφαρμογή σε ζητήματα υλικού, λογισμικού και πρωτοκόλλων επικοινωνίας.

Τα δίκτυα αισθητήρων διαφέρουν κατά κάποιο τρόπο από τις υπόλοιπες μορφές δικτύων, καθώς οι κόμβοι ενδέχεται να σταματήσουν να λειτουργούν, λόγω διαφόρων αιτιών (περιβαλλοντική φθορά, αστοχία ή καταστροφή κατά την ανάπτυξη του δικτύου), αλλά κυρίως λόγω των ενεργειακών περιορισμών που επιβάλλει η τροφοδοσία τους και των περιορισμών σε υπολογιστικούς, επικοινωνιακούς και αποθηκευτικούς πόρους. Η απώλεια κόμβων ενός WSN προκαλεί συχνές αλλαγές της τοπολογίας του δικτύου. Σε διαμορφώσεις WSN με χαρακτηριστικό την δυνατότητα

αυτόνομης αλλαγής θέσης των κόμβων (mobility), η διατήρηση της στιβαρότητας και σταθερότητας του δικτύου γίνεται ακόμα δυσολότερη.

Κατά συνέπεια, απαιτείται η δυνατότητα αυτό-οργάνωσης (self organizing) του δικτύου WSN, για όσο το δυνατό αποδοτικότερη αξιοποίηση των περιορισμένων και συχνά μεταβαλλόμενων πόρων του. Για να ικανοποιηθούν οι ανωτέρω απαιτήσεις αναπτύχθηκαν τα πρότυπα επικοινωνίας IEEE 802.15.4 και η τεχνολογία ZigBee, καθώς και πλήθος άλλων εξειδικευμένων πρωτοκόλλων στα οποία θα γίνει εκτεταμένη αναφορά στη συνέχεια. Με γνώμονα την ασφάλεια σε δίκτυα WSN, έχουν αναπτυχθεί επιπλέον πρωτόκολλα και μηχανισμοί, όπως θα δούμε στο Κεφάλαιο 4.

1.2 Εξέλιξη δικτύων αισθητήρων

Η προέλευση των δικτύων αισθητήρων εντοπίζεται στην έρευνα για στρατιωτικές εφαρμογές. Συγκεκριμένα, τα δίκτυα αισθητήρων σε πρώιμη μορφή έκαναν την εμφάνισή τους κατά την περίοδο του ψυχρού πολέμου, οπότε και υλοποιήθηκε από τις ΗΠΑ ένα δίκτυο ακουστικών υποθαλάσσιων αισθητήρων για τον εντοπισμό και την παρακολούθηση υποβρυχίων (ηχητικό σύστημα επιτήρησης SOSUS), το οποίο αξιοποιείται ακόμα από την αμερικανική ωκεανογραφική υπηρεσία (NOAA) για την παρακολούθηση υποθαλάσσιας σεισμικής δραστηριότητας. Επίσης, το δίκτυο RADAR αεράμυνας που υλοποιήθηκε στις ΗΠΑ και που αξιοποιούσε εναέρια μέσα (AWACS) ως αισθητήρια μέσα αποτελεί μια σημαντική πρώιμη μορφή δικτύου αισθητήρων.

Στη δεκαετία του 1980, με επίκεντρο τις ΗΠΑ και τις έρευνες που διεξήγαγε η DARPA (υπηρεσία προχωρημένων ερευνών για την άμυνα), εξετάστηκαν οι δυνατότητες της αξιοποίησης του ARPA NET (πρόγονος του INTERNET) και του πρόσφατα, τότε, αναπτυχθέντος TCP/IP πρωτοκόλλου στο πεδίο της μάχης υπό τη μορφή δικτύου αισθητήρων. Αυτή αποτέλεσε μια πρώτη προσέγγιση ενός κατανεμημένου δικτύου αισθητήρων (DSN) το οποίο αποτελούνταν από χαμηλού κόστους συσκευές οι οποίες συνεργάζονταν προκειμένου να επιτύχουν επιτήρηση και παρακολούθηση.

Κατάλληλοι αλγόριθμοι αναπτύχθηκαν και με οδηγό το πρόγραμμα DSN στην δεκαετία του 1990, επιχειρήθηκε η υλοποίηση DSN δικτύων αποτελούμενα από εξελιγμένους αισθητήρες αλλά με επιδίωξη να χρησιμοποιηθεί τεχνολογία και πρότυπα δικτύωσης ήδη διαθέσιμα στην αγορά. Σκοπός ήταν να μειωθεί το κόστος

και ο χρόνος ανάπτυξης. Το αποτέλεσμα ήταν η πλήρης ενσωμάτωση των δικτύων αισθητήρων στο πεδίο της μάχης και η δημιουργία ενός δίκτυο-κεντρικού θεάτρου επιχειρήσεων (Network Centric Warfare).

Με την αξιοποίηση αυτής της ερευνητικής κληρονομιάς και με την πρόοδο στις επικοινωνίες και τον τα υπολογιστικά συστήματα προέκυψε μια νέα γενιά τεχνολογιών δικτύων αισθητήρων. Η ενσωμάτωση ηλεκτρονικών συστημάτων κλίμακας μικρομέτρου (και πρόσφατα νανομέτρου) στις αισθητήριες συσκευές (motes ή sensor boards) και η χρήση ευρέως διαδεδομένων προτύπων ασύρματης δικτύωσης (οικογένεια προτύπων IEEE 802, τεχνολογία ZigBee, WiMax, Bluetooth), μείωσαν το κόστος και έκαναν εφικτή την ευρεία χρήση των δικτύων WSN.

1.3 Δομικά στοιχεία δικτύων WSN

Τα δομικά στοιχεία ενός δικτύου WSN είναι ένας αριθμός συσκευών, οι οποίοι έχουν αναπτυχθεί στην περιοχή ενδιαφέροντος, και τουλάχιστον μία συσκευή, η οποία αποτελεί το σημείο συγκέντρωσης της πληροφορίας που έχει συλλεχθεί από τους αισθητήριους κόμβους και καλείται σταθμός βάσης (base station) ή καταβόθρα (sink).

1.3.1 Κόμβοι δικτύου

Η εξέλιξη της τεχνολογίας μικροηλεκτρονικών συστημάτων (Micro Electro Machines Systems - MEMS) επιτάχυνε την ανάπτυξη έξυπνων αισθητήρων (Smart Sensors). Οι έξυπνοι αισθητήρες είναι διατάξεις μικρού κόστους και μεγέθους με περιορισμένες επεξεργαστικές, αποθηκευτικές και υπολογιστικές δυνατότητες και δυνατότητα ασύρματης δικτύωσης.

Λόγω του μικρού μεγέθους τους, οι κόμβοι μπορούν να χρησιμοποιηθούν για την παρακολούθηση φαινομένων σε μεγάλη εγγύτητα, ενώ η αυτονομία που έχουν επιτρέπει την ανάπτυξή τους σε περιοχές δυσπρόσιτες χωρίς υποδομή. Στην πλατφόρμα των κόμβων (motes ή sensor boards) μπορούν να ενσωματωθούν περισσότερες της μίας διατάξεις ανίχνευσης, ικανές να αντιλαμβάνονται ποικίλες παραμέτρους του περιβάλλοντος ανάπτυξης, οι οποίες με κριτήριο το μετρούμενο μέγεθος διακρίνονται αισθητήρες (α) ηλεκτρικών σημάτων (τάση, ένταση ρεύματος, φορτίο), (β) μαγνητικών σημάτων (ένταση μαγνητικού πεδίου, μαγνητική ροή, μαγνήτιση), (γ) θερμικών σημάτων (θερμοκρασία , θερμότητα , ροή θερμότητας), (δ) μηχανικών σημάτων (δύναμης, κίνησης, πίεσης, ταχύτητας, επιτάχυνσης), (ε)

ακτινοβολίας (ενέργεια, ισχύ, ένταση) και (στ) χημικών σημάτων (συγκεντρώσεις υλικών, σύνθεση, ρυθμός αντίδρασης).

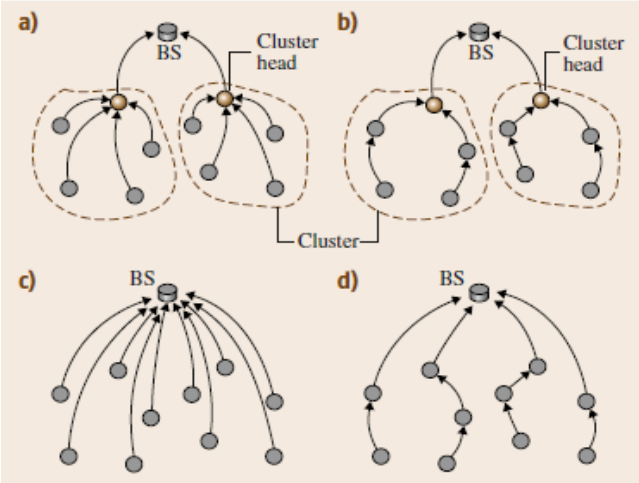
Οι κόμβοι διακρίνονται σε γενικού σκοπού (generic- multi purpose), σε κόμβους πύλες (gateway) και σε κόμβους αναμετάδοσης (relay). Οι διαφοροποιήσεις εντοπίζονται στις υπολογιστικές και επικοινωνιακές δυνατότητες που τους διακρίνουν. Οι κόμβοι πύλες αναλαμβάνουν να διαβιβάσουν τα δεδομένα αυτά στο σταθμό βάσης, όπου γίνεται η επεξεργασία των δεδομένων και ο έλεγχος του δικτύου WSN.

1.3.2. Σταθμός βάσης

Ο σταθμός βάσης αποτελεί το επίκεντρο ενός δικτύου WSN, αποτελεί μια οντότητα αυξημένων δυνατοτήτων υπολογισμών και αποθήκευσης, η οποία μπορεί να είναι ένα σημείο πρόσβασης προς τον χειριστή της εφαρμογής (human interface) ή ένας κόμβος – πύλη (gateway) προς ένα άλλο δίκτυο. Η επικοινωνία των κόμβων που ανήκουν σε ένα δίκτυο WSN με τον σταθμό βάσης πραγματοποιείται ανάλογα με τη διάταξη τους στο πεδίο, είτε μέσω άλλων κόμβων, είτε απευθείας. Πριν την αποστολή των δεδομένων στο σταθμό βάσης, τα δεδομένα υφίστανται επεξεργασία τοπικά. Η επεξεργασία αυτή μπορεί να αφορά τεχνικές συμπίεσης, κρυπτογράφησης και συλλογής της πληροφορίας. Τα δεδομένα πρέπει να είναι κατάλληλα καταχωρισμένα και διευθυνσιοδοτημένα (time stamp-position) ώστε να είναι δυνατός ο εντοπισμός τους κατά την υποβολή ερωτημάτων. Εφόσον οι κόμβοι διαθέτουν και δυνατότητα προσδιορισμού της θέσης τους (GPS) ή έχουν εξαρχής γνώση αυτής (σε προκαθορισμένη ανάπτυξη), είναι δυνατή η υποβολή στοχοποιημένων ερωτημάτων από το σταθμό βάσης προς εκείνες τις ομάδες που βρίσκονται εγγύτερα στην περιοχή ενδιαφέροντος.

Εξαιτίας περιορισμών εμβέλειας των κόμβων και για εξοικονόμηση ενέργειας η επικοινωνία μεταξύ μακρινών κόμβων και του σταθμού βάσης αποφεύγεται. Με κριτήριο την απαίτηση για βέλτιστη κατανάλωση ενέργειας οι τρόποι δρομολόγησης των δεδομένων χωρίζονται σε δύο κατηγορίες: (α) δρομολόγηση δεδομένων βασισμένο σε ομάδες κόμβων (clusters) και (β) δρομολόγηση δεδομένων με πολλαπλές αναπηδήσεις - άλματα (multi-hop). Η δρομολόγηση με βάση την ομαδοποίηση των κόμβων μπορεί να υλοποιηθεί είτε με πολλαπλά άλματα, είτε χωρίς. Οι παραπάνω τρόποι δρομολόγησης καθώς και η απευθείας δρομολόγηση, σε περίπτωση που οι συνθήκες το επιτρέπουν (εγγύτητα με

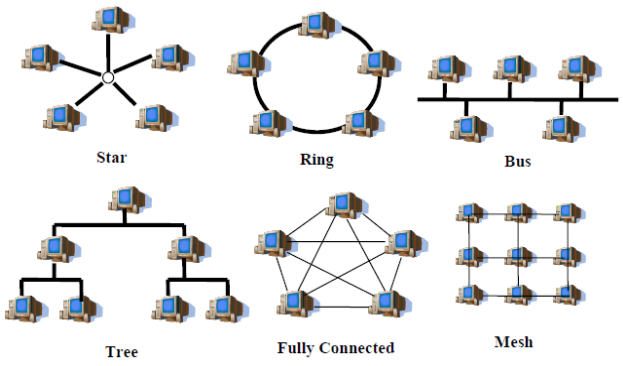
σταθμό βάσης) αποτελούν τις μεθόδους δρομολόγησης, οι οποίες απεικονίζονται στο Σχήμα 1.1.



Σχήμα 1.1. Τέσσερις μέθοδοι δρομολόγησης σε δίκτυα WSN: a) Απλής αναπήδησης σε ομάδες κόμβων, b) Πολλαπλής αναπήδησης σε ομάδες κόμβων, c) Απλής αναπήδησης χωρίς ομάδες κόμβων, d) Πολλαπλής αναπήδησης χωρίς ομάδες κόμβων

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 στο Σχήμα 1.2 είναι:



Σχήμα 1.2. Βασικές Τοπολογίες

- Τοπολογία αστέρα (Star): Κάθε κόμβος δεν μπορεί να επικοινωνήσει απευθείας με άλλους, αλλά δρομολογεί δεδομένα μέσω ενός κεντρικού κόμβου. Οι κόμβοι (αισθητήρες) συλλέγουν την πληροφορία και τη διοχετεύουν στο κεντρικό κόμβο, δηλαδή δεν υποστηρίζουν λειτουργία λήψης δεδομένων. Βασικό πλεονέκτημα

είναι ότι η απώλεια κάποιου κόμβου πλην του κεντρικού δεν θέτει το δίκτυο WSN εκτός λειτουργίας. Μειονέκτημα της τοπολογίας είναι η κρισιμότητα του κεντρικού κόμβου, που καθιστά το δίκτυο (α) λιγότερο ευέλικτο σε επέκταση, καθώς αυτή επηρεάζεται άμεσα από την ικανότητα του να εξυπηρετήσει νέους κόμβους και (β) περισσότερο ευαίσθητο σε περίπτωση κατάρρευσης του κεντρικού κόμβου, καθώς ένα τμήμα του δικτύου τίθεται εκτός λειτουργίας.

- Σημείο προς σημείο (Point to Point): Στη τοπολογία P-P κάθε κόμβος ανταλλάσσει με τους γειτονικούς του δεδομένα με αμφίδρομη λειτουργία (αποστολή και λήψη δεδομένων) δίχως να μεσολαβεί κεντρικός κόμβος. Αν και απλούστερη σε υλοποίηση σε σχέση με τη τοπολογία αστέρα, ενδεχόμενη απώλεια ενός κόμβου θέτει εκτός λειτουργίας ένα μεγαλύτερο τμήμα του δικτύου, γεγονός μειώνει την αξιοπιστία του.

- Δακτύλιος (Ring): Δεν υπάρχει κεντρικός κόμβος και όλοι οι κόμβοι επιτελούν την ίδια λειτουργία. Τα δεδομένα μεταδίδονται προς μία μόνο κατεύθυνση δηλαδή οι κόμβοι δεν λειτουργούν αμφίδρομα. Το γεγονός ότι οι κόμβοι συνδέονται αλυσιδωτά υπό μορφή δακτυλίου καθιστά το δίκτυο προβληματικό στη περίπτωση που ένας κόμβος καταρρεύσει. Μερική λύση στο πρόβλημα δίνει η σχεδίαση SHR (Self-Healing Ring Network), που χρησιμοποιεί δύο παράλληλους δακτυλίους (κύριο και εφεδρικό) και είναι λιγότερο επιρρεπής σε σφάλματα.

- Τοπολογία Bus: Στη σχεδίαση Bus, τα δεδομένα μεταδίδονται σε όλους τους κόμβους. Κάθε κόμβος ελέγχει την επικεφαλίδα του πλαισίου δεδομένων και εντοπίζει και επεξεργάζεται τα δεδομένα που απευθύνονται σε αυτόν.

- Δένδρο (Tree): Η τοπολογία δέντρου διαθέτει ένα κύριο κόμβο (root node), ο οποίος λειτουργεί ως κύριος δρομολογητής δεδομένων. Ο κύριος κόμβος συνδέεται με αριθμό κεντρικών κόμβων οι οποίοι υλοποιούν ένα δίκτυο τοπολογίας αστέρα, όπου συνδέονται οι εξαρτημένοι από αυτούς κόμβοι.

- Πλήρως διασυνδεδεμένη (Fully connected): Στη συγκεκριμένη τοπολογία η πληροφορία από τον αισθητήριο κόμβο προς το σταθμό βάσης δρομολογείται προς όλους τους κόμβους του δικτύου. Πρόκειται για την περισσότερο πολύπλοκη τοπολογία και με μεγάλο κόστος ανάπτυξης.

- Τοπολογία πλέγματος (Mesh): Πρόκειται για δίκτυα που επιτρέπουν την επικοινωνία γειτονικών κόμβων. Ως εκ τούτου, η πολυπλοκότητα σε σύγκριση με ένα δίκτυο πλήρως διασυνδεδεμένο είναι μικρότερη.

1.5 Έλεγχος και διαχείριση δικτύων WSN

Η βέλτιστη διαχείριση των πόρων και της λειτουργίας ενός δικτύου WSN συναντάται στην βιβλιογραφία υπό τον όρο «υπηρεσίες δικτύου» (network services). Πρόκειται για υπηρεσίες που συντονίζουν και ελέγχουν την λειτουργία των κόμβων, αντιμετωπίζοντας και επιλύοντας ζητήματα κρίσιμης σημασίας για την λειτουργία των δικτύων WSN, όπως:

- Εντοπισμός των κόμβων (Localization).
- Συγχρονισμός των κόμβων του δικτύου (Synchronization)
- Κάλυψη της περιοχής ενδιαφέροντος (Coverage)
- Ασφάλεια δεδομένων και επικοινωνιών του δικτύου (Security)
- Συνάθροιση των δεδομένων (Data Aggregation)
- Ανοχή σε σφάλματα (fault tolerance)
- Δυνατότητα κλιμάκωσης - Επεκτασιμότητα (Scalability)
- Ποιότητα της Υπηρεσίας (Quality of Service – QoS)

1.5.1 Προσδιορισμός θέσης

Στα δίκτυα WSN, οι κόμβοι που αναπτύσσονται στο πεδίο με τυχαίο τρόπο (ad hoc) δεν έχουν εκ των προτέρων γνώση της θέσης τους. Οι υπάρχουσες μέθοδοι προσδιορισμού της θέσης περιλαμβάνουν χρήση GPS, χρήση κόμβων φάρων (beacon) ή άγκυρες (anchors) και εντοπισμό θέσης με βάση την εγγύτητα προς άλλους κόμβους γνωστής θέσης.

Σε επίπεδο λογισμικού αξιοποιούνται αλγόριθμοι για τον εντοπισμό της θέσης των κόμβων. Στο [2] οι αλγόριθμοι εντοπισμού θέσης παρουσιάζονται ως η πιο ενδεδειγμένη από πλευράς κόστους τεχνική και ταξινομούνται σε δύο κατηγορίες: τους συγκεντρωτικούς (centralized) και τους κατανεμημένους (distributed). Σημαντικότεροι από τους αλγόριθμους που αναφέρονται στο [2] είναι ο αλγόριθμος του Moore, ο RIPS και ο Spotlight.

1.5.2 Συγχρονισμός

Ο συγχρονισμός (Synchronization) σε ένα δίκτυο WSN είναι σημαντικός για την επιτυχή δικτύωση και την εξοικονόμηση ενέργειας. Ο συγχρονισμός επιτρέπει στους κόμβους να συνεργάζονται και να μεταδίδουν δεδομένα σύμφωνα με ένα χρονικό προγραμματισμό. Η εξοικονόμηση της ενέργειας επιτυγχάνεται με την ασυνεχή λειτουργία των πομποδεκτών (sleep/wake up scheme).

Υπάρχουν πολλοί διαφορετικοί τύποι συγχρονισμού των ρολογιών του δικτύου. Η μέθοδος που προσεγγίζει καλύτερα τις παραμέτρους ενός δικτύου WSN, είναι η σχετική αντίληψη του ρολογιού (Relative notion of clock) [3, ενότητα 6.9]. Συγχρονισμός επίσης μπορεί να πραγματοποιηθεί με βάση τη φυσική σειρά γεγονότων, τα οποία κρίνονται από σχεδιαστική άποψη σημαντικότερα από την ακριβή χρονική στιγμή που πραγματοποιούνται. Τα πρωτόκολλα συγχρονισμού κατηγοριοποιούνται (α) με βάση ζητήματα συγχρονισμού και (β) με βάση τα χαρακτηριστικών που απορρέουν από την εφαρμογή.

Η αξιολόγηση των πρωτοκόλλων συγχρονισμού πραγματοποιείται με κριτήρια όπως η ακρίβεια, η κατανάλωση ενέργειας, η πολυπλοκότητα, η επεκτασιμότητα και τα περιθώρια λάθους.

1.5.3 Κάλυψη

Η ανάπτυξη των αισθητήρων και η παρεχόμενη κάλυψη εξαρτάται από τις απαιτήσεις της εφαρμογής. Συγκεκριμένα, η εξάρτηση αυτή αφορά στο κατά πόσο το υπό ανάπτυξη δίκτυο είναι στατικό (σταθεροί, μόνιμα τοποθετημένοι κόμβοι) ή κινητό (δυνατότητα κίνησης των κόμβων σε ένα δυναμικό περιβάλλον από πλευράς κάλυψης). Η πολυπλοκότητα που εισάγει σε ένα δίκτυο WSN η κινητικότητα των κόμβων είναι μεγάλη, τόσο σε φυσικό επίπεδο (δυνατότητες κίνησης-εποχούμενοι κόμβοι), όσο και σε επίπεδο αλγορίθμων. Η ρευστή τοπολογία του δικτύου επηρεάζει την κάλυψη, την συνδεσιμότητα, την διανομή και την προώθηση των δεδομένων.

Το πρόβλημα της κάλυψης διατυπώνεται στο [5, ενότητα 3.2.2]. Οι υπάρχοντες αλγόριθμοι για βέλτιστη κάλυψη, όπως ο OGDC (Optimal Geographical Density Control), βασίζονται στο παραπάνω πρόβλημα με παραμέτρους όπως η διατήρηση της συνδεσιμότητας ανάμεσα στους κόμβους και η ποιότητα των παρεχόμενων δεδομένων από το δίκτυο WSN.

1.5.4 Συνάθροιση/Συμπίεση δεδομένων (data aggregation/compression)

Οι τεχνικές συνάθροισης και συμπίεσης δεδομένων (data aggregation/compression) αποσκοπούν στη μείωση του κόστους επικοινωνίας, στη βελτίωση της αξιοπιστίας της παρεχόμενης υπηρεσίας και στην εξοικονόμηση ενέργειας στο δίκτυο. Με τον όρο συνάθροιση δεδομένων εννοούμε το συνδυασμό δεδομένων, προερχόμενων από πολλαπλούς αισθητήριους κόμβους, σε ένα κόμβο του δικτύου WSN. Η τεχνική συνάθροισης δεδομένων χρησιμοποιείται σε πρωτόκολλα

δρομολόγησης, με συχνότερη εφαρμογή σε βασισμένα στην ομαδοποίηση κόμβων (cluster-based) πρωτόκολλα. Η τεχνική συμπίεσης δεδομένων, περιλαμβάνει τη διαδικασία συμπίεσης του μεγέθους των δεδομένων στον αισθητήριο κόμβο και εν συνεχεία αποσυμπίεσης, η οποία λαμβάνει χώρα στο σταθμό βάσης.

1.5.5 Ασφάλεια

Η ασφάλεια αποτελεί κρίσιμο αντικείμενο στη σχεδίαση ενός δικτύου WSN, καθώς σε πολλές εφαρμογές θεωρείται σημαντική η αντιμετώπιση καταστάσεων, όπως το ρίσκο ακεραιότητας δεδομένων, οι υποκλοπές και παρεμβολές μεταδιδόμενης πληροφορίας, η είσοδος στο σύστημα μετάδοσης ψεύτικων μηνυμάτων πληροφορίας και η απώλεια πόρων του δικτύου. Τα ζητήματα ασφαλείας θα είχαν μικρότερη κρισιμότητα, εάν δεν υπήρχαν οι περιοριστικοί παράγοντες του δικτύου, οι οποίοι αφορούν σε δυνατότητες επικοινωνίας, υπολογισμών, επεξεργασίας, αποθήκευσης δεδομένων και ενέργειας.

Η εξασφάλιση αξιόπιστης λειτουργίας του δικτύου και η αντιμετώπιση πιθανών επιθέσεων υλοποιείται με την ανάπτυξη αλγορίθμων αυθεντικοποίησης και κρυπτογράφησης, οι οποίοι όμως επιβαρύνουν το δίκτυο ως προς τη κατανάλωση ενέργειας και το διαθέσιμο εύρος ζώνης της υπηρεσίας.

1.5.6 Ανοχή Σφαλμάτων (Fault Tolerance)

Σε ένα δίκτυο WSN με μεγάλο αριθμό κόμβων είναι πιθανό κάποιοι κόμβοι να οδηγηθούν σε σφάλματα (απώλεια ή αλλοίωση πακέτων δεδομένων). Παράγοντες που οδηγούν σε σφάλματα είναι η έλλειψη ενέργειας, η φυσική καταστροφή κόμβων, παρεμβολές από γειτονικούς κόμβους και δυσμενείς συνθήκες περιβάλλοντος. Η αξιοπιστία του δικτύου πρέπει να διασφαλίζεται με την ανοχή τέτοιου είδους σφαλμάτων (fault tolerance), δηλαδή η λειτουργία του δικτύου θα πρέπει να παραμένει ανεπηρέαστη από σφάλματα. Εάν αυτά εμφανιστούν σε κάποιο κρίσιμο αριθμό κόμβων, είναι αναγκαία η μέριμνα των πρωτοκόλλων MAC (Multiple Access Control) και των πρωτοκόλλων δρομολόγησης, ώστε να καθορίσουν νέες ζεύξεις και διαδρομές δρομολόγησης για τη μετάδοση και προώθηση των δεδομένων στο σταθμό βάσης. Το κατά πόσο μια σχεδίαση οφείλει να είναι ανεκτική σε σφάλματα είναι άρρηκτα συνδεδεμένο με το είδος της εφαρμογής και το επιθυμητό επίπεδο παρεχόμενης αξιοπιστίας.

1.5.7 Δυνατότητα κλιμάκωσης - Επεκτασιμότητα (Scalability)

Χαρακτηριστικό των δικτύων WSN είναι το μεγάλο πλήθος κόμβων, οι οποίοι μπορεί να είναι εκατοντάδες, χιλιάδες ή και περισσότεροι. Τα εφαρμοζόμενα πρωτόκολλα σε κάθε εφαρμογή οφείλουν να είναι σε θέση να διαχειρίζονται τόσο το μεγάλο πλήθος κόμβων, όσο και τη μεγάλη χωρική πυκνότητα που ενδεχομένως μπορεί να εμφανίζουν.

1.5.8 Ποιότητα της υπηρεσίας (Quality of Service – QoS)

Ο όρος QoS αποτελεί ένα μέτρο της ποιότητας υπηρεσίας, η οποία παρέχεται από το δίκτυο WSN στο τελικό χρήστη. Ο τελικός χρήστης καθορίζει κάποιες σχεδιαστικές απαιτήσεις ποιότητας του δικτύου και το δίκτυο παρέχει τα χαρακτηριστικά ποιότητας που έχει τις δυνατότητες να προσφέρει.

Τα δομικά στοιχεία ενός δικτύου οφείλουν να καλύπτουν τις απαιτήσεις ποιότητας, κάτι που αποτελεί μέριμνα του σχεδιαστή του δικτύου. Ειδικότερα σε δίκτυα WSN, οι απαιτήσεις ποιότητας μπορούν να επικεντρώνονται σε θέματα ακρίβειας δεδομένων, καθυστέρησης μετάδοσης, συνάθροισης δεδομένων, ανοχή σφαλμάτων και κατανάλωσης ενέργειας. Σημαντικές προκλήσεις που τίθενται σε ένα δίκτυο WSN και αφορούν στη ποιότητα της υπηρεσίας είναι οι ακόλουθες:

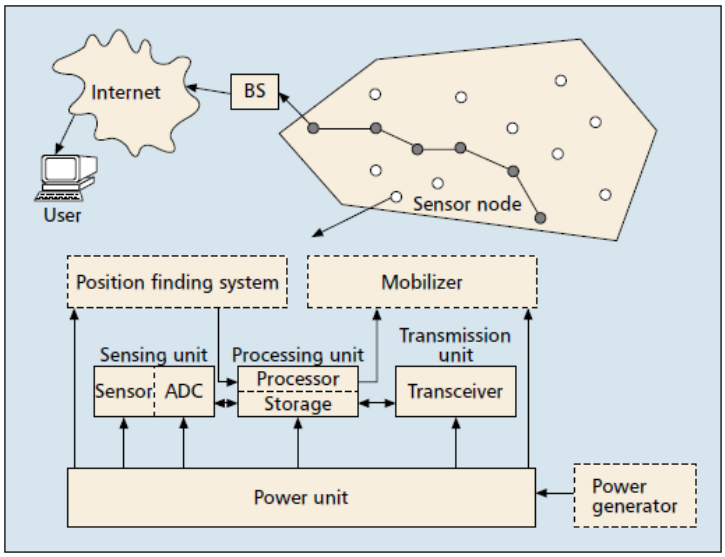
- Οι περιορισμοί πόρων δικτύου, οι οποίοι αφορούν στην ενέργεια, στο εύρος ζώνης και στις δυνατότητες αποθήκευσης, επεξεργασίας και επικοινωνίας των κόμβων.
- Η πλεονάζουσα πληροφορία, η οποία οφείλεται στη δομή του δικτύου. Συγκεκριμένα, οι κόμβοι βρίσκονται εγκατεστημένοι στο χώρο σε μεγάλη πυκνότητα, με αποτέλεσμα να είναι σύνηθες πληροφορία που παράγεται από ορισμένους κόμβους να πλεονάζει. Η πλεονάζουσα πληροφορία αν και προσδίδει στο δίκτυο μεγαλύτερη αξιοπιστία και ανοχή σε σφάλματα, ταυτόχρονα οδηγεί σε μεγαλύτερη κατανάλωση ενέργειας, και ως εκ τούτου, σε μείωση χρόνου ζωής των κόμβων. Το θέμα της πλεονάζουσας πληροφορίας επιλύεται με τεχνικές συνάθροισης (data aggregation) και συγχώνευσης (data fusion) δεδομένων.
- Η ανομοιομορφία των αισθητήριων κόμβων σε εφαρμογές, όπου απαιτούνται διαφορετικά αισθητήρια όργανα στους κόμβους για την παρακολούθηση διαφορετικών μεγεθών (π.χ. θερμοκρασία, υγρασία, κίνηση κτλ.). Επιπλέον, η ανομοιογένεια προέρχεται και από τον τρόπο που παρακολουθείται το επιτηρούμενο περιβάλλον από τους αισθητήρες. Συγκεκριμένα, κάποιοι αισθητήρες αποστέλλουν

συνεχώς δεδομένα στο σταθμό βάσης, και άλλοι να αποστέλλουν στιγμιαία, όταν λάβουν μια κρίσιμη μέτρηση.

- Η δυναμική τοπολογία του δικτύου, η οποία αφορά στη μεταβολή της τοπολογίας είτε λόγω απωλειών κόμβων, είτε λόγω αποτυχίας μιας ζεύξης. Για το λόγο αυτό οι κόμβοι πρέπει να έχουν δυνατότητα αυτό-οργάνωσης και να είναι προσαρμόσιμοι σε ένα δυναμικό περιβάλλον, του οποίου οι μεταβολές δεν πρέπει να επηρεάζουν δραστικά τη λειτουργία του δικτύου.
- Το αναξιόπιστο μέσο μετάδοσης σε ένα ασύρματο δίκτυο μπορεί να προκαλέσει ζητήματα μείωσης της ποιότητας, εξαιτίας μείωσης της αξιοπιστίας του από δυσμενείς παράγοντες μετάδοσης του διαύλου, όπως θόρυβος και παρεμβολές.
- Η διαχείριση πολλαπλών σταθμών βάσης είναι πρόκληση σε θέματα διασφάλισης ποιότητας της υπηρεσίας και το δίκτυο πρέπει να είναι σε θέση να υποστηρίζει διαφοροποιημένα επίπεδα QoS σε περίπτωση δικτύων με πολλά τερματικά.

1.6 Δομή κόμβων δικτύου WSN

Οι κόμβοι ενός δικτύου WSN είναι διατάξεις, οι οποίες έχουν τη δυνατότητα να επικοινωνήσουν με άλλες παρόμοιες διατάξεις, να εκτελέσουν επεξεργασία δεδομένων (ενσωμάτωση επεξεργαστή) και να λάβουν αποφάσεις με τη χρήση δεδομένων, τα οποία είτε τα συλλέγουν οι ίδιοι, είτε παρέχονται από το υπόλοιπο δίκτυο.



Σχήμα 1.3. Διάγραμμα τυπικής δομής κόμβου δικτύου WSN

Ένα τυπικό σύστημα κόμβου δικτύου WSN είναι ένας ολοκληρωμένος (integrated) αισθητήρας, ο οποίος συγκροτείται από επιμέρους υποσυστήματα (Σχήμα 1.3). Τα υποσυστήματα αυτά είναι τα παρακάτω:

- Το υποσύστημα αισθητήρων (sensing unit), το οποίο αποτελεί τον μετατροπέα (transducer ή sensor) εισόδου, ο οποίος είναι η διάταξη που μετατρέπει σήματα από το περιβάλλον (π.χ. μηχανικά, μαγνητικά, θερμικά κτλ.) σε ηλεκτρικά, δίνοντας τους την καταλληλότητα για ηλεκτρονική επεξεργασία. Το υποσύστημα αισθητήρων περιλαμβάνει επιπλέον την ενίσχυση και την μετατροπή του σήματος από αναλογικό σε ψηφιακό (A/D Conversion) πριν την επόμενη διεργασία, η οποία λαμβάνει χώρα στο υποσύστημα επεξεργασίας.
- Το υποσύστημα επεξεργασίας (processing unit), το οποίο αποτελεί τη μονάδα επεξεργασίας (processor) και αποθήκευσης (storage) δεδομένων. Στο υποσύστημα αυτό πραγματοποιείται η διαχείριση και η επεξεργασία του ψηφιακού σήματος. Ο επεξεργαστής ελέγχει μια σειρά άλλων κυκλωμάτων, τα οποία τροφοδοτούν το μετατροπέα εξόδου ή ενεργοποιητή (actuator). Ο ρόλος του ενεργοποιητή είναι η μετατροπή του ηλεκτρικού σήματος σε μια μορφή αντιληπτή από τις ανθρώπινες αισθήσεις ή η ενεργοποίηση κάποιας δράσης (άνοιγμα - κλείσιμο κάποιου άλλου συστήματος, μεταβολή θέσης κτλ). Επιπρόσθετα, το υποσύστημα μπορεί να ελέγχει ένα σύστημα ανίχνευσης θέσης (position finding system) ή ένα μηχανισμό κίνησης (mobilizer), εάν η κινητικότητα των κόμβων είναι επιθυμητή.
- Το υποσύστημα επικοινωνιών (transmission unit), το οποίο αποτελείται από διατάξεις αμφίδρομης ασύρματης επικοινωνίας, δηλαδή έναν πομποδέκτη RF και μία κεραία. Το υποσύστημα αυτό έχει τη μεγαλύτερη κατανάλωση ενέργειας στο σύστημα του κόμβου, επηρεάζοντας σε μεγαλύτερο βαθμό ζητήματα εξοικονόμησης ενέργειας.
- Το υποσύστημα τροφοδοσίας (power unit), το οποίο αποτελείται συνηθέστερα από ένα συσσωρευτή ξηρών στοιχείων ή εναλλακτικά από μονάδα μετατροπής ηλιακής ενέργειας σε ηλεκτρική (με χρήση PV cells). Η χρήση και των δύο τρόπων τροφοδοσίας είναι επιπλέον λύση με τη χρήση PV κυττάρων για φόρτιση των ξηρών στοιχείων (power generator).

Οι κόμβοι WSN ενσωματώνουν λειτουργικά συστήματα (operating systems - OS), τα οποία είναι ειδικά ανεπτυγμένα για τις πλατφόρμες αυτές. Ο σχεδιασμός των λειτουργικών συστημάτων για αισθητήριους κόμβους έγινε με κύριους άξονες την

διαχείριση και απόκριση σε πραγματικό χρόνο λειτουργιών, όπως η λήψη των ερεθισμάτων από τους αισθητήρες, η επεξεργασία και η δρομολόγηση των δεδομένων. Απαίτηση επίσης είναι να μην εξαρτάται το λειτουργικό σύστημα από το υλικό και να δίνει τη δυνατότητα στον χρήστη να επέμβει με ευκολία στις παραμέτρους λειτουργίας ώστε να τις μεταβάλλει ανάλογα με τις απαιτήσεις της εφαρμογής.

Από πλευράς υλικού, οι επικοινωνίες υλοποιούνται από ολοκληρωμένα κυκλώματα RF τεχνολογίας CMOS, είτε ανεξάρτητα πάνω στο board (όπως στα MicaZ, Telos από τη MEMSIC) είτε ενσωματωμένα στο μικροελεγκτή της πλατφόρμας. (όπως στο IRIS). Η επικρατούσα τάση είναι η δημιουργία SoC (System on Chip), η ολοκλήρωση δηλαδή όλων των διατάξεων σε ένα Chip, το οποίο εκτελεί όλες τις λειτουργίες του mote, ενώ περιορίζει τις καταναλώσεις (λιγότερες απώλειες). Η κεραία των πομποδεκτών τείνει επίσης να είναι ενσωματωμένη (τυπωμένη) στην πλακέτα του συστήματος, ενώ δίνεται η δυνατότητα όπως αναφέρθηκε προηγουμένως για εξωτερική επέκταση. Τα κυκλώματα αυτά περιλαμβάνουν και τις διατάξεις διαμόρφωσης/αποδιαμόρφωσης του σήματος.

1.7 Διαδραστική λειτουργία δικτύων WSN

Τα δίκτυα WSN είναι δομημένα με σχεδιαστικούς άξονες την χαμηλή πολυπλοκότητα, την χαμηλή κατανάλωση ενέργειας και την δυνατότητα δικτύωσης μεγάλου πλήθους αυτόνομων συσκευών. Το πρότυπο IEEE 802.15.4 ικανοποιεί αυτές τις επιδιώξεις, λειτουργώντας συμπληρωματικά προς τις άλλες WPAN τεχνολογίες. Με το πρότυπο IEEE 802.15.4 έγινε δυνατή η υλοποίηση εφαρμογών που παλιότερα θεωρούνταν μη πρακτικές ή είχαν μεγάλο κόστος.

Η μεγιστοποίηση της αυτονομίας στις συσκευές του δικτύου επιτυγχάνεται με βάση την υπόθεση, ότι ο όγκος των δεδομένων είναι μικρός και η εκπομπή τους γίνεται ακανόνιστα με διατήρηση μικρού κύκλου λειτουργίας (duty cycle). Επιπρόσθετα, η δομή των πακέτων σχεδιάστηκε, ώστε οι πληροφορίες που αφορούν την δρομολόγηση (overhead) να είναι οι ελάχιστες δυνατές σε σχέση με τα φορτίο των δεδομένων που μεταφέρονται.

Τα χαρακτηριστικά αυτά έρχονται σε ευθεία αντίθεση με αυτά των προτύπων WLAN. Στα πρότυπα 802.11 η βαρύτητα δίνεται στην επίτευξη μεγάλων ρυθμών μετάδοσης δεδομένων, ενώ ζητήματα κόστος και πολυπλοκότητας συσκευών έρχεται σε δεύτερη μοίρα. Επιπλέον, η απόδοση διευθύνσεων IP σε κάθε συσκευή και το

μεγάλο overhead στα δεδομένα αυξάνουν τη πολυπλοκότητα μιας υλοποίησης μεγάλης κλίμακας, όπως τα δίκτυα WSN.

Οι θεμελιώδεις διαφοροποιήσεις μεταξύ LR-WPAN και WLAN δικτύων περιπλέκουν την μεταξύ τους επικοινωνία. Κάθε δίκτυο που επιδιώκει να συνδεθεί με το Internet, πρέπει να λειτουργήσει διαδραστικά με το Internet Protocol (IP). Επίσης, υπάρχει η περίπτωση σε κάποιο δίκτυο WSN να είναι επιθυμητή η εκμετάλλευση δυνατοτήτων και χαρακτηριστικών ενός IP based δικτύου. Γίνεται φανερό, ότι για την παραγωγή ολοκληρωμένων λύσεων δικτύων WSN είναι αναγκαία η ευελιξία στον συνδυασμό χαρακτηριστικών και πρωτοκόλλων.

Στα ομογενή δίκτυα WSN η συλλογή δεδομένων γίνεται από όλους τους κόμβους, ίδιων επεξεργαστικών δυνατοτήτων, οι οποίοι μεταβιβάζουν τις συλλεγόμενες πληροφορίες σε έναν τελικό αποδέκτη (π.χ. ένα φορητό υπολογιστή). Η ενσωμάτωση σε ένα δίκτυο WSN επιπλέον δυνατοτήτων multimedia παρουσιάζει αυξημένες απαιτήσεις σε εύρος ζώνης, ενέργεια και αποθηκευτικό χώρο. Για παράδειγμα, η τεχνολογία Zigbee με μέγιστο ρυθμό μετάδοσης τα 250 kbps δεν μπορεί να ανταποκριθεί σε video streaming από μια π.χ. θερμική κάμερα. Αντίθετα, σε ένα δίκτυο WiFi δίνεται η δυνατότητα χρήσης απαιτητικών κόμβων πολυμέσων, καθώς οι ταχύτητες μετάδοσης που καθορίζει το πρωτόκολλο IEEE 802.11 είναι της τάξης των Mbps.

Κατά συνέπεια, οι δυνατότητες ενός δικτύου WSN μπορούν να διευρυνθούν μέσω της διάδρασης του με άλλα δίκτυα δομημένα πάνω σε διαφορετικά πρότυπα. Η επικοινωνία μεταξύ διαφορετικών δικτύων προϋποθέτει την ύπαρξη συσκευών στις οποίες πραγματοποιείται η μετατροπή των δεδομένων (δομή των πακέτων) από το ένα πρότυπο επικοινωνίας σε ένα άλλο, οι οποίοι ονομάζονται κόμβοι πύλες (gateways). Οι περισσότερες πύλες είναι είτε ενσωματωμένες σε κάποιο σύστημα Η/Υ, είτε ανεξάρτητες συσκευές αποκλειστικής χρήσης (dedicated). Ένας κόμβος του δικτύου WSN συνδεδεμένος με ένα φορητό υπολογιστή μέσω USB, με τη προϋπόθεση ότι ο Η/Υ διαθέτει τον απαραίτητο εξοπλισμό (ethernet, wifi, προσαρμογέα για mobile data) για σύνδεση με το Internet, είναι κόμβος πύλη. Παράλληλα ο Η/Υ διαθέτει την επεξεργαστική ισχύ και τις απεικονιστικές δυνατότητες για την αξιοποίηση του ως σταθμό βάσης. Από την άλλη πλευρά, οι αποκλειστικής χρήσης συσκευές είναι απλούστερες στη δομή τους, έχουν πολύ μικρότερο μέγεθος και κόστος και απαιτούν συγκριτικά πολύ λιγότερη ενέργεια σε σχέση με έναν Η/Υ. Σε ένα κόμβο πύλη περιλαμβάνεται ένας ραδιοπομπός, ένας

επεξεργαστής περιορισμένων δυνατοτήτων και μία διάταξη επικοινωνίας με το έτερο δίκτυο. Η ρύθμιση του γίνεται μέσω web browser ή άλλου τύπου απομακρυσμένης σύνδεσης και είναι δυνατή η σταθερή λειτουργία τους (δεν απαιτείται επανεκκίνηση) για μεγάλες χρονικές περιόδους.

Ένα ομογενές δίκτυο WSN μπορεί να αποστέλλει τα δεδομένα που συγκεντρώνει σε ένα Η/Υ, ο οποίος ταυτόχρονα είναι συνδεδεμένος μέσω WiFi με ένα σύστημα WMSN (Wireless Multimedia Sensor Network), επιτελώντας τον ρόλο του κόμβου πύλης. Ταυτόχρονα, μέσω του συστήματος Η/Υ γίνεται επεξεργασία και αποθήκευση των δεδομένων. Έπειτα από δεδομένο - κεντρική επεξεργασία εντός του δικτύου (data-centric in-network processing), τα αποτελέσματα συλλέγονται από το κόμβο πύλη και παρουσιάζονται στο χρήστη. Αυτή η προσέγγιση παρουσιάζει το μειονέκτημα του μεγάλου όγκου δεδομένων, ο οποίος δρομολογείται από τους κόμβους που γειτνιάζουν του κόμβου πύλη με συνέπεια τη γρήγορη ενεργειακή εξάντληση τους. Μία άλλη προσέγγιση είναι η ανάπτυξη περισσότερων του ενός κόμβων πυλών εντός του δικτύου WSN. Σε αυτή τη περίπτωση υπάρχει μια πιο ομοιόμορφη κατανομή της ενεργειακής κατανάλωσης στους κόμβους του δικτύου, με τη προϋπόθεση ότι η βαρύτητα των ερωτημάτων (όσον αφορά τα απαιτούμενα στοιχεία) είναι επίσης όμοια κατανεμημένη.

Τα ετερογενή δίκτυα (ύπαρξη κόμβων με αυξημένες δυνατότητες) επιτρέπουν την απόδοση διεύθυνσης IP στους πιο ικανούς κόμβους του δικτύου. Γενικά, οι πιο ικανοί κόμβοι μπορούν να εκτελέσουν περισσότερες εργασίες και συνολικά να επωμιστούν μεγάλο μέρος των εργασιών που επιτελούνται στο δίκτυο. Υπάρχουν και άλλοι λόγοι που υπαγορεύουν την διευθυνσιοδότηση τέτοιων κόμβων. Για παράδειγμα, στην περίπτωση κόμβων με ρόλο ενεργοποιητή (έλεγχος συσκευών , ρομποτικών μηχανισμών ή άλλων δράσεων) είναι χρήσιμη η απόδοση διευθύνσεων για ευκολότερη ανάθεση εργασιών. Σε άλλη εκδοχή δικτύου, οι κόμβοι με IP διευθύνσεις μπορούν να λειτουργούν σαν επικεφαλής ομάδων κόμβων. Στη περίπτωση αυτή είναι δυνατή η δόμηση ενός επικαλυπτικού IP δικτύου πάνω στο υφιστάμενο δίκτυο.

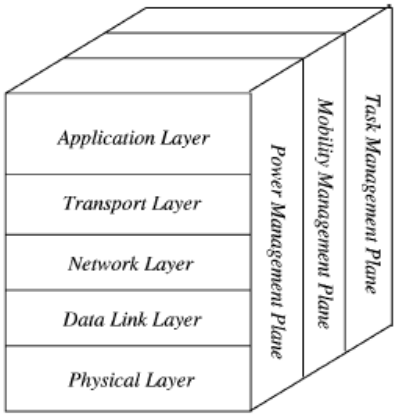
Κεφάλαιο 2

Αρχιτεκτονική – Πρότυπα Δικτύων WSN

2.1 Εισαγωγή

Η αρχιτεκτονική ενός ασύρματου δικτύου αισθητήρων βασίζεται στο μοντέλο αναφοράς OSI (μοντέλο αναφοράς ανοικτής διασύνδεσης συστημάτων – Open Systems Interconnection), γνωστό και ως μοντέλο επτά επιπέδων (φυσικό, ζεύξης και μετάδοσης δεδομένων, δικτύου, μεταφοράς, συνδιάλεξης, παρουσίασης και εφαρμογής) [11]. Το μοντέλο OSI αναπτύχθηκε μετά από πρόταση του Διεθνούς Οργανισμού Τυποποίησης (International Standards Organization – ISO) με στόχο τη διεθνή τυποποίηση των πρωτοκόλλων που χρησιμοποιούνται στα επίπεδα σχεδίασης των δικτύων. Τα επίπεδα του μοντέλου υλοποιούν τη κατακόρυφη στοίβα επιπέδων, τα οποία γειτνιάζουν και είναι αλληλοεξαρτώμενα. Κάθε επίπεδο αξιοποιεί τις λειτουργίες του κατώτερου του και ταυτόχρονα παρέχει λειτουργικότητα στο αμέσως ανώτερο του.

Σε ένα δίκτυο WSN δεν υλοποιούνται τα επίπεδα παρουσίασης και συνδιάλεξης του μοντέλου OSI, αλλά το μοντέλο που εφαρμόζεται περιλαμβάνει τα υπόλοιπα πέντε επίπεδα σχεδίασης καθώς και τρία διασταυρούμενα επίπεδα (cross layers/planes), όπως απεικονίζονται στο Σχήμα 2.1.



Σχήμα 2.1. Το μοντέλο αρχιτεκτονικής WSN

Η ύπαρξη των διασταυρούμενων επιπέδων (cross layers) αποσκοπεί στη διαχείριση του δικτύου, ώστε οι αισθητήριοι κόμβοι να συνεργάζονται με στόχο τη μεγιστοποίηση της αποδοτικότητας και του χρόνου λειτουργίας του δικτύου. Όπως παρουσιάζονται στο Σχήμα 2.1 τα διασταυρούμενα επίπεδα είναι το επίπεδο διαχείρισης ενέργειας (power management plane), το επίπεδο διαχείρισης

φορητότητας (mobility management plane) και το επίπεδο διαχείρισης λειτουργιών (task management plane).

Η λειτουργία ενός ασύρματου δικτύου αισθητήρων καθορίζεται από τα πρωτόκολλα επικοινωνίας που εφαρμόζονται σε καθένα από τα πέντε επίπεδα του μοντέλου WSN και αποτελούν τη στοίβα πρωτοκόλλων (protocol stack) του δικτύου. Η εφαρμοζόμενη στοίβα πρωτοκόλλων επικοινωνίας πρέπει να είναι ενεργειακά αποδοτική και να υποστηρίζει τη συνεργασία μεγάλου πλήθους κόμβων.

2.2 Επίπεδο εφαρμογής (application layer)

Το επίπεδο εφαρμογής παρέχει το λογισμικό της εφαρμογής, το οποίο είναι απαιτούμενο για να μορφοποιήσει τα δεδομένα σε μια κατανοητή μορφή για τον χειριστή, και ποικίλει αναλόγως των απαιτήσεων της εφαρμογής (π.χ. στρατιωτικής, ιατρικής, περιβαλλοντικής κλπ). Στο επίπεδο εφαρμογής τα πακέτα δεδομένων αναφέρονται ως μηνύματα (messages).

Οι στόχοι που πρέπει να υλοποιούνται από το πρωτόκολλο του επιπέδου εφαρμογής κινούνται σε δύο άξονες. Στο πρώτο, τίθεται το ερώτημα του τρόπου αποστολής εντολών ελέγχου από το σταθμό βάσης προς τους κόμβους του δικτύου (downlink), και στο δεύτερο τίθεται το ερώτημα της αντίστροφης αποστολής δεδομένων από τους κόμβους του δικτύου προς το σταθμό βάσης. Δηλαδή, το επίπεδο εφαρμογής ορίζει τον τρόπο με τον οποίο ανταλλάσσουν μηνύματα τα δύο τερματικά συστήματα (σταθμός βάσης και κόμβοι) κατά τις διεργασίες της εφαρμογής. Αναλυτικά πρέπει να ορίζονται (α) οι τύποι των μηνυμάτων που ανταλλάσσονται, (β) η σύνταξη των μηνυμάτων (πεδία εντός των μηνυμάτων και διάκριση μεταξύ τους), (γ) η σημασία των πεδίων εντός των μηνυμάτων και (δ) ο καθορισμός για το πότε μια διεργασία λαμβάνει ή αποστέλλει μηνύματα.

2.3 Επίπεδο μεταφοράς (transport layer)

Το επίπεδο μεταφοράς παρέχει στο δίκτυο αξιοπιστία, ανεξαρτήτως του επιπέδου αξιοπιστίας που παρέχει το υφιστάμενο δίκτυο, και ενεργεί προς τη κατεύθυνση αποφυγής συμφόρησης δεδομένων. Κατά την αποστολή, το επίπεδο μεταφοράς μετατρέπει τα μηνύματα που δέχεται από το επίπεδο εφαρμογής σε τμήματα δεδομένων (segments). Η μετατροπή αυτή γίνεται με διαίρεση των μηνυμάτων σε μικρότερα κομμάτια και προσθήκη σε αυτά επικεφαλίδων επιπέδου μεταφοράς. Στη συνέχεια, στο επίπεδο δικτύου το τμήμα δεδομένων ενσωματώνεται

σε ένα μεγαλύτερο πακέτο δεδομένων (δεδομενόγραμμα) και αποστέλλεται. Κατά τη λήψη, το επίπεδο δικτύου εξάγει το τμήμα δεδομένων από το δεδομενόγραμμα και το μεταβιβάζει προς το επίπεδο μεταφοράς, το οποίο το επεξεργάζεται και απομονώνει τα μηνύματα δεδομένων προωθώντας τα στο επίπεδο εφαρμογής. Το υλικό και το λογισμικό που συνθέτουν τις λειτουργίες του επιπέδου μεταφοράς καλούνται οντότητα μεταφοράς (transport entity).

Τα πρωτόκολλα του επιπέδου μεταφοράς υλοποιούνται στα τερματικά συστήματα (σταθμούς βάσης) και μπορούν να προσφέρουν αξιόπιστη μεταφοράς δεδομένων στο επίπεδο εφαρμογής, ακόμα και αν το πρωτόκολλο του επιπέδου δικτύου δεν τη προσφέρει. Σε στρατιωτικές εφαρμογές, στις οποίες η αξιοπιστία είναι πρωταρχικής σημασίας, προέχει ο σχεδιαστής του δικτύου να κινηθεί προς τον άξονα χρήσης πρωτοκόλλου επιπέδου μεταφοράς, το οποίο να καλύπτει αυστηρές απαιτήσεις. Η επίτευξη αξιοπιστίας εξασφαλίζει ότι τα μεταφερόμενα ψηφία δεδομένων δεν αλλοιώνονται, δεν χάνονται και παραδίδονται όλα με τη σειρά που στάλθηκαν. Η απώλεια πακέτων μπορεί να συμβεί εξαιτίας διαφόρων αστοχιών του δικτύου, οι οποίες μπορεί να είναι η μη αξιόπιστη επικοινωνία κόμβων, η συμφόρηση ή σύγκρουση πακέτων, η εξάντληση της χωρητικότητας μνήμης των κόμβων και οι αποτυχίες κόμβων. Κάθε απώλεια πακέτου έχει αρνητικό αντίκτυπο στην ποιότητα της υπηρεσίας (QoS) και στην εξοικονόμηση ενέργειας.

Για την επίτευξη της απαιτούμενης αξιοπιστίας του δικτύου αποδίδεται κυρίαρχη σημασία στην ανίχνευση απώλειας πακέτου δεδομένων, και εν συνεχεία στην επανάκτηση του πακέτου. Όσον αναφορά τη πρώτη λειτουργία χρησιμοποιούνται οι μηχανισμοί ACK και NACK, ενώ για τη δεύτερη χρησιμοποιούνται οι τεχνικές End to End και Hop by Hop. Στη χρησιμοποίηση των τεχνικών End to End και Hop by Hop υπάρχουν tradeoffs και καθεμία ενδείκνυται αναλόγως των χαρακτηριστικών της εφαρμογής (τύπος εφαρμογής, απαιτούμενη αξιοπιστία, ευαισθησία σε καθυστερήσεις). Στη τεχνική Hop by Hop κάθε ενδιάμεσος κόμβος αποθηκεύει προσωρινά το πακέτο δεδομένων που προωθεί για να το επαναπροωθήσει σε περίπτωση απώλειας του. Η απαίτηση αυτή δεν υπάρχει στη τεχνική End to End, στην οποία το πακέτο δεδομένων αποθηκεύεται στον αισθητήριο κόμβο, που είναι πηγή της πληροφορίας. Η τεχνική Hop by Hop επαναπροωθεί πακέτα μέσω λιγότερων κόμβων και χρειάζεται μικρότερη απόσταση εκ νέου αποστολής του πακέτου που χάθηκε, και ως εκ τούτου είναι αποδοτικότερος ως προς

την εξοικονόμηση ενέργειας. Το γεγονός αυτό καθιστά τη τεχνική Hop by Hop ελκυστικότερη σε εφαρμογές δικτύων WSN.

Ο έλεγχος και η ανίχνευση συμφόρησης δεδομένων οδηγούν το δίκτυο WSN προς τη κατεύθυνση εξοικονόμησης ενέργειας με τη μείωση απωλειών πακέτων και κατ' επέκταση τη μείωση επανεκπομπών. Όταν ανιχνευθεί μία συμφόρηση δεδομένων σε ένα σημείο του δικτύου, η τεχνική Hop by Hop επηρεάζει τη συμπεριφορά όλων των γειτονικών κόμβων, με αποτέλεσμα τη ταχύτερη μείωση της συμφόρησης. Αντίθετα, η αποκατάσταση με βάση τη τεχνική End to End είναι καθήκον των τερματικών κόμβων, γεγονός που την καθιστά πιο χρονοβόρα.

Συνήθη πρωτόκολλα που χρησιμοποιούνται σε εφαρμογές WSN είναι τα STCP (Sensor Transmission Control Protocol) [17], PORT (Price-Oriented Reliable Transport Protocol) [18], PSFQ (Pump Slowly, Fetch Quickly) [19], GARUDA [20], DST (Delay Sensitive Transport) [21], ESRT (Price-Oriented Reliable Transport Protocol) [22] και CODA (Congestion Detection and Avoidance) [23].

Το πρωτόκολλο STCP (Sensor Transmission Control Protocol) [17] υποστηρίζει επεκτασιμότητα και αξιοπιστία στην upstream ζεύξη. Προσφέρει στο δίκτυο ευελιξία στο καθορισμό επιπέδου αξιοπιστίας της υπηρεσίας, ανίχνευση και αποφυγή συμφόρησης δεδομένων. Η πλειονότητα των διεργασιών του πρωτοκόλλου λαμβάνει χώρα στο σταθμό βάσης του δικτύου. Το πρωτόκολλο υποστηρίζει τόσο δεδομένα συνεχής ροής όσο και event-driven ροές δεδομένων.

Το πρωτόκολλο PORT (Price-Oriented Reliable Transport Protocol) [18] είναι ένα downstream πρωτόκολλο, το οποίο παρέχει το αναγκαίο επίπεδο αξιοπιστίας, εξοικονομώντας ενέργεια και προσδίδοντας στο δίκτυο μηχανισμούς αποφυγής συμφόρησης δεδομένων. Το πρωτόκολλο PSFQ (Pump Slowly, Fetch Quickly) [19] είναι επίσης ένα downstream εύρωστο πρωτόκολλο, το οποίο υποστηρίζει αξιοπιστία και επεκτασιμότητα του δικτύου. Βασικοί στόχοι του πρωτοκόλλου είναι (α) η εξασφάλιση μετάδοσης των τμημάτων δεδομένων σε όλους τους προορισμούς εντός του δικτύου, (β) η ελαχιστοποίηση εκπομπών κατά την ανίχνευση και αποκατάσταση απωλειών πακέτων, (γ) η αξιοπιστία του δικτύου ακόμα και στη περίπτωση που το περιβάλλον ζεύξης δε την ευνοεί και (δ) η παροχή ελαστικών χρονικών περιορισμών στη μετάδοση δεδομένων προς όλους τους προορισμούς εντός του δικτύου.

Το πρωτόκολλο GARUDA [20] παρέχει αξιόπιστη διακίνηση δεδομένων από το σταθμό βάσης προς τους κόμβους (point-to-multipoint κατεύθυνση). Το πρωτόκολλο GARUDA υποστηρίζει επεκτασιμότητα και ευελιξία όσον αφορά το

μέγεθος του δικτύου, τα χαρακτηριστικά των πακέτων, το ρυθμό απωλειών και το επίπεδο αξιοπιστίας. Το πρωτόκολλο DST (Delay Sensitive Transport) [21] βασίζεται σε δύο μηχανισμούς: (α) το μηχανισμό αξιόπιστης μεταφοράς της πληροφορίας που περιγράφει το συμβάν που ανίχνευσαν οι κόμβοι και (β) το μηχανισμό μεταφοράς της ίδιας πληροφορίας σε πραγματικό χρόνο. Αντικείμενο του πρωτοκόλλου είναι η έγκαιρη και αξιόπιστη μεταφορά δεδομένων από το σημείο ανίχνευσης του συμβάντος (αισθητήριοι κόμβοι), προς το σταθμό βάσης, με την ελάχιστη κατανάλωση ενέργειας. Οι κύριες λειτουργίες του πρωτοκόλλου DST εκτελούνται στο σταθμό βάσης, ο οποίος θεωρούμε ότι δεν έχει ενεργειακούς περιορισμούς, γεγονός που κινείται προς τη κατεύθυνση εξοικονόμησης ενέργειας στους κόμβους του δικτύου.

Το πρωτόκολλο ESRT (Event-to Sink Reliable Transport) [22] αποσκοπεί στην επίτευξη του συνδυασμού αξιόπιστης ανίχνευσης του συμβάντος και χαμηλής κατανάλωσης, στόχος που υλοποιείται με τη χρησιμοποίηση ενός μηχανισμού ελέγχου συμφόρησης. Ο κύριος όγκος των λειτουργιών του εκτελούνται στο σταθμό βάσης με σκοπό την εξοικονόμηση ενέργειας. Το πρωτόκολλο ESRT είναι ευέλικτο ως προς το απαιτούμενο επίπεδο αξιοπιστίας, αλλάζοντας τους μηχανισμούς του αναλόγως της επίτευξης ή μη των απαιτήσεων. Το πρωτόκολλο CODA (Congestion Detection and Avoidance) [23] αποσκοπεί στην ενεργειακά αποδοτική ανίχνευση και αποτροπή συμφορήσεων και είναι κατάλληλο για event-driven δίκτυα αισθητήρων. Τα παραπάνω επιτυγχάνονται με συνεχή παρακολούθηση του φορτίου των καναλιών επικοινωνίας.

Στον Πίνακα 2.1 γίνεται συνοπτική αναφορά των χαρακτηριστικών των πρωτοκόλλων που αναφέρθηκαν προηγουμένως όπως αυτά συνοψίζονται στο [2].

		STCP	PORT	GARUDA	CODA	DST	PSFQ	ESRT
Congestion	Congestion control	Yes	Yes	No	Yes	Yes	No	Yes
	Congestion detection	Buffer size	Node price and link-loss rates	–	buffer size and channel load	Buffer size and average node delay calculation	–	Buffer size
	Congestion mitigation	Traffic redirection or end-to-end rate adjustment	Traffic redirection or end-to-end rate adjustment	–	Drop packets or adjust sending rate at each node	End-to-end rate adjustment	–	End-to-end rate adjustment
Reliability	Direction	Sensor to sink	Sensor to sink	Sink to sensor	Sensor to sink	Sensor to sink	Sensor to sink	Sensor to sink
	Reliability measure	Packet reliability	Event information reliability	Packet and destination reliability	–	Event reliability	Packet reliability	Event reliability
	End-to-end/Hop-by-hop	End-to-end	–	Hop-by-hop	–	End-to-end	Hop-by-hop	End-to-end
	Packet recovery	Yes	No	Yes	–	No	Yes	No
	Cache	Yes	–	Yes	–	–	Yes	–
	ACK/NACK	ACK, NACK	–	NACK	ACK	–	NACK	–
Energy conservation		Yes	Yes	Yes	Yes	Yes	–	Yes

Πίνακας 2.1. Σύγκριση πρωτοκόλλων επιπέδου μεταφοράς [2]

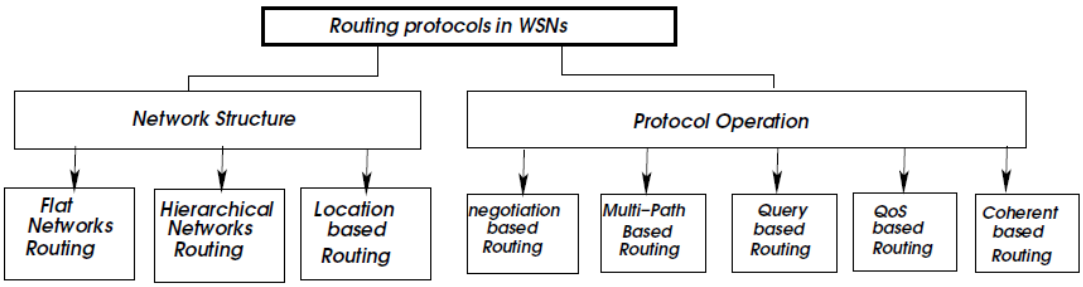
2.4 Επίπεδο δικτύου (network layer)

Η κυρίαρχη λειτουργία του επιπέδου δικτύου είναι η δρομολόγηση πακέτων δεδομένων με βασικές προκλήσεις την εξοικονόμηση ενέργειας, την αντιμετώπιση δυσχερειών λόγω περιορισμών μνήμης κόμβων και την απαίτηση δυνατότητας αυτό-οργάνωσης των κόμβων. Κατά την αποστολή, το επίπεδο δικτύου λαμβάνει τμήματα δεδομένων από το επίπεδο μεταφοράς, ενσωματώνει κάθε τμήμα μέσα σε ένα δεδομενόγραμμα, το οποίο αποστέλλεται στο κοντινότερο δρομολογητή. Κατά τη λήψη, το επίπεδο δικτύου λαμβάνει δεδομενογράμματα από τον πλησιέστερο δρομολογητή, εξάγει τα τμήματα δεδομένων και τα παραδίδει στο επίπεδο μεταφοράς.

Τα πρωτόκολλα επικοινωνίας του επιπέδου δικτύου ορίζουν ένα αξιόπιστο μονοπάτι δρομολόγησης των πακέτων καθώς και ένα αριθμό πλεοναζόντων μονοπατιών, με τρόπο που καθορίζει το κάθε πρωτόκολλο. Επιπλέον, διαφέρουν από τα πρωτόκολλα δρομολόγησης κλασικών εφαρμογών, καθώς στα δίκτυα WSN οι κόμβοι δε διαθέτουν IP (Internet Protocol) διεύθυνση και ως εκ τούτου δεν είναι δυνατή η χρήση IP-based πρωτοκόλλων. Η σχεδίαση των πρωτοκόλλων δρομολόγησης ενός WSN πρέπει να επικεντρώνεται στην διαχείριση επικοινωνίας πολυάριθμων κόμβων και τη διάδοση δεδομένων από αυτούς στο σταθμό βάσης, λαμβάνοντας υπόψη τους περιοριστικούς παράγοντες του δικτύου (περιορισμοί σε ενέργεια, μνήμη, εύρος ζώνης και υπολογιστικών δυνατοτήτων κόμβων). Με τον τρόπο αυτό, η διάρκεια ζωής του δικτύου αυξάνεται σημαντικά. Επιπλέον, ένα πρωτόκολλο δρομολόγησης πρέπει να εξετάζει ζητήματα ανοχής σφαλμάτων και ασφάλειας, ειδικά σε εφαρμογές που τα ζητήματα αυτά θεωρούνται κρίσιμης σημασίας.

Με βάση τη μέθοδο δρομολόγησης και τη δομή του δικτύου τα πρωτόκολλα του επιπέδου ταξινομούνται σε πρωτόκολλα επίπεδης δρομολόγησης (flat routing), πρωτόκολλα ιεραρχικής δρομολόγησης (hierarchal routing) και πρωτόκολλα δρομολόγησης βασισμένα στη θέση (location-based). Μια επιπλέον ταξινόμηση πρωτοκόλλων είναι με βάση τη λειτουργία τους σε πρωτόκολλα βασισμένα στη δρομολόγηση με διαπραγμάτευση (negotiation – based), στην πολυδιαδρομική δρομολόγηση (multipath-based), στη δρομολόγηση με αποστολή ερωτημάτων (query – based), στη βασισμένη στη ποιότητα υπηρεσίας δρομολόγηση (QoS – based) και στη βασισμένη στη συνεργατική λειτουργία των κόμβων δρομολόγηση (coherent – based), όπως απεικονίζεται στο Σχήμα 2.2. Τέλος, τα πρωτόκολλα δρομολόγησης μπορούν να χαρακτηριστούν ως αντιδραστικά (reactive), προληπτικά (proactive) και

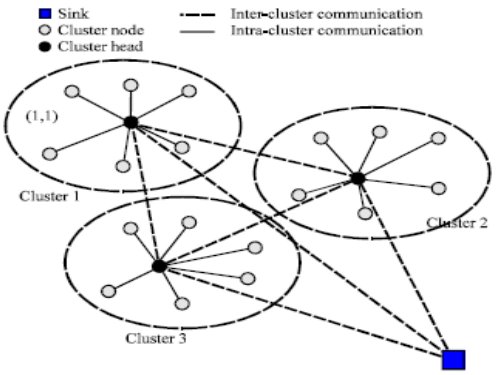
υβριδικά (hybrid), ανάλογα με τον τρόπο που μια πηγή πληροφορίας βρίσκει το δρομολόγιο προς το τελικό προορισμό. Ένα προληπτικό πρωτόκολλο προβλέπει αυτό το δρομολόγιο ακόμα και αν δεν υπάρχει ζήτηση, κρατώντας περιοδικά πίνακες δρομολόγησης, ένα αντιδραστικό ορίζει το δρομολόγιο μόλις καταστεί ανάγκη και το υβριδικό αποτελεί συνδυασμό των παραπάνω.



Σχήμα 2.2. Ταξινόμηση πρωτοκόλλων δρομολόγησης WSN [32]

Στην επίπεδη δρομολόγηση, που συχνά αναφέρεται ως δεδομένο – κεντρική δρομολόγηση, οι κόμβοι του δικτύου WSN δεν ομαδοποιούνται αλλά επιτελούν τις ίδιες λειτουργίες έχοντας ίδια καθήκοντα. Προορισμός της πληροφορίας που συλλέγεται από τους αισθητήριους κόμβους είναι ο σταθμός βάσης, στον οποίο δρομολογούνται τα πακέτα μέσω όμοιων κόμβων. Η ιεραρχική δρομολόγηση ενός δικτύου WSN στηρίζεται στην ομαδοποίηση των κόμβων με σκοπό τη κλιμάκωση του δικτύου. Δομικά στοιχεία ενός βασισμένου σε ιεραρχική δρομολόγηση δικτύου WSN είναι (α) οι αισθητήριοι κόμβοι (sensor nodes), (β) οι ομάδες (clusters), (γ) οι επικεφαλείς ομάδων (cluster heads) και (δ) ο σταθμός βάσης (base station), όπως αυτά περιγράφονται στο [25] (Σχήμα 2.3). Οι αισθητήριοι κόμβοι αποτελούν το πυρήνα του δικτύου, και έχουν τη δυνατότητα συλλογής πληροφορίας, αποθήκευσης, επεξεργασίας και δρομολόγησης δεδομένων. Οι ομάδες αποτελούν δομική μονάδα ενός ως ιεραρχημένου δικτύου WSN. Επιπλέον, οι επικεφαλείς ομάδων είναι ειδικοί κόμβοι με αυξημένες αρμοδιότητες και αυξημένη επεξεργαστική δυνατότητα, στους οποίους τίθεται ως βασική απαίτηση η οργάνωση των δραστηριοτήτων της ομάδας. Ο επικεφαλής ομάδας καλείται να συγκεντρώνει δεδομένα (συνάθροιση δεδομένων – data aggregation) από τους υφιστάμενους κόμβους και να τα προωθεί είτε στο σταθμό βάσης είτε σε άλλο γειτονικό επικεφαλή ομάδας, και αντίστροφα να λαμβάνει εντολές ή δεδομένα και είτε να τις διαμοιράζει στους υφιστάμενους κόμβους, είτε να τις προωθεί σε γειτονικό επικεφαλή ομάδας. Τέλος, η βασισμένη στη θέση δρομολόγηση βασίζεται στη χρήση πληροφορίας θέσης, η οποία βοηθάει τη διάδοση δεδομένων αξιοποιώντας την επεκτασιμότητα σε δίκτυα με

πολυάριθμους κόμβους. Όταν είναι γνωστή η θέση που ανιχνεύτηκε το συμβάν, εξαλείφεται σημαντικός αριθμός μεταδόσεων και κατ' επέκταση επιτυγχάνεται εξοικονόμηση ενέργειας.



Σχήμα 2.3. Δομή δικτύου WSN βασισμένου σε ομαδοποίηση κόμβων

2.4.1 Επίπεδη δρομολόγηση

Κυριότερα πρωτόκολλα επικοινωνίας επιπέδου δικτύου, τα οποία βασίζονται στην επίπεδη δρομολόγηση [25,26] είναι το SPIN (Sensor Protocol for Information via Negotiation), το MCFA (Minimum Cost Forwarding Algorithm), το COUGAR, το EAR (Energy – Aware Routing), το SAR (Sequential Assignment Routing) και το ACQUIRE (ACtive QUery forwarding In sensoR nEtworks). Επίσης, χρησιμοποιούνται οι τεχνικές Directed Diffusion, Rumor Routing, GBR (Gradient – Based Routing), IDSQ (Information-Driven Sensor Querying), CADR (Constrained Anisotropic Diffusion Routing) και τυχαίων βημάτων (Random Walks – Based Routing Techniques).

Το πρωτόκολλο SPIN (Sensor Protocol for Information via Negotiation) βασίζεται στην υπόθεση ότι όλοι οι κόμβοι του δικτύου είναι εν δυνάμει σταθμοί βάσης. Ως εκ τούτου, η πληροφορία διαδίδεται σε όλους τους κόμβους και ο χρήστης μπορεί να την αντλήσει ασκώντας ένα ερώτημα (query) σε οποιονδήποτε κόμβο. Η διάδοση γίνεται με time-driven τρόπο και η πληροφορία διαδίδεται σε όλο το δίκτυο, ακόμα και αν δεν έχει ζητηθεί. Ωστόσο το πρωτόκολλο SPIN διαφέρει από τη κλασσική τεχνική πλημμυρίσματος (flooding) του δικτύου ως εξής: (α) Οι κόμβοι διαδίδουν σε όλο το δίκτυο την πληροφορία, που περιλαμβάνει μία περιγραφή των δεδομένων που έχουν παραχθεί (μηνύματα ADV – διαφήμισης) και όχι όλα τα δεδομένα, (β) Δεν αποστέλλονται πολλά αντίγραφα όμοιων δεδομένων που μπορεί να έχουν συλλέξει γειτονικοί κόμβοι, καθώς υπάρχει η δυνατότητα διαπραγμάτευσης

(μέσω μηνύματος REQ – απαίτησης). Οι παραπάνω δύο διαφορές καθιστούν το πρωτόκολλο SPIN ενεργειακά αποδοτικότερο.

Η τεχνική κατευθυνόμενης διάδοσης (directed diffusion) βασίζεται στην ιδέα συνδυασμού δεδομένων που προέρχονται από διαφορετικές πηγές και έχουν κοινό προορισμό, περιορίζοντας τον πλεονασμό δεδομένων και τον αριθμό επανεκπομπών. Με τον τρόπο αυτό επιτυγχάνεται εξοικονόμηση ενέργειας και αυξάνεται ο χρόνος ζωής των κόμβων του δικτύου. Ο σταθμός βάσης αποστέλλει μηνύματα ενδιαφέροντος με τη τεχνική πλημμυρίσματος του δικτύου (flooding), στο οποίο περιγράφεται ο τύπος των δεδομένων που ενδιαφέρουν. Κάθε κόμβος λαμβάνοντας το μήνυμα ενδιαφέροντος το προωθεί στους γειτονικούς κόμβους. Στη συνέχεια υλοποιείται σους κόμβους μια διαβαθμισμένη δομή (gradient setup), η οποία προσδιορίζει το κατά πόσο οι μετρήσεις που αντιστοιχούν στο ενδιαφέρον του σταθμού βάσης μπορούν να προωθηθούν προς αυτόν. Η διαβαθμισμένη δομή προσδιορίζεται με βάση τη θέση του κόμβου, την ενεργειακή του κατάσταση και τις δυνατότητες επικοινωνίας του. Με βάση αυτή τη δομή καθορίζεται η βέλτιστη (με κριτήριο υψηλότερες διαβαθμίσεις σε κάθε άλμα) διαδρομή από τον αισθητήριο κόμβο προς το σταθμό βάσης και τελικά γίνεται μέσω αυτής η προώθηση των δεδομένων. Οι επιμέρους βέλτιστες διαδρομές από τις πηγές πληροφορίας προς το σταθμό βάσης υλοποιούν ένα δένδρο συνάθροισης δεδομένων.

Η τεχνική GBR (Gradient – Based Routing) αποτελεί παραλλαγή της κατευθυνόμενης διάδοσης. Η βασική ιδέα είναι η απομνημόνευση των αλμάτων που χρειάστηκε το μήνυμα ενδιαφέροντος, ώστε να φθάσει στον αισθητήριο κόμβο, όπου υπολογίζεται το ύψος του κόμβου, ο οποίος είναι ο ελάχιστος αριθμός αλμάτων για να φθάσει η πληροφορία από το κόμβο στο σταθμό βάσης. Το ύψος του κόμβου καθορίζει και τη διαδρομή δρομολόγησης των δεδομένων.

Μια επιπλέον παραλλαγή της κατευθυνόμενης διάδοσης είναι η δρομολόγηση με βάση τη φήμη (Rumor Routing). Η κεντρική ιδέα είναι η καθοδήγηση των μηνυμάτων ενδιαφέροντος προς τους κρίσιμους κόμβους και όχι το πλημμύρισμα του δικτύου. Με τον τρόπο αυτό όταν δεν έχει ζητηθεί μεγάλη ποσότητα δεδομένων από το σταθμό βάσης έχουμε εξοικονόμηση πόρων του δικτύου.

Το πρωτόκολλο EAR (Energy Aware Routing) βασίζεται στη τεχνική κατευθυνόμενης διάδοσης. Η διαφορά του εντοπίζεται στο ότι δεν ανιχνεύει μόνο τη βέλτιστη διαδρομή από τον αισθητήριο κόμβο προς το σταθμό βάσης, αλλά μια ομάδα εναλλακτικών διαδρομών. Η επιλογή κάθε διαδρομής γίνεται με ορισμένη

πιθανότητα, η οποία εξαρτάται από τη κατανάλωση ενέργειας που απαιτεί για τη διάδοση των δεδομένων. Η εν λόγω τεχνική αυξάνει το χρόνο ζωής του δικτύου καθώς η κατανάλωση ενέργειας είναι ομοιόμορφα κατανεμημένη μεταξύ των κόμβων.

2.4.2 Ιεραρχική δρομολόγηση

Κυριότερα πρωτόκολλα επικοινωνίας επιπέδου δικτύου, τα οποία βασίζονται στην ιεραρχική δρομολόγηση [25,26] είναι το LEACH (Low-Energy Adaptive Clustering Hierarchy), το TL-LEACH (Two-Level Hierarchy LEACH-επέκταση του LEACH), το TEEN (Threshold Sensitive Energy Efficient Network Protocol), το APTEEN (Adaptive Periodic Threshold Sensitive Energy Efficient Sensor Network Protocol – επέκταση του TEEN), το HEED [](Hybrid Energy Efficient Distributed Clustering), το PEGASIS (Power Efficient in Sensor Information Systems), το SOP (Self-Organization Protocol), το VGA (Virtual Grid Architecture Routing), το Sensor Aggregates Routing, το HPAR (Hierarchical Power – Aware Routing) και το TTDD (Tier-Tier Data Dissemination).

Σύμφωνα με το πρωτόκολλο LEACH (Low-Energy Adaptive Clustering Hierarchy) οι κόμβοι αρχικά οργανώνονται σε συμπλέγματα και επιλέγεται μέσω κατάλληλου αλγόριθμου ο επικεφαλής συμπλέγματος. Οι επικεφαλείς συμπλέγματος αποστέλλουν στο δίκτυο μηνύματα με τα οποία ενημερώνουν ότι είναι επικεφαλείς, και οι υπόλοιποι κόμβοι με βάση την ισχύ λήψης αυτών των μηνυμάτων επιλέγουν σε ποιο σύμπλεγμα θα ενσωματωθούν. Εν συνεχεία, οι κόμβοι που είναι ενεργοί εγκαθιστούν επικοινωνία με τον επικεφαλή του συμπλέγματος τους σύμφωνα με τον προγραμματισμό πολλαπλής πρόσβασης διαίρεσης χρόνου (TDMA), που ο ίδιος τους έχει καθορίσει. Αδυναμία του πρωτοκόλλου LEACH είναι η μη αποδοτική εφαρμογή του σε δυναμικά περιβάλλοντα, διότι εκεί θα απαιτείται ανταλλαγή μεγάλου πλήθους μηνυμάτων για τον καθορισμό συμπλεγμάτων, η οποία οδηγεί σε μη αποδοτικό ενεργειακά δίκτυο.

Το πρωτόκολλο TEEN (Threshold Sensitive Energy Efficient Network Protocol) είναι ένα πρωτόκολλο ιεραρχικής δρομολόγησης, στο οποίο οι επικεφαλείς ομάδων για τον έλεγχο της διαδιδόμενης πληροφορίας ορίζουν δύο στάθμες (κατώφλια) του μετρούμενου από τους αισθητήρες μεγέθους. Η πρώτη στάθμη, που καλείται σκληρό κατώφλι (hard threshold), ορίζει το κατώφλι του μετρούμενου μεγέθους, και η δεύτερη, που καλείται μαλακό κατώφλι (soft threshold), ορίζει την

ελάχιστη μεταβολή του μεγέθους, η οποία θα οδηγήσει το κόμβο στη μετάδοση. Στο σημείο αυτό διακρίνεται ένα tradeoff μεταξύ ακρίβειας μέτρησης (μεγάλη για χαμηλό μαλακό κατώφλι) και κατανάλωσης ενέργειας (μεγάλη για χαμηλό μαλακό κατώφλι). Επέκταση του πρωτοκόλλου TEEN είναι το APTEEN (Adaptive Periodic Threshold Sensitive Energy Efficient Sensor Network Protocol), σύμφωνα με το οποίο οι τιμές των δύο κατωφλίων μεταβάλλονται περιοδικά.

Το πρωτόκολλο PEGASIS (Power Efficient in Sensor Information Systems) προϋποθέτει τη γνώση από τους κόμβους της τοπολογίας του δικτύου, η μη κινητικότητα τους και η δυνατότητα όλων των κόμβων να επικοινωνήσουν απευθείας με το σταθμό βάσης. Στο πρωτόκολλο PEGASIS οι κόμβοι αναλαμβάνουν περιοδικά το ρόλο του επικεφαλή ομάδας, όπου γίνεται η συνάθροιση των δεδομένων και η προώθηση τους στο σταθμό βάσης. Το γεγονός αυτό προσφέρει το πλεονέκτημα της ομοιόμορφης κατανάλωσης ενέργειας από όλους τους κόμβους, καθώς τα καθήκοντα του επικεφαλής ομάδας εναλλάσσονται.

2.4.3 Βασισμένη στη θέση δρομολόγηση

Κυριότερα πρωτόκολλα δρομολόγησης [25,26] είναι το MECP (Minimum Energy Communication Protocol), το SMECP (Small Minimum Energy Communication Protocol), το GAF (Geographic Adaptive Fidelity), το GEAR (Geographical and Energy – Aware Routing), το MFR (Most Forward within Radius), το GEDIR (The Geographic Distance Routing), το GOAFR (The Greedy Other Adaptive Face Routing), και το SPAN.

Στο πρωτόκολλο GAF (Geographic Adaptive Fidelity) οι κόμβοι υλοποιούν ένα εικονικό πλέγμα, χωρίζοντας το δίκτυο σε ζώνες. Σε κάθε ζώνη ένας κόμβος παραμένει ενεργός ενώ οι υπόλοιποι βρίσκονται σε κατάσταση αναμονής. Ο εν λόγω κόμβος έχει την ευθύνη επικοινωνίας με το σταθμό βάσης για λογαριασμό και των υπόλοιπων κόμβων της ζώνης. Όταν το χρονικό διάστημα ενεργοποιημένου κόμβου παρέλθει, ένας άλλος κόμβος της ζώνης γίνεται ενεργός και παίρνει τη θέση του προηγούμενου. Με τον τρόπο αυτό επιτυγχάνεται εξοικονόμηση ενέργειας και ομοιόμορφη κατανάλωση της σε κόμβους που γειτνιάζουν. Το πρωτόκολλο GEAR (Geographical and Energy – Aware Routing) (GEAR) παραπέμπει στο μηχανισμό DD, αλλά περιορίζει τις εκπομπές μηνυμάτων ενδιαφέροντος από το σταθμό βάσης με χρήση γεωγραφικών κριτηρίων.

2.4.4 Πολυδιαδρομική δρομολόγηση

Τα πρωτόκολλα που υποστηρίζουν πολυδιαδρομική δρομολόγηση καθορίζουν πέραν του κυρίου και εναλλακτικά δρομολόγια διάδοσης των δεδομένων. Μέτρο της ανοχής σε σφάλματα (fault tolerance) ή ελαστικότητας (resilience) του δικτύου είναι η πιθανότητα ύπαρξης εναλλακτικού μονοπατιού μεταξύ της πηγής πληροφορίας και του τελικού προορισμού, όταν το κύριο μονοπάτι αποτύχει στη μετάδοση των δεδομένων. Η πολυδιαδρομική δρομολόγηση βελτιώνει τη λειτουργία του δικτύου ως προς την αξιοπιστία, με αντιστάθμισμα την υψηλότερη κατανάλωση ενέργειας και το ρίσκο συμφόρησης δεδομένων. Πρωτόκολλα που υποστηρίζουν πολυδιαδρομική δρομολόγηση [25,26] είναι το SPIN, το Directed Diffusion και το VGA, όπως φαίνεται στο Πίνακα 2.2.

2.4.5 Query-based δρομολόγηση

Στα query-based πρωτόκολλα ο προορισμός της πληροφορίας (σταθμός βάσης) αποστέλλει στους κόμβους ερωτήματα (queries). Κάθε κόμβος που λαμβάνει ένα ερώτημα, το οποίο ταιριάζει με τα δεδομένα που ενδεχομένως έχει συλλέξει, τα αποστέλλει στο προορισμό της πληροφορίας. Η τεχνικές Directed Diffusion και Rumor Routing και τα πρωτόκολλα SPIN, GBR, COUGAR, ACQUIRE, EAR, SAR και SPEED βασίζονται στη query-based δρομολόγηση, όπως φαίνεται στο Πίνακα 2.2 [25].

2.4.6 Negotiation-based δρομολόγηση

Η πρόκληση της δρομολόγησης με βάση τη διαπραγμάτευση είναι ο περιορισμός δρομολόγησης πλεονάζουσας πληροφορίας εντός του δικτύου. Η καταστολή της πλεονάζουσας πληροφορίας γίνεται με την χρήση μιας σειράς μηνυμάτων διαπραγμάτευσης μεταξύ κόμβων και σταθμού βάσης, πριν η ξεκινήσει η μετάδοση δεδομένων. Πρωτόκολλα που υποστηρίζουν αυτού του είδους δρομολόγηση είναι, όπως φαίνεται στο Πίνακα 2.2 [25], το SPIN, η τεχνική Directed Diffusion, το VGA, το SPAN και το SAR.

2.4.7 QoS-based δρομολόγηση

Τα πρωτόκολλα που εξυπηρετούν τη βασισμένη στο QoS δρομολόγηση αντιμετωπίζουν τη πρόκληση της βέλτιστης ισορροπίας μεταξύ των θεμάτων κατανάλωσης ενέργειας και ποιότητας δεδομένων. Το πρωτόκολλο δρομολόγησης πρέπει να ικανοποιεί τις προδιαγραφές που καθορίζονται από την υπηρεσία και

αφορούν στη κατανάλωση ενέργειας, στο διατιθέμενο εύρος ζώνης στην αποδεκτή καθυστέρηση κατά τη διάδοση δεδομένων από τον αισθητήριο κόμβο προς το σταθμό βάσης. Πρωτόκολλα που αντιμετωπίζουν την παραπάνω πρόκληση είναι το SAR και το SPEED, όπως φαίνεται στο Πίνακα 2.2 [25].

2.4.8 Coherent-based δρομολόγηση

Σημαντική λειτουργία σε ένα δίκτυο WSN είναι η επεξεργασία δεδομένων, η οποία διαφοροποιείται με βάση το εφαρμοζόμενο πρωτόκολλο δρομολόγησης. Οι κόμβοι σε ένα δίκτυο συνεργάζονται και επεξεργάζονται μαζί δεδομένα που διαδίδονται στη γειτονιά τους. Στη δρομολόγηση με μη συνεκτική επεξεργασία δεδομένων, οι κόμβοι επεξεργάζονται τοπικά τα καινούργια δεδομένα που συλλέγονται και αποστέλλονται σε άλλους κόμβους για περαιτέρω επεξεργασία. Οι κόμβοι που λαμβάνουν τα δεδομένα για περαιτέρω επεξεργασία καλούνται συναθροιστές ή συλλέκτες (aggregators). Στη δρομολόγηση με συνεκτική επεξεργασία δεδομένων οι κόμβοι που συλλέγουν τη πληροφορία προχωρούν στην ελάχιστες ενέργειες και λαμβάνουν μέριμνα ώστε να προωθηθεί η πληροφορία στους συναθροιστές για την κυρίως επεξεργασία. Γενικά η δρομολόγηση με συνεκτική επεξεργασία δεδομένων είναι ενεργειακά αποδοτικότερη και για το λόγο αυτό ελκυστικότερη σε εφαρμογές δικτύων WSN.

Στον Πίνακα 2.2 γίνεται συνοπτική αναφορά των χαρακτηριστικών των πρωτοκόλλων που αναφέρθηκαν προηγουμένως όπως αυτά συνοψίζονται στο [25].

	Classification	Mobility	Position Awareness	Power Usage	Negotiation based	Data Aggregation	Localization	QoS	State Complexity	Scalability	Multipath	Query based
SPIN	Flat	Possible	No	Limited	Yes	Yes	No	No	Low	Limited	Yes	Yes
Directed Diffusion	Flat	Limited	No	Limited	Yes	Yes	Yes	No	Low	Limited	Yes	Yes
Rumor Routing	Flat	Very Limited	No	N/A	No	Yes	No	No	Low	Good	No	Yes
GBR	Flat	Limited	No	N/A	No	Yes	No	No	Low	Limited	No	Yes
MCFA	Flat	No	No	N/A	No	No	No	No	Low	Good	No	No
CADR	Flat	No	No	Limited	No	Yes	No	No	Low	Limited	No	No
COUGAR	Flat	No	No	Limited	No	Yes	No	No	Low	Limited	No	Yes
ACQUIRE	Flat	Limited	No	N/A	No	Yes	No	No	Low	Limited	No	Yes
EAR	Flat	Limited	No	N/A	No	No		No	Low	Limited	No	Yes
LEACH	Hierarchical	Fixed BS	No	Maximum	No	Yes	Yes	No	CHs	Good	No	No
TEEN & APTEEN	Hierarchical	Fixed BS	No	Maximum	No	Yes	Yes	No	CHs	Good	No	No
PEGASIS	Hierarchical	Fixed BS	No	Maximum	No	No	Yes	No	Low	Good	No	No
MECN & SMECN	Hierarchical	No	No	Maximum	No	No	No	No	Low	Low	No	No
SOP	Hierarchical	No	No	N/A	No	No	No	No	Low	Low	No	No
HPAR	Hierarchical	No	No	N/A	No	No	No	No	Low	Good	No	No
VGA	Hierarchical	No	No	N/A	Yes	Yes	Yes	No	CHs	Good	Yes	No
Sensor aggregate	Hierarchical	Limited	No	N/A	No	Yes	No	No	Low	Good	No	Possible
TTDD	Hierarchical	Yes	Yes	Limited	No	No	No	No	Moderate	Low	Possible	Possible
GAF	Location	Limited	No	Limited	No	No	No	No	Low	Good	No	No
GEAR	Location	Limited	No	Limited	No	No	No	No	Low	Limited	No	No
SPAN	Location	Limited	No	N/A	Yes	No	No	No	Low	Limited	No	No
MFR, GEDIR	Location	No	No	N/A	No	No	No	No	Low	Limited	No	No
GOAFR	Location	No	No	N/A	No	No	No		Low	Good	No	No
SAR	QoS	No	No	N/A	Yes	Yes	No	Yes	Moderate	Limited	No	Yes
SPEED	QoS	No	No	N/A	No	No	No	Yes	moderate	Limited	No	Yes

Πίνακας 2.2. Ταξινόμηση πρωτοκόλλων δρομολόγησης [25]

2.5 Επίπεδο ζεύξης (data link layer)

Στο επίπεδο ζεύξης δεδομένων ο κόμβος που αποστέλλει τα δεδομένα ενθυλακώνει το δεδομενόγραμμα μέσα σε ένα πλαίσιο επιπέδου ζεύξης και ο κόμβος λήψης εξάγει από το λαμβανόμενο πλαίσιο το αντίστοιχο δεδομενόγραμμα. Κάθε πλαίσιο αποτελείται από την επικεφαλίδα, και το επίμετρο (trailer), τα οποία προστίθενται από το επίπεδο ζεύξης και το ωφέλιμο φορτίο που αποτελεί το δεδομενόγραμμα του επιπέδου δικτύου.

Τα πρωτόκολλα που αφορούν στο επίπεδο ζεύξης αποσκοπούν σε λειτουργίες όπως η πολύπλεξη, ανίχνευση πλαισίων δεδομένων και έλεγχο σφαλμάτων, εξασφαλίζοντας την αξιοπιστία της υπηρεσίας. Σφάλματα είναι δυνατόν να εντοπιστούν είτε λόγω διακαναλικής παρεμβολής (co-channel interference) στο επίπεδο MAC, είτε εξαιτίας δυσμενών παραγόντων του περιβάλλοντος διάδοσης, όπως πολυδιαδρομική διάδοση, διαλείψεις και σκίαση. Για την επίλυση των δυσχερειών που θέτουν σε κίνδυνο την αξιοπιστία του δικτύου έχουν σχεδιαστεί τα πρωτόκολλα MAC (Media Access Control) που παρέχουν λύση στα προβλήματα διακαναλικής παρεμβολής, και οι τεχνικές FEC (Forward Error Correction) [30] και ARQ (Automatic Repeat Request) [30], οι οποίες αποσκοπούν την μείωση των δυσμενών επιπτώσεων του περιβάλλοντος διάδοσης. Σε πολλά πρότυπα το επίπεδο ζεύξης διαιρείται σε δύο υποεπίπεδα, το επίπεδο LLC (Logical Link Control) και το επίπεδο MAC. Το επίπεδο LLC πολυπλέκει και αποπολυπλέκει τα δεδομενογράμματα του επιπέδου δικτύου, διαμορφώνοντας τα πλαίσια δεδομένων ενώ το επίπεδο MAC είναι υπεύθυνο για τη πρόσβαση στο μέσο μετάδοσης.

2.5.1 Έλεγχος Πρόσβασης στο Μέσο Μετάδοσης - MAC (Media Access Control)

Τα πρωτόκολλα MAC είναι υπεύθυνα για το προγραμματισμό πρόσβασης στο δίαυλο και τον έλεγχο σφαλμάτων και η εφαρμογή τους είναι ευεργετική για την επίτευξη αξιόπιστης, με μικρές καθυστερήσεις πρόσβασης και ενεργειακά αποδοτικής υπηρεσίας. Η πρόσβαση στο μέσο μπορεί να γίνει με τις παρακάτω μεθόδους:

(α) με χρήση τεχνικών πολλαπλής πρόσβασης διαίρεσης χρόνου, συχνότητας ή κώδικα (TDMA, FDMA ή CDMA – Time, Frequency or Code Division Multiple Access), οι οποίες επικεντρώνονται στη τμηματοποίηση του καναλιού και τη διάθεση των τμημάτων στους κόμβους για αποκλειστική χρήση,

(β) με χρήση τεχνικών τυχαίας (δυναμικής) πρόσβασης (CSMA - Carrier Sense Multiple Access , ALOHA), όπου η εκχώρηση του καναλιού γίνεται είτε με δυναμικό τρόπο με ανίχνευση φέροντος (carrier sensing) ή σύγκρουσης (collision detection) εντός του καναλιού, είτε με τυχαίο τρόπο.

Μερικά πρωτόκολλα MAC είναι το Sensor MAC (S-MAC), το Timeout MAC (T-MAC), το Dynamic Sensor MAC (DSMAC), το DMAC, το WiseMAC, το SIFT, το CC-MAC, το Z-MAC, το B-MAC, το Low-Power Distributed MAC, το Low-Power Reservation-based MAC και το Traffic Adaptive MAC (TRAMA) [2,29]. Στον Πίνακα 2.3 γίνεται μια σύντομη αναφορά των χαρακτηριστικών των βασικών πρωτοκόλλων MAC, όπως αυτά συνοψίζονται στο [2].

Attributes	TRAMA	B-MAC	Z-MAC	Low power reservation-based MAC	Low power distributed MAC	CC-MAC
Channel access mode	Time-slotted random and scheduled access	Clear channel assessment (CCA)	Time-slotted random and scheduled access	Time-slotted contention based slot reservation	Multi-channel access	Time-slotted contention based slot reservation
Time synchronization	Yes	No	Yes	Yes	No	No
Protocol type	TDMA/CSMA	CSMA	TDMA/CSMA	TDMA	CSMA/CA	CSMA/CA
Protocol specifics	Achieves adequate throughput and fairness through transmitter-election algorithm and channel re-use	Bi-directional interface for reconfiguration of system services to optimize performance	Exploits the strengths of TDMA and CSMA while offsetting their weaknesses	Increases the probability of success in packet transmission by adapting to traffic requirements to maximize data throughput	Combines CSMA and spread spectrum techniques to achieve higher power efficiency and bandwidth	Filters out correlated data and ensures prioritization of packets to the sink which results in achieving higher network performance
Energy conservation	Schedule sleep intervals and turn radio off when idle, collision avoidance scheduling	Low power listening (LPL) time for energy efficiency	Low power listening (LPL) time for energy efficiency	Nodes sleep and wake up based on assigned data slot	Power saving mode with low power wake up radio for channel listening and normal radio for data transmission	Dropping highly correlated information packet to reduce energy use in transmission

Πίνακας 2.3. Σύγκριση πρωτοκόλλων MAC [2]

2.5.2 Τεχνικές FEC (Forward Error Correction) - ARQ (Automatic Repeat Request)

Η ικανότητα αντιστάθμισης των λαθών κατά τη διάδοση είναι κρίσιμη για την εξασφάλιση αξιόπιστης υπηρεσίας. Οι τεχνικές FEC και ARQ [30] αποσκοπούν σε αυτήν με διαφορετικές μεθόδους. Συγκεκριμένα, στη τεχνική FEC ο κόμβος-αποστολέας αποστέλλει πλεονάζουσα πληροφορία, την οποία ο κόμβος-παραλήπτης χρησιμοποιεί για τη διόρθωση τυχόντων σφαλμάτων που θα εντοπίσει. Η τεχνική ARQ βασίζεται στην αναγνώριση της απεσταλμένης πληροφορίας από το κόμβο-παραλήπτη, εφόσον αυτή δεν είναι εσφαλμένη. Εάν αυτή δε συμβεί, ο κόμβος-αποστολέας επαναλαμβάνει την εκπομπή. Δεδομένου ότι η επικοινωνία μεταξύ των δύο κόμβων γίνεται με πολλαπλά άλματα (multiple hops), και ότι οι επανεκπομπές μειώνουν το χρόνο ζωής των κόμβων λόγω κατανάλωσης ενέργειας, προκύπτει ότι η

τεχνική FEC είναι ενεργειακά αποδοτικότερη και επομένως δημοφιλέστερη σε εφαρμογές δικτύων WSN.

2.6 Φυσικό Επίπεδο (Physical Layer)

Το φυσικό επίπεδο καθορίζει τη χρησιμοποιούμενη συχνότητα της εφαρμογής, την ανίχνευση σήματος και την επεξεργασία του (διαμόρφωση, κωδικοποίηση δεδομένων, κρυπτογράφηση). Επιπλέον καθορίζει τη διεπαφή, η οποία μεταδίδει την ακολουθία ψηφίων στο φυσικό μέσο. Το πρότυπο IEEE 802.15.4 είναι ευρέως χρησιμοποιούμενο σε δίκτυα WSN, με στόχο την επίτευξη χαμηλού κόστους, πολυπλοκότητας και χαμηλής κατανάλωσης του δικτύου. Αναπτύχθηκε από τον οργανισμό IEEE (Institute of Electrical and Electronics Engineers), και παρέχει υπηρεσίες στο φυσικό επίπεδο καθώς και στο επίπεδο MAC σε δίκτυα μικρής εμβέλειας που υποστηρίζουν χαμηλούς ρυθμούς μετάδοσης. Το συγκεκριμένο πρότυπο αποτελεί τη βάση για το πρότυπο ZigBee, το οποίο παρέχει υπηρεσίες στα ανώτερα επίπεδα της αρχιτεκτονικής του δικτύου WSN.

2.7 Διασταυρούμενα επίπεδα (cross layers)

Για την αποδοτικότερη λειτουργία του δικτύου είναι απαραίτητη η συνεργασία των κόμβων, η οποία επιμηκύνει το χρόνο ζωής του δικτύου. Τα διασταυρούμενα επίπεδα αλληλεπιδρούν με τα επίπεδα σχεδίασης που έχουν προαναφερθεί και δεν επιτρέπουν στους κόμβους να λειτουργούν ατομικά.

Το επίπεδο διαχείρισης ενέργειας (power management plane) διαχειρίζεται την ενέργεια των κόμβων του δικτύου. Για παράδειγμα, εάν ένας κόμβος έχει έλλειμμα υπολειπόμενης ενέργειας, ενημερώνει τους γειτονικούς του κόμβους ότι δεν μπορεί να συμμετέχει στη δρομολόγηση πακέτων προς το σταθμό βάσης. Με τον τρόπο αυτό εξοικονομεί ενέργεια για τη χρήση της αποκλειστικά για τη λειτουργία του ως πηγή της πληροφορίας. Το επίπεδο διαχείρισης φορητότητας (mobility management plane) παρακολουθεί τη κίνηση των κόμβων και καταχωρείται στη μνήμη κάθε κόμβου συνεχώς η θέση των γειτονικών του και τη θέση του ως προς το σταθμό βάσης. Η πληροφορία αυτή είναι σημαντική για τη διαχείριση της ενεργειακής κατάστασης των κόμβων. Τέλος, το επίπεδο διαχείρισης λειτουργιών (task management plane) διαχειρίζεται τις λειτουργίες των κόμβων (δρομολόγηση ή παρακολούθηση ενδιαφερόμενου περιβάλλοντος), λαμβάνοντας υπόψη τα ενεργειακά αποθέματα τους.

2.8 Πρότυπα δικτύων WSN

Τα πρότυπα επικοινωνίας των δικτύων WSN χαρακτηρίζονται από συμβατότητα σε χαμηλούς ρυθμούς μετάδοσης, χαμηλή κατανάλωση, μικρή εμβέλεια και δυνατότητες επεξεργασίας και αποθήκευσης συσκευών. Τα δημοφιλέστερα πρότυπα είναι η τεχνολογία ZigBee και τα πρότυπα Bluetooth LE, EnOcean, DASH7, RuBee, Isa100.11.a, και 6LoWPAN.

2.8.1 Τεχνολογία ZigBee

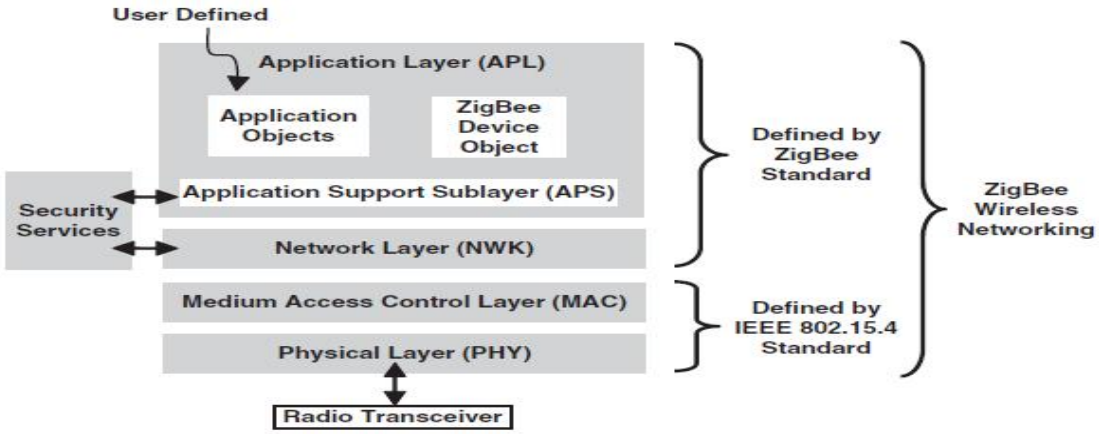
Το πρότυπο IEEE 802.15.4 αναπτύχθηκε με σκοπό τη παροχή υπηρεσιών φυσικού επιπέδου και επιπέδου ζεύξης σε δίκτυα χαμηλού ρυθμού μετάδοσης δεδομένων και περιορισμένης κατανάλωσης ενέργειας, θεμελιώδη χαρακτηριστικά ενός δικτύου WSN. Η αρχιτεκτονική του προτύπου IEEE 802.15.4 απεικονίζεται στην Σχήμα 2.4. Το πρότυπο ZigBee αποτελεί την επέκταση του IEEE 802.15.4 στα ανώτερα επίπεδα του δικτύου (επίπεδα δικτύου και εφαρμογής) και συνεργατικά υλοποιούν μια ενιαία εμπορική πλατφόρμα, η οποία καλείται τεχνολογία ZigBee [39] και βρίσκει εφαρμογή σε δίκτυα χαμηλού ρυθμού μετάδοσης (LPAN – Low-rate Personal Area Networks). Η τεχνολογία ZigBee χρησιμοποιεί τις ελεύθερες μπάντες συχνοτήτων περί τα 2.4 GHz (παγκόσμια χρήση), 915 MHz (Αμερική) και 868 MHz (Ευρώπη). Ο ρυθμός μετάδοσης της υπηρεσίας στη τεχνολογία είναι 250 kb/s στα 2.4 GHz, 40 kb/s στα 915 MHz και 100 kb/s στα 868 MHz. Τα δύο φυσικά στρώματα που εξετάζει η παρούσα εργασία είναι στις ζώνες 868 MHz και 2.4 GHz.

Για εκπομπή στη χαμηλή ζώνη στα 868 MHz χρησιμοποιούνται τα σχήματα διαμόρφωσης BPSK (Binary Phase Shift Keying), ASK (Amplitude Shift Keying) και O-QPSK (Offset Quadrature Phase Shift Keying). Το φυσικό στρώμα υψηλής ζώνης αξιοποιεί την ζώνη συχνοτήτων από 2.4GHz έως 2.483GHz. Προσφέρει 16 κανάλια με βήμα 5MHz με μέγιστο ρυθμό μετάδοσης τα 250kb/s. Η διαμόρφωση που χρησιμοποιείται στην ζώνη αυτή είναι η O-QPSK (Offset Quadrature Phase Shift Keying). Το πρότυπο 802.15.4 ορίζει την απαίτηση για ευαισθησία του δέκτη στα -92dbm για την χαμηλή ζώνη και στα -85dbm για την υψηλή ζώνη. Επίσης, απαιτεί δυνατότητα ισχύος εκπομπής 1mW, απαίτηση η οποία μπορεί να μεταβάλλεται ανάλογα με τους υφιστάμενους κανόνες και τα όρια ισχύος εκπομπής. Οι απαιτήσεις για όλο και υψηλότερους ρυθμούς μετάδοσης και η δυνατότητα χρήσης μεγαλύτερου αριθμού καναλιών έχουν οδηγήσει στην υιοθέτηση στα δίκτυα WSN ραδιοπομπών που αξιοποιούν την υψηλή ζώνη. Επιπλέον, η

τεχνολογία ZigBee χρησιμοποιεί για την αποφυγή παρεμβολών το μηχανισμό εξάπλωσης φάσματος άμεσης ακολουθίας (Direct – sequence spread spectrum – DSSS).

	Frequency (MHz)	Number of Channels	Modulation	Chip Rate (Kchip/s)	Bit Rate (Kb/s)	Symbol Rate (Ksymbol/s)	Spreading Method
	868–868.6	1	BPSK	300	20	20	Binary DSSS
	902–928	10	BPSK	600	40	40	Binary DSSS
Optional	868–868.6	1	ASK	400	250	12.5	20-bit PSSS
	902–928	10	ASK	1600	250	50	5-bit PSSS
Optional	868–868.6	1	O-QPSK	400	100	25	16-array orthogonal
	902–928	10	O-QPSK	1000	250	62.5	16-array orthogonal
	2400–2483.5	16	O-QPSK	2000	250	62.5	16-array orthogonal

Πίνακας 2.4. Συχνότητες λειτουργίας και ρυθμοί μετάδοσης προτύπου IEEE802.15.4



Σχήμα 2.4. Αρχιτεκτονική τεχνολογίας ZigBee

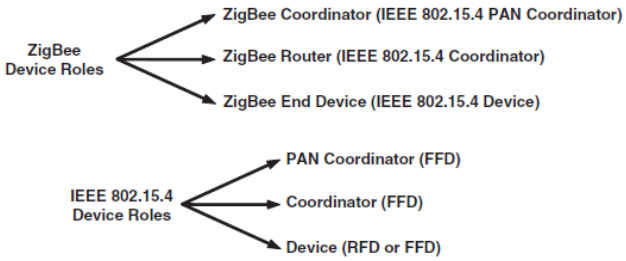
Ένα δίκτυο δομημένο με βάση το πρότυπο IEEE 802.15.4 αποτελείται από τριών ειδών συσκευές οι οποίες αναφέρονται ως:

- Συσκευές συντονιστές δικτύου (Coordinators PAN): Υπάρχει ένας συντονιστής PAN στο δίκτυο και χρησιμοποιείται για τον έλεγχο και τη διαχείριση της πληροφορίας που διακινείται στο δίκτυο. Πρόκειται για συσκευή με αυξημένες ικανότητες υπολογισμών και αποθήκευσης δεδομένων.
- Συσκευές πλήρους λειτουργίας (FFD – Full-Function Devices): Οι συσκευές FFD υλοποιούν κόμβους αυξημένων αρμοδιοτήτων, με μεγαλύτερη υπολογιστική ικανότητα. Είναι δυνατόν να χρησιμοποιούνται ως συντονιστές

(coordinators) ή δρομολογητές (routers) του δικτύου καθώς έχουν τη δυνατότητα να επικοινωνήσουν με όλους τους τύπους συσκευών στο δίκτυο.

- Συσκευές περιορισμένης λειτουργίας (RFD – Reduced-Function Devices): Οι συσκευές RFD σε αντίθεση με τις FFD εμφανίζουν περιορισμένες υπολογιστικές ικανότητες και ως εκ τούτου αναλαμβάνουν απλές λειτουργίες, για τις οποίες δεν απαιτείται διακίνηση μεγάλου όγκου δεδομένων. Οι συσκευές αυτές έχουν τη δυνατότητα να επικοινωνήσουν μόνο με συσκευές FFD.

Ένα WSN βασισμένο στο πρότυπο ZigBee διαχωρίζει τις συσκευές του δικτύου σε έναν συντονιστή (coordinator), τις τελικές συσκευές (end devices) και τους δρομολογητές (routers). Με βάση τη κατηγοριοποίηση συσκευών του προτύπου IEEE 802.15.4, ο συντονιστής και οι δρομολογητές είναι συσκευές πλήρους λειτουργίας (FFD), ενώ οι τελικές συσκευές μπορούν να είναι είτε πλήρους, είτε περιορισμένης λειτουργίας (FFD ή RFD) (Σχήμα 2.5).



Σχήμα 2.5. Κατηγορίες συσκευών τεχνολογίας ZigBee

Η τεχνολογία ZigBee υποστηρίζει τις τοπολογίες αστέρα (star), πλέγματος (mesh) και δέντρου συστάδων (cluster tree). Στη τοπολογία αστέρα η επικοινωνία βασίζεται σε ένα κεντρικό κόμβο, ο οποίος καλείται συντονιστής PAN και υλοποιείται από συσκευή FFD. Ο συντονιστής PAN μπορεί να ελέγχει τόσο συσκευές FFD, όσο και RFD. Στη τοπολογία πλέγματος υπάρχει συντονιστής PAN δικτύου, όπως και στην τοπολογία αστέρα, ωστόσο όλες οι υπόλοιπες συσκευές έχουν τη δυνατότητα να επικοινωνήσουν με οποιοδήποτε κόμβο εντός της εμβέλειας τους (ευρεία χρήση FFD συσκευών) και είναι εφικτή η επικοινωνία πολλαπλών αλμάτων (multi-hop). Η συγκεκριμένη τοπολογία βρίσκει εφαρμογή σε ad-hoc αυτό-οργανούμενα (self-organizing) και αυτό–ιάσιμα (self – healing) δίκτυα και είναι δημοφιλής σε εφαρμογές δικτύων WSN επιτήρησης και ελέγχου. Σε αυτά τα δίκτυα η τοπολογία πλέγματος ενισχύει την αξιοπιστία του δικτύου με τη παροχή πλεονασμού δεδομένων εξαιτίας της πολυδιαδρομικής δρομολόγησης.

Τέλος, η τοπολογία δέντρου συστάδων, η οποία μπορεί να μελετηθεί σαν ειδική περίπτωση της τοπολογίας πλέγματος έχει στην πλειονότητα του FFD συσκευές με πιθανή την ύπαρξη RFD συσκευών ως τερματικών κόμβων («φύλλα») «κλαδιών» του δικτύου. Αν και οποιαδήποτε συσκευή FFD μπορεί να παίξει το ρόλο του συντονιστή παρέχοντας συγχρονισμό στις υπόλοιπες συσκευές, μόνο μία μπορεί να επιλεγεί ως συντονιστής PAN του δικτύου, η οποία αναλαμβάνει καθήκοντα επικεφαλή της πρώτης αναπτυχθείσας ομάδος του δικτύου. Η συγκεκριμένη τοπολογία διευκολύνει την ανάπτυξη δικτύων μεγάλης κάλυψης περιοχής.

2.8.2 Πρότυπο Bluetooth Low Energy (Bluetooth LE)

Το πρότυπο Bluetooth LE [41] αναπτύχθηκε σε εφαρμογές διασύνδεσης συσκευών (WPAN), στις οποίες η χαμηλή κατανάλωση ενέργειας είναι πρωταρχικής σημασίας. Το πρότυπο βασίζεται στο πρωτόκολλο IEEE 802.15.1 και χρησιμοποιεί την ελεύθερη ζώνη συχνοτήτων των 2.4 GHz. Η πρόσβαση στο κανάλι γίνεται με πολλαπλή πρόσβαση διαίρεσης συχνότητας (FDMA) ή χρόνου (TDMA). Με χρήση FDMA δίνεται η δυνατότητα εκχώρησης 40 καναλιών εύρους 2 MHz, ενώ με χρήση TDMA το φυσικό κανάλι είναι διαιρεμένο σε μονάδες χρόνου που καλούνται γεγονότα (events). Ο ρυθμός μετάδοσης που υποστηρίζει το πρότυπο Bluetooth LE είναι 1 Mbps, μεγαλύτερο από τον αντίστοιχο της τεχνολογίας ZigBee (250 Kbps), με χρήση GFSK διαμόρφωσης.

Η εμβέλεια συσκευών του προτύπου είναι 50 m, με ισχύ εκπομπής των κόμβων 10 mW. Για αποφυγή παρεμβολών χρησιμοποιείται η τεχνική μεταπήδησης συχνότητας (Adaptive Frequency Hopping - AFH). Τέλος το πρότυπο υποστηρίζει εγκατάσταση 2^{32} συσκευών σε τοπολογία αστέρα, σημείου προς σημείο, ή ad hoc.

Σύγκριση του προτύπου Bluetooth LE και τεχνολογίας ZigBee γίνεται στο Πίνακα 2.5.

Χαρακτηριστικά	**ZigBee**	**Bluetooth LE**
Συχνότητα λειτουργίας	2400/915/868 MHz	2.4 GHz
Ρυθμός μετάδοσης	20 – 250 Kbps	1 Mbps
Εμβέλεια	100 m	50 m
Χρόνος ζωής	6 μήνες – 2 χρόνια	1 – 2 χρόνια
Ισχύς εκπομπής	Έως 30 mW	10 mW
Διαμόρφωση	O-QPSK/BPSK	GFSK

Πλήθος συσκευών	2^{16}	2^{32}
Τοπολογίες	Αστέρα, πλέγματος, συμπλέγματος δέντρου	Αστέρα, ad hoc, σημείου προς σημείο
Μέγεθος πακέτου δεδομένων	127 bytes	27 bytes
Μηχανισμός αποφυγής παρεμβολών	DSSS	AFH
Ασφάλεια	AES 128 bit	AES 128 bit

Πίνακας 2.5. Σύγκριση προτύπου Bluetooth LE και τεχνολογίας ZigBee

2.8.3 Ανταγωνιστικά πρότυπα WSN

Για εφαρμογές WSN έχουν επίσης αναπτυχθεί [41] τα πρότυπα EnOcean, DASH7, RuBee, Isa100.11.a, και 6LoWPAN, παράθεση των χαρακτηριστικών των οποίων, μαζί με αυτών των ZigBee και Bluetooth LE, γίνεται στο Πίνακα 2.6.

Πρότυπο	**Συχνότητα λειτουργίας**	**Ρυθμός μετάδοσης**	**Εμβέλεια**
ZigBee	2400/915/868 MHz	Έως 250 Kbps	100 m
Bluetooth LE	2.4 GHz	1Mbps	50 m
EnOcean	868/315 MHz	125 Kbps	300 m
DASH7	433 MHz	200 Kbps	2 km
RuBee	131 KHz	1.2 Kbps	30 m
Isa100.11.a	2.4 GHz	250 Kbps	100 m
6LoWPAN	2.4 GHz	20 – 250 Kbps	10 – 30 m

Πίνακας 2.6. Σύγκριση προτύπων WSN

Κεφάλαιο 3

Προδιαγραφές ασφαλείας και μοντέλο επιθέσεων

3.1 Εισαγωγή

Τα ζητήματα ασφαλείας είναι κρίσιμης σημασίας σε ασύρματα δίκτυα όπου οι απαιτήσεις αξιοπιστίας και των απαιτήσεων που απορρέουν από αυτή (διαθεσιμότητα, εμπιστευτικότητα, φρεσκάδα, αυθεντικότητα) είναι αυξημένες, όπως για παράδειγμα σε στρατιωτικές εφαρμογές. Η ασφάλεια ενός δικτύου WSN αποσκοπεί στην αντιμετώπιση δυσμενών καταστάσεων, οι οποίες σχετίζονται με το ρίσκο ακεραιότητας δεδομένων, τις υποκλοπές και παρεμβολές μεταδιδόμενης πληροφορίας, την είσοδο και μετάδοση στο σύστημα ψεύτικων ή τροποποιημένων μηνυμάτων πληροφορίας και την απώλεια ή κατασπατάληση πόρων του δικτύου. Ένα ασφαλές και αξιόπιστο σύστημα προϋποθέτει τη συμμετοχή σε αυτό οντοτήτων (συσκευές, μηχανισμοί κλπ), οι οποίες είναι σχεδιασμένες με επίκεντρο την ασφάλεια. Κάθε παρέκκλιση από αυτή την αρχή παρέχει περιθώρια σε επιτιθέμενους να ενεργήσουν με κακόβουλο τρόπο κατά του δικτύου.

3.2 Κενά ασφαλείας

Τα ζητήματα ασφαλείας και η ανάγκη μελέτης τους προκύπτουν από τα κενά ασφαλείας που εμφανίζει ένα ασύρματο δίκτυο αισθητήρων. Τα κενά αυτά είναι αποτέλεσμα των περιορισμών και ιδιαιτεροτήτων ενός δικτύου WSN, τα οποία αναφέρονται συνοπτικά παρακάτω:

- *Αναξιόπιστο μέσο μετάδοσης:* Εξαιτίας της ασύρματης σύνδεσης των κόμβων (ασύρματο μέσο μετάδοσης), το δίκτυο είναι περισσότερο ευαίσθητο σε επιθέσεις και κακόβουλες ενέργειες τρίτων. Για το λόγο αυτό, είναι απαραίτητο να ληφθεί κατάλληλη μέριμνα, ώστε κάθε κόμβος να είναι σε θέση να τις αντιμετωπίσει. Η ανάγκη αυτή ενισχύεται από το γεγονός ότι η μετάδοση της πληροφορίας βασίζεται σε δρομολόγηση με πολλαπλά άλματα μέσω των κόμβων (multi-hop routing).

- *Περιορισμοί των κόμβων σε θέματα υπολογιστικών δυνατοτήτων, ενέργειας και αποθήκευσης:* Οι κόμβοι ενός δικτύου WSN είναι σχεδιασμένοι να είναι χαμηλού κόστους, με περιορισμένες δυνατότητες υπολογισμών και αποθήκευσης και με σημαντικούς περιορισμούς σε ενεργειακά αποθέματα. Οι περιορισμοί αυτοί θέτουν θέματα αξιοπιστίας στο δίκτυο και οι περισσότεροι αλγόριθμοι ασφάλειας δικτύων

δεν είναι συμβατοί με δίκτυα WSN, καθώς κρίνονται απαγορευτικά πολύπλοκοι, εξαιτίας αυτής της ιδιαιτερότητας.

- *Δυσκολία συγχρονισμού συσκευών δικτύου:* Ο συγχρονισμός των συσκευών έχει κρίσιμη σημασία σε ορισμένους μηχανισμούς ασφαλείας και η επίτευξη του δυσχεραίνεται εξαιτίας της δρομολόγησης πακέτων με πολλαπλά άλματα (απαίτηση συγχρονισμού κάθε συσκευής που συμμετέχει στη δρομολόγηση).
- *Απομακρυσμένη λειτουργία:* Η συνήθης εφαρμογή δικτύων WSN υλοποιείται χωρίς ανθρώπινη επίβλεψη για μεγάλο χρονικό διάστημα. Το γεγονός αυτό κάνει τα δίκτυα WSN επιρρεπή σε φυσικές επιθέσεις.

3.3 Απαιτήσεις ασφαλείας

Η έννοια της ασφάλειας ενός δικτύου WSN έγκειται (α) στην προστασία δεδομένων από αλλοιώσεις ή καταστροφή, (β) στην εξασφάλιση των πόρων του δικτύου και (γ) στην ικανότητα παροχής από τους αισθητήριους κόμβους ορθής και αξιόπιστης πληροφορίας. Από τα παραπάνω πηγάζουν και οι απαιτήσεις ασφαλείας, οι οποίες αποτελούν τις προδιαγραφές ασφαλείας του δικτύου. Οι προδιαγραφές αυτές, οι οποίες πρέπει να ικανοποιούνται τόσο κατά τη συνήθη λειτουργία όσο και σε περίπτωση κακόβουλης ενέργειας (επίθεσης), είναι οι παρακάτω:

- *Διαθεσιμότητα (availability):* Διαθεσιμότητα ορίζεται ως η δυνατότητα προσπέλασης της πληροφορίας από εξουσιοδοτημένο χρήστη και από όλους τους κόμβους του δικτύου. Η διαθεσιμότητα της πληροφορίας πρέπει να υφίσταται ακόμα και σε περιπτώσεις διαταραχών (φυσικές καταστροφές, επιθέσεις, εξάντληση πόρων), δηλαδή οι κόμβοι δεν πρέπει να τίθενται σε κατάσταση άρνησης εξυπηρέτησης (Denial of Service – DoS). Η εξασφάλιση της διαθεσιμότητας γίνεται με καταπολέμηση επιθέσεων DoS, όπως θα δούμε στη συνέχεια.
- *Εμπιστευτικότητα (confidentiality):* Εμπιστευτικότητα ορίζεται η εξασφάλιση ανάγνωσης και γνωστοποίησης ύπαρξης δεδομένων μόνο από εξουσιοδοτημένες συσκευές και αποφυγή υποκλοπής από μη εξουσιοδοτημένους χρήστες με χρήση παθητικών επιθέσεων. Με άλλα λόγια, εμπιστευτικότητα καλείται η προστασία των μεταδιδόμενων μηνυμάτων από μη εξουσιοδοτημένη αποκάλυψη. Η εξασφάλιση της εμπιστευτικότητας υλοποιείται με χρήση κρυπτογραφικών μεθόδων συμμετρικού κλειδιού, όπως θα δούμε στη συνέχεια.

- *Ακεραιότητα (integrity):* Ακεραιότητα ορίζεται η εξασφάλιση πληρότητας των δεδομένων που διακινούνται στους κόμβους του δικτύου. Σύμφωνα με αυτή, πρέπει να εξασφαλίζεται η μη αλλοίωση των δεδομένων (τροποποίηση, προσθήκη, διαγραφή ή επανεκπομπή) κατά την προώθηση τους από το αισθητήριο κόμβο (πηγή της πληροφορίας – εξουσιοδοτημένη οντότητα) προς το σταθμό βάσης.

- *Πιστοποίηση ταυτότητας – Αυθεντικότητα (authentication)*: Πιστοποίηση ταυτότητας ή αυθεντικότητα ορίζεται ως η ορθή ταυτοποίηση του επικοινωνούντα κόμβου και επιτρέπει στο κόμβο παραλήπτη να επιβεβαιώσει ότι η πληροφορία στάλθηκε από συγκεκριμένο κόμβο αποστολέα του δικτύου. Με άλλα λόγια, η κάλυψη της συγκεκριμένης απαίτησης διασφαλίζει ότι οι οντότητες (συσκευές) που συμμετέχουν στην επικοινωνία είναι αυτές που ισχυρίζονται ότι είναι.

- *Ιδιωτικότητα ή απόρρητο επικοινωνίας (privacy):* Η ιδιωτικότητα παρέχει ανωνυμία στην επικοινωνία των οντοτήτων του δικτύου. Συνδέεται με την εμπιστευτικότητα, η οποία αφορά στην απόκρυψη του περιεχομένου των διακινούμενων μηνυμάτων, αλλά επιπλέον περιλαμβάνει τις απαιτήσεις (α) προστασίας του πλαισίου επικοινωνίας (protection of the communication context), (β) ελεγχόμενης προσπέλασης στις πληροφορίες που συλλέγονται (privacy sensitive information disclosure) και (γ) ελεγχόμενης συλλογής δεδομένων (privacy sensitive information gathering). Η απαίτηση προστασίας του πλαισίου επικοινωνίας παρέχει προστασία κατά της εμφάνισης στον επιτιθέμενο πληροφοριών που αφορούν στη ταυτότητα, στην θέση, στο μέγεθος μηνυμάτων και στη μέθοδο δρομολόγησης. Οι απαιτήσεις ελεγχόμενης προσπέλασης και συλλογής δεδομένων αποσκοπούν στην υλοποίηση των συγκεκριμένων διαδικασιών με επίκεντρο την ασφάλεια.

- *Μη αποποίηση (non-repudiation):* Μη αποποίηση ορίζεται η εξασφάλιση μη άρνησης παραδοχής μιας οντότητας του δικτύου, ως προς τη συμμετοχή της στη μετάδοση πληροφορίας. Η οντότητα αυτή μπορεί να είναι τόσο ο αποστολέας (origin) όσο ο παραλήπτης (destination) της. Η συγκεκριμένη απαίτηση είναι σημαντική για τον εντοπισμό κόμβων που έχουν εκτεθεί σε κακόβουλη ενέργεια.

- *Φρεσκάδα δεδομένων (data freshness):* Φρεσκάδα δεδομένων ορίζεται ως η εξασφάλιση του γεγονότος ότι τα δεδομένα που διακινούνται είναι πρόσφατα. Η φρεσκάδα δεδομένων επιτυγχάνεται με ένα καταμετρητή χρόνου, ο οποίος εντάσσεται στα πακέτα που διακινούνται στο δίκτυο. Με τον τρόπο αυτό

αποφεύγεται η διακίνηση παλαιών δεδομένων και η σπατάλη ενέργειας από άσκοπες επανεκπομπές.

- *Ευρωστία (robustness):* Το δίκτυο WSN πρέπει να είναι ανθεκτικό σε επιθέσεις ασφαλείας. Ένα εύρωστο σε επιθέσεις δίκτυο υποβαθμίζει τις δυσμενείς συνέπειες μιας κακόβουλης ενέργειας. Κάτι τέτοιο επιτυγχάνεται με ελαχιστοποίηση της επιρροής του συνολικού δικτύου από πιθανή προσβολή ενός αριθμού κόμβων.
- *Αυτό-οργάνωση (self-organization):* Η απαίτηση αυτό-οργάνωσης και αυτό-ίασης των δικτύων WSN αποτελεί πρόκληση σε θέματα ασφαλείας καθώς οι κρυπτογραφικοί μηχανισμοί πρέπει να είναι συμβατοί με τη συγκεκριμένη απαίτηση.
- *Συγχρονισμός (synchronization):* Όπως οι περισσότερες λειτουργίες ενός δικτύου WSN, έτσι και οι μηχανισμοί ασφαλείας απαιτούν το συγχρονισμό των συσκευών που το απαρτίζουν.

3.4 Επιθέσεις ασφαλείας

Επιθέσεις ασφαλείας (security attacks) ορίζονται οι κακόβουλες ενέργειες εξωτερικών οντοτήτων με σκοπό τη πρόκληση δυσμενών συνεπειών (υποκλοπή, τροποποίηση, εισαγωγή ή διαγραφή μηνυμάτων) στη λειτουργία του δικτύου WSN. Στη βιβλιογραφία συχνά οι επιθέσεις αναφέρονται και ως απειλές. Στο Λεξικό Ασφαλείας Διαδικτύου (Internet Security Glossary) RFC 2828 [70] γίνεται διαχωρισμός των δύο εννοιών όπως παρακάτω:

Απειλή (threat): «Απειλή καλείται η δυνατότητα για παραβίαση της ασφάλειας, η οποία υπάρχει όταν μπορεί να υφίσταται κάποιο περιστατικό, δυνατότητα, ενέργεια ή συμβάν που επιτρέπει την παραβίαση της ασφαλείας με πιθανές αρνητικές συνέπειες. Με άλλα λόγια, η απειλή είναι ο πιθανός κίνδυνος να εκμεταλλευτεί κάποιος μια ευπάθεια του συστήματος».

Επίθεση (attack): «Επίθεση καλείται η προσβολή της ασφάλειας του συστήματος που προέρχεται από μια έξυπνη απειλή. Με άλλα λόγια, είναι μια ευφυής πράξη που αποτελεί σκόπιμη απόπειρα (ειδικά με την έννοια μιας μεθόδου ή τεχνικής) για την παράκαμψη των υπηρεσιών ασφαλείας και την παραβίαση ενός συστήματος».

Ταξινόμηση επιθέσεων

Οι επιθέσεις μπορούν να ταξινομηθούν σε παθητικής και ενεργητικής μορφής. Στις επιθέσεις παθητικής μορφής (passive attacks) ο επιτιθέμενος δεν εκπέμπει εντός

του δικτύου ψεύτικα ή τροποποιημένα δεδομένα, αλλά στοχεύει στην μείωση της εμπιστευτικότητας στο δίκτυο (υποκλοπή δεδομένων). Αντίθετα, στις επιθέσεις επιθετικής μορφής (active attacks), εκτός από την εμπιστευτικότητα, ο επιτιθέμενος στοχεύει επιπλέον στην ακεραιότητα και διαθεσιμότητα δεδομένων (τροποποίηση δεδομένων ή δημιουργία ψεύτικων δεδομένων, άρνηση εξυπηρέτησης).

Συνήθεις επιθέσεις παθητικής μορφής είναι η υποκλοπή (eavesdropping) και η παρακολούθηση (monitoring) μιας ασύρματης ζεύξης, με σκοπό την άντληση των μεταδιδόμενων πληροφοριών από τον επιτιθέμενο. Οι επιθέσεις ενεργητικής μορφής μπορούν να στοχεύουν στη τροποποίηση ροής ή στη δημιουργία μια ψεύτικης ροής μηνυμάτων. Οι στόχοι αυτοί μπορούν να υλοποιηθούν με μεταμφιέσεις (masquerades) συσκευών, επανεκπομπές (replays), τροποποιήσεις μηνυμάτων (modification of messages) και αρνήσεις εξυπηρέτησης (denials of service) [45,46].

Μια επιπλέον κατηγοριοποίηση των επιθέσεων ασφαλείας είναι η ταξινόμηση τους σε εσωτερικές και εξωτερικές. Οι εσωτερικές επιθέσεις προέρχονται από συσκευές του δικτύου, που έχουν κακόβουλα προσβληθεί, και είναι δυσκολότερη η ανίχνευση τους. Στις εξωτερικές μία εκτός δικτύου συσκευή παρακολουθεί τα διακινούμενα πακέτα ή εισάγει στο δίκτυο μη έγκυρα πακέτα με σκοπό τη διατάραξη των λειτουργιών του.

Οι επιθέσεις μπορούν να επίσης να ταξινομηθούν με βάση την απαίτηση ασφαλείας, στην οποία στοχεύουν. Με τον τρόπο αυτό προκύπτουν οι επιθέσεις ασφαλείας κατά της (α) αυθεντικότητας, (β) διαθεσιμότητας ή (γ) ακεραιότητας δεδομένων στο δίκτυο. Οι επιθέσεις κατά της αυθεντικότητας του δικτύου στοχεύουν σε υποκλοπή ή τροποποίηση δεδομένων και αντιμετωπίζονται με κρυπτογραφικές τεχνικές που προστατεύουν το απόρρητο, όπως θα αναφερθεί στο επόμενο κεφάλαιο. Οι επιθέσεις κατά της διαθεσιμότητας αναφέρονται ως DoS επιθέσεις (Denial of Service Threats). Τέλος, οι επιθέσεις κατά της ακεραιότητας στοχεύουν στη διοχέτευση στο δίκτυο ψευδών ή τροποποιημένων δεδομένων μέσω των αισθητήριων κόμβων. Για την επίτευξη των σκοπών του, ο επιτιθέμενος στοχεύει στις λειτουργίες του δικτύου, οι οποίες δεν υλοποιούνται μεμονωμένα αλλά σύμφωνα με την πολυεπίπεδη αρχιτεκτονική δικτύων WSN, η οποία περιγράφηκε στο Κεφάλαιο 2. Για το λόγο αυτό, στη βιβλιογραφία οι επιθέσεις αναλύονται ξεχωριστά ανά επίπεδο σχεδίασης, στο οποίο ανήκει η λειτουργία που προσβάλλεται.

3.4.1 Επιθέσεις άρνησης εξυπηρέτησης (denial of service - DoS)

Οι επιθέσεις άρνησης εξυπηρέτησης ορίζονται ως οι επιθέσεις κατά της διαθεσιμότητας του δικτύου, δηλαδή οι επιθέσεις του τύπου αυτού στοχεύουν στη διαταραχή λειτουργιών και στην εξάλειψη πόρων του δικτύου. Οι συγκεκριμένες επιθέσεις είναι δυνατό να προκαλέσουν σφάλματα υλικού και λογισμικού, εξάντληση πόρων ή συνδυασμό αυτών. Οι κυριότερες επιθέσεις DoS περιγράφονται συνοπτικά παρακάτω.

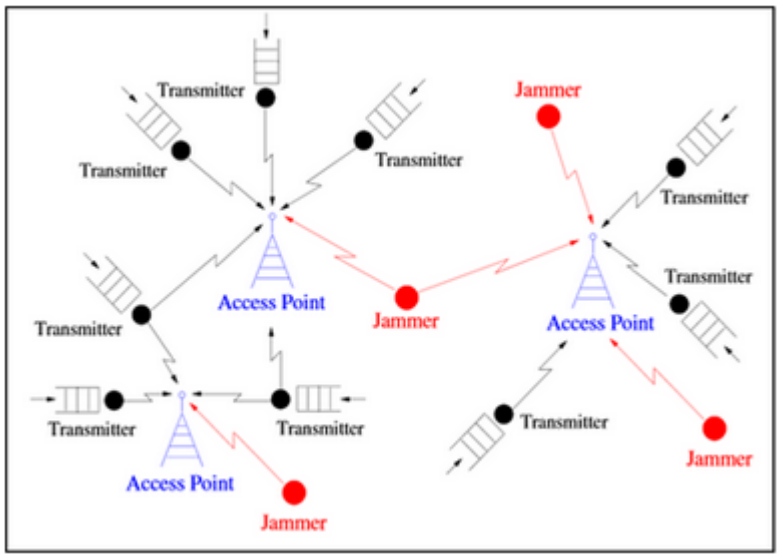
3.4.1.1 Φυσικό επίπεδο

Όπως έχει αναφερθεί στο Κεφάλαιο 2 της παρούσας εργασίας, το φυσικό επίπεδο καθορίζει τη χρησιμοποιούμενη συχνότητα λειτουργίας και την ανίχνευση και επεξεργασία σημάτων (διαμόρφωση, κωδικοποίηση δεδομένων, κρυπτογράφηση). Καθώς χρησιμοποιείται το ασύρματο μέσο μετάδοσης στο οποίο ο επιτιθέμενος έχει πρόσβαση, ένα δίκτυο WSN τίθεται επιρρεπές σε κακόβουλες ενέργειες είτε παρεμβολής, είτε τροποποίησης δεδομένων. Κακόβουλες ενέργειες που στοχεύουν σε λειτουργίες του φυσικού επιπέδου είναι οι επιθέσεις παρεμβολής (jamming attacks) και οι επιθέσεις αλλοίωσης και υποκλοπής δεδομένων (tampering attacks), οι οποίες επεξηγούνται παρακάτω.

- *Επίθεση παρεμβολής (jamming attack):* Η επίθεση παρεμβολής έχει ως στόχο την άρνηση εξυπηρέτησης. Με εκπομπή σήματος στη χρησιμοποιούμενη από το δίκτυο μπάντα συχνοτήτων, ο επιτιθέμενος δημιουργεί θόρυβο και στοχεύει στην απαγόρευση ορθής ανταλλαγής μηνυμάτων μεταξύ των κόμβων είτε σε ολόκληρο το δίκτυο, είτε σε ένα τμήμα του. Μηχανισμοί αντιμετώπισης της συγκεκριμένης επίθεσης είναι οι τεχνικές μεταπήδησης συχνότητας FHSS (Frequency – hopping spread spectrum) και διαμόρφωσης φάσματος (Code spreading). Στο Σχήμα 3.1 απεικονίζονται ελεγχόμενες από τον επιτιθέμενο συσκευές (jammers), οι οποίες εκπέμπουν εντός του δικτύου δημιουργώντας παρεμβολές στους παραλήπτες των απεσταλμένων πακέτων.

- *Επίθεση αλλοίωσης και υποκλοπής (tampering attack):* Η επίθεση αλλοίωσης και υποκλοπής δεδομένων στοχεύει στη φυσική καταστροφή των κόμβων, εκμεταλλευόμενη την απομακρυσμένη λειτουργία, και στην υποκλοπή ευαίσθητων δεδομένων, όπως κρυπτογραφικών κλειδιών, με σκοπό την ανάθεση στον επιτιθέμενο του ελέγχου του κόμβου που δέχεται τη κακόβουλη ενέργεια. Επιπλέον, ο επιτιθέμενος μπορεί να προβεί σε τροποποίηση ή αντικατάσταση κόμβου

(αναπαραγωγή κόμβου), έχοντας τον προσβεβλημένο κόμβο υπό τον έλεγχο του. Τρόποι άμυνας στην επίθεση αυτή είναι η χρήση μηχανισμών προστασίας από παραβίαση, οι μικροί σε μέγεθος κόμβοι και οι φυσική τους απόκρυψη.



Σχήμα 3.1 Επίθεση παρεμβολής (jamming)

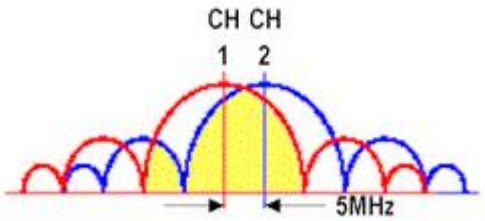
3.4.1.2 Επίπεδο ζεύξης

Το επίπεδο ζεύξης είναι υπεύθυνο για τη πολύπλεξη και ανίχνευση δεδομένων, την πρόσβαση στο μέσο μετάδοσης και τον έλεγχο λαθών. Οι επιθέσεις που στοχεύουν στις λειτουργίες του επιπέδου θέτουν σε κίνδυνο την αξιόπιστη επικοινωνία των κόμβων δημιουργώντας είτε συμφορήσεις δεδομένων, είτε εξάντληση των ενεργειακών πόρων σε σημεία του δικτύου που εκδηλώνονται.

- *Σύγκρουση δεδομένων (collision):* Η κατάσταση σύγκρουσης δεδομένων λαμβάνει χώρα όταν δύο ή περισσότεροι γειτονικοί κόμβοι αποστέλλουν ταυτόχρονα πακέτα δεδομένων στο ίδιο κανάλι επικοινωνίας. Σκοπός της επίθεσης είναι η απώλεια πακέτων, λόγω προσβολής του πρωτοκόλλου MAC, και η δημιουργία σφαλμάτων στο δίκτυο και ανάγκης επανεκπομπών. Τα πρωτόκολλα MAC που είναι επιρρεπή σε επιθέσεις σύγκρουσης δεδομένων είναι αυτά που λειτουργούν με το μηχανισμό RTS/CTS (Ready-to-Send/Clear-to-Send). Ο επιτιθέμενος τοποθετεί στην περιοχή κάλυψης του δικτύου κακόβουλους κόμβους, οι οποίοι λαμβάνουν τα μηνύματα RTS/CTS, υποδυόμενοι τους εξουσιοδοτημένους αποδέκτες. Οι κόμβοι αυτοί δεν επιβεβαιώνουν τη λήψη, με αποτέλεσμα ο κόμβος που επικοινωνεί μαζί του να αποστέλλει συνεχώς RTS πακέτα. Μέθοδοι αντιμετώπισης της επίθεσης αυτής είναι η χρήση πρωτοκόλλων MAC, που δεν

επιτρέπουν συγκρούσεις δεδομένων και η χρήση κωδίκων διόρθωσης σφαλμάτων (error-correcting codes). Στο Σχήμα 3.2 απεικονίζεται ένα παράδειγμα επίθεσης σύγκρουσης δεδομένων. Σε αυτό τα δύο σήματα επικαλύπτονται μεταξύ τους εντός ενός καναλιού επικοινωνίας. Αποτέλεσμα αυτής της επίθεσης είναι η απώλεια και των δύο σημάτων.

- *Εξάντληση ενεργειακών πόρων (exhaustion):* Η εξάντληση ενεργειακών πόρων σε ολόκληρο ή μέρος του δικτύου είναι μια DoS επίθεση η οποία είναι δυνατόν να προκληθεί από επαναλαμβανόμενες συμφορήσεις δεδομένων. Οι συμφορήσεις αυτές οδηγούν τους εκτιθέμενους κόμβους σε επαναλαμβανόμενες επανεκπομπές πακέτων, αποτέλεσμα των οποίων είναι η κατασπατάληση των ενεργειακών τους πόρων. Προστασία από τη συγκεκριμένη επίθεση προσφέρει η χρήση πολλαπλής πρόσβασης διαίρεσης χρόνου (TDMA), η δρομολόγηση πακέτων μόνο μετά από αυθεντικοποίηση του αποστολέα και η φραγή πακέτων με μέγεθος που υπερβαίνει το μέγεθος πακέτων της εφαρμογής.
- *Μεροληψία (unfairness):* Ο επιτιθέμενος μπορεί να ωθήσει το δίκτυο σε μεροληπτική συμπεριφορά των κόμβων με διαδοχική χρησιμοποίηση των επιθέσεων συμφόρησης δεδομένων και εξάντλησης ενεργειακών πόρων. Η μεροληψία εμποδίζει τη πρόσβαση των κόμβων στο κανάλι επικοινωνίας υποβαθμίζοντας την υπηρεσία και οδηγώντας σε καθυστερήσεις και απώλεια πακέτων. Υποβάθμιση των επιπτώσεων επιθέσεων μεροληψίας επιτυγχάνεται με τη χρήση μικρού μήκους πακέτων.



Σχήμα 3.2 Σύγκρουση δεδομένων (collision)

3.4.1.3 Επίπεδο δικτύου

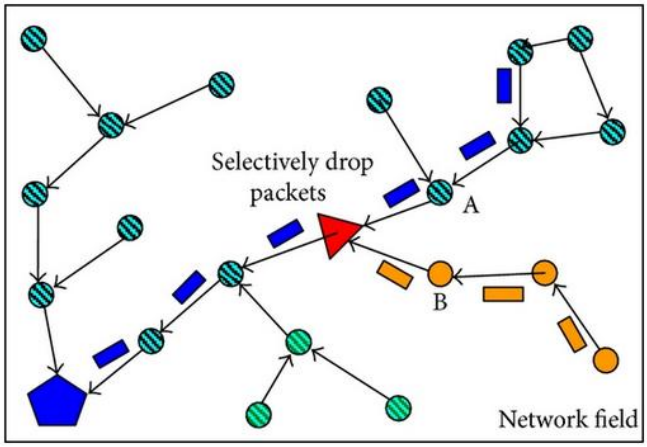
Το επίπεδο δικτύου, όπως έχει ήδη αναφερθεί είναι υπεύθυνο για τη δρομολόγηση των πακέτων εντός του δικτύου. Επομένως, οι επιθέσεις που στοχεύουν στις λειτουργίες του επιπέδου προκαλούν δυσλειτουργίες στη δρομολόγηση πακέτων μέσω των κόμβων του δικτύου.

- *Επιλεκτική προώθηση (selective forwarding):* Ένας κόμβος δικτύου WSN, λαμβάνοντας ένα πακέτο από γειτονικό του κόμβο, το προωθεί σε έναν άλλο γειτονικό του, σύμφωνα με το μονοπάτι πολλαπλών αλμάτων που έχει καθορίσει το πρωτόκολλο δρομολόγησης. Ένας κόμβος που έχει προσβληθεί θα προωθήσει επιλεκτικά ορισμένα πακέτα, απορρίπτοντας τα υπόλοιπα, τα οποία χάνονται (Σχήμα 3.3). Επέκταση της επίθεσης επιλεκτικής προώθησης θεωρείται η επίθεση μαύρης τρύπας (blackhole attack), στην οποία ο προσβεβλημένος κόμβος απορρίπτει κάθε πακέτο που λαμβάνει χωρίς να το προωθεί. Προστασία από την επιλεκτική προώθηση προσφέρει η τεχνική πολυδιαδρομικής δρομολόγησης, η οποία προσφέρει εναλλακτικές διαδρομές διακίνησης της πληροφορίας στο δίκτυο.

- *Πλαστογράφηση, τροποποίηση, ή αντικατάσταση πληροφοριών δρομολόγησης – επίθεση παραπλάνησης (misdirection):* Η πλαστογράφηση, τροποποίηση ή αντικατάσταση πληροφοριών δρομολόγησης είναι μέθοδος επίθεσης που στοχεύει στο πρωτόκολλο δρομολόγησης. Στόχος του επιτιθέμενου είναι η διατάραξη της διακίνησης μηνυμάτων εντός του δικτύου. Οι επιθέσεις αυτές δημιουργούν ανεπιθύμητους βρόχους δρομολόγησης, οι οποίοι προσελκύουν ή απωθούν τη διακίνηση μηνυμάτων και οδηγούν τόσο σε ενεργειακή εξάντληση κόμβων λόγω συνεχών εκπομπών ετεροχρονισμένων μηνυμάτων, όσο και σε καθυστερήσεις στην επικοινωνία μεταξύ του αισθητήριου κόμβου και του σταθμού βάσης.

- *Επίθεση homing:* Σε ένα δίκτυο WSN υπάρχουν κόμβοι με αυξημένες αρμοδιότητες (π.χ. συντονιστής, επικεφαλείς ομάδων, δρομολογητές). Η συγκεκριμένη επίθεση παρακολουθεί τη δρομολόγηση πακέτων στο δίκτυο και όταν ανιχνεύσει τους κρίσιμους κόμβους δίνει τη δυνατότητα στον επιτιθέμενο να ενεργήσει κακόβουλα κατά αυτών.

- *Πλαστογράφηση αναγνώρισης (acknowledgment spoofing):* Η συγκεκριμένη επίθεση λαμβάνει χώρα κατά προτύπων που προβλέπουν ανταλλαγή μηνυμάτων αναγνώρισης. Με την αλλοίωση ή αντιγραφή αυτών των μηνυμάτων, ο επιτιθέμενος στοχεύει στην δημιουργία δυσλειτουργιών στη διακίνηση πληροφοριών στο δίκτυο.

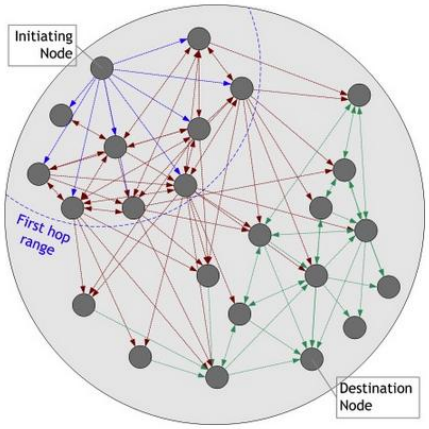


Σχήμα 3.3 Επίθεση επιλεκτικής προώθησης (selective forwarding)

3.4.1.4 Επίπεδο μεταφοράς

Το επίπεδο μεταφοράς είναι υπεύθυνο για την επίτευξη αξιόπιστης σύνδεσης μεταξύ δύο κόμβων και οι επιθέσεις που την θέτουν υπό αμφισβήτηση είναι το πλημμύρισμα και ο αποσυγχρονισμός.

- *Πλημμύρισμα (flooding):* Η επίθεση πλημμυρίσματος υλοποιείται με αποστολή επαναλαμβανόμενων πακέτων από το κακόβουλο κόμβο (initiating node) προς το κόμβο που πρόκειται να προσβληθεί (destination). Ο κόμβος που δέχεται την επίθεση διαθέτει πόρους ώστε να διατηρήσει τη σύνδεση με το κόμβο που ελέγχει ο επιτιθέμενος. Όπως απεικονίζεται στο Σχήμα 3.4 προκαλείται μεγάλος αριθμός εκπομπών, οι οποίοι εξαντλούν τους ενεργειακούς πόρους του δικτύου, και ακολούθως το χρόνο ζωής του.
- *Αποσυγχρονισμός (desynchronization):* Στόχος της επίθεσης αποσυγχρονισμού είναι η διαταραχή της σύνδεσης μεταξύ δύο τελικών συσκευών. Η επίθεση μπορεί να πραγματοποιηθεί με αποστολή πλαστογραφημένων μηνυμάτων σε μία τελική συσκευή, η οποία ζητάει την επανεκπομπή των μηνυμάτων που έχουν χαθεί.



Σχήμα 3.4 Επίθεση πλημμυρίσματος (flooding)

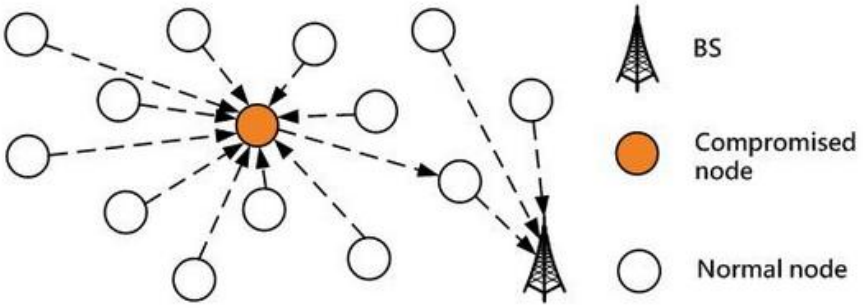
3.4.1.5 Επίπεδο εφαρμογής

Στο επίπεδο εφαρμογής οι πιθανές επιθέσεις DoS είναι η επίθεση καταπίεσης (overwhelm attack) και η επίθεση επαναπρογραμματισμού (reprogram attack).

- *Επίθεση καταπίεσης (overwhelm attack):* Η επίθεση καταπίεσης παρακινεί τους κόμβους του δικτύου να στείλουν μεγάλο όγκο πακέτων προς το σταθμό βάσης. Με τον τρόπο αυτό δημιουργείται συμφόρηση πακέτων και εξάντληση πόρων του δικτύου (ενέργεια κόμβων, εύρος ζώνης).
- *Επίθεση επαναπρογραμματισμού (reprogram attack):* Κατά τη διαδικασία απομακρυσμένου επαναπρογραμματισμού μίας συσκευής στο δίκτυο, είναι δυνατό να παρεισφρήσει κακόβουλα ο επιτιθέμενος. Στόχος της επίθεσης είναι η ανάληψη ελέγχου του κόμβου ή ενός τμήματος του δικτύου.

3.4.2 Επίθεση καταβόθρας (sinkhole)

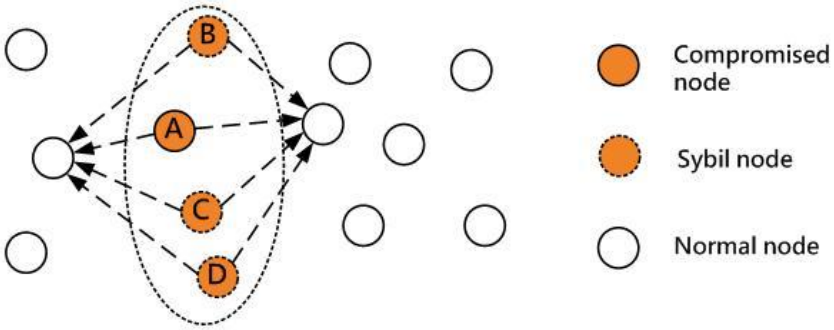
Στην επίθεση καταβόθρας (Σχήμα 3.5) ο προσβεβλημένος κόμβος διαχειρίζεται τις πληροφορίες δρομολόγησης που έχει υποκλέψει από το δίκτυο με σκοπό να γίνει ελκυστικός στους γειτονικούς του κόμβους για λήψη πακέτων από αυτούς. Ως αποτέλεσμα αυτού οι γειτονικοί κόμβοι επιλέγουν τον συγκεκριμένο κόμβο για την προώθηση των μηνυμάτων που λαμβάνουν. Με τον τρόπο αυτό ο επιτιθέμενος μπορεί να ελέγξει τη ροή πληροφοριών εντός του δικτύου μέσω του προσβεβλημένου κόμβου.



Σχήμα 3.5 Επίθεση καταβόθρας (sinkhole)

3.4.3 Σιβυλλική επίθεση (sybil attack)

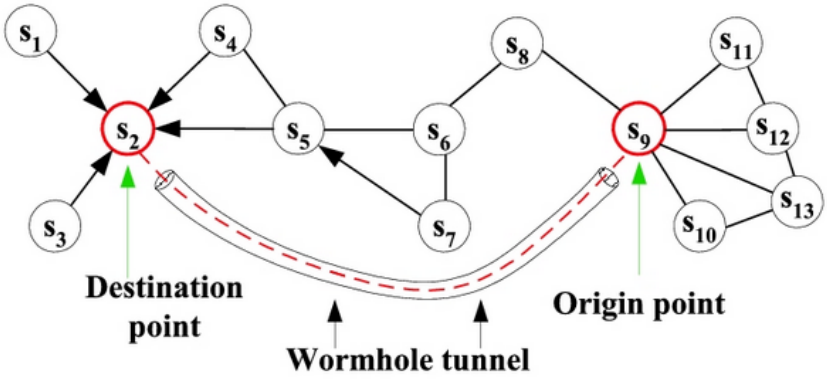
Η σιβυλλική επίθεση (Σχήμα 3.6) σκοπεύει στο να δώσει πολλαπλές ταυτότητες σε έναν κόμβο. Με τον τρόπο αυτό ένας προσβεβλημένος κόμβος μπορεί να μιμηθεί ταυτότητες άλλων κόμβων ή να αναπαράγει νέες ψεύτικες ταυτότητες. Οι ψεύτικες ταυτότητες υλοποιούν ισάριθμους εικονικούς κόμβους οι οποίοι καλούνται σιβυλλικοί κόμβοι. Οι κόμβοι αυτοί συμμετέχουν κανονικά στις λειτουργίες του δικτύου WSN, αν και αποτελούν στη πραγματικότητα μόνο μία συσκευή. Αποτέλεσμα της επίθεσης είναι η μεγαλύτερη ενεργειακή επιβάρυνση της προσβεβλημένης συσκευής σε σύγκριση με τις υπόλοιπες συσκευές του δικτύου.



Σχήμα 3.6 Σιβυλλική επίθεση (Sybil attack)

3.4.4 Σκουληκότρυπες (wormholes)

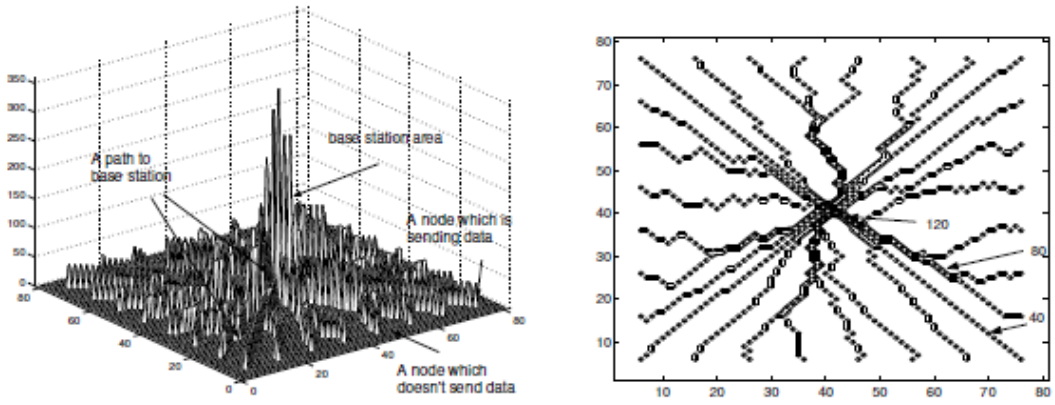
Η επίθεση σκουληκότρυπας (Σχήμα 3.7) χρησιμοποιείται από τον επιτιθέμενο με σκοπό την παραπλάνηση δύο απομακρυσμένων κόμβων ως προς την εγγύτητα τους, έτσι ώστε αυτοί να αναγνωρίζονται ως γειτονικοί. Οι συγκεκριμένη επίθεση μπορεί να χρησιμοποιηθεί σε συνδυασμό με άλλες επιθέσεις, όπως την επιλεκτική προώθηση, την επίθεση καταβόθρας και τη σιβυλλική επίθεση.



Σχήμα 3.7 Επίθεση σκουληκότρυπας (wormhole)

3.4.5 Επίθεση ανάλυσης κίνησης (traffic analysis)

Σκοπός της επίθεσης ανάλυσης κίνησης είναι η ανίχνευση και απενεργοποίηση του σταθμού βάσης του δικτύου WSN. Η ανίχνευση του από τον επιτιθέμενο του δίνει τη δυνατότητα να προβεί κακόβουλα εναντίον του. Η ανάλυση της κίνησης υλοποιείται με δύο τρόπους. Σύμφωνα με το πρώτο, γίνεται εκμετάλλευση του γεγονότος ότι οι κόμβοι πλησίον των σταθμών βάσης διαχειρίζονται περισσότερα πακέτα. Με μία επίθεση καταγραφής ρυθμού (rate monitoring attack) [56], ο επιτιθέμενος εντοπίζει τους κόμβους που στέλνουν περισσότερα πακέτα και εντοπίζει τελικά το σταθμό βάσης (Σχήμα 3.8). Σύμφωνα με το δεύτερο, ο επιτιθέμενος παράγει ανιχνεύσιμα από τους αισθητήριους κόμβους γεγονότα και παρακολουθεί προς τα πού γίνεται η αποστολή πακέτων. Η επίθεση αυτή καλείται επίθεση συσχέτισης χρόνου (time correlation attack) [56].



Σχήμα 3.8. Εντοπισμός θέσης σταθμού βάσης με επίθεση καταγραφής ρυθμού

3.4.6 Επίθεση HELLO flood

Παρόμοια με τις σκουληκότρυπες, η συγκεκριμένη επίθεση χρησιμοποιεί κακόβουλο κόμβο ο οποίος εκπέμπει σε μεγαλύτερη ισχύ και παραπλανεί

απομακρυσμένους κόμβους, οι οποίοι τον αναγνωρίζουν ως γειτονικό. Με τον τρόπο αυτό επιτυγχάνεται έλεγχος της δρομολόγησης πακέτων από τον επιτιθέμενο.

3.4.7 Επιθέσεις κατά του απορρήτου

Οι επιθέσεις κατά του απορρήτου στοχεύουν στην εξαγωγή ευαίσθητων δεδομένων που αφορούν στη λειτουργία του δικτύου ή στα δεδομένα που διακινούνται. Επιθέσεις εναντίον του απορρήτου θεωρούνται το κρυφάκουσμα (monitoring and eavesdropping), η ανάλυση κίνησης και η παραλλαγή (camouflage).

- *Παρατήρηση και κρυφάκουσμα (monitoring and eavesdropping):* Η συγκεκριμένη επίθεση στοχεύει στην μη εξουσιοδοτημένη ακρόαση (υποκλοπή) διακινούμενων δεδομένων και πληροφοριών ελέγχου του δικτύου.
- *Επίθεση ανάλυσης κίνησης (traffic analysis):* Η επίθεση ανάλυσης κίνησης αναλύει τη κίνηση στο δίκτυο και με τον τρόπο αυτό εντοπίζει τη θέση του σταθμού βάσης, όπως αναφέρθηκε παραπάνω.
- *Επίθεση παραλλαγής (camouflage):* Με την επίθεση παραλλαγής, ο επιτιθέμενος εισάγει στο δίκτυο ελεγχόμενους από αυτόν κόμβους, οι οποίοι προσελκύουν πακέτα με σκοπό την εξαγωγή πληροφοριών απορρήτου για το δίκτυο.

3.4.8 Φυσικές επιθέσεις – Αναπαραγωγή κόμβου

Η φυσική επίθεση στοχεύει στη φυσική καταστροφή του κόμβου από τον επιτιθέμενο. Οι κόμβοι που δέχονται φυσική επίθεση είναι δυνατόν να αντικατασταθούν από τον επιτιθέμενο με κόμβους που είναι προγραμματισμένοι από αυτόν και βρίσκονται υπό τον έλεγχο του (επίθεση αναπαραγωγής κόμβου). Με τον τρόπο αυτό ο επιτιθέμενος μπορεί να θέσει υπό τον έλεγχο του ένα τμήμα του δικτύου και να εξαπολύει μέσω αυτού επιθέσεις προς το υπόλοιπο δίκτυο. Προστασία από φυσικές επιθέσεις μπορεί να πραγματοποιηθεί με φυσική απόκρυψη των κόμβων στο χώρο ανάπτυξης του δικτύου.

3.5 Σύνοψη

Στο παρόν κεφάλαιο έγινε αναφορά στην ασφάλεια δικτύων WSN και συγκεκριμένα στις απαιτήσεις και στα κενά ασφαλείας τους. Επιπλέον, έγινε αναφορά στις πιθανές επιθέσεις ασφαλείας, οι οποίες θέτουν σε κίνδυνο την ασφάλεια και αξιοπιστία ενός δικτύου WSN. Οι συγκεκριμένες κακόβουλες ενέργειες

στοιχειοθετούν το μοντέλο επιθέσεων ενός δικτύου WSN. Στον Πίνακα 3.1 γίνεται ανασκόπηση των επιθέσεων ενός δικτύου WSN με αναφορά στους στόχους τους και τις προδιαγραφές που θέτουν υπό αμφισβήτηση.

Επίθεση	**Επίπεδο σχεδίασης**	**DoS**	**Προδιαγραφή**	**Στόχος επίθεσης**
Παρεμβολή (jamming)	Φυσικό επίπεδο	*	Διαθεσιμότητα Ακεραιότητα	Πλημμύρισμα τμήματος του δικτύου με θόρυβο
Αλλοίωση και υποκλοπή (tampering)		*	Διαθεσιμότητα, Ακεραιότητα Αυθεντικότητα	Καταστροφή κόμβων και υποκλοπή ευαίσθητων δεδομένων
Φυσική επίθεση			Διαθεσιμότητα	Καταστροφή κόμβου
Αναπαραγωγή κόμβου			Αυθεντικότητα	Αντικατάσταση κόμβου με κόμβο υπό τον έλεγχο του επιτιθέμενου
Σύγκρουση δεδομένων (collision)	Επίπεδο ζεύξης	*	Διαθεσιμότητα	Απώλεια δεδομένων
Εξάντληση ενεργειακών πόρων (exhaustion)		*		Εξάντληση ενεργειακών πόρων
Μεροληψία (unfairness)		*		Απώλεια δεδομένων
Καταβόθρα (sinkhole)	Επίπεδο ζεύξης, δικτύου		Αυθεντικότητα	Έλεγχος δρομολόγησης
Σκουληκότρυπα			Αυθεντικότητα	-//-
Παραπλάνηση (misdirection)	Επίπεδο δικτύου	*	Διαθεσιμότητα Ακεραιότητα	-//-
Επιλεκτική προώθηση (selective forwarding)		*	Διαθεσιμότητα Ακεραιότητα	Απώλεια δεδομένων
Μαύρη τρύπα (black hole)		*		-//-
HELLO flood			Αυθεντικότητα	Έλεγχος δρομολόγησης

Σιβυλλική επίθεση (sybil attack)				Δυσλειτουργία στη ταυτοποίηση κόμβου και έλεγχος δρομολόγησης
Επίθεση homing		*	Διαθεσιμότητα	Ανίχνευση κόμβων κρίσιμης σημασίας
Πλαστογράφηση αναγνώρισης (acknowledgment spoofing)		*	Διαθεσιμότητα, Ακεραιότητα	Διακίνηση ψευδών μηνυμάτων
Πλημμύρισμα (flooding)	Επίπεδο μεταφοράς	*	Διαθεσιμότητα Ακεραιότητα	Εξάντληση πόρων
Αποσυγχρονισμός (desynchronization)		*		Δυσλειτουργίες σύνδεσης
Καταπίεση (overwhelm)	Επίπεδο εφαρμογής	*		Εξάντληση πόρων δικτύου
Επαναπρογραμματισμός (reprogram)		*		Έλεγχος τμήματος δικτύου
Παρακολούθηση και κρυφάκουσμα (monitoring and eavesdropping)			Αυθεντικότητα	Υποκλοπή κρίσιμων πληροφοριών
Ανάλυση κίνησης (traffic analysis)				Ανίχνευση κόμβων κρίσιμης σημασίας
Παραλλαγή (camouflage)				Εξαγωγή πληροφοριών απορρήτου

Πίνακας 3.1 Στόχοι επιθέσεων δικτύων WSN

Κεφάλαιο 4

Μηχανισμοί Ασφάλειας Ασύρματων Δικτύων Αισθητήρων

4.1 Εισαγωγή

Στο προηγούμενο κεφάλαιο αναφέραμε τις επιθέσεις που θέτουν υπό αμφισβήτηση την ασφάλεια επικοινωνιών σε ένα δίκτυο WSN. Οι στόχοι του επιτιθέμενου αφορούν, όπως είδαμε, στη δημιουργία δυσχερειών ως προς την ικανοποίηση των προδιαγραφών ασφάλειας του δικτύου. Με τον τρόπο αυτό η κακόβουλη ενέργεια θίγει τόσο την ασφάλεια όσο και την αξιοπιστία του δικτύου. Η αξιοπιστία και η ασφάλεια έχουν κρίσιμη σημασία σε στρατιωτικές εφαρμογές και για το λόγο αυτό είναι απαραίτητη η πρόβλεψη μηχανισμών ασφαλείας, οι οποίοι λειτουργούν ως αντίμετρα στις επιθέσεις. Οι περισσότεροι μηχανισμοί ασφαλείας χρησιμοποιούν περισσότερους από έναν αλγορίθμους ή πρωτόκολλα επικοινωνίας, με αποτέλεσμα την αύξηση της πολυπλοκότητας. Επιπρόσθετα, είναι απαραίτητο οι συσκευές του δικτύου να χρησιμοποιούν μυστικά κλειδιά κρυπτογράφησης, γεγονός που περιπλέκει επιπλέον το σχεδιασμό, ως προς τη διακίνηση και προστασία αυτής της μυστικής πληροφορίας.

Ένας μηχανισμός ασφαλείας οφείλει να έχει κάποια χαρακτηριστικά, ώστε να κριθεί κατάλληλος για εφαρμογή σε ένα δίκτυο WSN. Τα χαρακτηριστικά αυτά είναι τα κάτωθι:

- *Ασφάλεια:* Ο μηχανισμός ασφαλείας οφείλει να συμμορφώνεται στις απαιτήσεις (προδιαγραφές) ασφαλείας, οι οποίες έχουν αναφερθεί στο προηγούμενο κεφάλαιο.
- *Ανθεκτικότητα:* Ο μηχανισμός ασφαλείας οφείλει να μην επηρεάζεται από ενδεχόμενη προσβολή κόμβων (ευρωστία) και να είναι σε θέση να συνεχίσει το έργο του.
- *Εξοικονόμηση ενέργειας:* Σε ένα δίκτυο WSN, όπου στόχος είναι η μεγιστοποίηση του χρόνου ζωής του, ο μηχανισμός ασφαλείας οφείλει να είναι συμβατός με αυτή την απαίτηση. Η απαίτηση αυτή ισχυροποιείται, αν λάβουμε υπόψη τους περιορισμούς σε ενεργειακούς πόρους, που έχουν οι κόμβοι ενός δικτύου WSN.

- *Ευελιξία:* Η διαχείριση κρυπτογραφικών κλειδιών και συνολικά ο μηχανισμός ασφαλείας πρέπει να χαρακτηρίζονται από ευελιξία στη χρήση σε διαφόρους τύπους ανάπτυξης δικτύου.
- *Δυνατότητα κλιμάκωσης:* Καθώς ένα δίκτυο WSN έχει τη δυνατότητα κλιμάκωσης, αυτή θεωρείται απαραίτητο χαρακτηριστικό ενός μηχανισμού ασφαλείας.
- *Ανοχή σε σφάλματα:* Ο μηχανισμός ασφαλείας οφείλει να μπορεί να παρέχει ασφάλεια στο δίκτυο ακόμα και με το ενδεχόμενο ύπαρξης σφαλμάτων σε αυτό, ή καταστάσεων που τα προκαλούν (π.χ. καταστροφή κόμβων ή παρουσία κακόβουλης ενέργειας).

4.2 Ανίχνευση παρείσφρησης (intrusion detection)

Οι μηχανισμοί ασφαλείας και ειδικότερα οι μηχανισμοί ασφαλούς δρομολόγησης και συνάθροισης δεδομένων, από μόνοι τους, δεν είναι αρκετοί ώστε να εξασφαλίσουν την πλήρη κάλυψη των απαιτήσεων ασφαλείας ενός δικτύου WSN. Το ενδεχόμενο εισαγωγής ψευδών δεδομένων από έναν επιτιθέμενο προωθεί την ανάγκη ανάπτυξης μηχανισμών ανίχνευσης παρεισφρήσεων και αντίδρασης σε αυτές.

Ένα σύστημα ανίχνευσης παρείσφρησης (Intrusion Detection System – IDS) βασίζεται στην παρακολούθηση του δικτύου και στον εντοπισμό παρατηρήσεων που διαφοροποιούνται από ένα φυσιολογικό πλαίσιο συμπεριφορών [42],[43]. Τα συστήματα ανίχνευσης παρείσφρησης ταξινομούνται σε δύο κατηγορίες: (α) βασισμένα σε κανόνες (rule – based) [70] και (β) βασισμένα στην ανίχνευση στατιστικών ανωμαλιών (anomaly – based) [70] συστήματα ανίχνευσης. Τα συστήματα IDS της πρώτης κατηγορίας είναι σχεδιασμένα ώστε να ανιχνεύουν γνωστά πρότυπα παρεισφρήσεων, ενώ τα anomaly – based συστήματα IDS κινούνται προς τη κατεύθυνση ανίχνευσης άγνωστης μορφής ανωμαλιών στο δίκτυο. Τα συγκεκριμένα συστήματα ενεργοποιούν κάποιου είδους ανάδραση (συναγερμό) στο δίκτυο με στόχο την αντίδραση και τη καταπολέμηση του προβλήματος. Τα rule-based συστήματα IDS χαρακτηρίζονται από χαμηλότερο ποσοστό ψευδών συναγερμών σε σύγκριση με τα αντίστοιχα anomaly – based, με αντίτιμο όμως το χαμηλότερο ποσοστό ανίχνευσης παρεισφρήσεων (μικρότερη αποτελεσματικότητα ανίχνευσης).

Στα δίκτυα WSN, εξαιτίας των υπολογιστικών, αποθηκευτικών και ενεργειακών περιορισμών, δεν βρίσκει εφαρμογή η ενημέρωση των κόμβων ως προς ένα φυσιολογικό πλαίσιο συμπεριφορών του δικτύου, καθώς κρίνεται μη αποδοτική ενεργειακά. Για το λόγο αυτό αποτελεί πρόκληση η σχεδίαση μηχανισμών ανίχνευσης παρεισφρήσεων σε δίκτυα WSN. Στη βιβλιογραφία αναφέρονται λύσεις όπως οι τεχνικές IHOP [63], LIDS [64], SEF [67] καθώς και οι τεχνικές που περιγράφονται στα άρθρα [65],[66].

Η τεχνική IHOP (Interleaved Hop-by-Hop Authentication) βρίσκει εφαρμογή σε δίκτυα ιεραρχικής δρομολόγησης και εξασφαλίζει ότι ο σταθμός βάσης θα ανιχνεύσει ψευδή δεδομένα που έχουν εισαχθεί στο δίκτυο με την προϋπόθεση ότι δεν ενεργούν κακόβουλα περισσότεροι από έναν αριθμό κόμβοι. Η συγκεκριμένη τεχνική καθορίζει ότι (α) κάθε κόμβος μοιράζεται ένα κρυπτογραφικό κλειδί με το σταθμό βάσης, (β) κάθε κόμβος γνωρίζει τους γειτονικούς του κόμβους (απόσταση ενός άλματος) και μοιράζεται με αυτούς κρυπτογραφικά κλειδιά και (γ) κάθε κόμβος μπορεί να καθορίσει κρυπτογραφικό κλειδί και με μη γειτονικούς κόμβους, εφόσον χρειαστεί. Επίσης, το σύστημα LIDS (Local Intrusion Detection System) είναι η βάση του μηχανισμού που περιγράφεται στο [64]. Ο μηχανισμός αυτός, αν και έχει σχεδιαστεί για εφαρμογή σε ad-hoc δίκτυα, είναι συμβατός με δομημένα δίκτυα WSN [43].

Ο μηχανισμός SEF (Statistical En-route Filtering) αποσκοπεί στην ανίχνευση και απόρριψη ψευδών δεδομένων μέσω της διαδικασίας προώθησης μηνυμάτων προς το σταθμό βάσης. Ο μηχανισμός λειτουργεί με την υπόθεση ότι το ψευδές γεγονός γίνεται αντιληπτό από έναν αριθμό αισθητήριων κόμβων, οι οποίοι λειτουργούν συνεργατικά για την ανίχνευση και την αντιμετώπιση της επίθεσης. Σύμφωνα με το άρθρο [67] είναι δυνατή η απόρριψη περισσότερο από το 70% ψευδών δεδομένων μέσα στα επόμενα πέντε άλματα και η επίτευξη σημαντικής εξοικονόμηση ενέργειας.

Στο άρθρο [65] προτείνονται τρεις αρχιτεκτονικές ανίχνευσης παρείσφρησης. Η πρώτη είναι η stand-alone αρχιτεκτονική, στην οποία κάθε κόμβος ενεργεί αυτόνομα προς τη κατεύθυνση ανίχνευσης κακόβουλης ενέργειας. Η δεύτερη προσέγγιση είναι η κατανεμημένη και συνεργατική αρχιτεκτονική. Στην αρχιτεκτονική αυτή κάθε κόμβος έχει αρμοδιότητες ανίχνευσης τοπικών απειλών ασφαλείας, αλλά συνεργάζεται με τους γειτονικούς του στην ανταλλαγή δεδομένων που αφορούν μια ενδεχόμενη παρείσφρηση. Επίσης, γίνεται αναφορά στην ιεραρχική αρχιτεκτονική, η οποία είναι κατάλληλη για ιεραρχικά δομημένα δίκτυα WSN. Τέλος, το άρθρο [66]

αναφέρει ένα μηχανισμό, ο οποίος στοχεύει στην εξακρίβωση για το αν ένας ή περισσότεροι κόμβοι του δικτύου έχουν προσβληθεί από κακόβουλο εισβολέα. Για το σκοπό αυτό οι γειτονικοί κόμβοι ανταλλάσσουν μηνύματα, αποτέλεσμα των οποίων καθορίζει την ανίχνευση ή μη παρείσφρησης στο δίκτυο.

4.3 Αντιμετώπιση επιθέσεων – αντίμετρα

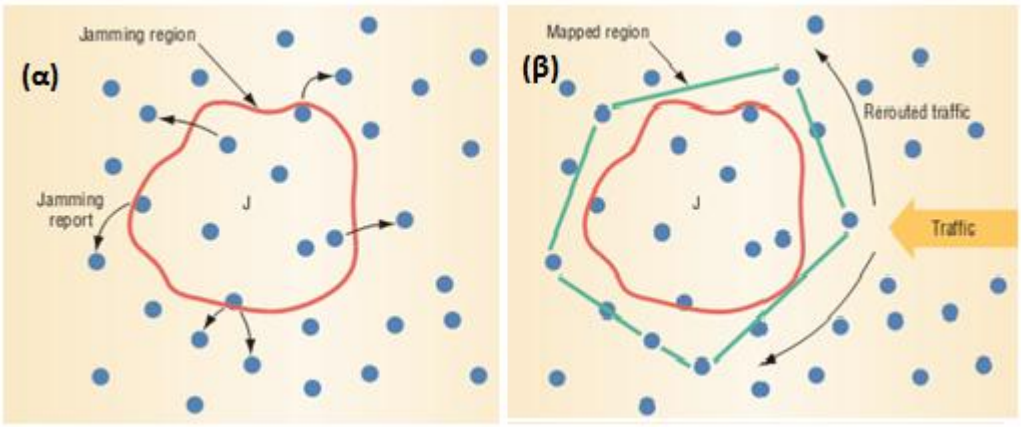
Οι μηχανισμοί ασφαλείας, οι οποίοι στοχεύουν στην αντιμετώπιση επιθέσεων παθητικής μορφής έχουν χαρακτήρα περισσότερο αποτροπής, παρά ανίχνευσης. Αυτό συμβαίνει, διότι οι συγκεκριμένες επιθέσεις είναι δύσκολο να ανιχνευθούν, καθώς ο επιτιθέμενος δεν προκαλεί τροποποιήσεις στα μεταδιδόμενα πακέτα. Η αντιμετώπιση των επιθέσεων παθητικής μορφής πραγματοποιείται κυρίως με αλγορίθμους κρυπτογράφησης, όπως θα δούμε στη συνέχεια. Αντίθετα με τις επιθέσεις αυτές, στις επιθέσεις ενεργητικής μορφής η αντιμετώπιση έχει περισσότερο χαρακτήρα ανίχνευσης της επίθεσης, με σκοπό την ανάκαμψη του δικτύου από δυσχέρειες, οι οποίες προκλήθηκαν από αυτή. Ωστόσο, η αποτροπή μιας ενεργητικής επίθεσης απαιτεί τη συνεχή φυσική προστασία όλων των επικοινωνιακών δομών και καναλιών, γεγονός που καθιστά την επίτευξη της δυσκολότερη.

4.3.1 Αντιμετώπιση επιθέσεων DoS

Η αναφορά στις μεθόδους αντιμετώπισης επιθέσεων DoS γίνεται με βάση τη πολυεπίπεδη αρχιτεκτονική του δικτύου WSN, όπως παρουσιάζεται παρακάτω.

4.3.1.1 Φυσικό επίπεδο

Η επίθεση παρεμβολής (jamming) μπορεί να αντιμετωπιστεί με τις τεχνικές μεταπήδησης συχνότητας FHSS (Frequency – hopping spread spectrum) και διαμόρφωσης φάσματος (Code spreading). Η τεχνική διαμόρφωσης φάσματος χαρακτηρίζεται από μεγαλύτερη πολυπλοκότητα και είναι απαιτητικότερη σε ενεργειακούς και υπολογιστικούς πόρους των κόμβων. Για το λόγο αυτό, είναι λιγότερο δημοφιλής λύση σε δίκτυα WSN. Επίσης στο [50] γίνεται αναφορά σε μία επιπλέον τεχνική αντιμετώπισης παρεμβολών. Η λογική της τεχνικής είναι ο αποκλεισμός, από το πλάνο δρομολόγησης, της περιοχής που έχει προσβληθεί από την επίθεση παρεμβολής. Σημαντική είναι η συμβολή των κόμβων που έχουν προσβληθεί και των γειτονικών στην ανίχνευση της επίθεσης και στη συνέχεια στην ενημέρωση του σταθμού βάσης.



Σχήμα 4.1. Τεχνική αντιμετώπισης επίθεσης παρεμβολής σύμφωνα με [11], (α) οι προσβεβλημένοι κόμβοι καθώς και οι γειτονικοί τους επιχειρούν ενημέρωση της κατάστασης τους (jamming report), (β) αποκλεισμός προσβεβλημένης περιοχής

Η τεχνική μεταπήδησης συχνότητας χρησιμοποιεί ένα στενό φασματικά φέρον σήμα, το οποίο μεταβάλλει συνεχώς την κεντρική του συχνότητα, σύμφωνα με μια ψευδό-τυχαία ακολουθία. Το σήμα μεταδίδεται σε μια συχνότητα για σύντομη χρονική διάρκεια και έπειτα μεταπηδά σε μια άλλη. Ο αλγόριθμος για τη μεταπήδηση (hopping) της συχνότητας είναι εκ των προτέρων γνωστός, τόσο στον πομπό, όσο και στο δέκτη. Εάν το σήμα ληφθεί από κάποιον μη εξουσιοδοτημένο δέκτη, ερμηνεύεται ως μικρής διάρκειας θόρυβος και αγνοείται. Ο επιτιθέμενος είναι αδύνατο να προβλέψει την ακολουθία μεταπήδησης συχνοτήτων και επομένως δεν μπορεί να δημιουργήσει παρεμβολή, η οποία να συμβαδίζει με αυτή. Ωστόσο, επειδή το διαθέσιμο φάσμα είναι περιορισμένο, ο επιτιθέμενος θα επιτύχει το σκοπό του, εάν παρεμβάλλει σε όλο το διαθέσιμο εύρος συχνοτήτων.

Η αντιμετώπιση επιθέσεων αλλοίωσης ή υποκλοπής γίνεται με μηχανισμούς προστασίας παραβίασης των συσκευών που απαρτίζουν το δίκτυο. Η επιτυχία εξαρτάται από την ακρίβεια και την πληρότητα που έλαβαν υπόψη οι σχεδιαστές για πιθανές απειλές, τους πόρους που διατίθενται για το σχεδιασμό, την κατασκευή και την δοκιμή, και την ευφυΐα και αποτελεσματικότητα των εισβολέων. Επιπλέον προστασία από τέτοιου είδους επιθέσεις προσφέρει η φυσική απόκρυψη των συσκευών στην περιοχή εφαρμογής τους, καθώς και οι μηχανισμοί απενεργοποίησης της συσκευής σε περίπτωση παραβίασης (self-termination).

4.3.1.2 Επίπεδο ζεύξης

Η επίθεση σύγκρουσης δεδομένων αντιμετωπίζεται εν μέρει με χρήση κωδίκων διόρθωσης λαθών (error-correcting codes). Οι κώδικες αυτοί λειτουργούν αποδοτικά σε μικρής έκτασης συγκρούσεις, αν και προσθέτουν πολυπλοκότητα. Σε μεγαλύτερης έκτασης προσβολή στο δίκτυο, οι κώδικες αυτοί δεν λειτουργούν αποδοτικά κάτι που αποτελεί κενό ασφαλείας ενός δικτύου WSN. Αποτελεσματικότερη είναι η αποφυγή χρήσης πρωτοκόλλων MAC που λειτουργούν με το σχήμα RTS/CTS.

Η αντιμετώπιση της επίθεσης εξάντλησης ενεργειακών πόρων μπορεί να γίνει με χρήση πολλαπλής πρόσβασης διαίρεσης χρόνου (TDMA). Σύμφωνα με αυτή, οι κόμβοι διαχωρίζονται στο πεδίο του χρόνου με εκχώρηση σε κάθε έναν εξ' αυτών χρονοθυρίδων (timeslots). Κρίσιμη είναι η επίτευξη συγχρονισμού των κόμβων, η οποία αν δεν επιτευχθεί δημιουργείται παρεμβολή μεταξύ τους. Επιπλέον, για την αντιμετώπιση της συγκεκριμένης επίθεσης μπορεί να προβλεφθεί η δρομολόγηση πακέτων μόνο μετά από αυθεντικοποίηση του αποστολέα και η φραγή πακέτων με μέγεθος που υπερβαίνει το μέγεθος πακέτων της εφαρμογής.

Για την αντιμετώπιση της επίθεσης μεροληψίας χρησιμοποιούνται μικρά πλαίσια δεδομένων, έτσι ώστε κάθε κόμβος να κάνει προσπέλαση στο κανάλι μόνο για ένα μικρό χρονικό διάστημα. Ωστόσο, τα μικρά πλαίσια συχνά μειώνουν την αποδοτικότητα και είναι επιρρεπή σε επιπλέον επίθεση, καθώς ο επιτιθέμενος πιθανόν να επιχειρήσει να επανεκπέμψει γρήγορα, αντί να περιμένει για ένα τυχαίο χρονικό διάστημα.

4.3.1.3 Επίπεδο δικτύου

Η αποτελεσματικότερη αντιμετώπιση των επιθέσεων, που αφορούν στο επίπεδο δικτύου βασίζεται στο εφαρμοζόμενο πρωτόκολλο δρομολόγησης. Το πρωτόκολλο δρομολόγησης οφείλει να παρακολουθεί τη λειτουργία του δικτύου, εντοπίζοντας μη φυσιολογικές συμπεριφορές και απομονώνοντας τους κόμβους που τις προκαλούν. Η απομόνωση αυτή επιτυγχάνεται με το καθορισμό εναλλακτικών μονοπατιών δρομολόγησης (πολυδιαδρομική δρομολόγηση). Επιπλέον εξασφάλιση προσφέρεται με την συμμετοχή στη δρομολόγηση μόνο εξουσιοδοτημένων κόμβων. Τέλος, ο πλεονασμός (redundancy) μεταδιδόμενης πληροφορίας, ο οποίος μπορεί να δημιουργείται είτε λόγω εγγύτητας των κόμβων, είτε σκόπιμα με εκπομπή επιπλέον πακέτων, διευκολύνει την αντιμετώπιση κακόβουλων ενεργειών.

4.3.1.4 Επίπεδο μεταφοράς

Τεχνική αντιμετώπισης της επίθεσης πλημμυρίσματος (flooding) είναι η τεχνική client puzzles [50]. Τα client puzzles διαμοιράζονται από το σταθμό βάσης στο δίκτυο και η επίλυση τους από κάθε κόμβο συνεπάγεται ότι η σύνδεση είναι έγκυρη. Ο επιτιθέμενος θα πρέπει να είναι σε θέση να τα επιλύσει, ώστε να ενεργήσει κακόβουλα εναντίον του δικτύου. Επιπλέον αντίμετρα προσφέρουν μέτρα περιορισμού αριθμού συνδέσεων και μηχανισμοί αυθεντικοποίησης.

Αντίμετρο της επίθεσης αποσυγχρονισμού είναι η πιστοποίηση (αυθεντικοποίηση) όλων των πακέτων που ανταλλάσσονται, συμπεριλαμβανομένων όλων των πεδίων ελέγχου τις επικεφαλίδας του πρωτοκόλλου μεταφοράς. Υποθέτοντας ότι ο αντίπαλος δεν μπορεί να παρακάμψει τον μηχανισμό ελέγχου ταυτότητας, οι συμμετέχοντες στην επικοινωνία κόμβοι θα μπορούν να εντοπίσουν και στην συνέχεια να αγνοήσουν τα κακόβουλα πακέτα.

4.3.2 Αντίμετρα – Επίθεση καταβόθρας

Τα κρυπτογραφικά πρωτόκολλα δρομολόγησης RESIST-0 και RESIST-1 (RESIlient and Simple Topology-based reconfiguration protocols) [57] παρέχουν ευρωστία σε δίκτυα WSN κατά των επιθέσεων καταβόθρας, με αντίτιμο όμως την αύξηση πολυπλοκότητας. Επίσης το πρωτόκολλο δρομολόγησης Mint-Route [52],[58],[59] παρέχει δυνατότητα ανίχνευσης και καταπολέμησης της συγκεκριμένης επίθεσης. Στο συγκεκριμένο πρωτόκολλο, κάθε κόμβος υπολογίζει την ποιότητα της ζεύξης (link quality) με τους γειτονικούς του κόμβους και σύμφωνα με αυτή, υλοποιείται ένα «δέντρο δρομολόγησης» προς το σταθμό βάσης. Η ποιότητα της ζεύξης μπορεί να μετρηθεί είτε με το ποσοστό πακέτων που χάνονται, είτε με βάση το σηματοθορυβικό λόγο (SNR) που επιτυγχάνεται. Για την επίτευξη του δέντρου δρομολόγησης κάθε κόμβος αποστέλλει περιοδικά στο σταθμό βάσης πακέτο ενημέρωσης (route update packet) με αυτές τις πληροφορίες. Επίσης, κάθε κόμβος αποθηκεύει τις ταυτότητες των γειτονικών του κόμβων στον πίνακα γειτονικών κόμβων (neighbor table), ο οποίος ανανεώνεται περιοδικά, αναγνωρίζοντας το γειτονικό κόμβο με τον οποίο υλοποιείται ποιοτικότερη σύνδεση (υψηλότερη ποιότητα ζεύξης).

4.3.3 Αντίμετρα – Σιβυλλική επίθεση

Στα [53],[61] γίνεται αναφορά στις προσεγγίσεις που έχουν γίνει στην αντιμετώπιση σιβυλλικής επίθεσης. Βασικός γνώμονας στις μεθόδους αντιμετώπισης είναι η πιστοποίηση ταυτότητας των κόμβων που συμμετέχουν στο δίκτυο. Μία λύση είναι η χρήση κρυπτογράφησης δημοσίου κλειδιού (συμμετρικής κρυπτογράφησης). Η προσέγγιση της αξιόπιστης πιστοποίησης (trusted certification) εξαλείφει εντελώς την επίθεση και εξασφαλίζει ότι κάθε οντότητα του δικτύου έχει μία πιστοποιημένη ταυτότητα. Στη προσέγγιση αυτή, είναι απαραίτητη η ανίχνευση των χαμένων ή κλεμμένων ταυτοτήτων και στη συνέχεια η ανάκληση τους (απόρριψη από το δίκτυο). Μια δεύτερη προσέγγιση είναι ο έλεγχος πόρων (resource testing), όπως ικανότητα υπολογισμών, αποθήκευσης, εύρος ζώνης, έτσι ώστε να ανιχνευθούν οι κόμβοι που έχουν λιγότερους από τους αναμενόμενους. Η προσέγγιση αυτή προσφέρει μερική λύση και είναι περισσότερο αποτρεπτικού χαρακτήρα. Επίσης, η προσέγγιση recurring costs and fees είναι μια άλλη προσέγγιση, η οποία είναι παραλλαγή της προηγούμενης και στηρίζεται στην δημιουργία εκ νέου ταυτοτήτων κατά διαστήματα και επικύρωση με χρήση δοκιμών. Επιπλέον προσεγγίσεις είναι αυτές των αξιόπιστων συσκευών (trusted devices), παρατήρησης (observation), και συστημάτων φήμης (reputation systems) [61].

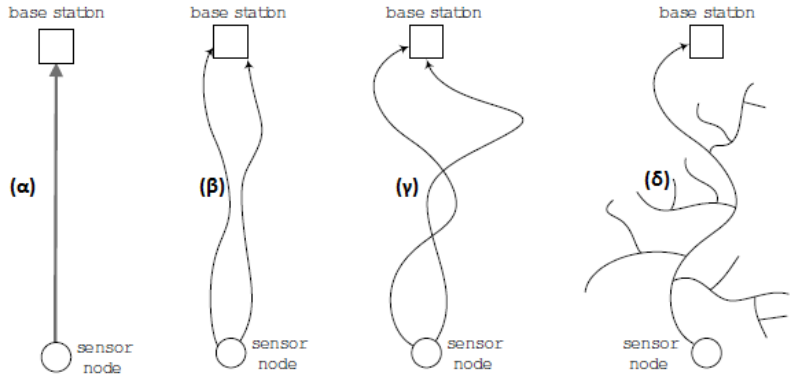
4.3.4 Αντίμετρα – Σκουληκότρυπα

Στο [54] παρουσιάζεται το πρωτόκολλο δρομολόγησης DAWSSEN (Defense mechanism Against Wormhole attacks in Wireless Sensor Networks). Πρόκειται για προληπτικό πρωτόκολλο δρομολόγησης, το οποίο βασίζεται σε ιεραρχική δόμηση του δικτύου WSN. Επίσης, στο [60] παρουσιάζονται λύσεις, οι οποίες βασίζονται σε χρήση από τους κόμβους πληροφοριών θέσης (geographic) ή χρόνου (temporal).

4.3.5 Αντίμετρα – Επίθεση ανάλυσης κίνησης

Σύμφωνα με το [56] προτείνονται τρεις μέθοδοι για την αντιμετώπιση επίθεσης ανάλυσης κίνησης. Οι μέθοδοι αυτοί στοχεύουν στη δημιουργία κίνησης σε τυχαίες κατευθύνσεις εντός του δικτύου, έτσι ώστε να επιτευχθεί παραπλάνηση του εισβολέα, ως προς τη θέση του σταθμού βάσης. Η πρώτη είναι η τεχνική MPR (multiple parent routing), η οποία επιτρέπει τη δρομολόγηση των πακέτων από τον αισθητήριο κόμβο μέχρι το σταθμό βάσης μέσω εναλλακτικών δρομολογίων (Σχήμα

4.2(β)) και όχι μέσω του συντομότερου μονοπατιού (Σχήμα 4.2(α)). Η δεύτερη μέθοδος είναι η τεχνική RW (random walk, Σχήμα 4.2(γ)). Σύμφωνα με αυτή το μονοπάτι δρομολόγησης καθορίζεται από έναν αλγόριθμο προώθησης που εισάγει τυχαιότητα στον προσδιορισμό του. Κάθε κόμβος που λαμβάνει ένα πακέτο το προωθεί ισοπίθανα σε οποιονδήποτε γειτονικό του. Αν και η τεχνική RW εισάγει τυχαιότητα και είναι αποτελεσματικότερη στην παραπλάνηση του εισβολέα σε σύγκριση με τη τεχνική MPR, μπορεί να οδηγήσει σε μεγάλου μήκους μονοπάτια δρομολόγησης. Μεγάλου μήκους μονοπάτια δρομολόγησης όμως οδηγούν σε μεγαλύτερη κατά μέσο όρο κατανάλωση ενέργειας στους κόμβους του δικτύου. Η τρίτη μέθοδος αντιμετώπισης αναφερόμενη ως κλασματική διάδοση (fractal propagation) βασίζεται στη δημιουργία ψευδών πακέτων και η δημιουργία εικονικής κίνησης στο δίκτυο (Σχήμα 4.(δ)). Σύμφωνα με αυτή τη τεχνική κάθε κόμβος, λαμβάνοντας ένα πακέτο, δημιουργεί με μία καθορισμένη πιθανότητα ένα ψευδές πακέτο και το προωθεί σε έναν γείτονα του. Η τεχνική αυτή έχει το μειονέκτημα ότι είναι επιρρεπής στη δημιουργία μεγάλης κυκλοφορίας πλησίον του σταθμού βάσης, γεγονός το οποίο αυξάνει το ποσοστό συγκρούσεων και απωλειών πακέτων.



Σχήμα 4.2. Τεχνικές αντιμετώπισης κίνησης: (α) συντομότερο μονοπάτι δρομολόγησης, (β) τεχνική MPR, (γ) τεχνική RW, (δ) τεχνική κλασματικής διάδοσης

4.3.6 Αντίμετρα – Επιθέσεις κατά του απορρήτου

Στο [44] αναφέρονται αρκετές στρατηγικές που στοχεύουν στην αντιμετώπιση επιθέσεων κατά του απορρήτου. Βασικό αντίμετρο είναι οι μηχανισμοί ανωνυμίας. Οι μηχανισμοί αυτοί μπορούν να υλοποιηθούν με (α) αποκέντρωση ευαίσθητων δεδομένων, (β) εξασφάλιση ασφαλούς καναλιού επικοινωνίας και (γ) τροποποίηση κυκλοφορίας δεδομένων. Η βασική ιδέα της αποκέντρωσης δεδομένων είναι ο διαμοιρασμός της πληροφορίας σε γειτονικούς κόμβους, έτσι ώστε να μην είναι διαθέσιμη η πληροφορία στο σύνολο της σε έναν κόμβο [44]. Η εξασφάλιση ασφαλούς καναλιού επικοινωνίας υλοποιείται με ασφαλή πρωτόκολλα επικοινωνίας

(π.χ. SPINS). Η τροποποίηση κυκλοφορίας δεδομένων υλοποιείται με τις τεχνικές που περιγράφτηκαν στην προηγούμενη παράγραφο (MPR,RW,fractal propagation). Παρόμοιες στρατηγικές, οι οποίες αποσκοπούν στην παραπλάνηση του επιτιθέμενου ως προς τη κίνηση πακέτων στο δίκτυο είναι οι τεχνικές πλημμυρίσματος αρχικής τιμής (baseline flooding), πιθανολογικού πλημμυρίσματος (probabilistic flooding), πλημμυρίσματος με ψεύτικα μηνύματα (flooding with fake messages) και πλημμυρίσματος φαντάσματος (phantom flooding) [44].

4.3.7 Αντίμετρα – Φυσικές επιθέσεις, αναπαραγωγή κόμβου

Οι μηχανισμοί αντιμετώπισης παρεμβολών (μηχανισμοί FHSS και διαμόρφωσης φάσματος) προσφέρουν μερική προστασία ως προς την ανίχνευση από έναν επιτιθέμενο της θέσης των κόμβων. Ένας επιπλέον μηχανισμός άμυνας είναι ο εξοπλισμός των κόμβων με υλικό, το οποίο θα τους προστατεύει από τους επιτιθέμενους. Για παράδειγμα, η ύπαρξη hardware αντίστασης τροποποίησης έχει σκοπό την αποτροπή του επιτιθέμενου στην τροποποίηση ή υποκλοπή δεδομένων που διαχειρίζονται οι κόμβοι. Τέλος, μία λύση στην αντιμετώπιση φυσικών επιθέσεων προσφέρει ο αυτό-τερματισμός της συσκευής (self-termination). Σύμφωνα με αυτή, ο κόμβος τερματίζει τη λειτουργία του, καταστρέφοντας δεδομένα και κρυπτογραφικά κλειδιά, όταν ανιχνεύσει μία πιθανή επίθεση. Η τεχνική αυτή είναι αποδοτικότερη σε δίκτυα που υπάρχει πλεονασμός πληροφορίας. Το κλειδί της προσέγγισης αυτής είναι ο εντοπισμός της επίθεσης και η περιοδική αναζήτηση των γειτονικών κόμβων. Τέλος, η αντιμετώπιση επιθέσεων αναπαραγωγής κόμβου μπορεί να γίνει σύμφωνα με το [44] με χρήση αλγορίθμων τυχαιοποιημένης πολυεκπομπής (randomized multicast) και line-selected πολυεκπομπής.

4.3.8 Σύνοψη

Η κρυπτογράφηση, η αυθεντικοποίηση, η πολυδιαδρομική δρομολόγηση, η επιβεβαίωση ταυτότητας, η αμφίδρομη επιβεβαίωση ζεύξης και η αυθεντικοποίηση εκπομπών δίνουν λύσεις σε θέματα προστασίας των πρωτοκόλλων δρομολόγησης που εφαρμόζονται σε ένα δίκτυο WSN. Οι περισσότερες επιθέσεις στοχεύουν στη προβληματική δρομολόγηση πακέτων στο δίκτυο και για το λόγο αυτό είναι ιδιαίτερης κρισιμότητας η σχεδίαση πρωτοκόλλων επιπέδου δικτύου που να περιορίζουν τις επιπτώσεις των επιθέσεων αυτών. Στον Πίνακα 4.1 γίνεται αναφορά

των μηχανισμών ασφαλείας που χρησιμοποιούνται για την αντιμετώπιση επιθέσεων που έχουν αναφερθεί.

Επίθεση	**Μηχανισμοί αντιμετώπισης επίθεσης**
Παρεμβολή (jamming)	Τεχνική μεταπήδησης συχνότητας FHSS (Frequency – hopping spread spectrum), τεχνική διαμόρφωσης φάσματος (Code spreading)
Αλλοίωση και υποκλοπή (tampering)	Μηχανισμοί προστασίας παραβίασης, φυσική απόκρυψη, μηχανισμοί απενεργοποίησης
Φυσική επίθεση	Φυσική απόκρυψη
Αναπαραγωγή κόμβου	Φυσική απόκρυψη, κρυπτογράφηση
Σύγκρουση δεδομένων (collision)	Κώδικας διόρθωσης σφαλμάτων (error-correcting code), αποφυγή χρήσης πρωτοκόλλων MAC που λειτουργούν με το σχήμα RTS/CTS
Εξάντληση ενεργειακών πόρων (exhaustion)	Χρήση πολλαπλής προσπέλασης διαίρεσης χρόνου (TDMA), δρομολόγηση πακέτων μόνο μετά από αυθεντικοποίηση του αποστολέα, φραγή πακέτων με μέγεθος που υπερβαίνει το μέγεθος πακέτων της εφαρμογής
Μεροληψία (unfairness)	Χρήση μικρών σε μήκος πακέτων
Καταβόθρα (sinkhole)	Πρωτόκολλο δρομολόγησης MintRoute [52][58][59], κρυπτογραφικά πρωτόκολλα RESIST-0/RESIST-1 [57]
Σκουληκότρυπα	Πρωτόκολλο DAWWSEN [54], χρήση πληροφοριών θέσης και χρόνου [60]
Παραπλάνηση (misdirection)	Τεχνικές αυθεντικοποίησης
Επιλεκτική προώθηση (selective forwarding)	Τεχνικές πλεονασμού
Μαύρη τρύπα (black hole)	Τεχνικές αυθεντικοποίησης
Hello flood	Τεχνικές αυθεντικοποίησης
Σιβυλλική επίθεση (sybil attack)	Πιστοποίηση ταυτότητας [53]
Επίθεση homing	Κρυπτογράφηση

Πλαστογράφηση αναγνώρισης (acknowledgment spoofing)	Τεχνικές αυθεντικοποίησης
Πλημμύρισμα (flooding)	Client puzzles, περιορισμός συνδέσεων, αυθεντικοποίηση
Αποσυγχρονισμός (desynchronization)	Τεχνικές αυθεντικοποίησης
Παρακολούθηση και κρυφάκουσμα (monitoring and eavesdropping)	Κρυπτογράφηση, τεχνική μεταπήδησης συχνότητας FHSS (Frequency – hopping spread spectrum)
Ανάλυση κίνησης (traffic analysis)	Τεχνικές MPR, RW, κλασματικής διάδοσης
Παραλλαγή (camouflage)	Τεχνικές αυθεντικοποίησης
Επιθέσεις κατά του απορρήτου	Μηχανισμοί ανωνυμίας

Πίνακας 4.1 Μηχανισμοί αντιμετώπισης επιθέσεων

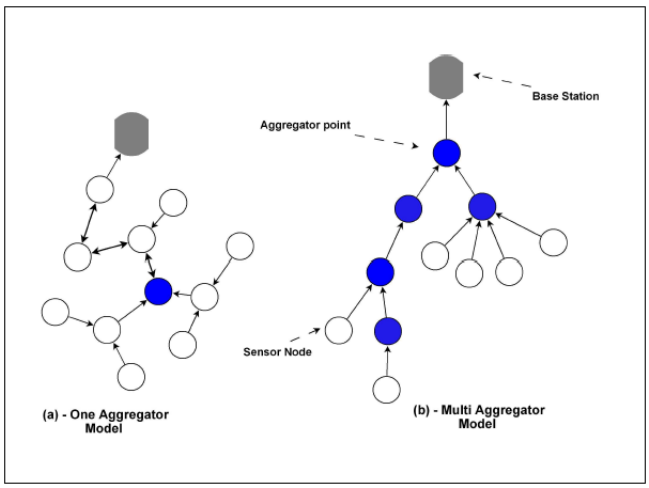
4.4 Ασφαλής συνάθροιση δεδομένων (Secure Data Aggregation)

Η συνάθροιση δεδομένων αποσκοπεί στην εξοικονόμηση ενέργειας με μείωση του όγκου μεταδιδόμενης κυκλοφορίας (μικρότερος αριθμός εκπομπών), εκμεταλλευόμενη τον πλεονασμό της πληροφορίας, που προκύπτει από την εγγύτητα των κόμβων του δικτύου WSN. Ένα τέτοιο δίκτυο περιλαμβάνει κόμβους, οι οποίοι καλούνται συλλέκτες (aggregators) και υλοποιούν τη συνάθροιση δεδομένων (data aggregation), όπως αυτή αναφέρθηκε στο πρώτο κεφάλαιο. Η επιλογή του συλλέκτη γίνεται από το δίκτυο με βάση τη θέση του και τα ενεργειακά αποθέματα του. Το ενδεχόμενο εκδήλωσης κακόβουλης ενέργειας εναντίον ενός συλλέκτη είναι υπαρκτό και για το λόγο αυτό είναι επιβεβλημένη η μελέτη της ασφαλούς συνάθροισης δεδομένων (secure data aggregation). Εάν ένας συλλέκτης προσβληθεί, το δίκτυο WSN είναι περισσότερο επιρρεπές στην διακίνηση ψευδών μηνυμάτων μέσω των κόμβων του.

Οι συλλέκτες συναθροίζουν τα δεδομένα σε ένα υποσύνολο του δικτύου, τα οποία τα συγκεντρώνουν με χρήση κατάλληλης συνάρτησης συνάθροισης. Εν συνεχεία το αποτέλεσμα της εν λόγω συνάθροισης διαβιβάζεται σε έναν ανώτερο συλλέκτη (querier). Ο ανώτερος συλλέκτης μπορεί να είναι ο σταθμός βάσης ή ένας εξωτερικός χρήστης, ο οποίος δύναται να αλληλεπιδράσει με το δίκτυο.

Η ασφαλής συνάθροιση δεδομένων απαιτεί αυθεντικοποίηση, εμπιστευτικότητα, ακεραιότητα δεδομένων και συνεργατική λειτουργία των κόμβων και συλλεκτών, με σκοπό τη ταυτοποίηση προσβεβλημένων κόμβων. Επιπλέον, ένα σύστημα ασφαλούς συνάθροισης δεδομένων σε ένα δίκτυο WSN πρέπει να έχει τα ακόλουθα χαρακτηριστικά: (α) δίκαιη προσέγγιση των μετρήσεων των αισθητήριων κόμβων, (β) ικανότητα περιορισμού του μεγέθους των δεδομένων που μεταδίδονται στο δίκτυο, (γ) εξασφάλιση φρεσκάδας και ακεραιότητας των δεδομένων, (δ) ευρωστία ως προς κακόβουλες δραστηριότητες με την εκτέλεση ενός μηχανισμού αυτό-ίασης και (ε) ύπαρξη δυναμικού μηχανισμού επιλογής συλλέκτη, με κριτήριο την εξισορρόπηση του φόρτου εργασιών και εξοικονόμησης ενέργειας. Επιπλέον, σε ένα μοντέλο συνάθροισης δεδομένων πρέπει να παρέχεται όσο το δυνατόν περισσότερη ακρίβεια στα δεδομένα συνάθροισης. Όσον αφορά την ακρίβεια, προκύπτει ένα trade – off μεταξύ του επιπέδου ακρίβειας και του μεγέθους των δεδομένων συνάθροισης, καθώς η μεγαλύτερη ακρίβεια απαιτεί αποστολή πακέτων μεγαλύτερου μήκους (περισσότερα ψηφία) και ως εκ τούτου, μεγαλύτερη κατανάλωση ενέργειας.

Τα μοντέλα συνάθροισης δεδομένων ταξινομούνται σε (α) ενός συλλέκτη ή (β) πολλαπλών συλλεκτών (Σχήμα 4.3). Στα μοντέλα ενός συλλέκτη, η συνάθροιση δεδομένων λαμβάνει χώρα αποκλειστικά σε μία συσκευή πριν την προώθηση της πληροφορίας στο σταθμό βάσης. Στα συγκεκριμένα μοντέλα, ο συλλέκτης πρέπει να είναι μια συσκευή με αυξημένες δυνατότητες υπολογισμών, έτσι ώστε να λάβει εις πέρας το έργο του. Αντίθετα, τα μοντέλα πολλαπλού συλλέκτη εκτελούν συνάθροιση δεδομένων σε πολλαπλά σημεία στο δίκτυο (πολλαπλοί συλλέκτες), εκμεταλλευόμενοι σε βέλτιστο βαθμό τον πλεονασμό δεδομένων και για το λόγο αυτό λειτουργούν αποδοτικότερα σε δίκτυα WSN με μεγάλο αριθμό κόμβων.



Σχήμα 4.3. Συνάθροιση δεδομένων (α) ενός συλλέκτη και (β) πολλαπλών συλλεκτών

Επιθέσεις που είναι δυνατόν να επηρεάσουν τη διαδικασία συνάθροισης δεδομένων είναι οι επιθέσεις άρνησης εξυπηρέτησης (DoS), η επίθεση αναπαραγωγής κόμβου (compromised node), η σιβυλλική επίθεση, η επιλεκτική προώθηση, η επίθεση επανεκπομπής (replay) και η επίθεση εκχώρησης ψευδών στοιχείων (stealthy) σε συσκευές που λειτουργούν ως συλλέκτες στο δίκτυο WSN [94]. Η επίθεση συμβιβασμένου κόμβου λαμβάνει χώρα όταν ο επιτιθέμενος είναι σε θέση να έχει πρόσβαση σε αισθητήριους κόμβους, να εξάγει πληροφορίες από αυτούς και να τους έχει υπό τον έλεγχο του. Η επίθεση επανεκπομπής λαμβάνει χώρα όταν ο επιτιθέμενος παρακολουθεί αρχικά τη κυκλοφορία πακέτων στο δίκτυο και επαναλαμβάνει εκπομπή αυτών με σκοπό την παραπλάνηση των συλλεκτών. Τέλος, η επίθεση stealthy στοχεύει στην εκχώρηση ψευδών στοιχείων στο δίκτυο, χωρίς την αποκάλυψη ύπαρξης τους. με αποτέλεσμα την επιρροή της διαδικασίας συνάθροισης.

Στη βιβλιογραφία έχουν προταθεί αρκετά μοντέλα ασφαλούς συνάθροισης δεδομένων, κατάλληλα για δίκτυα WSN. Ενδεικτικά, αναφέρονται σύμφωνα με το [94] τα μοντέλα πολλαπλού συλλέκτη CDA (Concealed Data Aggregation) [95], SDA (Secure Data Aggregation) [96], SHDA (Secure Hierarchical in-network Data Aggregation) [98], SRDA (Secure Reference – based Data Aggregation) [101], SDAP (Secure hop-by-hop Data Aggregation Protocol) [102], ESA (Efficient Secure Aggregation) [103], EDA (Event – oriented Data Aggregation) [104] και απλού συλλέκτη SIA (Secure Information Aggregation) [97], SecureDAV (Secure Data Aggregation and Verification Protocol) [100] και WDA (Witness – based Data Aggregation) [99].

Στον Πίνακα 4.2 γίνεται σύγκριση των παραπάνω μοντέλων, ως προς το τύπο επιτιθέμενου που αντιμετωπίζεται, η εφαρμοζόμενη μέθοδος κρυπτογράφησης, τις αντιμετωπιζόμενες επιθέσεις, τη κάλυψη των απαιτήσεων ασφαλείας και το επίπεδο προστασίας που επιτυγχάνεται. Το επίπεδο προστασίας καθορίζεται με βάση τη δυνατότητα αντιμετώπισης κακόβουλων ενεργειών είτε παθητικής μορφής (χαμηλή προστασία), είτε ενεργητικής από συσκευή χαμηλών (μέτρια προστασία) ή υψηλών υπολογιστικών δυνατοτήτων (υψηλή προστασία).

Μοντέλο	Τύπος επίθεσης	Κρυπτο – γράφηση	Ευρωστία σε επιθέσεις	Κάλυψη απαιτήσεων	Επίπεδο προστασίας
CDA	Παθητική	Συμμετρική	Επιθέσεις DoS, αναπαραγωγής κόμβου	Διαθεσιμότητα, εμπιστευτικότητα	Χαμηλό
SDA	Ενεργητική	Συμμετρική	Επιθέσεις DoS, αναπαραγωγής κόμβου, επιλεκτικής προώθησης, stealthy	Διαθεσιμότητα, ακεραιότητα, φρεσκάδα δεδομένων, αυθεντικότητα	Μέτριο
SIA	Ενεργητική	Συμμετρική	Επιθέσεις DoS, αναπαραγωγής κόμβου, επιλεκτικής προώθησης	Διαθεσιμότητα, εμπιστευτικότητα, ακεραιότητα, φρεσκάδα δεδομένων, αυθεντικότητα	Υψηλό
SHDA	Ενεργητική	Συμμετρική	Επιθέσεις DoS, αναπαραγωγής κόμβου, επιλεκτικής προώθησης	Διαθεσιμότητα, εμπιστευτικότητα, ακεραιότητα, φρεσκάδα δεδομένων, αυθεντικότητα	Υψηλό
WDA	Ενεργητική	Συμμετρική	Επιθέσεις DoS, αναπαραγωγής κόμβου, επιλεκτικής προώθησης, σιβυλλική, επανεκπομπής, stealthy	Διαθεσιμότητα, ακεραιότητα, αυθεντικότητα	Μέτριο
Secure DAV	Ενεργητική	Ασύμμετρη	Επιθέσεις DoS, αναπαραγωγής κόμβου, επιλεκτικής προώθησης, επανεκπομπής, stealthy	Διαθεσιμότητα, εμπιστευτικότητα, ακεραιότητα, αυθεντικότητα	Μέτριο
SRDA	Παθητική	Συμμετρική	Επιθέσεις DoS	Διαθεσιμότητα, εμπιστευτικότητα, φρεσκάδα δεδομένων,	Χαμηλό

				αυθεντικότητα	
SDAP	Ενεργητική	Συμμετρική	Επιθέσεις DoS, αναπαραγωγής κόμβου, επιλεκτικής προώθησης, stealthy	Διαθεσιμότητα, εμπιστευτικότητα, ακεραιότητα, φρεσκάδα δεδομένων, αυθεντικότητα	Μέτριο
ESA	Ενεργητική	Συμμετρική	Επιθέσεις DoS, αναπαραγωγής κόμβου, επιλεκτικής προώθησης, stealthy	Διαθεσιμότητα, εμπιστευτικότητα, ακεραιότητα, φρεσκάδα δεδομένων, αυθεντικότητα	Μέτριο
EDA	Παθητική	Συμμετρική	Επιθέσεις DoS	Διαθεσιμότητα, εμπιστευτικότητα	Χαμηλό

Πίνακας 4.2 Μοντέλα ασφαλούς συνάθροισης δεδομένων

4.5 Κρυπτογράφηση

Μηχανισμός αντιμετώπισης επιθέσεων που στοχεύουν στη διαρροή πληροφοριών, που αφορούν στο δίκτυο, είναι η κρυπτογράφηση (encryption) [48],[49]. Η κρυπτογράφηση στοχεύει στη μετατροπή του μηνύματος που πρόκειται να αποστείλει ο κόμβος αποστολέας σε μορφή, η οποία θα είναι αντιληπτή μόνο από το κόμβο παραλήπτη. Εξαιτίας των περιορισμών των δικτύων WSN σε ζητήματα επεξεργασίας δεδομένων και κατανάλωσης ενέργειας, δεν είναι δυνατή η εφαρμογή όλων των τύπων κρυπτογράφησης σε δίκτυα WSN. Στα δίκτυα αυτά χρησιμοποιείται εξ ολοκλήρου η συμμετρική κρυπτογράφηση, η οποία στη βιβλιογραφία αναφέρεται και ως συμβατική κρυπτογράφηση, ή κρυπτογράφηση μυστικού/ιδιωτικού κλειδιού, ή κρυπτογράφηση ενός κλειδιού.

Οι μηχανισμοί κρυπτογράφησης προσφέρουν σε ένα δίκτυο WSN αποτελεσματική προστασία των ροών δεδομένων (data streams), καθώς αυτές διακινούνται μέσω των κόμβων του. Για πληρέστερη κατανόηση των συγκεκριμένων μηχανισμών είναι απαραίτητη η παράθεση των βασικών ορισμών των κρυπτογραφικών συστημάτων.

- *Αρχικό ή απλό κείμενο (plaintext)* καλείται το αρχικό πακέτο δεδομένων που πρόκειται να κρυπτογραφηθεί. Αντίστοιχα *κρυπτογραφημένο κείμενο ή κρυπτογράφημα (ciphertext)* είναι το πακέτο δεδομένων που λαμβάνει ο κόμβος παραλήπτης και καλείται να αποκρυπτογραφήσει. Το κρυπτογράφημα εξαρτάται τόσο από το αρχικό κείμενο, όσο και από το κλειδί κρυπτογράφησης. Αυτό σημαίνει

ότι για δεδομένο αρχικό κείμενο με χρήση διαφορετικών κλειδιών προκύπτουν μέσω του αλγόριθμου κρυπτογράφησης ισάριθμα διαφορετικά κρυπτογραφήματα.

- *Αλγόριθμος κρυπτογράφησης (encryption algorithm)* είναι η μέθοδος που εφαρμόζεται για να μετατραπεί το αρχικό κείμενο σε κρυπτογραφημένο. Η μέθοδος αυτή περιλαμβάνει αντικαταστάσεις και μετασχηματισμούς (π.χ. μεταθέσεις και αναδιατάξεις) στο αρχικό κείμενο. Ο *αλγόριθμος αποκρυπτογράφησης (decryption algorithm)* αποτελεί την αντίστροφη διαδικασία, η οποία με εισόδους το κρυπτογράφημα και το κλειδί κρυπτογράφησης παράγει το αρχικό κείμενο.
- *Κρυπτογράφηση (encryption)* καλείται η μετατροπή του αρχικού κειμένου σε κρυπτογράφημα μέσω του αλγορίθμου κρυπτογράφησης και αποκρυπτογράφηση (decryption) η αντίστροφη διαδικασία.
- *Κλειδί (key) κρυπτογράφησης* καλείται η αναλυτική περιγραφή της μεθόδου κρυπτογράφησης (π.χ. αντιστοιχία συμβόλων αρχικού κειμένου και κρυπτογραφήματος) και δίνεται ως είσοδος στον αλγόριθμο κρυπτογράφησης.

4.5.1 Μέθοδοι κρυπτογράφησης

Η κρυπτογράφηση των μηνυμάτων που διακινούνται στο δίκτυο μπορεί να γίνει με δύο τρόπους: (α) τη κρυπτογράφηση ζεύξης (link encryption) και (β) τη κρυπτογράφηση από άκρο σε άκρο (end-to-end encryption). Σύμφωνα με τη κρυπτογράφηση ζεύξης (ή συνδέσμου), το πακέτο δεδομένων κρυπτογραφείται και αποκρυπτογραφείται σε κάθε συσκευή του δικτύου, έτσι ώστε να καθοριστεί ο παραλήπτης και να συνεχιστεί η δρομολόγηση. Ως εκ τούτου, κάθε συσκευή πρέπει να γνωρίζει το κλειδί κρυπτογράφησης και να είναι σε θέση να υλοποιήσει τους αλγορίθμους κρυπτογράφησης και αποκρυπτογράφησης. Η κρυπτογράφηση από άκρο σε άκρο καθορίζει ότι η κρυπτογράφηση και στη συνέχεια η αποκρυπτογράφηση λαμβάνουν χώρα αποκλειστικά στο κόμβο πηγή της πληροφορίας και στο τελικό αποδέκτη αντίστοιχα. Η ενδιάμεσοι κόμβοι που προωθούν τα πακέτα κατά τη δρομολόγηση με πολλαπλά άλματα δεν ενεργοποιούν τους αλγορίθμους κρυπτογράφησης/αποκρυπτογράφησης τους. Με άλλα λόγια, λαμβάνουν ένα κρυπτογράφημα και το προωθούν αυτούσιο. Το γεγονός ότι ο παραλήπτης πρέπει να είναι εμφανής στο κρυπτογράφημα αναγκάζει το κόμβο πηγή της πληροφορίας να μην κρυπτογραφεί ένα μέρος του πακέτου δεδομένων (επικεφαλίδα). Το γεγονός αυτό καθιστά τα δίκτυα που βασίζονται σε από άκρο σε

άκρο κρυπτογράφηση, επιρρεπή σε επιθέσεις ανάλυσης κίνησης, καθώς το μοτίβο της κίνησης πακέτων δεν αποκρύπτεται, παραμένοντας εκτεθειμένο σε πιθανές επιθέσεις.

4.5.2 Κρυπτογραφικοί αλγόριθμοι

Οι κρυπτογραφικοί αλγόριθμοι κατηγοριοποιούνται σε συμμετρικούς, ασύμμετρους και υβριδικούς. Στους συμμετρικούς αλγορίθμους, που είναι γνωστοί και ως ιδιωτικού ή μυστικού κλειδιού, χρησιμοποιείται το ίδιο κλειδί τόσο στην κρυπτογράφηση όσο και στην αποκρυπτογράφηση. Οι ασύμμετροι αλγόριθμοι, γνωστοί και ως δημοσίου κλειδιού, χρησιμοποιούν ένα δημόσιο κλειδί για τη κρυπτογράφηση και ένα μυστικό για κάθε παραλήπτη για την αντίστροφη διαδικασία. Οι υβριδικοί αλγόριθμοι αποτελούν συνδυασμό των παραπάνω. Αρχικά, χρησιμοποιούν ασύμμετρο αλγόριθμο για τη διανομή κλειδιού, και όταν αυτό γίνει γνωστό σε όλους τους συμμετέχοντες στο δίκτυο χρησιμοποιούνται συμμετρικοί αλγόριθμοι. Στη βιβλιογραφία έχει προταθεί πληθώρα συμμετρικών αλγορίθμων κρυπτογράφησης, όπως οι DES (Data Encryption Standard), AES (Advanced Encryption Standard), RC4, RC5, Serpent, Kasumi, Camellia, IDEA, SHA-1, MD5, TEA και MISTY1. Επίσης, σημαντικοί ασύμμετροι και υβριδικοί αλγόριθμοι κρυπτογράφησης είναι οι RSA, El-Gamal, NTRU, ελλειπτικών καμπυλών (ECC) και οι SSL, PGP και GPG αντίστοιχα [42, 48].

Η συμμετρική κρυπτογράφηση μπορεί να γίνει με δύο τρόπους. Σύμφωνα με το πρώτο, το αρχικό κείμενο τεμαχίζεται σε τμήματα n ψηφίων (block cipher). Κάθε τμήμα κρυπτογραφείται ανεξάρτητα από τα υπόλοιπα του αρχικού κειμένου. Οι αλγόριθμοι που χρησιμοποιούν αυτή τη τεχνική καλούνται αλγόριθμοι τμημάτων. Ο δεύτερος τρόπος κρυπτογράφησης είναι η κρυπτογράφηση ροής (stream cipher). Σύμφωνα με αυτόν, κάθε ψηφίο κρυπτογραφείται ανεξάρτητα από τα υπόλοιπα. Οι αλγόριθμοι που χρησιμοποιούν αυτή τη τεχνική καλούνται αλγόριθμοι ροής. Στους αλγόριθμους ροής υπεισέρχεται η δυσκολία συγχρονισμού πομπού και δέκτη, αλλά είναι δυσκολότερη η εξαγωγή του αρχικού κειμένου από έναν υποκλοπέα. Δημοφιλέστεροι αλγόριθμοι τμημάτων και ροής είναι ο AES και ο RC5 αντίστοιχα.

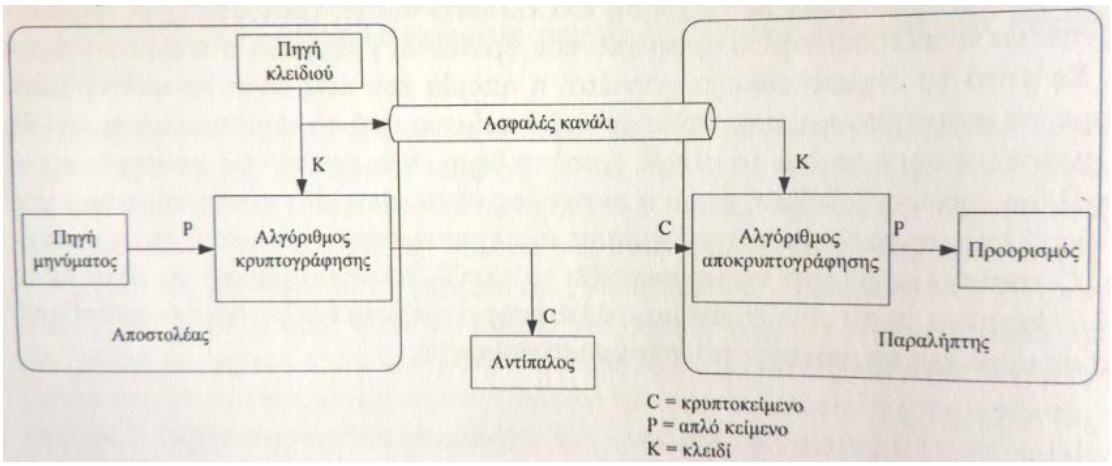
Εξαιτίας των περιορισμών που υφίσταται ένα δίκτυο WSN σε ικανότητες επεξεργασίας των κόμβων, όπως έχει ήδη αναφερθεί, η χρήση των πολυπλοκότερων ασύμμετρων και υβριδικών αλγορίθμων κρυπτογράφησης δεν προτιμάται [43].

Δημοφιλής αλγόριθμος κρυπτογράφησης σε εφαρμογές WSN είναι ο αλγόριθμος AES, ο οποίος βρίσκει εφαρμογή στα πρότυπα ZigBee και Bluetooth LE.

4.5.3 Συμμετρική κρυπτογράφηση

Η συμμετρική κρυπτογράφηση βασίζεται στη μυστικότητα του κλειδιού και όχι στη μυστικότητα του αλγορίθμου κρυπτογράφησης [70]. Στην πράξη, αυτό σημαίνει ότι είναι αδύνατο για κάποιον που έχει στη κατοχή του το κρυπτογράφημα και τον αλγόριθμο κρυπτογράφησης να παράγει το αρχικό κείμενο. Το συγκεκριμένο χαρακτηριστικό καθιστά τη δυνατότητα στους κατασκευαστές να υλοποιήσουν χαμηλού κόστους αλγορίθμους κρυπτογράφησης με χρήση ολοκληρωμένων κυκλωμάτων. Η παραπάνω διευκόλυνση που παρέχει η συμμετρική κρυπτογραφία έρχεται με αντιστάθμισμα τη κρισιμότητα διατήρησης της μυστικότητας του κλειδιού κρυπτογράφησης.

Στο Σχήμα 4.4 απεικονίζεται το μοντέλο επικοινωνίας του συμμετρικού κρυπτοσυστήματος. Το ασφαλές κανάλι, απαραίτητο για την ενημέρωση των κόμβων ως προς το μυστικό κλειδί κρυπτογράφησης αποτελεί την αδυναμία του κρυπτοσυστήματος, καθώς δεν είναι πάντοτε διαθέσιμο. Η ανταλλαγή του κλειδιού μπορεί να έχει συμβεί με την εγκατάσταση των συσκευών. Ένας άλλος τρόπος κοινοποίησης του κλειδιού είναι ο τεμαχισμός του και η αποστολή στους ενδιαφερόμενους παραλήπτες μέσω διαφορετικών καναλιών.



Σχήμα 4.4. Μοντέλο επικοινωνίας συμμετρικού συστήματος

Το προηγμένο πρότυπο κρυπτογράφησης ή αλγόριθμος AES (Advanced Encryption Standard – AES [48],[49],[70]) σχεδιάστηκε το 1997 από το ινστιτούτο NIST (National Institute of Standards and Technology) ως επέκταση του προτύπου κρυπτογράφησης δεδομένων (Data Encryption Standard – DES, [48],[49],[70]) και

είναι ο πλέον δημοφιλής σε δίκτυα WSN. Σκοπός της επέκτασης ήταν η δημιουργία συμμετρικού κρυπτογραφικού αλγορίθμου που είναι δυσκολότερο να «σπάσει» εξαιτίας της αύξηση του μήκους χρησιμοποιούμενων κλειδιών κρυπτογράφησης. Ο αλγόριθμός AES εκτός από ισχυρότερος έναντι του DES είναι επίσης ταχύτερος, ευκολότερος στην εφαρμογή του και έχει μικρότερες απαιτήσεις μνήμης. Επιπλέον, ο αλγόριθμος AES καθορίζει ότι το μέγεθος τμήματος εισόδου είναι 128 ψηφία και το μήκος του κλειδιού πρέπει να είναι 128, 192 ή 256 ψηφία. Σε δημοφιλή πρότυπα WSN (ZigBee, Bluetooth LE) γίνεται εφαρμογή του αλγορίθμου AES-128bits (μήκος κλειδιού 128 ψηφία). Με βάση αυτό το μήκος κλειδιού υπάρχουν $2^{128} \approx 3*10^{38}$ διατάξεις κλειδιών (ο αλγόριθμος DES προβλέπει 2^{56} διατάξεις κλειδιών).

4.5.4 Διαχείριση κρυπτογραφικού κλειδιού

Η έννοια της διαχείρισης κρυπτογραφικού κλειδιού (key management) αποτελεί θεμελιώδη παράγοντα στη διαδικασία εγκαθίδρυσης κρυπτογραφικών κλειδιών και επίτευξης ασφαλούς επικοινωνίας μεταξύ των κόμβων του δικτύου WSN, με βάση τις αρχές της συμμετρικής κρυπτογράφησης. Η διαχείριση κρυπτογραφικού κλειδιού στοχεύει τόσο στην ασφαλή διανομή του κρυπτογραφικού κλειδιού (key distribution) στους συμμετέχοντες κόμβους όσο και στην ανάκληση κρυπτογραφικών κλειδιών (key revocation) από κόμβους που έχουν προσβληθεί ή πρόκειται να αφαιρεθούν από το δίκτυο.

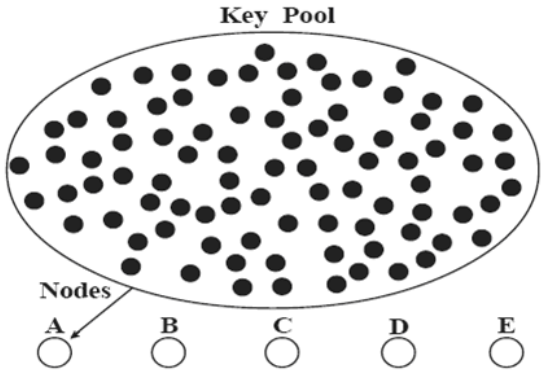
Κάθε μηχανισμός διαχείρισης κρυπτογραφικού κλειδιού σε ένα δίκτυο WSN πρέπει να παρέχει ασφαλή επικοινωνία μεταξύ των κόμβων και να είναι παράλληλα συμβατός με κάποιες θεμελιώδεις απαιτήσεις. Πρωταρχική απαίτηση είναι η συμμόρφωση με τις ιδιαιτερότητες ενός δικτύου WSN, ως προς τις δυνατότητες υπολογισμών και αποθήκευσης στους κόμβους του. Επιπλέον όμως της απαίτησης αυτής, είναι σημαντικό ο μηχανισμός να παρέχει τις δυνατότητες εισόδου στο δίκτυο νέων εξουσιοδοτημένων συσκευών καθώς και την απομάκρυνση άλλων προσβεβλημένων (ανάκληση κλειδιών). Επίσης, εξαιτίας του μεγέθους ενός δικτύου WSN και του μεγάλου αριθμού κόμβων η διαχείριση κρυπτογραφικών κλειδιών ανά ζεύγη (pairwise schemes) καθίσταται μη πρακτική, καθώς δημιουργεί αυξημένες απαιτήσεις σε θέματα αποθήκευσης και υπολογισμών [42]. Ένας ακόμα λόγος μη συμβατότητας της διαχείρισης με τον τρόπο αυτό είναι το γεγονός ότι οι κόμβοι του δικτύου WSN επικοινωνούν μόνο με γειτονικούς τους συμμετέχοντας στην προώθηση μηνυμάτων με πολλαπλά άλματα.

Οι μηχανισμοί διαχείρισης κρυπτογραφικού μπορούν να κατηγοριοποιηθούν είτε με βάση τη δομή του δικτύου (κεντρικοί ή κατανεμημένοι μηχανισμοί) είτε με βάση το τρόπο διανομής των κλειδιών (πιθανολογικοί και ντετερμινιστικοί μηχανισμοί). Οι κεντρικοί μηχανισμοί (centralized key schemes) διαχείρισης βασίζονται στον έλεγχο της διαδικασίας από μία κεντρική οντότητα (κόμβο αυξημένων δυνατοτήτων), αποκαλούμενη κέντρο διανομής κλειδιών (KDC – key distribution center). Το κέντρο διανομής κλειδιών συνηθέστερα είναι ο σταθμός βάσης του δικτύου. Βασικότερος μηχανισμός της κατηγορίας αυτής είναι ο μηχανισμός LKHW (βασισμένος στη τεχνική LKH – Logical Key Hierarchy). Αντιθέτως με τους κεντρικούς, οι κατανεμημένοι μηχανισμοί (distributed key schemes) βασίζουν τη διαδικασία αναπαραγωγής και διανομής τους σε περισσότερες από μία οντότητες. Ένας σημαντικός κατανεμημένος μηχανισμός διαχείρισης κρυπτογραφικού κλειδιού είναι ο LEAP (Localized Encryption and Authentication Protocol). Γενικότερα, στη βιβλιογραφία προτείνεται πληθώρα προσεγγίσεων για μηχανισμούς διαχείρισης κρυπτογραφικών κλειδιών με σημαντικές αναφορές να γίνονται στα [42], [72], [73] και [74].

Στο [76] παρουσιάζεται το πρωτόκολλο LEAP (Localized Encryption and Authentication Protocol), ο οποίος είναι κατανεμημένος και ντετερμινιστικός μηχανισμός διαχείρισης, και χρησιμοποιεί τέσσερα είδη κλειδιών σε κάθε κόμβο. Σε αυτά περιλαμβάνονται για κάθε κόμβο του δικτύου (α) ένα ατομικό κλειδί (individual key), το οποίο το γνωρίζει και ο σταθμός βάσης, (β) ένα ομαδικό κλειδί (group key), το οποίο το γνωρίζουν όλοι οι κόμβοι του δικτύου, (γ) κλειδιά ζεύξης (pairwise keys) για την επικοινωνία με γειτονικούς κόμβους και (δ) ένα κλειδί ομάδας (cluster key) για την επικοινωνία με το κόμβο επικεφαλή της ομάδας. Μειονέκτημα του μηχανισμού είναι ότι δεν παρέχει ολοκληρωμένη προστασία από επιθέσεις άρνησης εξυπηρέτησης σε εφαρμογές υψηλών απαιτήσεων ασφαλείας.

Μία σημαντική προσέγγιση στη διαχείριση κρυπτογραφικών κλειδιών είναι αυτή που αναφέρεται στο [77], κατά Eschenauer και Gligor, η οποία βασίζεται στην ύπαρξη μιας δεξαμενής από κρυπτογραφικά κλειδιά, τα οποία υπολογίζονται και κατανέμονται στους κόμβους πριν από την ανάπτυξη τους στην περιοχή επιτήρησης. Με τον τρόπο αυτό εξασφαλίζεται η ασφαλής διανομή των κρυπτογραφικών κλειδιών καταναλώνοντας, όσο το δυνατόν, λιγότερη ενέργεια, εξαιτίας της σημαντικής μείωσης τόσο των απαιτούμενων υπολογισμών (τα κρυπτογραφικά κλειδιά ήταν είδη υπολογισμένα και διανεμημένα), όσο και της ανταλλαγής μηνυμάτων. Ο

συγκεκριμένος μηχανισμός υποστηρίζει ανάκληση κλειδιών σε περιπτώσεις προσβολής κόμβων από επιτιθέμενο, αλλά δεν προβλέπει μεθόδους για την ανανέωση τους, γεγονός το οποίο αποτελεί μειονέκτημα του. Παρόμοιος με το μηχανισμό αυτόν, όπου γίνεται χρήση δεξαμενής κλειδιών, στο [78] παρουσιάζεται ο μηχανισμός Q-Composite Random Key Pre-distribution από τους Chan, Perrig και Song. Σε αυτόν το μηχανισμό οι κόμβοι διαμοιράζονται τουλάχιστον q κρυπτογραφικά κλειδιά. Σε περίπτωση προσβολής και αποκάλυψης ενός κλειδιού, αυτό απορρίπτεται και οι κόμβοι επικοινωνούν με τα υπόλοιπα κλειδιά. Ωστόσο, ο μηχανισμός είναι επιρρεπής σε περιπτώσεις επιθέσεων σε περισσότερους από έναν κόμβους, οπότε και δεν είναι πλέον αποτελεσματικός.



Σχήμα 4.5. Δεξαμενή κρυπτογραφικών κλειδιών κατά Eschenauer και Gligor

Ένας μηχανισμός κατάλληλος για ομαδοποιημένα δίκτυα WSN είναι ο SHELL (Scalable, Hierarchical, Efficient, Location aware and Light-weight protocol)[74]. Πρόκειται για ένα εύρωστο μηχανισμό με αντίτιμο όμως την αυξημένη πολυπλοκότητα, καθώς προβλέπει μεγάλο αριθμό τύπων κλειδιών για κάθε κόμβο του δικτύου. Ένας απλούστερος μηχανισμός για ομαδοποιημένα δίκτυα WSN έχει προταθεί από τους Panja, Madria και Bhargava, προσφέροντας περισσότερη ευελιξία κατά τη διαχείριση των κλειδιών και μεγάλες δυνατότητες υποστήριξης επεκτασιμότητας [74]. Ωστόσο, ο μηχανισμός αυτός είναι λιγότερο εύρωστος σε σχέση με τον SHELL, γεγονός που αποτελεί το σημαντικότερο μειονέκτημα του.

4.6 Πιστοποίηση ταυτότητας (αυθεντικοποίηση)

Οι διαδικασίες πιστοποίησης ταυτότητας σε ένα δίκτυο WSN αποτελούν πρωταρχικής σημασίας μηχανισμούς ασφαλείας, οι οποίοι στηρίζονται στην

αυθεντικοποίηση των συσκευών του. Κάθε συσκευή λαμβάνει μία ταυτότητα, με βάση την οποία αποδεικνύει τη γνησιότητα της. Είναι σημαντικό η ταυτότητα αυτή να προστατεύεται από υποκλοπές, κάτι το οποίο επιτυγχάνεται με την απαγόρευση συμμετοχής μη εξουσιοδοτημένων συσκευών στο δίκτυο (unauthorized devices). Αυθεντικοποίηση μπορεί να οριστεί η διαδικασία κατά την οποία μια οντότητα, επικοινωνεί με μια ή περισσότερες άλλες συμμετέχουσες σε ένα δίκτυο και αιτείται την απόκτηση άδειας πρόσβασης σε αυτό. Η αίτηση γίνεται βάσει ενός πρωτοκόλλου, μέσω του οποίου θα γίνει η επαλήθευση των πιστοποιητικών προκειμένου να δοθεί η άδεια πρόσβασης.

Μία οντότητα, η οποία κάνει αίτηση εισόδου σε ένα ασύρματο δίκτυο μπορεί να βρεθεί σε κατάσταση αρχικοποίησης (initialization), ανίχνευσης (discovery), επιλογής (selection), αυθεντικοποίησης (authentication), ή αξιολόγησης (evaluation) [105]. Κατά την αρχικοποίηση η οντότητα λαμβάνει τα εργαλεία (πρωτόκολλα ή μηχανισμοί αυθεντικοποίησης, πιστοποιητικά αυθεντικοποίησης, ταυτότητες έμπιστων οντοτήτων) που απαιτούνται για την έναρξη των διαδικασιών αυθεντικοποίησης. Στη κατάσταση ανίχνευσης, η οντότητα κάνει την εμφάνιση της στο δίκτυο και είναι πλέον σε θέση να επικοινωνήσει με άλλες σε αυτό. Με συσχέτιση των διαθέσιμων εργαλείων, η οντότητα έρχεται σε κατάσταση επιλογής, όπου επιλέγεται ο αποδοτικότερος συνδυασμός τους. Κατόπιν της επιλογής, ακολουθεί η αυθεντικοποίηση η οποία περιλαμβάνει την πιστοποίηση των κλειδιών της, με βάση τα επιλεγμένα εργαλεία αυθεντικοποίησης. Κατά τη κατάσταση αυτή, κάθε συσκευή λαμβάνει πιστοποιητικά (κλειδιά), τα αποστέλλει σε μία έμπιστη οντότητα, η οποία τα αξιολογεί ως προς τη γνησιότητα τους. Σε περίπτωση γνησιότητας των συγκεκριμένων κλειδιών, ξεκινάει η διαδικασία εγκαθίδρυσης τους μεταξύ των συσκευών. Η τελευταία κατάσταση είναι αυτή της αξιολόγησης, κατά την οποία αξιολογείται η συμπεριφορά της οντότητας, η οποία αν αποδειχθεί ότι λειτουργεί κακόβουλα, απορρίπτεται από το δίκτυο. Με το πέρας της όλης διαδικασίας, δίνεται άδεια στην οντότητα να συνδεθεί σε αυτό.

Η πληθώρα των μεθόδων αυθεντικοποίησης, που έχουν προταθεί για ασύρματα δίκτυα, δεν είναι δυνατό να εφαρμοσθούν σε δίκτυα WSN, εξαιτίας περιορισμών των εν λόγω δικτύων, οι οποίοι πρέπει να προσμετρηθούν στη μελέτη των καταστάσεων και διαδικασιών της αυθεντικοποίησης. Ο καθορισμός του σταθμού βάσης ως την έμπιστη οντότητα, η οποία θα λάβει μέρος στις διαδικασίες αυθεντικοποίησης είναι πιθανό να αυξήσει τον φόρτο εργασίας σε αυτόν, επηρεάζοντας δυσμενώς τη

λειτουργία του. Για το λόγο αυτό η επίτευξη πιστοποίησης ταυτότητας σε τέτοια δίκτυα είναι σημαντική πρόκληση. Στη βιβλιογραφία εντοπίζονται προτάσεις για την υλοποίηση της διαδικασίας αυθεντικοποίησης, όπως το σχήμα που προτείνεται στο [106] που βασίζεται στη χρήση κατάλληλου λογισμικού, παραλλαγή του οποίου είναι το πρωτόκολλο PIV (Program Integrity Verification) [107]. Επιπλέον μηχανισμοί αυθεντικοποίησης είναι το πρωτόκολλο Terra [108], το οποίο στηρίζεται στην αρχιτεκτονική των εικονικών συστημάτων παρακολούθησης (virtual machine monitor) και το πρωτόκολλο SWATT (Software – based Attestation [109], το οποίο επίσης βασίζεται σε λογισμικό με δυνατότητες ανάγνωσης των δεδομένων της μνήμης μιας συσκευής.

4.7 Προστασία απορρήτου

Η κρυπτογράφηση μηνυμάτων που ανταλλάσσονται σε ένα δίκτυο WSN ικανοποιεί τις απαιτήσεις εμπιστευτικότητας, αντιμετωπίζοντας επιθέσεις υποκλοπών. Ωστόσο, για την προστασία απορρήτου της επικοινωνίας (επικοινωνούντες οντότητες, θέσεις, όγκος δεδομένων και τρόπος δρομολόγησης) η κρυπτογράφηση από μόνη της κρίνεται ανεπαρκής. Για το λόγο αυτό, πρέπει να ληφθεί μέριμνα με κατάλληλους μηχανισμούς για την επίτευξη της εν λόγω προστασίας. Η προστασία του απόρρητου και της ιδιωτικότητας επικοινωνίας σε ένα δίκτυο WSN περιλαμβάνει ως επί το πλείστον ζητήματα προστασίας πλαισίου επικοινωνίας και ελεγχόμενης προσπέλασης και συλλογής δεδομένων [71], τα οποία κρίνονται ως απαιτήσεις ασφαλείας.

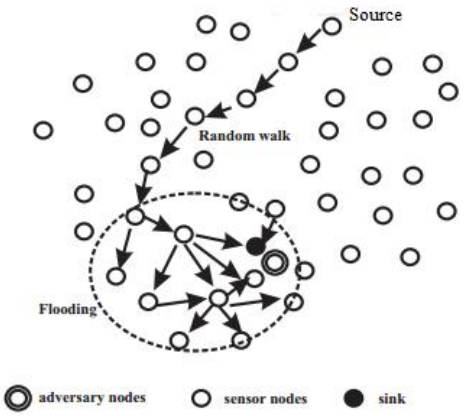
4.7.1 Προστασία πλαισίου επικοινωνίας

Τα κρυπτογραφημένα μηνύματα που διακινούνται στο δίκτυο είναι δυνατό να αποκαλύψουν πληροφορίες για το περιεχόμενο τους. Τεχνικές που στοχεύουν στην απόκρυψη τέτοιων πληροφοριών είναι (α) η χρονοσήμανση (timestamping), (β) η συμπλήρωση (padding), (γ) η χρήση αυξόντων αριθμών και (δ) η συχνή ανανέωση κρυπτογραφικών κλειδιών [71].

Η προστασία πληροφοριών θέσης (ανωνυμία θέσης) του κόμβου αποστολέα του μηνύματος αντιμετωπίζει τη δυσκολία που προσδίδουν οι παρεμβάσεις στο χρησιμοποιούμενο πρωτόκολλο δρομολόγησης. Εξαιτίας της δρομολόγησης των μηνυμάτων με πολλαπλά άλματα, ένας επιτιθέμενος μπορεί να ακολουθήσει την αντίστροφη διαδρομή δρομολόγησης με συσχέτιση των διακινούμενων μηνυμάτων, εντοπίζοντας με τον τρόπο αυτό τον αποστολέα του

μηνύματος (hop-by-hop traceback). Έχουν προταθεί διάφορες τεχνικές για την εξασφάλιση ανωνυμίας θέσης του κόμβου αποστολέα. Λύση στο πρόβλημα προσφέρουν οι στρατηγικές δρομολόγησης φαντάσματος (phantom routing) με χρήση τεχνικών (α) τυχαίων μονοπατιών και τεχνικών πλημμυρίσματος [80,81], (β) προσαρμοσμένου κατευθυνόμενου τυχαίου περιπάτου (self-adjusting directed random walk) [82] και (γ) τυχαίου περιπάτου δύο κατευθύνσεων [83], καθώς και οι μηχανισμοί περιττής κυκλοφορίας [84] και ενδιάμεσης αποθήκευσης μηνυμάτων (message buffering) [85].

Η εξασφάλιση ανωνυμίας ταυτοτήτων στο δίκτυο (network identity privacy) στοχεύει στην αποτροπή συσχέτισης των διακινούμενων μηνυμάτων με ανάγνωση των αναγνωριστικών των κόμβων που συμμετέχουν στη δρομολόγηση. Η απόκρυψη των μόνιμων ταυτοτήτων των κόμβων που συμμετέχουν στη δρομολόγηση και ανταλλαγή μηνυμάτων στο δίκτυο επιτυγχάνεται με τεχνικές ψευδωνυμίας κόμβων και μονοπατιών [71].



Σχήμα 4.6. Στρατηγική phantom routing

4.7.2 Ελεγχόμενη προσπέλαση δεδομένων

Η ελεγχόμενη προσπέλαση δεδομένων στοχεύει στην προστασία του περιεχομένου των μηνυμάτων από κοινοποίηση σε μη εξουσιοδοτημένες οντότητες (κακόβουλες συσκευές), με εφαρμογή κατάλληλων μηχανισμών για την εξασφάλιση της ιδιωτικότητας των συμμετεχόντων στην επικοινωνία κόμβων. Υλοποιείται με μηχανισμούς, οι οποίοι μπορούν να κατηγοριοποιηθούν σε μηχανισμούς που στοχεύουν (α) στην ελεγχόμενη πρόσβαση, (β) στην προσαρμογή επιπέδου λεπτομέρειας πληροφοριών και (γ) στην προστασία ενάντια σε εξαγωγή συμπεράσματος ταυτότητας και θέσης [71].

Η χρήση πολιτικών και δικαιωμάτων πρόσβασης (privacy policies and preferences) αποσκοπεί στην επίτευξη ελεγχόμενης πρόσβασης στο δίκτυο WSN, η οποία όμως προσθέτει πολυπλοκότητα ιδίως σε δίκτυα με σύνθετο περιβάλλον συλλογής πληροφορίας [71]. Στη βιβλιογραφία έχουν προταθεί μηχανισμοί για τον καθορισμό και εφαρμογή πολιτικών και δικαιωμάτων πρόσβασης, οι οποίοι είτε στηρίζονται σε μια κεντρική οντότητα διαχείρισης [86], είτε πραγματοποιούν ελεγχόμενη πρόσβαση με κατανεμημένο τρόπο [87], [88].

Η προσαρμογή του επιπέδου λεπτομέρειας γίνεται με γνώμονα την κάλυψη στο ελάχιστο δυνατό τις πληροφοριακές ανάγκες που τίθενται στο δίκτυο, οι οποίες μπορούν να αφορούν σε πληροφορίες θέσης, ταχύτητας, ταυτότητας ή χρόνου στον οποίο γίνονται οι μετρήσεις [71]. Ωστόσο, η προστασία ενάντια σε εξαγωγή συμπεράσματος ταυτότητας και θέσης σε δίκτυα WSN, στα οποία τίθενται προδιαγραφές που απαιτούν λεπτομερείς συλλεγόμενες πληροφορίες, έχουν προταθεί στη βιβλιογραφία μηχανισμοί που καλύπτουν τις απαιτήσεις ιδιωτικότητας. Τέτοιοι μηχανισμοί είναι η αρχιτεκτονική AnonySense [89] και μηχανισμοί που προτείνονται στα [90] και [91].

4.7.3 Ελεγχόμενη συλλογή δεδομένων

Η έννοια της ελεγχόμενης συλλογής δεδομένων επικεντρώνεται στην επίτευξη ανωνυμίας των οντοτήτων του δικτύου WSN, στο σημείο που τα δεδομένα συλλέγονται, πριν τη διεξαγωγή του ελέγχου προσπέλασης. Η επίτευξη ανωνυμίας και επομένως η ιδιωτικότητα επιτυγχάνεται με το καθορισμό των δυνατοτήτων συλλογής πληροφορίας στο ελάχιστο δυνατό με βάση τις απαιτήσεις της εφαρμογής για την κάλυψη των πληροφοριακών αναγκών της. Ένας τρόπος συμμόρφωσης στην παραπάνω συνθήκη είναι η επιβολή από τους χρησιμοποιούμενους μηχανισμούς της ελάχιστης απαραίτητης μείωσης του επιπέδου λεπτομέρειας σε διάφορα στάδια της διαδικασίας ιεραρχικής συνάθροισης πληροφοριών. Προς τη κατεύθυνση υλοποίησης ελεγχόμενης συλλογής δεδομένων έχουν προταθεί μηχανισμοί, όπως το σύστημα TinyCasper [92] και η τεχνική των αρνητικών ερευνών (negative surveys) [93].

4.8 Ασφαλής δρομολόγηση (Secure Routing) – Ασφάλεια ζεύξης επικοινωνίας

Στο δεύτερο κεφάλαιο έγινε αναφορά σε πρωτόκολλα δρομολόγησης, τα οποία έχουν σχεδιαστεί για τη κάλυψη τυπικών εφαρμογών δικτύων WSN. Ωστόσο, τα περισσότερα από τα πρωτόκολλα αυτά δεν εξετάζουν θέματα ασφαλείας, αλλά

στοχεύουν επί το πλείστον στην αξιοπιστία επικοινωνίας δίνοντας βαρύτητα στην εξοικονόμηση ενέργειας και την απλότητα υπολογισμών. Η επίτευξη αξιόπιστης επικοινωνίας και ανταλλαγής μηνυμάτων μεταξύ των κόμβων του δικτύου είναι κρίσιμη, αλλά δεν είναι αρκετή σε δίκτυα που προέχει η ασφάλεια καθώς πρέπει να καλύπτονται οι προδιαγραφές που αναφέρθηκαν στο προηγούμενο κεφάλαιο. Οι λειτουργίες του επιπέδου δικτύου και η απαίτηση διαθεσιμότητας ενός δικτύου WSN εξασφαλίζονται μέσω ενός ασφαλούς μηχανισμού δρομολόγησης.

Το επίπεδο δικτύου έχει να αντιμετωπίσει πληθώρα επιθέσεων με συνήθεις τις επιθέσεις μετάδοσης ψευδών μηνυμάτων, επιλεκτικής προώθησης, καταβόθρας, σιβυλλικής μορφής, σκουληκότρυπας, HELLO flood και πλαστογράφησης μηνυμάτων αναγνώρισης. Στον Πίνακα 4.3 απεικονίζονται οι επιθέσεις επιπέδου δικτύου που αφορούν σε τυπικά πρωτόκολλα δρομολόγησης [69].

Πρωτόκολλο δρομολόγησης	**Σχετιζόμενη επίθεση**
Κατευθυνόμενη διάδοση (directed diffusion)	Επίθεση μετάδοσης ψευδών μηνυμάτων, επιλεκτική προώθηση, καταβόθρες, σιβυλλική επίθεση, σκουληκότρυπες, HELLO floods
Πρωτόκολλα γεωγραφικής δρομολόγησης (GPSR, GEAR)	Επίθεση μετάδοσης ψευδών μηνυμάτων, επιλεκτική προώθηση, σιβυλλική επίθεση
Προώθηση ελάχιστου κόστους	Επίθεση μετάδοσης ψευδών μηνυμάτων, επιλεκτική προώθηση, καταβόθρες, σκουληκότρυπες, HELLO floods
Ιεραρχικά πρωτόκολλα (LEACH, TEEN, PEGASIS)	Επιλεκτική προώθηση, HELLO floods
Δρομολόγηση με βάση τη φήμη (rumor routing)	Επίθεση μετάδοσης ψευδών μηνυμάτων, επιλεκτική προώθηση, καταβόθρες, σιβυλλική επίθεση, σκουληκότρυπες
Πρωτόκολλα εξοικονόμησης ενέργειας (SPAN, GAF)	Επίθεση μετάδοσης ψευδών μηνυμάτων, σιβυλλική επίθεση, HELLO floods

Πίνακας 4.3. Συμβατές επιθέσεις με πρωτόκολλα δρομολόγησης

Ένας επικεντρωμένος σε ζητήματα ασφάλειας μηχανισμός δρομολόγησης έχει να αντιμετωπίσει τρεις βασικές προκλήσεις, οι οποίες είναι (α) η πρόληψη, (β) η ανίχνευση της επίθεσης, (γ) η ανάκτηση λειτουργιών και η ανθεκτικότητα σε επιθέσεις (ευρωστία). Για το σκοπό αυτό και την εξάλειψη των απειλών από ενδεχόμενες επιθέσεις, πρέπει να συμψηφιστούν στο σχεδιασμό του δικτύου τεχνικές αυθεντικοποίησης (πιστοποίηση ταυτότητας κόμβων) και κρυπτογράφηση. Επιπλέον, οι τεχνικές πλεονασμού της μεταδιδόμενης πληροφορίας και η πολυδιαδρομική δρομολόγηση κινούνται προς αυτή τη κατεύθυνση.

Με γνώμονα τις παραπάνω προκλήσεις έχουν σχεδιαστεί πρωτόκολλα [68], σημαντικότερα των οποίων είναι το SPINS (Security Protocols for Sensor Networks) [114], SIGF (Secure Implicit Geographic Forwarding) [115], INSENS (Intrusion Tolerant Routing protocol for Wireless Sensor Networks) [116], DAWWSEN (Defense Mechanism Against Wormhole attacks in Wireless Sensor Networks) [54], και SSNRP-CSA (Secure Sensor Network Routing Protocol – Clean-Slate Approach) [117].

Το πρωτόκολλο SPINS αποτελείται από δύο δομές, οι οποίες είναι τα πρωτόκολλα SNEP (Sensor Network Encryption Protocol) και μTESLA (micro version of Timed, Efficient, Streaming, Loss – tolerant Authentication Protocol). Το SNEP προσφέρει στην επικοινωνία εμπιστευτικότητα, αυθεντικοποίηση δύο μερών (two-party authentication) και φρεσκάδα δεδομένων, ενώ το μTESLA προσδίδει συμπληρωματικά αυθεντικοποίηση ευρυεκπομπής (broadcast authentication). Επιπρόσθετα, το μTESLA έχει σχεδιασθεί με γνώμονα την εξοικονόμηση πόρων του δικτύου, κάτι που είναι κρίσιμης σημασίας για δίκτυα WSN. Ωστόσο, το πρωτόκολλο SPINS λαμβάνει μέτρα μόνο για την πρόληψη επιθέσεων και όχι για την ανίχνευση, την ανάκτηση λειτουργιών και την ανθεκτικότητα σε επιθέσεις. Ως εκ τούτου, η ασφάλεια που παρέχει το πρωτόκολλο είναι περιορισμένη σε περίπτωση παρουσίας κακόβουλης ενέργειας. Για λόγο αυτό, κρίνεται ακατάλληλο για εφαρμογές, στις οποίες οι απαιτήσεις ασφαλείας είναι αυστηρές.

Το πρωτόκολλο SIGF βασίζεται στη θέση των κόμβων που συμμετέχουν στη δρομολόγηση, επιλέγοντας δυναμικά το επόμενο άλμα στην προώθηση της πληροφορίας με πολλαπλά άλματα. Περιλαμβάνει τρία πρωτόκολλα (SIGF-0, SIGF-1, SIGF-2), τα οποία συνεργατικά παρέχουν πρόληψη από επιθέσεις με ισχυρή εγγύηση στις απαιτήσεις ασφαλείας. Το εν λόγω πρωτόκολλο παρέχει προστασία από επιθέσεις ψευδών μηνυμάτων, σκουληκότρυπας, HELLO flood, μαύρης τρύπας,

σιβυλλικής μορφής και επανεκπομπής, με χρήση μεθόδων αυθεντικοποίησης και κρυπτογράφησης. Ωστόσο όμοια με το SPINS, επικεντρώνεται κυρίως στην πρόληψη εκδήλωσης επιθέσεων.

Το πρωτόκολλο INSENS βασίζεται στην εφαρμογή πολυδιαδρομικής δρομολόγησης της πληροφορίας, προσθέτοντας ανθεκτικότητα σε επιθέσεις στο επίπεδο δικτύου. Επιπλέον, το εν λόγω πρωτόκολλο προσδίδει προστασία από επιθέσεις άρνησης εξυπηρέτησης, κακόβουλες ενέργειες κατά την προώθηση δεδομένων και κακόβουλων ενεργειών κατά της εύρεσης μονοπατιού δρομολόγησης, όπως αποδεικνύεται από την προσομοίωση που διενεργείται στο [116]. Το πρωτόκολλο εκμεταλλεύεται τον πλεονασμό της πληροφορίας, επιτυγχάνοντας ευρωστία σε παρουσία κακόβουλης ενέργειας. Επιπλέον, αναθέτει αποκλειστικά όλες τις λειτουργίες με μεγάλες απαιτήσεις σε υπολογισμούς, περιορίζοντας τους αισθητήριους κόμβους σε υπολογισμούς που σχετίζονται με την ανεύρεση μονοπατιών δρομολόγησης και ανθεκτικότητας παρεισφρήσεων. Με τον τρόπο αυτό, ελαχιστοποιεί τις απαιτήσεις σε πόρους (υπολογισμοί, μνήμη, εύρος ζώνης) στους αισθητήριους κόμβους. Επίσης, με χρήση κρυπτογράφησης συμμετρικού κλειδιού και μηχανισμών αυθεντικοποίησης, το πρωτόκολλο επιτυγχάνει τον περιορισμό επιπτώσεων παρεισφρήσεων, που ενδεχομένως δεν έχουν ανιχνευθεί. Αν και δεν παρέχει ανίχνευση παρεισφρήσεων, το συγκεκριμένο πρωτόκολλο υπερτερεί έναντι των υπολοίπων καθώς λειτουργεί ικανοποιητικά ακόμα και σε περίπτωση παρείσφρησης σε ένα τμήμα του δικτύου.

Το πρωτόκολλο δρομολόγησης DAWWSEN παρέχει προστασία από επιθέσεις σκουληκότρυπας, όπως έχει ήδη αναφερθεί. Πρόκειται για ένα προληπτικό πρωτόκολλο, το οποίο βασίζεται στην ιεραρχική δρομολόγηση. Το εν λόγω πρωτόκολλο προσδίδει επιπλέον δυνατότητα ανίχνευσης της συγκεκριμένης επίθεσης. Πλεονεκτήματα του είναι η μη αναγκαιότητα διάθεσης πληροφορίας θέσης από τους κόμβους, και η απλότητα στη μέθοδο ανίχνευσης της επίθεσης, τα οποία κρίνονται σημαντικά σε ένα δίκτυο WSN, όπου οι περιορισμοί σε πόρους είναι υπαρκτοί.

Τέλος, το πρωτόκολλο SSNRP-CSA είναι αποτελεσματικό στην επίτευξη ευρωστίας σε παρουσία επιθέσεων ενεργητικής μορφής στο επίπεδο δικτύου. Το εν λόγω πρωτόκολλο βασίζεται σε ασύμμετρη κρυπτογράφηση, η οποία είναι ασυνήθης σε δίκτυα WSN. Ωστόσο, έχει ληφθεί μέριμνα από τους σχεδιαστές του, ώστε να περιορίσουν την πολυπλοκότητα της κρυπτογράφησης σε αποδεκτά όρια.

Σε επίπεδο ζεύξης επικοινωνίας μεταξύ κόμβων και στα πλαίσια των ιδιαιτεροτήτων ενός δικτύου WSN, έχουν αναπτυχθεί πρωτόκολλα για την υλοποίηση των λειτουργιών του επιπέδου ζεύξης, με γνώμονα την ασφάλεια. Σημαντικότερα πρωτόκολλα είναι το TinySec [130], το LLSP (Link-Layer Protocol) και το MiniSec [131]. Σημαντική κρίνεται η αυθεντικοποίηση στο επίπεδο ζεύξης, καθώς προσφέρει το πλεονέκτημα της γρήγορης ανίχνευσης παραποιημένων πακέτων, με αποτέλεσμα την εξοικονόμηση ενέργειας από επανεκπομπές πακέτων μεταξύ των κόμβων του δικτύου.

Το πρωτόκολλο TinySec παρέχει αυθεντικοποίηση, εμπιστευτικότητα, ακεραιότητα και φρεσκάδα δεδομένων με χρήση συμμετρικών αλγορίθμων κρυπτογράφησης RC5 και Skipjack. Το πρωτόκολλο LLSP είναι ενεργειακά αποδοτικότερο σε σχέση με το TinySec, καλύπτοντας όμως λιγότερες απαιτήσεις ασφαλείας. Συγκεκριμένα, το εν λόγω πρωτόκολλο παρέχει αυθεντικοποίηση και εμπιστευτικότητα στην επικοινωνία μεταξύ των κόμβων με χρήση του συμμετρικού αλγορίθμου κρυπτογράφησης AES. Το πρωτόκολλο MiniSec σχεδιάστηκε με γνώμονα, την εξισορρόπηση μεταξύ κάλυψης απαιτήσεων ασφαλείας και εξοικονόμησης ενέργειας. Συγκεκριμένα, επιτυγχάνει υψηλού επιπέδου αυθεντικοποίηση, μυστικότητα δεδομένων (data secrecy) και προστασία έναντι επανεκπομπών, με σημαντικά μικρότερη κατανάλωση ενέργειας, σε σύγκριση με το πρωτόκολλο TinySec (3 φορές μικρότερη, σύμφωνα με το [131]).

4.9 Ασφάλεια διασταυρωμένου επιπέδου (Cross Layer Security)

Η συνήθης πρακτική στην προσέγγιση ζητημάτων ασφάλειας σε δίκτυα WSN επικεντρώνεται στη μελέτη με βάση την πολυεπίπεδη αρχιτεκτονική ενός τέτοιου δικτύου. Στο πλαίσιο αυτό έχει πραγματοποιηθεί και η εξέταση των συγκεκριμένων ζητημάτων στην παρούσα εργασία. Ωστόσο, τα μοντέλα που βασίζονται σε αυτό το σκεπτικό υποφέρουν από πολυπλοκότητα, εξαιτίας του πλεονασμού μέτρων ασφαλείας και από έλλειψη ευελιξίας των εφαρμοζόμενων μηχανισμών. Στο [76] γίνεται μια διαφορετική προσέγγιση των ζητημάτων ασφαλείας, η οποία είναι εφαρμόσιμη και σε δίκτυα με υψηλές απαιτήσεις ασφαλείας (HSRA – Hard Security Requirement Applications). Η προσέγγιση αυτή, η οποία βασίζεται σε παράλληλη θεώρηση των επιπέδων WSN (διασταυρούμενη θεώρηση), διασφαλίζοντας ταυτόχρονα τις λειτουργίες όλων των επιπέδων, αφορά στο πρωτόκολλο CLIFFs (Cross Layer Integrated Framework for security for WSN). Το συγκεκριμένο

πρωτόκολλο κάνει χρήση του συμμετρικού αλγορίθμου RC5 για εφαρμογές HSRA με μήκος κλειδιού 80 ψηφίων (RC5/80/4). Επιπρόσθετα, το πρωτόκολλο CLIFFs επιδρά στις λειτουργίες του δικτύου ενεργειακά αποδοτικότερα με χρήση της οντότητας ISA (Intelligent Security Agent), η οποία προσφέρει ευφυΐα σε διαδικασίες ανίχνευσης κακόβουλων ενεργειών και λήψης προκαθορισμένων μέτρων αντιμετώπισης τους.

4.10 Ασφάλεια τεχνολογίας ZigBee και προτύπου Bluetooth

Το πρωτόκολλο IEEE 802.15.4 προσδίδει ευελιξία ως προς το εφαρμοζόμενο επίπεδο ασφάλειας. Το πρωτόκολλο χρησιμοποιεί το συμμετρικό αλγόριθμο κρυπτογράφησης AES-128bits και αλγορίθμους MICs (Message Integrity Code), προσφέροντας εμπιστευτικότητα και αυθεντικοποίηση δεδομένων σε κάθε ζεύξη [133]. Ωστόσο, δεν καθορίζει μηχανισμούς διανομής κρυπτογραφικών κλειδιών και πιστοποίησης ταυτότητας οντοτήτων (ιδιωτικότητα).

Το πρωτόκολλο ZigBee, το οποίο συμπληρώνει το IEEE 802.15.4 (Κεφάλαιο 2), προσθέτει μηχανισμούς διαχείρισης κρυπτογραφικών κλειδιών και πιστοποίησης ταυτότητας. Οι μηχανισμοί αυτοί βασίζονται στον καθορισμό τριών τύπων κλειδιών (pairwise keys, network keys και master keys) και ενός κέντρου εμπιστοσύνης (TC – Trust Center) καθώς και στο σχήμα SKKE (Symmetric – Key Key Exchange) [133]. Η οντότητα TC υλοποιείται στο σταθμό βάσης και είναι μια συσκευή, η οποία θεωρείται αξιόπιστη και εύρωστη έναντι κακόβουλων ενεργειών. Επιπλέον, το συγκεκριμένο πρωτόκολλο προσφέρει εμπιστευτικότητα, ακεραιότητα και αυθεντικοποίηση δεδομένων, με χρήση του κρυπτογραφικού αλγόριθμου AES-128bits και της λειτουργίας CCM (Counter with CBC-MAC) του πρωτοκόλλου [133].

Τέλος, το πρωτόκολλο Bluetooth παρέχει μηχανισμούς διαχείρισης κρυπτογραφικών κλειδιών παρέχοντας στην επικοινωνία πιστοποίηση ταυτότητας, εμπιστευτικότητα και ακεραιότητα δεδομένων. Η εξασφάλιση των παραπάνω απαιτήσεων επιτυγχάνεται με το συνδυασμό τριών τύπων κρυπτογραφικών κλειδιών (initialization keys, combination keys και master keys) [133].

Κεφάλαιο 5. Σενάριο διαχείρισης ζητημάτων ασφαλείας σε δίκτυο επιτήρησης περιοχής

5.1 Εισαγωγή

Με την εξέλιξη της μικροηλεκτρονικής και την παραγωγή σε ευρεία κλίμακα και με μικρό κόστος ολοκληρωμένων συστημάτων κόμβων (mote + μικροαισθητήρες) υπήρξε μεγάλο ενδιαφέρον για χρήση των WSN για στρατιωτικές εφαρμογές (εθνικής ασφάλειας) και ιδιαίτερα στην προστασία των συνόρων και στην επιτήρηση κρίσιμων περιοχών. Στις εφαρμογές που έχουν προταθεί από ερευνητικές ομάδες γίνεται χρήση αισθητήρων δόνησης (σεισμικοί), υπερύθρων (IR), συσκευών καταγραφής video (θερμικές ή μη) και ανιχνευτών κίνησης για τη συλλογή πληροφοριών. Ενδεικτικά, τέτοιες εφαρμογές είναι το σύστημα παρακολούθησης χαμηλής κατανάλωσης που προτείνεται στο [118] και τα συστήματα VigilNet [128], "A line in the sand" [126], FleGSens [127] και BorderSense [119].

Στο παρόν κεφάλαιο θα εξεταστεί η διαχείριση θεμάτων ασφαλείας σε ένα δίκτυο επιτήρησης περιοχής ενός δικτύου βασισμένου στο σύστημα BorderSense. Το εξεταζόμενο δίκτυο στοχεύει στην ανίχνευση κίνησης εντός μιας κρίσιμης περιοχής επιτήρησης, την εξακρίβωση του εισβολέα με χρήση ενός δικτύου πολυμέσων WMSN και εν συνεχεία την παρακολούθηση του σύμφωνα με τα καθοριζόμενα στο εν λόγω σύστημα. Η εγκατάσταση γίνεται σε χερσαία έκταση, όπου οι κόμβοι τοποθετούνται με δομημένο τρόπο (structured WSN), έτσι ώστε να μην υπάρχουν σημεία εντός της περιοχής κάλυψης που να βρίσκονται εκτός εμβέλειας τουλάχιστον δύο αισθητήριων κόμβων. Οι κόμβοι δεν έχουν απαραίτητα οπτική επαφή και επικοινωνούν με χρήση ραδιοσυχνοτήτων. Επίσης, θεωρούμε ότι ο τελικός χρήστης του δικτύου δεν ενδιαφέρεται τόσο για την πιθανότητα ενός ψευδούς συναγερμού, όσο για την πιθανότητα μη ανίχνευσης ή αδυναμίας δρομολόγησης πακέτων πληροφορίας προς το σταθμό βάσης. Η πιθανότητα ψευδούς συναγερμού μπορεί να ελεγχθεί με το δίκτυο πολυμέσων στο οποίο ο χρήστης θεωρούμε ότι έχει πλήρη πρόσβαση (θεωρούμε ότι το δίκτυο αυτό είναι πλήρως ασφαλισμένο). Με βάση αυτή την υπόθεση, στη συνέχεια γίνεται η μελέτη ζητημάτων ασφαλείας ενός δικτύου επιτήρησης με στόχο την κάλυψη προδιαγραφών που εξετάζονται στη συνέχεια. Προς αυτή την κατεύθυνση, θα προταθούν πρωτόκολλα επικοινωνίας και μηχανισμοί αντιμετώπισης επιθέσεων για την εξασφάλιση ασφαλούς και αξιόπιστης επικοινωνίας.

5.2 Προδιαγραφές ασφαλείας

Οι προδιαγραφές ασφαλείας του εξεταζόμενου μοντέλου, το οποίο θεωρείται υπηρεσία υψηλών απαιτήσεων ασφαλείας (HSRA – Hard Security Requirements Application) είναι η εμπιστευτικότητα, η ακεραιότητα, η φρεσκάδα, η διαθεσιμότητα και η αυθεντικότητα των δεδομένων, όπως αυτές αναφέρθηκαν στο Κεφάλαιο 3. Ωστόσο, βασικότερο ζήτημα ασφάλειας ενός δικτύου επιτήρησης περιοχής κρίνεται η συνεχής διαθεσιμότητα του δικτύου. Στο εξεταζόμενο μοντέλο θα δοθεί βαρύτητα στην επίτευξη αξιοπιστίας και διαθεσιμότητας κάτω από δυσμενείς συνθήκες (εκδήλωση κακόβουλων ενεργειών). Για το λόγο αυτό, στο εξεταζόμενο μοντέλο πρέπει να ληφθεί μέριμνα κυρίως κατά των επιθέσεων άρνησης εξυπηρέτησης (DoS). Ειδικότερα, το μοντέλο πρέπει να είναι ανθεκτικό κυρίως σε επιθέσεις παρεμβολών, σύγκρουσης δεδομένων, εξάντλησης ενεργειακών πόρων, μαύρης τρύπας και επιλεκτικής προώθησης. Επιπλέον, κρίνεται σκόπιμη η εξασφάλιση ανοχής κατά των φυσικών επιθέσεων, επιθέσεων αναπαραγωγής κόμβου, καταβόθρας σιβυλλικής και ανάλυσης κίνησης, οι οποίες μπορούν να επηρεάσουν άμεσα (φυσικές επιθέσεις, επιθέσεις καταβόθρας) ή έμμεσα (επιθέσεις αναπαραγωγής κόμβου σιβυλλικής και ανάλυσης κίνησης) τη διαθεσιμότητα των υπηρεσιών του δικτύου. Επίσης, απαιτήσεις του δικτύου, οι οποίες απορρέουν από τα παραπάνω, είναι η ασφαλής δρομολόγηση, η ασφαλής συνάθροιση δεδομένων και η ενεργειακά αποδοτική διαχείριση κρυπτογραφικών κλειδιών. Επιπρόσθετα, το δίκτυο είναι θεμιτό να λειτουργεί δυναμικά και να υποστηρίζει προσθήκη νέων κόμβων και αφαίρεση άλλων κατεστραμμένων ή κακόβουλων. Τέλος, στο πλαίσιο ασφαλούς επικοινωνίας των οντοτήτων του δικτύου, κρίνεται σημαντική η αξιοπιστία του συνόλου των λειτουργιών και της ποιότητας υπηρεσίας (QoS), η οποία πρέπει να διασφαλισθεί. Συνοψίζοντας, οι προδιαγραφές που πρέπει να έχει το συγκεκριμένο δίκτυο είναι:

- Εμπιστευτικότητα, ακεραιότητα, φρεσκάδα, διαθεσιμότητα και αυθεντικότητα δεδομένων
- Ανθεκτικότητα σε επιθέσεις άρνησης εξυπηρέτησης (DoS), φυσικές, αναπαραγωγής κόμβου, καταβόθρας, σιβυλλικής και ανάλυσης κίνησης
- Ασφαλής δρομολόγηση
- Ασφαλής συνάθροιση δεδομένων
- Δυνατότητα προσθήκης και αφαίρεσης κόμβου

- Ενεργειακά αποδοτική διαχείριση κρυπτογραφικών κλειδιών
- Μέριμνα για ζητήματα εξασφάλισης αξιοπιστίας και ποιότητας υπηρεσίας

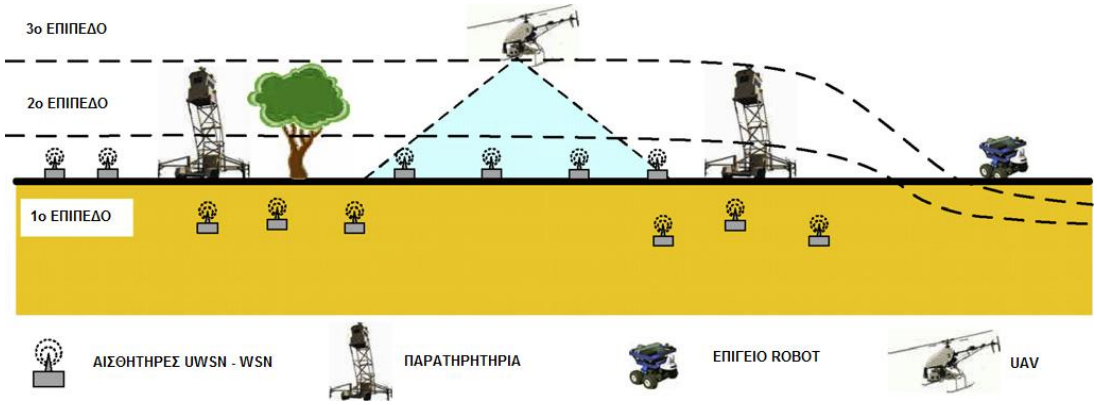
5.3 Περιγραφή συστήματος επιτήρησης

Το σύστημα BordeSense [119] αποτελεί μια εστιασμένη και ώριμη προσέγγιση πάνω στο θέμα της προστασίας και επιτήρησης των συνόρων. Στην εφαρμογή προτείνεται ο συνδυασμός διαφορετικών ειδών αισθητήριων μέσων (κινητά, προ-τοποθετημένα) με την εξής ιεράρχηση αποστολών για κάθε επίπεδο αισθητήρων: (α) αρχικός εντοπισμός, (β) εξακρίβωση απειλής και (γ) παρακολούθηση και περιορισμός του στόχου. Το μοντέλο προτείνει ένα σύστημα δομημένο σε τρία επίπεδα ως εξής:

- Ένα δίκτυο σεισμικών ασύρματων αισθητήρων είτε υπέργειων (WSN) είτε υπόγειων (UWSN) με σαφή μειονεκτήματα και πλεονεκτήματα στη κάθε περίπτωση. Στα UWSN υφίσταται διαφορετικός τρόπος διάδοσης λόγω του εδάφους όπως επισημαίνεται στα [120,121,123]. Η διάδοση δεν γίνεται πλέον στον αέρα, αλλά σε μέσο το οποίο αποτελείται από γαιώδες ή βραχώδες έδαφος και νερό. Κατά συνέπεια τα μοντέλα διάδοσης και απωλειών μεταβάλλονται, επηρεάζοντας και την εκτίμηση και την κάλυψη [122]. Επίσης, η υπόγεια τοποθέτηση των αισθητήρων δυσχεραίνει την φόρτιση, συντήρηση ή αντικατάσταση των κόμβων του δικτύου από τη στιγμή που λειτουργούν με περιορισμένη τροφοδοσία και κάτω από δυσμενείς περιβαλλοντικές συνθήκες. Η εταιρεία Trident προσφέρει ένα ολοκληρωμένο προϊόν UWSN με δυνατότητες προσομοίωσης και οπτικής απεικόνισης [124] μέσω software που παρέχεται μαζί με τους αισθητήρες. Στα υπέργεια WSN, αίρονται αυτές οι δυσκολίες αλλά για τον ίδιο τύπο αισθητήρα (σεισμικό) μειώνεται η εμβέλεια και η ευαισθησία ανίχνευσης. Τελικά, επιλέγεται για την εφαρμογή η χρήση των υπόγειων αισθητήρων, οι οποίοι δίνουν δυνατότητα ανίχνευσης δονήσεων και μαγνητικών ανωμαλιών (που αντιστοιχούν σε ανθρώπους και οχήματα που διασχίζουν την περιοχή ενδιαφέροντος) με μέγιστη εμβέλεια 50μ και 500μ αντίστοιχα. Παρά την αποτελεσματικότητα του UWSN στην ανίχνευση, η κατηγοριοποίηση της απειλής δεν πραγματοποιείται σ' αυτό το επίπεδο.
- Ένα ασύρματο δίκτυο αισθητήρων πολυμέσων (WMSN) [125], το οποίο αποτελείται από κόμβους πολυμέσων τοποθετημένους μόνιμα σε παρατηρητήρια (όμοια με αυτά που επανδρώνονται από τα ελληνικά φυλάκια στην συνοριακή γραμμή), οι οποίοι χρησιμοποιούν κάμερες σαν κύριο μέσο παρακολούθησης. Οι

κόμβοι αυτοί έχουν μεγάλη εμβέλεια και επιτελούν ρόλο επικεφαλής ομάδων κόμβων (cluster heads) καθώς έχουν μεγαλύτερες επεξεργαστικές και αποθηκευτικές δυνατότητες. Η ανίχνευση ενός πιθανού εισβολέα από το πρώτο επίπεδο αισθητήρων (UWSN) αφυπνίζει το WMSN το οποίο εστιάζει στη περιοχή που σημειώθηκε η παραβίαση. Η ταυτοποίηση μπορεί να γίνει είτε από προσωπικό τοπικά, είτε μέσω ειδικών αλγορίθμων επεξεργασίας εικόνας στους WMSN κόμβους, είτε σε κάποιο απομακρυσμένο εξυπηρετητή. Με το τέλος της κατηγοριοποίησης, δίνεται εντολή στο τρίτο επίπεδο για παρακολούθηση και περιορισμό του στόχου.

- Ένα δίκτυο κινητών κόμβων (με τη μορφή drones ή UAV ή ground-robots) με δυνατότητες παρακολούθησης του στόχου ακόμα και όταν φύγει από την περιοχή που επιτηρείται. Στο σύστημα που αναπτύσσεται στο BordeSense δίνεται έμφαση στην εκμετάλλευση των UAV, καθώς αυτά είναι ήδη ενταγμένα στη φύλαξη των συνόρων στις ΗΠΑ. Τα στοιχεία που προκύπτουν από τα πρώτα επίπεδα θα μπορούσαν να διαβιβαστούν σε οποιοδήποτε φορητό ή σταθερό σύστημα το οποίο θα αποτελούσε εργαλείο εντοπισμού του στόχου στη διάθεση μιας π.χ. εποχούμενης περιπόλου.



Σχήμα 5.1. Επίπεδα συστήματος BorderSense

Επισημαίνεται για το σύστημα, ότι η αξιοπιστία και το χαμηλό ποσοστό ψευδών συναγερμών προκύπτει από τον συνδυασμό και την επικάλυψη των υπηρεσιών που προσφέρει κάθε επίπεδο κι όχι μεμονωμένα.

5.4 Ζητήματα ποιότητας υπηρεσίας

Η έννοια της ποιότητας υπηρεσίας (QoS) χρησιμοποιείται για την εκτίμηση συμμόρφωσης των υπηρεσιών του δικτύου με τις προδιαγραφές ασφαλείας. Η εξασφάλιση της ποιότητας υπηρεσίας και επομένως της συμμόρφωσης με τις

προδιαγραφές γίνεται με διασφάλιση των πόρων του δικτύου. Εξαιτίας των περιορισμών των πόρων ενός δικτύου WSN (υπολογιστικοί, ρυθμών μετάδοσης, αποθήκευσης και κατανάλωσης ενέργειας), η μελέτη QoS αποτελεί σημαντική πρόκληση. Τα πολλαπλά άλματα δυσχεραίνουν την εξασφάλιση της ποιότητας υπηρεσίας, καθώς σε κάθε άλμα εμφανίζεται μια πιθανότητα αποτυχίας. Θεωρώντας πολλαπλά άλματα και ανεξάρτητα ενδεχόμενα αποτυχίας σε καθένα από αυτά, η συνολική διαδικασία μπορεί να εκπέσει σε αξιοπιστία εκτός προδιαγραφών (οι πιθανότητες αποτυχίας σε κάθε άλμα πολλαπλασιάζονται για τον καθορισμό της συνολικής πιθανότητας αποτυχίας).

Η ποιότητα υπηρεσίας εξαρτάται από παραμέτρους, οι οποίοι για να καλυφθούν οδηγούν το δίκτυο σε κατανάλωση πόρων. Για την πλήρη εξασφάλιση των παραμέτρων απαιτείται η αυξημένη κατανάλωση ενέργειας και επομένως η μείωση του χρόνου ζωής του δικτύου, κάτι το οποίο είναι ανεπιθύμητο. Επομένως, προκύπτει ένα trade – off μεταξύ ποιότητας υπηρεσίας και κατανάλωσης ενέργειας, το οποίο πρέπει να ληφθεί σοβαρά υπόψη (εκπτώσεις ποιότητας σε μη κρίσιμες παραμέτρους για τη διασφάλιση κρισιμότερων και την εξοικονόμηση ενέργειας). Οι παράμετροι ποιότητας ενός δικτύου WSN [133] είναι:

- Όγκος μεταδιδόμενης πληροφορίας (throughput): Το σχεδιαζόμενο δίκτυο WSN δεν απαιτεί μεγάλους ρυθμούς μετάδοσης για διακίνηση μεγάλου όγκου δεδομένων και ως εκ τούτου, τα διακινούμενα πακέτα είναι μικρά σε μέγεθος. Επομένως, η συγκεκριμένη παράμετρος μπορεί να μην θεωρηθεί κρίσιμη με σκοπό την εξοικονόμηση ενέργειας και τη διάθεση ενεργειακών πόρων σε εξασφάλιση άλλων παραμέτρων.
- Ακρίβεια δεδομένων (data accuracy): Οι κόμβοι του εξεταζόμενου δικτύου αντιλαμβάνονται την κίνηση στην περιοχή επιτήρησης. Το δίκτυο βασίζει τη λειτουργία του στον πλεονασμό της μεταδιδόμενης πληροφορίας εξαιτίας της εγγύτητας των αισθητήριων κόμβων, οι οποίοι αντιλαμβάνονται το ίδιο φαινόμενο. Ο μεγαλύτερος πλεονασμός προσφέρει μεγαλύτερη αξιοπιστία δεδομένων, ενώ η ελάττωση του με καθορισμό περιοδικών διαστημάτων παύσης λειτουργίας ορισμένων κόμβων (sleep mode) μειώνει την αξιοπιστία με κέρδος την εξοικονόμηση ενέργειας.
- Καθυστέρηση (latency): Η συγκεκριμένη παράμετρος καθορίζει τον απαιτούμενο χρόνο για τη διακίνηση της πληροφορίας από τους αισθητήριους κόμβους προς το σταθμό βάσης. Εξαιρουμένων των δικτύων WMSN, τα οποία

μεταφέρουν ροή πληροφορίας εικόνας σε πραγματικό χρόνο, στα υπόλοιπα δίκτυα WSN η συγκεκριμένη παράμετρος δεν είναι κρίσιμη.

- Κινητικότητα (mobility): Η παράμετρος κινητικότητας είναι κρίσιμη σε εφαρμογές, στις οποίες οι κόμβοι του δικτύου υποστηρίζουν μερική ή πλήρη κινητικότητα. Η κινητικότητα των κόμβων μεταβάλει τη χωρική διάταξη τους και τις συνθήκες ασύρματης ζεύξης και πρέπει να ληφθεί υπόψη. Ωστόσο, σε εφαρμογές WSN, σαν και αυτή που εξετάζεται στην παρούσα εργασία, όπου οι κόμβοι δεν κινούνται και έχουν εγκατασταθεί μόνιμα με δομημένο τρόπο, μπορεί να παραληφθεί.
- Αξιοπιστία (reliability): Η αξιοπιστία είναι κρίσιμη παράμετρος για την επίτευξη αποδεκτής ποιότητας υπηρεσίας. Για την επίτευξη της χρησιμοποιούνται μηνύματα αναγνώρισης (acknowledgements) και τεχνικές διόρθωσης σφαλμάτων (error correction). Επιπλέον, ο πλεονασμός δεδομένων αυξάνει την αξιοπιστία με αύξηση όμως κατανάλωσης ενέργειας, εξαιτίας περισσότερων εκπομπών εντός του δικτύου. Επιπρόσθετα, οι τεχνικές συνάθροισης δεδομένων μπορεί να μειώνει την αξιοπιστία στο δίκτυο (πιθανότητα απωλειών πακέτων), αλλά προσφέρει εξοικονόμηση ενέργειας.
- Ασφάλεια (security): Η ασφάλεια είναι κρίσιμης σημασίας σε εφαρμογές, στις οποίες υπάρχει υπόνοια ότι κάποιος επιτιθέμενος μπορεί να ενεργήσει κακόβουλα. Μια στρατιωτική εφαρμογή επιτήρησης περιοχής ανήκει σε αυτή την κατηγορία (εφαρμογή HSRA).

5.5 Υλοποίηση

Η υλοποίηση του σεναρίου επιτήρησης περιοχής, ενός μοντέλου τύπου BorderSense, γίνεται με εξέταση ζητημάτων ασφαλείας των λειτουργιών του. Διευκρινίζεται ότι στην παρούσα εργασία γίνεται εξέταση μόνο του δικτύου ανίχνευσης κίνησης WSN και όχι του δικτύου πολυμέσων WMSN, με το οποίο λειτουργεί διαδραστικά. Εξαιτίας των διαφορετικών χαρακτηριστικών τους (κυρίως σε θέμα ρυθμού μετάδοσης), οι λειτουργίες των δικτύων WMSN προσεγγίζονται με διαφορετικό τρόπο. Για το λόγο αυτό, θεωρούμε ότι το δίκτυο πολυμέσων είναι πλήρως ασφαλισμένο από κακόβουλες ενέργειες.

Οι κόμβοι του δικτύου υλοποιούνται με συσκευές, οι οποίες τοποθετούνται στο πεδίο επιτήρησης με δομημένο τρόπο, σε τοπολογία πλέγματος. Η τοπολογία αυτή ορίζει ότι η επικοινωνία γίνεται μεταξύ ισότιμων γειτονικών συσκευών. Κάθε

συσκευή εκπέμπει σε ένα κανάλι από τα συνολικά 16 της ζώνης συχνοτήτων 2400 – 2483.5 MHz, στα πρότυπα του πρωτοκόλλου IEEE 802.15.4. Η ρυθμοί μετάδοσης, οι οποίοι μπορούν να υποστηριχθούν είναι μέχρι 250 kbps με χρήση διαμόρφωσης O-QPSK.

Οι φυσικές επιθέσεις καθώς και οι επιθέσεις αναπαραγωγής κόμβου μπορούν να αποτραπούν ή περιοριστούν με φυσική απόκρυψη των αισθητήριων κόμβων του δικτύου. Επιπλέον, σημαντική είναι η χρήση συσκευών, οι οποίες παρέχουν ανθεκτικότητα ως προς τη τροποποίηση ή υποκλοπή ευαίσθητων δεδομένων (π.χ κρυπτογραφικών κλειδιών) και εμφανίζουν δυνατότητα αυτό-τερματισμού σε περίπτωση εκδήλωσης πρόθεσης αναπαραγωγής τους (robust low-frequency sensor). Σημαντική δικλείδα ασφαλείας για την επίτευξη προστασίας από αυτές τις επιθέσεις είναι η εφαρμογή τεχνικών ιδιωτικότητας, και συγκεκριμένα προστασίας θέσης του αισθητήριου κόμβου αποστολέα της πληροφορίας (π.χ τεχνική phantom routing).

Για αποφυγή παρεμβολών (επιθέσεις jamming) είναι σκόπιμη η εφαρμογή της τεχνικής μεταπήδησης συχνότητας FHSS (frequency-hopping spread spectrum), η οποία είναι ενεργειακά αποδοτικότερη από τη τεχνική διαμόρφωσης φάσματος. Η τεχνική μεταπήδησης συχνότητας στηρίζεται, όπως έχει ήδη αναφερθεί, σε αλγόριθμο καθορισμού του τρόπου μεταβολής της φέρουσας συχνότητας του σήματος πληροφορίας. Ο συγκεκριμένος αλγόριθμος ορίζει μια ακολουθία μεταπήδησης μεταξύ των χρησιμοποιούμενων φερόντων συχνοτήτων (16 κανάλια), η οποία είναι γνωστή μόνο στις αυθεντικοποιημένες οντότητες του δικτύου.

Στις λειτουργίες φυσικού επιπέδου δεν έγινε αναφορά σε ζητήματα εμπιστευτικότητας και αυθεντικότητας δικτύου. Η εξέταση των συγκεκριμένων προδιαγραφών παραλείφθηκε στη μελέτη λειτουργιών φυσικού επιπέδου, όπου δόθηκε βαρύτητα στη διαθεσιμότητα του δικτύου. Η παράλειψη αυτή έγινε με γνώμονα την εξοικονόμηση ενέργειας και την αποφυγή επιβάρυνσης του δικτύου με πληθώρα μηχανισμών ασφαλείας, οι οποίοι λειτουργούν πλεονασματικά και λειτουργούν αυξητικά ως προς την πολυπλοκότητα του δικτύου. Η πολυπλοκότητα αυξάνει τη κατανάλωση ενέργειας, καθώς απαιτείται μεγαλύτερος όγκος διακινούμενων πακέτων, και επομένως μειώνει το χρόνο ζωής του δικτύου.

Η επίθεση εξάντλησης ενεργειακών πόρων αντιμετωπίζεται με εφαρμογή πολλαπλής πρόσβασης διαίρεσης χρόνου TDMA. Τεχνική αυτή πρέπει να υλοποιηθεί σε συνδυασμό με τη τεχνική FHSS. Αυτό σημαίνει ότι σε μία γειτονιά κόμβων στο δίκτυο, εκπέμπει ένας μόνο κόμβος κατά τη διάρκεια μιας χρονοθυρίδας (timeslot),

σε συχνότητα που καθορίζει ο αλγόριθμος μεταπήδησης της τεχνικής FHSS. Επιπλέον, η χρήση TDMA, δεδομένου ότι ανά χρονοθυρίδα εκπέμπει μόνο ένας κόμβος, αποτρέπει επιθέσεις σύγκρουσης δεδομένων. Η παραπάνω θεώρηση όμως απαιτεί τον πλήρη συγχρονισμό των συσκευών του δικτύου. Για πληρέστερη εξασφάλιση έναντι τέτοιων επιθέσεων, μπορούν να εφαρμοσθούν συμπληρωματικά κώδικες διόρθωσης σφαλμάτων (error-correcting codes).

Το επίπεδο ζεύξης μπορεί να διασφαλιστεί με χρήση ενός ενεργειακά αποδοτικού πρωτοκόλλου, το οποίο όμως πρέπει να καλύπτει τις απαιτήσεις του δικτύου. Στην παρούσα λύση επιλέγεται η βέλτιστη λύση ως προς την εξισορρόπηση μεταξύ ζητημάτων κάλυψης απαιτήσεων ασφαλείας και κατανάλωσης ενέργειας, η οποία είναι το πρωτόκολλο MiniSec. Το συγκεκριμένο πρωτόκολλο επιτυγχάνει υψηλού επιπέδου αυθεντικοποίηση, μυστικότητα δεδομένων και προστασία έναντι επανεκπομπών (προστασία από επιθέσεις εξάντλησης πόρων), με σημαντικά μικρότερη κατανάλωση ενέργειας, σε σύγκριση με το δημοφιλές πρωτόκολλο TinySec.

Στο επίπεδο δικτύου πρέπει να εξασφαλιστεί η ασφαλής δρομολόγηση των πακέτων κατά τη μετάβαση τους με πολλαπλά άλματα, από τους αισθητήριους κόμβους προς το σταθμό βάσης και αντίστροφα. Η ασφαλής δρομολόγηση επιτυγχάνεται με την επιλογή κατάλληλου πρωτοκόλλου, το οποίο πρέπει να είναι εύρωστο σε επιθέσεις και να λειτουργεί αποτελεσματικά ακόμα και παρουσία τους. Στην παρούσα εργασία επιλέγεται το πρωτόκολλο INSENS, εξαιτίας της παρεχόμενης πληρότητας αντιμετώπισης επιθέσεων και της εξοικονόμησης πόρων (η πλειονότητα των διαδικασιών υλοποιούνται στο σταθμό βάσης). Το συγκεκριμένο πρωτόκολλο βασίζεται στην πολυδιαδρομική διάδοση, με καθορισμό πολλαπλών ανεξάρτητων μεταξύ τους μονοπατιών, δημιουργώντας με τον τρόπο αυτό πλεονασμό στη διακινούμενη πληροφορία. Ο πλεονασμός αυτός προσφέρει ευρωστία έναντι επιθέσεων επιλεκτικής προώθησης. Επιπλέον, οι επιθέσεις ανάλυσης κίνησης γίνονται λιγότερο αποτελεσματικές εξαιτίας της πολυδιαδρομικής διάδοσης.

Το πρωτόκολλο INSENS υποστηρίζει συμμετρική κρυπτογράφηση και κάθε κόμβος ανταλλάσσει με το σταθμό βάσης, κατά την αρχική εγκατάσταση του δικτύου, ένα κοινό κλειδί, μια μονόδρομη λειτουργία F και τον αρχικό αριθμό ακολουθίας K_o [116] τα οποία δεν μπορούν να υποκλαπούν από πιθανό επιτιθέμενο, χωρίς να προσβληθεί ο σταθμός βάσης. Τα στοιχεία αυτά αποτρέπει επιθέσεις αναπαραγωγής κόμβου και δυσχεραίνει τις σιβυλλικές επιθέσεις, καθώς προσφέρει αυθεντικοποίηση

στις οντότητες του δικτύου. Τέλος, το συγκεκριμένο πρωτόκολλο υποστηρίζει προσθήκη ή αφαίρεση κόμβου (τροποποιήσεις στο δίκτυο).

Ένα μειονέκτημα του πρωτοκόλλου INSENS, το οποίο πρέπει να καλυφθεί, είναι η έλλειψη δυνατότητας ανίχνευσης παρείσφρησης. Προς τη κατεύθυνση αυτή, γίνεται επιλογή της αρχιτεκτονικής IDS που περιγράφεται στο [65] και συγκεκριμένα της προσέγγισης ανίχνευσης με κατανεμημένο και συνεργατικό τρόπο. Με την αρχιτεκτονική αυτή, οι κακόβουλες ενέργειες που εντοπίζονται τοπικά ενεργοποιούν μια διαδικασία εξακρίβωσης της απειλής.

Η αξιοπιστία επικοινωνίας παρέχεται έμμεσα μέσω των εφαρμοζόμενων μηχανισμών ασφαλείας και άμεσα μέσω των εφαρμοζόμενων πρωτοκόλλων επικοινωνίας του επιπέδου μεταφοράς. Στο παρόν επίπεδο, δεν συνυπολογίζονται ζητήματα ασφαλείας, καθώς η κάλυψη των απαιτήσεων κρίνεται επαρκής, στα πλαίσια διατήρησης της πολυπλοκότητας σε ανεκτά επίπεδα και εξοικονόμησης ενέργειας. Όσον αφορά τη μετάδοση από τους αισθητήριους κόμβους προς το σταθμό βάσης επιλέγεται το πρωτόκολλο STCP, ενώ για την αντίστροφη μετάδοση το GARUDA. Τα συγκεκριμένα πρωτόκολλα παρέχουν αξιοπιστία μεταφοράς πακέτου με χρήση μηνυμάτων αναγνώρισης. Επιπλέον, το STCP προσφέρει δυνατότητες ελέγχου συμφορήσεων, ενώ το GARUDA αξιοπιστία του προορισμού του διακινούμενου πακέτου.

Επιπλέον, όσον αφορά την ασφαλή συνάθροιση δεδομένων, πρέπει να επιλεγεί μοντέλο, το οποίο (α) να καλύπτει το δίκτυο από επιθέσεις ενεργητικής μορφής, (β) να είναι συμβατό με συμμετρική κρυπτογράφηση, (γ) να είναι εύρωστο στο δυνατόν έναντι περισσότερων επιθέσεων και (δ) να καλύπτει το δυνατόν περισσότερες προδιαγραφές ασφαλείας σε υψηλό επίπεδο προστασίας. Τις παραπάνω προϋποθέσεις προσεγγίζει καλύτερα το μοντέλο SIA, το οποίο παρέχει με υψηλό επίπεδο προστασίας (α) ευρωστία σε επιθέσεις DoS, αναπαραγωγής κόμβου και επιλεκτικής προώθησης και (β) κάλυψη διαθεσιμότητας, εμπιστευτικότητας, ακεραιότητας, φρεσκάδας και αυθεντικότητας δεδομένων.

Τέλος, η διαχείριση κρυπτογραφικών κλειδιών πρέπει να γίνει με ενεργειακά αποδοτικό τρόπο. Η προσέγγιση των Eschenauer και Gligor είναι αυτή που ταιριάζει περισσότερο με την εφαρμογή καθώς διασφαλίζει την ασφαλή διανομή και με δυνατότητες ανάκλησης κρυπτογραφικών κλειδιών, με γνώμονα την εξοικονόμηση ενέργειας (προεγκατάσταση κρυπτογραφικών κλειδιών).

Στον Πίνακα 5.1 απεικονίζονται οι μηχανισμοί και τα πρωτόκολλα, που στοιχειοθετούν την υλοποίηση του σεναρίου.

Λειτουργία	**Μηχανισμός/Πρωτόκολλο**
Μετάδοση δεδομένων	2400 MHz/ 250 kbps/ O-QPSK, FHSS
Πρόσβαση στο μέσο μετάδοσης	TDMA, MiniSec
Δρομολόγηση	INSENS
Εξασφάλιση αξιοπιστίας	STCP, GARUDA
Ανίχνευση παρείσφρησης	Αρχιτεκτονική IDS ανίχνευσης με κατανεμημένο και συνεργατικό τρόπο
Συνάθροιση δεδομένων	SIA
Διαχείριση κρυπτογραφικών κλειδιών	Προσέγγιση Eschenauer και Gligor

Πίνακας 5.1. Μηχανισμοί και πρωτόκολλα υλοποίησης σεναρίου

5.6 Συμπεράσματα

Στην παρούσα εργασία, μελετήθηκαν ζητήματα που αφορούν σε ασύρματα δίκτυα αισθητήρων (WSN) και ειδικότερα σε ζητήματα ασφαλείας. Οι ιδιαιτερότητες των δικτύων WSN καθιστούν τη μελέτη των ζητημάτων αυτών μια συνεχή πρόκληση, καθώς τα συγκεκριμένα ζητήματα απαιτούν πολυπλοκότητα στη διαχείριση λειτουργιών του δικτύου. Η δυσκολία της μελέτης έγκειται στο γεγονός ότι οι κλασσικές μέθοδοι ασφαλείας που εφαρμόζονται σε άλλα δίκτυα δεν είναι συμβατές με δίκτυα WSN.

Το επιστημονικό πεδίο των δικτύων WSN είναι ταχέως αναπτυσσόμενο και τείνει να καθιερωθεί σε πληθώρα εφαρμογών. Σε εφαρμογές επιτήρησης περιοχής, παρέχει λύσεις αποτελεσματικότερης επιτήρησης και παρακολούθησης με μικρό οικονομικό κόστος και με την ελάχιστη και απομακρυσμένη ανθρώπινη επίβλεψη. Οι λύσεις αυτές, εξαιτίας των κενών ασφαλείας που παρουσιάζουν εν γένει τα δίκτυα WSN, πρέπει να προστατευθούν, έτσι ώστε η εφαρμογή να λειτουργεί το δυνατόν αποδοτικότερα. Για το σκοπό αυτό, έγινε εκτενής αναφορά μηχανισμών, οι οποίοι στοχεύουν προς αυτή τη κατεύθυνση και παρουσιάστηκε ένα σενάριο υλοποίησης ενός δικτύου της μορφής αυτής.

Αναφορές Βιβλιογραφίας

[1] Sohraby, K. , Minoli D. and Znati T. "Wireless Sensor Networks Technology , Protocols and Applications" Wiley 2007 , ISBN 978-0-471-74300-2

[2] Yick, J., Biswanath M. and Dipak G. "Wireless Sensor Network Survey" Computer Networks Journal (Elsevier) 52 (2008) 2292-2330

[3] Kumar S., "Wireless Sensor And Ad Hoc Networks Under Diversified Network Scenarios" , Artech House, 2012 ISBN: 978-1-60807-468-6

[4] Shimon Y. Nof and Wootae J. "Handbook Of Automation, Automation Design: Theory Elements and Methods", Chapter 20, Springer 2009 ISBN 978-3-540-78831-7

[5] Misra S., Woungang I. and Misra Sub., "Guide to Wireless Sensor Networks" Springer 2011 ISBN 978-1-84882-217-7

[6] "Clock Synchronization for Wireless Sensor Networks: A Survey" Ad Hoc Networks (Elsevier) Volume 3, Issue 3, May 2005, Pages 281–323

[7] Honghai Zhang and Jennifer C. Hou "Maintaining Sensing Coverage and Connectivity in Large Sensor Networks", Ad Hoc & Sensor Wireless Networks, Vol. 1, March 3 2005, pp. 89–124

[8] S. Kumar, Ten H. Lai and A. Arora "Barrier Coverage With Wireless Sensors" MobiCom 2005 ,Proceedings of the 11th annual international conference on Mobile computing and networking Pages 284-298

[9] Ai Chen , Ten H. Lai and Dong Xuan "Measuring and Guaranteeing Quality of Barrier-Coverage in Wireless Sensor Networks" ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), May 2008, pp. 421-430.

[10] James F. Kurose – Keith W. Ross: Δικτύωση Υπολογιστών, Εκδόσεις Γκιούρδας σελ. 679 – 756.

[11] Andrew S. Tanenbaum: Δίκτυα Υπολογιστών, Εκδόσεις Κλειδάριθμος, σελ. 827 – 952.

[12] Ahmad Abed Alhameed Alkhatib, Gurvinder Singh Baicher, Wireless Sensor Network Architecture, University of Wales Newport, City Campus, Usk Way, NP20 2BP, Newport, UK.

[13] F.L. Lewis, Wireless Sensor Networks, University of Texas at Arlington.

[14] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless Sensor Networks: a Survey, Broadband and Wireless Networking Laboratory, School

of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, USA.

[15] Khushboo Pawar, Y. Kelkar, A Survey of Hierarchical Routing Protocols in Wireless Sensor Network, International Journal of Engineering and Innovative Technology (IJEIT), Volume 1, Issue 5, May 2012.

[16] Changshun Chen, Design and Implementation of the Application Layer Communication Protocol Based on Wireless Sensor Network. College of Information Engineering, Yangzhou Polytechnic College, Yangzhou, China.

[17] Yogesh G. Iyer, Shashidhar Gandham, S. Venkatesan, STCP: A Generic Transport Layer Protocol for Wireless Sensor Networks, Telecommunications Engineering Program, Dept. of Computer Science University of Texas at Dallas.

[18] Yangfan Zhou and Michael R. Lyu, Jiangchuan Liu, Hui Wang, PORT: A Price-Oriented Reliable Transport Protocol for Wireless Sensor Networks, Department of Computer Science and Engineering, The Chinese University of Hong Kong, Hong Kong, China.

[19] Chieh-Yih Wan, Andrew T. Campbell, Lakshman Krishnamurthy, PSFQ: A Reliable Transport Protocol for Wireless Sensor Networks, Dept. of Electrical Engineering, Columbia University, New York.

[20] Seung-Jong Park, Ramanuja Vedantham, Raghupathy Sivakumar, Ian F. Akyildiz, GARUDA: Achieving Effective Reliability for Downstream Communication in Wireless Sensor Networks, IEEE Transactions on Mobile Computing, Volume 7, No2, Feb 2008.

[21] Vehbi C. Gungor, Ozgur B. Akan, DST: Delay Sensitive Transport in Wireless Sensor Networks, School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, Georgia, Department of Electrical and Electronics Engineering Middle East Technical University, Ankara, Turkey.

[22] Yogesh Sankarasubramaniam Özgür B. Akan Ian F. Akyildiz, ESRT: Event-to-Sink Reliable Transport in Wireless Sensor Networks, Broadband & Wireless Networking Laboratory, School of Electrical & Computer Engineering, Georgia Institute of Technology.

[23] Chieh-Yih Wan, Shane B. Eisenman, Andrew T. Campbell, CODA: Congestion Detection and Avoidance in Sensor Networks, Dept. of Electrical Engineering Columbia University, New York.

[24] Al-Sakib Khan Pathan, Hyung-Woo Lee, Security in Wireless Sensor Networks: Issues and Challenges Choong Seon Hong, Department of Computer Engg. Kyung Hee University, Korea.

[25] Jamal N. Al-Karaki Ahmed E. Kamal, Routing Techniques in Wireless Sensor Networks: A Survey, Dept. of Electrical and Computer Engineering, Iowa State University, Ames, Iowa.

[26] Rajashree.V.Biradar, V.C .Patil, Dr. S. R. Sawant, Dr. R. R. Mudholkar, Classification and Comparison of Routing Protocols in Wireless Sensor Networks, Department of Information Science and Engineering, Ballari Institute of Technology and Management.

[27] Ahmad Abed Alhameed Alkhatib, Gurvinder Singh Baicher, MAC Layer Overview for Wireless Sensor Networks University of Wales Newport, City Campus, Usk Way, Newport, U.K

[28] Ilker Demirkol, Cem Ersoy, and Fatih Alagöz, MAC Protocols for Wireless Sensor Networks: a Survey

[29] Lizhi Charlie Zhong, Jan Rabaey, Chunlong Guo, Rahul Shah, Data Link Layer Design for Wireless Sensor Networks, Berkeley Wireless Research Center, Department of EECS, University of California at Berkeley

[30] Jaein Jeong, Cheng-Tien Ee, Forward Error Correction in Sensor Networks, EECS Department, University of California, Berkeley, California, USA

[31] Bhaskar Bhuyan[1], Hiren Kumar Deva Sarma[1], Nityananda Sarma[2], Avijit Kar[3], Rajib Mall[4], Quality of Service (QoS) Provisions in Wireless Sensor Networks and Related Challenges, [1]Dept of IT, Sikkim Manipal Institute of Technology, Mazitar, Rangpo, INDIA, [2]Dept of Computer Science and Engineering, Tezpur University, Napaam, INDIA, [3]Dept of Computer Science and Engineering, Jadavpur University, Jadavpur, INDIA, [4]Dept of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, INDIA.

[32] Π.Γ. Κωττή, Π.Μ. Αράπογλου "Ασύρματες Επικοινωνίες" Κεφάλαιο 1, εκδόσεις Τζιόλα 2011, ISBN 978-960-418-268-8

[33] Howitt, I. Dept. of Electr. & Comput. Eng., North Carolina Univ., Charlotte, NC,USA Gutierrez, J.A."IEEE 802.15.4 Low Rate – Wireless Personal Area Network Coexistence Issues" Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE (Volume:3)

[34] Robert Faludi "Building Wireless Sensor Networks", Κεφάλαιο 7, O' Riley 2011 ISBN: 978-0-596-80773-3

[35] Holger Karl and Andreas Willig "Protocols and Architectures for Wireless Sensor Networks", Κεφάλαιο 5, Σελίδες 139-145, Wiley 2005 ISBN 978- 0-470-09510-2

[36] http://standards.ieee.org/getieee802/download/802.11-2012. pdf

[37] Sinem Coleri Ergen: ZigBee/IEEE 802.15.4 Summary

[38] Patrick Kinney: ZigBee Technology: Wireless Control that Simply Works, Kinney Consulting LLC Chair of IEEE 802.15.4 Task Group Secretary of ZigBee BoD Chair of ZigBee Building Automation Profile WG

[39] Shahin Farahani: ZigBee Wireless Networks and Tranceivers, Newnes, p. 1- 122

[40] Jongwon Yoon, Hyogon Kim and Jeong-Gil Ko: Data Fragmentation Scheme in IEEE 802.15.4, Wireless Sensor Networks Department of Computer Science and Engineering, Korea University

[41] Απόστολος Σπένδας: Ασύρματα Δίκτυα Αισθητήρων και Ζητήματα Ασφαλείας, Τμήμα Εφαρμοσμένης Πληροφορικής, Πανεπιστήμιο Μακεδονίας

[42] Yong Wang, Garhan Attebury, Byrav Ramamurthy: A Survey of Security Issues In Wireless Sensor Networks, University of Nebraska – Lincoln

[43] Jaydip Sen: A Survey on Wireless Sensor Network Security, Tata Consultancy Services Limited, Wireless & Multimedia Innovation Lab, Bengal Intelligent Park, Salt Lake Electronics Complex, Kolkata, India, p. 55-78

[44] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary: Wireless Sensor Network Security: A Survey, Department of Computer Science Wayne State University, Chapter 17.

[45] Huda Bader Hubboub: Denial of Service Attack in Wireless Sensor Networks, Islamic University – Gaza, Deanery of Higher Studies, Faculty of Engineering, Computer Engineering Department.

[46] Anthony D.Wood, John A. Stankovic, Denial of Service in Sensor Networks, University of Virginia, USA, p. 54 – 62

[47] Kalpana Sharma, M K Ghose: Wireless Sensor Networks: An Overview on its Security Threats, CSE Department, SMIT, Sikkim, India

[48] Ν. Αλεξανδρής, Β. Χρυσικόπουλος, Κ. Πατσάκης: Εισαγωγή στη θεωρία πληροφοριών, κωδίκων και κρυπτογραφίας, Εκδόσεις Βαρβαρίγου.

[49] Β.Α. Κάτος, Γ.Χ. Στεφανίδης: Τεχνικές κρυπτογραφίας και κρυπτανάλυσης, Εκδόσεις Ζυγός.

[50] Adrian Perrig, John Stankovic, David Wagner: Security in Wireless Sensor Networks, UC Berkeley Previously Published Works, Communications of the ACM, p. 53 – 57.

[51] Edith C. H. Ngai, Jiangchuan Liu, Michael R. Lyu1: On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks, Department of Computer Science and Engineering, The Chinese University of Hong Kong, School of Computer Science, Simon Fraser University, British Columbia, Canada, p.3383 – 3389.

[52] Min Jung Baek, Ki-Il Kim, SungHyun Cho : A Revised Mint-Route Protocol in Wireless Sensor Networks, Department of Informatics Gyeongsang National University, Jinju, Korea p. 258 – 259.

[53] John R. Douceur: The Sybil Attack, Microsoft Research

[54] Rouba El Kaissi, Ayman Kayssi, Ali Chehab, Zaher Dawy: DAWWSEN: A Defense Mechanism against Wormhole attack in Wireless Sensor Network, Proceedings of the Second International Conference on Innovations in Information Technology, Department of Electrical and Computer Engineering, American University of Beirut, Beirut, Lebanon (2005).

[55] Sencun Zhu, Sanjeev Setia, Sushil Jajodia: LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks, Center for Secure Information Systems, George Mason University

[56] Jing Deng, Richard, Han Shivakant Mishra: Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks, Computer Science Department, University of Colorado at Boulder, Boulder, Colorado, USA.

[57] Anthonis Papadimitriou, Fabrice Le Fessant, Aline Carneiro Viana, Cigdem Sengul: Cryptographic Protocols to Fight Sinkhole Attacks on Tree-based Routing in Wireless Sensor Networks

[58] Islam Hegazy, Reihaneh Safavi-Naini, Carey Williamson: Towards Securing MintRoute inWireless Sensor Networks, Department of Computer Science, University of Calgary, Calgary, AB, Canada.

[59] Ioannis Krontiris, Tassos Dimitriou, Thanassis Giannetsos, Marios Mpasoukos: Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks, Athens Information Technology p.150 -161

[60] Yih-Chun Hu, Adrian Perrig, David B. Johnson: Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks, Carnegie Mellon University.

[61] Brian Neil Levine,Clay Shields, N. Boris Margolin. A Survey of Solutions to the Sybil Attack

[62] Lingxuan Hu, David Evans: Secure Aggregation for Wireless Networks, Department of Computer Science, University of Virginia, Charlottesville, VA.

[63] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop by hop authentication scheme for filtering of injected false data in sensor networks", In Proceedings of IEEE Symposium on Security and Privacy, Oakland, CA, May 2004, pp. 259-271.

[64] P. Albers and O. Camp, "Security in ad hoc networks: A general intrusion detection architecture enhancing trust-based approaches", In Proceedings of the 1st International Workshop on Wireless Information Systems, 4th International Conference on Enterprise Information Systems, 2002.

[65] P. Brutch and C. Ko, "Challenges in intrusion detection for wireless ad-hoc networks", In Proceedings of the Symposium on Applications and the Internet Workshops (SAINT'03 Workshops) 2003.

[66] G. Wang, W. Zhang, C. Cao, and T.L. Porta, "On supporting distributed collaboration in sensor networks", In Proceedings of MILCOM, 2003.

[67] F. Ye et al., "Statistical En-Route Filtering of Injected False Datasensor Networks," Proc. IEEE INFOCOM, Hong Kong, 2004.

[68] Mohammad Sadeghi, Farshad Khosravi, Kayvan Atefi, Mehdi Barati: Security Analysis of Routing Protocols in Wireless Sensor Networks, Faculty of Computer and Mathematical Sciences, UiTM, Shah Alam, Malaysia, Faculty of Electrical Engineering, Islamic Azad University Eslam Abad Gharb, Iran.

[69] Chris Karlof, David Wagner: Secure routing in wireless sensor networks: attacks and countermeasures, University of California at Berkeley, Berkeley.

[70] William Stallings: Βασικές Αρχές Ασφαλείας Δικτύων, Εφαρμογές και Πρότυπα, Εκδόσεις Κλειδάριθμος.

[71] Κωνσταντίνος Λαμπρινουδάκης, Στέφανος Γκρίτζαλης, Λίλιαν Μήτρου, Σωκράτης Κάτσικας: Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών, Τεχνικά και Νομικά Θέματα, Εκδόσεις Παπασωτηρίου, σελ 241 – 244.

[72] Ms. Nimisha Chunilal Chaudhari: Key management in Wireless Sensor Network, A Survey, LDRP Institute of Technology and Research, Gandhinagar, Vol. 2, Issue 2, Feb 2013.

[73] Pratik P. Chaphekar: Survey of Key Distribution Schemes for Wireless Sensor Networks, Oklahoma State University.

[74] Tahira Laskar, Debasish Jena: A Survey on Key Management Issues in WSN, IJEIT, Vol. 1, Issue 5, May 2012.

[75] http://resources.infosecinstitute.com/wireless-attacks-unleashed

[76] Kalpana Sharma, M.K. Ghose: Cross Layer Security Framework for Wireless Sensor Networks, Department of CSE, SMIT, Sikkim, International Journal of Security and Its Applications, Vol. 5 No. 1, January, 2011.

[77] L. Eschenauer and V. D. Gligor: "A Key-Management Scheme for Distributed Sensor Networks," Electrical and Computer Engineering Department, University of Maryland, USA.

[78] Haowen Chan Adrian Perrig Dawn Song: Random Key Predistribution Schemes for Sensor Networks, Carnegie Mellon University.

[79] M. F. Younis, K. Ghumman, and M. Eltoweissy: Location- Aware Combinatorial Key Management Scheme for Clustered Sensor Networks, IEEE Trans. Parallel and Distrib. Sys, vol. 17, 2006, pp. 865–82.

[80] Celal Ozturk, Yanyong Zhang, Wade Trappe: Source-Location Privacy in Energy-Constrained Sensor Network Routing Wireless Information Network Laboratory (WINLAB) Rutgers University, p. 88 – 93, 2004.

[81] Pandurang Kamat, Yanyong Zhang, Wade Trappe, Celal Ozturk: Enhancing Source-Location Privacy in Sensor Network Routing Wireless Information Network Laboratory (WINLAB) Rutgers University.

[82] L. Zhang: A Self-adjusting Directed Random Walk Approach for Enhancing Source – Location Privacy in Sensor Network Routing, International Conference on Communications and Mobile computing, p. 33 – 38, 2006.

[83] Yong Xi, Loren Schwiebert, and Weisong Shi: Preserving Source Location Privacy in Monitoring-Based Wireless Sensor Networks, Wayne State University Department of Computer Science Detroit.

[84] Yi Yang, Min Shao, Sencun Zhu, Bhuvan Urgaonkar, Guohong Cao: Towards Event Source Unobservability with Minimum Network Traffic in Sensor

Networks, Department of Computer Science and Engineering The Pennsylvania State University, University Park.

[85] Pandurang Kamat, Wenyuan Xu, Wade Trappe, Yanyong Zhang: Temporal Privacy in Wireless Sensor Networks, Wireless Information Network Laboratory (WINLAB), Rutgers University.

[86] G. Myles, A. Friday, N. Davies: Preserving Privacy in Environments with Location – Based Applications, IEEE Pervasive Computing, vol.2, p. 56 – 64, 2003.

[87] U. Hengartner, P. Steenkiste: Access Control to People Location Information, ACM Transactions on Information Systems Security, vol. 8, p. 424 – 456, 2005.

[88] J. I. Hong, J. A. Landay: An Architecture for Privacy – Sensitive Ubiquitous Computing, 2nd International Conference on Mobile Systems, Applications and Services, p. 177 – 189, 2004.

[89] Cory Cornelius, Apu Kapadia, David Kotz, Dan Peebles, Minho Shin, Nikos Triandopoulos: AnonySense: Privacy – Aware People – Centric Sensing, Institute for Security Technology Studies, Dartmouth College, USA, Department of Computer Science University of Aarhus, Denmark.

[90] Alastair R. Beresford, Frank Stajano: Location Privacy in Pervasive Computing, University of Cambridge

[91] M. Gruteser, X. Liu: Protecting Privacy in Continuous Location Tracking Applications, IEEE Security & Privacy, vol.2, p. 28 – 34, 2004.

[92] Chi - Yin Chow, Mohamed F. Mokbel, Tian He: TinyCasper: A Privacy-Preserving Aggregate Location Monitoring System in Wireless Sensor Networks, Department of Computer Science and Engineering, University of Minnesota, Minneapolis, USA.

[93] Fernando Esponda: Negative Surveys, Yale University, Computer Science Department, New Haven, USA.

[94] Hani Alzaid, Ernest Foo, Juan Gonzalez Nieto: Secure Data Aggregation in Wireless Sensor Network: a survey, Information Security Institute, Qeensland University of Technology, Brisbane, Queensland.

[95] Joao Girao, Dirk Westhoff, Markus Schneider: CDA: Concealed Data Aggregation for Reverse Multicast Traffic in Wireless Sensor Networks, NEC Europe Ltd. Heidelberg, Germany.

[96] Hu L., Evans D.: Secure aggregation for wireless network, in 'SAINT Workshops', IEEE Computer Society, p. 384 – 394.

[97] Bartosz Przydatek, Dawn Song, Adrian Perrig: SIA: Secure Information Aggregation in Sensor Networks, Department of Electrical and Computer Engineering, Carnegie Mellon University, 2003.

[98] Chan H., Perrig A., Song D.: Secure hierarchical in – network aggregation in sensor networks, ACM Conference on Computer and Communications Security, ACM, 2006, p. 278 – 287.

[99] Du W., Deng J., Han Y.S., Varshney P.: A witness – based approach for data fusion assurance in wireless sensor networks, IEEE Global Communication Conference, 2003, vol.3, p. 1435 – 1439.

[100] A. Mahimkar, T. S. Rappaport, "SecureDAV: A Secure Data Aggregation and Verification Protocol for Sensor Networks", Proceedings of IEEE Global Telecommunications Conference, 2004, p. 2175 – 2179.

[101] H. Ozgur Sanli, Suat Ozdemir and Hasan C.: SRDA: Secure Reference-Based Data Aggregation Protocol for Wireless Sensor Networks, Department of Computer Science and Engineering Arizona State University.

[102] Yi Yang, Xinran Wang, Sencun Zhu, and Guohong Cao: SDAP: A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks, Department of Computer Science & Engineering The Pennsylvania State University.

[103] Jadia P., Mathuria A.: Efficient secure aggregation in sensor networks, in L. Boug'e & V. K. Prasanna, 'HiPC, 2004, vol. 3296 of Lecture Notes in Computer Science, Springer, p. 40 – 49.

[104] Ying Guo, Feng Hong, Zhongwen Guo, Zongke Jin, Yuan Feng: EDA: Event-oriented data aggregation in sensor networks, Dept. of Computer Science & Engineering, Ocean Univercity of China, Qingdao, China.

[105] Σκλιβάκης Εμμανουήλ: Πιστοποίηση ταυτότητας συσκευών σε ασύρματα περιβάλλοντα, Τμήμα Επικοινωνιακών και Πληροφοριακών Συστημάτων, Πανεπιστημίου Αιγαίου.

[106] M. Shaneck, K. Mahadevan, V. Kher, Y. Kim: Remote Software-based Attestation for Wireless Sensors Computer Science and Engineering University of Minnesota - Twin Cities.

[107] Taejoon Park, Student Member, IEEE, Kang G. Shin: Soft Tamper-Proofing via Program Integrity Verification in Wireless Sensor Networks, IEEE Transactions on Mobile Computing, 2003, vol. 4, No 3.

[108] Tal Garfinkel Ben Pfaff Jim Chow Mendel Rosenblum Dan Boneh: Terra: A Virtual Machine – based Platform for Trusted Computing, Computer Science Department, Stanford University.

[109] Arvind Seshadri, Adrian Perrig, Leendert van Doorn, Pradeep Khosla: SWATT: Software – based Attestation for embedded devices, in IEEE Symposium on Security and Privacy, 2004.

[110] P. S. Ramesh, F. Emily Manoz Priya, B. Santhi: Review on Security Protocols in Wireless Sensor Networks, Dept of Information Technology & Dept of Computer Science and Engineering, SASTRA University, Thanjavur, India, 2005.

[111] D. Boyle, T. Newe: Security Protocols for use with Wireless Sensor Networks, A Survey of Security Architectures, Department of Electronic and Computer Engineering, University of Limerick, Limerick, Ireland.

[112] Harald Vogt: Protocols for Secure Communication in Wireless Sensor Networks, Swiss Federal Institute of Technology Zurich, 2009.

[113] Jamal N. Al Karaki, Ahmed E. Kamal: Wireless Sensor Networks: A survey, The Hashemite University, Iowa State University, USA.

[114] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar: SPINS: Security Protocols for Sensor Networks, Department of Electrical Engineering and Computer Sciences, University of California, Berkeley.

[115] Anthony D. Wood, Lei Fang, Tian He, John Stankovic: Department of Computer Science, University of Virginia & Department of Computer Science and Engineering, University of Minnesota.

[116] Jing Deng, Richard Han, Shivakant Mishra: INSENS: Intrusion – Tolerant Routing in Wireless Sensor Networks, Department of Computer Science, University of Colorado.

[117] Evan Gaustad, Mark Luk, Bryan Parno, Adrian Perrig: Secure Sensor Network Routing: A Clean – Slate Approach, Carnegie Mellon University.

[118] T. He, S. Krishnamurthy, J. A. Stankovic, T. Abdelzaher, L. Luo, R. Stoleru, T. Yan, L. Gu, J. Hui and B. Krogh, *"An Energy-Efficient Surveillance System*

Using Wireless Sensor Networks," 2nd International Conference on Mobile Systems, Applications and Services, Boston, 6-9 June 2004.

[119] Z. Sun, et al., *"BorderSense: Border Patrol through Advanced Wireless Sensor Networks,"* Ad Hoc Networks, 2011, pp. 468-477.

[120] Z. Sun, I.F. Akyildiz, "Magnetic induction communications for wireless underground sensor networks" IEEE Transactions on Antenna and Propagation 58 (7) (2010) 2426–2435

[121] M.C. Vuran, I.F. Akyildiz, A.M. Al-Dhelaan *"Channel modeling and analysis for wireless underground sensor networks in soil medium"* Physical Communication Journal (Elsevier) (in press).

[122]Z. Sun, I.F. Akyildiz "*Connectivity in wireless underground sensor networks"* in: Proc. IEEE SECON '10, Boston, MA, USA, June 2010.

[123] I.F. Akyildiz, Z. Sun, M.C. Vuran *"Signal propagation techniques for wireless underground communication networks"* Physical Communication Journal (Elsevier) 2 (3) (2009) 167–183.

[124] http://www.tridsys.com/pdfs/ugsn-data-sheet.pdf

[125] I.F. Akyildiz, T. Melodia, K. Chowdhury *"Wireless multimedia sensor networks: applications and testbeds*" Proceedings of the IEEE 96 (10) (2008) 1588–1605 .

[126] Arora, P. Dutta, S. Bapat, V. Kulathumani, H. Zhang, V. Naik, V. Mittal, H. Cao, M. Demirbas1, M. Gouda, Y. Choi2, T. Herman3, S. Kulkarni, U. Arumugam4, M. Nesterenko, A. Vora, and M. Miyashita5 : *A Line in the Sand: A Wireless Sensor Network for Target Detection, Classification, and Tracking*, 1 Department of Computer Science and Engineering, 2 Department of Computer Sciences, The University of Texas at Austin, 3 Department of Computer Science, University of Iowa, 4 Department of Computer Science and Engineering, Michigan State University, 5 Department of Computer Science, Kent State University.

[127] Peter Rothenpieler, Daniela Krueger, Dennis Pfisterer, Stefan Fischer, Denise Dudek, Christian Haas, Martina Zitterbart: *FleGSens – Secure Area Monitoring Using Wireless Sensor Networks*, Institute of Telematics University of Luebeck, Institute of Telematics University of Karlsruhe, Germany.

[128] http://www.cs.berkeley.edu/~prabal/projects/xsm/

[129] Emad Felemban: Advanced Border Intrusion Detection and Surveillance Using Wireless Sensor Network Technology, Computer Engineering Department, College of Computing and Information Systems, Makkah, KSA, Int. J. Communications, Network and System Sciences, 2013, 6, 251-259, May 2013.

[130] Karlof, C., Sastry, N., and Wagner, D. Tinysec: a link layer security architecture for wireless sensor networks. Inn: SenSys '04: Proceedings of the 2nd international conference on Embedded Networked Sensor Systems, volume 1008, pages 162–175, ACM, New York, USA, 2004.

[131] Mark, L., Ghita, M., Adrian, P., and Virgil, G.: MiniSec: a secure sensor network communication architecture. In IPSN '07: Proceedings of the 6th international conference on Information processing in sensor networks, pages 479–488, NewYork, NY, USA, 2007. ACM.

[132] Li, T., Wu, H., Wang, X., and Bao, F. SenSec Design, I2R Sensor Network Flagship Project. Technical report, Infocomm Security Department, Institute for InfoComm Research, Singapore, 2005.

[133] Mauri Kuorilehto, Mikko Kohvakka, Jukka Suhonen, Panu Haemaelaeinen, Marko Haemaelaeinen, Timo D. Haemaelaeinen: Ultra – Low Energy Wireless Sensor Networks in Practice, Theory, Realization and Deployment, Tampere University of Technology, Finland, p. 125 – 142.