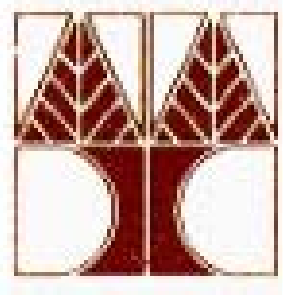
Ατομική Διπλωματική Εργασία

CLASSIFICATION AND ANALYSIS OF SECURE ROUTING PROTOCOLS IN SENSOR NETWORKS

Έλλη Δημητρίου

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ



ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Ιούνιος 2008

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Classification and Analysis of Secure Routing Protocols in Sensor Networks

Έλλη Δημητρίου

Επιβλέπων Καθηγητής

Αντρέας Πιτσιλλίδης

Η Ατομική αυτή Διπλωματική Εργασία υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων απόκτησης του πτυχίου Πληροφορικής του Τμήματος Πληροφορικής του Πανεπιστημίου Κύπρου

Ιούνιος 2008

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ. Αντρέα Πιτσιλλίδη για την υποστήριξη που μου πρόσφερε κατά την διάρκεια της υλοποίησης αυτής της εργασίας αλλά και για την επίτευξη μιας άψογης συνεργασίας.

Επίσης τον καθηγητή του Τμήματος Ηλεκτρολόγων Μηχανικών και Μηχανικών Ηλεκτρονικών Υπολογιστών, Δρ. Γιώργο Χ"Χριστοφή για την πολύτιμη βοήθεια που μου πρόσφερε κατά την διάρκεια της ανάλυσης των πρωτοκόλλων που μελέτησα και την καθοδήγησή του για την επιτυχημένη ολοκλήρωση της εργασίας αυτής.

Περίληψη

Τα ασύρματα δίκτυα αισθητήρων είναι μια νέα τεχνολογία η οποία αρχίζει να μπαίνει στις ζωές μας και αποτελεί πόλο έλξης για περαιτέρω έρευνα. Η ανάπτυξη που υπάρχει στον τομέα αυτό και οι ποικίλοι τρόποι χρήσης των δικτύων αυτών απαιτούν τη μελέτη και εύρεση νέων τρόπων και μηχανισμών για βελτίωση της λειτουργίας τους, εξασφάλιση αξιοπιστίας και ασφάλειας.

Τα δίκτυα αισθητήρων διαφέρουν από τα κοινά ασύρματα δίκτυα λόγω των διαφορετικών χαρακτηριστικών των κόμβων που αποτελούν το κάθε δίκτυο. Οι κόμβοι που μπορούν να συμμετέχουν σε ένα ασύρματο δίκτυο έχουν διάφορα μεγέθη – ατομικός φορητός υπολογιστής, σχετικά μεγάλο αποθηκευτικό χώρο και υπολογιστική ικανότητα καθώς και ανανεώσιμα ποσά ενέργειας. Αντίθετα, οι αισθητήρες είναι πολύ μικρές συσκευές οι οποίες έχουν περιορισμένο αποθηκευτικό χώρο, περιορισμένη υπολογιστική ικανότητα και περιορισμένα ποσά ενέργειας τα οποία στις πλείστες περιπτώσεις είναι μη ανανεώσιμα. Οι περιορισμοί αυτοί κάνουν αδύνατη την χρήση υφιστάμενων μεθόδων για βελτίωση των υπηρεσιών ενός τέτοιου δικτύου.

Στο άρθρο αυτό θα παρουσιάσουμε αρχικά την γενική θεωρία πίσω από τα δίκτυα αισθητήρων και τις διάφορες μεθόδους που χρησιμοποιούνται για ασφάλεια καθώς και τις πιο δημοφιλείς επιθέσεις που μπορούν να εφαρμοστούν σε ένα δίκτυο. Ακολούθως θα γίνει μια εκτενής ανάλυση της μεθοδολογίας που ακολουθήθηκε για την κατανόηση και αντιμετώπιση του προβλήματος της ασφάλειας στα δίκτυα αισθητήρων. Στη μεθοδολογία συμπεριλαμβάνεται η ανάλυση επτά πρωτοκόλλων και οι τρόποι αντιμετώπισης των επιθέσεων από διάφορα πρωτόκολλα. Τέλος, θα παρουσιάσουμε τα συμπεράσματα που θα διεξαχθούν μέσα από την έρευνα αυτή.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

1.1 Ορισμός του Προβλήματος

Τα τελευταία χρόνια έχει ανθήσει η έρευνα γύρω από τα ασύρματα δίκτυα αισθητήρων. Η τεχνολογία αυτή εισχωρεί στην καθημερινότητά μας κι έτσι το ερευνητικό ενδιαφέρων για το πεδίο αυτό γίνεται όλο και πιο έντονο. Μέχρι στιγμής έχουν μελετηθεί αρκετές πτυχές των ερωτημάτων και των αναγκών που περικλείονται στα δίκτυα αισθητήρων – για παράδειγμα η ανάγκη για αυτοοργάνωση των αισθητήρων και τρόποι που μπορεί να πραγματοποιηθεί, η ανάγκη για ένα ειδικό λειτουργικό σύστημα το οποίο θα λαμβάνει υπόψη τα ειδικά χαρακτηριστικά των αισθητήρων. Ένα εξίσου σημαντικό ερευνητικό πεδίο αποτελεί και η ανάγκη για ύπαρξη ασφάλειας.

Η χρήση των δικτύων αισθητήρων για μέτρηση και μετάδοση σημαντικών, απόρρητων και ευαίσθητων πληροφοριών, όπως η θερμοκρασία σε ένα εργοστάσιο παραγωγής εκρηκτικών και πληροφορίες για την κατάσταση ενός ασθενή, επιβάλλει την ανάπτυξη πρωτοκόλλων που εγγυώνται την ασφαλή μεταφορά των δεδομένων και την ομαλή λειτουργία του δικτύου παρά τις παρεμβολές που μπορεί να δεχτεί πιθανώς από κακόβουλους κόμβους. Η ασφάλεια σε ένα δίκτυο μπορεί να επιτευχθεί χρησιμοποιώντας πρωτόκολλα που μπορούν να εφαρμοστούν σε οποιοδήποτε protocol layer, στο Application Layer,

Transport Layer, Network Layer, Link Layer και Physical Layer. Κάθε ένα απ' αυτά έχει τα πλεονεκτήματα και τα μειονεκτήματά του.

1.2 Σκοπός της Μελέτης

Στην εργασία αυτή θα ασχοληθούμε με τα πρωτόκολλα που αναπτύχθηκαν για το Network Layer. Στο επίπεδο δρομολόγησης μπορούν να εφαρμοστούν ποικίλες επιθέσεις από κακόβουλους κόμβους. Κάθε ένα από τα προτεινόμενα πρωτόκολλα ακολουθεί ένα διαφορετικό τρόπο οργάνωσης του δικτύου και τρόπου προώθησης των πακέτων. Ακόμα και πρωτόκολλα που έχουν σαν βάση μια κοινή ιδέα παρουσιάζουν αρκετές διαφοροποιήσεις – για παράδειγμα μπορεί δύο πρωτόκολλα να απαιτούν την οργάνωση των αισθητήρων σε ομάδες αλλά ο τρόπος αποστολής των μηνυμάτων να είναι διαφορετικός. Οι παράγοντες που συντελούν ένα πρωτόκολλο επηρεάζουν και τον αριθμό και το είδος των επιθέσεων που μπορούν να εφαρμοστούν.

Στόχος λοιπόν αυτής της ατομικής διπλωματικής εργασίας είναι η μελέτη και αξιολόγηση των μεθοδολογιών που έχουν αναπτυχθεί από διάφορα πρωτόκολλα για την αντιμετώπιση συγκεκριμένων επιθέσεων στο επίπεδο δρομολόγησης.

1.3 Σημασία της Μελέτης

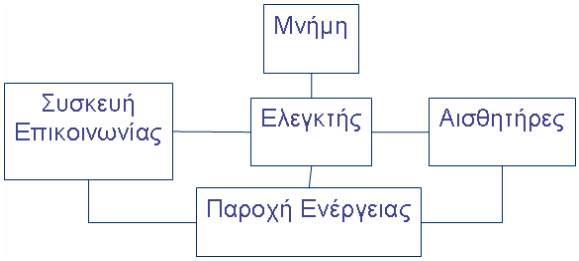
Η μαζεμένη γνώση των τρόπων που αναπτύχθηκαν μέχρι στιγμής για την αντιμετώπιση των διαφόρων επιθέσεων μπορεί να φανεί χρήσιμη σε πολλές περιπτώσεις. Χρήσιμη θα την βρουν άτομα που θέλουν να αξιολογήσουν τις μεθόδους αυτές και να επιλέξουν τις καταλληλότερες για να τις εφαρμόσουν σε ένα νέο πρωτόκολλο ή να τις συνδυάσουν για αναβάθμιση ενός υπάρχοντος.

Κεφάλαιο 2

Θεωρία

2.1 Οι Αισθητήρες Σήμερα

Ο αισθητήρας ορίζεται ως μια υπολογιστική μηχανή περιορισμένου μεγέθους που έχει την ικανότητα να μετρά δεδομένα από το περιβάλλον – για παράδειγμα τη θερμοκρασία, την κίνηση, την υγρασία – και να τα επεξεργάζεται [1]. Το μέγεθός τους κυμαίνεται από μερικά εκατοστά μέχρι και το μεγέθους ενός κόκκου σκόνης. Ο αισθητήρας αποτελείται από τον ελεγκτή ο οποίος είναι υπεύθυνος για τη γενική λειτουργία του αισθητήρα, μια συσκευή ασύρματης επικοινωνίας με τους άλλους αισθητήρες, την μνήμη για να αποθηκεύει δεδομένα και προγράμματα που είναι απαραίτητα για τη λειτουργία του, τους αισθητήρες οι οποίοι του δίνουν τη δυνατότητα να μετρά δεδομένα από το περιβάλλον και μια πηγή ενέργειας μέσω της οποίας θα του παρέχεται η απαιτούμενη ισχύ ώστε να λειτουργεί. Στο Σχήμα 2.1 παρατηρούμε το τρόπο με τον οποίο συνδέονται τα μέρη ενός αισθητήρα μεταξύ τους.



Σχήμα 2.1 Τα μέρη ενός αισθητήρα

Οι πιο διαδεδομένοι ελεγκτές που χρησιμοποιούνται για την κατασκευή αισθητήρων είναι της Texas Instruments και της Atmel οι οποίοι λειτουργούν σε ταχύτητες μέχρι και 4 MHz. Η τεχνολογία που χρησιμοποιείται για την κατασκευή της μνήμης των αισθητήρων είναι συνήθως FLASH.

Το πιο διαδεδομένο μέσο επικοινωνίας που χρησιμοποιείται για την επικοινωνία μεταξύ των αισθητήρων είναι το ηλεκτρομαγνητικό πεδίο σε ραδιοσυχνότητες. Ένας αισθητήρας μπορεί να βρεθεί σε τέσσερις πιθανές καταστάσεις, την λήψη δεδομένων (receive mode), τη μετάδοση δεδομένων (transmission mode), την κατάσταση μη απασχόλησης (idle mode) και την κατάσταση ύπνου (sleep mode). Η ακτίνα στην οποία έχει εμβέλεια ένας αισθητήρας για να μεταδώσει δεδομένα κυμαίνεται από μερικές δεκάδες μέχρι και μερικές εκατοντάδες μέτρα.

Νευραλγικής σημασίας για τη λειτουργία ενός αισθητήρα αποτελεί η παροχή ενέργειας η οποία συνήθως προσφέρεται σε αυτούς μέσω αλκαλικών μπαταριών ή μπαταριών λιθίου. Με στόχο τη μεγιστοποίηση του χρόνου ζωής ενός αισθητήρα η ενέργεια που καταναλώνεται πρέπει να είναι η ελάχιστη δυνατή. Οι κατασκευάστριες εταιρείες υποστηρίζουν ότι οι αισθητήρες που κατασκευάζουν έχουν μέχρι και τρία χρόνια ζωής – ο αισθητήρας εκτελεί τις βασικές του λειτουργίες: συλλέγει πληροφορίες από το περιβάλλον και τις αποστέλλει στους άλλους κόμβους. Πρακτικά όμως ο χρόνος ζωής τους φτάνει μέχρι και τους έξι μήνες λόγω των μεγάλων διαρροών ενέργειας προς το περιβάλλον και των επιπρόσθετων ποσών ενέργειας που καταναλώνονται με την προσθήκη λειτουργιών στον αισθητήρα.

Το λειτουργικό σύστημα που θα εγκατασταθεί σε μια τέτοια συσκευή πρέπει να έχει μικρό μέγεθος κώδικα ενώ ταυτόχρονα πρέπει να διασφαλίζει πρόσβαση στους πόρους της συσκευής με εύχρηστο και αποδοτικό τρόπο, ενώ παράλληλα να προστατεύει τους πόρους αυτούς από ταυτόχρονη πρόσβαση (πρόβλημα ταυτοχρονίας). Το TinyOS είναι το λειτουργικό σύστημα που είναι σήμερα πιο διαδεδομένο και εγκαθιστάται στους περισσότερους αισθητήρες.

Οι αισθητήρες χρησιμοποιούνται σε ποικίλες εφαρμογές όπως οι στρατιωτικές για σκοπούς παρακολούθησης των συνθηκών που επικρατούν στο πεδίο της μάχης. Χρησιμοποιούνται επίσης για έλεγχο και παρακολούθηση συγκεκριμένων περιβαλλόντων και φυσικών βιοτόπων, για τον έλεγχο της κυκλοφορίας αλλά και σε κάποιες περιπτώσεις σε ανίχνευση σεισμών και ακραίων καιρικών φαινομένων.

2.2 Δίκτυα Αισθητήρων

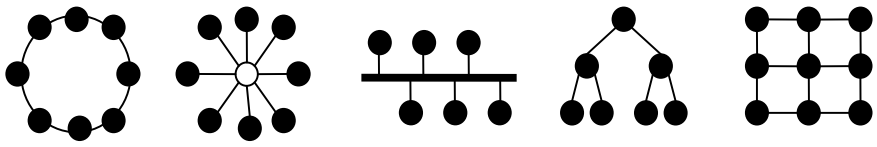
Τα ασύρματα δίκτυα αισθητήρων είναι συλλογές από μικρές αυτόνομες υπολογιστικές συσκευές, οι οποίες είναι κατανεμημένες στο χώρο και εργάζονται σαν ομάδα για να συλλέξουν δεδομένα από το περιβάλλον στο οποίο έχουν τοποθετηθεί [2]. Αφού συλλέξουν κάποια δεδομένα, στόχος τους είναι να τα προωθήσουν μέσω του ασύρματου δικτύου ούτως ώστε να είναι διαθέσιμα για περαιτέρω επεξεργασία και ανάλυση.

Λόγω του χαμηλού τους κόστους, μπορεί να χρησιμοποιηθεί ένας μεγάλος αριθμός από αισθητήρες σε μια περιοχή με αποτέλεσμα το ασύρματο δίκτυο να είναι ανθεκτικό σε πιθανές απώλειες αισθητήρων. Οι απώλειες μπορεί να είναι είτε λόγω εξασθένησης των ενεργειακών πόρων των αισθητήρων είτε λόγω υιοθέτησης μη πρέπουσας συμπεριφοράς στο δίκτυο – μη προώθηση πακέτων ή αλλοίωσή τους.

Τα δίκτυα αισθητήρων χαρακτηρίζονται από μερικά ιδιαίτερα χαρακτηριστικά τα οποία τα διαφοροποιούν από τα κοινά ασύρματα δίκτυα. Οι κόμβοι που μπορούν να συμμετέχουν σε ένα ασύρματο δίκτυο έχουν διάφορα μεγέθη, σχετικά μεγάλο αποθηκευτικό χώρο και υπολογιστική ικανότητα καθώς και ανανεώσιμα ποσά ενέργειας. Αντίθετα, οι αισθητήρες είναι πολύ μικρές συσκευές οι οποίες έχουν περιορισμένο αποθηκευτικό χώρο, περιορισμένη υπολογιστική ικανότητα και περιορισμένα ποσά ενέργειας τα οποία στις πλείστες περιπτώσεις είναι μη ανανεώσιμα. Οι περιορισμοί αυτοί κάνουν αδύνατη την χρήση υφιστάμενων μεθόδων για βελτίωση των υπηρεσιών ενός τέτοιου δικτύου.

Επιπρόσθετα, τοποθετούνται σε σκληρές περιβαλλοντικές συνθήκες, χαρακτηρίζονται από δυναμικές δικτυακές τοπολογίες, παρουσιάζουν φαινόμενα κινητικότητας των κόμβων (node mobility), αποτυχίας λειτουργίας των αισθητήρων (node failure) καθώς και λάθη στην μετάδοση των δεδομένων λόγω των ανωμαλιών του γύρω περιβάλλοντος. Τα δίκτυα αυτά λειτουργούν χωρίς την παρουσία κάποιου επόπτη-συντονιστή.

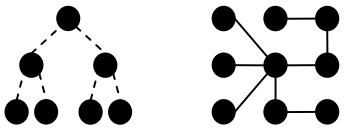
Οι τοπολογίες που συναντούμε στα δίκτυα αισθητήρων χωρίζονται σε fixed και adhoc. Οι σταθερές δικτυακές τοπολογίες, Σχήμα 2.2 – fixed network topologies – έχουν χρησιμοποιηθεί για δικτύωση προσωπικών ηλεκτρονικών υπολογιστών και αποτέλεσαν την αρχή για τη δημιουργία του διαδίκτυο. Οι τοπολογίες αυτές χρησιμοποιούνται τόσο σε ασύρματα όσο και σε ενσύρματα δίκτυα αισθητήρων.



Σχήμα 2.2 Fixed Network Topologies

Δεδομένου ότι τα δίκτυα αισθητήρων μπορούν να αναπτυχθούν και σε εχθρικά ή απάτητα περιβάλλοντα όπου δεν είναι δυνατή η σύνδεσή τους με καλώδια, οι σταθερές δικτυακές τοπολογίες δεν μπορούν να χρησιμοποιηθούν. Οι πιο

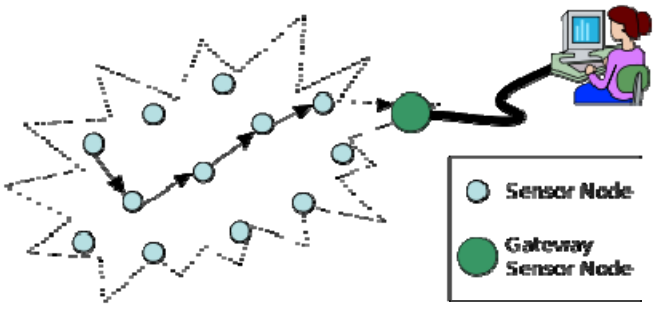
διαδεδομένες ασύρματες δικτυακές τοπολογίες φαίνονται στην ακόλουθη εικόνα, Σχήμα 2.3.



Σχήμα 2.3 Adhoc Network Topologies

Πολλά πρωτόκολλα και αλγόριθμοι έχουν αναπτυχθεί για τη λειτουργία και την επικοινωνία των αισθητήρων μεταξύ τους, ενώ πολλές τεχνολογίες και πλατφόρμες έχουν σχεδιαστεί για έλεγχο και δοκιμή των δικτύων αυτών. Οι αλγόριθμοι αυτοί στοχεύουν κυρίως στην μείωση της κατανάλωσης ενέργειας κατά την χρήση των αισθητήρων, στην αποδοτική και αξιόπιστη δρομολόγηση των πακέτων στο δίκτυο αισθητήρων καθώς και στην ευρωστία και αυτονομία του δικτύου αυτού.

Στις πλείστες των ρεαλιστικών εφαρμογών τα δεδομένα που συλλέγονται από το ασύρματο δίκτυο αισθητήρων αποθηκεύονται σε κάποιο κεντρικό σταθμό βάσης – base station ή sink, Σχήμα 2.4. Ο σταθμός αυτός είναι υπολογιστική μηχανή μεγαλύτερης ισχύος με ικανότητες επεξεργασίας και αποθήκευσης μεγάλης ποσότητας δεδομένων και επικοινωνεί με τον έξω κόσμο. Λειτουργεί σαν σύνδεσμος μεταξύ του δικτύου αισθητήρων και του υπόλοιπου δικτύου.



Σχήμα 2.4 Τυπικό Ασύρματο Δίκτυο Αισθητήρων

2.3 Ασφάλεια και Δικτυακή Επικοινωνία

Η ύπαρξη ασφάλειας σε κάθε μορφής δικτύου, ασύρματου ή ενσύρματου, είναι καίριας σημασίας μιας και μπορεί να μεταφέρουν προσωπικά ή απόρρητα δεδομένα που δεν πρέπει να γίνουν κατανοητά από τρίτα άτομα. Παράλληλα είναι σημαντικό να είμαστε σίγουροι πως δεν υπήρξε οποιαδήποτε παρέμβαση ή αλλοίωση στο πακέτο που παραλάβαμε και για την αυθεντικότητα της ταυτότητα του αποστολέα. Οι προϋποθέσεις αυτές είναι αναγκαίες για την ύπαρξη ασφαλούς επικοινωνίας [3]. Στη συνέχεια δίνονται οι αντίστοιχοι αγγλικοί όροι μαζί με μια σύντομη επεξήγηση.

Data Confidentiality: Το περιεχόμενο ενός πακέτου πρέπει να είναι κατανοητό μόνο από τον αποστολέα και τον παραλήπτη του. Για να το πετύχουμε αυτό, το πακέτο πρέπει να κρυπτογραφηθεί με τέτοιο τρόπο ώστε μόνο ο αποστολέας και ο παραλήπτης να μπορούν να το αποκρυπτογραφήσουν. Αναπτύχθηκαν διάφοροι μέθοδοι κρυπτογράφησης οι οποίοι θα αναλυθούν στην επόμενη ενότητα. Οι πιο γνωστοί απ' αυτούς είναι η μέθοδος κρυπτογράφησης με συμμετρικό κλειδί μεταξύ αποστολέα και παραλήπτη και η μέθοδος κρυπτογράφησης με δημόσιο κλειδί.

Authentication: Οι κόμβοι που συμμετέχουν σε μια επικοινωνία πρέπει να μπορούν να επιβεβαιώσουν τις ταυτότητες των κόμβων με τους οποίους επικοινωνούν ανταλλάζοντας πακέτα. Ο παραλήπτης ενός πακέτου πρέπει να μπορεί να επιβεβαιώσει πως τα δεδομένα που έπιασε τα έστειλε ο αναμενόμενος αποστολέας και όχι κάποιος άλλος.

Data Integrity: Ο παραλήπτης ενός πακέτου πρέπει να είναι σίγουρος πως τα δεδομένα που παρέλαβε δεν είναι αλλοιωμένα, δεν τροποποιήθηκαν από κάποιο τρίτο άτομο. Σε περίπτωση που κάποιο πακέτο είναι αλλοιωμένο πρέπει να μπορεί να το αναγνωρίσει και να το απορρίψει. Ταυτόχρονα τόσο ο παραλήπτης

ενός πακέτου όσο και ο αποστολέας του δεσμεύονται και δεν μπορούν να αρνηθούν τη συμμετοχή τους στην ανταλλαγή ενός συγκεκριμένου πακέτου.

Non Repudiation: Ο παραλήπτης ενός πακέτου πρέπει να είναι σε θέση να ”αποδείξει” σε ένα τρίτο κόμβο πως το πακέτο που πήρε πράγματι στάλθηκε από τον αναμενόμενο αποστολέα. Επίσης ο αποστολέας ενός μηνύματος δεν μπορεί να αρνηθεί πως έστειλε ένα πακέτο.

Availability: Οι υπηρεσίες και οι πληροφορίες που προσφέρονται μέσω του δικτύου πρέπει να είναι διαθέσιμες οποιαδήποτε στιγμή. Λόγω των διαφορετικών και ιδιαίτερων χαρακτηριστικών μερικών δικτύων η διαθεσιμότητά τους δεν είναι ικανοποιητική. Για παράδειγμα τα δίκτυα αισθητήρων υστερούν στον τομέα αυτό επειδή η ενέργεια που έχουν είναι περιορισμένη κι έτσι όταν αυτή τελειώσει και ο κόμβος “πεθάνει”. Διάφορες επιθέσεις που εφαρμόζονται σε δίκτυα αισθητήρων στοχεύουν στη μείωση της ενέργειας των κόμβων του δικτύου για να το παραλύσουν.

Access Control: Μη εξουσιοδοτημένοι κόμβοι δεν πρέπει να έχουν πρόσβαση στο δίκτυο πόσο μάλλον συμμετοχή στις διαδικασίες που εκτελούνται σε αυτό. Οι νόμιμοι, εξουσιοδοτημένοι κόμβοι πρέπει να είναι σε θέση να ανιχνεύουν τα πακέτα που στέλνονται από μη εξουσιοδοτημένους κόμβους και να τα απορρίπτουν.

2.4 Κρυπτογραφία

Η κρυπτογραφία χρησιμοποιείται από τα αρχαία χρόνια για κωδικοποίηση μηνυμάτων τα οποία δεν ήθελαν να γίνουν κατανοητά από άτομα μη εξουσιοδοτημένα. Ως απτό παράδειγμα έχουμε τον αλγόριθμο κρυπτογράφησης που επινόησε ο Ιούλιος Καίσαρας για να κωδικοποιεί τα μηνύματα που θα έστελνε στους επιτελείς του χωρίς να είναι δυνατόν να τα διαβάσουν οι εχθροί

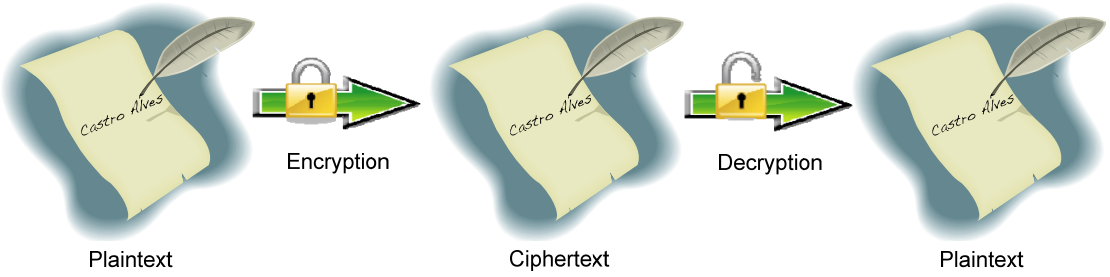
του. Ο αλγόριθμος βασιζόταν στην αντικατάσταση κάθε γράμματος του αλφαβήτου με κάποιο άλλο, ολίσθηση των γραμμάτων προς τα δεξιά, χρησιμοποιώντας κάποιο κλειδί. Για να το αποκρυπτογραφήσει κάποιος θα πρέπει να αντιστρέψει τη διαδικασία κρυπτογράφησης, να αντικαταστήσει το κάθε γράμμα χρησιμοποιώντας μια ολίσθηση προς τα αριστερά, ανάλογα με το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση του μηνύματος.

Η κρυπτογραφία γνώρισε μεγάλη ανάπτυξη λόγω της ραγδαίας ανάπτυξης των υπολογιστών και των τηλεπικοινωνιών. Έτσι και η μέθοδος της κρυπτογραφίας εξελίχθηκε και αναβαθμίστηκε. Αναπτύχθηκαν διάφορες τεχνικές κωδικοποίησης μηνυμάτων, οι πλείστες από τις οποίες απαιτούν μεγάλη υπολογιστική ικανότητα, με στόχο την ύπαρξη ασφάλειας στη μεταφορά και αποθήκευση δεδομένων και σημαντικών πληροφοριών.

2.4.1 Βασικές Έννοιες Κρυπτογράφησης

Η κρυπτογραφία είναι μια επιστήμη που βασίζεται στα μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων. Οι μέθοδοι κρυπτογράφησης καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι κι έτσι εξασφαλίζουν το απόρρητο στις ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών.

Το αρχικό μήνυμα ονομάζεται απλό κείμενο – plaintext, ενώ το μήνυμα που προκύπτει από την κρυπτογράφηση του απλού κειμένου ονομάζεται κρυπτογράφημα – ciphertext [4]. Στο Σχήμα 2.5 φαίνεται η διαδικασία κρυπτογράφησης και αποκρυπτογράφησης ενός κειμένου.



Σχήμα 2.5 Κρυπτογράφηση Απλού Κειμένου

Ο αλγόριθμος που χρησιμοποιείται για την αποκρυπτογράφηση του απλού κείμενου είναι αντίστροφος του αλγορίθμου που χρησιμοποιήθηκε για την κρυπτογράφηση του απλού κειμένου. Η κρυπτογραφημένη επικοινωνία είναι αποτελεσματική, όταν μόνο τα άτομα που συμμετέχουν σε αυτή μπορούν να ανακτήσουν το περιεχόμενο του αρχικού μηνύματος.

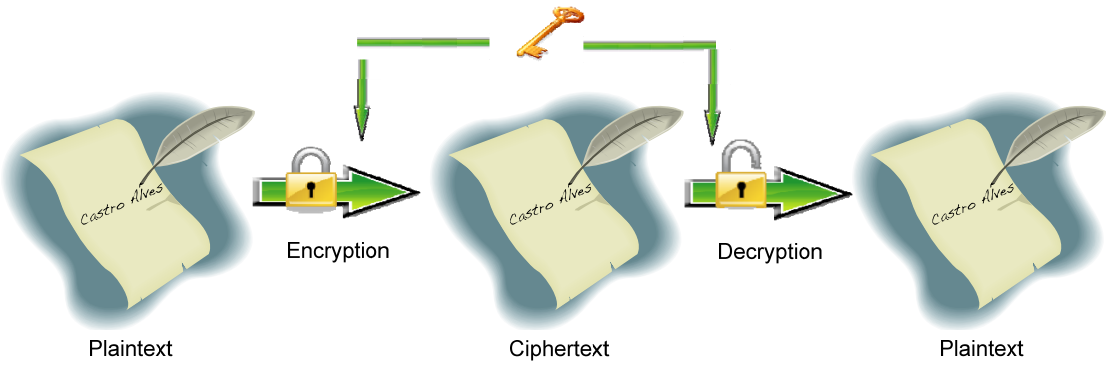
Ο αλγόριθμος κρυπτογράφησης είναι μια μαθηματική συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών. Αυξάνοντας τον βαθμό πολυπλοκότητας του αλγορίθμου κρυπτογράφησης μειώνεται η πιθανότητα να τον σπάσει κάποιος. Ο αλγόριθμος κρυπτογράφησης λειτουργεί σε συνδυασμό με ένα κλειδί (key), για την κρυπτογράφηση του απλού κειμένου. Το ίδιο απλό κείμενο κωδικοποιείται σε διαφορετικά κρυπτογραφήματα όταν χρησιμοποιούνται διαφορετικά κλειδιά.

2.4.2 Μέθοδοι Κρυπτογράφησης

Οι κύριοι μέθοδοι κρυπτογράφησης που χρησιμοποιούνται σήμερα είναι η κρυπτογράφηση με συμμετρικό κλειδί – symmetric key, η κρυπτογράφηση με δημόσιο κλειδί – public key [5], και η κρυπτογράφηση με τη χρήση hash function. Κάθε μια από αυτές έχει τα δικά την πλεονεκτήματα και μειονεκτήματα και σαφώς διαφορετικές απαιτήσεις σε θέματα μνήμης και υπολογιστικής δύναμης. Ανάλογα με τα χαρακτηριστικά των κόμβων ενός δικτύου θα επιλεγεί και η κατάλληλη μέθοδος.

2.4.2.1 Συμμετρικό Κλειδί – Symmetric Key

Η κρυπτογράφηση με συμμετρικό κλειδί είναι μια μέθοδος κρυπτογράφησης μηνυμάτων κατά την οποία ο αποστολέας και ο δέκτης ενός μηνύματος μοιράζονται ένα ενιαίο, κοινό κλειδί. Ο αποστολέας χρησιμοποιεί το κλειδί αυτό για να κρυπτογραφήσει το μήνυμα που θα στείλει και ο δέκτης το χρησιμοποιεί για να το αποκρυπτογραφήσει. Η διαδικασία αυτή αναπαριστάται στο Σχήμα 2.6. Επομένως, το κλειδί αυτό πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και, άρα, απαιτείται ασφαλές μέσο για τη μετάδοσή του, για παράδειγμα μία προσωπική συνάντηση κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται. Αν κάτι τέτοιο δεν είναι εφικτό, η συμμετρική κρυπτογραφία είναι αναποτελεσματική, αφού κάποιο μη εξουσιοδοτημένο άτομο μπορεί να υποκλέψει το κλειδί και να παρακολουθεί ή να επεμβαίνει στην επικοινωνία των εξουσιοδοτημένων κόμβων.



Σχήμα 2.6 Symmetric Key Cryptography

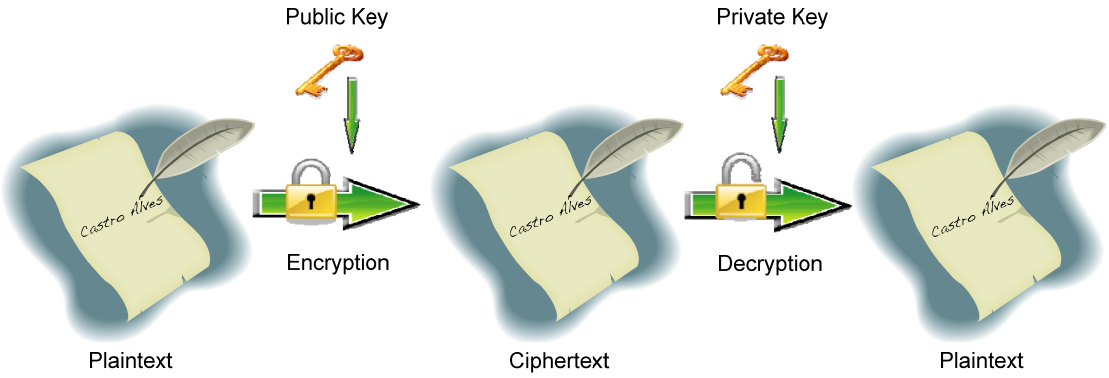
Το πρόβλημα που παρουσιάζει αυτή η τεχνική είναι η διανομή των κλειδιών, η εξασφάλιση δηλαδή ότι τα κλειδιά που αποστέλλονται στους παραλήπτες που θα τα χρησιμοποιήσουν δεν θα πέσουν σε λάθος χέρια. Κατά αυτόν τον τρόπο τα συστήματα συμμετρικής κρυπτογραφίας προϋποθέτουν την ύπαρξη ενός ασφαλούς καναλιού για την ανταλλαγή των μυστικών κλειδιών.

Επιπρόσθετα, όσο ο αριθμός των χρηστών αυτού του συστήματος ασφαλείας μεγαλώνει, μεγαλώνουν και τα προβλήματα της δημιουργίας, της διανομής, της

ασφάλειας αλλά και της καταγραφής και αντιστοιχίας των μυστικών κλειδιών. Άρα τα σχήματα αυτά δεν είναι εύκολο να επεκταθούν για την εξυπηρέτηση μεγάλων πληθυσμών και απαιτούν επίσης πρόσθετες διαδικασίες ασφάλειας, όπως την αποθήκευση των κλειδιών σε ένα κεντρικό ασφαλή εξυπηρετητή.

2.4.2.2 Δημόσιο Κλειδί – Public Key

Στην ασύμμετρη κρυπτογραφία, κρυπτογραφία με τη χρήση δημόσιου κλειδιού, ο κάθε κόμβος παίρνει ένα ζευγάρι κλειδιών [6], το δημόσιο – public, και το ιδιωτικό – private. Ο αποστολέας ενός μηνύματος πρέπει να γνωρίζει το δημόσιο κλειδί του παραλήπτη και να κρυπτογραφήσει το μήνυμα με αυτό [7]. Ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί, το οποίο γνωρίζει μόνο αυτός. Αναλυτικότερα, ένα μήνυμα ή και ένα αρχείο που έχει κρυπτογραφηθεί με το δημόσιο κλειδί ενός κατόχου, μπορεί να αποκρυπτογραφηθεί μόνο με το αντίστοιχο ιδιωτικό κλειδί του ίδιου κατόχου, πράγμα που σημαίνει ότι μόνο ο κάτοχος ενός δημόσιου κλειδιού μπορεί να διαβάσει τα μηνύματα που έχουν κρυπτογραφηθεί με το κλειδί αυτό, καθώς μόνο αυτός γνωρίζει το αντίστοιχο ιδιωτικό κλειδί, Σχήμα 2.7.



Σχήμα 2.7 Public Key Cryptography

Με την ύπαρξη δύο κλειδιών, ενός για την κρυπτογράφηση του μηνύματος και ενός άλλου για την αποκρυπτογράφηση του μηνύματος, δεν είναι αναγκαία η ανταλλαγή μυστικών κλειδιών μεταξύ των κόμβων που θα επικοινωνήσουν. Το

δημόσιο και ιδιωτικό κλειδί παράγονται έτσι ώστε ένα μήνυμα κρυπτογραφημένο με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί και αντίστροφα.

Συμπερασματικά, το δημόσιο κλειδί δεν αποτελεί μυστική πληροφορία κι έτσι μπορεί να μεταδοθεί χωρίς την απαίτηση ύπαρξης ασφαλούς μέσου. Το ιδιωτικό κλειδί χρησιμοποιείται μόνο από τον ιδιοκτήτη του και δε μεταδίδεται ποτέ. Όταν ένα μήνυμα έχει κρυπτογραφηθεί με το δημόσιο κλειδί κάποιου χρήστη, μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό του κλειδί. Και επειδή μόνο ο ίδιος ο χρήστης γνωρίζει το ιδιωτικό του κλειδί, μόνο αυτός μπορεί να αποκρυπτογραφήσει τα μηνύματα που απευθύνονται σε αυτόν. Ούτε καν το δημόσιο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση δεν μπορεί να αποκρυπτογραφήσει το μήνυμα, κι έτσι η γνώση του δημόσιου κλειδιού από τρίτους δεν αποτελεί πρόβλημα.

2.4.2.3 Διαφορές Συμμετρικής και Ασύμμετρης Κρυπτογράφησης

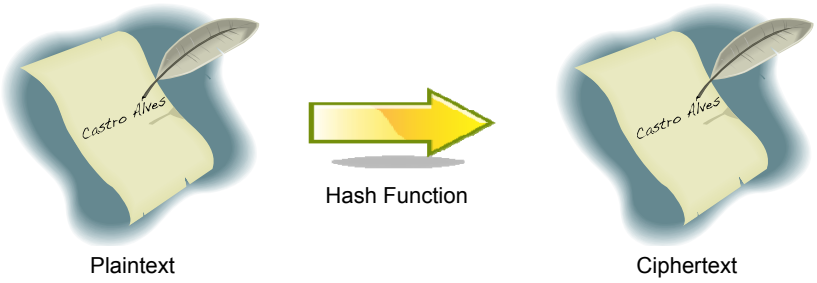
Μια φανερή διαφορά μεταξύ συμμετρικής και ασύμμετρης κρυπτογράφησης αποτελεί ο αριθμός των κλειδιών που απαιτούνται σε κάθε περίπτωση. Στην πρώτη χρειάζεται ένα κλειδί ενώ στη δεύτερη χρειάζονται δύο κλειδιά. Η ασύμμετρη κρυπτογραφία προσφέρει μεγαλύτερη ασφάλεια από τη συμμετρική, αφού όπως αναφέρθηκε δεν είναι απαραίτητη η ανταλλαγή ενός κοινού μυστικού κλειδιού μεταξύ αποστολέα και παραλήπτη. Έχει όμως το μειονέκτημα ότι οι αλγόριθμοι ασύμμετρης κρυπτογράφησης είναι πολύ πιο αργοί από τους αλγόριθμους συμμετρικής κρυπτογράφησης και απαιτούνται περισσότερες πράξεις.

Στα σύγχρονα κρυπτογραφικά συστήματα χρησιμοποιούνται και οι δύο προαναφερόμενες τεχνικές με στόχο την μέγιστη αποδοτικότητα και λειτουργικότητα του τελικού συστήματος, αφού θα εκμεταλλεύεται τις αρετές και

οι δύο μεθόδων κρυπτογράφησης. Όταν θα αρχίσει μια νέα επικοινωνία, χρησιμοποιείται ο αλγόριθμος ασύμμετρης κρυπτογράφησης για να διανεμηθούν τα συμμετρικά κλειδιά με ασφάλεια και κατά τη διάρκεια της επικοινωνίας τα μηνύματα κρυπτογραφούνται με το συμμετρικό κλειδί.

2.4.2.4 Hash Function

Η τρίτη μέθοδος κρυπτογράφησης Hash Function είναι γνωστή και σαν Message Digests και One-Way Encryption επειδή δεν είναι εύκολο από το αποτέλεσμα του κρυπτογραφημένου μηνύματος να πάρουμε το αρχικό κείμενο [8]. Σε αντίθεση με τις δύο προαναφερόμενες μεθόδους κρυπτογράφησης, δημόσιο κλειδί και συμμετρικό κλειδί, η μέθοδος αυτή δεν χρησιμοποιεί κάποιο κλειδί. Κρυπτογραφεί κάποιο απλό κείμενο οποιουδήποτε μεγέθους εφαρμόζοντας σε αυτό ένα μαθηματικό μετασχηματισμό και προκύπτει το κρυπτογραφημένο μήνυμα το οποίο έχει σταθερό μέγεθος, hash value, Σχήμα 2.8. Το κρυπτογράφημα θεωρείται ως μια σύντομη και περιεκτική αναπαράσταση του απλού κειμένου από το οποίο παράχθηκε. Το κρυπτογράφημα συνοδεύει το μήνυμα από το οποίο παράχθηκε και χρησιμοποιείται για επιβεβαίωση της αυθεντικότητας του μηνύματος που συνοδεύει και την μη αλλοίωσή του κατά τη μεταφορά του.



Σχήμα 2.8 Hash Function

2.5 Ασφάλεια και Ασύρματα Δίκτυα Αισθητήρων

Η χρήση των δικτύων αισθητήρων για μέτρηση και μετάδοση σημαντικών, απόρρητων και ευαίσθητων πληροφοριών, όπως η θερμοκρασία σε ένα εργοστάσιο παραγωγής εκρηκτικών και πληροφορίες για την κατάσταση ενός ασθενή, επιβάλλει την ανάπτυξη πρωτοκόλλων που εγγυώνται την ασφαλή μεταφορά των δεδομένων και την ομαλή λειτουργία του δικτύου παρά τις παρεμβολές που μπορεί να δεχτεί πιθανώς από κακόβουλους κόμβους.

Λόγω των ιδιαιτεροτήτων των δικτύων αισθητήρων δεν μπορούν να χρησιμοποιηθούν τα ήδη υπάρχοντα πρωτόκολλα ασφάλειας που αναπτύχθηκαν για πιο ισχυρά τερματικά. Τα συστήματα αυτά έχουν μεγάλες απαιτήσεις σε πόρους όπως μνήμη για δεδομένα, τον κώδικα, τους αλγορίθμους και τις πληροφορίες που πρέπει να αποθηκεύουν, μεγάλη υπολογιστική ικανότητα και μεγάλα ποσά διαθέσιμης ενέργεια. Στα δίκτυα αισθητήρων υπάρχει περιορισμός στους σημαντικούς αυτούς πόρους έτσι ο αλγόριθμος που θα αναπτυχθεί με στόχο την ασφάλεια στα δίκτυα αισθητήρων πρέπει να έχει κάποια ιδιαίτερα χαρακτηριστικά.

- Περιορισμένη μνήμη και αποθηκευτικός χώρος: Ο αισθητήρας είναι μια μικρή συσκευή με μικρό ποσό μνήμης και αποθηκευτικού χώρου. Έτσι, για να φτιάξουμε ένα ικανοποιητικό αλγόριθμο για ασφάλεια σε τέτοια δίκτυα, θα πρέπει να περιορίσουμε το μέγεθος του κώδικα και τον όγκο δεδομένων που θα αποθηκεύει.
- Περιορισμένα ποσά ενέργειας: Δεν είναι καθόλου εύκολο και πρακτικό να ανανεώνεις τις πηγές ενέργειας των αισθητήρων όταν τελειώσουν. Το πιο πρακτικό είναι η εξοικονόμηση της ενέργειάς τους. Ο αλγόριθμος που θα αναπτυχθεί για να κρυπτογραφεί τα μηνύματα, το κόστος για την αποστολή, αποθήκευση και επεξεργασία των πακέτων αυτών πρέπει να αναπτυχθούν με τέτοιο τρόπο ώστε να είναι λειτουργικά.
- Περιορισμένη υπολογιστική ικανότητα: Οι αισθητήρες για να έχουν μικρό κόστος και να έχουν μεγαλύτερη διάρκεια ζωής χρησιμοποιούνται

επεξεργαστές με μικρή υπολογιστική δύναμη. Έτσι δεν είναι αποτελεσματικοί για τους ήδη υπάρχοντες αλγόριθμους οι οποίοι απαιτούν αρκετές πράξεις με περίπλοκες μαθηματικές εξισώσεις και αλγορίθμους.

Η ασφάλεια σε ένα δίκτυο μπορεί να επιτευχθεί χρησιμοποιώντας πρωτόκολλα που μπορούν να εφαρμοστούν σε οποιοδήποτε protocol layer, στο Application Layer, Transport Layer, Network Layer, Link Layer και Physical Layer [9] ή σε συνδυασμό των layers. Σ' αυτή την ατομική διπλωματική εργασία θα μελετηθεί η ασφάλεια στο Network Layer και πιο συγκεκριμένα η ασφάλεια κατά τη δρομολόγηση των πακέτων.

2.6 Attacks σε Αισθητήρες

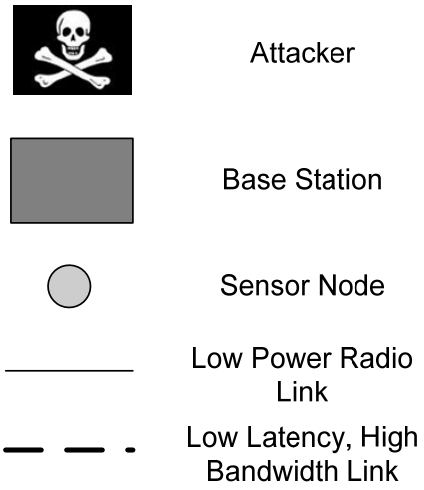
Η ασφάλεια στα δίκτυα εκτός από την προστασία της επικοινωνίας μεταξύ των κόμβων συμπεριλαμβάνει και την αντιμετώπιση διάφορων επιθέσεων που μπορεί να δεχτεί το δίκτυο, την αντιμετώπιση και εξουδετέρωσή τους.

Σε κάθε μορφής δικτύου, ενσύρματου και ασύρματου, μπορούν να εφαρμοστούν διάφορες επιθέσεις από εχθρικούς και κακόβουλους κόμβους με αποτέλεσμα να αμφιταλαντεύεται η ασφάλεια του δικτύου. Οι επιθέσεις αυτές μπορούν να κατηγοριοποιηθούν σε δύο ομάδες, τις απαθείς επιθέσεις – passive attacks – και τις ενεργείς επιθέσεις – active attacks [10]. Στις απαθείς επιθέσεις εμπίπτουν οι επιθέσεις κατά τις οποίες ο attacker απλά παρακολουθεί το δίκτυο, μαζεύει πληροφορίες από τα πακέτα που στέλνονται αλλά δεν τα αλλοιώνει και δεν επιδρά στο δίκτυο και τη λειτουργικότητά του. Αντίθετα, κατά τις ενεργείς επιθέσεις ο attacker αλλοιώνει τα μηνύματα που στέλνονται, απαντά σε παλιά μηνύματα ή δεν προωθεί τα μηνύματα που παίρνει και γενικότερα παρεμβαίνει στις λειτουργίες του δικτύου.

2.6.1 Attacks σε Επίπεδο Δρομολόγησης στα Δίκτυα Αισθητήρων

Τα ασύρματα δίκτυα σε σχέση με τα ενσύρματα δίκτυα είναι πιο τρωτά στις διάφορες δικτυακές επιθέσεις λόγω του μέσου μετάδοσης των πληροφοριών. Επιπρόσθετα, πολλά πρωτόκολλα δρομολόγησης που αναπτύχθηκαν για τα δίκτυα αισθητήρων είναι αρκετά απλά και δεν προστατεύουν τον αισθητήρα από τις εξωτερικές και εσωτερικές επιθέσεις.

Οι κύριες επιθέσεις περιγράφονται στις επόμενες υποενότητες [11]. Μερικές απ' αυτές επεξηγούνται και με γραφικό παράδειγμα το οποίο είναι βασισμένο στο υπόμνημα που φαίνεται στο Σχήμα 2.9.



Σχήμα 2.9 Υπόμνημα

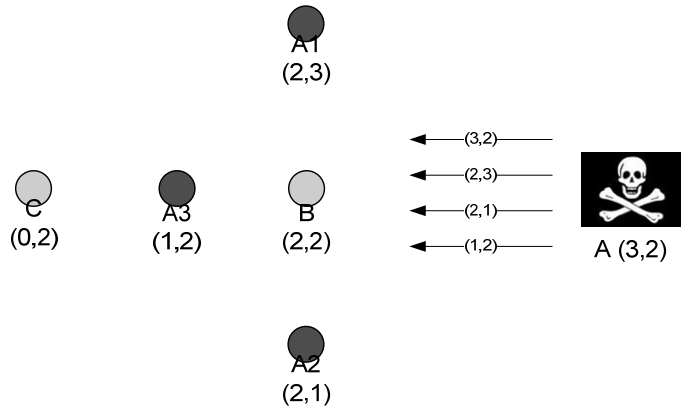
2.6.1.1 Spoofed, altered, or replayed routing information

Η αμεσότερη επίθεση ενάντια σε ένα πρωτόκολλο δρομολόγησης είναι να ελέγχονται οι πληροφορίες που ανταλλάσσονται μεταξύ των κόμβων. Με τον τρόπο αυτό οι εχθρικοί κόμβοι μπορούν να είναι σε θέση να δημιουργήσουν τους βρόχους δρομολόγησης, να προσελκύσουν ή να αποκρούουν την κυκλοφορία του δικτύου, να επεκτείνουν ή να μικρύνουν τις διαδρομές δρομολόγησης και να

παραγάγουν τα ψεύτικα μηνύματα λάθους. Με την εισαγωγή κακόβουλων πληροφοριών ή την αλλαγή των νόμιμων μηνυμάτων οργάνωσης δρομολόγησης, ένας attacker μπορεί να αποτρέψει το πρωτόκολλο δρομολόγησης από το να λειτουργήσει σωστά. Παραδείγματος χάριν, ένας επιτιθέμενος κόμβος μπορεί να πείσει τους νόμιμους κόμβους να προωθούν τα πακέτα από την πιο μακρινή διαδρομή.

2.6.1.2 Sybil Attack

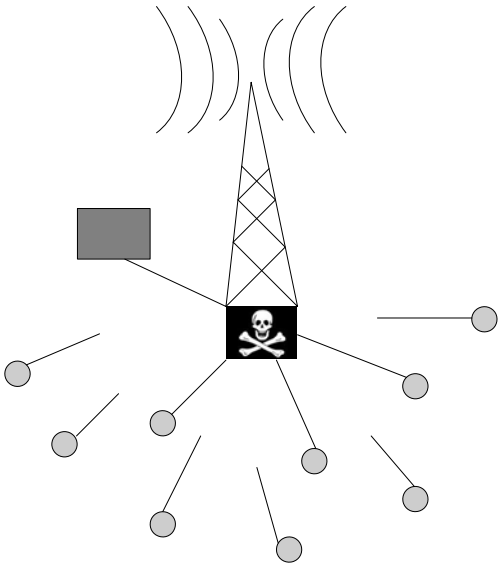
Κατά το Sybil attack, ο attacker παρουσιάζεται στους άλλους κόμβους του δικτύου με πολλές ταυτότητες και σε διαφορετική τοποθεσία. Για παράδειγμα ο attacker A στο Σχήμα 2.10 που βρίσκεται στην τοποθεσία (3,2) παρουσιάζει τον εαυτό του στον κόμβο B που βρίσκεται στην θέση (2,2) και σε άλλες διαφορετικές τοποθεσίες, στην (2,3) ως A1, στην (2,1) ως A2 και στην (1,2) ως A3. Η επίθεση αυτή αποτελεί πρόβλημα για πρωτόκολλα δρομολόγησης που βασίζονται στη γεωγραφική θέση των κόμβων, αφού θα λαμβάνουν υπόψη για τη δρομολόγηση των πακέτων κόμβους που στην ουσία δεν υπάρχουν.



Σχήμα 2.10 Sybil Attack

2.6.1.3 Hello Attack

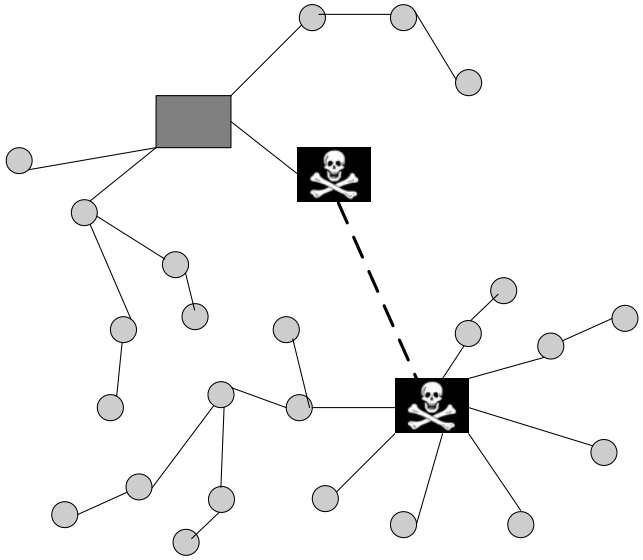
Αρκετά πρωτόκολλα που αναπτύχθηκαν για δίκτυα αισθητήρων απαιτούν από τους κόμβους να στείλουν hello message για να αναγγελθούν στους γείτονές τους, Σχήμα 2.11. Οι κόμβοι που θα λάβουν το hello message θεωρούν πως ο αποστολέας είναι στην ακτίνα εμβέλειας τους και τον καταχωρούν στη λίστα με τους γείτονές τους. Έτσι όταν ο κόμβος θα θελήσει να επικοινωνήσει με τους γείτονές του, θα στέλνει μηνύματα και στον attacker στέλνοντάς τα ουσιαστικά σε ένα κόμβο ο οποίος ίσως να μην το πάρει επειδή πολύ πιθανό να μην είναι στην ακτίνα εμβέλειάς του. Με τον τρόπο αυτό όμως μειώνεται η διάρκεια ζωής του κόμβου επειδή στέλνει επιπλέον μηνύματα προς τον εχθρικό κόμβο. Ένας attacker στέλνοντας συνέχεια hello messages δεσμεύει χώρο από το bandwidth του δικτύου και επιπλέον χρησιμοποιεί μέρος από τους buffers των αισθητήρων οι οποίοι είναι μικροί και είναι σημαντικό να είναι ελεύθεροι για να αποθηκεύουν τα πακέτα που θα λαμβάνουν από τους άλλους κόμβους του δικτύου.



Σχήμα 2.11 Hello Attack

2.6.1.4 Wormhole Attack

Στην επίθεση wormhole, δύο απομακρυσμένοι attackers δημιουργούν ένα δικό τους αποκλειστικό κανάλι επικοινωνίας μέσω του οποίου μεταφέρουν διάφορα δεδομένα και πληροφορίες που παίρνουν από τους άλλους κόμβους, Σχήμα 2.12. Η απλούστερη μορφή αυτής της επίθεσης είναι η τοποθέτηση ενός attacker μεταξύ δύο κόμβων με στόχο να διαβιβάζει τα πακέτα που στέλνουν. Το κανάλι αυτό μπορεί να κεντρίσει το ενδιαφέρον των άλλων κόμβων και να στέλνουν τα πακέτα τους μέσω αυτού, έχοντας την εντύπωση ότι τα πακέτα μεταφέρονται πολύ γρήγορα στον προορισμό τους. Με την επίθεση αυτή, δύο απομακρυσμένοι κόμβοι ίσως θεωρήσουν πως είναι γείτονες μέσω των δύο απομακρυσμένων attackers.



Σχήμα 2.12 Wormhole Attack

2.6.1.5 Selective Forwarding Attack

Η επίθεση αυτή επηρεάζει τα πρωτόκολλα δρομολόγησης που βασίζονται στην υπόθεση ότι οι συμμετέχοντες κόμβοι προωθούν τα πακέτα που παίρνουν. Κατά το Selective Forwarding Attack ο attacker δεν προωθεί τα πακέτα ή προωθεί

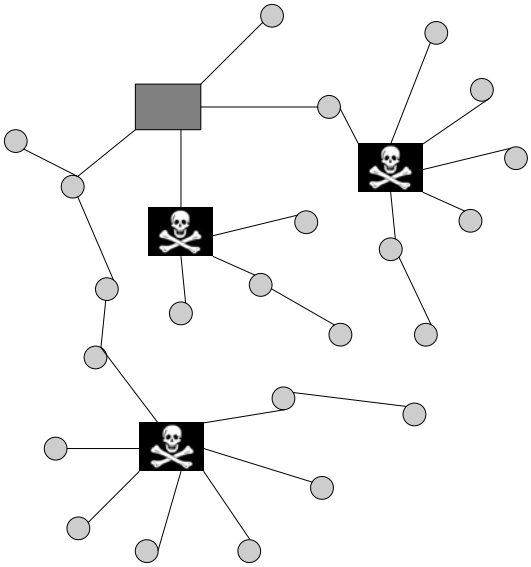
μερικά από τα πακέτα που παίρνει επηρεάζοντας έτσι την δρομολόγηση των πακέτων και την απόδοση του δικτύου. Αν ο attacker απορρίπτει όλα τα πακέτα που παίρνει διατρέχει τον κίνδυνο οι γειτονικοί κόμβοι να επιλέξουν κάποιο άλλο μονοπάτι για δρομολόγηση των πακέτων, στο οποίο πολύ πιθανός να μην συμπεριλαμβάνεται. Έτσι λοιπόν είναι πιο ασφαλής η τακτική διαβίβασης μερικών πακέτων.

2.6.1.6 Black Hole Attack

Ο attacker κατά την επίθεση αυτή διαφημίζει μια σύντομη απόσταση μεταξύ όλων των προορισμών και έτσι προσελκύει την κυκλοφορία μέσω αυτού. Με τον τρόπο αυτό μπορεί να έχει πρόσβαση στα πακέτα που δρομολογούνται. Κατά την επίθεση αυτή ο εχθρικός κόμβος δεν προωθεί τα πακέτα που παίρνει στους άλλους κόμβους κι έτσι δημιουργεί μια μαύρη τρύπα στο δίκτυο.

2.6.1.7 Sinkhole Attack

Ο εχθρικός κόμβος, όπως και στο black hole attack, παρουσιάζει τον εαυτό του με πολλά προτερήματα, όπως υψηλή ποιότητα δρομολόγησης και μεγάλα ποσά ενέργειας, με στόχο να δελεάσει τους άλλους κόμβους του δικτύου και να τον χρησιμοποιούν για τη μεταφορά των πακέτων, Σχήμα 2.13. Η διαφορά του από το black hole attack είναι ότι ο εχθρικός κόμβος προωθεί όποια πακέτα επιθυμεί, δεν τα απορρίπτει όλα εξορισμού, και έχει την επιλογή να τα αλλοιώσει. Η επίθεση αυτή μοιάζει και με την επίθεση selective forward. Η διαφορά μεταξύ των δύο είναι ότι στο selective forward ο attacker δεν προσπαθεί να ελκύσει την κυκλοφορία του δικτύου μέσω αυτού, η επίθεση περιορίζεται στα πακέτα που θα πάρει από τους άλλους κόμβους χωρίς να γίνει κάποια προσπάθεια για παραλαβή κάποιων πακέτων. Αντίθετα στο sinkhole attack ο attacker προσπαθεί να τραβήξει την κυκλοφορία του δικτύου μέσω αυτού κι έτσι να έχει πρόσβαση σε περισσότερα πακέτα.



Σχήμα 2.13 Sinkhole Attack

Κεφάλαιο 3

Περιγραφή Προβλήματος

3.1 Αναλυτική Περιγραφή Προβλήματος

Αφού παρουσιάστηκε αναλυτικά η γενική θεωρία γύρω από τα δίκτυα αισθητήρων, οι ιδιαιτερότητες τους, οι βασικές αρχές ασφάλειας σε ένα δίκτυο, οι κύριες μέθοδοι κρυπτογράφησης και οι διάφορες επιθέσεις που πιθανό να δεχτούν οι κόμβοι σε ένα δίκτυο μπορούμε να συνεχίσουμε με μια αναλυτική περιγραφή του προβλήματος και ακολούθως την μεθοδολογία που θα ακολουθηθεί για τη λύση του.

Για την ύπαρξη ασφάλειας σε ασύρματα δίκτυα αισθητήρων αναπτύχθηκαν αρκετά πρωτόκολλα τα οποία ακολουθώντας τη δική τους μεθοδολογία προσφέρουν προστασία τόσο στους κόμβους του δικτύου όσο και στα δεδομένα που μεταφέρονται σε αυτό. Στη μελέτη αυτή θα ασχοληθούμε με τα πρωτόκολλα που αναπτύχθηκαν για το Network Layer. Το κάθε πρωτόκολλο έχει κάποια χαρακτηριστικά τα οποία σχετίζονται με τη λειτουργικότητά του, functionality, και την ασφάλεια που προσφέρει.

Στόχος αυτής της διπλωματικής εργασίας είναι η μελέτη των διαφορετικών μεθοδολογιών που χρησιμοποιήθηκαν στα διάφορα πρωτόκολλα δρομολόγησης για την αντιμετώπιση των πιο δημοφιλή επιθέσεων που μπορούν να

εφαρμοστούν σε ένα δίκτυο, λαμβάνοντας φυσικά υπόψη τα ιδιαίτερα χαρακτηριστικά του κάθε πρωτοκόλλου.

3.2 Μεθοδολογία Λύσης Προβλήματος

Για να αναλύσουμε το τρόπο αντιμετώπισης διάφορων επιθέσεων από κάθε πρωτόκολλο είναι σημαντικό να καταλάβουμε πως λειτουργεί το πρωτόκολλο, να μελετήσουμε τις προϋποθέσεις κάτω από τις οποίες λειτουργεί, τις μεθόδους που χρησιμοποιεί για να προσφέρει ασφάλεια και τη λειτουργικότητά του. Για να είναι δυνατή και εύκολη η σύγκριση των διάφορων μεθοδολογιών που χρησιμοποιήθηκαν σε διάφορα πρωτόκολλα θα πρέπει να αναλυθούν όλα τα πρωτόκολλα με βάση κάποια χαρακτηριστικά.

Η ανάλυση των πρωτοκόλλων μπορεί να γίνει λαμβάνοντας υπόψη διάφορες παραμέτρους. Για τις ανάγκες της μελέτης αυτής δημιουργήθηκε ένας πίνακας με στοιχεία τα οποία χαρακτηρίζουν ένα πρωτόκολλο και πρέπει να ληφθούν υπόψη για την κατανόηση του τρόπου αντιμετώπισης διάφορων επιθέσεων καθώς και των αδυναμιών τους. Οι κατηγορίες που χρησιμοποιήθηκαν είναι οι ακόλουθες:

- Environmental Assumptions
- Security
- Functionality Provided
- Performance.

3.2.1 Environmental Assumptions

Το κάθε πρωτόκολλο αναπτύσσεται με βάση κάποιες προϋποθέσεις σχετικά με το περιβάλλον στο οποίο μπορεί να λειτουργήσει. Τα χαρακτηριστικά του περιβάλλοντος μπορούν να ομαδοποιηθούν σε πέντε κατηγορίες

1. Network Assumptions
2. Node Characteristics
3. Architecture for routing protocol

4. Security assumptions
5. Applicability relevant to the environment.

3.2.1.1 Network Assumptions

Στην ομάδα αυτή περιλαμβάνονται χαρακτηριστικά που σχετίζονται με τη δομή του δικτύου, τη δυναμικότητα των κόμβων, το τρόπο που επικοινωνούν οι κόμβοι μεταξύ τους καθώς και τα χαρακτηριστικά της επικοινωνίας που εγκαθιδρύουν, αν είναι reliable ή unreliable και τέλος τη μορφή του ίδιου του συστήματος, αν είναι “ανοιχτό” και να δέχεται νέους κόμβους ή αν είναι “κλειστό” και δεν μπορούν να προστεθούν νέοι κόμβοι. Η πιο διαδεδομένη δομή των δικτύων αισθητήρων είναι η οργάνωση σε clusters, δηλαδή οργανώνονται ιεραρχικά και σε ομάδες. Μέσα σε μια ομάδα από κόμβους ορίζεται ένας κόμβος ως ο cluster head. Αρμοδιότητά του είναι η επικοινωνία της ομάδας του με το υπόλοιπο δίκτυο. Με λίγα λόγια, αναλαμβάνει την αποστολή μηνυμάτων από τους κόμβους του cluster του στο υπόλοιπο δίκτυο και αντίστροφα. Τους μεταφέρει δηλαδή μηνύματα τα οποία προέρχονται από άλλους κόμβους που δεν ανήκουν στο ίδιο cluster.

3.2.1.2 Node Characteristics

Στην αγορά υπάρχουν αισθητήρες με διαφορετικά χαρακτηριστικά όπως διαφορετική υπολογιστική ικανότητα και χρήση διαφορετικού μέσου επικοινωνίας. Τα πρωτόκολλα που θα αναπτυχθούν γενικά για αισθητήρες δεν πρέπει να επηρεάζονται από τα χαρακτηριστικά αυτά.

3.2.1.3 Architecture for routing protocol

Το κάθε πρωτόκολλο ακολουθεί τη δική του φιλοσοφία για τον τρόπο δρομολόγησης των πακέτων του. Τα πακέτα μπορεί να δρομολογούνται με βάση

την τοποθεσία των κόμβων στο δίκτυο – location based, ή με βάση το ποσοστό εμπιστοσύνης που έχει ο κάθε κόμβος, πόσο έμπιστος είναι ένας κόμβος – trust based.

3.2.1.4 Security Assumptions

Αρκετά πρωτόκολλα για να υλοποιήσουν την ασφάλεια στο δίκτυο στο οποίο θα εφαρμοστούν προϋποθέτουν την ύπαρξη έμπιστων κόμβων, για παράδειγμα το base station ή κάποιους κόμβους στο δίκτυο. Επίσης, χρησιμοποιείται ένα σύνολο από κλειδιά ούτως ώστε να είναι δυνατή η κωδικοποίηση των πακέτων. Τα κλειδιά είτε αποθηκεύονται στους αισθητήρες πριν την εισαγωγή τους σε ένα δίκτυο – pre-deployment, είτε καθορίζονται δυναμικά – dynamic deployment. Παράλληλα υπάρχουν αρκετοί τρόποι με τους οποίους οι κόμβοι μπορούν να μοιραστούν τα κλειδιά. Δύο κόμβοι μπορούν να μοιράζονται ένα συμμετρικό κλειδί, ενότητα 2.4.2.1, τόσο για να κωδικοποιούν όσο και να αποκωδικοποιούν τα μηνύματα που ανταλλάζονται. Μια άλλη μέθοδος είναι η χρήση ασύμμετρου κλειδιού, ενότητα 2.4.2.2, όπου ο κάθε κόμβος έχει ένα δημόσιο κλειδί με το οποίο οι άλλοι κόμβοι κωδικοποιούν τα δεδομένα που θέλουν να του στείλουν και ένα μυστικό προσωπικό κλειδί το οποίο χρησιμοποιείται για την αποκωδικοποίηση των δεδομένων που παραλαμβάνει. Όλοι οι κόμβοι σε ένα δίκτυο μπορεί να μοιράζονται ένα κοινό κλειδί – global key, το οποίο χρησιμοποιούν για να επικοινωνήσουν μεταξύ τους. Γειτονικοί κόμβοι ή κόμβοι που ανήκουν στην ίδια ομάδα – cluster, μπορεί να μοιράζονται ένα επιπλέον κλειδί – group key, το οποίο χρησιμοποιούν για να επικοινωνούν μεταξύ τους.

3.2.1.5 Applicability relevant to the environment

Ανάλογα με την περιοχή στην οποία θα τοποθετηθεί ένα δίκτυο και τη λειτουργικότητα που θα έχει υπάρχουν διαφορετικές απαιτήσεις σε θέματα

ασφάλειας. Μερικές εφαρμογές όπου μπορούν να χρησιμοποιηθούν τα δίκτυα αισθητήρων είναι:

- Μέτρηση διάφορων περιβαλλοντικών παραμέτρων.
- Έλεγχος διάφορων παραμέτρων στον τομέα της υγείας.
- Παρατήρηση των συνθηκών που επικρατούν σε μια στρατιωτική περιοχή, σε ένα πεδίο μάχης.

Για παράδειγμα, για τα δεδομένα που παίρνουμε από ένα δίκτυο το οποίο είναι τοποθετημένο σε πεδίο μάχης είναι σημαντικό να είναι επιβεβαιωμένη η ταυτότητα του αποστολέα του πακέτου και το περιεχόμενο να μην είναι αλλοιωμένο. Επίσης, είναι σημαντικό το δίκτυο να μείνει ζωντανό για όσο το δυνατό περισσότερο χρόνο. Σε μια εφαρμογή η οποία παίρνει μετρήσεις από το σπίτι ενός ασθενή μας ενδιαφέρει πάλι τα δεδομένα που μεταφέρονται να είναι αυθεντικά αλλά αν η διάρκεια ζωής των αισθητήρων δεν είναι τόσο μεγάλη, δεν αποτελεί μεγάλο πρόβλημα επειδή πολύ εύκολα μπορούν να αντικατασταθούν.

3.2.2 Security

Όπως αναφέρθηκε και σε προηγούμενα κεφάλαια, η ασφάλεια είναι απαραίτητη και αναγκαία σε ένα σύγχρονο δίκτυο. Για να εξασφαλιστεί η ασφάλεια σε δίκτυα αναπτύχθηκαν πρωτόκολλα τα οποία πληρούν σημαντικές ιδιότητες για θέματα ασφάλειας. Οι ιδιότητες αυτές περιγράφονται στην ενότητα 2.3. Ταυτόχρονα, χρησιμοποιούν διάφορες μεθόδους κρυπτογράφησης, μερικές από τις οποίες εξηγούνται στην ενότητα 2.4, και ακολουθούν κάποια τακτική για αντιμετώπιση των εχθρικών κόμβων. Τα σημεία αυτά θα αναλυθούν περαιτέρω στις ενότητες που θα ακολουθήσουν.

3.2.2.1 Operational Objectives

Το κάθε πρωτόκολλο ασφάλειας αναπτύσσεται με διαφορετικό στόχο. Ένας από αυτούς μπορεί να θεωρηθεί η πρόληψη κάποιον επιθέσεων – prevention, δηλαδή

προσπαθούν να προστατέψουν το δίκτυο από κάποιες επιθέσεις πριν καν εμφανιστούν. Μια άλλη είναι ο εντοπισμός των διάφορων επιθέσεων και η δυναμική αντιμετώπισή τους κατά τον εντοπισμό τους – detection/ recovery. Ένα τρίτο στόχο αποτελεί και η απαίτηση για ευέλικτο και ανθεκτικό πρωτόκολλο – resilience.

3.2.2.2 Methods Used/ Provided

Υπάρχουν πολλές τακτικές οι οποίες μπορούν να χρησιμοποιηθούν για την κρυπτογράφηση των μηνυμάτων και επιβεβαίωση της μη τροποποίησής τους. Κάθε μια από αυτές έχει τα δικά της πλεονεκτήματα και μειονεκτήματα. Η κρυπτογράφηση ενός μηνύματος μπορεί να γίνει με τη χρήση τόσο συμμετρικού όσο και ασύμμετρου κλειδιού – ενότητα 3.2.1.4, αλλά και με τη χρήση ενός hash function – ενότητα 2.4.2.4. Ανάλογα με τις ανάγκες και τις αρχές του κάθε πρωτοκόλλου επιλέγετε και η καταλληλότερη μέθοδος. Αν για παράδειγμα σε ένα δίκτυο είναι υψίστης σημασίας η μεγιστοποίηση του χρόνου ζωής του, τότε πιθανός να μην χρησιμοποιηθεί η ασύμμετρη κρυπτογράφηση και να προτιμηθεί η συμμετρική κρυπτογράφηση. Η επιλογή αυτή βασίζεται στο ότι για την λειτουργία της ασύμμετρης κρυπτογράφησης είναι αναγκαία η ανταλλαγή περισσότερων μηνυμάτων σε σχέση με την συμμετρική κρυπτογράφηση έχοντας ως αποτέλεσμα την ταχύτερη εξάντληση των πόρων του αισθητήρα.

Με τη χρήση αλγορίθμων οι κόμβοι μπορούν να ελέγξουν στοιχεία τα οποία είναι αναγκαία για την ύπαρξη ασφάλειας και προστασίας δεδομένων. Παραδείγματος χάριν ένας MAC αλγόριθμος – Message Authentication Code, μπορεί να χρησιμοποιηθεί για την πιστοποίηση της μη τροποποίησης του περιεχομένου ενός μηνύματος κατά τη μεταφορά του αλλά και την ταυτότητα του αποστολέα. Για τη λειτουργία του αλγορίθμου αυτού, είναι αναγκαία η ανταλλαγή ενός κοινού κλειδιού μεταξύ αποστολέα και παραλήπτη και η χρήση μιας κοινής συνάρτησης για παραγωγή μιας σύντομης κωδικοποίησης ενός μηνύματος. Ο αποστολέας

ενός πακέτου χρησιμοποιεί το κλειδί και με τη χρήση της κοινής συνάρτησης παράγει ένα “κωδικό” ο οποίος χαρακτηρίζει το πακέτο. Ο κωδικός που παράγεται αποστέλλεται μαζί με το πακέτο στον παραλήπτη. Ο παραλήπτης με τη σειρά του, θα υπολογίσει το δικό του κωδικό για το πακέτο που παρέλαβε και αν αυτό συμφωνεί με τον κωδικό που πήρε μαζί με το πακέτο το αποδέχεται, διαφορετικά το απορρίπτει.

Τέλος, το κάθε πρωτόκολλο αντιμετωπίζει διαφορετικά τους εχθρικούς κόμβους. Μπορεί να ακολουθήσει μια στρατηγική ούτως ώστε να περιορίσει τις επιθέσεις τους – watchdog, ή να τους απομακρύνει πλήρως από το δίκτυο – blacklist.

3.2.2.3 Security Properties Provided

Όπως αναφέρεται και στην ενότητα 2.3, υπάρχουν κάποιες ιδιότητες οι οποίες είναι απαραίτητες για την ύπαρξη στοιχειώδους ασφάλειας σε ένα δίκτυο. Είναι σημαντικό να γνωρίζουμε ποιες από αυτές της ιδιότητες πληρούνται από ένα πρωτόκολλο. Με τη γνώση αυτή είναι πιο εύκολο να αξιολογήσουμε ένα πρωτόκολλο, να βρούμε τα μειονεκτήματα του και να αναγνωρίσουμε τα πρωτόκολλα που μπορεί να αντιμετωπίσει. Οι ιδιότητες που αφορούν την ασφάλεια ενός δικτύου είναι οι ακόλουθες:

- Integrity of Data: Ο παραλήπτης ενός πακέτου να μπορεί να ελεεί κατά πόσο το πακέτο που πήρε είναι αλλοιωμένο ή όχι. Τόσο ο παραλήπτης όσο και ο αποστολέας ενός πακέτου δεσμεύονται και δεν μπορούν να αρνηθούν τη συμμετοχή τους στην ανταλλαγή ενός πακέτου.
- Confidentiality: Το περιεχόμενο ενός πακέτου να είναι κατανοητό μόνο από τον αποστολέα και τον παραλήπτη του.
- Availability: Οι υπηρεσίες και οι πληροφορίες που προσφέρονται μέσω του δικτύου πρέπει να είναι διαθέσιμες οποιαδήποτε στιγμή.
- Non Repudiation: Ο παραλήπτης ενός πακέτου πρέπει να είναι σε θέση να ”αποδείξει” σε ένα τρίτο κόμβο πως το πακέτο που πήρε πράγματι

στάλθηκε από τον αναμενόμενο αποστολέα. Επίσης ο αποστολέας ενός μηνύματος δεν μπορεί να αρνηθεί πως έστειλε ένα πακέτο.

- Integrity of Origin/ Destination: Οι κόμβοι που συμμετέχουν σε μια επικοινωνία πρέπει να μπορούν να επιβεβαιώσουν τις ταυτότητες των κόμβων με τους οποίους επικοινωνούν ανταλλάζοντας πακέτα.

3.2.3 Functionality Provided

Μέχρι σήμερα έχουν αναπτυχθεί πολλά διαφορετικά πρωτόκολλα ασφάλειας για το επίπεδο δρομολόγησης σε δίκτυα αισθητήρων. Κάθε ένα από αυτά έχει τις δικές του ιδιαιτερότητες. Μερικές από αυτές τις ιδιαιτερότητες επηρεάζουν άμεσα και τη λειτουργικότητα του πρωτοκόλλου. Για παράδειγμα ο χρόνος ζωής του δικτύου είναι ανάλογος του αριθμού των μηνυμάτων που χρειάζεται να ανταλλαγούν για τη λειτουργία του πρωτοκόλλου. Άμεσα συνδεδεμένη μπορεί να θεωρηθεί και η ανάγκη για συγχρονισμό των κόμβων. Τέλος, αφού βρισκόμαστε στο επίπεδο δρομολόγησης, σημαντικό ρόλο στην λειτουργικότητα του πρωτοκόλλου διαδραματίζει ο τρόπος που χτίζονται οι πίνακες δρομολόγησης, αν υποστηρίζεται multi path routing και ο τρόπος με τον οποίο ενημερώνονται οι πίνακες αυτοί.

3.2.3.1 Synchronization

Για τη λειτουργία μερικών πρωτοκόλλων απαιτείται ισχυρό – strong, ή πιο χαλαρός – weak, συγχρονισμός μεταξύ των κόμβων του δικτύου. Σε αρκετές περιπτώσεις ο συγχρονισμός αυτός είναι απαραίτητος επειδή αποτελεί ένα μηχανισμό αποδοχής ή απόρριψης κάποιου πακέτου. Αν ένα πρωτόκολλο απαιτεί ισχυρό συγχρονισμό τότε τα μηνύματα που αναμένεται να ανταλλάξουν μεταξύ τους οι κόμβοι του δικτύου είναι περισσότερα, άρα και τα ποσά ενέργειας που καταναλωθούν είναι πιο πολλά.

3.2.3.2 Proactive / Reactive Nature

Υπάρχουν δύο τεχνικές οι οποίες μπορούν να χρησιμοποιηθούν για την ενημέρωση των πινάκων δρομολόγησης των αισθητήρων. Με βάση την πρώτη τεχνική οι πίνακες δρομολόγησης ανανεώνονται περιοδικά – proactive. Σύμφωνα όμως με την δεύτερη, ένας αισθητήρας θα προσθέσει στον πίνακα δρομολόγησής του ένα μονοπάτι που οδηγεί σε ένα κόμβο μόνο όταν θέλει να του στείλει κάτι – reactive. Τα πλεονεκτήματα ενός proactive συστήματος είναι ότι λαμβάνονται υπόψη οι αλλαγές που εμφανίζονται στο δίκτυο με τη πάροδο του χρόνου. Οι αλλαγές αυτές μπορεί να προκληθούν από την εισαγωγή νέων κόμβων στο δίκτυο ή από την απομάκρυνση κάποιων άλλων. Αυτό όμως εξυπακούει και την κατανάλωση περισσότερης ενέργειας αφού ανταλλάζονται περισσότερα μηνύματα περιοδικά από τους αισθητήρες για ενημέρωση των πινάκων δρομολόγησής τους. Σε αντίθεση με το proactive σύστημα, το reactive προσθέτει ένα μονοπάτι την στιγμή που θα το χρειαστεί και δεν συντηρεί ένα μεγάλο πίνακα δρομολόγησης με προορισμούς τους οποίους μπορεί να μην χρησιμοποιήσει ποτέ.

3.2.3.3 Multipath Routing

Μερικά πρωτόκολλα δρομολόγησης αναπτύσσονται λαμβάνοντας υπόψη και την δρομολόγηση των πακέτων χρησιμοποιώντας διαφορετικές διαδρομές, multipath routing. Η διαδικασία αυτή έχει θετικά στοιχεία αλλά και αρνητικά. Ένα θετικό στοιχείο μπορεί να σημειωθεί στο ακόλουθο σενάριο: έστω ένας κόμβος Α ο οποίος χρησιμοποιείται για την δρομολόγηση ενός πακέτου από τον κόμβο Κ στον κόμβο Μ. Αν ο κόμβος Α καταρρεύσει θα χρειαστεί κάποιος χρόνος μέχρι να δημιουργηθεί ένα νέο μονοπάτι μεταξύ του κόμβου Κ και Μ. Με τη χρήση ενός multi path πρωτοκόλλου κάθε στιγμή έχω και εναλλακτικά μονοπάτια για ένα προορισμό, έτσι η διαδικασία δρομολόγησης των πακέτων με τη χρήση άλλου μονοπατιού είναι πολύ πιο γρήγορη και εξοικονομείται ενέργεια.

3.2.3.4 Network Lifetime

Όπως φαίνεται και στις τρεις πιο πάνω υποενότητες, η ενέργεια που καταναλώνεται σε ένα δίκτυο εξαρτάται άμεσα από τον τρόπο που είναι σχεδιασμένα τα λογισμικά που θα εφαρμοστούν σε αυτό και κατ' επέκταση ο τρόπος λειτουργίας του πρωτοκόλλου που θα εφαρμοστεί για την ύπαρξη ασφάλειας στο επίπεδο δρομολόγησης. Όταν λοιπόν ένας αισθητήρας καταναλώνει λιγότερα ποσά ενέργειας αυξάνει την διάρκεια ζωής του. Όσο πιο "οικονομικά" σε θέματα ενέργειας είναι τα πρωτόκολλα που εφαρμόζονται σε ένα δίκτυο αισθητήρων τόσο αυξάνεται και η διάρκεια ζωής του δικτύου.

3.2.4 Performance

Η απόδοση ενός πρωτοκόλλου το οποίο αναπτύχθηκε για ασφάλεια στο επίπεδο δρομολόγησης μπορεί να καθοριστεί με βάση τις επιθέσεις που μπορεί να αντιμετωπίσει, όπως αυτές περιγράφονται στην ενότητα 2.6.1. Παράλληλα μπορεί να δοθεί βαρύτητα και στα ποσά ενέργειας που καταναλώνει. Γενικά, υπάρχουν τρεις τεχνικές οι οποίες χρησιμοποιούνται για την αξιολόγηση ενός πρωτοκόλλου. Η πρώτη είναι με μαθηματική ανάλυση, η δεύτερη με την υλοποίηση του πρωτοκόλλου και εφαρμογή του σε πραγματικούς αισθητήρες και η τρίτη αφορά την χρήση ενός προσομοιωτή ο οποίος προσομοιώνει το πρωτόκολλο που θέλουμε και κάνει διάφορες μετρήσεις για να υπολογίσει την απόδοσή του.

3.2.4.1 Defense / Attacks Addressed

Όπως προαναφέρθηκε, η ασφάλεια που προσφέρει ένα πρωτόκολλο είναι ανάλογη των επιθέσεων που μπορεί να αντιμετωπίσει. Παράλληλα, είναι σημαντικό να γνωρίζουμε τις επιθέσεις που αντιμετωπίζει το κάθε πρωτόκολλο ούτως ώστε να μπορούμε να επιλέξουμε το ιδανικότερο για την εφαρμογή που

θα το εφαρμόσουμε. Για τους σκοπούς της εργασίας αυτής θα μελετηθεί κατά πόσο ένα πρωτόκολλο αντιμετωπίζει τις επιθέσεις που ακολουθούν καθώς και τον τρόπο με τον οποίο τις αντιμετωπίζει. Θα μελετηθούν οι πιο κοινές επιθέσεις που μπορούν να εφαρμοστούν σε ένα δίκτυο – αφού είναι και οι κύριες επιθέσεις που τα πρωτόκολλα ασφάλειας προσπαθούν να αντιμετωπίσουν. Οι επιθέσεις αυτές είναι: Wormhole, Sinkhole, Sybil, Hello, Denial of Service και Selective forward. Περισσότερες πληροφορίες για τις επιθέσεις αυτές υπάρχουν στην ενότητα 2.6.1.

3.2.4.2 Energy Usage

Λόγω των ιδιαιτεροτήτων των δικτύων αισθητήρων τα πρωτόκολλα που θα εφαρμοστούν σε αυτά πρέπει να είναι όσο το δυνατό λιγότερο σπάταλα σε θέματα ενέργειας. Για να προσδιορίσουμε κατά μέσω όρο την ενέργεια που χρειάζεται ένα πρωτόκολλο μπορούμε να μετρήσουμε τον αριθμό των μηνυμάτων που αποστέλλονται για κάθε λειτουργία του. Ακόμα, μπορούμε να συγκρίνουμε το επιπρόσθετο κόστος που υπάρχει, overhead, μεταξύ πρωτοκόλλων. Το επιπρόσθετο κόστος μπορεί να μετρηθεί ως συνάρτηση των επιπλέον bytes που στέλνονται σε κάθε πακέτο ή ως συνάρτηση του αριθμού των μηνυμάτων που πρέπει να ανταλλαγούν για μια συγκεκριμένη διαδικασία – για παράδειγμα των αριθμό των μηνυμάτων που πρέπει να ανταλλαγούν για τον συγχρονισμό δύο κόμβων ή την ασφαλή επικοινωνία μεταξύ δύο κόμβων.

3.2.4.3 Analysis

Η ανάλυση των πρωτοκόλλων μπορεί να γίνει με τρεις τρόπους: μαθηματική ανάλυση, υλοποίηση του πρωτοκόλλου και εφαρμογή του σε πραγματικούς αισθητήρες ή να χρησιμοποιηθεί ένας προσομοιωτής στον οποίο το πρωτόκολλο προσομοιώνεται και γίνονται μετρήσεις για την απόδοσή του. Με τη μαθηματική ανάλυση πρέπει κάθε λειτουργία του πρωτοκόλλου να εξηγηθεί με μαθηματικούς

όρους και σύμβολα. Αν υλοποιήσουμε ένα πρωτόκολλο και το εφαρμόσουμε σε πραγματικούς αισθητήρες για να το αξιολογήσουμε και να κάνουμε τις απαραίτητες μετρήσεις θα έχουμε να αντιμετωπίσουμε αρκετά προβλήματα. Τα προβλήματα αυτά οφείλονται στις ιδιαιτερότητες τόσο των ίδιων των αισθητήρων όσο και του περιβάλλοντος στο οποίο θα τοποθετηθούν και στις παρεμβολές που υπάρχουν κατά τη μετάδοση των σημάτων. Αντίθετα, αν το πρωτόκολλο αξιολογηθεί με τη χρήση ενός προσομοιωτή δεν υπάρχουν αυτά τα προβλήματα. Επιπρόσθετα, μπορούν να γίνουν πολλά πειράματα αλλάζοντας πολύ εύκολα διάφορες παραμέτρους και περιλαμβάνοντας διαφορετικό αριθμό αισθητήρων. Ένα μειονέκτημα που μπορούμε να αναθέσουμε στην προσομοίωση ενός πρωτοκόλλου είναι ότι δεν λαμβάνονται υπόψη οι φυσικές δυσκολίες και τα φυσικά προβλήματα που είναι αναπόφευκτα όταν το πρωτόκολλο εφαρμοστεί σε πραγματικούς αισθητήρες και χρησιμοποιείται.

Για τους προαναφερόμενους λόγους ο αναγνώστης πρέπει να έχει υπόψη τον τρόπο που έγινε η ανάλυση ενός πρωτοκόλλου και αναλόγως να ξέρει τι απόδοση να περιμένει όταν το εφαρμόσει σε άλλες συνθήκες. Γι παράδειγμα, αν η ανάλυση έγινε με την χρήσης προσομοιωτή τότε όταν θα εφαρμόσουμε το ίδιο πρωτόκολλο σε πραγματικούς αισθητήρες δεν πρέπει να αναμένουμε την ίδια απόδοση.

Η ανάλυση η οποία θα ακολουθήσει στο κεφάλαιο 4 θα γίνει με βάση την ταξινόμηση που αναλύθηκε στο κεφάλαιο 3. Αυτή η ανάλυση είναι χρήσιμη για την κατανόηση του τρόπου λειτουργίας του πρωτοκόλλου. Ακολούθως, στο κεφάλαιο 5 θα γίνει μια πιο συγκεκριμένη και εκτενής ανάλυση για την μέθοδο που χρησιμοποιείται από το κάθε πρωτόκολλο για την αντιμετώπιση ενός attack.

Κεφάλαιο 4

Ανάλυση Πρωτοκόλλων που Μελετήθηκαν

4.1 Πρωτόκολλα που Μελετήθηκαν

Για τους σκοπούς της συγκεκριμένης ατομικής διπλωματικής εργασίας επιλέχθηκαν τα ακόλουθα επτά πρωτόκολλα:

1. CBSRP – Certainty Based Secure Routing Protocol
2. SecRout Secure Routing Protocol
3. Secure Sensor Network Routing: A Clean State Approach
4. SPINS
5. Secure SPIN
6. SHEER – Secure Hierarchical Energy Efficient Routing
7. OPSENET – Security Scheme for Optical Sensor Networks

Τα προαναφερόμενα πρωτόκολλα θα αναλυθούν με βάση τα στοιχεία που αναφέρονται στο κεφάλαιο 3. Ακολούθως στο κεφάλαιο 5 θα μελετηθούν με περισσότερη λεπτομέρεια οι τρόποι αντιμετώπισης των διάφορων επιθέσεων.

4.2 CBSRP – Certainty Based Secure Routing Protocol

Το πρωτόκολλο CBSRP [12] – Certainty Based Secure Routing Protocol, χτίστηκε με τη φιλοσοφία των clusters και στοχεύει στη μείωση της ενέργειας που χρειάζεται για την αποστολή ενός πακέτου. Για να το πετύχει αυτό αλλάζει δυναμικά το επίπεδο της ασφάλειας που προσφέρει στο δίκτυο, ανάλογα με τις ανάγκες της εφαρμογής και τα διαθέσιμα ποσά ενέργειας του δικτύου. Λόγω της δυναμικής αλλαγής στο επίπεδο ασφάλειας του δικτύου χρησιμοποιείται και μια τιμή βεβαιότητας – certainty, η οποία χρησιμοποιείται για την παραγωγή νέου κλειδιού κωδικοποίησης των μηνυμάτων που θα σταλούν. Ουσιαστικά η τιμή αυτή καθορίζει κατά πόσο το περιεχόμενο του πακέτου μπορεί να θεωρηθεί ασφαλές – trusted.

Όπως αναφέρεται και πιο πάνω, η αρχιτεκτονική του δικτύου στο οποίο εφαρμόζεται το CBSRP είναι ιεραρχική, οργανωμένη σε clusters και οι κόμβοι που συμμετέχουν σε αυτό είναι στατικοί. Ένας απλός κόμβος στέλνει μηνύματα μόνο στον cluster head της ομάδας στην οποία ανήκει. Ο cluster head επικοινωνεί με τους κόμβους που ανήκουν στο cluster του αλλά και με το sink, τον κεντρικό σταθμό στον οποίο στέλνουν δεδομένα ή παίρνουν request. Άρα με τη σειρά του το sink επικοινωνεί μόνο με τα cluster heads τα οποία αναλαμβάνουν να ενημερώσουν τους κόμβους που υπάρχουν στο cluster τους. Η επικοινωνία μεταξύ των κόμβων είναι unreliable, αφού δεν στέλνονται acknowledgments στην παραλαβή ενός πακέτου. Επίσης, το σύστημα είναι κλειστό, αφού δεν μπορούν να εισέλθουν σε αυτό δυναμικά νέοι κόμβοι.

Η αξιολόγηση του πρωτοκόλλου έγινε με την υλοποίηση και εφαρμογή του σε πραγματικούς αισθητήρες. Τα χαρακτηριστικά των αισθητήρων είναι τα ακόλουθα:

Processing Capabilities:

- CPU: Atmel Atmega 128L processor – 4 MHz
- Storage: 128Kbytes of flash memory
  4 Mbit serial flash
  4Kbytes of SRAM
  4Kbyte EEPROM

Battery Lifetime:

- 2 AA batteries - roughly 1 year life depending on the application

Radio Communication:

- 916 or 433 MHz radio
- Bandwidth 40 Kbps

Operating System:

- TinyOS

Η δρομολόγηση των πακέτων στο πρωτόκολλο αυτό γίνεται με βάση την τοποθεσία των κόμβων στο δίκτυο ενώ παράλληλα δεν γίνεται αναφορά για κάποια security assumptions. Τα κλειδιά που χρησιμοποιούνται για την κωδικοποίηση των μηνυμάτων υπολογίζονται δυναμικά – φυσικά είναι απαραίτητη η ύπαρξη ενός αρχικού κλειδιού καθώς και μια συνάρτηση η οποία παράγει τα νέα κλειδιά. Τα κλειδιά που παράγονται μπορούν να χαρακτηριστούν ως τυχαία, αφού για την παραγωγή τους χρησιμοποιείται ένας βαθμός βεβαιότητας ο οποίος αλλάζει με την πάροδο του χρόνου καθώς και ένας τυχαίος αριθμός. Για την αποκωδικοποίηση του μηνύματος που παραλήφθηκε χρησιμοποιείται η μέθοδος του συμμετρικού κλειδιού.

Λόγω του ότι το επίπεδο ασφάλειας που προσφέρει το πρωτόκολλο αλλάζει ανάλογα με τους διαθέσιμους ενεργειακά πόρους του δικτύου, δεν είναι ιδανικό για εφαρμογές που η ύπαρξη ασφάλειας είναι απαραίτητη. Τέτοιες εφαρμογές μπορούν να θεωρηθούν εκείνες που εφαρμόζονται σε εχθρικές περιοχές για έλεγχο του πεδίου μάχης καθώς και εφαρμογές για έλεγχο διάφορων

παραμέτρων στον τομέα της υγείας. Είναι κατάλληλο για εφαρμογές που μετρούν διάφορες περιβαλλοντικές παραμέτρους.

Ο τρόπος που επικοινωνούν οι κόμβοι του δικτύου και η δυναμική αλλαγή των κλειδιών που χρησιμοποιούνται βοηθά στην πρόληψη για μερικές επιθέσεις. Όπως ήδη αναφέρθηκε, χρησιμοποιείται συμμετρική κρυπτογράφηση. Όλες οι προϋποθέσεις για την ύπαρξη ασφάλειας, όπως αυτές περιγράφονται στην ενότητα 2.3, εφαρμόζονται στο πρωτόκολλο αυτό. Το δίκτυο αναδιοργανώνεται όταν το ζητήσει το base station – proactive.

Αντιμετωπίζονται οι επιθέσεις: wormhole, sinkhole, denial of service και selective forward. Η επίθεση Hello δεν μπορεί να εφαρμοστεί στο πρωτόκολλο αυτό επειδή οι κόμβοι δεν στέλνουν μηνύματα για να αναγγείλουν τον εαυτό τους στο δίκτυο. Ούτε και η επίθεση sybil μπορεί να εφαρμοστεί στο δίκτυο αφού το πρωτόκολλο CBSRP δεν λαμβάνει καθόλου υπόψη την τοποθεσία των κόμβων στο δίκτυο.

Με το πρωτόκολλο αυτό, σε κάθε πακέτο που στέλνεται, χρησιμοποιούνται 8 bytes για την αποστολή των παραμέτρων που χρειάζονται για την παραγωγή του κλειδιού αποκωδικοποίησης. Τέλος, η ανάλυση του πρωτοκόλλου – στο αντίστοιχο άρθρο που μελέτησα, έγινε με την υλοποίησή του και εφαρμογή του σε αισθητήρες. Εξέτασαν την σχέση μεταξύ της ενέργειας που καταναλώνεται και του βαθμού βεβαιότητας που χρησιμοποιείται για την κωδικοποίηση των πακέτων.

4.3 SecRout

Το πρωτόκολλο SecRout [13] – Secure Routing Protocol for Sensor Networks, εγγυάται ότι ο παραλήπτης ενός πακέτου μπορεί να αναγνωρίσει ποια από τα πακέτα που παρέλαβε είναι αλλοιωμένα και τα απορρίπτει.

Όταν θα δημιουργηθεί το δίκτυο είναι αναγκαία η αυτοοργάνωση των στατικών κόμβων σε clusters. Με βάση το SecRout, μετά την αυτοοργάνωση των κόμβων σε clusters, ο κάθε κόμβος ξέρει την ταυτότητα του cluster head του και με τη σειρά του το κάθε cluster head γνωρίζει τις ταυτότητες όλων των κόμβων που ανήκουν στο cluster του. Επίσης, το sink node γνωρίζει την τοπολογία του δικτύου που σχηματίζεται μετά την αυτοοργάνωσή του καθώς και τις ταυτότητες και τα κλειδιά όλων των κόμβων που υπάρχουν στο δίκτυο. Τα δεδομένα που συλλέγουν οι κόμβοι τα στέλνουν στο cluster head τους το οποίο αναλαμβάνει να στα στείλει στον προορισμό τους. Η επικοινωνία των κόμβων είναι reliable, αφού στέλνονται acknowledgments για τα πακέτα που ανταλλάζονται καθώς και για τα request. Το δίκτυο που δημιουργείται είναι κλειστό, αφού δεν μπορούν δυναμικά να εισέλθουν νέοι κόμβοι.

Για την λειτουργία του πρωτοκόλλου γίνεται η υπόθεση ότι ο κάθε κόμβος έχει μια ταυτότητα και υπάρχει ένας sink κόμβος ο οποίος είναι έμπιστος. Η αρχιτεκτονική του δικτύου είναι ιεραρχική και οργανώνονται με βάση την τοποθεσία των κόμβων. Οι κόμβοι του δικτύου πρέπει πριν την εισαγωγή τους σε αυτό να έχουν ένα κλειδί το οποίο θα χρησιμοποιούν για την κρυπτογράφηση των μηνυμάτων που θα στέλνουν. Όπως αναφέρεται και πιο πάνω, οι κόμβοι στέλνουν τα πακέτα στο cluster head και τα κωδικοποιούν χρησιμοποιώντας το cluster key το οποίο καθορίζεται κατά τη διάρκεια της αυτοοργάνωσης του δικτύου. Χρησιμοποιείται συμμετρική κρυπτογράφηση.

Το πρωτόκολλο αυτό μπορεί να χρησιμοποιηθεί τόσο σε εφαρμογές για μέτρηση διάφορων περιβαλλοντικών παραμέτρων όσο και σε εφαρμογές που ελέγχουν διάφορες παραμέτρους στον τομέα της υγείας. Δεν μπορούν να χρησιμοποιηθούν σε εφαρμογές που παρατηρούν τις συνθήκες που επικρατούν σε ένα πεδίο μάχης επειδή σε περίπτωση που η τοποθέτηση τους θα γίνει με το πέταγμά τους από αεροπλάνο τότε δεν υπάρχει καμία εγγύηση ότι θα είναι στο πεδίο εμβέλειας της ακτίνας του base station.

Το SecRout εντοπίζει τους κακόβουλους κόμβους – malicious nodes, και τους μπλοκάρει. Επίσης το πρωτόκολλο είναι ευέλικτο, αφού η αφαίρεση μερικών κόμβων από το δίκτυο – όπως για παράδειγμα η αφαίρεση των κακόβουλων κόμβων, δεν σημαίνει ταυτόχρονα και την παράλυσή του. Οι κακόβουλοι κόμβοι που εντοπίζονται μπαίνουν σε μαύρη λίστα – black list. Οι κόμβοι του δικτύου δεν αποδέχονται πακέτα ή request που λαμβάνουν από κόμβους που έχουν τοποθετήσει σε μαύρη λίστα. Γενικότερα, για την κρυπτογράφηση των πακέτων χρησιμοποιείται συμμετρική κρυπτογράφηση και για την πιστοποίηση της αυθεντικότητας του πακέτου χρησιμοποιείται το MAC – Message Authentication Code. Όλες οι προϋποθέσεις για την ύπαρξη ασφάλειας, εφαρμόζονται στο πρωτόκολλο αυτό.

Ο πίνακας δρομολόγησης που χρησιμοποιείται ενημερώνεται μόνο όταν ο κόμβος θέλει να στείλει δεδομένα σε ένα άλλο κόμβο στον οποίο δεν έστειλε ξανά κάτι – reactive. Λόγω του ότι κάθε κόμβος δημιουργεί μια μόνο εγγραφή για ένα προορισμό δεν υπάρχει δυνατότητα για multipath routing.

Αντιμετωπίζονται οι επιθέσεις: wormhole, sybil, denial of service και selective forward. Η επίθεση sinkhole δεν εφαρμόζεται στο δίκτυο αφού τα χαρακτηριστικά των κόμβων δεν λαμβάνονται υπόψη για τη δρομολόγηση των πακέτων. Όσων αφορά την επίθεση hello δεν υπάρχουν αρκετές πληροφορίες για τον τρόπο που χτίζεται το δίκτυο κι έτσι δεν μπορούμε να αποφασίσουμε κατά πόσο αντιμετωπίζεται ή όχι η επίθεση αυτή. Για παράδειγμα δεν ξέρουμε αν στέλνουν hello messages οι κόμβοι για να αναγγείλουν τον εαυτό τους στο δίκτυο και αν τα μηνύματα αυτά γίνονται δεκτά μόνο για μια χρονική περίοδο.

Συγκριτικά με το πρωτόκολλο AODV - Ad hoc on Demand Distance Vector Routing, το SecRout έχει περίπου 6% περισσότερο byte overhead. Η ανάλυση του πρωτοκόλλου έγινε με τη χρήση του προσομοιωτή NS2. Στην ανάλυση αυτή μετρήθηκε το packet delivery ratio, byte overhead και packet latency σε σχέση με τον χρόνο.

4.4 Secure Sensor Network Routing: A Clean State Approach

Το πρωτόκολλο αυτό [14] δεν απαιτεί κάποιο ειδικό υλικό για την λειτουργία του και εξασφαλίζει την παράδοση των πακέτων ακόμα και αν στο δίκτυο υπάρχουν ενεργοί αντίπαλοι – εχθρικοί κόμβοι. Στόχοι των σχεδιαστών του πρωτοκόλλου αυτού είναι η ύπαρξη ασφάλειας αλλά και αποδοτικότητας. Το πρωτόκολλο είναι ευέλικτο και προσαρμόζεται στις επιθέσεις των εχθρικών κόμβων.

Το πρωτόκολλο αυτό είναι ιεραρχικά δομημένο. Μετά την οργάνωση του δικτύου οι κόμβοι είναι οργανωμένοι σε groups και έχουν μοναδική διεύθυνση στο δίκτυο. Τα πακέτα προωθούνται από κόμβο σε κόμβο με βάση τα prefix που αποθηκεύονται στους πίνακες δρομολόγησής τους. Οι πίνακες δρομολόγησης συμπληρώνονται κατά τη διάρκεια οργάνωσης του δίκτυου. Οι κόμβοι στο δίκτυο αυτό είναι στατικοί αλλά μπορούν να είναι και κινητοί επειδή ο αλγόριθμος οργάνωσης του δικτύου τρέχει περιοδικά. Για το λόγο αυτό το δίκτυο είναι ανοιχτό αφού μπορούν μετά την αρχική οργάνωση του δικτύου να προστεθούν νέοι κόμβοι σε αυτό. Η επικοινωνία γίνετε μεταξύ των κόμβων του δικτύου και γίνεται με τη χρήση reliable broadcast.

Το πρωτόκολλο αυτό επηρεάζεται από την τοποθεσία των κόμβων στο δίκτυο και λειτουργεί με την προϋπόθεση ότι τόσο το hardware που αποτελεί τους αισθητήρες όσο και το base station είναι έμπιστα. Τα κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση των πακέτων αποθηκεύονται στους αισθητήρες πριν την εισαγωγή τους στο δίκτυο. Η κρυπτογράφηση γίνεται με τη χρήση ασύμμετρου κλειδιού – δημόσιου κλειδιού. Υπάρχει επίσης και η υπόθεση ότι στον κάθε κόμβο δίνεται μια μοναδική ταυτότητα η οποία συνοδεύεται με ένα certificate αυθεντικότητας.

Το πρωτόκολλο αυτό μπορεί να χρησιμοποιηθεί τόσο σε εφαρμογές για μέτρηση διάφορων περιβαλλοντικών παραμέτρων όσο και σε εφαρμογές που ελέγχουν

διάφορες παραμέτρους στον τομέα της υγείας ή παρατηρούν τις συνθήκες που επικρατούν σε ένα πεδίο μάχης.

Το Secure Sensor Network Routing: A Clean State Approach δεν παρεμποδίζει μόνο την ύπαρξη ενός κακόβουλου κόμβου αλλά τους εντοπίζει και τους απομακρύνει από το δίκτυο. Για παράδειγμα, οι κόμβοι δεν μπορούν να εισέλθουν στο δίκτυο όποτε το επιθυμούν. Η εισαγωγή τους μπορεί να γίνει μόνο κατά τη διάρκεια του discovery period. Με τον τρόπο αυτό οι attackers δεν μπορούν να εισέλθουν στο δίκτυο οποιαδήποτε στιγμή. Ένας άλλος τρόπος παρεμπόδισης των κακόβουλων κόμβων αποτελεί η χρήση multipath routing. Έτσι, δεν επιλέγονται πάντα οι ίδιοι κόμβοι για την δρομολόγηση των πακέτων από μια πηγή σε ένα προορισμό. Με τον τρόπο αυτό οι παρεμβολές των attacker περιορίζονται. Για τον εντοπισμό των εχθρικών κόμβων χρησιμοποιείται το Grouping Verification Tree το οποίο βασίζεται στη θεωρία των hash trees. Όσον αφορά την απομάκρυνση των κόμβων αυτών από το δίκτυο χρησιμοποιούνται οι μηχανισμοί Honeybee recovery. Επίσης το πρωτόκολλο είναι ανθεκτικό στις επιθέσεις. Ο αποστολέας ενός πακέτου μπορεί να ελέγχει την πορεία που ακολουθεί το πακέτο κι έτσι όταν εντοπίσει προβλήματα χρησιμοποιεί κάποιο άλλο μονοπάτι.

Έτσι, όλοι οι εχθρικοί κόμβοι μπαίνουν σε black list και σβήνονται από τους πίνακες δρομολόγησης των άλλων κόμβων. Για την κρυπτογράφηση των πακέτων χρησιμοποιείται η μέθοδος του δημόσιου κλειδιού σε συνδυασμό με hash chain. Παράλληλα, όλες οι προϋποθέσεις για την ύπαρξη ασφάλειας, εφαρμόζονται στο πρωτόκολλο αυτό.

Δεν χρειάζεται συγχρονισμός μεταξύ των κόμβων του δικτύου. Οι ανανέωση των πινάκων δρομολόγησης γίνονται περιοδικά – proactive, και όπως είδη αναφέρθηκε χρησιμοποιείται multipath routing. Αυτό επιτυγχάνεται με την καταχώρηση στον πίνακα δρομολόγησης περισσότερων από ενός πιθανών επόμενων κόμβων για ένα προορισμό. Αντιμετωπίζονται και οι έξι επιθέσεις που

επιλέχτηκαν για τους σκοπούς αυτής της διπλωματικής εργασίας – wormhole, sinkhole, sybil, hello, denial of service, selective forward. Η ανάλυση του πρωτοκόλλου έγινε με την χρήση προσομοιωτή και το μέγεθος του κώδικά του είναι 21 KB. Σε ένα δίκτυο με 16 κόμβους στέλνονται κατά μέσω όρο 101 μηνύματα από τον κάθε ένα. Στην ανάλυση μετρήθηκαν το routing setup overhead, path stretch, load distribution, load distribution with voids και path diversity.

4.5 SPINS

Το SPINS [15] σχεδιάστηκε για δίκτυα αισθητήρων και χρησιμοποιεί τα είδη υπάρχοντα πρωτόκολλα SNEP και μTESLA. Το SNEP προσφέρει data confidentiality, two-party data authentication και data freshness. Το μTESLA το συμπληρώνει προσφέροντας authenticated broadcast.

Η δομή του δικτύου είναι επίπεδη – στην κορυφή της βρίσκεται το base station. Οι κόμβοι στο δίκτυο είναι στατικοί και πρέπει να βρίσκονται σε τέτοια απόσταση ούτως ώστε να μπορούν να επικοινωνούν με το base station. Μηνύματα ανταλλάζονται μεταξύ του base station και ενός ή όλων των κόμβων και μεταξύ ενός κόμβου με το base station. Η επικοινωνία μεταξύ των κόμβων είναι unreliable και το σύστημα είναι ανοιχτό, αφού μπορούν να προστεθούν σε αυτό νέοι κόμβοι. Για την εισαγωγή τους είναι απαραίτητο να έχουν ένα authenticated key.

Η αξιολόγηση του πρωτοκόλλου έγινε με την υλοποίηση και εφαρμογή του σε πραγματικούς αισθητήρες. Τα χαρακτηριστικά των κόμβων στους οποίους τοποθετήθηκε το πρωτόκολλο είναι τα ακόλουθα:
Processing Capabilities:

- CPU: 8-bit, 4 MHz

- Storage: 512 bytes RAM
  512 bytes EEPROM
  8 Kbytes instruction flash
  Available code space 4500 bytes

Radio Communication:

- 916 MHz radio
- Bandwidth 10 Kbps

Operating System:

- TinyOS

Το δίκτυο λοιπόν είναι ιεραρχικό και είναι location based. Επίσης υπάρχει η προϋπόθεση πως το base station είναι trusted και κάθε κόμβος πρέπει να εμπιστεύεται τον εαυτό του.

Τα κλειδιά που θα χρησιμοποιηθούν από τους κόμβους για την κρυπτογράφηση των πακέτων τοποθετούνται σε αυτούς πριν την εισαγωγή τους στο δίκτυο – predeployment, και χρησιμοποιείται η μέθοδος του συμμετρικού κλειδιού.

Το πρωτόκολλο αυτό μπορεί να χρησιμοποιηθεί τόσο σε εφαρμογές για μέτρηση περιβαλλοντικών παραμέτρων όσο και σε εφαρμογές που σχετίζονται με τον τομέα της υγείας. Δεν μπορούν όμως να χρησιμοποιηθούν σε πεδία μάχης σε περίπτωση που η τοποθέτησή τους θα γίνει με το ρίξιμο τους από αεροπλάνο. Στην περίπτωση αυτή, δεν μπορούμε να εγγυηθούμε πως η τοποθεσία των κόμβων είναι τέτοια ούτως ώστε να βρίσκονται στο πεδίο εμβέλειας του base station για να μπορούν να επικοινωνούν μαζί του.

Το SPINS προσπαθεί να προλάβει την ύπαρξη εχθρικών κόμβων και είναι ανθεκτικό στις επιθέσεις. Οι εχθρικοί κόμβοι δεν μπαίνουν σε μαύρη λίστα αλλά ελέγχονται οι κινήσεις τους – watchdog. Για την κρυπτογράφηση των πακέτων χρησιμοποιείται το συμμετρικό κλειδί σε συνδυασμό με ένα μετρητή ο οποίος αυξάνεται στην παραλαβή/ αποστολή ενός πακέτου. Ακόμα, χρησιμοποιείται το

MAC για τον έλεγχο της αυθεντικότητας του πακέτου που παραλήφθηκε. Όλες οι προϋποθέσεις για την ύπαρξη ασφάλειας εφαρμόζονται στο πρωτόκολλο αυτό – Data Confidentiality, Authentication, Data Integrity, Non Repudiation, Availability, Access Control.

Στο πρωτόκολλο αυτό ελέγχεται και το πόσο φρέσκο είναι το πακέτο που παραλήφθηκε. Υπάρχουν δύο τρόποι ελέγχου της “φρεσκάδας” ενός πακέτου: weak και strong.

Στο SPINS τα πακέτα στέλνονται μέσω broadcast έτσι δεν ισχύει η έννοια του multipath routing. Η τοπολογία του δικτύου αλλάζει περιοδικά – proactive. Επίσης, αφού τα πακέτα στέλνονται μέσω broadcast και η τοποθεσία των κόμβων καθώς και τα χαρακτηριστικά τους δεν λαμβάνεται υπόψη μερικές επιθέσεις δεν μπορούν να εφαρμοστούν. Οι επιθέσεις αυτές είναι οι wormhole, sinkhole, sybil, selective forward. Η επίθεση hello αντιμετωπίζεται αλλά για την επίθεση denial of service δεν δίνονται αρκετές πληροφορίες για να αποφασιστεί κατά πόσο αντιμετωπίζεται ή όχι.

4.6 Secure SPIN

Το Secure SPIN [16] – Sensor Protocol for Information via Negotiation, είναι επέκταση του πρωτοκόλλου SPIN. Η συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση των πακέτων είναι τέτοια ώστε να απαιτεί μικρή μνήμη και ελάχιστη υπολογιστική ενέργεια. Το πρωτόκολλο μπορεί να χωριστεί σε τρεις φάσεις: διαφήμιση των δεδομένων που σύλλεξε ένας κόμβος – ADV, ζήτηση των δεδομένων από άλλους κόμβους – REQ, αποστολή των δεδομένων – DATA.

Το δίκτυο στο οποίο εφαρμόζεται το Secure SPIN οργανώνεται ιεραρχικά, σε clusters. Οι κόμβοι του δικτύου είναι σταθεροί ενώ το sink node μπορεί να είναι και κινητός. Τα cluster heads επικοινωνούν με το sink node και τους κόμβους που βρίσκονται στο cluster τους. Το sink node επικοινωνεί με τα cluster heads

και με όλους τους κόμβους του δικτύου. Οι αισθητήρες ενός cluster επικοινωνούν μόνο με το cluster head τους. Η επικοινωνία είναι unreliable αφού δεν στέλνονται acknowledgments. Το σύστημα είναι κλειστό κι έτσι δεν μπορούν να προστεθούν σε αυτό δυναμικά νέοι κόμβοι.

Τα πακέτα δρομολογούνται με βάση την τοποθεσία τον κόμβων στο δίκτυο και υπάρχει η προϋπόθεση για εμπιστοσύνη του sink node. Τα κλειδιά που θα χρησιμοποιούν οι κόμβοι για την κωδικοποίηση των πακέτων καθορίζονται πριν την εισαγωγή στους στο δίκτυο και το sink node έχει την λίστα με τα κλειδιά αυτά. Επίσης για την κωδικοποίηση των πακέτων χρησιμοποιείται ακόμα ένα κλειδί, το session key, το οποίο αλλάζει περιοδικά. Για τον λόγω αυτό μπορούμε να θεωρήσουμε πως τα κλειδιά καθορίζονται και δυναμικά. Με τον τρόπο αυτό προσπαθούν να παρεμποδίσουν επιθέσεις εχθρικών κόμβων. Χρησιμοποιείται η μέθοδος του συμμετρικού κλειδιού για την κωδικοποίηση των μηνυμάτων.

Το πρωτόκολλο αυτό μπορεί να χρησιμοποιηθεί τόσο σε εφαρμογές για μέτρηση διάφορων περιβαλλοντικών παραμέτρων όσο και σε εφαρμογές που ελέγχουν διάφορες παραμέτρους στον τομέα της υγείας ή παρατηρούν τις συνθήκες που επικρατούν σε ένα πεδίο μάχης.

Για την κρυπτογράφηση των πακέτων χρησιμοποιείται ένα συμμετρικό κλειδί, το hash function και το MAC για τον έλεγχο της αυθεντικότητας του πακέτου. Όλες οι προϋποθέσεις για την ύπαρξη ασφάλειας, όπως αυτές περιγράφονται στην ενότητα 2.3, εφαρμόζονται στο Secure SPIN.

Με τη χρήση του session key το οποίο αλλάζει περιοδικά δίνεται και μια χρονική σειρά στα πακέτα και μπορεί να καθοριστεί κατά πόσο ένα πακέτο μπορεί να θεωρηθεί ως φρέσκο ή όχι. Υπάρχει δηλαδή ένας έλεγχος για το freshness κάθε πακέτου.

Οι επιθέσεις sybil και sinkhole δεν μπορούν να εφαρμοστούν στο δίκτυο που χρησιμοποιεί το Secure SPIN επειδή το πρωτόκολλο δεν βασίζεται στη γεωγραφική θέση των κόμβων και για την επιλογή των κόμβων που θα οριστούν ως cluster heads δεν χρησιμοποιούνται τα χαρακτηριστικά των κόμβων. Ούτε και η επίθεση wormhole μπορεί να εφαρμοστεί επειδή τα πακέτα που στέλνουν οι κόμβοι στέλνονται απευθείας μέσω του cluster head. Άρα για να εφαρμοστεί η επίθεση αυτή θα πρέπει το cluster head και το base station να συνωμοτήσουν και να γίνουν οι δύο attackers, πράγμα όμως που δεν μπορεί να εφαρμοστεί αφού υπάρχει η προϋπόθεση ότι το base station είναι trusted. Η επίθεση selective forward μπορεί να εφαρμοστεί όταν ένας cluster head γίνει compromised. Αυτό συμβαίνει επειδή η μεταφορά των πακέτων γίνονται μέσω των cluster heads. Δεν δίνονται αρκετές πληροφορίες για τον τρόπο λειτουργίας του πρωτοκόλλου έτσι δεν μπορεί να κριθεί κατά πόσο αντιμετωπίζεται ή όχι η επίθεση αυτή. Τέλος, για τις επιθέσεις hello και denial of service δεν δίνονται αρκετές πληροφορίες για το πως οργανώνεται το δίκτυο κι έτσι δεν μπορούμε να αποφασίσουμε κατά πόσο οι επιθέσεις αυτές αντιμετωπίζονται ή όχι. Στο συγκεκριμένο άρθρο [16] δεν υπάρχει κάποια βαθιά ανάλυση του πρωτοκόλλου. Αντίθετα, δίνεται μια απλή λεκτική περιγραφή.

4.7 SHEER

Το SHEER [17] – Secure Hierarchical Energy Efficient Routing Protocol, στοχεύει στη δημιουργία ενός ενεργειακά αποδοτικού πρωτοκόλλου ασφαλείας.

Το δίκτυο που δημιουργείται έχει τρία επίπεδα ιεραρχίας, το base station, το cluster head 1 και το cluster head 2. Οι κόμβοι στο δίκτυο είναι στατικοί και επικοινωνούν μόνο με το cluster head τους. Με τη σειρά τους τα cluster heads επικοινωνούν με τους κόμβους που ανήκουν στο cluster τους, με τα άλλα cluster heads του επιπέδου 2 και τα cluster head του επιπέδου 2 επικοινωνούν με το base station. Η επικοινωνία είναι unreliable και το σύστημα είναι κλειστό – δεν μπορούν να προστεθούν δυναμικά νέοι κόμβοι.

Τα χαρακτηριστικά των αισθητήρων που λήφθηκαν υπόψη κατά το σχεδιασμό του πρωτοκόλλου είναι αυτά του MICA2:

Processing Capabilities:

- ATmega128L 8-bit processor at 8 MHz

Radio Communication:

- 433, 868/916, or 310 MHz Multi-Channel Radio Transceiver
- 38.4 Kpbs radio

Operating System:

- TinyOS

Η αρχιτεκτονική λοιπόν το δικτύου είναι ιεραρχική και για την δρομολόγηση των πακέτων λαμβάνεται υπόψη η τοποθεσία των κόμβων. Τα κλειδιά δίνονται στους αισθητήρες πριν την τοποθέτησή τους στο δίκτυο. Για την λειτουργία του SHEER είναι αναγκαία τα ακόλουθα κλειδιά:

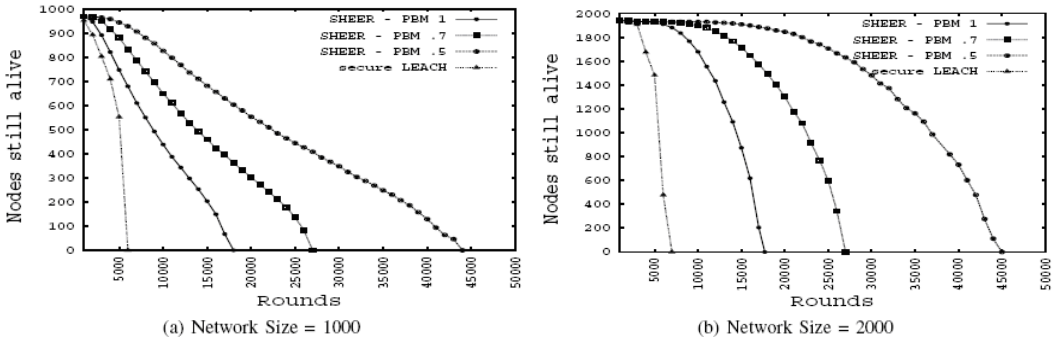
- Node key: το κλειδί που παράγει ο κόμβος για την κωδικοποίηση του πακέτου που θα αποστείλει.
- Symmetric Key:
    - Session Key: μυστικό κλειδί το οποίο μοιράζεται ένας κόμβος με ένα γείτονά του
    - Primary key: κλειδί που μοιράζεται ένας κόμβος με το base station
- Cluster key: κλειδί το οποίο το μοιράζεται ο κάθε κόμβος με τον cluster head του
- Backup cluster key: μοναδικό κλειδί για κάθε κόμβο το οποίο το μοιράζεται με τον εφεδρικό cluster head
- Group keying: κοινό κλειδί για τους κόμβους που ανήκουν στο ίδιο cluster
- Master key: χρησιμοποιείται για να δημιουργήσει νέα κλειδιά

Το πρωτόκολλο αυτό μπορεί να χρησιμοποιηθεί τόσο σε εφαρμογές για μέτρηση διάφορων περιβαλλοντικών παραμέτρων όσο και σε εφαρμογές που ελέγχουν

διάφορες παραμέτρους στον τομέα της υγείας ή παρατηρούν τις συνθήκες που επικρατούν σε ένα πεδίο μάχης.

Για την κρυπτογράφηση των πακέτων χρησιμοποιείται η μέθοδος του συμμετρικού κλειδιού και μια παραλλαγή του MAC για έλεγχο της αυθεντικότητας ενός πακέτου. Με τον τρόπο αυτό προσπαθεί να μειώσει τις επιθέσεις που μπορούν να εμφανιστούν στο δίκτυο. Επίσης όλα όσα απαιτούνται για την ύπαρξη ασφάλειας εφαρμόζονται – ενότητα 2.3. Η δρομολόγηση των πακέτων γίνεται μέσω του cluster head. Το cluster head αλλάζει όταν η ενέργεια που του απομένει γίνει μικρότερη από μια προκαθορισμένη τιμή. Σε τέτοια περίπτωση επιλέγετε ένα νέο cluster head κι έτσι αλλάζει η τοπολογία του δικτύου αλλά και ο κόμβος μέσω του οποίου θα στέλνονται από το συγκεκριμένο cluster τα πακέτα. Αλλάζει δηλαδή και η διαδικασία δρομολόγηση κάτω από συγκεκριμένες συνθήκες – proactive.

Στο σχήμα 4.1 φαίνεται η διάρκεια ζωής του δικτύου συγκριτικά με τη διάρκεια ζωής που έχει ένα δίκτυο όταν χρησιμοποιεί το πρωτόκολλο LEACH. Τα αποτελέσματα αυτά πάρθηκαν από την προσομοίωση του πρωτοκόλλου. Στην (a) γραφική συνάρτηση του σχήματος 4.1 το δίκτυο αποτελείται από 1000 κόμβους ενώ στη γραφική συνάρτηση (b) αποτελείται από 2000. Για το πρωτόκολλο SHEER έχουμε τρεις γραφικές: για probabilistic broadcast mechanism (PBM) 0.5, 0.7 και 1. Η τιμή του PBM καθορίζει τον ρυθμό με τον οποίο στέλνουν μηνύματα οι κόμβοι. Η μεγαλύτερη τιμή που μπορεί να πάρει το PBM είναι 1 και οι κόμβοι στέλνουν συνεχώς πακέτα. Ακόμα και στην περίπτωση αυτή η διάρκεια ζωής του δικτύου είναι μεγαλύτερη από τη διάρκεια ζωής ενός αντίστοιχου δικτύου που χρησιμοποιεί το πρωτόκολλο LEACH. Όπως φαίνεται μέσα από τα αποτελέσματα της προσομοίωσης η συνολική διάρκεια ζωής του δικτύου που χρησιμοποιεί το SHEER πρωτόκολλο είναι σχεδόν τριπλάσια για PBM 0.5, σχεδόν πενταπλάσια για PBM 0.7 και εννεαπλάσια για PBM 1. Μια ενδιαφέρον παρατήρηση είναι ότι με 2000 κόμβους στο δίκτυο η διάρκεια ζωής του δικτύου μειώνεται με πιο αργό τρόπο, πιο ομαλό.



Σχήμα 4.1 Διάρκεια Ζωής Δικτύου [17]

Το πρωτόκολλο αντιμετωπίζει την επίθεση hello και denial of service. Όσων αφορά την επίθεση selective forward δεν έχουμε αρκετές πληροφορίες για να καταλήξουμε σε μια απόφαση – κατά πόσο αντιμετωπίζεται ή όχι. Το sybil attack δεν μπορεί να εφαρμοστεί επειδή για τη δημιουργία του δικτύου και την οργάνωσή του δεν λαμβάνεται υπόψη η τοποθεσία των κόμβων. Ούτε και η επίθεση sinkhole μπορεί να εφαρμοστεί επειδή τα cluster heads δεν επιλέγονται με βάση τα χαρακτηριστικά τους αλλά με βάση ένα τυχαίο αριθμό. Αν ο αριθμός που παράγεται είναι μικρότερος από το 1/πυκνότητα cluster τότε γίνεται cluster head. Η επίθεση wormhole δεν μπορεί να εφαρμοστεί επειδή η δρομολόγηση των πακέτων γίνεται μέσω των cluster heads και δεν επηρεάζεται από την γρήγορη επικοινωνία που μπορεί να έχουν μεταξύ τους δύο clusters. Για την ανάλυση του SHEER χρησιμοποιήθηκε προσομοιωτής. Όπως είδη αναφέρθηκε μελετήθηκε η διάρκεια ζωής του δικτύου σε σχέση με το πρωτόκολλο LEACH, αναλύθηκε η αποδοτικότητα της οργάνωσης των κόμβων σε clusters σε σχέση με την διαχείριση της ενέργειας και η επίδραση του μεγέθους του δικτύου με την κατανάλωση ενέργειας.

4.8 OPSENET

Το OPSENET [18] – Security Enabled Routing Scheme for a System of Optical Sensor Networks, διαφέρει από τα πρωτόκολλα που μελετήσαμε μέχρι στιγμής επειδή έχει σχεδιαστεί ιδικά για δίκτυα αισθητήρων που επικοινωνούν με κατευθυνόμενα οπτικά μονοπάτια – directional optical links.

Το δίκτυο είναι οργανωμένο σε clusters – ιεραρχικό, και οι κόμβοι είναι στατικοί. Επικοινωνούν με το cluster head τους και αυτό με τη σειρά του επικοινωνεί με το base station και με τα cluster nodes του. Η επικοινωνία είναι reliable επειδή στέλνονται acknowledgments για τα μηνύματα που ανταλλάζονται. Το δίκτυο που δημιουργείται είναι κλειστό, δηλαδή μετά την δημιουργία του δεν μπορούν να προστεθούν δυναμικά νέοι κόμβοι.

Τα cluster heads επιλέγονται με βάση το αν είναι ευθυγραμμισμένος ο μηχανισμός αποστολής των μηνυμάτων τους με τον αντίστοιχο μηχανισμό του base station – στηρίζονται δηλαδή στην τοποθεσία των κόμβων, location based. Για το base station υπάρχει η υπόθεση ότι είναι έμπιστος. Λόγω της πιο πάνω ανάγκης για ευθυγράμμιση των μηχανισμών αποστολής μηνυμάτων υπάρχουν δυσκολίες στην εφαρμογή επιθέσεων.

Τα κλειδιά που θα χρησιμοποιούν οι κόμβοι για την κωδικοποίηση των πακέτων που θα στείλουν τοποθετούνται στους κόμβους πριν την τοποθέτησή τους στο δίκτυο – pre-deployment. Χρησιμοποιείται ένα συμμετρικό κλειδί για την κωδικοποίηση/ αποκωδικοποίηση ενός πακέτου. Για την επικοινωνία των κόμβων μεταξύ ενός cluster χρησιμοποιείται το group key.

Το πρωτόκολλο αυτό μπορεί να εφαρμοστεί σε εφαρμογές που μετρούν παραμέτρους για το περιβάλλον ή για εφαρμογές που σχετίζονται με την υγεία. Μπορούν να εφαρμοστούν σε τέτοιες εφαρμογές επειδή τα άτομα που θα τοποθετήσουν τους αισθητήρες μπορούν να ασχοληθούν με την ευθυγράμμισή τους ούτως ώστε να είναι δυνατή η επικοινωνία μεταξύ τους.

Για την κρυπτογράφηση των πακέτων που ανταλλάζονται χρησιμοποιείται το συμμετρικό κλειδί σε συνδυασμό με ένα hash function. Επίσης χρησιμοποιείται το MAC για έλεγχο της αυθεντικότητας του κάθε πακέτου. Όλες οι προϋποθέσεις για την ύπαρξη ασφάλειας εφαρμόζονται στο OPSENET και δεν υπάρχουν ανάγκες για συγχρονισμό των κόμβων. Υπάρχει επίσης δυνατότητα για multipath

routing επειδή ένας αισθητήρας μπορεί να ανήκει ταυτόχρονα σε περισσότερα από ένα clusters. Τα cluster heads αλλάζουν περιοδικά κι έτσι αλλάζει και η τοπολογία του δικτύου – proactive.

Τα attacks που μελετούμε αντιμετωπίζονται από το πρωτόκολλο αυτό. Η μόνη επίθεση που δεν μπορεί να εφαρμοστεί στο δίκτυο αυτό είναι το Hello attack. Η ανάλυση των πρωτοκόλλων έγινε με προσομοίωση του αλλά και με την υλοποίηση του. Αναλύεται το byre overhead και το κόστος για τη συντήρηση του δικτύου.

Τα πρωτόκολλα που αναλύονται στο κεφάλαιο 4 συνοψίζονται στον πίνακα που ακολουθεί. Για την κατανόηση του πίνακα πρέπει να έχουμε υπόψη κάποιες ενδείξεις που υπάρχουν σε αυτόν.

Το ø εμφανίζεται σε πεδία για τα οποία δεν δίνονται αρκετές πληροφορίες για το αντίστοιχο πρωτόκολλο. Αντιθέτως το – εμφανίζεται σε πεδία που δεν εφαρμόζονται για ένα πρωτόκολλο. Για παράδειγμα, αν ένα πρωτόκολλο αναλύθηκε με τη χρήση προσομοιωτή τότε στον πίνακα με τα χαρακτηριστικά των κόμβων στους οποίους εφαρμόστηκε το πρωτόκολλο θα έχει –.

Το σύμβολο √ τοποθετείται σε πεδία στα οποία ισχύει η αντίστοιχη τιμή στο συγκεκριμένο πρωτόκολλο και επιβεβαιώνεται από τους συγγραφείς του αντίστοιχου άρθρου. Μερικά από τα χαρακτηριστικά των κόμβων χωρίζονται σε δύο ή περισσότερες πιθανές επιλογές, παραδείγματος χάριν η αρχιτεκτονική του δικτύου η οποία μπορεί να είναι ή ιεραρχική ή flat. Στην περίπτωση αυτή το σύμβολο √ θα τοποθετηθεί στο πεδίο που ισχύει. Αν το πεδίο είναι κενό τότε δεν ισχύει η αναφορά για το πρωτόκολλο.

Το σύμβολο √ø εμφανίζεται σε πεδία στα οποία οι συγγραφείς αναφέρουν ότι ισχύουν για το αντίστοιχο πρωτόκολλο αλλά δεν δίνουν αρκετές λεπτομέρειες για το πως υλοποιείται – κάνοντας αδύνατη μια περαιτέρω ανάλυση και σχολιασμό.

Το σύμβολο √* εμφανίζεται σε πεδία στα οποία αναφέρονται έμμεσα στο αντίστοιχο άρθρο και επιβεβαιώνεται ότι ισχύουν. Το σύμβολο * εμφανίζεται σε πεδία στα οποία ισχύουν κι έγινε κάποια ανάλυση ή εκτέλεση σεναρίων για να αποφασιστεί αυτό.

Τέλος, στον πίνακα εμφανίζονται και τιμές οι οποίες μας παραπέμπουν σε αντίστοιχη τιμή στο τέλος του πίνακα. Η τεχνική αυτή χρησιμοποιήθηκε για να είναι πιο εύκολη η παρουσίαση μεγάλου όγκου δεδομένων.

Environmental Assumptions – Network Assumptions		CBSRP	SecRout	A clean state approach	SPINS	Secure SPIN	SHEER	OPSENET
Architecture	Flat				√*			
	Hierarchical	√*	√*	√		√*	√	√
Network Dynamics	Static nodes	√*	√*	√*	√*	√*	√*	√*
	Mobility of nodes							
Communication mode	Node to node			√				
	Node to base station/ cluster head	√	√		√	√	√	√
Communication characteristics	Reliable		√*	√				√
	Unreliable	√*			√*	√*	√*	
Close vs. Open System	open			√	√			
	close	√*	√*			√*	√*	√*

Πίνακας 4.1 Environmental Assumptions – Network Assumptions

Environmental Assumptions – Node Characteristics	CBSRP	SecRout	A clean state approach	SPINS	Secure SPIN	SHEER	OPSENET
Processing Capabilities	CBSPR[1]	–	–	SPINS[1]	ø	SHEER[1]	ø
Battery Lifetime	2AA Batteries – roughly 1 year	–	–	ø	ø	ø	ø
Cost	ø	–	–	ø	ø	ø	ø
Radio Communication	CBSPR[2]	–	–	SPINS[2]	ø	SHEER[2]	Laser
Operating System	TinyOS	–	–	TinyOS	ø	TinyOS	ø

Πίνακας 4.2 Environmental Assumptions – Node Characteristics

CBSPR[1]: Επεξεργαστής Atmel Atmega 128L, 4 MHz, 128Kbytes flash memory, 4 Mbit serial flash, 4Kbytes SRAM και 4Kbyte EEPROM.
CBSPR[2]: 916 ή 433 MHz radio
SPINS[1]: Επεξεργαστής 8-bit, 4 MHz, 512 bytes RAM, 512 bytes EEPROM, 8 Kbytes instruction flash, code space 4500 bytes

SPINS[2]: 916 MHz radio, Bandwidth 10 Kbps
SHEER[1]: Επεξεργαστής ATmega128L 8-bit, 8 MHz
SHEER[2]: 433, 868/916 ή 310 MHz Multi-Channel Radio Transceiver, 38.4 Kpbs radio

Environmental Assumptions – Architecture for Routing Protocol		**CBSRP**	**SecRout**	**A clean state approach**	**SPINS**	**Secure SPIN**	**SHEER**	**OPSENET**
Dominated by Architecture	Flat				√*			
	Hierarchical	√*	√*	√		√*	√	√
Routing Based	Location Based	√*	√*	√*	√*	√*	√*	√*
	Trust Based							

Πίνακας 4.3 Environmental Assumptions – Architecture for Routing Protocol

Environmental Assumptions – Security Assumptions		**CBSRP**	**SecRout**	**A clean state approach**	**SPINS**	**Secure SPIN**	**SHEER**	**OPSENET**
Trust Requirements	Trusted Base Station	Ø	√	√	√	√	Ø	√
	Trust itself	Ø			√		Ø	
	Trusted Sensor Nodes	Ø					Ø	
	Trusted Hardware	Ø		√			Ø	
Key Management	Pre-deployment		√	√	√	√	√	√
	Dynamic Deployment	√				√		
	Cluster Key		√				√	
	Backup Cluster Key						√	
	Node Key						√	
	Master Key						√	
	Global Key							
	Symmetric Key	√	√		√	√	√	√
	Asymmetric Key			√				
	Random Keying	√						
	Group Keying						√	√

Πίνακας 4.4 Environmental Assumptions – Security Assumptions

Environmental Assumptions – Architecture for Routing Protocol	CBSRP	SecRout	A clean state approach	SPINS	Secure SPIN	SHEER	OPSENET
Military			√*		√*	√*	
Health Care		√*	√*	√*	√*	√*	√*
Environmental	√*	√*	√*	√*	√*	√*	√*

Πίνακας 4.5 Environmental Assumptions – Architecture for Routing Protocol

Security – Operational Objectives	CBSRP	SecRout	A clean state approach	SPINS	Secure SPIN	SHEER	OPSENET
Prevention	√		√	√	√	√	√
Detection/ Recovery	Ø	√	√			Ø	√
Resilience	Ø	√*	√	√*		Ø	Ø

Πίνακας 4.6 Security – Operational Objectives

Security– Methods Used/ Provided		CBSRP	SecRout	A clean state approach	SPINS	Secure SPIN	SHEER	OPSENET
Cryptographic	Symmetric	√	√		√	√	√	√
	Asymmetric			√				
	Hash			√ - chain		√ - function		√ - function
	MAC		√		√	√	√	√
Intrusion Detection/ Behavior Evaluation	Black List	Ø	√	√		Ø	Ø	Ø
	Watchdog	Ø			√	Ø	Ø	Ø

Πίνακας 4.7 Security– Methods Used/ Provided

Security – Security Properties Provided	CBSRP	SecRout	A clean state approach	SPINS	Secure SPIN	SHEER	OPSENET
Integrity of Data	√	√	√	√	√	√	√
Confidentiality	√	√	√	√	√	√	√
Availability/ Robustness	√	√	√	√	√	√	√
Non Repudiation	√	√	√	√	√	√	√
Integrity of Origin/ Destination	√	√	√	√	√	√	√

Πίνακας 4.8 Security – Security Properties Provided

Functionality Provided – Network Lifetime	CBSRP	SecRout	A clean state approach	SPINS	Secure SPIN	SHEER	OPSENET
Network Lifetime	Ø	Ø	Ø	Ø	Ø	SHEER[3]	Ø

Πίνακας 4. 9 Functionality Provided – Network Lifetime

SHEER[3]: Όπως περιγράφεται στην ενότητα 4.7, η διάρκεια ζωής ενός δικτύου που χρησιμοποιεί το πρωτόκολλο SHEER είναι τρεις φορές μεγαλύτερη από την διάρκεια ζωής ενός δικτύου που χρησιμοποιεί το πρωτόκολλο LEACH.

Functionality Provided – Synchronization	CBSRP	SecRout	A clean state approach	SPINS	Secure SPIN	SHEER	OPSENET
Synchronization	Ø	Ø		SPINS[3]	Secure SPIN[1]	Ø	

Πίνακας 4.10 Functionality Provided – Synchronization

SPINS[3]: Weak και Strong Freshness.
Secure SPIN[1]: Υπάρχει έλεγχος “φρεσκάδας” των πακέτων με τη χρήση του session key, ενότητα 4.6.

Functionality Provided – Proactive vs. Reactive Nature		CBSRP	SecRout	A clean state approach	SPINS	Secure SPIN	SHEER	OPSENET
Proactive vs. Reactive Nature	Proactive	√*		√*	√*	–	√*	√*
	Reactive		√*			–		

Πίνακας 4.11 Functionality Provided – Proactive vs. Reactive Nature

Functionality Provided – Multipath Routing	CBSRP	SecRout	A clean state approach	SPINS	Secure SPIN	SHEER	OPSENET
Multipath Routing	–		√	–	–	Ø	√

Πίνακας 4.12 Functionality Provided – Multipath Routing

Performance – Defense/ Attacks Addressed	CBSRP	SecRout	A clean state approach	SPINS	Secure SPIN	SHEER	OPSENET
Wormhole	√*	*	√	–	–	–	√
Sinkhole	√Ø	–	√	–	–	–	√
Sybil	–	√*	√	–	–	–	√
Hello	–	Ø	√	√	Ø	√	–
Denial of Service	*	*	*	Ø	Ø	*	*
Selective Forwarding	√Ø	√*	√*	–	Ø	Ø	√

Πίνακας 4.13 Performance – Defense/ Attacks Addressed

Performance – Energy Usage	CBSRP	SecRout	A clean state approach	SPINS	Secure SPIN	SHEER	OPSENET
Computation Complexity	ø	ø	ø	ø	ø	ø	ø
Number of Transactions	ø	ø	CleanState[1]	ø	ø	ø	ø
Overhead per Message	CBSPR[3]	SecRout[1]	CleanState[2]	ø	ø	ø	ø

Πίνακας 4.14 Performance – Energy Usage

CBSPR[3]: Σε κάθε πακέτο που στέλνεται είναι απαραίτητη η αποστολή των παράμερων που θα χρησιμοποιηθούν για την παραγωγή του κλειδιού που θα αποκωδικοποιήσει το μήνυμα. Για του σκοπό αυτό χρησιμοποιούνται 8 bytes.
SecRout[1]: Συγκριτικά με το πρωτόκολλο AODV - Ad hoc on Demand Distance Vector Routing, έχει περίπου 6% περισσότερο byte overhead.
CleanState[1]: Σε ένα δίκτυο με 16 κόμβους στέλνονται κατά μέσω όρο 101 μηνύματα από τον κάθε κόμβο.
CleanState[2]: Ο κώδικας που αναπτύχθηκε για το πρωτόκολλο αυτό έχει μέγεθος 21 KB.

Performance – Analysis	CBSRP	SecRout	A clean state approach	SPINS	Secure SPIN	SHEER	OPSENET
Implementation	√			√			√
Simulation		√	√			√	√
Mathematical Analysis							

Πίνακας 4.15 Performance – Analysis

Κεφάλαιο 5

Ανάλυση Μεθόδων Αντιμετώπισης των Επιθέσεων

5.1 Στόχος Κεφαλαίου

Στο κεφάλαιο αυτό θα αναλύσουμε τις μεθόδους που χρησιμοποιήθηκαν στα πρωτόκολλα που μελετήσαμε για την αντιμετώπιση των επιθέσεων:

- Wormhole Attack
- Sinkhole Attack
- Sybil Attack
- Hello Attack
- Denial of Service
- Selective Forwarding.

Οι τεχνικές αυτές μπορεί να είναι κοινές ή να έχουν μικρές τροποποιήσεις ή μπορεί να είναι εντελώς διαφορετικές.

5.2 Wormhole Attack

Στην επίθεση wormhole, δύο απομακρυσμένοι attackers δημιουργούν ένα δικό τους αποκλειστικό κανάλι επικοινωνίας μέσω του οποίου μεταφέρουν διάφορα δεδομένα και πληροφορίες που παίρνουν από τους άλλους κόμβους, ενότητα 2.6.1.4. Στόχος τους είναι η ανάγνωση των δεδομένων που αποστέλλουν οι κόμβοι. Το κανάλι που δημιουργούν μεταξύ τους οι κόμβοι μπορεί να κεντρίσει το ενδιαφέρον των άλλων κόμβων και να στέλνουν τα πακέτα τους μέσω αυτού, έχοντας την εντύπωση ότι τα πακέτα μεταφέρονται πολύ γρήγορα στον προορισμό τους.

Η επίθεση wormhole μπορεί να εφαρμοστεί στο πρωτόκολλο CBSRP [12] νοούμενου ότι εφαρμόζεται από το cluster head, αφού όλες οι πληροφορίες μεταφέρονται μέσω αυτού. Με βάση το πρωτόκολλο αυτό, τα cluster heads που επιλέγονται διαγράφουν από τη μνήμη τους το κλειδί τους και την συνάρτηση που παράγει κλειδιά και ως επακόλουθο δεν μπορούν να αποκρυπτογραφήσουν τα πακέτα που παίρνουν. Έτσι η μόνη τους επιλογή είναι να τα προωθήσουν στον προορισμό τους.

Στο SecRout [13] η επίθεση αυτή μπορεί να εφαρμοστεί μεταξύ δύο κόμβων που συμμετέχουν στο ίδιο μονοπάτι δρομολόγησης ενός πακέτου. Η ροή των πακέτων στα οποία θα έχουν πρόσβαση δεν αλλάζει – είτε εφάρμοζαν την επίθεση αυτή είτε όχι ο αριθμός των πακέτων που θα προωθούσαν είναι ο ίδιος. Ακόμα, οι κόμβοι που θα χρησιμοποιηθούν για ένα μονοπάτι δεν επιλέγονται με βάση τα χαρακτηριστικά τους αλλά με βάση την γρηγορότερη ολοκλήρωση της διαδικασίας μέχρι το base station. Η επίθεση αυτή αντιμετωπίζεται αφού οι κακόβουλοι κόμβοι δεν θα μπορέσουν να αποκρυπτογραφήσουν το μήνυμα, αφού το κλειδί δεν το γνωρίζουν και δεν μπορούν να το υποκλέψουν, αφού δεν ανταλλάζεται μεταξύ των κόμβων.

Στο Secure Sensor Network Routing: A Clean-State Approach [14] αν και δεν εφαρμόζεται κάποια μέθοδος εντοπισμού του συγκεκριμένου attack – στο αντίστοιχο άρθρο αναφέρεται ότι μπορεί πολύ εύκολα να γίνει η επέκταση αυτή, το δίκτυο μπορεί να λειτουργήσει ακόμα και μετά την επίθεσή του. Αυτό συμβαίνει επειδή οι κόμβοι έχουν την δυνατότητα επιλογής του μονοπατιού μέσω του οποίου θα γίνει η δρομολόγηση των πακέτων. Έτσι, η δρομολόγηση των πακέτων μπορεί να ακολουθήσει διαφορετικά μονοπάτια και σε τελική ανάλυση να αποφευχθεί η μόνιμη χρήση ενός σταθερού μονοπατιού που ίσως περιλαμβάνει και εχθρικούς κόμβους.

Τέλος, το πρωτόκολλο OPSENET [18] με τον τρόπο λειτουργίας του κάνει αδύνατη την εφαρμογή του συγκριμένου attack. Κατά την επίθεση αυτή δύο κόμβοι ανταλλάζουν μεταξύ τους πακέτα τα οποία δρομολογούν άλλοι κόμβοι. Τα κανάλια επικοινωνίας όμως στο πρωτόκολλο αυτό είναι κατευθυνόμενα – μονής κατεύθυνσης, τα πακέτα στέλνονται μόνο από την μια πλευρά στην άλλη όχι και αντίθετα. Επίσης αν ο attacker θέλει να συνδυάσει την επίθεση αυτή με κάποια άλλη, για παράδειγμα replay attack, δεν μπορεί να εφαρμοστεί για τον ίδιο λόγο.

Γενικότερα μπορούμε να πούμε πως η τακτική που χρησιμοποιείται από το CBSRP [12] είναι έξυπνη και λειτουργική. Αυτό όμως ισχύει μόνο σε πρωτόκολλα στα οποία τα cluster heads παραμένουν σταθερά και δεν αλλάζουν δυναμικά. Σε περίπτωση που αλλάζουν δυναμικά μπορεί να χρησιμοποιηθεί η τεχνική που ακολουθείται από το Secure Sensor Network Routing: A Clean-State Approach [14], όπου οι κόμβοι μπορούν αν επιλέξουν δυναμικά το μονοπάτι μέσω του οποίου θα δρομολογηθεί ένα πακέτο. Έτσι, το κανάλι επικοινωνίας που χρησιμοποιούν οι δύο attackers κατά την επίθεση wormhole δεν θα χρησιμοποιείται πάντοτε. Η μεθοδολογία που χρησιμοποιείται στο OPSENET [18] βασίζεται στην ύπαρξη κατευθυνόμενων μονοπατιών για την αποστολή των μηνυμάτων, κάτι που δεν ισχύει για τα κοινά δίκτυα αισθητήρων που επικοινωνούν με τη χρήση ραδιοσυχνοτήτων.

5.3 Sinkhole Attack

Ο attacker κατά την επίθεση αυτή παρουσιάζει τον εαυτό του με πολλά προτερήματα, όπως υψηλή ποιότητα δρομολόγησης και μεγάλα ποσά ενέργειας, με στόχο να δελεάσει τους άλλους κόμβους του δικτύου και να τον χρησιμοποιούν για τη μεταφορά των πακέτων, ενότητα 2.6.1.7. Έτσι, ο εχθρικός κόμβος προωθεί όποια πακέτα επιθυμεί, δεν τα απορρίπτει όλα εξορισμού, και έχει την επιλογή να τα αλλοιώσει.

Η επίθεση αυτή με βάση τον ορισμό της μπορεί να εφαρμοστεί στο πρωτόκολλο CBSRP [12] αφού τα cluster heads επιλέγονται με βάση τα αποθέματα ενέργειας που έχουν. Με βάση τους συγγραφείς του αντίστοιχου άρθρου, η επίθεση αυτή αντιμετωπίζεται από το CBSRP. Ταυτόχρονο όμως δεν μας δίνουν αρκετές πληροφορίες για το πως γίνεται εφικτή η αντιμετώπιση της επίθεσης αυτής. Για τον λόγω αυτό δεν μπορούμε να συνεχίσουμε με μια πιο αναλυτική αναφορά στη μεθοδολογία που ακολουθήθηκε στο πρωτόκολλο αυτό.

Με τον ίδιο τρόπο η επίθεση αυτή μπορεί να εφαρμοστεί και στο Secure Sensor Network Routing: A Clean-State Approach [14]. Στο πρωτόκολλο αυτό οι κόμβοι οργανώνονται σε groups ακολουθώντας ένα επαναληπτικό αλγόριθμο με τον οποίο μάλιστα καθορίζεται και δυναμικά η διεύθυνσή τους στο δίκτυο. Οι κόμβοι αρχικά στέλνουν μεταξύ τους μηνύματα για να εντοπίσουν τους γειτονικούς τους κόμβους. Ακολούθως, στέλνουν στον κοντινότερό τους γείτονα μήνυμα με στόχο να δημιουργήσουν ένα δικό τους group – να συγχωνευτούν. Κατά τη διαδικασία προώθησης των πακέτων υπάρχει και η επιλογή δρομολόγησής τους μέσω των πιο κοντινών κόμβων. Γενικά λοιπόν δίνεται “προτεραιότητα” στους κοντινούς κόμβους κι έτσι αν ένας attacker διαφημίζει μια μικρή απόσταση από ένα κόμβο θα προτιμηθεί για τη δρομολόγηση των πακέτων. Όταν όμως ο κόμβος αυτός αρχίσει να μην προωθεί τα πακέτα τότε θα οδηγήσει τους κόμβους στη χρήση ενός άλλου μονοπατιού. Όπως αναφέρθηκε και στο κεφάλαιο 4 – ενότητα 4.4, στο πρωτόκολλο αυτό υποστηρίζεται multipath routing και η επικοινωνία είναι

reliable. Έτσι αν ένας κόμβος στείλει ένα πακέτο στο base station και δεν πάρει πίσω acknowledgment τότε προφανώς το μήνυμα δεν στάλθηκε. Ο κόμβος τότε με τη σειρά του στέλνει ξανά το πακέτο ακολουθώντας άλλη διαδρομή. Η αποστολή όμως του ίδιου πακέτου για δεύτερη φορά οδηγεί στην σπατάλη πόρων του δικτύου.

Στο OPSENET [18] οι κόμβοι μπαίνουν σε clusters λαμβάνοντας υπόψη την απόσταση που έχει το cluster head από το base station. Προσπαθούν να μπουν σε ένα cluster μέσω του οποίου θα προωθούνται όσο το δυνατό ποιο γρήγορα τα πακέτα τους προς το bases station ή θα λαμβάνουν τα πακέτα που θα στέλνει το base station γρήγορα. Με τον τρόπο αυτό ένας attacker μπορεί να εφαρμόσει την επίθεση sinkhole. Τα cluster heads όμως αλλάζουν περιοδικά. Η αλλαγή είναι απαραίτητη με την μετακίνηση του base station. Με τον τρόπο αυτό οι αποστάσεις μεταξύ των κόμβων και του base station αλλάζουν και οι πιθανότητες να επιλεγεί για πολλοστή φορά ένας κόμβος ως cluster head μειώνονται.

Η τακτική που χρησιμοποιείται από το πρωτόκολλο OPSENET [18] είναι όχι μόνο η πιο απλή αλλά μπορεί να εφαρμοστεί και στα περισσότερα δίκτυα – αφού τα περισσότερα πρωτόκολλα απαιτούν την οργάνωση του δικτύου σε clusters. Με την περιοδική αλλαγή των cluster heads εμποδίζεις ένα attacker από το να επιλέγεται συνεχώς ως σύνδεσμος επικοινωνίας με το υπόλοιπο δίκτυο.

5.4 Sybil Attack

Κατά το Sybil attack – ενότητα 2.6.1.2, ο attacker παρουσιάζεται στους άλλους κόμβους του δικτύου με πολλές ταυτότητες και σε διαφορετική τοποθεσία.

Στο SecRout [13] αν κάποιος κόμβος εμφανίζεται με πολλές ταυτότητες δεν θα το επηρεάσει. Παρόλα αυτά ακόμα και αν μια ταυτότητα του εχθρικού κόμβου καταφέρει να μπει σε μονοπάτι δρομολόγησης, αν ο attacker δεν συμπεριφερθεί σωστά – δεν προωθεί τα πακέτα, τότε θα εντοπιστεί από τους άλλους κόμβους

του δικτύου και η ταυτότητα αυτή θα μπει σε μαύρη λίστα. Το πακέτο που πρέπει να προωθηθεί θα φτάσει στον attacker επειδή τα πακέτα στέλνονται μέσω broadcast.

Μια διαφορετική τεχνική χρησιμοποιείται από το Secure Sensor Network Routing: A Clean-State Approach [14]. Στο πρωτόκολλο αυτό,οι κόμβοι έχουν ένα χρονικό περιθώριο στο οποίο κάνουν broadcast μηνύματα για να αναγγείλουν τους εαυτούς τους στο δίκτυο. Την στιγμή αυτή ένας εχθρικός κόμβος μπορεί να προβάλει διαφορετικές ταυτότητες στο δίκτυο. Δεν θα μπορέσει όμως να το καταφέρει επειδή ότι ταυτότητες και να δώσει στους ψεύτικους κόμβους που θα προσθέσει στο δίκτυο δεν θα μπορέσει να τους εφοδιάσει με τα αντίστοιχα certificates. Έτσι δεν θα γίνουν αποδεχτοί από τους άλλους κόμβους του δικτύου κατά τη διάρκεια του neighbor discovery. Ακολούθως τρέχει ο recursive grouping algorithm κατά τον οποίο οι κόμβοι του δικτύου ανακοινώνουν την ταυτότητά τους και την διεύθυνση που έχουν στο δίκτυο. Τα δεδομένα αυτά θα χρησιμοποιηθούν από τον replication detection algorithm μέσω του οποίου οι νόμιμοι κόμβοι του δικτύου θα μπορέσουν να εντοπίσουν τους κόμβους που χρησιμοποιούν πολλαπλές ταυτότητες στο δίκτυο.

Το OPSENET [18] αντιμετωπίζει την επίθεση αυτή μέσω του base station. Κατά τη διάρκεια οργάνωσης του δικτύου – base station circuit discovery algorithm, ανταλλάζονται πακέτα τα οποία περιέχουν πληροφορίες σχετικά με την τοποθεσία των κόμβων. Το base station χρησιμοποιεί τις πληροφορίες αυτές για να κατασκευάσει την τοπολογία του δικτύου. Με τον τρόπο αυτό μπορεί να εντοπίσει κόμβους οι οποίοι δεν υπάρχουν. Αν κάποιος κόμβος χρησιμοποιεί μια λανθασμένη τοποθεσία για τον εαυτό του και δεν εντοπιστεί από το base station, τότε απομονώνεται από μόνος του από το δίκτυο αφού οι κόμβοι οι οποίοι θα επικοινωνούν μεταξύ του θα στρέψουν σε λανθασμένη κατεύθυνση το μηχανισμό ανταλλαγής πληροφοριών κι έτσι δεν θα μπορεί να επικοινωνεί μαζί τους.

Η τεχνική που χρησιμοποιείται στο Secure Sensor Network Routing: A Clean-State Approach [14] ίσως είναι η πιο αποδοτική, αφού παράλληλα με την διαδικασία αναγγελίας των εαυτών τους το δίκτυο οι κόμβοι έχουν τη δυνατότητα να εντοπίσουν και τους κόμβους που χρησιμοποιούν μια ψεύτικη ταυτότητα. Αυτό επιτυγχάνεται με τη χρήση ενός certificate το οποίο δίνεται στους κόμβους πριν την εισαγωγή τους στο δίκτυο. Φυσικά και η μέθοδος που χρησιμοποιεί το πρωτόκολλο SecRout [13] είναι αρκετά αποδοτική, αφού οι κόμβοι μπορούν να εντοπίσουν τις ψεύτικες ταυτότητες του attacker και να τις καταχωρήσουν σε blacklist. Η πρώτη μέθοδος πιστεύω πως είναι πιο λειτουργική επειδή η όλη διαδικασία που ακολουθείται για την αντιμετώπιση της επίθεσης αυτής αποτελεί μέρος στοιχειώδους λειτουργίας του δικτύου – ο κάθε κόμβος πρέπει να αναγγείλει τον εαυτό του στο δίκτυο. Κατά τη δεύτερη μέθοδο, για να είναι δυνατός ο εντοπισμός των εχθρικών κόμβων ακολουθείται μια περίπλοκη διαδικασία κατά τη δημιουργία εγκαθίδρυσης του μονοπατιού δρομολόγησης. Λόγω της πολυπλοκότητας αυτής και του μεγάλου όγκου δεδομένων που χρειάζεται να κατακρατούν και να ενημερώνουν οι κόμβοι του δικτύου δεν θεωρώ την μέθοδο αυτή ως την βέλτιστη.

5.5 Hello Attack

Όπως επεξηγείται και στην ενότητα 2.6.1.3, για την λειτουργία μερικών πρωτοκόλλων είναι απαραίτητο οι αισθητήρες να στείλουν ένα hello message για να αναγγείλουν τον εαυτό τους στο δίκτυο. οι κόμβοι που θα λάβουν το hello message θεωρούν πως ο αποστολέας είναι στην ακτίνα εμβέλειάς τους και τον καταχωρούν στη λίστα με τους γείτονές τους. Κατά την επίθεση αυτή, ένας εχθρικός κόμβος στέλνει συνεχώς hello messages στους κόμβους του δικτύου με αποτέλεσμα να χρησιμοποιεί πολύτιμο bandwidth του δικτύου και να γεμίζει τους buffers των αισθητήρων. Ακόμα, με την καταχώρηση του attacker ως γειτονικού κόμβου, όταν ο αισθητήρας θελήσει να επικοινωνήσει με τους γείτονές του θα στέλνει μηνύματα και στον attacker – ο οποίος ίσως να μην είναι καν στην ακτίνα εμβέλειάς του. Με τον τρόπο αυτό όμως μειώνεται η διάρκεια ζωής του κόμβου.

Το πρωτόκολλο Secure Sensor Network Routing: A Clean State Approach [14] για την αντιμετώπιση της επίθεσης αυτής χρησιμοποιεί και την υπόθεση που έγινε ότι ο κάθε κόμβος έχει πριν την εισαγωγή του στο δίκτυο έχει μια μοναδική ταυτότητα και ένα certificate. Με βάση το πρωτόκολλο αυτό, οι κόμβοι του δικτύου έχουν ένα μικρό χρονικό περιθώριο μέσα στο οποίο ανταλλάζουν μηνύματα με τους γείτονές. Στόχος της συνομιλίας αυτής είναι η αναγνώριση των γειτονικών κόμβων και καταχώρησή τους στη λίστα με τους γειτονικούς τους κόμβους. Η διαδικασία αυτή αναφέρεται ως neighbor discovery protocol. Λόγω του περιορισμένου χρόνου που οι κόμβοι μπορούν να αναγγείλουν τον εαυτό τους μειώνεται το περιθώριο που έχει ένας attacker για να εφαρμόσει την επίθεσή του. Παράλληλα, τα μηνύματα που ανταλλάζονται κατά τη διαδικασία αυτή συμπεριλαμβάνουν την ταυτότητα του κόμβου καθώς και το αντίστοιχο certificate. Πακέτα που δεν περιέχουν αυτά τα δύο ή η ταυτότητα του κόμβου δεν αντιπροσωπεύει το certificate δεν γίνονται αποδεχτά. Έτσι ένας attacker θα δυσκολευτεί να εισβάλει στο δίκτυο. Μετά το πέρας του discovery protocol χρησιμοποιείται ένας αλγόριθμος – replication detection algorithm, ο οποίος εντοπίζει attackers που χρησιμοποιούσαν το certificate και την ταυτότητα ενός νόμιμου κόμβου. Τα στοιχεία αυτά φτάνουν στα χέρια του attacker κατά τη διάρκεια του neighbor discovery protocol από τους νόμιμους κόμβους που κάνουν broadcast τα πακέτα τους.

Μια παρόμοια τεχνική χρησιμοποιείται από το πρωτόκολλο SHEER [17]. Στο πρωτόκολλο αυτό ο κόμβος έχει τρεις ευκαιρίες για να στείλει ένα hello message και να πάρει απάντηση. Αρχικά τα μηνύματα αποστέλλονται σε ακτίνα r. Αν δεν πάρει απάντηση ο κόμβος τότε δοκιμάζει να το στείλει ακόμα μια φορά σε ακτίνα 2r. Αν πάλι δεν πάρει απάντηση στείλει το μήνυμα, με την τελευταία του επιλογή, έχοντας σαν ακτίνα 4r. Στα hello messages συμπεριλαμβάνεται η ταυτότητα του κόμβου κι ένα header το οποίο είναι κρυπτογραφημένο με το κλειδί του αντίστοιχου κόμβου. Ο γειτονικός κόμβος που θα παραλάβει το μήνυμα αυτό θα το αποκρυπτογραφήσει, θα προσθέσει τον κόμβο στον πίνακα με τους γείτονές του και θα του στείλει πίσω ένα acknowledgment για να τον καταχωρήσει κι

εκείνος με τη σειρά τους τον πίνακά του. Για την αντιμετώπιση ενός hello attack οι κόμβοι έχουν στη διάθεσή τους μια μικρή περίοδο από 2 μέχρι 10 μSeconds κατά την οποία μπορούν να στείλουν τα hello messages, όπως και στο Secure Sensor Network Routing: A Clean State Approach [14]. Αν δεν υπήρχε αυτός ο περιορισμός τότε ο εχθρικός κόμβος θα έκανε μεγάλη ζημιά στο δίκτυο. Οι αισθητήρες που θα έπαιρναν το μήνυμά του δεν θα τον καταχωρούσαν απλά στη λίστα με τους γείτονές τους αλλά επιπρόσθετα θα του έστελναν και απάντηση σπαταλώντας έτσι ποσά ενέργειας. Ως αποτέλεσμα οι κόμβοι θα εξαντλούσαν την ενέργειά τους και η διάρκεια ζωής του δικτύου θα ήταν πολύ περιορισμένη.

Στο πρωτόκολλο SPINS [15] η διαδικασία ανταλλαγής μηνυμάτων μεταξύ των κόμβων ονομάζεται route discovery. Ο τρόπος αντιμετώπισης του Hello attack είναι διαφορετικός από τον προαναφερόμενο. Στο SPINS, το base station ξεκινά την διαδικασία αυτή στέλνοντας ένα πακέτο στο οποίο περιλαμβάνεται η ώρα που έχει αυτή τη στιγμή το base station καθώς και ένα MAC μέσω του οποίου οι άλλοι κόμβοι που θα πάρουν το μήνυμα θα μπορούν να ελέγξουν την αυθεντικότητα του. Οι κόμβοι που θα πάρουν το μήνυμα θα συνεχίσουν την διαδικασία προώθησης του μηνύματος αν το μήνυμα που έλαβαν δεν ήταν τροποποιημένο και είναι το πρώτο μήνυμα που πήραν για την εποχή αυτή – το αναγνωρίζουν χρησιμοποιώντας την ώρα που περιλαμβάνεται στο πακέτο. Ο κόμβος θα καταχωρήσει τον κόμβο από τον οποίο έλαβε το μήνυμα σαν πατέρα του και θα συνεχίσει την προώθηση του μηνύματος προσθέτοντας την δική του ταυτότητα.

Συνοψίζοντας, μέσα από τα πρωτόκολλα που μελετήθηκαν εντοπίστηκαν δύο διαφορετικές τεχνικές για αντιμετώπιση του hello attack. Η πρώτη αφήνει ένα χρονικό περιθώριο στους κόμβους για να ανταλλάξουν τα hello μηνύματα. Τα μηνύματα που στέλνονται εκτός του χρόνου αυτού δεν γίνονται αποδεκτά. Η δεύτερη μέθοδος βασίζεται στο base station. Το base station δίνει το σήμα για να αρχίσει η διαδικασία “γνωριμίας” των κόμβων. Χρησιμοποιείται το MAC για να πιστοποιήσουν οι κόμβοι πως το μήνυμα στάλθηκε από το base station. Αν το

μήνυμα είναι αυθεντικό τότε οι κόμβοι προωθούν το πακέτο στους άλλους και ανανεώνουν τη λίστα με τους γείτονές τους.

Λόγω του ότι η δεύτερη μέθοδος βασίζεται κατά πολύ στο base station και συμπεριλαμβάνει την επεξεργασία των πακέτων που λαμβάνουν – άσχετα με το αν θα απορριφθεί τελικά το πακέτο, μπορούμε να πούμε πως η πρώτη μέθοδος είναι πιο αποτελεσματική και πιο οικονομική. Κατά τη διαδικασία αυτή, οι κόμβοι απλά κάνουν broadcast ένα hello μήνυμα στο δίκτυο και οι κόμβοι που θα το παραλάβουν ανανεώνουν τη λίστα με τους γείτονές τους. Η επεξεργασία που γίνεται για την ολοκλήρωση της διαδικασίας είναι πιο απλή. Με βάση τη δεύτερη μέθοδο, οι κόμβοι παραλαμβάνουν το hello message από το base station, το επεξεργάζονται – ελέγχουν αυθεντικότητα, το χρόνο στον οποίο στάλθηκε, και μετά προωθείται το μήνυμα στους άλλους κόμβους.

5.6 Selective Forwarding

Κατά την επίθεση αυτή ο attacker δεν προωθεί τα πακέτα ή προωθεί μερικά από τα πακέτα που παίρνει επηρεάζοντας έτσι την δρομολόγηση των πακέτων και την απόδοση του δικτύου – ενότητα 2.6.1.5. Συνήθως χρησιμοποιείται η τακτική διαβίβασης μερικών πακέτων επειδή με την απόρριψη όλων των πακέτων που παίρνει αυξάνει τις πιθανότητες να εντοπιστεί από το δίκτυο και τον αποκλεισμό του από τα μονοπάτια δρομολόγησης.

Η επίθεση αυτή μπορεί να εφαρμοστεί στο πρωτόκολλο CBSRP [12] σε περίπτωση που το cluster head δεν προωθεί τα πακέτα που λαμβάνει από τους κόμβους του cluster του. Με βάση τους συγγραφείς του αντίστοιχου άρθρου, η επίθεση αυτή αντιμετωπίζεται από το CBSRP αλλά ταυτόχρονο δεν μας δίνουν αρκετές πληροφορίες για το πως γίνεται εφικτή η αντιμετώπιση της επίθεσης αυτής. Για τον λόγω αυτό δεν μπορούμε να συνεχίσουμε με μια πιο αναλυτική αναφορά στη μεθοδολογία που ακολουθήθηκε στο πρωτόκολλο αυτό.

Το πρωτόκολλο SecRout [13] αντιμετωπίζει επιτυχώς την επίθεση αυτή, παρά το γεγονός ότι μπορεί να εφαρμοστεί σε τρεις διαφορετικές περιπτώσεις – κατά τη διάρκεια προώθησης ενός μηνύματος για την δημιουργία ενός μονοπατιού δρομολόγησης, κατά τη διάρκεια απάντησης στο αίτημα για δημιουργία μονοπατιού δρομολόγησης και κατά τη προώθηση των μηνυμάτων μέσω του μονοπατιού δρομολόγησης. Όταν ένας κόμβος θέλει να στείλει δεδομένα στο base station κάνει broadcast ένα request. Οι ενδιάμεσοι κόμβοι που θα παραλάβουν το request προσθέτουν σε αυτό την ταυτότητά τους και το κάνουν ξανά broadcast. Η διαδικασία αυτή επαναλαμβάνεται μέχρι το request να φτάσει στο base station. Έτσι, αν κάποιος κόμβος δεν προωθήσει το request που θα πιάσει δεν θα καταφέρει να σταματήσει την όλη διαδικασία αφού αυτή θα ολοκληρωθεί μέσω άλλων κόμβων. Το μόνο που θα πετύχει με το να μην προωθήσει το request είναι τον αποκλεισμό του από τη δρομολόγηση του μηνύματος. Όταν το base station πιάσει το request στέλνει πίσω στους κόμβους μια “απάντηση” για επιβεβαίωση του μονοπατιού. Όταν ένας κόμβος δεν προωθήσει το μήνυμα αυτό μπορεί να εντοπιστεί από τον κόμβο στον οποίο θα έπρεπε να στείλει κανονικά το μήνυμα. Ο εντοπισμός αυτός είναι εφικτός επειδή οι κόμβοι κρατούν ένα πίνακα στον οποίο καταχωρούν για μια διαδρομή τους δύο επόμενούς τους κόμβους και τους δύο προηγούμενούς τους. Ο πίνακας δημιουργείται κατά την διαδικασία ανεύρεσης μονοπατιού μέσω του οποίου θα γίνει και η δρομολόγηση κι έχει την ακόλουθη μορφή, πίνακας 5.1:

Source Node	Previous Two Hops	Next Tow Hops
$ID_{source1}$	ID_{prev1}, ID_{prev2}	ID_{next1}, ID_{next2}
$ID_{source2}$	ID_{prev1}, ID_{prev2}	ID_{next1}, ID_{next2}
…	…	…
$ID_{sourceN}$	ID_{prev1}, ID_{prev2}	ID_{next1}, ID_{next2}

Πίνακας 5.1 Πίνακας Δρομολόγησης για το SecRout

Η προώθηση των πακέτων μέσω του μονοπατιού δρομολόγησης στο SecRout [13] γίνεται με rebroadcast του πακέτου στο οποίο όμως γίνεται αλλαγή της

ταυτότητας του αποστολέα και του παραλήπτη. Όταν ένας κόμβος δεν προωθήσει τα πακέτα που θα πάρει τότε ο κόμβος ο οποίος θα του τα στείλει θα τον εντοπίσει αφού δεν θα “ακούσει” το rebroadcast message. Στις δύο τελευταίες περιπτώσεις όπου οι attackers εντοπίζονται, μπαίνουν σε μαύρη λίστα και δεν γίνονται δεχτά οποιαδήποτε request τους.

Μια διαφορετική μέθοδος αντιμετώπισης του selective forward attack χρησιμοποιείται στο Secure Sensor Network Routing: A Clean State Approach [14]. Στο πρωτόκολλο αυτό – ενότητα 4.4, υποστηρίζεται multipath routing. Έτσι οι κόμβοι που στέλνουν πακέτα έχουν τη δυνατότητα επιλογής του μονοπατιού που θα ακολουθηθεί. Αν εντοπίσει καθυστέρηση ή traffic κατά τη χρήση ενός μονοπατιού τότε μπορεί να επιλέξει κάποιο άλλο. Επίσης, η επικοινωνία είναι reliable κι έτσι ο όταν ένας κόμβος παραλάβει ένα πακέτο στέλνει πίσω ένα acknowledgment. Αν ένας κόμβος δεν παραλάβει το acknowledgment τότε πολύ πιθανό να μην πήγαν τα δεδομένα στον παραλήπτη κι έτσι τα στέλνει ξανά χρησιμοποιώντας κάποια άλλη διαδρομή.

Στο πρωτόκολλο OPSENET [18] χρησιμοποιήθηκε μια διαφορετική τεχνική. Με βάση το πρωτόκολλο αυτό, υπάρχει η υπόθεση ότι όταν το base station παραλάβει ένα πακέτο στέλνει πίσω στον κόμβο ένα acknowledgement. Έτσι όταν ένας κόμβος στείλει κάτι και δεν πάρει πίσω acknowledgement στέλνει ένα maintenance request στο base station μέσω όμως ενός διαφορετικού μονοπατιού από εκείνου που χρησιμοποίησε για την αποστολή του πακέτου. Το base station με τη σειρά του ελέγχει τους κόμβους που βρίσκονται στο δίκτυο στέλνοντας τους ένα route maintenance request στο οποίο οι κόμβοι καλούνται να απαντήσουν στέλνοντας πίσω στο base station ένα μήνυμα με τα στατιστικά τους και το time stamp του request που παρέλαβε. Ανάλογα με τις απαντήσεις που θα λάβει το base station θα καθόρισε τα validate μονοπάτια που θα εξακολουθήσουν να υπάρχουν στο δίκτυο.

Συνοψίζοντας, αν και η διαδικασία που απαιτείται για την δημιουργία του πίνακα δρομολόγησης στο πρωτόκολλο SecRout [13] είναι απαιτητική και χρησιμοποιείται μεγάλο μέρος της μνήμης για την αποθήκευσή του είναι και η βέλτιστη. Οι κόμβοι στο δίκτυο γνωρίζουν τους δύο επόμενους και τους δύο προηγούμενους τους κόμβους που συμμετέχουν στη δρομολόγηση του πακέτου. Ο τρόπος προώθησης των πακέτων – rebroadcast, βοηθά τους κόμβους να εντοπίσουν τους attackers που δεν προώθησαν τα πακέτα που πήραν και να τους απομονώσουν από το δίκτυο.

5.7 Denial of Service

Κατά την επίθεση αυτή ο attacker στοχεύει στην μείωση των πόρων του δικτύου ούτως ώστε να δυσκολεύουν τους νόμιμους κόμβους του δικτύου στην επικοινωνία μεταξύ τους.

Τα πρωτόκολλα Secure Sensor Network Routing: A Clean State Approach [14] και SHEER [17] αντιμετωπίζοντας το hello attack βάζοντας ένα χρονικό περιθώριο στο οποίο οι κόμβοι του δικτύου αποδέχονται τα hello messages, όπως περιγράφετε στην ενότητα 5.5, εμποδίζουν τον attacker από το να εξαντλήσει τους πόρους των κόμβων που συμμετέχουν στο δίκτυο. Ένας πόρος που προστατεύονται είναι οι buffers των αισθητήρων. Προστατεύονται υπό την έννοια ότι δεν υπάρχει κίνδυνος να γεμίσουν με τα hello messages του attacker, αφού τα πακέτα που δεν στέλνονται στα χρονικά πλαίσια δεν γίνονται αποδεχτά και δεν αποθηκεύονται στη μνήμη του αισθητήρα. Παράλληλα δεν σπαταλά ο αισθητήρας επιπρόσθετα ποσά ενέργειας για να επεξεργαστεί το hello message και να κάνει τις απαραίτητες αλλαγές στον πίνακα με τους γείτονές του.

Τα πρωτόκολλα που αντιμετωπίζουν το selective forward attack – SecRout [13], Secure Sensor Network Routing: A Clean State Approach [14] και OPSENET [18], αντιμετωπίζουν και την επίθεση denial of service αφού επιτυγχάνουν να

εντοπίσουν τους εχθρικούς κόμβους κι έτσι οι κόμβοι δεν αναγκάζονται να στέλνουν πολλές φορές το ίδιο μήνυμα εξοικονομώντας έτσι ποσά ενέργειας.

Για την αντιμετώπιση της επίθεσης αυτής δεν αναπτύχθηκε κάποια ιδιαίτερη μέθοδος από τα πρωτόκολλα που μελετήθηκαν. Η αντιμετώπιση των άλλων επιθέσεων που μπορούν να εφαρμοστούν στο δίκτυο έχει ως αποτέλεσμα και την αντιμετώπιση των denial of service attacks. Το δίκτυο προστατεύει τους πόρους του και τους πόρους των κόμβων που συμμετέχουν σε αυτό. Ένα χαρακτηριστικό παράδειγμα αποτελεί η προστασία των περιορισμένων buffers που έχουν οι αισθητήρες, όπως αυτό αναλύεται στην αρχή της ενότητας αυτής.

Κεφάλαιο 6

Συμπεράσματα

6.1 Γενικά Συμπεράσματα

Μέσα από την εργασία αυτή μας δόθηκε η ευκαιρία να έρθουμε σε επαφή με βασικές έννοιες και στοιχεία που πρέπει να ισχύουν ούτως ώστε να μπορέσει να υπάρξει ασφάλεια σε ένα δίκτυο αισθητήρων. Όπως αναφέρθηκε και στα πρώτα κεφάλαια της μελέτης αυτής, οι αισθητήρες έχουν κάποιες ιδιαιτερότητες οι οποίες δεν επιτρέπουν την εφαρμογή υφιστάμενων πρωτοκόλλων ασφαλείας σε αυτά – όπως για παράδειγμα η περιορισμένη υπολογιστική ικανότητα και τα περιορισμένα ποσά ενέργειας. Μελετήσαμε επιθέσεις που μπορούν να εφαρμοστούν σε ένα δίκτυο και αναλύσαμε σε βάθος επτά διαφορετικά πρωτόκολλα ασφαλείας τα οποία αναπτύχθηκαν ιδικά για αισθητήρες και πιο συγκεκριμένα για το επίπεδο δρομολόγησής τους. Ακολούθως αναλύθηκαν οι μέθοδοι που χρησιμοποιήθηκαν σε κάθε ένα από τα πρωτόκολλα για την αντιμετώπιση των πιο διαδεδομένων επιθέσεων που μπορούν να εφαρμοστούν σε ένα δίκτυο. Η ανάλυση που έγινε στο τομέα αυτό μας οδήγησε στα συμπεράσματα που ακολουθούν.

Ο τρόπος οργάνωσης του κάθε δικτύου, τα δεδομένα που κρατούν οι κόμβοι για τους υπόλοιπους κόμβους του δικτύου του καθώς και ο τρόπος επικοινωνίας των κόμβων επηρεάζει άμεσα τις επιθέσεις που μπορούν να εφαρμοστούν σε αυτό καθώς και τις επιθέσεις που μπορεί να αντιμετωπίσει.

Μέσα από τη μελέτη των πρωτοκόλλων CBSRP, SecRout, Secure Sensor Network Routing: A Clean State Approach, SPINS, Secure SPIN, SHEER και OPSENET συμπεραίνουμε ότι σε δίκτυα στα οποία χρησιμοποιείται το broadcast για την αποστολή των μηνυμάτων εντός του δικτύου δεν μπορεί να εφαρμοστεί η επίθεση selective forwarding, sinkhole, sybil και wormhole. Η επίθεση hello δεν μπορεί να εφαρμοστεί σε περίπτωση που με βάση το πρωτόκολλο οι κόμβοι δεν αναγγέλλουν τους εαυτούς τους στο δίκτυο. Όσων αφορά το sybil attack, δεν μπορεί να εφαρμοστεί σε πρωτόκολλα στα οποία δεν λαμβάνεται υπόψη η τοποθεσία του κόμβου. Το sinkhole attack δεν μπορεί να εφαρμοστεί σε πρωτόκολλα τα οποία δεν λαμβάνουν υπόψη τα χαρακτηριστικά των κόμβων.

Όλες οι επιθέσεις επηρεάζουν τους πόρους του δικτύου κι έτσι μπορούν να χαρακτηριστούν και ως επιθέσεις denial of service. Αυτό οφείλεται στο γεγονός ότι μερικές επιθέσεις, όπως το selective forwarding, αναγκάζουν τον κόμβο να αποστείλει το ίδιο πακέτο περισσότερες από μια φορά έχοντας ως αποτέλεσμα την επιπρόσθετη σπατάλη ενέργειας. Κάποιες άλλες, όπως το hello attack, έχουν ως αποτέλεσμα την δέσμευση ενός μέρους του συνολικού bandwidth του δικτύου από τον attacker και επιπρόσθετα οι buffers των αισθητήρων γεμίζουν από τα μηνύματα του εχθρικού κόμβου – δημιουργώντας την πιθανότητα απόρριψης πακέτων από νόμιμους κόμβους του δικτύου λόγο έλλειψης αποθηκευτικού χώρου.

Η μελέτη που έγινε στο κεφάλαιο 5 επιβεβαιώνει πως για την ύπαρξη αποδοτικών μεθόδων αντιμετώπισης μερικών επιθέσεων, όπως το selective forwarding, χρειάζεται η διατήρηση μεγάλου όγκου πληροφοριών και ο ιδανικότερος τρόπος για την συλλογή τους αποτελεί η διαδικασία εγκαθίδρυσης

του μονοπατιού δρομολόγησης από ένα αποστολέα σε ένα προορισμό. Γενικώς, αποδοτικές μέθοδοι αντιμετώπισης ενός attack, δεν θεωρούνται αυτές που απλά αναγνωρίζουν πως το δίκτυο δέχτηκε μια επίθεση και επιλέγουν ένα απλό τρόπο για να συνεχίσουν την ομαλή λειτουργία του δικτύου. Αντιθέτως, αποδοτικές μέθοδοι θεωρούνται αυτές που ναι μεν αναγνωρίζουν την ύπαρξη μιας επίθεσης αλλά καταφέρνουν να απομακρύνουν και τον εχθρικό κόμβο από το δίκτυο. Με τον τρόπο αυτό προστατεύουν το δίκτυο από μελλοντικές επιθέσεις από τον συγκεκριμένο εχθρικό κόμβο.

Φυσικά, η μελέτη που έγινε φανερώνει την ύπαρξη απλών τακτικών οι οποίες όμως είναι πολύ λειτουργικές και αντιμετωπίζουν με επιτυχία διάφορες επιθέσεις. Για παράδειγμα η επίθεση hello attack αντιμετωπίζεται επιτυχώς προσθέτοντας τον περιορισμό για τον χρόνο κατά τον οποίο οι κόμβοι μπορούν να αναγγείλουν τον εαυτό τους στο δίκτυο. Έτσι η επίδραση που μπορεί να έχει ο attacker με την επίθεση αυτή στο δίκτυο είναι περιορισμένη.

Με την διαγραφή των απαραίτητων στοιχείων από την μνήμη του αισθητήρα – συνάρτηση παραγωγής κλειδιών και αρχικό κλειδί, πετυχαίνουμε την επιτυχή αντιμετώπιση του wormhole attack. Στην περίπτωση αυτή όμως πρέπει να παραμένουν σταθερά τα cluster heads.

Προωθώντας τα πακέτα από κόμβο σε κόμβο μέχρι να φτάσουν στον προορισμό τους μέσω rebroadcast και έχοντας εν γνώση οι κόμβοι τους δύο κόμβους που τους προηγούνται και τους δύο κόμβους που τους ακολουθούν στο μονοπάτι δρομολόγησης, μπορούν να αντιμετωπίσουν το selective forward attack. Με την μέθοδο αυτή οι κακόβουλοι κόμβοι μπορούν να εντοπιστούν από τους άλλους κόμβους του δικτύου και να καταχωρηθούν σε μια μαύρη λίστα.

Όσον αφορά το sybil attack μπορεί πολύ εύκολα να αντιμετωπιστεί αν οι κόμβοι κατά τη διαδικασία γνωριμίας τους με τους άλλους κόμβους του δικτύου χρησιμοποιούν και ένα certificate το οποίο επιβεβαιώνει την γνησιότητά τους. Ο

εχθρικός κόμβος κατά τη διαδικασία γνωριμίας των κόμβων του δικτύου και αναγγελίας των εαυτών τους στο δίκτυο, βρίσκει την ευκαιρία να προβάλει κι άλλες ταυτότητες στο δίκτυο. Αυτό όμως δεν θα το καταφέρει αφού δεν θα μπορέσει να εφοδιαστεί με το αντίστοιχο certificate. Με τον τρόπο αυτό η αντιμετώπιση του sybil attack συνδυάζεται με μια στοιχειώδη και αναπόφευκτη διαδικασία του δικτύου.

Η επίθεση sinkhole μπορεί να αντιμετωπιστεί με μια απλή περιοδική αλλαγή των cluster heads. Χρησιμοποιώντας την τακτική αυτή, η πιθανότητα να επιλεγεί για δεύτερη φορά ένας εχθρικός κόμβος ως cluster head είναι ελάχιστες. Επιπρόσθετα, η τακτική αυτή μπορεί να εφαρμοστεί στα περισσότερα πρωτόκολλα που σχεδιάστηκαν για δίκτυα αισθητήρων αφού όπως φάνηκε και από τη μελέτη αυτή, απαιτούν την οργάνωση του δικτύου σε clusters.

Οι τακτικές αυτές μπορούν να προστεθούν στα υπάρχοντα πρωτόκολλα ασφαλείας κι έτσι να αναβαθμίσουν όχι μόνο τον αριθμό των επιθέσεων που αντιμετωπίζουν αλλά και την ποιότητα της μεθόδου αντιμετώπισης που προσφέρουν. Παράλληλα, ο συνδυασμός των προαναφερόμενων τακτικών μπορεί να οδηγήσει στη δημιουργία νέων, εξίσου αποδοτικών πρωτοκόλλων ασφαλείας για τα δίκτυα αισθητήρων τα οποία όμως να είναι πιο “ελαφριά” από τα υπάρχοντα και να απαιτούν λιγότερες πράξεις και υπολογισμούς από τα υπάρχοντα.

6.2 Μελλοντική Εργασία

Η συγκεκριμένη ατομική διπλωματική εργασία αποτελεί την αρχική βάση για έρευνα στον τομέα της ασφάλειας στα δίκτυα αισθητήρων. Τα αποτελέσματα της μελέτης αυτής μπορούν να χρησιμοποιηθούν για την δημιουργία ενός βασικού προφίλ που πρέπει να έχει ένα πρωτόκολλο για να αντιμετωπίζει αποδοτικά μια επίθεση ή ένα συνδυασμό επιθέσεων. Επίσης, οι πληροφορίες που προσφέρονται στη μελέτη αυτή μπορούν να χρησιμοποιηθούν για την

αναβάθμιση υφιστάμενων πρωτοκόλλων, έτσι ώστε να αντιμετωπίζουν επιθέσεις που μέχρι στιγμής δεν καλύπτουν ή να τροποποιήσουν τον τρόπο που τις αντιμετωπίζουν για να είναι πιο αποδοτικά.

Η μελέτη που έγινε στην εργασία αυτή μπορεί να εμβαθύνει με τον συνδυασμό πληροφοριών σχετικών με την κατανάλωση ενέργειας που απαιτεί η κάθε μέθοδος αντιμετώπισης ενός attack. Τα αποτελέσματα της έρευνας αυτής μπορούν να χρησιμοποιηθούν για τη δημιουργία πρωτοκόλλων ασφαλείας που προσφέρουν αξιόλογα επίπεδα ασφάλειας με χαμηλά ενεργειακό κόστος.

6.3 Προκλήσεις

Η ταυτόχρονη ύπαρξη μέγιστης ασφάλειας – επιτυχής αντιμετώπιση όλων των γνωστών επιθέσεων που μπορούν να εφαρμοστούν σε ένα δίκτυο, με το χαμηλότερο κόστος αποτελεί μια από τις μεγαλύτερες προκλήσεις για τους ερευνητές του συγκεκριμένου πεδίου. Για να αυξηθεί η απόδοση ενός πρωτοκόλλου ασφαλείας είναι αναγκαία και η προσθήκη επιπλέον ελέγχων και πληροφοριών που πρέπει να κατακρατεί και να ενημερώνει ο κόμβος. Άμεσο επακόλουθο όμως αποτελεί και η χρήση περισσότερης ενέργειας – θα καταναλώνεται περισσότερη ενέργεια για την εκτέλεση των επιπρόσθετων ελέγχων και ενημερώσεων. Απαιτείται περαιτέρω έρευνα και μελέτη για την εύρεση του ιδανικού συνδυασμού ή της χρυσής τομής μεταξύ ενέργειας και επίπεδου ασφάλειας.

6.4 Επίλογος

Η χρήση των τεχνολογικών επιτευγμάτων σε όλους τους τομείς της ζωής μας κάνει απαραίτητη την ύπαρξη ασφάλειας τόσο στη χρήση τους όσο και στις πληροφορίες που παίρνουμε από αυτές. Το ζήτημα της ασφάλειας σε ασύρματα δίκτυα αισθητήρων είναι ιδιαίτερα λεπτό, αφού πηγάζουν αρκετοί περιορισμοί

από την φύση τους – μικρές συσκευές με μικρή υπολογιστική ικανότητα και περιορισμένη ενέργεια. Παρόλους τους περιορισμούς μπούμε να βελτιώσουμε τα υπάρχοντα πρωτόκολλα ασφάλειας ούτως ώστε να προσφέρουν αξιόλογη ασφάλεια και παράλληλα να προστατεύονται και οι πόροι του κόμβου και κατ' επέκταση του δικτύου.

Βιβλιογραφία

[1] Holger Karl, Andreas Willig, “Protocols and Architectures for Wireless Sensor Networks”, Publisher: John Wiley & Sons, Ltd, 2005.

[2] http://en.wikipedia.org/wiki/Wireless_sensor_network.

[3] John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, “Wireless Sensor Network Security: A Survey”, Auerbach Publications, CRC Press, pp. 1-50, 2006.

[4] James F. Kurose, Keith W. Ross, “Computer Networking: A Top-Down Approach Featuring the Internet”, Third Edition, Publisher: Addison Wesley, 2005, ISBN: 0-321-26976-4.

[5] http://docs.sun.com/source/816-6154-10/contents.htm.

[6] http://www.cisl.ucar.edu/docs/ssh/guide/node4.html.

[7] http://www.acm.org/crossroads/xrds7-1/crypto.html.

[8] Charlie Kaufman, Radia Perlman, Mike Specinor, “Network Security – Private Communication in a Public World”, Second Edition, Publisher: Prentice Hall, 2002, ISBN: 0-13-046019-2.

[9] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, Erdal Cayirci, “A Survey on Sensor Networks”, IEEE Communications Magazine, pp. 102-114, August 2002.

[10] William Stallings, “Network Security Essentials: Applications and Standards”, Second Edition, Publisher: Prentice Hall, 2003, ISBN: 0-13-120271-5.

[11] Chris Karlof, David Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”, pp. 293-315, 2003 Elsevier B.V.

[12] Yao Lan, Zhao Zhibin, Gao Fuxiang, Yu Ge, “The Research on Certainty Based Secure Routing Protocol in Wireless Sensor Networks”, Wireless Communications, Networking and Mobile Computing, 2006, WiCOM 2006, pp. 1-5.

[13] Jian Yin, Sanjay Madria, “SecRout: A Secure Routing Protocol for Sensor Networks”, 20th International Conference on Advanced Information Networking and Applications (AINA’06), 2006.

[14] Bryan Parno, Mark Luk, Evan Gaustad, Adrian Perrig, “Secure Sensor Network Routing: A CleanSlate Approach”, CoNEXT 2006 Lisboa, Portugal

[15] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar. “SPINS: Security Protocols for Sensor Networks”, Mobile Computing and Networking, Rome, Italy, pp. 521-534, 2001.

[16] Debao Xiao, Meijuan Wei, Ying Zhou, “Secure-SPIN: Secure Sensor Protocol for Information via Negotiation for Wireless Sensor Networks”, Industrial Electronics and Applications, 2006 1ST IEEE Conference on Volume, May 2006, pp. 1-4.

[17] Jamil Ibriq, Imad Mahgoub, “A Secure Hierarchical Routing Protocol for Wireless Sensor Networks”, Communication systems, ICCS 2006, 10th IEEE Singapore International Conference on Volume, pp. 1-6.

[18] Unoma Ndili Okorafor, Deepa Kundur, “OPSENET: A Security-Enabled Routing Scheme for a System of Optical Sensor Networks”, 3rd International Conference on Broadband Communications, Networks and Systems (BROADNETS 2006), 1-5 October 2006, San José, California, USA, IEEE 2006.