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

Ασφάλεια στα Ασύρματα Δίκτυα Αισθητήρων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αλέξανδρος, Κ. Καπετανάκης

Επιβλέπων : Ιωάννης Ν. Αβαριτσιώτης
Καθηγητής Ε.Μ.Π

Αθήνα, Ιούλιος 2005

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

Ασφάλεια στα Ασύρματα Δίκτυα Αισθητήρων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αλέξανδρος, Κ. Καπετανάκης

Επιβλέπων : Ιωάννης Ν.Αβαριτσιώτης
Καθηγητής Ε.Μ.Π

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την Ιουλιος 2005.

.....	.....	.....
Ιωάννης Αβαριτσιώτης	Θεολόγου Μιχάλης	Συκάς Ευστάθιος
Καθηγητής Ε.Μ.Π	Καθηγητής Ε.Μ.Π	Καθηγητής Ε.Μ.Π

Αθήνα, Ιούλιος 2005

.....

Αλέξανδρος Κ.Καπετανάκης

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

Η εργασία αυτή εκπονήθηκε στο Εργαστήριο Μικροηλεκτρονικής του τμήματος Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Ε.Μ.Π.

Στο σημείο αυτό θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή, κ.Αβαριτσιώτη, για την βοήθεια και την καθοδήγηση καθ'όλη την διάρκεια της προσπάθειας. Επίσης, ευχαριστώ τον διδάκτορα κ. Παναγιώτη Κίκιρα για την πολύτιμη βοήθεια του στην εκπόνηση της παρούσης εργασίας.

ΠΕΡΙΛΗΨΗ

Τα ασύρματα δίκτυα αισθητήρων αποτελούν, τα τελευταία χρόνια, μία περιοχή με μεγάλη ερευνητική δραστηριότητα. Οι ιδιαιτερότητες αυτών των δικτύων καθιστούν τη μελέτη τους ξεχωριστή από τις ήδη υπάρχουσες τεχνολογίες ασύρματων δικτύων (όπως ad-hoc ή IEEE 802.11). Τα δίκτυα αυτά αποτελούνται από μικρού μεγέθους κόμβους, που έχουν περιορισμένη αυτονομία και υπολογιστικές δυνατότητες.

Στην εργασία αυτή θα αναφερθούμε γενικά για τα ασύρματα δίκτυα αισθητήρων, την αρχιτεκτονική και τα δομικά μέρη των κόμβων των ασυρμάτων δικτύων αισθητήρων, τις εφαρμογές τους σε διάφορους τομείς.

Επίσης θα παρουσιάσουμε τις απαιτήσεις ασφαλείας και τις ιδιαιτερότητες των ασυρμάτων δικτύων αισθητήρων.

Στη συνέχεια, θα εξετάσουμε αναλυτικά τις απειλές και τα αντίμετρα που δέχονται αυτά στο φυσικό επίπεδο, στο επίπεδο ζεύξης και στο επίπεδο δικτύου.

Τέλος, θα γίνει μια παρουσίαση υπαρχόντων πρωτοκόλλων στην ποιότητα υπηρεσίας, στην ενέργεια και την ασφάλεια που παρέχουν στα δίκτυα αυτά.

ABSTRACT

During the last few years wireless sensors networks (furthermore WSN) constitute a region with high inquiring activity.

The particularities of these networks render their study separate from the already existing technologies of wireless networks (such as ad-hoc or IEEE's 802.11 networks).These networks are composed by small size nodes, which have limitations in their available energy and in their processing capabilities.

This work deals with wireless sensor networks in general, and among the issues that examines are the architecture and the structural parts of nodes of WSN and their applications in various sectors. The main contribution of this work is focused on security issues of WSN's. Hence, we review the main protocols in this field and we present the security requirements, the main threats and countermeasures.

ΚΕΦΑΛΑΙΟ 1ο

ΕΙΣΑΓΩΓΗ

1.1 Γενικά για δίκτυα αισθητήρων

Η πρόσφατη πρόοδος στην τεχνολογία των μικρό-ηλεκτρομηχανικών συστημάτων (ΜΗΜΣ), στις ασύρματες επικοινωνίες και στα ψηφιακά ηλεκτρονικά έχει δώσει την δυνατότητα για την ανάπτυξη κόμβων αισθητήρων χαμηλού-κόστους, χαμηλής κατανάλωσης ενέργειας και πολλών λειτουργιών, οι οποίοι είναι μικροί σε μέγεθος και επικοινωνούν ,χωρίς ανθρώπινη παρέμβαση ή επιτήρηση, μεταξύ τους σε μικρές αποστάσεις. Αυτοί οι μικροσκοπικοί κόμβοι αισθητήρων, που αποτελούνται από υποσύστηματα αίσθησης, επεξεργασίας δεδομένων και επικοινωνιών, οδηγούν στην ιδέα των δικτύων αισθητήρων που βασίζονται στην συνεργατική λειτουργία ενός μεγάλου συνόλου κόμβων.

Ένα δίκτυο αισθητήρων αποτελείται από ένα μεγάλο αριθμό κόμβων αισθητήρων, οι οποίοι αναπτύσσονται πυκνά, είτε μέσα στο φαινόμενο είτε πολύ κοντά σε αυτό. Η θέση των κόμβων αισθητήρων δεν είναι ανάγκη να προσχεδιαστεί ή να προαποφασιστεί. Αυτό επιτρέπει την τυχαία εξάπλωσή τους σε μη προσβάσιμα εδάφη ή σε επιχειρήσεις για την αντιμετώπιση καταστροφών. Από την άλλη πλευρά, αυτό σημαίνει ότι τα πρωτόκολλα και οι αλγόριθμοι των δικτύων αισθητήρων πρέπει να διαθέτουν αυτό-οργανωτικές δυνατότητες. Ένα άλλο μοναδικό χαρακτηριστικό των δικτύων αισθητήρων είναι η συνεργατική λειτουργία των κόμβων αισθητήρων.

Τα παραπάνω χαρακτηριστικά εξασφαλίζουν ένα μεγάλο πλήθος εφαρμογών για τις οποίες είναι κατάλληλα τα δίκτυα αισθητήρων. Μερικές από τις περιοχές εφαρμογής είναι η υγεία, ο στρατός και η ασφάλεια. Για παράδειγμα, μια στρατιωτική εφαρμογή των δικτύων αισθητήρων είναι η χρησιμοποίησή τους στα συστήματα διοίκησης, ελέγχου, επικοινωνιών, πληροφορικής, πληροφοριών, επιτήρησης, αναγνωρίσεων και σκόπευσης (C4ISRT), εκμεταλλευόμενοι τις ιδιότητες τους όπως η ταχεία εγκατάσταση, η αυτό-οργάνωση και η αντοχή σε λάθη.

Προκειμένου να υλοποιηθούν οι παραπάνω αλλά και άλλες εφαρμογές των δικτύων αισθητήρων απαιτούνται τεχνικές ad-hoc δικτύωσης (καθόσον έχουν ομοιότητες με τα δίκτυα αισθητήρων). Παρόλο που αρκετοί αλγόριθμοι και πρωτόκολλα έχουν προταθεί για τα παραδοσιακά ad-hoc ασύρματα δίκτυα, δυστυχώς

δεν είναι δυνατόν να χρησιμοποιηθούν στα δίκτυα αισθητήρων εξαιτίας των μοναδικών χαρακτηριστικών και των απαιτήσεων των εφαρμογών των δικτύων αισθητήρων. Παρακάτω, αναφέρονται περιληπτικά οι διαφορές μεταξύ των δύο αυτών δικτύων που δικαιολογεί το παραπάνω πρόβλημα :

- Ο αριθμός των κόμβων σε ένα δίκτυο αισθητήρων μπορεί να είναι πολλές φορές πιο μεγάλος από ότι σε ένα ad hoc δίκτυο.
- Η χωρική πυκνότητα των δικτύων αισθητήρων είναι συχνά μεγάλη.
- Οι αισθητήριοι κόμβοι είναι εύκολο να καταστραφούν.
- Η τοπολογία ενός δικτύου αισθητήρων αλλάζει πολύ συχνά.
- Οι αισθητήριοι κόμβοι χρησιμοποιούν κυρίως επικοινωνία broadcast ενώ τα περισσότερα ad-hoc δίκτυα βασίζονται στην επικοινωνία σημείου προς σημείο.
- Οι αισθητήριοι κόμβοι διακρίνονται για τους σημαντικούς περιορισμούς που έχουν, από κατασκευής, στους τομείς της ενέργειας, της υπολογιστικής ισχύος και της μνήμης.
- Οι αισθητήριοι κόμβοι συνήθως δεν έχουν κάποιο παγκόσμιο αναγνωριστικό (ID), εξαιτίας του μεγάλου μεγέθους της επικεφαλίδας που απαιτεί μια τέτοια ιδιότητα, καθώς και του μεγάλου αριθμού των κόμβων.

Επειδή ένας μεγάλος αριθμός κόμβων αισθητήρων αναπτύσσεται με πυκνή διάταξη, οι γειτονικοί κόμβοι μπορεί να βρίσκονται πολύ κοντά ο ένας στον άλλο. Έτσι η επικοινωνία μεταξύ πολλαπλών διαδοχικών κόμβων (multi-hop communication) στα δίκτυα αισθητήρων αναμένεται να απαιτεί λιγότερη ενέργεια από ότι η παραδοσιακή επικοινωνία μεταξύ γειτονικών κόμβων (single-hop communication). Η επικοινωνία μεταξύ πολλαπλών διαδοχικών κόμβων (multi-hop) μπορεί να αντιμετωπίσει αποτελεσματικά κάποια από τα προβλήματα διάδοσης του σήματος σε μακρινές αποστάσεις.

Ένας από τα πιο σημαντικούς περιορισμούς στα δίκτυα ασύρματων αισθητήρων είναι η απαίτηση για χαμηλή κατανάλωση ενέργειας. Οι αισθητήριοι κόμβοι έχουν περιορισμένες και συνήθως αναντικατάστατες πηγές ενέργειας. Έτσι ενώ τα παραδοσιακά δίκτυα στοχεύουν να παρέχουν υπηρεσίες υψηλής ποιότητας, τα δίκτυα ασύρματων αισθητήρων έχουν ως πρωταρχικό στόχο την διατήρηση της ενέργειας. Επίσης θα πρέπει να έχουν ένα μηχανισμό που θα δίνει στον χρήστη του

δικτύου την επιλογή να παρατείνει την ζωή του δικτύου με αντάλλαγμα την μικρότερη διαμεταγωγή ή την μεγαλύτερη καθυστέρηση στην μετάδοση.

Τα Ασύρματα Δίκτυα Αισθητήρων (Wireless Sensor Networks, WSN) αποτελούν, τα τελευταία χρόνια, μία περιοχή με μεγάλη ερευνητική δραστηριότητα. Οι ιδιαιτερότητες αυτών των δικτύων καθιστούν τη μελέτη τους ξεχωριστή από τις ήδη υπάρχουσες τεχνολογίες ασύρματων δικτύων (όπως Ad-Hoc ή IEEE 802.11). Τα δίκτυα αυτά αποτελούνται από μικρού μεγέθους κόμβους που έχουν περιορισμένη αυτονομία και υπολογιστικές δυνατότητες. Συνήθως, αφού τοποθετηθούν για να παρακολουθήσουν ένα δεδομένο φαινόμενο, λειτουργούν αυτόνομα χωρίς ανθρώπινη παρέμβαση, καθ' όλη τη διάρκεια της ζωής τους. Η χρήση πρωτοκόλλων επικοινωνίας και συνεργασίας για την επεξεργασία δεδομένων, με μικρή κατανάλωση ενέργειας, είναι απαραίτητη για την διατήρηση του δικτύου στη ζωή όσο το δυνατόν περισσότερο.

1.2 Παράγοντες που επηρεάζουν το σχεδιασμό των δικτύων αισθητήρων.

Ο σχεδιασμός ενός δικτύου αισθητήρων επηρεάζεται από πολλούς παράγοντες. Παρακάτω αναφέρονται μερικοί από αυτούς. Η μελέτη αυτών των παραγόντων (που πρέπει ή δεν πρέπει να διαθέτουν τα δίκτυα αισθητήρων και οι αισθητήριοι κόμβοι) είναι πρωταρχικής σημασίας γιατί παρέχουν τις κατευθύνσεις γύρω από τις οποίες πρέπει να σχεδιαστεί ένα πρωτόκολλο ή αλγόριθμός για δίκτυα αισθητήρων.

1.2.1Αντοχή σε σφάλματα.

Κάποιοι αισθητήριοι κόμβοι είναι δυνατόν να αποτύχουν ή να μπλοκαριστούν εξαιτίας της έλλειψης ενέργειας ή μιας φυσικής ζημιάς, ή εξαιτίας περιβαλλοντολογικών παρεμβολών. Η αποτυχία ή καταστροφή (παροδική ή μόνιμη) μερικών αισθητήριων κόμβων δεν θα πρέπει να επηρεάζει τον συνολικό σκοπό του δικτύου των αισθητήρων. Αυτό το θέμα αναφέρεται ως αξιοπιστία ή αντοχή σε σφάλματα. Η αντοχή σε σφάλματα είναι η δυνατότητα του δικτύου αισθητήρων να διατηρεί τη λειτουργικότητά του χωρίς διακοπές που να οφείλονται στις αποτυχίες των κόμβων του. Η αξιοπιστία ή η αντοχή σε σφάλματα ενός αισθητήριου κόμβου συμβολίζεται με $R_k(t)$ και μοντελοποιείται στο χρησιμοποιώντας τη διασπορά Poisson προκειμένου να δείξει την πιθανότητα να μην έχουμε κάποια αποτυχία σε ένα χρονικό διάστημα (0,t) :

$$R_k(t) = \exp(-\lambda_k t) \quad \textbf{(1.1)}$$

όπου λ_k και t είναι αντίστοιχα ο ρυθμός αποτυχίας ενός κόμβου k και η χρονική περίοδος.

Οι αλγόριθμοι και τα πρωτόκολλα μπορούν να σχεδιαστούν ώστε να εμπεριέχουν τα επίπεδα αντοχής σε λάθη που απαιτούνται από τα δίκτυα αισθητήρων. Αν το περιβάλλον στο οποίο πρόκειται να αναπτυχθεί ένα δίκτυο αισθητήρων δημιουργεί μικρές παρεμβολές τότε τα πρωτόκολλα μπορούν ανάλογα να είναι πιο ελαστικά. Για παράδειγμα, αν ένα δίκτυο αισθητήρων βρίσκεται εγκατεστημένο σε μια οικία προκειμένου να παρακολουθεί τα επίπεδα υγρασίας και θερμοκρασίας, η αντοχή σε σφάλματα μπορεί να είναι χαμηλή αφού τέτοιου είδους αισθητήριοι κόμβοι δεν καταστρέφονται και δεν παρεμβάλλονται εύκολα από το περιβάλλον. Αντιθέτως σε ένα πεδίο μάχης το δίκτυο αισθητήρων που θα εγκατασταθεί πρέπει να έχει μεγάλη αντοχή σε σφάλματα διότι είναι πολύ εύκολο να καταστραφούν αρκετοί κόμβοι του από εχθρικές επιχειρήσεις. Από τα παραπάνω διαπιστώνεται ότι η αντοχή σε σφάλματα εξαρτάται και από την εφαρμογή για την οποία προορίζεται το δίκτυο. Συνεπώς αυτό πρέπει να λαμβάνεται υπόψη στο σχεδιασμό του δικτύου αισθητήρων αλλά και των ίδιων των κόμβων

1.2.2 Δυνατότητα Κλιμάκωσης.

Ο αριθμός των αισθητήριων κόμβων που έχουν αναπτυχθεί για την μελέτη ενός φαινομένου μπορεί να είναι της τάξης των εκατοντάδων ή χιλιάδων. Ανάλογα με την εφαρμογή, ο αριθμός αυτός μπορεί να φτάσει και την ακραία τιμή των εκατομμυρίων. Ό,τι πρωτόκολλο σχεδιαστεί θα πρέπει να μπορεί να χειριστεί αυτόν τον αριθμό των κόμβων. Πρέπει επίσης να χρησιμοποιήσουν την υψηλή πυκνότητα με την οποία εγκαθίστανται οι αισθητήριοι κόμβοι. Η πυκνότητα μπορεί να διαφέρει από μερικούς μέχρι εκατοντάδες κόμβους σε μια περιοχή η οποία μπορεί να είναι μικρότερη σε διάμετρο από 10m . Η πυκνότητα μπορεί να υπολογιστεί σύμφωνα με το:

$$\mu(R) = \frac{(N\pi R^2)}{(A)} \quad \textbf{(1.2)}$$

όπου N είναι ο αριθμός των διασπαρμένων κόμβων σε μια περιοχή A και R η εμβέλεια της ασύρματης μετάδοσης. Βασικά το $\mu(R)$ δίνει τον αριθμό των κόμβων μέσα στην εμβέλεια της ασύρματης μετάδοσης του κάθε κόμβου που ανήκει στην περιοχή A.

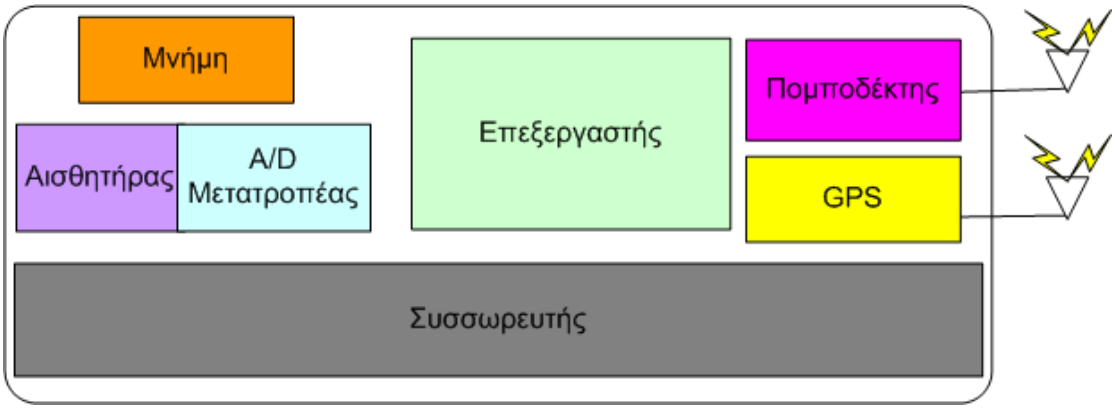
Επιπλέον, ο αριθμός των κόμβων σε μια περιοχή μπορεί να χρησιμοποιηθεί για να δείξει την πυκνότητα των κόμβων. Η πυκνότητα αυτή εξαρτάται από την εφαρμογή για την οποία εγκαταστάθηκαν οι αισθητήριοι κόμβοι. Για την παρακολούθηση μηχανημάτων, η πυκνότητα των αισθητήριων κόμβων είναι περίπου 300 για μια περιοχή $5m^2$, και η πυκνότητα για παρακολούθηση οχημάτων είναι περίπου 10 κόμβοι ανά περιοχή. Γενικά η πυκνότητα μπορεί να φτάνει μέχρι και 20 αισθητήριους κόμβους ανά m^3. Ένα σπίτι μπορεί να περιέχει περίπου δύο 12αδες οικιακών συσκευών που να περιέχουν αισθητήριους κόμβους, αλλά αυτός ο αριθμός θα μεγαλώσει αν οι αισθητήριοι κόμβοι εμφυτεύονται στην επίπλωση και σε άλλα μικροαντικείμενα. Για εφαρμογές παρακολούθησης οικιών, ο αριθμός των κόμβων κυμαίνεται από 25 ως 100 ανά περιοχή. Η πυκνότητα μπορεί να είναι εξαιρετικά υψηλή όταν ένα άτομο κάθεται σε ένα στάδιο μαζί με άλλους και ο κάθε ένας από αυτούς φέρει αισθητήρες στα ρούχα του, τα παπούτσια του και τα άλλα προσωπικά αντικείμενα που θα κουβαλάει μαζί του (ρολόι, γυαλιά, δαχτυλίδια, μπρελόκ κτλ.)

1.2.3Κόστος Παραγωγής.

Αφού τα δίκτυα αισθητήρων αποτελούνται από ένα μεγάλο αριθμό κόμβων, το κόστος ενός μόνο αισθητήριου κόμβου είναι πολύ σημαντικό για ένα τέτοιο δίκτυο. Αν το κόστος του δικτύου είναι πιο ακριβό από το να εγκατασταθούν οι παραδοσιακοί αισθητήρες, τότε τα δίκτυα αισθητήρων δεν θα συμφέρουν οικονομικά. Αποτέλεσμα του παραπάνω είναι ότι το κόστος του κάθε αισθητήριου κόμβου πρέπει να είναι όσο το δυνατόν μικρότερο.

1.2.4Περιορισμοί του Υλικού.

Ένας αισθητήριος κόμβος όπως φαίνεται και στην ***Εικόνα 1.1*** αποτελείται κατά βάση από τέσσερα τμήματα : μια μονάδα αισθήσεως, μια μονάδα επεξεργασίας, ένα πομποδέκτη και μια μονάδα ενέργειας.



Εικόνα 1.1. Τα τμήματα ενός αισθητήριου κόμβου

Ανάλογα με την εφαρμογή για την οποία προορίζεται μπορεί να διαθέτει επιπλέον τμήματα όπως σύστημα εντοπισμού θέσης, μονάδα παραγωγής ενέργειας και μονάδα κίνησης. Η μονάδα αισθήσεως συνήθως αποτελείται από δύο υπομονάδες : τους αισθητήρες και τους αναλογικό-ψηφιακούς μετατροπείς. Τα αναλογικά σήματα που παράγονται από τα αισθητήρια όργανα και βασίζονται στα παρατηρούμενα φαινόμενα μετατρέπονται σε ψηφιακά σήματα από τους αναλογικό-ψηφιακούς μετατροπείς και κατόπιν μεταφέρονται στην μονάδα επεξεργασίας. Αυτή η μονάδα, που γενικά σχετίζεται με μια μικρή μονάδα αποθήκευσης, διαχειρίζεται τις διαδικασίες που κάνουν τον αισθητήριο κόμβο να συνεργάζεται με άλλους κόμβους για να φέρει σε πέρας τους προσδιορισμένους στόχους. Η μονάδα του πομποδέκτη συνδέει τον αισθητήριο κόμβο στο δίκτυο. Ένα από τα πιο σημαντικά τμήματα του αισθητήριου κόμβου είναι η μονάδα ενέργειας. Οι μονάδες ενέργειας είναι δυνατόν να υποστηρίζονται από μια μονάδα εξαγωγής και παραγωγής ενέργειας (scavenging energy) από το περιβάλλον όπως οι ηλιακές κυψέλες. Υπάρχουν όμως και άλλες υπομονάδες, των οποίων η χρήση εξαρτάται από την εφαρμογή για την οποία χρησιμοποιούνται οι αισθητήριοι κόμβοι.

Οι περισσότερες από τις τεχνικές δρομολόγησης και οι εφαρμογές παρακολούθησης των δικτύων αισθητήρων απαιτούν την γνώση της θέσης με μεγάλη συνήθως ακρίβεια. Έτσι είναι σύνηθες για ένα αισθητήριο κόμβο να έχει προσαρτημένη και μια μονάδα εύρεσης θέσης. Μια μονάδα κίνησης είναι δυνατόν να χρησιμοποιηθεί όταν απαιτείται να κινηθούν οι αισθητήριοι κόμβοι προκειμένου να παρακολουθήσουν καλύτερα το παρατηρούμενο φαινόμενο.

Όλες αυτές οι υπομονάδες πρέπει να μπορούν να χωρέσουν σε ένα χώρο μεγέθους σπιρτόκουτου. Το απαιτούμενο μέγεθος μπορεί να απαιτείται να είναι μικρότερο από ένα κυβικό εκατοστό και να είναι αρκετά ελαφρύ για να παραμένει αιωρούμενο στον αέρα. Εκτός από το μέγεθος, υπάρχουν ακόμα πιο αυστηροί περιορισμοί για τους αισθητήριους κόμβους όπως:

- Πρέπει να καταναλώνουν εξαιρετικά χαμηλή ενέργεια.
- Πρέπει να λειτουργούν ακόμα και σε πολύ πυκνή χωρική τοποθέτηση.
- Πρέπει να έχουν χαμηλό κόστος παραγωγής και να είναι αναλώσιμοι.
- Πρέπει να είναι αυτόνομοι και να λειτουργούν χωρίς παρακολούθηση.
- Πρέπει να προσαρμόζονται στο περιβάλλον που θα λειτουργούν.

Αφού οι αισθητήριοι κόμβοι είναι συνήθως μη προσβάσιμοι, η διάρκεια ζωής ενός δικτύου αισθητήρων εξαρτάται άμεσα από την διάρκεια ζωής των πηγών ενέργειας των κόμβων. Η ενέργεια είναι ένας σπάνιος πόρος του συστήματος εξαιτίας των περιορισμών του μεγέθους. Για παράδειγμα η ολική αποθηκευμένη ενέργεια σε μια «έξυπνη σκόνη» (smart-dust) είναι της τάξης του 1J. Για το σύστημα του ολοκληρωμένου ασύρματου δικτύου αισθητήρων (Wireless Integrated Network Sensors WINS), η ολική ενέργεια που πρέπει να παρέχεται πρέπει να είναι μικρότερη των 30μA προκειμένου να έχει μεγάλη διάρκεια λειτουργίας. Οι κόμβοι στο παραπάνω σύστημα παίρνουν ενέργεια από μια τυπική μπαταρία Λιθίου (Li) τύπου νομίσματος (2.5 cm διάμετρος και 1 cm πάχος). Είναι δυνατόν να επεκτείνουμε την διάρκεια ζωής των δικτύων αισθητήρων χρησιμοποιώντας τεχνικές εξαγωγής και παραγωγής ενέργειας από το περιβάλλον. Παράδειγμα τέτοιας τεχνικής είναι οι ηλιακές κυψέλες.

Η μονάδα του πομποδέκτη των αισθητήριων κόμβων μπορεί να είναι μια παθητική ή ενεργητική οπτική συσκευή όπως στην περίπτωση της έξυπνης σκόνης (smart-dust) ή μια συσκευή ασυρμάτου (Radio Frequency RF). Οι ασύρματες επικοινωνίες μέσω ραδιοσυχνοτήτων απαιτούν διαμόρφωση, συχνότητα, φιλτράρισμα, αποδιαμόρφωση και κυκλώματα πολυπλεξίας τα οποία τις κάνουν περισσότερο πολύπλοκες και ακριβές. Επίσης οι απώλειες του μεταδιδόμενου σήματος μεταξύ δύο αισθητήριων κόμβων μπορεί να είναι υψηλές μέχρι την τέταρτη δύναμη της απόστασης μεταξύ τους, διότι οι αισθητήριοι κόμβοι και οι κεραίες τους είναι πολύ κοντά στο έδαφος. Παρόλα αυτά οι ραδιοσυχνότητες φαίνεται να προτιμούνται στα περισσότερα σχήματα μελέτης των δικτύων αισθητήρων, διότι τα

πακέτα που μεταφέρονται στα δίκτυα ασύρματων αισθητήρων είναι χαμηλών ρυθμών μετάδοσης (συνήθως μικρότερα του 1Hz), και ο παράγοντας επαναχρησιμο-ποίησης της συχνότητας είναι μεγάλος λόγω των μικρών αποστάσεων στην επικοινωνία. Αυτά τα χαρακτηριστικά κάνουν δυνατή τη χρήση ράδιο-ηλεκτρονικών κομματιών με χαμηλές απαιτήσεις σε κύκλους λειτουργίας (low duty cycles). Ο σχεδιασμός και η παραγωγή κυκλωμάτων που από την μία να είναι χαμηλής κατανάλωσης ενέργειας και από την άλλη να έχουν μικρό κύκλο λειτουργίας (λίγα Hz) είναι τεχνικώς δύσκολο, καθώς οι τρέχουσες εμπορικές ασύρματες τεχνολογίες όπως αυτές που χρησιμοποιούνται στο Bluetooth δεν είναι αρκετά επαρκείς για τα δίκτυα αισθητήρων διότι το άνοιγμα και το κλείσιμο τους καταναλώνει πολύ ενέργεια.

Αν και όλο και υψηλότερες υπολογιστικές δυνατότητες είναι διαθέσιμες σε όλο και μικρότερους επεξεργαστές, οι μονάδες επεξεργασίας και μνήμης που απαιτούνται για τα μεγέθη των δικτύων αισθητήρων είναι ακόμα ανεπαρκείς ή ανύπαρκτοι. Για παράδειγμα η μονάδα επεξεργασίας ενός πρωτοτύπου κόμβου «έξυπνης σκόνης» (smart dust mote) είναι ένας 4MHz Atmel AVR 8535 μικρό-ελεγκτής με 8 Kb μνήμη εντολών τύπου flash, 512 bytes RAM και 512 bytes EEPROM. Το λειτουργικό σύστημα TinyOS που χρησιμοποιείται σε αυτόν τον αισθητήρα έχει 3500 bytes κώδικα για το λειτουργικό και 4500 bytes διαθέσιμό χώρο για επιπλέον κώδικα. Η μονάδα επεξεργασίας ενός άλλου πρωτότυπου αισθητήριου κόμβου, που ονομάζεται μAMPS ασύρματος αισθητήριος κόμβος, έχει ένα 59-206 MHz SA-1110 μικρό-επεξεργαστή. Ένα πολυνηματικό (multithreading) μ-OS λειτουργικό σύστημα εκτελείται σε ένα επεξεργαστή του ασύρματου αισθητήριου κόμβου μAMPS.

Οι περισσότερες εφαρμογές για ένα κόμβο απαιτούν γνώση της θέσης (location-based applications). Αφού οι αισθητήριοι κόμβοι εγκαθίστανται γενικά με τυχαία διάταξη και λειτουργούν χωρίς παρακολούθηση, υπάρχει η ανάγκη να συνεργάζονται με ένα σύστημα εντοπισμού θέσης. Τα συστήματα εντοπισμού θέσης απαιτούνται επίσης και από μερικά πρωτόκολλα δρομολόγησης, προκειμένου να λειτουργήσουν. Είναι σύνηθες να θεωρείται ότι κάθε αισθητήριος κόμβος πρέπει να έχει και ένα σύστημα εντοπισμού θέσης (GPS) το οποίο να έχει τουλάχιστον 5m ακρίβεια. Στο άρθρο αυτό αναιρείται διότι ο εξοπλισμός των κόμβων με ένα σύστημα εντοπισμού θέσης δεν είναι εφικτός. Μια διαφορετική προσέγγιση είναι να έχουν μερικοί από τους κόμβους ενσωματωμένο ένα σύστημα GPS προκειμένου να

εντοπίσουν την θέσης τους αλλά και να βοηθήσουν και τους υπόλοιπους γειτονικούς κόμβους να εντοπίσουν και αυτοί τη δική τους θέση.

1.3 Τοπολογία δικτύων αισθητήρων.

Ένας μεγάλος αριθμός μη προσβάσιμων και χωρίς παρακολούθηση αισθητήριων κόμβων, οι οποίοι εύκολα μπορούν να χαλάσουν, κάνει την διατήρηση της τοπολογίας του δικτύου μια μεγάλη πρόκληση. Η πυκνότητα μπορεί να φθάνει και τους 20 κόμβους/m^3, κάτι που δυσκολεύει ακόμα περισσότερο την διαχείριση της τοπολογίας. Μπορούμε να εξετάσουμε την διατήρηση της τοπολογίας του δικτύου αισθητήρων σε 3 φάσεις.

1.3.1 Φάση πριν την εγκατάσταση και φάση εγκατάστασης.

Οι αισθητήριοι κόμβοι μπορούν είτε να διασπαρθούν μαζικά είτε να τοποθετηθούν ένας-ένας στο χώρο. Μπορούν να εγκατασταθούν με τους εξής τρόπους :

- Να πεταχτούν από ένα αεροπλάνο
- Να βρίσκονται σε ένα βλήμα πυροβολικού (ή πύραυλο) το οποίο εκρήγνυται και τους διασπείρει στην περιοχή.
- Να ριφθούν με ένα καταπέλτη π.χ. από το κατάστρωμα ενός πλοίου.
- Να τοποθετηθούν ένας – ένας από ένα άνθρωπο ή ένα ρομπότ.

Αν και ο μεγάλος αριθμός των αισθητήρων καθώς και η χωρίς παρακολούθηση εγκατάστασή τους συνήθως περιλαμβάνει την τοποθέτησή τους σύμφωνα με ένα προσεχτικά μελετημένο σχέδιο, η αρχική εγκατάσταση πρέπει να πληροί κάποια κριτήρια :

- Μείωση του κόστους εγκατάστασης.
- Εξαφάνιση της ανάγκης για οποιαδήποτε προ-οργάνωση ή προ-σχεδιασμό.
- Αύξηση της ευελιξίας τοποθέτησης.
- Προώθηση της αυτό-οργάνωσης και της αντοχής σε σφάλματα.

1.3.2 Φάση μετά την εγκατάσταση.

Μετά την εξάπλωση, οι αλλαγές στην τοπολογία οφείλονται σε αλλαγές στους αισθητήριους κόμβους όπως :

- Θέση.
- Δυνατότητα επικοινωνίας.
- Διαθέσιμη ενέργειας.

- Δυσλειτουργία.
- Λεπτομέρειες στο σκοπό για τον οποίο εγκαταστάθηκαν.

Οι αισθητήριοι κόμβοι μπορούν να εγκατασταθούν και στατικά. Οι αποτυχίες είναι ένα σύνηθες φαινόμενο λόγω έλλειψης ενέργειας ή καταστροφής. Είναι επίσης πιθανό να έχουμε δίκτυα αισθητήρων των οποίων οι κόμβοι συνεχώς κινούνται. Εκτός από τα προβλήματα τα οποία είναι φυσικό να αντιμετωπίζουν εξαιτίας των χαρακτηριστικών τους είναι δυνατόν ακόμα να έχουμε και δολιοφθορές. Αποτέλεσμα όλων των παραπάνω είναι οι τοπολογίες των δικτύων αισθητήρων να υπόκεινται σε συχνές αλλαγές.

1.3.3 Φάση εγκατάστασης επιπλέον κόμβων.

Επιπλέον κόμβοι είναι δυνατόν να εγκατασταθούν οποιαδήποτε χρονική στιγμή για να αντικαταστήσουν τους κόμβους που παρουσιάζουν δυσλειτουργίες ή λόγω αλλαγών στον αρχικό σκοπό για τον οποίο εγκαταστάθηκαν. Η πρόσθεση νέων κόμβων στο δίκτυο δημιουργεί την ανάγκη για επαναδιοργάνωση. Προκειμένου να αντιμετωπίσουμε τις συχνές αλλαγές στην τοπολογία ενός ασύρματου δικτύου αισθητήρων, το οποίο αποτελείται από ένα μεγάλο αριθμό κόμβων με μεγάλους περιορισμούς στην κατανάλωση ενέργειας χρειαζόμαστε ειδικά σχεδιασμένα πρωτόκολλα δρομολόγησης.

1.4 Περιβάλλον.

Οι αισθητήριοι κόμβοι εγκαθίστανται πυκνά είτε πολύ κοντά είτε κατευθείαν μέσα στο παρατηρούμενο φαινόμενο. Έτσι συνήθως εργάζονται χωρίς παρακολούθηση σε απομακρυσμένες γεωγραφικές περιοχές. Είναι δυνατόν να εργάζονται :

- Στο εσωτερικό ενός μεγάλου μηχανήματος.
- Στα βάθη του ωκεανού.
- Μέσα σε ένα κυκλώνα.
- Στην επιφάνεια ενός ωκεανού στην διάρκεια μια καταιγίδας.
- Σε μια περιοχή μολυσμένη από ραδιενέργεια ή χημικές ουσίες.
- Στο πεδίο της μάχης πίσω από τις γραμμές του εχθρού.
- Σε ένα σπίτι ή σε ένα μεγάλο κτίριο.
- Σε μια μεγάλη αποθήκη.
- Εμφυτευμένοι σε ζώα.

- Ενσωματωμένοι σε ταχέως κινούμενα οχήματα.
- Στα νερά ενός ποταμού.

Η παραπάνω λίστα εφαρμογών μας δίνει μια ιδέα για τις συνθήκες κάτω από τις οποίες λειτουργούν οι αισθητήριοι κόμβοι. Λειτουργούν σε συνθήκες υψηλής πίεσης στα βάθη ενός ωκεανού, στο σκληρό περιβάλλον ενός πεδίου μάχης, σε συνθήκες υψηλών ή χαμηλών θερμοκρασιών όπως η μύτη ενός αεροσκάφους ή σε συνθήκες υψηλού περιβαλλοντολογικού θορύβου.

1.5 Μέσα Μετάδοσης.

Σε ένα δίκτυο αισθητήρων, οι επικοινωνούντες κόμβοι συνδέονται ασύρματα. Αυτές οι ζεύξεις μπορούν να υλοποιηθούν από ραδιοσυχνότητες, υπέρυθρα ή οπτικά μέσα. Προκειμένου να έχουμε λειτουργία σε παγκόσμιο επίπεδο πρέπει να διαλέξουμε ένα μέσο το οποίο θα είναι διαθέσιμο παντού στον κόσμο.

Μια επιλογή για ασύρματες ζεύξεις είναι η χρήση της Βιομηχανικής, Επιστημονικής και Ιατρικής Μπάντας (Industrial Scientific Medical ISM Band), η οποία προσφέρεται χωρίς άδεια χρήσης στις περισσότερες χώρες. Κάποιες από αυτές τις συχνότητες χρησιμοποιούνται ήδη για επικοινωνία σε ασύρματα τηλέφωνα ή τοπικά ασύρματα δίκτυα (WLANs). Για τα δίκτυα αισθητήρων απαιτείται ένας μικρού μεγέθους, χαμηλού κόστους και πολύ χαμηλής ενέργειας πομποδέκτης. Σύμφωνα με το, υπάρχουν συγκεκριμένοι περιορισμοί στο υλικό, και το ανταλλαγή ανάμεσα στην αποτελεσματικότητα της κεραίας και την εξοικονόμηση ενέργειας περιορίζουν την επιλογή μιας συχνότητας για αυτούς τους πομποδέκτες στις πολύ υψηλές συχνότητες. Επίσης προτείνεται η χρήση των 433MHz στην Ευρώπη και των 915MHz στην Β. Αμερική.

Το κύριο πλεονέκτημα χρήσης των συχνοτήτων ISM είναι η δωρεάν χρήση, το τεράστιο φάσμα και η παγκόσμια διαθεσιμότητα. Δεν περιορίζονται από κάποιο συγκεκριμένο πρότυπο και έτσι δίνουν μεγαλύτερη ελευθερία στην υλοποίηση τεχνικών που θα εξοικονομούν ενέργεια στα δίκτυα ασύρματων αισθητήρων. Από την άλλη μεριά υπάρχουν διάφοροι κανόνες και περιορισμοί, όπως της ενέργειας και των παρεμβολών από ήδη υπάρχουσες εφαρμογές.

Οι περισσότερες διαθέσιμες εφαρμογές για δίκτυα αισθητήρων βασίζονται στην επικοινωνία με ραδιοσυχνότητες. Το μAMPS χρησιμοποιεί ένα πομποδέκτη συμβατό με Bluetooth στα 2.4 GHz με ένα ενσωματωμένο συνθέτη συχνοτήτων. Ο αισθητήρας χαμηλής ενέργειας χρησιμοποιεί πομποδέκτη ραδιοσυχνότητας ενός

καναλιού που λειτουργεί στα 916 MHz. Η αρχιτεκτονική WINS χρησιμοποιεί επίσης ραδιοσυχνότητες για την επικοινωνία μεταξύ των κόμβων.

Ένα άλλος πιθανός τρόπος επικοινωνίας είναι μέσω υπερύθρων. Η επικοινωνία μέσω υπερύθρων μπορεί να γίνει χωρίς άδεια χρήσης και είναι ανθεκτική στις παρεμβολές από ηλεκτρικές συσκευές. Οι πομποδέκτες υπερύθρων είναι φθηνότεροι και ευκολότεροι να κατασκευαστούν. Πολλές από τις σημερινές συσκευές όπως τηλέφωνα υπολογιστές κατασκευάζονται έχοντας ενσωματωμένο ένα πομποδέκτη υπερύθρων. Το μόνο μειονέκτημα τους είναι η απαίτηση για οπτική επαφή μεταξύ των επικοινωνούντων συσκευών. Το τελευταίο κάνει αποτρεπτική την επιλογή για χρήση υπερύθρων σαν μέσο μετάδοσης σε δίκτυα ασύρματων αισθητήρων.

Μια ενδιαφέρουσα λύση είναι αυτή του αισθητήρα «έξυπνης σκόνης» (smart dust mote), ο οποίος είναι ένα αυτόνομο σύστημα αισθήσεως και επεξεργασίας που χρησιμοποιεί οπτικό μέσο μετάδοσης. Δύο επιλογές για οπτική μετάδοση εξετάζονται στο μια παθητική και μια ενεργητική. Στην πρώτη περίπτωση δεν είναι απαραίτητη η ύπαρξη κάποιας ενσωματωμένης πηγής φωτός. Στην δεύτερη περίπτωση χρησιμοποιείται μια ενσωματωμένη δίοδος laser και ένα ανάλογο σύστημα επικοινωνίας προκειμένου να αποσταλεί μια δέσμη φωτός προς τον σκοπευμένο δέκτη.

Οι συνήθεις απαιτήσεις των εφαρμογών για τις οποίες χρησιμοποιούνται τα δίκτυα αισθητήρων δημιουργούν μεγάλη πρόκληση στην επιλογή ενός μέσου μετάδοσης. Για παράδειγμα σε εφαρμογές που μπορούν να είναι υποθαλάσσιες μπορεί να απαιτείται η χρήση του νερού ως μέσου μετάδοσης. Επιπλέον λόγω του ότι η κεραία ενός αισθητήρα μπορεί να μην έχει το απαιτούμενο ύψος ή ισχύ εκπομπής εκτός από την επιλογή του μέσου, μεγάλο ρόλο παίζει η χρήση ισχυρής κωδικοποίησης και η επιλογή συχνότητας προκειμένου να γίνει στο έπακρο εκμετάλλευση των χαρακτηριστικών του καναλιού.

1.6 Κατανάλωση ενέργειας.

Ο ασύρματος αισθητήριος κόμβος, αφού είναι μια μικρό-ηλεκτρονική συσκευή μπορεί να εφοδιαστεί με μια περιορισμένη πηγή ενέργειας (<0.5 Ah, 1.2V). Η αντικατάσταση αυτής της πηγής ενέργειας συνήθως είναι αδύνατη, συνεπώς η ζωή του αισθητήριου κόμβου εξαρτάται από αυτήν. Σε ένα δίκτυο αισθητήρων ο κάθε κόμβος παίζει το ρόλο του αποστολέα αλλά και του δρομολογητή. Τυχόν βλάβες σε

κάποιους από τους κόμβους δημιουργούν ανάγκη για αναδιοργάνωση του δικτύου και επαναδρομολόγηση των μηνυμάτων. Συνεπώς η σωστή διαχείριση της ενέργειας των κόμβων παίζει μεγάλο ρόλο. Η κατανάλωση ενέργειας μπορεί να αποδοθεί σε τρεις λειτουργίες: αίσθηση, επικοινωνία και επεξεργασία δεδομένων.

1.7 Επικοινωνία.

Η πιο απαιτητική λειτουργία από άποψη κατανάλωσης ενέργειας είναι η επικοινωνία. Συνήθως για τις μικρές αποστάσεις που λειτουργούν οι αισθητήριοι κόμβοι η κατανάλωση είναι ίδια κατά την εκπομπή και την λήψη. Βεβαίως, εκτός από αυτό, σοβαρό ρόλο παίζει και το άνοιγμα και κλείσιμο του κυκλώματος του πομποδέκτη. Η εξίσωση για την κατανάλωση της ενέργειας κατά την ασύρματη επικοινωνία είναι η ακόλουθη :

$$P_c = N_T\left[P_T\left(T_{on} + T_{st}\right) + P_{out}\left(T_{on}\right)\right] + N_R\left[P_R\left(R_{on} + R_{st}\right)\right] \qquad \textbf{(1.3)}$$

Όπου $P_{T/R}$ είναι η ενέργεια που καταναλώνεται από τον πομπό/ δέκτη, P_{out} η ενέργεια εξόδου του πομπού, T/R_{on} ο χρόνος που ο πομπός/ δέκτης είναι ενεργός, T/R_{st} ο χρόνος έναρξης του πομπού/ δέκτη και $N_{T/R}$ ο αριθμός των φορών που ο πομπός/ δέκτης ανοίγει στην μονάδα του χρόνου, ο οποίος και εξαρτάται από το ανατιθέμενο σκοπό αλλά και το πρωτόκολλο στο επίπεδο ζεύξης δεδομένων (MAC Layer). Οι σημερινοί πομποδέκτες έχουν τυπικές τιμές P_T και P_R περίπου στα 20 dbm και P_{out} κοντά στα 0 dbm.. φέρεται ο σχεδιασμός ενός χαμηλού κόστους και μικρού μεγέθους και μικρής ενέργειας πομποδέκτη.

1.8 Επεξεργασία δεδομένων.

Η καταναλισκόμενη ενέργεια είναι μικρότερη κατά την φάση της επεξεργασίας των δεδομένων σε σχέση με την επικοινωνία. Συνεπώς θα πρέπει ο κόμβος να έχει ενσωματωμένο κύκλωμα επεξεργασίας προκειμένου να επεξεργάζεται τα δεδομένα με απώτερο σκοπό να στέλνει το δυνατόν λιγότερα πακέτα κατά την φάση της επικοινωνίας. Η ενέργεια που καταναλώνει ένας επεξεργαστής εξαρτάται από την τάση και την συχνότητα λειτουργίας. Συνεπώς αν μειώσουμε τους δύο αυτούς παράγοντες θα έχουμε και μείωση της καταναλισκόμενης ενέργειας. Βέβαια θα πρέπει να συμβιβαστούμε διότι και η ικανότητα επεξεργασίας θα μειωθεί. Μια άλλη εναλλακτική είναι να εκμεταλλευτούμε το γεγονός ότι ο επεξεργαστής εργάζεται λίγες φορές στο μέγιστο της απόδοσής του και έτσι μπορούμε να έχουμε

ένα δυναμικό τρόπο αυξομείωσης του ρεύματος και της συχνότητας λειτουργίας του. Υπάρχουν τρόποι προκειμένου η δυναμική λειτουργία του επεξεργαστή να είναι όσο το δυνατόν πιο κοντά στις απαιτήσεις και να μειωθεί η απαιτούμενη ενέργεια.

<u>*Η ενέργεια που σπαταλάται μπορεί να δοθεί ως εξής*</u> :

$$P_p = CV_{dd}^2 f_T + V_{dd} I_0 e^{\frac{V_{dd}}{n'V_T}} \qquad \textbf{(1.4)}$$

όπου C είναι η ολική χωρητικότητα μεταγωγής (total switching capacitance), V_{dd} η τάση και f η συχνότητα αλλαγής.

ΚΕΦΑΛΑΙΟ 2ο

ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΔΙΚΤΥΩΝ ΑΙΣΘΗΤΗΡΩΝ

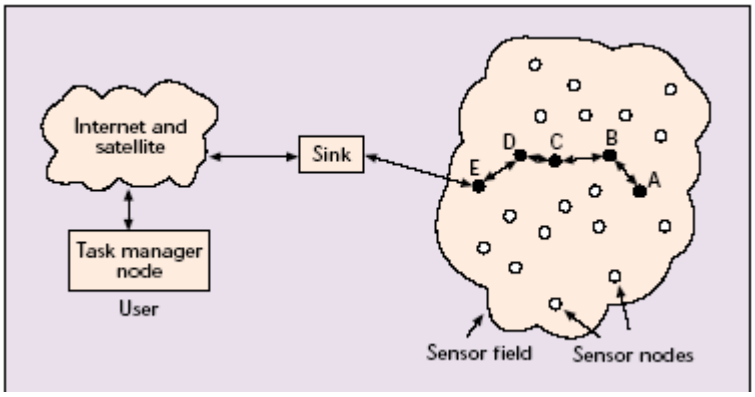
2.1 ΔΙΚΤΥΑ ΑΙΣΘΗΤΗΡΩΝ-ΣΦΑΙΡΙΚΗ ΑΠΟΨΗ ΚΑΙ ΑΠΑΙΤΗΣΕΙΣ

Έχουμε αναγνωρίσει έναν αριθμό χαρακτηριστικών των δικτύων των αισθητήρων τα οποία έχουν επιδράσει κατευθείαν στις αρχιτεκτονικές και σχεδιαστικές αποφάσεις. Αυτά τα χαρακτηριστικά προέρχονται φυσικά από απαιτήσεις και ανάγκες της τεχνολογίας.

Αυτά τα χαρακτηριστικά περιλαμβάνουν χαμηλό κόστος,μικρό μέγεθος,χαμηλή κατανάλωση ισχύος,ευρώστεια,ευκαμψία, ελαστικότητα σε λάθη και σφάλματα,αυτονομία λειτουργίας και συχνά ασφάλεια και μυστικότητα.

Τα δίκτυα αισθητήρων έχουν έξι στοιχεία: επεξεργαστή, πομποδέκτη, αποθηκευτικό χώρο, αισθητήρες και συσσωρευτή. Υπάρχει ένας αριθμός με σχετικά τεχνολογικά στοιχεία τα οποία πρέπει να εξεταστούν, π.χ. μια τεράστια ποικιλία από πανίσχυρες τεχνολογίες χαμηλής ισχύος, χαμηλής τιμής επεξεργαστές και χαμηλής τιμής μνήμης που είναι προσιτές, Επίσης, η μνήμη και ο επεξεργαστής γίνονται όλο και περισσότερο ισχυρά σύμφωνα με τον νόμο του Moore, και το ασύρματο εύρος ζώνης έχει μεγαλώσει περισσότερο του 25% στα τελευταία 5 χρόνια. Η χωριτικότητα των μπαταριών έχει αυξηθεί με ρυθμό χαμηλό και ίσο του 3% τον χρόνο. Το κόστος ειδικά σχεδιασμένων εφαρμογών έχει αυξηθεί αστραπιαία.

Οι ασύρματοι κόμβοι διασπείρονται σε ένα πεδίο όπως φαίνεται και στην ***Εικόνα 2.1.*** Κάθε ένας από αυτούς συλλέγει δεδομένα, τα επεξεργάζεται και τα στέλνει πίσω σε

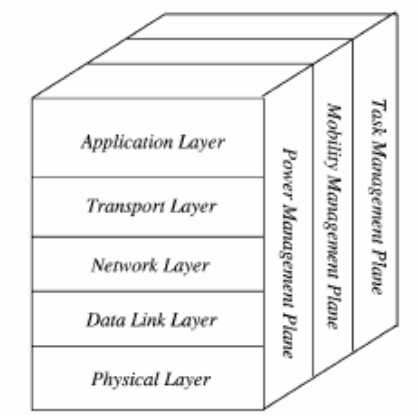


Εικόνα 2.1. Διασπορά ασύρματων κόμβων σε ένα πεδίο παρακολούθησης. **(1)**

ένα κεντρικό σημείο και από εκεί καταλήγουν στους ενδιαφερόμενους χρήστες.

Η στοίβα πρωτοκόλλου που χρησιμοποιείται από το κεντρικό σημείο αλλά και από όλους τους κόμβους φαίνεται στην ***Εικόνα 2.2.***.

Όπως φαίνεται αποτελείται από τα εξής επίπεδα: φυσικό, ζεύξης δεδομένων, δικτύου, μεταφοράς και εφαρμογής, καθώς και από τα κάτωθι επίπεδα διαχείρισης (management planes) ενέργειας, κινήσεως και στόχου.



Εικόνα 2.2. Η στοίβα πρωτοκόλλου των δικτύων αισθητήρων***. [2]***

Τα τρία τελευταία επίπεδα διαχείρισης βοηθούν τους αισθητήριους κόμβους να συνεργαστούν καλύτερα ο ένας με τον άλλο προκειμένου να φέρουν σε πέρας τον σκοπό για τον οποίο εγκαταστάθηκαν καταναλώνοντας όσο το δυνατόν λιγότερη ενέργεια. Τα υπόλοιπα επίπεδα λειτουργούν ανάλογα με αυτά του προτύπου OSI

2.2Μικρό φυσικό μέγεθος

Η μείωση του φυσικού μεγέθους πάντα ήταν το κλειδί σχεδιασμού. Γι'αυτό το λόγο, ο στόχος είναι η παροχή ισχυρού επεξεργαστή μνήμης, του πομποδέκτη και άλλων συστατικών διατηρώντας δικαιολογημένα μικρό μέγεθος περιγράφοντας συγκεκριμένες εφαρμογές.

2.3Χαμηλή κατανάλωση ισχύος

Η ικανότητα, ο χρόνος ζωής και η παρουσία των αισθητήρων, όλα πηγάζουν από την ενέργεια. Οι αισθητήρες μπορούν να είναι ενεργοί για μια μεγάλη περίοδο χρόνου χωρίς επαναφόρτωση της μπαταρίας, λόγω του ότι η συντήρηση είναι δαπανηρή.

2.4 Ενταντική λειτουργία

Προκειμένου να είναι επιτυχής όλη η παρουσία των κόμβων αισθητήρων, οι αισθητήρες πληροφοριών πρέπει να δεσμεύονται,να επεξεργάζονται, να συμπιέζονται και μετά να στέλνονται στο δίκτυο στιγμιαία, με pipelined επεξεργασία, σε αντίθεση με τις συνήθεις διαδικασίες. Εδώ υπάρχουν δύο σχετικές προσεγγίσεις:

I. Διαίρεση του επεξεργαστή σε πολλές μονάδες όπου κάθε μία είναι προσδιορισμένη να είναι υπεύθυνη για συγκεκριμένο σκοπό.
II. Αλλαγή στην εκτέλεση διεργασιών του κόμβου.

2.5 Ποικιλία στη χρήση και στον σχεδιασμό

Αφού θέλουμε τον κάθε κόμβο να είναι μικρού μεγέθους, χαμηλό στην κατανάλωση ισχύος και να έχει περιορισμένες φυσικές ομοιότητες, οι κόμβοι αισθητήρων τείνουν να είναι ειδικής εφαρμογής. Παρόλ'αυτά οι διαφορετικοί αισθητήρες έχουν διαφορετικές απαιτήσεις, π.χ. οι κάμερες και τα απλά θερμόμετρα είναι τα δύο ακραία κατά τη διάρκεια της λειτουργίας και της πολυπλοκότητας. Γι'αυτό, ο σχειδιασμός πρέπει να απλοποιεί τις συναλλαγές μεταξύ της επαναχρησιμότητας, του κόστους και της ικανότητας.

2.6 Ευέλικτες λειτουργίες

Αφού οι αισθητήρες τείνουν να αναπτυχθούν πάνω σε ένα μεγάλο και μερικές φορές εχθρικό περιβάλλον (δάση,στρατιωτικές εφαρμογές, ανθρώπινο σώμα) αναμένουμε τους αισθητήρες να είναι ανεκτικοί στα λάθη και σφάλματα. Γι'αυτό, οι αισθητήριοι κόμβοι χρειάζονται δυνατότητες αυτοελέγχου, αυοεξακρίβωσης και αυτοεπισκευής.

2.7 Ασφάλεια

Κάθε αισθητήρας πρέπει να έχει επαρκείς μηχανισμούς ασφάλειας προκειμένου να εμποδίσει μη εξουσιοδοτημένη πρόσβαση, επιθέσεις και άσκοπες καταστροφές πληροφοριών εντός του κόμβου δικτύου αισθητήρων. Παρ'ολα αυτά, πρόσθετοι μηχανισμοί μυστικότητας πρέπει να συμπεριλαμβάνονται.

2.8 Ευκαμψία

Υπάρχει η ανάγκη να συμβιβαστούν οι λειτουργικές και χρονικές αλλαγές. Η ευκαμψία μπορεί να επιτευχθεί μέσω δύο εννοιών:

I. Ικανότητα προγραμματισμού με την χρήση μικροεπεξεργαστών,DSP επεξεργαστών και μικροελεγκτών.
II. Αναδιαμόρφωση της λειτουργίας τους χρησιμοποιώντας τις FPGA

2.9 Στοιχεία Κόμβων δικτύων αισθητήρων

Τα δίκτυα αισθητήρων έχουν έξι στοιχεία: επεξεργαστή, μονάδα αποθήκευσης, πομποδέκτη, αισθητήρες και υποσυστήματα προμήθειας ισχύος. Είναι γεγονός ότι ο κυρίως επεξεργαστής μεγαλώνει με το DSP και τους άλλους επεξεργαστές και έτσι κάποιες μονάδες ASIC θα παρέχουν δυνατότητες επεξεργασίας. Επίσης, η έννοια των αισθητήρων είναι τέτοια,έτσι ώστε,αυτοί να μην χρησιμοποιούνται στην δημιουργία των αισθητήριων κόμβων δικτύου.

2.10 Χωρητικότητα (αποθηκευτικών μέσων)

Όλη η δομή των αισθητήρων δικτύου, καθώς και οι απαιτήσεις για χωρητικότητα σε κάθε κόμβο, πρέπει να είναι πολύ διαφορετική.Υπάρχουν τουλάχιστον δύο εναλλακτικές λύσεις για αποθήκευση πληροφοριών σε τοπικό κόμβο. Αντιθέτως, στην περίπτωση που ο κόμβος είναι μεγαλύτερος από την φύση του, κάποιος μπορεί να αποθηκεύσει την πληροφορία σε micro discs. Η πρώτη επιλογή είναι να χρησιμοποιηθούν μνήμες τύπου flash. Οι flash μνήμες είναι πολύ ελκυστικές σε σχέση με το κόστος και την χωρητικότητα αποθήκευσης την οποία παρέχουν. Παρ'όλα αυτά, έχει αυστηρούς, συγκριτικά, περιορισμούς σε σχέση με το πόσες φορές μπορεί να χρησιμοποιηθεί για αποθήκευση πληροφοριών στις ίδιες φυσικές τοποθεσίες. Η δεύτερη επιλογή είναι να χρησιμοποιήσει nano ηλεκτρονικά βασισμένα σε MRAM. Αναμενόταν ότι το MRAM θα είχε σύντομα σημαντικές εφαρμογές σε αριθμό περιοχών. Είναι αναγκαίο να σημειωθεί ότι οι non-volatile ημιαγωγοί και η χωρητικότητα αποθήκευσης δίσκου δημιουργήθηκαν σε βαθμό υψηλότερο από ότι στο νόμο του Moore. Η διαίρεση για μείωση ισχύος και η ανάπτυξη δομών μνήμης θα βοηθούσε το μήκος των λέξεων της πληροφορίας, να παράγεται από τους αισθητήρες.

2.11 Παροχή ισχύος

Είναι ευρέως αποδεκτό ότι η ενέργεια θα είναι ένας από τους κύριους τεχνολογικούς περιορισμούς για τους αισθητήριους κόμβους του δικτύου. Υπάρχουν δύο τουλάχιστον διαφορετικές μέθοδοι σύμφωνα με τις οποίες το πρόβλημα της παροχής ενέργειας μπορεί να επιλυθεί. Η πρώτη είναι να εξοπλιστεί κάθε κόμβος με μία (επαναφορτιζόμενη) πηγή ενέργειας. Συνήθως, η κυρίαρχη επιλογή είναι να χρησιμοποιηθούν κυψέλες μπαταρίας υψηλής πυκνότητας. Η άλλη εναλλακτική για αυτή την επιλογή είναι να χρησιμοποιηθούν ολοκληρωμένες κυψέλες. Αυτές παρέχουν υψηλή πυκνότητα και καθαρή πηγή ενέργειας. Παρ'όλα αυτά, συνήθως αυτά δεν διατίθεται σε μεγέθη που να ταιριάζουν για κόμβους δικτύων αισθητήρων. Η δεύτερη εναλλακτική μέθοδος είναι η συγκέντρωση από το περιβάλλον διαθέσιμης ενέργειας,όπως ηλιακή, ηλεκτρομαγνητική, μηχανική.

2.12 Αισθητήρες

Ο σκοπός των αισθητήριων κόμβων δικτύου δεν είναι ούτε ο υπολογισμός ούτε η επικοινωνία, παρά, η αίσθηση. Το κύριο συστατικό των κόμβων αισθητήρων δικτύου είναι η τρέχουσα περιορισμένη τεχνολογία. Επίσης, οι ημιαγωγοί παρέχονται στο πραγματικό φυσικό κόσμο, ενώ οι υπολογιστικές και επικοινωνιακές μονάδες έχουν να κάνουν με κάποια ελεγχόμενα περιβάλλοντα. Οι μορφομετατροπείς (transducers) είναι τα απαιτούμενα συστατικά σε κόμβους αισθητήρων και χρησιμοποιούνται να μετατρέψουν την μία μορφή ενέργειας σε άλλη. Σε αντίθεση, οι αισθητήρες μπορούν να έχουν 4 άλλα συστατικά: analog, A/D, ψηφιακά και μεκροελεγκτή. Η πιο καλή επιλογή σχεδιασμού περιλαμβάνει μόνο τον transducer. Παρ'όλα αυτά, η τρέχουσα τάση είναι να τοποθετείς όλο και πιο πολύ «εξυπνάδα» μέσα στους αισθητήριους κόμβους του δικτύου. Γι'αυτό, οι δυνατότητες επεξεργασίας καθώς και υπολογισμού έχουν προστεθεί στους κόμβους αισθητήρων. Παρατηρούμε ότι η επιλογή του τύπου και η ποιότητα αισθητήρων καθώς και η απόφαση για την τοποθέτησή τους, αποτελούν μία από τις κύριες προκλήσεις του δικτύου αισθητήρων. Το έργο αυτό είναι δύσκολο γιατί υπάρχουν πάρα πολλοί τύποι αισθητήρων με διαφορετικές ιδιότητες όπως η resolution, το κόστος, η ακρίβεια, το μέγεθος και η κατανάλωση ισχύος. Αντιθέτως, συχνά, περισσότεροι τους ενός αισθητήρα χρειάζονται να διασφαλίσουν την ακρίβεια των λειτουργιών και πληροφοριών από έναν διαφορετικό αισθητήρα που πιθανόν να συνδέεται. Άλλη πρόκληση είναι να επιλεγεί ο σωστός τύπος αισθητήρων και ο τρόπος λειτουργίας τους. Η πηγή δυσκολίας είναι η αλληεπόδραση των αισθητήρων π.χ. θεωρείστε τον υπολογισμό της απόστασης, χρησιμοποιώντας ακουστικούς αισθητήρες. Αφού η

ταχύτητα του ήχου εξαρτάται από τη θερμοκρασία και την υγρασία του περιβάλλοντος, είναι απαραίτητο να παρθούν μετρήσεις και για τα δύο προκειμένου να πάρουμε την ακριβή απόσταση. Επίσης υπάρχουν κάποια άλλα έργα σχεδιασμού που συνδέονται με τους αισθητήρες και συμπεριλαμβάνουν σφάλμα ανοχής, λάθος ελέγχου, λειτουργίες επαναφοράς και χρόνο συγχρονισμού.

2.13 Πομποδέκτες

Οι πομποδέκτες ως συστατικά επικοινωνίας είναι αναμφισβήτητα σημαντικοί γιατί ο προϋπολογισμός ενέργειας που αφιερώνεται στην αποστολή και λήψη μηνυμάτων συνήθως καλύπτει όλο το μπάτζετ ενέργειας. Κατά τη διάρκεια του σχεδιασμού και επιλογής των πομποδεκτών, ένας πρέπει να συγκεντρωθεί σε τουλάχιστον τρία διαφορετικά στρώματα: φυσικό, MAC και δικτύου. Το φυσικό στρώμα χειρίζεται την επικοινωνία μεταξύ των πομπών και δικτύων, παρά το γεγονός της εκατάστασης των φυσικών δεσμών. Τα κύρια έργα συνδέουν την αλλοίωση σήματος και κωδικοποίηση πληροφορίας, έτσι ώστε οι δέκτες να μπορούν να αποκωδικοποιήσουν τα παραληφθέντα μηνύματα παρουσία των καναλιών θορύβου και παρεμβολών. Προκειμένου να πετύχει η χρήση του εύρους ζώνης συχνοτήτων και κατά κάποιο τρόπο η μείωση του αναπτυγμένου κόστους, συχνά κάποιοι πομποδέκτες πρέπει να μοιράζονται το ίδιο συνδεόμενο μέσο. Σε αυτή την περίπτωση, υπάρχει η ανάγκη για coordinated access policy. Αυτό είναι ένα έργο το οποίο επιλύεται στο στρώμα MAC. Τέλος, το στρώμα δικτύου είναι υπεύθυνο για την εύρεση μονοπατιού από το οποίο πρέπει να περάσει το μήνυμα στους κόμβους του δικτύου προκειμένου να τεξιδέψει από την πηγή στον προορισμό. Ο σχεδιασμός πομποδέκτη είναι μία μεγάλη επίτευξη των σημερινών ερευνών. Κατά κάποιο τρόπο, η αρχιτεκτονική του πομποδέκτη συγκρούεται με την δομή του δικτύου και τα πρωτόκολλα. Η κύρια ανταλλαγή είναι μεταξύ του σχετικού κόστους ενέργειας μετάδοσης και λήψης. Η βασική παρατήρηση είναι ότι η ακοή του καναλιού είναι ακριβή. Γι'αυτό, χρειάζεται να υιοθετήσουμε τρόπους χρήσης των κόμβων και του δικτύου, οι οποίοι θα καθιστούν ικανές περιόδους μακράς σιγής για τους δέκτες. Για παράδειγμα, μία επιλογή είναι να χρησιμοποιήσουμε coordinated policy για να αποφασιστεί ποιός κόμβος θα συνεχίσει να ΄΄κοιμάται΄΄ ενώ η συνδετικότητα στον κόμβο θα διατηρείται. Η άλλη επιλογή είναι η χρησιμοποίηση δύο πομποδεκτών. Ένας από αυτούς είναι υπεύθυνος για λήψη πληροφορίας και δαπανά πολλή ισχύ. Χρησιμοποιείται μόνο όταν ο άλλος ο πολύ χαμηλός πομποδέκτης επικαλείται αυτό.

Ο πολύ χαμηλός πομποδέκτης ισχύος χρησιμοποιείται μόνο για να ερευνήσει εάν κάποιος θέλει να μεταδώσει πληροφορίες στον κόμβο.

2.14 Κόμβος Δικτύου αισθητήρων

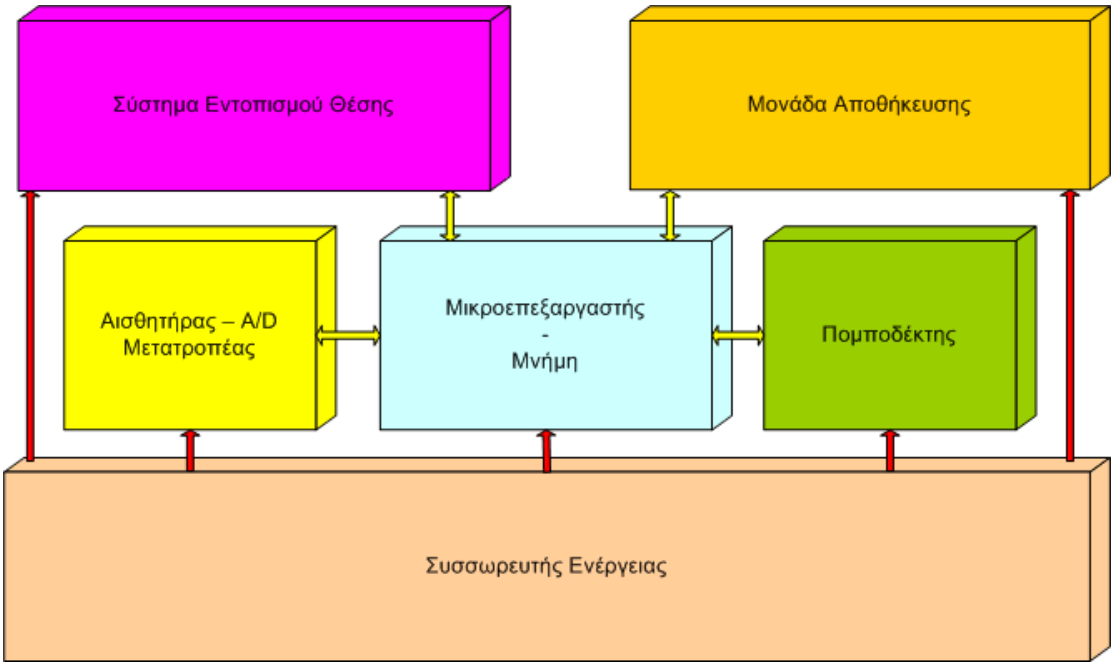
Οι απόψεις της αρχιτεκτονικής παρουσιάζονται μέσα από τις τρεις οδούς: **hardware, λογισμικό & middleware**, ενώ ο σχεδιασμός, παρουσιάζεται από τη σύνθεση και την ανάλυση των σημείων. Έχουν υπάρξει τρεις τουλάχιστον κύριες κατευθύνσεις κατά τις οποίες οι αρχιτεκτονικές των κόμβων δικτύων αισθητήρων έχουν απευθυνθεί. Το πρώτο group προσπαθειών είναι ένας αριθμός σχεδιασμού ξεχωριστών αισθητήρων κόμβων. Η έμφαση σε αυτή την προσπάθεια, έγινε στη διασφάλιση της δημιουργίας προτοτύπου εργασίας και σε μερικές περιπτώσεις στην αρχή της τέχνης των ξεχωριστών συστατικών. Το δεύτερο group παρουσιάσθηκε από το TinyOS group. Ήταν η πρώτη προσπάθεια που επιχείρησε να απευθύνει ανταλλαγές μεταξύ σημαντικών συστατικών του κόμβου με την ανάπτυξη νέου OS και η τελική προσπάθεια επικεντρώνεται στον αισθητήρα. Η έμφαση είναι στην εκμετάλλευση συγγενικών, μη δαπανηρών, συστατικών σχετικά με την ενέργεια, προκειμένου να μειώσει την επικοινωνία, την κατανάλωση ενέργειας, τόσο καλά, έτσι ώστε να οδηγήσει και να εκμεταλευθεί ποιοτικές ανταλλαγές μεταξύ στοιχείων κόμβων και των καθ'αυτών αισθητήρων. Είναι δύσκολο να προβλέψεις τεχνολογικές εξελίξεις αλλά μπορείς εύκολα να αναγνωρίσεις μερικές συγκρουόμενες έρευνες ,για παράδειγμα είναι φαινόμενο ότι χρειάζονται ισορροπημένες αρχιτεκτονικές για την ολική κατανάλωση ενέργειας. Άλλη σύγκρουση είναι η οργάνωση αισθητήρων και η ανάπτυξη της επιφάνειας, του κενού μεταξύ συστατικών. Τέλος εξαιτίας της μυστικότητας, της ασφάλειας και των αναγκών αυθεντικότητας, τεχνικές όπως η μοναδική ID για το CPU και τα άλλα συστατικά θα μπορούσαν να είναι υψηλής σημασίας.

Στο ***software*** η κύρια έμφαση θα είναι στο πραγματικό χρόνο λειτουργίας συστήματος (RTOS). Υπάρχει η ανάγκη για ακραία επιθετική και χαμηλής ισχύος διοίκηση, εξαιτίας των αναγκών ενέργειας. Επίσης υπάρχει η ανάγκη για περιεκτική πηγή λογαριασμού, εξαιτίας των απαιτήσεων για μυστικότητα και ασφάλεια που υποστηρίζουν επίσης την ευκινησία λειτουργιών (π.χ. εύρεση τοποθεσιών).

Το ***middleware***, είναι απαραίτητο για την ανάπτυξη νέων εφαρμογών. Έργα όπως το φιλτράρισμα πληροφορίας των αισθητήρων, συμπίεση, επεξεργασία

πληροφορίας αισθητήρα, η έρευνα πληροφορίας του αισθητήρα και η ασφάλεια έκθεσης καθώς και αναζήτησης θα είναι πανταχού παρών.

Στο παρακάτω σχήμα παρουσιάζονται τα συστατικά του αισθητήριου κόμβου.



Σχήμα 2.3 Συστατικά του αισθητήριου κόμβου

ΚΕΦΑΛΑΙΟ 3^{ο}

ΕΦΑΡΜΟΓΕΣ ΔΙΚΤΥΩΝ ΑΙΣΘΗΤΗΡΩΝ.

3.1Υφιστάμενες εφαρμογές

Τα δίκτυα αισθητήρων μπορούν να αποτελούνται από πολλούς διαφορετικούς τύπους αισθητήρων όπως σεισμικών, μαγνητικών χαμηλού ρυθμού δειγματοληψίας, θερμικών, οπτικών, υπερύθρων, ακουστικών και ραντάρ, οι οποίοι είναι ικανοί να παρακολουθούν μια ευρεία ποικιλομορφία περιβαλλοντολογικών συνθηκών και φαινομένων που περιλαμβάνουν τα ακόλουθα :

- Θερμοκρασία
- Υγρασία
- Κίνηση οχημάτων
- Συνθήκες φωτός.
- Πίεση.
- Διάρθρωση εδάφους.
- Επίπεδα θορύβου.
- Την παρουσία ή απουσία προκαθορισμένων ειδών αντικειμένων.
- Επίπεδα μηχανικής πίεσης σε προσκολλημένα αντικείμενα και
- Τα τρέχοντα χαρακτηριστικά όπως ταχύτητα, κατεύθυνση και μέγεθος ενός αντικειμένου.

Οι αισθητήριοι κόμβοι μπορούν να χρησιμοποιηθούν για συνεχή ανίχνευση, ανίχνευση συμβάντων, ανίχνευση ταυτοτήτων γεγονότων, ανίχνευση θέσης και τοπικό έλεγχο μηχανισμών κίνησης. Η ιδέα της μικρό-ανίχνευσης και της ασύρματης σύνδεσης αυτών των κόμβων υπόσχεται πολλές νέες περιοχές εφαρμογών. Οι εφαρμογές των δικτύων αισθητήρων μπορούν να ομαδοποιηθούν σε στρατιωτικές, υγείας, περιβάλλοντος, οικιακές και εμπορικές. Είναι δυνατόν να επεκτείνουμε την ομαδοποίηση με περισσότερες κατηγορίες όπως εξερεύνηση του διαστήματος, χημική επεξεργασία, αντιμετώπιση καταστροφών κ.α.

3.2 Στρατιωτικές Εφαρμογές.

Τα ασύρματα δίκτυα αισθητήρων μπορούν να είναι ένα ενσωματωμένο κομμάτι των στρατιωτικών συστημάτων διαταγών, ελέγχου, επικοινωνιών, υπολογισμού, ευφυΐας, παρακολούθησης, αναγνωρίσεων και στόχευσης. Τα χαρακτηριστικά των δικτύων αισθητήρων, όπως η ταχεία εγκατάσταση, η αυτό-οργάνωση και η αντοχή σε λάθη, τους κατατάσσουν σε ένα πολύ υποσχόμενο αισθητήριο μέσο για τα παραπάνω συστήματα. Καθώς τα δίκτυα αισθητήρων βασίζονται στην πυκνή χωρική εγκατάσταση, η καταστροφή μερικών κόμβων από εχθρικές δυνάμεις δεν επηρεάζει μια στρατιωτική επιχείρηση σε τέτοιο βαθμό όσο η καταστροφή των παραδοσιακών αισθητήρων, κάνοντας την χρήση των δικτύων αισθητήρων ιδανική για τα πεδία των μαχών. Κάποιες από τις στρατιωτικές εφαρμογές των δικτύων αισθητήρων είναι η παρακολούθηση των φιλικών δυνάμεων, του εξοπλισμού και των πυρομαχικών τους, η παρακολούθηση του πεδίου της μάχης, η αναγνώριση των εχθρικών δυνάμεων και του εδάφους, η στόχευση, η αποτίμηση των ζημιών της μάχης, καθώς και η ανίχνευση και αναγνώριση μιας ΡαδιοΒιολογικήςΧημικής και Πυρηνικής (ΡΒΧΠ) απειλής.

3.2.1Παρακολούθηση εξοπλισμού και πυρομαχικών των φίλιων δυνάμεων:

Οι ηγέτες και οι διοικητές μπορούν χρησιμοποιώντας τα δίκτυα αισθητήρων να παρακολουθούν την κατάσταση των τμημάτων τους καθώς και του εξοπλισμού και των πυρομαχικών τους. Κάθε στρατιώτης, όχημα, εξοπλισμός και κρίσιμο οπλικό σύστημα μπορεί να εξοπλιστεί με αισθητήρες που θα αναφέρουν την κατάστασή του. Αυτές οι αναφορές συγκεντρώνονται σε κεντρικούς κόμβους και προωθούνται προς τους διοικητές των τμημάτων. Τα δεδομένα μπορούν επίσης να προωθηθούν και σε μεγαλύτερα ιεραρχικά κλιμάκια αθροισμένα με δεδομένα από άλλες μονάδες του ίδιου επιπέδου.

3.2.2Παρακολούθηση του πεδίου της μάχης

Κρίσιμα εδάφη, δρομολόγια προσέγγισης, μονοπάτια και στενωποί μπορούν γρήγορα να καλυφθούν με δίκτυα αισθητήρων και να παρακολουθούνται στενά για εχθρικές δραστηριότητες. Καθώς οι επιχειρήσεις θα εξελίσσονται και θα ετοιμάζονται νέα επιχειρησιακά σχέδια, μπορούν κάθε φορά να εγκαθίστανται νέα δίκτυα αισθητήρων που θα καλύπτουν τις νέες ανάγκες.

3.2.3Αναγνώριση των εχθρικών δυνάμεων και του εδάφους

Τα δίκτυα αισθητήρων μπορούν να εγκατασταθούν σε κρίσιμα εδάφη και να συγκεντρώνουν έγκαιρα πολύτιμες και λεπτομερείς πληροφορίες για τις εχθρικές δυνάμεις και το έδάφος σε ελάχιστα λεπτά, προτού οι εχθρικές δυνάμεις να μπορέσουν να αναχαιτίσουν τα δίκτυα.

3.2.4Στόχευση

Τα δίκτυα αισθητήρων μπορούν να εμφυτευτούν σε συστήματα πλοήγησης των έξυπνων πυρομαχικών.

3.2.5Εκτίμηση των ζημιών μάχης

Πριν ή μετά από κάποια επίθεση δίκτυα αισθητήρων μπορούν να εγκατασταθούν στην περιοχή του στόχου ή των στόχων για να συγκεντρώσουν πληροφορίες προκειμένου να γίνει εκτίμηση των ζημιών.

3.2.6Ανίχνευση και αναγνώριση ΡΒΧΠ

Στον ΡΒΧΠ πόλεμο, όταν είσαι κοντά στο σημείο μηδέν (σημείο έκρηξης ΡΒΧΠ όπλου) είναι σημαντικό να διαθέτεις ακριβή και έγκαιρη πληροφορία για την ύπαρξη μόλυνσης. Τα δίκτυα αισθητήρων τα οποία εγκαθίστανται στην φίλια περιοχή και χρησιμοποιούνται σαν συστήματα αναγνώρισης και προειδοποίηση ΡΒΧΠ ουσιών, μπορούν να παρέχουν στις φίλιες δυνάμεις κρίσιμο χρόνο για να αντιδράσουν, και να μειώσουν δραστικά τις απώλειες. Τα δίκτυα αισθητήρων μπορούν επίσης να χρησιμοποιηθούν για την αναγνώριση μιας περιοχής που προσβλήθηκε από ΡΒΧΠ επίθεση χωρίς να είναι αναγκαίο να εκτεθεί μια ομάδα ανίχνευσης στην ραδιενέργεια.

3.3Περιβαλλοντολογικές Εφαρμογές.

Μερικές περιβαλλοντολογικές εφαρμογές των δικτύων αισθητήρων περιλαμβάνουν την παρακολούθηση των κινήσεων των πουλιών, μικρών ζώων και εντόμων, την παρακολούθηση των περιβαλλοντολογικών συνθηκών που επηρεάζουν την χλωρίδα και την πανίδα, την άρδευση, την εντολή σειράς ενεργειών για παρακολούθηση μεγάλης κλίμακας της γης και την εξερεύνηση του πλανήτη, την χημική και βιολογική ανίχνευση, την ακριβή γεωργία, την βιολογική και περιβαλλοντολογική παρακολούθηση της θάλασσας, του εδάφους και του αέρα, την

παρακολούθηση για φωτιές στα δάση, την μετεωρολογική και γεωφυσική έρευνα, την ανίχνευση πλημμύρων, την ανίχνευση σύνθετων ζωντανών οργανισμών του περιβάλλοντος, καθώς και την μελέτη μολύνσεων.

3.4 Ανίχνευση δασικών πυρκαγιών

Καθώς οι αισθητήριοι κόμβοι μπορούν να εγκατασταθούν στρατηγικά, τυχαία και πυκνά σε ένα δάσος, μπορούν να αναμεταδώσουν την ακριβή προέλευση της φωτιάς στους άμεσα ενδιαφερόμενους προτού η πυρκαγιά εξαπλωθεί ανεξέλεγκτα. Εκατομμύρια αισθητήριων κόμβων μπορούν εγκατασταθούν και να δημιουργήσουν ένα ολοκληρωμένο κύκλωμα χρησιμοποιώντας ασύρματες συχνότητες και οπτικά συστήματα. Επίσης μπορούν να εξοπλιστούν με αποτελεσματικές μεθόδους εκμετάλλευσης της ενέργειας όπως ηλιακές κυψέλες προκειμένου να λειτουργούν απρόσκοπτα χωρίς παρακολούθηση για μήνες ή και χρόνια. Οι αισθητήριοι κόμβοι μπορούν να συνεργάζονται ο ένας με τον άλλο προκειμένου να εκτελούν κατανεμημένη ανίχνευση και να υπερπηδούν εμπόδια όπως βράχια και δέντρα, που παρεμποδίζουν το πεδίο ανίχνευσης.

3.5 Ανίχνευση σύνθετων βιολογικών οργανισμών του περιβάλλοντος

Μια τέτοια ανίχνευση απαιτεί εξεζητημένες προσεγγίσεις για τον συνδυασμό των πληροφοριών χρόνου και χώρου. Η εξέλιξη των τεχνολογιών στον τομέα της ασύρματης ανίχνευσης και της αυτόματης συλλογής δεδομένων έχουν δώσει μεγαλύτερη φασματική, χωρική και χρονική ανάλυση με γεωμετρικά μειούμενο το κόστος ανά μονάδα περιοχής. Μαζί με αυτές τις εξελίξεις, οι αισθητήριοι κόμβοι έχουν επίσης την δυνατότητα να συνδέονται με το διαδίκτυο, το οποίο επιτρέπει σε απομακρυσμένους χρήστες να ελέγχουν, να παρακολουθούν και να παρατηρούν την βιοσυνθετικότητα του περιβάλλοντος.

Αν και οι δορυφορικοί και αεροπορικοί αισθητήρες είναι χρήσιμοι στην παρακολούθηση μεγάλης κλίμακας βιοδιαφορών, π.χ. χωρική πολυπλοκότητα των επικρατούντων ειδών φυτών, δεν έχουν δυνατότητα για διαχωρισμό των μικρών βιοδιαφορών οι οποίες είναι και οι περισσότερες σε ένα οικοσύστημα. Σαν αποτέλεσμα, είναι αναγκαία η εγκατάσταση ενός δικτύου ασύρματων αισθητήρων στο έδαφος για την παρακολούθηση της βιοσυνθετικότητας. Ένα παράδειγμα απεικόνισης της βιοσυνθετηκότητας του περιβάλλοντος έγινε στο καταφύγιο James στην Νότια Καλιφόρνια. Τρία παρακολουθούμενα πλέγματα από τα οποία το καθένα

είχε 25-100 αισθητήριους κόμβους υλοποιήθηκαν για σταθερή πολυμεσική θέα και συγκέντρωση πληροφοριών σε ημερολόγια περιβαλλοντολογικής φύσης.

3.6 Ανίχνευση πλημμύρων

Ένα παράδειγμα συστήματος ανίχνευσης πλημμύρων είναι το σύστημα ALERT το οποίο αναπτύχθηκε στις ΗΠΑ. Διάφοροι τύποι αισθητήρων αναπτύχθηκαν στο σύστημα ALERT όπως βροχόπτωσης, μέτρησης επιπέδων του νερού και καιρού. Αυτοί οι αισθητήρες παρέχουν πληροφορίες σε ένα κεντρικό σύστημα Βάσης Δεδομένων με ένα προκαθορισμένο τρόπο. Σχέδια έρευνας όπως το COUGAR στο πανεπιστήμιο του Cornell και το σχέδιο DataSpace στο πανεπιστήμιο του Rutgers, είναι κατανεμημένες προσεγγίσεις στην αλληλεπίδραση με αισθητήριους κόμβους στο πεδίο που αυτοί εγκαθίστανται για την παροχή απαντήσεων σε στιγμιαία και μακροπρόθεσμα ερωτήματα.

3.7Γεωργία Ακρίβειας (Precision Agriculture)

Κάποια από τα πλεονεκτήματα των δικτύων αισθητήρων είναι η ικανότητα της παρακολούθησης ακριβών επιπέδων του πόσιμου νερού, του επιπέδου διάβρωσης του εδάφους και του επιπέδου μόλυνσης του αέρα σε πραγματικό χρόνο.

3.8Εφαρμογές Υγείας.

Κάποιες από τις εφαρμογές των δικτύων αισθητήρων είναι : Παροχή μέσων αλληλεπίδρασης για άτομα με ειδικές ανάγκες, παρακολούθηση ασθενών, διάγνωση, διαχείριση φαρμάκων σε νοσοκομεία, παρακολούθηση των κινήσεων και των εσωτερικών διεργασιών των εντόμων και άλλων μικρών ζώων, τηλεπαρακολούθηση των φυσιολογικών δεδομένων ενός ανθρώπου καθώς και εντοπισμός και παρακολούθηση των γιατρών και ασθενών σε ένα νοσοκομείο.

3.8.1Τηλεπαρακολούθηση των φυσιολογικών δεδομένων ενός ατόμου :

Τα φυσιολογικά δεδομένα που συγκεντρώνονται από ένα δίκτυο αισθητήρων μπορούν να αποθηκευθούν για ένα μεγάλο χρονικό διάστημα, και μπορούν να χρησιμοποιηθούν για ιατρική εξερεύνηση. Το εγκατεστημένο δίκτυο αισθητήρων μπορεί επίσης να παρακολουθεί και να ανιχνεύει την συμπεριφορά ηλικιωμένων ατόμων, π.χ. μια πτώση. Αυτοί οι μικροί κόμβοι αισθητήρων επιτρέπουν στο άτομο μεγαλύτερη ελευθερία κινήσεων και επιτρέπουν στους γιατρούς να αναγνωρίσουν

προκαθορισμένα συμπτώματα έγκαιρα. Επίσης παρέχουν μια καλύτερη ποιότητα ζωής για τα άτομα σε σύγκριση με τα κέντρα παροχής θεραπείας. Ένα «έξυπνο σπίτι υγείας» έχει σχεδιαστεί στο Faculty της φαρμακευτικής στην Grenoble της Γαλλίας προκειμένου να εκτιμηθεί η δυνατότητα ύπαρξης ενός τέτοιου συστήματος.

3.8.2Εντοπισμός και παρακολούθηση γιατρών ασθενών ενός νοσοκομείου :

Κάθε ασθενής μπορεί να έχει προσκολλημένους μικρούς και ελαφρείς αισθητήριους κόμβους. Κάθε αισθητήριος κόμβος έχει ένα συγκεκριμένο σκοπό. Για παράδειγμα ένας αισθητήριος κόμβος μπορεί να ανιχνεύει τον καρδιακό χτύπο ενώ ένας άλλος να ανιχνεύει την πίεση του αίματος. Οι γιατροί επίσης μπορούν να κουβαλούν έναν αισθητήριο κόμβο, που θα στον εντοπισμό τους μέσα στο νοσοκομείο.

3.8.3Διαχείριση φαρμάκων σε ένα νοσοκομείο :

Με την εγκατάσταση αισθητήριων κόμβων σε φάρμακα, μπορούμε να ελαχιστοποιήσουμε την πιθανότητα να πάρει κάποιος ασθενής λάθος φαρμακευτική αγωγή. Αυτό θα συμβεί αν και οι ασθενείς έχουν αισθητήριους κόμβους που θα αναγνωρίζουν τις αλλεργίες τους και τις απαιτούμενες θεραπείες. Υπολογιστικά συστήματα έχουν δείξει ότι μπορούν να βοηθήσουν στην ελαχιστοποίηση των επιρροών από λάθος φάρμακα.

3.9 Οικιακές Εφαρμογές.

3.9.1 Αυτοματισμός σπιτιού

Καθώς η τεχνολογία εξελίσσεται, έξυπνοι αισθητήριοι κόμβοι και μηχανισμοί κίνησης μπορούν να εμφυτευτούν σε συσκευές, όπως ηλεκτρικές σκούπες, φούρνοι μικροκυμάτων, ψυγεία και βίντεο. Αυτοί οι αισθητήριοι κόμβοι μπορούν να αλληλεπιδρούν ο ένας με τον άλλον καθώς και με ένα εξωτερικό δίκτυο μέσω του Διαδικτύου ή ενός δορυφόρου. Επιτρέπουν στους τελικούς χρήστες να διαχειρίζονται τις οικιακές συσκευές τους από όπου βρίσκονται είτε τοπικά είτε απομακρυσμένα.

3.9.2Έξυπνο περιβάλλον

Ο σχεδιασμός ενός έξυπνου περιβάλλοντος μπορεί να έχει δύο διαφορετικές προοπτικές δηλ. ανθρωποκεντρική και τεχνοκεντρική. Για την άνθρωπο-κεντρική προσέγγιση, ένα έξυπνο περιβάλλον πρέπει να προσαρμοστεί στις ανάγκες των τελικών χρηστών σε ότι αφορά στις δυνατότητες εισόδου και εξόδου. Για την

τεχνοκεντρική προσέγγιση, νέες τεχνολογίες υλικού, δικτυακές λύσεις και ενδιάμεσες συσκευές πρέπει να αναπτυχθούν. Οι αισθητήριοι κόμβοι μπορούν να χρησιμοποιηθούν για να δημιουργήσουν ένα έξυπνο περιβάλλον. Οι αισθητήριοι κόμβοι μπορούν να εμφυτευτούν στην επίπλωση και σε οικιακές συσκευές και μπορούν να επικοινωνούν ο ένας με τον άλλον καθώς και με τον εξυπηρετητή του δωματίου. Ο εξυπηρετητής δωματίου μπορεί επίσης να επικοινωνεί με εξυπηρετητές από άλλα δωμάτια για να μαθαίνει για τις υπηρεσίες που μπορούν να προσφέρουν π.χ. εκτύπωση, σάρωση και αποστολή και λήψη φαξ. Αυτοί οι εξυπηρετητές δωματίων μπορούν να ενσωματωθούν με υπάρχουσες εμφυτευμένες συσκευές ώστε να γίνουν αυτό-οργανωτικοί, αυτό-ρυθμιζόμενοι, και προσαρμοζόμενοι σε θεωρητικά μοντέλα. Ένα άλλο παράδειγμα έξυπνου περιβάλλοντος είναι η «εργαστηριακή κατοικία» στο Ινστιτούτο τεχνολογίας της Georgia. Οι υπολογισμοί και η αίσθηση σε αυτό το περιβάλλον πρέπει να είναι αξιόπιστοι, συνεχείς και διαφανείς.

3.10 Άλλες εμπορικές Εφαρμογές.

Μερικές από τις εμπορικές εφαρμογές είναι η παρακολούθηση της καταπόνησης των υλικών, η κατασκευή κάθετων κατασκευών, η διαχείριση αποθεμάτων, η παρακολούθηση της ποιότητας της παραγωγής, η κατασκευή έξυπνων χώρων γραφείου, ο περιβαλλοντολογικός έλεγχος σε συγκροτήματα γραφείων, ο έλεγχος των ρομπότ και η καθοδήγηση σε περιβάλλοντα αυτόματης κατασκευής, αλληλεπιδραστικά παιχνίδια, αλληλεπιδραστικά μουσεία, ο έλεγχος των βιομηχανικών διεργασιών και αυτοματισμών, η παρακολούθηση περιοχών καταστροφής, οι έξυπνες κατασκευές με αισθητήριους κόμβους εμφυτευμένους σε αυτές, η διάγνωση μηχανών, οι μεταφορές, η εγκατάσταση βιομηχανικών οργάνων, ο τοπικός έλεγχος μηχανισμών κίνησης, η ανίχνευση και παρακολούθηση κλεφτών αυτοκινήτων, ο εντοπισμός και ανίχνευση κινούμενων οχημάτων.

3.11 Περιβαλλοντολογικός έλεγχος σε συγκροτήματα γραφείων

Ο κλιματισμός και η θέρμανση των περισσοτέρων κτιρίων ελέγχεται κεντρικά. Έτσι η θερμοκρασία σε κάθε δωμάτιο μπορεί να διαφέρει αρκετούς βαθμούς από πλευρά σε πλευρά (δηλ. μια πλευρά μπορεί να είναι θερμότερη από την άλλη διότι ο έλεγχος στο δωμάτιο και η ροή του αέρα από το κεντρικό σύστημα δεν είναι ομοιόμορφα κατανεμημένη). Ένα κατανεμημένο δίκτυο ασύρματων αισθητήρων μπορεί να εγκατασταθεί για να ελέγχει την ροή του αέρα και την

θερμοκρασία σε διάφορα κομμάτια του δωματίου. Έχει εκτιμηθεί ότι τέτοια κατανεμημένη τεχνολογία μπορεί να μειώσει την κατανάλωση ενέργειας κατά δύο BTUs στις ΗΠΑ, που αντιστοιχεί σε μια εξοικονόμηση $55 δις το χρόνο και μείωση στην εκπομπή υδρογονανθράκων κατά 35 εκατ. τόνους.

3.12Αλληλεπιδραστικά Μουσεία

Στο μέλλον τα παιδιά θα είναι ικανά να αλληλεπιδρούν με αντικείμενα στα μουσεία για να μπορούν να μαθαίνουν περισσότερο γι' αυτά. Αυτά τα αντικείμενα θα είναι ικανά να ανταποκριθούν στο άγγιγμα και στην ομιλία του επισκέπτη. Επίσης τα παιδιά μπορούν να συμμετάσχουν σε ένα πραγματικού χρόνου πείραμα δράσης και αντίδρασης, το οποίο μπορεί να τα διδάξει για το περιβάλλον και την επιστήμη. Επιπλέον τα δίκτυα ασύρματων αισθητήρων μπορούν να παρέχουν ομαδοποίηση και εντοπισμό σε ένα μουσείο. Ένα παράδειγμα τέτοιων μουσείων είναι στο San Franciso Exploratorium που παρέχει ένα συνδυασμό μετρικών δεδομένων και πειραμάτων δράσης και αντίδρασης.

3.13Ανίχνευση και παρακολούθηση κλοπών οχημάτων

Αισθητήριοι κόμβοι μπορούν να εγκατασταθούν προκειμένου να ανιχνεύσουν και να αναγνωρίσουν απειλές μέσα σε μια γεωγραφική περιοχή και κατόπιν να αναφέρουν αυτές τις απειλές σε απομακρυσμένους χρήστες μέσω του Διαδικτύου για ανάλυση.

3.14Παρακολούθηση και ανίχνευση οχημάτων

Υπάρχουν δύο προσεγγίσεις στην παρακολούθηση και ανίχνευση ενός οχήματος. Η πρώτη είναι ότι η κατεύθυνση του οχήματος αποφασίζεται τοπικά εντός των κόμβων και κατόπιν στέλνεται κεντρικά στον σταθμό βάσης και δεύτερη είναι ότι τα δεδομένα όπως συλλέγονται από τους αισθητήριους κόμβους προωθούνται στον σταθμό βάσης για να αποφασιστεί η θέση του οχήματος.

3.15Διαχείριση και έλεγχος αποθεμάτων

Κάθε αντικείμενο σε μια αποθήκη μπορεί να έχει ένα αισθητήριο κόμβο προσκολλημένο πάνω του . Ο τελικός χρήστης μπορεί να εντοπίσει την ακριβή θέση του αντικειμένου και να μετρήσει τα αντικείμενα της ίδιας κατηγορίας. Αν οι τελικοί χρήστες επιθυμούν να εισάγουν νέα αποθέματα, το μόνο που χρειάζεται να κάνουν είναι να προσκολλήσουν τους κατάλληλους αισθητήριους κόμβους στα αποθέματα

αυτά. Οι τελικοί χρήστες μπορούν να εντοπίσουν και να παρακολουθήσουν που βρίσκονται τα αποθέματα κάθε χρονική στιγμή.

ΚΕΦΑΛΑΙΟ 4ο

ΑΣΦΑΛΕΙΑ ΣΤΑ WSN

4.1Απαιτήσεις Ασφάλειας – Ιδιαιτερότητες των WSN

Η ασφάλεια δικτύου, είναι μία από τις σημαντικότερες ανησυχίες σε όλα τα ασύρματα δίκτυα, συμπεριλαμβανομένου και των ασύρματων δικτύων αισθητήρων. Στο κεφάλαιο αυτό θα παρουσιάσουμε το πρόβλημα ασφάλειας και θα εξηγήσουμε κάποια από τα ειδικά χαρακτηριστικά των ασυρμάτων δικτύων αισθητήρων. Οι σχειδιαστές τωνδικτύων πρέπει να προσέχουν και να επιλέγουν, μηχανοσμούς που να επιτυγχάνουν, έναν ή περισσότερους από τους ακόλουθους στόχους ασφαλείας.

4.2Διαθεσιμότητα

Η σημασία της είναι ότι τα προσόντα δικτύου είναι διαθέσιμα, για να εξουσιοδοτούν τμήματα, όταν χρειάζεται.Επίσης τα ασύρματα δίκτυα αισθητήρων πρέπει να διασφαλίζουν, τη βιωσιμότητα των υπηρεσιών του δικτύου, παρά την άρνηση των επιθέσεων στις υπηρεσίες (denial of service DOS) οι οποίες μπορούν να φορτωθούν σε οποιοδήποτε στρώμα των WSN. Για την διασφάλιση της διαθεσιμότητας της προστασίας μηνυμάτων, το ασύρματο δίκτυο αισθητήρων πρέπει να προστατεύει τις πηγές του (όπως αισθητήριοι κόμβοι), από τα μη απαραίτητα επαξεργασμένα μηνύματα από το κλειδί διοίκησης, προκειμένου να ελαχιστοποιήσει την κατανάλωση ενέργειας και να επεκτείνει τη ζωή του δικτύου.

4.3Αυθεντικότητα

Στα ασύρματα δίκτυα αισθητήρων, η αυθεντικότητα είναι απαραίτητη για πολλούς εκτελεστικούς σκοπούς (π.χ. επαναπρογραμματισμός δικτύου ή έλεγχος κύκλου ασφαλείας σε αισθητήριο κόμβο). Κατά την ίδια στιγμή, ένας εχθρός, μπορεί εύκολα να εισχωρήσει μηνύματα, όπότε ο δέκτης χρειάζεται να βεβαιωθεί ότι η πληροφορία χρησιμοποιήθηκε σε οποιαδήποτε μέθοδο λήψης απόφασης, και προέρχεται από την αξιόπιστη πηγή. Η αυθεντικότητα πληροφορίας, επιτρέπει στον δέκτη, να επιβεβαιώσει ότι η πληροφορία, στάλθηκε τοπικά από τον ισχυρίζοντα

αποστολέα. Σκληρότερα επίπεδα αυθεντικότητας (όπως αποκαλυπτικό κλειδί αυθεντικότητας), παρέχονται από κάποια βεβαιωμένα πρωτόκολλα. Παρ'όλα αυτά, τα περισσότερα WSN σενάρια, δεν απαιτούν την επιπλέον «ασφάλεια» και μπορούν να επιβεβαιώσουν κλειδιά παράδοσης, χρησιμοποιώντας, ένα σύστημα εφαρμογής πρωτοκόλλων. Η υπηρεσία αυτή πρέπει να είναι σωστή και έξυπνη αρκετά, έτσι ώστε μόνο τα εξουσιοδοτημένα μερη να μπορούν να χρησιμοποιούν το σύστημα. Επίσης, δεν πρέπει να αρνείται εξουσιοδοτημένα τμήματα από τη χρήση του συστήματος δικτύου.

4.4Εμπιστευτικότητα

Ένα εμπιστευτικό μήνυμα αντιστέκεται στην αποκάλυψη της σημασίας του σε έναν εισβολέα. Ακόμη και οι απ'ευθείας πληροφορίες στα WSN, χρειάζονται να παραμένουν εμπιστευτικές, αφού μπορεί να έχουν χρησιμοποιηθεί, σε μία DOS απειλή. Η κύρια λύση να διατηρήσει τη αυαίσθητη πληροφορία μυστική, είναι να κωδικοποιήσει την πληροφορία, με ένα μυστικό κλειδί το οποίο θα έχουν στην κατοχή τους, μόνο οι προτιθέμενοι δέκτες, γι'αυτό και επιτυγχάνεται η εμπιστευτικότητα. Η εμπιστευτικότητα πρέπει να παρέχεται με κλειδιά με ένα μικρό αντικείμενο(κλειδί κοκκοποιημένο) για να αποθαρύνει ένα απλό σπάσιμο από ένα συμβιβασμό μίας μεγάλης μερίδας του δικτύου αισθητήρων. Με άλλα λόγια, προτιμούνται, βεβαιωμένα μοναδικά κλειδιά μεταξύ κάθε ζεύγους κόμβου αισθητήρων επικοινωνίας σε μία ασφάλεια, στην χρησιμοποίηση ενός κλειδιού απλού δικτύου. Η υπηρεσία αυτή σημαίνει την προστασία της πληροφορίας που έχει μεταφερθεί από το δίκτυο από παθητικές επιθέσεις. Η υπηρεσία εκπομπής μέσων πρέπει να προστατευθεί από τις σταλμένες πληροφορίες από τους χρήστες. Άλλοι τύποι αυτής της υπηρεσίας εμπεριέχουν την ασφάλεια ενός απλού μηνύματος ή ενός συγκεκριμένου πεδίου του μηνύματος. Άλλη μια άποψη της εμπιστευτικότητας είναι η προστασία της κυκλοφορίας από έναν hacker που προσπαθεί να το αναλύσει. Με άλλα λόγια, πρέπει να υπάρχουν κάποια μέτρα τα οποία αρνούνται οι hackers από την παρατήρηση της συχνότητας και το μήκος της ενέργειας, τόσο καλά όσο άλλα χαρακτηριστικά κυκλοφορίας στο δίκτυο

4.5 Μη αποποίηση.

Η υπηρεσία αυτή εμποδίζει την αποστολή ή λήψη τμήματος από την άρνηση των σταλμένων ή παραληφθέντων μηνυμάτων. Αυτό σημαίνει ότι όταν ένα μήνυμα

παραλαμβάνεται, ο αποστολέας μπορεί να επιβεβαιώσει ότι το μήνυμα παρελήφθη πράγματι από τον υποτιθέμενο δέκτη

4.6 Ανανέωση-Φρεσκάδα

Αυτό θα μπορούσε να σημαίνει ανανέωση πληροφορίας και ανανέωση κλειδιού. Αφού όλα τα δίκτυα αισθητήρων παρέχουν κάποιες δομές χρόνου ποικίλων καταμετρήσεων, πρέπει να διασφαλίσουμε ότι κάθε μήνυμα είναι φρέσκο. Η ανανέωση πληροφορίας, συνεπάγεται ότι η πληροφορία είναι πρόσφατή και αυτό διασφαλίζει ότι κανένας εχθρός δεν έχει ξαναγράψει παλαιά μηνύματα. Ένα κλειδί βεβαιωμένης μεθόδου, μεταξύ των εμπλεκομένων μπορεί να εγγυηθεί ότι κάθε κλειδί μοιρασμένο είναι καινούργιο(δεν έχει ξαναχρησιμοποιηθεί από κανέναν από τους εμπλεκόμενους). Αυτό επίσης σημαίνει ότι ένα κλειδί, χρησιμοποιείται σε έναν κρυπτογραφικό συνδυασμό, δεν έχει χρησιμοποιηθεί σε άλλο συνδυασμό. Γι'αυτό τα μοιραζόμενα κλειδιά είναι αναγκαίο να αλλάζουν διαρκώς, αφού ένα κλειδί μπορεί να συβιβαστεί, κατά την διάρκεια της προανάτπυξης ή της λειτουργίας των φάσεων ενός WSN.

4.7 Ακεραιότητα πληροφορίας

Οι μετρήσεις ακεραιότητας, διασφαλίζουν ότι οι ληφθείσες πληροφορίες, δεν διαφοροποιήθηκαν κατά την μεταφορά από έναν εισβολέα. Η υπηρεσία της ακεραιότητας μπορεί να δημιουργηθεί, χρησιμοποιώντας κρυπτογραφικές λειτουργίες,κομμένες σε κομμάτια, με κάποια μέθοδο κωδικοποίησης.Η υπηρεσία της ακεραιότητας παρέχεται συχνά και απεριόριστα, από την υπηρεσία της αυθεντικότητας, προκειμένου να εξασφαλιστεί η ασφάλεια του δικτύου.

Διαφοροποιούμαστε μεταξύ των προσανατολισμένων συνδέσεων και των συνδέσεων που βασίζονται στις υπηρεσίες ακεραιότητας. Η υπηρεσία ακεραιότητας της προσανατολισμένης σύνδεσης, έρχεται αντιμέτωπη με πολλά μηνύματα και διαβεβαιώνει ότι τα μηνύματα στάλθηκαν χωρίς αναπαραγωγή εις διπλούν, τροποποίηση ή απάντηση. Εκτός απ' αυτό, η άρνηση της άποψης της επαναπαραγγελίας της υπηρεσίας κρύβεται κάτω απ' την υπηρεσία της προσανατολισμένης σύνδεσης. Η υπηρεσία ακεραιότητας της έλλειψης σύνδεσης έχει να κάνει μόνο με την προστασία ενάντια της τροποποίησης μηνυμάτων. Ένας

υβριδικός τύπος της υπηρεσίας της ακεραιότητας είχε προταθεί να κάνει με τις εφαρμογές που απαιτούν προστασία εναντίον της επαναπαραγγελίας , αλλά χρειάζεται αυστηρή ακολουθία. Ένα καλό ασφαλές σύστημα θα ήταν ικανό να ανιχνεύσει οποιοδήποτε πρόβλημα ακεραιότητας και αν μια παράβαση της διαπιστωθεί, τότε η υπηρεσία πρέπει να αναφέρει αυτό το πρόβλημα. Ένας μηχανισμός software ή παρέμβαση ανθρώπινη θα μπορούσε να λυθεί το πρόβλημα. Η προσέγγιση λογισμικού υποτίθεται να λύσει το πρόβλημα αυτόματα χωρίς παρέμβαση ανθρώπινη.

4.8 Διαθεσιμότητα

Κάποιες επιθέσεις μπορούν να έχουν ως αποτέλεσμα την απώλεια ή ελάττωση της διαθεσιμότητας του συστήματος. Κάποια από αυτά τα προβλήματα μπορούν να επιλυθούν, ενώ κάποια άλλα απαιτούν κάποιους τύπους φυσικών διαδικασιών.

4.9Επεκτασιμότητα και αυτό-οργάνωση

Σε αντίθεση με τα γενικά ad-hoc δίκτυα, τα οποία δεν είναι επεκτάσιμα, κατά κύρια προτεραιότητα, τα WSN, δεν μπορούν να χρησιμοποιήσουν βασικό διάγραμμα ο οποίο έχει φτωχές επεκτάσιμες ιδιότητες (είτε σε σχέση με το κόστος ενέργειας είτε με την αφάνεια). Γενικά, ο αριθμός των γειτόνων και οι αποστάσεις ή η απαιτούμενη ισχύς για την αποστολή μηνυμάτων με συγκεκριμένη εκτίμηση λάθους από έναν κόμβο στον άλλον, δεν θα είναι γνωστά στο μέλλον. Σαν συνέπεια οι κόμβοι των WSN πρέπει να είναι ικανοί να αυτοοργανώνονται και να επιλέγουν τους βασικούς μηχανισμούς που ταιριάζουν για την κάθε κατάσταση.

ΚΕΦΑΛΑΙΟ 5ο

Απειλές- Αντίμετρα

Μπορούν οι μετρήσεις ασφάλειας και τα κρυπτογραφικά πρωτόκολλα στα ασύρματα δίκτυα αισθητήρων να θεωρούνται τα ίδια με τους άλλους τύπους των δικτύων? Οι περισσότεροι συμφωνούν με την άποψη ότι η απάντηση είναι **«όχι»** για τους ακόλουθους λόγους:

1. Η δομή δικτύου ενός WSN είναι φτιαγμένη από μικρούς και μη δαπανηρούς κόμβους απλωμένους σε ένα πιθανό εχθρικό περιβάλλον.
2. Σε αντίθεση με άλλους τύπους δικτύων, είναι συχνά αδύνατον οι αισθητήριοι κόμβοι να αποτραπούν από τη φυσική προσβολή εισβολέων. Αυτό άλλωστε αναφέρεται ως αιχμαλωσία κόμβου.

Είναι δικαιολογημένο να υποθέσουμε ότι ένας εισβολέας μπορεί να επιτύχει ολικό έλεγχο πάνω σε ένα αιχμάλωτο κόμβο, και να διαβάσει τη μνήμη του ή να επιδράσει στη λειτουργία του λογισμικού κόμβου. Ειδικές ασφαλείς εντολές ή μνήμες θα χρειάζονταν να αποτρέψουν το διάβασμα της μνήμης από τον εισβολέα. .

Οι περιορισμοί σχετικά με τη μνήμη και τις υπολογιστικές ικανότητες αποτελούν σοβαρό εμπόδιο για χρήση κρυπτογραφικών αλγορίθμων. Ειδικότερα, η ασύμμετρη κρυπτογράφηση κλειδιών θεωρείτε πολύ «βαριά» για μικρούς επεξεργαστές, χωρίς να μνημονεύσουμε την εμπλοκή του κλειδιού διοίκησης.

Οι ενδιάμεσοι κόμβοι χρειάζονται να προσβάλλουν και να τροποποιήσουν την πληροφορία που εμπεριέχεται σε πακέτα μ, γι'αυτό ένας μεγάλος αριθμός τμημάτων εμπλέκεται σε μεταφορές πληροφοριών από τέλος σε τέλος (end to end).

Ο περιορισμένος προϋπολογισμός ενέργειας των αισθητήριων κόμβων κάνει διαθέσιμη μία σχετικά μεγάλη σειρά από επιθέσεις: Αναγκάζουν τα θύματα ΄΄κόμβους΄΄ να χρησιμοποιούν όλη την ενέργεια τους γρήγορα και να πεθαίνουν.

Επίσης, οι επιτιθέμενοι έχουν περισσότερη ενέργεια.Τέλος,όλες οι μετρήσεις ασφάλειας επιτυγχάνονται από τον αισθητήριο κόμβο με επιπλέον ενέργεια και η

πίεση των κόμβων από απειλές μπορεί να αποφέρει πρόωρη εξάντληση της μπαταρίας. Αυτό ισούται με την επιθεση denial-of-service(DOS).

5.1 Οι DOS επιθέσεις γενικά μπορούν να προσπαθήσουν

- να απενεργοποιήσουν λειτουργίες ή
- να κενώσουν τους προμηθευτές λειτουργιών π.χ. υπερλειτουργώντας.

Για την απενεργοποίηση λειτουργίας του δικτύου αισθητήρων ο εισβολέας μπορεί απλά να καταστρέψει τους κόμβους.

Παρόλο που τα δίκτυα αισθητήρων μπορούν να επανέρθουν σε περίπτωση αποτυχίας κόμβων, ο εισβολέας μπορεί να αλλοιώσει το δίκτυο, καταστρέφοντας μεγάλο αριθμό κόμβων ή επικεντρώνοντας το ενδιαφέρον του σε σημαντικούς κόμβους. Παρ'όλα αυτά, παρακάτω, θα αναλύσουμε πρωτόκολλα που συσχετίζονται με τις επιθέσεις, τύπου DOS.

5.2 Φυσικό στρώμα και επιθέσεις σε αυτό

Με τον συνωστισμό του φυσικού στρώματος, ένας εισβολέας απλά αλλοιώνει την επικοινωνία πομποδεκτών. Ένας τρόπος για να το πετύχει αυτό, είναι να τοποθετήσει ο εισβολέας κόμβους κάπου μέσα στο δίκτυο και να τους αφήσει συνεχώς να στέλνουν σήματα πομποδεκτών στην μπάντα συχνοτήτων του δικτύου αισθητήρων. Ειδικά αποτελεσματική είναι τέτοια επίθεση όταν οι κόμβοι του εισβολέα είναι κοντά στους κόμβους sink, μειώνοντας αποτελεσματικά την δυνατότητα του χρήστη να ελέγχει το δίκτυο ή να αποκτά πληροφορία από αυτό. Ένας απλός κόμβος εισβολέα μπορεί να αλλοιώσει πολλούς γειτονικούς σε μία φορά και με την στρατηγική θέση που έχουν οι κόμβοι του εισβολέα, μπορεί όλο το δίκτυο αισθητήρων να απενεργοποιηθεί. Ένα τρίτο μέτρο πρόληψης μπορεί να γίνει από πρωτόκολλα δρομολόγησης. Εάν ο εισβολέας συνωστίζει μόνο μία περιορισμένη περιοχή, πακέτα μπορεί να ορίζονται τριγύρω. Σε πρωτόκολλα μπορεί να βρει διευθύνσεις εργασίας. Τέλος, κόμβοι αισθητήρων με διαφορετικά φυσικά στρώματα μπορούν να αλλάζουν μεταξύ αυτών. (για παράδειγμα μεταξύ ενός πομποδέκτη και ενός μεταδότη). Ένας εξυπνότερος εισβολέας μπορεί να μαθαίνει για τα πρωτόκολλα μέσα στον λογαριασμό, να σώζει ενέργεια, δίνοντας έτσι πνοή στο συνωστισμό δεσμού στρώματος. Ειδικά, το MAC πρωτόκολλο είναι ένα υποψήφιο θύμα.

Ας υποθέσουμε για παράδειγμα πρωτόκολλα βασισμένα στην ανταλλαγή πακέτων RTS/CTS, όπως το PAMAS ή S-MAC. Όποτε ένας κόμβος εισβολέας δέχεται ένα RTS πακέτο που προέρχεται από κάποιο κόμβο Χ, μπορεί να απαντήσει με σήμα συνωστισμού, επεμβαίνοντας με οποιοδήποτε άλλο σταλθέν πακέτο CTS στο Χ. Σαν συνέπεια, το Χ δεν έχει καμία ευκαρία εκπομπής, γυρνά πίσω και ξαναπροσπαθεί αργότερα με άλλο πακέτο RTS. Ο εισβολέας μπορεί να εκμεταλευτεί το πρωτόκολλο MAC αργότερα για να σώσει ενέργεια. Για παράδειγμα στο S-MAC ο εισβολέας μπορεί να προσαρμόσει τις περιόδους δραστηριότητας του στα πλάνα των γειτόνων του.

Άλλη μία επίθεση εκμεταλεύεται το πρωτόκολλο MAC χρησιμοποιώντας άμεσες αναγνωρίσεις και επανεκπομπές. Κατά τη λήψη πλαισίου πληροφοριών από τον κόμβο Χ, ο κόμβος εισβολέα μπορεί να συνωστίσει την αναγνώριση: πλαίσιο προορισμένο στον Χ. Αυτό έχει σαν αιτία ο Χ να γυρίσει πίσω, να επαναεκπέμψει το ίδιο πακέτο και να χάσει ενέργεια. Άλλος τρόπος κένωσης του κόμβου Χ είναι να στέλνονται συνεχώς RTS πακέτα σε αυτόν τον κόμβο αναγκάζοντας αυτόν να απαντήσει με CTS πακέτα. Ο τύπος αυτού του συστήματος απεικονίζεται από την εξωτερική περίπτωση σχεδιασμού ενός ATM. Ισχυρό ατσάλι ή άλλα ανθεκτικά υλικά χρησιμοποιούνται για να ελαττώσουν την επίθεση από απαιτούμενα εργαλεία και τη μεγάλη προσπάθεια προκειμένου να πέσει το σύστημα. Ο τύπος αυτός του συστήματος μπορεί να χρησιμοποιηθεί σε πολλά περιβάλλοντα και κάποιες φορές έχει το πλεονέκτημα το ότι είναι τόσο βαρύ αποό τη φύση του(όπως τα ATMs). Παρόλα αυτά πρόσφατες κλοπές σε ATM αποδεικνύουν ότι τα ATM δεν ανθίστανται αρκετά στη διαφθορά. Ένα σύστημα το οποίο απέχει στη διαφθορά έχει το μειονέκτημα ότι ο ιδιοκτήτης μπορεί να μην ανησυχεί για την απώλεια μέχρι να ανακαλυφθεί η κλοπή. Αυτό μπορεί να μην γίνει πότε, εάν ο εισβολέας κάνει σωστά τη δουλειά του και αντικαταστήσει οποιοδήποτε υλικό που μετακίνησε.

Η ασφάλεια του φυσικού επιπέδου είναι συνήθως το ευκολότερο για την αποδοχή. Σχέδια ατσάλινα και κλειδαριές είναι γνωστές από τεχνολογικής απόψεως και κατασκευάζονται εύκολα. Το βάρος και ο όγκος μπορεί να είναι ένα πρόβλημα ή ένα όφελος, εξαρτάται από την εφαρμογή.

Η πολυπλοκότητα ή το μέγεθος μπορεί να είναι άλλη μια ποικιλία της αντοχής στην παραβίαση (tamper resistance)...

Τα συστήματα “tamper responding” χρησιμοποιούν την προσέγγιση συναγερμού του κλέφτη. Η άμυνα είναι ο εντοπισμός της εισβολής. Στην περίπτωση

των παρευρισκόμενων συστημάτων, η απάντηση μπορεί να βρίσκεται στον ήχο ενός συναγερμού.

Η διαγραφή ή η καταστροφή μιας μυστικής πληροφορίας είναι μερικές φορές χρήσιμο στο να αποτρέπει κλοπές στην περίπτωση απομονωμένων συστημάτων τα οποία δεν βασίζονται σε εξωτερική απάντηση. TR συστήματα δεν βασίζονται σε εύρωστες κατασκευές ή βάρη για φύλαξη κεφαλαίου (asset). Γι' αυτό, αυτά είναι καλά για φορητά ή κινητά συστήματα, ή άλλα συστήματα όπου το μέγεθος και ο όγκος είναι ένα μειονέκτημα.

Τα Tamper καταφανή συστήματα είναι σχεδιασμένα για την διασφάλιση του ότι εάν συμβεί μια κλοπή, μένουν πίσω αποδεικτικά στοιχεία της. Αυτό είναι πάντα επιτυχημένο με χημικές ή μηχανικές σημασίες, όπως λευκή μπογιά που φεύγει όταν γδαρθεί ή κασέτες που δείχνουν αποδεικτικά της μετακίνησης.

Αυτά τα συστήματα δεν σχεδιάστηκαν για να αποτρέψουν μια επίθεση ή να απαντήσουν σε ένδειξη που είναι σε επεξεργασία. Η δουλειά τους είναι να διασφαλίσουν ότι το γεγονός της κλοπής θα παραμείνει γνωστό και θα μπορεί να εξακριβωθεί αργότερα. Μια δοκιμή τακτικής πρέπει να υπάρχει, πρέπει να προσκολλείται προκειμένου το καταφανές σύστημα tamper να είναι αποτελεσματικό. Ειδάλλως μπορεί να μην γίνει γνωστό ή όταν το σύστημα ήταν φθαρμένο.

5.3Επιθέσεις υψηλής τεχνολογίας

Οι επιθέσεις όπως περιγράφονται παρακάτω, απέχουν πολύ από τα τυπικά επίπεδα επιδεξιοτήτων και διαθέσιμων πηγών στους κοινούς εισβολείς. Παρόλ' αυτά τα επίπεδα επιδεξιότητας του κοινού εισβολέα αυξάνονται. Οι επιθέσεις αυτές και οι άμυνες παρουσιάζονται για να προβάλλουν της απαιτήσεις των αγορών όπως τα τραπεζικά. Παρόλ' αυτά όσο οι αξίες πληροφοριών αυξάνονται, όπως συμβαίνει σήμερα με την αύξηση του internet εμπορίου, αυτές οι τεχνικές άμυνας μπορούν να αποτελέσουν ένα κύριο μέρος της κοινής πρακτικής. Παρακάτω παρουσιάζονται οι επιθέσεις:

5.3.1Probe Επιθέσεις

Ο σκοπός μιας probe επίθεσης είναι να συνάψει κατευθείαν οδηγούς στην περιοχή που προστατεύεται έτσι ώστε η πληροφορία να μπορεί να αποκτηθεί και οι αλλαγές να εκχέονται μέσα στο υπό επίθεση σύστημα.

5.3.2 Παθητικά Probes

Αυτά μπορεί να χρησιμοποιηθούν για παρακολούθηση και εγγραφή πληροφορίας που εμπεριέχεται στις περιοχές. Όταν χρησιμοποιείται με ένα λογικό αναλυτή, ο εισβολέας περιμένει για ένα προαποφασισμένο γεγονός και μετά ξεκινάει την εγγραφή.

5.3.3 Ενεργά ή Injector Probes

Τα ενεργά Probes γενικά χρησιμοποιούνται ως σύνδεσμοι με τα παθητικά probes. Χρησιμοποιώντας πρότυπο γεννήτορα ή παρόμοιες συσκευές, αυτά τα probes μπορούν να εισάγουν σήματα ή πληροφορίες μέσα σε ένα ενεργό σύστημα.

5.3.4Pico-Probes

Τα pico-probes μπορούν να χρησιμοποιηθούν σε κάθε μια από τις ικανότητες που περιγράφηκαν παραπάνω. Τα pico-probes είναι πολύ μικρά και χρησιμοποιούνται κατευθείαν για να εξετάσουν τις επιφάνειες των συνεργαζόμενων περιοχών.

5.3.5Ενεργά Probes

Τα ενεργά probes μπορούν να είναι ακτίνες ηλεκτρονίων και ακτίνες ιόντων συγκεντρωμένες ακτίνες φωτός. Εξαρτώμενα από την τεχνολογία που δέχεται επίθεση, τα ενεργά probes μπορούν να γράψουν ή διαβάσουν τα περιεχόμενα της καταχώρησης των ημί-οδηγών, ή να αλλάξουν τα σήματα ελέγχου. Η καταχώρηση ακτίνας ιόντος χρησιμοποιήθηκε για να αποσυνδέσει επιτυχημένα fuse links, να επιστρέψει κάρτες έξυπνες προϊόντος στην κατάσταση επαναφοράς (εξάλειψη λαθών) όπου η έξοδος των εγγραφών κλειδιών κ.ο.κ. επιτράπηκε.

5.3.6 Μέθοδοι επεξεργασίας

Ο σκοπός της επεξεργασίας είναι να κόψει ή μετακινήσει υλικό. Εάν το σύστημα προστατεύεται από φυσική ασφάλεια, η πρόσθεση είναι να εκτελέσει την λειτουργία χωρίς να προσπεράσει έναν αισθητήρα ή να εγκαταλείψει στοιχεία. Αφού μετακινηθεί το κάλυμμα ο αισθητήρας τότε απενεργοποιεί ή παραλείπεται έτσι ώστε μια frobbing επίθεση να μπορεί να ξεκινήσει. Εάν το σύστημα προστατεύεται από σύστημα tamper evident, τότε μπορεί να υπάρξει μια προσπάθεια να καλύψει τα στοιχεία αφού ολοκληρωθεί η επίθεση. Η λίστα των μεθόδων επεξεργασίας συμπεριλαμβάνει χημικές και ενεργειακές μεθόδους για την μετακίνηση του υλικού, τόσο καλά και όπως οι παραδοσιακές μέθοδοι

5.3.7 Χειροκίνητη απομάκρυνση Υλικού

Αναφέρεται συχνά και ως «εγχείρηση μυαλού» αυτή η επίθεση. Σ' αυτό το σενάριο ένας εισβολέας χρησιμοποιώντας ένα μαχαίρι ή άλλο εργαλείο, προσπαθεί να μετακινήσει ένα σφραγισμένο δοχείο ενώ σταματάει μικρά προσπεράσματα του αισθητήρα (short of tripping a sensor). Η επίθεση αυτή είναι περισσότερο αποτελεσματική απ' ότι μπορεί κανείς να φανταζόταν. Εάν ο εισβολέας είναι έξυπνος και έχει καλή αρμονία hand-eye μια ακραία λεπτή δουλειά μπορεί να επιτευχθεί.

5.3.8 Μηχανικές επεξεργασίες

Η μέθοδος αυτή μετακινεί πολύ υλικό, πολύ συγκεκριμένο στον μικρότερο χρόνο. Τα μειονεκτήματα της έγκειται στο γεγονός ότι υπάρχει μικρή ή καμία ανταπόκριση. Αυτό συχνά έχει σαν αιτία κοψίματα τα οποία είναι πολύ βαθιά. Εάν ο κόφτης είναι αγωγός, μπορεί τότε να ανιχνευθεί από τον ανιχνευτή tamper.

5.3.9 Επεξεργασία Νερού

Η επεξεργασία νερού είναι μια πολύ συγκεκριμένη μέθοδος για μετακίνηση υλικού. Ο «κόφτης» μπορεί να είναι μη αγωγός (εάν το νερό είναι αγνό) και αν είναι πολύ αποτελεσματικός για όλα πλην των πολύ μαλακών υλικών. Το κύριο μειονέκτημα του είναι ο εξοπλισμός του που είναι τυπικά πολύ μεγάλος. Παρόλ' αυτά, σε καταστάσεις όπου το κόστος και το μέγεθος είναι μια ανησυχία, αλλά όχι και ο χρόνος, είναι απ' ευθείας αργή, σταθερή σταγόνα νερού θα κόψει αποτελεσματικά τον επαρκή χρόνο μέσα από πολλά χρόνια.

5.3.10 Laser επεξεργασία

Αυτή η τεχνική έχει πολλά από τα πλεονεκτήματα του νερού ένα μειονέκτημα είναι ότι η επεξεργασία μπορεί να δημιουργήσει μεγάλο πρόβλημα θερμότητας. Το Laser πρέπει να χρησιμοποιείται για τα υλικά ενδιαφέροντος, π.χ. τα EXCIMER (U.V.) Lasers είναι εξαιρετικά για την απομάκρυνση οργανικών υλικών (όπως epoxy).

5.3.11 Χημικά υλικά

Μέχρι σήμερα, σχεδόν όλα τα υλικά μπορούν να καταστραφούν και τα συναφή εμπορικά εργαλεία είναι πολύ καλά για την μετακίνηση καλυμμένων υλικών. Οι τεχνικές αυτές λειτουργούν χρησιμοποιώντας υψηλή πίεση, πολύ συγκεκριμένο spray διαλυτικού υγρού ή οξέως για να καταστρέψουν το υλικό. Το διαλυτικό υγρό ή το οξύ μπορεί να θερμανθεί ώστε να αυξήσει την αποτελεσματικότητα του. Το κύριο μειονέκτημα είναι η ικανότητα υψηλής μεταδοτικότητας ιονισμένων υγρών, τα οποία μπορεί να δημιουργήσουν μικρές περιοχές (circuits).

5.3.12 Μορφοποιημένη Τεχνολογία

Αυτές οι τεχνικές έχουν τα πλεονεκτήματα του να είναι ακριβή και παρά πολύ γρήγορα. Η ταχύτητα διαπέρασης αγγίζει τα 25,000ft/sec. Σε αυτές τις τεράστιες ταχύτητες, ένα πακέτο μπορεί να εισχωρήσουν και οι περιοχές (circuits) να απενεργοποιηθούν πριν απαντήσουν. Για παράδειγμα μια περιοχή μνήμης μηδενικής μπορεί να αποδυναμωθούν πριν η ενέργεια μπορέσει να μετακινηθεί από την μνήμη. Αυτό μπορεί να δώσει στον εισβολέα μερικά δευτερόλεπτα ως και ένα λεπτό να τελειώσει την εισαγωγή πακέτου και να ξαναζητήσει ισχύ στην μνήμη πριν να φθίνουν τα περιεχόμενά του.

5.3.13 Tempest

Αυτή είναι μια παθητική επίθεση. Ηλεκτρομαγνητικές πηγές από υπολογιστή ή άλλες ηλεκτρονικές συσκευές, μπορούν να ανιχνευθούν στη στιγμή και να κωδικοποιηθούν για να αποφασίσουν περιεχόμενα ή συμπεριφορά. Η τρέχουσα κατανομή παροχής ισχύος μπορεί να μετρηθεί για να αποφασίσει δράση περιοχών. Οι περισσότερες πληροφορίες στο Tempest είναι εμπιστευτικές κυβερνητικές στον τομέα της εθνικής ασφαλείας. Παρόλ' αυτά είναι γνωστό και έχει εξηγηθεί ότι μια επίδειξη video ή σειριακές επικοινωνιακές γραμμές μπορούν να χτυπηθούν σε αποστάσεις εκατοντάδων μέτρων πρόσφατα περισσότερες απόψεις για την Tempest τεχνολογία έχουν ανεξάρτητα ανακαλυφθεί στον εμπορικόν τομέα.

Έξυπνες κάρτες δέχονται επίθεση επιτυχώς ως αποτέλεσμα της μελέτης των τρεχούσων παροχών ισχύων τους και άλλες έχουν αναπτύξει νέες προσεγγίσεις για την χρησιμοποίηση αυτής της μεθόδου.

5.3.14 Ενεργές επιθέσεις

Αυτές οι επιθέσεις είναι ένα είδος επιθέσεων της επαφής και της μη επαφής. Παρόλ' αυτά ακόμα και οι επιθέσεις της μη επαφής συνήθως απαιτούν κοντινή πρόσβαση στο σύστημα.

5.3.15 Έκθεση στην ακτινοβολία

Με την ακτινοβολία των CMOS RAM στη ζώνη των Ακτίνων – Χ (και πιθανώς σε άλλες ζώνες) τα περιεχόμενα μπορεί να «καούν» τόσο που η πτώση ισχύος ή η επανεγγραφή (over-write) να αποτύχει να διαγράψει τα περιεχόμενα. Η βασική επίθεση χρησιμοποιεί για να αποθηκεύσει κρυπτογραφικά κλειδιά ή άλλες μυστικές πληροφορίες, έπειτα η μονάδα ισχύος παθαίνει ρήγμα φυσικώς χωρίς προσοχή για πτώση ισχύος ή επανεγγράψιμων μηχανισμών. Η RAM μπορεί τότε να διαβαστεί at leisure.

5.3.16 Έκθεση Υψηλής τάσης

Με «επιτάχυνση» η CMOS RAM με μικρή διάρκεια, παλμούς υψηλής τάσης, μπορεί πιθανόν να αποτυπώνει τα περιεχόμενα κατά παρόμοιο τρόπο στην imprinting ακτινοβολίες.

5.3.17 Υψηλή ή χαμηλή τάση

Αλλάζοντας την Vcc σε ασυνήθιστα υψηλές ή χαμηλές τιμές περίεργες συμπεριφορές μπορεί να προκληθούν σε πολλές περιοχές (circuit). Η περίεργη αυτή συμπεριφορά μπορεί να περιλαμβάνει τις χωρίς διερμηνεία οδηγίες του επεξεργαστή, να διαγράψει ή επαναγράψει αποτυχίες ή να διατηρήσει στη μνήμη πληροφορίες της που δεν είναι επιθυμητές.

5.3.18 Κακή λειτουργία ρολογιού

Με την αύξηση ή μείωση των παλμών του ρολογιού σε μια περιοχή όπως ο επεξεργαστής, η λειτουργία του μπορεί να ανατραπεί. Οδηγίες ή έλεγχοι μπορούν να παραμερηθούν και γενικά η περίεργη λειτουργία μπορεί να επηρεαστεί.

5.3.19 Διάρρηξη περιοχής

Η περιοχή αυτή δεν έχει μελετηθεί ακόμα σε βάθος, παρόλ' αυτά είναι γνωστό ότι δυνατές ηλεκτρομαγνητικές παρεμβολές μπορεί να προκαλέσουν διάρρηξη στον τύπο διόδου-θορύβου τυχαία αριθμού γεννητόρων και υπολογιστικών περιοχών.

5.3.20 Electron Beam Red/write

Η ηλεκτρονική ακτίνα ενός συνήθους ηλεκτρονικού μικροσκοπίου, μπορεί να χρησιμοποιηθεί για να διαβάσει και πιθανόν γράψει, bits σε ένα EPROM, EEPROM ή RAM. Για να γίνει αυτό, πρέπει η επιφάνεια του chip να είναι εκτεθειμένη πρώτα, πάντα σε χημικό machining. Αυτή είναι μια πολύ ισχυρή επίθεση από την ώρα που το chip είναι εκτεθειμένο μέχρι να εξαφανιστεί, κανονικά και να μην ξαναδιαβάζεται, κλειδιά και μυστικά μπορεί να κλαπούν πιθανώς ή να τροποποιηθούν.

5.3.21 IR Laser Read/write

Η σιλικόνη είναι διαφανής στις συχνότητες IR. Εξαιτίας αυτού, είναι πιθανόν να διαβαστούν και να γραφούν αποθήκευσης κελιά σε μια υπολογιστική συσκευή χρησιμοποιώντας ένα laser IR κατευθείαν διαμέσου της ογκώδους πλευράς της σιλικόνης του chip. Με την διαπέραση της ογκώδους πλευράς δεν χρειάζεται να χαραχτεί (jet etch) ή αλλιώς να μετακινήσει την μη ενεργή συσκευή.

5.3.22 Φανταστικές τεχνολογίες

Οποιαδήποτε από τις τωρινές φανταστικές τεχνολογίες συμπεριλαμβανομένου τις ακτίνες X, τομογραφία κ.λ.π. μπορούν να χρησιμοποιηθούν για να κάνουν ορατά

τα περιεχόμενα ενός σφραγισμένου πακέτου. Αυτό μπορεί να βοηθήσει τον εισβολέα να παρατηρήσει περιοχές ή τρωτά σημεία, να αναγνωρίσει τυπωμένες περιοχές καρτών σχεδιασμού, και πιθανόν να αναγνωρίσει συγκεκριμένα κομμάτια.

5.4.Υψηλές τεχνολογικά Άμυνες

Οι μέθοδοι ανίχνευσης που αναφέρονται παρακάτω διακρίνονται σε τρεις κατηγορίες: αποτροπής εισβολής, ανίχνευσης εισβολής, ανίχνευση μη-επιδρομικών ενεργών επιθέσεων (κρύο, ακτινοβολία κ.λ.π.). Μετά την ανίχνευση, υπάρχουν ποικίλες μεθόδοι απαντήσεων. Κάθε μέθοδος πρέπει να εξεταστεί κατά την επιλογή του σημείου σχεδιασμού. Για παράδειγμα, ένας σχεδιασμός που γίνεται για τον αισθητήρα χαμηλής θερμοκρασίας πρέπει να λαμβάνει υπόψιν τις θερμοκρασίες στις οποίες η μονάδα θα μπορούσε να εκτεθεί κατά την μεταφορά.

5.4.1 Φυσική αντοχή

Αυτή είναι μια βασική αποθήκη τεχνολογίας. Για παράδειγμα μια αυτόματη μηχανή teller, απαιτούσε μια ίντρα πάχους ατσάλινης κάσας η οποία είχε μέσα της άλλο ένα κοντί μετρητών μιας ίντσας πάχους. Οι τύποι αυτοί του συστήματος επίσης αντέχουν τις κλοπές λόγω του όγκου. Άλλη μια προσέγγιση είναι να συνάψει την συσκευή σε tamper φραγμό τόσο σωστά ώστε η προσπάθεια να διαχωρίσει τα στρώματα, ή να διαπεράσει την προστασία έχει ως αποτέλεσμα την καταστροφή των προστατευμένων συσκευών.

5.4.2 Σκληροί φραγμοί

Το Ατσάλι, το τούβλο, τα κεραμικά μπορούν όλα να χρησιμοποιηθούν σαν αποτελεσματικοί φραγμοί. Όπως προαναφέρθηκε, αυτό μπορεί να βοηθήσει να αναχαιτίσει τις κλοπές.

5.4.3 Απλά chip επικάλυψης

Η τεχνική αυτή χρησιμοποιείται για να εμποδίσει επίθεση στο απλό επίπεδο chip (π.χ. pico-probing). Η επιφάνεια του chip μπορεί να μην εξετάζεται λεπτομερώς με την επικάλυψη σε μέρος και αυτές οι επικαλύψεις παρέχονται έτσι ώστε η απομάκρυνση να καταστρέψει το chip παρά την ανάκτηση. Αυτό είναι ένα πολύ πολύπλοκο θέμα όσο η νέα χημεία σταθερά αναπτύσσεται.

5.4.4 Insnlator Bases Substrates

Για να εμποδιστεί ένας εισβολέας να αποφύγει μια προστατευμένη επικάλυψη χρησιμοποιώντας την τεχνική IR Laser, η ογκώδης σιλικόνη πρέπει να αντικατασταθεί με ένα υλικό το οποίο δεν είναι διαφανές σε συνήθεις συχνότητες.

Simox (Silicon.metal oxide), SOS (Silicon-on-Sapphire) ή άλλες τεχνολογίες απομονώνουν σιλικόνης, συνεργαζόμενα με προχωρημένες passivation επαναπαρουσιάζουν τα υψηλά επίπεδα παθητικότητας, απλού chip., προστασία. Κάποιος πρέπει να εκτιμήσει προσεκτικά την πιθανότητα της χρησιμοποίησης τεχνικών τριμάτων επιφάνειας για να λεπτύνει το substrate στο σημείο της διαφάνειας.

5.4.5 Ειδικές τοπογραφίες ημιοδηγών

Για την προστασία επιθέσεων σκαναρίσματος ηλεκτρονικού μικροσκοπίου ή pico-probing επιθέσεων, ακόμα και με την παρουσία χημικών machining ή άλλων τεχνικών που απομακρύνουν επικαλύψεις, ένα chip μπορεί να σχεδιαστεί έτσι ώστε να μην εκθέτει κρίσιμες δομές χωρίς την απομάκρυνση ενεργών στρωμάτων της συσκευής.

5.4.6 Φυσικά στοιχεία

Τα συστήματα ΄΄tamper evident΄΄ δεν είναι σχεδιασμένα να αποτρέπουν επίθεση ή είσοδο μέσα σε προστατευμένη περιοχή. Είναι σχεδιασμένα με τέτοιο τρόπο ώστε η είσοδος να αφήνει αποδεικτικά στοιχεία προς ανακάλυψη κατά τη διάρκεια φυσικών εξετάσεων λογαριασμών.

5.4.7 Εύθραυστα πακέτα

Η συσκευή σφραγίζεται σε ένα πακέτο φτιαγμένο από κεραμικό υλικό, γυαλί ή άλλο εύθραυστο υλικό. Εάν μια προσπάθεια γίνεται για την εισχώρηση στο πακέτο, αυτό σπάει ή θρυμματίζεται αφήνοντας αποδεικτικά στοιχεία.

5.4.8 Crazed Alouminum

Το πακέτο είναι φτιαγμένο από αλουμίνιο ή άλλο παρόμοιο υλικό το οποίο έχει θερμανθεί (συνήθως πάνω από 1000 βαθμού F^o) και σβήνεται. Η θέρμανση αυτή δημιουργεί εκκατομύρια τήξεις, διάφορα σπασίματα να εμφανίζονται στην επιφάνεια. Αυτά τα σπασίματα, όπως αποτύπωμα δαχτύλου είναι μοναδικά σε κάθε κομμάτι. Η περίπτωση αυτή μπορεί να φωτογραφηθεί και κατά συνέπεια να υπολογισθεί χρησιμοποιώντας την οπτική και φωτογραφική αντιστοίχιση συσκευών.

5.4.9 Μολυσμένα πακέτα

Παρομοίως με τα τρελά αλουμίνια, το πακέτο επιθεωρείται για αλλαγές στην εμφάνιση της επιφάνειας. Στην περίπτωση αυτή οποιοδήποτε σημάδι αντιπροσωπεύει μια προσπάθεια παραβίασης.

5.4.10 Αισθητήρες Τάσης

Είναι χρήσιμοι σε κάθε περίπου σχεδιασμό ο οποίος απαιτεί κατάλληλη παράδοση ισχύος για σωστή λειτουργία. Μαζί η υψηλή και η χαμηλή τάση μπορεί να είναι μια μελετημένη ή τυχαία επίθεση. Για την εγγύηση σωστής λειτουργίας περιοχών όλες οι προμήθειες ισχύος πρέπει να καταγράφονται. Οποιαδήποτε εξωτερική κίνηση εκτός του κανονικού βαθμού λειτουργίας θα πρέπει να θεωρείται επίθεση, και η απάντηση πρέπει να προσυμφωνείται. Οι αναφορές για τα μόνιτορ πρέπει να είναι ανεξάρτητες των διαφορών παροχών ισχύος.

5.4.11 Robe Αισθητήρες

Αποκλειστικοί σχεδιασμοί μπορεί να χαρακτηρίζουν την αντίσταση tamper ή αποδεικτικά στοιχεία, τόσο καλά όσο η ανίχνευση tamper για πρόσθετες ασφάλειες. Κάποιοι σχεδιασμοί είναι περισσότερο ή λιγότερο δαπανηροί, ή βαρείς απ' ότι άλλοι.

5.4.12 Αισθητήρες καλωδίων

Το καλώδιο θα πρέπει να έχει υψηλή αντίσταση έτσι ώστε το καλώδιο να μπορεί να χρησιμοποιηθεί σαν αντίσταση διανομής έτσι ώστε μικρές αλλαγές να μπορούν να ανιχνευθούν. Εάν το καλώδιο αποτύχει γύρω από τον εαυτό του ή φθαρεί, η ποιότητα της αίσθησης αυξάνεται επειδή δυο γειτονικά καλώδια μπορεί να είναι ηλεκτρικά μακριά. Έτσι μικραίνοντας δυο καλώδια δίνεται μεγαλύτερο σήμα απ' ότι δυο γειτονικές ίνες σε συνεχές περιτύλιγμα. Η απομόνωση του καλωδίου θα μπορούσε να είναι παρόμοια με το potting υλικό σε εμφάνιση και χημεία. Αυτό κάνει το machining περισσότερο δύσκολο γιατί κανείς υπαινιγμός για την προέλευση του καλωδίου δε γίνεται. Χημικές επιθέσεις γίνονται πιο δύσκολες εξαιτίας της δυσκολίας της διάλυσης του potting χωρίς να διαλυθεί η απομόνωση και τα cansing shorts. Είναι επίσης ένα πλεονέκτημα εάν το καλώδιο είναι φτιαγμένο από υλικό το οποίο είναι δύσκολο να το επισυνάψεις.

5.4.13 Αισθητήρες τυπωμένου κυκλώματος

Ένας αισθητήρας παρόμοιος του ενσύρματου μπορεί να δημιουργηθεί με πολύ χαμηλότερο κόστος τυπώνοντας την καλωδίωση πάνω σε πλακέτα περιοχής (Circuit board). Παρόλ' αυτά η κανονική τοποθέτηση των γραμμών και το συνήθες υλικό από χαλκό δίνουν κάτι λιγότερο ασφαλές. Αυτό γίνεται εξαιτίας της ευκολίας με την οποία οι οδηγοί πιθανόν να απομονώνονται εξαιτίας της κανονικότητας του ακάμπτου board περιοχή. Εάν μια φορά ο οδηγός εντοπιστεί, είναι πολύ εύκολο να συνάψεις άλλη γραμμή σ' αυτόν με σκοπό να ανιχνεύσει την λανθασμένη πληροφορία του tamper. Παρόλ' αυτά με καλό potting και μικρές γραμμές, αυτός ο σχεδιασμός δίνει μια μέτρια ασφάλεια.

5.4.14 Ευέλικτοι Printed Circuit Αισθητήρες

Ο σχεδιασμός αυτός συναίνει στα καλύτερα χαρακτηριστικά των δυο προηγούμενων. Η ευέλικτη επιφάνεια βοηθάει να καταστρέψει την κανονικότητα των επιπέδων της επιφάνειας. Οι γραμμές μπορούν να είναι φτιαγμένες silk-skreened conductive paste, η οποία επιτρέπει υψηλή αντίσταση. Είναι ακόμη καλύτερα να χρησιμοποιηθούν γραμμές φτιαγμένες από μεταβιβάσιμες εκδοχές του ίδιου υλικού που χρησιμοποιείται για την τελική στεγανοποίηση. Το σύνολο των μορφών των πακέτων είναι πιο ευρύ γιατί το πακέτο μπορεί να είναι «χαρισματικά τυλιγμένο» με το υλικό και μετά στεγανοποιημένο. Επίσης τις περιορισμένες γραμμές θα είναι περισσότερο δύσκολο να τις βρεις χωρίς σπάσιμο. Πολύπλοκα στρώματα μπορούν να χρησιμοποιούνται για πρόσθετη ασφάλεια.

5.4.15 Αισθητήρες σε περιοχές αποτυπωμένοι σε πιεσμένο γυαλί

Γραμμές μεταλλικές ή με οξείδια του μετάλλου μπορούν να αποτυπώνονται στο γυαλί, κατά τον ίδιο τρόπο που αποτυπώνεται ο αισθητήρας στο board περιοχής. Επαφές στο γυαλί μπορεί να φτιαχτούν χρησιμοποιώντας ελαστικούς συνδετήρες «Zebra». Πιεσμένο γυαλί μπορεί να θεωρηθεί ότι είναι πραγματικά αδιαπέραστο χωρίς το σπάσιμο του. Η μέθοδος αυτή είναι πολύ καλή για μεγάλες επίπεδες επιφάνειες ή πιθανών για ασφαλείς πόρτες.

5.4.16 Πιεσμένο Γυαλί με Piezo – ηλεκτρικό Αισθητήρα

Χρησιμοποιώντας το ίδιο γυαλί όπως το προηγούμενο παράδειγμα, αισθητήρας αυτός χρησιμοποιεί ένα στοιχείο με ηλεκτρική πίεση για να σημειώσει το σπάσιμο του γυαλιού. Η δύναμη του σπασίματος του πιεσμένου γυαλιού είναι αρκετή να επιφέρει ένα μεγάλο σήμα από την συσκευή ηλεκτρικής πίεσης συνημμένη στο εσωτερικό του γυαλιού.

5.4.17 Φύλλο ηλεκτρικής πίεσης

Πλαστικά φύλλα ηλεκτρικής πίεσης μπορούν να χρησιμοποιηθούν σαν φραγμοί probe. Εάν μια προστατευόμενη περιοχή από ένα φύλλο ηλεκτρικής πίεσης είναι εξετάσιμο (probed) ή τρυπημένο, δημιουργείται μια ηλεκτρική φόρτιση στην εφαρμοζόμενη δύναμη. Η φόρτιση αυτή μπορεί να μετρηθεί και να χρησιμοποιηθεί ή για να ενεργοποιήσει απάντηση του tamper circuitry. Υπάρχουν βέβαια προβλήματα με την εφαρμογή αυτή εξαιτίας της ευαισθησίας στην πίεση και τη δόνηση οι οποίες κάνουν τη σχεδίαση πολύ ευαίσθητη σε περιβαλλοντικές συνθήκες, και μη ευαίσθητες να μειώσουν κατασκευαστικές επιθέσεις.

5.4.18 Αισθητήρες κίνησης

Οι αισθητήρες αυτοί τυπικά χρησιμοποιούνται για να ευαισθητοποιούν κίνηση σε μια περιοχή ή σε κουτί. Χρειάζεται να χρησιμοποιούνται σε ζευγάρια επειδή ο κάθε τύπος μπορεί μερικές φορές να δημιουργήσουν μια λανθασμένη πραγματικότητα ή να αποτύχουν κάτω από ασυνήθιστες συνθήκες. Ένας infrared αισθητήρας μπορεί να ενεργοποιηθεί λάθος όταν οι πρώτες ακτίνες του ήλιου πέσουν στο προστατευμένο πακέτο μέσα από ένα παράθυρο.

5.4.19 Αισθητήρες υπερήχων

Οι αισθητήρες υπερήχων προσδιορίζουν κατά μέσο όρο μια εικόνα από ένα προστατευμένο χώρο μέσω της προστασίας υπερήχων και της αντανάκλασης. Μπορούν να είναι πολύ αποτελεσματικά, αλλά μπορεί να έχουν λανθασμένες πραγματικότητες εξαιτίας των ρευμάτων αέρα κλπ

5.4.20 Μικροκύματα

Παρόμοια με τους υπέρηχους με την ίδια δύναμη και αδυναμία, αλλά με υψηλότερη συχνότητα. Το υλικό των τοιχών των προστατευμένων περιοχών πρέπει να λαμβάνεται υπόψιν με τον τύπο από του συστήματος αφού μερικά μη μεταλλικά υλικά μπορεί να είναι καθαρά σ' αυτές τις συχνότητες. Αυτό μπορεί να δημιουργήσει λανθασμένη πραγματικότητα εξαιτίας της δραστηριότητας εκτός της προστατευμένης περιοχής.

5.4.21 Αισθητήρες επιτάχυνσης

Αυτοί οι αισθητήρες χρησιμοποιούνται για ανίχνευση κίνησης ή δόνησης. Οι κύριες χρησιμότητες τους είναι να αποτρέπουν κλοπές, και να ανιχνεύουν σφυροκοπήματα και τρυπήματα με τρυπάνι.

5.4.22 Συμπαγής κατάσταση (solid state)

Ο αισθητήρας αυτός ανιχνεύει μια αχτίδα φωτός ανακλώμενη από καθρέφτες οι οποίοι είναι συναπτόμενοι σε εύκαμπτα όρη, ή μια συσκευή ηλεκτρικής πίεσης και μια μικρή μάζα. Είναι αρκετά ευαίσθητοι και αξιόπιστοι.

5.4.23 Αισθητήρες θερ/σιας

Είναι ευρέως γνωστοί και διαθέσιμοι σε όλα τα κόστη ανάλογα με την χρησιμότητα τους.

5.4.24 Tamper Responding- Response Τεχνολογία

Οι μέθοδοι της τεχνολογίας του tamper response που αναλύονται εδώ έχουν την έννοια της απομάκρυνσης πληροφοριών από περιοχές RAM οι οποίες πιθανόν να διατηρούν μυστικές πληροφορίες. Αυτή η τρέχουσα και πιο διαδεδομένη μέθοδος

καταχώρησης τέτοιων πληροφοριών επειδή η συνοχή είναι αξιόπιστη και η διαγραφή αιτιολογημένη επίσης. Εάν κάποιος ήταν να χρησιμοποιήσει το υψηλότερο επίπεδο της διαθέσιμης τεχνολογίας για την προσπάθεια ανάκτησης πληροφοριών, που είχαν αποθηκευτεί και μετά διαγραφές στα περισσότερα γνωστά μέσα, υπάρχει ένα μικρό ενδεχόμενο, εκτός της φυσικής καταστροφής αυτό θα μπορεί να αποτρέψει την ανάκτηση.

5.4.25 Πέσιμο ισχύος RAM

Αυτή είναι η πιο απευθείας μέθοδος για την διαγραφή πληροφορίας. Εάν βοηθούμενη από ένα ατσάλινο bar circuit το οποίο παρέχει ένα πολύ χαμηλό εμπόδιο μονοπάτι από Vcc στο έδαφος, είναι αξιόπιστο εάν η προστασία αποτυπωμένη έχει απασχοληθεί. Αφού υπάρχει μια τάση για τα περιεχόμενα της RAM να αποτυπώνουν απεριόριστα οποιαδήποτε πληροφορία που είναι αποθηκευμένη στην RAM για πολύ καιρό, θα πρέπει να αντιστρέψει ή αλλιώς να αλλάξει για να αποτρέψει την αποτύπωση.

5.4.26 Απεριόριστη επανεγγραφή η RAM

Η μέθοδος αυτή είχε την πιο ευρεία αποδοχή σε κυβερνητικές εφαρμογές, παρόλ' αυτά σε μια καταστροφική συνθήκη θα είναι δύσκολο να εγγυηθεί κανείς ότι η αξιόπιστη ισχύς θα είναι διαθέσιμη να λειτουργήσει τη επανεγγράψιμη περιοχή. Η συνήθης μέθοδος είναι να επανεγγράψη κάποιες αρκετές φορές όλα τα Ο, έπειτα τα 1 ψηφία. Θα φαινόταν τυχαία η psendo-random πληροφορία να είναι περισσότερο αποτελεσματική, αλλά αυτό δεν φάνηκε. Θα έπαιρνε επίσης πολύ καιρό να συμπληρωθεί η επανεγγραφή απεριόριστη αφού η πληροφορία θα έπρεπε να είχε δημιουργηθεί.

5.4.27 Φυσική καταστροφή

Αυτή είναι η μοναδική μέθοδος διαγραφής πληροφορίας που είναι ολοκληρωτικά αξιόπιστη. Η Καταστροφή μπορεί να επιτευχθεί με την ελάχιστη βία. Το συμβάν θα ήταν ανιχνεύσιμο στην επιφάνεια του μεταλλικού υβριδικού πακέτου. Παρόλ' αυτά, η μέθοδος αυτή διατηρείται για τις περισσότερες ευαίσθητες καταστάσεις.

5.5 Επιθέσεις στρώματος δικτύου

Αρκετοί τύποι επιθέσεων μπορούν να εκτελεστούν στο στρώμα δικτύου. Πρώτον, οι κόμβοι ενός εισβολέα μπορούν να συμπεριφέρονται το ίδιο, όπως οι

κανονικοί κόμβοι. Συγκεκριμένα, μπορούν να λαμβάνουν μέρος στην δρομολόγηση (routing) πρωτοκόλλων ή διασπορά ενδιαφερόντων με στόχο τα απ'ευθείας routes στον εαυτό τους και να πετάξουν αργότερα πακέτα. Αυτή η επίθεση καλείται επίθεση μαύρη τρύπα Σε ένα παρόμοιο τρόπο επίθεσης που ονομάζεται αλλαγή κατευθύνσεων, ο εχθρός δημιουργεί λάθος δρομολόγια, για παράδειγμα, στέλνοντας λάθος διαφημιστικά πακέτα ή κατά λάθος απαντώντας στο αίτημα πακέτων δρομολογίων. Ένα λάθος δρομολογίου μπορεί για παράδειγμα να περιλαμβάνει ένα Loop και αιτιολογεί χάσιμο ενέργειας. Άλλο πιθανό αποτέλεσμα είναι ότι η κυκλοφορία δεν φτάνει τους προτιθέμενους κόμβους βύθισης. Όλοι οι κόμβοι που συμμετέχουν στην επιλογή δρομολογίων χάνουν την ενέργειά τους. Ακόμα και χωρίς ενεργή προσπάθεια να συμπεριληφθεί σαν προηθημένος μέσα στα routes, ένας κόμβος εισβολέας μπορεί να στείλει άλλα πακέτα κόμβων και να προωθήσει μόνο τα δικά του πακέτα. Τέτοια επίθεση ονομάζεται "neglect and greed"(αμέλεια και πλεονεξία). Ο κόμβος εισβολέα μπορεί να πετάξει πακέτα με τυχαία σειρά ή όλα από αυτά. Τα πρωτόκολλα routing ή πληροφοριακής διασποράς τα οποία αποθηκεύονται σε ασφαλή χώρο(DSP ή απ'ευθείας διάχυση) είναι εκτεθειμένα στην επίθεση αυτή.

Ένας άλλος τύπος επιθέσεων αναγνωρίζεται ως desychronization, ο οποίος μπορεί να εφαρμοσθεί στην μεταφορά πρωτοκόλλων τα οποίαστηρίζονται σε ακολουθία αριθμών. Θεωρώντας, τα ψεύτικα πακέτα με λάθος ακολουθία αριθμών ο εισβολέας μπορεί να δημιουργήσει σπατάλη των μετεχόντων για τον τερματισμό συνδέσεων.

Στα δίκτυα αισθητήρων που αναπτύσονται για να εντοπίσουν συγκεκριμένα γεγονότα περιβάλλοντος, ένας κόμβος εισβολέα μπορεί να παράγει πληροφορία αισθητήρα δηλώνοντας το γεγονός, προξενώντας κόμβους στο εγγύς ή και σε ολόκληρο το δίκτυο για να ξυπνήσει και να ξεκινήσει διάφορες ενέργειες. Πιθανά προληπτικά μέτρα μπορούν να αναπτυνθούν ξεκινώντας από εξωτερικές τεχνικές εντοπισμού.

5.6 Επιθέσεις στα ασύρματα δίκτυα

Η εξάρτηση των ανθρώπων στα υπολογιστικά δίκτυα συμπεριλαμβανομένου και των ασύρματων δικτύων,έχει αυξηθεί τρομακτικά τα τελευταία χρόνια και πολλές επιχειρήσεις βασίζονται κυριολεκτικά στις αποτελεσματικές, κατάλληλες και ασφαλείς λειτουργίες αυτών των δικτύων. Ο συνολικός αριθμός των υπολογιστικών δικτύων που είναι εγκατεστημένοι σε πολλούς οργανισμούς έχει αυξηθεί κατά πρωτοφανή βαθμό.

Μεγάλες εταιρείες αποθηκεύουν ευαίσθητες και εμπιστευτικές πληροφορίες στο marketing, εισροή φόρων, μυστικά συνναλαγών, εθνικές ασφαλείς πληλοφορίες και απόρρητες στρατιωτικές πληροφορίες ανάμεσα σε όλα τα άλλα. Η προσβολή τέτοιων πληροφοριών από μη εγκεκριμένους χρήστες μπορεί να αποφέρει απώλεια χρημάτων ή ελευθέρωση εμπιστευτικών πληροφοριών σε ανταγωνιστές ή εχθρούς.

Οι επιθέσεις στα υπολογιστικά συστήματα και τα δίκτυα μπορούς να διαιρεθούν σε παθητικές και ενεργές επιθέσεις. Οι ενεργές επιθέσεις εμπλέκουν μεταβαλλομενες πληροφορίρες ή δημιουργία ψεύτικων ρευμάτων (streams). Αυτοί οι τύποι επιθέσεων μπορούν να διαιρεθούν στις ***ακόλουθες υποκατηγορίες:***

- Μεταμφιέσεις
- Αποκρίσεις
- Τροποποίηση μηνυμάτων και
- Αρνηση εξυπηρέτησης.

Η μεταμφίεση (masquerade) συμβαίνει όταν μία οντότητα προσποιείται ότι είναι μία δημιουργική οντότητα. Για παράδειγμα, η αυθεντικότητα μπορεί να συγκεντρωθεί και να ξαναπαίξει μετά την τοποθέτηση μίας γνήσιας αυθεντικότητας ακολουθίας.

Η απόκριση εμπλέκει την παθητική σύλληψη μονάδων πληροφοριών και την ακολουθιακή τους επανεκπομπή για τη δημιουργία μη θελημένων προσβολών.

Η τροποποίηση μηνυμάτων σημαίνει ότι ένα μέρος γνήσιων μηνυμάτων έχει αλλάξει ή ότι τα μηνύματα έχουν καθυστέρηση ή γράφονται για να παράγουν ένα μη εξουσιοδοτημένο αποτέλεσμα.

Οι παθητικές επιθέσεις συνυπάρχουν με την κλοπή πληροφοριών ή την κατασκοπεία στην εκπομπή. Ο εισβολέας προσπαθεί να προσβάλλει πληροφορίες που έχουν μεταδοθεί.

Εδώ υπάρχουν **δύο υποκατηγορίες:** Ελευθέρωση των περιεχομένων μηνυμάτων και η ανάλυση κυκλοφοριών.

Στον πρώτο τύπο, ο εισβολέας προσεγγίζει τα μηνύματα email ή ένα αρχείο που έχει μεταδοθεί.

Στην ανάλυση κυκλοφορίας, ο εισβολέας θα μπορούσε να ανακαλύψει την τοποθεσία και την ταυτότητα των επικοινωνιακών hosts και να παραχωρήσει την συχνότητα και το μήκος των κωδικοποιημένων μηνυμάτων που έχουν ανταλλαχθεί. Τέτοια πληροφορία θα μπορούσε να είναι χρήσιμη σε έναν εισβολέα για να μπορεί να

ανακαλύψει χρήσιμες πληροφορίες στην αναζήτηση της φύσης των πληροφοριών που ανταλλάχθηκαν.

Γενικά, οι παθητικές επιθέσεις είναι δύσκολο να ανιχνευτούν παρ'όλα αυτά υπάρχουν κάποια μέτρα που μπορούν να χρησιμοποιηθούν για να τις αποφύγεις. Από την άλλη, είναι δύσκολο να εμποδίσεις ενεργές επιθέσεις.

5.7. Κύριες κατηγορίες επιθέσεων σε ασύρματα υπολογιστικά δίκτυα

5.7.1Διακοπή service

Εδώ οι πηγές του συστήματος είναι κατεστραμμένες ή έχουν γίνει μη διαθέσιμες.

5.7.2Τροποποίηση

Αυτή είναι μία επίθεση στην ταυτότητα του συστήματος. Στην περίπτωση αυτή, ο εισβολέας όχι μόνο προσβάλλει το δίκτυο, αλλά διαφθείρει με πληροφορίες όπως την αλλαγή values, σε μία βάση δεδομένων, μεταβάλλοντας το πρόγραμμα έτσι ώστε να έχει διαφορετικούς σκοπούς.

5.7.3Κατασκεύασμα

Αυτή είναι μία επίθεση στην εμπιστευτικότητα του δικτύου όπως την παρακολούθηση για δέσμευση του δικτύου. Η παρακολούθηση (eavesdropping) είναι εύκολη σε ασύρματο δίκτυο αφού όταν κάποιος στέλνει ένα μήνυμα πάνω σε μονοπάτι πομποδέκτη, ο καθένας που είναι εξοπλισμένος με κατάλληλο εξοπλισμό στον τομέα της εκπομπής μπορεί να κλέψει πληροφορίες. Αυτοί οι τύποι μηχανημάτων δεν είναι συνήθως ακριβοί.

Ο αποστολέας ή οι προτιθέμενοι δέκτες μπορεί να μην είναι ικανοί να ανακαλύψουν αν τα μηνύματά τους έχουν υποστεί δολιοφθορά ή όχι. Ακόμα περισσότερο εάν δεν υπάρχει καμμία ηλεκτρομαγνητική ασπίδα, η κυκλοφορία ενός ασύρματου δικτύου, μπορεί να υποστεί δολιοφθορά από εξωτερικούς παράγοντες του κτιρίου όπου τα δίκτυο κατασκευάζεται. Στα περισσότερα ασύρματα δίκτυα, υπάρχει ένα είδος link level που κωικοποιείται από ονότητες MAC.

5.7.4Συνωστισμός

Διακοπή service επιθέσεων επίσης εφαρμόζεται στα ασύρματα δίκτυα. Σε τέτοια περίπτωση, οι νόμιμες κυκλοφορίες(traffic) δεν μπορεί να πλησιάσει πελάτες ή προσβολή σημείων εκαιτίας του γεγονότος ότι μη νόμιμη κυκλοφορία κατακλυζει τις συχνότητες. Ένας εισβολέας μπορεί να χρησιμοποιήσει ειδικό εξοπλισμό να κατακλύσουν τα 2,4 GTLZ των μπάντων των συχνοτήτων. Τέτοια άρνηση service μπορεί να δημιουργήσει απ'έξω την περιοχή service των σημείων προσβολής, ή από

άλλες ασύρματες συσκευές εγκατεστημένες σε άλλες περιοχές εργασίας οι οποίες υποβιβάζουν την ολική δύναμη του σήματος.

5.7.5Client – to client επιθέσεις.

Οι χρήστες ασυρμάτων δικτύων χρειάζονται να αμύνονται τους clients όχι μόνο ενάντια σε μία εξωτερική απειλή, αλλά επίσης, εναντίον καθενός. Ασύρματοι clients οι οποίοι τρέχουν TCP/IP πρωτόκολλα όπως μοίρασμα αρχείων είναι τρωτοί στις ίδιες misconfigurations όπως στα ενσύρματα δίκτυα. Επίσης, αντιγραφή εις διπλούν των IP ή MAC δύσεων είτε είναι με σκοπό ή τυχαίο μπορεί να δημιουργήσει κατάρρευση του service.

Επιθέσεις εναντίον κωδικοποίησης: Το IEEE802.116 χρησιμοποιεί μία φόρμα κρυπτογράφησης που ονομάζεται WEP(wired equivalent privacy) η οποία έχει αποδειχθεί ότι έχει κάποιες αδυναμίες. Ένας έξυπνος εισβολέας μπορείνα σπάσει τη φόρμα WEP.

5.7.6 Μη διαμόρφωση

Προκειμένου να έχουμε εύκολη και αστραπιαία ανάπτυξη, η πλειονότητα των σημείων προσβολής, έχει ένα μη ασφαλή διαμόρφωση. Αυτό σημαίνει ότι αφού ο διαχειριστής δικτύου διαμορφώνει κάθε σημείο προσβλής κατάλληλα, αυτά τα σημεία προσβολής διατηρούνται σε υψηλό ρίσκο να είναι προσβαλλόμενα από μη εξουσιοδοτημένα parties ή hackers.

5.7.7 Επιθέσεις εναντίον passwords των σημείων προσβολής

Η πλειονότητα σημείων προσβολής χρησιμοποιεί ένα απλό κωδικό ή κλειδί, το οποίο μοιράζεται σε όλους τους συνδεδεμένους ασύρματους πελάτες. Οι εισβολείς μπορούν να προσπαθήσουν να συμβιβάσουν των κωδικό από το κλειδί εξαντλώντας όλες τις πιθανότητες. Αν ο εισβολέας μαντέψει το κλειδί ή τον κωδικό, μπορεί να έχει πρόσβαση στα σημεία προσβολής και να συμβιβάσει την ασφάλεια του συστήματος. Επίσης, η μη αλλαγή των κωδικών ή κλειδιών σε μία κανονική βάση μπορεί να τοποθετήσει το σύστημα δικτύου σε μεγάλο ρίσκο, ιδιαίτερα εάν οι υπάλληλοι φύγουν από την εταιρεία. Σε άλλη περίπτωση, η διεύθυνση, ενός μεγάλου αριθμού των σημείων προσβολής και πελατών περιπλέκει το σύστημα ασφάλειας.

5.7.8 Παρεμβολή επιθέσεων

Ο τύπος αυτός των επιθέσεων βασίζεται στην ανάπτυξη νέων ασύρματων δικτύων χωρίς την ακολούθηση διαδικασίας ασφαλείας. Επίσης, μπορεί να είναι αξαιτίας της εγκατάστασης μη εξουσιοδοτημένης συσκευής χωρίς κατάλληλο review ασφάλειας. Για παράδειγμα, μία εταιρεία μπορεί να μην γνωρίζει ότι κάποιοι από

τους υπαλλήλους της έχουν αναπτύξει ασύρματες ευκολίες στο δίκτυο της. Χρησιμοποιώντας τέτοια άτιμα σημεία προσβολής, η βάση δεδομένων της εταιρείας θα είναι συμβιβάσιμη.

Ασφαλώς, υπάρχει η ανάγκη για εκπλήρωση τακτικής για να διασφαλίσουν την διαμόρφωση όλων των σημείων προσβολής, σε αντίθεση με την επεξεργασία ρουτίνας με την οποία το δίκτυο σκανάρεται για μη εξουσιοδοτημένες συσκευές στα ασύρματα μέρη. Άλλο παράδειγμα είναι ότι ο εισβολέας μπορεί να συνδέσει ένα laptop ή PDA σε ένα σημείο προσβολής χωρίς την εξουσιοδότηση του ιδιοκτήτη του ασύρματου δικτύου. Εάν ο εισβολέας ήταν ικανός να αποκτήσει πρόσβαση παίρνοντας κωδικό ή εάν δε χρειαζόταν κωδικός ή απαίτηση κλειδιού, τότε ο εισβολέας θα είναι ικανός να συνδεθεί σε εσωτερικό δίκτυο.

Κάθε σύστημα δικτύου ασφάλειας πρέπει να διατηρεί τα ακόλουθα χαρακτηριστικά:

- ***Ακεραιότητα***

Η απαίτηση αυτή σημαίνει ότι λειτουργίες όπως η υποκατάσταση, παρεμβολή ή διαγραφή πληροφοριών μπορεί μόνο να εκτελείται από εξουσιοδοτημένους χρήστες χρησιοποιώντας εξουσιοδοτημένες μεθόσους. Τρεις απόψεις της ακεραιότητας είναι συνήθως αναγνωρίσιμες: εξουσιοδοτημένες δράσεις, προστασία πηγών και ανίχνευση λαθώς και σωστότητα.

- ***Εμπιστευτικότητα***

Αυτό σημαίνει ότι το σύστημα δικτύου μπορεί να προσβληθεί από εξουσιοδοτημένους χρήστες. Ο τύπος της προσβολής μπορεί να διαβαστεί μόνο από πρόσβαση.

- ***Άρνηση service***

Είναι γνωστή και ως αντίθετη, διαθεσιμότητα, μη εξουσιοδοτημένη οντότητα,και δεν πρέπει να εμποδίζεται ή να απαρνείται πρόσβαση σε αντικείμενα στα οποία έχει νόμιμη πρόσβαση. Η πρόσβαση αυτή εφαρμόζεται στο service και στην πληροφορία.

Η αποτελεσματικότητα του ελέγχου πρόσβασης βασίζεται σε δύο ιδέες: α) στην αναγνώριση χρήστη και β) στην προστασία του δικαιώματος πρόσβασης των χρηστών.

5.8.Τα υπολογιστικά δίκτυα, γενικώς, έχουν προβλήματα εξαιτίας

5.8.1Μοίρασμα

Αφού οι πηγές δικτύου μοιράζονται, οι περισσότεροι χρήστες έχουν την δυνατότητα να προσβάλλουν δίκτυα συστημάτων παρά μόνο έναν απλό κόμβο υπολογιστή.

5.8.2Πολυπλοκότητα

Εξαιτίας της πολυπλοκότητας των υπολογιστικών δικτύων όλων των τύπων, οι αξιόπιστες και ασφαλείς λειτουργίες είναι μία πρόκληση. Σε αντίθεση με όσα έχουν ειπωθεί, τα δίκτυα υπολογιστών, μπορεί να έχουν κόμβους με διαφορετικά συστήματα λειτουργίας, τα οποία κάνουν την ασφάλεια περισσότερο προκλητική.

5.8.3Ανωνυμία

Ένας hacker ή εισβολέας μπορεί να επιτεθεί σε σύστημα δικτύου από πολύ μακριά και γι'αυτό ποτέ δεν πρέπει να αγγίζει το δίκτυο ή να έρθει ακόμα και σε επαφή με κάποιον χρήστη ή το διακομιστή.

5.8.4Πολλαπλά σημεία επιθέσεων

Όταν ένα αρχείο υπάρχει φυσικώς σε ένα host remote, μπορεί να περάσουν πολλοί κόμβοι στο δίκτυο πριν να τους εντοπίσει ο χρήστης.

5.8.5Άγνωστο μονοπάτι

Στα υπολογιστικά δίκτυα, τα routes που παίρνουν απ'ευθείας πακέτα είναι σπάνια γνωστά στην έννοια του χρόνου από τον χρήστη δικτύου. Επίσης, αυτοί οι χρήστες δεν έχουν έλεγχο των routes που έχουν πάρει από μόνα τους τα πακέτα. Αυτά τα routes εξαρτώνται από κατασκευαστές όπως traffic patterns,συνθήκες φόρτωσης και κόστος.

5.9 Επίπεδο Ζεύξης

5.9.1Εισαγωγή στις επιθέσεις του επιπέδου ζεύξης(side channel attacks)

Οι επιθέσεις του επιπέδου ζεύξης είναι επιθέσεις βασισμένες στις πληροφορίες επιπέδου ζεύξης. Η πληροφορία επιπέδου ζεύξης είναι πληροφορία η οποία μπορεί να έχει ανακτηθεί από συσκευή κωδικοποίησης η οποία δεν έχει αποκωδικοποιήσει ούτε το κυρίως κείμενο, ούτε το κείμενο κώδικα, από την διαδικασία κωδικοποίησης. Στο παρελθόν, μια συσκευή κωδικοποίησης εννοείτο ως μια μονάδα η οποία παραλαμβάνει στην είσοδο κύριο κείμενο και παράγει στην έξοδο κείμενο κώδικα και vice-versa. Γι' αυτό οι επιθέσεις βασίζονταν είτε στην γνώση του κώδικα κειμένου (τέτοιες είναι κώδικα κειμένου-επιθέσεις) είτε

γνωρίζοντας και τα δυο (γνωστές ως «γνωστού κυρίως κειμένου-επιθέσεις) ή την ικανότητα να αναγνωρίζουν ποιο κυρίως κείμενο είναι κωδικοποιημένο και μετά να δουν τα αποτελέσματα της κωδικοποίησης. Σήμερα, είναι γνωστό ότι οι συσκευές κωδικοποίησης έχουν πρόσθετες εξόδους και συχνά πρόσθετες εισόδους οι οποίες δεν είναι το κυρίως κείμενο ούτε το κείμενο κώδικα. Οι συσκευές κωδικοποίησης παρέχουν πληροφορίες χρονισμού (πληροφορίες για το χρόνο που χρειάζεται μια λειτουργία) το οποίο είναι εύκολα μετρήσιμο, ακτινοβολία διαφόρων ειδών, στατιστικά κατανάλωσης ενέργειας (τα οποία μπορούν να μετρηθούν εύκολα) και άλλα πολλά. Συχνά η συσκευή κωδικοποίησης έχει επίσης προσθετικές «άσκοπες» εισόδους, όπως η τάση, η οποία μπορεί να τροποποιηθεί για να δημιουργήσει αναμενόμενες εξόδους.

Οι επιθέσεις επιπέδου ζεύξης κάνουν χρήση κάποιων ή και όλων των πληροφοριών μαζί με άλλες (γνωστές) τεχνικές κρυπτοανάλυσης για να ανακαλύψουν το κλειδί που χρησιμοποιεί η συσκευή. Οι επιθέσεις τυπικά εργάζονται για εύρεση κάποιων πληροφοριών για την εσωτερική κατάσταση του κώδικα. Οι πιο κοινοί τύποι πληροφοριών του επιπέδου ζεύξης είναι οι παρακάτω:
Επιθέσεις χρονισμού, SPA (απλή ανάλυση ισχύος) και DPA (διαφοροποιημένη ανάλυση ισχύος και επίθεση σφαλμάτων).

5.9.2 Επιθέσεις χρονισμού

Βασίζεται στην μέτρηση του χρόνου που χρειάζεται για μια μονάδα να εκτελεί λειτουργίες. Η πληροφορία αυτή μπορεί να οδηγήσει στα μυστικά κλειδιά. Για παράδειγμα, με την προσεκτική μέτρηση του συνολικού χρόνου που απαιτείται για να εκτελούνται ιδιωτικές λειτουργίες κλειδιών, ένας εισβολέας μπορεί να βρει σταθερούς δείκτες Diffie-Hellman, παραγόμενα κλειδιά RSA, και να σπάσει άλλα συστήματα crypto. Εάν μια μονάδα είναι τρωτή, η επίθεση είναι υπολογίσιμα απλή και συχνά απαιτεί μόνο γνωστό κώδικα κειμένου.

Συστήματα crypto, συχνά, παίρνουν ελαφρώς διαφορετικούς συνολικούς χρόνους για να επεξεργαστούν διαφορετικές εισόδους. Αιτία γι’ αυτό είναι η θέληση για επεξεργασία διαφορετικών εισόδων. Επίσης η θέληση για προσπέραση μη απαραίτητων λειτουργιών διακλαδώσεις και υποθετικές δηλώσεις, RAM κρυψώνες, οδηγίες επεξεργαστή (όπως πολυπλοκότητα και διαίρεση) τα οποία τρέχουν σε μη συγκεκριμένο χρόνο και μια μεγάλη ποικιλία άλλων αιτιών. Τα χαρακτηριστικά αυτά εξαρτώνται από το κλειδί κωδικοποίησης και την εισερχόμενη πληροφορία (π.χ. κυρίως κείμενο, ή κώδικα κειμένου). Σαν προαίσθημα μπορεί να υποτεθεί ότι τα

άσκοπα χαρακτηριστικά χρονισμού θα αποκάλυπταν ένα μικρό σύνολο πληροφοριών από ένα κρυπτογραφικό σύστημα. Παρόλ' αυτά οι επιθέσεις εκείνες οι οποίες μπορούν να εκμεταλλευθούν μέτρα χρονισμού, από τρωτά συστήματα, υπάρχουν για την εύρεση των ολικών μυστικών κλειδιών.

Τα μέτρα χρονισμού αναπτύχθηκαν σε ένα στατιστικό μοντέλο το οποίο μπορεί να παρέχει το αναζητούμενο bit του κλειδιού με κάποιο βαθμό σιγουριάς (ελέγχοντας συσχετισμούς μεταξύ των μέτρων χρόνων).

Ο υπολογισμός των διαφορών είναι εύκολος και παρέχει έναν καλό τρόπο για την αναγνώριση σωστών ερμηνειών αναζητούμενων bit. Ο αριθμός των δειγμάτων, ο οποίος χρειαζόταν για να αποκτήσει αρκετές πληροφορίες για να επιτρέψει την ανάκτηση των κλειδιών, είναι ορισμένος από τη κυριότητα των σημάτων και του θορύβου. Όσο περισσότερος θόρυβος υπάρχει, τόσο περισσότερα δείγματα θα απαιτούνται. Γενικά, οι τεχνικές λανθασμένης διόρθωσης αυξάνουν τις απαιτήσεις της επεξεργασίας και την μνήμη για την επίθεση, αλλά μπορούν να μειώσουν πολύ τον αριθμό των δειγμάτων που απαιτούνται.

Τα συγκεκριμένα παραδείγματα που ακολουθούν παρουσιάζουν συγκεκριμένες πληροφορίες σε βάθος για επιθέσεις χρονισμού εναντίον λειτουργιών που συσχετίζονται με την ασύμμετρη κωδικοποίηση. Ακόμη, πρέπει να θυμηθούμε ότι οι επιθέσεις χρονισμού μπορούν να χρησιμοποιηθούν με ικανότητα εναντίον άλλων κρυπτογραφικών συστημάτων, συμπεριλαμβανομένου και των συμμετρικών λειτουργιών.

5.9.3 Κρυπτανάλυση ενός απλού αλλοιωμένου ερμηνευτή

Οι λειτουργίες Diffie-Helman και RSA θεωρούν για τον υπολογισμό $R=y^x \bmod n$, όπου n είναι τυχαίο, και y μπορεί να βρεθεί από έναν υποκλοπέα . Ο στόχος του εισβολέα είναι να βρει το x, το μυστικό κλειδί. Για την επίθεση, το θύμα πρέπει να υπολογίσει $y^x \bmod n$ για αρκετές τιμές του y, όπου τα y, n και οι χρόνοι υπολογισμού είναι γνωστοί στον εισβολέα και το x παραμένει το ίδιο.

Στατιστικές μέθοδοι θα οδηγήσουν στην ανακάλυψη του κλειδιού απ' αυτά τα μέτρα. Οι απαραίτητες πληροφορίες και τα μέτρα χρονισμού πιθανόν να αποκτηθούν από παθητικούς υποκλοπείσε ένα πρωτόκολλο που αντεπιδρά, αφού ο εισβολέας θα μπορούσε να αντιγράψει τα μηνύματα που λήφθηκαν από τον στόχο και να μετρήσει τον συνολικό χρόνο που χρειάσθηκε να απαντήσει σε κάθε y. Η επίθεση υποθέτει ότι ο εισβολέας γνωρίζει τον σχεδιασμό του συστήματος που έχει σαν στόχο, αν και αυτό πρακτικά θα μπορούσε πιθανόν να το συμπεραίνει από την πληροφορία χρονισμού.

5.9.4 Πολυπλοκότητα Montgomery και το CRT

Τα σχετικά βήματα μείωσης δημιουργούν συνήθως την αλλαγή χρόνου σε μια σχετικά πολύπλοκη λειτουργία. Η πολυπλοκότητα Montgomery καταστρέφει τα βήματα μείωσης mod (n) και σαν αποτέλεσμα τείνει να μειώσει το μέγεθος των χαρακτηριστικών χρονισμού.

Η Υπόλοιπη Κινεζική θεωρία (Chinese Remainder Theoresm) CRT χρησιμοποιείται συνήθως για να κάνει λειτουργικές τις λειτουργίες των ιδιωτικών κλειστών RSA. Με το CRT (ymod p) και (y mod q) υπολογίζονται πρώτα όπου y είναι το μήνυμα. Αυτά τα αρχικά σχετικά βήματα μείωσης μπορεί να είναι τρωτά στις επιθέσεις χρονισμού. Η πιο απλή τέτοια επίθεση είναι να επιλέγεις τιμές του y οι οποίες είναι κοντά στο p ή το n, μετά να χρησιμοποιείς μέτρα χρονισμού για να αποφασίσεις εάν η ζητούμενη τιμή είναι μεγαλύτερη ή μικρότερη του p, υπολογίζοντας το y mod p δεν έχει αποτέλεσμα ενώ αν το y είναι μεγαλύτερο του p, είναι απαραίτητο να αφαιρεθεί το p από το y τουλάχιστον μια φορά. Τα συγκεκριμένα χαρακτηριστικά χρονισμού εξαρτώνται από τα επιτεύγματα.

Σε μερικές περιπτώσεις είναι δυνατόν να βελτιώνεται η CRT RSA επίθεση για να χρησιμοποιήσει γνωστούς κώδικες κειμένου (όχι επιλεγμένους), μειώνοντας τον αριθμό των απαιτουμένων μηνυμάτων κάνοντας έτσι δυνατόν να επιτεθεί στης ψηφιακές υπογραφές RSA. Σχετική μείωση γίνεται αφαιρώντας multiples of the modulus και οι εκμεταλλεύσιμες αλλαγές χρονισμού μπορούν να δημιουργηθούν από αλλαγές στον αριθμό συγκρίσιμων και αφαιρούντων βημάτων.

5.9.5 Κρυπτανάλωση χρονισμού του DSS

Όταν η σχετική μείωση της λειτουργίας τρέχει σε μη συγκεκριμένο χρόνο, ο ολικός χρόνος υπογραφής θα μπορούσε να συσχετισθεί με τον χρόνο για τον (x.r mod q) υπολογισμό. Ο εισβολέας μπορεί να υπολογίσει και να αποζημιώσει για τον απαιτούμενο χρόνο για υπολογισμό H(m). Αφού το H(m) είναι κατά προσέγγιση το ίδιο μέγεθος όπως το q, η πρόσθεσή του έχει μικρό αποτέλεσμα στον χρόνο μείωσης. Τα πιο σημαντικά bits του x.r. είναι χαρακτηριστικά τα πρώτα που χρησιμοποιούνται στην σχετική μείωση. Αυτά εξαρτώνται από το v, το οποίο είναι γνωστό, και τα πιο σημαντικά bits της μυστικής τιμής του Y. Θα μπορούσε γι' αυτό να υπάρχει μια συσχέτιση μεταξύ των τιμών των ανωτέρων bits του x και του συνολικού χρόνου για τη σχετική μείωση.

Εξετάζοντας για τις μεγαλύτερες πιθανότητες των παραδειγμάτων, ο εισβολέας θα προσπαθούσε να αναγνωρίσει το παραπάνω bit. Όσα περισσότερα παραπάνω bits του x γίνουνε γνωστά, τόσο περισσότερα γινόμενα x-x γίνονται γνωστά, επιτρέποντας έτσι στον εισβολέα να επεξεργαστεί μέσω περισσοτέρων επαναλήψεων το σχετικό loop της μείωσης για να επιτεθεί σε νέα bits του x.

5.9.6 Επιθέσεις κατανάλωσης ισχύος

Οι επιθέσεις αυτές βασίζονται στην ανάλυση της κατανάλωσης ισχύος της μονάδας καθώς αυτή εκτελεί τη λειτουργία της κωδικοποίησης. Καταναλώνοντας η μονάδα την ισχύ είτε με την απλή ή με την διαφορική ανάλυση ένας εισβολέας μπορεί να μάθει τις πράξεις που συμβαίνουν μέσα στην μονάδα και να αποκτήσει κάποιες πληροφορίες οι οποίες συνδυαζόμενες με άλλες τεχνικές κρυπτοανάλυσης, μπορούν να βοηθήσουν στην ανάκτηση του μυστικού κλειδιού.

Όπως περιγράφηκε νωρίτερα, ολοκληρωμένα κυκλώματα είναι φτιαγμένα από ανεξάρτητα tramsistors, τα οποία δρουν σε διακόπτες ελέγχου τάσεως. Το ρεύμα διαχέεται διαμέσου του τραντζίστορ ή απομακρύνεται απ'αυτή. Το ρεύμα έπειτα μεταφέρει φόρτιση στις πύλες των άλλων τραντζίστορ, διασυνδεόμενων καλωδίων και άλλα φορτία ρεύματος. Η κίνηση του ηλεκτρικού φορτίου καταναλώνει ισχύ και παράγει ηλεκτρομαγνητική ακτινοβολία που και τα δυο μαζί είναι παρά πολύ ανιχνεύσιμα.

Για τον υπολογισμό της κατανάλωσης ισχύος κυκλωμάτων ένας μικρός (περ. 50ohm) αντιστάτης εισέρχεται σε σειρά με την είσοδο ισχύος ή της γείωσης. Η διαφορά δυναμικού διαμέσου του αντιστάτη διαιρείται από τις τρέχουσες αμείωτες τιμές της αντίστασης. Τα καλά εξοπλισμένα ηλεκτρονικά εργαστήρια έχουν τέτοιο εξοπλισμό που μπορεί να δοκιμάσουν ψηφιακά, διαφορές τάσης σε εξαιρετικά ψηλές συχνότητες (πάνω από 1GHZ) με καταπληκτική ακρίβεια (μικρότερη του 1% σφάλμα). Οι συσκευές αυτές είναι ικανές για δοκιμές στα 20MHZ.

5.9.7 SPA επιθέσεις (Απλή ανάλυση ισχύος)

Βασίζεται κυρίως στην έρευνα της αντιπροσώπευσης της κατανάλωσης ισχύος μιας μονάδος καθώς η λειτουργία της κωδικοποιήσεις έχει εκτελεστεί. SPA είναι μια τεχνική που εμπεριέχει απευθείας διερμηνεία των μέτρων κατανάλωσης ισχύος η οποία συσσωρεύεται κατά τη διάρκεια λειτουργιών κρυπτογράφησης SPA μπορεί να αποφέρει πληροφορίες για μια λειτουργία συσκευής τόσο καλά όσο και ένα κλειδί.

Ο εισβολέας κατευθείαν παρατηρεί την κατανάλωση ισχύος του συστήματος. Το σύνολο της ισχύος που καταναλώνεται ποικίλλει εξαρτημένο από τις οδηγίες του επεξεργαστή που εκτελούνται.

Επειδή το SPA μπορεί να αποκαλύψει τις ακολουθίες των εντολών που εκτελούνται, μπορεί να χρησιμοποιηθεί για να σπάσει κρυπτογραφικές επιτυχίες μέσα στις οποίες το μονοπάτι εκτέλεσης εξαρτάται από την επεξεργασμένη πληροφορία, όπως το κλειδί προγράμματος DES, ανταλλαγές DES, συγκρίσεις, πολλαπλασιαστές και exponentiators.

Οι περισσότερες κρυπτογραφικές μονάδες που έχουν εξεταστεί βρέθηκαν να είναι τρωτές στις SPA επιθέσεις, ακόμα κι αν τέτοια συστήματα που να μην είναι τρωτά δεν είναι δύσκολο να σχεδιαστούν.

Μεγάλα χαρακτηριστικά όπως DES rounds, RSA λειτουργίες κ.λ.π. μπορούν να αναγνωρισθούν, αφού οι λειτουργίες προκαλούνται ποικίλως από τον μικροεπεξεργαστή κατά τη διάρκεια διαφορετικών τμημάτων των λειτουργιών αυτών. Η ανάλυση SPA μπορεί για παράδειγμα μπορεί να χρησιμοποιηθεί για να σπάσει RSA επιτυχίες αποκαλύπτοντας διαφορές μεταξύ λειτουργιών και πολυπλοκότητας και λειτουργιών ισορροπίας.

Ομοίως, πολλές επιτυχίες του DES έχουν ορατές διαφορές μέσα στις ανταλλαγές και τις αλλαγές και γι' αυτό μπορούν να σπάσουν χρησιμοποιώντας SPA.

5.9.8 Επιθέσεις Διαφορικής Ανάλυσης Ισχύος (DPA)

Οι επιθέσεις DPA αποτρέπονται πιο δύσκολα. Σύγκεινται όχι μόνο σε οπτικές αλλά και σε στατιστικές αναλύσεις και διορθώσεις λαθών των στατιστικών μεθόδων προκειμένου να αποκτήσουν πληροφορίες γύρω από τα κλειδιά. Το DPA συνήθως σύγκειται στη συλλογή πληροφοριών και στα στάδια ανάλυσης πληροφοριών, οι οποίες κάνουν μακρά χρήση των στατιστικών λειτουργιών για φιλτράρισμα θορύβου τόσο καλό όσο απαιτείται για την απόκτηση προσθετικών πληροφοριών για τις επεξεργασίες που η μονάδα εκτελεί.

Σε αντίθεση με τις παραλλαγές των μεγάλων βαθμίδων ισχύος εξαιτίας της ακολουθίας οδηγών, υπάρχουν αποτελέσματα που συσχετίζονται με τις τιμές των πληροφοριών που έχουν χειριστεί. Αυτές οι παραλλαγές τείνουν να είναι μικρότερες από την μέτρηση λαθών και άλλων θορύβων. Σε τέτοιες περιπτώσεις, είναι πιθανόν να σπάσει το σύστημα χρησιμοποιώντας στατιστικές λειτουργίες σχεδιασμένες στον αλγόριθμο του στόχου.

Επειδή το DPA αυτόματα εντοπίζει συσχετιζόμενα πεδία στην κατανάλωση ισχύος σε μια συσκευή, ο εισβολέας μπορεί να αυτοματοποιηθεί και να απαιτεί λίγες ή καθόλου πληροφορίες για τον επικείμενο στόχο.

Σε γενικές γραμμές, για την επιτυχία μιας επίθεσης DPA, ένας εχθρός παρατηρεί πρώτα τις λειτουργίες κωδικοποίησης της και αιχμαλωτίζει ίχνη ισχύος T[1::m] [1::K] διατηρώντας το καθένα τα K δείγματα. Εξάλλου ο εισβολέας εγγράφει τον κώδικα κειμένου c[1::m]. Δεν απαιτείται καμία γνώση του κυρίως κειμένου. Η ανάλυση DPA χρησιμοποιεί μέτρα κατανάλωσης ισχύος και στατιστικές μεθόδους για να αποφασίσει εάν το κλειδί K είναι σωστό. Αναλύοντας πρώτα μια εξωτερική λειτουργία DES, χρησιμοποιώντας το κλειδί που προκύπτει για να αποκωδικοποιήσει τα κείμενα κώδικα, και επιθέτοντας το επόμενο DES κλειδί μπορεί να βρει τα τριπλά DES κλειδιά. Το DPA μπορεί να χρησιμοποιεί γνωστό κυρίως κείμενο ή γνωστό κώδικα κειμένου και να βρει κλειδιά κωδικοποίησης ή αποκωδικοποίησης.

Κάποιες βελτιώσεις μπορούν να εφαρμοστούν στη συλλογή πληροφοριών και στις επικείμενες αναλύσεις DPA για να μειώσει τον αριθμό των απαιτούμενων δειγμάτων ή να καταστρατηγήσει countermeasures. Για παράδειγμα, είναι χρήσιμο να εφαρμόζεις διορθώσεις για διαφορετικά μέτρα ενδίδοντας στη σημασία των διαφοροποιήσεων αντί των μεγεθών τους.

Μια παραλλαγή αυτής της προσέγγισης, το αυτόματο υποστήριγμα DPA, μπορεί να βρει κλειδιά DES χρησιμοποιώντας λιγότερα από 15 ίχνη από τις πιο έξυπνες κάρτες. Τα κοινά αλγοριθμικά κλειδιά μπορούν να αναλυθούν χρησιμοποιώντας το DPA συσχετίζοντας υποψήφιες τιμές για υπολογισμό ενδιάμεσων με τα μέτρα κατανάλωσης ισχύος.

Το (HO-DPA) εμπεριέχει σε καταναλώσεις ισχύος μεταξύ κάποιων υπολειτουργιών της λειτουργίας κωδικοποίησης (και όχι μόνο στην λειτουργία γενικώς). Επίσης, αφού οι τεχνικές DPA περιγράφονται πάνω από αναλυμένες πληροφορίες δια μέσου ενός απλού γεγονότος μεταξύ δειγμάτων, η ζητούμενη DPA μπορεί να χρησιμοποιηθεί για να συσχετίσει πληροφορίες μεταξύ πολύ κρυπτογραφικών υπολειτουργιών. Αξίζει να σημειωθεί ότι εκεί δεν είναι καμία γνωστή μονάδα που είναι τρωτή στο HO-DPA και δεν είναι τρωτή στη DPA επίσης. Ακόμη ότι έχει γίνει για να εμποδίσει το DPA πρέπει να λειτουργήσει εναντίον του HO-DPA.

Με άλλα λόγια, οι προφυλάξεις που έχουν παρθεί για να εμποδίσουν το DPA πρέπει να είναι τέτοιες ώστε να λειτουργήσουν ενάντια των HO-DPA όσο καλύτερα

γίνεται, αν και κανένα σύστημα δεν είναι γνωστό ότι αντιστέκεται στο DPA και στο HO-DPA.

5.9.9 Επιθέσεις (DFA) σε διαφορική ανάλυση σφάλματος

Συσχετίζει την ικανότητα να ερευνήσει κώδικες και να αποσπάσει κλειδιά δημιουργώντας σφάλματα σε ένα σύστημα το οποίο είναι υπό κατοχή ενός εισβολέα, ή από φυσικά λάθη που συμβάλλουν. Τα λάθη περισσότερα συμβαίνουν συχνά από αλλαγή της τάσης, από ζημιές στο ρολόι, ή με την εφαρμογή ακτινοβολίας διαφόρων τύπων.

Οι επιθέσεις βασίζονται στην κωδικοποίηση του ίδιου τμήματος πληροφορίας (το οποίο δεν είναι απαραίτητα γνωστό στον εισβολέα), δυο φορές, και συγκρίνοντας τα αποτελέσματα. Η διαφορά ενός bit δηλώνει ένα σφάλμα σε μια από τις λειτουργίες. Σήμερα, ένας μικρός υπολογισμός μπορεί να εφαρμοστεί για το DES, π.χ. για να αναγνωρίσει που ακριβώς έγινε το λάθος. Ένα ολόκληρο σετ λειτουργιών μπορεί να επιτευχθεί για την ανάκτηση ενός υποκλειδίου DES το οποίο είναι γνωστό ο εισβολέας μπορεί είτε να μαντέψει τα 8 bit που λείπουν (το τελευταίο υποκλείδι χρησιμοποιεί 48bits), για τα οποία υπάρχουν μόνο 256 επιλογές, ή απλώς να εγκαταλείψουν τον τελευταίο γύρο για τον οποίο ξέρει το υποκλείδι και εκτελεί την επίθεση στο μειωμένο DES. Η δεύτερη αυτή μέθοδος μπορεί να χρησιμοποιηθεί επίσης εναντίον Triple-DES.

Συχνά, το DFA μπορεί να συνδυαστεί με άλλες επιθέσεις όπως τις διαφορικές επιθέσεις κλειδιών ή διαφορικές κρυπταναλύσεις συσχετιζόμενων κλειδιών.

Ένας άλλος τύπος ανάλυσης λάθους είναι η NDFA (Non-Differential Fanlt Analysis) αλλά αυτή βασίζεται στη προξένηση μόνιμων βλαβών σε συσκευές για τον σκοπό της απόσπασης συμμετρικών κλειδιών (τέτοια όπως το DES). Πρέπει να αναφερθεί ότι αυτό το χαρακτηριστικό τέτοιων επιθέσεων είναι ότι δεν απαιτούν διορθωμένα κείμενα κώδικα (τα κείμενα κώδικα που παρήχθησαν πριν την βλάβη της μονάδας). Αυτό οδηγεί στο να γίνει ικανός ο εισβολέας να χρησιμοποιήσει λανθασμένες μονάδες.

5.10 Γενικά μέτρα αντιμετώπισης εναντίον όλων των επιθέσεων

5.10.1 Γενικοί υπολογισμοί Ανεξάρτητων πληροφοριών

Γενικά, όλες οι λειτουργίες που εκτελούνται από το πρότυπο μπορεί να είναι ανεξάρτητες της πληροφορίας στον χρόνο κατανάλωσης τους. Με άλλα λόγια, ο

χρόνος που παίρνουν οι λειτουργίες πρέπει να είναι καθ' ολοκλήρου ανεξάρτητες από την είσοδο πληροφορίας ή του κλειδιού πληροφορίας. Οπότε οι διαφορετικές υπολειτουργίες εκτελούνται σχετικά με την είσοδο ή τα bits κλειδιών, και αυτές οι υπολειτουργίες πρέπει να παίρνουν τον ίδιο αριθμό κύκλων ρολογιού.

Το γενικό χαρακτηριστικό της δημιουργίας του χρόνου που χρειάζεται για την λειτουργία εκτέλεσης ορισμένο για κάθε κομμάτι πληροφορίας εμποδίζει όλες τις επιθέσεις χρονισμού. Αυτό συμβαίνει γιατί αυτές οι επιθέσεις βασίζονται στις παραλλαγές στον υπολογισμό του χρόνου σχετικά με την είσοδο και τα bits κλειδιών. Η μόνη είσοδος που μπορεί να έχει ένα αποτέλεσμα στον χρόνο που χρειάζεται η λειτουργία, είναι το μήκος του διανύσματος (exponent) στις διανυσματικές λειτουργίες. Παρόλ' αυτά το μήκος αυτό είναι: πληροφορία με καμία αξία σημασίας για τον εισβολέα.

5.10.2 Τύφλωση

Οι τεχνικές που χρησιμοποιούνται για τις τυφλές υπογραφές μπορούν να προσαρμοστούν για να εμποδίσουν εισβολείς από την γνώση της εισόδου στην πρότυπη λειτουργία. Αυτό θα μπορούσε να βοηθήσει εναντίον οποιουδήποτε τύπου side-channel επίθεσης (επίπεδο ζεύξης).

Ακόμα και με την τύφλωση (blinding), η δοκιμή θα αποκαλύψει τον μέσο χρόνο ανά λειτουργία, ο οποίος μπορεί να χρησιμοποιηθεί για να συμπεράνει το βάρος Hamming του δείκτη. Εάν η αυτονομία είναι σημαντική ή η μεταμφίεση απαιτείται, ένα τυχαίο πολ/σιο μπορεί να προστεθεί στον δείκτη before each modular exponentiation. Εάν αυτό συμβεί, πρέπει να φροντίσουμε να διασφαλίσουμε ότι η πρόσθετη επεξεργασία δεν έχει χαρακτηριστικά χρονισμού, τα οποία μπορούν να αποκαλύψουν τα τυχαία πολ/σια. Η τεχνική αυτή μπορεί να βοηθήσει στην αποτροπή επιθέσεων που αποκτούν πληροφορίες διαρρεόμενες κατά τη διάρκεια της πρότυπης λειτουργίας exfonentiation εξαιτίας της ηλεκτρομαγνητικής ακτινοβολίας, διακύμανσης εμφάνισης συστήματος, αλλαγές στην κατανάλωση ισχύος κλπ αφού τα bits του δείκτη αλλάζουν με κάθε μια λειτουργία.

5.10.3 Αποφυγή συνηθισμένων διακλαδώσεων και μυστικών ενδιάμεσων

Η αποφυγή διαδικασιών που χρησιμοποιούν μυστικούς διαμεσολαβητές ή κλειδιά για συνήθεις λειτουργίες θα αποκρύψει πολλά SPA χαρακτηριστικά.

Οι υπολογισμοί θα εκτελεσθούν χρησιμοποιώντας λειτουργίες που χρησιμοποιούν στοιχειώδεις λειτουργίες (όπως AND, OR και XOR) και όχι χρησιμοποιώντας διακλάδωση και συνήθη εκτέλεση τμημάτων του κώδικα. Το

χαρακτηριστικό αυτό μπορεί να κάνει παρά πολύ δύσκολη την είσοδο και τις τιμές των κλειδιών προσπαθώντας να βρεί μέτρα κατανάλωσης χρόνου ή ισχύος.Μια συνήθης εκτέλεση, η οποία εξαρτάται από πληροφορία κλειδιού ή από την είσοδο, μπορεί εύκολα να αποκαλύψει μέρη πληροφορίας, εάν ο εισβολέας μετρήσει τον χρόνο ή την ισχύ που πήρε για να εκτελέσει συγκεκριμένες πράξεις. Όταν όλες οι γραμμές του κώδικα τρέχουν πάντα χωρίς να λογαριάζουν την είσοδο και τα bits κλειδιών, ο χρόνος και η ισχύς που πάρθηκε για την εκτέλεση αυτών των πράξεων δεν εξαρτάται από την πληροφορία και γι' αυτό δεν αποκαλύπτει κάποιο από τα μέρη του.

Το χαρακτηριστικό αυτό εμποδίζει όλους τους τύπους επιθέσεων χρονισμού σε ασύμμετρους κώδικες τόσο καλά όσο κάποιες επιθέσεις κατανάλωσης ισχύος.

5.10.4 Άδεια τροποποιημένων αλγορίθμων

Η πιο αποτελεσματική λύση είναι ο σχεδιασμός για την επιτυχία κρυπτοσυστημάτων, με την υπόθεση πάντα, ότι η πληροφορία θα διαρρεύσει. Μερικές εταιρείες αναπτύσσουν προσεγγίσεις για την ασφάλεια υπαρχόντων κρυπτογραφικών αλγορίθμων (συμπεριλαμβανόμενου RSA, DES, DSA, Diffie-Hellman, GI Gamal, Elliptic Curse Systems) για την δημιουργία συστημάτων που να παραμένουν ασφαλή ακόμα και αν τα βασικά κυκλώματα μπορεί να διαρρέουν πληροφορίες.

5.11 Μέτρα αντιμετώπισης εναντίον επιθέσεων χρονισμού

5.11.1 Πρόσθεση καθυστερήσεων

Ο πιο συνήθης τρόπος να εμποδιστούν επιθέσεις χρονισμού, είναι να μπορούν όλες οι λειτουργίες να παίρνουν ακριβώς τον ίδιο χρόνο. Δυστυχώς αυτό είναι συχνά δύσκολο, εάν ένας timer χρησιμοποιείται για να καθυστερήσει επιστροφές αποτελεσμάτων μέχρι του λεπτομερούς χρόνου, γιατί, παράγοντες όπως η ανταπόκριση συστήματος ή η κατανάλωση ισχύος μπορούν να αλλάξουν ακόμη και όταν η λειτουργία τελειώνει κατά τέτοιο τρόπο που θα μπορούσε να ανιχνευθεί.

Συγκεκριμένοι χρόνοι επιτυχίας συνηθίζονται να είναι αργοί,επίσης πολλές μεθοδολογίες εμφάνισης δεν μπορούν να χρησιμοποιηθούν αφού όλες οι λειτουργίες πρέπει να παίρνουν τόσο χρόνο όσο και οι αργές λειτουργίες. Όταν οι καθυστερήσεις προστίθενται τυχαία, αν και αυτές οι τυχαίες καθυστερήσεις αυξάνουν τον απαιτούμενο αριθμό των κειμένων του κώδικα, οι εισβολείς μπορούν να επιτύχουν συγκεντρώνοντας περισσότερα μέτρα.

Ο αριθμός των δειγμάτων που απαιτούνται αυξάνεται ανώμαλα όπως square of the timing troise. Έτσι, οι τυχαίες καθυστερήσεις μπορούν να κάνουν την επίθεση ένα bit περισσότερο δύσκολη, αλλά ακόμα πιθανή.

5.12 Μέτρα αντιμετώπισης εναντίον επιθέσεων ανάλυσης ισχύος

5.12.1 1Ισορροπία Κατανάλωσης ισχύος

Οι τεχνικές αυτές θα είναι εφαρμόσιμες όπου είναι δυνατόν. Όποτε μια λειτουργία εκτελείται στο hardware, μια συμπληρωματική λειτουργία θα πρέπει να εκτελείται για να διαβεβαιώσει ότι η συνολική κατανάλωση ισχύος της μονάδας διατηρεί ισορροπία σχετικά με τις ψηλές τιμές.

Τέτοα σχετική λειτουργία με την οποία η κατανάλωση ισχύος είναι σταθερή και ανεξάρτητη από τις εισόδους και τα bits κλειδιών, εμποδίζει όλα τα είδη των επιθέσεων κατανάλωσης ισχύος όπως το SPA και DPA.

5.12.2 Μείωση του μεγέθους του σήματος

Μια προσέγγιση για την αποτροπή επιθέσεων DPA είναι η μείωση των μεγεθών σημάτων, όπως η χρησιμοποίηση ενός σταθερού μονοπατιού εκτέλεσης κώδικα, και ισορροπώντας βάρη Hanging και να αναφέρουν μεταβάσεις ή να προασπίζουν φυσικώς την συσκευή. Δυστυχώς, τέτοια μείωση μεγέθους σήματος γενικά, δεν μειώνει το μέγεθος του σήματος στο μηδέν, όπως ένας εισβολέας με έναν άπειρο αριθμό δειγμάτων, που είναι ικανός να εκτελέσει DPA στο (υψηλά διαβαθμισμένο) σήμα.

5.12.3 Πρόσθεση θορύβου

Άλλη μια προσέγγιση εναντίον του DPA είναι η εισαγωγή θορύβου μέσα στα μέτρα για την κατανάλωση ισχύος.

Όπως οι μειώσεις μεγέθους σήματος,έτσι και η πρόσθεση θορύβου αυξάνει τον αριθμό των απαιτούμενων δειγμάτων για την επίθεση, πιθανώς σε ένα μεγάλο αριθμό. Εξάλλου, η εκτέλεση χρονισμού και η τάξη μπορεί να υποτίθεται ότι παράγει ένα παρόμοιο αποτέλεσμα. Ξανά, μόνος του ο χρόνος αυξάνει τον αριθμό των δειγμάτων που απαιτούνται, παρόλα αυτά εάν αυτός αυξάνεται, είναι αρκετά μεγάλος για να κάνει την δειγματοληψία ακατόρθωτη, εξαιτίας του απαιτούμενου αριθμού δειγμάτων, οπότε το μέτρο αντιμετώπισης λειτουργεί κανονικά

Μια επίλυση του προβλήματος για να αποφευχθούν επιθέσεις DPA χρησιμοποιώντας τον θόρυβο, είναι η πρόσθεση τυχαίων υπολογισμών που αυξάνουν το επίπεδο θορύβου αρκετά, για να κάνει τα σημεία κλίσης DPA (DPA bias spikes)

μη ανιχνεύσιμα. Ο κύριος στόχος είναι να προστεθεί αρκετός τυχαίος θόρυβος για να σταματήσει μια επίθεση, και όχι μόνο να προσθέσει μια minimal επικεφαλίδα.

5.12.4 Προστασία

Πρακτικά, μια φυσική ασπίδα μπορεί να κάνει τις επιθέσεις ακατόρθωτες αλλά και να προσθέσει σημαντικά σε μια συσκευή το κόστος και το μέγεθος.

5.12.5 Τροποποίηση του Σχεδιασμού Αλγορίθμου

Μια τελευταία προσέγγιση εναντίον των επιθέσεων του DPA είναι ο σχεδιασμός κρυπτοσυστημάτων με ρεαλιστικές υποθέσεις για το επικείμενο (underlying) hardware. Σαν απλό παράδειγμα, hashing ένα 160 bito κλειδί με το SHA πριν την χρησιμοποίηση του σαν κλειδί θα μπορούσε αποτελεσματικά να καταστρέψει μερικές πληροφορίες που πιθανόν ένας εισβολέας να έχει μαζέψει για το κλειδί. Ομοίως, η χρήση του δείκτη και της τροποποίησης του προτύπου (modulus) των επεξεργαστών σε κοινό κλειδί σχεδίων μπορεί να χρησιμοποιηθεί για να εμποδίσει τους εισβολείς από μια συσσώρευση πληροφοριών μέσα από έναν μεγάλο αριθμό λειτουργιών.

Αυτό μπορεί να λύσει το πρόβλημα, αλλά απαιτεί αλλαγές σχεδιασμού στους αλγόριθμους και στα ίδια τα πρωτόκολλα τα οποία είναι δυνατόν να κάνουν το αποτελεσματικό προϊόν να μη ενδίδει με τα στάνταρ και τις λεπτομέρειες.

5.13 Μέτρα αντιμετώπισης εναντίον λαθών επιθέσεων

5.13.1Τρέξιμο δυο φορές της κωδικοποίησης

Μια πιθανή λύση εναντίον ενός DFA είναι να τρέξει η μονάδα την κωδικοποίηση δυο φορές και να εξάγει τα αποτελέσματα, μόνο εάν αυτά τα δυο είναι εντελώς ίδια. Το κυρίως πρόβλημα με την προσέγγιση είναι ότι αυτό αυξάνει τον χρόνο υπολογισμού. Επίσης, η πιθανότητα ότι το σφάλμα δεν θα συμβεί δυο φορές δεν είναι επαρκώς μικρό. Αφού το σφάλμα μπορεί ακόμα να συμβεί δυο φορές αυτό το μέτρο αντιμετώπισης θα κάνει τον εισβολέα πιο αποτελεσματικό προκειμένου να πετύχει.

5.14 .Επίπεδο δικτύου (Routing Network)

5.14.1 Επιθέσεις στο επίπεδο δικτύου αισθητήρα

Πολλά πρωτόκολλα επιπέδου δικτύου αισθητήρων είναι αρκετά απλά, και γι' αυτό το λόγο είναι κάποιες φορές ευαίσθητα σε επιθέσεις. Οι περισσότερες επιθέσεις στρώματος δικτύου εναντίον δικτύων αισθητήρων ανήκουν σε μια από τις ακόλουθες κατηγορίες:

- Εξαπάτηση, αλλαγή ή ξαναπαίξιμο πληροφοριών δρομολόγησης
- Επιλεκτικές προωθήσεις
- Sinkhole επιθέσεις
- Sybil επιθέσεις
- Wormholes επιθέσεις
- HELLO flood επιθέσεις
- Ομολογία εξαπάτησης

5.14.2 Εξαπάτηση, αλλαγή ή ξαναπαίξιμο πληροφοριών δρομολόγησης

Η πιο απευθείας επίθεση εναντίον ενός πρωτοκόλλου δρομολόγησης είναι η στόχευση στις ανταλλασόμενες πληροφορίες της δρομολόγησης μεταξύ των κόμβων. Εξαπατώντας, ή αλλάζοντας ή ξαναπαίζοντας τις δρομολογημένες πληροφορίες, οι εχθροί μπορούν να γίνουν ικανοί να δημιουργήσουν loops δρομολόγησης, να έλκουν ή να απωθούν την κυκλοφορία δικτύου ή μεγάλα ή μικρά δρομολόγια πηγών, να δημιουργήσουν λανθασμένα μηνύματα λαθών, διαίρεση του δικτύου, αύξηση αφάνειας end to end κ.ο.κ.

5.14.3 Επιλεκτική προώθηση

Τα δίκτυα πολλαπλών κόμβων συνήθως βασίζονται στην υπόθεση ότι οι συμμετέχοντες κόμβοι θα προωθήσουν τα λαμβανόμενα μηνύματα. Σε μια επίθεση επιλεκτικής προώθησης, οι κακεντρεχείς κόμβοι, μπορεί να αρνηθούν να προωθήσουν συγκεκριμένα μηνύματα και απλά να τα πετάξουν διαβεβαιώνοντας ότι δεν θα διαδοθούν άλλο. Μια απλή μορφή αυτής της επίθεσης είναι όταν ο κακοντρεχής κόμβος συμπεριφέρεται σαν blackhole και αρνείται να προωθήσει κάθε πακέτο που βλέπει. Παρόλα αυτά ένας τέτοιος εισβολέας παίρνει το ρίσκο ότι οι γειτονικοί κόμβοι θα τελειώσουν ό,τι αυτός έχει αποτύχει και θα αποφασίσει να ψάξει άλλο δρομολόγιο. Μια περισσότερο έξυπνη μορφή αυτής της επίθεσης είναι όταν ένας εχθρός επιλεκτικά προωθεί πακέτα.

Οι επιθέσεις σε επιλεκτικές προωθήσεις είναι τυπικά οι πιο αποτελεσματικές,όταν ο εισβολέας συμπεριλαμβάνεται ρητώς στο μονοπάτι της πληροφορίας που τρέχει. Παρόλα αυτά είναι κατανοητό, ότι ένας εισβολέας που υποκλέπτει μια ροή διαμέσου γειτονικών κόμβων θα μπορούσε να είναι ικανός να πλαστογραφεί επιλεκτικές προωθήσεις συνωστίζοντας ή δημιουργώντας μια σύγκρουση σε κάθε προωθούμενο ενδιαφέρον πακέτο. Πιστεύουμε ότι ένας εχθρός κάνοντας μια επίθεση επιλεκτικής προώθησης θα ακολουθήσει το μονοπάτι της

λιγότερης αντίστασης και θα προσπαθήσει να συμπεριλάβει τον εαυτό του στο πραγματικό μονοπάτι της ροής πληροφοριών.

5.14.4 Sinkhole επιθέσεις

Σε μια sinkhole επίθεση, ο στόχος του εχθρού είναι να ελκύσει (δελεάσει) κοντά όλη τη κυκλοφορία από μια ιδιαίτερη περιοχή μέσω ενός συμβιβαστικού κόμβου, δημιουργώντας ένα μεταφορικό sinkhole με τον εχθρό στον κέντρο.

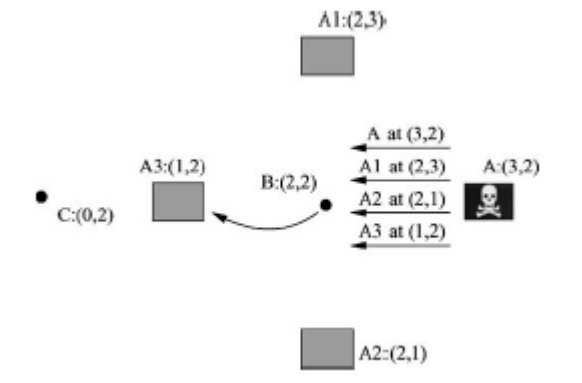
Οι επιθέσεις sinkhole χαρακτηριστικά δουλεύουν κάνοντας έναν συμβιβαστικό κόμβο να φαίνεται ελκυστικό στους γύρω κόμβους με σεβασμό στον αλγόριθμο δρομολόγησης. Για μια στιγμή, ένας εχθρός θα μπορούσε να εξαπατήσει ή να ξαναπαίξει μια αγγελία για ένα ακραίο υψηλής-ποιότητας δρομολόγιο, σε μια βάση σταθμό. Κάποια πρωτόκολλα θα μπορούν να προσπαθήσουν να επιβεβαιώσουν την ποιότητα του δρομολογίου με αναγνωρίσεις end-to-end εμπεριέχοντας αξιοπιστία ή αφάνεια πληροφορίας. Σ' αυτή την περίπτωση, ένας εχθρός μπορεί πράγματι «να παρέχει» ένα δρομολόγιο υψηλής ποιότητας εκπέμποντας με αρκετή ισχύ για να προσεγγίσει την βάση σταθμό σε ένα απλό hop, ή χρησιμοποιώντας μια επίθεση wormhole. Εξαιτίας, είτε της πραγματικής, είτε της φανταστικής υψηλής ποιότητας δρομολογίου διαμέσου του συμβιβαστικού κόμβου, είναι σαν ο κάθε γειτονικός κόμβος του εχθρού να προωθεί πακέτα προοριζόμενα για την βάση σταθμό μέσω του εχθρού και να διαδίδει την ελκυστικότητα του δρομολογίου στους γειτονικούς του. Αποτελεσματικά, ο εχθρός δημιουργεί μια μεγάλη «σφαίρα επιρροής», έλκοντας όλες τις κυκλοφορίες που προορίζονται για μια βάση σταθμό από κόμβους μερικών ή περισσοτέρων hops μακριά από τον συμβιβασμένο κόμβο. Ένα κίνητρο για την αύξηση μιας επίθεσης sinkhole είναι ότι αυτή κάνει ασήμαντες επιλεκτικές προωθήσεις. Διαβεβαιώνοντας ότι όλες οι κυκλοφορίες στην περιοχή στόχου διακινούνται μέσω ενός συμβιβαστικού κόμβου, ένας εχθρός μπορεί επιλεκτικά να καταστείλει ή να τροποποιήσει πακέτα δημιουργημένα από οποιονδήποτε κόμβο στην περιοχή.

Θα έπρεπε να σημειωθεί ότι ο λόγος που τα δίκτυα αισθητήρων είναι ιδιαίτερα ευαίσθητα σε επιθέσεις sinkhole είναι εξαιτίας των ειδικευμένων προτύπων επικοινωνίας. Αφού όλα τα πακέτα μοιράζονται τον ίδιο τελικό προορισμό (στα δίκτυα με μια μόνο βάση σταθμό) ένας συμβιβαστικός κόμβος χρειάζεται μόνο να παρέχει ένα απλό δρομολόγιο υψηλής ποιότητας στη βάση σταθμό προκειμένου να επιδράσει έναν δυνατό μεγάλο αριθμό κόμβων.

5.14.5 Η επίθεση Sybil

Σε μια επίθεση Sybil, ένας απλός κόμβος παρουσιάζει πολλαπλές ταυτότητες στους άλλους κόμβους στο δίκτυο. Η επίθεση Sybil μπορεί σημαντικά να μειώσει την αποτελεσματικότητα των εσφαλμένων ανεκτικών σχεδίων όπως διανεμειμένη χωρητικότητα, διασπορά και δρομολόγηση πολλών μονοπατιών, και συντήρηση τοπολογίας.

Οι επιθέσεις Sybil επίσης παρουσιάζουν μια σημαντική απειλή στα γεωγραφικά πρωτόκολλα δρομολόγησης. Η ενημέρωση τοποθεσίας δρομολόγησης.συχνά απαιτεί τους κόμβους να ανταλλάσσουν ίσες πληροφορίες με τους γειτονικούς τους σε ικανά απευθυνόμενα πακέτα σε γεωγραφικά δρομολόγια. Δικαιολογείται να περιμένουμε έναν κόμβο να δέχεται όχι μόνο ένα απλό σετ με ίδιους από τον καθένα γειτονικό του (κόμβο) αλλά χρησιμοποιώντας την επίθεση Sybil ένας εχθρός μπορεί να είναι σε περισσότερα από ένα μέρη μια φορά. Στο παρακάτω σχήμα φαίνεται μία επίθεση SYBIL εναντίον γεωγραφικής δρομολόγησης.



Σχήμα 5.1 Ο εχθρός Α στην τοποθεσία (3,2) πλαστογραφεί τοποθεσίες για τους μη υπάρχοντες κόμβους Α1,Α2 και Α3τόσο καλά σαν να διαφημίζει την τοποθεσία του.Μετα απ'αυτό εάν ο Β θέλει να στείλει ένα μήνυμα στον προορισμό (0,2) θα προσπαθήσει να το κάνει μέσω του Α3.Η μετάδοση αυτή μπορεί να υποκλαπεί και να χειριστεί από τον εχθρό Α. **(9)**

5.14.6 Wormholes

Στην επίθεση wormholes ένας εχθρός εισέρχεται σε παρεληφθέντα μηνύματα σε ένα μέρος του δικτύου πάνω από τους δεσμούς με χαμηλή αφάνεια και επαναλαμβάνοντας αυτά σε διαφορετικό κομμάτι.

Το πιο απλό παράδειγμα τέτοιας επίθεσης είναι ένας απλός κόμβος εντοπισμένος ανάμεσα σε δυο άλλους κόμβους προωθώντας μηνύματα μεταξύ των δυο απ' αυτών. Παρόλα αυτά, οι επιθέσεις wormhole κοινώς εμπλέκουν δυο

μακρινούς κακεντρεχείς κόμβους που συνομωτούν να υποτιμήσουν την απόστασή τους από το κάθε ένα αντικατεστημένο πακέτο, σε συμφωνία με ένα end-of-bound κανάλι διαθέσιμο μόνο στον εισβολέα.

Ένας εχθρός εντοπισμένος σε μια βάση σταθμό μπορεί να γίνει ικανός να διακόψει εξ' ολοκλήρου τη δρομολόγηση δημιουργώντας ένα καλώς τοποθετημένο wormhole. Ένας εχθρός θα μπορούσε να πείσει τους κόμβους, που θα ήθελαν να είναι κανονικά πολλά hops από μια βάση σταθμό, ότι αυτοί είναι ένα ή δυο hops μακριά επίσης από το wormhole. Αυτό μπορεί να δημιουργήσει ένα sinhhole.

Το σχήμα 6 δείχνει ένα παράδειγμα ενός wormhole που χρησιμοποιείται για τη δημιουργία sinkhole.

Γενικότερα, τα wormholes μπορούν να χρησιμοποιηθούν για να εκμεταλλευτούν συνθήκες δρομολόγησης. Μια δρομολόγηση χαρακτηριστικά δημιουργείται όταν ένας κόμβος κάνει κάποιες ενέργειες βασισμένος στην πρώτη υπόδειξη του μηνύματός που λαμβάνει και ακολούθως αγνοεί αργότερα υποδείξεις αυτού του μηνύματος.

Στην περίπτωση αυτή ένας εχθρός μπορεί να γίνει ικανός να ασκήσει κάποια επιρροή στην αποτελεσματική τοπολογία εάν αυτό μπορεί να προξενήσει έναν κόμβο να λάβει κάποιες πληροφορίες δρομολόγησης πριν τις προσεγγίσει κανονικά ακόμα και με τη δρομολόγηση πολλών hop. Τα wormholes είναι ένας τρόπος για να γίνει αυτό, και είναι αποτελεσματικά ακόμα κι αν οι πληροφορίες δρομολόγησης είναι γνήσια ή κωδικοποιημένα. Οι επιθέσεις wormholes μπορούν επίσης να χρησιμοποιηθούν απλώς για να πείσουν δυο απομακρυσμένους κόμβους ότι είναι γείτονες με την αντικατάσταση πακέτων μεταξύ των δυο απ' αυτών.

Οι επιθέσεις wormhole θα μπορούσαν να χρησιμοποιούνται σε συνδυασμό με επιλεκτικές προωθήσεις ή υποκλοπές. Η ανίχνευση είναι αδύνατη όταν χρησιμοποιείται μαζί με την Sybil επίθεση.

5.14.7 Επίθεση HELLO ροών

Πολλά πρωτόκολλα απαιτούν κόμβους να εκπέμψουν HELLO πακέτα για να ανακοινώσουν τους εαυτούς τους στους γείτονες τους, και ένας κόμβος που λαμβάνει τέτοια πακέτα μπορεί να υποθέσει ότι αυτό είναι μέσα (κανονικά) στην τάξη πομποδεκτών του αποστολέα.

Η υπόθεση αυτή μπορεί να είναι εσφαλμένη: Ένας εισβολέας με ένα laptop εκπέμποντας δρομολογήσεις ή άλλες πληροφορίες με αρκετά μεγάλη ισχύ μετάδοσης θα μπορούσε να πείσει κάθε κόμβο στο δίκτυο ότι ο εχθρός είναι γείτονας του.

Για παράδειγμα, ένας εχθρός διαφημίζοντας ένα δρομολόγιο υψηλής ποιότητας στη βάση σταθμό σε κάθε κόμβο στο δίκτυο θα μπορούσε να παρακινήσει ένα μεγάλο αριθμό κόμβων να προσπαθήσουν να χρησιμοποιήσουν αυτό το δρομολόγιο, αλλά τέτοιοι κόμβοι θα έστελναν πακέτα μακριά από τον εχθρό . Το δίκτυο μένει σε κατάσταση σύγχυσης. Ο κόμβος που διαπιστώνει ότι ο δεσμός στον εχθρό είναι λάθος θα μπορούσε να έχει μερικές επιλογές. Όλοι οι γειτονικοί του μπορεί να προσπαθούν να προωθήσουν πακέτα στον εχθρό όσο το δυνατό πιο καλά.Επίσης, πρωτόκολλα που εξαρτώνται από ανταλλαγή πληροφοριών μεταξύ των γειτονικών κόμβων για συντήρηση τοπολογίας ή έλεγχο ροής, υπόκεινται σ' αυτήν την επίθεση.

Ένας εχθρός δεν χρειάζεται απαραίτητα να είναι ικανός να κατασκευάσει νόμιμες κυκλοφορίες προκειμένου να χρησιμοποιήσει επίθεση HELLO ροής. Αυτή μπορεί απλά να επανακπέμψει πακέτα επικεφαλίδας με αρκετή ισχύ για να λαμβάνονται από κάθε κόμβο στο δίκτυο. Οι ροές HELLO μπορούν επίσης να θεωρηθούν κατά κάποιο τρόπο ως wormholes εκπομπής.

5.14.8 Εξαπάτηση αναγνώρισης

Κάποιοι αλγόριθμοι δρομολόγησης δικτύου αισθητήρων βασίζονται σε υπονοούμενους ή σαφείς δεσμούς στρώματος αναγνώρισης. Εξαιτίας της ουσιαστικής μέσης εκπομπής, ένας εχθρός μπορεί να εξαπατήσει δεσμούς στρώματος αναγνωρίσεων για πακέτα επικεφαλίδος που απευθύνονται σε γειτονικούς κόμβους. Οι στόχοι περιλαμβάνουν το γεγονός ότι ο αποστολέας πρέπει να πειστεί ότι ο αδύναμος δεσμός είναι δυνατός ή ότι ένας νεκρός ή απενεργοποιημένος κόμβος είναι ζωντανός. Για παράδειγμα ένα πρωτόκολλο δρομολόγησης μπορεί να επιλέξει το επόμενο hop σε ένα μονοπάτι χρησιμοποιώντας αξιόπιστα δεσμούς. Ο τεχνητά εξαναγκασμός ενός αδύνατου ή νεκρού δεσμού είναι ένας λεπτός τρόπος για χειρισμό τέτοιων σχεδίων. Αφού τα πακέτα που στάλθηκαν με αδύναμους νεκρούς δεσμούς χάθηκαν, ένας εχθρός μπορεί αποτελεσματικά να εμφανίσει μια επίθεση επιλεκτικής προώθησης, χρησιμοποιώντας εξαπάτηση αναγνώρισης και ενθαρρύνοντας τον στόχο κόμβο να μεταδώσει πακέτα σ' αυτούς τους δεσμούς.

5.15. Αντίμετρα (Countermeasures)

5.15.1 Εξωτερικές επιθέσεις και ασφάλεια δεσμού στρώματος

Η πλειοψηφία των εξωτερικών επιθέσεων εναντίον των πρωτοκόλλων δρομολόγησης (routing) δικτύων αισθητήρων μπορούν να εμποδιστούν από απλή κωδικοποίηση δεσμού στρώματος και αυθεντικότητα χρησιμοποιώντας ένα σφαιρικό μοιρασμένο κλειδί. Η επίθεση Sybil δεν είναι σχετική γιατί οι κόμβοι είναι απρόθυμοι να δεχτούν ακόμα και μια απλή ταυτότητα του εχθρού. Η πλειοψηφία των sinkhole επιθέσεων και των επιλεκτικών προωθήσεων επιθέσεων δεν είναι δυνατή γιατί ο εχθρός εμποδίζεται από τη σύνδεση της τοπολογίας.

Οι δεσμοί στρώματος αναγνωρίσεων μπορούν τώρα να αυθεντικοποιηθούν. Οι περισσότερες μορφές των επιθέσεων που δεν μετρούνται από κωδικοποίηση δεσμού στρώματος και μηχανισμών αυθεντικότητας είναι οι επιθέσεις wormhole και οι HELLO flood επιθέσεις. Αν και ο εχθρός εμποδίζεται από τη σύνδεση του δικτύου, τίποτα δεν την εμποδίζει από την χρήση ενός wormhole στα πακέτα που στάλθηκαν από νόμιμους κόμβους σε ένα τμήμα του δικτύου σε νόμιμους κόμβους σε άλλο τμήμα να πείσει αυτά ότι είναι γειτονικά ή ενισχύοντας ένα πακέτο εκπομπής επικεφαλίδος με ακόλουθη ισχύ να λαμβάνεται από κάθε κόμβο στο δίκτυο.

Οι επιθέσεις εναντίον Tinyos εμφανίζουν αυτές τις τεχνικές, και οι μηχανισμοί ασφαλείας δεσμού στρώματος (επιπέδου ζεύξης) δεν μπορούν να κάνουν τίποτα για να τις εμποδίσουν. Εάν ένα wormhole έχει εμφανισθεί, η κωδικοποίηση μπορεί να κάνει κάποιες επιθέσεις επιλεκτικής προώθησης εναντίον πακέτων χρησιμοποιώντας το wormhole πιο δύσκολα.

Οι μηχανισμοί ασφαλείας επιπέδου ζεύξης που χρησιμοποιούν ένα σφαιρικά μοιραζόμενο κλειδί είναι εντελώς αναποτελεσματικές στην παρουσία εσωτερικών επιθέσεων ή συμβιβασμένων κόμβων. Οι εσωτερικοί (insiders) μπορούν να επιτεθούν στο δίκτυο εξαπατώντας ή παρεμβάλοντας.

Περισσότεροι έξυπνοι μηχανισμοί άμυνας χρειάζονται να παρέχουν λογική προστασία εναντίον wormholes και εσωτερικών υποθέσεων.

5.15.2 Η επίθεση Sybil

Ένας εσωτερικός (insider) δεν μπορεί να εμποδισθεί από την συμμετοχή του στο δίκτυο, αλλά θα μπορούσε να είναι ικανός να το κάνει έτσι ,χρησιμοποιώντας τις ταυτότητες των κόμβων που έχει συμβιβάσει. Οι ταυτότητες πρέπει να επιβεβαιώνονται. Σύμφωνα με την παράδοση, αυτό θα μπορούσε να συμβεί χρησιμοποιώντας δημόσιο κρυπτογραφικό κλειδί, αλλά δημιουργώντας και

επιβεβαιώνοντας ψηφιακές υπογραφές,όμως αυτό είναι υπεράνω των δυνατοτήτων των κόμβων αισθητήρων.

Μια λύση είναι να μοιράζεται ο κάθε κόμβος ένα μοναδικό συμμετρικό κλειδί με μια εμπιστευτική βάση σταθμό. Δυο κόμβοι μπορούν τότε να χρησιμοποιούν ένα Needham-Schroeder πρωτόκολλο για να επιβεβαιώσει κάθε ταυτότητα άλλου και να εγκαταστήσει ένα μοιραζόμενο κλειδί. Ένα ζεύγος γειτονικών κόμβων μπορεί να χρησιμοποιεί το αποτελεσματικό κλειδί για να επιτύχει μια αυθεντική, κωδικοποιημένη ζεύξη ανάμεσά τους. Προκειμένου να εμποδιστεί ένας insider να περιπλανιέται γύρω από ένα ακίνητο δίκτυο και να εγκαθιστά μοιραζόμενα κλειδιά με κάθε κόμβο στο δίκτυο, η βάση σταθμός μπορεί να περιορίσει λογικά τον αριθμό των γειτονικών κόμβων, που ένας κόμβος επιτρέπεται να έχει, και να στέλνει ένα λάθος μήνυμα όταν ο κόμβος τον υπερβαίνει.

Γι' αυτό όταν ένας κόμβος είναι συμβιβασμένος, απαγορεύεται να επικοινωνεί μόνο με τους επιβεβαιωμένους γειτονικούς του. Αυτό δεν είναι μόνο για να πούμε ότι οι κόμβοι απαγορεύονται να στέλνουν μηνύματα στη βάσεις σταθμούς ή να αθροίζουν σημεία πολλαπλών hops μακριά, αλλά ότι απαγορεύονται από την χρησιμοποίηση οποιουδήποτε κόμβου εκτός των επιβεβαιωμένων γειτονικών τους να το κάνουν έτσι. Εξάλλου, ένας εχθρός μπορεί ακόμα να χρησιμοποιήσει ένα wormhole για να δημιουργήσει μια τεχνητή ζεύξη ανάμεσα σε δυο κόμβους για να τους πείσει ότι είναι γειτονικοί, αλλά ο εχθρός δεν θα είναι ικανός να υποκλέψει ή τροποποιήσει οποιεσδήποτε μελλοντικές επικοινωνίες μεταξύ τους.

5.15.3 Επιθέσεις HELLO flood

Η πιο απλή άμυνα εναντίον της επίθεσης HELLO flood είναι να επιβεβαιώσει την τοποθέτηση, σε δυο διαφορετικές κατευθύνσεις, μιας ζεύξης πριν πάρει σημαντική δράση βασισμένη σε ένα ληφθέν μήνυμα πάνω απ' αυτή τη ζεύξη. Παρόλα αυτά, το μέτρο αυτό αντιμετώπισης είναι λιγότερο αποτελεσματικό όταν ένας εχθρός έχει έναν πολύ ευαίσθητο δέκτη, τόσο όσο κι ένας ισχυρός πομπός. Τέτοιος εχθρός μπορεί αποτελεσματικά να δημιουργήσει ένα wormhole σε κάθε έναν κόμβο μέσα στην ευρύτερη περιοχή του πομπού ή του δέκτη του. Αφού οι ζεύξεις μεταξύ αυτών των κόμβων και του εχθρού είναι τοποθετημένες σε διαφορετικές συνθήκες, η παραπάνω προσέγγιση θα είναι απίθανα ικανή να εντοπίσει τοπικά ή να εμποδίσει μια HELLO flood.

Μια πιθανή επίλυση αυτού του προβλήματος είναι ότι κάθε κόμβος πρέπει να αυθεντικοποιεί κάθε έναν από τους γειτονικούς του με ένα πρωτόκολλο επιβεβαίωσης

ταυτότητας. Εάν το πρωτόκολλο στέλνει μηνύματα και στις δυο κατευθύνσεις πάνω από τη ζεύξη μεταξύ των κόμβων, τα HELLO floods εμποδίζονται όταν ο εχθρός έχει μόνον έναν ισχυρό πομπό, γιατί το πρωτόκολλο επιβεβαιώνει την τοποθέτηση ζεύξης σε διαφορετικές κατευθύνσεις. Αν και αυτό δεν εμποδίζει έναν συμβιβασμένο κόμβο με ευαίσθητο δέκτη και ισχυρό πομπό από την αυθεντικοποίηση του σε ένα μεγάλο αριθμό βομβών στο δίκτυο, μια βάση σταθμός – παρατηρητής μπορεί να γίνει ικανή να ανιχνεύσει μια HELLO flood που επίκειται.

5.15.4 Συνδυασμός Wormhole και Sinkhole επιθέσεων

Και οι δυο επιθέσεις είναι πολύ δύσκολο να τις εμποδίσεις, ειδικά όταν και τα δυο χρησιμοποιούνται σε συνδυασμό. Οι Wormholes είναι δύσκολο να ανιχνευθούν γιατί χρησιμοποιούν ένα ιδιωτικό, εκτός μπάντας, κανάλι αόρατο στο ήδη υπάρχον δίκτυο αισθητήρων.

Οι Sinkholes είναι δύσκολο να τις εμποδίσεις σε πρωτόκολλα τα οποία χρησιμοποιούν γνωστοποιημένες πληροφορίες όπως η διατήρηση ενέργειας ή μια υπολογίσιμη αξιοπιστία ενός end-to-end για τη δημιουργία μιας τοπολογίας δρομολόγησης, επειδή η πληροφορία αυτή είναι δύσκολο να επιβεβαιωθεί. Τα δρομολόγια τα οποία μειώνουν το μέτρημα των hop σε μια βάση σταθμό είναι ευκολότερο να επιβεβαιωθούν. Παρόλα αυτά το μέτρημα των hop μπορεί εξολοκλήρου να εξαπατηθούν μέσω ενός wormhole. Όταν τα δρομολόγια εγκαθίστανται βασισμένα απλώς στην αποδοχή ενός πακέτου όπως στο Tinyos ή στην απευθείας διάλυση, τα sinkholes είναι εύκολο να δημιουργηθούν γιατί δεν υπάρχει καμιά πληροφορία επιθέσεων wormhole γιατί αυτή απαιτεί πολύ συγκεκριμένο χρόνο συγχρονισμού και γι’ αυτό είναι ακατόρθωτο για τα περισσότερα δίκτυα αισθητήρων. Επειδή είναι πολύ δύσκολο να τροποποιήσεις τα υπάρχοντα πρωτόκολλα με άμυνες εναντίον τέτοιων επιθέσεων, η καλύτερη λύση είναι να σχεδιαστούν προσεκτικά πρωτόκολλα δρομολόγησης τα οποία αποφεύγουν συνθήκες routing race και κάνουν τις επιθέσεις αυτές λιγότερο σημαντικές.

Για παράδειγμα, μια τάξη πρωτοκόλλων που αντέχουν στις επιθέσεις αυτές είναι τα πρωτόκολλα γεωγραφικής δρομολόγησης. Πρωτόκολλα που κατασκευάζουν μια τοπολογία που ξεκινά από μια βάση σταθμό είναι πιο ευαίσθητα στις wormhole και sinkhole επιθέσεις. Τα γεωγραφικά πρωτόκολλα κατασκευάζουν μια τοπολογία κατόπιν απαιτήσεως χρησιμοποιώντας μόνο τοπικών αντιδράσεων και πληροφοριών και χωρίς ξεκίνημα από τη βάση τοποθεσία μιας βάσης σταθμός,όμως αυτό είναι δύσκολο να το προσελκύσει οπουδήποτε για να δημιουργήσει μια sinkhole.

Ένα wormhole είναι περισσότερο αποτελεσματικό, όταν χρησιμοποιείται για να δημιουργήσει sinkholes ή τεχνητές ζεύξεις που ελκύουν κυκλοφορίες.Οι τεχνητές ζεύξεις είναι εύκολο να ανιχνευθούν στα πρωτόκολλα γεωγραφικής δρομολόγησης, επειδή οι «γειτονικοί» κόμβοι, θα παρατηρήσουν ότι η απόσταση μεταξύ τους είναι καλή πάνω από τη φυσιολογική σειρά πομποδέκτη.

5.15.5 Εκμετάλλευση σφαιρικής γνώσης

Μια σημαντική πρόκληση στην ασφάλεια μεγάλων δικτύων αισθητήρων είναι η συνυπάρχουσα φύση της αυτοοργάνωσης της. Όταν το μέγεθος του δικτύου είναι περιορισμένο ή η τοπολογία είναι καλά δομημένη ή ελεγχόμενη, η σφαιρική γνώση μπορεί να εκμεταλλευτεί μηχανισμούς ασφάλειας. Εάν θεωρηθεί ότι κανείς κόμβος δεν συμβιβάζεται κατά τη διάρκεια της ανάπτυξης, τότε μετά την αρχική τοπολογία που σχηματίζεται, κάθε κόμβος θα μπορούσε να στείλει πληροφορίες όπως τους γειτονικούς κόμβους και την γεωγραφική τοποθεσία (εάν είναι γνωστή) πίσω στη βάση σταθμό. Χρησιμοποιώντας αυτή την πληροφορία οι βάσεις σταθμοί μπορούν να εντοπίσουν την τοπολογία όλου του δικτύου. Για να αναλύσουμε τις αλλαγές τοπολογίας, εξαιτίας παρεμβάσεων ή αποτυχιών κόμβων, οι κόμβοι θα αναβάθμιζαν περιοδικά μια βάση σταθμού- με την κατάλληλη πληροφορία. Δραστικές ή ύποπτες αλλαγές στην τοπολογία, πιθανόν να δηλώνει έναν συμβιβασμό κόμβου και η κατάλληλη πράξη μπορεί να γίνει. Το κύριο πρόβλημα που παραμένει στις επιθέσεις wormhole, sinkhole και Sybil με τη γεωγραφική δρομολόγηση είναι ότι οι τοποθεσίες με γνωστοποιημένες πληροφορίες από γειτονικούς κόμβους πρέπει να τις εμπιστεύονται. Ένας συμβιβασμένος κόμβος γνωστοποιώντας την τοποθεσία του σε μια γραμμή μεταξύ του στοχευμένου κόμβου και μιας βάσης σταθμού θα εγγυηθεί ότι αυτός είναι ο προορισμός για όλα τα προωθημένα πακέτα απ’ αυτόν τον κόμβο.

Η επιλογή βασισμένη στην πιθανότητα ενός επόμενου hop από κάποιους προορισμούς ή πολλών μονοπατιών δρομολόγησης σε πολλαπλές βάσεις σταθμούς μπορεί να βοηθήσει στο πρόβλημα αυτό, αλλά δεν είναι και ό,τι τέλειο. Η επαρκής απαγόρευση της δομής της τοπολογίας μπορεί να εξαλείψει την γνωστοποίηση της τοποθεσίας των κόμβων εάν όλες οι τοποθεσίες είναι καλά γνωστές.

Κάθε κόμβος μπορεί εύκολα να παράγει τις γειτονικές του τοποθεσίες από μόνος του, και οι κόμβοι μπορούν να απευθύνονται στην τοποθεσία παρά στον αναγνωριστή.

5.15.6 Επιλεκτική προώθηση

Ακόμα και στα πρωτόκολλα που αντέχουν εξ' ολοκλήρου σε sinkholes, wormholes και σε Sybil επιθέσεις, ένας συμβιβασμένος κόμβος έχει μια σημαντική πιθανότητα να περιέχει τον εαυτό του σε μια ροή πληροφοριών για να εκτελέσει μια επίθεση,, επιλεκτικής προώθησης, εάν αυτή είναι στρατηγικά τοποθετημένη κοντά στην πηγή ή στη βάση σταθμό.

Μηνύματα που είναι δρομολογημένα πάνω σε μονοπάτια των οποίων οι κόμβοι είναι τελείως εξαρθρωμένοι, προστατεύονται τελείως απέναντι στις επιθέσεις επιλεκτικής προώθησης εμπλέκοντας τους περισσότερους και συμβιβασμένους κόμβους και ακόμη προσφέρουν προστασία βασισμένη στην πιθανότητα όταν πάνω από οι κόμβοι είναι συμβιβασμένοι.

Παρόλα αυτά, τα τελείως εξαρθρωμένα μονοπάτια μπορεί να είναι δύσκολο να δημιουργηθούν. Μπλεγμένα μονοπάτια ίσως έχουν κοινούς κόμβους αλλά δεν έχουν κοινές.ζεύξεις Η χρήση των πολλαπλών μπλεγμένων μονοπατιών μπορεί να παρέχει προστασία βασισμένη στη προώθηση και να χρησιμοποιεί μόνο τοπικές πληροφορίες. Η επίτρεψη στους κόμβους να επιλέξουν δυναμικά το επόμενο hop των πακετών βασισμένα στην πιθανότητα από ένα σετ πιθανών υποψηφίων, μπορεί να μειώσει τις ευκαιρίες ενός εχθρού να αποκτήσει ολικό έλεγχο ροής πληροφοριών.

5.15.7Αυθεντικοποιημένη εκπομπή και ροή

Αφού οι βάσεις σταθμοί είναι αξιόπιστοι, οι εχθροί δεν πρέπει να είναι ικανοί να εξαπατήσουν την εκπομπή ή διαρρεόμενα μηνύματα από οποιαδήποτε βάση σταθμού. Αυτό απαιτεί κάποιο επίπεδο ασυμμετρίας. Αφού κάθε κόμβος στο δίκτυο μπορεί να είναι δυνατόν συμβιβασμένος, κανένας κόμβος δεν θα είναι ικανός να εξαπατήσει μηνύματα από τη βάση σταθμό, κι ακόμη κάθε κόμβος θα είναι ικανός να επιβεβαιώσει αυτούς. Η αυθεντική εκπομπή είναι επίσης χρήσιμη για τοπικές αντεπιδράσεις κόμβων. Πολλά πρωτόκολλα απαιτούν κόμβους για να εκπέμψουν μηνύματα HELLO στα γειτονικά τους. Αυτά τα μηνύματα θα μπορούσαν να είναι αυθεντικά και αδύνατον να εξαπατηθούν.

Προτάσεις για αυθεντικές εκπομπές προτίθενται για χρήση σε ένα περισσότερο συνήθες setting είτε χρήσης ψηφιακών υπογραφών και/ή να έχουν πακέτα επικεφαλίδας τα οποία να μεγαλώνουν το μήκος χαρακτηριστικών πακέτων δικτύων αισθητήρων.

Το μTesla είναι ένα πρωτόκολλο με αποτελεσματική αυθεντική εκπομπή και ροή, το οποίο χρησιμοποιεί μόνο συμμετρικό κλειδί κρυτογραφίας και απαιτεί ελάχιστο πακέτο επικεφαλίδας. Το μTesla πετυχαίνει την ασυμμετρία να είναι απαραίτητη για αυθεντική εκπομπή (γνήσια) και ροή χρησιμοποιώντας κλειδί που καθυστερεί για την αποκάλυψη μιας οδού αλυσίδας κλειδιών κατασκευασμένη με ένα μίγμα λειτουργιών για υπολογίσιμη κρυπτογραφική ασφάλεια. Το ξαναπαίξιμο (replay) εμποδίζεται γιατί τα αυθεντικά μηνύματα με προηγούμενα αποκαλυπτικά κλειδιά αγνοούνται. Το μTesla επίσης απαιτεί χαμένο χρόνο συγχρονισμού.

Η ροή μπορεί να είναι μια σημαντική σημασία για μια διασπορά πληροφοριών σε εχθρικό περιβάλλον, επειδή αυτή απαιτεί το σέτ των συμβιβασμένων κόμβων να δημιουργήσουν μια κορυφή (vertex cut) στην επικείμενη τοπολογία για να εμποδίσουν ένα μήνυμα από την προσέγγιση κάθε κόμβου στο δίκτυο. Οι κάτω πλευρές (downsides) της ροής περιλαμβάνουν πολλά μηνύματα και αντιστοιχίες σε κόστη ενέργειας, τόσο όσο και οι ικανές απώλειες που δημιουργούνται από συγκρούσεις. Οι αλγόριθμοι SPIN και οι gossiping είναι τεχνικές για να μειώνουν τα κόστη των μηνυμάτων και των συγκρούσεων, οι οποίες επιτυγχάνουν ακόμη, εύρωστες διασπορές μηνυμάτων, βασισμένα στη πιθανότητα, σε κάθε κόμβο στο δίκτυο.

5.16 Περίληψη μέτρων αντιμετώπισης

I. Η κωδικοποίηση ζεύξης-στρώματος και η αυθεντικότητα, η δρομολόγηση πολλαπλών μονοπατιών, η επιβεβαίωση ταυτοτήτων, η επιβεβαίωση ζεύξης που λαμβάνει μέρος σε δυο αντίθετες κατευθύνσεις και η αυθεντική εκπομπή μπορούν να προστατεύσουν πρωτόκολλα δρομολόγησης δικτύων αισθητήρων από εισβολείς, και ψεύτικες πληροφορίες δρομολόγησης.

II. Οι επιθέσεις SYBIL, HELLO ροές, και εξαπάτηση αναγνώρισης κατορθώνουν να αυξήσουν τα υπάρχοντα πρωτόκολλα μ' αυτούς τους μηχανισμούς.

III. Οι επιθέσεις Sinkhole και wormholes θέτουν σημαντικές προκλήσεις να ασφαλίσουν τον σχεδιασμό πρωτοκόλλων δρομολόγησης και είναι απίθανο να υπάρχουν αποτελεσματικά μέτρα αντιμετώπισης αυτών των επιθέσεων, τα οποία μπορούν να εφαρμοστούν μετά την ολοκλήρωση του σχεδιασμού του πρωτοκόλλου. Είναι σημαντικό να σχεδιάζονται πρωτόκολλα δρομολόγησης στα οποία οι επιθέσεις αυτές δεν έχουν αποτέλεσμα και δεν είναι σημαντικές.Τα πρωτόκολλα με γεωγραφική δρομολόγηση είναι μια τάξη πρωτοκόλλων που υπόσχεται πολλά.

5.17 Δρομολόγηση με πολλαπλές επανεκπομπές (multihop routing)

Ένας τελικός περιορισμός δημιουργίας μιας τοπολογίας δρομολόγησης με πολλαπλά hop γύρω από ένα καθορισμένο set από βάσεις σταθμούς είναι ότι αυτοί οι κόμβοι, μέσα σε ένα ή δυο hops της βάσης σταθμού, είναι ιδιαιτέρως ελκυστικοί για συμβιβασμό.

Μετά από έναν σημαντικό αριθμό κόμβων που έχουν συμβιβαστεί, όλα χάνονται.

Μια άλλη επιλογή είναι να έχει ένα τυχαίο rotating σετ «κατ' ουσίαν» βάσεων σταθμών για να δημιουργήσει μια επικάλυψη δικτύου. Αφού επιλεχθεί το σετ των κατ' ουσίαν βάσεων σταθμών, μια τοπολογία πολλαπλών hop (multihop) κατασκευάζεται χρησιμοποιώντας τα. Οι κατ' ουσίαν βάσεις σταθμοί, έπειτα επικοινωνούν κατευθείαν με τις αληθινές βάσεις σταθμών.

5.18 Συμπεράσματα

Η ασφαλής δρομολόγηση (routing) είναι απαραίτητη για την αποδοχή και χρήση των δικτύων αισθητήρων για πολλές εφαρμογές, αλλά εξηγήσαμε ότι τα τωρινά προτεινόμενα πρωτόκολλα δρομολόγησης ,για αυτά τα δίκτυα, είναι ανασφαλή. Το αφήνουμε σαν ένα ανοιχτό πρόβλημα για να σχεδιαστεί ένα πρωτόκολλο δρομολόγησης δικτύου αισθητήρων το οποίο να ικανοποιεί τους προτεινόμενους στόχους ασφαλείας. Η κωδικοποίηση ζεύξης στρώματος και οι μηχανισμοί αυθεντικότητας μπορεί να είναι μια πρώτη λογική προσέγγιση για άμυνα από mote-class insiders, άλλα η κρυπτογράφηση, από μόνη της, δεν είναι αρκετή. Η πιθανή παρουσία εχθρών με lap-top, insiders και η περιορισμένη συσχέτιση μηχανισμών ασφαλείας end-to-end απαιτούν προσεκτικό σχεδιασμό πρωτοκόλλων.

ΚΕΦΑΛΑΙΟ 6ο

ΥΠΑΡΧΟΝΤΑ ΠΡΩΤΟΚΟΛΛΑ

6.1ΠΡΩΤΟΚΟΛΛΟ SPINS

Το πρωτόκολλο SPINS θα το εξετάσουμε ως τα σημαντικότερα σημεία:

α) Για την ασφάλεια

β) Σχεδιασμός και ανάπτυξης του μTesla

γ) Σχεδιασμός και ανάπτυξης του SNEP

δ) Σχεδιασμός και ανάπτυξη αυθεντικού πρωτοκόλλου

6.2Αρχιτεκτονική δομή

Γενικά, οι κόμβοι των αισθητήρων επικοινωνούν με ασύρματο δίκτυο. Αυτό από την μια επηρεάζει την αξιοπιστία του συστήματος και από την άλλη ελαττώνει τη χρήση ενέργειας.

Ένα τυπικό Smart Dust δίκτυο αισθητήρων δημιουργείται γύρω από ένα ή περισσότερους σταθμούς βάσης το οποίο μεταδίδει το δίκτυο αισθητήρων στο εξωτερικό δίκτυο. Οι κόμβοι αισθητήρων δημιουργούν διαδρομές εκπομπής όπου κάθε μια έχει μια βάση. Κάθε κόμβος μπορεί να μεταδώσει μήνυμα σε μια βάση αναγνωρίζει πακέτα κατευθυνόμενα σ' αυτό και χειρίζεται εκπομπές μηνυμάτων. Η βάση λαμβάνεται κάθε έναν κόμβο χρησιμοποιώντας καθοδήγηση από την πηγή. Υποθέτουμε ότι η βάση έχει δυνατότητες παρόμοιες με το δίκτυο των κόμβων εκτός του ότι έχει επαρκή δύναμη να παρατείνει τη ζωή όλων κόμβων των αισθητήρων, επαρκή μνήμη να αποθηκεύσει κρυπτογραφικές έννοιες και μέσα για επικοινωνία με εξωτερικές. Με τα δίκτυα αισθητήρων υπάρχει πλεόνασμα γιατί το μεγαλύτερο μέρος επικοινωνιακών συσχετίζεται με τη βάση και όχι μεταξύ δυο τοπικών κόμβων. Τα συστήματα επικοινωνίας μεταξύ αυτού του δικτύου χωρίζονται σε τρεις κατηγορίες:

- Από κόμβο στη βάση επικοινωνίας ,π.χ. ανάγνωση αισθητήρων.
- Από βάση στον κόμβο επικοινωνίας, π.χ. συγκεκριμένα αιτήματα.
- Από τη βάση σε όλους τους κόμβους, π.χ. επαναπρογραμματισμός όλου του δικτύου.

6.2.1 Απαιτήσεις αξιοπιστίας

Το δίκτυο αισθητήρων μπορεί να βρίσκεται σε αναξιόπιστες τοποθεσίες. Παράλληλα είναι πιθανόν να εγγυάται την αξιοπιστία του κάθε κόμβου μέσω μικροελεγκτών ασφαλείας. Αυτή η αρχιτεκτονική δεν ακολουθείται στην πλειονότητα των δικτύων αισθητήρων. Αντιθέτως, υποθέτουμε ότι οι αισθητήρες από μόνοι τους είναι αναξιόπιστοι. Η βασική ασύρματη επικοινωνία δεν είναι ασφαλής. Κι αυτό διότι μπορεί ανά πάσα στιγμή μπορεί να γίνει κλοπή μηνυμάτων και αρχείων.

Ο στόχος είναι να σχεδιαστεί το SPINS πρωτόκολλο έτσι ώστε ο ένας κόμβος να μην εκπέμπει στους άλλους κόμβους.

6.2.2 Εμπιστευτικότητα πληροφορίας

Ένα δίκτυο αισθητήρων δεν πρέπει να διαρρέει ανάλυση αισθητήρων σε γειτονικά δίκτυα. Σε πολλές εφαρμογές οι κόμβοι μεταδίδουν πληροφορίες.υψηλής ευαισθησίας Η κοινή τακτική για να κρατιούνται τέτοιου είδους πληροφορίες μυστικές είναι να κωδικοποιούν την πληροφορία με μυστικό κλειδί που μόνο οι αποδέκτες γνωρίζουν, οπότε επιτυγχάνεται και η εμπιστευτικότητα. Ακολουθώντας αυτόν τον τρόπο επικοινωνίας δημιουργούνται ασφαλή κανάλια μεταξύ κόμβων και βάσεων.

6.2.3 Αυθεντικότητα πληροφορίας

Η γνησιότητα των μηνυμάτων είναι σημαντική για πολλές εφαρμογές στα δίκτυα αισθητήρων. Η γνησιότητα πληροφορίας επιτρέπει στον δέκτη να επιβεβαιώσει ότι η πληροφορία είναι σταλμένη από αυτόν που ισχυρίζεται ότι την έστειλε.

Στην επικοινωνία μεταξύ δυο μελών η γνησιότητα πληροφορίας μπορεί να επιτυχθεί με έναν καθαρά συμμετρικό μηχανισμό: Ο αποστολέας και ο δέκτης μοιράζονται ένα μυστικό κλειδί να δημιουργήσουν ένα κωδικό γνησιότητας μηνύματος (MAC) για όλες τις πληροφορίες. Όταν ένα μήνυμα με το σωστό MAC φτάσει, ο δέκτης ξέρει ότι στάλθηκε από το σωστό αποστολέα. Αν ένας αποστολέας θέλει να στείλει γνήσια πληροφορία σε μη αξιόπιστους δέκτες, χρησιμοποιώντας ένα συμμετρικό MAC είναι μη ασφαλές. Γιατί κάθε ένας από τους δέκτες γνωρίζουν το κλειδί MAC και άρα μπορούν να χρησιμοποιούν την ταυτότητα αποστολέα και να πλαστογραφούν μηνύματα προς άλλους δέκτες.

6.2.4 Αξιοπιστία πληροφορίας

Στην επικοινωνία η αξιοπιστία πληροφορίας εξασφαλίζει στον δέκτη ότι η πληροφορία ,που δέχτηκε, δεν έχει παραβιαστεί κατά τη διάρκεια της μεταφοράς από

κάποιον «εχθρό». Στο SPINS, επιτυγχάνεται η αξιοπιστία της πληροφορίας μέσω της γνησιότητας αυτής.

6.3Μέρη ασφαλείας SPINS

Υπάρχουν δυο μέρη τα οποία συντελούν στην ασφάλεια του SPINS. Το πρώτο είναι το SNEP και το δεύτερο το μTesla. Το SNEP παρέχει εμπιστευτικότητα πληροφορίας, την γνησιότητα πληροφορίας δυο μελών, αξιόπιστα και την επικαιρότητα. Το μTesla παρέχει γνησιότητα για την εκπομπή πληροφορίας. Η ασφάλεια για τους δυο μηχανισμούς υποστηρίζεται από ένα μυστικό κλειδί μεταξύ των κόμβων και της βάσης.

6.4 SNEP

6.4.1Εμπιστευτικότητα, γνησιότητα, αξιοπιστία και επικαιρότητα πληροφοριών.

Το SNEP παρέχει έναν αριθμό ξεχωριστών πλεονεκτημάτων.

Πρώτον, έχει χαμηλή επιβάρυνση στην επικοινωνία. Προσθέτει μόνο 8 bytes ανά μήνυμα.

Δεύτερον, όπως πολλά κρυπτογραφικά πρωτόκολλα, χρησιμοποιεί έναν μετρητή, αλλά αποφεύγεται η μετάδοση της αξίας μετρητή διατηρώντας θέση στα τελικά σημεία.

Τρίτον, το SNEP επιτυγχάνει σημασιολογική ασφάλεια η οποία αποτρέπει έναν εισβολέα να δει το περιεχόμενο μηνύματος.

Τέλος, αυτό το επαρκές και απλό πρωτόκολλο μας δίνει επίσης γνησιότητα πληροφορίας, ασφάλεια για απάντηση. Η εμπιστευτικότητα πληροφοριών είναι μια από τις πολλές βασικές αρχές ασφάλειας που χρησιμοποιείται σε κάθε πρωτόκολλο και μπορεί να επιτευχθεί μέσω κωδικοποίησης, αλλά αυτή δεν είναι επαρκής. Άλλη μια σημαντική πηγή ασφαλείας είναι η σημασιολογική ασφάλεια, η οποία εξασφαλίζει ότι κάποιος εισβολέας δεν έχει πληροφορίες για το τρέχον κείμενο ακόμα κι αν δει πολλές κωδικοποιήσεις του ίδιου κειμένου. Π.χ. ακόμα κι αν ένας εισβολέας έχει μια κωδικοποίηση του 0 bit και άλλη μια του 1 bit δεν θα καταφέρει να διαχωρίσει είτε η καινούργια κωδικοποίηση είναι του 0 bit ή του 1 bit. Μια βασική τεχνική για την επίτευξη του είναι η σπανιότητα. Πριν κωδικοποιηθεί το μήνυμα με μια αλυσιδωτή κωδικοποίηση (π.χ. DES-CBC) ο αποστολέας προβλέπει το μήνυμα με τυχαία σειρά bit. Αυτό αποτρέπει τον εισβολέα από το να καταλάβει το κείμενο με τα κωδικοποιημένα μηνύματα.

Στέλνοντας την τυχαία πληροφορία μέσω ενός ασυρμάτου καναλιού απαιτείται περισσότερη ενέργεια. Δημιουργείται λοιπόν άλλος ένας κρυπτογραφικός

μηχανισμός που εξασφαλίζει την σημασιολογική ασφάλεια χωρίς επιπλέον επιβάρυνση για την μετάδοση. Χρησιμοποιούνται δυο μετρητές οι οποίοι μοιράζονται (ένας για κάθε μια κατεύθυνση επικοινωνίας) για το κομμάτι της αποκρυπτογράφησης.

Ένας κλασικός τρόπος διαχείρισης μετρητών είναι να στείλεις την μέτρηση μαζί με κάθε μήνυμα. Αλλά αφού χρησιμοποιούμε αισθητήρες οι οποίοι έχουν κοινό μετρητή και κοινές αυξήσεις, ο αποστολέας σώζει ενέργεια αφού δεν στέλνει το μετρητή με το μήνυμα.

Μια καλή εφαρμογή σχεδιασμού ασφαλείας δεν είναι να ξαναχρησιμοποιηθεί το ίδιο κρυπτογραφικό κλειδί για διαφορετικές κρυπτογραφικές έννοιες. Αυτό αποτρέπει οποιαδήποτε συνήθη αλληλεπίδραση μεταξύ αρχικών τα οποία μπορεί να εισάγουν μια αδυναμία.

Τα δυο μέρη επικοινωνίας A και B μοιράζονται ένα κύριο μυστικό κλειδί XAB και παράγουν ανεξάρτητα κλειδιά χρησιμοποιώντας μια τυχαία ψεύτικη λειτουργία F: κωδικοποιημένα κλειδιά $K_{AB} = F_x$ και $K_{BA} = F_x$ για κάθε κατεύθυνση επικοινωνίας και κλειδιά MAC $K'_{AB} = F_x$ και $K'_{BA} = F_x$ για κάθε κατεύθυνση επικοινωνίας.

Ο συνδυασμός αυτών των μηχανισμών σχηματίζει το SNEP πρωτόκολλο. Η κωδικοποιημένη πληροφορία έχει την ακόλουθη μορφή $E = \{D\}_{(KC)}$ όπου D είναι η πληροφορία, το κωδικοποιημένο κλειδί είναι το K και ο μετρητής το C. Το MAC είναι $M = MAC(K', C \mid E)$ Το ολοκληρωμένο μήνυμα που στέλνει το A στο B είναι

A → B: $\{D\}_{(K_{AB}, C_A)}, MAC(K'_{AB} C_A \mid \{D\}_{(k_{AB}, C_A)})$(1)

Το SNEP προσφέρει τις επόμενες ιδιότητες

6.4.2 Σημασιολογική ασφάλεια

Η αξία του μετρητή είναι αρκετά μεγάλη ώστε να μην επαναληφθεί κατά τη διάρκεια ζωής του κόμβου.

6.4.3 Γνησιότητα πληροφορίας

Αν το MAC επιβεβαιώσει σωστά, ο δέκτης ξέρει ότι το μήνυμα δημιουργήθηκε από το αναφερόμενο αποστολέα.

6.4.4 Προστασία απάντησης

Η αξία του μετρητή στο MAC αποτρέπει την απάντηση σε παλιά μηνύματα. Με την ύπαρξη του μετρητή στο MAC ένας εισβολέας δεν μπορεί εύκολα να απαντήσει σε μηνύματα.

6.4.5 Αδύναμη ανανέωση (Weak freshness)

Αν το μήνυμα επιβεβαιώσει σωστά ο δέκτης ξέρει ότι το μήνυμα πρέπει να έχει σταλεί μετά το προηγούμενο μήνυμα που έλαβε επιτυχές.

6.4.6 Χαμηλή επικοινωνιακή επιβάρυνση

Η μέτρηση βρίσκεται σε κάθε τελικό σημείο και δεν χρειάζεται να στέλνεται σε κάθε μήνυμα. Ένα απλό SNP παρέχει αδυναμία στη φρεσκάδα πληροφοριών γιατί αναγκάζει να υπάρχει σειρά στα μηνύματα που στάλθηκαν στον κόμβο B, αλλά καμία απόλυτη επιβεβαίωση στον κόμβο A ότι ένα μήνυμα δημιουργήθηκε από το B σε απάντηση ενός συμβάντος στον κόμβο A. Ο κόμβος A επιτυγχάνει φρεσκάδα πληροφοριών για απάντηση από τον κόμβο B μέσω του NA. Ο κόμβος A ανιχνεύει τυχαία τον NA και τον στέλνει με μήνυμα αίτησης RA στον κόμβο B.

Ο πιο απλός τρόπος για την επίτευξη της φρεσκάδας πληροφοριών είναι για τον κόμβο B να επιστρέψει τον NA με μήνυμα απάντησης RB σε ένα αυθεντικό πρωτόκολλο. Παρόλα αυτά, αντί της επιστροφής του NA στον αποστολέα μπορούμε να τελειοποιήσουμε την διαδικασία χρησιμοποιώντας το nonce χωρίς αμφιβολία στον υπολογισμό MAC. Η φρεσκάδα πληροφοριών που παρέχει το πρωτόκολλο SNEP για την απάντηση του κόμβου B είναι:

A → B: NA, RA

B → A:

$$\{R_{R_B}\}_{(K_{BA,}C_B),} MAC\left(K'_{BA}, N_A \,||\, C_B \,||\, \{R_B\}_{(K_{BA,}C_B)}\right)$$

Αν το MAC επιβεβαιώσει σωστά, ο κόμβος A γνωρίζει ότι ο κόμβος B δημιούργησε την απάντηση αφότου στάλθηκε το αίτημα. Το πρώτο μήνυμα μπορεί επίσης να χρησιμοποιήσει το απλό SNEP εάν η εμπιστευτικότητα και η αυθεντικότητα χρειάζονται.

6.4.7 Πρωτόκολλο απαλλαγής μετρητή (counter)

Για την επίτευξη μικρών SNEP μηνυμάτων, υποθέτουμε ότι τα μέρη Α και Β γνωρίζουν τις αξίες μετρητών τους CA και CB και έτσι ο μετρητής δεν χρειάζεται να προστεθεί σε κάθε κρυπτογραφημένο μήνυμα. Παρόλα αυτά, πρακτικά μπορεί να χαθούν μηνύματα και η κατάσταση του μετρητή μπορεί να γίνει inconsistent. Εδώ παρουσιάζονται πρωτόκολλα που συγχρονίζουν την κατάσταση του μετρητή. Για να βοηθήσουμε τις αξίες αρχικά του μετρητή χρησιμοποιούμε το παρακάτω πρωτόκολλο.

A → B: CA

B → A: $C_{B,}MAC\left(K'_{(BA)}\, C_A \middle|\middle| C_b\right)$

A → B: $MAC\left(K'_{AB,}\, C_A \middle|\middle| C_B\right)$

Δεν χρειάζεται κρυπτογράφηση διότι οι αξίες του μετρητή δεν είναι μυστικές. Παρόλα αυτά, αυτό το πρωτόκολλο χρειάζεται φρεσκάδα γι' αυτό και τα δυο μέρη Α, Β (κόμβοι) χρησιμοποιούν τους μετρητές τους σαν **nonce** (υποθέτοντας ότι το πρωτόκολλο ποτέ δεν τρέχει δυο φορές με τις ίδιες αξίες μετρητή). Επίσης, σημειώνεται ότι το MAC δεν χρειάζεται να συμπεριλάβει τα ονόματα των Α ή Β, αφού τα κλειδιά MAC K'_{AB} και K'_{BA} αναμφίβολα ασφαλίζουν τα μηνύματα στα μέρη και εξασφαλίζουν την κατεύθυνση των μηνυμάτων.

Αν το μέρος Α συνειδητοποιήσει ότι ο μετρητής CB του Β δεν είναι συγχρονισμένος πια, το Α μπορεί να ζητήσει να εξασφαλίσει τη φρεσκάδα της απάντησης.

A → B: N_A

B → A: $C_{B,}MAC\left(K'_{BA}, N_A \middle|\middle| C_B\right)$

Για να αποτραπεί μια ικανή άρνηση εξυπηρέτησης μιας επίθεσης (DOS), όπου ένας εισβολέας στέλνει συνεχώς πλαστά μηνύματα για να εξαναγκάσει τους κόμβους να ολοκληρώσουν τον συγχρονισμό του μετρητή, οι κόμβοι μπορούν να αλλάξουν την αποστολή του μετρητή με κάθε ένα κωδικοποιημένο μήνυμα που στέλνουν. Μια άλλη προσέγγιση για την ανακάλυψη τέτοιας DOS επίθεσης είναι να συνάψεις ένα άλλο μικρό MAC στα μηνύματα τα οποία δεν εξαρτώνται από τον μετρητή.

6.5 μTesla: Αυθεντική εκπομπή

Προηγούμενες προτάσεις για αυθεντικότητα εκπομπής είναι μη πρακτικές για δίκτυα αισθητήρων. Οι περισσότερες προτάσεις βασίζονται σε ασύμμετρες ψηφιακές υπογραφές για αυθεντικότητα, οι οποίες είναι μη πρακτικές για πολλούς λόγους.

Το προσφάτως προτεινόμενο TESLA πρωτόκολλο παρέχει παραγωγική αυθεντικότητα εκπομπής. Παρόλα αυτά το TESLA δεν σχεδιάστηκε για τα περιορισμένα υπολογιστικά περιβάλλοντα που αριθμούνται στα δίκτυα αισθητήρων, για τους ακόλουθους τρεις λόγους:

Το πρωτόκολλο TESLA αυθεντικοποιεί το αρχικό πακέτο με μια ψηφιακή υπογραφή. Οι ψηφιακές υπογραφές, πράγματι, είναι πολύ ακριβές για να υπολογίσουν τους κόμβους αισθητήρων, από τότε που η σύνδεση κωδικών μέσα σε μνήμη είναι μια πρόκληση. Για τον ίδιο λόγο που αναφέραμε και παραπάνω, η υπογραφή μιας φοράς είναι μια πρόκληση να χρησιμοποιηθούν στους κόμβους.

Το TESLA έχει μια επικεφαλίδα με 24bytes ανά πακέτο. Για τα συνδεόμενα δίκτυα σταθμών εργασίας δεν έχει συνήθως καμία έννοια. Παρόλα αυτά, οι κόμβοι αισθητήρων στέλνουν πολύ μικρά μηνύματα τα οποία είναι γύρω στα 30 bytes. Είναι μη πρακτικό να εκθέσεις το κλειδί TESLA για τα προηγούμενα κενά με το κάθε πακέτο: με 64 bit κλειδιά και το MAC, το μέρος του πακέτου που συνδέεται με το TESLA μπορεί να αποτελέσει άνω το 50% του πακέτου.

Τελικά, το κλειδί αλυσίδας μιας διαδρομής δεν ταιριάζει μέσα στη μνήμη των κόμβων αισθητήρων. Έτσι, το φτωχό TESLA δεν είναι πρακτικό για έναν κόμβο να εκπέμπει αυθεντική πληροφορία.

Έτσι σχεδιάστηκε το TESLA πρωτόκολλο για να λυθούν οι παρακάτω ανεπάρκειες του TESLA στα δίκτυα αισθητήρων.

- Το TESLA αυθεντικοποιεί το αρχικό πακέτο με μια ψηφιακή υπογραφή, η οποία είναι πολύ ακρική για τους κόμβους αισθητήρων. Το μTESLA χρησιμοποιεί μόνο συμμετρικούς μηχανισμούς.
- Η γνωστοποίηση κλειδιού σε κάθε πακέτο απαιτεί πολύ ενέργεια για αποστολή και παραλαβή. Το μTESLA γνωστοποιεί το κλειδί μια φορά ανά γεγονός (perepoch).
- Είναι ακριβή η αποθήκευση του κλειδιού αλυσίδας μιας διαδρομής σε ένας κόμβο αισθητήρα. Το μTESLA περιορίζει τον αριθμό των αυθεντικοποιημένων αποστολέων.

Μια αυθεντικοποιημένη εκπομπή απαιτεί ένα ασύμμετρο μηχανισμό, ειδάλλως οποιοσδήποτε παραλήπτης θα μπορούσε να πλαστογραφεί μηνύματα από τον αποστολέα. Δυστυχώς, ασύμμετροι κρυπτογραφικοί μηχανισμοί έχουν υψηλό υπολογισμό, επικοινωνία και καταχώρηση επικεφαλίδας, κάνοντας έτσι την χρήση των διαδικασιών περιορισμένης πηγής μη πρακτική. Το μTESLA ξεπερνά αυτό το πρόβλημα με την εισαγωγή ασυμμετρίας μέσω καθυστερημένης γνωστοποίησης συμμετρικών κλειδιών, η οποία έχει σαν αποτέλεσμα την παραγωγική αυθεντικότητα εκπομπής.

Το μTESLA πρωτόκολλο απαιτεί ότι η βάση σταθμός και οι κόμβοι είναι σε λάθος χρόνο συγχρονισμένοι, και κάθε κόμβος γνωρίζει ένα άνω σημείο του μεγίστου συγχρονισμένου λάθους.

Για την αποστολή ενός αυθεντικού πακέτου, η βάση σταθμός υπολογίζει ένα MAC στο πακέτο με ένα κλειδί το οποίο είναι μυστικό την συγκεκριμένη στιγμή. Όταν ο κόμβος λάβει το πακέτο μπορεί να επιβεβαιώσει ότι το συμφωνημένο κλειδί MAC δεν ήταν ακόμη γνωστοποιημένο από τη βάση σταθμό (βασισμένο στο λάθος συγχρονισμένο ρολόι, στο μέγιστο λάθος συγχρονισμένου και στον προγραμματισμένο χρόνο στον οποίο τα κλειδιά γνωστοποιούνται).

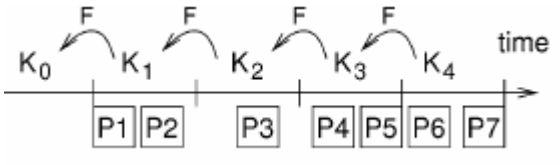
Αφού ο παραλαμβάνων κόμβος διαβεβαιώνει ότι το κλειδί MAC είναι γνωστό ότι μόνο από τη βάση σταθμό, ο παραλαμβάνων κόμβος διαβεβαιώνει ότι κανένας εχθρός δεν μπορεί να κάνει αλλάξει το πακέτο κατά τη μεταφορά. Ο κόμβος αποθηκεύει το πακέτο σε buffer. Τη στιγμή της γνωστοποίησης του κλειδιού, η βάση σταθμός εκπέμπει το κλειδί επιβεβαίωσης σε όλους τους δέκτες. Όταν ο κόμβος παραλάβει το κλειδί γνωστοποίησης, μπορεί να επιβεβαιώσει την γνησιότητα του κλειδιού. Αν το κλειδί είναι σωστό ο κόμβος μπορεί να το χρησιμοποιήσει για να αυθεντικοποιήσει το ήδη αποθηκευμένο πακέτο στο buffer.

Κάθε κλειδί MAC είναι ένα κλειδί από μια αλυσίδα κλειδιών που έχουν δημιουργηθεί από μια κοινή λειτουργία μιας διαδρομής F. Για να δημιουργηθεί το κλειδί αλυσίδας μιας διαδρομής, ο αποστολέας επιλέγει τυχαία το τελευταίο κλειδί Kn από την αλυσίδα, και συνεχώς χρησιμοποιεί το F για να υπολογίσει όλα τα άλλα κλειδιά: Ki = F (Ki+1). Κάθε κόμβος μπορεί εύκολα να διεκπεραιώσει τον χρόνο συγχρονισμού και να ανακτήσει ένα αυθεντικό κλειδί από την αλυσίδα σε ένα ασφαλές και αυθεντικό τρόπο, χρησιμοποιώντας το SNEP building block.

6.5.1 Λεπτομερής περιγραφή μTESLA

Το μTESLA έχει πολλές φάσεις: Εγκατάσταση αποστολέα, απεσταλμένα αυθεντικοποιημένα πακέτα, νέοι βοηθητικοί παραλήπτες, και πακέτα αυθεντικά. Θα εξηγήσουμε πρώτα πως το μTESLA επιτρέπει στην βάση σταθμό να εκπέμπει αυθεντικές πληροφορίες στους κόμβους και μετά πως το TESLA επιτρέπει τους κόμβους να εκπέμπουν αυθεντικοποιημένα μηνύματα.

Στο παρακάτω σχήμα φαίνεται η μονόδρομη αλυσίδα κλειδιών μTESLA



Σχήμα 6.1. Ο αποστολέας δημιουργεί την μονόδρομη αλυσίδα κλειδιών από δεξιά προς αριστερά με την επαναλαμβανόμενη αποδοχή της μονόδρομης λειτουργίας F.Ο αποστολέας συνδέει κάθε κλειδί της μονόδρομης αλυσίδας με ένα χρονικό κενό. Ο χρόνος κυλαει από αριστερά προς τα δεξιά ετσι ο αποστολέαςχρησιμοποιεί τα κλειδιά της αλυσίδας κλειδιών σε αντίθετη φορά και υπολογίζει το MAC των πακέτων σε ένα χρονικό κενό με το κλειδί αυτού του χρονικού κενού. **(12)**

6.5.2 Εγκατάσταση αποστολέα.

Ο αποστολέας πρώτα δημιουργεί μια σειρά από μυστικά κλειδιά (κλειδί μιας διαδρομής αλυσίδας). Για τη δημιουργία ενός κλειδιού αλυσίδας μιας διαδρομής μήκους n, ο αποστολέας επιλέγει τυχαία το τελευταίο κλειδί Kn, και δημιουργεί τις σταθερές αξίες με την επιτυχημένη χρησιμοποίηση λειτουργίας μιας διαδρομής F.

Kj = F (Kj + 1). Επειδή το F είναι μιας διαδρομής λειτουργίας, οποιοσδήποτε μπορεί να υπολογίσει π.χ. Ko, ….Kj δεδομένου του Kj+1. Σε άλλη περίπτωση, κανένας δεν μπορεί να υπολογίσει το ανάποδο, π.χ. να υπολογίζει τα Kj + 1 με δεδομένα μόνο Ko, ……Kj, επειδή η λειτουργία παραγωγής είναι μιας διαδρομής. Το S/κλειδί κωδικού ενός χρόνου συστήματος χρησιμοποιεί μια απλή προσέγγιση.

6.5.3 Εκπεμπόμενα αυθεντικά πακέτα.

Ο χρόνος διαιρείται σε κενά χρόνου και ο αποστολέας συσχετίζει κάθε κλειδί από την αλυσίδα κλειδιών μιας διαδρομής με ένα χρονικό κενό. Στο χρονικό κενό i, ο αποστολέας χρησιμοποιεί το κλειδί από το τρέχον κενό, Ki, για να υπολογίσει τον κώδικα αυθεντικότητας μηνύματος (MAC) των πακέτων στο κενό αυτό. Στο χρονικό κενό (its), ο αποστολέας αποκαλύπτει το κλειδί Ki. Η γνωστοποίηση του καθυστερημένου χρόνου του κλειδιού εξαρτάται από τα μερικά χρονικά κενά, τόσο

όσο πιο μεγάλα είναι από οποιοδήποτε χρονικό όριο απόσταση μεταξύ του αποστολέα και των παραληπτών.

6.5.4 Διαδικάσία αρχικοποίησης νέου δέκτη.

Σε μια αλυσίδα κλειδιών μιας διαδρομής, τα κλειδιά αυτό-αυθεντικοποιούνται. Ο δέκτης μπορεί εύκολα και επιτυχώς να αυθεντικοποιήσει αντικατεστημένα κλειδιά από αυτήν την αλυσίδα χρησιμοποιώντας ένα αυθεντικό κλειδί. Π.χ., εάν ένας δέκτης έχει μια αυθεντικοποιημένη αξία Ki από την αλυσίδα κλειδιών, μπορεί εύκολα να αυθεντικοποιήσει Ki+1, επιβεβαιώνοντας Ki = F (Ki+1). Για να αρχικοποιηθεί το μTESLA, κάθε δέκτης χρειάζεται να έχει αυθεντικό κλειδί από την αλυσίδα μιας διαδρομής σαν δέσμευση σε όλη την αλυσίδα. Άλλες απαιτήσεις είναι ότι ο αποστολέας και ο δέκτης πρέπει να είναι συγχρονισμένοι σε λάθος χρόνο και το δεσμευμένο αυθεντικοποιημένο κλειδί της αλυσίδας πρέπει να έχει μηχανισμό που να παρέχει φρεσκάδα και αυθεντικότητα σημείο με σημείο. Ο δέκτης R στέλνει ένα υπάρχον NR στο ζητούμενο μήνυμα του αποστολέα S. Ο αποστολέας S απαντάει με ένα μήνυμα συμπεριλαμβανομένου της χρονικής στιγμής του Ts, ένα κλειδί Ki από την αλυσίδα της μιας διαδρομής χρησιμοποιούμενο στο προηγούμενο κενό i (η δέσμευση στην αλυσίδα), ο χρόνος εκκίνησης Ti του κενού i, η διάρκεια Tint του χρόνου του κενού, και την καθυστέρηση γνωστοποίησης δ (οι τελευταίες τρεις αξίες περιγράφουν το πρόγραμμα γνωστοποίησης κλειδιού):

$\mathrm{M} \rightarrow \mathrm{S}: \; N_M$

$$\mathrm{S} \rightarrow \mathrm{M}: \begin{array}{l} T_S \left| K_i \right| T_i \left| T_{\mathrm{int}} \right| \delta \\ MAC\left(K_{MS}, N_M, \left| T_S \right| K_i \left| T_i \right| T_{\mathrm{int}} \left| \delta \right.\right) \end{array}$$

Αφού δεν χρειαζόμαστε εμπιστευτικότητα, ο αποστολέας δεν χρειάζεται να κρυπτογραφήσει την πληροφορία. Το MAC χρησιμοποιεί το μυστικό κλειδί μοιρασμένο στον κόμβο και στη βάση σταθμό για να αυθεντικοποιήσει την πληροφορία, το υπάρχον Nm επιτρέπει στον κόμβο να επιβεβαιώσει την φρεσκάδα. Αντί να χρησιμοποιούμε ψηφιακή υπογραφή όπως στο TESLA, χρησιμοποιούμε το αυθεντικοποιημένο κανάλι κόμβος προς βάση σταθμό για να βοηθήσουμε την αυθεντικότητα εκπομπής.

6.5.5 Αυθεντικοποιημένα πακέτα εκπομπής.

Όταν ο δέκτης δέχεται πακέτα με το MAC, χρειάζεται να διαβεβαιωθεί ότι το πακέτο δεν είναι απάτη από τον εχθρό. Ο εχθρός ήδη γνωρίζει το γνωστοποιημένο κλειδί του χρονικού κενού, έτσι θα μπορούσε να πλαστογραφήσει το πακέτο αφού

γνωρίζει το χρησιμοποιούμενο κλειδί για να υπολογίσει το MAC. Λέμε ότι ο δέκτης χρειάζεται να είναι βέβαιος ότι το πακέτο είναι ασφαλές, δηλαδή ότι ο αποστολέας δεν γνωστοποίησε ακόμη το κλειδί το οποίο χρησιμοποιήθηκε για να υπολιστεί το MAC ενός εισερχόμενου πακέτου. Όπως αναφέρθηκε παραπάνω, ο αποστολέας και ο παραλήπτης χρειάζεται να είναι συγχρονισμένοι (be loosely) και οι δέκτες χρειάζεται να γνωρίζουν το πρόγραμμα γνωστοποίησης κλειδιού. Αν το εισερχόμενο πακέτο είναι ασφαλές, ο δέκτης αποθηκεύει το πακέτο (το επιβεβαιώνει μόνο μια φορά ότι το κλειδί είναι γνωστοποιημένο). Αν το εισερχόμενο πακέτο δεν είναι ασφαλές (είχε μια ασυνήθιστη μεγάλη καθυστέρηση), τότε ο δέκτης χρειάζεται να πετάξει το πακέτο αφού ο εχθρός μπορεί να το έχει τροποποίηση.

Όσο πιο γρήγορα ο κόμβος παραλάβει καινούργιο κλειδί Ki, αυθεντικοποιεί το κλειδί ελέγχοντας εάν ταιριάζει με το τελευταίο αυθεντικό κλειδί που ξέρει Kv, χρησιμοποιώντας μικρό αριθμό εφαρμογών της λειτουργίας μιας διαδρομής
F: $Kv=F^{i-v}$ (Ki). Εάν ο έλεγχος είναι επιτυχής, το νέο κλειδί Ki είναι αυθεντικό και ο δέκτης μπορεί να αυθεντικοποιήσει όλα τα πακέτα που είχαν σταλεί μέσα στα χρονικά όρια v ως i. Ο δέκτης επίσης αντικαθιστά τα αποθηκευμένα Kv με Ki.

6.5.6 Αυθεντικοποιημένες πληροφορίες εκπομπής κόμβων

Αφού ο κόμβος είναι περιορισμένης μνήμης, δεν μπορεί να αποθηκεύσει τα κλειδιά αλυσίδας μιας διαδρομής. Ακόμα περισσότερο, ο επαναυπολογισμός κάθε κλειδιού από τα αρχικά δημιουργούμενα κλειδιά Kn είναι πανάκριβος. Ακόμη, ο κόμβος ίσως να μην διέθετε ένα κλειδί με κάθε κόμβο, έτσι ώστε στέλνοντας την αυθεντικοποιημένη δέσμευση στην αλυσίδα κλειδιών θα μπορούσε να επιτευχθεί μια ακριβή συμφωνία κλειδιού από κόμβο σε κόμβο. Τέλος, η εκπομπή των γνωστοποιημένων κλειδιών σε όλους τους δέκτες είναι ακριβή για τους κόμβους και τα φίλτρα πολύτιμης ενέργειας.

Δυο λύσεις για το πρόβλημα είναι:

- Ο κόμβος εκπέμπει την πληροφορία μέσω της βάσης σταθμού. Χρησιμοποιεί SNEP για να στείλει πληροφορία με αυθεντικό τρόπο στη βάση σταθμό, η οποία και το εκπέμπει.
- Ο κόμβος εκπέμπει την πληροφορία. Παρόλα αυτά, η βάση σταθμός διατηρεί την αλυσίδα κλειδιού μιας διαδρομής και στέλνει κλειδιά στον εκπεμπόμενο κόμβο, που χρειάζεται. Για συνάρτηση ενέργειας για την εκπομπή κόμβου, η βάση σταθμός

μπορεί επίσης να εκπέμπει τα γνωστοποιημένα κλειδιά και να διεκπεραιώσει τις αρχικές βοηθητικές διαδικασίες για νέους δέκτες.

6.5.7 Εφαρμογή

Το μέγεθος της μνήμης είναι ένας περιορισμός. Οι κόμβοι των αισθητήρων έχουν 8Kbytes προγράμματος ROM και 512 bytes RAM. Η μνήμη προγράμματος χρησιμοποιείται για TinyOS, για την ασφάλεια συστήματος, και την εφαρμογή αισθητήρων διαδικτύου.

6.5.8 Κρυπτογράφηση block.

Μια αρχική επιλογή ήταν ο AES αλγόριθμος Rijndael. Παρόλα αυτά, μετά από έρευνα, δοκιμάσαμε εναλλακτικές προτάσεις με μικρότερο κώδικα και υψηλότερη ταχύτητα. Η βασική έκδοση του Rijndael χρησιμοποιεί πάνω από 800 bytes of lookup tables, τα οποία είναι πολύ μεγάλα για την μετακίνηση μνήμης των κόμβων.

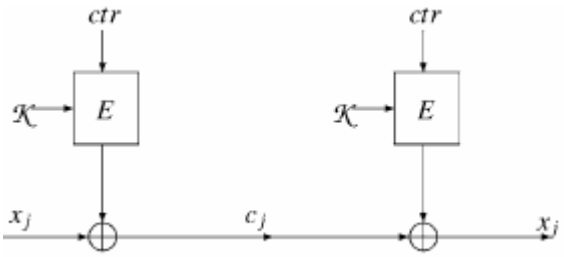
Μια λειτουργική έκδοση αυτού του αλγόριθμου (περίπου 100 φορές γρηγορότερη) χρησιμοποιεί πάνω από 10kbytes of lookup tables. Απορρίψαμε το DES block κρυπτογράφηση η οποία απαιτεί μια 512-είσοδο 5Box table και μια 256-είσοδο table για συνήθεις αλλαγές. Μια μικρή κρυπτογράφηση αλγόριθμού όπως η TEA, είναι μια πιθανότητα, αλλά δεν είναι ακόμα ικανή για κρυπτοαναλυτική έρευνα. Χρησιμοποιείται RC5 λόγω του μικρού μεγέθους κώδικα και υψηλής παραγωγικότητας. Το RC5 δεν βασίζεται στην πολυπλοκότητα και δεν απαιτεί μεγάλα tables. Παρόλα αυτά το RC5 χρησιμοποιεί 32-βιτ πληροφορίας εξαρτώμενα περιστροφής, τα οποία είναι ακριβά στον επεξεργαστή Atmel (υποστηρίζει μόνο ένα 8-bit μόνο bit περιστροφής).

6.5.9 Λειτουργία αποκρυπτογράφησης

Για να γλιτώσουμε χώρο κωδικού, χρησιμοποιούμε την ίδια λειτουργία και για την κρυπτογράφηση και την αποκρυπτογράφηση. Η μέθοδος CTR είναι μια κινητή κρυπτογράφηση. Το μέγεθος του κειμένου κρυπτογράφησης is ακριβώς το μέγεθος του κυρίως κειμένου και όχι πολλαπλάσιο του μεγέθους block. Η αποστολή και λήψη μηνυμάτων εξοικονομούν πολλή ενέργεια. Επίσης, μεγάλα μηνύματα έχουν υψηλή πιθανότητα διαστρέβλωσης πληροφορίας. Γι' αυτό τα κρυπτογραφημένα μηνύματα μεγάλης έκτασης είναι ανεπιθύμητα. Η μέθοδος CTR απαιτεί έναν μετρητή

για κάθε λειτουργία. Η μέθοδος αυτή προσφέρει σημαντική ασφάλεια. Το ίδιο κυρίως κείμενο που στάλθηκε σε διαφορετικές στιγμές είναι αποκρυπτογραφημένο μέσα σε διαφορετικά κείμενα κρυπτογράφησης αφού τα μονοπάτια δημιουργήθηκαν από διαφορετικούς μετρητές. Για έναν εχθρό που δεν ξέρει το κλειδί, αυτά τα μηνύματα θα εμφανιστούν σαν άσχετα τυχαία αντικείμενα.

Αφού ο αποστολέας και ο δέκτης μοιράζονται τον μετρητή, δεν χρειάζεται να τον συμπεριλάβουμε στο μήνυμα. Αν οι δυο κόμβοι χάσουν τον συγχρονισμό του μετρητή, μπορούν να μεταδώσουν τον μετρητή για να επανασυγχρονιστεί χρησιμοποιώντας SNEP με δυνατή φρεσκάδα.



Σχήμα 6.2 Λειτουργία κωδικοποίησης και αποκωδικοποίησης του μετρητή.Η λειτουργία κωδικοποίησης εφαρμόζεται σε ένα μονοτονικό αυξανόμενο μετρητή για να δημιουργήσει ένα pad. Αυτό το pad είναι με XOR με το αποκωδικοποιημένο κείμενο .Η λειτουργία της αποκωδικοποίσης είναι απαράλλαχτη. **(12)**

6.5.10 Ανανέωση-Φρεσκάδα

Αφού ο αποστολέας μεγαλώνει τον μετρητή μετά από κάθε μήνυμα, ο δέκτης επιβεβαιώνει την αδυναμία της φρεσκάδας με την επιβεβαίωση ότι τα παρεληφθέντα μηνύματα έχουν αυξήσει μονότονα τον μετρητή. Για αιτήσεις που απαιτούν φρεσκάδα, ο αποστολέας δημιουργεί ένα τυχαίο Nm (μια απρόβλεπτη 64-bit αξία) και το περιλαμβάνει στο αιτούμενο μήνυμα στον δέκτη.

Ο δέκτης δημιουργεί το μήνυμα απάντηση και περιλαμβάνει το Nm στον υπολογισμό MAC. Εάν το MAC επιβεβαιώσει την απάντηση επιτυχώς, ο κόμβος ξέρει ότι η απάντηση δημιουργήθηκε μετά αφότου στάλθηκε το αιτούμενο μήνυμα οπότε επιτυγχάνεται φρεσκάδα (ανανέωση).

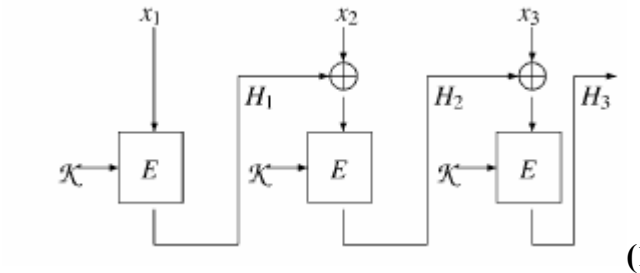
6.5.11 Τυχαία δημιουργία αριθμών

Ο κόμβος έχει τους δικούς του αισθητήρες, ασυρμάτους δέκτες και προγραμματισμένες διαδικασίες από τις οποίες μπορούμε να πάρουμε τυχαία ψηφία. Όμως για να ελαχιστοποιήσουμε τις απαιτήσεις δύναμης, χρησιμοποιούμε την

λειτουργία MAC σαν μια τυχαία ψεύτικη γεννήτρια αριθμών (PRG) με το κλειδί Xrand. Επίσης διατηρούμε έναν μετρητή C τον οποίο μεγαλώνουμε μετά από κάθε τυχαίο ψεύτικο στοιχείο που δημιουργούμε. Υπολογίζουμε την C-ιοστή ψεύτική και τυχαία έξοδο του στοιχείου ως MAC (Xrands). Αν το C wraps around (το οποίο δεν θα ξανασυμβεί γιατί ο κόμβος θα μείνει πρώτος από ενέργεια) μπορούμε να πάρουμε ένα νέο PRG κλειδί από το κύριο μυστικό κλειδί και το τρέχον PRG κλειδί χρησιμοποιώντας το MAC ως λειτουργία ψεύτικη και τυχαία (PRF): Xrand=MAC (X, Xrand).

6.5.12 Αυθεντικότητα μηνύματος

Επειδή θέλουμε να ξαναχρησιμοποιήσουμε την κρυπτογράφηση στοιχείου, χρησιμοποιούμε το γνωστό CBC-MAC. Ένα διάγραμμα στοιχείου για υπολογισμό CBC MAC φαίνεται στο σχήμα 6. 3



(12)

Σχήμα 6.3 CBC .Η έξοδος του τελευταίου τμήματος εξυπηρετεί σαν τον κώδικα αυθεντικότητας

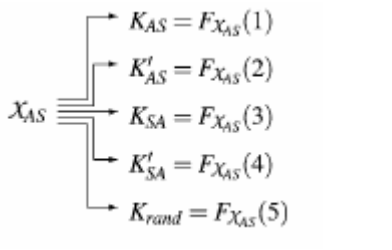
Για την επίτευξη αυθεντικότητας και αξιοπιστίας μηνύματος χρησιμοποιούμε την παρακάτω προσέγγιση. Υποθέτοντας ένα μήνυμα M, ένα κλειδί αποκρυπτογράφησης K και ένα κλειδί MAC K΄, χρησιμοποιούμε την παρακάτω δομή:

{M}K, MAC (K΄, {M}K). Αυτή η δομή αποτρέπει τους κόμβους από κρυπτογραφημένο λανθασμένο κείμενο, το οποίο είναι ένα πιθανόν ρίσκο ασφαλείας. Στην εφαρμογή μας αποφασίσαμε να υπολογίσουμε ένα MAC ανά πακέτο. Το MAC χρησιμοποιήθηκε για να ελέγχει αυθεντικότητα και αξιοπιστία μηνυμάτων μαζί, εξαφανίζοντας την ανάγκη για μηχανισμούς όπως ο CRC.

6.5.13 Εγκατάσταση κλειδιού

Η ανάκληση εγκατάστασης κλειδιού εξαρτάται από το κύριο μυστικό κλειδί, αυτό που αρχικά που μοιράζονται ο κόμβος και η βάση σταθμός. Το αποκαλούμε αυτό το κλειδί ως X_{AS} για τον κόμβο A και τη βάση σταθμό S. Όλα τα άλλα κλειδιά

είναι βοηθητικά από τα αρχικά κυρίως μυστικά κλειδιά. Το σχέδιο 6.4 δείχνει την διαδικασία προορισμού των κλειδιών.



Σχήμα 6.4 Αφιχθέντα εσωτερικά κλειδιά από το κύριο μυστικό κλειδί. **(12)**

Πάλι χρησιμοποιούμε το (PRF) και τη λειτουργία F με τη σχέση $F_K(x) = MAC(K, x)$.

Αυτό ξανά επιτρέπει για περισσότερη χρήση κώδικα. Εξαιτίας της κρυπτογραφικής ποιότητας του MAC, θα πρέπει να είναι μια καλή ψεύτικη-τυχαία λειτουργία. Όλα τα κλειδιά που αναχωρούν είναι υπολογίσιμα ανεξάρτητα. Ακόμα και αν ο εισβολέας μπορούσε να σπάσει ένα από αυτά, η γνώση ενός τέτοιου κλειδιού δεν θα τον βοηθούσε να βρει το κύριο μυστικό ή ένα άλλο κλειδί. Εάν ανακαλύψουμε ότι ένα κλειδί έχει αποκαλυφθεί, τότε και τα δυο μέρη μπορούν να στείλουν νέο κλειδί χωρίς εκπομπή κάποιας εμπιστευτικής πληροφορίας.

6.6 Εκτίμηση

Εκτιμούμε την εφαρμογή των πρωτοκόλλων από το μέγεθος του κώδικα, μέγεθος RAM, και την επικεφαλίδα του επεξεργαστή και επικοινωνίας.

6.7 Μέγεθος κώδικα

Ο πίνακας 6.5 δείχνει το μέγεθος κώδικα από τρεις εφαρμογές κρυπτό ρουτίνες στο TinyOS. Η μικρότερη εκδοχή από αυτές απασχολεί περίπου το 20% του χώρου του κώδικα. Το μTESLA πρωτόκολλο χρησιμοποιεί άλλα 574 bytes. Μαζί, η βιβλιοθήκη κρύπτο, και η εφαρμογή του πρωτοκόλλου χρησιμοποιούν περίπου 2 Kbytes της μνήμης του προγράμματος, το οποίο είναι δεκτό στις περισσότερες αιτήσεις. Το Open SSL εφαρμόζει RC5 αποκρυπτογράφηση ως λειτουργία. Στο hardware αισθητήρων, το μέγεθος του κώδικα της εγκατάστασης και της επιστροφής (return) ξεπερνά το μέγεθος κώδικα του κυρίως μέρους της λειτουργίας του RC5.

Table 2
Code size breakdown (in bytes) for the security modules.

Version	Total size	MAC	Encrypt	Key setup
Smallest	1580	580	402	598
Fastest	1844	728	518	598
Original	2674	1210	802	686

Πίνακας 6.5 Σπάσιμο μεγέθους κώδικα (σε bytes) για τα μοντέλα ασφάλειας. **(12)**

6.7.1Παραμένοντα θέματα ασφαλείας

Αν και το πρωτόκολλο αυτό επιλύει πολλά σχετικά προβλήματα με την ασφάλεια, υπάρχουν κάποια πρόσθετα θέματα που μένουν άλυτα. Πρώτον, δεν επιλύουμε το πρόβλημα της πληροφορίας που διαρρέετε μέσω κρυφών καναλιών. Δεύτερον, δεν έχουμε να κάνουμε με συμβιβασμένους κόμβους, απλώς διαβεβαιώνουμε ότι ο συμβιβασμός ενός απλού κόμβου δεν αποκαλύπτει τα κλειδιά όλων των αισθητήρων στο δίκτυο. Τρίτον, δεν έχουμε να κάνουμε, με επιθέσεις DOS (denial-of service) άρνηση εξυπηρέτησης, σ' αυτή την λειτουργία. Αφού λειτουργούμε σε ένα ασύρματο δίκτυο, ένας εχθρός μπορεί πάντα να προκαλέσει μια επίθεση DOS με συνωστισμό των ασυρμάτων σημάτων με ένα δυνατό σήμα.

Τέλος, εξαιτίας των περιορισμένων hardware δεν μπορούμε να παρέχουμε συμφωνία με το κλειδί Diffie – Hellman ή να χρησιμοποιήσουμε ψηφιακές υπογραφές για την επίτευξη της μη απάρνησης. Για την πλειοψηφία των εφαρμογών στα δίκτυα αισθητήρων η αυθεντικότητα είναι επαρκής.

6.8Εφαρμογές

6.8.1 Αυθεντική δρομολόγηση

Χρησιμοποιώντας το μTESLA πρωτόκολλο, αναπτύξαμε ένα ελαφρύ, αυθεντικό, ad hoc πρωτόκολλο δρομολόγησης το οποίο κατασκευάζει μια αυθεντική τοπολογία δρομολόγησης.

Υπάρχουν δύο μηχανισμοί που προστατεύουν ένα δίκτυο ad hoc εναντίον κόμβων που αποτυγχάνουν να προωθήσουν σωστά πακέτα.

Ένας απ'αυτούς είναι ένα watchdog για να ανιχνεύσει απροσάρμοστους γειτονικούς κόμβους κι έναν pathrater να αναφέρει για την καλή λειτουργία των άλλων κόμβων.

Συνιστάται το ''τρέξιμο'' αυτών των μηχανισμών σε κάθε κόμβο.Παρ'όλα αυτά δεν φοβόμαστε ένα πρωτόκολλο δρομολόγησης το οποιό χρησιμοποιεί αυθεντικά μηνύματα δρομολόγησης. Είναι δυνατόν για έναν κακεντρεχή χρήστη να

αποκτήσει τον έλεγχο του δικτύου ρίχνοντας ψεύτικες , παλιές ξαναπαιγμένες πληροφορίες δρομολόγησης.

Το σχέδιο δρομολόγησης, μέσα στο πρωτότυπο δίκτυο μας, υποθέτει κανάλια επικοινωνίας σε δύο διαφορετικές κατευθύνσεις π.χ εάν ο κόμβος Α ακούσει τον κόμβο Β , τότε ο κόμβος Β ακούει τον κόμβο Α. Η ανακάλυψη του δρόμου εξαρτάται από την περιοδική εκπομπή σημάτων. Κάθε κόμβος πάνω από την υποδοχή πακέτου σήματος, ελέγχει εάν αυτό έχει ήδη παραλάβει ένα σήμα εκπεμπόμενο (το οποίο είναι ένα φυσιολογικό πακέτο με μία μοναδική σφαιρική ID αποστολέα και τρεχον χρόνο στη βάση σταθμό, προστατευμένο από ένα MAC για να διαβεβαιώσει την ακεραιότητα και ό,τι η πληροφορία είναι αυθεντική) στο τρέχον διάστημα μεταξύ αναβαθμίσεων δρομολόγησης.

Εάν ένας κόμβος ακούσει το εκπεμπόμενο σήμα (σινιάλο) μέσα στο διάστημα αυτό, δεν έχει περαιτέρω δράση. Ειδάλλως, ο κόμβος δέχεται τον αποστολέα του σήματος σαν τον ‘’γονέα του’’ για να το δρομολογήσει γύρω από τη βάση σταθμό. Πρόσθετα, ο κόμβος θα επαναλάμβανε το ‘’σινιάλο’’ με την ID του αποστολέα αλλαγμένη στον εαυτό του. Η ανακάλυψη αυτού του δρόμου μοιάζει με ένα διανεμημένο αλγόριθμο έρευνας πλάτους και παράγει μια τοπολογία δρομολόγησης. Παρόλα αυτά στον παραπάνω ακγόριθμό, η ανακάλυψη δρόμου εξαρτάται μόνο από την υποδοχή του πακέτου route και όχι των περιεχομένων του.

Αντιθέτως, σημειώνουμε ότι τα μTESLA πακέτα αποκάλυψης κλειδιών μπορούν εύκολα να λειτουργήσουν όπως τα σινιάλα δρομολόγησης. Δεχόμαστε μόνο τις πηγές των αυθεντικών σινιάλων σαν νόμιμους ‘’γονείς’’. Η υποδοχή ενός μTESLA εγγυάται ότι το πακέτο δημιουργήθηκε στη βάση σταθμό και αυτό είναι φρέσκο. Για κάθε χρονικό διάστημα δεχόμαστε σαν τον ‘’γονέα’’ τον πρώτο κόμβο στέλνοντας ένα αποτυχημένο αυθεντικό πακέτο. Η σύγκριση του μTESLA αποκάλυψης κλειδιών με την διανομή των σινιάλων δρομολόγησης επιτρέπει σε μας να συνδυάσουμε μεταδόσεις των κλειδιών με την συντήρηση δικτύων.

Περιγράψαμε ένα σχέδιο που οδηγεί σε ένα ελαφρύ, αυθεντικό πρωτόκολλο δρομολόγησης για δίκτυα αισθητήρων. Αφού κάθε κόμβος δέχεται μόνο το πρώτο αυθεντικό πακέτο σαν το μοναδικό για χρήση στη δρομολόγηση, είναι αδύνατον για έναν εχθρό να δρομολογήσει εχθρικές ζεύξεις μέσα στο δίκτυο αισθητήρων. Κάθε κόμβος επιβεβαιώνει την συμπεριφορά του ‘’γονέα’’ με την επίτευξη λειτουργιών όμοιων με το watchdog που περιγράφτηκε. Το παραπάνω αυθεντικό σχέδιο δρομολόγησης είναι ένας μόνος τρόπος να κατασκευάσεις αυθεντικά πρωτόκολλα ad-

hoc δρομολόγησης χρησιμοποιώντας το μTESLA. Σε πρωτόκολλα όπου οι βάσεις σταθμοί δεν εμπλέκονται σε κατασκευές δρομολόγησης το μTESLA μπορεί να χρησιμοποιείται για ασφάλεια. Σε τέτοιες περιπτώσεις, ο αρχικός κόμβος θα δράσει προσωρινά σαν βάση σταθμός.

6.8.2 Κλειδί συμφωνίας κόμβου-προς κόμβο

Μια κατάλληλη τεχνολογία για ασφαλείς συνδέσεις είναι να χρησιμοποιούνται πρωτόκολλα για κρυπτογραφημένα δημόσια κλειδιά για εγκατάσταση συμμετρικών κλειδιών.

Είναι ανάγκη να κατασκευάζουμε τα πρωτόκολλα μας μόνο από αλγόριθμους συμμετρικών κλειδιών. Σχεδιάζουμε ένα συμμετρικό πρωτόκολλο το οποίο χρησιμοποιεί τη βάση σταθμό για εγκατάσταση κλειδιού.

Υποθέτουμε ότι ο κόμβος Α θέλει να δημιουργήσει μία σειρά μυστικών κλειδιών S_{KAB} με τον κόμβο Β. Αφού ο Α και ο Β δεν μοιράζονται μυστικά, είναι ανάγκη να χρησιμοποιήσουν ένα εμπιστευτικό τρίτο μέρος S το οπίο είναι η βάση σταθμός, στην περίπτωση μας. Ο Α και ο Β μοιράζονται ένα κύριο μυστικό κλειδί με την βάση σταθμό X_{AS} και X_{BS}. Το ακόλουθο πρωτόκολλο πετυχαίνει μια συμφωνία ασφαλούς κλειδιού τόσο καλά όσο μια δυνατή φρεσκάδα κλειδιού.(Σχέσεις στη σελίδα 531 του spins)

Το πρωτόκολλο χρησιμοποιεί το πρωτόκολλο SNEP με μεγάλη φρεσκάδα. Οι nonces N_A και N_B διαβεβαιώνουν μεγάλη φρεσκάδα κλειδιών και στον Α και στον Β. Το πρωτόκολλο SNEP εξασφαλίζει εμπιστευτικότητα (μέσω της κωδικοποίησης με τα κλειδιά K_{AS} και K_{BS}) της εγκαθισταμένης σειράς κλειδιών S_{KAB} τόσο καλά όσο και η αυθεντικότητα μηνυμάτων α9μέσω του MAC που χρησιμοποιεί κλειδιά K'_{AS} και K'_{BS}), ετσι είμαστε σίγουροι ότι το κλειδί ήταν πράγματι δημιουργημένο από τη βάση σταθμό. Σημειώστε ότι το MAC στο δεύτερο μήνυμα πρωτοκόλου βοηθά να αμυνθεί η βάση σταθμός από τις επιθέσεις άρνησης εξυπηρέτησης και η βάση σταθμός στέλνει μόνο δύο μηνύματα στον Α και Β εάν αυτό παρέλαβε μια νόμιμη αίτηση από έναν από τους κόμβους.

Ένα καλό χαρακτηριστικό του παραπάνω πρωτοκόλλου είναι ότι η βάση σταθμός προκαλεί το περισσότερο έργο μετάδοσης. Πολλά άλλα πρωτόκολλα εμπεριέχουν ένα εισιτήριο (ticket) το οποίο ο server το στέλνει σε ένα από τα μέρη τα

οποία το προωθούν σε άλλο κόμβο , ο οποίος απαιτεί περισσότερη ενέργεια για τους κόμβους να προωθήσουν το μήνυμα.

Το πρωτόκολλο συμφωνίας κλειδιού Kerberos πετυχαίνει παρόμοιες ιδιότητες, αλλά δεν παρέχει μεγάλη φρεσκάδα κλειδιών. Εάν το Kerberos χρησιμοποιούσε το SNEP με μεγάλη φρεσκάδα, τότε το Kerberos θα είχε περισσότερη ασφάλεια.

6.9 ΠΡΩΤΟΚΟΛΛΟ SEKEN

6.9.1.Εισαγωγή.

Στο κεφάλαιο αυτό, θα περιγράψουμε το SEKEN πρωτόκολλο (Secure and Efficient Key Exchange for sensor Networks) δηλ. ασφαλές και αποτελεσματικό κλειδί ανταλλαγής για δίκτυα αισθητήρων, το οποίο ασφαλίζει την ανταλλαγή κλειδιών μεταξύ δυο γειτονικών κόμβων με την ελάχιστη κατανάλωση πόρων.

6.9.2 Υποθέσεις

Πριν ξεκινήσουμε να περιγράψουμε το πρωτόκολλο, πρέπει να ταυτοποιήσουμε τις υποθέσεις που υποστηρίζει το μοντέλο μας. Υποθέτουμε ότι το radio μοντέλο είναι συμμετρικό. Π.χ. για μια δοσμένη σχέση σήματος-θορύβου, η απαιτούμενη ενέργεια για να μεταδώσει ένα μήνυμα m bit από τον κόμβο A στον κόμβο B είναι η ίδια με την απαιτούμενη ενέργεια που απαιτείται για την μετάδοση το ίδιο m bit μήνυμα από τον κόμβο B στον A. εξάλλου, υποθέτουμε ότι η βάση σταθμός έχει περισσότερους πόρους από ότι ένας κανονικός κόμβος αισθητήρα. Ειδικότερα, αφού η βάση σταθμός θα έβρισκε προστασία on-shore, θα μπορεί να λειτουργήσει σε συνηθισμένο ηλεκτρισμό και να χρησιμοποιήσει ισχυρούς υπολογιστές με περισσότερη μνήμη και ισχύ εκτελεστική.

Η βάση σταθμός μπορεί να διατηρεί ένα αντίγραφο των κλειδιών τα οποία μοιράζεται με κάθε ένα από τους αισθητήριους κόμβους και να χρησιμοποιεί τα κλειδιά αυτά για να στέλνει εμπιστευτικά μηνύματα σε ανεξάρτητους κόμβους. Εξαιτίας της εύκολα διαθέσιμης ηλεκτρικής ισχύος, η βάση σταθμός μπορεί επίσης να κάνει μια μεγάλη σειρά από radio μεταδόσεις για την προσέγγιση ενός κόμβου οπουδήποτε μέσα στον δίκτυο αισθητήρων. Παρόλα αυτά, προκειμένου να ταξιδέψουν μηνύματα από κόμβο αισθητήρα στη βάση σταθμό, το μήνυμα πρέπει να πηδάει από κόμβο σε κόμβο προκειμένου να μεγιστοποιήσει την διατήρηση ενέργειας.

Επίσης κάνουμε κάποιες υποθέσεις για την γενική αρχιτεκτονική και τις απαιτήσεις εμπιστοσύνης των αισθητήριων δικτύων. Πρώτα, υποθέτουμε ότι οι

αισθητήριοι κόμβοι δημιουργήθηκαν με τη μοναδική συσκευή αναγνώρισης (Did) Device Identifier, η οποία είναι γνωστή μόνο από αυτόν τον ιδιαίτερο αισθητήριο κόμβο. Το Did όλων των κόμβων πρέπει να είναι προγραμματισμένο δια χειρός μέσα στη βάση σταθμό και κάθε (Did) να δρα σαν ένα αρχικό μοιρασμένο μυστικό ανάμεσα στη συσκευή αυτή και στη βάση σταθμό. Το Did χρησιμοποιείται μόνο κατά τη διάρκεια της αρχικής-χωρίς βοήθεια διαδικασίας και ποτέ δεν ανταλλάσσεται στο καθαρό κείμενο, για αυτό διαβεβαιώνει ότι αυτή η συσκευή αναγνώρισης ποτέ δεν αποκαλύπτει ρητώς σε κανέναν άλλο αισθητήριο κόμβο. Οι μηχανισμοί tamper resistance της συσκευής μπορεί να έχουν απασχοληθεί για να διαβεβαιώσουν ότι η μνήμη κατακλύσει (flushed) εάν κάποια προσπάθεια έχει γίνει για φυσικό χειρισμό της συσκευής προκειμένου να ανακτήσει αυτή την πληροφορία. Εξάλλου, υποθέτουμε ότι το κοινό κλειδί της βάσης σταθμού έχει προαναπτυχθεί μέσα στους αισθητήρες. Οι αισθητήριοι κόμβοι μπορούν καταλλήλως να προγραμματισθούν με αυτό το κλειδί πριν τη πραγματική τους απασχόληση στο πεδίο. Αυτό αφαιρεί την ανάγκη για μια αξιόπιστη πανταχού παρών αρχή πιστοποίησης (Certification Anthority) CA.

6.9.3 Σημείωση

Θα χρησιμοποιήσουμε τους ακόλουθους συμβολισμούς για να διευκρινίσουμε διαφορετικά αρχικά στις κρυπτογραφικές λειτουργίες μας.

- Ένα μήνυμα Μ κωδικοποιημένο με κλειδί Κ παρουσιάζεται ως Εκ(Μ).
- ΤοE_{PUB} (Μ) είναι μια κωδικοποίηση μηνύματος Μ με το κοινό κλειδί της βάσης σταθμού.
- Α, Β1, Β2 είναι παραδείγματα των κόμβων /Ds. Οι κόμβοι /Ds είναι διαφορετικοί από D/ds στο ότι ο προηγούμενος (former) είναι μόνο ένα προσωρινό tag σχεδιασμένο από τη βάση σταθμό για μια συγκεκριμένη τοπολογία δικτύου, ενώ ο επόμενος (latter) είναι ένας περισσότερο διαρκής αναγνωριστής για τη συσκευή.
- Ν1, ΝΑ, κ.λ.π. είναι παραδείγματα του παρόντος (της στιγμής) ένα τυχαίο bit string) και TS είναι το τρέχον timestamp. Αυτά βοηθούν στην παροχή προστασίας από επιθέσεις επαναλαμβανόμενες.
- MAC (K, C) είναι ένα μήνυμα με γνήσιο κώδικα υπολογισμένο πάνω από έναν μετρητή C χρησιμοποιώντας κλειδί Κ.

6.9.4 Το πρωτόκολλο

Ερμηνεύουμε τρεις βασικούς τύπους μηνυμάτων που χρησιμοποιούνται για να ξεκινήσουν το πρωτόκολλο SEKEN. Ένας κόμβος θέλοντας να λάβει μέρος στο δίκτυο στέλνει ένα «join-network» μήνυμα. Κατόπιν της επιτυχημένης αυθεντικότητας με τη βάση σταθμό, ο κόμβος αυθεντικοποιείται με τους γειτονικούς του (κόμβους) χρησιμοποιώντας ένα «αυθεντικοποίησε με» μήνυμα. Τέλος, ο κόμβος που θα αποτύχει να λάβει μια απάντηση από τον προηγούμενο γειτονικό του, στέλνει ένα μήνυμα «update-neighbor» στη βάση σταθμό. Το κάθε ένα από αυτά τα μηνύματα αναγνωρίζεται από ένα πεδίο ταυτότητας στη κεφαλή του μηνύματος, και αυτός υπόσχεται μια άνετη πράξη (δράση) στις κατάλληλες συσκευές δικτύου.

6.9.5 Φάση εγκατάστασης κλειδιού

Ο πιο κοντινός κόμβος στην βάση σταθμό ξεκινάει την φάση εγκατάστασης του κλειδιού σαν αποτέλεσμα του μηνύματος «join-network». Αυτό ανακτάει το Did του από την μνήμη, προσάρτει σ' αυτό την τρέχουσα timestamp, TS και κωδικοποιεί όλο το πακέτο με το κοινό κλειδί της βάσης σταθμού. Περιμένει έναν τυχαίο χρόνο πριν να μεταδώσει το πακέτο αυτό στη βάση σταθμό:

$$\text{A} \rightarrow \text{BS}: E_{PUB}\left(DId_A, TS\right) \qquad (1)$$

Ο κόμβος επίσης υπολογίζει το τοπικό αντίγραφο του κλειδιού KA, το οποίο θα μοιραστεί με την βάση σταθμό υπολογίζοντας το KA=MAC(DId, TS). Η βάση σταθμός αποκωδικοποιεί το ληφθέν μήνυμα με το αντίστοιχο ιδιωτικό κλειδί της και αναζητά βάση πληροφοριών της για μια συσκευή με τον ίδιο αναγνωριστή. Για την επιβεβαίωση της γνησιότητας της συσκευής και την αντίληψη ότι αυτός είναι ο πρώτος κόμβος που ζητά σχέση, η βάση σταθμός υπολογίζει το δικό της αντίγραφο από το προτεινόμενο κλειδί KA=MAC(DId, TS). Χρησιμοποιεί αυτό το κλειδί για να στείλει τις ακόλουθες κωδικοποιημένες πληροφορίες στον κόμβο A. Ο κόμβος ID, IDA και ο μετρητής CA, ξεκίνησαν να παίρνουν τυχαίες τιμές. Ο κόμβος ID είναι μια μοναδική προσωρινή συσκευή αναγνώρισης εκχωρημένης σε μια συσκευή για το τρέχον δίκτυο μόνο και βοηθάει με το routing των μηνυμάτων. Τέλος ID μπορεί να είναι μια γεωγραφική αντιπροσώπευση της τοποθεσίας κόμβου μέσα στο δίκτυο αισθητήρων.

Η τιμή μετρητή χρησιμοποιείται σε ένα MAC για να δημιουργήσει ένα κλειδί συνόδου μεταξύ του κόμβου αυτού και του δυνατού γειτονικού του, και αυξάνεται

και στα δυο η βάση σταθμός τόσο καλά όσο και στον αισθητήριο κόμβο μετά από κάθε αυθεντικότητα κλειδιού μεταξύ του κόμβου και του γειτονικού του.

$$BS \rightarrow A: E_{KA} (CA, ID_A)$$

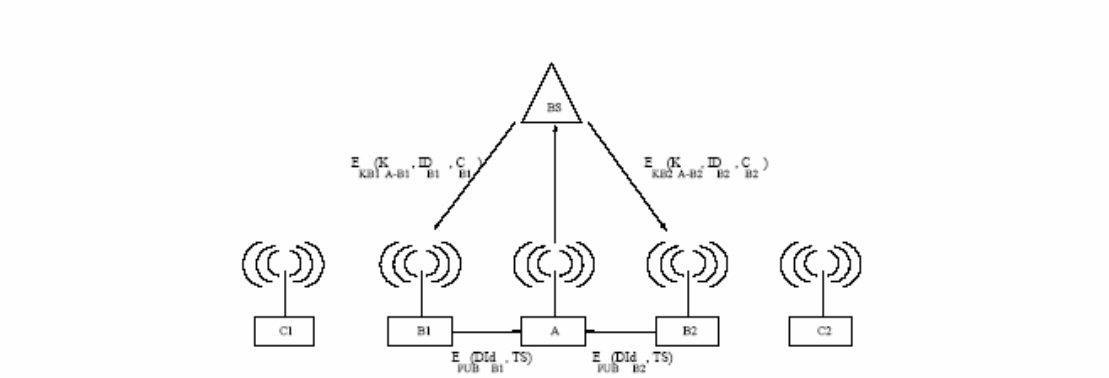
Ο πρώτος κόμβος που καταφέρνει να ολοκληρώσει την διαδικασία εγκατάστασης κλειδιού με τη βάση σταθμό, δρα σαν μια gateway για όλους τους άλλους κόμβους στο δίκτυο, βοηθώντας τους να επικοινωνήσουν με το εξωτερικό κόσμο. Ο επόμενος αισθητήριος κόμβος (έστω B1) επιθυμεί να λάβει μέρος στο δίκτυο και προκαλεί την ίδια ακολουθία βημάτων. Ξεκινάει με την προσάρτηση των τρεχόντων timestamp του στο DId του, κωδικοποιεί το αποτέλεσμα με το κοινό κλειδί της βάσης σταθμού, και υπολογίζει το τοπικό αντίγραφο του KB1.Το κωδικοποιημένο πακέτο εκπέμπεται τότε, και ο πιο κοντινός γειτονικός του στη σειρά κοντά στη βάση σταθμό προσαρτά το δικό του κωδικοποιημένο ID στο μήνυμα (για να βοηθήσει την βάση σταθμό εκτιμά την τοποθεσία, κατά προσέγγιση, του νέου κόμβου), και το μήνυμα τελικά μεταφέρεται στη βάση σταθμό.

$$B1 \rightarrow A= EPUB (DidB_4, TS) \qquad (3)$$

$$A \rightarrow BS: EPUB (DidB_1, TS), EKA (IDA) \qquad (4)$$

Η βάση σταθμός προκαλεί την ρουτίνα των ελέγχων γνησιότητας στον κόμβο, υπολογίζει το προτεινόμενο κλειδί από τον αισθητήριο κόμβο και έπειτα στέλνει στον κόμβο την πληροφορία που χρειάζεται για να γίνει κομμάτι του δικτύου. Εξάλλου, στο ID_{B1} και C_{B1}, η βάση σταθμός στέλνει επίσης το κλειδί στον B1 κόμβο KA-B1=MAC(KA, CA) το οποίο μοιράζεται με το γειτονικό του A.

$$BS \rightarrow B_1: EK_{B1} (K_{A-B1}, IDB1, C_{B1}) \qquad (5)$$



Σχήμα 6.6 Η ανταλλαγή μηνυμάτων για το πρωτόκολλο SEKEN. Οι κόμβοι B1 και B2 εγκαθιστούν ένα ασφαλές κλειδί με την βάση σταθμό. Ο κεντρικός κόμβος A έχει λάβει ήδη το $E_{KA}(C_a, ID_A)$ από τη βάση σταθμό BS. **(11)**

6.9.6 Αυθεντικότητα κλειδιού

Όποια φορά η πληροφορία αυτή είναι διαθέσιμη στον κόμβο B1, αυτός προσπαθεί να αυθεντικοποιήσει τον γειτονικό του A χρησιμοποιώντας ένα σχέδιο «πρόσκληση – απάντηση». Ο κόμβος B_1 δημιουργεί το παρών (nonce), N1, κωδικοποιεί αυτό με το κλειδί K_{A-B1}, και το μεταδίδει στον γειτονικό του κόμβο A. Ο κόμβος A, κατά την λήψη ενός «authenticate-me» μηνύματος, υπολογίζει το δικό του αντίγραφο K_{A-B1}=MAC (KA, CA) και απαντάει με τον γνήσιο nonce N1 και έναν νέο nonce N2, και οι δυο κωδικοποιημένοι με το πρόσφατα συμφωνημένο κλειδί K_{A-B1}. Για να ολοκληρώσει ο κόμβος A την γνησιότητα του (αυθεντικότητα), το B1 απαντάει με τον nonce N2 κωδικοποιημένο με το μοιραζόμενο κλειδί K_{A-B1}.

$$B_1 \rightarrow A: EK_{A-B1} (NA) \quad (6)$$

$$A \rightarrow B_1: E\ K_{A-B1} (NA, NB) \quad (7)$$

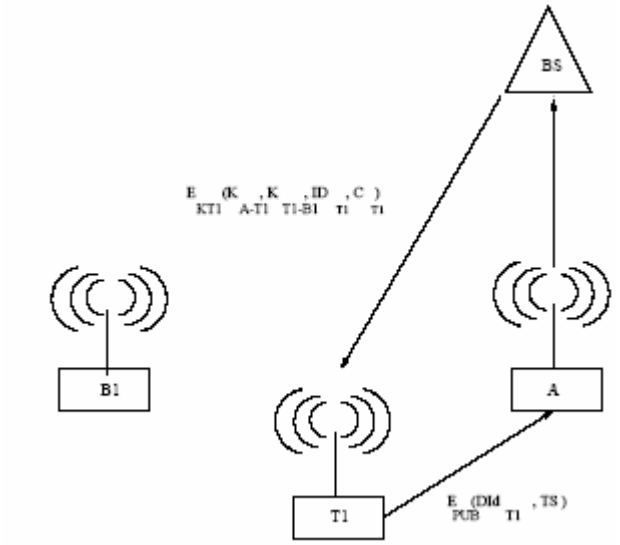
$$B_1 \rightarrow A: E\ K_{A-B1} (NB) \quad (8)$$

Η ίδια πορεία τότε επιτυγχάνεται για όλους τους παραμέτοντες κόμβους όταν αυτοί συνδέονται στο δίκτυο. Για παράδειγμα, σε απάντηση του αιτήματος του κόμβου C1, η βάση σταθμός απαντά με το E_{KC1} (K_{B1-C1}, ID_{C1}, C_{C1}). Αυτό σημαίνει ότι ο κόμβος C1 θα μοιράζεται τελικά το K_{B1-C1}= MAC (K_{B1}, C_{B1}) όπως ένα κλειδί με κόμβο B_1.

6.9.7 Πρόσθεση κόμβου και απόσπαση

Υποθέτουμε ότι ένας κόμβος δικτύου θέλει να επιτεθεί από μόνος του σε αυτή την αλυσίδα των αισθητήριων κόμβων κάνοντας την εμφάνιση του μεταξύ δυο υπαρχόντων κόμβων. Για παράδειγμα ο κόμβος T1 συνδέεται στο δίκτυο μεταξύ των κόμβων A και B1 στο σχήμα 6.7 Θεωρεί ένα μήνυμα «join-network» στο οποίο ο κόμβος A προσαρτά το δικό του ID και προωθεί αυτό στη βάση σταθμό έτσι ακριβώς όπως για έναν άλλο κόμβο. Η βάση σταθμός διατηρεί το τοπολογικό γράφημα όλου του δικτύου, το οποίο την βοηθάει να ανακαλύψει ότι ένας νέος κόμβος έχει προσαρτηθεί μεταξύ δύο υπαρχόντων κόμβων. Επίσης με το να στέλνει την ρουτίνα περιγραφής πληροφορίας του δικτύου (IDT1 και CT1), η βάση σταθμός επίσης στέλνει τις τιμές MAC υπολογισμένες πάνω από το γειτονικό κλειδί και των τρεχούσων τιμών μετρητή για να δράσει σαν ένα μοιραζόμενο κλειδί μεταξύ αυτού του νέου κόμβου και των γειτονικών του. Μετά την παραλαβή αυτής της πληροφορίας, ο νέος κόμβος αυθεντικοποιεί τον εαυτό του σε κάθε ένα από τους δυο γειτονικούς του όπως φαίνεται στις σχέσεις (6)-(8).

Τώρα υποθέτουμε ότι ο κόμβος T1 έχει αντικατασταθεί και κανένας μεγαλύτερος δεν υπάρχει μέσα στο πεδίο radio των γειτονικών του A και B1. Υποθέτωντας ότι η αναγνώριση πακέτων έχει γίνει σε μια βάση hop-by-hop, ο κόμβος B1 ανακαλύπτει ότι έχει χαθεί επαφή με τον γειτονικό του T1. Αυτό δημιουργεί ένα μήνυμα «update-neighbor» και ακολουθείται ξανά η ακολουθία των βημάτων (3) και (4) που αναφέρθηκαν. Η βάση σταθμός ανακαλύπτει ότι ο κόμβος B1 είναι ήδη ένα μέρος του δικτύου. Απλώς υπολογίζει ένα νέο κλειδί μεταξύ των δυο αισθητήρων κόμβων A και B1 και το στέλνει στο B1. Έπειτα ο κόμβος B1 αυθεντικοποιεί τον εαυτό του στον κόμβο A χρησιμοποιώντας την διαδικασία που προαναφέρθηκε παραπάνω.



Σχήμα 6.7 Πρόσθεση μέλους στο πρωτόκολλο SEKEN Ο κόμβος T1 προσπαθεί να ενωθεί με το δίκτυο συμπεριλαμβάνοντας και τους κόμβους A,B1 και τους άλλους. Η χρήση του αυξημένου μετρητή κατά τη διάρκεια της διαδικασίας εγκατάστασης καθιστά ικανό τον αισθητήριο κόμβο να μοιραστεί μυστικά κλειδιά με ένα πλήθος γειτονικών του κόμβων. **(11)**

6.10 Συγκριτική Ανάλυση και Αποτελέσματα

Στο κεφάλαιο αυτό θα συγκρίνουμε την αποτελεσματικότητα του SEKEN απέναντι σε κάποια άλλα κοινά πρωτόκολλα εγκατάστασης κλειδιών εξαιτίας των αντίστοιχων ενεργειακών κόστων.

Τα αποτελέσματα δεικνύουν ότι το SEKEN δείχνει καλά εκτελεστικά χαρακτηριστικά απέναντι σε κάποια από τα υπάρχοντα πρωτόκολλα εγκατάστασης κλειδιών χωρίς να απαγορεύεται η **scalability** του συστήματος. Ένα από τα πιο απλά πρωτόκολλα εγκατάστασης κλειδιών έχει προαναπτυχθεί των κλειδιών πριν οι

αισθητήριοι κόμβοι τεθούν σε ενεργή λειτουργία. Όποια φορά αναπτυχθεί, οι κόμβοι ήδη μοιράζουν τα κρυπτογραφικά κλειδιά, και γι' αυτό το πρωτόκολλο απαιτεί μόνο αυθεντικότητα κόμβου χρησιμοποιώντας σχέδιο «πρόκληση-απάντηση». (Ίδιο όπως βήματα (6)-(8) ορισμένα για το SEKEN πιο πάνω). Αν και αυτό το πρωτόκολλο έχει μια ελάχιστη επικεφαλίδα, αυξάνει τις ανησυχίες ασφάλειας ειδικά για την αλλαγή διαμόρφωσης αποστολών π.χ. εάν γεννηθεί η ανάγκη για δυο διαφορετικά δίκτυα αισθητήρων να επικοινωνήσουν μεταξύ τους, το υλικό του κλειδιού ενός από αυτά τα δίκτυα αισθητήρων να επικοινωνήσουν μεταξύ τους, το υλικό του κλειδιού ενός από αυτά τα δίκτυα πρέπει να είναι επαναγράψιμο με αυτό του άλλου. Νέες μέθοδοι ασφάλειας θα χρειάζονταν να αναπτυχθούν για να προκαλέσουν αυτές τις λειτουργίες για αισθητήριους κόμβους που είναι ήδη αναπτυγμένα στο πεδίο.

Επίσης συγκρίνουμε το πρωτόκολλο SEKEN απέναντι στην εγκατάσταση ανταλλαγής του κλειδιού Kerberos μεταξύ δυο τμημάτων. Ένας αριθμός πρωτοκόλλων εγκατάστασης κλειδιών, που έχουν αναλυθεί για το περιβάλλον των δικτύων αισθητήρων και το Kerberos βρέθηκαν να είναι τα πιο ενεργειακά αποτελεσματικά μετά από τον προαναπτυγμένο μηχανισμό. Στο Kerberos πρωτόκολλο, κάθε κόμβος μοιράζει ένα long-term pairwise κλειδί με έναν εμπιστευτικό server a priori. Υποθέτουμε ότι η βάση σταθμός παίζει τον ρόλο ενός KDC (Key Distribution Center) κέντρο διανομής κλειδιών, και από μόνη της προτείνει το κλειδί session (συνόδου). Η εκδοχή 5 του πρωτοκόλλου Kerberos απλοποιημένη για το περιβάλλον του δικτύου αισθητήρων δείχνεται παρακάτω:

$$B1 \rightarrow T= B1, A, NB \quad (9)$$

$$T \rightarrow B1, ticket_A, EK_{BT} (K, NB, A) \quad (10)$$

$$B1 \rightarrow A: ticket_A, autenticator \quad (11)$$

$$A \rightarrow B1: E_K CTB \quad (12)$$

Το $Ticket_A$ ερμηνεύεται από το EKAT(K, B) ενώ ο αυθεντικοποιητής=Εκ (B, TB) όπου K_{AT} ή K_{BT} είναι το μοιραζόμενο κλειδί μεταξύ της βάσης σταθμού Τ και κόμβου Α ή κόμβου Β1, Κ είναι το κλειδί-session επιλεγμένο από το Τα, και ΤΒ είναι ένα timestamp από το τυπικό ρολόι του Β.

χρησιμοποιούμε το μοντέλο radio «πρώτη-παραγγελία» για να υπολογίσουμε τα κόστη ενέργειας σχετιζόμενα με την μετάδοση και την αποδοχή των πακέτων στο δίκτυο αισθητήρων. Για την μετάδοση Κ bits πληροφορίας σε άλλη απόσταση κόμβου, Β η πηγή κόμβος καταναλώνει

$$Etx(K, d) = E_{Tx}\text{-}elec(K) + E_{Tx}\text{-}amp(K, d) = E_{elec} + K + E_{amp} + K + d^2$$

Για την παραλαβή αυτού του μηνύματος, το radio ξοδεύει

Erx (K) = ERX-elec (K) = Eelec* K όπου Eelec = 50nj/bit είναι η απαιτούμενη ενέργεια για να «τρέξει» το κύκλωμα του Πομπού ή δέκτη και Eamp=100pj/bit/m^2 είναι η ενέργεια που χρησιμοποιείται για να αυξήσεις το μεταδιδόμενο σήμα.

Υποθέτουμε ότι όλα τα μεγέθη συμμετρικών κλειδιών είναι 64bits. Παρόλο που τα αποτελέσματα εξομοίωσης μπορούν εύκολα να αυξηθούν σε μεγέθη μεγαλύτερων κλειδιών, πιστεύουμε ότι το μήκος αυτό του κλειδιού είναι αρκετό για να παρέχει επαρκή προστασία απέναντι σε μια βίαιη επίθεση πάνω στον τρόπο ζωής του δικτύου αισθητήρων. Όλα τα nonce, οι κόμβοι IDS και τα timestamps υποτίθεται ότι είναι 32 bits σε μήκος.

Προγράμματα εξομοίωσης γράφτηκαν για να υπολογίσουν το σύνολο της καταλωθείσας ενέργειας για το «τρέξιμο» κάθε ενός πρωτοκόλλου πάνω από linear sensor array κάτω από το τεστ των συνθηκών και των υποθέσεων που αναγνωρίσθηκαν νωρίτερα. Το Cryptix Crypto 3.0 (ένα καθαρό μέρος επιτυχίας του SunSCE) χρησιμοποιούταν για να επιτύχει τα αρχικά κρυπτογραφικά και τα σχετικά με την ασφάλεια χειρονακτικά μηνύματα ανταλλάσσονταν χρησιμοποιώντας κοιλώδη επικοινωνία (socket communication).

Η κατανάλωση ενέργειας είναι το σύνολο της ενέργειας που καταναλώθηκε από τους αισθητήριους κόμβους που εμπεριέχονται στην εγκατάσταση του κλειδιού και στην ακόλουθη διαδικασία αυθεντικότητας (π.χ. μετάδοση και αποδοχή κόστων για τη βάση σταθμό αγνοούνται).

Η απόσταση μεταξύ κάθε οντότητος δικτύου υποτίθεται ότι είναι 100m. Αυτό σημαίνει ότι το κόστος μετάδοσης υπολογίστηκε να είναι 1050nj/bit αφού το κόστος υποδοχής είναι 50nj/bit κάτω από το μοντέλο ράδιο που περιγράψαμε παραπάνω.

Για τους προ-αναπτυσσόμενους μηχανισμούς κλειδιών, κάθε αισθητήριος κόμβος πρέπει μόνο να αυθεντικοποιήσει τα κλειδιά του με τους γειτονικούς του (κόμβους).

Η εφαρμογή του SEKEN σε τέτοιο δίκτυο αισθητήρων έχει ήδη εξηγηθεί παραπάνω. Για να διατηρηθεί συνέπεια στην αρχιτεκτονική του δικτύου μας, το Kerberos απαιτεί ότι ο κόμβος που αιτείται ένα ασφαλές κλειδί έχει την εγκάρσια αίτηση από κόμβο σε κόμβο (hop-by-hop) μέχρι να προσεγγίσει την βάση σταθμό. Παρόλα αυτά η απάντηση από τον εμπιστευτικό server μπορεί να προσεγγίσει τους κόμβους όλους κατευθείαν.

Τα αποτελέσματα της εξομοίωσης επιβεβαιώνουν ότι η ανάπτυξη από πριν είναι πράγματι η πιο αποτελεσματική μέθοδος για την αυθεντικότητα δυο γειτονικών αισθητήριων κόμβων. Το πρωτόκολλο, παρόλα αυτά είναι πραγματικά ακατόρθωτο γιατί η ανάπτυξη τέτοιων δικτύων απαιτεί painstaking φροντίδα και ακρίβεια στην οποία πρέπει να διασφαλίσουμε ότι οι δυο αισθητήρες που μοιράζονται το προ-ορισμένο κλειδί κάνουν τελικά end-up όπως οι γειτονικοί (αισθητήρες) στο πεδίο. Για παράδειγμα, στην περίπτωση των αισθητήριων συσκευών που χρησιμοποιούνται σε ένα στρατιωτικό περιεχόμενο, θα ήταν περισσότερο βολικό να πεταχτούν οι συσκευές από μια αεροπορική πτήση πάνω από εχθρική περιοχή, και να αφήσει τους αισθητήριους κόμβους να οργανωθούν μέσα σε ένα μοιραζόμενο δίκτυο πληροφοριών όταν αυτές ακουμπήσουν το έδαφος.

Τα αποτελέσματα δεικνύουν ότι η αποτελεσματικότητα του SEKEN βρίσκεται μεταξύ εκείνης του Kerberos και των προ-αναπτυγμένων μηχανισμών κλειδιών. Αν και δεν υπάρχει τεράστια διαφορά μεταξύ της κατανάλωσης ενέργειας στο SEKEN και του Kerberos, η απαίτηση του Kerberos ότι ο server μοιράζεται ένα ρητώς κύριο κλειδί με κάθε αισθητήριο κόμβο είναι ένα σημαντικό μειονέκτημα για μεγάλα δίκτυα. Καμία τέτοια υπόθεση δεν έχει γίνει στο πρωτόκολλο SEKEN, στο οποίο όλα αυτά τα κλειδιά εγκαθίστανται κατά τη διάρκεια της εκτέλεσης του πρωτοκόλλου. Το SEKEN απαιτεί μόνο όλους τους δυνατούς κόμβους δικτύου να μοιράζονται ένα μυστικό μόνο μια φορά με τη βάση και να είναι από πριν προγραμματισμένα με το κοινό κλειδί της βάσης σταθμού.

Πρόσθετα, στο SEKEN, η βάση σταθμός επίσης προσδιορίζει έναν κόμβο ID σε όλους τους αισθητήριους κόμβους, αφού στην επιτυχία του Kerberos υποθέτουμε ότι υπάρχει ένας μηχανισμός για έναν αισθητήριο κόμβο να αποκτήσει ένα αξιόπιστο αντίγραφο του ID του κόμβου με το οποίο αυτός θέλει να δημιουργήσει ένα κλειδί ασφαλείας. Για αυτό παρόλη την επικοινωνία περισσοτέρων χρήσιμων πληροφοριών τα χαρακτηριστικά εμφάνισης του SEKEN περίπταντας μεταξύ ενός ιδανικού πρωτοκόλλου (προ-ανάπτυξη κλειδιών) και ενός σύγχρονου πρακτικού πρωτοκόλλου (Kerberos).

Ο πίνακας 6.9 δίνει την ενέργεια που καταναλώνεται όταν ένας αισθητήριος κόμβος προστίθεται μεταξύ δυο υπαρχόντων κόμβων οι οποίοι είναι ήδη ένα τμήμα του δικτύου. Η προανάπτυξη των κλειδιών καταναλώνει ένα σταθερό ποσό 0.2816mj. Παρόλα αυτά η κατανάλωση ενέργειας για το SEKEN και το Kerberos είναι μια λειτουργία της τοποθεσίας κόμβου στο δίκτυο. Άλλη μια φορά ξανά, το SEKEN

δείχνει υψηλά χαρακτηριστικά εμφάνισης από ότι το Kerberos. Η ανάλυση των υπολογιστικών κόστων δημιουργεί την βάση των συνεχόμενων εργασιών μας, ακόμη τα προκαταρκτικά αποτελέσματα επιβεβαιώνουν, παρόλο που προκαλείται μια κωδικοποίηση κοινού κλειδιού κατά τη διάρκεια του χρόνου ζωής του αισθητήριου κόμβου (κωδικοποίηση κοινού κλειδιού, που προκαλείται από τον αισθητήριο κόμβο μια φορά κατά τη διάρκεια του χρόνου ζωής του, απαιτεί περίπου 20 φορές λιγότερες λειτουργίες όταν συγκρίνεται με την αποκρινόμενη κωδικοποίηση με το ιδιωτικό κλειδί, που προκαλείται από τη βάση σταθμό) το SEKEN διατηρεί όλα του τα πλεονεκτήματα από όλα τα άλλα πρωτόκολλα, γιατί ο τοπικός υπολογισμός της πληροφορίας είναι περισσότερο αποτελεσματικός συγκρινόμενος με την μετάδοση radio, εξαιτίας των λόγων που προαναφέρθηκαν.

Οι πίνακες 6.8, 6.9 παρουσιάζουν τα αποτελέσματα εξομοίωσης που βγήκαν από ένα «ασφαλές εργαστηριακό» περιβάλλον. Σε ένα πραγματικό δίκτυο έχουμε να κάνουμε με ένα πλήθος χαμένων πηγών, πολλές από τις οποίες βρίσκονται τυχαία στη φύση. Για τις προσομοιώσεις μας, υποθέτουμε ότι δεν υπάρχουν απώλειες μηνυμάτων και γι' αυτό καμία αναμετάδοση. Αυτό μπορεί να μην είναι αληθές, ειδικότερα σε ασύρματα δίκτυα, όπου το κανάλι είναι πολύ ευαίσθητο σε απώλειες ζεύξης και σε άλλες πηγές παρέμβασης. Παρόλα αυτά, δικαιολογούμε ότι σε ένα πραγματικό δίκτυο το Kerberos και οι προ-αναπτυσσόμενοι μηχανισμοί κλειδιών μαζί, θα μπορούσαν να είναι υποκείμενοι στην ίδια διαβάθμιση δικτύου και τα χαρακτηριστικά τους θα υποφέρουν επίσης.

Η ασφάλεια, όπως θυμόμαστε, είναι μόνο μια βοηθητική λειτουργία για τους αισθητήριους κόμβους και για αυτό δεν θα έπρεπε να είναι φορτίο στα μέσα (πόρους) του συστήματος. Μια τυπική αλκαλική ΑΑ μπαταρία (MN 1500) με μια χωρητικότητα των 2.85 Ampere hours, λειτουργώντας των 15.39Kj. Ένα δίκτυο 200 κόμβων θα έχει ένα συνδυασμό wattage των 3.08MJ από τα οποία το SEKEN καταναλώνει μόνο 1,106 για εγκατάσταση κλειδιού. Αυτό είναι ενθαρρυντικό και προτείνει ότι το τελικό κόστος επιτυχίας στην ασφάλεια μπορεί να μένει δεσμευμένο μέσω αποτελεσματικών πρωτοκόλλων.

Nodes	Pre-deployed Keys	SEKEN	Kerberos
50	6.899 mJ	78.15 mJ	81.84 mJ
100	14.08 mJ	288.55 mJ	296.0 mJ
150	20.98 mJ	630.95 mJ	642.16 mJ
200	28.16 mJ	1.105 J	1.120 J

Πίνακας 6.8 Κατανάλωση ενέργειας για μεγαλύτερα δίκτυα αισθητήρων **(11)**

Distance from gateway	SEKEN	Kerberos
50	5.566 mJ	5.720 mJ
100	10.84 mJ	11.00 mJ
150	16.12 mJ	16.28 mJ
200	21.40 mJ	21.56 mJ

Πίνακας6.9 Κατανάλωση ενέργειας για πρόσθεση μέλους. **(11)**

6.11 Συμπεράσματα

Το πρωτόκολλο SEKEN παρέχει ασφαλή επικοινωνία με αποτελεσματική ισχύ για ένα δίκτυο ασύρματων αισθητηρίων, με τη μείωση της σαφούς ανταλλαγής μηνυμάτων πάνω από το ασύρματο μέσο και υποκαταστώντας τις προστιθέμενες τοπικές processing στον κόμβο host. Το πρωτόκολλο επιτρέπει αυτό-διαμορφωμένες λειτουργίες σε ένα αυτόνομο δίκτυο με ελάχιστη παρεμβολή χρήστη η οποία είναι ιδανική για ένα ασύρματο δίκτυο αισθητήρων με υψηλό ρίσκο με τοπολογία αλλαγών. Το πρωτόκολλο καθιστά ικανό κάθε αισθητήριο κόμβο για να μοιράσει δυο τύπους κλειδιών:

I. Ένα κύριο κλειδί που μοιράζεται με τη βάση σταθμό για εμπιστευτική ανταλλαγή μηνυμάτων.

II. Ένα σαφές κλειδί μεταξύ γειτονικών κόμβων, επιτρέποντας ασφαλή ανταλλαγή πληροφοριών.

Εξαρτώμενοι από το επίπεδο της απαιτούμενης ασφάλειας, ικανοί μηχανισμοί μπορούν να τοποθετηθούν επίσης σε μέρη που, περιοδικά, θα ανανεώνουν τα κλειδιά αυτά ,προκειμένου να τα προφυλάξουν από βίαιες και δυναμικές επιθέσεις.

6.12ΠΡΩΤΟΚΟΛΛΟ INSENS

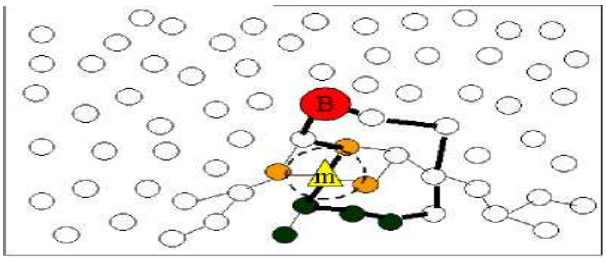
6.12.1Εισαγωγή

Οι εφαρμογές ασυρμάτων δικτύων αισθητήρων (WSNs) είναι πολυάριθμες και αυξανόμενες, και κυμαίνονται στο σπίτι και το γραφείο ως τις φυσικές, στρατιωτικές και ενσωματωμένες τοποθετήσεις. Για τις στρατιωτικές τοποθετήσεις, η διασπορά των ασυρμάτων δικτύων αισθητήρων WSNs στο έδαφος ενός αντιπάλου επιτρέπει την ανίχνευση και την καταδίωξη των εχθρικών στρατιωτών και των οχημάτων. Για το σπίτι το γραφείο, και τα περιβάλλοντα, τα δίκτυα αισθητήρων προσφέρουν τη δυνατότητα να ελεγχθεί η υγεία των ηλικιωμένων και να ανιχνευθούν οι εισβολείς μέσω ενός ασύρματου συστήματος εγχώριας ασφάλειας.Σε κάθε ένα από αυτά τα σενάρια, οι ζωές μπορούν να εξαρτηθούν από την επικαιρότητα και την ακρίβεια των στοιχείων αισθητήρων που λαμβάνονται από τους διασκορπισμένους κόμβους αισθητήρων. Κατά συνέπεια, τέτοιο ασύρματο δίκτυο αισθητήρων πρέπει να εξασφαλιστεί για να αποτρέψει έναν εισβολέα από την παρεμπόδιση της παράδοσης των σωστών στοιχείων αισθητήρων και από τα πλαστά στοιχεία αισθητήρων . Για την αντιμετώπιση αυτών των ζητημάτων, παρουσιάζεται παρακάτω ένα ασφαλές σύστημα δρομολόγησης που είναι ελαστικό στις προσπάθειες να εμποδιστεί η παράδοση στοιχείων, και με αυτές τις ενέργειες επίσης αναπτύσσει δίπλα δίπλα σύνολο ελέγχων ακεραιότητας στοιχείων και τα σχέδια επικύρωσης που μπορούν να χρησιμοποιηθούν για να ανιχνεύσουν διαφθορές με τα στοιχεία αισθητήρων.

Ο σχεδιασμός και η εφαρμογή της ασφαλούς δρομολόγησης σε WSNs πρέπει ταυτόχρονα να εξετάσουν τρεις δύσκολες ερευνητικές προκλήσεις.

Κατ' αρχάς, η ασύρματη επικοινωνία μεταξύ των κόμβων αισθητήρων αυξάνει την ευπάθεια του δικτύου για να υποκλέψει, τις αναρμόδιες επιθέσεις πρόσβασης, υποκρισίας, επανάληψης και άρνηση των υπηρεσιών (DOS).

Δεύτερον, οι ίδιοι οι κόμβοι αισθητήρων περιορίζονται ως προς τις πηγές τους, ιδιαίτερα από την άποψη της περιορισμένης μνήμης, της CPU , του εύρους ζώνης επικοινωνίας, και ειδικά της ζωής μπαταριών



Σχήμα 6.10 Τοπολογία ασσύμετρων δειγμάτων ασύρματων δικτύων αισθητήρων που δρομολογημένα στο σταθμό βάσεων. Ο κόμβος τριγώνων είναι ένας κακόβουλος κόμβος. Οι μαύροι κόμβοι είναι οι προς τα κάτω κόμβοι του. Η παρείσφρυση-ανεκτική δρομολόγηση βοηθιέται από τις πολλαπλάσιες πορείες. Οι προς τα κάτω κόμβοι μπορούν ακόμα να επικοινωνήσουν με το σταθμό βάσεων. **(14)**

Αυτοί οι περιορισμοί των πόρων περιορίζουν το βαθμό κρυπτογράφησης, αποκρυπτογράφησης, και αυθεντικότητας που μπορεί να εφαρμοστεί στους μεμονωμένους κόμβους αισθητήρων.

Τρίτον, τα ασύρματα δίκτυα αισθητήρων αντιμετωπίζουν τον προστιθέμενο φυσικό κίνδυνο ασφάλειας ανάπτυξης στον τομέα, έτσι ώστε οι μεμονωμένοι κόμβοι αισθητήρων να μπορούν να ληφθούν και να υπάγονται στις επιθέσεις από έναν ενδεχομένως εξοπλισμένο καλά εισβολέα προκειμένου για να συμβιβάσουν έναν ενιαίο ΄΄φτωχό΄΄ κόμβο.

Μετά από μια επιτυχή επίθεση, ένας συμβιβασμένος κόμβος αισθητήρων θα μπορούσε έπειτα να χρησιμοποιηθεί για να υποκινήσει τέτοιους κακόβουλους δεσμούς όπως διαφημίζοντας ψεύτικες πληροφορίες δρομολόγησης , ενδεχομένως εν αγνοία του δίκτυου αισθητήρων, και τις επιθέσεις DOS προώθησης από μέσα από το δίκτυο αισθητήρων.

Λαμβάνοντας υπόψη αυτές τις απειλές και τους περιορισμούς των πόρων, η προσέγγισή μας για την εξασφάλιση ασύρμάτων δικτύων αισθητήρων παραδέχεται ότι ένας εξοπλισμένος καλά εισβολέας μπορεί να συμβιβάσει τους μεμονωμένους κόμβους αισθητήρων, αλλά ότι το γενικό σχέδιο του ασφαλούς συστήματος δρομολόγησής μας πρέπει να ανεχτεί αυτές τις παρεισφρύσεις έτσι ώστε το δίκτυο συνολικά να παραμένει σε λειτουργία

Υποθέτουμε ότι ο σταθμός βάσεων έχει αρκετά περισσότερους πόρους για να υπερασπιστεί ενάντια στις επιθέσεις, και επομένως να επικεντρωθεί στην εξασφάλιση του συστήματος ενάντια στις επιθέσεις στις πιό αδύνατες συνδέσεις, δηλαδή στους ΄΄φτωχούς΄΄ κόμβους αισθητήρων.

Έχουμε σχεδιάσει και έχουμε εφαρμόσει ένα ανεκτικό στην εισβολή πρωτόκολλο δρομολόγησης για ασύρματο δίκτυο αισθητήρων (INSENS) που έχει γνωρίζει ότι ένας ενιαίος συμβιβασμένος κόμβος μπορεί μόνο να αναστατώσει μια εντοπισμένη μερίδα του δικτύου, και δεν μπορεί να ρίξει το ολόκληρο δίκτυο αισθητήρων.

Το ασφαλές σύστημα δρομολόγησης INSENS εμμένει στις ακόλουθες αρχές σχεδίου. Κατ' αρχάς, για να αποτρέψουν τις τρέχουσες επιθέσεις DOS, οι μεμονωμένοι κόμβοι δεν επιτρέπονται για να μεταδώσουν σε ολόκληρο δίκτυο. Μόνο ο σταθμός βάσεων που παρουσιάζεται στο σχήμα 1 επιτρέπεται για να μεταδώσει. Ο σταθμός βάσεων ενεργεί ως πύλη στο συνδεμένο με καλώδιο κόσμο, π.χ. δορυφορικό uplink που συνδέει με τα επίγεια δίκτυα. Ο σταθμός βάσεων είναι αόριστα αυθεντικός μέσω ενός μονόδρομου αριθμού ακολουθίας, έτσι ώστε οι μεμονωμένοι κόμβοι να μην μπορούν να εξαπατήσουν αυθαίρετα την βάση σταθμό και με αυτόν τον τρόπο να γεμίσουν το δίκτυο.

Οι κόμβοι αισθητήρων είναι περιορισμένοι μόνο σε ένα πακέτο, και έπειτα μόνο στο σταθμό βάσεων, με αυτόν τον τρόπο αποτρέποντας τις επιθέσεις μετάδοσης DOS/DDOS.

Η peer-to-peer επικοινωνία αισθητήρων δεν υποστηρίζεται άμεσα, παρόλο που το άνοιγμα μέσω των σταθμών βάσεων επιτρέπει στην άμεση επικοινωνία αισθητήρα με αισθητήρα.

Δεύτερον, για να αποτρέψουν τη διαφήμιση των ψεύτικων στοιχείων δρομολόγησης, οι πληροφορίες δρομολόγησης ελέγχου πρέπει να αυθεντικοποιηθούν. Μια βασική συνέπεια αυτής της προσέγγισης είναι ότι ο σταθμός βάσεων λαμβάνει πάντα τη γνώση της τοπολογίας που είναι σωστή, αν και μπορεί μόνο να αντιπροσωπεύσει μια μερική εικόνα λόγω της κακόβουλης μείωσης πακέτων.

Τρίτον, για να εξετάσει τους περιορισμούς των πόρων.Αυτοί είναι:

1) το συμμετρικό βασικό σύστημα κρυπτογραφία επιλέγεται για την εμπιστευτικότητα και την επικύρωση μεταξύ του σταθμού βάσεων και κάθε πόρος-περιορισμένου κόμβου αισθητήρων, δεδομένου ότι είναι αρκετά λιγότερο υπολογίσιμο από το δημόσιο βασικό σύστημα κρυπτογραφίας, και

2) ο πλούσιος σε πηγές σταθμός βάσεων επιλέγεται ως κεντρικό σημείο για τον υπολογισμό και τη διάδοση των πινάκων δρομολόγησης.

Τέταρτο, για να εξετάσει την έννοια των συμβιβασμένων κόμβων, η πλεονάζουσα δρομολόγηση πολλαπλών διαδρομών κατασκευάζεται σε INSENS για να

επιτύχει την ασφαλή δρομολόγηση, όπως φαίνεται στο σχήμα 6.10. Ο στόχος είναι ότι πρέπει να χωρίσει τις πορείες έτσι ώστε ακόμα κι αν ένας εισβολέας καταλάβει έναν απλό κόμβο ή μια πορεία, οι δευτεροβάθμιες πορείες θα υπάρξουν για να διαβιβάσουν το πακέτο στο σωστό προορισμό.

6.12.2 Περιγραφή πρωτοκόλλου

Το INSENS αποτελείται από μια φάση ανακαλύψεων διαδρομών και μια φάση προώθησης πληροφοριών. Η φάση ανακαλύψεων διαδρομών εξακριβώνει την τοπολογία του δικτύου αισθητήρων και χτίζει τους κατάλληλους πίνακες αποστολής στους διάφορους κόμβους. Η ανακάλυψη διαδρομών υποδιαιρείται σε τρεις κύκλους.

I. Στον πρώτο κύκλο, η βάση σταθμός εισρέει (περιορισμένη εισροή) ένα *μήνυμα αιτήματος* σε όλους τους εφικτούς κόμβους αισθητήρων στο δίκτυο.

II. Στο δεύτερο κύκλο, κάθε κόμβος αισθητήρων στέλνει τις πληροφορίες τοπολογίας γειτονικών του πίσω στο σταθμό βάσεων χρησιμοποιώντας ένα *μήνυμα ανατροφοδότησης*.

III. Στον τρίτο κύκλο, ο σταθμός βάσεων αυθεντικοποιεί τις πληροφορίες τις γειτονικές, κατασκευάζει μια τοπολογική εικόνα του δικτύου, υπολογίζει τους πίνακες αποστολής για κάθε κόμβο αισθητήρων, και στέλνει τους πίνακες στους αντίστοιχους κόμβους χρησιμοποιώντας ένα *μήνυμα αναπροσαρμογών δρομολόγησης*. Το στοιχείο που διαβιβάζει τη φάση επιτρέπει την αποστολή των στοιχείων από κάθε κόμβο αισθητήρων στο σταθμό βάσεων, και αντίστροφα. Ένα συμμετρικό κανάλι επικοινωνίας υποτίθεται, δηλ. εάν ο κόμβος *α* μπορεί να ακούσει ένα μήνυμα από τον κόμβο *β,* κατόπιν ο *α* μπορεί να στείλει ένα μήνυμα *στο β.*

Κάθε κόμβος έχει ένα κοινό συμμετρικό κλειδί με το σταθμό βάσεων. Κάθε κόμβος κατέχει επίσης μια συνολικά γνωστή μονόδρομη λειτουργία F και τον αρχικό αριθμό ακολουθίας K_0. *Το F* και K_0 χρησιμοποιούνται μαζί για να επικυρώσουν αόριστα τα μηνύματα από το σταθμό βάσεων, όπως εξηγείται έπειτα. Και τα τρία κομμάτια των πληροφοριών, δηλαδή *F,* K_0 και το κοινό συμμετρικό κλειδί, διανέμονται εκ των προτέρων, δηλ. προγραμματίζονται εκ των πρότερων σε κάθε κόμβο αισθητήρων πριν από την επέκταση.

Προβλέπουμε ότι οι στρατιωτικές εφαρμογές θα επιτρέψουν παραδείγματος χάριν στα μυστικά κλειδιά για να προγραμματιστούν εκ των πρότερων στους κόμβους αισθητήρων πριν από την επέκταση.

6.12.3 Ανακάλυψη διαδρομών: Αίτημα διαδρομών

Ο σταθμός βάσεων αρχίζει τον πρώτο κύκλο όποτε πρέπει να κατασκευάσει τους πίνακες αποστολής όλων των κόμβων αισθητήρων. Ο σταθμός βάσεων μεταδίδει ένα *μήνυμα αιτήματος* που παραλαμβάνεται από όλους τους γειτονικούς του. Μια μετάδοση μηνυμάτων αιτήματος από έναν κόμβο *X* περιλαμβάνει μια πορεία από το σταθμό βάσεων *στο X*. Όταν ένας κόμβος λάβει ένα μήνυμα αιτήματος για πρώτη φορά, διαβιβάζει (μεταδόσεις) αυτό το μήνυμα μετά από την επισύναψη της ταυτότητάς του στο μονοπάτι. Καταγράφει επίσης την ταυτότητα του αποστολέα αυτού του μηνύματος στο σύνολο γειτόνων του. Όταν ένας κόμβος λαμβάνει ένα διπλό μήνυμα αιτήματος, η ταυτότητα του αποστολέα προστίθεται στο σύνολο γειτόνων της, αλλά το αίτημα δεν είναι επαναμετάδοση.

Ένας κακόβουλος κόμβος στο δίκτυο μπορεί να προσπαθήσει να προωθήσει διάφορες επιθέσεις σε αυτόν τον κύκλο. Κατ' αρχάς, μπορεί να προσπαθήσει στον υποκριτικό σταθμό βάσεων με την αποστολή ενός πλαστού μηνύματος αιτήματος. Δεύτερον, μπορεί να περιλάβει μια πλαστή πορεία στο μήνυμα αιτήματος που προωθεί. Τρίτον, μπορεί να μην διαβιβάσει ένα μήνυμα αιτήματος, ή να προωθήσει μια DOS επίθεση με επανειλημμένες αιτήσεις διάφόρων μηνυμάτων.

Χρησιμοποιούμε δύο μηχανισμούς για να αντιμετωπίσουμε αυτές τις επιθέσεις. Και οι δύο μηχανισμοί απαιτούν τους κόμβους αισθητήρων για να προ-διαμορφωθούν με τις κατάλληλες τιμές.

Κατ' αρχάς, ο σταθμός βάσεων χρησιμοποιεί μια μονόδρομη κρυπτογραφική hash λειτουργία *F* στη δημιουργία μιας ακολουθίας αριθμών K_0*., K1... ,Kn,* έτσι ώστε *Ki = F(Ki + 1),* όπου $0 \le i \le n$. Αρχικά, κάθε κόμβος ξέρει *το F* και K_0. Στην πρώτη φάση ανακαλύψεων διαδρομών, ο σταθμός βάσεων περιλαμβάνει *K1* στο μήνυμα αιτήματος που μεταδίδει .

Γενικά , ο σταθμός βάσεων χρησιμοποιεί *Ki* στην i^{th} φάση ανακαλύψεων διαδρομών. Κάθε κόμβος μπορεί να ελέγξει ότι ο αριθμός ακολουθίας πράγματι προήλθε από το σταθμό βάσεων με τον υπολογισμό *Ki = F(Ki + 1).* Ένας επιτιθέμενος που συμβίβασε έναν κόμβο αισθητήρων θα ήταν ανίκανος να υποθέσει

τον επόμενο μονόδρομο αριθμό ακολουθίας δεδομένου του πιό πρόσφατου αριθμού ακολουθίας, δηλ. λαμβάνοντας υπόψη *το F,* K_0 , και την πιό πρόσφατη ακολουθία *Ki,* στο tacker δεν μπορεί να αναστρέψει *το F,* για να παραγάγει τον επόμενο αριθμό ακολουθίας Ki+1. Κατά συνέπεια, ένας συμβιβασμένος κόμβος δεν μπορεί να εξαπατήσει την βάση σταθμό με την παραγωγή των νέων αριθμών ακολουθίας. Παρόλ'αυτά, ένας συμβιβασμένος κόμβος θα μπορούσε να επαναλάβει την τρέχουσα ακολουθία αριθμών σε ένα μήνυμα αιτήματος στους προς τα κάτω κόμβους του, οι οποίοι έπειτα θα θεωρούσαν ότι ο συμβιβασμένος κόμβος είναι ο σταθμός βάσεων. Η ζημια είναι σε αυτήν την περίπτωση εντοπισμένη στο συμβιβασμένο κόμβο, ο οποίος ήταν ο στόχος σχεδίου μας. Το υπόλοιπο του δικτύου θα λάβει το αίτημα διαδρομών του αυθεντικού σταθμού βάσεων πρώτα, και επομένως θα αγνοήσει το συμβιβασμένο αίτημα διαδρομών του κόμβου. Η χρήση μονόδρομων δυνάμεων μας λειτουργεί ως μέθοδος που υιοθετείται από το πρωτόκολλο μTESLA , αλλά διαφέρει υπό την έννοια ότι οι αριθμοί στη μονόδρομη αλυσίδα είναι αριθμοί ακολουθίας παρά τα συμμετρικά κλειδιά.

Ο δεύτερος μηχανισμός που χρησιμοποιούμε είναι ένας κλειδωμένος αλγόριθμος του MAC. Κάθε κόμβος αισθητήρων διαμορφώνεται με ένα χωριστό μυστικό κλειδί που μοιράζεται μόνο με το σταθμό βάσεων. Όταν ένας κόμβος *X* λαμβάνει ένα μήνυμα αιτήματος για πρώτη φορά, επισυνάπτει την ταυτότητά του στον κατάλογο πορειών, και παράγει έπειτα τη MAC του νέου πλήρους μονοπατιού με το κλειδί του.

Αυτή η MAC επισυνάπτεται επίσης στο μήνυμα αιτήματος, προτού να διαβιβαστεί προς τα κάτω το τροποποιημένο μήνυμα αιτήματος. Αυτή η MAC θα χρησιμοποιηθεί τελικά από το σταθμό βάσεων για να ελέγξει την ακεραιότητα της πορείας που περιλαμβάνεται στο πακέτο. Επίσης, όταν συμβιβάζεται ένας κόμβος, μόνο ένα μυστικό κλειδί αποκαλύπτεται, έτσι ένας επιτιθέμενος δεν μπορεί να συμβιβάσει ολόκληρο το δίκτυο.

Η γενική επίδραση αυτών των μηχανισμών ασφάλειας είναι ότι ένας κακόβουλος κόμβος μπορεί να επιτεθεί στον πρώτο κύκλο μόνο με την εντοπισμένη εισροή, με την μη αποστολή ενός μηνύματος αιτήματος, και με την αποστολή της πλαστής πορείας στο αίτημα που είναι έπειτα ανιχνευμένος στο δεύτερο κύκλο. Οι τελευταίες δύο επιθέσεις θα οδηγήσουν σε μερικούς από τους κόμβους προς τα κάτω από τον κακόβουλο κόμβο που δεν λαμβάνει ένα μήνυμα αιτήματος ή που δεν είναι σε θέση να

διαβιβάσουν το μήνυμα ανατροφοδότησής τους στο σταθμό βάσεων στο δεύτερο κύκλο.

6.12.4 Ανακάλυψη διαδρομών: Ανατροφοδότηση διαδρομών

Στο δεύτερο κύκλο, κάθε κόμβος αισθητήρων στέλνει τις τοπικές πληροφορίες συνδετικότητάς του (ένα σύνολο ταυτοτήτων των κόμβων γειτόνων του καθώς επίσης και της πορείας σε αυτό από το σταθμό βάσεων) πίσω στο σταθμό βάσεων χρησιμοποιώντας ένα *μήνυμα ανατροφοδότησης*. Αφότου έχει διαβιβάσει ένας κόμβος *X* το μήνυμα αιτήματός του , περιμένει ένα ορισμένο διάστημα διαλείμματος πρίν παράγει ένα μήνυμα ανατροφοδότησης. Κατά τη διάρκεια του διαστήματος αυτής της περιόδου, ακούει τις τοπικές μεταδόσεις από τους γειτονικούς κόμβους διαβιβάζοντας το ίδιο μήνυμα αιτήματος, και αποθηκεύει την ταυτότητα του γείτονα και τη MAC του γείτονα που ενσωματώνονται μέσα στο μήνυμα αιτήματος. Μετά από το διάλειμμα, ο κόμβος αισθητήρων θα στείλει τον κατάλογο γειτόνων του (προς τα πάνω, και προς τα κάτω) πίσω στο σταθμό βάσεων, όπου κάθε γείτονας προσδιορίζεται από την ταυτότητα του γείτονα και τη MAC του γείτονα. Ο κόμβος αισθητήρων εφαρμόζει την κλειδωμένη MAC του στα στοιχεία τοπολογίας, δηλ. ο κατάλογος γειτόνων, για να προστατεύσει περαιτέρω την ακεραιότητα του μηνύματος ανατροφοδότησης. Τα μηνύματα που φθάνουν στο σταθμό βάσεων είναι εγγυημένα μετά από την επαλήθευση για να είναι σωστά και ασφαλή από την διαφθορά

Η δρομολόγηση του *μηνύματος ανατροφοδότησης* από έναν κόμβο *X* στο σταθμό βάσεων ακολουθεί την αντίστροφη πορεία που λαμβάνεται από το μήνυμα αιτήματος που άρχισε την απάντηση ανατροφοδότησης. Για να εξασφαλίσει ότι οι κακόβουλοι κόμβοι δεν παράγουν τις ψεύτικες πορείες διαβιβάζοντας ένα μήνυμα ανατροφοδότησης, ένας κόμβος τοποθετεί τις πληροφορίες προσδιορισμού γονέων του μαζί με τη MAC του γονέα του, την οποία έλαβε στο πρώτο μήνυμα αιτήματος. Κάθε κόμβος θα επιλέξει ότι το ένα νομιμοποιεί τον προς τα πάνω γονέα, διαμορφώνοντας μια γονική αλυσίδα των κόμβων πίσω στο σταθμό βάσεων. Ένας συμβιβασμένος κόμβος θα είναι σε θέση το πολύ-πολύ να μην πλημμυρίσει κάθε έναν από τις αλυσίδες των γονέων του πίσω στους σταθμούς βάσεων, αλλά κανέναν άλλο κόμβο. Αυτό εντοπίζει την επίδραση μιας επίθεσης.

Για να περιορίσει περαιτέρω τις επιθέσεις, ο έλεγχος ποσοστού εφαρμόζεται σε κάθε κόμβο ανεξάρτητα από το εισερχόμενο ποσοστό κυκλοφορίας, το εξερχόμενο ποσοστό κυκλοφορίας κάθε κόμβου είναι περιορισμένο σε κάποιο μέγιστο ποσοστό,

με αυτόν τον τρόπο αποτρέποντας την πλημμύρα. Επίσης, κάθε κόμβος κρυπτογραφεί τις σωστές πληροφορίες στο μήνυμα ανατροφοδότησης που στέλνει για να παρέχει την εμπιστευτικότητα ενάντιον της υποκλοπής από έναν κακόβουλο κόμβο.

Η γενική επίδραση αυτών των μηχανισμών ασφάλειας είναι ότι ένας κακόβουλος κόμβος είναι περιορισμένος στη ζημία που μπορεί να επιβάλει, είτε επιτιθειμένος από την επίθεση DOS, με την μη αποστολή ενός *μηνύματος ανατροφοδότησης* είτε με την τροποποίηση των πληροφοριών γειτονιάς των κόμβων, οι οποίες μπορούν να ανιχνευθούν στο σταθμό βάσεων. Αυτές οι επιθέσεις θα οδηγήσουν σε μερικούς από τους κόμβους προς τα κάτω από τον κακόβουλο κόμβο που δεν είναι σε θέση να παρέχουν τις σωστές πληροφορίες συνδεσιμότητας τους στο σταθμό βάσεως. Αν και ένας κακόβουλος κόμβος θα μπορούσε να προωθήσει μια επίθεση μπαταρία-αγωγών με διαρκώς αποστολή πλαστών μηνυμάτων ανατροφοδότησης στο ποσοστό-ελεγχόμενο όριο, μια τέτοια επίθεση θα είχε επιπτώσεις ακόμα μόνο σε έναν περιορισμένο αριθμό προς τα πάνω κόμβων.

6.12.5Ανακάλυψη διαδρομών: Υπολογισμός και διάδοση των πολλαπλών διαδρομών πινάκων δρομολόγησης

Μετά την αποστολή του αιτουμένου μηνύματος του στον πρώτο κύκλο, ο σταθμός βάσης περιμένει μια ορισμένη χρονική περίοδο να συλλέξει όλες τις πληροφορίες συνδετικότητας που παραλαμβάνονται μέσω *των μηνυμάτων ανατροφοδότησης.* Κάθε κόμβος επιστρέφει έναν επικυρωμένο κατάλογο γειτονικών κόμβων του. Κατά συνέπεια, ο σταθμός βάσεων είναι σε θέση να επαληθεύσει τις πληροφορίες γειτόνων και να ανιχνεύσει διαφθορά μηνυμάτων ανατροφοδότησης. Ο σταθμός βάσης κατασκευάζει μια τοπολογία του δικτύου από αυτά τα επικυρωμένα μηνύματα ανατροφοδότησης, αν και αυτή η εικόνα του δικτύου μπορεί να οφείλεται ελλιπώς στα πεταγμένα μηνύματα ανατροφοδότησης. Από αυτές τις πληροφορίες συνδετικότητας, ο σταθμός βάσης υπολογίζει τους πίνακες αποστολής κάθε κόμβου στο δίκτυο.

Το INSENS ενσωματώνει τον πλεονασμό στη δρομολόγηση με την δημιουργία των πολλαπλάσιων περιττών μονοπατιών για να παρακάμψει τους εισβολείς καθοδηγώντας τα μηνύματα, όπως φαίνεται στο σχήμα 1. Αυτά τα μονοπάτια είναι ανεξάρτητα το ένα από το άλλο υπό την έννοια που μοιράζονται ως κοινοί κόμβοι/συνδέσεις , μόνο η πηγή και οι κόμβοι προορισμού μοιράζονται μεταξύ των μονοπατιών. Η παρουσία ενός ή περισσότερων εισβολέων κατά μήκος μερικών από

αυτά τα μονοπάτια μπορεί να διακινδυνεύσει την παράδοση μερικών από τα αντίγραφα ενός μηνύματος. Παρόλ'αυτά, εφ' όσον υπάρχει τουλάχιστον μια πορεία που δεν επηρεάζεται από έναν εισβολέα, ο προορισμός θα λάβει τουλάχιστον ένα αντίγραφο του μηνύματος που δεν έχει πειραχτεί.

Ενώ το INSENS είναι κατά ένα μεγάλο μέρος αγνωστικιστικό στα ιδιαίτερα κριτήρια για την επιλογή πολλαπλών μονοπατιών, επιλέξαμε ακόλουθο πολλαπλών διαδρομών τ προκειμένου να συνεχίσουμε με την εφαρμογή INSENS μας. Για έναν κόμβο *A* αισθητήρων, η πρώτη πορεία από *το A* στο σταθμό βάσεων επιλέγεται χρησιμοποιώντας τον πιό σύντομο αλγόριθμο πορειών Dijkstra. Για να καθορίσουν τη δεύτερη πορεία, τρία σύνολα κόμβων, S1, *S2,* και S3 κατασκευάζονται αρχικά. Το *S1* είναι το σύνολο κόμβων που ανήκουν στην πρώτη πορεία, το *S2* είναι το σύνολο κόμβων που ανήκουν στο *S1* και οποιωνδήποτε κόμβων γειτόνων των κόμβων *S1* και S3 είναι το σύνολο που ανήκει στους κόμβους S2 και οποιουςδήποτε κόμβους γειτονικών των κόμβων S2. Και τα τρία σύνολα αποκλείουν *το A* ή το σταθμό βάσεων. Η δεύτερη πορεία υπολογίζεται έπειτα ως εξής:

Αφαιρούμε όλους τους κόμβους S3 από το δίκτυο, και βρίσκουμε το μικρότερομονοπάτι*Α*στοσταθμόβάσεων.

Εάν ένα τέτοιο μονοπάτι βρεθεί, ολοκληρώνουμε τον υπολογισμό. Το μονοπάτι που βρέθηκε είναι το δεύτερο μονοπάτι

Διαφορετικά, αφαιρούμε όλους τους κόμβους S2 από το αρχικό δίκτυο. Βρίσκουμετο μικρότερο μονοπάτι από *το A* στο σταθμό βάσεων. Εάν ένα τέτοιο μονοπάτι βρεθεί,, ολοκληρώνουμε τον υπολογισμό. Το μονοπάτι που βρέθηκε είναι τοδεύτερομονοπάτι.

Αφαιρούμε όλους τους κόμβους S1 από το αρχικό δίκτυο. Βρίσκουμε το μικρότερο μονοπάτι από *το A* στο σταθμό βάσεων. Εάν ένα τέτοιο μονοπάτι βρεθεί,,είναιτοδεύτερομονοπάτι. Διαφορετικά, δεν υπάρχει κανένα δεύτερο μονοπάτιαπό*το*Α*σ*τοσταθμόβάσης.

Σημειώνουμε ότι ανάλογα με την τοπολογία δικτύων, είναι πιθανόν ότι καμία δεύτερη πορεία δεν βρίσκεται. Σε εκείνη την περίπτωση, η τρέχουσα εφαρμογή INSENS διατηρεί μόνο ένα ενιαίο μονοπάτι. Η εύρεση ενός καλύτερου αλγορίθμου για να υπολογίσει τα πολλαπλάσια μονομάτια σε INSENS είναι μέρος της μελλοντικής εργασίας μας.

Μετά από τον υπολογισμό των περιττών μονοπατιών για κάθε κόμβο η βάση σταθμόςυπολογίζει τους πίνακες προώθησης κάθε κόμβου. Αυτοί που διαβιβάζουν τους

πίνακες διαδίδονται στους αντίστοιχους κόμβους με έναν τρόπο εύρους. Ο σταθμός βάσεων στέλνει αρχικά τους πίνακες αποστολής όλων των κόμβων που είναι οι άμεσοι γείτονές του. Στέλνει έπειτα τους πίνακες αποστολής των κόμβων που είναι σε μια απόσταση δύο hop από αυτον, και τα λοιπά. Αυτός ο μηχανισμός χρησιμοποιεί έξυπνα τον περιττό μηχανισμό δρομολόγησης που φτιάχτηκε ακριβώς για να διανείμει τους πίνακες αποστολής. Οι τυποποιημένες τεχνικές ασφάλειας μπορούν να χρησιμοποιηθούν για να συντηρήσουν την αυθεντικότητα, την ακεραιότητα, και την εμπιστευτικότητα των πινάκων αποστολής.

6.12.6Αποστολή στοιχείων

Ένας κόμβος διατηρεί έναν πίνακα αποστολής που έχει διάφορες καταχωρήσεις, μια για κάθε διαδρομή στην οποία ο κόμβος ανήκει. Κάθε είσοδος είναι ένα τρίπτυχο: *προορισμός, πηγή, άμεσος αποστολέας. Ο προορισμός* είναι η ταυτότητα κόμβων του κόμβου προορισμού στον οποίο ένα πακέτο στοιχείων στέλνεται, *η πηγή* είναι η ταυτότητα κόμβων του κόμβου που δημιούργησε αυτό το πακέτο στοιχείων, και *ο άμεσος αποστολέας* είναι η ταυτότητα κόμβων του κόμβου που διαβίβασε ακριβώς αυτό το πακέτο. Παραδείγματος χάριν, λαμβάνοντας υπόψη μια διαδρομή από τον κόμβο StoD: $S \to a \to b \to c \to D$ ο πίνακας αποστολής του κόμβου α περιέχει μια είσοδο < D,S,S>, η αποστολή του πίνακα του β περιέχει μια είσοδο <D,S,a >, και ο πίνακας αποστολής του c περιέχει μια είσοδο < D,S,b>. Με την αποστολή των πινάκων που κατασκευάζονται κατ' αυτό τον τρόπο, η αποστολή των πακέτων στοιχείων είναι αρκετά απλή. Στη λήψη ενός πακέτου στοιχείων, ένας κόμβος ψάχνει για μια είσοδο που ταιριάζει < *έναν προορισμό, πηγή, άμεσος αποστολέας* > στον πίνακα αποστολής του. Εάν βρίσκει μια αντιστοιχία, διαβιβάζει (μεταδίδει) το πακέτο στοιχείων.

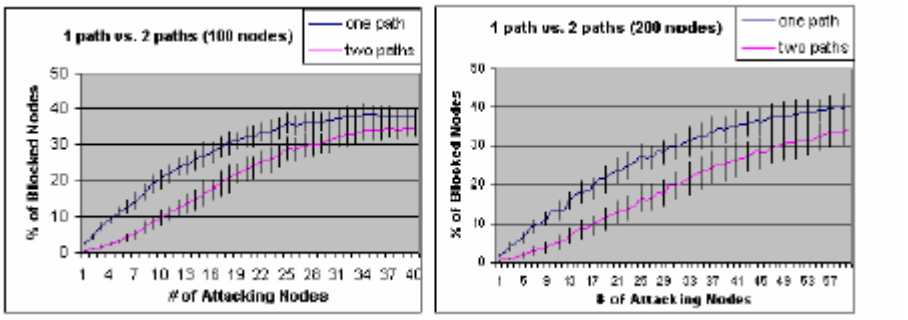
6.12.7Η κακόβουλη επίθεση κατά τη διάρκεια προώθησης πληροφοριών

Το INSENS δημιουργεί δύο μονοπάτια για να παρακάμψει τους κακόβουλους κόμβους. Με δύο ανεξάρτητες διαδρομές διαθέσιμες μεταξύ κάθε κόμβου και του σταθμού βάσεων, ο στόχος του πρωτοκόλλου μας είναι να καθοδηγηθούν τα μηνύματα σωστά παρουσία ενός ενιαίου κακόβουλου κόμβου. Κατά τρόπο ενδιαφέροντα, το πρωτόκολλό μας ασχολείται αρκετά καλά με τους πολλαπλάσιους κακόβουλους κόμβους . Έχουμε εκτελέσει ένα σύνολο πειραμάτων για να μετρήσουμε τον αριθμό κόμβων

που μπορεί να εμποδιστηκε όταν ένα σύνολο πολλαπλάσιων κόμβων γίνεται κακόβουλο και πετάει τα πακέτα στοιχείων.

Το σχήμα 6.11 παρουσιάζει μέσο αριθμό κόμβων που μπορεί να εμποδιστεί ως λειτουργία του αριθμού κακόβουλων κόμβων. Για τη σύγκριση, έχουμε υπολογίσει επίσης αυτόν τον αριθμό όταν χρησιμοποιείται αντ' αυτού ένας αλγόριθμος δρομολόγησης ενιαίος-πορειών.

Αυτά τα αποτελέσματα είναι βασισμένα σε ένα δίκτυο 200 κόμβων που κατανέμονται τυχαία ένα διάστημα $1500 \times 1500 m^2$. Οι αριθμοί που αναφέρονται σε αυτόν τον αριθμό υπολογίζονται κατά μέσο όρο άνω των 50 διαφορετικών συνδυασμών κόμβων που επιλέγονται τυχαία για να είναι κακόβουλοι Παραδείγματος χάριν, για 10 κακόβουλους κόμβους, μετρήσαμε τον αριθμό παρεμποδισμένων κόμβων για 50 διαφορετικούς συνδυασμούς που επιλέχτηκαν τυχαία από 10 κόμβους που γίνονται κακόβουλοι. Για κάθε δοκιμή, 20 τυχαίες τοπολογίες επιλέχτηκαν.



Σχήμα 6.11 Επίθεση πολλών κόμβων σε δίκτυο αισθητήρων που έχει ασφαλές απλο μονοπάτι δρομολόγηση πολλαπλών μονοπατιών. Το αριστερό γράφημα δείχνει 100 κόμβους.Το δεξί γράφημα δείχνει 200 κόμβους. Ο άξονας των χ δείχνει τους επιτιθέμενους κόμβους και ο ψ άξονας δείχνει τους εμποδισμένους κόμβους ανίκανους να στείλουν πακέτα. **(14)**

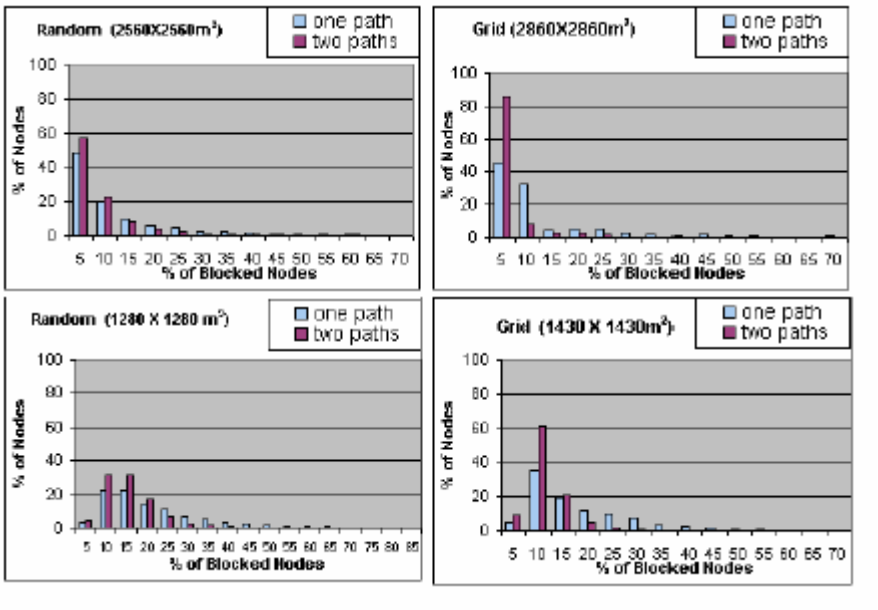
6.12.8 Επιθέσεις DOS

Έχουμε εκτελέσει ένα σύνολο πειραμάτων για να αναλύσουμε την επίδραση των επιθέσεων DOS που ένας κακόβουλος κόμβος μπορεί να προωθήσει. Η επίθεση DOS που έχουμε εξομοιώσει σε αυτά τα πειράματα αποτελείται από επανειλημμένες αποστολές πακέτων στοιχείων στο σταθμό βάσης για να εμποδίσει το ασύρματο μέσο και να μην επιτρέψει σε άλλους κόμβους για να στείλει τα πακέτα στοιχείων τους. Οι επιθέσεις DOS είναι δύσκολο να εξεταστούν εντελώς στο επίπεδο δικτύων. Κατά την άποψή μας, αυτές οι επιθέσεις πρέπει να εξεταστούν σε πολλαπλάσια επίπεδα. Στην ανάλυσή μας, έχουμε υποθέσει τα εξής:

- Οι κόμβοι αισθητήρων χρησιμοποιούν έναν κατάλληλο ποσοστό-βασισμένο μηχανισμό ελέγχου διαβιβάζοντας τα πακέτα στοιχείων. Αυτό υπονοεί ότι ένας κακόβουλος κόμβος που στέλνει επανειλημμένα τα πακέτα στοιχείων θα είναι σε θέση να εμποδίσει τους γείτονές του, αλλά όχι άλλους (προς τα πάνω) κόμβους.
- Ο σταθμός βάσεων έχει το αρκετά μεγάλο εύρος ζώνης διαθέσιμο έτσι ώστε ένας κακόβουλος κόμβος αισθητήρων στην εγγύτητά του δεν μπορεί να εμποδίσει το σταθμό βάσεων με τη χρησιμοποίηση μιας επίθεσης DOS.

Το σχήμα 6.12 παρουσιάζει τη ζημια που ένας κακόβουλος κόμβος μπορεί να προκαλέσει με την προώθηση μιας επίθεσης DOS. Η ζημια που προκαλείται από μια επίθεση DOS εξαρτάται από την αποτελεσματικότητα της πολλαπλών διαδρομών δρομολόγησης, την πυκνότητα της διασύνδεσης του δικτύου αισθητήρων, και την τοπολογία της γραφικής παράστασης.

Σε αυτό το πείραμα, δύο πυκνότητες δικτύων (αραιές και πυκνές) και δύο τοπολογίες (τυχαίες και πλέγμα) εξετάζονται. Στις τυχαίες παραγμένες τοπολογίες, η θέση κάθε κόμβου επιλέγεται τυχαία, και ο σταθμός βάσεων τοποθετείται στο κέντρο. Ο συνολικός αριθμός κόμβων για κάθε τυχαία τοπολογία είναι 200. Στην τοπολογία πλέγματος, κάθε κόμβος τοποθετείται σε ένα τετραγωνικό πλέγμα. Για να προσαρμόσει τον προσομοιωτή, ήταν απαραίτητο να διαταραχτεί κάθε θέση σε μια μικρή περιοχή γύρω από κάθε vertex σε μια τετραγωνική γραφική παράσταση πλέγματος. Κατ' αυτό τον τρόπο, οι τυχαίες τοπολογίες θα μπορούσαν να παραχθούν ακόμη και για ένα σχεδόν ομοιόμορφο τετραγωνικό πλέγμα. Το πλέγμα είναι ένα τετράγωνο 14×14



Σχήμα 6.12 Ιστόγραμμα των μιμούμενων επιθέσεων DOS για τις αραιές και πυκνές τυχαίες και τοπολογίες πλέγματος. **(14)**

Το σχήμα 6.12 αποκαλύπτει την απόδοση INSENS ενάντια σε έναν ενιαίο κόμβο προωθώντας μια επίθεση DOS. Για είτε τα ομοιόμορφα πλέγματα είτε τον τυχαίο προσδιορισμό θέσης, παράγουμε αρχικά μια δεδομένη τοπολογία των διεσπαρμένων κόμβων. Για αυτήν την τοπολογία, αφήνουμε κάθε κόμβο τη φορά γινόμαστε εισβολέας DOS και μετράμε τον αριθμό παρεμποδισμένων κόμβων που επηρεάζονται προς τα κάτω από τον εισβολέα DOS. Αυτό παράγει ένα ιστόγραμμο ανά τοπολογία. Ο Χ- άξονας καταγράφει το ποσοστό των κόμβων που μπορεί να εμποδιστεί από μια επίθεση DOS ενιαίων-κόμβων, και ο Υ-άξονας καταγράφει το ποσοστό τέτοιων κόμβων στην τοπολογία ,που εάν έγιναν κακόβουλοι, θα είχε τη δύναμη να εμποδίσει τον αριθμό κόμβων που απαριθμούνται στον Χ-άξονα. Για τη σαφήνεια, έχουμε ομαδοποιήσει τον Χ-άξονα στα δοχεία 0-5 %, 6-10 %, κ.λπ.... Και για τις τυχαίες και τοπολογίες πλέγματος, παράγουμε 50 τέτοιες τοπολογίες και σχεδιάζουμε το υπολογισμένο κατά μέσο όρο ιστόγραμμο που παρουσιάζεται ανωτέρω.

Από αυτόν τον αριθμό, μπορούμε να δούμε ότι η προστασία ενάντια στις επιθέσεις **DOS** ποικίλλει σημαντικά στις διαφορετικές πυκνότητες δικτύων και τις διαφορετικές τοπολογίες. Όπως πριν, σε όλες τις περιπτώσεις, ο πολλαπλών διαδρομών αλγόριθμος παρέχει την καλύτερη προστασία ενάντια στις επιθέσεις **DOS** από την

ενιαία προσέγγιση πορειών. Η πολλαπλών διαδρομών προσέγγιση αποδίδει πολύ καλύτερα για την τοπολογία πλέγματος, επειδή το πλέγμα σχεδόν πάντα προσφέρει μια έγκυρη περιττή δεύτερη πορεία. Η καλύτερη απόδοση της προσέγγισης πολλαπλών διαδρομών λαμβάνεται για τα αραιά πλέγματα (ανώτερη δεξια γραφική παράσταση), όπου 85% των κόμβων εισβολέων περιορίζονται στο φράξιμο πέντε ή λιγότερων κόμβων. Η σποραδικότητα περιορίζει έναν εισβολέα στο φράξιμο μόνο μερικών κόμβων, ενώ το πλέγμα σχεδόν πάντα προσφέρει στον αποστολέα μια έγκυρη δευτεροβάθμια πορεία. Η χειρότερη απόδοση της προσέγγισης πολλαπλών διαδρομών λαμβάνεται για τις αραιές τυχαίες τοπολογίες (ανώτερη αριστερή γραφική παράσταση), στις οποίες οι κόμβοι έχουν λίγους γειτονικούς και λιγα εναλλάσσομενα μονοπατια (συνήθως μόνο μια πορεία) στο σταθμό βάσεων. Σε αυτήν την περίπτωση, η προσέγγιση πολλαπλών διαδρομών εκτελεί μόνο ελαφρώς καλύτερα από την ενιαία δρομολόγηση πορειών.

Δεδομένου ότι το δίκτυο γίνεται πυκνότερο, κινούμενος από την κορυφαία σειρά των γραφικών παραστάσεων προς την κατώτατη σειρά στο σχήμα 6.12, οι επιτιθέμενοι είναι σε θέση να εμποδίσουν τους αυξανόμενους αριθμούς κόμβων, και τη μετατόπιση ιστογράμμων στο δικαίωμα. Αυτό ισχύει και για τις τυχαίες και τοπολογίες πλέγματος. Ενώ οι αριθμοί μετρούν τη μέση απάντηση INSENS, ένας επιτιθέμενος θα ωφελούταν με την εκμετάλλευση της δομής της τοπολογίας και τον προσδιορισμό των πιό αδύνατων κόμβων που θα χώριζαν τη γραφική παράσταση. Μια τέτοια επίθεση χωρισμού θα ήταν κατά ένα μεγάλο μέρος ατελέσφορη στα πλέγματα ή/και τις πυκνές τοπολογίες, επειδή τέτοιες τοπολογίες δεν χωρίζουν εύκολα λόγω των εναλλάσσομαι πορειών. Ο χωρισμός είναι μια αποτελεσματικότερη επίθεση για τις τοπολογίες που είναι και τυχαίες και αραιές. Δεν έχουμε μετρήσει συγκεκριμένα την απόδοση INSENS κατά μιας τέτοιας επίθεσης χωρισμού.

6.12.9Κρυπτογραφικός αλγόριθμος

Για να εφαρμόσουμε το INSENS στους κόκους, πρέπει να επιλέξουμε έναν ασφαλή, αποδοτικό κρυπτογραφικό αλγόριθμο που μπορεί να λειτουργήσει σωστά, λαμβάνοντας υπόψη τους περιορισμούς των πόρων των κόκων. Για να σώσουμε τη μνήμη, πρέπει να επαναχρησιμοποιήσουμε έναν ενιαίο κρυπτογραφικό αλγόριθμο για την κρυπτογράφηση στοιχείων, την παραγωγή της MAC, και το μονόδρομο αριθμό ακολουθίας, εφ' όσον οι εφαρμογές τους είναι ασφαλείς. Επιλέξαμε RC4, RC5, και Rijndael (AES) ως υποψηφίους.

Η εφαρμογή RC5S ποικίλλει σύμφωνα με τον αριθμό κύκλων. Περισσότεροι κύκλοι οδηγούν στην υψηλότερη ασφάλεια, αλλά απαιτούν περισσότερους πόρους. ImpleRC5 με 5 κύκλους και 12 κύκλους. Η παραγωγή 5 κύκλων δεν είναι πρακτικα διαφορετική από έναν τυχαίο αριθμό.

Εξετάσαμε την απόδοση ρευμάτων κώδικα RC4 για να συγκρίνουμε την απόδοσή της με φραγμούς κώδικα τους αλγορίθμους. Το RC4 είναι πολύ γρήγορο ρευμα κωδικα, αλλά έχει μερικές αδυναμίες όταν χρησιμοποιούνται στα ασύρματα δίκτυα.

Εφαρμόσαμε επίσης Rijndael στους κόκους και συγκρίναμε την απόδοσή της με RC5. Χρησιμοποιήσαμε μια τυποποιημένη έκδοση Rijndael. Χρησιμοποιεί για 1KB τη μνήμη. Υπάρχει μια γρήγορη έκδοση που χρησιμοποιεί 4KB τους πίνακες συμβούλευσης, αλλά αυτή υπερβαίνει τις ικανότητες μνήμης του κόκου.

Για να μετρήσουμε την απόδοση, εφαρμόσαμε RC4, RC5, και Rijndael στους κόκους για να κρυπτογραφήσουμε 200 X 128 μπιτ των στοιχείων με τον τρόπο CBC. Για να μετρήσουμε την ταχύτητα αυτών των αλγορίθμων στους κόκους, αφήνουμε το σταθμό βάσεων να στείλει *"αρχίζουμε"* το σήμα σε έναν κόκο. Στη λήψη αυτού του σήματος, ένας κόκος αρχίζει τον υπολογισμό του, και μετά από να ολοκληρώσει τον υπολογισμό, στέλνει το αποτέλεσμα στο σταθμό βάσεων. Ο σταθμός βάσεων καταγράφει το χρονικό διάστημα μεταξύ του όταν έστειλε το σήμα και όταν πήρε τα στοιχεία πίσω, ελέγχει το αποτέλεσμα, αφαιρεί τον μετ'επιστροφής χρόνο (που μετριέται με τον ίδιο τρόπο χωρίς τον κόκο που κάνει οποιαδήποτε κρυπτογράφηση), και παίρνει το χρόνο υπολογισμού. Για κάθε αλγόριθμο, τον εξετάσαμε για 20 φορές. Ο πίνακας 1 παρουσιάζει υπολογισμένο μέσο χρόνο για τον υπολογισμό 128 μπιτ των στοιχείων για κάθε αλγόριθμο.

Από τον πίνακα 6.13 βλέπουμε ότι:

1) Ο RC5 είναι καλός υποψήφιος για τους κόκους. Χρησιμοποιεί τη λιγότερη μνήμη (και στο μέγεθος κώδικα και το μέγεθος στοιχείων), και είναι πολύ αποδοτικό.

2) Συγκρινόμενο με τους RC5, Rijndael είναι πολύ αργό. Με βάση το αποτέλεσμά μας, για να κρυπτογραφήσει ένα πακέτο 30Bytes, θα περνούσε περίπου 0,2 δευτερόλεπτα. Εντούτοις, πιστεύουμε ότι στο εγγύς μέλλον, καθώς οι κόμβοι αισθητήρων γίνονται γρηγορότεροι και αποκτούν περισσότερη μνήμη, Rijndael θα γίνει καλός υποψήφιος για τον κρυπτογραφικό αλγόριθμο στα δίκτυα αισθητήρων. Στην εφαρμογή μας, χρησιμοποιήσαμε RC5 με 5 κύκλους. Σκεφτόμαστε ότι είναι αρκετά καλό

για τα δίκτυα αισθητήρων. Μπορούμε επίσης να χρησιμοποιήσουμε RC5 με 12 κύκλους.

	RC4	RC5		AES
		5 Rounds	12 Rounds	
Speed (128bits/ms)	1.299	5.471	12.475	102.483
Data Size (B)	258	68	124	1165
Code Size (B)	580	1436	1436	9492

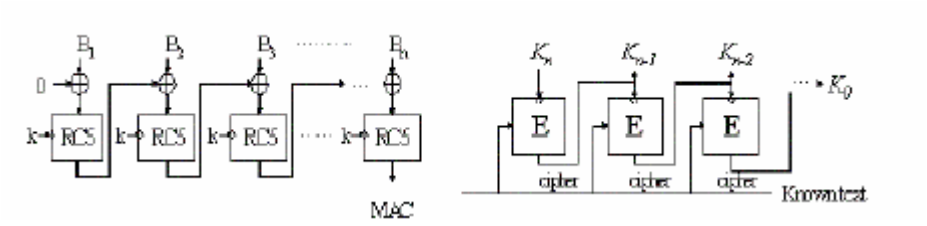
Πίνακας 6.13. Κρυπτογραφικός Αλγόριθμος Επικεφαλίδος **(14)**

Έχουμε εφαρμόσει επίσης το κοινό κλειδί κρυπτογραφίας RSA στη μορφή κόκκων και εκθέτουμε τα παρακάτω προκαταρτικά αποτελέσματα.

Αποκρυπτογραφήσαμε 64 bytes των στοιχείων όσον αφορά τον κόκο με ένα δημόσιο κλειδί RSA 1024-bits. Διαπιστώσαμε ότι η μετρημένη καθυστέρηση για την αποκρυπτογράφηση ήταν περίπου 15 δευτερόλεπτα. Αυτό προτείνει ότι το δημόσιο σύστημα κρυπτογραφίας κλειδιού θα μπορούσε να χρησιμοποιηθεί με έναν περιορισμένο τρόπο, π.χ. για τη συμμετρική βασική ανταλλαγή, για ορισμένα δίκτυα αισθητήρων. Προσπαθήσαμε επίσης να εφαρμόσουμε την κρυπτογράφηση με ένα ιδιωτικό κλειδί RSA στον κόκο, αλλά διαπιστώσαμε ότι ο κώδικας κρυπτογράφησης ΄΄πέθανε΄΄ κατά τη διάρκεια της εκτέλεσης. Υποθέτουμε ότι η κρυπτογράφηση υπερέβη τη χωρητικότητα μνήμης του κόκου , δεδομένου ότι η κρυπτογράφηση RSA καταναλώνει περισσότερη μνήμη από την αποκρυπτογράφηση, αν και περισσότερες δοκιμές απαιτούνται για να επιβεβαιώσουν αυτήν την υπόθεση.

6.12.10Παραγωγή κώδικα επικύρωσης μηνυμάτων.

Η MAC διαδραματίζει έναν κρίσιμο ρόλο στο INSENS. Χρησιμοποιείται για να επικυρώσει κάθε κόμβο, το μονοπάτι του, και την πληροφορία των γειτόνων του. Χρησιμοποιούμε τον τυποποιημένο τρόπο CBC για να παραγάγουμε τη MAC με κώδικα φραγμών RC5



(α)CBC λειτουργία δημιουργίας MAC (β) Μονόδρομη ακολουθία δημιουργίας αλυσίδας

Σχήμα 6.14 Το CBC βασισμένο στη δημιουργία MAC **(14)**

6.12.11Μονόδρομη παραγωγή αριθμού ακολουθίας

Ο μονόδρομος αριθμός ακολουθίας χρησιμοποιείται για να επικυρώσει αόριστα το σταθμό βάσεων. Για να παραγάγουμε το μονόδρομο αριθμό ακολουθίας, χρειαζόμαστε μια ασφαλή μονόδρομη λειτουργία. Η προσέγγισή μας είναι βασισμένη στα ακόλουθα κριτήρια:

Με τη γνώση ενός plaintext και του αντίστοιχου κρυπτογραφήματος που υπολογίζονται χρησιμοποιώντας έναν αλγόριθμο κώδικα φραγμών, όπως το RC5, δεν μπορούμε να ξέρουμε το κλειδί που χρησιμοποιήθηκε για να παραγάγει το κρυπτογράφημα. Η μονόδρομη γεννήτρια αριθμού ακολουθίας μας παρουσιάζεται στο σχήμα 6.14 (β). Ο σταθμός βάσεων επιλέγει ένα τυχαίο βασικό *Kn* και το χρησιμοποιεί για να κρυπτογραφήσει ένα γνωστό plaintext και παίρνει κώδικα. αυτός ο κώδικας είναι K_{n-1} και ο σταθμός βάσεων το χρησιμοποιεί ως κλειδί για να κρυπτογραφήσει το ίδιο πράγμα γνωστό ως plaintext. Αυτή η διαδικασία συνεχίζεται έως ότου παίρνουμε *K0.*

6.13 Ζητήματα εφαρμογής

6.13.1 Σταθμός και κόμβος βάσεων.

Εφαρμόσαμε το σταθμό βάσεων στην Java. Η βάση σταθμός παίρνει τις πληροφορίες από τον κόκο για τον προγραμματισμό του πίνακα και επεξεργάζεται τις πληροφορίες, και στέλνει τους πίνακες δρομολόγησης πίσω σε κάθε κόκο. Στην εφαρμογή μας, χρησιμοποιήσαμε την ίδια στρατηγική που περιγράφηκε για να βρεί δύο πορείες για κάθε κόμβο. Αλλά επιλέγουμε τον αλγόριθμο BFS αντί του Dijkstra επειδή υποθέτουμε ότι το κόστος κάθε σύνδεσης είναι ίδιο. Εφαρμόσαμε τον INSENS σε TinyOS 1,0 με NesC. Όλες οι εντατικές λειτουργίες υπολογισμού μας γράφονται καθώς οι στόχοι, για να τις αποτρέψουν από το φράξιμο των πακέτων ή του χρονομέτρου διακόπτουν.

6.13.2Κατάτμηση μηνυμάτων ανατροφοδότησης.

Στο τρέχον TinyOS, το μέγεθος πακέτων προεπιλογής είναι 30 bytes αν και αυτό μπορεί να τροποποιηθεί. Εντούτοις η ανατροφοδότηση μηνυμάτων INSENS μπορεί να είναι πολύ μακρύτερη, επειδή περιέχει έναν επικυρωμένο κατάλογο γειτόνων. Στην εφαρμογή μας, τέμνουμε ένα μήνυμα ανατροφοδότησης στα πακετα 30 bytes ανατροφοδότησης. Προσθέτουμε δύο περιορισμούς για την κατάτμηση του πακέτου ανατροφοδότησης. για να το κάνει να εργαστεί με το INSENS και να αποτρέψει τις πιθανές επιθέσεις

Κάθε πακέτο τμήματος έχει έναν αριθμό ακολουθίας. Οποιοσδήποτε κόμβος πρέπει προς τα εμπρός να χαμηλώσει το πακέτο ακολουθίας πρίν διαβιβάσει ένα υψηλότερο πακέτο ακολουθίας. Όταν ένας κόμβος παίρνει ένα υψηλότερο πακέτο ακολουθίας ενώ δεν έχει πάρει ένα χαμηλότερο πακέτο ακολουθίας, πρέπει να πετάξει εκείνο το πακέτο.

Ολόκληρες οι πληροφορίες των μονοπατιών πρέπει να τεθούν στο πρώτο πακέτο. Οι προς τα πάνω κόμβοι το χρειάζονται για να διαβιβάσουν τα πακέτα. Αυτός περιορίζει το μακρύτερο μονοπάτι σε 9. Αυτό είναι κατάλληλο για ένα δίκτυο με συγκρατημένο μέγεθος. Επειδή κάθε μήνυμα ανατροφοδότησης περιέχει έναν αριθμό της MAC, ο οποίος παράγεται από CBC τρόπο, ο κακόβουλος κόμβος δεν μπορεί να αλλάξει την ακολουθία πακέτου τμήματος, ή να αντικαταστήσει ένα πακέτο τμήματος. Ο σταθμός βάσεων μπορεί να ελέγξει την ακεραιότητα των πακέτων ακολουθίας μηνυμάτων ανατροφοδότησης με τη MAC.

6.13.3 Απώλεια πακέτων.

Κατά τη διάρκεια των πειραμάτων μας, διαπιστώσαμε ότι υπήρξαν πολλές απώλειες πακέτων. Οι λόγοι για αυτό μπορούν να είναι:

I. Το στρώμα της MAC (έλεγχος πρόσβασης μέσων) TinyOS δεν μπορεί να εξετάσει την απώλεια πακέτων, και INSENS πρέπει να στείλει τα μέρη των πακέτων.

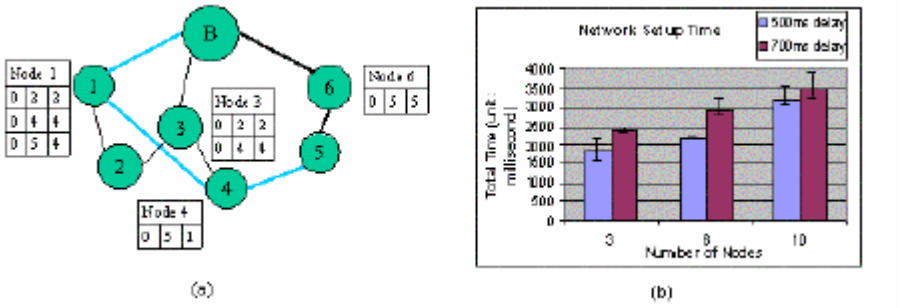
II. Το πακέτο που στέλνει ή που λαμβάνει τα συστατικά TinyOS δεν μπορεί να λάβει τα πακέτα εγκαίρως.

Υιοθετήσαμε τις ακόλουθες μεθόδους για να ανακουφίσουμε την απώλεια πακέτων. Κατ' αρχάς, η τυχαία καθυστέρηση εισάγεται σε κάθε κόκο πρίν να προωθηθεί για να μειώσει τις συγκρούσεις. Δεύτερον, όταν παίρνει ένας κόκος ένα πακέτο, αντιγράφει το πακέτο στο μεταβλητό του πλαίσιο αμέσως. Με αυτούς τους

μηχανισμούς, η απώλεια πακέτων μειώθηκε σημαντικά. Σημειώνουμε ότι τα βελτιωμένα πρωτόκολλα της MAC θα μπορούσαν να υιοθετηθούν στο μέλλον.

6.14 Αξιολόγηση απόδοσης

Έχουμε εφαρμόσει το INSENS στους κόκους για να δημιουργήσουμε τα δίκτυα 3-κόμβων, 6-κόμβων και 10-κόμβων. Το σχήμα 6.15(α) παρουσιάζει οργάνωση τοπολογίας δικτύων από το INSENS για ένα δίκτυο 6 κόμβων. Κάθε κόμβος έχει τον πίνακα δρομολόγησής του για να καθοδηγεί τα πακέτα. Βλέπουμε ότι ο κόμβος 5 έχει δύο πορείες για να βασίσει το σταθμό, ο πρώτος περνά από τον κόμβο 6, ο δεύτερος εξετάζει τους κόμβους 4 και 1. Λόγω των απωλειών πακέτων, ο σταθμός βάσης δεν μπορεί να λάβει τις πλήρεις πληροφορίες τοπολογίας δικτύων, όμως μπορεί ακόμα να χτίσει μέρος του δικτύου βασισμένου στα μηνύματα αιτήματος και ανατροφοδότησης που φθάνουν. Αυτό είναι ένα σημαντικό χαρακτηριστικό γνώρισμα του INSENS. Μετρήσαμε τη χρήση μνήμης INSENS και του συνολικού χρόνου στην οργάνωση ολόκληρου του δικτύου με το INSENS, για να αξιολογήσουμε την πρακτικότητα INSENS.



Σχήμα 6.15 Οργάνωση τοπολογίας δικτύου 6 κόμβων από το INSENS **(14)**

6.15Χρήση μνήμης του INSENS στους κόκους.

Ο πίνακας 6.16 παρουσιάζει χρήση μνήμης του INSENS. *"Η ανατροφοδότηση"* είναι για τη διάσωση ολόκληρου του ανατροφοδοτημένου μηνύματοςπριν τη κατατμησή του. *"Το πακέτο"* είναι για τη διάσωση των εισερχόμενων πακέτων. Στην εφαρμογή μας, δεν εστιάσαμε στο διάστημα μνήμης αποταμίευσης, αλλά το αποτέλεσμα δείχνει ότι οι απαιτήσεις μνήμης του INSENS μπορούν να ικανοποιηθούν εύκολα από τους περιορισμούς των τρεχόντων δικτύων αισθητήρων βασισμένων στους κόκους. Η πρόσθετη αποταμίευση μνήμης θα μπορούσε να επιτευχθεί. Παραδείγματος χάριν, με έναν καλό μηχανισμό επεξεργασίας πακέτων,

δεν χρειαζόμαστε το διάστημα *"πακέτων "*, και με μια καλύτερη εφαρμογή κατάτμησης πακέτων, δεν χρειαζόμαστε *"την ανατροφοδότηση"*.

code	total data	Crypto	neighbor info	msg & MAC	feedback	packet	OS and others
19000	1200	68	105	105	200	360	360

Πίνακας 6.16 Κατανάλωση ενέργειας του INSENS(bytes) **(14)**

6.16Χρόνος οργάνωσης δικτύων

Στην εφαρμογή μας, ο σταθμός βάσεων μεταδίδει ένα μήνυμα αιτήματος, λαμβάνει **όλα** τα μηνύματα ανατροφοδότησης, και υπολογίζει τους πίνακες δρομολόγησης. Στέλνει τον πίνακα δρομολόγησης κάθε κόμβου, και περιμένει ένα *λαμβανόμενο "* μήνυμα *πίνακα " δρομολόγησης* από κάθε κόμβο. Μετράμε το χρονικό διάστημα μεταξύ του χρόνου που οι σταθμοί βάσης μεταδίδουν το αιτούμενο μήνυμα της και του χρόνου που λαμβάνει **όλα τα** λαμβανόμενα " μηνύματα πίνακα " δρομολόγησης. Θέτουμε το δίκτυο ως πυκνό δίκτυο, έτσι κάθε κόμβος έχει διάφορους γείτονες. Δεδομένου ότι ο αριθμός κόμβων αυξήθηκε, δοκιμάσαμε περισσότερες απώλειες πακέτων. Αλλά λόγω του πλεονασμού στις πληροφορίες γειτόνων, ο σταθμός βάσεων ήταν συνήθως ικανός στην οργάνωση του δικτύου, βασισμένο στον περιορισμένο αριθμό μηνυμάτων ανατροφοδότησης που έφθασε.

Υπάρχουν διάφοροι παράγοντες που έχουν επιπτώσεις στο χρόνο οργάνωσης:

- Ο χρόνος εκτέλεσης του κρυπτογραφικού αλγορίθμου,
- Ο χρόνος εκτέλεσης της επεξεργασίας πακέτων, όπως η αποστολή, η λήψη, η αντιγραφή, και η δρομολόγηση, και
- Ο χρόνος αναμονής στο INSENS, το οποίο περιλαμβάνει την τυχαία καθυστέρηση, τον χρόνο αναμονής μηνυμάτων ανατροφοδότησης, και τον χρόνο αναμονής σταθμών βάσης.

Ο σταθμός βάσης περιμένει 500ms μετά την παραλαβή ενός πακέτου ανατροφοδότησης. Αυτός ο χρόνος αναμονής επαναρυθμίζεται με κάθε νέο μήνυμα ανατροφοδότησης. Τελικά, δεν θα φθάσουν άλλα μηνύματα ανατροφοδότησης και ο σταθμός βάσεων θα σταματήσει και θα κινηθεί προς τον υπολογισμό των πινάκων δρομολόγησης. Κάθε κόμβος αισθητήρων περιμένει επίσης 500ms για τις πληροφορίες γειτόνων που συλλέγονται. Εξετάσαμε επίσης 700ms διαλείμματα για τους κόμβους αισθητήρων μόνο (όχι σταθμός βάσεων). Διαπιστώσαμε ότι ο συνολικός χρόνος

οργάνωσης δικτύων κυριαρχεί μέχρι τον χρόνο αναμονής των κόμβων αισθητήρων. Συγκριτικά, ο χρόνος υπολογισμού των RC5-βασισμένων κρυπτογραφικών αλγορίθμων είναι σχετικά σύντομος. Το σχήμα 6.15 (β) παρουσιάζει συνολικά αποτελέσματα της δοκιμής μας.

6.17Συμπεράσματα

Αξιολόγήσαμε το INSENS, το οποίο είναι ένα ανεκτικό πρωτόκολλο δρομολόγησης για τα ασύρματα δίκτυα αισθητήρων. Η ανθεκτικότητα της απόδοσης πολλαπλών διαδρομών του INSENS ενάντια στις διάφορες μορφές επιθέσεων βασισμένων στην επικοινωνία από τους εισβολείς, αξιολογείται στην προσομοίωση. Το έγγραφο περιγράφει την πρακτική εμπειρία με τις εφαρμογές RC5 και κρυπτογράφησης AES των προτύπων στους κόκους, ένα RC5-βασισμένο σχέδιο για να παραχθούν οι κώδικες αυθεντικότητας μηνυμάτων (MACs), και μια RC5-βασισμένη παραγωγή των μονόδρομων αριθμών ακολουθίας.

6.18ΠΡΩΤΟΚΟΛΛΟ LHAP

6.18.1Εισαγωγή

Στα ad-hoc ασύρματα δίκτυα, κανένας σταθμός βάσης δεν υπάρχει και κάθε κινητός κόμβος δρα ως δρομολογητής και ως οικοδεσπότης. Οι κόμβοι σε ένα ad-hoc δίκτυο μπορούν να επικοινωνήσουν ο ένας με τον άλλον οποιαδήποτε στιγμή, κάτω από περιορισμούς συνδετικότητας. Αυτήν την περίοδο, τα περισσότερα ad-hoc δίκτυα δεν έχουν οποιεσδήποτε παροχές για να περιορίσουν ή να ρυθμίσουν την κυκλοφορία που γίνεται μέσω ενός κόμβου, δηλ., δεν εφαρμόζουν οποιοδήποτε *έλεγχο πρόσβασης στο δίκτυο*. Αυτό αφήνει αυτά τα δίκτυα τρωτά στις επιθέσεις *κατανάλωσης των πόρων* όπου ένας κακόβουλος κόμβος εγχέει τα πακέτα στο δίκτυο με στόχο την κενωση των πόρων των κόμβων που αναμεταδίδουν τα πακέτα.

Σαφώς, μια ικανότητα ελέγχου πρόσβασης στο δίκτυο είναι ουσιαστική για τα ad-hoc δίκτυα σε ένα εχθρικό περιβάλλον όπως ένα πεδίο μάχης.

Μια επίθεση κατανάλωσης των πόρων μπορεί να είναι ειδικάτ αποτελεσματική εάν ένα πακέτο που εγχέεται σε ένα ad-hoc δίκτυο από τα άκρα κακόβουλων κόμβων, που είναι πολλαπλής διανομής, ή τη μετάδοση μέσα από το δίκτυο.

Παραδείγματος χάριν, η λειτουργία των περισσότερων πρωτοκόλλων δρομολόγησης περιλαμβάνει τα βήματα στα οποία ένα πακέτο ελέγχου, π.χ., ένα πακέτο αιτήματος διαδρομών, εκπέμπεται σε όλους τους κόμβους.

Επιπλέον, πολλές εφαρμογές για τα ad-hoc δίκτυα περιλαμβάνουν το συνεργάσιμο υπολογισμό γι'αυτό η πολλαπλή επικοινωνία είναι πιθανό να αυξηθεί σημαντικά όπως τα πρωτόκολλα πολλαπλής δρομολόγησης , για τα ad-hoc δίκτυα, που γίνονται ωριμότερα.

Έχουν προταθεί επεκτάσεις ασφάλειας στα υπάρχοντα πρωτόκολλα δρομολόγησης που περιλαμβάνουν τους μηχανισμούς για τα πακέτα ελέγχου δρομολόγησης στο δίκτυο. Παρόλ'αυτά, κανένα από τα προτεινόμενα ασφαλή πρωτόκολλα δρομολόγησης δεν περιλαμβάνει οποιεσδήποτε διατάξεις για τα πακέτα στοιχείων επικύρωσης. Γι'αυτό, μια επίθεση κατανάλωσης των πόρων, βασισμένη στα πακέτα στοιχείων, ειδικά σε πολλές εφαρμογές , μπορεί να προωθηθεί εύκολα. Υπό αυτήν τη μορφή, πιστεύουμε ότι είναι σημαντικό να παρέχεται ο έλεγχος πρόσβασης στο δίκτυο και για τα στοιχεία, και για τα πακέτα ελέγχου.

Για την παροχή του πλήρους ελέγχου πρόσβασης στο δίκτυο, μια λύση είναι η επικύρωση όλων των πακέτων, έτσι ώστε ένας κόμβος μόνο να προωθεί τα πακέτα

από τους εξουσιοδοτημένους κόμβους. Μια απλή λύση είναι να χρησιμοποιηθεί ένα ευρύ κλειδί δικτύου κοινό σε όλους τους κόμβους και κάθε κόμβος να χρησιμοποιεί αυτό το κοινό κλειδί για να υπολογίσει τους κώδικες αυθεντικότητας μηνυμάτων (MACs) στα πακέτα που στέλνει και λαμβάνει.

Αυτό το σχέδιο, παρόλ'αυτά, απαιτεί μια ακριβή σφαιρική λειτουργία επανεισαγωγής κλειδιού εάν το κοινό κλειδί συμβιβάζεται. Μία άλλη περίπτωση είναι να χρησιμοποιηθούν οι τεχνικές αυθεντικότητας βασισμένες στο σύστημα ασύμμετρης κρυπτογραφίας.

Παρόλ'αυτά, αυτές οι τεχνικές συνήθως δεν προσαρμόζονται καλά στα ad-hoc δίκτυα. Στα ασύρματα ad-hoc δίκτυα με την υψηλή κινητικότητα κόμβων, το σύνολο γειτόνων ενός κόμβου μπορεί να διατηρήσει αλλαγές, επομένως η συχνότητα, και ως εκ τούτου το κόστος για την αμοιβαία επικύρωση μεταξύ των κόμβων είναι πολύ μεγαλύτερη από αυτή στα ενσύρματα δίκτυα που δεν έχουν την κινητικότητα κόμβων. Περαιτέρω, οι πόροι ενός κινητού κόμβου όπως η δύναμη μπαταριών, η υπολογιστική ικανότητα και το εύρος ζώνης είναι συνήθως αρκετά περιορισμένα.

Όλα αυτά τα γεγονότα κάνουν, το μεγαλύτερο μέρος των εφαρμογών που προτείνονται, μη πρακτικά για την εφαρμογή ελέγχου πρόσβασης για ad-hoc δίκτυα.

Εδώ, παρουσιάζουμε το LHAP, ένα εξελικτικό και αποδοτικό πρωτόκολλο ελέγχου πρόσβασης στο δίκτυο για τα ad-hoc δίκτυα. Για να αποτρέψει τις επιθέσεις κατανάλωσης των πόρων, το LHAP εφαρμόζει την αυθεντικότητα hop-by-hop, δηλ., ενδιάμεσοι κόμβοι επικυρώνουν όλα τα πακέτα που λαμβάνουν πριν την προώθησή τους.

Χρησιμοποιώντας το LHAP, ένας κόμβος που ενώνει ένα ad-hoc δίκτυο πρέπει μόνο να εκτελέσει κάποιες ανέξοδες λειτουργίες αυθεντικότητας για να δελεάσει μια σχέση εμπιστοσύνης με τους γείτονικούς του. Μεταπηδά έπειτα σε ένα πολύ ελαφρύ πρωτόκολλο για τις επόμενες αυθεντικοποιήσεις κυκλοφορίας.

Το LHAP είναι διαφανές και ανεξάρτητο των πρωτοκόλλων δρομολόγησης δικτύων. Μπορεί να θεωρηθεί σαν την ύπαρξη μεταξύ του στρώματος συνδέσεων στοιχείων και του στρώματος δικτύων, που παρέχει ένα στρώμα της προστασίας που μπορεί να αποτρέψει ή να ανατρέψει πολλές επιθέσεις από να συμβεί, συμπεριλαμβανομένων των επιθέσεων στα ειδικά πρωτόκολλα δρομολόγησης που πραγματοποιούνται από την έλλειψη υποστήριξης για την επικύρωση πακέτων σε αυτά τα πρωτόκολλα.

Παρακάτω φαίνονται οι λεπτομέρειες του πρωτοκόλλου LHAP , και αναλύεται η ασφάλειά της. Επίσης αναλύουμε την απόδοση του πρωτοκόλλου.

6.19Ένα ελαφρύ πρωτόκολλο αυθεντικότητας hop-by-hop (LHAP)

Σε αυτό το τμήμα, περιγράφουμε αρχικά τις υποθέσεις που κάναμε κατά τη διάρκεια του σχεδιασμού του πρωτοκόλλου. Έπειτα δίνουμε μια επισκόπηση των στόχων σχεδιασμού και της βασικής λειτουργίας LHAP. Τέλος, συζητάμε τις διαδικασίες LHAP λεπτομερώς.

6.19.1Υποθέσεις

Κάνουμε τις ακόλουθες υποθέσεις . Κατ' αρχάς, οι συνδέσεις δικτύων είναι αμφίδρομες. Δεύτερον, υποθέτουμε ότι ένα πακέτο που στέλνεται από έναν κόμβο παραλαμβάνεται από έναν γειτονικό κόμβο προτού να μπορέσει ένας τρίτος κόμβος να επαναλάβει το πακέτο σε αυτο, εκτός αν ο γείτονας ‘’έχει ρίξει‘’υπό εξέταση το πακέτο. Τρίτον, υποθέτουμε κάθε κόμβος ότι υπογράφει ένα δημόσιο βασικό πιστοποιητικό από μια εμπιστευμένη αρχή (CA) πιστοποιητικών και επίσης ένα αυθεντικό δημόσιο κλειδί.

Το πρωτόκολλό μας στηρίζεται σε αυτά τα δημόσια κλειδιά για να δελεάσει την εμπιστοσύνη στο ad-hoc δίκτυο. Η διανομή των πιστοποιητικών και των κλειδιών μπορεί να γίνει με οποιοδήποτε αξιόπιστο τρόπο. Τέταρτο, υποθέτουμε ότι οι κινητοί κόμβοι υπό εξέταση είναι σχετικά μικρής ισχύος. Οι λειτουργίες των κοινών κλειδιών, όπως οι ψηφιακές υπογραφές είναι σχετικά ακριβές για τον υπολογισμό. Τέλος, υποθέτουμε το χαλαρό χρονικό συγχρονισμό στο ad-hoc δίκτυο δεδομένου ότι το LHAP χρησιμοποιεί το ευρύ χυτό πρωτόκολλο αυθεντικότητας TESLA

6.19.2Σημείωση

Χρησιμοποιούμε την ακόλουθη σημείωση για να περιγράψουμε το πρωτόκολλο ασφάλειας και τις διαδικασίες κρυπτογραφίας συστήματος

- *τα A,B* είναι κύριες ταυτότητες των κινητών κόμβων.
- *το Cert A* είναι δημόσιο-βασικό πιστοποιητικό κόμβων *A* που εκδίδεταιαπότοεμπιστευμένοCA.
- *το SignA (M)* δείχνει την ψηφιακή υπογραφή του μηνύματος *M,* που υπογράφεταιμετοιδιωτικόκλειδίκόμβωνA.
- Τα M1|M2 δείχνουν την αλληλουχία του μηνύματος *M1 και M2*
- *Το MAC(K, M)* δείχνει τον υπολογισμό του MAC πάνω στο μήνυμα Μμετοβασικόκλειδί*K*.

- *Το* $K_A^T(i)$ δείχνει το κλειδί i^{th} κόμβων A στο κλειδί TESLA του αλυσίδα, ενώ $K_A^F(i)$ δείχνει το κλειδί i^{th} του κλειδιού σε αλυσίδα κυκλοφορίας κλειδιων.

6.20 Περιγραφή πρωτοκόλλου

Ο κύριος στόχος του πρωτοκόλλου είναι να παρασχεθεί ο έλεγχος πρόσβασης στο δίκτυο, δηλ., για να αποτρέψει τους αναρμόδιους κόμβους από το να είναι σε θέση να εγχεθεί η κυκλοφορία στο ad-hoc δίκτυο. Για να επιτύχει αυτόν τον στόχο, κάτω από το LHAP, κάθε κόμβος στο δίκτυο αυθεντικοποιεί κάθε πακέτο, ανεξάρτητα από το εάν είναι ένα πακέτο στοιχείων ή ένα πακέτο ελέγχου δρομολόγησης, που παραλαμβάνεται από τους γείτονές του πριν την προώθησή τους. Τα πακέτα από τους αναρμόδιους κόμβους πέφτουν, αποτρέποντας τους κατά συνέπεια από τη διάδοση μέσω του δικτύου.

Το LHAP είναι διαφανές και ανεξάρτητο του πρωτοκόλλου δρομολόγησης δικτύων. Μπορεί να θεωρηθεί σαν την ύπαρξη μεταξύ του στρώματος συνδέσεων στοιχείων και του στρώματος δικτύων, που παρέχει ένα στρώμα της προστασίας που μπορεί να αποτρέψει ή να ανατρέψει πολλές επιθέσεις να συμβούν. Αυτη η διαφάνεια και ανεξαρτησία επιτρέπουν το LHAP να είναι ενεργό η όχι χωρίς επιρροή των διαδικασιών άλλων στρωμάτων.

Τα κέρδη αποδοτικότητας LHAP πέρα από τα παραδοσιακά πρωτόκολλα αυθεντικότητας προέρχονται από δύο τεχνικές: (ι) ελαφριά αυθεντικοποίηση πακέτων, και (ΙΙ) ελαφριά διαχείριση εμπιστοσύνης. Δεδομένου ότι όλα τα πακέτα επικυρώνονται σε κάθε hop στις πορείες τους (αναφερόμαστε σε αυτό όπως επικύρωση hop-by-hop), είναι απαραίτητο ότι η τεχνική αυθεντικοποίησης πακέτων που χρησιμοποιείται από το LHAP είναι όσο το δυνατόν πιό ανέξοδη.

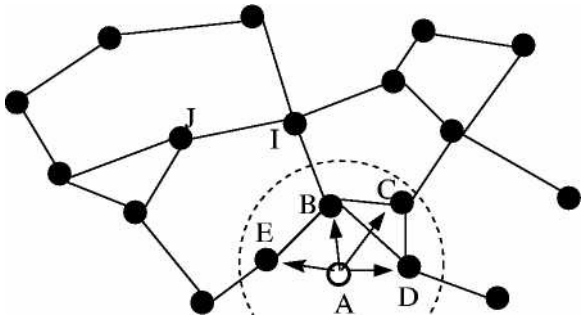
Το LHAP υιοθετεί μια τεχνική αυθεντικοποίησης πακέτων βασισμένη στη χρήση μονόδρομων αλυσίδων. Αφετέρου, το LHAP χρησιμοποιεί TESLA για να μειώσει τον αριθμό δημόσιων βασικών διαδικασιών για την εμπιστοσύνη έναρξης μεταξύ των κόμβων, και επίσης τη χρήση TESLA για τη διατήρηση της σχέσης εμπιστοσύνης μεταξύ των κόμβων.

6.20.1Αυθεντικότητα ελαφράς κυκλοφορίας

Όπως στο TESLA, η τεχνική αυθεντικοτητας κυκλοφορίας ,που χρησιμοποιείται από το LHAP, βασίζεται στη χρήση των μονόδρομων αλυσίδων κλειδιών.

Αντίθετα από το TESLA, παρόλαυτά, η τεχνική αυθεντικότητας μας, δεν χρησιμοποιεί την περιοδική και καθυστερημένη βασική κοινοποίηση. Η καθυστερημένη επικύρωση (όπως στο TESLA) δεν είναι κατάλληλη για το LHAP αφού ένα πακέτο θα καθυστερούσε σε κάθε κόμβο στην πορεία από την πηγή στον προορισμό. Επιπλέον, δεδομένου ότι κάθε κόμβος πρέπει να αποθηκεύσει τα πακέτα κυκλοφορίας που έχει λάβει έως ότου να επικυρωθούν, η καθυστερημένη αυθεντικότητα θα οδηγήσει στη μεγάλη αποθήκευση απαιτήσεων σε κάθε κόμβο.

Στο LHAP, κάθε κόμβος παράγει μια μονόδρομη αλυσίδα κλειδιών που χρησιμοποιείται για την αυθεντικότητα κυκλοφορίας από τους άμεσους γείτονές της. Χρησιμοποιούμε τον όρο κλειδί κυκλοφορίας (traffic) για να αναφερθούμε στα κλειδιά σε αυτήν την μονόδρομη βασική αλυσίδα. Παραδείγματος χάριν, εξετάζουμε έναν κόμβο A που θέλει να μεταδώσει ραδιοφωνικά ένα πακέτο μ. Αφήνουμε το επόμενο κλειδί κυκλοφορίας (traffic) του να είναι $K_A^F(i)$. Θα στείλει το ακόλουθο μήνυμα :



Σχήμα 6.17 Ένα σενάριο όπου ο κόμβος Α ενώνει το ειδικό δίκτυο **(13)**

$A; > \quad *: \quad \mu,\ K_A^F(i)$

Κάθε λαμβάνων κόμβος ελέγχει την αυθεντικότητα αυτού του πακέτου με την επαλήθευση της κυκλοφορίας κλειδιού $K_A^F(j), j \angle i$ βασισμένη στο πιό πρόσφατο κλειδί κυκλοφορίας, $K_A^F(j), j \angle i$, τα οποία έλαβε από τον κόμβο Α.

Στο LHAP, ένας κόμβος επικυρώνει μόνο το πακέτο κυκλοφορίας από τους άμεσους γείτονές του, κατά συνέπεια είναι πολύ δύσκολο, εάν όχι αδύνατο, για έναν επιτιθέμενο να προωθήσει τις επιθέσεις επανάληψης.

Η χρησιμοποίηση των κλειδιών για την επικύρωση κυκλοφορίας έχει τα ακόλουθα οφέλη.

Κατ' αρχάς, επιτρέπει τη στιγμιαία επαλήθευση των πακέτων κυκλοφορίας.Δεύτερον, δεν είναι απαραίτητο να αποκαλυφθούν τα κλειδιά κυκλοφορίας περιοδικά.Η αποκάλυψη των κλειδιών περιοδικά, θα οδηγούσε σε μια αυστηρή απώλεια των κλειδιών όταν δεν έχει ένας κόμβος κανένα πακέτο που διαβιβάζει. Στην πράξη, στο LHAP, το ποσοστό στο οποίο ένας κόμβος καταναλώνει τα κλειδιά κυκλοφορίας του μπορεί να προσαρμοστεί στο πραγματικό ποσοστό κυκλοφορίας . Τρίτον, είναι υπολογιστικά αποδοτικότερο από ό,τι υπολογίζοντας το HMAC πέρα από το ολόκληρο μήνυμα, επειδή απαιτεί μόνο hash πέρα από ένα κλειδί ενός μικρού σταθερού μεγέθους (π.χ., 8 bytes).

Εντούτοις, σημειώνουμε επίσης ότι αυτό το σχέδιο δεν επιτυγχάνει το ίδιο επίπεδο ασφάλειας όπως στο TESLA, ως ανταλλαγή μεταξύ της ασφάλειας και της απόδοσης. Θα συζητήσουμε τις πιθανές επιθέσεις στα κλειδιά κυκλοφορίας, παρακάτω.

6.20.2 Διαχείριση εμπιστοσύνης

Η διαχείριση εμπιστοσύνης περιλαμβάνει την έναρξη εμπιστοσύνης, τη συντήρηση εμπιστοσύνης και τη λήξη εμπιστοσύνης.

6.20.3Η έναρξη εμπιστοσύνης

Όταν θέλει να ενώσει ένας κόμβος ένα ad-hoc δίκτυο, αυτό προ-υπολογίζει αρχικά μια μονόδρομη βασική αλυσίδα και μια βασική αλυσίδα TESLA. Κατόπιν υπογράφει τις υποχρεώσεις αυτών των βασικών αλυσίδων και τις μεταδίδει ραδιοφωνικά στους γείτονές του.

Στο σχήμα. 6.17, παρουσιάζουμε ένα σενάριο όπου ο κόμβος *A* αρχίζει να ενώνει ένα δίκτυο όπου οι γείτονές του είναι B,C,D και E. Ο κόμβος *A* μεταδίδει ραδιοφωνικά ένα JOIN μήνυμα με *TTL* = 1.

$$A \rightarrow *: Cert_A, Sign_A\left\{A \middle| K_A^T(0) \middle| K_A^F(0) \middle| T_A^T(0) \middle| T_A^F(0)\right\}$$

όπου $T_A^T(0), T_A^F(0)$ είναι οι αρχικοί χρόνοι για τις βασικές αλυσίδες του TESLA και κυκλοφορίας αντίστοιχα.

Κάθε λαμβάνων κόμβος ελέγχει αρχικά την αυθεντικότητα του κόμβου, χρησιμοποιώντας το δημόσιο κλειδί (CA), κατόπιν χρησιμοποιεί το δημόσιο κλειδί κόμβου *A* στο πιστοποιητικό για να ελέγξει την υπογραφή στο μήνυμα. Θα καταγράψει τις υποχρεώσεις των βασικών αλυσίδων κόμβου *A* και των αρχικών χρόνων τους εάν όλες οι επαληθεύσεις είναι επιτυχείς.

Για να δελεασει ένα αυθεντικό κλειδί κυκλοφορίας και ένα κλειδί TESLA για τον κόμβο *A,* κάθε ένας από τους γείτονές του (έστω *B)* μεταφέρει το ακόλουθο μήνυμα ACK *στο A:*

$$B \to A:\ Cert_B, Sign_B\left\{B \middle| K_B^T(0) \middle| K_B^F(0) \middle| T_B^T(0) \middle| T_B^F(0)\right\},\ MAC\left(K_B^T(i), K_B^F(j)\right)$$

όπου η υπογραφή παρήχθη όταν ένώθηκε αρχικά ο κόμβος Β με το δίκτυο, $K_B^F(j)$ είναι το προσφάτως απελευθερωμένο κλειδί κυκλοφορίας κόμβου Β, και $K_B^T(i)$ είναι το επόμενο κλειδί TESLA κόμβου Β που απελευθερώνεται

Κατά τη λήψη αυτού του μηνύματος, ο κόμβος *A* κάνει δύο επαληθεύσεις και λαμβάνει τις αυθεντικές δεσμεύσεις βασικών αλυσίδων κόμβου Β.Σημειώνεται ότι ο κόμβος *A* δεν μπορεί να ελέγξει τη MAC έως ώτου απελευθερώσει ο κόμβος Β το $K_B^T(i)$. Η καθυστέρηση κοινοποίησης είναι το μισό από ένα διάστημα TESLA, κατά μέσον όρο. Αφότου λαμβάνει και ελέγχει το $K_B^T(i)$ αργότερα, ο κόμβος *A* αρχίζει να διαβιβάζει την έγκυρη κυκλοφορία από τον κόμβο Β.

<u>6.20.4Η συντήρηση εμπιστοσύνης</u>.

Περιοδικά, κάθε κόμβος μεταδίδει ραδιοφωνικά ένα μήνυμα αναβάθμισης κλειδιών (με TTL=1) στους γείτονές της, το οποίο περιέχει το πρόσφατα αποκαλυπτόμενο κλειδί κυκλοφορίας του. Το μήνυμα αναβάθμισης κλειδιών επικυρώνεται με το επόμενο κλειδί TESLA στη βασική αλυσίδα του. Για παράδειγμα, η αναβάθμιση κλειδιών μηνυμάτων που ο κόμβος Α στέλνει, είναι :

$$A \to *:\ \mathrm{A}, K_A^T(i-1), MAC\left(K_A^T(i), K_A^F(j)\right)$$

όπου το $K_A^F(j)$ είναι το πρόσφατο απελευθερωμένο κλειδι κυκλοφορίας κόμβου Α, και $K_A^T(i)$ είναι το επόμενο κλειδί TESLA κόμβου Α που απελευθερώνεται.

Επιπλέον ο κόμβος Α περιλαμβάνει το $K_A^T(i-1)$ για να επιτρέψει στους γείτονές του να ελέγξει τα προηγούμενα μηνύματα αναβάθμισης κλειδιών από τον κόμβο A.

Ο σκοπός της αναμετάδοσης μηνυμάτων αναβάθμισης κλειδιών είναι να αποτρέψει κακόβουλους κόμβους να εξαπατήσουν την κυκλοφορία χρησιμοποιώντας τα κλειδια κυκλοφορίας του κόμβου Α που εχουν ήδη απελευθερωθεί.

Ένας γειτονικός κόμβος που λαμβάνει το ανωτέρω μήνυμα αναβάθμιση κλειδιών μπορεί να ελέγξει την αυθεντικότητα $K_A^F(j)$ βασισμένη στο πιό πρόσφατο κλειδί σε αυτήν την βασική αλυσίδα, ακόμα κι αν δεν μπορεί να ελέγξει τη MAC αμέσως. Εντούτοις, ο κόμβος δεν ξέρει εάν $K_A^F(j)$ είναι το πιό πρόσφατο κλειδί από τον κόμβο Α έως ότου λαβει το καθυστερημένο αποκαλυπτόμενο $K_A^T(i)$.

6.20.5Λήξη εμπιστοσύνης

Στο LHAP, υπάρχουν δύο σενάρια κάτω από τα οποία η σχέση εμπιστοσύνης μεταξύ των κόμβων θα εκτελεστεί.

Κατ' αρχάς, όταν ανιχνεύεται ένας συμβιβασμένος κόμβος, όλοι οι κόμβοι θα ολοκληρώσουν τη σχέση εμπιστοσύνης τους με εκείνο τον κόμβο μόνιμα.

Δεύτερον, όταν δεν λαμβάνει ένας κόμβος ένα (μήνυμα έγκυρο) αναβάθμισης κλειδιών από έναν γείτονικό, μέσα σε ένα διάστημα TESLA, επειδή το τελευταίο έχει κινηθεί από τη σειρά μετάδοσής του, θα το εμπιστευθεί προσωρινά.

Εάν οι δύο κόμβοι κινούνται μέσα στη σειρά μετάδοσης πάλι, μπορούν να τρέξουν τη διαδικασία έναρξης εμπιστοσύνης για να επανεγκαθιδρύσουν πάλι τη σχέση εμπιστοσύνης τους, εάν δεν έχουν οποιεσδήποτε εναποθηκευμένες υποχρεώσεις της άλλης βασικής αλυσίδας. Διαφορετικά, μπορούν να επανεγκαθιδρύσουν τη σχέση εμπιστοσύνης τους χρησιμοποιώντας το TESLA, με μια καθυστέρηση μισού διαστήματος TESLA κατά μέσον όρο.

6.21Ανάλυση ασφάλειας

Σε αυτό το τμήμα, συζητάμε μερικές πιθανές επιθέσεις ενάντια στο LHAP, οι οποίες είναι όλες ενάντια στις βασικές αλυσίδες κυκλοφορίας. Υποθέτουμε ότι το TESLA είναι ασφαλές, λαμβάνοντας υπόψη το χαλαρό χρονικό συγχρονισμό στο δίκτυο.

6.21.1Επιθέσεις ξένων

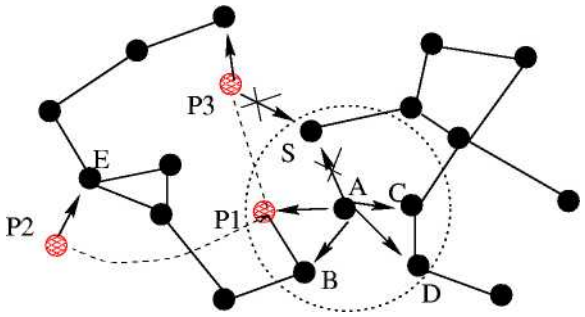
Οι επιθέσεις ξένων είναι επιθέσεις που προωθούνται από τους κόμβους που δεν κατέχουν ένα έγκυρο πιστοποιητικό. Προσδιορίζουμε τρεις τύπους επιθέσεων ξένων εδώ.

6.21.2Ενιαία επίθεση ξένων.

Στο σχήμα 6.17, παρουσιάσαμε μια κατάσταση όπου ο κόμβος Ε έλαβε ένα JOIN μήνυμα από τον κόμβο Α όταν ένώθηκε ο κόμβος Α στο δίκτυο.

Από το JOIN μήνυμα, ο κόμβος Ε έλαβε τις αυθεντικές υποχρεώσεις των βασικών αλυσίδων κόμβων Α. Τώρα εξετάζουμε ένα σενάριο ,στο σχήμα 2 ,όπου ο κόμβος Ε έχει κινηθεί από τη σειρά μετάδοσης κόμβων Α για ένα χρονικό διάστημα (έστω για διάφορα διαστήματα TESLA). Κατά τη διάρκεια αυτής της περιόδου, ο κόμβος Α έχει αποκαλύψει πολλά από τα κλειδιά TESLA του και τα κλειδιά κυκλοφορίας.

Ένας εξωτερικός επιτιθέμενος, κόμβος Ρ2, μπορεί να υποκλέψει και να χρησιμοποιήσει αυτά τα κλειδιά για να εκπροσωπήσει τον κόμβο Α. Παραδείγματος χάριν, υποθέτουμε ότι ο κόμβος Α έχει μεταδώσει ένα πακέτο με το περιεχόμενο Μ και $K_A^F(i)$.



Σχήμα 6.18. Διάφορες επιθέσεις σε LHAP. Οι P1 και P2 είναι οι κακόβουλοι κόμβοι, και οι διακεκομμένες γραμμές ανάμεσά τους είναι ιδιωτικά κανάλια**.** **(13)**

Υποθέτουμε ότι ο κόμβος P2 υπόκλεψε το μήνυμα και κινήθηκε έπειτα μέσα στη σειρά του κόμβου Ε. Μπορεί να τροποποιήσει το Μ στο Μ΄ με το ίδιο κλειδί κυκλοφορίας, και να το στείλει στον κόμβο Ε.

Επειδή τα κλειδιά κυκλοφορίας δεν αποκαλύπτονται περιοδικά, ο κόμβος Ε δεν μπορεί να καθορίσει ποιο κλειδί κυκλοφορίας ο κόμβος Α χρησιμοποιεί

Για να ανατρέψουμε αυτήν την επίθεση, σχεδιάσαμε τη φάση λήξης εμπιστοσύνης. Δεδομένου ότι ο κόμβος Ε δεν έχει λάβει νέα από τον κόμβο Α για ένα χρονικό διάστημα περισσότερων από ενός διαστημάτων TESLA, δεν θα διαβιβάσει οποιαδήποτε κυκλοφορία από τον κόμβο P2 έως ότου λαβει ένα έγκυρο μήνυμα αναβάθμισης κλειδιών.

Αφού τα κλειδιά TESLA αποκαλύπτονται περιοδικά, ο κόμβος Ε ξέρει ποια κλειδια TESLA ο κόμβος Α έχει απελευθερώσει. Επομένως, ο κόμβος P2 δεν μπορεί να χρησιμοποιήσει τα κλειδιά TESLA που ο κόμβος Α που αποκαλύφτηκε προηγουμένως να πλαστογραφεί ένα μήνυμα αναβάθμισης κλειδιών.

Αφ' ετέρου, ο κόμβος P2 δεν μπορεί να πλαστογραφήσει ένα έγκυρο μήνυμα αναβάθμισης κλειδιών, χρησιμοποιώντας οποιαδήποτε κλειδιά TESLA που δεν έχουν απελευθερωθεί ακόμα από τον κόμβο Α .

6.21.3Η συνεργάσιμη επίθεση ξένων.

Η συνεργάσιμη επίθεση ξένων (επίσης αποκαλούμενη επίθεση wormhole) προωθείται με την πολλαπλάσια συνέργεια έξω από τους επιτιθεμένους.

Στο σχέδιο 6.18, οι επιτιθέμενοι P1 και P2 έχουν ένα ιδιωτικό κανάλι που επιτρέπει σ'αυτούς να επικοινωνήσουν άμεσα. Ο P1 διαβιβάζει κάθε μήνυμα που υποκλέπτει από τον κόμβο Α, συμπεριλαμβανομένων των μηνυμάτων αναβάθμισης κλειδιών και των πακέτων κυκλοφορίας,στον P2 μέσω του wormhole.

Ο P2 έπειτα επαναεκπέμπει τα μηνύματα αναβάθμισης κλειδιών και τροποποιεί τα πακέτα κυκλοφορίας για να εξαπατήσουν τον κόμβο Ε.

Λόγω των λαθών χρονικού συγχρονισμού, ο κόμβος Ε μπορεί ακόμα να δεχτεί τα επαναλήφθέντα μηνύματα αναβάθμισης κλειδιών, και θα διαβιβάσει το τροποποιημένο πακέτα κυκλοφορίας από τον κόμβο P2.

Αυτή η επίθεση μπορεί να ανιχνευθεί εάν οι κινητοί κόμβοι φέρνουν συσκευές όπως τα GPS

Ένας κόμβος μπορεί να βάλει τις συντεταγμένες GPS του στα μηνύματα αναβάθμισης κλειδιών του για να επιτρέψει σε έναν λαμβάνοντα κόμβο να καθορίσει εάν είναι ικανά να ακούσουν το ένα το άλλο.

Παραδείγματος χάριν, στο σχήμα 6.18 ο κόμβοι Ε και Α δεν πρέπει να είναι ικανοί να ακούσουν ο ένας τον άλλο βασισμένα στις συντεταγμένες τους. Γι'αυτό ο κόμβος Ε θα ανιχνεύσει την ασυνέπεια της θέσης του κόμβου Α όταν λαβει τα επαναλαμβανόμενα μηνύματα αναβάθμισης κλειδιών από Ρ2, και ρίξει τα μηνύματα που παραλαμβάνονται αργότερα από το Ρ2.

Σημειώνουμε ότι το πρωτόκολλό μας δεν εξετάζει αυτήν την επίθεση εντελώς. Λόγω της καθυστέρησης ενός διαστήματος TESLA για την επαλήθευση ενός μηνύματος αναβάθμισης κλειδιών ο κόμβος Ε θα διαβιβάσει ακόμα τα (πιθανώς τροποποιημένα) πακέτα κυκλοφορίας από τον Ρ2 σε αυτό το διάστημα εάν τα πακέτα φέρουν τα κλειδιά κυκλοφορίας που ελέγχονται για να είναι σωστά και πιό αργά από αυτό στο μήνυμα αναβάθμισης κλειδιών στον κόμβο μια βασική αλυσίδα κυκλοφορίας.

Εντούτοις, υπάρχει ένας ανώτερος δεσμός στον αριθμό πλαστογραφημένων πακέτων, ο οποίος είναι ο αριθμός κόμβου Α πακέτων που στέλνει πραγματικά σε αυτό το διάστημα, επειδή ένας επιτιθέμενος δεν μπορεί να υπολογίσει τα κλειδιά κυκλοφορίας που ο κόμβος Α δεν έχει αποκαλύψει ακόμα.

6.21.4 Η κρυμμένη τελική επίθεση.

Η κρυμμένη τελική επίθεση στα κλειδιά κυκλοφορίας είναι λεπτότερη, και παρακινείται από το κρμμένο-τελικό πρόβλημα στην κινητή δικτύωση.

Το Ieee 802.11 λύνει το πρόβλημα χρησιμοποιώντας το CSMA/CA με τα πακέτα ACKs και προαιρετικού ελέγχου RTS/CTS.

Για να λειτουργήσει αυτό το σχέδιο , παρόλ'αυτά, πρέπει να υποθέσουμε, ότι οι ισχυριζόμενοι κόμβοι θα συνεργαστούν. Στο σχήμα 6.18 παρουσιάζουμε μια επίθεση που προσπαθεί να διακόψει αυτήν την συνεργασία, την οποία καλούμε κρυμμένη τελική επίθεση

Υποθέτουμε ότι ο κόμβος Α εκπέμπει ένα πακέτο κυκλοφορίας που περιλαμβάνει ένα κλειδί κυκλοφορίας $K_A^F(i)$ για την αυθεντικότητα πακέτων.

Για να επιτεθεί στον κόμβο S, ένας κακόβουλος κόμβος Ρ3 διαβιβάζει ένα πακέτο στον κόμβο S συγχρόνως, ο οποίος αναγκάζει τον κόμβο S για να ρίξει και τα

δύο πακέτα. Εν τω μεταξύ, ο κόμβος P1 μπορεί να στείλει $K_A^F(i)$ στον κόμβο P3 μέσω ενός wormhole. Τώρα ο κόμβος P3 μπορεί να στείλει ένα λανθασμένο πακέτο στον κόμβο S εκπροσωπώντας τον κόμβο A χρησιμοποιώντας $K_A^F(i)$, προτού να κάνει ο κόμβος A μια αναμετάδοση.

Συνεπώς, ο κόμβος S θα πετάξει το αυθεντικό πακέτο από τον κόμβο A. Παρόλ'αυτά, δεδομένου ότι το διάστημα αναμετάδοσης είναι συνήθως πολύ μικρό (δεκάδες των μικροδευτερολέπτων), οι επιτιθέμενοι μπορεί να πρέπει να τρέξουν τις συνεχείς επιθέσεις στο S για να αποτρέψουν τα πακέτα που ο κόμβος A αναμετέδωσε από τη λήψη επιτυχώς. Αυτό μπορεί να ανιχνευθεί εύκολα επειδή το κρυμμένο-τελικό πρόβλημα δεν συμβαίνει αυτό συχνά σε ένα δίκτυο όπου τα πακέτα ελέγχου RTS/CTS επεκτείνονται. Επιπλέον, εκπροσωπώντας έναν κόμβο μέσα σε μια σειρά δύο hops είναι πολύ πιθανό να ανιχνευθεί αυτός από άλλους κόμβους.

6.21.5Επιθέσεις μελών

Οι επιθέσεις μελών είναι επιθέσεις που προωθούνται από έναν ή περισσότερους συμβιβασμένους κόμβους που κατέχουν τα έγκυρα πιστοποιητικά. Προσδιορίζουμε τρεις πιθανές επιθέσεις μελών.

6.21.6Η εσωτερική ενιαία επίθεση

Ένας συμβιβασμένος κόμβος πιθανόν να προσπαθει να πλημμυρίσει το δίκτυο με πολλά πακέτα κυκλοφορίας. Για τα σχέδια που παρέχουν την αυθεντικότητα της πηγής, έχοντας έναν ανώτερο δεσμό στο βαθμό κυκλοφορίας , θα μπορούσαν να περιορίσουν αυτή την επίθεση.

Παρόλ'αυτά, το σχέδιο αυθεντικότητας hop-by-hop δεν παρέχει ισχυρή αυθεντικότητα πηγής, επειδή κάθε κόμβος αυθεντικοποιεί μόνο τους γείτονές του αντί των αρχικών πηγών κυκλοφορίας με σκοπό την εξελιξιμότητα. Κατά συνέπεια, ένας συμβιβασμένος κόμβος ισως να μεταδώσει την κακόβουλη κυκλοφορία προσποιούμενος ότι είναι ένας κόμβος προώθησης.

6.21.7Η επίθεση εσωτερικών κλώνων.

Η επίθεση εσωτερικών κλώνων εμφανίζεται όταν μοιράζεται ένας συμβιβασμένος κόμβος το ιδιωτικό κλειδί του (ως εκ τούτου τη ταυτότητά του) με τους εξωτερικούς συνωμότες του. Λόγω της κατοχής της ίδιας ταυτότητας, αυτοί οι κόμβοι είναι λιγότερο πιθανό να προωθήσουν τις συνεργάσιμες επιθέσεις χωρίς ανίχνευση. Οι κλωνοποιημένοι κόμβοι είναι εκεί πιθανότερο να διανεμηθούν στις

διαφορετικές θέσεις του δικτύου. Πράγματι, αυτή η επίθεση κλώνων μπορεί να θεωρηθεί ως πολλαπλάσιες ανεξάρτητες ενιαίες επιθέσεις μελών.

6.21.8Επιθέσεις πολλαπλών μελών

Αυτή η επίθεση προωθείται από τα πολλαπλά συμβιβασμένα μέλη, κάθε ένα από τα οποία φέρει ένα νόμιμο πιστοποιητικό. Ο συνασπισμός αυτών των μελών θα μπορούσε να οδηγήσει στις πολύ περίπλοκες επιθέσεις.

Γενικά, είναι δυσκολότερο να ανιχνευθούν οι επιθέσεις που προωθούνται από τους κόμβους μελών, ειδικά από τους πολλαπλάσιους συνεργάσιμους κόμβους.

Το LHAP μόνο του ,δεν έχει τις πλήρεις λύσεις για την εξέταση αυτών των επιθέσεων, αν και η χρήση μερικών τεχνικών να μετριάσουν τη δριμύτητα. Παραδείγματος χάριν, στην ενιαία επίθεση μελών, οι γείτονες θα μπορούσαν να γνωρίζουν την επίθεση εάν ένας κόμβος προσποιείται ότι είναι ο αποστολέας για το πακέτο που προέρχεται από αυτο.

Σημειώνουμε ότι μια καλύτερη λύση είναι ότι κάθε κόμβος εγκαθίσταται με ένα σύστημα ανίχνευσης παρείσφρυσης (IDS) που συλλέγει τα στοιχεία ιχνών που εισάγονται από όλα τα καθαρά στρώματα εργασίας, επειδή οι συμβιβασμένοι κόμβοι μπόρεσαν να προωθήσουν τις επιθέσεις ενάντια στα πολλαπλάσια στρώματα, όπως η δρομολόγηση του στρώματος και του στρώματος εφαρμογών. Επιπλέον, οι πολλαπλάσιοι κόμβοι θα μπορούσαν επίσης να προκαλέσουν συνεταιριστική ανίχνευση μορφής.

Παραδείγματος χάριν, στην επίθεση κλώνων μελών, μετά από ανταλλαγή των στοιχείων του με έναν άλλο κόμβο Ε, ένας κόμβος Α μπορεί να ανιχνεύσει την επίθεση εάν και τα δύο έχουν συναντήσει έναν τρίτο κόμβο Π στο σχεδόν ίδιο χρόνο αλλά σε διαφορετικές τοποθεσίες (εάν το GPS είναι εξοπλισμένο).

Τέλος, μετά από εντοπισμό των επιθέσεων και προσδιορισμό των συμβιβασμένων κόμβων, όλοι οι υπόλοιποι κόμβοι προσθέτουν τους συμβιβασμένους κόμβους στις τοπικές ανακλημένν λίστες κόμβων (RNL).

6.22Ανάλυση απόδοσης

Εξετάζουμε κυρίως τις ακόλουθες μετρικές απόδοσης σε LHAP.

6.22.1Υπολογιστικά έξοδα

Η κύρια υπολογιστική δαπάνη του LHAP είναι μια ψηφιακή υπογραφή RCA την οποίακάθε κόμβος δημιουργεί πρίν ενωθεί με το δίκτυο, το οποίο μπορεί να γίνει off-line.

Άλλα υπολογιστικά γενικά έξοδα προκύπτουν από τις επαληθεύσεις

υπογραφών και hash υπολογισμούς, που είναι προσιτά ακόμη και για τις συσκευές με πολύπεριορισμένηυπολογιστικήικανότητα.

6.22.2Αφάνεια

Στο LHAP, ένας κόμβος επιβεβαιώνει ένα πακέτο κυκλοφορίας που λαμβάνει με τον υπολογισμό ενός ή περισσότερων hashes. Γι'αυτό, η η πρόσθετη αφάνεια που το LHAP εισάγει είναι συνήθως αμελητέα, σε σύγκριση με την end-to-end μετάδοση αφάνειας πακέτου.

6.22.3Byte κυκλοφορίας επικεφαλίδος

Καθορίζουμε τα byte κυκλοφορίας επικεφαλίδος σαν τον αριθμό όλων των bytes μη-κυκλοφορίας που ο κόμβος μεταδίδει ανά χρονική μονάδα. Υπάρχουν τέσσερις πηγές byte κυκλοφορίας επικεφαλίδος στο LHAP. Πρώτον, ένας κόμβος προσθέτει ένα κλειδί κυκλοφορίας για κάθε πακέτο κυκλοφορίας που στέλνει.

Έτσι η επικεφαλίδα είναι ένα κλειδί ανά πακέτο κυκλοφορίας και κυρίως όλη η επικεφαλίδα καθορίζεται κυρίως από τον αριθμό πηγών στοιχείων και τα πρότυπα κυκλοφορίας τους.

Δεύτερον, ένας κόμβος στέλνει το μήνυμα join στο χρόνο που ενώνεται με το δίκτυο, και η επικεφαλίδα καθορίζεται για το μήνυμα αυτό από το μέγεθος δημόσιου κλειδιού πιστοποιητικό και το μέγεθος μιας ψηφιακής υπογραφής.

Τρίτον, ένας κόμβος στέλνει ένα πακέτο ACK σε κάθε νέο γειτονικό κόμβο και ένα πακέτο ACK είναι ένα μέγεθος κλειδιού και ένα μέγεθος MAC μεγαλύτερο από ένα μήνυμα join

Η ολική επικεφαλίδα καθορίζεαι από την πυκνότητα δικτύων και την κινητικότητα κόμβων.

Τέταρτο, ένας κόμβος στέλνει περιοδικά ένα μήνυμα αναβάθμισης κλειδιών (το οποίο περιλαμβάνει δύο κλειδιά και ένα MAC), και η επικεφαλίδα του εξαρτάται από το διάστημα TESLA. Όσο μεγαλύτερο διάστημα έχει το TESLA τόσο μικρότερη η επικεφαλίδα

6.22.4Παράδειγμα

Υποθέτουμε ότι χρησιμοποιούμε 10 bytes για ένα κλειδί (συμπεριλαμβανομένης μιας ταυτότητας κλειδιού 2-bytes), 10 bytes για το MAC, 500 bytes κατά μέσον όρο για ένα πακέτο κυκλοφορίας, 256 bytes για ένα δημόσιο πιστοποιητικό κλειδί, 128 bytes (1024 bits RSA) για μια ψηφιακή υπογραφή. Υποθέτουμε ότι ένας κόμβος ενώνει το δίκτυο για μια ώρα, κατά τη διάρκεια της

οποίας στέλνει (ή διαβιβάζει) 1000 πακέτα και αντιμετωπίζει 100 κόμβους. Εάν το διάστημα lTESLA είναι 1 sec, τα bytes κυκλοφορίας επικεφαλίδος είναι 44 bytes/s. Εάν χρησιμοποιούμε 2 sec για το διάστημα TESLA, τα γενικά έξοδα ψηφιολέξεων κυκλοφορίας είναι 29 bytes/s. Πιστεύουμε ότι αυτή επικεφαλίδα είναι λογική για μια υπηρεσία ασφάλειας.

6.22.5Αναλογία παράδοσης κυκλοφορίας

Καθορίζουμε αυτήν ως αναλογία του αριθμού πακέτων κυκλοφορίας που ένας κόμβος δέχεται στο συνολικό αριθμό πακέτων που λαμβάνει από τους γειτονικούς του.

Στο LHAP, ένας κόμβος θα μπορούσε να πετάξει πακέτα κυκλοφορίας που είναι από τους νόμιμους γείτονες σε δύο σενάρια.

Το πρώτο σενάριο προκύπτει όταν αντιμετωπίζει έναν γείτονα για πρώτη φορά, και το δεύτερο σενάριο προκύπτει όταν αυτό ξανααντιμετωπίζει έναν γειτονικό του μετά από περισσότερα από ένα ,διαστήματα TESLA που έχουν παρέλθει από την τελευταία σύγκρουσή τους. Και στις δύο περιπτώσεις, θα πετάξει τα πακέτα από αυτόν τον γειτονικό του εάν αυτός μεταδίδει πακέτα μέχρι αυτό να λαβει ένα έγκυρο μήνυμα ACK ή το μήνυμα αναβάθμισης κλειδιών από αυτόν τον γειτονικό του μέσα σε ένα διάστημα TESLA.

Επομένως, η αναλογία παράδοσης κυκλοφορίας επηρεάζεται κυρίως από το διάστημα TESLA, το ποσοστό κυκλοφορίας, και το πρότυπο κινητικότητας κόμβων.

Η ανωτέρω ανάλυση απόδοσης παρουσιάζει ότι το LHAP είναι ένα ελαφρύ πρωτόκολλο ασφάλειας και από την άποψη του υπολογισμού και της επικοινωνίας.

6.22.6Αλληλεπίδραση με τα πρωτόκολλα δρομολόγησης

Το LHAP είναι ανεξάρτητο και βρίσκεται κάτω από τα πρωτόκολλα στρώματος δικτύων. Στην πράξη, θα μπορούσε να εκμεταλλευθεί το αναπτυγμένο πρωτόκολλο δρομολόγησης δικτύων για να επιτύχει την καλύτερη αποτελεσματικότητα.

Μερικά από τα ειδικά πρωτόκολλα δρομολόγησης, π.χ., AODV, TORA, απαιτούν κόμβους που περιοδικά ανταλλάσουν πληροφορίες δρομολόγησης ή αναγνωριστικών μηνυμάτων με τους γειτονικούς τους.

Γι’αυτό το LHAP μπορεί να θέσει σε λειτουργία τα μηνύματα αναβάθμισης κλειδιών του σε αυτά τα μηνύματα για να αποφύγει τα μεταδιδόμενα, χωριστά, πακέτα αναβάθμισης κλειδιών, αν και το εύρος ζώνης και η ενέργεια για τη μετάδοση και τη λήψη δεν είναι μειωμένα.

Σημειώνουμε ότι αυτό δεν έχει επιπτώσεις στη διαφάνεια του LHAP όσον αφορά το πρωτόκολλο δρομολόγησης, επειδή το LHAP σε έναν λαμβάνοντα κόμβο αφαιρεί το εγκαταστημένο μήνυμα αναβάθμισης κλειδιών πριν από την υποβολή του μηνύματος στο στρώμα δικτύων.

Δεδομένου ότι κανένα από τα ασφαλή πρωτόκολλα δρομολόγησης που προτείνονται δεν εξετάζει την αυθεντικότητα των πακέτων στοιχείων, το τρέξιμο του LHAP κάτω από αυτά τα πρωτόκολλα θα ενισχύσει περαιτέρω την ασφάλεια ενός ειδικού δικτύου.

Επιπλέον, με την ανάπτυξη του LHAP κάτω από τα (επισφαλή) πολλαπλής διανομής πρωτόκολλα δρομολόγησης που έχουν προταθεί για τα ειδικά δίκτυα, πιστεύουμε ότι πολλές από τις επιθέσεις σε τέτοια πρωτόκολλα που είναι πιθανά από την έλλειψη υποστήριξης για την αυθεντικότητα πακέτων , μπορούν να αποτραπούν.

Γι'αυτό, το σχέδιο των ασφαλών, πολλαπλής διανομής ,πρωτοκόλλων δρομολόγησης θα μπορούσε περισσότερο να στραφεί στη λειτουργία που το LHAP δεν μπορεί να παρέχει, π.χ., την επικύρωση πηγής. Εμείς αναμένουμε ότι αυτό θα οδηγήσει στα πιό ελαφριά ασφαλή πρωτόκολλα δρομολόγησης.

6.22.7Υποστήριξη των πολύ μακριών βασικών αλυσίδων

Στο LHAP, τα κλειδιά TESLA αποκαλύπτονται περιοδικά. Για ένα δίκτυο με μια διάρκεια ζωής πέντε ωρών και το διάστημα TESLA ενός δευτερολέπτου, η βασική αλυσίδα TESLA θα έχει ένα μήκος 5 * 3600 = 18.000 κλειδιά. Αφ' ετέρου, τα κλειδιά κυκλοφορίας καταναλώνονται συνήθως σε ένα πολύ υψηλότερο ποσοστό, ανάλογα με την εφαρμογή.

Κατά συνέπεια, οι πολύ μακριές αλυσίδες κλειδιών απαιτούνται στο LHAP. Το LHAP υιοθετεί το πολλαπλό σχέδιο αλυσίδων κλειδιών που προτείνεται από τον Liu και τον Ning για να δημιουργήσει τις μακριές αλυσίδες κλειδιών.

6.23Συμπεράσματα

Το LHAP, είναι ένα ελαφρύ πρωτόκολλο επικύρωσης hop-by-hop για τον έλεγχο πρόσβασης δικτύου στο δίκτυο ad-hoc.

Το LHAP είναι βασισμένο σε δύο τεχνικές:

i) hop-by-hop αυθεντικότητα για την επιβεβαίωση αυθεντικότητας όλων των πακέτων που διαβιβάζονται στο δίκτυο και

ii) μονόδρομη αλυσίδα κλειδιώνκαι TESLA για την αυθεντικότητα πακέτων και για τη μείωση επικεφαλίδος για την καθιέρωση της εμπιστοσύνης μεταξύ των κόμβων.

Ο σχεδιασμός του LHAP είναι διαφανής και ανεξάρτητος από τα πρωτόκόλλα δρομολόγησης. Κατόπιν τούτου διαπιστώνουμε ότι το LHAP είναι απαραίτητο και συνάμα πρακτικό.

ΚΕΦΑΛΑΙΟ 7ο

ΣΥΜΠΕΡΑΣΜΑΤΑ

Η ασφάλεια είναι ο ακρογωνιαίος λίθος για μια σειρά από εφαρμογές στις οποίες δραστηριοποιούνται τα δίκτυα αισθητήρων, π.χ στις βιοιατρικές, στις στρατιωτικές, στις εφαρμογές βιομηχανικού ελέγχου, και γενικά οπουδήποτε κρίσιμες αποφάσεις στρατηγικού επιπέδου, εξαρτώνται από πληροφορίες οι οποίες συγκεντρώνονται και επεξεργάζονται από αυτά.

Οι κυριότερες απειλές ενάντια στην ασφαλή λειτουργία των δικτύων αισθητήρων είναι: 1) Μη εξουσιοδοτημένη Ακρόαση-Eavesdropping, 2) Εκπομπή λαθεμένων ή επανεκπομπή ετεροχρονισμένωνπαλαιοτέρων μηνυμάτων (Message injection or replay),3) Αντιποίηση και μη εξουσιοδοτημένη μεταβολή των μηνυμάτων (Impersonation & messagemodification) ,και 4) Ανάλυση κίνησης και εκμετάλλευσης παράπλευρων πληροφοριών καναλιού (Traffic-Side channel analysis).

Αφού διαπιστώσαμε την σημασία της ασφάλειας στα δίκτυα αισθητήρων, τις απειλές ανά επίπεδο του OSI, και κάναμε μια επισκόπηση της υπάρχουσας βιβλιογραφίας, παρουσιάσαμε τα πρωτόκολλα ασφαλείας SPINS, SEKEN, INSENS και LHAP.

Και τα τέσσερα πρωτόκολλα εξασφαλίζουν την ασφαλή διακίνηση δεδομένων στα δίκτυα αισθητήρων, βασιζόμενα 1) στην με ισχυρούς αλγόριθμους κρυπτογράφηση των δεδομένων, 2) στην χρήση μεθόδων συμμετρικής κρυπτογραφίας για την μετάδοση των κρυπτογραφημάτων, και 3) στην μεγάλη αντοχή των κόμβων σε επιθέσεις-προσπάθειες φυσικής παραβίασης τους.

Κατά την εξέταση των πρωτοκόλλων δείξαμε τους παράγοντες που επηρεάζουν την επιλογή ενός αλγόριθμου κρυπτογράφησης και καταδείξαμε την αδυναμία χρησιμοποίησης στα δίκτυα αισθητήρων με λγόριθμους ασύμμετρης κρυπτογράφησης.

Ολοκληρώνοντας, δείξαμε γενικά ένα δίκτυο αισθητήρων για να είναι σε θέση να μπορεί να παρέχει ασφαλείς υπηρεσίες πρέπει να χρησιμοποιεί ασφαλή πρωτόκολλα, τεχνικές διαμόρφωσης εύρους φάσματος για την εκπομπή των μηνυμάτων, να υλοποιούνται σε αυτό ισχυροί αλγόριθμοι κρυπτογράφησης, και τέλος να έχει κόμβους ανθεκτικούς ενάντια σε τυχόν προσπάθειες φυσικής παραβίασης τους.

ΑΝΑΦΟΡΕΣ

(1) Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, ΄΄A survey on Sensor Networks΄΄, IEEE Communications Magazines, August 2002

(2) Ian F.Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci,΄΄Wireless Sensor Networks:A Survey΄΄.Computer Networks (Elsevier), March 2002

(3) G.J Pottie and W.J Kaiser,΄΄Wireless Integrated Network Sensors΄΄.Communications of Theach, May 2000.

(4) Vivek Mhatre,Catherine Rosenberg,΄΄Design guidelines for Wireless sensor networks: communication,clustering and aggregation, Computer Networks (Elsevier),Julie 2003

(5) Jessica Feng, Farinaz Koushanfar, and Miodrag Potkonjak,΄΄ System-Architectures for Networks Issues, Alternatives, and Directions΄΄IEEE International Conference on Computer Design, 2002

(6) Fei Hu, Neeraj K. Sharma, ΄΄Security considerations in ad hoc sensor networks΄΄Computer Science (Elsevier),September 2003

(7) Adrian Perrig, John Stankovic, and David Wagner ΄΄Security in Wireless Sensor Networks΄΄ Communications of the ACM ,June 2004

(8) Steve H. Weingart ΄΄Physical Security Devices for Computer Subsystems:A Survey of Attacks and Defenses΄΄,Springer-Verlag Berlin Heidelberg 2000

(9) Chris Karlof, David Wagner,΄΄ Secure routing in wireless sensor networks:attacks and countermeasures΄΄,Computer Science (Elsevier),2003

(10) Hagai Bar-El,΄΄Introduction to Side Channel Attacks΄΄,Discretix Technologies

(11) Kamran Jamshaid, Loren Schwiebert, ΄΄SEKEN (Secure and Efficient Key Exchange for Sensor Networks),National Science Foundation

(12) Adrian Perrig, Robert Szewczyk, J.D Tygar,Victor Wen, and David E.Culler,΄΄SPINS: Security Protocols for Sensor Networks,Kluwer Academic Publishers 2002

(13) Sencun Zhu, Shouhuai Xu, Sanjeev Setia, Sushil Jajodia, ΄΄LHAP: A Lightweight Hop-by-Hop Authentication Protocol for Ad-Hoc Networks, IEEE International Conference on Distributed Computing Systems Workshops,2003

(14) Jing Deng , Richard Han ,and Shivakant Mishra,΄΄ A Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks΄΄, Springer-Verlag Berlin Heidelberg 2003