ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Επισκόπηση θεμάτων ασφαλείας και ακεραιότητας δεδομένων σε Δίκτυα Αισθητήρων

ΓΕΩΡΓΑΚΟΠΟΥΛΟΣ ΙΩΑΝΝΗΣ
ΝΙΚΟΛΑΚΟΠΟΥΛΟΣ ΑΛΕΞΙΟΣ

ΕΠΙΒΛΕΠΩΝ: ΒΑΣΙΛΕΙΟΣ ΤΣΑΚΑΝΙΚΑΣ, Επιστημονικός συνεργάτης

ΑΝΤΙΡΡΙΟ 2015

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή.

Αντίρριο, 21 Ιουλίου 2015

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Ονοματεπώνυμο, Υπογραφή
2. Ονοματεπώνυμο, Υπογραφή
3. Ονοματεπώνυμο, Υπογραφή

Περίληψη

Στις μέρες μας η «βιομηχανία» των ασύρματων κινητών τηλεπικοινωνιών βρίσκεται σε μια διαρκή μεταβολή και ενσωματώνει διαρκώς όλο και μεγαλύτερο αριθμό υπηρεσιών.
Είδαμε συγκεκριμένα, τρόπους ασφάλειας ασυρμάτων δικτύων, και για την αναγκαιότητα της ύπαρξης ασφάλειας στα ασύρματα δίκτυα. Αφού ερευνήσαμε τα πρωτόκολλα που χρησιμοποιούνται στα ασύρματα δίκτυα και τα πρωτόκολλα που χρησιμοποιούνται στους ασύρματους αισθητήρες, καταγράψαμε τα χαρακτηριστικά τους καθώς και κάναμε θεωρητική σύγκριση των πρωτοκόλλων αυτών .
Σε πειραματικό επίπεδο μελετήσαμε τις ανάγκες κατανάλωσης ενέργειας ενός ασυρμάτου δικτύου λαμβάνοντας υπόψη μας, αν ευνοεί ή όχι το κανάλι την επικοινωνία των κόμβων. Δηλαδή αν έχουμε μεγάλο αριθμό σφαλμάτων ή όχι.
Έγινε έλεγχος αποτελεσμάτων, και από αυτά τα αποτελέσματα βγάλαμε συμπεράσματα για το πόση ενέργεια καταναλώνεται, ανάλογα με το επίπεδο κρυπτογράφησης.
Έτσι, μπορούμε να κρίνουμε ποιό επίπεδο ασφάλειας χρειάζεται, ανάλογα με τις ανάγκες και τις δυνατότητες του δικτύου μας.

Abstract

In recent years, the wireless mobile telecommunication industry is constantly evolving and changing, adapting new technologies and offering a constantly higher amount of services to its customers.
We examined methods of ensuring a secure mobile network connection, and the necessity of the existence of security itself, in wireless networks. After researching the protocols commonly used in wireless communication networks and the ones used in sensor networks we took notes of their characteristics, and made a theoretical comparison between those protocols.
On an experimental level we analyzed the needs of energy consumption of a wireless network. We took into consideration if the channel supports or not a healthy communication between the nodes, basically if we have a high error rate or not.
There was a result check, and conclusions were arrived at, on the subject of how much energy is consumed, depending on the level of cryptography.
That way, we can judge which security level is required based on the network needs and capabilities.

Περιεχόμενα

1. Ιστορική Αναδρομή στα Δίκτυα Κινητής Τηλεφωνίας Καθώς και Χρονολογική Ανάπτυξη Τεχνολογίας Ασυρμάτων Δικτύων..... 5

1.1 Στοιχεία Αναφορικά με την Ανάπτυξη των Ασύρματων Κινητών Τηλεπικοινωνιών στις μέρες μας Παγκοσμίως.....5
1.2 Τεχνολογία που Χρησιμοποιείται στις μέρες μας για την Ανάπτυξη των Ασύρματων Κινητών Τηλεπικοινωνιών 8
1.3 Ιστορική Αναδρομή στην Ανάπτυξη Τεχνολογίας Ασυρμάτων Δικτύων και Ποιότητα Παροχής Υπηρεσιών 9

2. Ασφάλεια Ασυρμάτων Δικτύων..... 12

2.1 Ορισμός Ασφάλειας Ασυρμάτων Δικτύων 12
2.2 Αναγκαιότητα Ασφάλειας Δικτύων 13
2.3 Ορισμός, Υλοποίηση, Δομές και Πρωτόκολλα στα Δίκτυα Αισθητήρων.....14
2.3.1 Ορισμός Δικτύων Αισθητήρων 14
2.3.2 Υλοποίηση Δικτύων Αισθητήρων 15
2.3.3 Πρωτόκολλα και Δομές στα Δίκτυα Αισθητήρων..... 16
2.4 Χρήση Ασφάλειας Δικτύων.....26

3. Πρωτόκολλα που Χρησιμοποιούνται στην Ανάπτυξη Δικτύων Αισθητήρων..... 27

3.1 Πρωτόκολλα Δικτύων Αισθητήρων.....27
3.2 Περιγραφή Πρωτοκόλλων 29
3.2.1 SPINS..... 29
3.2.2 TINYSEC..... 30
3.2.3 LEAP..... 32
3.2.4 ZigBee 34
3.2.5 SM (Security Manager)..... 35
3.3 Συγκεντρωτικός Πίνακας Περιγραφής Πρωτοκόλλων Ασφάλειας Δικτύων 35
3.4 Θεωρητική Σύγκριση Πρωτοκόλλων.....36

4. Πειραματικές Μετρήσεις..... 37

4.1 Εισαγωγή.....37
4.2 Δομή Δικτύου.....38
4.3 Πίνακας Γειτνίασης.....41
4.4 Πρωτόκολλο Flooding 42
4.5 Κανάλι.....43
4.6 Μέγεθος Πακέτων.....45
4.7 Πειραματικά Αποτελέσματα.....46
4.8 Συμπεράσματα 49

4.9 Επεκτάσεις-Ανοικτά Ζητήματα 50
Βιβλιογραφία..... 51

Διαδικτυακές Πηγές.....52

Εισαγωγή

1. Ιστορική Αναδρομή στα Δίκτυα Κινητής Τηλεφωνίας Καθώς και Χρονολογική Ανάπτυξη Τεχνολογίας Ασυρμάτων Δικτύων

1.1 Στοιχεία Αναφορικά με την Ανάπτυξη των Ασύρματων Κινητών Τηλεπικοινωνιών στις μέρες μας Παγκοσμίως

Στις μέρες μας ότι η «βιομηχανία» των ασύρματων κινητών τηλεπικοινωνιών βρίσκεται σε μια διαρκή μεταβολή και ενσωματώνει διαρκώς όλο και μεγαλύτερο αριθμό υπηρεσιών. Οι υπηρεσίες αυτές προσφέρονται από διαρκώς αυξανόμενους σε πλήθος παρόχους (providers), ενώ εκρηκτική είναι και η αύξηση του αριθμού των συνδρομητών. Ενδεικτικό είναι ότι στο τέλος του έτους 2000, ο αριθμός των συνδρομητών κινητής τηλεφωνίας ξεπέρασε τα 700 εκατομμύρια, ενώ περισσότερα από 8 δισεκατομμύρια μηνύματα στάλθηκαν μόνο κατά το μήνα Ιούνιο του ίδιου έτους. (1)

Στην Ιαπωνία, η υπηρεσία i-mode είχε το έτος 2001 περίπου 17 εκατομμύρια συνδρομητές, με ρυθμό αύξησης 1 εκατομμύριο το μήνα. Η γνωστή εταιρεία Sony-Ericsson εκτιμούσε το 2001 ότι στο τέλος του 2005 θα υπήρχαν πάνω από 1,6 δισεκατομμύρια χρήστες, από τους οποίους 1 δισεκατομμύριο θα χρησιμοποιούν τις υπηρεσίες κινητού Διαδικτύου (mobile Internet). Στην πραγματικότητα οι ρυθμοί ανάπτυξης ήταν αρκετά μεγαλύτεροι με αποτέλεσμα στο 3ο τετράμηνο του 2005, το πλήθος των χρηστών υπηρεσιών κινητής τηλεφωνίας να έχει ξεπεράσει τα 2 δισεκατομμύρια. (2)

Τα σημαντικότερα αίτια είναι η γεωγραφική εξάπλωση των σχετικών υποδομών, η σημαντική μείωση του κόστους αλλά και η βελτίωση της ποιότητας των προσφερόμενων υπηρεσιών. Η κινητή τηλεφωνία στον Ευρωπαϊκό χώρο ξεκίνησε στη Γερμανία το 1958 με το αναλογικό δίκτυο A-Netz χρησιμοποιώντας τη συχνότητα των 160 MHz. Το 1971 το σύστημα αυτό κάλυπτε γεωγραφικά το 80% και

είχε 11.000 συνδρομητές. Το 1972 το παραπάνω δίκτυο εξελίχθηκε στο B-Netz χρησιμοποιώντας την ίδια συχνότητα. Το εν λόγω σύστημα ήταν επίσης διαθέσιμο στην Αυστρία, Λουξεμβούργο και Ολλανδία, ενώ μόνο στη Δυτική Γερμανία το 1979 είχε 13.000 συνδρομητές.

Οι συσκευές (πομπός και δέκτης), λόγω του βάρους τους, ήταν συνήθως εγκατεστημένες μέσα σε κάποιο αυτοκίνητο. Το ίδιο διάστημα στις Βόρειες Ευρωπαϊκές χώρες (Δανία, Νορβηγία, Φιλανδία και Σουηδία) αναπτύχθηκε το αναλογικό σύστημα NMT (Nordic Mobile Telephone) στη συχνότητα των 450 MHz. Αρκετά ακόμη αναλογικά συστήματα κινητής τηλεφωνίας αναπτύχθηκαν μέχρι το 1980 στον Ευρωπαϊκό χώρο, τα οποία όμως χρησιμοποιούσαν τελείως διαφορετικά και ασύμβατα πρότυπα. Τα παραπάνω συστήματα είναι γνωστά ως η 1η γενιά κινητών επικοινωνιών (1G). (1)

Οι Ευρωπαϊκές χώρες συμφώνησαν να αναπτύξουν ένα πανευρωπαϊκό σύστημα ή πρότυπο κινητής τηλεφωνίας το 1982. Το νέο σύστημα θα χρησιμοποιούσε το νέο φάσμα των 900 MHz και θα επέτρεπε τη μεταγωγή κλήσεων μεταξύ των Ευρωπαϊκών χωρών. Επιπλέον, θα ήταν πλήρως ψηφιακό και θα πρόσφερε τόσο φωνητικές όσο και υπηρεσίες δεδομένων. Το αποτέλεσμα αυτής της προσπάθειας κατέληξε στο σύστημα δεύτερης γενιάς κινητών επικοινωνιών (2G) ευρύτερα γνωστό ως GSM (Global System for Mobile Communication).

Το GSM βασίζεται στην τεχνολογία Time Division Multiple Access (TDMA), λειτουργεί στις συχνότητες των 900 και 1800 MHz και ξεκίνησε τη λειτουργία του το έτος 1991. Τα συστήματα 2G πρόσφεραν και συνεχίζουν να προσφέρουν μεγαλύτερη χωρητικότητα (capacity) δικτύου, χαμηλότερα κόστη στους παρόχους, ενώ χαμηλού ρυθμού (low-rate) υπηρεσίες δεδομένων προστέθηκαν στις φωνητικές υπηρεσίες. Ένα άλλο πλεονέκτημα των συστημάτων GSM είναι η ευρεία - σε όλο σχεδόν τον πλανήτη - δυνατότητα περιαγωγής (roaming). Άλλα συστήματα 2G, εκτός του GSM, είναι τα TDMA, Personal Digital Cellular (PDC) και cdma One.

Το PDC χρησιμοποιείται στην Ιαπωνία, ενώ όλα τα υπόλοιπα συμπεριλαμβανομένου και του GSM, λειτουργούν στις Ηνωμένες Πολιτείες. Η

εξέλιξη των συστημάτων 2G ώστε να συμπεριλάβουν υπηρεσίες δεδομένων (packet-switched data services) έγινε γνωστή και ως 2.5 γενιά κινητών επικοινωνιών (2.5G). Στα συστήματα GSM η υπηρεσία δεδομένων ονομάζεται General Packet Radio Service (GPRS). Θεωρητικά, το GPRS μπορεί να προσφέρει ρυθμούς δεδομένων που φτάνουν τα140.8 kbit/s, αν και τυπικά η απόδοσή του δεν ξεπερνά τα 56 kbit/s - περίπου 20Kbit/s για κάθε χρονοθυρίδα (time slot). Συμπληρωματικά η τεχνολογία E-GPRS ή πιο απλά Enhanced Data rates for Global Evolution (EDGE) αποτελεί μια εξέλιξη του GPRS που βασίζεται σε νέα εξελιγμένα σχήματα κωδικοποίησης (coding schemes).

Με την τεχνολογία αυτή οι πραγματικοί ρυθμοί μετάδοσης μπορούν να φτάσουν στην πράξη τα 180 kbit/s. Τα συστήματα EDGE συχνά αναφέρονται ως συστήματα 2.75G. Το 1992 η Ευρωπαϊκή Ένωση συμφώνησε στην ανάπτυξη του συστήματος τρίτης γενιάς (3G) με το όνομα UMTS (Universal Mobile Telecommunications System) ως Ευρωπαϊκή (& Ιαπωνική) πρόταση στη Διεθνή Ένωση Τηλεπικοινωνιών ITU (International Telecommunication Union) για το IMT-2000 (ITU-R, 2000). Τα συστήματα 3G αναπτύσσονται και προτυποποιούνται από δύο μη κερδοσκοπικούς οργανισμούς γνωστούς ως 3rd Generation Partnership Project (3GPP) και 3GPP2. Ο πρώτος οργανισμός ξεκινώντας το 1998 ασχολείται με την εξέλιξη των συστημάτων GSM, ενώ ο δεύτερος με την εξέλιξη του συστήματος cdma One. (1)

Κοινός στόχος και των δύο οργανισμών είναι η εξέλιξη των δικτύων των παρόχων ώστε να βασίζονται αποκλειστικά στο πρωτόκολλο IP (all-IP). Τα 3G δίκτυα μπορούν να λειτουργήσουν στις μπάντες συχνοτήτων 1885-2025 MHz και 2110-2200 MHz. Ειδικότερα, τα 3GPP δίκτυα εκμεταλλεύονται τις περιοχές συχνοτήτων 1920-1980 και 2110-2170 MHz και βασίζονται στην τεχνολογία Wideband CDMA (W-CDMA). Το πρώτο μεγάλης κλίμακας εμπορικό UMTS δίκτυο ξεκίνησε τη λειτουργία του στην Ιαπωνία το 2001 από την εταιρεία NTT DoCoMo. Περίπου δύο χρόνια μετά στην Ευρωπαϊκή ήπειρο το πρώτο UMTS σύστημα λειτούργησε στην Αυστρία το Δεκέμβριο του 2003 από την T-Mobile.

1.2 Τεχνολογία που Χρησιμοποιείται στις μέρες μας για την Ανάπτυξη των Ασύρματων Κινητών Τηλεπικοινωνιών

Σήμερα, περισσότερα από εξήντα 3G/UMTS δίκτυα που χρησιμοποιούν την W-CDMA τεχνολογία λειτουργούν σε 25 χώρες, ενώ ήδη έχουν διανεμηθεί πάνω από 120 άδειες λειτουργίας. Παραδείγματος χάριν, στη Γερμανία οι εταιρείες που απέκτησαν τη σχετική UMTS άδεια δαπάνησαν όλες μαζί το ποσό των 50.8 δισεκατομμυρίων Ευρώ. Ανάμεσα στα πλεονεκτήματα των UMTS δικτύων ξεχωρίζουμε τους αυξημένους ρυθμούς μετάδοσης των δεδομένων και την ταυτόχρονη υποστήριξη μεγαλύτερου όγκου δεδομένων και φωνής. Πιο συγκεκριμένα, το UMTS δίκτυο στην αρχική του φάση, θεωρητικά προσφέρει ρυθμούς μετάδοσης δεδομένων έως και 384 kbit/s σε περιπτώσεις όπου παρατηρείται αυξημένη κινητικότητα του χρήστη (vehicular). Αντίθετα, όταν ο χρήστης είναι πεζός (pedestrian) ή καλύτερα παραμένει ακίνητος, οι ρυθμοί μετάδοσης αυξάνουν κατά πολύ πλησιάζοντας την θεωρητική τιμή των 2 Mbit/s (1920 kbit/s) (2) (3).

Χαρακτηριστικό είναι το γεγονός ότι στην Ιαπωνία βρίσκονται ήδη σε φάση προετοιμασίας αναβαθμίσεις του συστήματος στα 3 Mbit/s. Εκτιμάται δε ότι στο μέλλον θα υπάρξει περαιτέρω αύξηση των ρυθμών μετάδοσης δεδομένων. Ήδη, ο 3GPP έχει θέσει σαν πρότυπα (standard) δύο νέες τεχνολογίες. Πρόκειται για το High Speed Downlink Packet Access (HSDPA) – γνωστό και ως 3.5 G - και το High Speed Uplink Packet Access (HSUPA) αντίστοιχα. Οι συγκεκριμένες τεχνολογίες ουσιαστικά αποτελούν εξέλιξη του UMTS, αφού υπόσχονται ρυθμούς μετάδοσης των δεδομένων έως και 14,4 Mbit/s στο downlink και 5.8 Mbit/s στο uplink.

Όπως ήδη αναφέρθηκε, τα συστήματα ασύρματων κινητών επικοινωνιών αντιμετωπίζουν περισσότερες απειλές σε σχέση με τα ενσύρματα. Επίσης, τα συστήματα 3G θα είναι βασισμένα αποκλειστικά στο πρωτόκολλο IP (all-IP).Παράλληλα, σε εξέλιξη βρίσκονται ερευνητικές προσπάθειες για την πλήρη ενοποίηση όλων των ασύρματων και ενσύρματων συστημάτων διαφορετικών (ετερογενών) τεχνολογιών σε ένα κοινό περιβάλλον, με στόχο την παροχή υψηλής ποιότητας υπηρεσιών στους συνδρομητές ανεξάρτητα από τη γεωγραφική περιοχή που αυτοί θα κινούνται.

Αυτή η προοπτική εξέλιξης - προς την ενοποίηση των συστημάτων επικοινωνίας - είναι γνωστή ως η 4η γενιά κινητών επικοινωνιών (4G). Ταυτόχρονα όμως, η ανάπτυξη και εξέλιξη των συστημάτων 3G σε αυτά της τέταρτης γενιάς (4G) αναμένεται να οξύνει πολύ περισσότερο αυτή την κατάσταση. Οι μελετητές της ασφάλειας των συστημάτων αυτών τονίζουν την ανάγκη για νέες ή βελτιωμένες τεχνικές και μεθόδους προστασίας, αναγνωρίζοντας τις επικείμενες απειλές. (3)

1.3 Ιστορική Αναδρομή στην Ανάπτυξη Τεχνολογίας Ασυρμάτων Δικτύων και Ποιότητα Παροχής Υπηρεσιών

Στον πίνακα 1 παρουσιάζονται τα σημαντικότερα γεγονότα στον τομέα των τηλεπικοινωνιών:

Χρονιά	***Γεγονότα***
1821	Το πρώτο μικρόφωνο γεννιέται
1830	Μετάδοση πρώτου ηλεκτρικού σήματος
1843	Επινόηση ΦΑΞ
1844	Πρώτη γραμμή τηλεγράφου
1858	Πρώτο Υπερατλαντικό Καλώδιο Τηλεγράφου
1861	Οι ΗΠΑ ενώνονται πλέον με τηλέγραφο από τη μια άκρη στην άλλη
1865	Πρόβλεψη με μαθηματικά από Maxwell για τη μετάδοση Η/Μ κυμάτων
1870	Πολυπλεξία στην τηλεγραφία από Thomas Edison
1874	Αρχή λειτουργίας τηλεφώνου από Alexander Graham Bell
1876	Πρώτη πατέντα τηλεφώνου
1877	Τοποθέτηση πρώτης μόνιμης εξωτερικής γραμμής τηλεφώνου
1878	Πρώτο εμπορικό τηλεφωνικό κέντρο στο κόσμο
1880	Ίδρυση American Bell Telephone Company και τα πρώτα pay stations στη Ν/Υ
1884	Πρώτη τηλεφωνική κλήση μεγάλης απόστασης
1885	Δημιουργία της AT&T ως θυγατρική της American Bell Telephone Company
1893	Πρώιμη μορφή ραδιοφωνικής μετάδοσης
1895	Ο G. Marconi εφεύρε τον ασύρματο
1902	Κατασκευή Τελ. κέντρου μηχανικής μεταγωγής γραμμής από AT&T

1903	Πρώτα τηλέφωνα κερματοδέκτη στην Ν/Υ
1904	Πρώτος αυτόματος τηλεφωνητής
1914	Πρώτη τηλεφωνική κλήση μεταξύ δύο ηπείρων
1915	Εφευρέθηκε το ηλεκτρικό μεγάφωνο
1919	Εφευρέθηκε το ραδιόφωνο μικροκυμάτων
1920	Πρώτη εγγραφή ηλεκτρονικού ήχου με επιτυχία
1921	Κατασκευή πρώτου ταλαντωτή με χαλαζία και η πρώτη αποστολή εικόνας
1922	Ίδρυση British Broadcasting Corporation (BBC)
1923	Μια εικόνα σπασμένη σε κουκίδες στέλνεται ενσύρματα
1924	Εικόνες μεταδίδονται πάνω σε τηλεφωνικές γραμμές
1925	Ίδρυση Bell Telephone Laboratories
1929	Καταγραφή ήχου σε μαγνητική ταινία και Επίδειξη έγχρωμης τηλεόρασης
1930	Δοκιμές για εικονοτηλέφωνο από AT&T
1931	Ραδιοαστρονομία
1933	Επίδειξη διαμόρφωσης συχνότητας από Edwin Armstrong
1934	Κατασκευή πρώτης συσκευής καταγραφής ήχου σε μαγνητική ταινία
1937	Κατασκευή Ηλ. Αριθμομηχανής και Φωτοτυπικού
1940	Εισαγωγή τηλεφωνικών συστημάτων μεγάλου εύρους ζώνης
1942	Κατασκευή πρώτου ηλεκτρονικού ψηφιακού υπολογιστή
1946	Κατασκευή ENIAC
1947	Κατασκευή Transistor
1949	Η δικτυακή τηλεόραση ξεκινά να εκπέμπει στις Η.Π.Α.
1951	Οι Η/Υ πωλούνται στο εμπόριο
1952	Έγχρωμες μεταδώσεις τηλεόρασης
1956	Πρώτες ενσύρματες υπερατλαντικές κλήσεις
1958	Μετάδοση δεδομένων πάνω από τις τηλεφωνικές γραμμές
1959	Εφεύρεση microchip
1960	Εφεύρεση Lazer
1961	Πρώτα πειράματα για επικοινωνία μέσο κυμάτων φωτός
1962	Κατασκευάζεται ο μίνι-υπολογιστής και μετάδοση εικόνων από δορυφόρο
1963	Οι επικοινωνιακοί δορυφόροι τοποθετούνται σε γεωστατική τροχιά
1966	Μεταφορά δεδομένων τηλεφωνικής κλήσης με οπτική ίνα στις Η.Π.Α.
1967	Πρώτα ασύρματα τηλέφωνα
1968	Πλήρη απεικόνιση της γης από Δορυφόρους
1969	Εγκατάσταση ARPANET σε 4 πανεπιστήμια
1970	Χρήση Πολυπλεξίας Χρόνου (TDM) και Κατασκευή δισκέτας (Floppy)
1971	Πρώτος μικροεπεξεργαστής, πρώτο FAX, πρώτος Text Editor (Word)
1972	Εφεύρεση Ψηφιακής Τηλεόρασης, Διεθνές Συνδέσεις ARPANET

1973	Επινόηση του Ethernet από τον Bob Metcalfe
1974	Δημοσιοποίηση TCP, Teletext από BBC, Πρώτη αριθμομηχανή τσέπης
1975	Εκτυπωτές Lazer από IBM
1978	Διαχώριση πρωτοκόλλου TCP σε TCP και IP
1979	Πρώτο ραδιοκασετόφωνο, Πρώτο κυψελωτό δίκτυο κινητής στην Ιαπωνία
1980	Αύξηση χωρητικότητας των microchip, Πρώτος Υπολογιστής τσέπης
1981	IBM PC, MS-DOS από Microsoft, Πρώτος φορητός Η/Υ, Πρώτο Ποντίκι
1982	Εγκαθιδρύεται το πρωτόκολλο TCP/IP
1983	AT&T Διαλύεται, Δοκιμές Τεχνολογίας ISDN στην Ιαπωνία
1984	32-bit CPU, 1MB Memory Chip, Εισαγωγή DNS
1985	Μεγάλη εξάπλωση κυψελωτών τηλεφώνων στα αυτοκίνητα
1986	Εγκαθιδρύεται το NSFNET για 5 υπερυπολογιστές
1987	Η γη χαρτογραφείται πλήρως από το διάστημα
1988	Πρώτο Υπερατλαντικό Καλώδιο Οπτικών Ινών
1989	Επινοείτε το WWW, Παρουσίαση Τηλεόρασης Υψηλής Ευκρίνειας
1990	Πρώτη μηχανή αναζήτησης Gopher
1991	Το PGP(Pretty Good Privacy) μοιράζεται ως Freeware
1992	Η φράση "Σερφάρω στο Ιντερνέτ" πλάστηκε από την Jean Armour Polly
1993	Εισαγωγή IPv4, DSL ως πρότυπο, Pentium CPU, Εξάπλωση των Worms
1994	Ίδρυση W3 - World Wide Web Consortium
1995	Παρουσίαση προτύπων USB
1996	Ξεκινά η προτυποποίηση 1000Base-T για 1Gbps Ethernet
1997	DVD, Pentium II, Μετάδοση Real Time εικόνων από διάστημα από NASA
1998	Ίδρυση Google, Παρουσίαση Intel Celeron, Ανάπτυξη προτύπου Bluetooth
1999	Pentium III, Αναβάθμιση Δικτύου κορμού Η.Π.Α. στα 2.5Gbps
2000	Μαζικές DoS, Πάνω από 1 δισ. Ιστοσελίδες, Δοκιμή πρωτοκόλλου IPv6
2001	Πρώτη μετάδοση στην τηλεόραση Υψηλής Ευκρίνειας
2002	Το Internet2 συγκεντρώνει 200 Πανεπιστήμια, 60 επιχειρήσεις και 40 μέλη

Πίνακας 1: Ιστορική Αναδρομή

2. Ασφάλεια Ασυρμάτων Δικτύων

2.1 Ορισμός Ασφάλειας Ασυρμάτων Δικτύων

Ως ορισμό της Ασφάλειας Δικτύου, μπορούμε να πούμε ότι σχετίζεται με την ικανότητα ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του, δηλαδή την υποκλοπή των δεδομένων. Εκτός αυτού, θεωρείται ως η δυνατότητα ενός δικτύου ή συστήματος πληροφοριών να αντισταθεί, σε δεδομένο επίπεδο αξιοπιστίας, σε τυχαία συμβάντα ή κακόβουλες ενέργειες που θέτουν σε κίνδυνο τη διάθεση, την ακεραιότητα και την τήρηση του απορρήτου των δεδομένων που έχουν αποθηκευτεί ή μεταδοθεί είτε είναι προσβάσιμες μέσω των δικτύων και συστημάτων αυτών. (1)

Η έννοια της ασφάλειας των δικτύων υπολογιστών έχει τρεις βασικές έννοιες:

i. Διαθεσιμότητα (Availability), δηλαδή την ικανότητα να γίνεται εφικτή η προσπέλαση και χωρίς καθυστέρηση των υπηρεσιών ενός δικτύου όταν τις χρειάζεται μία εξουσιοδοτημένη οντότητα.

ii. Εμπιστευτικότητα (Confidentiality), δηλαδή την πρόληψη από μη εξουσιοδοτημένη πρόσβαση σε δεδομένα. Αυτά τα δεδομένα διακινούνται μόνο μεταξύ των υπολογιστών στα οποία μπορούν τα έχουν πρόσβαση τα άτομα που έχουν συγκεκριμένη άδεια. Υποενότητες της εμπιστευτικότητας είναι η ιδιωτικότητα που είναι η προστασία των δεδομένων προσωπικού χαρακτήρα από τρίτους και η μυστικότητα που αφορά το απόρρητο σε οργανισμούς και επιχειρήσεις.

iii. Ακεραιότητα (Integrity). Είναι και η πιο σημαντική από όλες τις παραπάνω έννοιες και αφορά την μη αξιόπιστη μεταβολή των δεδομένων δηλαδή τα

δεδομένα να μην τροποποιούνται χωρίς την απαραίτητη άδεια, συμπεριλαμβανομένης της μη επιτρεπτής δημιουργίας πληροφορίας.

2.2 Αναγκαιότητα Ασφάλειας Δικτύων

Είναι γεγονός ότι, παρά την προφανή της χρησιμότητα, η λήψη των απαραίτητων μέτρων ασφάλειας δημιουργεί πολλές φορές κάποια πρόσθετη επιβάρυνση στην απόδοση και το κόστος λειτουργίας του δικτύου υπολογιστών μιας επιχείρησης. Θα πρέπει ακόμη να αποδεχτούμε το κόστος της ασφάλειας και ως κόστος χρόνου και ως κόστος χρήματος. Συνεπώς, μπορεί να θεωρηθεί ότι η ασφάλεια βρίσκεται σε σχέση αντιστρόφως ανάλογη με την αποδοτικότητα του δικτύου υπολογιστών μιας επιχείρησης. Αυτό όμως δεν είναι σωστό γιατί η ασφάλεια είναι κόστος αναγκαίο για την ομαλή και εύρυθμη λειτουργία του (2).

Το συγκεκριμένο κόστος για την ασφάλεια των δικτύων μιας επιχείρησης εξαρτάται και προκύπτει από την εκάστοτε ακολουθούμενη πολιτική ασφάλειας. Απαιτείται συνεπώς μια πολιτική ασφαλείας η οποία θα πρέπει να εξισορροπεί το κόστος εισαγωγής ασφάλειας από την μία πλευρά και το κόστος ζημιών από πιθανολογούμενο κίνδυνο από την άλλη. Επίσης, θα πρέπει να δημιουργούνται τέτοιες συνθήκες ασφάλειας ώστε να μη παρεμποδίζεται η ευελιξία και η ανάπτυξη της επιχείρησης.

Η αναγκαία πολιτική ασφάλειας καθορίζεται από μία δυναμική εκτίμηση του κόστους των μέτρων ασφάλειας σε σχέση με τις συνέπειες που θα έχει για τον οργανισμό οποιαδήποτε πρόκληση δυσλειτουργίας. Ο βασικός αυτός κανόνας ισχύει για όλους τους τομείς και όλα τα επίπεδα ασφάλειας. Έτσι, σε κάθε περίπτωση όπου απαιτείται η λήψη κάποιου μέτρου ασφάλειας, πρέπει να εξετάζεται η πιθανότητα να συμβεί κάποιο πρόβλημα ασφάλειας, σε σχέση με τις συνέπειες που αυτό θα δημιουργήσει. Εάν η τιμή των δύο αυτών παραμέτρων είναι υψηλή, τότε πρέπει απαραίτητα να ληφθούν μέτρα, ανεξάρτητα από το κόστος πρόληψης. (1)

Τέλος, πρέπει να σημειωθεί ότι η ασφάλεια χαρακτηρίζεται από την φύση της ως δυναμική παράμετρος και όχι στατική, καθώς η τεχνολογία, ο ανταγωνισμός, η πολυπλοκότητα των πληροφοριακών συστημάτων και η ολοένα βελτιούμενη επιτηδειότητα των 'επιτιθέμενων', απαιτούν τη λήψη νέων και συνεχώς αυστηρότερων μέτρων ασφάλειας. Συνεπώς, η ακολουθούμενη πολιτική ασφαλείας θα πρέπει να επανεξετάζεται τακτικά και να διορθώνεται όπου αυτό κρίνεται απαραίτητο. (3)

Παρακάτω αναφέρονται μερικές περιπτώσεις (*μέθοδοι επίθεσης*)που μπορεί να παραβιαστεί η ασφάλεια σε ένα δίκτυο:

i. *Denial-of-Service (DoS)*: Αποστολή περισσοτέρων αιτήσεων σύνδεσης από όσες μπορεί να επεξεργαστεί ένας server
ii. *Μη εξουσιοδοτημένη πρόσβαση (Unauthorized access attacks)*: διάφοροι τρόποι επίθεσης που εμπεριέχουν την ανάκτηση του δικαιώματος εισόδου, εκτέλεσης εντολών, ή ανάκτησης πληροφορίας σε ένα μηχάνημα που δεν παρέχει τέτοιες υπηρεσίες στον επιτιθέμενο<
iii. *Password attacks*: Αποτελεί την μέθοδο εύρεσης ενός password,είτε με επαναληπτικό τρόπο δοκιμάζοντας όλους τους δυνατούς συνδυασμούς, είτε με αποκρυπτογράφηση του password δοκιμάζοντας όλους τους δυνατούς συνδυασμούς των πιθανών κλειδιών κρυπτογράφησης
iv. *Trojan Horses*: Είναι ένα πρόγραμμα που περιέχει η εγκαθιστά μία «κακόβουλη» (malicious) εφαρμογή
v. *Network packet sniffers*: Είναι ένα πρόγραμμα ή μηχάνημα το οποίο μπορεί να υποκλέψει κίνηση που μεταφέρεται από ένα δίκτυο.

2.3 Ορισμός, Υλοποίηση, Δομές και Πρωτόκολλα στα Δίκτυα Αισθητήρων

2.3.1 Ορισμός Δικτύων Αισθητήρων

Ένα Δίκτυο Αισθητήρων είναι μια ομάδα από μετατροπέων σε μία υποδομή επικοινωνιών που προορίζονται να τα παρακολουθούν και να καταγράφουν, διάφορες συνθήκες σε διαφορετικές τοποθεσίες.

Πιο συνήθως, παρακολουθούνται οι παράμετροι που έχουν σχέση με :

i) Θερμοκρασία

ii) Υγρασία

iii) Πίεση

iv) Κατεύθυνση και Ταχύτητα ανέμου

v) Ένταση

α. Φωτισμού

β. Δόνησης

γ. Ήχου

vi) Επίπεδα ρύπων

vii) Παρακολούθηση ζωτικής σημασίας λειτουργιών σώματος (4)

2.3.2 Υλοποίηση Δικτύων Αισθητήρων

Ένα δίκτυο αισθητήρων αποτελείτε από πολλαπλούς σταθμούς ανίχνευσης που ονομάζονται Κόμβοι Αισθητήρων, που ο καθένας είναι φορητός, ελαφρύς και μικρός. Τα δίκτυα αισθητήρων έχουν έξι στοιχεία: μικρό-υπολογιστής ,πομποδέκτης, αποθηκευτικό χώρο, αισθητήρες και συσσωρευτή. Κάθε κόμβος του αισθητήρα έχει ένα αισθητήριο, ένα μικρό-υπολογιστή, ένα πομποδέκτη και μία πηγή φωτός.
Ο μετατροπέας παράγει ηλεκτρικά σήματα που βασίζονται σε φυσικά γεγονότα και φαινόμενα τα οποία "αισθάνεται".
Ο μικρό-υπολογιστής επεξεργάζεται τα δεδομένα και τα αποθηκεύει στην έξοδο του αισθητήρα.
Ο πομποδέκτης, ο οποίος μπορεί να είναι ενσύρματος ή ασύρματος, λαμβάνει εντολές από ένα κεντρικό υπολογιστή και μεταδίδει τα δεδομένα σε αυτόν.
Η ισχύς για κάθε κόμβο αισθητήρα προέρχεται από την ηλεκτρική παροχή ή από μπαταρία.

Πιθανές εφαρμογές των δικτύων αισθητήρων:

I) Βιομηχανικοί αυτοματισμοί

ii) Έξυπνα σπίτια (Smart Houses)

iii) Επίβλεψη

iv) Παρακολούθηση κυκλοφορίας

v) Παρακολούθηση ιατρικών μηχανημάτων
vi) Παρακολούθηση καιρικών συνθηκών
vii) Έλεγχος εναέριας κυκλοφορίας
viii) Έλεγχος Ρομπότ
ix) Ασφάλεια Χώρου / Συναγερμοί (4)

2.3.3 Πρωτόκολλα και Δομές στα Δίκτυα Αισθητήρων

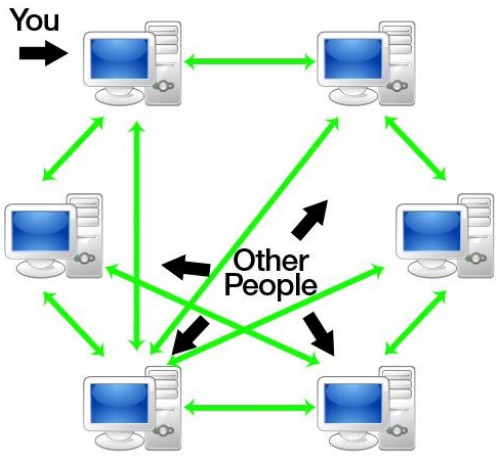
Με την πρόοδο των δικτύων αισθητήρων, δημιουργήθηκαν πολλά πρωτόκολλα τα οποία είναι σχεδιασμένα ειδικά για τα δίκτυα αισθητήρων, ώστε να λαμβάνουν υπόψη τους την κατανάλωση ενέργειας.
Σε ένα περιβάλλον όπου η ενέργεια είναι πολύ σημαντική, το πρωτόκολλο που βοηθάει περισσότερο στην μακροζωία του δικτύου είναι πολύτιμο.
Έχουμε αναγνωρίσει έναν αριθμό χαρακτηριστικών των δικτύων 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, ευρωστία, ευκαμψία, ελαστικότητα σε λάθη και σφάλματα, αυτονομία λειτουργίας και συχνά ασφάλεια και μυστικότητα.
Γενικά. υπάρχουν δύο δομικά στοιχεία στην δομή: αυτά που παράγουν πληροφορία και ονομάζονται πηγές(sources),και από τα στοιχεία που συλλέγουν την πληροφορία από τις πηγές και ονομάζονται αποδέκτες (sinks).Η σύνδεση και ο τρόπος που επικοινωνούν μεταξύ τους, καθορίζουν την τοπολογία του δικτύου. Υπάρχουν τέσσερεις δημοφιλής τοπολογίες:

i. Peer-to-Peer (Ισο προς ίσο)
ii. Star (Αστέρα)
iii. Tree (Δέντρου)
iv. Mesh (Πλέγμα)

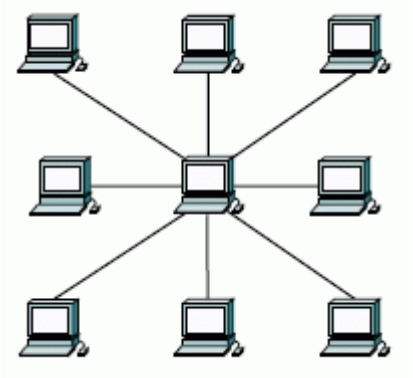
Το peer-to-peer είναι ένα δίκτυο που επιτρέπει στους κόμβους του να μοιράζονται ισοδύναμα τους πόρους τους και να ταυτόχρονα μπορεί να χρησιμοποιήσει τον

αποθηκευτικό χώρο και το bandwidth.Οι κόμβοι μεταξύ τους είναι ίσος προς ίσο – ιξού και το όνομα της τοπολογίας-έχουν δηλαδή τα ίδια δικαιώματα στο δίκτυο και ο κάθε κόμβος έχει πρόσβαση στους υπολοίπους κόμβους. Με τη σειρά τους, τα peer-to-peer χωρίζονται σε I)συγκεντρωτικά peer-to-peer, ii)υποκεντρικά peer-to-peer δίκτυα, iii) peer-to-peer δίκτυα τρίτης γενιάς(με έμφαση την ασφάλεια).



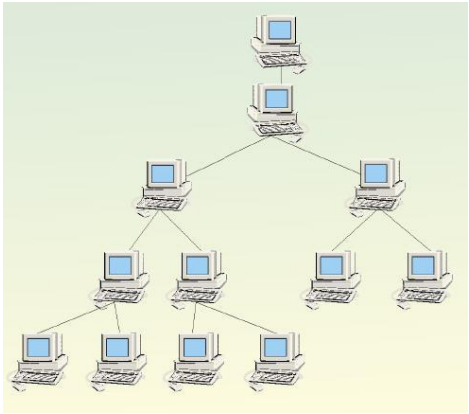
Εικόνα 1: Τοπολογία Peer-to-Peer

Από την άλλη τα δίκτυα αστέρα είναι μία από τις πιο διαδεδομένες τοπολογίες διασύνδεσης. Σε κάθε τέτοια τοπολογία υπάρχει ο κεντρικός κόμβος ο οποίος λειτουργεί σαν μεσολαβητής και μεταφέρει μηνύματα μεταξύ των κόμβων που βρίσκονται γύρω του, μέσο αυτού. Η συγκεκριμένη τοπολογία μειώνει την πιθανότητα δικτύου ενώνοντας όλους τους κόμβους με τον κεντρικό κόμβο. Τα θετικά αυτής της τοπολογίας είναι ότι έχουμε καλύτερη απόδοση αφού η μεταφορά ενός μηνύματος μεταξύ δύο κόμβων θα παρεμβάλλονται πάντα 3 συσκευές και 2 μέσα μεταφοράς. Ένα τέτοιο δίκτυο ,όμως, έχει και αρκετά μειονεκτήματα όπως: το δίκτυο να εξαρτάται εξ ολοκλήρου από τον κεντρικό κόμβο.



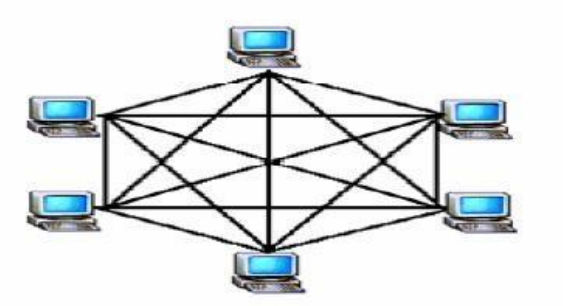
Εικόνα 2: Τοπολογία Αστέρα

Όσο αφορά τώρα τα δίκτυα δέντρου, βρίσκουμε πρώτο στην ιεραρχία το root note μετά πιο κάτω από αυτό είναι τα central hub τα οποία το καθένα ξεχωριστά δημιουργεί μια δική του τοπολογία τύπου αστέρα. Γι' αυτό και ονομάζεται υβριδικό.
Τα πλεονεκτήματα αυτής της τοπολογίας είναι ότι είναι μια πολύ διαδεδομένη τοπολογία, που υποστηρίζεται από πολλούς κατασκευαστές ενώ όλοι οι κόμβοι έχουν πρόσβαση στο δικό τους μικρό δίκτυο αλλά και στο μεγαλύτερο δίκτυο που υλοποιείται από τους γονείς τους. Το μειονέκτημα είναι ότι ολόκληρο το δίκτυο βασίζεται στο κεντρικό κόμβο και αν αυτός καταρρεύσει τότε όλο το δίκτυο καταρρέει.



Εικόνα 3: Τοπολογία Δέντρου

Τέλος, με την τοπολογία του πλέγματος, ο κάθε κόμβος δεν πρέπει να παραλάβει και να διαδώσει τα δικά του δεδομένα μόνο ,αλλά πρέπει να συνεργαστεί με τους υπόλοιπους κόμβους και να λειτουργήσει συνδετικός κρίκος για να υπάρξει συνολική μεταφορά δεδομένων στο δίκτυο. Ο σχεδιασμός τέτοιου είδους δικτύου μπορεί να επιτευχθεί με δύο τρόπους, με καθορισμένη δρομολόγηση ή με πλημμύρισμα του δικτύου.



Εικόνα 4: Τοπολογία Πλέγματος

Η δρομολόγηση στα δίκτυα αισθητήρων είναι σημαντική λόγω των χαρακτηριστικών που τα διακρίνουν από την επικοινωνία του σήμερα και τα ασύρματα δίκτυα. Πρώτον, δεν γίνεται να χτιστεί ένα ενιαίο σχέδιο για την επέκταση του καθαρού αριθμού των κόμβων. Επομένως, τα κλασικά IP πρωτόκολλα δεν μπορούν να εφαρμοστούν στα δίκτυα αισθητήρων. Δεύτερον, σε αντίθεση με τα τυπικά δίκτυα επικοινωνίας ,οι εφαρμογές των δικτύων αισθητήρων απαιτούν τη ροή των ανιχνεύσιμων στοιχείων από τις πολλαπλές περιοχές σε έναν προορισμό. Τρίτον, η παραγόμενη κυκλοφορία δεδομένων έχει πλεονασμό δεδομένου ότι, οι πολλαπλοί αισθητήρες μπορούν να παράγουν τα ίδια στοιχεία κοντά σε ένα φαινόμενο. Ο πλεονασμός δεδομένων πρέπει να επεξεργαστεί από τα πρωτόκολλα δρομολόγησης για να βελτιώσει τη χρησιμοποίηση ενέργειας και του εύρους ζώνης. Τέταρτο, οι κόμβοι αισθητήρων έχουν περιορισμούς από την άποψη της ενέργειας μετάδοσης, της εγκατεστημένης ενέργειας, της επεξεργασίας και αποθήκευσης και απαιτούν έτσι ιδιαίτερη διαχείριση πόρων. Πέμπτο, ανάλογα με το περιβάλλον που εγκαθίσταται οι κόμβοι αισθητήρων, πρέπει να χρησιμοποιούν τις παρακάτω τεχνικές δρομολόγησης: I) ενεργειακά βέλτιστης δρομολόγησης πρωτόκολλα, ii)πρωτόκολλα ενεργειακά ενήμερης δρομολόγησης και iii)λογικής διασποράς κυκλοφορίας πρωτόκολλα.

Τα πρωτόκολλα χωρίζονται επίσης, ανάλογα με τις ιδιότητες τους σε:

i. Ιεραρχικά πρωτόκολλα (Hierarchical Routing-Protocols)
ii. Βασισμένα στη θέση πρωτόκολλα (Location Based Protocols)
iii. Πρωτόκολλα πολλαπλών διαδρομών (Multipath Based Protocols)
iv. Πρωτόκολλα ερωτήσεων (Query Based Protocols)
v. Πρωτόκολλα διαπραγμάτευσης (Negotiation Based Protocols)
vi. Πρωτόκολλα με ποιότητα υπηρεσίας (Quos based protocols)

Παρακάτω παρουσιάζονται τα πιο συνήθεις χρησιμοποιούμενα πρωτόκολλα οποία εκτός του ότι εξελίσσονται συνεχώς, χρησιμοποιούνται σε όλες σχεδόν τις εγκαταστάσεις των κόμβων αισθητήρων, με ή χωρίς παραλλαγές τους.

LEACH: Είναι ένα πρωτόκολλο βασισμένο σε συστάδες που ελαχιστοποιεί την ενεργειακή κατανάλωση στα δίκτυα αισθητήρων. Τα κύρια χαρακτηριστικά του είναι:

i. Τοπικός συντονισμός και έλεγχος για την οργάνωση και τη λειτουργία των συστάδων.
ii. Τυχαία περιστροφή «σταθμών βάσης» της συστάδας ή «επικεφαλής-συστάδας» και οι αντίστοιχες συστάδες.
iii. Τοπική συμπίεση για μείωση της συνολικής επικοινωνίας.

Το LEACH (Low-Energy Adaptive Clustering Hierarchy) είναι ένα αυτό-οργανωμένο, πρωτόκολλο συστάδων που χρησιμοποιεί τυχαία σειρά για να διανείμει το ενεργειακό φορτίο ομοιόμορφα μεταξύ των αισθητήρων στο δίκτυο. Επιπλέον, το LEACH είναι σε θέση να εκτελέσει έναν υπολογισμό σε κάθε συστάδα για να μειώσει το ποσό δεδομένων που πρέπει να διαβιβαστεί στο σταθμό βάσης. Αυτό πετυχαίνει μια μεγάλη μείωση της ενεργειακής κατανάλωσης, δεδομένου ότι ο υπολογισμός είναι πολύ φτηνότερος από την επικοινωνία.
Στα πλεονεκτήματα του, συγκαταλέγονται:

i. Μικρές αποστάσεις μετάδοσης για τους περισσότερους κόμβους
ii. Τοπικός συντονισμός και έλεγχος
iii. Τυχαία περιστροφική εναλλαγή των επικεφαλής συστάδων για την ομοιόμορφη κατανομή του ενεργειακού φορτίου
iv. Τοπική συμπίεση δεδομένων
v. Μείωση της κατανάλωσης ενέργειας κατά 7-8 φορές σε σχέση με την άμεση επικοινωνία και το MTE.
vi. Αύξηση της χρήσιμης διάρκειας ζωής του δικτύου κατά 2 φορές σε σχέση με την άμεση επικοινωνία και το MTE.

Από την άλλη όμως έχει και μειονεκτήματα:

i. Κατά την ανάθεση των επικεφαλής συστάδων δεν λαμβάνεται υπόψη η υπολειπόμενη ενέργεια των κόμβων.
ii. Οι κόμβοι που επιλέγονται επικεφαλής συστάδας καταναλώνουν πολύ ενέργεια

iii. Η συμπίεση των δεδομένων που πραγματοποιείται από τους επικεφαλής συστάδων είναι με απώλειες.
iv. Υπάρχει καθυστέρηση στην μετάδοση των δεδομένων μέσα στις συστάδας λόγω της χρήσεως προγράμματος TDMA.

Εξέλιξη του πρωτοκόλλου αποτελούν τα: ενεργειακά ενήμερη των επικεφαλής Συστάδων (E-LEACH),πρωτόκολλο LEACH δύο επιπέδων (TL-LEACH),πρωτόκολλο Multichip LEACH (M-LEACH),πρωτόκολλα LEACH-C και LEACH-V. (5)

PEGASIS: Το PEGASIS (Power-Efficient Gathering in Sensor Information System) είναι το βελτιωμένο πρωτόκολλο και αποτελεί εξέλιξη του LEACH, όπου μόνο ένας κόμβος επιλέγεται ως κυρίαρχος κόμβος που στέλνει τα συγχωνευμένα δεδομένα στους κόμβους ανά γύρο. Αυτό δημιουργεί έναν παράγοντα βελτίωσης, έναντι του πρωτοκόλλου LEACH.Το πρωτόκολλο έχει ως προϋπόθεση το δίκτυο να έχει το σχηματισμό τύπου αλυσίδας.

Τα πλεονεκτήματα του πρωτοκόλλου έναντι του LEACH είναι:

i. Σε σύγκριση με τον LEACH η απόσταση μετάδοσης για το μεγαλύτερος μέρος των κόμβων μειώνεται στον PEGASIS.
ii. Τα μηνύματα που παραλαμβάνονται από κάθε επικεφαλής κόμβο είναι το πολύ 2 στον PEGASIS, λιγότερα έναντι του LEACH.
iii. Τα πειραματικά αποτελέσματα δείχνουν ότι το PEGASIS παρέχει βελτίωση παράγοντα 2 έναντι του πρωτοκόλλου LEACH για το δίκτυο 50m X 50m και τη βελτίωση παράγοντα 3 για το δίκτυο 100m X 100m.
iv. Δεδομένου ότι κάθε κόμβος επιλέγεται μια φορά, η ενεργειακή κατανάλωση είναι ισορροπημένη μεταξύ των κόμβων αισθητήρων.

Εξέλιξη του πρωτοκόλλου αποτελεί το PEGASIS με κόμβους CDMA,όπου για να μην υπάρχει καθυστέρηση των δεδομένων, χρησιμοποιούνται τόσα πολλά ζευγάρια, όσα είναι δυνατόν σε κάθε επίπεδο. (5)

TEEN: Το TEEN (Threshold sensitive Energy Efficient sensor Network protocol) είναι ένα πρωτόκολλο δικτύου, που στοχεύει τα λεγόμενα <<αντιδραστικά>> δίκτυα, δηλαδή εκείνα τα δίκτυα στα οποία οι κόμβοι αντιδρούν στις απότομες και δραστικές αλλαγές μιας λειτουργίας. Υπό αυτήν την έννοια, είναι κατάλληλο για τις χρονικά κρίσιμες εφαρμογές.

Τα κύρια χαρακτηριστικά γνωρίσματα του πρωτοκόλλου APTEEN είναι:

i. Με την αποστολή περιοδικών δεδομένων, δίνεται στο χρήστη μια πλήρη εικόνα του δικτύου. Ανταποκρίνεται επίσης αμέσως στις δραστικές αλλαγές, καθιστώντας το κατά συνέπεια ότι πρέπει για χρονικά κρίσιμες καταστάσεις. Κατά συνέπεια, συνδυάζει και τις δυναμικές και παθητικές πολιτικές.
ii. Προσφέρει μια ευελιξία επιτρέποντας στο χρήστη να θέτει το χρονικό διάστημα και τις τιμές των κατώτατων ορίων για τις καταστάσεις λειτουργίας.
iii. Η κατανάλωση ενέργειας μπορεί να ελεγχθεί από το χρόνο αρίθμησης και τις τιμές των κατώτατων ορίων.
iv. Το υβριδικό δίκτυο μπορεί να μιμηθεί ένα δυναμικό δίκτυο ή ένα παθητικό δίκτυο, με κατάλληλη ρύθμιση του χρόνου αρίθμησης και τις τιμές των κατώτατων ορίων.

Το κύριο μειονέκτημα αυτού του σχεδίου είναι η πολυπλοκότητα που απαιτείται για να εφαρμόσει τις λειτουργίες των κατώτατων ορίων και το χρόνο αρίθμησης. Εντούτοις, αυτό είναι μια λογική ανταλλαγή και παρέχει πρόσθετη ευελιξία και μεταβλητότητα.
Εξέλιξη του TEEN αποτελεί το APTEEN (Adaptive Periodic Threshold-sensitive Energy Efficient sensor Network protocol), που είναι ουσιαστικά μια υβριδική λειτουργία, με τα δεδομένα να στέλνονται και όταν υπάρχει ανίχνευση της κατάστασης και κατά την αποστολή των καταστάσεων λειτουργιών. (5)

HEED: Το HEED (Hybrid Energy-Efficient Distributed clustering) έχει τους εξής στόχους:

i. Παράταση της διάρκειας ζωής δικτύου με τη κατανομή της κατανάλωσης ενέργειας,
ii. Ολοκλήρωση της διαδικασίας συγκέντρωσης μέσα σε έναν σταθερό αριθμό επαναλήψεων/βημάτων,
iii. Ελαχιστοποίηση των επικεφαλίδων ελέγχου (για να είναι γραμμικό στον αριθμό κόμβων), και
iv. Παραγωγή καλά κατανεμημένων συστάδων και συμπαγείς συστάδες.

Ο στόχος του πρωτοκόλλου είναι να παραταθεί η διάρκεια ζωής του δικτύου. Για αυτόν τον λόγο, η επιλογή επικεφαλής συστάδας είναι βασισμένη ως πρώτο λόγο στην υπολειπόμενη ενέργεια κάθε κόμβου.
Σημειώστε ότι η υπολειπόμενη ενεργειακή μέτρηση δεν είναι απαραίτητη, μιας και η ενέργεια που χρειάζεται για την ανίχνευση, επεξεργασία και την επικοινωνία είναι χαρακτηριστικά γνωστή. Για να αυξηθεί η ενεργειακή αποδοτικότητα και να παραταθεί η διάρκεια ζωής του δικτύου, λαμβάνουμε υπόψη το κόστος επικοινωνίας μέσα στην ομάδα ως μια δευτερεύουσα παράμετρο ομαδοποίησης.
Τα πλεονεκτήματα του συγκεκριμένου πρωτοκόλλου είναι ότι i) ο αριθμός των επαναλήψεων για την ολοκλήρωση του αλγόριθμου είναι ανεξάρτητος από την ακτίνα των συστάδων, ii)η διάρκεια ζωής του δικτύου επεκτείνεται σε σχέση με το gen-LEACH (ο χρόνος που ο πρώτος κόμβος πεθαίνει και ο χρόνος που ο τελευταίος κόμβος πεθαίνει).Το μειονέκτημα του είναι ότι οι δοκιμαστικοί επικεφαλής κόμβοι επιλέγονται τυχαία βασισμένοι στην ενέργεια που τους έχει απομείνει και έτσι δεν μπορεί το πρωτόκολλο να εγγυηθεί τη βέλτιστη επιλογή επικεφαλής του κόμβου, από την άποψη της ενέργειας. (6)

PEDAP: Το PEDAP (Power Efficient Data gathering and Aggregation Protocol), έχει την ιδιότητα να παρατείνει τη διάρκεια ζωής του τελευταίου κόμβου, παρέχοντας μια μεγαλύτερη διάρκεια ζωής στο πρώτο κόμβο, ενώ άλλο πλεονέκτημα αυτού του

πρωτοκόλλου είναι ότι βελτιώνουν τη διάρκεια ζωής του συστήματος ακόμα και αν ο σταθμός βάσης είναι μέσα στον τομέα, ενώ το LEACH και το PEGASIS δεν μπορούν.

Ο κεντρικός στόχος, προκειμένου να μεγιστοποιηθεί η διάρκεια ζωής του δικτύου, πρέπει να είναι να ελαχιστοποιηθεί η συνολική ενέργεια που χρησιμοποιείται στο σύστημα σε έναν κύκλο επικοινωνίας, ισορροπώντας ταυτόχρονα την κατανάλωση ενέργειας μεταξύ των κόμβων. (6)

Πλεονεκτήματα:

i. Καλύτερη απόδοση από το LEACH και το PEGASIS όσον αφορά τον χρόνο που ο πρώτος κόμβος και ο τελευταίος κόμβος πεθαίνουν ανεξάρτητα εάν ο σταθμός βάσης βρίσκεται στο κέντρο του πεδίου ή εκτός.
ii. Καλύτερη απόδοση στην περίπτωση που ο σταθμός βάσης βρίσκεται μέσα στο κέντρο του πεδίου ελέγχου.
iii. Μπορεί να εφαρμοστεί και στην περίπτωση που ο σταθμός βάσης και κάποιοι κόμβοι δεν βρίσκονται σε άμεση επικοινωνία, με την εφαρμογή ενός κατανεμημένου αλγόριθμου ελάχιστου δέντρου ανάπτυξης. Αυξάνεται όμως το κόστος δημιουργία του δέντρου.

Μειονεκτήματα:

i. Γνώση από το σταθμό βάσης, της θέσεως των κόμβων.
ii. Δυνατότητα άμεσης επικοινωνίας με το σταθμό βάσης.
iii. Ο αλγόριθμος είναι συγκεντρωτικός και τον έλεγχο τον έχει ο σταθμός βάσης.

Αλγόριθμος αυτό-οργάνωσης (Self-Organizing Algorithm):

Ο συγκεκριμένος αλγόριθμος, όπως δηλώνει και το όνομα του, βοηθά στην αυτό-οργάνωση ενός συνόλου κόμβων αισθητήρων που διασκορπίζεται τυχαία σε μια περιοχή. Το δίκτυο αποτελείται από δύο τύπους αισθητήρων: i)τους αισθητήρες δρομολογητές που στέλνουν τα δεδομένα και ii)τους εξειδικευμένους αισθητήρες που ανιχνεύουν τα γεγονότα. Οι αισθητήρες δρομολογητές αυτό-διαμορφώνονται σε ένα

δίκτυο χρησιμοποιώντας αυτόν τον αλγόριθμο και οι εξειδικευμένοι αισθητήρες παρακολουθούν μόνο τους κοντινότερους αισθητήρες δρομολογητές που είναι ζωντανοί.

Πλεονεκτήματα:

i. Η ιεραρχία που διαμορφώνεται από τον αλγόριθμο είναι αυστηρά ισορροπημένη.
ii. Η κατάσταση δρομολόγησης που διατηρείται από οποιοδήποτε αισθητήρα δρομολογητή είναι αυστηρώς λογαριθμική υποστηριζόμενη.
iii. Ο αλγόριθμος υπολογίζει αυξητικά ένα γράφημα μετάδοσης ανοικτής εκπομπής που είναι 2-συνδεδεμένο.
iv. Το γράφημα μετάδοσης ανοικτής εκπομπής μπορεί να προσανατολιστεί ως κατευθυνόμενο κυκλικό γράφημα από οποιοδήποτε κόμβο κατά τρόπο μοναδικό.
v. Η ιδιότητα ότι κάθε εξειδικευμένος αισθητήρας συνδέεται με κάποιο αισθητήρα δρομολογητή επιτρέπει σε αυτούς τους αισθητήρες να είναι κινητοί.

Μειονεκτήματα:

i. Ο αλγόριθμος έχει μια αρχική φάση οργάνωσης. Η αρχική οργάνωση είναι καλή για τις εφαρμογές που απαιτούν το διευθυνσιοδότηση ή δρομολόγηση. Ισχύει πολύ στα σενάρια όπου η φάση συντήρησης δεν είναι πολύ δαπανηρή.
ii. Η διαμόρφωση μιας ιεραρχίας σε περιπτώσεις όπου υπάρχουν πολλοί κόμβοι περικοπών στο δίκτυο δεν θα ήταν μια καλή ιδέα. Αυτό θα αύξανε την πιθανότητα της φάσης αναδιοργάνωσης.
iii. Ο αλγόριθμος δεν έχει προϋποθέσεις όσο αφορά το πρωτόκολλο που απαιτείται για τη διαβίβαση των στοιχείων από έναν κόμβο σε έναν άλλο κόμβο. Συγκεκριμένα, δεν αντιμετωπίζει το ζήτημα όταν πρέπει ένας κόμβος να διαβιβάσει πληροφορίες σε έναν άλλο κόμβο. (6)

SHPER: Το μοντέλο του πρωτοκόλλου SHPER (Scaling Hierarchical Power Efficient Routing) υποθέτει τη συνύπαρξη ενός σταθμού βάσης και ενός συνόλου ομοιογενών κόμβων αισθητήρων που διανέμονται τυχαία μέσα σε μια οριοθετημένη περιοχή. Ο σταθμός βάσης βρίσκεται σε μια απόμακρη θέση μακριά από το πεδίο των αισθητήρων. Και ο σταθμός βάσης και το σύνολο των κόμβων αισθητήρων υποτίθεται ότι είναι ακίνητοι (στάσιμοι). Περαιτέρω, υποτίθεται ότι ο σταθμός βάσης είναι σε θέση να διαβιβάσει με την αρκετά υψηλή ενέργεια σε όλους τους κόμβους, λόγω της συνεχής παροχής ηλεκτρικού ρεύματός του. Όλοι οι κόμβοι δικτύου ομαδοποιούνται δυναμικά σε συστάδες. Ένας από τους κόμβους μέσα σε κάθε συστάδα εκλέγεται για να είναι ο επικεφαλής κόμβος της συστάδας. Η υιοθέτηση ενός τέτοιου σχεδίου εξασφαλίζει την εκλεξιμότητα του δικτύου δηλ., η δυνατότητα των διαδικασιών δρομολόγησης να διατηρήσει την απόδοσή του απρόσβλητη από την αύξηση του μεγέθους του δικτύου, περιορίζοντας το πρόβλημα της υπερφόρτωσης του δικτύου. (6)

2.4 Χρήση Ασφάλειας Δικτύων

Οι υπηρεσίες ασφάλειας δικτύου (Network Security Services – NSS) αποτελούνται από ένα σύνολο βιβλιοθηκών που είναι σχεδιασμένες να υποστηρίζουν εξυπηρετητές (server) εφαρμογές με προαιρετική υποστήριξη για hardware SSL acceleration από μεριά server και hardware έξυπνες κάρτες από μεριά client. Προγονός τους θεωρείται το SSL γνωστό πρωτόκολλο ασφαλείας, το οποίο δημιουργήθηκε από την Netscape. Τα NNS παρέχουν μια ολοκληρωμένη ανοιχτού-κώδικα εφαρμογή από βιβλιοθήκες κρυπτογράφησης που υποστηρίζουν SSL /TLS (Secure Sockets Layer /Transport Layer Security) και S/MIME. (3)

Διάφορες εταιρείες όπως η AOL, A, A Microsystems, Google έχουν συνεισφέρει στην ανάπτυξη και στην έρευνα των υπηρεσιών αυτών. Ειδικότερα η

Mozilla η εταιρεία που αναπτύσσει τον γνωστό φυλλομετρητή Firefox, προσφέρει μεγάλη υποστήριξη όπως διόρθωση σφαλμάτων(bugs) ,καθώς και ομάδες συζήτησης. Μερικές εφαρμογές που χρησιμοποιούν τα NNS είναι ο Mozilla Firefox, τα πρόγραμμα άμεσης ανταλλαγής μηνυμάτων όπως το AOL Instant Messenger της AOL, ο φυλλομετρητής Google Chrome της Google ,προγράμματα ανοιχτού κώδικα (open source) όπως Evolution, Pidgin, Open Office.Προγράμματα Server όπως Redhat, Sun Java Enterprise System κ.α.. (2)

3. Πρωτόκολλα που Χρησιμοποιούνται στην Ανάπτυξη Δικτύων Αισθητήρων

Σε αυτό το κεφάλαιο θα εξετάσουμε τα πρωτόκολλα που χρησιμοποιούνται στα σύγχρονα δίκτυα αισθητήρων και τις τεχνικές που εξασφαλίζουν την ακεραία λειτουργία των κόμβων ενός τέτοιου δικτύου. Στο τέλος θα συγκρίνουμε τα πρωτόκολλα μεταξύ τους και θα δούμε ποιά είναι τα ιδανικότερα για κάθε περίπτωση.

3.1 Πρωτόκολλα Δικτύων Αισθητήρων

Για την σωστή λειτουργία ενός δικτύου αισθητήρων, πρέπει το πρωτόκολλο ασφαλείας του δικτύου να καλύπτει κάποιες ορισμένες προϋποθέσεις, δηλαδή να παρέχει κάποιες υπηρεσίες, όπως:

i. Πιστοποίηση Δεδομένων (Data Authentication)
ii. Ακεραιότητα Δεδομένων (Data Integrity)
iii. Πόσο πρόσφατα είναι τα Δεδομένα (Data Freshness)
iv. Η Εμπιστευτικότητα των Δεδομένων (Data Confidentiality)

Ένα σύνολο πρωτοκόλλων που εφαρμόζεται ονομάζεται SPINS.

Το SPINS αποτελείτε από δύο πρωτόκολλα, το SNEP και το μTESLA.
Το SNEP εξασφαλίζει την Εμπιστευτικότητα των Δεδομένων, την Πιστοποίηση μεταξύ δύο κόμβων και την απόδειξη ότι τα δεδομένα είναι πρόσφατα. Το μTESLA εξασφαλίζει την Πιστοποίηση μετάδοσης δεδομένων σε περιβάλλον στο οποίο οι πόροι είναι περιορισμένοι.

Ένα άλλο πρωτόκολλο ασφαλείας δικτύου αισθητήρων είναι το TINYSEC.
Το TINYSEC είναι σχετικά παρόμοιο με το SNEP στο θέμα των υπηρεσιών, δηλαδή παρέχει: πιστοποίηση δεδομένων, ακεραιότητα δεδομένων, εμπιστευτικότητα δεδομένων και προστασία επανάληψης.Το TINYSEC είναι γενικώς ένα ελαφρύ πακέτο ασφάλειας, και έτσι μπορεί να ενσωματωθεί εύκολο στις εφαρμογές δικτύων αισθητήρων.
Καλύπτει τις βασικές ανάγκες ασφάλειας για όλα εκτός των πιο σημαντικών εφαρμογών ασφάλειας.

Άλλο πρωτόκολλο ασφάλειας δικτύου αισθητήρων είναι το LEAP.
Είναι ένα πρωτόκολλο που λειτουργεί ως διαχειριστής κλειδιών, σχεδιασμένο για την επεξεργασία στοιχείων μέσα στο ίδιο το δίκτυο, καθώς και περιορίζει τις επιπτώσεις ενός διακινδυνευμένου κόμβου στο δίκτυο.

Πρωτόκολλο το οποίο χρησιμοποιεί την έννοια του «Κέντρου αξιοπιστίας» είναι το ZigBee. Ο συντονιστής ZigBee έχει τον ρόλο του Κέντρου.
Το κέντρο αυτό επιτρέπει στους άλλους κόμβους/συσκευές να συνδέονται στο δίκτυο, καθώς και μοιράζει τα κλειδιά.

Τέλος, το Security Manager είναι ένα πρωτόκολλο το οποίο, υλοποιεί ένα νέο τύπο συμφωνίας κλειδιού. Όταν μια νέα συσκευή μπαίνει στο δίκτυο, το SM δίνει διάφορες παραμέτρους. Αφού υπολογίσει το δημόσιο κλειδί (public key) χρησιμοποιώντας το σημείο βάσης και το ιδιωτικό κλειδί (private key), η συσκευή στέλνει ένα δημόσιο κλειδί στο SM. Το SM κρατάει μία public key λίστα για τις συσκευές του δικτύου.

3.2 Περιγραφή Πρωτοκόλλων

Εδώ θα εξετάσουμε αναλυτικά τα πρωτόκολλα και τα χαρακτηριστικά τους, τις προδιαγραφές και τους τρόπους υλοποίησης του κάθε πρωτοκόλλου που χρησιμοποιούνται για την ασφαλή επικοινωνία μεταξύ κόμβων ενός δικτύου αισθητήρων.

3.2.1 SPINS

Τα πρωτόκολλα αισθητήρα για πληροφορίες μέσω Διαπραγμάτευσης (SPINS) αποτελούν μια σουίτα πρωτοκόλλων ασφαλείας που έχουν βελτιστοποιηθεί για εξαιρετικά περιορισμούς στους πόρους ενός δικτύου αισθητήρων.
Το SPINS περιλαμβάνει δύο ασφαλή blocks, το SNEP και μTESLA, που τρέχουν πάνω από το TinyOS.Το TinyOS έχει υιοθετηθεί από χιλιάδες προγραμματιστές σε όλο τον κόσμο, σε πολλές πλατφόρμες για ένα ευρύ εύρος των ασύρματων δικτύων αισθητήρων. Το TinyOS βασίζεται σε ένα μοντέλο προγραμματισμού event-driven πολυνηματικό (multithreading).

Η Ασφαλής Κρυπτογράφηση πρωτοκόλλου δικτύου (SNEP) παρέχει τα στοιχεία ταυτότητας, προστασία από επαναλαμβανόμενες επιθέσεις και την «ουσιώδη» ασφάλεια (μια ιδιότητα που εμποδίζει κακόβουλες οντότητες από το να μαθαίνουν πληροφορίες σχετικά με ένα μεταδιδόμενο μήνυμα), η οποία είναι μια σημαντική ιδιότητα ασφαλείας, καθώς αποτρέπει αδιάκριτους από το να διαβάζουν το περιεχόμενο του μηνύματος από το κρυπτογραφημένο μήνυμα.
Αυτό επιτυγχάνεται ως τιμή του μετρητή προσαυξάνεται μετά από κάθε μήνυμα, πράγμα που σημαίνει ότι το μήνυμα είναι κρυπτογραφημένο με διαφορετικό τρόπο κάθε φορά. Ο μετρητής αξία είναι επαρκώς αρκετά ασφαλής οπότε δεν υπάρχει κίνδυνος να επαναληφθεί εντός η διάρκεια ζωής του κόμβου. Εκτός από την ακεραιότητα το παρέχει εμπιστευτικότητα μέσω κρυπτογράφησης και ταυτότητας με κωδικό επαλήθευσης ταυτότητας μηνύματος MAC.

Από την άλλη, το μTESLA είναι η μικρό-εκδοχή του TESLA (Χρονική Αποδοτική Αποτελεσματική Πιστοποίηση),που εξασφαλίζει μια επικυρωμένη εκπομπή, δηλαδή, οι κόμβοι που λαμβάνουν ένα πακέτο μπορεί να είναι σίγουροι για την ταυτότητα του αποστολέα του είναι.
Απαιτεί έναν χρόνο συγχρονισμού μεταξύ του σταθμού βάσης και των κόμβων, με ένα ανώτερο φράγμα για μέγιστο σφάλμα συγχρονισμού.
Για ένα επικυρωμένο πακέτο που θα σταλεί, ο σταθμός βάσης υπολογίζει ένα MAC στο πακέτο με το κλειδί που είναι μυστικό σε εκείνο το χρονικό σημείο. Όταν ένας κόμβος παίρνει ένα πακέτο, μπορεί να επιβεβαιώσει ότι η βάση σταθμός δεν έχει ακόμη γνωστοποιήσει το αντίστοιχο κλειδί MAC, χρησιμοποιώντας αόριστα το συγχρονισμένο ρολόι, και έχει το μέγιστο σφάλμα συγχρονισμού και ο χρόνος κατά τον οποίο είναι τα κλειδιά, για να κοινολογηθούν. Ο κόμβος αποθηκεύει το πακέτο σε ένα buffer, γνωρίζει όμως ότι το MAC κλειδί είναι γνωστό μόνο στο σταθμό βάσης, και ότι κανένας αντίπαλος δεν θα μπορούσε να έχει αλλάξει το πακέτο κατά τη διάρκεια της διαβίβασης. Όταν τα κλειδιά να δημοσιοποιούνται, ο σταθμός βάσης εκπέμπει το κλειδί για όλους τους δέκτες. Ο δέκτης μπορεί κατόπιν ελέγξει την ορθότητα του κλειδιού και να χρησιμοποιήσει τον έλεγχο ταυτότητας του πακέτου, που αποθηκεύεται στο buffer. (7)

Γενικά, το SPIN έχει τέσσερις τύπους:

i. SPIN-PP
ii. SPIN-EK
iii. SPIN-BC
iv. SPIN-RL

3.2.2 TINYSEC

Αντικατάσταση για το ημιτελές SNEP, που είναι γνωστό ως TinySec . Εγγενώς παρέχει παρόμοιες υπηρεσίες, συμπεριλαμβανομένης της ταυτότητας, την ακεραιότητα του μηνύματος, εμπιστευτικότητας και προστασίας από

επαναλαμβανόμενα μηνύματα. Μια σημαντική διαφορά μεταξύ TinySec και SNEP είναι ότι δεν χρησιμοποιούνται το TinySec μετρητές.

Το TinySec καθορίζει μια MAC address των 4 Bytes, πολύ λιγότερο από ό, τι το συμβατικό 8 ή 16 Bytes των προηγούμενων πρωτοκόλλων ασφάλειας. Στο πλαίσιο των δικτύων αισθητήρων αυτό δεν είναι επιζήμιο .Επίσης, το TinySec, ένα ελαφρύ, πακέτο ασφάλειας που οι προγραμματιστές μπορούν εύκολα να ενσωματώσουν σε δίκτυο αισθητήρων και σε εφαρμογές. Το TinySec θα καλύπτει τη βασική ασφάλεια ανάγκες όλων, αλλά και τις πιο κρίσιμες εφαρμογές ασφάλειας.

Υπάρχουν δύο μορφές των πακέτων που ορίζονται από TinySec.
Αυτά είναι το TinySec-Auth, για επικυρωμένα μηνύματα, και το TinySec-AE, για τη γνησιότητα και κρυπτογραφημένα μηνύματα. Για την κρυπτογράφηση, χρησιμοποιεί κατάσταση CBC με cipher για αποφυγή κλοπής κειμένου, καθώς και για τον έλεγχο ταυτότητας, CBC-MAC, που χρησιμοποιείται σε έλεγχο ταυτότητας μόνο λειτουργία, Το TinySec επικυρώνει ολόκληρο το πακέτο με χρήση της MAC address , αλλά το ωφέλιμο φορτίο δεδομένων δεν είναι κρυπτογραφημένο.
Παρακάτω, γίνεται αναφορά των δύο ιδιοτήτων του TinySec:
I) Κρυπτογράφηση: Η χρήση της κρυπτογράφησης σημασιολογικά ασφαλές απαιτεί συνήθως δύο αποφάσεις για το σχεδιασμό: επιλογή ένα σύστημα κρυπτογράφησης και προσδιορίζοντας την IV διαμόρφωση. Αυτός ο σχεδιασμός TinySec χρησιμοποιεί ένα ειδικά διαμορφωμένο 8 byte IV μορφής, και κρυπτογράφησης μπλοκ (CBC) . Εισαγάγει τη δομή της μορφή IV και συγκρούονται για το ποιο CBC είναι τοκαταλληλότερο σύστημα κρυπτογράφησης για τους κόμβους των αισθητήρων .

ii) Ακεραιότητα Μηνύματος: Η Ιστορία έχει αποδείξει ότι η χρήση κρυπτογράφησης χωρίς έλεγχο ταυτότητας είναι ανασφαλή. Το TinySec, χρησιμοποιεί ένα μπλοκ κρυπτογράφησης κατασκευής, CBC-MAC address, για τον υπολογισμό και την επαλήθευση τα MAC. Το CBC-MAC είναι αποτελεσματικό γρήγορο, και το γεγονός ότι βασίζεται σε ένα μπλοκ κρυπτογράφησης, καθώς ελαχιστοποιεί τον αριθμό των κρυπτογραφικών εργαλείων. Το CBC-MAC είναι αποδεδειγμένα ασφαλές , ωστόσο το standard πρότυπο CBC-MAC από κατασκευής δεν είναι ασφαλές για ποικίλου μεγέθους μηνύματα. Οι αντίπαλοι μπορούν να δημιουργήσουν ένα MAC για ορισμένα μηνύματα. Γι'αυτό τον λόγο οι κατασκευαστές προτείνουν

τρεις εναλλακτικές λύσεις για τη δημιουργία MAC, για μεταβλητή μεγέθους των μηνυμάτων που στέλνονται μέσα στο σύστημα. (7)

3.2.3 LEAP

LEAP: Το LEAP (Localized Encryption and Authentication Protocol), είναι ένα βασικό πρωτόκολλο διαχείρισης για δίκτυα αισθητήρων, σχεδιασμένο για να παρέχει υποστηρίζει επεξεργασία εργασιών σε ένα δίκτυο, ενώ παράλληλα περιορίζει έναν διακινδυνευμένο κόμβο μέσα στο δίκτυο. Παλαιότερα, η χρήση προκαθορισμένων κλειδιών ήταν ο πιο πρακτικός τρόπος προσέγγισης για <<εκκίνηση>> και <<αναπαραγωγή>> μυστικών κλειδιών (secret keys) στους κόμβους αισθητήρων. Αυτό συνεπάγεται ότι οι κόμβοι φορτώθηκαν σε όλους τους αισθητήρες πριν είχαν στελεχώσουν το πεδίο του αισθητήρια ζευγάρια των κλειδιών, θα μπορούσαν να αναγεννηθούν μεταξύ δυο κόμβων με αυτές τις προκαθορισμένες πληροφορίες. Προβλήματα που μπορούν να προκύψουν από αυτή την λειτουργία είναι ότι μπορεί να γίνει διακινδύνευση από ένα μόνο κόμβο αποκαλύπτει το μυστικό κλειδί το οποίο χρησιμοποιείται από όλους τους κόμβους του δικτύου. Αυτό θα με τη σειρά τους αποκαλύπτουν όλες τις μελλοντικές επικοινωνιών, καθώς και το παρελθόν καταγεγραμμένη επικοινωνία με παθητικό αντίπαλο. Επίσης, γίνεται δύσκολο για να προστεθούν νέοι κόμβοι στο δίκτυο αισθητήρων. Εφόσον προστεθούν πρόσφατοι κόμβοι θα πρέπει να έχουν όλο το φάσμα του κλειδί του δικτύου πριν να προκαθοριστεί, ή όλοι οι κόμβοι του δικτύου θα πρέπει να καθοδηγούνται με ασφάλεια, χρησιμοποιώντας ένα νέο κοινόχρηστο κλειδί.
Το LEAP είναι ένα βασικό πρωτόκολλο διαχείρισης που προορίζεται για δίκτυα αισθητήρων βασίζεται σε αλγόριθμους συμμετρικού κλειδιού, δηλαδή, το ίδιο κλειδί χρησιμοποιείται από τον αποστολέα και του δέκτη. σε ένα δίκτυο, απαιτώντας από κάθε ζεύγος κόμβων να έχουν κοινόχρηστο κλειδί που θα χρησιμοποιηθεί για την επικοινωνία μεταξύ τους. Είναι ιδανικό για την ασφάλεια, επειδή μια οποιαδήποτε επίθεση σε κάθε έναν κόμβο δεν διακυβεύει την ασφάλεια των άλλων κόμβων. Όμως, στα δίκτυα αισθητήρων, οι γειτονικοί κομβόι δεν είναι σε θέση να γνωρίζουν εκ των προτέρων, την ανταλλαγή την κλειδιών μέσα σε ένα δίκτυο που έχει

προκαθοριστεί όπως είπαμε ,έτσι μπορεί να υπάρξουν προβλήματα επιβάρυνσης όπως πχ υπερφόρτωση των πληροφοριών.
Επίσης, τα δίκτυα αισθητήρων, μπορούν να χρησιμοποιούν ορισμένες βελτιστοποιήσεις επεξεργασίας όπως το να αποφασίζουν να μην αναφέρουν μια ΄΄κατάσταση΄΄ ενός κόμβου εάν ΄΄κρυφακούει΄΄ τον γειτονικό κόμβο. Τέτοιες βελτιστοποιήσεις θα αποκλείουν , τη χρήση ενός ξεχωριστού κλειδιού για όλους τους κόμβους του δικτύου άρα χαμηλότερη κίνηση άρα λιγότερος κίνδυνος υπερφόρτωσης , με όμως συμβιβασμούς για ολόκληρο το σύστημα των κόμβων.

Γενικά, το LEAP καθορίζει τέσσερις τύπους κλειδιών:

i. Μεμονωμένα κλειδιά (Individual keys)
ii. Κοινά ζεύγη κλειδιών (Pair wise keys)
iii. Κλειδιά συστάδας (Cluster Keys)
iv. Ομαδικά κλειδιά.(Group Keys)

Τα μεμονωμένα κλειδιά είναι συμμετρικά κλειδιά οποία διαμοιράζονται μεταξύ του κεντρικού σταθμού βάσεως και καθένα από τους κόμβους.
Τα κοινά ζεύγη κλειδιών είναι κ αυτά συμμετρικά κλειδιά, τα οποία μοιράζονται μεταξύ ενός κόμβου και καθένα ξεχωριστά από τους γειτονικούς κόμβους.
Από την άλλη τα κλειδιά συστάδας, είναι συμμετρικά που κάνουν χρήση κοινών στοιχείων μεταξύ ενός κόμβου και όλων των γειτονικών. Αυτά τα κλειδιά, μπορούν να χρησιμοποιηθούν για τοπική εκπομπή μηνυμάτων όπως για πχ ενός πρωτόκολλου δρομολόγησης.
Τέλος, τα ομαδικά κλειδιά διαμοιράζονται με όλους τους κόμβους ενός συστήματα και του κεντρικού σταθμού. Επιτρέπει, κρυπτογραφημένα και πιστοποιημένα μηνύματα να μεταδοθούν σε ολόκληρο το δίκτυο κόμβων.

Ο κύριος στόχος του LEAP είναι να ικανοποιήσει τις ιδιότητες ασφάλειας της πιστοποίησης και της εμπιστευτικότητας σε ένα περιβάλλον, όπου ένας εισβολέας μπορεί να <<παρατηρεί>>, να επηρεάζει τα πακέτα δεδομένων και να κάνει επανάληψη μηνυμάτων. Οι δημιουργοί του LEAP, επιθυμούν επίσης το πρωτόκολλο να είναι ανθεκτικό σε επιθέσεις ασφάλειας και ότι οι επιπτώσεις των ενδεχομένων

επιθέσεων να είναι όσο το δυνατόν λιγότερες στους κόμβους του συστήματος. Ένα μειονέκτημα του όμως είναι ότι δεν φέρει ευθύνη για τις επαναλαμβανόμενες επιθέσεις ή της επιθέσεις DoS (Denial of Service). (7)

3.2.4 ZigBee

Η έννοια του "Κέντρο αξιοπιστίας" εισάγεται στις προδιαγραφές αυτού του πρωτοκόλλου. Γενικά, ο συντονιστής ZigBee εκτελεί αυτό το καθήκον. Αυτό το κέντρο αξιοπιστίας, επιτρέπει σε άλλες συσκευές να συνδέονται στο δίκτυο και διανέμει επίσης τα κλειδιά. Υπάρχουν τρεις ρόλους που κάνει:

i. διευθυντής αξιοπιστίας, σύμφωνα με την οποία ταυτοποιεί τις συσκευές που ζητούν να ενταχθούν στο δίκτυο
ii. διαχειριστή του δικτύου, που συντηρεί και τη διανέμει τα κλειδιά δικτύου, και
iii. διαχειριστής διάρθρωσης, επιτρέποντας end-to-end ασφάλειας μεταξύ των συσκευών

Υπάρχουν τρεις τύποι των κλειδιών που χρησιμοποιούνται, το Master Κλειδί, το κλειδί Link και το κλειδί δικτύου. Τα κλειδιά Master, εγκαθίστανται πρώτα, είτε στο εργοστάσιο είτε εκτός ζώνης. Αποστέλλονται από τα Κέντρο αξιοπιστίας και αποτελούν τη βάση για την μακροπρόθεσμη ασφάλεια μεταξύ δύο συσκευών. Το κλειδί Link, είναι η βάση της ασφάλειας μεταξύ των δύο συσκευών και τα Κλειδιά δικτύου είναι η βάση της ασφάλειας σε ολόκληρο το δίκτυο. Τα Link και κλειδιά Δικτύου, τα οποία είτε έχουν προ-εγκατασταθεί στο εργοστάσιο ή εκτός, χρησιμοποιούν συμμετρικά κλειδιά ανταλλαγής κλειδιών (SKKE) (με χρήση της ανταλλαγής <<χειραψίας>>),μεταξύ συσκευών.

Οι προδιαγραφές ασφαλείας ZigBee εφαρμόζουν απλούστερη και ενοποιημένο τρόπο λειτουργίας του CCM (αυτή η λειτουργία είναι μία συγχώνευση τόσο της κρυπτογράφησης και ταυτότητας ορίζει βασικά είδη Master, Link, Network) και περιγράφει τις βασικές εγκαταστάσεις των κλειδιών και συντήρηση των κόμβων. Επιπροσθέτως, το ZigBee παρέχει τη συνεχή ενημέρωση των λειτουργιών των κόμβων μέσω της χρήσης των συνέχων ελέγχων .
Οι έλεγχοι αυτοί εμποδίζουν επαναλαμβανόμενες επιθέσεις , καθώς οι συσκευές ZigBee διατηρούν τις εισερχόμενες και εξερχόμενες μετρητές που κάνουν συνεχή έλεγχο στο ολόκληρο σύστημα των κόμβων ενός συστήματος. (7)

3.2.5 SM (Security Manager)

Το SM είναι ένα πρωτόκολλο που για κάθε νέα συσκευή που μπαίνει στο δίκτυο, στέλνει κάποιες παραμέτρους στατικού Domain όπως την διάταξη καμπύλης και τους συντελεστές ελλειπτικής καμπύλης . Το δημόσιο κλειδί υπολογίζετε χρησιμοποιώντας το σημείο βάσης και το ιδιωτικό κλειδί. Αφού υπολογιστεί το δημόσιο κλειδί, στέλνετε το κλειδί αυτό στο SM από την συσκευή. Το SM κρατάει λίστα με κλειδιά, στην οποία υπάρχουν τα δημόσια κλειδιά για κάθε συσκευή του δικτύου.
Στο SM υπάρχουν δύο επίπεδα ασφάλειας, το μέτριο και το υψηλό. Το επίπεδο ασφάλειας εξαρτάτε από την ισχύς και τη πολιτική ασφάλειας της κάθε συσκευής. Το κάθε επίπεδο ασφάλειας ξεχωρίζει από τους φυσιολογικούς ή πολυωνιμικούς υπολογισμούς.
Η κρυπτογράφηση Ελλειπτικής Καμπύλης (Elliptic Curve Cryptography – ECC) δίνει φυσιολογικά υπολογιστικά φορτία και μικρότερα μεγέθη κλειδιών για ισοδύναμη ασφάλεια σε σχέση με τις άλλες τεχνικές.
Η EC-MQV (Menezes-Quad-Vanstone) είναι ένα σχέδιο πιο εξελιγμένο από το Diffie-Hellman, και η κεντρική ιδέα είναι να εμποδιστεί η επίθεση τύπου Man-In-The-Middle (MITM) και η πιστοποίηση αυτών που έχουν κλειδί. Με αυτό το σχέδιο, κάθε μέρος μιας επικοινωνίας έχει δύο κλειδιά.
Οι συσκευές στο δίκτυο, χρησιμοποιούν αρχικές παραμέτρους εμπιστοσύνης (Pre-Deployed Recognition Function) για να στήσουν το δημόσιο κλειδί και το εφήμερο κλειδί, που χρησιμοποιούνται για την ασφαλή επικοινωνία των φορτίων δεδομένων. Το overhead βασίζεται στον αριθμό των επιλεγμένων bits για το EC σύστημα. Ένας αλγόριθμος ελλειπτικής καμπύλης παρέχει την ίδια ασφάλεια για 160bit μέγεθος κλειδιού, όπως ένας συμμετρικός αλγόριθμος μπορεί για 128bit μέγεθος. Αυτό το επίπεδο ασφάλειας μπορεί να αυξηθεί ανάλογα με τις ανάγκες ασφάλειας και έτσι να επιτρέπει ένα μεταβλητό overhead.
Τα χαρακτηριστικά του SM πρωτοκόλλου είναι τα εξής: Εμπιστευτικότητα, Πιστοποίηση Χρήστη και Σιωπηρή Πιστοποίηση. (7)

3.3 Συγκεντρωτικός Πίνακας Περιγραφής Πρωτοκόλλων Ασφάλειας Δικτύων

Εδώ θα δούμε συγκεντρωμένα στον πίνακα 2 τα βασικά χαρακτηριστικά των πρωτοκόλλων που είδαμε στο παραπάνω μέρος του κεφαλαίου.

Όνομα Πρωτοκόλλου	Εμπιστευτικότητα (Confidentiallity)	Πρόσφατα Δεδομένα (Freshness)	Ακεραιότητα (Integrity)	Διαθεσιμότητα (Availability)	Πιστοποίηση Χρήστη (User Authentication)	Σιωπηρή Πιστοποίηση (Implicit Authentication)
SPINS(SNEP + μTesla)	Ναι	Όχι	Ναι	Όχι	Ναι	Ναι
TINYSEC	Ναι	Όχι	Όχι	-	Ναι	Ναι
LEAP	Ναι	Όχι	Όχι	Όχι	Ναι	Ναι
ZIGBEE	Ναι	Ναι	Ναι	Όχι	Ναι	Ναι
SM(SECURITY MANAGER)	Ναι	Όχι	Όχι	-	Ναι	Ναι

Πίνακας 2: Περιγραφή Πρωτοκόλλων

3.4 Θεωρητική Σύγκριση Πρωτοκόλλων

Υπάρχουν αρκετά πρωτόκολλα, ώστε κάποιος να μπορέσει να επιλέξει το ιδανικότερο ανάλογα με τις ανάγκες του δικτύου του.

Το SPINS είναι ένα από τα πλέον ασφαλή και αποδοτικά πρωτόκολλα δικτύων αισθητήρων.

Το LEAP είναι ένα πρωτόκολλο που επιβιώνει επιθέσεις ασφάλειας και έχει την ικανότητα να ελαχιστοποιεί τις επιπτώσεις των οποιοδήποτε τύπου επιθέσεων.

Το TINYSEC είναι ένα ποιό δυνατό, και ποιό αποδοτικό σε θέμα κατανάλωσης ενέργειας, πρωτόκολλο.

Στο ZigBee πρωτόκολλο εισάγεται η έννοια του Κέντρου Αξιοπιστίας (Trust Center).

Τέλος, το Security Manager (SM) χρησιμοποιεί το πλάνο του EC-MQV για

εγκαθίδρυση κλειδιών (ιδιωτικά και δημόσια), που είναι πιο εξειδικευμένο και η κεντρική ιδέα είναι η αποφυγή επιθέσεων τύπου Man-In-The-Middle(MITM).
Γενικώς, το κάθε πρωτόκολλο, είναι καλύτερο σε κάποιο τομέα σε σχέση με κάποιο άλλο, και ο διαχειριστής του δικτύου καλείται να επιλέξει ποιό ταιριάζει περισσότερο στο σύστημά του.(7)

Υπάρχουν πολλά προγράμματα που μας επιτρέπουν να προσομοιώσουμε ένα δίκτυο αισθητήρων. Κάποια από αυτά είναι:

- NS-2
- OMNET++
- Matlab
- OPnet (Riverbed)

4. Πειραματικές Μετρήσεις

4.1 Εισαγωγή

Για τη διεξαγωγή των μετρήσεων με ότι η επικοινωνία αφορά τη μετάδοση ενός γεγονότος από έναν κόμβο προς όλους τους υπόλοιπους, δηλαδή την περίπτωση όπου η επικοινωνία γίνεται με χρήσης Flooding.

Η χρήση Flooding αν και απλοϊκή αποτελεί μία σίγουρη μέθοδο διακίνησης πληροφορίας καθώς ο κάθε κόμβος ενημερώνει τους γειτονικούς του, εκτός από εκείνον από τον οποίο έλαβε την πληροφορία.

Κάτι τέτοιο οδηγεί σε σημαντική κίνηση πακέτων δεδομένων στο δίκτυο, αλλά πολλές φορές αποτελεί τη μόνο αξιόπιστη μέθοδο επικοινωνίας.
Σε πολλά πρωτόκολλα χρησιμοποιείται ως το πρώτο βήμα στην αναγνώριση των γειτονικών κόμβων, ώστε να καθοριστεί η δομή του δικτύου.

Επίσης αποτελεί μία μέθοδο μέτρησης της αποδοτικότητας της χρησιμοποιούμενης μεθόδου επικοινωνίας.

Για την ακριβέστερη προσομοίωση της επικοινωνίας μεταξύ των κόμβων επιχειρήσαμε να προσδιορίσουμε και την κατάσταση του καναλιού, το οποίο μπορεί να ευνοεί ή όχι την χωρίς σφάλματα μετάδοση των πακέτων δεδομένων.

Η προσομοιώσεις έγιναν με τη χρήση του περιβάλλοντος **Matlab** και συγκεκριμένα της έκδοσης R2013a.

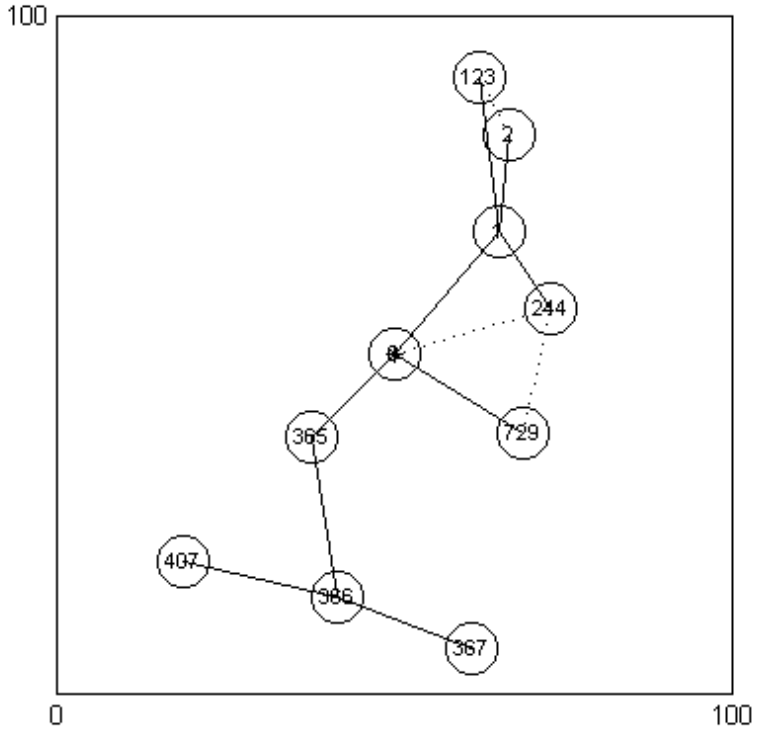
4.2 Δομή Δικτύου

Η δομή του δικτύου παίζει ιδιαίτερο ρόλο όταν ο σκοπός είναι η μελέτη της απόδοσης ενός πρωτοκόλλου επικοινωνίας κάτω από συγκεκριμένες συνθήκες.
Οι συνθήκες αυτές μπορεί να αφορούν το φυσικό περιβάλλον (για παράδειγμα αστικό περιβάλλον, δάσος), αριθμό κόμβων για συγκεκριμένη κάλυψη μιας περιοχής, καθώς και ανάγκες ενέργειας δηλαδή αυτονομίας για δεδομένο χρονικό διάστημα.

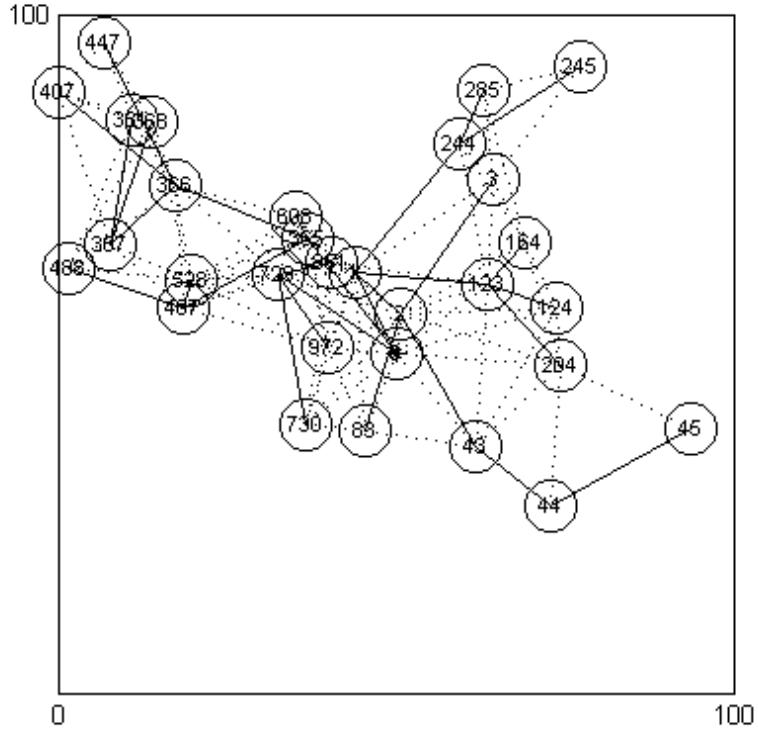
Οι συνθήκες αυτές δεν προσδιορίζονται στο πρόβλημα που μελετούμε αφού εστιάζουμε στη σύγκριση της απόδοσης του πρωτοκόλλου ZigBee με χρήση ή όχι ασφάλειας δεδομένων.

Για το λόγο αυτό η τοπολογία του δικτύου θεωρούμε ότι είναι τυχαία. Το στοιχείο που μας ενδιαφέρει είναι εκείνο της σύνδεσης όλων των κόμβων μεταξύ τους ώστε να εξασφαλίζεται η μετάδοση δεδομένων για καθένα από αυτούς.

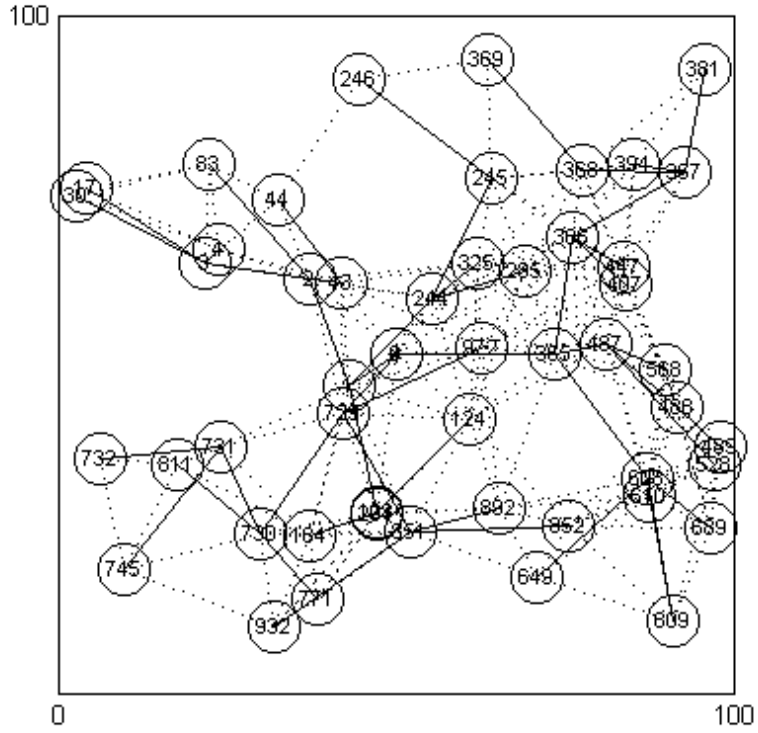
Με χρήση του περιβάλλοντος Matlab δημιουργούμε τέτοια δίκτυα, όπως φαίνεται και από τις επόμενες γραφικές παραστάσεις.



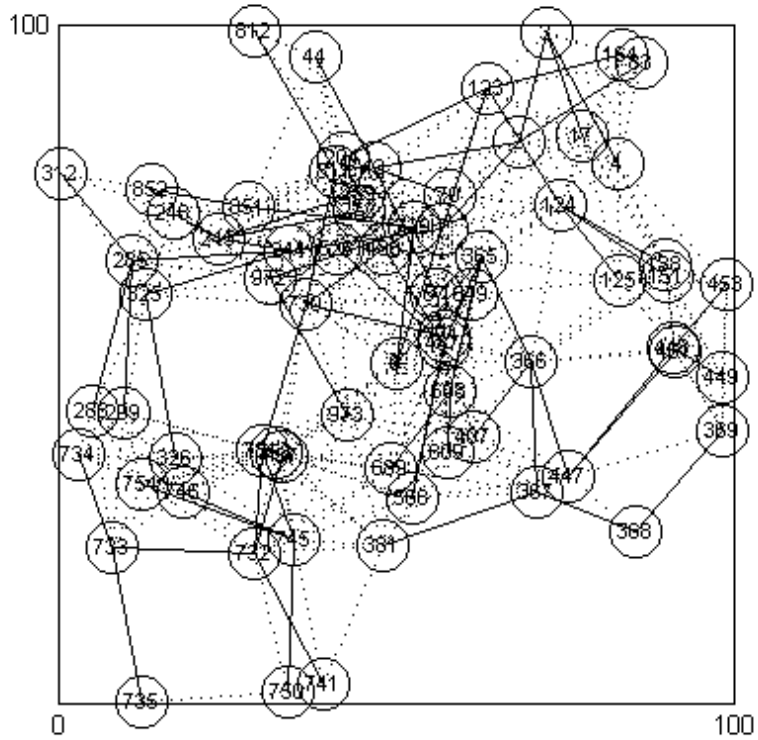
Εικόνα 5: Δίκτυο 10 κόμβων



Εικόνα 6: Δίκτυο 20 κόμβων



Εικόνα 7: Δίκτυο 50 κόμβων



Εικόνα 8: Δίκτυο 70 κόμβων

Στις παραπάνω γραφικές παραστάσεις βλέπουμε τόσο του κόμβους όσο και τις συνδέσεις μεταξύ τους . Τα id των κόμβων είναι μοναδικοί τυχαίου αριθμοί που τους χαρακτηρίζουν.

Οι συνδέσεις απεικονίζονται με συνεχόμενη γραμμή όταν πρόκειται για τη βέλτιστη σύνδεση μεταξύ ενός κόμβου και του υπόλοιπου δικτύου, είτε με διακεκομμένη γραμμή όταν υπάρχει σύνδεση μεταξύ δύο κόμβων.

Η χρήση η όχι όλων των συνδέσεων εξαρτάται από το πρωτόκολλο επικοινωνίας, όπου στην περίπτωσή μας είναι το Flooding.

4.3 Πίνακας Γειτνίασης

Για τη χρήση τους σε υπολογισμούς, οι συνδέσεις μεταξύ των κόμβων πρέπει να βρίσκονται σε μορφή κατάλληλη προς επεξεργασία. Στο σημείο αυτό έρχεται ο πίνακας γειτνίασης.
Πρόκειται για έναν πίνακα στον οποίο η κάθε στήλη αντιστοιχεί σε έναν κόμβο και σε κάθε γραμμή σημειώνεται αν ο κόμβος της γραμμής συνδέεται με κάποιον από τους υπόλοιπους.
Για το δίκτυο της Εικόνας 5 ο πίνακας γειτνίασης είναι ο ακόλουθος:

0	2	4	5	8	-1	-1	-1	-1	-1
1	1	3	6	8	-1	-1	-1	-1	-1
2	2	6	-1	-1	-1	-1	-1	-1	-1
365	1	7	-1	-1	-1	-1	-1	-1	-1
729	1	8	-1	-1	-1	-1	-1	-1	-1
123	2	3	-1	-1	-1	-1	-1	-1	-1
366	4	9	10	-1	-1	-1	-1	-1	-1
244	1	2	5	-1	-1	-1	-1	-1	-1
367	7	-1	-1	-1	-1	-1	-1	-1	-1
407	7	-1	-1	-1	-1	-1	-1	-1	-1

Στον πίνακα αυτό η πρώτη στήλη έχει τους κόμβους με το μοναδικό αναγνωριστικό τους (id) και στη συνέχεια τους κόμβους με τους οποίους συνδέονται.
Επειδή στους υπολογισμούς αυτό που έχει σημασία είναι η θέση του κόμβου στον πίνακα και όχι το αναγνωριστικό τους, η ερμηνεία του συγκεκριμένου πίνακα γειτνίασης μπορεί να διευκολυνθεί με το ακόλουθο παράρτημα:

id	Αριθμός στον Πίνακα
0	1
1	2
2	3
365	4
729	5
123	6
366	7
244	8
367	9
407	10

Όπως γίνεται κατανοητό ο πίνακας γειτνίασης για μεγαλύτερα δίκτυα δεν μπορεί να απεικονιστεί, η λογική του όμως παραμένει η ίδια. Δεδομένου λοιπόν του πίνακα, έχουμε σε κατάλληλη μορφή τις πληροφορίες που αφορούν τη δυνατότητα αποστολής πακέτων δεδομένων αλλά και τον ίδιο τον αριθμό τους, αν υποθέσουμε ότι δεν υπάρχουν απώλειες. Στο μοντέλο μας, προκειμένου να ανταποκρίνεται στην πραγματικότητα έχουμε εισάγει απώλειες λόγω κακής κατάστασης καναλιού.

4.4 Πρωτόκολλο Flooding

Πρόκειται για ένα πρωτόκολλο το οποίο χρησιμοποιείται συνήθως για δρομολόγηση. Υπάρχουν δύο μορφές του: α) ελεγχόμενη και β) μη ελεγχόμενη.
Στη δεύτερη περίπτωση το δίκτυο κατακλύζεται από πακέτα τα οποία ανταλλάσσονται μεταξύ των κόμβων χωρίς κανένα έλεγχο.
Στην περίπτωση του ελεγχόμενου Flooding κάθε πακέτο χαρακτηρίζεται από μία μοναδική χρονοσφραγίδα, που του επιτρέπει να χαρακτηρίζεται ως καινούριο ή ήδη ληφθέν.

Ο αλγόριθμος που ακολουθεί το πρωτόκολλο ακολουθεί τα εξής βήματα:

1. Κάθε κόμβος λειτουργεί τόσο ως πομπός όσο και ως δέκτης.

2. Κάθε κόμβος επιχειρεί να προωθήσει το μήνυμα που έλαβε σε όλους τους γείτονές του εκτός από εκείνους από τους οποίους το έλαβε.

Το πρωτόκολλο αυτό έχει το πλεονέκτημα ότι είναι απλό και εξασφαλίζει την ορθή μετάδοση των πακέτων σε όλο το δίκτυο. Ωστόσο έχει και αρκετά μειονεκτήματα όπως:

- Όλοι οι κόμβοι θα λάβουν το μήνυμα ακόμα και αν ο προορισμός του πακέτου είναι συγκεκριμένος κόμβος

- Σπαταλούνται οι πόροι του δικτύου καθώς δε χρησιμοποιούνται μόνο οι βέλτιστες συνδέσεις

- Αν οι κόμβοι του δικτύου έχουν περιορισμένη ενέργεια, τότε το πρωτόκολλο οδηγεί σύντομα σε εξάντληση της ενέργειας των κόμβων

Δεδομένου του ντετερμινιστικού τρόπου λειτουργίας του πρωτοκόλλου καθώς και της απλότητάς του, αποτελεί μία εφικτή μέθοδο υπολογισμού των πακέτων τα οποία συνολικά θα ανταλλάξουν οι κόμβοι μεταξύ τους.
Για το λόγο αυτό στα πειράματά μας υποθέτουμε ότι η δρομολόγησης των πακέτων χρησιμοποιεί το εν λόγω πρωτόκολλο.

4.5 Κανάλι

Μία καθοριστική παράμετρος για τη προσομοίωση της λειτουργίας του δικτύου αποτελεί και το μοντέλο του καναλιού. Σε ένα πραγματικό περιβάλλον το κανάλι υπόκειται σε μεταβολές οι οποίες επιτρέπουν ή όχι την χωρίς σφάλματα επικοινωνία. Στην περίπτωση σφάλματος, πρέπει να γίνει αναμετάδοση του πακέτου, η οποία επιβαρύνει την κίνηση του δικτύου.

Ανάλογα με τη συμπεριφορά του καναλιού μπορεί να έχουμε τον ελάχιστο αριθμό μεταδόσεων, αν για παράδειγμα ένα καλό κανάλι επιτρέψει σε όλα τα πακέτα ορθή μετάδοση, ή και πολύ μεγάλη επιβάρυνση του δικτύου, αν το ίδιο πακέτο πρέπει να αναμεταδοθεί πολλές φορές. Η κατάσταση του καναλιού καθορίζεται από παράγοντες οι οποίοι εξαρτώνται τόσο από την τοποθεσία του δικτύου όσο και τις καιρικές συνθήκες που επικρατούν.

Οι παράγοντες που επηρεάζουν την κατάσταση του καναλιού μπορούν να διαιρεθούν σε δύο κατηγορίες:

- Εξασθένιση μεγάλης κλίμακας
- Εξασθένιση μικρής κλίμακας

Στην πρώτη κατηγορία ανήκουν παράγοντες όπως η απόσταση, φυσικά εμπόδια καθώς και τα καιρικά φαινόμενα. Στη δεύτερη κατηγορία έχουμε μικρές μεταβολές στη θέση των εμποδίων ή των κόμβων καθώς και τα φαινόμενα της ανάκλασης, διάθλασης και σκέδασης των σημάτων επικοινωνίας.

Όπως γίνεται κατανοητό ο καθορισμός όλων των παραγόντων που επηρεάζουν το ασύρματο μέσο δεν είναι εφικτός λόγω του πλήθους και της χρονική μεταβολής τους. Για το λόγο αυτό ένα κανάλι μοντελοποιείται σύμφωνα με κάποιο στατιστικό μοντέλο ώστε να γνωρίζουμε την κατάστασή του κάθε χρονική στιγμή.
Στα πειράματά μας χρησιμοποιούμε το μοντέλο Rayleigh το οποίο προτείνεται για αστικά περιβάλλοντα όπου τα αντικείμενα που μεταβάλλουν το σήμα μέσω ανάκλασης, διάθλασης και σκέδασης είναι πολλά.

Η χρήση του μοντέλου Rayleigh οδηγεί στον θεωρητικό υπολογισμό του Bit Error Rate για την απλούστερη μορφή διαμόρφωσης σήματος, της δυαδικής διαμόρφωσης φάσης (Binary Phase Shift Keying - BPSK). Αυτό αποτελεί την απλούστερη εκδοχή καναλιού μετάδοσης όπου η πληροφορία αποτυπώνεται στη φάση του φέροντος σήματος. Αν και η δυαδική διαμόρφωση αποτελεί την πιο αργή περίπτωση μετάδοσης πληροφορίας, αποτελεί ένα απλό μοντέλο με χαμηλό ρυθμό σφαλμάτων.

Το μοντέλο Rayleigh βασίζεται στην ισχύ του θορύβου ο οποίος υποβαθμίζει την ποιότητα του σήματος. Ο θόρυβος θεωρείται τυχαία μεταβλητή Γκαουσιανής κατανομής:

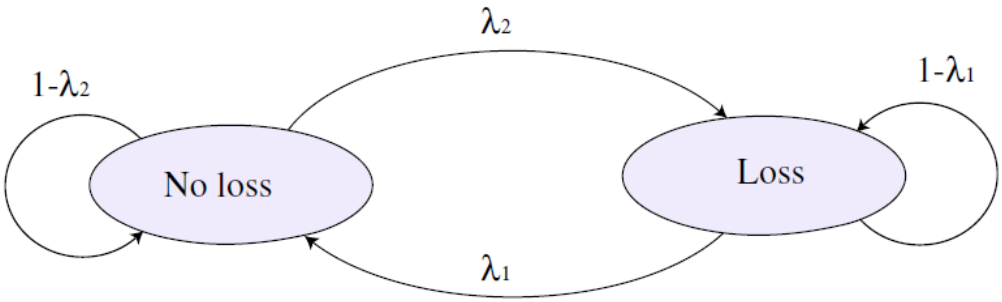
$$f = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

Όπου μ η μέση τιμή και σ η διασπορά. Δεδομένου ότι ο θόρυβος επηρεάζει το πραγματικό και φανταστικό κομμάτι του σήματος, η κατανομή της ισχύος του ακολουθεί την κατανομή chi-square, η οποία αποτελεί άθροισμα τετραγώνων Γκαουσιανής κατανομής.

Η κατανομή chi-square χαρακτηρίζεται από έναν αριθμό που ονομάζεται βαθμός ελευθερίας. Ο προσδιορισμός του ουσιαστικά χαρακτηρίζει τον θόρυβο και επομένως την ποιότητα του καναλιού. Στα πειράματά μας ο βαθμός αυτός ισούται με 3 (8).

Μέχρι στιγμής μοντελοποιήσαμε το κανάλι αναφορικά με το σφάλμα το οποίο προκύπτει κατά την αποστολή ενός πακέτου. Κάτι τέτοιο όμως δεν αντιστοιχεί στην πραγματικότητα αφού το κανάλι μπορεί να παραμείνει σε "κακή" κατάσταση για διάστημα μεγαλύτερο του ενός πακέτου. Τα σφάλματα που ανήκουν στην περίπτωση αυτή ονομάζονται burst errors και αφορούν μία ακολουθία πακέτων.

Η συμπεριφορά του καναλιού όσον αφορά τα burst errors μπορεί να προσομοιωθεί μέσω της χρήσης του μοντέλου Gilbert-Elliot. Πρόκειται για μία απλή Μαρκοβιανή αλυσίδα όπως φαίνεται στην εικόνα 9:



Εικόνα 9: Μαρκοβιανή αλυσίδα

Στην ουσία έχουμε δύο πιθανότητες λ_1, λ_2 που αντιστοιχούν στα ενδεχόμενα το κανάλι να βρίσκεται σε "καλή" και "κακή" κατάσταση αντίστοιχα.
Οι πιθανότητες αυτές παίζουν καθοριστικό ρόλο στη μοντελοποίηση της κατάστασης του καναλιού (9).

4.6 Μέγεθος Πακέτων

Στο πρωτόκολλο ZigBee καθορίζονται δύο μεγέθη πακέτων ανάλογα με τη χρήση ασφάλειας ή όχι. Όπως είναι λογικό, στην περίπτωση της χρήσης μηχανισμών ασφαλείας έχουμε επιβάρυνση όσον αφορά το μέγεθος των πακέτων, αφού τα δεδομένα πρέπει να κωδικοποιηθούν, και να συμπεριληφθούν πληροφορίες σχετικά με την αποκωδικοποίησή τους.

Ένα τυπικό πακέτο στο πρωτόκολλο ZigBee έχει την παρακάτω μορφή:

1 byte	2 bytes	1 byte	0/2/4/10 bytes	0/2/4/10 bytes	variable	2 bytes
Len.	Flags	Seq. No	Dest. Address	Source Address	Data payload	CRC

Έχουμε κατά σειρά: το μέγεθος, bit ελέγχου, θέση στην ακολουθία, διεύθυνση προορισμού, διεύθυνση αποστολέα, δεδομένα και bit ελέγχου ορθότητας (Cyclic Redundancy Check).

Ανάλογα με το βαθμό ασφάλειας και τον επιλεγμένο αλγόριθμο κρυπτογράφησης προκύπτουν και οι αντίστοιχες μορφές πακέτων. Στο επόμενο πίνακα αναφέρονται οι βαθμοί ασφαλείας που προβλέπονται από το πρωτόκολλο ZigBee:

Όνομα	Περιγραφή
AES-CBC-MAC-128	128 bit MAC
AES-CBC-MAC-64	64 bit MAC
AES-CBC-MAC-32	32 bit MAC
AES-CCM-128	Κρυπτογράφηση δεδομένων και 128 bit MAC
AES-CCM-64	Κρυπτογράφηση δεδομένων και 64 bit MAC
AES-CCM-32	Κρυπτογράφηση δεδομένων και 32 bit MAC

Ο όρος MAC (message authentication cod) αναφέρεται στο κομμάτι του πακέτου το οποίο είναι κρυπτογραφημένο και πιστοποιεί την αυθεντικότητα των αποστελλόμενων δεδομένων. Οι παραπάνω αλγόριθμοι οδηγούν στις ακόλουθες μορφές πακέτων:

4 bytes	1 byte	variable
Frame Counter	Key Ctr	Encrypted Payload

(a) AES-CTR

variable	4/8/16 bytes
Payload	MAC

(b) AES-CBC-MAC-b, $b \in \{4, 8, 16\}$ MAC size

4 bytes	1 byte	variable	4/8/16 bytes
Frame Counter	Key Ctr	Encrypted Payload	Encrypted MAC

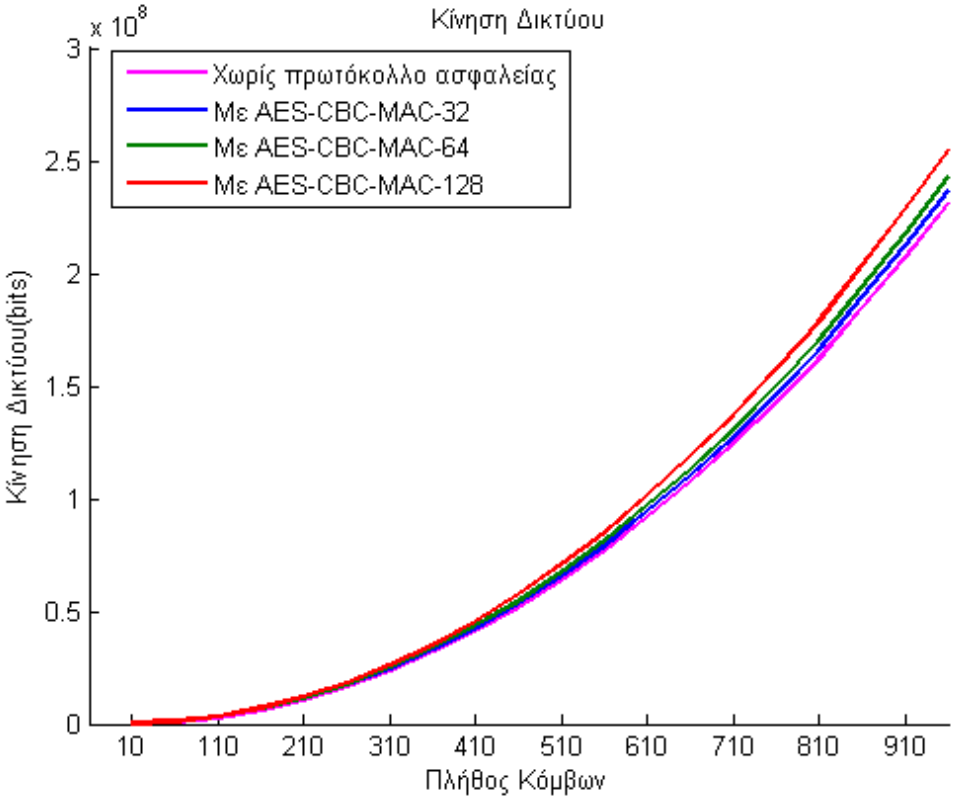
(c) AES-CCM-b, $b \in \{4, 8, 16\}$ MAC size

Εικόνα 10: Μορφές Πακέτων (10)

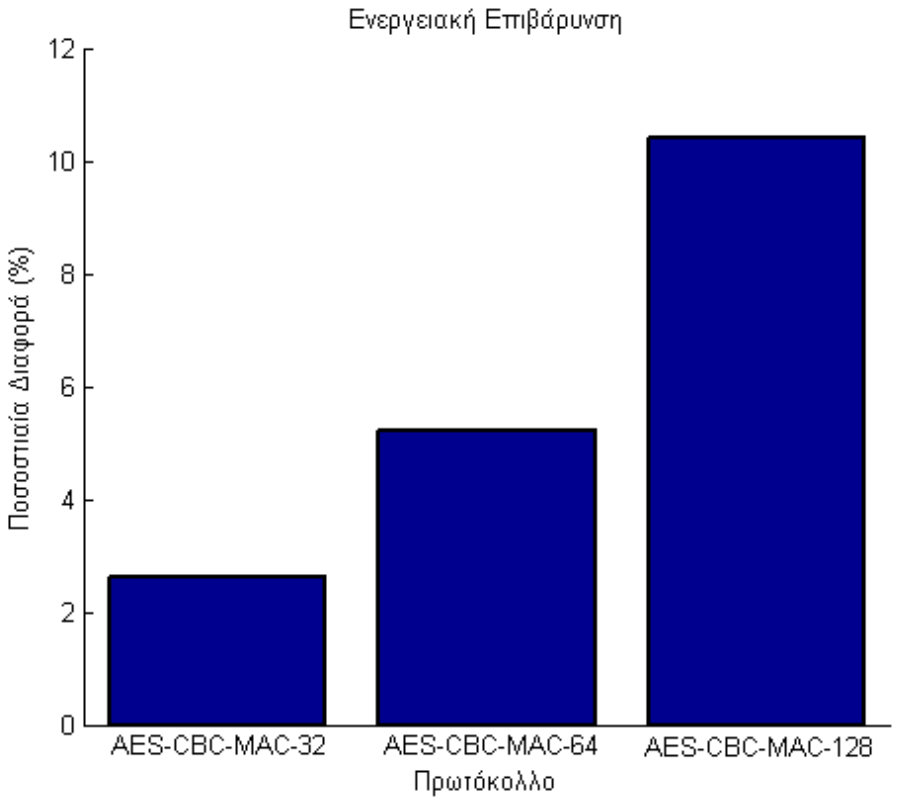
4.7 Πειραματικά Αποτελέσματα

Δημιουργώντας δίκτυα διαφόρων μεγεθών προσομοιώσαμε τη λειτουργία τους με χρήση πρωτοκόλλου ασφαλείας του προτύπου ZigBee.

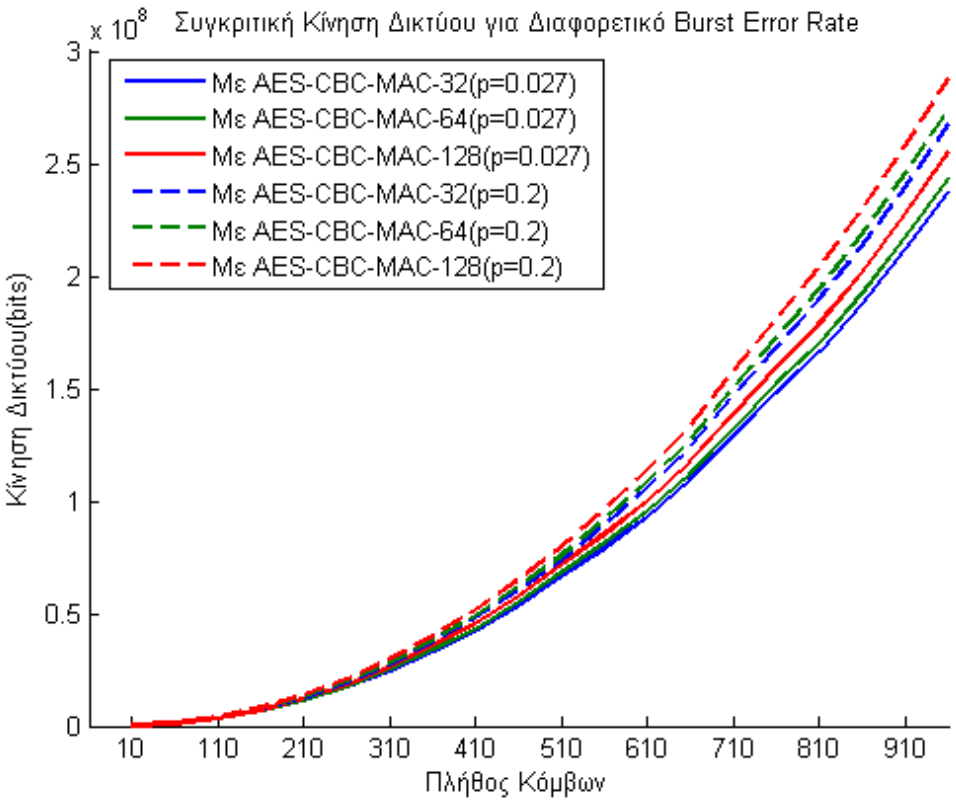
Στην επόμενη γραφική παράσταση φαίνονται τα αποτελέσματα σχετικά με τη συνολική κίνηση του δικτύου:



Η διαφορά στη συνολική κατανάλωση ενέργειας φαίνεται στην επόμενη γραφική παράσταση:

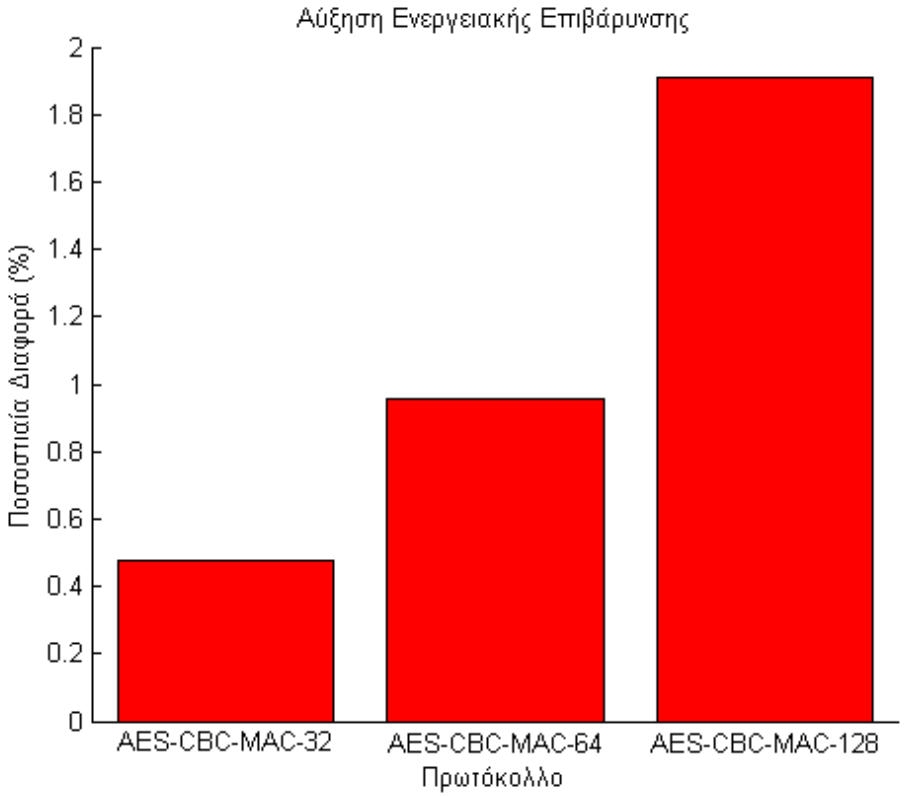


Τα προηγούμενα πειραματικά αποτελέσματα αφορούν την περίπτωση όπου το κανάλι δεν επιβαρύνει την επικοινωνία. Ο παράγοντας που το καθορίζει αυτό είναι ο χαμηλός ρυθμός burst σφαλμάτων, ο οποίος προσδιορίζεται από την πιθανότητα να μεταβούμε σε κακής ποιότητας κανάλι η οποία ισούται με p=0.027.
Αν αυξηθεί η πιθανότητα αυτή αναμένεται να έχουμε περισσότερες αναμεταδόσεις χαμένων πακέτων.
Για να το διαπιστώσουμε αυτό προχωρήσαμε στη σύγκριση της ενεργειακής κατανάλωσης όταν p=0.027 και p=0.2. Τα αποτελέσματα φαίνονται στις επόμενες γραφικές παραστάσεις.



Στην παραπάνω γραφική παράσταση βλέπουμε ότι όσο η πιθανότητα ύπαρξης burst σφαλμάτων αυξάνεται, τόσο αυξάνεται και η συνολική κίνηση δεδομένων στο δίκτυο.
Αυτό οφείλεται στην αναμετάδοση των χαμένων πακέτων.

Ένα ακόμη στοιχείο το οποίο πρέπει να σημειωθεί είναι ότι η κίνηση αυξάνεται εκθετικά σε σχέση με τον αριθμό των κόμβων.
Στην γραφική παράσταση που ακολουθεί παρουσιάζονται τα πειραματικά αποτελέσματα σχετικά με τον επιπλέον ποσοστιαίο κόστος ενέργειας ανάλογα με τον ρυθμό burst σφαλμάτων.
Εκεί βλέπουμε ότι χρησιμοποιώντας το πρωτόκολλο AES-CBC-MAC-128 η κατανάλωση ενέργειας μπορεί να αυξηθεί κατά 2%, όσον αφορά το σύνολο του δικτύου.
Δε θα πρέπει να ξεχνάμε ότι ορισμένοι κόμβοι ενδέχεται να επιβαρύνονται περισσότερο από άλλους, ανάλογα με τον αριθμό των γειτόνων τους.



4.8 Συμπεράσματα

Τα πειραματικά αποτελέσματα επιβεβαιώνουν ότι η χρήση πρωτοκόλλου κρυπτογράφησης των δεδομένων έχει επίδραση στη συνολική κατανάλωση ενέργειας του δικτύου. Συγκεκριμένα, παρατηρήσαμε ότι ανάλογα με το βαθμό ασφαλείας του πρωτοκόλλου η ενεργειακή επιβάρυνση κυμαίνεται από 2% ως 11%.

Με τις δεδομένες περιβαλλοντικές συνθήκες προσομοίωσης, το ποσοστό της ενέργειας που καταναλώνεται για το σκοπό της κρυπτογράφησης είναι σημαντικό, ωστόσο αναμένεται να αυξηθεί στην περίπτωση όπου πρόσθετοι παράγοντες επιβάρυνσης είναι παρόντες.

Σε ένα πραγματικό δίκτυο, οι αποστάσεις, τα εμπόδια και οι φυσικοί ανακλαστήρες του πεδίου αναμένεται να δυσχεραίνουν ακόμη περισσότερο την επικοινωνία των κόμβων. Αυτό μεταφράζεται σε επιπλέον ενεργειακή επιβάρυνση στην περίπτωση όπου χρησιμοποιηθεί κάποιο πρωτόκολλο ασφαλείας όπως το AES-CBC-MAC-128.

Όπως διαπιστώσαμε από το σχετικό πείραμα, η επιβάρυνση λόγω πρόσκαιρης αύξησης του ρυθμού σφαλμάτων μπορεί να οδηγήσει μέχρι και σε 2% μεγαλύτερη κατανάλωση ενέργειας.
Μία τέτοια αύξηση σημαίνει 2% λιγότερη ενεργειακή αυτονομία του δικτύου, κάτι που μπορεί να καθιστά απαγορευτική τη χρήση της εν λόγω κρυπτογράφησης.
Αν σε αυτό συμπεριλάβουμε το γεγονός ότι κάποιο κόμβοι λόγω της κεντρικής τους θέσης μπορεί να συμμετέχουν σε πολλές μεταδόσεις πακέτων, τότε η επιβάρυνση αυτή μπορεί να σημαίνει την πρόωρη εξάντλησή τους.

Ο κίνδυνος εξάντλησης της ενέργειας ενός κόμβου αποτελεί σοβαρό παράγοντα υποβάθμισης της αποτελεσματικότητας του δικτύου, από τη στιγμή που αποτελούν του κυριότερους κόμβους μετάδοσης δεδομένων.
Η απενεργοποίησή τους, εκτός από την αναγκαστική μεταβολή του πίνακα δρομολόγησης, οπότε και σωρεία διαγνωστικών πακέτων, εμπεριέχει και τον κίνδυνο της μη συνεκτικότητας του δικτύου.

Τα ζητήματα αυτά μας οδηγούν στο συμπέρασμα ότι η χρήση πρωτοκόλλου ασφαλείας θα πρέπει να εξετάζεται ανά περίπτωση ανάλογα με τις παρακάτω συνθήκες:

- φυσικό περιβάλλον του δικτύου
- κλιματολογικές συνθήκες
- δυνατότητα τροφοδότησης των κόμβων με ενέργεια
- πλήθος κόμβων

4.9 Επεκτάσεις-Ανοικτά Ζητήματα

Η μελέτη της επίδρασης της χρήσης πρωτοκόλλου ασφαλείας στην ενεργειακή αυτονομία του δικτύου αποτελεί ένα πολύπλευρο ζήτημα. Στην παρούσα εργασία το ενδιαφέρον εστιάστηκε στον κυριότερο παράγοντα υποβάθμισης της επικοινωνίας, αυτόν του καναλιού.
Η κατάσταση του καναλιού, καθώς και ο ρυθμός μεταβολής της, καθορίζουν το ποσοστό της ενέργειας που θα πρέπει να καταναλώσει ο κάθε κόμβος στην πιο ενεργοβόρα λειτουργία του, αυτή της ασύρματης επικοινωνίας.
Εκτός του καναλιού όμως υπάρχουν και άλλοι παράγοντες που χρήζουν μελέτης.
Η επιβάρυνση των κόμβων από υπολογιστικής πλευράς επηρεάζει επίσης σημαντικά την κατανάλωση ενέργειας. Ο υπολογιστικός φόρτος προκύπτει από τις ανάγκες κρυπτογράφησης/αποκρυπτογράφησης των δεδομένων.
Μία διερεύνηση του κατά πόσο η κατανάλωση αυτή επιτρέπει τη χρήση του εκάστοτε πρωτοκόλλου κρυπτογράφησης θα συμπλήρωνε την παρούσα μελέτη.

Βιβλιογραφία

1. **McCarthy, L.** Intranet Security. s.l. : Prentice Hall, 1997.
2. **Taylor, A.** The Hackers. s.l. : Routledge, 1999.
3. **Pfleeger.** Security in Computing. s.l. : Prentice Hall, 1997.
4. **Rouse, Margaret.** http://searchdatacenter.techtarget.com/definition/sensor-network. *searchdatacenter.techtarget.com*. [Ηλεκτρονικό] June 2006. http://searchdatacenter.techtarget.com/definition/sensor-network.
5. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3290468/. *http://www.ncbi.nlm.nih.gov/*. [Ηλεκτρονικό] September 2009.
6. www.mdpi.com/journal/sensors. *www.mdpi.com*. [Ηλεκτρονικό] 2009. https://www.google.gr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0CCwQFjAB&url=http%3A%2F%2Fwww.mdpi.com%2F1424-8220%2F9%2F11%2F8399%2Fpdf&ei=j8q_U5DEH8mK7Ab5vIEo&usg=AFQjCNHBhDUJh_hCl8haYVYo2R92xPtzpg&bvm=bv.70810081,d.ZGU.
7. **Anupma Sangwan, Deepti Sindhu, Kulbir Singh.** A Review of various security protocols in Wireless Sensor Network. [Ηλεκτρονικό] August 2011. www.ijcta.com.
8. **Buratti, Chiara.** *Performance Analysis of IEEE 802.15.4 Beacon-Enabled Mode.* 2010.
9. **Pallassini, David.** *Packet Loss Performance and MAC Design for estimation in Wireless Sensor Networks.* 2005.
10. **Naveen Sastry, David Wagner.** *Security Considerations for IEEE 802.15.4 Networks.*

Διαδικτυακές Πηγές

1. http://el.wikipedia.org/wiki/ΑσφαλειαΔικτυωνΥπολογιστων
2. http://utopia.duth.gr/~kdrakato/thesis/chapter3.doc
3. https://developer.mozilla.org/en-US/docs/NSS
4. http://en.wikipedia.org/wiki/Network_Security_Services
5. http://kouloukith.blogspot.gr/p/3.html
6. http://en.wikipedia.org/wiki/Code_division_multiple_access
7. http://cellphones.about.com/od/phoneglossary/g/cdma.htm
8. http://link.springer.com/article/10.1007%2Fs11416-006-0017-x
9. http://www.bee.net/mhendry/vrml/library/cdma/cdma.htm
10. http://www.pcmag.com/article2/0,2817,2407896,00.asp