ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Προκλήσεις και απειλές ασφαλείας των ασύρματων δικτύων αισθητήρων και των υλοποιήσεων τους στο Διαδίκτυο των Πραγμάτων (IoT). Μελέτη περίπτωσης συστήματος αυτοματισμού, τηλεπισκόπησης κι ελέγχου στην ΔΕΥΑΚ Καστοριάς.

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

του

ΓΕΩΡΓΙΟΥ ΣΤΑΥΡΑΚΑΚΗ

(ΑΕΜ:2537)

Επιβλέπων : ΝΙΚΟΛΑΟΥ ΣΠΥΡΙΔΩΝ

ΛΕΚΤΟΡΑΣ

Καστοριά – Οκτώβριος 2023

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Προκλήσεις και απειλές ασφαλείας των ασύρματων δικτύων αισθητήρων και των υλοποιήσεων τους στο Διαδίκτυο των Πραγμάτων (IoT). Μελέτη περίπτωσης συστήματος αυτοματισμού, τηλεπισκόπησης κι ελέγχου στην ΔΕΥΑΚ Καστοριάς.

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

του

ΓΕΩΡΓΙΟΥ ΣΤΑΥΡΑΚΑΚΗ

(ΑΕΜ:2537)

Επιβλέπων : ΝΙΚΟΛΑΟΥ ΣΠΥΡΙΔΩΝ
ΛΕΚΤΟΡΑΣ

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 25 Οκτωβρίου 2023

.....	.....	.....
Ον/μο Μέλους	Ον/μο Μέλους	Ον/μο Μέλους
Ιδίοτητα Μέλους	Ιδίοτητα Μέλους	Ιδίοτητα Μέλους

Καστοριά – Οκτώβριος 2023

Ευχαριστίες

Ευχαριστώ την οικογένεια μου για την υποστήριξη όλα αυτά τα χρόνια, και τους καθηγητές μου για την καθοδήγηση τους.

Περίληψη

Η παρούσα πτυχιακή εργασία κάνει μία εισαγωγή στα ασύρματα δίκτυα αισθητήρων (Wireless Sensor Networks – WSNs), πως ξεκίνησαν, ποιες είναι οι κυριότερες εφαρμογές τους, τι τοπολογίες υπάρχουν και σε ποια πρωτόκολλα βασίζονται για την υλοποίηση τους. Παράλληλα, εξετάζει πως το Διαδίκτυο των Πραγμάτων (Internet of Things – IoT) σχετίζεται και αλληλοεπιδρά με τα ασύρματα δίκτυα αισθητήρων και ακολουθεί ανάλυση των προκλήσεων και θεμάτων ασφαλείας των ασύρματων δικτύων αισθητήρων και ποιοι μηχανισμοί ενισχύουν την ασφάλειά τους.

Στα πλαίσια του εφαρμοσμένου μέρους της παρούσας πτυχιακής εργασίας, γίνεται ανάλυση μελέτης περίπτωσης εφαρμογής ασύρματων δικτύων αισθητήρων στο σύστημα αυτοματισμού, τηλεπισκόπησης και ελέγχου της Δημοτικής Επιχείρησης Ύδρευσης & Αποχέτευσης (Δ.Ε.Υ.Α.) Καστοριάς και παρουσιάζονται συνοπτικά τα συμπεράσματα αυτής της υλοποίησης.

Λέξεις Κλειδιά: Ασύρματο Δίκτυο Αισθητήρων, Διαδίκτυο των πραγμάτων, Μοντέλο Αναφοράς OSI, MAC, Πρωτόκολλα Δρομολόγησης, Ασφάλεια, Κρυπτογράφηση, Απειλές, Επιθέσεις, Ποιότητα υπηρεσιών, Αισθητήρες, Ενεργοποιητές, Προγραμματιζόμενοι Λογικοί Ελεγκτές, Εποπτικός Έλεγχος και Απόκτηση Στοιχείων, Κεραίες, Mikrotik, Ubiquiti

Abstract

This thesis gives an introduction to Wireless Sensor Networks (WSNs), how they started, what are their main applications, what topologies exist and what protocols are used for their implementation. It also examines how the Internet of Things (IoT) relates and interacts with wireless sensor networks, followed by an analysis of the security challenges and issues of WSNs and what mechanisms enhance their security.

In the context of the applied part of this thesis, a case study of the implementation of WSN in the automation, remote monitoring and control system of the Municipal Water Supply & Sewerage Company (D.E.Y.A.) of Kastoria is analyzed and the conclusions of this implementation are summarized.

Key Words: Wireless Sensor Network, Internet of Things, OSI Reference Model, MAC, Routing Protocols, Security, Cryptography, Threats, Attacks, Quality of Service, Sensors, Actuators, Programmable Logic Controllers, Supervisory Control And Data Acquisition, Antennas, Mikrotik, Ubiquiti

Πίνακας Περιεχομένων

Λίστα Εικόνων

Λίστα Πινάκων

Εισαγωγή

Η παρούσα πτυχιακή εργασία έχει ως σκοπό να δημιουργήσει μία εξοικείωση και κατανόηση για τα ασύρματα δίκτυα αισθητήρων, γνωστά και ως Wireless Sensor Networks (WSNs), πως συνδυάζονται τα WSNs με το Internet of Things (IoT), μία αναφορά στο θέμα ασφάλειας των δικτύων αυτών και τέλος μία μελέτη περίπτωσης σε τοπική επιχείρηση που χρησιμοποιεί WSNs.

Πιο συγκεκριμένα στο πρώτο κεφάλαιο παρουσιάζεται μία ιστορική αναδρομή για τα Wireless Sensor Networks (WSNs), εφαρμογές που βασίζονται σε WSNSs, ποια είναι η αρχιτεκτονική και οι στόχοι των δικτύων αυτών, καθώς επίσης αναφέρονται οι βασικές τοπολογίες, τα πρότυπα και τα πρωτόκολλα που χρησιμοποιούν τα ασύρματα δίκτυα αισθητήρων.

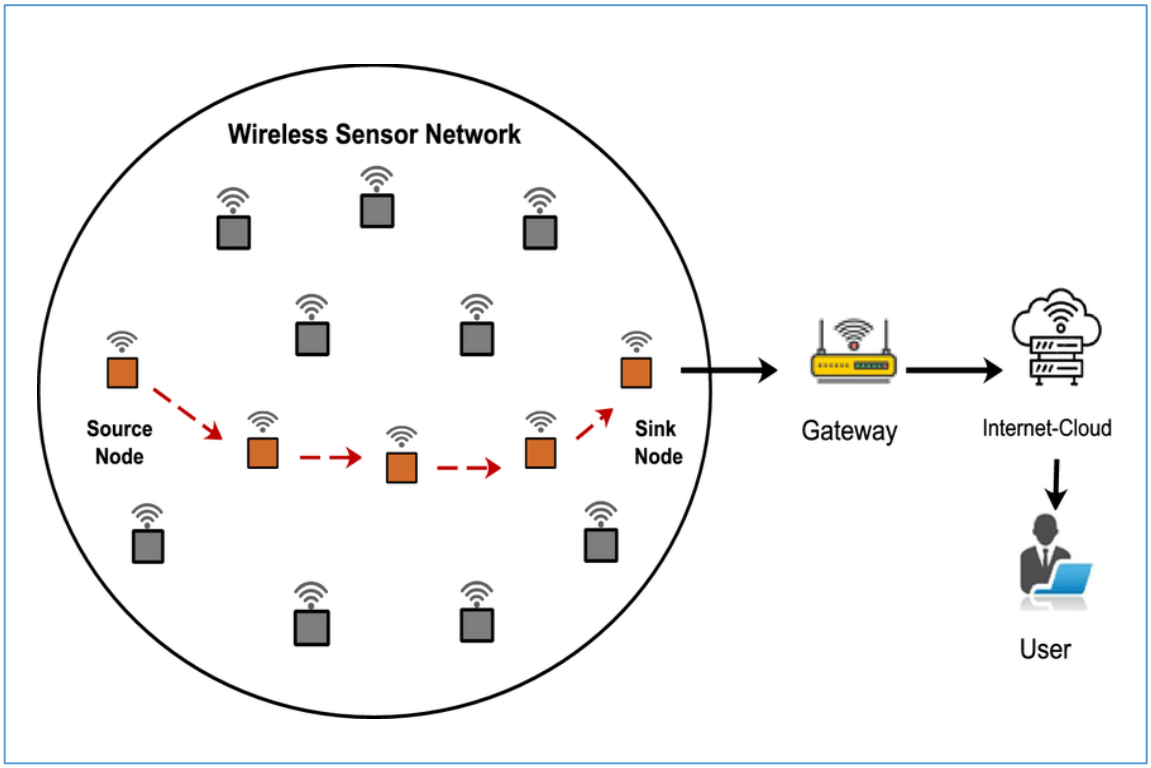
Στο δεύτερο κεφάλαιο αναλύεται η συσχέτιση και η αλληλεπίδραση των ασύρματων δικτύων αισθητήρων με το Διαδίκτυο των Πραγμάτων (IoT). Αναλυτικότερα, πως λειτουργούν οι αισθητήρες, πως γίνεται η ανίχνευση και ποιες κατηγορίες αισθητήρων υπάρχουν. Πως είναι μία δομή ενός κόμβου αισθητήρα, από τι αποτελείται η αρχιτεκτονική του IoT, ποια πρωτόκολλα υπάρχουν σε αυτό τον τομέα, αλλά και μία ανάλυση των κυριότερων προκλήσεων σε θέματα ασφαλείας των WSNs, των επιθέσεων και των μηχανισμών ασφάλειας για την αντιμετώπισή τους.

Τέλος στο τρίτο κεφάλαιο παρουσιάζεται η μελέτη περίπτωσης εφαρμογής ασύρματων δικτύων αισθητήρων που έγινε στη Δημοτική Επιχείρηση Ύδρευσης & Αποχέτευσης (Δ.Ε.Υ.Α.) Καστοριάς, όπου αναλύεται συνοπτικά το σύστημα αυτοματισμού, τηλεπισκόπησης και ελέγχου. Περιγράφεται η υποδομή του δικτύου, τόσο από την πλευρά του υλικού, όσο και από την πλευρά του λογισμικού που χρησιμοποιήθηκε για να δημιουργηθεί ένα τέτοιο δίκτυο. Επίσης, παρουσιάζονται οι εφαρμογές τύπου SCADA για την ανάλυση των δεδομένων που λαμβάνουν οι αισθητήρες που χρησιμοποιούνται για την απομακρυσμένη διαχείριση του δικτύου. Τέλος, παρουσιάζονται τα συμπεράσματα αυτής της υλοποίησης,

1. Ασύρματο Δίκτυο Αισθητήρων

1.1 Τι είναι ένα Ασύρματο Δίκτυο Αισθητήρων

Ένα ασύρματο δίκτυο αισθητήρων (Wireless Sensor Network– WSN) [1] είναι ένα δίκτυο το οποίο αποτελείται από κόμβους αισθητήρων που αισθάνονται ή αλληλεπιδρούν με το φυσικό τους περιβάλλον με σκοπό την καταγραφή, επεξεργασία και συγκέντρωση δεδομένων χωρίς καλώδια Για να είναι σωστές οι μετρήσεις συνήθως χρησιμοποιούνται εκατοντάδες ή χιλιάδες κόμβοι που επικοινωνούν με έναν κεντρικό σταθμό επεξεργασίας όπου συλλέγονται οι πληροφορίες και μεταγενέστερα μετά από επεξεργασία να βλέπουμε με κάποιο γράφημα από τα δεδομένα που συλλέχθηκαν. Όταν χρησιμοποιούμε ένα WSN και με την βοήθεια ενεργοποιητή, τότε η επικοινωνία των κόμβων είναι αμφίδρομη, δηλαδή όπως μεταδίδουν πληροφορίες στον σταθμό επεξεργασίας, με τον ίδιο τρόπο δέχονται πληροφορίες από αυτόν και εκτελούν κάποια ενέργεια [2]. Στην φωτογραφία παρακάτω βλέπουμε πως είναι ένα τυπικό WSN όπου οι κόμβοι αισθητήρων μεταδίδουν της πληροφορίες στον κόμβο πύλη (sink node) που είναι η τελευταία συσκευή πριν την επικοινωνία με το ίντερνετ.



Εικόνα 1. Δίκτυο WSN

Πηγή: https://www.researchgate.net/figure/Architecture-of-wireless-sensor-network-for-IoT-applications_fig1_337921971

1.2 Ιστορία των Ασύρματων Δικτύων Αισθητήρων

Πολλές από τις τεχνολογίες που χρησιμοποιούμε σήμερα αναπτύχθηκαν εδώ και αρκετές δεκαετίες. Κύριος λόγος της ανάπτυξής τους ήταν οι περίοδοι των πολέμων, καθώς υπήρχε ανάγκη του πλεονεκτήματος έναντι του εχθρού. Έτσι και με τα ασύρματα δίκτυα αισθητήρων η πρώτη εμφάνισή τους έγινε στην δεκαετία του 1950 από τον Αμερικάνικο στρατό με ένα εγχείρημα με την ονομασία Sound Surveillance System (SOSUS). Το SOSUS δημιουργήθηκε για την αναγνώριση και παρακολούθηση των Σοβιετικών υποβρυχίων με την χρήση βυθισμένων ακουστικών αισθητήρων (υδροφώνων) τα οποία διανεμήθηκαν στους ωκεανούς του Ειρηνικού και του Ατλαντικού στην περίοδο του ψυχρού πολέμου.

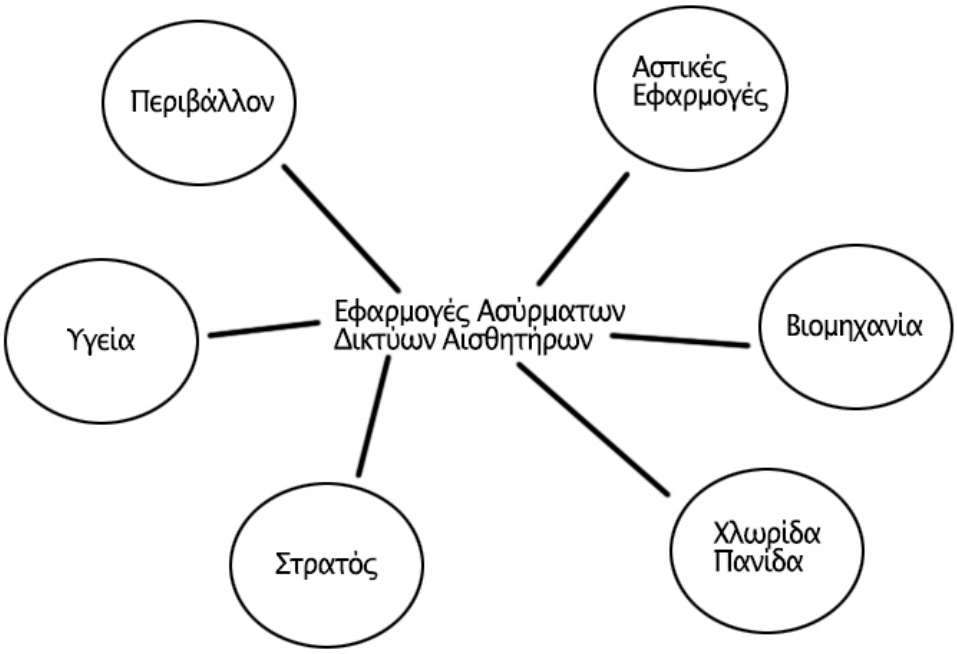
Αυτό το εγχείρημα του στρατού χρησιμοποιείται ακόμα και σήμερα αλλά για τελείως διαφορετικό σκοπό, όπως για την παρακολούθηση ηφαιστειακής δραστηριότητας αλλά και την άγρια υποθαλάσσια ζωή. Σχεδόν δύο δεκαετίες μετά το 1969 για αμυντικό σκοπό αυτήν την φορά ο στρατός δημιούργησε ένα δίκτυο άμυνας στον αέρα με αερόστατα σαν αισθητήρες. Την ίδια χρονιά ίσως και το σημαντικότερο δίκτυο στην ιστορία των ασύρματων δικτύων αισθητήρων και όχι μόνο το ARPANET (Advanced Research Projects Agency Network) που χρηματοδοτήθηκε από το Υπουργείο Άμυνας των Ηνωμένων Πολιτειών μέσω μίας υπηρεσίας με την ονομασία Υπηρεσία Έρευνας Προηγμένων Αμυντικών Προγραμμάτων ή στα αγγλικά DARPA. Το δίκτυο αυτό δημιουργήθηκε για να μπορεί να υπάρξει επικοινωνία μεταξύ πανεπιστημίων και ερευνητικών κέντρων στις Ηνωμένες Πολιτείες Αμερικής (Η.Π.Α).

Μετά από μία σειρά από επιτυχημένων προσπαθειών και χρηματοδοτήσεων στις δεκαετίες 1960 και 1970 η DARPA δημιούργησε αυτό που σήμερα ονομάζουμε ίντερνετ. Οι επόμενες κινήσεις της υπηρεσίας DARPA ήταν να ξεκινήσει το 1980 ένα καινούργιο εγχείρημα για την δημιουργία ενός κατανεμημένου δικτύου αισθητήρων Distributed Sensor Network (DSN) με σκοπό να ανακαλύψουν τυχόν δυσκολίες στην εφαρμογή ενός κατανεμημένου ασύρματου δικτύου αισθητήρων (WDSN). Μετά από αρκετές δεκαετίες έχουν γίνει πολλά άλματα σε αυτές τις τεχνολογίες, οι αισθητήρες έχουν μικρύνει αρκετά σε μέγεθος, το κόστος για την δημιουργία τέτοιων δικτύων είναι σημαντικά μικρότερο όπως και η κατανάλωση ενέργειας επίσης. [3]

1.3 Εφαρμογές Ασύρματων Δικτύων Αισθητήρων

Τις τελευταίες δεκαετίες η τεχνολογία εξελίσσεται με ραγδαίους ρυθμούς όπως επίσης, αυξάνονται και οι ανάγκες της σύγχρονης κοινωνίας. Αυτό έχει ως αποτέλεσμα τα ασύρματα δίκτυα αισθητήρων να μπορούν να βοηθούν και να προσφέρουν δυνατότητες σε αρκετούς τομείς. Οι κύριοι πυλώνες είναι έξι, περιβάλλον, υγεία, στρατός, χλωρίδα και πανίδα, βιομηχανία και αστικές εφαρμογές. Οι εφαρμογές των δικτύων στους κύριους αυτούς πυλώνες είναι αμέτρητοι και σε αρκετές από αυτές τα στάδια ανάπτυξής τους είναι είτε σε αρχικό είτε σε ώριμο στάδιο. Ο στρατός έπαιξε καθοριστικό ρόλο στην

ανάπτυξη και στην έρευνα των δικτύων αισθητήρων και είναι ένα από τα αρχικά έργα που ανέπτυξε ήταν το Smart Dust. Το Smart Dust ήταν ένα έργο που σαν μέριμνα είχε την δημιουργία μικροσκοπικών αισθητήρων που να είναι ικανά να χρησιμοποιηθούν για κατασκοπεία και να ξοδεύουν το δυνατόν λιγότερη ενέργεια, ώστε να μπορούν να είναι ενεργοποιημένοι για αρκετά μεγάλο χρονικό διάστημα.



Εικόνα 2. Εφαρμογές Ασύρματων Δικτύων Αισθητήρων

Πηγή:https://www.mdpi.com/2571-5577/3/1/14

Ο στρατός κατέχει τα ηνία στις εφαρμογές των ασύρματων δικτύων αισθητήρων καθώς έχει εφαρμογές, όπως παρακολούθηση μάχης, παρακολούθηση πεδίου μάχης και ανίχνευση εισβολέα. Χρησιμοποιούν αισθητήρες για την ανίχνευση επικίνδυνων ουσιών όπως χημικά, βιολογικά, ραδιενεργά, πυρηνικά η ακόμα και εκρηκτικά. Για την ανίχνευση οποιουδήποτε εισβολέα θα μπορούσαν να χρησιμοποιηθούν ανιχνευτές όπως υπέρυθρες, φωτοηλεκτρικοί, λέιζερ ακόμη και ακουστική και αισθητήρες δόνησης. Με την χρήση διάφορων ραντάρ όπως Radio Detection And Ranging (RADAR), Light Detection And Ranging (LIDAR) ή Laser Detection And Ranging (LADAR) καθώς και υπερηχητικούς αισθητήρες για την ανίχνευση αντικειμένων ζωτικής σημασίας. Η χρήση LADAR και αισθητήρων υπέρυθρων γινόταν για την εικονικούς σκοπούς. Αναλυτικότερα το Radio Detection And Ranging (RADAR), ή αλλιώς ανίχνευση με ηλεκτρομαγνητικά κύματα και μέτρηση αποστάσεως (ραντάρ) που χρησιμοποιούταν για τον εντοπισμό και την παρακολούθηση ακίνητων και κινητών στόχων, σε αρκετά μεγάλες αποστάσεις και αντίξοες συνθήκες φωτισμού ώστε να μην υπάρχει οπτική επαφή. [4] Η τεχνολογία LIDAR χρησιμοποιεί λέιζερ για την σάρωση του εδάφους αλλά και της βλάστησης σε

οποιαδήποτε συνθήκη φωτισμού κάνοντας την στρατιωτική της χρήση πολύ σημαντική και απαραίτητη. [5] Το πολεμικό ναυτικό χρησιμοποιούσε ένα δίκτυο αισθητήρων σόναρ, παθητικών αλλά και ενεργών ώστε να μπορούν να εντοπίζουν την τοποθεσία υποβρυχίων. Άλλη μια εφαρμογή που είναι συνδυαστική και με την κατηγορία υγεία είναι οι αισθητήρες σώματος στο κράνος στρατιωτών, για την παρακολούθηση στρατιωτών σε πραγματικό χρόνο.

Μερικά από τα στατιστικά είναι ο κορεσμός οξυγόνου στο αίμα, το επιταχυνσιόμετρο, την πίεση, ακόμα και τον καρδιακό ρυθμό. Η υγεία μας είναι το πολυτιμότερο πράγμα που έχουμε και με την βοήθεια των ασύρματων αισθητήρων σε εφαρμογές, όπως τα νοσοκομεία μπορούν οι γιατροί να παρακολουθούν τους ασθενείς όλη μέρα σε πραγματικό χρόνο απλά φορώντας στον ασθενή έναν μικρό αισθητήρα. Ένα πρωτοποριακό σύστημα βοήθειας για το σπίτι δημιουργήθηκε με την βοήθεια αισθητήρα που φοριέται στο στήθος ή ακόμα και εσωτερικά στο σώμα με την βοήθεια χειρουργείου. Με την χρήση αισθητήρα και μίας εφαρμογής κινητού μπορεί ο οποιοσδήποτε να κάνει διάγνωση στο σπίτι του και να στείλει απομακρυσμένα τα δεδομένα στον γιατρό του.

Μετά από αρκετές δεκαετίες που σαν ανθρωπότητα είχαμε παραμελήσει το περιβάλλον αρχίσαμε σιγά σιγά να το μελετάμε εκτενέστερα, είτε από απειλές που σαν ανθρώπινο είδες έπρεπε να αντιμετωπίσουμε είτε επειδή έπρεπε να διασφαλίσουμε πόρους και πληροφορίες από αυτό. Η θέληση του ανθρώπινου γένους για επιβίωση μας ανάγκασε να δημιουργήσουμε ένα συστήματα παρακολούθησης ηφαιστειακής δραστηριότητας, σεισμικής δραστηριότητας, ανίχνευση τσουνάμι αλλά και πρόληψη δασικών πυρκαγιών. Επίσης, χρειάστηκε να παρακολουθούμε τον αέρα αλλά και το νερό αλλά και να δημιουργήσουμε ένα σύστημα που θα λαμβάνει όλες αυτές τις πληροφορίες και θα ενημερώνει τον κόσμο με την μορφή της έκτακτής ανάγκης. Η χλωρίδα και πανίδα παίζουν πολύ σημαντικό ρόλο και στην καθημερινότητα μας και υπάρχει ανάγκη για ένα εξειδικευμένο σύστημα που να παρακολουθεί αλλά και να ενεργεί. Μερικές από τις σημαντικότερες εφαρμογές σε αυτό τον πυλώνα είναι η παρακολούθηση της καλλιέργειας, των θερμοκηπίων αλλά και η κτηνοτροφία. Η καλλιέργεια είναι ένα πολύ δύσκολο και πολύπλευρο κομμάτι που με την εγκατάσταση ενός δικτύου παρακολούθησης μπορούν να κάνουν την άρδευση και λίπανση των καλλιεργειών μία αυτοματοποιημένη διαδικασία που με τις κατάλληλες πληροφορίες από διάφορους αισθητήρες θα παράγουν το κατάλληλο αποτέλεσμα. Η διαφορά της κανονικής καλλιέργειας με την καλλιέργεια θερμοκηπίου είναι ότι μπορείς να δημιουργήσεις τις κατάλληλες συνθήκες, ώστε να μπορούν να παραχθούν προϊόντα όλο τον χρόνο και όχι συγκεκριμένους μήνες, όπως γίνεται στις κανονικές καλλιέργειες.

Ο τομέας της κτηνοτροφίας είναι αρκετά πολυμορφικός και πολυεπίπεδος, γιατί χρειάζεται η παρακολούθηση πολλών σταδίων από την αρχή που εισέρχεται το ζώο στην

κτηνοτροφική μονάδα μέχρι και το τελευταίο στάδιο που φεύγει. Θα πρέπει να παρακολουθείται το ζώο όταν κοιμάται, όταν βοσκάει ακόμα και όταν μασάει τροφή για να παραχθεί το δυνατότερο καλύτερο αποτέλεσμα. Ο πυλώνας της βιομηχανίας έχει αρκετές εφαρμογές που μπορούν να βοηθήσουν στην καλύτερη διεκπεραίωση του σχεδιασμού, υλοποίησης, ελέγχου, της ρομποτικής αλλά και της υγείας των μηχανημάτων. Για την καλύτερη λειτουργεία χρειάζονται πολύ αισθητήρες που να παρακολουθούν συλλογικά και σε πραγματικό χρόνο όλα τα συστήματα, ώστε να υπάρχει μία ομαλή λειτουργία παρότι υπάρχει μεγάλος όγκος πακέτων και οχημάτων.

Στον τομέα της ρομποτικής με την βοήθεια ρομπότ και των ασύρματων δικτύων αισθητήρων μπορούν να δημιουργηθούν πχ σε μία μεγάλη αποθήκη με πολλές χιλιάδες προϊόντα, χάρτες ώστε τα ρομπότ με αυτοματοποιημένο τρόπο να μπορούν είτε να τοποθετούν είτε να προμηθεύονται προϊόντα από ράφια. Για την λειτουργεία αυτού του αυτοματισμού θα πρέπει να υπάρχουν αισθητήρες στο πάτωμα στα ράφια αλλά και στο ταβάνι για να μπορεί να λειτουργεί τελείως αυτοματοποιημένα και γρήγορα. Τα τελευταία χρόνια που στα εργοστάσια όλα δημιουργούνται με μεγάλα μηχανήματα χρησιμοποιούνται αισθητήρες στα μηχανήματα για να ανιχνεύσουν αλλά και να προβλέψουν πιθανόν λάθη που ενδεχομένως να εμποδίζουν την εύρυθμη λειτουργία τους ή ακόμα χειρότερα το ενδεχόμενο να καταστραφούν ολοκληρωτικά.

Οι αστικές εφαρμογές είναι ο τελευταίος μεγάλος πυλώνας και είναι ένας πυλώνας που ο περισσότερος κόσμος έχει μεγάλη επαφή μαζί του χωρίς να το γνωρίζει, αποτελείται από τα έξυπνα σπίτια, έξυπνες πόλεις, συστήματα μεταφορών και παρακολούθηση δομικής υγείας. Σε πόλεις που είναι μεγάλες σε έκταση αλλά και πολύ πυκνοκατοικημένες πρέπει να παρθούν κάποια μέτρα ώστε οι πολίτες να έχουν μία βέλτιστη ζωή. Κάποια από τα μέτρα που θα μπορούσαν να εφαρμοστούν είναι αισθητήρες σε δρόμους, ώστε να μπορούν να ελέγχουν οι πολίτες ποιοι δρόμοι έχουν κίνηση και ποιοι όχι. Ένα «έξυπνο» σύστημα σε περιοχές πάρκινγκ για αυτοκίνητα όπου με έναν αισθητήρα θα δίνει την δυνατότητα να ενημερώνει την βάση δεδομένων και να ξέρουν οι διαχειριστές αν υπάρχει ή όχι κάποιο αυτοκίνητο στο συγκεκριμένο σημείο. Με αυτό τον τρόπο θα μπορούσε να δημιουργηθεί ένας αυτοματισμός και οι πληρωμές να γίνονται αυτόματα ανάλογα με τον χρόνο που έχουν παραμείνει στην θέση πάρκινγκ έτσι ώστε να μπορεί να είναι αυτόνομο και να μην χρειάζεται ο πολίτης να περιμένει τους υπαλλήλους για να πληρώσει και να φύγει. Με αυτό τον τρόπο θα μπορούσαν να δημιουργηθούν και στατιστικά για τις πιο έντονες ώρες που χρησιμοποιείτε το πάρκινγκ και να παρθούν καλύτερες αποφάσεις.

Το «έξυπνο» σπίτι πλέον δεν είναι ένα μακρινό όνειρο αλλά πραγματικότητα και «μπήκε» στις ζωές τον ανθρώπων για την καταπολέμηση πολλών προβλημάτων. Ένα από αυτά είναι η εσωτερική ποιότητα αέρα στα κτήρια, το οποίο παίζει πολύ σημαντικό ρόλο μιας και πολύ άνθρωποι τις περισσότερες ώρες της ημέρας τις περνάνε μέσα σε κάποιο κτήριο

ή σπίτι. Σε πολλά σπίτια έχει καθιερωθεί η εγκατάσταση αισθητήρων αερίου μιας και πολλά σπίτια τα τελευταία χρόνια χρησιμοποιούν αέριο είτε για θέρμανση είτε για να μαγειρέψουν.

Τέλος, η παρακολούθηση δομικής υγείας είναι η τελευταία υποκατηγορία των αστικών εφαρμογών και παίζει πολύ σημαντικό ρόλο σε μία πόλη, διότι λόγο τον αναγκών τα τελευταία χρόνια χρειάζεται να χτίζονται όλο και μεγαλύτερα κτήρια. Επιπλέον, πρέπει να υπάρχει και ένα σύστημα παρακολούθησης που θα παρακολουθεί την ακεραιότητα του κτιρίου, αν έχουν γίνει ζημιές και το είδος των ζημιών σε περίπτωση σεισμού. [4]

1.4 Χαρακτηριστικά Ασύρματων Δικτύων Αισθητήρων

Τα χαρακτηριστικά των ασύρματων δικτύων αισθητήρων ποικίλουν ανάλογα με τις ανάγκες και την τοποθεσία του δικτύου αλλά κυρίως και ως προς το μέγεθός τους. Συγκεκριμένα, ένα μικρό δίκτυο σε μία εταιρία θα έχει διαφορετικές ανάγκες και χαρακτηριστικά σε σχέση με ένα δίκτυο το οποίο θα είναι σε μέγεθος ενός μητροπολιτικού δικτύου. Πλέον, τέτοιου είδους δίκτυα είναι κατασκευασμένα ώστε να μην χρειάζονται επίβλεψη, και τα δεδομένα που μετράνε στο φυσικό περιβάλλον μεταδίδονται σε πραγματικό χρόνο. Κάποια από τα σημαντικότερα χαρακτηριστικά λοιπόν αυτών των δικτύων είναι τα παρακάτω:

- **Κόστος:** Όταν γίνεται ο σχεδιασμός του δικτύου συνήθως χρειάζονται πολλούς εκατοντάδες κόμβους αισθητήρων για να παρθούν σωστές μετρήσεις σε ένα φυσικό περιβάλλον. Αυτό σημαίνει ότι το συνολικό κόστος αν δεν σχεδιαστεί σωστά το δίκτυο μπορεί να εκτοξευτεί.

- **Χαμηλή κατανάλωση και ενεργειακά αποδοτική:** Η ενέργεια παίζει πολύ σημαντικό ρόλο και χρησιμοποιείται για την τροφοδοσία τον κόμβων αισθητήρων, υπολογισμό, επικοινωνία και αποθήκευση δεδομένων. Επειδή σε αυτά τα δίκτυα αισθητήρων συνήθως οι αισθητήρες τροφοδοτούνται με μπαταρίες, αν γίνει αλόγιστη κατανάλωση ενέργειας τότε θα χρειάζονται συνέχεια επιτήρηση και το κόστος θα ανέβει πολύ. Τα πρωτόκολλα επικοινωνίας και οι αλγόριθμοι που θα χρησιμοποιηθούν θα πρέπει να τα λαμβάνουν υπόψιν τους κατά τον σχεδιασμό για την βελτιστοποίηση του δικτύου.

- **Υπολογιστική ισχύς:** Λόγο του ότι πρέπει να έχουμε όσο το δυνατών λιγότερη κατανάλωση ενέργειας η υπολογιστική ισχύ που χρησιμοποιείται είναι η πλήρως απαραίτητη για την λειτουργεία του δικτύου.

- **Επικοινωνιακές δυνατότητες:** Όπως είναι λογικό στα ασύρματα δίκτυα η επικοινωνία γίνεται μέσω ραδιοκυμάτων χρησιμοποιώντας ένα ασύρματο κανάλι επικοινωνίας. Ανάλογα με την υποδομή, την τοποθεσία, και το μέγεθος του δικτύου χρησιμοποιούνται και οι αντίστοιχες κεραίες και υποδομές ώστε να υπάρχει

αμφίδρομη ή μονόδρομη επικοινωνία. Πολλές φορές λόγω του περιβάλλοντος και των συνθηκών που υπάρχουν σε αυτό με καταιγίδες και κεραυνούς γίνεται αρκετά δύσκολο ώστε να λειτουργήσει ομαλά ένα ασύρματο δίκτυο αισθητήρων. Για αυτόν το λόγο, το υλικό που θα χρησιμοποιηθεί και το λογισμικό πρέπει να είναι εξειδικευμένα για εξωτερική χρήση και να έχουν υπολογίσει την στιβαρότητα, την ασφάλεια και την ανθεκτικότητα του δικτύου.

- **Ασφάλεια και απόρρητο:** Η ασφάλεια είναι πολύ σημαντική και θα πρέπει να είναι πολυεπίπεδη. Αρχικά, θα πρέπει να υπάρχει φυσική ασφάλεια του χώρου αλλά και του εξοπλισμού και μετέπειτα να υπάρχει ασφάλεια σε επίπεδο λογισμικού. Επίσης, θα πρέπει να υπάρχει ασφάλεια στο ασύρματο δίκτυο ώστε να μην επιτρέπει την μη εξουσιοδοτημένη πρόσβαση, επιθέσεις εξωτερικές αλλά και εσωτερικές στους κόμβους αισθητήρων. Μεγάλο ρόλο παίζει επίσης και η ακεραιότητα των πληροφοριών, ώστε να αποφευχθούν τυχόν ακούσιες βλάβες που μπορούν να παραμετροποιήσουν τα δεδομένα. Τέλος, θα πρέπει να υπάρχουν και μηχανισμοί για την ιδιωτικότητα και το απόρρητο.

- **Κατανεμημένη ανίχνευση και επεξεργασία**: Καθώς ο αριθμός των κόμβων των αισθητήρων τους είναι αρκετά μεγάλος, κατανέμονται είτε ομοιόμορφα η τυχαία. Στα ασύρματα δίκτυα αισθητήρων ο κάθε κόμβος είναι ικανός να συλλέγει, ταξινομεί, επεξεργάζεται και να συγκεντρώνει τα δεδομένα ώστε να σταλούν στον κεντρικό σταθμό. Με αυτό τον τρόπο και έχοντας κατανέμει τους αισθητήρες, παρέχεται στο σύστημα μία ανθεκτικότητα.

- **Δυναμική τοπολογία δικτύου:** Τα ασύρματα δίκτυα αισθητήρων είναι σχεδιασμένα με τέτοιον τρόπο ώστε αν κάποιος αισθητήρας σταματήσει να λειτουργεί λόγω εξάντλησης της μπαταρίας ή άλλων περιστάσεων, όπως εάν διακοπεί η επικοινωνία, θα συνεχίσουν να λειτουργούν και να είναι δίνουν πληροφορίες. Επίσης, ακόμα και αν πρέπει να προστεθούν επιπλέον αισθητήρες ή κόμβοι αισθητήρων θα πρέπει το δίκτυο δυναμικά να μπορεί να αλλάζει. Θα πρέπει λοιπόν να μπορούν να αναδιαμορφώνονται και να ρυθμίζονται από μόνα τους τέτοιου είδους δίκτυα.

- **Αυτο-οργάνωση:** Επειδή το περιβάλλον στο οποίο βρίσκονται οι κόμβοι αισθητήρων είναι εχθρικό, αφύλακτο και αναπτύσσονται με άγνωστο τρόπο, θα πρέπει να αυτό-οργανώνονται. Συνήθως υπάρχει κάποιος κατανεμημένος αλγόριθμος ο οποίος προσαρμόζει τους κόμβους αισθητήρων για να σχηματίζουν αυτόματα το δίκτυο.

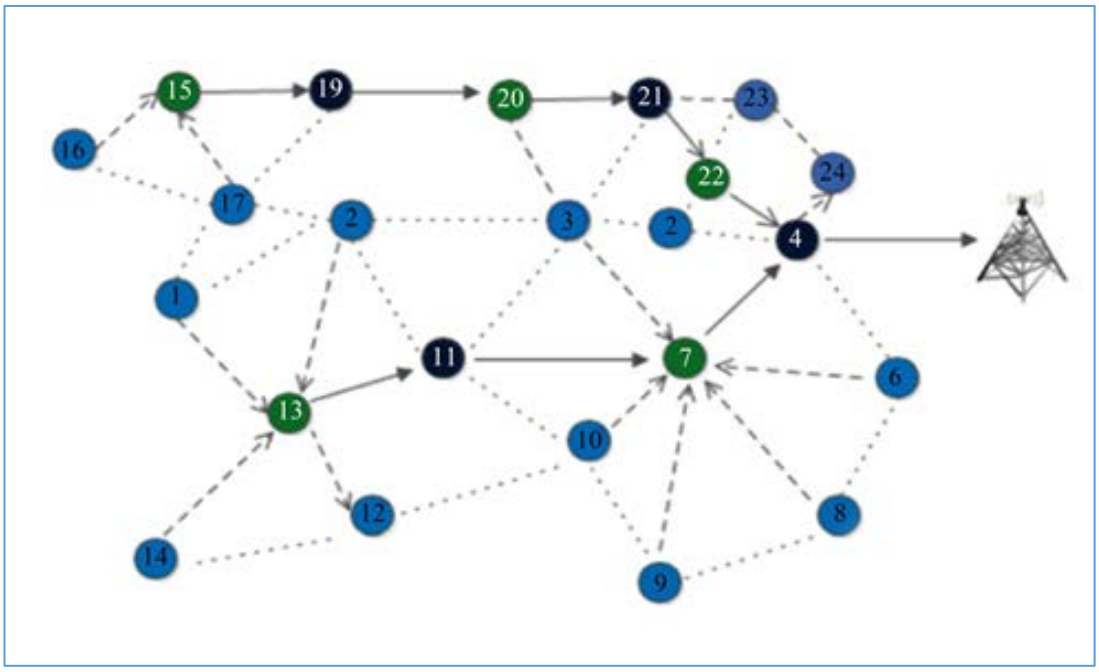
- **Προσανατολισμός στην εφαρμογή:** Λόγω της φύσης τους τα ασύρματων δίκτυα αισθητήρων διαφέρουν από τα συμβατικά δίκτυα και πολλοί παράγοντες εξαρτούνται σε μεγάλο βαθμό από τις εφαρμογές που θα χρησιμοποιηθούν. Οι κόμβοι αισθητήρων αναπτύσσονται τυχαία λόγω της τοποθεσίας αλλά και της χρήσης της εφαρμογής.

- **Στιβαρές λειτουργίες:** Οι αισθητήρες σε αυτού του τύπου δικτύων συνήθως βρίσκονται σε εχθρικό περιβάλλον για την λειτουργία τους, οπότε υπάρχουν συγκεκριμένες ανάγκες που πρέπει να καλυφθούν. Θα πρέπει οι αισθητήρες να είναι

αρκετά ανθεκτικοί σε σφάλματα και λάθη, επομένως και οι κόμβοι αισθητήρων θα πρέπει να έχουν την δυνατότητα να ερμηνεύουν αυτά τα δεδομένα και να τρέχουν κάποια διαγνωστικά ώστε να αυτοεπιδιορθώνονται.

- **Μικρό φυσικό μέγεθος:** Οι αισθητήρες πλέον έχουν πάρα πολύ μικρό μέγεθος, πράγμα που σημαίνει ότι δεν σπαταλάνε και πολλή ενέργεια. Λόγω όμως του μικρού τους μεγέθους, η εμβέλεια τους είναι σημαντικά μικρότερη και για αυτό το λόγο σε δίκτυα αισθητήρων υπάρχουν πάρα πολλοί αισθητήρες ή κόμβοι αισθητήρων. Λόγω της μικρής ενέργειας που διαθέτουν η επικοινωνιακή τους ικανότητα είναι αρκετά χαμηλή.

- **Multi-hop επικοινωνία:** Σε μεγάλα ασύρματα δίκτυα αισθητήρων ο αριθμός των κόμβων αισθητήρων αναπτύσσεται με ραγδαίο ρυθμό και ο πιο εφικτός τρόπος επικοινωνίας γίνεται με ενδιάμεσους σταθμούς βάσεων που βοηθούν στην καλύτερη δρομολόγηση των δεδομένων δικτύου. Εάν εμφανιστεί η ανάγκη επικοινωνίας ενός σταθμού βάσης ή κόμβου αισθητήρων που είναι σε άλλη ραδιοσυχνότητα, θα πρέπει να γίνει μέσω multi-hop διαδρομής, δηλαδή, μέσω ενός η περισσότερων ενδιάμεσων κόμβων.



Εικόνα 3. Multi-hop Επικοινωνία

Πηγή:https://www.scirp.org/journal/paperinformation.aspx?paperid=104323

1.5 Στόχοι Αρχιτεκτονικής Σχεδιασμού WSN

Ο σχεδιασμός ασύρματου δικτύου αισθητήρων είναι αρκετά δύσκολος, διότι χωρίζεται σε αρκετούς τομείς τεχνολογιών οι οποίοι αναπτύσσονται ραγδαία και καινούργιες

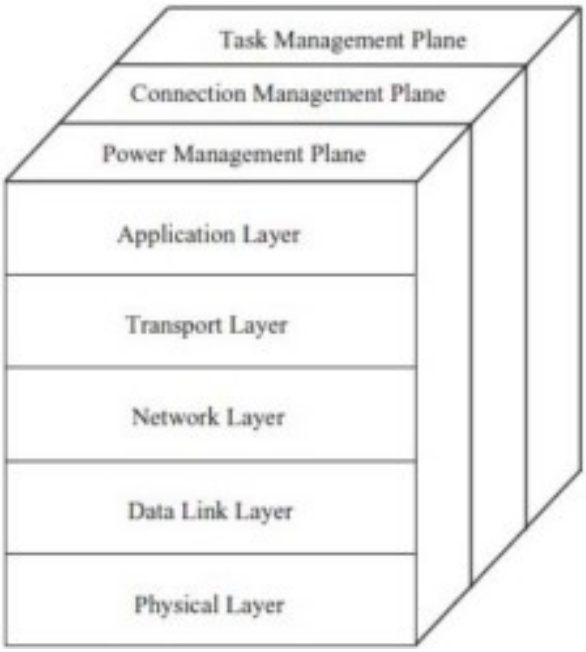
τεχνολογίες «γεννιούνται» καθημερινά για όλων των ειδών εφαρμογής. Λόγω των χαρακτηριστικών αυτών των δικτύων και των πολυάριθμων προκλήσεων που υπάρχουν για την ανάπτυξη των κόμβων αισθητήρων, πρέπει να τεθούν πρώτα κάποιοι στόχοι, πριν γίνει ο σχεδιασμός του δικτύου. Ωστόσο, για την κατάλληλη αντιμετώπιση οποιασδήποτε πρόκλησης θα πρέπει το δίκτυο αισθητήρων να διαθέτει ευέλικτους μηχανισμούς ούτως ώστε να υπάρχει αποτελεσματική και άνετη χρήση. Για να μπορεί να γίνει αυτό κάποιοι από τους στόχους που πρέπει να λάβουμε υπόψιν μας για την σχεδίαση της αρχιτεκτονικής σχεδιασμού είναι οι παρακάτω:

- ✓ **Προσδιορισμός των απαιτήσεων της εφαρμογής:** Όπως έχουμε αναλύσει πιο πάνω, για να γίνει σωστή σχεδίαση ενός πολύπλοκου συστήματος θα πρέπει να έχουμε πλήρη και σαφή εικόνα των αναγκών της εφαρμογής και να γίνει ολοκληρωτική ανάλυση για να υπάρξει ο καλύτερος δυνατόν σχεδιασμός.
- ✓ **Προσδιορισμός σχετικών τεχνολογικών τάσεων:** Αφού έχουμε εικόνα με τις ανάγκες τις εφαρμογής θα πρέπει να γίνει έλεγχος για την καλύτερη δυνατή τεχνολογική λύση διότι σε ένα πολύπλοκο δίκτυο αισθητήρων το κόστος μπορεί να αυξηθεί ραγδαία. Πρέπει να βρεθεί μία λύση με το λιγότερο δυνατό κόστος αλλά επίσης και με την καλύτερη δυνατή βελτιστοποίηση μέγιστης ενέργειας με βάση την εφαρμογή.
- ✓ **Βελτιστοποίηση σχεδιασμού:** Οι κόμβοι αισθητήρων έχουν περιορισμένους πόρους και για αυτό το λόγο θα πρέπει η σχεδίαση του δικτύου να είναι πάρα πολύ καλά βελτιστοποιημένη ώστε να έχουμε την μέγιστη δυνατή αξιοποίηση του αισθητήρα με την ελάχιστη δυνατή χρήση των πόρων του.
- ✓ **Τεχνικές και τεχνολογία σχεδιασμού:** Όταν γίνεται ο σχεδιασμός ενός ασύρματου δικτύου αισθητήρων θα πρέπει να σχεδιαστεί όχι μόνο με βάση με τα σημερινά δεδομένα αλλά και με την επερχόμενη τεχνολογία και αρχιτεκτονική που θα ακολουθήσει. Υπάρχουν όμως και κάποια εξαρτήματα, όπως ο αποθηκευτικός χώρος και η τροφοδοσία ισχύος που η τεχνολογία τους θεωρείται ώριμη και δεν αναπτύσσεται με πολύ γρήγορους ρυθμούς. Το αντίθετο ισχύει όμως για την ασύρματη επικοινωνία με εξαιρετικά χαμηλή ισχύ, τους αισθητήρες και τους ενεργοποιητές που αναβαθμίζονται πολλές φορές μέσα στον χρόνο. [6]

1.6 Μοντέλο OSI (Open Systems Interconnection)

Το μοντέλο αναφοράς OSI είναι ένα πλαίσιο ή μια ιεραρχική δομή επτά επιπέδων που καθορίζει τις προδιαγραφές επικοινωνίας που απαιτούνται για την επικοινωνία μεταξύ δύο υπολογιστών ή δικτυωμένων συστημάτων. Στην περίπτωση των ασύρματων δικτύων αισθητήρων υπάρχουν πέντε επίπεδα αντί για εφτά και δεν χρησιμοποιούνται τα επίπεδα συνόδου και παρουσίασης. Προστέθηκαν πάνω από αυτά τα πέντε επίπεδα τρία ακόμα επίπεδα για την καλύτερη διαχείριση του δικτύου και των αισθητήρων ώστε να

συνεργάζονται καλύτερα και να υπάρχει καλύτερη αποδοτικότητα στο δικτύου. Αναπτύχθηκε από τον Οργανισμό Διεθνών Προτύπων (International Organization for Standardization ISO) στα τέλη της δεκαετίας του 1970 και χρησιμοποιείται ακόμα και σήμερα σαν μοντέλο αναφοράς.



Εικόνα 4 Μοντέλο OSI WSN

Πηγή:https://ijcsit.com/docs/Volume%206/vol6issue04/ijcsit2015060490.pdf

Πηγή:https://ijcsit.com/docs/Volume%206/vol6issue04/ijcsit2015060490.pdf

Η επικοινωνία μεταξύ δύο συστημάτων γίνεται κυρίως με τα πρώτα τρία επίπεδα, (**Φυσικό, Σύνδεσης Δεδομένων** και **Δικτύου**) όπου γίνεται ο έλεγχος της μετάδοσης μηνυμάτων, ενώ τα υπόλοιπα δύο επίπεδα (**Μεταφοράς,** και **Εφαρμογής**) είναι εκεί για να παρέχουν την αξιοπιστία και την ακεραιότητα των δεδομένων από το ένα άκρο της επικοινωνίας στο άλλο. Η επικοινωνία δεν είναι πάντα ίδια, πράγμα που σημαίνει ότι μπορεί να μην χρειάζεται να περάσει από όλα τα επίπεδα για να δημιουργηθεί, αλλά αυτό κρίνεται από τις ανάγκες της εφαρμογής. Παρακάτω θα αναλυθούν ένα προς ένα τα επίπεδα σε μεγαλύτερο βάθος:

1. **Φυσικό Επίπεδο:** Είναι το πρώτο επίπεδο του OSI μοντέλου και εκεί καθορίζονται οι ηλεκτρικές και φυσικές προδιαγραφές του συνδέσμου δεδομένων. Εδώ καθορίζεται η σχέση μεταξύ των συσκευών όπου το φυσικό μέσο μετάδοσης είναι συνήθως χαλκός ή όπως τα τελευταία χρόνια καλώδιο οπτικών ινών. Αυτό περιλαμβάνει την διάταξη ακροδεκτών σε ένα καλώδιο, την τάση, την εμπέδηση, προδιαγραφές του καλωδίου, χρονισμός σήματος, hubs, αναμεταδότες, προσαρμογείς δικτύου, προσαρμογείς διανομέων που χρησιμοποιούνται συνήθως στην αποθήκευση. Επίσης, καθορίζει το πρωτόκολλο για τη δημιουργία και τον τερματισμό μιας

σύνδεσης μεταξύ δύο άμεσα συνδεδεμένων κόμβων μέσω ενός μέσου επικοινωνίας. Μπορεί να οριστεί ένα πρωτόκολλο για τον έλεγχο της ροής των πληροφοριών αλλά και την δημιουργία μιας (όχι απαραίτητα αξιόπιστης) σύνδεσης μεταξύ δύο άμεσα συνδεδεμένων κόμβων. Επίσης, εδώ γίνεται και η διαμόρφωση ή μετατροπή ψηφιακών δεδομένων στον εξοπλισμό του χρήστη αλλά και τα σήματα που μεταδίδονται μέσω ενός φυσικού καναλιού επικοινωνίας. Τέλος είναι υπεύθυνο για την επιλογή και δημιουργία συχνότητας, ανίχνευση σήματος, διαμόρφωσης και κρυπτογράφησης των δεδομένων.

2. **Επίπεδο Ζεύξης Δεδομένων:** Σε αυτό το επίπεδο παρέχεται η αξιοπιστία μετάδοσης δεδομένων που γίνεται σε κομμάτια (frames) μεταξύ μιας συσκευής τοπικού δικτύου σε μία άλλη ενώ έχει χτιστεί πάνω από την αναξιόπιστη μεταφορά δεδομένων bit που παρέχεται από το προηγούμενο φυσικό επίπεδο. Για να επιτευχθεί αυτό, το επίπεδο ζεύξης δεδομένων εκτελεί κάποιους ελέγχους σφαλμάτων Cyclic Redundancy Check(CRC). Θα πρέπει να δώσουμε βάση ότι αυτό το επίπεδο ζεύξης παρέχει την αξιοπιστία των δεδομένων όταν πρόκειται για μετάδοση που γίνεται μεταξύ 2 συσκευών που τα συνδέει μόνο μία ζεύξη. Εάν ανάμεσα στις δύο συσκευές υπάρχουν και άλλες ζεύξεις και δεν είναι άμεσα συνδεδεμένες μεταξύ τους, τότε δεν διασφαλίζεται η αξιοπιστία και την ευθύνη την αναλαμβάνει κάποιο ανώτερο επίπεδο. Επίσης, σε αυτό το επίπεδο η επικοινωνία γίνεται με βάση την διεύθυνση MAC κάθε συσκευής και για αυτόν τον λόγο ονομάζεται και επίπεδο MAC (Media Access Control) η αλλιώς ελέγχου προσπέλασης στο μέσο. Αυτές οι διευθύνσεις είναι ενσωματωμένες σε κάθε συσκευή από τον κατασκευαστή και είναι μοναδικές φυσικές διευθύνσεις. Από τα πιο γνωστά πρωτόκολλά αυτού του επιπέδου είναι τα Ethernet, LAP-D σε δίκτυα ISDN.

3. **Επίπεδο Δικτύου:** Στο προηγούμενο επίπεδο αναλύσαμε πώς χρησιμοποιείται για την μέθοδο με την οποία γίνεται η μεταφορά δεδομένων στο φυσικό επίπεδο. Σε αυτό το επίπεδο γίνεται η οργάνωση και ο τεμαχισμός των δεδομένων που ονομάζονται πακέτα αλλά και η επανασυναρμολόγηση τους. Για την αποστολή των πακέτων θα πρέπει να τους δοθεί μία διαδρομή και κάποια διεύθυνση, ώστε να ξέρουν πώς να δρομολογηθούν. Έτσι, λοιπόν, το επίπεδο δικτύου εκτελεί λειτουργίες δρομολόγησης αλλά και έλεγχο ροής για την αποφυγή πιθανών λαθών, μιας και τα δεδομένα ή αλλιώς πακέτα δεν φεύγουν πάντα από την ίδια διαδρομή, αλλά αναλόγως τις συνθήκες μπορεί να διαλέξουν διαφορετική διαδρομή. Για αυτόν τον λόγο επειδή τα πακέτα για να αποσταλούν πρέπει να τεμαχιστούν και όταν φτάσουν στον παραλήπτη να επανασυναρμολογηθούν θα πρέπει να γίνεται και αναφορά σφαλμάτων παράδοσης πακέτων. Το πρωτόκολλο είναι γνωστό με το όνομα IP (Internet Protocol) Πρωτόκολλο Διαδικτύου. Υπάρχει μία διαφοροποίηση για τα WSN όπου θα πρέπει να λάβει υπόψιν του το επίπεδο κάποιες σημαντικές προκλήσεις όπως η εξοικονόμηση ενέργειας, η περιορισμένη μνήμη αλλά και η κρυφή μνήμη στους αισθητήρες.

4. **Επίπεδο Μεταφοράς:** Η αξιόπιστη μεταφορά δεδομένων παρέχεται από το επίπεδο μεταφοράς και παρέχει επικοινωνία από άκρο σε άκρο μεταξύ διάφορων διεργασιών που εκτελούνται σε διαφορετικούς υπολογιστές. Υπάρχουν κάποιες διαφορές από το επίπεδο ζεύξης δεδομένων και μερικές από αυτές είναι προσανατολισμό στον χρήστη, διαπραγμάτευση της ποιότητας και του τύπου των υπηρεσιών, εγγύηση υπηρεσίας, έλεγχο ροής και συμφόρησης αλλά και δημιουργία, χρήση και τερματισμός μιας σύνδεσης. Τα πρωτόκολλα στα WSN χρησιμοποιούν ποικίλους μηχανισμούς για την ανίχνευση και την αποκατάσταση απωλειών.

5. **Επίπεδο Εφαρμογής:** Είναι υπεύθυνο για τη διαχείριση της κυκλοφορίας και της παροχής λογισμικού για διάφορες εφαρμογές που μετατρέπουν τα δεδομένα σε μία κατανοητή μορφή ώστε να μπορούν να τα χρησιμοποιήσουν ή στέλνουν ερωτήματα για την απόκτηση πληροφοριών. Εδώ υποστηρίζονται οι διεργασίες εφαρμογών και τελικών χρηστών και λαμβάνονται πληροφορίες όπως η πιστοποίηση ταυτότητας και προσδιορίζονται τυχόν περιορισμοί στη σύνταξη των δεδομένων. [7]

   Τέλος τα τρία επιπλέον επίπεδα για την καλύτερη διαχείριση των WSN είναι:

   1. **Επίπεδο διαχείρισης ισχύος:** Είναι υπεύθυνο για την διαχείριση ισχύος ενός κόμβου αισθητήρα κατά την διάρκεια της ανίχνευσης, της επεξεργασίας και της επικοινωνίας.

   2. **Επίπεδο διαχείρισης σύνδεσης:** Είναι υπεύθυνο για την διαμόρφωση και αναδιαμόρφωση των κόμβων αισθητήρων και για την δημιουργία και διατήρηση της συνδεσιμότητας του δικτύου.

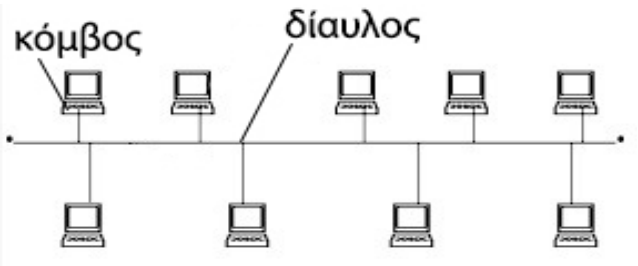
   3. **Επίπεδο διαχείρισης εργασιών:** Είναι υπεύθυνο για την κατανομή εργασιών ανάμεσα στους κόμβους αισθητήρων ώστε να βελτιστοποιηθεί η κατανάλωση ενέργειας και να αυξηθεί η διάρκεια ζωής τους δικτύου. [8]

1.7 Τοπολογίες WSN

Η ανάπτυξη, η δομή αλλά και η εγκατάσταση ενός ασύρματου δικτύου αισθητήρων έχουν δώσει μία διαφορετική νότα στις παραδοσιακές τοπολογίες δικτύων. Υπάρχουν πάρα πολλές διαφορετικές τοπολογίες υλοποίησης ασύρματων δικτύων αισθητήρων [8], αλλά παρακάτω θα αναλυθούν οι πιο γνωστές όπως Bus, Tree, Mesh, Star, Ring, Flat-based, Cluster-based, Hierarchical -based topology, κλπ. [9].

- **Τοπολογία Διαύλου (Bus):** Στην τοπολογία διαύλου υπάρχουν κόμβοι αισθητήρων που συνδέονται σε ένα κεντρικό καλώδιο το οποίο είναι ο κορμός

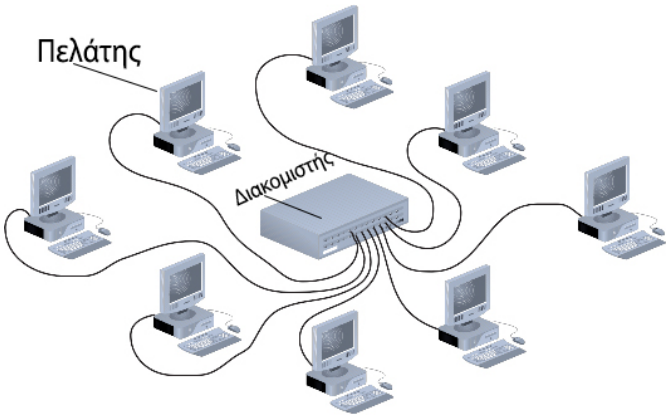
του δικτύου και η διαφορά του σε ένα ασύρματο δίκτυο αισθητήρων είναι ότι οι κόμβοι είναι συνδεδεμένοι ασύρματα. Ο τρόπος που λειτουργεί είναι ότι ο κόμβος αισθητήρων στέλνει ένα μήνυμα broadcast (δηλαδή σε όλο το υποδίκτυο που ανήκει) σε ένα άλλο κόμβο και όλοι μπορούν να το δουν, αλλά μόνο ο προοριζόμενος παραλήπτης λαμβάνει και μπορεί να επεξεργαστεί το μήνυμα. Η τοπολογία αυτή είναι πολύ απλή και εύκολη στην εγκατάσταση και λειτουργεί καλά μόνο με μικρό αριθμό κόμβων αισθητήρων, καθώς όσο ανεβαίνει ο αριθμός των κόμβων παρουσιάζονται προβλήματα απόδοσης.



Εικόνα 5. Τοπολογία Διαύλου

Πηγή:https://ijcrt.org/papers/IJCRT2205629.pdf

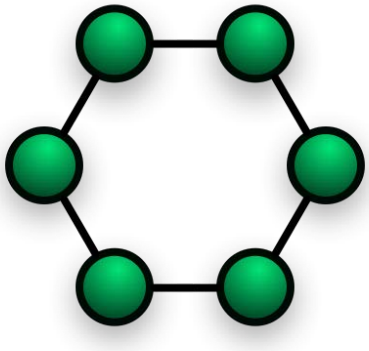
- **Τοπολογία Αστέρα (Star):** Η τοπολογία αστέρα χρησιμοποιείται συχνότερα από όλες τις υπόλοιπες τοπολογίες για την δημιουργία δικτύων αισθητήρων. Σε αυτήν την τοπολογία όλοι οι κόμβοι αισθητήρων είναι συνδεδεμένοι άμεσα με έναν κεντρικό κόμβο όπου όλα τα δεδομένα καταλήγουν σε αυτόν και μετά φεύγουν εκτός δικτύου. Λόγω της τοπολογίας που έχει, ένας κεντρικός κόμβος λειτουργεί σαν δίκτυο προσωπικού χώρου και οι υπόλοιποι κόμβοι δεν μπορούν να επικοινωνήσουν άμεσα μεταξύ τους παρά μόνο αν η πληροφορία περάσει πρώτα από τον κεντρικό κόμβο. Ο κεντρικός κόμβος ονομάζεται “διακομιστής” ενώ οι κόμβοι που είναι άμεσα συνδεδεμένοι σε αυτόν “πελάτες” και επειδή οι κόμβοι πελάτες εξαρτώνται από τον κόμβο διακομιστή υπάρχουν θετικά και αρνητικά. Κάποια από τα αρνητικά είναι ότι το δίκτυο πρέπει να σχεδιαστεί με συγκεκριμένο τρόπο ώστε η επικοινωνία να είναι μέσα στην έγκυρη εμβέλεια ραδιομετάδοσης που είναι από 30-100 μέτρα. Αν καταρρεύσει ο κεντρικός κόμβος, τότε καταρρέει όλο το δίκτυο, όπως επίσης και αν φορτωθεί ο κεντρικός κόμβος με πολλούς κόμβους πελάτη, τότε θα υπάρχει εξάντληση πόρων κατανάλωσης ενέργειας και δεν μπορεί να γίνει περεταίρω επέκταση του δικτύου. Μερικά από τα θετικά είναι ότι αν κάποιος κόμβος πελάτη καταρρεύσει δεν επηρεάζεται όλο το δίκτυο, είναι επίσης πολύ εύκολο στον σχεδιασμό και στην υλοποίηση αλλά και στην επέκταση του. Η απόδοση της τοπολογίας αστέρα είναι αρκετά ταχύτερη σε σχέση με άλλες τοπολογίες, αν υπάρχει μικρός αριθμός από κόμβους πελάτη που συνδέονται με τον κόμβο διακομιστή.



Εικόνα 6. Τοπολογία Αστέρα

Πηγή:https://networksmania.wordpress.com/topics/network-topology/star-topology/

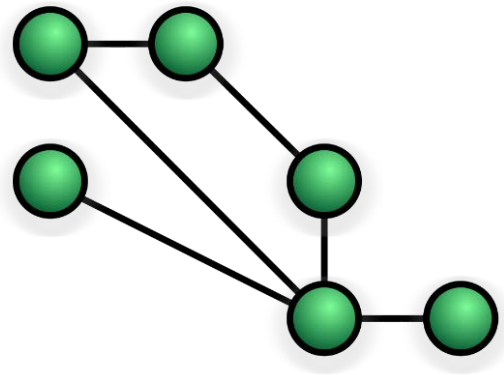
- **Τοπολογία Δακτυλίου (Ring):** Στην Τοπολογία δακτυλίου κάθε κόμβος αισθητήρων συνδέεται άμεσα με τους δύο διπλανούς του κόμβους αισθητήρων δημιουργώντας έτσι έναν δακτύλιο. Όλες οι πληροφορίες ταξιδεύουν είτε αριστερόστροφα είτε δεξιόστροφα επειδή δεν υπάρχει κάποιος κεντρικός κόμβος σε αυτήν την τοπολογία, έτσι όλοι οι κόμβοι μπορούν να μεταδώσουν πακέτα πληροφορίων χρησιμοποιώντας γειτονικούς κόμβους αισθητήρων. Με αυτό το τρόπο το μήνυμα που μεταδίδει ένας κόμβος αισθητήρων θα μεταδοθεί από κάθε κόμβο σε μία συνεχή και κυκλική διαδρομή αλλά μόνο ο κόμβος που προοριζόταν για αυτό το μήνυμα το λαμβάνει και το επεξεργάζεται. Η τοπολογία δακτυλίου είναι αρκετά εύκολη στην εγκατάσταση και τροποποίηση ειδικά όταν πρέπει να αφαιρέσεις ή να προσθέσεις κόμβους αισθητήρων, όπως μάλιστα και όταν υπάρχει ελαττωματικός κόμβος να απομονωθεί. Στα αρνητικά που έχει η τοπολογία αυτή είναι ότι το κάθε μήνυμα πρέπει να μεταδοθεί σε ολόκληρο το δίκτυο (broadcast packet) κάνοντας το έτσι αρκετά χρονοβόρο αλλά και αρκετά ενεργοβόρο. Ένα ακόμα αρνητικό είναι η μεγάλη συμφόρηση που δημιουργείται στο δίκτυο άλλα και όταν υπάρχει μεταφορά δεδομένων και δεξιόστροφα και αριστερόστροφα τότε το πρόβλημα είναι εμφανέστατο. Η καθυστέρηση της επικοινωνίας είναι ανάλογη με τον αριθμό των κόμβων αισθητήρων στο δίκτυο κάτι που δεν μας επιτρέπει την δημιουργία μεγάλων δικτύων αισθητήρων.



Εικόνα 7. Τοπολογία Δακτυλίου

Πηγή:https://ijcrt.org/papers/IJCRT2205629.pdf

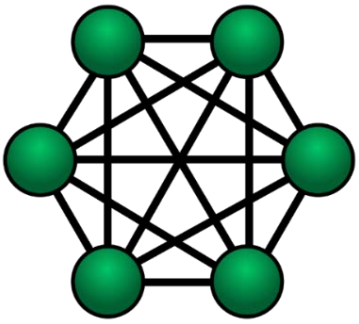
- **Κατανεμημένη Τοπολογία (Mesh):** Οι κατανεμημένες τοπολογίες συναντώνται συχνότερα στην ασύρματη δικτύωση αισθητήρων λόγω της ευελιξία τους αλλά και της λογικής τους τοπολογίας. Στις κατανεμημένες τοπολογίες οι κόμβοι συνδέονται μεταξύ τους και μεταδίδουν δεδομένα από έναν κόμβο σε άλλους κόμβους του δικτύου εφόσον είναι σε εμβέλεια μετάδοσης. Ένα καλό που έχει αυτή η τοπολογία είναι ότι μας επιτρέπεται η επικοινωνία πολλαπλών βημάτων, πράγμα που σημαίνει ότι, εάν κάποιος κόμβος αισθητήρα βρίσκεται εκτός εμβέλειας μετάδοσης, τότε μπορεί να μεταδώσει το μήνυμα σε άλλο κόμβο αισθητήρα χρησιμοποιώντας την μέθοδο πολλαπλών βημάτων. Με αυτό τον τρόπο χρησιμοποιεί ενδιάμεσους κόμβους αισθητήρων για την επικοινωνία και μετάδοση του μηνύματος στον επιθυμητό κόμβο αισθητήρων που θεωρητικά βρίσκεται εκτός εμβέλειας. Υπάρχουν δύο υποκατηγορίες της τοπολογίας, η μερικώς κατανεμημένη και η πλήρως κατανεμημένη. Στην μερικώς κατανεμημένη ένας κόμβος είναι συνδεδεμένος με περισσότερο από έναν κόμβο αισθητήρων, ενώ στην πλήρως κατανεμημένη τοπολογία όλοι οι κόμβοι είναι πλήρως συνδεδεμένη μεταξύ τους.



Εικόνα 8. Μερικώς Κατανεμημένη Τοπολογία

Πηγή:https://ijcrt.org/papers/IJCRT2205629.pdf

Το να είναι όλοι οι κόμβοι συνδεδεμένοι μεταξύ τους έχει πλεονεκτήματα όπως το να είναι πολύ εύκολα στην επέκτασή τους αλλά και στην δημιουργία εφεδρικών κόμβων αν κάτι πάει στραβά να μην κατάρρευση το δίκτυο. Όταν είναι πλήρως συνδεδεμένοι δεν υπάρχουν προβλήματα όπως η εμβέλεια μετάδοσης αλλά επίσης δεν υπάρχει περίπτωση κατάρρευσης του δικτύου μιας και όλοι οι κόμβοι είναι πλήρως συνδεδεμένοι μεταξύ τους. Σε μία τοπολογία που όλοι οι κόμβοι αισθητήρων είναι πλήρως συνδεδεμένοι μεταξύ τους και χρησιμοποιούν την μέθοδο επικοινωνίας πολλαπλών βημάτων (multihop communication) είναι ότι η κατανάλωση ενέργειας είναι αρκετά μεγαλύτερη από τις κατανεμημένες τοπολογίες. Εάν χρειαστεί σε μία τοπολογία να γίνουν πολλαπλές επικοινωνίες με την μέθοδο πολλαπλών βημάτων τότε ο χρόνος παράδοσης του μηνύματος αυξάνεται ραγδαία οπότε ανάλογα με την εγκατάσταση και της ανάγκες μπορεί να εξασθενήσει γρήγορα την ζωή της μπαταρίας. Η τοπολογία αυτή έχει την δυνατότητα να ελέγχει αν κάποιος από τους κόμβους αισθητήρων έχει αποτύχει να επικοινωνήσει ή να μεταδώσει ένα μήνυμα με αποτέλεσμα ο πλησιέστερος κόμβος να επικοινωνήσει ή θα μεταδώσει το μήνυμα αυτόματα. Αυτή η τεχνική είναι αρκετά σημαντική για την σωστή μέτρηση των αισθητήρων στο να μην υπάρχουν κενά επικοινωνίας μεταξύ τον κόμβων.

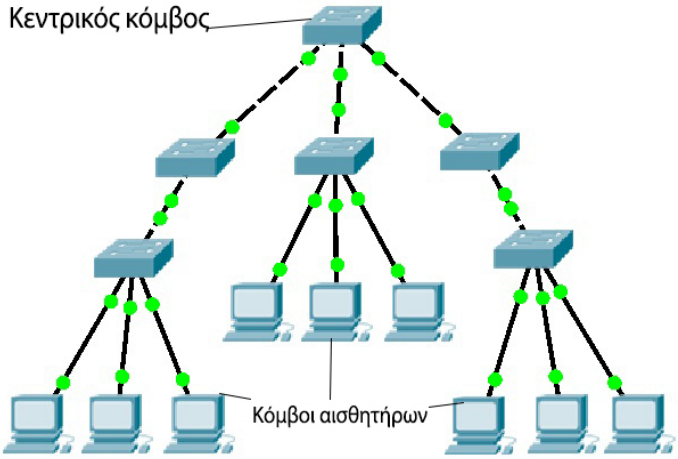


Εικόνα 9. Πλήρως Κατανεμημένη Τοπολογία

Πηγή:https://ijcrt.org/papers/IJCRT2205629.pdf

- **<u>Τοπολογία Δέντρου (Tree):</u>** Η τοπολογία δέντρου είναι μία τροποποιημένη τοπολογία της τοπολογίας διαύλου και αστέρα. Στην τοπολογία δέντρο υπάρχει μία ιεραρχία κόμβων αισθητήρων όπως σε ένα δέντρο η μία ρίζα όπου το υψηλότερο σημείο της ιεραρχίας είναι ο κεντρικός κόμβος. Όλοι οι κόμβοι συνδέονται με τον κεντρικό κόμβο και δημιουργείται μία πολυεπίπεδη τοπολογία που η διαδρομή των πακέτων είναι τέτοια που μπορεί να χρειαστεί ένα ή πολλαπλά βήματα (single or multiple hops) ώστε να μεταφερθούν τα δεδομένα μέσα στην τοπολογία και τέλος, στον κεντρικό κόμβο. Ο κεντρικός κόμβος μπορεί να θεωρηθεί σαν γονέας και οι χαμηλότεροι κόμβοι τα παιδιά, τα οποία είναι οι κόμβοι που αντλούν πληροφορίες από το περιβάλλον και μεταδίδουν από κάτω προς τα πάνω την πληροφορία στον γονικό κόμβο. Το μήνυμα ή τα δεδομένα πρέπει να μεταδίδονται με την ελάχιστη χρονική πολυπλοκότητα και με τη

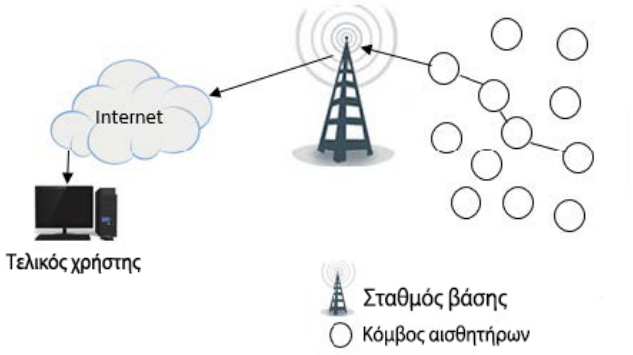
συντομότερη δυνατή διαδρομή για να παραμένει όσο λιγότερο ενεργοβόρα γίνεται η τοπολογία. Το πλεονέκτημα αυτής της τοπολογίας είναι το πόσο εύκολη γίνεται η επεκτασιμότητα της αλλά και η ανίχνευση λάθους από κάποιον κόμβο. Ένα από τα προβλήματα που μπορεί να δημιουργηθούν είναι όταν πρέπει να γίνει εξισορρόπηση του φορτίου (load balancing) μεταξύ των κόμβων και σε αυτήν την τοπολογία υπάρχουν πολλές διαφορετικές διαδρομές που μπορεί να μεταφερθεί η πληροφορία. Μεγάλο αρνητικό είναι επίσης, ότι όσο πιο κοντά στον κεντρικό κόμβο καταρρεύσει κάποιος κόμβος, τότε όλα τα επίπεδα κάτω από αυτό τον κόμβο θα καταρρεύσουν και αυτά μιας και δεν θα είναι συνδεδεμένα με την υπόλοιπη τοπολογία.



Εικόνα 10. Τοπολογία Δέντρου

Πηγή:https://www.hitechmv.com/wp-content/uploads/2014/05/tree-toplo.jpg

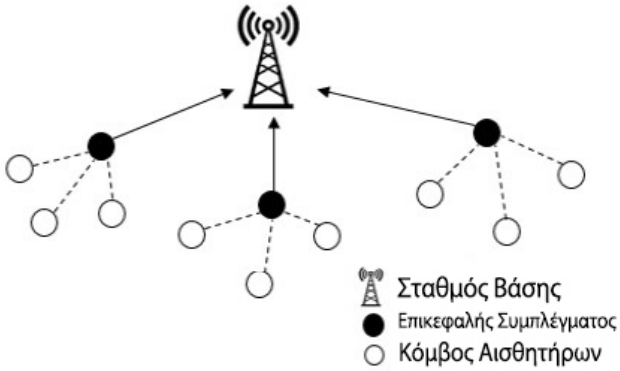
- **Flat-based τοπολογία:** Στην συγκεκριμένη τοπολογία τα πράγματα είναι τελείως διαφορετικά από τις προηγούμενες τοπολογίες και αυτό γιατί όλοι οι κόμβοι αισθητήρων παίζουν τον ίδιο ρόλο, δηλαδή να ανιχνεύουν και να συλλέγουν πληροφορίες, να τις επεξεργάζονται αλλά και να τις μεταδίδουν μέσω πολλαπλών βημάτων (multiple hops). Συνήθως αυτή η τοπολογία χρησιμοποιείται από πρωτόκολλα που συγκεντρώνουν δεδομένα για ανώτατη ανάλυση, πρωτόκολλα δρομολόγησης και πρωτόκολλα χρονοπρογραμματισμού κόμβων. Αυτή η τοπολογία χρησιμοποιεί εξαιρετικά ποιοτικές διαδρομές για τη μετάδοση δεδομένων από τον κόμβο πηγή έως τον ιδιαίτερο κόμβο sink node. Τα δεδομένα λοιπόν που συλλέγονται από τους διάφορους κόμβους αισθητήρων προωθούνται συλλογικά στον ειδικό κόμβο που ονομάζεται sink node και η τοποθέτηση του παίζει μεγάλο ρόλο για την καθυστέρηση αλλά και την κατανάλωση ενέργειας του δικτύου. Η μεταφορά των δεδομένων σε αυτό τον ειδικό κόμβο ονομάζεται πλημμύρα (flooding), γιατί «πλημμυρίζει» τους υπόλοιπους κόμβους με πληροφορίες και ελέγχει τα πακέτα που έχει λάβει από άλλους κόμβους. Η διαδικασία επαναλαμβάνεται μέχρι το πακέτο να φτάσει στον κόμβο προορισμού και σταματάει όταν ο κόμβος, που το μήνυμα προοριζόταν για αυτόν στέλνει πίσω ένα πακέτο ότι έλαβε το μήνυμα.



Εικόνα 11. Flat Based Τοπολογία

Πηγή:https://www.researchgate.net/publication/322668253_Denial_of_Service_DoS_Defence_for_Resource_Availability_in_Wireless_Sensor_Networks

- **Cluster-based τοπολογία:** Η τοπολογία αυτή χρησιμοποιεί μία τεχνική που ομαδοποιεί τους κόμβους σε τρείς κατηγορίες, σε κόμβους αισθητήρων, σε σταθμούς βάσεων αλλά και σε σύμπλεγμα. Όπως και σε άλλες τοπολογίες οι κόμβοι αισθητήρων παίζουν τον ίδιο ρόλο, δηλαδή την παρακολούθηση και ανίχνευση του περιβάλλοντος αλλά και την συλλογή δεδομένων. Η μόνη διαφορά με άλλες τοπολογίες είναι ότι οι κόμβοι αισθητήρων στέλνουν τα δεδομένα που ανιχνεύουν και έχουν είδη επεξεργαστεί πρώτα σε έναν κόμβο που είναι ο επικεφαλής του συμπλέγματος. Κάθε σύμπλεγμα που έχει δημιουργηθεί επιλέγει ποιος κόμβος θα είναι επικεφαλής για να λειτουργήσει ως γέφυρα επικοινωνίας με τον σταθμό βάσης. Η λειτουργία του επικεφαλή κόμβου είναι πολύ απλή καθώς αρχικά συγκεντρώνει δεδομένα για όλους τους κόμβους αισθητήρων και μετά μεταφέρει τα δεδομένα στον σταθμό βάσης. Υπάρχει και η δυνατότητα οι επικεφαλής κόμβοι να επικοινωνούν μεταξύ τους πρώτα πριν επικοινωνήσουν με τον σταθμό βάσης. Η τοπολογία αυτή μπορεί να ταξινομηθεί είτε ομοιογενής είτε ως ετερογενής αλλά και τα συμπλέγματα που σχηματίζονται στατικά ή δυναμικά. Μπορεί να χρησιμοποιηθεί σε όλο το δίκτυο και να δημιουργήσει διάφορα επίπεδα της ιεραρχικής τοπολογίας.



Εικόνα 12. Cluster Based Τοπολογία

Πηγή:https://www.researchgate.net/publication/322668253_Denial_of_Service_DoS_Defence_for_Resource_Availability_in_Wireless_Sensor_Networks

- **Ιεραρχική Τοπολογία:** Η τοπολογία αυτή σχεδιάστηκε με γνώμονα στο μυαλό να κατανέμει τις εργασίες των κόμβων (ανίχνευση και επεξεργασία πληροφορίας) σε διαφορετικά επίπεδα του συστήματος. Αυτό σημαίνει ότι η τοπολογία είναι σχεδιασμένη σαν μία δενδροειδής δομή με διαφορετικούς τύπους συμπλεγμάτων. Υπάρχουν τέσσερα επίπεδα της ιεραρχικής τοπολογίας και αυτά είναι τα εξής: **επίπεδο αισθητήρων, επίπεδο κόμβων, επίπεδο ομάδας** και **επίπεδο βάσης**. Το επίπεδο βάσης είναι το χαμηλότερο επίπεδο και αποτελείται από μεμονωμένους αισθητήρες με αλγόριθμο ανίχνευσης που ανιχνεύει και ταξινομεί αντικείμενα. Αφού γίνει επεξεργασία των δεδομένων που έχουν συλλεχθεί ο αλγόριθμος ανίχνευσης αποστέλλει τα αποτελέσματα της ταξινόμησης στο επίπεδο κόμβου. Στην συνέχεια, θα γίνει συγχώνευση των δεδομένων που λαμβάνονται από κάθε κόμβο. Το επίπεδο ομάδας σχηματίζεται από το σύνολο κόμβων που είναι οργανωμένοι σε ομάδες, όπου εκλέγεται κάποιος κόμβος ηγέτης της ομάδας για να εκτελεί την ταξινόμηση σε επίπεδο ομάδας. Το συνολικό αποτέλεσμα από τα χαρακτηριστικά των ταξινομήσεων σε επίπεδο κόμβου είναι στην ουσία η τροφή για το επίπεδο ομάδας όπου οι ηγέτες των ομάδων μπορούν να επιτύχουν προηγμένες εργασίες. Η ταξινόμηση σε επίπεδο βάσης είναι το υψηλότερο επίπεδο που λαμβάνει αποτελέσματα από την ταξινόμηση σε επίπεδο ομάδας και τα μεταδίδει τα δεδομένα στον σταθμό βάσης μέσω τεχνικής πολλαπλών διαδρομών. Ο αλγόριθμος ταξινόμησης σε επίπεδο βάσης ταξινομεί τα συλλεχθέντα αποτελέσματα και μειώνει τους ψευδείς συναγερμούς μεταξύ των αποτελεσμάτων που αναφέρθηκαν.

1.8 Πρότυπα WSN

Τα πρότυπα για τα WSN ήταν αναγκαία να δημιουργηθούν διότι υπήρξε παγκόσμια ανάπτυξη και εφαρμογή των δικτύων αυτών με αποτέλεσμα να παραχθούν πολλά και διαφορετικά μοντέλα αισθητήρων που θα έπρεπε να μπορούν να επικοινωνούν μεταξύ τους χωρίς προβλήματα. Πριν την δημιουργία κάποιου παγκόσμιου προτύπου ήταν πολύ δύσκολή η σύνθεση ενός WSN χωρίς προβλήματα και ασυμβατότητες.

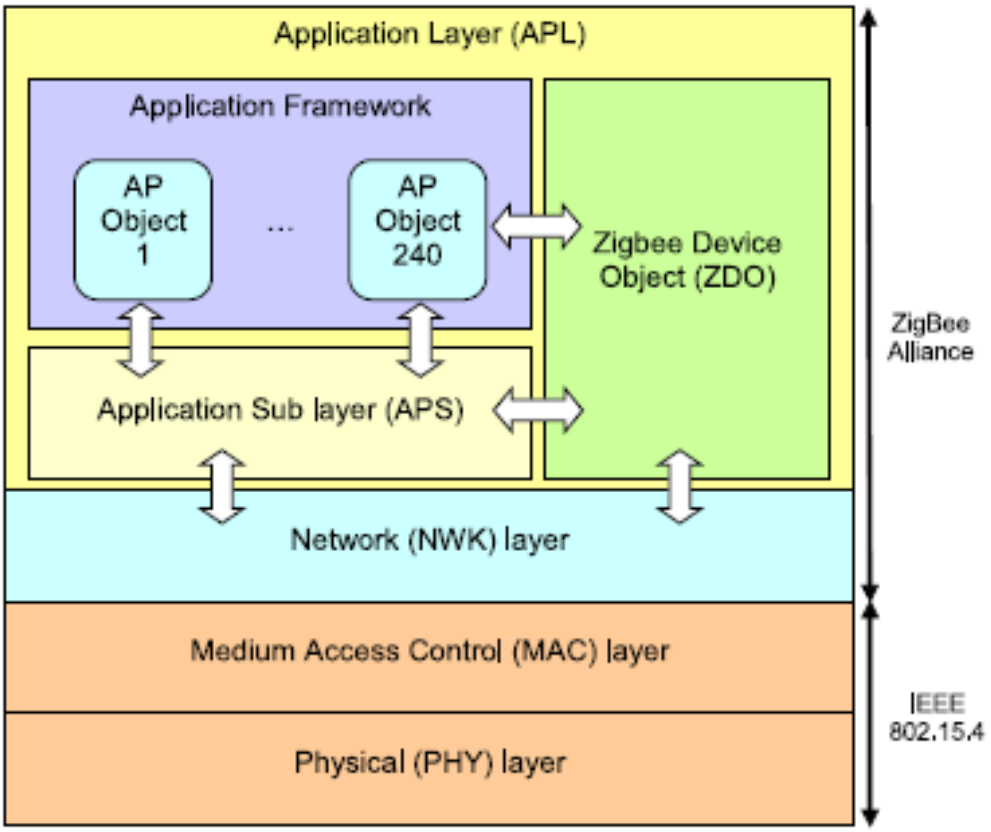
1.8.1 Πρότυπο IEEE 802.11 (Wi-Fi)

Το πρότυπο IEEE 802.11 δημοσιεύτηκε από το Institute of Electrical and Electronics Engineers (IEEE) το 1999 συνδυάζοντας τα επίπεδα ζεύξης δεδομένων και το φυσικό για να πετύχουν τα πρώτα ασύρματα τοπικά δίκτυα. Το πρότυπο αυτό ανήκει στην οικογένεια προτύπων IEEE 802 που μέχρι τότε υπήρχαν μόνο τα ενσύρματα τοπικά δίκτυα (Local area network LAN). Το πρότυπο IEEE 802.11 είναι κοινός γνωστό ως Wireless Fidelity ή Wi-Fi που δόθηκε σαν πιστοποίηση από την ομάδα Wi-Fi Alliance. Η ομάδα αυτή εξασφάλιζε την συμβατότητα μεταξύ των συσκευών που έπαιρναν την πιστοποίηση για το πρότυπο IEEE 802.11 έτσι ώστε να περισσότερος κόσμος να μπορεί να έχει δίκαιη πρόσβαση μέσο (medium), με υποστήριξη υψηλής απόδοσης και

κινητικότητας. Βέβαια μπορεί να ήταν κάτι επαναστατικό για τα δίκτυα αλλά τα ασύρματα δίκτυα έχουν προβλήματα όπως ότι οι συσκευές ξοδεύουν πολύ χρόνο στο να ακούγοντας το μέσο με αποτέλεσμα να συμβαίνουν πάρα πολλές συγκρούσεις. Για τα WSN αυτό είναι αρκετά μεγάλο πρόβλημα διότι υπάρχει μεγάλη σπατάλη πόρων και ενέργειας, ωστόσο το πρότυπο παρέχει μία λειτουργία εξοικονόμησης ενέργειας σε συσκευές που λειτουργούν με λειτουργία συντονισμού σημείου (point coordination function PCF). [2]

1.8.2 Πρότυπο IEEE 802.15.4 και ZigBee

Το πρότυπο IEEE 802.15.4 δημιουργήθηκε το 2003 για συσκευές χαμηλής ισχύος που θα λειτουργούν στις ζώνες συχνοτήτων 868 MHz με μέγεθος ένα κανάλι, 915 MHz με μέγεθος 10 κανάλια και 2450 MHz ή 2.45 GHz με μέγεθος 16 κανάλια. Οι τότε υποστηριζόμενοι ρυθμοί μεταφοράς δεδομένων ήταν 20, 40 και 250 kilobits per second (kbps) αντίστοιχα. Η ZigBee Alliance λίγο νωρίτερα εργαζόταν στην ανάπτυξη μίας τεχνολογίας επικοινωνίας χαμηλού κόστους με χαμηλούς ρυθμούς δεδομένων και χαμηλή κατανάλωση ενέργειας. Τελικά η IEEE και η ZigBee Alliance συνεργάστηκαν και έβγαλαν το πρότυπο μαζί, με την εμπορική ονομασία ZigBee χρησιμοποιώντας την τεχνολογία IEEE 802.15.4. [2] [10]



Εικόνα 13. ZigBee και IEEE 802.15.4

Πηγή:https://www.sciencedirect.com/science/article/abs/pii/S0140366406004749

Υποστηρίζονται δύο ειδών τοπολογίας: αστέρα και ομότιμου δικτύου (peer-to-peer) όπου στην τοπολογία αστέρα ολόκληρη η επικοινωνία γίνεται με μέσω του δικτύου προσωπικού χώρου (Personal area Network PAN). Από την άλλη, στην τοπολογία ομότιμου δικτύου, όλες οι συσκευές είναι ελεύθερες να επικοινωνούν απευθείας μεταξύ τους αλλά θα πρέπει και πάλι να επικοινωνούν με τον συντονιστή PAN για να συμμετάσχουν σε peer to peer επικοινωνία.

Η τοπολογία αστέρα έχει δύο διαφορετικούς τρόπους λειτουργίας: ο συγχρονισμένος ή αλλιώς ενεργοποιημένος ραδιοφάρος (beacon - enabled) και ο ασυγχρόνιστος τρόπος λειτουργίας. Ο τρόπος με τον οποίο λειτουργεί είναι ότι ο συντονιστής PAN εκπέμπει σε όλους περιοδικά μηνύματα beacon ώστε να γίνεται καλύτερη διαχείριση και συγχρονισμός των συσκευών. Ο συγχρονισμός είναι πολύ σημαντικός γιατί χωρίς αυτόν δεν μπορεί να γίνει ο πρόσβαση στο κανάλι με θυρίδες (slotted channel access) με σκοπό μία συσκευή να έχει την δυνατότητα να κάνει μία τυχαία επαναφορά (backoff) πριν το εντοπιστεί το κανάλι. Εάν δεν υπάρχει δραστηριότητα στο κανάλι τότε η συσκευή περιμένει την αμέσως επόμενη κενή θυρίδα για να προσπαθήσει να ξανά εντοπίσει το κανάλι μέχρι να μην υπάρχει δραστηριότητα για δύο συνεχόμενες θυρίδες. Αν ανιχνευτεί δραστηριότητα τότε η διαδικασία backoff επαναλαμβάνεται αλλιώς δεν είναι δυνατή η πρόσβαση στο κανάλι.

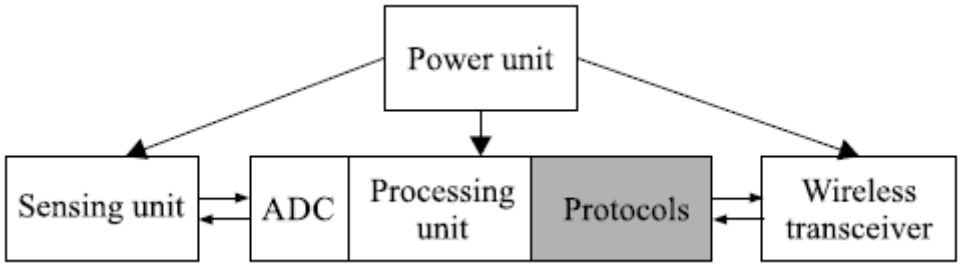
1.8.3 Bluetooth Low Energy (BLE)

Το Bluetooth Low Energy γνωστό και ως Bluetooth Smart αναπτύχθηκε από την ίδια ομάδα που δημιούργησε και το Bluetooth. Η εμβέλεια του BLE είναι μικρότερη και για αυτό καταναλώνει λιγότερη ενέργεια σε σχέση με άλλες τεχνικές και πρωτόκολλά. Αποτελείται από δύο μέρη, τον ελεγκτή (controller) και τον εξυπηρετητή (host) όπου στον ελεγκτή βρίσκεται το φυσικό επίπεδο και το επίπεδο σύνδεσης που είναι ο συνδυασμός του φυσικού με του επίπεδου ζεύξης δεδομένων. Ο ελεγκτής συνήθως βρίσκεται σε ένα σύστημα που ονομάζεται SOC (System On Chip) μαζί με μία κεραία.

Όλα τα υπόλοιπα επίπεδα βρίσκονται και υλοποιούνται στον host οπότε το BLE μπορεί να μεταδώσει πακέτα με ρυθμό μετάδοσης δεδομένων 1 Mbps (Megabits per second) αρκεί τα πακέτα να είναι μικρά σε μέγεθος. Για να είναι αποδοτικό το BLE λειτουργεί με βάση δύο τύπων συσκευών αφέντης (master) και σκλάβος (slave) και μία μεγάλη διαφορά που έχουν μεταξύ τους είναι ότι ο master μπορεί να είναι συνδεδεμένος με πολλές συσκευές slave ενώ ο slave μόνο σε μία. Για να είναι αρκετά ενεργειακά αποδοτικό το πρότυπο όταν υπάρχει μία σύνδεση μεταξύ ενός master και slave οι συσκευές slave μπαίνουν σε κατάσταση αναστολής λειτουργίας και ανά τακτά χρονικά διαστήματα ξυπνούν για να επικοινωνούν με τον master. Το BLE είναι 2,5 φορές πιο αποδοτικό από το πρότυπο ZigBee και μπορεί να υποστηρίξει και επικοινωνία με βάση την διεύθυνση IP (Internet Protocol).

1.9 Πρωτόκολλα WSN

Οι ανάγκες και οι απαιτήσεις της κάθε εφαρμογής ενός ασύρματου δικτύου αισθητήρων για να λειτουργήσει χρειάζεται την ανίχνευση του φυσικού περιβάλλοντος ώστε να μπορούν να σταλθούν τα δεδομένα σε έναν σταθμό βάσης. Η διαδικασία αυτή για να γίνει απαιτείται ισχύ και θα πρέπει να αντληθεί από κάποια μπαταρία είτε από κάποια φυσική πηγή. Ο κόμβος αισθητήρα αποτελείται από τέσσερεις μονάδες που είναι υπεύθυνες για την ενέργεια, την επεξεργασία αλλά και τις επικοινωνίες όπως φαίνεται στο σχήμα παρακάτω.



Εικόνα 14. Κόμβος Αισθητήρα

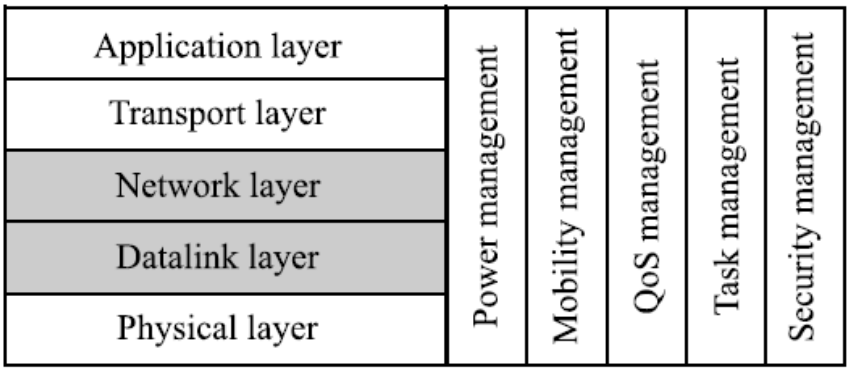
Πήγη:https://www.itl.waw.pl/czasopisma/JTIT/2018/1/77.pdf

Σε δίκτυα αισθητήρων η περισσότερη ενέργεια που καταναλώνεται είναι από την επεξεργασία των δεδομένων αλλά και την διαδικασία της επικοινωνίας. Κάποιους από τους προβληματισμούς και περιορισμούς που πρέπει να ξεπεραστούν είναι η ενέργεια, η κίνηση δεδομένων, η διάρκεια ζωής του δικτύου αλλά και η στοίβα πρωτοκόλλων επικοινωνίας να είναι πολύ προσεκτικά σχεδιασμένη. Η αποδοτικότητα και το πόσο καλά λειτουργεί ένα ασύρματο δίκτυο αισθητήρων εξαρτάται σε πολύ μεγάλο βαθμό από τον σχεδιασμό της στοίβας πρωτοκόλλων γιατί διαφέρουν αρκετά από τα συμβατικά δίκτυα επικοινωνίας υπολογιστών. Μερικές από τις διαφορές που έχουν είναι οι εξής:

- Οι φυσικές τοπολογίες σε ένα δίκτυο υπολογιστών είναι αρκετά καλοσχεδιασμένες ενώ σε ένα ασύρματο δίκτυο αισθητήρων οι κόμβοι είναι πυκνοί και τυχαίοι.
- Τα δίκτυα υπολογιστών μόλις σχεδιαστούν παραμένουν στατικά ενώ σε αντίθεση τα ασύρματα δίκτυα αισθητήρων είναι από φύση τους δυναμικά. Ανάλογα την τοπολογία υπάρχει περίπτωση η αποτυχία ενός κόμβου να αλλάξει ολόκληρη τοπολογία και για αυτό τον λόγο θα πρέπει να είναι αυτορρυθμιζόμενα.
- Τα δίκτυα υπολογιστών έχουν διευθύνσεις IP για την επικοινωνία με όλο τον κόσμο. Οι κόμβοι ασύρματων δικτύων αισθητήρων δεν έχουν παγκόσμια αναγνώριση επειδή αυτό δημιουργεί μεγάλη επιβάρυνση.
- Τα δίκτυα υπολογιστών διαθέτουν συνεχόμενη ροή ρεύματος, ενώ τα ασύρματα δίκτυα αισθητήρων έχουν περιορισμένους πόρους. Έτσι, η στοίβα πρωτοκόλλων

σε ένα δίκτυο αισθητήρων πρέπει να έχει σαν γνώμονα την κατανάλωση ενέργειας.

Η στοίβα πρωτοκόλλων χωρίζεται σε πέντε οριζόντια επίπεδα και πέντε κάθετα επίπεδα διαχείρισης όπως φαίνεται και στην εικόνα παρακάτω



Εικόνα 15. Στοίβα Πρωτοκόλλων

Πηγή:https://www.itl.waw.pl/czasopisma/JTIT/2018/1/77.pdf

1.9.1 Πρωτόκολλα στο Επίπεδο Ζεύξης Δεδομένων

Στο επίπεδο ζεύξης δεδομένων υπάρχουν δύο υποεπίπεδα: το υποεπίπεδο **Medium Access Control (MAC) ή Ελέγχου Προσπέλασης στο Μέσο** και το υποεπίπεδο **Logical Link Control (LLC) ή Ελέγχου Λογικής Σύνδεσης.** Το υποεπίπεδο ελέγχου λογικής σύνδεσης LLC χρησιμοποιείται για τη διαχείριση της σύνδεσης, τη ροή δεδομένων αλλά και τον έλεγχο σφαλμάτων. Το υποεπίπεδο ελέγχου προσπέλασης στο μέσο MAC είναι υπεύθυνο για τη συναρμολόγηση των δεδομένων σε πλαίσια, όπως και για την αποσυναρμολόγηση των πλαισίων, ώστε να μπορεί να γίνει ανάκτηση πληροφοριών. Σε ένα ασύρματο δίκτυο αισθητήρων οι κόμβοι μπορεί να χρειαστεί να μοιράζονται ένα ενιαίο κανάλι για την μεταφορά δεδομένων είτε προς τον σταθμό βάσης είτε προς έναν άλλο κόμβο. Όταν όμως γίνεται ταυτόχρονη μετάδοση δεδομένων σε ένα κανάλι, τότε δημιουργείται σύγκρουση (collision), η οποία έχει σαν αποτέλεσμα απώλεια δεδομένων αλλά και σπατάλη ενέργειας που είναι πολύ σημαντική σε αυτά τα δίκτυα.

Για την αποφυγή συγκρούσεων μπορούν οι κόμβοι να έρθουν σε συμφωνία μεταξύ τους, ποιος κόμβος θα χρησιμοποιεί το μέσο για ένα συγκεκριμένο διάστημα και ποιος θα περιμένει. Σε αυτήν την περίπτωση θα πρέπει να λάβουμε υπόψιν και την καθυστέρηση διάδοσης της πληροφορίας με αποτέλεσμα να είναι δύσκολο για έναν κόμβο να γνωρίζει σε τι στιγμιαία κατάσταση βρίσκονται οι άλλοι κόμβοι, με αποτέλεσμα ο πομποδέκτης να καταναλώνει μεγάλη ποσότητα ενέργειας όσο έχει πρόσβαση στο μέσο. Η δουλειά του πρωτοκόλλου MAC είναι να ελέγχει την δραστηριότητα του πομποδέκτη, ώστε να υπάρχει καλύτερη διατήρηση ενέργειας.

1.9.2 Πρωτόκολλο MAC

1.9.2.1 Κατανάλωση Ενέργειας στο Πρωτόκολλο MAC

Η κατανάλωση ενέργειας μπορεί να προέρχεται από πολλές πηγές και μερικές από αυτές είναι οι εξής:

- **Σύγκρουση:** Σύγκρουση μπορεί να δημιουργηθεί όταν δύο ή περισσότεροι κόμβοι προσπαθούν να στείλουν πληροφορίες σε ένα κανάλι ταυτόχρονα με αποτέλεσμα τα πακέτα να συγκρούονται. Ανάλογα με την υλοποίηση τα πακέτα απορρίπτονται και πρέπει να μεταδοθούν ξανά.
- **Υπερακρόαση:** Συμβαίνει όταν ένας κόμβος λαμβάνει ένα πακέτο που προοριζόταν για κάποιον άλλο κόμβο με αποτέλεσμα να γίνετε σπατάλη ενέργειας.
- **Επιβάρυνση:** Η αποστολή και λήψη πληροφοριών ελέγχου απαιτεί ενέργεια αλλά και επιπλέον επιβάρυνση.
- **Ακρόαση σε αδράνεια:** Η ακρόαση σε αδράνεια είναι η ακρόαση σε ένα κανάλι σε αδράνεια στο οποίο αναμένεται να υπάρχει κίνηση.
- **Υπερεκπομπή:** Αποστολή πληροφοριών σε έναν κόμβο που δεν είναι έτοιμος να λάβει πληροφορίες ως εκ τούτου, τα πακέτα απορρίπτονται και πρέπει να σταλθούν ξανά.

1.9.2.2 Απαιτήσεις Επιδόσεων MAC

Όταν σχεδιάζεται ένα πρωτόκολλο MAC θα πρέπει να λαμβάνονται υπόψιν και κάποιες απαιτήσεις:

- **Ρυθμαπόδοση (Throughput):** Είναι μία μέτρηση για την αποδοτικότητα του πρωτοκόλλου και μετριέται από τον ρυθμό μετάδοσης. Στην περίπτωση μιας ασύρματης ζεύξης, μπορεί να σχετίζεται με τη χωρητικότητα.
- **Επεκτασιμότητα:** Στην επεκτασιμότητα αναφερόμαστε στην προσαρμογή του πρωτοκόλλου όταν αυξάνεται το μεγέθους του δικτύου, της διαδρομής, της κίνησης, αλλά και της επιβάρυνσης του φορτίου. Ένας τρόπος αντιμετώπισης αυτού του προβλήματος είναι ο εντοπισμός των αλληλεπιδράσεων, ώστε οι κόμβοι να χρειάζονται λιγότερες πληροφορίες για το πώς λειτουργεί όλο το δίκτυο για να λειτουργήσουν.
- **Καθυστέρηση:** Η καθυστέρηση μπορεί να αναφέρεται ως η χρονική καθυστέρηση μεταξύ της μετάδοσης και της άφιξης του μηνύματος. Η καθυστέρηση είναι ένας σημαντικός περιορισμός για εφαρμογές που βασίζονται πολύ στην σωστή διαχείριση του χρόνου και πρέπει να ελαχιστοποιηθεί όσο το δυνατόν περισσότερο.

- **Αριθμός Βημάτων(Hops):** Είναι ο αριθμός των βημάτων σε μία διαδρομή που χρειάζονται τα πακέτα για να φθάσουν στον κόμβο που θα στείλει τα δεδομένα στον σταθμό βάσης . Η λειτουργία του πρωτοκόλλου MAC ποικίλλει όταν χρειάζεται να γίνει η επικοινωνία με μέθοδο ενός ή πολλών βημάτων. Στην περίπτωση πολλαπλών βημάτων πρέπει να συγκεντρωθούν όλα τα δεδομένα ώστε να σταλούν στον κόμβο αποστολής δεδομένων.

1.9.2.3 Κατηγορίες Πρωτοκόλλων MAC

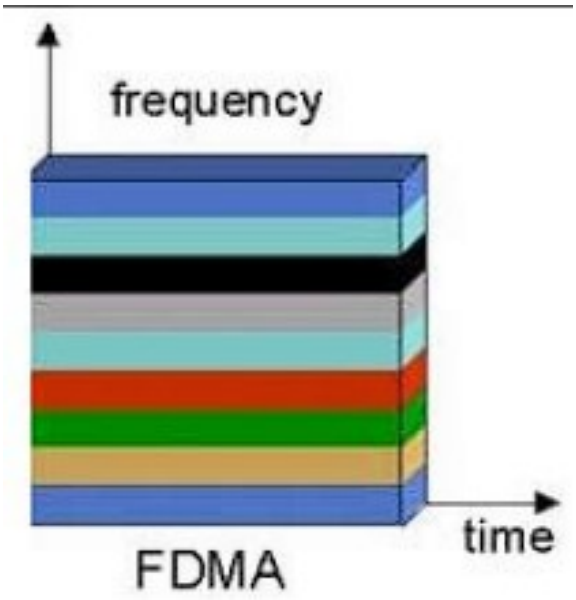
Υπάρχουν πολλές κατηγορίες πρωτοκόλλων MAC αλλά χωρίζονται σε δύο κύριες κατηγορίες: την κατηγορία MAC με βάση το χρονοδιάγραμμα, ή αλλιώς **schedule-based protocols** και την κατηγορία πρωτοκόλλου MAC με βάση την τυχαία πρόσβαση των κόμβων, ή αλλιώς **random access – based protocols** [11].

Στην πρώτη κατηγορία, η έννοια χρονοδιάγραμμα μπορεί να αναλυθεί ότι ο κάθε κόμβος έχει ένα σταθερό χρονικό όριο στο οποίο έχει πρόσβαση στο κανάλι για να μεταδώσει δεδομένα. Όταν δεν είναι η σειρά τους βάσει του χρονοδιαγράμματος να στείλουν δεδομένα μπαίνουν σε μία κατάσταση ύπνου για να μην γίνεται σπατάλη πόρων αλλά και για αποφυγή συγκρούσεων και υπερακρόασης. Με αυτό τον τρόπο ο κύκλος ζωής τον αισθητήρων αυξάνεται μιας και λειτουργούν ορισμένο χρονικό διάστημα.

Στη δεύτερη κατηγορία, με βάση την τυχαία πρόσβαση οι κόμβοι «ανταγωνίζονται» μεταξύ τους για το ποιος κόμβος θα έχει πρόσβαση στο κανάλι για επικοινωνία. Με αυτό τον τρόπο υπάρχουν όμως συγκρούσεις και θα πρέπει οι κόμβοι μετά από κάθε σύγκρουση να περιμένουν για ένα τυχαίο χρονικό διάστημα πριν τους δοθεί πάλι πρόσβαση στο μέσο για επικοινωνία. Υπάρχει μεγαλύτερη σπατάλη πόρων με αυτό τον τρόπο και η αποδοτικότητα του πρωτοκόλλου είναι αρκετά χαμηλή.

Κάποια από τα πρωτόκολλα που ανήκουν στην κατηγορία πρωτοκόλλων με χρονοδιάγραμμα είναι το **Time Division Multiple Access protocol (TDMA)**, ή αλλιώς **πρωτόκολλο πολλαπλής πρόσβασης διαίρεσης χρόνου** [12]. Σε αυτό το πρωτόκολλο το ίδιο το κανάλι που μεταδίδει δεδομένα προγραμματίζεται σε χρονικές περιόδους. Αυτό σημαίνει ότι κάθε κόμβος μεταδίδει ή λαμβάνει μόνο όταν είναι μέσα στην χρονική περίοδο που έχει ορίσει ο κόμβος και όλες τις υπόλοιπες χρονικές περιόδους που δεν είναι η σειρά του είναι σε κατάσταση ύπνου. Αυτό το πρωτόκολλο είναι κατάλληλο κυρίως για δίκτυα με μεγάλο φορτίο κίνησης και δεν είναι τόσο ενεργοβόρο.

Ένα διαφορετικό πρωτόκολλο αλλά με την ίδια λογική είναι το πρωτόκολλο **Frequency Division Multiple Access (FDMA) ή πρωτόκολλο πολλαπλής πρόσβασης με διαίρεση συχνότητας** [13]. Σε αυτό το πρωτόκολλο αντί γίνεται διαίρεση του χρόνου όπως στο TDMA γίνεται συχνότητας. Μία μεγάλη διαφορά είναι ότι επειδή το κανάλι μετάδοσης χωρίζεται σε συχνότητες και όλοι οι κόμβοι μπορούν να έχουν πρόσβαση στο κανάλι ταυτόχρονα.



Εικόνα 16. Πρωτόκολλο πολλαπλής πρόσβασης με διαίρεση συχνότητας (FDMA)

Πηγή:http://www.iject.org/vol4/spl2/aseem.pdf

Πρωτόκολλο με Πολλαπλή Πρόσβαση με Διαίρεση Κώδικα, ή αλλιώς **Code Division Multiple Access (CDMA)** [14] το οποίο είναι μία ειδική περίπτωση όπου οι χρήστης του καναλιού έχουν πρόσβαση για αποστολή δεδομένων ταυτόχρονα και συγχρονισμένα. Για να επιτευχθεί αυτό τα δεδομένα υπογράφονται με μία προκαθορισμένη υπογραφή που ονομάζεται ψευδοθόρυβος. Το πρωτόκολλο αποτελείται από τρία βασικά στοιχεία:

- ✓ Για την αποστολή πληροφοριών το σήμα καταλαμβάνει αρκετά μεγαλύτερο εύρος ζώνης για την αποστολή πληροφοριών σε σχέση με άλλους αλγόριθμους.
- ✓ Τα δεδομένα διαδίδονται με κώδικα ψευδοθορύβου που είναι όμως ανεξάρτητος από τα δεδομένα.
- ✓ Ο δέκτης πρέπει να είναι συγχρονισμένος με τον πομπό με την τεχνική του ψευδοθορύβου ώστε να μπορεί να αποκωδικοποιεί τα κωδικοποιημένα δεδομένα.

Η χρήση του ψευδοτυχαίου θορύβου χρησιμοποιείται για την προστασία των δεδομένων αλλά και την ασφάλεια αυτών. Ο κώδικας ψευδοθορύβου δεν είναι τυχαίος αλλά έχει ντετερμινιστική σειρά για τον δέκτη κατά την ανακατασκευή του κώδικα.

1.9.2.4 Πρωτόκολλο MAC με Βάση τον Ανταγωνισμό (Contention Based MAC Protocols)

Στο πρωτόκολλο αυτό οι κόμβοι ανταγωνίζονται με τους γειτονικούς κόμβους για το ποιος θα έχει πρόσβαση στο κανάλι για αποστολή δεδομένων. Η διαδικασία αυτή γίνεται όμως μόνο όταν ο κόμβος καταλάβει ότι υπάρχει δυνατότητα για αποστολή δεδομένων,

έτσι ξεκινάει τον ανταγωνισμό πριν αρχίσει η μεταφορά. Εάν ο φορέας ρυθμιστή ως αδρανής, τότε ξεκινάει ο κόμβος την μετάδοση δεδομένων αλλιώς ο κόμβος αναβάλει την μετάδοση για κάποιο τυχαίο χρονικό διάστημα. Η αναβολή της μετάδοσης καθορίζεται από έναν αλγόριθμο που ονομάζεται backoff, το πρωτόκολλο αυτό χρησιμοποιείται γιατί μειώνονται αρκετά οι πόροι που χρειάζονται για την επεξεργασία της πληροφορίας και είναι αρκετά ευέλικτα και δυναμικά σε μεγάλης κλίμακας δικτύων. Δεν χρειάζονται πληροφορίες όπως η ομαδοποίηση(clustering) και το είδος τοπολογίας για να γίνουν αυτές οι ενέργειες οπότε ο κάθε κόμβος σε ολόκληρο το δίκτυο αποφασίζει ο ίδιος για τον ανταγωνισμό χωρίς να κάνει έλεγχο πακέτων ανταλλαγής. Με αυτό τον τρόπο η μετάδοση χειρίζεται εξολοκλήρου από τον αποστολέα καθώς και τα προβλήματα όπως συγκρούσεις, ακρόαση σε αδράνεια αλλά και υπερακρόαση να έχουν ως αποτέλεσμα χαμηλότερο απόδοση.

1.9.2.5 Πρωτόκολλα MAC Βασισμένα στη Δημοσκόπηση Καναλιού (Channel Polling-Based MAC Protocols)

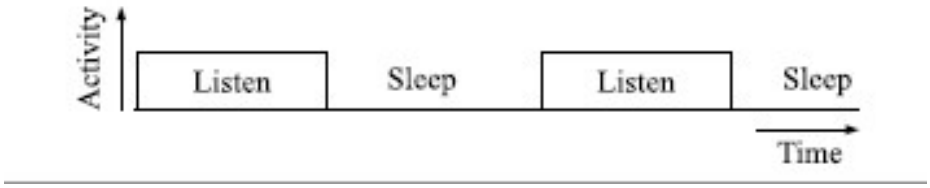
Το σχήμα δημοσκόπησης καναλιού είναι γνωστό ως δειγματοληψία προοιμίου και ακρόαση χαμηλής ισχύος (Low Power Listening LPL) [15]. Η αποστολή προθεμάτων πακέτων δεδομένων με επιπλέον bytes από τον κόμβο ονομάζεται προοίμιο. Στο πρωτόκολλο αυτό ο κόμβος με τον ρόλο αποστολέα στέλνει το προοίμιο στο κανάλι, ώστε να διασφαλίσει ότι ο κόμβος που λαμβάνει την πληροφορία ανιχνεύει την ράδιο δραστηριότητα, ώστε να τον «ξυπνήσει» πριν αρχίσει να λαμβάνει το πραγματικό ωφέλιμο φορτίο. Όταν ο κόμβος «ξυπνήσει» και ανιχνεύσει ράδιο δραστηριότητα από τον παραλήπτη, τότε θα ενεργοποιηθεί και θα αρχίσει να λαμβάνει την σωστή πληροφορία, διαφορετικά ο κόμβος που δέχεται τα δεδομένα θα επιστρέψει σε κατάσταση ηρεμίας μέχρι το επόμενο διάστημα δημοσκόπησης. Ο έλεγχος αυτός θα πρέπει να εκτελείται καθ’ όλη την διάρκεια που ο κόμβος περιμένει για την αποστολή του προοιμίου. Αυτό έχει σαν αποτέλεσμα ότι τα κοινά χρονοδιαγράμματα ενεργού/ύπνου δεν εκτελούνται σε πρωτόκολλα βασισμένα στη δημοσκόπηση καναλιού, τότε ο συγχρονισμός, ο προγραμματισμός ή η ομαδοποίηση μεταξύ των κόμβων δεν απαιτείται.

1.9.2.6 Υβριδικό Πρωτόκολλο MAC (Hybrid MAC Protocol)

Στο υβριδικό πρωτόκολλο MAC [16] υπάρχει ένας συνδυασμός πρωτοκόλλων αλλά και προσεγγίσεων που βασίζονται στον ανταγωνισμό και το χρονοδιάγραμμα (Schedule-based & TDMA). Το TDMA πρωτόκολλο ότι εξεταστεί ότι είναι η καλύτερη επιλογή όταν υπάρχει υψηλή κίνηση αποφεύγοντας συγκρούσεις αλλά χρειάζεται να είναι τα πάντα συγχρονισμένα οπότε δεν είναι εύκολο να προσαρμοστεί σε διάφορες τοπολογίες δικτύου και είναι επίσης δύσκολο να διαπιστωθεί η παρεμβολή μεταξύ των γειτονικών κόμβων (ακανόνιστη παρεμβολή).

1.9.2.7 Sensor-MAC (S-MAC)

Οι κόμβοι συγχρονίζονται τοπικά ώστε να λειτουργούν σύμφωνα με ένα πρόγραμμα ύπνου/ακρόασης όπως φαίνεται και στην φωτογραφία παρακάτω. Κάθε κόμβος ανήκει σε μία εικονική συστάδα και κάθε συστάδα έχει κοινό πρόγραμμα ύπνου/ακρόασης όπως επίσης και κάθε κόμβος πρέπει να ανακαλύπτει τους γειτονικούς κόμβος αρκετά συχνά και να υπάρχει σύνδεση μεταξύ τους. Έπειτα σε κάθε σύνδεση που έχει με κάθε γειτονικό κόμβο αναθέτει μία ξεχωριστή συχνότητα, χρόνο ή κώδικα και τα μεγάλα πακέτα διαιρούνται σε μικρότερα για να μπορέσει να γίνει η αποστολή τους. Με αυτό τον τρόπο το δίκτυο οργανώνεται μόνο του όταν πρέπει να αλλάξει η τοπολογία λόγω του ότι κάποιος κόμβος «πέθανε» ή μετακινήθηκε. Επιπλέον, η κατανάλωση ενέργειας είναι αρκετά χαμηλή, διότι λειτουργεί με χαμηλότερο κύκλο λειτουργίας, με αποτέλεσμα η ισχύς που χρησιμοποιείται για την υπερακρόαση και την αδρανή ακρόαση να είναι λιγότερη. Λόγω του προγράμματος ύπνου/ακρόασης η καθυστέρηση είναι αυξημένη, διότι οι κόμβοι πρέπει να εναλλάσσονται των καταστάσεων το οποίο μπορεί να αποφευχθεί εντελώς αν ένας κόμβος ξυπνήσει αφού αντιληφθεί την αφύπνιση του γείτονά του. Η αποδοτικότητα μπορεί να πέσει σε περίπτωση που η κίνηση του δικτύου τύχη να πέσει σε περίοδο που ο κόμβος κοιμάται.



Εικόνα 17. S-MAC

Πηγή:https://jtit.pl/jtit/article/view/599

1.9.2.8 Timeout MAC (T-MAC)

Το πρωτόκολλο S-MAC έχει σταθερές περιόδους ύπνου/ακρόασης αλλά πολλές φορές οι ανάγκες των εφαρμογών με μεταβλητό φορτίο χρειάζονται δυναμικές περιόδους ύπνου/ακρόασης. Εδώ έρχεται το πρωτόκολλο T-MAC μία βελτιστοποιημένη έκδοση του S-MAC όπου η περίοδος ακρόασης λήγει όταν για ένα συγκεκριμένο χρονικό διάστημα δεν έχει λάβει χώρα κανένα συμβάν όπως είναι η λήψη δεδομένων και το μέγεθος αυτού του χρονικού διαστήματος εξαρτάται από το πόσο πολύ είναι το τρέχον φορτίο. Η μετάδοση δεδομένων γίνεται με ειδικά πακέτα όπως το αίτηση για αποστολή Request-To-Sent (RTS), έτοιμο για αποστολή Clear-To-Send (CTS) και επιβεβαίωση acknowledgement (ACK). Οι κόμβοι που βρίσκονται κοντά στον κόμβο αποστολέα συνήθως έχουν περισσότερα δεδομένα να στείλουν οπότε και οι περίοδοι ακρόασης είναι μεγαλύτερες. Με την χρήση όμως των ειδικών πακέτων RTS,CTS και ACK οι συγκρούσεις μειώνονται αρκετά και η αξιοπιστία του δικτύου αυξάνεται ραγδαία.

Αν οι περίοδοι ακρόασης είναι σταθερές τότε οι κόμβοι που δεν είναι τόσο κοντά στον κόμβο αποστολέα θα έχουν λιγότερα δεδομένα να στείλουν, οπότε θα σπαταλούν ενέργεια λειτουργώντας με αδρανή ακρόαση. Υπάρχει τρόπος να λυθεί αυτό το πρόβλημα αποστέλλοντας δεδομένα σε μεταβλητής ριπές. Κάποια αρνητικά είναι ότι δεν μπορεί να υποστηρίξει εφαρμογές που βασίζονται σε πολύ μεγάλο ρυθμό δεδομένων το δευτερόλεπτο καθώς πρέπει να γίνουν συμβιβασμοί στην απόδοση για να διατηρηθεί η κατανάλωση ενέργειας στο κατώτατο επίπεδο.

1.9.2.9 Berkeley MAC (B-MAC)

Το B-MAC χρησιμοποιεί την τεχνική δειγματοληψία προοιμίου και κάθε φορά που ο κόμβος «ξυπνάει» θα πρέπει να ελέγχει το δίκτυο για οποιαδήποτε δραστηριότητα πριν ξεκινήσει να αποστέλλει. Όταν ο κόμβος τελειώνει με την αποστολή δεδομένων και περάσει ένα χρονικό διάστημα τότε επιστρέφει στην κατάσταση αναστολή λειτουργίας για την λιγότερη δυνατή κατανάλωση πόρων. Επίσης, το πρωτόκολλο χρησιμοποιεί τεχνική ανάθεση καναλιών και λαμβάνει τοπικές αποφάσεις πολιτικής ώστε να βελτιστοποιήσει την απόδοση του δικτύου. Λόγω της τεχνικής που χρησιμοποιεί με την δειγματοληψία προοιμίου, ο κύκλος λειτουργίας μειώνεται, έτσι έχει σαν αποτέλεσμα την αύξηση της αποδοτικότητας και της ρυθμαπόδοσης. Στη μικρότερη κατανάλωση ισχύος παίζει μεγάλο ρόλο ότι το πρωτόκολλο χρησιμοποιεί ακρόαση χαμηλής ισχύος και υποστηρίζει αναδιαμόρφωση για την βελτίωση της καθυστέρησης. Μερικά από τα μειονεκτήματα είναι ότι δεν έχει την δυνατότητα ώστε να μπορεί να διαχειριστεί περιβάλλοντα που απαιτούν πολλαπλά πακέτα, αλλά υποφέρει επίσης, και από το πρόβλημα του κρυμμένου τερματικού μεγαλώνοντας έτσι την επιβάρυνση του πρωτοκόλλου. Υπάρχει όμως χώρος για βελτίωση στο πρωτόκολλο καθώς μπορεί να χρησιμοποιηθεί προσαρμοστική δειγματοληψία προοιμίου λύνοντας πολλά από τα προβλήματα που ειπώθηκαν προηγουμένως.

1.9.2.10 Predictive Wake-up MAC (PW-MAC)

Στο PW-MAC [11] το πότε «ξυπνάνε» οι κόμβοι μπορεί είναι τυχαίο και για να ενημερώσει του συγκεκριμένους πομπούς που χρειάζεται κάθε φορά που ξυπνάει στέλνει ένα σήμα ότι ξύπνησε. Για λόγους εξοικονόμησης ενέργειας ο αποστολέας μπορεί να προβλέψει το πότε θα ξυπνήσει ο παραλήπτης, ώστε να ξυπνήσει ταυτόχρονα, επίσης για την αντιμετώπιση των χρονικών προκλήσεων το πρωτόκολλο διαθέτει έναν μηχανισμό που τον χρησιμοποιεί όταν χρειάζεται για διόρθωση σφαλμάτων βάσει πρόβλεψης. Λόγω της λειτουργίας τυχαίας αφύπνισης των κόμβων, το πρωτόκολλο λειτουργεί με μειωμένο κύκλο λειτουργίας και έτσι η απόδοση του είναι αρκετά βελτιωμένη σε σχέση με το S-MAC και το B-MAC μιας και αποφεύγονται και οι συγκρούσεις. Η καθυστέρηση είναι επίσης σαφώς μικρότερη από άλλα πρωτόκολλα MAC, διότι ένας κόμβος χρειάζεται μόλις 10 bytes μνήμη για να αποθηκεύσει την προβλεπόμενη κατάσταση των άλλον κόμβων. Η επιβάρυνση είναι αυξημένη αλλά σε σχέση με άλλα πρωτόκολλα είναι μικρότερη λόγο

του σήματος αφύπνισης των κόμβων όπως επίσης και το υλικό μπορεί να προκαλέσει κάποια σφάλματα στην πρόβλεψη της αφύπνισης του κόμβου δέκτη.

1.9.2.11 Optimized MAC Πρωτόκολλο

Στο βελτιστοποιημένο πρωτόκολλο MAC ο κύκλος λειτουργίας των αισθητήρων προσαρμόζεται και αλλάζει ανάλογα με το φορτίο του δικτύου. Όταν υπάρχει αυξημένο φορτίο, ο κύκλος λειτουργίας αυξάνεται και το αντίθετο γίνεται όταν το φορτίο είναι συγκριτικά μικρότερο. Το φορτίο του δικτύου προσδιορίζεται με βάση τον αριθμό των μηνυμάτων που υπάρχουν στην ουρά αναμονής ενός αισθητήρα και η επιβάρυνση των πακέτων ελέγχου μειώνεται όταν ελαττώνεται ο αριθμός και το μέγεθος των πακέτων ελέγχου σε σύγκριση με το πρωτόκολλο S-MAC. Αυτό το πρωτόκολλο είναι ιδανικό για εφαρμογές που απαιτείται μεγάλη ανάγκη για ενεργειακή απόδοση αλλά και πολύ μικρή καθυστέρηση.

1.9.2.12 Traffic Adaptive Medium Access Protocol (TRAMA)

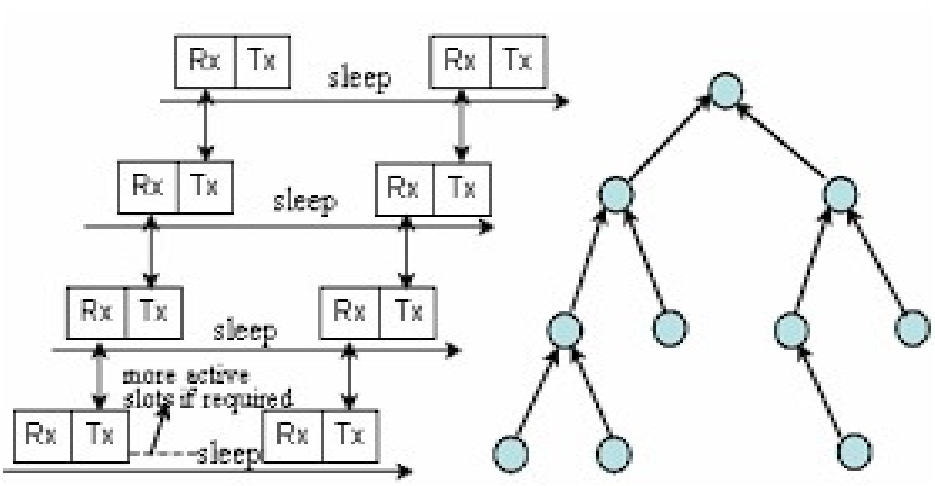
Το TRAMA πρωτόκολλο είναι βασισμένο στο πρωτόκολλο TDMA, το οποίο είναι σχεδιασμένο για να λειτουργεί με την λιγότερη δυνατή ενέργεια αλλά και να αποφεύγει τις συγκρούσεις στα ασύρματα δίκτυα αισθητήρων. Το ίδιο μπορεί να καταφέρει και το TRAMA χρησιμοποιώντας μία τεχνική μετάβασης των κόμβων σε κατάσταση αδράνειας χαμηλής ισχύος όταν δεν χρειάζεται να στείλουν και να λάβουν δεδομένα. Το πρωτόκολλο χωρίζεται σε τρία μέρη:

1. Το Γειτονικό πρωτόκολλο που η δουλειά του είναι να συλλέγει πληροφορίες σχετικά με τους γειτονικούς κόμβους του κάθε κόμβου.
2. Το πρωτόκολλο ανταλλαγής χρονοδιαγράμματος που γίνεται η ανταλλαγή πληροφοριών και χρονοδιαγραμμάτων τον γειτονικών κόμβων σε απόσταση δύο βημάτων.
3. Ο αλγόριθμος προσαρμοστικής εκλογής που έχοντας όλες τις πληροφορίες για όλους τους κόμβους αλλά και τα χρονοδιαγράμματα τους αποφασίζει ποιος κόμβος θα κάνει την εκπομπή και ποιος θα λαμβάνει την πληροφορία για την συγκεκριμένη χρονική στιγμή. Οι κόμβοι που δεν παίρνουν μέρος σε αυτήν την ανταλλαγή μεταβαίνουν σε κατάσταση χαμηλής ισχύος.

Το πρωτόκολλο TRAMA με αυτό τον τρόπο είναι σαφώς καλύτερο και ενεργειακά αποδοτικότερο αλλά έχει, επίσης, και υψηλότερη απόδοση σε σχέση με το πρωτόκολλο S-MAC. Βέβαια, κάθε πρωτόκολλο έχει και τα αρνητικά του, όπως ότι η καθυστέρηση του TRAMA είναι συγκριτικά μεγαλύτερη σε σχέση με άλλα MAC πρωτόκολλα που βασίζονται στην τεχνική του ανταγωνισμού.

1.9.2.13 Data Gathering MAC (D-MAC)

Το DMAC (Data-Gathering Medium Access Control) είναι ένα πρωτόκολλο βασισμένο και αυτό στο χρονοδιάγραμμα το οποίο όμως έχει σχεδιαστεί και βελτιστοποιηθεί ειδικά για δενδροειδή συλλογή δεδομένων (επικοινωνία με συγκλίνουσες ρίψεις) σε ένα ασύρματο δίκτυο αισθητήρων. Το κύριο μέλημα αυτού του πρωτοκόλλου είναι να υπάρχει η λιγότερο δυνατή καθυστέρηση, αλλά να είναι και ισορροπημένο στην ενεργειακή απόδοσή του. Ο χρόνος στο πρωτόκολλο αυτό διαιρείται σε μικρές χρονοθυρίδες (time slots) και έρχεται και βοηθάει ένα άλλο πρωτόκολλο το Carrier Sensing Multiple Access (CSMA), το οποίο ζητά επιβεβαίωση μέσα στην κάθε χρονοθυρίδα για να γίνει αποστολή η λήψη ενός πακέτου. Ο κόμβος αισθητήρα εκτελεί περιοδικά τη βασική ακολουθία '1'. εκπομπής, '1' λήψης και 'n' θυρίδες ύπνου, το οποίο σημαίνει ότι σε αυτήν την προσέγγιση ένα πακέτο από έναν κόμβο-πηγή σε ένα βάθος ‘k’ στο δέντρο θα φτάσει με καθυστέρηση ‘k’ χρονοθυρίδων στον κόμβο-αποστολέα. Η καθυστέρηση είναι μικρή της τάξεως των δεκάδων χιλιοστών του δευτερολέπτου, όπου στην φωτογραφία παρακάτω απεικονίζεται μία συλλογή δεδομένων (converge cast) σε δέντρο με κλιμακωτές χρονοθυρίδες DMAC.



Εικόνα 18. D-MAC

Πηγή:https://www.specialcabledeals.com/assets/pdf/11_339.pdf

Στο πρωτόκολλο D-MAC υποστηρίζεται ένας μηχανισμός υπερχείλισης με σκοπό να αντιμετωπιστεί το πρόβλημα, όταν ο κάθε κόμβος πηγή στο δίκτυο έχει χαμηλό ρυθμό κίνησης αλλά ο συνολικός ρυθμός στον ενδιάμεσο κόμβο είναι μεγαλύτερος από τον βασικό ρυθμό κύκλο λειτουργίας. Στον μηχανισμό αυτόν ο κόμβος αισθητήρα αφού θα αποστείλει το πακέτο θα παραμείνει για ακόμα μία χρονοθυρίδα ενεργός, με αποτέλεσμα στο δέντρο ένα δύο παιδιά αγωνιζόντουσαν για να λάβουν την θυρίδα του γονέα το χαμένο από την μάχη παιδί θα πάρει μία δεύτερη ευκαιρία ώστε να στείλει το πακέτο. Η δενδροειδής κατάσταση του πρωτοκόλλου χρήζει ανάγκης για έναν ξεχωριστό έλεγχο πακέτων με την ονομασία MTS(More To Send) μεταξύ κόμβων σε διαφορετικούς

κλάδους του δέντρου. Έτσι, το MTS πακέτο αναγκάζει όλους τους κόμβους στο μονοπάτι πολλαπλών βημάτων να παραμείνουν ενεργεί σε περίπτωση που υπάρξει κάποια αποτυχία κάποιου κόμβου λόγω μεγάλης παρεμβολής. Σε θέματα ενεργειακής απόδοσης, καθυστέρησης αλλά και σε διάφορες τοπολογίες το πρωτόκολλο D-MAC είναι καλύτερο από το S-MAC.

1.9.2.14 WiseMAC Πρωτόκολλο

Στο πρωτόκολλο WiseMAC [17] όλοι οι κόμβοι χρησιμοποιούν δύο κανάλια επικοινωνίας ένα για το πρωτόκολλο TDMA) και ένα για το πρωτόκολλο CSMA που χρησιμοποιεί δειγματοληψία προοιμίου. Το TDMA σε αυτήν την περίπτωση χρησιμοποιείται για την πρόσβαση στο κανάλι των δεδομένων ενώ το CSMA για την πρόσβαση στο κανάλι ελέγχου. Το WiseMAC για να ελαττώσει την κατανάλωση ισχύος χρησιμοποιεί non-persistent CSMA με την τεχνική της δειγματοληψίας προοιμίου για να καταφέρει το επιθυμητό αποτέλεσμα όταν οι κόμβοι βρίσκονται σε κατάσταση αδρανής ακρόασης. Οι άμεσοι γείτονες παίζουν σημαντικό ρόλο στο πρωτόκολλο, γιατί με βάση τις πληροφορίες που αντλεί από το πρόγραμμα δειγματοληψίας τους χρησιμοποιεί το προοίμιο ελάχιστου μεγέθους. Επίσης, τα χρονοδιαγράμματα ύπνου των γειτονικών κόμβων ενημερώνονται κάθε φορά που γίνεται μεταφορά δεδομένων από το μήνυμα επιβεβαίωσης (ACK) και το πρωτόκολλο προσαρμόζεται στα φορτία κίνησης του δικτύου παρέχοντας χαμηλή κατανάλωση ενέργειας όταν η κίνηση είναι χαμηλή και υψηλή ενεργειακή απόδοση όταν η κίνηση είναι σε υψηλά επίπεδα.

1.9.3 Quality of Service στο Επίπεδο MAC

Τα ασύρματα δίκτυα αισθητήρων ξεκίνησαν σαν απλές εφαρμογές για παρακολούθηση σε εφαρμογές, όπως η γεωργία και η περιβαλλοντική παρακολούθηση που βασίζονταν στην συλλογή δεδομένων με χαμηλό ρυθμό. Οι ανάγκες και η τεχνολογία με την πάροδο του χρόνου όμως αναπτύχθηκαν και άλλαξαν οπότε άρχισε να υπάρχει ανάγκη για τον έλεγχο της ποιότητας των υπηρεσιών (Quality of Service QoS). Το QoS μπορεί να ταξινομηθεί σε δύο κατηγορίες, ως ειδικές για την εφαρμογή και ως ειδικές για το δίκτυο.

Ειδικές για εφαρμογή: Επικεντρώνεται στην ποιότητα της ίδιας της εφαρμογής και εξασφαλίζει την εκπλήρωση των απαιτήσεων που επιβάλλονται από την ίδια την εφαρμογή όπως διάρκεια ζωής, ανάπτυξη εφαρμογής, την ποιότητα και τον αριθμό των αισθητήρων αλλά και την ποιότητα μίας κάμερας που μπορεί να υπάρχει στο δίκτυο.

Ειδικές για το δίκτυο: Στην περίπτωση του δικτύου παρέχεται ποιότητα υπηρεσιών όταν γίνεται η παράδοση των δεδομένων από το εκάστοτε δίκτυο επικοινωνίας, έτσι οι πόροι του δικτύου χρησιμοποιούνται με πιο αποτελεσματικό τρόπο σε κάθε επίπεδο της στοίβας πρωτοκόλλων επικοινωνίας. Σκοπός είναι να εκπληρωθούν οι απαιτήσεις που

επιβάλλονται από τα μεταφερόμενα δεδομένα όπως η καθυστέρηση, η απώλεια πακέτων αλλά και η αξιοπιστία των δεδομένων.

1.9.3.1 Προκλήσεις QoS

Όπως και τα παραδοσιακά ασύρματα δίκτυα έτσι και τα ασύρματα δίκτυα αισθητήρων όταν αναπτύχθηκαν αρκετά, ήταν εμφανές ότι υπήρχαν κάποιες προκλήσεις στην ποιότητα των υπηρεσιών που έπρεπε να αντιμετωπίσουν. Ωστόσο τα δίκτυα αισθητήρων έχουν παραπάνω προβλήματα όπως, περιορισμένοι πόροι και ότι οι αισθητήρες βρίσκονται σε εξωτερικό περιβάλλον που οι περιβαλλοντικές συνθήκες είναι αρκετά δύσκολες. Οι προκλήσεις QoS για τα ασύρματα δίκτυα αισθητήρων είναι τα εξής:

Περιορισμοί πόρων: Τα ασύρματα δίκτυα αισθητήρων έχουν περιορισμένους πόρους, όπως η μνήμη, το εύρος ζώνης, η ενέργεια αλλά και η επεξεργασία δεδομένων. Το μεγαλύτερο πρόβλημα υπάρχει με τον περιορισμό της ενέργειας, επειδή σε πολλά σενάρια είναι δύσκολη έως αδύνατη η αντικατάσταση ή η επαναφόρτιση των μπαταριών στους κόμβους αισθητήρων. Αν και υπάρχουν ηλιακά πάνελ που θα μπορούσαν να βοηθήσουν σε αυτήν την πρόκληση, δυστυχώς τα πάνελ είναι αρκετά μεγάλα για τους μικροσκοπικούς αισθητήρες. Καθώς υπάρχει το πρόβλημα της ενέργειας, θα πρέπει το QoS να σχεδιαστεί καταλλήλως, ώστε να είναι ελαφρύ και αρκετά απλό για να μην βαραίνει παραπάνω το δίκτυο.

Ανάπτυξη κόμβων: Η ανάπτυξη των κόμβων μπορεί να είναι είτε τυχαία είτε ντετερμινιστική. Στην περίπτωση της ντετερμινιστικής ανάπτυξης οι κόμβοι τοποθετούνται σε συγκεκριμένο σημείο από τον χρήστη και η δρομολόγηση γίνεται με συγκεκριμένο τρόπο, αφού έχει αναλυθεί η τοπολογία του δικτύου μέσω προκαθορισμένων διαδρομών. Στην περίπτωση της τυχαίας ανάπτυξης οι κόμβοι αισθητήρων αναπτύσσονται τυχαία και οργανώνονται με ad hoc τρόπο. Στην τυχαία ανάπτυξη υπάρχουν προβλήματα, όπως η ανακάλυψη γειτονικών κόμβων, η ανακάλυψη μονοπατιών η ομαδοποίηση αλλά και οι γεωγραφικές πληροφορίες των κόμβων, που είναι προκλήσεις που θα πρέπει να επιλυθούν.

Αλλαγές στην Τοπολογία: Όταν το περιβάλλον στο οποίο βρίσκονται οι κόμβοι αισθητήρων είναι αρκετά απειλητικό πολλές φορές θα χρειαστεί να γίνουν αλλαγές στην τοπολογία, επειδή μπορεί να υπάρχουν αποτυχίες στη διασύνδεση των κόμβων, προβλήματα με την κινητικότητα των κόμβων, δυσλειτουργία ενός ή πολλών κόμβων, εξάντληση ενέργειας και φυσικά φαινόμενα, όπως πλημμύρα αλλά και πυρκαγιά. Αρκετά πρωτόκολλα MAC χρησιμοποιούν διάφορες τεχνικές για να αποφεύγουν να χρειάζεται να κάνουν αλλαγές στην τοπολογία όπως, οι αισθητήρες να μην είναι συνέχεια ενεργοποιημένοι αλλά να είναι σε κατάσταση “ύπνου” και να ενεργοποιούνται όταν χρειάζεται. Είναι ,λοιπόν, φυσικό η δυναμική φύση των τοπολογιών ενός ασύρματου δικτύου αισθητήρων να προσθέτει ακόμα μία πρόκληση για το QoS.

Data redundancy: Σε ένα μεγάλο δίκτυο αισθητήρων χρησιμοποιούνται πάρα πολλοί αισθητήρες για να καλύψουν το μεγάλο αυτό μέγεθος που σημαίνει ότι ο αριθμός των δεδομένων που μεταφέρονται είναι αρκετά μεγάλος. Για να υπάρχει αξιοπιστία στα δεδομένα αποθηκεύονται σε δύο διαφορετικά σημεία, ώστε να υπάρχει data redundancy. Αυτό όμως προκαλεί στο δίκτυο «περιττή» μεταφορά δεδομένων με αποτέλεσμα να οδηγεί σε συμφόρηση του δικτύου. Για να αποφευχθεί αυτό, μπορεί να χρησιμοποιηθεί ένας μηχανισμός που θα «μαζεύει» όλα τα δεδομένα με έναν κόμβο αποστολέα για να μειωθεί το πρόβλημα αλλά μπορεί να προσθέσει αρκετή καθυστέρηση και πολυπλοκότητα στο δίκτυο.

Πολλαπλοί τύποι κυκλοφορίας: Σε ένα WSN χρησιμοποιούμαι πολλαπλούς αισθητήρες που ανάλογα με το είδος του αισθητήρα και το φαινόμενο που ανιχνεύουν παράγουν διαφορετικό τύπου κίνησης δεδομένων. Για παράδειγμα έχει διαφορά αν μεταδίδουμε δεδομένα πολυμέσων, την θέση ενός εντοπισμένου στόχου ή τις περιοδικές πληροφορίες θερμοκρασίας που μπορούμε να αντλούμε από μία περιοχή υπάρχει περίπτωση να μεταφέρονται ταυτόχρονα για τις ανάγκες μίας εφαρμογής. Όταν οι ανάγκες μίας εφαρμογής απαιτεί να υπάρχουν πολλαπλών ειδών κυκλοφορίας τότε προσθέτει προκλήσεις για το QoS μιας και ο κάθε τύπος κυκλοφορίας χρειάζεται διαφορετική αντιμετώπιση.

Κίνηση δεδομένων σε πραγματικό χρόνο: Η μεταφορά δεδομένων σε πραγματικό χρόνο παίζει πολύ μεγάλο ρόλο σε ορισμένες εφαρμογές όπως, η παρακολούθηση φυσικών καταστροφών και η παρακολούθηση ασφαλείας. Τα δεδομένα που συλλέγονται είναι αρκετά σημαντικά και θα πρέπει να συγκεντρωθούν αλλά και να αποσταλούν πριν λήξει η προθεσμία τους, γιατί τα δεδομένα αυτά ισχύουν μόνο για ένα περιορισμένο χρονικό διάστημα. Το QoS παίζει πολύ μεγάλο ρόλο σε μεταφορά δεδομένων σε πραγματικό χρόνο και θα πρέπει να εκτελέσει τους κατάλληλους μηχανισμούς για να ανταπεξέλθει.

Ανισόρροπη κυκλοφορία: Στα ασύρματα δίκτυα αισθητήρων που μελετάμε τις περισσότερες φορές υπάρχει τουλάχιστον μία κεντρική οντότητα που λαμβάνει την σφαιρική εικόνα του περιβάλλοντος και ονομάζεται sink node. Επίσης, μπορεί να υπάρχει και ενδιάμεσα στάδια αυτής της οντότητας με την ονομασία κεφαλές συστάδων. Πολλές φορές όταν γίνεται ανταλλαγή δεδομένων ανάμεσα στο sink node τις κεφαλές συστάδων αλλά και τους κόμβους αισθητήρων, εντοπίζονται μη ισορροπημένες ροές κίνησης. Υπάρχει περίπτωση μερικές φορές αυτό να ευθύνεται σε εφαρμογές που λειτουργούν με βάση κάποιον συμβάν, το οποίο μπορεί να προκαλεί σποραδικές αλλαγές στην κυκλοφορία. Υπάρχουν πρωτόκολλα δρομολόγησης που μπορούν να κατανέμουν το φορτίο σε διαφορετικές διαδρομές, ώστε να μην υπάρχει μεγάλη συμφόρηση στο δίκτυο. Το πρωτόκολλο MAC θα πρέπει να μπορεί να ανταπεξέλθει σε μη ισορροπημένες κυκλοφορίες αλλά και σε περιπτώσεις βαριάς κυκλοφορίας στο δίκτυο.

Επεκτασιμότητα: Όταν ένα ασύρματο δίκτυο αισθητήρων αποτελείται από εκατοντάδες ή χιλιάδες κόμβους και οι απαιτήσεις για την ποιότητα των παρατηρήσεων αυξάνονται συνεχώς τότε θα πρέπει και ο μηχανισμός QoS που θα υπάρχει στην εφαρμογή να υποστηρίζει την επεκτασιμότητα του δικτύου εξίσου καλά, σε πυκνά και μεγάλα δίκτυα.

1.9.3.2 Απαιτήσεις Δεδομένων QoS

Τα ασύρματα δίκτυα αισθητήρων μπορούν να υποστηρίξουν πάρα πολλές και διαφορετικές εφαρμογές πράγμα που κάνει την ανάλυση των απαιτήσεων τους αρκετά δύσκολο. Για αυτό το λόγο είναι πιο εύκολο να αναλύσουμε τις απαιτήσεις των μοντέλων παράδοσης δεδομένων που χρησιμοποιούνται σε διαφορετικές εφαρμογές και να αντιστοιχίσουμε τις απαιτήσεις αυτών των μοντέλων συλλογής δεδομένων σε ένα σύνολο μετρήσεων QoS. Τα κύρια μοντέλα για την παράδοση δεδομένων είναι το συνεχές μοντέλο, το μοντέλο με βάση τα ερωτήματα, και το μοντέλο με βάση τα συμβάντα. Υπάρχει και ένα τέταρτο μοντέλο που είναι το υβριδικό και δημιουργείτε όταν συνυπάρχουν παραπάνω από ένα μοντέλο στο ίδιο δίκτυο.

1) **Συνεχές μοντέλο (Continuous):** Το συνεχές μοντέλο παράδοσης δεδομένων θεωρείται ως το πιο βασικό μοντέλο για παραδοσιακές εφαρμογές παρακολούθησης στα ασύρματα δίκτυα αισθητήρων που βασίζονται στη συλλογή πληροφοριών. Συνήθως οι ρυθμοί μετάδοσης δεδομένων μπορεί να είναι χαμηλοί και αυτό γίνεται για εξοικονόμηση ενέργειας, επίσης οι ραδιοπομποί ενεργοποιούνται μόνο όταν γίνεται μετάδοση δεδομένων, εάν και εφόσον συλλέγονται κλιμακωτά δεδομένα. Δεδομένα πραγματικού χρόνου, όπως η φωνή ή η εικόνα δεν είναι ανεκτικά στις καθυστερήσεις που μπορεί να υπάρξουν και απαιτούν ένα συγκεκριμένο επίπεδο εύρους ζώνης και υπάρχει μικρή ανεκτικότητα στην απώλεια πακέτων. Όμως για περιοδικά συλλεγόμενα δεδομένα που δεν είναι πραγματικού χρόνου, η απώλεια πακέτων και η καθυστέρηση είναι ανεκτές, όπως για παραδείγματα η παρακολούθηση και η αναγνώριση.
2) **Μοντέλο με βάση ένα συμβάν:** Στο μοντέλο με βάση ένα συμβάν οι αισθητήρες αποστέλλουν δεδομένα μόνο όταν συμβεί το συμβάν που παρακολουθεί το μοντέλο, αλλά συνήθως τα συμβάντα είναι σπάνια. Βέβαια όταν συμβεί το συμβάν, τότε σε πολύ μικρό χρονικό διάστημα δημιουργούνται πάρα πολλά πακέτα που θα πρέπει να μεταφερθούν αξιόπιστα σε πραγματικό χρόνο σε κάποιον σταθμό βάσης. Για να μπορεί να δουλέψει σωστά το δίκτυο αυτό θα πρέπει να υπάρχει αποτελεσματική ανίχνευση και ειδοποίηση του συμβάντος που παρακολουθεί το εκάστοτε δίκτυο. Αυτό έχει ως αποτέλεσμα η ποιότητα και η ακρίβεια των μετρήσεων της παρατήρησης να παίζουν πολύ μεγάλο ρόλο, ώστε να γίνεται γρήγορη και αξιόπιστη μεταφορά των πληροφοριών. Σε ένα μεγάλο ασύρματο δίκτυο αισθητήρων το συμβάν που παρακολουθούν θα το ανιχνεύσουν παραπάνω από ένας κόμβος αισθητήρα με αποτέλεσμα να παραχθούν δεδομένα που θα είναι ίδια μεταξύ τους. Αυτό δημιουργεί μεγάλη συμφόρηση στο δίκτυο μιας και πολλά και ίδια δεδομένα θα πλημμυρίσουν το δίκτυο. Ο τύπος των εφαρμογών αυτών δεν είναι end-to-end

δηλαδή από την μία άκρη του δικτύου στην άλλη άκρη και μερικά παραδείγματα τέτοιων εφαρμογών είναι ο εντοπισμός στόχων αλλά και η παρακολούθηση.

3) **Με βάση τα ερωτήματα:** Το μοντέλο αυτό είναι αρκετά παρόμοιο με αυτό με βάση ένα συμβάν αλλά υπάρχει μία εξαίρεση. Τα δεδομένα που ανιχνεύονται θα μεταφερθούν κατευθείαν στον κόμβο sink χωρίς απαιτήσεις από τους κόμβους αισθητήρων στο μοντέλο με βάση ένα συμβάν ενώ στο μοντέλο με βάση τα ερωτήματα ο κόμβος sink θα ζητήσει τα δεδομένα για να αποσταλούν από τους κόμβους. Στο δίκτυο επειδή ο κόμβος sink ζητάει τα δεδομένα υπάρχει αμφίδρομη κίνηση δεδομένων και θα πρέπει να δεδομένα να παραδίδονται γρήγορα και αξιόπιστα για να έχει υψηλή επίδοση. Κάποια παραδείγματα τέτοιων εφαρμογών είναι ο περιβαλλοντικός έλεγχος και η παρακολούθηση οικοτόπων.

4) **Υβριδικό μοντέλο:** Το υβριδικό μοντέλο μπορεί να υπάρξει μόνο όταν κάποια από τα παραπάνω μοντέλα που προαναφέρθηκαν συνυπάρχουν στο ίδιο δίκτυο με αποτέλεσμα η κυκλοφορία των δεδομένων θα πρέπει πρώτα να ταξινομείται και οι απαιτήσεις των δεδομένων θα πρέπει να ικανοποιούνται. Παράδειγμα υβριδικού μοντέλου μπορεί να είναι μία εφαρμογή που τραβάει βίντεο όταν συμβεί κάποιο γεγονός αλλά επίσης θα αποστέλλει και περιοδικές θερμοκρασίες πίσω στον χρήστη.

1.9.3.3 Μετρήσεις και Παράμετροι QoS

Στην προηγούμενη ενότητα αναλύθηκαν οι απαιτήσεις των δεδομένων στο QoS έτσι ώστε τώρα να μπορούμε να αναλύσουμε ποιες μετρήσεις και με βάση ποιες παραμέτρους ποσοτικοποιούνται αυτές οι απαιτήσεις. Υπάρχουν πολλές μετρήσεις από πλευράς δικτύων που παίζουν ρόλο όπως η μεγιστοποίηση της απόδοσης και της καλής απόδοσης, η ελαχιστοποίηση της καθυστέρησης, η μεγιστοποίηση της αξιοπιστίας, η ελαχιστοποίηση της καθυστέρησης διακύμανσης (jitter) αλλά και η μεγιστοποίηση της ενεργειακής απόδοσης. Το QoS είναι αρκετά πολύπλοκο και θα πρέπει να κοιτάξουμε συνολικά όλοι την στοίβα πρωτοκόλλων για να μπορέσουμε να αξιοποιήσουμε καλύτερα το QoS ως σύνολο. Εμείς θα εστιάσουμε όμως στο επίπεδο MAC και ποιες μετρήσεις θα μπορούσε το πρωτόκολλο αυτό να εκπληρώσει.

- **Ελαχιστοποίηση της καθυστέρησης πρόσβασης στο μέσο:** Θα πρέπει να λάβουμε υπόψιν ότι για να ελαχιστοποιηθεί η καθυστέρηση από άκρο σε άκρο δηλαδή από τον αισθητήρα μέχρι και τον κόμβο sink θα πρέπει να δούμε και την απόδοση του επιπέδου δρομολόγησης. Ωστόσο, στο επίπεδο MAC αυτό το οποίο θα μπορούσε να γίνει είναι η μείωση της καθυστέρησης της πρόσβασης στο μέσο των αισθητήρων, έτσι ώστε να εξασφαλιστεί ότι η καθυστέρηση των πακέτων θα βελτιωθεί μέχρι να φτάσει στις απαιτήσεις καθυστέρησης από άκρο σε άκρο.
- **Ελαχιστοποίηση των συγκρούσεων:** Το πρόβλημα με το να υπάρχουν συγκρούσεις σε ένα δίκτυο είναι ότι η πληροφορία χάνεται και θα πρέπει να ξανά γίνει η αποστολή της πληροφορίας, το οποίο σημαίνει ότι επηρεάζει της μετρήσεις δικτύου όπως η

απόδοση, η καθυστέρηση και η ενεργειακή απόδοση. Το επίπεδο MAC όμως είναι υπεύθυνο για τον διαμοιρασμό του ασύρματου μέσου οπότε έχει και την ευθύνη για την ελαχιστοποίηση των συγκρούσεων. Το θετικό είναι ότι οι συγκρούσεις μπορούν αποφευχθούν χρησιμοποιώντας προσεκτικές μεθόδους ανίχνευσης, όπως επίσης και να προσαρμοστεί το παράθυρο του ανταγωνισμού σύμφωνα με τις απαιτήσεις της κυκλοφορίας λαμβάνοντας πάντα υπόψιν τα πρωτόκολλα που βασίζονται στον ανταγωνισμό. Με την ίδια λογική θα μπορούσε να γίνει το ίδιο για τις απαιτήσεις των δικτύων αν προσαρμοστεί ο αριθμός των χρονοθυρίδων αλλά και των συχνοτήτων σύμφωνα με τις απαιτήσεις του δικτύου με αποτέλεσμα να αποτραπούν οι συγκρούσεις στην περίπτωση που χρησιμοποιείται πρωτόκολλο χωρίς ανταγωνισμό.

- **Μεγιστοποίηση της αξιοπιστίας:** Η μεγιστοποίηση της αξιοπιστίας συνδυάζεται με την ελαχιστοποίηση των συγκρούσεων και χρησιμοποιούνται μηχανισμοί επιβεβαίωσης για τον εντοπισμό πακέτων και αν υπάρχει απώλεια να γίνει αναμετάδοση τους. Το επίπεδο MAC μπορεί να συμβάλει στην διασφάλιση της αξιοπιστίας και η αναμετάδοση των χαμένων πακέτων να γίνεται εγκαίρως ώστε να διορθώνονται το συντομότερο δυνατόν.

- **Ελαχιστοποίηση της κατανάλωσης ενέργειας:** Στα ασύρματα δίκτυα αισθητήρων η πιο σημαντική απαίτηση είναι αυτή της ενεργειακής απόδοσης λόγω του ότι τα περισσότερα δίκτυα αυτού του τύπου λειτουργούν με μπαταρίες. Το επίπεδο MAC έχει την δύναμη να βοηθάει το δίκτυο στην αποφυγή των συγκρούσεων οπότε και των αναμεταδόσεων με αποτέλεσμα να συμβάλει στην ελαχιστοποίηση της κατανάλωσης ενέργειας. Επίσης, έχει την δυνατότητα να συντονίζει τον κύκλο λειτουργίας των αισθητήρων ανάλογα με την δυναμική του δικτύου. Σε ένα ασύρματο δίκτυο αισθητήρων ο κύκλος λειτουργίας παίζει πολύ σημαντικό ρόλο, γιατί η ασύρματη λειτουργεία καταναλώνει το μεγαλύτερο ποσοστό ενέργειας, οπότε ο πομπός αναγκάζεται να είναι ανενεργός όταν δεν χρειάζεται. Μεγαλύτερη εξοικονόμηση ενέργειας μπορεί να δημιουργηθεί με το να προσαρμόζουμε δυναμικά την ισχύ της μετάδοσης από τους αισθητήρες ανάλογα με τις συνθήκες του δικτύου, έτσι ώστε να μειωθεί ακόμα περισσότερο η κατανάλωση ενέργειας.

- **Ελαχιστοποίηση παρεμβολών:** Τα ασύρματα δίκτυα λειτουργούν με συχνότητες οι οποίες δεν είναι ιδιωτικές αλλά κοινόχρηστες. Αυτό σημαίνει ότι αν κάποιο άλλο δίκτυο χρησιμοποιεί το ίδιο φάσμα συχνότητας, τότε θα υπάρχουν ανεπιθύμητες παρεμβολές. Η ύπαρξη παρεμβολών σε ένα δίκτυο προκαλούν απώλεια πακέτων το οποίο με την σειρά του καταστρέφει την απόδοση του δικτύου, αυξάνει την καθυστέρηση και επηρεάζει αρνητικά και την ενεργειακή απόδοση του. Υπάρχει τρόπος να συνυπάρχουν δίκτυα στον ίδιο χώρο αρκεί να έχουν πρόσβαση σε διαφορετικό κομμάτι του φάσματος της συχνότητας, ώστε να μην υπάρχουν τέτοιου είδους προβλήματα. Το επίπεδο MAC μπορεί να πετύχει ελάχιστη παρεμβολή και με άλλους τρόπους, όπως να παραμετροποιεί το παράθυρο ανταγωνισμού, το χρονοδιάγραμμα, την ισχύ της μετάδοσης αλλά και το κανάλι λειτουργίας.

- **<u>Μεγιστοποίηση της προσαρμοστικότητας στις αλλαγές:</u>** Η φύση των ασύρματων δικτύων αισθητήρων είναι αρκετά δυναμική και αυτό σημαίνει ότι μπορεί κάποιο κόμβοι να αποσυνδεθούν από το δίκτυο, γιατί εξαντλήθηκε η μπαταρία τους ή να προστεθούν καινούργιοι κόμβοι στο δίκτυο. Οι περιβαλλοντικές συνθήκες συνήθως είναι αρκετά κακές, το οποίο έχει σαν αποτέλεσμα με την πάροδο του χρόνου το δίκτυο να μην είναι πάντα σταθερό και οι συνδέσεις μεταξύ των κόμβων να πρέπει να αλλάξουν. Ανάλογα με το δίκτυο την εφαρμογή του αλλά και το φαινόμενο που παρακολουθεί ενδέχεται να πρέπει να γίνουν αλλαγές, όπως αλλαγή της τοπολογίας και των συνθηκών της κυκλοφορίας. Το πρωτόκολλο MAC θα πρέπει, λοιπόν, να είναι αρκετά προσαρμοστικό ανάλογα με την δυναμική του δικτύου, για παράδειγμα εάν στο δίκτυο τα περισσότερα δεδομένα είναι δεδομένα υψηλού ρυθμού και πραγματικού χρόνου, τότε οι κόμβοι θα πρέπει να αναγκαστούν να αυξήσουν τον κύκλο εργασίας τους. Θα πρέπει όμως να μπορεί να κάνει και το αντίθετο, δηλαδή αν οι ανάγκες της εφαρμογής είναι τέτοιες ούτως ώστε η κίνηση να είναι χαμηλού ρυθμού, τότε θα πρέπει να εκτελούνται και οι ανάλογες αλλαγές, όπως οι κόμβοι να μπαίνουν σε κατάσταση “ύπνου” για εξοικονόμηση ενέργειας.

1.9.4 Πρωτόκολλα MAC με Επίγνωση QoS

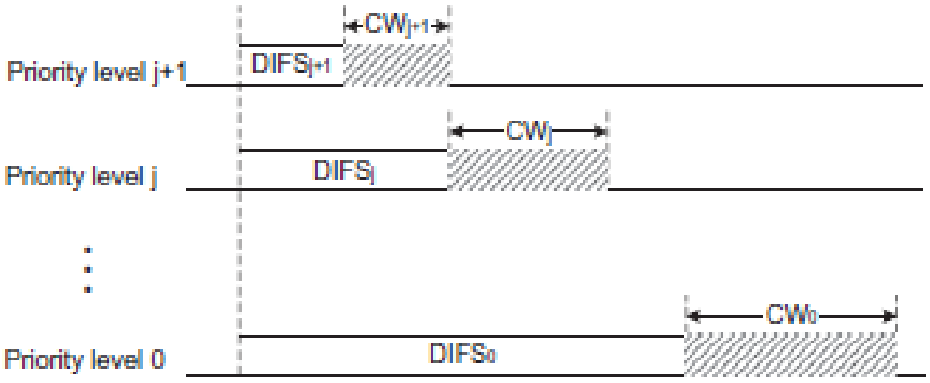
1.9.4.1 PSIFT

Το PSIFT είναι ένα πρωτόκολλο MAC το οποίο έχει επίγνωση του QoS και είναι σχεδιασμένο για εφαρμογές που βασίζονται σε συμβάντα με την χρήση του πρωτοκόλλου SIFT. Επίσης «εκμεταλλεύεται» την ιδιότητα της χωρικής συσχέτισης των ασύρματων δικτύων αισθητήρων. Το πρωτόκολλο βασίζεται σε μία τεχνική που υποθέτει ότι οι πρώτες R από τις N αναφορές για τον εντοπισμό ενός συμβάντος είναι το σημαντικότερο κομμάτι της ανταλλαγής μηνυμάτων και θα πρέπει να μεταδίδονται με πολύ χαμηλή καθυστέρηση. Το πρωτόκολλο θεωρεί ότι οι R αναφορές θα είναι επαρκής αριθμός για τον κόμβο sink έτσι ώστε να μπορεί να αναγνωριστεί το συμβάν με ακρίβεια και να εξαλείψει τον πλεονασμό των δεδομένων που με την σειρά τους μειώνουν τις συγκρούσεις αλλά και την καθυστέρηση.

Το PSIFT βασίζεται πάνω στο πρωτόκολλο CSMA και παρέχει διαφοροποίηση στην κίνηση αλλάζοντας τα διαστήματα ανάμεσα από τα πλαίσια (IFS) αλλά, επίσης, και το παράθυρο του ανταγωνισμού (CW) για κάθε διαφορετική κατηγορία κίνησης όπως φαίνεται στην φωτογραφία παρακάτω. Ο τρόπος με τον οποίο διαχωρίζονται οι κλάσεις της κίνησης είναι δυναμικός και βασίζεται στον αριθμό αλμάτων (hops) που έχει κάνει είδη το πακέτο, όσα περισσότερα άλματα έχει κάνει τόσο ανεβαίνει η προτεραιότητα που θα έχει στο δίκτυο.

Το PSIFT είναι μία πολύ καλή επιλογή για εφαρμογές που βασίζονται σε συμβάν αλλά δεν θα ήταν πολύ κακή επιλογή για οποιαδήποτε άλλη εφαρμογή. Εάν αφαιρεθεί ο

πλεονασμός τότε τα δεδομένα παράδοσης δεν θα είναι αξιόπιστα αφού η ταυτοποίηση των αναφορών που ανήκουν σε διαφορετικά συμβάντα θα ήταν πολύ δύσκολη. Αν μειωθεί ο αριθμός των αναφορών, τότε δεν θα υπάρχει πολλή κίνηση στο δίκτυο και αυτό θα έχει ως αποτέλεσμα να υπάρχουν πάρα πολλοί αδρανείς κόμβοι. Από πλευράς βέβαια κατανάλωσης ενέργειας του δικτύου αυτό συμφέρει, ειδικά αν χρησιμοποιήσουμε την τεχνική ύπνου/ακρόασης.



Εικόνα 19. PSIFT

Πηγή:https://www.sciencedirect.com/science/article/abs/pii/S1389128611000703

1.9.4.2 RL-MAC

Το RL-MAC λειτουργεί με μία τεχνική που λέγεται ενισχυτική μάθηση και το ίδιο το πρωτόκολλο έχει επίσης επίγνωση του QoS και χρησιμοποιεί επίσης ένα σχήμα CSMA. Το πρωτόκολλο προσαρμόζει τον κύκλο λειτουργίας των κόμβων όχι μόνο με βάση τις τοπικές παρατηρήσεις του συγκεκριμένου κόμβου αλλά και από τις παρατηρήσεις των γειτονικών κόμβων. Μια τυπική παρατήρηση θα μπορούσε να είναι ο αριθμός των πακέτων που έχουν ληφθεί και μεταδοθεί επιτυχώς κατά την διάρκεια της ενεργής περιόδου που καταγράφεται, για να χρησιμοποιηθεί, ούτως ώστε να παραμετροποιηθεί ο κύκλος λειτουργίας ανάλογα με το φορτίο που υπάρχει και τις ουρές αναμονών που μπορεί να υπάρχουν. Ο τρόπος με τον οποίο λειτουργούν οι γειτονικές παρατηρήσεις είναι ότι όταν αποστέλλονται τα πακέτα δεδομένων, προστίθεται μία έξτρα πληροφορία στην επικεφαλίδα του πακέτου, η οποία παρέχει την πληροφορία για τον αριθμό των αποτυχημένων προσπαθειών μετάδοσης από τον αποστολέα προς τον κόμβο λήψης. Με αυτό τον τρόπο εξοικονομεί ενέργεια και μειώνεται αισθητά ο αριθμός των χαμένων πακέτων λόγω πρόωρου ύπνου του κόμβου. Τα πρωτόκολλα που χρησιμοποιούν ενισχυτική μάθηση με κάποιον αλγόριθμο μπορούν να προσαρμοστούν πολύ καλά στις συνθήκες ενός δικτύου αλλά δεν θα μπορέσουν να εφαρμοστούν σε δίκτυα που είναι περιορισμένα σε ενέργεια και επεξεργαστική ισχύ.

1.9.4.3 PR-MAC

Το PR-MAC [18] μέσω των κόμβων αισθητήρων αναγνωρίζει τα διαφορετικά συμβάντα που παρακολουθεί και τους δίνει διαφορετικές προτεραιότητες αλλά και παρέχει υπηρεσίες διαφοροποίησης ανάλογα το συμβάν. Κάποιες από τις αλλαγές που μπορεί να κάνει είναι να αλλάξει το παράθυρο του ανταγωνισμού (CW) και τα διαστήματα ανάμεσα από τα πλαίσια (IFS) για κάθε διαφορετικό συμβάν. Για να έχει πρόσβαση στο μέσο και να το κρατήσει για τον εαυτό του ο κόμβος αποστολέας στέλνει έναν παλμό αντί να χρησιμοποιήσει πακέτα Request To Send (RTS) και Clear to Send (CTS). Αυτό έχει σαν αποτέλεσμα η μόνη σύγκρουση που μπορεί να συμβεί στο δίκτυο είναι όταν οι κόμβοι έχουν ίδιες προτεραιότητες.

Ο μηχανισμός επιβεβαίωσης πετυχαίνετε με την αποστολή πολύ ισχυρού σήματος εκπομπής από τον κόμβο sink προς όλους τους κόμβους του δικτύου και η επιβεβαίωση από τους ενδιάμεσους κόμβους δεν εφαρμόζεται. Με αυτήν την τεχνική δεν υπάρχει η έννοια της επαναμετάδοσης στο PR-MAC αφού ενδιαφερόμαστε περισσότερο για την καθυστέρηση παράδοσης του αισθητοποιημένου συμβάντος περισσότερο από την αξιοπιστία του. Ένα αρνητικό του πρωτοκόλλου αυτού είναι ότι για να μπορεί να ακουστεί σε όλους τους αισθητήρες απαιτείται ένας πολύ δυνατός κόμβος sink και έτσι καταλήγει να μην είναι αρκετά πρακτικό.

Επίσης, επειδή δεν υπάρχουν επιβεβαιώσεις μεταξύ των αναμεταδόσεων μειώνεται πάρα πολύ η αξιοπιστία του πρωτοκόλλου. Ένα θετικό που έχει όμως είναι ότι μπορεί ένας κόμβος να διατηρήσει το μέσο χωρίς μηνύματα RTS και CTS με αποτέλεσμα να μειώνεται η επιβάρυνση του δικτύου. Ωστόσο, ένα μικρό πρόβλημα που αντιμετωπίζει είναι ότι για να υποστηρίξει την παράδοση μεταβλητού μεγέθους πακέτων θα πρέπει τα πακέτα RTS να περιλαμβάνουν την διάρκεια που το μέσο είναι κρατημένο.

1.9.5 Επίπεδο Δικτύου

Τα ασύρματα δίκτυα αισθητήρων χρόνο με τον χρόνο γίνονται πιο πολύπλοκα και απαιτητικά έτσι με περισσότερες απαιτήσεις. Αυτό έχει σαν επακόλουθο να δημιουργούνται καινούργιες τεχνολογίες και τεχνικές ελαχιστοποίησης πόρων για να μπορέσουν να βελτιστοποιηθούν τα δίκτυα αυτά. Για να γίνουν όμως όλα αυτά, τα ασύρματα δίκτυα αισθητήρων βασίζονται στο επίπεδο δικτύου, ώστε να χρησιμοποιήσουν ένα αποτελεσματικό πρωτόκολλο δρομολόγησης, ώστε να επιλεχθεί μία διαδρομή με χαρακτηριστικά όπως με την λιγότερη καθυστέρηση, μεγάλη διάρκεια ζωής, ενέργεια και οποιοδήποτε άλλο χαρακτηριστικό είναι σημαντικό για την εκάστοτε εφαρμογή. Στο επίπεδο δικτύου αυτό που καταναλώνει πολλή ενέργεια και είναι η δρομολόγηση κάτι το οποίο χρειάζεται βελτίωση. Η εφαρμογή και οι ανάγκες της παίζουν μεγάλο ρόλο στο πως θα σχεδιαστεί το πρωτόκολλο δρομολόγησης και κάποια χαρακτηριστικά που το επιβαρύνουν είναι, ο αριθμός των αλμάτων αλλά επίσης και η απόσταση των αλμάτων.

1.9.5.1 Περιορισμοί για την Σχεδίαση ενός Πρωτοκόλλου Δρομολόγησης

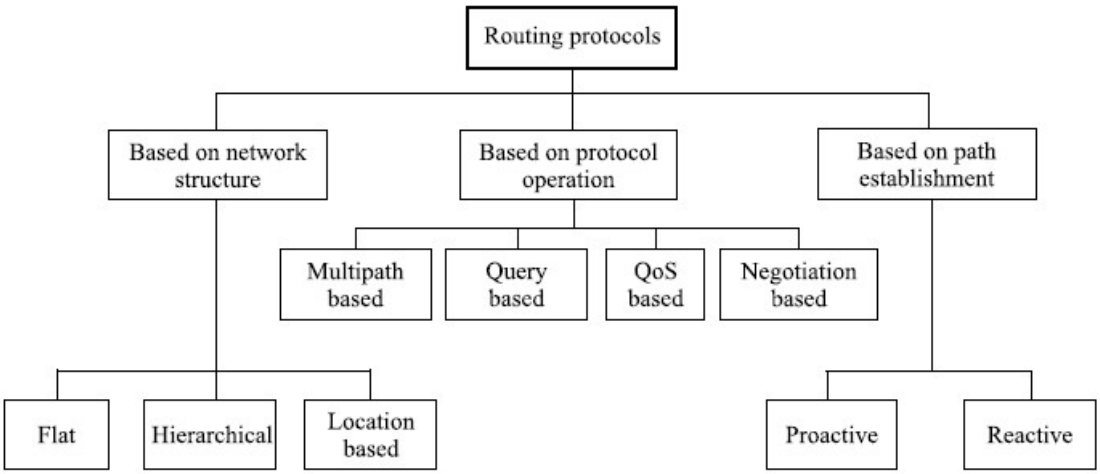
Τα πρωτόκολλα δρομολόγησης υπήρχαν και πριν δημιουργηθούν τα ασύρματα δίκτυα αισθητήρων αλλά είχαν σχεδιαστεί με γνώμονα τους ηλεκτρονικούς υπολογιστές και πως αυτοί θα βρίσκονται σταθεροί σε ένα κτίριο. Για να μπορέσουν να λειτουργήσουν τα πρωτόκολλα δρομολόγησης στα ασύρματα δίκτυα αισθητήρων θα πρέπει να μπορούν να αντιμετωπίσουν αρκετές προκλήσεις και περιορισμούς. Κάποιες από τις προκλήσεις είναι:

- **Κλίμακα Δικτύου:** Η κλίμακα του δικτύου κρίνεται από την εφαρμογή και σε τι έκταση πρέπει να κινηθεί και πόσους εκατοντάδες η χιλιάδες κόμβους αισθητήρων χρειάζεται. Όταν η κλίμακα ενός δικτύου είναι τόσο μεγάλη οι κόμβοι αισθητήρων θα πρέπει να έχουν την δυνατότητα να αυτό διοργανώνονται με την βοήθεια του πρωτοκόλλου δρομολόγησης που θα έχει σφαιρικές γνώσεις για όλο το δίκτυο.
- **Δυναμική του Κόμβου:** Τα ασύρματα δίκτυα αισθητήρων είναι στην φύση τους δυναμικά λόγω του ότι η τοπολογία αλλάζει συνεχώς λόγω εξάντλησης ισχύος, εξάντληση μπαταρίας και κίνησης. Η δρομολόγηση του πρωτοκόλλου θα πρέπει να προσαρμόζεται στις αλλαγές αυτές, ώστε να είναι αποδοτικό το δίκτυο.
- **Περιορισμένος αριθμός πόρων:** Στα ασύρματα δίκτυα αισθητήρων ένα από τα μεγαλύτερα προβλήματα που υπάρχουν είναι ο λιγοστός αριθμός πόρων και ειδικά οι πόροι της μπαταρίας. Το πρωτόκολλο δρομολόγησης θα πρέπει να είναι σε θέση να αποστέλλει δεδομένα στο μισό κύκλο λειτουργίας. Ανάλογα τον τύπο της εφαρμογής και τις ανάγκες που έχει το πρωτόκολλο θα πρέπει να μπορεί να μεταδίδει τα δεδομένα με ακρίβεια, αλλά ταυτόχρονα να μην καταναλώνει πολλή ενέργεια.
- **Φύση των κόμβων:** Οι πληροφορίες που συλλέγουν και αποστέλλουν οι κόμβοι σε ορισμένη κάλυψη, ανάλογα με την εφαρμογή και τις ανάγκες της μπορεί να είναι ομοιογενείς ή ετερογενείς. Το πρωτόκολλο δρομολόγησης χρειάζεται να υποστηρίζει όλων των ειδών πληροφοριών και κόμβους με διαφορετικές παραμέτρους και δυνατότητες.
- **QoS:** Στα ασύρματα δίκτυα αισθητήρων η πληροφορία που ανιχνεύεται από τους κόμβους αισθητήρων έχει πολύ μεγάλη σημασία και αν καθυστερήσει να γίνει η μετάδοση, τότε δεν θα είναι χρήσιμα τα δεδομένα και έτσι θα χάσουν την σημασία τους. Θα πρέπει να υπάρχει μία ισορροπία ανάμεσα στην ακρίβεια που μπορεί να χρειάζεται η εφαρμογή, να έχουν οι πληροφορίες που μεταδίδονται και στην ενέργεια που θα καταναλώνεται.

1.9.5.2 Κατηγοριοποίηση Πρωτοκόλλων Δρομολόγησης

Στα πρωτόκολλα δρομολόγησης υπάρχει μία μεγάλη πληθώρα επιλογών και ταξινόμησης με βάση τα διαφορετικά κριτήρια που θα καθορίσουν την διαδρομή προς τον κόμβο sink.

Υπάρχουν τρεις κεντρικές κατηγορίες πρωτοκόλλων δρομολόγησης, πρωτόκολλα δρομολόγησης με βάση τη δομή του δικτύου, πρωτόκολλα δρομολόγησης με βάση τη λειτουργία του πρωτοκόλλου και πρωτόκολλα δρομολόγησης με βάση την καθιερωμένη διαδρομή.



Εικόνα 20. Κατηγοριοποίηση Πρωτοκόλλων Δρομολόγησης

Πηγή:https://jtit.pl/jtit/article/view/599

1.9.5.2.1 Πρωτόκολλα δρομολόγησης με βάση τη δομή του δικτύου

- **Δρομολόγηση Flat structure:** Σε αυτό το πρωτόκολλο δρομολόγησης όλοι οι κόμβοι έχουν τον ίδιο ρόλο, είναι δηλαδή κάθε κόμβος σταθμός βάσης. Με αυτήν την τακτική όλοι οι κόμβοι διαθέτουν τις απαραίτητες πληροφορίες, ώστε ο χρήστης να μπορεί να κάνει κάποιο ερώτημα σε οποιονδήποτε κόμβο θέλει και να λάβει τις απαραίτητες πληροφορίες.
- **Δρομολόγηση Hierarchical structure:** Σε αντίθεση με την δρομολόγηση flat structure εδώ οι κόμβοι δεν έχουν όλοι την ίδια ικανότητα αλλά υπάρχουν κόμβοι με υψηλότερες ικανότητες από τους υπόλοιπους. Αυτοί οι κόμβοι εκτελούν τα πιο κρίσιμα καθήκοντα και είναι πιο σημαντικοί για το δίκτυο, ενώ όλα τα υπόλοιπα καθήκοντα πηγαίνουν σε κόμβους με λιγότερες ικανότητες. Η δρομολόγηση αυτή είναι μία δομή με δύο ή περισσοτέρων επιπέδων.
- **Δρομολόγηση Location-based:** Η επικοινωνία των κόμβων γίνεται με βάση την τοποθεσία τους, ενώ για τους αισθητήρες η επικοινωνία γίνεται με την χρήση δορυφόρου. Το σύστημα για να μην ξοδεύει πολλή ενέργεια, θα πρέπει να είναι εξοπλισμένο με έναν δέκτη GPS χαμηλής ισχύος, αλλά εάν δεν υπάρχει αυτή η επιλογή υπάρχει και ένα άλλος τρόπος. Μπορεί να μετρηθεί η σχετική απόσταση ενός κόμβου με την βοήθεια των γειτονικών κόμβων όπου με βάση την ισχύ του λαμβανόμενου σήματος μπορεί να υπολογιστεί η απόσταση.

1.9.5.2.2 Πρωτόκολλα δρομολόγησης με βάση τη λειτουργία του πρωτοκόλλου

- **Δρομολόγηση Multipath:** Η δρομολόγηση αυτή για να μεταδοθούν τα δεδομένα από την πηγή στον προορισμό έχει στην διάθεση της πολλαπλές διαδρομές. Αυτό έχει σαν αποτέλεσμα το δίκτυο να είναι αρκετά ανεκτικό σε σφάλματα αλλά μπορεί επίσης να αυξηθεί η κατανάλωση ενέργειας όπως και οι έξτρα πληροφορίες που χρειάζεται το πρωτόκολλο για τις πολλαπλές διαδρομές. Για να είναι βιώσιμο σε ένα δίκτυο θα μπορούσε να χρησιμοποιηθεί ο αλγόριθμος μόνο σε κόμβους με μεγάλο αριθμό ενέργειας. Το πρωτόκολλο μπορεί και αλλάζει μόνο του τις διαδρομές που θα επιλέξει, όταν βρει καλύτερη διαδρομή από την υπάρχουσα και έτσι ανεβαίνει η αξιοπιστία του δικτύου σε αρκετά αναξιόπιστα περιβάλλοντα. Ένα σημαντικό κατόρθωμα που μπορεί να κάνει η δρομολόγηση αυτή είναι ότι η πληροφορία διχοτομείται σε μικρότερα πακέτα και έχει την δυνατότητα να σταλούν από διαφορετικά μονοπάτια. Στο τέλος, συναρμολογούνται για να μπορούν να διαβαστούν αλλά ακόμα και εάν κάποιο από τα πακέτα που στάλθηκαν χαθεί λόγω σφάλματος της σύνδεσης, το μήνυμα μπορεί να ανακατασκευαστεί.
- **Δρομολόγηση Query based:** Στην query based δρομολόγηση ένας κόμβος ξεκινάει ένα ερώτημα και το διαδίδει στο δίκτυο, κάθε κόμβος στο δίκτυο αυτό θα λάβει το ερώτημα και μόνο ο σωστός κόμβος που έχει τα δεδομένα που ταιριάζουν απαντά. Αυτό είναι αρκετά ενεργοβόρο, οπότε αντί να διαδίδει το ερώτημα σε όλο το δίκτυο το διαδίδει σε μία τυχαία κατεύθυνση και περιμένει απάντηση. Από αυτήν την τυχαία κατεύθυνση εάν κανένας κόμβος δεν απαντήσει τότε το ερώτημα θα μεταδοθεί σε όλο το δίκτυο.
- **Δρομολόγηση QoS based:** Στο QoS μεγάλο ρόλο παίζουν οι παράμετροι των εφαρμογών όπως η καθυστέρηση, οι πόροι του συστήματος και το εύρος ζώνης. Το πρωτόκολλο δρομολόγησης θα πρέπει να μπορεί να διατηρήσει την ποιότητα και τις προδιαγραφές των παραμέτρων της εφαρμογής όση ώρα μεταδίδονται τα δεδομένα. Είναι, επίσης, υπεύθυνο για την διατήρηση της ενέργειας σε χαμηλά επίπεδα όπως και άλλων μετρήσεων.
- **Δρομολόγηση Negotiation based:** Ο κατακλυσμός πακέτων και το πρωτόκολλο gossip έχουν σαν αποτέλεσμα ένας κόμβος να λάβει πολλαπλά δεδομένα που είναι ίδια μεταξύ τους. Το πρωτόκολλο gossip επιτρέπει τον διαμοιρασμό κατάστασης σε κατανεμημένα συστήματα, οπότε με το πρωτόκολλο δρομολόγησης για να μην υπάρχει το πρόβλημα με τα διπλότυπα δεδομένα βασίζεται στην διαπραγμάτευση. Οι κόμβοι στέλνουν μεταξύ τους μία ακολουθία από μηνύματα διαπραγμάτευσης, έτσι ώστε να μπορούν να μεταφέρονται τα διπλότυπα μηνύματα σε επόμενους κόμβους, αν ο τωρινός κόμβος έχει ήδη τα δεδομένα αυτά.

1.9.5.2.3 Πρωτόκολλα Δρομολόγησης με Βάση την Καθιερωμένη Διαδρομή

- **Δρομολόγηση Reactive path establishment:** Η δρομολόγηση αυτή επηρεάζεται από τα γεγονότα που γίνονται στο δίκτυο. Ο τρόπος με τον οποίο λειτουργεί το

πρωτόκολλο είναι ότι όταν ένα πακέτο δεδομένων φεύγει από τον έναν κόμβο και πηγαίνει προς τον τελικό προορισμό του περνώντας από ενδιάμεσους κόμβους. Για να αποφασίσει ποια διαδρομή θα ακολουθήσει η πληροφορία ώστε να φτάσει στον προορισμό που πρέπει αποφασίζεται από το ιστορικό που υπάρχει συνήθως στην κρυφή μνήμη (cache) του κόμβου. Σε ορισμένες εφαρμογές όμως που δεν υπάρχει περιθώριο πόρων οι κόμβοι έχουν περιορισμένη μνήμη και έχουν μικρή υπολογιστική ικανότητα, με αποτέλεσμα να μην υπάρχει ιστορικό κρυφής μνήμης. Επίσης παίζουν ρόλο και άλλες μετρήσεις για την απόφαση του επόμενου κόμβου όπως, η απόσταση, το κόστος, το εύρος ζώνης αλλά και η ενέργεια του κόμβου.

- **Δρομολόγηση Proactive path establishment:** Η απόφαση για την διαδρομή που θα ακολουθήσουν τα πακέτα δεδομένων αποφασίζεται στην αφετηρία. Η διαδρομή που θα αποφασιστεί δημιουργείται με βάση το ελάχιστο κόστος το μέγιστο εύρος ζώνης η τους κόμβους με τα υψηλότερα επίπεδα ενέργειας. Όταν αποφασιστεί και δημιουργηθεί η διαδρομή που θα ακολουθήσουν τα πακέτα τότε όλα τα πακέτα δεδομένων θα σταλούν από την συγκεκριμένη διαδρομή και καμία άλλη. Αυτό μπορεί να είναι και μειονέκτημα γιατί το πρωτόκολλο δεν είναι ανεκτικό σε σφάλματα καθώς τα πακέτα δεδομένων μπορεί να χαθούν ή η επιλεγμένη διαδρομή να σταματήσει να λειτουργεί.

1.9.5.2.4 Παραδείγματα Πρωτοκόλλων στο Επίπεδο Δικτύου

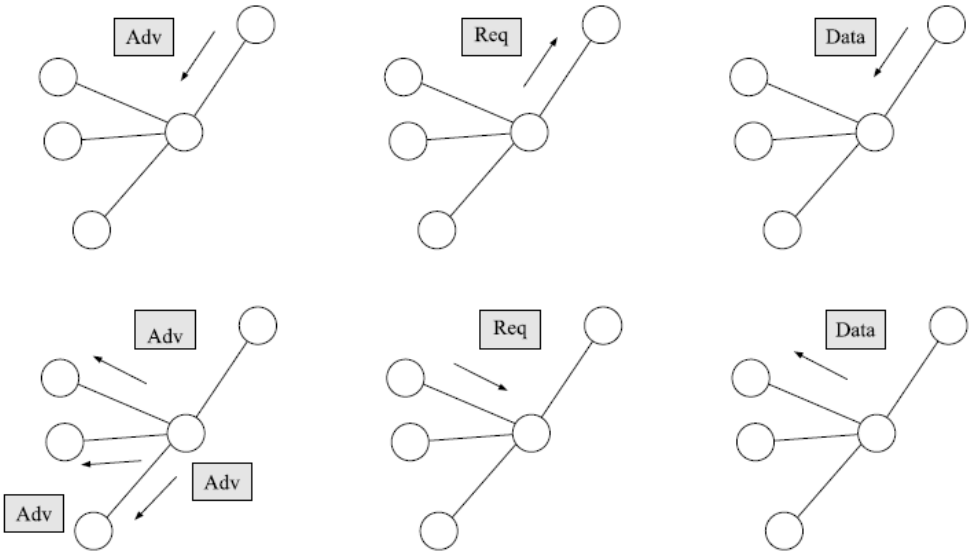
1.9.5.2.4.1 Flooding and Gossiping

Ο όρος «πλημμύρα» χρησιμοποιείται για να εξηγηθεί ότι ο κόμβος έχει την δυνατότητα να στείλει πακέτα δεδομένων μέσω όλων των διαθέσιμων συνδέσεων. Βέβαια για να αποφευχθεί η συνεχής επανάληψη ενός πακέτου στο δίκτυο ώστε να μην υπάρχει μεγάλη και αχρείαστη κατανάλωση ενέργειας, το πακέτο έχει έναν μέγιστο αριθμό hops και συγκεκριμένο χρόνο ζωής στο δίκτυο Time To Live (TTL) και αυτές οι πληροφορίες υπάρχουν πάνω στο πακέτο την ώρα που μεταδίδεται. Μία άλλη προσέγγιση είναι το gossiping όπου το πακέτο δεδομένων μεταδίδεται σε έναν τυχαίο γειτονικό κόμβο όπου με αυτό τον τρόπο εξοικονομείται αρκετό εύρος ζώνης στο δίκτυο αλλά παράλληλα αυξάνεται αρκετά η καθυστέρηση στο δίκτυο.

1.9.5.2.4.2 Sensor Protocols for Information via Negotiation (SPIN)

Το πρωτόκολλο SPIN έχει βελτιώσει πολλά μειονεκτήματα παλαιότερων πρωτοκόλλων διάδοσης δεδομένων. Βασίζεται όχι στα ίδια τα δεδομένα αλλά στα μεταδεδομένα τους (metadata). Ο τρόπος με τον οποίο λειτουργεί το πρωτόκολλο είναι ότι ο πομπός θα μεταδώσει τα μεταδεδομένα των δεδομένων και αν κάποιος δέκτης που έχει ελέγξει τα δεδομένα και τον ενδιαφέρουν, στέλνει μήνυμα ο δέκτης στον πομπό να ξεκινήσει την αποστολή τους. Στην φωτογραφία παρακάτω τα Adv πακέτα είναι διαφημιστικά πακέτων των μεταδεδομένων, τα Req είναι αιτήματα για τα δεδομένα που διαφημιζόντουσαν

προηγουμένως και τα Data είναι τα κανονικά πακέτα δεδομένων που αποστέλλονται στους ενδιαφερόμενους κόμβους.

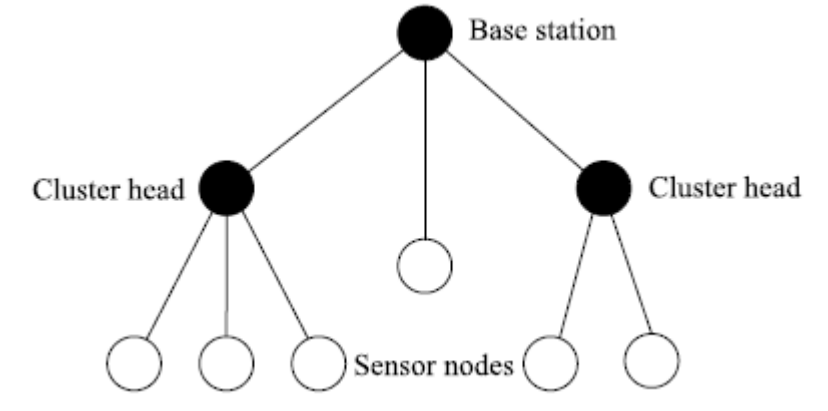


Εικόνα 21. SPIN

Πηγή:https://jtit.pl/jtit/article/view/599

1.9.5.2.4.3 Low-Energy Adaptive Clustering Hierarchy (LEACH)

Το πρωτόκολλο LEACH είναι ένα ιεραρχικό πρωτόκολλο το οποίο βασίζεται σε συστάδες (clusters). Οι κόμβοι με την μεγαλύτερη ενέργεια αποκαλούνται «επικεφαλείς» της εκάστοτε συστάδας και εκτελούν κάποιες επιπλέον εργασίες, όπως την συλλογή όλων των δεδομένων της συστάδας, την συμπίεση αλλά και την αποστολή τους στον κόμβο sink. Με αυτήν την τεχνική το LEACH μειώνει σημαντικά την κατανάλωση ενέργειας επιλέγοντας αποτελεσματικά τους επικεφαλής συστάδων, αυξάνοντας έτσι την διάρκεια ζωής του δικτύου. [11]



Εικόνα 22. LEACH

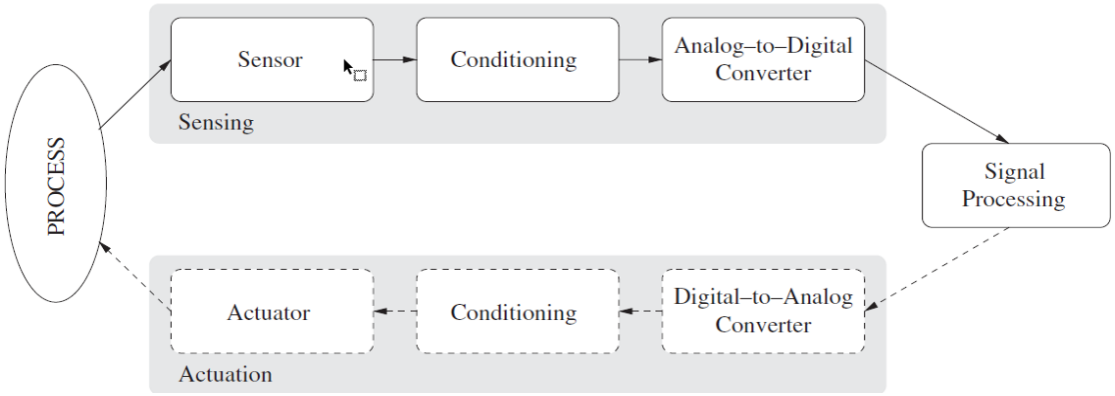
Πηγή:https://jtit.pl/jtit/article/view/599

2. WSN και IoT

2.1 Αισθητήρες και Ανίχνευση

Η ανίχνευση είναι μία τεχνική που χρησιμοποιείται με σκοπό την συλλογή πληροφοριών για ένα φυσικό αντικείμενο ή μία διαδικασία συμπεριλαμβανομένου και την εμφάνιση γεγονότων, όπως για παράδειγμα η αλλαγή στην θερμοκρασία και η πίεση. Το αντικείμενο που πραγματοποιεί αυτή την διαδικασία ανίχνευσης ονομάζεται αισθητήρας. Το καλύτερο παράδειγμα και το πιο συνηθισμένο που θα μπορούσε να δοθεί είναι το ανθρώπινο σώμα, καθώς διαθέτει πληθώρα αισθητήρων όπως μάτια, αυτιά και μύτη. Τα μάτια τα χρησιμοποιούμε για οπτικές πληροφορίες, τα αυτιά για ηχητικές πληροφορίες και την μύτη για όσφρηση. Αυτού του είδους αισθητήρες ανήκουν στην κατηγορία των απομακρυσμένων αισθητήρων, διότι αντλούν τις πληροφορίες που χρειάζονται χωρίς να έρχονται σε επαφή με το αντικείμενο ή το φαινόμενο που παρακολουθούν.

Οι αισθητήρες μετατρέπουν τα δεδομένα που λαμβάνουν από το περιβάλλον τους σε ηλεκτρονικό σήμα (0 και 1) ώστε να μπορεί να αναγνωριστεί από τους ηλεκτρονικούς υπολογιστές με σκοπό να μετρηθούν και να αναλυθούν. Αυτή η διαδικασία δεν είναι τόσο απλή, γιατί το σήμα που λαμβάνουν οι αισθητήρες συνήθως έχει πολύ θόρυβο από διπλανά ηλεκτρικά καλώδια και πολλές φορές χρειάζεται να γίνει ενίσχυση ή εξασθένηση του σήματος, για να ταιριάζει καλύτερα στην μετατροπή του αναλογικού σήματος σε ψηφιακό. Αναλόγως την τοποθεσία και την πυκνότητα των θορύβων που αντιλαμβάνεται ένας αισθητήρας, χρησιμοποιούνται κάποια φίλτρα για να είναι καλύτερα διαχειρίσιμη η πληροφορία και ποιο καθαρή. Κάποια από τα πιο συνηθισμένα φίλτρα που εφαρμόζονται είναι η αφαίρεση του θορύβου στο εύρος 50 ή 60 Hz λόγο των καλωδίων του ρεύματος. Τέλος το ψηφιακό σήμα πλέον είναι διαθέσιμο για επεξεργασία, αποθήκευση ή απεικόνιση για καλύτερη κατανόηση των δεδομένων.



Εικόνα 23. Συλλογή δεδομένων και ενεργοποίηση

Πηγή:https://www.researchgate.net/publication/261958666_Fundamentals_of_Wireless_Sensor_Networks_Theory_and_Practice

Ένας από τους κύριους λόγους που χρησιμοποιούμε ασύρματα δίκτυα αισθητήρων δεν είναι μόνο για να παρακολουθούμε τα δεδομένα απομακρυσμένα αλλά και για να μπορούμε να επέμβουμε απομακρυσμένα σε φυσικό επίπεδο. Αυτό επιτυγχάνεται με τη χρήση ενεργοποιητών, συσκευών δηλαδή που μετατρέπουν ένα σήμα εντολής σε μία αλλαγή που συνήθως είναι μηχανική όπως για παράδειγμα άνοιγμα ή κλείσιμο βαλβίδας ή διακόπτη. Η επιλογή του σωστού ενεργοποιητή παίζει σημαντικό ρόλο, καθώς θα πρέπει να γνωρίζουμε την τοποθεσία που θα εγκατασταθούν αλλά και τις συνθήκες που θα επικρατούν στο χώρο. Θα πρέπει, επίσης, να είναι συμβατός με την συσκευή που θα τον ελέγχει, ώστε να μπορούμε να τον διαχειριζόμαστε απομακρυσμένα. Υπάρχουν αρκετοί τύποι από ενεργοποιητές, ωστόσο, οι ποιο συνηθισμένοι είναι οι ηλεκτρικοί, υδραυλικοί και οι πνευματικοί ενεργοποιητές. [19]

Εικόνα 24. Τύποι ενεργοποιητών

Πηγή:https://learnmech.com/types-of-actuators-function-of-actuators-used-in-machines/

Η υλοποίηση ενός τέτοιο δικτύου ονομάζεται WSN και ενεργοποιητή (Wireless Sensor and Actuator Network – WSAN).

2.1.1 Κατηγοριοποίηση Αισθητήρων

Η επιλογή του αισθητήρα είναι το πιο σημαντικό κομμάτι σε ένα τόσο μεγάλο και πολύπλοκο δίκτυο. Οι παράγοντες που πρέπει να λάβουμε υπόψιν μας για μία τέτοια επιλογή είναι αμέτρητοι .Πριν ξεκινήσουμε, πρέπει να ξέρουμε τη φυσική ιδιότητα που θα παίρνουμε μετρήσεις. Κάποιες από τις ιδιότητες αυτές είναι η θερμοκρασία, η πίεση, το φως και η υγρασία. Στον πίνακα 1.1 παρακάτω υπάρχουν οι πιο συνηθισμένοι τύποι αισθητήρων και οι τρόποι με τους οποίους μπορούμε να τους μετρήσουμε. Οι αισθητήρες χωρίζονται σε 2 υποκατηγορίες, ενεργοί και παθητικοί αισθητήρες. Για να θεωρηθεί ένας αισθητήρας ενεργητικός θα πρέπει να χρησιμοποιεί ένα εξωτερικό τροφοδοτικό και επίσης θα πρέπει να εκπέμπει κάποιου είδους ενέργειας όπως ήχο, μικροκύματα, φως για να προξενήσει μία αντίδραση ή να ανιχνεύσει κάποια αλλαγή στην ενέργεια από το μεταδιδόμενο σήμα. Παθητικός αισθητήρας είναι αυτός ο οποίος ανιχνεύει την ενέργεια που υπάρχει στο περιβάλλον που βρίσκεται και αντλεί την

απαραίτητη ενέργεια για να λειτουργήσει από εκεί. Για παράδειγμα ένας αισθητήρας που δουλεύει με αυτήν την τεχνολογία είναι ο παθητικός αισθητήρας υπέρυθρων, ο οποίος μετρά το υπέρυθρο φως που ακτινοβολεί από αντικείμενα σε κοντινή απόσταση. [2]

Πίνακας 1. Τύποι και παραδείγματα αισθητήρων

Τύπος	Παραδείγματα
Θερμοκρασία	Θερμίστορ, θερμοστοιχείο
Πίεση	Πιεσόμετρο, Βαρόμετρο, Μετρητής ιονισμού
Οπτικός	Φωτοδίοδος, Φωτοτρανζίστορ, Αισθητήρας υπέρυθρων
Ακουστικός	Πιεζοηλεκτριστικό αντηχείο, Μικρόφωνα
Μηχανικός	Μηκυνσιόμετρο, Αισθητήρας αφής
Κινούμενος, Δονούμενος	Επιταχυνσιόμετρο, γυροσκόπιο
Ροή	Ανεμόμετρο, Αισθητήρας Μέτρηση μάζα αέρα
Τοποθεσία	GPS (Global Positioning System)
Ηλεκτρομαγνητικό	Μαγνητόμετρο, Αισθητήρας Χολ
Χημικό	Αισθητήρας pH/Ηλεκτροχημείας/Υπέρυθρων αερίων
Υγρασία	Υγρόμετρο, Χωρητικοί και Ωμικοί αισθητήρες
Ακτινοβολία	Αισθητήρας ιονισμού/Ιονίζουσας ακτινοβολίας

Πηγή:
https://www.researchgate.net/publication/261958666_Fundamentals_of_Wireless_Sensor_Networks_Theory_and_Practice

2.1.2 Περιβαλλοντικοί και Χημικοί Αισθητήρες

Οι περιβαλλοντικοί και χημικοί παίζουν πολύ σημαντικό ρόλο πλέον μιας και είμαστε σε συνεχή επαφή με το περιβάλλον και εξαρτόμαστε σε πολύ μεγάλο βαθμό από αυτό. Μπορούν να ανιχνευτούν στο φυσικό περιβάλλον παράμετροι όπως θερμοκρασία, υγρασία, πίεση, ρύπανση του νερού, ατμοσφαιρική ρύπανση και ποιότητα του αέρα. Οι χημικοί αισθητήρες επίσης βοηθούν στην ανίχνευση χημικών και βιοχημικών ουσιών που μπορεί να είναι επιβλαβείς για το περιβάλλον και τον άνθρωπο. Οι αισθητήρες αυτοί αποτελούνται από ένα σύστημα αναγνώρισης και έναν μορφοτροπέα (transducer) και παρέχουν τεχνολογίες όπως ηλεκτρονική μύτη (e-nose) και ηλεκτρονική γλώσσα (e-tongue). Με την βοήθεια αυτών των τεχνολογιών γίνεται η ανίχνευση των χημικών ουσιών με βάση την οσμή και την γεύση, διότι αποτελούνται από μία μεγάλη συστοιχία αισθητήρων και λογισμικό αναγνώρισης μοτίβων. Πλέον που έχουμε εξελιχθεί σαν ανθρωπότητα και ζούμε σε μεγάλες πόλεις, μπορούμε να εγκαταστήσουμε αισθητήρες ώστε να ζούμε πλέον με την βοήθεια του IoT σε έξυπνες πόλεις. Με αυτό τον τρόπο μπορούμε να παρακολουθούμε τα επίπεδα ρύπανσης, να γίνεται έλεγχος ποιότητας σε τρόφιμα, να έχουμε έξυπνα σπίτια, να έχουμε καλύτερα αποτελέσματα στην γεωργία και

σε εφοδιαστικές αλυσίδες. Παρακάτω στην φωτογραφία μπορούμε να δούμε έναν έξυπνο αισθητήρα νερού που μπορεί να παρέχει πολύτιμες πληροφορίες για το νερό. Υπάρχουν αντίστοιχα και άλλοι σύγχρονοι αισθητήρες για υλοποιήσεις όπως, έξυπνες πόλεις, έξυπνη ασφάλεια, έξυπνο παρκάρισμα, έλεγχος ακτινοβολίας, έξυπνη μέτρηση ηλεκτρισμού, έξυπνοι γεωργία και τέλος έξυπνο περιβάλλον. [20]

Εικόνα 25. Έξυπνος αισθητήρας νερού

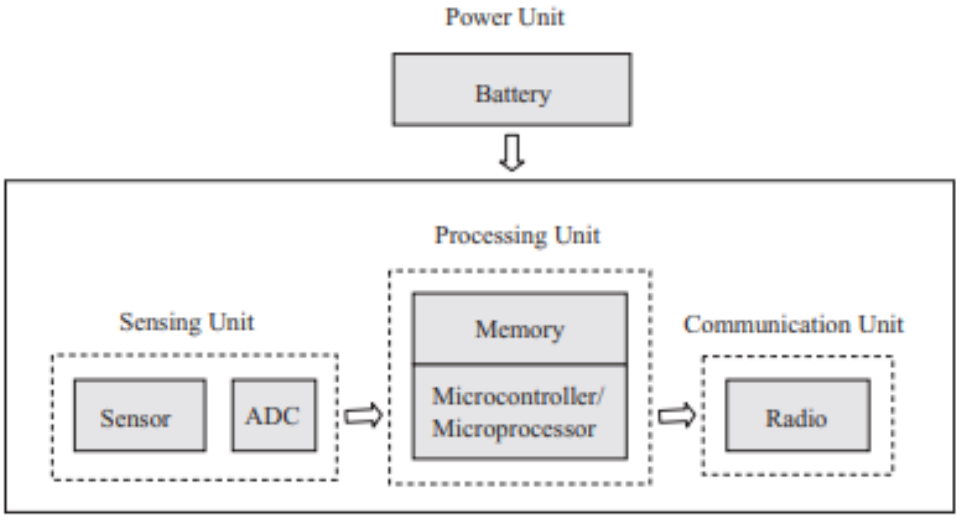
Πηγή:https://www.save9.com/internet-and-wireless-networks/wireless-sensor-networks/

2.1.3 Δομή Κόμβου Αισθητήρα

Η δομή ενός κόμβου αισθητήρα σε ένα WSN συνήθως αποτελείται από τέσσερα βασικά εξαρτήματα, μία μονάδα ισχύος, μία μονάδα ανίχνευσης, μία μονάδα επεξεργασίας και τέλος μία μονάδα επικοινωνίας [21].

- **Μονάδα Ανίχνευσης:** Σε μία μονάδα ανίχνευσης υπάρχουν τουλάχιστον ένας ή περισσότεροι αισθητήρες και μετατροπείς αναλογικού σήματος σε ψηφιακό (Analog-Digital-Converter ADC). Η δουλειά των αισθητήρων είναι να παρακολουθούν το φυσικό φαινόμενο και να παράγουν αντίστοιχα αναλογικά σήματα. Στην συνέχεια οι μετατροπείς παίρνουν το αναλογικό σήμα και το μετατρέπουν σε ψηφιακό ώστε να είναι έτοιμο να μεταφερθεί στην μονάδα επεξεργασίας.

- **Μονάδα Επεξεργασίας:** Στην μονάδα επεξεργασίας συνήθως υπάρχει ένας μικροελεγκτής ή μικροεπεξεργαστής με μικρή μνήμη ώστε να υπάρχει ευφυής έλεγχος στον κόμβο αισθητήρα.
- **Μονάδα Επικοινωνίας:** Η μονάδα επικοινωνίας αποτελείται από μία μικρή κεραία ραδιοσυχνοτήτων για να μπορεί να γίνει μετάδοση και λήψη δεμένων.
- **Μονάδα Ισχύος:** Για να μπορεί να λειτουργήσει όλο το σύστημα χρειάζεται μία μονάδα ισχύος όπως μία μπαταρία για να δίνει ενέργεια στα εξαρτήματα. Μερικές φορές ανάλογα με την εφαρμογή και τι δεδομένα πρέπει να συλλεχθούν. Για παράδειγμα σε μερικές εφαρμογές για να λειτουργήσει σωστά το δίκτυο και τα πρωτόκολλα μπορεί να χρειάζονται την ακριβή τοποθεσία με την βοήθεια ενός παγκόσμιου συστήματος εντοπισμού θέσης (GPS). Οτιδήποτε μπορεί να χρειαστεί το σύστημα θα πρέπει να μπορεί να ενσωματωθεί σε πολύ μικρή μονάδα, να παρέχεται πολύ μικρή κατανάλωση ενέργειας και να έχει όσο το δυνατόν χαμηλότερο κόστος παραγωγής. Στα WSN ανάλογα την περιοχή που πρέπει να καλυφθεί το κόστος ανεβαίνει κατακόρυφα οπότε θα πρέπει να σχεδιαστεί κατάλληλα για την κάθε εφαρμογή.



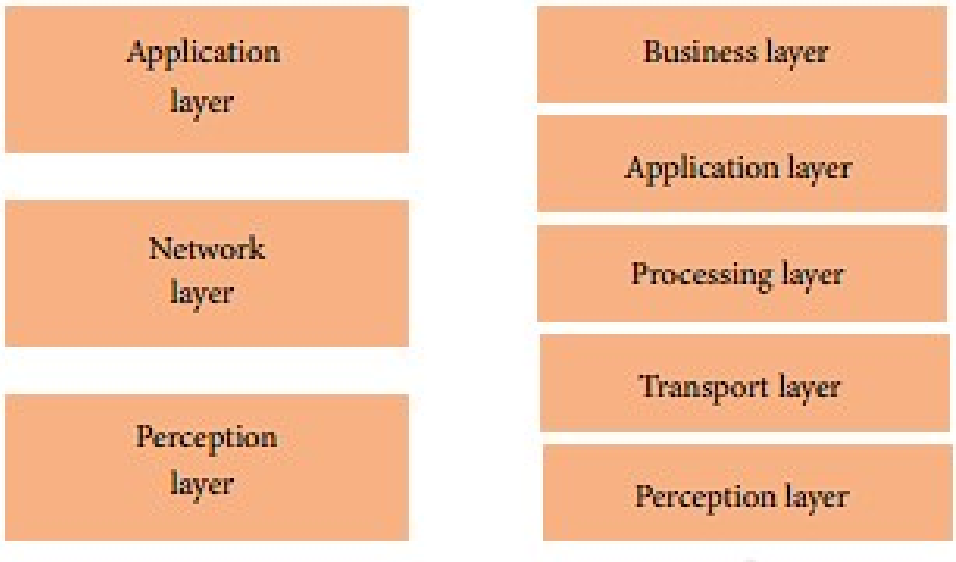
Εικόνα 26. Δομή κόμβου αισθητήρα

Πηγή:https://worldcat.org/title/1127206856

2.2 IoT Αρχιτεκτονική

Στο IoT δεν υπάρχει κάποια συγκεκριμένη αρχιτεκτονική που να ακολουθείται από όλη την παγκόσμια επιστημονική κοινότητα και τη βιομηχανία. Όταν το IoT ήταν ακόμη σε πρώιμο ερευνητικό στάδιο, προτάθηκε μία βασική αρχιτεκτονική με τρία επίπεδα, όμως μετά από καιρό έγινε αντιληπτό πως οι ανάγκες επανασχεδιασμού της αρχιτεκτονικής του IoT ήταν πολύ περισσότερες και έτσι προτάθηκαν μοντέλα αρχιτεκτονικής τριών,

τεσσάρων ή πέντε επιπέδων αντίστοιχα. Ωστόσο, το βασικό μοντέλο αρχιτεκτονικής IoT αποτελείται από τα επίπεδα αντίληψης, δικτύου και εφαρμογής.



Εικόνα 27. IoT Αρχιτεκτονική

Πηγή:https://www.hindawi.com/journals/jece/2017/9324035/

- **Επίπεδο Αντίληψης:** Το επίπεδο αντίληψης είναι στην ουσία το φυσικό επίπεδο όπου βρίσκονται οι αισθητήρες για ανίχνευση του περιβάλλοντος και την συλλογή πληροφοριών. Μπορεί να αντιληφθεί ορισμένες φυσικές παραμέτρους ή να εντοπίζει έξυπνα αντικείμενα στο περιβάλλον.
- **Επίπεδο Δικτύου:** Το επίπεδο δικτύου είναι υπεύθυνο για την σύνδεση μεταξύ έξυπνων πραγμάτων (smart things), συσκευές του δικτύου αλλά και διακομιστές. Επίσης βοηθάει στην μετάδοση και την επεξεργασία των δεδομένων από τους αισθητήρες.
- **Επίπεδο Εφαρμογής:** Στο επίπεδο εφαρμογής γίνεται η εξειδικευμένη παροχή υπηρεσιών εφαρμογής στον χρήστη. Επίσης καθορίζονται σε ποιες εφαρμογές μπορεί να γίνει η ανάπτυξη του IoT όπως έξυπνο σπίτι, έξυπνες πόλεις και έξυπνη υγεία.

Στο μοντέλο αρχιτεκτονικής IoT πέντε επιπέδων διακρίνουμε τα επίπεδα αντίληψης, μεταφοράς, επεξεργασίας, εφαρμογής, καθώς και το επιχειρησιακό επίπεδο. Ο ρόλος του επιπέδου αντίληψης και του επιπέδου εφαρμογής παραμένει ο ίδιος όπως και στο μοντέλο των τριών επιπέδων που αναφέρθηκε παραπάνω.

- **Επίπεδο Μεταφοράς:** Το επίπεδο μεταφοράς μεταφέρει τα δεδομένα που συλλέγουν οι αισθητήρες στο επίπεδο αντίληψης στο επίπεδο επεξεργασίας και αντίστροφα μέσω διάφορων δικτύων όπως ασύρματα, 3G/4G/5G, WLAN, Bluetooth, Radio Frequency Identification (RFID) και Near Field Communication (NFC).

- **Επίπεδο Επεξεργασίας:** Το επίπεδο επεξεργασίας θεωρείτε το ενδιάμεσο στρώμα διότι αποθηκεύει, αναλύει και επεξεργάζεται τεράστιες ποσότητες δεδομένων (Big Data) που μεταφέρονται από το επίπεδο μεταφοράς. Έχει αρκετές δυνατότητες ώστε να μπορεί να βοηθάει τα χαμηλότερα επίπεδα αλλά μπορεί επίσης και να χρησιμοποιεί τεχνολογίες όπως βάσεις δεδομένων, υπολογιστικό νέφος (cloud computing) και επεκτάσεις εφαρμογών όπως επεξεργασία μεγάλων δεδομένων.
- **Επίπεδο Επιχείρησης:** Το επιχειρησιακό επίπεδο είναι υπεύθυνο για την διαχείριση ολόκληρου του IoT συστήματος. Διαχειρίζεται δηλαδή τις εφαρμογές, τα επιχειρηματικά μοντέλα, το μοντέλο κέρδους (profit) αλλά και την ιδιωτικότητα των χρηστών.

2.2.1 Radio Frequency Identification (RFID)

Το RFID είναι μία τεχνολογία αναγνώρισης που με την βοήθεια ενός πολύ μικρού τσιπ και μιας κεραίας καταφέρνει να μεταδίδει δεδομένα μέσω ραδιοκυμάτων. Τα δεδομένα αυτά διαβάζονται μετά από ένα άλλο τσιπάκι RFID που κάνει την δουλειά της ανάγνωσης. Το τσιπάκι δεν χρειάζεται να έχει οπτική επαφή με το τσιπάκι αναγνώρισης και δεν χρειάζεται επίσης ανθρώπινο χειριστή μια και η επικοινωνία μπορεί να γίνει από αρκετή απόσταση. Το πόσο μεγάλη εμβέλεια θα έχει το RFID ποικίλλει ανάλογα με την συχνότητα που χρησιμοποιείται εκείνη την στιγμή και μπορεί να φτάσει μέχρι και κάποια εκατοντάδες μέτρα. Υπάρχουν δύο τύποι RFID τσιπ: ενεργής λειτουργίας και παθητικής λειτουργίας. Η διαφορά μεταξύ των δύο καταστάσεων είναι ότι στην ενεργή λειτουργία το τσιπ έχει πηγή ενέργειας ενώ στην παθητική δεν υπάρχει καμία πηγή ενέργειας. Τα τσιπ με παθητική λειτουργία για να λειτουργήσουν αντλούν ενέργεια από τα ηλεκτρομαγνητικά κύματα που εκπέμπονται από το τσιπ ανάγνωσης. Αυτό έχει ως αποτέλεσμα το κόστος αγοράς να είναι πολύ μικρό και η διάρκεια ζωής αρκετά μεγάλη.

Οι τεχνολογίες που χρησιμοποιεί το RFID χωρίζονται επίσης σε δύο τύπους και είναι η κοντινή τεχνολογία και η μακρινή. Για την κοντινή λειτουργεία το RFID τσιπ αναγνώρισης χρησιμοποιεί ένα πηνίο του οποίου περνάει από μέσα του εναλλασσόμενο ρεύμα έτσι ώστε να δημιουργηθεί ένα μαγνητικό πεδίο. Η τάση στην συνέχεια συνδέεται με έναν πυκνωτή για να συσσωρευτή το φορτίο ώστε να τροφοδοτηθεί το τσιπ με ενέργεια. Το τσιπ παράγει ένα μικρό μαγνητικό πεδίο που κωδικοποιεί το σήμα που θα μεταδοθεί έτσι ώστε να μπορεί να το αντιληφθεί το τσιπ ανάγνωσης. Στην τεχνολογία μακρινής λειτουργίας το RFID τσιπ ανάγνωσης διαθέτει μία διπολική κεραία για να διαδίδει ηλεκτρομαγνητικά κύματα. Το τσιπ έχει επίσης και αυτό μία διπολική κεραία για να μπορεί να αναγνωρίσει την διαφορά δυναμικού και να τροφοδοτείται με ενέργεια για να μεταδώσει με την σειρά του μηνύματα. Η τεχνολογία RFID είναι χρήσιμη σε πάρα πολλές εφαρμογές όπως η διαχείριση εφοδιαστικής αλυσίδας, έλεγχος πρόσβασης, για λόγους ταυτοποίησης ταυτότητας αλλά και για εντοπισμό αντικειμένων.

2.3 Πρωτόκολλα WSN και IoT

2.3.1 Πρωτόκολλο Near Field Communication (NFC)

Το NFC είναι μία τεχνολογία ασύρματης επικοινωνίας με πάρα πολύ μικρή εμβέλεια και χρησιμοποιείτε συνήθως από συσκευές κινητών για να αλληλοεπιδράσουν μεταξύ τους. Μπορεί να γίνει μεταφορά όλων τον τύπων δεδομένων αρκεί οι συσκευές να είναι πάρα πολύ κοντά η μία στην άλλη και να έχουν ενεργοποιημένη την NFC δυνατότητα. Το NFC βασίζεται πάνω στην τεχνολογία RFID που ανιχνεύει και χρησιμοποιεί τις μεταβολές του μαγνητικού πεδίου για να γίνει η αποστολή δεδομένων, χρησιμοποιώντας μία ζώνη συχνοτήτων 13,56 MHz.

Υπάρχουν δύο τρόποι λειτουργίας ο ενεργητικός και ο παθητικός. Στην ενεργητική λειτουργεία και οι δύο συσκευές παράγουν μαγνητικά πεδία ενώ, στην παθητική λειτουργεία μόνο η μία συσκευή παράγει το μαγνητικό πεδίο ενώ η άλλη συσκευή χρησιμοποιεί διαμόρφωση φορτίου ώστε να μεταφέρει δεδομένα. Η παθητική λειτουργεία είναι πιο ευρέως χρήσιμη διότι είναι πολύ χρήσιμη για συσκευές που λειτουργούν με μπαταρίες οπότε βοηθάει στην λιγότερη κατανάλωση ενέργειας. Το NFC θεωρείται αρκετά ασφαλές διότι οι συσκευές πρέπει η μία να ακουμπάει την άλλη, με αποτέλεσμα να είναι μία καλή λύση για ασφαλείς πληρωμές με κινητό. Μία βασική διαφορά του NFC με το RFID είναι ότι το NFC μπορεί να χρησιμοποιηθεί για αμφίδρομη μεταφορά δεδομένων ενώ το RFID όχι.

2.3.2 Πρωτόκολλο Low Power Wi-Fi

Το WiFi χαμηλής ισχύος, ή αλλιώς WiFi HaLow [20] βασίζεται στο πρότυπο IEEE 802.11ah και έχει την δυνατότητα να καταναλώνει λιγότερη ενέργεια αλλά ταυτόχρονα να έχει και μεγαλύτερη εμβέλεια από το παραδοσιακό WiFi. Δημιουργήθηκε με βάση τις ανάγκες των εφαρμογών IoT (Internet of Things) και WSN, και υποστηρίζεται επίσης επικοινωνία με διεύθυνση IP. Το πρότυπο λειτουργεί σε συχνότητες κάνω του ενός Gigahertz (GHz) δηλαδή στα 900 Megahertz (MHz) που σημαίνει ότι επειδή η συχνότητα είναι χαμηλότερη σε σχέση με άλλα πρωτόκολλα και πρότυπα η εμβέλεια του είναι διπλάσια από το παραδοσιακό WiFi. Τα κύματα υψηλής συχνότητας υποφέρουν από υψηλή εξασθένηση (attenuation) και η εμβέλεια φτάνει μέχρι και το ένα χιλιόμετρο. Μπορεί να παραμετροποιηθεί η συχνότητα και να μειωθεί ώστε να αυξηθεί η εμβέλεια αλλά το αρνητικό είναι πως μειώνεται ο ρυθμός μετάδοσης των δεδομένων.

2.3.3 Πρωτόκολλο Long Range Radio (LoRa)

Το LoRa [22] δημιουργήθηκε το 2015 και είναι μία ψηφιακή τεχνολογία ασύρματης επικοινωνίας δεδομένων με μεγάλο φάσμα που χρησιμοποιεί ραδιοφωνικό φάσμα διαμόρφωσης σήματος. Είναι σχεδιασμένη με την τεχνολογία Chirp Spread Spectrum (CSS) και χρησιμοποιεί την ελεύθερη ζώνη ραδιοσυχνοτήτων 169 MHz, 433 MHz, 868

MHz στην Ευρώπη ενώ στης Ηνωμένες Πολιτείες Αμερικής (ΗΠΑ) χρησιμοποιεί τα 915 MHz. Το πρωτόκολλο χωρίζεται σε δύο σκέλη, το πρώτο σκέλος που είναι το φυσικό επίπεδο όπου εκεί παρουσιάζονται οι συσκευές και τα ανώτερα στρώματα που παρουσιάζονται ως μεγάλης εμβέλειας δίκτυα ευρείας περιοχής Long Range Wide Area Network (LoRaWAN). Είναι ιδανικό γιατί παρέχει με χαμηλό κόστος αμφίδρομη κινητή επικοινωνία σε IoT και σε συσκευές με ανάγκη για μεγάλη ρυθμαπόδοση (throughput) όπως machine-to-machine (M2M).

Ο τρόπος επικοινωνίας τους γίνεται συνήθως με την χρήση 3G, καλωδίου ethernet (τοπικό δίκτυο), Wi-Fi ή κυψελωτές τεχνολογίες (cellular technologies). Ένα από τα πλεονεκτήματα του πρωτοκόλλου είναι ότι είναι εύκολα επεκτάσιμο σε μεγάλο αριθμό κόμβων και το πόσο καλά μπορεί να προσαρμοστεί στις παρεμβολές και τον θόρυβο.

Ένα παράδειγμα εφαρμογής που θα μπορούσε να χρησιμοποιήσει το πρωτόκολλο αυτό είναι ένας υγροβιότοπος. Με τη βοήθεια αισθητήρων που θα παρακολουθούν το περιβάλλον σε πραγματικό χρόνο θα παρέχονται δεδομένα όπως η θερμοκρασία του νερού, το pH, την αγωγιμότητα, το πόσο θολό είναι το νερό, το επίπεδο νερού ακόμη και πόσο διαλυμένο οξυγόνο υπάρχει. Το μέγεθος των δεδομένων δεν θα πρέπει να ξεπερνάει μερικά kbps διότι η αποστάσεις είναι αρκετά μεγάλες που πρέπει να μεταφερθούν τα δεδομένα, (έως 3 χιλιόμετρα).

2.3.4 Πρωτόκολλο Low Power Wide Area Networks (LPWAN)

Το πρωτόκολλο LPWAN χρησιμοποιείται για μεγάλης εμβέλειας δίκτυα που οι ανάγκες των συσκευών είναι να λειτουργούν χαμηλή ισχύ. Το πρωτόκολλο διαθέτει αρκετές τεχνολογίες επικοινωνίας χαμηλού ρυθμού ιδανικά για εφαρμογές με IoT, και μερικές από αυτές είναι:

- **Narrow band IoT:** Η τεχνολογία αυτή έχει δημιουργηθεί για να μπορεί να ανταπεξέλθει σε ένα μεγάλο αριθμό συσκευών που έχουν περιορισμούς ενέργειας, και αυτό πετυχαίνετε με την μείωση του ρυθμού μετάδοσης των δεδομένων. Η ταχύτητες που μπορεί να υποστηρίξει είναι κυμαίνονται μεταξύ των σαράντα kbps και τα δέκα Mbps και μπορούν να χρησιμοποιηθούν δίκτυα όπως το Global System for Mobile Communications (GSM) και Long-Term Evolution (LTE), ή αλλιώς 4G Advanced.
- **Sigfox:** Η τεχνολογία αυτή χρησιμοποιείται σε συχνότητες κάτω των δέκα MHz και χρησιμοποιεί τμήματα του ραδιοφάσματος ISM band ώστε να μπορεί να μεταδίδει δεδομένα. Η εμβέλεια του Sigfox μπορεί να φτάσει άνετα τα δέκα χιλιόμετρα σε αστικές περιοχές και τα σαράντα χιλιόμετρα σε αγροτικές περιοχές που είναι πιο αραιοκατοικημένες. Το μήνυμα για να μπορεί να σταλεί τόσο μακριά είναι μόνο δώδεκα bytes και κάθε συσκευή μπορεί να μεταδώσει 140 μηνύματα ημερησίως. Μπορεί να χρησιμοποιεί σε υποβρύχιες εφαρμογές, γεωεντοπισμό, παρακολούθηση απομακρυσμένων τοποθεσιών αλλά και σε ιατρικές εφαρμογές. [23]

- **Weightless:** Η τεχνολογία Weightless μία μέθοδο διαφορικής δυαδικής μετατόπισης φάσεως ώστε να μεταδίδει σήματα σε πολύ χαμηλές συχνότητες. Επειδή όμως υπάρχει πρόβλημα με παρεμβολές, για να τις αποφύγει χρησιμοποιεί μεταπήδηση μεταξύ συχνοτήτων αντί για το πρωτόκολλο CSMA. Για περεταίρω αποφυγή συγκρούσεων χρησιμοποιεί το πρωτόκολλο TDMA αλλά και πολλαπλά υποκανάλια που κατανέμονται σε κόμβους αποστολής δεδομένων αφού πρώτα επικοινωνήσουν με κάποιον κεντρικό διακομιστή. Εφαρμογές που χρησιμοποιούν αυτήν την τεχνική είναι έξυπνοι μετρητές, παρακολούθηση οχημάτων, παρακολούθηση υγείας, και παρακολούθηση βιομηχανικών μηχανημάτων.
- **Neul:** Το Neul λειτουργεί στην ζώνη κάτω του ενός GHz και χρησιμοποιεί τμήμα του φάσματος αχρησιμοποίητων συχνοτήτων της ψηφιακής τηλεόρασης. Αυτό γίνεται με σκοπό την δημιουργία δικτύων χαμηλού κόστους και χαμηλής ισχύος που υποστηρίζουν μεγάλη επεκτασιμότητα. Η εμβέλεια που υποστηρίζει είναι τα δέκα χιλιόμετρα και χρησιμοποιεί την τεχνική weightless για την επικοινωνία. [20]

2.4 Διαφορές Ανάμεσα σε IoT και WSN

Υπάρχουν κάποιες βασικές διαφορές μεταξύ του IoT και του WSN όπως ότι συνήθως τα WSN χρησιμοποιούνται για την παρακολούθηση του περιβάλλοντος αλλά και την συλλογή πληροφοριών φυσικών ή περιβαλλοντικών συνθηκών. Στην περίπτωση του IoT η τεχνολογία αυτή συνδέει το υλικό (hardware) με το διαδίκτυο έτσι ώστε να μπορεί να γίνεται η επικοινωνία με άλλες συσκευές και να μοιράζονται δεδομένα.

Οι εφαρμογές WSN για να δημιουργηθούν πρέπει πρώτα να μελετηθούν λεπτομερώς και κάθε εγκατάσταση είναι μοναδική διότι οι συνθήκες που επικρατούν είναι μοναδικές και για μία συγκεκριμένη ανάγκη. Αντίθετα στο IoT μπορεί να δημιουργηθεί κάτι πιο γενικό και αρκετά ευέλικτο ώστε να μπορούν περισσότεροι άνθρωποι να το χρησιμοποιήσουν. Επίσης σε δύσκολές ή επικίνδυνες καταστάσεις σχεδόν πάντα επιλέγονται να χρησιμοποιούν WSN ειδικά για σκοπούς παρακολούθησης, ενώ το IoT χρησιμοποιείται περισσότερο για σύνδεση πολλαπλών συσκευών και αντικειμένων που χρησιμοποιούν οι άνθρωποι στην καθημερινότητα τους.

Το IoT βασίζεται σε βιομηχανικά πρότυπα και πρωτόκολλα όπως το Transmission Control Protocol (TCP) και IP ενώ τα WSN χρησιμοποιούν περισσότερο ιδιόκτητες τεχνολογίες και πρωτόκολλα. Επιπροσθέτως στο IoT συνήθως συνδέονται μικρός αριθμός συσκευών στο διαδίκτυο είτε ενσύρματα είτε ασύρματα. Στο WSN οι εφαρμογές απαιτούν μεγάλο αριθμό από αισθητήρες χαμηλών δυνατοτήτων που να μεταφέρουν ασύρματα τα δεδομένα σε κάποιον κεντρικό σταθμό βάσης.

Μία μεγάλη και σημαντική διαφορά είναι ότι το IoT είναι πολύ πιο δυναμικό από το WSN διότι οι συσκευές έχουν την δυνατότητα να μετακινούνται και να συνδέονται σε πολλαπλά δίκτυα. Στην περίπτωση των WSN οι υλοποιήσεις που δημιουργούνται είναι

συνήθως στατικές με τους αισθητήρες να τοποθετούνται σε μία συγκεκριμένη τοποθεσία και να παραμένουν σε αυτήν. Η ανάπτυξη τεχνολογιών για τα WSN αναπτύσσονται από έναν μόνο οργανισμό ενώ στο IoT ασχολούνται πολλαπλοί οργανισμοί.

Ο τύπος των εφαρμογών και των δεδομένων που μπορεί να συλλέγονται στα WSN μπορεί να είναι ιδιωτικά και να μην μπορούν να μοιραστούν με άλλους οργανισμούς η άτομα. Το IoT από την άλλη είναι πιο ανοικτό τέτοια θέματα οπότε μπορεί και να αναπτύσσεται γρηγορότερα αφού μπορούν να μοιράζονται πληροφορίες μεταξύ τους οι οργανισμοί. Τέλος η αγορά του τομέα IoT είναι πιο ανεπτυγμένη από αυτήν των WSN που ακόμα βρίσκεται υπό ανάπτυξη. [24]

2.5 Ασφάλεια σε Ασύρματα Δίκτυα Αισθητήρων

Η ασφάλεια σε όλα τα δίκτυα είτε ασύρματα είτε ενσύρματα είναι ένας αρκετά δύσκολος τομέας και πολύ γρήγορα εξελισσόμενος, και από την πλευρά του επιτιθέμενου αλλά και από την πλευρά του αμυνόμενου. Όπως η ασφάλεια έτσι και η ιδιωτικότητα είναι τεράστιες προκλήσεις στα ασύρματα δίκτυα αισθητήρων εξαιτίας των ιδιαίτερων χαρακτηριστικών που έχουν αυτά τα δίκτυα. Μεγάλο ρόλο παίζουν και οι εφαρμογές των δικτύων αυτών μιας και συνήθως είναι κριτικής σημασίας όπως επιτήρηση πεδίου μάχης, εντοπισμός στόχων, παρακολούθηση υποδομών όπως γέφυρες και σήραγγες, σε νοσοκομεία για παρακολούθηση ασθενών αλλά και στην φύση για παρακολούθηση της χλωρίδας και πανίδας.

Τέτοιου είδους εφαρμογές γίνονται αρκετά ελκυστικές για επιτήδειους εγκληματίες που θα προσπαθήσουν να παραβιάσουν την ασφάλεια του δικτύου με αποτέλεσμα την παραβίαση πληροφοριών, διακοπή λειτουργίας της εφαρμογής, παραμετροποίηση της σωστής συμπεριφοράς της εφαρμογής, αλλά επίσης και η προσθήκη ψεύτικων πληροφοριών για παραπλάνηση.

Τα ασύρματα δίκτυα αισθητήρων συχνά βρίσκονται σε κάποιο απομακρυσμένο χώρο, σε εχθρικό φυσικό περιβάλλον με λίγους πόρους και συνήθως μικρή έως μηδαμινή ασφάλεια με αποτέλεσμα να είναι ευάλωτα σε παραβιάσεις ασφάλειας. Αυτό καθιστά αρκετά δύσκολο το κομμάτι της ασφάλειας γιατί γίνεται αρκετά δύσκολη η διάκριση των απειλών από μία απλή βλάβη ενός κόμβου αισθητήρα. Συνεπώς, η ασφάλεια ασύρματων δικτύων αισθητήρων είναι ένα αρκετά δύσκολο και πολύπλοκο εγχείρημα και θα πρέπει να προσαρμοστεί στις ανάγκες και τους περιορισμούς των δικτύων αυτών. [2]

2.6 Εφαρμογές στο IoT

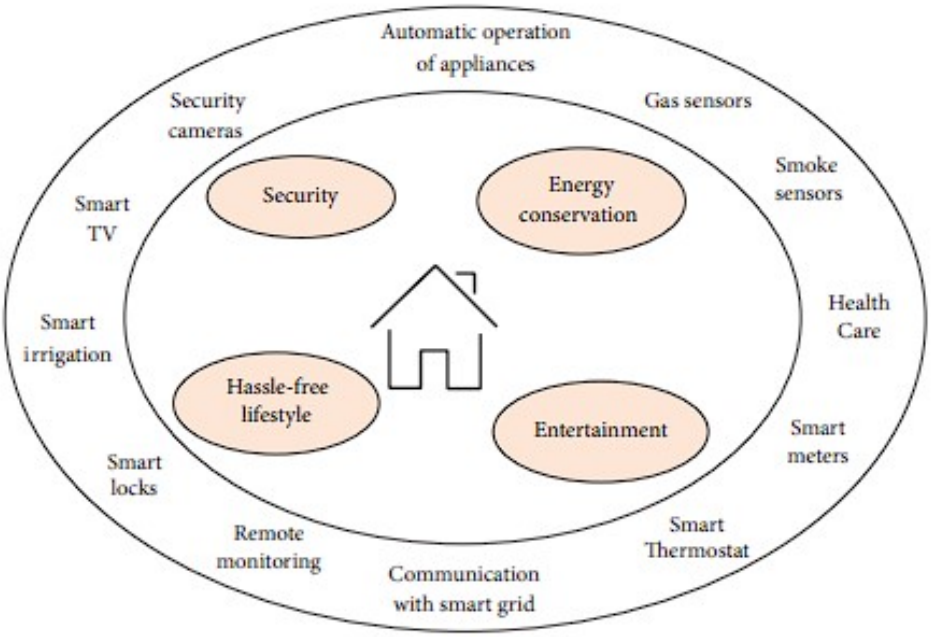
Το IoT είναι πάρα πολύ χρήσιμο και υπάρχουν εφαρμογές σε ποικίλους τομείς βελτιώνοντας την ποιότητα ζωής στην κοινωνία [20]. Κάποιες από τις εφαρμογές είναι:

- **Οικιακός Αυτοματισμός:** Ο οικιακός αυτοματισμός και τα έξυπνα σπίτια την σήμερον ημέρα γίνεται όλο και πιο δημοφιλή. Οι τεχνολογίες των IoT και των WSN έχουν ωριμάσει αρκετά και είναι κοινός αποδεκτές από τους χρήστες ώστε να τις εμπιστευτούν και να βελτιώσουν την ποιότητα ζωής. Στα έξυπνα σπίτια μπορούν να αναπτυχθούν διάφοροι αισθητήρες που με τις μετρήσεις που θα κάνουν μπορούν να παρέχουν έξυπνες και αυτοματοποιημένες υπηρεσίες στον χρήστη. Οι αυτοματισμοί μπορούν να μας κάνουν την ζωή πολύ εύκολη με τρόπους όπως, εγκατάσταση αισθητήρων κίνησης σε ένα δωμάτιο που να ανοίγει το φως με το που αισθάνονται κίνηση εξοικονομώντας ρεύμα. Επίσης, μπορεί να χρησιμοποιηθούν και για λόγους ασφάλειας σε κάποια έξυπνη κάμερα. Πλέον σε αρκετές χώρες είναι αναγκαστικό τα σπίτια να έχουν έξυπνους αυτόματους αισθητήρες για καπνό, για διοξείδιο του άνθρακα, για φυσικό αέριο ή ακόμα και για προπάνιο, με σκοπό να ανακαλυφθεί κάποια διαρροή. Για συγκεκριμένες ηλικιακές ομάδες και για άτομα με ειδικές ανάγκες υπάρχουν εφαρμογές για να μπορούν να παρακολουθούν την υγεία των ατόμων αυτών και να μπορούν να επέμβουν αν υπάρχει κάποια ιατρική ανάγκη ή να καλέσουν βοήθεια σε περίπτωση ανάγκης. Στις οικιακές IoT εφαρμογές όμως υπάρχουν και πολλές προκλήσεις που πρέπει να αντιμετωπιστούν όπως, η ασφάλεια και η ιδιωτικότητα καθώς οι αισθητήρες λειτουργούν συνέχεια. Είναι λοιπόν πολύ σημαντικό να υπάρχει πολύ μεγάλη ασφάλεια και να μην μπορεί κάποιος εισβολέας να χρησιμοποιήσει τις πληροφορίες αυτές κακόβουλα. Μπορεί να χρησιμοποιηθεί και τεχνολογία τεχνητής νοημοσύνης (artificial intelligence) μαζί με αλγόριθμους μηχανικής μάθησης (machine learning) ώστε να εντοπίζονται ανωμαλίες στα δεδομένα του χρήστη σε σχέση με ιστορικό του. Επειδή δεν υπάρχει κάποιος διαχειριστής του εκάστοτε συστήματος για να παρακολουθεί το σύστημα η αξιοπιστία των δεδομένων παίζει πολύ μεγάλο ρόλο.
- **Έξυπνες Πόλεις:** Σε μία έξυπνη πόλη υπάρχουν πληθώρα εφαρμογών που μπορούν να υλοποιηθούν και μία από αυτές είναι οι έξυπνες μεταφορές. Με την βοήθεια υλοποιήσεων όπως οι έξυπνες μεταφορές, σε μία πόλη μπορούν να χρησιμοποιηθούν αισθητήρες και έξυπνα συστήματα επεξεργασίας πληροφοριών για να γίνεται καλύτερη διαχείριση της κυκλοφορίας. Αυτό θα έχει σαν αποτέλεσμα να υπάρχει λιγότερο κυκλοφοριακή συμφόρηση, εύκολη εύρεση στάθμευσης, αποφυγή ατυχημάτων με σωστή δρομολόγηση της εκάστοτε κυκλοφορίας ανάλογα με τις ανάγκες, αλλά και τον εντοπισμό μεθυσμένων οδηγών. Για να επιτευχθεί αυτό χρειάζονται αισθητήρες όπως GPS για την τοποθεσία, επιταχυνσιόμετρα για την ταχύτητα, γυροσκόπια για την κατεύθυνση, RFID για αναγνώριση των οχημάτων, υπέρυθρες για την καταμέτρηση επιβατών και οχημάτων, αλλά και κάμερες για την επίβλεψη της κίνησης και της κυκλοφορίας. Πιθανές εφαρμογές που μπορούν να υλοποιηθούν με την χρήση των αισθητήρων αυτών είναι: παρακολούθηση και διαχείριση της κυκλοφορίας, διασφάλιση της ασφάλειας, ευφυής διαχείριση χώρων στάθμευσης, έξυπνοι φωτεινοί σηματοδότες και εφαρμογή ανίχνευσης ατυχημάτων.

- **Κοινωνική ζωή και ψυχαγωγία:** Η κοινωνική ζωή και η ψυχαγωγία παίζουν πολύ σημαντικό ρόλο στις ζωές μας και έχουν αναπτυχθεί αρκετές εφαρμογές που παρακολουθούν τις δραστηριότητες αυτές. Χρησιμοποιώντας προσωπικές συσκευές όπως, tablet, wearables και κινητά τηλέφωνα χρησιμοποιούν τεχνολογίες ανίχνευσης και επικοινωνία μικρής εμβέλειας για να επικοινωνούν με άλλες συσκευές. Ένα παράδειγμα είναι η εφαρμογή ψυχαγωγίας Logmusic η οποία λαμβάνει πληροφορίες όπως, ο καιρός, η θερμοκρασία, η ώρα και η τοποθεσία με την βοήθεια του κινητού για να προτείνει μουσική στην χρήστη.
- **Υγεία και φυσική κατάσταση:** Ο τομέας της υγείας και ευεξίας είναι αρκετά σημαντικός και με την βοήθεια των εφαρμογών IoT, δεν άργησε να μπει στις ζωές μας. Αναπτύχθηκαν πάρα πολλές φορητές συσκευές για την παρακολούθηση της υγείας ενός ατόμου, ή σε ειδικές περιπτώσεις όπως οι ηλικιωμένοι και άτομα με σοβαρές παθήσεις πλέον μπορούν να ζουν ανεξάρτητα την ζωή τους. Με την χρήση λοιπόν αισθητήρων και την συνεχή παρακολούθηση του ατόμου καταγράφονται πληροφορίες για τις συνθήκες υγείας του, και μπορούν να ειδοποιήσουν τον χρήστη εάν διαπιστώσουν οι αισθητήρες κάτι μη φυσιολογικό.
- **Έξυπνο περιβάλλον και γεωργία:** Η γεωργία είναι ένα αρκετά σύνθετο επάγγελμα και απαιτεί πολύ χρόνο και χειρωνακτική εργασία. Με την βοήθεια αισθητήρων που θα παρακολουθούν παραμέτρους όπως θερμοκρασία και υγρασία, μπορούν να έχουν δεδομένα που θα τους βοηθήσουν να έχουν μία αποτελεσματικότερη παραγωγή. Ένα παράδειγμα IoT εφαρμογής θα μπορούσε να είναι ότι ανάλογα με τις καιρικές συνθήκες μπορεί να αυτοματοποιηθεί η άρδευση. Βέβαια τα τελευταία χρόνια όλο και περισσότεροι γεωργοί δημιουργούν θερμοκήπια οπότε η χρήση λύσεων IoT είναι μονόδρομος. Για να είναι καλύτερη η σοδιά μπορούν να χρησιμοποιηθούν αισθητήρες όπως, η θερμοκρασία, η υγρασία και διάφορες πληροφορίες του χώματος όπου θα παίρνουν δεδομένα σε πραγματικό χρόνο και ύστερα θα αναλύονται για την βελτίωση της ποιότητας. Με την χρήση ενός βιοαισθητήρα μπορούν να ανιχνευτούν τα υπολείμματα φυτοφαρμάκων στην παραγωγή καλλιεργειών. Ύστερα τα δεδομένα αυτά μπορούν να αποθηκευτούν και να αναλυθούν ώστε να βγουν χρήσιμα συμπεράσματα, όπως το μέγεθος του δείγματος, ο χρόνος, η τοποθεσία και η ποσότητα των υπολειμμάτων αυτών, ώστε να διατηρηθεί η ποιότητα της καλλιέργειας.
- **Έξυπνο σύστημα υδροδότησης:** Το πρόβλημα της λειψυδρίας χρόνο με τον χρόνο μεγαλώνει σε αρκετά σημεία ανά τον κόσμο και θα πρέπει να διαχειριζόμαστε τους υδάτινους πόρους με πιο αποτελεσματικό τρόπο. Αρκετές πόλεις εγκαθιστούν μετρητές σε παροχές νερού και σε φρεάτια με σκοπό την μέτρηση της εισροής και εκροής νερού αλλά και τον εντοπισμό πιθανών διαρροών. Επίσης οι έξυπνοι μετρητές σε συνδυασμό με μετεωρολογικά δεδομένα και αισθητήρες σε νερά

ποταμών μπορούν να μας βοηθήσουν να προβλέψουμε πιθανόν πλημμύρες που μπορεί να υπάρξουν.

- **Αλυσίδα εφοδιασμού και logistics:** Οι αλυσίδες εφοδιασμού και τα logistics είναι ένας τομέας πολύ πολύπλοκος που μπορεί όμως να αυτοματοποιηθεί αρκετά. Με την βοήθεια του IoT τα προϊόντα μπορούν να παρακολουθούνται εύκολα από την αρχή της διαδικασίας κατασκευής τους, μέχρι και τον τελικό τόπο διανομής τους, χρησιμοποιώντας αισθητήρες και τεχνολογίες όπως το RFID και το NFC. Οι πληροφορίες καταγράφονται σε πραγματικό χρόνο και αποθηκεύονται για περεταίρω παρακολούθηση. Επίσης πληροφορίες σχετικά με το προϊόν και την χρηστικότητα του μπορούν να αποθηκευτούν σε μία ετικέτα RFID που θα συνοδεύει την αποστολή του πακέτου. Είναι αρκετά σημαντικό να υπάρχει αυτή η τεχνική διότι οι ετικέτες αυτές στην ουσία ταυτοποιούν μοναδικά ένα προϊόν με αυτόματο τρόπο δημιουργώντας έτσι ένα δίκτυο πληροφοριών. Το δίκτυο με την σειρά του μεταδίδει τις πληροφορίες αυτές σε πραγματικό χρόνο μαζί με τις πληροφορίες τοποθεσίας. Έτσι με αυτό τον τρόπο υπάρχουν δεδομένα για τα πάντα οπότε, μπορεί να γίνει ανάλυση της παρελθοντικής ζήτησης για να γίνει πρόβλεψη της μελλοντικής.
- **Εξοικονόμηση ενέργειας:** Με τη χρήση της ηλεκτρικής ενέργειας έχουμε κάνει τις ζωές μας καλύτερες και έχουμε πλέον περισσότερες ανέσεις. Το έξυπνο δίκτυο παρέχει πληροφορίες και τεχνολογίες επικοινωνιών έτσι ώστε να υπάρχει ένα σύγχρονο σύστημα παραγωγής, μεταφοράς, διανομής και κατανάλωσης ηλεκτρικής ενέργειας. Προσθέτοντας σε κάθε βήμα της αλυσίδας αυτής έξυπνες λύσεις και νοημοσύνη μπορεί να γίνει αμφίδρομη ροή της ενέργειας από τον καταναλωτή στον προμηθευτή. Για να μπορεί να υπάρξει ένα έξυπνο δίκτυο θα πρέπει πρώτα να υπάρχουν αισθητήρες παντού και να κατανεμηθεί το δίκτυο σε μικροδίκτυα (microgrids). Το μικροδίκτυα μπορούν να παράγουν ενέργεια για τις ανάγκες μιας τοπικής περιοχής και αν χρειάζεται να ζητήσουν παραπάνω από το κεντρικό δίκτυο, ή αν έχουν πλεονάζουσα ενέργεια να την μεταδίδουν πίσω στο κεντρικό δίκτυο. Όταν υπάρχει αμφίδρομη ροή της ενέργειας επωφελούνται χρήστες που παράγουν την δικιά τους ενέργεια με τρόπους όπως, ηλιακή ή αιολική ενέργεια. Την ενέργεια που δεν χρησιμοποιούν μπορούν να την μεταφέρουν πίσω και να πληρωθούν από αυτήν. Παραδείγματα IoT εφαρμογών σε ένα τέτοιο δίκτυο είναι οι εξής, παρακολούθηση γραμμών που μεταφέρουν ηλεκτρική ενέργεια για πρόληψη καταστροφών και αποτελεσματική χρήση ηλεκτρικής ενέργειας σε σπίτια με εγκατάσταση έξυπνου μετρητή ώστε να παρακολουθείται η κατανάλωση ενέργειας.



Εικόνα 28. IoT Εφαρμογές

Πηγή:https://www.hindawi.com/journals/jece/2017/9324035

2.7 Απαιτήσεις Ασφάλειας WSN και IoT

Οι απαιτήσεις ασφάλειας μπορούν να χωριστούν σε δύο κατηγορίες απαιτήσεων, την κύρια κατηγορία απαιτήσεων και την δευτερεύουσα κατηγορία απαιτήσεων.

2.7.1 Κύρια Κατηγορία Απαιτήσεων Ασφάλειας

- **Εμπιστευτικότητα Δεδομένων:** Στα ασύρματα δίκτυα αισθητήρων είναι βασικό να υπάρχει η ικανότητα της διασφάλισης ότι τα απόρρητα και ευαίσθητα δεδομένα που συλλέγονται δεν θα βρεθούν στα χέρια επιτήδειου εγκληματία. Τα δεδομένα πρέπει να παραμένουν εμπιστευτικά και αυτό μπορεί να γίνει με την χρήση κρυπτογράφησης δεδομένων με χρήση μυστικού κλειδιού όταν συλλέγονται τα δεδομένα. Με αυτό τον τρόπο οι πληροφορίες γίνονται αντιληπτές μόνο από τους επιθυμητούς παραλήπτες και δέκτες.
- **Αυθεντικοποίηση Δεδομένων Πηγής:** Υπάρχουν διάφορες επιθέσεις που μπορούν να παριστάνουν ότι είναι ένας κόμβος αισθητήρων που συλλέγει δεδομένα αλλά αντί για αυτό να στέλνει ψευδή δεδομένα και να έχει μεγάλο αντίκτυπο στα συμπεράσματα που θα βγουν από τα δεδομένα. Θα πρέπει λοιπόν να υπάρχει η διασφάλιση της αξιοπιστίας των δεδομένων που συλλέγονται και μεταδίδονται στο δίκτυο και να υπάρχει επαλήθευση της πηγής και της προέλευσης των δεδομένων. Σαν αποτέλεσμα αυτής της τεχνικής είναι ότι ένας κακόβουλος χρήστης δεν θα μπορεί να έχει τα κατάλληλα πιστοποιητικά, ώστε να προσποιηθεί ότι είναι ένας αξιόπιστος κόμβος.

- **Ακεραιότητα δεδομένων:** Η ακεραιότητα των δεδομένων παίζει πολύ σημαντικό ρόλο για την αξιοπιστία του δικτύου και θα πρέπει να διασφαλίζεται και να επιβεβαιώνονται τα δεδομένα που συλλέγονται, ότι δεν έχουν αλλοιωθεί ποτέ, τροποποιηθεί ή αλλοιωθεί από κακόβουλους χρήστες η κακόβουλους ενδιάμεσους χρήστες που παριστάνουν κόμβους. Επίσης, λόγω του δύσκολου περιβάλλοντος που υπάρχει συνήθως σε τέτοια δίκτυα, μπορεί να υπάρξει δυσκολία στην επικοινωνία για οποιονδήποτε λόγο, όπως η κακοκαιρία.
- **Διαθεσιμότητα:** Πρέπει να διασφαλιστεί ότι το ίδιο το δίκτυο σαν σύνολο είναι διαθέσιμο και μπορεί να παρέχει τις υπηρεσίες επικοινωνίας όπου πρέπει, όπως επίσης και ότι ο κάθε κόμβος θα μπορεί να έχει στην διάθεση του πόρους του δικτύου. Αυτό θα πρέπει να ισχύει και στην περίπτωση που υπάρχει κάποια επίθεση άρνησης παροχής υπηρεσιών (Denial of Service DoS).

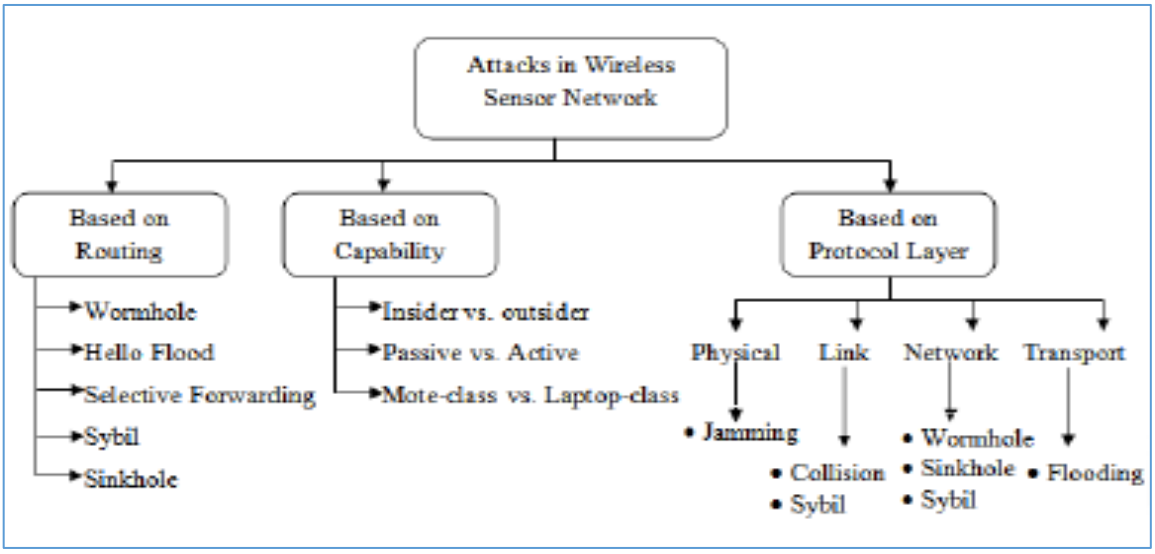
2.7.2 Δευτερεύουσα Κατηγορία Απαιτήσεων Ασφάλειας

- **Πρωτοτυπία Δεδομένων:** Πρωτοτυπία δεδομένων ή αλλιώς data freshness προστατεύει το δίκτυο από επιθέσεις αναπαραγωγής δεδομένων. Με την τεχνική αυτή εξασφαλίζεται ότι τα παλιά μηνύματα δεν θα αναπαραχθούν ξανά, οπότε ότι δεδομένα μεταδίδονται είναι πάντα καινούργια και “τα πρωτότυπα”. Αυτό κατορθώνεται με την προσθήκη ενός μετρητή χρόνου στο πακέτο που μεταδίδεται.
- **Αυτο-οργάνωση:** Η φύση ενός ασύρματου δικτύου αισθητήρων είναι τέτοια που δεν υπάρχει σταθερή υποδομή, όπως ένα κτήριο σε μία πόλη. Αυτό έχει σαν αποτέλεσμα κάθε κόμβος αισθητήρων να είναι ανεξάρτητος και ευέλικτος, έτσι ώστε να μπορεί να αυτό-οργανώνεται σε διαφορετικές καταστάσεις και συνθήκες.
- **Συγχρονισμός ώρας:** Όπως η ασφάλεια έτσι και η κατανάλωση ενέργειας είναι μεγάλη πρόκληση σε ασύρματα δίκτυα αισθητήρων. Για να μειωθεί η κατανάλωση ενέργειας μπορεί ο αισθητήρας να απενεργοποιηθεί περιοδικά όταν δεν χρειάζεται. Με αυτό τον τρόπο όμως εκτός από μικρότερη κατανάλωση ενέργειας αυξάνεται και η ασφάλεια, γιατί αφού απενεργοποιηθεί ο αισθητήρας δεν μπορεί να έχει κάποιος πρόσβαση σε αυτόν για να επιχειρήσει κάποια επίθεση.
- **Ασφαλής εντοπισμός:** Τα ασύρματα δίκτυα αισθητήρων έχουν έναν μηχανισμό ασφάλειας που βασίζεται στην ικανότητα του δικτύου να εντοπίζει με ακρίβεια και με αυτόματο τρόπο όλους τους αισθητήρες του δικτύου. Αυτό πρέπει να γίνεται με αποτελεσματικό τρόπο γιατί κάποιος επιτιθέμενος που έχει την δυνατότητα να στείλει ψευδή δεδομένα έντασης σήματος ή να αναπαράγουν σήματα σε τοποθεσίες που δεν είναι ασφαλής. [25]

- **Ανθεκτικότητα:** Για να μπορεί να θεωρηθεί ένα ασύρματο δίκτυο αισθητήρων ανθεκτικό θα πρέπει πρώτα να είναι αρκετά ευέλικτο και να έχει ισχυρή προσαρμοστικότητα. Επειδή αυτά τα δίκτυα λόγω του περιβάλλοντος που βρίσκονται, η τοπολογία συνήθως αλλάζει συνέχεια είναι ιδιαίτερα δυναμικά. Το πρόβλημα που θα κληθεί να αντιμετωπίσει ο χρήστης είναι όταν το δίκτυο βρίσκεται σε κατάσταση επίθεσης η οποία επιτυγχάνει κιόλας σε ένα βαθμό, θα πρέπει να έχει προσαρμοστικότητα το δίκτυο. Με αποτέλεσμα να μπορεί να αμυνθεί και να μην έχει αντίκτυπο στην απόδοση του δικτύου ή τουλάχιστον να ελαχιστοποιηθεί η ζημιά.
- **Έλεγχος πρόσβασης χρήστη:** Ένα επιπλέον μέτρο ασφάλειας που υπάρχει είναι ο έλεγχος πρόσβασης των χρηστών που θα έχουν πρόσβαση στο δίκτυο, ώστε να διασφαλιστεί η ιδιότητα τους και η νομιμότητα τους. Με αυτό τον τρόπο έχουμε πλήρη έλεγχο ποιος έχει πρόσβαση στο δίκτυο, σε ποιους πόρους του συστήματος αλλά και με ποιον τρόπο γίνεται η χρήση των πόρων αυτών. [26]

2.8 Ταξινόμηση των Απειλών στα Ασύρματα Δίκτυα Αισθητήρων

Όσο η τεχνολογία προχωράει και η γνώση γίνεται πιο εύκολα προσβάσιμη εμφανίζονται όλο και περισσότερα άτομα που τις γνώσεις τους θα τις χρησιμοποιήσουν για αθέμιτους σκοπούς. Οι επιθέσεις που μπορεί να γίνουν σε ένα ασύρματο δίκτυο αισθητήρων είναι πάρα πολλές και έχουν δυνατότητες όπως, επίθεση στην μετάδοση σήματος, να προσθέσουν επιπλέον πληροφορίες στο μέσο επικοινωνίας, να αναπαράγουν παλιά πακέτα και άλλα πολλά. Οι απειλές ταξινομούνται συνήθως σε τρεις κατηγορίες, με βάση τις ικανότητες, με βάση την δρομολόγηση και με βάση το επίπεδο στην στοίβα πρωτοκόλλου. [27]



Εικόνα 29. Κατηγοριοποίηση Επιθέσεων σε WSN

Πηγή:https://ieeexplore.ieee.org/abstract/document/7784988

2.8.1 Κατηγορίες Επιθέσεων με βάση την ικανότητα

Οι κατηγορίες επιθέσεων που είναι αρκετά αποτελεσματικές σε ασύρματα δίκτυα αισθητήρων είναι τρεις με βάση την ικανότητα [26]:

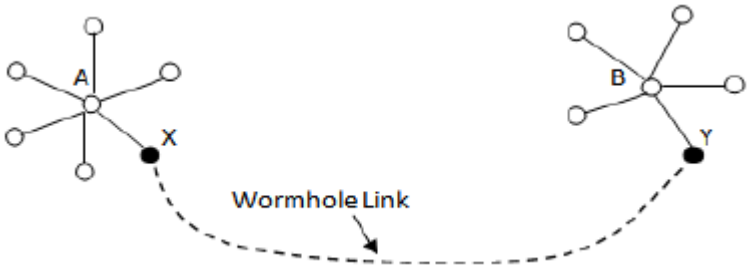
1) **Εκ των έσω Vs Εξωτερικές Επιθέσεις:** Οι επιθέσεις εκ των έσω είναι οι επιθέσεις που γίνονται από κάποιον παράγοντα που έχει επίγνωση του δικτύου και το πώς λειτουργεί. Από την άλλη, οι εξωτερικές επιθέσεις είναι επιθέσεις που γίνονται από άγνωστους εξωτερικούς παράγοντες που δεν έχουν καμία επίγνωση για την λειτουργεία του δικτύου και θα πρέπει να μαζέψουν πληροφορίες με διάφορες επιθέσεις. Οι εξωτερικές επιθέσεις μπορούν να εισχωρήσουν μέχρι και από τα δεδομένα "σκουπίδια" και να δημιουργήσουν μέχρι και επιθέσεις άρνησης παροχής υπηρεσιών με σκοπό την διακοπή των υπηρεσιών του δικτύου. Οι εσωτερικές επιθέσεις προσπαθούν να διακόψουν τις διαδικασίες που εκτελεί το δίκτυο η να εκμεταλλευτούν πόρους του συστήματος χωρίς συνήθως να γίνουν αντιληπτές ότι υπάρχουν.
2) **Παθητικές Vs Ενεργές επιθέσεις:** Οι παθητικές επιθέσεις είναι αρκετά δύσκολες στην ανίχνευση και πολύ ύπουλες, διότι δεν τροποποιούν καμία πληροφορία κατά την διάρκεια της ανταλλαγής πληροφοριών. Η διαφορά της παθητικής με την ενεργή επίθεση είναι ότι ο επιτιθέμενος έχει πρόσβαση και δυνατότητα, ώστε να μπορεί να αφαιρέσει ή να τροποποιήσει τελείως τα μηνύματα τη στιγμή που μεταδίδονται.
3) **Επιθέσεις κατηγορίας Mote Vs Φορητού υπολογιστή:** Στην επίθεση κατηγορίας Mote ο επιτιθέμενος επιτίθεται σε κόμβους που έχουν περίπου ίδιες δυνατότητες με έναν κανονικό κόμβο στο δίκτυο. Επίσης, συνήθως υπάρχει ένα κλειδί ή κωδικός που λειτουργεί σαν μέσο κρυπτογραφίας και οι επιτιθέμενοι θα πρέπει να έχουν πρόσβαση σε τουλάχιστον έναν εξουσιοδοτημένο κόμβο στο δίκτυο, ώστε να κλέψουν τον κωδικό ή το κλειδί. Όταν υπάρχει κρυπτογραφία στο δίκτυο, οι πληροφορίες είναι άχρηστες όταν δεν έχουμε κάποιο μέσο για να τις αποκρυπτογραφήσουμε. Συνήθως σε τέτοιες περιπτώσεις η επίθεση μοιάζει και σαν επίθεση εκ των έσω. Στην κατηγορία επίθεσης με φορητό υπολογιστή ο επιτιθέμενος δεν έχει πρόσβαση στο δίκτυο αλλά οι επιθέσεις μπορούν να γίνουν πιο αποτελεσματικές. Με την χρήση του φορητού υπολογιστή έχει στην διάθεση του πόρους του ίδιου του υπολογιστή που είναι πολύ πιο γρήγοροι. Με την χρήση μίας εξωτερικής κεραίας και τους πόρους του φορητού υπολογιστή μπορεί να προκαλέσει μεγαλύτερη ζημιά στα κοντινά δίκτυα μειώνοντας έτσι την αξιοπιστία του δικτύου.

2.8.2 Κατηγορίες Επιθέσεων με βάση την δρομολόγηση

Πρωτόκολλα δρομολόγησης υπάρχουν αρκετά για τα ασύρματα δίκτυα αισθητήρων και ανάλογα το πρωτόκολλο ο επιτιθέμενος μπορεί να αξιοποιήσει πολλαπλές επιθέσεις έτσι

ώστε να κλέψει ή να τροποποιήσει πληροφορίες. Κάποιες από τις επιθέσεις που ανήκουν σε αυτήν την κατηγορία είναι:

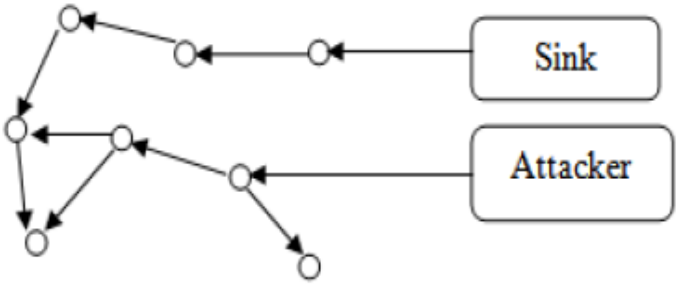
- **Επίθεση Wormhole:** Στην επίθεση Wormhole υπάρχουν τουλάχιστον δύο ή περισσότεροι μολυσμένοι κόμβοι σε διαφορετικές τοποθεσίες, ώστε να υπάρχει μεγάλη απόσταση μεταξύ τους. Οι δύο μολυσμένοι κόμβοι μπορεί να έχουν μεγάλη απόσταση μεταξύ τους αλλά είναι άμεσα συνδεδεμένοι μεταξύ τους, ώστε να μπορούν να ανταλλάζουν πληροφορίες. Όταν ο κόμβος αποστολέας στέλνει δεδομένα, τότε ο μολυσμένος κόμβος θα μεταφέρει τις πληροφορίες στον άλλο μολυσμένο κόμβο και αυτός με την σειρά του μοιράζει της πληροφορίες στους γειτονικούς κόμβους. Με την τεχνική αυτή πείθουν τους κόμβους αποστολέα και παραλήπτη ότι βρίσκονται πιο κοντά ο ένας στον άλλον από ότι πραγματικά βρίσκονται. Η κανονική απόσταση μεταξύ τον κόμβων μπορεί να είναι multiple hops μακριά αλλά με την επίθεση αυτή θεωρούν ότι βρίσκονται σε απόσταση ένα η δύο αλμάτων. Η επίθεση Wormhole συνήθως συνδυάζεται με την επίθεση selective forwarding και την επίθεση Sybil και τότε γίνεται πολύ δύσκολη η ανίχνευση τους στο δίκτυο.



Εικόνα 30. Wormhole Attack

Πηγή:https://ieeexplore.ieee.org/abstract/document/7784988

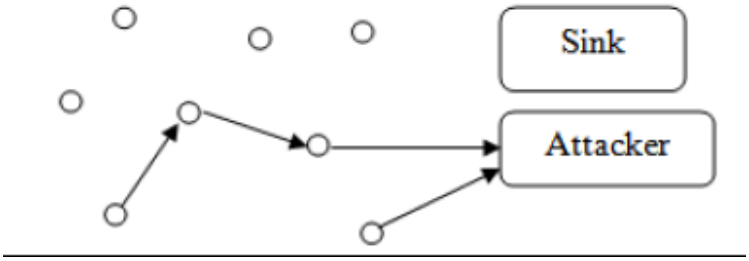
- **Επίθεση πλημμύρας HELLO:** : Όπως και στα δίκτυα γενικότερα έτσι και στα δίκτυα αισθητήρων για την πραγματοποίηση της ανακάλυψης γειτονικών κόμβων, μεταδίδονται πακέτα HELLO. Ο τρόπος με τον οποίο η επίθεση λειτουργεί είναι ότι ο κόμβος δέκτης θεωρεί ότι ο κόμβος πηγή βρίσκεται σε εμβέλεια μετάδοσης δεδομένων και στέλνει τα δεδομένα που έχει ανιχνεύσει στον κόμβο. Ο επιτιθέμενος μεταδίδει το μήνυμα HELLO από έναν μολυσμένο κόμβο με πολύ υψηλή ισχύ μετάδοσης έτσι ώστε οι κόμβοι που θα το λάβουν να αναγκαστούν να στείλουν μήνυμα HELLO πίσω στον μολυσμένο κόμβο. Ο επιτιθέμενος έχει την ευχέρεια να μπορεί να αλλάξει, να τροποποιήσει το πακέτο ή ακόμα και να το απορρίψει. Η επίθεση αυτή έχει σαν αποτέλεσμα να γίνεται πολύ μεγάλη σπατάλη ενέργειας αλλά και να πλημμυρίζει το δίκτυο με άχρηστα δεδομένα που προκαλούν συμφόρηση. Στην παρακάτω φωτογραφία το μήνυμα HELLO μεταδίδεται με μεγαλύτερη ισχύ από το Sink.



Εικόνα 31. Hello Flood Attack

Πηγή:https://ieeexplore.ieee.org/abstract/document/7784988

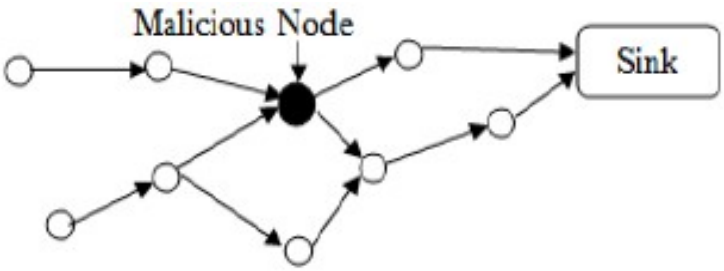
Στην παρακάτω περίπτωση οι κόμβοι εξαπατώνται θεωρώντας ότι το μήνυμα HELLO έρχεται από γειτονικό κόμβο.



Εικόνα 32. Hello Flood Attack από γειτονικό κόμβο

Πηγή:https://ieeexplore.ieee.org/abstract/document/7784988

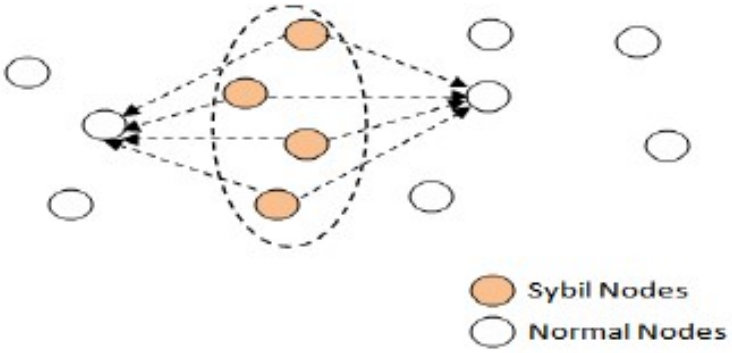
- **<u>Επίθεση επιλεκτικής προώθησης (Selective Forwarding Attack):</u>** Στην επίθεση της επιλεκτικής προώθησης ένας μολυσμένος κόμβος του δικτύου διακόπτει τελείως την επικοινωνία του με το δίκτυο. Ανάλογα το την περίπτωση μπορεί να υπάρχουν και περισσότεροι μολυσμένοι κόμβοι οι οποίοι δρουν με τον ίδιο τρόπο, δηλαδή προωθούν επιλεκτικά ορισμένα πακέτα από όλο τον όγκο δεδομένων που λαμβάνουν. Ο μολυσμένος κόμβος μπορεί να έχει και την ονομασία “μαύρη τρύπα” διότι μπορεί να απορρίψει όλα τα πακέτα που λαμβάνει. Το αποτέλεσμα αυτής της τακτικής είναι ότι οι γειτονικοί κόμβοι νομίζουν ότι αφού όλα τα δεδομένα που στέλνουν στον μολυσμένο κόμβο απορρίπτονται, τότε πιστεύουν ότι είναι ανενεργός και ψάχνουν για διαφορετική διαδρομή. Στην περίπτωση που ο μολυσμένος κόμβος ενεργεί σαν μαύρη τρύπα και απορρίπτει όλα τα πακέτα είναι αρκετά εύκολο να εντοπιστεί σαν επίθεση αλλά εάν προωθεί επιλεκτικά κάποια πακέτα τότε η εύρεση της επίθεσης γίνεται αρκετά δυσκολότερη. Οι επιθέσεις αυτές είναι πιο εύκολα να γίνουν όταν γίνονται εξωτερικά του δικτύου μέσω μία εξωτερικής διαδρομής στο δίκτυο. Η απόρριψη των πακέτων χωρίζεται σε δύο κατηγορίες, απορρίψεις πακέτων ορισμένων συγκεκριμένων κόμβων και απορρίψεις πακέτων ορισμένων συγκεκριμένων τύπων. Στην παρακάτω φωτογραφία απεικονίζεται η επίθεση όπου οι κόμβοι στέλνουν εν αγνοία τους δεδομένα στον μολυσμένο κόμβο.



Εικόνα 33. Selective Forwarding Attack

Πηγή:https://ieeexplore.ieee.org/abstract/document/7784988

- **Επίθεση Sybil:** Η επίθεση Sybil επιτίθεται με σκοπό την μείωση της αποτελεσματικότητας του δικτύου, στην ανοχή του δικτύου στα σφάλματα, αύξηση της σπατάλης ενέργειας. Οι επιθέσεις Sybil χρησιμοποιούνται εναντίον αλγορίθμων δρομολόγησης και τοπολογίας όπως επίσης και κατά του μηχανισμού πλεονασμού δεδομένων στα κατανεμημένα συστήματα. Ο τρόπος με τον οποίο λειτουργεί αυτή η επίθεση είναι ότι ένας επιτιθέμενος θα μολύνει έναν κόμβο και μετά θα έχει την δυνατότητα να δημιουργήσει πολλές και ψεύτικες ταυτότητες για αυτό τον κόμβο. Με αυτό τον τρόπο έχει την δυνατότητα να μπερδεύει τους κόμβους και να νομίζουν ότι ο μολυσμένος κόμβος βρίσκεται σε περισσότερα από ένα σημεία ταυτόχρονα. Αυτή η επίθεση είναι αρκετά αποτελεσματική σε πρωτόκολλα που βασίζονται στην τοποθεσία όπου πληροφορίες τοπολογίας ανταλλάζονται μεταξύ των κόμβων για αποτελεσματικότερη δρομολόγηση στο δίκτυο.

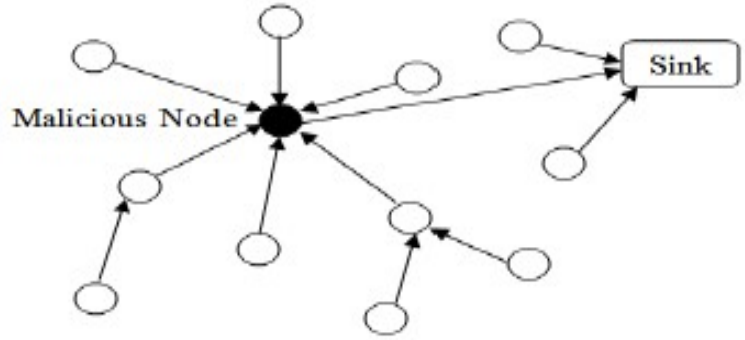


Εικόνα 34. Sybil Attack

Πηγή:https://ieeexplore.ieee.org/abstract/document/7784988

- **Επίθεση Sinkhole:** Ο επιτιθέμενος στην επίθεση sinkhole [27] έχει πρόσβαση σε έναν μολυσμένο κόμβο όπου διαφημίζει ψεύτικες πληροφορίες για την δρομολόγηση με σκοπό να αλλάξει η κυκλοφορία των δεδομένων στο δίκτυο. Όλα τα ασύρματα δίκτυα αισθητήρων είναι ευάλωτα σε αυτήν την επίθεση επειδή ο τρόπος επικοινωνίας των κόμβων σε έναν σταθμό βάσεις είναι του τύπου πολλοί προς έναν. Για να γίνει πιο

επικίνδυνη η επίθεση μπορεί να συνδυαστεί με την επίθεση Wormhole. Στην φωτογραφία παρακάτω βλέπουμε ένα παράδειγμα επίθεσης sinkhole όπου ο κακόβουλος κόμβος έχει πολύ μεγαλύτερη ισχύ από τους γειτονικούς κόμβους και συνδέεται με τον κόμβο sink χρησιμοποιώντας ένα μόνο άλμα. Εξαπατά τους γειτονικούς κόμβους ότι η δικιά του διαδρομή είναι η καλύτερη, έτσι ώστε να περνάει ολόκληρη η κυκλοφορία των γειτονικών κόμβων από αυτών. Αυτή η επίθεση δουλεύει τις περισσότερες φορές, διότι αρκετοί αλγόριθμοι δρομολόγησης έχουν σαν χαρακτηριστικό να επιλέγουν την συντομότερη διαδρομή για την μεταφορά δεδομένων.



Εικόνα 35. Sinkhole Attack

Πηγή:https://ieeexplore.ieee.org/abstract/document/7784988

2.8.3 Κατηγορίες Επιθέσεων με Βάση το Επίπεδο στην Στοίβα Πρωτοκόλλου

1. **Φυσικό Επίπεδο:** Το φυσικό επίπεδο χρησιμοποιείται για την μετάδοση πληροφοριών σε bits μέσω ασύρματου ή ενσύρματου μέσου. Είναι επίσης υπεύθυνο για την επιλογή συχνότητας, δημιουργία συχνότητας φορέα, την ανίχνευση και την διαμόρφωση του σήματος. Στα ασύρματα δίκτυα μία αρκετά εύκολη επίθεση είναι η παρεμβολή (jamming) ενός ραδιοφωνικού σήματος, αλλά υπάρχουν και άλλες επιθέσεις όπως υποκλοπή μέσω συνακρόασης (eavesdropping) και αλλοίωση (tampering)

   - Στην επίθεση υποκλοπής μέσω συνακρόασης (eavesdropping) [26] κάποιος μη εξουσιοδοτημένος χρήστης υποκλέπτει πληροφορίες. Η επίθεση υποκλοπής που αναφέρεται επίσης ως επίθεση sniffing ή snooping. Αυτού του είδους οι επιθέσεις είναι πιο επιτυχημένες επειδή δεν προκαλούν κανενός είδους ειδοποίηση κατά τη διάρκεια της μετάδοσης, επειδή εκμεταλλεύονται τις μη ασφαλείς επικοινωνίες δικτύου για πρόσβαση σε δεδομένα κατά την αποστολή ή τη λήψη τους από τον χρήστη. Αυτές οι επιθέσεις μπορεί να οδηγήσουν σε οικονομική απώλεια, κλοπή ταυτότητας ή απώλεια απορρήτου κ.λπ.
   - Η επίθεση με παρεμβολή (jamming) [27] παρεμποδίζει τους κόμβους του δικτύου από το να χρησιμοποιούν της ραδιοσυχνότητες. Με αυτό τον τρόπο ο

επιτιθέμενος δεν επιτρέπει την πρόσβαση στο πρωτόκολλο MAC, ειδικά αν στο δίκτυο χρησιμοποιείται μόνο μία συχνότητα για την μετάδοση δεδομένων σε όλο το δίκτυο. Επιπλέον, προκαλείται πολύ μεγάλη κατανάλωση ενέργειας, επειδή διοχετεύει στο δίκτυο άχρηστα πακέτα που οι κόμβοι-δέκτες θα συνεχίσουν να δέχονται.

- Η επίθεση αλλοίωσης (tampering) [28] οι κόμβοι είναι ευάλωτοι σε αλλοίωση δεδομένων αλλά και σε φυσική βλάβη αν κάποιος έχει πρόσβαση στην φυσικό περιοχή. Επίσης, μπορούν να εφαρμοστούν στο φυσικό επίπεδο επίθεσης, όπως η Sybil και σαν μέτρο ασφάλειας εναντίον αυτής της επίθεσης θα πρέπει να υπάρχει πολύ καλή φυσική ασφάλεια των συσκευών. Στην επίθεση παρεμβολής ως άμυνα θα πρέπει να χρησιμοποιηθεί η τεχνική εναλλαγής καναλιών συχνότητας και δημιουργία μαύρης λίστας για τους επιτιθέμενους. Με την επίθεση αλλοίωσης θα πρέπει να υπάρχει πολύ καλή προστασία του κλειδιού αλλά και συχνή αλλαγή του.

2. <u>Επίπεδο Ζεύξης Δεδομένων:</u> Το επίπεδο ζεύξης δεδομένων είναι υπεύθυνο για την ανίχνευση και διόρθωση σφαλμάτων στα δεδομένα, την κωδικοποίηση αυτών, την πολυπλεξία και την πρόληψη συγκρούσεων των πακέτων. Επίσης, θα πρέπει να ελέγχει αν γίνεται επαναλαμβανόμενη μετάδοση δεδομένων και για σχέσεις στο δίκτυο σημείο σε σημείο (point to point) και σημείο σε πολλαπλά σημεία (point to multipoint). Επιπλέον, χρησιμοποιείται για να εξασφαλιστεί η σωστή επικοινωνία στο φυσικό επίπεδο μεταξύ των κόμβων του δικτύου. [26] Το επίπεδο ζεύξης δεδομένων είναι ευάλωτο σε επιθέσεις, όπως επίθεση παρεμβολής και άρνησης παροχής υπηρεσιών (DoS) αλλά παίζει ρόλο και το πρωτόκολλο που θα χρησιμοποιείται. Πρωτόκολλα όπως το LMAC έχουν καλύτερες άμυνες εναντίον στης παρεμβολές και είναι μία καλή επιλογή για αυτό το επίπεδο. [28]
Ένας κακόβουλος χρήστης μπορεί να προκαλέσει μεγάλη ζημιά στο δίκτυο στέλνοντας συνέχεια μηνύματα, ώστε να προκαλέσει συγκρούσεις, την ανάκριση αλλά και την επανάληψη των πακέτων που έχουν συγκρουστεί. Ως άμυνα μπορεί να χρησιμοποιηθούν τεχνικές, όπως ανίχνευση και διόρθωση σφαλμάτων, ώστε να μειωθούν οι συγκρούσεις. Βέβαια, προσθέτει επιπλέον επιβάρυνση στο δίκτυο με αποτέλεσμα να γίνεται μεγάλη κατανάλωση ενέργειας. Το επίπεδο αυτό κινδυνεύει από επίθεση άρνησης ύπνου όπου η επίθεση δεν αφήνει τους κόμβους του δικτύου να μπουν σε κατάσταση ύπνου. Η κατανάλωση ενέργειας είναι τεράστια και έτσι μειώνεται σε ολόκληρο το δίκτυο η διάρκεια ζωής. [27]

3. <u>Επίπεδο Δικτύου:</u> Το επίπεδο δικτύου είναι υπεύθυνο για σωστή και αποτελεσματική δρομολόγηση των δεδομένων στις συσκευές του δικτύου. Οι συσκευές αυτές σε ένα ασύρματο δίκτυο αισθητήρων μπορεί να είναι από κόμβο σε κόμβο, από κόμβο σε κόμβο sink, από κόμβο σε σταθμό βάσης και από κόμβο σε κόμβο επικεφαλής συστάδας και αντίστροφα. [26] Ο επιτιθέμενος στο επίπεδο

δικτύου έχει σκοπό να κερδίσει πρόσβαση στο μέσο με το οποίο γίνεται η κυκλοφορία δεδομένων στο δίκτυο ανάμεσα στην πηγή και τον προορισμό. Αυτό έχει σαν αποτέλεσμα τον έλεγχο της ροής των δεδομένων και της αποτελεσματικότητας ολόκληρου του δικτύου. Επιθέσεις που μπορούν να το καταφέρουν αυτό είναι η επίθεση Wormhole, η πλαστογράφηση, η επιλεκτική προώθηση και οι μαύρες τρύπες. [27]

Προβλήματα που μπορούν να εμφανιστούν από τέτοιες επιθέσεις είναι τα πακέτα να απορρίπτονται τελείως ή επιλεκτικά, το δίκτυο να πλημμυρίζει από μηνύματα broadcast, διάδοση ψευδών πληροφοριών για ύπαρξη κόμβων σε άλματα μακριά η ότι μερικοί κόμβοι δεν υπάρχουν καθόλου στο δίκτυο. Αν υπάρχουν το λιγότερο δύο μολυσμένοι κόμβοι μπορούν να δημιουργήσουν μία σήραγγα μεταξύ τους και να διοχετεύεται η κυκλοφορία του δικτύου μέσα από αυτήν στερώντας έτσι την κίνηση από άλλους κανονικούς κόμβους. Η ασφάλεια στο επίπεδο δικτύου εξαρτάται και από την θέση που έχουν οι κόμβοι στο δίκτυο αλλά και εάν υπάρχουν τεχνικές κρυπτογράφησης. [29]

4. **<u>Επίπεδο Μεταφοράς:</u>** Το επίπεδο μεταφοράς ευθύνεται για την διαχείριση των συνδέσεων από άκρο σε άκρο στο δίκτυο. Στο δίκτυο αισθητήρων συγκεκριμένα είναι υπεύθυνο για την επικοινωνία. Οι πιο συχνές επιθέσεις σε αυτό το επίπεδο είναι η επίθεση πλημμύρας και αποσυγχρονισμού. [26] [27]

   - Στην επίθεση πλημμύρας (flooding) ο επιτιθέμενος προσπαθεί να εξαντλήσει τους πόρους των κόμβων στέλνοντας πολύ μεγάλο αριθμό αιτημάτων για εγκαθίδρυση σύνδεσης, απασχολώντας τον κόμβο με άχρηστες πληροφορίες με αποτέλεσμα να αυξάνεται η κατανάλωση ενέργειας.
   - Στην επίθεση αποσυγχρονισμού (desynchronization) ο μολυσμένος κόμβος πλαστογραφεί πακέτα και τα στέλνει σε τουλάχιστον ένα από τα δύο άκρα της σύνδεσης με διαφορετική αριθμητική ακολουθία βομβαρδίζοντας έτσι την συσκευή με αιτήματα για αναμετάδοση πακέτων που χάθηκαν.

2.9 Γενικές επιθέσεις σε ασύρματα δίκτυα αισθητήρων

Μερικές κατηγορίες γενικών επιθέσεων σε ασύρματα δίκτυα αισθητήρων είναι οι εξής [29]:

- **Παθητική συλλογή πληροφοριών:** Ένας επιτιθέμενος με πολλούς πόρους μπορεί να συλλέγει πληροφορίες που δεν είναι κρυπτογραφημένες.
- **Υπονόμευση Κόμβων:** Η πρόσβαση σε έναν μολυσμένο κόμβο μπορεί πολλές φορές να δώσει στον επιτιθέμενο πληροφορίες για τον ίδιο τον κόμβο αλλά και για κλειδιά κρυπτογράφησης που θέτουν όλο το δίκτυο σε κίνδυνο.

- **Ανάλυση κυκλοφορίας:** Ακόμα και κρυπτογραφημένα να είναι τα δεδομένα που μεταφέρονται υπάρχει περίπτωση να μπορεί να γίνει ανάλυση των μοτίβων επικοινωνίας και των δραστηριοτήτων που εκτελούν οι αισθητήρες. Ως αποτέλεσμα κάποιος κακόβουλος χρήστης μπορεί να συλλέξει αρκετές πληροφορίες για ώστε να κάνει ζημιά στο δίκτυο.
- **Βρόχοι δρομολόγησης:** Η επίθεση αυτή επιτίθεται στις πληροφορίες που ανταλλάσσονται μεταξύ των κόμβων, όταν κατά την διάρκεια της επίθεσης δημιουργούνται ψευδή μηνύματα σφάλματος, επειδή τροποποιούνται και αναπαράγονται πίσω οι πληροφορίες δρομολόγησης, με αποτέλεσμα να αυξάνουν την καθυστέρηση ανάμεσα στους κόμβους και να δημιουργούν πρόβλημα σε όλο το δίκτυο.

2.10 Πρωτόκολλα Ασφάλειας

2.10.1 SPIN (Sensor Protocols for Information via Negotiation)

Το πρωτόκολλο SPIN διαφημίζει στο δίκτυο πακέτα μεταδεδομένων και μόνο ο κόμβος που ενδιαφέρεται για αυτά τα μεταδεδομένα απαντάει θετικά και ανταλλάσσεται η πληροφορία. Το SPIN για παραπάνω ασφάλεια χρησιμοποιεί δύο τεχνικές, την μTESLA (Timed Efficient Stream Loss-tolerant Authentication) και την τεχνική SNEP (Sensor Network Encryption Protocol). Στην τεχνική SNEP παρέχεται εμπιστευτικότητα, αυθεντικοποίηση και ακεραιότητα χρησιμοποιώντας κρυπτογράφηση. Για την αυθεντικοποίηση των δεδομένων χρησιμοποιείται ένα κωδικός αυθεντικοποίησης μηνύματος Message authentication code (MAC) το οποίο προσθέτει 8 bytes στο μέγεθος του μηνύματος. Για να υπάρχει μικρότερη επιβάρυνση στο δίκτυο η τεχνική SNEP χρησιμοποιεί έναν μετρητή που κάθε φορά που περνάει από κάποιον κόμβο η πληροφορία αυξάνεται. Με αυτό τον τρόπο μπορεί να έχει μία εικόνα για το πόσο καινούργια η παλιά είναι η πληροφορία. Στην τεχνική μTESLA χρησιμοποιούνται ψηφιακές υπογραφές για να πιστοποιηθούν αν τα δεδομένα είναι αυθεντικά. Ο κόμβος sink προσθέτει στο πακέτο τον κωδικό αυθεντικοποίησης του μηνύματος αφού έχει λάβει το πακέτο πρώτα με το μυστικό κλειδί έτσι ώστε να μπορεί να στείλει ένα αυθεντικοποιημένο πακέτο πίσω στην πηγή. Ο κόμβος-πηγή ελέγχει την αυθεντικότητα του πακέτου και επιβεβαιώνει ότι δεν αποκάλυψε τον κωδικό αυθεντικοποίησης στους γειτονικούς κόμβους, με αποτέλεσμα να είναι βέβαιος πως το πακέτο είναι το πρωτότυπο και δεν υπάρχουν αλλοιώσεις.

2.10.2 LEAP (Localized Encryption and Authentication Protocol)

Το LEAP είναι ένα πρωτόκολλο που χρησιμοποιεί ένα σύστημα ασφάλειας με βάση κλειδιά διαχείρισης που είναι βελτιστοποιημένο για ασύρματα δίκτυα αισθητήρων μεγάλης κλίμακας. Υποστηρίζει εργασίες στο εσωτερικό του δικτύου όπως η επεξεργασία

και η συγκέντρωση των δεδομένων διότι υπάρχει μείωση της κατανάλωσης με τον τρόπο αυτό. Για την ασφάλεια, την εμπιστευτικότητα αλλά και τον έλεγχο των δεδομένων του δικτύου το πρωτόκολλο έχει έναν μηχανισμό με πολλαπλά κλειδιά. Για κάθε κόμβο χρησιμοποιούνται τέσσερα κλειδιά, ατομικά, σε ζεύγος, κατά συστάδες και το ομαδικό κλειδί. Αυτά τα τέσσερα κλειδιά είναι συμμετρικά και χρησιμοποιούνται με ως εξής:

- **Ατομικό κλειδί:** Είναι το μοναδικό κλειδί το οποίο θα χρησιμοποιηθεί για την επικοινωνία μεταξύ κόμβου πηγής και κόμβου sink.
- **Κλειδί ζεύγος:** Το κλειδί ζεύγος μοιράζεται σε όλους τους κόμβους αισθητήρων του δικτύου.
- **Κλειδί Συστάδας:** Το κλειδί συστάδας χρησιμοποιείται όταν γίνεται η τοπική μετάδοση μηνυμάτων μεταξύ γειτονικών κόμβων.
- **Κλειδί ομάδας:** Κοινόχρηστο παγκόσμιο κλειδί που χρησιμοποιείται από όλους τους κόμβους του δικτύου.

Η χρήση των κλειδιών αυτών δεν είναι αποκλειστική από το πρωτόκολλο αλλά μπορούν να χρησιμοποιηθούν και από άλλα πρωτόκολλα που δεν έχουν μέτρα ασφάλειας έτσι ώστε να αυξηθεί η ασφάλεια του δικτύου. Το πρωτόκολλο LEAP είναι αρκετά αποτελεσματικό στην απώθηση επιθέσεων πλημύρας HELLO πακέτων, επιθέσεις Sybil και επιθέσεων Wormhole.

2.10.3 TinySec

Το πρωτόκολλο TinySec χρησιμοποιεί μία αρχιτεκτονική ασφάλειας ζεύξης δεδομένων σε ασύρματα δίκτυα αισθητήρων και είναι ένα αρκετά ελαφρύ πρωτόκολλο στην χρήση του. Υποστηρίζει τεχνικές όπως ακεραιότητα, εμπιστευτικότητα και αυθεντικοποίηση. Η εμπιστευτικότητα επιτυγχάνεται με την χρήση κρυπτογράφησης CBC (Cipher-Block Chaining) και κλοπή του κρυπτογραφικού αλγόριθμου. Η αυθεντικοποίηση γίνεται με την χρήση ενός CBC-MAC αλλά δεν χρησιμοποιούνται μετρητές κόμβων για το πόσο καινούργιο είναι ένα πακέτο. Υπάρχουν εξουσιοδοτημένοι αποστολείς και παραλήπτες στο δίκτυο που μοιράζονται ένα μυστικό κλειδί που ονομάζεται κωδικός αυθεντικοποίησης μηνύματος (MAC). Το πρωτόκολλο διαθέτει δύο διαφορετικές επιλογές ασφάλειας, την TinySec-AE για αυθεντικοποιημένα και κρυπτογραφημένα μηνύματα και την επιλογή TinySec-Auth για αυθεντικοποιημένα μηνύματα μόνο. Στην περίπτωση της επιλογής TinySec-AE τα επιπρόσθετα δεδομένα ενός πακέτου κρυπτογραφούνται και το πακέτο που λαμβάνεται πιστοποιείται με τον MAC. Στο TinySec-Auth κρυπτογραφείται ολόκληρο το πακέτο με έναν MAC, αλλά δεν κρυπτογραφούνται τα επιπλέον δεδομένα του πακέτου. Στο CBC για να μπορέσει να υπάρξει σημασιολογική ασφάλεια, χρησιμοποιείται ένα διάνυσμα αρχικοποίησης (Initialization Vector) IV, διότι τα περισσότερα μηνύματα είναι σχεδόν πανομοιότυπα με μικρές διαφορές μεταξύ τους. Οπότε το διάνυσμα αρχικοποίησης προσθέτει στην

κρυπτογράφηση την μικρή διαφορά που έχουν μεταξύ τους τα πακέτα και για να μπορεί να αποκρυπτογραφηθεί το μήνυμα θα πρέπει ο παραλήπτης να χρησιμοποιήσει και αυτός ένα διάνυσμα αρχικοποίησης. Τα διανύσματα αυτά δεν είναι κρυφά και περιλαμβάνονται στο ίδιο το πακέτο με τα κρυπτογραφημένα δεδομένα.

2.10.4 ZigBee

Το πρωτόκολλο ZigBee [27] μπορεί να θεωρηθεί ένα τυπικό πρωτόκολλο ασύρματης επικοινωνίας αλλά χρησιμοποιείται σε αρκετά σημαντικές εφαρμογές όπως η στρατιωτική ασφάλεια, ο οικιακός αυτοματισμός αλλά και στην παρακολούθηση του περιβάλλοντος. Το πρότυπο IEEE 802.15.4 χρησιμοποιείται στο ZigBee για την υποστήριξη της εμπιστευτικότητας και της ακεραιότητας των δεδομένων. Ο μηχανισμός ασφάλειας χρησιμοποιεί κλειδιά μήκους 128 bit όπου υπάρχει επίσης και ένα κέντρο εμπιστοσύνης που πιστοποιεί όλες τις συσκευές και τους κόμβους και τους επιτρέπει να μπουν στο δίκτυο εφόσον έχει γίνει η διανομή των κλειδιών. Το πρωτόκολλο έχει τρεις διαφορετικούς ρόλους στο δίκτυο:

- **Διαχειριστής εμπιστοσύνης:** Ο διαχειριστής πιστοποιεί τις συσκευές που ζητούν να ενταχθούν στο δίκτυο.
- **Διαχειριστής δικτύου**: Διαχειρίζεται τα κλειδιά του δικτύου και βοηθά στη διατήρηση και διανομή των κλειδιών δικτύου.
- **Διαχειριστής ρυθμίσεων:** Διαμορφώνει τις παραμέτρους του μηχανισμού ασφαλείας και παρέχει ασφάλεια από άκρο σε άκρο μεταξύ των συσκευών του δικτύου.

Το πρωτόκολλο επίσης υποστηρίζει δύο διαφορετικές λειτουργίες, την οικιακή λειτουργία και την εμπορική λειτουργία. Η διαφορά τους είναι ότι στην οικιακή λειτουργία δεν υπάρχουν κλειδιά ασφαλείας οπότε η ασφάλεια είναι μικρότερη ενώ στην εμπορική λειτουργία υποστηρίζει την υψηλότερη δυνατή ασφάλεια με την χρήση κλειδιών αλλά και μετρητή για καινούργια δεδομένα.

2.11 Τμηματοποίηση Δικτύου

Η τμηματοποίηση ενός δικτύου είναι μία πολύ καλή τεχνική που χρησιμοποιείται για την καλύτερη διαχείριση ενός δικτύου, αλλά κυρίως επειδή με την διαίρεση του δικτύου σε ομάδες, συστάδες ή τομείς μπορούμε να παρέχουμε διαφορετικά πράγματα σε κάθε ομάδα. Οι ανάγκες τις κάθε ομάδας μπορεί να είναι διαφορετικές οπότε θα πρέπει και η διαχείριση του φόρτου εργασίας να κατανέμετε δίκαια αλλά και να καλύπτονται και οι διαφορετικές ανάγκες ασφάλειας. Για την καλύτερη διαχείριση υπάρχουν πρωτόκολλα για να μπορούν να γίνονται αλλαγές στο δίκτυο πιο εύκολα, όπως προσθήκη ή αφαίρεση κόμβων από κάποια ομάδα αλλά και να οριστεί καινούργιος αρχηγός συστάδας.

Επιπλέον, βοηθάνε στο να επιτευχθεί λιγότερη κατανάλωση πόρων και ενέργειας στο δίκτυο αλλά και καλύτερη επεξεργασία ακατέργαστων δεδομένων. Όταν υπάρχει τμηματοποίηση, ο αρχηγός ομάδας θα πρέπει να πιστοποιεί τα δεδομένα που λαμβάνει από άλλους κόμβους της ίδιας ομάδας. Για να επιτευχθεί αυτό θα πρέπει να υπάρχει διαχείριση κλειδιών ομάδας. Ωστόσο, προκύπτει ένα μειονέκτημα αφού η προσθήκη ή η αφαίρεση κόμβων προκαλεί αρκετά προβλήματα στο δίκτυο, όπως προβλήματα σχετικά με την ασφάλεια. Θα πρέπει να γίνεται με ασφάλεια η επιλογή και η εκλογή ενός κόμβου σε αρχηγό ομάδας, γιατί αν προστεθεί στο δίκτυο ένας κακόβουλος κόμβος και εκλεγεί σε αρχηγό ομάδας, θα υπάρχει πρόβλημα ασφάλειας. Το πρωτόκολλο LEACH δημιουργεί συστάδες και κάθε κόμβος αποφασίζει αν θα γίνει αρχηγός συστάδας ή όχι στον τρέχοντα γύρο. Υπάρχουν και κριτήρια για την επιλογή αρχηγών συστάδας όπως πόσες φορές ένας κόμβος αισθητήρας έχει γίνει αρχηγός μέχρι τώρα αλλά κυρίως χωρίζονται σε δύο διαφορετικές μεθόδους.

- **Κεντρική Μέθοδος:** Στην κεντρική μέθοδο ο τωρινός αρχηγός συστάδας μαζεύει πληροφορίες και ενέργεια από γειτονικούς κόμβους και να έχει μία συνολική εικόνα της συστάδας ώστε να κάνει πιο σωστά την επιλογή του.
- **Κατανεμημένη Μέθοδος:** Στην κατανεμημένη μέθοδο όταν το επίπεδο ενέργειας του αρχηγού συστάδας πέσει από ένα κατώτατο επίπεδο που έχει οριστεί μεταδίδει στην συστάδα ένα μήνυμα για να ξεκινήσει η διαδικασία επιλογής καινούργιου αρχηγού. Κάθε κόμβος της συστάδας ελέγχει τα επίπεδα ενέργειας του και αν είναι υψηλότερα από το κατώτατο επίπεδο τότε απαντάνε θετικά ότι διεκδικούν την θέση του αρχηγού.

2.12 Σύστημα Ανίχνευσης Εισβολής

Τα συστήματα ανίχνευσης εισβολών είναι ένα είδος ασφάλειας που χρησιμοποιείται από όλα τα παραδοσιακά δίκτυα και υπολογιστές. Η δουλειά ενός τέτοιου συστήματος είναι η συλλογή και ανάλυση πληροφοριών του δικτύου για να εντοπίζει πιθανές επιθέσεις είτε εσωτερικές, είτε εξωτερικές του δικτύου. Κάποιες από τις βασικές λειτουργίες είναι:

- ✓ Παρακολούθηση και ανάλυση δραστηριοτήτων τόσο του συστήματος αλλά και του χρήστη
- ✓ Ανάλυση των αλλαγών και των τρωτών σημείων που μπορεί να υπάρχουν στο σύστημα και στο δίκτυο.
- ✓ Αξιολόγηση της ακεραιότητας του συστήματος και των δεδομένων
- ✓ Ικανότητα αναγνώρισης των πιο γνωστών επιθέσεων
- ✓ Ανάλυση ανώμαλων μοτίβων δραστηριότητας στο σύστημα

Τα ασύρματα δίκτυα αισθητήρων λειτουργούν διαφορετικά από τα παραδοσιακά δίκτυα στο πως γίνεται η συλλογή δεδομένων, οπότε θα πρέπει να παραμετροποιηθεί ανάλογα.

Στα ασύρματα δίκτυα αισθητήρων δεν υπάρχουν σταθερά κεντρικά σημεία όπου γίνεται η συλλογή δεδομένων, αλλά υπάρχουν οι σταθμοί βάσεων, αρχηγοί συστάδας και αρχηγοί ομάδας που συλλέγουν δεδομένα. Ένα σύστημα ανίχνευσης εισβολών για να μπορεί να λειτουργήσει σωστά θα πρέπει να χρησιμοποιεί το λιγότερο δυνατόν σε πόρους του συστήματος όπως εύρος ζώνης, ισχύς και ενέργειας. Καθώς οι κόμβοι στο δίκτυο είναι πολύ εύκολο να παραβιαστούν, το σύστημα ανίχνευσης θα πρέπει να λειτουργεί με γνώμονα ότι κανένας κόμβος του δικτύου δεν μπορεί να είναι τελείως αξιόπιστος.

Για την καλύτερη λειτουργία του συστήματος ανίχνευσης μπορεί να τοποθετηθούν κόμβοι παρακολούθησης στο δίκτυο, αλλά θα πρέπει να είναι σε θέση το σύστημα ανίχνευσης να αμυνθεί και σε επιθέσεις εναντίον του εαυτού του. Αν κάποιος κακόβουλος χρήστης έχει πρόσβαση σε έναν κόμβο παρακολούθησης τότε θα μπορούσε να αλλοιώσει της πληροφορίες του και να έχει δυνατότητες όπως να διώξει έναν κανονικό κόμβο από το δίκτυο ή να αποτρέψει έναν κακόβουλο κόμβο από το να ανακαλυφθεί. Επειδή οι πληροφορίες που συλλέγει το σύστημα αυτό είναι πολύ σημαντικές για την ασφάλεια του δικτύου, δεν θα πρέπει να συλλέγονται σε μόνο ένα μέρος αλλά να είναι κατανεμημένες σε διάφορες τοποθεσίες στο δίκτυο.

2.13 Ασφαλή Συλλογή Δεδομένων

Ο τρόπος με τον οποίο γίνεται η συλλογή δεδομένων στα ασύρματα δίκτυα αισθητήρων είναι ελκυστική σε επιθέσεις. Οι αισθητήρες στέλνουν πρώτα τα δεδομένα τους σε έναν κόμβο sink όπου συλλέγονται πρώτα όλα τα δεδομένα και μετά αποστέλλονται για επεξεργασία σε κάποιον σταθμό βάσης. Αυτό είναι σχεδιασμένο έτσι διότι η κατανάλωση ενέργειας είναι αρκετά μικρότερη για να γίνει η συλλογή πληροφοριών στο εσωτερικό του δικτύου παρά σε κάποιον εξωτερικό παράγοντα. Η μεγαλύτερη κατανάλωση ενέργειας που καταναλώνει ένας κόμβος αισθητήρα είναι κατά την διάρκεια υπολογισμών όπως επίσης και στην λήψη – αποστολή δεδομένων. Για να σταλεί ένα bit πληροφορία απαιτείται ίδια ποσότητα ενέργειας όσο η εκτέλεση 50 έως 150 εντολών στο επίπεδο του αισθητήρα.

Η κίνηση που δημιουργείται στο δίκτυο έχει μεγάλη επιρροή στο πόσο ενέργεια θα καταναλωθεί οπότε θα πρέπει να βρεθούν τρόποι για την καλύτερη και ασφαλέστερη συλλογή δεδομένων. Υπάρχουν τύποι επιθέσεων που μπορούν να επιτεθούν σε κόμβους συγκέντρωσης δεδομένων ή και σε κόμβους αισθητήρων και να τεθούν σε κίνδυνο τα ιδιαίτερα ευαίσθητα δεδομένα που συλλέγονται. Υπάρχουν τεχνικές για την ασφαλή συλλογή δεδομένων όπως ασφάλεια βήμα προς βήμα (hop by hop) όπου τα δεδομένα καταφτάνουν μεμονωμένα και αθροίζονται με τέτοιον τρόπο έτσι ώστε ο κόμβος sink να μπορεί να ανιχνεύσει εάν έχουν εισέλθει παράνομα πακέτα. Βέβαια αυξάνεται η κατανάλωση του εύρους ζώνης του δικτύου διότι τα πακέτα είναι μεγαλύτερα. [30]

2.14 Κρυπτογραφία σε Ασύρματα Δίκτυα Αισθητήρων

Οι εφαρμογές στα ασύρματα δίκτυα αισθητήρων πολλές φορές διαχειρίζονται πολύ σημαντικά δεδομένα και θα πρέπει να υπάρχει ένα μέτρο ασφάλειας για αυτά. Ένα πρόβλημα που αντιμετωπίζουν τέτοια δίκτυα βέβαια είναι ότι ο αριθμός των κόμβων αισθητήρων είναι αρκετά μεγάλος οπότε ο κρυπτογραφικός αλγόριθμος θα πρέπει να μπορεί να ανταπεξέλθει στον μεγάλο αριθμό κόμβων και παράλληλα να μην καταναλώνει πολύ ενέργεια. Υπάρχουν πολύ λίγοι πόροι σε απομακρυσμένα ασύρματα δίκτυα αισθητήρων οπότε δεν μπορούν να χρησιμοποιηθούν πρακτικές κρυπτογραφίας όπως γίνεται στα παραδοσιακά δίκτυα.

Ένας τρόπος για να υπάρξει κρυπτογραφία είναι με την χρήση συμμετρικού κλειδιού. Το μειονέκτημα στην χρήση του συμμετρικού κλειδιού είναι ότι όλοι οι κόμβοι χρησιμοποιούν το ίδιο κλειδί οπότε σε περίπτωση που κάποιος κακόβουλος χρήστης έχει πρόσβαση σε έναν από τους κόμβους μπορεί να έχει στην κατοχή του το κλειδί για την κρυπτογράφηση. Μία διαφορετική εκδοχή για την χρήση κρυπτογραφίας είναι η χρήση κοινού κλειδιού μεταξύ δύο κόμβων σε ολόκληρο το δίκτυο. Με αυτό τον τρόπο δεν έχει όλο το δίκτυο το ίδιο κλειδί και γίνεται με πιο ασφαλή τρόπο η κρυπτογραφία. Ωστόσο, υπάρχει ένα τεράστιο μειονέκτημα καθώς δεν μπορούν να προστεθούν καινούργιοι κόμβοι στο δίκτυο μετά την διαδικασία ανάπτυξης του δικτύου. Σε ένα δίκτυο αισθητήρων με n κόμβους, κάθε κόμβος πρέπει να αποθηκεύει (n - 1) κλειδιά. [28]

2.14.1 Διαχείριση Αλγοριθμικών Κλειδιών

Η διαχείριση κλειδιών είναι αρκετά σημαντική τεχνική για τα ασύρματα δίκτυα αισθητήρων διότι παρέχουν ασφάλεια μεταξύ εξουσιοδοτημένων συσκευών. Χρησιμοποιεί ένα σύνολο από τεχνικές και διαδικασίες που υποστηρίζουν την καθιέρωση και διατήρηση των σχέσεων στις συσκευές που χρησιμοποιούν αλγοριθμικά κλειδιά. Υπάρχουν δύο βασικοί τύποι αλγοριθμικών κλειδιών, το συμμετρικό αλγοριθμικό κλειδί και το ασύμμετρο.

Οι αλγόριθμοι συμμετρικού κλειδιού χρησιμοποιούνται σε συστήματα που περιλαμβάνουν δύο μετασχηματισμούς, έναν για μία πηγή/αποστολέα και έναν για τον παραλήπτη. Οι μετασχηματισμοί αυτοί χρησιμοποιούν και οι δύο είτε το ίδιο μυστικό κλειδί δηλαδή χρήση συμμετρικού κλειδιού είτε δύο κλειδιά που δημιουργούνται αρκετά εύκολα από την πηγή/αποστολέα και τον παραλήπτη.

Για να γίνει η χρήση αλγόριθμου ασύμμετρου κλειδιού το σύστημα θα πρέπει να υποστηρίζει ένα δημόσιο κλειδί και ένα ιδιωτικό. Το ιδιωτικό κλειδί δεν θα πρέπει να είναι εύκολα προσβάσιμο από το δημόσιο κλειδί ώστε να υπάρχει μεγαλύτερη ασφάλεια. Το δημόσιο κλειδί χρησιμοποιείται για την κρυπτογράφηση δεδομένων ενώ το ιδιωτικό για την αποκρυπτογράφηση τους.

Η διαχείριση κλειδιών παίζει σημαντικό ρόλο σε κρυπτογραφικές τεχνικές όπως εμπιστευτικότητα, πιστοποίηση οντότητας, προέλευση δεδομένων αυθεντικοποίησης, ακεραιότητα δεδομένων και ψηφιακές υπογραφές. Με την χρήση κλειδιών και τεχνικών κρυπτογράφησης το δίκτυο ασφαλίζεται από διάφορες επιθέσεις προστατεύοντας έτσι ολιστικά το δίκτυο.

Η ύπαρξη αλγοριθμικών κλειδιών βοηθάει πολύ το έργο των τεχνικών κρυπτογράφησης διότι δημιουργούνται σχέσεις μεταξύ συσκευών, δημόσιων και ιδιωτικών κλειδιών. Ένα πρόβλημα που υπάρχει με την ασύμμετρη κρυπτογραφία είναι ότι απαιτεί πάρα πολλούς παραπάνω πόρους από το σύστημα σε σχέση με την συμμετρική κρυπτογραφία οπότε πολλές φορές δεν προτιμάται.

Βέβαια η χρήση συμμετρικού κλειδιού επίσης μπορεί να γίνει λιγότερο αποδοτική στο κομμάτι ενέργειας και πόρων του συστήματος αν αποφασίσει ότι θα χρησιμοποιεί διαφορετικά κλειδιά για όλα τα πιθανά ζευγάρια κόμβων αισθητήρων που σημαίνει ότι θα αυξηθεί και η πολυπλοκότητα του αλγόριθμου. Αυτό επιτυγχάνεται με το να αποθηκευτούν n-1 κλειδιά όπου n είναι το μέγεθος του ασύρματου δικτύου αισθητήρων στους κόμβους οπότε υπάρχει πολύ μικρή πιθανότητα παραβιάσεων. Από κάποιο μέγεθος δικτύων και πάνω δεν συμφέρει η συγκεκριμένη τεχνική διότι η επιβάρυνση στους κόμβους αυξάνεται γραμμικά και δεν έχουν αρκετά μεγάλη μνήμη ώστε να μπορεί να είναι βιώσιμη επιλογή.

2.14.2 Διαφορετικοί Τύποι Διαχείρισης Κλειδιών

2.14.2.1 Key Pool Based Key Management

Η συγκεκριμένη διαχείριση κλειδιών [30] είναι ένα σύστημα πιθανολογικό που διανέμει τα κλειδιά από πριν στις συσκευές και χωρίζεται σε τρεις κατηγορίες:

1) **<u>Key pre-distribution (Κλειδί προ-διανομής):</u>** Ο τρόπος με τον οποίο λειτουργεί η συγκεκριμένη διαχείριση κλειδιών είναι ότι υπάρχει μία μεγάλη δεξαμενή κλειδιών όπου όλα τα κλειδιά έχουν μοναδικά χαρακτηριστικά. Ο κάθε κόμβος εξοπλίζεται με συγκεκριμένο αριθμό κλειδιών, η επιλογή των κλειδιών γίνεται με τυχαίο τρόπο από την δεξαμενή κλειδιών. Όταν σε όλους τους κόμβους έχουν διανεμηθεί μοναδικά κλειδιά τότε το σύστημα επιλέγει κάποιους κόμβους ως πιο έμπιστους ώστε να διαχειρίζονται και να αποθηκεύονται όλα τα αναγνωριστικά κλειδιών και όλα τα αναγνωριστικά των κόμβων αισθητήρων. Έτσι εξασφαλίζεται ότι δύο κόμβοι θα μοιράζονται τουλάχιστον ένα κοινό κλειδί είτε με την βοήθεια γειτονικών κόμβων είτε όχι.
2) **<u>Shared-key discovery (Ανακάλυψη κοινού κλειδιού):</u>** Σε αυτήν την τεχνική μόλις αναπτυχθεί το δίκτυο κάθε ζεύγος κόμβων εντός της εμβέλειας επικοινωνίας που έχουν, δημιουργούν ένα κοινό κλειδί. Μόλις τελειώσει η διαδικασία αυτή εάν μοιράζονται κάποιο κοινό κλειδί ή κλειδιά σε σχέση με τα κλειδιά που τους έχουν

ανατεθεί τότε μπορούν να αποφασίσουν ποιο από αυτά θα χρησιμοποιούν σαν μυστικό κλειδί. Υπάρχουν πολλοί και διαφορετικοί τρόποι για να διαπιστωθεί εάν δύο κόμβοι έχουν κάποιο κοινό κλειδί αλλά ο απλούστερος τρόπος είναι, οι κόμβοι να μεταδώσουν μεταξύ τους την λίστα με τα αναγνωριστικά κλειδιά που έχουν. Με αυτό τον τρόπο διαπιστώνουν ένα μοιράζονται κάποιο κλειδί με άλλον κόμβο και χρησιμοποιούν το συγκεκριμένο κλειδί ως μυστικό κλειδί πλέον ώστε να υπάρχει ασφαλή επικοινωνία. Η ασφάλεια του δικτύου έτσι ενισχύεται και είναι αρκετά δύσκολο να δημιουργηθούν κενά ασφαλείας ώστε να υπάρξει κάποια επίθεση. Η μόνη επίθεση που μπορεί να γίνει είναι η επίθεση ανάλυσης της κίνησης του δικτύου όταν όμως υπάρχει η ελλείψει των αναγνωριστικών κλειδιών στο δίκτυο.

3) **Path key establishment (Εγκαθίδρυση κλειδιού διαδρομής):** Όπως αναφερθήκαμε και στην διαχείριση κλειδιών shared-key discovery δύο κόμβοι μπορούν να επικοινωνήσουν εάν έχουν κοινό κλειδί. Η διαφορά που έχει με την διαχείριση path key establishment είναι ότι μπορεί να δημιουργηθεί σύνδεση μεταξύ δύο κόμβων ακόμα και αν δεν μοιράζονται κάποιο κοινό κλειδί. Αυτό επιτυγχάνεται με την βοήθεια ενός τρίτου κόμβου όπου ο πρώτος κόμβους στέλνει ένα μήνυμα ότι θέλει να έρθει σε επικοινωνία με τον δεύτερο κόμβο. Το μήνυμα κρυπτογραφείται χρησιμοποιώντας το κοινό κλειδί του πρώτου και του τρίτου κόμβου και επιτυγχάνεται η επικοινωνία. Στην τεχνική αυτή ο τρίτος κόμβος λειτουργεί σαν μεσολαβητής τον άλλον δύο κόμβων που επιχειρούν να επικοινωνήσουν μεταξύ τους αυξάνοντας έτσι το πόσο ευέλικτο, αποτελεσματικό και απλό σε εφαρμογή μπορεί να γίνει το δίκτυο. Αυτή η λύση βέβαια δεν είναι για όλες τις εφαρμογές των WSN που απαιτούν το ύψιστο επίπεδο ασφάλειας καθώς δεν παρέχουν πιστοποίηση από κόμβο σε κόμβο.

2.14.2.2 Polynomial Pool-Based Key Pre-Distribution

Στην προδιανομή κλειδιών με βάση την πολυωνυμική δεξαμενή η ασφαλής επικοινωνία ανά ζεύγη γίνεται με πρωτόκολλα διανομής κλειδιών βασισμένα σε πολυώνυμα και σε πλέγματα. Είναι μία βελτιωμένη έκδοση της διαχείρισης Key pool based όπου αντί να προμοιράζουν κλειδιά, προμοιράζουν πολυώνυμα από μία δεξαμενή πολυωνύμων. Σε σχέση με άλλες εκδοχές είναι αρκετά αποδοτική γιατί έχει χαρακτηριστικά όπως:

- Όταν δεν υπάρχουν κόμβοι που να έχουν παραβιαστεί τότε οποιοσδήποτε κόμβος θέλει μπορεί να δημιουργήσει ένα κλειδί ανά ζεύγος.
- Ακόμα και αν υπάρχουν κόμβοι αισθητήρων που μπορεί να έχουν παραβιαστεί τότε, το υπόλοιπο WSN μπορεί να συνεχίσει και να δημιουργεί κλειδιά ανά ζεύγη.

- Οι κόμβοι μπορούν να βρίσκουν κοινά κλειδιά με άλλους κόμβους και να δημιουργούν κλειδιά ανά ζευγάρια μειώνοντας έτσι την επιβάρυνση στην επικοινωνία.

2.14.2.3 Location-Dependent Key Management

Σε αυτήν την περίπτωση η διαχείριση κλειδιών εξαρτάται από την τοποθεσία και αποφασίζει ποια κλειδιά θα τοποθετηθούν σε ποιους κόμβους ανάλογα με την θέση που έχουν στο περιβάλλον. Οι κόμβοι είναι στατική και επικοινωνούν μόνο μέσω κρυπτογραφημένων καναλιών επικοινωνίας και μπορούν να προστεθούν καινούργιοι κόμβοι ανά πάσα στιγμή στο δίκτυο. Οι κόμβοι θα πρέπει να είναι ικανοί να μπορούν να μεταδίδουν πληροφορίες σε διαφορετικά επίπεδα ισχύος και να παρέχουν διαφορετικές εμβέλειες μετάδοσης. Στο δίκτυο προστίθενται καινούργιοι κόμβοι με την ονομασία anchor όπου η διαφορά τους από τους κανονικούς κόμβους αισθητήρων είναι ότι μεταδίδουν σε διαφορετικά επίπεδα ισχύος και δεν μπορούν να παραβιαστούν. Στο σύστημα αυτό υπάρχουν τρεις διαφορετικές φάσεις: μία φάση προδιανομής, μία φάση αρχικοποίησης και μία φάση επικοινωνίας.

- **Φάση προδιανομής:** Στην φάση προδιανομής ένας διακομιστής κλειδιών (key server) είναι υπεύθυνος για τον υπολογισμό των κλειδιών που θα χρησιμοποιηθούν από τους κόμβους του δικτύου και τα τοποθετεί σε μία δεξαμενή. Κάθε κόμβος τοποθετεί ένα μερίδιο κλειδιών από την δεξαμενή στον εαυτό του μαζί με ένα κοινό κλειδί που μοιράζεται κάθε κόμβος, επίσης οι κανονικοί κόμβοι και οι κόμβοι anchors κατανέμονται τυχαία στο δίκτυο.
- **Φάση αρχικοποίησης:** Κατά την διάρκεια της αρχικοποίησης οι κόμβοι anchor βοηθούν τους άλλους κόμβους αισθητήρων να αλλάξουν τα υπάρχοντα κλειδιά τους με την βοήθεια σημάτων. Με την χρήση των παλιών κλειδιών και των σημάτων που λαμβάνουν από τους κόμβους anchor, οι κόμβοι αισθητήρων υπολογίζουν τα καινούργια κλειδιά. Στην μνήμη του κόμβου υπάρχει ένα υποσύνολο των κλειδιών που τοποθετήθηκαν εκεί όταν πήρε τα προηγούμενα “παλιά” κλειδιά οπότε θα διαγραφούν για να τοποθετηθούν τα καινούργια.
- **Φάση επικοινωνίας:** Τέλος στην φάση της επικοινωνίας υπολογίζονται τα κλειδιά ανά ζεύγος που χρησιμοποιούν οι κόμβοι αισθητήρων μεταξύ τους για να υπάρχει ασφαλή επικοινωνία. Με την τεχνική της διαχείρισης κλειδιών με βάση της τοποθεσίας ένα θετικό είναι ότι οι κόμβοι που έχουν παραβιαστεί δεν μπορούν να επηρεάσουν άλλους κόμβους στο δίκτυο. Από την άλλη δεν έχει τόσο καλές επιδόσεις σε σχέση με ένα τυχαίο σύστημα διανομής κλειδιών μεγέθους δεξαμενής 5000 κλειδιών και 175 κλειδιά σε κάθε κόμβο αισθητήρων.

Άλλοι τύποι διαχείρισης κλειδιών που αξίζουν να σημειωθούν είναι με βάση την συνεδρία όπου οι περισσότερες τεχνολογίες χρησιμοποιούν χρονοσφραγίδες (time

stamps) για τη δημιουργία κλειδιών ώστε να υπάρχει επικοινωνία μεταξύ των κόμβων. Ένα πρωτόκολλο που ανήκει σε αυτήν την κατηγορία είναι το SPIN. Υπάρχει και ο τύπος διαχείρισης κλειδιών που είναι με βάση την ιεραρχία που κατά κόρον ανήκουν τοπολογίες δένδρου και οι κόμβοι γονείς και παιδιά αισθητήρων δημιουργούν κλειδιά ανάλογα την μορφή του δέντρου. Ένα πρωτόκολλο που ανήκει σε αυτήν την κατηγορία είναι το LEAP.

Επίσης υπάρχει και η διαχείριση κλειδιών με βάση τις συστάδες όπου το δίκτυο είναι δομημένο με συστάδες όπου σε κάθε συστάδα υπάρχει και πύλη (gateway) η οποία στην ουσία είναι ένας υπερκόμβος. Η πύλη είναι υπεύθυνη για την καλή λειτουργία σε κάθε συστάδα, επίσης κάθε αισθητήρας αποθηκεύει δύο κλειδιά τα οποία το ένα το μοιράζεται με μία πύλη και το άλλο με έναν κόμβο sink. Τα μειονεκτήματα που έχει αυτή η διαχείριση είναι ότι σε περίπτωση που ένας κόμβος πύλης παραβιαστεί, τότε η εμπιστευτικότητα των δεδομένων και η επικοινωνία της συστάδας βρίσκεται σε κίνδυνο.

3. Μελέτη Περίπτωσης Λογισμικού Δ.Ε.Υ.Α Καστοριάς

3.1 Εισαγωγή

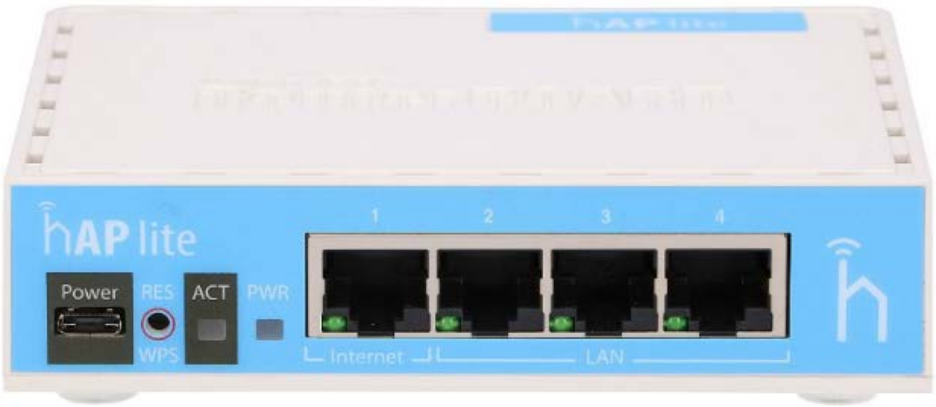
Η Δημοτική Επιχείρηση Ύδρευσης και Αποχέτευσης Καστοριάς (ΔΕΥΑΚ) δημιουργήθηκε 31-12-1980 και είναι ιδιωτική επιχείρηση του δημοσίου. Ο νέος δήμος Καστοριάς που συστάθηκε το 2010 αποτελείται από τους πρώην Δήμους Καστοριάς, Αγίας Τριάδος, Μεσοποταμίας, Κορεστείων, Αγίων Αναργύρων, Μακεδνών, Βιτσίου, Κλεισούρας και την πρώην κοινότητα Καστρακίου που συνολικά έχει υπερδιπλάσιο πληθυσμό και δεκαεφτά φορές μεγαλύτερη έκταση από τον προηγούμενο δήμος Καστοριάς. Αρκετοί δήμοι δεν είχαν για αρκετό καιρό κάποια ΔΕΥΑ που να τους υποστηρίζει στην λειτουργία των δικτύων ύδρευσης και αποχέτευσης, αλλά αυτό άλλαξε και η ΔΕΥΑΚ με αρκετές επενδύσεις όπως υδατοδεξαμενές, αντλιοστάσια και πηγές υδροδότησης, αλλά και χιλιάδες μέτρα δικτύων που εξυπηρετούν περίπου 40000 καταναλωτές. Επίσης η επιχείρηση είναι αρμόδια για τη μελέτη, κατασκευή, συντήρηση, εκμετάλλευση, διοίκηση και λειτουργία των δικτύων ύδρευσης, αποχέτευσης και ομβρίων υδάτων, καθώς και της μονάδας επεξεργασίας των λυμάτων της πόλης της Καστοριάς.

Τα τελευταία χρόνια η ΔΕΥΑΚ κάνει συνεχείς επενδύσεις στις εγκαταστάσεις τις αλλά και στην τοπική κοινωνία ώστε να μπορεί να παρέχει καλύτερα αποτελέσματα για τους καταναλωτές. Μία από τις σημαντικότερες επενδύσεις που έκανε η εταιρία είναι η ανάπτυξη ενός ασύρματου δικτύου αισθητήρων με ενεργοποιητές για την παρακολούθηση και διαχείριση των αντλιοστασίων. Το σύστημα αυτοματισμού, τηλεπισκόπησης και ελέγχου που διαθέτει η ΔΕΥΑΚ είναι αρκετά σύγχρονο και επιτρέπει στην ΔΕΥΑΚ να παρακολουθεί σε πραγματικό χρόνο πολλά δεδομένα για τα αντλιοστάσια αλλά και να επεμβαίνει απομακρυσμένα αν χρειάζεται με αυτοματισμούς που έχουν τεθεί σε λειτουργία αλλά και χειροκίνητα. [31]

3.2 Υποδομή Ασύρματου Δικτύου

Έχει δημιουργηθεί ένα ασύρματο δίκτυο με την βοήθεια κεραιών ώστε να υπάρχει αμφίδρομη επικοινωνία στα αντλιοστάσια τις ΔΕΥΑΚ. Υπάρχει ένας κεντρικός υπολογιστής που λειτουργεί σαν διακομιστής (server) που σε αυτό τον υπολογιστή έχει γίνει όλοι η υλοποίηση του δικτύου αλλά και η εγκατάσταση του λειτουργικού για την απομακρυσμένη διαχείριση των αντλιοστασίων. Μέχρι τώρα υποστηρίζονται 20 από τα 90 αντλιοστάσια και σιγά σιγά υπάρχει πλάνο για την προσθήκη περισσότερων. Για την διαχείριση του δικτυακού εξοπλισμού υπάρχει ένα MikroTik hAP lite RB941-2nD Router (δρομολογητής) που μπορεί να υποστηρίξει την υλοποίηση αλλά ταυτόχρονα να μας παρέχει επίσης και πολύ μεγάλη ασφάλεια. Το router διαθέτει επεξεργαστή με έναν πυρήνα σε συχνότητα 650 MHz, 32 MB ram και εκπέμπει Wi-Fi στα 2.4GHz έτσι ώστε να

έχει αρκετούς πόρους αν χρειαστεί να προστεθούν παραπάνω συσκευές ή, η πολυπλοκότητα του δικτύου αυξηθεί αρκετά. [32]



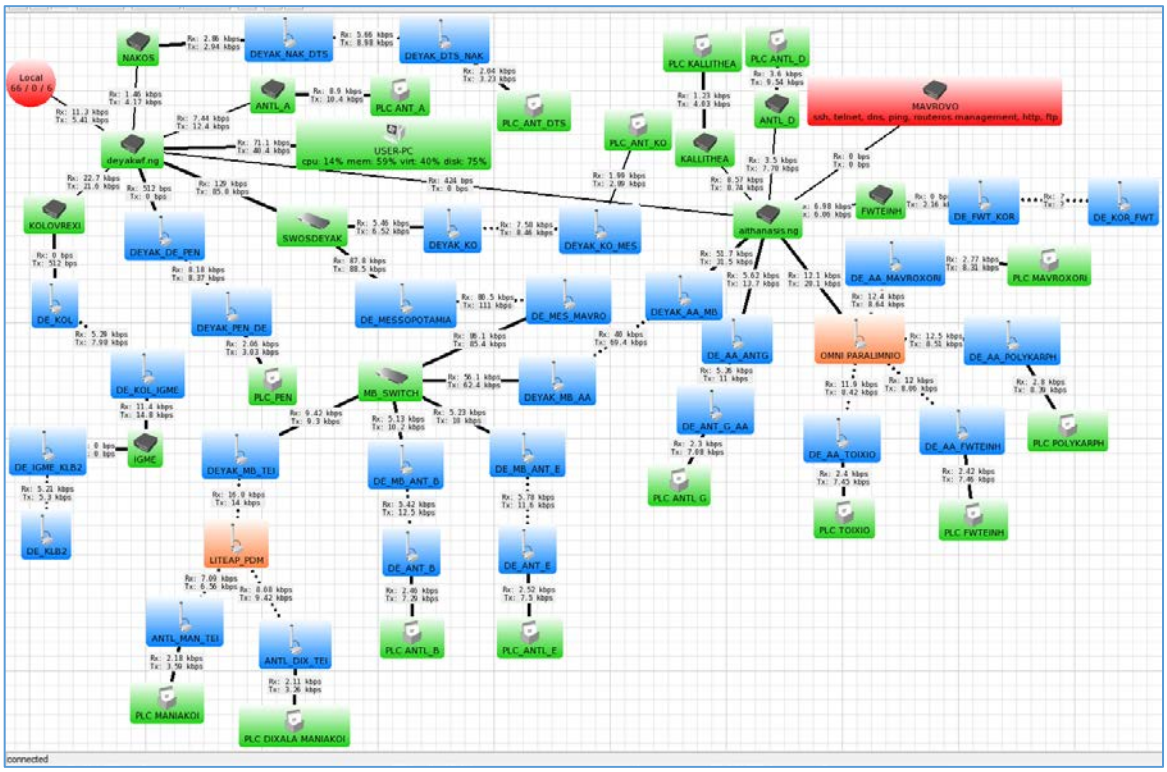
Εικόνα 36. MikroTik hAP lite

Πηγή:https://mikrotik.com/product/RB941-2nD

Η εταιρία MikroTik έχει δημιουργήσει ένα λογισμικό που μας επιτρέπει να επιβλέπουμε ολοκληρωτικά το δίκτυο αλλά και να επεμβαίνουμε πάνω σε αυτό μιας και λειτουργεί με το πρωτόκολλο Simple Network Management Protocol (SNMP). Μπορούμε να βλέπουμε την κίνηση στο δίκτυο σε πραγματικό χρόνο και να πραγματοποιούμε σχολαστικές δοκιμές για την βελτιστοποίηση του δικτύου.

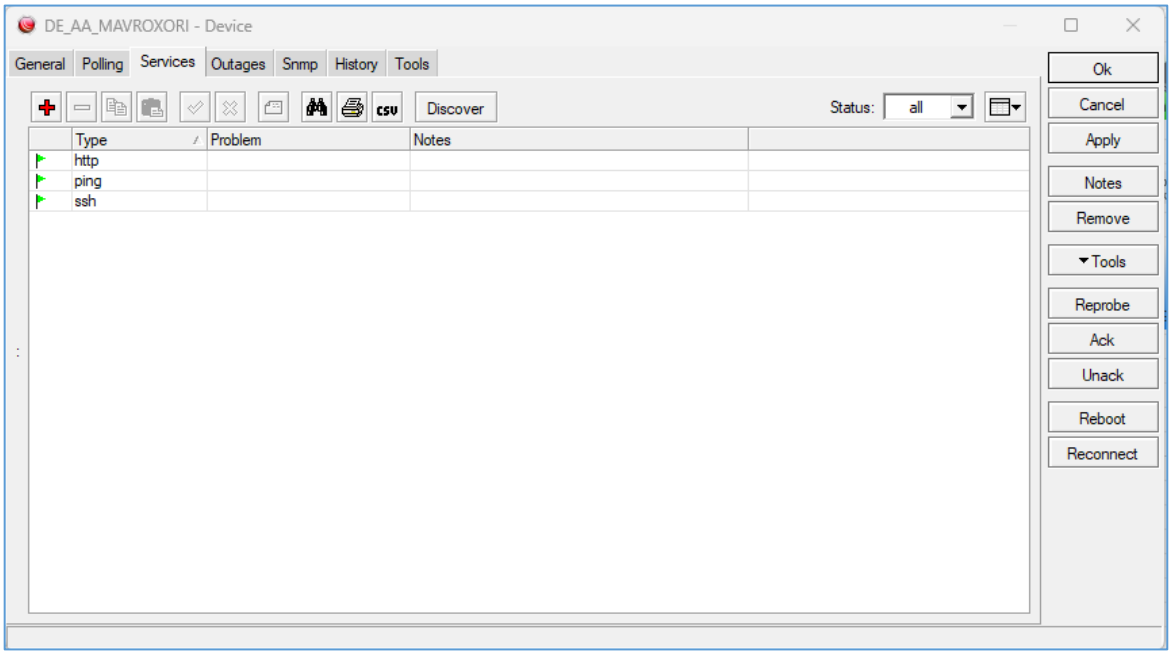
Η εφαρμογή μας παρέχει γραφικό περιβάλλον χρήστη και μπορούμε να προσθέσουμε στο δίκτυο μας όλες τις συσκευές που χρησιμοποιούμε όπως κεραίες, switch, Programmable Logic Controllers (PLC) και άλλα ότι άλλο θέλουμε. Μας δίνει την δυνατότητα να επιλέξουμε διαφορετικές εικόνες για την κάθε συσκευή ώστε να μπορούμε να διακρίνουμε το δίκτυο καλύτερα όπως επίσης και διαφορετικά χρώματα. Όσο το δίκτυο αυξάνεται σε μέγεθος και προστίθενται συσκευές θα είναι και πιο δύσκολο στην κατανόηση του εάν προκύψει κάποιο πρόβλημα. Σε κάθε συσκευή μπορούμε να δούμε την IP, την διεύθυνση MAC αλλά και την ονομασία που έχουμε επιλέξει να έχει. Επίσης μας δίνεται η δυνατότητα από το πρόγραμμα να επιλέξουμε με τι ρυθμό θέλουμε να ανανεώνονται τα δεδομένα όπως επίσης και αν θέλουμε να έρχονται ειδοποιήσεις για συγκεκριμένα γεγονότα.

Στην παρακάτω εικόνα βλέπετε την σχεδίαση του δικτύου της ΔΕΥΑΚ με τις κεραίες να έχουν μπλε χρώμα και τα PLC να έχουν πράσινο. Οι μαύρες συνεχόμενες γραμμές που είναι ενδιάμεσα από τις συσκευές συμβολίζουν την ασύρματη σύνδεση των δύο συσκευών, ενώ με διακεκομμένη μαύρη γραμμή είναι η ασύρματη σύνδεση. Πάνω στις γραμμές μας δίνει το πρόγραμμα πληροφορίες για την ταχύτητα αποστολής (Tx) και παραλαβής δεδομένων (Rx).



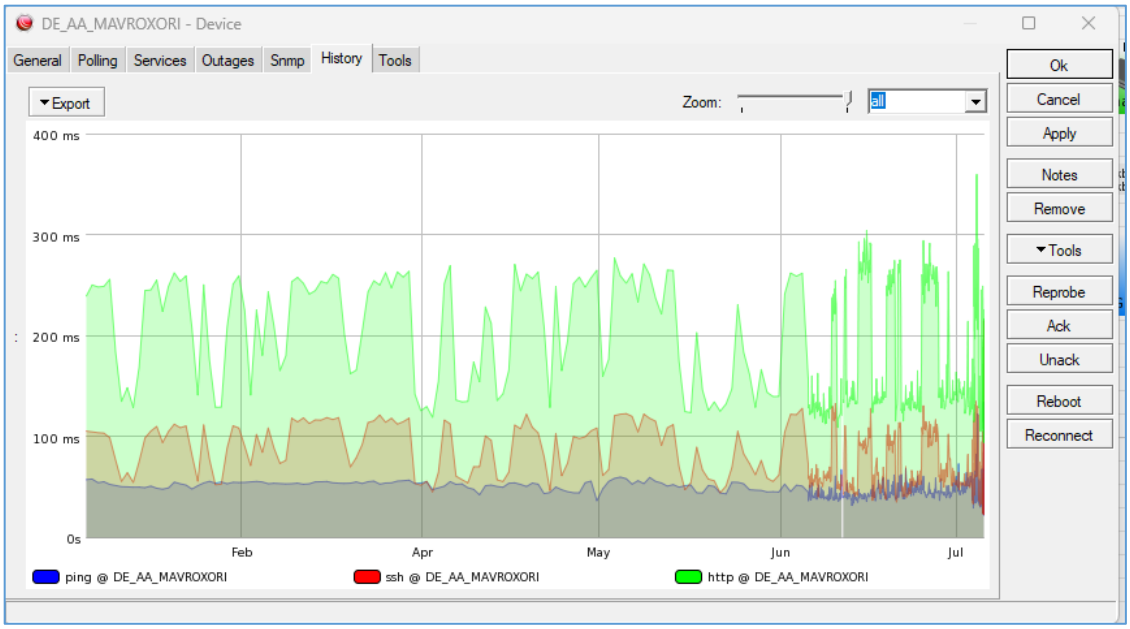
Εικόνα 37. The Dude Τοπολογία Δικτύου

Όταν πατάμε πάνω σε μία συσκευή μπορούμε να ρυθμίσουμε τι υπηρεσίες θέλουμε να παρακολουθούμε και να ενημερωνόμαστε για το αν δεν είναι ενεργές, όπως στην φωτογραφία παρακάτω. Στην συγκεκριμένη περίπτωση η συσκευή που ελέγχουμε της υπηρεσίες http, ping και ssh είναι μία κεραία Ubiquiti LBE-5AC-23.



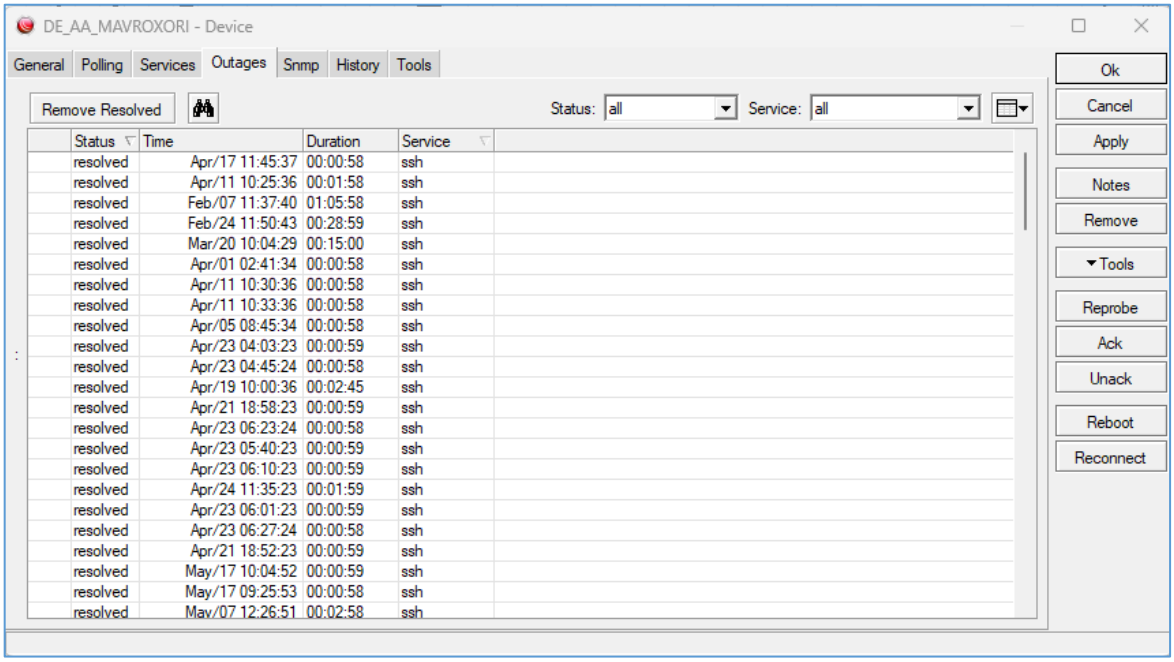
Εικόνα 38 The Dude Υπηρεσίες

Επίσης μας δίνεται η δυνατότητα να έχουμε ένα ιστορικό σε μορφή γραφήματος όπου εμφανίζονται ότι υπηρεσίες έχουμε προσθέσει προηγουμένως με διαφορετικά χρώματα για την κάθε μία, και τι καθυστέρηση έχει η κάθε υπηρεσία αντίστοιχα.



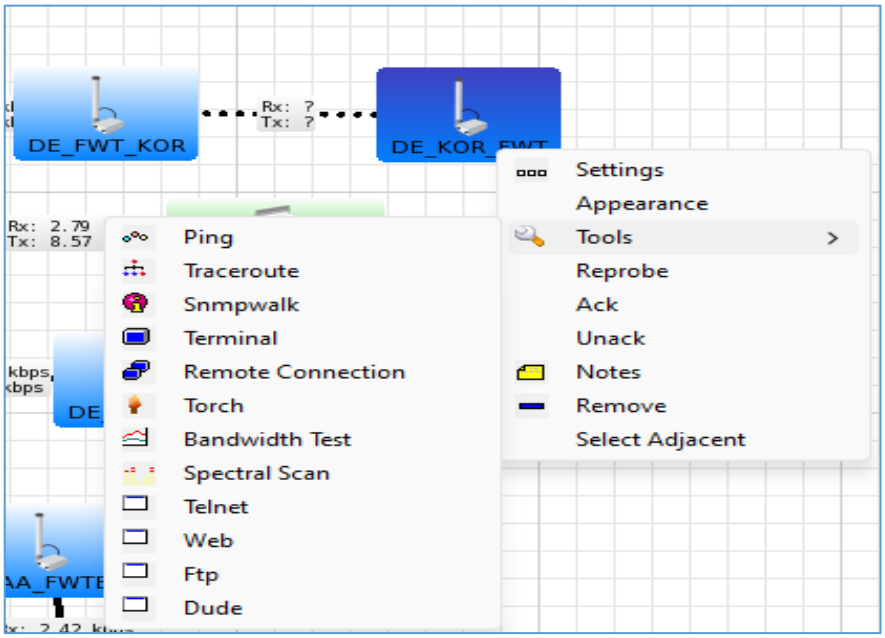
Εικόνα 39. The Dude Ιστορικό καθυστέρησης

Ακόμη μία επιλογή που έχει το πρόγραμμα είναι ότι μπορεί να μας ενημερώνει για μία υπηρεσία όταν σταμάτησε να είναι σε λειτουργία αλλά και σε πόση ώρα το πρόβλημα λύθηκε.



Εικόνα 40. The Dude Διακοπή Λειτουργίας

Τέλος στο πρόγραμμα περιλαμβάνεται μία σουίτα από προγράμματα που μπορούν να μας βοηθήσουν να δοκιμάσουμε την λειτουργία του δικτύου, να επέμβουμε απομακρυσμένα ή ακόμα και αν μεταφέρουμε αρχεία με File Transfer Protocol (FTP).



Εικόνα 41. The Dude Σουίτα Εργαλείων

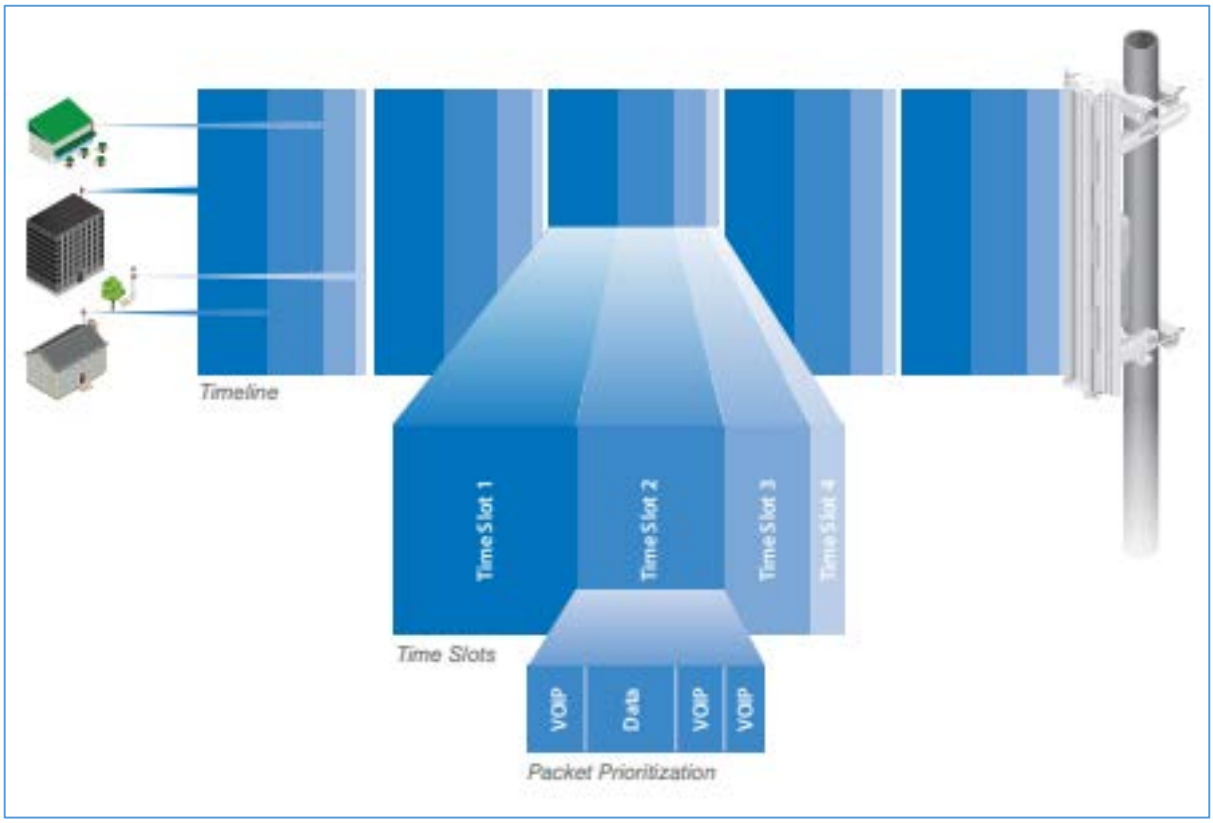
3.3 Δίκτυο Κεραιών Δ.Ε.Υ.Α.Κ

Οι κεραίες που έχουν χρησιμοποιηθεί για την υλοποίηση του ασύρματου δικτύου αισθητήρων στην Δ.Ε.Υ.Α.Κ είναι της εταιρίας Ubiquiti και είναι το μοντέλο LBE 5AC 23. Είναι μία κεραία παραβολική με απολαβή κεραίας 23 dBi και εύρος ζώνης συχνοτήτων 2400-2483,5 GHz και 5.150 - 5.875 GHz. Η συγκεκριμένη κεραία είναι ιδανική και για μακρινές αποστάσεις χρησιμοποιώντας όχι μόνο τα πρότυπα IEEE 802.11 b/g/n και 802.11ac αλλά και σύνδεση point – to – point (σημείο σε σημείο) που συνδέει δύο απομακρυσμένες συσκευές μεταξύ τους.

Εικόνα 42. Ubiquiti LiteBeam AC Gen2

Πηγή:https://dl.ubnt.com/datasheets/LiteBeam/LiteBeam_DS.pdf

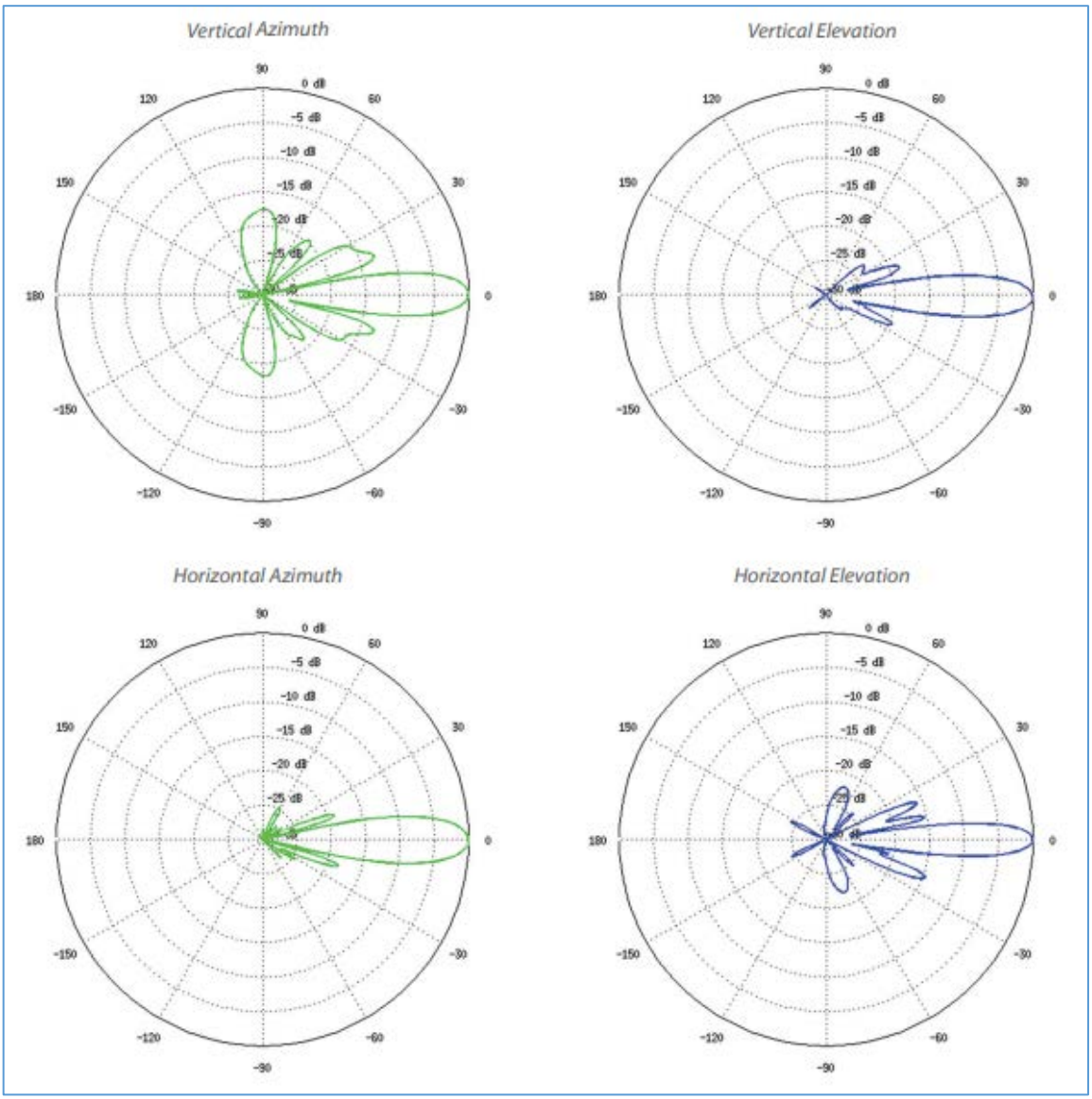
Επίσης η ίδια η εταιρία έχει δημιουργήσει τεχνολογίες για την καλύτερη επικοινωνία μεταξύ των συσκευών όπως InnerFeed® Technology ενσωματώνει ολόκληρο το ράδιο σύστημα στην τροφοδοσία της κεραίας. Επίσης δημιούργησαν την τεχνολογία airMAX με πρωτόκολλο TDMA που ενισχύει την απόδοση και την επεκτασιμότητα του δικτύου. Επίσης υποστηρίζει την τεχνολογία 2x2 Multiple-Input and Multiple-Output (MIMO) που χρησιμοποιεί πολλαπλές κεραίες ανάμεσα σε έναν πομπό και έναν δέκτη έτσι ώστε να μεταφερθούν περισσότερες πληροφορίες από διαφορετικές διαδρομές.



Εικόνα 43. Τεχνολογία Ubiquiti AirMax με Πρωτόκολλο TDMA

Πηγή:https://dl.ubnt.com/datasheets/LiteBeam/LiteBeam_DS.pdf

Η κεραία έχει επεξεργαστή τον Atheros MIPS 74Kc, 533 MHz και μνήμη 64MB και είναι πάρα πολύ καλός για τις δυνατότητες που έχει η κεραία. Το διάγραμμα ακτινοβολίας της κεραίας εμφανίζεται παρακάτω. [33]



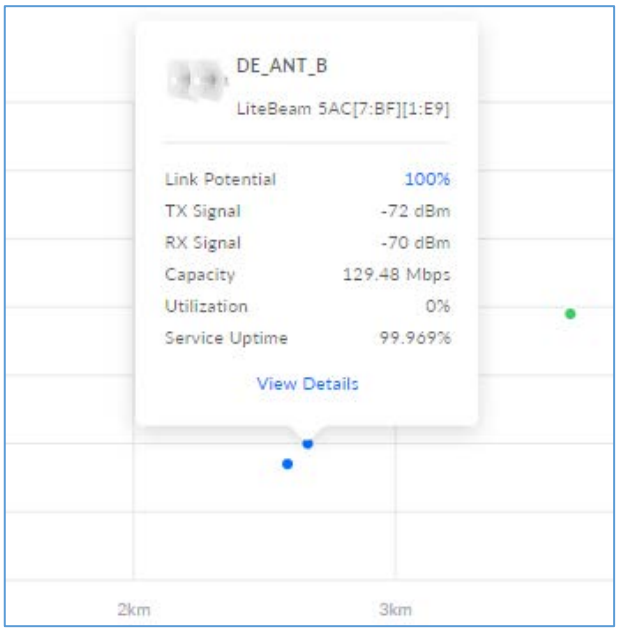
Εικόνα 44. Διάγραμμα Ακτινοβολίας Κεραίας

3.4 Ubiquiti USIP Λογισμικό

Οι κεραίες που έχουν επιλεχθεί για την υλοποίηση του δικτύου στην εταιρία Δ.Ε.Υ.Α Καστοριάς είναι μάρκας Ubiquiti και από την εταιρία παρέχεται ένα λογισμικό για τον απομακρυσμένο έλεγχο αλλά και την απομακρυσμένη παραμετροποίηση τους για καλύτερη διαχείριση του δικτύου που ονομάζεται Ubiquiti USIP. Στην εικόνα 45 παρακάτω μπορούμε να δούμε πληροφορίες για όλο το δίκτυο όπως ποια είναι η μέση τιμή για την δύναμη του σήματος των κεραιών, σε ποια απόσταση χιλιομέτρων βρίσκονται η κεραίες όπου με διαφορετικά χρώματα μπορούμε να δούμε πόσο καλό σήμα έχει η σύνδεση την κάθε δεδομένη στιγμή. Αρκετά σημαντικό είναι ότι μπορούμε να δούμε όλο το φάσμα των 5 GHz που μπορούμε να χρησιμοποιήσουμε έτσι ώστε να προγραμματίσουμε καλύτερα την χρήση των συχνοτήτων.

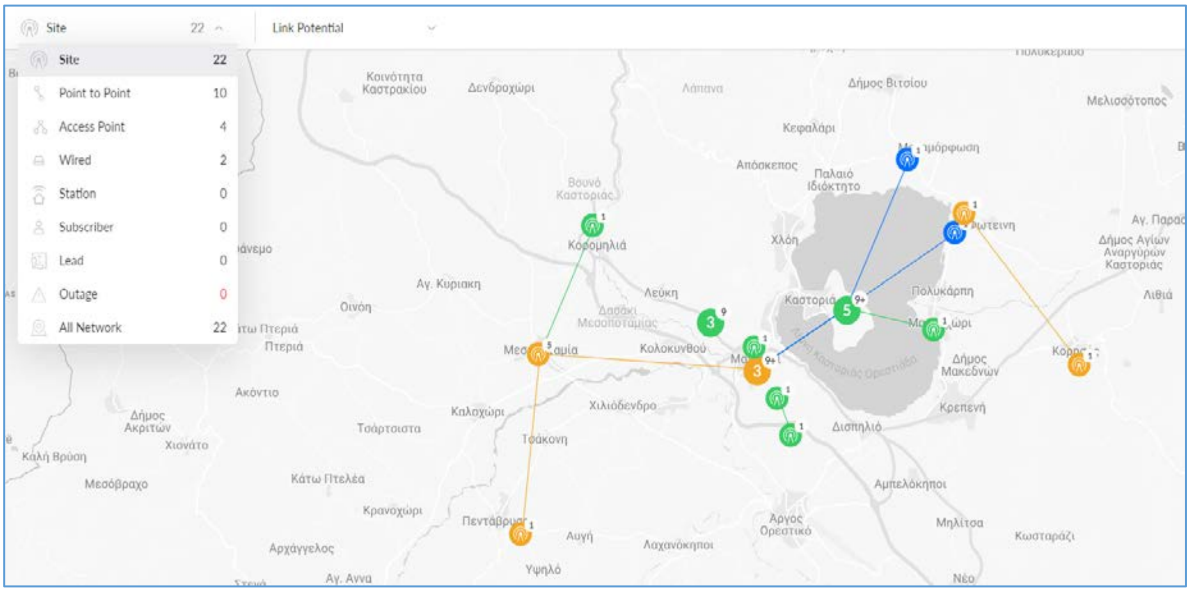
Εικόνα 45. Ubiquiti USIP Dashboard

Πατώντας πάνω σε κάποια κεραία μπορούμε να δούμε πληροφορίες όπως την δύναμη του σήματος που στέλνει και λαμβάνει η κεραία, τι ίντερνετ λαμβάνει η κεραία αλλά και ένα ποσοστό του χρόνου διαθεσιμότητας υπηρεσιών της κεραίας από την αρχή της λειτουργίας της μέχρι σήμερα.



Εικόνα 46. Πληροφορίες Κεραίας

Εδώ με την βοήθεια του προγράμματος που έχουν οι κεραίες μπορούμε να δούμε που ακριβώς βρίσκονται στον χάρτη οι κεραίες, πως είναι η συνδεσμολογία των κεραιών μεταξύ τους, τι τύπος κεραίας είναι όπως Point to Point, αν υπάρχουν Access Point συσκευές στο δίκτυο μας ή αν έχουμε συνδέσει συσκευές στο δίκτυο με καλώδιο.



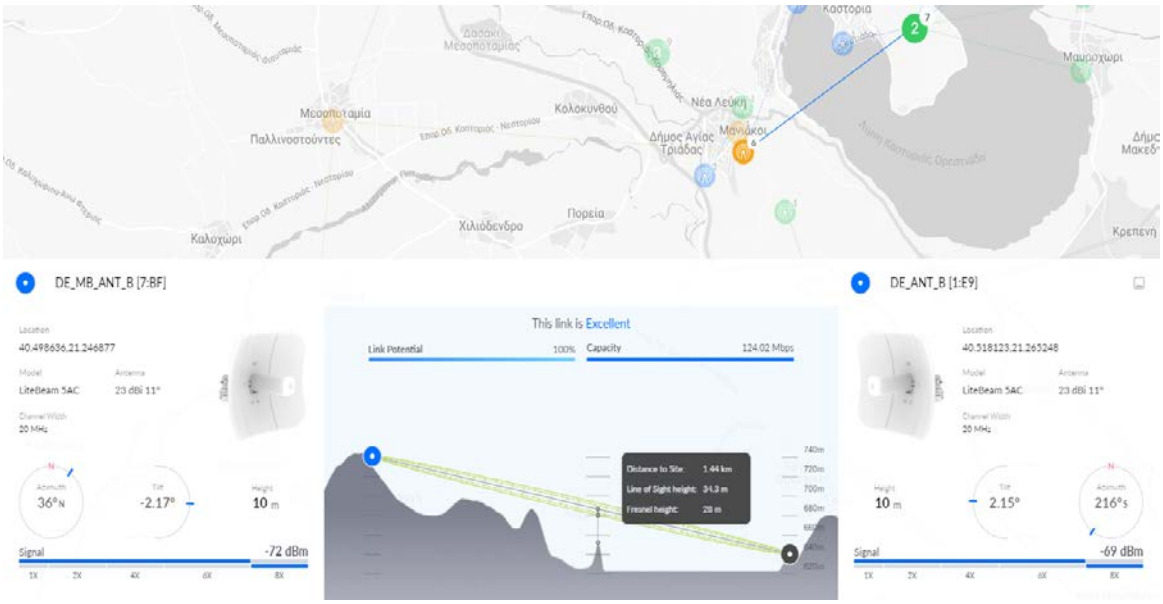
Εικόνα 47. Ubiquiti USIP Τοπολογία στον Χάρτη

Εδώ μπορούμε να δούμε ακριβώς με ένα ιεραρχικό μοντέλο πως ακριβώς είναι συνδεδεμένες μεταξύ τους οι κεραίες.

Εικόνα 48. Ιεραρχική Τοπολογία Δικτύου

Ένα από τα καλύτερα προτερήματα που έχει η συγκεκριμένη εφαρμογή είναι ότι μας δίνει πάρα πολλές πληροφορίες για την σωστή εγκατάσταση των κεραιών αλλά και τι βελτιστοποιήσεις μπορούν να γίνουν μεταγενέστερα όσο το δίκτυο μεγαλώνει. Στην εικόνα βλέπουμε μία σύνδεση μεταξύ δύο κεραιών και πολλές και χρήσιμες πληροφορίες. Αριστερά και δεξιά στην φωτογραφία είναι οι δύο κεραίες με τις πληροφορίες τους και στο κέντρο έχουμε πληροφορίες για την ίδια την σύνδεση. Πληροφορίες για την κεραία έχουμε την τοποθεσία της, το όνομα του μοντέλου της, προς τα που στοχεύει η κεραία και με τι δύναμη, το μέγεθος του καναλιού, το ύψος στο οποίο

βρίσκεται η κεραία, την κλίση που έχει η κεραία αλλά και το πόσο καλό σήμα έχει η κεραία. Στο κέντρο της φωτογραφίας μπορούμε να δούμε κάτι πολύ σημαντικό και αυτό είναι η απεικόνιση του εδάφους και το που ακριβώς βρίσκονται στον χώρο οι κεραίες. Επίσης μπορούμε ανά πάσα στιγμή να επιλέξουμε ένα σημείο και να δούμε την απόσταση που έχει από την κεραία, το ύψος του αλλά και το σημαντικότερο από όλα το ύψος Fresnel. Η ζώνη Fresnel όπως ονομάζεται είναι αρκετά σημαντικός παράγοντας για την σωστή λειτουργία των κεραιών και θα πρέπει να ρυθμιστεί με μεγάλη ακρίβεια αλλιώς δεν θα υπάρχει αξιοπιστία στην σύνδεση.

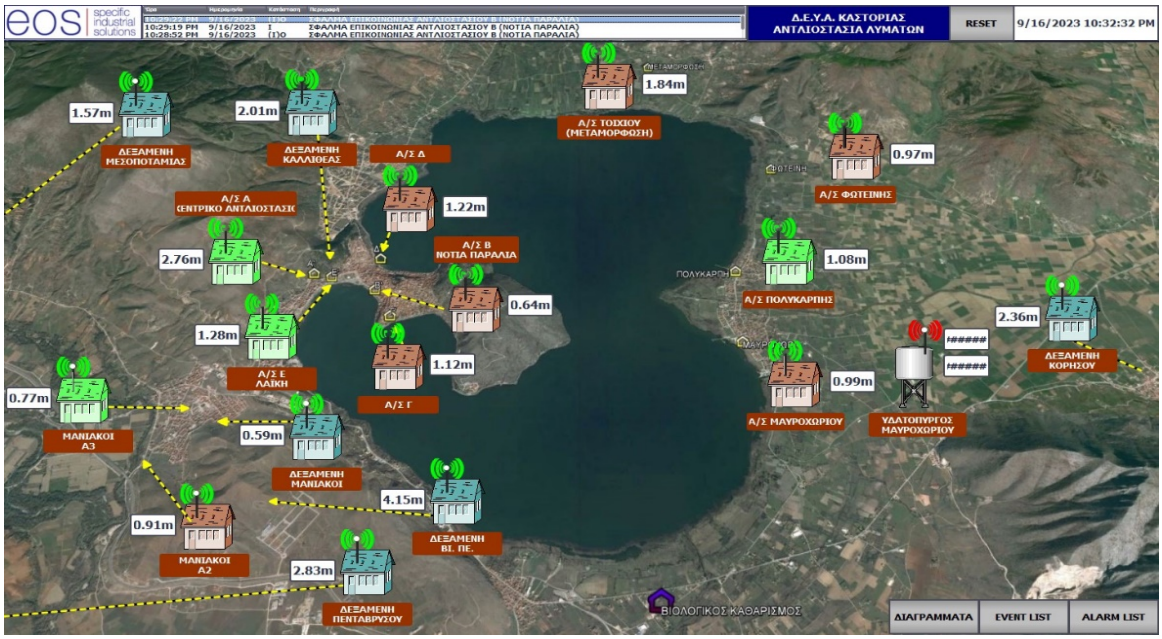


Εικόνα 49. Πληροφορίες Σύνδεσης Μεταξύ Κεραιών

3.5 Εφαρμογή SCADA

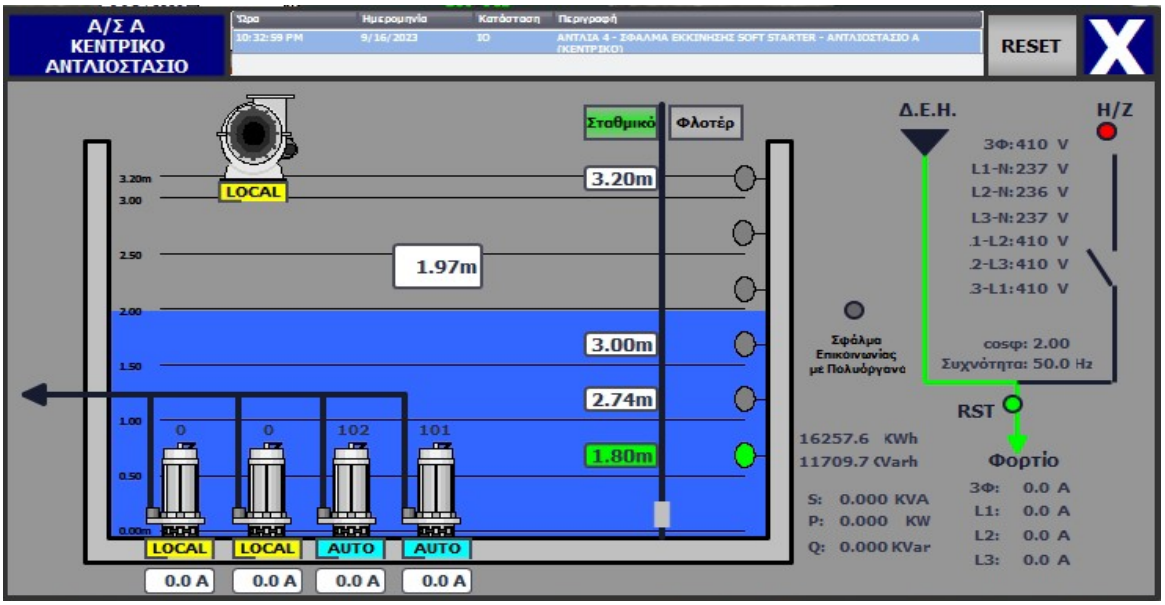
Το πρόγραμμα που έχει χρησιμοποιηθεί για την συλλογή και εμφάνιση δεδομένων ονομάζεται SCADA (Supervisory Control And Data Acquisition). Το 2013 δημοσιεύτηκε το πρωτόκολλο IEC 61131-3 το οποίο ορίζει πέντε γλώσσες προγραμματισμού για τα PLC, FBD (Function Block Diagram), LD (Ladder Diagram), ST (Structured Text, πχ γλώσσα Pascal) IL (Instruction List) SFC (Sequential function chart). [34]

Στην εικόνα 50 βλέπουμε μία αποτύπωση του περιβάλλοντος της εφαρμογής SCADA και πιο συγκεκριμένα τα δεδομένα που αντλούνται με την χρήση PLC (Programmable Logic Controllers), τα οποία είναι εγκατεστημένα σε δεξαμενές, αντλιοστάσια και υδατόπυργους. Αυτά τα δεδομένα αποστέλλονται μέσω των κεραιών πίσω στο κεντρικό υπολογιστή ώστε να εμφανιστούν τα δεδομένα στην εφαρμογή SCADA. Τα PLC μπορούν να προγραμματιστούν σε διάφορες γλώσσες προγραμματισμού όπως ladder logic, Basic ή C και τα προγράμματα δημιουργούνται σε κάποιον υπολογιστή και μετά φορτώνεται στην μνήμη του PLC.



Εικόνα 50. Περιβάλλον SCADA

Στην εικόνα 51 βλέπουμε μία απεικόνιση αντλιοστασίου όπου μπορούμε να δούμε αρκετές πληροφορίες για το αντλιοστάσιο. Το πρόγραμμα μας παρέχει πληροφορίες όπως αν το αντλιοστάσιο παίρνει ρεύμα από την Δ.Ε.Η ή από κάποια γεννήτρια, το ότι είναι τριφασικό ρεύμα και πόσα Volt είναι. Στο αντλιοστάσιο υπάρχουν τέσσερις αντλίες και ένας αποσμητής και μπορούμε να πατήσουμε πάνω και να δούμε πληροφορίες για αυτά. Επίσης μπορούμε να παρακολουθούμε την στάθμη των λυμάτων και να θέσουμε αυτοματισμούς όπως πχ, όταν έχει ανέβει αρκετά η στάθμη να ανοίγει κάποια βάνα.



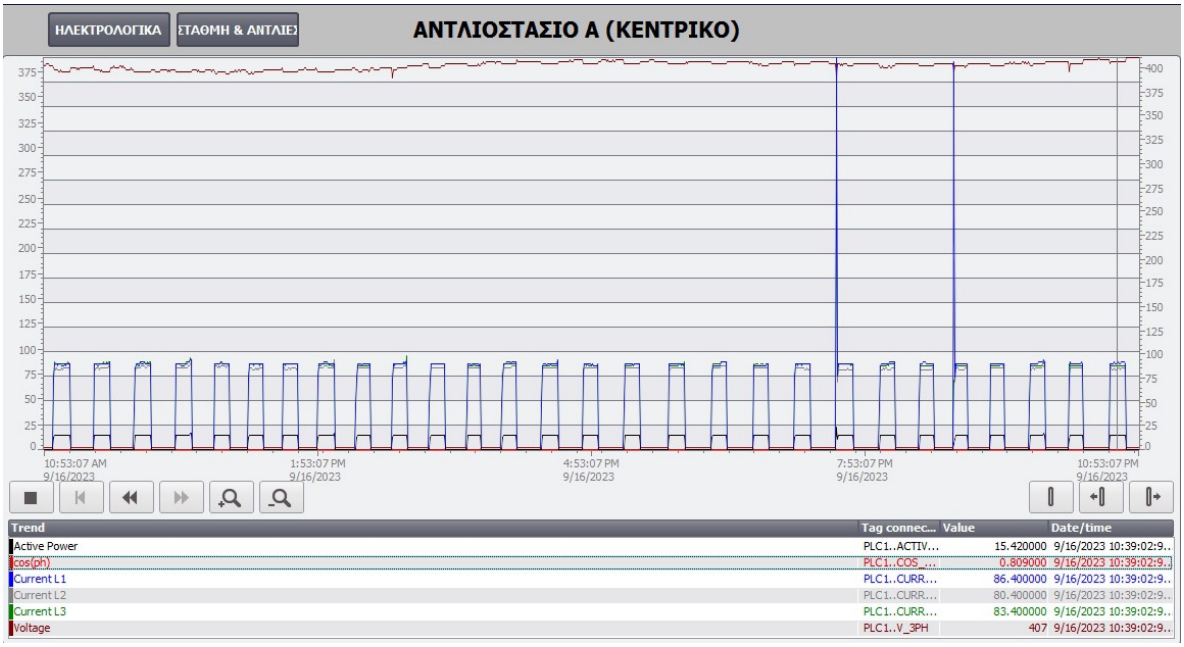
Εικόνα 51. Απεικόνιση Αντλιοστασίου

Το πρόγραμμα υποστηρίζει επίσης την δυνατότητα να μπορούμε να δημιουργήσουμε αυτοματισμούς αλλά και να μπορούμε να επέμβουμε απομακρυσμένα σε κάποιο

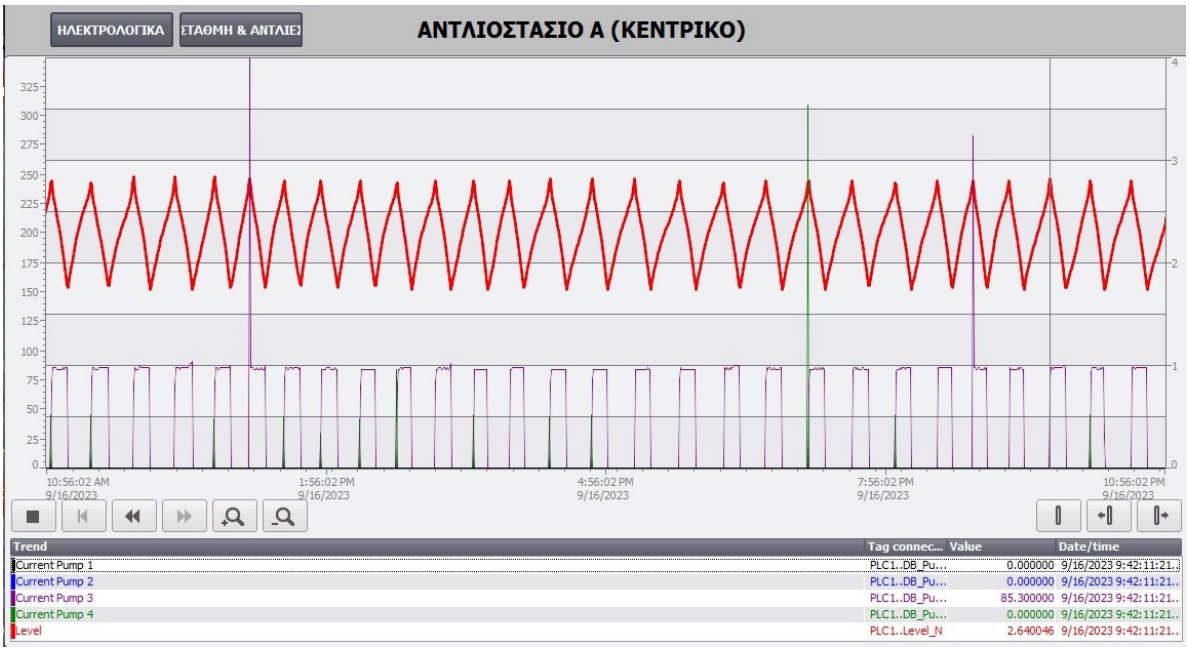
αντικείμενο όπως μία αντλία. Μας δίνει την δυνατότητα να ξεκινήσουμε ή να σταματήσουμε απομακρυσμένα την αντλία αλλά και να την θέσουμε σε χειροκίνητη λειτουργία. Μερικά από τα δεδομένα που μπορούμε να αντλήσουμε είναι πόσες ώρες είναι σε λειτουργία η αντλία, πόσο ρεύμα καταναλώνει, την ισχύ αλλά και το φορτίο. Επίσης υπάρχουν ενδείξεις για διάφορα σφάλματα που μπορεί να προκύψουν ώστε να μπορεί ο χρήστης να γνωρίζει απομακρυσμένα τι πάει λάθος.

Εικόνα 52. Απεικόνιση αντλίας

Στα αντλιοστάσια μπορούμε επίσης να έχουμε και διαγράμματα με δεδομένα όπως ηλεκτρολογικά, στάθμη και αντλίες. Παρακάτω στην εικόνα 53 μπορούμε να δούμε στο διάγραμμα στον άξονα χ την ώρα και την ημερομηνία και στον άξονα ψ την τιμή που παίρνει από το PLC.

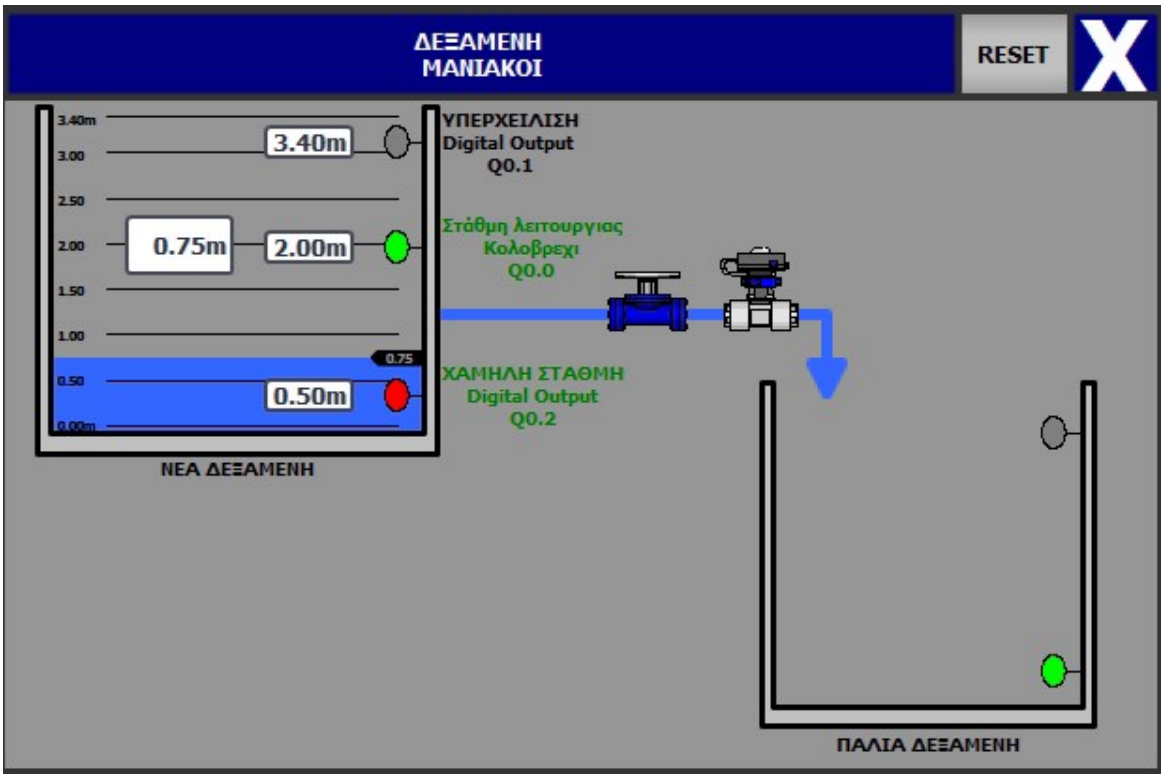


Εικόνα 53. Ηλεκτρολογικό διάγραμμα



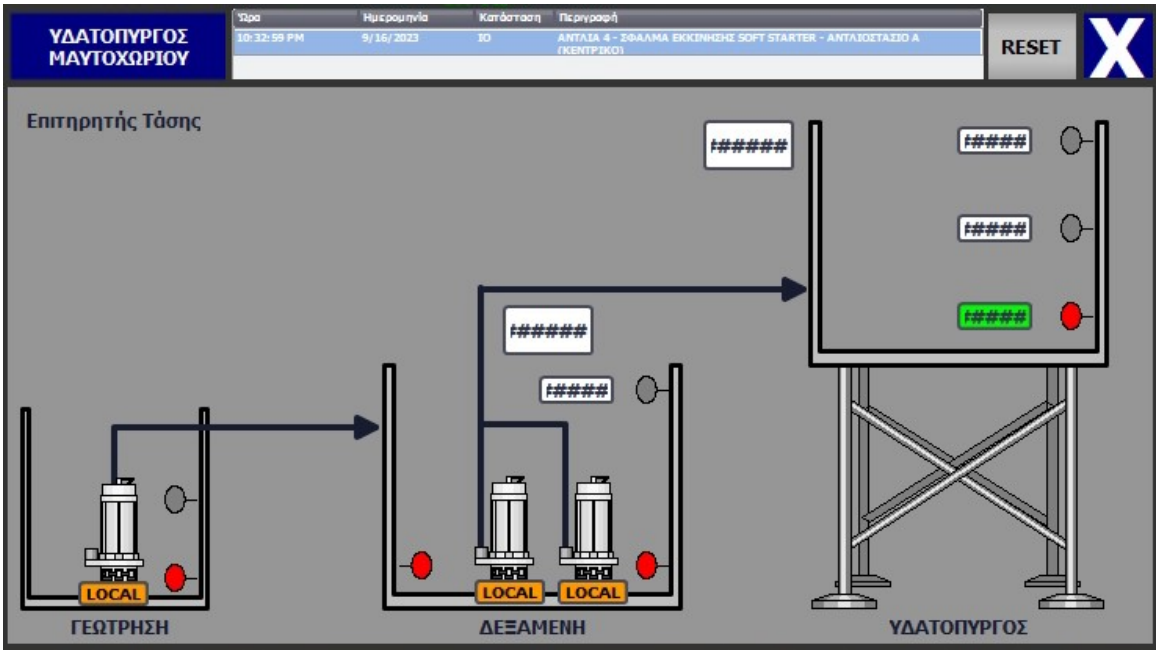
Εικόνα 54. Διάγραμμα στάθμη & Αντλίες

Εκτός από αντλιοστάσια στο SCADA υπάρχουν και δεξαμενές που πρέπει να έχουμε πληροφορίες για αυτά και να δημιουργήσουμε αυτοματισμούς. Στην εικόνα 55 βλέπουμε ότι στην δεξαμενή μπορούμε να δημιουργήσουμε έναν αυτοματισμό που όταν η στάθμη φτάσει σε ένα συγκεκριμένο σημείο να αδειάζει το νερό σε μία άλλη δεξαμενή.



Εικόνα 55. Απεικόνιση δεξαμενής

Ακόμα ένα κτήριο που υπάρχει στο SCADA είναι ο υδατόπυργος και μπορούμε να πάρουμε πληροφορίες για την γεώτρηση, την δεξαμενή αλλά και τον ίδιο τον υδατόπυργο.



Εικόνα 56. Απεικόνιση υδατόπυργου

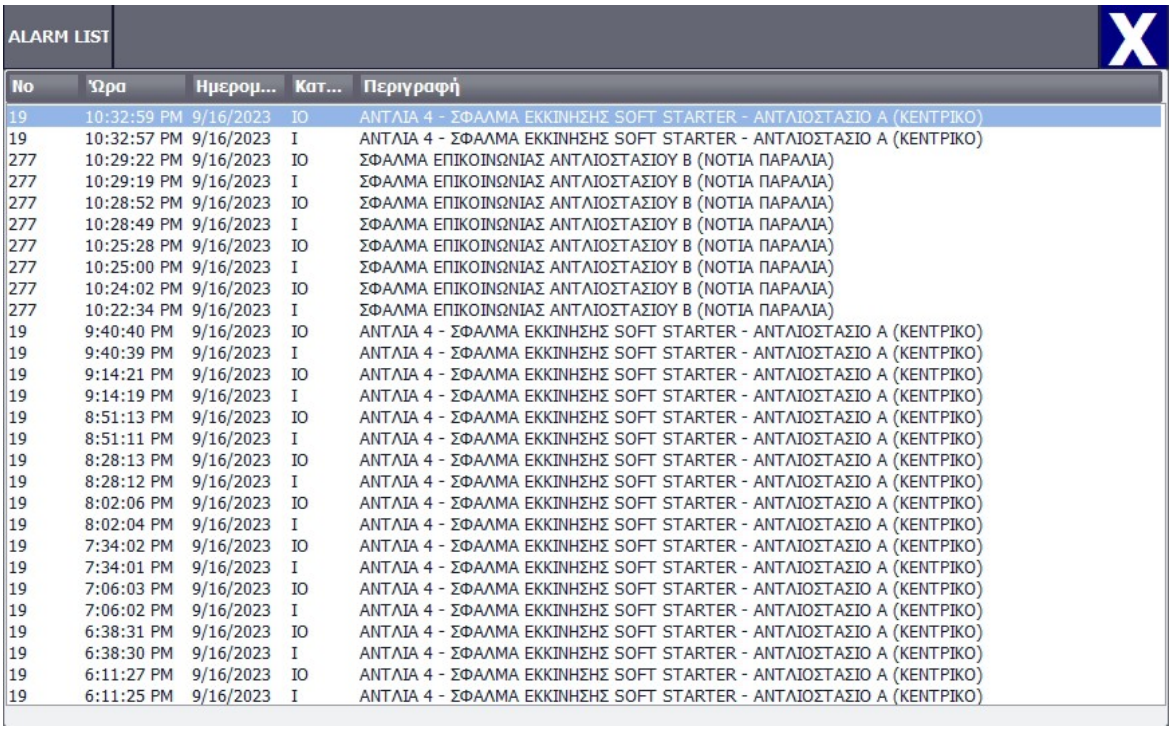
Τέλος στην αρχική οθόνη του προγράμματος υπάρχει ένα κουμπί που μπορούμε να επιλέξουμε σε πιο κτήριο θέλουμε να δούμε μία λίστα με γεγονότα. Τα γεγονότα αυτά μπορούμε εμείς να τα ορίσουμε πια θα είναι και να μας ενημερώνει όταν χρειάζεται.

EVENT LIST — ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)

No	Ώρα	Ημερομ...	Κατ...	Περιγραφή
536	10:44:13 PM	9/16/2023	I	ΑΝΑΛΟΓΙΚΗ ΣΤΑΘΜΗ LL - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
521	10:43:06 PM	9/16/2023	IO	ΑΝΤΛΙΑ 3 - FEEDBACK - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
520	10:43:06 PM	9/16/2023	IO	ΑΝΤΛΙΑ 3 - ΕΝΤΟΛΗ ΕΚΚΙΝΗΣΗΣ - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
536	10:42:55 PM	9/16/2023	IO	ΑΝΑΛΟΓΙΚΗ ΣΤΑΘΜΗ LL - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
541	10:35:40 PM	9/16/2023	IO	ΦΛΟΤΕΡ H1 - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
537	10:33:31 PM	9/16/2023	IO	ΑΝΑΛΟΓΙΚΗ ΣΤΑΘΜΗ H1 - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
521	10:33:02 PM	9/16/2023	I	ΑΝΤΛΙΑ 3 - FEEDBACK - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
527	10:32:57 PM	9/16/2023	IO	ΑΝΤΛΙΑ 4 - ΕΝΤΟΛΗ ΕΚΚΙΝΗΣΗΣ - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
520	10:32:57 PM	9/16/2023	I	ΑΝΤΛΙΑ 3 - ΕΝΤΟΛΗ ΕΚΚΙΝΗΣΗΣ - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
528	10:32:47 PM	9/16/2023	IO	ΑΝΤΛΙΑ 4 - FEEDBACK - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
528	10:32:32 PM	9/16/2023	I	ΑΝΤΛΙΑ 4 - FEEDBACK - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
537	10:32:29 PM	9/16/2023	I	ΑΝΑΛΟΓΙΚΗ ΣΤΑΘΜΗ H1 - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
527	10:32:29 PM	9/16/2023	I	ΑΝΤΛΙΑ 4 - ΕΝΤΟΛΗ ΕΚΚΙΝΗΣΗΣ - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
541	10:32:22 PM	9/16/2023	I	ΦΛΟΤΕΡ H1 - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
536	10:16:44 PM	9/16/2023	I	ΑΝΑΛΟΓΙΚΗ ΣΤΑΘΜΗ LL - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
521	10:15:38 PM	9/16/2023	IO	ΑΝΤΛΙΑ 3 - FEEDBACK - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
520	10:15:38 PM	9/16/2023	IO	ΑΝΤΛΙΑ 3 - ΕΝΤΟΛΗ ΕΚΚΙΝΗΣΗΣ - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
536	10:15:28 PM	9/16/2023	IO	ΑΝΑΛΟΓΙΚΗ ΣΤΑΘΜΗ LL - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
541	10:09:14 PM	9/16/2023	IO	ΦΛΟΤΕΡ H1 - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
537	10:07:19 PM	9/16/2023	IO	ΑΝΑΛΟΓΙΚΗ ΣΤΑΘΜΗ H1 - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
521	10:06:48 PM	9/16/2023	I	ΑΝΤΛΙΑ 3 - FEEDBACK - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
527	10:06:43 PM	9/16/2023	IO	ΑΝΤΛΙΑ 4 - ΕΝΤΟΛΗ ΕΚΚΙΝΗΣΗΣ - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
520	10:06:43 PM	9/16/2023	I	ΑΝΤΛΙΑ 3 - ΕΝΤΟΛΗ ΕΚΚΙΝΗΣΗΣ - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
528	10:06:31 PM	9/16/2023	IO	ΑΝΤΛΙΑ 4 - FEEDBACK - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
528	10:06:16 PM	9/16/2023	I	ΑΝΤΛΙΑ 4 - FEEDBACK - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
537	10:06:14 PM	9/16/2023	I	ΑΝΑΛΟΓΙΚΗ ΣΤΑΘΜΗ H1 - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
527	10:06:14 PM	9/16/2023	I	ΑΝΤΛΙΑ 4 - ΕΝΤΟΛΗ ΕΚΚΙΝΗΣΗΣ - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
541	10:06:11 PM	9/16/2023	I	ΦΛΟΤΕΡ H1 - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)

Εικόνα 57. Λίστα γεγονότων

Επίσης υπάρχει και άλλο ένα κουμπί που εμφανίζονται τα σφάλματα σε όλα τα κτήρια που υπάρχουν στο πρόγραμμα και μπορούμε να τα έχουμε σαν σημείο αναφοράς όταν χρειαστεί. Μία μελλοντική επέκταση της λίστας σφαλμάτων θα ήταν να μπορεί να στέλνει μήνυμα sms στον χρήστη όταν συμβαίνουν πολύ σημαντικά σφάλματα ώστε να μπορεί να πάρει γρήγορα τα απαραίτητα μέτρα. Το s.c.a.d.a υποστηρίζει αυτήν την δυνατότητα και είναι απαραίτητο να υπάρχει εάν δεν υπάρχει κάποιος να επιβλέπει το δίκτυο όλη μέρα.



No	Ώρα	Ημερομ...	Κατ...	Περιγραφή
19	10:32:59 PM	9/16/2023	IO	ΑΝΤΛΙΑ 4 - ΣΦΑΛΜΑ ΕΚΚΙΝΗΣΗΣ SOFT STARTER - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
19	10:32:57 PM	9/16/2023	I	ΑΝΤΛΙΑ 4 - ΣΦΑΛΜΑ ΕΚΚΙΝΗΣΗΣ SOFT STARTER - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
277	10:29:22 PM	9/16/2023	IO	ΣΦΑΛΜΑ ΕΠΙΚΟΙΝΩΝΙΑΣ ΑΝΤΛΙΟΣΤΑΣΙΟΥ Β (ΝΟΤΙΑ ΠΑΡΑΛΙΑ)
277	10:29:19 PM	9/16/2023	I	ΣΦΑΛΜΑ ΕΠΙΚΟΙΝΩΝΙΑΣ ΑΝΤΛΙΟΣΤΑΣΙΟΥ Β (ΝΟΤΙΑ ΠΑΡΑΛΙΑ)
277	10:28:52 PM	9/16/2023	IO	ΣΦΑΛΜΑ ΕΠΙΚΟΙΝΩΝΙΑΣ ΑΝΤΛΙΟΣΤΑΣΙΟΥ Β (ΝΟΤΙΑ ΠΑΡΑΛΙΑ)
277	10:28:49 PM	9/16/2023	I	ΣΦΑΛΜΑ ΕΠΙΚΟΙΝΩΝΙΑΣ ΑΝΤΛΙΟΣΤΑΣΙΟΥ Β (ΝΟΤΙΑ ΠΑΡΑΛΙΑ)
277	10:25:28 PM	9/16/2023	IO	ΣΦΑΛΜΑ ΕΠΙΚΟΙΝΩΝΙΑΣ ΑΝΤΛΙΟΣΤΑΣΙΟΥ Β (ΝΟΤΙΑ ΠΑΡΑΛΙΑ)
277	10:25:00 PM	9/16/2023	I	ΣΦΑΛΜΑ ΕΠΙΚΟΙΝΩΝΙΑΣ ΑΝΤΛΙΟΣΤΑΣΙΟΥ Β (ΝΟΤΙΑ ΠΑΡΑΛΙΑ)
277	10:24:02 PM	9/16/2023	IO	ΣΦΑΛΜΑ ΕΠΙΚΟΙΝΩΝΙΑΣ ΑΝΤΛΙΟΣΤΑΣΙΟΥ Β (ΝΟΤΙΑ ΠΑΡΑΛΙΑ)
277	10:22:34 PM	9/16/2023	I	ΣΦΑΛΜΑ ΕΠΙΚΟΙΝΩΝΙΑΣ ΑΝΤΛΙΟΣΤΑΣΙΟΥ Β (ΝΟΤΙΑ ΠΑΡΑΛΙΑ)
19	9:40:40 PM	9/16/2023	IO	ΑΝΤΛΙΑ 4 - ΣΦΑΛΜΑ ΕΚΚΙΝΗΣΗΣ SOFT STARTER - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
19	9:40:39 PM	9/16/2023	I	ΑΝΤΛΙΑ 4 - ΣΦΑΛΜΑ ΕΚΚΙΝΗΣΗΣ SOFT STARTER - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
19	9:14:21 PM	9/16/2023	IO	ΑΝΤΛΙΑ 4 - ΣΦΑΛΜΑ ΕΚΚΙΝΗΣΗΣ SOFT STARTER - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
19	9:14:19 PM	9/16/2023	I	ΑΝΤΛΙΑ 4 - ΣΦΑΛΜΑ ΕΚΚΙΝΗΣΗΣ SOFT STARTER - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
19	8:51:13 PM	9/16/2023	IO	ΑΝΤΛΙΑ 4 - ΣΦΑΛΜΑ ΕΚΚΙΝΗΣΗΣ SOFT STARTER - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
19	8:51:11 PM	9/16/2023	I	ΑΝΤΛΙΑ 4 - ΣΦΑΛΜΑ ΕΚΚΙΝΗΣΗΣ SOFT STARTER - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
19	8:28:13 PM	9/16/2023	IO	ΑΝΤΛΙΑ 4 - ΣΦΑΛΜΑ ΕΚΚΙΝΗΣΗΣ SOFT STARTER - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
19	8:28:12 PM	9/16/2023	I	ΑΝΤΛΙΑ 4 - ΣΦΑΛΜΑ ΕΚΚΙΝΗΣΗΣ SOFT STARTER - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
19	8:02:06 PM	9/16/2023	IO	ΑΝΤΛΙΑ 4 - ΣΦΑΛΜΑ ΕΚΚΙΝΗΣΗΣ SOFT STARTER - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
19	8:02:04 PM	9/16/2023	I	ΑΝΤΛΙΑ 4 - ΣΦΑΛΜΑ ΕΚΚΙΝΗΣΗΣ SOFT STARTER - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
19	7:34:02 PM	9/16/2023	IO	ΑΝΤΛΙΑ 4 - ΣΦΑΛΜΑ ΕΚΚΙΝΗΣΗΣ SOFT STARTER - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
19	7:34:01 PM	9/16/2023	I	ΑΝΤΛΙΑ 4 - ΣΦΑΛΜΑ ΕΚΚΙΝΗΣΗΣ SOFT STARTER - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
19	7:06:03 PM	9/16/2023	IO	ΑΝΤΛΙΑ 4 - ΣΦΑΛΜΑ ΕΚΚΙΝΗΣΗΣ SOFT STARTER - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
19	7:06:02 PM	9/16/2023	I	ΑΝΤΛΙΑ 4 - ΣΦΑΛΜΑ ΕΚΚΙΝΗΣΗΣ SOFT STARTER - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
19	6:38:31 PM	9/16/2023	IO	ΑΝΤΛΙΑ 4 - ΣΦΑΛΜΑ ΕΚΚΙΝΗΣΗΣ SOFT STARTER - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
19	6:38:30 PM	9/16/2023	I	ΑΝΤΛΙΑ 4 - ΣΦΑΛΜΑ ΕΚΚΙΝΗΣΗΣ SOFT STARTER - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
19	6:11:27 PM	9/16/2023	IO	ΑΝΤΛΙΑ 4 - ΣΦΑΛΜΑ ΕΚΚΙΝΗΣΗΣ SOFT STARTER - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)
19	6:11:25 PM	9/16/2023	I	ΑΝΤΛΙΑ 4 - ΣΦΑΛΜΑ ΕΚΚΙΝΗΣΗΣ SOFT STARTER - ΑΝΤΛΙΟΣΤΑΣΙΟ Α (ΚΕΝΤΡΙΚΟ)

Εικόνα 58. Λίστα σφαλμάτων

Συμπεράσματα

Τα ασύρματα δίκτυα αισθητήρων αποτελούν μία τεχνολογία που σιγά σιγά μπαίνει όλο και περισσότερο στις ζωές μας και τα τελευταία χρόνια εξελίσσεται με γρήγορους ρυθμούς. Όσο μειώνεται το κόστος των υλικών για την δημιουργία ενός τέτοιου δικτύου γίνεται περισσότερο προσβάσιμο ώστε να δώσει λύσεις σε επιστημονικά και εμπορικά προβλήματα μιας και οι αισθητήρες γίνονται φθηνότεροι και καλύτερη στην ακρίβεια των δεδομένων που καταγράφουν.

Ένα από τα προβλήματα που πρέπει να αντιμετωπίσει κάποιος είναι το δυσπρόσιτο και συνήθως επιθετικό περιβάλλον που πρέπει να εγκατασταθούν τέτοια δίκτυα ώστε να μπορεί να γίνει η λειτουργία τους απομακρυσμένα χωρίς κάποια φυσική παρουσία. Το αποτέλεσμα όμως δικαιώνει την προσπάθεια για την δημιουργία ενός τέτοιου δικτύου. Το υλικό που χρησιμοποιείται γίνεται ολοένα και καλύτερο ώστε να είναι πιο ανθεκτικό στο πέρασμα του χρόνου σε ένα απομακρυσμένο και επιθετικό περιβάλλον αλλά επίσης και αρκετά δυνατό στο κομμάτι της υπολογιστικής ισχύς, της κατανάλωσης ενέργειας αλλά και της μνήμης. Η τοπολογία λόγω της μορφολογίας της περιοχής χρειάζεται να αλλάζει οπότε θα πρέπει να είναι δυναμική.

Η τεχνολογία βέβαια αναπτύσσεται οπότε πάντα θα υπάρχουν βελτιώσεις σε τωρινά προβλήματα που αντιμετωπίζουν τα δίκτυα αυτά. Όπως και τα ασύρματα δίκτυα αισθητήρων έτσι και στο Internet of Things είναι ένας τομέας της τεχνολογίας που χρησιμοποιείται αρκετά τα τελευταία χρόνια και έχει κάνει τεράστια τεχνολογικά άλματα όχι μόνο σε εμπορικές η επιστημονικές λύσεις αλλά και σε προσωπικές με μία πληθώρα εφαρμογών που ο κόσμος έχει μία πιο άμεση επαφή.

Όσο αναπτύσσονται βέβαια καινούργιες τεχνολογίες και πλέον χρησιμοποιούνται σε όλο και περισσότερες εφαρμογές γίνονται και στόχος κακόβουλών χρηστών. Αυτό έχει σαν αποτέλεσμα να πρέπει να δημιουργηθούν πρωτόκολλα και διαδικασίες ασφαλείας ώστε η εκάστοτε εφαρμογή να είναι ασφαλείς. Υπάρχουν πολλών ειδών επιθέσεων και σε πολλαπλά επίπεδα όχι μόνο στο κομμάτι του δικτύου αλλά και στο κομμάτι των κόμβων αισθητήρων, οπότε είναι ένας δύσκολος τομέας που θέλει πολύ προετοιμασία. Η ανάγκη για ασφάλεια δεν θα σταματήσει ποτέ και πλέον υπάρχει ένας αγώνας και από την πλευρά τον επιτιθέμενων αλλά και από την πλευρά των αμυνόμενων για την ασφάλεια.

Τέλος στο κομμάτι της μελέτης περίπτωσης που έγινε σε τοπική επιχείρηση αναλύθηκε το κομμάτι του ασύρματου δικτύου αισθητήρων, των υλικών που χρησιμοποιήθηκαν αλλά και το πρόγραμμα για την εμφάνιση των δεδομένων. Η διαχείριση του δικτύου γίνεται τελείως απομακρυσμένα, όπως και η εφαρμογή για την καταγραφή και εμφάνιση των δεδομένων (SCADA). Επίσης, το σύστημα SCADA παρέχει τη δυνατότητα για τη δημιουργία αυτοματισμών καθιστώντας την εγκατάσταση σε ένα

πολύ μεγάλο βαθμό αυτόματη. Η υλοποίηση του δικτύου είναι αρκετά δυναμική και μπορεί χωρίς κανένα πρόβλημα να υποστηρίξει μεγαλύτερες ανάγκες σε μελλοντικό χρόνο, όπως το ίδιο ισχύει και για το σύστημα SCADA.

Προτάσεις Μελλοντικής Επέκτασης

Τα ασύρματα δίκτυα αισθητήρων έχουν ευρύ πεδίο εφαρμογών και στα πλαίσια αυτής της πτυχιακής εργασίας δεν μπορούν δυστυχώς να αναλυθούν όλες σε πάρα πολύ μεγάλο βαθμό. Στο μέλλον θα μπορούσε να γίνει μία πιο εκτεταμένη συγκριτική μελέτη περιπτώσεων των υλοποιήσεων ασύρματων δίκτυα αισθητήρων, σε ποικίλους τομείς εφαρμογών, καθώς επίσης και μεγαλύτερη και εις βάθος ανάλυση των πρωτοκόλλων επικοινωνίας και να γίνουν αντίστοιχα πειράματα για το ποιο είναι πιο αποτελεσματικό πρωτόκολλο για τη μετάδοση δεδομένων σε σχέση με την κατανάλωση ενέργειας.

Μια επιπλέον επέκταση που θα μπορούσε να γίνει όσον αφορά τη συγκριτική μελέτη των λειτουργικών συστημάτων των ασύρματων δικτύων αισθητήρων, όπως TinyOs, SOS, Contiki, LiteOS. Πως ακριβώς λειτουργούν, ποια είναι η αρχιτεκτονική τους ποια τα υπέρ και τα κατά στο να υπάρχουν σε ένα δίκτυο, πως διαχειρίζονται τα δεδομένα, την ενέργεια, την μνήμη και πως γίνεται ο προγραμματισμός τους.

Στην παρούσα πτυχιακή εργασία, όπως και στα περισσότερα πρωτόκολλα θεωρούμε ότι οι κόμβοι αισθητήρων και οι σταθμοί βάσης βρίσκονται σε σταθερές θέσεις. Όμως, υπάρχουν περιπτώσεις εφαρμογών ασύρματων δίκτυα αισθητήρων, όπως σε στρατιωτικές εφαρμογές, όπου οι κόμβοι αισθητήρων και οι σταθμοί βάσης θα πρέπει να μπορούν να μετακινηθούν ανά πάσα στιγμή. Αυτό έχει μεγάλο αντίκτυπο στην τοπολογία του δικτύου, όπως και στα πρωτόκολλα δρομολόγησης, διότι θα πρέπει να εξεταστεί η αποδοτική λειτουργία τους και να αντιμετωπιστούν οι προκλήσεις ως προς την ασφάλειά τους.

Τέλος, στον τομέα της ασφάλειας θα μπορούσε να γίνει επέκταση με πειράματα και μεγαλύτερη ανάλυση για την επιλογή των καταλληλότερων μηχανισμών ασφαλείας και κρυπτογραφικών μεθόδων, ανάλογα με το είδος των ασύρματων δικτύων αισθητήρων και των πεδίων εφαρμογής τους.

Βιβλιογραφία

[1] Dr.E.N.Ganesh, «Wireless Sensor Network: The Challenges of Design and Programmability,» Μάρτιος 2017. [Ηλεκτρονικό]. Available: https://www.researchgate.net/publication/316877046_Wireless_Sensor_Network_The_Challenges_of_Design_and_Programmability. [Πρόσβαση 19 03 2023].

[2] W. &. P. C. Dargie, «Fundamentals of Wireless Sensor Networks: Theory and Practice,» 2011. [Ηλεκτρονικό]. Available: https://www.researchgate.net/publication/261958666_Fundamentals_of_Wireless_Sensor_Networks_Theory_and_Practice. [Πρόσβαση 20 03 2023].

[3] I. Silicon Laboratories, «The Evolution of Wireless Sensor Networks,» 2013. [Ηλεκτρονικό]. Available: https://www.silabs.com/documents/public/white-papers/evolution-of-wireless-sensor-networks.pdf. [Πρόσβαση 26 3 2023].

[4] C. N. D. V. a. G. K. D. Kandris, «Applications of Wireless Sensor Networks: An Up-to-Date Survey,» Φεβρουάριος 2020. [Ηλεκτρονικό]. Available: https://www.mdpi.com/2571-5577/3/1/14. [Πρόσβαση 19 04 2023].

[5] Geomatics, «Εφαρμογές Lidar,» 2013. [Ηλεκτρονικό]. Available: http://www.geomatics.gr/el/%CF%85%CF%80%CE%B7%CF%81%CE%B5%CF%83%CE%AF%CE%B5%CF%82/%CE%B5%CF%86%CE%B1%CF%81%CE%BC%CE%BF%CE%B3%CE%AD%CF%82_lidar. [Πρόσβαση 23 04 2023].

[6] X. H. D. S. H. C. Muhammad R Ahmed, «Wireless Sensor Network: Characteristics and Architectures,» 2012. [Ηλεκτρονικό]. Available: https://publications.waset.org/9345/wireless-sensor-network-characteristics-and-architectures. [Πρόσβαση 29 04 2023].

[7] S. D. V. D. Sumit Kumar, «The OSI model: Overview on the seven layers of computer networks,» 2014. [Ηλεκτρονικό]. Available: https://www.researchpublish.com/upload/book/THE%20OSI%20MODEL%20OVERVIEW%20ON%20THE%20SEVEN%20LAYERS-607.pdf. [Πρόσβαση 7 05 2023].

[8] D. M. M. Maitri Rashmikant Sakarvadia, «NETWORK TOPOLOGIES IN WIRELESS SENSOR NETWORK,» 2022. [Ηλεκτρονικό]. Available: https://ijcrt.org/papers/IJCRT2205629.pdf. [Πρόσβαση 30 05 2023].

[9] A. S. A. G. P. H. Opeyemi Osanaiye, «Denial of Service (DoS) Defence for Resource Availability in Wireless Sensor Networks,» 2018. [Ηλεκτρονικό]. Available:

https://www.researchgate.net/publication/322668253_Denial_of_Service_DoS_Defence_for_Resource_Availability_in_Wireless_Sensor_Networks. [Πρόσβαση 24 6 2023].

[10] P. P. V. W. C. S. C. A. G. Y. F. H. Paolo Baronti, «Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards,» 2007. [Ηλεκτρονικό]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0140366406004749 . [Πρόσβαση 20 07 2023].

[11] P. K. S. S. P. S. Aarti Kochhar, «Protocols for Wireless Sensor Networks: A Survey,» 2018. [Ηλεκτρονικό]. Available: https://jtit.pl/jtit/article/view/599. [Πρόσβαση 07 06 2023].

[12] D. K. Tarunpreet Kaur, «TDMA-based MAC protocols for wireless sensor networks: A survey and comparative analysis,» 2016. [Ηλεκτρονικό]. Available: https://ieeexplore.ieee.org/document/7993426. [Πρόσβαση 6 17 2023].

[13] G. K. G. S. Aseem Kaushal, «Spread Spectrum,» 2013. [Ηλεκτρονικό]. Available: http://www.iject.org/vol4/spl2/aseem.pdf. [Πρόσβαση 17 6 2023].

[14] K. Benkic, «Proposed use of a CDMA technique in wireless sensor networks,» 2007. [Ηλεκτρονικό]. Available: https://ieeexplore.ieee.org/abstract/document/4381112. [Πρόσβαση 17 6 2023].

[15] M. A. Ahlam Saud Althobaiti, «Medium Access Control Protocols for Wireless Sensor Networks Classifications and Cross-Layering,» 2015. [Ηλεκτρονικό]. Available: https://www.sciencedirect.com/science/article/pii/S1877050915029002?ref=pdf_download&fr=RR-2&rr=7d8d862d1c17eefc. [Πρόσβαση 18 6 2023].

[16] C. P. P. N. K. Joice Olempia, «A Survey on Energy Efficient Contention based and Hybrid MAC Protocols for Wireless Sensor Networks,» 2016. [Ηλεκτρονικό]. Available: https://indjst.org/articles/a-survey-on-energy-efficient-contention-based-and-hybrid-mac-protocols-for-wireless-sensor-networks. [Πρόσβαση 18 6 2023].

[17] S. V. N. M. Rajesh Yadav, «A SURVEY OF MAC PROTOCOLS FOR WIRELESS SENSOR,» 2009. [Ηλεκτρονικό]. Available: https://www.specialcabledeals.com/assets/pdf/11_339.pdf. [Πρόσβαση 21 6 2023].

[18] O. D. I. C. E. M. Aykut Yigitel, «QoS-aware MAC protocols for wireless sensor networks: A survey,» 2011. [Ηλεκτρονικό]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1389128611000703. [Πρόσβαση 27 6 2023].

[19] «learnmech.com,» 2023. [Ηλεκτρονικό]. Available: https://learnmech.com/types-of-actuators-function-of-actuators-used-in-machines/. [Πρόσβαση 22 6 2023].

[20] S. R. S. Pallavi Sethi, «Internet of Things: Architectures, Protocols, and Applications,» 2017. [Ηλεκτρονικό]. Available: https://www.hindawi.com/journals/jece/2017/9324035/. [Πρόσβαση 24 7 2023].

[21] A. J. Jun Zheng, «Wireless sensor networks : a networking perspective,» 2015. [Ηλεκτρονικό]. Available: https://worldcat.org/title/1127206856. [Πρόσβαση 19 7 2023].

[22] F. E. G. S.-K. G. E. B. B. A. D. Kofi Sarpong Adu-Manu, «WSN Protocols and Security Challenges for Environmental Monitoring Applications: A Survey,» 2022. [Ηλεκτρονικό]. Available: https://www.hindawi.com/journals/js/2022/1628537/. [Πρόσβαση 24 7 2023].

[23] «Assess your project's needs,» [Ηλεκτρονικό]. Available: https://build.sigfox.com/study. [Πρόσβαση 29 07 2023].

[24] «Difference between Wireless Sensor Networks (WSN) and IoT,» 8 3 2023. [Ηλεκτρονικό]. Available: https://mimlearnovate.com/difference-between-wireless-sensor-networks-and-iot/. [Πρόσβαση 29 7 2023].

[25] A. A.-J. M. R. I. M. E. H. A. N. K. H. B. M. A. Burhanuddin, «A Review on Security Challenges and Features in Wireless Sensor Networks: IoT Perspective,» 2018. [Ηλεκτρονικό]. Available: https://jtec.utem.edu.my/jtec/article/view/3589. [Πρόσβαση 25 07 2023].

[26] S. N. S. Parli B. Hari, «Security issues in Wireless Sensor Networks: Current research and challenges,» 2016 . [Ηλεκτρονικό]. Available: https://ieeexplore.ieee.org/abstract/document/7578876. [Πρόσβαση 18 07 2023].

[27] S. S. Jitender Grover, «Security issues in Wireless Sensor Network - A review,» 2016. [Ηλεκτρονικό]. Available: https://ieeexplore.ieee.org/abstract/document/7784988. [Πρόσβαση 7 7 2023].

[28] R. S. A. M. Hero Modares, «Overview of Security Issues in Wireless Sensor Networks,» 2011. [Ηλεκτρονικό]. Available: https://ieeexplore.ieee.org/document/6076376. [Πρόσβαση 7 2023].

[29] A. Z. Tanveer Zia, «Security Issues in Wireless Sensor Networks,» 2006. [Ηλεκτρονικό]. Available: https://ieeexplore.ieee.org/abstract/document/4041555. [Πρόσβαση 8 7 2023].

[30] M. M. Q. S. D. L.-J. Kashif Kifayat, «Security in Wireless Sensor Networks,» 2010. [Ηλεκτρονικό]. Available: https://link.springer.com/chapter/10.1007/978-3-642-04117-4_26. [Πρόσβαση 10 7 2023].

[31] «Ταυτότητα,» 2023. [Ηλεκτρονικό]. Available: https://www.deyakastorias.gr/tautotita. [Πρόσβαση 30 7 2023].

[32] mikrotik, «hAP lite,» 2023. [Ηλεκτρονικό]. Available: https://mikrotik.com/product/RB941-2nD. [Πρόσβαση 5 8 2023].

[33] «ubnt.com,» 2023. [Ηλεκτρονικό]. Available: https://dl.ubnt.com/datasheets/LiteBeam/LiteBeam_DS.pdf. [Πρόσβαση 10 8 2023].

[34] P. &. S. P. &. L. C. &. D. P. &. T. S. Kadam, «PLC & SCADA, a Case Study: -Autoclave Automation,» 2008. [Ηλεκτρονικό]. Available: https://www.researchgate.net/publication/296754469_PLC_SCADA_a_Case_Study_-Autoclave_Automation. [Πρόσβαση 23 09 2023].