



ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Τεχνολογίες Ασύρματης Διασύνδεσης Αισθητήρων στο Διαδίκτυο των Αντικειμένων (IoT)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Βασιλάκη Κωνσταντίνου

Επιβλέπων:

Επ. Καθηγητής Σκούτας Δημήτριος

Μέλη εξεταστικής επιτροπής:

Καθηγητής Σκιάνης Χαράλαμπος,

Καθηγητής Βουγιούκας Δημοσθένης

Σάμος, Ιούλιος 2021

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος και ευχαριστίες

Η επαφή μου με τα δίκτυα τηλεπικοινωνιών μέχρι τώρα έχει περιοριστεί σε καθαρά θεωρητικό, ακαδημαϊκό επίπεδο. Η παρούσα πτυχιακή, μου έδωσε την δυνατότητα να μελετήσω σε ένα μεγαλύτερο βάθος κάποιες πιο σύγχρονες και πρακτικές έννοιες, με τις οποίες αν και σήμερα δεν είμαστε τόσο εξοικειωμένοι, είναι σίγουρο ότι σε λίγα χρόνια θα τις βλέπουμε παντού μπροστά μας.

Για το λόγο αυτό αποφάσισα να ασχοληθώ στην παρούσα εργασία στα δίκτυα διασύνδεσης αισθητήρων, την, θα λέγαμε, τελευταία λέξη της τεχνολογίας των δικτύων, από θέμα λειτουργικότητας.

Ευχαριστώ θερμά τον καθηγητή μου, κύριο Σκούτα Δημήτριο που με τις συνεχείς υποδείξεις του βοήθησε ώστε να ολοκληρωθεί το παρόν έργο, καθώς και την οικογένειά μου που με στηρίζει καθόλη τη διάρκεια του ακαδημαϊκού μου κύκλου.

Τέλος, η εργασία αυτή δε θα αφιερωθεί σε κάποιο συγγενικό ή φιλικό πρόσωπο, μα στη μνήμη των δύο νεαρών θυμάτων που έχασαν τη ζωή τους από τον φονικό σεισμό που έπληξε το νησί μας, ένα μήνα πριν την ολοκλήρωσή της.

© 2021

του

Βασιλάκη Κωνσταντίνου

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Υπεύθυνη Δήλωση πρωτοτυπίας διπλωματικής εργασίας

Είμαι συγγραφέας αυτής της διπλωματικής εργασίας και δηλώνω ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω αναφέρει τις πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τη συγκεκριμένη διπλωματική εργασία.

Υπογραφή

Κωνσταντίνος Βασιλάκης.

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

1	Εισαγωγή	1
2	Η έννοια του WSN.....	3
2.1	Ιστορικό υπόβαθρο	3
2.2	Υλικοτεχνική υποδομή	5
2.2.1	Ενσωματωμένος επεξεργαστής	5
2.2.2	Πομποδέκτης	6
2.2.3	Μνήμες	6
2.2.4	Τροφοδοσία	6
2.2.5	Αισθητήρες.....	7
3	Δικτύωση	8
3.1	Αρχιτεκτονική Δικτύου	8
3.2	Στοιβά πρωτοκόλλου WSN	9
3.3	Απειλές για την ασφάλεια των WSNs	11
3.3.1	Προβλήματα στο φυσικό επίπεδο	12
3.3.2	Απειλές επιπέδου συνδέσμου δεδομένων.....	12
4	Εφαρμογές	14
4.1	Διαδίκτυο των Αντικειμένων (Internet of Things - IoT)	14
4.2	Περιβαλλοντική παρακολούθηση.....	16
4.3	Συστήματα παρακολούθησης παραμέτρων υγείας	17
4.4	Δίκτυα αισθητήρων ελέγχου κυκλοφορίας.....	17
4.5	Βιομηχανική ανίχνευση	18
4.6	Ασφάλεια υποδομών.....	19
5	Ασύρματη δικτύωση με συστήματα χαμηλής ισχύος ευρείας περιοχής (LPWAN).....	20

5.1	LoWPAN.....	20
5.2	LoRaWAN.....	22
5.3	SigFox.....	24
5.4	Weightless.....	25
5.5	IEEE 802.11 (Wi-Fi)	27
6	Ασύρματα Προσωπικά Δίκτυα (WPAN)	29
6.1	ZigBee.....	29
6.2	6LoWPAN	30
6.3	Bluetooth.....	31
6.4	Bluetooth Low Energy (BLE)	33
6.5	RFID	34
6.6	NFC.....	35
7	Κυψελωτά δίκτυα και IoT	36
7.1	LTE.....	37
7.2	LTE-M	40
7.3	Narrow Band - IoT.....	42
7.4	EC-GSM - IoT	44
8	Προσομοίωση Έξυπνου Σπιτιού με χρήση του Cisco Packet Tracer.....	46
8.1	Πλεονεκτήματα του Packet Tracer	47
8.2	Μεθοδολογία	48
8.3	Σύνδεση μέσω δικτύων κινητής τηλεφωνίας.....	59
9	Συμπεράσματα.....	68
	Βιβλιογραφία	70

Λίστα Εικόνων

Εικόνα 1 Οι λειτουργίες ενός WSN.....	9
Εικόνα 2: Η στοίβα πρωτοκόλλων για τα WSNs.....	11
Εικόνα 3: Σύνοψη του Internet of Things	15
Εικόνα 4: Συνδεσμολογία LoWPAN – LoRa	21
Εικόνα 5: Οι τρεις κλάσεις του LoRaWANδικτύου.	23
Εικόνα 6: Σχήμα συνδεσμολογίας SigFox.....	24
Εικόνα 7: Τοπολογίες Zigbee: Αστέρα, δένδρο συστάδων, πλέγματος, όπου φαίνονται οι συσκευές (κίτρινοι κόμβοι), οι δρομολογητές (μπλε κόμβοι) και οι συντονιστές (κόκκινοι κόμβοι)	30
Εικόνα 8: Τοπολογίες Bluetooth, όπου φαίνεται η σχέση μεταξύ Masterκαι Slave στους κόμβους των δικτύων a, b, c.	32
Εικόνα 9: Τοπολογία δικτύου BLE, χωρισμένο σε 3 υποδίκτυα (piconet 1,2,3)	33
Εικόνα 10: Αρχιτεκτονική της τεχνολογίας RFID.....	34
Εικόνα 11: Παράδειγμα LTE τοπολογίας.....	37
Εικόνα 12: Σχηματική αναπαράσταση της διαφοράς των δικτύων LTE (δεξιά) και LTE -M (αριστερά).	42
Εικόνα 13: Παράδειγμα τοπολογίας NB-IoT.....	43
Εικόνα 14: Ρυθμίσεις Home Gateway.	51
Εικόνα 15: Ρυθμίσεις Wireless Router 1.	51
Εικόνα 16: Ρυθμίσεις Wireless Router 0.	52
Εικόνα 17: Ρυθμίσεις Access Point.	52
Εικόνα 18: Ρυθμίσεις Wireless PC.	53
Εικόνα 19: Ρυθμίσεις Network Adapter.	54
Εικόνα 20: Smart Home.....	55
Εικόνα 21: Login με default credentials στο IoT Monitor.....	56
Εικόνα 22: IoT Monitor.	57
Εικόνα 23: Αυτοματοποίηση λειτουργίας ανεμιστήρα.....	58
Εικόνα 24: Συσκευή ενάντια στα cyber attacks.....	58
Εικόνα 25: Ανάθεση IP.....	63
Εικόνα 26: Ανάθεση IP στον IoT server.....	64

Εικόνα 27: Σύνδεση συσκευής στον server.	65
Εικόνα 28: Σύνδεση στο server μέσω Smartphone απομακρυσμένα.	66
Εικόνα 29: Έλεγχος Smart Home απομακρυσμένα μέσω Smartphone με χρήση δικτύων κινητής τηλεφωνίας.....	67

Κατάλογος Πινάκων

Πίνακας 1: Χαρακτηριστικά LoRa	22
Πίνακας 2: Χαρακτηριστικά LoRaWan.....	22
Πίνακας 3: Χαρακτηριστικά Sigfox	25
Πίνακας 4: Χαρακτηριστικά Weightless-W	26
Πίνακας 5: Χαρακτηριστικά Weightless-N	26
Πίνακας 6: Χαρακτηριστικά Weightless-P	27
Πίνακας 7: Συγκεντρωτικός πίνακας τεχνολογιών	44

Ακρωνύμια

ARPANET	Advanced Research Projects Agency Network
ASIC	Application-Specific Integrated Circuit
BSN	Body Sensor Network
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DARPA	Defense Advanced Research Projects Agency
DOS	Denial of Service
DSN	Distributed Sensor Networks
DSP	Digital Signal Processor
EPC	Evolved Packet Core
EUTRAN	Evolved Universal Terrestrial Radio Access Network
FFD	Full Function Device
FPGA	Field Programmable Gate Array
IETF	Internet Engineering Task Force
IoT	Internet of Things
ISM	Industrial, Scientific and Medical
LowPAN	Low Power Personal Area Network
LTE	Long-Term Evolution
MANET	Mobile Ad Hoc Network
MBMS	Multimedia Broadcast Multicast Services
NB-IoT	Narrowband Internet of Things
PAN	Personal Area Network
QoS	Quality of Service
RFD	Reduced Function Device

RFI	Radio Frequency Identification
WSN	Wireless Sensor Networks

Περίληψη

Οι εξελίξεις που σημειώνονται στις νέες τεχνολογίες και πιο συγκεκριμένα στη δικτύωση και τη συνδεσιμότητα είναι τα τελευταία χρόνια ραγδαίες. Πλέον ο άνθρωπος μπορεί μέσα από ποικίλες συσκευές να γίνει μέλος δικτύων που κυμαίνονται από απλά μικρά οικιακά δίκτυα έως σύνθετα δίκτυα που ενώνουν χρήστες και συσκευές των οποίων η φυσική απόσταση μπορεί να μετριέται σε χιλιάδες χιλιόμετρα.

Μετά την επανάσταση της πληροφορίας η οποία είχε ως επίκεντρο την ανάπτυξη του διαδικτύου, με τις δεκάδες πλατφόρμες κοινωνικής δικτύωσης και την πρόσβαση του ανθρώπου στον παγκόσμιο ιστό μέσα από διάφορες συσκευές, όπως το κινητό τηλέφωνο, τον ηλεκτρονικό υπολογιστή ή την ταμπλέτα, το επόμενο βήμα στη δικτύωση είναι η συμμετοχή και η αλληλεπίδραση συσκευών. Με την πραγματικότητα αυτή να εκδηλώνεται σε ολοένα και πιο απλές και καθημερινές μορφές, η ανάγκη για μία εμβάθυνση στην κατανόηση της έννοιας του Διαδικτύου των Αντικειμένων (Internet of Things – IoT) μοιάζει επιβεβλημένη.

Στα πλαίσια λοιπόν της παρούσας εργασίας θα συζητηθούν οι πιο σύγχρονες έννοιες της δικτύωσης, θα αναλυθεί διεξοδικά το Διαδίκτυο των Αντικειμένων (ΔτΑ) όπως και όλες οι συνιστώσες και πτυχές του. Ταυτόχρονα θα γίνει μία εκτενής αναφορά στην ιστορία των τηλεπικοινωνιακών δικτύων, με σκοπό να καταλάβει ο αναγνώστης πώς φτάσαμε στο σημείο αυτό, τι χαρακτηριστικά έχουν τα δίκτυα συσκευών, ποιες τεχνολογίες είναι οι πιο διαδεδομένες καθώς και ποιες είναι οι νέες τάσεις.

Συμπληρώνοντας την θεωρία, στην εργασία συμπεριλαμβάνεται ένα σενάριο προσομοίωσης δικτύου IoT συσκευών, το οποίο υλοποιείται μέσω της εφαρμογής Cisco Packet Tracer και αφορά την απεικόνιση / χαρτογράφηση των στοιχείων που αποτελούν ένα έξυπνο σπίτι (smart home) κάτι το οποίο αν και μοιάζει φουτουριστικό αναμένεται ότι θα έχει καταστεί τετριμμένο σε μία δεκαετία από σήμερα.

Λέξεις Κλειδιά: Διαδίκτυο των Αντικειμένων, Δίκτυα αισθητήρων, Δίκτυα Τηλεπικοινωνιών

Abstract

Developments in new technologies and more specifically on networking and connectivity have been rapid in recent years. Now the end user is able, through a variety of devices, to connect to multiple communication networks that connect users and devices whose physical distance can be measured from a few meters to thousands of kilometers.

After the revolution of the information era, that focused on the development of the Internet, with dozens of social networking platforms and the ability to access internet through various devices such as a mobile phone, a computer or a tablet, the next step in networking is the active involvement of network devices and the interaction between them.

As this reality is increasingly manifested in everyday life, the need for in-depth understanding of the concept of the Internet seems imperative. In the context of this work, the most modern concepts of networking will be discussed, and the Internet of Things concept will be analyzed thoroughly in all its aspects. At the same time, an extensive report on the history of telecommunication networks is provided in order to help the reader to understand the course of the technological evolution and the characteristics of network devices and at the same time to inform him about the most widespread technologies and the new technologic trends.

Finally, this thesis concludes with a network simulation scenario, which is implemented through the Cisco Packet Tracer application and refers to the display / mapping of the elements that make up a smart home. Such a scenario although it seems very futuristic to date, is expected that it will become trivial in less than a decade from today.

Keywords: *Internet of Things, Wireless Sensor Network, Computer Networking*

1

Εισαγωγή

Η έννοια της δικτύωσης πέρα από δημοφιλής γίνεται με την πάροδο του χρόνου όλο και πιο σύνθετη. Χρειάζεται αρκετές επεξηγήσεις για να περιγράψει κάποιος τα συστατικά ενός δικτύου. Στα πρώτα βήματα της ανάπτυξης των υπολογιστών, σε ένα δίκτυο ήταν σχεδόν αυτονόητο ότι οι τερματικοί κόμβοι ήταν ηλεκτρονικοί υπολογιστές ή αλλιώς προσωπικοί υπολογιστές (personal computer) όπως είχε επικρατήσει να ονομάζονται. Σήμερα, οι τερματικές συσκευές μπορεί να είναι από ηλεκτρονικοί υπολογιστές μέχρι συσκευές που απλά φέρουν έναν αισθητήρα, τα δεδομένα του οποίου μεταφέρονται στο δίκτυο.

Επίσης, ολοένα και πιο συχνά χρησιμοποιούνται οι όροι της ταχύτητας μετάδοσης δεδομένων, της ασφάλειας υπηρεσιών ή της κρυπτογράφησης, όσο τα δίκτυα πολλαπλασιάζονται και συναντώνται σε ολοένα και περισσότερους τομείς της ανθρώπινης δραστηριότητας. Αυτή η αύξηση στον αριθμό των δικτύων συντελείται ταυτόχρονα με μία εξέλιξη, κατά την οποία τα δίκτυα δεν χρησιμεύουν μόνο για την απλή επικοινωνία μεταξύ χρηστών, αλλά περνούν σε ένα πιο υψηλό επίπεδο: την επικοινωνία μεταξύ συσκευών.

Αυτά λοιπόν τα νέου τύπου δίκτυα, στα οποία συμμετέχουν πέρα από χρήστες και συσκευές αποτελούν το κυρίως θέμα το οποίο θα πραγματευτεί η παρούσα εργασία. Στην ελληνική βιβλιογραφία χρησιμοποιείται πολλές φορές ο όρος WSN (Wireless Sensor Network), δηλαδή δίκτυο αισθητήρων, ένας τύπος δικτύων όποιος πραγματώνεται μέσα από διάφορες τεχνολογίες που έχουν αναπτυχθεί και που συνεχίζουν να αναπτύσσονται, αλλάζοντας την ιστορία της δικτύωσης έτσι όπως αυτή εμφανίσθηκε πριν από αρκετές δεκαετίες καταρχήν στην επιστημονική κοινότητα και ακολούθως σε ολόκληρες κοινωνίες.

Η παρούσα εργασία αποτελεί μία ανασκόπηση των εννοιών γύρω από το WSN. Μετά το παρόν εισαγωγικό κεφάλαιο, στο δεύτερο κεφάλαιο γίνεται μία πλήρης αναφορά στην έννοια του WSN, στο πώς αυτό ξεκίνησε και στο υλικό (hardware) από το οποίο αποτελείται.

Το τρίτο κεφάλαιο αναφέρεται στις αρχιτεκτονικές δικτύου και στη στοίβα πρωτοκόλλων του WSN. Το τέταρτο κεφάλαιο αναφέρεται στις εφαρμογές που βρίσκουν τα WSN, στη σημερινή εποχή, μέσα από την λογική του του Διαδικτύου των Αντικειμένων. Το πέμπτο κεφάλαιο αφιερώνεται στην ασύρματη δικτύωση με συστήματα χαμηλής ισχύος ευρείας περιοχής (Low Power Wide Area Network – LPWAN) ενώ στο έκτο και έβδομο κεφάλαιο γίνεται αναφορά αντίστοιχα σε τεχνολογίες ασύρματων δικτύων προσωπικής περιοχής (Wireless Personal Area Networks - WPAN) και κυψελωτών δικτύων (Cellular Networks) σε σχέση με την διασύνδεση συσκευών του Διαδικτύου των Αντικειμένων (IoT). Τελευταίο κεφάλαιο της εργασίας αποτελεί το σενάριο υλοποίησης της προσομοίωσης ενός έξυπνου σπιτιού (Smart Home) με τη χρήση του προγράμματος Cisco Packet Tracer.

2

Η έννοια του WSN

2.1 Ιστορικό υπόβαθρο

Οι απαρχές της έρευνας για τα Δίκτυα Διασύνδεσης Αισθητήρων (Wireless Sensor Networks – στο εξής WSNs) εντοπίζονται στο πρόγραμμα Distributed Sensor Networks (DSN) του Defense Advanced Research Projects Agency (DARPA) (Οργανισμός Προηγμένων Ερευνητικών Έργων Άμυνας) περίπου το 1980. Μέχρι τότε, το ARPANET (Advanced Research Projects Agency Network – Δίκτυο Προηγμένων Ερευνητικών Έργων) είχε τεθεί σε λειτουργία πριν αρκετά χρόνια, με περίπου 200 παρόχους σε πανεπιστήμια και ερευνητικά ιδρύματα. Τα DSN διέθεταν πολλούς κόμβους ανίχνευσης χαμηλού κόστους που επικοινωνούσαν μεταξύ τους αλλά λειτουργούσαν αυτόνομα, με τις πληροφορίες να δρομολογούνται σε οποιονδήποτε κόμβο, κάτι που ήταν η καλύτερη επιλογή για να χρησιμοποιηθούν οι πληροφορίες με τη μεγαλύτερη επάρκεια [1].

Η κυριαρχία του ARPANET ήταν καθολική και οι χρήστες θεωρούσαν το πρόγραμμα αυτό προηγμένο σε μια εποχή που δεν υπήρχαν προσωπικοί υπολογιστές (PC). Η επεξεργασία της πληροφορίας που συλλεγόταν πραγματοποιούνταν κυρίως σε μικροϋπολογιστές, και το Ethernet μόλις είχε αρχίσει να συστήνεται στο ευρύ κοινό. Τα τεχνολογικά συστατικά του DSN, όπως καθορίστηκαν το 1978 στο συνέδριο (workshop) Distributed Sensor Nets και περιελάμβαναν αισθητήρες ήχου (μικρόφωνα), λειτουργικές μονάδες επικοινωνίας και επεξεργασίας και το αντίστοιχο λογισμικό.

Ένα ιδιαίτερα εύχρηστο σύστημα, το Accent, αναπτύχθηκε στο Carnegie Mellon University, του οποίου ο προσανατολισμός στην ανταλλαγή πληροφοριών ήταν σαφέστερος. Το πρόγραμμα αυτό διέθετε τη δυνατότητα να επιτρέπει εύκολη πρόσβαση σε κατανεμημένους πόρους, πράγμα που έχει πρωταρχική σημασία για ένα DSN πρόγραμμα που θα περιορίζει την πιθανότητα σφάλματος εντός ανεκτών ορίων. Αξιοσημείωτη όσο και εντυπωσιακή εφαρμογή του προγράμματος DSN ήταν αυτή που ανέπτυξε το Ινστιτούτο Τεχνολογίας της Μασαχουσέτης (MIT) και είχε ως στόχο τον εντοπισμό ελικοπτέρων. Για το σκοπό αυτό το πρόγραμμα χρησιμοποιούσε μια διάταξη μικρόφωνων σε συνδυασμό με τεχνικές επεξεργασίας σημάτων [2].

Παρόλο που οι πρώτοι ερευνητές σε δίκτυα αισθητήρων είχαν κατά νου το όραμα ενός DSN, η τεχνολογία δεν ήταν ακόμα αρκετά έτοιμη για να γίνει η αντίστοιχη υλοποίηση. Ο όγκος των αισθητήρων την εποχή εκείνη ήταν λίγο μεγαλύτερος από μία κυβική παλάμη, πράγμα που εμπόδιζε την εφαρμογή τους σε πολλά συστήματα. Ακόμη το DSN στην αρχή δεν είχε τη δυνατότητα να συνδέεται ασύρματα. Οι πρόσφατες εξελίξεις στον τομέα της πληροφορικής, της επικοινωνίας και της μικροηλεκτρομηχανικής έχουν προκαλέσει μια σημαντική μετάβαση στην έρευνα των WSN και την έφεραν πιο κοντά στην επίτευξη του αρχικού οράματος. Οι νέες δικτυακές τεχνικές και η δυνατότητα συλλογής πληροφορίας από το δίκτυο υποστηρίζουν ένα ad hoc δικτυακό περιβάλλον, που παρουσιάζει μεγάλη δυναμική. Επίσης ερευνώνται σχολαστικά οι κόμβοι αισθητήρων που παρουσιάζουν συγκριτικά πλεονεκτήματα, όπως μικρότερες ενεργειακές απαιτήσεις.

Παράλληλα, οι κόμβοι αισθητήρων έχουν πλέον πολύ μικρότερο μέγεθος και αρκετά χαμηλότερες τιμές και έτσι πολλές νέες εφαρμογές δικτύων αισθητήρων έχουν γίνει εφικτές, όπως η παρακολούθηση περιβαλλοντικών συνθηκών ή το δίκτυο αισθητήρων οχημάτων. Νέα δυναμική στα δίκτυα των αισθητήρων που χρησιμοποιούνται σήμερα έδωσε το πρωτοποριακό πρόγραμμα SensIT από την DARPA. Μερικές από τις νέες διεργασίες που προσφέρει στα δίκτυα είναι η αναζήτηση με καλύτερες προϋποθέσεις, ο ευκολότερος τρόπος εργασίας, η δικτύωση ad hoc και η δυνατότητα επαναπρογραμματισμού.

Δεν διέφυγε επίσης της προσοχής του IEEE (Institute of Electrical and Electronics Engineers) ο συνδυασμός χαμηλού κόστους και μεγάλων δυνατοτήτων, ο οποίος παρέχεται από τα δίκτυα αισθητήρων και έτσι καθόρισε το πρότυπο IEEE 802.15.4 για να προσδιορίσει τα ασύρματα δίκτυα προσωπικής περιοχής και χαμηλού ρυθμού μετάδοσης δεδομένων. Με βάση το παραπάνω πρότυπο, η ZigBee Alliance πρότεινε το δικό της πρότυπο για την επικοινωνία σε υψηλό επίπεδο, το οποίο περιλαμβάνει πρωτόκολλα, τα οποία είναι δυνατόν να εφαρμοσθούν σε WSNs [3].

Σήμερα, τα δίκτυα διασύνδεσης αισθητήρων έχουν ενταχθεί σε ερευνητικά προγράμματα των μεγάλων κρατών του πλανήτη και υποστηρίζονται από παλαιότερες αλλά και νεότερες εταιρείες στον χώρο των τηλεπικοινωνιών. Δίκαια λοιπόν τα WSN θεωρούνται ως η βάση για την ανάπτυξη πολλών άλλων τεχνολογιών.

2.2 Υλικοτεχνική υποδομή

Ένα ασύρματο δίκτυο αισθητήρων αποτελείται από κόμβους αισθητήρων που βρίσκονται διάσπαρτοι μέσα σε έναν ευρύτερο χώρο. Κάθε κόμβος έχει αυτονομία ως προς τον εντοπισμό και την επεξεργασία πληροφοριών σε σχέση με τους υπόλοιπους, το δε σύνολο των πληροφοριών προωθούνται από τους κόμβους αισθητήρων είτε σε ένα κέντρο επεξεργασίας, είτε σε μία τοπική μονάδα αποθήκευσης, όπου τα δεδομένα μπορούν να αποθηκευτούν και να αναλυθούν. Μια πλατφόρμα κόμβου αισθητήρων που χρησιμοποιείται ευρέως είναι το Mica2 Mote που αναπτύχθηκε από την Crossbow Technology. Από άποψη υλικοτεχνικής υποδομής, ένας κόμβος περιλαμβάνει ένα κλασικό πομπό και δέκτη, μονάδα επεξεργασίας και τροφοδοσίας, καθώς και μνήμες για αποθήκευση αλλά και έναν αριθμό αισθητήρων ή σπανιότερα μόνο έναν.

2.2.1 Ενσωματωμένος επεξεργαστής

Σε έναν κόμβο, η λειτουργία του ενσωματωμένου επεξεργαστή έγκειται στον προγραμματισμό των διεργασιών, την επεξεργασία δεδομένων και τον έλεγχο της λειτουργίας των υπολοίπων στοιχείων του κόμβου. Οι τεχνολογίες που μπορούν να χρησιμοποιηθούν σε έναν κόμβο αισθητήρα είναι οι εξής [4]:

1. Υλοποίηση με χρήση μικροελεγκτή (Microcontroller)
2. Υλοποίηση με χρήση Ψηφιακού Επεξεργαστή Σήματος – DSP (Digital Signal Processor)
3. Υλοποίηση με χρήση FPGA (Field Programmable Gate Array)
4. Υλοποίηση με χρήση εξειδικευμένου ολοκληρωμένου κυκλώματος – ASIC (Application-Specific Integrated Circuit)

Το χαμηλό κόστος του μικροελεγκτή καθώς και το γεγονός ότι είναι εύχρηστος και έχει δυνατότητα σύνδεσης με πλήθος άλλων συσκευών, τον κατέστησε ως την βασική λύση υλοποίησης.

2.2.2 Πομποδέκτης

Στον κόμβο του αισθητήρα, η συσκευή αυτή εξασφαλίζει τη δυνατότητα να επιτυγχάνεται η επικοινωνία, όχι μόνο μέσω καλωδίων αλλά και μέσω ραδιοκυμάτων, laser ή υπέρυθρης ακτινοβολίας. Οι εφαρμογές WSN κατά κανόνα χρησιμοποιούν ραδιοσυχνότητες (RF) και η λειτουργία τους προσαρμόζεται σε αυτές.

Η συσκευή πομπού - δέκτη μπορεί να βρίσκεται σε μία κατάσταση λειτουργίας από τις παρακάτω τέσσερις:

1. Αδράνεια (Idle)
2. Λειτουργία σε Ελάχιστη Ενέργεια (Sleep)
3. Κατάσταση Λήψης
4. Κατάσταση Εκπομπής

Χρησιμοποιώντας τις συχνότητες των RFM TR 1000 και Chipcon CC1000 το Mica 2 Mote επιτυγχάνει βεληνεκές εκπομπής που πλησιάζει τα 160 μέτρα.

2.2.3 Μνήμες

Οι μνήμες σε έναν κόμβο αισθητήρα περιλαμβάνουν τη μνήμη flash in-chip, τη μνήμη RAM (Random-Access Memory) του μικροελεγκτή καθώς και την και εξωτερική μνήμη flash. Για παράδειγμα, ο μικροελεγκτής ATmega128L που λειτουργεί στο Mica2 Mote διαθέτει μνήμη προγράμματος flash 128-Kbyte και στατική μνήμη 4-Kbyte. Επιπλέον, ένα σειριακό τσιπ 4-Mbit Atmel AT45DB041B μπορεί να παρέχει εξωτερικές μνήμες για Mica και Mica2 Motes[3].

2.2.4 Τροφοδοσία

Σε έναν κόμβο αισθητήρα, η ενέργεια καταναλώνεται για τους σκοπούς της ανίχνευσης, της επικοινωνίας και της επεξεργασίας δεδομένων αν και απαιτείται περισσότερη ενέργεια για την επικοινωνία δεδομένων παρά για την ανίχνευση και την επεξεργασία δεδομένων. Η ενέργεια αποθηκεύεται και παρέχεται από μία μπαταρία ή ένα πυκνωτή. Στον κόμβο του αισθητήρα, ως πηγή ισχύος χρησιμοποιούνται συνήθως μπαταρίες. Επειδή όμως οι μπαταρίες εξαντλούνται γρήγορα, ο σχεδιασμός κάθε WSN απαιτεί προσεκτική θεώρηση ως προς μέρος της κατανάλωσης ενέργειας. Για την εξάλειψη του ενεργειακού περιορισμού, έχουν πραγματοποιηθεί έρευνες πάνω

στις τεχνικές συλλογής ενέργειας για WSN. Η σύγχρονη έρευνα προσανατολίζεται στην χρήση ηλιακής ή αιολικής ενέργειας, η οποία μετατρέπόμενη σε ηλεκτρική, εξασφαλίζει τη μόνιμη τροφοδοσία στον κόμβο του αισθητήρα.

2.2.5 Αισθητήρες

Όταν μία περιβαλλοντική παράμετρος μεταβάλλεται, ο αισθητήρας ανιχνεύει τη μεταβολή, και αποκρίνεται παράγοντας σήμα, το οποίο είναι τόσο μεγαλύτερο αριθμητικά, όσο ευρύτερη είναι η μεταβολή. Ο αισθητήρας ανιχνεύει αναλογικό σήμα, το οποίο μετατρέπεται σε ψηφιακό από κατάλληλο μετατροπέα σήματος, και διαβιβάζεται στον ενσωματωμένο επεξεργαστή. Ο αισθητήρας είναι απαραίτητο να έχει μικρή κατανάλωση, ώστε η τροφοδοσία του να είναι δυνατή από την μικρή μπαταρία, που περιλαμβάνεται συνήθως στον κόμβο. Επίσης, ο κόμβος περιλαμβάνει συνήθως πολλούς αισθητήρες διαφορετικών τύπων και οι οποίοι είναι συνδεδεμένοι με συγκεκριμένη διάταξη η οποία εξασφαλίζει την εύρυθμη λειτουργία του [6].

Το TinyOS ανήκει στα λειτουργικά συστήματα τα οποία σχεδιάστηκαν ώστε να ταιριάζουν στο WSN [5]. Διαθέτει αρχιτεκτονική που επιτρέπει την εύκολη εφαρμογή του σε WSNs και ελαχιστοποιεί ταυτόχρονα το μέγεθος του απαιτούμενου κώδικα αλλά και της ανάγκης για μεγάλο μέγεθος ενσωματωμένης μνήμης. Παρέχει την δυνατότητα χειρισμού των αισθητήρων, πρωτόκολλα διασύνδεσης για πολλά δίκτυα καθώς και μηχανισμούς συλλογής πληροφοριών αλλά και δυνατότητες για πολλές άλλες λειτουργίες οι οποίες επιδέχονται περαιτέρω βελτιώσεις. Το παραπάνω σύστημα έχει την ιδιαιτερότητα να χρησιμοποιεί προγραμματιστικό πρότυπο βασισμένο σε γεγονότα (event driven) και όχι σε multi - threading. Όταν συμβαίνει ένα εξωτερικό συμβάν, δηλαδή όταν εισέλθουν δεδομένα στον αισθητήρα, το TinyOS καλεί τον κατάλληλο διαχειριστή συμβάντων. Οι διαχειριστές συμβάντων μπορούν να μεταθέσουν εργασίες που έχουν προγραμματιστεί από τον πυρήνα του TinyOS ώστε να πραγματοποιηθούν σε μεταγενέστερο στάδιο.

Το λογισμικό TinyOS όπως και κάθε πρόγραμμα που έχει δημιουργηθεί για το σύστημα αυτό χρησιμοποιεί την γλώσσα NesC η οποία αποτελεί παραλλαγή της προγραμματιστικής γλώσσας C. Με την γλώσσα NesC ανιχνεύονται εύκολα οι σχέσεις ανάμεσα στις πληροφορίες και τη διαχείρισή τους [5].

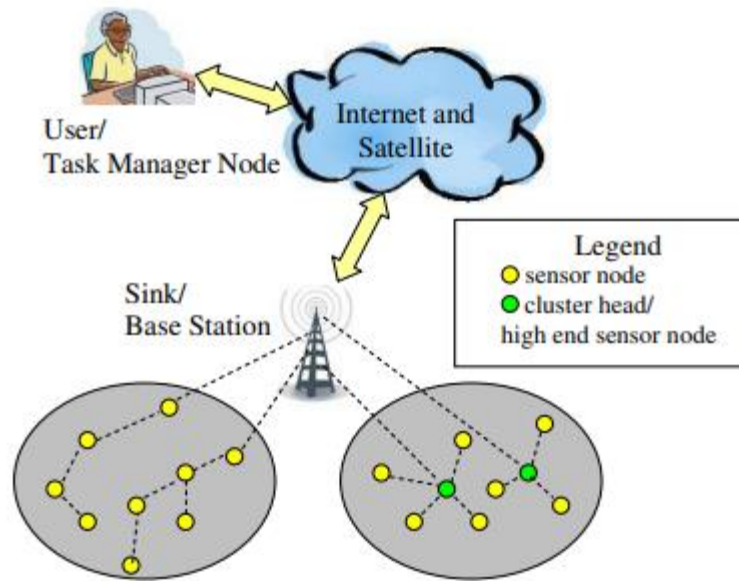
3

Δικτύωση

3.1 Αρχιτεκτονική Δικτύου

Οι κόμβοι αισθητήρων ενός δικτύου WSN παρουσιάζουν μεγάλη ποικιλία δυνατοτήτων, όπως να επικοινωνούν με δίκτυα υποδομής, να έχουν ικανότητες επεξεργασίας και να ανιχνεύουν το περιβάλλον. Το πεδίο δράσης τους είναι ο φυσικός κόσμος, στον οποίο εντοπίζουν διάφορα φυσικά μεγέθη.

Τα φυσικά μεγέθη που ανιχνεύουν οι αισθητήρες μπορούν να συλλεχθούν ως δεδομένα από κατάλληλους κόμβους στο Διαδίκτυο. Μέσω του Διαδικτύου ο τελικός χρήστης μπορεί να αποκτήσει πρόσβαση στα δεδομένα τόσο στην ανεπεξέργαστη όσο και στην αναλυμένη τους μορφή. Στο Σχήμα 1 απεικονίζονται οι λειτουργίες των WSN. Παρατηρούμε ότι υπάρχουν δύο διαφορετικές τοπολογίες σχετικά με το δίκτυο: η επίπεδη η οποία συγκροτείται από τους κόμβους που έχουν θέση δρομολογητών και μεταβιβάζουν πληροφορίες ο ένας στον άλλον μέχρι να φτάσουν στον τελικό χρήστη και η ιεραρχική τοπολογία κατά την οποία οι πληροφορίες έχουν πορεία από κάτω προς τα πάνω έως ότου τις παραλάβει ο τελικός χρήστης [8].



Εικόνα 1 Οι λειτουργίες ενός WSN

Πηγή: <http://ijetemr.org/2017/09/22/efficient-clustering-technique-for-improving-network-performance-in-wireless-sensor-networks/>

3.2 Στοιβά πρωτοκόλλου WSN

Η στοιβά πρωτοκόλλων που χρησιμοποιείται στα δίκτυα αισθητήρων μοιάζει πολύ με την παραδοσιακή στοιβά πρωτοκόλλων των κλασικών δικτύων και περιλαμβάνει τα ακόλουθα επίπεδα [7]:

- Επίπεδο εφαρμογής
- Επίπεδο μεταφοράς
- Επίπεδο δικτύωσης
- Επίπεδο συνδέσμου δεδομένων
- Φυσικό επίπεδο.

Το φυσικό επίπεδο καθορίζει την συχνότητα επικοινωνίας για την μετάδοση πληροφοριών. Το επίπεδο σύνδεσης δεδομένων είναι υπεύθυνο για την πολυπλεξία ροών δεδομένων (multiplexing), την ανίχνευση του πλαισίου δεδομένων, την πρόσβαση στο φυσικό μέσο αλλά και τον έλεγχο σφαλμάτων. Με αυτό τον τρόπο διασφαλίζεται η επικοινωνία, τόσο από το ένα σημείο στο άλλο, όσο και από το ένα σημείο προς πολλαπλά σημεία (Point – to – Multipoint) εντός του δικτύου. Το επίπεδο δικτύου φροντίζει για τη δρομολόγηση των δεδομένων που παρέχονται από το επίπεδο

μεταφοράς. Ο σχεδιασμός του επιπέδου δικτύου στα WSNs πρέπει να λαμβάνει υπόψη την απόδοση ισχύος, την επικοινωνία με βάση τα δεδομένα κ.λπ. Η υλοποίηση του επιπέδου εφαρμογής εξαρτάται από τις χρησιμοποιούμενες διαδικασίες της ανίχνευσης και είναι δυνατόν να ρυθμιστεί και να χρησιμοποιηθεί με διαφορετικούς τρόπους.

Για τον καλύτερο τρόπο λειτουργίας των WSN ρυθμίζονται με κατάλληλο τρόπο και οι παρακάτω παράμετροι [7]:

1. Ευχρηστία
2. Εμβέλεια
3. Αξιοπιστία
4. Ασφάλεια
5. Χειρισμός

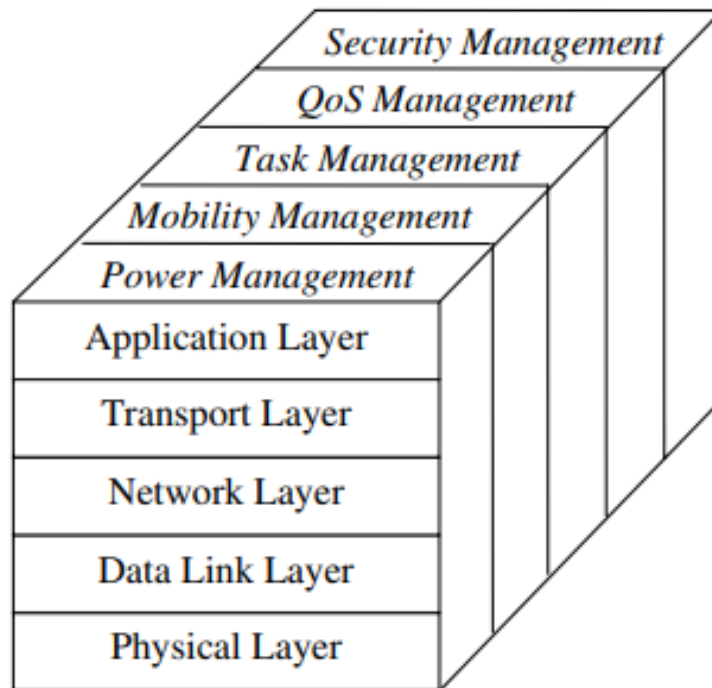
Μεγαλύτερη βαρύτητα έχουν οι λειτουργίες διαχείρισης διεργασίας, διαχείρισης κινητικότητας και διαχείρισης ισχύος. Ο τρόπος με τον οποίο γίνεται η χρήση της ενέργειας απαιτεί προσεκτικούς χειρισμούς ώστε τα επίπεδα κατανάλωσης να είναι τα χαμηλότερα δυνατά. Περιλαμβάνει και την αυτόματη απενεργοποίηση λειτουργίας με σκοπό να εξοικονομείται ενέργεια.

Το επίπεδο διαχείρισης της κινητικότητας ανιχνεύει και καταγράφει την κίνηση των κόμβων, ώστε να διατηρείται πάντα μια διαδρομή δεδομένων από τους κόμβους αισθητήρων στα ανώτερα επίπεδα της ιεραρχίας του δικτύου. Ως προς τον τρόπο που γίνεται ο χειρισμός των διαφόρων διαδικασιών, εξισορροπείται και γίνεται προγραμματισμός των ενεργειών ανίχνευσης, ώστε να απασχολούνται οι λιγότεροι δυνατοί κόμβοι, ώστε οι υπόλοιποι να μπορούν να απασχοληθούν με τη συλλογή και διαχείριση των πληροφοριών.

Η διαχείριση ποιότητας υπηρεσιών στα WSNs μπορεί να είναι πολύ σημαντική εάν υπάρχει απαίτηση σε πραγματικό χρόνο όσον αφορά τις υπηρεσίες δεδομένων, κάτι που είναι αναγκαιότητα στα περισσότερα τέτοια δίκτυα. Ποιότητα υπηρεσίας σημαίνει διαχείριση του ρυθμού σφάλματος, εξασφάλιση ενός επιπέδου ανοχής σφάλματος αλλά και μεγιστοποίηση της απόδοσης.

Το πώς συμπεριφέρεται ένα δίκτυο, η παρακολούθησή του, και ο έλεγχος της λειτουργίας του, διεκπεραιώνεται από την ασφάλεια του δικτύου. Η κύρια λειτουργία της διαχείρισης ασφαλείας είναι ο έλεγχος των σημείων πρόσβασης σε κρίσιμα ή ευαίσθητα δεδομένων. Για να είναι

ασφαλές ένα δίκτυο πρέπει να συμπεριλαμβάνει πλήθος από διαφορετικές λειτουργικές μονάδες, και κυρίως να έχει τη δυνατότητα να ασκεί έλεγχο ταυτοποίησης και να αναχαιτίζει κάθε πιθανό εισβολέα. Έτσι, η στοίβα πρωτοκόλλων για τα WSNs παίρνει σχηματικά την παρακάτω μορφή:



Εικόνα 2: Η στοίβα πρωτοκόλλων για τα WSNs.

Πηγή: https://www.researchgate.net/figure/The-protocol-stack-and-the-management-plane-of-WSNs-50_fig3_322115417

3.3 Απειλές για την ασφάλεια των WSNs

Ενώ το μέλλον των WSN έχει πολλές προοπτικές ανάπτυξης, τα WSN δεν θα αναπτυχθούν στο άμεσο μέλλον με επιτυχία εάν τα θέματα ασφάλειας, αξιοπιστίας και απορρήτου δεν αντιμετωπιστούν επαρκώς δεδομένου ότι τα WSN προσανατολίζονται σε πολύ σημαντικές και ευαίσθητες εφαρμογές. Επιπλέον, τα WSNs είναι πολύ ευάλωτα και, επομένως, καθίστανται ελκυστικά σε επιθέσεις λόγω της χαμηλού επιπέδου ασφάλειας τους αλλά και της αρχιτεκτονικής τους η οποία περιλαμβάνει πολλές αυτόματες διαδικασίες [15].

Ενα συνηθισμένο WSN απαρτίζεται από πλήθος αισθητήρων. Αυτοί κατανέμονται σε μια περιοχή για τη συλλογή πληροφοριών οι οποίες σε κάποιες περιπτώσεις είναι ευαίσθητες. Ο κάθε κόμβος

αισθητήρων είναι συνδεδεμένοι ασύρματα με αναμεταδότες οι οποίοι αποστέλλουν μέσα από υποδίκτυα τα δεδομένα των αισθητήρων σε μία βάση δεδομένων. Σε ένα τυπικό σενάριο WSN, οι περιορισμένοι πόροι, η δυνατότητα ασύρματης επικοινωνίας, τα δεδομένα που είναι ευαίσθητα από πλευράς ασφάλειας, το ανεξέλεγκτο περιβάλλον και ακόμη και η κατανεμημένη ανάπτυξη αποτελούν το καθένα με τον τρόπο του, και ένα τρωτό σημείο στο πλέγμα του δικτύου. Αυτές οι ευπάθειες κάνουν τα WSN ευάλωτα σε έναν μεγάλο αριθμό απειλών ασφαλείας και επομένως η χρήση των WSN προορίζεται μόνο για ειδικές εφαρμογές.

3.3.1 Προβλήματα στο φυσικό επίπεδο

Στα WSN εντοπίζονται προβλήματα στο φυσικό επίπεδο, εξαιτίας του ότι είναι εύκολη τόσο η παραβίαση των κόμβων του WSN καθώς και η παρέμβαση στην ασύρματη μετάδοση. Οι συνήθεις τύποι επιθέσεων στο φυσικό επίπεδο περιλαμβάνουν την καταστροφή ενός κόμβου ή την αποσύνδεσή του από το δίκτυο.

3.3.2 Απειλές επιπέδου συνδέσμου δεδομένων

Η βάση δεδομένων ευθύνεται για την πολυπλεξία ροών δεδομένων, την διερεύνηση του πλαισίου δεδομένων, την πρόσβαση και τον έλεγχο σφαλμάτων. Σύμφωνα με τους ειδικούς [16], στο επίπεδο σύνδεσης των WSN, μπορούν να συμβούν τα ακόλουθα είδη επιθέσεων:

- **Παρεμβολή (Jamming)**

Η παρεμβολή πραγματοποιείται στις ραδιοσυχνότητες που χρησιμοποιούν οι κόμβοι ενός WSN δικτύου. Μια πηγή παρεμβολής μπορεί είτε να είναι αρκετά ισχυρή ώστε να διαταράξει ολόκληρο το δίκτυο ή να είναι λιγότερο ισχυρή και να είναι ικανή να διαταράξει μόνο ένα μικρότερο τμήμα του δικτύου. Για την άμυνα κατά της απειλής αυτής χρησιμοποιούνται τεχνικές επικοινωνίας όπως το frequency hopping, δηλαδή η μετάβαση από τη μία συχνότητα σε άλλη σε μη αναμενόμενες χρονικές στιγμές αλλά και τεχνικές απευθείας διασποράς φάσματος με χρήση κώδικα.

- **Σύγκρουση (Collision)**

Στην περίπτωση που περισσότεροι από ένας κόμβος μεταδίδουν στην ίδια συχνότητα δεδομένα, πραγματοποιείται σύγκρουση. Σε αυτή την περίπτωση, μπορεί να συμβεί μεταβολή σε κάποιο τμήμα των μεταδιδόμενων δεδομένων με αποτέλεσμα να προκαλείται

σφάλμα στον δέκτη και το αντίστοιχο πακέτο δεδομένων τότε θα απορριφθεί ως μη έγκυρο. Ένας τρόπος άμυνας έναντι των συγκρούσεων είναι η υιοθέτηση κωδικών διόρθωσης σφαλμάτων όπως αυτοί που χρησιμοποιούνται στα κλασικά δίκτυα.

- **Εξάντληση πόρων**

Ένας εισβολέας μπορεί να δημιουργήσει επαναλαμβανόμενες συγκρούσεις για να προκαλέσει εξάντληση πόρων. Για παράδειγμα, μια εφαρμογή μπορεί συνεχώς να προσπαθεί να επαναμεταδώσει τα κατεστραμμένα πακέτα. Τα ενεργειακά αποθέματα του κόμβου μετάδοσης εξαντλούνται, εκτός εάν ανακαλυφθούν ή αποτραπούν οι πηγές των συνεχών αναμεταδόσεων. Μια λύση στην απειλή της εξάντλησης είναι η εφαρμογή ορίων και ελέγχου, ώστε να διασφαλίζεται ότι κανένας κόμβος δε θα αναμεταδίδει με ρυθμό που να δημιουργεί προβλήματα στο δίκτυο [17].

4

Εφαρμογές

4.1 Διαδίκτυο των Αντικειμένων (Internet of Things - IoT)

Η ιδέα του Internet of Things (IoT– Διαδίκτυο των Πραγμάτων / Αντικειμένων) επινοήθηκε από ένα μέλος της κοινότητας αναγνώρισης μέσω ραδιοσυχνοτήτων (RFID - Radio Frequency Identification) το 1999 και πρόσφατα έγινε ευρύτερα γνωστό, κυρίως λόγω της ανάπτυξης κινητών συσκευών, της δυνατότητας απρόσκοπτης τηλεπικοινωνίας, του υπολογιστικού νέφους (cloud computing) αλλά και της ανάλυσης δεδομένων (data analytics) [8]. Η ιδέα του Internet of Things βασίζεται στο όραμα ενός κόσμου όπου δισεκατομμύρια αντικείμενα μπορούν να ανιχνεύσουν, να επικοινωνήσουν και να μοιραστούν πληροφορίες, μένοντας διασυνδεδεμένα μέσω δημόσιων ή ιδιωτικών δικτύων. Αυτά τα διασυνδεδεμένα αντικείμενα συλλέγουν, αναλύουν και χρησιμοποιούν τακτικά δεδομένα για την έναρξη της λειτουργίας τους, παρέχοντας πληθώρα πληροφοριών για τον σχεδιασμό, τη διαχείριση και τη λήψη αποφάσεων.

Το IoT είναι ένα δίκτυο φυσικών αντικειμένων. Δεν είναι απλά ένα δίκτυο που συνδέει υπολογιστές, αλλά έχει εξελιχθεί σε ένα δίκτυο συσκευών όλων των τύπων και μεγεθών, οχημάτων, έξυπνων τηλεφώνων, οικιακών συσκευών, παιχνιδιών, φωτογραφικών μηχανών, ιατρικών οργάνων και βιομηχανικών συστημάτων, ζώων, ανθρώπων, κτιρίων, όπου όλα αυτά είναι συνδεδεμένα μεταξύ τους και, όλες οι πληροφορίες επικοινωνίας και ανταλλαγής βασίζονται σε καθορισμένα πρωτόκολλα, προκειμένου να επιτευχθούν έξυπνες αναδιοργανώσεις, εντοπισμοί

Το Διαδίκτυο των Αντικειμένων (ΔτΑ) αναφέρεται στη γενική ιδέα της σύνδεσης των συσκευών, ειδικά των καθημερινών αντικειμένων, τα οποία μπορούν να αναγνωριστούν, να εντοπιστούν και έχουν συγκεκριμένη διεύθυνση μέσα στο δίκτυο ανεξάρτητα από τα μέσα επικοινωνίας που χρησιμοποιούνται (ασύρματο ή ενσύρματο δίκτυο). Τα αντικείμενα που συνδέονται περιλαμβάνουν όχι μόνο ηλεκτρονικές συσκευές ή εξελιγμένα τεχνολογικά προϊόντα τα οποία έχουν σχετιστεί στο μυαλό μας με τις τηλεπικοινωνίες, αλλά και πράγματα που συνήθως δεν θεωρούμε ηλεκτρονικά – όπως το φαγητό, τα ρούχα, οι καρέκλες, το νερό κλπ. [10].

Τα αντικείμενα καθίστανται αναγνωρίσιμα και αποκτούν νοημοσύνη λαμβάνοντας ή παίρνοντας αποφάσεις σχετικές με το περιβάλλον, χάρη στο γεγονός ότι μπορούν να επικοινωνούν και να μεταδίδουν πληροφορίες που μπορούν να αξιοποιηθούν. Μπορούν να έχουν πρόσβαση σε πληροφορίες όπου έχουν συγκεντρωθεί από άλλες συσκευές και να τις αξιοποιήσουν προς όφελός τους ή μπορεί να αποτελούν μέρος μιας πιο σύνθετης υπηρεσίας. Αυτός ο μετασχηματισμός της λειτουργίας των συσκευών συμπορεύεται με τις δυνατότητες που παρέχει το υπολογιστικό νέφος αλλά και η μετάβαση από το πρωτόκολλο IPv4 στο IPv6, που παρέχει ένα πρακτικά απεριόριστο αριθμό δικτυακών διευθύνσεων. Ο στόχος του ΔτΑ είναι να επιτρέψει τη σύνδεση των αντικειμένων ανά πάσα στιγμή, οπουδήποτε, με οτιδήποτε και με οποιονδήποτε [11].

Το αρχικό κίνητρο πίσω από την έρευνα των WSNs ήταν η στρατιωτική εφαρμογή. Παραδείγματα δικτύων στρατιωτικών αισθητήρων περιλαμβάνουν συστήματα μεγάλης κλίμακας όπως ακουστικά συστήματα παρακολούθησης ωκεανών για την ανίχνευση υποβρυχίων, δίκτυα για επιτήρηση πεδίου μάχης και σύνδεση μικρο-αισθητήρων σε όπλα για την παρακολούθηση των αποθεμάτων πυρομαχικών. Καθώς το κόστος για κόμβους αισθητήρων και δίκτυα επικοινωνίας έχει μειωθεί, έχουν προκύψει πολλές άλλες πιθανές εφαρμογές, συμπεριλαμβανομένων εκείνων που δεν σχετίζονται με στρατιωτικούς σκοπούς. Οι βασικότερες κατηγορίες εφαρμογών στην καθημερινή και βιομηχανική ζωή είναι οι εξής:

4.2 Περιβαλλοντική παρακολούθηση

Η περιβαλλοντική παρακολούθηση είναι εφικτό να χρησιμοποιηθεί για την παρακολούθηση ζώων, την παρακολούθηση δασών, την ανίχνευση πλημμυρών και την πρόγνωση του καιρού. Οι εφαρμογές αυτές είναι κατάλληλες για την ανάπτυξη WSNs, επειδή οι μεταβλητές που πρέπει να παρακολουθούνται, συνήθως είναι διεσπαρμένες σε μια μεγάλη περιοχή. Ένα παράδειγμα είναι ότι ερευνητές από το Πανεπιστήμιο του Σαουθάμπτον έχουν δημιουργήσει ένα σύστημα παρακολούθησης του παγετού στο περιβάλλον, χρησιμοποιώντας WSNs σε περιοχές της

Νορβηγίας [14]. Στην εφαρμογή αυτή συλλέγονται δεδομένα από κόμβους αισθητήρων που είναι εγκατεστημένοι στον πάγο και το υπόγειο ίζημα χωρίς τη χρήση καλωδίων, τα οποία θα μπορούσαν να διαταράξουν το περιβάλλον. Ένα άλλο παράδειγμα είναι ότι οι ερευνητές από το EPFL έχουν πραγματοποιήσει την ανάπτυξη ενός εξωτερικού WSN σε μια τραχιά ορεινή περιοχή που βρίσκεται μεταξύ Ελβετίας και Ιταλίας [14]. Η ανάπτυξη του συγκεκριμένου WSN χρησιμοποιείται για την παροχή πληροφοριών στις ελβετικές αρχές που είναι υπεύθυνες για τη διαχείριση των κινδύνων και το μοντέλο που προκύπτει βοηθά στην πρόληψη των χιονοστιβάδων στην περιοχή αυτή.

4.3 Συστήματα παρακολούθησης παραμέτρων υγείας

Τα δίκτυα WSN μπορούν να αναπτυχθούν σε κτίρια νοσοκομείων για την παρακολούθηση και τον έλεγχο των ασθενών αλλά και όλων των ιατρικών πόρων. Υπάρχουν ειδικοί αισθητήρες που μπορούν να μετρήσουν την αρτηριακή πίεση, τη θερμοκρασία του σώματος και δεδομένα που τώρα μετρούνται με ηλεκτροκαρδιογράφημα, ενώ μπορούν να τοποθετηθούν σε ρούχα για να παρέχουν απομακρυσμένη παρακολούθηση για ηλικιωμένους. Όταν οι αισθητήρες βρίσκονται πάνω στους ασθενείς (στα ρούχα τους) για λόγους υγειονομικής περίθαλψης, σχηματίζεται ένα ειδικό είδος δικτύου αισθητήρων που ονομάζεται δίκτυο αισθητήρων σώματος (Body Sensor Network - BSN). Το BSN αποτελεί έναν ευρύ διεπιστημονικό τομέα που φέρνει επανάσταση στο σύστημα υγειονομικής περίθαλψης επιτρέποντας την ανέξοδη, συνεχή και απρόσκοπτη απομακρυσμένη παρακολούθηση της υγείας των ατόμων και με ενημερώσεις ιατρικών αρχείων σε πραγματικό χρόνο μέσω του διαδικτύου. Μία από τις πρώτες έρευνες για τα BSNs πραγματοποιήθηκε στο Imperial College London, όπου έχουν αναπτυχθεί εξειδικευμένοι κόμβοι αισθητήρων BSN και ο αντίστοιχος εξοπλισμός που αξιοποιεί τον αισθητήρα και μεταφέρει την πληροφορία στη βάση δεδομένων.

4.4 Δίκτυα αισθητήρων ελέγχου κυκλοφορίας

Αυτά τα δίκτυα αισθητήρων έχουν χρησιμοποιηθεί αποτελεσματικά για την παρακολούθηση και τον έλεγχο της κυκλοφορίας οχημάτων. Σε αρκετές διασταυρώσεις, υπάρχουν αισθητήρες που βρίσκονται είτε υπερυψωμένοι είτε χαμηλότερα από το επίπεδο του δρόμου για την ανίχνευση οχημάτων και τον έλεγχο των σηματοδοτών. Επιπρόσθετα, βιντεοκάμερες χρησιμοποιούνται επίσης συχνά για την παρακολούθηση τμημάτων δρόμου με μεγάλη κίνηση. Ωστόσο, τα

παραδοσιακά δίκτυα επικοινωνίας που χρησιμοποιούνται για τη σύνδεση αυτών των αισθητήρων είναι δαπανηρά και επομένως η παρακολούθηση της κυκλοφορίας είναι συνήθως διαθέσιμη μόνο σε ορισμένα κρίσιμα σημεία των πόλεων [12]. Τα WSN, όσο συνεχίζουν να αναπτύσσονται, είναι πιθανό ότι θα αλλάξουν εντελώς το τοπίο της παρακολούθησης και ελέγχου της κυκλοφορίας με την εγκατάσταση φτηνών κόμβων αισθητήρων στο αυτοκίνητο, στους χώρους στάθμευσης, κατά μήκος των δρόμων κ.λπ. Η Streetline Inc. είναι μια εταιρεία που χρησιμοποιεί τεχνολογία αισθητήρων για να βοηθήσει τους οδηγούς να βρουν θέσεις στάθμευσης, καθώς επίσης και για να αποφύγουν την κυκλοφοριακή συμφόρηση. Οι λύσεις που παρέχει η Streetline μπορούν να βελτιώσουν σημαντικά τη διαχείριση της κυκλοφορίας εντός μιας πόλης και να μειώσουν τις εκπομπές διοξειδίου του άνθρακα [13].

4.5 Βιομηχανική ανίχνευση

Καθώς η υποδομή ενός εργοστασίου μεγαλώνει, οι βλάβες του εξοπλισμού προκαλούν όλο και μεγαλύτερους χρόνους διακοπής λειτουργίας, οι οποίοι σαφώς δεν ήταν προγραμματισμένοι. Η συμβουλευτική εταιρεία ARC εκτιμά ότι το 5% της παραγωγής στη Βόρεια Αμερική χάνεται σε μη προγραμματισμένο χρόνο διακοπής λειτουργίας. Επειδή οι κόμβοι αισθητήρων μπορούν να ενσωματωθούν σε μηχανήματα χωρίς να υπάρχει κάποια ιδιαίτερη υποδομή, τα WSN καθιστούν οικονομικά εφικτή την παρακολούθηση της κατάστασης των μηχανών και διασφαλίζουν την ασφαλή λειτουργία τους. Για παράδειγμα, η γήρανση των αγωγών και των δεξαμενών είναι πλέον ένα σημαντικό πρόβλημα στη βιομηχανία πετρελαίου και φυσικού αερίου. Η παρακολούθηση της διάβρωσης στην οποία χρησιμοποιούνται χειροκίνητες διαδικασίες είναι εξαιρετικά δαπανηρή, χρονοβόρα και αναξιόπιστη. Ένα δίκτυο ασύρματων αισθητήρων διάβρωσης μπορεί να αναπτυχθεί χωρίς μεγάλα κόστη ώστε να εντοπίζει αξιόπιστα τα όποια προβλήματα πριν αυτά καταστούν καταστροφικά. Η Rohrback Cosasco Systems (RCS) είναι αυτή τη στιγμή ο παγκόσμιος ηγέτης στην τεχνολογία παρακολούθησης της διάβρωσης και εφαρμόζει αποτελεσματικά την ιδέα των WSN. Τα WSNs βρίσκουν επίσης εφαρμογή στην βιομηχανία τροφίμων, για να αποφεύγονται περιστατικά μόλυνσης της αλυσίδας εφοδιασμού τροφίμων και ελέγχου των ημερομηνιών λήξης [11].

4.6 Ασφάλεια υποδομών

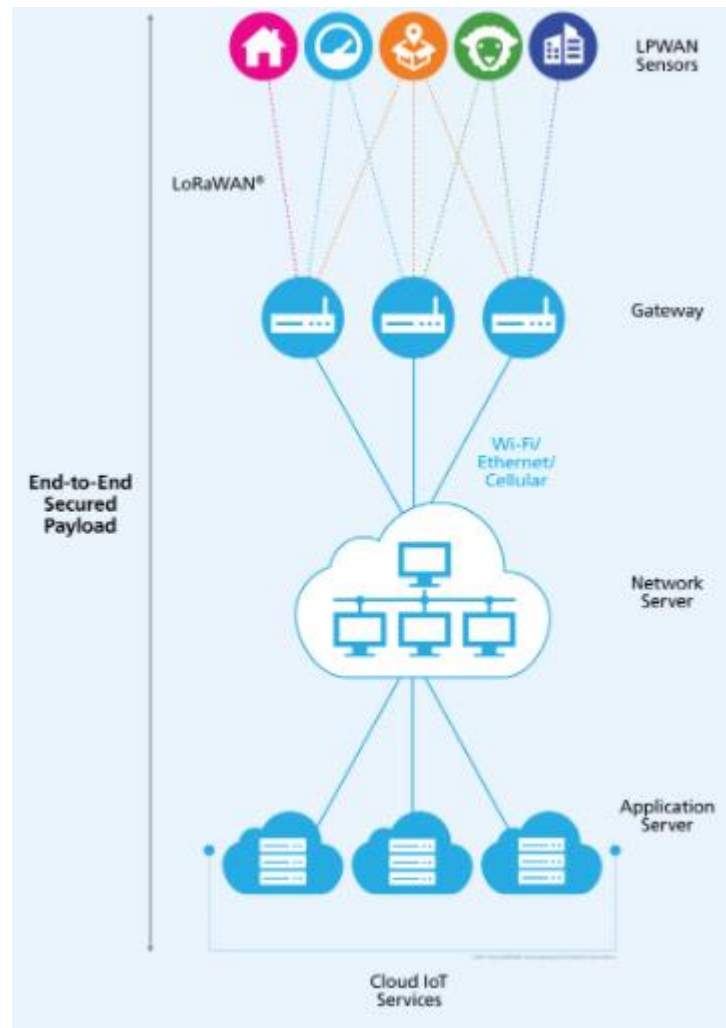
Τα WSN είναι κατάλληλα για χρήση σε συστήματα ασφάλειας σε χώρους με υψηλό κίνδυνο π.χ. για την αντιτρομοκρατία. Τέτοιες ευαίσθητες υποδομές και εγκαταστάσεις είναι οι σταθμοί παραγωγής ενέργειας, τα αεροδρόμια και οι στρατιωτικές βάσεις, οι οποίες πρέπει να προστατεύονται από πιθανές εισβολές. Δίκτυα βιντεοσκόπησης, μαγνητοφώνησης και άλλων αισθητήρων αποτελούν εφαρμογές που έχουν κατά καιρούς αναπτυχθεί γύρω από αυτές τις εγκαταστάσεις [13]. Για παράδειγμα, στο Διεθνές Αεροδρόμιο Πουντόνγκ στη Σαγκάη, εγκαταστάθηκε ένα σύστημα το οποίο εντοπίζει εισβολείς στο χώρο του αεροδρομίου και έτσι αποτρέπονται απροσδόκητα γεγονότα.

5

Ασύρματη δικτύωση με συστήματα χαμηλής ισχύος ευρείας περιοχής (LPWAN)

5.1 LoWPAN

Ένας τρόπος υλοποίησης LPWAN (Low Power Wide Area Networks) είναι η τεχνολογία LoRa (Long Range), που είναι κατάλληλη για την δημιουργία χαμηλής ισχύος δικτύων WAN. Τα δίκτυα αυτά έχουν τα κατάλληλα χαρακτηριστικά για να υποστηρίξουν κινητή αμφίδρομη επικοινωνία με χαμηλό κόστος σε εφαρμογές IoT. Παρά τη χαμηλή ενεργειακή κατανάλωση, είναι δυνατόν να υποστηρίξουν τη σύνδεση εκατομμυρίων τερματικών κόμβων, με ταχύτητες ικανοποιητικές για τον χρήστη, που φτάνουν μέχρι τα 50 Kbps [18].



Εικόνα 4: Συνδεσμολογία LoWPAN – LoRa

Πηγή: <https://www.semtech.com/lora/what-is-lora>

Η τεχνολογία LoRa λόγω της χρησιμοποίησης της τεχνικής της διασποράς φάσματος, έχει μεγαλύτερο εύρος ζώνης από ότι οι ανταγωνιστές της. Επίσης ένα χαρακτηριστικό που διαθέτει είναι η ενσωματωμένη δυνατότητα διόρθωσης σφαλμάτων (FEC – Forward Error Correction), και έτσι η μεταφορά των δεδομένων μπορεί να γίνει με χαμηλότερη ισχύ από το επίπεδο θορύβου του περιβάλλοντος, κάτι που επιτρέπει την επικοινωνία σε πολύ μεγάλες αποστάσεις. Ένα δεύτερο σπουδαίο χαρακτηριστικό που διαθέτει αυτή η υλοποίηση είναι η αμφίδρομη λειτουργικότητα, δηλαδή μπορεί εξίσου αποτελεσματικά να λαμβάνει μηνύματα από τα end points (τελικά σημεία), αλλά και να αποστέλλει μηνύματα από τους σταθμούς βάσης στα σημεία αυτά, κάτι απαραίτητο σε εφαρμογές εντολών ελέγχου [12].

Πίνακας 1: Χαρακτηριστικά LoRa

Συχνότητα	< 1GHz
Εμβέλεια σε υπαίθριες περιοχές	15 χλμ.
Εμβέλεια σε αστικές περιοχές	2-5 χλμ.
Ρυθμός μετάδοσης δεδομένων	0,3 - 50 Mbps

5.2 LoRaWAN

Το LoRaWAN ανήκει στα πρωτόκολλα LPWAN και είναι σχεδιασμένο με τρόπο που επιτρέπει μεγάλη εμβέλεια και χαμηλό ρυθμό μετάδοσης επικοινωνίας μεταξύ συσκευών, (π.χ. αισθητήρες). Χαρακτηριστικά της δικτύωσης LoRaWAN είναι η σημαντικά χαμηλή κατανάλωση, που οφείλεται στον χαμηλό ρυθμό μετάδοσης. Συγκεκριμένα, στα δίκτυα αυτά, ο ρυθμός μεταφοράς δεδομένων κυμαίνεται από 0.3 kbit / s ως 50 kbit / s σε κάθε κανάλι του δικτύου. Το LoRaWAN λειτουργεί σε μη αδειοδοτημένη περιοχή συχνοτήτων και έχει μεγάλη ασφάλεια σε όλο το φάσμα του δικτύου, από τις τελικές συσκευές μέχρι τον κάθε διακομιστή, αντίστοιχη με τα δίκτυα κινητής τηλεφωνίας.

Το δίκτυο καλύπτει τις ανάγκες των οργανισμών που χρησιμοποιούν εφαρμογές τόσο εσωτερικού όσο και εξωτερικού χώρου. Το πρωτόκολλο LoRaWAN σε συνδυασμό με τις LoRa συσκευές εκμεταλλεύονται όλα τα θετικά χαρακτηριστικά των ασύρματων δικτύων, προσφέροντας μια αποδοτική και ευέλικτη λύση οικονομικής συνδεσιμότητας που κρίνεται ως ιδανική για κάθε εφαρμογή IoT. Οι αισθητήρες μεταφέρουν τα δεδομένα που συγκεντρώνουν σε πλατφόρμες ανάλυσης, όπως σε πλατφόρμες μηχανικής μάθησης. Αυτή τη στιγμή υπάρχουν χιλιάδες δίκτυα LoRaWAN είτε δημόσια, είτε ιδιωτικά είτε υβριδικά σε πάνω από 110 χώρες [11].

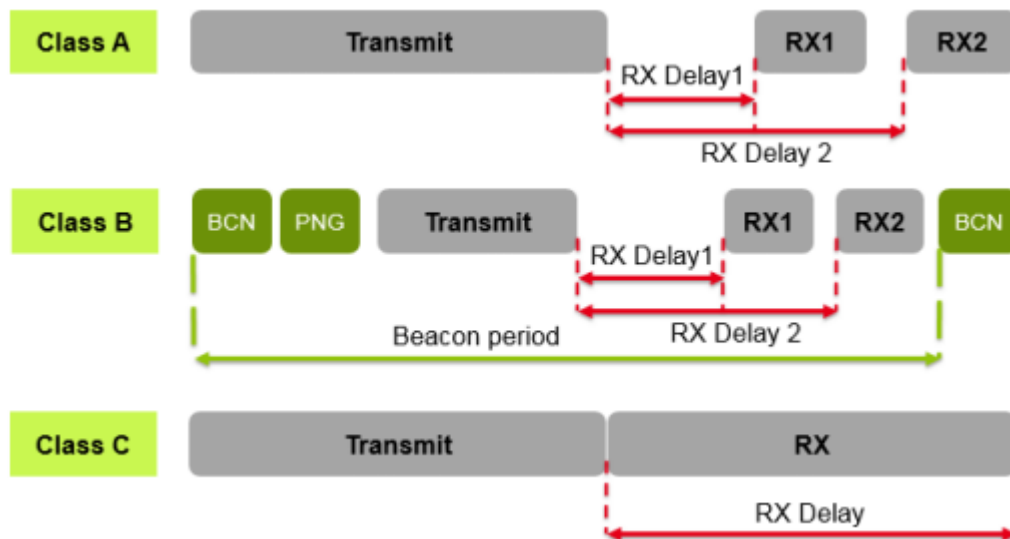
Πίνακας 2: Χαρακτηριστικά LoRaWan

Συχνότητα	868 / 902 MHz
Εμβέλεια σε υπαίθριες περιοχές	30-50 χλμ.
Εμβέλεια σε αστικές περιοχές	Έως 10 χλμ.
Ρυθμός μετάδοσης δεδομένων	0,3 – 50 Mbps

Υπάρχουν 3 κλάσεις LoRaWAN. Η κλάση A είναι πλήρως ασύγχρονη, και είναι γνωστή ως σύστημα ALOHA. Οι τελικοί κόμβοι μεταδίδουν όποτε κρίνεται απαραίτητο, χωρίς να απαιτείται κάποια άδεια / σήμα και το υπόλοιπο διάστημα παραμένουν αδρανείς. Όταν ολοκληρώσει ένας κόμβος τη μετάδοση του μηνύματός του, τότε μπορεί κάποιος άλλος να ξεκινήσει τη δική του μετάδοση, ώστε να γίνει η μετάδοση χωρίς πρόβλημα. Θεωρητικά, η μέγιστη χωρητικότητα ενός δικτύου ALOHA είναι περίπου 18.4% του μέγιστου. Αυτό συμβαίνει λόγω των συγκρούσεων, που συμβαίνουν αν δύο κόμβοι μεταδίδουν την ίδια στιγμή (στην ίδια συχνότητα).

Στην κλάση B κάθε gateway του LoRaWAN δικτύου, εκπέμπει κάθε 128 δευτερόλεπτα ένα beacon. Όλοι οι κόμβοι της κλάσης B έχουν ένα χρονικό παράθυρο εντός του κύκλου των 128 δευτερολέπτων και εκεί προσδιορίζεται πότε θα «ακούνε». Ένας κόμβος μπορεί να ακούει σε ένα δέκατο του παραθύρου, οπότε και επιτρέπεται η μετάδοση μηνυμάτων στην κατερχόμενη ζεύξη (downlink).

Στην κλάση C επιτρέπεται σε όλους στους κόμβους να ακούνε και να στέλνουν στην κατερχόμενη ζεύξη μηνύματα χωρίς περιορισμούς. Η κλάση αυτή χρησιμοποιείται κυρίως για εφαρμογές που δεν λειτουργούν με μπαταρία, επειδή χρειάζεται πολύ ενέργεια ώστε οι κόμβοι να είναι ενεργοί και να λαμβάνουν μηνύματα ανά πάσα στιγμή [8].



Εικόνα 5: Οι τρεις κλάσεις του LoRaWAN δικτύου.

Πηγή: https://www.researchgate.net/figure/a-LoRaWAN-network-architecture-and-b-LoRaWAN-protocol-stack_fig3_326134076

5.3 SigFox

Μία δεύτερη μορφή υλοποίησης LPWAN είναι η τεχνολογία SigFox, που λειτουργεί επίσης αρκετά αποτελεσματικά σε μεγάλες αποστάσεις. Η SigFox χρησιμοποιεί τις ζώνες ISM (Industrial, Scientific and Medical) για να μεταδώσει δεδομένα από αντικείμενα που είναι συνδεδεμένα (αλλά και προς αυτά), σε ένα πολύ στενό εύρος ζώνης.

Η φιλοσοφία της τεχνολογίας SigFox βασίζεται στο γεγονός ότι πολλές από τις συνδεδεμένες συσκευές τροφοδοτούνται με μικρής χωρητικότητας μπαταρίες, και έτσι μπορούν να υποστηρίξουν τη μεταφορά μικρών ποσοτήτων δεδομένων, σε αποστάσεις όπου δεν μπορούν να καλυφθούν από Wi-Fi, ενώ αν καλυφθούν από δίκτυα κινητής τηλεφωνίας, το κόστος της υλοποίησης αλλά και η κατανάλωση ισχύος θα ανέρθει σε υπερβολικά επίπεδα.

Η τεχνολογία SigFox απαιτεί την κατανάλωση μόνο 50 microwatts, δηλαδή το ένα εκατοστό σε σχέση με τις απαιτήσεις ενός δικτύου κινητής τηλεφωνίας. Αυτό στην πράξη σημαίνει ότι μπορεί με μία μπαταρία χωρητικότητας 3Ah να εκατονταπλασιαστεί ο χρόνος αναμονής (stand - by) μιας συσκευής, οπότε αν σε ένα δίκτυο κινητής τηλεφωνίας ο χρόνος αυτός είναι έξι μήνες, σε ένα SigFox δίκτυο μπορεί να είναι έως 600 μήνες [15].



Εικόνα 6: Σχήμα συνδεσμολογίας SigFox.

Πηγή: <https://www.cooking-hacks.com/documentation/tutorials/sigfox-connectivity-arduino-raspberry-pi-868mhz-europe-900mhz-us/index.html>

Η τεχνολογία SigFox είναι βασισμένη στο BPSK (Binary Phase-Shift Keying - Δυναδική Κωδικοποίηση Μετατόπισης Φάσης) σε εξαιρετικά στενά εύρη ζώνης - Ultra Narrow Band (UNB), όπου η μετάδοση γίνεται στις ζώνες 868 και 902 MHz, ανάλογα με την εκάστοτε περιοχή. Η ενεργειακή πυκνότητα του θορύβου στις UNB μεταδόσεις των Sigfox σημάτων είναι πιο πιθανό να υπερβαίνει το επίπεδο του θορύβου του περιβάλλοντος. Τα σήματα αυτά προσαρμόζονται πολύ καλά σε εφαρμογές που δεν απαιτούν πολύ υψηλή ταχύτητα μετάδοσης (μικρότερη από 300 Mbps), και συχνότητα μετάδοσης μηνυμάτων (έως 150 μηνύματα την ημέρα).

Για το λόγο αυτό, η τεχνολογία αυτή προτείνεται κυρίως για την επικοινωνία από τα τελικά σημεία προς τους σταθμούς βάσης, και όχι για την αντίστροφη διαδρομή, η οποία σίγουρα θα απαιτεί υψηλότερες ταχύτητες μετάδοσης και μεγαλύτερες συχνότητες μετάδοσης μηνυμάτων. Ωστόσο προσφέρει ένα πολύ ισχυρό και αρκετά οικονομικό δίκτυο με δυνατότητα επέκτασης, στο οποίο μπορούν να επικοινωνούν εκατομμύρια, ενεργειακά περιορισμένες, συσκευές τοποθετημένες σε πολύ μεγάλες αποστάσεις μεταξύ τους, Για αυτό και οι πρακτικές εφαρμογές είναι πάρα πολλές (π.χ. περιβαλλοντικοί αισθητήρες, αυτόματος φωτισμός, παρακολούθηση κλπ.) [18].

Πίνακας 3: Χαρακτηριστικά Sigfox

Συχνότητα	868 / 902 MHz
Εμβέλεια σε υπαίθριες περιοχές	30-50 χλμ
Εμβέλεια σε αστικές περιοχές	Έως 10 χλμ
Ρυθμός μετάδοσης δεδομένων	0,3 Mbps

5.4 Weightless

Το Weightless απαρτίζεται από ένα σύνολο LPWAN τεχνολογιών, που η διαχείριση τους γίνεται κεντρικά από την Weightless-Special Interest Group (SIG). Τα επιμέρους πρότυπα είναι τα Weightless – W, Weightless – N και Weightless – P [19].

- **Weightless - W:** Αυτό το πρότυπο έχει σχεδιαστεί για να λειτουργεί στο TVWS (TV White Space - τηλεοπτικό λευκό φάσμα). Η χρήση του TVWS είναι ελκυστική

θεωρητικά, επειδή εκμεταλλεύεται το φάσμα UHF (Ultra-High Frequency-εξαιρετικά υψηλής συχνότητας φάσμα) που δεν χρησιμοποιείται. Ωστόσο, στην πράξη, μπορεί να είναι αρκετά δύσκολο. Πρώτον, οι κανόνες και οι κανονισμοί για τη χρήση του TVWS για IoT διαφέρουν ανά γεωγραφική περιοχή. Επίσης, οι τελικοί κόμβοι είναι συνήθως σχεδιασμένοι να λειτουργούν μόνο σε ένα μικρό μέρος του φάσματος και είναι αδύνατο να κατασκευαστεί μια κεραία που μπορεί να χρησιμοποιεί όλα τα εύρη συχνοτήτων, από 400 MHz έως 800 MHz καθώς σε μια περιοχή μπορεί να υπάρχει διαθέσιμο κανάλι στα 500 MHz, ενώ σε άλλη μπορεί να υπάρχει διαθεσιμότητα στα 700 MHz. Επομένως, το TVWS στην πράξη δεν είναι τόσο πρακτικό. Το Weightless-W είναι ιδανικό για χρήση στην παρακολούθηση αποθεμάτων πετρελαίου και φυσικού αερίου, λόγω της διαθεσιμότητας του TVWS [20].

Πίνακας 4: Χαρακτηριστικά Weightless-W

Συχνότητα	400 - 800 MHz
Εμβέλεια	5 χλμ
Ρυθμός μετάδοσης δεδομένων	1 Kbps - 10 Mbps

- **Weightless-N:** είναι ένα σύστημα εξαιρετικά στενής ζώνης που μοιάζει πολύ με το SigFox, (κατά πολλούς αποτελεί την αντίστοιχη έκδοση του SigFox που βασίζεται στη LoRa Alliance). Δεν είναι ένα ολοκληρωμένο, από άκρο σε άκρο, κλειστό σύστημα, αλλά αποτελείται από ένα δίκτυο επιμέρους τομέων και συσκευών. Χρησιμοποιεί τον ίδιο τύπο διαμόρφωσης - BPSK - σε κανάλια στενής ζώνης και προορίζεται για μετάδοση δεδομένων από τερματικές συσκευές σε σταθμούς βάσης. Το Weightless-N είναι ιδανικό για δίκτυα που φέρουν συσκευές αισθητήρων, μετρητές θερμοκρασίας, παρακολούθηση αλλαγής καταστάσεων (π.χ. τη στάθμη μιας δεξαμενής) κλπ. [21].

Πίνακας 5: Χαρακτηριστικά Weightless-N

Συχνότητα	< 1 GHz
Εμβέλεια	2 χλμ
Ρυθμός μετάδοσης δεδομένων	100 bps

- **Weightless-P:** Αναπτύχθηκε το 2016 και αποτελεί την τελευταία από τις τεχνολογίες Weightless. Προσφέρει αμφίδρομο χαρακτηριστικά και ένα υψηλό επίπεδο ποιότητας υπηρεσιών. Λειτουργεί σε ένα σχετικά στενό εύρος ζώνης στα 12,5 kHz. Το Weightless χρησιμοποιεί διαμόρφωση GMSK (Gaussian Minimum Shift Keying - Gaussian Διαμόρφωση Ελάχιστης Μετατόπισης), και μια πιο τυπική διαμόρφωση την QPSK (Quadrature Phase Shift Keying - Ορθογώνια Μεταλλαγή Μετατόπισης Φάσης). Το Weightless-P είναι ιδανικό για ιδιωτικά δίκτυα και γενικότερα για πιο περίπλοκες υλοποιήσεις, όπου απαιτείται ικανοποιητική ταχύτητα και αμφίδρομη επικοινωνία [22].

Πίνακας 6: Χαρακτηριστικά Weightless-P

Συχνότητα	< 1 GHz
Εμβέλεια	3 χλμ
Ρυθμός μετάδοσης δεδομένων	200 bps - 100 Kbps

5.5 IEEE 802.11 (Wi-Fi)

Η τεχνολογία IEEE 802.11 ή, κοινώς, Wi-Fi περιλαμβάνει ένα σύνολο πρωτοκόλλων. Υπάρχουν τρία βασικά πρωτόκολλα της οικογένειας 802.11 με τις εξής κωδικοποιήσεις: 802.11a, 802.11b, 802.11g. Το κομμάτι της ασφάλειας αρχικά συμπεριλαμβανόταν στα πρότυπα αυτά αλλά τώρα είναι ανήκει κυρίως στο 802.11i.

Η πρώτη έκδοση του IEEE 802.11 προτυποποιήθηκε το 1997 και είχε δύο ρυθμούς μετάδοσης: 1 και 2 Mbps και τα μηνύματα μεταδίδονταν στην περιοχή των 2.4 GHz. Δεύτερο πρωτόκολλο ήταν το 802.11b το οποίο κάλυπτε μια ακτίνα έως και 50 μέτρα ενώ βασίζονταν σε χαμηλής ισχύος μονοκατευθυντικές κεραιές που ήταν τοποθετημένες στις 802.11b συσκευές. Σε μεταδόσεις υψηλής ισχύος το πρωτόκολλο αυτό μπορεί να χρησιμοποιηθεί σε επικοινωνίες από σημείο σε σημείο (point to point) σε εύρος μεγαλύτερο των 8 χιλιομέτρων. Το πρωτόκολλο 802.11b μεταδίδει με ρυθμό 11Mbps αλλά περίπου το μισό εύρος ζώνης δεσμεύεται για την προετοιμασία της επικοινωνίας, αφήνοντας έναν πραγματικό ρυθμό μετάδοσης δεδομένων στα 5,5Mbps. Προκειμένου να αυξηθεί ο ρυθμός μετάδοσης, κυκλοφόρησαν κάποιες επεκτάσεις που έφτασαν (θεωρητικά) το εύρος ζώνης στα 22 - 44 Mbps (πρωτόκολλο 802.11b+).

Συνεχίζοντας, το 802.11a προτυποποιήθηκε το 2001 και λειτουργεί στα 5 GHz με ρυθμό μετάδοσης 54 Mbps (πραγματικός ρυθμός μετάδοσης δεδομένων στα 20 Mbps). Το πρωτόκολλο 802.11a δεν έτυχε ευρείας εφαρμογής λόγω της υψηλής κατανάλωσης ενέργειας και άλλων προβλημάτων της συχνότητας των 5 GHz. Το 2003 επικυρώθηκε το πρότυπο 802.11.g που λειτουργεί στη συχνότητα 2,4 GHz, με στόχο να περιορίσει τα προβλήματα του 802.11.a, με ίδιο ρυθμό μετάδοσης δεδομένων (54 Mbps). Το πρωτόκολλο αυτό είναι συμβατό με το πρωτόκολλο 802.11.b, αν και ορισμένες φορές η χρήση πρωτοκόλλου 802.11.b σε δίκτυα 802.11.g, καθιστά το δίκτυο πιο αργό.

6

Ασύρματα Προσωπικά Δίκτυα (WPAN)

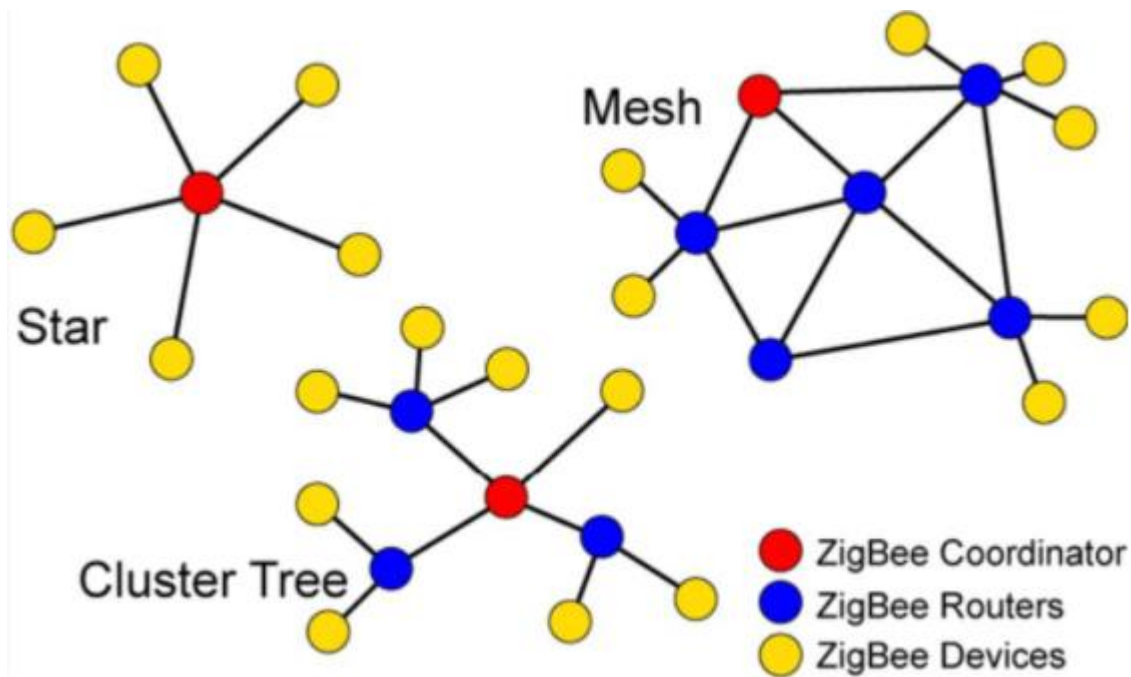
6.1 ZigBee

Μια τεχνολογία WPAN (Wireless Personal Area Networks) δικτύων είναι τα δίκτυα ZigBee. Στα δίκτυα αυτά οι συνδεόμενες συσκευές μπορεί να είναι:

- Συντονιστές (coordinators),
- Τερματικές διατάξεις (end devices)
- Δρομολογητές (routers).

Οι συντονιστές μαζί με τους δρομολογητές είναι κόμβοι πλήρους λειτουργίας (FFD - Full-Function Device). Οι τερματικές διατάξεις μπορεί να είναι κόμβοι είτε πλήρους λειτουργίας είτε περιορισμένης (FFD ή RFD - Reduced-Function Device). Τα δίκτυα ZigBee επηρεάζονται συχνά από παρεμβολές που δημιουργούνται εξαιτίας της ύπαρξης άλλων ασύρματων δικτύων. Η μείωση αυτών των παρεμβολών, γίνεται με τη χρήση του πρωτόκολλου CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) και με την τεχνική CCA (Clear Channel Assessment), ώστε οι κόμβοι να μεταδίδουν μόνο όταν είναι ελεύθερο το κανάλι, και αν δεν είναι, να μετατίθεται η εντολή της μετάδοσης.

Αναφορικά με τις τοπολογίες, στα δίκτυα τεχνολογίας ZigBee υποστηρίζεται η τοπολογία του αστέρα (star), του πλέγματος και του δένδρου συστάδων (cluster tree)[23].



Εικόνα 7: Τοπολογίες Zigbee: Αστέρα, δένδρο συστάδων, πλέγματος, όπου φαίνονται οι συσκευές (κίτρινοι κόμβοι), οι δρομολογητές (μπλε κόμβοι) και οι συντονιστές (κόκκινοι κόμβοι)

Πηγή: https://www.researchgate.net/figure/ZigBee-network-topologies-51_fig2_23307553

Στην πρώτη από αυτές, ο κεντρικός κόμβος είναι ο συντονιστής PAN (Personal Area Network), που συντονίζει τη λειτουργία των διατάξεων FFD και RFD, Στην δεύτερη, ενώ επίσης υπάρχει ο συντονιστής PAN, μπορούν οι υπόλοιποι κόμβοι να συνδέονται μεταξύ τους μέσω επικοινωνίας multi-hop (πολλαπλών αλμάτων). Περισσότερο η τοπολογία αυτή εφαρμόζεται σε ad-hoc δίκτυα. Τέλος, στην τρίτη τοπολογία κυρίως υπάρχουν συσκευές FFD και συνήθως λιγότερες RFD που λειτουργούν ως τερματικοί κόμβοι. Μόνο μία συσκευή FFD μπορεί να επιλεγεί ως συντονιστής PAN στο δίκτυο και είναι μοναδική, δεν μπορεί δηλαδή ταυτόχρονα να υπάρχει άλλη συσκευή FFD με τον ρόλο του συντονιστή [24].

6.2 6LoWPAN

Το πρωτόκολλο 6LoWPAN (Low Power WPAN) αποτελείται από ένα μεγάλο πλήθος συσκευών που έχουν χαμηλό κόστος και συνδέονται ασύρματα. Αντίθετα από άλλες τεχνολογίες, η τεχνολογία 6LoWPAN έχει κάποια σημαντικά πλεονεκτήματα όπως το μικρό μέγεθος των πακέτων, η χαμηλή απαίτηση σε ισχύ και οι μικρές απαιτήσεις σε εύρος ζώνης συχνοτήτων

(Bandwidth). Όμοια με την τεχνολογία Zigbee, στο πρωτόκολλο αυτό, τα IPV6 πακέτα μεταφέρονται μέσα από δίκτυα IEEE 802.15.4. Λόγω του χαμηλού κόστους αλλά και της χαμηλής κατανάλωσης σε ισχύ, το πρωτόκολλο αυτό θεωρείται ως ένα από τα καταλληλότερα για τις εφαρμογές IoT.

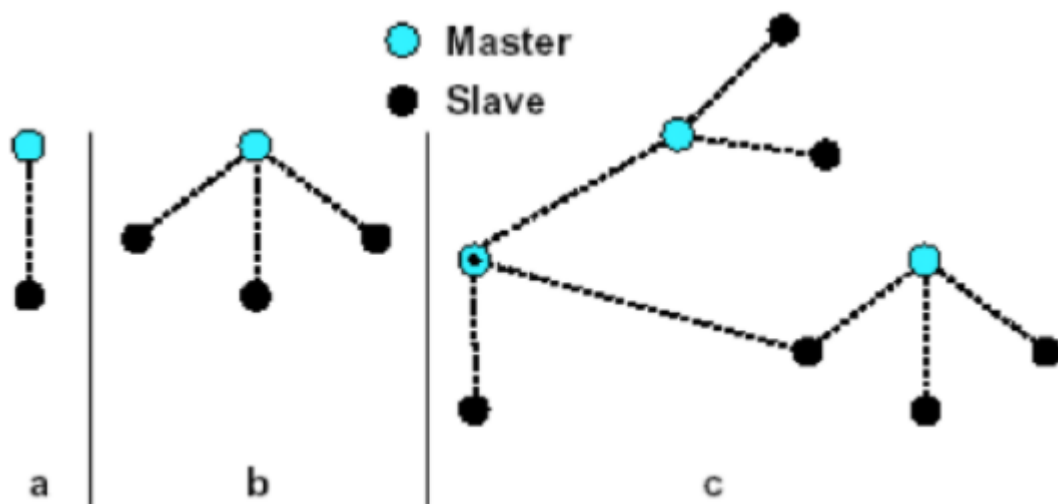
6.3 Bluetooth

Η τεχνολογία Bluetooth είναι βασισμένη στο πρωτόκολλο IEEE 802.15 και αποτελεί ένα βιομηχανικό πρότυπο ασύρματων προσωπικών δικτύων (WPAN). Χρησιμοποιεί στην ασύρματη μετάδοση σημάτων σε μικρές αποστάσεις και χρησιμοποιείται κατά κόρον για την επικοινωνία μεταξύ κινητών τηλεφώνων, φορητών και σταθερών υπολογιστών, tablets και άλλων συσκευών που μπορεί να υπάρχουν σε ένα προσωπικό δίκτυο (π.χ. κάμερες). Είναι μία αρκετά ασφαλής και οικονομική τεχνολογία, περιορισμένης εμβέλειας που λειτουργεί στη ζώνη των 2.4 GHz [25].

Η συχνότητα στην οποία λειτουργεί το Bluetooth είναι στα 2.4 GHz, ώστε να μπορούν οι συσκευές με την τεχνολογία αυτή να λειτουργούν οπουδήποτε και αν βρίσκονται. Για την ελαχιστοποίηση των παρεμβολών, που μπορεί να δημιουργηθούν από άλλες συσκευές, το Bluetooth χρησιμοποιεί τη μέθοδο μετάδοσης διασποράς φάσματος Frequency Hopping (μέχρι 1600 εναλλαγές συχνοτήτων ανά δευτερόλεπτο) για αμφίδρομη επικοινωνία. Η μετάδοση των δεδομένων, γίνεται με διαμοιρασμό των δεδομένων σε πακέτα και ακολούθως, μετάδοση του κάθε πακέτου, μέσα από κάποιο εκ των 70 διακριτών καναλιών που διαθέτει, καθένα από τα οποία έχει εύρος 1 MHz. Αρχικά χρησιμοποιούταν διαμόρφωση GFSK (Gaussian Frequency Shift Keying) με βασικό ρυθμό μετάδοσης (Basic Rate – BR) 1 Mb/s. Οι πιο σύγχρονες εκδόσεις Bluetooth χρησιμοποιούν DQPSK (Differential Quadrature Phase Shift Keying) που έχει ρυθμό μετάδοσης 2 Mbps και 8-DPSK, και που έχει ρυθμό μετάδοσης 3 Mbps. Ο συνδυασμός τους, προσφέρει έναν αυξημένο ρυθμό μετάδοσης δεδομένων (Enhanced Data Rate – EDR) και αποτελεί το «Basic Rate/Enhanced Data Rate Radio» [26].

Το Bluetooth προσφέρει τη δυνατότητα απευθείας σύνδεσης (point – to – point) ταυτόχρονα μέχρι 7 συσκευών σε μια μοναδική συχνότητα. Η τεχνολογία Bluetooth αναπτύχθηκε και υποστηρίζεται από το Bluetooth Special Interest Group. Βασική δομική μονάδα των δικτύων Bluetooth είναι το piconet, όπου όλοι οι κόμβοι μοιράζονται τον ίδιο κώδικα διασποράς και ελέγχονται από έναν κοινό Master κόμβο. Ο Master κόμβος έχει την αρμοδιότητα να διαμοιράζει στους κόμβους

(Slaves) την πρόσβαση με τη μέθοδο TDMA/TDD, ώστε καθένας να διαθέτει συγκεκριμένες χρονοθυρίδες στις οποίες θα μπορεί να στείλει πακέτα. Η εκπομπή του Master γίνεται σε περιττές χρονοθυρίδες και η εκπομπή των Slaves στις άρτιες. Όταν ένας κόμβος επιθυμήσει να εκπέμψει, ο Master του εκχωρεί δικαίωμα μετάδοσης σε συνεχόμενες περιττές χρονοθυρίδες, με κάθε πακέτο να εκπέμπεται στην ίδια συχνότητα. Κάθε κόμβος Slave έχει μια μοναδική διεύθυνση μήκους 48-bit και αποστέλλει αποκλειστικά στον Master. Στη συνέχεια αυτός αποστέλλει τα πλαίσιά στον παραλήπτη. Μπορούν να βρίσκονται περισσότερα από ένα piconets στον ίδιο χώρο χωρίς περιορισμό ενώ και οι κόμβοι μπορούν ταυτόχρονα να συμμετέχουν σε άνω του ενός piconets με την επικοινωνία τους να σχηματίζει ένα πιο σύνθετο δίκτυο (scatternet) [23].



Εικόνα 8: Τοπολογίες Bluetooth, όπου φαίνεται η σχέση μεταξύ Master και Slave στους κόμβους των δικτύων a, b, c.

Πηγή: https://www.researchgate.net/figure/Fig1-Bluetooth-Network-Topology-Bluetooth-SIG_fig1_328891203

Δύο τύποι συνδέσεων υπάρχουν:

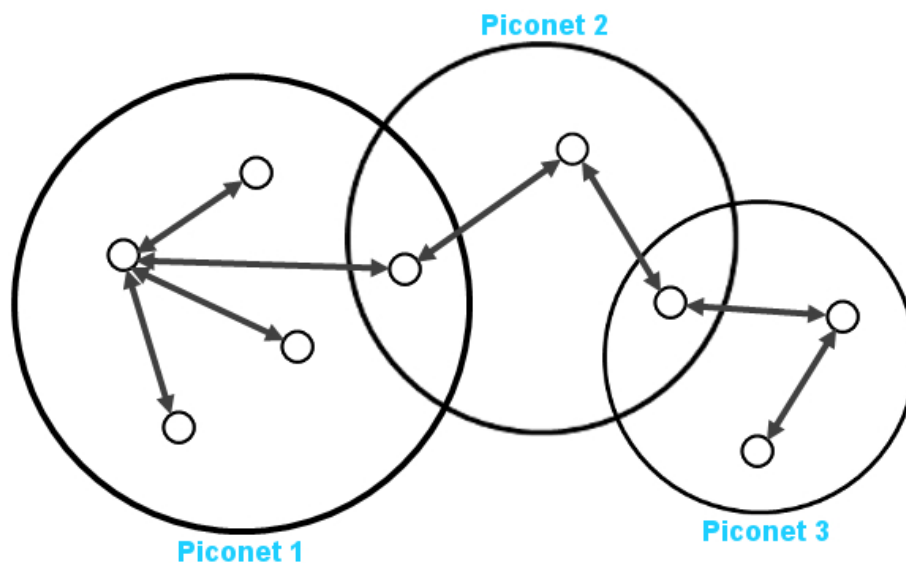
- 1) Οι σύγχρονες συνδέσεις, που έχουν ρυθμό μετάδοσης 64 kbps και υλοποιούν αμφίδρομη επικοινωνία σημείου προς σημείο, χρησιμοποιώντας αλγορίθμους για την ανίχνευση και διόρθωση σφαλμάτων (FEC), ενώ δεν πραγματοποιούν επιβεβαιώσεις ή επανεκπομπές και οι κόμβοι μπορεί να δεσμεύσουν έως μία χρονοθυρίδα και
- 2) Οι ασύγχρονες συνδέσεις, που έχουν ρυθμό μετάδοσης 24 kb/s, και έχουν δυνατότητα πολυεκπομπής (multicast). Ακόμα, οι συνδέσεις αυτές μπορούν να κάνουν έλεγχο

σφαλμάτων και ροής, μέσω της αποστολής θετικών ή αρνητικών επιβεβαιώσεων. Η εκπομπή ενός πακέτου δεδομένων, γίνεται για κάθε κόμβο με δέσμευση 1, 3 ή 5 χρονοθυρίδων [26].

6.4 Bluetooth Low Energy (BLE)

Όπως συμβαίνει και με το Bluetooth, η τεχνολογία αυτή είναι ένα πρότυπο για WPAN. Έχει αναπτυχθεί από το Bluetooth Special Interest Group. Είναι δημοφιλής σε καταστάσεις όπου υπάρχει επικοινωνία με κόμβους μικρού μεγέθους, κόστους και εμβέλειας, όπου απαιτείται χαμηλή κατανάλωση ενέργειας.

Είναι βασισμένη στο πρωτόκολλο IEEE 802.15.1 και η λειτουργία της λαμβάνει χώρα στη ζώνη των 2.4 GHz, ωστόσο χρησιμοποιεί διαφορετικό αριθμό καναλιών. Ειδικότερα, κάνει χρήση 40 καναλιών των 2 MHz σε αντίθεση με τα 70 κανάλια του 1 MHz που χρησιμοποιεί το Bluetooth. Η πρόσβαση αποκτάται μέσω Πολλαπλής Πρόσβασης Διαίρεσης Συχνότητας (FDMA) ή χρόνου (TDMA). Ο ρυθμός με τον οποίο μεταδίδονται τα δεδομένα είναι 1 Mb/s με χρήση GFSK διαμόρφωσης (Gaussian Frequency Shift Modulation) και η μέγιστη ισχύς εκπομπής είναι τα 10 mW. Επιπρόσθετα, γίνεται χρήση και της τεχνικής Frequency Hopping έτσι ώστε να αποφευχθούν τυχόν παρεμβολές. Μια από τις κύριες διαφορές με το τυπικό Bluetooth είναι ότι το BLE είναι σχεδιασμένο για να μπορεί να χρησιμοποιείται από συσκευές που απαιτούν μικρή κατανάλωση ενέργειας [21].

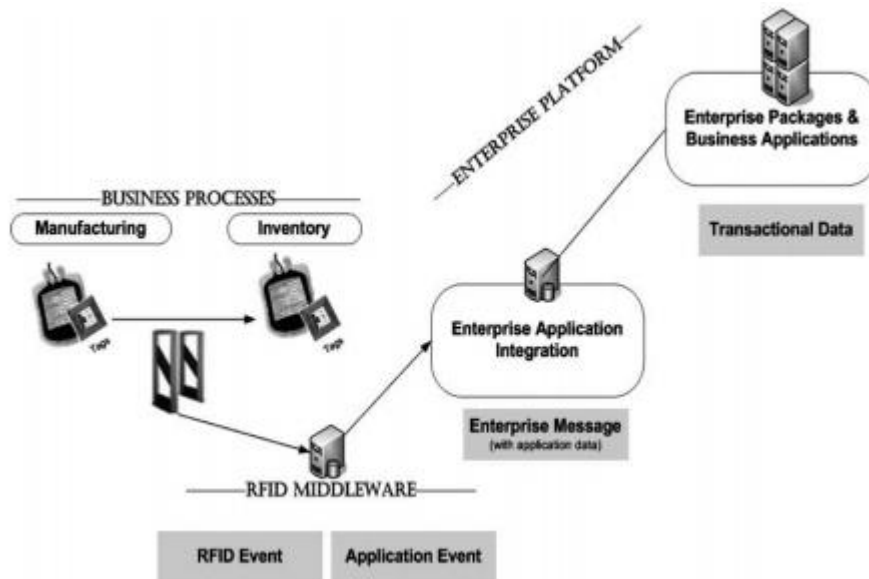


Εικόνα 9: Τοπολογία δικτύου BLE, χωρισμένο σε 3 υποδίκτυα (piconet 1,2,3)

Πηγή: <http://www.summitdata.com/blog/ble-overview/>

6.5 RFID

Η τεχνολογία RFID (Radio frequency identification) αποτελεί μια ασύρματη τεχνολογία για την ανταλλαγή των δεδομένων ανάμεσα σε έναν RFID αναγνώστη και σε μια ηλεκτρονική RFID ετικέτα (RFID Tag) μέσω ραδιοκυμάτων. Τα ηλεκτρομαγνητικά κύματα καθιστούν εφικτή τη μεταφορά δεδομένων ώστε ο αναγνώστης να διαβάσει ή να γράφει δεδομένα στην RFID tag (ή αντίστροφα).



Εικόνα 10: Αρχιτεκτονική της τεχνολογίας RFID

Πηγή: https://www.researchgate.net/figure/RFID-System-Architecture_fig3_278726171

Το σύστημα αρχίζει να λειτουργεί όταν μια RFID ετικέτα βρεθεί μέσα στην εμβέλεια του αναγνώστη. Τότε ενεργοποιείται το εσωτερικό κύκλωμα του αναγνώστη και ξεκινούν να μεταφέρονται τα δεδομένα. Μια RFID ετικέτα αποτελείται από δύο κύρια στοιχεία: ένα ολοκληρωμένο κύκλωμα και μια κεραία. Στο ολοκληρωμένο κύκλωμα γίνεται η αποθήκευση και η επεξεργασία των δεδομένων αλλά και η διαμόρφωση / αποδιαμόρφωση του ραδιοκύματος (RF Signal). Μέσω της κεραίας γίνεται η αποστολή και λήψη των σημάτων.

Τα RFID Tags χωρίζονται σε ενεργά και παθητικά. Τα ενεργά έχουν ενσωματωμένο το ολοκληρωμένο κύκλωμα και την κεραία, ενώ έχουν και μια πηγή ενέργειας μέσω της οποίας ενεργοποιείται το κύκλωμα προκειμένου να παραχθεί το σήμα που θα αποσταλεί. Τα ενεργά RFID tags είναι πιο ισχυρά από θέμα εμβέλειας και έχουν μεγαλύτερη μνήμη από ότι τα παθητικά, για αυτό και το μέγεθός τους είναι μεγαλύτερο από τα παθητικά. Τα δεύτερα, έχουν την

ίδια δομή αλλά δεν έχουν κάποια πηγή ενέργειας για αυτό και λειτουργούν παθητικά. Ενεργοποιούνται, δηλαδή, όταν δεχτούν ένα ραδιοκύμα προκειμένου να απαντήσουν. Εξ αιτίας της απουσίας της πηγής είναι μικρά σε μέγεθος και πολύ οικονομικά, ενώ έχουν μεγάλη διάρκεια ζωής.

6.6 NFC

Η τεχνολογία επικοινωνίας κοντινού πεδίου (Near Field Communication - NFC) είναι η εξέλιξη της τεχνολογίας RFID η οποία επιτρέπει αμφίδρομη επικοινωνία. Η μεταφορά των δεδομένων πραγματοποιείται με ρυθμό 106, 212 και 424 kbps σε αποστάσεις 4 έως 10 εκατοστών και σε συχνότητα 13.56 MHz. Υπάρχουν 3 είδη συσκευών με ενσωματωμένα NFC:

- NFC tags
- NFC αναγνώστες
- NFC κινητά τηλέφωνα

Τα τελευταία ανάλογα με το αν δρουν ως εκκινητές της διάδρασης ή ως αποδέκτες, έχουν ρόλο ενεργό ή παθητικό αντίστοιχα στην διαδικασία της επικοινωνίας. Ο διαχωρισμός αυτός αφορά το αν μια NFC συσκευή έχει δική της πηγή ενέργειας προκειμένου να έχει την δυνατότητα ασύρματης (RF) επικοινωνίας. Όταν μια ζεύξη λειτουργεί ενεργά, τότε οι δύο συσκευές παράγουν πεδίο NFC για την ανταλλαγή των δεδομένων. Αντίστοιχα, στην παθητική λειτουργία ο εκκινητής παράγει RF πεδίο και ο αποδέκτης χρησιμοποιεί την ενέργεια από το πεδίο του εκκινητή. Συνεπώς, ένα NFC tag που δεν διαθέτει εσωτερική πηγή ενέργειας λειτουργεί πάντα παθητικά στη διαδικασία της διάδρασης, όπως και στην περίπτωση του RFID, και εξαρτάται από την ενέργεια που έχει το πεδίο του NFC αναγνώστη ώστε να γίνει η ανταλλαγή των δεδομένων.

7

Κυψελωτά δίκτυα και IoT

Οι κυψελωτές τεχνολογίες αναφορικά με το IoT στοχεύουν στην υποστήριξη τις επικοινωνίας των αντικειμένων παρέχοντας την καλύτερη δυνατή ποιότητα και τη μέγιστη κάλυψη. Ωστόσο, οι απαιτήσεις της σύγχρονης επικοινωνίας δεν καλύπτονται από μια τεχνολογία, κάτι το οποίο σημαίνει ότι πρέπει να υπάρχουν προσαρμογές και να χρησιμοποιούνται για κάθε είδος επικοινωνίας οι αντίστοιχες τεχνολογίες.

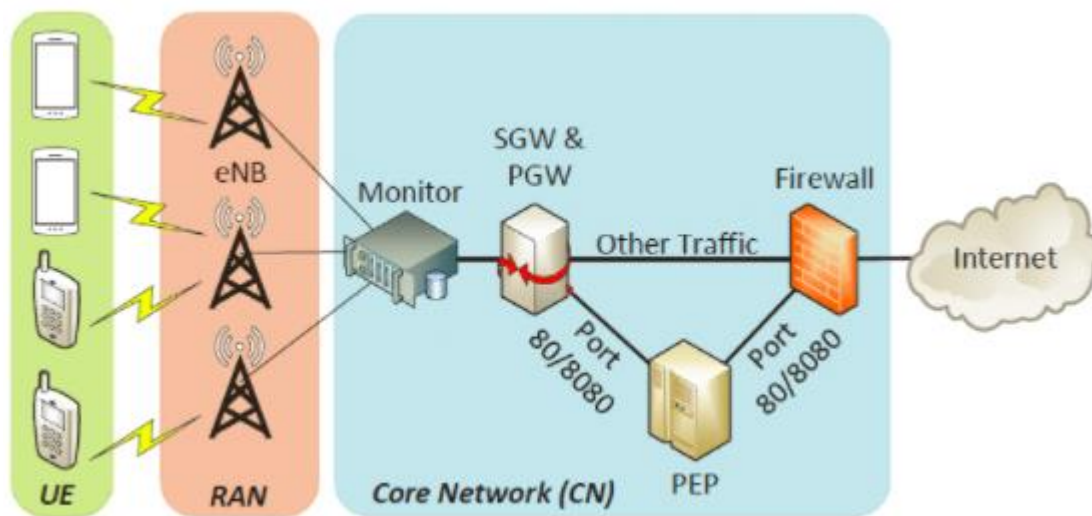
Η κύρια διαφορά των κυψελωτών συστημάτων σε σχέση με τις υπόλοιπες ασύρματες τεχνολογίες είναι ότι τα πρώτα έχουν σχεδιαστεί για να λειτουργούν μέσα σε αδειοδοτημένα εύρη συχνοτήτων, δηλαδή στις υπάρχουσες ζώνες των GSM και LTE, που προσφέρουν ασφάλεια και αποφυγή των παρεμβολών, κάτι που βελτιώνει την ποιότητα εξυπηρέτησης.

Οι επικοινωνίες μεταξύ αντικειμένων απαιτούν αμεσότητα και αξιοπιστία. Για το λόγο αυτό, το δίκτυο μέσω του οποίου επικοινωνούν τα αντικείμενα θα πρέπει να ικανοποιεί αυστηρές απαιτήσεις σε καθυστέρηση, να είναι αξιόπιστο ώστε να μην χάνονται πακέτα κατά την αποστολή και να παρέχει ασφάλεια σε περίπτωση σφαλμάτων [26]. Τα κυψελωτά δίκτυα 3G - 4G αποτελούν ένα πολύ δελεαστικό πλαίσιο για τη συνδεσιμότητα των αντικειμένων και την υλοποίηση των εφαρμογών IoT. Οι κυψέλες μπορούν να υποστηρίξουν ευρεία κάλυψη, με χαμηλό σχετικά κόστος. Παρακάτω παρουσιάζονται οι κυριότερες τεχνολογίες κυψελωτών δικτύων για διασύνδεση αντικειμένων.

7.1 LTE

Η τεχνολογία LTE η οποία χρησιμοποιείται σε κυψελωτά δίκτυα, επιτρέπει την ασύρματη επικοινωνία κινητών συσκευών με πολύ υψηλές ταχύτητες. Η τεχνολογία αυτή χρησιμοποιεί εξελιγμένες τεχνικές διαμόρφωσης προκειμένου να επιτύχει την αύξηση της ταχύτητας μετάδοσης αλλά και της συνολικής χωρητικότητας. Στην ουσία πρόκειται για ένα πραγματικά παγκόσμιο πρότυπο για ασύρματες συνδέσεις, μέσω του οποίου θα μπορεί να συνδεθεί κάθε ασύρματη συσκευή [27].

Η αύξηση της χωρητικότητας και της ταχύτητας των υφιστάμενων δικτύων με την τεχνολογία των LTE γίνεται με χρήση καινοτόμων τεχνικών για την ψηφιακή επεξεργασία και τη διαμόρφωση σήματος. Σημαντικό στοιχείο είναι ότι λειτουργεί σε διαφορετικά εύρη ζώνης συχνοτήτων σε σχέση με τα δίκτυα 2G και 3G. Χρειάστηκε μάλιστα να γίνουν κάποιες τροποποιήσεις προκειμένου να πληροί τις απαραίτητες προϋποθέσεις για να θεωρηθεί σύστημα 4G.



Εικόνα 11: Παράδειγμα LTE τοπολογίας.

Πηγή: https://www.researchgate.net/figure/The-LTE-network-topology-used-measurements-in-62_fig5_292945813

Το LTE για πρώτη φορά προτάθηκε το 2004 στην Ιαπωνία. Το 2008 οριστικοποιήθηκε το πρότυπο αυτό και τα πρώτα δίκτυα που υλοποιήθηκαν στον κόσμο για δημόσια χρήση, ήταν στη Στοκχόλμη και το Όσλο, μέσα από ενέργειες της εταιρίας TeliaSonera, το Δεκέμβρη του 2009. Τα πρώτα LTE έξυπνα κινητά τηλέφωνα (smartphones) που ήταν διαθέσιμα για εμπορική χρήση

διεθνώς ήταν τα Samsung Galaxy Indulge της Metro PCS και HTC Thunderbolt και κυκλοφόρησαν στην Β. Αμερική [28].

Το πρότυπο LTE έχει σχεδιαστεί για να παρέχει κατερχόμενη ζεύξη μεταφοράς δεδομένων (downlink) με ταχύτητες 300 Mbps και ανερχόμενη ζεύξη (uplink) έως 75 Mbps. Το εύρος ζώνης του σήματος δεν είναι σταθερό αλλά μεταβάλλεται σε ένα εύρος από τα 1.4 ως τα 20 MHz και υποστηρίζει τόσο το FDD (διπλεξία διαίρεσης συχνότητας) όσο και το TDD (διπλεξία διαίρεσης χρόνου). Η αρχιτεκτονική των LTE δικτύων χρησιμοποιεί την λογική του πρωτοκόλλου IP μέσω του λεγόμενου Evolved Packet Core (EPC), και υποστηρίζει την μετάδοση δεδομένων και φωνής απρόσκοπτα ακόμα και προς παλαιότερης τεχνολογίας δίκτυα, όπως τα GSM και UMTS. Η απλούστερη αυτή αρχιτεκτονική αποσκοπούσε στην ελαχιστοποίηση των λειτουργικών εξόδων [29].

Ο κυριότερος στόχος της τεχνολογίας LTE είναι η μετάβαση από τα δίκτυα 3G UMTS σε ένα ολοκληρωμένο δίκτυο με IP αρχιτεκτονική. Η ασύρματη διεπαφή των δικτύων LTE ονομάζεται E-UTRA και έχει τα ακόλουθα χαρακτηριστικά:

- Ρυθμό μετάδοσης δεδομένων κατερχόμενης ζεύξης μέχρι 300 Mbps και ανερχόμενης ζεύξης μέχρι τα 75 Mbps. Η πραγματική ταχύτητα ποικίλει ανάλογα με το είδος του εξοπλισμού που διαθέτει ο χρήστης. Υπάρχουν πέντε κατηγορίες (κλάσεις) τερματικών συσκευών. Η χαμηλότερη από αυτές υποστηρίζει αποκλειστικά απλή τηλεφωνία και η μεγαλύτερη, που απευθύνεται σε υψηλών προδιαγραφών τερματικές συσκευές υποστηρίζει τη μέγιστη δυνατή ταχύτητα μεταφοράς δεδομένων. Ωστόσο, οι τερματικές συσκευές κάθε κατηγορίας μπορούν να επεξεργαστούν σήματα σε εύρος ζώνης 20 MHz.
- Χαμηλή καθυστέρηση κατά τη διαδικασία της μεταφοράς δεδομένων (η καθυστέρηση των IP πακέτων είναι μικρότερη από 5 ms)
- Καλύτερη υποστήριξη επικοινωνίας με κινούμενους δέκτες μέχρι το όριο ταχύτητας των 500 χλμ./ώρα.
- Χρήση της OFDMA διαμόρφωσης στην κατερχόμενη ζεύξη και της SC-FDMA διαμόρφωσης στην ανερχόμενη.

- Υποστήριξη TDD, FDD (διπλεξία στο χρόνο και τη συχνότητα αντίστοιχα) αλλά και ημι - αμφίδρομη FDD όπου χρησιμοποιείται ίδια τεχνολογία πρόσβασης.
- Καλύτερη φασματική ευελιξία: προτυποποίηση καναλιών στα 1.4 MHz, 3 MHz, 5 MHz, 10 MHz, 15 MHz, 20 MHz.
- Υποστηρίζονται κυψέλες με μεταβλητό μέγεθος ξεκινώντας από μερικά μέτρα έως και 100 χλμ. Σε αγροτικές περιοχές η κυψέλη έχει μεγάλο εύρος και χρησιμοποιούνται χαμηλότερες συχνότητες ενώ στις αστικές περιοχές γίνεται χρήση υψηλών συχνοτήτων με το σκοπό να υποστηρίζονται υψηλότερες ταχύτητες και η κυψέλη συνήθως έχει μέγεθος το οποίο δεν ξεπερνά το 1 χλμ.
- Απλούστερη αρχιτεκτονική δικτύου.
- Υποστηρίζονται τουλάχιστον 200 ενεργές συνδέσεις δεδομένων σε κάθε κανάλι με εύρος 5 MHz.
- Υποστηρίζεται η δια-λειτουργικότητα και η συνύπαρξη παλαιότερων προτύπων. Οι χρήστες έχουν τη δυνατότητα να κάνουν μια τηλεφωνική κλήση ή σύνδεση δεδομένων σε μια περιοχή με κάλυψη LTE. Επίσης, η σύνδεσή τους δεν διακόπτεται ακόμα και όταν βρίσκονται σε περιοχές όπου δεν υπάρχει κάλυψη LTE, με τη χρήση του υφιστάμενου δικτύου GSM/GPRS ή W-CDMA.
- Υποστηρίζονται υπηρεσίες μετάδοσης τηλεοπτικών προγραμμάτων σε κινητές συσκευές, χρησιμοποιώντας τις υποδομές του LTE, κάτι το οποίο το καθιστά ανταγωνιστή του προτύπου DVB-H [16, 29].

Κάτι που υποστηρίζεται από το πρότυπο LTE είναι η μεταγωγή πακέτων, καθώς η όλη δομή του βασίζεται στην λογική IP. Όμως οι τηλεφωνικές κλήσεις προς τα δίκτυα GSM και UMTS πραγματοποιούνται με μεταγωγή κυκλώματος. Έτσι οι τηλεφωνικοί πάροχοι έπρεπε να επανακαθορίσουν τη λειτουργία του δικτύου για την πραγματοποίηση τηλεφωνικών κλήσεων. Για να επιλυθεί αυτό το ζήτημα, αναπτύχθηκαν τρεις εναλλακτικές επιλογές [25].

Αρχικά, εκείνοι που χρηματοδότησαν το εγχείρημα του LTE, ανέπτυξαν το Voice over LTE (VoLTE). Όμως, η απουσία υποστήριξης εφαρμογών για τις τερματικές συσκευές αλλά και για τις συσκευές που βρίσκονται στον πυρήνα του δικτύου, οδήγησαν κάποιους πάροχους στην ανάπτυξη του Voice over LTE Generic Access (VoLGA) ως μια μέση λύση. Η ιδέα που προκρίθηκε ήταν να

χρησιμοποιηθεί η φιλοσοφία πάνω στην οποία βασίστηκε το GAN (Generic Access Network), που καθορίζει τα πρωτόκολλα μέσω των οποίων τα κινητά τηλέφωνα μπορούν να πραγματοποιούν τηλεφωνικές κλήσεις, μέσω μιας ιδιωτικής σύνδεσης στο Ίντερνετ, κάτι που συνήθως γίνεται μέσω ενός ασύρματου τοπικού δικτύου. Ωστόσο, το VoLGA δεν έτυχε μεγάλης αποδοχής, επειδή το VoLTE υποσχόταν μεγαλύτερη ευελιξία στις υπηρεσίες του παρά το κόστος για την αναβάθμιση ολόκληρης της υποδομής του δικτύου. Παρόλο που η βιομηχανία του LTE έχει φαινομενικά καταλήξει στο VoLTE, η ανάγκη της άμεσης και ομαλής πραγματοποίησης τηλεφωνικών κλήσεων, οδήγησε τους παρόχους LTE στην εισαγωγή του Circuit Switched Fall Back (CSFB) ως μια προσωρινή λύση.

Το LTE έχει τη δυνατότητα να λειτουργεί σε ποικίλες συχνότητες. Στις ΗΠΑ και στον Καναδά, γίνεται χρήση των συχνοτήτων 700 MHz και 1.7 GHz. Στην Ευρώπη αντίστοιχα, γίνεται χρήση των συχνοτήτων 800 MHz, 1.8 και 2.6 GHz. Στην Ασία χρησιμοποιούνται οι συχνότητες 1.8 και 2.6 GHz και στην Αυστραλία οι συχνότητες στα 2.6 GHz. Επομένως για να πραγματοποιηθεί παγκόσμια περιαγωγή η LTE συσκευή πρέπει να έχει τη δυνατότητα να συντονίζεται σε πολλαπλές μπάντες συχνοτήτων [24].

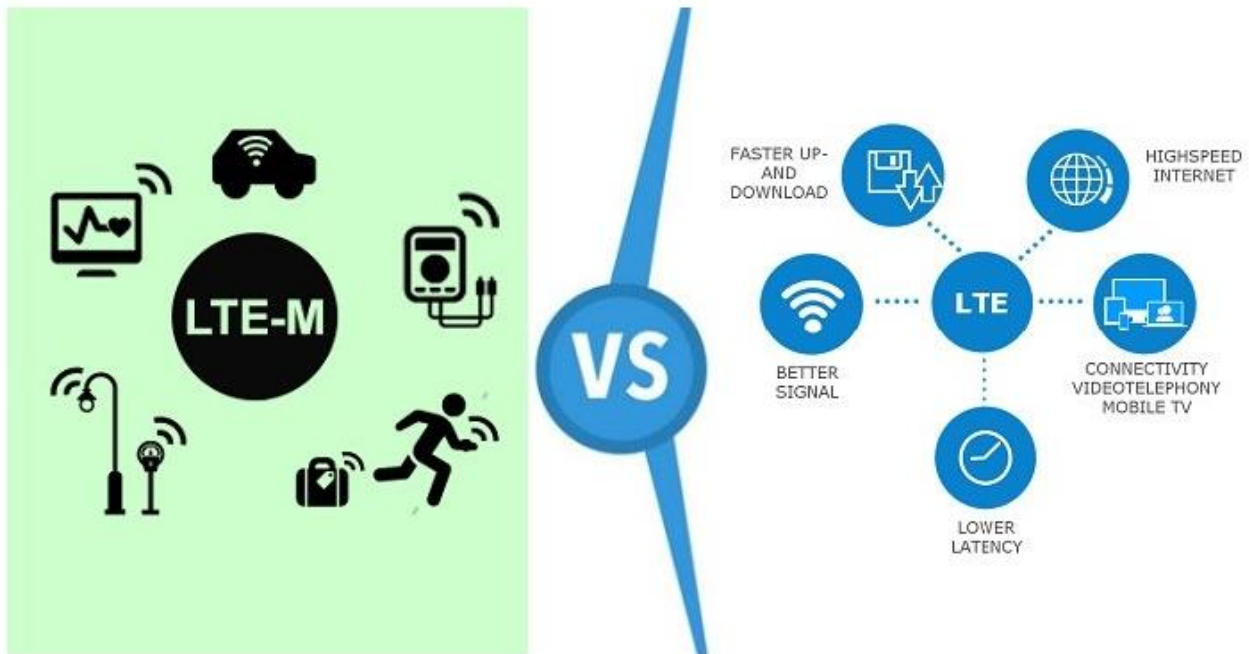
7.2 LTE-M

Το πρότυπο LTE-M (Machine) μελετήθηκε από την 3GPP για επικοινωνίες τύπου μηχανής σε ευρείες περιοχές αξιοποιώντας το πρότυπο LTE. Έτσι στο LTE-M έχουν εισαχθεί σχετικές τροποποιήσεις, όπως:

- Βελτιστοποιήσεις των υπηρεσιών VoLTE και άλλων υπηρεσιών για μετάδοση σε πραγματικό χρόνο.
Οι συσκευές των χρηστών υποστηρίζουν VoLTE, ωστόσο τέθηκαν περιορισμοί στην τάξη διαμόρφωσης, με το σταθμό βάσης (eNB) να έχει πλέον τη δυνατότητα να περιορίζει την τάξη διαμόρφωσης των δεδομένων τόσο στην κατερχόμενη όσο και στην ανερχόμενη ζεύξη.
- Λιγότερο αυστηρός έλεγχος επανεπιλογής κελιού.

Όταν ενεργοποιείται το χαρακτηριστικό αυτό, το κινητό έχει τη δυνατότητα μείωσης των μετρήσεων παρακολούθησης της στάθμης ισχύος των σημάτων των γειτονικών του κελιών. Έτσι είναι εφικτή η μείωση της κατανάλωσης ισχύος των συσκευών, ιδιαίτερα όταν υπάρχουν προβλήματα στην κάλυψη του δικτύου. Επίσης, ο σταθμός eNB έχει τη δυνατότητα να επιλέξει την κεραία μετάδοσης της συσκευής, αν αυτή υποστηρίζει πολλαπλές κεραίες για τη μετάδοση των σημάτων.

- Τρίτη εφαρμογή για τη βελτίωση της κάλυψης είναι τα σήματα αναφοράς (Sounding Reference Signal – SRS), που υποστηρίζουν την βελτίωση της λειτουργίας της προσαρμογής της μετάδοσης στο κανάλι (link adaption).
- Κατηγορία ισχύος 6 (14 dBm).
Για να μειωθεί η κατανάλωση ισχύος, ανάλογα με την κατηγορία στην οποία εντάσσονται οι συσκευές, εισήχθη μια νέα κατηγορία όπου η μέγιστη ισχύς μετάδοσης είναι τα 14 dBm.
- Αυξημένη φασματική απόδοση.
Εισήχθη η διαμόρφωση 64 QAM για τη μετάδοση χωρίς επαναλήψεις στα κανάλια της κατερχόμενης ζεύξης προκειμένου να αυξηθεί η φασματική απόδοση. Επίσης, χρησιμοποιείται η λογική του πίνακα CQI (Channel Quality Indicator), μέσω του οποίου γίνεται αντιληπτή από τις συσκευές η ποιότητα των καναλιών [19]



Εικόνα 12: Σχηματική αναπαράσταση της διαφοράς των δικτύων LTE (δεξιά) και LTE -M (αριστερά).

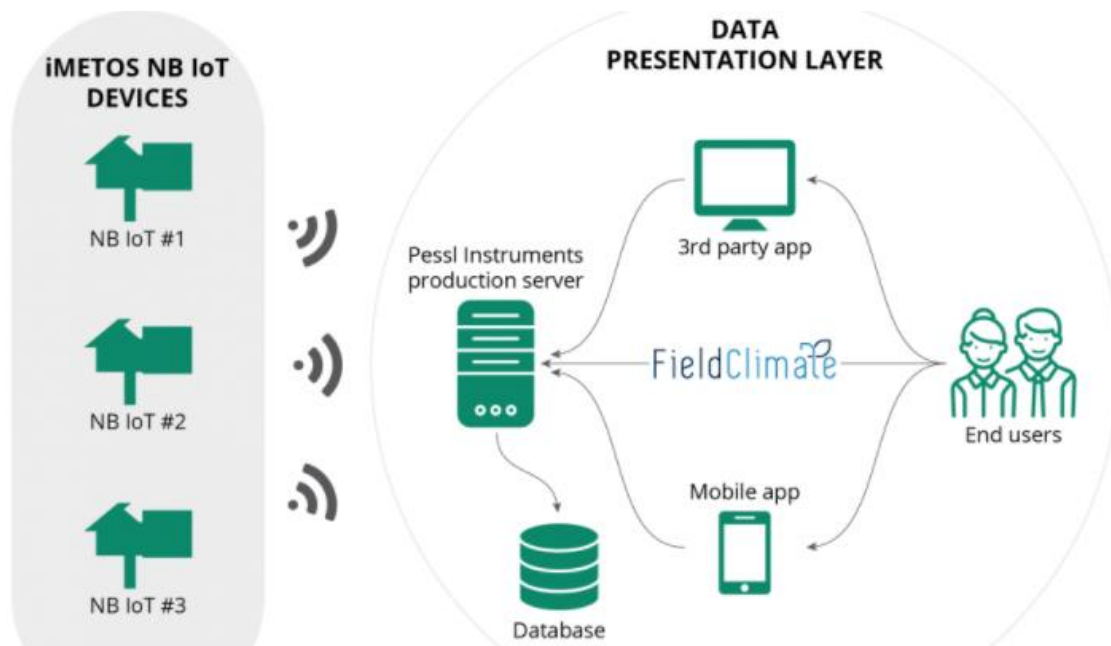
Πηγή: <https://www.everythingrf.com/community/what-is-difference-between-lte-and-lte-m>

7.3 Narrow Band - IoT

Το πρότυπο NB-IoT (Narrow Band-IoT), αποτελεί την εξέλιξη του LTE Cat-M1 και αναπτύχθηκε από τη 3GPP (Release-13) [20]. Η τεχνολογία NB-IoT σχεδιάστηκε για να διευκολύνει την ανάπτυξη του IoT ώστε οι υπάρχοντες διαχειριστές των δικτύων να μπορούν να εισάγουν τη τεχνολογία αυτή σε δίκτυα που είναι ήδη εγκατεστημένα και να μην υπάρχει η ανάγκη δημιουργίας νέων εξ αρχής.

Σχεδιάστηκε με τρόπο που να διασφαλίζει την υποστήριξη σε ευαίσθητες εφαρμογές, για παράδειγμα αισθητήρες που βρίσκονται σε απομακρυσμένα σημεία, ή σε έξυπνα σπίτια και σε έξυπνους μετρητές. Το NB - IoT μπορεί να λειτουργήσει εντός του πλαισίου των υπολοίπων κυψελωτών δικτύων GSM, GPRS αλλά και με LTE δίκτυα, πολύ αποδοτικά. Έτσι, το NB-IoT λειτουργεί με τις ελάχιστες απαιτήσεις εύρους ζώνης (180 KHz) τόσο στην κατερχόμενη όσο και στην ανερχόμενη ζεύξη. Επιπλέον, η ανάπτυξη των δικτύων NB-IoT μπορεί να πραγματοποιηθεί με τους εξής τρόπους:

- **In-band:** Η μετάδοση των δεδομένων ελέγχου γίνεται μέσω των πόρων που χρησιμοποιούνται συνήθως για επικοινωνία με τους σταθμούς βάσης.
- **Guard band:** Αξιοποιούνται φάσματα συχνοτήτων που δεν χρησιμοποιούνται (180 kHz)
- **Standalone system:** Η μετάδοση των δεδομένων γίνεται σε κανάλια και συχνότητες υπάρχοντων δικτύων, όπως είναι το GSM / GPRS.



Εικόνα 13: Παράδειγμα τοπολογίας NB-IoT.

Πηγή: <https://metos.at/imetos-nbiot/>

Για να παραμείνει σε χαμηλά επίπεδα η πολυπλοκότητα των συσκευών αλλά και το κόστος των δικτύων NB-IoT και να υπάρχει λειτουργικότητα, ο μέγιστος ρυθμός δεδομένων στην κατερχόμενη ζεύξη είναι ακόμα χαμηλότερος κατά τις καταστάσεις In-Band και Standalone (32 kbps και 34 kbps αντίστοιχα). Εξίσου χαμηλός είναι και ο μέγιστος ρυθμός της ανερχόμενης ζεύξης, (66 kbps) που φτάνει σε ακόμα χαμηλότερα επίπεδα στις multi-tone και single-tone μεταδόσεις 16.9 kbps [19].

7.4 EC-GSM - IoT

Το εκτεταμένης κάλυψης GSM IoT – (EC-GSM-IoT) πήρε το όνομά του από την επέκταση κατά 20 dB που επιτυγχάνει, χάρη στη χρήση των ζωνών sub – GHz, που στην πράξη οδηγεί σε αύξηση της ισχύος του σήματος στους εσωτερικούς χώρους, ενώ υποστηρίζει την σύνδεση 50000 συσκευών σε κάθε σταθμό βάσης. Το link budget (ισοζύγιο ζεύξης), κυμαίνεται μεταξύ 154 και 164 dB, και καθορίζεται από την ισχύ της εκπομπής. Το EC-GSM αξιοποιεί την τεχνική των επαναληπτικών μεταδόσεων ενώ η επεξεργασία σήματος που υποστηρίζει βοηθά στη βελτίωση της κάλυψης του κλασικού δικτύου GPRS. Χρησιμοποιεί τις τεχνολογίες Gaussian Minimum Shift Keying (GMSK) και 8-Phase Shift Keying (8PSK) για τη διαμόρφωση των πακέτων, οι οποίες παρέχουν ευελιξία στην ταχύτητα μετάδοσης με 240 Kbps peak rate (ρυθμό αιχμής) [4].

Η τεχνολογία αυτή οδηγεί σε κυψελοειδή συστήματα μεγαλύτερης χωρητικότητας και εμβέλειας με χαμηλές ενεργειακές απαιτήσεις και χαμηλή πολυπλοκότητα και χρησιμοποιείται κατά κόρον για να υποστηρίξει σχήματα IoT. Δεν απαιτεί εκ νέου δημιουργία δικτύου, αλλά μπορεί να διαμορφωθεί μέσα από την αναβάθμιση λογισμικού, των υπαρχόντων δικτύων GSM. Οι συσκευές, που συνδέονται στα EC – GSM-IoT, έχουν διάρκεια ζωής (μπαταρίας) που φτάνει τα 10 χρόνια, σε περιπτώσεις ευρείας χρήσης [30]. Ακόμα, οι υπάρχουσες μονάδες GSM δεν επηρεάζονται λόγω της εγκατάστασης των συσκευών EC-GSM, με τις παλαιότερες συσκευές GSM και τις συσκευές EC – GSM-IoT να μπορούν να συνυπάρξουν μέσω πολυπλεξίας ακόμα και στο ίδιο φυσικό κανάλι. Τέλος, τα δίκτυα EC-GSM-IoT χρησιμοποιούν 200 KHz εύρος ζώνης ανά κανάλι, φτάνοντας τα 2.4 MHz (συνολικό εύρος ζώνης) [14].

Πίνακας 7: Συγκεντρωτικός πίνακας τεχνολογιών

Τεχνολογία	Συχνότητα	Ρυθμός μετάδοσης	Εμβέλεια	Κατανάλωση	Κόστος
Bluetooth/BLE	2.4 GHZ	1, 2, 3 Mbps	~300 feet	Χαμηλό	Χαμηλό
802.15.4	SubGHZ, 2.4 GHZ	40, 250 kbps	> 100 square miles	Χαμηλό	Χαμηλό
LoRa	subGHZ	<50 kbps	1-3 miles	Χαμηλό	Μεσαίο
LTE Cat 0/1	Cellular Bands	1-10 Mbps	Several miles	Μεσαίο	Υψηλό

NB -IoT	Cellular Bands	0.1-1 Mbps	Several miles	Μεσαίο	Υψηλό
SigFox	subGHZ	<1 kbps	Several miles	Χαμηλό	Μεσαίο
Weightless	subGHZ	0.1-24 Mbps	Several miles	Χαμηλό	Χαμηλό
Wi-Fi	SubGHZ, 2.4 GHZ, 5 GHZ	0.1-54 Mbps	<300 feet	Μεσαίο	Χαμηλό
ZigBee	2.4 GHZ	250 kbps	~300 feet	Χαμηλό	Μεσαίο
RFID	LF/HF/UHF/ Microwave 13.56 MHZ	50 kbit/s	>3m	Υψηλό	Χαμηλό
NFC	13.56 MHZ	424 kbit/s	>0,10m	Χαμηλό	Χαμηλό
EC-GSM-IoT	700- 1000MHZ	70 kbps for GMSK, 240 kbps for 8PSK	<15km	Χαμηλό	Χαμηλό

8

Προσομοίωση Έξυπνου Σπιτιού με χρήση του Cisco Packet Tracer

Στον σημερινό τεχνολογικά αναπτυσσόμενο κόσμο, η τεχνολογία βρίσκει εφαρμογή συχνά στη καθημερινή ζωή. Το σπίτι που περιλαμβάνει έξυπνα αντικείμενα με συγκεκριμένες λειτουργίες ονομάζεται έξυπνο σπίτι. Σκοπός του είναι να βελτιώσει την ασφάλεια, την άνεση και την αποδοτικότητα μέσω της αυτοματοποίησης των οικιακών δραστηριοτήτων. Υπάρχουν συνήθως εργαλεία παρακολούθησης και οι συσκευές, που είναι ελεγχόμενες και αυτόματες, μπορούν να προσεγγιστούν μέσω ενός υπολογιστή συνδεδεμένου στο Διαδίκτυο ή μιας έξυπνης κινητής συσκευής.

Αντί να παρέχει την κλασσική μορφή ασφάλειας του παρελθόντος, το έξυπνο σπίτι μπορεί να παρέχει διάφορες λειτουργίες για την παροχή ασφάλειας χρησιμοποιώντας αυτόματα συστήματα συναγερμού που συνδυάζουν την χρήση οθονών και ήχου (σειρήνας) αλλά και την αποστολή μηνύματος (π.χ. email) σε προεπιλεγμένους χρήστες, εάν ένας αισθητήρας εντοπίσει προβλήματα ασφαλείας. Ο οικιακός αυτοματισμός αναφέρεται στον χειρισμό και την παρακολούθηση οικιακών αντικειμένων χρησιμοποιώντας μικροελεγκτές ή υπολογιστές. Η αυτοματοποίηση καθιστά τη διαδικασία απλή, παραγωγική και ασφαλή.

Όλες οι έξυπνες συσκευές είναι καταχωρημένες στην home gateway στην παρακάτω μελέτη περίπτωσης και ελέγχονται από αρμόδιο άτομο. Συμπεριλαμβάνοντας διαφορετικούς αισθητήρες στον οικιακό αυτοματισμό, το Smart Home εξαλείφει την ανάγκη των χρηστών για την παρακολούθηση των ρυθμίσεων λειτουργίας των οικιακών συσκευών. Το Διαδίκτυο των Αντικειμένων (IoT) αποτελεί το δίκτυο επικοινωνίας πληθώρας συσκευών και γενικά κάθε αντικειμένου που ενσωματώνει ηλεκτρονικά μέσα, λογισμικό, αισθητήρες και συνδεσιμότητα σε δίκτυο ώστε να είναι δυνατή η ανταλλαγή δεδομένων. Απλούστερα, η φιλοσοφία του IoT είναι η σύνδεση όλων των ηλεκτρονικών συσκευών μεταξύ τους (τοπικό δίκτυο) ή με δυνατότητα σύνδεσης στο διαδίκτυο (παγκόσμιο ιστό). Το Διαδίκτυο των Πάντων (IoE) είναι μια θεωρία που επιτείνει την έμφαση στην επικοινωνία μεταξύ μηχανών (M2M) του Διαδικτύου των Αντικειμένων για να περιγράψει ένα πιο περίπλοκο σύστημα που περιλαμβάνει επίσης ανθρώπους και διαδικασίες. Το IoE είναι μια έξυπνη σχέση ανθρώπων, μεθόδων και πληροφοριών. Το Διαδίκτυο των Πάντων (IoE) περιγράφει ένα σύστημα στο οποίο δισεκατομμύρια οντότητες έχουν αισθητήρες για τη μέτρηση και τον προσδιορισμό της κατάστασής τους και διασυνδέονται μέσω δημόσιων ή ιδιωτικών δικτύων.

Αυτό το κεφάλαιο περιγράφει την εφαρμογή του έξυπνου σπιτιού με τη χρήση της τελευταίας έκδοσης του Cisco Packet Tracer (7.2.), καθώς αυτή η έκδοση περιλαμβάνει διαφορετικούς αισθητήρες, ενεργοποιητές και έξυπνες συσκευές που χρησιμοποιούνται για οικιακό αυτοματισμό. Τα έξυπνα φώτα, έξυπνα παράθυρα, έξυπνοι ανεμιστήρες, έξυπνες πόρτες με διάφορους ανιχνευτές και αισθητήρες είναι μερικές από τις συσκευές που θα μελετηθούν. Η τελευταία έκδοση του προγράμματος προσομοίωσης για μοντελοποίηση και διαμόρφωση συστημάτων είναι το IoE Cisco Packet Tracer.

8.1 Πλεονεκτήματα του Packet Tracer

Το Cisco Packet Tracer είναι μια εφαρμογή μοντελοποίησης δικτύων της Cisco system Academy που μπορεί να προσομοιώσει / δημιουργήσει ένα δίκτυο. Είναι μια απλή στη χρήση και εξαιρετικά αποτελεσματική [11], [12] εφαρμογή ενώ επιπλέον, στην έκδοση 7.2 μπορεί να λειτουργήσει υβριδικά συνδυάζοντας πραγματικά δίκτυα με εικονικά δίκτυα [13].

Τα πλεονεκτήματα του Packet Tracer είναι:

- Παρέχει πρακτικές προσομοιώσεις και απεικονίσεις μηχανών IoT.
- Επιτρέπει στους χρήστες να σχεδιάζουν, να δημιουργούν, να προσαρμόζουν έξυπνα σπίτια, έξυπνες πόλεις, παρέχοντάς τους διάφορα έξυπνα αντικείμενα.
- Παροχή πλακέτας για τον έλεγχο ευφυών αντικειμένων.
- Επιτρέπει στους μαθητές να εξερευνήσουν τις έννοιες των αρχών του IoE.
- Παρέχει αισθητήρες ανίχνευσης

8.2 Μεθοδολογία

Στο πρακτικό μέρος της παρούσας εργασίας, ο βασικός στόχος είναι ο σχεδιασμός ενός έξυπνου σπιτιού στο λογισμικό περιβάλλον “Packet Tracer”, με τη χρήση της τεχνολογίας Internet of Things και δικτύων κινητής τηλεφωνίας. Το σπίτι διαθέτει τα εξής δωμάτια / χώρους:

- Κουζίνα
- Σαλόνι
- Μπάνιο
- 2 κρεβατοκάμαρες
- Δωμάτιο γραφείου
- Κήπο

Κάθε δωμάτιο έχει ένα διαφορετικό σύνολο έξυπνων συσκευών, όπου όλες συνδέονται στο ίδιο δίκτυο, ώστε η οικογένεια που διαμένει εκεί να μπορεί να τις ελέγχει μέσω του κινητού τηλεφώνου, οπουδήποτε και αν βρίσκεται.

Ο διαμοιρασμός συσκευών σε δωμάτια έχει ως εξής:

Κουζίνα

- Σώμα καλοριφέρ
- Θερμόμετρο
- Θερμοστάτης
- Καφετιέρα
- Ανεμιστήρας
- Λάμπα

- Ανιχνευτή καπνού
- Παράθυρο
- Σειρήνα συναγερμού

Κήπος

- Γκαραζόπορτα
- Μετρητής υγρασίας
- Ηλιακό πάνελ
- Λάμπα
- Ανεμόμετρο
- Αυτόματο πότισμα (2X)
- Πόρτα

Δωμάτιο γραφείου

- Θερμόμετρο
- Σώμα καλοριφέρ
- Παράθυρο
- Σειρήνα συναγερμού
- Ανιχνευτής καπνού
- Web κάμερα
- Ανεμιστήρας οροφής
- Φως
- Εκτυπωτής
- Η / Υ

Σαλόνι

- Σώμα καλοριφέρ
- Κλιματιστικό
- Θερμόμετρο

- Παράθυρο
- Ηχεία (2Χ)
- Θερμοστάτης
- Μετρητής υγρασίας
- Αφυγραντήρας
- 2 λάμπες
- Σειρήνα συναγερμού
- Ανιχνευτής καπνού

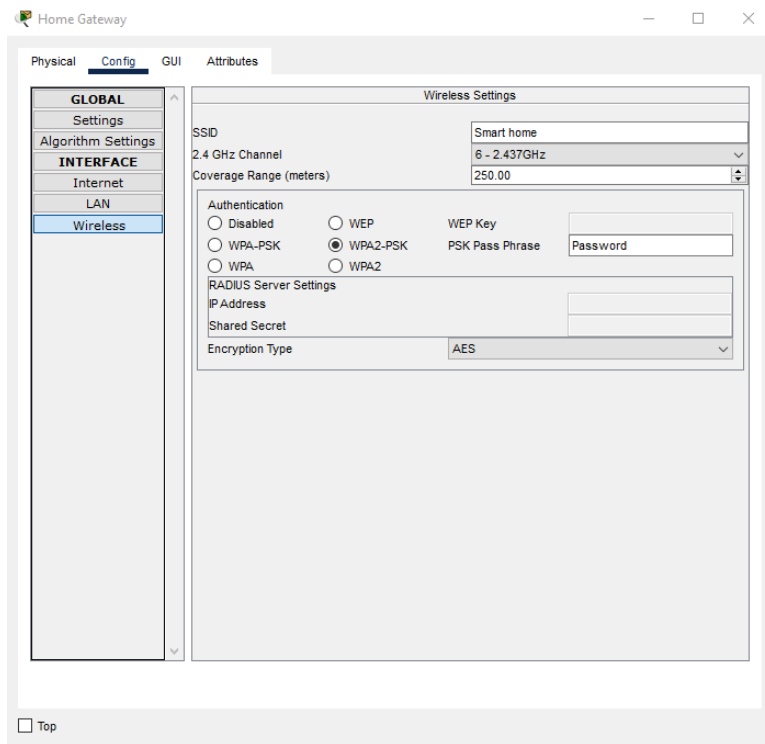
Κρεβατοκάμαρες (2)

- Ανεμιστήρας
- Σώμα καλοριφέρ
- Θερμόμετρο
- Παράθυρο
- Σειρήνα συναγερμού
- Ανιχνευτής καπνού
- Λάμπα
- Μπάνιο
- Δείκτης υγρασίας
- Έλεγχος στάθμης νερού
- Θερμόμετρο
- Παράθυρο
- Σώμα καλοριφέρ
- Λάμπα

Αυτές οι συσκευές θα συνδέονται ασύρματα στο δίκτυο του σπιτιού και θα ελέγχονται τοπικά από έναν υπολογιστή. Επιπλέον, με τη χρήση δικτύων κινητής τηλεφωνίας, θα είναι δυνατός ο έλεγχος του Smart Home απομακρυσμένα.

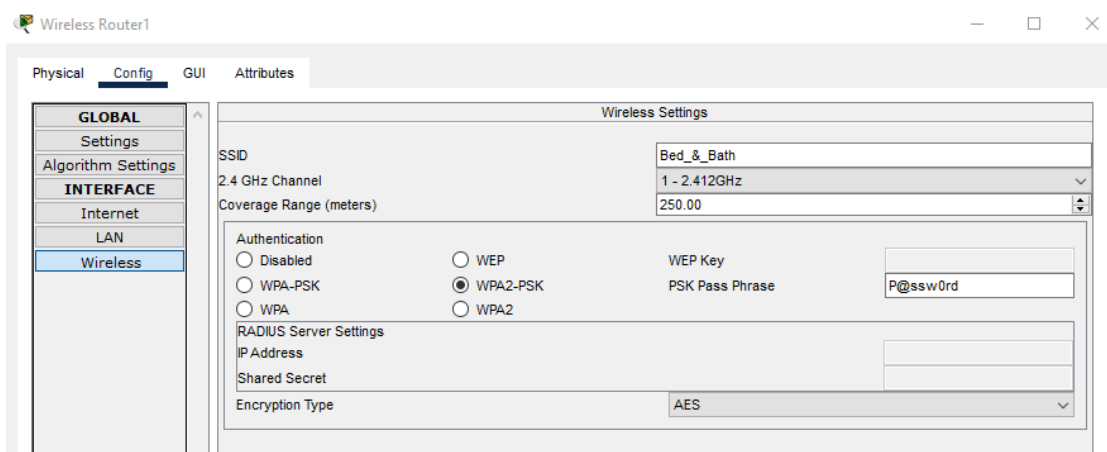
Για την προσομοίωση του Smart Home στο Packet Tracer, ακολουθούμε τα εξής βήματα:

Προσθέτω Home Gateway, wireless routers, Access Point από «Network Devices» → «Wireless Devices». Στο Home Gateway, στην καρτέλα «Config»→«Wireless» αλλάζω το SSID, τον τύπο αυθεντικοποίησης και password.



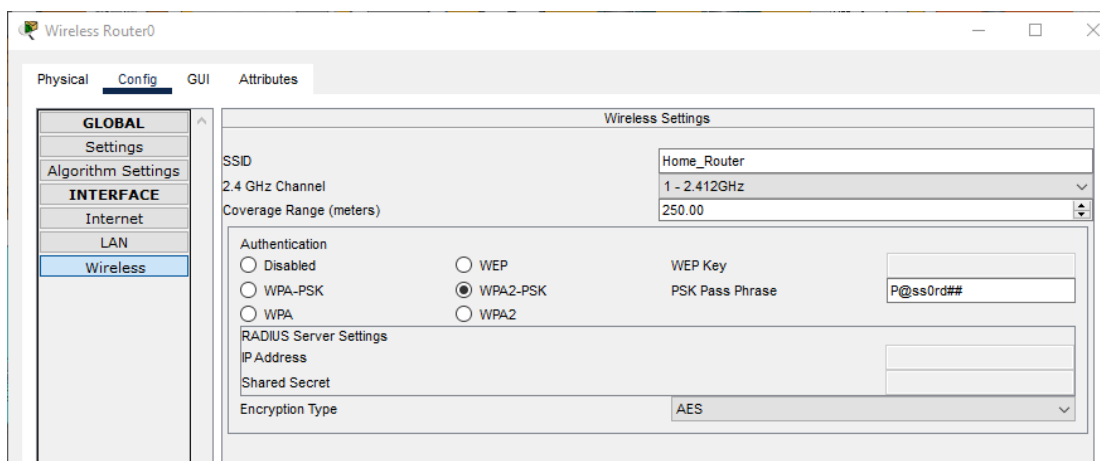
Εικόνα 14: Ρυθμίσεις Home Gateway.

Σχετική Πηγή: <https://www.noip.com/support/knowledgebase/finding-your-default-gateway/>



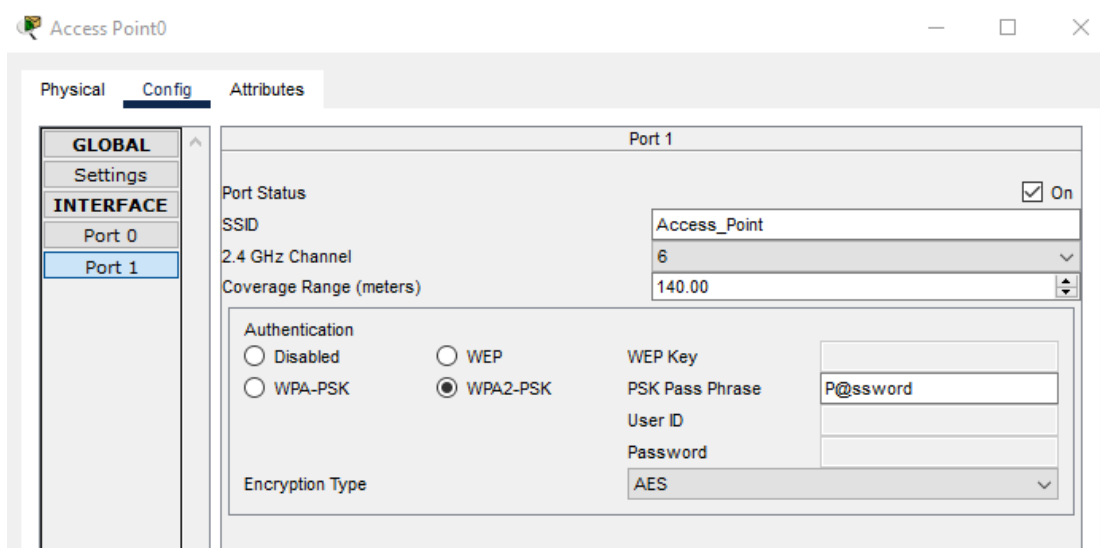
Εικόνα 15: Ρυθμίσεις Wireless Router 1.

Σχετική Πηγή : <https://www.home-network-help.com/wireless-router.html>



Εικόνα 16: Ρυθμίσεις Wireless Router 0.

Σχετική Πηγή : <https://www.home-network-help.com/wireless-router.html>



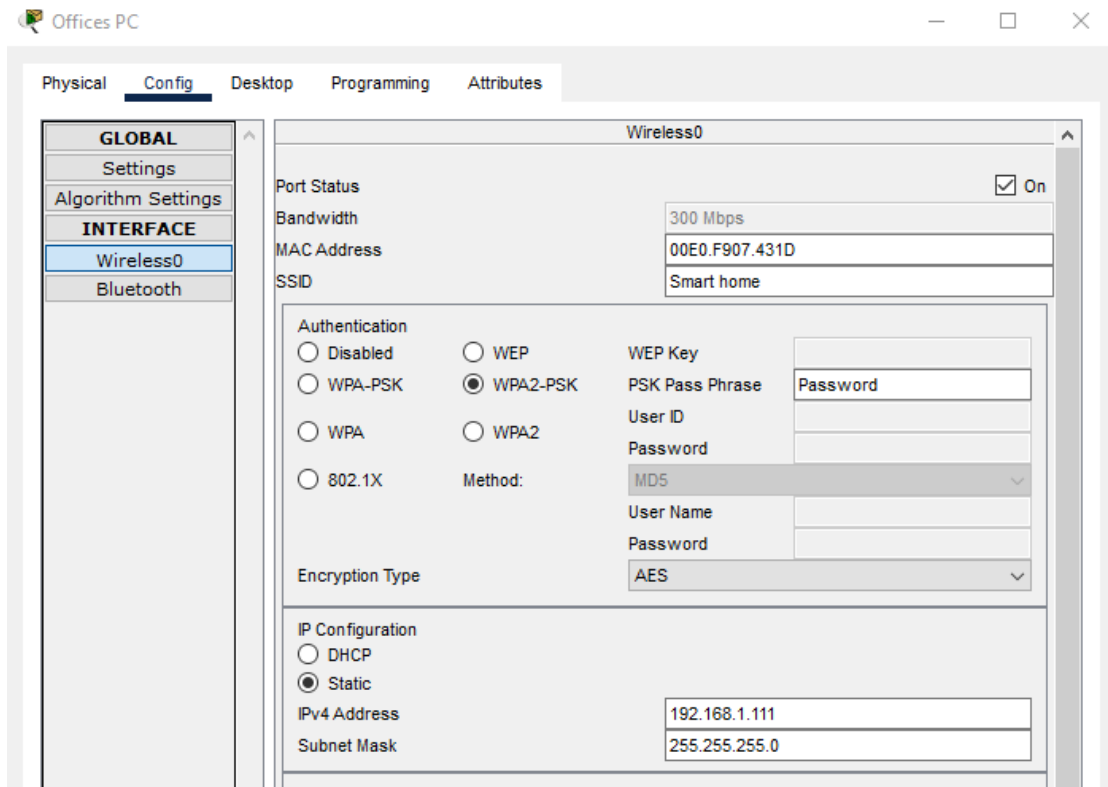
Εικόνα 17: Ρυθμίσεις Access Point.

Σχετική Πηγή : <https://www.home-network-help.com/wireless-router.html>

Όλες οι συσκευές έχουν κρυπτογράφηση WPA2 –PSK που είναι η ισχυρότερη κρυπτογράφηση από όσες έχουν διαθέσιμες οι συσκευές και η οποία βασίζεται στο πρότυπο AES (προηγμένο πρότυπο κρυπτογράφησης). Αυτή είναι στην ουσία η νεότερη μορφή του WPA-PSK (TKIP) και έχει ισχυρότερη κρυπτογράφηση παρέχοντας μεγαλύτερη ασφάλεια στο δίκτυο.

Τα SSID είναι, με απλά λόγια, το αναγνωριστικό ενός δικτύου Wi-Fi, ώστε να μπορεί να γίνεται ορατό από τις συσκευές. Στη συνέχεια, προσθέτω ένα PC από «Miscellaneous» → «Miscellaneous». Ρυθμίζω την διεπαφή «Wireless» για να συνδεθεί με το Home Gateway και

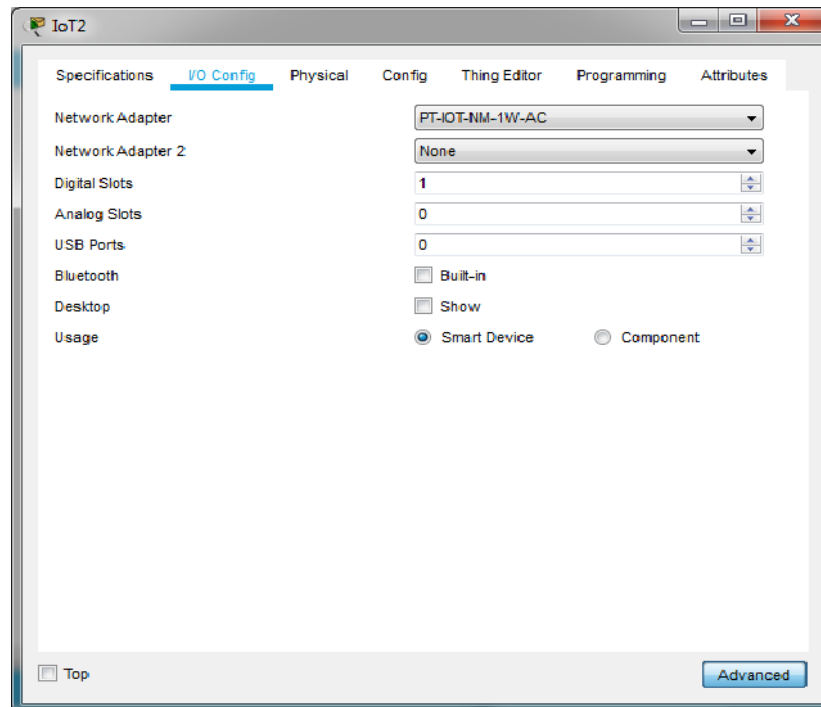
απενεργοποιώ τον DHCP, επιλέγοντας static (στατικές IP) ώστε να μην έχουν τυχαίες διευθύνσεις οι συσκευές, αλλά συγκεκριμένες, τις οποίες θα έχουμε καταγράψει κάπου ώστε να είναι πιο εύκολη η συντήρηση και ο έλεγχος του δικτύου. Για παράδειγμα, αν λόγω βλάβης, χρειαστεί να αντικατασταθεί μια δικτυακή συσκευή, αυτή θα ρυθμιστεί να έχει την ίδια IP.



Εικόνα 18: Ρυθμίσεις Wireless PC.

Σχετική Πηγή : <https://www.home-network-help.com/wireless-router.html>

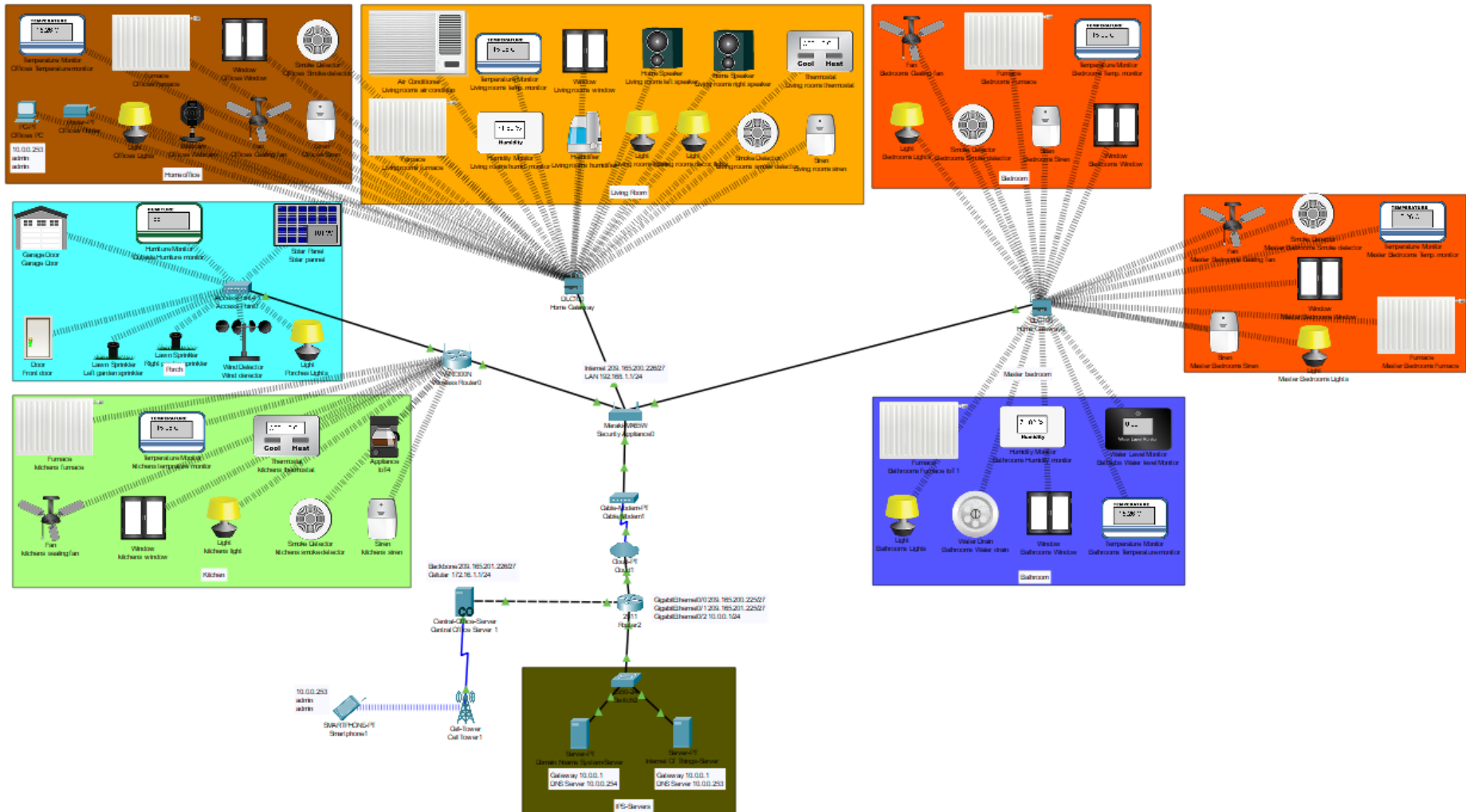
Έπειτα, για να συνδέσουμε τις υπόλοιπες συσκευές στο δίκτυο του Smart Home μας, στην καρτέλα κάθε συσκευής επιλέγουμε «Advanced» και στο μενού «I/O Config» τροποποιούμε τη ρύθμιση του «Network Adapter» ως εξής:



Εικόνα 19: Ρυθμίσεις Network Adapter.

Σχετική Πηγή : <https://www.home-network-help.com/wireless-router.html>

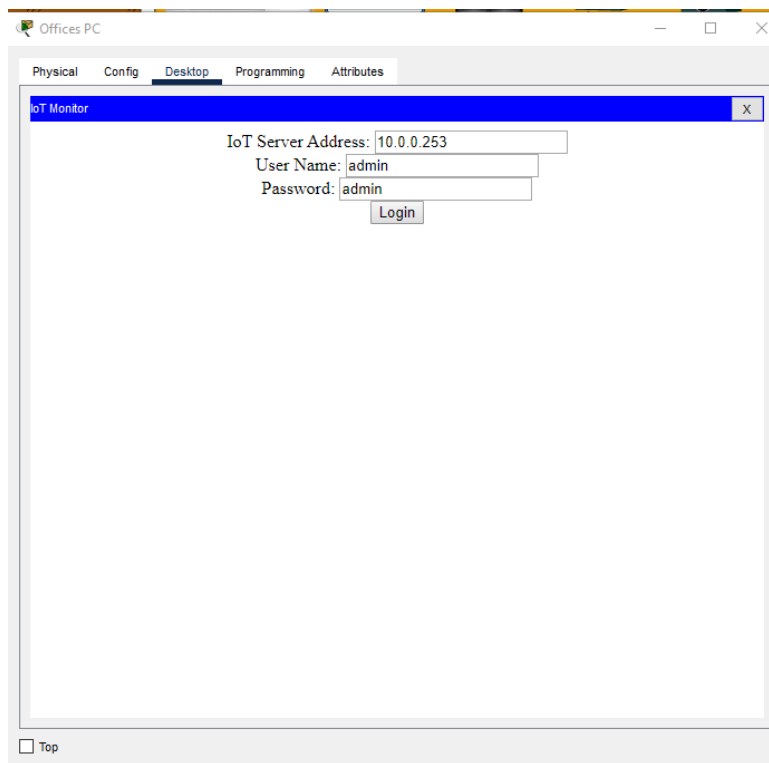
Έπειτα, επιλέγουμε το μενού «Config» → «Wireless». Επαναλαμβάνουμε τη διαδικασία για κάθε ένα από τα στοιχεία του Smart Home, οπότε τελικά διαμορφώνεται το εξής δίκτυο:



Εικόνα 20: Smart Home.

Σχετική Πηγή : https://endnowfoundation.org/secure_smart_homes.php

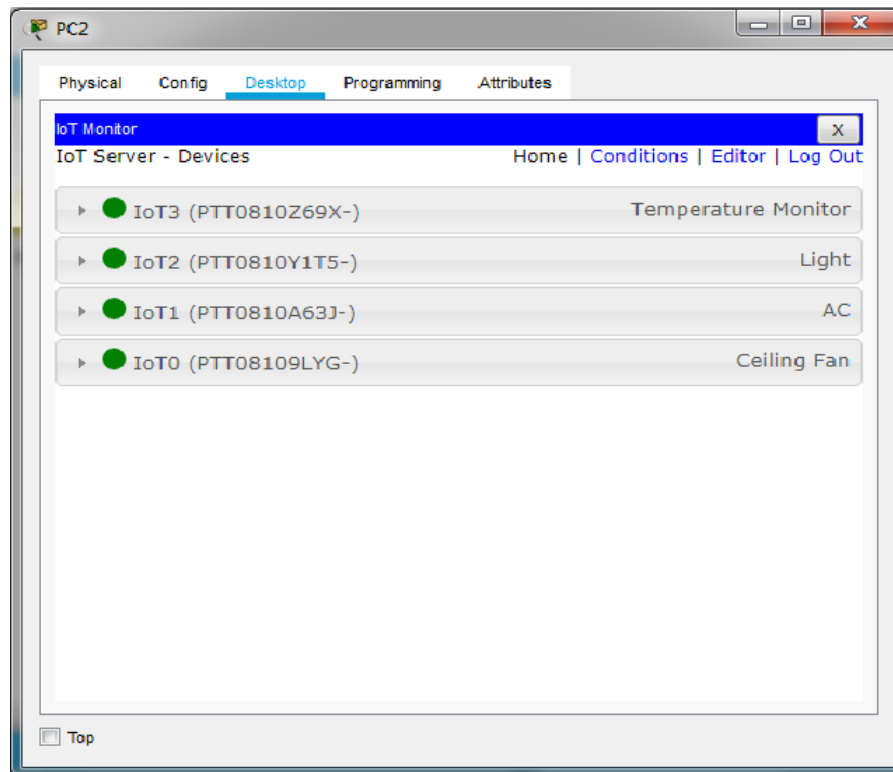
Για να ορίσουμε κάποιες αυτοματοποιήσεις στο Smart Home μας, πηγαίνουμε στο PC, στην καρτέλα «Desktop» → «IoT Monitor». Εκεί βλέπουμε όλες τις συνδεδεμένες έξυπνες συσκευές του σπιτιού, αλλά πρώτα πρέπει να κάνουμε login χρησιμοποιώντας τα default credentials:



Εικόνα 21: Login με default credentials στο IoT Monitor.

Σχετική Πηγή : <https://www.home-network-help.com/wireless-router.html>

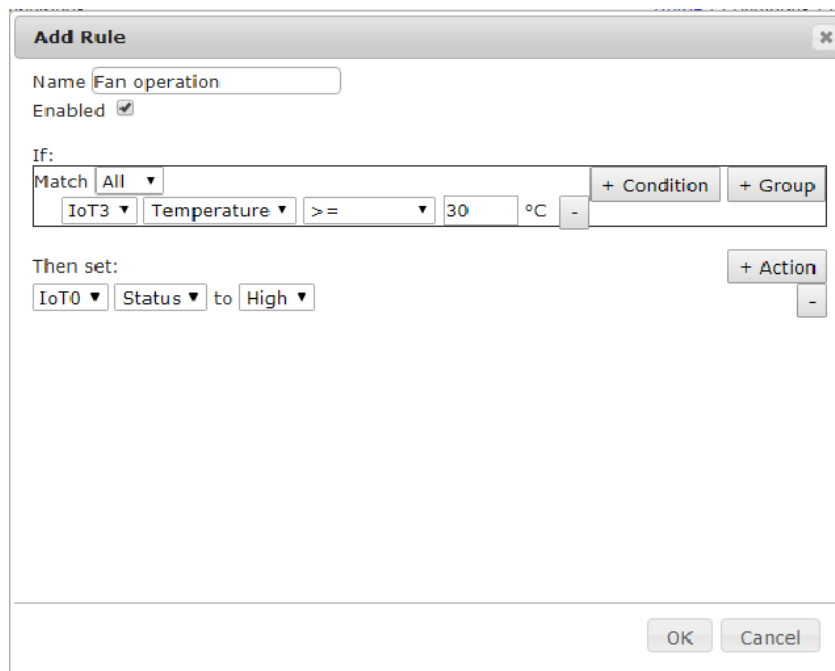
Μόλις συνδεθούμε, μας εμφανίζεται μία λίστα με τις έξυπνες συσκευές του σπιτιού:



Εικόνα 22: IoT Monitor.

Σχετική Πηγή : <https://www.home-network-help.com/wireless-router.html>

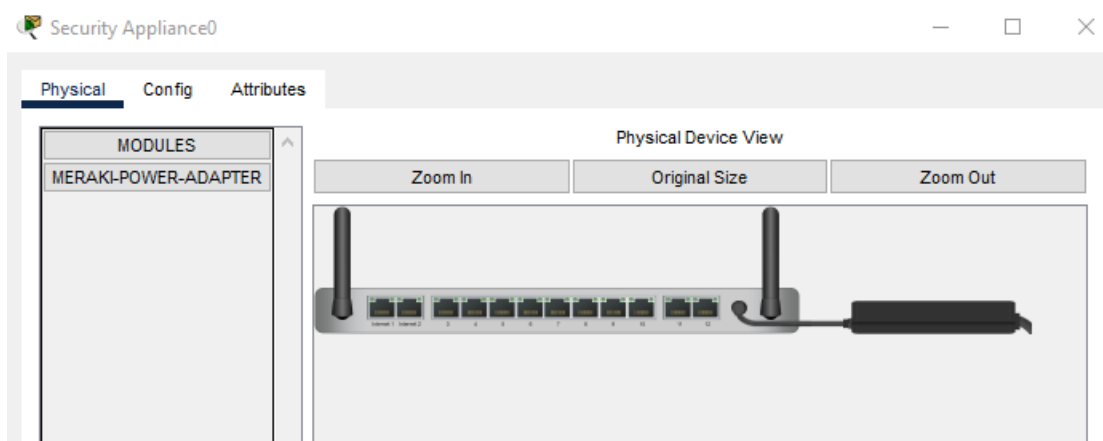
Ενδεικτικά, θα ορίσουμε την αυτοματοποίηση ότι όταν η θερμοκρασία ανεβαίνει πάνω από τους 30 βαθμούς, θα ανοίγει ο ανεμιστήρας. Επιλέγοντας «Conditions» και στην συνέχεια «Add», εισάγουμε την εξής παραμετροποίηση:



Εικόνα 23: Αυτοματοποίηση λειτουργίας ανεμιστήρα.

Σχετική Πηγή : <https://www.home-network-help.com/wireless-router.html>

Επίσης τοποθετήθηκε και μια συσκευή της cisco για φιλτράρισμα κυβερνοεπιθέσεων (cyber attacks), ώστε να αποτρέπεται η είσοδος κακόβουλων χρηστών και η διαρροή ευαίσθητων πληροφοριών των χρηστών του δικτύου του συστήματος, όπως για παράδειγμα τραπεζικοί κωδικοί.



Εικόνα 24: Συσκευή ενάντια στα cyber attacks.

Σχετική Πηγή : <https://www.home-network-help.com/wireless-router.html>

Φυσικά, μπορούμε να ορίσουμε πολλές αυτοματοποιήσεις, ιδιαίτερα εάν εισάγουμε και άλλες έξυπνες συσκευές, με τον ίδιο τρόπο.

8.3 Σύνδεση μέσω δικτύων κινητής τηλεφωνίας

Τώρα έχουμε ολοκληρώσει τη προσομοίωση του Smart Home στο Packet Tracer. Ωστόσο, η λειτουργία ελέγχεται μόνο μέσω του υπολογιστή όταν αυτός είναι συνδεδεμένος στο τοπικό δίκτυο. Θα κάνουμε χρήση λοιπόν των δικτύων κινητής τηλεφωνίας ώστε ο χρήστης να μπορεί να συνδέεται στο Smart Home απομακρυσμένα.

Για να το κάνουμε αυτό, προσθέτουμε τα εξής στοιχεία:

- **Access Point –PT:** επεκτείνει το Wi-Fi σήμα και συνδέει ασύρματα ένα χώρο με συσκευές (συνήθως ένα δωμάτιο).
- **Cable Modem (Network Devices→Security):** Συσκευή που μοιράζει την δικτυακή πρόσβαση μέσα στο σπίτι.
- **Wireless Router x2:** Συσκευή που επεκτείνει το Wi-Fi σήμα και συνδέει ένα χώρο με συσκευές (συνήθως ένα δωμάτιο), τόσο ασύρματα όσο και ενσύρματα
- **Home Gateway DLC100:** επεκτείνει το Wi-Fi σήμα και συνδέει ασύρματα ένα χώρο με συσκευές (συνήθως ένα δωμάτιο).
- **Security Appliance - Meraki MX65W:** Συσκευή Firewall που απαγορεύει την κίνηση σε ύποπτα πακέτα δεδομένων από μέσα προς τα έξω και αντίστροφα. Κάνει filtering και monitoring των πακέτων.
- **2911 Router (Network Devices→Routers):** Η βασική συσκευή μέσω της οποίας προσπελάνουν το Cloud οι servers.
- **2950 24 Switch (Network Devices→Switches):** Συσκευή μέσω της οποίας το δίκτυο διαμοιράζεται σε όλες τις συσκευές.
- **Serverx 2 (End Devices→End Devices):** ο ένας server (IoTServer) είναι αυτός στον οποίο ρυθμίζονται όλες οι συσκευές, δηλαδή είναι αυτός που κάνει τη διαχείριση. Ο δεύτερος server (DNS Server) μεταφράζει τις IP διευθύνσεις σε ονοματικές (π. χ. την 173.194.77.104 σε www.google.com)
- **COserver (Network Devices→Wireless Devices):** Είναι αυτός στον οποίο συνδέονται τα κινητά τηλέφωνα ώστε να έχουν επικοινωνία με το υπόλοιπο σύστημα
- **Cell Tower (Network Devices → Cell Tower):** Διασυνδέει το κινητό τηλέφωνο.

- **SmartPhone (End Devices→End Devices):** Οι συσκευές που έχουν οι χρήστες για να συνδέονται στο δίκτυο.

Για να ολοκληρώσουμε τη σχεδίαση, πηγαίνουμε στο Router→«CLI» και δίνουμε τις εξής εντολές:

```
Router(config-router)#do show run
Building configuration...

Current configuration : 1345 bytes

version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption

hostname Router

ip dhcp excluded-address 209.165.201.225
ip dhcp excluded-address 209.165.201.229
ip dhcp excluded-address 209.165.200.225
ip dhcp excluded-address 209.165.200.229

ip dhcp pool CELL
network 209.165.201.224 255.255.255.224
default-router 209.165.201.225
dns-server 10.0.0.254
```

```
ip dhcp pool WAN
network 209.165.200.224 255.255.255.224
default-router 209.165.200.225
dns-server 10.0.0.254

ip cef
no ipv6 cef

license udi pid CISCO2911/K9 sn FTX152425I9-

spanning-tree mode pvst

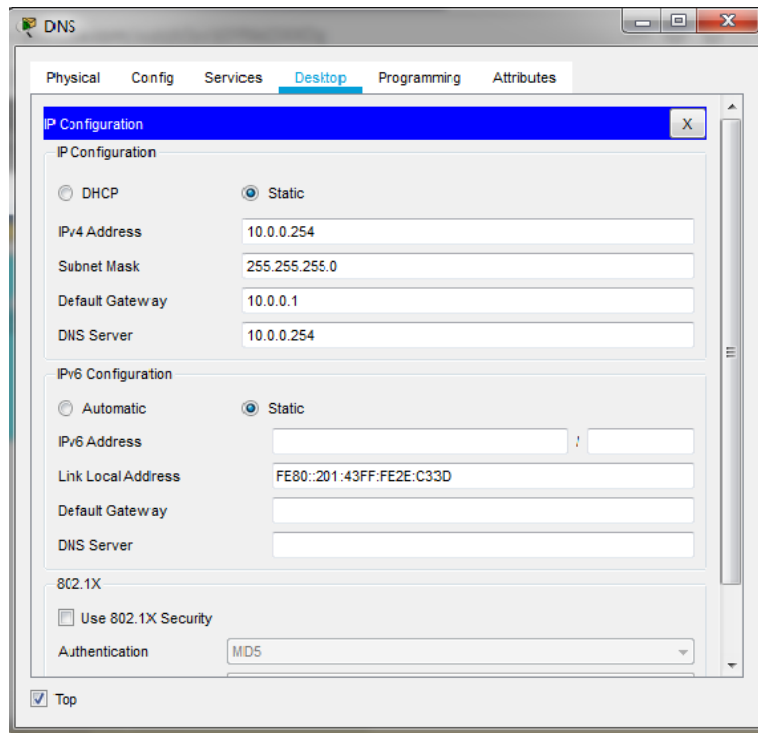
interface GigabitEthernet0/0
ip address 209.165.200.225 255.255.255.224
duplex auto
speed auto

interface GigabitEthernet0/1
ip address 209.165.201.225 255.255.255.224
duplex auto
speed auto

interface GigabitEthernet0/2
ip address 10.0.0.1 255.255.255.0
duplex auto
speed auto
```

```
!  
interface Vlan1  
no ip address  
shutdown  
!  
router rip  
version 2  
passive-interface GigabitEthernet0/1  
passive-interface GigabitEthernet0/2  
network 10.0.0.0  
network 172.16.0.0  
network 209.165.200.0  
network 209.165.201.0  
default-information originate  
  
ip classless  
  
ip flow-export version 9  
  
line con 0  
  
line aux 0  
  
line vty 0 4  
login  
end
```

Αναθέτουμε την IPδιεύθυνση στον DNS server ως εξής:

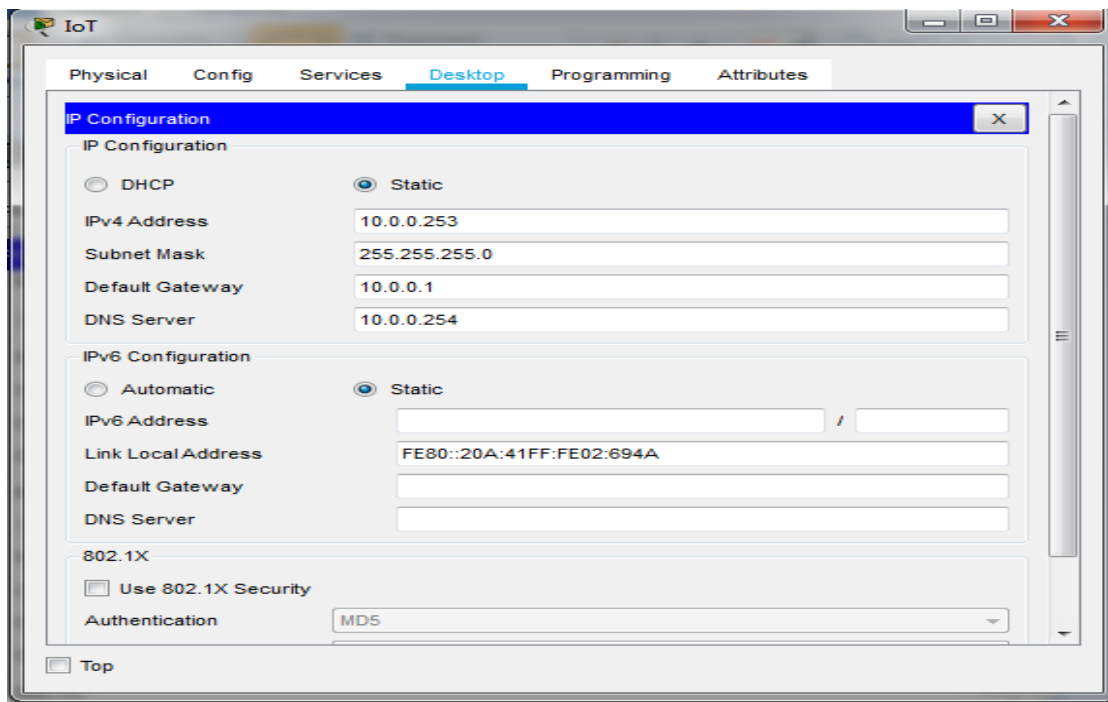


Εικόνα 25: Ανάθεση IP.

Σχετική Πηγή : <http://windowsbulletin.com/how-to-change-router-dns-server-settings-in-windows-10/>

Και στην καρτέλα «Services» → «DNS», επιλέγουμε το «DNS Service On».

Αναθέτουμε IP διεύθυνση στον IoT server ως εξής:



Εικόνα 26: Ανάθεση IP στον IoT server.

Σχετική Πηγή : <http://windowsbulletin.com/how-to-change-router-dns-server-settings-in-windows-10/>

Και στην καρτέλα «Services» → «IoT» επιλέγουμε «On».

Έπειτα, στο PC, πηγαίνουμε στο «Desktop» → «Command Prompt» και τρέχουμε τις εξής δύο εντολές:

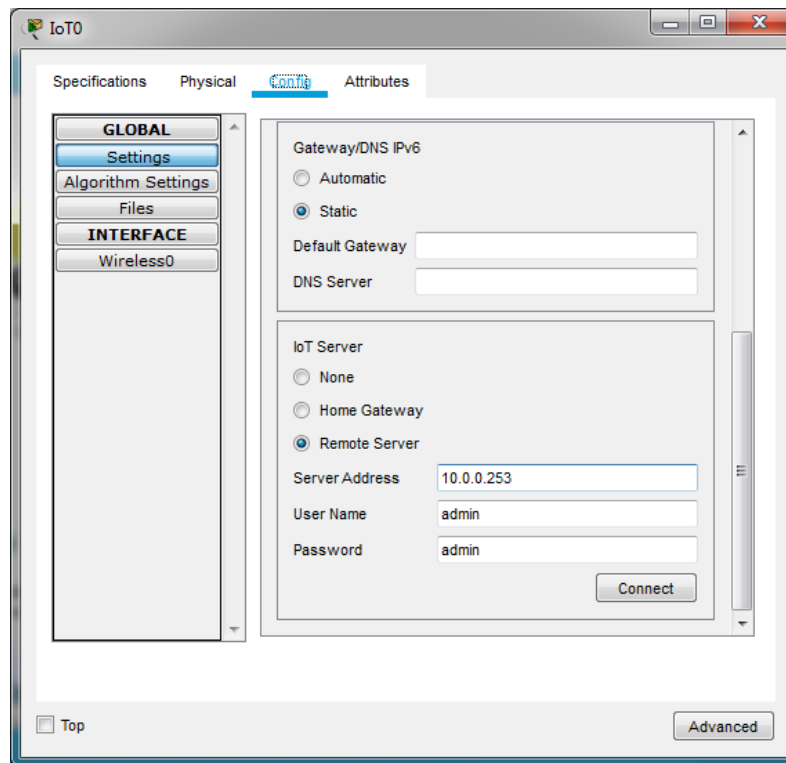
```
ping 10.0.0.253
```

```
ping 10.0.0.254
```

προκειμένου να ελέγξουμε την εγκυρότητα των συνδέσεων με τους server. Όταν οι server απαντούν, οι συνδέσεις είναι εντάξει.

Τώρα μένει να συνδέσουμε τις smart` συσκευές μας στον server. Για να το κάνουμε αυτό, αρχικά πηγαίνουμε στο PC → «IoT Monitor» και προσπαθούμε να κάνουμε σύνδεση στον server (IP: 10.0.0.253). Θα δούμε μήνυμα λάθους ότι δεν έχουμε λογαριασμό και θα μας δώσει την επιλογή να κάνουμε «Sign Up». Το κάνουμε με όνομα και κωδικό χρήστη «admin». Έπειτα, πηγαίνουμε

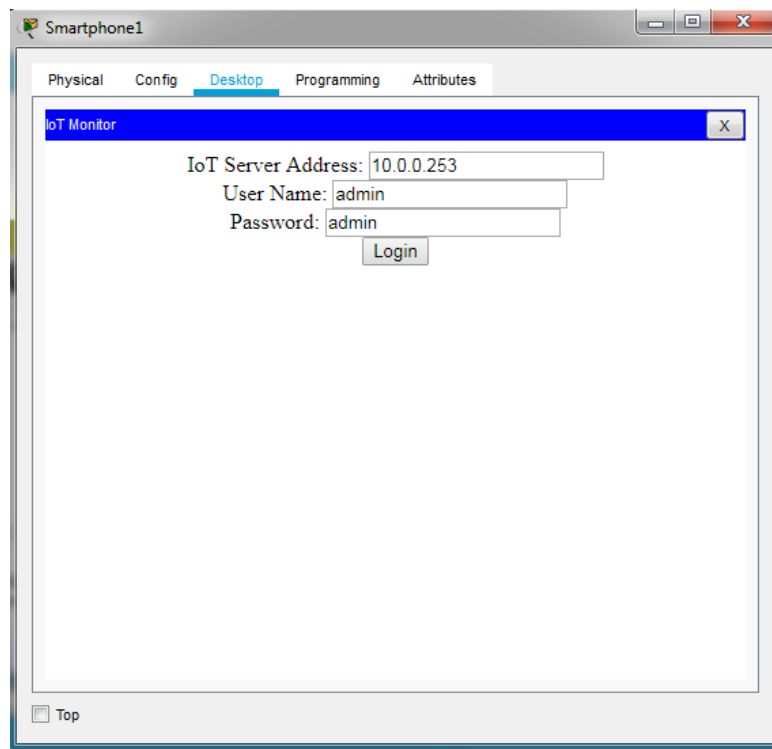
σε κάθε Smartσυσκευή και στην καρτέλα «Config» → «Settings» και θέτουμε τις ρυθμίσεις ως εξής:



Εικόνα 27: Σύνδεση συσκευής στον server.

Σχετική Πηγή : <https://www.tp-link.com/no/support/faq/14/>

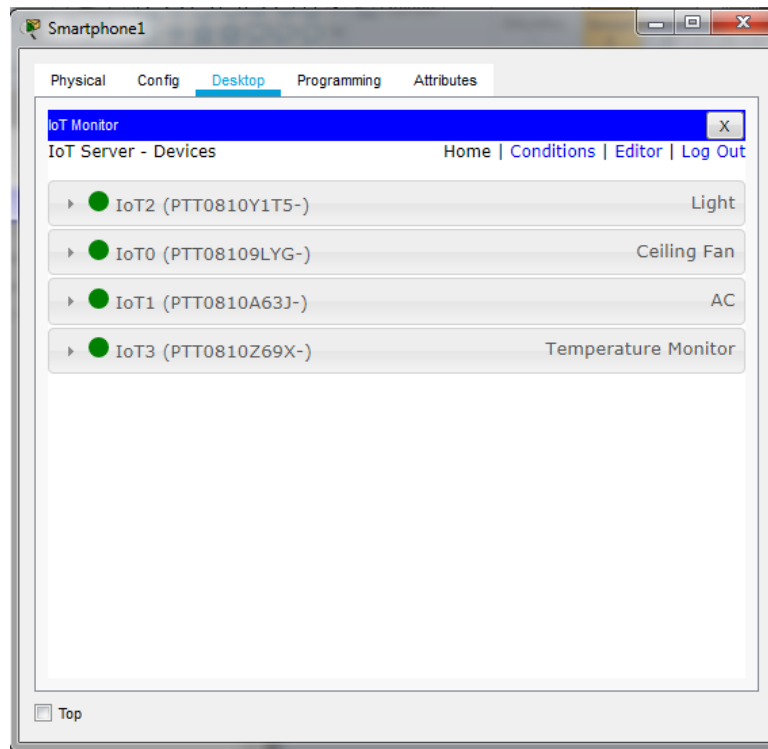
Εάν έχουμε εισάγει σωστά τις πληροφορίες έως τώρα, το «Connect» θα αλλάξει από μόνο του σε «Refresh». Το κάνουμε αυτό για κάθε Smart Device του Smart Home μας. Το Smart Home μας τώρα είναι επιτυχώς συνδεδεμένο με τον server και η πρόσβαση μπορεί να γίνει και απομακρυσμένα μέσω δικτύων κινητής τηλεφωνίας. Συγκεκριμένα, εάν επιλέξουμε στο Smartphone στην καρτέλα «Desktop» την εφαρμογή «IoT Monitor», θα μπορούμε να συνδεθούμε στον server:



Εικόνα 28: Σύνδεση στο server μέσω Smartphone απομακρυσμένα.

Σχετική Πηγή : <http://www.ijera.com/papers/vol9no4/Series-3/F0904033439.pdf>

Έτσι, μπορούμε να ελέγξουμε τη κατάσταση του Smart Home μας :



Εικόνα 29: Έλεγχος Smart Home απομακρυσμένα μέσω Smartphone με χρήση δικτύων κινητής τηλεφωνίας.

Σχετική Πηγή : <http://www.ijera.com/papers/vol9no4/Series-3/F0904033439.pdf>

Τα βήματα που παρουσιάζονται σε αυτήν την αναφορά παραδίδονται υλοποιημένα με τη μορφή project του Packet Tracer μαζί με την αναφορά.

9

Συμπεράσματα

Η εξέλιξη στις τηλεπικοινωνίες προχωρά με ραγδαίο ρυθμό τα τελευταία χρόνια. Οι τεχνολογίες και τα πρωτόκολλα επικοινωνίας συνεχώς εμπλουτίζονται, σε μια προσπάθεια η τηλεπικοινωνία να πραγματοποιείται με τη μεγαλύτερη δυνατή ταχύτητα μετάδοσης και πρακτικά οπουδήποτε. Έτσι οι αδυναμίες που εντοπίζονταν σε παλαιότερες τεχνολογίες έχουν μετριαστεί σημαντικά από τις νέες που τις αντικατέστησαν.

Το Διαδίκτυο των Αντικειμένων (IoT) είναι η νέα πραγματικότητα του χώρου των τηλεπικοινωνιών. Αποτελείται από ένα πλήθος έξυπνων συσκευών οι οποίες συλλέγουν και ανταλλάσσουν δεδομένα ευρισκόμενες σε συνεχή επικοινωνία μεταξύ τους. Το IoT έχει ένα ευρύ φάσμα εφαρμογών τόσο στην καθημερινή ζωή, όσο και στη βιομηχανία, τις μεταφορές, την υγειονομική περίθαλψη, το περιβάλλον κ.α. Οι έξυπνες συσκευές μπορεί να έχουν ενσύρματη ή ασύρματη σύνδεση. Αναφορικά με την ασύρματη σύνδεση, υπάρχουν πολλά διαφορετικά πρωτόκολλα και τεχνολογίες επικοινωνίας που χρησιμοποιούνται (π.χ. LoWPAN, ZigBee, Bluetooth και BLE, NFC).

Στην παρούσα εργασία παρουσιάστηκαν διάφορα πρωτόκολλα επικοινωνίας, με στόχο την σωστή επιλογή ανάλογα με την εκάστοτε εφαρμογή. Τα κριτήρια που οδηγούν στην σωστή απόφαση είναι η ασφάλεια, η διάρκεια ζωής των μπαταριών η ισχύς, και σε τελική ανάλυση οι απαιτήσεις της κάθε εφαρμογής.

Στο πρακτικό κομμάτι της εργασίας, χρησιμοποιήσαμε την τελευταία έκδοση Cisco Packet Tracer για να παρουσιάσουμε το έξυπνο σπίτι, καθώς αυτή η έκδοση περιλαμβάνει πολλές συσκευές IoT. Ο στόχος του πρακτικού μέρους της έρευνας ήταν να προσομοιώσει ένα έξυπνο σπίτι. Η τεχνολογική καινοτομία και η αύξηση της χρήσης smartphone ήταν το κίνητρο πίσω από αυτήν την εργασία. Το IoT είναι μια νέα και εξαιρετική ιδέα για να κάνει το περιβάλλον μας πιο έξυπνο. Οι χρήστες, δηλαδή οι ένοικοι του σπιτιού, μέσω της συνδεσμολογίας που υλοποιήθηκε, και λόγω των χαρακτηριστικών των αισθητήρων που βρίσκονται σε έξυπνες συσκευές καθημερινής χρήσης, μπορούν να χρησιμοποιήσουν το smartphone τους για να ελέγχουν το σπίτι από οποιοδήποτε σημείο και αν βρίσκονται. Προφανώς, η εφαρμογή μέτρων ασφάλειας είναι ιδιαίτερα σημαντική προκειμένου να αποφευχθούν κακόβουλες ενέργειες από τρίτους.

Βιβλιογραφία

- [1] Lucero, S. IoT Platforms: Enabling the Internet of Things. 2019. Available online: <https://cdn.ihs.com/www/pdf/enabling-IoT.pdf> (accessed on 12 January 2019).
- [2] Salman, L.; Salman, S.; Jahangirian, S.; Abraham, M.; German, F.; Blair, C.; Krenz, P. Energy efficient IoT-based smart home. In Proceedings of the IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, 12–14 December 2016.
- [3] Bardyn, J.; Melly, T.; Seller, O.; Sornin, N. IoT: The era of LPWAN is starting now. In Proceedings of the ESSCIRC Conference 2016: 42nd European Solid-State Circuits Conference, Lausanne, Switzerland, 12–15 September 2016; pp. 25–30, doi:10.1109/ESSCIRC.2016.7598235.
- [4] Devalal, S.; Karthikeyan, A. LoRa Technology—An Overview. In Proceedings of the Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Tamilnadu, India, 29–30 March 2018.
- [5] Mekki, K.; Bajic, E.; Chaxel, F.; Meyer, F. A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express* 2019, 5, 1–7, doi:10.1016/j.icte.2017.12.005.
- [6] Lauridsen, M.; Nguyen, H.; Vejlgard, B.; Kovacs, I.Z.; Mogensen, P.; Sorensen, M. Coverage Comparison of GPRS, NB-IoT, LoRa, and SigFox in a 7800 square km Area. In Proceedings of the IEEE 85th Vehicular Technology Conference (VTC Spring), Sydney, Australia, 4–7 June 2017.
- [7] Sinha, R.S.; Wei, Y.; Hwang, S.H. A survey on LPWA technology: LoRa and NB-IoT. *ICT Express* 2017, 3, 14–21.
- [8] Garima Jain, Nasreen Noorani, Nisha Kiran, Sourabh Sharma, Designing & simulation of topology network using Packet Tracer, *International Research Journal of Engineering and Technology (IRJET)*, 2(2), 2015.

- [9] S. Raja Gopal, P. Saleem Akram, S. Sriram, T. Pavan Koushik, V. Mohana Krishna, —Design and Analysis of Heterogeneous Hybrid topology for VLAN configuration—, International Journal of Emerging Trends in Engineering Research, Vol 7, No 11, PP 487 – 491, 2019.
- [10] www.wikipedia.org/wiki/computer_networks, Retrieved 10th October 2016.
- [11] Tim Reardon, Planning, Designing and operating local area networks, DISAM Journal, Summer, 1997
- [12] Kenan Xu, Device Deployment Strategies for Largescale Wireless Sensor Networks 2018
- [13] Kenan Xu, Performance analysis of differentiated QoS MAC in wireless local area networks (WLANs), Thesis Submitted to the Department of Electrical and Computer Engineering, Queen's University, Canada. September 2003.
- [14] P. Srikanth Reddy, P. Saleem Akram, M. Adarsh Sharma, P. Aditya Sai Ram, R. Pruthvi Raj, —Study and Analysis of Routing Protocols—, International Journal of Emerging Trends in Engineering Research, Vol 7, No 11, PP 434 – 440, 2019 [8] David D. C., Kenneth T.P., David P.R, An introduction to local area networks, Proc. of the IEEE conf., Vol. 66, 1978
- [15] Todd Lammle, Cisco Certified network associate study guide (Wiley Publishing Inc., 2007)
- [16] Saleem Akram P., Ramana T.V., "Stacked electromagnetic band gap ground optimization for low profile patch antenna design", International Journal of Engineering and Advanced Technology, ISSN:22498958, Vol No: 8, Issue No:3, 2019, pp:146 – 154.
- [17] Muzammil Parvez M., Shanmugam J., Mohan Rao K.R.R., Lakshmana C., Shameem S.. Alive node and network lifetime analysis of DEEC protocol and EDDEEC protocol —,2018, International Journal of Engineering and Technology (UAE),Vol: 7,Issue:, pp: 661 to:: 664, DOI:, ISSN: 2227524X
- [18] Pavithra T., Sastry J.K.R. Strategies to handle heterogeneity prevalent within an IoT based network —, 2018, International Journal of Engineering and Technology (UAE), Vol: 7, Issue: 2, pp: 203 to:: 208, DOI: 10.14419/ijet.v7i2.7.10293, ISSN: 2227524X
- [19] Devi Susmitha, N., Sowmya, S., Akram, P. S.Ramana, T. V. (2017). Tuning of L-C meta-material structure for antenna applications. Paper presented at the International

- Conference on Signal Processing, Communication, Power and Embedded System, SCOPES2016-Proceedings, 1845-1850. DoI:10.1109/SCOPES.2016.7955764
- [20] Poonam Jain S., Pooja S., Sripath Roy K., Abhilash K., Arvind B.V. Implementation of asymmetric processing on multi core processors to implement IoT applications on GNU/Linux framework —, 2018, International Journal of Engineering and Technology (UAE), Vol: 7, Issue: 1.1, pp: 494 to:: 499, DOI:, ISSN: 2227524X
- [21] Rambabu K., Venkatram N. Traffic flow features as metrics (TFFM): Detection of application layer level DDOS attack scope of IoT traffic flows —, 2018, International Journal of Engineering and Technology (UAE), Vol: 7, Issue: 1.1, pp: 554 to:: 559, DOI:, ISSN: 2227524X
- [22] N V V N J Sri Lakshmi, P. Saleem Akram, V. Madhu Bhargavi, G. Harshika, A. Sravani, —Study and Analysis of Defense Techniques for Various Network Topologies—, International Journal of Emerging Trends in Engineering Research, Vol 7, No 11, PP 481 – 486, 2019.
- [23] Booi, T. M., Chiscop, I., Meeuwissen, E., Moustafa, N., & den Hartog, F. T. (2021). ToN IoT-The role of heterogeneity and the need for standardization of features and attack types in IoT network intrusion datasets. *IEEE Internet of Things Journal*.
- [24] Savolainen, T., Soininen, J., & Silverajan, B. (2013). IPv6 addressing strategies for IoT. *IEEE Sensors Journal*, 13(10), 3511-3519.
- [25] Srinivasan, C. R., Rajesh, B., Saikalyan, P., Premasagar, K., & Yadav, E. S. (2019). A review on the different types of Internet of Things (IoT). *Journal of Advanced Research in Dynamical and Control Systems*, 11(1), 154-158.
- [26] Adelantado, F., Vilajosana, X., Tuset-Peiro, P., Martinez, B., Melia-Segui, J., & Watteyne, T. (2017). Understanding the limits of LoRaWAN. *IEEE Communications magazine*, 55(9), 34-40.
- [27] Wixted, A. J., Kinnaird, P., Larijani, H., Tait, A., Ahmadiania, A., & Strachan, N. (2016, October). Evaluation of LoRa and LoRaWAN for wireless sensor networks. In *2016 IEEE SENSORS* (pp. 1-3). IEEE.
- [28] Davcev, D., Mitreski, K., Trajkovic, S., Nikolovski, V., & Koteli, N. (2018, June). IoT agriculture system based on LoRaWAN. In *2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)* (pp. 1-4). IEEE.