



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

**Internet of Things & Zigbee Network**  
**Απομακρυσμένος έλεγχος θερμοκηπίου**

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΤΩΝ

**ΓΕΩΡΓΙΟΥ ΠΛΑΤΟΚΟΥΚΗ**  
**και**  
**ΞΕΝΟΦΩΝΤΑ ΓΚΟΛΦΙΝΟΠΟΥΛΟΥ**

**Επιβλέπων : Ευστάθιος Συκάς**  
Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούνιος 2015



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

## **Internet of Things & Zigbee Network Απομακρυσμένος έλεγχος θερμοκηπίου**

### **ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**

των

**ΓΕΩΡΓΙΟΥ ΠΛΑΤΟΚΟΥΚΗ  
και  
ΞΕΝΟΦΩΝΤΑ ΓΚΟΛΦΙΝΟΠΟΥΛΟΥ**

**Επιβλέπων : Ευστάθιος Συκάς  
Καθηγητής Ε.Μ.Π.**

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την .....

.....

Ευστάθιος Συκάς

Καθηγητής Ε.Μ.Π.

.....

Μιχαήλ Θεολόγου

Καθηγητής Ε.Μ.Π.

.....

Γεώργιος Στασινόπουλος

Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούνιος 2015



Γκολφινόπουλος Ξενοφώντας

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

Πλατοκούκης Γεώργιος

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

Copyright © ΠΛΑΤΟΚΟΥΚΗΣ ΓΕΩΡΓΙΟΣ, ΓΚΟΛΦΙΝΟΠΟΥΛΟΣ ΞΕΝΟΦΩΝΤΑΣ, 2015

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα.

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Εθνικού Μετσόβιου Πολυτεχνείου.



# Περίληψη

Ο σκοπός της εν λόγω διπλωματικής εργασίας είναι η μελέτη και η ανάλυση των τεχνολογιών ασύρματης δικτύωσης που αφορούν την παρατήρηση, τον έλεγχο και την καταγραφή μετρήσιμων παραμέτρων σε βιομηχανικό, οικιακό και αγροτικό περιβάλλον. Οι παραπάνω διαδικασίες ανήκουν στον ταχέα αναπτυσσόμενο κλάδο του Internet of Things (IoT).

Αρχικά ασχολούμαστε με την ανάλυση του όρου Internet of Things, την παρούσα κατάσταση του κλάδου και την διεύθυνση του στην αγορά, αλλά και τις προοπτικές του στο μέλλον. Κατά την διερεύνηση αυτή μελετάμε την πλειοψηφία των τεχνολογιών που επαφίονται στον κλάδο IoT. Στα πλαίσια της διπλωματικής διαλέξαμε δυο τεχνολογίες για εις βάθος ανάλυση (Zigbee και 6LoWPAN) οι οποίες όπως διαφαίνεται θα κυριαρχήσουν στο κομμάτι της δικτύωσης του IoT.

Συνεχίσαμε με την πρακτική εφαρμογή του προτύπου Zigbee σε ένα ασύρματο δίκτυο αισθητήρων. Το δίκτυο αυτό αφορά τον έλεγχο και την παρατήρηση παραμέτρων σε αγροτικό περιβάλλον και πιο συγκεκριμένα σε ένα θερμοκήπιο.

Συγκεκριμένα το δίκτυο αποτελείται από 4 κόμβους, καθένας από τους οποίους επιτελεί ένα διαφορετικό έργο. Ο 1<sup>ος</sup> κόμβος αποτελεί τον συντονιστή του δικτύου και την συσκευή προορισμού όλων των μετρήσεων και ελέγχων και διαθέτει σειριακή επικοινωνία με τον υπολογιστή που φέρει την εφαρμογή για την δημοσιοποίηση των στοιχείων στο διαδίκτυο. Ο 2<sup>ος</sup> κόμβος επιτελεί την λειτουργία του δρομολογητή στην συσκευή προορισμού αλλά ταυτόχρονα συλλέγει και αποστέλλει μετρήσεις και ο ίδιος από το εσωτερικό του θερμοκηπίου. Οι 2 τελευταίοι κόμβοι είναι ενεργειακά αυτόνομοι (τροφοδοτούνται από μπαταρίες) και αποτελούν τελικές συσκευές που έχουν ως ρόλο την συλλογή και αποστολή μετρήσεων από του αισθητήρες που διαθέτουν.

Η συλλογή των μετρήσεων στον υπολογιστή γίνεται μέσω ενός Java app που καταγράφει τις μετρήσεις σε μια τοπική βάση δεδομένων. Η δημοσιοποίηση των μετρήσεων γίνεται μέσω ενός web app που δημιουργεί μια διεπαφή με την παρουσίαση των στοιχείων και την καθιστά προσβάσιμη από το διαδίκτυο με την χρήση DDNS (Dynamic Domain Name System). Η διεπαφή δίνει την δυνατότητα στον χρήστη για απομακρυσμένο έλεγχο παραμέτρων.

Η επιλογή του αγροτικού κλάδου έγινε βάσει της σημασίας του στην εγχώρια οικονομία αλλά και τις προοπτικές που θα έχει η διείσδυση του IoT στον συγκεκριμένο κλάδο. Η χρήση του εν λόγω δικτύου βοηθάει στην βελτιστοποίηση των διαδικασιών λειτουργίας ενός θερμοκηπίου, της παραγωγικότητας και εξοικονόμησης πόρων (ενεργειακών, εργασίας).

Τέλος με την ενασχόληση και την κατασκευή του συγκεκριμένου δικτύου, καθίσταται δυνατή η επέκταση του σε οποιαδήποτε εφαρμογή απαιτεί παρατήρηση και έλεγχο παραμέτρων με την τροποποίηση των χρησιμοποιούμενων αισθητήρων.

#### **Λέξεις Κλειδιά:**

Internet of Things, IoT, Zigbee, 6LoWPAN, θερμοκήπιο, cc2530, ds18b20, dht11, java, vaadin, μικροελεγκτής, actuator, αισθητήρες ,ZB500, ZB502, Z-stack





# Abstract

The purpose of this thesis is the study and analysis of wireless networking technologies on the observation, control and recording of measurable parameters in industrial, residential and rural environment. These procedures belong to the fast growing industry of Internet of Things (IoT).

First we deal with the analysis of the term Internet of Things, the current situation of the industry and market penetration, but also the prospects of the future. When investigating this study the majority of technologies that have to do with the IoT sector. In this thesis we chose two technologies for in-depth analysis (Zigbee and 6LoWPAN) who will dominate in the part of networking of IoT.

We continued with the practical application of the Zigbee standard in a wireless sensor network. This network concerns the control and observation of parameters in rural areas and more specifically in a greenhouse.

Specifically, the network consists of four nodes, each of which performs a different task. The first node is the network coordinator and the target device of all measurements and controls and features serial communication with the computer which runs the application for disclosure of information on the internet. The second node performs the function of the router to the destination device but also collects and sends measurements itself from inside the greenhouse. The two last nodes are energy autonomous (powered by batteries) and are end devices that hold the function of collecting and sending measurements from the featured sensors.

The collection of measurements to the computer is done through a Java app that records the measurements in a local database. The disclosure of the measurement is done through a web app that creates an interface with the presentation of data and makes it accessible from the Internet using DDNS (Dynamic Domain Name System). The interface enables the user to remotely control parameters.

The choice of the agricultural industry was based on the importance of the domestic economy and the prospects that the penetration of IoT will have in this sector. The use of this network helps to optimize operating procedures of a greenhouse, productivity and savings (energy, labor).

Finally, with the occupation and the construction of the network, it becomes possible to extend into any application requires observation and control parameters with the modification of the used sensors.

**Keywords:**

Internet of Things, IoT, Zigbee, 6LoWPAN, greenhouse, cc2530, ds18b20, dht11, java, vaadin, microcontroller, actuator, sensors ,ZB500, ZB502, Z-stack



## Περιεχόμενα

Περίληψη .....	6
Abstract .....	9
Υπόμνημα .....	7
1 Εισαγωγή.....	9
1.1 Αντικειμενικός σκοπός .....	9
1.2 Δομή διπλωματικής .....	9
1.3 Ευχαριστίες .....	10
2 Internet of Things.....	11
2.1 Ξεπερνώντας τις προκλήσεις σύνδεσης έξυπνων κόμβων στο Internet of Things .....	12
2.2 Συλλαμβάνοντας την ιδέα του Internet of Things .....	13
2.3 Διαλειτουργικότητα μέσω στάνταρ πρωτόκολλων .....	16
2.4 Πετυχαίνοντας χαμηλότερη κατανάλωση ισχύος .....	17
2.5 Σημασία λογισμικού και σχεδιασμού εφαρμογών.....	18
2.6 Μικρότερος χρόνος στην αγορά για τις εφαρμογές IoT.....	19
3 Ασύρματες τεχνολογίες δικτύωσης .....	20
3.1 Μοντέλο OSI.....	20
3.2 Wi-Fi .....	21
3.2.1 Εμβέλεια .....	21
3.2.2 Κατανάλωση .....	21
3.2.3 Ασφάλεια .....	21
3.2.4 Υλικό.....	22
3.3 Bluetooth.....	22
3.3.1 Λειτουργία .....	22
3.3.2 Κατανάλωση .....	22
3.3.3 Ρυθμός μετάδοσης .....	23
3.4 GSM.....	23
3.4.1 Κυψελοειδής δομή δικτύου .....	23
3.4.2 Αρχιτεκτονική.....	24
3.4.3 Πιστοποίηση και ασφάλεια.....	24
3.5 IEEE 802.15.4.....	24

3.5.1	ISA100.11a .....	25
3.5.2	WirelessHART.....	25
3.5.3	6LoWPAN .....	25
3.5.4	MiWi.....	26
3.5.5	Zigbee.....	26
3.6	Σύγκριση επιλογών ασύρματης δικτύωσης.....	26
4	IPv6 6lowpan.....	29
4.1	6LoWPAN Αρχιτεκτονική Δικτύου.....	29
4.2	IPv6 πάνω στο 802.15.4 .....	30
4.3	Στρώμα προσαρμογής 6LoWPAN .....	31
4.3.1	Ενσωμάτωση μορφής επικεφαλίδας.....	32
4.3.2	Επικεφαλίδα κατακερματισμού .....	33
4.3.3	Επικεφαλίδα διευθυνσιοδότησης πλέγματος.....	34
4.3.4	Συμπίεση επικεφαλίδας IPv6 κατά RFC4944.....	34
4.3.5	Συμπίεση επικεφαλίδας UDP κατά RFC4944 .....	35
4.3.6	Παραδείγματα συμπίεσης.....	36
4.3.7	Βελτιωμένη συμπίεση επικεφαλίδας UDP/IPv6.....	37
4.3.8	Βελτιωμένα παραδείγματα συμπίεσης επικεφαλίδων UDP/IPv6 .....	39
4.4	IPv6/6LoWPAN αρχιτεκτονική .....	39
4.4.1	IEEE 802.15.4 στη πράξη.....	40
4.4.2	Πλέγμα «χαμηλά» ή δρομολόγηση «ψηλά».....	41
4.4.3	Διευθυνσιοδότηση και αυτόματη διαμόρφωση.....	42
4.4.4	Εύρεση γείτονα (Neighbor Discovery).....	43
4.4.5	Δρομολόγηση.....	43
4.4.6	Θέματα ασφάλειας.....	43
5	Zigbee.....	44
5.1	Εισαγωγή.....	44
5.2	Εισαγωγικές έννοιες.....	45
5.2.1	Devices .....	45
5.2.2	Services .....	46
5.2.3	Primitives .....	46
5.2.4	Binding .....	46

5.2.5	SDUs και PDUs .....	47
5.2.6	Management entities, data entities and SAPs.....	49
5.3	802.15.4 Φυσικό επίπεδο .....	50
5.3.1	Energy detection .....	50
5.3.2	Carrier sense .....	50
5.3.3	Link Quality Indicator .....	51
5.3.4	Clear Channel Assessment .....	51
5.3.5	Σταθερές και Χαρακτηριστικά .....	52
5.3.6	Υπηρεσίες φυσικού επιπέδου .....	52
5.3.7	Πλαίσιο φυσικού επιπέδου .....	55
5.3.8	Συνοπτική παρουσίαση των αρμοδιοτήτων του φυσικού επιπέδου ...	55
5.4	802.15.4 Επίπεδο MAC .....	56
5.4.1	CSMA/CA .....	56
5.4.2	Beacon-Enabled vs. Nonbeacon Networking .....	59
5.4.3	Superframe .....	60
5.4.4	Υπηρεσίες επιπέδου MAC .....	61
5.4.5	Πλαίσιο επιπέδου MAC .....	65
5.4.6	Συνοπτική παρουσίαση των αρμοδιοτήτων του επιπέδου MAC.....	66
5.5	Zigbee Επίπεδο δικτύου .....	67
5.5.1	Μηχανισμοί Επικοινωνίας .....	68
5.5.2	Τοπολογίες .....	71
5.5.3	Δρομολόγηση (routing) .....	74
5.5.4	Υπηρεσίες επιπέδου δικτύου .....	76
5.5.5	Πλαίσιο επιπέδου δικτύου .....	78
5.5.6	Συνοπτική παρουσίαση των αρμοδιοτήτων του επιπέδου δικτύου .....	79
5.6	Zigbee Επίπεδο εφαρμογής .....	79
5.6.1	Application Framework.....	80
5.6.2	ZDO (Zigbee Device Objects) .....	83
5.6.3	APS (Application Support Sublayer).....	84
5.6.4	Πλαίσιο APS .....	84
5.6.5	Συνοπτική παρουσίαση των αρμοδιοτήτων του επιπέδου εφαρμογής ...	86

5.7	Ασφάλεια .....	87
5.7.1	Encryption .....	87
5.7.2	Authentication .....	89
5.7.3	Auxiliary frame header .....	89
5.8	Zigbee στην πράξη .....	90
5.9	Τελική επιλογή πρωτοκόλλου .....	91
6	Ασύρματο δίκτυο αισθητήρων: εφαρμογή σε θερμοκήπιο .....	92
6.1	Μηχανική του θερμοκηπίου .....	92
6.1.1	Ορισμός- Ιστορία .....	92
6.1.2	Σύστημα ελέγχου αυτοματισμών για θερμοκήπια .....	92
6.1.3	Περιβάλλον θερμοκηπίου .....	93
6.1.4	Παράμετροι ελέγχου θερμοκηπίου .....	93
6.2	Συστήματα διαχείρισης θερμοκηπίων .....	95
6.2.1	Libellium Agriculture .....	95
6.2.2	GrowTronix .....	96
6.3	Περιγραφή δικτύου .....	96
7	Hardware and Software .....	98
7.1	Υλικό-Hardware .....	98
7.1.1	CC2530 .....	98
7.1.2	ZB500-ZB502 .....	101
7.1.3	DEBUGGER .....	103
7.1.4	CC2531 .....	103
7.1.5	SENSORS .....	104
7.1.6	Υπολογισμός συνολικού κόστους υλικού .....	107
7.2	Λογισμικό-Software .....	108
7.2.1	Z-Stack .....	108
7.2.2	IAR Embedded Workbench for 8051 .....	109
7.2.3	Ubiqua Protocol Analyzer .....	110
7.2.4	IntelliJ IDEA .....	111
8	Έλεγχος θερμοκηπίου: ανάπτυξη και λειτουργία εφαρμογής .....	113
8.1	Ανάπτυξη λογισμικού μικροελεγκτών .....	113
8.1.1	Τροποποιήσεις .....	115

8.1.2	Βήματα λειτουργίας.....	116
8.2	Ανάπτυξη λογισμικού Web Application.....	117
8.2.1	Host.....	117
8.2.2	Diplomatiki.....	123
8.3	Διαδικασία σύνδεσης κόμβων και λειτουργία δικτύου .....	128
8.3.1	Σχηματισμός δικτύου.....	128
8.3.2	Τοπολογία δικτύου .....	131
8.3.3	Διαδικασία Binding.....	133
8.4	Λειτουργία κόμβων.....	137
8.4.1	Λειτουργία End Devices.....	137
8.4.2	Λειτουργία Router .....	139
8.4.3	Λειτουργία Coordinator.....	141
8.5	Λειτουργία Web Application.....	144
8.5.1	Διεπαφή χρήστη.....	144
9	Συμπεράσματα και ανοιχτά θέματα.....	147
10	Βιβλιογραφία-Παραπομπές.....	149





## Υπόμνημα

AES	Advanced Encryption Standard
AF	Application Framework
APDU	Application Protocol Data Unit
APS	Application Support Sublayer
APSDE	Application Support Sublayer Data Entity
APSME	Application Support Sublayer Management Entity
ASDU	Application Service Data Unit
CAP	Contention Access Period
CCA	Clear Channel Assessment
CFP	Contention Free Period
CS	Carrier Sense
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
DE	Data Entity
ED	Energy Detection
FFD	Full Function Device
GTS	Guaranteed Time Slot
HAL	Hardware Abstraction Layer
IOT	Internet Of Things
LQI	Link Quality Indication
MCPS	MAC Common Part Sublayer
ME	Management Entity
MIC	Message Integrity Code
MLME	MAC Layer Management Entity
MPDU	MAC Protocol Data Unit
MSDU	MAC Service Data Unit
MTU	Maximum Transmission Unit
ND	Neighbor Discovery
NLDE	Network Layer Data Entity
NLME	Network Layer Management Entity
NPDU	Network Protocol Data Unit
NSDU	Network Service Data Unit
OSAL	Operating System Abstraction Layer
OSI	Open System Interconnect
PAN	Personal Area Network
PDU	Protocol Data Unit
PIB	PAN Information Base
PIB	PAN Information Base
PLDE	Physical Layer Data Entity
PLME	Physical Layer Management Entity

PPDU	Physical Protocol Data Unit
PSDU	Physical Service Data Unit
RFD	Reduced Function Device
RSS	Received Signal Strength
RTS	Request To Send
SAP	Service Access Point
SDU	Service Data Unit
SNR	Signal to Noise Ratio
SOC	System On Chip
ZC	Zigbee Coordinator
ZCL	Zigbee Cluster Library
ZDO	Zigbee Device Objects
ZDP	Zigbee Device Profile
ZED	Zigbee End Device
ZR	Zigbee Router

# 1 Εισαγωγή

## 1.1 Αντικειμενικός σκοπός

Ο αντικειμενικός σκοπός της παρούσας διπλωματικής είναι η κατανόηση και η εμβάθυνση σε εφαρμογές βιομηχανικών και οικιακών αυτοματισμών με την χρήση ασύρματων τεχνολογιών δικτύωσης. Οι εφαρμογές τέτοιου τύπου εντάσσονται σε έναν γενικότερο τεχνολογικό τομέα που ονομάζεται Internet of Things (IoT). Η έννοια του IoT έχει αναδειχθεί τα τελευταία χρόνια και η ιδέα που προτείνει είναι η σύνδεση «αντικειμένων» στο διαδίκτυο και η αξιοποίηση και μελέτη της πληροφορίας που προέρχεται από αυτά.

Η έλευση του τομέα IoT έθεσε το ζήτημα της οικονομικής διασύνδεσης σε επίπεδο ενέργειας και κόστους. Για αυτό τον λόγο έχουν αναπτυχθεί πρωτόκολλα τα οποία βασίζονται κυρίως στο πρότυπο 802.15.4 της IEEE. Κύριο γνώρισμα αυτών των πρωτοκόλλων είναι η πολύ χαμηλή απαίτηση σε ισχύ, που τα καθιστά κατάλληλα για εφαρμογές που δεν υπάρχουν υποδομές τροφοδοσίας ή χαρακτηρίζονται από συνεχώς μεταβαλλόμενη θέση (mobility).

Στα πλαίσια της πρακτικής εφαρμογής του IoT, δημιουργούμε ένα δίκτυο αισθητήρων για θερμοκήπιο. Στόχος μας είναι ο απομακρυσμένος έλεγχος και παρακολούθηση των παραμέτρων ενός θερμοκηπίου που διέπουν την λειτουργία του. Ταυτόχρονα προσπαθούμε να εξασφαλίσουμε τον περιορισμό του κόστους της εφαρμογής, ούτως ώστε να κρίνεται ανταγωνιστική.

## 1.2 Δομή διπλωματικής

Η διπλωματική αυτή χωρίζεται σε εννιά επιμέρους κεφάλαια. Τα πρώτα 4 κεφάλαια καλύπτουν το θεωρητικό κομμάτι του θέματος και τα υπόλοιπα ασχολούνται με την υλοποίηση της πρακτικής εφαρμογής.

Στο δεύτερο κεφάλαιο αναλύεται η σημασία και οι προοπτικές του Internet of Things.

Στο τρίτο κεφάλαιο γίνεται μία επιγραμματική ανασκόπηση των υπάρχοντων τεχνολογιών ασύρματης δικτύωσης. Αναφέρονται τα βασικά τους λειτουργικά χαρακτηριστικά και καταλήγει συγκρίνοντας και διαλέγοντας τις καταλληλότερες τεχνολογίες για εφαρμογές IoT.

Στο τέταρτο κεφάλαιο εξετάζουμε το πρωτόκολλο 6LoWPAN σε κάθε δικτυακό επίπεδο και αναλύονται οι δυνατότητες που προσφέρει.

Στο πέμπτο κεφάλαιο παρουσιάζεται εκτενώς το πρωτόκολλο ZigBee που βασίζεται στο πρότυπο IEEE 802.15.4. Αναλύονται όλα τα επίπεδα δικτύωσης, το φυσικό και το MAC (802.15.4) και τα δικτύου και εφαρμογής (ZigBee).

Στο έκτο κεφάλαιο ασχολούμαστε πλέον με το πρακτικό μέρος της διπλωματικής το οποίο βασίζεται στα προηγούμενα κεφάλαια. Πιο συγκεκριμένα αναφέρεται συνοπτικά στην λειτουργία του θερμοκηπίου, τις ανάγκες του και παρουσιάζονται κάποιες λύσεις που κυκλοφορούν ήδη στην αγορά.

Στο έβδομο κεφάλαιο παρουσιάζουμε τα εργαλεία που χρησιμοποιήθηκαν για την ανάπτυξη της εφαρμογής. Αυτά χωρίζονται σε δύο υποκατηγορίες το hardware και το software.

Στο όγδοο κεφάλαιο ο αναγνώστης έχει την δυνατότητα να παρακολουθήσει σε βήματα την υλοποίηση της εφαρμογής. Τέλος εμφανίζονται εικόνες της λειτουργίας της, από την πλευρά του τελικού χρήστη.

Στο ένατο και τελευταίο κεφάλαιο παρουσιάζονται τα συμπεράσματα της διπλωματικής καθώς και ανοιχτά θέματα και προτάσεις συνέχισης της στο μέλλον.

### **1.3 Ευχαριστίες**

Η παρούσα διπλωματική είναι αποτέλεσμα ομαδικής προσπάθειας. Για αυτό το λόγο θα θέλαμε να ευχαριστήσουμε ο καθένας με την σειρά του τον ανώνυμο συνδιπλωματικό για την επίτευξη της ολοκλήρωσης της. Βέβαια δεν πρέπει παραλείψουμε τις ευχαριστίες μας στον επιβλέπων της διπλωματικής Αποστόλη Κοτοπούλη, ο οποίος μας βοήθησε να ξεπεράσουμε τον αρχικό μας ενδοιασμό για την ανάληψη της και μας έδωσε τις κατάλληλες συμβουλές για να συνεχίσουμε και να την ολοκληρώσουμε μέχρι τέλους. Ευχαριστούμε επίσης τον καθηγητή και δάσκαλο κ. Συκά για την επίβλεψη της διπλωματικής και τις παρατηρήσεις για την ολοκλήρωση της. Τέλος είναι χρέος μας να ευχαριστήσουμε τον συμφοιτητή και φίλο μας Ζαννή Καλαμπούκη ο οποίος μας εισήγαγε σε κάποιες έννοιες του Web Development.

## 2 Internet of Things

Το Internet of things (Διαδίκτυο των αντικειμένων) είναι μία ιδέα κατά την οποία ο εικονικός κόσμος της τεχνολογίας της πληροφορίας (Information Technology) ενσωματώνεται με τον πραγματικό κόσμο των αντικειμένων. Ο πραγματικός κόσμος γίνεται ακόμα πιο προσβάσιμος μέσω υπολογιστών και δικτυωμένων συσκευών τόσο στις επιχειρήσεις όσο και σε καθημερινές εφαρμογές. Έχοντας πρόσβαση σε κατάλληλα επεξεργασμένη πληροφορία, έχουμε την δυνατότητα να διαχειριστούμε ελεύθερα από μακροσκοπικό σε μικροσκοπικό επίπεδο, και ανάστροφα, και μπορούμε να υπολογίζουμε, να οργανώνουμε και να δρούμε αναλόγως. Ωστόσο, το Internet of Things είναι κάτι παραπάνω από ένα εργαλείο σχεδιασμένο για επιχειρήσεις, για την διαχείριση των διαδικασιών της πιο αποδοτικά και πιο αποτελεσματικά, αφού θα εισάγει μία ευκολότερη καθημερινότητα.

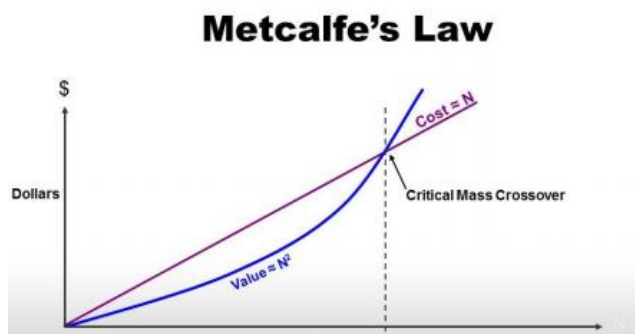
Η πρόσβαση σε πληροφορία πραγματικού χρόνου χρησιμοποιώντας υποδομές επικοινωνιών, οπουδήποτε οποτεδήποτε όπως προτείνει η ιδέα του Internet of Things, απαιτεί ανοιχτές, επεκτάσιμες, ασφαλείς και τυποποιημένες υποδομές, οι οποίες δεν υπάρχουν ολοκληρωμένες σήμερα.

Ο όρος Internet of things δεν είναι ορισμένος με σαφήνεια. Έχει χρησιμοποιηθεί και έχει παρερμηνευθεί ως όρος εντυπωσιασμού, τόσο από την επιστημονική έρευνα όσο και από στρατηγικές πωλήσεων και μάρκετινγκ. Μέχρι και σήμερα παραμένει δύσκολο να καταλήξουμε σε ένα ξεκάθαρο ορισμό. Ένας ορισμός που έχει διατυπωθεί:

«Το Internet of Things είναι ένα ολοκληρωμένο μέρος του Future Internet και θα μπορούσε να οριστεί ως ένα δυναμικό παγκόσμιο δίκτυο με δυνατότητα αυτορρύθμισης, βασισμένο σε πρότυπα και διαλειτουργικά πρωτόκολλα επικοινωνίας, όπου φυσικά και εικονικά αντικείμενα έχουν ταυτότητα, φυσικές ιδιότητες, εικονικές προσωπικότητες και χρησιμοποιούν ευφυείς διεπαφές και είναι απρόσκοπτα ενσωματωμένο στο δίκτυο της τεχνολογίας. Στο Internet of Things, τα «αντικείμενα» (things) προβλέπεται ότι θα έχουν ενεργή συμμετοχή στις επιχειρήσεις, στην πληροφορία και στις κοινωνικές διαδικασίες, όπου θα είναι σε θέση να αλληλεπιδρούν και να επικοινωνούν μεταξύ τους και με το περιβάλλον ανταλλάσσοντας πληροφορίες και δεδομένα που «αισθάνονται» από το περιβάλλον τους, ενώ αντιδρούν αυτόνομα στα γεγονότα του πραγματικού κόσμου και το επηρεάζουν τρέχοντας διεργασίες που εκκινούν ενέργειες και δημιουργούν υπηρεσίες, με ή χωρίς την άμεση παρέμβαση ανθρώπινου παράγοντα. Διασυνδέσεις στην μορφή υπηρεσιών διευκολύνουν την αλληλεπίδραση με αυτά τα έξυπνα αντικείμενα μέσω του διαδικτύου, εξετάζοντας και αλλάζοντας την κατάσταση τους και κάθε πληροφορία που σχετίζεται με αυτά, λαμβάνοντας υπόψη θέματα ασφάλειας και ιδιωτικότητας.»

## 2.1 Ξεπερνώντας τις προκλήσεις σύνδεσης έξυπνων κόμβων στο Internet of Things

Το διαδίκτυο έχει εξελιχθεί πολύ τα τελευταία 30 χρόνια. Το παλιό IPv4 δίνει την σκυτάλη στο καινούργιο IPv6 έτσι ώστε κάθε συσκευή συνδεδεμένη στο διαδίκτυο να έχει την δικιά της IP. Η επικοινωνία μηχανής με μηχανή (M2M) βρίσκεται σε άνοδο, επιτρέποντας να ανταλλάσσουν και να δρουν πάνω σε δεδομένα χωρίς να ανθρώπινη επέμβαση. Η έκταση και η κλίμακα του διαδικτύου έχουν αλλάξει καθώς οι ηγέτες της βιομηχανίας προβλέπουν ότι ο αριθμός των διασυνδεδεμένων συσκευών θα ξεπεράσει τα 15 δις κόμβους μέχρι το 2015 και να φτάσει πάνω από 50 δις μέχρι το 2020. Η πρόκληση της βιομηχανίας ενσωματωμένων είναι να ξεκλειδώσει την αξία αυτού του αναπτυσσόμενου δικτύου διασυνδεδεμένων συσκευών, που συχνά αναφέρεται ως Internet of Things.

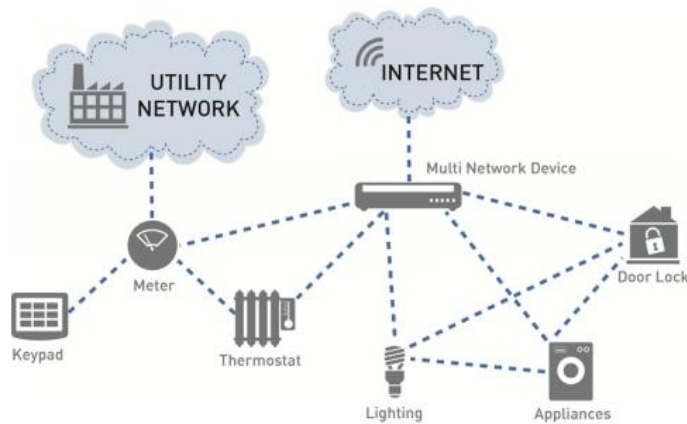


Εικόνα 2-1 Metcalfe's Law

Σύμφωνα με τον νόμο του Metcalfe, η αξία ενός δικτύου είναι ίση με το τετράγωνο του αριθμού συσκευών που είναι συνδεδεμένες σε αυτό. Στα άκρα του Internet of Things είναι συσκευές και εξοπλισμός που χρησιμοποιούμε κάθε μέρα. Αυτά τα «πράγματα» είναι διασυνδεδεμένα μέσω μίας υποδομής χρησιμοποιώντας έναν συνδυασμό τρόπων επικοινωνίας παρέχοντας μια ισχυρή αμφίδρομη σχέση επικοινωνίας, χαμηλής καθυστέρησης για γρήγορη ανταπόκριση, χαμηλής ισχύος και επαρκή ρυθμό δεδομένων για την συγκέντρωση δεδομένων από πολλές συνδεδεμένες συσκευές. Η υποδομή αυτή χρησιμεύει επίσης ως πύλη (gateway) προς το διαδίκτυο και επιτρέπει την απομακρυσμένη παρακολούθηση και τον έλεγχο συσκευών από άλλα δίκτυα, εταιρίες κοινής ωφέλειας και τελικούς χρήστες.

Η πλειοψηφία των συνδεδεμένων συσκευών στο Iot είναι κόμβοι οι οποίοι βρίσκονται στα άκρα του δικτύου. Αυτοί οι κόμβοι περιέχουν μικροελεγκτές (MCU), ασύρματες συσκευές, αισθητήρες και ενεργοποιητές (actuators) τα οποία είναι για το Internet of Things το 'μουαλό', τα 'μάτια' και τα 'δάκτυλα' του. Είναι λογικό ότι οι χρήστες δεν θέλουν να παρακολουθούν 50 ή και παραπάνω αισθητήρες που είναι τοποθετημένοι στο σπίτι τους για να ελέγξουν αν έχουν ενεργοποιημένο τον

κλιματισμό ταυτόχρονα με ανοιχτά παράθυρα. Οι πληροφορίες που συλλέγουν αυτές οι συσκευές είναι σημαντικές, όπως και η ικανότητα τους να επικοινωνούν μεταξύ τους και να παίρνουν μόνες τους αποφάσεις ώστε να μην χρειάζεται να το κάνουμε εμείς.



Εικόνα 2-2

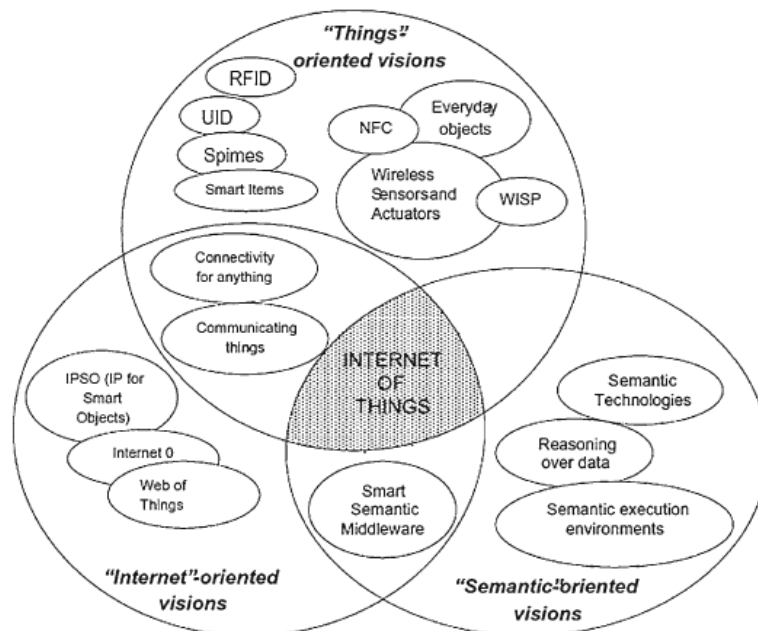
Οι προκλήσεις για την ενσωμάτωση εφαρμογών διασυνδεδεμένων συσκευών στο Internet of Things είναι αρκετά διαφορετικές από τις παραδοσιακές δικτυακές τερματικές συσκευές. Οι κατασκευαστές οικιακών συσκευών και φωτισμού, για παράδειγμα, πρέπει να βρουν νέους τρόπους δικτύωσης και ενσωματωμένο λογισμικό ώστε τα προϊόντα τους να ξεπεράσουν τις βασικές τους ικανότητες. Αυτή τη ανάπτυξη μπορούν να την κάνουν οι εταιρίες είτε μόνες τους είτε σε συνεργασία με εταιρίες που έχουν ήδη δημιουργήσει τέτοια προϊόντα και μπορούν εύκολα να τα εισάγουν στα δικά τους συστήματα.

## 2.2 Συλλαμβάνοντας την ιδέα του Internet of Things

Οι ευφυείς μετρητές (smart meters) είναι ένα πολύ χαρακτηριστικό παράδειγμα μίας υψηλού-προφίλ εφαρμογής IoT. Αντί να μετρούν απλά την κατανάλωση ηλεκτρικής ενέργειας, οι μετρητές αυτοί επιτρέπουν στις εταιρίες κοινής ωφέλειας (πχ ΔΕΗ) να επικοινωνούν με τους καταναλωτές σχεδόν σε πραγματικό χρόνο ώστε να απενεργοποιήσουν τις συσκευές υψηλού φορτίου, όπως οι συσκευές κλιματισμού, κατά την αιχμή της ζήτησης. Το αποτέλεσμα είναι χαμηλότερος λογαριασμός για τους καταναλωτές, καθώς και μια μετατόπιση του υψηλού φορτίου με αποτέλεσμα οι εταιρίες παροχής ηλεκτρισμού να μην χρειάζεται να επενδύσουν για εγκατάσταση παραπάνω φορτιών για να ανταπεξέλθουν στην ζήτηση μόλις λίγων ημερών, που η ζήτηση τείνει να ξεπεράσει την παραγωγή.



Οι ευφυείς μετρητές είναι μόνο μία πτυχή του επερχόμενου έξυπνου σπιτιού (smart home). Εκτός από την κοινή χρήση αρχείων και περιεχόμενου πολυμέσων, τα οικιακά δίκτυα επιτρέπουν ένα πιο μεγάλο εύρος εφαρμογών ασφαλείας, παρακολούθησης και αυτοματοποίησης που περιλαμβάνουν έξυπνο φωτισμό και συσκευές. Η ύπαρξη ακόμα και μικρού αριθμού αισθητήρων (πχ κίνησης, υγρασίας, θερμοκρασίας, θραύση γυαλιού) δημιουργεί ένα ισχυρό δίκτυο πλέγμα (mesh network) το οποίο επεκτείνει τις δυνατότητες όλων των συσκευών που είναι συνδεδεμένες σε αυτό. Το Ιot για την ακρίβεια μπορεί να προσφέρει σημαντικό όφελος στον βιομηχανικό αυτοματισμό, έλεγχο φωτισμού, οικιακό/κτιριακό αυτοματισμό, ασφάλεια και παρακολούθηση, υγεία και γυμναστική. Ο όρος appcessory (εφαρμογή-αξεσουάρ) έχει ήδη επινοηθεί για να περιγράψει εφαρμογές έξυπνων κινητών που μπορούν να επικοινωνήσουν και να ελέγξουν αισθητήρες και φώτα στο σπίτι ή στην επιχείρηση.



Εικόνα 2-3

Μία εφαρμογή του νόμου του Metcalfe περιλαμβάνει συσκευές που δεν είναι χρήσιμες όταν εγκαθίστανται μόνες τους, αλλά μπορούν να προσθέσουν τεράστια αξία όταν μπορούν να αξιοποιήσουν τις υπάρχουσες υποδομές. Σκεφτείτε την μείωση της ενέργειας αναμονής, της ενέργειας δηλαδή που καταναλώνουν συσκευές που δεν χρησιμοποιούνται όπως τηλεοράσεις και υποσυστήματα. Εκτιμάται ότι αυτή η ισχύς είναι μεταξύ του 7-15% της συνολικής οικιακής ηλεκτρικής ισχύς. Η εγκατάσταση ενός αισθητήρα κίνησης για την ανίχνευση

παρουσίας μέσα σε ένα δωμάτιο ώστε να ενεργοποιείται- απενεργοποιείται η ισχύς σε αυτές τις συσκευές θα ήταν ίσως απαγορευτική λόγω κόστους. Ωστόσο αν η τηλεόραση μπορεί να χρησιμοποιήσει τους αισθητήρες κίνησης που είναι ήδη εγκατεστημένοι από το σύστημα συναγερμού, τότε η ενέργεια αναμονής μπορεί να μειωθεί με έναν οικονομικά αποδοτικό τρόπο.

Οι αισθητήρες ενός συστήματος συναγερμού μπορούν να χρησιμοποιηθούν για ένα ευρύ φάσμα εφαρμογών. Για παράδειγμα για να ανοιγοκλείνουν τα φώτα όταν ένα άτομο εισέρχεται- εξέρχεται σε ένα δωμάτιο. Τέτοιου είδους αλληλεπιδράσεις μεταξύ διαφορετικών συστημάτων μπορεί να δώσει έναν μεγάλο αριθμό πλεονεκτημάτων στους χρήστες:

- Υψηλότερη απόδοση: όταν μια συσκευή είναι συνδεδεμένη στο Internet of Things τότε μπορεί να καθορίζει την καλύτερη χρονική στιγμή για να λειτουργήσει πχ λειτουργία πλυντηρίου τις ώρες χαμηλής ζήτησης (βραδινό τιμολόγιο)
- Προληπτική χρήση: σήμερα μπορεί ένας χρήστης να ρυθμίσει το κλιματιστικό να δουλεύει λίγο πριν γυρίσει σπίτι από την δουλειά του. Αν αργήσει όμως τότε θα λειτουργεί χωρίς λόγο. Έξυπνα οικιακά συστήματα μπορούν να ελέγχονται απομακρυσμένα ώστε να μην υπάρχουν αυτές οι απώλειες.
- Προληπτική συντήρηση: έξυπνες συσκευές μπορούν να παρακολουθούν την λειτουργική τους 'υγεία' και να ειδοποιήσουν τους χρήστες οι τις εταιρίες κατασκευής τους για πιθανές βλάβες προτού οδηγηθεί σε παύση λειτουργίας.
- Κοινή διεπαφή ελέγχου: δεδομένου ότι οι χρήστες μπορούν να χρησιμοποιήσουν τις δίκτες τους έξυπνες συσκευές (smartphones- tablets) για να διαχειριστούν το δίκτυο τους, υπάρχει η δυνατότητα για μία εφαρμογή ελέγχου για όλες τις συσκευές και έτσι ο χρήστης δεν χρειάζεται να μάθει ένα διαφορετικό γραφικό περιβάλλον για κάθε νέα συσκευή ή κόμβο που συνδέεται στο δίκτυο.
- Ευκολία χρήσης: όταν οι συσκευές μπορούν να διαχειρίζονται μέσα σε ένα δίκτυο, οι χρήστες έχουν την δυνατότητα να ελέγχουν το δίκτυο από οπουδήποτε επιθυμούν, χρησιμοποιώντας τις εφαρμογές που επιθυμούν. Η αντιμετώπιση προβλημάτων επίσης απλοποιείται σε μεγάλο βαθμό. Για παράδειγμα, αντί μία συσκευή όταν παρουσιάζει σφάλμα να ενεργοποιεί κάποια LED, θα μπορούσε να περιγράψει με σαφήνεια τα λειτουργικά σφάλματα και προβλήματα.

Αξίζει να αναφερθεί σε αυτό το σημείο ότι πολλές από αυτές τις αλληλεπιδράσεις γίνονται μεταξύ συσκευών (M2M) και δεν απαιτούν την ανάμειξη του χρήστη. Αντί δηλαδή κάθε σύστημα να λειτουργεί ανεξάρτητα και να παίρνει αποφάσεις με

περιορισμένα δεδομένα, το Internet of Things επιτρέπει τα συστήματα να μοιράζονται πληροφορίες για να επεκτείνουν σε μεγάλο βαθμό τις δυνατότητες και την αξία τους πέρα από τον αρχικό τους σχεδιασμό. Η σύγκλιση των διάφορων εφαρμογών επιτρέπει σε όλες να δουλεύουν καλύτερα.

Η ισχύς του νόμου του Metcalfe σημαίνει ευκαιρίες για τις επιχειρήσεις σε κάθε κλάδο. Ενώ μία εταιρία συστημάτων ασφαλείας θα μπορούσε να επεκταθεί στον χώρο του φωτισμού και των οικιακών αυτοματισμών, θα μπορούσε αντ' αυτού να συνεργαστεί με καθιερωμένους κατασκευαστές φωτισμού ή αυτοματισμών, ώστε να δημιουργήσουν προϊόντα και υπηρεσίες προστιθέμενης αξίας. Αυτή είναι η δύναμη ενός οικοσυστήματος. Το Internet of Things επιτρέπει προμηθευτές ηλεκτρονικών εξαρτημάτων, προμηθευτές λογισμικού, κατασκευαστές ηλεκτρικών συσκευών και παρόχους υπηρεσιών να επικεντρωθούν στις ικανότητες τους και να αξιοποιήσουν τα πλεονεκτήματα των εταιρικών σχέσεων για την δημιουργία καινοτόμων εφαρμογών για τους καταναλωτές.

### **2.3 Διαλειτουργικότητα μέσω στάνταρ πρωτόκολλων**

Για να λειτουργήσει το Internet of Things πρέπει όλες οι συσκευές να συνδέονται χωρίς διακοπή. Ωστόσο δεν υπάρχει μόνο μία ασύρματη ή ενσύρματη τεχνολογία που να μπορεί να εξυπηρετήσει αποτελεσματικά ένα ολόκληρο δίκτυο. Για την ανάπτυξη οικονομικά αποδοτικών προϊόντων, οι μηχανικοί πρέπει να είναι σε θέση να επιλέξουν τον βέλτιστο τρόπο και πρωτόκολλο επικοινωνίας για την εφαρμογή τους. Ως αποτέλεσμα το Internet of Things στηρίζεται σε μια ποικιλία διαφορετικών διασυνδέσεων.

Για να μπορούν οι συσκευές να επικοινωνήσουν με το διαδίκτυο πρέπει σε κάποιο σημείο του καναλιού επικοινωνίας να υποστηρίζει πρωτόκολλο IP. Στα άκρα του δικτύου ωστόσο, το πρωτόκολλο IP μπορεί να είναι πολύ πλήρες πρωτόκολλο με μεγάλη επιβάρυνση σε δεδομένα αλλά και σε κόστος. Ομοίως αν και το Wi-Fi έχει πολύ καλή συνδεσιμότητα, καταναλώνει μεγάλη ισχύ, την στιγμή που πολλές συσκευές είναι περιορισμένες στην χρήση μπαταρίας ή ανανεώσιμων πηγών ενέργειας.

Οι συνδεδεμένες συσκευές πρέπει να είναι σε θέση να χρησιμοποιούν πρωτόκολλα όπως το ZigBee και το 6LoWPAN που είναι 'ελαφριά' και ο ρυθμός μεταφοράς δεδομένων αντανακλά τις απαιτήσεις τους. Συσκευές που συνδέονται στο Internet of Things μέσω ενός κεντρικού ελεγκτή μπορούν να χρησιμοποιήσουν IP πρωτόκολλο, δεδομένου ότι τα δεδομένα συγκεντρώνονται και μετατρέπονται πριν περάσουν στο διαδίκτυο μέσω μιας συσκευής πύλης (gateway).

Ο ιδανικός συνδυασμός ασύρματων τεχνολογιών και πρωτοκόλλων εξαρτάται από τις ανάγκες της κάθε εφαρμογής. Σήμερα, το Wi-Fi αποτελεί την κατάλληλη τεχνολογία όταν χρειάζομαστε υψηλή ταχύτητα μεταφοράς δεδομένων, όπως κατά

την μεταφορά βίντεο. Για εφαρμογές με χαμηλό εύρος ζώνης, που δεν χρειάζονται άμεση αλληλεπίδραση με τον χρήστη, το 2.4 GHz ZigBee και τεχνολογίες που δουλεύουν κάτω από το 1 GHz παρουσιάζουν πολύ χαμηλότερη κατανάλωση για την δημιουργία ασύρματης σύνδεσης, ιδιότητα η οποία τις καθιστά ιδανικές για ενσωματωμένα συστήματα. Για απλές εφαρμογές, όπως το άνοιγμα μιας γκαραζόπορτας ή γενικά συστήματα που απαιτούν μεγάλες αποστάσεις συνδεσιμότητας, πχ συστήματα άρδευσης, η βέλτιστη προσέγγιση είναι τεχνολογίες κάτω από GHz (sub-GHz). Αν η εφαρμογή μας χρειάζεται αμφίδρομη επικοινωνία, ασφάλεια ή/και ένα μεγάλο αριθμό κόμβων που πρέπει να συνδεθούν στο δίκτυο πλέγμα (mesh), τότε είναι καταλληλότερη λύση το ZigBee ή αντίστοιχες τεχνολογίες.

Υιοθετώντας τοπολογία πλέγματος (mesh topology) είναι ιδανική για πολλές εφαρμογές Internet of Things. Θεωρείστε ένα οικιακό σύστημα φωτισμού που ο αριθμός των κόμβων μπορεί εύκολα να υπερβεί 30 φώτα και αισθητήρες. Λαμβάνοντας υπόψη ότι ένα Wi-Fi router μπορεί να μην είναι σε θέση να παρέχει κάλυψη σε ολόκληρο το σπίτι, ένα δίκτυο πλέγματος επιτρέπει κάλυψη σε κάθε θέση του σπιτιού με το χαμηλότερο κόστος ανά κόμβο. Επιπλέον, πλεγματικά δίκτυα, μπορούν αυτόματα να ρυθμίζουν νέες συσκευές, έτσι ώστε να αξιοποιήσουν πρότυπα χρήσης που το σύστημα ήδη γνωρίζει. Η επεκτασιμότητα είναι επίσης ένας κρίσιμος παράγοντας. Το Bluetooth για παράδειγμα περιορίζεται στις 7 συσκευές ανά δίκτυο και το Wi-Fi στις 32. Δίκτυα πλέγματος είναι σε θέση να ενσωματώσουν πολλές περισσότερες συσκευές.

## **2.4 Πετυχαίνοντας χαμηλότερη κατανάλωση ισχύος**

Επειδή οι συσκευές στα άκρα του δικτύου συνήθως εκτελούν πολύ περιορισμένες εργασίες, τείνουν να έχουν αρκετά απλή αρχιτεκτονική που επικεντρώνεται στην συλλογή, την επεξεργασία απλών δεδομένων και την λειτουργία συνδεσιμότητας. Αν μια τέτοια συσκευή χρειάζεται ένα μικροελεγκτή 8-bit ή 32-bit εξαρτάται κυρίως από τους τύπους των υπολογισμών που πρέπει να εκτελέσει. Ο μεγαλύτερος διάυλος επικοινωνίας, και τα προηγμένα περιφερειακά ενός μικροελεγκτή 32-bit επιτρέπουν σημαντικά ταχύτερη μεταφορά δεδομένων και επεξεργαστική ισχύ από ένα 8-bit μικροελεγκτή, έτσι ώστε οι συσκευές να μπορούν να επιστρέψουν γρηγορότερα σε αδρανοποίηση (sleep mode) για καλύτερη ενεργειακή απόδοση.

Για πολλές συσκευές στα άκρα του δικτύου, όπως αισθητήρες φωτός και κίνησης που τοποθετούνται σε όλο το σπίτι, το κόστος εγκατάσταση καινούργιας καλωδίωσης για να τροφοδοτηθούν αυτές οι συσκευές είναι απαγορευτικό σε σύγκριση με το ίδιο το κόστος της συσκευής και την λειτουργία που θα εκτελέσει. Κατά συνέπεια αυτές οι συσκευές πρέπει να προσφέρουν υψηλότερη αποδοτικότητα ισχύος, ώστε να μπορούν να λειτουργούν με την χρήση μπαταρίας ή ανανεώσιμων πηγών ενέργειας. Επιπλέον αυτές οι συσκευές πρέπει να είναι

εύκολες στην εγκατάσταση, ακόμα και σε δύσκολα προστάσια σημεία και πρέπει να είναι σε θέση να λειτουργούν μεγάλο χρονικό διάστημα χωρίς να απαιτείται αντικατάσταση της μπαταρίας τους.

Οι μικροεπεξεργαστές που χρησιμοποιούν οι συσκευές στα άκρα του δικτύου, ιδανικά στηρίζουν πολλές λειτουργίες ενέργειας, επιτρέποντας στα περιφερειακά να λειτουργούν αυτόνομα σε διαφορετικές συχνότητες όταν ο επεξεργαστής αδρανοποιείται. Για παράδειγμα, μπορεί να χρησιμοποιηθεί άμεση πρόσβαση στην μνήμη (DMA) για συλλογή δεδομένων του αισθητήρα και ο επεξεργαστής να ενεργοποιείται μόνο όταν η προσωρινή μνήμη (buffer) έχει γεμίσει με δεδομένα προς επεξεργασία. Αυτές οι αρχιτεκτονικές είναι επίσης πολύ εξειδικευμένες για την μετάβαση από και προς την κατάσταση αναμονής γρηγορότερα, με στόχο την χαμηλότερη κατανάλωση κατά την ενεργοποίηση του επεξεργαστή.

## **2.5 Σημασία λογισμικού και σχεδιασμού εφαρμογών**

Το λογισμικό διαδραματίζει έναν πολύ σημαντικό ρόλο στην επίτευξη των χαρακτηριστικών και των δυνατοτήτων που χρειάζονται για να οικοδομηθεί το Internet of Things. Μπορεί το υλικό (hardware) να είναι το θεμέλιο για συνδεσιμότητα, το λογισμικό όμως επιτρέπει να πραγματοποιούνται οι αλληλεπιδράσεις μεταξύ των συσκευών (M2M) που εξασφαλίζουν ότι οι συσκευές λειτουργούν με έναν αξιόπιστο και συνεπή τρόπο ανεξάρτητα από το περιβάλλον λειτουργίας τους.

Αρκεί να σκεφτούμε πόσο σημαντικό ρόλο παίζει η ποιότητα μίας ασύρματης σύνδεσης στο περιβάλλον λειτουργίας της, πχ κάθε χρήστης κινητού, έχει νιώσει την ανάγκη να μετακινηθεί μέσα στο σπίτι του για να έχει καλύτερο σήμα. Συσκευές όπως ένας θερμοστάτης δεν πρόκειται να μετακινηθούν μετά την εγκατάσταση τους για να έχουν καλύτερο σήμα. Η καθυστέρηση (latency) έχει επίσης σημασία, μετά από 100ms χωρίς ανταπόκριση, οι περισσότεροι χρήστες έχουν την τάση να ξαναπατήσουν ένα κουμπί.

Το λογισμικό είναι αυτό που κάνει τα ασύρματα δίκτυα ισχυρά. Διασφαλίζει ότι τα μηνύματα έχουν ληφθεί και αξιοποιούνται, όπως πχ το ότι ένα φως όντως άναψε. Το λογισμικό επίσης είναι αυτό που επιτρέπει στους προγραμματιστές να εφαρμόσουν μεγαλύτερη ευφυΐα και ευελιξία σε συσκευές, ώστε να μπορούν να εντοπίζουν προβλήματα, να δημιουργούν εξαιρέσεις και ενδεχομένως να λύνουν προβλήματα χωρίς να χρειάζεται ανθρώπινη παρέμβαση.

Οι προγραμματιστές μπορούν επίσης να εφαρμόσουν προηγμένες λειτουργίες μέσω του λογισμικού. Για παράδειγμα, είναι χρήσιμο να μπορεί κάποιος να ενεργοποιήσει ένα φως απομακρυσμένα, αλλά είναι ακόμα πιο χρήσιμο να μπορεί να ενημερώσει τον χρήστη ότι χρειάζεται αντικατάσταση. Το λογισμικό είναι αυτό που επεκτείνει το δυνατό εύρος του αυτόνομου ελέγχου με στόχο την περαιτέρω

βελτίωση της αποτελεσματικότητας και της ευκολίας. Σκεφτείτε ότι ένα έξυπνο δίκτυο αισθητήρων θα μπορούσε να καθορίσει αν δεν είναι κανείς στο σπίτι και να απενεργοποιήσει όλες τις ηλεκτρικές και ηλεκτρονικές συσκευές. Το αποτέλεσμα μιας τέτοιας λειτουργίας, αν πολλαπλασιαστεί επί εκατοντάδες εκατομμύρια νοικοκυριά, είναι σημαντική εξοικονόμηση ενέργειας.

Το λογισμικό χρησιμεύει επίσης ως γέφυρα μεταξύ δικτύων και ελεγκτών. Για παράδειγμα, ορισμένοι χρήστες θα προτιμούσαν να ελέγχουν τις συσκευές τους από το κινητό τους και άλλοι από τον υπολογιστή τους. Ευέλικτο, εύκολο στην χρήση λογισμικό, είναι ένα τρόπος για τις κατασκευάστριες εταιρίες να ξεχωρίζουν τα προϊόντα τους από τους ανταγωνιστές τους.

Η πραγματικότητα είναι ότι οδηγούμαστε σε έναν κόσμο βασισμένο στις εφαρμογές. Μικροελεγκτές, αισθητήρες και ασύρματες συνδέσεις μπορεί να αποτελούν το θεμέλιο του Internet of Things, αλλά η πραγματική καινοτομία θα συμβεί στον χώρο του λογισμικού. Έτσι και αλλιώς, τι αξία θα είχαν τα δεδομένα από αισθητήρες αν δεν ξέραμε πώς να τα επεξεργαστούμε. Το κλειδί σε αυτό είναι η διαλειτουργικότητα και τα ανοιχτά πρότυπα, που επιτρέπουν σε ένα μεγάλο εύρος συσκευών να επικοινωνούν μεταξύ τους. Αυτή η δυνατότητα επικοινωνίας συσκευή με συσκευή αυξάνει την αξία του δικτύου και αφού έχει δημιουργηθεί το δίκτυο, περισσότερη πληροφορία και ευφυΐα μπορούν να αποκομισθούν με ένα αμελητέο πρόσθετο κόστος. Για να επιτευχθεί αυτό το επίπεδο πολυπλοκότητας, το λογισμικό πρέπει να παρέχει στις συσκευές ένα κοινό επίπεδο εφαρμογής το οποίο να μοιράζονται οι συσκευές και οι εφαρμογές. Με αυτό τον τρόπο η υποβόσκουσα τεχνολογία που χρησιμοποιείται για την μεταφορά δεδομένων, ελευθερώνει τον προγραμματιστή να καινοτομήσει γύρω από μία εφαρμογή IoT.

## **2.6 Μικρότερος χρόνος στην αγορά για τις εφαρμογές IoT**

Για να βοηθήσει τους μηχανικούς να βγάλουν στην αγορά τις IoT εφαρμογές τους γρηγορότερα, οι κατασκευαστές ημιαγωγών πρέπει να προσφέρουν ένα ευρύ φάσμα σχεδιαστικών εργαλείων, όπως βιβλιοθήκες εφαρμογών για την γρηγορότερη ενσωμάτωση κοινότυπων εφαρμογών, δείγματα εφαρμογών έτοιμα για την αγορά, εργαλεία ανάπτυξης εφαρμογών, πλήρη πρωτόκολλα επικοινωνίας και απλές εφαρμογές που παρουσιάζουν πχ την σύνδεση ενός αισθητήρα με κινητό μέσω διαδικτύου. Σήμερα, υπάρχουν εργαλεία ανάπτυξης, τα οποία μπορούν να δώσουν μία μακροσκοπική άποψη ενός δικτύου από μία κονσόλα για την διευκόλυνση αντιμετώπισης προβλημάτων και εντοπισμό πακέτων μέσα στο δίκτυο. Εξειδικευμένα εργαλεία ανάπτυξης είναι επίσης διαθέσιμα, που επιτρέπουν στους προγραμματιστές με λίγη ή ακόμα και καμία εμπειρία σχεδιασμού RF δικτύων να δημιουργήσουν ένα αποτελεσματικό και ισχυρό δίκτυο.

### 3 Ασύρματες τεχνολογίες δικτύωσης

#### 3.1 Μοντέλο OSI

Το μοντέλο αναφοράς Ανοικτής Διασύνδεσης Συστημάτων, ή μοντέλο αναφοράς OSI (αγγλ. OSI reference model) είναι μια διαστρωματωμένη, αφηρημένη περιγραφή για τη σχεδίαση τηλεπικοινωνιακών και δικτυακών πρωτοκόλλων η οποία καθορίστηκε από την πρωτοβουλία Ανοικτή Διασύνδεση Συστημάτων – OSI. Είναι γνωστό και ως μοντέλο των επτά επιπέδων. Το μοντέλο OSI υποδιαιρεί τις λειτουργίες ενός τηλεπικοινωνιακού δικτύου σε μια «κατακόρυφη» στοίβα από επίπεδα, για το καθένα από τα οποία μπορεί να οριστεί κάποιο πρωτόκολλο σε μία συγκεκριμένη υλοποίηση. Κάθε επίπεδο αξιοποιεί τις λειτουργίες του κατώτερου του στη στοίβα επιπέδου, ενώ στόχος του είναι να παρέχει λειτουργικότητα στο αμέσως ανώτερο επίπεδό του. Μία συγκεκριμένη υλοποίηση του μοντέλου, με καθορισμένα πρωτόκολλα για κάθε επίπεδο, ονομάζεται στοίβα πρωτοκόλλων ή απλά στοίβα. Το κάθε πρωτόκολλο υλοποιείται είτε σε υλικό είτε σε λογισμικό. Συνήθως τα κατώτερα επίπεδα υλοποιούνται στο υλικό ενώ τα ανώτερα σε λογισμικό. Τα επίπεδα, η ιεράρχηση τους και οι βασικές λειτουργίες τους φαίνονται στον παρακάτω πίνακα:

	Επίπεδο	Λειτουργία
Λογισμικό	7. Εφαρμογών	Παρέχεται στις εφαρμογές πρόσβαση στο δίκτυο
	6. Παρουσίασης	Αναπαράσταση δεδομένων και κρυπτογράφηση
	5. Συνόδου	Έλεγχος του διαλόγου μεταξύ των άκρων της επικοινωνίας
	4. Μεταφοράς	Αξιόπιστη επικοινωνία από άκρο σε άκρο
Υλικό	3. Δικτύου	Καθορισμός διαδρομών και λογικών διευθύνσεων των κόμβων στα πλαίσια ενός διαδικτύου
	2. Ζεύξης δεδομένων	Φυσική διευθυνσιοδότηση (MAC & LLC)
	1. Φυσικό	Δυαδική μετάδοση σήματος μέσω του φυσικού μέσου

Πίνακας 3-1 Μοντέλο OSI

## 3.2 Wi-Fi

Το IEEE 802.11 είναι μια οικογένεια προτύπων της IEEE για ασύρματα τοπικά δίκτυα (WLAN) που είχαν ως σκοπό να επεκτείνουν το 802.3 (Ethernet) στην ασύρματη περιοχή. Τα πρότυπα 802.11 είναι ευρύτερα γνωστά ως «WiFi» επειδή η WiFi Alliance, ένας οργανισμός ανεξάρτητος της IEEE, παρέχει την πιστοποίηση για τα προϊόντα που υπακούουν στις προδιαγραφές του 802.11. Αυτή η οικογένεια πρωτοκόλλων αποτελεί το καθιερωμένο πρότυπο της βιομηχανίας στο χώρο των ασύρματων τοπικών δικτύων.

### 3.2.1 Εμβέλεια

Τα δίκτυα Wi-Fi έχουν περιορισμένη εμβέλεια. Ένα τυπικό ασύρματο σημείο πρόσβασης (AP) που χρησιμοποιεί 802.11b ή 802.11g με εργοστασιακή κεραία έχει εμβέλεια μέχρι 35 m σε εσωτερικό χώρο και 100 m σε εξωτερικό. Το πρωτόκολλο IEEE 802.11n, ωστόσο, μπορεί να υπερδιπλασιάσει την εμβέλεια. Η εμβέλεια ποικίλλει επίσης με τη ζώνη συχνοτήτων. Wi-Fi στο εύρος συχνοτήτων 2,4 GHz έχει ελαφρώς καλύτερη εμβέλεια από Wi-Fi στο εύρος συχνοτήτων των 5 GHz που χρησιμοποιείται από 802.11a και προαιρετικά με 802.11n. Στις ασύρματους δρομολογητές (routers) με αποσπώμενη κεραία, είναι δυνατόν να βελτιωθεί η εμβέλεια με την εγκατάσταση αναβαθμισμένων κεραιών οι οποίες έχουν υψηλότερο κέρδος σε συγκεκριμένες κατευθύνσεις. Η εμβέλεια σε εξωτερικούς χώρους μπορεί να φτάσει σε πολλά χιλιόμετρα μέσω της χρήσης υψηλού κέρδους κατευθυντικές κεραιές στο δρομολογητή και στις απομακρυσμένες συσκευές.

	802.11n	802.11g	802.11b	802.11a
FREQUENCY	2.4 and 5 Ghz	2.4 Ghz	2.4 Ghz	5Ghz
N. antenna	at least 2	1	1	1
Max. Data rate	300Mbps	54Mbps	11Mbps	54Mbps
Non-Overlapping Channels	9-12	12	3-Jan	12
Cost of AP	+++	++	+	+++

Πίνακας 3-2 Χαρακτηριστικά 802.11

### 3.2.2 Κατανάλωση

Λόγω των αποστάσεων που μπορεί να φθάσει το Wi-Fi έχει σχετικά υψηλή κατανάλωση ισχύος. Η υψηλός ρυθμός μεταφοράς δεδομένων συμβάλλει επίσης αρνητικά στην κατανάλωση ισχύος. Μία τυπική κατανάλωση για δρομολογητή είναι 8-10 W.

### 3.2.3 Ασφάλεια

Το πιο κοινό πρωτόκολλο ασύρματης κρυπτογράφησης είναι το WEP (Wireless Equivalent), το οποίο έχει αποδειχθεί ότι παραβιάζεται πολύ εύκολα ακόμα και



όταν είναι σωστά ρυθμισμένο. Η κρυπτογράφηση WPA και WPA2 (Wi-Fi Protected Access) έγινε διαθέσιμο το 2003 με σκοπό να επιλύσει αυτό το πρόβλημα.

#### 3.2.4 Υλικό

Ένα σημείο ασύρματης πρόσβασης (WAP) συνδέει μία ομάδα ασύρματων συσκευών σε ένα παρακείμενο ενσύρματο δίκτυο LAN. Ένα σημείο πρόσβασης αντιπροσωπεύει έναν κόμβο του δικτύου, ο οποίος μεταφέρει δεδομένα μεταξύ των συνδεδεμένων συσκευών σε αυτό, και συνήθως είναι συνδεδεμένο με κάποια ενσύρματη συσκευή (πχ Ethernet switch ή ADSL modem) επιτρέποντας στις ασύρματες συσκευές να επικοινωνούν με άλλες ενσύρματες συσκευές και δίκτυα.

### 3.3 Bluetooth

Το Bluetooth είναι ένα ασύρματο πρότυπο για την μεταφορά δεδομένων σε μικρές αποστάσεις χρησιμοποιείται από σταθερές και φορητές συσκευές για την δημιουργία προσωπικών δικτύων (PAN). Εφευρέθηκε από την Ericsson το 1994, και αρχικά είχε σχεδιαστεί ως μία ασύρματη εναλλακτική για τα καλώδια δεδομένων RS-232. Μπορεί να συνδέσει διάφορες συσκευές, ξεπερνώντας τα προβλήματα συγχρονισμού.

#### 3.3.1 Λειτουργία

Το Bluetooth λειτουργεί στην περιοχή εύρους 2.4-2.4835 GHz. Το Bluetooth χρησιμοποιεί ασύρματη τεχνολογία FHSS. Τα προς μεταφορά δεδομένα χωρίζονται σε πακέτα και κάθε πακέτο μεταδίδεται σε ένα από 79 κανάλια, εύρους 1MHz το καθένα. Το Bluetooth 4.0 έχει εύρος 2Mhz και χρησιμοποιεί 40 κανάλια.

Ο τρόπος σύνδεσης συσκευών Bluetooth είναι master-slave. Ένας κόμβος μπορεί να είναι ανά πάσα στιγμή master και μπορεί να συνδεθεί ταυτόχρονα μέχρι και 7 συσκευές, αν και δεν έχουν όλες οι συσκευές αυτή την δυνατότητα. Οι συσκευές μπορούν να αλλάξουν ρόλους, με κοινή συμφωνία και ένα slave να γίνει master.

#### 3.3.2 Κατανάλωση

Όπως προαναφέρθηκε, το Bluetooth χρησιμοποιείται για δημιουργία δικτύων μικρής απόστασης. Η κατανάλωση κάθε συσκευής εξαρτάται από την απόσταση λειτουργίας, οποία την κατατάσσει ανάλογα σε μια κλάση. Χαρακτηριστικές καταναλώσεις φαίνονται στον παρακάτω πίνακα.

ΚΛΑΣΗ	ΜΕΓ. ΙΣΧΥΣ (mW)	ΕΜΒΕΛΕΙΑ
1	100	~100
2	2,5	~10
3	1	~1

Πίνακας 3-3 Κλάσεις Bluetooth

Οι πλειοψηφία των συσκευών που τροφοδοτούνται με μπαταρία είναι κλάσης 2. Ακόμα και αν επικοινωνούν με κάποια συσκευή κλάσης 1, είναι προφανές ότι η εμβέλεια της σύνδεσης ορίζεται από την συσκευή μικρότερης εμβέλειας.

### 3.3.3 Ρυθμός μετάδοσης

Ο ρυθμός μετάδοσης καθορίζεται από την έκδοση του Bluetooth. Η εμβέλεια λειτουργίας καθώς και ο ρυθμός απόδοσης εξαρτάται από τις συνθήκες διάδοσης, τα υλικά που παρεμβάλλονται, ρύθμιση των κεραιών καθώς και η κατάσταση της μπαταρίας. Ο ρυθμός μετάδοσης (data rate) βάσει της έκδοσης φαίνεται στον παρακάτω πίνακα.

ΕΚΔΟΣΗ	ΡΥΘΜΟΣ ΜΕΤΑΔΟΣΗΣ (Mbit/s)
1.2	1
2.0+EDR	3
3.0+HS	24
4.0	24

Πίνακας 3-4 Ρυθμοί μετάδοσης Bluetooth

### 3.4 GSM

Το GSM (παγκόσμιο σύστημα κινητών επικοινωνιών) είναι ένα πρότυπο που αναπτύχθηκε από το ευρωπαϊκό ινστιτούτο τηλεπικοινωνιών (ETSI) και περιγράφει πρωτόκολλα δεύτερης γενιάς (2G) κυψελοειδών δικτύων κινητής τηλεφωνίας.

#### 3.4.1 Κυψελοειδής δομή δικτύου

Η εμβέλεια ενός δικτύου GSM σε μία γεωγραφική περιοχή για να γίνει, η περιοχή αυτή διαμερίζεται σε μικρότερες περιοχές που λέγονται κυψέλες, οι οποίες εφάπτονται μεταξύ τους με κάθε κυψέλη να έχει και ένα σταθμό βάσης (Base Station), συνθέτοντας έτσι μια δομή κυψελών. Η δομή αυτή επαναλαμβάνεται όσες φορές χρειάζεται για την απαιτούμενη κάλυψη της μιας περιοχής κάνοντας επαναχρησιμοποίηση των συχνοτήτων. Με την μέθοδο αυτή αυξάνεται η χωρητικότητα του δικτύου αλλά πρέπει η ισχύς κάθε κυψέλης να είναι όση χρειάζεται ώστε να μην ξεπερνάει τα όρια της και να υπερχειλίζει άλλες κυψέλες της ίδιας δομής ενώ για να μην δημιουργείται ενδοκαναλική παρεμβολή σε γειτονικές κυψέλες η επαναχρησιμοποίηση συχνοτήτων πρέπει να σχεδιάζεται έτσι ώστε να απέχουν επαρκή απόσταση οι κυψέλες μιας δομής που έχουν την ίδια συχνότητα με τις κυψέλες μιας άλλης δομής. Η ενδοκαναλική παρεμβολή μειώνεται όσο αυξάνει ο αριθμός των κυψελών της δομής. Η ακτίνα κάθε κυψέλης σε αραιοκατοικημένες περιοχές είναι έως και 35Km ενώ σε πυκνοκατοικημένες περιοχές δεν ξεπερνά τα 300 μέτρα. Σε περιοχές με πολύ μεγάλη ζήτηση χωρητικότητας δικτύου όπως σε αστικά κέντρα, οι σταθμοί βάσης υπερφορτώνονται και έτσι υπάρχει ανάγκη για μεγαλύτερη χωρητικότητα του δικτύου. Έτσι για να επιτευχθεί αυτός ο σκοπός γίνεται διάσπαση των υπάρχοντων κυψελών σε μικρότερες, ενώ για αυτές χρησιμοποιούνται κεραιές μικρότερης ισχύος (macro bs - micro- bs - pico bs) όπως σε κτήρια, στο μετρό, Δημόσιους Οργανισμούς, οδικές αρτηρίες κτλ..

### 3.4.2 Αρχιτεκτονική

Ένα GSM δίκτυο χωρίζεται σε 3 βασικά μέρη:

1) Τον Κινητό Σταθμό (Mobile Station): Έχει οπωσδήποτε πομπό-δέκτη, κεραία, οθόνη και την κάρτα SIM. Η μέγιστη επιτρεπόμενη ισχύς εκπομπής στην Ευρώπη μιας κινητής μονάδας είναι στα 2 Watt ενώ σε Αυστραλία και Αμερική είναι 1,6W, οι τιμές αυτές καθορίστηκαν από την Διεθνή Επιτροπή για την προστασία από τη μη ιονίζουσα ακτινοβολία.

2) Το Βασικό Υποσύστημα Σταθμού (Base Station Subsystem): Το BSS διαχειρίζεται τις κλήσεις σε μια γεωγραφική περιοχή όπου καλύπτεται από ένα σύνολο κεραιών διαφόρων μεγεθών σε σειρά σαν αυτούς που βλέπουμε σε λόφους, τaráτσες πολυκατοικιών-εταιριών-σχολείων-οργανισμών κτλ. και κάθε τέτοια κεραία εξυπηρετεί και από μια κυψέλη. Το BSS χωρίζεται στο βασικό σταθμό πομπό-δέκτη Base Transceiver Station (BTS) και στο βασικό σταθμό ελέγχου Base Station Controller (BSC).

3) Το Υποσύστημα Δικτύου μεταγωγής (NNS- Network Switching Subsystem) που αποτελείται από: Το Κέντρο Διανομής (Mobile Switching Center), είναι υπεύθυνο για την διασύνδεση, τον έλεγχο και την δρομολόγηση εισερχόμενων/εξερχόμενων κλήσεων μεταξύ του δικτύου κινητής τηλεφωνίας και ενός άλλου δικτύου ή άλλων.

### 3.4.3 Πιστοποίηση και ασφάλεια

Ένας χρήστης για να μπορέσει να χρησιμοποιήσει το δίκτυο τότε το δίκτυο θα πρέπει πρώτα να τον πιστοποιήσει. Καταρχήν για να γίνει αυτό κάθε κινητό θα πρέπει να διαθέτει ένα κρυμμένο κλειδί το οποίο βρίσκεται συγκεκριμένα στην κάρτα SIM του και στο Κέντρο Πιστοποίησης (AC). Όταν ενεργοποιείται το κινητό, το Κέντρο Πιστοποίησης στέλνει ένα τυχαίο αριθμό στο κινητό και αυτόν τον αριθμό τον χρησιμοποιούν μαζί με το κρυμμένο κλειδί και με έναν κρυπτογραφημένο αλγόριθμο για την δημιουργία ενός νέου αριθμού. Το κινητό στέλνει πίσω στον κέντρο πιστοποίησης τον αριθμό αυτό και το κέντρο πιστοποίησης με την σειρά του ελέγχει αν είναι ίδιος με αυτόν που έφτιαξε. Αν ο αριθμός είναι ίδιος τότε ο χρήστης πιστοποιήθηκε ειδάλλως τον ειδοποιεί ότι διαδικασία εγγραφής στο δίκτυο ήταν ανεπιτυχής.

### 3.5 IEEE 802.15.4

Το IEEE 802.15.4 είναι ένα πρότυπο που ορίζει το φυσικό και το MAC (media access control) επίπεδο για ασύρματα δίκτυα προσωπικού χώρου μικρής ρυθμοαπόδοσης (low-rate wireless personal area networks, LR-WPANs). Διατηρείται από την IEEE 802.15, από την οποία ορίστηκε το 2003. Οι ορισμοί των επιπέδων είναι βασισμένοι στο μοντέλο OSI και παρόλο που μόνο τα κατώτερα επίπεδα ορίζονται, ο σκοπός είναι η αλληλεπίδραση με υψηλότερα επίπεδα.

Σημαντικά χαρακτηριστικά είναι:

1. Υποστήριξη απλής πρόσβασης αλλά και εγγυημένης πρόσβασης με χρονοσχισμές
2. Ταχύτητες μεταφοράς δεδομένων από 20 έως 250 Kbps
3. Διαφορετικές τοπολογίες όπως ο συμβατικός αστέρας αλλά και mesh network
4. Διευθυνσιοδότηση βασισμένη σε 16bits ή 64bits διευθύνσεις MAC
5. Αποφυγή συγκρούσεων με την χρησιμοποίηση του πρωτοκόλλου CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)
6. Υποστήριξη για μεταφορά δεδομένων με επιβεβαιώσεις αλλά και υποστήριξη δομής beaconing
7. Ανίχνευση ενέργειας για την επιλογή του καλύτερου καναλιού για μετάδοση
8. Ολοκληρωμένη υποστήριξη για ασφαλείς επικοινωνίες (Multilevel security)
9. Λειτουργίες διαχείρισης ενέργειας

Το 802.15.4 αποτελεί την βάση για τις προδιαγραφές: ZigBee, ISA100.11a, WirelessHART και άλλα, κάθε ένα από τα οποία επεκτείνει το πρότυπο αναπτύσσοντας τα υψηλότερα επίπεδα τα οποία δεν έχουν οριστεί από το 802.15.4. Εναλλακτικά, μπορεί να χρησιμοποιηθεί με το 6LoWPAN και τα τυπικά πρωτόκολλα του Internet για την σύνθεση ασύρματου ενσωματωμένου Internet.

### **3.5.1 ISA100.11a**

Το ISA100.11a αποτελεί ένα πρότυπο ασύρματης τεχνολογίας που αναπτύχθηκε από τον ISA (International Society of Automation) και ανακοινώθηκε το 2009. Αποτελεί ένα πρότυπο για την εφαρμογή ασύρματων δικτύων σε περιβάλλον βιομηχανικού αυτοματισμού.

### **3.5.2 WirelessHART**

Η τεχνολογία WirelessHART είναι μια τεχνολογία ασύρματου δικτύου αισθητήρων βασισμένη στο πρωτόκολλο HART (Highway Addressable Remote Transducer Protocol). Αξιοποιεί μια αρχιτεκτονική mesh δικτύου με ικανότητα συγχρονισμού, αυτο-οργάνωσης και αυτο-ίασης. Χρησιμοποιείται σε βιομηχανικές εφαρμογές ασύρματων δικτύων αισθητήρων.

### **3.5.3 6LoWPAN**

Το 6LoWPAN είναι ένα ακρωνύμιο για το IPv6 over Low power Wireless Personal Area Networks. Η ιδέα πάνω στην οποία χτίστηκε ήταν ότι το πρωτόκολλο του Internet θα πρέπει να μπορεί να εφαρμοστεί ακόμα και στις πιο μικρές συσκευές. Αποτελεί εφαρμογή της στοίβας IPv6 πάνω στο πρότυπο 802.15.4 ώστε οποιαδήποτε συσκευή να έχει την δυνατότητα σύνδεσης στο internet. Χρησιμοποιείται σε οικιακές εφαρμογές (αυτοματισμοί, ψυχαγωγία), αλλά και σε

περιβάλλοντα εργασίας όταν επιζητούμε σύνδεση στο internet με μικρή ρυθμοαπόδοση.

#### **3.5.4 MiWi**

Τα MiWi και MiWi P2P είναι ιδιόκτητα πρωτόκολλα σχεδιασμένα από την Microchip Technology. Είναι σχεδιασμένα για μικρούς ρυθμούς μετάδοσης δεδομένων και μικρές αποστάσεις. Χρησιμοποιούνται για δίκτυα περιορισμένου κόστους όπως αυτοματισμοί σπιτιών και κτηρίων, έλεγχος φωτισμού αλλά και παρακολούθηση και έλεγχο σε βιομηχανικό περιβάλλον.

#### **3.5.5 Zigbee**

Το Zigbee είναι ουσιαστικά μια σουίτα πρωτοκόλλων υψηλού επιπέδου βασισμένη στο 802.15.4. Αποτελεί μια από τις πιο δημοφιλείς λύσεις όταν αναφερόμαστε σε δίκτυα προσωπικού χώρου χαμηλής ισχύος, εξαιτίας της ικανότητας της να μεταφέρει δεδομένα σε πολύ μακρινές αποστάσεις χρησιμοποιώντας ως ενδιάμεσους κόμβους τις μονάδες, δημιουργώντας mesh networks.

Τα βασικά χαρακτηριστικά της τεχνολογίας Zigbee είναι τα παρακάτω:

1. Ρυθμός μετάδοσης έως 250 Kbps
2. Εμβέλεια μετάδοσης 10-100m
3. Ικανότητα δημιουργίας συμβατικών αλλά και mesh δικτύων
4. Επιπρόσθετες υπηρεσίες κρυπτογράφησης και ασφάλειας (στις ήδη υπάρχουσες του 802.15.4)
5. Χρήση του πρωτοκόλλου δρομολόγησης AODV (Ad hoc On-Demand Distance Vector) για την διαδικασία δρομολόγησης και προώθησης σε οποιοδήποτε κόμβο του δικτύου
6. Συσχέτιση και πιστοποίηση ώστε μόνο έγκυροι κόμβοι να συνδέονται στο δίκτυο
7. Zigbee Device Object (ZDO), που αποτελεί μια υπηρεσία του στρώματος εφαρμογής που παρέχει πολλές βασικές λειτουργίες αρχικοποίησης και διαχείρισης

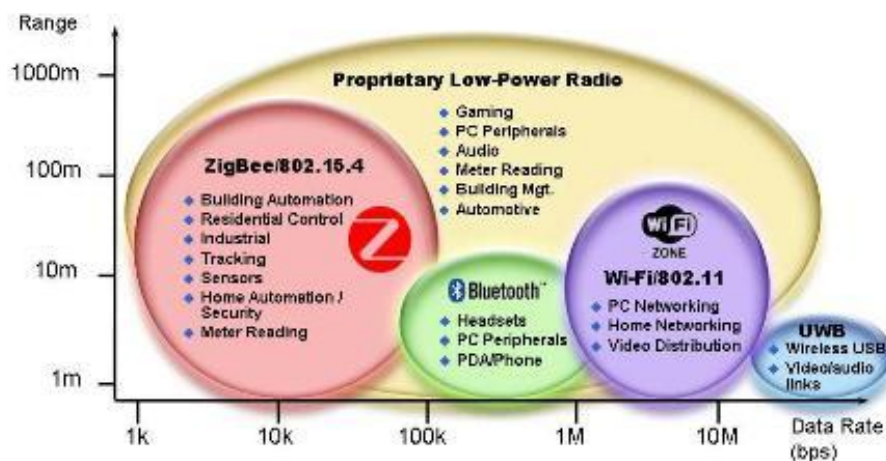
### **3.6 Σύγκριση επιλογών ασύρματης δικτύωσης**

Οι ασύρματες τεχνολογίες δικτύωσης που αναφέρθηκαν παραπάνω έχουν διαφορετικά χαρακτηριστικά, τα οποία καθορίζουν την χρησιμότητα σε συγκεκριμένες εφαρμογές. Στον παρακάτω πίνακα φαίνονται συνοπτικά τα βασικά χαρακτηριστικά λειτουργίας τους

	802.15.4	WiFi 802.11n	Bluetooth 4.0	GSM (4G)
Εύρος ζώνης	20-250 Kbps	300 Mbps	24Mbps	100Mbps
Μέγεθος δικτύου (κόμβοι)	$2^{16}$	255	7	1000+
Μέγιστη εμβέλεια	10-500m	70-250m	100m	200m-10km
Κατανάλωση	~2mW	~160mW (client)	~1mW	~180mW

Πίνακας 3-5 Σύγκριση ασύρματων τεχνολογιών

Στην Εικόνα 3-1 γίνεται σύγκριση των βασικών ασύρματων τεχνολογιών ως προς την ρυθμοαπόδοση (data rate) και την εμβέλεια τους.



Εικόνα 3-1

Σύμφωνα με τις απαιτήσεις της εφαρμογής που θέλουμε να υλοποιήσουμε θα στηριχτούμε στο πρότυπο 802.15.4. Οι απαιτήσεις της εφαρμογής μας είναι η χαμηλή κατανάλωση ισχύος και η ευελιξία ως προς τον αριθμό των κόμβων. Καθώς η υψηλή ρυθμοαπόδοση δεν κρίνεται αναγκαία, πρωτόκολλα όπως το WiFi και το GSM(4G) απορρίπτονται λόγω της υψηλής τους κατανάλωσης. Το Bluetooth επίσης θεωρείται μη ιδανικό λόγω των περιορισμών που τίθενται στη δομή και το μέγεθος του δικτύου.

	<b>Zigbee</b>	<b>6LoWPAN</b>
<b>Μεγ. εμβέλεια (εξωτ. χώρος)</b>	~500m	~200m
<b>Εύρος ζώνης</b>	250Kbps	200Kbps
<b>Μέγεθος δικτύου</b>	65536	100
<b>Μέση κατανάλωση</b>	~2mW	~2mW
<b>Δυνατότητα Multi-Hop</b>	ΝΑΙ	ΝΑΙ
<b>Κόστος πιστοποίησης</b>	Μέτριο	Χαμηλό
<b>Αποδοχή αναπτυξιακής κοινότητας</b>	Υψηλή	Μέτρια
<b>Διαλειτουργικότητα</b>	Υψηλή	Χαμηλή

Πίνακας 3-6 Σύγκριση τεχνολογιών 802.15.4

Όπως έχει αναφερθεί υπάρχουν πολλά πρωτόκολλα που στηρίζονται στο 802.15.4. Τα 2 επικρατέστερα προς υλοποίηση είναι το 6LoWPAN και το Zigbee. Τα βασικά τους χαρακτηριστικά φαίνονται στον παράπανω πίνακα. Στα επόμενα δύο κεφάλαια γίνεται εκτενέστερη ανάλυση για αυτά τα δύο πρωτόκολλα με σκόπο την τελική επιλογή που θα χρησιμοποιήσουμε στην εφαρμογή.

## 4 IPv6 6lowpan

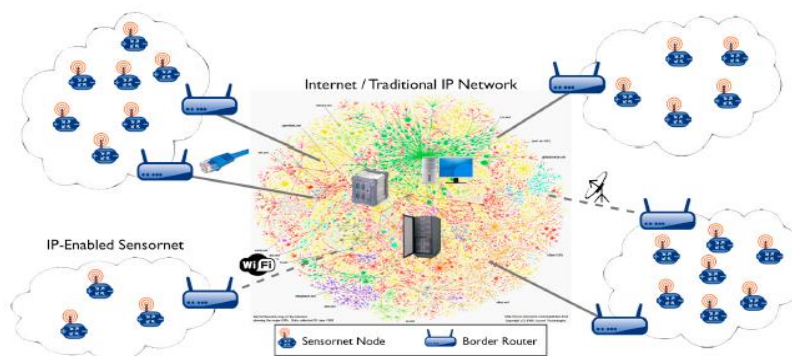
Πολλοί κορυφαίοι κατασκευαστές ασύρματων τεχνολογιών έχουν ενσωματώσει το IEEE 802.15.4, το οποίο ορίζει ασύρματη σύνδεση σε προσωπικά δίκτυα χαμηλής ισχύος ( Low power personal area networks-LoWPANs) και ήδη χρησιμοποιείται σε πληθώρα εφαρμογών. Οι δυνατότητες των LoWPANs είναι περιορισμένες σε σχέση με τα υπόλοιπα δίκτυα λόγω της χαμηλής κατανάλωσης που εισάγουν. Για αυτό το λόγο πολλές εταιρίες έχουν δημιουργήσει ασύρματα πρωτόκολλα χαμηλής κατανάλωσης τα οποία δεν έχουν συμβατότητα με τα κλασσικά πρωτόκολλα όπως το IP(proprietary), χωρίς κάποιον μετατροπέα, καθώς το πρωτόκολλο IP θεωρείται πολύ απαιτητικό σε μνήμη και εύρος ζώνης.

Το 6LoWPAN αλλάζει ριζικά το τοπίο με την εισαγωγή ενός στρώματος προσαρμογής μεταξύ του πρωτοκόλλου IP και του 802.15.4 για την αποτελεσματική μετάδοση πακέτων IPv6, μειώνοντας δραματικά την επικεφαλίδα IP. Το στρώμα προσαρμογής είναι ένα πρότυπο IETF το οποίο παρέχει συμπίεση της επικεφαλίδας ώστε να μειωθεί το overhead (επικεφαλίδα) μετάδοσης, τεμαχισμό για να υποστηρίξει την απαίτηση MTU του IPv6 και υποστήριξη του επιπέδου 2 του OSI για παράδοση πακέτων IPv6 μέσα πολλαπλούς κόμβους. Το 6LoWPAN επιτυγχάνει χαμηλό overhead εφαρμόζοντας βελτιστοποιήσεις ανάμεσα στα στρώματα, πιο συγκεκριμένα χρησιμοποιεί πληροφορίες από τα στρώματα ζεύξης δεδομένων και προσαρμογής ώστε να συμπίεσει τις επικεφαλίδες τους.

### 4.1 6LoWPAN Αρχιτεκτονική Δικτύου

Επικοινωνώντας εγγενώς με IP, τα LoWPAN δίκτυα συνδέονται με άλλα IP δίκτυα με την χρήση απλών δρομολογητών. Όπως φαίνεται και στην Εικόνα 4-1 τα δίκτυα χαμηλής κατανάλωσης λειτουργούν συνήθως στα άκρα του δικτύου, ως αυτόνομα δίκτυα. Συνδεσιμότητα με άλλα δίκτυα IP μπορεί να επιτευχθεί μέσα από οποιαδήποτε σύνδεση, συμπεριλαμβανομένων των Wi-Fi, GPRS, ή ακόμα και μέσω δορυφόρου. Επειδή το 6LoWPAN πρωτόκολλο λειτουργεί μόνο με IPv6, πολλές φορές χρειάζεται οι δρομολογητές που τα συνδέουν στο ευρύτερο διαδίκτυο να αλλάζουν το IPv6 ώστε να προσαρμόζεται στο IPv4.





Εικόνα 4-1 Αρχιτεκτονική δικτύου

Οι συνοριακοί δρομολογητές προωθούν τα πακέτα στο επίπεδο δικτύου και για αυτό το λόγο δεν διατηρούν την κατάσταση του στρώματος εφαρμογής. Σε άλλες αρχιτεκτονικές αυτοοργανομένων δικτύων (ad-hoc) απαιτούν πολύπλοκους δρομολογητές για την σύνδεση τους στο διαδίκτυο. Στην περίπτωση του 6LoWPAN όμως ο δρομολογητής που συνδέει το ακραίο δίκτυο με το διαδίκτυο, λόγω του IPv6, δεν χρειάζεται υλοποίηση για να προσαρμοστεί.

#### 4.2 IPv6 πάνω στο 802.15.4

Το πρωτόκολλο IPv6 είναι σχεδιασμένο ως ο διάδοχος του IPv4 και επιτρέπει στο διαδίκτυο να κλιμακώσει για πολλά χρόνια ακόμα. Για να ξεπεραστεί το πρόβλημα της έλλειψης διευθύνσεων και προβλέποντας ότι οι διασυνδεδεμένες συσκευές και όργανα θα υπερτερήσουν σε πλήθος τις συμβατικές υπολογιστικές συσκευές, το IPv6 επέκτεινε την διεύθυνση IP από 32 σε 128 bits. Λαμβάνοντας υπόψη την αύξηση του εύρους ζώνης, το IPv6 αυξάνει το ελάχιστο μήκος πακέτου από 576 σε 1280 bytes. Για την απλοποίηση των δρομολογητών και για να αυξηθεί η απόδοση, το IPv6 υλοποιεί τον κατακερματισμό των πακέτων στα άκρα του δικτύου και όχι στους ενδιάμεσους δρομολογητές. Η αποτελεσματικότητα του IPv6 περιλαμβάνει την αποστολή προς πολλούς (scoped multicast) ως δομικό στοιχείο του. Άλλα βασικά στοιχεία του IPv6 είναι η εύρεση γείτονα (ND), χρησιμοποίηση multicast για αναγνώριση διεύθυνσης, ανίχνευση διπλότυπης διεύθυνσης (DAD), και εύρεση δρομολογητή. Τέλος, διαμόρφωση διευθύνσεων από τους ίδιους τους κόμβους, επιτρέποντας τους να εκχωρήσουν στους εαυτούς του διευθύνσεις με νόημα.

Το IPv6 αντανάκλα την εξέλιξη στον τομέα της τεχνολογίας σύνδεσης στο διαδίκτυο. Το Ethernet έχει επικρατήσει ως κυρίαρχο μέσο σύνδεσης, και η απόδοση του έχει αυξηθεί σε πολύ υψηλό βαθμό. Οι τωρινές τεχνολογίες ασύρματης ζεύξης δεν

βρίσκονται πολύ πίσω σε απόδοση από το Ethernet, καθώς έχουν παρόμοιους ρυθμούς μετάδοσης. Αμφότερες οι δύο συνδέσεις, λειτουργούν στα πλαίσια υψηλής ισχύος και σε μηχανήματα υψηλών επιδόσεων. Από την άλλη οι τεχνολογίες WPAN λειτουργεί σε πολύ χαμηλή ισχύ. Το IEEE 802.15.4 σχεδιάστηκε συγκεκριμένα για εφαρμογές που απαιτούν μεγάλο χρόνο αυτονομίας και πολυάριθμους κόμβους χαμηλού κόστους. Αυτές οι προδιαγραφές περιορίζουν την επίδοση της ζεύξης των LoWPAN καθώς και των μικροελεγκτών που βρίσκονται σε κάθε κόμβο. Ο ρυθμός μετάδοσης φτάνει τα 250 Kbps, και το μέγεθος πακέτου τα 128 bytes, γι να εξασφαλίσει σχετικά χαμηλό ποσοστό σφάλματος μετάδοσης, καθώς η δυνατότητα αποθήκευσης και διαχείρισης των μικροελεγκτών είναι χαμηλή. Το 802.15.4 ορίζει σύντομες 16-bit διευθύνσεις, μαζί με την IEEE EUI-64 διεύθυνση, για να μειώσει το overhead και τις απαιτήσεις σε μνήμη. Η απόσταση επικοινωνίας είναι μικρή, της τάξεως των δεκάδων μέτρων, επειδή η ισχύς μετάδοσης αυξάνεται πολυωνυμικά συναρτήσει της απόστασης. Σε αντίθεση με άλλα τυπικά δίκτυα WPAN και WLAN, τα LoWPANs λειτουργούν μέσω πολλαπλών μεταδόσεων (Multiple hops). Τέλος οι μικροελεγκτές που συνδέονται συνήθως στους κόμβους, έχουν περίπου 8Kbytes RAM δεδομένων, και 64Kbytes ROM προγραμματισμού.

### 4.3 Στρώμα προσαρμογής 6LoWPAN

Η μορφή του 6LoWPAN καθορίζει πως γίνεται επικοινωνία IPv6 μέσω πακέτων 802.15.4 και προσδιορίζει τα βασικά στοιχεία του επιπέδου προσαρμογής. Τρία βασικά στοιχεία είναι:

Συμπίεση επικεφαλίδας. Οι επικεφαλίδες IPv6 συμπιέζονται υποθέτοντας χρησιμοποίηση κοινών στοιχείων. Το πεδίο της επικεφαλίδας παραλείπεται από ένα πακέτο όταν το στρώμα προσαρμογής μπορεί να αντλήσει πληροφορίες από το επίπεδο ζεύξης σε ένα πακέτο 802.15.4 ή βασισμένο σε απλές υποθέσεις βάσει κοινού περιεχομένου.

Κατακερματισμός. Τα πακέτα IPv6 χωρίζονται σε πολλαπλά πλαίσια επιπέδου ζεύξης, ώστε να καλυφθεί το ελάχιστο MTU του IPv6.

Πρώθηση στο δεύτερο στρώμα. Για την υποστήριξη πρώτωσης πακέτων IPv6, το στρώμα προσαρμογής μπορεί να μεταφέρει τις διευθύνσεις για τα άκρα ενός βήματος μετάδοσης IP (IP hop).

Η έννοια κλειδί που εφαρμόζεται σε όλο το στρώμα προσαρμογής 6LoWPAN είναι η χρήση χωρίς κατάσταση ή κοινού περιεχομένου συμπίεσης, με σκοπό να παραλείπονται κάποιες από τις επικεφαλίδες προσαρμογής, δικτύου και μεταφοράς (γίνεται συμπίεση και των τριών σε λίγα μόλις bytes). Μπορούμε να

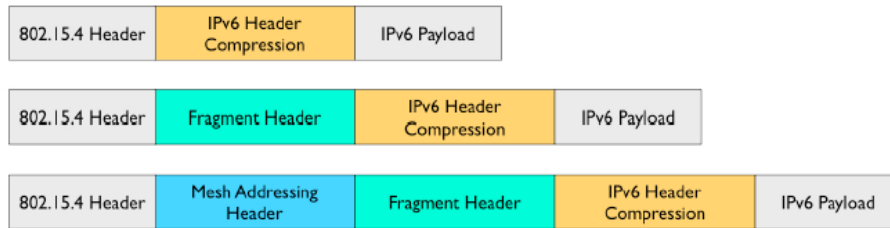
παρατηρήσουμε ότι είναι δυνατό να συμπιέσουμε πεδία της επικεφαλίδας σε λίγα bits όταν παρουσιάζουν πολλές κοινές τιμές, διατηρώντας μία τιμή διαφυγής όταν εμφανίζονται λιγότερο συνηθισμένες επικεφαλίδες. Οι κοινές τιμές προκύπτουν λόγω συχνής χρήσης ενός υποσυνόλου λειτουργιών του IPv6 (πχ UDP, TCP, ICMPv6 επικεφαλίδων) και απλών υποθέσεων κοινού περιεχομένου (πχ κοινό πρόθεμα ίδιου δικτύου).

Οι παραδοσιακές τεχνικές συμπίεσης επικεφαλίδων IP είναι stateful (δηλαδή λαμβάνουν υπόψη όλες τις προηγούμενες αιτήσεις) και γενικά επικεντρώνονται στην βελτιστοποίηση μεμονωμένων ροών μέσα από ένα εξαιρετικά περιορισμένο δίκτυο. Αυτές οι μέθοδοι προϋποθέτουν ότι ο κόμβος συμπίεστης και ο κόμβος αποσυμπιεστής, βρίσκονται σε απευθείας και αποκλειστική επικοινωνία και συμπιέζουν τις επικεφαλίδες στρώματος μεταφοράς και δικτύου μαζί. Βελτιστοποιούν ροές μεγάλης διάρκειας, αναγνωρίζοντας τα κοινά σημεία πακέτων σε μία ροή με την πάροδο του χρόνου, απαιτώντας από τους κόμβους επικοινωνίας αρχικά να στέλνουν τα πακέτα ασυμπιεστά. Αυτοί οι μέθοδοι συμπίεσης είναι ακατάλληλες για δίκτυα LoWPAN. Η κίνηση σε πολλές εφαρμογές LoWPAN αποτελείται συνήθως από σπάνιες ενδείξεις ή ειδοποιήσεις, παρά από ροές ορισμένες για μεγάλο χρονικό διάστημα. Η επικοινωνία μέσω πολλαπλών κόμβων απαιτεί συμπίεση και αποσυμπίεση σε κάθε βήμα. Πολλά πρωτόκολλα δρομολόγησης LoWPAN αποκτούν πληροφορίες για την ποικιλομορφία του δικτύου μέσω αναδρομολόγησης, η οποία όμως χρειάζεται γνώση προηγούμενων καταστάσεων επομένως μειώνει την αποτελεσματικότητα συμπίεσης. Αντίθετα η συμπίεση στο 6LoWPAN δεν απαιτεί γνώση της κατάστασης μίας συγκεκριμένη ροής και επιτρέπει στο πρωτόκολλο δρομολόγησης να λειτουργεί δυναμικά επιλέγοντας διαδρομές χωρίς να επηρεάζει την αποδοτικότητα της συμπίεσης.

#### **4.3.1 Ενσωμάτωση μορφής επικεφαλίδας**

Το 6LoWPAN χρησιμοποιεί στοίβαγμα των επικεφαλίδων, ώστε να κρατήσει διακριτές τις έννοιες κάθε επικεφαλίδας και να μπορεί να εκφράσει τις δυνατότητες του. Όπως και στο IPv6, έτσι και στο 6LoWPAN οι επικεφαλίδες επέκτασης εκφράζουν κάθε στοιχείο σε υποεπικεφαλίδες, πχ κατακερματισμό και συμπίεση. Η διευθυνσιοδότηση πλέγματος (mesh) υποστηρίζει προώθηση στο δεύτερο στρώμα και ο κατακερματισμός υποστηρίζει το ελάχιστο MTU του IPv6. Το 6LoWPAN αναγνωρίζει όλες τις μορφές των επικεφαλίδων χρησιμοποιώντας ένα πεδίο στην αρχή κάθε επικεφαλίδας. Ο τύπος 6LoWPAN Not-A-LoWPAN (NALP) του επιτρέπει να συνυπάρχει με άλλα πρωτόκολλα που λειτουργούν κατευθείαν στο επίπεδο της ζεύξης. Η στοίβα των επικεφαλίδων είναι εύκολο να αναλυθεί και επιτρέπει την παράλειψη επικεφαλίδων όταν αυτές είναι περιττές. Ομοίως, η επικεφαλίδα του δικτύου πλέγματος (mesh header) παραλείπεται όταν το πλαίσιο παραδίδεται μέσω μόνο μίας μετάβασης σε κόμβο, έτσι ώστε η διαδρομή πηγής και προορισμού

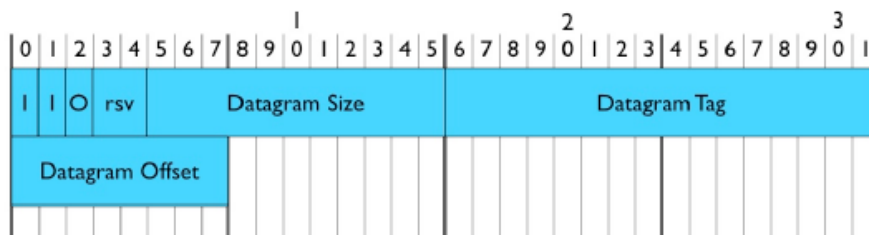
να ταυτίζονται με αυτές της επικεφαλίδας του στρώματος ζεύξης. Η Εικόνα 4-2 δείχνει τυπικές στοίβες επικεφαλίδων.



Εικόνα 4-2 Επικεφαλίδα 6LoWPAN

### 4.3.2 Επικεφαλίδα κατακερματισμού

Η επικεφαλίδα κατακερματισμού χρησιμοποιείται όταν το ωφέλιμο φορτίο είναι πολύ μεγάλο για να χωρέσει σε ένα και μόνο 802.15.4 πλαίσιο. Είναι ανάλογη με την επικεφαλίδα κατακερματισμού που χρησιμοποιεί το IEEE1394 και περιλαμβάνει τρία πεδία: μέγεθος πλαισίου, αναγνωριστικό πλαισίου (tag) και υπόλοιπο πλαισίου (offset). Το μέγεθος πλαισίου προσδιορίζει το συνολικό μέγεθος του αρχικού ωφέλιμου φορτίου Πριν τον κατακερματισμό και περιλαμβάνεται σε κάθε πακέτο-θραύσμα για να απλοποιήσει την εύρεση προσωρινής μνήμης στην μεριά του δέκτη όταν τα πακέτα παραδίδονται εκτός σειράς. Το αναγνωριστικό πλαισίου προσδιορίζει το σύνολο των πλαισίων-θραυσμάτων που αντιστοιχούν σε ένα ωφέλιμο φορτίο Και χρησιμοποιείται για να συγκεντρώνει πακέτα που αντιστοιχούν στο ίδιο ωφέλιμο φορτίο Το υπόλοιπο πλαισίου προσδιορίζει το υπόλοιπο του ωφέλιμου φορτίου πριν τον κατακερματισμό και μετριέται σε μονάδες 8-byte. Αν επιτρεπόταν αυθαίρετα το υπόλοιπο να μετράτε σε μονάδες του 1-byte τότε η επικεφαλίδα, λόγω απαίτησης ελάχιστου MTU 1280 bytes, θα ήταν 11 bits. Με 8-bytes μονάδα χρειαζόμαστε μόλις 8.



Εικόνα 4-3 Επικεφαλίδα κατακερματισμού

Η μορφή της επικεφαλίδας κατακερματισμού φαίνεται στην Εικόνα 4-3. Ο τύπος της επικεφαλίδας είναι μόνο 2 bits. Το τρίτο bit χρησιμοποιείται για να συμπιέσει το

υπόλοιπο του πλαισίου στο πρώτο θραύσμα και είναι πάντα 0. Η επικεφαλίδα κατακερματισμού είναι 4 bytes για το πρώτο θραύσμα και 5 bytes για κάθε επόμενο.

### 4.3.3 Επικεφαλίδα διευθυνσιοδότησης πλέγματος

Η επικεφαλίδα αυτή χρησιμοποιείται για να προωθήσει ωφέλιμα φορτία 6LoWPAN με μεταβάσεις μέσα από πολλούς κόμβους και υποστηρίζει προώθηση στρώματος δύο. Περιλαμβάνει τρία πεδία: όριο μεταβάσεων, διεύθυνση πηγής και διεύθυνση προορισμού. Το πεδίο του ορίου μεταβάσεων είναι ανάλογο του IPv6 και περιορίζει τον αριθμό μεταβάσεων από κόμβο σε κόμβο στην προώθηση του πλαισίου. Το πεδίο αυτό μειώνεται κατά 1 σε κάθε επόμενη μετάβαση και μόλις φτάσει στο 0, προφανώς δεν θα έχει παραδοθεί, απορρίπτεται. Οι διευθύνσεις πηγής και προορισμού ορίζουν τον αποστολέα και τον παραλήπτη κάθε πλαισίου. Και οι δύο διευθύνσεις είναι σε μορφή IEEE 802.15.4 και μπορούν είτε να είναι σύντομες είτε εκτεταμένες.



Εικόνα 4-4 Επικεφαλίδα διευθυνσιοδότησης πλέγματος

Η μορφή της επικεφαλίδας διευθυνσιοδότησης πλέγματος φαίνεται στην Εικόνα 4-4. Ο τύπος της επικεφαλίδας είναι πάλι 2 bits. Το τρίτο και τέταρτο bit υποδεικνύουν ποια λειτουργία διευθυνσιοδότησης να χρησιμοποιηθεί από την πηγή και τον προορισμό. Τα υπόλοιπα bits περιλαμβάνουν το όριο μεταβάσεων και τις διευθύνσεις. Το συνολικό μήκος της επικεφαλίδας δεν είναι σταθερό και κυμαίνεται από 5 μέχρι 17 bytes ανάλογα με την λειτουργία διευθυνσιοδότησης.

### 4.3.4 Συμπύεση επικεφαλίδας IPv6 κατά RFC4944

Το RFC4944 καθορίζει το HC1, ένα σχήμα συμπύεσης χωρίς την ανάγκη προηγούμενης κατάστασης, βελτιστοποιημένο για τοπική επικοινωνία IPv6. Το HC1 προσδιορίζεται από ένα κωδικοποιημένο byte ακολουθούμενο από την συμπιεσμένη επικεφαλίδα αποστολής IPv6 και λειτουργεί στα πεδία των επικεφαλίδων των ανώτερων στρωμάτων. Το 6LoWPAN παραλείπει κάποια πεδία υποθέτοντας κοινές παραμέτρους. Για παράδειγμα, συμπιέζει το 64-bit πρόθεμα

δικτύου και για τις δύο διευθύνσεις πηγής και προορισμού σε ένα και μόνο bit όταν και οι δύο ανήκουν στο ίδιο τοπικό δίκτυο. Επίσης συμπιέζει το πεδίο της επόμενης επικεφαλίδας σε 2 bits όταν το πακέτο χρησιμοποιεί UDP, TCP ή ICMPv6. Επιπλέον συμπιέζει την κλάση κίνησης (traffic class) και την ετικέτα ροής (flow label) σε ένα ενιαίο κομμάτι όταν οι τιμές και των δύο είναι μηδέν. Κάθε συμπιεσμένη μορφή έχει δεσμευμένες παραμέτρους που δείχνουν ότι τα πεδία μεταφέρονται σε σειρά προβλέποντας κάποια περίπτωση που δεν ταιριάζει. Το 6LoWPAN παραλείπει και άλλα πεδία αξιοποιώντας περιττές πληροφορίες μεταξύ στρωμάτων. Μπορεί να αντλήσει το μήκος του ωφέλιμου φορτίου από το πλαίσιο 802.15.4 ή από την επικεφαλίδα κατακερματισμού. Το 64-bit αναγνωριστικό διεπαφής (IID) για τις δύο διευθύνσεις, παραλείπεται αν η διεύθυνση προορισμού μπορεί να προκύψει από την διεύθυνση του στρώματος ζεύξης του 802.15.4 ή από την επικεφαλίδα διευθυνσιοδότησης πλέγματος. Τέλος, το 6LoWPAN πάντα παραλείπει την έκδοση καθώς επικοινωνεί πάντα με IPv6.



Εικόνα 4-5 Κωδικοποίηση HC1

Η κωδικοποίηση HC1 φαίνεται στην Εικόνα 4-5. το πρώτο byte είναι αυτό της αποστολής και υποδεικνύει την χρήση του HC1. Ακολουθάνε 8 bits που δείχνουν πως έχουν συμπιεστεί τα πεδία του IPv6. Για κάθε διεύθυνση, χρησιμοποιείται ένα bit για να υποδείξει εάν το πρόθεμα του IPv6 είναι τοπικό και παραλείπεται και ένα bit για να δείξει αν το αναγνωριστικό διεπαφής μπορεί να προκύψει από την διεύθυνση ζεύξης του 802.15.4. Το TF bit υποδεικνύει αν η κλάση κίνησης και η ετικέτα ροής είναι και τα δύο 0 άρα παραλείπονται. Τα δύο επόμενα Next Header bits δείχνουν αν έχουμε UDP, TCP ή ICMP και εάν είναι συμπιεσμένο ή μεταφέρεται σειριακά. Το HC2 bit δείχνει αν η επόμενη επικεφαλίδα είναι συμπιεσμένη χρησιμοποιώντας HC2. Σε πλήρη συμπίεση η κωδικοποίηση HC1 περιορίζει την επικεφαλίδα IPv6 στα 3 bytes, συμπεριλαμβανομένης της επικεφαλίδας αποστολής. Το πεδίο του ορίου μεταβάσεων είναι το μονό που δεν συμπιέζεται και μεταφέρεται ολόκληρο.

#### 4.3.5 Συμπίεση επικεφαλίδας UDP κατά RFC4944

Το RFC4944 χρησιμοποιεί τεχνικές συμπίεσης χωρίς μνήμη για να μειώσει την επιβάρυνση της επικεφαλίδας UDP. Όταν ορίζεται το HC2 bit στην κωδικοποίηση HC1 κατευθείαν συμπεριλαμβάνονται επιπλέον 8 bits ακολουθώντας τα bits κωδικοποίησης του HC1 που καθορίζουν πως θα συμπιεστεί η επικεφαλίδα UDP.

Για να συμπιεστούν αποδοτικά οι θύρες του UDP, το 6LoWPAN εισάγει μία πληθώρα γνωστών θυρών (61616-61631). Όταν η θύρα UDP συμπέσει με κάποια από αυτές τις θύρες τότε τα πρώτα 12 bits μπορούν να παραλειφθούν. Αν και οι δύο θύρες, πηγής και προορισμού συμπέσουν στις παραπάνω τότε το πεδίο που καθορίζει τις θύρες συμπιέζεται σε ένα μονό byte. Το HC2 επιτρέπει επίσης την παράλειψη του μήκους UDP αφού μπορεί να προκύψει από το πεδίο του ωφέλιμου φορτίου του IPv6. Η κωδικοποίηση φαίνεται στην Εικόνα 4-6.

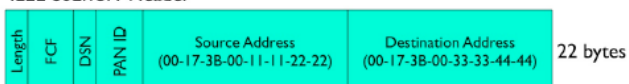


Εικόνα 4-6 Κωδικοποίηση HC2

### 4.3.6 Παραδείγματα συμπίεσης

Τυπικές διαμορφώσεις επικεφαλίδας που χρησιμοποιούν κωδικοποίηση HC1 και HC2 φαίνονται στην Εικόνα 4-7. Η πιο αποδοτική συμπίεση προκύπτει όταν έχουμε επικοινωνία σε τοπικό δίκτυο με αποστολή σε μοναδικό παραλήπτη, όπου τα HC1 και HC2 μπορούν να συμπιέσουν αθροιστικά τις επικεφαλίδες UDP/IPv6 σε 7 bytes. Η έκδοση, η κλάση κίνησης, η ετικέτα ροής, το μήκος ωφέλιμου φορτίου, επόμενη επικεφαλίδα (Next Header) και τα προθέματα του τοπικού δικτύου για τις διευθύνσεις πηγής και προορισμό. Η κατάληξη για τις δύο διευθύνσεις IPv6 εκπίπτει από την επικεφαλίδα 802.15.4.

IEEE 802.15.4 Header



Compressed UDP/IPv6 Header (fe80::0217:3b00:1111:2222 → fe80::0217:3b00:3333:4444)



Compressed UDP/IPv6 Header (fe80::0217:3b00:1111:2222 → ff02::1)



Compressed UDP/IPv6 Header (2001:5a8:4:3721:0217:3b00:1111:2222 → 2001:4860:b002::68)



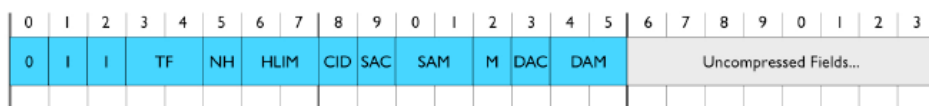
Εικόνα 4-7 Παραδείγματα συμπίεσης

Ωστόσο, το RFC4944 δεν συμπιέζει αποτελεσματικά τις επικεφαλίδες όταν επικοινωνεί εξωτερικά του τοπικού δικτύου ή όταν χρησιμοποιεί την αποστολή προς πολλούς (multicast). Κάθε πρόθεμα εκτός του τοπικού πρέπει να μεταφερθεί όπως είναι. Κάθε επίθεμα πρέπει να είναι τουλάχιστον 64-bits ακόμα και αν μπορεί να προκύψει από την σύντομη διεύθυνση του 802.15.4. Όπως φαίνεται στην Εικόνα 4-7, το HC1/HC2 μπορεί να συμπιέσει μία τοπική αποστολή προς πολλούς σε 23 bytes κατά το καλύτερο σενάριο. Όταν επικοινωνεί με κόμβους εκτός LoWPAN, το πρόθεμα της διεύθυνσης πηγής IPv6 ολόκληρη η διεύθυνση IPv6 πρέπει να παραμείνουν ασυμπιεστά.

#### 4.3.7 Βελτιωμένη συμπίεση επικεφαλίδας UDP/IPv6

Για να παρέχει καλύτερη συμπίεση σε ένα ευρύτερο φάσμα σεναρίων, το 6LoWPAN έχει προτυποποιήσει μία βελτιωμένη μορφή κωδικοποίησης συμπίεσης, το HC. Το πρότυπο αυτό καθορίζει μία καινούργια κωδικοποίησης επικεφαλίδας IPv6, το IPHC. Το πρότυπο αυτό επιτρέπει στις επικεφαλίδες Traffic Class και Flow Label να συμπιέζονται μεμονωμένα, συμπίεση της επικεφαλίδας Hop Limit όταν έχουν κοινές τιμές, και χρησιμοποίησης του κοινού περιεχομένου για την παράλειψη του προθέματος των διευθύνσεων IPv6, καθώς και υποστήριξη διευθύνσεων multicast που χρησιμοποιούνται συνήθως για IPv6 ND και SLAAC.

Το πλαίσιο (context) ενεργεί ως μία κοινή κατάσταση για όλους του κόμβους μέσα σε ένα LoWPAN. Ένα ενιαίο πλαίσιο κατέχει ένα ενιαίο πρόθεμα. Το IPHC αναγνωρίζει το πλαίσιο χρησιμοποιώντας ένα δείκτη 4-bit, επιτρέποντας του να υποστηρίξει μέχρι και 16 διαφορετικά πλαίσια ταυτόχρονα σε ένα LoWPAN. Όταν μία διεύθυνση IPv6 ταυτίζεται με το αποθηκευμένο πρόθεμα ενός πλαισίου, το IPHC συμπιέζει το πρόθεμα της διεύθυνσης στο 4-bit αναγνωριστικό του πλαισίου. Αξίζει να σημειωθεί ότι τα προθέματα των πλαισίων δεν περιορίζονται στα προθέματα που παίρνουν εντός ενός LoWPAN αλλά μπορεί να πάρουν οποιαδήποτε αυθαίρετη τιμή. Ως αποτέλεσμα, κοινά πλαίσια μπορούν να διαμορφωθούν έτσι ώστε οι κόμβοι του LoWPAN να μπορούν να συμπιέσουν το πρόθεμα του πλαισίου και στην πηγή και στον προορισμό, ακόμα και αν αυτά επικοινωνούν με κόμβους εξωτερικά του LoWPAN.



Εικόνα 4-8 Βελτιωμένη κωδικοποίηση

Η βελτιωμένη κωδικοποίησης συμπίεσης επικεφαλίδας φαίνεται στην Εικόνα 4-8. Τα πρώτα 3 bits 011 καθορίζουν τον τύπο της επικεφαλίδας και την χρήση του IPHC. Τα TF bits υποδεικνύουν αν τα πεδία Traffic Class και/ή Flow Label είναι



συμπιεσμένα. Τα HLIM bits δείχνει αν το Hop Limit παίρνουν την τιμή 1 ή 255 και συμπιέζονται, ή μεταφέρονται ασυμπιεστα.

Τα bits 8-15 της κωδικοποίησης IHPC αναφέρονται στις μεθόδους συμπίεσης που χρησιμοποιούνται για τις διευθύνσεις πηγής και προορισμού. Όταν το Context Identifier (CID) bit έχει οριστεί μηδέν, τότε διαλέγεται το προεπιλεγμένο πλαίσιο συμπίεσης για τις δύο διευθύνσεις. Αυτή η λειτουργία επιτελείται συνήθως όταν και οι δύο διευθύνσεις βρίσκονται μέσα στο ίδιο τοπικό δίκτυο. Όταν το CID bit είναι ορισμένο στο 1, τότε προσθέτονται στην επικεφαλίδα δύο επιπλέον πεδία τα οποία αναφέρουν ποιο πλαίσιο χρησιμοποιείται για την διεύθυνση πηγής και προορισμού αντίστοιχα.

Το πεδίο συμπίεσης διεύθυνσης πηγής (SAC) υποδεικνύει αν χρησιμοποιείται συμπίεση με μνήμη ή χωρίς, για τοπική επικοινωνία ή ευρύτερη επικοινωνία αντίστοιχα. Το πεδίο λειτουργίας της διεύθυνσης πηγής (SAM) δείχνει αν όλο το μήκος της διεύθυνσης μεταφέρεται στην επικεφαλίδα ή αν παραλείπονται 16/64 bits. Όταν το SAC bit είναι ορισμένο ένα και το πρόθεμα διεύθυνσης πηγής παραλείπεται, χρησιμοποιείται το προσδιορισμένο πλαίσιο για την αποκατάσταση αυτών των bits.

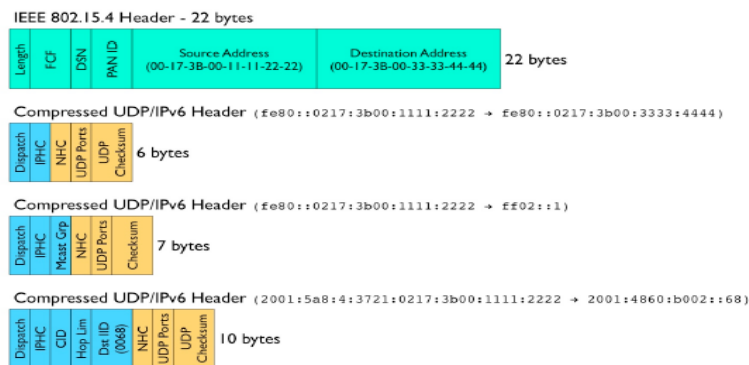
Το πεδίο Multicast ορίζει αν η διεύθυνση προορισμού είναι μοναδική ή αν είναι αποστολή προς πολλούς. Όταν είναι μοναδική τα bits DAC και DAM είναι ανάλογα των SAC και SAM. Όταν έχουμε αποστολή προς πολλούς, τότε το DAM bit υποδεικνύει την μορφή multicast συμπίεσης.

Το HC ορίζει ένα νέο πλαίσιο αυθαίρετης συμπίεσης επόμενων επικεφαλίδων, το NHC. Το HC2 κατά RFC4944 μπορεί να συμπιέσει επικεφαλίδες μόνο UDP, TCP και ICMPv6. Αντί αυτού η επικεφαλίδα NHC ορίζει μια καινούργια μεταβλητή-πεδίο το Next Header Identifier, αφήνοντας ανοικτό για μελλοντικούς ορισμούς συμπίεσης αυθαίρετων επικεφαλίδων.

Το HC καθορίζει αρχικά μία κωδικοποίηση συμπίεσης για τις επικεφαλίδες UDP, παρόμοια με αυτήν που ορίζεται στο RFC4944. Όπως και στο RFC4944, το HC χρησιμοποιεί το ίδιο εύρος θυρών (61616-61631) για να συμπιέσει αποτελεσματικά τις θύρες UDP βέλτιστα σε 4 bits. Ωστόσο, το HC δεν παρέχει επιλογή για μεταφορά του ωφέλιμου φορτίου ασυμπιεστο, αφού μπορεί πάντα να εκπίπτει από την επικεφαλίδα IPv6. Τέλος, το HC επιτρέπει την παράλειψη του UDP Checksum όταν ένα η ακεραιότητα ενός μηνύματος από υψηλότερο στρώμα καλύπτει τις κατάλληλες πληροφορίες. Αυτό έχει ως αποτέλεσμα την συμπίεση της επικεφαλίδας UDP σε 2 bytes στην καλύτερη περίπτωση.

### 4.3.8 Βελτιωμένα παραδείγματα συμπίεσης επικεφαλίδων UDP/IPv6

Οι τυπικές διαμορφώσεις που χρησιμοποιούν IPHC και NHC φαίνονται στην Εικόνα 4-9. Όπως και με το RFC4944, η καλύτερη περίπτωση για απόδοση συμπίεσης συμβαίνει σε επικοινωνία σε τοπικό δίκτυο με αποστολή προς έναν προορισμό (unicast) – το IPHC και το NHC μπορούν να συμπίεσουν την επικεφαλίδα UDP/IPv6 σε 6 bytes. Τα προθέματα κίνησης, ετικέτα ροής, μήκος ωφέλιμου φορτίου, επόμενης επικεφαλίδας, όριο μεταβάσεων και τοπικού συνδέσμου παραλείπονται. Τα προθέματα για τις διευθύνσεις IPv6 πηγής και προορισμού προέρχονται από την επικεφαλίδα IEEE 802.15.4.



Εικόνα 4-9 Παραδείγματα βελτιωμένης συμπίεσης

Οι βελτιώσεις που έγιναν στο IPHC γίνονται εμφανείς σε επικοινωνία πολλαπλής διανομής (multicast) και επικοινωνία εκτός τοπικού δικτύου. Όπως φαίνεται στην Εικόνα 4-9, το IPHC μπορεί να συμπίεσει γνωστές διευθύνσεις multicast σε 7 bytes (αντίθετα με το HC1 23 bytes). Οι γνωστές διευθύνσεις multicast περιορίζουν το αναγνωριστικό τους μόνο στα τελευταία bytes, κάτι που εκμεταλλεύεται το IPHC. Σε επικοινωνία εκτός τοπικού δικτύου, το IPHC μπορεί να συμπίεσει μία επικεφαλίδα UDP/IPv6 σε 9 ή 10 bytes (αντίθετα το HC1 31 bytes). Οι διεύθυνση αποστολής μπορεί να συμπιεστεί αν εξάγεται από την επικεφαλίδα του IEEE 802.15.4.

## 4.4 IPv6/6LoWPAN αρχιτεκτονική

Το πρότυπο 6LoWPAN καθορίζει πως αναπαριστάται ο κατακερματισμός, η συμπίεση και η προώθηση στο επίπεδο δύο του OSI σε ένα πλαίσιο 802.15.4. Οι εξαρτήσεις του 6LoWPAN που ορίζονται σε συγκεκριμένες ενέργειες στο 802.15.4 MAC είναι ελάχιστες, υποστηρίζοντας ουσιαστικά κάθε πρωτόκολλο MAC που παρέχει η μορφή του πλαισίου 802.15.4. ομοίως, η μορφή του 6LoWPAN δεν διευκρινίζει πως οι δυνατότητες του IPv6, όπως το ND και το SAA, ενσωματώνονται για να διαμορφώσουν το LoWPAN να έχει συνοχή με το στρώμα προσαρμογής.

#### 4.4.1 IEEE 802.15.4 στη πράξη

Το IEEE 802.15.4 παρουσιάζει αρκετά πρακτικά ζητήματα που έχουν σημαντικές αρχιτεκτονικές επιπτώσεις, πέρα από το στρώμα 6LoWPAN. Ενώ στις συμβατικές ρυθμίσεις WPAN, ο χρήστης τυπικά ρυθμίζει την θέση της συσκευής και του host έτσι ώστε η σύνδεση μεταξύ τους να είναι επαρκής, σε ένα κλασικό LoWPAN οι ρυθμίσεις σε ένα δίκτυο με πολλές συσκευές είναι ενσωματωμένο σε συγκεκριμένα ουσιαστικά σημεία. Τα πρωτόκολλα δικτύου πρέπει να αντιμετωπίσουν τα έκτακτα συμβάντα που εμφανίζονται. Η δρομολόγηση πολλών μεταβάσεων (multihop) αυξάνει την εμβέλεια και βοηθά στην αποφυγή εμποδίων. Έτσι, ένα LoWPAN δίκτυο δεν είναι συνήθως απλής εκπομπής. Επιπλέον, η ποιότητα σύνδεσης μεταξύ ενός ζευγαριού κόμβων είναι συχνά πολύπλοκη και χρονικά μεταβαλλόμενη λόγω περιβαλλοντικών παραγόντων. Τα σχήματα αναμετάδοσης hop-by-hop βοηθάνε την μετάδοση μεταξύ συνδέσεων 802.15.4, που συνήθως έχει απώλειες, να γίνει βιώσιμη, αλλά από μόνη της δεν είναι αρκετή. Συνδέσεις που χαρακτηρίζονται ως καλές – έχουν 90% επιτυχία αποστολής για παράδειγμα- συχνά έχουν «ξεσπάσματα» απωλειών που οφείλονται σε αλλαγές στο επίπεδο θορύβου και παρασιτικές παρεμβολές. Η δρομολόγηση μπορεί να αντιμετωπίσει τέτοια «ξεσπάσματα» όταν προωθεί πακέτα διαλέγοντας εναλλακτική διαδρομή. Στην πραγματικότητα, η δρομολόγηση εκμεταλλεύεται την ποικιλομορφία του δέκτη διαλέγοντας δυναμικά κάθε επόμενο υποψήφιο κόμβο για μετάδοση. Για να αντιμετωπίσει τις προκλήσεις των συνδέσεων, το στρώμα δικτύου απαιτεί επιπλέον ορατότητα σε πιο λεπτομερή συμπεριφορά κάθε σύνδεσης για να χτίσει και να διατηρήσει αποτελεσματικές δομές δρομολόγησης.

Πολλές εφαρμογές LoWPAN έχουν σημαντική κινητικότητα συσκευών μέσα στο δίκτυο, προκαλώντας αύξηση σε χρονικά μεταβαλλόμενες σχέσεις συνδεσιμότητας, όπως και εναλλαγές που προκύπτουν από τους εναλλασσόμενους περιβαλλοντικούς παράγοντες. Για παράδειγμα, η παρακολούθηση πακέτων μπορεί να περιλαμβάνει πολλές συσκευές να μετακινούνται σε σχέση με έναν αριθμό σταθερών συσκευών. Αυτό δεν σημαίνει απαραίτητα και φορητότητα της IP με την κλασική έννοια, καθώς οι συσκευές μπορεί να παραμένουν παρά την κινητικότητα εντός του τοπικού τους δικτύου και να παραμένουν συνδεδεμένα σε αυτό. Εν τούτοις, τέτοιες αλλαγές απαιτούν από την τοπολογία της δρομολόγησης να προσαρμόζεται σε κάθε θέμα συνδεσιμότητας που προκύπτει.

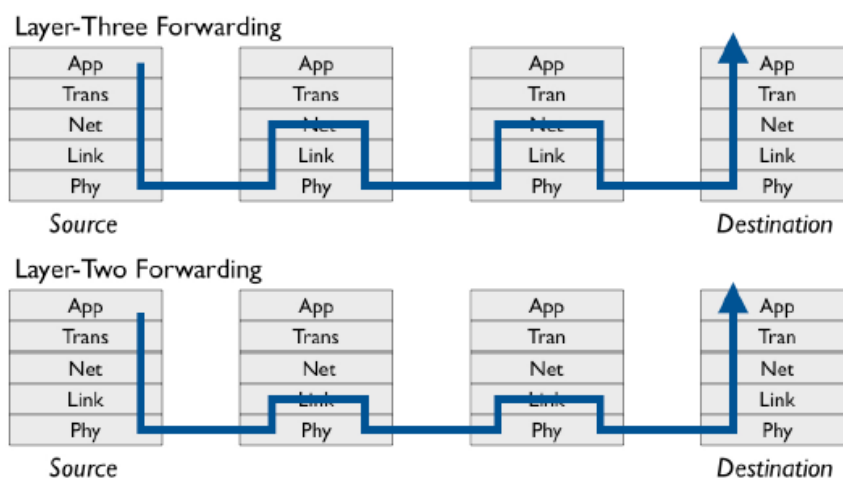
Το 802.15.4 ορίζει μόνο ένα περιορισμένο σύνολο μηχανισμών διαχείρισης ενέργειας για τις συσκευές στα άκρα του δικτύου και κανέναν για τις συσκευές προώθησης. Συνεπώς, οι περισσότερες εμπορικές εφαρμογές και τα βιομηχανικά πρότυπα που στηρίζονται στο 802.15.4 καθορίζουν τους μηχανισμούς διαχείρισης ενέργειας κατά τον ορισμό των πρωτόκολλων δρομολόγησης. Για να διατηρηθούν τα επίπεδα ενέργειας χαμηλά, οι κόμβοι πρέπει να καθορίσουν τον ενεργό χρόνο μετάδοσης, κάτι που απαιτεί αμφότερος πομπό και δέκτη να συγχρονιστούν για το

πότε και πώς θα επικοινωνήσουν. Συνήθεις μηχανισμοί για αυτό περιλαμβάνουν τεχνικές δειγματοληψίας, ή τεχνικές προγραμματισμού, που περιλαμβάνουν συγχρονισμό του χρόνου μεταξύ κόμβων. Το 6LoWPAN, μέχρι τώρα, αποφεύγει την απαίτηση συγκεκριμένων χαρακτηριστικών MAC. Όταν εξαρτήματα IPv6 προσαρμόζονται για να λειτουργήσουν σε συνδέσεις 802.15.4, θα πρέπει να δοθεί σημασία στις εξαρτήσεις με το συγκεκριμένο υποκείμενο πρωτόκολλο MAC.

#### 4.4.2 Πλέγμα «χαμηλά» ή δρομολόγηση «ψηλά»

Δύο σημαντικά αρχιτεκτονικά ζητήματα για το IPv6 όταν λειτουργεί σε LoWPAN είναι πως οι παράγοντες επιπέδου ζεύξης ενημερώνουν την δρομολόγηση και σε ποιο επίπεδο συμβαίνει η προώθηση των πακέτων μέσα στο LoWPAN.

Παραδοσιακά, η δρομολόγηση IP επιτελείται στο επίπεδο δικτύου με τρόπο ανεξάρτητο των υποκείμενων συνδέσεων που εφαρμόζουν τις ανεξάρτητες μεταβάσεις. Το 6LoWPAN, ως στρώμα προσαρμογής μεταξύ του επιπέδου ζεύξης και δικτύου (2 και 3 αντίστοιχα), μπορεί να υποστηρίξει δρομολόγηση σε οποιοδήποτε από τα δύο επίπεδα. Η Εικόνα 4-10 δείχνει την διαφορά στην επεξεργασία των πακέτων μεταξύ των δύο προσεγγίσεων.



Εικόνα 4-10 Δρομολόγηση στο επίπεδο δικτύου και ζεύξης

Σε ένα δίκτυο πλέγμα κατά την οργάνωση, η στοίβα δικτύου δεν εκτελεί καμία δρομολόγηση IP μέσα στο LoWPAN, αν'ταυτού το στρώμα προσαρμογής επιδιώκει να καλύψει την πλήρους εκπομπής στο φυσικό επίπεδο δρομολογώντας με διαφάνεια και προωθώντας πλαίσια εσωτερικά του LoWPAN. Με την μίμηση πλήρους εκπομπής (broadcast), δυνητικά παρέχει συμβατότητα με τα πρωτόκολλα IPv6 που αναμένουν τέτοια συμπεριφορά κατά την επικοινωνία. Οι τοπολογίες πλέγματος απαιτούν προώθηση με πολλαπλές μεταβάσεις, και η τοπική ζεύξη multicast πρέπει να παραδώσει πακέτα σε όλους τους κόμβους σε ολόκληρο το LoWPAN. Πολλοί μηχανισμοί υπάρχουν για το σχηματισμό, διατήρηση και διάγνωση

δρομολόγησης IP πρέπει να ξαναδημιουργηθούν στο επίπεδο ζεύξης για να λειτουργήσει αξιόπιστα η «πλεγματοποίηση».

Εναλλακτικά, η δρομολόγηση «ψηλά» εκτελεί δρομολόγηση στο στρώμα IP, και κάθε κόμβος εξυπηρετεί σαν IP δρομολογητής. Αντίθετα με το πλέγμα «χαμηλά», η δρομολόγηση «ψηλά» υποστηρίζει μηχανισμούς προώθησης στο στρώμα δικτύου μέσα στο LoWPAN που μπορούν να χρησιμοποιήσουν τις δυνατότητες που καθορίζει το IP για το στρώμα δικτύου, όπως δρομολόγηση IPv6 και ICMPv6 για διαμόρφωση και διαχείριση. Επίσης επιτρέπει σε πρωτόκολλα δρομολόγησης IP να συνεργάζονται με περισσότερες τεχνολογίες ζεύξης, επιτρέποντας καλύτερη ενσωμάτωση σε περισσότερα δίκτυα. Θέματα δρομολόγησης στο στρώμα ζεύξης ή στρώμα δικτύου δεν ισχύουν μόνο για το 6LoWPAN, αλλά προκύπτουν και σε άλλες τεχνολογίες όπως το Frame Relay, Asynchronous Transfer Mode (ATM), switched Ethernet και 802.11 σε λειτουργία πλέγματος. Για παράδειγμα, παρόμοιες προκλήσεις έχουν εμφανιστεί με την IP σε ATM, στην οποία ανεξάρτητη δρομολόγηση επιπέδου ζεύξης καθιστά δύσκολή την βελτιστοποίηση της διαδρομής IP από άκρη σε άκρη καθώς δύο πρωτόκολλα που δεν επικοινωνούν μεταξύ τους, λειτουργούν σε διαφορετικά στρώματα. Επιπλέον, δύο ανεξάρτητα στρώματα δρομολόγησης μπορεί να έχουν ακούσιες αλληλεπιδράσεις μεταξύ τους, ειδικά όταν επεμβαίνουν σε αλλαγές στην κατάσταση ζεύξης. Αξίζει επίσης να αναφερθεί ότι μία πολυστρωματική αρχιτεκτονική δρομολόγησης είναι πρόκληση όσον αναφορά την βέλτιστη διαδρομή και την ανάκτηση.

#### **4.4.3 Διευθυνσιοδότηση και αυτόματη διαμόρφωση**

Χρησιμοποιώντας αυτόματη διαμόρφωση διεύθυνσης πηγής (SAA), κάθε εξυπηρετητής δημιουργεί μία τοπική διεύθυνση IPv6 αποκλειστικής μετάδοσης (unicast) από την διεύθυνση IEEE EUI-64 ή την 16-bit διεύθυνση του, ή και από τα δύο. Στο πλέγμα «χαμηλά», για την επικοινωνία στο εσωτερικό του LoWPAN (ακόμα και με πολλαπλές μεταβάσεις) αρκεί η τοπική διεύθυνση ζεύξης, ενώ χρειάζεται μία δρομολογημένη διεύθυνση για επικοινωνία εκτός του τοπικού δικτύου. Αντίθετα όταν η δρομολόγηση γίνεται «ψηλά» η τοπική διεύθυνση ζεύξης είναι αρκετή μόνο για επικοινωνία με τους κοντινούς κόμβους που έχουν άμεση επικοινωνία με τον πομπό, και οποιαδήποτε μετάδοση πέρα αυτών γίνεται με δρομολογημένη διεύθυνση.

Για όλες τις unicast διευθύνσεις, ανεξάρτητα από την εμβέλεια τους, είναι αποτελεσματικό να τις διαχωρίσουμε από τις διευθύνσεις ζεύξης του 802.15.4. Το 6LoWPAN λόγω της δέσμευση στην ζεύξη και της επικεφαλίδας IP, μπορεί να παραλείπει διευθύνσεις IP που εκπίπτουν από την διεύθυνση ζεύξης και αφαιρεί την ανάγκη για ανάλυση της διεύθυνσης. Αντίστοιχα, η αυτόματη διαμόρφωση πρέπει να ρυθμίσει την διευθυνσιοδότηση διεπαφής χρησιμοποιώντας ένα κοινό

πρόθεμα ώστε η συμπίεση επικεφαλίδας του 6LoWPAN να μειώσει το συνολικό μήκος της.

#### **4.4.4 Εύρεση γείτονα (Neighbor Discovery)**

Η εύρεση γείτονα IPv6 (ND) επιτρέπει σε έναν κόμβο να βρει τους γείτονες του, να διατηρήσει πληροφορίες προσβασιμότητας, να διαμορφώσει τις προεπιλεγμένες διαδρομές και να διαδώσει παραμέτρους διαμόρφωσης. Επειδή η λειτουργία ND προορίζεται για αλληλεπίδραση μεταξύ γειτονικών κόμβων, το ND ορίζεται για λειτουργία πάνω σε μία IP σύνδεση. Το ND εκτελεί ανάλυση διεύθυνσης και ανίχνευση μη προσιτότητας γείτονα στέλνοντας αιτήσεις σε όλους τους γειτονικούς κόμβους. Οι κόμβοι χρησιμοποιούν επίσης την λειτουργία ND για την ανίχνευση διπλότυπης διεύθυνσης (DAD). Όλες οι επικοινωνίες ND συμβαίνουν στο τοπικό επίπεδο ζεύξης.

Ωστόσο υπάρχουν σημαντικές προκλήσεις για την χρήση των τρεχόντων προδιαγραφών ND στα δίκτυα LoWPAN. Συγκεκριμένα, η εύρεση γείτονα κάνει εκτεταμένη χρήση του multicast, για την αναζήτηση της διεύθυνσης του κάθε κόμβου, με αποτέλεσμα την αύξηση της κίνησης στο δίκτυο και του κόστους. Για μικρά δίκτυα είναι αρκετά αξιόπιστο, αλλά όταν εφαρμόζεται σε μεγάλα mesh δίκτυα με πολλαπλές μεταβάσεις (multihop) έχουμε και αυξημένη καθυστέρηση.

#### **4.4.5 Δρομολόγηση**

Η μειωμένη μνήμη καθώς και οι περιορισμένες δυνατότητες επικοινωνίας, περιορίζουν την κατάσταση δρομολόγηση κάθε κόμβου, όπως και τις πληροφορίες δρομολόγησης που μπορούν να διαμοιραστούν. Οι περιορισμοί αυτοί αποκλείουν την χρήση πρωτόκολλων που βασίζονται μόνο στην πληροφορίες κατάστασης του επιπέδου ζεύξης. Τα παραδοσιακά πρωτόκολλα διανύσματος απόστασης σε ασύρματα δίκτυα φορητών κόμβων (MANET) χαρακτηρίζονται επίσης ακατάλληλα καθώς υποθέτουν φορητότητα όλων των κόμβων, ενώ στα LoWPAN έχουμε φορητότητα κάποιων κόμβων σε σχέση με ένα δίκτυο σταθερών κόμβων. Συνεπώς τα πρωτόκολλα που χρησιμοποιούν τα MANET χρησιμοποιούν συνέχεια ροές μέσα στο δίκτυο για να ανακαλύψουν και να διατηρήσουν τις δρομολογήσεις μέσα στο δίκτυο. Οι ρυθμοί μετάδοσης που χρησιμοποιούν αυτά τα πρωτόκολλα ξεπερνάνε συνήθως κατά πολύ την δυνατότητα που έχει ένα τυπικό δίκτυο LoWPAN. Για αυτό τον λόγο τα πρωτόκολλα δρομολόγησης που χρησιμοποιούν τα LoWPAN χρησιμοποιούν ελλιπείς πληροφορίες δικτύου και έχουν ανοχή στη μη συνοχή.

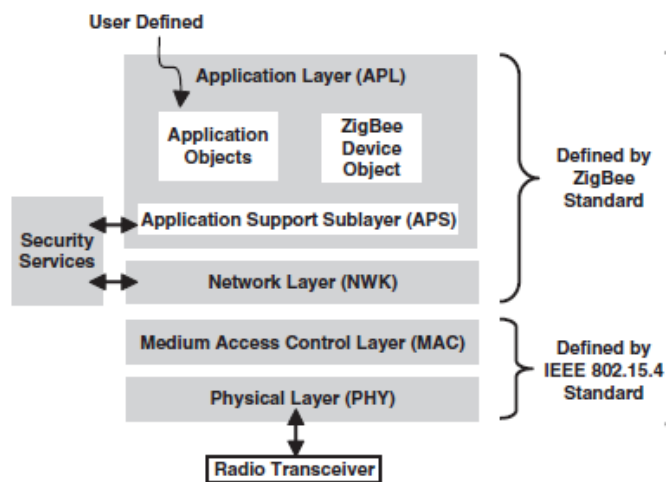
#### **4.4.6 Θέματα ασφάλειας**

Το 6LoWPAN εκμεταλλεύεται του μηχανισμού ασφαλείας AES-128 που του παρέχει το 802.15.4. Μηχανισμοί ασφαλείας στο επίπεδο μεταφοράς είναι επίσης εφικτοί σε δίκτυα 6LoWPAN. Ωστόσο, καθώς μηχανισμοί ασφαλείας στο επίπεδο δικτύου όπως ο IPsec και η ασφαλής εύρεση γείτονα (SND) ωριμάζουν, η συμβατότητα τους με δίκτυα 6LoWPAN είναι ακόμα υπό διερεύνηση.

## 5 Zigbee

### 5.1 Εισαγωγή

Το επίπεδα του πρωτοκόλλου Zigbee (Εικόνα 5-1) βασίζονται στο μοντέλο αναφοράς OSI (Open System Interconnect). Η τακτική αυτή είναι χρήσιμη στην δικτύωση καθώς κάθε επίπεδο είναι ανεξάρτητο από τα άλλα με αποτέλεσμα να μπορούμε να κάνουμε αλλαγές στο κάθε ένα από αυτά χωρίς να επηρεάζονται τα υπόλοιπα. Όπως φαίνεται και στην Εικόνα 5-1, το Zigbee αποτελείται από 4 επίπεδα. Τα 2 πρώτα που αποτελούνται από το φυσικό και το MAC επίπεδο ορίζονται από το πρότυπο 802.15.4 ενώ το Zigbee καθορίζει το επίπεδο δικτύου και εφαρμογής καθώς και την ασφάλεια που διέπει τα επίπεδα αυτά.



Εικόνα 5-1 Επίπεδα πρωτοκόλλου Zigbee

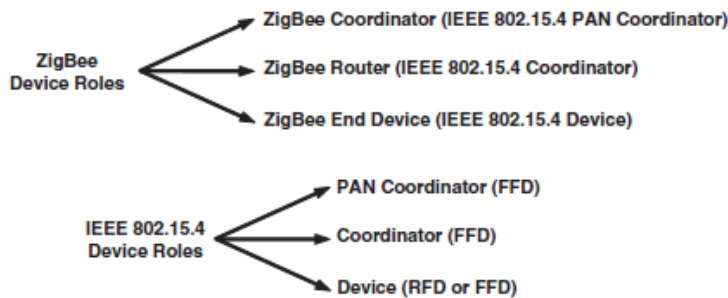
## 5.2 Εισαγωγικές έννοιες

### 5.2.1 Devices

Σε ένα δίκτυο Zigbee οι συσκευές που υπάρχουν είναι 3 ειδών:

- **ZigBee Coordinator (ZC):** αποτελεί την κύρια συσκευή και είναι αυτή που σχηματίζει το δίκτυο αρχικά και μπορεί να αποτελέσει και γέφυρα διασύνδεσης με άλλα δίκτυα. Επίσης διατηρεί πληροφορίες για το δίκτυο και αποτελεί αποθήκη των κλειδιών ασφαλείας του δικτύου.
- **ZigBee Router (ZR):** εκτός από το να κάνει κάποια λειτουργία για μια εφαρμογή, μπορεί να αναμεταδίδει δεδομένα από άλλες συσκευές.
- **ZigBee End Device (ZED):** διαθέτει την λειτουργικότητα για να εκτελεί μια λειτουργία και να επικοινωνεί με έναν κόμβο (router ή coordinator node) χωρίς να μπορεί να διαδώσει πληροφορία αλλού στο δίκτυο. Αυτό της επιτρέπει να είναι αδρανής (asleep) το μεγαλύτερο μέρος του χρόνου προσφέροντας μεγάλη διάρκεια ζωής μπαταρίας. Τέλος έχει μικρές απαιτήσεις σε μνήμη, γεγονός που την καθιστά πιο οικονομική σε σχέση με τους άλλους 2 τύπους.

Στο πρότυπο 802.15.4 τα είδη των συσκευών που ορίζονται είναι 2: FFD (Full Function Device) και RFD (Reduced Function Device). Οι ρόλοι σε αντιστοιχία με τους ρόλους στο Zigbee δίκτυο είναι: PAN coordinator, coordinator και device. Η αντιστοιχία των συσκευών φαίνεται στην Εικόνα 5-2.



Εικόνα 5-2 Είδη συσκευών Zigbee και 802.15.4



### 5.2.2 Services

Κάθε επίπεδο παρέχει μια σειρά από υπηρεσίες (Services) που εκτελούνται συνήθως για λογαριασμό του μόλις ανώτερου επιπέδου. Όλες οι υπηρεσίες πραγματοποιούνται από το Management Entity εκτός από την μεταφορά δεδομένων που γίνεται από το Data Entity. Ένα υψηλότερο επίπεδο αποκτά πρόσβαση στις υπηρεσίες του χαμηλότερου σε αυτό επιπέδου, με τη βοήθεια των Service Access Points (SAP). Για παράδειγμα αν θέλουμε να ενεργοποιήσουμε το πομποδέκτη, θα πρέπει το MAC επίπεδο να χρησιμοποιήσει μέσω του PD-SAP το PHY data service το οποίο θα επιτρέψει την αποστολή και λήψη των PDUs.

### 5.2.3 Primitives

Κάθε Service αποτελείται από μια σειρά εντολών που ονομάζονται Primitives. Όλα τα primitive έχουν τις παρακάτω λειτουργίες ή ορισμένες από αυτές:

- Request
- Confirm
- Indication
- Response

Το όνομα του primitive υποδεικνύει συνήθως το επίπεδο στο οποίο ανήκει καθώς και τη χρήση του. Η σύνταξη ενός primitive που περιλαμβάνει κάποια λειτουργία γίνεται ως εξής, **όνομα\_primitive . τύπος λειτουργίας**, π.χ. όταν το φυσικό επίπεδο ολοκληρώσει ένα CCA το αντίστοιχο primitive γράφεται PLME-CCA.confirm. Στην Εικόνα 5-3 φαίνεται η ακολουθία ανταλλαγής πληροφοριών μεταξύ δυο επιπέδων μέσω ενός primitive. Θεωρούμε τα επίπεδα N και N+1. Όταν το επίπεδο N+1 θέλει να κάνει χρήση μιας υπηρεσίας του N, απαιτείται πρώτα να κάνει request (αίτηση) στο επίπεδο N. Στη συνέχεια θα πρέπει το επίπεδο N να πληροφορήσει το N+1 αν η υπηρεσία ολοκληρώθηκε με επιτυχία ή όχι με το confirm δηλαδή την επιβεβαίωση. Το indication (ένδειξη) χρησιμοποιείται από το επίπεδο N όταν θέλει να αναφέρει ένα συμβάν στο N+1. Αν στο indication ζητείται απάντηση τότε το επίπεδο N+1 θα πρέπει να στείλει response (απόκριση) στο N.



Εικόνα 5-3 Λειτουργίες primitive

### 5.2.4 Binding

Οι συσκευές που συσχετίζονται μεταξύ τους λέμε ότι είναι λογικά συνδεδεμένες και ως Binding ορίζεται η διαδικασία δημιουργίας αυτών των «λογικών» διασυνδέσεων. Για παράδειγμα σε ένα ασύρματο σύστημα συναγερμού η μονάδα ZigBee του αισθητηρίου κίνησης είναι λογικά συνδεδεμένη με την μονάδα ZigBee του

κεντρικού πίνακα του συναγερμού. Οι πληροφορίες σχετικά με τις λογικές διασυνδέσεις αποθηκεύονται σε έναν πίνακα ο οποίος ονομάζεται Binding table και δημιουργείται στο επίπεδο εφαρμογής. Οι λογικά συνδεδεμένες συσκευές λέγονται Bound devices.

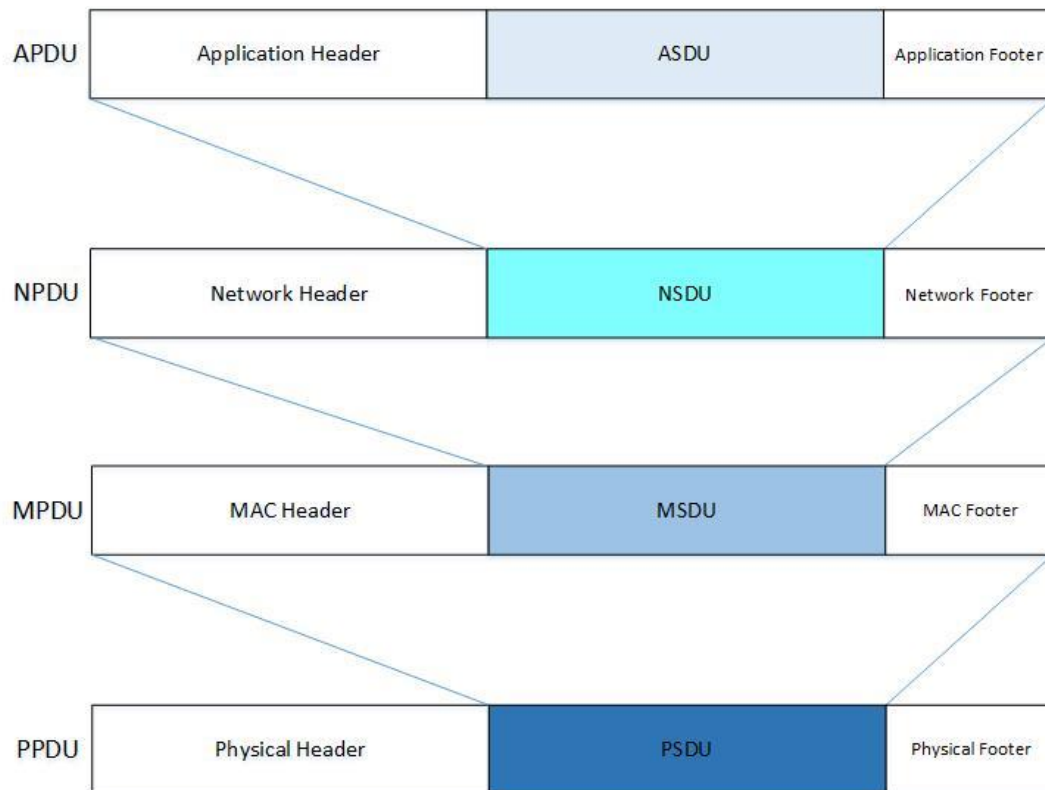
### **5.2.5 SDUs και PDUs**

Το πακέτο δεδομένων ενός επιπέδου αναφέρεται ως PDU (Protocol Data Unit) και διακρίνεται για το κάθε επίπεδο προσθέτοντας άλλο ένα γράμμα στην ονομασία. Πιο συγκεκριμένα είναι APDU (Application Protocol Data Unit) για το επίπεδο εφαρμογής, NPDU (Network Protocol Data Unit) για το επίπεδο δικτύου, MPDU (MAC Protocol Data Unit) για το επίπεδο MAC και PPDU (Physical Protocol Data Unit) για το φυσικό επίπεδο.

Το ωφέλιμο φορτίο κάθε επιπέδου αποτελεί τα δεδομένα που λήφθηκαν από το αμέσως ανώτερο επίπεδο και αναφέρεται ως SDU (Service Data Unit). Αντίστοιχα οι ονομασίες που προκύπτουν είναι οι εξής: ASDU (Application Service Data Unit) για το επίπεδο εφαρμογής, NSDU (Network Protocol Data Unit) για το επίπεδο δικτύου, MSDU (MAC Service Data Unit) για το επίπεδο MAC και PSDU (Physical Service Data Unit) για το φυσικό επίπεδο.

Γενικά κάθε επίπεδο δημιουργεί την PDU η οποία μετατρέπεται σε SDU (Service Data Unit) του αμέσως από κάτω επιπέδου. Ένα γενικευμένο σχήμα που εξηγεί αυτή

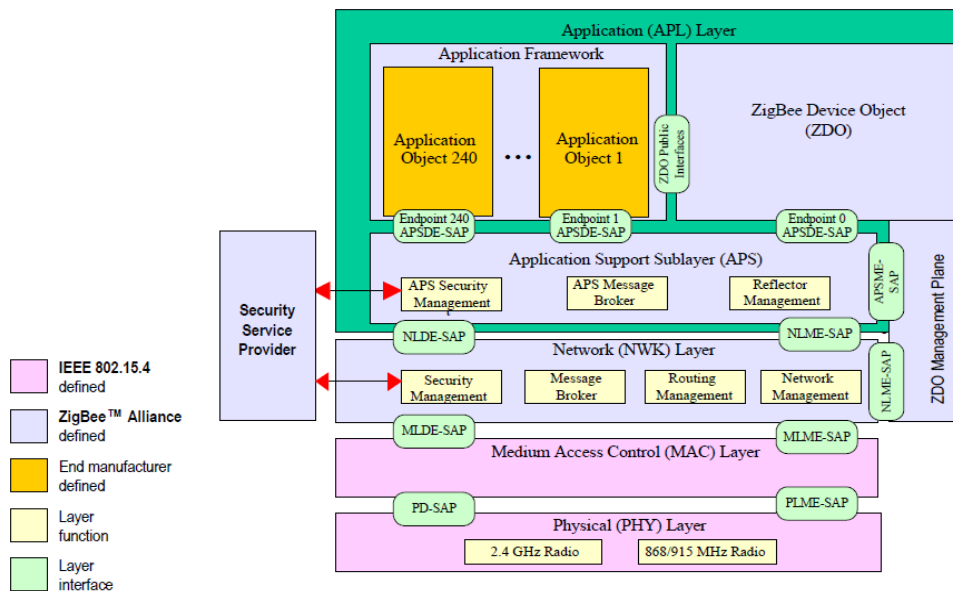
την λειτουργία ενθυλάκωσης φαίνεται παρακάτω:



Εικόνα 5-4 Διαδικασία ενθυλάκωση πακέτων επιπέδων

### 5.2.6 Management entities, data entities and SAPs

Κάθε επίπεδο περιλαμβάνει δύο οντότητες: Μια οντότητα δεδομένων (Data Entity) που διαχειρίζεται την υπηρεσία μεταφοράς δεδομένων και μια οντότητα διαχείρισης (Management Entity) όπου διαχειρίζεται τις υπόλοιπες παρεχόμενες υπηρεσίες του επιπέδου. Ένα υψηλότερο επίπεδο αποκτά πρόσβαση στις υπηρεσίες του αμέσως χαμηλότερου με την βοήθεια των Service Access Points (SAP). Τα SAPs διαχωρίζονται σε αυτά που αποκτούν πρόσβαση σε υπηρεσίες δεδομένων (DE-SAP) και σε αυτά που αποκτούν πρόσβαση σε υπηρεσίες διαχείρισης (ME-SAP). Στην Εικόνα 5-5 φαίνεται η λειτουργία των SAPs για τα επίπεδα του Zigbee.



Εικόνα 5-5 Λειτουργία Service Access Points (SAPs)

(source: zigbee specs)

### 5.3 802.15.4 Φυσικό επίπεδο

Το φυσικό επίπεδο είναι το πρώτο επίπεδο στο μοντέλο OSI που χρησιμοποιείται παγκοσμίως. Παρέχει την υπηρεσία για την μετάδοση των δεδομένων, καθώς και την διεπαφή για τον φορέα διαχείρισης φυσικού στρώματος, που παρέχει πρόσβαση στις λειτουργίες διαχείρισης όλων των επιπέδων και διατηρεί μια βάση με πληροφορίες σχετικές με συσχετιζόμενα δίκτυα προσωπικού χώρου. Έτσι το φυσικό επίπεδο διαχειρίζεται τον RF πομποδέκτη και αποφασίζει για την επιλογή καναλιού και την διαχείριση της ενέργειας και του σήματος. Λειτουργεί σε μια από τις τρεις ζώνες συχνοτήτων χωρίς άδεια :

- 868.0–868.6 MHz: Ευρώπη, επιτρέπει ένα κανάλι επικοινωνίας
- 902–928 MHz: Βόρεια Αμερική, μέχρι 10 κανάλια επικοινωνίας (2003), επεκτάθηκε στα 30 (2006)
- 2400–2483.5 MHz: παγκόσμια, μέχρι 16 κανάλια επικοινωνίας (2003, 2006)

Παρακάτω αναλύονται οι βασικές λειτουργίες του φυσικού επιπέδου.

#### 5.3.1 Energy detection

Όταν μια συσκευή σκοπεύει να μεταδώσει ένα μήνυμα, πρώτα εισέρχεται σε κατάσταση λήψης ώστε να ανιχνεύσει τα επίπεδα ενέργειας σήματος στο επιθυμητό κανάλι. Αυτή η διαδικασία είναι γνωστή ως energy detection(ED). Σε αυτή τη διαδικασία μόνο το επίπεδο ενέργειας εκτιμάται και όχι ο τύπος του σήματος. Οπότε δεν μπορούμε να ξέρουμε αν κάποιο σήμα είναι συμβατό με το πρότυπο 802.15.4. Σημαντικό ρόλο παίζει η ευαισθησία του δέκτη, που αποτελεί το σήμα ελάχιστης ενέργειας που μπορεί να εντοπίσει και να αποδιαμορφώσει με σφάλμα μικρότερο του 1%. Το επίπεδο MAC ζητάει από το φυσικό επίπεδο να εκτελέσει την διαδικασία ED και αυτό επιστρέφει έναν 8-bit ακέραιο που αποτελεί το επίπεδο ενέργειας στο επιθυμητό κανάλι.

#### 5.3.2 Carrier sense

Παρόμοια με την διαδικασία ED, η διαδικασία carrier sense (CS) αποτελεί άλλον ένα τρόπο για ελεγχθεί εάν ένα κανάλι είναι διαθέσιμο για χρήση. Όταν μια συσκευή σκοπεύει να μεταδώσει ένα μήνυμα, πρώτα εισέρχεται σε κατάσταση λήψης ώστε να ανιχνεύσει τον τύπο από οποιοδήποτε σήμα εντοπίσει στο επιθυμητό κανάλι. Σε αντίθεση με την ED, το σήμα αποδιαμορφώνεται και εκτιμάται ο τύπος του. Εάν προκύψει ότι το σήμα είναι συμβατό με το πρότυπο 802.15.4 τότε το κανάλι θεωρείται απασχολημένο.

### 5.3.3 Link Quality Indicator

Ο δείκτης ποιότητας ζεύξης (link quality indicator) αποτελεί μια ένδειξη της ποιότητας των πακέτων που λαμβάνει ο δέκτης. Η ισχύς του λαμβανόμενου σήματος (received signal strength, RSS) είναι μια μέτρηση της συνολικής ενέργειας του σήματος και αποτελεί έναν δείκτη για την ποιότητα του. Ένας ακόμη δείκτης είναι ο SNR (signal-to-noise ratio), που αποτελεί την αναλογία της ενέργειας του πραγματικού σήματος και θορύβου. Όσο υψηλότερος είναι ο δείκτης SNR τόσο καλύτερης ποιότητας θεωρείται το σήμα. Ο LQI μπορεί να υπολογιστεί με κάποιον από τους παραπάνω δείκτες ή και με συνδυασμό αυτών.

Ο LQI υπολογίζεται για κάθε εισερχόμενο πακέτο και διαβιβάζεται στο επίπεδο MAC όπου γίνεται διαθέσιμο και για τα υψηλότερα επίπεδα, δικτύου και εφαρμογής. Το επίπεδο δικτύου χρησιμοποιεί τα διάφορα LQI ανά το δίκτυο για να καθορίσει το μονοπάτι στο οποίο θα δρομολογηθεί ένα μήνυμα. Γενικά μια διαδρομή με το υψηλότερο συνολικό LQI έχει καλύτερες πιθανότητες επιτυχούς μετάδοσης του μηνύματος. Βέβαια υπάρχουν και άλλοι παράγοντες που καθορίζουν την δρομολόγηση.

### 5.3.4 Clear Channel Assessment

Όπως θα δούμε παρακάτω το επίπεδο MAC χρησιμοποιεί το πρωτόκολλο CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) για την πρόσβαση στο επιθυμητό κανάλι. Στο πρώτο βήμα αυτού του πρωτοκόλλου το επίπεδο MAC ζητάει από το φυσικό επίπεδο να εκτελέσει ένα Clear Channel Assessment (CCA) με σκοπό να δει αν το κανάλι χρησιμοποιείται από κάποια άλλη συσκευή. Κατά το CCA, τα αποτελέσματα από τις διαδικασίες ED και CS που αναφέρθηκαν παραπάνω χρησιμοποιούνται για να καθοριστεί ένα το κανάλι είναι διαθέσιμο ή όχι. Υπάρχουν τρεις λειτουργίες για το CCA:

- Mode 1: Σε αυτή τη λειτουργία μόνο το αποτέλεσμα από την διαδικασία ED λαμβάνεται υπόψη. Αν το επίπεδο ενέργειας είναι πάνω από το κατώφλι, το κανάλι θεωρείται απασχολημένο.
- Mode 2: Σε αυτή τη λειτουργία μόνο το αποτέλεσμα από την διαδικασία CS λαμβάνεται υπόψη. Αν εντοπιστεί σήμα συμβατό με το πρότυπο 802.15.4, το κανάλι θεωρείται απασχολημένο.
- Mode 3: Σε αυτή τη λειτουργία χρησιμοποιείται ένας λογικός συνδυασμός (AND/OR) των δυο προηγούμενων λειτουργιών.

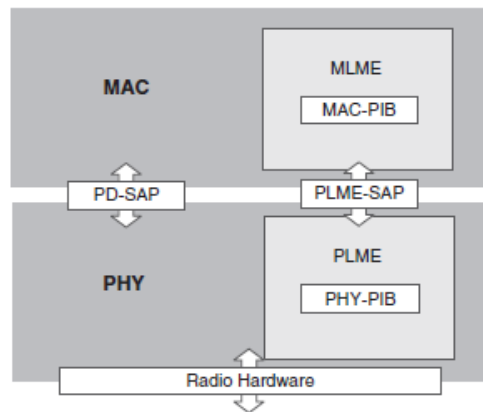
### 5.3.5 Σταθερές και Χαρακτηριστικά

Οι σταθερές αποτελούν τα χαρακτηριστικά εκείνα τα οποία μένουν αμετάβλητα κατά την λειτουργία. Κάθε επίπεδο έχει τις δικές του σταθερές. Το φυσικό επίπεδο διαθέτει δυο σταθερές: 1) *aMaxPHYPacketSize* που καθορίζει το μέγιστο μέγεθος της PSDU (Physical Service Data Unit) στα 127 bytes και 2) *aTurnaroundTime* που είναι ο μέγιστος χρόνος που θέλει ο πομποδέκτης για να αλλάξει από κατάσταση αποστολής (TX) σε κατάσταση λήψης (RX) και αντίστροφα. Η τιμή αυτή είναι 12 symbol periods. Στο φυσικό επίπεδο και το επίπεδο MAC, όλες οι σταθερές έχουν το πρόθεμα *a*. Στα επίπεδα δικτύου και εφαρμογής, τα προθέματα είναι *nwks* και *arpc* αντίστοιχα.

Τα χαρακτηριστικά αποτελούν τις μεταβλητές. Δηλαδή τα στοιχεία τα οποία αλλάζουν κατά την λειτουργία. Αυτά βρίσκονται στην βάση πληροφοριών του φυσικού επιπέδου (Physical-PIB, Physical PAN Information Base) και είναι απαραίτητα για την διαχείριση των υπηρεσιών του επιπέδου. Τέτοια χαρακτηριστικά είναι το κανάλι που χρησιμοποιείται (*phyCurrentChannel*), η λίστα με τα διαθέσιμα κανάλια (*phyChannelsSupported*), η λειτουργία CCA (*phyCCAMode*) και άλλα.

### 5.3.6 Υπηρεσίες φυσικού επιπέδου

Το φυσικό επίπεδο παρέχει δυο είδη υπηρεσιών: υπηρεσία δεδομένων και υπηρεσία διαχείρισης. Η υπηρεσία δεδομένων επιτρέπει την αποστολή και λήψη PPDU (Physical Protocol Data Unit) δηλαδή της μονάδας δεδομένων του επιπέδου και είναι προσβάσιμη διαμέσου του PD-SAP (Physical Data-Service Access Point). Η υπηρεσία δεδομένων αποτελείται από την PLME (Physical Layer Management Entity) από όπου καλούνται οι διάφορες διαχειριστικές συναρτήσεις και η οποία είναι προσβάσιμη διαμέσου του PLME-SAP. Μέσω των SAPs οι υπηρεσίες του φυσικού επιπέδου γίνονται διαθέσιμες στο επίπεδο MAC. (Εικόνα 5-5) Επίσης η οντότητα αυτή διατηρεί και την βάση πληροφοριών του φυσικού επιπέδου (Physical-PIB).



Εικόνα 5-6 Υπηρεσίες φυσικού επιπέδου και διασύνδεση με επίπεδο MAC

### 5.3.6.1 Υπηρεσία δεδομένων φυσικού επιπέδου (PD-DATA)

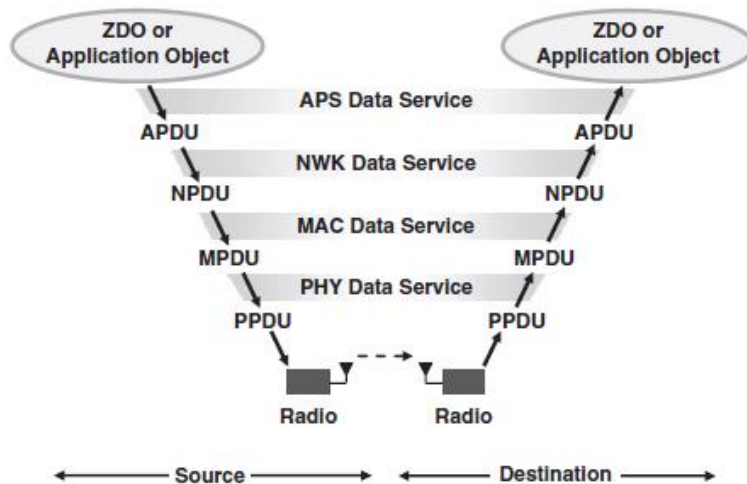
Όταν έχουμε δεδομένα που πρέπει να μεταδοθούν, αυτά πάντα λαμβάνονται από το φυσικό επίπεδο ως μια MPDU (MAC Protocol Data Unit) από το επίπεδο MAC. Το φυσικό επίπεδο προσθέτει κάποια στοιχεία επικεφαλίδας δημιουργώντας την PPDU, επιχειρεί την αποστολή και ενημερώνει το επίπεδο MAC αν ήταν επιτυχής ή όχι. Οι λόγοι για να αποτύχει μια αποστολή είναι οι εξής:

- Ο πομποδέκτης είναι απενεργοποιημένος
- Ο πομποδέκτης είναι σε κατάσταση λήψης
- Ο πομποδέκτης είναι απασχολημένος, δηλαδή υπάρχει άλλη μετάδοση σε εξέλιξη

Όταν έχουμε λήψη δεδομένων από τον πομποδέκτη, το φυσικό επίπεδο ενημερώνει το επίπεδο MAC και του παρέχει την MPDU αλλά και τον δείκτη LQI.

Στην Εικόνα 5-7 φαίνεται η μεταφορά ενός πακέτου δεδομένων μιας εφαρμογής από μια συσκευή σε μια άλλη. Τα δεδομένα δεν είναι ανάγκη να προέρχονται από το επίπεδο εφαρμογής. Παρατηρούμε ότι κάθε επίπεδο προσθέτει κατά την αποστολή και αφαιρεί κατά την λήψη τα στοιχεία επικεφαλίδας που το αφορούν και παρέχει το πακέτο δεδομένων στο επόμενο αρμόδιο επίπεδο.





Εικόνα 5-7 Μεταφορά πακέτου μεταξύ 2 συσκευών

### 5.3.6.2 Υπηρεσία διαχείρισης φυσικού επιπέδου (PLME)

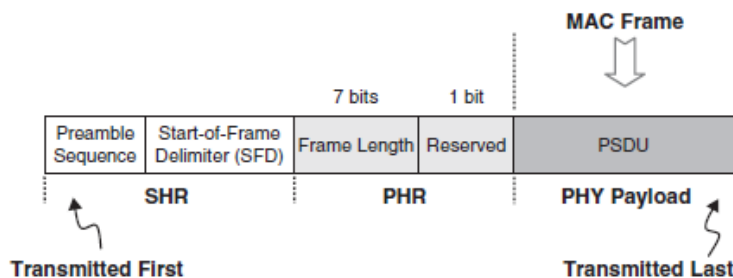
Όπως αναφέραμε η PLME (Physical Layer Management Entity) προσπελάζεται διαμέσου του PLME-SAP. Σκοπός της είναι να μεταφέρει εντολές από και προς την αντίστοιχη οντότητα του επιπέδου MAC (MLME) και να καλεί τις διάφορες διαχειριστικές συναρτήσεις. Οι υπηρεσίες που παρέχονται είναι (στις παρενθέσεις αναφέρονται τα ονόματα των service primitives):

- **Clear channel assessment (PLME-CCA):** Το επίπεδο MAC (συγκεκριμένα η MLME) ζητάει από την PLME να εκτελέσει ένα CCA κάθε φορά που το πρωτόκολλο CSMA/CA το απαιτεί. Το αποτέλεσμα αυτού του CCA είναι ένα από τα ακόλουθα:
  - ο πομποδέκτης είναι απενεργοποιημένος, οπότε το CCA δεν εκτελείται
  - το κανάλι είναι διαθέσιμο και μπορεί να χρησιμοποιηθεί για μετάδοση
  - το κανάλι ή ο πομποδέκτης είναι απασχολημένος
- **Energy detection (PLME-ED):** Παρόμοια η MLME ζητάει από την PLME να εκτελέσει την διαδικασία ED. Αν αυτή εκτελεστεί με επιτυχία το επίπεδο ενέργειας επιστρέφεται στην MLME.
- **Ενεργοποίηση και απενεργοποίηση του πομποδέκτη (PLME-SET-TRX-STATE):** Η MLME μπορεί να ζητήσει από την PLME να θέσει τον πομποδέκτη σε μια από τις τρεις καταστάσεις: πομποδέκτης απενεργοποιημένος, πομπός ενεργός, δέκτης ενεργός.

- **Λήψη πληροφοριών από την βάση πληροφοριών του φυσικού επιπέδου (PLME-GET):** Η PLME μπορεί να διαβάσει τα χαρακτηριστικά του επιπέδου και να παρέχει τις τιμές τους στην MLME.
- **Αλλαγή τιμής χαρακτηριστικού του φυσικού επιπέδου (PLME-SET)**

### 5.3.7 Πλαίσιο φυσικού επιπέδου

Η δομή του πακέτου δεδομένων του φυσικού στρώματος φαίνεται στην παρακάτω Εικόνα 5-8. Αποτελείται από την επικεφαλίδα συγχρονισμού (SHR), την επικεφαλίδα του επιπέδου (PHR) και το ωφέλιμο φορτίο.



Εικόνα 5-8 Δομή πακέτου φυσικού επιπέδου

Η επικεφαλίδα συγχρονισμού αποτελείται από δυο πεδία. Το preamble που χρησιμοποιείται για τον συγχρονισμό του δέκτη και το SFD που ορίζει το τέλος του SHR και την αρχή του PHR.

Η PHR αποτελείται και αυτή από δυο πεδία. Το πρώτο προσδιορίζει τον αριθμό bytes του ωφέλιμου φορτίου (PSDU) και το δεύτερο διατηρείται για μελλοντική χρήση.

Το ωφέλιμο φορτίο ή αλλιώς PSDU (Physical Service Data Unit) αποτελεί τα δεδομένα που λήφθηκαν από το επίπεδο MAC ως MPDU ή αλλιώς πλαίσιο MAC.

### 5.3.8 Συνοπτική παρουσίαση των αρμοδιοτήτων του φυσικού επιπέδου

Το φυσικό επίπεδο είναι το κοντινότερο στο υλικό επίπεδο και μπορεί να ελέγχει και να επικοινωνεί άμεσα με τον πομποδέκτη. Οι αρμοδιότητες του είναι:

- Ενεργοποίηση και απενεργοποίηση πομποδέκτη
- Μετάδοση και λήψη δεδομένων
- Επιλογή καναλιού και συχνότητας
- Εκτέλεση διαδικασίας ED (Energy Detection) και CS (Carrier Sense)
- Εκτέλεση CCA (Clear Channel Assessment)

- Παραγωγή του δείκτη LQI (Link Quality Indicator)

#### 5.4 802.15.4 Επίπεδο MAC

Το επίπεδο MAC αποτελεί την διεπαφή μεταξύ του φυσικού στρώματος και του αμέσως ανώτερου επιπέδου. Στην πλατφόρμα του Zigbee αυτό είναι το επίπεδο δικτύου. Παρόμοια με το φυσικό επίπεδο, το MAC διαθέτει την οντότητα MLME (MAC Layer Management Entity) που είναι υπεύθυνη για την διαχείριση των υπηρεσιών και την MCPS για την διαχείριση των δεδομένων. Επίσης το επίπεδο MAC διαθέτει την δικιά του βάση πληροφοριών, γνωστή ως MAC-PIB (MAC PAN Information Base).

##### 5.4.1 CSMA/CA

Το πρότυπο 802.15.4 χρησιμοποιεί ένα απλό πρωτόκολλο για να επιτρέπει σε πολλαπλές συσκευές να χρησιμοποιούν το ίδιο κανάλι. Το πρωτόκολλο αυτό ονομάζεται CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Σε αυτή τη μέθοδο, κάθε φορά που μια συσκευή θέλει να μεταδώσει, εκτελεί πρώτα ένα CCA (Clear Channel Assessment) για να σιγουρευτεί ότι το κανάλι δεν χρησιμοποιείται από κάποια άλλη συσκευή. Έπειτα από αυτόν το έλεγχο ξεκινάει να μεταδίδει. Ο παράγοντας που καθορίζει πότε ένα κανάλι χρησιμοποιείται, είναι είτε η ενέργεια του σήματος στο κανάλι (ED), είτε ο τύπος του σήματος που εντοπίζεται στο κανάλι (CS). Αν ένα κανάλι χρησιμοποιείται, τότε η συσκευή οπισθοχωρεί κατά μια τυχαία περίοδο χρόνου και έπειτα ξαναπροσπαθεί. Τρεις είναι οι βασικές μεταβλητές του αλγορίθμου του CSMA/CA: ο εκθέτης οπισθοχώρησης (back-off exponent, BE), ο αριθμός των οπισθοχωρήσεων (number of back-offs, NB) και το μήκος παραθύρου ανταγωνισμού (contention window, CW). Η περίοδος χρόνου που περιμένει μια συσκευή έως ότου ξαναπροσπαθήσει δίνεται από την παρακάτω σχέση:

$$\text{Back-off} = (\text{A random integer between } 0 \text{ and } 2^{BE} - 1) \\ * aUnitBackoffPeriod$$

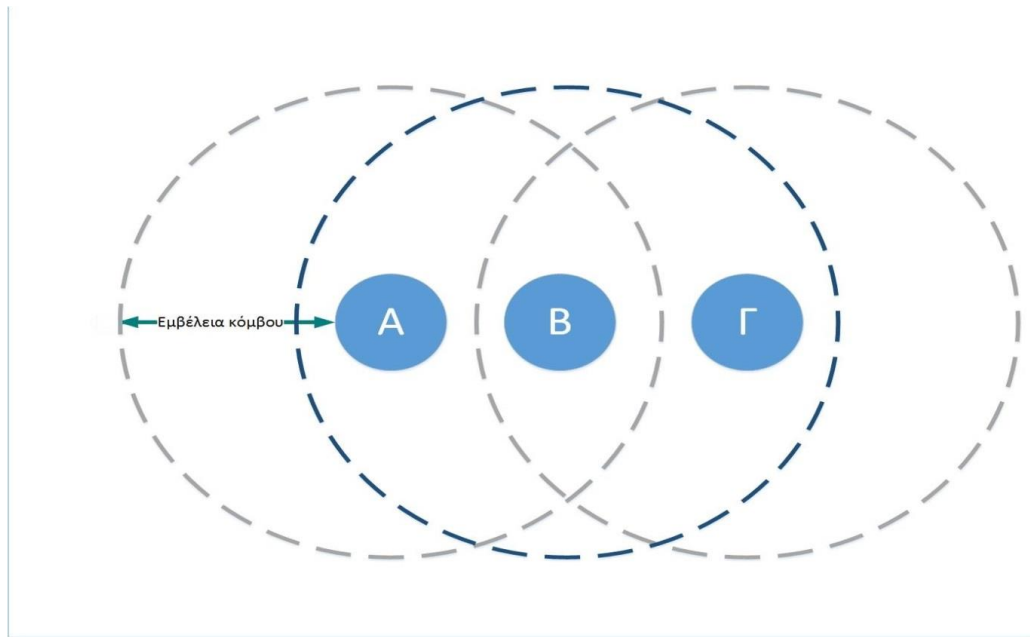
Όπου *aUnitBackoffPeriod* είναι η μονάδα της περιόδου.

Το παράθυρο ανταγωνισμού καθορίζει τον αριθμό των οπισθοδρομήσεων που πρέπει να συμβούν και κατά τις οποίες το κανάλι είναι διαθέσιμο, πριν αρχίσει η συσκευή να μεταδίδει. Για παράδειγμα, εάν το παράθυρο ανταγωνισμού είναι 2, τότε η συσκευή μεταδίδει μόνο μετά από 2 συνεχόμενες οπισθοδρομήσεις όπου κατέληξαν σε διαθέσιμο κανάλι.

Διακρίνουμε δύο είδη του πρωτοκόλλου: CSMA/CA με χρονοσχισμές (slotted) και CSMA/CA χωρίς χρονοσχισμές (unslotted). Το slotted CSMA/CA χρησιμοποιείται στην περίπτωση που έχουμε χρήση πλαισίου superframe (Ενότητα 5.4.3) όπου η ενεργή περίοδος χωρίζεται σε 16 ίσες χρονοσχισμές. Το unslotted χρησιμοποιείται στην περίπτωση που δεν έχουμε superframe ή το δίκτυο δεν υποστηρίζει beacons (Ενότητα 5.4.2).

#### **5.4.1.1 Hidden Node Problem**

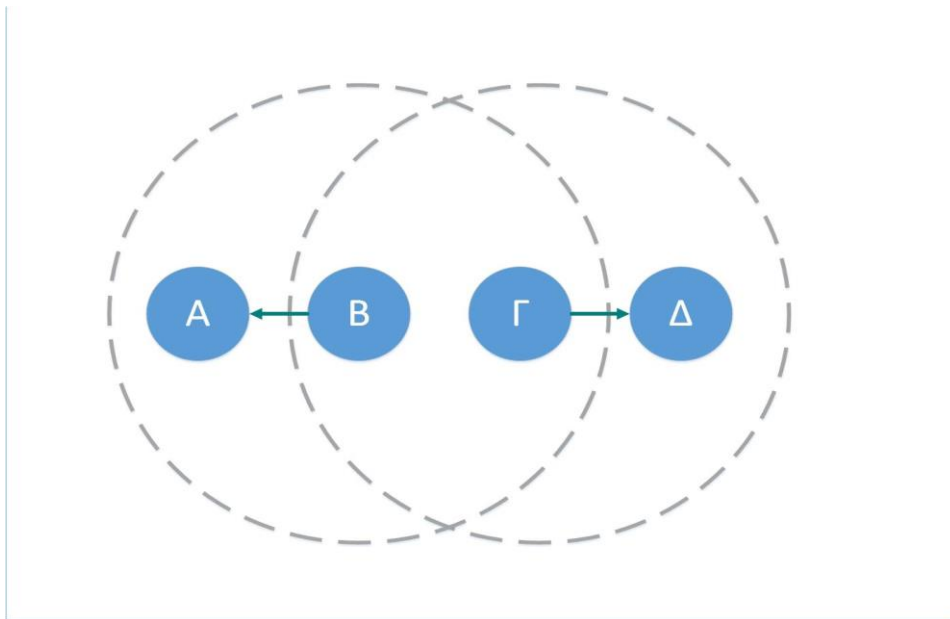
Μια από τις αδυναμίες του πρωτοκόλλου CSMA/CA είναι το πρόβλημα του κρυμμένου κόμβου. Ας υποθέσουμε ότι έχουμε τρεις κόμβους Α, Β και Γ όπως φαίνεται και στην Εικόνα 5-9 Πρόβλημα κρυμμένου κόμβου. Οι κόμβοι Α και Γ βρίσκονται πολύ μακριά, εκτός της εμβέλειας τους και κατά συνέπεια δεν μπορούν να επικοινωνούν. Και οι δυο όμως κόμβοι μπορούν να επικοινωνούν με τον Β. Σε κάθε κόμβο, η ενέργεια του σήματος μειώνεται όσο η απόσταση από την κεραία αυξάνεται. Οπότε εάν ο Α μεταδίδει στον Β, ο μηχανισμός ελέγχου (ED) του Γ δεν μπορεί να εντοπίσει την παρουσία άλλου σήματος, οπότε θεωρεί το κανάλι διαθέσιμο. Συνεπώς μπορεί ο Α και ο Γ μεταδώσουν ταυτόχρονα στον Β χρησιμοποιώντας το ίδιο κανάλι, με αποτέλεσμα να έχουμε σύγκρουση. Ένας τρόπος να αποφύγουμε αυτό το πρόβλημα είναι αλλάζοντας την διάταξη των κόμβων ή αυξάνοντας την ενέργεια του προς μετάδοση σήματος, ώστε πλέον ο Α να μπορεί να εντοπίσει τυχόν μετάδοση του Γ και αντίστροφα. Σε επίπεδο λογισμικού λίγα μπορούν να γίνουν καθώς το IEEE 802.15.4 MAC δεν υποστηρίζει τον μηχανισμό RTS/CTS (request-to-send/clear-to-send) που χρησιμοποιείται στο IEEE 802.11 για την αποφυγή του προβλήματος του κρυμμένου κόμβου.



Εικόνα 5-9 Πρόβλημα κρυμμένου κόμβου

#### 5.4.1.2 Exposed Node Problem

Ένα ακόμα πρόβλημα που συναντάμε στο πρωτόκολλο CSMA/CA είναι το πρόβλημα του εκτεθειμένου κόμβου. Σε αυτή την περίπτωση όπως φαίνεται και στην Εικόνα 5-10, ο κόμβος B θέλει να μεταδώσει ένα μήνυμα στον A καθώς ο Γ μεταδίδει στον Δ. Ο κόμβος A είναι εκτός της εμβέλειας του Γ. Για αυτό τον λόγο ο B και ο Γ μπορούν να μεταδώσουν χωρίς να υπάρξουν συγκρούσεις. Όμως το CSMA/CA θα εμποδίσει τον B από το να μεταδώσει, διότι ο B είναι στην εμβέλεια του Γ και ο έλεγχος CCA που θα εκτελέσει θα δείξει ότι το κανάλι είναι απασχολημένο. Αντίστοιχα με πριν, εφόσον ο μηχανισμός RTS/CTS δεν χρησιμοποιείται, ο τρόπος για να αποφύγουμε αυτό το ζήτημα είναι η αναδιάταξη των κόμβων ή η μείωση της ενέργειας του προς μετάδοση σήματος.



Εικόνα 5-10 Πρόβλημα εκτεθειμένου κόμβου

#### 5.4.2 Beacon-Enabled vs. Nonbeacon Networking

Υπάρχουν δυο μηχανισμοί πρόσβασης στο κοινό μέσο: 1) με ανταγωνισμό (contention based), 2) χωρίς ανταγωνισμό (contention free). Στον μηχανισμό πρόσβασης με ανταγωνισμό, όλες οι συσκευές που θέλουν να μεταδώσουν στην ίδια συχνότητα χρησιμοποιούν το πρωτόκολλο CSMA/CA και η πρώτη που ελέγχει και βρίσκει το κανάλι ελεύθερο ξεκινά να μεταδίδει. Στον μηχανισμό χωρίς ανταγωνισμό, έχουμε ύπαρξη χρονοσχισμών και μια συσκευή που ονομάζεται συντονιστής (coordinator) του δικτύου προσωπικού χώρου (PAN) αποδίδει την εκάστοτε χρονοσχιμή σε μια συγκεκριμένη συσκευή. Για αυτό τον λόγο οι χρονοσχιμές αυτές ονομάζονται εγγυημένες χρονοσχιμές (Guaranteed Time Slot, GTS). Επομένως όταν σε μια συσκευή ανατεθεί κάποια εγγυημένη χρονοσχιμή, μπορεί να μεταδώσει κατά τη διάρκεια αυτής χωρίς να χρησιμοποιήσει το πρωτόκολλο CSMA/CA για έλεγχο του μέσου. Αυτό το χαρακτηριστικό καθιστά το πρότυπο 802.15.4 κατάλληλο και για real-time εφαρμογές.

Για να παρέχει αυτές τις χρονοσχιμές (GTS), ο συντονιστής πρέπει να σιγουρευτεί ότι όλες οι συσκευές του δικτύου είναι συγχρονισμένες. Τα beacons είναι μηνύματα με συγκεκριμένη δομή που χρησιμοποιούνται για να συγχρονίζουν τα ρολόγια όλων των κόμβων του δικτύου. Η δομή τους παρουσιάζεται στην ενότητα 5.4.5.1. Ένα δίκτυο στο οποίο ο συντονιστής μπορεί να μεταδίδει beacons για να συγχρονίζει όλες τις συσκευές που υπάγονται σε αυτόν ονομάζεται beacon-enabled PAN. Το

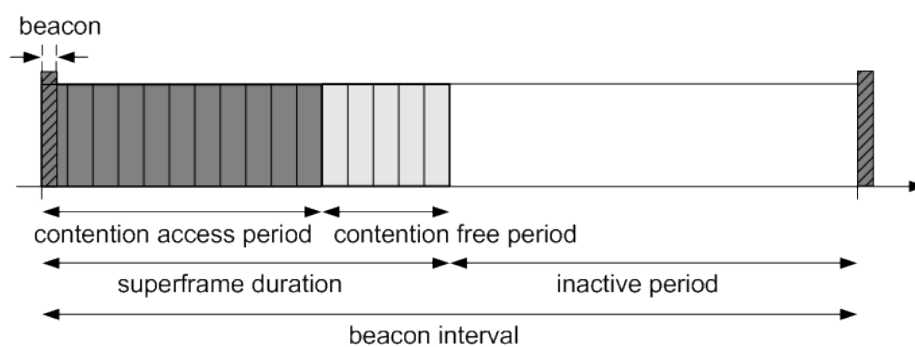
μειονέκτημα της χρήσης beacons είναι ότι όλες οι συσκευές πρέπει να ενεργοποιούνται («ξυπνούν») σε τακτική βάση για να λαμβάνουν τα beacons, να συγχρονίζουν τα ρολόγια τους και έπειτα να απενεργοποιούνται (sleep). Αυτό σημαίνει ότι πολλές από τις συσκευές στο δίκτυο μπορεί να ενεργοποιούνται μόνο για συγχρονισμό, χωρίς να έχουν να στείλουν ή να λάβουν κάτι όσο είναι σε λειτουργία. Επομένως η διάρκεια μπαταρίας σε ένα beacon-enabled PAN είναι μικρότερη συγκριτικά με ένα δίκτυο χωρίς beacons (nonbeacon). Σε ένα nonbeacon δίκτυο υπάρχουν μόνο περίοδοι ανταγωνισμού και οι συσκευές προσπελαύνουν το μέσο χρησιμοποιώντας το πρωτόκολλο CSMA/CA.

### 5.4.3 Superframe

Σε ένα beacon-enabled PAN υπάρχει η δυνατότητα χρήσης ενός διαφορετικού είδους πλαισίου που ονομάζεται superframe. Το πλαίσιο αυτό ορίζεται από τον συντονιστή του δικτύου και η γενική δομή του φαίνεται στην Εικόνα 5-11. Το πλαίσιο superframe πλαισιώνεται από πλαίσια beacons τα οποία χρησιμεύουν στον συγχρονισμό. Μπορεί να χωριστεί σε έως τρεις περιόδους: την περίοδο ανταγωνισμού (Contention Access Period, CAP), την περίοδο χωρίς ανταγωνισμό (Contention Free Period, CFP) και την ανενεργή περίοδο.

Κατά την CAP όλες οι συσκευές που θέλουν να μεταδώσουν χρησιμοποιούν το πρωτόκολλο CSMA/CA για πρόσβαση στο μέσο. Η πρώτη συσκευή που βρίσκει ελεύθερο το μέσο, αρχίζει να μεταδίδει και μπορεί να μεταδώσει μέχρι την άφιξη του επόμενου beacon.

Κατά την CFP, σε μια συγκεκριμένη συσκευή αποδίδεται μια εγγυημένη χρονοσχιμή, οπότε δεν χρειάζεται να χρησιμοποιήσει CSMA/CA για πρόσβαση στο μέσο. Αυτή είναι μια καλή επιλογή για εφαρμογές όπου οι συσκευές δεν μπορούν να περιμένουν μέχρι να γίνει ελεύθερο το μέσο και απαιτούν χαμηλό χρόνο απόκρισης (low latency).



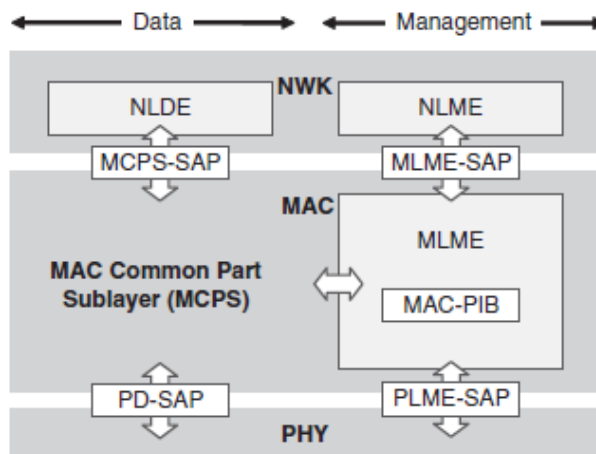
Εικόνα 5-11 Δομή πλαισίου superframe

Η CAP και η CFP αποτελούν την ενεργή περίοδο του superframe. Αυτή χωρίζεται σε 16 ίσες χρονοσχιμαστές. Το πρώτο beacon ξεκινάει στην αρχή της πρώτης από αυτές.

Επίσης μπορεί να υπάρχει και ανενεργή περίοδος όπως αναφέρθηκε, κατά τη διάρκεια της οποίας ο συντονιστής μπορεί να εξοικονομεί μπαταρία εισερχόμενος σε power saving mode.

#### 5.4.4 Υπηρεσίες επιπέδου MAC

Το επίπεδο MAC παρέχει δυο είδη υπηρεσιών: υπηρεσία δεδομένων και υπηρεσία διαχείρισης. Η υπηρεσία δεδομένων MAC είναι προσβάσιμη από την οντότητα δεδομένων του επιπέδου δικτύου (Network Layer Data Entity, NLDE) διαμέσου του MAC Common Part Sublayer SAP (MCPS-SAP). Η υπηρεσία διαχείρισης MAC είναι προσβάσιμη από την οντότητα διαχείρισης του επιπέδου δικτύου (Network Layer Management Entity, NLME) διαμέσου του MLME-SAP (MAC Layer Management Entity- Service Access Point). Η επικοινωνία με το φυσικό επίπεδο περιγράφηκε στο προηγούμενο κεφάλαιο. Όλα τα παραπάνω φαίνονται στο σχήμα της Εικόνα 5-12.



Εικόνα 5-12 Υπηρεσίες επιπέδου MAC και διασύνδεση με επίπεδο δικτύου και φυσικό επίπεδο

##### 5.4.4.1 Υπηρεσία δεδομένων επιπέδου MAC (MCPS)

Το MAC παρέχει την υπηρεσία δεδομένων του στο επίπεδο δικτύου. Τα δεδομένα προς μετάδοση παρέχονται ως NPDU (Network Protocol Data Unit) και αποτελούν το ωφέλιμο φορτίο για το επίπεδο MAC ή αλλιώς την MSDU.

Σε περίπτωση λήψης δεδομένων η υπηρεσία δεδομένων MAC μεταφέρει τα δεδομένα στο επίπεδο δικτύου διαμέσου του MCPS-SAP. Εκτός από τα δεδομένα, ο δείκτης ποιότητας ζεύξης (LQI) που μετρήθηκε κατά την λήψη της MPDU και ο ακριβής χρόνος στον οποίο λήφθηκε (timestamp) παρέχονται στο επίπεδο δικτύου.

Υπάρχουν τρεις επιλογές μετάδοσης:



- Μετάδοση με ή χωρίς επιβεβαιώσεις: Σε μια μετάδοση με επιβεβαίωση, η συσκευή αποστολέας ζητάει από την συσκευή παραλήπτη να στείλει πίσω ένα πλαίσιο επιβεβαίωσης (ACK) σε περίπτωση που λάβει τα δεδομένα επιτυχώς. Στην περίπτωση χωρίς επιβεβαίωση δεν έχουμε αποστολή τέτοιων ενημερωτικών πλαισίων.
- Μετάδοση κατά τη διάρκεια εγγυημένης χρονοσχιμής και CAP
- Άμεση (direct) ή έμμεση (indirect) μετάδοση: Όπως ορίζει και το όνομα, στην περίπτωση της έμμεσης μετάδοσης τα δεδομένα δεν μεταδίδονται κατευθείαν στην συσκευή παραλήπτη. Αντ' αυτού σε ένα beacon-enabled δίκτυο, τα δεδομένα μπορούν να αποθηκευτούν στον συντονιστή (coordinator) και η συσκευή παραλήπτη να ενημερωθεί ότι εκκρεμούν δεδομένα για αυτή. Αυτή η ειδοποίηση είναι μέρος των μηνυμάτων beacon που στέλνονται σε τακτική βάση. Μόλις μια συσκευή λάβει μια τέτοια ειδοποίηση στέλνει αίτηση για δεδομένα στον συντονιστή. Μόνο ο συντονιστής μπορεί να διαχειρίζεται έμμεσες μεταδόσεις.

#### **5.4.4.2 Υπηρεσία διαχείρισης επιπέδου MAC (MLME)**

Η MLME (MAC Layer Management Entity) προσπελάζεται διαμέσου του MLME-SAP και του PLME-SAP. Σκοπός της είναι να μεταφέρει εντολές από και προς την αντίστοιχη οντότητα του επιπέδου δικτύου (NLME) και του φυσικού επιπέδου (PLME) και να καλεί τις διάφορες διαχειριστικές συναρτήσεις. Οι υπηρεσίες που παρέχονται είναι (στις παρενθέσεις αναφέρονται τα ονόματα των service primitives):

##### **5.4.4.2.1 Διαχείριση της βάσης MAC PIB (MLME-GET και MLME-SET)**

Το επίπεδο MAC, παρόμοια με το φυσικό επίπεδο, έχει τα δικά του χαρακτηριστικά και σταθερές. Τα χαρακτηριστικά βρίσκονται στην βάση πληροφοριών του επιπέδου (MAC-PIB, MAC PAN Information Base) και είναι προσβάσιμα από το επίπεδο δικτύου. Δηλαδή το επίπεδο δικτύου μπορεί να ζητήσει από την MLME την τιμή ενός χαρακτηριστικού από την MAC-PIB ή ακόμα και από την Physical-PIB. Επίσης μπορεί να ζητήσει την αλλαγή ενός τέτοιου χαρακτηριστικού, εφόσον βέβαια δεν αποτελεί read-only χαρακτηριστικό.

##### **5.4.4.2.2 Επαναφορά επιπέδου MAC (MLME-RESET)**

Το επίπεδο δικτύου μπορεί να ζητήσει από την MLME να επαναφέρει (reset) το επίπεδο MAC στην αρχική του κατάσταση και να θέσει όλες τις εσωτερικές μεταβλητές στις προκαθορισμένες τιμές τους. Επίσης μπορεί να ζητήσει όλα τα χαρακτηριστικά της MAC-PIB να τεθούν στις προκαθορισμένες τιμές τους. Το MAC χρησιμοποιεί την υπηρεσία διαχείρισης του φυσικού επιπέδου για να απενεργοποιήσει τον πομποδέκτη προτού κάνει τις παραπάνω ενέργειες.

#### 5.4.4.2.3 Device Association and Disassociation (MLME-ASSOCIATE και DISASSOCIATE)

Το επίπεδο MAC παρέχει διαδικασίες στο επίπεδο δικτύου, που επιτρέπουν την σύνδεση συσκευών στο δίκτυο αλλά και την έξοδο τους από αυτό. Αυτό συμβαίνει διότι το επίπεδο δικτύου διαχειρίζεται την δομή του δικτύου.

#### 5.4.4.2.4 Communication Status (MLME-COMM-STATUS)

Η MLME παρέχει στο επίπεδο δικτύου πληροφορίες σχετικά με την κατάσταση μιας μετάδοσης. Σε περίπτωση αποτυχίας παρέχει και τον λόγο για τον οποίο συνέβη. Επίσης ενημερώνει για τυχόν προβλήματα ασφαλείας στα εισερχόμενα πακέτα.

#### 5.4.4.2.5 Ενεργοποίηση και απενεργοποίηση του δέκτη (MLME-RX-ENABLE)

Το επίπεδο δικτύου μπορεί να ζητήσει από την MLME να ενεργοποιήσει τον δέκτη για κάποια συγκεκριμένη χρονική περίοδο. Ο χρόνος για τον οποίο θα μείνει ενεργός ο δέκτης προσδιορίζεται από το επίπεδο δικτύου. Επίσης μπορεί να ζητήσει την απενεργοποίηση του δέκτη. Η διαδικασία αυτή αντιμετωπίζεται ως δευτερεύουσα από την MLME και την αγνοεί σε περίπτωση που εκκρεμεί κάποια άλλη διαδικασία.

#### 5.4.4.2.6 Διαχείριση εγγυημένων χρονοσχημάτων (MLME-GTS)

Σε ένα beacon-enabled δίκτυο υπάρχουν εγγυημένες χρονοσχημές (GTS) τις οποίες μπορεί μια συσκευή να χρησιμοποιήσει για να μεταδώσει χωρίς να γίνει χρήση του CSMA/CA. Το επίπεδο δικτύου μιας συσκευής μπορεί να χρησιμοποιήσει την υπηρεσία διαχείρισης του MAC για να ζητήσει να της αποδοθεί μια τέτοια χρονοσχημή. Ο συντονιστής του δικτύου μπορεί να δεχτεί ή να αρνηθεί μια τέτοια αίτηση. Επίσης μπορεί να καταργήσει μια χρονοσχημή που έχει αποδοθεί σε μια συσκευή και να την παραχωρήσει αλλού. Τέλος μπορεί και η ίδια η συσκευή να ζητήσει την κατάργηση μιας δοσμένης σε αυτήν GTS σε περίπτωση που δεν την χρειάζεται πλέον.

#### 5.4.4.2.7 Ενημέρωση και διαμόρφωση της δομής superframe

Σε ένα beacon-enabled δίκτυο, το επίπεδο δικτύου μπορεί να ζητήσει από την MLME την εκκίνηση της δομής πλαισίου superframe. Για να γίνει αυτό παρέχει όλες τις απαραίτητες πληροφορίες όπως το μήκος της ενεργής περιόδου, πόσο συχνά πρέπει να μεταδίδονται τα beacons, πόσο χρόνο μπορεί ο συντονιστής να εξοικονομεί ενέργεια και άλλα.

#### 5.4.4.2.8 Orphan Notification (MLME-ORPHAN)

Μια συσκευή πρέπει να είναι συνδεδεμένη σε κάποιο δίκτυο για να μπορεί να επικοινωνεί με άλλες συσκευές. Μια συσκευή η οποία άνηκε σε κάποιο δίκτυο, αλλά πλέον δεν αποτελεί μέρος του θεωρείται «ορφανή». Εάν η συσκευή αποσυνδεθεί από το δίκτυο με την προβλεπόμενη διαδικασία εξόδου τότε δεν θεωρείται ορφανή. Εάν το επίπεδο δικτύου εντοπίσει πολλές αποτυχημένες

προσπάθειες επικοινωνίας τότε μπορεί να συμπεράνει ότι πρόκειται για ορφανή συσκευή.

Σε αυτή την περίπτωση μπορούν να γίνουν οι εξής ενέργειες:

- Επαναφορά (reset) του MAC και εκκίνηση διαδικασίας σύνδεσης σε δίκτυο
- Επαναπροσδιορισμός της ορφανής συσκευής: Σε αυτή την περίπτωση στέλνεται ειδοποίηση στον συντονιστή, ο οποίος ελέγχει αν η συσκευή ήταν προηγουμένως συσχετισμένη με αυτόν και σε αυτή την περίπτωση πραγματοποιείται ο επαναπροσδιορισμός και στέλνονται τις ρυθμίσεις του δικτύου στην συσκευή. Σε διαφορετική περίπτωση ο συντονιστής δεν εκτελεί καμία ενέργεια.

#### 5.4.4.2.9 Channel Scanning (MLME-SCAN)

Η δυνατότητα channel scanning παρέχεται σαν υπηρεσία από το MAC στο επίπεδο δικτύου και παρέχει πληροφορίες για την δραστηριότητα στον προσωπικό χώρο λειτουργίας (personal operating space, POS) της συσκευής. Υπάρχουν 4 είδη scan και είναι τα εξής:

- ED scan: Το επίπεδο ενέργειας σε κάθε κανάλι υπολογίζεται χρησιμοποιώντας την υπηρεσία ED(Energy Detection) του φυσικού στρώματος.
- Orphan scan: Η MLME της ορφανής συσκευής στέλνει ειδοποίηση στον συντονιστή κάθε καναλιού και αναμένει απάντηση για επαναπροσδιορισμό.
- Active scan: Σε αυτή την περίπτωση η MLME στέλνει μια αίτηση για beacon και έπειτα ενεργοποιεί τον δέκτη και αναμένει απάντηση. Μπορεί να χρησιμοποιηθεί από κάποιο συντονιστή που θέλει να δημιουργήσει το δικό του δίκτυο για να εντοπίσει τα αναγνωριστικά των PANs στην εμβέλεια του και να αποδώσει μοναδικό αναγνωριστικό στο δικό του.
- Passive scan: Σε αυτή την περίπτωση δεν έχουμε αποστολή αίτησης για beacon. Η συσκευή απλά καταγράφει την πληροφορία από το μέσο. Μπορεί να χρησιμοποιηθεί από μια συσκευή που δεν ανήκει σε κάποιο δίκτυο για να εντοπίσει κάποιο συντονιστή.

#### 5.4.4.2.10 Beacon Notification (MLME-BEACON-NOTIFY)

Όταν μια συσκευή λαμβάνει ένα πλαίσιο beacon, η MLME στέλνει την πληροφορία που βρίσκεται στις παραμέτρους του στο επίπεδο δικτύου. Επίσης στέλνεται και ο δείκτης ποιότητα ζεύξης(LQI).

#### 5.4.4.2.11 Συγχρονισμός με τον συντονιστή (MLME-SYNC και MLME-SYNC-LOSS)

Το επίπεδο δικτύου μιας συσκευής σε ένα beacon-enabled δίκτυο μπορεί να ζητήσει το συγχρονισμό με τον συντονιστή. Αυτό συμβαίνει είτε με την λήψη ενός beacon, είτε με συνεχόμενη παρακολούθηση των beacons. (beacon tracking). Στην τελευταία περίπτωση η συσκευή ενεργοποιεί τον δέκτη της σε περιοδική βάση ακριβώς πριν την αναμενόμενη άφιξη του beacon.

#### 5.4.4.2.12 Αίτηση για δεδομένα από τον συντονιστή (MLME-POLL)

Ο συντονιστής του δικτύου μπορεί να ενημερώσει μέσω των πλαισίων beacons μια συσκευή, ότι εκκρεμούν δεδομένα προς αποστολή για αυτή αποθηκευμένα σε αυτόν. Σε αυτή την περίπτωση η συσκευή αποστέλλει στον συντονιστή μια αίτηση για δεδομένα .

### 5.4.5 Πλαίσιο επιπέδου MAC

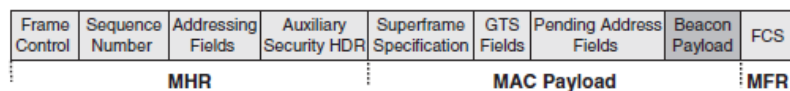
Υπάρχουν 4 είδη πλαισίων MAC:

- πλαίσιο beacon,
- πλαίσιο δεδομένων
- πλαίσιο επιβεβαίωσης
- πλαίσιο εντολής MAC.

Η γενική δομή του πλαισίου MAC αποτελείται από: την επικεφαλίδα MAC (MHR), το ωφέλιμο φορτίο (payload), και την MAC footer(MFR).

#### 5.4.5.1 Πλαίσιο beacon

Η δομή του πλαισίου beacon φαίνεται στην Εικόνα 5-13. Το πεδίο frame control ορίζει τον τύπο του πλαισίου, τα πεδία διευθύνσεων και άλλα πεδία ελέγχου. Το πεδίο sequence number ορίζει τον αύξοντα αριθμό των beacons. Τα πεδία διευθύνσεων περιλαμβάνουν τις διευθύνσεις πηγής και προορισμού και το πεδίο auxiliary security header είναι προαιρετικό και περιλαμβάνει πληροφορίες σχετικές με την ασφάλεια.



Εικόνα 5-13 Πλαίσιο beacon

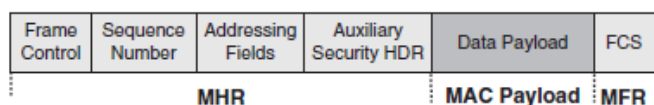
Το πεδίο superframe είναι και αυτό προαιρετικό και καθορίζει αν χρησιμοποιείται δομή superframe ή όχι. Τα πεδία GTS ορίζουν αν μια εγγυημένη χρονοσχισμή χρησιμοποιείται για αποστολή ή λήψη καθώς και μια λίστα με όλες τις GTS που έχουν αποδοθεί. Το πεδίο pending address fields πληροφορεί για τις διευθύνσεις συσκευών για τις οποίες εκκρεμούν δεδομένα προς αποστολή στο συντονιστή. Το

πεδίο beacon payload είναι προαιρετικό και μπορεί να χρησιμοποιηθεί από το επίπεδο δικτύου.

Τέλος το πεδίο FCS(Frame Check Sequence) του footer χρησιμοποιείται για να ελεγχθεί αν υπήρξε κάποιο σφάλμα με το πλαίσιο.

#### 5.4.5.2 Πλαίσιο δεδομένων

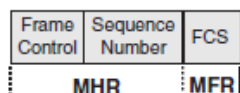
Η δομή του πλαισίου δεδομένων φαίνεται στην Εικόνα 5-14. Το ωφέλιμο φορτίο παρέχεται από το επίπεδο δικτύου και αναφέρεται και ως MSDU. Τα πεδία είναι παρόμοια με το πλαίσιο beacon εκτός από τα πεδία superframe specification, GTS fields και pending address fields που δεν είναι παρόντα εδώ.



Εικόνα 5-14 Πλαίσιο δεδομένων MAC

#### 5.4.5.3 Πλαίσιο επιβεβαίωσης

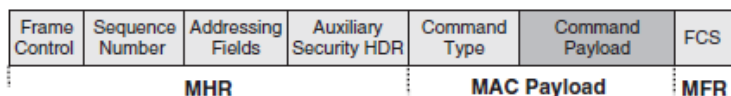
Η δομή του πλαισίου επιβεβαίωσης φαίνεται στην Εικόνα 5-15. Δεν εμπεριέχει ωφέλιμο φορτίο και στέλνεται για να επιβεβαιώσει επιτυχή λήψη ενός πακέτου.



Εικόνα 5-15 Πλαίσιο επιβεβαίωσης MAC

#### 5.4.5.4 Πλαίσιο εντολής MAC

Η δομή του πλαισίου εντολής φαίνεται στην Εικόνα 5-16. Το πεδίο command type ορίζει τον τύπο της εντολής πχ αίτηση για σύνδεση σε δίκτυο, αίτηση για δεδομένα κλπ. Το ωφέλιμο φορτίο περιέχει την ίδια την εντολή.



Εικόνα 5-16 Πλαίσιο εντολής MAC

### 5.4.6 Συνοπτική παρουσίαση των αρμοδιοτήτων του επιπέδου MAC

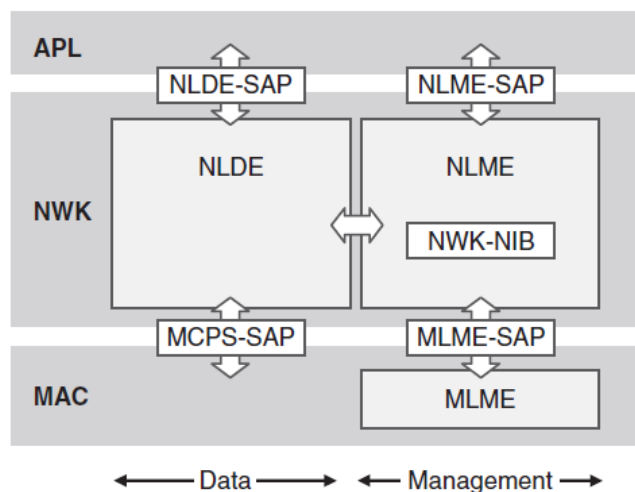
Οι αρμοδιότητες του επιπέδου MAC είναι:

- Η δημιουργία των πλαισίων beacons (αν η συσκευή είναι συντονιστής)

- Συγχρονισμός με τα beacons (σε beacon-enabled δίκτυο)
- Η χρησιμοποίηση του CSMA/CA για πρόσβαση στο μέσο
- Η διαχείριση των GTS
- Η παροχή αξιόπιστης ζεύξης μεταξύ δυο ομότιμων οντοτήτων MAC
- Παροχή υπηρεσιών σύνδεσης και αποσύνδεσης από το δίκτυο
- Παροχή υποστήριξης για ασφάλεια. Το επίπεδο MAC είναι υπεύθυνο για την δικιά του ασφάλεια, αλλά τα ανώτερα επίπεδα καθορίζουν το επίπεδο ασφαλείας που θα χρησιμοποιηθεί.

## 5.5 Zigbee Επίπεδο δικτύου

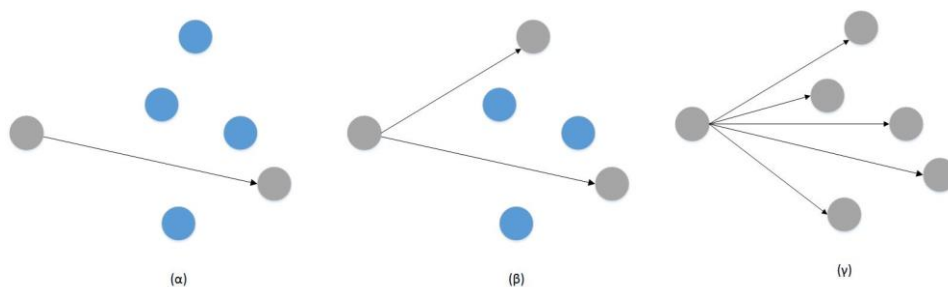
Το επίπεδο δικτύου εξασφαλίζει την λειτουργικότητα του 802.15.4 ελέγχοντας το επίπεδο MAC μέσω των primitives. Παρόμοια με τα υπόλοιπα επίπεδα, το επίπεδο δικτύου διαθέτει την οντότητα NLME (NWK Layer Management Entity) που είναι υπεύθυνη για την διαχείριση των υπηρεσιών και την NLDE (NWK Layer Data Entity) που είναι υπεύθυνη για την μετάδοση των δεδομένων. Αυτές οι οντότητες είναι προσβάσιμες από το ανώτερο επίπεδο εφαρμογής διαμέσου του NLME-SAP και NLDE-SAP αντίστοιχα (Εικόνα 5-17). Επίσης το επίπεδο δικτύου διαθέτει την δικιά του βάση πληροφοριών, γνωστή ως Network-IB (Network Information Base), όπου βρίσκονται αποθηκευμένες οι σταθερές και τα χαρακτηριστικά του επιπέδου. Οι σταθερές ξεκινούν με *nwkc* και τα χαρακτηριστικά με *nwk*.



Εικόνα 5-17 Υπηρεσίες επιπέδου δικτύου και διασύνδεση με επίπεδο εφαρμογής

Το επίπεδο δικτύου ενός συντονιστή Zigbee αναθέτει 16-bits διευθύνσεις δικτύου σε κάθε συσκευή στο δίκτυο. Επίσης αναθέτει και 64-bits MAC διευθύνσεις εάν μια συσκευή εισέλθει στο δίκτυο και χρειάζεται μια.

Ο μηχανισμός επικοινωνίας μπορεί να διαχωριστεί σε τρεις γενικές κατηγορίες: broadcast, multicast και unicast. Ένα broadcast μήνυμα προορίζεται για όλες τις συσκευές του δικτύου που θα το λάβουν. Ένα multicast μήνυμα προορίζεται για μια συγκεκριμένη ομάδα συσκευών του δικτύου. Τέλος, unicast χρησιμοποιείται όταν το μήνυμα προορίζεται για μια και μόνο συσκευή. Ένα μήνυμα unicast περιέχει την ακριβή διεύθυνση της συσκευής παραλήπτη. Εκτός και αν ορίζεται διαφορετικά, ο μηχανισμός unicast είναι ο προκαθορισμένος τρόπος επικοινωνίας. Οι άλλοι δυο μηχανισμοί αναλύονται στην επόμενη ενότητα.



Εικόνα 5-18 Μηχανισμοί επικοινωνίας α)unicast β)multicast γ)broadcast

## 5.5.1 Μηχανισμοί Επικοινωνίας

### 5.5.1.1 Broadcast

Στον μηχανισμό broadcast το μήνυμα προορίζεται για όλες τις συσκευές που χρησιμοποιούν ένα συγκεκριμένο κανάλι, ανεξάρτητα από την διεύθυνση τους. Κάθε φορά που μια συσκευή λαμβάνει ένα πακέτο, ελέγχει την διεύθυνση προορισμού σε αυτό για να δει αν αποτελεί παραλήπτη. Στο broadcast χρησιμοποιείται short addressing δηλαδή χρησιμοποιούνται 16-bit διευθύνσεις δικτύου και η διεύθυνση προορισμού τίθεται στην τιμή 0xFFFF. Αυτή η διεύθυνση γίνεται αποδεκτή από όλες τις συσκευές του δικτύου και λαμβάνουν τα broadcast πακέτα. Το υποεπίπεδο APS του επιπέδου εφαρμογής που θα αναλυθεί στην επόμενη ενότητα είναι αυτό που εκκινεί τον μηχανισμό broadcast για μια μετάδοση χρησιμοποιώντας την υπηρεσία δεδομένων του επιπέδου δικτύου.

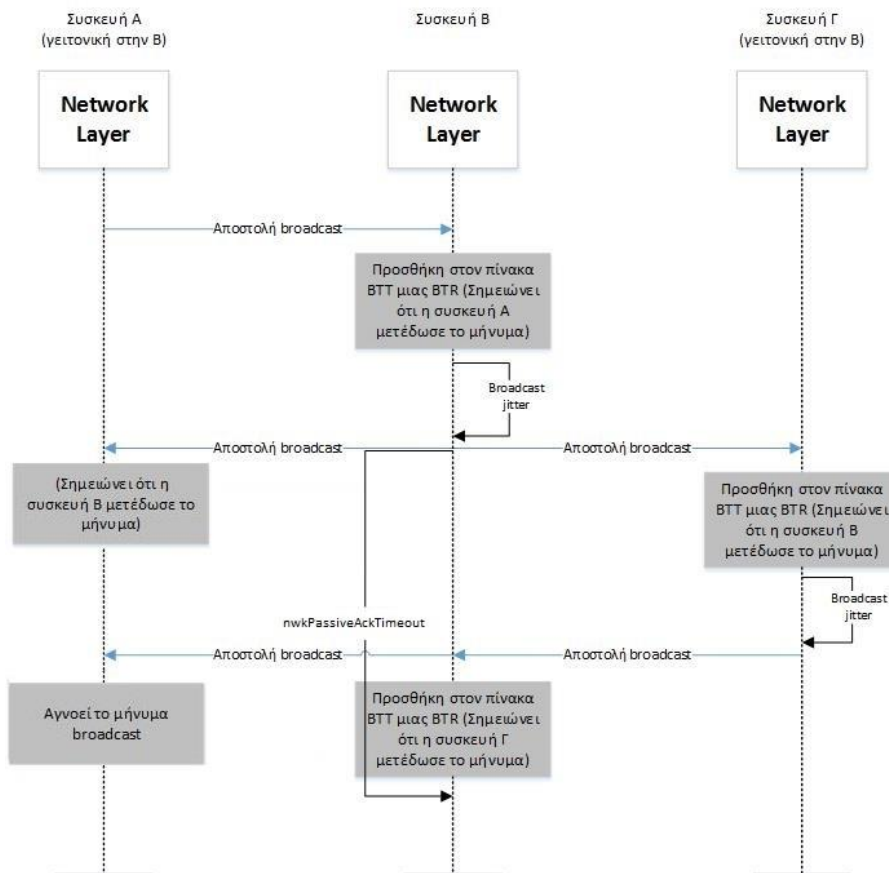
Σε ένα μεγάλο δίκτυο, είναι δύσκολο να αναμένονται επιβεβαιώσεις στον αρχικό αποστολέα, από κάθε συσκευή που λαμβάνει το broadcast μήνυμα. Για αυτό το λόγο οι τελικοί παραλήπτες δεν επιτρέπεται να στέλνουν επιβεβαιώσεις. Για την αξιόπιστη λοιπόν μεταφορά χρησιμοποιείται ένας μηχανισμός που ονομάζεται passive acknowledgment mechanism. Σε αυτόν ο Zigbee coordinator και οι routers επαληθεύουν ότι οι γειτονικές τους συσκευές έχουν επαναμεταδώσει επιτυχώς το μήνυμα. Αφού μια συσκευή μεταδώσει ένα broadcast μήνυμα, εισέρχεται σε κατάσταση λήψης (receive mode) και περιμένει μέχρι το ίδιο μήνυμα να ξανασταλθεί από κάποια γειτονική συσκευή. Έτσι λαμβάνει την ένδειξη ότι το μήνυμα που έστειλε, λήφθηκε και αναμεταδόθηκε με επιτυχία. Επειδή όπως βλέπουμε κατά τον μηχανισμό broadcast, το μήνυμα αναμεταδίδεται από πολλές

συσκευές, υπάρχει ο κίνδυνος σύγκρουσης εξαιτίας του προβλήματος του κρυμμένου κόμβου (ενότητα 5.4.1.1). Για να μειωθεί αυτή η πιθανότητα το επίπεδο δικτύου ορίζει ότι πριν από κάθε επαναμετάδοση, η συσκευή πρέπει να περιμένει για μια τυχαία περίοδο χρόνου, που ονομάζεται *broadcast jitter*.

Ο συντονιστής Zigbee και οι routers διατηρούν αρχείο με όλα τα broadcast μηνύματα σε ένα πίνακα που ονομάζεται *broadcast transaction table* (BTT). Οι εγγραφές στον πίνακα ονομάζονται *broadcast transaction records* (BTR) και περιέχουν την διεύθυνση πηγής του μηνύματος, καθώς και ένα *sequence number*. Κάθε router πρέπει να έχει την δυνατότητα να διατηρεί στον buffer του επιπέδου δικτύου τουλάχιστον ένα πλαίσιο. Αυτό βοηθά σε περίπτωση που χρειαστεί επαναμετάδοση του πλαισίου.

Στο Εικόνα 5-19 φαίνεται ο μηχανισμός broadcast για ένα μήνυμα σε ένα δίκτυο τριών συσκευών. Κάθε φορά που μια συσκευή λαμβάνει το μήνυμα από μια γειτονική της ανανεώνει τον πίνακα BTT. Η συσκευή A ξεκινά την broadcast μετάδοση και λαμβάνει το μήνυμα πάλι πίσω από την συσκευή B. Την δεύτερη φορά που λαμβάνει το μήνυμα το αγνοεί καθώς έχει ήδη κάνει την διαδικασία του *passive acknowledgment*. Αντίστοιχα η συσκευή B κάνει broadcast στις A και B και αναμένει για *passive acknowledgment* (την μετάδοση πίσω από την Γ). Εάν δεν την λάβει μετά από κάποιο χρόνο (*nwkPassiveAckTimeout*), επαναμεταδίδει το μήνυμα.





Εικόνα 5-19 Μηχανισμός broadcast σε δίκτυο 3 συσκευών

### 5.5.1.2 Multicast

Στον μηχανισμό multicast, το μήνυμα μεταδίδεται σε μια ομάδα (group) συσκευών μέσα σε ένα δίκτυο. Κάθε τέτοια ομάδα συσκευών προσδιορίζεται από ένα 16-bit ID. Μια συσκευή μπορεί να ανήκει σε περισσότερες από μια τέτοιες ομάδες. Κάθε συσκευή διατηρεί ένα πίνακα με όλα τα ID των ομάδων multicast στις οποίες ανήκει που ονομάζεται multicast table (nwkGroupIDTable).

Μια συσκευή δεν χρειάζεται να είναι μέλος μιας ομάδας multicast για να μπορεί να χρησιμοποιεί τον μηχανισμό και να στέλνει σε μια ομάδα. Υπάρχουν δυο τρόποι λειτουργίας στον μηχανισμό multicast: η λειτουργία μέλους (member-mode) και η λειτουργία μη-μέλους (nonmember-mode). Στην πρώτη περίπτωση ένα μέλος της ομάδας εκκινεί τον μηχανισμό για να στείλει σε όλα τα υπόλοιπα μέλη της. Στην περίπτωση μη-μέλους, ο μηχανισμός εκκινείται από μια συσκευή που δεν ανήκει στην ομάδα και στέλνεται αρχικά σε μια συσκευή-μέλος από όπου πλέον προωθείται σε όλες τις υπόλοιπες συσκευές-μέλη.

Κατά τον μηχανισμό multicast, το μήνυμα ουσιαστικά στέλνεται με τον μηχανισμό broadcast και καταγράφεται στον BTT των συσκευών (members και nonmembers) από τις οποίες προωθείται, η λήψη όμως του μηνύματος από μια συσκευή και η προώθηση του στο ανώτερο επίπεδο γίνεται μόνο όταν η συσκευή είναι μέλος της ομάδας στην οποία απευθύνεται. Επίσης δεν έχουμε passive acknowledgment.

Μια περίπτωση χρήσης του μηχανισμού multicast είναι σε μια εφαρμογή ελέγχου φωτισμού, όπου μια συσκευή που λειτουργεί σαν διακόπτης στέλνει ένα πακέτο για να ανάψει ή να σβήσει μια ομάδα φωτιστικών σε ένα σπίτι. Το ίδιο αποτέλεσμα μπορεί να επιτευχθεί και με συνεχόμενα unicast σε κάθε φωτιστικό ξεχωριστά, αλλά ο μηχανισμός multicast είναι πιο αποδοτικός στην περίπτωση αυτή.

Στο πρότυπο Zigbee, το multicast χρησιμοποιείται μόνο για μετάδοση πλαισίων δεδομένων και δεν επιτρέπει την μετάδοση πλαισίων εντολής.

### **5.5.1.3 Many to one**

Ένα άλλο σενάριο επικοινωνίας είναι όταν μια συσκευή λαμβάνει μηνύματα από πολλές συσκευές στο ίδιο δίκτυο. Αυτή η περίπτωση είναι γνωστή ως επικοινωνία many-to-one. Η συσκευή αυτή ονομάζεται sink και φροντίζει να δημιουργήσει διαδρομές επικοινωνίας με όλους του routers και coordinators σε μια ακτίνα.

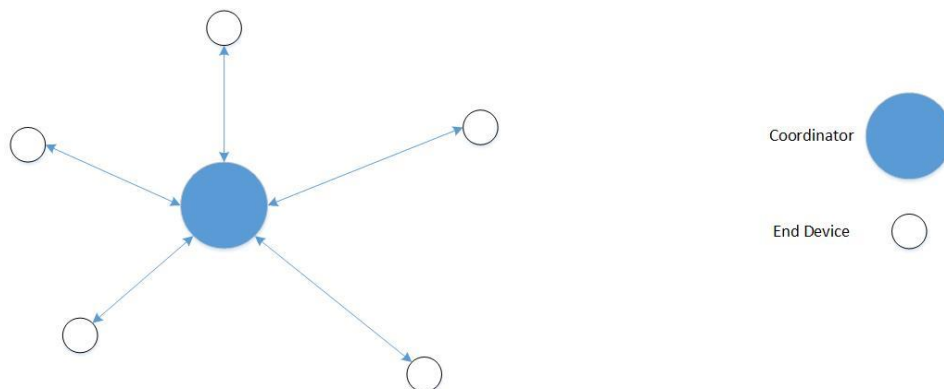
## **5.5.2 Τοπολογίες**

Η τοπολογία του δικτύου καθορίζεται και διαχειρίζεται από το επίπεδο δικτύου. Οι διαθέσιμες τοπολογίες δικτύου όπως ορίζονται από το 802.15.4 είναι δυο:

1)τοπολογία αστέρα και 2)τοπολογία ομότιμων (peer-to peer). Η δεύτερη τοπολογία χωρίζεται σε άλλες δυο κατηγορίες ανάλογα με τους κανόνες επικοινωνίας μεταξύ των ομότιμων: 1)τοπολογία δέντρου(tree) και 2)τοπολογία πλέγματος(mesh).

### **5.5.2.1 Τοπολογία αστέρα**

Στην τοπολογία αστέρα, που φαίνεται στην Εικόνα 5-20, κάθε συσκευή μπορεί να επικοινωνεί μόνο με τον PAN coordinator. Η δημιουργία ενός τέτοιου δικτύου γίνεται από τον PAN coordinator ο οποίος επιλέγει το αναγνωριστικό του δικτύου (PAN ID), ελέγχοντας ότι είναι μοναδικό στην σφαίρα εμβέλειας του. Ως PAN coordinator μπορεί να οριστεί οποιαδήποτε συσκευή Zigbee router ή Zigbee coordinator.

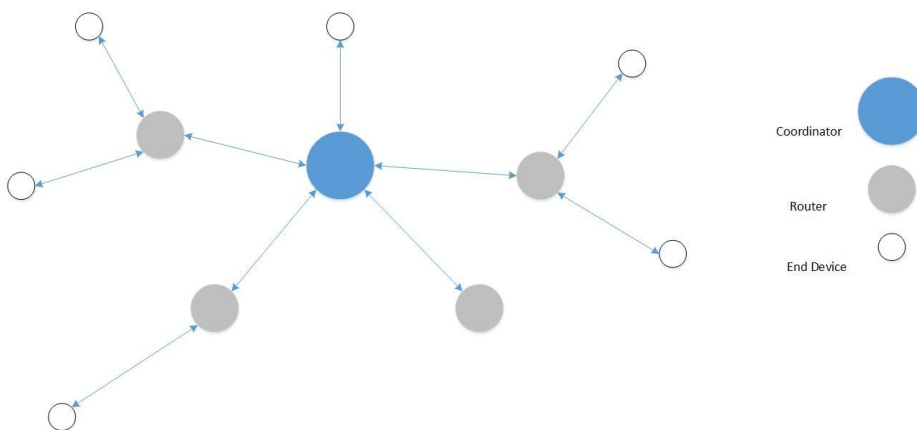


Εικόνα 5-20 Τοπολογία αστέρα

### 5.5.2.2 Τοπολογίες ομότιμων

#### 5.5.2.2.1 Tree Topology

Στην τοπολογία δέντρου που φαίνεται στην Εικόνα 5-21, η δημιουργία του δικτύου γίνεται από μια συσκευή Zigbee coordinator που ονομάζεται ρίζα (root). Κάθε συσκευή coordinator και router μπορεί να λειτουργεί σαν συσκευή γονιός (parent device) και να συσχετίζεται με άλλες συσκευές που θεωρούνται παιδιά της. Τα μηνύματα που αφορούν μια συσκευή παιδί δρομολογούνται σε αυτή μέσω της συσκευής γονιού. Οι end devices μπορούν να είναι μόνο συσκευές παιδιά καθώς δεν διαθέτουν δυνατότητα προώθησης και δρομολόγησης μηνυμάτων.



Εικόνα 5-21 Τοπολογία δέντρου

Το βάθος του δικτύου (network depth) ορίζεται ως ο ελάχιστος αριθμός hops που απαιτούνται για να φτάσει ένα πλαίσιο στον coordinator διαμέσου ζεύξεων παιδιού-γονέα. Για παράδειγμα τα παιδιά του coordinator έχουν βάθος 1. Ο ίδιος ο coordinator έχει βάθος 0.

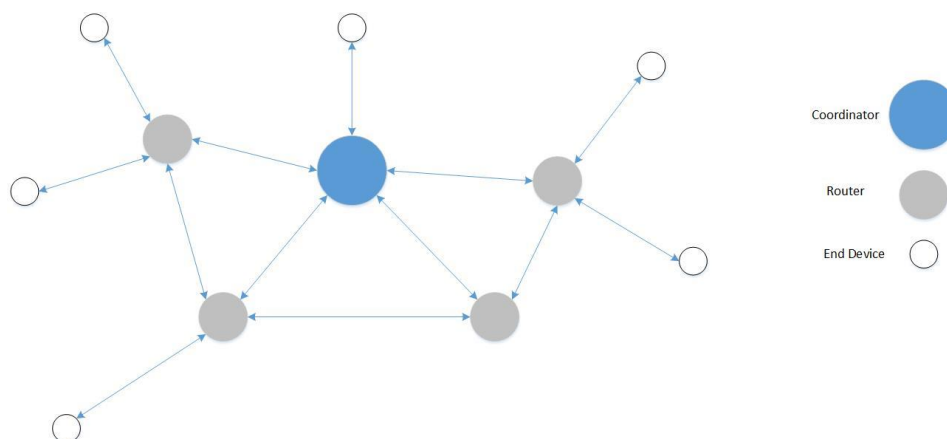
Η τοπολογία αστέρα θα μπορούσε να θεωρηθεί υποπερίπτωση της τοπολογίας δέντρου όπου ο μόνος γονιός είναι ο coordinator και όλες οι συσκευές έχουν βάθος 1.

#### 5.5.2.2.1 Απόδοση διευθύνσεων (Address Allocation)

Αυτή η δομή της τοπολογίας δέντρου αποτελεί και την βάση για τον αλγόριθμο κατανομής και απόδοσης διευθύνσεων στους κόμβους του δικτύου. Ο Zigbee coordinator ορίζει τον μέγιστο αριθμό routers και end-devices που μπορεί να έχει ως παιδιά κάθε router και το μέγιστο βάθος. Οπότε κάθε router ανάλογα με το βάθος στο οποίο βρίσκεται λαμβάνει ένα εύρος διευθύνσεων (16-bit ακεραίων) από τους οποίους ο πρώτος λαμβάνεται από τον ίδιο και οι υπόλοιποι είναι διαθέσιμοι για τα παιδιά του.

#### 5.5.2.2.2 Τοπολογία πλέγματος (mesh)

Στην τοπολογία πλέγματος, σε αντίθεση με την τοπολογία δέντρου, δεν υπάρχουν ιεραρχικοί κανόνες. Μια συσκευή σε ένα τέτοιο δίκτυο μπορεί να επιχειρήσει να επικοινωνήσει με οποιαδήποτε άλλη συσκευή, είτε κατευθείαν, είτε εκμεταλλευόμενη τις συσκευές με δυνατότητα προώθησης (routers και coordinators). Σε μια τέτοια τοπολογία η διαδρομή από την πηγή στον προορισμό δημιουργείται κατά απαίτηση και μπορεί να αλλάξει σε περίπτωση αλλαγής της τοπολογίας. Αυτή η δυνατότητα του mesh δικτύου να δημιουργεί και να αλλάζει δυναμικά τις διαδρομές μεταξύ των κόμβων αυξάνει την αξιοπιστία του ασύρματου δικτύου. Εάν για οποιοδήποτε λόγο, η πηγή δεν μπορεί να επικοινωνήσει με τον προορισμό χρησιμοποιώντας την εγκατεστημένη διαδρομή, οι συσκευές του δικτύου με δυνατότητα δρομολόγησης συνεργάζονται για να βρουν εναλλακτική διαδρομή. Η τοπολογία πλέγματος φαίνεται στην Εικόνα 5-22.



Εικόνα 5-22 Τοπολογία πλέγματος

### 5.5.3 Δρομολόγηση (routing)

Δρομολόγηση (routing) είναι η διαδικασία επιλογής της διαδρομής ενός πακέτου για να φτάσει στην συσκευή προορισμού. Ο Zigbee coordinator και οι Zigbee routers είναι υπεύθυνοι για την εύρεση και διατήρηση αυτών των διαδρομών σε ένα δίκτυο καθώς οι end devices δεν διαθέτουν τέτοια δυνατότητα.

Παράμετροι όπως η ποιότητα ζεύξης, ο αριθμός των hops και η κατανάλωση ενέργειας χρησιμοποιούνται για να υπολογιστεί η βέλτιστη διαδρομή για ένα πακέτο. Σε κάθε ζεύξη υπολογίζεται τελικά ένα κόστος ζεύξης (link cost). Η πιθανότητα επιτυχούς μεταφοράς του πακέτου σε κάθε ζεύξη καθορίζει το κόστος της. Όσο μικρότερη είναι η πιθανότητα αυτή, τόσο μεγαλύτερο είναι το κόστος της ζεύξης. Στο πρότυπο Zigbee ο υπολογισμός του κόστους βασίζεται στον LQI (Link Quality Indicator) που αναλύθηκε στην ενότητα 5.3.3.

Οι συσκευές σε ένα δίκτυο Zigbee διαθέτουν κάποιους πίνακες που περιέχουν πληροφορίες που αφορούν την δρομολόγηση και την διαδικασία εύρεσης νέων διαδρομών. Αυτοί είναι:

- **Routing table** (πίνακας δρομολόγησης): Χρησιμοποιείται κατά την δρομολόγηση ενός μηνύματος για την εύρεση του επόμενου κόμβου (hop) της διαδρομής. Είναι διαθέσιμος σε coordinators και routers.
- **Route discovery table** (πίνακας εύρεσης διαδρομής): Χρησιμοποιείται κατά την εύρεση μιας καινούργιας διαδρομής. Περιέχει τα κόστη των διάφορων διαδρομών, την διεύθυνση της συσκευής που ζήτησε την δρομολόγηση και την διεύθυνση της προηγούμενης συσκευής που αναμετάδωσε το αίτημα στην τρέχουσα. Η τελευταία συσκευή επιστρέφει στην πηγή (συσκευή που έκανε αίτηση εύρεσης διαδρομής) το αποτέλεσμα. Είναι διαθέσιμος σε coordinators και routers.
- **Neighbor table** (πίνακας γειτνίασης): Περιέχει πληροφορίες για όλες τις συσκευές που βρίσκονται μέσα στην εμβέλεια της τρέχουσας συσκευής. Ενημερώνεται κάθε φορά που η συσκευή λαμβάνει ένα πακέτο από μια γειτονική της. Χρησιμοποιείται για την εύρεση γειτονικού router ή σε περίπτωση που επιχειρείται επανασύνδεση στο δίκτυο.

#### 5.5.3.1 Route discovery

Το επίπεδο εφαρμογής μπορεί να κάνει αίτηση (request) για χρήση της υπηρεσίας NLME-ROUTE-DISCOVERY που θα δούμε και παρακάτω, για την εύρεση διαδρομών για unicast, multicast και many-to-one επικοινωνίες. Το πρότυπο Zigbee δεν επιτρέπει την χρήση της υπηρεσίας για επικοινωνία broadcast. Εάν η αίτηση περιέχει την διεύθυνση μιας συγκεκριμένης συσκευής τότε εκτελείται εύρεση διαδρομής unicast. Εάν διεύθυνση προορισμού είναι ένα 16-bit ID ομάδας συσκευών τότε εκτελείται εύρεση διαδρομής multicast. Τέλος εάν δεν παρέχεται διεύθυνση προορισμού τότε θεωρείται many-to-one επικοινωνία και η τρέχουσα

συσκευή λαμβάνει τον ρόλο του sink. Μόνο οι Zigbee coordinators και routers έχουν την δυνατότητα να βρίσκουν διαδρομές στο δίκτυο.

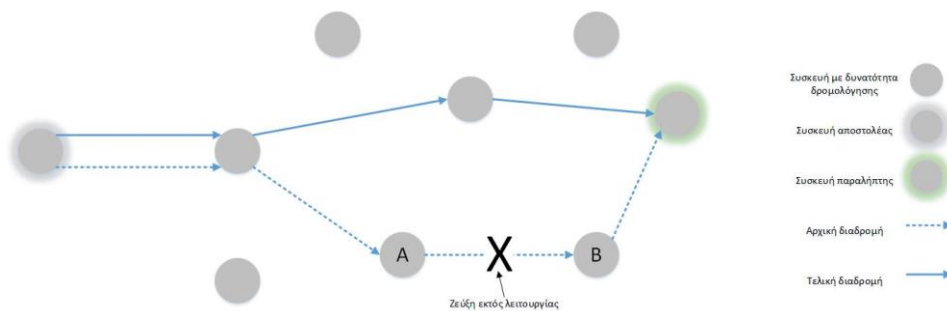
Η διαδικασία της εύρεσης διαδρομής για unicast επικοινωνία είναι η εξής: η συσκευή αποστολέας κάνει broadcast την αίτηση εύρεσης (route request) σε όλες τις συσκευές στην εμβέλεια της. Όλες οι συσκευές εκτός των end devices λαμβάνουν το μήνυμα, ενημερώνουν τους πίνακες τους και το κόστος διαδρομής στην αίτηση και επαναλαμβάνουν το broadcast έως ότου η αίτηση φτάσει την συσκευή προορισμού. Τελικά η συσκευή προορισμός λαμβάνει όλες τις αιτήσεις με τα κόστη των διάφορων διαδρομών και επιλέγει την βέλτιστη. Έπειτα στέλνει πίσω στον αποστολέα την απάντηση (route reply). Στην περίπτωση επικοινωνίας multicast η διαδικασία είναι παρόμοια μόνο που όλες οι συσκευές που ανήκουν στην ομάδα πρέπει να στείλουν route replies στον αποστολέα.

#### 5.5.3.1.1 Source Routing

Το επίπεδο δικτύου του προτύπου Zigbee επιτρέπει την χρήση source routing. Στον μηχανισμό αυτό ο αποστολέας του μηνύματος καθορίζει τις συσκευές στις οποίες μπορεί να προωθηθεί το μήνυμα, το οποίο περιέχει και τις διευθύνσεις τους. Επομένως οι routers για την αναζήτηση του επόμενου κόμβου κοιτούν πλέον την λίστα του αποστολέα και όχι τον δικό του πίνακα δρομολόγησης.

#### 5.5.3.2 Route Maintenance and Repair

Μια διαδρομή η οποία χρησιμοποιείται για την μεταφορά μηνυμάτων σε ένα δίκτυο μπορεί να σταματήσει να έχει αυτήν την ικανότητα. Οι λόγοι για αυτό είναι είτε ένας κόμβος (ένας router που έκλεισε) είτε μια ζεύξη (ένα φυσικό εμπόδιο μεταξύ 2 κόμβων) που έχει βγει εκτός λειτουργίας. Εάν μια αποστολή αποτύχει λόγω αποτυχίας ζεύξης (link failure) για ένα προκαθορισμένο αριθμό αποστολών τότε θεωρείται πλέον εκτός λειτουργίας. Σε αυτή την περίπτωση το πρωτόκολλο εκκινεί μια διαδικασία επιδιόρθωσης της διαδρομής. Η Εικόνα 5-23 δείχνει μια διαδικασία επιδιόρθωσης σε ένα δίκτυο με τοπολογία πλέγματος (mesh).



Εικόνα 5-23 Διαδικασία επιδιόρθωσης διαδρομής

Η ζεύξη μεταξύ των κόμβων A και B βγαίνει εκτός λειτουργίας και εκκινείται η διαδικασία επιδιόρθωσης. Η διαδικασία αυτή είναι παρόμοια με την διαδικασία

route discovery μόνο που εκκινείτε από την συσκευή A και όχι από την συσκευή αποστολέα του μηνύματος. Μετά από συνεχόμενα broadcast όπως αναλύθηκε στο route discovery βρίσκεται μια καινούργια διαδρομή για την αποστολή του μηνύματος. Επειδή χρησιμοποιείται αίτηση εύρεσης (route request) όπως και στο route discovery, έχουμε διαχωρισμό των δυο διαδικασιών σύμφωνα με ένα bit (route repair) στην επικεφαλίδα του πλαισίου.

#### **5.5.4 Υπηρεσίες επιπέδου δικτύου**

Όπως έχει ήδη αναφερθεί το επίπεδο δικτύου διαθέτει τις οντότητες NLDE και NLME για την διαχείριση των δεδομένων και των υπηρεσιών αντίστοιχα.

##### **5.5.4.1 Υπηρεσία δεδομένων επιπέδου δικτύου (NLDE-DATA)**

Το επίπεδο δικτύου παρέχει την υπηρεσία δεδομένων του στο επίπεδο εφαρμογής. Τα δεδομένα προς μετάδοση παρέχονται ως APDU (APS Sublayer Protocol Data Unit) και αποτελούν το ωφέλιμο φορτίο για το επίπεδο δικτύου ή αλλιώς την NSDU. Το επίπεδο δικτύου προσθέτοντας την επικεφαλίδα με τα απαραίτητα στοιχεία διαμορφώνει την NPDU.

Σε περίπτωση αποστολής το APS Sublayer ζητάει την μετάδοση στο αντίστοιχο επίπεδο μιας άλλης συσκευής, του πλαισίου. Επίσης περιορίζει την απόσταση που μπορεί να διανύσει το πλαίσιο μέσα στο δίκτυο θέτοντας την ακτίνα (radius parameter) και προσθέτοντας και έναν αύξοντα αριθμό σε αυτό (sequence number). Στην συσκευή λήψης το επίπεδο δικτύου παρέχει τα δεδομένα, τον αύξοντα αριθμό και το LQI στο δικό της APS Sublayer.

##### **5.5.4.2 Υπηρεσία διαχείρισης επιπέδου δικτύου (NLME)**

Οι βασικές αρμοδιότητες της υπηρεσίας διαχείρισης του επιπέδου δικτύου είναι: ο σχηματισμός του δικτύου, η είσοδος και έξοδος από δίκτυο, η εύρεση διαδρομής και η επιδιόρθωση και συντήρηση διαδρομής. Οι υπηρεσίες δρομολόγησης εξετάστηκαν σε προηγούμενη ενότητα. Παρακάτω αναλύονται οι υπόλοιπες (στις παρενθέσεις αναφέρονται τα ονόματα των service primitives).

###### **5.5.4.2.1 Εύρεση υπάρχοντος δικτύου (NLME-NETWORK-DISCOVERY)**

Χρησιμοποιείται για την εύρεση εν ενεργεία δικτύων στην περιοχή λειτουργίας (POS) της συσκευής. Επιστρέφεται το NLME-NETWORK-DISCOVERY.confirm φέρνοντας πληροφορίες για τα δίκτυα που βρέθηκαν μέσω της κατάστασης στην οποία έχει τεθεί.

###### **5.5.4.2.2 Δημιουργία νέου δικτύου (NLME-NETWORK-FORMATION)**

Χρησιμοποιείται όταν θέλουμε η εν λόγω συσκευή να δημιουργήσει ένα νέο δίκτυο ως Coordinator. Το πρώτο βήμα είναι να εκτελέσει τις διαδικασίες ED scan και active scan του επιπέδου MAC ώστε να επιλέξει κάποιο διαθέσιμο. Έπειτα

προσδίδει στο δίκτυο ένα διαθέσιμο 16-bit αναγνωριστικό (PAN Identifier) που αποτελεί και την διεύθυνση δικτύου του ίδιου του coordinator. Από τις πρώτες εργασίες του coordinator είναι η διαμόρφωση της δομής του superframe χρησιμοποιώντας τις υπηρεσίες του MAC.

#### 5.5.4.2.3 Establishing the Device as a Router (NLME-START-ROUTER)

Το NLME-START-ROUTER.request παράγεται ώστε ο router να αρχίσει να εκτελεί μια σειρά από εργασίες που βρίσκονται υπό την αρμοδιότητά του. Οι εργασίες αυτές είναι η αποδοχή αιτήσεων από άλλες συσκευές που θέλουν να συνδεθούν στο δίκτυό του, η δρομολόγηση των πλαισίων και η λειτουργία route discovery.

#### 5.5.4.2.4 Είσοδος και έξοδος από δίκτυο (NLME-JOIN, NLME-DIRECT-JOIN, NLME-LEAVE)

Το επίπεδο εφαρμογής χρησιμοποιεί το NLME-JOIN.request για να ζητήσει από το επίπεδο δικτύου να συνδεθεί σε κάποιο υπάρχον δίκτυο ως router ή ως end-device. Αφού λάβει λίστα με τα διαθέσιμα δίκτυα, επιλέγει την συσκευή γονιό και λαμβάνει διεύθυνση από αυτή. Μια εναλλακτική μέθοδος είναι αυτή του direct join (NLME-DIRECT-JOIN). Σε αυτή την περίπτωση η συσκευή γονιός έχει προκαθορισμένα παιδιά και στέλνει αίτηση σύνδεσης τους σε αυτή, στην γειτονική του περιοχή.

Αντίστοιχα μια συσκευή μπορεί να αποσυνδεθεί από ένα δίκτυο είτε από μόνη της, είτε με αίτηση από την συσκευή γονιό της χρησιμοποιώντας το NLME-LEAVE.request. Όταν αποσυνδεθεί, μπορούν να αποσυνδεθούν και τα παιδιά της (αν είναι router) και στην συνέχεια να βρουν άλλες συσκευές γονείς ή να συνδεθούν σε άλλο δίκτυο. Όταν η συσκευή που σκοπεύει να αποσυνδεθεί είναι coordinator ή router τότε κάνει broadcast την αίτηση αποσύνδεσης για να ενημερώσει όλες τις συσκευές ότι δεν μπορούν να την χρησιμοποιούν πλέον. Αντίθετα οι end-devices στέλνουν με unicast την αίτηση μόνο στην συσκευή γονιό τους. Τέλος και η συσκευή γονιός μπορεί να εκκινήσει την διαδικασία σε περίπτωση που θέλει να αποσυνδέσει ένα παιδί του στέλνοντας σε αυτό την αίτηση με unicast.

#### 5.5.4.2.5 Επαναφορά του επιπέδου δικτύου (NLME-RESET)

Το NLME-RESET.request επαναφέρει το επίπεδο δικτύου στην αρχική του κατάσταση. Πρώτα επαναφέρει το επίπεδο MAC και έπειτα την βάση δεδομένων του (NIB) και τους πίνακες δρομολόγησης στις προκαθορισμένες τιμές τους.

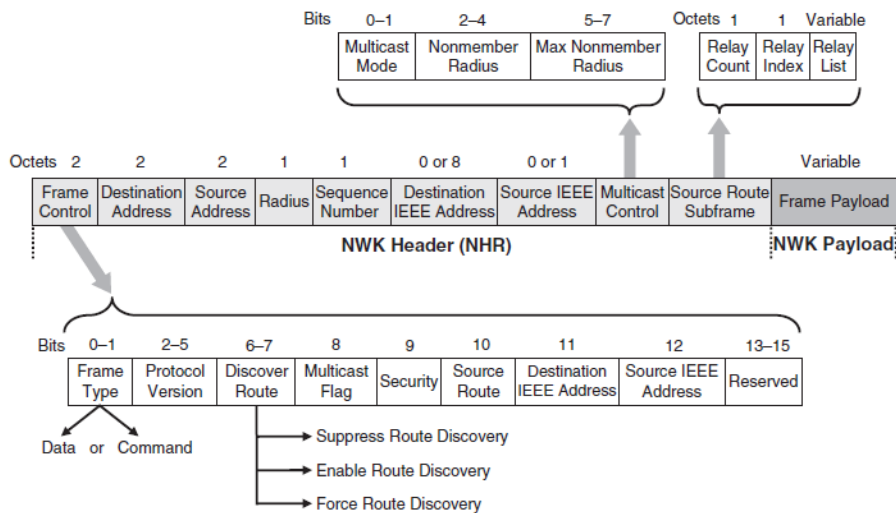
#### 5.5.4.2.6 Συγχρονισμός (NLME-SYNC)

Χρησιμοποιείται για να συγχρονιστεί μια συσκευή με τον coordinator ή για να ζητήσει την λήψη δεδομένων που εκκρεμούν για αυτή. Υπάρχουν δυο σενάρια συγχρονισμού: beacon enabled και non-beacon enabled. Στην περίπτωση beacon-enabled η συσκευή συγχρονίζεται με τον coordinator και ενημερώνεται για την συχνότητα των beacons με την βοήθεια της υπηρεσίας MLME-SET του MAC. Στην άλλη περίπτωση έχουμε χρήση polling (υπηρεσία MLME-POLL) για συγχρονισμό.



### 5.5.5 Πλαίσιο επιπέδου δικτύου

Η γενική δομή του πλαισίου δικτύου (NPDU) φαίνεται στην Εικόνα 5-24 και αποτελείται από την επικεφαλίδα (Network Header, NHR) και το ωφέλιμο φορτίο (Network payload).

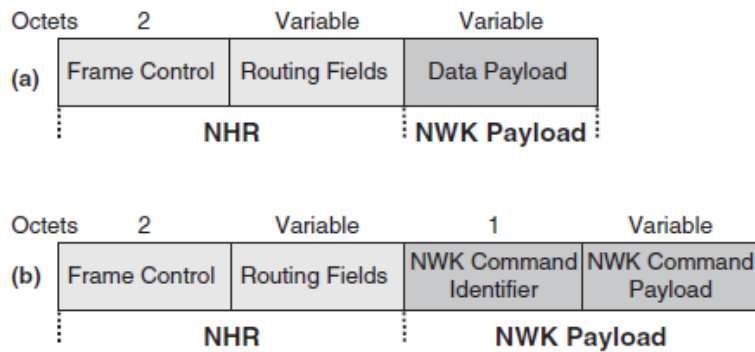


Εικόνα 5-24 Πλαίσιο επιπέδου δικτύου

Τα στοιχεία της επικεφαλίδας είναι:

- **Frame type:** περιλαμβάνει σήματα ελέγχου και πληροφορίες για το πακέτο όπως: αν είναι πλαίσιο δεδομένων ή εντολής, αν χρησιμοποιείται multicast ή source routing, καθώς και τον τρόπο χρήσης εύρεσης διαδρομής (source discovery).
- **Destination & Source address:** οι διευθύνσεις δικτύου (16 bit) των συσκευών δέκτη και αποστολέα αντίστοιχα.
- **Radius:** ο μέγιστος αριθμός hops που επιτρέπεται να διανύσει το πλαίσιο. Μειώνεται κατά ένα σε κάθε hop.
- **Sequence number:** αύξων αριθμός. Αυξάνεται κατά ένα σε κάθε νέο πακέτο.
- **Destination & Source IEEE address:** οι διευθύνσεις (64 bit) των συσκευών δέκτη και αποστολέα αντίστοιχα.
- **Multicast Control:** Σε περίπτωση που η τιμή του multicast flag είναι ένα, το πεδίο αυτό καθορίζει τις παραμέτρους του μηχανισμού.
- **Source Route Subframe:** Σε περίπτωση που η τιμή του source route είναι ένα, το πεδίο αυτό καθορίζει τις παραμέτρους του μηχανισμού.

Στην παρακάτω Εικόνα 5-25 φαίνεται η δομή του πλαισίου δεδομένων και εντολής αντίστοιχα



Εικόνα 5-25 Δομή πλαισίου α)δεδομένων β)εντολής επιπέδου δικτύου

Οι εντολές διακρίνονται με ένα 8-bit αναγνωριστικό (NWK Command Identifier) το οποίο μαζί με το ωφέλιμο φορτίο της εντολής διαμορφώνουν το ωφέλιμο φορτίο του πλαισίου εντολής επιπέδου δικτύου.

### 5.5.6 Συνοπτική παρουσίαση των αρμοδιοτήτων του επιπέδου δικτύου

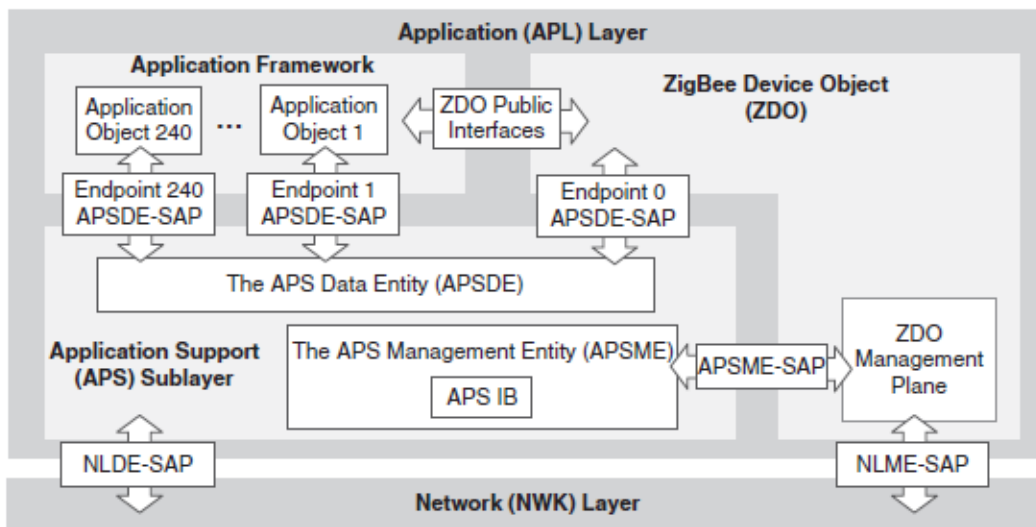
Οι αρμοδιότητες του επιπέδου δικτύου είναι:

- Διαχείριση νέων συσκευών
- Δημιουργία νέου δικτύου
- Σύνδεση και αποσύνδεση από δίκτυο
- Δρομολόγηση πλαισίων. Μόνο οι coordinators και οι routers έχουν αυτή την δυνατότητα
- Εύρεση και διατήρηση διαδρομών μεταξύ συσκευών
- Εύρεση γειτονικών συσκευών (one-hop neighbors) και διατήρηση σχετικών πληροφοριών
- Απόδοση διευθύνσεων δικτύου σε συσκευές. Μόνο οι coordinators και οι routers έχουν αυτή την δυνατότητα

### 5.6 Zigbee Επίπεδο εφαρμογής

Το επίπεδο εφαρμογής αποτελεί το ανώτερο επίπεδο που ορίζεται από την σουίτα του Zigbee. Αυτό αποτελείται από 3 μέρη: 1) το πρωτόκολλο ZDO (Zigbee Device Object), 2) το υποεπίπεδο APS (application support sublayer) και 3) το Application Framework. Η δομή του επιπέδου εφαρμογής φαίνεται στην Εικόνα 5-26. Το υποεπίπεδο APS αποτελεί τον συνδετικό κρίκο μεταξύ του επιπέδου δικτύου και του επιπέδου εφαρμογής και παρόμοια με τα υπόλοιπα επίπεδα παρέχει 2 ειδών

υπηρεσίες: δεδομένων και διαχείρισης. Η υπηρεσία δεδομένων (APS data service) παρέχεται από την APS Data Entity (APSD) και προσπελάζεται διαμέσου του APSDE-Service Access Point (SAP). Η υπηρεσία διαχείρισης αντίστοιχα παρέχεται από την APS Management Entity (APSM) και προσπελάζεται διαμέσου του APSME-SAP. Οι μεταβλητές και οι σταθερές του επιπέδου αυτού βρίσκονται αποθηκευμένες στην βάση APS Information Base (APS IB or AIB).



Εικόνα 5-26 Δομή επιπέδου εφαρμογής

Το Application Framework περιέχει τα αντικείμενα (application objects) που χρησιμοποιούνται για την διαχείριση και τον έλεγχο των επιπέδων σε μια συσκευή Zigbee. Τα application objects αναπτύσσονται από τον κάθε κατασκευαστή και αποτελούν το κύριο σημείο στο οποίο μια συσκευή προσαρμόζεται για κάποια συγκεκριμένη εφαρμογή. Μπορούν να υπάρχουν μέχρι 240 application objects σε μια συσκευή.

Το ZDO (Zigbee Device Object) παρέχει τον σύνδεσμο μεταξύ του APS και του application framework. Περιέχει τις λειτουργίες που είναι κοινές σε όλες τις εφαρμογές όπως για παράδειγμα τον καθορισμό του ρόλου μιας συσκευής (end-device, router, coordinator κλπ) αλλά και για την ανακάλυψη νέων γειτονικών κόμβων και την αναγνώριση των παρεχόμενων από αυτές υπηρεσιών.

### 5.6.1 Application Framework

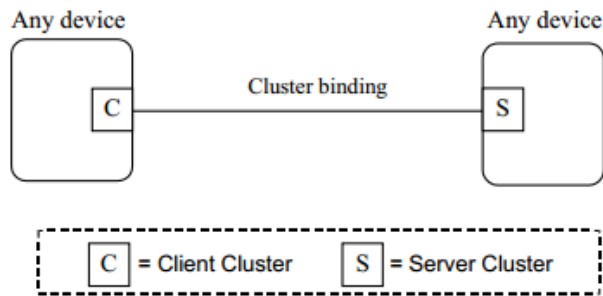
Αποτελεί τον σκελετό για την ανάπτυξη εφαρμογών στο περιβάλλον ενός δικτύου Zigbee. Ο σκοπός του είναι να μειώνει τα γενικά θέματα που προκύπτουν κατά την ανάπτυξη εφαρμογών. Αυτό επιτυγχάνεται με την χρήση κοινόχρηστου από όλες τις συσκευές κώδικα. Στα πλαίσια του application framework εντάσσονται 2 βασικά χαρακτηριστικά, τα *Application profiles* και *Application objects*. Τα Application objects ενσωματώνουν ένα σύνολο χαρακτηριστικών (δεδομένων, εσωτερικής κατάστασης κλπ) και παρέχουν υπηρεσίες για ρύθμιση/ανάκτηση των τιμών αυτών των χαρακτηριστικών ή για ενημέρωση όταν η τιμή ενός αλλάζει. Τα Application

profiles αποτελούν κάποιες συμβάσεις για μηνύματα, μορφές μηνυμάτων και λειτουργίες. Η χρήση των application profiles παρέχει μεγαλύτερη διαλειτουργικότητα μεταξύ προϊόντων από διαφορετικές εταιρίες που χρησιμοποιούνται σε μια συγκεκριμένη διανεμημένη εφαρμογή. Τα application profiles αναφέρονται συχνά και ως zigbee profiles.

Κάθε application profile ταυτοποιείται από έναν αριθμό 16bit γνωστό ως αναγνωριστικό (profile identifier). Μόνο η Zigbee Alliance μπορεί να εκδίδει τέτοια αναγνωριστικά. Zigbee profiles αναπτύσσονται είτε από τα επίσημα μέλη του Zigbee Alliance και αποτελούν τα public profiles είτε από εταιρίες και αποτελούν τα manufacturer specific profiles. Μια εταιρία που έχει αναπτύξει ένα application profile μπορεί να κάνει αίτηση για απόδοση αναγνωριστικού και αφού αξιολογηθεί και εφόσον τηρεί τις προδιαγραφές θα γίνει η έκδοση. Το όνομα που λαμβάνουν τα application profiles προκύπτουν από την εφαρμογή στην οποία θα χρησιμοποιηθούν.

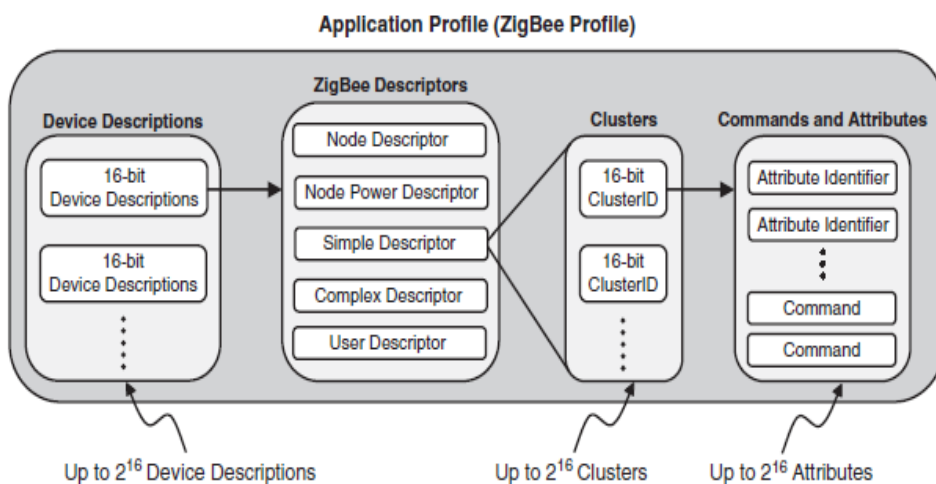
Η δομή των application profiles φαίνεται στην Εικόνα 5-28. Αποτελούνται από δυο βασικά μέρη: 1)τα clusters και 2)τα device descriptions. Το cluster αποτελεί ένα σύνολο χαρακτηριστικών και εντολών συγκεντρωμένων μαζί που χρησιμοποιούνται κυρίως για την αποθήκευση και έλεγχο δεδομένων και τιμών κατάστασης. Χαρακτηρίζεται από έναν μοναδικό αριθμό 16bit που ονομάζεται cluster identifier. Κάθε χαρακτηριστικό του cluster χαρακτηρίζεται επίσης από ένα 16bit αριθμό γνωστό ως attribute identifier.

Τα clusters ουσιαστικά καθορίζουν διεπαφές επικοινωνίας μεταξύ δυο συσκευών. Παίζουν σημαντικό ρόλο για την λογική σύνδεση των συσκευών (binding-Εικόνα 5-27) και διαθέτουν τις απαραίτητες πληροφορίες για να επιδρούν με τον επιθυμητό τρόπο στα χαρακτηριστικά τους. Δυο λογικά συνδεδεμένες συσκευές διατηρούν και οι δυο τα clusters που χρησιμοποιούν. Η μια συνήθως λειτουργεί ως server και είναι αυτή που διατηρεί τις τιμές των attributes (των εκάστοτε χρησιμοποιούμενων clusters) και η άλλη λειτουργεί ως client και είναι αυτή που επιδρά και χειρίζεται τις τιμές των attributes αυτών. Βέβαια πολλές φορές μπορεί να απαιτείται η client συσκευή να διατηρεί και αυτή τις τιμές των attributes.



Εικόνα 5-27 Binding μεταξύ 2 συσκευών

Όσον αφορά τα device descriptions, αυτά παρέχουν τις πληροφορίες που αφορούν την εκάστοτε συσκευή. Για παράδειγμα, πληροφορίες που αφορούν τις ζώνες συχνότητας που υποστηρίζονται, το είδος της συσκευής (end-device, router, coordinator) καθώς και την εναπομένουσα ενέργεια της μπαταρίας. Κάθε device description χαρακτηρίζεται από έναν αριθμό 16bit.



Εικόνα 5-28 Δομή application profile

Τα application profiles του Zigbee χρησιμοποιούν την ιδέα της δομής δεδομένων με χρήση descriptors (16bit). Με αυτόν τον τρόπο, ένα application profile αντί να περιέχει τα ίδια τα δεδομένα, περιέχει αριθμούς των 16bit που λειτουργούν σαν δείκτες στα δεδομένα (Εικόνα 5-28). Κάθε φορά που μια συσκευή ανακαλύπτει την ύπαρξη μίας καινούργιας συσκευής στο δίκτυο, τα device descriptions μεταφέρονται από την μία στην άλλη παρέχοντας τις απαραίτητες πληροφορίες σύμφωνα με αυτή.

Τα device description αποτελούνται από πέντε τομείς: node descriptor, node power descriptor, simple descriptor, complex descriptor, and user descriptor. Ο node

descriptor παρέχει πληροφορίες σχετικά με τον τύπο της συσκευής, τον κωδικό από τον κατασκευαστή, την ζώνη συχνότητας, το μέγιστο μέγεθος της APSDU (APS Sublayer Data Unit) και άλλα. Ο node power descriptor προσδιορίζει αν η συσκευή τροφοδοτείται από μπαταρία και σε αυτή την περίπτωση παρέχει το επίπεδο της μπαταρίας. Ο simple descriptor παρέχει το αναγνωριστικό του application profile και τα clusters. Οι άλλοι δύο τομείς είναι προαιρετικοί και περιέχουν πληροφορίες για το σειριακό αριθμό και το όνομα του μοντέλου της συσκευής αλλά και οποιαδήποτε άλλη επιπρόσθετη πληροφορία.

### 5.6.2 ZDO (Zigbee Device Objects)

Το ZDO λειτουργεί σαν διεπαφή μεταξύ του APS και του application framework. Είναι υπεύθυνο για την προετοιμασία και την αρχικοποίηση του APS, του επιπέδου δικτύου και του Security Service Provider (SSP). Παρόμοια με τα application profiles που ορίζονται στο application framework, υπάρχει ένα profile ορισμένο για το ZDO, το οποίο ονομάζεται Zigbee Device Profile (ZDP) ή απλά *device profile*. Αυτό περιέχει device descriptions και clusters όπως περιγράφηκαν και στην προηγούμενη ενότητα, όμως τα clusters σε αυτή την περίπτωση δεν χρησιμοποιούν χαρακτηριστικά (attributes). Μια άλλη διαφορά μεταξύ του device profile και οποιουδήποτε application profile είναι ότι το application profile δημιουργείται για μια συγκεκριμένη εφαρμογή, ενώ το device profile ορίζει δυνατότητες που υποστηρίζονται από όλες τις Zigbee συσκευές. Το device profile έχει μόνο ένα device description. Τα clusters χωρίζονται σε δύο κατηγορίες, τα υποχρεωτικά που πρέπει να ενσωματώνονται σε όλες τις συσκευές και τα προαιρετικά.

Το device profile μπορεί να ρυθμιστεί είτε ως πελάτης (client), είτε ως εξυπηρετητής (server). Ο client είναι η συσκευή η οποία ζητάει μια υπηρεσία, όπως αναζήτηση συσκευής ή κάποιου binding και ο server είναι η συσκευή που παρέχει την υπηρεσία αυτή. Επομένως έχουμε δύο κατηγορίες υπηρεσιών: client services και server services. Και στις δύο περιπτώσεις, οι υπηρεσίες παρέχονται με την μορφή εντολών (ZDP commands) με μοναδικά αναγνωριστικά (clusterIDs). Σε μια ανταλλαγή μηνύματος μεταξύ ενός client και ενός server, ο client αναφέρεται ως local device και ο server ως remote device. Για την αποστολή των μηνυμάτων αυτών χρησιμοποιείται η υπηρεσία δεδομένων του APS που θα δούμε στην επόμενη ενότητα. Το μήνυμα αποτελείται από δύο πεδία, το πρώτο αποτελεί ένα 8-bit αριθμό που ονομάζεται transaction number και αυξάνεται κάθε φορά που μια καινούργια ανταλλαγή λαμβάνει μέρος και το δεύτερο πεδίο αποτελεί την εντολή (ZDP command) και δεδομένα που μπορεί να σχετίζονται με αυτή.

Οι εντολές λοιπόν χωρίζονται σε δύο κατηγορίες ανάλογα με τις υπηρεσίες που αφορούν (client services ή server services). Επιπροσθέτως αυτές χωρίζονται σε

άλλες τρεις κατηγορίες η κάθε μια οι οποίες είναι: device and service discovery, bind management και network management.

- **device and service discovery:** οι εντολές αυτές επιτρέπουν σε μια συσκευή να ζητήσει πληροφορίες όπως διευθύνσεις δικτύου και descriptors οποιασδήποτε συσκευής στο δίκτυο.
- **bind management:** οι εντολές αυτές επιτρέπουν σε μια συσκευή να δημιουργήσει ή να καταργήσει και γενικά να διαχειρίζεται τα binding relationships σε ένα δίκτυο.
- **network management:** οι εντολές αυτές επιτρέπουν σε μια συσκευή να βρίσκει γειτονικά δίκτυα, πληροφορίες που αφορούν δρομολόγηση και να διαχειρίζεται την είσοδο και την έξοδο συσκευών από το δίκτυο.

Οι παραπάνω τρεις κατηγορίες εντολών σχηματίζουν και τρία αντίστοιχα αντικείμενα του ZDO: device and service discovery object, binding manager object, και network manager object. Υπάρχει επίσης και το security manager object που αφορά την αλληλεπίδραση με την APS Sublayer Management Entity (APSME).

### 5.6.3 APS (Application Support Sublayer)

Το υποεπίπεδο APS αποτελείται από δύο βασικά δομικά στοιχεία: την APS sublayer Data Entity (APSD) και την APS sublayer Management Entity (APSME) που παρέχουν υπηρεσίες δεδομένων και διαχείρισης αντίστοιχα. Η APSD παρέχει υπηρεσίες δεδομένων στο ZDO και στα application objects. Λαμβάνει τα δεδομένα στην μορφή μιας μονάδας δεδομένων (Protocol Data Unit-PDU) και αφού προσθέσει τις κατάλληλες επικεφαλίδες και δημιουργήσει ένα πλαίσιο APS, το μεταφέρει στο επίπεδο δικτύου για την περαιτέρω προετοιμασία του για αποστολή. Η APSME εκτελεί τρεις υπηρεσίες διαχείρισης: 1) διαχείριση bindings, 2) διαχείριση AIB (APS Information Base) και 3) διαχείριση ομάδων (groups) για περιπτώσεις multicast.

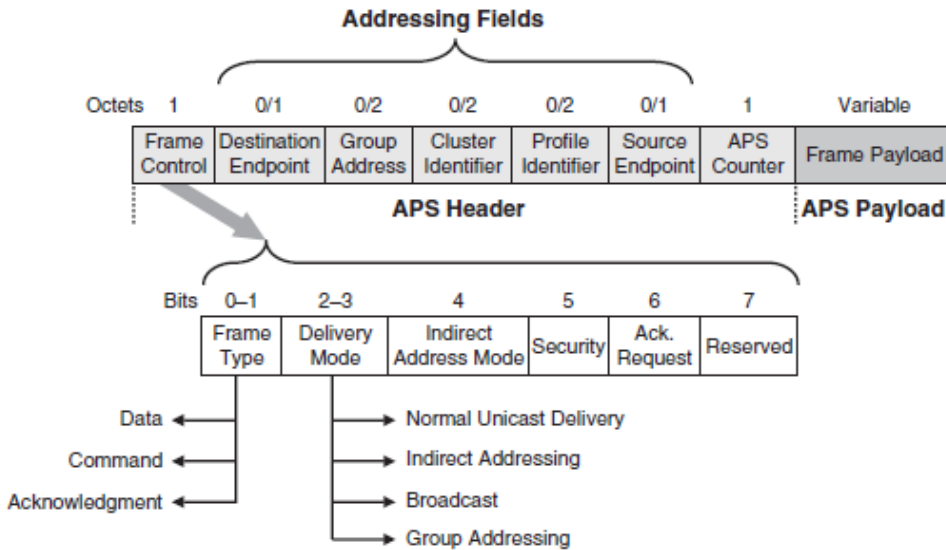
Εκτός από τους τρεις τρόπους μεταφοράς ενός μηνύματος, δηλαδή *unicast*, *multicast* και *broadcast*, υπάρχει και ένας τέταρτος τρόπος που υποστηρίζεται από το APS και ονομάζεται *indirect addressing*. Σε αυτή την περίπτωση μια συσκευή χωρίς να γνωρίζει την διεύθυνση της συσκευής προορισμού μπορεί να επικοινωνήσει με αυτή. Το μήνυμα αρχικά στέλνεται στον coordinator και αυτός αποφασίζει κοιτώντας τα binding tables και τα clusterIDs που θα επαναμεταδώσει το μήνυμα.

### 5.6.4 Πλαίσιο APS

Υπάρχουν τρεις τύποι πλαισίου APS:

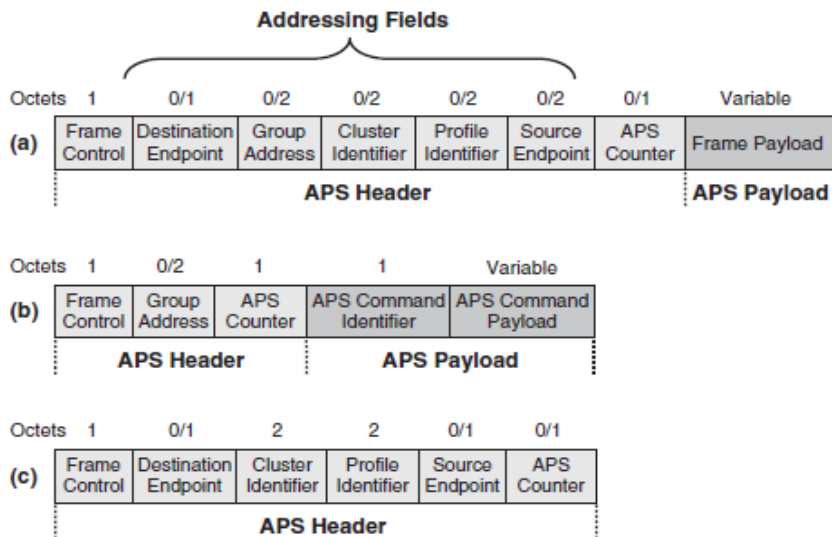
- πλαίσιο δεδομένων
- πλαίσιο εντολής

- πλαίσιο επιβεβαίωσης.



Εικόνα 5-29 Γενική δομή πλαισίου εφαρμογής

Η γενική δομή του πλαισίου φαίνεται στην Εικόνα 5-29. Η μορφή καθενός από τα τρία είδη στην Εικόνα 5-30.



Εικόνα 5-30 Δομή πλαισίου α)δεδομένων β)εντολής γ)επιβεβαίωσης

Το υποπεδίο frame type προσδιορίζει το είδος του πλαισίου. Το υποπεδίο delivery mode καθορίζει τον τρόπο μετάδοσης. Σε περίπτωση indirect addressing το υποπεδίο indirect address mode καθορίζει ποιά πεδία διεύθυνσης (source ή destination) παραλείπεται. Όταν είναι ίσο με μηδέν παραλείπεται το destination



endpoint διότι παραλήπτης είναι ο coordinator και όταν είναι ίσο με ένα, παραλείπεται το source endpoint που είναι πάλι ο Zigbee coordinator. Το υποπεδίο security ορίζεται από τον Security Service Provider (SSP) και αφορά το επίπεδο ασφαλείας. Τέλος αν το υποπεδίο Ack Request είναι ένα, ο παραλήπτης πρέπει να στείλει πίσω επιβεβαίωση. Αν το πεδίο group address είναι ορισμένο τότε το μήνυμα στέλνεται στις συσκευές που ανήκουν στην συγκεκριμένη ομάδα (group). Δεν μπορεί στο ίδιο πλαίσιο να υπάρχει και group address και destination endpoint. Στο πεδίο cluster identifier υπάρχει το clusterID που θα χρησιμοποιηθεί για κάποια διαδικασία binding και στο profile identifier προσδιορίζεται το application profile το οποίο αφορά το μήνυμα. Τέλος το πεδίο APS counter είναι ένας 8-bit μετρητής που αυξάνεται κάθε φορά που κάποιο καινούργιο πλαίσιο μεταδίδεται και χρησιμεύει στον εντοπισμό αντίγραφων πλαισίων (duplicates).

### 5.6.5 Συνοπτική παρουσίαση των αρμοδιοτήτων του επιπέδου εφαρμογής

Το επίπεδο εφαρμογής αποτελείται από τρία βασικά στοιχεία

- APS (application support sublayer)
- ZigBee Device Objects (ZDO)
- Application framework

Το APS παρέχει την διεπαφή μεταξύ του επιπέδου δικτύου και του επιπέδου εφαρμογής. Οι αρμοδιότητες του είναι οι εξής:

- Διατήρηση των binding tables
- Προώθηση μηνυμάτων μεταξύ συσκευών που διατηρούν binding relationships
- Διαχείριση διευθύνσεων ομάδων (groups)
- Αντιστοίχιση των 64-bit IEEE διευθύνσεων σε 16-bit διευθύνσεων δικτύου και αντίστροφα
- Υποστήριξη αξιόπιστης μεταφοράς δεδομένων

Το ZDO λειτουργεί σαν διεπαφή μεταξύ του APS και του application framework. Οι αρμοδιότητες του είναι οι εξής:

- Καθορισμός του ρόλου της συσκευής στο δίκτυο
- Ανακάλυψη συσκευών στο δίκτυο και των εφαρμογών τους
- Έναρξη ή απόκριση σε αιτήσεις για binding
- Εκτέλεση εργασιών σχετικών με την ασφάλεια

Τέλος το Application Framework αποτελεί το περιβάλλον όπου διατηρούνται τα application objects και application profiles.

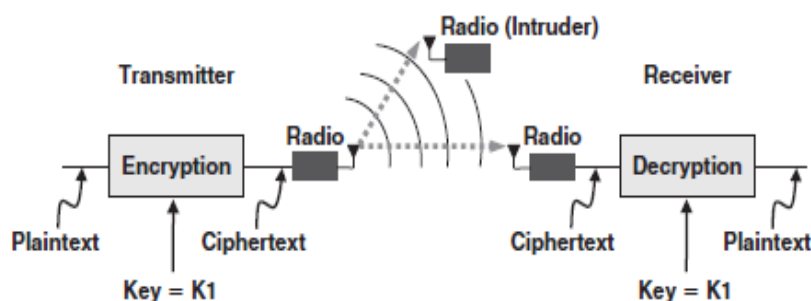
## 5.7 Ασφάλεια

Το Zigbee χρησιμοποιεί τις υπηρεσίες ασφαλείας του προτύπου 802.15.4 και τις εφαρμόζει και στο επίπεδο δικτύου και στο επίπεδο εφαρμογής. Το 802.15.4 ορίζει τον αλγόριθμο κρυπτογράφησης που θα χρησιμοποιηθεί κατά την μεταφορά των δεδομένων αλλά δεν καθορίζει πως θα γίνεται η διαχείριση των κλειδιών, αλλά και σύμφωνα με ποιούς κανόνες θα γίνεται η ταυτοποίηση αυθεντικότητας. Ένας από τους βασικούς περιορισμούς στην εισαγωγή ασφαλείας στα δίκτυα Zigbee είναι οι περιορισμένοι πόροι καθώς οι συσκευές τροφοδοτούνται κατά κύριο λόγο με μπαταρίες και έχουν περιορισμένη υπολογιστική ισχύ και μνήμη. Οι βασικές υπηρεσίες ασφαλείας που παρέχονται είναι οι εξής:

- Κρυπτογράφηση δεδομένων (confidentiality)
- Πιστοποίηση δεδομένων και συσκευών (authentication)
- Αποφυγή και προστασία από duplicate frames

### 5.7.1 Encryption

Χρησιμοποιεί το *Advanced Encryption Standard (AES)*. Η γενική ιδέα της κρυπτογράφησης είναι η εξής: ο αποστολέας του μηνύματος χρησιμοποιεί έναν αλγόριθμο για να κρυπτογραφήσει το μήνυμα και μόνο ο αποδέκτης γνωρίζει τον «τρόπο» για να ανακτήσει το μήνυμα. Ο αλγόριθμος είναι κοινώς γνωστός και διαθέσιμος στον καθένα, οπότε η υλοποίηση επιτυγχάνεται με την χρήση κάποιου κλειδιού. Το κλειδί είναι ένας δυαδικός αριθμός και το ίδιο κλειδί χρησιμοποιείται τόσο για την κωδικοποίηση από τον αποστολέα όσο και για την αποκωδικοποίηση από τον αποδέκτη, πράγμα που είναι γνωστό ως *μέθοδος συμμετρικού κλειδιού*. Το Zigbee χρησιμοποιεί κλειδιά των 128 bits που σημαίνει ότι υπάρχουν  $2^{128}$  πιθανά κλειδιά. Ο αλγόριθμος του AES αποτελεί μια σειρά καλά ορισμένων ενεργειών που χρησιμοποιούν το κλειδί των 128 bits και παράγουν μια κρυπτογραφημένη έκδοση του αρχικού μηνύματος. Όλες οι ενέργειες αυτές είναι αναστρέψιμες αν είναι γνωστό το κλειδί, πράγμα που επιτρέπει την αποκωδικοποίηση του μηνύματος από τον αποδέκτη.



Εικόνα 5-31 Διαδικασία κρυπτογράφησης-αποκρυπτογράφησης AES

Πέντε διαφορετικοί τύποι κλειδιών μπορούν να χρησιμοποιηθούν σε ένα ασφαλές δίκτυο:

- Το *link key* το μοιράζονται δύο συσκευές και μπορεί να χρησιμοποιηθεί για επικοινωνία με unicast
- Το *network key* είναι γνωστό σε όλο το δίκτυο και χρησιμοποιείται σε περιπτώσεις broadcast επικοινωνίας
- Το *master key* χρησιμοποιείται για την εγκαθίδρυση link keys μεταξύ 2 συσκευών
- Το *key-transport key* χρησιμοποιείται για την ασφαλή μεταφορά οποιουδήποτε κλειδιού εκτός του master key, από το trust center.
- Το *key-load key* χρησιμοποιείται για την ασφαλή μεταφορά των master keys

Το Zigbee παρέχει μεθόδους για την εγκαθίδρυση και τον διαμοιρασμό των κλειδιών μεταξύ δύο ή περισσότερων συσκευών. Δύο τύποι κλειδιών χρησιμοποιούνται κατά την διάρκεια ασφαλούς επικοινωνίας: το link key και το network key. Κάθε δίκτυο Zigbee που χρησιμοποιεί ασφάλεια έχει μια συσκευή που ονομάζεται trust center και που ορίζεται από τον coordinator, η οποία διατηρεί και διαμοιράζει τα κλειδιά στις υπόλοιπες συσκευές. Το trust center έχει δύο τρόπους λειτουργίας: 1) commercial mode: σε αυτή την περίπτωση το trust center διατηρεί λίστα με τις συσκευές και όλα τα κλειδιά (link, network και master) και κάνει και έλεγχο για duplicates των πακέτων. 2) residential mode: το trust center διατηρεί μόνο το network key. Στην περίπτωση του commercial mode οι απαιτήσεις σε μνήμη είναι πολύ μεγαλύτερες και αυξάνονται με το αριθμό των κόμβων.

Υπάρχουν 3 μέθοδοι για την απόκτηση ενός link key:

1. Προεγκατάσταση (preinstallation): ο κατασκευαστής ενσωματώνει το κλειδί στην συσκευή, έτσι δεν χρειάζεται να ζητήσει κλειδί από το trust center όταν εισέλθει στο δίκτυο.
2. Μεταφορά κλειδιού (*key transport*): η συσκευή ζητάει κλειδί από το trust center και η μεταφορά του κλειδιού γίνεται με την χρήση ενός ειδικού κλειδιού (*key-transport key*)
3. Εγκαθίδρυση κλειδιού (*Key establishment*): δυο συσκευές δημιουργούν ένα τυχαίο κλειδί χωρίς να το στείλουν η μία στην άλλη. Βασίζεται στο πρωτόκολλο SKKE (Symmetric Key Key Establishment) και χρησιμοποιεί το από πριν γνωστό σε όλες τις συσκευές master key.

## 5.7.2 Authentication

### 5.7.2.1 Device Authentication

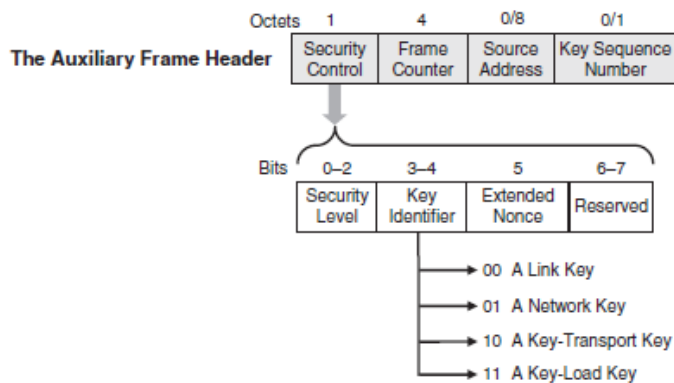
Όταν μια συσκευή εισέρχεται στο δίκτυο, έχει κατάσταση «joined, but unauthenticated». Αν το trust center αποφασίσει να μην πιστοποιήσει την νέα συσκευή, τότε ζητάει την απομάκρυνσή της από το δίκτυο.

### 5.7.2.2 Data Authentication

Ο σκοπός της λειτουργίας αυτής είναι να εγγυάται ότι τα δεδομένα δεν άλλαξαν κατά την μεταφορά. Για τον λόγο αυτό ο αποστολέας στέλνει μέσα στο μήνυμα και έναν κωδικό γνωστό ως Message Integrity Code (MIC). Ο κωδικός αυτός υπολογίζεται με τον ίδιο τρόπο και από τον αποδέκτη και σε περίπτωση που οι κωδικοί ταιριάζουν, τα δεδομένα θεωρούνται αυθεντικά.

### 5.7.3 Auxiliary frame header

Η ενσωμάτωση των χαρακτηριστικών ασφαλείας στα πακέτα που στέλνονται γίνεται στο πεδίο Auxiliary frame header που είναι προαιρετικό και προστίθεται στο επίπεδο εφαρμογής. Η μορφή του πεδίου αυτού φαίνεται στην Εικόνα 5-32.



Εικόνα 5-32 Auxiliary frame header

Το πεδίο security lever ορίζει το επίπεδο ασφαλείας ανάλογα με τον αν έχουμε κρυπτογράφηση των δεδομένων και ορίζοντας και το μήκος του MIC. Οι 8 διαθέσιμες επιλογές φαίνονται στον Πίνακας 5-1.

Security Level	Security Attributes	Data Encryption	Frame Integrity
000	Non	OFF	NO
001	MIC-32	OFF	YES (32 bits)
010	MIC-64	OFF	YES (64 bits)
011	MIC-128	OFF	YES (128 bits)
100	ENC	ON	NO
101	ENC-MIC-32	ON	YES (32 bits)
110	ENC-MIC-64	ON	YES (64 bits)
111	ENC-MIC-128	ON	YES (128 bits)

Πίνακας 5-1

## 5.8 Zigbee στην πράξη

Οι τομείς που έχει εφαρμογή το Zigbee έχουν σχέση κυρίως με την συλλογή δεδομένων και τον απομακρυσμένο έλεγχο. Κάποιοι χαρακτηριστικοί τομείς είναι:

- Έλεγχος και αυτοματισμοί οικιακών συσκευών
- Ασύρματα δίκτυα αισθητήρων
- Βιομηχανικός έλεγχος
- Συλλογή ιατρικών δεδομένων
- Κτιριακοί αυτοματισμοί
- Συστήματα ασφαλείας
- Αυτοματισμοί και έλεγχος στην γεωργία

Το ZigBee αν και προτυποποιήθηκε σχετικά πρόσφατα (2003) και είναι μια καινούργια τεχνολογία επικοινωνίας, έχει εφαρμοστεί από πολλές εταιρίες σε προϊόντα τους. Ο πλήρης κατάλογος των πιστοποιημένων προϊόντων υπάρχει στην ιστοσελίδα του ZigBee Alliance στο URL:

<http://zigbee.org/Products/ByStandard/AllStandards.aspx> .

Τα προϊόντα που είναι βασισμένα στο ZigBee χωρίζονται σε δύο κατηγορίες. Η πρώτη είναι τα εργαλεία ανάπτυξης και το υλικό για την δημιουργία DIY projects ή κατασκευή ολοκληρωμένων custom εφαρμογών. Η δεύτερη κατηγορία είναι τα προϊόντα που αποτελούν έτοιμες λύσεις και είναι έτοιμα προς χρήση από το ευρύ καταναλωτικό κοινό.

Στην πρώτη κατηγορία δραστηριοποιούνται εταιρίες τεχνολογίας ημιαγωγών όπως η Texas instruments και η Silicon Labs. Κάποια από τα προϊόντα τους είναι:

- TI CC2530/CC2520/CC2531 με ενσωματωμένο 8-bit μικροελεγκτή (8051) και CC2530 Development kit
- TI MPS430 με 16-bit μικροελεγκτή
- Silicon labs EM385x με 32-bit (ARM Cortex M3) μικροελεγκτή
- Xbee ZB (network module)

Στην δεύτερη κατηγορία συναντάμε πληθώρα προϊόντων από πολλούς κατασκευαστές. Κάποια παραδείγματα είναι:

- Indesit smart aqualtis (πλυντήριο)
- LG Air-conditioner (FNW182ASV)
- Philips Hue Connected Lamp BR30
- Meazon web plug basic
- Legrand 400W Universal Dimmer
- Samsung DR Gateway

Τα προϊόντα στην δεύτερη κατηγορία είναι αρκετά μεγάλα σε αριθμό και είναι προφανές ότι δεν μπορούν να αναφερθούν στα πλαίσια μίας διπλωματικής εργασίας. Πολλές μεγάλες εταιρίες (Lg,Samsung) έχουν αρχίσει να υιοθετούν το ZigBee και να το ενσωματώνουν σε προϊόντα τους, πράγμα που ενισχύει τις φήμες ότι στο κοντινό μέλλον φορητές συσκευές όπως smartphone και tablet θα ενσωματώνουν πομποδέκτη ZigBee ώστε να μπορούν να επικοινωνούν απευθείας με δίκτυα ZigBee χωρίς την παρεμβολή κάποιου ενδιάμεσου βοηθητικού gateway.

### **5.9 Τελική επιλογή πρωτοκόλλου**

Μετά από την σύγκρισή των δύο επικρατέστερων ασύρματων τεχνολογιών (Zigbee και 6LoWPAN) καταλήξαμε στη επιλογή του Zigbee. Οι λόγοι που καταλήξαμε εκεί αφορούν κυρίως οικονομικά κριτήρια υλικού αλλά και μεγαλύτερη αποδοχή που μας δίνει το πλεονέκτημα καλύτερης υποστήριξης. Επίσης η ανάπτυξη εφαρμογών με την χρήση 6LoWPAN είναι σημαντικά δυσκολότερη και εξαιτίας της μικρότερης κοινότητας που ασχολείται με αυτό αλλά και του γεγονότος ότι απαιτεί βαθιά γνώση όλων των πτυχών του πρωτοκόλλου. Δεν πρέπει να παραλείψουμε βέβαια ότι πιθανότατα σε λίγα χρόνια να έχουν αντιστραφεί οι ρόλοι, καθώς το 6LoWPAN είναι πιο πρόσφατη τεχνολογία που ίσως επικρατήσει στον χώρο IoT λόγω της συμβατότητας του με το Ipv6. Άλλωστε στην κατεύθυνση αυτή κινείται και η ίδια η Zigbee Alliance που ήδη έχει εισάγει μια έκδοση συμβατή με το Ipv6 (Zigbee IP).

## **6 Ασύρματο δίκτυο αισθητήρων: εφαρμογή σε θερμοκήπιο**

Το αντικείμενο της διπλωματικής εργασίας πραγματεύεται την χρήση των ασύρματων δικτύων χαμηλής ενέργειας σε εφαρμογές που διευκολύνουν την καθημερινότητα μας, είτε οικιακά είτε βιομηχανικά. Σε αυτά τα πλαίσια διαλέξαμε να διαμορφώσουμε ένα τέτοιο δίκτυο το οποίο προτείνει λύση σε έναν τομέα αρκετά σημαντικό για την χώρα μας, αλλά και σε παγκόσμιο επίπεδο, την γεωργία. Το δίκτυο που δημιουργήσαμε έχει εφαρμογή σε θερμοκήπιο, αυτό όμως δεν αναιρεί την δυνατότητα με κατάλληλη προσαρμογή να απευθυνθεί σε κάθε επιμέρους κλάδο της καλλιέργειας.

Η εφαρμογή που προτείνουμε δεν έρχεται για να δώσει λύση στο πρόβλημα της διαχείρισης καλλιέργειας σε θερμοκήπια, αλλά για να βελτιστοποιήσει την διαδικασία αυτή. Η καλλιέργεια σε θερμοκήπιο για να είναι βέλτιστη πρέπει να ακολουθεί κάποιους κανόνες, περισσότεροι από τους οποίους σχετίζονται με τις κλιματικές συνθήκες. Η δυνατότητα που δίνουμε με το συγκεκριμένο δίκτυο είναι η παρακολούθηση και ο έλεγχος μέσω διαδικτύου απομακρυσμένα. Σκοπός αυτής της διπλωματικής δεν είναι να αναλύσει σε βάθος την θεωρία πίσω από την λειτουργία των θερμοκηπίων και σε καμία περίπτωση από την σκοπιά κάποιου ειδικότερου κλάδου όπως είναι η γεωπονική, αλλά να δώσει ένα εργαλείο το οποίο διευκολύνει και δίνει πρόσθετη αξία.

### **6.1 Μηχανική του θερμοκηπίου**

#### **6.1.1 Ορισμός- Ιστορία**

Θερμοκήπιο ονομάζεται το κτίριο οπου καλλιεργούνται φυτά. Ένα θερμοκήπιο χτίζεται είτε με πλαστικό είτε με γυαλί και θερμαίνεται από τις εισερχόμενη υπεριώδη ηλιακή ακτινοβολία, η οποία θερμαίνει τας φυτά και το χώμα. Ο αέρας που θερμαίνεται από τις ζεστές εσωτερικές επιφάνειες διατηρείται μέσα στο κτίριο λόγω της κελύφους του. Το γυαλί που χρησιμοποιείται στα θερμοκήπια λειτουργεί ως ένα μέσο μετάδοσης για διάφορες φασματικές συχνότητες, και η επίδραση του είναι να παγιδεύει ενέργεια μέσα στο κτίριο, η οποία θερμαίνει τόσο τα φυτά όσο και το έδαφος στο εσωτερικό του.

#### **6.1.2 Σύστημα ελέγχου αυτοματισμών για θερμοκήπια**

Ο αυτοματισμός μπορεί να οριστεί ως η τεχνολογία που χρησιμοποιεί προγραμματισμένες εντολές για τη λειτουργία διαδικασιών, συνδυασμένων με ανάδραση πληροφοριών ώστε να προσδιορισθεί ότι η εντολή εκτελέστηκε σωστά. Οι αυτοματισμοί μπορούν να λειτουργήσουν και χωρίς την ανθρώπινη παρέμβαση. Για την ακρίβεια, τα περισσότερα συστήματα αυτοματισμών εκτελούν τις λειτουργίες τους με μεγαλύτερη ακρίβεια και λιγότερο χρόνο από τον άνθρωπο.

Σκοπός των αυτοματισμών είναι να εξοπλίσει τα συστήματα μηχανικής με ανθρώπινες ικανότητες, όπως η αντίληψη, η λογική/ εκμάθηση, επικοινωνία και τον προγραμματισμό/ εκτέλεση διεργασιών. Υπάρχουν δύο κατηγορίες αυτοματισμών: οι σταθεροί και οι ελαστικοί.

Η ανάλυση συστήματος και η ολοκλήρωση του είναι μία μεθοδολογία που ξεκινά με τον ορισμό ενός συστήματος και τους στόχους του και οδηγεί σε συμπεράσματα σχετικά με την λειτουργικότητα, την παραγωγικότητα και άλλων δεικτών επίδοσης του συστήματος. Δύο βασικοί πόροι για την ανάλυση συστήματος είναι: οι πληροφορίες που αφορούν κάθε επιμέρους υποσύστημα και τις διασυνδέσεις τους, οι διαδικασίες και επεξεργασία δεδομένων με σκοπό την δημιουργία πληροφοριών προστιθέμενης αξίας.

### **6.1.3 Περιβάλλον θερμοκηπίου**

Το περιβάλλον των φυτών σε ένα θερμοκήπιο αποτελείται από τις κλιματικές , θρεπτικές συνθήκες, όπως και τις κατασκευαστικές, μηχανικές συνθήκες. Ο έλεγχος περιβάλλοντος θεωρείται μία βασική πρόκληση στην ελεγχόμενη καλλιέργεια τα τελευταία χρόνια. Οι κλιματικές συνθήκες είναι το κύριο θέμα έρευνας. Ο βαθμός πολυπλοκότητας για τον έλεγχο του κλίματος εξαρτάται από την φυσική δομή που ξεχωρίζει το εσωτερικό με το εξωτερικό περιβάλλον. Η αλληλεπίδραση του περιβάλλοντος μέσα και έξω από το θερμοκήπιο επιβάλλει την διευρυμένη χρήση τεχνικού εξοπλισμού, λογισμικού και ενεργοποιητών.

Οι προκλήσεις που αντιμετωπίζει η αυτοματοποίηση ενός θερμοκηπίου είναι οι εξής: η ελκυστική απόδοση αρχικής επένδυσης, βελτιστοποίηση συστήματος ενσωματώνοντας κατάλληλα αυτοματισμούς, εξισορρόπηση σταθερών και ελαστικών αυτοματισμών, περιορισμένη ζήτηση και συνεχής έρευνα για την βελτιστοποίηση των δυνατοτήτων.

### **6.1.4 Παράμετροι ελέγχου θερμοκηπίου**

Ο περιβαλλοντικός έλεγχος θερμοκηπίου περιλαμβάνει τον έλεγχο και την τροποποίηση της ημερήσιας και βραδινής θερμοκρασίας, της σχετικής υγρασίας, και του επιπέδου διοξειδίου του άνθρακα για την βέλτιστη ανάπτυξη των φυτών. Τα ελεγχόμενα συστήματα παραγωγής φυτών προσφέρουν την δυνατότητα μεγάλου αριθμού υψηλής ποιότητας καλλιεργειών με μεγαλύτερη προβλεψιμότητα. Στόχος αυτών των συστημάτων είναι να ενισχύσουν την ανάπτυξη του φυτού ώστε να επιτυγχάνονται έγκαιροι χρόνοι ωρίμανσης με την επιθυμητή ποιότητα που απαιτεί ο παραγωγός. Τα καλύτερα συστήματα ελέγχου δεν είναι μόνο αποτελεσματικά στην δημιουργία του κατάλληλου περιβάλλοντος για το φυτό, αλλά έχουν σχεδιαστεί και κατασκευαστεί ώστε να ενσωματώνονται στο οικοσύστημα του θερμοκηπίου.



Οι σημαντικότερες μεταβλητές που σχηματίζουν το περιβάλλον του θερμοκηπίου είναι η ηλιακή ακτινοβολία, η θερμοκρασία αέρα, η υγρασία εδάφους, η συγκέντρωση υδρατμών και διοξειδίου του άνθρακα στον αέρα. Λόγω της υψηλής διαπεραστικότητας και χαμηλής θερμικής αντίστασης του γυαλιού, το εσωτερικό του θερμοκηπίου επηρεάζεται άμεσα από την ηλιακή ακτινοβολία και την εξωτερική θερμοκρασία. Συνεπώς για την παραγωγή εμπορικών καλλιεργειών με αποδεκτή απόδοση και ποιότητα, οι εσωτερικές συνθήκες πρέπει να ελέγχονται.

## 6.2 Συστήματα διαχείρισης θερμοκηπίων

Σε αυτό το κεφάλαιο γίνεται μία σύντομη αναφορά σε κάποιες ενδεικτικές λύσεις που βρίσκονται στην αγορά και ασχολούνται με την αυτοματοποίηση των θερμοκηπίων. Θα γίνει ανάλυση της εγκατάστασης και της λειτουργίας τους καθώς και του ενδεικτικού τους κόστους.

### 6.2.1 Libellium Agriculture

Η εταιρία Libellium δραστηριοποιείται στα ασύρματα δίκτυα αισθητήρων. Η πλατφόρμα της Libellium βασίζεται στο δίκτυο που δημιουργούν οι τελικές συσκευές WaspMote και ο συντονιστής του δικτύου Meshlium. Δίνεται η δυνατότητα στον καταναλωτή να διαλέξει μέσα από μία μεγάλη γκάμα αισθητήρων για να συνδεθούν με τις τελικές συσκευές και να δημιουργήσει το δίκτυο που επιθυμεί. Ο συντονιστής του δικτύου μπορεί να συνδεθεί στο διαδίκτυο μέσω υπηρεσιών Cloud που προσφέρεται.



Εικόνα 6-1 WaspMote και Meshlium

Το κόστος εγκατάστασης και λειτουργίας ενός ολοκληρωμένου πακέτου Libellium αποτελείται από τα εξής. Το προϊόν Meshlium που λειτουργεί ως συντονιστής στο δίκτυο Zigbee και μπορεί να συνδεθεί στο διαδίκτυο μέσω Wi-Fi, κοστολογείται στα 690€. Οι υπηρεσίες για απομακρυσμένη διαχείριση μέσω Cloud, κοστίζουν 500€ για τους 5 πρώτους κόμβους και 20€ για κάθε επόμενο το οποίο αποτελεί εφάπαξ ποσό. Το τελικό κόστος μίας τελικής συσκευής μαζί με τους απαραίτητους αισθητήρες, κυμαίνεται στα 560€ με δυνατότητα προσθήκης ηλιακού panel και μπαταρίας, για αυτονομία του κόμβου από τροφοδοσία, με επιπλέον 65€. Αν

αθροίσουμε τα κόστη αυτά και με την παραδοχή ότι σε ένα πραγματικό σενάριο θα χρειαστούμε δεκάδες κόμβους το κόστος για ένα ολοκληρωμένο δίκτυο μπορεί να ξεπεράσει τα 10000€.

[http://www.libelium.com/xhjs76gd/libelium\\_products\\_catalogue.pdf](http://www.libelium.com/xhjs76gd/libelium_products_catalogue.pdf)

### 6.2.2 GrowTronix

Η λύση της GrowTronix αποτελείται από ένα ενσύρματο δίκτυο αισθητήρων και ενεργοποιητών που αναφέρονται σε καλλιέργειες είτε σε θερμοκήπιο είτε σε εσωτερικό χώρο. Η εγκατάσταση ενός τέτοιου δικτύου είναι πιο δύσκολη και χρονοβόρα, ειδικά αν έχουμε να αντιμετωπίσουμε μεγάλη περιοχή εγκατάστασης, υπερέρχει όμως στην τιμή.



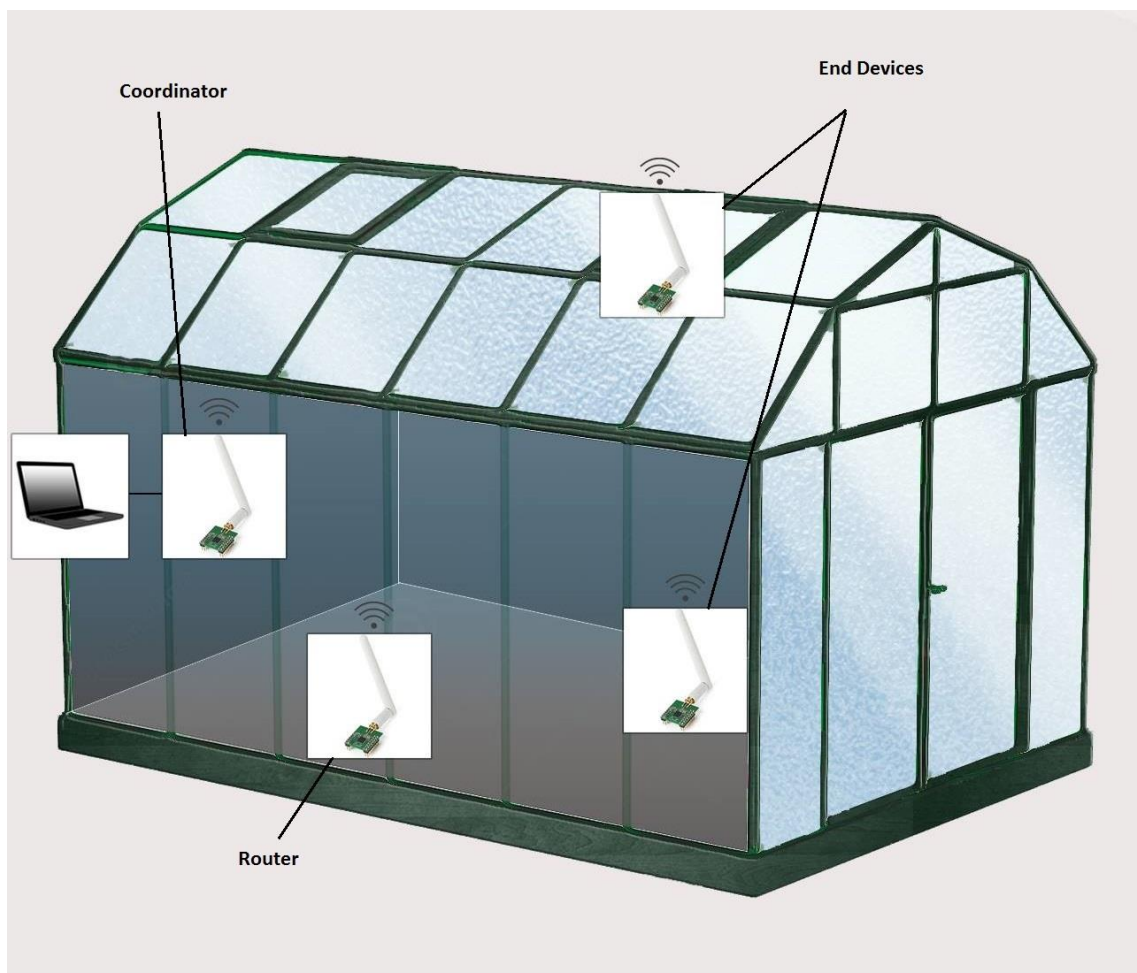
Εικόνα 6-2 Growtronix Kit

Το βασικό πακέτο (GrowTronix Base System) αποτελείται από τους βασικούς αισθητήρες υγρασίας και θερμοκρασίας και δύο ενεργοποιητές, κοστίζει 499\$. Πάνω σε αυτό το πακέτο μπορούν να προστεθούν και άλλοι αισθητήρες και ενεργοποιητές με κόστος που ενδεικτικά για έναν αισθητήρα κυμαίνεται από 39\$ για θερμοκρασία μέχρι 349\$ για CO2. Είναι σημαντικό να αναφερθεί ότι το κόστος της πλατφόρμας απομακρυσμένης διαχείρισης παρέχεται δωρεάν από το βασικό πακέτο.

### 6.3 Περιγραφή δικτύου

Το δίκτυο που δημιουργήσαμε στηρίζεται στο πρωτόκολλο ασύρματης τεχνολογίας Zigbee. Υπάρχουν τέσσερις κόμβοι οι οποίοι επικοινωνούν ασύρματα μέσω Zigbee,

και ένας από αυτούς επικοινωνεί με ενσύρματη σειριακή σύνδεση (UART) με έναν υπολογιστή. Οι τρεις κόμβοι συλλέγουν μετρήσεις από το περιβάλλον μέσω των αισθητήρων και ο τελευταίος κόμβος που συνδέεται με τον υπολογιστή συλλέγει όλες αυτές τις τιμές. Ο υπολογιστής αναλαμβάνει το έργο της δημιουργίας ενός server ο οποίος δημοσιεύει τις μετρήσεις σε μία ιστοσελίδα, δίνοντας την δυνατότητα να παρακολουθείται το θερμοκήπιο από οπουδήποτε υπάρχει σύνδεση στο διαδίκτυο. Επιπλέον υπάρχει η δυνατότητα απομακρυσμένου ελέγχου, καθώς ο χρήστης έχει την δυνατότητα να ορίσει τις παραμέτρους που επιθυμεί και το δίκτυο των μικροελεγκτών με κατάλληλες ενέργειες (θέρμανση, πότισμα κλπ) να τις προσεγγίσει. Εκτενέστερη ανάλυση γίνεται στα επόμενα κεφάλαια.



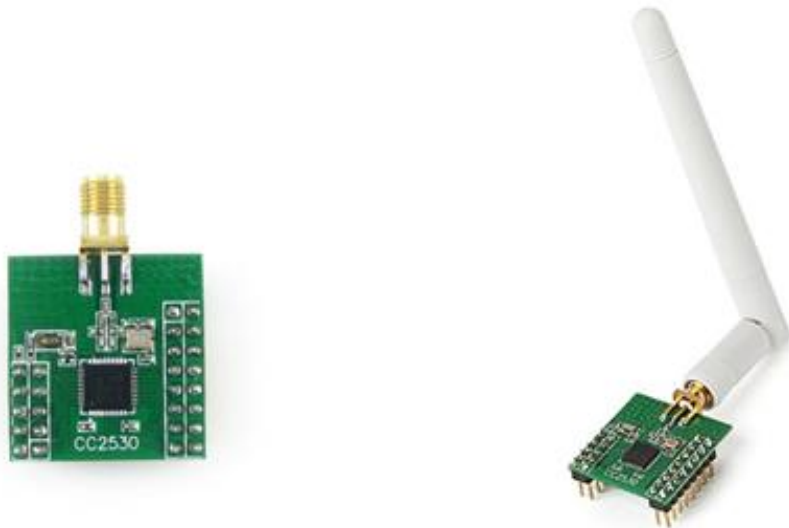
Εικόνα 6-3 Δίκτυο θερμοκηπίου

## 7 Hardware and Software

### 7.1 Υλικό-Hardware

#### 7.1.1 CC2530

Για τις ανάγκες της εφαρμογής μας χρησιμοποιήσαμε την System-on-Chip (SoC) λύση CC2530 της Texas Instruments. Ο όρος System-on-Chip αναφέρεται στην τεχνολογία της ενσωμάτωσης σε ένα chip, όλων των απαραίτητων κυκλωμάτων και στοιχείων για ένα σύστημα. Ένα ολοκληρωμένο κύκλωμα SoC μπορεί να περιλαμβάνει αναλογικές, ψηφιακές, RF και άλλες λειτουργίες αλλά και μνήμη μεγαλύτερη των 100 kB σε αντίθεση με τους τυπικούς μικροελεγκτές. Επίσης βασικό χαρακτηριστικό των SoCs είναι η χαμηλή κατανάλωση για αυτό και συνηθίζονται στην αγορά των mobile ηλεκτρονικών.



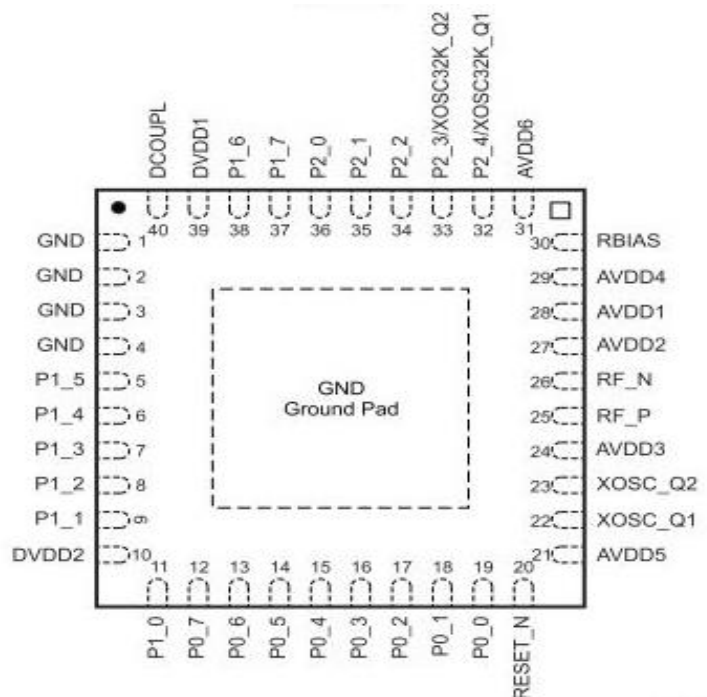
Εικόνα 7-1 Texas Instruments CC2530

Τα συγκεκριμένα χαρακτηριστικά του microchip CC2530 είναι τα εξής:

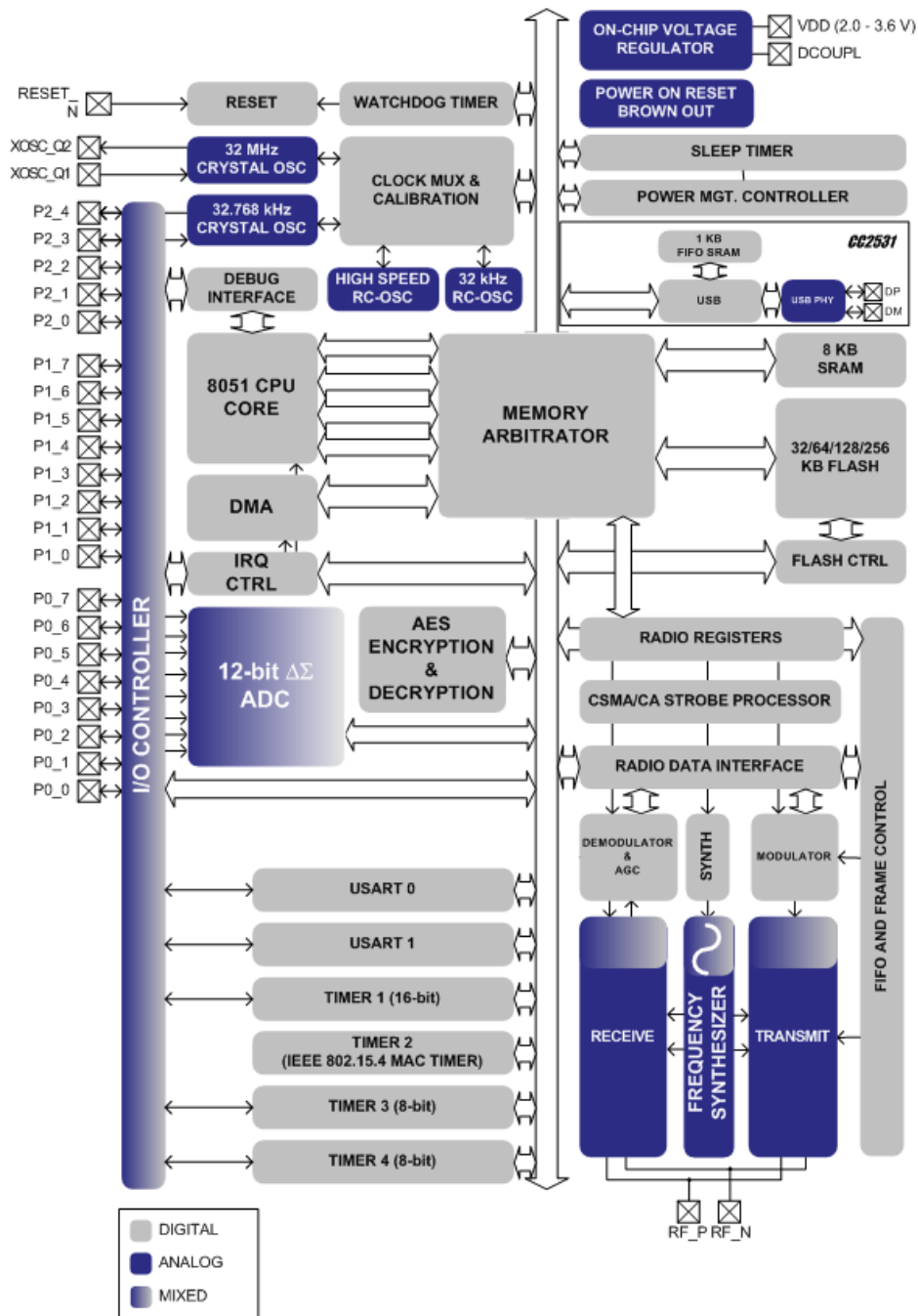
- **RF-διεπαφή:** Διαθέτει RF πομποδέκτη συμβατό με το πρότυπο 2.4GHz IEEE 802.15.4. Παρέχει ταχύτητες ασύρματης μετάδοσης έως 250kbrps και αξιόπιστη επικοινωνία σε απόσταση μεγαλύτερη των 250 μέτρων (open area). Διαθέτει μεγάλη ευαισθησία δέκτη και μεγάλη αντοχή στις παρεμβολές.
- **Μικροελεγκτής:** Υψηλής επίδοσης και χαμηλής κατανάλωσης μικροεπεξεργαστής 8051 (8-bit). Προγραμματιζόμενη μνήμη flash 256 kB. 8 kB RAM.
  - Active-Mode RX (CPU Idle): 24 mA
  - Active Mode TX at 1 dBm (CPU Idle): 29 mA

- Χαμηλή κατανάλωση:
  - Power Mode 1 (4  $\mu$ s Wake-Up): 0.2 mA RF4CE
  - Power Mode 2 (Sleep Timer Running): 1  $\mu$ A
  - Power Mode 3 (External Interrupts): 0.4  $\mu$ A
- Περιφερειακά:
  - Working voltage: 2.0V-3.6V
  - 21 General-Purpose I/O Pins (19  $\times$  4 mA, 2\*20 mA)
  - Διο USARTs (universal synchronous/asynchronous receiver/transmitter) με υποστήριξη για διάφορα πρωτόκολλα σειριακής επικοινωνίας.
  - 12-bit ADC (Analog-Digital Converter)
  - CSMA/CA Hardware Support
  - Powerful Five-Channel DMA
  - Accurate Digital RSSI/LQI Support
  - AES Security Coprocessor
  - Battery Monitor and Temperature Sensor
  - Watchdog Timer
- Ενδεικτικό κόστος: 10€

Παρακάτω φαίνονται το pinout (Εικόνα 7-7-2) και το block διάγραμμα (Εικόνα 7-3) με τις λειτουργίες του CC2530:



Εικόνα 7-7-2 Pinout CC2530

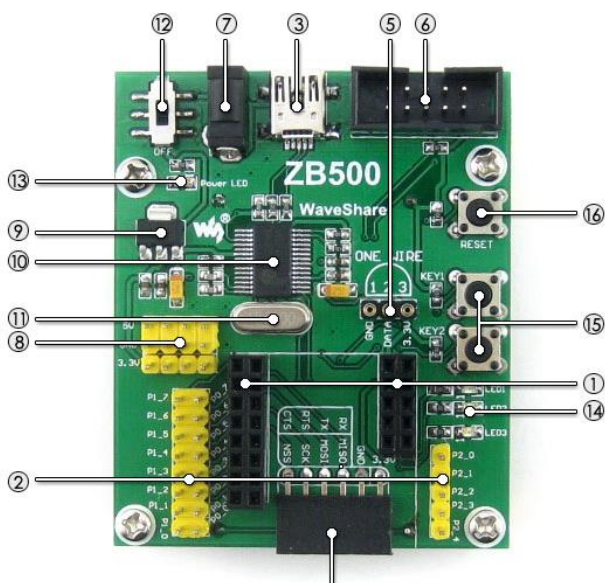


Εικόνα 7-3 Block διάγραμμα του CC2530

### 7.1.2 ZB500-ZB502

Για την κατανόηση της λειτουργίας, την ανάπτυξη της εφαρμογής και τον προγραμματισμό των CC2530 χρησιμοποιήθηκαν οι αναπτυξιακές πλακέτες ZB500 και ZB502 της Waveshare Electronics. Οι πλακέτες αυτές παρέχουν έτοιμες διεπαφές για τις διάφορες περιφερειακές λειτουργίες που παρέχει το CC2530 (UART-SPI interface, I/O Interface κλπ) αλλά έχουν και κάποια επιπρόσθετα χαρακτηριστικά, όπως κουμπιά, leds, έλεγχο τροφοδοσίας (από USB ή μπαταρίες) και άλλα. Οι 2 πλακέτες είναι κατά βάση ίδιες, με την ZB502 να έχει μετρικές παραπάνω λειτουργίες καθώς αποτελεί την επόμενη έκδοση της ZB500. Το ενδεικτικό κόστος της κάθε πλακέτας σύμφωνα με την επίσημη ιστοσελίδα της Waveshare Electronics είναι 8€. Αναλυτικά τα χαρακτηριστικά της κάθε πλακέτας αναφέρονται παρακάτω και στις εικόνες φαίνεται σε ποιο στοιχείο της πλακέτας αντιστοιχεί η κάθε λειτουργία-λειτουργικότητα.

#### 7.1.2.1 ZB500



Εικόνα 7-7-4 Waveshare ZB500

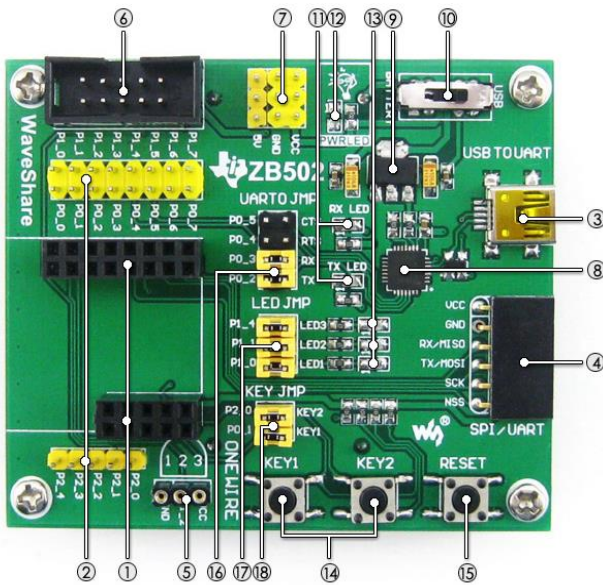
1. Θύρα υποδοχής Zigbee module
2. Διεπαφή I/Os
3. Διεπαφή USB
4. Διεπαφή UART/SPI
5. Διεπαφή ONE-WIRE
6. Διεπαφή debugging
7. 5V DC jack
8. Power pin headers (5V,3.3V,GND)
9. Ρυθμιστής τάσης AMS1117-3.3
10. PL2303 (USB to Serial Bridge Controller)
11. Onboard Crystal Oscillator
12. Power switch
13. Power Indicator

14. User LEDs
15. User Keys
16. Reset button

Ενδεικτικό κόστος: 8 €



### 7.1.2.2 ZB502



Εικόνα 7-5 Waveshare ZB502

1. Θύρα υποδοχής Zigbee module
2. Διεπαφή I/Os
3. Διεπαφή USB
4. Διεπαφή UART/SPI
5. Διεπαφή ONE-WIRE
6. Διεπαφή debugging
7. 5V/3.3V power input/output
8. CP2102 USB to UART Bridge
9. Ρυθμιστής τάσης AMS1117-3.3
10. Power switch
11. Serial port RX/TX

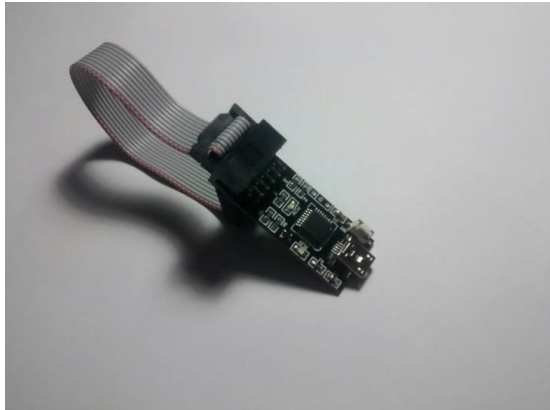
indicator

12. Power Indicator
13. User LEDs
14. User Keys
15. Reset button
16. UART0 jumper
17. LED jumper
18. KEY jumpe

**Ενδεικτικό κόστος: 8 €**

### 7.1.3 DEBUGGER

Για το κατέβασμα του κώδικα στο chip αλλά και το debugging χρησιμοποιήθηκε ο Zigbee Emulator Debugger Programmer που συνδέεται στην θύρα debugging της αναπτυξιακής πλακέτας μέσω 10-pin καλωδίου. Ενδεικτικό κόστος: 12€



Εικόνα 7-6 Debugger

### 7.1.4 CC2531

Για την παρατήρηση του δικτύου Zigbee και των πακέτων στον αέρα χρησιμοποιήθηκε το CC2531 USB Dongle της Webee με προεγκατεστημένο λογισμικό για packet sniffing. Τα γενικά χαρακτηριστικά του CC2531 είναι παρόμοια με αυτά του CC2530, μόνο που διαθέτει διεπαφή USB για απευθείας σύνδεση πράγμα που το καθιστά ιδανική επιλογή για χρήση ως packet sniffer. Ενδεικτικό κόστος : 12€



Εικόνα 7-7 Webee CC2531 sniffer

## 7.1.5 SENSORS

### 7.1.5.1 Ψηφιακό θερμομέτρο DS18B20

Για την μέτρηση θερμοκρασίας χρησιμοποιήθηκε το ψηφιακό θερμομέτρο DS18B20. Το θερμομέτρο αυτό χρησιμοποιεί 1-Wire επικοινωνία και παρέχει μετρήσεις θερμοκρασίας από 9 έως 12 bits ανάλογα με το resolution που έχει τεθεί. Επίσης κάθε τέτοιο θερμομέτρο φέρει έναν μοναδικό 64-bit κωδικό, πράγμα που επιτρέπει την πολλαπλή σύνδεση τέτοιων αισθητήρων σε έναν μικροελεγκτή. Ενδεικτικό κόστος: 2€



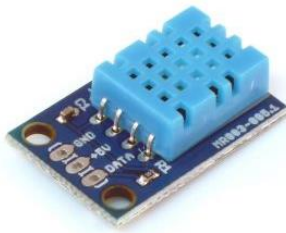
Εικόνα 7-8 Ψηφιακό θερμομέτρο DS28B20 - pins

Παρακάτω αναφέρονται αναλυτικά τα χαρακτηριστικά του αισθητήρα.

- Διεπαφή 1-Wire (απαιτείται μόνο 1 port-pin για λειτουργία)
- Μέτρηση θερμοκρασιών από -55°C έως +125°C (-67°F to +257°F)
- $\pm 0.5^\circ\text{C}$  ακρίβεια από -10°C to +85°C
- Ορισμός ανάλυσης θερμοκρασίας από τον χρήστη (9-12bits)
- 64bit σειριακός κωδικός σε κάθε αισθητήρα
- Δυνατότητα τροφοδοσίας από data pin. Εύρος τροφοδοσίας 3-5.5V
- Δυνατότητα μη πτητικής αποθήκευσης προτιμήσεων και ρυθμίσεων από τον χρήστη(upper and lower trigger points, alarm settings κλπ)

### 7.1.5.2 Ψηφιακός αισθητήρας θερμοκρασίας και υγρασίας DHT11

Για την μέτρηση θερμοκρασίας και της υγρασίας του αέρα χρησιμοποιήθηκε το ψηφιακό θερμόμετρο DHT11. Το θερμόμετρο αυτό χρησιμοποιεί 1-Wire επικοινωνία και παρέχει μετρήσεις θερμοκρασίας και υγρασίας 8bit. Συνδέεται στην διεπαφή one-Wire της αναπτυξιακής πλακέτας μέσω 3 pin (τροφοδοσία, data και GND). Ενδεικτικό κόστος: 3€



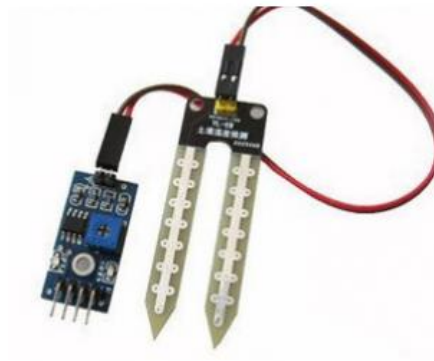
Εικόνα 7-9 Ψηφιακός αισθητήρας DHT11

Παρακάτω αναφέρονται αναλυτικά τα χαρακτηριστικά του αισθητήρα.

- Διεπαφή 1-Wire (απαιτείται μόνο 1 port-pin για λειτουργία)
- Εύρος θερμοκρασιών 0-50°C
- Ακρίβεια μέτρησης θερμοκρασίας  $\pm 2^{\circ}\text{C}$
- Εύρος σχετικής υγρασίας 20-90%
- Ακρίβεια μέτρησης υγρασίας  $\pm 5\%$

### 7.1.5.3 Αισθητήρας υγρασίας χώματος LM393

Για την μέτρηση της υγρασίας του χώματος χρησιμοποιήθηκε ο εν λόγω αισθητήρας που χρησιμοποιεί τον διαφορικό συγκριτή LM393. Από τα 4 pins που διαθέτει συνδέονται τα 3 τα οποία αποτελούν την τροφοδοσία(3.3V-5V), την γείωση και το 3ο είναι είτε η ψηφιακή είτε η αναλογική έξοδος. Στην συγκεκριμένη εφαρμογή έγινε χρήση της αναλογικής εξόδου σε συνδυασμό με την ADC (Analog to Digital Converter) λειτουργία του CC2530. Ενδεικτικό κόστος: 4€



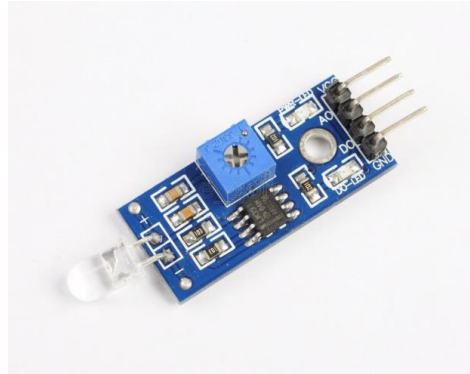
Εικόνα 7-10 Αισθητήρας υγρασίας χώματος

Παρακάτω αναφέρονται αναλυτικά τα χαρακτηριστικά του αισθητήρα.

- Ρυθμιζόμενη ευαισθησία μέσω ποτενσιόμετρου
- Ψηφιακή και αναλογική έξοδος (πιο ακριβής)
- Θερμοκρασία λειτουργίας -40°C έως +125°C
- Τροφοδοσία λειτουργίας: 3.3-5V
- Κατανάλωση ισχύος 1-6W
- 4-pins: VCC (3.3-5V), GND, DO-digital output (0-1), AO-analog output
- 2 LEDs: ένα κόκκινο που λειτουργεί ως power indicator και ένα πράσινο που λειτουργεί ως digital output indicator (ανάβει όταν η τιμή της υγρασίας είναι μικρότερη από μια τιμή κατωφλιού που έχει θέσει ο χρήστης)

#### 7.1.5.4 Αισθητήρας φωτεινότητας LM393

Ο εν λόγω αισθητήρας φωτεινότητας που χρησιμοποιήθηκε έχει παρόμοια λειτουργία με τον αισθητήρα υγρασίας χώματος που αναλύθηκε προηγουμένως και χρησιμοποιεί και αυτός τον διαφορικό συγκριτή LM393 συνδεδεμένο με μια φωτοαντίσταση. Η σύνδεση έγινε μέσω της αναλογικής εξόδου και με χρήση του ADC. Ενδεικτικό κόστος: 2€



Εικόνα 7-11 Αισθητήρας φωτεινότητας

Παρακάτω αναφέρονται αναλυτικά τα χαρακτηριστικά του αισθητήρα.

- Ρυθμιζόμενη ευαισθησία μέσω ποτενσιόμετρου
- Ψηφιακή και αναλογική έξοδος (πιο ακριβής)
- Τροφοδοσία λειτουργίας: 3.3-5V
- 4-pins: VCC (3.3-5V), GND, DO-digital output (0-1), AO-analog output

#### 7.1.6 Υπολογισμός συνολικού κόστους υλικού

Για τον υπολογισμό του συνολικού κόστους δεν θα ληφθεί υπόψη το CC2531 Usb Dongle καθώς χρησιμοποιήθηκε μόνο για λόγους κατανόησης και παρατήρησης του δικτύου και δεν χρησιμεύει στην ανάπτυξη και λειτουργία του ασύρματου δικτύου.

Το συνολικό κόστος υπολογίζεται στον Πίνακα 7-1.

Περιγραφή υλικού	Αριθμός	Κόστος(€)
CC2530	4	40
ZB500-ZB502	4	32
DEBUGGER	1	12
DS18B20	1	2
DHT11	1	3
Αισθητήρας υγρασίας χώματος	1	4
Αισθητήρας φωτεινότητας	1	2
Σύνολο		96

Πίνακας 7-1 Συνολικό κόστος υλικού

## 7.2 Λογισμικό-Software

### 7.2.1 Z-Stack

Για την ανάπτυξη της εν λόγω εφαρμογής χρησιμοποιήθηκε η στοίβα πρωτοκόλλων Z-Stack της Texas Instruments. Το Z-Stack διαθέτει πλήρη συμβατότητα με τις προδιαγραφές IEEE 802.15.4 και Zigbee (ZigBee και ZigBee PRO). Παρέχει βιβλιοθήκες για όλες τις λειτουργικότητες που παρέχει το πρότυπο Zigbee καθώς και υποστηρικτικές βιβλιοθήκες και ενδεικτικές εφαρμογές για ορισμένες αναπτυξιακές πλακέτες της Texas Instruments.

Το Z-Stack παρέχεται σε διάφορες παραλλαγές ανάλογα με τα Zigbee Profiles τα οποία ενσωματώνει και τις λειτουργίες τις οποίες έρχεται να καλύψει. Οι παραλλαγές που παρέχει η Texas Instruments είναι οι εξής:

- **Z-Stack Home:** Παρέχει βιβλιοθήκες και εργαλεία για την ανάπτυξη εφαρμογών στον τομέα του Home Automation ενσωματώνοντας το Home Automation profile της προδιαγραφής Zigbee.
- **Z-Stack-Energy:** Παρέχει βιβλιοθήκες και εργαλεία για την ανάπτυξη εφαρμογών στους τομείς της ενεργειακής διαχείρισης και παρακολούθησης ενσωματώνοντας το Smart Energy profile της προδιαγραφής Zigbee.
- **Z-Stack Lighting:** Παρέχει βιβλιοθήκες και εργαλεία για την ανάπτυξη εφαρμογών που εξειδικεύονται σε έλεγχο και διαχείριση φωτισμού βιομηχανικών ή οικιακών εγκαταστάσεων.
- **Z-Stack-Mesh:** Παρέχει βιβλιοθήκες και εργαλεία για την ανάπτυξη εφαρμογών που απαιτούν την ύπαρξη και διατήρηση μεγάλης κλίμακας mesh δικτύου

Για την παρούσα εφαρμογή χρησιμοποιήθηκε η έκδοση 1.2.1 του Z-Stack Home η οποία παρέχει τα εξής:

- Βιβλιοθήκες με τις παρεχόμενες από την προδιαγραφή Zigbee λειτουργίες όλων των επιπέδων δικτύωσης.
- Βιβλιοθήκες HAL (Hardware Abstraction Layer) που αφορούν τις περιφερειακές λειτουργίες του CC2530 και της αναπτυξιακής πλακέτας.  
Επίσης παρέχονται οι ίδιες βιβλιοθήκες για το microchip CC2538 που αποτελεί την ARM-Based λύση της Texas Instruments.
- Βιβλιοθήκη με όλα τα παρεχόμενα clusters (ZCL- Zigbee Cluster Library)
- Sample projects για εφαρμογές Home Automation: όπως Lighting control, HVAC (heating, ventilating, and air conditioning) Control και Security control (Door-lock).

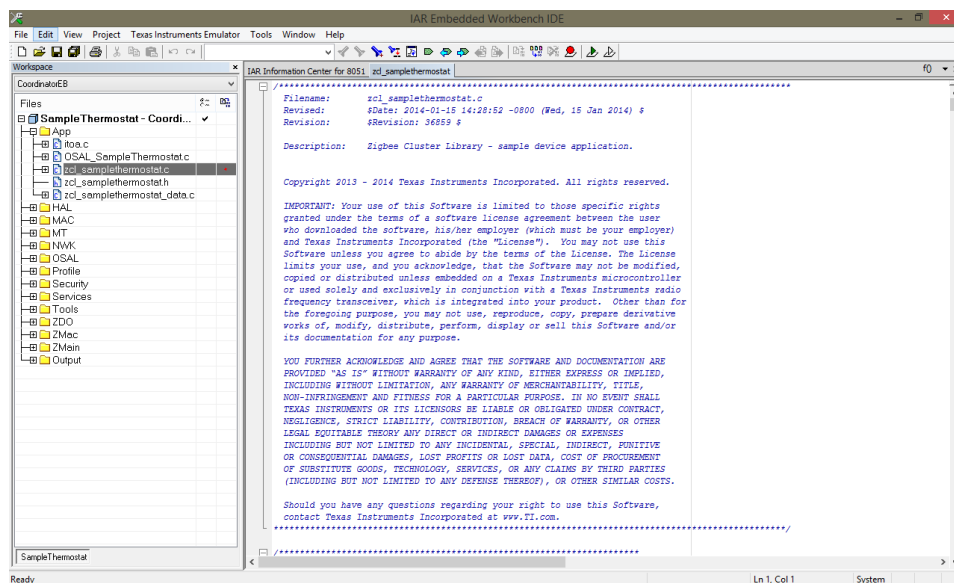
- Βιβλιοθήκες OTA (Over The Air) για ασύρματο update των συσκευών μετά την εγκατάστασή τους.

Όλος ο πηγαίος κώδικας και οι βιβλιοθήκες του Z-Stack παρέχονται δωρεάν.

## 7.2.2 IAR Embedded Workbench for 8051

Το αναπτυξιακό εργαλείο που χρησιμοποιήθηκε για την συγγραφή του κώδικα των microchips καθώς και για το κατέβασμα του κώδικα στις συσκευές και το debugging ήταν το IAR Embedded Workbench for 8051 της IAR Systems. Η έκδοση που χρησιμοποιήθηκε είναι η 9.10.

Το αναπτυξιακό αυτό εργαλείο αποτελεί ένα IDE (Integrated Development Environment) που έχει πλήρη συμβατότητα με το Z-Stack καθώς και με τα microchips της Texas Instruments και τις αναπτυξιακές πλακέτες.



Εικόνα 7-12 Περιβάλλον ανάπτυξης IAR Embedded Workbench

Τα βασικά χαρακτηριστικά του είναι:

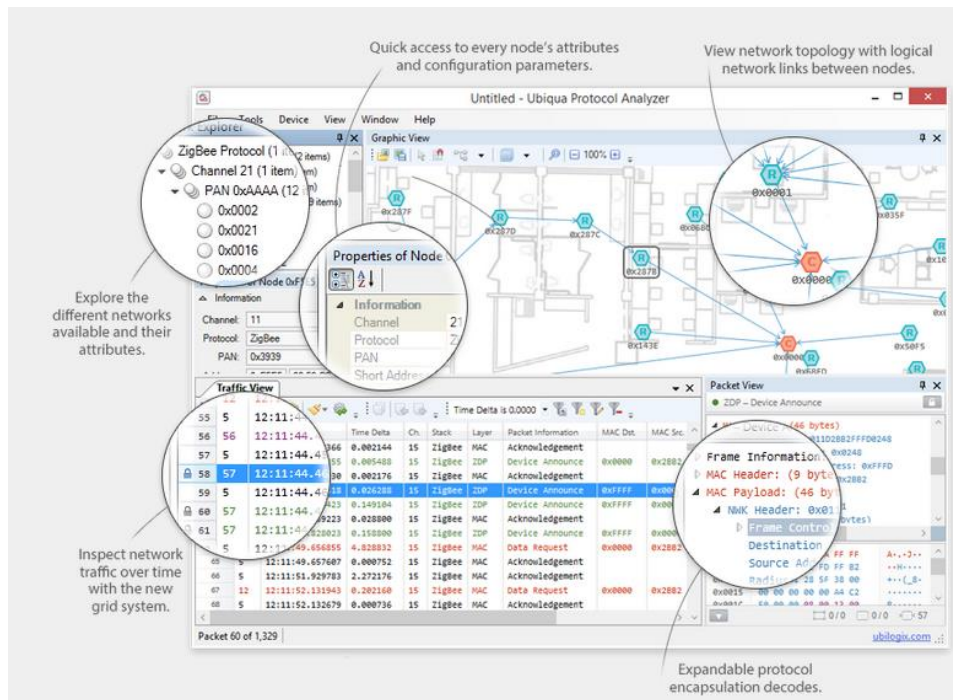
- Φιλικό προς τον χρήστη περιβάλλον ανάπτυξης
- Εύκολη περιήγηση στον πηγαίο κώδικα και τις βιβλιοθήκες
- Εύκολο και γρήγορο κατέβασμα κώδικα και debugging

Το IAR Embedded Workbench IDE παρέχεται με δωρεάν license ενός μήνα και έπειτα διατίθεται επί πληρωμή.



### 7.2.3 Ubiqia Protocol Analyzer

Για την παρατήρηση του δικτύου χρησιμοποιήθηκε το λογισμικό Ubiqia Protocol Analyzer της Ubilogix σε συνδυασμό με το microchip CC2531 που αναφέρθηκε στην προηγούμενη ενότητα. Το λογισμικό αυτό υποστηρίζει όλα τα πρωτόκολλα που στηρίζονται στο 802.15.4 όπως Zigbee, Zigbee IP και 6LoWPAN.



Εικόνα 7-13 Ubiqia Protocol Analyzer

Οι βασικές λειτουργίες που παρέχει είναι:

- Παρατήρηση όλων των υπάρχοντων δικτύων και των κόμβων που ανήκουν στο κάθε ένα
- Γραφική απεικόνιση της δομής του κάθε δικτύου με αναφορά του ρόλου κάθε συσκευής (C-coordinator, R-router, E-end device)
- Χρονική απεικόνιση όλων των πακέτων με δυνατότητα φιλτραρίσματος
- Δυνατότητα εξερεύνησης της πλήρους δομής του κάθε πακέτου και όλως των πεδίων του σε όλα τα στάδια της ενθυλάκωσης

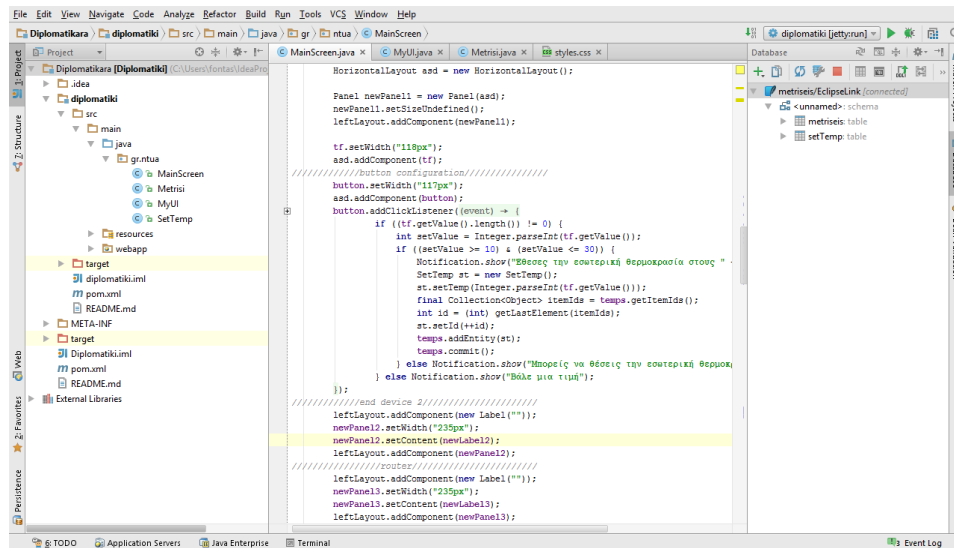
Εξαιτίας του επιπέδου προστασίας του πρωτοκόλλου Zigbee που χρησιμοποιεί το Z-Stack Home Automation για την αποκωδικοποίηση των μηνυμάτων πρέπει να εισάγουμε στο πρόγραμμα το Network key και το Trust Center Link key. Αυτά έχουν προκαθορισμένη τιμή που βρίσκεται στο documentation του Z-Stack HA αλλά μπορούν και να αλλάξουν.

Το λογισμικό Ubiqua Protocol Analyzer παρέχεται με δωρεάν license ενός μήνα και έπειτα διατίθεται επί πληρωμή.

Ένα άλλο πρόγραμμα για την παρατήρηση του δικτύου που παρέχεται δωρεάν είναι το Packet Sniffer της Texas Instruments αλλά προτιμήθηκε το Ubiqua Protocol Analyzer εξαιτίας του πιο φιλικού user interface.

## 7.2.4 IntelliJ IDEA

Για την ανάπτυξη της διεπαφής με τον υπολογιστή-server μέσω του UART αλλά και της web εφαρμογής για την παρατήρηση και τον έλεγχο της εγκατάστασης του θερμοκηπίου χρησιμοποιήθηκε το ολοκληρωμένο περιβάλλον ανάπτυξης σε Java, IntelliJ IDEA της JetBrains. Χρησιμοποιήθηκε η έκδοση v14.



Εικόνα 7-14 Περιβάλλον ανάπτυξης IntelliJ IDEA

### 7.2.4.1 Apache Maven v3.2.5

Για την εύκολη ανάπτυξη χρησιμοποιήθηκε το εργαλείο διαχείρισης apache maven. Το εργαλείο αυτό βασίζεται στην ιδέα του project object model (POM), μέσω του οποίου γίνεται η διαχείριση του java project και περιγράφεται το πώς γίνεται το build αυτού αλλά περιγράφονται και οι εξαρτήσεις (dependencies) του project, οι οποίες αποτελούν άλλα εξωτερικά modules, plug-ins και άλλα χρήσιμα μέρη που απαιτούνται στο project. Εκτός αυτών το apache maven έχει την δυνατότητα να κατεβάσει δυναμικά βιβλιοθήκες της Java αλλά και plug-ins και να τα αποθηκεύει σε τοπική cache.

Το εργαλείο αυτό είναι διαθέσιμο και για άλλες γλώσσες προγραμματισμού όπως C#, Ruby, Scala και άλλες. Παρέχεται και αναπτύσσεται από τον οργανισμό ASF (Apache Software Foundation).

#### **7.2.4.2 Jetty Server**

Ο jetty server χρησιμοποιήθηκε ως ο server που φιλοξενεί την web εφαρμογή. Αποτελεί Java HTTP Server και Java Servlet Container που σημαίνει ότι υποστηρίζει web περιεχόμενο όπως servlet και JSPs (JavaServer Pages) και ενσωματώνεται ως plug-in στο apache maven. Είναι open source και αναπτύσσεται από τον οργανισμό Eclipse Foundation.

#### **7.2.4.3 VAADIN Framework**

Για την ανάπτυξη της web εφαρμογής και της διεπαφής χρήστη (User Interface) χρησιμοποιήθηκε το Vaadin framework. Αυτό αποτελεί ένα java framework που δίνει την δυνατότητα για ανάπτυξη web εφαρμογών και μοντέρνων διεπαφών, παρέχοντας ένα αξιόπιστο μοντέλο server-side προγραμματισμού αλλά και client-side αναπτυξιακά εργαλεία που βασίζονται στο GWT (Google Web Toolkit) και στο HTML5. Το vaadin είναι open source και χρησιμοποιεί το Apache 2 license που σημαίνει ότι δεν υπάρχει κανένας περιορισμός για την χρήση του. Το vaadin επίσης ενσωματώνεται ως plug-in στο apache maven.

#### **7.2.4.4 Sqlite3 database**

Για την βάση δεδομένων που διατηρεί τις μετρήσεις για την εφαρμογή, χρησιμοποιήθηκε η sQLite που αποτελεί ένα σύστημα για την διαχείριση σχεσιακών βάσεων δεδομένων. Επιλέχθηκε καθώς επικεντρώνεται στην απλότητα και την αξιοπιστία και αποτελεί ιδανική επιλογή για εφαρμογές με μικρές απαιτήσεις όπως στην εν λόγω διπλωματική όπου απαιτείται η αποθήκευση μόνο 2 πινάκων και δεν απαιτούνται περίπλοκοι χειρισμοί.

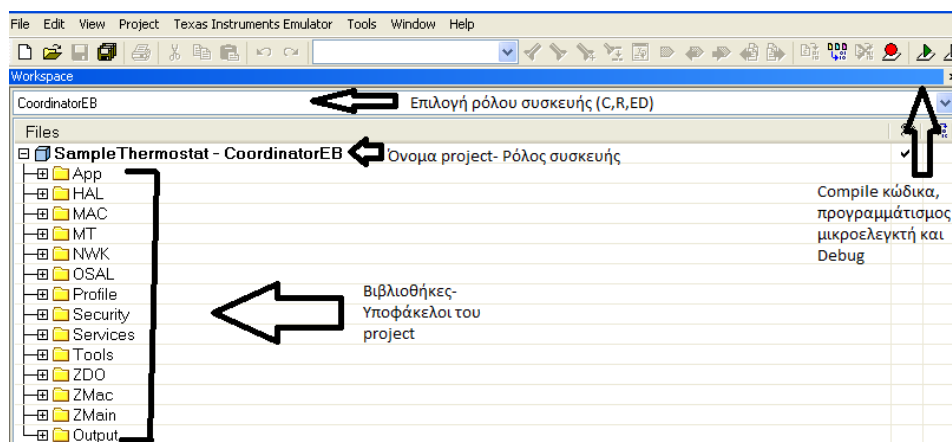
## 8 Έλεγχος θερμοκηπίου: ανάπτυξη και λειτουργία εφαρμογής

Το κεφάλαιο αυτό πραγματεύεται την εφαρμογή που δημιουργήσαμε στα πλαίσια της διπλωματικής. Η εφαρμογή χωρίζεται σε δύο διακριτά σκέλη. Από την μία έχουμε το δίκτυο αισθητήρων Zigbee και από την άλλη το Web Application που διαχειρίζεται τα δεδομένα του δικτύου. Αρχικά προσπαθούμε να παρουσιάσουμε βήμα προς βήμα τον προγραμματισμό των δύο σκελών. Έπειτα γίνεται μία αναφορά για την διαδικασία διασύνδεσης των κόμβων του δικτύου. Τέλος γίνεται επίδειξη των δυνατοτήτων που δίνει η εφαρμογή στον τελικό χρήστη.

### 8.1 Ανάπτυξη λογισμικού μικροελεγκτών

Η ανάπτυξη του λογισμικού των μικροελεγκτών, στηρίζεται στις βιβλιοθήκες της TI για το Z-Stack που αναφέρονται συγκεκριμένα για τον ελεγκτή CC2530. Σε αυτό το κεφάλαιο στόχος είναι η ανάλυση της δομής του Z-Stack και το πώς ο χρήστης κατανοώντας την μπορεί να δημιουργήσει οποιαδήποτε εφαρμογή. Το όριο βέβαια των δυνατοτήτων μας το καθορίζει το ίδιο το υλικό, πχ το σύνολο των PINS που διαθέτει, την συχνότητα λειτουργίας του και το μέγεθος της μνήμης.

Το περιβάλλον ανάπτυξης που χρησιμοποιούμε είναι το IAR λόγω της συμβατότητας του με τα project του Z-Stack. Στην Εικόνα 8-1 βλέπουμε πώς είναι δομημένο κάθε project, που προορίζεται για τον προγραμματισμό του CC2530.



Εικόνα 8-1 Δομή project IAR

Βλέπουμε ότι οι υποφάκελοι του project απαρτίζονται από 14 στοιχεία. Αν εξαιρέσουμε τον πρώτο φάκελο App, όλοι οι υπόλοιποι φάκελοι ασχολούνται με λειτουργίες που είναι καθολικές για όλες τις εφαρμογές. Αυτό σημαίνει ότι η τροποποίηση τους πρέπει να γίνεται με πολύ προσοχή καθώς είναι κοινί σε όλα τα project.

Οι βιβλιοθήκες- υποφάκελοι συνοπτικά είναι οι εξής:

- App: Περιέχει τα αρχεία .c και .h που είναι ξεχωριστά για κάθε εφαρμογή και διέπει τις «εξατομικευμένες» λειτουργίες
- HAL (Hardware Abstraction Layer): Περιέχει τις βιβλιοθήκες που περιγράφουν τον καθορισμό του υλικού (πχ ποια PIN αντιστοιχούν σε LEDs) και τις λειτουργίες του υλικού (πχ συναρτήσεις για λειτουργία των LEDs ON-OFF-Toggle-Blink).
- MAC: Περιέχει τους ορισμούς και τις συναρτήσεις για την λειτουργία του επιπέδου MAC (πχ συνάρτηση που σε ένα μήνυμα προς αποστολή δημιουργεί την εκάστοτε επικεφαλίδα MAC )
- MT (Monitor and Test): Περιέχει συναρτήσεις που επικοινωνούν με λογισμικό της TI εγκαθίσταται στο PC με στόχο την live παρακολούθηση ενεργειών του μικροελεγκτή
- NWK: Περιέχει συναρτήσεις και ορισμούς που ασχολούνται με το επίπεδο δικτύου για την επικοινωνία μέσω ZigBee
- OSAL (Operating System Abstraction Layer): Περιέχει μία πληθώρα συναρτήσεων που αποτελούν τις λειτουργίες ενός τυπικού λειτουργικού συστήματος και έτσι διευκολύνει την ανάπτυξη κάποιων λειτουργιών
- Profile: Περιέχει τους ορισμούς και τις συναρτήσεις για την επικοινωνία στο επίπεδο εφαρμογής και πιο συγκεκριμένα στο ZCL (Zigbee Cluster Layer). Οι ορισμοί, πχ των clusters και των layers, ακολουθούν την τυποποίηση του Zigbee Alliance.
- Security: Περιέχει συναρτήσεις και ορισμούς για την λειτουργία της ασφάλειας αποστολής των δεδομένων
- Tools: Ο φάκελος αυτός είναι πολύ σημαντικός καθώς περιέχει ορισμούς για τις πρωταρχικές ρυθμίσεις των παραμέτρων του δικτύου Zigbee. Αυτές ενδεικτικά είναι η επιλογή καναλιού, η επιλογή ή όχι PAN ID και το βάθος του mesh δικτύου με εκκίνηση τον Coordinator
- ZDO (Zigbee Device Object): Περιέχει τις συναρτήσεις για την πρώτη λειτουργία του επιπέδου εφαρμογής, πχ την αναγνώριση συσκευών Zigbee στο ίδιο δίκτυο
- ZMac: Περιέχει τις συναρτήσεις που αν και ανήκουν στην διαχείριση του Zigbee (άρα επίπεδο δικτύου και εφαρμογής) χρησιμοποιούν το επίπεδο MAC για να καλύψουν κάποιες ανάγκες όπως η σάρωση των συχνοτήτων που λειτουργούν δίκτυα ώστε ο Coordinator να διαλέξει την κατάλληλη.
- Zmain: Περιέχει κάποιες βασικές συναρτήσεις για την λειτουργία του υλικού, αλλά το σημαντικότερο είναι ότι στο αρχείο το Zmain.c υπάρχει η main που εκκινεί τον μικροελεγκτή

Είναι προφανές ότι οι παραπάνω επιμέρους βιβλιοθήκες για λόγους ευκολίας στην ανάπτυξη του χρησιμοποιούν συναρτήσεις από άλλες βιβλιοθήκες. Η βιβλιοθήκη

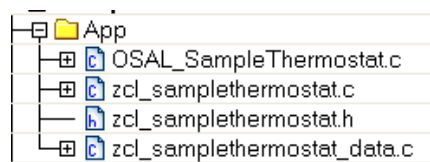
NWK πχ ενθυλακώνει κάποια συνάρτηση από την MAC καθώς το τελικό μήνυμα αποστέλεται από το επίπεδο MAC

Το output δεν είναι βιβλιοθήκη, αλλά είναι ένα αρχείο που κρατάει τις πληροφορίες που δημιουργήθηκαν κατά το compile του κώδικα, όπως τα logs και το τελικό αρχείο που θα περαστεί στον μικροελεγκτή.

## 8.1.1 Τροποποιήσεις

### 8.1.1.1 App

Αναφέραμε παραπάνω ότι η σημαντικότερη βιβλιοθήκη είναι η App, καθώς περιέχει ότι τις λειτουργίες κάθε ξεχωριστής εφαρμογής που θα προγραμματίσει έναν συγκεκριμένο μικροελεγκτή ή μια ομάδα μικροελεγκτών που θα εκτελούν τις ίδιες ακριβώς λειτουργίες.



Εικόνα 8-2 Δομή υποφακέλου App

Βλέπουμε στην Εικόνα 8-2 ότι αποτελείται πάντα από 4 τουλάχιστον αρχεία. Τα βασικά αρχεία αυτά συνοπτικά είναι:

- OSAL\_xxx.c : Περιέχει πάντα την συνάρτηση OsalInitTasks που δημιουργεί έναν πίνακα με τα Tasks (έργα) και αρχικοποιεί τις λειτουργίες τους
- Zcl\_xxx.c : Περιέχει σίγουρα τις συναρτήσεις εκκίνησης του Task (zcl\_xxxInit) που ανήκει στην εφαρμογή zcl\_xxx και την zclxxx\_event\_loop που μπορεί να αναγνωρίσει ποιο συμβάν έχει προκύψει και να το διαχειριστεί. Πέρα από αυτές τις δύο συναρτήσεις υπάρχουν υποχρεωτικά και κάποιοι ορισμοί struct, πινάκων και σταθερών.

Σε αυτό το αρχείο ο χρήστης έχει την δυνατότητα να προσθέσει συναρτήσεις που θα χρησιμοποιήσει για την τελική λειτουργία της εφαρμογής του. Ενδεικτικά μπορεί να δημιουργήσει τις συναρτήσεις για αποστολή δεδομένων στην UART, το διάβασμα μετρήσεων από τους αισθητήρες και την αναγνώριση εισερχομένων μηνυμάτων

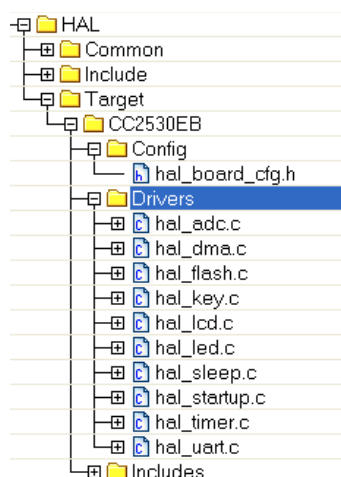
- Zcl\_xxx.h : Αυτό το αρχείο περιέχει κατά κύριο λόγο ορισμούς σταθερών. Η πιο σημαντική σταθερά είναι ο ορισμός του EndPoint που μπορεί να καταστήσει την συσκευή μοναδική στο δίκτυο και να αναγνωρίζεται βάσει αυτού του χαρακτηριστικού. Εδώ ο χρήστης μπορεί να προσθέσει παραπάνω Event τα οποία μετα θα δημιουργήσει στο Zcl\_xxx.c.

- `Zcl_xxx_data.c` : Αυτό το αρχείο φιλοξενεί, όπως μαρτυρα και το όνομα του, τις πληροφορίες του Zigbee. Πιο συγκεκριμένα έχει πληροφορίες σχετικά με τα χαρακτηριστικά της συσκευής (πχ τροφοδοσία, ημερομηνία παραγωγής) και περιέχει τα Attributes που θα χρησιμοποιήσει η συγκεκριμένη συσκευή

Τέλος, εκτός από όλα τα παραπάνω, ο χρήστης έχει την δυνατότητα να προσθέσει κάποιο επιπλέον αρχείο, το οποίο μπορεί για παράδειγμα να περιέχει την βιβλιοθήκη για έναν ψηφιακό αισθητήρα που χρησιμοποιεί η συσκευή. Έτσι την χρησιμοποιεί απλά ενσωματώνοντας το κατάλληλο `#include` στο `Zcl_xxx.c`.

### 8.1.1.2 HAL

Η βιβλιοθήκη HAL είναι το εργαλείο του χρήστη για να επικοινωνεί με το υλικό (Hardware) της συσκευής.



Εικόνα 8-3 Δομή φακέλου HAL

Οι λειτουργίες που περιέχονται αφορούν τα : ADC(Analog-Digital Conversion), DMA (Direct Memory Access), flash, LCD, LED, Sleep, Startup, Timer, UART. Το αρχείο `hal_board_cfg` πρέπει να τροποποιείται ανάλογα την αναπτυξιακή πλακέτα που χρησιμοποιούμε ή το custom hardware που έχουμε στήσει γύρω από το CC2530. Οι προεπιλεγμένες ρυθμίσεις αντιστοιχούν στο επίσημο αναπτυξιακό της TI. Στην περίπτωση μας χρησιμοποιούμε τα ZB500 και ZB502 οπότε έγιναν οι κατάλληλες αλλαγές για να λειτουργούν οι εξωτερικές συσκευές, πχ LEDs, κουμπιά, UART.

### 8.1.2 Βήματα λειτουργίας

Η λειτουργία του μικροελεγκτή ξεκινάει από `main`. Στην `main` αρχικά απενεργοποιούνται τα Interrupts και γίνεται μια σειρά εκκινήσεων, δηλαδή εκτελούνται διάφορες συναρτήσεις που χαρακτηρίζονται με `xxxInit` και εκτελούνται μόνο στην αρχή για την αρχικοποίηση κάποιων παραμέτρων, υλικού κυρίως.

Αφού γίνει η αρχικοποίηση η `main` καταλήγει στην `osal_start_system` όπου εκκινεί την κυρίως λειτουργία του μικροελεγκτή. Η `osal_start_system` εκτελεί μία αέναη επανάληψη της `osal_run_system`.

Πρέπει να σημειώσουμε σε αυτό το σημείο ότι ο προγραμματισμός του Z-Stack είναι event-driven. Αυτό σημαίνει ότι δημιουργεί μία σειρά από συμβάντα και όταν προκύψει κάποιο το εξυπηρετεί με την σειρά που εκχωρήθηκε στον πίνακα αναμονής των συμβάντων. Κάθε κωδικός event χαρακτηρίζεται από έναν δυαδικό αριθμό ο οποίος έχει 1 σε διαφορετική θέση κάθε φορά. Όπως αναφέρθηκε νωρίτερα, η `zclxxx_event_loop` διαχειρίζεται τα συμβάντα αυτά κάνοντας κάθε φορά μία σειρά από if με συνθήκη τον κωδικό του τρέχοντος event με όλα τα πιθανά event. Όταν η συνθήκη γίνει αληθής εξυπηρετεί το συγκεκριμένο event.

Συνοπτικά η διαδικασία κυρίως λειτουργίας είναι η μόνιμη ανίχνευση για την εμφάνιση συμβάντων και η εξυπηρέτηση τους με την σειρά που δηλώθηκαν. Βάσει αυτού ο προγραμματιστής έχει απεριόριστες δυνατότητες, καθώς μπορεί να δημιουργεί πολλά event που θα εκτελούν διαφορετικές λειτουργίες. Όμως είναι σημαντικό κατά τον προγραμματισμό της συσκευής να θυμόμαστε ότι οι πόροι του μικροελεγκτή είναι περιορισμένοι και συνεπώς πολλές φορές μπορεί να εμφανιστεί σφάλμα, λόγω περιορισμένης μνήμης για παράδειγμα.

## 8.2 Ανάπτυξη λογισμικού Web Application

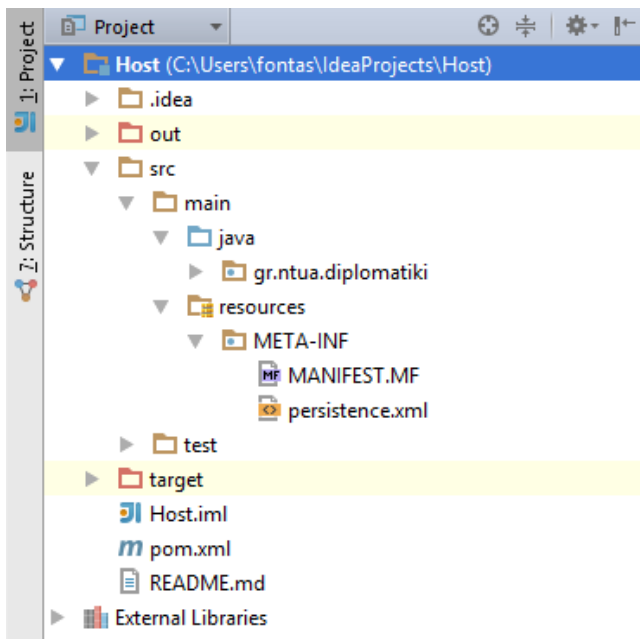
Στο προηγούμενο κεφάλαιο αναλύθηκαν τα εργαλεία που χρησιμοποιήθηκαν για την ανάπτυξη της διεπαφής μεταξύ του υπολογιστή-server και της σειριακής (UART) και της web εφαρμογής για την δημοσίευση των μετρήσεων στο internet και τον έλεγχο παραμέτρων του θερμοκηπίου. Σε αυτή την ενότητα γίνεται η περιγραφή της λειτουργίας και της ανάπτυξης των παραπάνω και ο αναγνώστης έχει την ευκαιρία να δει βήμα-βήμα τα βασικά στάδια της διαδικασίας αυτής.

Οι παραπάνω λειτουργίες χωρίστηκαν σε 2 διαφορετικά project. Το ένα που ονομάζεται Host (βλ. συνοδευτικό υλικό) αποτελεί μια τοπική εφαρμογή java που αναλαμβάνει τις λειτουργίες διαβάσματος και γραψίματος στην σειριακή (UART) και το πέρασμα των τιμών σε μια τοπική βάση δεδομένων. Το άλλο project (Diplomatiki βλ. συνοδευτικό υλικό) αναλαμβάνει τον ρόλο του server της web εφαρμογής και είναι υπεύθυνο για την κατασκευή και απεικόνιση της διεπαφής χρήστη στον browser όταν ο χρήστης κάνει μια αίτηση σε αυτόν.

### 8.2.1 Host

Η βασική δομή του project του Host φαίνεται στην Εικόνα 8-4.



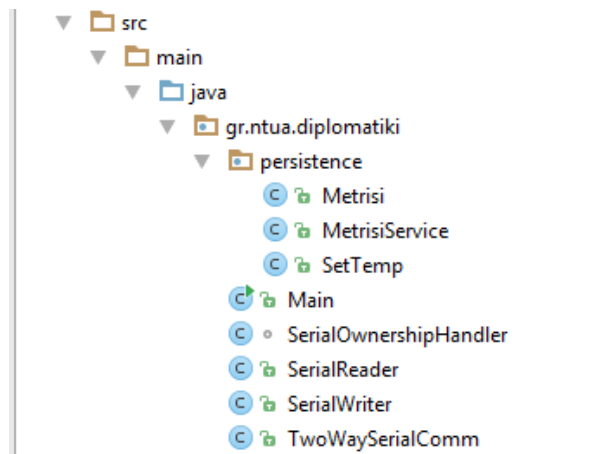


Εικόνα 8-4 Δομή Host

Τα βασικά στοιχεία της δομής αυτής είναι:

1. Ο φάκελος java που περιέχει τον πηγαίο κώδικα της τοπικής εφαρμογής δηλαδή όλες τις κλάσεις και την Main κλάση που εκτελείται.
2. Ο φάκελος resources περιέχει στον υποφάκελο META-INF το αρχείο persistence.xml οπού ορίζεται η σχέση με την βάση δεδομένων, οι κλάσεις των στοιχείων που θα περιέχει και δίνεται και το path στο οποίο βρίσκεται η ίδια η βάση δεδομένων.
3. Το αρχείο pom.xml που όπως αναφέρθηκε στο προηγούμενο κεφάλαιο περιέχει όλα τα dependencies του project και τα plugins όπως πχ το javax.persistence για την βάση δεδομένων και το plug-in του maven-compiler.

Η δομή του φακέλου java φαίνεται στην Εικόνα 8-5.



Εικόνα 8-5 Δομή φακέλου java

Ο υποφάκελος persistence περιέχει κλάσεις που αφορούν την βάση και την σχέση του main προγράμματος με αυτή. Η κλάση Metrisi ορίζει ένα αντικείμενο που αποτελείται από τις μετρήσεις που διαβάζονται περιοδικά από την σειριακή. Για κάθε πακέτο μετρήσεων που καταφθάνει στην σειριακή κατασκευάζεται ένα τέτοιο αντικείμενο. Οι μεταβλητές της κλάσης φαίνονται στην Εικόνα 8-6.

```

@Entity
@Table(name = "metriseis", schema = "", catalog = "")
public class Metrisi {
    private Integer id;
    private int t1;
    private int t2;
    private int h1;
    private int h2;
    private int l;
    private Date timestamp;

    @Id
    @Column(name = "ID")
    public Integer getId() { return id; }

    public void setId(Integer id) { this.id = id; }
}

```

Εικόνα 8-6 Μεταβλητές κλάσης Metrisi

Εκτός από τις 5 int μετρήσεις (θερμοκρασίες t1,t2, υγρασίες h1,h2, φωτεινότητα l) έχουμε άλλα 2 πεδία: το id που αποτελεί το αναγνωριστικό που θα χρησιμοποιηθεί για την αποθήκευση στην βάση δεδομένων και το timestamp που ανήκει στην κλάση Date και αποτελεί όλα τα στοιχεία ώρας και ημερομηνίας που αφορούν το αντικείμενο και την εισαγωγή του στην βάση. Τα 2 αυτά πεδία παράγονται αυτόματα. Η κλάση επίσης περιέχει όλους τους setters και getters για τις μεταβλητές της.

Η κλάση SetTemp αποτελεί την τιμή της θερμοκρασίας που ο χρήστης ορίζει από την διεπαφή της web εφαρμογής και περιέχει την int τιμή της οριζόμενης θερμοκρασίας και τα 2 αυτομάτως οριζόμενα πεδία που αναφέρθηκαν παραπάνω (id και timestamp).

```

@Entity
@Table(name = "setTemp", schema = "", catalog = "")
public class SetTemp {
    private Integer id;
    private int temp;
    private Date timestamp;
}

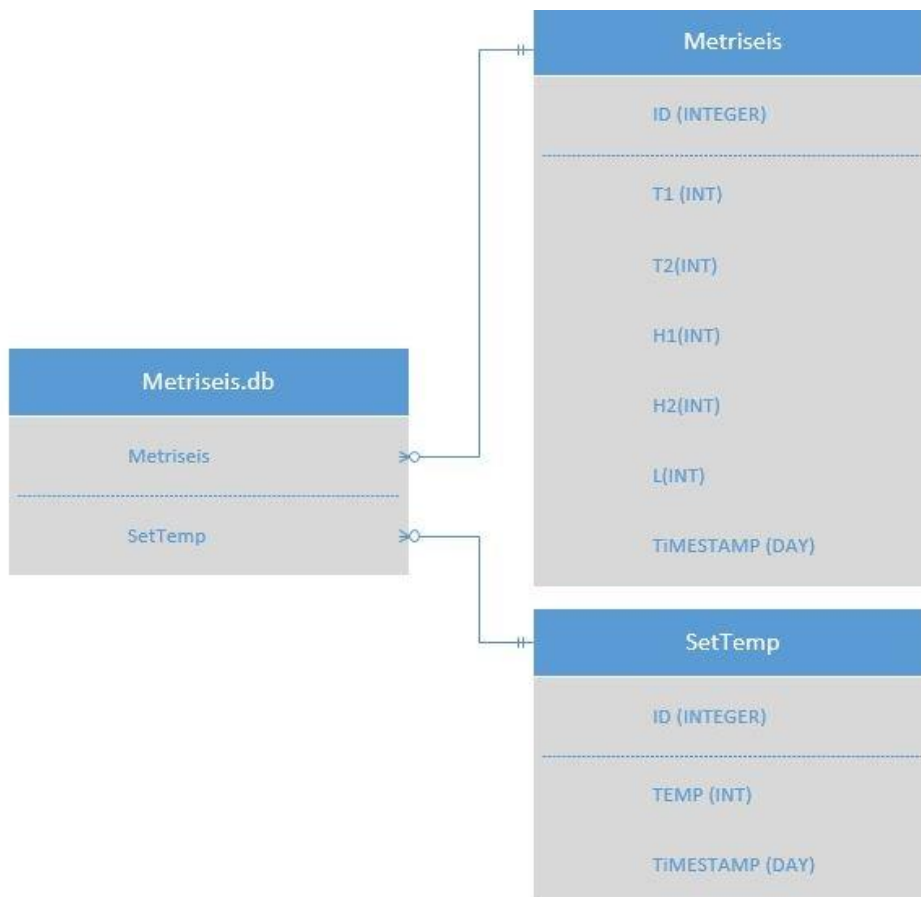
```

Εικόνα 8-7 Μεταβλητές κλάσης SetTemp

Τέλος η κλάση MetrisiService περιέχει τις συναρτήσεις που αλληλεπιδρούν με την βάση δεδομένων. Έχουμε 3 συναρτήσεις: 1)addNew, η οποία δέχεται σαν όρισμα ένα αντικείμενο τύπου Metrisi και το τοποθετεί στην βάση στον πίνακα metriseis 2)getTempCount, η οποία υπολογίζει το πλήθος των στοιχείων του πίνακα setTemp της βάσης και το επιστρέφει ως int και 3) getLastTemp η οποία επιστρέφει την τελευταία τιμή του πίνακα setTemp.

Στο σημείο αυτό θα ήταν χρήσιμο να αναφερθεί η δομή της βάσης δεδομένων για να γίνει ευκολότερη η κατανόηση των παραπάνω, αλλά και των μετέπειτα βημάτων.

Η βάση αποτελείται από 2 πίνακες: 1)τον πίνακα metriseis και 2)τον πίνακα setTemp. Ο 1<sup>ος</sup> περιέχει μια μετά την άλλη τις μετρήσεις που καταφθάνουν στην σειριακή και ο 2<sup>ος</sup> περιέχει τις τιμές για την θερμοκρασία που ορίζει ο χρήστης από την διεπαφή της web εφαρμογής. Σχηματικά η βάση φαίνεται στην παρακάτω



Η εκτέλεση της τοπικής εφαρμογής ξεκινάει από την Main κλάση, η οποία το μόνο που κάνει είναι να ορίζει το αναγνωριστικό της σειριακής πόρτας που θέλουμε (COM5 στην περίπτωση μας) και να καλεί την συνάρτηση σύνδεσης σε αυτή.

```

public class Main {
    public static void main(String[] args) {
        try {
            new TwoWaySerialComm().connect("COM5");
        } catch (UnsupportedCommOperationException e) {
            e.printStackTrace();
        }
    }
}

```

Εικόνα 8-8 Main class

Η TwoWaySerialComm περιέχει την συνάρτηση connect που καλείται από την Main και αφού ορίσει τις παραμέτρους για την σειριακή επικοινωνία (baud rate, stop\_bits κλπ), καθώς και τα streams για ανάγνωση και γράψιμο σε αυτή εκκινεί 2 threads, ένα που αναλαμβάνει την ανάγνωση από την σειριακή όταν υπάρχουν bytes δεδομένων σε αυτή και ένα που αναλαμβάνει το περιοδικό έλεγχο της βάσης (συγκεκριμένα του πίνακα setTemp) για εντοπισμό νέας τιμής οριζόμενης θερμοκρασίας από τον χρήστη και εγγραφή της τιμής στην σειριακή. Επίσης περιέχει και μια συνάρτηση disconnect σε περίπτωση που θέλουμε να αποσυνδεθούμε από την σειριακή πόρτα.

```

serialPort.setSerialPortParams(115200, SerialPort.DATABITS_8, SerialPort.STOPBITS_1, SerialPort.PARITY_NONE);

in = serialPort.getInputStream();
out = serialPort.getOutputStream();

(new Thread(new SerialReader(in))).start();
(new Thread(new SerialWriter(out))).start();

```

Εικόνα 8-9 Συνάρτηση connect() της κλάσης TwoWaySerialComm

Η κλάση SerialReader διαβάζει τα διαθέσιμα δεδομένα που υπάρχουν στην σειριακή και δημιουργεί ένα αντικείμενο Metrиси την φορά με τα δεδομένα που συνέλλεξε. Έπειτα καλεί την addNew της κλάσης MetrисиService και προσθέτει το αντικείμενο στην βάση δεδομένων στον πίνακα metriseis. Ο τρόπος με τον οποίο επιλέξαμε να στέλνονται οι μετρήσεις από τον μικροελεγκτή είναι της μορφής **xx-xx-xx** όπου xx είναι η κάθε μέτρηση σε μορφή διψήφιου ακεραίου. Η SerialReader διαχωρίζει τις επιμέρους τιμές και δημιουργεί το αντικείμενο Metrиси.

```

Metrиси m = new Metrиси();
m.setT1(t1);
m.setT2(t2);
m.setH1(h1);
m.setH2(h2);
m.setL(l);
ms.addNew(m);

```

Εικόνα 8-10 SerialReader

Η κλάση `SerialWriter` διαβάζει ανα 5 δευτερόλεπτα τις αλλαγές στον πίνακα `setTemp` της βάσης δεδομένων (συγκρίνοντας τα συνολικά στοιχεία πριν και μετά) και αν εντοπίσει αλλαγή, στέλνει την καινούργια τιμή στην σειριακή.

```
while(true) {
    Thread.sleep(5000);
    int newcount = ms.getTempCount(); //works
    System.out.println("COUNT IS: " + newcount);
    if (newcount > lastcount) {
        SetTemp last = ms.getLastTemp();
        System.out.println("it works! " + last.getTemp());
        lastcount=newcount;
        try {
            this.out.write((Integer.toString(last.getTemp()).getBytes()));
        } catch (IOException e) {
            e.printStackTrace();
        }
    }
}
```

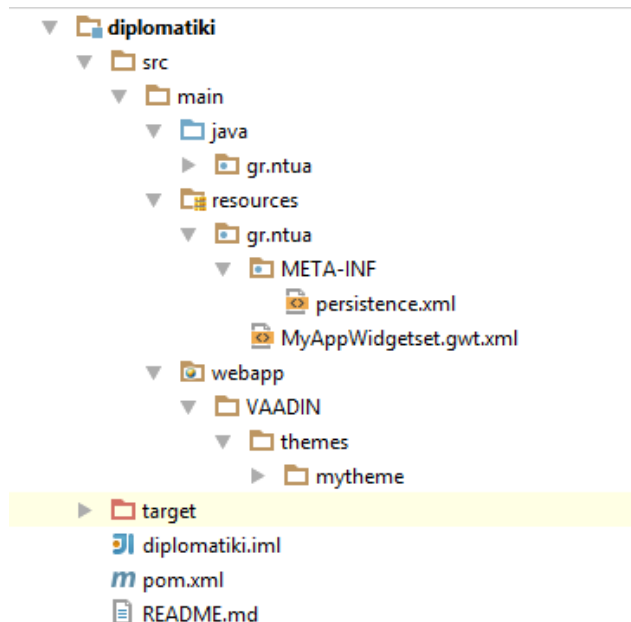
Εικόνα 8-11 `SerialWriter`

Τέλος η κλάση `SerialOwnershipHandler` αποτελεί έναν handler που μας ενημερώνει για την κατάσταση της πόρτας της σειριακής.

Οι πλήρεις κώδικες του `Host` είναι διαθέσιμοι στο συνοδευτικό υλικό.

## 8.2.2 Diplomatiiki

Η βασική δομή του project `Diplomatiki` φαίνεται στην Εικόνα 8-4.

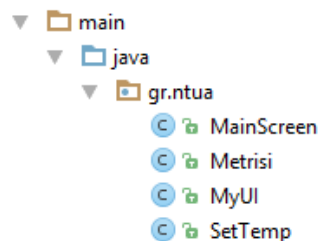


Εικόνα 8-12 Δομή `Diplomatiki`

Τα βασικά στοιχεία της δομής αυτής είναι:

1. Ο φάκελος java που περιέχει τον πηγαίο κώδικα της εφαρμογής δηλαδή όλες τις κλάσεις σε μορφή package με το όνομα gr.ntua.
2. Ο φάκελος resources περιέχει στον υποφάκελο META-INF το αρχείο persistence.xml οπου ορίζεται η σχέση με την βάση δεδομένων, οι κλάσεις των στοιχείων που θα περιέχει και δίνεται και το path στο οποίο βρίσκεται η ίδια η βάση δεδομένων.
3. Ο φάκελος webapp όπου εμπεριέχει αρχείο που σχετίζονται με το vaadin και συγκεκριμένα το θέμα mytheme που χρησιμοποιήθηκε στο project (css αρχεία που ορίζουν την εμφάνιση και μορφοποίηση των στοιχείων της διεπαφής).
4. Το αρχείο pom.xml που όπως αναφέρθηκε στο προηγούμενο κεφάλαιο περιέχει όλα τα dependencies του project και τα plugins όπως πχ το javax.persistence για την βάση δεδομένων, το plug-in του maven-compiler και το plug-in του vaadin framework.

Η δομή του φακέλου java φαίνεται στην Εικόνα 8-5.



Εικόνα 8-13 Δομή φακέλου java

Οι κλάσεις Metrisi και SetTemp αναφέρθηκαν στην ανάλυση του Host. Η κλάση MyUI η οποία κάνει extend την κλάση UI της βιβλιοθήκης του vaadin αποτελεί το βασικό στοιχείο της διεπαφής χρήστη. Φέρει την συνάρτηση init η οποία αρχικοποιεί την οθόνη που βλέπει ο χρήστης μόλις κάνει κλήση στον server. Έπειτα εκκινεί ένα thread (updateUiThread) που κάθε 5 δευτερόλεπτα ανανεώνει την οθόνη (Εικόνα 8-14).

```

@Theme("mytheme")
@Push
@Widgetset("gr.ntua.MyAppWidgetset")
public class MyUI extends UI {

    MainScreen mainScreen = new MainScreen();

    @Override
    protected void init(VaadinRequest vaadinRequest) {

        setContent(mainScreen);
        new updateUiThread().start();

    }
}

```

Εικόνα 8-14 Συνάρτηση init της MyUI

Η κλάση MainScreen αποτελεί την βασική οθόνη της εφαρμογής. Κάνει extend την κλάση VerticalLayout του vaadin και αρχικοποιεί την οθόνη εμφανίζοντας τις τελευταίες μετρήσεις από την βάση δεδομένων, αλλά και διαγράμματα με τις τελευταίες 20 τιμές για κάθε μετρούμενο μέγεθος. Επίσης διαθέτει τις συναρτήσεις refresh() και refreshCharts() οι οποίες ανανεώνουν τα στοιχεία της οθόνης (τρέχουσες τιμές και διαγράμματα αντίστοιχα). Οι 2 αυτές συναρτήσεις καλούνται από το updateUiThread κάθε 5 δευτερόλεπτα (Εικόνα 8-15).

```

class updateUiThread extends Thread {

    @Override
    public void run() {

        while (true) {
            try {
                Thread.sleep(5000);
            } catch (InterruptedException e) {
                e.printStackTrace();
            }

            access() → {
                mainScreen.refresh();
                mainScreen.refreshCharts();
            };

        }
    }
}

```

Εικόνα 8-15 updateUiThread

Η εντολή access() δίνει την δυνατότητα στο Thread να μεταβάλει τα στοιχεία της διεπαφής χρήστη.

Στην κλάση MainScreen για τον σχηματισμό της οθόνης της διεπαφής χρησιμοποιήθηκαν τα εξής στοιχεία που παρέχει το vaadin framework:



1. **Labels:** αποτελούν μη τροποποιήσιμο κείμενο και χρησιμοποιήθηκαν για την παρουσίαση των τρεχουσών τιμών των μετρήσεων. Η δημιουργία ενός label γίνεται με τον παρακάτω κώδικα. Το κείμενο που εμφανίζεται μπορεί να αλλάξει μέσω του κώδικα με την συνάρτηση setValue που χρησιμοποιούμε για την ανανέωση της διεπαφής.

```
public Label leftTitle = new Label("Τρέχουσες τιμές",  
    ContentMode.TEXT);
```

2. **Panels:** αποτελούν πάνελ που μπορούν να περιέχουν ένα ή περισσότερα άλλα στοιχεία διεπαφής. Χρησιμοποιήθηκαν για να εμπεριέχουν τις μετρήσεις κάθε συσκευής ξεχωριστά. Η δημιουργία ενός τέτοιου στοιχείου γίνεται με την εξής γραμμή κώδικα:

```
newPanel = new Panel("End Device 1-Εσωτερικός χώρος");
```

3. **Text field και Button:** ένα στοιχείο TextField χρησιμοποιήθηκε για την εισαγωγή από τον χρήστη της επιθυμητής τιμής θερμοκρασίας και ένα στοιχείο button για την εισαγωγή της τιμής στην βάση. (Εικόνα 8-16) Η διαδικασία αυτή επιτεύχθηκε με την χρήση ενός ClickListener που ελέγχει την εισαγόμενη τιμή και αν είναι αποδεκτή την εισάγει στην βάση ως αντικείμενο setTemp εμφανίζοντας και τα κατάλληλα μηνύματα (Εικόνα 8-17).

```
public final TextField tf = new TextField();  
public Button button = new Button("Set Temp");
```

Εικόνα 8-16 Δημιουργία πεδίου κειμένου και button

```
button.setOnClickListener((event) -> {  
    if ((tf.getValue().length()) != 0) {  
        int setValue = Integer.parseInt(tf.getValue());  
        if ((setValue >= 10) & (setValue <= 30)) {  
            Notification.show("Θέσεις την εσωτερική θερμοκρασία στους " + tf.getValue() + "°C");  
            SetTemp st = new SetTemp();  
            st.setTemp(Integer.parseInt(tf.getValue()));  
            final Collection<Object> itemIds = temps.getItemIds();  
            int id = (int) getLastElement(itemIds);  
            st.setId(++id);  
            temps.addEntity(st);  
            temps.commit();  
        } else Notification.show("Μπορείτε να θέσετε την εσωτερική θερμοκρασία απο 10 έως 30°C");  
    } else Notification.show("Βάλτε μια τιμή");  
});
```

Εικόνα 8-17 ClickListener

4. **Charts και DataSeries** : Για τα διαγράμματα χρησιμοποιήθηκε η βιβλιοθήκη charts του vaadin. Αρχικά δημιουργήσαμε τα 4 διαγράμματα με εντολές σαν την παρακάτω:

```
Chart chart = new Chart();
```

Στην συνέχεια συσχετίσαμε το κάθε chart με μια ή περισσότερες dataSeries στις οποίες κάθε φορά προστίθεται η καινούργια μέτρηση.

```
DataSeries dataSeries = new DataSeries("Εξωτερική  
Θερμοκρασία");  
Configuration configuration = chart.getConfiguration();  
configuration.addSeries(dataSeries);
```

Τέλος για την επικοινωνία με την βάση δεδομένων και το διάβασμα και την εγγραφή τιμών σε αυτή χρησιμοποιήθηκε το JPAContainer του vaadin που επιστρέφει σε μορφή λίστας τα στοιχεία της βάσης. Με τις παρακάτω εντολές

```
JPAContainer<Metrisi> metriseis;  
JPAContainer<SetTemp> temps;  
metriseis = JPAContainerFactory.make(Metrisi.class, "metriseis");  
temps = JPAContainerFactory.make(SetTemp.class, "metriseis");
```

δημιουργούμε 2 τέτοια containers, ένα με τις μετρήσεις από τον πίνακα metriseis της βάσης και ένα με τις θερμοκρασίες που ορίζει ο χρήστης από τον πίνακα setTemp της βάσης (temps).

Οι πλήρεις κώδικες του project Diplomatiki είναι διαθέσιμοι στο συνοδευτικό υλικό.

## 8.3 Διαδικασία σύνδεσης κόμβων και λειτουργία δικτύου

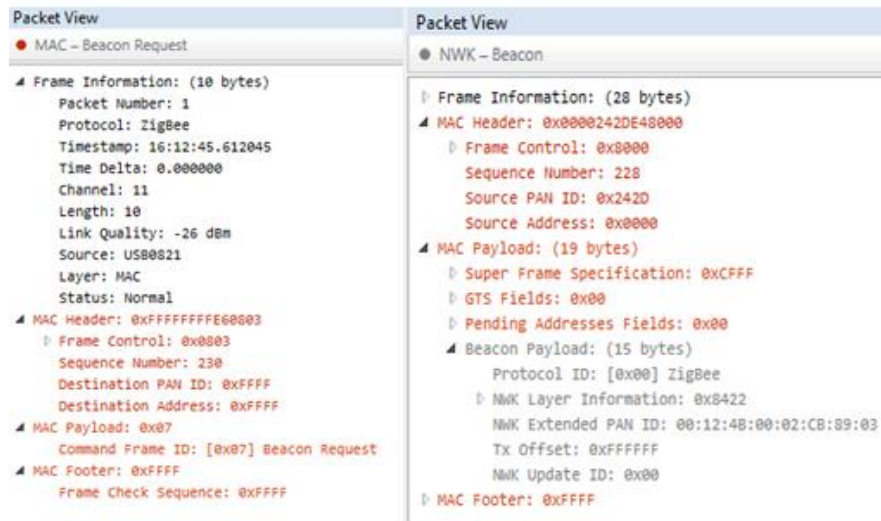
### 8.3.1 Σχηματισμός δικτύου

Κατά την πρώτη εκκίνηση των συσκευών ο Coordinator αναλαμβάνει το έργο να σχηματίσει το δίκτυο. Η διαδικασία αυτή φαίνεται συνοπτικά στην παρακάτω λίστα πακέτων.

	Ch.	Stack	Layer	Packet Information	MAC Src.	MAC Dst.	MA...
1	11	ZigBee	MAC	Beacon Request		0xFFFF	185
2	11	ZigBee	MAC	Beacon Request		0xFFFF	142
3	11	ZigBee	MAC	Beacon Request		0xFFFF	186
4	11	ZigBee	MAC	Beacon Request		0xFFFF	187
5	11	ZigBee	NWK	Beacon	0x0000		228
6	11	ZigBee	MAC	Association Request	00:12...	0x0000	188
7	11	ZigBee	MAC	Acknowledgement			188
8	11	ZigBee	MAC	Data Request	00:12...	0x0000	189
9	11	ZigBee	MAC	Acknowledgement			189
10	11	ZigBee	MAC	Association Response	00:12...	00:12:4...	143
11	11	ZigBee	MAC	Acknowledgement			143
12	11	ZigBee	MAC	Data Request	0x2EAB	0x0000	190
13	11	ZigBee	MAC	Acknowledgement			190
14	11	ZigBee	APS	Transport Key	0x0000	0x2EAB	144
15	11	ZigBee	MAC	Acknowledgement			144
16	11	ZigBee	MAC	Data Request	0x2EAB	0x0000	191
17	11	ZigBee	MAC	Acknowledgement			191
18	11	ZigBee	ZDP	Device Announce	0x2EAB	0x0000	192
19	11	ZigBee	MAC	Acknowledgement			192
20	11	ZigBee	ZDP	Device Announce	0x0000	0xFFFF	145

Εικόνα 8-18 Αλληλουχία πακέτων σχηματισμού δικτύου

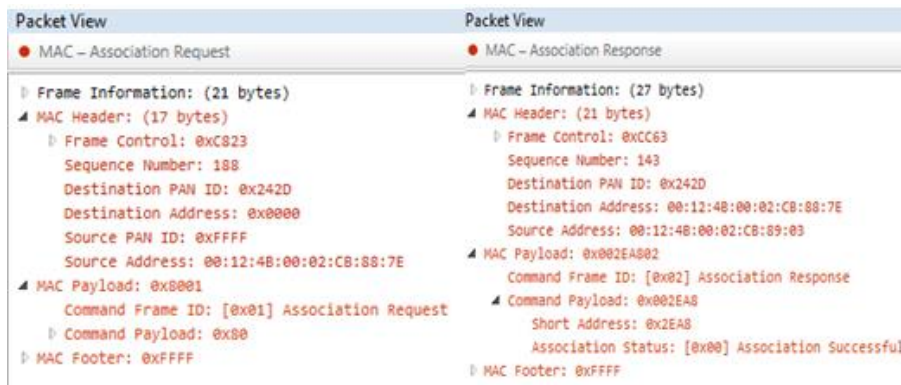
1. Οι συσκευές Router και End Device ανιχνεύουν τον περιβάλλοντα χώρο τους στέλνοντας μηνύματα Beacon Request (πακέτα 1-4) αναζητώντας εάν υποψήφιο δίκτυο ή αλλιώς μία συσκευή Coordinator. Αν δεν υπάρχει ενεργοποιημένος κόμβος Coordinator στέλνονται Beacon Request μέχρι να ενεργοποιηθεί. Όταν μπει σε λειτουργία ο Coordinator στέλνει μήνυμα Beacon (πακέτο 5) με την χρήση Broadcast σε όλες τις περιβάλλουσες συσκευές.



Εικόνα 8-19 Beacon και Beacon Request

Η επιλογή του PAN ID του δικτύου δεν έχει καθοριστεί ακόμα και για αυτό το Beacon έχει ως PAN ID την 64-bit MAC διεύθυνση του η οποία είναι μοναδική για κάθε κόμβο και καθορίζεται από την κατασκευή του.

2. Ο Coordinator έχει εκκινήσει το δίκτυο και περιμένει να δεχτεί αιτήματα σύνδεσης στο επίπεδο MAC. Η συσκευή End Device στέλνει Association Request στον Coordinator για να συνδεθεί στο δίκτυο.

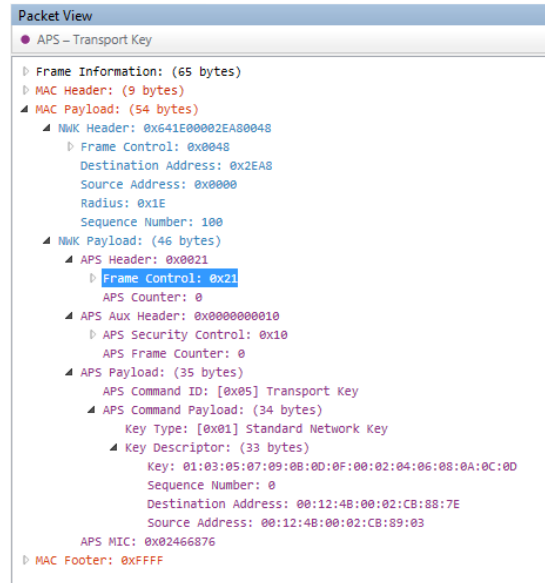


Εικόνα 8-20 Association Request και Response

Στο Association Request (πακέτο 6) φαίνεται ότι το μόνο αναγνωριστικό του End Device είναι η μοναδική 64-bit διεύθυνση του. Ο Coordinator στέλνοντας

Association Response (πακέτο 10) αναθέτει στο End Device 16-bit διεύθυνση η οποία είναι το αναγνωριστικό της πια μες στο δίκτυο.

3. Σε αυτό το βήμα γίνεται η αποστολή του κλειδιού του δικτύου προς το End Device. Αξίζει να αναφερθεί ότι αυτό είναι το μόνο τρωτό σημείο της ασφάλειας όταν εκτελείται με αυτόν τον τρόπο καθώς με ένα πρόγραμμα Sniffer μπορεί να αποσπαστεί το κλειδί του δικτύου. (πακέτο 14)



Εικόνα 8-21 Transport Key

4. Τέλος, το End Device έχει ολοκληρώσει την διαδικασία σύνδεσης στο επίπεδο MAC και έχει λάβει το κλειδί του δικτύου, στέλνει Broadcast μήνυμα μέσω του Coordinator ανακοινώνοντας τα στοιχεία του, στο επίπεδο της εφαρμογής και πιο συγκεκριμένα στο ZDP (Zigbee Device Profile).

```

Packet View
ZDP - Device Announce

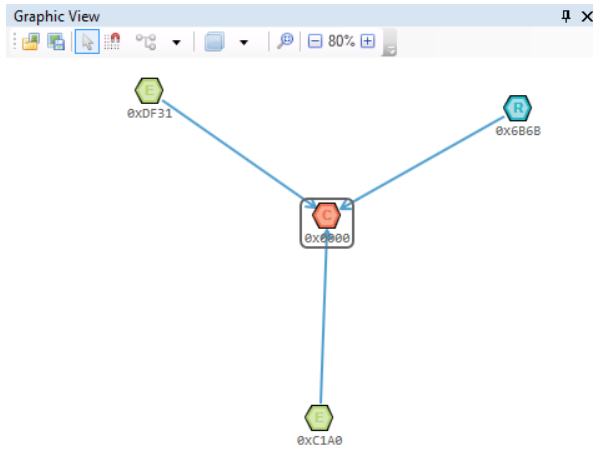
▷ Frame Information: (57 bytes)
▷ MAC Header: (9 bytes)
▲ MAC Payload: (46 bytes)
  ▷ Nwk Header: 0x9C1D2E88FFFD0208
  ▷ Nwk Aux Header: (14 bytes)
  ▲ Nwk Payload: (20 bytes)
    ▲ APS Header: 0x00000000130008
      ▷ Frame Control: 0x08
      Destination Endpoint: 0x00
      Cluster ID: [0x0013] Device Announce
      Profile ID: [0x0000] ZigBee Device Profile
      Source Endpoint: 0x00
      APS Counter: 0
    ▲ APS Payload: (12 bytes)
      ZDP Transaction Sequence Number: 0
      ▲ Device Announce: (11 bytes)
        Nwk Address of Local Device: 0x2EA8
        IEEE Address of Local Device: 00:12:4B:00:02:CB:88:7E
        ▲ Capability Information: 0x80
          .... 0 = Alternate PAN Coordinator Capability: 0x0
          .... 0 = Device Type: [0x0] End Device
          .... 0 = Power Source: [0x0] Other Power Source
          .... 0 = Receiver On When Idle: [0x0] No
          ..00 .... = Reserved: 0x0
          .0.. .... = Security Capability: [0x0] Standard Security Mode
          1... .... = Allocate Address: [0x1] Device Must be Issued a 16-bit Network
        Nwk NIC: 0x39706130
      ▷ MAC Footer: 0xFFFF
  
```

Εικόνα 8-22 Device announce

### 8.3.2 Τοπολογία δικτύου

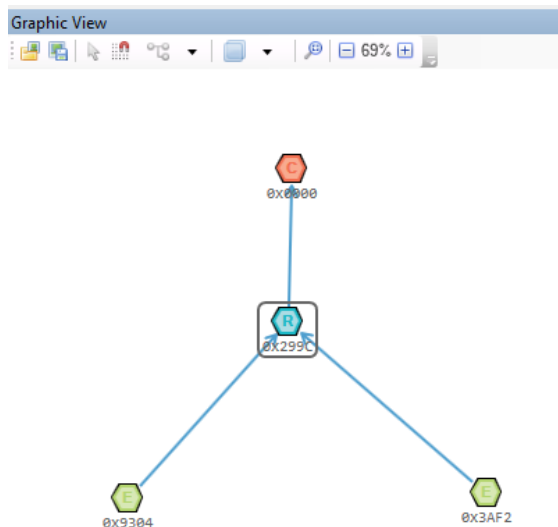
Τα δίκτυα Zigbee χαρακτηρίζονται από την δυνατότητα τους να συνδέονται σε mesh δίκτυο. Αυτό προϋποθέτει ότι στην εμβέλεια κάθε End Device υπάρχει ένας Router ή απευθείας ο Coordinator, και σε κάθε περίπτωση ότι υπάρχει μία διαδρομή που να συνδέεται με τον Coordinator. Το δίκτυο που στηρίχτηκε η εφαρμογή μας αποτελείται από 4 κόμβους από τους οποίους οι δυο είναι End Devices, ένας Router και ένας Coordinator. Μέσω του Ubiquiti (packet sniffer) παρατηρήσαμε τις παρακάτω τοπολογίες ανάλογα με την τοποθέτηση που κάναμε στους κόμβους.

- Η πιο απλή τοπολογία είναι η σύνδεση όλων των κόμβων στο καθώς η εμβέλεια του καλύπτει όλες τις συσκευές.



Εικόνα 8-23 Σύνδεση όλων απευθείας στο Coordinator

- Η επόμενη περίπτωση είναι τα End Devices να είναι στην εμβέλεια μόνο του Router και αυτός με την σειρά του να συνδέεται με τον Coordinator.



Εικόνα 8-24 Σύνδεση μέσω Router (mesh)

- Στην γενική περίπτωση επειδή τα End Devices μπορεί να έχουν κινητικότητα μες στο δίκτυο, αφού συνήθως έχουν ανεξάρτητη πηγή ενέργειας (πχ μπαταρία, μικρό φωτοβολταϊκό) η τοπολογία του δικτύου προσαρμόζεται εξασφαλίζοντας στα πακέτα την συντομότερη διαδρομή. Συνεπώς τα End

Devices μπορούν να κινούνται ελεύθερα στην ένωση των ακτινών εμβέλειας που καθορίζει ο Router και ο Coordinator.

### 8.3.3 Διαδικασία Binding

Το δίκτυο Zigbee για να διαμορφωθεί χρησιμοποιείται μια διαδικασία σύνδεσης (Binding) των συσκευών. Όπως έχει περιγραφεί και στα πρώτα κεφάλαια για το στήσιμο του δικτύου είναι απαραίτητη η ύπαρξη μίας συσκευής Coordinator και βέβαια οποιονδήποτε συνδυασμό συσκευών Router και End Device. Σε αυτό το σημείο θα περιγραφούν τα μηνύματα που ανταλλάσσονται μεταξύ του Coordinator και ενός End Device για την σύνδεση τους. Η ίδια αλληλουχία έχει ισχύ σε κάθε σύνδεση μεταξύ δύο συσκευών. Μια συσκευή μπορεί να συνδεθεί και με παραπάνω από μία συσκευές. Με κάθε σύνδεση μεταξύ δύο ενημερώνεται το Binding Table της κάθε μίας. Ωστόσο με τον τρόπο που διαχειριζόμαστε το δίκτυο η διαδικασία Binding γίνεται ανά δύο συσκευές. Η λίστα του συνόλου των μηνυμάτων φαίνεται στην παρακάτω εικόνα.

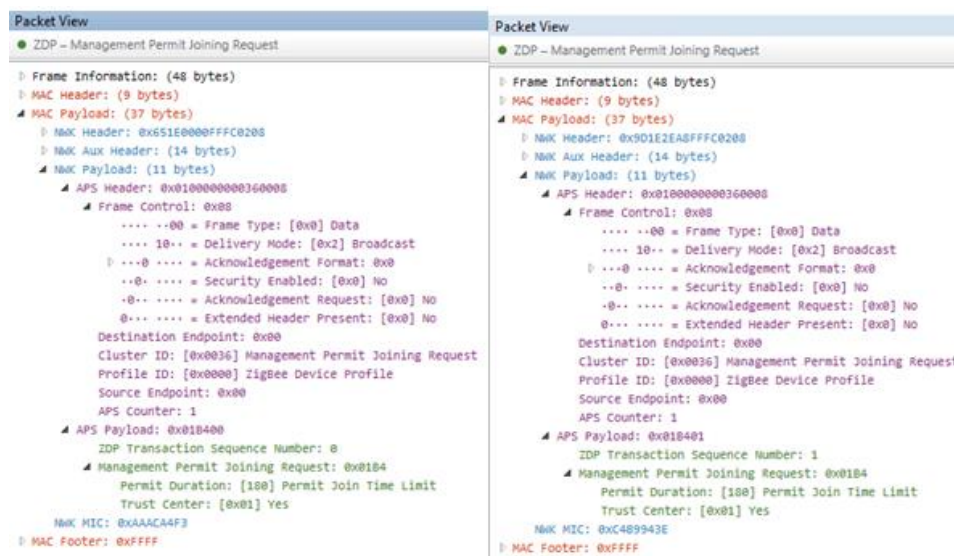
	Ch.	Stack	Layer	Packet Information	MAC Src.	MAC Dst.	MA...
23	11	ZigBee	ZDP	Management Permit Joining Request	0x0000	0xFFFF	146
24	11	ZigBee	ZDP	Management Permit Joining Request	0x2EAB	0x0000	194
25	11	ZigBee	MAC	Acknowledgement			194
26	11	ZigBee	ZDP	Management Permit Joining Request	0x0000	0xFFFF	147
27	11	ZigBee	ZCL	Identify: Identify Query	0x2EAB	0x0000	195
28	11	ZigBee	MAC	Acknowledgement			195
29	11	ZigBee	ZCL	Identify: Identify Query	0x0000	0xFFFF	148
30	11	ZigBee	MAC	Data Request	0x2EAB	0x0000	196
31	11	ZigBee	MAC	Acknowledgement			196
32	11	ZigBee	ZCL	Identify: Identify Query Response	0x0000	0x2EAB	149
33	11	ZigBee	MAC	Acknowledgement			149
34	11	ZigBee	ZDP	Match Descriptor Request	0x2EAB	0x0000	197
35	11	ZigBee	MAC	Acknowledgement			197
36	11	ZigBee	MAC	Data Request	0x2EAB	0x0000	198
37	11	ZigBee	MAC	Acknowledgement			198
38	11	ZigBee	ZDP	Match Descriptor Response	0x0000	0x2EAB	150
39	11	ZigBee	MAC	Acknowledgement			150
40	11	ZigBee	APS	Acknowledgement	0x2EAB	0x0000	199
41	11	ZigBee	MAC	Acknowledgement			199
42	11	ZigBee	MAC	Data Request	0x2EAB	0x0000	200
43	11	ZigBee	MAC	Acknowledgement			200
44	11	ZigBee	MAC	Data Request	0x2EAB	0x0000	201
45	11	ZigBee	MAC	Acknowledgement			201
46	11	ZigBee	MAC	Data Request	0x2EAB	0x0000	202
47	11	ZigBee	MAC	Acknowledgement			202
48	11	ZigBee	MAC	Data Request	0x2EAB	0x0000	203
49	11	ZigBee	MAC	Acknowledgement			203
50	11	ZigBee	ZDP	Management Permit Joining Request	0x0000	0xFFFF	151
51	11	ZigBee	ZDP	Management Permit Joining Request	0x2EAB	0x0000	204
52	11	ZigBee	MAC	Acknowledgement			204
53	11	ZigBee	ZDP	Management Permit Joining Request	0x0000	0xFFFF	152

Εικόνα 8-25 Αλληλουχία μηνυμάτων Binding



Το πρώτο βήμα από την μεριά του κόμβου είναι να εκκινήσει την διαδικασία του Binding. Σε κάθε πλακέτα αυτό έχει ανατεθεί σε ένα κουμπί το οποία εκτελεί μία σειρά ενεργειών που θα αναλυθούν παρακάτω.

1. Η πρώτη ενέργεια είναι να στείλει η συσκευή ένα πακέτο προς όλο το δίκτυο (broadcast) για να ανακοινώσει ότι είναι ανοικτή στο να δεχτεί αιτήματα για σύνδεση. Τα πακέτα αυτά είναι τα 23,24 και 25. Το 23 το εκπέμπει ο Coordinator και τα 24,25 τα εκπέμπει το End Device μέσω του Coordinator.



Εικόνα 8-26 Permit Join Request στο επίπεδο ZDP της εφαρμογής, χρόνος λήξης 180sec

Όπως φαίνεται και στις εικόνες κάθε μήνυμα περιέχει και τον χρόνο λήξης της περιόδου αποδοχής που στην περίπτωση μας έχει ρυθμιστεί στα 180 sec.

2. Οι συσκευές που παίρνουν μέρος στην διαδικασία του Binding μπορούν να είναι ρυθμισμένες ως Initiator. Αυτό σημαίνει εκτός από το να αποδέχονται αιτήματα, στέλνουν αιτήματα στις άλλες συσκευές για να γίνει το «ζευγάρι» με μία άλλη συσκευή που έχει δηλώσει ότι επιτρέπει αιτήματα σύνδεσης. Το πακέτο αυτό γίνεται broadcast σε όλο το δίκτυο και φαίνεται στα πακέτα 27 και 29.

```

Packet View
● ZCL – Identify: Identify Query
└─ Frame Information: (48 bytes)
  └─ MAC Header: (9 bytes)
    └─ MAC Payload: (37 bytes)
      └─ NWK Header: 0x9E1E2EA8FFFF0208
        └─ NWK Aux Header: (14 bytes)
          └─ NWK Payload: (11 bytes)
            └─ APS Header: 0x020801040003FF08
              └─ Frame Control: 0x08
                └─ Destination Endpoint: 0xFF
                  └─ Cluster ID: [0x0003] General: Identify
                    └─ Profile ID: [0x0104] ZigBee Home Automation
                      └─ Source Endpoint: 0x08
                        └─ APS Counter: 2
                          └─ APS Payload: 0x010011
                            └─ ZCL Header: 0x010011
                              └─ Frame Control: 0x11
                                └─ Transaction Sequence Number: 0
                                  └─ Command ID: [0x01] Identify Query
                                    └─ NWK MIC: 0x633F1F32
                                      └─ MAC Footer: 0xFFFF

```

Εικόνα 8-27 Μήνυμα Initiator για εκκίνηση Binding

Έπειτα η συσκευή που είχε δηλώσει ότι επιτρέπει σύνδεση απαντά στον κόμβο που έστειλε το αίτημα (πακέτο 32).

```

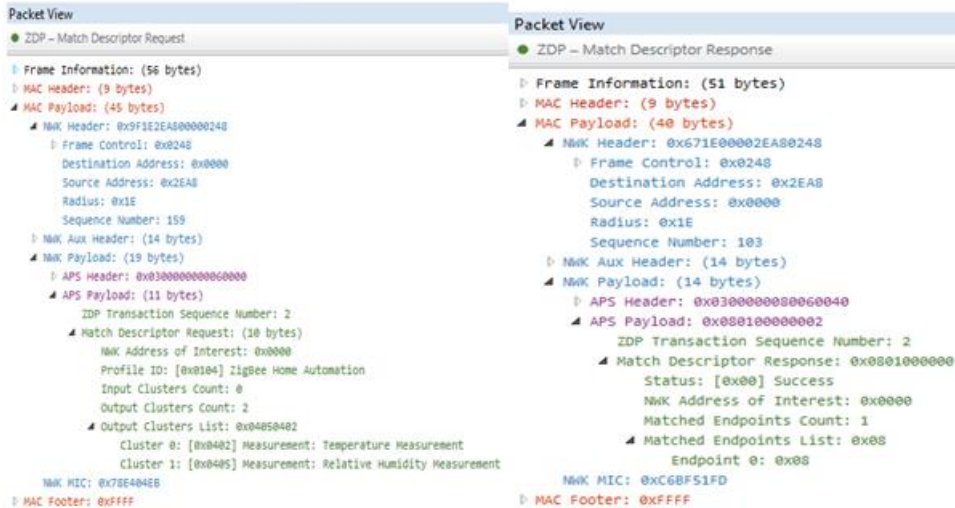
Packet View
● ZCL – Identify: Identify Query Response
└─ Frame Information: (50 bytes)
  └─ MAC Header: (9 bytes)
    └─ MAC Payload: (39 bytes)
      └─ NWK Header: 0x661E0002EA80248
        └─ NWK Aux Header: (14 bytes)
          └─ NWK Payload: (13 bytes)
            └─ APS Header: 0x0208010400030B00
              └─ Frame Control: 0x08
                └─ Destination Endpoint: 0x08
                  └─ Cluster ID: [0x0003] General: Identify
                    └─ Profile ID: [0x0104] ZigBee Home Automation
                      └─ Source Endpoint: 0x08
                        └─ APS Counter: 2
                          └─ APS Payload: 0x0084000019
                            └─ ZCL Header: 0x000019
                              └─ Frame Control: 0x19
                                └─ Transaction Sequence Number: 0
                                  └─ Command ID: [0x00] Identify Query Response
                                    └─ ZCL Payload: 0x00B4
                                      └─ Timeout: 180
                                        └─ NWK MIC: 0xDB3121FA
                                          └─ MAC Footer: 0xFFFF

```

Εικόνα 8-28 Απάντηση στο αίτημα του Initiator

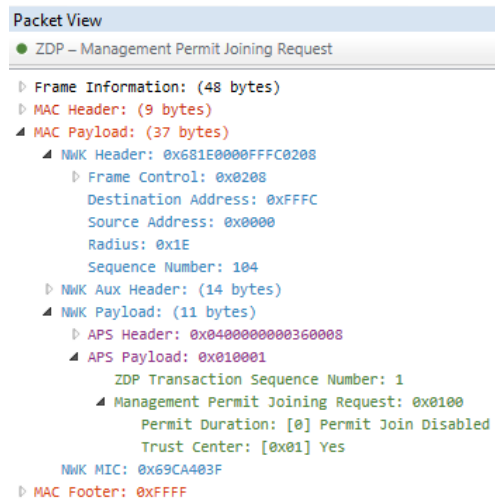
3. Το πιο σημαντικό βήμα στην διαδικασία, αφού έχουν γίνει όλες οι ενέργειες ώστε να καθοριστούν οι διευθύνσεις των συσκευών που δήλωσαν ότι θέλουν να συνδεθούν είναι το Match Description (ταυτοποίηση των περιγραφών). Σε αυτό το βήμα ο Initiator, το End Device στην περίπτωση μας, στέλνει στο Coordinator τα Clusters που δραστηριοποιείται (Temperature και Humidity) και αν ταυτίζονται με τα Clusters που έχει ο Coordinator δηλωμένα στέλνει πίσω

μήνυμα για την επιτυχία της ταυτοποίησης. Τα μηνύματα αυτά είναι τα 34 και 38.



Εικόνα 8-29 Μηνύματα ταυτοποίησης Clusters μεταξύ δύο συσκευών

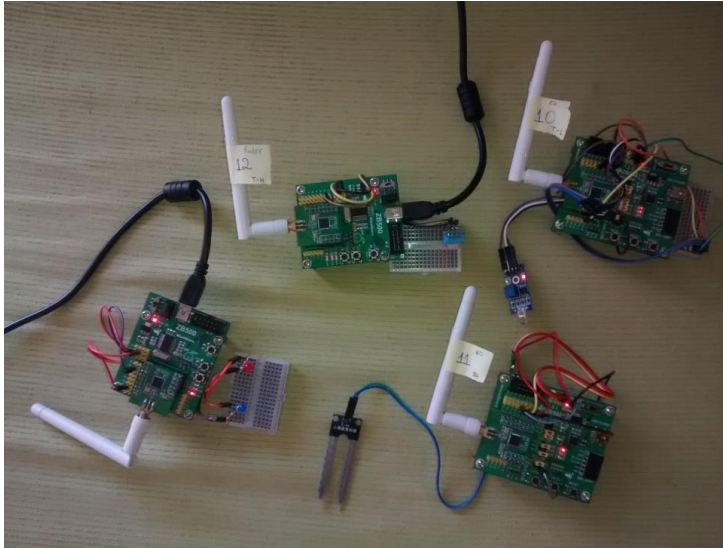
- Τέλος, καθώς οι δύο συσκευές έχουν ταυτίσει τα Clusters και συνεπώς έχει γίνει η εγγραφή στα Binding Tables τους, στέλνουν και οι δύο Broadcast μήνυμα σε όλο το δίκτυο ότι διακόπτον να επιτρέπουν αιτήματα σύνδεσης. Αυτό θα μπορούσε να συμβεί αν έληγε ο χρόνος των 180 sec που έχει τεθεί ως χρονικό όριο. (Πακέτα 50,51,53)



Εικόνα 8-30 Μήνυμα παύσης αποδοχής αιτημάτων Binding

## 8.4 Λειτουργία κόμβων

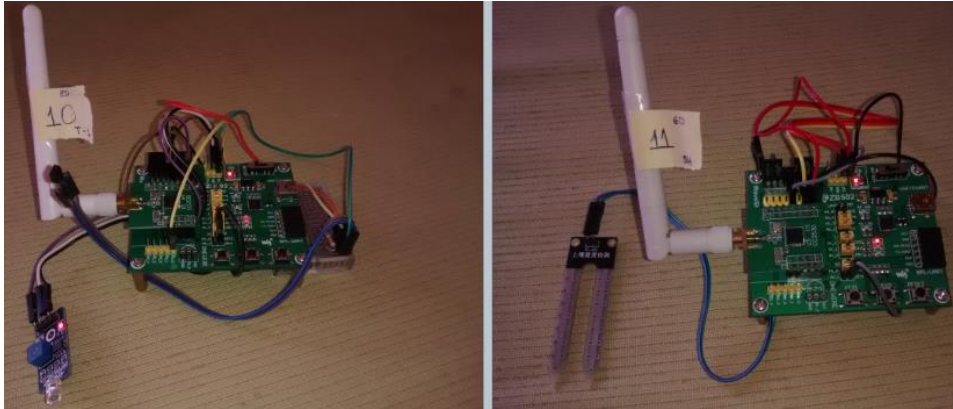
Σε αυτή την ενότητα ασχολούμαστε πιο εξειδικευμένα με την λειτουργία της κάθε κατηγορίας συσκευών που υπάρχουν στο δίκτυο. Οι τέσσερις συσκευές του δικτύου χωρίζονται σε 2 End Devices, 1 Router και 1 Coordinator και φαίνονται στην Εικόνα 8-31 Κόμβοι δικτύου



Εικόνα 8-31 Κόμβοι δικτύου

### 8.4.1 Λειτουργία End Devices

Στο δίκτυο που δημιουργήσαμε υπάρχουν δύο End Devices τα οποία είναι υπεύθυνα για την καταγραφή κάποιων μετρήσεων. Το πρώτο End Device βρίσκεται στο εξωτερικό του θερμοκηπίου και είναι υπεύθυνο για την καταγραφή της εξωτερικής θερμοκρασίας και του επίπεδου φωτισμού. Το δεύτερο End Device, που βρίσκεται στο εσωτερικό καταγράφει την υγρασία χώματος. Και τα δύο End Devices λειτουργούν σε Sleep Mode, δηλαδή την ώρα που δεν έχουν κάποια εργασία να εκτελέσουν περνάνε σε Sleep το οποίο αυξάνει την διάρκεια ζωής της μπαταρίας που έχουν ως πηγή ενέργειας.



Εικόνα 8-32 End Devices

Το ED (EP 11) που βρίσκεται στο εσωτερικό χρησιμοποιεί τον αισθητήρα υγρασίας χρώματος LM393 και καταγράφει την υγρασία με την μέθοδο ADC.

```
static void zclSampleHumiditySensor_SendHum( void )
{
#ifdef ZCL_REPORT
    zclReportCmd_t *pReportCmd;
    zclSampleHumiditySensor_MeasuredValue= HalAdcRead
(HAL_ADC_CHANNEL_6, HAL_ADC_RESOLUTION_12);
    pReportCmd = osal_mem_alloc( sizeof(zclReportCmd_t) + sizeof(zclReport_t) );
    if ( pReportCmd != NULL )
    {
        pReportCmd->numAttr = 1;
        pReportCmd->attrList[0].attrID = ATTRID_MS_RELATIVE_HUMIDITY_MEASURED_VALUE;
        pReportCmd->attrList[0].dataType = ZCL_DATATYPE_INT16;
        pReportCmd->attrList[0].attrData = (void
*)(&zclSampleHumiditySensor_MeasuredValue);
        zcl_SendReportCmd( SAMPLETEMPERATURESENSOR_ENDPOINT,
&zclSampleTemperatureSensor_DstAddr,
                        ZCL_CLUSTER_ID_MS_RELATIVE_HUMIDITY,
                        pReportCmd, ZCL_FRAME_SERVER_CLIENT_DIR, TRUE,
zclSampleTemperatureSensorSeqNum++ );
    }
    osal_mem_free( pReportCmd );
#endif // ZCL_REPORT
}

```

Το μήνυμα που στέλνει στον Coordinator στέλνεται μέσω της συνάρτησης `zcl_SendReportCmd` και έχει την εξής μορφή όπως μπορούμε να δούμε στο πρόγραμμα Sniffer:

```

● ZCL – Relative Humidity Measurement: Report Attributes
┆ Frame Information: (53 bytes)
┆ MAC Header: (9 bytes)
▲ MAC Payload: (42 bytes)
┆ NWK Header: 0xB81EEAF100000248
┆ NWK Aux Header: (14 bytes)
▲ NWK Payload: (16 bytes)
  ▲ APS Header: 0x600B010404050800
    ┆ Frame Control: 0x00
    Destination Endpoint: 0x88
    Cluster ID: [0x0405] Measurement: Relative Humidity Measurement
    Profile ID: [0x0104] ZigBee Home Automation
    Source Endpoint: 0x8B
    APS Counter: 96
  ▲ APS Payload: 0x07FF290000A2E18
    ┆ ZCL Header: 0x0A2E18
    ▲ ZCL Payload: 0x07FF290000
      ▲ Attributes 0: 0x07FF290000
        Attribute ID: [0x0000] Reserved
        Attribute Data Type: [0x29] Signed 16-bit Integer
        Unknown Attribute: 0x07FF
      NWK MIC: 0xD6CC9816
    ┆ MAC Footer: 0xFFFF

```

Εικόνα 8-33 Αναφορά υγρασίας χρώματος από EndPoint 11

Το δεύτερο End Device (EP 10) στέλνει δύο μετρήσεις από το εξωτερικό του θερμοκηπίου. Η θερμοκρασία αποσπάται μέσω του ψηφιακού θερμόμετρου DS18B20 και η τιμή της φωτεινότητας μέσω του ADC αισθητήρα φωτισμού LM393. Με τον ίδιο τρόπο στέλνονται οι μετρήσεις που έχουν την εξής μορφή.

<pre> ● ZCL – Temperature Measurement: Report Attributes ┆ Frame Information: (53 bytes) ┆ MAC Header: (9 bytes) ▲ MAC Payload: (42 bytes) ┆ NWK Header: 0x561E0F0400000248 ┆ NWK Aux Header: (14 bytes) ▲ NWK Payload: (16 bytes)   ▲ APS Header: 0xAE0A010404020800     ┆ Frame Control: 0x00     Destination Endpoint: 0x88     Cluster ID: [0x0402] Measurement: Temperature Measurement     Profile ID: [0x0104] ZigBee Home Automation     Source Endpoint: 0x8A     APS Counter: 174   ▲ APS Payload: 0x0012290000A5518     ┆ ZCL Header: 0x0A5518     ▲ ZCL Payload: 0x0012290000       ▲ Attributes 0: 0x0012290000         Attribute ID: [0x0000] Measured Value         Attribute Data Type: [0x29] Signed 16-bit Integer         Value: [18] °C       NWK MIC: 0xE135719C     ┆ MAC Footer: 0xFFFF </pre>	<pre> ● ZCL – Illuminance Measurement: Report Attributes ┆ Frame Information: (53 bytes) ┆ MAC Header: (9 bytes) ▲ MAC Payload: (42 bytes) ┆ NWK Header: 0x511E0F0400000248 ┆ NWK Aux Header: (14 bytes) ▲ NWK Payload: (16 bytes)   ▲ APS Header: 0xA40A010404000800     ┆ Frame Control: 0x00     Destination Endpoint: 0x88     Cluster ID: [0x0400] Measurement: Illuminance Measurement     Profile ID: [0x0104] ZigBee Home Automation     Source Endpoint: 0x8A     APS Counter: 164   ▲ APS Payload: 0x0526290000A5018     ┆ ZCL Header: 0x0A5018     ▲ ZCL Payload: 0x0526290000       ▲ Attributes 0: 0x0526290000         Attribute ID: [0x0000] Measured Value         Attribute Data Type: [0x29] Signed 16-bit Integer         Value: [1318] Lux       NWK MIC: 0x19EEE588     ┆ MAC Footer: 0xFFFF </pre>
---	--

Εικόνα 8-34 Αναφορές Θερμοκρασίας και Φωτισμού εξωτερικού χώρου από EndPoint 10

### 8.4.2 Λειτουργία Router

Ο Router βρίσκεται στο κεντρικά μέσα στο θερμοκήπιο και αναλαμβάνει μία σειρά λειτουργιών. Μετά τον Coordinator είναι υπεύθυνος για την συνοχή του δικτύου. Αυτό σημαίνει ότι αν έχει στην εμβέλεια του κάποιο End Device που δεν

επικοινωνεί με το Coordinator, αναμεταδίδει τα μηνύματα που προορίζονται προς αυτόν. Έπειτα σε περίπτωση που ο Coordinator βρεθεί εκτός λειτουργίας, συντηρεί το δίκτυο καθώς γίνεται ανάδοχος του Coordinator, δηλαδή λαμβάνει όλα τα μηνύματα προς τον Coordinator, τα αποθηκεύει και όταν επανέλθει σε λειτουργία ο Coordinator του τα προωθεί.



Εικόνα 8-35 Router

Στην εφαρμογή μας εκτός από τις δικτυακές λειτουργίες του Router, λόγω της θέσης του μέσα στο θερμοκήπιο καταγράφει την θερμοκρασία και την υγρασία αέρα στο εσωτερικό του θερμοκηπίου. Με αντίστοιχο τρόπο με τα End Devices προωθεί αυτές τις μετρήσεις στον Coordinator. Ο αισθητήρας που χρησιμοποιεί είναι ο DHT11. Το EP του Router είναι το 12 και τα μηνύματα που στέλνει στον Coordinator έχουν την παρακάτω μορφή.

ZCL - Relative Humidity Measurement: Report Attributes	ZCL - Temperature Measurement: Report Attributes
<pre> Frame Information: (53 bytes) MAC Header: (9 bytes) MAC Payload: (42 bytes)   NWK Header: 0x51E198E0000248   NWK Aux Header: (14 bytes)   MAC Payload: (16 bytes)     APS Header: 0xB80C010404020800       Frame Control: 0x00       Destination Endpoint: 0x08       Cluster ID: [0x0405] Measurement: Relative Humidity Measurement       Profile ID: [0x0104] ZigBee Home Automation       Source Endpoint: 0x0C       APS Counter: 184     APS Payload: 0x0057290000A5A1B       ZCL Header: 0xB8A5A1B       ZCL Payload: 0x0057290000         Attributes #: 0x0057290000           Attribute ID: [0x0000] Reserved           Attribute Data Type: [0x29] Signed 16-bit Integer           Unknown Attribute: 0x0057         NWK MIC: 0xB80C2EF       MAC Footer: 0xFFFF           </pre>	<pre> Frame Information: (53 bytes) MAC Header: (9 bytes) MAC Payload: (42 bytes)   NWK Header: 0x5E1E198E0000248   NWK Aux Header: (14 bytes)   MAC Payload: (16 bytes)     APS Header: 0x5E0C010404020800       Frame Control: 0x00       Destination Endpoint: 0x08       Cluster ID: [0x0402] Measurement: Temperature Measurement       Profile ID: [0x0104] ZigBee Home Automation       Source Endpoint: 0x0C       APS Counter: 94     APS Payload: 0x0014290000A2D1B       ZCL Header: 0xB8A2D1B       ZCL Payload: 0x0014290000         Attributes #: 0x0014290000           Attribute ID: [0x0000] Measured value           Attribute Data Type: [0x29] Signed 16-bit Integer           Value: [20] °C         NWK MIC: 0xB80F765D       MAC Footer: 0xFFFF           </pre>

Εικόνα 8-36 Αναφορές Θερμοκρασίας και Υγρασίας εσωτερικού χώρου από EndPoint 12

### 8.4.3 Λειτουργία Coordinator

Ο Coordinator έχει ως αρχικό του σκοπό την δημιουργία του δικτύου. Λόγω αυτής του της ιδιότητας, έχει επιλεχθεί στην εφαρμογή μας ως ο κόμβος που επικοινωνεί με τον υπολογιστή, του κοινοποιεί τις τιμές των μετρήσεων μέσα από το δίκτυο και δέχεται εντολές. Η λειτουργία στο μέρος του υπολογιστή θα αναλυθεί στην επόμενη ενότητα.

Τα μηνύματα- αναφορές που δέχεται ο Coordinator από τους υπόλοιπους κόμβους τα επεξεργάζεται ώστε να αποσπάσει τις τιμές των μετρήσεων και να τις ταυτίσει με την πηγή τους και την ιδιότητα τους.

```
static void zclSampleThermostat_ProcessInReportCmd( zclIncomingMsg_t *pInMsg )
{
    zclReportCmd_t *pInTempSensorReport;
    pInTempSensorReport = (zclReportCmd_t *)pInMsg->attrCmd;
    uint16 cluster= pInMsg->clusterId;
    afAddrType_t address=pInMsg->srcAddr;
    uint8 endpoint= address.endPoint;
    if (endpoint==0x0A) {
        if ( cluster == ZCL_CLUSTER_ID_MS_TEMPERATURE_MEASUREMENT)
        {
            zclSampleThermostat_LocalTemperature = BUILD_UINT16(pInTempSensorReport-
>attrList[0].attrData[0], pInTempSensorReport->attrList[0].attrData[1]);

            return;
        }
        if (cluster == ZCL_CLUSTER_ID_MS_ILLUMINANCE_MEASUREMENT )
        {
            zclSampleThermostat_LocalLight = BUILD_UINT16(pInTempSensorReport-
>attrList[0].attrData[0], pInTempSensorReport->attrList[0].attrData[1]);

            return;
        }
    }
    else if (endpoint==0x0B){
        /* if ( cluster == ZCL_CLUSTER_ID_MS_TEMPERATURE_MEASUREMENT)
        {
            zclSampleThermostat_LocalTemperature1 = BUILD_UINT16(pInTempSensorReport-
>attrList[0].attrData[0], pInTempSensorReport->attrList[0].attrData[1]);
            return;
        }*/
        if (cluster == ZCL_CLUSTER_ID_MS_RELATIVE_HUMIDITY )
        {
            zclSampleThermostat_LocalHumidity = BUILD_UINT16(pInTempSensorReport-
>attrList[0].attrData[0], pInTempSensorReport->attrList[0].attrData[1]);
            osal_set_event (zclSampleThermostat_TaskID, SAMPLETHERMOSTAT_TEMP_SEND_UART);
            return;
        }
    }
    else if (endpoint==0x0C){
        if ( cluster == ZCL_CLUSTER_ID_MS_TEMPERATURE_MEASUREMENT)
        {
            zclSampleThermostat_LocalTemperature1 = BUILD_UINT16(pInTempSensorReport-
>attrList[0].attrData[0], pInTempSensorReport->attrList[0].attrData[1]);
            if (!flag){
                osal_set_event (zclSampleThermostat_TaskID, SAMPLETHERMOSTAT_TEMP_CHECK);
                flag=true;}
            return;
        }
        if (cluster == ZCL_CLUSTER_ID_MS_RELATIVE_HUMIDITY )
        {
            zclSampleThermostat_LocalHumidity1 = BUILD_UINT16(pInTempSensorReport-
>attrList[0].attrData[0], pInTempSensorReport->attrList[0].attrData[1]);
            return;
        }
    }
}
```



Μέσα από μία σειρά ελέγχων if γίνεται εκχώρηση των μετρήσεων στις κατάλληλες μεταβλητές. Έπειτα ο Coordinator συνθέτει ένα String με τις μετρήσεις το οποίο και στέλνει μέσω σειριακής στον υπολογιστή που με την σειρά του το επεξεργάζεται κατάλληλα. Το String έχει την μορφή αριθμών που χωρίζονται από παύλες.

```

if ( events & SAMPLETHERMOSTAT_TEMP_SEND_UART )
{
    unsigned char final[15];

    ////////////EP10- Temp & Light//////////

    _itoa(zclSampleThermostat_LocalTemperature, c, 10);
    if (osal_strlen((char*)c)==1){ osal_memcpy( final, "0", 1 ); osal_memcpy(
&final[1], c, 1 );}
    else osal_memcpy( final, c, 2 );
    osal_memcpy( &final[2], "-", 1 );

    int16 value = zclSampleThermostat_LocalLight;
    value=100-(value/21);
    _itoa(value, c, 10);
    if (osal_strlen((char*)c)==1) { osal_memcpy( &final[3], "0", 1 ); osal_memcpy(
&final[4], c, 1 );}
    else osal_memcpy( &final[3], c, 2 );
    osal_memcpy( &final[5], "-", 1 );

    ////////////EP11- Soil//////////

    value = zclSampleThermostat_LocalHumidity;
    value=100-(value/21);
    _itoa(value, c, 10);
    if (osal_strlen((char*)c)==1) { osal_memcpy( &final[6], "0", 1 ); osal_memcpy(
&final[7], c, 1 );}
    else osal_memcpy( &final[6], c, 2 );
    osal_memcpy( &final[8], "-", 1 );

    ////////////EP12- Temp & Humidity//////////

    _itoa(zclSampleThermostat_LocalTemperature1, c, 10);
    if (osal_strlen((char*)c)==1) { osal_memcpy( &final[9], "0", 1 ); osal_memcpy(
&final[10], c, 1 );}
    else osal_memcpy( &final[9], c, 2 );
    osal_memcpy( &final[11], "-", 1 );

    _itoa(zclSampleThermostat_LocalHumidity1, c, 10);
    if (osal_strlen((char*)c)==1) { osal_memcpy( &final[12], "0", 1 ); osal_memcpy(
&final[13], c, 1 );}
    else osal_memcpy( &final[12], c, 2 );
    osal_memcpy( &final[14], "-", 1 );

    if (final[13]>= 0x30 && final[13]<= 0x39 )
        HalUARTWrite(HAL_UART_PORT_0,(unsigned char*) final,15);

    return ( events ^ SAMPLETHERMOSTAT_TEMP_SEND_UART );
}

```

Το παραπάνω event συμβαίνει κάθε φορά που ο Coordinator δέχεται αναφορά υγρασίας. Όπως βλέπουμε, η διαδικασία είναι αρχικά η μετατροπή των int16 μετρήσεων σε uint8 σε μορφή ASCII και έπειτα η ένωση τους σε ένα κοινό String (πίνακα unsigned char). Τέλος γίνεται η αποστολή των δεδομένων μέσω της σειριακής με την εντολή HalUARTWrite.

Ο Coordinator είναι υπεύθυνος και για την διατήρηση της επιθυμητής θερμοκρασίας στο εσωτερικό του θερμοκηπίου. Αυτό γίνεται συγκρίνοντας την επιθυμητή θερμοκρασία που καθορίζουμε από το περιβάλλον διεπαφής με εύρος ενός βαθμού C°. Ο έλεγχος γίνεται περιοδικά κάθε 5 sec, καθώς η τιμή της θερμοκρασίας είναι δυναμική. Τα 5 sec είναι πολύ μικρό χρονικό διάστημα για να παρατηρηθεί αλλαγή στην θερμοκρασία ενός χώρου και επιλέχθηκε καθαρά για ευκολία επίδειξης. Οι λειτουργίες θέρμανσης και ψύξης αναπαρίστανται με την ενεργοποίηση ενός κόκκινου και μπλε LED αντίστοιχα και φαίνονται στον παρακάτω κώδικα.

```

if ( events & SAMPLETHERMOSTAT_TEMP_CHECK )
{

    if (zclSampleThermostat_LocalTemperature<preftemp-1){
        HalLedSet ( HAL_LED_2, HAL_LED_MODE_ON );

        HalLedSet ( HAL_LED_4, HAL_LED_MODE_OFF );}
    else if (zclSampleThermostat_LocalTemperature>preftemp+1){
        HalLedSet ( HAL_LED_2, HAL_LED_MODE_OFF );
        HalLedSet ( HAL_LED_4, HAL_LED_MODE_ON );}
    else { HalLedSet ( HAL_LED_2, HAL_LED_MODE_OFF );

        HalLedSet ( HAL_LED_4, HAL_LED_MODE_OFF );}
    osal_start_timerEx( zclSampleThermostat_TaskID, SAMPLETHERMOSTAT_TEMP_CHECK, 5000
);
    return ( events ^ SAMPLETHERMOSTAT_TEMP_CHECK );
}

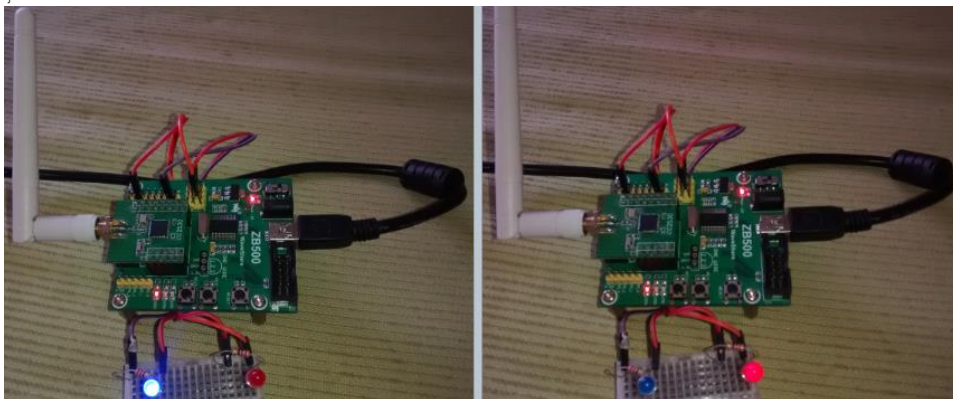
```

Η επιθυμητή θερμοκρασία (preftemp) αποσπάται από το διάβασμα της σειριακής θύρας, μέσω της συνάρτησης `uart_write_CB` που καλείται όταν έχουν γραφτεί δεδομένα στον buffer της UART.

```

void uart_write_CB(uint8 port, uint8 event )
{
    if ((event != HAL_UART_TX_FULL) && (event != HAL_UART_TX_EMPTY))
    {
        HalUARTRead (port, ch, 2);
        preftemp=atoi((char*)ch);
    }
}

```

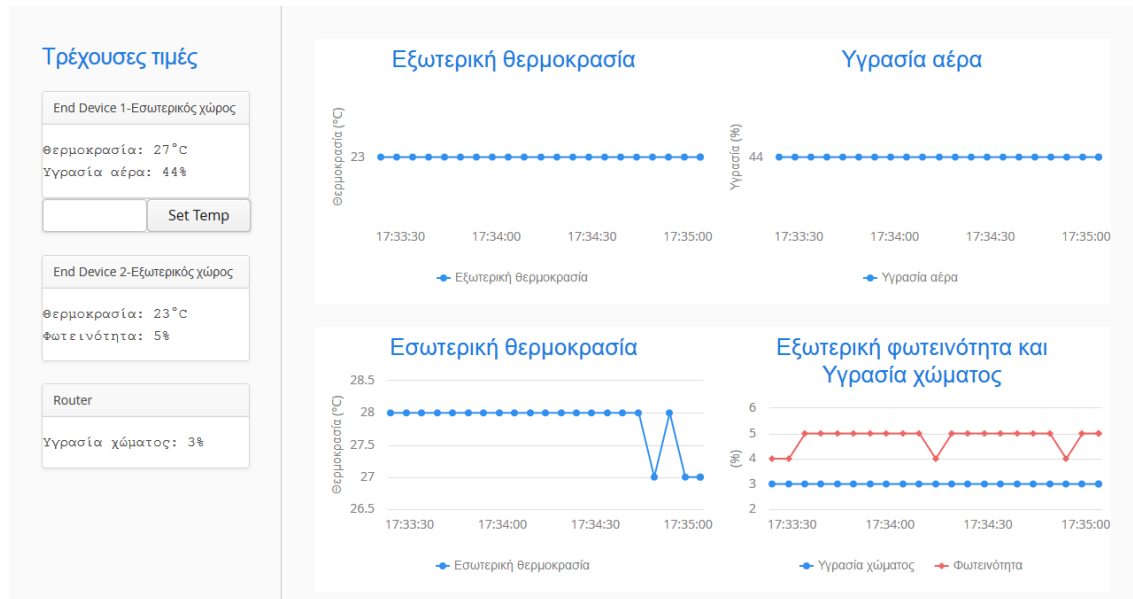


Εικόνα 8-37 Coordinator σε λειτουργία ψύξης και θέρμανσης

## 8.5 Λειτουργία Web Application

### 8.5.1 Διεπαφή χρήστη

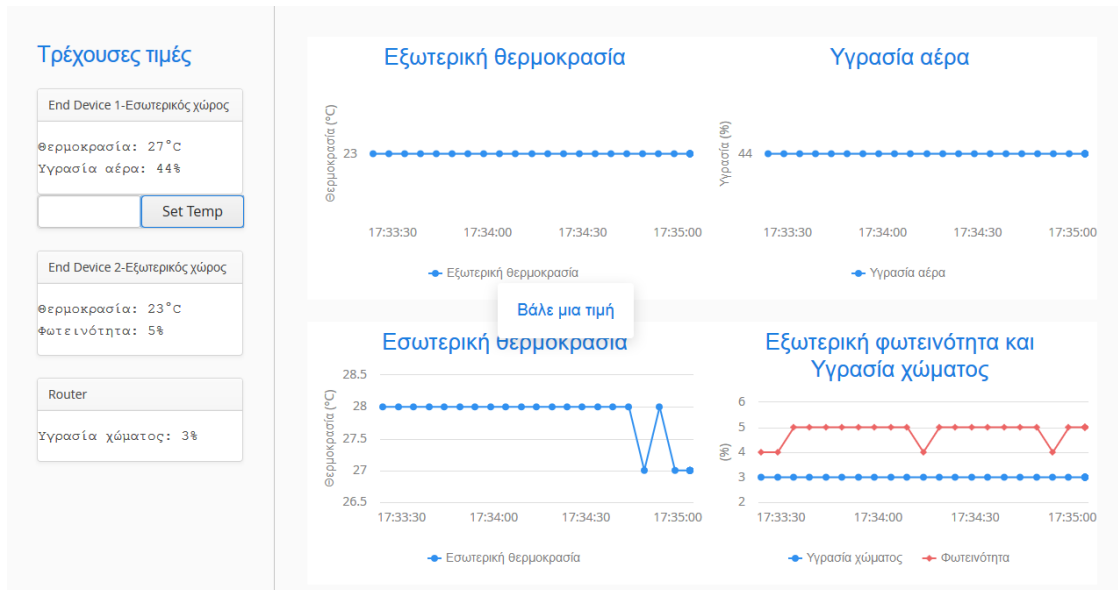
Ο χρήστης μπορεί να συνδεθεί στον server πληκτρολογώντας στον browser του υπολογιστή του το εξής link: [greenhouse.thesis.ddns.net](http://greenhouse.thesis.ddns.net). Μόλις γίνει η σύνδεση και φορτωθεί η σελίδα ο χρήστης βλέπει τις τελευταίες μετρήσεις ως τρέχουσες τιμές και τα διαγράμματα με το ιστορικό των τελευταίων 20 μετρήσεων (Εικόνα 8-38).



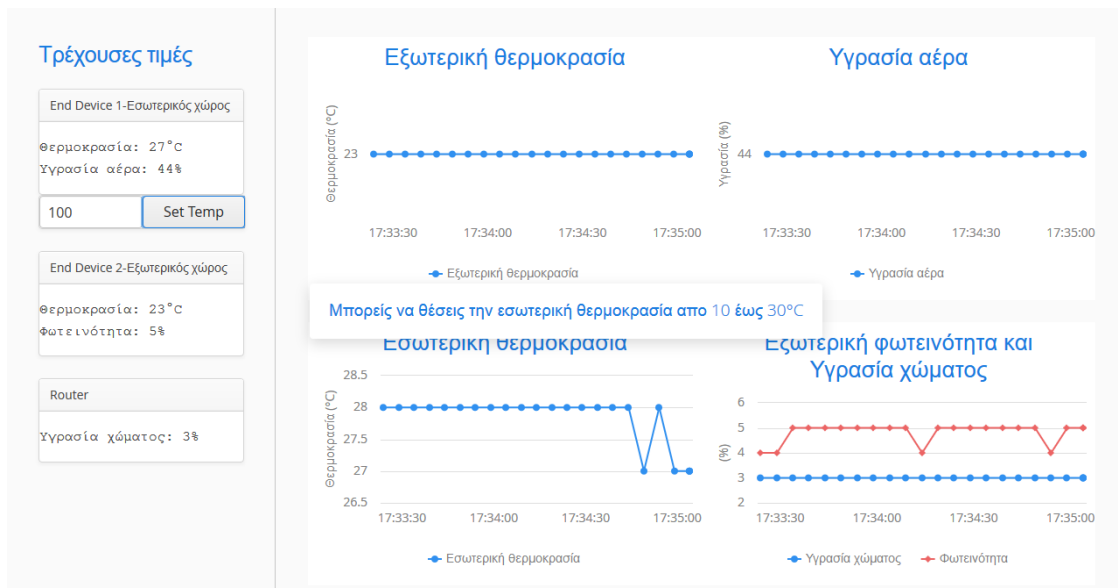
Εικόνα 8-38 Διεπαφή χρήστη

Στην συνέχεια οι τιμές αυτές ανανεώνονται κάθε 5 δευτερόλεπτα όπως και τα διαγράμματα.

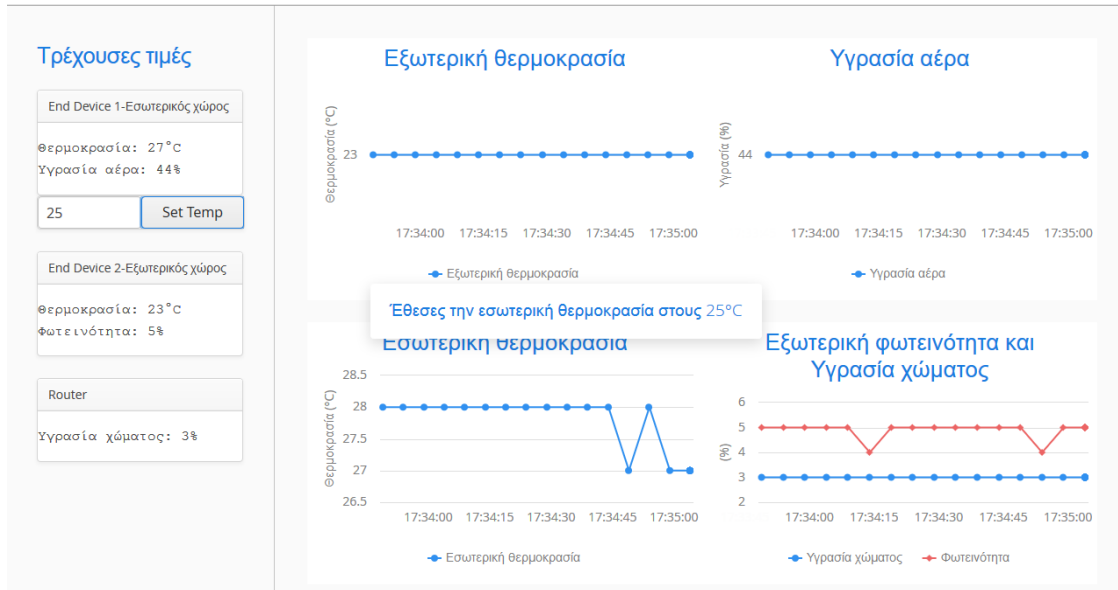
Ο χρήστης από εκεί και πέρα μπορεί να θέσει την επιθυμητή εσωτερική θερμοκρασία του θερμοκηπίου, συμπληρώνοντας την τιμή στο πεδίο text και πατώντας το κουμπί Set Temp. Γίνεται έλεγχος για εγκυρότητα της τιμής και εμφανίζονται κατάλληλα μηνύματα ανάλογα με την περίπτωση ().



Εικόνα 8-39 Πάτημα κουμπιού με κενό πεδίο text



Εικόνα 8-40 Πάτημα κουμπιού με μη έγκυρη τιμή θερμοκρασίας



## 9 Συμπεράσματα και ανοιχτά θέματα

Το σύστημα που υλοποιήθηκε στα πλαίσια της παρούσας διπλωματικής καλύπτει τις προδιαγραφές που ζητήθηκαν για την θεωρητική ανάλυση αλλά και για τη λήψη και συγκέντρωση των μετρήσεων στα πλαίσια της εφαρμογής. Πιο συγκεκριμένα:

1. Εμβαθύνσαμε και κατανοήσαμε σε βάθος την λειτουργία και την εφαρμογή των σύγχρονων πρωτοκόλλων ασύρματης δικτύωσης που αφορούν κυρίως προσωπικά δίκτυα (PANs) χαμηλής ισχύος.
2. Χρησιμοποιήσαμε το πρωτόκολλο Zigbee για την ανάπτυξη της εφαρμογής για την παρατήρηση και τον έλεγχο του θερμοκηπίου. Οι κόμβοι συλλέγουν μετρήσεις από τους αισθητήρες που διαθέτουν και στέλνουν μετρήσεις στον συντονιστή του δικτύου κάθε 5 δευτερόλεπτα. Το διάστημα αποστολών είναι πολύ μικρό και χρησιμοποιήθηκε στα πλαίσια της ανάπτυξης και real-time παρατήρησης των αλλαγών. Σε πραγματικές συνθήκες ένα λογικό διάστημα μεταξύ των αποστολών θα ήταν 30-60 λεπτά και ενδεχομένως και η δυνατότητα χειροκίνητης απαίτησης μετρήσεων από τον χρήστη να ήταν βολική.
3. Το δίκτυο που αναπτύχθηκε τηρεί τις απαιτήσεις για χαμηλή κατανάλωση, καθώς οι τελικές συσκευές ενεργοποιούνται μόνο για την αποστολή δεδομένων προσφέροντας έτσι μεγάλη διάρκεια μπαταρίας.
4. Αναπτύξαμε τον web server που διατηρεί την διαδικτυακή εφαρμογή της διπλωματικής, με την οποία ο χρήστης έχει την δυνατότητα της παρατήρησης και ελέγχου του θερμοκηπίου από οπουδήποτε έχει πρόσβαση στο διαδίκτυο. Η λειτουργία αυτή γίνεται με την χρήση dDNS (dynamic DNS) με την οποία επιτυγχάνεται η πρόσβαση στον server-τοπικό υπολογιστή με την χρήση custom URL. Έτσι η εφαρμογή εντάσσεται πλήρως στον τομέα του Internet Of Things.
5. Αν και η εφαρμογή που υλοποιήθηκε αφορά την εγκατάσταση ενός θερμοκηπίου, χρησιμοποιώντας ως βάση το ίδιο δίκτυο με κάποιες μετατροπές (είδος αισθητήρων, αριθμός κόμβων) υπάρχει δυνατότητα για εγκατάσταση για οποιοδήποτε περιβάλλον (οικιακό ή βιομηχανικό) που απαιτεί παρατήρηση και έλεγχο κάποιων παραμέτρων.
6. Το κόστος της εφαρμογής που αναπτύχθηκε επίσης διατηρήθηκε σε χαμηλά επίπεδα, πράγμα που την θα την καθιστούσε ανταγωνιστική στην αγορά, καθώς οι έτοιμες λύσεις που υπάρχουν ήδη είναι περίπου μια τάξη μεγέθους πιο ακριβές.

Ο web server της εφαρμογής τρέχει σε ένα υπολογιστή που θεωρείται ότι βρίσκεται στην εγκατάσταση του θερμοκηπίου και συνδέεται με τον coordinator. Μια πιο εύχρηστη λύση θα ήταν να τρέχει σε ένα Single Body Computer (πχ Raspberry PI ή Beaglebone) που θα ήταν πιο οικονομική λύση από άποψη κόστους και κατανάλωσης ισχύος. Η πιο ολοκληρωμένη υλοποίηση είναι η εγκατάσταση της βάσης δεδομένων και του web service σε κάποιον απομακρυσμένο server. Με αυτό

τον τρόπο η λειτουργία του τοπικού υπολογιστή θα αφορούσε την συλλογή των μετρήσεων και την εγγραφή τους στην απομακρυσμένη βάση δεδομένων.

Οι κόμβοι του δικτύου έχουν βασιστεί στην χρήση των development boards τα οποία μας διευκόλυναν στην διασύνδεση των περιφερειακών συσκευών αλλά και σε μια σειρά δοκιμών για την εξακρίβωση της σωστής λειτουργίας τους. Είναι προφανές ότι δεν αποτελεί προϊόν έτοιμο για διάθεση στην αγορά. Για να συμβεί αυτό πρέπει να προχωρήσουμε σε μια ολοκληρωμένη πλακέτα με την μέθοδο PCB καθώς και στην δημιουργία ενός προστατευτικού κελύφους δεδομένων των συνθηκών ενός θερμοκηπίου (πχ υγρασία).

Η παρούσα υλοποίηση του δικτύου προϋποθέτει την χρήση UART για την επικοινωνία με κάποιο τερματικό. Μια μελλοντική υλοποίηση υλοποίηση είναι η ανάπτυξη ενός gateway το οποίο θα ενσωματώνει κάποιο module ασύρματης δικτύωσης (πχ GSM, WiFi, Bluetooth, GPRS). Με την χρήση GSM υπάρχει η δυνατότητα απευθείας επικοινωνίας με SMS για την ενημέρωση του χρήστη. Με τις υπόλοιπες τρεις έχουμε την δυνατότητα σύνδεσης του δικτύου ZigBee με το διαδίκτυο.

## 10 Βιβλιογραφία-Παραπομπές

- 1) Shanin Farahani. 2008. *ZigBee Wireless Networks and Transceivers*. Newnes Newton. USA
- 2) Drew Gislason. 2008. *Zigbee Wireless Networking*. Newnes Newton
- 3) Stefano Tennina, Anis Koubaa, Roberta Daidone, Mário Alves, Petr Jurčík, Ricardo Severino, Marco Tiloca, Jan-Hinrich Hauer, Nuno Pereir. 2013. *IEEE 802.15.4 and ZigBee as Enabling Technologies for Low-Power Wireless Systems with Quality-of-Service Constraints*. Springer (SpringerBriefs in Electrical and Computer Engineering)
- 4) Houda Labiod, Hossam Afifi, Costantino de Santis. 2007. *Wi-Fi, Bluetooth, Zigbee and WiMax*. Springer
- 5) Dieter Uckelmann, Mark Harrison, Florian Michahelles. 2011. *Architecting the Internet of Things*, Springer
- 6) A. Dunkels, JP. Vasseur. September 2008. IP for Smart Objects. IPSO Alliance White Paper
- 7) G. Montenegro, N. Kushalnagar, J. Hui, D. Culler. September 2007. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC 4944 (Proposed Standard)
- 8) IPv6 over Low power WPAN (6lowpan) Working Group. Internet Engineering Task Force (IETF)
- 9) Paolo Baronti, Prashant Pillai, Vince W.C. Chook, Stefano Chessa ,Alberto Gotta, Y. Fun Hu. December 2006. Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards
- 10) Texas Instruments Z-stack <http://www.ti.com/tool/z-stack>
- 11) Vaadin book <https://vaadin.com/book>
- 12) IAR 8051 IDE <https://www.iar.com/iar-embedded-workbench/8051/>
- 13) Libelium solution <http://www.libelium.com/libeliumworld/agriculture/>
- 14) Growtronix solution <http://www.growtronix.com/store/index.php?route=common/home>

Αλλαγή κωδικού πεδίου

Αλλαγή κωδικού πεδίου

Αλλαγή κωδικού πεδίου

Αλλαγή κωδικού πεδίου

Αλλαγή κωδικού πεδίου