ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΥΓΚΡΙΤΙΚΗ ΑΞΙΟΛΟΓΗΣΗ ΤΩΝ ΠΡΩΤΟΚΟΛΛΩΝ ΑΣΥΡΜΑΤΗΣ ΔΙΚΤΥΩΣΗΣ ΑΙΣΘΗΤΗΡΩΝ SMARTMESH IP ΚΑΙ ZIGBEE

ΠΑΠΑΔΗΜΗΤΡΙΟΥ ΓΕΩΡΓΙΟΣ

ΠΥΡΟΜΑΛΗΣ ΔΗΜΗΤΡΙΟΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΑΥΤΟΜΑΤΙΣΜΟΥ

ΜΑΙΟΣ 2019

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ (1η ή 2η σελίδα)

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο/Η κάτωθι υπογεγραμμένος/η ΠΑΠΑΔΗΜΗΤΡΙΟΥ ΓΕΩΡΓΙΟΣ του ΝΙΚΟΛΑΟΥ, φοιτητής του Τμήματος ΜΗΧΑΝΙΚΩΝ ΑΥΤΟΜΑΤΙΣΜΟΥ του Πανεπιστημίου Δυτικής Αττικής, πριν αναλάβω την εκπόνηση της Πτυχιακής Εργασίας μου δηλώνω ότι ενημερώθηκα για τα παρακάτω:

«Η Πτυχιακή Εργασία (ΠΕ) αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο του συγγραφέα, όσο και του Ιδρύματος και θα πρέπει να έχει μοναδικό χαρακτήρα και πρωτότυπο περιεχόμενο.

Απαγορεύεται αυστηρά οποιοδήποτε κομμάτι κειμένου της να εμφανίζεται αυτούσιο ή μεταφρασμένο από κάποια άλλη δημοσιευμένη πηγή. Κάθε τέτοια πράξη αποτελεί προϊόν λογοκλοπής και εγείρει θέμα Ηθικής Τάξης για τα πνευματικά δικαιώματα του άλλου συγγραφέα. Αποκλειστικός υπεύθυνος είναι ο συγγραφέας της Π.Ε. ο οποίος φέρει και την ευθύνη των συνεπειών, ποινικών και άλλων, αυτής της πράξης.

Πέραν των όποιων ποινικών ευθυνών του συγγραφέα, σε περίπτωση που το Ίδρυμα του έχει απονείμει Πτυχίο, αυτό ανακαλείται με απόφαση της Συνέλευσης του Τμήματος. Η Συνέλευση του Τμήματος με νέα απόφασή της, μετά από αίτηση του ενδιαφερόμενου, του αναθέτει εκ νέου την εκπόνηση Π.Ε με άλλο θέμα και διαφορετικό επιβλέποντα καθηγητή. Η εκπόνηση της ενλόγω Π.Ε πρέπει να ολοκληρωθεί εντός του λάχιστον ενός ημερολογιακού έτους από την ημερομηνία ανάθεσής της.

Ο Δηλών

Ημερομηνία

6/7/2020

Περίληψη

Σκοπός της παρούσας εργασίας είναι η παρουσίαση των δυνατοτήτων των πρωτοκόλλων επικοινωνίας Smartmesh IP και ZigBee, καθώς και του hardware που φιλοξενεί τα πρωτόκολλα αυτά. Αρχικά γίνεται μια γενική εισαγωγή, σχετική με την επικοινωνία μέσω πρωτοκόλλων επικοινωνίας. Σημαντική είναι η κατανόηση όλων των παραμέτρων για τις λειτουργίες των πρωτοκόλλων και ως εκ τούτου δίνεται βάση και στην συνοπτική παράθεση συνοδευτικών πληροφοριών. Η εργασία καταλήγει στην τελική σύγκριση των δύο στις πιο κομβικές κατηγορίες που μπορούν να απασχολήσουν τον τελικό χρήστη. Η επιλογή ενός εκ των δύο συγκρινόμενων πρωτοκόλλων και του hardware τους για την χρήση τους σε μια εφαρμογή κρίνεται από λεπτομέρειες που, ανάλογα την περίσταση και τις απαιτήσεις τις εκάστοτε εφαρμογής, μπορούν να αποδειχθούν μέγιστης σημασίας.

Περιεχόμενα

Κεφάλαιο 1: Εισαγωγή

1.1 Το μοντέλο OSI

Το μοντέλο OSI (Open System Interconnection) δημιουργήθηκε από την ISO (International Organization for Standardization) για να επιτρέψει και να διευκολύνει την επικοινωνία μεταξύ υπολογιστικών συστημάτων διαφορετικών εταιρειών και κατασκευαστών με τη χρήση εγκεκριμένων πρωτόκολλων. Αποτελείται από επτά στρώματα (layers) τα οποία είναι:

1. Physical
2. Data link
3. Network
4. Transport
5. Session
6. Presentation
7. Application

Τα πρώτα τρία κατηγοριοποιούνται στην ομάδα των Host layers, ενώ τα υπόλοιπα τέσσερα στην ομάδα των Media layers.

Κατά τη μετάδοση δεδομένων, ένα πακέτο δεδομένων συντίθεται στο τελευταίο layer της αποστέλλουσας συσκευής (Application layer) ως ένα PDU (protocol data unit) και μεταβαίνει στο επόμενο layer. Πλέον ονομάζεται SDU (service data unit), του προστίθεται ένα header, footer ή και τα δύο και τελικά γίνεται ένα PDU του τωρινού layer. Αυτή η διαδικασία συνεχίζεται μέχρι και το physical layer όπου τα δεδομένα περνούν-μεταδίδονται στην συσκευή παραλήπτη. Από το physical layer του παραλήπτη το SDU περνάει στα επόμενα layers, ενώ σε κάθε μετάβαση του αφαιρούνται και headers/footers από τα layers του αποστολέα, έτσι ώστε όταν το πακέτο δεδομένων φτάσει στο Application layer να απορροφηθούν ατόφια τα δεδομένα. Ακολουθεί μια συνοπτική παρουσίαση των λειτουργιών του κάθε στρώματος.

1.1.1 Physical Layer

Είναι υπεύθυνο για τη μετάδοση δεδομένων μεταξύ μιας συσκευής και ενός μέσου φυσικής μετάδοσης, δηλαδή μετατρέπει τα ψηφιακά bits σε ηλεκτρικά, ραδιοφωνικά ή οπτικά σήματα.

1.1.2 Data Link Layer

Προσφέρει τη δυνατότητα μεταφοράς δεδομένων μεταξύ κόμβων, καθώς και καθορίζει το ποιο πρωτόκολλο θα χρησιμοποιηθεί για την επικοινωνία τους. Κόμβος ονομάζεται μια συσκευή συνδεδεμένη σε ένα δίκτυο που στέλνει ή/και λαμβάνει δεδομένα μέσω προκαθορισμένων διαδρομών. Το IEEE 802 χωρίζει το Data Link σε δύο υποστρώματα (sublayers). Το πρώτο είναι το MAC (Medium Access Control) layer που είναι υπεύθυνο για τον έλεγχο της διαδικασίας όπου κάποιες συσκευές σε ένα δίκτυο πρόκειται να έχουν πρόσβαση σε ένα μέσο και να στείλουν δεδομένα μέσω αυτού. Το δεύτερο είναι το LLC (Logical Link Control) layer που είναι υπεύθυνο για την διαχείριση των πρωτοκόλλων του Network layer αλλά και ελέγχει τα σφάλματα και το συγχρονισμό των frames.

1.1.3 Network Layer

Το Network Layer παρέχει τα διαδικαστικά και λειτουργικά μέσα για την μεταφορά πακέτων δεδομένων μεταξύ κόμβων που βρίσκονται σε διαφορετικά δίκτυα. Ένα δίκτυο είναι το μέσο στο οποίο μπορούν να συνδεθούν κόμβοι με διαφορετικές διευθύνσεις και να στείλουν δεδομένα σε άλλους κόμβους, με το δίκτυο να βρίσκει την σωστή λύση για τη δρομολόγηση του πακέτου στον προορισμό του. Αν τα δεδομένα προς αποστολή είναι πολύ μεγάλου μεγέθους για να σταλούν μέσω Data Link Layer, το δίκτυο μπορεί να διαχωρίσει τα δεδομένα σε κομμάτια για αποστολή στον προορισμό τους και να τα επανενώσει μετά την άφιξή τους. Η σωστή και ελεγχόμενη άφιξη των πακέτων στον προορισμό τους δεν είναι κάτι που το Network Layer μπορεί να εγγυηθεί, για αυτό τον σκοπό χρησιμοποιούνται network layer protocols.

1.1.4 Transport Layer

Είναι υπεύθυνο για την μεταφορά των δεδομένων στο προορισμό τους διατηρώντας ταυτόχρονα την ποιότητα των υπηρεσιών που παρέχει. Αυτό το επιτυγχάνει με την αποστολή πακέτων acknowledgment (επιβεβαίωσης) κατά την επιτυχή άφιξη τμήματος ενός μηνύματος, καθώς και με την αρίθμηση τους για να είναι σίγουρο ότι θα φτάσουν με τη σωστή σειρά για να συναρμολογηθούν.

1.1.5 Session Layer

Το Session Layer έχει ως αρμοδιότητα την διαχείριση, έναρξη αλλά και διακοπή της σύνδεσης και των αλληλεπιδράσεων μιας εφαρμογής. Χαρακτηριστικό παράδειγμα της λειτουργίας του Session Layer είναι η διαχείριση της ομαλής διεξαγωγής μιας βιντεοκλήσης, όπου ο συγχρονισμός εικόνας και ήχου είναι κρίσιμος για όλη την διάρκειά της.

1.1.6 Presentation Layer

Το Presentation Layer λειτουργεί ως μεσάζοντας στην διαδικασία μετατροπής της ανθρώπινης εντολής μέσω της εφαρμογής στο Application Layer, σε «γλώσσα» κατανοητή από το δίκτυο, αλλά και το αντίθετο.

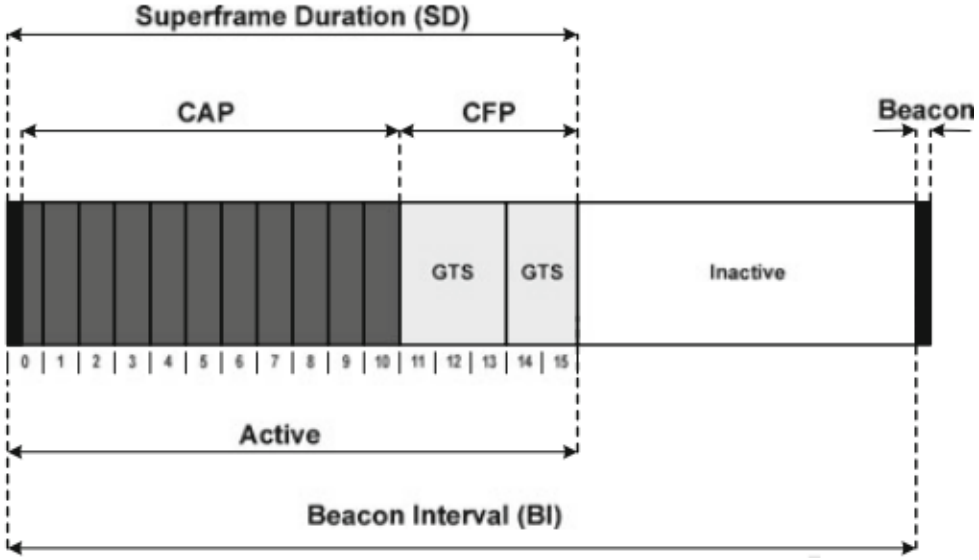
1.1.7 Application Layer

Επικοινωνεί με όσες εφαρμογές λογισμικού μπορεί να αλληλεπιδράσει ο χρήστης. Μερικές από τις αρμοδιότητές του είναι η αναγνώριση των συσκευών με τις οποίες θα γίνει η επικοινωνία, ο συγχρονισμός της επικοινωνίας και γενικά ο έλεγχος της διαθεσιμότητας των απαραίτητων παραμέτρων για την ομαλή επικοινωνία. Πιο συγκεκριμένα αποτελεί το μέσο διεπαφής για την απεικόνιση των πληροφοριών στον χρήστη.

Κεφάλαιο 2: Παρουσίαση δυνατοτήτων IEEE 802.15.4 και IEEE 802.15.4e

2.1 IEEE 802.15.4

Αρχικά, το 802.15.4 είναι ένα standard για PAN (Personal Area Networks) η τοπολογία των οποίων μπορεί να είναι star, tree ή mesh. Ένα PAN δημιουργείται από έναν συντονιστή, που ως στόχο έχει την διοίκηση των κόμβων ενός δικτύου. Οι κόμβοι είναι δύο τύπων: Full-Function Device(FFD) και Reduced-Function Device (RFD). Ένα FFD μπορεί να δράσει ως συντονιστής αλλά και ως απλός κόμβος. Ένα RFD έχει πολύ περιορισμένες δυνατότητες επικοινωνίας, οπότε μπορεί να επικοινωνήσει μόνο με FFDs. Ένα δίκτυο 802.15.4 λειτουργεί σε συχνότητα συνήθως 2400-2483.5 MHz (έως 16 κανάλια, παγκόσμια χρήση) αλλά υπάρχουν και οι επιλογές των 868-868.6 MHz (ένα κανάλι, μόνο για Ευρώπη) και 902-928 MHz (έως 10 κανάλια, μόνο για Β. Αμερική). Μια τυπική δομή δικτύου περιέχει κόμβους με εμβέλεια περίπου 10 μέτρων και ρυθμό μετάδοσης 250 kbit/s. Το 802.15.4 παρέχει δύο τρόπους αξιοποίησης των καναλιών, το beacon enabled mode και το non-beacon enabled mode, όπου beacons είναι frames συγχρονισμού τα οποία δημιουργεί περιοδικά ο συντονιστής. Στη πρώτη περίπτωση γίνεται χρήση του slotted Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA), ενώ στην δεύτερη περίπτωση γίνεται χρήση του unslotted CSMA/CA.
Το beacon enabled mode χρησιμοποιεί μια δομή superframe η οποία βασίζεται σε beacons.



Σχετικά με το superframe (θεωρείται ότι το δίκτυο λειτουργεί στα 2.4 GHz): -Beacon Interval (BI) είναι ο χρόνος μεταξύ δύο beacons. Εξαρτάται από την παράμετρο Beacon Order (BO) και χαρακτηρίζεται από τον ακόλουθο τύπο:

$$BI = 15.36 \cdot 2^{BO} ms, \;\; 0 \leq BO \leq 14$$

-Superframe Duration (SD) είναι η ενεργή περιοχή του superframe. Εξαρτάται από την παράμετρο Superframe Order (SO) και χαρακτηρίζεται από τον ακόλουθο τύπο:

$$SD = 15.36 \cdot 2^{SO} ms, \qquad 0 \leq SO \leq BO \leq 14$$

-Contention Access Period (CAP) είναι υποδιαίρεση του SD. Σε αυτό το στάδιο μπορεί να γίνει χρήση του slotted CSMA/CA.

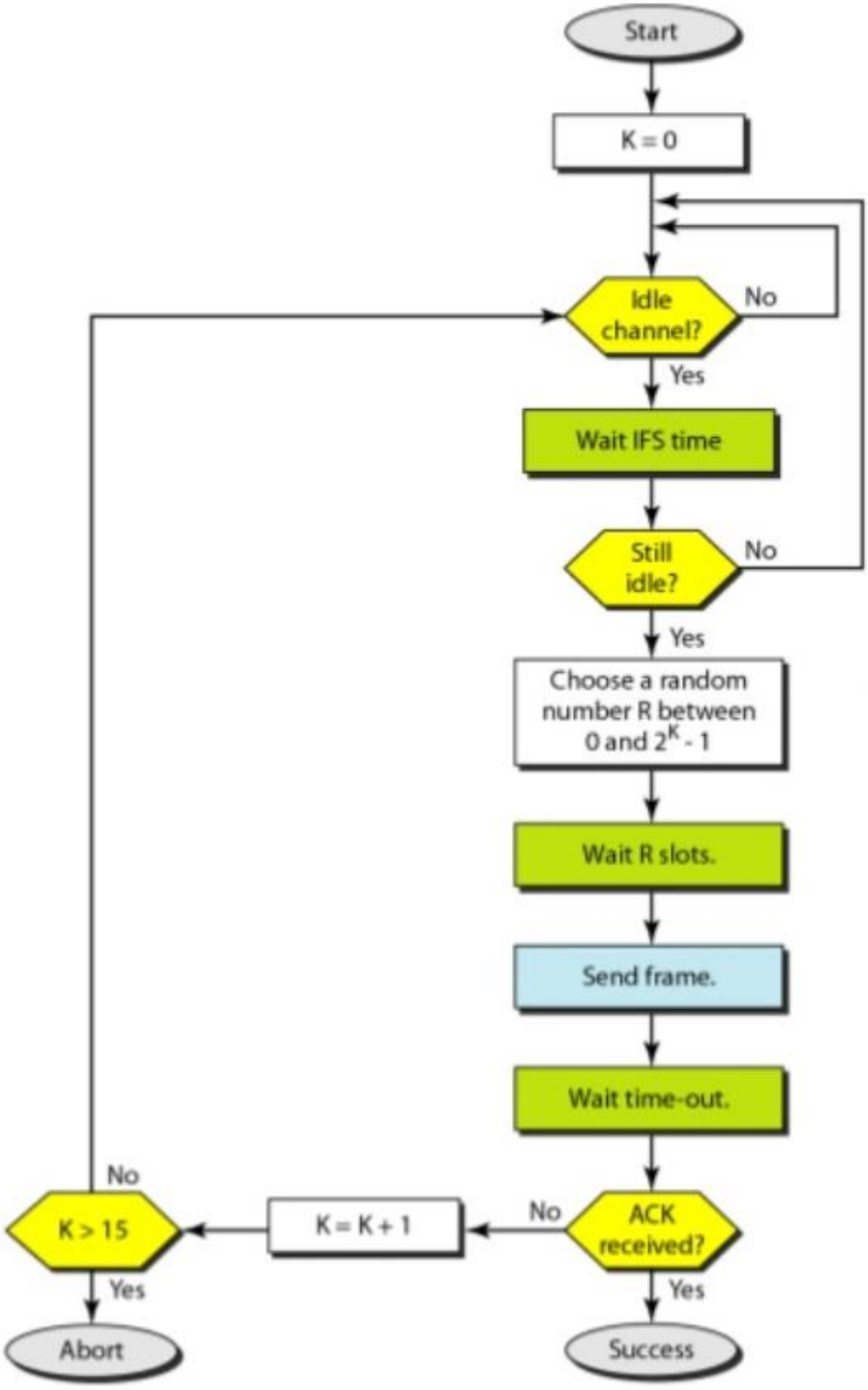
-Contention Free Period (CFP) είναι υποδιαίρεση του SD. Σε αυτό το στάδιο μπορεί να γίνει χρήση του Time Division Multiple Access (TDMA) με την βοήθεια των Guaranteed Time Slots (GTS) τα οποία είναι διανεμημένα στους κόμβους εκ των προτέρων. Εν ολίγοις το TDMA είναι μια μέθοδος πρόσβασης στο μέσο επικοινωνίας που επιτρέπει στους κόμβους να στείλουν πακέτα γρήγορα και διαδοχικά, χάρη στο ότι υπάρχει «αφιερωμένο» για το καθένα ένα time slot. Στον υπόλοιπο χρόνο του BI (Inactive period) ο κόμβος βρίσκεται σε κατάσταση low power για να εξοικονομήσει ενέργεια.

Το non-beacon enabled mode δεν έχει superframe και χρησιμοποιεί το unslotted CSMA/CA πρωτόκολλο για την πρόσβαση στο κανάλι. Οι κόμβοι είναι πάντα ενεργοί και έτσι η διαχείριση της ενέργειας γίνεται μόνο από τα layers πάνω από το MAC.

2.1.1 CSMA/CA

Το CSMA/CA είναι ένα πρωτόκολλο (Data Link layer) που επιτρέπει στους κόμβους να αποφύγουν - σε έναν βαθμό - τα δεδομένα τους να «συγκρουστούν», δηλαδή να επιχειρήσουν να στείλουν πακέτα στον συντονιστή ταυτόχρονα, μεταδίδοντας τα δεδομένα μόνο όταν ανιχνεύσουν ότι το επιλεγμένο κανάλι είναι σε κατάσταση "idle". Πριν την μετάδοση, ο κόμβος ελέγχει το μέσο μετάδοσης για τυχόν μεταδόσεις άλλου κόμβου. Αν ανιχνευτεί μετάδοση άλλου κόμβου, περιμένει για ένα τυχαίο χρονικό πλαίσιο (από ένα σύνολο συγκεκριμένων χρόνων) και ξεκινάει πάλι να ελέγξει το μέσο. Ο τυχαίος χρόνος βοηθάει στη μείωση της πιθανότητας συμφόρησης, χωρίς φυσικά να εγγυάται την εξάλειψή της. Εδώ παρουσιάζεται και το πρόβλημα του αποκαλούμενου hidden node ή κρυμμένου κόμβου, όταν δηλαδή ένας κόμβος επικοινωνεί άμεσα με τον Access Point κόμβο ή συντονιστή, αλλά όχι με τους υπόλοιπους κόμβους που επικοινωνούν με τον συντονιστή. Αυτό έχει ως αποτέλεσμα κάποιοι κόμβοι να αποστείλουν δεδομένα στον συντονιστή ταυτόχρονα και έτσι να μην παραδοθεί σε αυτόν τίποτα. Σύμφωνα με σχετική έρευνα[1], το unslotted CSMA έχει περισσότερες πιθανότητες επιτυχούς παράδοσης της πληροφορίας. Στο παρακάτω διάγραμμα ροής απεικονίζεται η βασική λειτουργία του CSMA/CA (όπου K είναι ο αριθμός των προσπαθειών αποστολής των δεδομένων και $2^K + 1$ είναι το contention window).

[1] Analysis and Compare of Slotted and Unslotted CSMA in IEEE 802.15.4 https://www.researchgate.net/publication/224610070_Analysis_and_Compare_of_Slotted_and_Unslotted_CSMA_in_IEEE_802154


Start
K = 0
Idle channel?
No
Yes
Wait IFS time
Still idle?
No
Yes
Choose a random number R between 0 and $2^K - 1$
Wait R slots.
Send frame.
Wait time-out.
ACK received?
No
Yes
Success
K = K + 1
K > 15
No
Yes
Abort

2.1.2 Περιορισμοί και αδύναμα σημεία του IEEE 802.15.4

Ακριβώς επειδή το πρωτόκολλο βασίζεται στο CSMA/CA, δεν γίνεται με κάποιον τρόπο να εγγυηθεί ότι τα δεδομένα θα φτάσουν στο προορισμό τους στον επιθυμητό χρόνο. Η περίπτωση, δηλαδή, τα δεδομένα να καθυστερήσουν ή και να μη παραδοθούν καν είναι φυσιολογική. Έτσι, το 802.15.4 δεν είναι κατάλληλο για εφαρμογές που απαιτούν πολύ μεγάλη ακρίβεια και καθυστερήσεις εντός του προβλεπόμενου πλαισίου (όπως βιομηχανικά και ιατρικά συστήματα). Αυτό συμβαίνει τόσο στο beacon enabled mode, εξαιτίας της μέθοδου των τυχαίων χρόνων του CSMA/CA και του συγχρονισμού των beacons, όσο και στο non-beacon enabled mode εάν πολλοί κόμβοι προσπαθήσουν να εκπέμψουν ταυτόχρονα. Επιπροσθέτως, δεν υπάρχει προστασία από παρεμβολές και fading (όταν η ίδια πληροφορία φτάνει στον δέκτη από διαφορετικούς προορισμούς, συνήθως λόγω ανακλάσεων). Το IEEE 802.15.4 MAC πρωτόκολλο χρησιμοποιεί ένα κανάλι και δεν διαθέτει τρόπους για προστασία από αυτά τα προβλήματα, όπως frequency hopping. Ως εκ τούτου το δίκτυο μπορεί να βιώσει τακτικές αστάθειες ή ακόμα και να καταρρεύσει πλήρως. Τέλος, οι ενδιάμεσοι κόμβοι αναμετάδοσης (routers) σε ένα δίκτυο πολλών κόμβων στη πράξη καταλήγουν να είναι πάντα radio on καταναλώνοντας πολύ μεγαλύτερα ποσοστά ενέργειας από όσο θα έπρεπε. Αυτό αντιτίθεται στο ότι, *θεωρητικά*, σε ένα δίκτυο με 802.15.4 οι ενδιάμεσοι κόμβοι αναμετάδοσης δεν χρειάζεται να είναι πάντα ενεργοί.

2.2 IEEE 802.15.4e

Το 802.15.4e είναι ένα MAC πρωτόκολλο με βασικό στόχο την αποτελεσματικότερη λειτουργία και τη γενική βελτίωση σχετικά με το 802.15.4 στο οποίο και βασίζεται. Πιο συγκεκριμένα, είναι εξοπλισμένο με MAC behaviors, τα οποία καλύπτουν τις ανάγκες συγκεκριμένων εφαρμογών, και με βελτιώσεις για τη γενική λειτουργία του πρωτοκόλλου. Ακολουθεί μια συνοπτική παρουσίαση για το κάθε behavior.

2.2.1 MAC behaviors

- Radio Frequency Identification Blink (BLINK). Ιδιαίτερα χρήσιμο σε περιπτώσεις όπου ένας κόμβος δεν λειτουργεί τακτικά.
- Asynchronus Multi-Channel adaptation (AMCA). Βοηθάει στις εφαρμογές που απαιτούν μεγάλους αριθμούς κόμβων.
- Deterministic and Synchronous Multi-channel Extension (DSME). Σκοπό έχει την ενίσχυση της αξιοπιστίας όσον αφορά την επιτυχή και γρήγορη αποστολή δεδομένων.
- Low Latency Deterministic Network (LLDN). Στοχεύει στην καταπολέμηση των καθυστερήσεων.
- Time Slotted Channel Hopping (TSCH). Επιτρέπει την αξιόπιστη και ταχύτερη μετάδοση δεδομένων, καθώς και την εξοικονόμηση ενέργειας.

2.2.2 Time Slotted Channel Hopping

Το TSCH είναι ένα MAC behavior με πολύ σημαντικό ρόλο στην επικοινωνία των συσκευών που χρησιμοποιούν το 802.15.4e. Όπως φαίνεται και από το όνομα, το TSCH θεωρητικά μεταχειρίζεται 16 κανάλια μέσω offset τους για να επιτρέψει την ταυτόχρονη μετάδοση δεδομένων μεταξύ διαφορετικών συσκευών σε περισσότερες συσκευές. Έτσι, περιορίζεται το πρόβλημα που είχε το 802.15.4 σχετικά με το fading. Για την λειτουργία των συσκευών με το TSCH πρέπει να καθοριστούν οι σύνδεσμοι (links) μεταξύ των συσκευών, δηλαδή ποια θα στείλει και σε ποια, και τι τύπος συνδέσμου χρησιμοποιείται. Οι τύποι των συνδέσμων είναι δύο, ο dedicated και ο shared. Ένας dedicated σύνδεσμος είναι αποκλειστικός στη συσκευή με την οποία έχει συνδυαστεί, ενώ σε έναν shared σύνδεσμο έχουν πρόσβαση πολλοί πομποί. Αυτό με μια πρώτη ματιά προϋποθέτει έναν σχεδιασμό του δικτύου έτσι ώστε να μην προσπαθήσει κάποια συσκευή να κάνει μετάδοση στο ίδιο shared link και timeslot με κάποια άλλη, με λίγα λόγια δεν πρέπει να υπάρξουν συγκρούσεις (collisions). Σε μια τοπολογία πολλών συσκευών ο χρήστης πρέπει χειροκίνητα να «συνδέσει» τις συσκευές που επιθυμεί (πομπός προς δέκτη) με το link τους. Αυτή η δουλειά, όμως, μπορεί να γίνει και μέσω των πιο υψηλών layers. Το πρωτόκολλο Smartmesh IP με τη βοήθεια του TSCH προσφέρει δυναμική ανταπόκριση στις mesh τοπολογίες του, μπορεί δηλαδή με ευκολία να αποφασίζει κάθε φόρα ποιος σύνδεσμος μεταξύ συσκευών θα χρησιμοποιηθεί, κάτι που θα σχολιαστεί σε επόμενο κεφάλαιο.

Πέρα, όμως, από τα MAC behaviors το πρωτόκολλο 802.15.4e επιτυγχάνει μικρότερους χρόνους αλληλεπίδρασης μεταξύ των συσκευών που το υποστηρίζουν, χάρη στο Fast Association (FastA). Δίνει επίσης τη δυνατότητα για πολύ περιορισμένη κατανάλωση ρεύματος χάρη στη λειτουργία Low Energy (LE). Το τίμημα της λειτουργίας αυτής είναι παραπάνω latency, αλλά επιτρέπει σε μια συσκευή να λειτουργεί με duty cycle ακόμα και μικρότερο του 1%, ενώ στα πιο υψηλά layers φαίνεται σαν να είναι πάντα σε λειτουργία (always on). Αυτό είναι ιδιαίτερα χρήσιμο σε σενάρια σχετικά με το Internet of Things διότι τα πρωτόκολλα ιντερνέτ είναι σχεδιασμένα να λειτουργούν με συσκευές που είναι «always on».

Κεφάλαιο 3: Το πρωτόκολλο ZigBee

Το ZigBee είναι ένα πρωτόκολλο επικοινωνίας για μικρό ρυθμό διάδοσης δεδομένων σε μικρές αποστάσεις. Είναι κατάλληλο για star, tree και mesh τοπολογίες και βασίζεται πάνω στο IEEE 802.15.4 για το PHY και το MAC, ενώ καθορίζει τα NWK και APL layers του OSI. Παρακάτω παρατίθενται περιεκτικά τα καθήκοντα κάθε layer ξεχωριστά.

Το PHY layer είναι υπεύθυνο για:

- Την ενεργοποίηση και απενεργοποίηση του radio πομποδέκτη
- Την μετάδοση και την λήψη δεδομένων
- Την επιλογή της συχνότητας καναλιού που θα λειτουργήσει ο πομποδέκτης
- Τον έλεγχο του αν η συγκεκριμένη συχνότητα χρησιμοποιείται ήδη, ώστε να μπορεί να χρησιμοποιηθεί για μετάδοση
- Την χρήση του Clear Channel Assessment, δηλαδή την εκτίμηση της κατάστασης του καναλιού μέσω του CSMA/CA.
- Την δημιουργία LQI, δηλαδή μια ένδειξη που αντανακλά την ποιότητα των πακέτων δεδομένων, συνήθως σχετική με την ποιότητα του σήματος.

Το MAC layer είναι υπεύθυνο για:

- Τη δημιουργία beacon frames (αν η συσκευή είναι συντονιστής)
- Τον συγχρονισμό της συσκευής με το beacon (σε ένα δίκτυο με ενεργοποιημένα τα beacons)
- Την χρήση του CSMA/CA για την πρόσβαση στο κανάλι
- Την διαχείριση των GTS
- Την παροχή αξιόπιστης σύνδεσης μεταξύ δύο συσκευών
- Την διευκόλυνση της αλληλεπίδρασης μεταξύ γειτονικών PAN

Το NWK layer είναι υπεύθυνο για:

- Τη διαμόρφωση μιας νέας συσκευής, για παράδειγμα να τεθεί στη θέση συντονιστή ή να εισέλθει σε ένα υπάρχον δίκτυο
- Τη δημιουργία ενός δικτύου

- Την είσοδο ή έξοδο μιας συσκευής από ένα δίκτυο
- Την εφαρμογή ασφάλειας του NWK layer
- Την δρομολόγηση των πακέτων στο προορισμό τους από τις κατάλληλες συσκευές
- Την ανακάλυψη και διατήρηση των πιο κατάλληλων «δρόμων» για την επικοινωνία των συσκευών
- Την ανακάλυψη και καταγραφή των γειτονικών κόμβων που απέχουν ένα hop
- Την διευθυνσιοδότηση στους κόμβους που εισέρχονται σε ένα δίκτυο

Το APL layer χωρίζεται σε τρία μέρη, το APS (Application Support) sublayer, τα ZDO (ZigBee Device Objects) και το Application framework. Το APS παρέχει τη μετάβαση από το NWK στο APL και το ανάποδο. Το ZDO είναι μια εφαρμογή που χρησιμοποιεί τα NWK και APS για να θέσει σε μια συσκευή έναν από τους τρεις ZigBee ρόλους, του συντονιστή, του δρομολογητή ή της απλής συσκευής.

Το APS sublayer είναι υπεύθυνο για:

- Τη διατήρηση των πινάκων δέσμευσης
- Την προώθηση μηνυμάτων μεταξύ συζευγμένων συσκευών
- Τη διαχείριση των διευθύνσεων
- Την αντιστοίχιση 64-bit IEEE διευθύνσεων σε 16-bit διεύθυνση δικτύου και το ανάποδο
- Την υποστήριξη της ασφαλούς και αξιόπιστης μεταφοράς δεδομένων

Η εφαρμογή ZDO είναι υπεύθυνη για:

- Την διευκρίνιση του ρόλου της κάθε συσκευής στο δίκτυο
- Την ανακάλυψη συσκευών στο δίκτυο και τη σύζευξη τους με άλλες
- Την εφαρμογή των ρουτινών ασφαλείας

Ένα δίκτυο ZigBee αποτελείται από τρία είδη συσκευών, coordinator, router και end device. Το πρώτο υπάρχει μόνο μια φορά σε κάθε δίκτυο και είναι υπεύθυνο για την εκκίνηση του δικτύου, την επιλογή του καναλιού επικοινωνίας καθώς και του 16-bit αριθμού ταυτότητας του δικτύου. Πρόκειται για συσκευή που λειτουργεί αδιάκοπα, διότι είναι υπεύθυνη για τους περισσότερους μηχανισμούς ασφαλείας και μετακίνησης μηνυμάτων του δικτύου. Το δεύτερο

λειτουργεί ως μεσάζοντας, με την έννοια ότι προωθεί δεδομένα σε μακρινούς κόμβους, πέρα φυσικά από τις κανονικές λειτουργίες ενός κόμβου που είναι η είσοδος σε δίκτυο, αποστολή και λήψη δεδομένων. Παρομοίως πρέπει πάντα να λειτουργεί αδιάκοπα, αφού δίνει τη δυνατότητα σε άλλους κόμβους να εισέλθουν στο δίκτυο. Μπορούν να υπάρχουν περισσότεροι από ένας router κόμβοι σε κάθε δίκτυο. Το τρίτο είδος συσκευής είναι μια απλοποιημένη έκδοση του δεύτερου. Δρα ως πομπός-δέκτης δεδομένων αλλά δεν μπορεί να προωθήσει δεδομένα, παρά μόνο στον γειτονικό του router ή coordinator κόμβο. Εισέρχεται σε δίκτυο μόνο μέσω κάποιου από τους παραπάνω τύπους συσκευών, και μπορεί να τεθεί σε καταστάσεις χαμηλής κατανάλωσης.

3.1 ZigBee και οικιακός αυτοματισμός

Τα τελευταία χρόνια όλο και περισσότερες εταιρείες εστιάζουν σε εφαρμογές που σκοπό έχουν έναν ποιοτικότερο τρόπο ζωής στο σπίτι. Παραδείγματα τέτοια περιλαμβάνουν από τηλεχειριζόμενα, μέσω εφαρμογής κινητού, κλιματιστικά και οικιακές συσκευές μέχρι και εφαρμογές για τον καθολικό έλεγχο των συστημάτων ασφαλείας ενός σπιτιού. Οι συσκευές με το πρωτόκολλο ZigBee παρέχουν στον χρήστη την δυνατότητα μιας φθηνής λύσης για ολοκληρωτικό έλεγχο εκείνων, καθώς και των λειτουργιών του σπιτιού του. Η κεντρική ιδέα περιλαμβάνει μια εφαρμογή που δρα ως κεντρικό χειριστήριο του σπιτιού, και τα ελεγχόμενα αντικείμενα που δημιουργούν μεταξύ τους ένα mesh δίκτυο. Το ZigBee μη εσκεμμένα είναι πλέον συνυφασμένο με τον οικιακό αυτοματισμό από το γενικό καταναλωτικό κοινό διότι η τεχνολογία του είναι εύκολα προσβάσιμη και στους μη έχοντες τεχνολογικές γνώσεις, χωρίς αυτό να σημαίνει ότι οι δυνατότητες του σταματούν εκεί.

3.2 ZigBee Security

Το ZigBee διαθέτει μια πληθώρα τρόπων επισφράγισης της ασφάλειας των δικτύων του. Στη συνέχεια παρουσιάζονται μερικά βασικά χαρακτηριστικά ασφαλείας. Χρησιμοποιεί το Advanced Encryption Standard (AES) με το οποίο επιτυγχάνεται ή κρυπτογράφηση και η αποκρυπτογράφηση των αποσταλμένων μηνυμάτων. Με το AES κάθε αλγόριθμος κρυπτογράφησης σχετίζεται με ένα κλειδί (key). Ο αλγόριθμος είναι γνωστός για όλο το δίκτυο,

απλά κάθε φορά αλλάζει το χρησιμοποιούμενο κλειδί. Ένα κλειδί είναι δυαδικός αριθμός, με τον αριθμό των bits του να καθορίζει το πόσο ισχυρό είναι. Το ZigBee υποστηρίζει κλειδιά των 128 bits, πράγμα που σημαίνει πως, εάν μια ξένη συσκευή προσπαθούσε να βρει τον σωστό συνδυασμό για να αποκρυπτογραφήσει το μήνυμα θα έπρεπε να δοκιμάσει έως και 2^{128} αριθμούς, που είναι υπολογιστικά αδύνατο. Ο αλγόριθμος AES περιλαμβάνει μια σειρά βημάτων που χρησιμοποιούν το εκάστοτε κλειδί για να «ανακατέψουν» και «μπερδέψουν» τα περιεχόμενα ενός block δεδομένων των 128 bits. Τα βήματα αυτά έχουν τη δυνατότητα να πραγματοποιηθούν προς τα πίσω, έτσι ώστε η συσκευή-λήπτης να μπορέσει να αποκρυπτογραφήσει τα μηνύματα. Υποστηρίζεται, επίσης, ένας τρόπος ελέγχου αυθεντικότητας των μηνυμάτων με το Message Integrity Code (MIC). Το MIC είναι ένας κωδικός που συνοδεύει το μήνυμα κατά τη μετάδοση. Φυσικά ο τρόπος δημιουργίας του είναι γνωστός από κάθε εγκεκριμένη στο δίκτυο συσκευή. Έτσι, όταν κατά τη λήψη του μηνύματος ο λήπτης ακολουθήσει την ίδια μεθοδολογία εύρεσης του MIC και προκύψει το ίδιο αποτέλεσμα συμπεραίνει ότι το μήνυμα είναι αυθεντικό.

Συνοπτική περιγραφή των παροχών ασφαλείας του ZigBee:

- Δυνατότητα για κρυπτογράφηση των δεδομένων
- Έλεγχος αυθεντικότητας/συμβατότητας δεδομένων και συσκευών
- Προστασία κατά των διπλών πακέτων
- Link key, μοιράζεται σε μόνο δύο συσκευές και χρησιμοποιείται στις μεταξύ τους μεταδόσεις δεδομένων
- Network key, μοιράζεται σε όλο το δίκτυο και χρησιμοποιείται όταν αναμεταδίδεται ένα μήνυμα
- Master key, χρησιμοποιείται για να δώσει το link key σε δύο συσκευές
- Key-transport key, χρησιμοποιείται για να σιγουρέψει την μετάδοση οποιοδήποτε κλειδιού (εκτός του master key) στον προορισμό του
- Key-load key, χρησιμοποιείται για να σιγουρέψει την μετάδοση ενός master key

Σύμφωνα με τα παραπάνω το ZigBee θεωρητικά έχει τις υποδομές για να στηρίξει την ασφάλεια των δικτύων του. Απ’ ότι φαίνεται, όμως, στη πράξη δεν ισχύει κάτι τέτοιο. Όπως είναι γνωστό, η πιο διαδεδομένη χρήση του ZigBee είναι στον οικιακό αυτοματισμό. Μέχρι

προηγουμένως ο οικιακός αυτοματισμός περιλάμβανε κυρίως ελεγχόμενο φωτισμό και θερμοκρασία χώρου, τα τελευταία χρόνια, όμως, χρησιμοποιείται και για το κλείδωμα πορτών ασφαλείας, κλείσιμο και άνοιγμα ηλεκτρικών παραθυρόφυλλων κ.α., ακόμα και σε συνδυασμό με τα συστήματα συναγερμού. Οπότε πλέον υπάρχει το ερώτημα του κατά πόσο μπορεί να βασιστεί η ασφάλεια ενός σπιτιού στις αντίστοιχες συσκευές ZigBee.

Η ασφάλεια ενός ZigBee δικτύου βασίζεται πάνω στην ανταλλαγή κλειδιών ασφαλείας. Πειράματα και δοκιμές πάνω στις πιο ευρεία χρησιμοποιούμενες συσκευές ZigBee δείχνουν ότι πρόκειται για συσκευές κατασκευασμένες με σκοπό το γρήγορο setup και την εύκολη συνεργασία τους με άλλες ZigBee συσκευές άλλου καθήκοντος (και πιθανώς και άλλης εταιρείας) χωρίς να προσφέρουν επιλογές διαμόρφωσης για την ασφάλεια. Ακόμα και αν το χρονικό πλαίσιο στο οποίο ένας εξωτερικός παράγοντας μπορεί να υποκλέψει το network key είναι πολύ περιορισμένο, δεν είναι αδύνατο να το καταφέρει. Η επικοινωνία μεταξύ ZigBee συσκευών μπορεί εύκολα να σταματήσει με την εκπομπή θορύβων στο κανάλι επικοινωνίας (jamming). Ένας μη υποπτευόμενος χρήστης δεν καταλαβαίνει ότι πρόκειται για προσπάθεια εισχώρησης και έτσι θα προσπαθήσει να πραγματοποιήσει το re-pairing των συσκευών, ουσιαστικά βοηθώντας τον εισβολέα να κάνει sniffing του network key. Αυτό έχει ως αποτέλεσμα ο εισβολέας να έχει πλέον τη δυνατότητα ελέγχου ολόκληρου του ZigBee δικτύου, αφού αυτό βασίζεται εξ ολοκλήρου στη μυστικότητα του network key.

Συμπερασματικά, η τεχνολογία ZigBee εκ πρώτης όψεως δίνει την εντύπωση ότι πρόκειται για ένα πρωτόκολλο επικοινωνίας με επισφραγισμένη ασφάλεια, κάτι που δεν ισχύει. Η πρωτοποριακή του ευελιξία όσον αφορά στις επιλογές μορφοποίησης ενός δικτύου επισκιάζεται από το γεγονός ότι η ασφάλεια εξαρτάται από ένα επιρρεπές σε επιθέσεις σύστημα κλειδιών. Αυτό, σε συνδυασμό με τους προαναφερθέντες περιορισμούς του IEEE 802.15.4 καθιστούν το ZigBee μια εύκολη και φθηνή λύση με το κόστος της πιθανής αναξιοπιστίας.

Κεφάλαιο 4: Το πρωτόκολλο Smartmesh IP

Το πρωτόκολλο Smartmesh IP είναι πόνημα της Dust Networks, η οποία πλέον αποτελεί παρακλάδι της Analog Devices. Ένα Smartmesh IP δίκτυο αποτελείται από ένα αυτοδημιούργητο multi-hop πλέγμα κόμβων (Smartmesh IP motes) και έναν network manager. Τα motes είναι ικανά να συλλέξουν και να αναμεταδώσουν δεδομένα, το δε network manager ελέγχει τη κατάσταση και την ασφάλεια του δικτύου. Υπάρχουν δύο είδη manager, ο Embedded manager και ο VManager, των οποίων τα χαρακτηριστικά θα παρουσιαστούν παρακάτω. Ένα δίκτυο με Embedded manager υποστηρίζει μέχρι 32 κόμβους ενώ ένα δίκτυο με VManager χιλιάδες κόμβους, με τη χρήση Access Point (AP) κόμβων. Στην πραγματικότητα, ο Embedded manager λειτουργεί και ως Access Point κόμβος ενώ παράλληλα εκτελεί και τα καθήκοντα του συντονιστή, εξαιτίας αυτού έχει τον περιορισμό στους 32 κόμβους στο δίκτυο που επιτηρεί. Από την άλλη, αν κάθε Access Point κόμβος μπορεί να υποστηρίξει μέχρι 32 κόμβους και ο VManager υποστηρίζει πάρα πολλούς Access Point κόμβους, το αποτέλεσμα είναι ένα δίκτυο μεταβλητής κατά το επιθυμητό εμβέλειας. Μερικά από τα ατού της συγκεκριμένης σειράς προϊόντων της Analog είναι η δυνατότητα τους να καταναλώνουν ελάχιστο ρεύμα κατά τη λειτουργία τους, η απλή και εύχρηστη δημιουργία και αυτοσυντήρηση ενός δικτύου, καθώς και η πλήρης αξιοποίηση των δυνατοτήτων του TSCH και BLINK που προσφέρεται από το IEEE 802.15.4e .

4.1 Η δημιουργία ενός δικτύου Smartmesh IP

Ένα δίκτυο αρχίζει να διαμορφώνεται όταν ο Network Manager ανακοινώνει στο/α access point mote(s) την αποστολή πακέτων-advertisements (802.11.4e Beacon frames, περιέχουν πληροφορίες συγχρονισμού) που σκοπό έχουν να επιτρέψουν σε μια συσκευή να συγχρονιστεί με το δίκτυο και να εισέλθει σε αυτό. Αυτό το πακέτο είναι τμήμα της «χειραψίας ασφαλείας» (security handshake) που θεμελιώνει την επικοινωνία μεταξύ του manager ή της εφαρμογής με το mote. Όταν τα motes μπουν στο δίκτυο, διατηρούν με ακρίβεια τον συγχρονισμό τους δια μέσω μηνυμάτων time correction που αποστέλλουν στις γειτονικές συσκευές. Μέσω της «διαδικασίας ανακάλυψης» (discovery process), το δίκτυο συνεχώς ανακαλύπτει νέους τρόπους διασύνδεσης των motes όσο οι συνθήκες αλλάζουν. Επιπλέον, κάθε κόμβος στο δίκτυο καταγράφει τα

στατιστικά του, τα οποία μεταξύ άλλων συμπεριλαμβάνουν τη ποιότητα των δοκιμασμένων paths μεταξύ κόμβων και λίστες με τα ενδεχόμενα καλύτερα paths. Αυτά τα στατιστικά (health reports) στέλνονται από κάθε κόμβο στον manager ανά τακτά χρονικά διαστήματα. Ο manager χρησιμοποιεί αυτή την πληροφορία για να βελτιστοποιεί συνέχεια το δίκτυο και να κρατάει το ποσοστό επιτυχούς αποστολής δεδομένων πάνω από 99.999% ακόμα και σε αντίξοες συνθήκες.

Για να εισέλθει ένα mote στο δίκτυο, πρέπει πρώτα να συγχρονιστεί με τις υπόλοιπες συσκευές που περιλαμβάνει το δίκτυο. Αυτό επιτυγχάνεται με το να «ακούσει» το mote ένα advertisement από ένα AP mote ή από ένα άλλο mote που βρίσκεται ήδη στο δίκτυο. Εκτός από τον συγχρονισμό μιας συσκευής, ένα advertisement αναφέρει και το πότε η συσκευή μπορεί να στείλει request για να μπει στο δίκτυο, καθώς και το πότε να περιμένει την απάντηση. Αυτό επιφέρει προσωρινά shared links στο mote τα οποία θα χρησιμοποιεί μέχρι να λάβει τα δικά του dedicated links από τον manager. Με τις αρχικές ρυθμίσεις, ένα AP στέλνει advertisement περίπου κάθε 500ms. Τα πρώτα motes εισέρχονται στο δίκτυο μετά από περίπου 188s με join duty cycle = 5%. Ο χρόνος αυτός μπορεί να μειωθεί αν αυξηθεί και το join duty cycle, κάτι το οποίο επιβαρύνει την κατανάλωση ρεύματος του mote κατά τη διαδικασία του search.

Η δημιουργία ενός δικτύου έχει χαρακτήρα αλυσιδωτής αντίδρασης. Όταν το AP mote ξεκινήσει να στέλνει advertisements τα υπόλοιπα motes τα «ακούν» και ως εκ τούτου εισέρχονται στο δίκτυο και έπειτα αρχίζουν με τη σειρά τους να στέλνουν advertisements. Έτσι, ακόμα και τα απομακρυσμένα motes από το AP μπορούν να εισέλθουν με τη βοήθεια των advertisements των γειτονικών τους κόμβων.

4.2 Ταυτότητα ενός κόμβου

Το μέγεθος των πακέτων που αποστέλλονται κάθε φορά είναι σημαντικό για τις εφαρμογές του εκάστοτε χρήστη του Smartmesh IP. Για αυτό το λόγο, κάθε φορά που ένα mote εισέρχεται στο δίκτυο ο manager το «βαφτίζει» με μια κωδική ονομασία μεγέθους 2 Byte. Το δίκτυο χρησιμοποιεί αυτή την ονομασία (αντί της 8 Byte MAC διεύθυνσης του κόμβου) κάθε φορά που το συγκεκριμένο mote πρόκειται να αλληλεπιδράσει με κάποια άλλη συσκευή στο δίκτυο και έτσι εξοικονομείται χώρος και ενεργειακοί πόροι. Αυτή η κωδική ονομασία είναι σε ισχύ για όσο το mote παραμένει στο δίκτυο. Στη περίπτωση που αυτό αποσυνδεθεί και επανασυνδεθεί, η κωδική

του ονομασία αλλάζει. Αυτό το χαρακτηριστικό είναι ιδιαίτερα βολικό για τον χρήστη που διαβάζει τα στατιστικά ενός δικτύου, παρόλα αυτά στην σχεδίαση εφαρμογών για το Smartmesh IP πρέπει πάντα για ευνόητους λόγους να χρησιμοποιείται μόνο η διεύθυνση MAC για την επίκληση σε κάποιον κόμβο.

4.3 Εύρος ζώνης και καθυστερήσεις

Ο καθοριστικός παράγοντας για το συνολικό upstream bandwidth (εύρος ζώνης) ενός Smartmesh IP δικτύου είναι κατά κανόνα ο αριθμός των πακέτων που μπορούν να περάσουν ανά δευτερόλεπτο από τα AP motes. Για παράδειγμα, στην περίπτωση που χρησιμοποιείται ο Embedded manager, το μέγιστο όριο διακίνησης δεδομένων είναι 24 πακέτα (μεγέθους έως και 90 Byte) ανά δευτερόλεπτο (χωρίς εξωτερική SRAM) ή 36 πακέτα ανά δευτερόλεπτο (με εξωτερική SRAM) ενώ για τον VManager κάθε AP mote προσφέρει μέγιστο όριο διακίνησης δεδομένων 40 πακέτα ανά δευτερόλεπτο. Έτσι, σε ένα υποθετικό δίκτυο με VManager που αποτελείται από 4 AP motes και κόμβους, το όριο διακίνησης δεδομένων είναι 200 πακέτα ανά δευτερόλεπτο και μπορεί να διαμοιραστεί κατά βούληση στους κόμβους του δικτύου. Στη περίπτωση που το όριο αυτό αποπειραθεί να ξεπεραστεί, ο manager απορρίπτει περαιτέρω upstream αποστολές δεδομένων. Η κατανομή του εύρους ζώνης στα motes μπορεί να τροποποιηθεί και με την αλλαγή των σχετικών παραμέτρων μέσω του περιβάλλοντος διεπαφής χρήστη-συστήματος. Αναλυτικότερα, για τις περιπτώσεις που υπάρχουν στο δίκτυο πολλοί κόμβοι και απαιτείται η ελάχιστη κατανάλωση ισχύος προτείνεται ο ίσος καταμερισμός του εύρους ζώνης στους κόμβους. Για τις περιπτώσεις όπου κάθε mote ή κάποιες ομάδες motes στο δίκτυο χρειάζονται μεγαλύτερη ή μικρότερη μερίδα του εύρους ζώνης τότε ο χρήστης οφείλει να τροποποιήσει την σχετική με το bandwidth παράμετρο κάθε κόμβου ξεχωριστά. Όσον αφορά στις εφαρμογές που στηρίζονται στη γρήγορη upstream αποστολή δεδομένων (χωρίς καθυστερήσεις/latency), συνιστάται κάθε κόμβος να έχει τουλάχιστον δύο γειτονικούς κόμβους σε κοντινή εμβέλεια. Επίσης, για τους κόμβους του δικτύου όπου ο χρήστης επιθυμεί την όσο το δυνατόν γρηγορότερη upstream αποστολή δεδομένων μπορεί να αφιερώσει μια πολύ μεγάλη μερίδα του εύρους ζώνης. Έτσι, εξασφαλίζεται η συνδεσιμότητα του με άλλους κόμβους και ως εκ τούτου η ταχύτητα και η αξιοπιστία που ο χρήστης επιζητεί.

Η τεχνική που ακολουθεί ο manager για να εξασφαλίσει την σωστή upstream μετάδοση ενός κόμβου με πολλούς «απογόνους» (για παράδειγμα ενός κόμβου που απέχει ένα hop από τον manager) ονομάζεται τεχνική συνδέσεων καταρράκτη (cascading links). Κατά την τεχνική αυτή ο manager κοιτάει την ποσότητα των RX (receive) συνδέσεων ενός κόμβου, δηλαδή το πόσους απογόνους έχει, και ανάλογα συνδέει τον κόμβο με τον απαραίτητο αριθμό άλλων κόμβων. Αυτό συμβαίνει για να εξασφαλιστεί η μετάδοση όλων των δεδομένων που έχουν ανατεθεί στον κόμβο να διαδώσει. Οι επιπλέον συνδέσεις προσθέτουν αξιοπιστία.

4.4 Ασφάλεια δικτύου

Το Smartmesh IP διαθέτει ποικίλα μέσα επισφράγισης της ασφάλειας ενός δικτύου του. Τα αποστελλόμενα πακέτα ελέγχονται σε κάθε μεταπήδηση (hop) από τον manager. Πιο συγκεκριμένα, ελέγχεται ένα τρέχον κλειδί και ένας μετρητής χρόνου, έτσι ώστε ο manager να επιτρέπει μόνο στους κόμβους που έχουν εισέλθει στο δίκτυο και είναι συγχρονισμένοι με αυτό να στείλουν. Επίσης, το Smartmesh IP προσφέρει περαιτέρω σιγουριά με την χρήση session keys και κοινών μετρητών για να είναι σίγουρο ότι ένα πακέτο θα σταλεί στον σωστό παραλήπτη χωρίς να επαναληφθεί η μετάδοση, να αλλοιωθεί το μήνυμα ή να υποκλαπεί από τρίτους.

Κατά την είσοδο ενός κόμβου στο δίκτυο γίνεται ένα join request (δήλωση εισόδου) στον manager στέλνοντας ένα κρυφό join key (κλειδί εισόδου) το οποίο φυσικά ο manager γνωρίζει. Ο κόμβος κρυπτογραφεί το join request του με το join key και ο manager έπειτα του στέλνει ένα session key για την από άκρη σε άκρη (end-to-end) κρυπτογράφηση του μηνύματος. Αυτό μαζί με τα προαναφερθέντα, συγκροτεί την «χειραψία ασφαλείας». Το Smartmesh IP προσφέρει τρείς τρόπους όσον αφορά στο πώς ο manager θα αποκρυπτογραφήσει το join request. Επιγραμματικά αυτοί είναι η χρήση common key, η χρήση ACL (Access Control List ή Λίστα Ελέγχου Πρόσβασης) και ο συνδυασμός αυτών των δύο.

Το common key είναι ο λιγότερο «αυστηρός» τρόπος ασφαλούς σύνδεσης του κόμβου στο δίκτυο. Είναι διανεμημένο σε όλο το δίκτυο και έτσι κάθε κόμβος που θα κρυπτογραφήσει το join request του με αυτό γίνεται αποδεκτός από τον manager. Το πρόβλημα αυτού του τρόπου είναι ότι

οι manager κατά την αγορά τους διαθέτουν ένα συγκεκριμένο, εργοστασιακά τοποθετημένο common key πού ενδέχεται, αν δεν αλλαχτεί μετά την αγορά, να επιτρέψει σε τρίτους την υποκλοπή-ακρόαση αποστελλόμενων πακέτων.

Η ACL είναι μια λίστα που περιέχει όλες τις διευθύνσεις MAC των κόμβων που βρίσκονται ήδη συνδεδεμένοι ή πρόκειται να εισέλθουν στο δίκτυο, καθώς και ένα μοναδικό join key για καθέναν από αυτούς συνυφασμένο με την αντίστοιχη MAC. Όταν ο κόμβος επιχειρήσει να εισέλθει στο δίκτυο ο manager πρώτα κοιτάει την MAC του κόμβο, ύστερα αποκρυπτογραφεί το join request με το αντίστοιχο για τον κόμβο join key και, αν τα δύο αυτά βήματα πραγματοποιηθούν με επιτυχία, ο κόμβος εισέρχεται στο δίκτυο. Αυτός ο τρόπος είναι σαφώς πιο αποτελεσματικός από τον προηγούμενο αλλά απαιτεί από τον χρήστη την καταχώριση των κόμβων έναν-έναν στη λίστα. Βέβαια αυτό το αρνητικό μπορεί να αποφευχθεί αν ο χρήστης χρησιμοποιήσει ένα ίδιο common key για όλες τις διευθύνσεις MAC, βασιζόμενος ουσιαστικά στην ιδιωτικότητα των διευθύνσεων για την ασφάλεια του δικτύου στη περίπτωση που το common key μαθευόταν.

Ο τρίτος τρόπος περιλαμβάνει αρχικά την δημιουργία ενός δικτύου με τους κόμβους να εισέρχονται με ένα common key. Αφού γίνει αυτό συγκροτείται η ACL και κάθε κόμβος αποκτά το δικό του join key στη θέση του common key με την «εναέρια» (over-the-air) αλλαγή τους με την εντολή exchangeMoteJoinKey στο πρόγραμμα διεπαφής χρήστη-κόμβου. Κάθε επιπλέον κόμβος που επρόκειτο να εισέλθει στο δίκτυο πιο μετά θα πρέπει πρώτα να καταγράφεται στη λίστα. Αυτός ο τρόπος είναι επισφαλής κατά την εκκίνηση του αλλά παρέχει πολύ μεγαλύτερη ασφάλεια στη συνέχεια, δίνει επίσης τη δυνατότητα στον χρήστη να θέσει μοναδικό join key στους κόμβους με μεγαλύτερη ευκολία.

Όταν η είσοδος του κόμβου στο δίκτυο στεφθεί με επιτυχία παραλαμβάνει τέσσερα session keys για την κρυπτογράφηση των αποστελλόμενων πακέτων κατά τη λειτουργία του. Αυτά είναι:

- Κλειδί αποκλειστικό για τον συγκεκριμένο κόμβο για την κρυπτογράφηση πακέτων που προορίζονται για το δίκτυο.
- Κλειδί αποκλειστικό για τον συγκεκριμένο κόμβο για την κρυπτογράφηση πακέτων που προορίζονται για την εκάστοτε τρέχουσα εφαρμογή.

- Κλειδί κοινό για όλους τους κόμβους (broadcast key) για την κρυπτογράφηση πακέτων που προορίζονται για το δίκτυο.
- Κλειδί κοινό για όλους τους κόμβους για την κρυπτογράφηση πακέτων που προορίζονται για την εκάστοτε τρέχουσα εφαρμογή.

Με αυτά τα τέσσερα κλειδιά όλα τα πακέτα κρυπτογραφούνται από τον κόμβο-αποστολέα και μπορούν να αποκρυπτογραφηθούν μόνο από τον manager, χωρίς να μπορούν να αποκρυπτογραφηθούν από υποκλοπείς ή από άλλους κόμβους πού απλά τα προωθούν. Με την ίδια λογική οι εντολές του manager σε κάποιον κόμβο δεν γίνονται αντιληπτές από κανέναν άλλον. Για παράδειγμα, για την αποστολή μιας εντολής σε όλους τους κόμβους πρέπει να χρησιμοποιηθεί το κατάλληλο broadcast key.

4.5 Λειτουργία BLINK

Η λειτουργία Blink είναι μια πολύ χρήσιμη προσθήκη στη φαρέτρα των πλεονεκτημάτων του Smartmesh IP, το οποίο εκμεταλλεύεται στο έπακρο αυτή τη παροχή του επιπέδου MAC του 802.14.5e. Ένας κόμβος που βρίσκεται σε blink mode έχει τη δυνατότητα να στείλει πακέτα σε ένα Smartmesh IP δίκτυο χωρίς να είναι μέρος αυτού, με την προϋπόθεση να στέλνει πακέτα περιστασιακά. Αυτό έχει ως αποτέλεσμα ο κόμβος να χρησιμοποιεί πολύ μικρό μέσο ρεύμα και να καθιστά την λειτουργία αυτή ως ζωτικής σημασίας σε σενάρια που απαιτούν περισσότερους κόμβους από το δυνατό σε ένα δίκτυο, με όριο έως και περίπου 500.000 blink κόμβους στο ίδιο δίκτυο με VManager (1.200 σε δίκτυο με embedded manager, απαιτείται εξωτερική SRAM). Πέρα από την ευελιξία στο μέγεθος του δικτύου, με τη λειτουργία blink ο κόμβος αποστέλλει πιο γρήγορα τα πακέτα, αφού παραβλέπεται η διαδικασία της εισόδου στο δίκτυο. Παράλληλα η ασφάλεια των κόμβων σε blink mode ακολουθεί τις προδιαγραφές του υπόλοιπου δικτύου, πρόκειται δηλαδή για κόμβους που εντάσσονται κανονικά σε μια ACL. Πρέπει επίσης να σημειωθεί ότι οι συγκεκριμένοι κόμβοι δεν μπορούν να λάβουν δεδομένα παρά μόνο να στείλουν. Όλα αυτά τα χαρακτηριστικά συμβάλουν στην πολύ μικρή κατανάλωση ρεύματος που παρέχει η λειτουργία, της τάξεως των περίπου 2 μA. Στην περίπτωση που θεωρηθεί αναγκαίο-επιθυμητό, ένας blink κόμβος μπορεί ανά πάσα στιγμή να εισέλθει στο δίκτυο ως κανονικός mesh κόμβος.

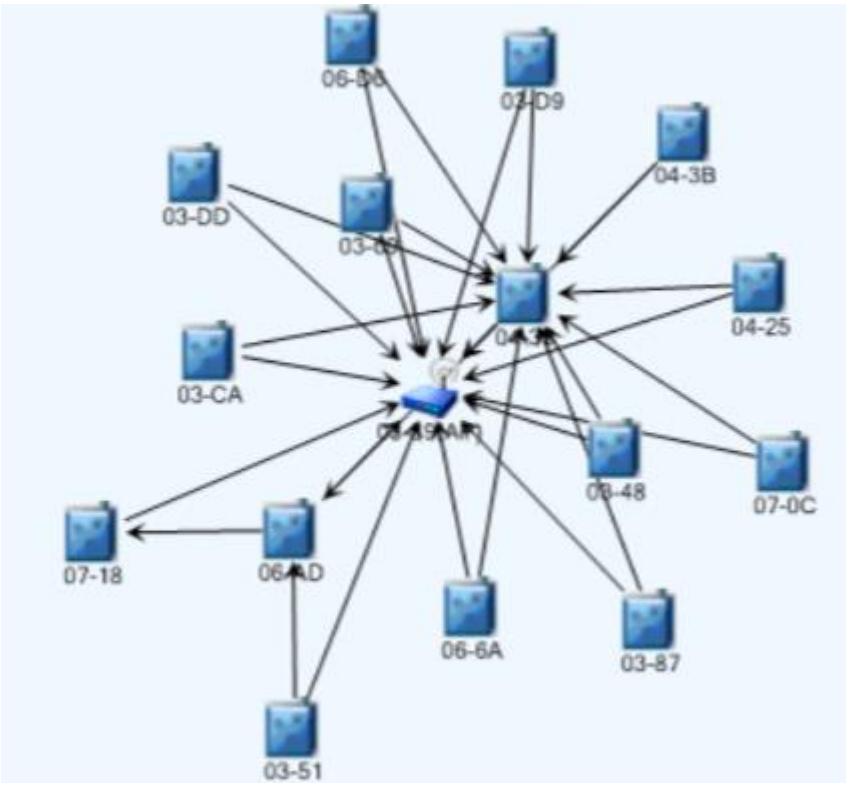
Η διαδικασία της έναρξης λειτουργίας του κόμβου σε κατάσταση blink έχει ως ακολούθως. Αντί να υπάρξει η χειραψία ασφαλείας μεταξύ κόμβου-manager (αφού πρώτα ο κόμβος λάβει εντολή blink), μόλις ο κόμβος «ακούσει» το advertisement δεν στέλνει πακέτο join αλλά κατευθείαν πακέτο blink και έτσι παρακάμπτεται η διαδικασία join. Οι τρεις φάσεις από τις οποίες περνάει ένας blink κόμβος αφού λάβει μια εντολή blink είναι τρείς, η αναζήτηση για ένα πακέτο advertisement, η αποστολή του blink πακέτου που είναι προγραμματισμένος να στείλει, και τέλος η λειτουργία του σε κατάσταση χαμηλής κατανάλωσης ενέργειας μέχρι να λάβει την επόμενη εντολή blink.

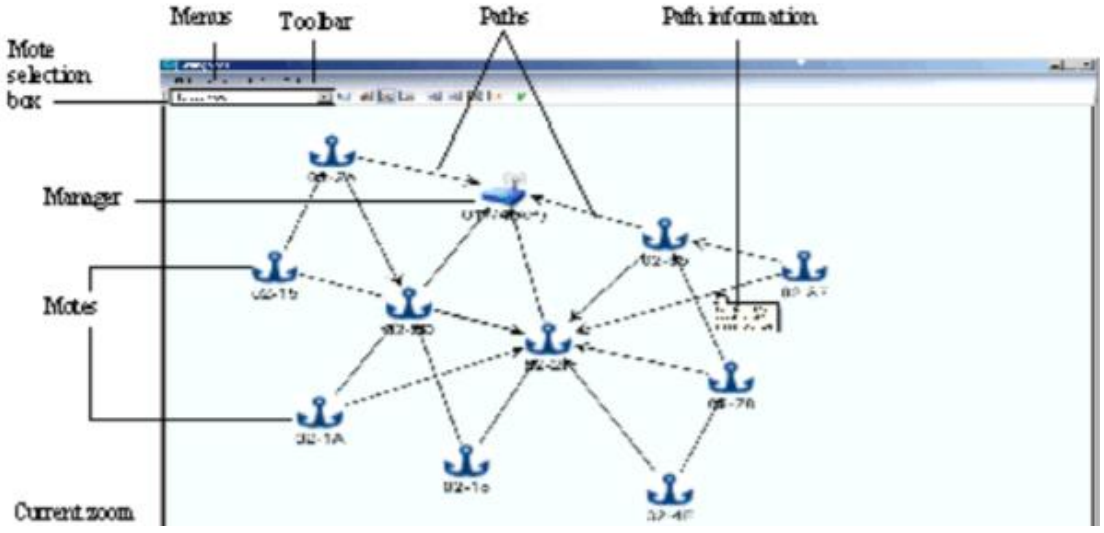
Τα αποστελλόμενα πακέτα από μη-blink κόμβους χρησιμοποιούν διαύλους επικοινωνίας αποκλειστικούς σε κάθε ζευγάρι κόμβων. Έτσι, η συμφόρηση του δικτύου δεν αποτελεί πρόβλημα. Στην περίπτωση, όμως, των blink κόμβων κάτι τέτοιο δεν ισχύει, διότι τα πακέτα τους στέλνονται στο κοινό δίαυλο επικοινωνίας που συνήθως χρησιμοποιείται για την αποστολή join requests. Επιπροσθέτως, τα blink motes καταναλώνουν το μεγαλύτερο μέρος του μέσου ρεύματος κατά τη διάρκεια του search, όταν δηλαδή περιμένουν να «ακούσουν» ένα advertisement. Είναι επομένως προτιμότερο να είναι προγραμματισμένα να στέλνουν τα πακέτα τους συγχρονισμένα για να μειωθεί η καταναλισκόμενη ενέργεια. Συμπερασματικά, αν ο πληθυσμός των blink motes είναι μεγάλος θα πρέπει να ομαδοποιηθεί η διαδικασία του search ώστε να αποφευχθεί η συμφόρηση στο δίκτυο.

4.6 Stargazer Graphical User Interface

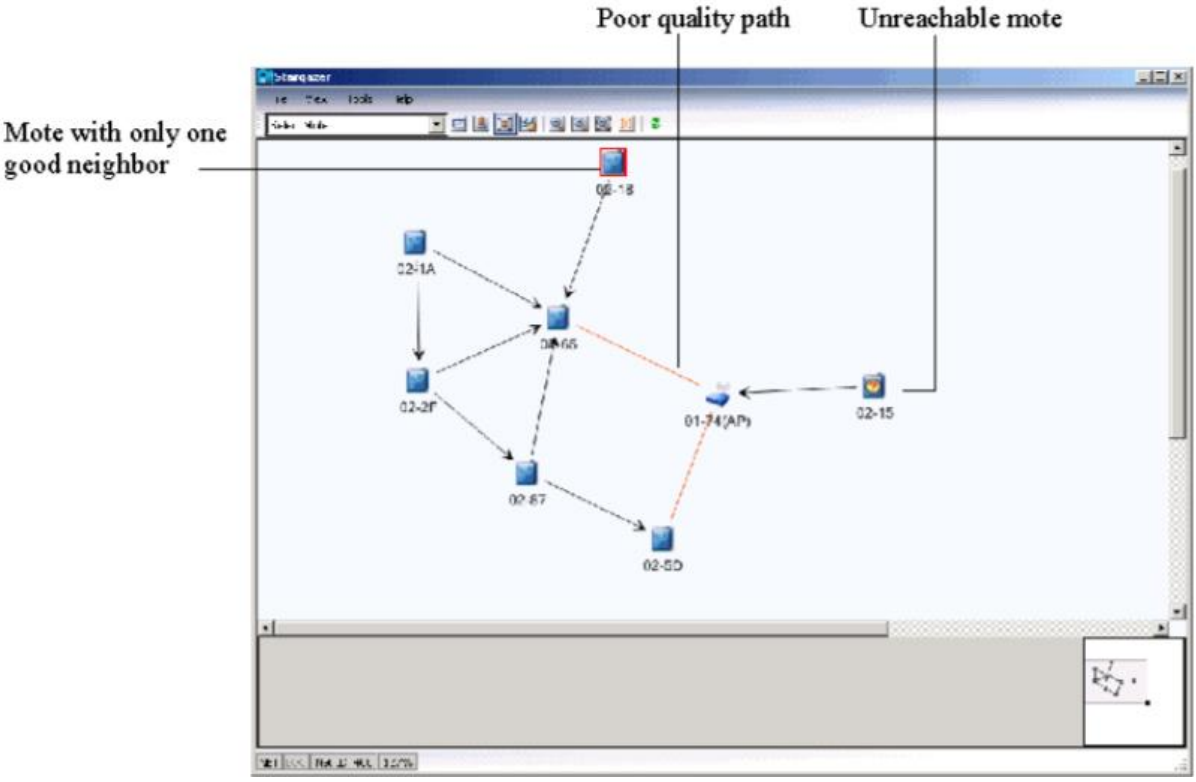
Μαζί με τα απαραίτητα για την δημιουργία ενός δικτύου δίνεται στον χρήστη και ένα πρόγραμμα, το Stargazer. Το Stargazer είναι μια εφαρμογή που απεικονίζει γραφικά την τοπολογία ενός δικτύου Smartmesh IP. Η απεικόνιση αυτή είναι δυναμική, δηλαδή ακόμα και ενώ το δίκτυο βρίσκεται σε λειτουργία, οι αλλαγές στις αποστάσεις μεταξύ των κόμβων αλλάζουν ώστε να δείχνουν πάντα τις σωστές τιμές, με μια μικρή καθυστέρηση. Η εφαρμογή αυτή επίσης διαθέτει πίνακες για κάθε κόμβο που περιέχουν πληροφορίες όπως το πόσους γονεϊκούς κόμβους διαθέτει ο καθένας, τι απόσταση έχει από τον κοντινότερο κόμβο, τι ποιότητας είναι η σύνδεση μεταξύ δύο κόμβων και το σημαντικότερο, χρονική σήμανση για το πότε απεστάλη ή ελήφθη πακέτο από έναν

κόμβο. Παρακάτω παρουσιάζονται ενδεικτικές εικόνες σχετικά με το Stargazer, με την αμέσως επόμενη να απεικονίζει ένα δίκτυο πλέγματος με δεκαπέντε κόμβους.





Στην προηγούμενη εικόνα φαίνεται το περιβάλλον απεικόνισης της τοπολογίας δικτύου σε σχέση με τον χώρο. Δίνεται επίσης η δυνατότητα εισαγωγής εικόνας για το background της τοπολογίας, με ιδανικό σενάριο την τοποθέτηση της κάτοψης του χώρου που βρίσκεται το δίκτυο για μεγαλύτερη ακρίβεια. Το σύμβολο της άγκυρας χρησιμοποιείται προς ένδειξη του κόμβου, ενώ το σύμβολο με την κεραία χρησιμοποιείται προς ένδειξη του manager. Οι μεταξύ των κόμβων συνδέσεις φαίνονται με τα μαύρα βέλη, τα οποία αλλάζουν χρώμα σε πορτοκαλί σε περίπτωση αδύναμης σύνδεσης. Επίσης, το σύμβολο των κόμβων αποκτάει κόκκινο περίγραμμα στην περίπτωση που ο κόμβος έχει μόνο έναν «καλό γονέα» δηλαδή καλή σύνδεση με μόνο έναν άλλον κόμβο. Η ύπαρξη περισσότερων από ενός γειτονικών κόμβων είναι επιθυμητή για την σωστή και αδιάκοπη λειτουργία όλων των κόμβων. Όταν ένας κόμβος δεν βρίσκεται πια στην εμβέλεια ενός άλλου κόμβου τότε το σύμβολο του αλλάζει σε αγγλικό ερωτηματικό για την οπτική ενημέρωση του χρήστη. Τα σφάλματα αυτά φαίνονται στην επόμενη εικόνα.

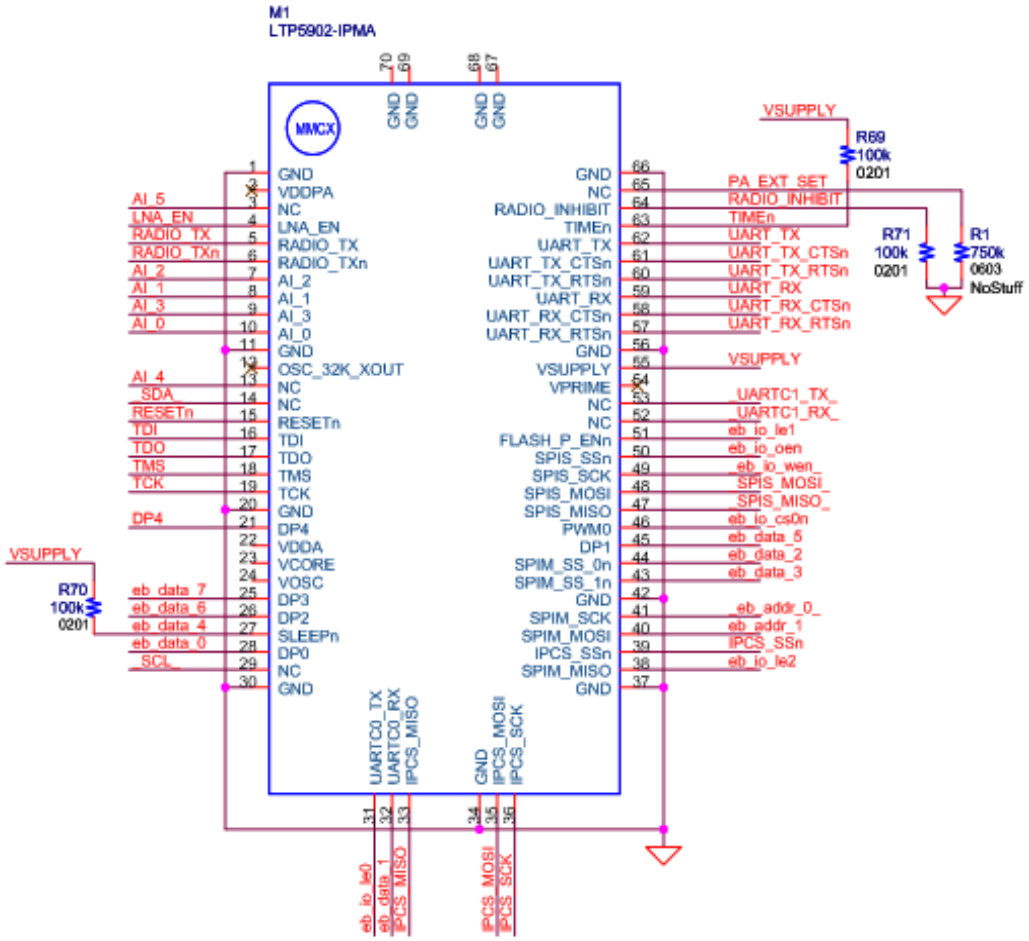


Ένας χρήστης του Smartmesh IP έχει επίσης τη δυνατότητα δημιουργίας της εφαρμογής που ανταποκρίνεται καλύτερα στις ανάγκες του χάρη στο Smartmesh SDK (Starter Development Kit), μια συλλογή από εφαρμογές Python που σκοπό έχουν την διευκόλυνση της εξοικείωσης του

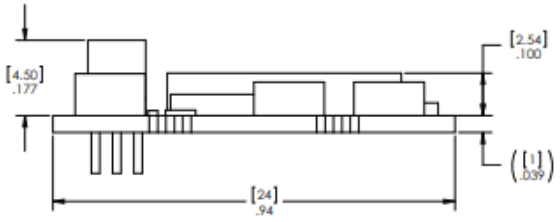
χρήστη με αυτό τον τομέα. Μαζί με αυτό το SDK δίνονται στον χρήστη δοκιμαστικές έτοιμες εφαρμογές με λειτουργίες όπως μια απλή αποστολή πακέτου blink, στοχεύοντας έτσι στην απλοποίηση του προγραμματισμού του API για όσους το χρησιμοποιούν ακόμα και πρώτη φορά.

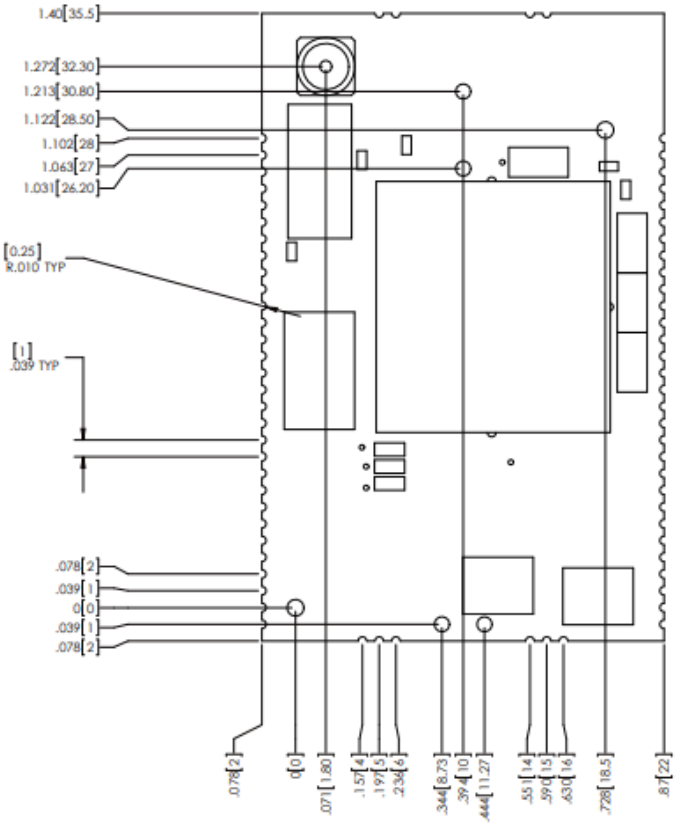
Κεφάλαιο 5: Σχεδιασμός και λειτουργία κόμβου Smartmesh IP

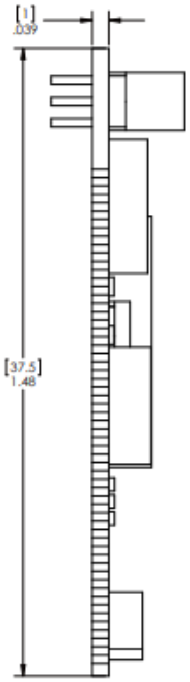
Ο κάθε κόμβος (mote) που λειτουργεί με το πρωτόκολλο Smartmesh IP, διαθέτει ενσωματωμένα την πλακέτα LTP5902, η οποία κατασκευάζεται σύμφωνα με το παρακάτω pin layout και ουσιαστικά αποτελεί το κύριο μέρος ενός κόμβου. Στον κόμβο επίσης βρίσκονται: η κεραία η οποία είναι αποσπώμενη, διακόπτες για λειτουργία και επαναφορά του κόμβου, LED για τη σήμανση της κάθε διαφορετικής κατάστασης του κόμβου καθώς και θύρες για την σύνδεση του κόμβου με άλλες συμβατές συσκευές ακόμα και να μην προέρχονται από την ίδια την Linear.

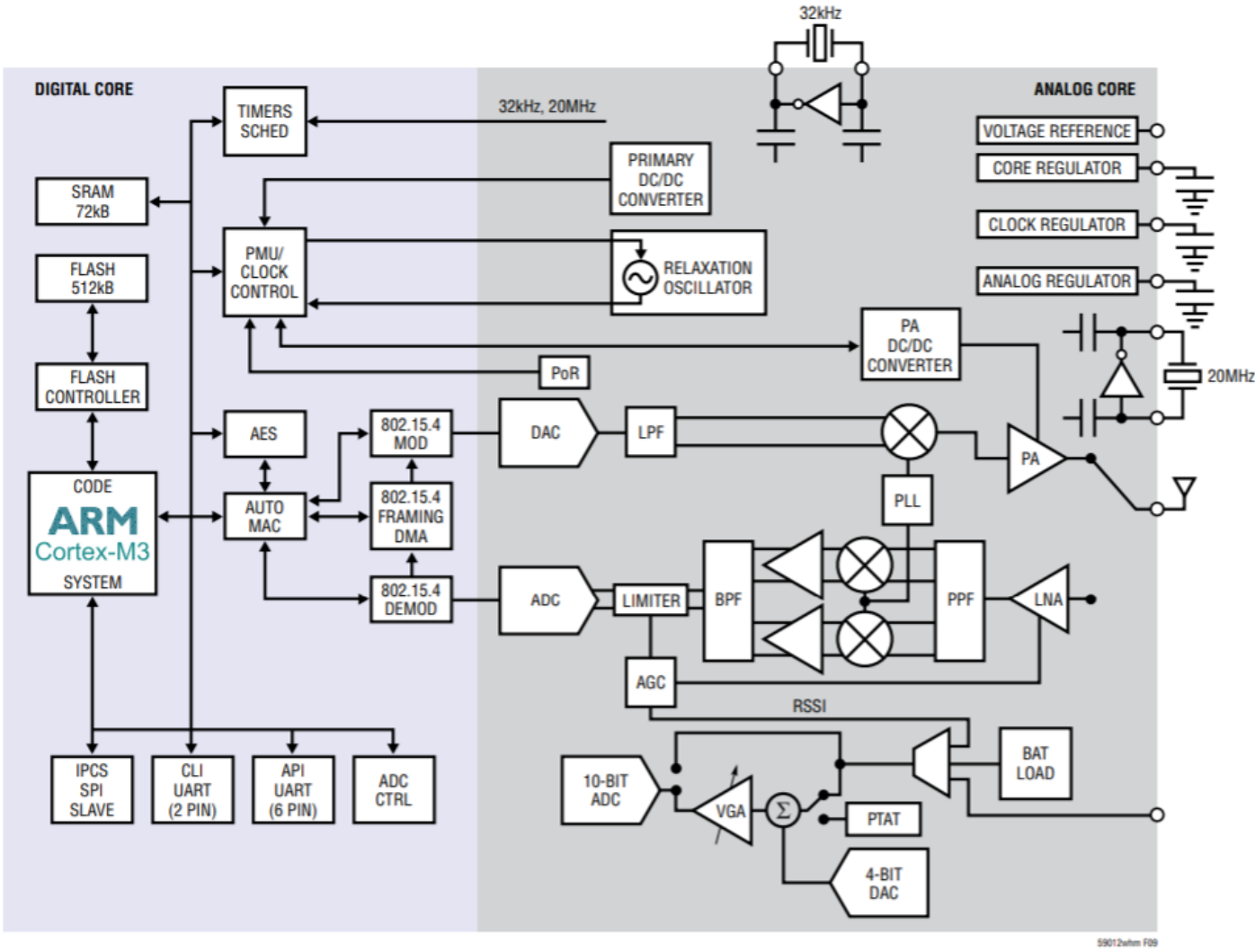


Ακολουθούν τα σχέδια κάτοψης, πρόσοψης και πλάγιας όψης του LTP5902, καθώς και το block diagram των εξαρτημάτων ενός κόμβου.


[4.50]
.177
[2.54]
.100
([1])
(.039)
[24]
.94


1.40[35.5]
1.272[32.30]
1.213[30.80]
1.122[28.50]
1.102[28]
1.063[27]
1.031[26.20]
[0.25]
R.010 TYP
[1]
.039 TYP
.078[2]
.039[1]
0[0]
.039[1]
.078[2]
.078[2]
0[0]
.071[1.80]
.157[4]
.197[5]
.236[6]
.344[8.73]
.394[10]
.444[11.27]
.551[14]
.591[15]
.630[16]
.728[18.5]
.87[22]


[1]
.039
[37.5]
1.48



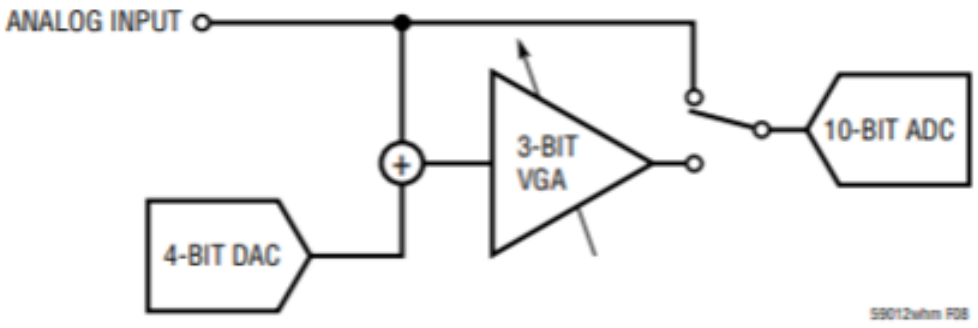
5.1 Pin functions

VSUPPLY: Παρέχει την απαραίτητη ισχύ στον κόμβο και στις εισόδους/εξόδους (I/O).

ANTENNA: Αποτελείται από είσοδο και έξοδο (δέκτη-πομπό) πολυπλεγμένου σήματος με αντίσταση 50Ω στο MMCX (το εξάρτημα στο οποίο τοποθετείται η κεραία).

AI_0 – 3: Αναλογικές είσοδοι πολυπλεγμένες στο σύστημα Analog Input Chain (αλυσίδα αναλογικών εισόδων) που χρησιμοποιείται στον κόμβο, με τιμές από 0 έως 1.8V. Το σύστημα αυτό διαθέτει πολλαπλασιαστή με μεταβλητές τιμές μέσω λογισμικού, έναν πολλαπλασιαστή μεταβλητού κέρδους, έναν ψηφιακό σε αναλογικό μετατροπέα τεσσάρων bit για την επιθυμητή

τροποποίηση του εύρους εισόδου και έναν αναλογικό σε ψηφιακό μετατροπέα δέκα bit. Το διάγραμμα του Analog Input Chain είναι το ακόλουθο.



RESETn: Κατά τη χρήση αυτού του pin επανεκκινείται ο επεξεργαστής του κόμβου (ARM Cortex M3) και χάνεται η σύνδεση στο δίκτυο.

RADIO_INHIBIT: Το συγκεκριμένο pin παρέχει τη δυνατότητα σε εξωτερικό παράγοντα-συσκευή να διακόψει προσωρινά την επικοινωνία του κόμβου.

TMS, TCK, TDI, TDO: Θύρα JTAG για λειτουργίες όπως το debugging του χρησιμοποιούμενου λογισμικού.

SLEEPn: Αχρησιμοποίητο pin κατά τη συγκεκριμένη έκδοση του κόμβου. Δεν υποστηρίζεται η εντολή μέσω λογισμικού για να τεθεί ο κόμβος σε sleep.

UART_RX, UART_RX_RTSn, UART_RX_CTSn, UART_TX, UART_TX_RTSn, UART_TX_CTSn: Χρησιμοποιούμενα από το API UART περιβάλλον διεπαφής.

TIMEn: Χρησιμοποιείται για την εύρεση του χρόνου δικτύου. Το timestamp του δικτύου προσκολλάται στην ακμή του σήματος TIMEn και παρέχει ένα πακέτο με την πληροφορία του χρονισμού μέσω της σειριακής θύρας API.

UARTC0_RX, UARTC0_TX: Παρέχουν τους απαραίτητους μηχανισμούς για την παρακολούθηση, τροποποίηση καθώς και έλεγχο του κόμβου κατά την λειτουργία του, με τη χρήση του CLI UART.

FLASH_P_ENn, IPCS_SSn, IPCS_SCK, IPCS_MISO, IPCS_SSn: Μέσω του διαύλου IPCS (In-circuit Programming Control System), παρέχεται η δυνατότητα στον χρήστη να προγραμματίζει την flash μνήμη του κόμβου.

5.2 Λειτουργία κόμβου

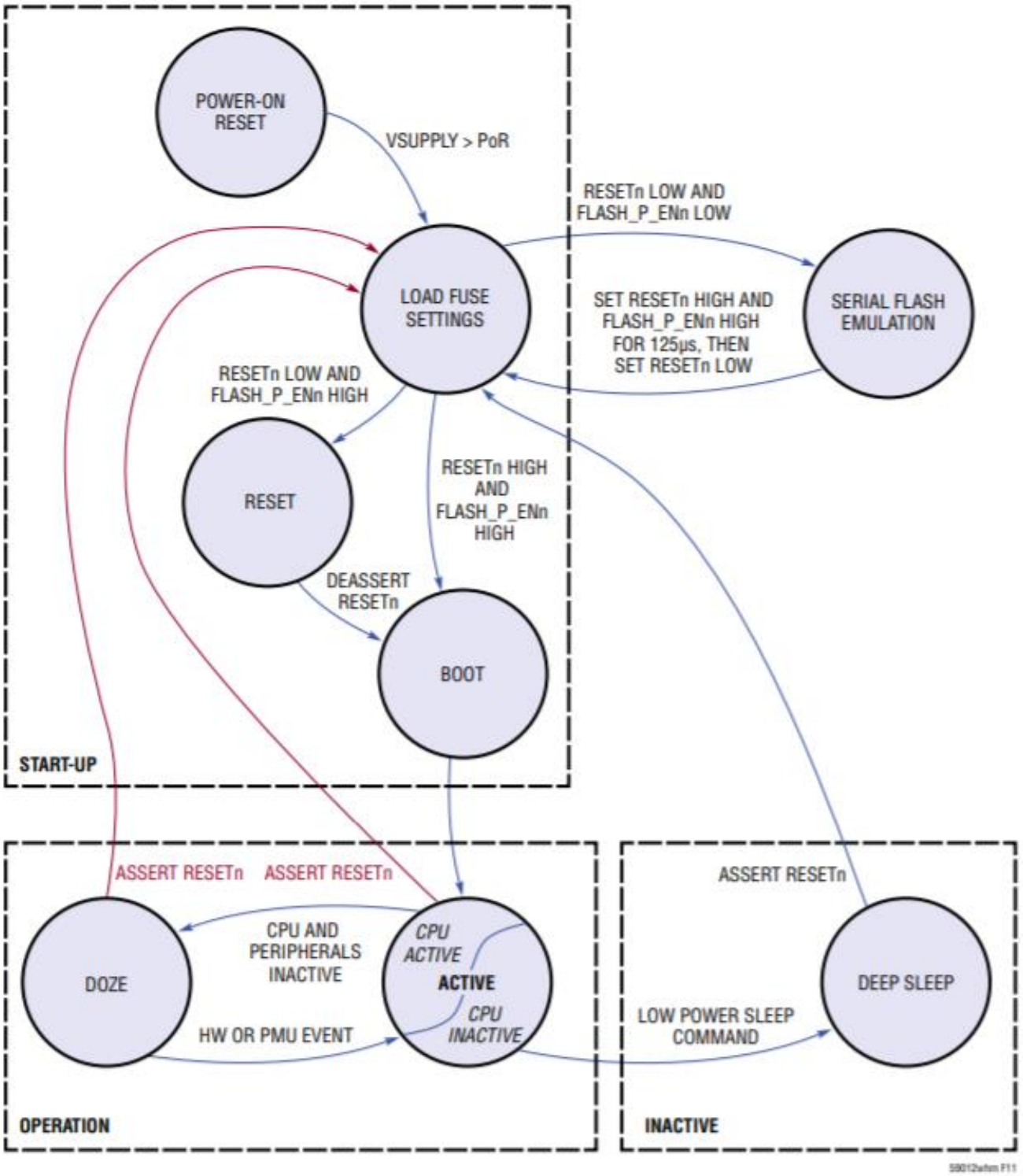
Η φιλοσοφία πίσω από τη μελέτη και την κατασκευή ενός κόμβου Smartmesh IP βασίζεται στην ανάγκη για μεγάλη αυτονομία και ιδεατή διαχείριση ενέργειας. Όπως φαίνεται στο παραπάνω block diagram, χρησιμοποιούνται δύο DC/DC μετατροπείς για την ελαχιστοποίηση της κατανάλωσης ενώ λειτουργεί κανονικά ο κόμβος, αλλά απενεργοποιούνται κατά πιθανή τοποθέτησή του σε κατάσταση χαμηλής κατανάλωσης έτσι ώστε να μην έχουν επίδραση στην τελευταία. Επίσης, παρέχονται πολλές δυνατότητες για διαφορετικού είδους τροφοδοσία, διότι το εύρος τάσεων λειτουργίας ενός κόμβου είναι αρκετά μεγάλο (υποστήριξη και για μπαταρίες λιθίου μακράς διαρκείας). Επιπροσθέτως, η ύπαρξη των αλγορίθμων χρονισμού του πρωτοκόλλου, καθώς και εξαρτημάτων χαμηλής κατανάλωσης με λειτουργίες χρονισμού δίνουν το πάνω χέρι στο πρωτόκολλο αφού επιτυγχάνει ακρίβεια στο «πότε» θα εκκινηθεί η διαδικασία radio listening, ελαχιστοποιώντας τον χρόνο που η συσκευή βρίσκεται σε αυτή την ενεργειοβόρα κατάσταση. Αυτή η διαδικασία έχει ως αποτέλεσμα την καλύτερη χρήση του δικτύου, αφού τα πακέτα μεταδίδονται πιο άμεσα, με την ελάχιστη καθυστέρηση.

Όπως προαναφέρθηκε, το Smartmesh IP δίκτυο διαθέτει τρόπους ώστε να είναι καθολικά συγχρονισμένο. Έτσι, η ακρίβεια των συμβάντων-επικοινωνιών στο κάθε δίκτυο καθορίζεται από αυτόν τον συγχρονισμό και κάθε τι που συμβαίνει έχει την «σφραγίδα» της χρονικής στιγμής που συνέβη, σύμφωνα με τον τοπικό χρόνο δικτύου. Όταν ζητηθεί μέσω API ο χρόνος δικτύου ή όταν δοθεί σήμα μέσω του pin TIMEn, ο κόμβος στέλνει σειριακά το πακέτο με τις ζητούμενες πληροφορίες. Στη δεύτερη περίπτωση του TIMEn υπάρχει μεγαλύτερη ακρίβεια διότι χρησιμοποιείται ειδικό hardware που παίρνει ως τιμή την ακμή του σήματος TIMEn, ενώ στην πρώτη περίπτωση μπορεί να υπάρξει μια μικρή απόκλιση μεταξύ πραγματικής τιμής και αποτελέσματος, εξαιτίας της διαδικασίας επεξεργασίας πακέτων μέσω API. Το κυρίως εξάρτημα του κόμβου που αναλαμβάνει τον χρονισμό του CPU, των υπόλοιπων συστημάτων μνήμης και περιφερειακών είναι ένας relaxation oscillator (ταλαντωτής χαλάρωσης-ανατροπής) ο οποίος είναι ρυθμισμένος στα 7.3728 MHz. Ο ταλαντωτής αυτός εκκινεί σε μόλις λίγα μικροσεκόντ, παρέχοντας έτσι ευελιξία κατά την αλλαγή της κατάστασης του κόμβου από κανονική λειτουργία σε λειτουργία χαμηλής κατανάλωσης.

Όσον αφορά στο κομμάτι της επικοινωνίας (κεραία), χρησιμοποιείται radio με συχνότητα 2.4 GHz (με βάση το IEEE 802.15.4e) και την χαμηλότερη δυνατή κατανάλωση. Επιπλέον, με την χρήση ενός Media Access Controller αφοσιωμένο στη λειτουργία του hardware, για την ακριβή διαδοχική λειτουργία (ανάλογα την εφαρμογή) των περιφερειακών και των εξαρτημάτων του κόμβου (συμπεριλαμβάνεται και η κεραία-πομπός/δέκτης) ελαχιστοποιείται η λειτουργία του CPU και επακολούθως περιορίζεται ακόμα περισσότερο η άσκοπη κατανάλωση ισχύος. Για παράδειγμα, ο Media Access Controller διασφαλίζει τον σωστό συγχρονισμό όλων των λειτουργιών που σχετίζονται με την αποστολή και λήψη δεδομένων μέσω κεραίας. Το γεγονός ότι αυτές οι διαδικασίες βρίσκονται στην δικαιοδοσία ενός μικροελεγκτή και όχι στα χέρια ενός λογισμικού, καθιστά διασφαλισμένη την εύρυθμη λειτουργία των ραδιοεπικοινωνιών.

Πέρα από την ασφάλεια που παρέχεται μέσω του πρωτοκόλλου Smartmesh IP σε ένα δίκτυο κόμβων, κάθε κόμβος είναι σχεδιασμένος ώστε να προστατεύεται και από φυσικές επιθέσεις, με ηλεκτρονικά κλειδωμένες τις RAM και flash memory. Με αυτόν τον τρόπο προστατεύονται τα security keys που διαθέτει ο κάθε κόμβος για να μπορεί να επικοινωνεί με το υπόλοιπο δίκτυο.

Τέλος, όσον αφορά στους διαφορετικούς τύπους λειτουργίας ενός κόμβου, αυτοί είναι δύο, ο active state (ενεργή κατάσταση) και ο doze state (κατάσταση ημι-καταστολής). Παρακάτω παρουσιάζεται ένα σχεδιάγραμμα της αλληλουχίας μεταξύ καταστάσεων και έπειτα μια περίληψη του τί συμβαίνει σε κάθε μια. Παρατίθενται επίσης πληροφορίες για την λειτουργία εκκίνησης ενός κόμβου καθώς και για την υπολειτουργία serial flash emulation.



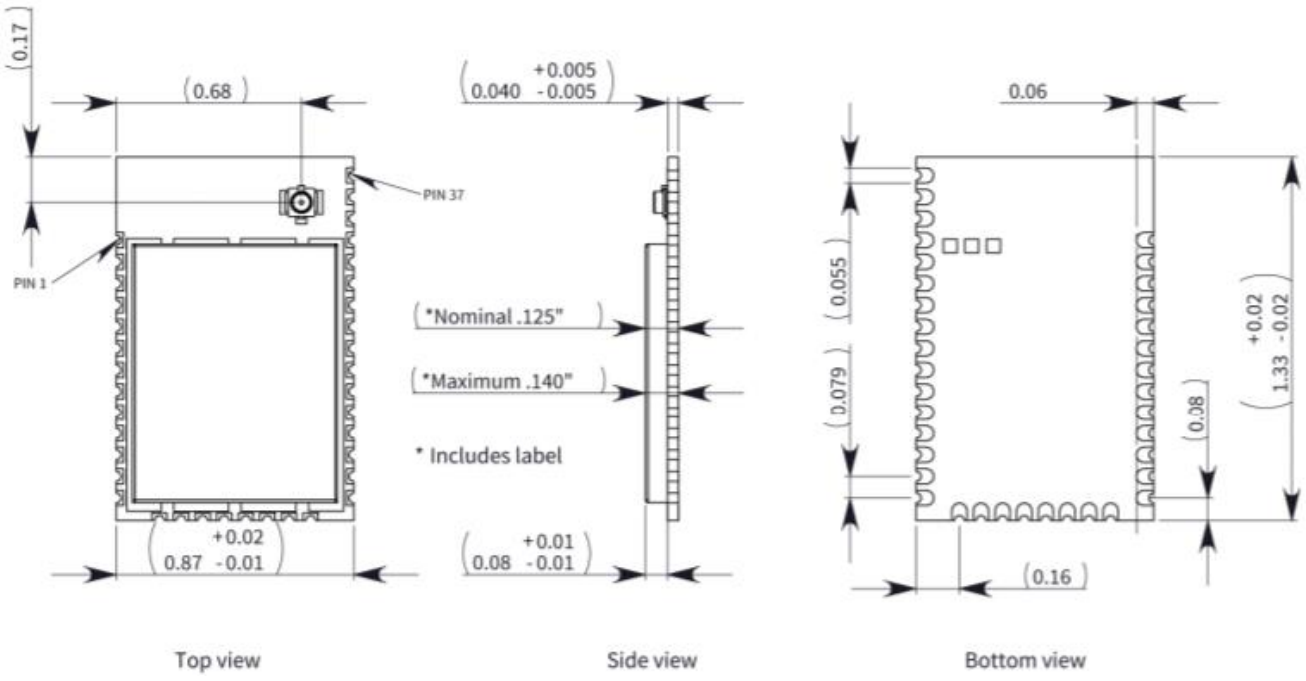
Κατά τη διάρκεια του active state ο ταλαντωτής χαλάρωσης και το CPU λειτουργούν ανάλογα με τα καθήκοντά τους και τα περιφερειακά συστήματα του κόμβου είναι έτοιμα προς χρήση. Στην περίπτωση που το CPU και τα περιφερειακά (όπως η κεραία) δεν χρησιμοποιούνται

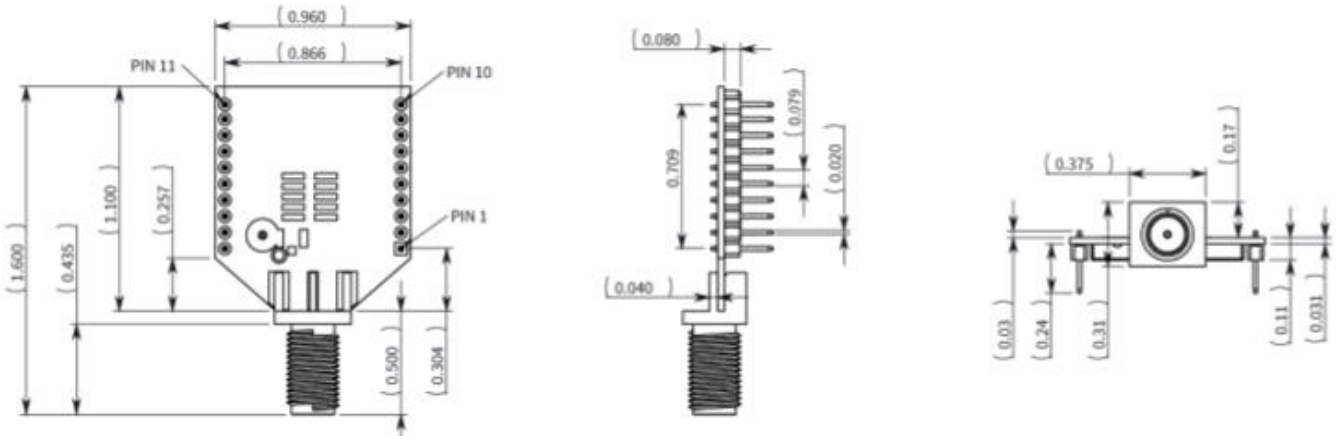
για ένα συγκεκριμένο χρονικό πλαίσιο, ο κόμβος τοποθετείται αυτόματα σε doze state. Σε αυτή την κατάσταση ο κόμβος καταναλώνει λιγότερο ρεύμα, παρόλα αυτά είναι προγραμματισμένος να ανιχνεύει τυχόντα σήματα στις θύρες του και στη συνέχεια να «ξυπνά» για να μπορέσει να αντεπεξέλθει άμεσα. Ένα τέτοιο παράδειγμα αποτελεί ένα σήμα TIMEn για την ζήτηση πληροφοριών χρόνου του δικτύου. Συμπερασματικά, ο ταλαντωτής χαλάρωσης και όλα τα σχετικά με τον χρονισμό εξαρτήματα του κόμβου είναι ενεργά κατά το doze state.

Σε ένα δίκτυο Smartmesh IP οι κόμβοι τείνουν να περνούν το μεγαλύτερο χρονικό διάστημα της λειτουργίας τους στη κατάσταση που καταναλώνουν τη λιγότερη ισχύ, δηλαδή το doze state. Σε ένα τέτοιο τυπικό παράδειγμα δικτύου οι κόμβοι αυτοί «ξυπνούν» από την κατάσταση doze για να επικοινωνήσουν με έναν άλλον κόμβο. Αυτή η διαδικασία θεωρείται ως «ατομική» με την έννοια ότι δεν μπορεί να χωριστεί σε περεταίρω μικρότερες διαδικασίες κατά τη διάρκεια της εκπόνησης μιας λειτουργίας του κόμβου, με χαρακτηριστικό παράδειγμα ατομικής λειτουργίας την αποστολή ενός πακέτου μέσω της κεραίας του κόμβου. Όταν σε ένα timeslot ένας κόμβος στείλει επιτυχώς ένα πακέτο, η διαδικασία της «ατομικής αποστολής» περιέχει τα βήματα της προετοιμασίας πριν την αποστολή, την αποστολή του πακέτου, την λήψη του μηνύματος επιβεβαίωσης και την μετέπειτα επεξεργασία του αποτελέσματος της όλης διαδικασίας. Ομοίως, όταν σε ένα timeslot ένας κόμβος λάβει επιτυχώς ένα πακέτο, η διαδικασία της «ατομικής λήψης» περιέχει τα βήματα της προετοιμασίας για το listening, το listening μέχρι την αρχή της μετάβασης του πακέτου, την λήψη του πακέτου, την αποστολή μηνύματος επιβεβαίωσης και την μετέπειτα επεξεργασία του αποτελέσματος της λήψης πακέτου. Για την εύρυθμη λειτουργία της επικοινωνίας, κάθε κόμβος στο δίκτυο διαθέτει αριθμό timeslots για κάθε πακέτο που πρόκειται να στείλει ή να προωθήσει, που ποικίλει ανάλογα με την προς τα πάνω επικοινωνία (upstream) του κάθε κόμβου. Αυτό το προνόμιο, σε συνδυασμό με την εναλλαγή συχνοτήτων (frequency-channel hopping) όπως παρουσιάστηκε σε προηγούμενο κεφάλαιο, παρέχει χρονική, χωρική και φασματική ευελιξία. Στον συνδυασμό αυτό οφείλεται το γεγονός ότι ένας κόμβος συνήθως διαθέτει τρία timeslots για κάθε ένα πακέτο προς αποστολή ή προώθηση και πολλές φορές μπορεί να καταλήγει να περιμένει για ένα μήνυμα (listening) χωρίς να υπάρχει κάτι για εκείνον. Αυτό ονομάζεται και Idle Listen, και συμβαίνει πιο πολλές φορές από ότι μια διαδικασία ατομικής αποστολής ή ατομικής λήψης

Κεφάλαιο 6: Σχεδιασμός και λειτουργία κόμβου ZigBee

Σε αυτό το κεφάλαιο παρουσιάζονται τα στοιχεία λειτουργίας ενός κόμβου που λειτουργεί με το πρωτόκολλο Zigbee. Πιο συγκεκριμένα, πρόκειται για τον κόμβο XBee S2C της εταιρείας Digi. Η εταιρεία παρέχει δύο εκδοχές του ίδιου κόμβου, την κανονική και την PRO, με την δεύτερη να διαθέτει λίγο πιο ενισχυμένες δυνατότητες σε σχέση με την πρώτη. Για παράδειγμα η κανονική έκδοση του κόμβου διαθέτει δυνατότητα αποστολής δεδομένων-εμβέλεια- 1200 μέτρα σε θεωρητικά ανεμπόδιστη απόσταση μεταξύ κόμβων, ενώ η έκδοση PRO υποστηρίζει απόσταση 3200 μέτρα στις ίδιες συνθήκες. Στο παρόν κεφάλαιο θα παρουσιαστούν οι ιδιότητες και οι δυνατότητες της κανονικής έκδοσης, διότι στόχος κυρίως είναι η σύγκριση κόμβων με δυνατότητες mesh δικτύωσης με την χαμηλότερη δυνατή κατανάλωση, κάτι στο οποίο η PRO έκδοση υστερεί. Παρακάτω παρουσιάζονται τα σχέδια του module, τόσο για την μορφή surface-mount όσο και για την μορφή through-hole.





(Οι παραπάνω όψεις για την μορφή through-hole περιλαμβάνουν και RPSMA συνδεσιμότητα)

Ο κόμβος για την λειτουργία του απαιτεί 2.1-3.6 V και παρομοίως 2.7-3.6 V για την PRO έκδοση. Το ρεύμα που καταναλώνεται κατά την διαδικασία της χρήσης της κεραίας για την μετάδοση δεδομένων είναι από 33 έως 45 mA (ανάλογα με το αν η συσκευή είναι προγραμματισμένη για ενισχυμένες λειτουργίες αποστολής και λήψης δεδομένων) ενώ το ρεύμα που καταναλώνεται ενώ βρίσκεται σε Idle mode ή ενώ λαμβάνει δεδομένα είναι από 28 έως 31 mA. Αυτό το εύρος ρεύματος σχεδόν δεκαπλασιάζεται σε έναν κόμβο PRO, για αυτό τον λόγο δεν αποτελεί κατάλληλη περίπτωση για σύγκριση με άλλες low-power λύσεις.

Πέρα, όμως, από τις παραπάνω εκδοχές του ίδιου μοντέλου η εταιρεία διαθέτει και μια προγραμματιζόμενη εκδοχή τους. Αυτοί οι κόμβοι είναι περαιτέρω εξοπλισμένοι με έναν δευτερεύοντα επεξεργαστή (NXP MC9S08QE32) με 32kB flash και 2kB RAM, και χρησιμοποιεί τα pin DIN, DOUT, RESET, CTS για να ελέγχεται μέσω του επιθυμητού κώδικα οποιαδήποτε ενέργεια σχετική με την αποστολή και λήψη δεδομένων. Διαθέτουν επίσης bootloader για τον εξ αποστάσεως (και μη) προγραμματισμό του επεξεργαστή.

Κάθε κόμβος σε ένα δίκτυο διαθέτει μια 64-bit και μια 16-bit διεύθυνση. Η πρώτη του αντιστοιχείται κατά την κατασκευή του και ονομάζεται αλλιώς και MAC address του κόμβου. Η δεύτερη διεύθυνση αποκτάται κατά την είσοδο του κόμβου σε ένα δίκτυο και είναι μοναδική επειδή δημιουργείται τυχαία. Η 16-bit διεύθυνση είναι η πιο σημαντική αφού αυτή χρησιμοποιείται κατά την αποστολή δεδομένων σε ένα δίκτυο ZigBee. Παρόλα αυτά λόγω της επιρρεπούς σε αλλαγή κατάσταση της πολλές φορές για την αποστολή δεδομένων συμπεριλαμβάνεται και η διεύθυνση MAC, για σιγουριά. Η 16-bit διεύθυνση πρέπει να αλλάξει στη περίπτωση που δύο

κόμβοι εσφαλμένα έχουν την ίδια. Μπορεί επίσης να αλλάξει στην περίπτωση που ένας κόμβος που έχει αποσυνδεθεί από ένα δίκτυο εισέλθει ξανά. Κάθε κόμβος διαθέτει έναν πίνακα διευθύνσεων στον οποίο αποθηκεύει τις 64-bit και 16-bit διευθύνσεις των κόμβων του δικτύου έτσι ώστε να είναι εύκολα προσπελάσιμες για την μετάδοση δεδομένων. Στην περίπτωση που ένας κόμβος δεν γνωρίζει την 16-bit διεύθυνση του προορισμού, προβαίνει σε μια διαδικασία εύρεσής του.

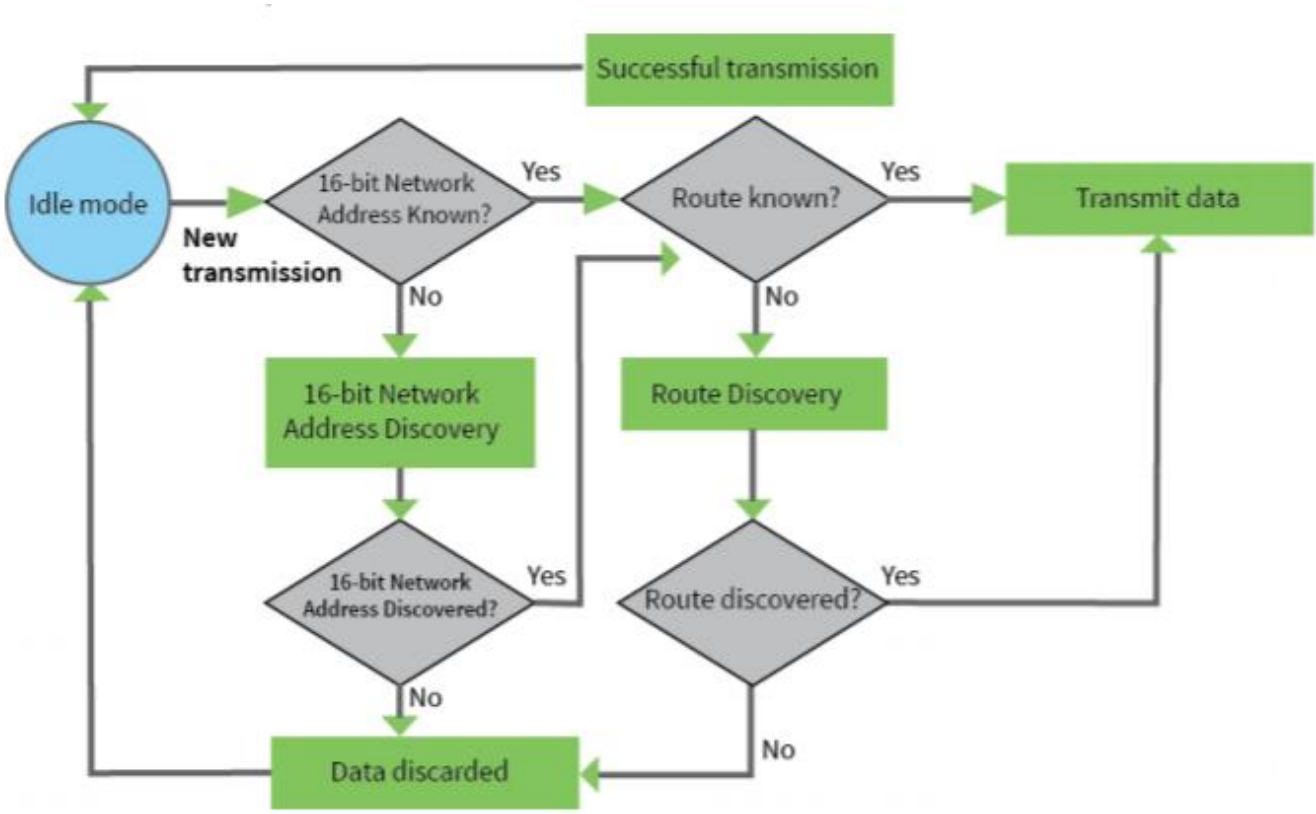
6.1 Λειτουργία κόμβου end device

Όπως έχει προαναφερθεί, το ZigBee βασίζεται στον από προηγουμένως διορισμό των ρόλων των συσκευών του στο δίκτυο, χωρίς αυτές κατά τη λειτουργία του να μπορούν να αλλάξουν ρόλο. Με αυτή την λογική εξετάζονται παρακάτω οι περιορισμοί και ιδιότητες των κόμβων που λειτουργούν ως end devices σε ένα ZigBee δίκτυο. Όταν ένας κόμβος που έχει σκοπό να λειτουργήσει ως end device εισέλθει επιτυχώς στο δίκτυο δημιουργεί μια σχέση parent-child με τη συσκευή που είναι υπεύθυνη για την «επιστράτευση» νέων κόμβων στο δίκτυο της (router ή coordinator). Όσο ο κόμβος λειτουργεί, στέλνει στον κόμβο-γονέα του μηνύματα με σκοπό να ανιχνεύσει αν υπάρχει μήνυμα για αυτόν. Τα μηνύματα αυτά ονομάζονται poll requests και αφού ο κόμβος-γονέας λάβει ένα, στέλνει πίσω ένα μήνυμα επιβεβαίωσης το οποίο περιέχει πληροφορία για το αν έπεται ή όχι μήνυμα με δεδομένα για το end device. Δίνεται η δυνατότητα να τίθεται ο κόμβος σε Idle mode ή Sleep mode όταν το πακέτο επιβεβαίωσης δείχνει ότι δεν υπάρχουν δεδομένα για να παραλάβει, επιτυγχάνοντας έτσι μείωση στην κατανάλωση ισχύος. Πολύ σημαντικό είναι το γεγονός ότι ένας κόμβος end device δεν μπορεί να στείλει δεδομένα σε κανέναν άλλον κόμβο παρά μόνο στον γονεϊκό του, ο οποίος μπορεί απλά να προωθήσει ένα πακέτο αν δεν προορίζεται για εκείνον. Από την άλλη, ο κάθε κόμβος που λειτουργεί ως γονέας των end devices διαθέτει τρόπο αποθήκευσης των δεδομένων όλων των end devices που διαχειρίζεται. Η λίστα στην οποία τοποθετούνται τα end devices δεν έχει άπειρη χωρητικότητα, έτσι αν ένα router mote δεν έχει άλλο χώρο, το end device θα πρέπει να συνδεθεί με άλλον γονέα. Τα router motes επίσης διαθέτουν buffer για να μπορούν να αποθηκεύουν προσωρινά δεδομένα. Αυτό είναι ιδιαίτερα χρήσιμο για παράδειγμα στην περίπτωση που πρέπει να στείλουν δεδομένα σε ένα end device ενώ αυτό βρίσκεται σε Sleep mode. Αν βέβαια περάσει το προγραμματισμένο διάστημα, τα δεδομένα χάνονται. Τα end devices στέλνουν τα μηνύματα poll κάθε φορά που εξέρχονται της κατάστασης Sleep. Στην περίπτωση που δεν λάβουν πίσω κάποια επιβεβαίωση υποθέτουν ότι ο γονεϊκός

κόμβος είναι πλέον εκτός εμβέλειας και αναζητούν άλλον. Παρομοίως, αν ένα end device δεν έχει στείλει κάποιο poll request μέσα σε ένα προκαθορισμένο χρονικό πλαίσιο τότε ο κόμβος-γονέας το θεωρεί ως εκτός εμβέλειας και το διαγράφει από τη λίστα του, ελευθερώνοντας χώρο για κάποιο άλλο.

Ένας τέτοιος κόμβος μπορεί να εισέλθει σε διαφορετικές καταστάσεις λειτουργίας ανάλογα με τις απαιτήσεις της εκάστοτε εφαρμογής και του χρήστη. Στην περίπτωση που ένας κόμβος Zigbee δεν δέχεται αλλά ούτε και στέλνει δεδομένα τότε τίθεται σε Idle mode (αδράνεια). Ενώ βρίσκεται σε αυτή την κατάσταση, ο κόμβος περιμένει σήμα από τις σειριακές θύρες ή το pin RF για να λειτουργήσει στην αντίστοιχη κατάσταση. Θα μεταβεί σε Transmit mode (κατάσταση αποστολής) όταν χρειάζεται να στείλει δεδομένα σειριακά, ενώ θα τεθεί σε receive mode (κατάσταση αποδοχής) όταν δεχτεί κατάλληλα δεδομένα από την κεραία του. Τέλος, θα μεταβεί σε command mode (κατάσταση εντολών) όταν δεχτεί αντίστοιχο έναυσμα.

Κατά το Transmit mode ο κόμβος ελέγχει αν η 16 bit διεύθυνση δικτύου του κόμβου-δέκτη είναι γνωστή αλλά και τον «δρόμο» που πρέπει να διασχίσει το πακέτο για να φτάσει εκεί. Στην περίπτωση που ένα από αυτά τα δύο στάδια δεν είναι γνωστό τότε γίνεται προσπάθεια εύρεσής τους μέσω των διαδικασιών 16-bit Network Address Discovery και Route Discovery αντίστοιχα. Αν οποιαδήποτε από αυτές τις διαδικασίες αποτύχει, το πακέτο προς αποστολή απορρίπτεται και ο κόμβος επανέρχεται σε Idle state μέχρι νεοτέρας. Στην περίπτωση επιτυχούς αποστολής πακέτου, ο κόμβος περιμένει πακέτο acknowledgment από τον δέκτη. Αν δεν το λάβει εντός συγκεκριμένου χρονικού πλαισίου, τότε ξαναστέλνει το αρχικό πακέτο. Ως σημείωση από τον κατασκευαστή των συγκεκριμένων κόμβων, υπάρχει περίπτωση ένα πακέτο να φτάσει στον προορισμό του αλλά το acknowledgment να μην παραδοθεί ποτέ, με αποτέλεσμα τον «βομβαρδισμό» του κόμβου-δέκτη με το ίδιο πακέτο, πρόβλημα που λύνεται μόνο με παρέμβαση του χρήστη.



Το Receive mode είναι η κατάσταση στην οποία βρίσκεται ο κόμβος συνήθως για το μεγαλύτερο μέρος της λειτουργίας του και όταν δεν αποστέλλει δεδομένα.

Στο Command mode ο κόμβος βρίσκεται σε θέση να λάβει εντολές AT (attention) και να τις ερμηνεύσει ως εντολές μέσω του λογισμικού του. Πιο συγκεκριμένα, οι εντολές AT είναι ένας τρόπος αλληλεπίδρασης του χρήστη με τον κόμβο με την έννοια ότι μέσω αυτών μπορούν να τροποποιηθούν οι παράμετροι του κόμβου. Η συσκευή εισέρχεται σε command mode μέσω αντίστοιχης εντολής από UART και περιμένει για εντολές AT. Αν περάσουν δέκα δευτερόλεπτα χωρίς εντολή τότε ο κόμβος επιστρέφει στη προηγούμενη κατάσταση λειτουργίας του. Για την αποστολή μιας τέτοιας εντολής χρησιμοποιείται πρώτα το πρόθεμα AT και ύστερα η παράμετρος που πρόκειται να τροποποιηθεί.

Τέλος, χρησιμοποιείται και το Sleep mode για την μετάβαση των end device κόμβων σε κατάσταση χαμηλής κατανάλωσης όταν δεν χρησιμοποιούνται. Αυτό γίνεται είτε σε προγραμματισμένη χρονική στιγμή, είτε μέσω ειδικού pin. Το Sleep mode χωρίζεται σε τρείς υποκατηγορίες, το pin sleep, cyclic sleep και cyclic sleep with pin wake-up. Η πρώτη βασίζεται

στο Sleep pin (SLEEP_RQ) του κόμβου στο οποίο έχει πρόσβαση ο επιπρόσθετος μικροελεγκτής και καθορίζει μέσω αυτού την στιγμή που ο κόμβος θα τεθεί σε Sleep mode. Στην δεύτερη περίπτωση, μέσω εντολών AT προγραμματίζονται οι επιθυμητές χρονικές στιγμές πού ο κόμβος θα βρίσκεται σε Sleep mode, ενώ στην τρίτη περίπτωση δίνεται η δυνατότητα διακοπής του Sleep mode ακόμα και αν ο προγραμματισμένος χρόνος δεν έχει τελειώσει.

Κεφάλαιο 7: UART των Smartmesh IP και ZigBee

Το UART είναι τμήμα hardware που δίνει τη δυνατότητα για ασύγχρονη σειριακή επικοινωνία μεταξύ πομπού και δέκτη, με μεταβλητά (κατά βούληση) τα στοιχεία της δομής των αποστελλόμενων δεδομένων και της ταχύτητας αποστολής τους. Ο τρόπος λειτουργίας του αποτελείται από τα ακόλουθα δύο βήματα: το UART-αποστολέας χωρίζει τα δεδομένα (bytes) σε bits τα οποία έπειτα μεταδίδονται ένα-ένα με τη σειρά, και κατά την άφιξή τους, το UART-παραλήπτης συναρμολογεί τα bit στην αρχική τους μορφή. Η επικοινωνία μπορεί να έχεις τρεις μορφές, simplex (μονόπλευρη, αποστολή ή λήψη δεδομένων), half duplex (και οι δύο συσκευές υποστηρίζουν αποστολή και λήψη, αλλά κάθε φορά λαμβάνει χώρα μόνο ένα από τα δύο) και full duplex (και οι δύο συσκευές υποστηρίζουν αποστολή και λήψη, ταυτόχρονα). Παράδειγμα της αποστολής ενός byte παρουσιάζεται στην ακόλουθη εικόνα.

Κάθε χαρακτήρας τμηματοποιείται με αυτόν τον τρόπο σε ένα start bit, τα data bits, πιθανώς ένα parity bit και ένα stop bit. Το πιο σύνηθες είναι να βρίσκεται το λιγότερο σημαντικό bit στα αριστερά, δηλαδή μεταδίδεται πρώτο. Το start bit ανακοινώνει στον δέκτη την αποστολή δεδομένων, ενώ μετά το τέλος των δεδομένων μπορεί να αποσταλεί το parity bit. Το stop bit (λογικό 1 όπως φαίνεται και στην εικόνα) σηματοδοτεί την λήξη των δεδομένων. Χάρη στο γεγονός ότι τα bit των δεδομένων και τα start bits στέλνονται με λογικό 0, υπάρχουν τουλάχιστον δύο αλλαγές σήματος ανάμεσα σε κάθε δύο αποστελλόμενους χαρακτήρες.

Οι λειτουργίες του UART ελέγχονται από ένα σήμα χρονισμού (εσωτερικό ρολόι) με ταχύτητα συνήθως 8 ή 16 φορές μεγαλύτερη από το bit rate του. Ο δέκτης ψάχνει για το start bit για να ξεκινήσει να καταγράφει τον μεταδιδόμενο χαρακτήρα. Αυτό συμβαίνει με τον συνεχή έλεγχο του δεχόμενου σήματος από το ρολόι σε κάθε παλμό του. Υπάρχει μια πιθανότητα το σήμα που θα δεχτεί ο δέκτης να είναι αποτέλεσμα σφάλματος, κάτι που διασταυρώνεται με τη διάρκεια αυτού του σήματος. Εάν δεν είναι πολύ μικρή (κάτω από το μισό του χρόνου κάθε bit) τότε θεωρείται σωστό start bit και σηματοδοτείται η έναρξη άφιξης νέου χαρακτήρα. Επικοινωνούντες συσκευές UART δεν διαθέτουν κάποιο τρόπο χρονισμού παρά μόνο όταν δέχονται ένα start bit (κατά την δεύτερη ακμή του σήματος) και έπειτα απλά διαβάζουν το περιεχόμενο του κάθε bit.

Επίσης σημαντική λειτουργία τους είναι η αποθήκευση του πιο πρόσφατου χαρακτήρα μέχρι να ληφθεί ο επόμενος, πράγμα που αφήνει στην συσκευή-δέκτη ένα χρονικό περιθώριο μιας αποστολής χαρακτήρα για να τον επεξεργαστεί περεταίρω. Η λειτουργία αυτή ονομάζεται double buffering και χρησιμοποιείται αρκετές φορές με την μέθοδο FIFO (first in first out) έτσι ώστε ο επεξεργαστής-δέκτης να έχει παραπάνω χρόνο να χρησιμοποιήσει τους προσωρινά αποθηκευμένους χαρακτήρες ακόμα και σε υψηλές ταχύτητες.

Όσον αφορά στην αποστολή των δεδομένων, απλά αποστέλλονται τα bits στη σειρά. Στην συνηθισμένη περίπτωση του full duplex, τόσο το UART-αποστολέας όσο και το UART-δέκτης διαθέτουν δύο shift registers για τους προς αποστολή και τους προς επεξεργασία από το CPU χαρακτήρες. Το shift register είναι μια αλληλουχία από flip flop που έχει ως σκοπό την μετατροπή των δεδομένων από σειριακή μορφή (για παράδειγμα ο τρόπος μετάδοσης δεδομένων μεταξύ δύο UART) σε παράλληλη. Εκεί αποθηκεύονται οι πρόσφατα ειλημμένοι χαρακτήρες μέχρι την αποστολή του επόμενου.

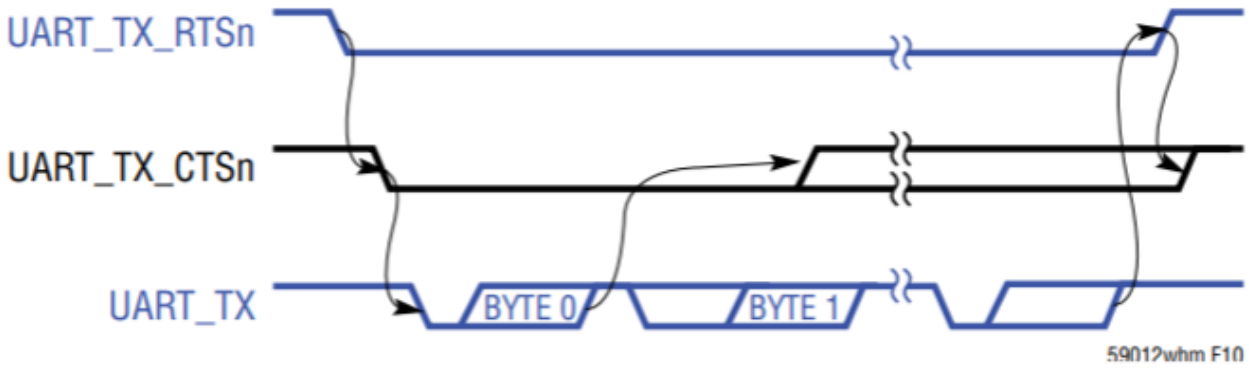
Για την ομαλή αποστολή και λήψη δεδομένων μέσω UART απαιτείται οι δύο συσκευές να είναι ρυθμισμένες με τις ίδιες τιμές ταχύτητας αποστολής bit, μήκος χαρακτήρα σε bits, αριθμού stop bits, καθώς και προσδιορισμός ύπαρξης ή όχι parity bit. Μη σωστή ρύθμιση με τους παραπάνω κανόνες μπορεί να εμφανίσει αντίστοιχο error ή ακόμα και να μεταφέρει λάθος χαρακτήρες.

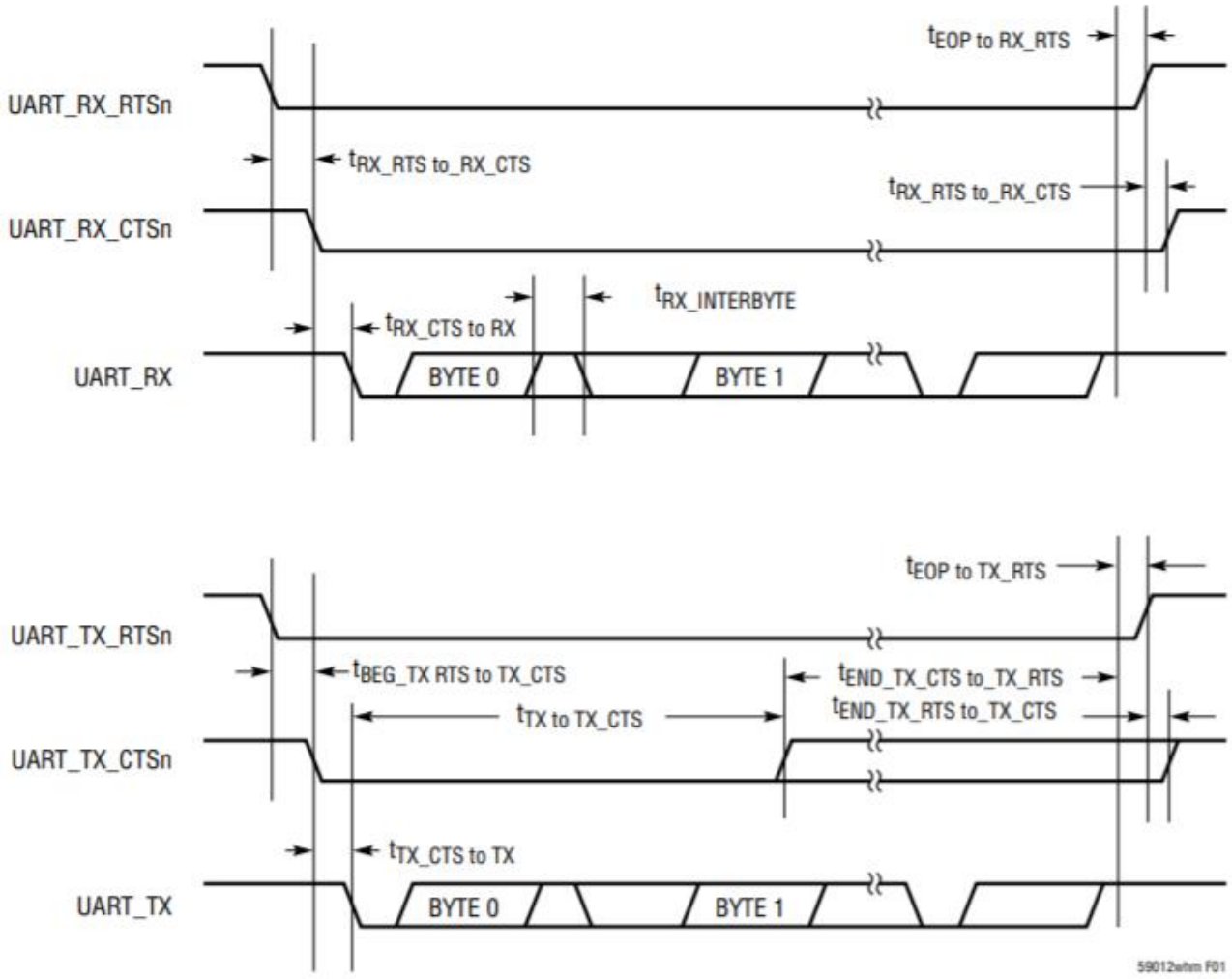
Οι κόμβοι της τεχνολογίας Smartmesh IP υποστηρίζουν την αλληλεπίδραση μεταξύ χρήστη και δικτύου μέσω UART εξειδικευμένου για την χρήση με το application programming interface (API) των κόμβων, ενώ ένα δεύτερο UART είναι υπεύθυνο για την χρήση με το command-line interface (CLI) για τις δοκιμές δικτύου και το debugging. Και τα δύο αυτά UART είναι συνέχεια σε «εγρήγορση», περιμένοντας να στείλουν ή να παραλάβουν δεδομένα χωρίς να καταναλώνουν σχεδόν καθόλου ρεύμα. Μετά την αποστολή δεδομένων επιστρέφουν πάλι σε κατάσταση χαμηλής κατανάλωσης.

Το πρωτόκολλο για την λειτουργία του API UART δημιουργήθηκε με γνώμονα την υποστήριξη μεγάλης γκάμας χρησιμοποιούμενων MCUs (multipoint control units) αλλά και την ελαχιστοποίηση της κατανάλωσης ρεύματος. Για το κομμάτι της μετάδοσης χρησιμοποιούνται τρία σήματα, τα UART_TX, UART_TX_RTSn και UART_TX_CTSn ενώ για το κομμάτι της λήψης τα UART_RX, UART_RX_RTSn και UART_RX_CTSn. Τα σήματα RTSn και CTSn αφορούν στο flow control (για τον έλεγχο της συχνότητας μετάδοσης-λήψης). Κατά τη λήψη

δεδομένων δεν χρειάζεται flow control και το baud rate φτάνει το 115200. Κατά την μετάδοση απαιτείται flow control για να επιτευχθεί baud rate άνω του 9600. Σχετικό διάγραμμα παρουσιάζεται παρακάτω. Τα σήματα με μπλε χρώμα προέρχονται από τον κόμβο, ενώ το σήμα με το μαύρο χρώμα προέρχεται από το χρησιμοποιούμενο MCU. Ένα σήμα UART_TX_RTSn δίνει το έναυσμα για την μετάδοση δεδομένων ενώ το σήμα UART_TX_CTSn είναι υπεύθυνο για τη σηματοδότηση ότι το MCU μπορεί να δεχθεί δεδομένα (γίνεται να τοποθετηθεί μόνιμα σε λογικό 0 για να είναι πάντα έτοιμο προς επικοινωνία). Τέλος, το σήμα UART_TX ξεκινάει την αποστολή bits. Όπως φαίνεται και στο διάγραμμα, περνάει ένα μικρό και προκαθορισμένο χρονικό πλαίσιο από την αποστολή του τελευταίου bit μέχρι την επανεκκίνηση της διαδικασίας με το σήμα UART_TX_RTSn. Αναλυτικότερα διαγράμματα τόσο για την μετάδοση όσο και για την λήψη παρατίθενται στην επόμενη σελίδα.

Σχετικά με τους χρόνους που μεσολαβούν μεταξύ των σημάτων και των bits, αυτοί είναι: μέγιστο 100ms μεταξύ byte, μέγιστο 20ms μεταξύ σημάτων UART_TX_CTSn και UART_TX, μέγιστο 22ms από την μετάδοση του πακέτου μέχρι το επόμενο UART_TX_RTSn και μέγιστο 22 ms μεταξύ σημάτων UART_TX_RTSn και UART_TX_CTSn.

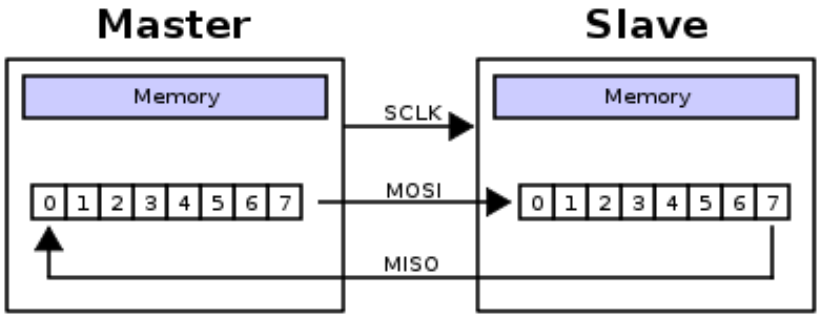




Όσον αφορά στο UART των κόμβων XBee, η λειτουργία του δεν παρουσιάζει μεγάλες διαφορές σε σύγκριση με εκείνο των κόμβων Smartmesh IP. Τα pins υπεύθυνα για την λειτουργία του είναι τα DOUT, DIN/CONFIG, CTS και RTS. Τα πρώτα δύο αντιπροσωπεύουν την είσοδο και έξοδο του UART αντίστοιχα. Τα pins CTS και RTS αφορούν στο flow control και λειτουργούν ως εξής: όταν το CTS είναι ενεργοποιημένο και το serial receive buffer (του δέκτη) απέχει 17 bytes από το να γεμίσει, η συσκευή αυτόματα σταματάει μέσω του CTS την αποστολή δεδομένων μέχρι ο buffer να έχει τουλάχιστον 34 byte χώρο ξανά. Στην περίπτωση του RTS, ενώ είναι ενεργοποιημένο δεν στέλνονται δεδομένα από τον serial transmit buffer προς το pin DOUT. Μη σωστή χρήση του τελευταίου μπορεί να προκύψει σε υπερχείλιση του buffer και σε χαμένα δεδομένα, λόγω έλλειψης χώρου. Το flow control και άρα και η χρήση των pins CTS και RTS είναι

απαραίτητα σε εφαρμογές όπου αποστέλλονται παραπάνω δεδομένα από όσα λαμβάνονται και το αντίθετο. Ακριβείς χρόνοι για την λειτουργία του UART των κόμβων XBee δεν παρέχονται από την εταιρεία. Παρακάτω παρουσιάζονται σχηματικά και κωδικοποιημένα οι λειτουργίες των pins.

Πέρα όμως από το UART, και οι δύο κόμβοι υποστηρίζουν τη δυνατότητα αποστολής δεδομένων με το πρωτόκολλο SPI (serial peripheral interface). Πρόκειται για επικοινωνία full duplex που λειτουργεί με βάση το σύστημα master-slave, με έναν κόμβο-master και έναν ή περισσότερους κόμβους-slave. Για την έναρξη της επικοινωνίας ο κόμβος-master ρυθμίζει το ρολόι (serial clock, SCLK) με συχνότητα συμβατή με τις δυνατότητες του κόμβου-slave. Οι γραμμές επικοινωνίας έχουν τα αρχικά MOSI (master out slave in) και MISO (master in slave out) και αντιπροσωπεύουν την κατεύθυνση από και προς τον κόμβο-master αντίστοιχα. Κάθε έναν κύκλο του ρολογιού στέλνεται ένα bit μέσω MOSI και ένα bit μέσω MISO (full duplex αποστολή δεδομένων).



Κεφάλαιο 8: Σύγκριση δυνατοτήτων Smartmesh IP και ZigBee

Αρχικά, τα πεδία στα οποία πρέπει να συγκριθούν τα δύο πρωτόκολλα και οι κόμβοι τους είναι τέσσερα, το κόστος, η κατανάλωση, η ασφάλεια και η ευρωστία firmware/hardware, οι δυνατότητες των κόμβων, και βάσει αυτών κρίνεται η ευελιξία που θα έχει ο μελλοντικός χρήστης τους για την διεκπεραίωση των επιθυμητών εφαρμογών. Σε προηγούμενο κεφάλαιο έγινε παράθεση των κύριων δυνατοτήτων και λειτουργιών των πρωτοκόλλων επικοινωνίας IEEE 802.15.4 και IEEE 802.15.4e. Αυτό το κεφάλαιο σκοπό έχει την παράθεσή όλων των παραμέτρων που θα μπορούσαν να καταστήσουν το κάθε ένα εκ των δύο πρωτόκολλων αναγκαίο για χρήση στις εκάστοτε εφαρμογές που απαιτούν mesh networking.

8.1 Κόστος

Όσον αφορά στο κόστος των Smartmesh IP και XBee για την επίλυση ενός προβλήματος του χρήστη πρέπει να ληφθούν υπόψη διάφοροι παράγοντες. Αρχικά, το κόστος στη συγκεκριμένη περίπτωση είναι μια μεταβλητή που προφανώς αυξάνεται όσο οι απαιτήσεις του χρήστη μεγαλώνουν. Για αυτό το λόγο πρέπει να θεωρηθεί ένα παράδειγμα προβλήματος προς επίλυση με ρεαλιστικές διαστάσεις και αντίκρισμα στην πραγματικότητα. Μια ιδανική χρήση ενός mesh δικτύου με ευνοϊκές συνθήκες για το δίκτυο και τους κόμβους του είναι για παράδειγμα η παρακολούθηση των συνθηκών μιας γεωργικής έκτασης. Οι κόμβοι τοποθετούνται σε σταθερά σημεία ανά την επιθυμητή έκταση και λειτουργούν σε αρμονία ώστε οι πληροφορίες που επεξεργάζεται ο καθένας να συλλέγονται από τον χρήστη. Η παραπάνω περίπτωση είναι ιδανική διότι (συνήθως) σε τέτοιες εκτάσεις δεν υπάρχουν εμπόδια για τις εκπομπές των κεραιών και έτσι επισφραγίζεται η επιτυχής αποστολή και λήψη δεδομένων ακόμα και στο όριο των αναγραφόμενων εμβελειών. Τα δεδομένα καλύπτουν ένα ευρύ φάσμα των σημαντικών πληροφοριών σε μια γεωργική καλλιέργεια, όπως θερμοκρασία και υγρασία αέρα και εδάφους.

Στο παράδειγμα αυτό για λόγους ευκολίας θεωρείται ότι χρησιμοποιούνται είκοσι συνολικά κόμβοι. Στην περίπτωση που ο χρήστης αποφασίσει να καλύψει αυτές τις θέσεις με κόμβους Smartmesh IP, το όλο εγχείρημα θα του κοστίσει το λιγότερο $4,875.00. Αυτό το ποσό

χωρίζεται σε $3,000.00 για το Starter Kit που περιέχει πέντε κόμβους, έναν embedded manager για τοπικό δίκτυο και έναν VManager και τα απαραίτητα παρελκόμενα για debugging και υποστήριξη άλλων εξαρτημάτων, και έπειτα $125 για κάθε επιπλέον κόμβο ξεχωριστά. Στην άλλη περίπτωση που αποφασιστεί η χρήση κόμβων XBee της Digi, το κόστος της εφαρμογής μειώνεται δραματικά. Οι τιμές αυτών των συσκευών ποικίλουν αλλά πλησιάζουν ποσά της τάξης των $20 για την κάθε μια. Με τα απαραίτητα παρελκόμενα, το συνολικό κόστος της τοποθέτησης κόμβων XBee θα ήταν κοντά στα $500 για το παραπάνω παράδειγμα.

8.2 Κατανάλωση ρεύματος

Σχετικά με την κατανάλωση ρεύματος των κόμβων των δύο συγκρινόμενων τεχνολογιών, ο μελλοντικός χρήστης θα πρέπει να γνωρίζει αναλυτικά την κατανάλωση τους σε όλες τις φάσεις λειτουργίας τους για να μπορεί να προβεί στις απαραίτητες ενέργειες κατά την τοποθέτησή τους. Αν πρόκειται να χρησιμοποιηθούν σε μια εφαρμογή η οποία δεν προβλέπεται να χρειάζεται συχνή επίβλεψη, τότε ο τελικός χρήστης είναι αναγκαίο να γνωρίζει πόσο καιρό μπορεί να αντέξει σε κάθε περίπτωση η μπαταρία της κάθε συσκευής. Φυσικά αυτή η διαδικασία βασίζεται σε έναν υπολογισμό της διάρκειας ζωής της μπαταρίας με βάση την διάρκεια που ο κάθε κόμβος βρίσκεται σε κάποια συγκεκριμένη κατάσταση λειτουργίας και ως εκ τούτου το αποτέλεσμα του υπολογισμού αυτού ενδέχεται να επηρεάζεται από εξωτερικούς παράγοντες όπως οι καιρικές συνθήκες. Πολλές φορές, επίσης, αυτή η σύγκριση μπορεί να μην είναι αναγκαία διότι ενδέχεται για παράδειγμα η τροφοδοσία των κόμβων να γίνεται μέσω μεθόδων energy harvesting όπως ένα φωτοβολταϊκό πάνελ.

Αρχικά ας παρουσιαστούν τα στοιχεία κατανάλωσης των κόμβων της τεχνολογίας Smartmesh IP. Ένας κόμβος ενώ βρίσκεται σε Active state (ενεργή κατάσταση) καταναλώνει 1.3 mA (το δευτερόλεπτο), σημαντική πληροφορία για την περίπτωση των κόμβων που λειτουργούν ως manager και πρέπει να παραμένουν συνέχεια σε αυτή την κατάσταση λειτουργίας. Κατά την διάρκεια της παραμονής του κόμβου σε κατάσταση doze, το καταναλισκόμενο ρεύμα είναι μόλις 1.2 μA ενώ σε κατάσταση deep sleep 0.8 μA. Σχετικά με την διακίνηση δεδομένων, ένας κόμβος καταναλώνει 5.4 mA κατά την αποστολή δεδομένων στα +0 dBm και 9.7 mA στα +8 dBm ενώ καταναλώνει 4.5 mA κατά την λήψη δεδομένων. Παρατίθενται επίσης και οι καταναλώσεις

ρεύματος όπως για το Reset του κόμβου ενώ αυτός λειτουργεί, για την καταχώρηση στην flash μνήμη ή την διαγραφή αυτής, με την σειρά: 12 mA, 3.7 mA και 2.5 mA.

Όσο για τους κόμβους πρωτοκόλλου ZigBee της XBee τα στοιχεία κατανάλωσης τους έχουν ως εξής. Μέσω datasheet των κόμβων της εταιρείας σημειώνονται οι καταναλώσεις ρεύματος στις δύο περιπτώσεις της αποστολής δεδομένων και της λήψης δεδομένων. Στην πρώτη περίπτωση καταναλώνονται 45 mA στα + 8dBm και 33 mA στα +5 dBm ενώ στην δεύτερη περίπτωση 31 mA και 28 mA αντίστοιχα. Η κατανάλωση ρεύματος για την δεύτερη περίπτωση είναι ίδια και για όσο ένας κόμβος βρίσκεται σε Idle mode.

Και με τις δύο τεχνολογίες, ο τελικός χρήστης καλείται να υπολογίσει για κάθε μια την τελική κατανάλωση ρεύματος του κάθε κόμβου μέσω απλής πρόσθεσης του χρόνου στον οποίο βρίσκεται η κάθε συσκευή σε κάποια κατάσταση λειτουργίας, επί την κατανάλωση ρεύματος της λειτουργίας αυτής. Το πρόβλημα στην συγκεκριμένη φάση είναι ότι δεν παρέχεται κάποια ακριβής τιμή για την κατανάλωση των κόμβων XBee σε Command mode ή Sleep mode από τα datasheet της εταιρείας οπότε η σύγκριση από τον χρήστη θα πρέπει να γίνει κυρίως αναφορικά στις διαδικασίες αποστολής και λήψης δεδομένων.

8.3 Ασφάλεια και ευρωστία firmware/hardware

Ένα πολύ σημαντικό στοιχείο, το οποίο κάθε υποψήφιος χρήστης mesh δικτύων απαιτεί είναι η ασφάλεια του δικτύου του. Αυτό σημαίνει ότι αρχικά οι κόμβοι δεν πρέπει να είναι επιρρεπείς σε φυσικές επιθέσεις από κακοβουλία ή ακραίες καιρικές συνθήκες, και κατά δεύτερον ότι το ενσωματωμένο σύστημα ασφαλείας της κάθε τεχνολογίας κόμβων πρέπει να είναι προετοιμασμένο για τα πάντα. Σε προηγούμενα κεφάλαια έγινε μια παράθεση των δυνατοτήτων ασφαλείας τόσο του Smartmesh IP αλλά και του ZigBee.

Η ασφάλεια δικτύου που παρέχεται από το πρωτόκολλο ZigBee βασίζεται στην ανταλλαγή κλειδιών ασφαλείας με τον συνδυασμό αλγορίθμων κρυπτογράφησής τους, καθώς και με μια μέθοδο εξακρίβωσης της αυθεντικότητας των αποσταλμένων μηνυμάτων. Όπως έχει

προαναφερθεί, μπορεί η λογική πίσω από τα θεμέλια της ασφάλειας του πρωτοκόλλου ZigBee να μοιάζει αλεξίσφαιρη, υπάρχουν όμως σχετικά απλοί τρόποι, όπως το jamming, που μπορούν να καταφέρουν ένα μεγάλο πλήγμα σε μια εγκατάσταση με κόμβους ZigBee. Οι κόμβοι XBee της ZigBee δεν προσφέρουν κάποια ιδιαίτερη βελτίωση σχετικά με την ασφάλεια δικτύου, παρά στηρίζονται στην ήδη υπάρχουσα που παρέχει το πρωτόκολλο ZigBee. Τα παραπάνω σε συνδυασμό με τα μειονεκτήματα του IEEE 802.15.4 στο οποίο βασίζεται το πρωτόκολλο ZigBee (μεγάλη βάση στο CSMA/CA) το καθιστούν μια επισφαλή λύση για εφαρμογές δικτύωσης πλέγματος.

Από την άλλη μεριά του νομίσματος το πρωτόκολλο Smartmesh IP και αυτό στηρίζεται στην ασφάλεια του δικτύου του μέσω ειδικών κλειδιών ασφαλείας. Την διαφορά εδώ κάνει το γεγονός ότι, τα τέσσερα διαφορετικά είδη κλειδιών διανέμονται σε κάθε κόμβο, με τα δύο εξ αυτών να είναι μοναδικά για αυτόν τον κόμβο, επισφραγίζοντας με τις προαναφερθείσες λειτουργίες τους την ασφαλή μετάδοση και αποστολή δεδομένων. Συνδυαστικά με την Access Control List προσφέρεται ασφάλεια δικτύου φαινομενικά αδιαπέραστη. Αξίζει εδώ να σημειωθεί ότι τα παραπάνω ατού της ασφάλειας του Smartmesh IP δικτύου υποβοηθούνται από τα ήδη βελτιωμένα και νέα χαρακτηριστικά του IEEE 802.15.4e (σε σχέση με το IEEE 802.15.4) στο οποίο το πρωτόκολλο αυτό βασίζεται, με το πιο σημαντικό από αυτά να είναι το Time Slotted Channel Hopping. Χάρη σε αυτό περιορίζονται τα περισσότερα προβλήματα που πρόκυπταν από την χρήση ενός καναλιού για την επικοινωνία.

Όσον αφορά στην ασφάλεια και ευρωστία του hardware των δύο ειδών κόμβων, η κατάσταση και στις δύο περιπτώσεις είναι παρόμοια. Ως προς την αποφυγή βλάβης από καιρικές συνθήκες κανένας από τους δύο κόμβους δε διαθέτει κάποια προστασία, ούτε παρέχεται από τις εταιρείες τους το οποιοδήποτε προστατευτικό παρελκόμενο. Είναι στο χέρι του χρήστη να βελτιστοποιήσει τις συνθήκες στις οποίες θα τεθεί το hardware της εφαρμογής του. Τέλος, αναφέρεται ότι οι κόμβοι Smartmesh IP διαθέτουν ένα προστατευτικό μεταλλικό καλυπτήριο πάνω από τον επεξεργαστή τους ως ένα μικρό μέτρο προστασίας κατά των επιθέσεων από τρίτους.

8.4 Δυνατότητες

Οι δυνατότητες του κάθε προϊόντος είναι εκείνες που έχουν την μεγαλύτερη βαρύτητα όταν ο πιθανός αγοραστής ψάχνει έναν τρόπο να επιλύσει το πρόβλημά του. Είναι πιθανό ο τελικός χρήστης να καταλήξει σε μια αγορά προϊόντος υποκινούμενη από την φήμη του εκάστοτε προϊόντος ή της εταιρείας που το παράγει. Παρόλα αυτά στη συγκεκριμένη περίπτωση υπάρχουν και άλλοι παράγοντες που επηρεάζουν τις επιδόσεις του κάθε είδους κόμβου και τεχνολογίας που δεν είναι στο χέρι της κατασκευάστριας εταιρείας να τροποποιηθούν. Αυτοί οι παράγοντες σχετίζονται με τα πρωτόκολλα επικοινωνίας στα οποία βασίζονται τα Smartmesh IP και ZigBee, τα IEEE 802.15.4e και IEEE 802.15.4 αντίστοιχα.

Όπως αναφέρθηκε και σε προηγούμενο κεφάλαιο, το πρωτόκολλο επικοινωνίας IEEE 802.15.4 είναι ένας δοκιμασμένος τρόπος για επικοινωνία μορφής star ή tree. Χαρακτηρίζεται για την διευκόλυνση των εφαρμογών που απαιτούν ελάχιστη κατανάλωση και μεταχειρίζονται μικρές ποσότητες δεδομένων, και πάνω σε αυτό βασίστηκε η εξέλιξη του πρωτόκολλου επικοινωνίας ZigBee. Έτσι το ZigBee αποτελεί μια εξελιγμένη μορφή του IEEE 802.15.4 σχετικά με τις λειτουργίες που προσθέτει στη φαρέτρα του πρωτοκόλλου. Αυτές έχουν να κάνουν με τα OSI layers 3 έως 7, ενώ οι δυνατότητες των πρώτων δύο layers (PHY, MAC) δεν τροποποιούνται από το ZigBee. Σημαντικότερη δυνατότητα του ZigBee είναι η δημιουργία δικτύου με τοπολογία πλέγματος. Το γεγονός ότι έτσι δημιουργείται ένα δίκτυο που προσαρμόζεται στις αλλαγές τοποθεσίας των κόμβων του καθιστά το ZigBee αναπόσπαστο κομμάτι εφαρμογών συλλογής δεδομένων. Επιπροσθέτως, ένα δίκτυο ZigBee έχει την δυνατότητα να υποστηρίξει μέχρι και 232 κόμβους, προσφέροντας έτσι μεγάλη ευελιξία στον χρήστη για την διαμόρφωση του επιθυμητού του δικτύου. Τα παραπάνω σε συνδυασμό με την μικρή κατανάλωση των κόμβων στην κατάσταση λειτουργίας τους, την συχνότητα που μπορούν να βρίσκονται σε κατάσταση αναμονής και την ύπαρξη του ZigBee Alliance (συνδυασμός μεγάλων εταιρειών που συμμετέχουν στην διαμόρφωση του πρωτοκόλλου) παρουσιάζουν το ZigBee ως κυρίαρχη δύναμη στον τομέα των mesh networks.

Όσον αφορά στο πρωτόκολλο επικοινωνίας Smartmesh IP, δεν βρίσκεται υπό την αιγίδα κάποιου συνασπισμού εταιρειών όπως το ZigBee αλλά αναπτύσσεται από την Analog. Σημαντική διαφορά του από το ZigBee είναι ότι αποτελεί εξελιγμένη μορφή του IEEE 802.15.4e και εκμεταλλεύεται στο έπακρο όλες τις βελτιωμένες λειτουργίες του σε σχέση με εκείνες του IEEE 802.15.4. Τα θεμέλια του Smartmesh IP συνεπώς δίδουν από μόνα τους στον χρήστη την σιγουριά

της μεταχείρισης πολλών καναλιών επικοινωνίας για την μετάδοση και λήψη πληροφοριών, γεγονός που παραμερίζει την αδυναμία του ZigBee με το jamming του καναλιού και την αντιμετώπιση αυτού. Φυσικά, και το πρωτόκολλο Smartmesh IP ειδικεύεται στην δημιουργία και συντήρηση δικτύων τοπολογίας πλέγματος. Μεγάλο του πλεονέκτημα απέναντι σε άλλες τεχνολογίες όπως και το ZigBee είναι ότι κάθε του κόμβος, πέρα από τον κόμβο που τελεί καθήκοντα manager, μπορεί να αναμεταδώσει, να λάβει και να στείλει δεδομένα, δυναμικά κάθε φορά και ανάλογα με τις εκάστοτε απαιτήσεις. Πρόκειται επίσης για τεχνολογία που σχεδιάστηκε έχοντας κατά νου ότι η δικτύωση πλέγματος χρειάζεται ακόμα λιγότερη κατανάλωση από ότι οι συμβατικές μέχρι εκείνη την περίοδο τεχνολογίες, γεγονός που επιτρέπει στους κόμβους της να λειτουργούν για χρόνια αδιάκοπα, πιθανόν και περισσότερο από το προσδόκιμο ζωής των μπαταριών τους (αν χρησιμοποιούνται). Επιπροσθέτως υπενθυμίζεται ότι μπορεί μεν ένα «απλό» δίκτυο Smarmesh IP με embedded manager να υποστηρίζει μόνο 32 κόμβους, η ύπαρξη όμως της εναλλακτικής του VManager προσφέρει την δυνατότητα εφαρμογής χιλιάδων κόμβων και την χρήση υποδικτύων που ενώνονται σε ένα συνολικό, διαχειριζόμενο από το εκάστοτε αρμόδιο application.

8.5 Σύγκριση και συμπεράσματα

Ο κύριος λόγος που τα πρωτόκολλα επικοινωνίας Smartmesh IP και ZigBee μοιάζουν να έχουν πολλά κοινά, όμως διαφέρουν πάρα πολύ, είναι δίοτι μπορεί μεν και τα δύο να δημιουργήθηκαν με σκοπό την εξέλιξη και βελτιστοποίηση της δικτύωσης πλέγματος με χαμηλή κατανάλωση, καθορίζονται δε από τα πολύ σημαντικά χαρακτηριστικά των πρωτόκολλων στα οποία βασίζονται. Λέγοντας σημαντικά χαρακτηριστικά, δεν γίνεται προσπάθεια υποβάθμισης των μετέπειτα εμπλουτισμών τους από τις εταιρείες που δημιούργησαν τα δύο συγκρινόμενα πρωτόκολλα, παρά μόνο μια παράθεση του τί επηρεάζει θετικά και τι αρνητικά ένα πρωτόκολλο δικτύωσης πλέγματος.

Το πρωτόκολλο ZigBee, βασισμένο στο IEEE 802.15.4 έχει ένα πολύ σημαντικό μειονέκτημα που σχετίζεται με το ότι χρησιμοποιεί ένα κανάλι επικοινωνίας. Το να βρίσκεται ένα σύστημα κόμβων σε μειονεκτική θέση λόγω εύκολου jamming δεν αποτελεί ατού για το ZigBee. Το παραπάνω είναι απόρροια του μειονεκτήματος του IEEE 802.15.4 να βασίζεται στο

πρωτόκολλο CSMA/CA του data link layer με την πιθανότητα τα αποστελλόμενα αρχεία να χαθούν κατά τη διάρκεια της μετάδοσης. Από την άλλη μεριά, το IEEE 802.15.4e στο οποίο στηρίχθηκε το Smartmesh IP διαθέτει το TSCH και διαχειρίζεται την εναλλαγή ανάμεσα σε 16 κανάλια για να διασφαλίσει την σίγουρη μετάδοση και λήψη δεδομένων αλλά και την ταυτόχρονη επικοινωνία, χωρίς το «άγχος» των χαμένων πακέτων ή του jamming. Οι δύο αυτές πολύ σημαντικές διαφορές στα πρωτόκολλα της IEEE καθορίζουν εξ αρχής το προβάδισμα του Smartmesh IP ως πρωτόκολλο με σωστή βάση για mesh networks.

Σχετικά με την ασφάλεια των πρωτόκολλων το Smartmesh IP έχει πλεονέκτημα αφού στοχεύει στην καταπολέμηση του “eavesdropping” ή αλλιώς της υποκλοπής των αποστελλόμενων δεδομένων με την χρήση πολλών κλειδιών ασφαλείας για κάθε κόμβο στο δίκτυο. Στην περίπτωση του ZigBee κάτι τέτοιο δεν είναι εφικτό αφού με ένα επιτυχημένο jamming από τρίτους ο κόμβος είναι ευάλωτος και κατά συνέπεια και το υπόλοιπο δίκτυο.

Όσον αφορά στο τι μπορεί να «κάνει» κάθε πρωτόκολλο, δηλαδή ποιες είναι οι ειδοποιές διαφορές του συγκριτικά με το άλλο, συμπεραίνεται εύκολα με την σύγκριση των δύο στον τομέα αυτόν. Το ZigBee είναι θεμελιωμένο ως η απλή λύση mesh δικτύωσης και προσφέρει αυτό ακριβώς στον τελικό χρήστη, χωρίς πολλές επιπλέον λειτουργίες, πέρα φυσικά από τις λειτουργίες που το καθιστούν πρωτόκολλο για δικτύωση πλέγματος (όπως το low power mode των κόμβων). Υποστηρίζει σχετικά μεγάλο αριθμό κόμβων σε ένα δίκτυο πράγμα θετικό για εφαρμογές μεγάλης έκτασης. Το Smartmesh IP είναι σχεδιασμένο με σκοπό να είναι το πιο οικονομικό από άποψη κατανάλωσης, όπως διαφημίζουν οι κατασκευαστές του, και για να το επιτύχει αυτό του έχουν δωθεί ανάλογα χαρακτηριστικά όπως το blink mode. Τα νούμερα που παρατέθηκαν σε παραπάνω παράφραφο δείχνουν την μεγάλη διαφορά στην κατανάλωση, κοντά στα 40 mA παραπάνω για τις διαδικασίες αποστολής και λήψης δεδομένων από τη μεριά των κόμβων ZigBee της XBee. Εδώ γίνεται και ξεκάθαρο το γεγονός ότι δεν γινόταν να συγκριθεί η PRO έκδοση των κόμβων της XBee με εκείνων της Analog διότι τότε η διαφορά στην κατανάλωση θα ήταν ακόμα μεγαλύτερη, με εύρος της τάξης των 100-150 mA.

Συμπερασματικά, ο μελλοντικός καταναλωτής μπορεί να αποφασίσει στο τι τον διευκολύνει με μια ματιά στους τέσσερις αυτούς συγκριτικούς παράγοντες μεταξύ των δύο πρωτόκολλων. Το ZigBee είναι μια απλή και φθηνή λύση που σκοπό έχει να καλύψει τις ανάγκες απλών καθημερινών χρηστών έως και τις ανάγκες ενός εργασιακού περιβάλλοντος (εξαρτάται με

το μέγεθος και τη σημασία των αναγκών αυτών). Το χαμηλό του κόστος το καθιστά σίγουρα ως την πρώτη επιλογή για εφαρμογή σε συστήματα οικιακού αυτοματισμού, γεγονός που υποστηρίζεται από την πληθώρα επιλογών που έχει ο καταναλωτής λόγω του ZigBee Alliance. Όταν όμως το ζήτημα είναι μια αδιάκοπη και ασφαλής λύση για δικτύωση πλέγματος, υστερεί τόσο σε θέματα ασφαλείας όσο σε θέματα παρεχόμενων επιλογών. Αυτό το καθήκον έρχεται να καλύψει το πρωτόκολλο Smartmesh IP. Το πολύ υψηλό του κόστος μπορεί να το καθιστά απαγορευτικό για απλές εφαρμογές, είναι όμως μια ασφαλής λύση με πολλές δυνατότητες που υπόσχεται χρόνια ασταμάτητης λειτουργίας. Η ηδη υπάρχουσα ευρωστία που βρίσκεται «χτισμένη» μέσα στο IEEE 802.15.4e και στις ενισχυμένες δυνατότητες του Smartmesh IP, κάνουν το δεύτερο συγκριτικά με το ZigBee την καλύτερη επιλογή για απαιτητικές εφαρμογές δικτύωσης πλέγματος.

Βιβλιογραφία

1 https://www.analog.com/media/en/technical-documentation/user-guides/SmartMesh_IP_Tools_Guide.pdf τελευταία προσπέλαση στις 2/5/2020

2 https://www.analog.com/media/en/technical-documentation/user-guides/Eterna_LTP5901_LTP5902_Integration_Guide.pdf τελευταία προσπέλαση στις 2/5/2020

3 https://www.analog.com/media/en/reference-design-documentation/design-notes/board_specific_configuration_guide.pdf τελευταία προσπέλαση στις 2/5/2020

4 Shahin Farahani *'Zigbee Wireless Networks and Transceivers'* Newnes, 2008

5 https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf τελευταία προσπέλαση στις 20/8/2019

6 https://www.ijcaonline.org/research/volume130/number9/aju-2015-ijca-907130.pdf τελευταία προσπέλαση στις 22/8/2019

7 https://www.ledinside.com/news/2015/8/experts_find_serious_security_flaws_in_zigbee_connected_devices τελευταία προσπέλαση στις 22/8/2019

8 Sanatan Mohanty '*Energy Efficient Routing Algorithms for Wireless Seonsort Networks and Performance Evaluation of Quality Servie for IEEE 802.15.4 Networks'* https://www.researchgate.net/publication/47737848_Energy_Efficient_Routing_Algorithms_for_Wireless_Sensor_Networks_and_Performance_Evaluation_of_Quality_of_Service_for_IEEE_802154_Networks

9 https://www.cister.isep.ipp.pt/docs/ieee_802_15_4e_in_a_nutshell__survey_and_performance_evaluation/1352/view.pdf τελευταία προσπέλαση στις 29/8/2019

10 https://www.analog.com/media/en/technical-documentation/user-guides/smartmesh_ip_user_s_guide.pdf τελευταία προσπέλαση στις 2/5/2020

11 https://www.digi.com/resources/documentation/digidocs/pdfs/90002002.pdf τελευταία προσπέλαση στις 15/4/2020

12 https://www.silabs.com/documents/public/user-guides/ug103-02-fundamentals-zigbee.pdf τελευταία προσπέλαση στις 15/4/2020

13 https://en.wikipedia.org/wiki/Serial_Peripheral_Interface τελευταία προσπέλαση στις 17/7/2019

14 https://en.wikipedia.org/wiki/Shift_register τελευταία προσπέλαση στις 29/09/2019

15 https://en.wikipedia.org/wiki/Asynchronous_serial_communication τελευταία προσπέλαση στις 22/10/2019

16 https://en.wikipedia.org/wiki/Universal_asynchronous_receiver-transmitter τελευταία προσπέλαση στις 3/2/2020

17 https://en.wikipedia.org/wiki/Time-division_multiple_access#cite_note-Zander-1 τελευταία προσπέλαση στις 1/6/2019

18 https://en.wikipedia.org/wiki/Carrier-sense_multiple_access_with_collision_avoidance τελευταία προσπέλαση στις 28/5/2019

19 https://en.wikipedia.org/wiki/OSI_model τελευταία προσπέλαση στις 28/5/2019 τελευταία προσπέλαση στις 28/5/2019

20 https://dustcloud.atlassian.net/wiki/spaces/SMSDK/pages/37650587/AclCommissioning τελευταία προσπέλαση στις 2/5/2020

21 https://www.slideshare.net/ampas03/9-multiple-access τελευταία προσπέλαση στις 28/5/2019