



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ
ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ ΔΙΑΤΜΗΜΑΤΙΚΟ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΜΙΚΡΟΣΥΣΤΗΜΑΤΑ ΚΑΙ ΝΑΝΟΔΙΑΤΑΞΕΙΣ

ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΑΙΣΘΗΤΗΡΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΧΡΗΣΤΟΥ ΜΑΥΡΙΔΗ

Επιβλέπων : Τσουκαλάς Δημήτρης
Καθηγητής Ε.Μ.Π

Αθήνα, Ιούλιος 2014



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ
ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ ΔΙΑΤΜΗΜΑΤΙΚΟ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΜΙΚΡΟΣΥΣΤΗΜΑΤΑ ΚΑΙ ΝΑΝΟΔΙΑΤΑΞΕΙΣ

ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΑΙΣΘΗΤΗΡΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΧΡΗΣΤΟΥ ΜΑΥΡΙΔΗ

Επιβλέπων : Τσουκαλάς Δημήτρης
Καθηγητής Ε.Μ.Π

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή Ιούλιος 2014

.....
Τσουκαλάς Δημήτρης
Καθηγητής Ε.Μ.Π

.....
Δρ. Χατζανδρούλης Σταύρος
Ερευνητής ΕΚΕΦΕ «Δημόκριτος»

.....
Ζεργιώτη Ιωάννα
Καθηγήτρια Ε.Μ.Π

Αθήνα, Ιούλιος 2014

.....
Χρήστος Μαυρίδης

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π

Copyright © Χρήστος Μαυρίδης 2014

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

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

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

ΠΕΡΙΛΗΨΗ

Σκοπός αυτής της διπλωματικής εργασίας είναι η μελέτη της χρήσης των ασύρματων δικτύων αισθητήρων. Για το λόγο αυτό, αρχικά δίνεται ο ορισμός του όρου «δίκτυο αισθητήρων», δίνονται τα χαρακτηριστικά του και αναλύονται ορισμένοι τύποι αισθητήρων. Έπειτα μελετώνται οι ιδιαιτερότητες που έχουν τα Sensor Networks στα ζητήματα ασφάλειας καθώς και οι διάφορες προτάσεις και συζητήσεις που υπάρχουν στον τομέα αυτό.

Στη συνέχεια, αναλύονται τα χαρακτηριστικά του ZigBee και του IEEE 802.15.4 τα οποία βασίζονται σε πρότυπα πρωτόκολλα. Παρουσιάζονται επίσης η δομή τους, οι τοπολογίες και οι συνδέσεις που χρησιμοποιούν τα δίκτυα ZigBee. Επιπλέον, γίνεται λεπτομερής περιγραφή του ZigBee protocol Stack και των ζωνών συχνοτήτων που χρησιμοποιούν αυτά τα ασύρματα πρότυπα. Ιδιαίτερη αναφορά γίνεται στην ασφάλεια ZigBee και στα ιδιωτικά απόρρητα θέματα τα οποία μας προβληματίζουν ακόμα και σήμερα.

Προκειμένου να δούμε στην πράξη, λοιπόν, τα ασύρματα δίκτυα αισθητήρων πραγματοποιούμε μετρήσεις τηλεπικοινωνιακής κίνησης μεταξύ των ασύρματων κόμβων αισθητήρων. Οι αισθητήρες που χρησιμοποιήθηκαν ήταν θερμοκρασίας και επιταχυνσιόμετρο οι οποίοι ήταν ενσωματωμένοι πάνω στην Wasmote πλακέτα της Libelium η οποία και έφερε και τον μικροελεγκτή ATmega 1281 των 8 bits, τεχνολογίας CMOS χαμηλής ισχύος. Όσον αφορά τον coordinator (συντονιστής), χρησιμοποιήθηκε η μονάδα XBee Module - ZB Series 2. Για τον προγραμματισμό κάθε κόμβου, χρησιμοποιήσαμε το ελεύθερο λογισμικό X-CTU, το οποίο παρέχεται από την Digi International, ενώ για την εμφάνιση των αποτελεσμάτων δημιουργήσαμε ένα δικό μας Serial Monitor (σειριακή οθόνη) σε γλώσσα προγραμματισμού C# μέσω του Visual Studio. Τέλος, οι μετρήσεις αυτές αναλύονται, ερμηνεύονται και αξιολογούνται.

Λέξεις Κλειδιά : « Ασύρματα δίκτυα αισθητήρων, ZigBee, IEEE 802.15.4, Wasmote, Libelium, XBee Module - ZB Series 2»

ABSTRACT

The aim of this thesis is to investigate the use of wireless sensor networks. For this reason, initially is given the definition of the term "sensor network", its characteristics and analyze certain types of sensors. Then we study the peculiarities that have Sensor Networks in security issues and the various proposals and discussions that exist in this area.

Then we analyzed the characteristics of ZigBee and IEEE 802.15.4, which are based on standard protocols. It also presents the structure, topologies and connections that ZigBee networks use. In addition, is given a detailed description of the ZigBee protocol Stack and the bands of frequencies which wireless standards use. Particular reference is made to the ZigBee security secrets and private matters that trouble us even today.

To see in practice, therefore, WSNs performs telecommunication traffic measurements between wireless sensor nodes. The sensors which used were temperature and accelerometer which were incorporated on the board of Waspote Libelium and which brought on it the microcontroller ATmega 1281 of 8 bits, low-power CMOS technology. Regarding the coordinator, the unit which used was XBee Module - ZB Series 2. To schedule each node, we used the free software X-CTU, which is supplied by Digi International, while displaying the results we created our own Serial Monitor on the programming language C # through Visual Studio. Finally, these measurements are analyzed, interpreted and evaluated.

Keywords : « Wireless Sensor Networks, ZigBee, IEEE 802.15.4, Waspote, Libelium, XBee Module - ZB Series 2»

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τον κ. Στ. Χατζανδρούλη για την πολύτιμη βοήθεια και την αμέριστη υποστήριξη που μου έδειξε κατά τη διάρκεια εκπόνησης αυτής της εργασίας.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΕΦΑΛΑΙΟ 1 : Εισαγωγή	12
1.1 Μικροεπεξεργαστές	12
1.2 Δίκτυα αισθητήρων	13
1.3 Στρατηγική έρευνα	14
1.4 Αισθητήρες.....	15
1.4.1 Θερμοκρασίας	15
1.4.2 Χωρητικότητας	15
1.4.3 Επιταχυνσιόμετρο.....	15
1.5 Εφαρμογές.....	16
ΚΕΦΑΛΑΙΟ 2 : Δίκτυα Αισθητήρων	18
2.1 Εισαγωγή	18
2.2 Τοπολογίες	20
2.3 Τρόποι μετάδοσης στα δίκτυα αισθητήρων - ομοιότητες και διαφορές ad-hoc WSN	23
2.4 Εφαρμογές.....	23
2.4.1 Παρακολούθηση περιοχής.....	24
2.4.2 Παρακολούθηση περιβάλλοντος και καιρικών συνθηκών	24
2.4.2.1 Παρακολούθηση ατμοσφαιρικών ρύπων.....	24
2.4.2.2 Παρακολούθηση δασών	24
2.4.2.3 Παρακολούθηση φαινόμενου θερμοκηπίου	24
2.4.2.4 Παρακολούθηση κατολισθήσεων	24
2.4.3 Άλλες πιθανές εφαρμογές.....	25
2.5 Χαρακτηριστικά των δικτύων αισθητήρων	25
2.6 Γενικά περί ασφάλειας δικτύου.....	25
2.7 Ζητήματα ασφάλειας και διατήρησης απορρήτου σε δίκτυα αισθητήρων	26
2.8 Έκθεση σε κίνδυνο του κόμβου σε δίκτυο SN	26
2.9 Υποκλοπή	27
2.10 Απόρρητο των δεδομένων.....	28
2.11 Επιθέσεις τύπου DoS (Denial of Service)	29
2.12 Επίβουλη χρήση καταναλωτικών δικτύων	29
2.13 Περί ασφαλούς επικοινωνίας σε ασύρματα.....	31
ad-hoc δίκτυα αισθητήρων	31
2.14 Αρχιτεκτονική του δικτύου αισθητήρων	32
2.14.1 Εντοπισμένοι αλγόριθμοι	32
2.14.2 Τοπικό μοντέλο μετάδοσης επικοινωνίας	32
2.14.3 Mobile Code.....	32
2.15 Απειλές ασφάλειας	33
2.16 Σχήμα Ασφάλειας Επικοινωνίας	33
2.16.1 Επίπεδο ασφάλειας I	35
2.16.2 Επίπεδο ασφάλειας II.....	35
2.16.3 Επίπεδο ασφάλειας III	36
2.17 Ασφαλής δρομολόγηση σε ασύρματα δίκτυα αισθητήρων	36
2.17.1 Παραποιημένη, αλλαγμένη ή αναπαραχθείσα πληροφορία δρομολόγησης	37
2.17.2 Επιλεκτική προώθηση.....	37
2.17.3 Επιθέσεις τύπου καταβόθρας (sinkhole)	38
2.17.4 Επιθέσεις Σίββυλας (Sibyl attacks).....	39

2.17.5 Επιθέσεις Wormholes.....	39
2.17.6 Επίθεση τύπου HELLO flood	40
2.17.7 Επιθέσεις με παραποίηση αναγνώρισης (acknowledgment spoofing).....	40
2.18 Επιθέσεις σε συγκεκριμένα πρωτόκολλα δικτύου	41
2.18.1 TinyOS beaconing	41
2.18.2 Directed Diffusion	41
2.18.3 Geographic routing (GEAR , Geographic and energy aware routing/ GPSR , greedy perimeter stateless routing)	42
2.18.4 Minimum Cost forwarding	42
2.19 Μέτρα αντιμετώπισης απειλών δρομολόγησης σε δίκτυα αισθητήρων.....	42
2.20 Ασφαλής ομαδοποίηση δεδομένων (Data Aggregation) στα Ασύρματα Δίκτυα αισθητήρων	43
2.21 Ασφαλής Εντοπισμός (Localization) στα Ασύρματα Δίκτυα αισθητήρων.....	46
2.22 Διαθέσιμα Ασφαλή Συστήματα Εντοπισμού	47
2.22.1 SeRLoc.....	47
2.22.2 Beacon Suite	48
2.22.3 Attack Resistant Location Estimation	48
2.22.4 Robust Statistical Methods.....	48
2.22.5 SPINE	48
2.22.6 ROPE.....	49
2.22.7 Transmission Range Variation	49
2.22.8 DRBTS.....	49
2.22.9 HiRLoc.....	49
2.23 Σύνοψη	49
ΚΕΦΑΛΑΙΟ 3 : ZigBee και IEEE 802.15.4	50
3.1 Τι είναι το ZigBee	50
3.2 Τυπικές εφαρμογές	51
3.3 Κίνητρα για ZigBee	51
3.4 The ZigBee Protocol Stack	52
3.4.1 Application (APL) Layer	53
3.4.2 Application Framework.....	53
3.4.3 Application Objects.....	53
3.4.4 ZigBee Device Object (ZDO)	53
3.4.5 ZDO Management Plane.....	53
3.4.6 Application Support (APS) Sublayer.....	53
3.4.7 Security Service Provider (SSP).....	53
3.4.8 Network (NWK) Layer	54
3.5 IEEE 802.15.4	54
3.5.1 Medium Access Control (MAC) Layer.....	54
3.5.1.1 Design Drivers	55
3.5.2 Physical (PHY) Layer.....	55
3.6 The ZigBee Network.....	57
3.6.1 Τύποι συσκευών	57
3.6.1.1 Συντονιστής.....	57
3.6.1.2 Δρομολογητής.....	57
3.6.1.3 Τερματικές συσκευές	57
3.6.2 Κατηγορίες συσκευών.....	57
3.6.2.1 Συσκευή πλήρους λειτουργίας (FFD).....	57
3.6.2.2 Συσκευή μειωμένης λειτουργίας (RFD)	58
3.6.3 Typical Network Topologies	58
3.6.4 Οφέλη	61

3.7 Συνδέσεις.....	61
3.7.1 Broadcast.....	61
3.7.2 Unicast.....	62
3.7.2.1 Network Address Discovery.....	62
3.7.2.2 Route Discovery.....	62
3.7.2.3 Retries and ACKs.....	63
3.7.3 Many to one.....	63
3.8 Συγκριτικός πίνακας.....	64
3.9 Ασφάλεια Zigbee.....	65
3.9.1 Κέντρο αξιοπιστίας.....	65
3.9.2 Κλειδιά ασφαλείας.....	65
3.9.2.1 Master Keys.....	66
3.9.2.2 Network Keys.....	66
3.9.2.3 Link Keys.....	66
3.9.3 Security Modes.....	66
3.9.3.1 Standard Security Mode.....	66
3.9.3.2 High Security Mode.....	67
ΚΕΦΑΛΑΙΟ 4 : Γενικά Χαρακτηριστικά- Hardware.....	68
4.1 Προδιαγραφές Waspnote.....	68
4.2 Block Diagram.....	69
4.3 Ηλεκτρικά δεδομένα.....	70
4.3.1 Πειραματικές τιμές.....	70
4.3.2 Απόλυτες μέγιστες τιμές.....	70
4.4 ATmega1281.....	71
4.4.1 Γενικά χαρακτηριστικά.....	71
4.4.2 Κεντρική Μονάδα Επεξεργασίας (CPU - Central Processing Unit).....	73
4.4.3 Μνήμες.....	75
4.4.4 Σύστημα χρονισμού.....	77
4.4.5 Διακοπές και Επανατοποθέτηση.....	79
4.4.6 Μονάδα σύγχρονης και ασύγχρονης επικοινωνίας (Universal Synchronous & Asynchronous Receiver Transmitter - USART).....	80
4.4.7 Διεπαφή I ² C.....	81
4.4.8 Μετατροπέας αναλογικού σήματος σε ψηφιακό (ADC - Analog to Digital Converter).....	83
4.4.9 Διεπαφή JTAG.....	84
4.4.10 Πρόγραμμα εκκίνησης (Boot Loader).....	85
4.5 Αισθητήρες.....	87
4.5.1 Θερμοκρασίας.....	87
4.5.1.1 RTC.....	88
4.5.2 Επιταχυνσιόμετρο.....	88
4.6 LEDs.....	93
4.7 Prototyping Board 2.0.....	94
4.7.1 Γενική περιγραφή.....	94
4.7.2 Προδιαγραφές.....	95
4.7.3 Ηλεκτρικά χαρακτηριστικά.....	95
4.7.4 Prototyping area.....	96
4.7.4.1 Pads Area.....	96
4.7.4.2 Integrated Circuits Area.....	98
4.7.5 Analog-to-Digital Converter.....	99
4.8 XBee Module - ZB Series 2.....	100
4.8.1 Γενικά.....	100
4.8.2 Τεχνικά χαρακτηριστικά.....	101
4.8.2.1 Επιδόσεις.....	101

4.8.2.2 Χαρακτηριστικά.....	101
4.8.2.3 Λογισμικό	101
4.8.2.4 Δίκτυα και ασφάλεια.....	101
4.8.2.5 Απαιτήσεις ισχύος.....	102
4.8.3 XBee ZB Hardware και Pin Layout	102
ΚΕΦΑΛΑΙΟ 5 : Λογισμικό-Μετρήσεις	104
5.1 Setup πειράματος.....	104
5.2 Λογισμικό.....	106
5.3 Πειραματικές μετρήσεις και αποτελέσματα	109
5.3.1 Κατασκευή Serial Monitor	109
5.3.2 Εμφάνιση αποτελεσμάτων	112
ΚΕΦΑΛΑΙΟ 6 : Γενικά Συμπεράσματα	116
Βιβλιογραφία – Πηγές	118

ΚΕΦΑΛΑΙΟ 1 : Εισαγωγή

1.1 Μικροεπεξεργαστές

Τα τελευταία χρόνια η επανάσταση στον τομέα υπολογιστών συντέλεσε στην παραγωγή νέας γενιάς υπολογιστών που έχουν ταχύτητες και υπολογιστική ισχύ χιλιάδες φορές μεγαλύτερη από εκείνη των πρώτων εμπορικών υπολογιστών. Αυτό ήταν αποτέλεσμα των ολοκληρωμένων κυκλωμάτων που συνδυάζουν ένα μεγάλο αριθμό δυνατοτήτων πάνω σε μια φέτα πυριτίου (chip), και ειδικότερα στη δημιουργία και αλματώδη εξέλιξη των μικροεπεξεργαστών (microprocessors).

Σήμερα διατίθεται μια πλειάδα μικροελεγκτών που ενσωματώνουν στο ίδιο ολοκληρωμένο κύκλωμα την CPU μαζί με έναν αριθμό περιφερειακών, (μνήμη, χρονιστές/μετρητές, ακροδέκτες γενικής χρήσεως, DAC και ADC, σειριακές και παράλληλες Θύρες επικοινωνίας κ.α). Διαλέγοντας τον κατάλληλο μικροελεγκτή για μία εφαρμογή μπορεί να ελαχιστοποιηθεί το πλήθος των απαιτούμενων εξωτερικών εξαρτημάτων

Ένα χαρακτηριστικό παράδειγμα σύγχρονων μικροελεγκτών είναι εκείνοι της οικογένειας AVR της εταιρείας ATMEL. Οι μικροελεγκτές αυτοί προσφέρονται με ένα πλήθος εναλλακτικού αριθμού ακροδεκτών, ξεκινώντας από μικρά και φτηνά ολοκληρωμένα των 8 ακροδεκτών για εφαρμογές πολύ χαμηλού κόστους με περιορισμένες απαιτήσεις και φτάνοντας σε πλήθος προγραμματιζόμενων ακροδεκτών γενικού σκοπού. Οι πιο εξελιγμένοι μικροελεγκτές της οικογένειας διαθέτουν περισσότερους από 60 προγραμματιζόμενους ακροδέκτες γενικού σκοπού. Επίσης πολλά μέλη της σειράς διατίθενται σε τρεις παραλλαγές: τους απλούς μικροελεγκτές που λειτουργούν στα 5V, τους χαμηλής κατανάλωσης στα 2.7V (κατάληξη L) και τους πολύ χαμηλούς με κατανάλωση στα 1.8V (κατάληξη V). Συνήθως οι ακροδέκτες γενικού σκοπού έχουν περισσότερες από μία λειτουργίες, όπως για παράδειγμα είσοδοι με ικανότητα να προκαλούν διακοπή (interrupt) στον εσωτερικό επεξεργαστή, είσοδοι αναλογικών συγκριτών ή μετατροπέων αναλογικού σε ψηφιακό (ADC), είσοδοι κεντρικού u961 ρολογιού (oscillator) ή ασύγχρονης οδήγησης μετρητών (counters), ακροδέκτες για σύνδεση με διάφορες διεπαφές όπως USART, SPI κ.α. Στα πιο εξελιγμένα μέλη της οικογένειας διατίθενται ενσωματωμένα περιφερειακά ακόμα και για την οδήγηση LCD οθόνης ή τη σύνδεση με USB interface. Στο εσωτερικό ενός μικροελεγκτή όπως ο AVR υπάρχει ένας αριθμός από διαφορετικούς τύπους μνήμης, όπως Flash για την εγγραφή του λογισμικού συστήματος (firmware), EEPROM για την αποθήκευση διαφόρων παραμέτρων, καθώς και κάποιος αριθμός θέσεων μνήμης Ram για τις μεταβλητές του λογισμικού. Για το λόγο αυτό οι AVR δεν βγάζουν σε ακροδέκτες την εσωτερική αρτηρία διευθύνσεων ή δεδομένων παρά μόνο ακροδέκτες γενικού σκοπού. Με όλα τα παραπάνω περιφερειακά είναι φανερό ότι το πλήθος των εξωτερικών στοιχείων που απαιτούνται για τη δημιουργία ενός συστήματος με μικροελεγκτή AVR είναι ελάχιστο. Το βασικό μειονέκτημα μιας τέτοιας αρχιτεκτονικής μικροελεγκτή είναι η δυσκολία επεκτασιμότητας. Π.χ, αν οι απαιτήσεις σε μνήμη RAM είναι μεγάλες, ο μικροελεγκτής δεν είναι εύκολο να συνδεθεί με εξωτερική μνήμη, μια και δεν έχει

αρτηρία διευθύνσεων και δεδομένων. Για να γίνει αυτό θα πρέπει να υλοποιηθούν τέτοιες αρτηρίες με τη χρήση ακροδεκτών γενικού σκοπού οι οποίες ωστόσο θα ήταν αδύνατο να επιτύχουν γρήγορους χρόνους προσπέλασης της μνήμης. Επίσης η συχνότητα ρολογιού στην οποία λειτουργούν τέτοιοι μικροελεγκτές δεν ξεπερνά τα 20 MHz στα πιο εξελιγμένα μοντέλα μιας σειράς όπως οι AVR mega.

1.2 Δίκτυα αισθητήρων

Τα δίκτυα μικροηλεκτρονικών αισθητήρων αποτελούν μια ευρεία και δημοφιλή ερευνητική περιοχή των μικροσυστημάτων, της πληροφορικής και όχι μόνο. Τα τελευταία χρόνια, η περιοχή αυτή έχει αποκτήσει έντονο ενδιαφέρον λόγω των πολλών εφαρμογών και ευκαιριών για εμπλοκή από ερευνητές διαφόρων κλάδων της μικροηλεκτρονικής και των μικροσυστημάτων γενικότερα.

Αισθητήρας γενικά ονομάζεται η ηλεκτρονική συσκευή που έχει τη δυνατότητα να παρατηρεί και να καταγράφει/αναφέρει κάποια παράμετρο του περιβάλλοντος όπως θερμοκρασία, υγρασία, ήχο, εικόνα (video), πίεση, ύπαρξη συγκεκριμένων αερίων κλπ. Οι μετρήσεις που λαμβάνονται από τον καθένα από αυτούς μπορεί να χρησιμοποιηθεί με πολλούς τρόπους και να αξιοποιηθεί ανάλογα.

Από την άλλη, δίκτυο αισθητήρων είναι ένα σύνολο από μικροεπεξεργαστές οι οποίοι εφοδιάζονται με ένα ή περισσότερους αισθητήρες καθώς και την δυνατότητα της μεταξύ τους επικοινωνίας. Ενώ οι μικροηλεκτρονικοί αισθητήρες λειτουργούν σε πληροφορικά συστήματα εδώ και πολλά χρόνια, το έντονο ερευνητικό ενδιαφέρον των τελευταίων ετών έγκειται κυρίως στους εξής λόγους.

- Η ταχεία ανάπτυξη της τεχνολογίας των μικροεπεξεργαστών που ενώ παρουσιάζονται συνεχώς με μικρότερο μέγεθος, εφοδιάζονται με ισχυρότερους επεξεργαστές, μεγαλύτερη μνήμη καθώς και ενσωματωμένες επιπλέον δυνατότητες όπως ασύρματη επικοινωνία και δυνατότητα επαναπρογραμματισμού. Παρά το γεγονός αυτό, το κόστος παραγωγής πέφτει αισθητά. Η τελευταία παρατήρηση είναι η πλέον κρίσιμη καθώς επιτρέπει τη δημιουργία προσωρινών και αναλώσιμων δικτύων από τέτοιες συσκευές σε ad-hoc περιβάλλοντα.
- Η ανάπτυξη και βελτίωση των μεταφερόμενων πηγών ενέργειας (μπαταρίες) που επιτρέπει την αυτόνομη λειτουργία των μικροσυσκευών για εκτεταμένο χρονικό διάστημα, σε πολλές περιπτώσεις, χρόνια χωρίς ανθρώπινη επίβλεψη. Η ανάγκη για εφαρμογές που απαιτούν τη λειτουργία παρακολούθησης του περιβάλλοντος με μεγάλη λεπτομέρεια και χρονική διάρκεια (όπως παρακολούθηση δύσβατων δασικών περιοχών, θαλάσσιος βυθός, ζώα που μετακινούνται αλλά και κατασκόπευση σε πεδία μαχών) μπόρεσαν να εκμεταλλευτούν και να επιβάλουν αυτή τη δυνατότητα.
- Η ραγδαία ανάπτυξη των ασύρματων επικοινωνιών και των μικρομηχανικών συστημάτων – micromechanical systems (MEMs), έγινε εφικτή η κατασκευή χαμηλού κόστους, χαμηλής κατανάλωσης ενέργειας, πολυλειτουργικών και μικροσκοπικών αισθητήρων.

Κάποια, λοιπόν, συγκεκριμένα χαρακτηριστικά ορίζουν το ελάχιστο πλαίσιο των μοντέρνων δικτύων μικροηλεκτρονικών αισθητήρων.

- Η ύπαρξη ολοκληρωμένου ενσωματωμένου μικροεπεξεργαστή και μνήμης.
- Η ύπαρξη ενός ή περισσότερων ενσωματωμένων αισθητήρων και μέθοδοι πρόσβασης στις τιμές που μετρούνται.
- Η δυνατότητα ασύρματης επικοινωνίας και πρωτοκόλλου επικοινωνίας με άλλους κόμβους.
- Η δυνατότητα προγραμματισμού και επαναπρογραμματισμού στο επίπεδο βασικού συστήματος λειτουργίας.
- Αυτονομία με χρήση μπαταρίας για ανεξάρτητη λειτουργία για εκτεταμένο χρονικό διάστημα.
- Το μικρό μέγεθος και το εξαιρετικά μικρό κόστος αγοράς ανά συσκευή.

1.3 Στρατηγική έρευνα

Σαφώς, πολλές περιοχές της έρευνας εμπλέκονται στην ανάπτυξη τέτοιων δικτύων. Αρχικά, στην περιοχή των ενσωματωμένων συστημάτων (embedded hardware systems) νέες τεχνολογίες για ταχύτερο υπολογισμό, μικρότερη κατανάλωση ενέργειας και αποτελεσματική διαχείριση των πόρων του κατώτερου (φυσικού) επιπέδου είναι αναγκαία. Η περιοχή των ασύρματων και κινητών δικτύων υπολογισμού επικεντρώθηκε στην επέκταση των πολύ δημοφιλών λύσεων για κινητούς υπολογιστές σε μικροεπεξεργαστές ούτως ώστε να μειώσουν στο ελάχιστο την κατανάλωση ενέργειας. Τα διάφορα πρωτόκολλα για δρομολόγηση πακέτων, ανταλλαγή πληροφοριών και συντονισμού διαφοροποιήθηκαν ή ανασχεδιάστηκαν ώστε να μειώσουν στο ελάχιστο την εκπομπή μηνυμάτων που αποτελεί τη βασική πηγή κατανάλωσης ενέργειας. Τα νέα πρωτόκολλα επικοινωνίας σχετίζονται επίσης με την περιοχή του διάχυτου υπολογισμού όπου οι αισθητήρες αποτελούν αυτόνομους επικοινωνιακούς κόμβους και απαιτούν συντονισμό για την επίτευξη ενός κοινού σκοπού. Επιπλέον, η συγκέντρωση και συλλογή πληροφοριών από αισθητήρες απαιτεί νέες τεχνολογίες στον τομέα των βάσεων δεδομένων και της διαχείρισης των δεδομένων αυτών. Ο μεγάλος αριθμός των αισθητήρων που έχουν επίσης αναπτυχθεί και οι οποίοι επιτρέπουν τη λήψη πολλών διαφορετικών δεδομένων από ένα μόλις διασυνδεδεμένο δίκτυο, όπως και η ανάπτυξη της νανοτεχνολογίας, που έχει οδηγήσει στην κατασκευή αισθητήρων πολύ μικρών διαστάσεων κατάλληλους για οποιαδήποτε μέτρηση ακόμα και σε πολύ μικρές διαστάσεις. Τέλος, μέθοδοι οργάνωσης, παρακολούθησης και οπτικοποίησης των δεδομένων αλλά και συστήματα διασυνδετικής διάταξης για ευκολότερη πρόσβαση από τους τελικούς χρήστες βρίσκονται υπό ανάπτυξη.

1.4 Αισθητήρες

1.4.1 Θερμοκρασίας

Οι αισθητήρες τύπου θερμοκρασίας, μέσω κατάλληλης διάταξης μπορούν να καταγράφουν τις εξωτερικές συνθήκες θερμοκρασίας. Πιο συγκεκριμένα με ειδικές μικροηλεκτρονικομηχανικές διατάξεις (MEMS) πραγματοποιείται ο προσδιορισμός της θερμοκρασίας σε συγκεκριμένα σημεία ή περιοχές και η μετέπειτα εξαγωγή της τιμής του μετρούμενου μεγέθους ως συνάρτηση αυτών. Με τον τρόπο αυτό οι ανιχνεύμενες μεταβολές στη θερμοκρασία προκύπτουν ως αποτέλεσμα της επίδρασης των μηχανισμών διάδοσης της θερμότητας, δηλαδή της αγωγής, της διαγωγής και της ακτινοβολίας.

1.4.2 Χωρητικότητας

Οι αισθητήρες τύπου χωρητικότητας αποτελούν ειδικές μικροηλεκτρονικομηχανικές διατάξεις (MEMS) στις οποίες η μεταβολή μιας φυσικής ποσότητας προκαλεί αντίστοιχη μεταβολή στην χωρητικότητα των αισθητήρων. Ανάλογα με την υλοποίηση του αισθητήρα αυτός μπορεί να μετρήσει με μεγάλη ακρίβεια φυσικές ποσότητες όπως η πίεση, η δύναμη, η ροή κάποιου ρευστού ή με ειδικές διατάξεις μπορεί να ανιχνεύσει χημικές ενώσεις ακόμα και για βιολογικούς σκοπούς.

1.4.3 Επιταχυνσιόμετρο

Το επιταχυνσιόμετρο είναι μια μικροηλεκτρονικομηχανική διατάξη (MEM) που έχει την ικανότητα να μετρά δυνάμεις επιτάχυνσης. Αυτές οι δυνάμεις μπορεί να είναι στατικές, όπως είναι η επιτάχυνση της βαρύτητας, οι δυναμικές όταν προκαλούνται – προέρχονται από αλλαγές στην ταχύτητα ή στη διεύθυνση της κίνησης (επιταχύνσεις, επιβραδύνσεις, στροφές). Υπάρχουν διάφοροι τρόποι να υλοποιηθεί ένα επιταχυνσιόμετρο. Ένας τρόπος είναι η αξιοποίηση του πιεζοηλεκτρικού φαινομένου. Αυτά χρησιμοποιούν πιεζοκρύσταλο ο οποίος πιέζεται από μάζα ανάλογη της επιτάχυνσης που δέχεται αυτή και παράγει τάση λόγω πιεζοηλεκτρικού φαινομένου ανάλογη της επιτάχυνσης.

1.5 Εφαρμογές

Τα πεδία στα οποία μπορούν να βρουν εφαρμογή τα δίκτυα των αισθητήρων είναι πάρα πολλά και μπορούν να καλύψουν κάθε είδους απαιτήσεις. Εφαρμογές τους υπάρχουν σε όλους τους τομείς της τεχνολογίας. Ακόμα και όταν αναφερόμαστε σε δίκτυα που απαιτούν ενσύρματη δικτύωση, είναι πάρα πολλές οι λύσεις που μπορούν να προσφέρουν. Πόσο μάλλον όταν γίνεται επέκταση και στα ασύρματα δίκτυα.

Ενδεικτικά μπορούμε να αναφέρουμε:

- Εφαρμογές ασφαλείας (Security Applications).
- Βιομηχανικός έλεγχος (Industrial Control).
- Έλεγχος οδικής κυκλοφορίας (Traffic Control).
- Δομικά συστήματα παρακολούθησης υγείας (Structural Health Monitoring).
- Παρακολούθηση περιβαλλοντικών συνθηκών (Environmental Monitoring).

ΚΕΦΑΛΑΙΟ 2 : Δίκτυα Αισθητήρων

Τα δίκτυα αισθητήρων (sensor networks) έχουν αναγνωρισθεί ως μια από τις πιο σημαντικές τεχνολογίες του 21ου αιώνα. Η εξέλιξη των δικτύων αυτών απαιτεί τεχνολογίες από 3 διαφορετικές περιοχές έρευνας: των αισθητήρων, των επικοινωνιών και των υπολογιστών (συμπεριλαμβανομένου hardware, software και αλγορίθμων). Τα επιτεύγματα σε κάθε μία από αυτές τις περιοχές (ξεχωριστά αλλά και σε συνδυασμό) έχουν δώσει μεγάλη ώθηση στην ανάπτυξη πολλών εφαρμογών που βασίζονται στα sensor networks.

Από τις πρώτες στρατιωτικές εφαρμογές της τεχνολογίας αυτής, όπως του SOSUS, (Sound Surveillance System) ένα σύστημα ακουστικών αισθητήρων (hydrophones) τοποθετημένων στον πυθμένα του ωκεανού σε στρατηγικά σημεία για την ανίχνευση και εύρεση της διαδρομής των Σοβιετικών υποβρυχίων κατά τη διάρκεια του ψυχρού πολέμου, έως τις σημερινές εφαρμογές που βασίζονται στα MEMS (microelectromechanical system) έχει σημειωθεί σημαντική πρόοδος και αύξηση του πεδίου εφαρμογών.

2.1 Εισαγωγή

Ένα δίκτυο αισθητήρων (sensor network) αποτελείται από μια ομάδα καταναμημένων στο χώρο αυτόνομων και εξειδικευμένων transducers (αισθητήρες-μετατροπείς) οι οποίοι παρακολουθούν και καταγράφουν φυσικές ή περιβαλλοντικές συνθήκες. Σε αυτό το δίκτυο υπάρχει μια υποδομή επικοινωνίας και οι αισθητήρες συνεργάζονται έτσι ώστε να μεταφέρουν τα δεδομένα που καταγράφουν σε μια κύρια τοποθεσία.

Οι συνήθεις παράμετροι που παρακολουθούνται είναι:

- θερμοκρασία, υγρασία, πίεση
- η κατεύθυνση και ταχύτητα ανέμου
- ένταση: φωτισμού, δόνησης, ήχου
- η τάση γραμμής μεταφοράς ρεύματος
- οι συγκεντρώσεις χημικών
- τα επίπεδα των ρύπων
- οι ζωτικές λειτουργίες του σώματος

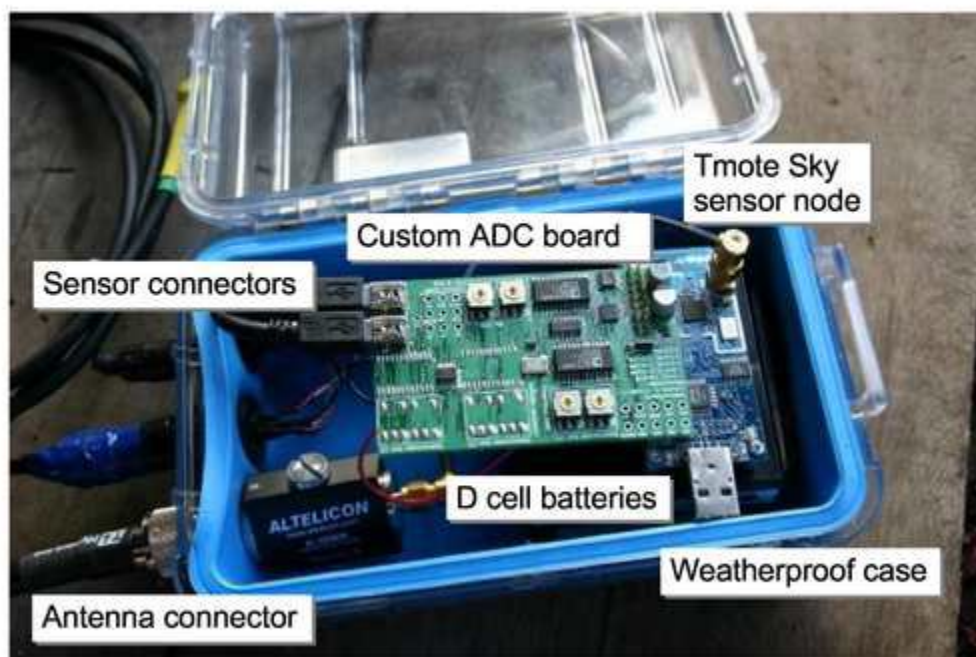
Ένα δίκτυο αισθητήρων αποτελείται από πολλαπλούς σταθμούς ανίχνευσης που ονομάζονται κόμβοι (sensor nodes). Συνήθως οι κόμβοι είναι φορητοί, μικρού μεγέθους και βάρους. Κάθε κόμβος είναι εφοδιασμένος με ένα αισθητήρα-μετατροπέα (transducer), ένα μικροϋπολογιστή, ένα πομποδέκτη (transceiver) και μια πηγή τροφοδοσίας.

Για να ολοκληρώσουμε τη θεώρηση του δικτύου πρέπει να συμπεριλάβουμε και ένα κεντρικό υπολογιστή στον οποίο θα καταλήγουν όλες οι καταγραφές των κόμβων.

Ο μετατροπέας (transducer) μετατρέπει σε ηλεκτρικό σήμα την είσοδο που παίρνει από τα φυσικά φαινόμενα που παρακολουθεί.

Ο μικροϋπολογιστής επεξεργάζεται και αποθηκεύει το σήμα εξόδου του αισθητήρα.

Ο πομποδέκτης, που μπορεί να είναι συνδεδεμένος ενσύρματα ή ασύρματα, μεταδίδει τα δεδομένα στον κεντρικό υπολογιστή. Στην περίπτωση που ο πομποδέκτης συνδέεται ασύρματα θα πρέπει να έχει επιπλέον μια εσωτερική κεραία ή μια σύνδεση σε κάποια εξωτερική κεραία. Η ηλεκτρική ισχύς που απαιτείται για τη λειτουργία του κάθε κόμβου-αισθητήρα προέρχεται είτε από το δημόσιο ηλεκτρικό δίκτυο ή από μια μπαταρία.



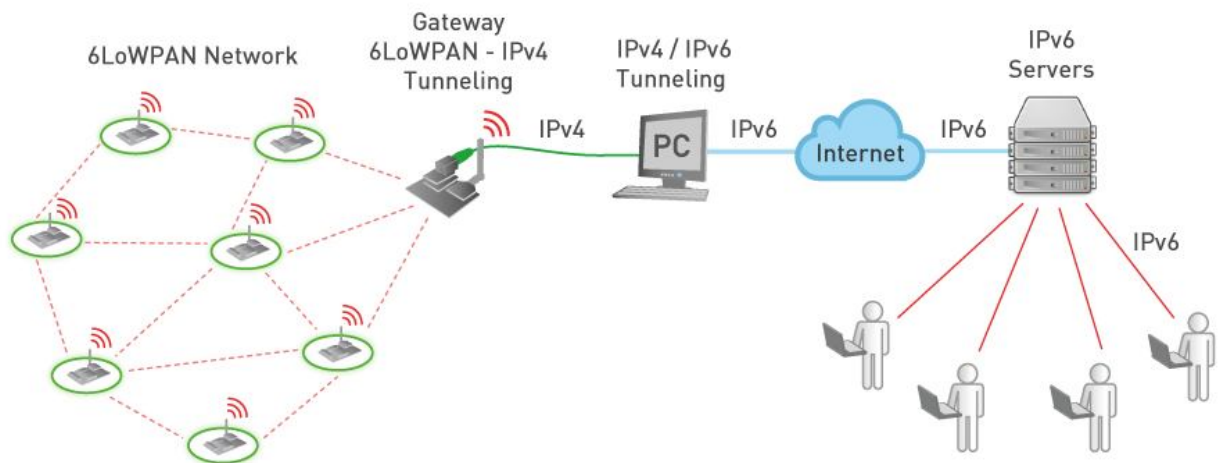
Εικόνα 1: Εξοπλισμός κόμβου αισθητήρα

Τα πιο σύγχρονα δίκτυα είναι αμφίδρομης επικοινωνίας. Ο κάθε κόμβος επικοινωνεί με τον κεντρικό υπολογιστή όχι μόνο για να μεταδώσει τα δεδομένα που έχει καταγράψει αλλά και να δεχτεί εντολές από αυτόν, έτσι ώστε να είναι δυνατή η διαδικασία ελέγχου του αισθητήρα από μακριά.

Αυτή η απαίτηση καθώς επίσης και το γεγονός ότι η χρήση των sensor networks προορίζεται για περιοχές πολύ απομακρυσμένες ή δυσπρόσιτες με μεγάλη πιθανότητα να είναι εκτός του δημόσιου δικτύου ηλεκτροδότησης επέβαλε τη χρήση των ασυρμάτων δικτύων (Wireless Sensor Networks) που θα αναφέρονται από δω και πέρα για συντομία WSN.

Σε ένα τυπικό WSN οι κόμβοι επικοινωνούν ασύρματα με μία κεντρική πύλη η οποία συνδέεται ενσύρματα (συνήθως μέσω Ethernet) με τον κεντρικό υπολογιστή όπου συλλέγονται, αναλύονται και παρουσιάζονται τα δεδομένα των μετρήσεων που καταγράφηκαν στους κόμβους.

Σε περίπτωση που απαιτείται να αυξηθεί η απόσταση του WSN από την κεντρική πύλη (central gateway) ή θέλουμε να αυξήσουμε την αξιοπιστία του δικτύου χρησιμοποιούνται οι δρομολογητές (routers) για μια πρόσθετη σύνδεση επικοινωνίας μεταξύ των κόμβων και της κεντρικής πύλης.



Εικόνα 2: Μια συνήθης αρχιτεκτονική για WSN

2.2 Τοπολογίες

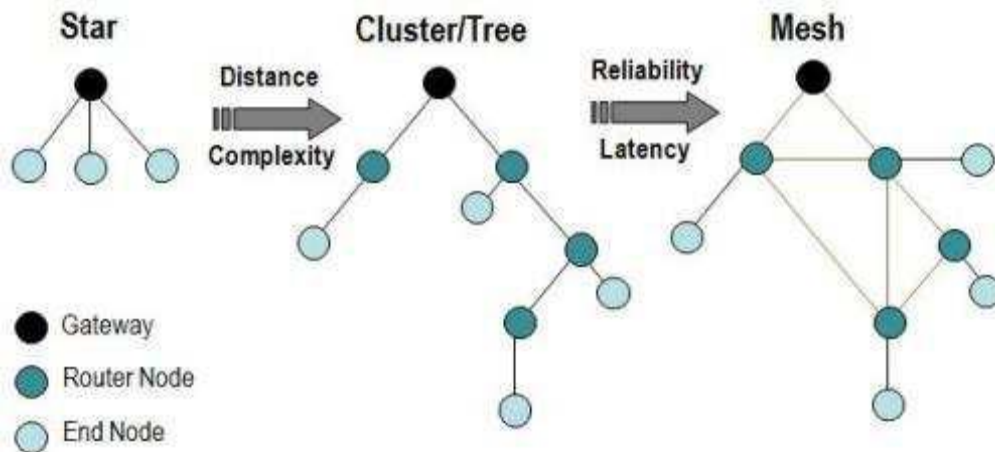
Υπάρχουν διάφορες επιλογές τοπολογίας για το συντονισμό των τελικών κόμβων, των κόμβων του δρομολογητή και της κεντρικής πύλης σε ένα WSN που μπορούν να χρησιμοποιηθούν. Οι κόμβοι δρομολογητή είναι παρόμοιοι με αυτούς των τελικών κόμβων επειδή κι αυτοί μπορούν να έχουν δεδομένα μετρήσεων αλλά μπορούν να χρησιμοποιηθούν για να περάσουν τα δεδομένα από άλλους κόμβους.

Η πιο απλή τοπολογία είναι αυτή του αστέρα στην οποία κάθε κόμβος διατηρεί ένα απευθείας μονοπάτι επικοινωνίας με την κεντρική πύλη. Ο περιορισμός αυτής της τοπολογίας είναι προφανώς η μικρή συνολική απόσταση που μπορεί να καλύπτει το δίκτυο.

Για να αυξήσουμε την απόσταση που μπορεί να καλύψει ένα WSN μπορούμε να επιλέξουμε μια τοπολογία cluster ή δένδρου. Σε αυτές κάθε κόμβος διατηρεί ένα απευθείας μονοπάτι επικοινωνίας με την κεντρική πύλη αλλά μπορεί να χρησιμοποιεί άλλους κόμβους για να δρομολογήσει τα δεδομένα του κατά μήκος του μονοπατιού αυτού. Βασικό πρόβλημα αυτής της τοπολογίας είναι ότι σε περίπτωση βλάβης κάποιου δρομολογητή όλοι οι κόμβοι που τον χρησιμοποιούν θα χάσουν το μονοπάτι επικοινωνίας με την κεντρική πύλη.

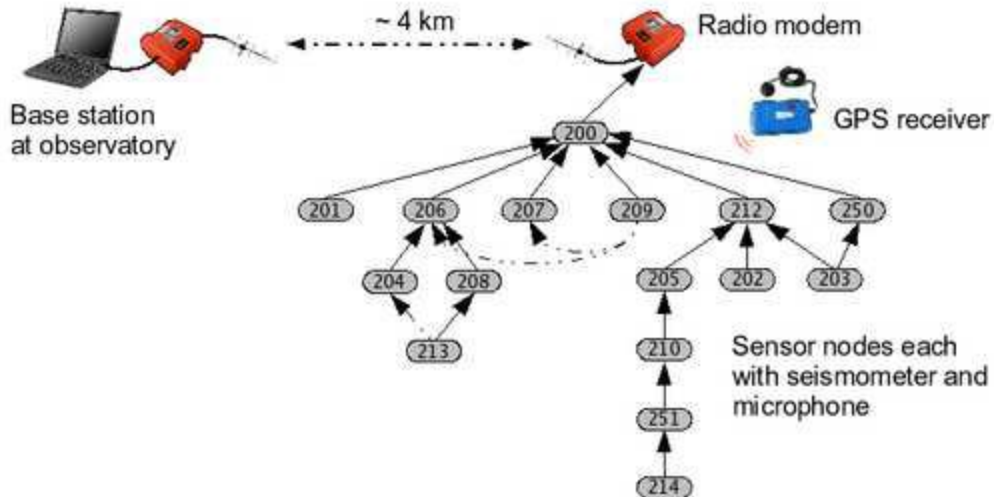
Η τοπολογία δικτύου βρόχων (mesh network) λύνει το παραπάνω πρόβλημα χρησιμοποιώντας επιπλέον εναλλακτικά μονοπάτια προς την πύλη και αυξάνοντας έτσι την αξιοπιστία του δικτύου.

Σε ένα δίκτυο βρόχων οι κόμβοι διατηρούν πολλαπλά μονοπάτια προς την πύλη έτσι σε περίπτωση που πέσει ένας κόμβος δρομολογητή, το δίκτυο να επαναδρομολογήσει τα δεδομένα από διαφορετικό μονοπάτι. Η αύξηση στην αξιοπιστία που προσφέρει όμως αυτή η τοπολογία έχει το κόστος της καθυστέρησης (network latency) επειδή τα δεδομένα πρέπει να κάνουν πολλαπλά hops ώσπου να φτάσουν στην πύλη.



Εικόνα 3: Τοπολογίες δικτύου αισθητήρων

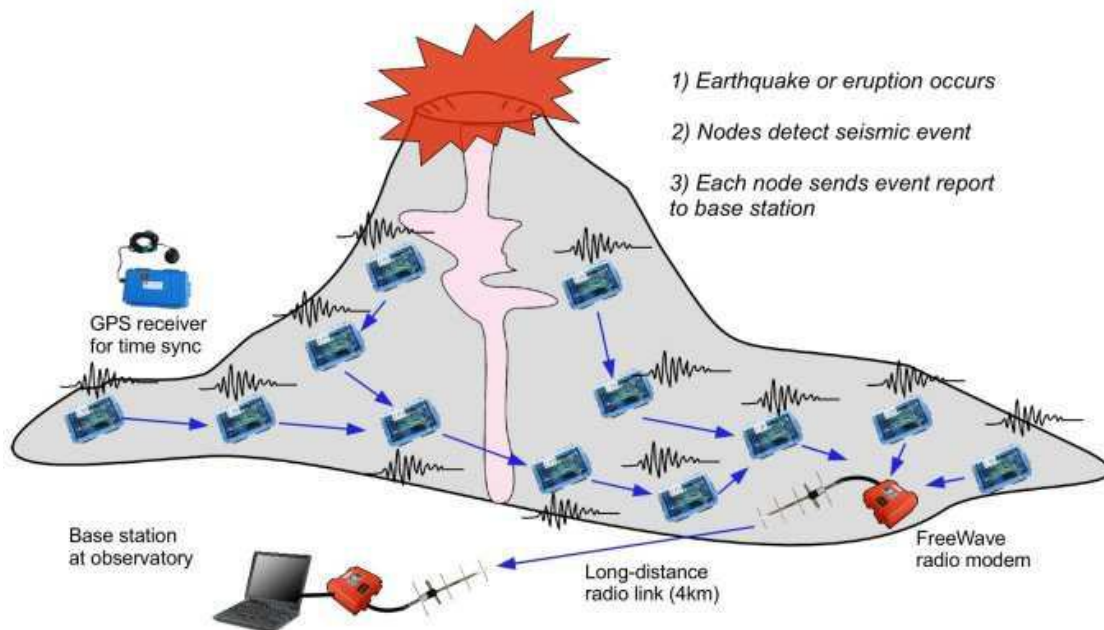
Το παρακάτω παράδειγμα τοπολογίας προέρχεται από μια εργασία όπου χρησιμοποιήθηκε ένα sensor network για την παρακολούθηση της δραστηριότητας του ενεργού ηφαιστείου Reventador στο Εκουαδόρ επί 19 μέρες (Geoff Werner-Allen, Konrad Lorincz, Jeff Johnson, Jonathan Lees, and Matt Welsh: Fidelity and Yield in a Volcano Monitoring Sensor Network).



Εικόνα 4: Η τοπολογία δικτύου που χρησιμοποιήθηκε στο Reventador.

Οι κόμβοι σχηματίζουν μια τοπολογία δρομολόγησης multihop μεταφέροντας τα δεδομένα στο παρατηρητήριο μέσω ενός radio modem μεγάλων αποστάσεων. Χρησιμοποιήθηκε ένας δέκτης GPS για συγχρονισμό (global time base)

Καθένας από τους 16 αισθητήρες κατέγραφε συνεχώς δείγματα σεισμικών και ηχητικών δεδομένων στα 100 Hz. Οι κόμβοι χρησιμοποιούσαν έναν αλγόριθμο ανίχνευσης γεγονότος (event detection) για να ενεργοποιήσουν την καταγραφή μιας ενδιαφέρουσας ηφαιστειακής δραστηριότητας και να ξεκινήσουν την αξιόπιστη μεταφορά δεδομένων στο σταθμό βάσης. Κατά τη διάρκεια της επιχείρησης, το δίκτυο κατέγραψε 229 σεισμούς, εκρήξεις και άλλα σεισμό-ακουστικά γεγονότα.



Εικόνα 5: sensor network για την παρακολούθηση της δραστηριότητας του ενεργού ηφαιστείου Reventador

2.3 Τρόποι μετάδοσης στα δίκτυα αισθητήρων - ομοιότητες και διαφορές ad-hoc WSN

Η κύρια μέθοδος επικοινωνίας είναι η multihop δικτύωση. Στα δίκτυα αισθητήρων έχουν ένα πιο συγκεκριμένο πρότυπο επικοινωνίας ενώ τα ad-hoc ασύρματα δίκτυα αισθητήρων υποστηρίζουν τη δρομολόγηση μεταξύ οποιουδήποτε ζεύγους κόμβων. Στα δίκτυα αισθητήρων η κίνηση μπορεί να κατηγοριοποιηθεί ως εξής:

1. Many-to –one: Πολλαπλοί κόμβοι αισθητήρων στέλνουν τις καταγραφές τους σε ένα σταθμό βάσης ή σημείο ομαδοποίησης δεδομένων (aggregation point) στο δίκτυο.
2. One-to –many: Ένας κόμβος (τυπικά ο σταθμός βάσης) στέλνει με τρόπο multicast ή flood μια επερώτηση ή μια πληροφορία ελέγχου προς πολλούς κόμβους αισθητήρων.
3. Τοπική επικοινωνία: Οι γειτονικοί κόμβοι στέλνουν τοπικά μηνύματα για να ανακαλύψουν τους άλλους γειτονικούς τους κόμβους και να συντονιστούν με αυτούς. Ο κόμβος μπορεί να στέλνει μηνύματα προς όλους τους γειτονικούς του κόμβους ή μόνο προς ένα (unicast).

Οι κόμβοι σε ένα WSN γενικά θεωρείται ότι έχουν περιορισμένους πόρους, τα δίκτυα αισθητήρων είναι ακόμα πιο περιορισμένα. Ο πιο πιεστικός περιορισμός είναι αυτός της κατανάλωσης ενέργειας. Μετά την υλοποίηση τους τα δίκτυα αισθητήρων αφήνονται χωρίς επιμέλεια για μεγάλα χρονικά διαστήματα και η αντικατάσταση ή επαναφόρτιση της μπαταρίας τους μπορεί να μην είναι εφικτή ή ακόμα και αδύνατη. Οι κόμβοι σε ένα δίκτυο αισθητήρων συχνά επιδεικνύουν εμπιστοσύνη σε σχέσεις πέρα από αυτές που τυπικά απαντώνται σε ένα ad-hoc ασύρματο δίκτυο.

Οι γειτονικοί κόμβοι των πρώτων συχνά παρακολουθούν τα ίδια ή συσχετισμένα περιβαλλοντικά συμβάντα. Αν κάθε κόμβος στέλνει σαν απάντηση ένα πακέτο πληροφορίας γι' αυτό το συμβάν σπαταλάται πολύτιμη ενέργεια και εύρος ζώνης μετάδοσης.

Για να μειωθούν αυτά τα πλεονάζοντα μηνύματα και κατ' επέκταση η κίνηση του δικτύου και να εξοικονομηθεί ενέργεια απαιτείται να υπάρχει επεξεργασία εντός του δικτύου, ομαδοποίηση δεδομένων (aggregation) και ελαχιστοποίηση των διπλοτύπων. Αυτό καθιστά αναγκαίο να υπάρχουν σχέσεις μεταξύ των κόμβων του δικτύου που να είναι αξιόπιστες. Κάτι τέτοιο δεν είναι τυπικά δεδομένο σε ένα ad-hoc ασύρματο δίκτυο.

2.4 Εφαρμογές

Η ανάπτυξη των sensor networks ξεκίνησε από στρατιωτικές εφαρμογές για την επόπτευση του πεδίου μάχης. Σύντομα όμως βρήκαν χρήση τόσο σε εφαρμογές βιομηχανικής κλίμακας όσο και καταναλωτικές.

Μπορούμε να διακρίνουμε τις εφαρμογές στα παρακάτω:

2.4.1 Παρακολούθηση περιοχής

Μια από τις πιο συνηθισμένες εφαρμογές των WSN είναι η παρακολούθηση περιοχής. Το δίκτυο υλοποιείται σε μια περιοχή όπου πρέπει να καταγραφεί κάποιο φαινόμενο. Οι στρατιωτικές εφαρμογές θα μπορούσαν να καταταχτούν σ' αυτή την κατηγορία. Οι αισθητήρες σε αυτή την περίπτωση χρησιμοποιούνται για να ανιχνεύσουν μια πιθανή εισβολή του εχθρού. Οι αισθητήρες θα μπορούσαν να ανιχνεύουν την κίνηση ή τη θερμοκρασία και σε περίπτωση μεταβολών να αναφέρουν σε ένα από τους σταθμούς βάσης το γεγονός, στέλνοντας ένα μήνυμα μέσω internet ή δορυφόρου.

2.4.2 Παρακολούθηση περιβάλλοντος και καιρικών συνθηκών

2.4.2.1 Παρακολούθηση ατμοσφαιρικών ρύπων

Οι παράμετροι που καταγράφονται είναι οι τιμές των CO, CO₂, NO₂ ή CH₄ αέρια που παράγονται από τα οχήματα ή τη βιομηχανία και έχουν σοβαρή επίπτωση στην ανθρώπινη υγεία.

Η πληροφορία που παρέχουν μπορεί να αξιοποιηθεί για τη βελτίωση ή και τον εκ νέου σχεδιασμό συστημάτων μείωσης των ρύπων και βελτίωσης της ποιότητας του αέρα.

2.4.2.2 Παρακολούθηση δασών

Σκοπός είναι η άμεση ειδοποίηση για το ξεκίνημα μιας πυρκαγιάς σε ένα δάσος. Η έγκαιρη ειδοποίηση είναι πολύ σημαντική για την πυρόσβεση.

2.4.2.3 Παρακολούθηση φαινομένου θερμοκηπίου

Καταγράφεται και παρακολουθείται η θερμοκρασία και τα επίπεδα υγρασίας. Όταν αυτά ξεπερνούν τις ασφαλείς τιμές μπορούν με μήνυμα που θα αποσταλεί στο διαχειριστή του δικτύου να ενεργοποιηθούν μηχανισμούς οι οποίοι θα προσπαθήσουν να βελτιώσουν την κατάσταση, όπως να ανοίξουν αεραγωγούς, να ανοίξουν ανεμιστήρες κ.α.

2.4.2.4 Παρακολούθηση κατολισθήσεων

Ανίχνευση της κίνησης του εδάφους και άλλων παραμέτρων που μπορεί να συμβαίνουν πριν ή κατά τη διάρκεια μιας κατολίσθησης. Δίνει τη δυνατότητα της έγκαιρης πρόβλεψής της.

2.4.3 Άλλες πιθανές εφαρμογές

- Συστήματα ελέγχου για βιομηχανίες
- Παρακολούθηση καταγραφών video
- Παρακολούθηση κυκλοφορίας δρόμων
- Παρακολούθηση ιατρικών συσκευών
- Παρακολούθηση καταγραφή σεισμικής ή ηφαιστειακής δραστηριότητας.
- Έλεγχος εναέριας κυκλοφορίας
- Έλεγχος robot
- Συστήματα ελέγχου για το σπίτι (Smart homes)
- Παρακολούθηση στόλου οχημάτων
- Αγροτικές καλλιέργειες

2.5 Χαρακτηριστικά των δικτύων αισθητήρων

Τα κύρια χαρακτηριστικά ενός δικτύου αισθητήρων περιλαμβάνουν:

- Περιορισμούς στην κατανάλωση ισχύος στους κόμβους που συνήθως είναι μια συστοιχία μπαταρίας.
- Ικανότητα αντιμετώπισης κάποιας αστοχίας στους κόμβους
- Κινητικότητα των κόμβων
- Δυναμική τοπολογία δικτύου
- Βλάβες επικοινωνίας
- Ετερογένεια των κόμβων
- Επεκτασιμότητα, ανάπτυξη δικτύων μεγάλης κλίμακας

2.6 Γενικά περί ασφάλειας δικτύου

Ιδανικά κάθε δίκτυο θα πρέπει να ικανοποιεί τους ακόλουθους στόχους για να διασφαλίζει την ασφάλεια του:

- Confidentiality: Διασφάλιση ότι το μήνυμα παραμένει ανέπαφο από κάθε επίθεση.
- Integrity: Αναφέρεται στην αξιοπιστία των μηνυμάτων τα οποία δεν έχουν αλλοιωθεί.
- Authentication: Επιβεβαιώνει ότι το μήνυμα προέρχεται από τον κόμβο που ισχυρίζεται ότι προέρχεται.
- Access control: Είναι η ικανότητα να καθορίζεται αν ο κόμβος έχει πρόσβαση στους σωστούς πόρους του συστήματος

2.7 Ζητήματα ασφάλειας και διατήρησης απορρήτου σε δίκτυα αισθητήρων

Τα δίκτυα αισθητήρων προσφέρουν οικονομικά βιώσιμες λύσεις για μια ποικιλία εφαρμογών. Για παράδειγμα, σύγχρονες εφαρμογές τους χρησιμοποιούνται για την παρακολούθηση βιομηχανικών οργάνων, τα επίπεδα μόλυνσης την κίνηση στους αυτοκινητοδρόμους και της δομικής ακεραιότητας κτηρίων. Άλλες εφαρμογές περιλαμβάνουν τον έλεγχο του κλίματος σε κτήρια γραφείων αλλά και συστήματα οικιακής χρήσης για τον έλεγχο της θερμοκρασίας, του φωτός, της υγρασίας ή της κίνησης.

Τα δίκτυα αισθητήρων παίζουν σημαντικό ρόλο στη δημιουργία «έξυπνων» χώρων, οι οποίοι ενσωματώνουν την επιστήμη της πληροφορικής στην καθημερινή ζωή, στο οικιακό αλλά και το εργασιακό περιβάλλον.

Τα ζητήματα ασφάλειας και διατήρησης απορρήτου που θέτονται από τη χρήση αυτών των συστημάτων αποτελούν ένα ευρύ πεδίο έρευνας.

Η βελτίωση του εξοπλισμού όσον αφορά το υλικό (hardware) και το λογισμικό (software) που χρησιμοποιείται μπορεί να δώσει λύση για κάποια από τα ζητήματα που ανακύπτουν, ωστόσο κάποια άλλα απαιτούν την ανάπτυξη νέων τεχνολογιών.

2.8 Έκθεση σε κίνδυνο του κόμβου σε δίκτυο SN

Αναμένεται ότι μελλοντικά τα SNs θα αποτελούνται από εκατοντάδες ή χιλιάδες κόμβους-αισθητήρων. Κάθε κόμβος αποτελεί εν δυνάμει ένα πιθανό σημείο επίθεσης και λόγω του πλήθους τους καθίσταται μη πρακτικό να παρακολουθείται και να παρέχεται στον κάθε κόμβο προστασία από μια φυσική ή λογική επίθεση. Τα δίκτυα μπορεί να είναι διασπαρμένα σε μια πολύ μεγάλη περιοχή κι αυτό εκθέτει τους κόμβους ακόμα περισσότερο σε κίνδυνο να καταληφθούν ή να αναπρογραμματιστούν από έναν επίβουλο εισβολέα. (capture and reprogram).

Οι εισβολείς του συστήματος μπορεί ακόμα να κάνουν χρήση δικών τους κόμβων και να προτρέψουν το δίκτυο να τους δεχτεί σα νόμιμους. Όταν ο εισβολέας καταφέρει να αποκτήσει τον έλεγχο ορισμένων κόμβων μέσα στο δίκτυο, μπορεί να οργανώσει διάφορες επιθέσεις. Για παράδειγμα θα μπορούσε να παραποιήσει τα δεδομένα του κόμβου, να αποσπάσει απόρρητα δεδομένα από τις καταγραφές των κόμβων ή να προκαλέσει άρνηση υπηρεσίας (DoS).

Για να αντιμετωπιστεί το πρόβλημα που προκύπτει από την έκθεση σε κίνδυνο των κόμβων απαιτούνται τεχνολογικές λύσεις.

Για παράδειγμα η χρήση φτηνού εξοπλισμού δικτύου θα μπορούσε να κάνει εύκολο να καταληφθεί και να αναπρογραμματιστεί ένας κόμβος. Ωστόσο το να κάνουμε τους κόμβους απρόσβλητους σε επιθέσεις δεν είναι οικονομικά εφικτό.

Επομένως ξεκινάμε με την υπόθεση ότι ο επίβουλος εισβολέας θα είναι σε θέση να θέσει σε κίνδυνο ένα υποσύνολο των κόμβων-αισθητήρων του δικτύου.

Ως εκ τούτου, θα πρέπει να υπάρχει το κατάλληλο λογισμικό στα δίκτυα αισθητήρων που να διασφαλίζει την ασφαλή λειτουργία ακόμα και με την παρουσία μερικών κακόβουλων κόμβων στο δίκτυο.

Το Node-to node authentication (πιστοποίηση από κόμβο σε κόμβο) είναι μια βασική τεχνική που επιτρέπει στους κόμβους του δικτύου να πιστοποιούν την ταυτότητα τους, ο ένας στον άλλο.

Με το Node revocation (ανάκληση κόμβου) μπορεί να γίνει ο αποκλεισμός των επίβουλων κόμβων.

Για να επιτευχθεί αυτός ο στόχος με το μικρότερο δυνατό κόστος σε εξοπλισμό (hardware), θα πρέπει να γίνει χρήση «ελαφρών» πρωτοκόλλων ασφάλειας.

Επιπλέον, όλα τα πρωτόκολλα επικοινωνίας και επεξεργασίας δεδομένων που θα χρησιμοποιηθούν στα δίκτυα αισθητήρων θα πρέπει να γίνουν ανθεκτικά με την έννοια ότι θα πρέπει να λειτουργούν με υψηλή αποδοτικότητα ακόμα και με την παρουσία μικρού αριθμού κακόβουλων κόμβων στο δίκτυο.

Για παράδειγμα τα πρωτόκολλα δρομολόγησης θα πρέπει να είναι ανθεκτικά σε κόμβους που έχουν εκτεθεί σε επίθεση και μπορεί να συμπεριφέρονται με κακόβουλο τρόπο.

2.9 Υποκλοπή

Σε ένα ασύρματο δίκτυο αισθητήρων (WSN), ένας εχθρός μπορεί να αποκτήσει πρόσβαση σε απόρρητες πληροφορίες παρακολουθώντας τις εκπομπές (μετάδοση) των δεδομένων μεταξύ των κόμβων.

Για παράδειγμα, αν είχαν τοποθετηθεί μερικοί ασύρματοι δέκτες έξω από ένα σπίτι, θα μπορούσαν να παρακολουθούν τις καταγραφές θερμοκρασίας του δικτύου αισθητήρων που υπάρχει μέσα σ' αυτό, και να συγκεντρώνουν έτσι λεπτομερείς πληροφορίες για τις προσωπικές καθημερινές συνήθειες των κατοίκων του.

Η κρυπτογράφηση της επικοινωνίας των κόμβων μπορεί να απαντήσει εν μέρει στο πρόβλημα της υποκλοπής. Χρειάζεται τόσο το κλειδί κρυπτογράφησης όσο και το σχήμα κατανομής να είναι ισχυρά.

Το σχήμα θα πρέπει να είναι απλό στην εκτέλεση και εφικτό στην υλοποίησή του από την άποψη των περιορισμών ως προς τον εξοπλισμό- για τον ιδιοκτήτη του δικτύου. Θα πρέπει επίσης να διατηρεί τη μυστικότητα στο υπόλοιπο δίκτυο όταν μετά από μια εχθρική επίθεση κάποιοι από τους κόμβους και τα κλειδιά τους είναι εκτεθειμένα. Ιδανικά θα πρέπει να επιτρέπουν την ανάκληση της λειτουργίας των κλειδιών που είναι γνωστό ότι έχουν εκτεθεί και θα πρέπει να δίνει καινούργια κλειδιά στους κόμβους.

Μια end-to-end κρυπτογράφηση δεν είναι πρακτικά εφικτή λόγω του μεγάλου αριθμού κόμβων που επικοινωνούν αναμεταξύ τους γιατί ο εξοπλισμός των κόμβων σπάνια μπορεί να αποθηκεύει ένα μεγάλο αριθμό από μοναδικά κλειδιά κρυπτογράφησης.

Αντί αυτού, οι σχεδιαστές δικτύων αισθητήρων μπορούν να επιλέξουν μια κρυπτογράφηση hop-by-hop, στην οποία κάθε κόμβος αποθηκεύει μόνο τα κλειδιά κρυπτογράφησης που είναι μοιρασμένα στους άμεσους γειτονικούς του κόμβους. Σε αυτή την περίπτωση ο έλεγχος της επικοινωνίας ενός κόμβου από κάποιο κακόβουλο

εισβολέα του δικτύου, ελαχιστοποιεί την αποτελεσματικότητα της κρυπτογράφησης κάθε επικοινωνίας που κατευθύνεται μέσω ενός κόμβου που έχει εκτεθεί σε επίθεση. Αυτή η κατάσταση μπορεί να οξυνθεί ακόμα περισσότερο, αν ο εισβολέας χειραγωγήσει την υποδομή δρομολόγησης για να στείλει πολλές επικοινωνίες μέσω του κακόβουλου κόμβου.

Μια λύση σ' αυτό το πρόβλημα θα ήταν η χρήση πιο ισχυρών πρωτοκόλλων δρομολόγησης. Μια άλλη λύση θα ήταν η δρομολόγηση από πολλαπλά μονοπάτια (multipath routing), στην οποία τμήματα του μηνύματος δρομολογούνται μέσω πολλαπλών τμημάτων- μονοπατιών και επανασυναρμολογούνται στον προορισμό. Η επιλογή των πιο αποδοτικών τμημάτων –μονοπατιών είναι μια ακόμα ερευνητική πρόκληση.

2.10 Απόρρητο των δεδομένων

Τα δίκτυα αισθητήρων είναι εργαλεία συλλογής πληροφορίας και κάποιος θα μπορούσε να αποκτήσει πρόσβαση σε πολύ ευαίσθητη πληροφορία είτε από τα αποθηκευμένα δεδομένα ή κάνοντας επερωτήσεις ή υποκλέπτοντας το δίκτυο. Οι εισβολείς του δικτύου μπορούν να αντλήσουν ευαίσθητες πληροφορίες από δεδομένα που φαίνονται αβλαβή, αν γνωρίζουν πως να συσχετίσουν τις πολλαπλές εισόδους των αισθητήρων. Για παράδειγμα ένας εισβολέας μπορεί να αποκτήσει πρόσβαση στους εξωτερικούς και στους εσωτερικούς αισθητήρες ενός σπιτιού και να μπορέσει να απομονώσει τον εσωτερικό από τον εξωτερικό θόρυβο, αποσπώντας έτσι πληροφορίες για τις ιδιωτικές δραστηριότητες των κατοίκων του σπιτιού.

Το κύριο πρόβλημα απορρήτου δε είναι ότι τα δίκτυα αισθητήρων επιτρέπουν τη συλλογή πληροφοριών, γιατί στην πραγματικότητα πολλές από αυτές τις πληροφορίες θα μπορούσαν να συλεχθούν με την άμεση παρακολούθηση του χώρου. Το πρόβλημα απορρήτου επιδεινώνεται με τα δίκτυα αισθητήρων μάλλον από το γεγονός ότι κάνουν εύκολα προσβάσιμους μεγάλους όγκους πληροφορίας από απομακρυσμένη είσοδο στο σύστημα. Έτσι ο εισβολέας του συστήματος δεν χρειάζεται να έχει φυσική παρουσία για να συνεχίσει την παρακολούθηση. Μπορεί να συλλέξει την πληροφορία με τρόπο ανώνυμο και χαμηλό κίνδυνο. Η απομακρυσμένη πρόσβαση επιτρέπει σε ένα εισβολέα να παρακολουθεί ταυτόχρονα πολλαπλές θέσεις.

Η διασφάλιση ότι η πληροφορία που συλλέγεται από τους αισθητήρες παραμένει μέσα στο δίκτυο αισθητήρων και είναι προσβάσιμη μόνο στους έμπιστους χρήστες, είναι ένα ουσιαστικό βήμα για την επίτευξη της διατήρησης του απορρήτου.

Μια προσέγγιση είναι η κρυπτογράφηση των δεδομένων και ο έλεγχος πρόσβασης. Ένας άλλος τρόπος θα ήταν ο περιορισμός της ικανότητας του δικτύου να συλλέγει λεπτομερή δεδομένα για να μην τεθεί σε κίνδυνο το απόρρητο. Για παράδειγμα, το δίκτυο αισθητήρων θα μπορούσε να κάνει ανώνυμα τα δεδομένα κάνοντας αναφορά μόνο των συνολικών θερμοκρασιών σε μια ευρεία περιοχή ή προσεγγιστικών τοποθεσιών στα σημεία λήψης της πληροφορίας. Το σύστημα θα μπορούσε να αποθηκεύει τα δεδομένα των αισθητήρων ανώνυμα σε μια βάση δεδομένων, απομακρύνοντας τις λεπτομέρειες που ο εισβολέας θα μπορούσε να βρει χρήσιμες. Μια άλλη προσέγγιση θα ήταν να γίνεται η επεξεργασία των αναζητήσεων (queries)

στο δίκτυο αισθητήρων με κατανομημένο τρόπο έτσι ώστε κανένας κόμβος από μόνος του να μην μπορεί να παρατηρήσει τα αποτελέσματα αυτής της αναζήτησης στο ακέραιο. Αυτή η προσέγγιση διαφυλάττει το σύστημα από πιθανή κατάχρηση από κόμβους που έχουν εκτεθεί σε επίβουλη επίθεση.

2.11 Επιθέσεις τύπου DoS (Denial of Service)

Καθώς εφαρμογές, κρίσιμες για την ασφάλεια, χρησιμοποιούν περισσότερα δίκτυα αισθητήρων, μια πιθανή δολιοφθορά μέσω διακοπών λειτουργίας γίνεται σημαντική. Είναι εξαιρετικά δύσκολο να αμυνθεί κανείς σε επιθέσεις αρνήσεως υπηρεσίας (DoS), γιατί σκοπός αυτών είναι πιο πολύ να καταστρέψουν τη λειτουργικότητα του δικτύου παρά να την ανατρέψουν ή να χρησιμοποιήσουν την πληροφορία.

Οι επιθέσεις DoS μπορούν να συμβούν στο φυσικό επίπεδο, για παράδειγμα μέσω ραδιοφωνικών παρεμβολών. Μπορεί ακόμα να συμπεριλαμβάνουν επίβουλες εκπομπές στο δίκτυο με σκοπό την παρεμβολή στα πρωτόκολλα του δικτύου αισθητήρων ή τη φυσική καταστροφή των κεντρικών κόμβων του δικτύου.

Οι εισβολείς μπορούν να προκαλέσουν την εξάντληση της μπαταρίας των κόμβων – αισθητήρων για παράδειγμα στέλνοντας μια συνεχή σειρά από άχρηστα μηνύματα επικοινωνίας τα οποία όμως θα προκαλέσουν την εξάντληση της ενέργειας των κόμβων που είχαν σαν στόχο, επειδή αυτοί θα πρέπει να ξοδεύουν ενέργεια για την επεξεργασία των άχρηστων μηνυμάτων ή γιατί θα τα προωθούν σε άλλους κόμβους.

Πιο επίβουλες επιθέσεις μπορούν να προκύψουν από το εσωτερικό του δικτύου αισθητήρων, αν οι εισβολείς μπορέσουν να εκθέσουν σε κίνδυνο τους κόμβους αισθητήρων. Για παράδειγμα μπορούν να δημιουργήσουν βρόχους δρομολόγησης που τελικά θα εξαντλήσουν (ενεργειακά) όλους τους κόμβους του βρόχου.

Υπάρχουν ποικίλοι τρόποι άμυνας ενάντια σε επιθέσεις DoS όσο ποικίλοι είναι και το είδος των εισβολέων. Τεχνικές όπως επικοινωνία ευρέος φάσματος ή μετατόπισης συχνοτήτων μπορούν να εξουδετερώσουν επιθέσεις τύπου παρεμβολής στη συχνότητα εκπομπής. Η κατάλληλη πιστοποίηση μπορεί να εμποδίσει να γίνουν αποδεκτά από το δίκτυο τα εμβόλιμα μηνύματα από κάποιο εισβολέα.

Ωστόσο, τα σχετικά πρωτόκολλα πρέπει να είναι αποτελεσματικά έτσι ώστε να μη γίνονται τα ίδια στόχοι μιας επίθεσης με σκοπό την εξάντληση ενέργειας. Για παράδειγμα μπορούν να παρέχουν μηνύματα πιστοποίησης χρησιμοποιώντας υπογραφές που βασίζονται στην ασύμμετρη κρυπτογράφηση. Πάντως η δημιουργία και η πιστοποίηση ασύμμετρων υπογραφών απαιτούν αρκετή υπολογιστική ισχύ και οι εισβολείς που θα μπορέσουν να προκαλέσουν πολλές τέτοιες λειτουργίες μπορούν ουσιαστικά να κάνουν μια αποτελεσματική επίθεση εξάντλησης ενέργειας.

2.12 Επίβουλη χρήση καταναλωτικών δικτύων

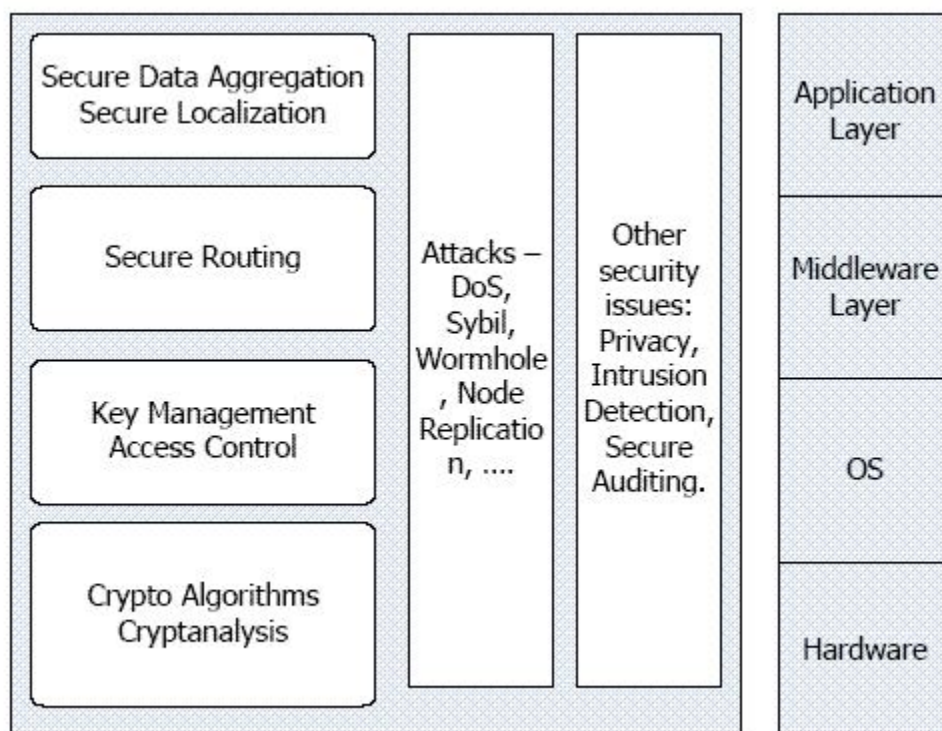
Η αύξηση των δικτύων αισθητήρων αναπόφευκτα θα επεκταθεί και σε χρήστες - εγκληματίες που θα μπορούν να τα χρησιμοποιούν για παράνομους σκοπούς. Για παράδειγμα, ο κλέφτης θα μπορούσε να απλώσει αισθητήρες στα θεμέλια μιας

ιδιωτικής κατοικίας για να ανιχνεύσει τη παρουσία των κατοίκων της. Αν οι αισθητήρες είναι αρκετά μικροί, μπορούν να εμφυτευτούν σε υπολογιστές και κινητά τηλέφωνα για να εξάγουν απόρρητη πληροφορία και κωδικούς πρόσβασης.

Οι φραγμοί του κόστους και της διαθεσιμότητας τέτοιων αισθητήρων θα πέσουν με την αύξηση της ζήτησης τους. Οι ανιχνευτές αισθητήρων προσφέρουν μια πιθανή προστασία απέναντι σε τέτοιου είδους επιθέσεις. Ένας ανιχνευτής θα πρέπει να μπορεί όχι μόνο να ανιχνεύει την παρουσία πιθανά εχθρικών ασύρματων επικοινωνιών μέσα σε μια περιοχή που μπορεί να έχει υψηλό επίπεδο παρεμβολών, αλλά και να μπορεί να διακρίνει τις εκπομπές από εξουσιοδοτημένα και μη εξουσιοδοτημένα δίκτυα αισθητήρων και άλλων διατάξεων.

Τέτοιες τεχνολογίες μπορεί να μην αποτρέπουν τα μη εξουσιοδοτημένα μέρη από το να αναπτύξουν δίκτυα αισθητήρων σε ευαίσθητες περιοχές αλλά θα τα έκαναν πιο ακριβή, ελαφρύνοντας κατά κάποιο τρόπο το πρόβλημα.

Στη συνέχεια θα γίνει αναφορά στα επιμέρους θέματα που αφορούν την ασφάλεια των δικτύων αισθητήρων και κυρίως θα παρουσιαστούν θέματα που αφορούν τη δρομολόγηση, την ομαδοποίηση δεδομένων (Data Aggregation) και τον εντοπισμό (Localization). Θα βασιστούμε στον παρακάτω πίνακα κατηγοριοποίησης και θα παρουσιαστούν κάποιες από τις προτάσεις που έχουν γίνει για την αντιμετώπιση προβλημάτων ασφάλειας.



Εικόνα 6: Security Map

2.13 Περί ασφαλούς επικοινωνίας σε ασύρματα ad-hoc δίκτυα αισθητήρων

Η εργασία αυτή παρέχει ένα σχήμα ασφάλειας επικοινωνίας για ασύρματα δίκτυα αισθητήρων που βασίζονται σε μια συγκεκριμένη αρχιτεκτονική (DARPA SensIT program). Κύριες συνεισφορές της είναι:

- Αξιολόγηση των απειλών ασφάλειας στην επικοινωνία των δικτύων Αισθητήρων.
- Μηχανισμοί ασφαλείας ξεχωριστοί για δεδομένα διαφορετικού επιπέδου ευαισθησίας. Ένας τέτοιος διαχωρισμός επιτρέπει την αποδοτικότερη διαχείριση πόρων που είναι πολύ σημαντικό για τα WSN.
- Σχήμα βασισμένο στην τοποθεσία το οποίο προστατεύει το υπόλοιπο το δικτύου ακόμα και όταν ένα τμήμα του έχει εκτεθεί σε κάποια απειλή.

Η προσέγγιση αυτή βασίζεται στην αρχή της ασφάλειας δικτύων η οποία λέει ότι τα δεδομένα πρέπει να προστατεύονται σε τέτοιο βαθμό που να είναι ανάλογη της σημασίας τους.

Στη συγκεκριμένη αρχιτεκτονική για την οποία αναπτύχθηκε το σχήμα ασφάλειας επικοινωνίας, έχει γίνει η εξής διάκριση των δεδομένων που στέλνονται μέσω του δικτύου σε:

1. Mobile code
2. δεδομένα τοποθεσίας των κόμβων αισθητήρων
3. δεδομένα σχετικά με εφαρμογή

Ακολουθώντας αυτή την κατηγοριοποίηση διακρίνονται οι κυριότερες απειλές και οι κατάλληλοι μηχανισμοί ασφαλείας.

Απειλές:

- Κατασκευασμένος κακόβουλος κώδικας που εγχύεται σε ένα δίκτυο και μπορεί να αλλάξει τη συμπεριφορά του δικτύου με απρόβλεπτο τρόπο.
- Η ανάκτηση της πληροφορίας της θέσης των κόμβων αισθητήρων μπορεί να βοηθήσει τον εισβολέα του δικτύου να ανακαλύψει τη θέση των κόμβων αισθητήρων ευκολότερα από ότι με τεχνικές ραδιεντοπισμού τους.
- Η προστασία δεδομένων που σχετίζονται με κάποια εφαρμογή εξαρτάται από τις απαιτήσεις για ασφάλεια της συγκεκριμένης εφαρμογής.

Ο κύριος σκοπός ήταν η ελαχιστοποίηση της ενεργειακής κατανάλωσης που απαιτείται για το σκοπό της ασφάλειας.

2.14 Αρχιτεκτονική του δικτύου αισθητήρων

Τα πιο σημαντικά μέρη της αρχιτεκτονικής που χρησιμοποιήθηκε είναι:

- Εντοπισμένοι αλγόριθμοι (localized algorithms)
- Τοπικό μοντέλο μετάδοσης επικοινωνίας
- Mobile Code

2.14.1 Εντοπισμένοι αλγόριθμοι

Το πιο ιδιαίτερο χαρακτηριστικό των δικτύων αισθητήρων, είναι η περιορισμένη ενέργεια, που είναι διαθέσιμη στους κόμβους αισθητήρων. Κατά συνέπεια η προσεκτική κατανομή της διαθέσιμης ενέργειας είναι θεμελιώδης για το σχεδιασμό του δικτύου. Έχοντας στο μυαλό ότι η επικοινωνία μεταξύ των κόμβων καταναλώνει σημαντικό ποσό των ενεργειακών πόρων, το λογισμικό των εφαρμογών και του συστήματος θα πρέπει να επιτυγχάνει το επιθυμητό επίπεδο απόδοσης με την ελάχιστη δυνατή κίνηση στο δίκτυο.

Στην αρχιτεκτονική SensorWare όλες οι εφαρμογές έχουν σχεδιαστεί με βάση εντοπισμένους αλγορίθμους, όπου οι κόμβοι ενεργοποιούνται από κάποιο γεγονός ανταλλάσσουν μηνύματα μόνο με τους άμεσα γειτονικούς στους κόμβους. Μόνο ένας κόμβος συλλέγει όλες τις καταγραφές των αισθητήρων και στέλνει τα συνδυασμένα δεδομένα σε ένα κόμβο-πύλη (ένας κόμβος που μπορεί να λειτουργεί ως proxy ανάμεσα στο χρήστη και το δίκτυο).

2.14.2 Τοπικό μοντέλο μετάδοσης επικοινωνίας

Κάθε κόμβος του δικτύου μπορεί να είναι πομπός ή δέκτης ενός μηνύματος μετάδοσης. Στο σχήμα ασφάλειας της εργασίας αυτής χρησιμοποιήθηκαν συμμετρικά κλειδιά κρυπτογράφησης. Η λύση αυτή απλοποιεί τη διαχείριση του κλειδιού και διατηρεί την απόδοση ενέργειας της τοπικής μετάδοσης αλλά δεν προσφέρει ιδιαίτερα δυνατή πιστοποίηση.

2.14.3 Mobile Code

Είναι η ικανότητα για την εκτέλεση προγραμμάτων, κώδικα ή αντικείμενων με σκοπό την μεταφορά από ένα μηχάνημα (host) σε ένα άλλο.

Λόγοι που κάνουν το mobile code σημαντικό για δίκτυα αισθητήρων.

1. Η περιορισμένη δυνατότητα αποθήκευσης των κόμβων δεν επιτρέπει το να διατηρούνται όλες οι εφαρμογές σε ένα κόμβο συνέχεια.
2. Οι εφαρμογές που θα πρέπει να εκτελεστούν στο δίκτυο μπορεί να μην είναι γνωστές κατά την περίοδο υλοποίησης του δικτύου.

Εφόσον δεν είναι δυνατή η χειροκίνητη επαναρύθμιση των κόμβων αισθητήρων μετά την υλοποίησή τους, υπάρχει ένας επιπλέον λόγος για τη χρήση του κατανεμημένου κώδικα (mobile code).

2.15 Απειλές ασφάλειας

Τα ασύρματα δίκτυα είναι γενικά πιο ευάλωτα σε επιθέσεις απ' ό,τι τα ενσύρματα λόγω της φύσης της μετάδοσης εκπομπής. Ένας επιπλέον λόγος είναι ότι οι κόμβοι συχνά είναι τοποθετημένοι σε εχθρικά ή επικίνδυνα περιβάλλοντα και δεν προστατεύονται με κάποιο φυσικό τρόπο.

Διακρίνονται οι ακόλουθες απειλές ανάλογα με την κατηγοριοποίηση των δεδομένων που έγινε παραπάνω:

1. Εισαγωγή κακόβουλου κώδικα. Είναι η πιο επικίνδυνη από όλες τις απειλές. Ο κακόβουλος κώδικας μπορεί να εισαχθεί στο δίκτυο και να διασπαρθεί σε όλους τους κόμβους και εν δυνάμει να καταστρέψει ολόκληρο το δίκτυο ή ακόμα χειρότερα να καταλάβει το δίκτυο για λογαριασμό του εισβολέα. Ένα κατελυμμένο δίκτυο μπορεί να στέλνει είτε ψευδείς παρατηρήσεις για το περιβάλλον σε ένα νόμιμο χρήστη ή να στέλνει τις αληθείς παρατηρήσεις σε ένα κακόβουλο χρήστη.
2. Υποκλοπή των μηνυμάτων που περιέχουν πληροφορία τοποθεσίας των κόμβων αισθητήρων επιτρέπει στον εισβολέα να εντοπίσει και να καταστρέψει τους κόμβους. Η σημασία της απόκρυψης της θέσης των κόμβων έχει να κάνει με το γεγονός ότι οι κόμβοι αισθητήρων έχουν πολύ μικρές διαστάσεις και η τοποθεσία τους δεν μπορεί να εντοπιστεί με εύκολο τρόπο. Για αυτό είναι σημαντικό να αποκρύπτεται η τοποθεσία τους. Στην περίπτωση στατικών κόμβων η πληροφορία αυτή θα πρέπει να προστατεύεται καθ' όλη τη διάρκεια της ζωής του δικτύου.
3. Εκτός από την πληροφορία θέσης ένας επίδοξος εισβολέας μπορεί να παρατηρεί μηνύματα που σχετίζονται με κάποια εφαρμογή όπως μηνύματα IDs, timestamps και άλλα πεδία.
4. Ένας εισβολέας μπορεί να διοχετεύσει ψεύτικα μηνύματα που δίνουν αναληθή πληροφορία για το περιβάλλον στο χρήστη. Τέτοια μηνύματα καταναλώνουν την λιγοστή διαθέσιμη ενέργεια των κόμβων. Αυτό το είδος της επίθεσης ονομάζεται και «μαρτύριο στέρησης ύπνου» (sleep deprivation torture).

2.16 Σχήμα Ασφάλειας Επικοινωνίας

Το προτεινόμενο σχήμα αποτελείται από τρία επίπεδα ασφαλείας που βασίζονται στην κρυπτογράφηση ιδιωτικού κλειδιού χρησιμοποιώντας ομαδικά κλειδιά. Θεωρείται ότι όλοι οι τύποι των δεδομένων περιέχουν λιγότερο ή περισσότερο εμπιστευτικά δεδομένα και γι' αυτό το περιεχόμενο όλων των μηνυμάτων του

δικτύου είναι κρυπτογραφημένο. Επίσης θεωρείται ότι επιτρέπεται σε όλους τους κόμβους αισθητήρων να έχουν πρόσβαση στο περιεχόμενο οποιουδήποτε μηνύματος. Εξετάζεται μόνο η ασφάλεια της επικοινωνίας και όχι η προστασία των δεδομένων μέσα στον κόμβο.

Η υλοποίηση των μηχανισμών ασφάλειας σε ένα δίκτυο αισθητήρων όχι μόνο αυξάνει την καθυστέρηση του δικτύου (latency) λόγω της εκτέλεσης των επιπρόσθετων διαδικασιών ασφάλειας αλλά και η ενέργεια που καταναλώνεται μειώνει το χρόνο ζωής του δικτύου. Γι' αυτό το λόγο προτείνεται το μοντέλο τριών επιπέδων ασφαλείας ανάλογα με την κατηγοριοποίηση των δεδομένων:

- Το επίπεδο ασφάλειας I προορίζεται για mobile code, την πιο ευαίσθητη πληροφορία στο δίκτυο.
- Το επίπεδο ασφάλειας II είναι αφιερωμένο στην πληροφορία τοποθεσίας που μεταφέρεται στα μηνύματα.
- Το επίπεδο ασφάλειας III προορίζεται για την πληροφορία που σχετίζεται με τις εφαρμογές.

Ο βαθμός της κρυπτογράφησης για κάθε επίπεδο ασφαλείας αντιστοιχεί στο πόσο ευαίσθητη είναι η πληροφορία που κρυπτογραφείται. Γι' αυτό το λόγο το επίπεδο I είναι το ισχυρότερο από όλα και το επίπεδο II είναι ισχυρότερο από το III.

Τα διαφορετικά επίπεδα ασφάλειας υλοποιούνται είτε χρησιμοποιώντας διάφορους αλγόριθμους είτε χρησιμοποιώντας τον ίδιο με προσαρμογή των παραμέτρων για να αλλαχθεί η ισχύς του και να αυξηθούν οι υπολογισμοί που γίνονται. Η χρήση του ίδιου αλγορίθμου με προσαρμόσιμες παραμέτρους έχει το όφελος της μικρότερης απαίτησης για αποθήκευση στη μνήμη.

Στην συγκεκριμένη εργασία επιλέχθηκε ο αλγόριθμος RC6. Το overhead για τον αλγόριθμο κρυπτογράφησης RC6, αυξάνει με την ισχύ της κρυπτογράφησης που μετριέται με τον αριθμό των επαναλήψεών του.

Η αρχιτεκτονική SensorWare που χρησιμοποιήθηκε έχει ένα multicast μοντέλο επικοινωνίας και γι' αυτό χρησιμοποιούνται ομαδικά κλειδιά. Διαφορετικά αν κάθε ζεύγος κόμβων απαιτούσε ένα κλειδί ή ένα ζεύγος κλειδιών η επικοινωνία μεταξύ των κόμβων θα ήταν unicast, και θα είχαμε ένα αυξημένο αριθμό μηνυμάτων.

Όλοι οι κόμβοι στο δίκτυο μοιράζονται ένα αρχικό σύνολο master κλειδιών, ο αριθμός αυτός εξαρτάται από τη διάρκεια ζωής του δικτύου (όσο μεγαλύτερος τόσο περισσότερα κλειδιά απαιτούνται). Μια προσέγγιση που τα κλειδιά θα δημιουργούνταν δυναμικά και θα μεταδίδονταν στο δίκτυο δεν είναι αποδεκτή, γιατί στην περίπτωση αυτή θα απαιτούνταν ένα πρωτόκολλο που θα διασφάλιζε ότι όλοι οι κόμβοι θα λαμβάνουν ένα κλειδί και αυτό δεν είναι δυνατό σε ένα δίκτυο, όπου οι κόμβοι δεν θα παρακολουθούν τους γειτονικούς τους κόμβους. Ένα κλειδί από την αρχική λίστα είναι ενεργό κάθε στιγμή. Ο αλγόριθμος επιλογής κλειδιού βασίζεται σε μια ψευδο-τυχαία γεννήτρια αριθμών που τρέχει με το ίδιο seed σε κάθε κόμβο. Περιοδικά και συγχρονισμένα σε κάθε κόμβο παράγεται ένας νέος αριθμός που χρησιμοποιείται για να παρέχει ένα δείκτη στον πίνακα των διαθέσιμων κλειδιών.

2.16.1 Επίπεδο ασφάλειας I

Το ισχυρότερο από άποψη ασφάλειας προορίζεται για μηνύματα που περιέχουν mobile code και συγκριτικά είναι λιγότερα σε αριθμό από τα άλλα είδη μηνυμάτων. Ο κόμβος χρησιμοποιεί το master κλειδί. Για να μπορέσει να γίνει εισαγωγή κώδικα σε αυτό το επίπεδο από ένα χρήστη χρειάζονται τα ακόλουθα πιστοποιητικά:

- το σύνολο των master κλειδιών
- η αντίστοιχη ψευδό-τυχαία γεννήτρια αριθμών και το
- seed

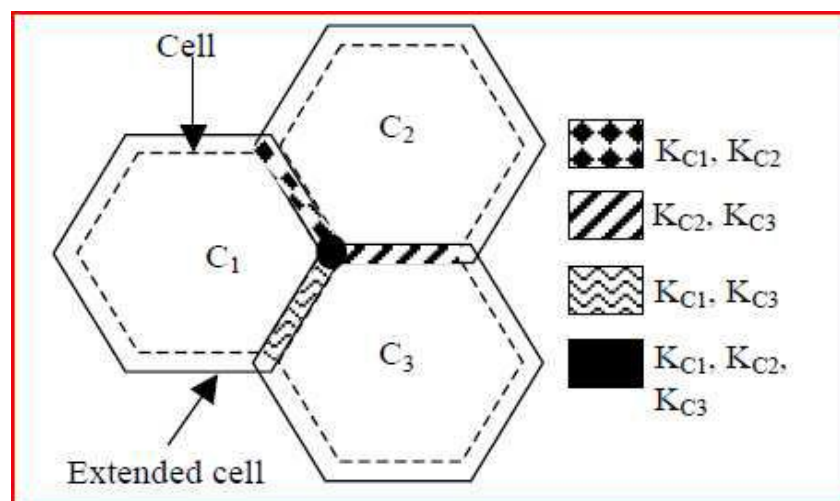
Σε περίπτωση που ένας κακόβουλος χρήστης σπάσει την κρυπτογράφηση σ' αυτό το επίπεδο χρησιμοποιώντας επίθεση «ωμής βίας» (brute force attack) μπορεί να εισάγει βλαβερό κώδικα στο δίκτυο

2.16.2 Επίπεδο ασφάλειας II

Είναι επίπεδο μικρότερης ασφαλείας και απευθύνεται σε δεδομένα που περιέχουν πληροφορία για την τοποθεσιών των κόμβων αισθητήρων.

Η μέριμνα που γίνεται εδώ είναι σε περίπτωση που κάποιοι από τους κόμβους έχουν εκτεθεί σε κάποια επίθεση και η πληροφορία της τοποθεσίας τους έχει γίνει γνωστή, να περιοριστεί κατά το δυνατό η ζημιά αφήνοντας ανέπαφα τα υπόλοιπα τμήματα του δικτύου.

Η περιοχή που καλύπτει το δίκτυο διαιρείται σε κελιά. Οι κόμβοι μέσα σε ένα κελί μοιράζονται ένα κοινό κλειδί που είναι μια συνάρτηση της τοποθεσίας και του τρέχοντος master κλειδιού. Μεταξύ των κελιών υπάρχουν οι συνοριακές περιοχές των οποίων το πλάτος είναι ίσο με το εύρος μετάδοσης. Οι κόμβοι που ανήκουν σ' αυτές τις περιοχές έχουν τα κλειδιά των παρακείμενων περιοχών. Αυτό διασφαλίζει το να έχουν κοινό κλειδί οι κόμβοι που βρίσκονται μέσα στη ζώνη μετάδοσης. Η διάσταση των κελιών πρέπει να είναι αρκετά μεγάλη ώστε οι τοπικοί αλγόριθμοι να διασφαλίζουν ότι η κίνηση μεταξύ των κελιών είναι μικρή σχετικά με τη συνολική κίνηση.



Εικόνα 7: Κελιά, κελιά επέκτασης και περιοχές με πολλαπλά κλειδιά

Το σχήμα των κελιών είναι αυθαίρετο και η μόνη προϋπόθεση είναι να καλύπτεται όλη η περιοχή του δικτύου. Στην παρούσα εργασία έχει γίνει ο διαχωρισμός σε εξαγωνικά κελιά για λόγους ομοιομορφίας και επειδή εξασφαλίζεται ότι οι κόμβοι των πυλών θα έχουν το πολύ 3 κλειδιά. Σαν κελιά επέκτασης θεωρούνται τα κελιά που περιλαμβάνουν το κυρίως κελί και τις αντίστοιχες συνοριακές περιοχές.

Κάθε κόμβος συγκρίνει την περιοχή του έναντι αυτής του κελιού επέκτασης και καθορίζει έτσι αν βρίσκεται στο κελί ή στο κελί επέκτασης

2.16.3 Επίπεδο ασφάλειας III

Στο επίπεδο αυτό χρησιμοποιείται ο πιο αδύναμος αλγόριθμος κρυπτογράφησης. Στο επίπεδο αυτό η συχνότητα των μηνυμάτων εφαρμογών είναι απαγορευτική για τη χρήση ισχυρότερων αλγορίθμων γιατί αυτό θα είχε σα συνέπεια τη μεγαλύτερη κατανάλωση ενέργειας. Επομένως χρησιμοποιείται ένας αλγόριθμος που έχει μικρότερες απαιτήσεις σε υπολογιστική ισχύ με ανάλογη μείωση των επιπέδων ασφάλειας που παρέχει. Το κλειδί του τρίτου επιπέδου προέρχεται από το master κλειδί μέσω της MD5 hash function και αλλάζει περιοδικά.

2.17 Ασφαλής δρομολόγηση σε ασύρματα δίκτυα αισθητήρων

Στον παρακάτω πίνακα παρουσιάζονται τα πιο διαδεδομένα πρωτόκολλα δρομολόγησης που χρησιμοποιούνται στα δίκτυα αισθητήρων και αντιπαρατίθενται με τις αντίστοιχες απειλές.

Protocol	Relevant attacks
TinyOS beaconing	Bogus routing information, selective forwarding, sink-holes, Sybil, wormholes, HELLO floods
Directed diffusion and its multipath variant	Bogus routing information, selective forwarding, sink-holes, Sybil, wormholes, HELLO floods
Geographic routing (GPSR, GEAR)	Bogus routing information, selective forwarding, Sybil
Minimum cost forwarding	Bogus routing information, selective forwarding, sink-holes, wormholes, HELLO floods
Clustering based protocols (LEACH, TEEN, PEGASIS)	Selective forwarding, HELLO floods
Rumor routing	Bogus routing information, selective forwarding, sink-holes, Sybil, wormholes
Energy conserving topology maintenance (SPAN, GAF, CEC, AFECA)	Bogus routing information, Sybil, HELLO floods

Πίνακας 1: Συνοπτικός πίνακας επιθέσεων σε διάφορα προτεινόμενα πρωτόκολλα δρομολόγησης σε ασύρματα δίκτυα αισθητήρων

Πολλά από τα πρωτόκολλα δρομολόγησης που χρησιμοποιούνται στα δίκτυα αισθητήρων είναι αρκετά απλά και γι' αυτό το λόγω είναι ευάλωτα σε επιθέσεις. Οι περισσότερες επιθέσεις στο επίπεδο δικτύου στα δίκτυα αισθητήρων βρίσκονται σε μια από τις επόμενες κατηγορίες:

- Παραποιημένη, αλλαγμένη ή αναπαραχθείσα πληροφορία δρομολόγησης
- Επιλεκτική προώθηση
- Επίθεση τύπου καταβόθρας (sinkhole)
- Επιθέσεις Σίββυλας (Sibyl attacks)
- Wormholes
- HELLO flood
- Παραποίηση αναγνώρισης (acknowledgment spoofing)

Θα γίνει μια παρουσίαση αυτών των απειλών και στη συνέχεια θα επικεντρωθούμε στις αδυναμίες συγκεκριμένων πρωτοκόλλων δρομολόγησης σε σχέση με αυτές τις απειλές. Τέλος θα γίνει μια αναφορά στα μέτρα προστασίας που μπορούν να ληφθούν.

2.17.1 Παραποιημένη, αλλαγμένη ή αναπαραχθείσα πληροφορία δρομολόγησης

Η πιο άμεση απειλή σε ένα πρωτόκολλο δρομολόγησης, είναι η στόχευση της πληροφορίας δρομολόγησης, που ανταλλάσσεται μεταξύ δύο κόμβων. Με την παραποίηση, αλλαγή ή αναπαραγωγή της πληροφορίας δρομολόγησης οι εισβολείς μπορούν να δημιουργήσουν βρόχους, να προσελκύσουν ή να απωθήσουν την κίνηση του δικτύου να επεκτείνουν ή να συντομεύσουν τις πηγαίες διαδρομές, να παράγουν ψευδή μηνύματα λάθους, να διαμελίσουν το δίκτυο, να αυξήσουν την καθυστέρηση του δικτύου κ.τλ.

2.17.2 Επιλεκτική προώθηση

Τα multihop δίκτυα συχνά βασίζονται στη θεώρηση ότι οι κόμβοι που παίρνουν μέρος θα προωθήσουν πιστά τα μηνύματα που έλαβαν. Σε μια επίθεση επιλεκτικής προώθησης, κακόβουλοι κόμβοι μπορεί να αρνηθούν να προωθήσουν κάποια μηνύματα και απλά τα απορρίπτουν, κάνοντας βέβαιο ότι αυτά δε θα μεταδοθούν περαιτέρω.

Μια απλή μορφή αυτής της απειλής είναι όταν ένας κακόβουλος κόμβος συμπεριφέρεται σε μια μαύρη τρύπα και αρνείται κάθε πακέτο που βλέπει. Πάντως μια τέτοια απειλή μπορεί να αποτύχει αν οι γειτονικοί κόμβοι συμπεράνουν ότι έχει βλάβη και αποφασίσουν να ψάξουν κάποια άλλη διαδρομή.

Μια πιο ευφυής μορφή αυτής της απειλής είναι όταν ο εισβολέας προωθεί επιλεκτικά τα πακέτα. Ο εισβολέας που έχει σκοπό να καταστείλει ή να τροποποιήσει τα πακέτα που προέρχονται από μερικούς επιλεγμένους κόμβους μπορεί να προωθεί κανονικά την υπόλοιπη κίνηση και έτσι να περιορίζει τις υποψίες.

Οι επιθέσεις αυτού του τύπου είναι πιο αποτελεσματικές όταν ο εισβολέας έχει συμπεριληφθεί κανονικά στο μονοπάτι ροής των δεδομένων. Ένα πιο προχωρημένο σενάριο θα ήταν ο εισβολέας να παρακολουθεί τη ροή όλων των πακέτων και να μπορεί να μιμηθεί την επιλεκτική προώθηση παρεμβάλλοντας ή προκαλώντας σύγκρουση σε κάθε προωθούμενο πακέτο που τον ενδιαφέρει.

Ο μηχανισμός μιας τέτοιας προσπάθειας θα ήταν αρκετά δύσκολος έως και αδύνατος. Γι' αυτό το λόγο πιστεύεται ότι ο εισβολέας που θα κάνει τέτοιου είδους επίθεση είναι πιθανότερο να ακολουθήσει το μονοπάτι της μικρότερης αντίστασης και θα προσπαθήσει να συμπεριληφθεί στο κανονικό μονοπάτι ροής των δεδομένων.

2.17.3 Επιθέσεις τύπου καταβόθρας (sinkhole)

Σε μια επίθεση τύπου καταβόθρας, ο σκοπός του εισβολέα είναι να παρασύρει σχεδόν όλη την κίνηση μιας συγκεκριμένης περιοχής μέσω του κόμβου που έχει καταλάβει.

Επειδή οι κόμβοι που βρίσκονται μέσα ή κοντά στο μονοπάτι που ακολουθούν τα πακέτα μπορούν να παραποιήσουν τα δεδομένα πολλών εφαρμογών, οι επιθέσεις τύπου καταβόθρας μπορούν να υποβοηθήσουν και άλλα είδη απειλών όπως για παράδειγμα της επιλεκτικής προώθησης.

Ο τρόπος που δουλεύει η απειλή αυτού του είδους είναι να κάνει ελκυστικό τον εκτεθειμένο κόμβο στους γύρω κόμβους του, μέσω του αλγόριθμου δρομολόγησης. Για παράδειγμα ο εισβολέας μπορεί να παραποιήσει ή να αναπαράγει μια αγγελία για μια πολύ καλή διαδρομή προς ένα σταθμό βάσης. Κάποια πρωτόκολλα μπορεί να προσπαθήσουν να επιβεβαιώσουν την ποιότητα αυτής της διαδρομής με μηνύματα end-to-end γνωστοποίησης (acknowledgments) που περιέχουν πληροφορία αξιοπιστίας, ή latency.

Σε αυτή την περίπτωση ένας εισβολέας που έχει εξοπλισμό με ισχυρό αναμεταδότη μπορεί να παρέχει μια διαδρομή καλής ποιότητας εκπέμποντας με αρκετή ισχύ για να φτάσει το σταθμό βάσης με μία αναπήδηση (single hop) ή να χρησιμοποιήσει μια επίθεση τύπου wormhole. Λόγω αυτής της προτεινόμενης διαδρομής (που είναι είτε πραγματική είτε πλασματική), είναι πιθανό κάθε γειτονικός κόμβος να προωθεί όλα τα πακέτα που προορίζονται για το σταθμό βάσης μέσω του κόμβου που έχει παρεμβάλει ο εισβολέας και ακόμα να αναμεταδίδει στους υπόλοιπους γείτονες το πόσο ελκυστική είναι αυτή η διαδρομή.

Ο εισβολέας καταφέρνει έτσι να δημιουργήσει αποτελεσματικά μια σφαίρα επιρροής, προσελκύοντας την κίνηση κόμβων που μπορεί να βρίσκονται ακόμα και αρκετές αναπηδήσεις (hops) μακριά από τον εκτεθειμένο κόμβο. Μπορεί λοιπόν να καταστείλει ή να τροποποιήσει επιλεκτικά πακέτα που προέρχονται από οποιοδήποτε κόμβο σε μια περιοχή.

Θα πρέπει να σημειωθεί εδώ ότι τα δίκτυα αισθητήρων είναι ιδιαίτερα ευάλωτα σε τέτοιου είδους επιθέσεις, λόγω του ειδικού προτύπου επικοινωνίας τους.

Εφόσον όλα τα πακέτα έχουν τον ίδιο τελικό προορισμό (μιλάμε για δίκτυα με ένα μόνο σταθμό βάσης), ο εκτεθειμένος στην επίθεση κόμβος χρειάζεται μόνο να παρέχει μια καλής ποιότητας διαδρομή στο σταθμό βάσης για να επηρεάσει δυναμικά ένα μεγάλο αριθμό κόμβων.

2.17.4 Επιθέσεις Σίββυλας (Sibyl attacks)

Σε μια επίθεση Σίββυλας ένας κόμβος παρουσιάζει πολλαπλές ταυτότητες στους υπόλοιπους κόμβους του δικτύου.

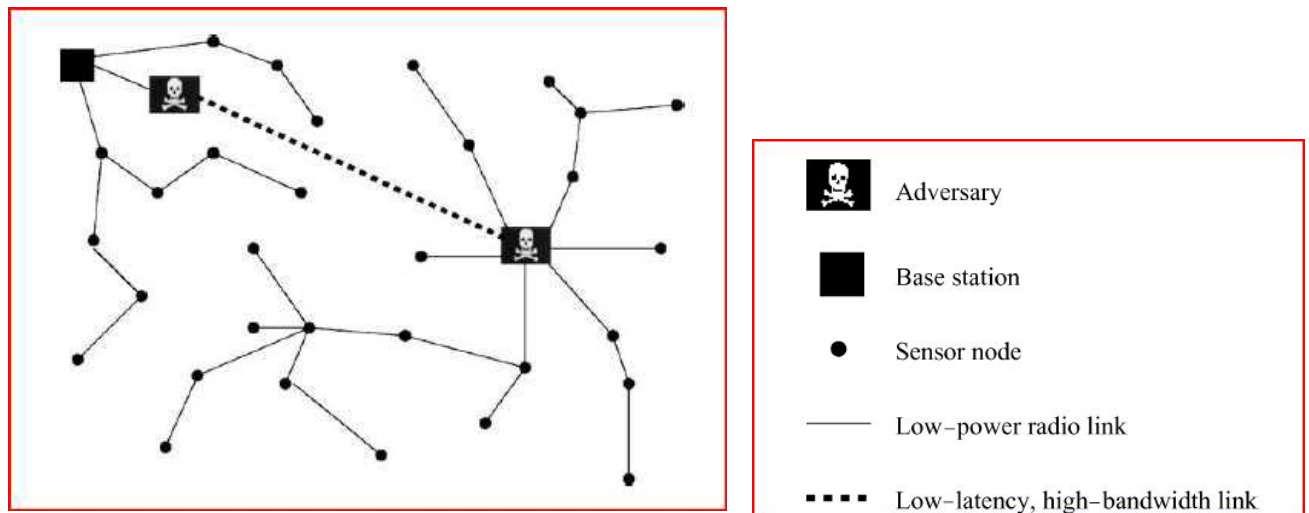
Η επίθεση αυτού του είδους μπορεί να επιδεινώσει την αποτελεσματικότητα διαφόρων μεθόδων που χρησιμοποιούνται για τη μείωση του σφάλματος του δικτύου όπως είναι η κατανεμημένη αποθήκευση, η διασπορά και η multipath δρομολόγηση. Τα αντίγραφα (replicas), τα διαμερίσματα αποθήκευσης (storage partitions) που θα πιστεύαμε ότι χρησιμοποιούν ξεχωριστούς κόμβους μπορεί στην πραγματικότητα να χρησιμοποιούν τον ίδιο (εκτεθειμένο κόμβο) που παρουσιάζεται με διαφορετικές ταυτότητες.

Ιδιαίτερο πρόβλημα δημιουργεί αυτή η επίθεση σε πρωτόκολλα γεωγραφικής δρομολόγησης. Σε πρωτόκολλα δρομολόγησης που βασίζονται στη γνώση της θέσης απαιτείται από τους κόμβους να ανταλλάσσουν πληροφορία των συντεταγμένων με τους γειτονικούς κόμβους για να γίνει αποτελεσματικά η γεωγραφική δρομολόγηση των πακέτων. Είναι λοιπόν λογικό ο κάθε κόμβος να αναμένει ένα μόνο σύνολο συντεταγμένων για κάθε ένα από τους γείτονες του. Στην περίπτωση όμως μιας επίθεσης Σίββυλας ο εισβολέας μπορεί να είναι σε περισσότερα από ένα μέρη την ίδια στιγμή.

2.17.5 Επιθέσεις Wormholes

Στην επίθεση wormhole ο αντίπαλος οδηγεί μέσω μιας σήραγγας τα μηνύματα που λαμβάνονται σε ένα τμήμα του δικτύου μέσω μιας ζεύξης μικρού latency και τα αναπαράγει σε ένα διαφορετικό τμήμα. Ένα απλό παράδειγμα αυτού του είδους απειλής είναι ένας απλός κόμβος μεταξύ δύο άλλων που προωθεί μηνύματα και στους δύο. Συνήθως όμως αυτές οι επιθέσεις περιλαμβάνουν δύο απομακρυσμένους κακόβουλος κόμβους σε συνεννόηση μεταξύ τους ώστε η απόσταση μεταξύ τους να θεωρείται μειωμένη, οι οποίοι εκτρέπουν τα πακέτα μέσω ενός καναλιού εκτός της κανονικής δρομολόγησης που είναι διαθέσιμο μόνο στον εισβολέα.

Ο εισβολέας που μπορεί να εγκατασταθεί πολύ κοντά στο σταθμό βάσης μπορεί με αυτό τον τρόπο να διακόψει τελείως τη δρομολόγηση προς αυτή. Ο εισβολέας μπορεί να πείσει τους κόμβους, οι οποίοι στη κανονική κατάσταση θα χρειάζονταν πολλαπλές «αναπηδήσεις» μέχρι το σταθμό βάσης, ότι βρίσκονται μόνο μία ή δύο «αναπηδήσεις» ως αυτή μέσω του wormhole. Αυτό μπορεί να δημιουργήσει μια καταβόθρα (sinkhole): εφόσον ο εισβολέας από την άλλη πλευρά του wormhole μπορεί τεχνητά να προσφέρει μια καλής ποιότητας διαδρομή στο σταθμό βάσης, μπορεί ενδυνάμει όλη η κίνηση της γύρω περιοχής να κατευθυνθεί προς το wormhole, αν αυτό προσφέρει μια πιο ελκυστική (σύντομη) διαδρομή.



Εικόνα 8: Παράδειγμα επίθεσης που χρησιμοποιεί ένα wormhole για τη δημιουργία καταβόθρας.

2.17.6 Επίθεση τύπου HELLO flood

Πολλά πρωτόκολλα απαιτούν να εκπέμπονται πακέτα μηνυμάτων ‘HELLO’ από ένα κόμβο για να αναγγείλει την παρουσία του στους γειτονικούς κόμβους του. Ένας κόμβος που θα λάβει τέτοια μηνύματα θα υποθέσει ότι βρίσκεται εντός της εμβέλειας ζεύξης με τον κόμβο που τα αποστέλλει. Στην περίπτωση μας αυτή μπορεί να είναι μια ψευδής υπόθεση, γιατί ο εισβολέας που κάνει μια επίθεση HELLO flood μπορεί να έχει εξοπλισμό αρκετής ισχύος που να του επιτρέπει να εκπέμπει από μια απομακρυσμένη θέση στην πραγματικότητα και να παραπλανεί με αυτό τον τρόπο τον αποδέκτη κόμβο.

2.17.7 Επιθέσεις με παραποίηση αναγνώρισης (acknowledgment spoofing)

Σε πολλά δίκτυα αισθητήρων η δρομολόγηση γίνεται με αλγόριθμους που βασίζονται άμεσα ή έμμεσα σε ανταλλαγή μηνυμάτων γνωστοποίησης στο επίπεδο ζεύξης δεδομένων.

Λόγω του μέσου εκπομπής μετάδοσης που χρησιμοποιείται ο εισβολέας μπορεί να παραποιήσει τα μηνύματα γνωστοποίησης του επιπέδου ζεύξης μεταξύ δύο γειτονικών κόμβων.

Σκοπός του είναι να πείσει τον αποστολέα ότι μια αδύναμη ζεύξη είναι ισχυρή ή ότι ένας κόμβος λειτουργεί ενώ στη πραγματικότητα δε λειτουργεί. Για παράδειγμα ένα πρωτόκολλο δρομολόγησης μπορεί να επιλέγει την επόμενη αναπήδηση σε ένα μονοπάτι κάνοντας εκτίμηση της αξιοπιστίας της ζεύξης.

Ένας έξυπνος τρόπος επίθεσης θα ήταν να ενισχυθεί τεχνητά μια αδύναμη ή νεκρή ζεύξη έτσι ώστε να προτιμηθεί από τη δρομολόγηση, μιας και τα πακέτα που στέλνονται σε τέτοιες ζεύξεις χάνονται.

2.18 Επιθέσεις σε συγκεκριμένα πρωτόκολλα δικτύου

Όλα τα προτεινόμενα πρωτόκολλα δρομολόγησης είναι ιδιαίτερα ευάλωτα σε επιθέσεις.

Οι εισβολείς μπορούν να προσελκύσουν ή να απωθήσουν τη ροή της κίνησης των δεδομένων, να αυξήσουν το latency του δικτύου ή να αδρανοποιήσουν ολόκληρο το δίκτυο πολλές φορές καταβάλλοντας τόσο μικρή προσπάθεια, όσο το να στείλουν ένα απλό πακέτο. Στη συνέχεια παρουσιάζονται κάποια από τα πρωτόκολλα δρομολόγησης που έχουν προταθεί για χρήση σε δίκτυα αισθητήρων και τονίζονται οι σχετικές απειλές.

2.18.1 TinyOS beaconing

Κατασκευάζει μια δομή δένδρου με κορυφή το σταθμό βάσης. Ο σταθμός βάσης εκπέμπει περιοδικά μια ενημέρωση για τη διαδρομή. Όλοι οι κόμβοι που λαμβάνουν την ενημέρωση σημειώνουν το σταθμό βάσης σαν τον γονέα τους και αναμεταδίδουν την ενημέρωση. Ο αλγόριθμος συνεχίζει αναδρομικά και κάθε κόμβος σημειώνει σαν γονικό τον κόμβο από τον οποίο έλαβε την ενημέρωση. Όλα τα πακέτα που λαμβάνονται ή παράγονται σε ένα κόμβο προωθούνται στον γονικό κόμβο μέχρις ότου φτάσουν το σταθμό βάσης.

Είναι ιδιαίτερα ευάλωτος σε επιθέσεις όπως συνδυασμένες wormhole-sinkhole καθώς και σε επιθέσεις τύπου Hello flood.

2.18.2 Directed Diffusion

Είναι ένας αλγόριθμος δρομολόγησης δεδομένο-κεντρικός για την εξαγωγή πληροφορίας από ένα δίκτυο αισθητήρων. Οι σταθμοί βάσης κατακλύζουν το δίκτυο με ερωτήματα για συγκεκριμένα δεδομένα δημιουργώντας βαθμίδες μέσα στο δίκτυο για να προσελκύσουν συγκεκριμένα events.

Οι κόμβοι που καταφέρνουν να ικανοποιήσουν τα ερωτήματα, διαδίδουν στη συνέχεια την πληροφορία, χρησιμοποιώντας το αντίστροφο μονοπάτι από αυτό της μετάδοσης.

Οι επιθέσεις που μπορεί να δεχθεί έχουν στόχο:

- Την κατάργηση της ροής δεδομένων DoS
- Την κλωνοποίηση (υποβοηθά την υποκλοπή). Αν ο εισβολέας λάβει την πληροφορία από ένα νόμιμο σταθμό βάσης μπορεί να αναπαράγει το ερώτημα και να θεωρηθεί και αυτός σαν νόμιμος σταθμός βάσης- οι απαντήσεις θα στέλνονται και στον πραγματικό και στον κλώνο σταθμό βάσης.
- Την επιρροή του μονοπατιού: ο εισβολέας μπορεί να επηρεάσει το μονοπάτι που θα ακολουθήσει η ροή των δεδομένων, παραποιώντας θετικές ή αρνητικές ενισχύσεις και δημιουργώντας ψεύτικα γεγονότα.
- Την επιλεκτική προώθηση και παραποίηση των δεδομένων.

2.18.3 Geographic routing (GEAR , Geographic and energy aware routing/ GPSR , greedy perimeter stateless routing)

Είναι αλγόριθμοι που παρέχουν τη γεωγραφική θέση των κόμβων και των προορισμών των πακέτων έτσι ώστε να κάνουν τη διάδοση των ερωτημάτων και των απαντήσεων διαδρομών με αποτελεσματικό τρόπο.

Οι επιθέσεις που μπορεί να δεχθούν: Επιθέσεις τύπου Σίββυλας

2.18.4 Minimum Cost forwarding

Είναι ένας αλγόριθμος για την αποτελεσματική προώθηση πακέτων από τους κόμβους των αισθητήρων στο σταθμό βάσης. Δεν απαιτεί να διατηρούν οι κόμβοι την ακριβή πληροφορία του μονοπατιού ή ακόμα το να υπάρχουν μοναδικά αναγνωριστικά κόμβων.

Κατασκευάζει ένα πεδίο κόστους ξεκινώντας από το σταθμό βάσης, ο οποίος έχει κόστος 0. Κάθε κόμβος διατηρεί το ελάχιστο κόστος που απαιτείται για να φτάσει στο σταθμό βάσης. Το κόστος μπορεί να αντιστοιχεί σε κάποια από τις παρακάτω μετρικές: αριθμός αναπηδήσεων (hop count) , ενέργεια, latency, απώλειες κτλ.

Είναι ιδιαίτερα ευάλωτος σε επιθέσεις όπως sinkhole καθώς και σε επιθέσεις τύπου Hello flood.

2.19 Μέτρα αντιμετώπισης απειλών δρομολόγησης σε δίκτυα αισθητήρων

Η πλειοψηφία των επιθέσεων στη δρομολόγηση ενός δικτύου αισθητήρων μπορεί να προληφθεί με κρυπτογράφηση και πιστοποίηση του επιπέδου ζεύξης με τη χρήση ενός global κλειδιού. Με τον τρόπο αυτό επιθέσεις τύπου Σίββυλας εξουδετερώνονται γιατί οι κόμβοι δεν είναι διατεθειμένοι να δεχθούν ούτε μία από τις πολλαπλές ταυτότητες που μπορεί να πάρει ο κόμβος του εισβολέα. Το ίδιο ισχύει και για επιθέσεις τύπου επιλεκτικής προώθησης και καταβόθρας γιατί ο εισβολέας αποτρέπεται από το να ενταχθεί στην τοπολογία του δικτύου.

Ωστόσο αυτή πρόταση δεν δίνει ικανοποιητική απάντηση για επιθέσεις τύπου 'wormhole' και 'HELLO flood' καθώς και για επιθέσεις που οργανώνονται στο εσωτερικό του δικτύου.

Άλλες προτάσεις:

- κάθε κόμβος να χρησιμοποιεί ένα μοναδικό συμμετρικό κλειδί με τον σταθμό βάσης που θεωρείται αξιόπιστος.
- Δύο κόμβοι μπορούν να χρησιμοποιήσουν ένα πρωτόκολλο τύπου Needham-Schroeder για να πιστοποιήσουν ο ένας την ταυτότητα του άλλου και να εγκαταστήσουν ένα κλειδί που θα μοιράζονται μεταξύ τους. Με βάση αυτό το κλειδί οι γειτονικοί κόμβοι θα μπορούν να δημιουργήσουν μια πιστοποιημένη κρυπτογραφημένη σύνδεση μεταξύ τους. Ο σταθμός βάσης μπορεί να

περιορίσει τον αριθμό των γειτόνων που επιτρέπονται σε ένα κόμβο και να στέλνει ένα μήνυμα σφάλματος όταν αυτός υπερβαίνεται.

- Ειδικά για την περίπτωση επιθέσεων 'HELLO flood' ένας τρόπος άμυνας θα ήταν απλά να επιβεβαιώνεται το μήνυμα που λαμβάνεται και προς τις δύο κατευθύνσεις.
- Ειδικά για τις περιπτώσεις επιθέσεων wormhole και sinkhole επειδή αυτές είναι πολύ δύσκολο να ανιχνευτούν και πολύ δαπανηρό να αντιμετωπιστούν προτείνεται να γίνεται ιδιαίτερη πρόνοια κατά το σχεδιασμό του δικτύου.
- Επιλέγοντας πρωτόκολλα δρομολόγησης όπως για παράδειγμα τα πρωτόκολλα γεωγραφικής δρομολόγησης που παρέχουν μεγαλύτερη ασφάλεια απέναντι σε τέτοιες απειλές.

2.20 Ασφαλής ομαδοποίηση δεδομένων (Data Aggregation) στα Ασύρματα Δίκτυα αισθητήρων

Όπως έχει ήδη αναφερθεί ένα από τα σημαντικότερα προβλήματα που σχετίζεται με το θέμα της ασφάλειας στα δίκτυα αισθητήρων είναι αυτό της κατανάλωσης ενέργειας. Σε προηγούμενες παραγράφους έχει συζητηθεί ότι η πολυπλοκότητα κάποιων αλγορίθμων κρυπτογράφησης ή δρομολόγησης αυξάνουν την υπολογιστική ισχύ που απαιτείται καταναλώνοντας έτσι τη διαθέσιμη ενέργεια του δικτύου και θέτοντας σε κίνδυνο τη λειτουργία του. Πολλές απειλές στοχεύουν ακριβώς στην εξάντληση της διαθέσιμης ενέργειας είτε προβάλλοντας ανάγκη για επιπλέον υπολογισμούς είτε για αναμετάδοση δεδομένων.

Μελέτες όπως του Wagner (2004) και Krishnamachari et al. (2002) έχουν αποδείξει ότι η εκπομπή των δεδομένων καταναλώνει πολύ περισσότερη ενέργεια από ότι η υπολογιστική ισχύς που απαιτείται.

Μια απάντηση σε αυτό το πρόβλημα θα ήταν η ομαδοποίηση των δεδομένων (data aggregation) η οποία μειώνει τα πλεονάζοντα δεδομένα και επομένως την απαίτηση για μετάδοση αυτών.

Ωστόσο τα σημεία στα οποία γίνεται η ομαδοποίηση (aggregators) είναι και αυτά ευάλωτα σε επιθέσεις, ειδικά αν ο εξοπλισμός τους δεν είναι απαραβίαστος.

Όταν ο κόμβος που γίνεται η ομαδοποίηση εκτεθεί σε μια απειλή, είναι εύκολο για τον εισβολέα να αλλάξει το αποτέλεσμα της ομαδοποίησης και να διοχετεύσει ψευδή δεδομένα στο ασύρματο δίκτυο. Ειδικά για τα WSN οι μηχανισμοί ασφαλείας που εφαρμόζονται σε άλλα δίκτυα δεν είναι εφικτοί. Ο λόγος είναι ότι βασίζονται σε κρυπτογράφηση δημόσιου κλειδιού.

Τα υπάρχοντα σχήματα ασφάλειας για την ομαδοποίηση δεδομένων είναι:

- Hop-by-hop κρυπτογράφηση και
- End-to end κρυπτογράφηση της ομαδοποίησης δεδομένων

Τυπικά μπορούμε να διακρίνουμε τους κόμβους ενός ασύρματου δικτύου αισθητήρων στους παρακάτω τύπους:

- Κανονικούς κόμβους αισθητήρων
- Ομαδοποιητές (aggregators) και ένα
- Querier

Οι aggregators συλλέγουν τα δεδομένα από ένα υποσύνολο του δικτύου ομαδοποιούν τα δεδομένα χρησιμοποιώντας μια κατάλληλη συνάρτηση για την ομαδοποίηση και μεταδίδουν το αποτέλεσμα αυτής σε ένα ανώτερο ομαδοποιητή ή σε ένα querier ο οποίος παράγει το ερώτημα. Ο querier είναι επιφορτισμένος με το καθήκον της επεξεργασίας των δεδομένων του αισθητήρα και εξαγωγής πληροφορίας που έχει νόημα και αντανακλά τα γεγονότα που καταγράφονται από τον αισθητήρα από το πεδίο στο οποίο στοχεύει. Το ρόλο αυτό τον παίρνει συνήθως ο σταθμός βάσης αλλά μπορεί να είναι και κάποιος εξωτερικός χρήστης που έχει την άδεια να αλληλεπιδρά με το δίκτυο, ανάλογα με την αρχιτεκτονική του δικτύου. Η επικοινωνία των δεδομένων μεταξύ των παραπάνω κόμβων καταναλώνει ένα μεγάλο ποσοστό των διαθέσιμων πόρων ενέργειας του δικτύου.

Ένα σχήμα ασφάλειας για την ομαδοποίηση των δεδομένων στα WSNs θα πρέπει να έχει τα ακόλουθα χαρακτηριστικά:

- Να παρέχει μια καλή προσέγγιση των καταγραφών των αισθητήρων ακόμα και αν κάποιος από τους κόμβους έχουν εκτεθεί σε κάποια απειλή.
- Να έχουν την ικανότητα να μειώσουν το μέγεθος των δεδομένων που εκπέμπονται μέσω του δικτύου.
- Είναι σημαντικό τα δεδομένα να μην είναι έωλα και να έχουν ακεραιότητα και αυτές οι απαιτήσεις πρέπει να συμπεριληφθούν στο σχήμα. Ωστόσο ο τύπος εφαρμογής του WSN επηρεάζει την απόφαση σχετικά με το αν θα πρέπει να συμπεριληφθεί η εμπιστευτικότητα και η διαθεσιμότητα στο σχεδιασμό.
- Να παρέχει δυναμική απόκριση σε επιθετικές δραστηριότητες μέσω εκτέλεσης μηχανισμού αυτό-ίασης.
- Να έχει μηχανισμό για δυναμική επιλογή/εναλλαγή του aggregator για τη στάθμιση του φόρτου εργασίας των aggregators.

Οι απαιτήσεις για την ασφάλεια ομαδοποίησης δεδομένων στα WSN είναι παρόμοιες με αυτές των παραδοσιακών ασύρματων δικτύων και περιλαμβάνουν:

- Data Confidentiality
- Data Integrity
- Data Freshness
- Data Availability
- Authentication

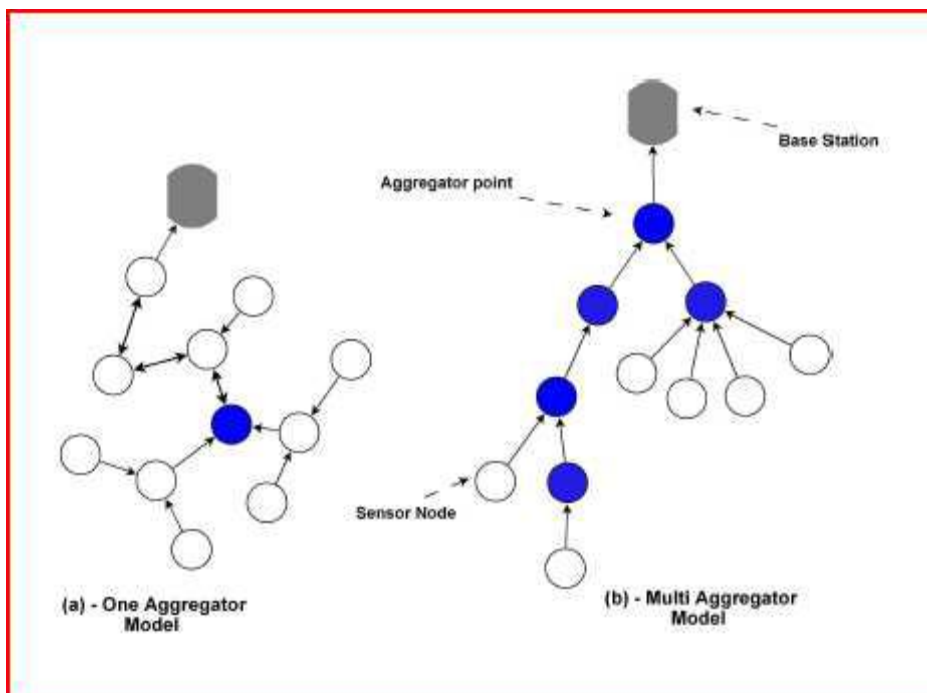
- Non-repudiation: διασφαλίζει ότι ένα πακέτο που μεταφέρεται έχει σταλεί και παραληφθεί από το άτομο το οποίο ισχυρίζεται ότι το έστειλε και το παρέλαβε.
- Data Accuracy

Οι τύποι επιθέσεων απαντώνται κατά την ομαδοποίηση σε ένα WSN είναι:

- Denial of Service (DoS)
- Node Compromise (έκθεση κόμβου σε απειλή).
- Sybil Attack
- Replay Attack (επίθεση αναπαραχθείσας πληροφορίας).
- Stealthy Attack: σε αυτό το είδος απειλής ο εισβολέας έχει σκοπό να διοχετεύσει ψευδή δεδομένα στο δίκτυο χωρίς να αποκαλύπτει την ύπαρξή του.

Τα σχήματα ασφάλειας για data aggregation κατατάσσονται σε δύο μοντέλα:

1. Single Aggregator: Σ' αυτό το μοντέλο η διαδικασία της ομαδοποίησης εκτελείται μόνο μια φορά μεταξύ των κόμβων αισθητήρων και του σταθμού βάσης ή του εξωτερικού χρήστη.
2. Multiple Aggregator: Σ' αυτό το μοντέλο τα δεδομένα που συλλέγονται ομαδοποιούνται περισσότερο από μια φορές πριν να φτάσουν στον τελικό τους προορισμό (querier). Επιτυγχάνει μεγαλύτερη μείωση του αριθμού των bits που εκπέμπονται μέσα στο δίκτυο, πράγμα ιδιαίτερα σημαντικό για δίκτυα μεγάλου μεγέθους.



Εικόνα 9: Αναπαράσταση μοντέλου απλού και πολλαπλού aggregator

2.21 Ασφαλής Εντοπισμός (Localization) στα Ασύρματα Δίκτυα αισθητήρων

Ο εντοπισμός (localization) είναι η διαδικασία με την οποία οι κόμβοι αισθητήρων καθορίζουν τη θέση τους. Είναι με απλά λόγια ένας μηχανισμός για να ανακαλύψουμε τις χωρικές σχέσεις μεταξύ των αντικειμένων.

Υπάρχουν διάφορες προσεγγίσεις για την επίλυση του προβλήματος αυτού, καθεμιά κάνοντας διαφορετική θεώρηση του δικτύου και των δυνατοτήτων του.

Οι υποθέσεις που γίνονται αφορούν τον εξοπλισμό του δικτύου, το μοντέλο μετάδοσης του σήματος, τις απαιτήσεις για ενέργεια και συγχρονισμό, τη σύνθεση του δικτύου (ομογενές-ετερογενές), το περιβάλλον λειτουργίας, το κόστος επικοινωνίας, τις απαιτήσεις σφάλματος, την κινητικότητα των κόμβων (στατικοί, κινητοί και συνδυασμός αυτών) κ.α.

Στα μοντέλα εντοπισμού που χρησιμοποιούν GPS σαν μέσο, η διαδικασία εντοπισμού είναι απλή. Σε ένα μοντέλο όπου χρησιμοποιούνται κόμβοι –φάροι (beacon nodes) για τον εντοπισμό, οι κόμβοι αυτοί είτε ρυθμίζουν χειρονακτικά τη θέση τους ή έχουν κάποιο δέκτη GPS για να την καθορίσουν. Οι κόμβοι αυτοί στη συνέχεια παρέχουν την πληροφορία της θέσης τους στους κόμβους αισθητήρων για να μπορέσουν να κάνουν αυτοί τον υπολογισμό της δικής τους θέσης.

Η διαδικασία του εντοπισμού μπορεί να ταξινομηθεί σε δύο βαθμίδες.

Η πρώτη βαθμίδα απλά εκτιμά την απόσταση ενός κόμβου από τους γειτονικούς του χρησιμοποιώντας ένα ή περισσότερα χαρακτηριστικά του σήματος λήψης.

Στη δεύτερη βαθμίδα, ο κόμβος χρησιμοποιεί όλες τις εκτιμήσεις που έχει κάνει στην πρώτη βαθμίδα για να υπολογίσει τη πραγματική του θέση.

Ο ασφαλής εντοπισμός θέσης στα δίκτυα αισθητήρων έχει τις ίδιες απαιτήσεις που αναφέρθηκαν και στις παραγράφους που αφορούν την ασφάλεια στη δρομολόγηση και την ομαδοποίηση δεδομένων.

Μπορούμε να κατατάξουμε τις τεχνικές εντοπισμού σε δύο κατηγορίες:

1. Άμεσης προσέγγισης (absolute localization): Διακρίνουμε δύο τύπους άμεσης προσέγγισης. Ο πρώτος περιλαμβάνει τη χειρονακτική ρύθμιση. Είναι μια μέθοδος αρκετά δυσκίνητη και ακριβή. Δεν είναι καθόλου πρακτική για δίκτυα μεγάλης κλίμακας ή για επεκτάσιμα δίκτυα.

Ο δεύτερος τρόπος χρησιμοποιεί τον εντοπισμό που βασίζεται σε GPS. Σε αυτή τη μέθοδο κάθε κόμβος αισθητήρα είναι εξοπλισμένος με ένα δέκτη GPS.

Είναι πιο ευέλικτη σε μέθοδος και προσαρμόζεται καλά στα επεκτάσιμα δίκτυα.

Ωστόσο δεν είναι οικονομικά εφικτό να γίνει ο εξοπλισμός όλων των κόμβων (είναι συνήθως της τάξης των χιλιάδων) ενώ αυξάνουν και το μέγεθος του κόμβου αισθητήρα πράγμα που τους κάνει ακατάλληλους για κάποια περιβάλλοντα. Επιπλέον οι δέκτες GPS δουλεύουν καλά όταν βρίσκονται εξωτερικά, πάνω στη γη και ικανοποιούν την απαίτηση οπτικής επαφής. Επομένως δεν είναι κατάλληλη μέθοδος για δίκτυα που βρίσκονται υποβρύχια όπως αυτά που παρακολουθούν το υποθαλάσσιο περιβάλλον, τα επίπεδα μόλυνσης ύδατος, που παρακολουθούν τα tsunami κτλ.

2. Έμμεσης προσέγγισης (relative localization): Οι κόμβοι υπολογίζουν τη θέση τους σε σχέση με τους κόμβους που βρίσκονται στη γειτονία τους. Οι μέθοδοι αυτοί εισήχθησαν για να ξεπεραστούν κάποια από τα μειονεκτήματα των τεχνικών που βασίζονται στη χρήση του GPS, ενώ θα διατηρούν τα πλεονεκτήματα αυτών όπως είναι η ακρίβεια του εντοπισμού.

Στην προσέγγιση αυτή, ένα μικρό υποσύνολο των κόμβων του δικτύου, θα τους ονομάζουμε beacon κόμβους (κόμβοι φάροι), είτε είναι εξοπλισμένοι με δέκτες GPS για να υπολογίσουν τη θέση του ή κάνουν με χειρωνακτικό τρόπο αυτούς τους υπολογισμούς. Οι beacon-κόμβοι εκπέμπουν σήμα δίνοντας με αυτό τη θέση τους σε όλους τους κόμβους αισθητήρων στη γειτονία τους που δεν έχουν δέκτη GPS. Οι κόμβοι αισθητήρες στη συνέχεια χρησιμοποιώντας την πληροφορία του σήματος υπολογίζουν τη δική τους θέση. Αυτή η μέθοδος μειώνει τα επιπλέον έξοδα που θα συνεπάγετο μια άμεση μέθοδος βασισμένη σε GPS. Ωστόσο, ως προς το θέμα της ασφάλειας, πέρα από το ότι γενικά θα ίσχυε και με τις δύο προσεγγίσεις, εδώ εμφανίζεται ένα επιπλέον πρόβλημα: αυτό της παραποίησης των δεδομένων των κόμβων-beacon.

2.22 Διαθέσιμα Ασφαλή Συστήματα Εντοπισμού

2.22.1 SeRLoc

Στην τεχνική αυτή γίνεται η θεώρηση ότι οι κόμβοι του δικτύου είναι δυο τύπων:

- Τύπος N, είναι το σύνολο των κόμβων αισθητήρων που είναι εξοπλισμένοι με πολυκατευθυντική κεραία και
- Τύπος L που είναι ένα σύνολο κόμβων εντοπισμού εξοπλισμένων με κατευθυντικές κεραίες. Οι αισθητήρες καθορίζουν τη θέση τους βασισμένοι στην πληροφορία εντοπισμού που παρέχεται από αυτούς τους εντοπιστές (locators). Κάθε εντοπιστής εκπέμπει σήμα που περιέχει τις εξής πληροφορίες: τις συντεταγμένες του εντοπιστή και τις γωνίες των οριακών γραμμών της κεραίας ως προς ένα κοινό άξονα συντεταγμένων. Η χρήση των κατευθυντικών κεραιών βελτιώνει την ακρίβεια του εντοπισμού.

Στην τεχνική SeRLoc, ο εισβολέας θα πρέπει να υποδυθεί αρκετούς κόμβους-beacon για να μπορέσει να θέσει σε κίνδυνο τη διαδικασία εντοπισμού. Επίσης, επειδή οι κόμβοι αισθητήρων υπολογίζουν τη θέση τους χωρίς τη βοήθεια άλλων αισθητήρων, ο εισβολέας δεν έχει κίνητρο να υποδυθεί τον κόμβο αισθητήρων.

Η τεχνική SeRLoc είναι πολύ ανθεκτική απέναντι σε απειλές τύπου Σίβυλλας και wormhole.

Οι επιθέσεις τύπου Wormhole εξουδετερώνονται λόγω των ιδιοτήτων της τεχνικής SeRLoc: την ιδιότητα της μοναδικότητας του τομέα και την ιδιότητα της παραβίασης του εύρους επικοινωνίας.

Για τη βελτίωση της ακρίβειας θα μπορούσαν να χρησιμοποιηθούν είτε πιο πολλοί εντοπιστές ή πιο πολλές κατευθυντικές κεραίες.

2.22.2 Beacon Suite

Βασίζεται σε μια σειρά από τεχνικές για την ανίχνευση κακόβουλων κόμβων- beacon. Οι κόμβοι - beacon είναι υπεύθυνοι για την παροχή λανθασμένων πληροφοριών στους κόμβους-αισθητήρων, αυτοί με τη σειρά τους παρέχουν την υπηρεσίες εντοπισμού σε διάφορες εφαρμογές του δικτύου.

Η ακολουθία των τεχνικών περιλαμβάνει:

- ανίχνευση σημάτων που προέρχονται από κακόβουλους κόμβους- beacon.
- ανίχνευση αναπαραγωγής σημάτων κόμβων- beacon.
- ταυτοποίηση των κακόβουλων κόμβων- beacon.
- αποφυγή ψευδούς ανίχνευσης
- ανάκληση των κακόβουλων κόμβων- beacon

2.22.3 Attack Resistant Location Estimation

Σε αυτή την κατηγορία προτείνονται δύο μέθοδοι για την αντιμετώπιση κακόβουλων επιθέσεων σε δίκτυο που κάνει τον εντοπισμό θέσης με βάση την πληροφορία κόμβων-beacon.

Στην πρώτη μέθοδο φιλτράρονται τα σήματα κακόβουλων κόμβων- beacon χρησιμοποιώντας την Minimum Mean Square Estimation. Εξετάζονται διάφορα σήματα εντοπισμού από κόμβους- beacon, και ιδιαίτερα η ασυνέπεια μεταξύ των αναφορών της θέσης που παρέχουν. Μέτρο αυτής της ασυνέπειας είναι η μέση τιμή του τετραγώνου του σφάλματος του υπολογισμού θέσης.

Η δεύτερη μέθοδος βασίζεται σε ένα σύστημα ψηφοφορίας. Η περιοχή του δικτύου κβαντίζεται με ένα πλέγμα κελιών. Κάθε αναφορά θέσης μπορεί να 'ψηφίσει' το κελί στο οποίο μπορεί να βρίσκεται ο κόμβος. Με επαναληπτικό τρόπο αυτή η διαδικασία ψήφου μπορεί να ελαχιστοποιήσει την επίδραση των κακόβουλων κόμβων- beacon.

2.22.4 Robust Statistical Methods

Βασίζονται στην ιδέα του φιλτραρίσματος των ακραίων τιμών στους υπολογισμούς που γίνονται κατά την εκτίμηση της θέσης που γίνεται στους κόμβους-αισθητήρων.

2.22.5 SPINE

Η μέθοδος SPINE δουλεύει ως εξής: κάθε κόμβος αισθητήρα συνδέεται με τουλάχιστον 3 σημεία αναφοράς. Χρησιμοποιώντας χρονόμετρα με ακρίβεια nanosecond κάθε αισθητήρας μπορεί να υπολογίσει την απόστασή του από κάθε σημείο αναφοράς του.

2.22.6 ROPE

Σε αυτή την τεχνική στο δίκτυο διακρίνουμε τους κόμβους αισθητήρων και τους κόμβους- locators. Κάθε αισθητήρας μοιράζεται κατά ζεύγη ένα κλειδί με κάθε locator. Ο αριθμός των locator είναι γενικά μικρότερος από τον αριθμό των κόμβων αισθητήρων οπότε δεν υπάρχει ιδιαίτερα επιπλέον ανάγκες για αποθήκευση.

2.22.7 Transmission Range Variation

Βασίζεται σε ένα αλγόριθμο SLA (Secure Location Algorithm), και δεν έχει κάποια εξάρτηση από τον εξοπλισμό του δικτύου.

2.22.8 DRBTS

Στο μοντέλο αυτό οι ψευδείς πληροφορίες που παρέχονται από κακόβουλους κόμβους- beacon, αποκλείονται κατά τη διαδικασία του εντοπισμού.

Αυτό επιτυγχάνεται επιτρέποντας στους κόμβους-beacon να παρακολουθούν ο ένας τον άλλον και να παρέχουν την πληροφορία έτσι ώστε ο κόμβος-αισθητήρα να μπορεί να αποφασίσει ποιον να εμπιστευτεί. Για να πάρει αυτή την απόφαση, ο κόμβος αισθητήρων πρέπει να πάρει ψήφους αξιοπιστίας τουλάχιστον από τους μισούς γειτονικούς του κόμβους.

2.22.9 HiRLoc

Στο μοντέλο αυτό οι αισθητήρες καθορίζουν τη θέση τους με παθητικό τρόπο χωρίς καμιά αλληλεπίδραση μεταξύ τους. Η εκπομπή του κόμβου – beacon είναι κρυπτογραφημένη χρησιμοποιώντας ένα global συμμετρικό κλειδί. Είναι πολύ ανθεκτική απέναντι σε απειλές τύπου Σίβυλλας και wormhole και έκθεσης κόμβου.

2.23 Σύνοψη

Παρουσιάστηκαν ο σκοπός, η δομή και τα ιδιαίτερα ζητήματα ασφάλειας των δικτύων αισθητήρων.

Αναφέρθηκαν τα είδη των απειλών.

Εξετάστηκε ιδιαίτερα η ασφάλεια στη δρομολόγηση, στην ομαδοποίηση δεδομένων και στον εντοπισμό θέσης και παράλληλα παρουσιάστηκαν κάποιες από τις τεχνικές που έχουν προταθεί για την αντιμετώπιση τους.

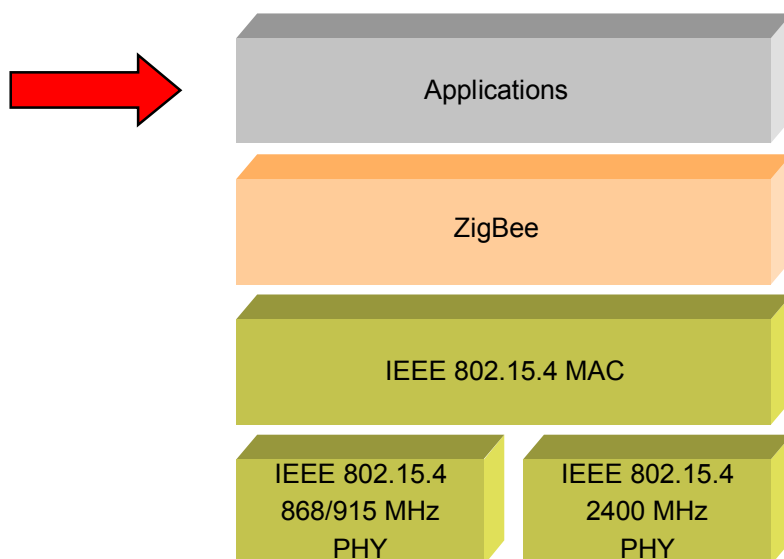
ΚΕΦΑΛΑΙΟ 3 : ZigBee και IEEE 802.15.4

3.1 Τι είναι το ZigBee

Το ZigBee είναι ένα πρότυπο ασύρματης δικτύωσης μικρής εμβέλειας που υποστηρίζεται από κορυφαίες εταιρείες του κλάδου όπως η Motorola, Texas Instruments, Philips, Samsung, Siemens, Freescale, κλπ. Υποστηρίζει mesh δικτύωση, καθώς κάθε κόμβος μπορεί να μεταδώσει και να λάβει δεδομένα, προσφέρει υψηλή ασφάλεια και ευρωστία, έχει υιοθετηθεί από τις βιομηχανίες, προσφέρεται για έλεγχο / παρακολούθηση και χρησιμοποιείται σε ιατρικές εφαρμογές.

Το ZigBee και το IEEE 802.15.4 βασίζονται σε πρότυπα πρωτόκολλα που παρέχουν την υποδομή του δικτύου που απαιτείται για εφαρμογές ασύρματων δικτύων αισθητήρων. Το 802.15.4 ορίζει το φυσικό και το MAC στρώμα, και το ZigBee καθορίζει το δίκτυο και τα στρώματα της εφαρμογής. Για εφαρμογές δικτύων αισθητήρων, οι βασικές απαιτήσεις σχεδιασμού περιστρέφονται γύρω από τη μεγάλη διάρκεια ζωής της μπαταρίας, το χαμηλό κόστος, το μικρό αποτύπωμα, και τη δικτύωση των κόμβων για να υποστηρίξει την επικοινωνία μεταξύ μεγάλων αριθμών συσκευών σε ένα διαλειτουργικό και πολλαπλό περιβάλλον εφαρμογών.

802.15.4 / ZigBee Architecture



Σχήμα 1

3.2 Τυπικές εφαρμογές

Υπάρχουν πολλές εφαρμογές που είναι ιδανικές για τις υπεράριθμες, και αυτορυθμιζόμενες δυνατότητες των ZigBee ασύρματων δικτύων πλέγματος. Βασικά αυτές περιλαμβάνουν:

- Ασύρματα δίκτυα αισθητήρων
- Συστήματα ελέγχου για το σπίτι
- Συστήματα ελέγχου για βιομηχανίες
- Ιατρική συλλογή δεδομένων μέσω βιοαισθητήρων

Η διαλειτουργική φύση του ZigBee σημαίνει ότι αυτές οι εφαρμογές μπορούν να συνεργαστούν, παρέχοντας ακόμα μεγαλύτερα οφέλη.

3.3 Κίνητρα για ZigBee

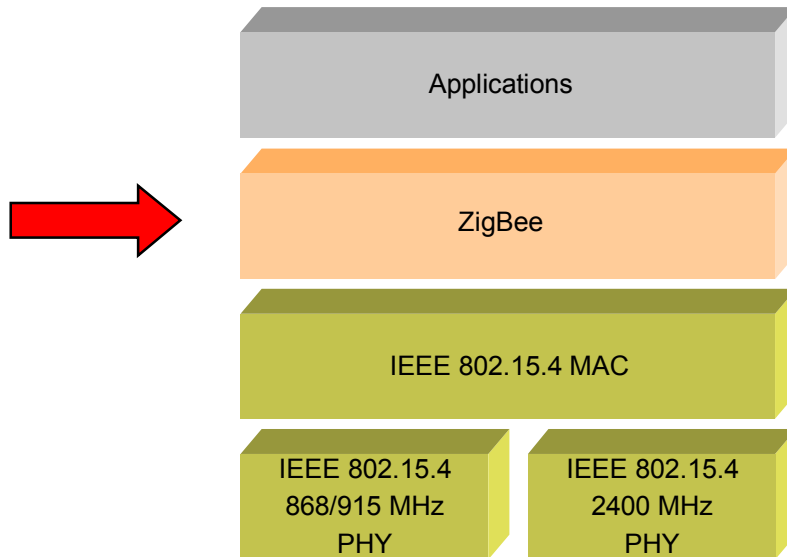
Το πρότυπο ZigBee αναπτύχθηκε για να αντιμετωπίσει τις ακόλουθες ανάγκες:

- Χαμηλό κόστος
- Ασφάλεια
- Αξιοπιστία και αυτοθεραπεία
- Ευελιξία και επεκτασιμότητα
- Χαμηλή κατανάλωση ενέργειας
- Εύκολη και ανέξοδη για την ανάπτυξη

Το ZigBee είναι το μόνο πρότυπο βασισμένο στην τεχνολογία που θα ανταποκρίνεται στις μοναδικές ανάγκες για παρακολούθηση και έλεγχο από απόσταση για αισθητήριες εφαρμογές δικτύου.

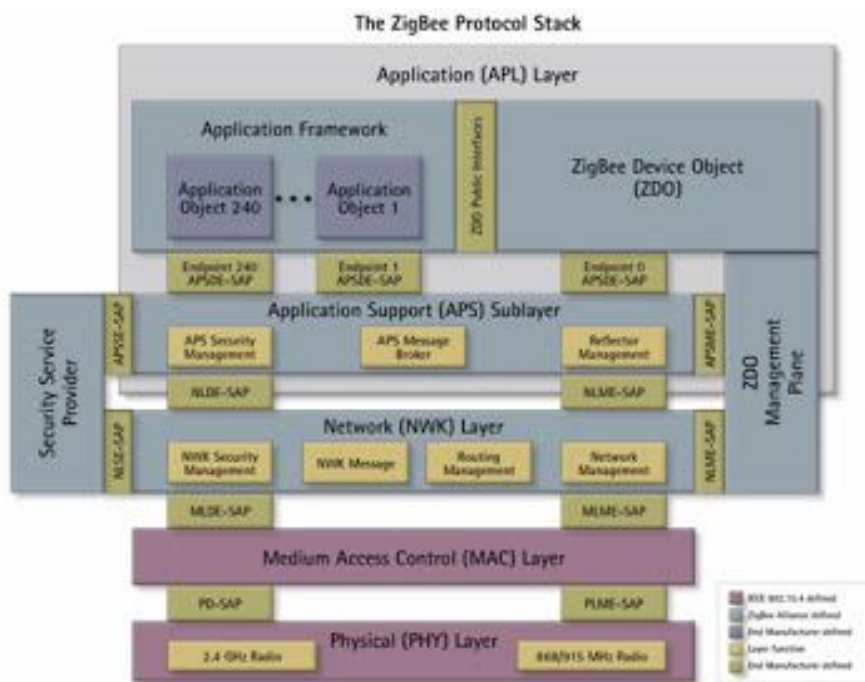
3.4 The ZigBee Protocol Stack

802.15.4 / ZigBee Architecture



Σχήμα 2

Κάθε στρώμα εκτελεί ένα συγκεκριμένο σύνολο υπηρεσιών για το πιο πάνω στρώμα. Κάθε φορέας παροχής υπηρεσιών παρέχει μια διεπαφή για το ανώτερο στρώμα μέσω ενός σημείου πρόσβασης υπηρεσίας (SAP).



Εικόνα 10: The ZigBee Protocol Stack

3.4.1 Application (APL) Layer

Το κορυφαίο στρώμα της στοίβας ZigBee, αποτελείται από το πλαίσιο εφαρμογής, το αντικείμενο συσκευής ZigBee (ZDO), και το υπόστρωμα υποστήριξης εφαρμογών (APS).

3.4.2 Application Framework

Παρέχει μια περιγραφή για το πώς να κτιστεί ένα προφίλ στη στοίβα ZigBee. Διευκρινίζει, επίσης, μια σειρά από βασικούς τύπους δεδομένων για τα προφίλ.

3.4.3 Application Objects

Το λογισμικό θεωρείται ως μια παράμετρος που ελέγχει τη συσκευή ZigBee. Ένας ενιαίος κόμβος ZigBee υποστηρίζει έως και 240 αντικείμενα εφαρμογής. Κάθε αντικείμενο εφαρμογής υποστηρίζει τελικά σημεία που αριθμούνται μεταξύ 1 και 240.

3.4.4 ZigBee Device Object (ZDO)

Καθορίζει το ρόλο μιας συσκευής στο δίκτυο (συντονιστής, δρομολογητής ή τερματική συσκευή), η οποία εκκινεί ή / και ανταποκρίνεται στις δεσμεύσεις και στην ανακάλυψη των αιτήσεων, και καθιερώνει μια ασφαλή σχέση μεταξύ των συσκευών του δικτύου. Παρέχει επίσης μια πλούσια σειρά από εντολές διαχείρισης που καθορίζονται στο προφίλ συσκευής ZigBee.

3.4.5 ZDO Management Plane

Διευκολύνει την επικοινωνία μεταξύ των APS και NWK στρωμάτων με την ZDO. Επιτρέπει στην ZDO να ασχοληθεί με το χειρισμό των αιτήσεων για την πρόσβαση στο δίκτυο, και την ασφάλεια χρησιμοποιώντας ZDP (ZigBee Device Profile) μηνύματα.

3.4.6 Application Support (APS) Sublayer

Υπεύθυνο για την παροχή υπηρεσιών δεδομένων στην εφαρμογή και στο προφίλ των ZigBee συσκευών. Παρέχει επίσης μια υπηρεσία διαχείρισης για τη διατήρηση και αποθήκευση των υπαρχόντων συνδέσεων.

3.4.7 Security Service Provider (SSP)

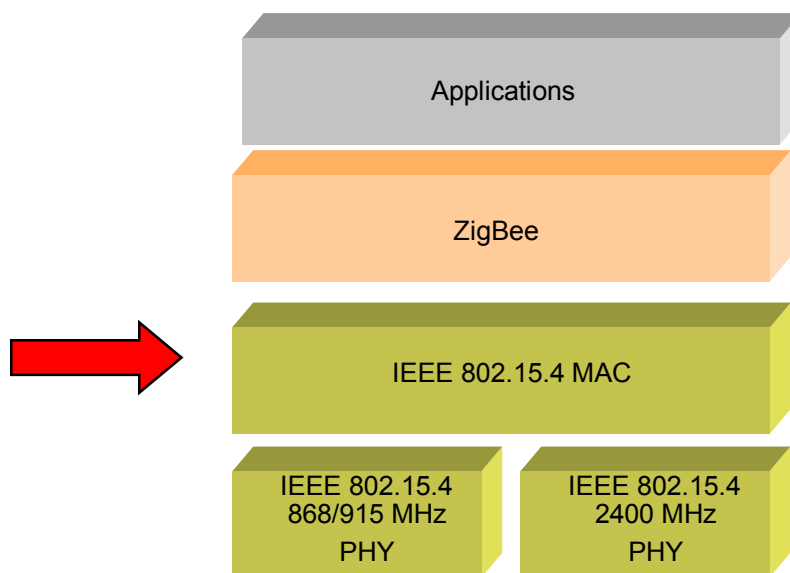
Παρέχει μηχανισμούς ασφαλείας στην αποκρυπτογράφηση των στρωμάτων (NWK και APS). Προετοιμάζεται και ρυθμίζεται μέσω του ZDO.

3.4.8 Network (NWK) Layer

Χειρίζεται τη διεύθυνση δικτύου και τη δρομολόγηση επικαλούμενο δράσεις στο στρώμα MAC. Τα καθήκοντά του περιλαμβάνουν την έναρξη του δικτύου (συντονιστής), την ανάθεση διευθύνσεων στο δίκτυο, την προσθαφαίρεση συσκευών δικτύου, τη δρομολόγηση των μηνυμάτων, και την ασφάλεια αυτού.

3.5 IEEE 802.15.4

802.15.4 Architecture



Σχήμα 3

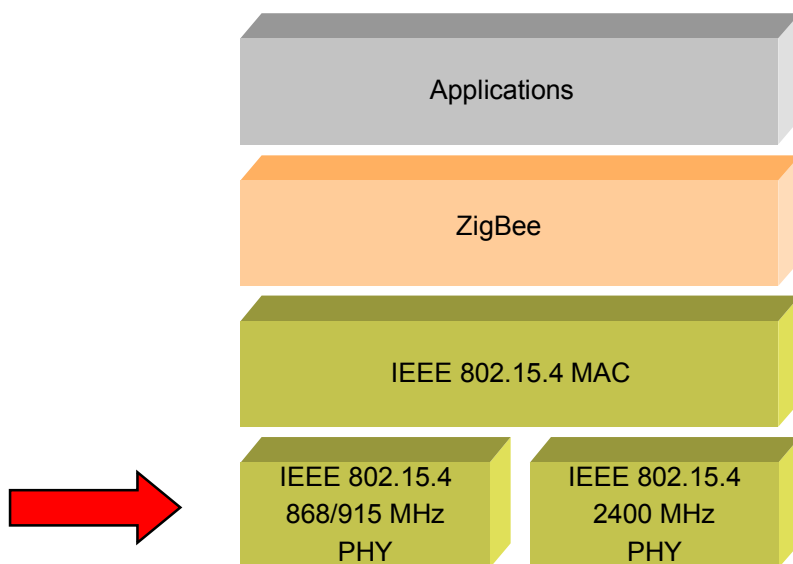
3.5.1 Medium Access Control (MAC) Layer

Υπεύθυνος για την παροχή αξιόπιστης επικοινωνίας μεταξύ ενός κόμβου και των άμεσων γειτόνων του, συμβάλλοντας στην αποφυγή συγκρούσεων και στη βελτίωση της αποτελεσματικότητας. Το στρώμα MAC είναι επίσης υπεύθυνο για τη συναρμολόγηση και την αποσύνθεση των πακέτων δεδομένων και πλαισίων.

3.5.1.1 Design Drivers

- Εξαιρετικά χαμηλό κόστος
- Ευκολία εφαρμογής
- Αξιόπιστη μεταφορά δεδομένων
- Λειτουργία μικρής εμβέλειας
- Πολύ χαμηλή κατανάλωση ενέργειας

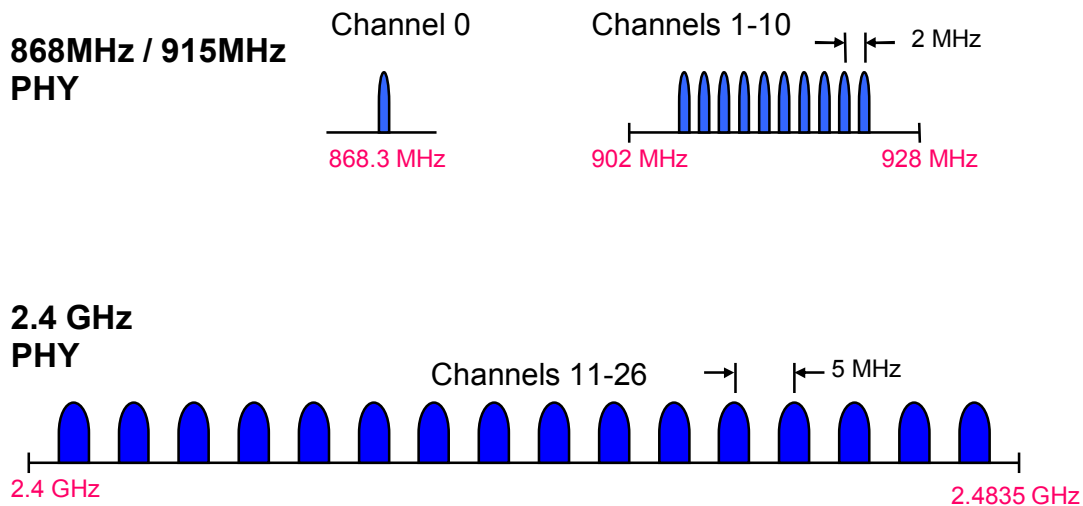
802.15.4 Architecture



Σχήμα 4

3.5.2 Physical (PHY) Layer

Παρέχει τη διασύνδεση με το φυσικό μέσο μετάδοσης (π.χ. ραδιόφωνο). Το PHY αποτελείται από δύο στρώματα που λειτουργούν σε δύο ξεχωριστές περιοχές συχνοτήτων. Η χαμηλότερη συχνότητα PHY στρώμα καλύπτει τόσο την ευρωπαϊκή ζώνη 868MHz και 915MHz μπάντα που χρησιμοποιούνται σε χώρες όπως οι ΗΠΑ και η Αυστραλία. Η υψηλότερη συχνότητα PHY στρώμα (2.4GHz) χρησιμοποιείται σχεδόν σε όλο τον κόσμο.



Εικόνα 11: Operating Frequency Bands

Ενώ και τα δύο αυτά ασύρματα πρότυπα ασχολούνται με εφαρμογές υψηλότερου εύρους ζώνης πρόσβασης στο Διαδίκτυο, το 802.15.4 αναπτύχθηκε με χαμηλότερο ρυθμό μετάδοσης δεδομένων, για απλή συνδεσιμότητα και χαμηλή κατανάλωση ενέργειας. Το πρότυπο 802.15.4 ορίζει ότι η επικοινωνία μπορεί να κυμαίνεται στα 868 - 868,8 MHz, στα 902-928 MHz ή 2,400 - 2,4835 GHz για τις βιομηχανικές, επιστημονικές και ιατρικές (ISM) ζώνες. Αν οποιαδήποτε από αυτές τις μπάντες είναι τεχνικά δυνατόν να χρησιμοποιηθεί από τις συσκευές , η ζώνη των 2,4 GHz είναι πιο δημοφιλής, καθώς είναι ανοιχτή στις περισσότερες χώρες σε όλο τον κόσμο. Τα 868 MHz, καθορίζονται κατά κύριο λόγο για ευρωπαϊκή χρήση , ενώ η ζώνη 902-928 MHz μπορεί να χρησιμοποιηθεί μόνο στις Ηνωμένες Πολιτείες, τον Καναδά και σε μερικές άλλες χώρες και εδάφη που δέχονται την FCC (**Federal Communications Commission**) Ομοσπονδιακή Επιτροπή Επικοινωνιών.

Το πρότυπο 802.15.4 ορίζει ότι η επικοινωνία πρέπει να γίνεται σε κανάλια των 5 MHz που κυμαίνονται μεταξύ 2,405 - 2,480 GHz . Στη ζώνη συχνοτήτων 2,4 GHz, κατ 'ανώτατο όριο over-the -air, ο ρυθμός δεδομένων έχει καθοριστεί στα 250 kbps, αλλά λόγω του γενικού του πρωτοκόλλου το πραγματικό θεωρητικό μέγιστο ποσοστό των δεδομένων είναι περίπου το μισό από αυτό. Ενώ το πρότυπο καθορίζει κανάλια των 5 MHz, μόνο τα 2 MHz περίπου του καναλιού καταναλώνονται από το χρησιμοποιούμενο εύρος ζώνης. Στα 2,4 GHz, το 802.15.4 καθορίζει τη χρήση του Direct Sequence Spread Spectrum και χρησιμοποιεί ένα Offset Quadrature Phase Shift Keying (O - QPSK) με παλμό μισού ημιτόνου διαμόρφωσης ώστε να διαμορφώνει το RF φορέα.

3.6 The ZigBee Network

3.6.1 Τύποι συσκευών

Τα δίκτυα ZigBee περιλαμβάνουν τους ακόλουθους τύπους συσκευών:

- Συντονιστές
- Δρομολογητές
- Τερματικές συσκευές

3.6.1.1 Συντονιστής

Αυτή η συσκευή ξεκινά και ελέγχει το δίκτυο. Επιτρέπει στους δρομολογητές και στις τερματικές συσκευές να ενταχθούν στο δίκτυο. Ο συντονιστής αποθηκεύει πληροφορίες σχετικά με το δίκτυο, το οποίο περιλαμβάνει τις δράσεις ως Κέντρο αξιοπιστίας και είναι η αποθήκη για τα κλειδιά ασφαλείας. Στα δίκτυα ZigBee ο συντονιστής πρέπει να επιλέξει ένα PAN ID (64-bit and 16-bit) και ένα κανάλι για να τεθεί σε λειτουργία το δίκτυο. Μετά από αυτό συμπεριφέρεται κατ'ουσίαν ως δρομολογητής. Τέλος ο συντονιστής πρέπει να είναι πάντα σε λειτουργία.

3.6.1.2 Δρομολογητής

Αυτές οι συσκευές επεκτείνουν την περιοχή κάλυψης του δικτύου, τη δυναμική διαδρομή γύρω από τα εμπόδια, και παρέχουν εναλλακτικές διαδρομές σε περίπτωση συμφόρησης του δικτύου ή βλάβης της συσκευής. Μπορούν να συνδεθούν με το συντονιστή και με άλλους δρομολογητές, και επίσης υποστηρίζουν συσκευές «παιδί». Τέλος ο δρομολογητής πρέπει να είναι πάντα σε λειτουργία.

3.6.1.3 Τερματικές συσκευές

Αυτές οι συσκευές μπορούν να μεταδώσουν ή να λάβουν ένα μήνυμα, αλλά δεν μπορούν να εκτελέσουν οποιαδήποτε δρομολόγηση εργασιών. Θα πρέπει να συνδεθούν είτε στον συντονιστή ή σε ένα δρομολογητή, και δεν υποστηρίζουν συσκευές «παιδί». Τέλος οι τερματικές συσκευές εάν χρειαστεί μπορούν και να τεθούν εκτός λειτουργίας.

3.6.2 Κατηγορίες συσκευών

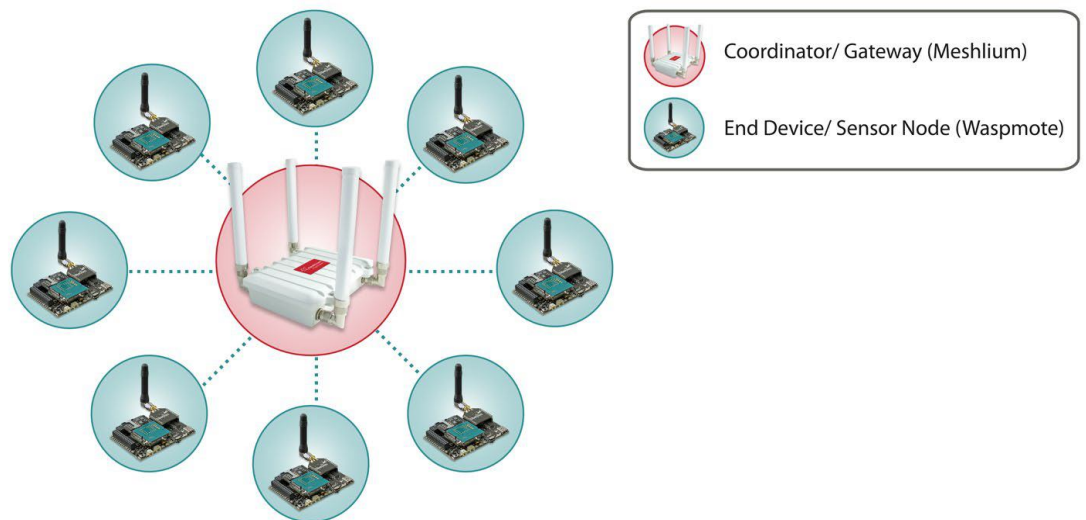
3.6.2.1 Συσκευή πλήρης λειτουργίας (FFD)

- Κάθε τοπολογία
- Ικανή για συντονιστής δικτύου
- Επικοινωνεί με οποιαδήποτε άλλη συσκευή

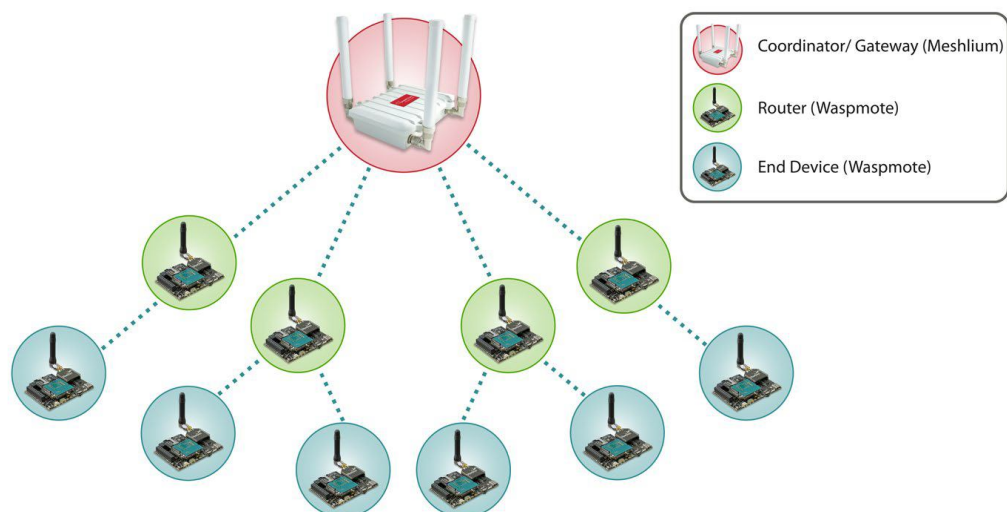
3.6.2.2 Συσκευή μειωμένης λειτουργίας (RFD)

- Περιορίζεται σε τοπολογία αστέρα
- Δεν μπορεί να γίνει συντονιστής δικτύου
- Επικοινωνεί μόνο με ένα συντονιστή δικτύου
- Πολύ απλή εφαρμογή

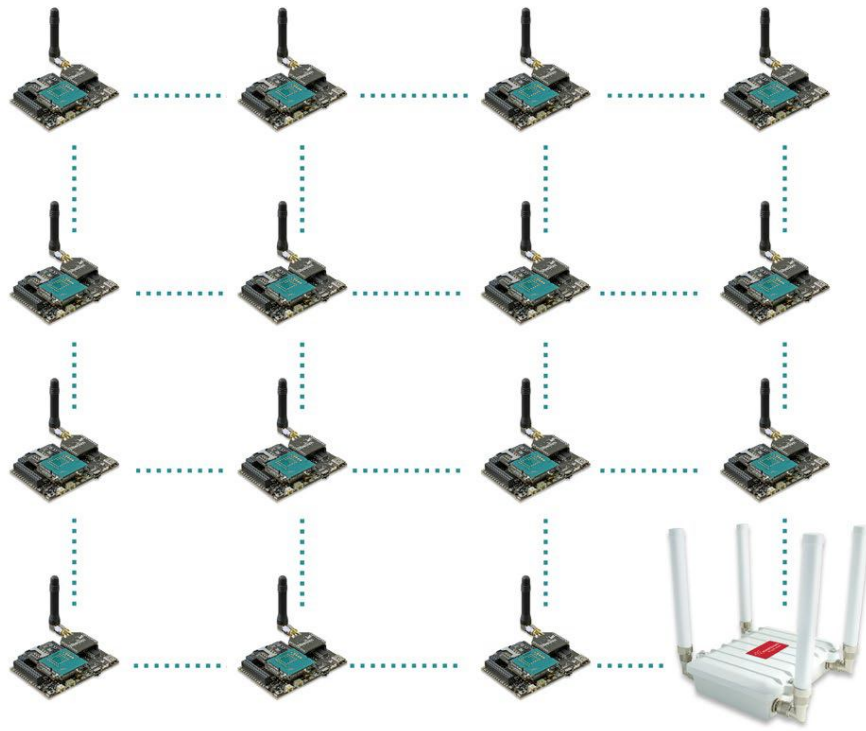
3.6.3 Typical Network Topologies



Εικόνα 12: Τοπολογία αστέρα



Εικόνα 13: Τοπολογία δέντρου



Εικόνα 14: Τοπολογία πλέγματος

ETRX2 USB stick –PC

```

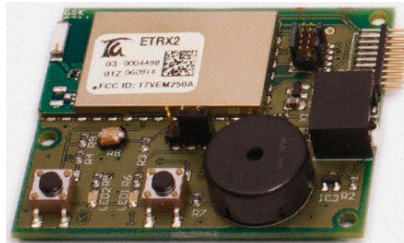
Status:    Connected to COM6
OK
LeftPAN
AT+JN
JPAN: 21, 2E01
OK
AT+SN
OK
FFD: 000D6F000019D936
FFD: 000D6F0000178D6A
FFD: 000D6F0000178E0F
FFD: 000D6F00001BF435
    
```

MCB - Node 3

Discover Devices

Name	Device ID	Device
Node1	000D6F000019D936	FFD
Node2	000D6F0000178D6A	FFD
Node3	000D6F0000178E0F	FFD
Node4	000D6F00001BF435	FFD

MCB - Node 1



MCB - Node2



Development board - Node 4

Σχήμα 5: Παράδειγμα τοπολογίας αστέρα

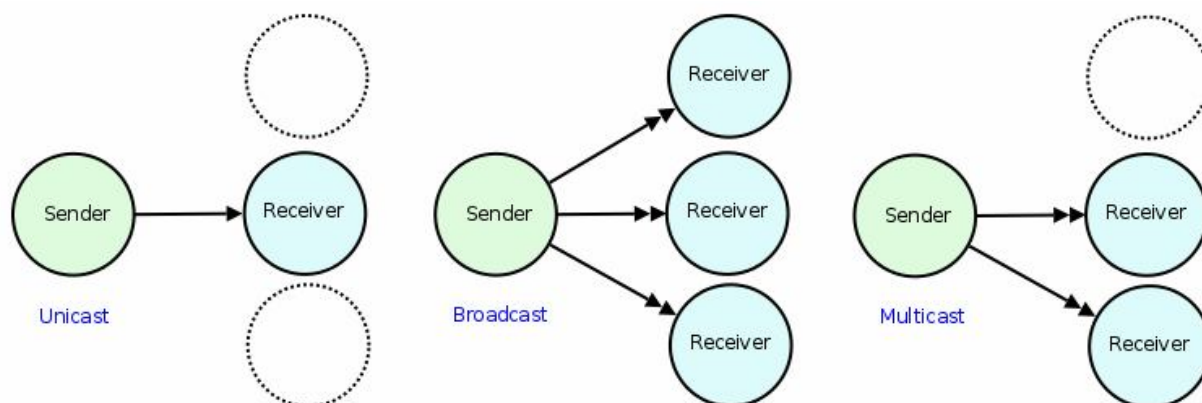
Η τοπολογία πλέγματος, που ονομάζεται επίσης peer-to-peer, αποτελείται από ένα πλέγμα διασυνδεδεμένων δρομολογητών και τερματικών συσκευών. Κάθε δρομολογητής τυπικά συνδέεται μέσω δύο τουλάχιστον οδών, και μπορεί να μεταδίδει μηνύματα για τους γείτονές της. Ένα δίκτυο πλέγματος περιέχει ένα ενιαίο συντονιστή, πολλαπλούς δρομολογητές και τερματικές συσκευές. Η τοπολογία πλέγματος υποστηρίζει multi-hop επικοινωνία, μέσω της οποίας τα δεδομένα μεταδίδονται, μεταπηδώντας από συσκευή σε συσκευή χρησιμοποιώντας τις πιο αξιόπιστες συνδέσεις επικοινωνίας και την πιο οικονομικά αποδοτική διαδρομή μέχρι τον τελικό προορισμό τους. Η multi-hop ικανότητα βοηθά επίσης να παρέχει ανοχή σε σφάλματα, υπό την έννοια ότι, αν μια συσκευή αποτύχει ή βιώνει παρεμβολές, το δίκτυο μπορεί να αναδρομολογηθεί χρησιμοποιώντας τις υπόλοιπες συσκευές.

3.6.4 Οφέλη

- Αυτή η τοπολογία είναι εξαιρετικά αξιόπιστη και ανθεκτική. Σε περίπτωση που κάποιος δρομολογητής καταστεί απρόσιτος, εναλλακτικές διαδρομές μπορεί να ανακαλυφθούν και να χρησιμοποιηθούν.
- Η χρήση των ενδιάμεσων συσκευών στην μετεγκατάσταση των δεδομένων σημαίνει ότι το εύρος του δικτύου μπορεί να αυξηθεί σημαντικά, καθιστώντας τα δίκτυα πλέγματος εξαιρετικά επεκτάσιμα.
- Τα ασθενή σήματα και οι νεκρές ζώνες μπορούν να εξαλειφθούν με την απλή προσθήκη περισσότερων δρομολογητών στο δίκτυο.

3.7 Συνδέσεις

Τα δεδομένα μπορούν να αποστέλλονται χρησιμοποιώντας broadcast, unicast ή multicast συνδέσεις.



Εικόνα 15: Τύποι συνδέσεων

3.7.1 Broadcast

Οι broadcast μεταδόσεις εντός του πρωτοκόλλου ZigBee προορίζονται να πολλαπλασιάζονται σε ολόκληρο το δίκτυο, έτσι ώστε όλοι οι κόμβοι να λαμβάνουν τη μετάδοση. Για να επιτευχθεί αυτό, όλες οι συσκευές που λαμβάνουν broadcast μετάδοση θα αναμεταδίδουν το πακέτο 3 φορές. Κάθε κόμβος που μεταδίδει broadcast θα δημιουργήσει επίσης μια καταχώρηση σε ένα τοπικό πίνακα μετάδοσης. Αυτή η καταχώρηση χρησιμοποιείται για την παρακολούθηση κάθε εισερχόμενου broadcast πακέτου ώστε να εξασφαλίσει ότι τα πακέτα δεν μεταδίδονται ασταμάτητα. Για κάθε μετάδοση, η στοίβα ZigBee πρέπει να κρατήσει χώρο στο buffer για ένα αντίγραφο του πακέτου δεδομένων. Δεδομένου ότι οι broadcast μεταδόσεις

αναμεταδίδονται από κάθε συσκευή στο δίκτυο, τα broadcast μηνύματα θα πρέπει να χρησιμοποιούνται με φειδώ.

Οι broadcast μεταδόσεις αποστέλλονται χρησιμοποιώντας μια 64-bit διεύθυνση του τύπου 0x000000000000FFFF. Κάθε RF κόμβος στο PAN δέχεται ένα πακέτο που περιέχει μια broadcast διεύθυνση. Όταν ρυθμιστεί να λειτουργεί σε Broadcast Mode, οι κόμβοι που δέχονται τα δεδομένα δεν στέλνουν ACKs (Επιβεβαιώσεις).

3.7.2 Unicast

Οι Unicast ZigBee μεταδόσεις απευθύνονται πάντα στο γεγονός ότι η διεύθυνση της συσκευής προορισμού είναι 16-bit . Ωστόσο, μόνο η 64-bit διεύθυνση μιας συσκευής είναι μόνιμη, λόγω του ότι η 16-bit διεύθυνση μπορεί να αλλάξει. Ως εκ τούτου, οι συσκευές ZigBee μπορούν να χρησιμοποιήσουν την ανακαλυφθείσα διεύθυνση δικτύου και διαδρομή για να προσδιορίσουν την τρέχουσα 16-bit διεύθυνση που αντιστοιχεί σε μια γνωστή 64-bit και να καθιερώσουν μία διαδρομή.

3.7.2.1 Network Address Discovery

Οι μεταδόσεις δεδομένων αποστέλλονται πάντα στην 16-bit διεύθυνση δικτύου της συσκευής προορισμού. Ωστόσο, δεδομένου ότι η 64-bit διεύθυνση είναι μοναδική για κάθε συσκευή, είναι γενικά γνωστό ότι οι συσκευές ZigBee πρέπει να ανακαλύψουν τη διεύθυνση του δικτύου που ανατέθει σε μια συγκεκριμένη συσκευή, όταν εντάχθηκε στο PAN πριν ακόμη μπορέσουν να μεταδίδουν δεδομένα.

Για να γίνει αυτό, η συσκευή ξεκινά τη μετάδοση στέλνοντας μία υπάρχουσα broadcast διεύθυνση δικτύου σε όλο το δίκτυο. Οι συσκευές που λαμβάνουν αυτή την broadcast μετάδοση ελέγχουν να δουν εάν η 64-bit διεύθυνση τους ταιριάζει με τη 64-bit διεύθυνση που εμπεριέχεται στην broadcast μετάδοση. Εάν οι διευθύνσεις ταιριάζουν, η συσκευή στέλνει ένα πακέτο επιβεβαίωσης πίσω στην πηγή, παρέχοντας τη διεύθυνση δικτύου της συσκευής με το ταίριασμα της 64-bit διεύθυνσης. Όταν αυτή η απάντηση παραληφθεί, η πηγή μπορεί στη συνέχεια να μεταδώσει δεδομένα.

3.7.2.2 Route Discovery

Το ZigBee χρησιμοποιεί την δρομολόγηση πλέγματος για να καθιερώσει μια διαδρομή μεταξύ της πηγής και του προορισμού. Οι δρομολογητές και οι συντονιστές μπορούν να συμμετέχουν στην καθιέρωση διαδρομών μεταξύ πηγής και προορισμού χρησιμοποιώντας μια διαδικασία που ονομάζεται εντοπισμός διαδρομής. Η διαδικασία ανακάλυψης διαδρομής βασίζεται στο AODV (Ad-hoc On demand Distance Vector δρομολόγησης) πρωτόκολλο.

3.7.2.3 Retries and ACKs

Το ZigBee περιλαμβάνει πακέτα επιβεβαίωσης τόσο σε στρώματα Mac όσο και σε στρώματα Υποστήριξης Εφαρμογών (APS). Όταν τα δεδομένα μεταδίδονται σε μια απομακρυσμένη συσκευή, μπορούν να διασχίσουν πολλούς κόμβους, ώστε να φτάσουν στον προορισμό. Καθώς τα δεδομένα μεταδίδονται από τον ένα κόμβο στον γειτονικό του, ένα πακέτο επιβεβαίωσης (ACK) μεταδίδεται προς την αντίθετη κατεύθυνση έτσι ώστε να δείξει ότι η μετάδοση έγινε δεκτή με επιτυχία. Εάν το πακέτο επιβεβαίωσης (ACK) δεν παραληφθεί, η συσκευή μεταδόσεως θα αναμεταδώσει τα δεδομένα μέχρι 4 φορές. Αυτό το (ACK) ονομάζεται Mac στρώμα επιβεβαίωσης. Επιπλέον, η συσκευή από την οποία προήλθε τη μετάδοση αναμένει να λάβει ένα πακέτο επιβεβαίωσης (ACK) από τη συσκευή προορισμού. Αυτό το (ACK) θα διασχίσει την ίδια διαδρομή που διέσχισαν τα δεδομένα, αλλά προς την αντίθετη κατεύθυνση. Εάν ο εντολέας δεν λάβει αυτό το πακέτο επιβεβαίωσης, αυτό θα αναμεταδοθεί μέχρι 2 φορές μέχρι να ληφθεί ένα ACK. Αυτό το (ACK) ονομάζεται στρώμα επιβεβαίωσης ZigBee Υποστήριξης Εφαρμογών (APS).

3.7.3 Many to one

Από την στιγμή που οι ZigBee unicast μεταδόσεις μπορεί να χρειάζονται κάποιο συνδυασμό broadcast διεύθυνσης δικτύου και διαδρομής, το να μεταδίδει unicast σε μια μόνο πύλη εξόδου (gateway) ή σε μια συσκευή συλλογής δεδομένων μπορεί να μην είναι η καλύτερη λύση για τα μεγάλα δίκτυα δεδομένου της ύπαρξης μεγάλου αριθμού συσκευών.

Για την επίλυση αυτού του πιθανού προβλήματος, το ZigBee περιλαμβάνει διατάξεις για την υποστήριξη μεταδόσεων πολλών-προς-έναν, όπου πολλές συσκευές σε ένα δίκτυο μπορούν να μεταδίδουν δεδομένα σε μια πύλη εξόδου ή μια συσκευή συλλογής δεδομένων χωρίς να προκαλούν υπερφόρτιση στις υπάρχουσες διαδρομές. Για να επιτευχθεί αυτό, η συσκευή συλλογής δεδομένων στέλνει μία περιοδική broadcast μετάδοση. Όλες οι άλλες συσκευές που λαμβάνουν αυτή την broadcast μετάδοση δημιουργούν μια αντίστροφη δρομολόγηση πίσω στο συλλέκτη. Όταν οι απομακρυσμένες συσκευές μεταδίδουν δεδομένα στο συλλέκτη, πρώτα μεταδίδουν ένα καταγεγραμμένο πλαίσιο δρομολόγησης, πριν από τη μετάδοση των δεδομένων. Το καταγεγραμμένο πλαίσιο δρομολόγησης παρέχει στο συλλέκτη ολόκληρη τη διαδρομή για κάθε απομακρυσμένο κόμβο που λαμβάνει δεδομένα από αυτόν.

Ο συλλέκτης μπορεί να χρησιμοποιήσει τις πληροφορίες στα καταγεγραμμένα πλαίσια δρομολόγησης για να αποθηκεύσει τις διαδρομές επιστροφής. Αυτή η διαδικασία δημιουργεί αξιόπιστες διαδρομές μεταξύ του συλλέκτη και άλλων συσκευών στο δίκτυο χρησιμοποιώντας μια μόνο broadcast μετάδοση αντί για πολλές άλλες.

3.8 Συγκριτικός πίνακας

	ZigBee and 802.15.4	GSM/GPRS CDMA	802.11	Bluetooth
Στόχος εφαρμογών	Παρακολούθηση και έλεγχος	Wide Area Voice and Data	Internet Υψηλών ταχυτήτων	Συνδεσιμότητα συσκευών
Διάρκεια μπαταρίας	Χρόνια	1 εβδομάδα	1 εβδομάδα	1 εβδομάδα
Ρυθμός μετάδοσης	250 Kbps	Up to 2 Mbps	Up to 54 Mbps	720 Kbps
Εμβέλεια	100+ Meters	Several Kilometers	50-100 Meters	10-100 Meters
Πλεονεκτήματα	Χαμηλή κατανάλωση και κόστος	Υπάρχουσες υποδομές	Υψηλός ρυθμός μετάδοσης	Διαλειτουργικότητα

Πίνακας 2

Το χαμηλότερο ποσοστό δεδομένων των συσκευών ZigBee παρέχει μεγαλύτερη ευαισθησία και εύρος, αλλά φυσικά προσφέρει μικρότερη απόδοση. Το κύριο πλεονέκτημα του ZigBee έγκειται στην ικανότητά του να προσφέρει χαμηλής ισχύος και εκτεταμένη διάρκεια ζωής της μπαταρίας.

Συμπέρασμα

Εάν η εφαρμογή θα πρέπει υποχρεωτικά να επικοινωνεί σε μια κατάσταση point-to-point ή point-to-multipoint, το 802.15.4 θα πρέπει είναι σε θέση να χειριστεί όλες τις συνδέσεις μεταξύ των συσκευών και θα είναι απλούστερο να εφαρμόσει αυτή η προσπάθεια χρησιμοποιώντας μια μονάδα με ZigBee firmware έτσι ώστε να επιτευχθεί ο ίδιος στόχος. Το ZigBee είναι απαραίτητο, αν απαιτούνται οι συνεχείς επαναλήψεις ή η λειτουργικότητα των κόμβων δικτύωσης στο σύστημά μας.

3.9 Ασφάλεια Zigbee

Η ασφάλειας ZigBee, η οποία βασίζεται σε ένα 128-bit AES (*Advanced Encryption Standard*) αλγόριθμο, προστίθεται στο μοντέλο ασφαλείας που παρέχεται από το IEEE 802.15.4. Οι υπηρεσίες ασφαλείας ZigBee περιλαμβάνουν μεθόδους για την εγκατάσταση και διαβίβαση κλειδιών, διαχείριση συσκευών, καθώς και την προστασία του πλαισίου. Η προδιαγραφή ZigBee ορίζει την ασφάλεια για τα στρώματα MAC, NWK και APS. Η ασφάλεια για τις εφαρμογές συνήθως παρέχεται μέσω των προφίλ των εφαρμογών.

3.9.1 Κέντρο αξιοπιστίας

Το Κέντρο αξιοπιστίας αποφασίζει εάν θα επιτρέψει ή όχι στις νέες συσκευές να ενταχθούν στο δίκτυο.

Το Κέντρο αξιοπιστίας μπορεί να αναπροσαρμόζεται περιοδικά και να στρέφεται σε ένα νέο κλειδί δικτύου. Εκπέμπει πρώτο το νέο κλειδί το οποίο κρυπτογραφείται με το παλιό κλειδί δικτύου. Αργότερα, λέει σε όλες τις συσκευές να γυρίσουν στο νέο κλειδί.

Το Κέντρο αξιοπιστίας είναι συνήθως ο συντονιστής του δικτύου, αλλά μπορεί επίσης να είναι μια ειδική συσκευή. Είναι υπεύθυνο για τους ακόλουθους ρόλους ασφαλείας:

- Διευθυντής Εμπιστοσύνης, για τον έλεγχο ταυτότητας των συσκευών που ζητούν να ενταχθούν στο δίκτυο.
- Διευθυντής Δικτύου, για τη διατήρηση και τη διανομή των κλειδιών του δικτύου.
- Configuration Manager, για να μπορέσει να διασφαλίσει μέχρι τέλους την ασφάλεια μεταξύ των συσκευών.

3.9.2 Κλειδιά ασφαλείας

Το ZigBee χρησιμοποιεί τρεις τύπους κλειδιών για τη διαχείριση της ασφαλείας:

- Master Keys
- Network Keys
- Link Keys

3.9.2.1 Master Keys

Αυτά τα προαιρετικά κλειδιά δεν χρησιμοποιούνται για την κρυπτογράφηση των πλαισίων. Χρησιμοποιούνται ως ένας κοινός κωδικός μεταξύ δύο συσκευών για την παραγωγή των κλειδιών σύνδεσης. Τα κλειδιά που προέρχονται από το Κέντρο αξιοπιστίας ονομάζονται Trust Center Master Keys, ενώ όλα τα άλλα κλειδιά ονομάζονται Application Layer Master Keys.

3.9.2.2 Network Keys

Αυτά τα κλειδιά παρέχουν την ασφάλεια σε ένα δίκτυο ZigBee. Όλες οι συσκευές του δικτύου μοιράζονται το ίδιο κλειδί. Τα κλειδιά σε ένα High Security Network πρέπει πάντα να αποστέλλονται κρυπτογραφημένα μέσω του αέρα, ενώ τα κλειδιά σε ένα Standard Security Network μπορούν να σταλούν είτε κρυπτογραφημένα ή χωρίς κρυπτογράφηση. Σημειώνεται ότι η High Security υποστηρίζεται μόνο για ZigBee PRO.

3.9.2.3 Link Keys

Αυτά τα προαιρετικά κλειδιά εξασφαλίζουν unicast μηνύματα μεταξύ δύο συσκευών σε επίπεδο εφαρμογών. Τα κλειδιά που προέρχονται από το Κέντρο αξιοπιστίας ονομάζονται Trust Center Link Keys, ενώ όλα τα άλλα κλειδιά ονομάζονται Application Layer Link Keys.

3.9.3 Security Modes

3.9.3.1 Standard Security Mode

Στην κανονική λειτουργία ασφαλείας, η λίστα των συσκευών, και τα Master, Network και Link Keys μπορούν να υποστηριχτούν είτε από το Κέντρο αξιοπιστίας ή από τις ίδιες τις συσκευές τους. Το Κέντρο αξιοπιστίας εξακολουθεί να είναι υπεύθυνο για τη διατήρηση ενός προτύπου κλειδιού δικτύου και ελέγχει τις προϋποθέσεις για την είσοδο στο δίκτυο. Σε αυτή τη λειτουργία, οι απαιτήσεις μνήμης για το Κέντρο αξιοπιστίας είναι πολύ λιγότερες από ό, τι είναι για την High Security mode.

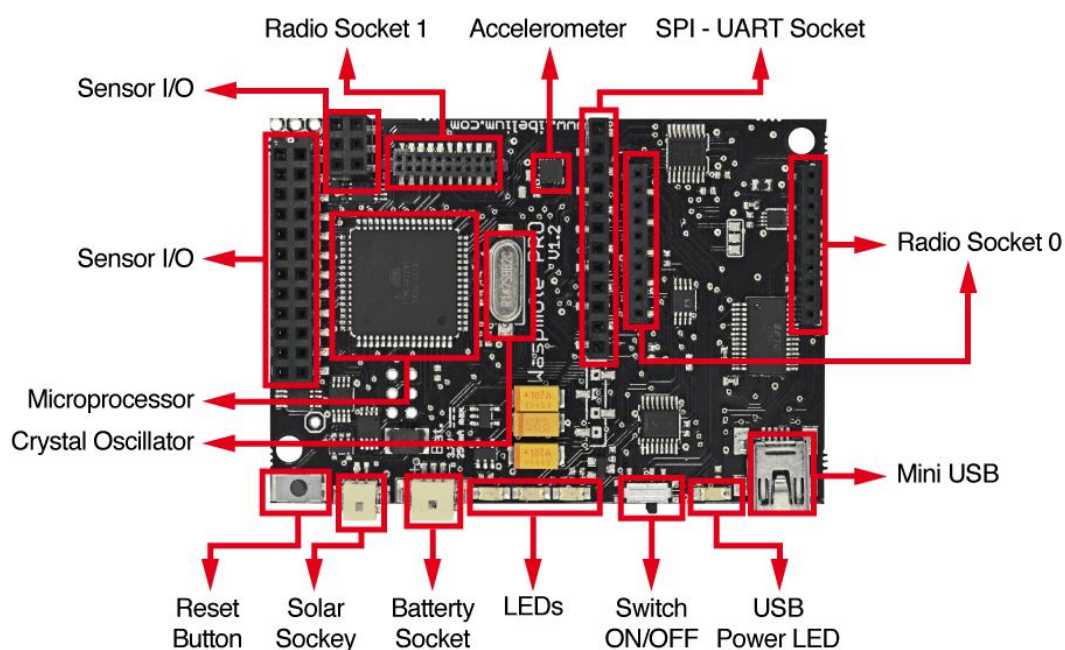
3.9.3.2 High Security Mode

Στη High Security Mode, το Κέντρο αξιοπιστίας διατηρεί μια λίστα των συσκευών, και των Master, Network και Link Keys που χρειάζεται για τον έλεγχο και την επιβολή των προϋποθέσεων της αναβάθμισης του κλειδιού δικτύου και της εισόδου στο δίκτυο. Δεδομένου ότι ο αριθμός των συσκευών στο δίκτυο μεγαλώνει, το ίδιο κάνει η μνήμη που απαιτείται για το Κέντρο αξιοπιστίας. Οι πρόσθετες δυνατότητες ασφάλειας που συνδέονται με το ZigBee PRO είναι κρίσιμες, αφού το ZigBee χρησιμοποιείται σε ολοένα και πιο σημαντικές εφαρμογές. Δεν πρέπει να υπάρχει συμβιβασμός όσον αφορά τον έλεγχο των κρίσιμων συστημάτων των υποδομών, είτε πρόκειται για ένα εμπορικό κτίριο, είτε για ένα ηλεκτρικό δίκτυο, είτε για μια βιομηχανική εγκατάσταση, είτε ακόμα για ένα σύστημα ασφαλείας ενός σπιτιού.

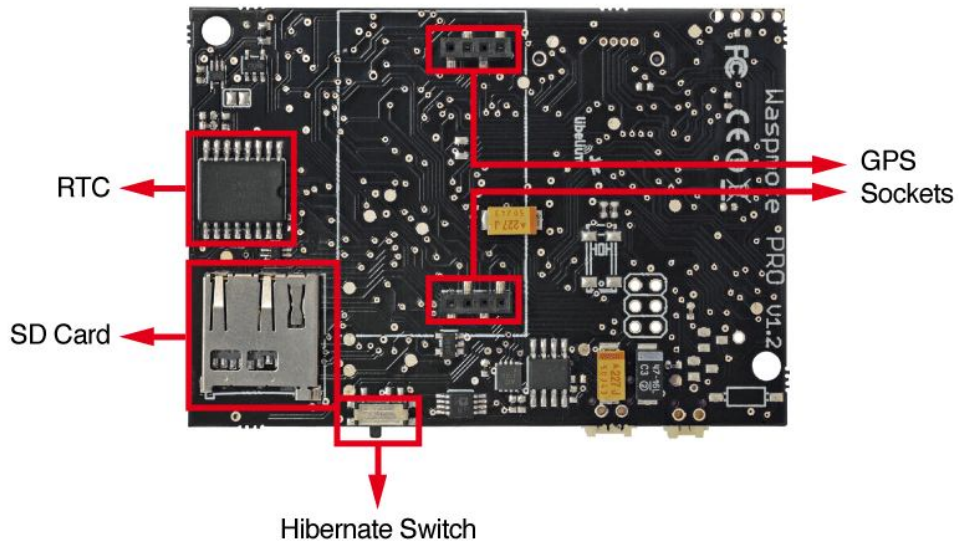
ΚΕΦΑΛΑΙΟ 4 : Γενικά Χαρακτηριστικά- Hardware

4.1 Προδιαγραφές Wasp mote

- Microcontroller: ATmega1281
- Frequency: 14.7456 MHz
- SRAM: 8KB
- EEPROM: 4KB
- FLASH: 128KB
- SD Card: 2GB
- Weight: 20gr
- Dimensions: 73.5 x 51 x 13 mm
- Temperature Range: [-10°C, +65°C]



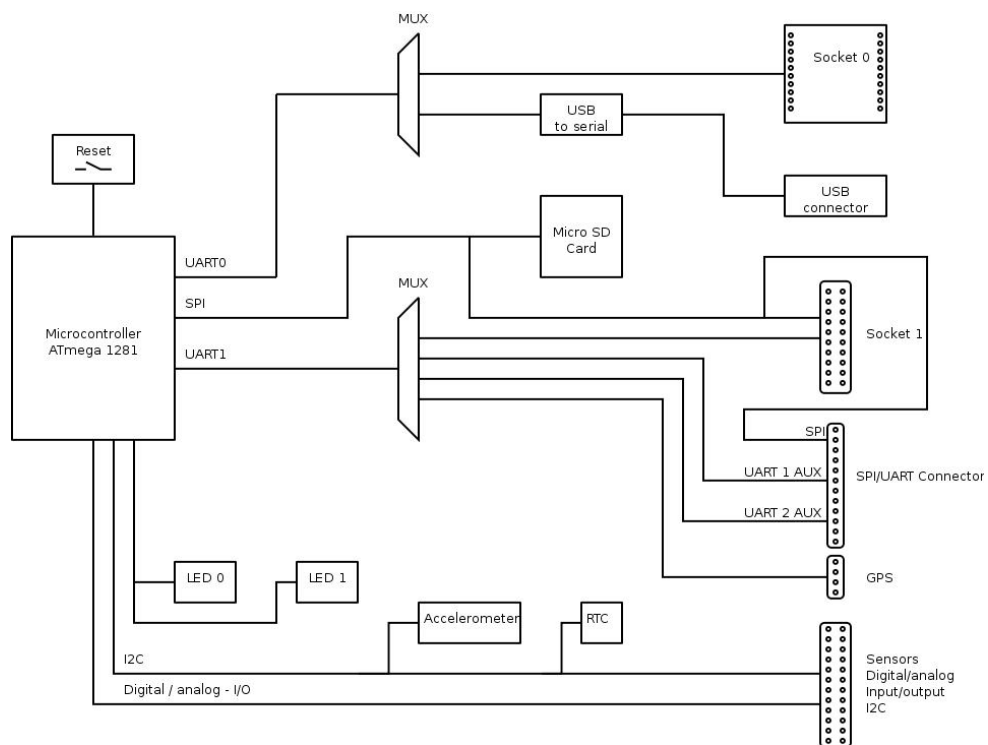
Εικόνα 16: Main Wasp mote components – Top side



Εικόνα 17: Main Wasp mote components – Bottom side

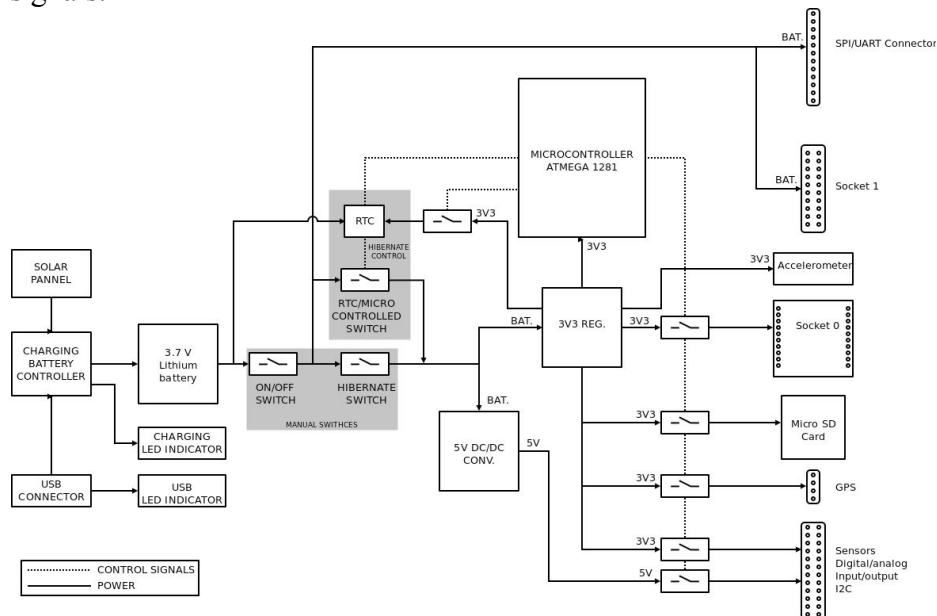
4.2 Block Diagram

Data signals:



Εικόνα 18: Wasp mote block diagrams – Data signals

Power signals:



Εικόνα 19: Wasp mote block diagrams – Power signals

4.3 Ηλεκτρικά δεδομένα

4.3.1 Πειραματικές τιμές

- Minimum operational battery voltage 3.3 V
- Maximum operational battery voltage 4.2V
- USB charging voltage 5 V
- Solar panel charging voltage 6 - 12 V
- Battery charging current from USB 100 mA (max)
- Battery charging current from solar panel 280 mA (max)

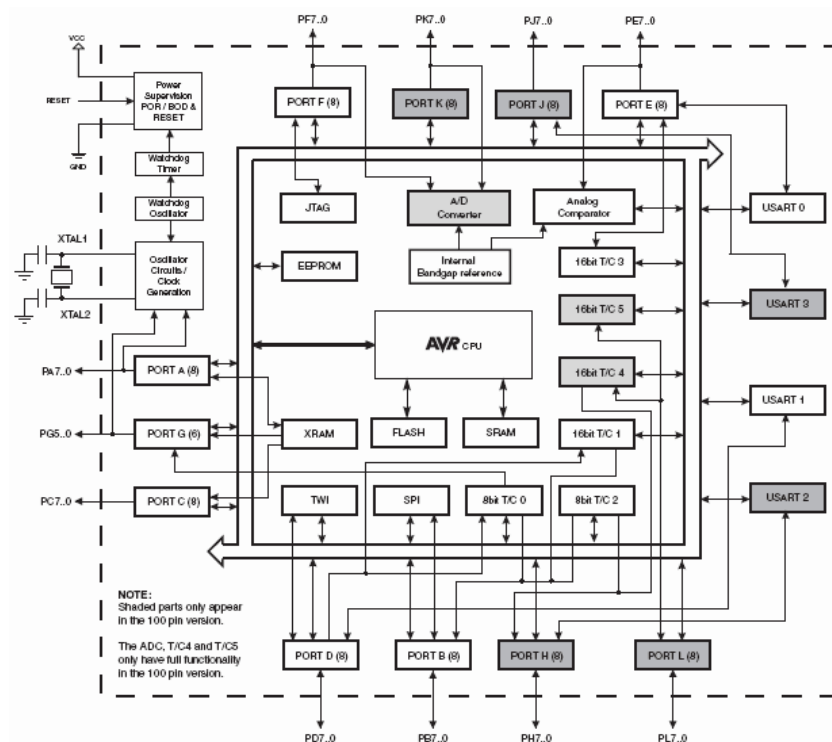
4.3.2 Απόλυτες μέγιστες τιμές

- Voltage in any pin [-0.5 V, +3.8 V]
- Maximum current from any digital I/O pin 40 mA
- USB power voltage 7V
- Solar panel power voltage 18V
- Charged battery voltage 4.2 V

4.4 ATmega1281

4.4.1 Γενικά χαρακτηριστικά

Ο μικροϋπολογιστής AVR ATmega 1281, αποτελεί την καρδιά του αναπτυξιακού συστήματος που υλοποιήθηκε.



Εικόνα 20: Διάγραμμα της αρχιτεκτονικής του AVR

Ο ATmega 1281 είναι ένας μικροελεγκτής των 8 bits, τεχνολογίας CMOS χαμηλής ισχύος, που περιλαμβάνει έναν επεξεργαστή RISC. Επιτρέπει την εκτέλεση πολύπλοκων εντολών σε ένα κύκλο ρολογιού. Με τον τρόπο αυτό καταφέρνει να έχει αποδόσεις που αγγίζουν το 1MIPS ανά MHz, επιτρέποντας βελτιστοποίηση της κατανάλωσης τάσης σε σχέση με την υπολογιστική ισχύ.

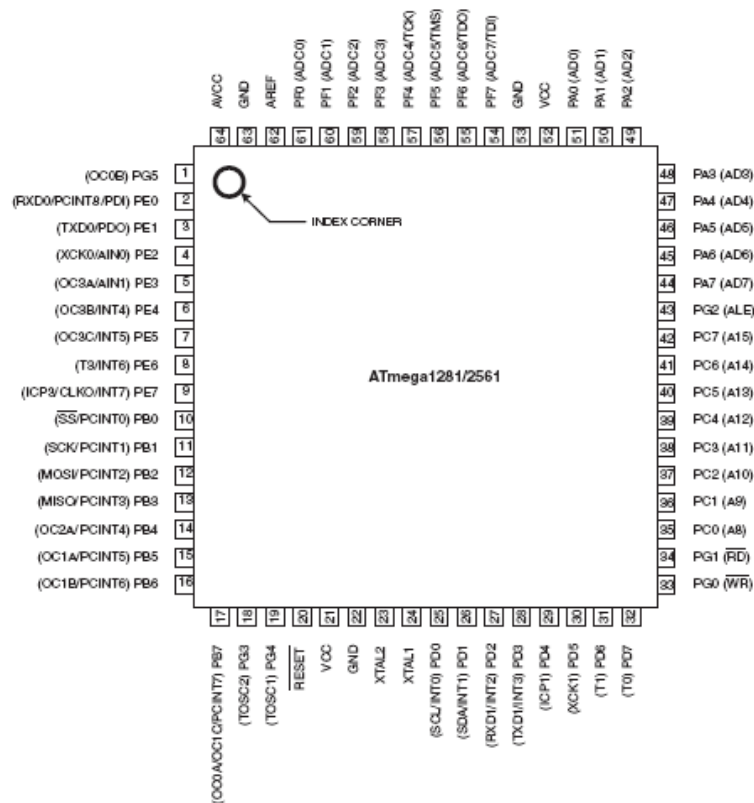
Ο πυρήνας του AVR συνδυάζει πλούσιο ρεπερτόριο εντολών με 32 καταχωρητές εργασίας γενικής χρήσης. Οι 32 αυτοί καταχωρητές συνδέονται άμεσα στην Αριθμητική Λογική Μονάδα (ALU - Arithmetic Logic Unit) με τρόπο που επιτρέπει την πρόσβαση σε δύο ανεξάρτητους καταχωρητές με μία μόνο εντολή που εκτελείται σε ένα κύκλο ρολογιού. Η αρχιτεκτονική που προκύπτει λοιπόν είναι περισσότερο αποδοτική ως προς τον κώδικα σε σχέση με συμβατικούς μικροελεγκτές CISC.

Ο ATmega 1281 παρουσιάζει τα ακόλουθα χαρακτηριστικά:

- Μνήμη προγράμματος 128K bytes ταχείας αποθήκευσης (flash memory) με δυνατότητα προγραμματισμού εντός του συστήματος (ISP - In System Programmable) και δυνατότητα ανάγνωσης κατά τη διάρκεια της εγγραφής,
- Μνήμη δεδομένων που αποτελείται από 8K byte στατικής μνήμης (SRAM - Static Random Access Memory) και 4K bytes ηλεκτρικά επαναπρογραμματιζόμενης μνήμης μόνο για ανάγνωση (EEPROM - Electrically Erasable Programmable Read Only Memory),
- 54 γραμμές εισόδου - εξόδου γενικής χρήσης,
- 32 καταχωρητές εργασίας γενικού σκοπού,
- Real Time Counter (RTC),
- Διεπαφή JTAG,
- Ενσωματωμένη υποστήριξη αποσφαλμάτωσης (debugging) και προγραμματισμού,
- 6 ευέλικτα χρονόμετρα / απαριθμητές (Timer / Counters),
- Εσωτερικές και εξωτερικές διακοπές,
- Προγραμματιζόμενες μονάδα σύγχρονης - ασύγχρονης σειριακής επικοινωνίας (USART - Universal Synchronous - Asynchronous Receiver Transmitter),
- Διεπαφή I²C,
- Μετατροπέα αναλογικού σήματος σε ψηφιακό (ADC - Analog to Digital Converter) με 16 κανάλια των 10 bits,
- Προγραμματιζόμενο χρονόμετρο - φύλακα (Watchdog Timer) με εσωτερικό ταλαντωτή,
- Σειριακή θύρα διασύνδεσης περιφερειακών (SPI - Serial Peripheral Interconnect),
- 6 καταστάσεις εξοικονόμησης ενέργειας (power save modes).

Η συσκευή κατασκευάζεται με την τεχνολογία μη πτητικής μνήμης υψηλής πυκνότητας της Atmel. Η ενσωματωμένη ISP Flash δίνει τη δυνατότητα στη μνήμη προγράμματος να επαναπρογραμματίζεται εντός του συστήματος μέσω μιας σειριακής διεπαφής SPI, είτε μέσω ενός συμβατικού προγραμματιστή μη πτητικής μνήμης, είτε μέσω ενός ενσωματωμένου προγράμματος εκκίνησης (Boot program) τοποθετημένου στον πυρήνα του AVR. Το πρόγραμμα εκκίνησης μπορεί να χρησιμοποιήσει οποιαδήποτε διεπαφή (RS232, I²C ή I/O ports) για να κατεβάσει την εφαρμογή στο τμήμα εφαρμογών της μνήμης. Το λογισμικό στο τμήμα εκκίνησης της μνήμης θα συνεχίσει να εκτελείται καθώς το τμήμα εφαρμογών θα αναβαθμίζεται. Συνδυάζοντας κεντρική μονάδα επεξεργασίας (CPU - Central Processing Unit) των 8 bits με αρχιτεκτονική RISC με ενσωματωμένη αυτοπρογραμματιζόμενη μνήμη ταχείας πρόσβασης (In-System Self-Programmable Flash) πάνω σε ένα μονολιθικό ολοκληρωμένο κύκλωμα, ο ATmega 1281 είναι ένας ισχυρός μικροελεγκτής και αποτελεί μια ευέλικτη και οικονομική επιλογή για πολλές εφαρμογές.

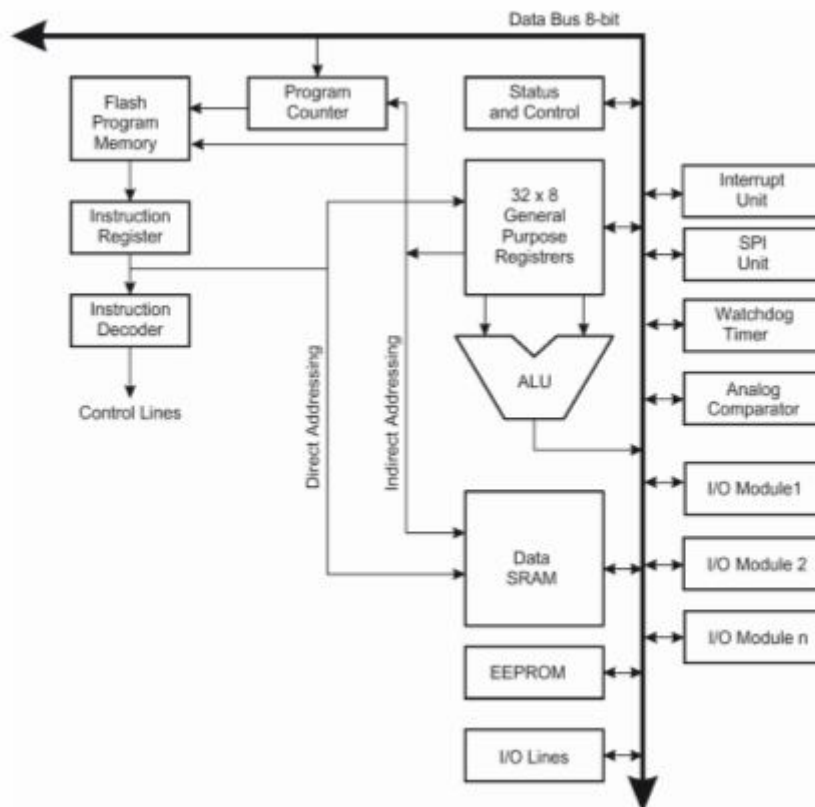
Ο ATmega 1281 υποστηρίζεται από πολλά εργαλεία ανάπτυξης λογισμικού.



Εικόνα 21: Οι ακροδέκτες του Atmega1281

4.4.2 Κεντρική Μονάδα Επεξεργασίας (CPU - Central Processing Unit)

Η CPU του ATmega 1281 οφείλει να εξασφαλίζει τη σωστή εκτέλεση του προγράμματος, πρέπει λοιπόν να έχει πρόσβαση στις μνήμες, να εκτελεί υπολογισμούς, να ελέγχει περιφερειακά και να διαχειρίζεται διακοπές. Ο μικροελεγκτής έχει σχεδιαστεί σύμφωνα με την αρχιτεκτονική Harvard, έχει δηλαδή ξεχωριστές μνήμες και ξεχωριστούς διαύλους για το πρόγραμμα και για τα δεδομένα. Οι εντολές στη μνήμη προγράμματος εκτελούνται με διοχέτευση ενός επιπέδου (single level pipeline), δηλαδή ενώ εκτελείται μία εντολή, η αμέσως επόμενη καλείται από τη μνήμη προγράμματος. Με τον τρόπο αυτό εντολές εκτελούνται σε κάθε κύκλο ρολογιού.



Εικόνα 22: Διάγραμμα της αρχιτεκτονικής της κεντρικής μονάδας ελέγχου (MCU) του AVR

Το αρχείο καταχωρητών γρήγορης πρόσβασης περιλαμβάνει τους 32 καταχωρητές εργασίας και έχει χρόνο πρόσβασης ένα μόνο κύκλο ρολογιού. Έτσι η λειτουργία της ALU γίνεται σε ένα κύκλο μηχανής. Σε μια τυπική πράξη της ALU, δύο τελεστές καλούνται από το αρχείο καταχωρητών, η εντολή εκτελείται και το αποτέλεσμα αποθηκεύεται πίσω στο αρχείο καταχωρητών, και όλα αυτά συμβαίνουν σε ένα κύκλο μηχανής. Πέρα από εντολές μεταξύ καταχωρητών, εκτελούνται και εντολές μεταξύ ενός καταχωρητή και μιας σταθεράς ή και εντολές μονού καταχωρητή. Οι λειτουργίες της ALU χωρίζονται σε τρεις βασικές κατηγορίες : αριθμητικές, λογικές και εντολές σε επίπεδο ενός bit.

Έξι από τους καταχωρητές (οι R26 ως και R31) μπορούν να χρησιμοποιηθούν σε ζεύγη ως καταχωρητές δεικτών έμμεσης διευθυνσιοδότησης των 16 bits, διευκολύνοντας έτσι τους υπολογισμούς διευθύνσεων. Ένας από τους καταχωρητές αυτούς μπορεί να χρησιμοποιηθεί επιπλέον και ως δείκτης διεύθυνσης για πρόσβαση σε πίνακες δεδομένων αποθηκευμένων στην Flash μνήμη προγράμματος (παραβιάζοντας χάριν αποτελεσματικότητας την αρχιτεκτονική Harvard). Οι τρεις αυτοί καταχωρητές καλούνται X, Y και Z.

Η ροή του προγράμματος ελέγχεται με εντολές άλματος (είτε υπό συνθήκη είτε χωρίς) και με εντολές κλήσης (jump και call), ικανές να αναφερθούν άμεσα σε όλο το εύρος διευθύνσεων. Οι περισσότερες εντολές έχουν απλή μορφοποίηση λέξης των 16

bits. Κάθε διεύθυνση της μνήμης προγράμματος περιλαμβάνει μια εντολή των 16 ή 32 bits.

Η CPU περιλαμβάνει επιπλέον τον καταχωρητή κατάστασης (status register) ο οποίος περιέχει πληροφορίες για το αποτέλεσμα της πιο πρόσφατης αριθμητικής εντολής. Στις πληροφορίες αυτές βασίζεται η εκτέλεση των εντολών άλματος υπό συνθήκη.

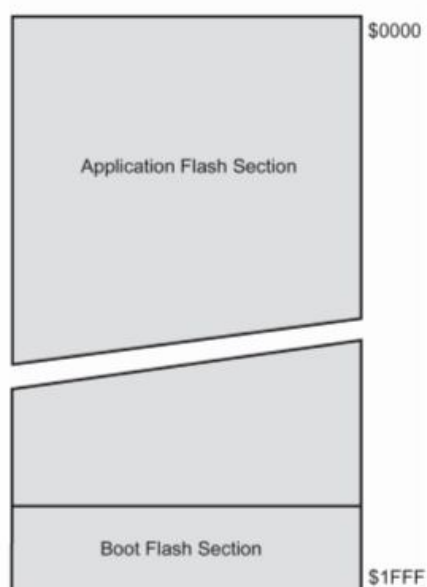
Ένας άλλος καταχωρητής της CPU είναι ο δείκτης στοίβας (stack pointer) ο οποίος χρησιμεύει στην αποθήκευση προσωρινών δεδομένων, στην αποθήκευση τοπικών μεταβλητών και στην αποθήκευση διευθύνσεων επιστροφής μετά από διακοπές και υπορουτίνες.

4.4.3 Μνήμες

Η αρχιτεκτονική των μικροεπεξεργαστών AVR προβλέπει δύο βασικούς αποθηκευτικούς χώρους, τη μνήμη δεδομένων και τη μνήμη προγράμματος. Επιπλέον, ο ATmega 1281 έχει και συμπληρωματική μνήμη EEPROM για αποθήκευση δεδομένων. Και οι τρεις αυτοί χώροι μνήμης είναι γραμμικοί.

Ο ATmega1281 περιλαμβάνει 128K bytes ενσωματωμένης μνήμης Flash επαναπρογραμματιζόμενης στο τελικό σύστημα για την αποθήκευση προγραμμάτων. Η μνήμη αυτή είναι οργανωμένη ως 8K x 16bits καθώς όλες οι εντολές του AVR έχουν μήκος 16 ή 32 bits και έχει αντοχή τουλάχιστον 10.000 κύκλους εγγραφής/διαγραφής. Για την προστασία του λογισμικού, η μνήμη προγράμματος Flash είναι χωρισμένη σε δύο περιοχές, την περιοχή του προγράμματος εκκίνησης (Boot Program) και την περιοχή του προγράμματος εφαρμογών (Application Program).

Η αρχιτεκτονική του ATmega1281 περιλαμβάνει και μερικές δεκάδες καταχωρητές οι οποίοι προγραμματίζονται τη λειτουργία των περιφερειακών και αποτελούν τις διεπαφές με αυτά. Συλλογικά οι καταχωρητές αυτοί ονομάζονται μνήμη εισόδου – εξόδου.



Εικόνα 23: Χάρτης της μνήμης προγράμματος

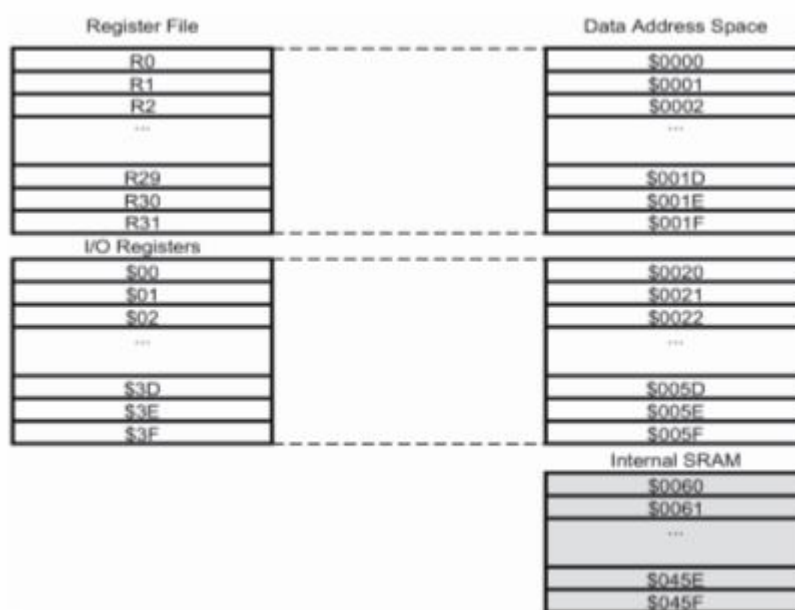
Όσον αφορά τώρα στη μνήμη δεδομένων, στις κατώτερες 1120 θέσεις της βρίσκονται το αρχείο καταχωρητών, η μνήμη εισόδου - εξόδου και η εσωτερική μνήμη SRAM που έχει μέγεθος 8K byte. Υπάρχουν τέσσερις τρόποι προσπέλασης της μνήμης δεδομένων : Άμεσα, Έμμεσα με βάση και μετατόπιση, Έμμεσα με μείωση εκ των προτέρων, Έμμεσα με αύξηση εκ των υστέρων. Για έμμεση πρόσβαση χρησιμοποιούνται οι καταχωρητές X, Y ή Z (R26 έως R31 σε ζεύγη) ως δείκτες διεύθυνσης.

Με τον άμεσο τρόπο προσπέλασης έχουμε πρόσβαση σε ολόκληρο το χώρο δεδομένων.

Στην έμμεση προσπέλαση με μετατόπιση, είναι δυνατή η πρόσβαση σε 63 θέσεις διευθύνσεων με αρχή τη βάση που βρίσκεται στον καταχωρητή Y ή στον καταχωρητή Z.

Στην έμμεση προσπέλαση με μείωση εκ των υστέρων ή αύξηση εκ των προτέρων, οι καταχωρητές διευθύνσεων X, Y και Z μειώνονται ή αυξάνονται αντίστοιχα.

Η διευθυνσιοδότηση αυτών των τριών περιοχών (αρχείο καταχωρητών, μνήμη εισόδου – εξόδου και SRAM) είναι συνεχόμενη όπως φαίνεται στην (Εικόνα 24).



Εικόνα 24: Χάρτης της μνήμης δεδομένων

Ο ATmega1281 περιλαμβάνει επιπλέον μνήμη δεδομένων EEPROM των 4K bytes που είναι οργανωμένη χωριστά και από την οποία μπορούν να διαβαστούν και να γραφούν μονά bytes. Έχει διάρκεια ζωής τουλάχιστον 100.000 κύκλους εγγραφής / διαγραφής και η επικοινωνία της με την CPU καθορίζεται μέσω ειδικών καταχωρητών διεύθυνσης, δεδομένων και ελέγχου.

4.4.4 Σύστημα χρονισμού

Στην (Εικόνα 25) φαίνεται το βασικό σύστημα χρονισμού του AVR καθώς και η διανομή των ρολογιών. Δεν είναι αναγκαίο να είναι όλα τα ρολόγια ενεργά κάθε χρονική στιγμή. Για λόγους οικονομίας της ενέργειας που καταναλώνεται, τα ρολόγια που δεν χρησιμοποιούνται μπαίνουν σε κατάσταση ύπνου (sleep mode).

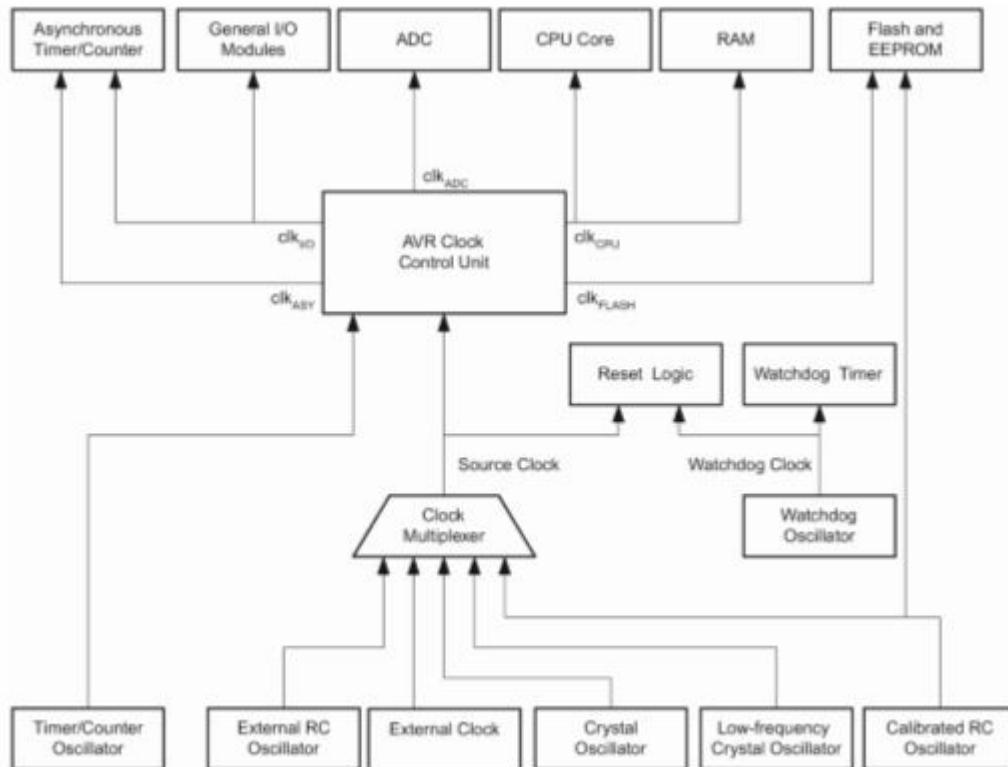
Το ρολόι της CPU (clk_{CPU}) οδηγείται στα τμήματα του συστήματος τα σχετικά με τη λειτουργία του πυρήνα του AVR, όπως για παράδειγμα το αρχείο καταχωρητών γενικής χρήσης, ο καταχωρητής κατάστασης και ο δείκτης στοίβας. Παύση της λειτουργίας του ρολογιού της CPU οδηγεί τον πυρήνα σε αδυναμία εκτέλεσης γενικών λειτουργιών και υπολογισμών.

Το ρολόι εισόδου-εξόδου ($clk_{I/O}$) χρησιμοποιείται από την πλειοψηφία των μονάδων εισόδου - εξόδου όπως για παράδειγμα οι χρονιστές / μετρητές και η USART καθώς επίσης και από τη μονάδα εξωτερικών διακοπών, αν και όχι σε όλες τις περιπτώσεις έτσι ώστε κάποιες διακοπές να είναι ενεργές ακόμη και όταν το $clk_{I/O}$ είναι σταματημένο.

Το ρολόι Flash (clk_{FLASH}) χρησιμοποιείται στην διεπαφή Flash και είναι συνήθως ενεργό ταυτόχρονα με το ρολόι της CPU.

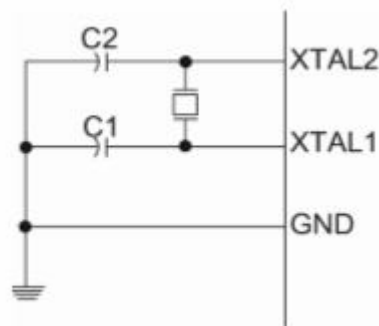
Το ρολόι του ασύγχρονου χρονιστή (clk_{ASY}) επιτρέπει στον ασύγχρονο χρονιστή / μετρητή να δέχεται κατευθείαν σήμα χρονισμού από εξωτερικό κρύσταλλο των 32KHz. Έτσι ο χρονιστής / μετρητής αυτός μπορεί να χρησιμοποιηθεί σαν μετρητής πραγματικού χρόνου ακόμα και όταν η συσκευή βρίσκεται σε sleep mode.

Τέλος, ο ADC έχει ξεχωριστό ρολόι (clk_{ADC}) ώστε να είναι δυνατή η παύση των clk_{CPU} και $clk_{I/O}$ κατά τη λειτουργία του ADC με στόχο τη μείωση του θορύβου και, κατά συνέπεια, τη μεγαλύτερη ακρίβεια στα αποτελέσματα της μετατροπής A/D.



Εικόνα 25 : Δημιουργία και κατανομή ρολογιού

Ο AVR διαθέτει πολλές πηγές ρολογιού: εξωτερικό ή εσωτερικό ταλαντωτή RC, τελείως ανεξάρτητη εξωτερική πηγή ή κρυσταλλικό ταλαντωτή (χαμηλής ή υψηλής συχνότητας). Σε εφαρμογές που είναι κρίσιμη η ακρίβεια της συχνότητας του ρολογιού (π.χ. χρήση της USART για τηλεπικοινωνίες) συνήθως χρησιμοποιείται ένας κρυσταλλικός ταλαντωτής. Για το σκοπό αυτό υπάρχουν οι ακροδέκτες XTAL1 και XTAL2 οι οποίοι είναι είσοδος και έξοδος αντίστοιχα ενός ενισχυτή που αντιστρέφει. Μεταξύ των ακροδεκτών αυτών μπορεί να συνδεθεί είτε κρύσταλλος χαλαζία (quartz) είτε κεραμικός συντονιστής (resonator).



Εικόνα 26 : Οι συνδέσεις του κρυσταλλικού ταλαντωτή

4.4.5 Διακοπές και Επανατοποθέτηση

Ο AVR υποστηρίζει αρκετές διαφορετικές πηγές διακοπών σε κάθε μία από τις οποίες αντιστοιχεί ένας διαφορετικός δείκτης προγράμματος στο χώρο της μνήμης προγράμματος. Κάθε διακοπή έχει ένα bit επίτρεψης (enable bit) σε κατάλληλο καταχωρητή ελέγχου της πηγής της διακοπής, ανεξάρτητο από αυτό των άλλων διακοπών, στο οποίο θα πρέπει να δοθεί η τιμή 1 ώστε να ενεργοποιηθεί η συγκεκριμένη διακοπή. Επίσης υπάρχει ένα γενικό bit επίτρεψης διακοπών (Global Interrupt Enable bit) που βρίσκεται στον καταχωρητή κατάστασης το οποίο πρέπει να έχει την τιμή 1 προκειμένου να ενεργοποιηθεί ολόκληρος ο μηχανισμός διακοπών.

Στις χαμηλότερες διευθύνσεις στο χώρο της μνήμης εφαρμογής βρίσκονται οι δείκτες προς τις διευθύνσεις των ρουτινών εξυπηρέτησης των διακοπών καθώς και της ρουτίνας επανατοποθέτησης (Reset). Η σειρά των δεικτών αυτών υποδεικνύει και την προτεραιότητα κάθε διακοπής: όσο πιο χαμηλά βρίσκεται τόσο μεγαλύτερη και η προτεραιότητά της. Τη μέγιστη προτεραιότητα έχει το Reset ενώ ακολουθεί η INT0, η εξωτερική διακοπή 0. Τόσο τα διανύσματα των διακοπών όσο και το διάνυσμα του Reset μπορούν να μετακινηθούν στην αρχή του τμήματος της μνήμης Flash όπου βρίσκεται ο Boot Loader.

Υπάρχουν δύο βασικοί τύποι διακοπών. Οι διακοπές που ανήκουν στον πρώτο τύπο είναι ακμοπυροδότητες, δηλαδή ενεργοποιούνται τη στιγμή που ένα γεγονός θέτει 1 στη αντίστοιχη σημαία διακοπών (Interrupt Flag), ενώ οι διακοπές του δεύτερου τύπου είναι διακοπές κατάστασης δηλαδή παραμένουν ενεργοποιημένες για όσο χρόνο ισχύει η συνθήκη διακοπής. Τα περισσότερα περιφερειακά υποστηρίζουν και τους δύο τύπους διακοπών και η επιλογή γίνεται κατά τον προγραμματισμό τους.

Όταν συμβαίνει μια διακοπή, το Global Interrupt Enable bit γίνεται 0 και όλες οι διακοπές αυτομάτως απενεργοποιούνται. Το πρόγραμμα εφαρμογής μπορεί, αν θέλει, να επιτρέψει την ενεργοποίηση διακοπών μέσα σε διακοπές θέτοντας 1 στο Global Interrupt Enable bit.

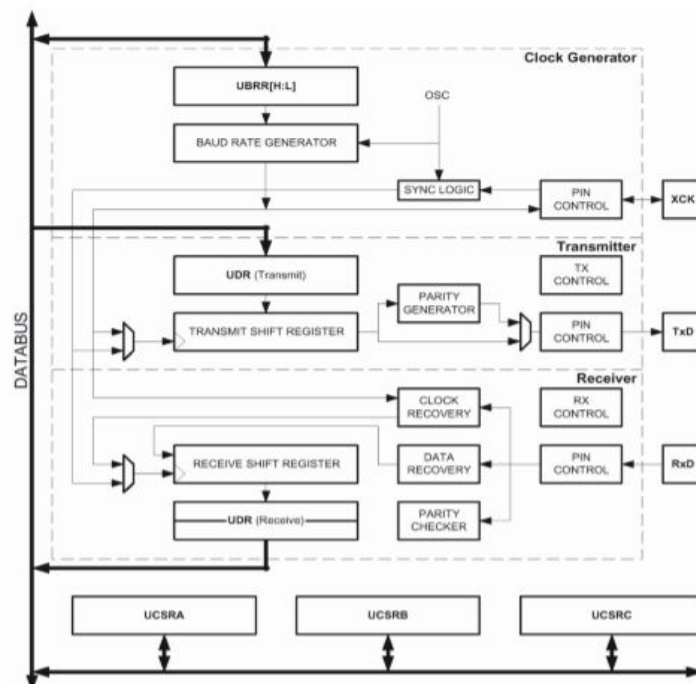
Ο καταχωρητής κατάστασης δεν αποθηκεύεται αυτόματα όταν ο AVR εισέρχεται σε μια ρουτίνα εξυπηρέτησης διακοπής. Το πρόγραμμα εφαρμογής οφείλει να τον αποθηκεύσει καθώς και να τον αποκαταστήσει κατά την επιστροφή στο κυρίως πρόγραμμα.

Ο ελάχιστος χρόνος απόκρισης εκτέλεσης της διακοπής είναι τέσσερις κύκλοι ρολογιού, κατά τη διάρκεια των οποίων ο μετρητής προγράμματος ωθείται στη στοίβα. Μετά από τέσσερις κύκλους ρολογιού εκτελείται η εντολή που βρίσκεται στο διάνυσμα που αντιστοιχεί στη διακοπή και που συνήθως είναι εντολή άλματος προς τη ρουτίνα εξυπηρέτησης της διακοπής. Η εντολή άλματος διαρκεί τρεις κύκλους ρολογιού. Η επιστροφή από τη ρουτίνα εξυπηρέτησης της διακοπής διαρκεί τέσσερις κύκλους ρολογιού κατά τη διάρκεια των οποίων ο μετρητής προγράμματος (δύο bytes) εξάγεται από τη στοίβα, ο δείκτης στοίβας μειώνεται κατά δύο και το I-bit (Interrupt enable bit) στον SREG γίνεται 1.

4.4.6 Μονάδα σύγχρονης και ασύγχρονης επικοινωνίας (Universal Synchronous & Asynchronous Receiver Transmitter - USART)

Η προγραμματιζόμενη μονάδα σύγχρονης - ασύγχρονης σειριακής επικοινωνίας (USART) είναι μια εξαιρετικά ευέλικτη συσκευή επικοινωνίας που διαθέτει τρία βασικά μέρη, (Εικόνα 27).

- Γεννήτρια Ρολογιού
- Πομπό
- Δέκτη



Εικόνα 27 : Διάγραμμα της USART

Η γεννήτρια ρολογιού παράγει το ρολόι βάσης για τον πομπό και τον δέκτη. Η USART υποστηρίζει τέσσερις καταστάσεις λειτουργίας του ρολογιού : Κανονική Ασύγχρονη, Ασύγχρονη Διπλής ταχύτητας, Master Σύγχρονη και Slave Σύγχρονη. Η USART πρέπει να αρχικοποιηθεί προτού αρχίσει κάθε επικοινωνία. Η διαδικασία ενεργοποίησης συνήθως περιλαμβάνει καθορισμό της ταχύτητας μετάδοσης, και της μορφής πλαισίου. Σχετικά με τη μορφή πλαισίου, η USART δέχεται ως έγκυρες μορφές τους 30 συνδυασμούς των παρακάτω περιπτώσεων :

- 1 bit αρχικοποίησης
- 5, 6, 7, 8 ή 9 bits δεδομένων
- μονό, ζυγό ή καθόλου bit ισοτιμίας (parity bit)
- 1 ή 2 bit τερματισμού

Ο πομπός της USART ενεργοποιείται δίνοντας την τιμή 1 στο bit ενεργοποίησης εκπομπής στον καταχωρητή UCSRB (B Καταχωρητής Ελέγχου και Κατάστασης της USART – USART Control and Status Register B). Όταν ο πομπός ενεργοποιηθεί, η κανονική λειτουργία του ακροδέκτη PD1 καταργείται και αυτός λειτουργεί ως έξοδος της USART (TxD). Στην περίπτωση σύγχρονης λειτουργίας το ρολόι στον ακροδέκτη XCK λειτουργεί ως ρολόι μετάδοσης ενώ η κανονική λειτουργία του ακροδέκτη PB0 καταργείται.

Ο δέκτης της USART ενεργοποιείται δίνοντας την τιμή 1 στο bit ενεργοποίησης λήψης στον καταχωρητή UCSRB. Όταν ο δέκτης ενεργοποιηθεί, η κανονική λειτουργία του ακροδέκτη PD0 καταργείται και αυτός λειτουργεί ως είσοδος της USART (RxD). Στην περίπτωση σύγχρονης λειτουργίας το ρολόι στον ακροδέκτη XCK λειτουργεί ως ρολόι μετάδοσης ομοίως με παραπάνω.

4.4.7 Διεπαφή I²C

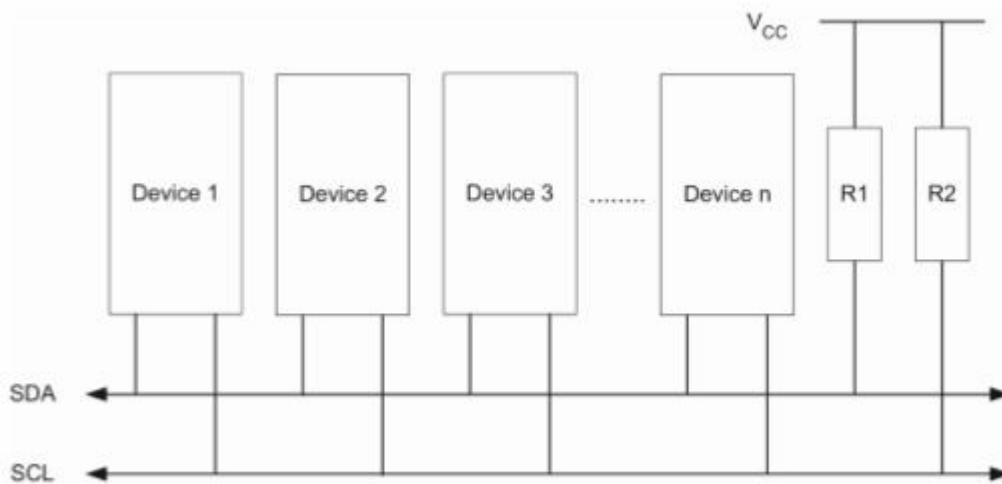
Ο Δίαυλος Διασύνδεσης Ολοκληρωμένων Κυκλωμάτων (I²C – Inter Integrated Circuit) είναι ένας δίαυλος επικοινωνίας που αναπτύχθηκε από την εταιρία Philips και, λόγω των πλεονεκτημάτων που προσφέρει, χρησιμοποιείται ευρύτατα από πολλές άλλες εταιρίες με ποικίλες ονομασίες. Σκοπός του είναι η εύκολη επικοινωνία μιας Κεντρικής Μονάδας Επεξεργασίας (Central Processor Unit – CPU) με περιφερειακές συσκευές. Ο ATmega16 υποστηρίζει τον δίαυλο αυτό με μόνη διαφορά την ονομασία που δίνει σε αυτόν η Atmel : Σειριακή Διεπαφή Δύο Καλωδίων (TWI – Two-wire Serial Interface). Ο διάδρομος αποτελείται από δύο ενεργές γραμμές και μια τρίτη γραμμή γείωσης. Οι δύο ενεργές γραμμές είναι διπλής κατεύθυνσης και ονομάζονται SDA και SCL από τις λέξεις Serial Data Line (Σειριακή Γραμμή Δεδομένων) και Serial Clock Line (Σειριακή Γραμμή Ρολογιού). Αυτό είναι και το βασικό του πλεονέκτημα.

Το I²C interface είναι τύπου αφέντη/σκλάβου. Σε κάθε συσκευή που συνδέεται στον δίαυλο αντιστοιχεί μια μοναδική διεύθυνση και λαμβάνουν χώρα απλές σχέσεις κύριας / εξαρτώμενης διάταξης (Master / Slave) με τον Master να μπορεί να λειτουργήσει είτε ως πομπός είτε ως δέκτης.

Είναι δυνατόν να υπάρχουν πάνω από ένας Master στον ίδιο δίαυλο χωρίς να χάνονται δεδομένα χάρη στην ανίχνευση και διαιτησία των συγκρούσεων. Ο χρονισμός του διαδρόμου δημιουργείται πάντα από τη συσκευή-αφέντη, όπως και τα σήματα για τη μεταφορά των δεδομένων. Μια συσκευή-σκλάβος δεν μπορεί να αρχίσει μια μεταφορά δεδομένων. Το I²C interface παρέχει τη δυνατότητα να συνδεθούν στο διάδρομο περισσότερες από μια συσκευές-αφέντες, των οποίων η προτεραιότητα ορίζεται με τυχαίο τρόπο. Ο ρυθμός μετάδοσης των δεδομένων ισούται με 100 Kbits/sec κατά την τυπική λειτουργία, 400 Kbits/sec στην γρήγορη λειτουργία και 3.4 Mbits/sec κατά τη λειτουργία υψηλής ταχύτητας. Ο ATmega1281 λειτουργεί μέχρι τα 400 Kbits/sec.

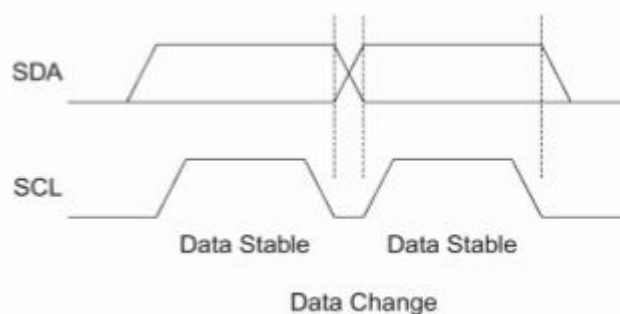
Κάθε byte που μεταδίδεται στον δίαυλο I²C συνοδεύεται από ένα bit επιβεβαίωσης (acknowledge bit) οπότε όλα τα πακέτα δεδομένων έχουν μήκος εννέα bits. Κατά τη διάρκεια μιας μετάδοσης δεδομένων, ο Master, δηλαδή στην πλακέτα που

υλοποιήθηκε ο Atmega1281 την επικοινωνία στέλνοντας στον διάδρομο το σήμα χρονισμού και ένα συγκεκριμένο σήμα αρχής (start condition). Το τέλος της μεταφοράς δεδομένων σηματοδοτείται αντίστοιχα από ένα συγκεκριμένο σήμα τέλους (stop condition). Ως σήμα αρχής θεωρείται η μετάβαση της γραμμής SDA από HIGH σε LOW, ενώ η γραμμή του ρολογιού SCL παραμένει HIGH. Ως σήμα τέλους θεωρείται η μετάβαση της γραμμής SDA από LOW σε HIGH, ενώ η γραμμή του ρολογιού SCL παραμένει HIGH. Τα δεδομένα μεταφέρονται σε επίπεδο byte (8-bit). Μετά την παραλαβή κάθε byte, η συσκευή-δέκτης παράγει ένα bit επιβεβαίωσης (acknowledge bit). Τα bits τοποθετούνται διαδοχικά στη γραμμή SDA αρχίζοντας από το MSB. Για να είναι έγκυρα τα δεδομένα η γραμμή SDA πρέπει να παραμένει σε σταθερή κατάσταση κατά τη διάρκεια της μεταφοράς.



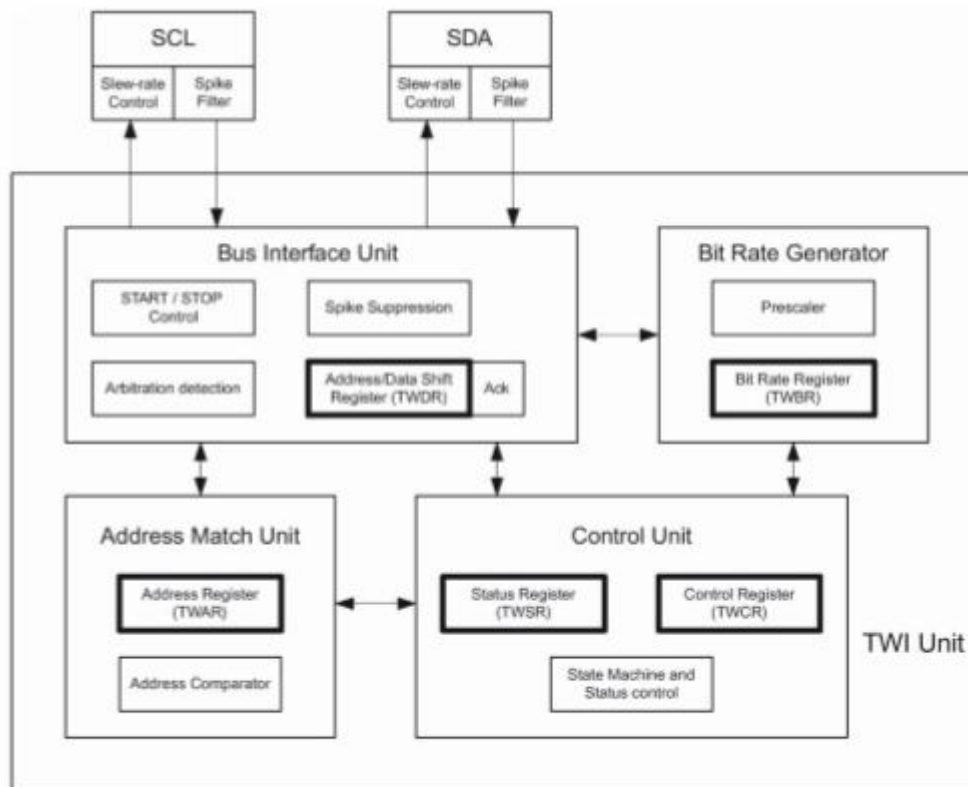
Εικόνα 28 : Διασύνδεση του διαύλου I²C

Ο αριθμός των συσκευών που μπορούν να συνδεθούν στο δίαυλο περιορίζεται μόνο από το μέγιστο χωρητικό φορτίο του διαύλου των 400pF και τον αριθμό των συνδυασμών των 7 bit των διευθύνσεων (δηλαδή 128) των Slaves.



Εικόνα 29 : Έγκυρα δεδομένα

Παρακάτω φαίνεται η λειτουργική μονάδα του ATmega1281 που υλοποιεί την επικοινωνία μέσω διαύλου I²C.



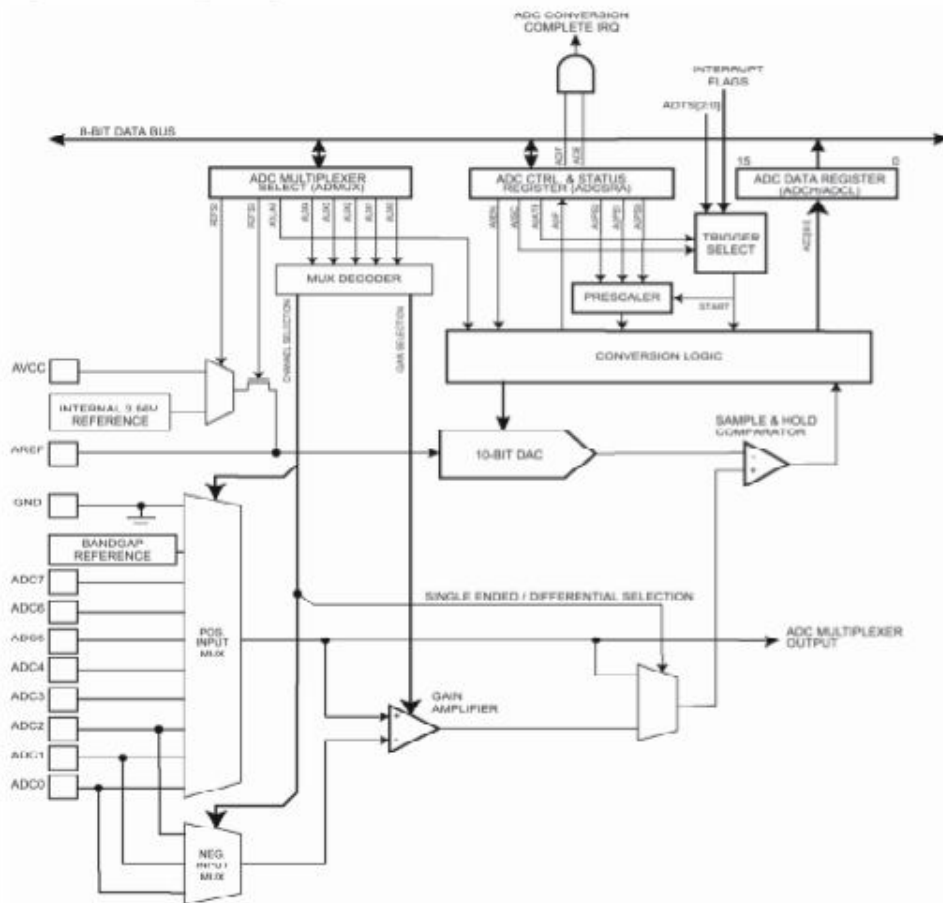
Εικόνα 30 : Απεικόνιση της λειτουργικής μονάδας I²C

4.4.8 Μετατροπές αναλογικού σήματος σε ψηφιακό (ADC - Analog to Digital Converter)

Ο ATmega1281 περιλαμβάνει έναν ADC ο οποίος μετατρέπει ένα αναλογικό σήμα εισόδου σε ψηφιακό σήμα των 10 bits με τη μέθοδο των διαδοχικών προσεγγίσεων. Ο ADC είναι συνδεδεμένος σε έναν αναλογικό πολυπλέκτη 8 καναλιών που επιτρέπει τη λήψη 8 τάσεων εισόδου από τους ακροδέκτες της Port A. Οι ακροδέκτες αυτοί είναι μη διαφορικοί (η τάση τους είναι σε αναφορά προς τη γη).

Η συσκευή επίσης υποστηρίζει 16 συνδυασμούς διαφορικών τάσεων εισόδου. Δύο από τις εισόδους αυτές (η ADC1, ADC0 και η ADC3, ADC2) είναι εξοπλισμένες με προγραμματιζόμενο στάδιο κέρδους με δυνατότητα ενίσχυσης 0dB (1x), 20dB (10x) ή 46dB (200x) της διαφορικής τάσης εισόδου πριν την A/D μετατροπή. Επτά κανάλια διαφορικών εισόδων τάσης μοιράζονται κοινό αρνητικό τερματικό (ADC1) ενώ για θετικό μπορεί να επιλεγεί οποιαδήποτε άλλη είσοδος του ADC.

Ο ADC περιλαμβάνει κύκλωμα δειγματοληψίας και διατήρησης (Sample and Hold) που εξασφαλίζει τη διατήρηση της τάσης εισόδου σε σταθερό επίπεδο κατά την μετατροπή. Διαθέτει επίσης ξεχωριστό ακροδέκτη τροφοδοσίας για το αναλογικό του μέρος.



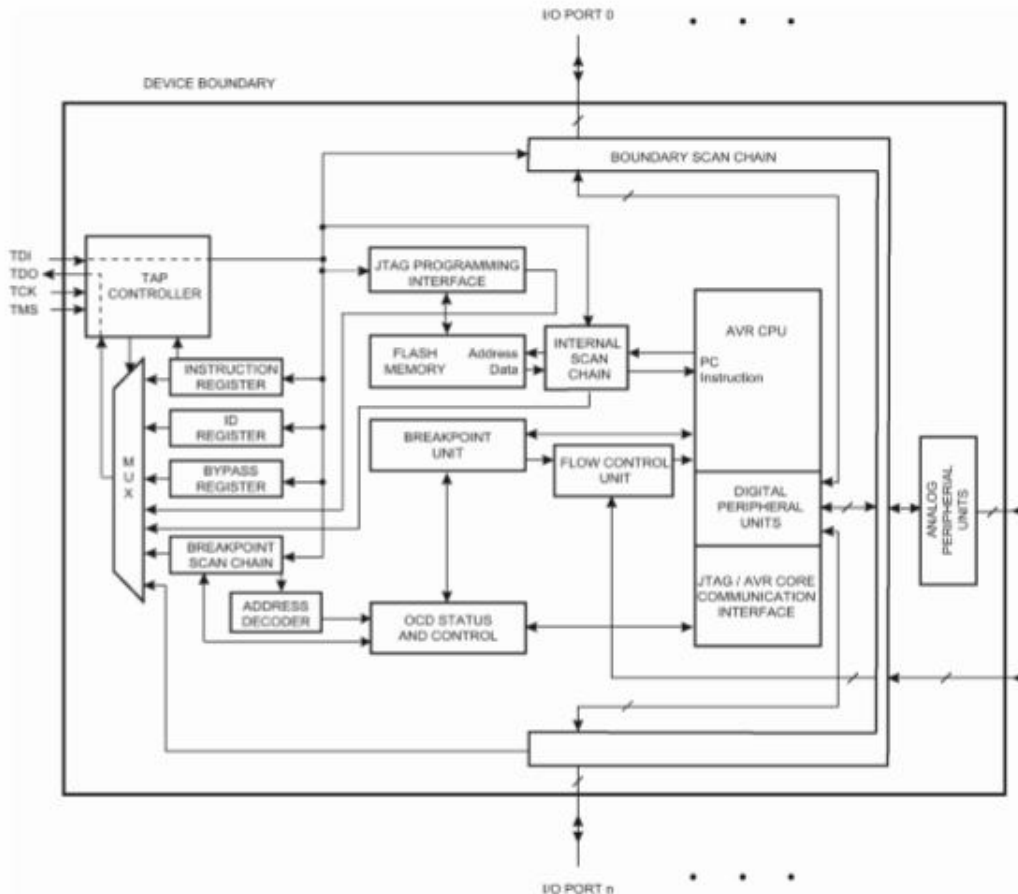
Εικόνα 31 : Σχηματικό διάγραμμα του ADC

4.4.9 Διεπαφή JTAG

Η διεπαφή JTAG του AVR μπορεί να χρησιμοποιηθεί για :

- Έλεγχο καρτών τυπωμένου κυκλώματος (PCBs) μέσω της δυνατότητας JTAG Boundary-scan
- Προγραμματισμό μη πτητικών μνημών, ασφαλειών και bits κλειδώματος
- Αποσφαλμάτωση πάνω στο chip (on-chip debugging)

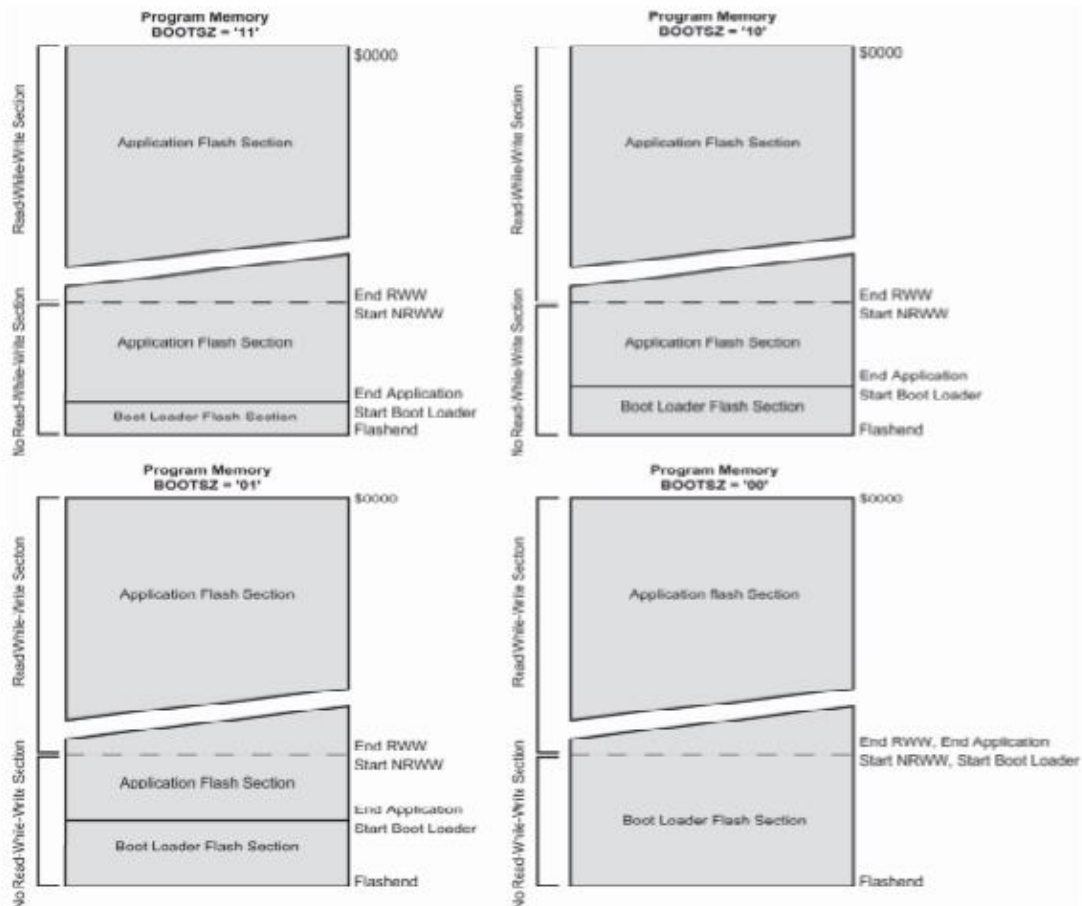
Στην (Εικόνα 32) φαίνεται το σχηματικό διάγραμμα της διεπαφής JTAG και του συστήματος αποσφαλμάτωσης. Ο ελεγκτής TAP είναι μια μηχανή κατάστασης που ελέγχεται από τα σήματα TCK και TMS. Ο ελεγκτής αυτός επιλέγει είτε τον καταχωρητή εντολών της JTAG είτε έναν από τους διάφορους καταχωρητές δεδομένων. Ο καταχωρητής εντολών περιέχει τις εντολές JTAG οι οποίες ελέγχουν τη συμπεριφορά κάποιου καταχωρητή δεδομένων.



Εικόνα 32 : Σχηματικό διάγραμμα της διεπαφής JTAG

4.4.10 Πρόγραμμα εκκίνησης (Boot Loader)

Η υποστήριξη Boot Loader παρέχει πραγματικό μηχανισμό αυτοπρογραμματισμού με δυνατότητα εγγραφής κατά την ανάγνωση. Με τον τρόπο αυτό είναι εφικτή η ευέλικτη ενημέρωση του λογισμικού κάτω από τον έλεγχο της MCU. Το πρόγραμμα Boot Loader μπορεί να χρησιμοποιήσει κάθε διαθέσιμη διεπαφή δεδομένων και το σχετικό πρωτόκολλο, για να διαβάσει κώδικα και να τον καταγράψει στη μνήμη Flash ή για να διαβάσει τον κώδικα από τη μνήμη προγράμματος είτε για να επαληθεύσει την σωστή εγγραφή είτε απλά για να επιστρέψει στη συσκευή προγραμματισμού το υπάρχον πρόγραμμα. Ο κώδικας προγράμματος του τμήματος Boot Loader έχει την ικανότητα να γράφει σε ολόκληρη τη Flash, περιλαμβανομένης και της μνήμης Boot Loader. Ο Boot Loader μπορεί επομένως να τροποποιήσει τον εαυτό του, ακόμα και να τον διαγράψει εάν δεν είναι πια αναγκαίος. Το μέγεθος της μνήμης Boot Loader καθορίζεται από ασφάλειες προγραμματισμού και ο Boot Loader έχει δύο ξεχωριστές διατάξεις bits κλειδώματος που καθορίζονται ανεξάρτητα. Με τον τρόπο αυτό ο χρήστης έχει μοναδική ευελιξία στην επιλογή επιπέδου ασφαλείας που επιθυμεί.



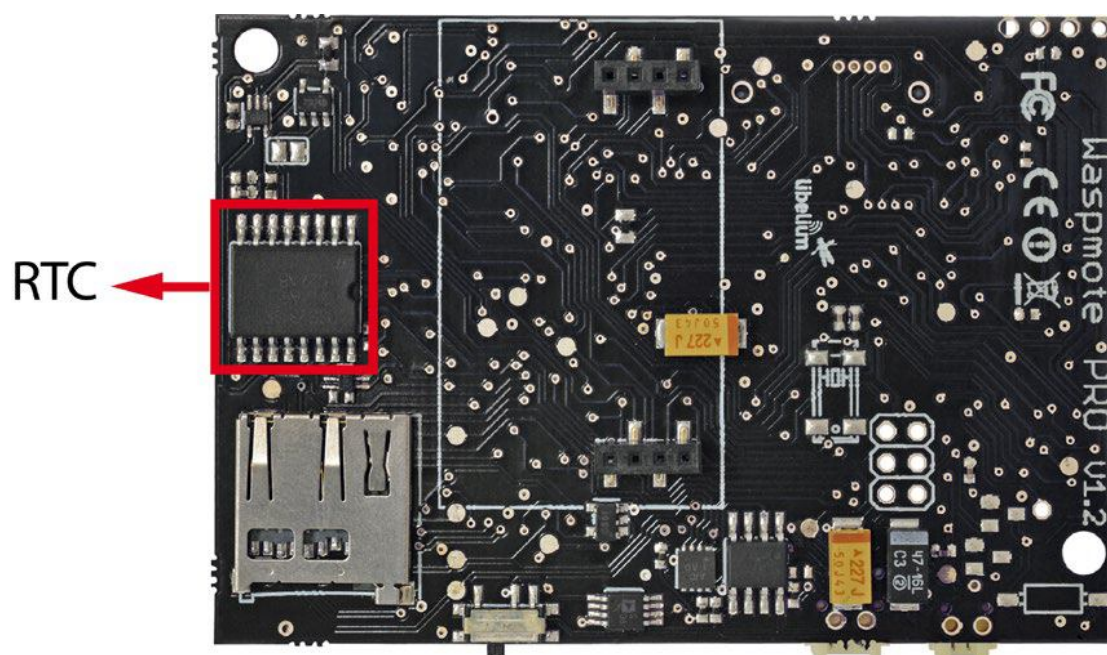
Εικόνα 33 : Τμήματα μνήμης

Η μνήμη Flash χωρίζεται σε δύο βασικά τμήματα, το τμήμα εφαρμογής και το τμήμα του Boot Loader, καθένα από τα οποία έχει διαφορετικό επίπεδο ασφάλειας. Το μέγεθος κάθε τμήματος καθορίζεται από τις ασφάλειες προγραμματισμού BOOTSZ, όπως φαίνεται στην (Εικόνα 33). Το τμήμα εφαρμογής είναι το τμήμα που η Flash χρησιμοποιεί για την αποθήκευση του κώδικα της εφαρμογής. Στο τμήμα αυτό δεν είναι δυνατή η αποθήκευση κώδικα Boot Loader καθώς η εντολή SPM (Store Program Memory) είναι ανενεργή όταν εκτελείται από το τμήμα εφαρμογής. Η εντολή SPM μπορεί να ενεργοποιηθεί προγραμματισμό μόνο όταν εκτελείται από το τμήμα Boot Loader και για αυτό εκεί αποθηκεύεται το λογισμικό του Boot Loader.

4.5 Αισθητήρες

4.5.1 Θερμοκρασίας

Το Waspnote RTC (DS3231SN from Maxim) έχει ένα ενσωματωμένο αισθητήρα θερμοκρασίας στο εσωτερικό του που τον χρησιμοποιεί για να καλιμπράρει τον εαυτό του. Το Waspnote μπορεί να έχει πρόσβαση στην τιμή αυτού του αισθητήρα μέσω της διεπαφής I²C.



Εικόνα 34: Temperature sensor in the RTC

Λήψη τιμών θερμοκρασίας:

```
{  
    RTC.getTemperature();  
}
```

Ο αισθητήρας παρουσιάζεται σε μια 10-bit μορφή συμπληρώματος ως προς δύο. Η μετρήσιμη θερμοκρασία είναι μεταξύ -40°C και $+85^{\circ}\text{C}$.

Δεδομένου ότι είναι ένας αισθητήρας ενσωματωμένος στο RTC, οποιαδήποτε εφαρμογή που απαιτεί ενσύρματα έναν αισθητήρα θερμοκρασίας μέσω καλωδίου, πρέπει να ενσωματωθεί στις αναλογικές και ψηφιακές εισόδους, όπως έχει γίνει στην περίπτωση των sensor boards που σχεδιάστηκαν από την Libelium.

4.5.1.1 RTC

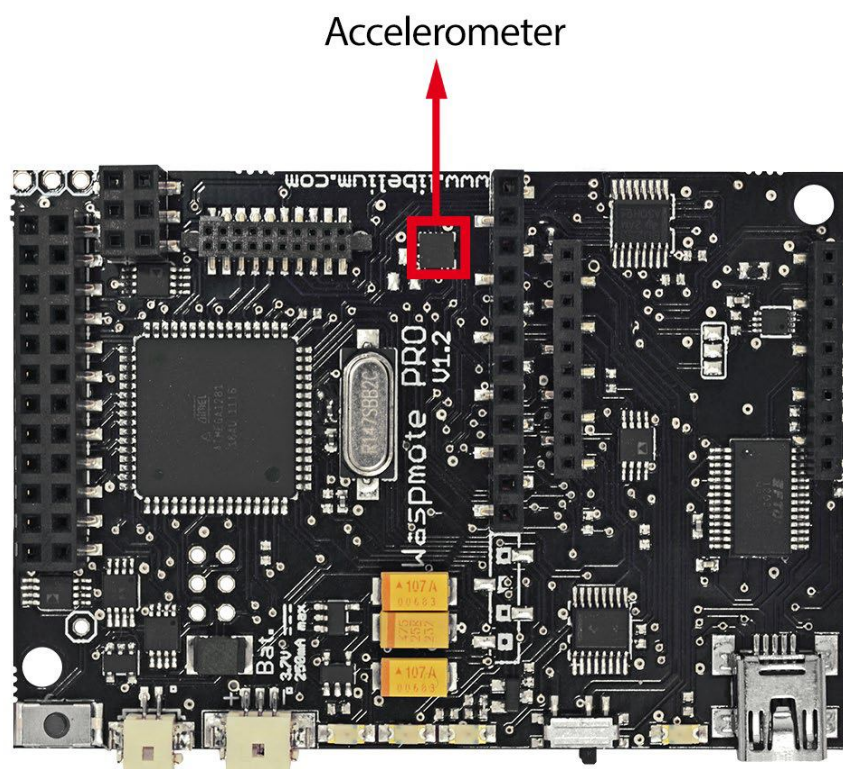
Το Wasmote έχει ένα ρολόι πραγματικού χρόνου (RTC) το οποίο «τρέχει» στα 32KHz και μπορεί να προγραμματιστεί προσδιορίζοντας την ημέρα / ώρα / λεπτό / δευτερόλεπτο. Αυτό επιτρέπει τον πλήρη έλεγχο όταν το Wasmote εκκινά για να καταγράψει τις τιμές και να εκτελεί τις δράσεις που προγραμματίζονται σε αυτό. Επίσης, το RTC επιτρέπει στο Wasmote να λειτουργεί στο μέγιστο λειτουργίας εξοικονόμησης ενέργειας και να επανέρχεται σε λειτουργία μόνο όταν αυτό είναι απαραίτητο. Τα διαστήματα αδρανοποίησης μπορούν να κυμαίνονται από 8sec-min-hours-days.

4.5.2 Επιταχυνσιόμετρο

Το Wasmote έχει ενσωματωμένο έναν αισθητήρα επιτάχυνσης (LIS3331LDH STMicroelectronics) ο οποίος το ενημερώνει για μεταβολές που σημειώνεται σε κάθε έναν από τους 3 άξονες (X, Y, Z).

Η ενσωμάτωση αυτού του αισθητήρα επιτρέπει την μέτρηση της επιτάχυνσης πάνω στους 3 άξονες (X, Y, Z), καθιερώνοντας 4 είδη κινήσεων :

- Ελεύθερη πτώση
- Διακοπή αδρανοποίησης
- 6D κίνηση
- 6D θέση

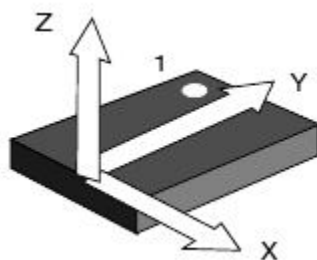


Εικόνα 35: Accelerometer

Ο LIS331DLH είναι ικανός να μετρά επιταχύνσεις με εξερχόμενους ρυθμούς δεδομένων από 0,5 Hz έως 1 kHz. Η συσκευή διαθέτει εξαιρετικά χαμηλής ισχύος λειτουργίες που επιτρέπουν την εξοικονόμηση ενέργειας και την επιλεκτική αδρανοποίηση. Το επιταχυνσιόμετρο έχει 7 επίπεδα λειτουργίας ισχύος, ο εξερχόμενος ρυθμός δεδομένων (ODR) θα εξαρτηθεί από το επιλεγμένο επίπεδο ισχύος. Τα επίπεδα λειτουργίας και ο εξερχόμενος ρυθμός δεδομένων εμφανίζονται στον (Πίνακας 3):

Power mode	Output data rate (Hz)
Power down	--
Normal mode	1000
Low-power 1	0,5
Low-power 2	1
Low-power 3	2
Low-power 4	5
Low-power 5	10

Πίνακας 3



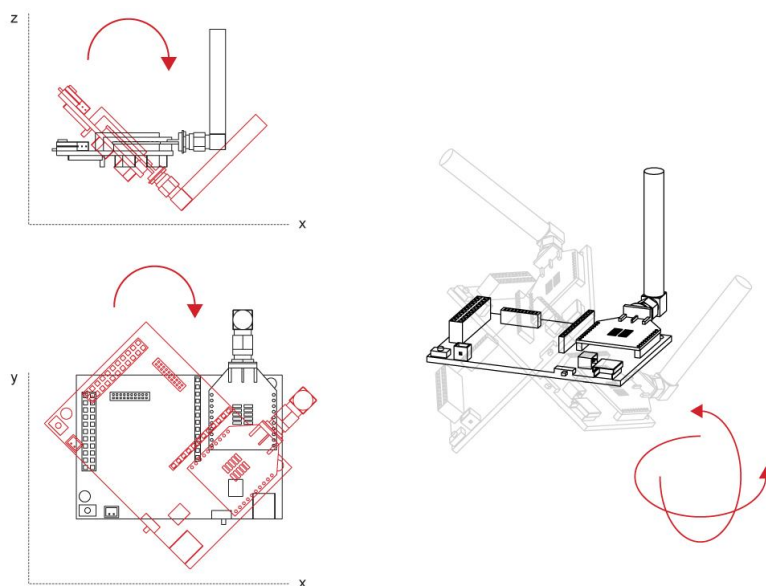
Εικόνα 36: Axes in the LIS3LV02DL accelerometer

Το επιταχυνσιόμετρο έχει την ικανότητα του αυτοελέγχου που επιτρέπει στο χρήστη να ελέγχει τη λειτουργία του αισθητήρα στην τελική εφαρμογή. Το εύρος θερμοκρασίας λειτουργίας του είναι μεταξύ -40°C και $+85^{\circ}\text{C}$. Το επιταχυνσιόμετρο επικοινωνεί με τον μικροελεγκτή μέσω της διεπαφής I²C.

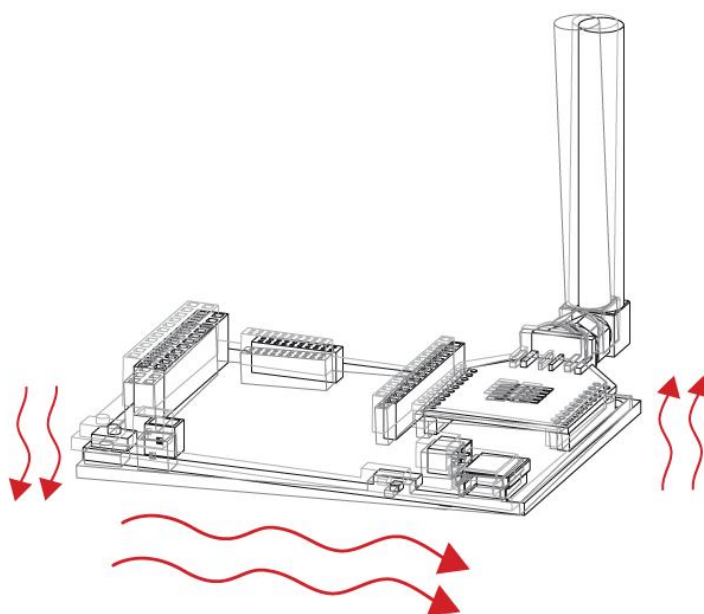
Λήψη τιμών θερμοκρασίας:

```
{  
ACC.ON();  
ACC.getX();  
ACC.getY();  
ACC.getZ();  
}
```

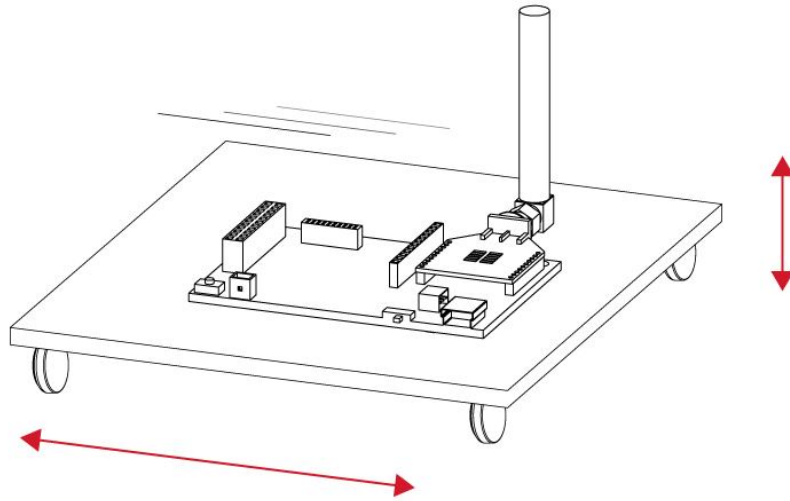
Παρακάτω φαίνονται ορισμένες χρήσεις του επιταχυνσιόμετρου.



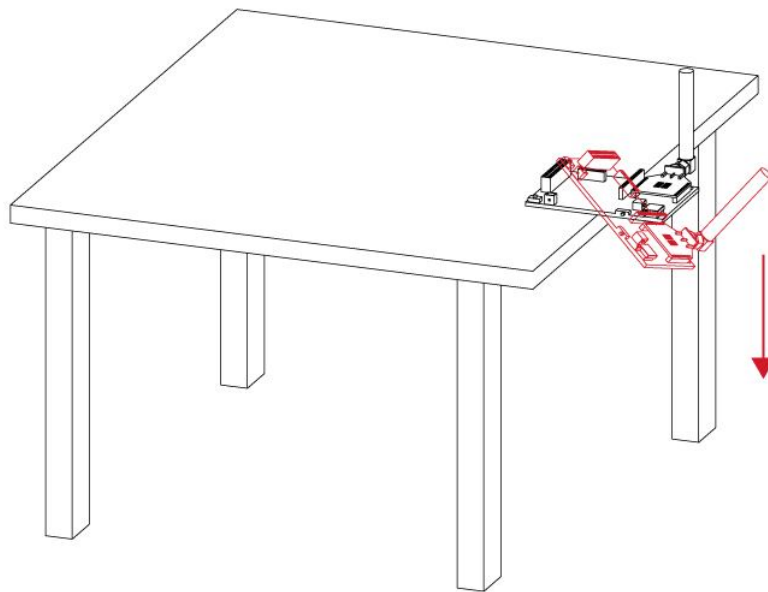
Εικόνα 37: Rotation and Twist



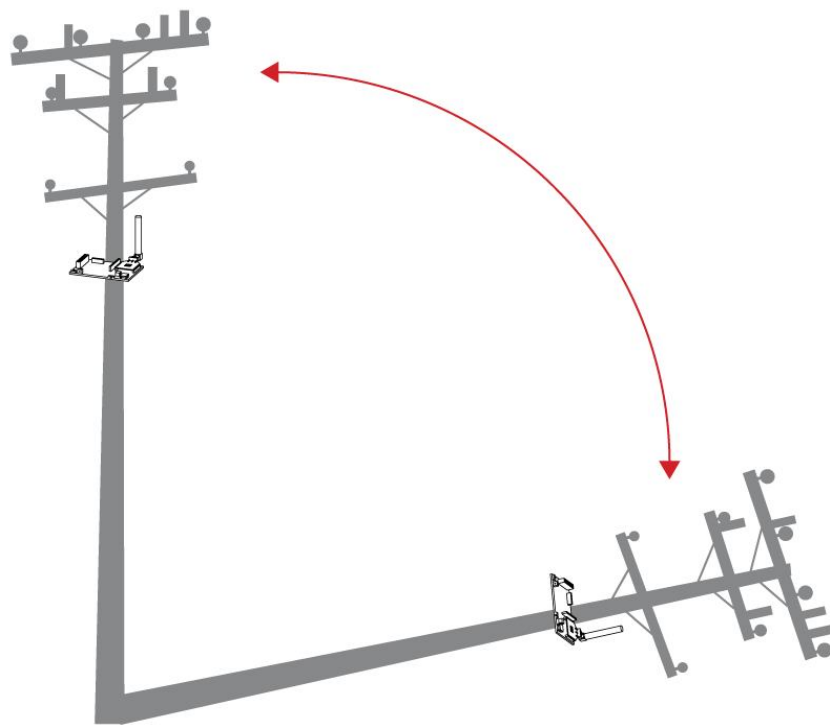
Εικόνα 38: Vibration



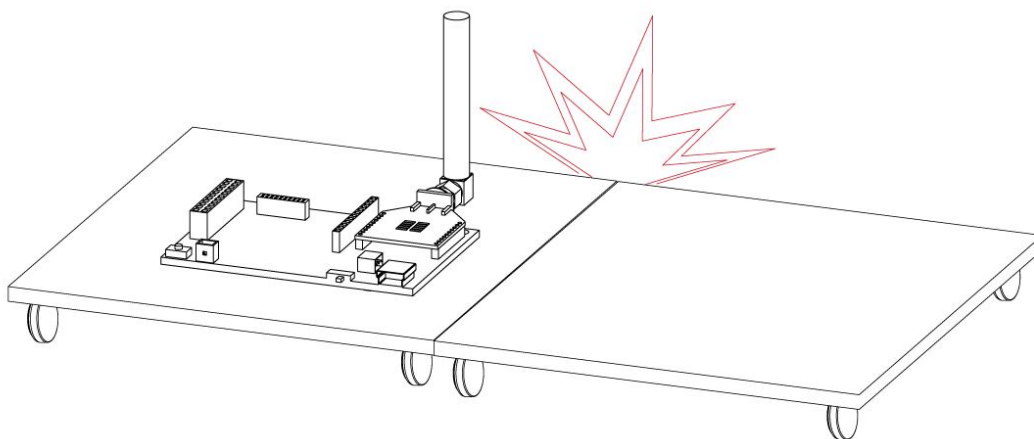
Εικόνα 39: Acceleration



Εικόνα 40: Free fall

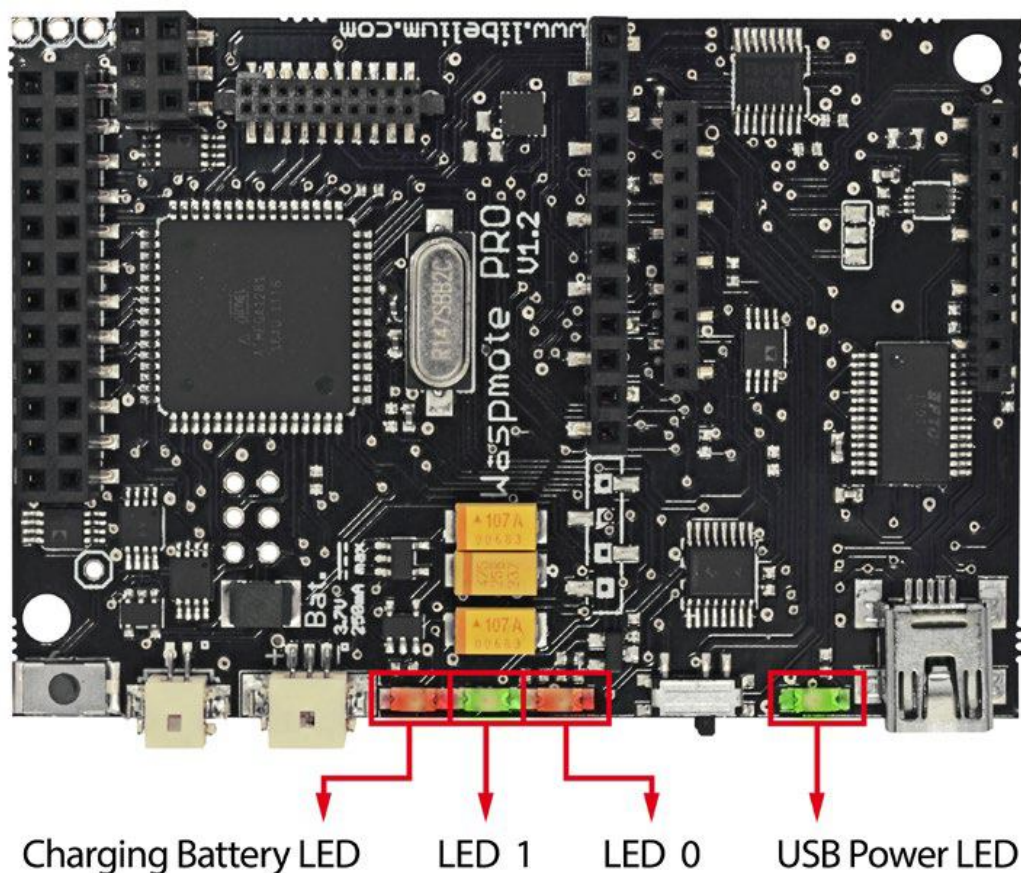


Εικόνα 41: Free fall of objects in which it is installed



Εικόνα 42: Crash

4.6 LEDs



Εικόνα 43: Visual indicator LEDs

- Charging battery LED indicator

Το κόκκινο LED υποδεικνύει ότι η μπαταρία είναι συνδεδεμένη στο WaspMote, η οποία και φορτίζεται μέσω μίας mini USB ή μέσω ενός solar panel τα οποία είναι συνδεδεμένα πάνω στο WaspMote. Από την στιγμή που η μπαταρία έχει φορτιστεί πλήρως, το LED σβήνει αυτόματα.

- LED 0 – programmable LED

Το πράσινο LED είναι συνδεδεμένο στον μικροελεγκτή, το οποίο και είναι πλήρως προγραμματίσιμο από τον χρήστη. Επιπλέον το LED 0 αναβοσβήνει κάθε φορά που ενεργοποιείται το reset button πάνω στο WaspMote.

- LED 1 – programmable LED

Ένα κόκκινο LED είναι συνδεδεμένο στον μικροελεγκτή το οποίο και είναι πλήρως προγραμματίσιμο από τον χρήστη.

- USB Power LED indicator

Πράσινο LED το οποίο υποδεικνύει ότι το Wasmote είναι συνδεδεμένο είτε για φόρτιση της μπαταρίας, είτε για τον προγραμματισμό του μικροελεγκτή. Όταν το LED ανάβει μας δείχνει ότι το η mini USB είναι σωστά συνδεδεμένη, ενώ όταν αυτή αφαιρεθεί το LED σβήνει αυτόματα.

Προγραμματιστικό κομμάτι:

Τα LED0 και LED1 αφορούν το προγραμματιστικό κομμάτι και οι λειτουργίες που χειρίζονται αυτά τα LEDs είναι οι:

- `Utils.setLED(LED_SELECTED, LED_MODE)`
- `Utils.getLED(LED_SELECTED)`
- `Utils.blinkLEDs()`

Τα άλλα δύο LEDs ανοιγοκλείνουν αυτόματα ανάλογα με την λειτουργία τους.

```
{  
  
    Utils.setLED(LED0, LED_ON);  
    Utils.setLED(LED1, LED_OFF);  
    Utils.blinkLEDS(1000);  
}
```

4.7 Prototyping Board 2.0

4.7.1 Γενική περιγραφή

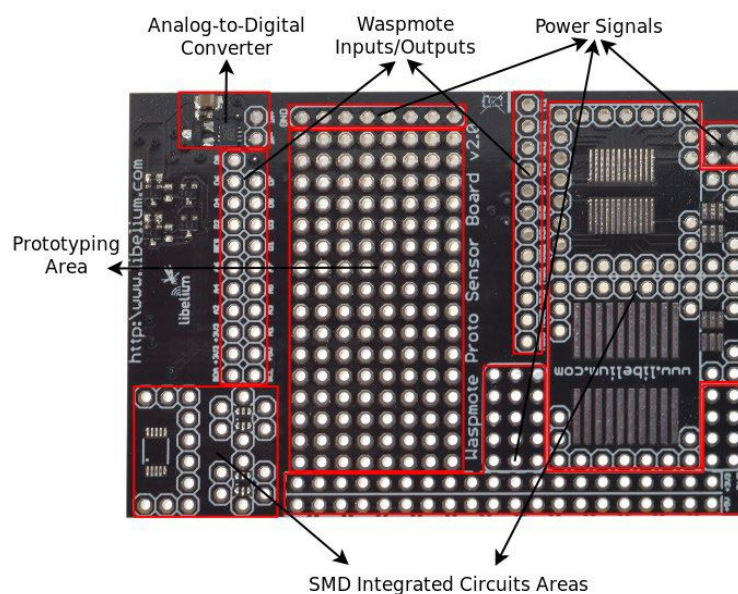
Το Wasmote Prototyping Board 2.0 έχει σχεδιαστεί ώστε να είναι όσο το δυνατόν ευκολότερο για το χρήστη να ενσωματώνει οποιοδήποτε τύπου αισθητήρα. Με αυτό το σκεπτικό, η πλακέτα έχει πάνω της ένα 16-bit μετατροπέα αναλογικού σε ψηφιακό σήμα (ADC).

4.7.2 Προδιαγραφές

Weight: 20gr

Dimensions: 73.5 x 51 x 1.3 mm

Temperature Range: [-20°C, 65°C]



Εικόνα 44: Upper side

4.7.3 Ηλεκτρικά χαρακτηριστικά

4.7.3.1 Πειραματικές τιμές

- Board supply voltages: 3.3V and 5V
- Analog-to-Digital converter supply voltage: 5V
- Maximum admitted current (continuous): 200mA
- Maximum admitted current (peak): 400mA

4.7.3.2 Απόλυτες μέγιστες τιμές

- Microprocessor pin voltage: -0.5V to 3.8V
- Analog-to-Digital converter input voltage: -0.3V to 5.3V
- Microprocessor pin current: 40mA

4.7.4 Prototyping area

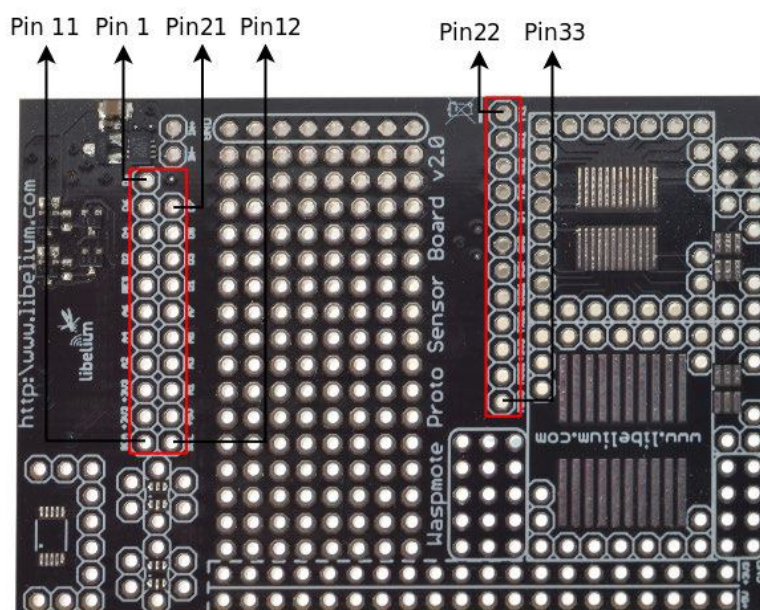
Η prototyping περιοχή η οποία συμπεριλαμβάνεται πάνω στην πλακέτα, χωρίζεται σε δύο περιοχές :

- pads area
- integrated circuits area

4.7.4.1 Pads Area

Αυτή είναι μια μήτρα που αποτελείται από 16x8 pads, διαμέτρου 1mm , στόχος των οποίων είναι να συνδέονται με ξεχωριστά στοιχεία, όπως αντιστάσεις, πυκνωτές ή ολοκληρωμένα κυκλώματα. Η επιμεταλλωμένη περιοχή κάθε pad είναι διαμορφωμένη έτσι ώστε να διευκολύνει τη συγκόλληση των στοιχείων προς τα αυτήν.

Στο πάνω και στο κάτω μέρος της μήτρας υπάρχουν λωρίδες από pads που παρέχουν την έξοδο όλων των σημάτων των κόμβων των αισθητήρων. Στην (Εικόνα 45) και στον (Πίνακας 4) μπορούμε να δούμε ποιο pin του μικροεπεξεργαστή αντιστοιχεί σε κάθε pad.

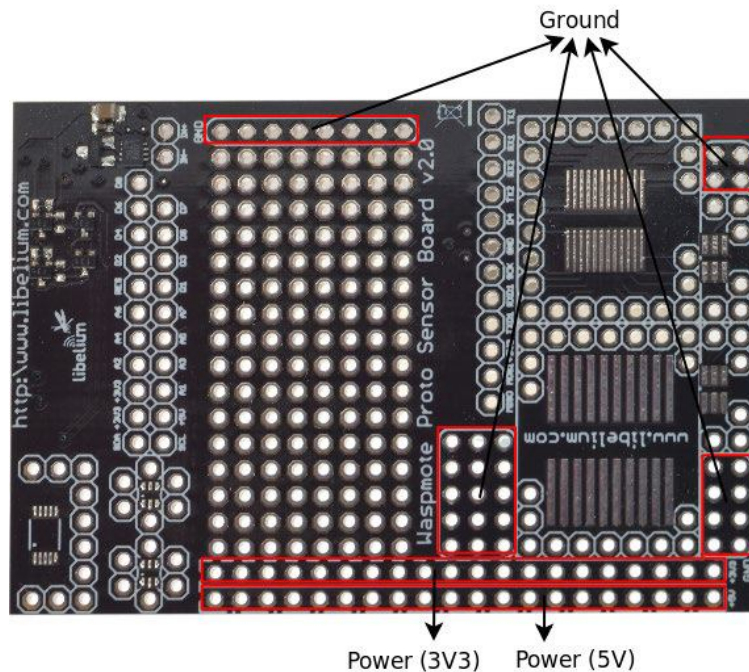


Εικόνα 45: Waspimote inputs and outputs

Pin	Description
1	Digital input/output signal DIGITAL8
2	Digital input/output signal DIGITAL6
3	Digital input/output signal DIGITAL4
4	Digital input/output signal DIGITAL2
5	Reserved
6	Digital input/output signal and analog input ANALOG6
7	Digital input/output signal and analog input ANALOG4
8	Digital input/output and analog input signal ANALOG2
9	3.3V Power supply (SENS_PW_3V3)
10	3.3V Power supply (GPS_PW)
11	SDA (I2C bus signal)
12	SCL (I2C bus signal)
13	5V Power supply (SENS_PW_5V)
14	Digital input/output signal and analog input ANALOG1
15	Digital input/output signal and analog input ANALOG3
16	Digital input/output signal and analog input ANALOG5
17	Digital input/output signal and analog input ANALOG7
18	Digital input/output signal DIGITAL1
19	Digital input/output signal DIGITAL3
20	Digital input/output signal DIGITAL5
21	Digital input/output signal DIGITAL7
22	Transmission Output UART 1 SERIAL_1_TX
23	Reception Input UART 1 SERIAL_1_RX
24	Reception Input UART 2 SERIAL_2_RX
25	Transmission Output UART 2 SERIAL_2_TX
26	Battery Supply Voltage
27	Ground GND
28	SCK (SPI bus signal)
29	High interrupt input signal RXD1
30	Low interrupt input signal TXD1
31	3.3V Supply Voltage (SENS_PW_3V3)
32	MOSI (SPI bus signal)
33	MISO (SPI bus signal)

Πίνακας 4

Στην (Εικόνα 46) βλέπουμε δύο σειρές από pad τροφοδοσίας, των 3.3 V και 5V, όπως επίσης και την γείωση.

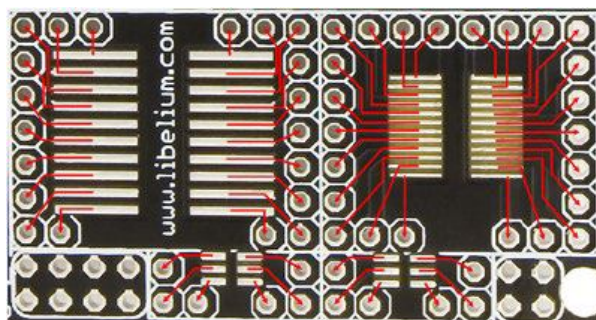


Εικόνα 46: Power supply pads

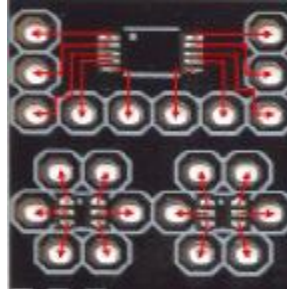
4.7.4.2 Integrated Circuits Area

Επτά ίχνη έχουν δοθεί στα SMD ολοκληρωμένα κυκλώματα για διαφορετικά μεγέθη: Μία 20 θύρα SO τύπου, μία 24 θύρα TSSOP, μία 10 θύρα micro-SOIC, δύο 6 θύρες SOT-23 και δύο 6 θύρες SC-70. Η έξοδος για κάθε θύρα των ίχνων δίνεται μέσω ενός pad με διάμετρο 1 mm, από το οποίο είναι δυνατή η πρόσβαση στο κύκλωμα.

Στις (Εικόνα 47) και (Εικόνα 48) φαίνονται τα ίχνη των ολοκληρωμένων κυκλωμάτων.



Εικόνα 47: SO, TSSOP and SOT-23 circuit area



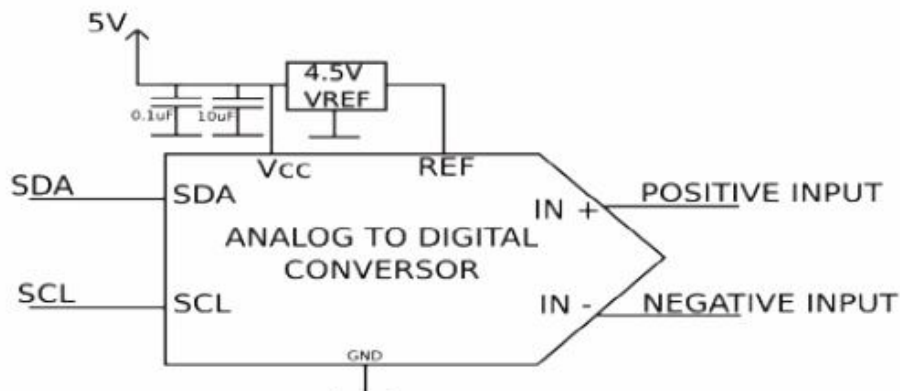
Εικόνα 48: Micro-SOIC and SC-70 circuit area

4.7.5 Analog-to-Digital Converter

Ο μικροεπεξεργαστής του Waspote ενσωματώνει ένα 10-bit μετατροπέα αναλογικού σε ψηφιακό σήμα ο οποίος και μπορεί να προσεγγιστεί μέσω οποιασδήποτε από τις αναλογικές εισόδους των 2x11 ακίδων. Στην περίπτωση που κάποια εφαρμογή απαιτεί ψηλότερη ανάλυση, ένας 16-bit μετατροπέας Sigma-Delta (ΣΔ) αναλογικού σε ψηφιακό σήμα έχει προστεθεί στην prototyping πλακέτα, με μέγιστο χρόνο μετατροπής τα 23ms.

Η επικοινωνία με τη συσκευή αυτή πραγματοποιείται μέσω της διεπαφής I²C. Κάθε μία από τις εισόδους παρέχει ένα εύρος τιμών τάσης μεταξύ 0 και 4.5V, επιτρέποντας ως εκ τούτου μετρήσεις διαφοράς μεταξύ 4.5V-4.5V. Για να έχουμε μια πιο ακριβή ανάγνωση, η τάση αναφοράς για τη μετατροπή καθορίζεται από την τάση αναφοράς των 4.5V, μοντέλο MAX6107.

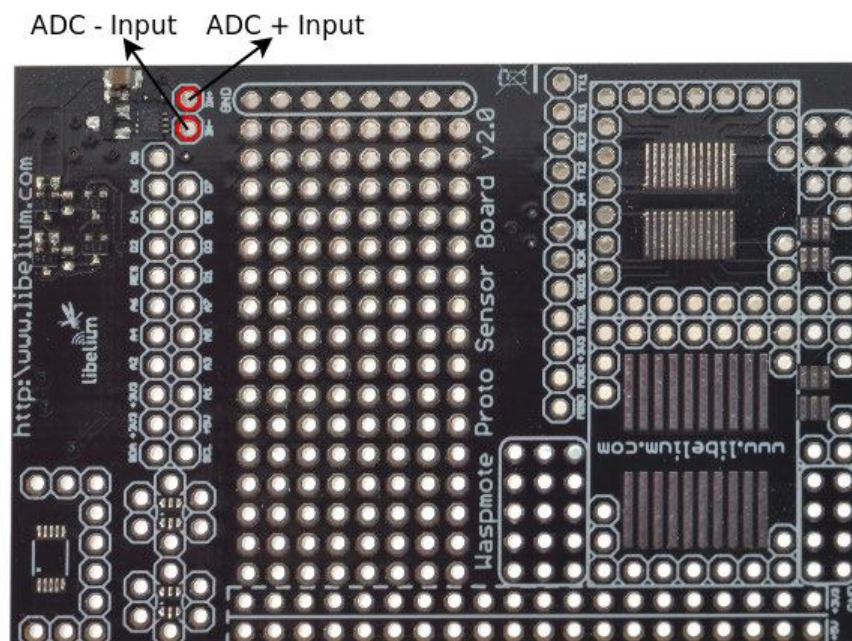
Στην (Εικόνα 49) υπάρχει ένα διάγραμμα των συνδέσεων του μετατροπέα, και στην (Εικόνα 50) φαίνονται τα pads των συνδέσεών του.



Εικόνα 49: Analog-to-digital converter

Basic reading code:

```
{  
float value;  
SensorProtov20.ON();  
delay(10);  
value = SensorProtov20.readADC();  
}
```



Εικόνα 50: Input pins to the analog-to-digital converter

4.8 XBee Module - ZB Series 2

4.8.1 Γενικά

Τα XBee-ZB έχουν ενσωματωμένες RF μονάδες οι οποίες και παρέχουν οικονομική-αποδοτική ασύρματη επικοινωνία για συσκευές σε δίκτυα πλέγματος ZigBee. Τα προϊόντα της οικογένειας XBee είναι εύκολα στη χρήση. Δεν απαιτούν καμία ρύθμιση με αποτέλεσμα οι χρήστες να μπορούν να θέσουν το δίκτυο σε λειτουργία σε μόλις λίγα λεπτά.

Οι προγραμματιζόμενες εκδόσεις της μονάδας ZB XBee κάνουν την προσαρμογή των εφαρμογών ZigBee ευκολότερη. Ο προγραμματισμός απευθείας πάνω στην μονάδα ZigBee εξαλείφει την ανάγκη για ένα ξεχωριστό επεξεργαστή. Επειδή το ασύρματο λογισμικό είναι απομονωμένο, οι εφαρμογές μπορούν να αναπτυχθούν χωρίς κίνδυνο μέσω της μονάδος RF.

Οι XBee μονάδες είναι διαθέσιμες σε μια ποικιλία πρωτοκόλλων και συχνοτήτων. Τα κοινά pins που χρησιμοποιούν από κοινού οι μονάδες XBee Digi αποσκοπούν στην εύκολη αντικατάσταση ενός XBee από ένα άλλο σε ελάχιστο χρόνο και χωρίς κανένα κίνδυνο.

4.8.2 Τεχνικά χαρακτηριστικά

4.8.2.1 Επιδόσεις

- RF Data Rate : 250 Kbps
- Indoor/Urban Range : 133 ft (40 m)
- Outdoor/RF Line-of-Sight Range: 400 ft (120 m)
- Transmit Power : 1.25 mW (+1 dBm) / 2 mW (+3 dBm) boost mode
- Receiver Sensitivity (1% PER) : -96 dBm in boost mode

4.8.2.2 Χαρακτηριστικά

- I/O Interface : 3.3V CMOS UART, ADC, DIO
- Configuration Method : API or AT commands, local or over-the-air
- Frequency Band : 2.4 GHz
- Interference Immunity : DSSS (Direct Sequence Spread Spectrum)
- Serial Data Rate : 1200 bps - 1 Mbps
- ADC Inputs: (4) 10-bit ADC inputs
- Digital I/O : 10
- Antenna Options : Chip, Wire Whip, U.FL, RPSMA
- Operating Temperature : -40° C to +85° C, 0-95% humidity non-condensing

4.8.2.3 Λογισμικό

- Memory : N/A
- CPU/Clock Speed : N/A

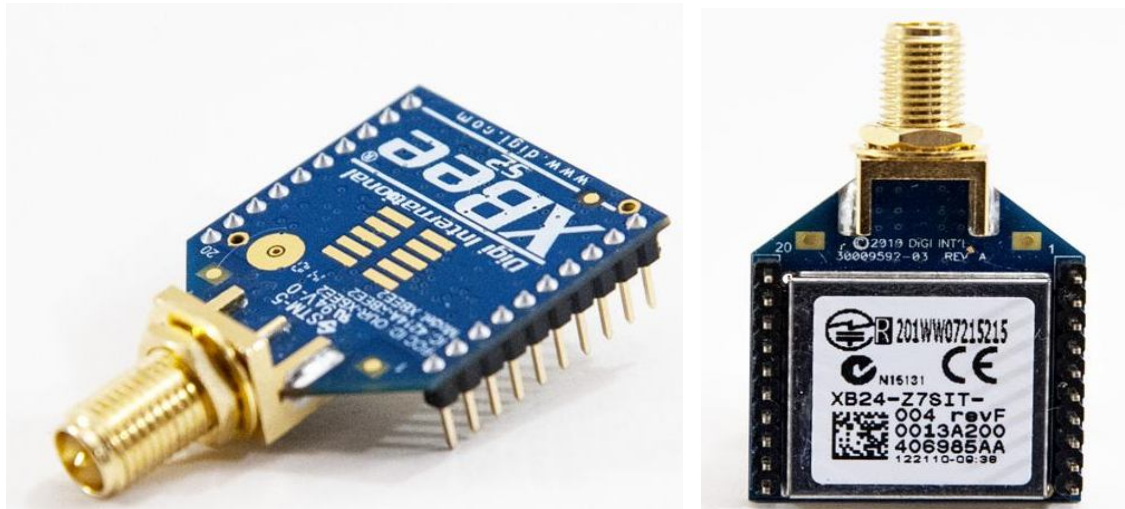
4.8.2.4 Δίκτυα και ασφάλεια

- Encryption : 128-bit AES
- Reliable Packet Delivery : Retries/Acknowledgments
- IDs and Channels : PAN ID, 64-bit IEEE MAC, 16 channels

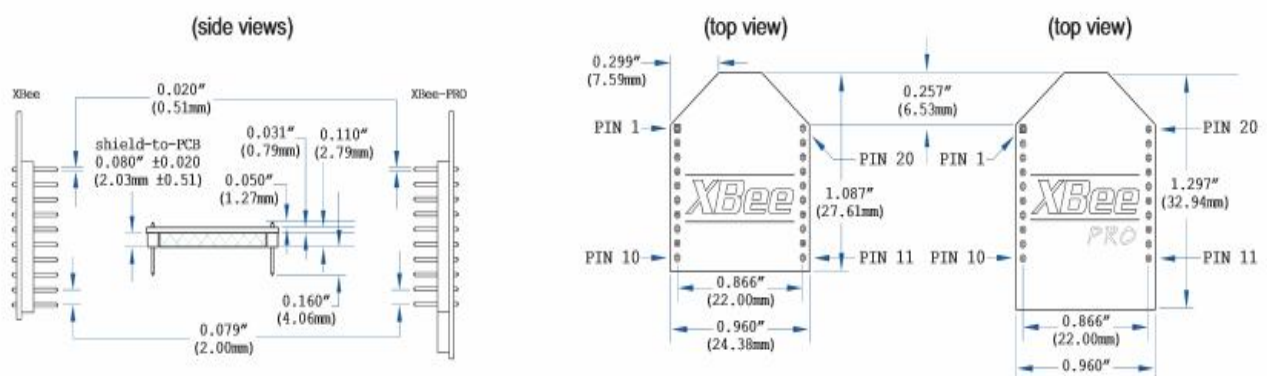
4.8.2.5 Απαιτήσεις ισχύος

- Supply Voltage : 2.1 - 3.6VDC
- Transmit Current : 35 mA / 45 mA boost mode @ 3.3VDC
- Receive Current : 38 mA / 40 mA boost mode @ 3.3VDC
- Power-Down Current : <1 uA @ 25° C

4.8.3 XBee ZB Hardware και Pin Layout



Εικόνα 51 : XBee Module - ZB Series 2



Εικόνα 52 : Διαστάσεις ZigBee, ZigBee-Pro

1	VCC3.3	SDA/I0	20
2	TX/I0	SCL/I0	19
3	RX/I0	I08	18
4	I00	I07	17
5	RESET	RTS/I0	16
6	I01	I06	15
7	I02	VREF	14
8	I03	I05	13
9	DTR/I0	CTS/I0	12
10	GND	I04	11

Εικόνα 53 : Pin Layout

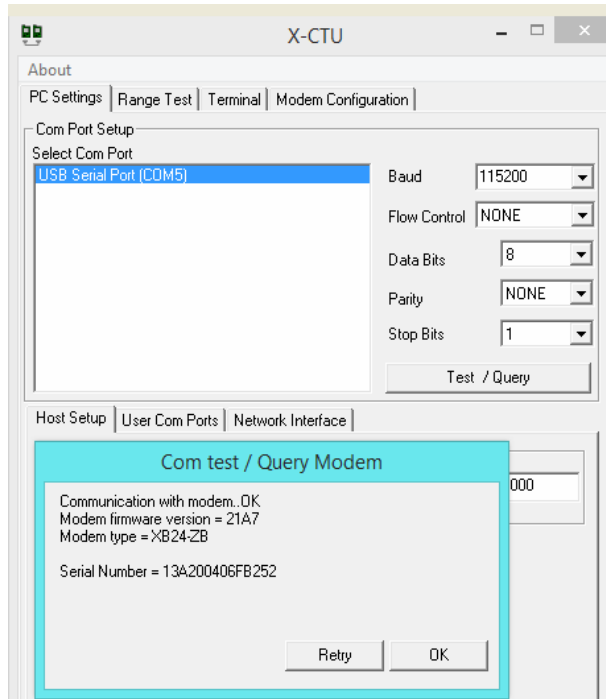
ΚΕΦΑΛΑΙΟ 5 : Λογισμικό-Μετρήσεις

5.1 Setup πειράματος

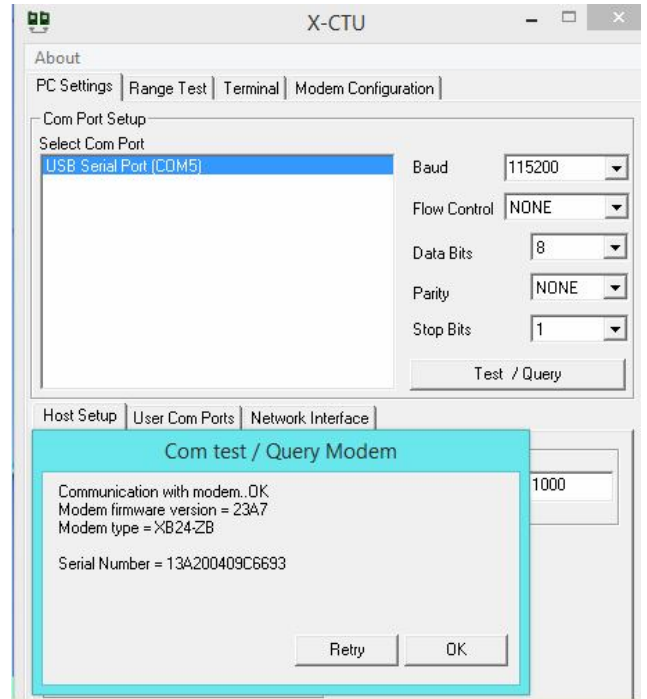
Για τα πειράματά μας χρησιμοποιήσαμε το XBee Series 2, 2mW, model XB24-ZB της Digi International. Κάθε μονάδα είναι εφοδιασμένη με μία ενσύρματη κεραία. Στήνουμε τα single-hop και multi-hop ασύρματα δίκτυα αισθητήρων, όπου κάθε κόμβος εμπεριέχει μία μονάδα XBee. Για τον προγραμματισμό κάθε κόμβου, χρησιμοποιήσαμε το ελεύθερο λογισμικό X-CTU, το οποίο παρέχεται από την Digi International. Με το X-CTU, ο χρήστης είναι σε θέση να ενημερώνει τις παραμέτρους, να αναβαθμίζει το λογισμικό του μικροεπεξεργαστή και να εκτελεί εύκολα δοκιμαστικές συνδέσεις. Η επικοινωνία με τις μονάδες XBee γίνεται μέσω της διεπαφής I²C, η οποία συνδέεται μέσω ενός καλωδίου USB στον υπολογιστή μας (Εικόνα 54). Όλοι οι κόμβοι έχουν ρυθμιστεί ώστε να χρησιμοποιούν το ίδιο PAN (Personal Area Network) ID (Εικόνα 57) και (Εικόνα 58) με baud rate (ρυθμός εκπομπής σημάτων) τα 115200bps (Εικόνα 55) και (Εικόνα 56). Το XBee προσφέρει μεταδόσεις εμβέλειας 40 m για εσωτερικούς χώρους και 120 m για εξωτερικούς. Όλα τα πειράματα πραγματοποιηθήκαν σε εσωτερικό χώρο στην ζώνη των 2.4 GHz αφού το XBee υποστηρίζει μόνο αυτή τη ζώνη συχνοτήτων.



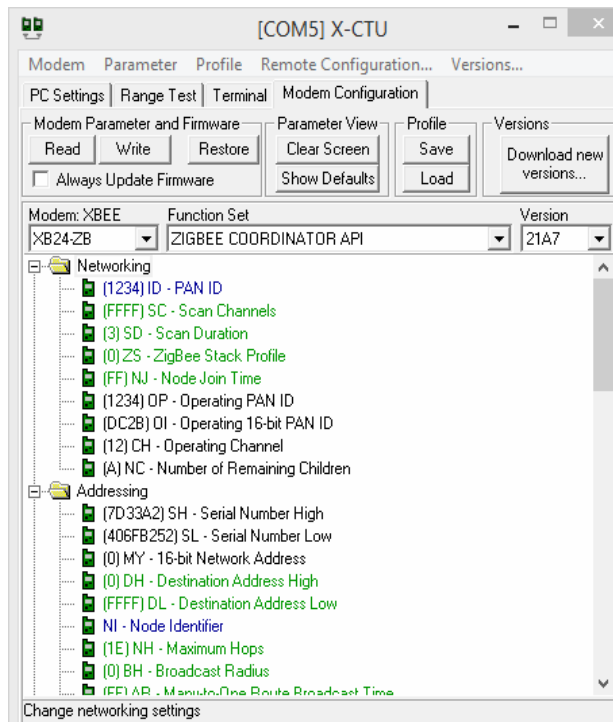
Εικόνα 54 : XBee connected to PC via Xbee interface board



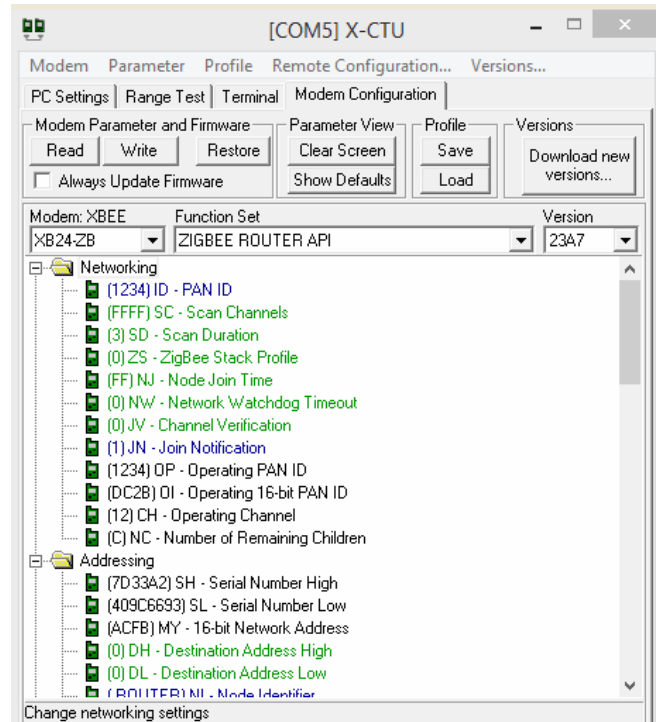
Εικόνα 55 : Coordinator



Εικόνα 56 : Router



Εικόνα 57 : Coordinator



Εικόνα 58 : Router

5.2 Λογισμικό

Μέσω του ελεύθερου λογισμικού Waspnote Pro IDE version04 (Εικόνα 59), φορτώνουμε σειριακά (Εικόνα 60) στον μικροελεγκτή ATmega 1281 του Waspnote PRO v1.2 τον παρακάτω κώδικα.

```
#include <WaspXBeeZB.h>
#include <WaspFrame.h>

// Declare global variables
packetXBee* packet;
char macHigh[10];
char macLow[11];

void setup()
{
    //////////////////////////////////////
    // 1. set up the XBee module
    //////////////////////////////////////
    xbeeZB.ON();

    //////////////////////////////////////
    // 2. Set up RTC and ACC
    //////////////////////////////////////
    delay(500);
    RTC.ON();
    ACC.ON();

    //////////////////////////////////////
    // 3. LEDs management
    //////////////////////////////////////
    Utils.setLED(LED0, LED_ON);
    Utils.setLED(LED1, LED_ON);
    delay(2000);
    Utils.setLED(LED0, LED_OFF);
    Utils.setLED(LED1, LED_OFF);
    for (int i=0;i<24;i++)
    {
        Utils.blinkLEDs(125);
    }

    //////////////////////////////////////
}
```

```

// 4. Get the XBee MAC address
////////////////////////////////////
xbeeZB.ON();
delay(1000);
xbeeZB.flush();
// Get the XBee MAC address
int counter = 0;
while((xbeeZB.getOwnMac()!=0) && (counter<12))
{
  xbeeZB.getOwnMac();
  counter++;
}

// convert mac address from array to string
Utils.hex2str(xbeeZB.sourceMacHigh, macHigh, 4);
Utils.hex2str(xbeeZB.sourceMacLow, macLow, 4);

////////////////////////////////////
// 5. Print XBee module information
////////////////////////////////////
USB.ON();
USB.print("mac address:");
USB.print(macHigh);
USB.println(macLow);
USB.OFF();
}

void loop()
{
  //////////////////////////////////////
  // 6. Message composition
  //////////////////////////////////////

  // 6.1 Create new frame (No mote id)
  frame.createFrame(ASCII,"");

  // 6.2 Add frame fields
  frame.addSensor(SENSOR_MAC, macLow);
  frame.addSensor(SENSOR_ACC, ACC.getX(), ACC.getY(), ACC.getZ() );
  frame.addSensor(SENSOR_IN_TEMP, RTC.getTemperature());
  frame.addSensor(SENSOR_BAT, PWR.getBatteryLevel());

  // 6.3 Print frame

```

```

//Example:<=>· ª #35690399##5#MAC:4066EF6B#ACC:-47;-
26;1000#IN_TEMP:26.25#BAT:59#
frame.showFrame();

////////////////////////////////////
// 7. Send the packet
////////////////////////////////////

// 7.1 set packet to send
packet=(packetXBee*) calloc(1,sizeof(packetXBee)); // memory allocation
packet->mode=BROADCAST; // set Unicast mode

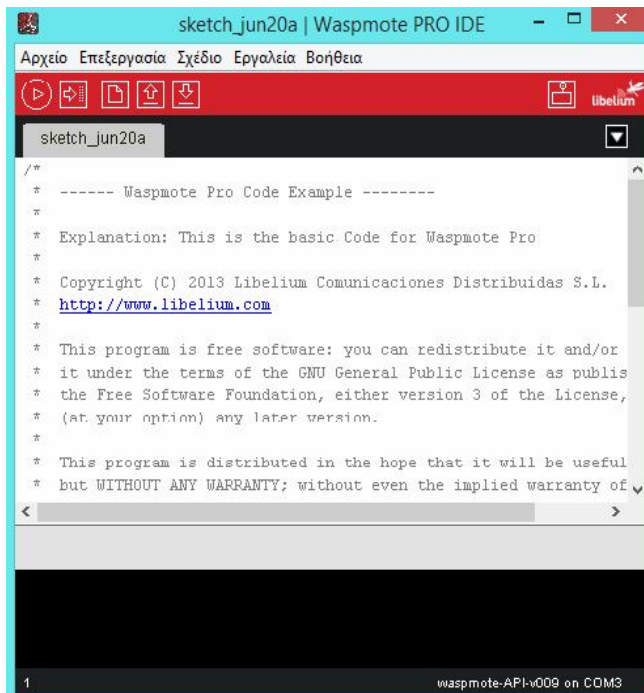
// 7.2 send the packet via the correct object depending on the protocol
// turn XBee on
xbeeZB.ON();
// sets Destination parameters
xbeeZB.setDestinationParams(packet, "000000000000FFFF", frame.buffer,
frame.length);
// send data
xbeeZB.sendXBee(packet);

// check TX flag
if( xbeeZB.error_TX == 0 )
{
  USB.println(F("sending ok"));
}
else
{
  USB.println(F("sending error"));
}

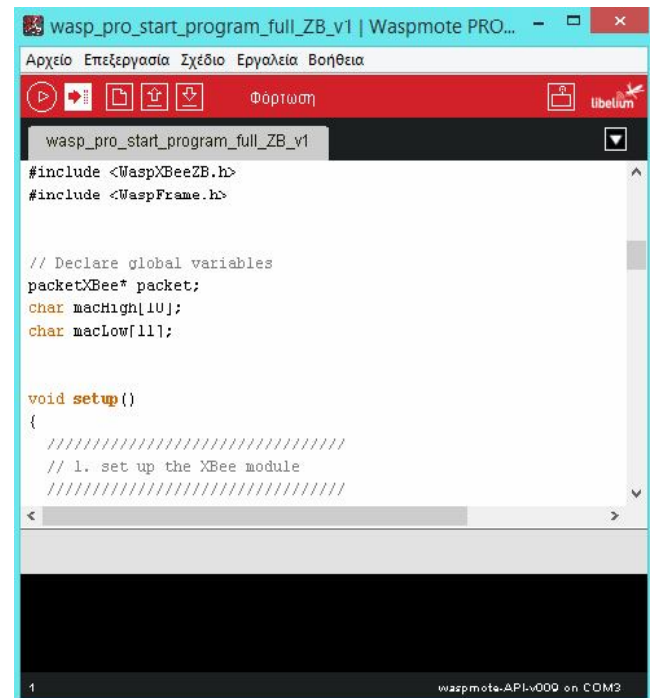
// 7.3 free memory
free(packet);
packet = NULL;

delay(1000);
}

```



Εικόνα 59 : Waspnote PRO IDE



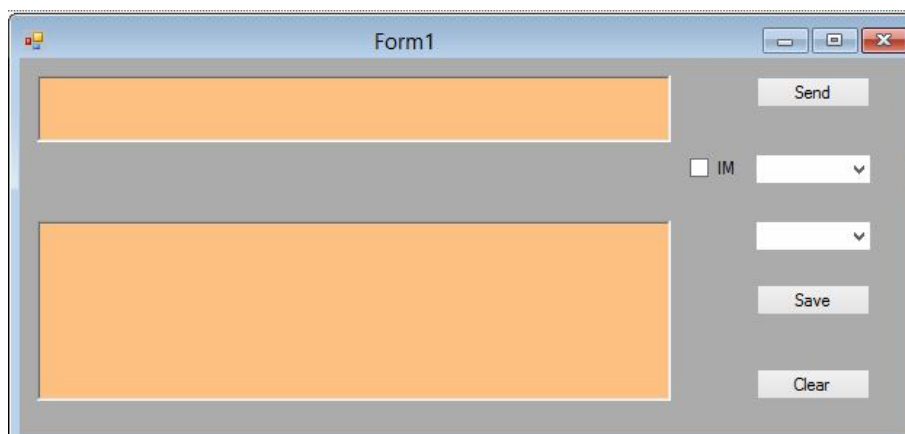
Εικόνα 60 : Φόρτωση κώδικα

5.3 Πειραματικές μετρήσεις και αποτελέσματα

5.3.1 Κατασκευή Serial Monitor

Για τα αποτελέσματα των μετρήσεων που θα λαμβάναμε ασύρματα μέσω του ZigBee Coordinator API, κατασκευάσαμε μία σειριακή οθόνη (Serial monitor) σε γλώσσα προγραμματισμού C# μέσω του Visual Studio, η οποία εκτός από το να εμφανίζει τα αποτελέσματα των μετρήσεων μπορεί και να τα αποθηκεύει σε οποιοδήποτε τύπου αρχείου επιθυμούμε.

Παρακάτω φαίνεται η σειριακή οθόνη (Εικόνα 61) και ο κώδικας που τρέχει κάτω από αυτή.



Εικόνα 61 : Serial Monitor

```

using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.IO;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;

namespace SerialPort
{
    public partial class Form1 : Form
    {
        public Form1()
        {
            InitializeComponent();
            if (!myserialPort.IsOpen)
            {
                myserialPort.Open();
                tbRX.Text = "port opened:";
            }
            else
                tbRX.Text = "busy";
        }
        private string rxString;
        private void myserialPort_DataReceived(object sender,
System.IO.Ports.SerialDataReceivedEventArgs e)
        {
            rxString = myserialPort.ReadExisting();
            this.Invoke(new EventHandler(displayText));
        }
        private void displayText(object o, EventArgs e)
        {
            tbRX.AppendText(rxString);
        }

        private void bSend_Click(object sender, EventArgs e)
        {
            myserialPort.Write(tbTX.Text);
        }
    }
}

```

```

private void bClear_Click(object sender, EventArgs e)
{
    tbTX.Clear();
    tbRX.Clear();
}

private void Form1_FormClosed(object sender, FormClosedEventArgs e)
{
    myserialPort.Close();
}

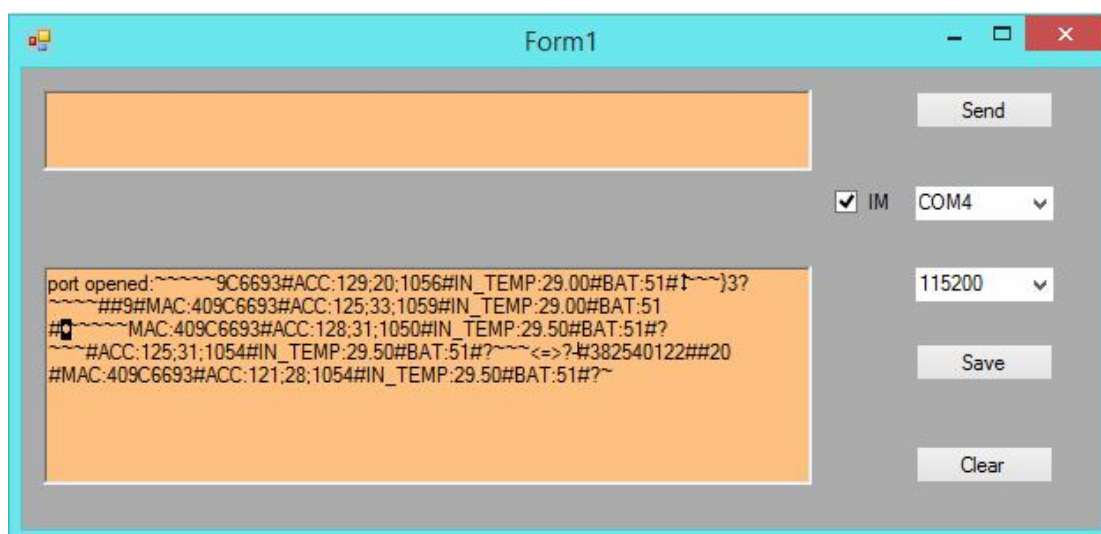
private void tbTX_KeyPress(object sender, KeyPressEventArgs e)
{
    if (myserialPort.IsOpen && checkBox1.Checked)
    {
        char[] ch = new char[1];
        ch[0] = e.KeyChar;
        myserialPort.Write(ch, 0, 1);
    }
}

private void bSave_Click(object sender, EventArgs e)
{
    if (saveFileDialog1.ShowDialog() ==
System.Windows.Forms.DialogResult.OK);
    {
        File.WriteAllText(saveFileDialog1.FileName, tbRX.Text);
    }
}
}
}

```


5.3.2 Εμφάνιση αποτελεσμάτων

Με την ενεργοποίηση του Wasmote PRO v1.2 LED 1, LED 0, ξεκινάει η αποστολή δεδομένων με baud rate 115200 bps από τον ZigBee Router API στον ZigBee Coordinator API (COM 4) και στη συνέχεια αυτά εμφανίζονται στο Serial Monitor (Εικόνα 62).



Εικόνα 62 : Serial Monitor

Από την εμφάνιση των μετρήσεων βλέπουμε ότι εκτός από την ωφέλιμη πληροφορία, εμφανίζονται και κάποια λάθη, του τύπου « ~~~~ » , « ~~~}3? » και « ~~~<=>?^l » που ίσως οφείλονται στον θόρυβο. Για αυτό τον λόγο αναπτύξαμε έναν κώδικα, έτσι ώστε να κρατάμε μόνο την πληροφορία που μας χρειάζεται και στην συνέχεια να την αποθηκεύουμε εκ νέου έτσι ώστε να μπορούμε να την επεξεργαστούμε.

Παρακάτω φαίνεται ο κώδικας, η ωφέλιμη πληροφορία (Εικόνα 63) και η μεταφορά της στο excel (Εικόνα 64) ώστε να μπορεί να επεξεργαστεί.

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Web;
using System.IO;
using System.Xml;
using System.Threading.Tasks;

public class Program
{
    static void Main()
    {

        FileStream fs = new FileStream(@"C:\Users\chris\Desktop\test.xls ",
        FileMode.Append);
        TextWriter standard = Console.Out; // save standard output
        foreach (string line in
        File.ReadAllLines(@"C:\Users\chris\Desktop\new\serial7"))
        {
            string[] parts = line.Split('#');
            List<Test> stringSplit = new List<Test>();
            Test t = new Test();
            foreach (string part in parts)
            {

                if (part.Contains("ACC"))
                {
                    t = new Test();
                    string[] accSZplit = part.Split(':');
                    t.output = part.ToString();
                    stringSplit.Add(t);
                }
                if (part.Contains("TEMP"))
                {
                    string[] tempSZplit = part.Split(':');
                    t.output += ", TEMP:" + tempSZplit[1].ToString();
                }

                if (part.Contains("BAT"))
```

```

        {
            string[] batSZplit = part.Split(':');
            t.output += ", BAT:" + batSZplit[1].ToString();

        }

    }

    //Output to console
    foreach (Test test in stringSplit)
    {
        Console.WriteLine(test.output);
    }
    using (StreamWriter sw = new StreamWriter(fs))
    {
        foreach (Test test in stringSplit)
        {
            Console.SetOut(sw); // redirect output to file
            Console.WriteLine(test.output);
        }
    }

    fs.Close();
    Console.ReadKey();

    Console.ReadLine();

}

}

public class Test
{
    public string output;
}

}

```

```

file:///C:/Users/chris/Documents/Visual S
ACC:129;20;1056, TEMP:29.00, BAT:51
ACC:125;33;1059, TEMP:29.00, BAT:51
ACC:128;31;1050, TEMP:29.50, BAT:51
ACC:125;31;1054, TEMP:29.50, BAT:51
ACC:121;28;1054, TEMP:29.50, BAT:51

```

Εικόνα 63 : Ωφέλιμη πληροφορία σε περιβάλλον DOS

	A	B	C	D	E	F	G	H
1								
2	ACC	129	20	1056	TEMP	29.00	BAT	51
3	ACC	125	33	1059	TEMP	29.00	BAT	51
4	ACC	128	31	1050	TEMP	29.50	BAT	51
5	ACC	125	31	1054	TEMP	29.50	BAT	51
6	ACC	121	28	1054	TEMP	29.50	BAT	51

Εικόνα 64 : Δεδομένα στο excel

ΚΕΦΑΛΑΙΟ 6 : Γενικά Συμπεράσματα

Συμπερασματικά αναφέρουμε ότι τα ασύρματα δίκτυα αισθητήρων αναπτύσσονται σε δυσπρόσιτα περιβάλλοντα στα οποία δεν μπορεί να πραγματοποιηθεί εύκολα συντήρηση και δεν απαιτείται η φυσική παρουσία του ανθρώπου. Επιπλέον η εξοικονόμηση ενέργειας είναι πολύ σημαντική για την απρόσκοπτη λειτουργία των ασύρματων δικτύων αισθητήρων, λόγω του ότι η ανάπτυξη των κόμβων γίνεται σε περιοχές όπου είναι αδύνατο ή αντιοικονομικό να πραγματοποιείται αντικατάσταση της πηγής ενέργειας. Στην εξοικονόμηση ενέργειας συμβάλλει επίσης ότι οι ρυθμοί μεταφοράς δεδομένων είναι χαμηλοί.

Οι κόμβοι πρέπει να είναι συσκευές χαμηλού κόστους και για να κρατηθεί χαμηλά αυτό, οι συσκευές αυτές έχουν περιορισμένες ικανότητες επεξεργασίας και αποθήκευσης δεδομένων. Αποτέλεσμα είναι τα πρωτόκολλα ασύρματων δικτύων να αποφεύγουν τις διεργασίες που απαιτούν αυξημένους πόρους, καθώς επίσης να υλοποιούν μηχανισμούς ασφάλειας με περιορισμένη επεξεργαστική ισχύ και μνήμη.

Ένα ασύρματο δίκτυο θα πρέπει να γνωρίζει τις πιθανές απειλές καθώς επίσης και τα αντίμετρα ώστε να αποφεύγει τις επιθέσεις. Οι απειλές που δέχεται ένα δίκτυο μπορούν να χωριστούν σε δύο κατηγορίες, στις επιθέσεις και στην κακή συμπεριφορά των κόμβων. Παρά την ανάπτυξη νέων μηχανισμών ασφάλειας, τα επεισόδια ασφάλειας (security incidents) δεν φαίνεται να μειώνονται, αντίθετα, νέες απειλές κάνουν την εμφάνισή τους.

Στη συνέχεια βλέπουμε ότι τα ασύρματα πρότυπα πρωτόκολλα ZigBee και 802.15.4 λειτουργούν στην παγκοσμίως ελεύθερη βιομηχανική, επιστημονική και ιατρική ζώνη (ISM band) που βρίσκεται στα 2,4 GHz. Επιπλέον το 802.15.4 λειτουργεί στις ζώνες συχνοτήτων, 868-868,6 MHz και 902-928 MHz, για τις οποίες δεν απαιτείται κάποια άδεια.

Τα προϊόντα της οικογένειας XBee είναι εύκολα στη χρήση. Δεν απαιτούν καμία ρύθμιση με αποτέλεσμα οι χρήστες να μπορούν να θέσουν το δίκτυο σε λειτουργία σε μόλις λίγα λεπτά. Οι προγραμματιζόμενες εκδόσεις της μονάδας XBee - ZB Series 2 κάνουν την προσαρμογή των εφαρμογών ZigBee ευκολότερη. Ο προγραμματισμός απευθείας πάνω στην μονάδα ZigBee εξαλείφει την ανάγκη για ένα ξεχωριστό επεξεργαστή και επίσης επειδή το ασύρματο λογισμικό είναι απομονωμένο, οι εφαρμογές μπορούν να αναπτυχθούν χωρίς κίνδυνο μέσω της μονάδος RF.

Ολοκληρώνοντας πρέπει να αναφέρουμε ότι τα ασύρματα δίκτυα αισθητήρων αποτελούν εξ' ορισμού περιβάλλον μελέτης για όλους τους τομείς της μικροηλεκτρονικής και των μικροσυστημάτων, μιας και παρουσιάζουν προοπτικές για σημαντικές εφαρμογές.

Βιβλιογραφία – Πηγές

1. Sasha Slijepcevic, Miodrag Potkonjak, Vlasios Tsiatsis, Scott Zimbeck, and Mani B.Srivastava. On communication security in wireless ad-hoc sensor networks. In WETICE, pages 139-144. IEEE Computer Society, 2002.
2. Chris Karlof and David Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks*, 1(2-3):293-315, 2003.
3. Hani Alzaid, Ernest Foo, and Juan Manuel Gonzalez Nieto. Secure data aggregation in wireless sensor network: a survey. In Ljiljana Brankovic and Mirka Miller, editors, Sixth Australasian Information Security Conference (AISC 2008), volume 81 of CRPIT, pages 93-105, Wollongong, NSW, Australia, 2008. ACS.
4. Avinash Srinivasan and Jie Wu. A survey on secure localization in wireless sensor networks, 2007.
5. Virendra Pal Singh¹, Sweta Jain² and Jyoti Singhai: Hello Flood Attack and its Countermeasures in Wireless Sensor Networks.
6. James Newsome, Elaine Shi, Dawn Xiaodong Song, and Adrian Perrig. The sybil attack in sensor networks: analysis & defenses. In Kannan Ramchandran, Janos Sztipanovits, Jennifer C. Hou, and Thrasyvoulos N. Pappas, editors, IPSN, pages 259- 268. ACM, 2004.
7. Security and Privacy in Sensor Networks, Howen Chan & Andrian Perrig, October 2003.
8. Geoff Werner-Allen, Konrad Lorincz, Jeff Johnson, Jonathan Lees, and Matt Welsh: Fidelity and Yield in a Volcano Monitoring Sensor Network.
9. Rajeev Piyare, Seong-ro Lee, Performance Analysis of XBee ZB Module Based Wireless Sensor Networks, Mokpo National University April-2013.
10. Howen Chan & Andrian Perrig, Security and Privacy in Sensor Networks, October 2003.
11. <http://www.libelium.com/>
12. http://www.digi.com/pdf/wp_zigbee.pdf
13. www.atmel.com
14. <http://www.daintree.net/>
15. <http://www.wsn-security.info>
16. Lejla Batina, Nele Mentens, Kazuo Sakiyama, Bart Preneel, and Ingrid Verbauwhede. Low-cost elliptic curve cryptography for wireless sensor networks. In Buttyan et al.
17. Chris Karlof, Naveen Sastry, and David Wagner. Tinysec: a link layer security architecture for wireless sensor networks. In John A. Stankovic, Anish Arora, and Ramesh Govindan, editors, SenSys, pages 162-175. ACM, 2004.
18. H. Ozgur Sanli, Suat Ozdemir, and Hassan Cam. SRDA: Secure Reference-Based Data Aggregation Protocol for Wireless Sensor Networks. In VTC2004-Fall, pages 4650- 4654, 2004.
19. Baruch Awerbuch, David Holmer, Cristina Nita-Rotaru, and Herbert Rubens. An on-demand secure routing protocol resilient to byzantine failures. In W. Douglas Maughan and Nitin H. Vaidya, editors, Workshop on Wireless Security, pages 21-30. ACM, 2002.

20. Weichao Wang, Bharat K. Bhargava, Yi Lu, and Xiaoxin Wu. Defending against wormhole attacks in mobile ad hoc networks. *Wireless Communications and Mobile Computing*, 6:483-503, 2006.
21. Jonathan M. McCune, Elaine Shi, Adrian Perrig, and Michael K. Reiter. Detection of denial-of-message attacks on sensor network broadcasts. In *IEEE Symposium on Security and Privacy* [138], pages 64-78.
22. Laurent Eschenauer and Virgil D. Gligor. A key-management scheme for distributed sensor networks. In Vijayalakshmi Atluri, editor, *ACM Conference on Computer and Communications Security*, pages 41-47. ACM, 2002.
23. Naveen Sastry, Umesh Shankar, and David Wagner. Secure verification of location claims. In Maughan and Perrig [130], pages 1-10.