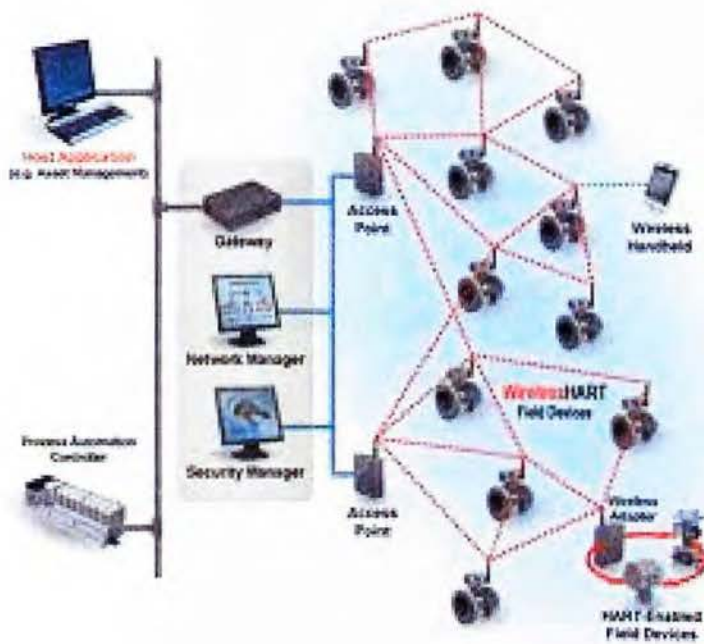


**Α.Τ.Ε.Ι. ΠΕΙΡΑΙΑ**  
**ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ**  
**ΤΜΗΜΑ ΑΥΤΟΜΑΤΙΣΜΟΥ**

**“Ασύρματα Δίκτυα στο Βιομηχανικό Αυτοματισμό”**



Επιβλέπων Καθηγητής: Αγγελόπουλος Ιωάννης

Σπουδαστής: Σφήκας Κωνσταντίνος

ΑΜ: 29551



Πειραιάς, Ιανουάριος 2012

Η σελίδα αυτή είναι σκόπιμα λευκή.

## **ΕΥΧΑΡΙΣΤΙΕΣ**

Θα ήθελα να ευχαριστήσω όσους έκαναν υπομονή και όσους με βοήθησαν ώστε να πραγματοποιηθεί αυτή η εργασία. Επίσης, θα ήθελα να ευχαριστήσω τον κ. Αγγελόπουλο Ιωάννη για την κατανόηση που έδειξε κατά τη συγγραφή αυτής της εργασίας.

Σφήκας Κωνσταντίνος

## ΠΕΡΙΕΧΟΜΕΝΑ

Ευχαριστίες.....	i
Περιεχόμενα.....	ii
Λίστα Εικόνων.....	iv
Λίστα Πινάκων.....	vii
Πρόλογος.....	viii
<b>1<sup>ο</sup> - Κεφάλαιο “Εισαγωγή”.....</b>	<b>1</b>
1.1 Ιστορική Αναδρομή στο Βιομηχανικό Αυτοματισμό.....	1
1.2 Σκοπός της Εργασίας.....	3
<b>2<sup>ο</sup> - Κεφάλαιο “Ασύρματη Επικοινωνία στο Βιομηχανικό Αυτοματισμό ”.....</b>	<b>4</b>
2.1 Εισαγωγή.....	4
2.2 Ανάγκες Βιομηχανικού Αυτοματισμού.....	4
2.3 Μειονεκτήματα Ενσύρματης Επικοινωνίας.....	7
2.4 Πλεονεκτήματα Ασύρματης Επικοινωνίας.....	8
2.5 Χρήση Ασύρματης τεχνολογίας.....	9
2.6 Τοπολογίες Ασύρματων Δικτύων.....	10
2.6.1 Τοπολογία Αστέρα.....	11
2.6.2 Τοπολογία Δέντρου.....	12
2.6.3 Τοπολογία Πλέγματος.....	13
2.7 Διάκριση Ασύρματων Δικτύων.....	15
2.7.1 Ασύρματα τοπικά δίκτυα WLAN.....	15
2.7.2 Ασύρματο Μητροπολιτικό Δίκτυο WMAN.....	17
2.7.3 Ασύρματο Προσωπικό Δίκτυο Περιοχής WPAN.....	20
2.8 Σύγκριση Ασύρματης και Ενσύρματης Τεχνολογίας.....	22
<b>3<sup>ο</sup> - Κεφάλαιο “Ασύρματα Δίκτυα Αισθητήρων στο Βιομηχανικό Αυτοματισμό ”.....</b>	<b>26</b>
3.1 Εισαγωγή.....	26
3.2 Βασικά Χαρακτηριστικά ενός Ασύρματου Δικτύου Αισθητήρων.....	27
3.3 Παράμετροι Σχεδίασης και Αρχιτεκτονικής Ασύρματων Δικτύων Αισθητήρων στο Βιομηχανικό Αυτοματισμό.....	28
3.3.1 Απόδοση και Ποιότητα Παροχής Υπηρεσιών.....	29
3.3.2 Ισχύς Λειτουργίας.....	34
3.3.3 Μεταβλητότητα και Επεκτασιμότητα.....	34
3.3.4 Τοπολογία.....	35



3.3.5	Ασύρματη Εκπομπή.....	35
3.3.6	Σύστημα και Λογισμικό (Software) .....	36
3.4	Παράδειγμα Χρήσης ενός Ασύρματου Δικτύου Αισθητήρων στο Βιομηχανικό Αυτοματισμό.....	38
<b>4°</b>	<b>- Κεφάλαιο “Πρωτόκολλα Ασύρματης Δικτύωσης στο Βιομηχανικό Αυτοματισμό”</b>	<b>41</b>
4.1	Ad-hoc Δίκτυα στο Βιομηχανικό Αυτοματισμό.....	41
4.2	Wi-Fi.....	44
4.2.1	Εφαρμογές του Wi-Fi στο Βιομηχανικό Αυτοματισμό και Οφέλη από τη χρήση του....	45
4.3	Bluetooth.....	47
4.3.1	Αρχιτεκτονική Bluetooth.....	47
4.3.2	Τεχνικά Χαρακτηριστικά του Bluetooth .....	50
4.3.3	Ασφάλεια Συστημάτων με Bluetooth .....	51
4.3.4	Τεχνικές για την Αξιοποίηση των Δυνατοτήτων του Bluetooth στις Βιομηχανικές Επικοινωνίες.....	53
4.3.5	Εφαρμογές του Bluetooth στο Βιομηχανικό Αυτοματισμό και Οφέλη από τη χρήση του	56
4.4	ZigBee.....	57
4.4.1	Αρχιτεκτονική ZigBee.....	58
4.4.2	Τεχνικά Χαρακτηριστικά του ZigBee .....	60
4.4.3	Ασφάλεια Συστημάτων με ZigBee .....	62
4.4.4	Εφαρμογές του ZigBee στο Βιομηχανικό Αυτοματισμό και οφέλη από τη χρήση του ..	63
4.5	Wireless Hart .....	66
4.5.1	Αρχιτεκτονική του Wireless Hart.....	67
4.5.2	Τεχνικά Χαρακτηριστικά του Wireless Hart.....	71
4.5.3	Ασφάλεια Συστημάτων με Wireless Hart.....	733
<b>5°</b>	<b>- Κεφάλαιο “Σύγκριση Πρωτοκόλλων Ασύρματης Δικτύωσης”</b> .....	<b>766</b>
<b>6°</b>	<b>- Κεφάλαιο “Σύνοψη - Συμπεράσματα ”</b> .....	<b>800</b>
	<b>Αναφορές - Βιβλιογραφία.....</b>	<b>833</b>

## ΛΙΣΤΑ ΕΙΚΟΝΩΝ

Εικόνα 1 – Τοπολογία Αστέρα για ασύρματα δίκτυα. [2].....	11
Εικόνα 2 – Τοπολογία Δέντρου για ασύρματα δίκτυα. [2].....	13
Εικόνα 3 – Τοπολογία πλέγματος για ασύρματα δίκτυα. [2] .....	14
Εικόνα 4 – Γενική Μορφή δικτύου WLAN. [3].....	16
Εικόνα 5 – Τυπικό παράδειγμα δικτύου WMAN. [4] .....	18
Εικόνα 6 – Τυπική μορφή ασύρματου δικτύου που βασίζεται στην τεχνική WiMax. [3] .....	19
Εικόνα 7 – Παράδειγμα σύγκρισης ενός ενσύρματου με ένα ασύρματο δίκτυο. [9] .....	24
Εικόνα 8 – Ασύρματο δίκτυο Αισθητήρων. [12].....	27
Εικόνα 9 – Διαφορετικοί τύποι επιθέσεων σε WSN δίκτυα.....	30
Εικόνα 10 – Η έννοια του Timeliness και του Jitter. [3] .....	32
Εικόνα 11 – Διεργασίες στον ατμολέβητα και λήψη μετρήσεων. [14] .....	39
Εικόνα 12 – Το WSN δίκτυο και οι αισθητήρες που χρησιμοποιούνται για την παρακολούθηση της θερμοκρασίας και της πίεσης του ατμολέβητα. [14] .....	40
Εικόνα 13 – Παράδειγμα ενός βιομηχανικού δικτύου ad-hoc. [16] .....	41
Εικόνα 14 – Οι διαμορφώσεις IBSS (independent basic service set) και ESS (extended service set) ενός Wi-Fi δικτύου. [18].....	44
Εικόνα 15 – Συσσκευή βιομηχανικού Wi-Fi Ethernet. [31] .....	46
Εικόνα 16 – Αρχιτεκτονική master/slave για το Bluetooth. [20] .....	47
Εικόνα 17 – Scatternet το οποίο προκύπτει από επικάλυψη πολλών piconets. [20] .....	48
Εικόνα 18 – Γενική μορφή της αρχιτεκτονικής της στοίβας (stack) στο Bluetooth. [20] .....	49
Εικόνα 19 – Απλοποιημένο chip GFSK διαμόρφωσης. [20].....	50
Εικόνα 20 – Τυπικό σχήμα ελέγχου για καταναμημένα συστήματα ελέγχου διεργασιών (distributed process control systems – DPCSs). [21].....	54
Εικόνα 21 – Πρόγραμμα μεταδόσεων ενός piconet που υποστηρίζει το σχήμα ελέγχου της εικόνας 18. [21].....	54
Εικόνα 22 - Ελεγκτής (controller) με ενσωματωμένο Bluetooth. [29].....	57
Εικόνα 23 – Τοπολογίες και κατηγορίες κόμβων στο πρότυπο IEEE 802.15.4. [20] .....	58
Εικόνα 24 – Τοπολογία πλέγματος. [20] .....	59
Εικόνα 25 – Κατανομή καναλιών σε διαφορετικές χώρες. [20].....	59
Εικόνα 26 – Ανταγωνισμός και τυχαία πρόσβαση. [20] .....	60

Εικόνα 27 – Παρακολούθηση προσωπικού σε ένα κτήριο γραφείων με ZigBee ασύρματη δικτύωση. [23] .....	64
Εικόνα 28 – Ασύρματη ZigBee συσκευή. [32].....	65
Εικόνα 29 – Hart σηματοδότη (αναλογική και ψηφιακή). [24] .....	66
Εικόνα 30 – Αρχιτεκτονική ενός Wireless Hart δικτύου. [24] .....	67
Εικόνα 31 – Αρχιτεκτονική του Wireless Hart. [25] .....	68
Εικόνα 32 – Αρχιτεκτονική του επίπεδου ζεύξης δεδομένων (data link layer). [25].....	70
Εικόνα 33 – Wireless Hart πομπός για τη μέτρηση της θερμοκρασίας. [34] .....	755

## ΛΙΣΤΑ ΠΙΝΑΚΩΝ

Πίνακας 1 – Συχνότητες που χρησιμοποιούνται για την ασύρματη επικοινωνία στο βιομηχανικό περιβάλλον. [3] .....	36
Πίνακας 2 – Τεχνικά χαρακτηριστικά του Wi-Fi. [18].....	45
Πίνακας 3 – Τεχνικά χαρακτηριστικά του Bluetooth. [18] .....	51
Πίνακας 4 – Τεχνικά χαρακτηριστικά του ZigBee. [18] .....	62
Πίνακας 5 – Τεχνικά χαρακτηριστικά του Wireless Hart. [25], [26] .....	73
Πίνακας 6 – Συγκριτικός πίνακας Wi-Fi, Bluetooth, ZigBee και Wireless Hart. ....	77

## ΠΡΟΛΟΓΟΣ

Κάθε εξέλιξη και πρόοδος που παρατηρείται στα τεχνολογικά χαρακτηριστικά των ηλεκτρονικών υπολογιστών, έχει άμεσο αντίκτυπο στην ανάπτυξη και τη βελτιστοποίηση των αντίστοιχων πληροφοριακών συστημάτων τα οποία αποτελούν στις μέρες μας βασικό κινητήριο μοχλό πολλών εφαρμογών. Η ραγδαία εξέλιξη και η αύξηση των τομέων στους οποίους βρίσκουν εφαρμογή, κατέστησε τα πληροφοριακά συστήματα αναπόσπαστο κομμάτι και του βιομηχανικού αυτοματισμού. Αρχικά προσέφεραν βελτίωση του τρόπου ελέγχου των επιμέρους διαδικασιών, αυξάνοντας το ρυθμό και την ποσότητα της παραγωγής και καθιέρωσαν ένα συγκεντρωτικό τρόπο ελέγχου των επιμέρους συστημάτων. Η ταχύτατη ανάπτυξη της τεχνολογίας σε συνδυασμό με την ταυτόχρονη αύξηση των απαιτήσεων των συστημάτων βιομηχανικού αυτοματισμού οδήγησαν στην ανάγκη ύπαρξης τόσο νεότερων πιο σύγχρονων πληροφοριακών συστημάτων, όσο και νέων καινοτόμων τρόπων επικοινωνίας των επιμέρους συστημάτων μεταξύ τους. Οι ανάγκες της σύγχρονης εποχής έχουν οδηγήσει στη χρησιμοποίηση ασύρματων δικτύων και στο βιομηχανικό αυτοματισμό. Επιπρόσθετα για την καλύτερη και κατά το δυνατόν ποιοτικότερη επικοινωνία μεταξύ των επιμέρους συστημάτων κρίθηκε απαραίτητη η χρήση κατάλληλων πρωτοκόλλων ασύρματης δικτύωσης.

Στο πρώτο κεφάλαιο της παρούσας πτυχιακής εργασίας πραγματοποιείται μία ιστορική αναδρομή στο βιομηχανικό αυτοματισμό με παράλληλη αναφορά των σκοπών και των στόχων της παρούσας μελέτης.

Στο δεύτερο κεφάλαιο της εργασίας γίνεται εκτενής αναφορά στη χρήση ασύρματης επικοινωνίας, για την κάλυψη των αναγκών των βιομηχανικών συστημάτων αυτοματισμού. Κατόπιν, πραγματοποιείται αναφορά στις ανάγκες των σύγχρονων συστημάτων του βιομηχανικού αυτοματισμού με αναφορά στα μειονεκτήματα που παρουσιάζει η ενσύρματη επικοινωνία αλλά και στα πλεονεκτήματα που παρουσιάζει η ασύρματη επικοινωνία και οδήγησαν στην καθιέρωση της. Παρουσιάζονται οι κυριότερες τοπολογίες ασύρματων δικτύων και οι τρόποι διάκρισης αυτών των δικτύων μεταξύ τους. Στο τέλος του κεφαλαίου πραγματοποιείται σύγκριση της ασύρματης με την ενσύρματη τεχνολογία.

Στο τρίτο κεφάλαιο της εργασίας παρουσιάζονται τα ασύρματα δίκτυα αισθητήρων. Πραγματοποιείται εκτενής αναφορά και παρουσίαση της αρχιτεκτονικής τους, των

τεχνολογικών τους χαρακτηριστικών και των σημαντικότερων εφαρμογών στις οποίες χρησιμοποιούνται. Αναφέρονται επίσης οι βασικότεροι παράμετροι σχεδίασης αυτών.

Στο κεφάλαιο τέσσερα παρουσιάζουμε τα κυριότερα πρωτόκολλα ασύρματης δικτύωσης. Η αρχή γίνεται με τη συνοπτική παρουσίαση του, Wi-Fi το οποίο βασίζεται στο IEEE 802.11. Πραγματοποιούμε αναφορά στην εξελικτική πορεία και στην αρχιτεκτονική του IEEE 802.11. Στη συνέχεια ακολουθεί παρουσίαση των επιπέδων και των εφαρμογών του Wi-Fi, καθώς και της ασφάλειας που παρέχουν τα συστήματα που χρησιμοποιούν Wi-Fi. Αμέσως μετά πραγματοποιούμε εκτενή αναφορά στο Bluetooth παρουσιάζοντας την αρχιτεκτονική του και τις διαφορετικές εκδόσεις του. Αναφερόμαστε στα επίπεδα από τα οποία αποτελείται, στην ασφάλεια που παρέχουν τα συστήματα με Bluetooth και στις κυριότερες εφαρμογές στις οποίες το συναντάμε. Η συνέχεια στις αναφορές μας στα πρωτόκολλα ασύρματης δικτύωσης πραγματοποιείται με το ZigBee. Παρουσιάζουμε την αρχιτεκτονική του, τα επίπεδα από τα οποία αποτελείται και τη δομή των πλαισίων του. Εκθέτουμε την ασφάλεια που παρέχουν τα συστήματα στα οποία χρησιμοποιείται το ZigBee και τις κυριότερες εφαρμογές στις οποίες χρησιμοποιείται το συγκεκριμένο πρωτόκολλο. Κλείνοντας την αναφορά μας στα πρωτόκολλα ασύρματης δικτύωσης παρουσιάζουμε το Wireless Hart. Αναφερόμαστε στα βασικά του χαρακτηριστικά, στους ενδιάμεσους κόμβους από τους οποίους αποτελείται και στην αρχιτεκτονική του. Παρουσιάζουμε τα επίπεδα που το συγκροτούν, την ασφάλεια που παρέχει και τις βασικότερες εφαρμογές στις οποίες χρησιμοποιείται.

Στο πέμπτο κεφάλαιο συγκρίνουμε τα πρωτόκολλα ασύρματης δικτύωσης που παρουσιάσαμε στο κεφάλαιο τέσσερα με βάση τα κυριότερα τεχνικά τους χαρακτηριστικά και τις σημαντικότερες τους εφαρμογές. Παρουσιάζουμε τα πλεονεκτήματα και τα μειονεκτήματα που εμφανίζει το κάθε ένα από αυτά.

Στο έκτο και τελευταίο της πτυχιακής εργασίας παρουσιάζουμε τα συμπεράσματα μας τα οποία συνοψίζουν τη συνολική μελέτη και έρευνα στα ασύρματα δίκτυα που χρησιμοποιούνται στο βιομηχανικό αυτοματισμό.

**Λέξεις κλειδιά:** Ασύρματα δίκτυα, Πρωτόκολλα ασύρματης δικτύωσης, Wi-Fi, Bluetooth, ZigBee, Wireless Hart.



# 1<sup>ο</sup> - ΚΕΦΑΛΑΙΟ

## “ΕΙΣΑΓΩΓΗ”

### 1.1 Ιστορική Αναδρομή στο Βιομηχανικό Αυτοματισμό

Τα σύγχρονα συστήματα που χρησιμοποιούνται στο βιομηχανικό αυτοματισμό αποτελούνται από επιμέρους ψηφιακές υπομονάδες οι οποίες συνδέονται μεταξύ τους με τη βοήθεια κατάλληλων δικτύων επικοινωνίας, τα οποία είναι αρμόδια για τη συλλογή των δεδομένων και την εκτέλεση ενδιάμεσων ελεγκτικών λειτουργιών. Στα σύγχρονα συστήματα του βιομηχανικού αυτοματισμού ο τρόπος επικοινωνίας και ανταλλαγής πληροφοριών έχει στις μέρες μας ιδιαίτερη σημασία. Για να μπορούν να επικοινωνούν όλες οι συσκευές μεταξύ τους άριστα χρησιμοποιείται ένα σύνολο από πρότυπα επικοινωνίας. Αυτά τα πρότυπα στις μέρες μας ονομάζονται πρωτόκολλα επικοινωνίας και χρησιμοποιούνται ευρύτερα ώστε να λύσουν αποτελεσματικά όσα προβλήματα προκύπτουν κατά την επικοινωνία των διαφόρων συσκευών αυτοματισμού μεταξύ τους.

Στις αρχές του 20<sup>ου</sup> αιώνα τα κατασκευαστικά και ελεγκτικά βιομηχανικά συστήματα δημιουργούνταν με τη βοήθεια αναλογικών συσκευών και με χρήση μηχανικών τεχνικών. Μετέπειτα χρησιμοποιήθηκαν υδραυλικά συστήματα, αλλά και συστήματα που παρείχαν δυνατότητα έλεγχου εξ αποστάσεως από μία κατάλληλη κεντρική ελεγκτική μονάδα. Κατά τη δεκαετία του 50 ενισχύθηκε η χρήση τέτοιων συστημάτων απομακρυσμένου ελέγχου και διαχείρισης εξαιτίας της ραγδαίας ανάπτυξης των ηλεκτρονικών και ψηφιακών ελεγκτικών συστημάτων, τα οποία έβρισκαν χρήση στις επικοινωνίες μακρινών αποστάσεων. Ταυτόχρονα τα βιομηχανικά συστήματα επικοινωνίας άρχιζαν να βρίσκουν όλο και πιο πολλές εφαρμογές, κάνοντας χρήση αναλογικών σημάτων και διεκπεραιώνοντας συνδέσεις μεταξύ ενός κεντρικού επεξεργαστή, των περιφερειακών και των τερματικών συσκευών. Στις αρχές της δεκαετίας του 60 ο ρόλος του ψηφιακού ελεγκτή ανατέθηκε σε ένα κεντρικό υπολογιστή, ο οποίος είχε ως αρμοδιότητα των άμεσο έλεγχου κάθε διεργασίας. Βέβαια εκείνη την εποχή η χρήση υπολογιστή οδηγούσε και σε μεγάλο οικονομικό κόστος. Παράλληλα εξελίχθηκαν σημαντικά οι Προγραμματιζόμενοι Λογικοί Ελεγκτές (Programmable Logic Controllers – PLC), οι οποίοι αντικατέστησαν σταδιακά το ρελέ που χρησιμοποιούταν παλιότερα στα συστήματα αυτοματισμού. Προς το τέλος της δεκαετίας η Αγγλική εταιρία Molins παρουσίασε το «Σύστημα 24», το οποίο παρείχε δυνατότητα ελέγχου

και διαχείρισης πολλαπλών συσκευών μέσω ενός κεντρικού υπολογιστή. Αυτό είχε ως αποτέλεσμα την επιτάχυνση των επιμέρους διαδικασιών και την αύξηση της παραγωγικότητας, αφού βελτιώθηκε ο τρόπος χρήσης και αξιοποίησης των επιμέρους συσκευών. Μετέπειτα έγιναν προσπάθειες για ενοποίηση όλων των βιομηχανικών διαδικασιών ελέγχου και παρακολούθησης σε κάθε κομμάτι της παραγωγής, με απώτερο σκοπό τη διεκπεραίωση αυτών από ένα κεντρικό ψηφιακό υπολογιστή. Αυτό είχε ως άμεση συνέπεια την ανάγκη εύρεσης και ανάπτυξης εξειδικευμένων πρωτοκόλλων επικοινωνίας για την καλύτερη και αποτελεσματικότερη επικοινωνία των επιμέρους συσκευών μεταξύ τους. Στα μέσα της δεκαετίας του 70 παρουσιάστηκε από την εταιρία Honeywell το πρώτο κατανεμημένο υπολογιστικό σύστημα. Έκτοτε η ιδέα πανομοιότυπων συστημάτων χρησιμοποιήθηκε ευρύτερα σε συστήματα βιομηχανικού αυτοματισμού.

Η περαιτέρω εξέλιξη των συστημάτων βιομηχανικού αυτοματισμού, η καθιέρωση της χρήσης τους και η αύξηση τόσο του πλήθους τους όσο και της πολυπλοκότητας τους, οδήγησε στην ανάγκη κατάργησης των καλωδίων ως μέσα διασύνδεσης και επικοινωνίας αυτών και έδωσε ώθηση προς την ασύρματη δικτύωση. Το πρώτο βήμα προς αυτή την κατεύθυνση πραγματοποιήθηκε στις αρχές της δεκαετίας του 80, όπου ασύρματα δίκτυα έκαναν την εμφάνισή τους αρχικά σε εφαρμογές γραφείου και έπειτα σε μεγαλύτερο πλήθος εφαρμογών. Στη συνέχεια πραγματοποιήθηκαν ακόμα περισσότερα βήματα προς την εξέλιξη των ασύρματων επικοινωνιών, αλλά και τη χρήση κατάλληλων και αποτελεσματικών πρωτοκόλλων ασύρματης δικτύωσης. Στις μέρες μας η ασύρματη δικτύωση έχει αποκτήσει χαρακτηριστικά εφάμιλλά, ή και καλύτερα, σε σχέση με την ενσύρματη δικτύωση, και, σε πολλές εφαρμογές, τείνει να αντικαταστήσει την ενσύρματη επικοινωνία. Τα Τοπικά Ασύρματα Δίκτυα (Wireless Local Area Networks – WLAN), τα Μητροπολιτικά Ασύρματα Δίκτυα (Wireless Metropolitan Area Networks – WMAN), τα Ευρείας Περιοχής Ασύρματα Δίκτυα (Wireless Wide Area Networks – WWAN) και τα Ασύρματα Δίκτυα Αισθητήρων (Wireless Sensor Networks – WSN) αποτελούν τις βασικότερες κατηγορίες ασύρματων δικτύων που χρησιμοποιούνται στις μέρες μας. [11]



## 1.2 Σκοπός της Εργασίας

Η ασύρματη επικοινωνία των συστημάτων αυτοματισμού είναι αναμφίβολα μια ιδιαίτερα μεγάλη πρόκληση για τη βιομηχανία του 21<sup>ου</sup> αιώνα. Στην παρούσα πτυχιακή εργασία θα παρουσιάσουμε όλες εκείνες τις ανάγκες που υπάρχουν στα σύγχρονα συστήματα του βιομηχανικού αυτοματισμού και οδηγούν στη χρήση ασύρματης δικτύωσης, με αναφορά στα πλεονεκτήματα που αυτή προσφέρει. Θα πραγματοποιηθεί παρουσίαση των βασικότερων τοπολογιών ασύρματων δικτύων αλλά και του τρόπου διάκρισης των ασύρματων δικτύων σε επιμέρους κατηγορίες. Στη συνέχεια θα ακολουθήσει σύγκριση της ασύρματης με την ενσύρματη τεχνολογία.

Ξεχωριστή αναφορά θα πραγματοποιηθεί στα ασύρματα δίκτυα αισθητήρων δίνοντας βάση στην αρχιτεκτονική τους, τα τεχνολογικά τους χαρακτηριστικά και στις κυριότερες εφαρμογές στις οποίες βρίσκουν χρήση. Θα παρουσιαστούν οι βασικότερες παράμετροι που καθορίζουν τον τρόπο σχεδίασης αυτών των δικτύων όπως είναι η απόδοση και η ποιότητα των υπηρεσιών που παρέχουν, η ισχύς λειτουργίας τους, η μεταβλητότητα και η επεκτασιμότητα τους, καθώς και η τοπολογία τους.

Το μεγαλύτερο μέρος της εργασίας μας αναλώνεται στην αναλυτική παρουσίαση των κυριότερων πρωτοκόλλων ασύρματης δικτύωσης, όπως είναι το Wi-Fi, το Bluetooth, το ZigBee και το Wireless Hart. Για κάθε ένα από τα παραπάνω πρωτόκολλα πραγματοποιείται παρουσίαση των ιδιαίτερων χαρακτηριστικών, της αρχιτεκτονικής, των επιπέδων από τα οποία αποτελούνται, της ασφάλειας που παρέχουν και των βασικότερων εφαρμογών στις οποίες βρίσκουν χρήση. Αμέσως μετά θα ακολουθήσει σύγκριση των πρωτοκόλλων ασύρματης δικτύωσης που παρουσιάστηκαν, με βάση τα πλεονεκτήματα και τα μειονεκτήματα του καθενός.

## 2<sup>ο</sup> - ΚΕΦΑΛΑΙΟ

### “ΑΣΥΡΜΑΤΗ ΕΠΙΚΟΙΝΩΝΙΑ ΣΤΟ ΒΙΟΜΗΧΑΝΙΚΟ ΑΥΤΟΜΑΤΙΣΜΟ ”

#### 2.1 Εισαγωγή

Σε κάθε εποχή αλλά και σε όλο το φάσμα του βιομηχανικού αυτοματισμού το κυρίαρχο ζητούμενο ήταν η βελτίωση των επιμέρους διαδικασιών με απώτερο στόχο τη βελτιστοποίηση της ποιότητας, της ποσότητας και της ταχύτητας της συνολικής παραγωγικής διαδικασίας. Για το σκοπό αυτό καταβάλλονταν προσπάθειες ανά τις δεκαετίες, ώστε η ανταλλαγή και η διαχείριση πληροφοριών μεταξύ των επιμέρους συστημάτων να είναι κατά το δυνατόν ασφαλέστερη και ταχύτερη. Καίρια λύση σε αυτή την πρόκληση μπορεί να προσφέρει η ασύρματη τεχνολογία, η οποία είναι εφικτό να παρέχει οικονομικές, αποτελεσματικές και ολοκληρωμένες υπηρεσίες στην απόκτηση, ανταλλαγή και διαχείριση πληροφοριών σε μία ολόκληρη βιομηχανική εγκατάσταση. Ο παγκόσμιος ανταγωνισμός ωθεί τη βιομηχανία σε συνεχή βελτίωση των λειτουργικών της διεργασιών, σε συνεχή βελτίωση της ποιότητας των παραγόμενων προϊόντων με ταυτόχρονη αύξηση της παραγωγικότητας, αύξηση της αξιοπιστίας και συμμόρφωση με τους νέους κανονισμούς. Τα ασύρματα δίκτυα στη συνολική παραγωγική διαδικασία παρέχουν τη δυνατότητα συγκέντρωσης περισσότερων δεδομένων και πληροφοριών από τις επιμέρους διαδικασίες με μεγαλύτερη ταχύτητα. Επίσης τα ασύρματα δίκτυα χαρακτηρίζονται από ευκολία συντήρησης, αποτελεσματικότητα και χαμηλό κόστος, εξαλείφοντας παράλληλα τα προβλήματα που σχετίζονται με τα ενσύρματα δίκτυα. [1]

#### 2.2 Ανάγκες Βιομηχανικού Αυτοματισμού

Ο βιομηχανικός αυτοματισμός αποτελεί ένα δύσκολο πεδίο όσον αφορά την εισαγωγή οποιασδήποτε νέας τεχνολογίας. Ο ρυθμός με τον οποίο απορροφάται κάθε νέα τεχνολογία στη βιομηχανία είναι σχετικά αργός. Ακόμα και όταν η νέα τεχνολογία εφαρμόζεται πλήρως, υπάρχει σοβαρή πιθανότητα να προκύψουν προβλήματα τα οποία θα έχουν σχέση με τις ιδιαιτερότητες του βιομηχανικού περιβάλλοντος και θα πρέπει στην πορεία να ξεπεραστούν. Στον κλάδο του βιομηχανικού αυτοματισμού οι κυριότερες απαιτήσεις που πρέπει να

καλύπτει ένα νέο είδος τεχνολογίας ώστε να είναι εφικτό να χρησιμοποιηθεί με επιτυχία είναι:

- **Αντοχή στο Βιομηχανικό Περιβάλλον.** Ο βιομηχανικός αυτοματισμός αποτελείται από δύο βασικές κατηγορίες: Τον αυτοματισμό των εργοστασίων(factory automation) και τον αυτοματισμό των διεργασιών(process automation).

Ο αυτοματισμός των εργοστασίων περιλαμβάνει συνήθως μηχανουργεία στα οποία πραγματοποιείται η κατεργασία μετάλλων και λοιπών υλικών, τα οποία χρησιμοποιούνται για την κατασκευή των προϊόντων, και γραμμές συναρμολόγησης, όπου από τα επιμέρους μέρη κατασκευάζονται τα τελικά προϊόντα. Ως αυτοματισμός εργοστασίων λογίζονται οι μηχανές κατεργασίας (π.χ CNC εργαλειομηχανές), συναρμολόγησης (ρομποτικά συστήματα), ταξινόμησης, ποιοτικού ελέγχου (π.χ. οπτικός έλεγχος), μέτρησης (π.χ ζυγιστικές, μετρητικές μηχανές), διαλογής (π.χ. διαχωρισμός μεγεθών, χρωμάτων, υλικών), μεταφοράς ( π.χ ιμάντες μεταφοράς) και αποθήκευσης. Στις βιομηχανίες συνήθως το περιβάλλον συνήθως υπάρχει ελλιπής καθαριότητα, σκόνη, λάδια, καύσιμα, θόρυβοι και δονήσεις. Επίσης στις βιομηχανίες, ο πιο έντονος θόρυβος είναι ο «ηλεκτρικός» θόρυβος που προκαλείται από τους ηλεκτροκινητήρες, που χρησιμοποιούνται σε ευρύτατα για τη λειτουργία των μηχανών. Η θερμοκρασία, αν και είναι συχνά ανεξέλεγκτη, συνήθως έχει τιμές που καθιστούν εφικτή την ανθρώπινη παρουσία. Όσον αφορά το πάτωμα του εργοστασίου αυτό είναι συνήθως στεγνό, καθώς το σύνολο του εξοπλισμού βρίσκεται σε στεγασμένο χώρο.

Αντίθετα ο αυτοματισμός των διεργασιών χρησιμοποιείται συχνά σε υπαίθριες μονάδες και η γραμμή παραγωγής δεν είναι ορατή από το χειριστή της μονάδας. Αυτό συμβαίνει διότι η γραμμή παραγωγής βρίσκεται συνήθως στο εσωτερικό σωληνώσεων ή δεξαμενών ή αντιδραστήρων. Τα προϊόντα και οι πρώτες ύλες αυτών των μονάδων είναι συνήθως υγρά. Συχνά, τόσο τα τελικά προϊόντα όσο και τα ενδιάμεσα προϊόντα είναι πτητικά και μερικές φορές εύφλεκτα ή δηλητηριώδη για τον άνθρωπο. Στις περισσότερες περιπτώσεις τα υγρά είναι και διαβρωτικά. Και σε αυτή την περίπτωση ο «ηλεκτρικός» θόρυβος είναι αρκετά έντονος εξαιτίας των ηλεκτροκινητήρων που χρησιμοποιούνται για την κίνηση των αντλιών και των αναδευτήρων(mixer). Η θερμοκρασία είναι συχνά ανεξέλεγκτη στο σύνολο της μονάδας, αν εξαιρέσουμε ορισμένα σημεία που ονομάζονται δωμάτια ελέγχου (control rooms) και προορίζονται για ανθρώπινη παρουσία. Η περιοχή των

διεργασιών είναι συνήθως εκτεθειμένη σε όλους τους τύπους των καιρικών συνθηκών συμπεριλαμβανομένης της βροχής, του χιονιού, του πάγου, του άνεμου και της ηλιακής ακτινοβολίας.

- **Ασφάλεια.** Η ασφάλεια ενός δικτύου βιομηχανικού αυτοματισμού αφορά την αποτροπή πιθανής καταστροφίας, δολιοφθοράς ή επίθεσης. Για την αποτροπή όλων αυτών, πρέπει να εξαλειφθεί ο κίνδυνος που μπορεί να προκαλέσει κάθε εξωτερική πηγή. Η δουλειά ενός δικτύου βιομηχανικού αυτοματισμού είναι να λειτουργεί συνεχώς, να διαχειρίζεται και να ανταλλάσσει δεδομένα. Ο βασικός στόχος ενός δικτύου βιομηχανικού αυτοματισμού είναι η εξασφάλιση τόσο της ασφάλειας των διεργασιών όσο και της ανθρώπινης ασφάλειας. Με τον όρο ασφάλεια πολλοί υπονοούν την προστασία δεδομένων και την αξιοπιστία, ωστόσο πρόκειται για διαφορετικές έννοιες.
- **Προστασία Δεδομένων.** Η προστασία δεδομένων σχετίζεται με την υφαρπαγή δεδομένων του δικτύου από τρίτους. Στην ουσία αφορά τον αποκλεισμό ανεπιθύμητων εισβολέων, με στόχο να μην τους επιτρέπεται η πρόσβαση στα δεδομένα του δικτύου. Αν η προστασία του δικτύου αποτρέπει κάθε μη εξουσιοδοτημένη εισβολή, τότε έχει κάνει σωστά τη δουλειά της. Ακόμα όμως και αν εάν ένα δίκτυο προστατεύεται επαρκώς από εξωτερικές εισβολές, θα πρέπει να προστατεύεται και από μη εξουσιοδοτημένους χρήστες εντός του δικτύου. Συνήθως η πληροφορική τεχνολογία επιτρέπει στους υπαλλήλους μίας επιχείρησης να έχουν πρόσβαση μόνο σε προκαθορισμένες περιοχές δεδομένων.
- **Αξιοπιστία.** Πιθανή βλάβη του δικτύου οδηγεί σε βλάβη του συστήματος αυτοματισμού, από το οποίο καθορίζεται η διαδικασία ελέγχου και λειτουργίας των επιμέρους μηχανημάτων. Οι αιτίες των βλαβών στα ασύρματα δίκτυα συνήθως εντοπίζονται σε βλάβες υλικού και ηλεκτρομαγνητικές παρεμβολές. Αν το δίκτυο «πέσει», τότε είναι απαραίτητη μία κατάλληλη αντίδραση του συστήματος η οποία θέτει τη διαδικασία και τα μηχανήματα σε ασφαλή κατάσταση λειτουργίας. Αυτή η αντίδραση καθορίζεται από τη φύση των δεδομένων που ανταλλάσσονται μέσω του δικτύου. Αύξηση της αξιοπιστίας μπορεί να επιτευχθεί χρησιμοποιώντας ηλεκτρονικά υψηλότερης ποιότητας και ανθεκτικότητας. Επίσης, αυξάνοντας τη στάθμη της εκπεμπόμενης ισχύος των ασύρματων δικτύων, συνήθως προκαλείται μείωση των παρεμβολών αφού ισχυροποιείται το εκπεμπόμενο σήμα έναντι άλλων σημάτων ή θορύβων που πιθανώς εκπέμπονται στην ίδια περιοχή. Βέβαια η αύξηση της στάθμης



της εκπεμπόμενης ισχύος υπόκειται σε περιορισμούς, οι οποίοι καθορίζονται από τους κρατικούς ή διεθνείς κανονισμούς.

- **Τροφοδοσία Ισχύος.** Τα ενσύρματα βιομηχανικά δίκτυα συνήθως συνοδεύονται από γραμμές τροφοδοσίας ισχύος, προκειμένου να τροφοδοτούνται οι συσκευές του δικτύου. Σε πολλές μονάδες διεργασιών, το δίκτυο πρέπει να μην προσθέτει κίνδυνο εκρήξεων, που δύναται να προκύψει από τη φθορά των καλωδιώσεων, σε συνδυασμό με το εκρηκτικό περιβάλλον που συχνά υπάρχει στην ατμόσφαιρα (π.χ. εύφλεκτα αέρια σε διωλιστήρια). Τα ασύρματα δίκτυα διαθέτουν το πλεονέκτημα της απουσίας καλωδίων σημάτων, πράγμα που περιορίζει τον παραπάνω κίνδυνο. Ωστόσο, ο κίνδυνος παραμένει, διότι οι κόμβοι εξακολουθούν να χρειάζονται τροφοδοσία ισχύος.

Καθώς η χρήση μπαταριών για την τροφοδοσία συσκευών δεν είναι ακόμη πλήρως αποδεκτή, η χρήση τους περιορίζεται για την εφεδρική τροφοδοσία των συσκευών. Με τη χρήση ασύρματων αισθητήρων χαμηλής ενεργειακής κατανάλωσης (low power devices), είναι δυνατή η αποφυγή της χρήσης καλωδίων σε πολλές περιπτώσεις (ορισμένες συσκευές μπορούν να λειτουργούν με μια μπαταρία μέχρι και 2 χρόνια), ωστόσο είναι προφανές ότι η σωστότερη λύση παραμένει η χρήση τοπικών πηγών εναλλασσόμενης (AC) ή συνεχούς (DC) ισχύος. [2]

### 2.3 Μειονεκτήματα Ενσύρματης Επικοινωνίας

Η ενσύρματη τεχνολογία αποτέλεσε τον πρωταρχικό τρόπο επικοινωνίας των επιμέρους κόμβων ενός δικτύου βιομηχανικού αυτοματισμού, βασισμένη σε πρωτόκολλα ενσύρματης δικτύωσης όπως είναι το Can Bus, το ProfiBus, CC-Link κ.α. Ωστόσο με την πάροδο των ετών και καθώς οι ανάγκες και οι απαιτήσεις του βιομηχανικού αυτοματισμού αυξάνονταν, αυτό το είδος επικοινωνίας άρχισε να παρουσιάζει ορισμένα μειονεκτήματα:

- Πολύπλοκος σχεδιασμός και σύνθετη υλοποίηση με αποτέλεσμα να αυξάνεται πολύ και το κόστος εγκατάστασης και το κόστος συντήρησης.
- Δυσκολία στην αντιμετώπιση προβλημάτων με τις επιμέρους συνδέσεις στους connectors τερματισμού των καλωδίων.
- Μειωμένη ευελιξία εξαιτίας της ύπαρξης σταθερών συνδέσεων και καλωδιώσεων.
- Κατά τη σχεδίαση ενός ενσύρματου δικτύου πρέπει να λαμβάνονται υπόψη πιθανές ανάγκες μελλοντικής του επέκτασης. Συνεπώς πρέπει να είναι διαθέσιμοι επιπλέον

πίνακες τερματισμού (marshalling cabinets), κουτιά διακλάδωσης (junction boxes), κάρτες, μεταγωγείς (switches) και συνδέσεις για κάθε πιθανή μελλοντική επέκταση.

- Η κίνηση και η περιστροφή των συστημάτων (π.χ ρομποτικά συστήματα) είναι πιθανό να δημιουργήσει βαθμιαία φθορά των καλωδίων σύνδεσης με αποτέλεσμα να προκύπτουν βλάβες οι οποίες είναι δύσκολες ως προς τον εντοπισμό και την επιδιόρθωσή τους. [1]

## 2.4 Πλεονεκτήματα Ασύρματης Επικοινωνίας

Εξαιτίας των προαναφερθέντων μειονεκτημάτων που παρουσίασε ο ενσύρματος τρόπος επικοινωνίας μεταξύ των κόμβων ενός δικτύου βιομηχανικού αυτοματισμού σε συνδυασμό με τις αυξανόμενες ανάγκες επικοινωνίας και δικτύωσης της σύγχρονης βιομηχανίας, άρχισε να κερδίζει έδαφος ο ασύρματος τρόπος επικοινωνίας. Επιπρόσθετα η χρήση αυτού του τρόπου επικοινωνίας για την κάλυψη των αναγκών του βιομηχανικού αυτοματισμού παρουσίασε αρκετά βασικά πλεονεκτήματα. Τα κυριότερα από αυτά είναι:

- Ένα ασύρματο δίκτυο δεν υφίσταται φθορές κατά την καθημερινή του λειτουργία και τη διακίνηση των δεδομένων μεταξύ των ενδιάμεσων κόμβων.
- Για τη σωστή εγκατάσταση και συντήρηση ενός ασύρματου δικτύου απαιτούνται λιγότερα έξοδα.
- Συνήθως υπάρχει εφεδρεία (redundancy) ασύρματου εξοπλισμού, οπότε η απώλεια ενός κόμβου, δεν σταματά τη λειτουργία του αυτοματισμού ή της διεργασίας.
- Εύκολος εντοπισμός και αντιμετώπιση βλαβών από τους χρήστες.
- Ευκολότερη ανάπτυξη ασύρματου δικτύου σε κινητό ή περιστρεφόμενο εξοπλισμό και σε απρόσιτες ή απομακρυσμένες θέσεις.
- Οι ευκαιρίες ανάπτυξης και εξέλιξης των Μικρο-ηλεκτρομηχανικών συστημάτων (Micro-Electromechanical Systems – MEMs) των οποίων τα κύρια πλεονεκτήματα είναι το χαμηλό κόστος, η χαμηλότερη κατανάλωση ισχύος, οι υψηλές επιδόσεις αίσθησης και η ολοκλήρωση.
- Προσφέρει αξιόπιστη επικοινωνία χωρίς μεγάλη πολυπλοκότητα και χωρίς τη χρήση ακριβών connectors.

Γενικότερα η χρήση της ασύρματης τεχνολογίας μπορεί να βοηθήσει τη βιομηχανία να ξεπεράσει τους περιορισμούς που θέτει η ενσύρματη τεχνολογία. Παράλληλα η

βιομηχανία μπορεί να επωφεληθεί από την ευελιξία και την ελευθερία σε επίπεδο σχεδιασμού, που προσφέρουν τα ασύρματα δίκτυα. [1]

## 2.5 Χρήση Ασύρματης τεχνολογίας

Το κόστος λειτουργίας ενός εργοστασίου εξαρτάται σε μεγάλο βαθμό από τα συστήματα αυτοματισμού που χρησιμοποιούνται σε αυτό. Η χρήση της ασύρματης τεχνολογίας και του διαδικτύου μπορεί να δώσει αρκετές λύσεις σε πολλούς τομείς των διαδικασιών του βιομηχανικού αυτοματισμού, προσφέροντας παράλληλα υψηλές αποδόσεις και καλύτερη ποιότητα υπηρεσιών με σχετικά χαμηλό κόστος. Η ασύρματη τεχνολογία είναι ελκυστική για χρήση στις διεργασίες του βιομηχανικού αυτοματισμού όχι μόνο επειδή παρουσιάζει χαμηλότερο κόστος εγκατάστασης, αλλά και επειδή προσφέρει ευκολία αναδιαμόρφωσης του δικτύου χωρίς να απαιτείται η χρήση καλωδίων. Στις μέρες μας το μεγαλύτερο μέρος του συνολικού κόστους μίας μονάδας παραγωγής αφορά την εγκατάσταση, τη διαμόρφωση και την αναδιαμόρφωση αυτής. Αν μία βιομηχανική μονάδα υπόκειται σε αλλαγές κατά τη διάρκεια του χρόνου λειτουργίας της οι οποίες οφείλονται σε εισαγωγή νέου εξοπλισμού ή σε αντικατάσταση του ήδη υπάρχοντος, τότε ο χρόνος που θα παραμείνει εκτός λειτουργίας είναι πιθανό να οδηγήσει σε μεγάλη οικονομική ζημιά. Το φαινόμενο αυτό δεν υφίσταται κατά τη χρήση ασύρματων δικτύων, αφού προσφέρουν απλότητα και ταχύτητα τόσο στην εγκατάσταση όσο και στην επέκταση του δικτύου. Στη σύγχρονη βιομηχανία μερικά από τα κυριότερα εμπόδια που παρουσιάζονταν κατά την αναδιαμόρφωση του δικτύου οφείλονταν στην έλλειψη ευελιξίας της ενσύρματης υποδομής και στη δυσκολία προσαρμογής του υπάρχοντος λογισμικού ή στη δυσκολία εύρεσης και ανάπτυξης νέου κατάλληλου λογισμικού. Αυτά τα εμπόδια μπορούν να λυθούν με τη χρήση ασύρματης τεχνολογίας.

Συνοψίζοντας οι κυριότεροι λόγοι που προώθησαν τη χρήση της ασύρματης τεχνολογίας στο βιομηχανικό αυτοματισμό είναι:

- **Ικανότητα προσαρμογής σε συγκεκριμένες εφαρμογές.** Σε ορισμένες εφαρμογές η χρήση της ασύρματης τεχνολογίας καθίσταται υποχρεωτική. Αυτό συμβαίνει στην περίπτωση που είναι απαραίτητη η ελεύθερη κίνηση των συσκευών. Επίσης στο βιομηχανικό αυτοματισμό είναι πιθανό να υπάρξουν εφαρμογές οι οποίες να προκαλέσουν φθορά στα καλώδια, όπως για παράδειγμα

ορισμένα χημικά προϊόντα ή συνεχείς δονήσεις. Σε αυτή την περίπτωση η χρήση ασύρματης δικτύωσης κρίνεται απαραίτητη.

- **Οικονομικά πλεονεκτήματα.** Σε πολλές περιπτώσεις δεν είναι απαραίτητη η χρήση ασύρματης δικτύωσης, όμως είναι πιθανό το κόστος μίας ενσύρματης εγκατάστασης να είναι απαγορευτικό όπως για παράδειγμα μπορεί να συμβεί αν θελήσουμε να εγκαταστήσουμε ένα μικρό αριθμό ενσύρματων αισθητήρων σε μεγάλη απόσταση μεταξύ τους. Επίσης, είναι πιθανό να μην υπάρχει σύντομη και ασφαλής διαδρομή για την εγκατάσταση καλωδίου επικοινωνίας ή να απαιτείται εγκατάσταση επιπλέον συσκευών σε υπάρχον σύστημα αυτοματισμού (modification), όπου εγκατάσταση ενσύρματων συσκευών θα απαιτούσε τροποποίηση του σχεδιασμού όλου του ενσύρματου δικτύου. Έτσι, με την εγκατάσταση ενός βιομηχανικού ασύρματου δικτύου αυτοματισμού, είναι προφανές ότι προκύπτει μείωση του κόστους εγκατάστασης.
- **Ευελιξία.** Υπάρχουν περιπτώσεις στις οποίες το ζητούμενο δεν είναι απλά η μείωση του κόστους. Η ασύρματη τεχνολογία συνδυάζει το χαμηλό κόστος εγκατάστασης με τη δυνατότητα αναδιάρθρωσης του δικτύου χωρίς να είναι απαραίτητη η χρήση καλωδίων. Η ασύρματη επικοινωνία όταν χρησιμοποιείται σε συνδυασμό με άλλες τεχνολογίες (όπως είναι οι υπηρεσίες web και η τεχνολογία agent) είναι εφικτό να διαδραματίσει σημαντικό ρόλο όσον αφορά την ευελιξία και την εκ νέου ρύθμιση των παραμέτρων των βιομηχανικών συστημάτων αυτοματισμού. [8]

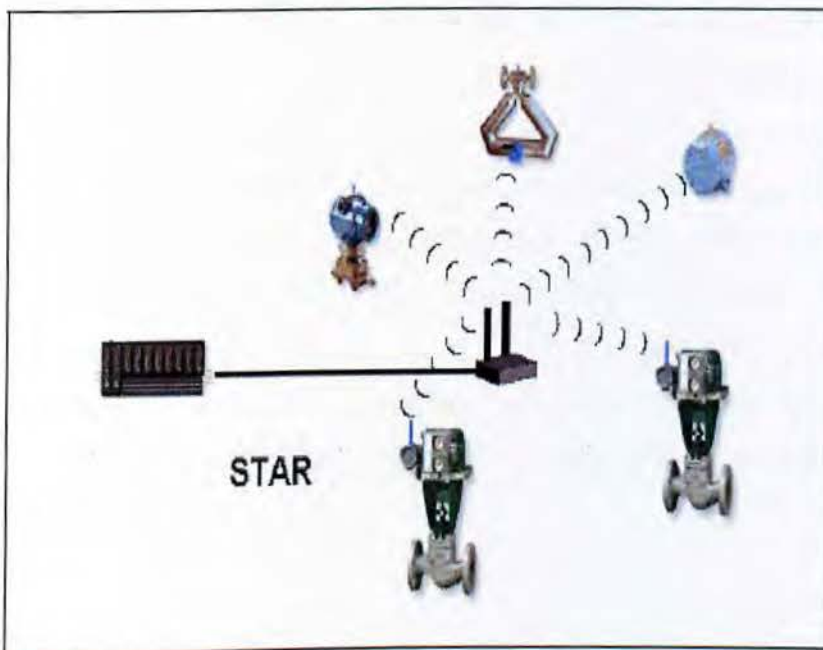
## 2.6 Τοπολογίες Ασύρματων Δικτύων

Τα ενσύρματα δίκτυα σχηματίζουν τοπολογίες οι οποίες καθορίζονται από τη θέση των κόμβων και των εξαρτημάτων του δικτύου. Στα ασύρματα δίκτυα οι τοπολογίες καθορίζονται από τις «λογικές δυνατότητες» των εξαρτημάτων του δικτύου. Σε πολλές περιπτώσεις ο χρήστης είναι αυτός που καθορίζει τη μορφή της τοπολογίας του ασύρματου δικτύου, η οποία ρυθμίζεται έπειτα από την εγκατάσταση και την προσωρινή χρήση του δικτύου. Στην ουσία πραγματοποιείται μία «δοκιμή» της χρήσης του δικτύου με βάση τις ανάγκες του εργοστασίου και έπειτα η τοπολογία του παίρνει την τελική της μορφή. Στη συνέχεια παρουσιάζονται οι κυριότερες τοπολογίες ασύρματων δικτύων.



## 2.6.1 Τοπολογία Αστέρα

Η χαρακτηριστικότερη τοπολογία ασύρματου δικτύου είναι η τοπολογία αστέρα. Πρόκειται για ένα σύμπλεγμα κόμβων στο κέντρο του οποίου βρίσκεται το ασύρματο σημείο πρόσβασης. Στην τοπολογία αστέρα κάθε ασύρματη συσκευή επικοινωνεί με το κοινό σημείο πρόσβασης, το οποίο συνδέεται συνήθως μέσω καλωδίων στον κόμβο μεταγωγής (switch) ενός δικτύου. Αυτός ο τρόπος σύνδεσης θέτει όλες τις ασύρματες συσκευές στο ίδιο πεδίο σύγκρουσης (collision domain), δημιουργώντας έτσι ένα ασύρματο δίκτυο. Συνήθως τα δίκτυα αυτού του τύπου δεν εμφανίζουν πρόβλημα συγκρούσεων διότι το σημείο πρόσβασης (access point) από μόνο του δεν είναι σε θέση να λαμβάνει περισσότερα του ενός μηνύματα κάθε φορά, αφού αγνοεί όποιο μήνυμα φτάσει δεύτερο. Δυστυχώς όμως η δεύτερη συσκευή δεν ενημερώνεται ότι το μήνυμά της δεν παραλήφθηκε επιτυχώς επειδή το μήνυμά απόρριψης υφίσταται στο επίπεδο 1 του δικτύου και δεν υπάρχει κάποιο εξουσιοδοτημένο πρωτόκολλο αρμόδιο για το μήνυμά απόρριψης του επιπέδου 1. Εφόσον τα μηνύματα αποστέλλονται στα επίπεδα 3 και 4 του δικτύου χρησιμοποιώντας το πρωτόκολλο TCP/IP (Transmission Control Protocol/ Internet Protocol), η δεύτερη συσκευή θα ειδοποιηθεί από το TCP ότι το μήνυμά της δεν παραλήφθηκε και έπειτα θα ξαναπροσπαθήσει. Σε περίπτωση που χρησιμοποιείται το πρωτόκολλο UDP (User Datagram Protocol) για την αποστολή των μηνυμάτων δεν είναι εφικτή η αποστολή μηνύματος επιβεβαίωσης. Η τοπολογία αστέρα για ασύρματα δίκτυα παρουσιάζεται στην επόμενη εικόνα.



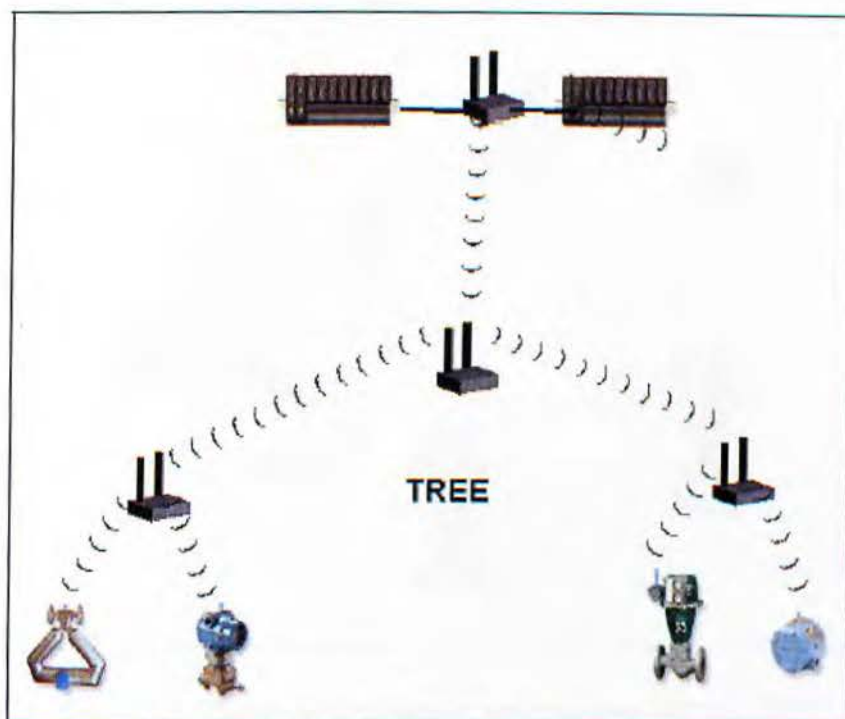
Εικόνα 1 – Τοπολογία Αστέρα για ασύρματα δίκτυα. [2]

Σε αυτή την τοπολογία δικτύου είναι εφικτό να μάθει ένας κόμβος μεταγωγής (switch) τη διεύθυνση των συνδεδεμένων σε αυτόν συσκευών, “ακούγοντας” απλά τα μηνύματα που αυτές στέλνουν. Σε αυτή την περίπτωση δρομολογούνται ταχύτατα όλα τα μηνύματα που φθάνουν στον κόμβο μεταγωγής (switch) προς τις επιμέρους συσκευές. Η σημασία αυτής της τοπολογίας δικτύου στην ταχύτατη αναδιαμόρφωση του βιομηχανικού αυτοματισμού είναι προφανής, αφού δίνει δίκτυα αυξημένης αξιοπιστίας που χρησιμοποιούνται κυρίως στην παραγωγική διαδικασία. Όμως αν υπάρχουν στον ίδιο χώρο συσκευές που εκπέμπουν στο φάσμα των ραδιοσυχνοτήτων, τότε είναι πιθανή η ύπαρξη παρεμβολών και η αποτυχία αποστολής μηνυμάτων στον τελικό προορισμό. Σε αυτή την περίπτωση χρησιμοποιείται ένα δεύτερο σημείο μεταγωγής ή ένα δεύτερο σημείο πρόσβασης ώστε να υπάρξει εναλλακτική διαδρομή και να διατηρήσει το δίκτυο την υψηλή του αξιοπιστία. Αυτή η εναλλακτική διαδρομή μπορεί να εξυπηρετήσει πολλές πρωτογενείς διαδρομές και λειτουργεί ως εφεδρικό μονοπάτι. [2]

## 2.6.2 Τοπολογία Δέντρου

Όπως συμβαίνει και με τα ενσύρματα δίκτυα, έτσι και τα ασύρματα δίκτυα είναι εφικτό να οργανωθούν με τη μορφή μίας τοπολογίας δέντρου. Κάθε κόμβος είναι προσαρμοσμένος με κατάλληλες ρυθμίσεις σε ένα δίκτυο το οποίο είναι συνδεδεμένο σε ένα συγκεκριμένο σημείο πρόσβασης ή σε ένα συγκεκριμένο σημείο μεταγωγής. Αυτό το σημείο πρόσβασης ή μεταγωγής συνδέεται με ένα άλλο σημείο πρόσβασης το οποίο βρίσκεται κοντά σε ένα ενσύρματο δίκτυο. Αυτές οι συνδέσεις μεταξύ των σημείων πρόσβασης ή μεταγωγής επαναλαμβάνονται διαδοχικά μέχρι να πραγματοποιηθεί η τελική σύνδεση με το ενσύρματο δίκτυο. Στα δίκτυα αυτής της μορφής οι επιμέρους κόμβοι καταναλώνουν ενέργεια μόνο κατά τη μετάδοση ή τη λήψη δεδομένων. Συνήθως η κατανάλωση ενέργειας αυξάνεται όταν αυξάνεται η απόσταση μετάδοσης ή όταν παρεμβάλλονται εμπόδια. Επίσης στην κατανάλωση της ενέργειας παίζει ρόλο και η ποσότητα των προς μετάδοση δεδομένων, αφού περισσότερα δεδομένα οδηγούν σε περισσότερες μεταδόσεις άρα και σε μεγαλύτερη κατανάλωση ενέργειας. Η τοπολογία δέντρου για ασύρματα δίκτυα παρουσιάζεται στην εικόνα που ακολουθεί. [2]

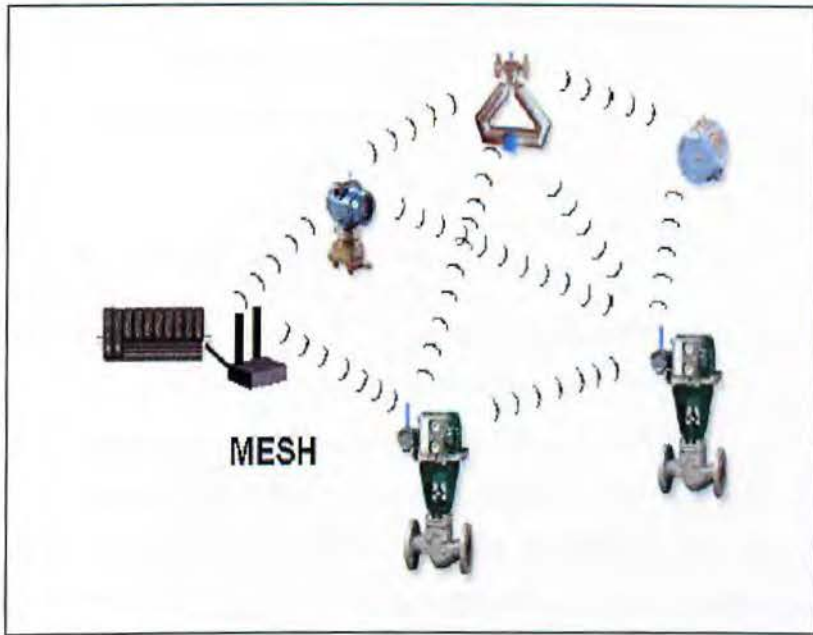




Εικόνα 2 – Τοπολογία Δέντρον για ασύρματα δίκτυα. [2]

### 2.6.3 Τοπολογία Πλέγματος

Η νεότερη και πιο επαναστατική τοπολογία ασύρματου δικτύου είναι η τοπολογία πλέγματος. Σε μία τέτοια τοπολογία κάθε κόμβος αποτελεί ταυτόχρονα μία τερματική συσκευή αλλά και ένα στοιχείο επέκτασης του δικτύου. Η τοπολογία πλέγματος παραπέμπει σε δίκτυα τα οποία είναι από τη φύση τους αυτοσυντηρούμενα δίκτυα με εφεδρεία, και παρουσιάζουν ακριβώς εκείνες τις ιδιότητες που είναι απαραίτητες για δίκτυα που χρησιμοποιούνται σε βιομηχανικούς αυτοματισμούς. Σε αυτά τα δίκτυα κάθε κόμβος έχει την ευθύνη να προωθήσει ένα μήνυμα το οποίο έλαβε από το δίκτυο και δεν προορίζεται για αυτόν, στους υπόλοιπους κόμβους που βρίσκονται εντός της εμβέλειας εκπομπής του. Στη συνέχεια αυτοί οι κόμβοι στέλνουν με τη σειρά τους το μήνυμα σε τουλάχιστον ένα ακόμα κόμβο ο οποίος βρίσκεται εντός της εμβέλειας εκπομπής τους. Με αυτό τον τρόπο κάθε κόμβος του δικτύου γίνεται και ένας μεταγωγέας του δικτύου. Αξίζει να τονίσουμε ότι σε αυτές τις τοπολογίες υπεισέρχονται πολλά επιμέρους μονοπάτια (paths). Έτσι κάθε κόμβος ο οποίος λαμβάνει ένα μήνυμα το οποίο έχει παραλάβει και νωρίτερα από ένα άλλο κόμβο, το απορρίπτει. Ένα δίκτυο σε τοπολογία πλέγματος μπορεί να επεκταθεί όσο επιθυμούμε και να παρουσιάσει μεγάλη ανοχή σε λανθασμένες μεταδόσεις. Η τοπολογία πλέγματος για ασύρματα δίκτυα παρουσιάζεται στην εικόνα που ακολουθεί.



*Εικόνα 3 – Τοπολογία πλέγματος για ασύρματα δίκτυα. [2]*

Τα πρωτόκολλα που χρησιμοποιούνται στα ασύρματα δίκτυα τα οποία βασίζονται στην τοπολογία πλέγματος έχουν τη δυνατότητα δημιουργίας και διατήρησης πινάκων δρομολόγησης ώστε να παρέχουν ενδείξεις που αφορούν τον παραλήπτη όλων των μηνυμάτων που πρόκειται να προωθηθούν. Αυτή η δυνατότητα αποτρέπει τα μηνύματα να προωθούνται προς κατευθύνσεις διαφορετικές από τις επιθυμητές με αποτέλεσμα το δίκτυο να αυξάνει την αποτελεσματικότητά του. Οι πίνακες δρομολόγησης κατασκευάζονται κατά τη διέλευση των μηνυμάτων από τους επιμέρους κόμβους δρομολόγησης του ασύρματου δικτύου πλέγματος. Τα δίκτυα πλέγματος που προορίζονται για εφαρμογές του βιομηχανικού αυτοματισμού τείνουν να έχουν 256 ή λιγότερους κόμβους, οπότε οι πίνακες δρομολόγησης που δημιουργούνται είναι κατά κανόνα μικροί και οι διαδρομές που σχηματίζονται απλές. Επίσης οι πίνακες δρομολόγησης πρέπει να ενημερώνονται όταν προστίθενται νέοι κόμβοι στο ασύρματο δίκτυο αλλά και όταν για κάποιο λόγο ορισμένοι κόμβοι δεν ανταποκρίνονται στα διαβιβασθέντα μηνύματα.

Τα ασύρματα δίκτυα πλέγματος αντιμετωπίζουν ένα πρόβλημα το οποίο δεν υπάρχει στα ενσύρματα δίκτυα πλέγματος (όπως το Internet). Το πρόβλημα αυτό έχει να κάνει με την περιττή διάδοση μηνυμάτων και την αυξημένη κατανάλωση ενέργειας που προκύπτει. Προκειμένου να λυθεί αυτό το πρόβλημα, συχνά τα ασύρματα δίκτυα πλέγματος χρησιμοποιούν κεραίες υψηλής κατευθυντικότητας ώστε να αποτρέπουν τη λήψη ενός μηνύματος από κόμβους για τους οποίους δεν προορίζεται. Αυτό έχει ως αποτέλεσμα να



αποτρέπεται τελικά η δρομολόγηση πολλαπλών περιττών διαδρομών ή η άσκοπη επανάληψη πολλών μηνυμάτων. Με αυτό τον τρόπο διασφαλίζεται τόσο η αξιοπιστία του δικτύου, η ταχύτητα του και η ελάχιστη κατανάλωση ισχύος. [2]

## 2.7 Διάκριση Ασύρματων Δικτύων

Ο βασικότερος τρόπος διάκρισης των ασύρματων δικτύων σε επιμέρους κατηγορίες πραγματοποιείται με κριτήριο την εμβέλεια μετάδοσης του ασύρματου δικτύου. Έτσι τα ασύρματα δίκτυα διακρίνονται σε **Ασύρματα Τοπικά Δίκτυα** (Wireless Local Area Network – WLAN), σε **Ασύρματα Μητροπολιτικά Δίκτυα** (Wireless Metropolitan Area Network – WMAN) και σε **Ασύρματα Προσωπικά Δίκτυα Περιοχής** (Wireless Personal Area Network – WPAN). Στη συνέχεια παρουσιάζουμε αυτές της μορφές δικτύων, με ταυτόχρονη συνοπτική παρουσίαση των βασικότερων προτύπων που αυτά χρησιμοποιούν.

### 2.7.1 Ασύρματα τοπικά δίκτυα WLAN

Ένα Ασύρματο Τοπικό Δίκτυο (Wireless Local Area Network – WLAN) αποτελεί στην ουσία το αποτέλεσμα της ασύρματης σύνδεσης δύο ή περισσότερων συσκευών μεταξύ τους εντός μίας σχετικά μικρής περιοχής. Ένα τέτοιο δίκτυο παρέχει τη δυνατότητα στους χρήστες του να κινηθούν με ευκολία εντός της περιοχής που καλύπτει χωρίς να χάσουν τη σύνδεση τους με αυτό. Βασικό χαρακτηριστικό του αποτελεί η ευκολία εγκατάστασης σε συνδυασμό με το σχετικά χαμηλό κόστος υλοποίησης. Το πρώτο WLAN βασίστηκε στις χρήσιμες υπέρυθρες ακτινοβολίες. Μεταγενέστερα χρησιμοποιώντας ασύρματα modem, δημιουργήθηκαν WLAN με ταχύτητες μετάδοσης της τάξης του bit/sec. Στη συνέχεια οι ταχύτητες αυτές αυξήθηκαν αρχικά σε Kbit/sec και στη συνέχεια σε Mbit/sec. Στις μέρες μας ένα WLAN λειτουργεί στη ζώνη συχνοτήτων των 2,4 GHz ή στη ζώνη συχνοτήτων των 5 GHz προσφέροντας ταχύτητες έως και 54 Mbit/sec.

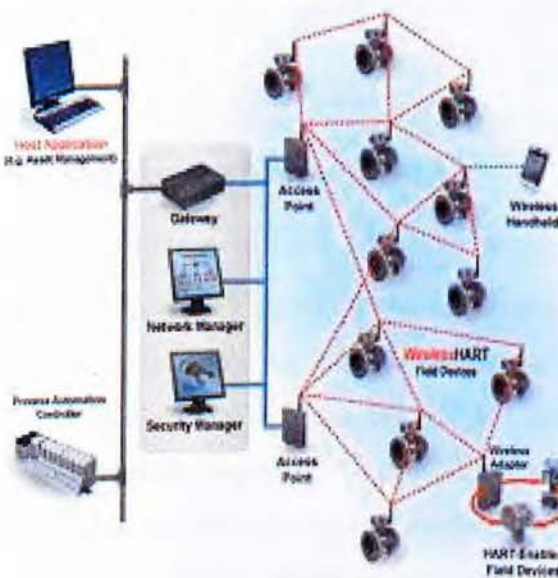
Τα WLAN δίκτυα υποστηρίζουν δύο τρόπους λειτουργίας: τον **ad-hoc** και τον **infrastructure**. Ο **ad-hoc** τρόπος λειτουργίας επιτρέπει στους ενδιαμέσους κόμβους να σχηματίσουν αυθόρμητα ένα ασύρματο LAN στο οποίο όλοι οι επιμέρους κόμβοι επικοινωνούν μεταξύ τους «peer to peer». Δηλαδή επικοινωνούν ο ένας με τον άλλο με διαδοχικές αλυσιδωτές συνδέσεις. Στον τρόπο λειτουργίας **infrastructure** το δίκτυο διαθέτει ένα σημείο πρόσβασης μέσω του οποίου επικοινωνεί κάθε κόμβος. Ένα τυπικό σημείο

πρόσβασης ενός WLAN έχει εμβέλεια γύρω στα 45 m για εσωτερικούς χώρους και γύρω στα 90 m για εξωτερικούς χώρους. Αυτό το σημείο πρόσβασης ονομάζεται Wi-Fi AP (Wi-Fi Access Point). Στην αυτοματοποίηση των διαδικασιών τα Wi-Fi AP χρησιμεύουν ως μέσο συγκέντρωσης δεδομένων και ως μέσο δικτύωσης. Για παράδειγμα τα δίκτυα αυτού του είδους είναι εφικτό να χρησιμοποιηθούν σε ένα ασύρματο δίκτυο σε συνδυασμό με συσκευές μικρής εμβέλειας και χαμηλής ισχύος για τη συλλογή δεδομένων από την πύλη και τη μετέπειτα αποστολή τους στην αίθουσα ελέγχου (control room) ή στο σημείο συλλογής δεδομένων (data collection point).

Τα WLAN προσφέρουν αρκετά πλεονεκτήματα κατά τη χρήση τους σε διεργασίες του βιομηχανικού αυτοματισμού με αποτέλεσμα τα τελευταία χρόνια να έχει αυξηθεί κατακόρυφα τόσο η έρευνα, όσο και η χρήση τους. Τα κυριότερα από αυτά τα πλεονεκτήματα είναι:

- Ικανοποιητική εμβέλεια μετάδοσης δεδομένων
- Ευελιξία προτύπων
- Αξιοπιστία
- Άριστη σχέση απόδοσης-τιμής
- Υψηλή ταχύτητα μετάδοσης δεδομένων
- Ευκολία πρόσβασης ακόμα και από περιφερόμενους, εντός του χώρου εμβέλειας του δικτύου, εργαζόμενους

Στην επόμενη εικόνα παρουσιάζεται η γενική μορφή ενός δικτύου WLAN.



Εικόνα 4 – Γενική Μορφή δικτύου WLAN. [3]



Στο δίκτυο της προηγούμενης εικόνας χρησιμοποιούνται Ασύρματοι Αισθητήρες (Wireless Sensors), Προγραμματιζόμενοι Λογικοί Ελεγκτές (Programmable Logic Controllers – PLC), Κινητοί Σταθμοί (Mobile Stations), κινητά τηλέφωνα (Mobile Phones), Wi-Fi και πραγματοποιείται ασύρματη σύνδεση με το υπόλοιπο αυτοματοποιημένο σύστημα μέσω πυλών (Gateways).

Στον τομέα της ασφάλειας τα WLAN έχουν υποστεί δύο πολύ σημαντικές βελτιώσεις. Οι βελτιώσεις αυτές είναι η Ασύρματη Προστατευόμενη Πρόσβαση (Wi-Fi Protected Access - WPA) και η Ασύρματη Προστατευόμενη Πρόσβαση 2 (WPA2) οι οποίες αντικατέστησαν την προηγούμενη και λιγότερο ασφαλή τεχνολογία WEP. Επιπρόσθετα, όταν ένα WLAN χρησιμοποιείται σε συνδυασμό με ένα ασύρματο δίκτυο αισθητήρων, παρέχει επαρκές εύρος ζώνης για την υποστήριξη πολλαπλών μεταδόσεων. Ωστόσο τα WLAN ενδέχεται να μην είναι και τόσο αποτελεσματικά για τη δημιουργία συνδέσεων από συσκευή σε συσκευή διότι στην περίπτωση αυτή αυξάνεται κατακόρυφα η κατανάλωση ισχύος αφού απαιτείται η χρήση καλωδίων τροφοδοσίας ή η διαβίβαση ισχύος μέσω Ethernet (Power Over Ethernet - POE). Σε αρκετές περιπτώσεις το κόστος των γραμμών τροφοδοσίας ενδέχεται να περιορίσει το συνολικό μέγεθος του ασύρματου δικτύου. Τα ασύρματα LAN είναι σχεδιασμένα για εφαρμογές υψηλής απόδοσης με μικρό αριθμό τερματικών συσκευών.

[3]

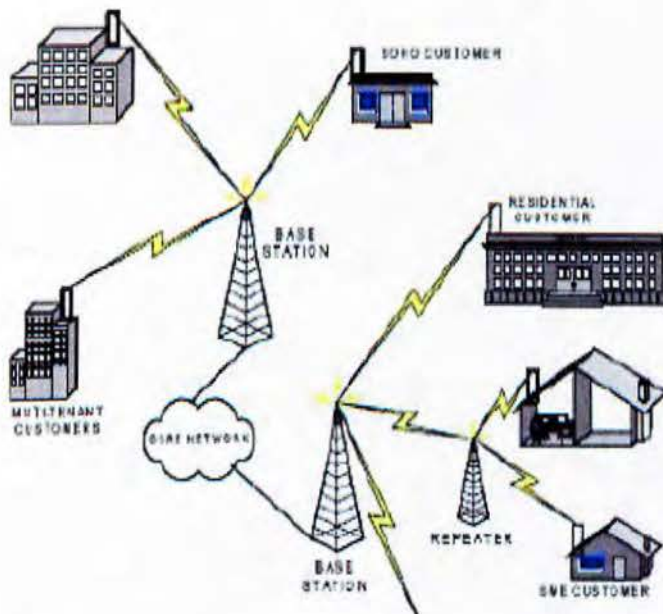
Στο σημείο αυτό πρέπει να τονίσουμε ότι η παραπάνω σύντομη παρουσίαση του Wi-Fi πραγματοποιήθηκε για τις ανάγκες παρουσίασης και ερμηνείας των δικτύων WLAN. Η αναλυτική παρουσίαση του πρωτόκολλου αυτού θα πραγματοποιηθεί στο κεφάλαιο 4 της πτυχιακής εργασίας.

## 2.7.2 Ασύρματο Μητροπολιτικό Δίκτυο WMAN

Ένα Ασύρματο Μητροπολιτικό Δίκτυο (Wireless Metropolitan Area Network – WMAN) είναι στην ουσία ένα WLAN μεγαλύτερης εμβέλειας το οποίο διαθέτει πάρα πολλούς κόμβους πρόσβασης. Στην ουσία το WMAN είναι η επέκταση ενός WLAN αφού αποτελείται από WLAN Hotspots αλλά και από WLAN hot zones με πολλαπλά σημεία πρόσβασης τοποθετημένα σε διάφορες περιοχές. Τα σημεία πρόσβασης επικοινωνούν το ένα με το άλλο ώστε όλοι οι χρήστες του WMAN να είναι συνδεδεμένοι σε ένα ενιαίο ασύρματο δίκτυο. Στα WMAN δίκτυα οι συνδέσεις μπορεί να είναι από σημείο σε σημείο (point to

point) ή από ένα σημείο σε πολλαπλά σημεία (point to multipoint) ώστε να είναι εφικτό να συνδεθούν διαφορετικά ασύρματα LAN, σχηματίζοντας ένα ενιαίο ασύρματο MAN. [4]

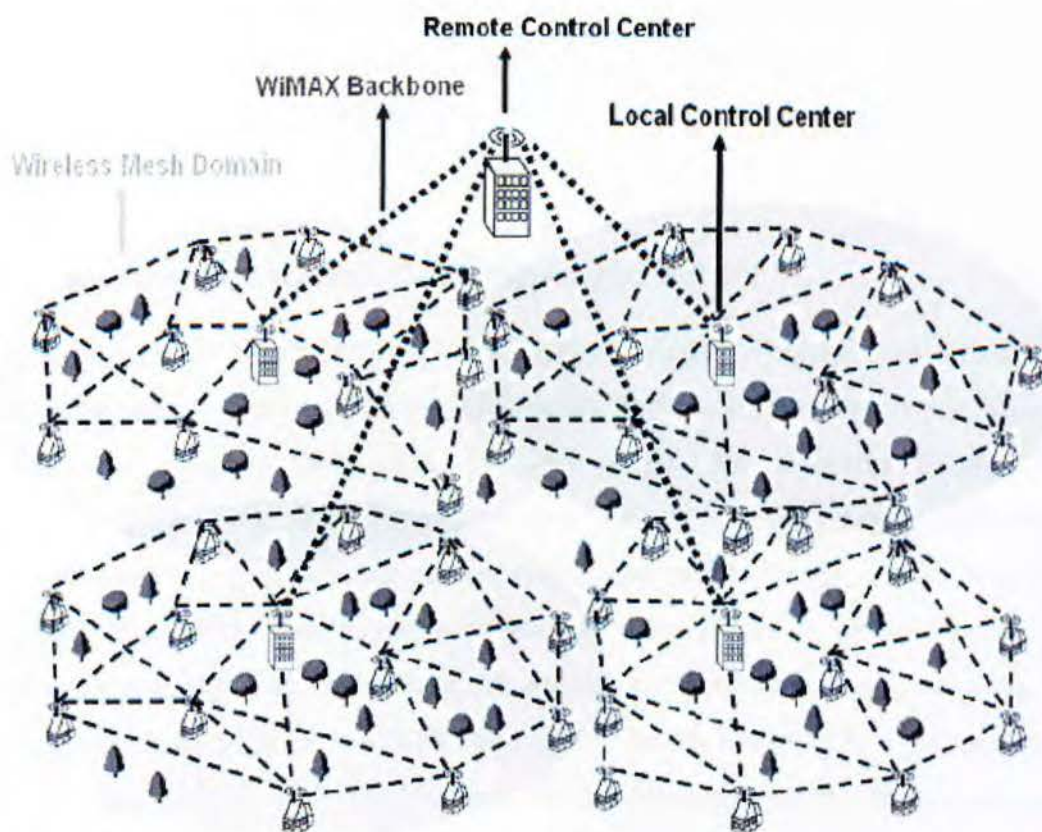
Ένα τυπικό παράδειγμα δικτύου WMAN παρουσιάζεται στην επόμενη εικόνα.



*Εικόνα 5 – Τυπικό παράδειγμα δικτύου WMAN. [4]*

Το WiMax (Worldwide Interoperability for Microwave Access) το οποίο είναι συνώνυμο με το πρότυπο IEEE 802.16 είναι μία μητροπολιτική τεχνική πρόσβασης με βασικά χαρακτηριστικά τη μετάδοση σε μεγάλες αποστάσεις και τη δυνατότητα μεταφοράς σχετικά μεγάλου όγκου δεδομένων. Η ακτίνα κάλυψης που προσφέρει μπορεί να φτάσει τα 50 χιλιόμετρα και ο ρυθμός μετάδοσης μπορεί να αγγίξει τα 75 Mbit/sec. Το Wimax παρέχει ασύρματη πρόσβαση και μεγάλες δυνατότητες επέκτασης του δικτύου. Στις διεργασίες του βιομηχανικού αυτοματισμού το WiMax χρησιμοποιείται ως δίκτυο κορμού (backbone) για την επέκταση του ασύρματου δικτύου. Η τυπική μορφή της αρχιτεκτονικής ενός ασύρματου δικτύου που στηρίζεται στην τεχνική WiMax προσδιορίστηκε από τους Cungor και Lambert το 2006 και παρουσιάζεται στην επόμενη εικόνα. [3]





*Εικόνα 6 – Τυπική μορφή ασύρματου δικτύου που βασίζεται στην τεχνική WiMax. [3]*

Η τεχνολογία WiMax παρουσιάζει πολλά πλεονεκτήματα που την καθιστούν ελκυστική και προσιτή για χρήση σε πάρα πολλές εφαρμογές. Τα κυριότερα από αυτά τα πλεονεκτήματα είναι:

- Η αυξημένη αξιοπιστία.
- Το χαμηλό κόστος εγκατάστασης.
- Η μεγάλη περιοχή κάλυψης που προσφέρει.
- Η δυνατότητα αυτόματης σύνδεσης με το δίκτυο.

Οι Cungor και Lambert αναφέρουν ως πρόκληση για το Wimax τη βέλτιστη τοποθέτηση πύλων Wimax, την παροχή ευελιξίας, την παροχή καλών δυνατοτήτων επέκτασης, την ολοκλήρωση ετερογενών δικτύων, τη σωστή διαχείριση των πόρων και την ικανοποιητική παροχή ασφάλειας. [3]

Το Wimax ως μέλος του γκρουπ IEEE 802 είναι το πρότυπο που καθορίζει τη διεπαφή της σταθερής Ασύρματης Ευρυζωνικής Πρόσβασης (Broadband Wireless Access – BWA) και σχεδιάστηκε αρχικά για WMAN με οπτική επαφή (Line of Sight – LOS) που λειτουργούσαν σε συχνότητες από 10 έως 66 GHz. Επόμενη του έκδοση η οποία διαθέτει όλα τα χαρακτηριστικά των προηγούμενων προτύπων, υποστηρίζει λειτουργία χωρίς οπτική



επαφή (Non Line of Sight – NLOS) σε συχνότητες από 2 έως 11 GHz. Η περαιτέρω εξέλιξη του Wimax έχει ως στόχο την παροχή ευελιξίας στην Ασύρματη Ευρυζωνική Πρόσβαση (Broadband Wireless Access – BWA). [5]

### 2.7.3 Ασύρματο Προσωπικό Δίκτυο Περιοχής WPAN

Ένα Ασύρματο Προσωπικό Δίκτυο Περιοχής (Wireless Personal Area Network – WPAN) χρησιμοποιείται για την επικοινωνία συσκευών οι οποίες βρίσκονται είτε πάνω σε ένα άτομο είτε τοποθετημένες γύρω από ένα άτομο. Τα ασύρματα δίκτυα PAN παρουσιάζουν εμβέλεια της τάξεως λίγων μόνο μέτρων και προτιμούνται για την επικοινωνία μεταξύ συσκευών που χρησιμοποιούνται προσωπικά από κάποιο άτομο, αλλά και για την αποτελεσματική σύνδεση των συσκευών αυτών με άλλα δίκτυα ή με το Internet. Τα ασύρματα δίκτυα PAN μπορούν επίσης να συνδεθούν, χρησιμοποιώντας καλώδια, με διαύλους υπολογιστών όπως είναι το USB και το FireWire. Οι συσκευές που χρησιμοποιούν τις τεχνικές επικοινωνίας των PAN δικτύων για τη μετάδοση και τη λήψη δεδομένων ονομάζονται συσκευές PAN. Συνήθως στα WPAN δίκτυα χρησιμοποιούνται οι τεχνολογίες Bluetooth, ZigBee και Wireless Hart. [6]

Το Bluetooth λειτουργεί στη συχνότητα των 2.4 GHz και χρησιμοποιεί την τεχνική διαμόρφωσης Διάχυτου Φάσματος με Μεταπήδηση Συχνότητας (Frequency Hopping Spread Spectrum – FHSS). Αποτελείται από 8 κόμβους συνδεδεμένους σε μία δομή αφέντη-σκλάβου (master-slave). Ένας από αυτούς τους κόμβους παίζει το ρόλο του αφέντη (master) και οι υπόλοιποι 7 είναι οι σκλάβοι (slaves). Η εμβέλεια εκπομπής είναι γύρω στα 10 μέτρα. Βέβαια υπό ιδανικές συνθήκες είναι εφικτό να επιτευχθεί εμβέλεια και γύρω στα 100 μέτρα. Το Bluetooth ειδικεύεται σε εφαρμογές υψηλής απόδοσης που περιλαμβάνουν μικρό αριθμό τερματικών τα οποία είναι τοποθετημένα σε μικρό χώρο. Χρησιμοποιείται για ανταλλαγή δεδομένων τόσο από σταθερές όσο και από κινητές πηγές με αποτέλεσμα τη δημιουργία μικρών ασύρματων δικτύων PAN. Έχει την ικανότητα να συνδέει πολλές ασύρματες συσκευές ταυτόχρονα χωρίς να προκύπτουν προβλήματα παρεμβολών κατά την επικοινωνία των συσκευών αυτών. Ο ρυθμός μετάδοσης δεδομένων πλησιάζει το 1 Mbit/sec για αποστάσεις γύρω στα 5 με 10 μέτρα. Βασικό χαρακτηριστικό του Bluetooth είναι η μικρή κατανάλωση ισχύος. [3], [7]

Το ZigBee αποτελεί ένα μικρού κόστους και μικρής εμβέλειας πρότυπο ασύρματης δικτύωσης, το οποίο χαρακτηρίζεται από χαμηλή κατανάλωση ισχύος και χαμηλές ταχύτητες



ασύρματης δικτύωσης. Το συγκεκριμένο πρότυπο έχει τη δυνατότητα να χρησιμοποιείται σε εφαρμογές του βιομηχανικού αυτοματισμού, σε εφαρμογές οικιακού αυτοματισμού και σε εφαρμογές αυτοματισμού κτηρίων. Τα βασικότερα του πλεονεκτήματα είναι η πολύ χαμηλή κατανάλωση ισχύος, η οποία προφανώς οδηγεί σε επιμήκυνση του χρόνου λειτουργίας του δικτύου με τη χρήση ασύρματων πηγών ενέργειας (μπαταρίες), και το γεγονός ότι μπορεί να υποστηρίξει πολλές τοπολογίες δικτύων. Χάρη στα δύο αυτά πλεονεκτήματα το ZigBee μπορεί να φανεί χρήσιμο σε πολλές εφαρμογές δικτύων αισθητήρων. Συνήθως βέβαια χρησιμοποιείται σε εφαρμογές που απαιτούν χαμηλή κατανάλωση ισχύος και χαμηλή ταχύτητα μετάδοσης δεδομένων. Το βασικότερο του μειονέκτημα του είναι ότι δε μπορεί να καλύψει τις απαιτήσεις όλων των βιομηχανικών εφαρμογών, αφού για παράδειγμα δε μπορεί να εξυπηρετήσει μεγάλο πλήθος κόμβων σε μικρά χρονικά διαστήματα. Επίσης είναι αξίζει να αναφέρουμε ότι το πρότυπο IEEE 802.15.4 είναι αυτό που ορίζει τα φυσικά επίπεδα και τα επίπεδα δεδομένων για το ZigBee. [3]

Το Wireless Hart χαρακτηρίζεται από μεταπήδηση συχνότητας, από εφεδρικές διαδρομές δεδομένων και από μηχανισμούς επανάληψης της αποστολής δεδομένων που δεν παρελήφθησαν κατά την αρχική του αποστολή. Οι συσκευές που συμμορφώνονται με τις προδιαγραφές του Wireless Hart είναι διαλειτουργικά και υποστηρικτικά εργαλεία συμβατά τόσο με ενσύρματο εξοπλισμό όσο και με τον εξοπλισμό του Wireless Hart. Τα ασύρματα δίκτυα που χρησιμοποιούν το Wireless Hart δίνουν τη δυνατότητα σε κάθε συσκευή να μεταδώσει τα δικά της δεδομένα, αλλά και τα δεδομένα άλλων κόμβων του δικτύου. Επίσης κάθε κόμβος του δικτύου διαθέτει δύο διαδρομές για τη δρομολόγηση των δεδομένων. Η πρώτη διαδρομή ονομάζεται κύρια (primary) και η δεύτερη διαδρομή ονομάζεται εναλλακτική (alternative). Η εναλλακτική διαδρομή χρησιμοποιείται όταν η κύρια διαδρομή είναι μπλοκαρισμένη είτε εξαιτίας συμφόρησης δεδομένων είτε εξαιτίας παρεμβολών. Επιπρόσθετα στην περίπτωση που μία διαδρομή είναι μονίμως αποκλεισμένη, εγκαθίσταται μία νέα διαδρομή. Το συγκεκριμένο πρότυπο χρησιμοποιεί την Πολυπλεξία Πολλαπλής Πρόσβασης με Διαίρεση Χρόνου (Time Division Multiple Access - TDMA) για δρομολόγηση των μεταδόσεων. [3]

Στο σημείο αυτό οφείλουμε να σημειώσουμε ότι η παραπάνω σύντομη παρουσίαση των πρωτοκόλλων ασύρματης δικτύωσης Bluetooth, ZigBee και Wireless Hart πραγματοποιήθηκε για τις ανάγκες παρουσίασης και ερμηνείας των δικτύων WPAN. Η αναλυτική παρουσίαση των πρωτοκόλλων αυτών θα πραγματοποιηθεί στο κεφάλαιο 4 της πτυχιακής εργασίας.



## 2.8 Σύγκριση Ασύρματης και Ενσύρματης Τεχνολογίας

Τα ενσύρματα δίκτυα έχουν σχεδιαστεί ώστε να διεκπεραιώνουν την επικοινωνία μεταξύ συσκευών τοποθετημένων επί σταθερών θέσεων. Αντίστοιχα τα ασύρματα δίκτυα έχουν σχεδιαστεί ώστε να διεκπεραιώνουν την επικοινωνία μεταξύ συσκευών που κινούνται ελεύθερα στο χώρο. Η διάκριση μεταξύ ασύρματων και ενσύρματων δικτύων δεν υφίσταται όταν πρόκειται για συσκευές που βρίσκονται σε σταθερές θέσεις. Ωστόσο οι πρώτες εφαρμογές της ασύρματης επικοινωνίας στο βιομηχανικό αυτοματισμό αφορούν σταθερές θέσεις. Σίγουρα όμως τα ασύρματα δίκτυα στηρίζονται και στα ενσύρματα αφού για τη λειτουργία ενός ασύρματου δικτύου είναι απαραίτητη η ενσύρματη σύνδεση με ένα υπολογιστή ή με ένα ενσύρματο δίκτυο κορμού (backbone), μία πηγή ισχύος και πομποδέκτες.

### Κόστος ανάπτυξης

Στον οικονομικό τομέα, η εκτίμηση του συνολικού κόστους ενός ενσύρματου δικτύου είναι εύκολη αφού προκύπτει αθροίζοντας τα κόστη των καλωδίων, των κόμβων, των συνδέσεων και της εγκατάστασης αυτών. Αντίστοιχα, στα ασύρματα δίκτυα, το συνολικό κόστος είναι πιο δύσκολο να υπολογιστεί, αφού προκύπτει από το κόστος της καλωδίωσης στα σημεία πρόσβασης, από το πλήθος των σημείων πρόσβασης που θα απαιτηθούν, από το κόστος του εξοπλισμού πρόσβασης, από το κόστος των ασύρματων διεπαφών και από το κόστος συντήρησης.

Συγκριτικά, το κόστος ενός ενσύρματου δικτύου εξαρτάται εν πολλοίς από το κόστος εγκατάστασης των καλωδίων, το οποίο μπορεί να είναι από αμελητέο έως και εξαιρετικά σημαντικό. Το κόστος ενός ασύρματου δικτύου εξοικονομεί οικονομικούς πόρους από την ανάγκη εγκατάστασης καλωδίωσης, ωστόσο επιβαρύνεται από το γεγονός ότι οι αισθητήρες διαθέτουν πομποδέκτη ασύρματης επικοινωνίας, καθώς και από το πλήθος των σημείων πρόσβασης που απαιτούνται, ειδικά σε πρωτόκολλα που απαιτούν οπτική επαφή μεταξύ των συσκευών. Έτσι, είναι εφικτό να συγκριθεί το κόστος μεταξύ ενσύρματων και ασύρματων μόνο μελετώντας κάποια συγκεκριμένη εφαρμογή.

### Τροφοδοσία ισχύος

Ένα αξιοσημείωτο πρόβλημα των ασύρματων συσκευών είναι η ανάγκη χρήσης κινητής πηγής ενέργειας, οπότε η λειτουργία τους εξαρτάται σε μεγάλο βαθμό από τις



μπαταρίες που χρησιμοποιούν, ή από άλλες μορφές παροχής ενέργειας (π.χ φόρτιση από φωτοβολταϊκή κυψέλη. Η χρήση μπαταρίας, στην περίπτωση ασύρματων αισθητήρων, μπορεί να διαρκεί μέχρι και 2 έτη, ωστόσο σε πιο σύνθετες συσκευές (όπως οι συσκευές ελέγχου), η κατανάλωση ενέργειας είναι σημαντική, οπότε είναι απαραίτητη η χρήση ενσύρματης πηγής ενέργειας. Το γεγονός αυτό, αφαιρεί το πλεονέκτημα της φορητότητας, ωστόσο είναι ένας απαραίτητος συμβιβασμός.

Από την πλευρά των ενσύρματων δικτύων, η τροφοδοσία ισχύος γίνεται με καλώδια που μπορούν να τοποθετούνται παράλληλα με τα καλώδια δικτύου, οπότε δεν αντιμετωπίζεται κάποιο ιδιαίτερο πρόβλημα τροφοδοσίας ισχύος. Ωστόσο, νεότερες τεχνολογίες, όπως το πρότυπο IEEE 802.3af Power over Ethernet (PoE) δίνουν τη δυνατότητα να αποφύγουμε ακόμη και τα καλώδια ισχύος, τροφοδοτώντας τις συσκευές μέσω των καλωδίων δικτύου. Σημειώνεται όμως ότι η χρήση της παραπάνω τεχνολογίας δεν θεωρείται ακόμη αρκετά δημοφιλής σε βιομηχανικές εφαρμογές.

## Απώλεια επικοινωνίας

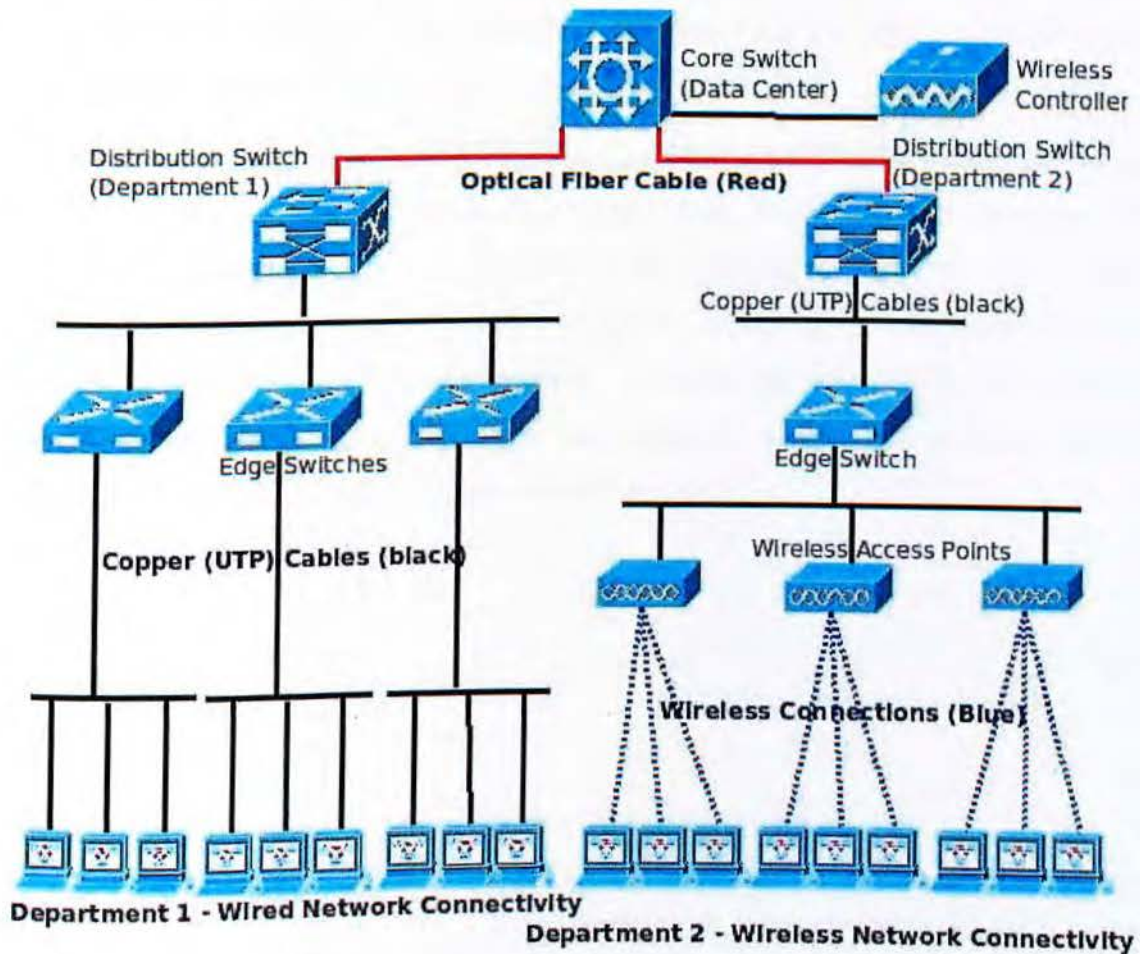
Το σημαντικότερο πρόβλημα που παρουσιάζουν τα ασύρματα δίκτυα έχει να κάνει με την απώλεια ή την εξασθένηση του σήματος. Στις αρχές του 21<sup>ου</sup> αιώνα τα σύρματα δίκτυα εξακολουθούν να υποφέρουν από ορισμένα «νεκρά» σημεία, τα οποία αντιστοιχούν σε μικρές περιοχές όπου υπάρχει απώλεια του σήματος. Ακόμα και στην περίπτωση που το ασύρματο δίκτυο σχεδιαστεί πολύ προσεκτικά είναι σχεδόν αδύνατο να εκλείψουν αυτά τα «νεκρά» σημεία, αφού στην καλύτερη περίπτωση θα μετατραπούν σε «ζωντανά» σημεία με εξασθενημένο σήμα. Η απώλεια της επικοινωνίας είναι ένα από τα μεγαλύτερα προβλήματα που αντιμετωπίζουν τα ασύρματα δίκτυα. Αυτή η απώλεια σήματος που παρουσιάζουν τα ασύρματα δίκτυα μπορεί να προκληθεί από την παρεμβολή άλλων σημάτων που υπάρχουν στο ίδιο φασματικό πεδίο ή από τη μετακίνηση του εξοπλισμού. Επίσης υπάρχει μεγάλη πιθανότητα να δημιουργηθεί ένα «ζωντανό» σημείο από ανάκλαση του σήματος σε κάποιο γειτονικό αντικείμενο. Νεκρά σημεία παρατηρούνται συχνά στο εσωτερικό των κτηρίων. Επίσης, κατά της διάδοση του σήματος μέσα από στερεά παρατηρείται εξασθένηση. [2]

## Σύγκριση υλικού (hardware)

Στη συνέχεια, επιχειρώντας να κάνουμε μία γενικότερη σύγκριση της ασύρματης με την ενσύρματη τεχνολογία, χρησιμοποιούμε το παρακάτω απλό παράδειγμα. Τοποθετούμε



ένα ενσύρματο και ένα ασύρματο δίκτυο το ένα δίπλα στο άλλο. Τα δίκτυα αυτά παρουσιάζονται στην εικόνα 7 της επόμενης σελίδας. Με τη βοήθεια αυτής της εικόνας θα συγκρίνουμε τα εξαρτήματα που χρησιμοποιούνται στο ασύρματο και στο ενσύρματο δίκτυο. Όπως φαίνεται στην εικόνα 7 οι συσκευές του αριστερού δικτύου συνδέονται ενσύρματα, ενώ οι συσκευές του δεξιού δικτύου συνδέονται ασύρματα. Το αριστερό δίκτυο είναι πλήρως καλωδιωμένο, οπότε όλες οι συσκευές συνδέονται απευθείας στις θύρες των μεταγωγέων (edge switch ports) χρησιμοποιώντας καλώδια χαλκού (UTP). Αντίστοιχα το δεξιό δίκτυο είναι πλήρως ασύρματο, οπότε όλες οι συσκευές συνδέονται ασύρματα με τα σημεία πρόσβασης (access points). Στο ενσύρματο δίκτυο οι μεταγωγείς (edge switch) και τα σημεία πρόσβασης (access points) συνδέονται με τους μεταγωγείς διανομής (distribution switches). Με τη σειρά τους οι μεταγωγείς διανομής (distribution switches) συνδέονται στον κεντρικό μεταγωγέα (core switch) στο κέντρο δεδομένων (data center) με χρήση οπτικών ινών. Αντίστοιχα στο ασύρματο δίκτυο υπάρχει ένας ασύρματος ελεγκτής ο οποίος συνδέεται με τον κεντρικό μεταγωγέα (core switch) και είναι αρμόδιος για τη διαχείριση όλων των σημείων πρόσβασης (access points).



Εικόνα 7 – Παράδειγμα σύγκρισης ενός ενσύρματου με ένα ασύρματο δίκτυο. [9]

Συνοψίζοντας παρουσιάζουμε τις διαφορές που εμφανίζει το ασύρματο δίκτυο σε σχέση με το ενσύρματο.

- Το ασύρματο δίκτυο διαθέτει ένα μεταγωγέα (edge switch), ενώ το ενσύρματο δίκτυο τρεις.
- Το ασύρματο δίκτυο διαθέτει τρία ασύρματα σημεία πρόσβασης (access points) για τη σύνδεση των συσκευών με το δίκτυο.
- Τα μεμονωμένα καλώδια που καταλήγουν σε κάθε συσκευή, καθώς και τα υπόλοιπα παθητικά στοιχεία του ενσύρματου δικτύου είναι αισθητά λιγότερα στο ασύρματο δίκτυο, αφού σε αυτό, καλώδια υπάρχουν μόνο στα σημεία πρόσβασης και όχι σε κάθε συσκευή ξεχωριστά.
- Στο ασύρματο δίκτυο οι συσκευές συνδέονται απευθείας με χρήση ασύρματων προσαρμογέων (wireless adaptors) και ασύρματων καρτών.
- Το ασύρματο δίκτυο διαθέτει ένα ασύρματο ελεγκτή ο οποίος παρέχει κεντρική διαχείριση των ασύρματων σημείων πρόσβασης (access points).
- Ο κεντρικός μεταγωγέας (core switch), οι μεταγωγείς διανομής (distribution switches), τα καλώδια και τα υπόλοιπα εξαρτήματα είναι ίδια τόσο στο ασύρματο όσο και στο ενσύρματο δίκτυο. [9]

Από τα παραπάνω, προκύπτει το εύλογο συμπέρασμα ότι ένα ασύρματο δίκτυο δεν μπορεί να αντικαταστήσει πλήρως ένα ενσύρματο, διότι πάντα υπάρχουν κομμάτια του δικτύου που υλοποιούνται με ενσύρματη δικτύωση. Επίσης, ως προς το κόστος, είναι ευνόητο ότι, προκειμένου να συγκριθεί το κόστος μεταξύ ενός ασύρματου και ενός ενσύρματου δικτύου, πρέπει να υπολογισθούν τα κόστη της καλωδίωσης αλλά και των τερματικών συσκευών, καθώς ενδέχεται να υπάρχουν ιδιαίτερες συνθήκες που θα καταστήσουν το ένα σύστημα ακριβότερο έναντι του άλλου.



## 3<sup>ο</sup> - ΚΕΦΑΛΑΙΟ

# “ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΑΙΣΘΗΤΗΡΩΝ ΣΤΟ ΒΙΟΜΗΧΑΝΙΚΟ ΑΥΤΟΜΑΤΙΣΜΟ ”

### 3.1 Εισαγωγή

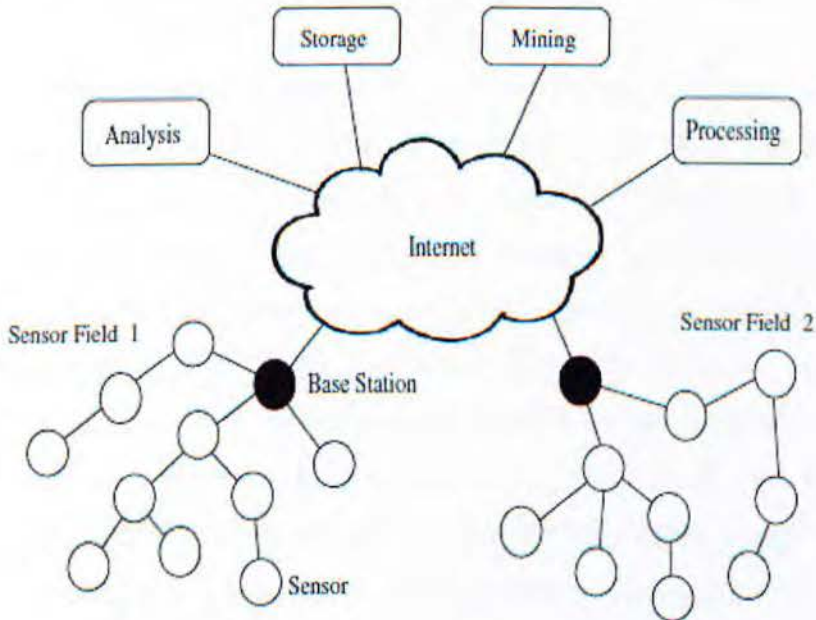
Από τεχνικής άποψης ένας αισθητήρας (sensor) είναι μία συσκευή που μετασχηματίζει παραμέτρους ή γεγονότα από το φυσικό κόσμο, σε σήματα τα οποία είναι εφικτό να μετρηθούν και να αναλυθούν. Ένας άλλος κοινά διαδεδομένος όρος που συναντάται για τη συσκευή αυτή είναι ο χαρακτηρισμός της ως «διάταξη μετατροπής» (transducer) και χρησιμοποιείται για να περιγράψει μία συσκευή η οποία μπορεί να πραγματοποιήσει μετατροπές ενέργειας από μία μορφή σε μία άλλη. Έτσι ένας αισθητήρας είναι στην ουσία μία διάταξη που μετατρέπει την ενέργεια του φυσικού περιβάλλοντος σε ηλεκτρική ενέργεια, η οποία μπορεί να διαβιβαστεί σε ένα υπολογιστικό σύστημα (computing system) ή σε ένα ελεγκτή (controller).

Πολλοί αισθητήρες συνδέονται απευθείας με ελεγκτές και με τους σταθμούς επεξεργασίας (processing stations) χρησιμοποιώντας, για παράδειγμα, LANs. Ταυτόχρονα υπάρχει ένας ολοένα αυξανόμενος αριθμός αισθητήρων, που μεταδίδουν ασύρματα τα επιμέρους δεδομένα που έχουν συλλέξει σε ένα κεντρικό σταθμό επεξεργασίας. Αυτή η δυνατότητα είναι ιδιαίτερα σημαντική, αφού πολλές εφαρμογές δικτύων, οι οποίες αναπτύσσονται σε απομακρυσμένες και δυσπρόσιτες περιοχές, απαιτούν εκατοντάδες ή ακόμα και χιλιάδες κόμβους αισθητήρων. Ως εκ τούτου, ένας ασύρματος αισθητήρας (wireless sensor) δε διαθέτει μόνο τη δυνατότητα της ανίχνευσης. Διαθέτει επίσης τις δυνατότητες της επεξεργασίας, της επικοινωνίας και της αποθήκευσης. Με αυτές τις βελτιώσεις ένας κόμβος αισθητήρα δεν είναι μόνο υπεύθυνος για τη συλλογή δεδομένων. Είναι επίσης υπεύθυνος να πραγματοποιεί αναλύσεις στο εσωτερικό του δικτύου, συσχέτιση και συνένωση τόσο των δεδομένων που αυτός κατέχει όσο και των δεδομένων που προέρχονται από άλλους κόμβους.

Όταν πολλοί αισθητήρες εποπτεύουν από κοινού μεταξύ τους ένα ευρύτερο φυσικό περιβάλλον, τότε σχηματίζουν ένα Ασύρματο Δίκτυο Αισθητήρων (Wireless Sensor Network – WSN). Οι κόμβοι αισθητήρων δεν επικοινωνούν μόνο μεταξύ τους. Επικοινωνούν επίσης με ένα σταθμό βάσης (Base Station - BS) χρησιμοποιώντας τους ασύρματους πομποδέκτες



τους. Με αυτό τον τρόπο υπάρχει η δυνατότητα διάδοσης των δεδομένων τους σε απομακρυσμένα συστήματα επεξεργασίας, απεικόνισης, ανάλυσης και αποθήκευσης. Στην εικόνα που ακολουθεί παρουσιάζεται ως παράδειγμα ένα ασύρματο δίκτυο αισθητήρων με δύο πεδία αισθητήρων, τα οποία εποπτεύουν δύο διαφορετικές περιοχές και συνδέονται με το Internet χρησιμοποιώντας τους σταθμούς βάσης τους. [12]



Εικόνα 8 – Ασύρματο δίκτυο Αισθητήρων. [12]

### 3.2 Βασικά Χαρακτηριστικά ενός Ασύρματου Δικτύου Αισθητήρων

Στην συνέχεια παρουσιάζονται τα βασικότερα στοιχεία της αρχιτεκτονικής ενός Ασύρματου Δικτύου Αισθητήρων (Wireless Sensor Network – WSN). Αυτά τα στοιχεία και οι σχεδιαστικές αρχές πρέπει να εντάσσονται στα πλαίσια του WSN περιβάλλοντος, το οποίο περιγράφεται από όλα ή σχεδόν όλα τα ακόλουθα χαρακτηριστικά:

- Μεγάλο πλήθος αισθητήρων.
- Αυξημένος όγκος ροής δεδομένων.
- Αβέβαια δεδομένα ή δεδομένα με ελλείψεις.
- Υψηλή δυναμική αποτυχία κόμβων
- Υψηλή δυναμική αποτυχία συνδέσεων εξαιτίας παρεμβολών.
- Περιορισμούς στην επεξεργαστική ισχύ.

- Τοπολογία πολλαπλών αλμάτων (multihop).
- Έλλειψη σφαιρικής γνώσης του δικτύου.
- Περιορισμένη διαχειριστική υποστήριξη για το δίκτυο.

Η εξέλιξη ενός WSN δικτύου βασίζεται στα πλεονεκτήματα της τεχνολογίας αισθητήρων, της επικοινωνίας και στη χρήση υπολογιστών (αλγόριθμοι διαχείρισης δεδομένων, υλικού (hardware) και λογισμικού (software)). Τα WSN πρωτόκολλα δρομολόγησης πρέπει να είναι ενημερωμένα όσον αφορά την ενέργεια, προκειμένου να πραγματοποιείται αποτελεσματική διαχείριση των πόρων του WSN δικτύου. Τόσο οι διεργασίες του δικτύου όσο και οι διεργασίες που αφορούν τη δρομολόγηση δεδομένων αποτελούν σημαντικές έννοιες που σχετίζονται άρρηκτα με ένα WSN δίκτυο. Τα ολοκληρωμένα συστήματα δρομολόγησης που έχουν προταθεί για τα κινητά ad-hoc δίκτυα δεν είναι κατάλληλα για τα WSN δίκτυα. Αντίθετα οι τεχνολογίες που έχουν ως επίκεντρο τα δεδομένα είναι απαραίτητες διότι συγκεντρώνουν τα δεδομένα στο εσωτερικό του δικτύου, αποφέροντας ενεργειακά αποδοτική μεταφορά δεδομένων. Τα βασικά στοιχεία της αρχιτεκτονικής ενός WSN δικτύου που μόλις παρουσιάσαμε, έχουν άμεση σχέση με τις σχεδιαστικές παραμέτρους του δικτύου που θα παρουσιάσουμε αναλυτικά στη συνέχεια. [13]

### **3.3 Παράμετροι Σχεδίασης και Αρχιτεκτονικής Ασύρματων Δικτύων Αισθητήρων στο Βιομηχανικό Αυτοματισμό**

Η ανάπτυξη ενός Ασύρματου Δικτύου Αισθητήρων (Wireless Sensor Network – WSN) για βιομηχανικές εφαρμογές, αποτελεί συνδυασμό ειδικών γνώσεων από πολλούς επιστημονικούς τομείς. Οι σημαντικότερες από τις γνώσεις που απαιτούνται και παράλληλα αποτελούν ένα είδος σχεδιαστικής πρόκλησης για τους σχεδιαστές, είναι:

- Η βιομηχανική τεχνογνωσία είναι απαραίτητη για τη γνώση του πεδίου εφαρμογών.
- Η τεχνογνωσία των αισθητήρων είναι απαραίτητη για την κατανόηση θεμάτων που σχετίζονται με τη βαθμονόμηση (calibration), με την μεταβολή των χαρακτηριστικών με την πάροδο του χρόνου (drift), με την ψηφιοποίηση (digitalization), με τη δειγματοληψία (sampling) και με τις διατάξεις μετατροπής (transducers).
- Η τεχνογνωσία των ασύρματων συσκευών και του RF περιβάλλοντος είναι απαραίτητη για την αντιμετώπιση ζητημάτων που σχετίζονται με την καταλληλότητα



της τεχνολογίας, με την ηλεκτρομαγνητική συμβατότητα και με τις ηλεκτρομαγνητικές παρεμβολές που συναντάμε στο βιομηχανικό περιβάλλον.

- Η γνώση της τεχνολογίας των δικτύων είναι απαραίτητη για την κατανόηση των περίπλοκων ιεραρχικών αρχιτεκτονικών που απαιτούνται στα βιομηχανικά WSN.

Στις παραγράφους που ακολουθούν παρουσιάζουμε τις κυριότερες παραμέτρους σχεδίασης ενός WSN δικτύου για βιομηχανικές εφαρμογές. [3]

### 3.3.1 Απόδοση και Ποιότητα Παροχής Υπηρεσιών

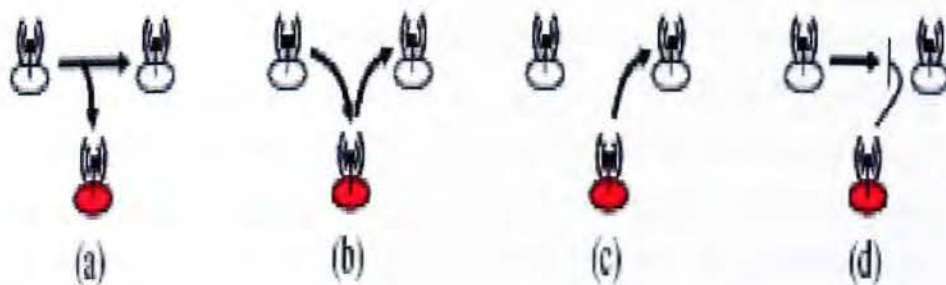
Στα βιομηχανικά δίκτυα WSN η απόδοση μπορεί να εξεταστεί από την άποψη της αξιοπιστίας, της παροχέτευσης δεδομένων, της διακίνησης, της χρονικής καθυστέρησης, της προσαρμοστικότητας και της οικονομικής ανταγωνιστικότητας. Οι παραπάνω παράγοντες μπορούν να χρησιμοποιηθούν για τον καθορισμό της ποιότητας παροχής υπηρεσιών του συστήματος (Quality of Service – QoS).

#### Αξιοπιστία

Η αξιοπιστία σχετίζεται με την ικανότητα του δικτύου να πραγματοποιεί όλες τις λειτουργικές του απαιτήσεις μεταδίδοντας πληροφορίες (σε όλα τα μήκη και τα πλάτη του δικτύου) που σχετίζονται με τις βιομηχανικές εφαρμογές, σε ένα ευρύτατο φάσμα συνθηκών λειτουργίας. Η ικανότητα των δικτύων να αντιμετωπίζουν τις παρεμβολές στην επικοινωνία, τις απρόβλεπτες διακυμάνσεις του ρυθμού διακίνησης δεδομένων και τις εναλλαγές του περιβάλλοντος λειτουργίας, πρέπει να τεθεί υπό μελέτη. Το σύστημα πρέπει να είναι σε θέση να αντιδράσει σε αυτές τις καταστάσεις χρησιμοποιώντας έναν αναμενόμενο, ασφαλή έναντι της αποτυχίας (fail-safe), μηχανισμό ο οποίος σε πολλές περιπτώσεις αναφέρεται ως “ανθεκτικότητα του σχεδιασμού” (robustness of design). Επίσης, στα WSN δίκτυα παρουσιάζονται συχνά ενεργειακοί περιορισμοί, οπότε για να διατηρήσει το δίκτυο την αξιοπιστία του θα πρέπει να έχει την ικανότητα να διατηρήσει τη λειτουργική του ακεραιότητα υπό ενεργειακούς περιορισμούς όπως είναι για παράδειγμα η περίπτωση λειτουργίας με μπαταρία, η περίπτωση λειτουργίας με ενέργεια που προέρχεται από εξωτερικές πηγές (π.χ. ηλιακή ενέργεια, θερμική ενέργεια, αιολική ενέργεια) ή η περίπτωση λειτουργίας με ενέργεια εκτός προδιαγραφών τροφοδοσίας της συσκευής (π.χ. διακύμανση τάσης, συχνότητας κλπ). [3]

## Ασφάλεια

Τα WSN δίκτυα υφίστανται τις κοινές απειλές που βάζουν την ασφάλεια των δικτύων. Οι κυριότερες από αυτές είναι η τροποποίηση μηνυμάτων, η υποκλοπή, η δημιουργία μηνυμάτων, η διακοπή της επικοινωνίας και της λειτουργίας. Επιπρόσθετα, είναι πιθανό να πραγματοποιηθούν επιθέσεις από κακόβουλους που κατέχουν ή δεν κατέχουν πληροφορίες για το δίκτυο. Έτσι είναι επιθυμητό να μπλοκάρονται οι «εξωτερικές» επιθέσεις, ενώ στην περίπτωση «εσωτερικής» επίθεσης φροντίζει η ασφάλεια του συστήματος για την ομαλή αντιμετώπισή της. Στην επόμενη εικόνα παρουσιάζονται μερικές διαφορετικές περιπτώσεις επίθεσης.



*Εικόνα 9 – Διαφορετικοί τύποι επιθέσεων σε WSN δίκτυα.*

*(a) Παρεμβολή (b) Τροποποίηση (c) Δημιουργία (d) Παρεμβολή. [3]*

Τα WSN δίκτυα διαθέτουν ιδιαίτερα χαρακτηριστικά τα οποία επιτρέπουν την ανάπτυξη νέων τρόπων επιθέσεων κατά της ασφαλείας των δικτύων. Οι «παθητικές» επιθέσεις (passive attacks), οι οποίες πραγματοποιούνται με υποκλοπές στις μεταδόσεις, είναι πιθανό, για παράδειγμα, να περιλαμβάνουν την ανάλυση της μετάδοσης των δεδομένων ή τη γνωστοποίηση του περιεχόμενου ενός μηνύματος. Οι «ενεργητικές» επιθέσεις (active attacks) πραγματοποιούνται με τροποποίηση (modification), δημιουργία (fabrication) και παρεμβολή (interruption) οι οποίες σε πολλές περιπτώσεις WSN δικτύων ενδέχεται να περιλαμβάνουν κατάληψη κόμβων (node capturing), επίθεση σε δρομολογήσεις (routing attacks) ή πλημμύρες δεδομένων (flooding). Πρέπει να σημειωθεί επίσης ότι ακόμα και αν τα WSN δίκτυα διαθέτουν περιορισμένους πόρους, ένας «εισβολέας» μπορεί να διαθέτει πιο ισχυρό εξοπλισμό (πχ laptop ή pc) ώστε να κάνει την επίθεση του πιο αποτελεσματική.

Κατά το σχεδιασμό της ασφάλειας ενός ασύρματου δικτύου αισθητήρων πρέπει να διευθετηθούν τόσο οι θεμελιώδεις αρχές ασφάλειας χαμηλού επιπέδου (low level) όσο και οι



θεμελιώδεις αρχές ασφάλειας υψηλού επιπέδου (high level). Οι θεμελιώδεις αρχές ασφάλειας χαμηλού επιπέδου (low level) περιλαμβάνουν τη δημιουργία κλειδιού και τον έλεγχο πρόσβασης, το απόρρητο και την ταυτοποίηση των στοιχείων, την προστασία προσωπικών δεδομένων, την αξιοπιστία έναντι άρνησης επικοινωνίας (Denial of Service), την ασφαλή δρομολόγηση και την αντοχή σε επιθέσεις κατάληψης κόμβων. Αντίστοιχα οι θεμελιώδεις αρχές ασφάλειας υψηλού επιπέδου (high level) περιλαμβάνουν την ασφαλή διαχείριση ομάδων χρηστών, την ανίχνευση εισβολών και την ασφαλή συλλογή δεδομένων. Βέβαια πρέπει να σημειωθεί ότι μερικές από τις παραπάνω λύσεις ενδέχεται να μην εφαρμόζονται εξαιτίας των περιορισμένων πόρων του συστήματος.

Τα WSN δίκτυα που χρησιμοποιούνται στο βιομηχανικό περιβάλλον μπορεί να διαθέτουν και υβριδικές λύσεις. Αυτή η λύση αποτελεί πρόκληση αφού διασπά την ασφάλεια του δικτύου σε δύο κατηγορίες. Στην πρώτη κατηγορία ανήκει η ασφάλεια που παρέχει το δίκτυο συλλογής δεδομένων, η οποία αποτελεί ένα σύνολο από κόμβους αισθητήρων (που έχουν ως αποστολή τη μέτρηση των φυσικών δεδομένων του περιβάλλοντος τους) και έναν ή περισσότερους σταθμούς βάσης (για τη συλλογή των δεδομένων από τους κόμβους και την προώθηση των πληροφοριών ελέγχου που προέρχονται από τους χρήστες). Στη δεύτερη κατηγορία ανήκει η ασφάλεια που παρέχει το δίκτυο διάδοσης δεδομένων, το οποίο αποτελεί ένα συνδυασμό ενσύρματων και ασύρματων δικτύων παρέχοντας σε κάθε χρήστη μία διεπαφή του δικτύου συλλογής δεδομένων. [3]

### **Παροχέτευση**

Η παροχέτευση ορίζει την ικανότητα του δικτύου να πραγματοποιήσει τη διακίνηση των δεδομένων που προέρχονται από τις βιομηχανικές εφαρμογές. Η παροχέτευση επηρεάζεται από το περιβάλλον στο οποίο πραγματοποιείται η επικοινωνία. Συνήθως, το εύρος ζώνης που απαιτείται για τα δεδομένα ενός δικτύου αισθητήρων είναι σχετικά χαμηλό. Ωστόσο, υπάρχει πάντα η πιθανότητα να προκύψουν δεδομένα από πολλαπλούς αισθητήρες σε μικρό χρονικό διάστημα, πράγμα που οδηγεί σε αύξηση του απαιτούμενου εύρους ζώνης, η οποία πρέπει να προσδιοριστεί κατά τη φάση του σχεδιασμού. [3]

### **Χρονική καθυστέρηση, Χρονικό περιθώριο, Χρονική προθεσμία**

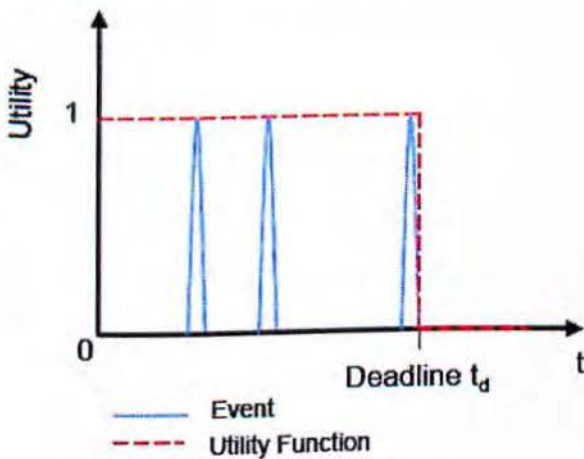
Η χρονική καθυστέρηση (Latency) αντιπροσωπεύει το χρονικό διάστημα που απαιτείται για τη διάδοση των δεδομένων από τον κόμβο του αισθητήρα στο σταθμό βάσης. Οι απαιτήσεις όσον αφορά τη χρονική καθυστέρηση (Latency) εξαρτώνται από την κίνηση που παρατηρείται κατά τη διεκπεραίωση της επικοινωνίας. Για παράδειγμα οι αισθητήρες

ελέγχου σερβοκινητήρων έχουν πιο αυστηρά κριτήρια από τους αισθητήρες που υποστηρίζουν π.χ έναν μάντα μεταφοράς υλικών. Η χρονική καθυστέρηση επηρεάζεται από την πυκνότητα αισθητήρων κάθε κόμβου, από το ρυθμό των αιτήσεων, από την τοπολογία του δικτύου και το πλήθος των ταυτόχρονων ενεργειών.

Εκτός όμως από τη χρονική καθυστέρηση, ορίζονται δύο ακόμα έννοιες για τον καθορισμό των επιδόσεων του δικτύου σε πραγματικό χρόνο. Πρόκειται για το χρονικό περιθώριο (timeliness) και το χρονικό παράθυρο(jitter). Το χρονικό περιθώριο (Timeliness) καθορίζει την απόλυτη προθεσμία που δίνεται στις ενέργειες του δικτύου για να εκτελεστούν ή για να ολοκληρωθούν. Το παράθυρο χρόνου (jitter) καθορίζει το ακριβές χρονικό διάστημα (παράθυρο) εντός του οποίου οι απλές ενέργειες ή οι συντονισμένες ενέργειες πρέπει να εκτελεστούν ή να ολοκληρωθούν. Στην τελευταία περίπτωση παρουσιάζεται σφάλμα αν μία ενέργεια ολοκληρωθεί νωρίτερα. Έτσι το Jitter χρησιμοποιείται συνήθως για τον καθορισμό των απαιτήσεων του συγχρονισμού. Η έννοια του Timeliness και του Jitter παρουσιάζεται στην επόμενη εικόνα χρησιμοποιώντας μία συνάρτηση χρόνου/λειτουργίας (time/utility function). Μία τέτοια συνάρτηση χρησιμοποιείται για να περιγράψει τη χρησιμότητα εκτέλεσης και ολοκλήρωσης μίας συγκεκριμένης ενέργειας σε συνάρτηση με το χρόνο. [3]

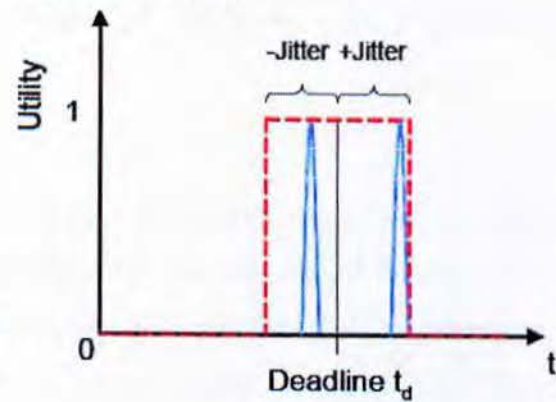
### Time/Utility Function with Demand for:

#### Timeliness



Deadline = deadline for execution

#### Synchronisation



Deadline = point of execution

Εικόνα 10 – Η έννοια του Timeliness και του Jitter. [3]

### Προσαρμοστικότητα

Ένα μεγάλο πλεονέκτημα των WSN δικτύων είναι η ικανότητα τους να προσαρμόζονται τόσο σε νέες ρυθμίσεις όσο και σε νέες αποστολές. Στο βιομηχανικό



περιβάλλον, η ικανότητα προσαρμογής είναι απαραίτητη εξαιτίας της κινούμενης λειτουργίας ορισμένων αισθητήρων, της πιθανής αναδιαμόρφωσης που μπορεί να υποστεί το WSN δίκτυο προκειμένου να χειριστεί νέες διεργασίες ή της πιθανής τροποποίησης που μπορεί να υποστεί το WSN δίκτυο προκειμένου να χειριστεί μία υπάρχουσα διεργασία. Επίσης οι ρυθμίσεις ενός WSN δικτύου είναι πιθανό να αλλάξουν εξαιτίας της απώλειας βασικών εξαρτημάτων, όπως είναι οι κόμβοι μεταγωγής και οι πύλες.

Επίσης είναι πιθανό να αλλάξει το φυσικό βιομηχανικό περιβάλλον με την πάροδο του χρόνου και να προκαλέσει αλλαγές στο ηλεκτρομαγνητικό περιβάλλον. Επιπροσθέτως, είναι πιθανό να υπάρξουν αλλαγές στη ροή των δεδομένων εξαιτίας της αλλαγής θέσης κάποιου αισθητήρα ή εξαιτίας της αλλαγής στον τρόπο χρήσης μίας διεργασίας. Το WSN δίκτυο πρέπει να είναι σε θέση να προσαρμοστεί σε αυτές τις αλλαγές διατηρώντας παράλληλα τα απαιτούμενα επίπεδα διακίνησης, χρονικής καθυστέρησης, απόδοσης, ασφάλειας και αξιοπιστίας. [3]

### **Ανταγωνιστικότητα κόστους**

Το κόστος περιλαμβάνει όλες τις δαπάνες που απαιτούνται από τον ιδιοκτήτη ενός WSN δικτύου. Στις δαπάνες αυτές εντάσσονται οι απαιτήσεις συσκευασίας, οι τροποποιήσεις, η συντήρηση, το κόστος υλοποίησης, το κόστος αντικατάστασης, το κόστος διαχείρισης, το κόστος εκπαίδευσης προσωπικού, καθώς και το κόστος αγοράς ανά μονάδα. Το κόστος πρέπει συνολικά να είναι ανταγωνιστικό σε σχέση με την εγκατάσταση ενσύρματου δικτύου επικοινωνίας.

### **Συνύπαρξη**

Οι παρεμβολές κατά την αποστολή κρίσιμων δεδομένων μπορεί να έχουν δαπανηρές συνέπειες σε επίπεδο οικονομικό, σε επίπεδο ανθρώπινου δυναμικού, ακόμα και στις ζωές των εργαζομένων και του κοινού. Για αυτό ακριβώς το λόγο πρέπει να εξεταστεί η συνύπαρξη WSN δικτύων με άλλα συστήματα τα οποία λειτουργούν στην ίδια ζώνη συχνοτήτων. Η συνύπαρξη με τις άλλες συσκευές πρέπει να εξεταστεί και από την πλευρά του συστήματος και προς την πλευρά του συστήματος. Για παράδειγμα πρέπει να γνωρίζουμε πως μπορεί το σύστημα να μειώσει την επίδραση που ασκεί σε άλλα συστήματα, αλλά και πως μπορεί να μειώσει τις επιδράσεις που ασκούνται σε αυτό από άλλα συστήματα ή από πηγές παρεμβολών. [3]



### 3.3.2 Ισχύς Λειτουργίας

Η κατανάλωση ισχύος αποτελεί ένα σημαντικό σχεδιαστικό περιορισμό για τους ασύρματους αισθητήρες που τροφοδοτούνται από μπαταρία. Οι κόμβοι του δικτύου παραμένουν σε κατάσταση αδράνειας (sleep mode) για σημαντικά χρονικά διαστήματα, προκειμένου να εξοικονομηθεί ενέργεια. Έτσι είναι απαραίτητος ένας αλγόριθμος συγχρονισμού ώστε να εξασφαλίζεται η ταυτόχρονη ενεργοποίηση και απενεργοποίηση των κόμβων. Το περιβάλλον της σχεδίασης πρέπει να προβλέπει την πρόσβαση σε επίπεδο MAC για ενεργούς και απενεργούς κόμβους προκειμένου να μειωθούν οι επιπλέον καθυστερήσεις σωρού (stack) και να καταστεί εφικτός ο ακριβής συγχρονισμός. Η επικοινωνία αποτελεί την πιο απαιτητική, σε κατανάλωση ενέργειας, λειτουργία που εκτελεί ένας κόμβος. Η μετάδοση και η λήψη πακέτων, αλλά και το «άκουσμα» των μεταδόσεων καταναλώνουν ενέργεια. Έτσι κατά τη διαδικασία της σχεδίασης ενός WSN λαμβάνεται υπόψη τόσο η ενέργεια που καταναλώνεται ανά bit όσο και ο ρυθμός μετάδοσης και λήψης των δεδομένων. Σε περίπτωση που αποφασιστεί η χρήση μπαταριών μπορεί, να δημιουργηθούν προβλήματα εξαιτίας του περιορισμένου χρόνου ζωής τους, με αποτέλεσμα να κρίνεται αναπόφευκτη η περιοδική τους αντικατάσταση. Σε αρκετές περιπτώσεις χρησιμοποιούνται ειδικές συσκευές ανάκτησης ενέργειας οι οποίες είναι κατάλληλες για τη λήψη της ενέργειας (ηλιακής, ηλεκτρομαγνητικής και μηχανικής) που περιέχεται στο περιβάλλον γύρω από τις ηλεκτρονικές διατάξεις και τη μετατροπή της σε χρήσιμη ηλεκτρική ενέργεια. [3]

### 3.3.3 Μεταβλητότητα και Επεκτασιμότητα

Τα WSN δίκτυα πρέπει να χαρακτηρίζονται ταυτόχρονα από τις δυνατότητες της μεταβλητότητας και της επεκτασιμότητας. Για παράδειγμα πρέπει να παρουσιάσουν τη δυνατότητα υποστήριξης και μικρού και μεγάλου πλήθους αισθητήρων και επενεργητών (actuators) χωρίς να επηρεάζεται καθόλου η απόδοση του συστήματος. Βέβαια πρέπει να αναλυθούν με μεγάλη προσοχή τα χαρακτηριστικά των διαφόρων συνιστωσών ραδιοεπικοινωνίας του συστήματος. Χαρακτηριστικό παράδειγμα αποτελεί το γεγονός ότι το Bluetooth μπορεί να υποστηρίξει μόνο μέχρι επτά συνδέσεις ανά συσκευή σε μία δομή δικτύου piconet. Επιπρόσθετα κατά την υλοποίηση μίας προσέγγισης που αφορά την ασφάλεια σε ένα ασύρματο δίκτυο αισθητήρων, η δυνατότητα επέκτασης της λύσης είναι ένας ιδιαίτερα σημαντικός παράγοντας. [3]



### 3.3.4 Τοπολογία

Τα δίκτυα πλέγματος έχουν περισσότερες δυνατότητες επέκτασης, προσφέρουν καλύτερη ποιότητα υπηρεσιών και είναι ενεργειακά αποδοτικότερα από τα ισοδύναμα δίκτυα μονού άλματος (single-hop). Επίσης τα δίκτυα πλέγματος προσφέρουν εφεδρεία στην τοπολογία, γεγονός που τα καθιστά πιο ασφαλή έναντι της αποτυχίας αποστολής/λήψης σε ένα κόμβο αφού υπάρχει η δυνατότητα να δρομολογηθούν τα μηνύματα μέσω εναλλακτικών διαδρομών. Στην τοπολογία αστέρα αν ένα σήμα μπλοκαριστεί από μία φυσική ή από μία RF παρεμβολή, το δίκτυο δεν μπορεί να ανακάμψει μέχρι να αφαιρεθεί η πηγή της παρεμβολής.

Προκειμένου να επιτύχουμε εξοικονόμηση ενέργειας στους κόμβους, είναι συχνά απαραίτητο να υπάρχει χαμηλός φόρτος εργασίας σε κάθε κόμβο, πράγμα που προϋποθέτει την υποβάθμιση της ποιότητας των παρεχόμενων υπηρεσιών, ώστε να επιμηκυνθεί ο χρόνος ζωής της μπαταρίας κάθε κόμβου. Όπως είναι αντιληπτό, ο συμβιβασμός αυτός δεν είναι εφικτός σε εφαρμογές πραγματικού χρόνου, οι οποίες προϋποθέτουν συνεχή μετάδοση δεδομένων. Για αυτό το λόγο, η τοπολογία αστέρα συνίσταται για βιομηχανικές εφαρμογές πραγματικού χρόνου με αισθητήρες και επενεργητές, καθώς σε αυτή αποφεύγεται η περιττή διάδοση μηνυμάτων και η ενεργειακή σπατάλη σε κόμβους, πέρα από τους απαραίτητους. Μία υβριδική τοπολογία μπορεί να συνδυάσει τα πλεονεκτήματα που προσφέρονται από τις δύο προαναφερθείσες τοπολογίες δικτύων προσφέροντας αποτελεσματικότητα και ευελιξία. Σε μία υβριδική τοπολογία οι κόμβοι αστέρα (star nodes) ελέγχονται από κόμβους πλέγματος (mesh nodes), για αυτό και τα υβριδικά δίκτυα προσφέρουν αποτελεσματικότητα και ευελιξία. [3]

### 3.3.5 Ασύρματη Εκπομπή

Η χρήση των κατάλληλων τεχνολογιών ραδιοσυχνοτήτων μπορεί να μειώσει την επίδραση παρεμβολών σε ένα ασύρματο δίκτυο. Ένας τρόπος αποφυγής των παρεμβολών είναι η εφαρμογή τεχνικών διαμόρφωσης διάχυτου φάσματος. Οι τεχνικές αυτές προσφέρουν δυνατότητα πολλαπλής πρόσβασης (multiple access), δυνατότητα εξάλειψης της εξασθένισης που προκύπτει από την ύπαρξη πολλαπλών διαδρομών (anti-multipath fading) και δυνατότητα αποφυγής των παρεμβολών (anti-jamming). Οι δύο κυριότερες τεχνικές διάχυτου φάσματος που χρησιμοποιούνται είναι η τεχνική διαμόρφωσης Διάχυτου Φάσματος Άμεσης Ακολουθίας (Direct Sequence Spread Spectrum – DSSS) και η τεχνική διαμόρφωσης Διάχυτου Φάσματος με Μεταπηδήσεις Συχνότητας (Frequency Hopping Spread Spectrum –



FHSS). Οι δύο αυτές τεχνικές έχουν διαφορετικούς φυσικούς μηχανισμούς με αποτέλεσμα να αντιδρούν διαφορετικά στις διάφορες βιομηχανικές ρυθμίσεις που μπορεί να απαιτηθούν. Η επιλογή κάποιας από τις δύο παραπάνω τεχνικές καθορίζεται από τα χαρακτηριστικά της εφαρμογής και από το περιβάλλον.

Οι τεχνικές διαμόρφωσης RF μπορούν να συνδυαστούν με άλλες στρατηγικές για τη βελτίωση της ποιότητας των συνδέσεων στο βιομηχανικό περιβάλλον. Αυτές οι στρατηγικές περιλαμβάνουν ποικιλία καναλιών (channel diversity), ποικιλία διαδρομών (path diversity), χρονική ποικιλία (temporal diversity) και αυξημένη ισχύ εκπομπής. Επίσης, βασικά θέματα που απασχολούν και συσχετίζονται με την ασύρματη δικτύωση στο βιομηχανικό περιβάλλον είναι η μέγιστη εμβέλεια εκπομπής και διάφορα ρυθμιστικά θέματα που αφορούν την ασύρματη τεχνολογία. Επιπρόσθετα, πρέπει να μελετηθεί ο τύπος της κεραίας και πιθανοί περιορισμοί ως προς αυτόν, καθώς είναι ευνόητο ότι η απόδοση μίας κεραίας εξαρτάται από μέγεθος της, από τον τύπο της και από τον προσανατολισμό της. Στον πίνακα που ακολουθεί παρουσιάζονται οι συχνότητες στις οποίες πραγματοποιείται η ασύρματη δικτύωση για την κάλυψη των αναγκών που παρουσιάζουν οι εφαρμογές του βιομηχανικού αυτοματισμού. [3]

Συχνότητα (MHz)	Μέγιστο εύρος ζώνης καναλιού/raster καναλιού (kHz)	Μέγιστη ισοδύναμη εκπεμπόμενη ραδιοισχύς/μέγιστη ένταση μαγνητικού πεδίου	Χρόνος χρήσης της σχετικής συχνότητας
26.957-27.283	Δεν υπάρχουν περιορισμοί	10 mW	Δεν υπάρχουν περιορισμοί
40.660-40.700	Δεν υπάρχουν περιορισμοί	10 mW	Δεν υπάρχουν περιορισμοί
433.050-434.790	Δεν υπάρχουν περιορισμοί	10 mW	Δεν υπάρχουν περιορισμοί
868.000-868.600	Δεν υπάρχουν περιορισμοί	25 mW	< 1%
868.700-869.200	Δεν υπάρχουν περιορισμοί	25 mW	< 0.1%
869.300-869.400	25	10 mW	Δεν υπάρχουν περιορισμοί
869.400-869.650	25	500 mW	< 10%
869.700-870.000	Δεν υπάρχουν περιορισμοί	5 mW	Δεν υπάρχουν περιορισμοί
2400-2483.5	Δεν υπάρχουν περιορισμοί	10 mW	Δεν υπάρχουν περιορισμοί
5725-5875	Δεν υπάρχουν περιορισμοί	25 mW	Δεν υπάρχουν περιορισμοί

*Πίνακας 1 – Συχνότητες που χρησιμοποιούνται για την ασύρματη επικοινωνία στο βιομηχανικό περιβάλλον. [3]*

### 3.3.6 Σύστημα και Λογισμικό (Software)

Το σύστημα οφείλει να απαιτεί το ελάχιστο δυνατό πλήθος παρεμβάσεων από το χειριστή. Για ένα WSN δίκτυο, αυτή η προϋπόθεση θα οδηγούσε σε ένα σύστημα με δυνατότητες αυτό-οργάνωσης (self-organizing), αυτό-ρύθμισης (self-configuring) και αυτό-



ανάκαμψης (self-healing). Οποσδήποτε η χειροκίνητη ρύθμιση και η διαχείριση των WSN δικτύων δεν είναι πρακτική και ως εκ τούτου οι κόμβοι θα πρέπει να είναι σε θέση να αυτο-οργανωθούν. Επιπρόσθετα θα πρέπει να καθίσταται δυνατή η διαχείριση και ο προγραμματισμός των κόμβων ως ένα σύνολο και όχι ως μεμονωμένες συσκευές. Επιπλέον η αρχιτεκτονική του δικτύου πρέπει να υποστηρίζει τα υπάρχοντα (παλαιού τύπου), σταθερής εγκατάστασης πρότυπα και συστήματα (πχ έξυπνοι αισθητήρες και Ethernet).

Το λογισμικό (software) των εφαρμογών θα πρέπει να είναι προσβάσιμο μέσω μίας απλής διασύνδεσης προγραμματισμού εφαρμογών (Application Programming Interface – API) και να προσαρμόζεται εύκολα τόσο σε απαιτήσεις που βασίζονται σε πρότυπα όσο και σε εξειδικευμένες απαιτήσεις πελατών, επιτρέποντας την ταχύτατη ανάπτυξη και εγκατάσταση του δικτύου. Επιπλέον τα WSN δίκτυα πρέπει να επικοινωνούν άψογα με το κεντρικό PLC και τα παραδοσιακά ενσύρματα δίκτυα.

Έπειτα από την ανάπτυξη του δικτύου σε ένα πεδίο, κρίνεται απαραίτητη τόσο η διαχείριση του όσο και η ύπαρξη εργαλείων παρακολούθησης. Μία γραφική απεικόνιση χρήστη θα μπορούσε για παράδειγμα να παρουσιάσει τη συνδεσιμότητα του δικτύου και να παραθέσει τις παραμέτρους των κόμβων. Η διαχείριση του λογισμικού μπορεί να παρέχει την ανάλυση των επιδόσεων ολόκληρου του δικτύου και άλλες δυνατότητες διαχείρισης όπως είναι η ανίχνευση αποτυχημένων κόμβων (με σκοπό την αντικατάσταση), την ανάθεση καθηκόντων ανίχνευσης, την παρακολούθηση της σωστής λειτουργίας του δικτύου, την αναβάθμιση του λογισμικού και την εκτίμηση της ποιότητας παροχής υπηρεσιών. Επίσης πρέπει να εξεταστεί η δυνατότητα αναβάθμισης του ενσωματωμένου λογισμικού (firmware) κάθε συσκευής. [3]

### **Λειτουργικό σύστημα (operating system)**

Το λογισμικό (software) που ενσωματώνεται στους κόμβους πρέπει να έχει τον πλήρη έλεγχο του υλικού τους (hardware). Το λειτουργικό σύστημα πρέπει να υποστηρίζει εφαρμογές στο υψηλότερο επίπεδο οι οποίες να έχουν ως αποστολή τον άμεσο και αποτελεσματικό έλεγχο του υλικού του κατώτερου επιπέδου αν χρειαστεί. Αν δεν υπάρχει πρόσβαση στο στρώμα MAC (Medium Access Control), ο συγχρονισμός θα πρέπει να υλοποιηθεί στο επίπεδο του δικτύου (NTW), πράγμα το οποίο θα εισαγάγει μία επιπρόσθετη καθυστέρηση σωρού (stack) η οποία μπορεί να μην είναι αποδεκτή για ορισμένες εφαρμογές. Μία εναλλακτική λύση θα ήταν να παραμένουν ενεργοί οι κόμβοι διαρκώς, πράγμα το οποίο δε θα ήταν εφικτό από ενεργειακής άποψης. Αξίζει να τονιστεί ότι η καθυστέρηση, η



παροχέτευση και η αξιοποίηση του εύρους ζώνης μπορεί να είναι δευτερεύουσες έννοιες στα WSN δίκτυα, όμως στις βιομηχανικές εφαρμογές μπορεί να αποτελέσουν απαραίτητες ιδιότητες ανάλογα και με τα ιδιαίτερα χαρακτηριστικά της κάθε εφαρμογής.

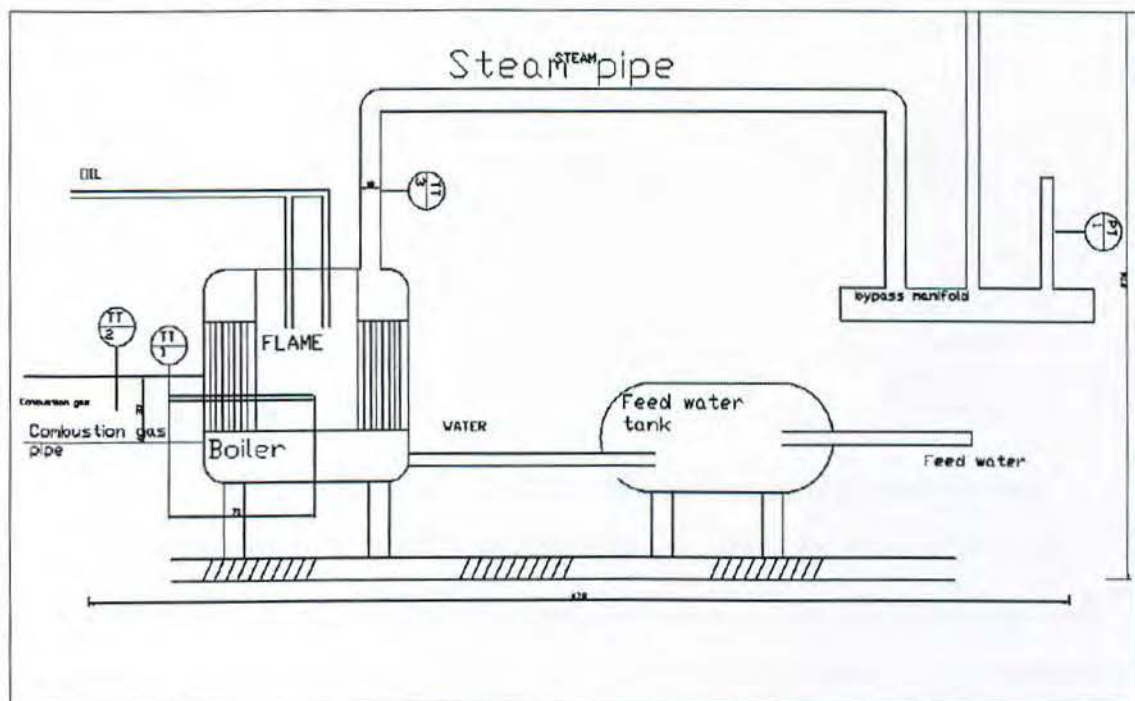
Ένα άλλο παράδειγμα που καταδεικνύει ότι ο έλεγχος του υλικού (hardware) είναι απαραίτητος, είναι η λειτουργία εξοικονόμησης ενέργειας. Για παράδειγμα υπάρχει περίπτωση να χρειάζεται να ελεγχθεί ένας αισθητήρας (πχ ένας on/off αισθητήρας κραδασμών) ο οποίος απενεργοποιείται αμέσως μετά την αποστολή δεδομένων. Εναλλακτικά μπορεί μία εφαρμογή να χρειάζεται να έχει απευθείας πρόσβαση στο ασύρματο RSSI ώστε να ληφθούν αποφάσεις δρομολόγησης. Η παραδοσιακή τμηματική (ανά επίπεδο) αφαίρεση λειτουργιών τόσο για τα δίκτυα, όσο και για το σωρό (stack) του δικτύου, παρουσιάζει αναποτελεσματικότητα. Αντί αυτού θα πρέπει να αναζητηθεί η ισορροπία μεταξύ του ακριβούς ελέγχου του υλικού (hardware) και της ευκολίας με την οποία μπορεί να επιτευχθεί ο γενικότερος σκοπός του προγραμματισμού και η ζητούμενη αποτελεσματικότητα. [3]

### **3.4 Παράδειγμα Χρήσης ενός Ασύρματου Δικτύου Αισθητήρων στο Βιομηχανικό Αυτοματισμό**

Στο ιδιαίτερα απαιτητικό περιβάλλον του βιομηχανικού αυτοματισμού, τα WSN δίκτυα εφαρμόζονται συχνά στα ρουλεμάν των μηχανών, σε αντλίες πετρελαίου και σε κινητήρες. Αισθητήρες κραδασμών (vibration sensors) χρησιμοποιούνται συχνά σε κιβώτια συσκευασίας αλλά και σε κάποιο απρόσιτο ή επικίνδυνο περιβάλλον όπου αποφεύγονται τα καλώδια εξαιτίας της ύπαρξης υγρασίας, ισχυρού μαγνητικού πεδίου και διαφόρων δονήσεων. Στη συνέχεια παρουσιάζεται ένα αντιπροσωπευτικό παράδειγμα χρήσης WSN δικτύου στο βιομηχανικό αυτοματισμό.

Πρόκειται για ένα μικρό σύστημα demo που αναπτύχθηκε στο εργαστήριο μηχανικού ελέγχου του πανεπιστήμιου του Oulu, με σκοπό τη δοκιμή των επιδόσεων ενός WSN δικτύου στο βιομηχανικό περιβάλλον. Ένας λέβητας ατμού παράγει ατμό για μία, εργαστηριακής κλίμακας, χημική διεργασία πολτοποίησης. Στη διεργασία χρησιμοποιείται μαζούτ, μία δεξαμενή αποθήκευσης νερού, ένας λέβητας και αγωγοί. Η θερμοκρασία του νερού τροφοδοσίας είναι περίπου 20 °C και έπειτα από το πέρασμα από το λέβητα παράγεται ατμός με θερμοκρασία γύρω στους 200 °C. Στη διάρκεια της διεργασίας πραγματοποιούνται τέσσερις μετρήσεις. Οι τρεις αφορούν τη θερμοκρασία και η μία την πίεση του ατμού. Στην εικόνα 11 της επόμενης σελίδας φαίνονται οι θέσεις που λαμβάνονται οι μετρήσεις. Η

θερμοκρασία μετριέται από τη φλόγα στο θάλαμο καύσης (με εύρος μέτρησης από τη θερμοκρασία δωματίου έως τους 1500 °C περίπου), από το σωλήνα παροχής φυσικού αερίου (με εύρος μέτρησης από τη θερμοκρασία δωματίου έως λίγο παραπάνω από τους 300 °C) και από την επιφάνεια του σωλήνα του ατμού (με εύρος μέτρησης από τη θερμοκρασία δωματίου έως τους 300 °C περίπου). Η πίεση, η οποία είναι συνήθως γύρω στα 13 bar, μετριέται από παράκαμψη (by-pass) του διανομέα. Βέβαια κατά τη διάρκεια της διακοπής της λειτουργίας και της συντήρησης η τιμή της πίεσης μπορεί να κυμαίνεται από 0 έως 40 bars. [14]

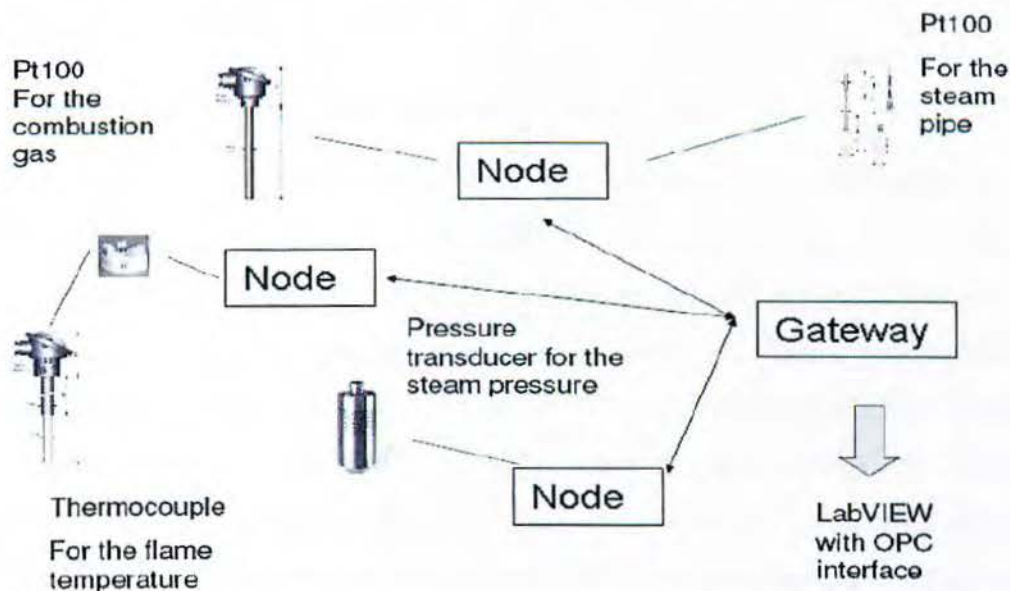


**Εικόνα 11 – Διεργασίες στον ατμολέβητα και λήψη μετρήσεων. [14]**

Οι χαμηλότερες θερμοκρασίες, δηλαδή αυτές από το σωλήνα παροχής φυσικού αερίου και από την επιφάνεια του σωλήνα του ατμού μετρούνται με αισθητήρες Pt-100. Δεδομένου ότι οι μετρήσεις βρίσκονται κοντά η μία στην άλλη, οι αισθητήρες συνδέονται με τον κόμβο που παίζει το ρόλο ενός ασύρματου δικάναλου πομποδέκτη. Η υψηλότερη θερμοκρασία, δηλαδή αυτή που προέρχεται από τη φλόγα στο θάλαμο καύσης, μετράται με το θερμοστοιχείο τύπου-S το οποίο διαθέτει το δικό του κόμβο που παίζει το ρόλο του ασύρματου πομποδέκτη. Για τη λειτουργία του μεταδότη (transmitter) θερμοκρασίας του θερμοστοιχείου απαιτείται εξωτερική πηγή ισχύος. Επιπρόσθετα ο αισθητήρας της πίεσης διαθέτει και αυτός το δικό του κόμβο μετάδοσης (transmitter) και απαιτεί εξωτερική πηγή ισχύος για την τροφοδοσία του. Συνολικά ο εξοπλισμός αποτελείται από τρεις κόμβους και μία πύλη όπως φαίνεται στην εικόνα 12. Η πύλη χρησιμοποιεί τη διασύνδεση OPC η οποία διαβιβάζει πληροφορίες σχετικές με τις μετρήσεις στο σύστημα ανάπτυξης LabVIEW [15]. Αξίζει να



αναφέρουμε ότι ο τυπικός χρόνος άφιξης μίας μέτρησης είναι της τάξεως μερικών δεκάτων του δευτερολέπτου. Το περιβάλλον στο οποίο πραγματοποιείται η δοκιμή χαρακτηρίζεται από δυναμικές πηγές διαταραχών, όπως είναι για παράδειγμα χοντροί τσιμεντένιοι τοίχοι, μεταλλικοί σωλήνες, υγρασία και έντονες θερμοκρασιακές διαφορές.



*Εικόνα 12 – Το WSN δίκτυο και οι αισθητήρες που χρησιμοποιούνται για την παρακολούθηση της θερμοκρασίας και της πίεσης του ατμολέβητα. [14]*

Ένα τέτοιο σύστημα παρακολούθησης θα μπορούσε να χρησιμοποιηθεί ώστε να ενημερώνει το χειριστή για υπερβολικές αλλαγές στην τιμή της πίεσης ή της θερμοκρασίας. Εξαιτίας του ότι η διεργασία είναι σχετικά αργή, οι απαιτήσεις όσον αφορά τις επιμέρους χρονικές προθεσμίες (timeliness) παράδοσης των μηνυμάτων είναι σχετικά χαμηλές. [14]

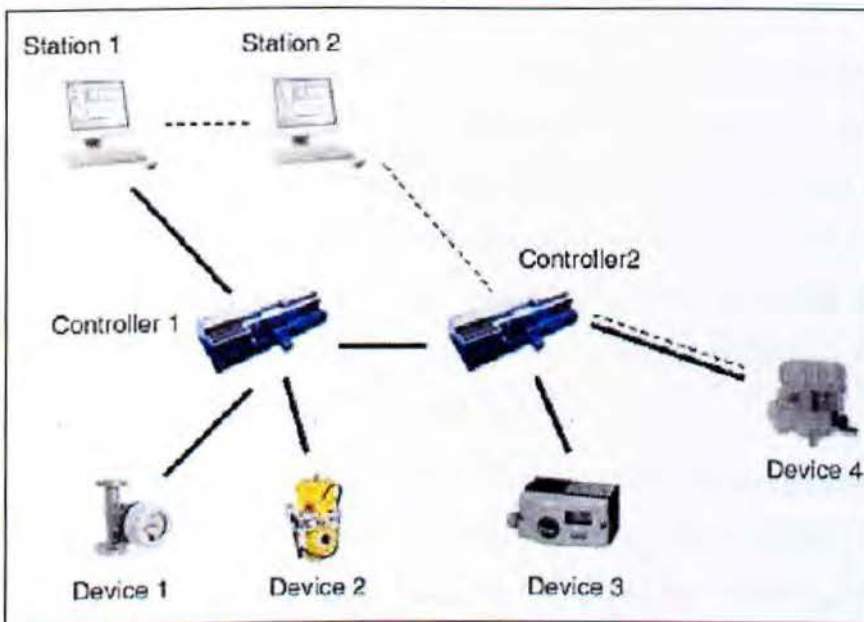


## 4<sup>ο</sup> - ΚΕΦΑΛΑΙΟ

### “ΠΡΩΤΟΚΟΛΛΑ ΑΣΥΡΜΑΤΗΣ ΔΙΚΤΥΩΣΗΣ ΣΤΟ ΒΙΟΜΗΧΑΝΙΚΟ ΑΥΤΟΜΑΤΙΣΜΟ ”

#### 4.1 Ad-hoc Δίκτυα στο Βιομηχανικό Αυτοματισμό

Τα ad-hoc δίκτυα αποτελούνται συνήθως από ένα σύνολο κινητών κόμβων (mobile nodes) οι οποίοι εισέρχονται στο δίκτυο ή εξέρχονται από αυτό, επιφέροντας την ελάχιστη δυνατή επιβάρυνση. Οι κόμβοι του δικτύου επικοινωνούν απευθείας μεταξύ τους εντός της εμβέλειας μετάδοσης που τους χαρακτηρίζει. Σε μεγαλύτερες αποστάσεις χρησιμοποιούνται ενδιάμεσοι κόμβοι ως αναμεταδότες. Ένα ad-hoc δίκτυο χαρακτηρίζεται από αυτό-οργάνωση (self-organized) και από δυνατότητα αυτό-ανάκαμψης (self-healing) σε περίπτωση σφάλματος. Έτσι σε περίπτωση που αποτύχει ένα μονοπάτι μετάδοσης, υπάρχουν εναλλακτικά μονοπάτια τα οποία εγκαθιδρύονται αυτομάτως στη θέση του. Στην επόμενη εικόνα παρουσιάζεται ένα παράδειγμα βιομηχανικού δικτύου ad-hoc. Το κανονικό μονοπάτι δρομολόγησης μεταξύ του σταθμού 1 και της συσκευής 4 αναπαρίσταται με μία συνεχή γραμμή. Σε περίπτωση που αποτύχει κάποιο τμήμα αυτής της διαδρομής, τα δεδομένα μπορούν να δρομολογηθούν εναλλακτικά μέσω μίας νέας διαδρομής η οποία παριστάνεται με διακεκομμένη γραμμή. [16]



Εικόνα 13 – Παράδειγμα ενός βιομηχανικού δικτύου ad-hoc. [16]

Ένα ad-hoc δίκτυο είναι ένα peer to peer δίκτυο πολλαπλών αλμάτων (multihop) και αποτελείται συνήθως από δεκάδες ή ακόμα και από εκατοντάδες κινητούς κόμβους. Τα δίκτυα αυτού του είδους ονομάζονται και «Mobile Ad-hoc Networks» (MANETs). Κάθε κόμβος του δικτύου χαρακτηρίζεται από εμβέλεια μετάδοσης της τάξεως μερικών εκατοντάδων μέτρων. Επίσης κάθε κόμβος του δικτύου πρέπει να είναι σε θέση να δημιουργήσει τόσο τη ροή δεδομένων του χρήστη όσο και τη ροή δεδομένων των εφαρμογών, αλλά και να είναι σε θέση να δράσει ως μεταγωγός (router), ο οποίος πραγματοποιεί τον έλεγχο του δικτύου και των πρωτοκόλλων δρομολόγησης. Το γεγονός ότι οι κόμβοι κινούνται, κάνει τη διαδικασία αυτό-ρύθμισης (self-configuring) του δικτύου σαφώς δυσκολότερη. Επίσης παρά το γεγονός ότι οι κόμβοι του δικτύου τροφοδοτούνται με μπαταρία, η ενεργειακή κατανάλωση δεν αποτελεί μία τόσο σημαντική παράμετρο για τη λειτουργία των ad-hoc δικτύων (σε αντίθεση με τα ασύρματα δίκτυα αισθητήρων) αφού κάθε συσκευή μπορεί να φορτίσει ή να αντικαταστήσει τη μπαταρία της όποτε αυτό κριθεί αναγκαίο, χωρίς να δημιουργηθεί δυσλειτουργία στο υπόλοιπο δίκτυο.

Η ποιότητα υπηρεσιών (Quality of Service – QoS), η οποία αντιστοιχεί στην αποτελεσματική δρομολόγηση των πακέτων, αποτελεί το πιο σημαντικό ζήτημα που αφορά τα ad-hoc δίκτυα και πρέπει να μπορεί να επεκταθεί στα πλαίσια της μεταβαλλόμενης ad-hoc τοπολογίας, του περιορισμένου εύρους ζώνης και της περιορισμένης ισχύος κατά τη μετάδοση. Σε ένα ad-hoc δίκτυο οι κόμβοι πρέπει να μοιράζονται αποτελεσματικά τον ασύρματο τρόπο επικοινωνίας και να είναι σε θέση να εκτελούν δρομολογήσεις για τα διαβιβαζόμενα δεδομένα.

Ένα δύσκολο πρόβλημα που καλείται να αντιμετωπίσει ένα Ad-Hoc δίκτυο είναι το πρόβλημα του κρυμμένου τερματικού (hidden terminal problem). Σε αυτό το πρόβλημα ένας κόμβος θεωρείται τερματικό. Υποθέτοντας ότι την ίδια στιγμή, δύο τερματικά είναι πιθανό να πραγματοποιήσουν αποστολή δεδομένων στο ίδιο κανάλι, αντιμετωπίζουμε τον κίνδυνο παρεμβολών μεταξύ τους, που έχει σαν αποτέλεσμα τη μετάδοση αλλοιωμένων ή μη ολοκληρωμένων. Έτσι, το δίκτυο πρέπει να διασφαλίζει ότι δεν θα εκπέμπουν περισσότερες από μία συσκευές στο ίδιο κανάλι, την ίδια χρονική στιγμή. [17]

Τα ad-hoc δίκτυα προσφέρουν γενικότερα τη δυνατότητα βελτίωσης των κυψελωτών (cellular) λειτουργιών του σήμερα δημιουργώντας νέες τοπολογίες υβριδικών δικτύων με αυξημένη έκταση και καλύτερη κατανομή της κυκλοφορίας των δεδομένων. Στις βιομηχανικές εγκαταστάσεις, η καλή επικοινωνία είναι απαραίτητη, αφού οι πληροφορίες μεταδίδονται μέσω κατάλληλων διαύλων πεδίου κατά μήκος της γραμμής παραγωγής ή κατά



μήκος των εγκαταστάσεων των επιμέρους διεργασιών. Τα ad-hoc δίκτυα χαρακτηρίζονται από εξοικονόμηση του κόστους κατασκευής εξαιτίας της απλότητας σχεδιασμού, της ευκολίας εγκατάστασης και του χαμηλού κόστους συντήρησης που τα χαρακτηρίζει. Όσον αφορά το μέλλον, αυτό το είδος δικτύωσης αναμένεται να υποστηρίξει αποκεντρωμένες (decentralized) αρχιτεκτονικές αυτοματισμού στις οποίες οι διαδικασίες της αίσθησης (sensing), της ενεργοποίησης (actuating), αλλά και οι λειτουργίες ελέγχου θα κατανέμονται ελεύθερα σε ολόκληρη τη βιομηχανική μονάδα.

Κατά τη διάρκεια της σύντομης ιστορίας των ασύρματων ad-hoc δικτύων, έχουν αναπτυχθεί αρκετές λύσεις για την αποτελεσματική αξιοποίηση των δυνατοτήτων τους και για τη λύση των προβλημάτων που σχετίζονται με την ανάπτυξη τους. Πολλές εταιρίες προσφέρουν λύσεις που επιτρέπουν την ad-hoc ασύρματη σύνδεση μεταξύ μικρών και ενεργειακά αποδοτικών συσκευών. Ωστόσο υπάρχουν δύο σημαντικά ζητήματα που σχετίζονται με αυτές τις προσεγγίσεις και οδήγησαν στην ανάπτυξη διαφορετικών ασύρματων προτύπων.

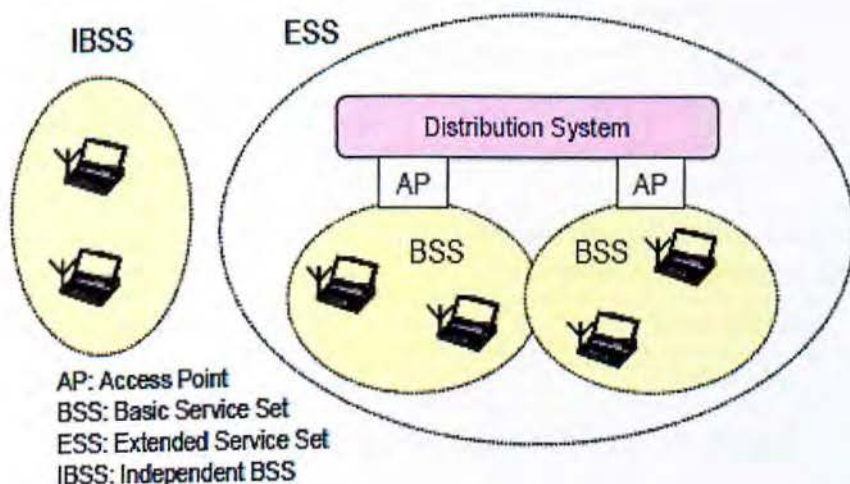
- Το πρώτο από αυτά σχετίζεται με το ζήτημα της συνδεσιμότητας μεταξύ συσκευών. Αν οι συσκευές επικοινωνούν η μία με την άλλη ανεξαρτήτως τύπου και λειτουργίας που εκτελούν, πρέπει να το κάνουν σε μία κοινή πλατφόρμα της οποίας η κύρια λειτουργία αφορά τη διασφάλιση της διαλειτουργικότητας μεταξύ αυτής και άλλων πλατφορμών.
- Το δεύτερο ζήτημα αφορά τους κατασκευαστές προϊόντων που βασίζονται σε ασύρματη ad-hoc συνδεσιμότητα. Ο βασικός εξοπλισμός που παρέχεται από τρίτους κατασκευαστές θα πρέπει να είναι εύκολα αντικαταστάσιμος. Έτσι σε περίπτωση που αποφασίσει κάποιος κατασκευαστής να εγκαταλείψει την αγορά, να είναι εφικτή η εύρεση αντικαταστατών προμηθευτών, που να συμμορφώνονται με τις ίδιες προδιαγραφές.

Ως εκ τούτου, πολλές βιομηχανίες παραγωγής τεχνολογικού υλικού έχουν υιοθετήσει ασύρματα πρότυπα. Τόσο τα αναδυόμενα όσο και τα υφιστάμενα πρότυπα που χρησιμοποιούνται σε σημαντικές βιομηχανικές διεργασίες παρουσιάζονται αναλυτικά στις παραγράφους που ακολουθούν. [16]



## 4.2 Wi-Fi (IEEE802.11a/b/g)

Το Wi-Fi (Wireless Fidelity) περιλαμβάνει τα πρότυπα IEEE 802.11a/b/g και χρησιμοποιείται σε τοπικά ασύρματα δίκτυα (Wireless Local Area Networks – WLANs). Το Wi-Fi επιτρέπει στους χρήστες να συνδέονται ασύρματα με ένα δίκτυο που, μέσω ενός σημείου πρόσβασης (access point - AP) ή σε ένα ad-hoc δίκτυο. Η αρχιτεκτονική του IEEE 802.11 αποτελείται από διάφορες συσκευές οι οποίες αλληλεπιδρούν με σκοπό τη δημιουργία ενός ασύρματου LAN το οποίο υποστηρίζει την κινητικότητα των σταθμών με διαφάνεια προς τα ανώτερα επίπεδα. Η βασική κυψέλη (cell) του IEEE 802.11 LAN καλείται βασικό σύνολο υπηρεσιών (basic service set – BSS) και είναι ένα σύνολο από κινητούς και σταθερούς σταθμούς. Αν ένας σταθμός μετακινηθεί εκτός του BSS του, δε θα μπορεί να επικοινωνεί άμεσα με άλλους σταθμούς η οποίοι ανήκουν ακόμα σε αυτό το BSS. Το πρότυπο IEEE 802.11 βασιζόμενο στο BSS διαχειρίζεται δύο επιπλέον διαμορφώσεις του δικτύου. Το ανεξάρτητο σύνολο βασικών υπηρεσιών (independent basic service set – IBSS) και το εκτεταμένο σύνολο υπηρεσιών (extended service set – ESS). Στην εικόνα που ακολουθεί φαίνεται ότι η λειτουργία IBSS είναι εφικτή όταν οι σταθμοί του IEEE 802.11 είναι σε θέση να επικοινωνούν απευθείας χωρίς τη διαμεσολάβηση κάποιου σημείου πρόσβασης (Access point – AP).



*Εικόνα 14 – Οι διαμορφώσεις IBSS (independent basic service set) και ESS (extended service set) ενός Wi-Fi δικτύου. [18]*

Επειδή αυτός ο τύπος του IEEE 802.11 δικτύου LAN σχηματίζεται συνήθως χωρίς να υπάρξει κάποιο προσχέδιο και μόνο για το διάστημα που υπάρχει ανάγκη χρήσης του δικτύου, αυτός ο τύπος λειτουργίας αναφέρεται συχνά και ως ad-hoc δίκτυο. Αντί να υφίσταται μόνο του ως ένα ανεξάρτητο στοιχείο, το BSS μπορεί να αποτελέσει ένα μέρος της

εκτεταμένης μορφής του δικτύου το οποίο αποτελείται από πολλαπλά BSSs. Το στοιχείο αρχιτεκτονικής που χρησιμοποιείται για τη διασύνδεση των BSSs μεταξύ τους είναι το σύστημα διανομής (distribution system – DS). Το DS σε συνδυασμό με τα APs (access points) επιτρέπουν στο IEEE 802.11 να δημιουργήσει ένα δίκτυο ESS (extended service set) με αυθαίρετο μέγεθος και αυθαίρετη πολυπλοκότητα. Αυτός ο τύπος λειτουργίας αναφέρεται συχνά ως δίκτυο υποδομής (infrastructure network). [18]

Τα τεχνικά χαρακτηριστικά του πρωτοκόλλου ασύρματης δικτύωσης Wi-Fi παρουσιάζονται συγκεντρωμένα στον επόμενο πίνακα.

IEEE προδιαγραφή	802.11 a/b/g
Ζώνη συχνοτήτων	2.4 GHz και 5 GHz
Μέγιστος ρυθμός σήματος (signal rate)	54 Mb/sec
Ονομαστικό εύρος μετάδοσης	100 m
Ονομαστική ισχύς εκπομπής	15 – 20 dBm
Πλήθος RF καναλιών	14 (2.4 GHz)
Εύρος ζώνης καναλιού	22 MHz
Τύπος διαμόρφωσης	BPSK, QPSK, COFDM, CCK, M-QAM
Μέθοδος διάδοσης (διασποράς)	DSSS, CCK, OFDM
Μηχανισμός συνύπαρξης	Δυναμική επιλογή συχνότητας, έλεγχος μεταδιδόμενης ισχύος (802.11 h)
Βασική κυψέλη (cell)	BSS
Μέθοδος επέκτασης βασικής κυψέλης (cell)	ESS
Μέγιστος αριθμός κόμβων κυψέλης (cell nodes)	2007
Κρυπτογράφηση	RC4 ροή κρυπτογράφησης (stream cipher) (WEP), AES μπλοκ κρυπτογράφησης (block cipher)
Πιστοποίηση (authentication)	WPA2 (802.11i)
Προστασία δεδομένων	32-bit CRC

*Πίνακας 2 – Τεχνικά χαρακτηριστικά του Wi-Fi. [18]*

#### 4.2.1 Εφαρμογές του Wi-Fi στο Βιομηχανικό Αυτοματισμό και Οφέλη από τη χρήση του

Στις σύγχρονες βιομηχανικές μονάδες, υπάρχουν αυξημένες απαιτήσεις για παρακολούθηση, έλεγχο, εντοπισμό βλαβών, μεγιστοποίηση της ασφάλειας, ελαχιστοποίηση του χρόνου διακοπής των επιμέρους λειτουργιών. Το Wi-Fi αποτελεί μία ενδιαφέρουσα λύση



για τις βιομηχανικές εφαρμογές, καθότι μπορεί να ενσωματωθεί εύκολα και με χαμηλό κόστος στα υπάρχοντα συστήματα (Ethernet). Η συνδεσιμότητα που χαρακτηρίζει το Wi-Fi προσφέρει ολοκληρωμένες δυνατότητες παρακολούθησης με σημαντική μείωση του κόστους και της πολυπλοκότητας και παράλληλη αύξηση των σημείων πρόσβασης για τη λήψη μετρήσεων. Προσφέρει αύξηση της αξιοπιστίας, απλοποίηση του τρόπου εγκατάστασης και της ικανότητας διαχείρισης και δίνει τη δυνατότητα στους μηχανικούς να λαμβάνουν τις μετρήσεις που χρειάζονται, όταν τις χρειάζονται, με απώτερο στόχο τη βελτιστοποίηση της παραγωγικής διαδικασίας. Οι επιμέρους συσκευές μπορούν συνδεθούν ασύρματα στο Internet, να παρακολουθούνται και να ελέγχονται από ένα κεντρικό σημείο ελέγχου.

Ένα παράδειγμα χρήσης Wi-Fi στη βιομηχανία είναι η απομακρυσμένη παρακολούθηση των μεταβλητών των διεργασιών, καθώς και των συμβάντων. Δηλαδή, με τη χρήση μιας Wi-Fi συσκευής, ο χειριστής μιας βιομηχανικής μονάδας μπορεί να επιτηρεί τις βιομηχανικές διεργασίες, χωρίς να βρίσκεται συνεχώς στο κέντρο ελέγχου (control room). Επίσης, σε περιπτώσεις όπου η εγκατάσταση καλωδίου ενός δικτύου Ethernet συναντά δυσκολίες διέλευσης, είναι εφικτή η γεφύρωση (bridging) δύο άκρων ενός Ethernet δικτύου, με τη χρήση συσκευών ασύρματης γεφύρωσης (wireless bridge). Μια ακόμη εφαρμογή του Wi-Fi είναι η επικοινωνία ενός συστήματος παρακολούθησης με ασύρματες κάμερες. Ο χρήστης, εκτός από την πολύ εύκολη παρατήρηση της εικόνας, μέσω Η/Υ, μπορεί να εισάγει εντολές στο σύστημα, οι οποίες εκτελούνται από κόμβους που συνδέονται ασύρματα (π.χ άνοιγμα-κλείσιμο θυρών, έλεγχος πρόσβασης) [28]

Στην εικόνα που ακολουθεί απεικονίζεται μία συσκευή βιομηχανικού Wi-Fi Ethernet για τη διασύνδεση απομακρυσμένων συσκευών.



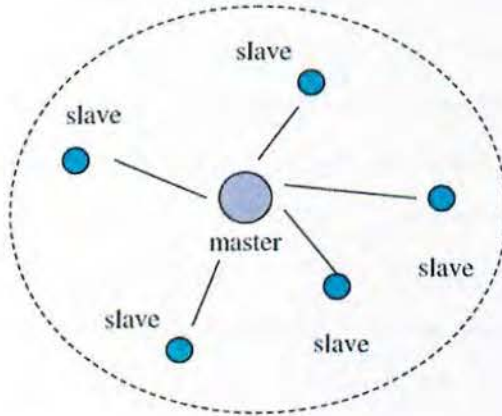
*Εικόνα 15 – Συσκευή βιομηχανικού Wi-Fi Ethernet. [31]*

### 4.3 Industrial Bluetooth

Οι βιομηχανικές μονάδες αποτελούνται από πολλές συσκευές οι οποίες συνδέονται μεταξύ τους με διαφορετικούς τρόπους. Οι κυριότερες από αυτές τις συσκευές είναι μονάδες συλλογής δεδομένων χωρίς ενσωματωμένη νοημοσύνη (built-in intelligence), πιο «έξυπνες» συσκευές (π.χ. αισθητήρες με ενσωματωμένη νοημοσύνη ή ελεγκτές ενός βρόχου ή προγραμματιζόμενοι ελεγκτές) και συστήματα παρακολούθησης τα οποία χρησιμοποιούνται για την καταγραφή δεδομένων και την πραγματοποίηση εποπτικού ελέγχου. Όλες αυτές οι συσκευές συνδέονται μεταξύ τους με διάφορα πρωτόκολλα επικοινωνίας τα οποία σε πολλές περιπτώσεις είναι εφικτό να αντικατασταθούν από την ασύρματη τεχνολογία Bluetooth. [19]

#### 4.3.1 Αρχιτεκτονική Bluetooth

Η επικοινωνία με χρήση της τεχνολογίας Bluetooth βασίζεται σε δύο προϋποθέσεις. Πρώτα πρέπει να γνωρίζουμε τις άλλες συσκευές (γείτονες) που πιθανώς υπάρχουν στην περιοχή (στάδιο ανακάλυψης – discovery) που θέλουμε να χρησιμοποιήσουμε το Bluetooth και δεύτερον πρέπει να υπάρχει ένα προκαθορισμένο κύκλωμα. Η επικοινωνία βασίζεται σε μία αρχιτεκτονική master-slave (αφέντη-σκλάβου). Η αρχιτεκτονική αυτή παρουσιάζεται στην επόμενη εικόνα.

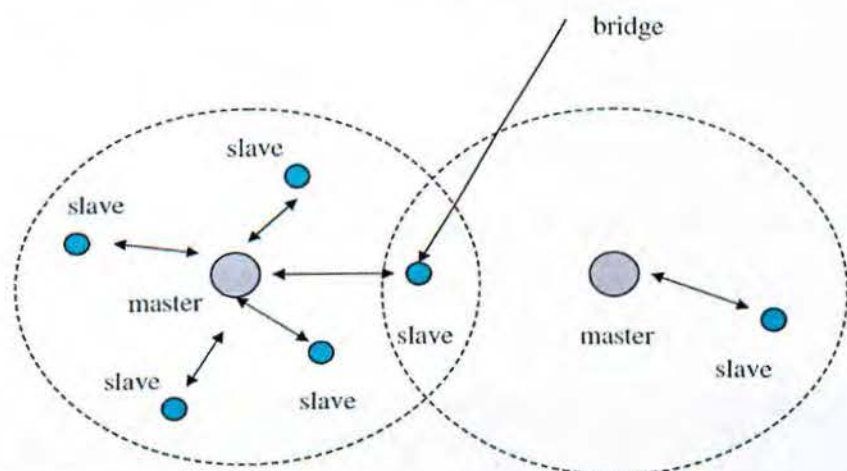


*Εικόνα 16 – Αρχιτεκτονική master/slave για το Bluetooth. [20]*

Στην αρχιτεκτονική αυτή ένα σύνολο συσκευών δημιουργεί μία κυψέλη (cell) η οποία καλείται piconet. Ένα piconet αποτελείται από ένα αφέντη (master) και επτά το πολύ σκλάβους (slaves). Σε ένα piconet η επικοινωνία βασίζεται στον αφέντη (master) ο οποίος είναι υπεύθυνος για την εναρμόνιση των συχνοτήτων και των καναλιών. Αν επικαλυφθούν πολλά piconets θα έχουμε το σχηματισμό ενός scatternet όπως φαίνεται στην εικόνα 16 που



ακολουθεί στην επόμενη σελίδα. Σε ένα piconet οι γείτονες είναι γνωστοί μέσω του σταδίου της ανακάλυψης (discovery phase), ενώ σε ένα scatternet υπάρχει ανάγκη για δρομολόγηση δεδομένων μεταξύ των αφέντηδων (masters) και των κόμβων αναμετάδοσης (relay nodes). Βέβαια πρέπει να τονιστεί ότι τα scatternets δεν έχουν αναπτυχθεί επαρκώς στην τεχνολογία Bluetooth, σε αντίθεση με την τεχνολογία ZigBee που θα παρουσιάσουμε αναλυτικά στη συνέχεια όπου έχουν βελτιωθεί με συγκεκριμένες διαδικασίες δρομολόγησης.



**Εικόνα 17 – Scatternet το οποίο προκύπτει από επικάλυψη πολλών piconets. [20]**

Δύο σκλάβοι (slaves) δεν μπορούν να επικοινωνήσουν απευθείας ο ένας με τον άλλο, παρά μόνο στο στάδιο της ανακάλυψης (discovery phase). Ο αφέντης (master) έχει την ευθύνη της κατανομής των καναλιών και της εγκαθίδρυσης της επικοινωνίας. Παρά το γεγονός ότι σε προηγούμενες εκδόσεις του Bluetooth υπήρχε περιορισμός όσον αφορά τον αριθμό των ταυτόχρονων καναλιών σε ένα piconet, στις σύγχρονες εκδόσεις δεν ισχύει κάτι τέτοιο διότι έχει αυξηθεί σημαντικά η χωρητικότητα της κυψέλης (cell). Το συγκεκριμένο πρότυπο υποστηρίζει επίσης μετάδοση (broadcasting) με μία απλή αφαίρεση της διεύθυνσης του προορισμού από τα προς μετάδοση μηνύματα. Ο αφέντης (master) είναι υπεύθυνος για την καταγραφή των κόμβων και για την κατανομή ή το κλείδωμα του εύρους ζώνης κάθε νέας σύνδεσης. Επίσης είναι υπεύθυνος για τη ρύθμιση του ρολογιού συγχρονισμού του piconet και λαμβάνει αποφάσεις για την ακολουθία μεταπήδησης συχνοτήτων (frequency hopping sequence – FHS). Ένας σκλάβος μπορεί να είναι μέλος πολλών piconets.

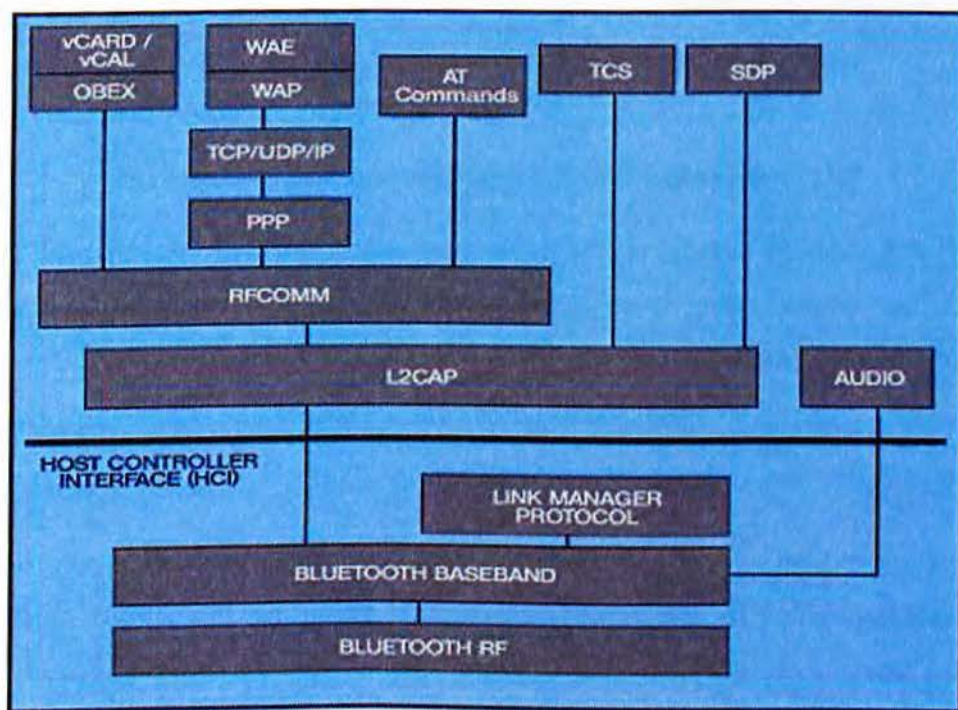
Ένα σημαντικό και ενδιαφέρον χαρακτηριστικό του Bluetooth είναι ότι δεν εξαρτάται από το πρωτόκολλο IP (Internet Protocol). Αυτό το σχεδιαστικό προτέρημα διευκολύνει την ανάπτυξη συσκευών στο δίκτυο, χωρίς να υπάρχει ανησυχία για προβλήματα του ανώτερου επιπέδου (upper layer) όπως η κατανομή των διευθύνσεων, η προεπιλογή μεταγωγέων

(routers), η μάσκα του δικτύου κλπ. Με αυτό τον τρόπο η αυτόματη ρύθμιση του δικτύου γίνεται σαφώς πιο εύκολη.

Στο Bluetooth εντοπίζονται διάφορα επιμέρους πρωτόκολλα:

- Πρωτόκολλα κατώτερου επιπέδου: Baseband, LMP, L2CAP, πρωτόκολλο ανακάλυψης υπηρεσίας (service discovery protocol – SDP).
- Πρωτόκολλα διεπαφής (interfacing): RFCOMM.
- Προδιαγραφές ελέγχου εφαρμογών: Δυαδικό (binary) TCS, εντολές AT.
- Πρωτόκολλα εφαρμογών: PPP, TCP/IP, OBEX, WAP, vCard, VCal, WAE.

Με βάση τα παραπάνω, αντιλαμβανόμαστε ότι στο Bluetooth οι εφαρμογές είναι μέρος των γενικών προδιαγραφών. Η γενική μορφή της αρχιτεκτονικής της στοίβας (stack) παρουσιάζεται στην εικόνα που ακολουθεί. [20]



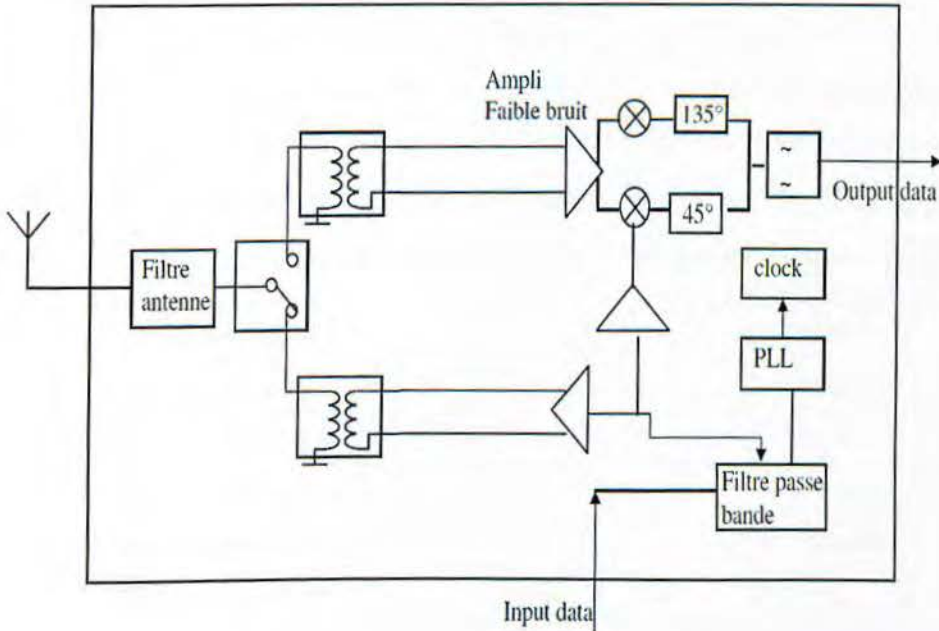
Εικόνα 18 – Γενική μορφή της αρχιτεκτονικής της στοίβας (stack) στο Bluetooth. [20]

### Φυσικό επίπεδο

Το φυσικό επίπεδο βασίζεται (για το βασικό ρυθμό μετάδοσης) στις μεταπηδήσεις συχνότητας με διαμόρφωση GFSK (Gaussian Frequency Shift Keying – Γκαουσιανή Μεταλλαγή Ολίσθησης Συχνότητας). Η διαμόρφωση αυτή προσφέρει στο πρωτόκολλο ρυθμό μετάδοσης της τάξεως των 712 kbps. Σε αυτό το είδος διαμόρφωσης δημιουργείται ένα δυαδικό '1' από μία θετική συχνοτική απόκλιση και ένα δυαδικό '0' από μία αρνητική



συχνοτική απόκλιση. Το πλεονέκτημα της τεχνικής αυτής είναι ότι δεν απαιτεί σύνθετη αποδιαμόρφωση και RF front-ends. Στην εικόνα που ακολουθεί παρουσιάζεται ένα απλοποιημένο chip GFSK διαμόρφωσης.



*Εικόνα 19 – Απλοποιημένο chip GFSK διαμόρφωσης. [20]*

Η μεταπήδηση συχνοτήτων χρησιμοποιείται στις τρέχουσες εκδόσεις του Bluetooth, ως μία στοιχειώδης τεχνική διάχυσης φάσματος. Στο πρότυπο χρησιμοποιούνται 79 κανάλια, αλλά σε ορισμένες περιπτώσεις (ανάλογα και με τη χώρα) είναι πιθανό να χρησιμοποιηθούν και λιγότερα, με αποτέλεσμα τη μείωση του εύρους ζώνης. [20]

### **Επίπεδο βασικής ζώνης**

Το επίπεδο βασικής ζώνης υλοποιεί ένα πολύ μεγάλο μέρος διαδικασιών συνδέοντας τη διαβίβαση των δεδομένων με τη ράδιο-κωδικοποίηση και τη ράδιο-διαμόρφωση. Στο επίπεδο αυτό ορίζεται το ρολόι, οι μορφές των πακέτων δεδομένων, οι ρόλοι αφέντη/σκλάβου, η διαχείριση κατάστασης σύνδεσης/αναμονής, ο έλεγχος ζεύξης, η μετάδοση ήχου, η προώθηση διόρθωσης σφαλμάτων (Forward Error Correction - FEC) και η κωδικοποίηση. [20]

### **4.3.2 Τεχνικά Χαρακτηριστικά του Bluetooth**

Το Bluetooth είναι επίσης γνωστό ως πρότυπο IEEE 802.15.1 και βασίζεται σε ένα ασύρματο σύστημα ραδιοεπικοινωνίας το οποίο είναι ειδικά σχεδιασμένο για φθηνές

συσκευές μικρής εμβέλειας. Αυτό το πρότυπο έχει ως στόχο να αντικαταστήσει τα καλώδια σε περιφερειακές συσκευές υπολογιστών όπως είναι τα ποντίκια, τα πληκτρολόγια, τα joystick και οι εκτυπωτές. Όπως είδαμε και στην προηγούμενη παράγραφο, στο Bluetooth διατίθενται δύο τοπολογίες σύνδεσης: Το piconet και το scatternet. Μία συσκευή Bluetooth μπορεί ταυτόχρονα να λαμβάνει μέρος σε διάφορα piconets, παρέχοντας έτσι τη δυνατότητα να διακινείται η πληροφορία και πέρα από τα όρια της περιοχής κάλυψης ενός μεμονωμένου piconet. Μία συσκευή ενός scatternet μπορεί να είναι σκλάβος (slave) σε διάφορα piconets, όμως αφέντης (master) μπορεί να είναι σε ένα μόνο από αυτά. Τα τεχνικά χαρακτηριστικά του Bluetooth συγκεντρώνονται και παρουσιάζονται στον επόμενο πίνακα. [18]

IEEE προδιαγραφή	802.15.1
Ζώνη συχνοτήτων	2.4 GHz
Μέγιστος ρυθμός μετάδοσης σήματος (signal rate)	1 Mb/sec
Ονομαστικό εύρος μετάδοσης	10 m
Ονομαστική ισχύς εκπομπής	0 – 10 dBm
Πλήθος RF καναλιών	79
Εύρος ζώνης καναλιού	1 MHz
Τύπος διαμόρφωσης	GFSK
Μέθοδος διάδοσης (διασποράς)	FHSS
Μηχανισμός συνύπαρξης	Προσαρμοζόμενες μεταπηδήσεις συχνότητας (adaptive frequency hopping)
Βασική κυψέλη (cell)	Piconet
Μέθοδος επέκτασης βασικής κυψέλης (cell)	Scatternet
Μέγιστος αριθμός κόμβων κυψέλης (cell nodes)	8
Κρυπτογράφηση	E0 ροή κρυπτογράφησης (stream cipher)
Πιστοποίηση (authentication)	Κοινό μυστικό (shared secret)
Προστασία δεδομένων	16-bit CRC

**Πίνακας 3 – Τεχνικά χαρακτηριστικά του Bluetooth. [18]**

### 4.3.3 Ασφάλεια Συστημάτων με Bluetooth

Οι απαιτήσεις ασφάλειας στο Bluetooth εξαρτώνται από τρεις παράγοντες:

- Από το στρατηγικό χαρακτήρα των δεδομένων που ανταλλάσσονται: Στην περίπτωση ενός εσωτερικού δικτύου PAN το οποίο συνδέει συσκευές που βρίσκονται πολύ



κοντά μεταξύ τους, η εμπιστευτικότητα των δεδομένων δεν είναι απαραίτητη. Βέβαια πάντα θα υπάρχει η δυνατότητα να αποκτήσει κάποιος το κατάλληλο υλικό για την εκτροπή των δεδομένων, αλλά αυτό δεν αποτελεί συνήθως στόχο.

- Από την πιθανότητα επιθέσεων: Τα δεδομένα σε ένα ασύρματο δίκτυο μπορεί να είναι «κρίσιμα» για τη λειτουργία του δικτύου (critical data), από τη στιγμή που επηρεάζουν την ορθή λειτουργία του εξοπλισμού. Έτσι τα δίκτυα πρέπει να είναι σωστά ασφαλισμένα.
- Από τις υπηρεσίες: Τυπικά η ασφάλεια είναι περισσότερο σημαντική όταν το Bluetooth χρησιμοποιείται από επαγγελματίες. Έτσι το δίκτυο κάθε επιχείρησης πρέπει να προστατεύεται καλά.

Το πρότυπο Bluetooth περιλαμβάνει μία αποκλειστική οντότητα ασφάλειας που ονομάζεται διαχειριστής ασφάλειας (security manager). Πριν από τη δημιουργία μίας σύνδεσης ο διαχειριστής ασφάλειας αποφασίζει ποια πολιτική ασφάλειας πρέπει να εφαρμοστεί. Η απόφαση του, δηλαδή ο τύπος και το επίπεδο ασφάλειας, καθορίζεται από τον τύπο της υπηρεσίας που χρησιμοποιείται και από την απομακρυσμένη συσκευή με την οποία θα πραγματοποιηθεί η επικοινωνία. Οι πληροφορίες που σχετίζονται με την ασφάλεια και είναι απαραίτητες για τον διαχειριστή ασφάλειας, αποθηκεύονται σε δύο βάσεις δεδομένων. Η πρώτη είναι η βάση δεδομένων των φυσικών συσκευών στην οποία αποθηκεύεται ο τύπος της συσκευής, το επίπεδο αξιοπιστίας της και το μέγεθος των κλειδιών κρυπτογράφησης της. Η δεύτερη είναι η βάση δεδομένων των υπηρεσιών στην οποία αποθηκεύονται πληροφορίες που σχετίζονται με το επίπεδο ασφάλειας των υπηρεσιών και τον τρόπο δρομολόγησης των δεδομένων.

Το Bluetooth ορίζει διάφορα επίπεδα ασφάλειας, τόσο για τις περιφερειακές συσκευές όσο και για τις υπηρεσίες. Κάθε περιφερειακή συσκευή αποκτά μία κατάσταση (status) όταν συνδέεται με μία άλλη περιφερειακή συσκευή για πρώτη φορά. Στα προφίλ γενικής πρόσβασης (generic access profiles – GAP) ορίζονται τρεις τρόποι λειτουργίας:

- Τρόπος λειτουργίας 1 (Κανένας): Σε αυτό τον τρόπο δεν ενεργοποιείται καμία λειτουργία ασφάλειας, με αποτέλεσμα να μπορούν όλες οι συσκευές να συνδεθούν ελεύθερα.
- Τρόπος λειτουργίας 2 (Ασφάλεια στο επίπεδο εφαρμογών): Αυτός ο τρόπος εγγυάται την ασφάλεια μετά την εγκαθίδρυση της σύνδεσης και υποστηρίζει

διάφορους τρόπους ελέγχου με βάση τις εφαρμογές και τις σχετικές λειτουργίες που πραγματοποιούνται στο επίπεδο εφαρμογών.

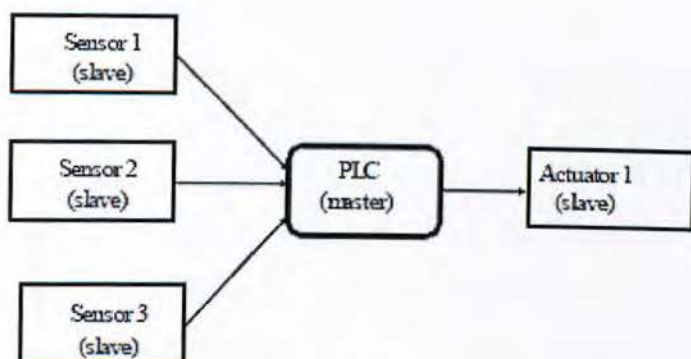
- Τρόπος λειτουργίας 3 (Ασφάλεια στο επίπεδο σύνδεσης): Είναι ο πιο ασφαλής τρόπος λειτουργίας. Ο τρόπος αυτός «κληρονομεί» λειτουργίες από τον τρόπο λειτουργίας 2 προσθέτοντας ένα προκαταρκτικό έλεγχο (αυθεντικοποίηση, κρυπτογράφηση) κατά τη χρονική στιγμή που πραγματοποιείται προσπάθεια σύνδεσης.

Ο τρόπος λειτουργίας 2 εφαρμόζει διαδικασίες ταυτοποίησης κατά την πρόσβαση στις υπηρεσίες. Ο τρόπος λειτουργίας 3 είναι πιο αυστηρός, αφού εκτελεί τη διαδικασία αυθεντικοποίησης (authentication) κατά τη διάρκεια της εγκατάστασης της σύνδεσης. Μετά από μία επιτυχημένη αυθεντικοποίηση (authentication), τα κλειδιά δημιουργούνται πριν την εγκαθίδρυση μιας προστατευμένης κρυπτογραφημένης επικοινωνίας. Εκτός από τους τρεις αυτούς τρόπους λειτουργίας, το Bluetooth προσφέρει δύο επίπεδα ασφάλειας για φυσικές συσκευές (αξιόπιστες ή μη αξιόπιστες). Επίσης ορίζονται επίπεδα εμπιστοσύνης (trust levels). Οι περιφερειακές συσκευές διαθέτουν δύο τιμές εμπιστοσύνης. Την αξιόπιστη και τη μη αξιόπιστη. Έτσι μία αξιόπιστη περιφερειακή συσκευή (αφού περάσει το στάδιο αυθεντικοποίησης) μπορεί να έχει πρόσβαση σε όλες τις υπηρεσίες χωρίς περιορισμό. Η μη αξιόπιστη περιφερειακή συσκευή έχει πρόσβαση σε περιορισμένο αριθμό υπηρεσιών. Κάθε νέα περιφερειακή συσκευή στο δίκτυο, θεωρείται άγνωστη και χαρακτηρίζεται ως μη αξιόπιστη. [20]

#### **4.3.4 Τεχνικές για την Αξιοποίηση των Δυνατοτήτων του Bluetooth στις Βιομηχανικές Επικοινωνίες**

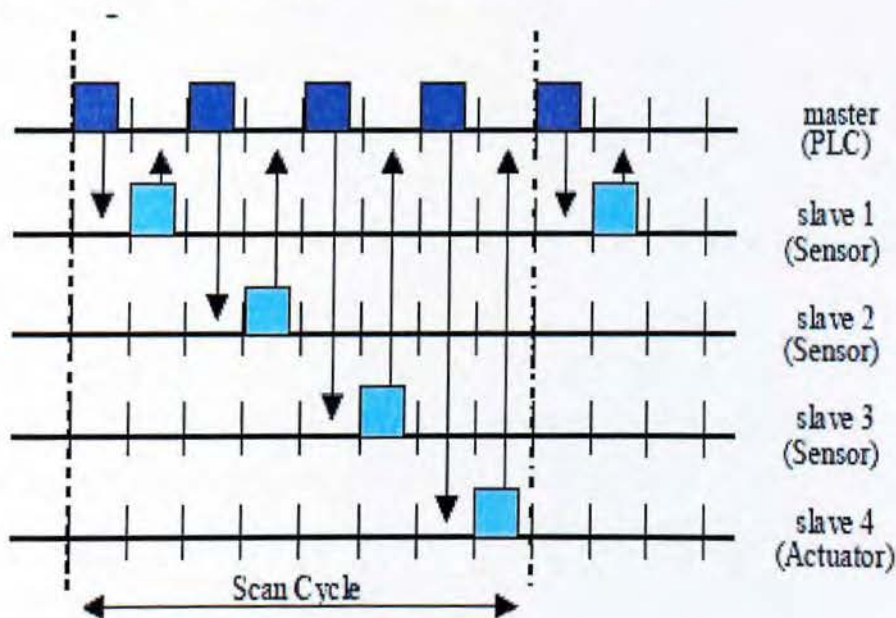
Στην επόμενη εικόνα παρουσιάζεται ένα τυπικό σενάριο, το οποίο αφορά τα καταναμημένα συστήματα ελέγχου διεργασιών (distributed process control systems – DPCSs). Ένας προγραμματιζόμενος λογικός ελεγκτής (programmable logic controller – PLC) επικοινωνεί με αισθητήρες και επεξεργάζεται τα δεδομένα τους ώστε να εξάγει εντολές για τον επενεργητή (actuator). Το πρωτόκολλο επικοινωνίας Bluetooth είναι απολύτως κατάλληλο για αυτή την απλή και ιδιαίτερα δημοφιλή αρχιτεκτονική ελέγχου.





**Εικόνα 20 – Τυπικό σχήμα ελέγχου για καταναμημένα συστήματα ελέγχου διεργασιών (distributed process control systems – DPCSs). [21]**

Αν συνδέσουμε το PLC στον κόμβο του αφέντη (master node) και όλες οι άλλες συσκευές γίνουν σκλάβοι (slaves), μπορούμε να σχηματίσουμε ένα riconet. Μέσα σε ένα κύκλο σάρωσης (scan cycle) ο αφέντης (master) επικοινωνεί με τους αισθητήρες σε μία καθορισμένη αλληλουχία, δίνοντας τους έτσι τη δυνατότητα να μεταδώσουν τα δεδομένα τους και έπειτα στέλνει εντός του ίδιου κύκλου σάρωσης την εντολή στον επενεργητή (actuator). Στην επόμενη εικόνα παρουσιάζεται ένα ενδεικτικό πρόγραμμα μεταδόσεων για ένα riconet που υποστηρίζει το σχήμα ελέγχου της εικόνας 18.



**Εικόνα 21 – Πρόγραμμα μεταδόσεων ενός riconet που υποστηρίζει το σχήμα ελέγχου της εικόνας 18. [21]**

Όπως προαναφέραμε, ο αφέντης (master) του riconet επικοινωνεί με κάθε σκλάβο (slave) καθιστώντας με αυτό τον τρόπο εφικτή τη μετάδοση. Όμως, αυτή η απλή προσέγγιση παρουσιάζει ορισμένες ελλείψεις. Μόνο στην περίπτωση που ο αφέντης (master) ή ο

σκλάβος (slave) έχουν δεδομένα να στείλουν, το MAC πρωτόκολλο του Bluetooth εισάγει επικεφαλίδα (overhead), θυσιάζοντας μία χρονοθυρίδα. Ως εκ τούτου η απόδοση του πρωτοκόλλου και κατά συνέπεια η πραγματική παροχέτευση (throughput), είναι περιορισμένη ειδικά στην περίπτωση ανταλλαγής σύντομων μηνυμάτων. Αυτό συμβαίνει συχνά στα καταναμημένα συστήματα ελέγχου διεργασιών (distributed process control systems – DPCSs) όπου τα μηνύματα που ανταλλάσσονται και ιδιαίτερα αυτά που χαρακτηρίζονται από αυστηρούς χρονικούς περιορισμούς (π.χ. περιοδικές μεταβλητές), είναι μικρά σε μέγεθος. Η επικεφαλίδα μετάδοσης (transmission overhead) επηρεάζει επίσης την καθυστέρηση μετάδοσης του μηνύματος, όπως φαίνεται από την προγραμματισμένη ακολουθία της εικόνας 19.

Αυτοί οι περιορισμοί μπορούν να λυθούν με την καθιέρωση της επικοινωνίας μεταξύ σκλάβων (slave/slave communication – S/S communication). Το τρέχον πρωτόκολλο Bluetooth δεν επιτρέπει την άμεση S/S επικοινωνία. Έτσι αν ένα ζευγάρι σκλάβων (π.χ. «έξυπνοι» αισθητήρες ή επενεργτές) θελήσουν να επικοινωνήσουν μεταξύ τους, αυτό θα πρέπει να γίνει μέσω του αφέντη (master). Ωστόσο στα καταναμημένα συστήματα έλεγχου διεργασιών (distributed process control systems – DPCSs), η περιοδική μετάδοση δεδομένων αποτελεί ένα ιδιαίτερα κοινό φαινόμενο και οι απαιτήσεις μετάδοσης των σκλάβων (slaves) είναι εκ των προτέρων γνωστές. Έτσι η απευθείας επικοινωνία μεταξύ σκλάβων καθίσταται εφικτή και μπορεί να επιφέρει ευεργετικά αποτελέσματα, αφού μπορεί να μειώσει σημαντικά τη γενικότερη επιβάρυνση στο πρωτόκολλο και να εξοικονομήσει εύρος ζώνης. Επίσης η S/S επικοινωνία μικραίνει τη διάρκεια του κύκλου σάρωσης (scan cycle), επιτρέποντας έτσι στο πρωτόκολλο να υποστηρίξει ταχύτερες διεργασίες.

Αφού οι τρέχουσες εκδόσεις Bluetooth δεν υποστηρίζουν την S/S επικοινωνία, κατατέθηκαν διάφορες προτάσεις σχετικές με αυτό το πρόβλημα. Αρχικά προτάθηκε μία προσέγγιση που ονομάζεται «μίσθωση» χρονοθυρίδας (Time-Slot Leasing - TSL), όπου τα προσωρινά piconets καταλαμβάνουν («μισθώνουν») θυρίδες (slots) από το αρχικό piconet με στόχο την υποστήριξη της S/S επικοινωνίας. Αυτή η προσέγγιση καθιστά εφικτή την ύπαρξη πολλαπλών προσωρινών piconets, επιτρέποντας έτσι πολλαπλές επικοινωνίες ταυτόχρονα. Τα προσωρινά piconets παραμένουν συγχρονισμένα ως προς το χρόνο και ως προς τη συχνότητα με τον αρχικό αφέντη (master). Ο αρχικός αφέντης (master) εκτελεί τη λειτουργία ορισμού ενός σκλάβου (slave) ως προσωρινού αφέντη (temporary master) ενός προσωρινού piconet.



Μία άλλη ενδιαφέρουσα προσέγγιση για την ύπαρξη S/S επικοινωνίας στο Bluetooth σχετίζεται με το σκεπτικό της δυναμικής διαχείριση δομής/ρολού. Σύμφωνα με αυτή την προσέγγιση όταν ένας σκλάβος (slave) χρειάζεται να επικοινωνεί συχνά με έναν άλλο σκλάβο (slave), τότε ενεργοποιείται μία εναλλαγή μεταξύ αφέντη (master) και σκλάβου (slave) ή ένας διαμερισμός του riconet. Μια βελτίωση αυτής της τεχνικής μπορεί να πραγματοποιηθεί με την εισαγωγή των τεχνικών εναλλαγής ψευδό-ρόλων (Pseudo Role Switching) και ψευδό-διαμερισμού (Pseudo Partitioning), οι οποίες χρησιμοποιούνται με στόχο τη μείωση της συμφόρησης που παρατηρείται από της διαδοχικές εναλλαγές στην προηγούμενη προσέγγιση.

Ωστόσο όλες αυτές οι προαναφερθείσες προσεγγίσεις επιτρέπουν μόνο επικοινωνία μεταξύ σκλάβων (slaves), περιορίζοντας έτσι τη δυνατότητα εφαρμογής των τεχνικών αυτών στη μεταφορά αρχείων ή σε παρόμοιες εφαρμογές. Αξίζει όμως να τονιστεί ότι οι αρχιτεκτονικές που παρουσιάστηκαν παραπάνω επιτρέπουν στους σκλάβους (slaves) να επικοινωνούν με οποιοδήποτε μέλος μίας ομάδας σκλάβων (slaves), χαρακτηριστικό που καθιστά τις προτεινόμενες προσεγγίσεις απολύτως κατάλληλες για την υποστήριξη των τυπικών αναγκών επικοινωνίας στα κατανεμημένα συστήματα έλεγχου διεργασιών (distributed process control systems – DPCSs). [21]

#### **4.3.5 Εφαρμογές του Bluetooth στο Βιομηχανικό Αυτοματισμό και Οφέλη από τη χρήση του**

Στο βιομηχανικό περιβάλλον, το Bluetooth μπορεί να χρησιμοποιηθεί σε διακοπτόμενες φορητές εφαρμογές ή σε εφαρμογές όπου λειτουργεί μόνιμα και συνεχόμενα. Αν για παράδειγμα υπάρχει μία συσκευή στην άκρη του βραχίονα ενός ρομπότ που πρέπει να επικοινωνεί με ένα ελεγκτή (controller) σε συνεχή βάση, με χρήση Bluetooth μειώνονται τόσο τα καλώδια όσο και η συντήρηση που χρειάζονται.

Επίσης στην περίπτωση που υπάρχουν πίνακες οι οποίοι περιέχουν PLCs ή άλλους ελεγκτές σε διάφορα σημεία μιας βιομηχανικής μονάδας, και είναι απαραίτητη η επικοινωνία ανά τακτά χρονικά διαστήματα, χρησιμοποιούνται φορητές συσκευές ασύρματης σύνδεσης με τα PLC, χωρίς να είναι απαραίτητο να ανοιχθούν οι πίνακες. Έτσι αποφεύγεται οποιοσδήποτε κίνδυνος απευθείας έκθεσης των εσωτερικών εξαρτημάτων του πίνακα σε παράγοντες του βιομηχανικού περιβάλλοντος, όπως είναι η υγρασία και η σκόνη. [30]

Σε πολλές βιομηχανικές μονάδες χρησιμοποιείται σε ελεγκτές (controllers) οι οποίοι είναι κατανεμημένοι σε ολόκληρη τη μονάδα και είναι επιφορτισμένοι με τον έλεγχο των παραγωγικών διεργασιών, των μιάντων μεταφοράς, των μηχανημάτων κλπ. Οι ελεγκτές (controllers) πρέπει να επικοινωνούν τόσο με τις συσκευές που απαρτίζουν τη διεργασία που ελέγχουν, όσο και με το κατανεμημένο σύστημα ελέγχου, προκειμένου να ανταλλάσσει δεδομένα και εντολές. Το Bluetooth συνήθως προσφέρεται ως ενσωματωμένο σε κάποιους ελεγκτές ή ως προσθήκη(add-on), με την εγκατάσταση κάρτας Bluetooth, ώστε να επιτυγχάνεται η επικοινωνία μεταξύ των συσκευών της διεργασίας. Η επικοινωνία των ελεγκτών με το κατανεμημένο σύστημα ελέγχου γίνεται μέσω κλασσικών ενσύρματων δικτύων. Έτσι προσφέρεται συνδεσιμότητα μικρής εμβέλειας και παρέχεται ευέλικτη και αξιόπιστη μετάδοση δεδομένων με στόχο την υποστήριξη της εγκατάστασης, την ενεργοποίηση επιμέρους λειτουργιών και την αποτελεσματική συντήρηση. Ένας τέτοιος ελεγκτής (controller) παρουσιάζεται στην επόμενη εικόνα. [29]



*Εικόνα 22 - Ελεγκτής (controller) με ενσωματωμένο Bluetooth. [29]*

#### 4.4 ZigBee

Το ZigBee είναι ένα πρωτόκολλο κατάλληλο για αποδοτική, χαμηλού ρυθμού και μικρής ισχύος ασύρματη επικοινωνία. Χρησιμοποιείται κυρίως σε διαδικασίες αυτοματισμού, παρακολούθησης και ελέγχου, τόσο σε σταθερά, όσο και σε κινητά συστήματα.. Το ZigBee παρέχει ασύρματη δικτύωση σε μικρές αποστάσεις, είναι επεκτάσιμο (scalable), ασφαλές και χαρακτηρίζεται από αυτό-οργάνωση (self-organizing). Συνήθως

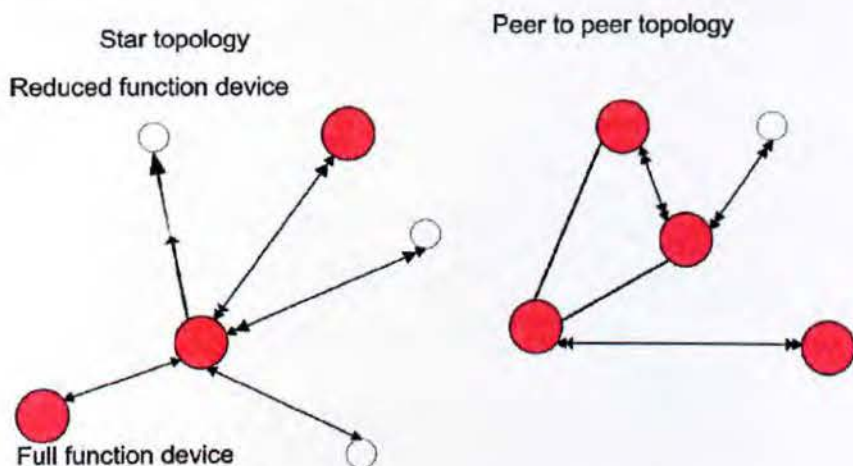


παρέχει δικτύωση πλέγματος (mesh networking) με πολλαπλά άλματα (multi-hop) και υψηλή αξιοπιστία. Η διάρκεια ζωής της μπαταρίας του μπορεί να φτάσει μέχρι και τα δύο χρόνια. Το ZigBee βασίζεται στο πρότυπο IEEE 802.15.4, χρησιμοποιείται σε WPAN δίκτυα χαμηλότερου ρυθμού (lower rate WPAN - LRWPAN) και υποστηρίζει απλές συσκευές οι οποίες καταναλώνουν ελάχιστη ενέργεια και λειτουργούν σε μία ακτίνα της τάξεως των δέκα μέτρων. [18], [22]

#### 4.4.1 Αρχιτεκτονική ZigBee

Το πρότυπο ZigBee έχει ως μοντέλο αναφοράς τη στοίβα του προτύπου IEEE 802.15.4, αφού η αρχιτεκτονική του αναπτύσσεται πάνω από αυτή. Έτσι εκμεταλλεύεται πλήρως τα πλεονεκτήματα του δυναμικού φυσικού ράδιο-επιπέδου του IEEE 802.15.4. Ο συνδυασμός του IEEE 802.15.4 και του ZigBee εξασφαλίζει ολοκληρωμένες και πλήρεις λύσεις για την αγορά και ειδικότερα σε εφαρμογές που έχουν ως βάση τα δίκτυα αισθητήρων. Το ZigBee παρέχει υπηρεσίες όπως είναι η ασφάλεια, η ανακάλυψη (discovery) και η σκιαγράφηση (profiling) για τα δύο επίπεδα που προσδιορίζονται από την ομάδα IEEE.

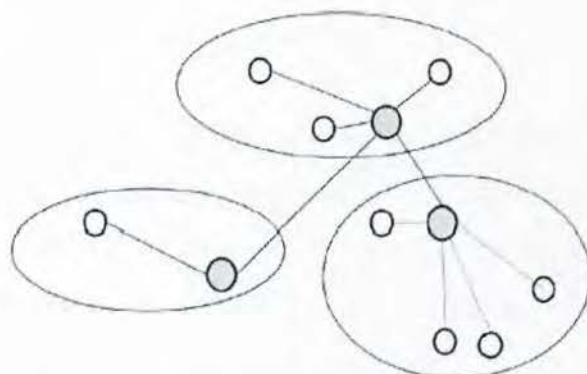
Όπως φαίνεται και από την εικόνα 23 που ακολουθεί, υπάρχουν διαφορετικές τοπολογίες οι οποίες ποικίλλουν από την αρχιτεκτονική αστέρα ή δένδρου μέχρι ένα ολοκληρωμένο δίκτυο πλέγματος (mesh network).



Εικόνα 23 – Τοπολογίες και κατηγορίες κόμβων στο πρότυπο IEEE 802.15.4. [20]

Στην περίπτωση του δικτύου πλέγματος υπάρχει η ανάγκη ενός πρόσθετου πρωτόκολλου δρομολόγησης. Μία πιθανή αρχιτεκτονική του δικτύου πλέγματος

παρουσιάζεται στην επόμενη εικόνα. Η δικτύωση πλέγματος (mesh networking) δίνει τη δυνατότητα αύξησης της εμβέλειας μετάδοσης, αύξησης της αξιοπιστίας (self-healing) και αύξησης της έκτασης των ad-hoc δικτύων, αφού παρέχει εφεδρικά μονοπάτια δρομολόγησης.



*Εικόνα 24 – Τοπολογία πλέγματος. [20]*

Ως εκ τούτου το IEEE 802.15.4 αποτελεί μία χαμηλού ρυθμού μετάδοσης WPAN (low rate – LRWPAN) ασύρματη λύση. Έχει σχεδιαστεί έτσι ώστε να εμφανίζεται απλό για συσκευές μικρής ισχύος και «ελαφριά» ασύρματα δίκτυα. Αυτές οι συσκευές στηρίζονται στη μεγάλη διάρκεια ζωής της μπαταρίας (μέχρι και 2 χρόνια) και δεν διαθέτουν υψηλές επιδόσεις, γι αυτό και δε χρησιμοποιούνται σε εφαρμογές που απαιτούνται υψηλές επιδόσεις. Ορισμένες συσκευές, όπως είναι για παράδειγμα οι αισθητήρες, έχουν υιοθετήσει αυτό το πρότυπο και επωφελούνται από την καλή του απόδοση σε διάφορα πεδία όπως είναι οι στρατιωτικές, οι οικιακές, οι βιομηχανικές, οι εμπορικές και οι περιβαλλοντικές εφαρμογές. [20]

### Φυσικό επίπεδο

Το φυσικό επίπεδο είναι απλό, με μία μικρή ιδιαιτερότητα όσον αφορά τη συχνότητα λειτουργίας. Όπως φαίνεται από την εικόνα που ακολουθεί, οι διαφορετικές διαμορφώσεις εφαρμόζονται σε συνάρτηση με τη συχνότητα του φέροντος.

<u>Band</u>	<u>Applicability</u>	<u>bandwidth</u>	<u>Channels</u>
2.4 GHz	ISM world	250 kbps	16
915 MHz	ISM USA	40 kbps	10
868 MHz	Europe	20 kbps	1

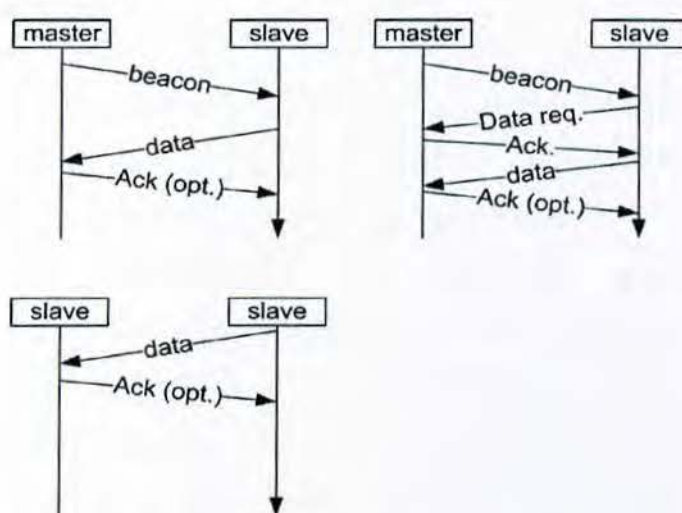
*Εικόνα 25 – Κατανομή καναλιών σε διαφορετικές χώρες. [20]*



Οι πολλές συχνοτικές ζώνες περιορίζουν τη χρήση του προτύπου επειδή μερικές από αυτές δε χρησιμοποιούνται στην Ευρώπη. Ο συνολικός αριθμός καναλιών είναι 27. Τα 16 από αυτά τα κανάλια βρίσκονται στη ζώνη των 2450 MHz, τα 10 στη ζώνη των 915 MHz και το 1 στη ζώνη των 868 MHz.

### Επίπεδο MAC

Στο επίπεδο αυτό λαμβάνει χώρα η πρόσβαση στα κανάλια και η μετάδοση των πλαισίων. Ένας κόμβος μπορεί να είναι «σιωπηλός» σε μία περίοδο contention-free ή σε μία περίοδο contention access (CAP). Η CAP οριοθετείται από την περίοδο μετάδοσης (beacon) και από την περίοδο contention-free, όπως φαίνεται στην εικόνα που ακολουθεί.



Εικόνα 26 – Ανταγωνισμός και τυχαία πρόσβαση. [20]

Βέβαια είναι πιθανό να εκτείνεται μεταξύ δύο μεταδόσεων (beacons) αν δεν υπάρχει περίοδος contention-free. Αυτή η ζώνη είναι δυναμική και μπορεί να μεταβάλλεται με το χρόνο. Όλα τα πλαίσια χρησιμοποιούν το μηχανισμό θυρίδων CSMA/CA και η μετάδοση πρέπει να ολοκληρώνεται (π.χ. συμπεριλαμβάνοντας την επιβεβαίωση εντός του ίδιου υπερπλαισίου). Τα μηνύματα εντολών του επιπέδου MAC, μεταδίδονται σε αυτή τη ζώνη. [20]

### 4.4.2 Τεχνικά Χαρακτηριστικά του ZigBee

Όπως έχει αναφερθεί, το ZigBee ορίζει μέσω του IEEE 802.15.4 WPAN δίκτυα χαμηλού ρυθμού (low rate WPAN – LRWPAN) και υποστηρίζει απλές συσκευές οι οποίες καταναλώνουν χαμηλή ισχύ και λειτουργούν σε μικρή απόσταση μεταξύ τους. Σε ένα LRWPAN δίκτυο συναντάμε δύο διαφορετικούς τύπους συσκευών. Τις συσκευές πλήρους



λειτουργίας (full function devices – FFDs) και τις συσκευές μειωμένης λειτουργίας (reduced function devices – RFDs). Μία συσκευή FFD μπορεί να λειτουργήσει με τρεις τρόπους. Ως PAN συντονιστής, ως απλός συντονιστής και ως απλή συσκευή. Μία FFD συσκευή μπορεί να επικοινωνεί με τις RFD συσκευές ή με άλλες FFD συσκευές, ενώ μία RFD συσκευή μπορεί να επικοινωνεί μόνο με FFD συσκευές. Μία RFD συσκευή προορίζεται για εξαιρετικά απλές εφαρμογές, όπως είναι για παράδειγμα ένας διακόπτης φωτός ή ένας παθητικός αισθητήρας υπέρυθρων. Επίσης δε χρειάζεται να αποστείλει μεγάλες ποσότητες δεδομένων και μπορεί να συνδεθεί με μία μόνο συσκευή FFD κάθε φορά. Κατά συνέπεια μία συσκευή RFD μπορεί να υλοποιηθεί χρησιμοποιώντας ελάχιστους πόρους και ελάχιστη μνήμη. Από τη στιγμή που μία συσκευή FFD ενεργοποιείται για πρώτη φορά, μπορεί να εγκαθιδρύσει το δικό της δίκτυο και να γίνει PAN συντονιστής.

Κάθε δίκτυο αστέρα λειτουργεί ανεξάρτητα από όλα τα υπόλοιπα δίκτυα αστέρα που βρίσκονται ήδη σε λειτουργία. Αυτό επιτυγχάνεται με την επιλογή ενός προσδιοριστή (identifier) PAN ο οποίος δε χρησιμοποιείται από κανένα άλλο δίκτυο εντός της περιοχής ραδιοκάλυψης. Αφού επιλεγεί ο προσδιοριστής (identifier) PAN, ο συντονιστής PAN μπορεί να επιτρέψει και σε άλλες συσκευές να εισέλθουν στο δίκτυο. Μία συσκευή RFD μπορεί να συνδεθεί σε ένα δίκτυο τοπολογίας δέντρου (cluster tree) ως ένας ελεύθερος κόμβος στην άκρη ενός κλάδου, επειδή μπορεί να συνδεθεί με μία μόνο FFD συσκευή κάθε φορά. Οποιαδήποτε από τις συσκευές FFD μπορεί να ενεργήσει ως συντονιστής και να παρέχει υπηρεσίες συγχρονισμού σε άλλες συσκευές ή σε άλλους συντονιστές. Από αυτούς τους συντονιστές, μόνο ένας μπορεί να γίνει γενικός συντονιστής PAN και να διαθέτει περισσότερους υπολογιστικούς πόρους από οποιαδήποτε άλλη συσκευή στο PAN. [18]

Σε ένα δίκτυο ZigBee όλοι οι κόμβοι μοιράζονται το ίδιο κανάλι, με αποτέλεσμα να είναι πολύ μικρή η ευελιξία του τρόπου αξιοποίησης της συχνότητας. Σε ένα τέτοιο δίκτυο δεν παρουσιάζονται μεταπηδήσεις συχνότητας (frequency hopping). Αυτό έχει ως αποτέλεσμα, η μόνη επιλογή ανίχνευσης καναλιού με ελάχιστες παρεμβολές, να παρατηρείται κατά την εκκίνηση. Το ZigBee μπορεί να λειτουργήσει με δύο τρόπους. Ως αναμεταδότης (beaconed mode) και ως μη αναμεταδότης (non-beaconed mode). Στον τρόπο λειτουργίας ως αναμεταδότης (beaconed mode) οι κόμβοι είναι σε κάποιο βαθμό συγχρονισμένοι και το υπερπλαίσιο (superframe) διαιρείται σε 16 θυρίδες (slots). Οι θυρίδες (slots) στο πλαίσιο (frame), βασίζονται στη χρήση CSMA/CA. Υπάρχει επιλογή να χρησιμοποιηθούν μέχρι και επτά από αυτές τις αποκλειστικές θυρίδες (slots) σε συγκεκριμένους κόμβους ώστε να αυξηθεί ο ντετερμινισμός (determinism) του συστήματος.



Οι αποκλειστικές αυτές θυρίδες καλούνται εγγυημένες χρονοθυρίδες (guaranteed slot time – GST). Βέβαια αξίζει να τονιστεί ότι η υποστήριξη αυτής της δυνατότητας δεν είναι υποχρεωτική, αφού η χρήση αυτού του χαρακτηριστικού μπορεί να διαταράξει τη διαλειτουργικότητα του συστήματος. [22]

Συνοψίζοντας πραγματοποιείται συγκεντρωτική παρουσίαση των τεχνικών χαρακτηριστικών του ZigBee στον επόμενο πίνακα.

IEEE προδιαγραφή	802.15.4
Ζώνη συχνότητας	868/915 MHz και 2.4 GHz
Μέγιστος ρυθμός μετάδοσης σήματος (signal rate)	250 Kb/sec
Ονομαστικό εύρος μετάδοσης	10 – 100 m
Ονομαστική ισχύς εκπομπής	(-25) – 0 dBm
Πλήθος RF καναλιών	0.1 και 16
Εύρος ζώνης καναλιού	0.3/0.6 MHz και 2 MHz
Τύπος διαμόρφωσης	BPSK (+ASK) και O-QPSK
Μέθοδος διάδοσης (διασποράς)	DSSS
Μηχανισμός συνύπαρξης	Δυναμική επιλογή συχνότητας (dynamic frequency selection)
Βασική κυψέλη (cell)	Αστέρας (Star)
Μέθοδος επέκτασης βασικής κυψέλης (cell)	Δένδρο (cluster tree), πλέγμα (mesh)
Μέγιστος αριθμός κόμβων κυψέλης (cell nodes)	>65000
Κρυπτογράφηση	AES μπλοκ κρυπτογράφησης (block cipher) (CTR, counter mode)
Πιστοποίηση (authentication)	CBC-MAC (επέκταση του CCM)
Προστασία δεδομένων	16-bit CRC

*Πίνακας 4 – Τεχνικά χαρακτηριστικά του ZigBee. [18]*

#### 4.4.3 Ασφάλεια Συστημάτων με ZigBee

Στη έκδοση του 2006 η ασφάλεια δεν αποτελούσε έναν επιτακτικό παράγοντα των προδιαγραφών. Ωστόσο παρέχεται υποστήριξη για διαδικασίες πιστοποίησης (authentication), ακεραιότητας (integrity) και κρυπτογράφησης (encryption) τόσο για το δίκτυο όσο και για το επίπεδο εφαρμογών. Η ασφάλεια του επιπέδου MAC η οποία είναι διαθέσιμη μέσω του προτύπου 802.15.4 δεν αναφέρεται ρητά στο πρότυπο ZigBee και η χρήση της μπορεί να διαταράξει τη διαλειτουργικότητα μεταξύ προϊόντων προερχόμενων



από διαφορετικούς κατασκευαστές. Η προστασία από επαναλαμβανόμενες επιθέσεις πραγματοποιείται με χρήση διαδοχικής αρίθμησης (sequential numbering). Το ZigBee κάνει χρήση των μηχανισμών ασφάλειας του 802.15.4 μετρώντας με CBC-MAC4 και με κρυπτογράφηση AES-128, με την προϋπόθεση χρήσης μίας μόνο εκ των διαδικασιών κρυπτογράφησης και ακεραιότητας. Οι τύποι κλειδιών που χρησιμοποιούνται είναι τρεις: κλειδί αφέντη (master key), κλειδί σύνδεσης (link key), κλειδί δικτύου (network key). Το master key είναι απαραίτητο για την είσοδο στο δίκτυο. Το link key χρησιμοποιείται για κρυπτογράφηση από άκρη σε άκρη (end to end) και παρέχει με αυτό τον τρόπο τα υψηλότερα δυνατά επίπεδα ασφάλειας έχοντας αντίστοιχα υψηλές απαιτήσεις αποθήκευσης. Το network key μοιράζεται μεταξύ όλων των συσκευών και ως εκ τούτου παρουσιάζει χαμηλότερο επίπεδο ασφάλειας σε συνδυασμό με μειωμένες απαιτήσεις αποθήκευσης στις συσκευές. Όλα τα κλειδιά είναι εφικτό να ρυθμιστούν στο εργοστάσιο ή να διανεμηθούν από το κέντρο αξιοπιστίας (trust center) το οποίο είναι υπό την εποπτεία του συντονιστή του δικτύου ή να διανεμηθούν ασύρματα ή μέσω μίας φυσικής διεπαφής (interface). Στις εμπορικές εφαρμογές, το κέντρο αξιοπιστίας (trust center) μπορεί να ελέγχει την είσοδο νέων συσκευών στο δίκτυο και να ανανεώνει περιοδικά το κλειδί του δικτύου. [22]

#### 4.4.4 Εφαρμογές του ZigBee στο Βιομηχανικό Αυτοματισμό και οφέλη από τη χρήση του

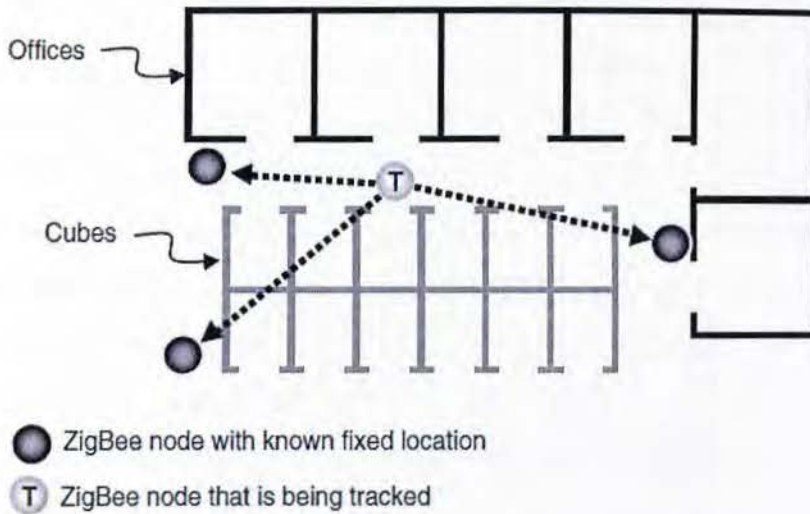
Στο βιομηχανικό αυτοματισμό η δικτύωση πλέγματος (mesh networking) που παρέχει το ZigBee μπορεί να προσφέρει βοήθεια σε τομείς όπως είναι η διαχείριση ενέργειας, ο έλεγχος του φωτισμού, ο έλεγχος των διεργασιών και η διαχείριση των πόρων. Στις παραγράφους που ακολουθούν παρουσιάζονται δύο παραδείγματα χρήσης του ZigBee σε βιομηχανικές εφαρμογές.

##### Διαχείριση των πόρων του δικτύου και παρακολούθηση προσωπικού

Οι παθητικές ετικέτες ταυτοποίησης ραδιοσυχνοτήτων (radio frequency identification – RFID) χρησιμοποιούνται εδώ και πολλά χρόνια. Παρά το γεγονός ότι μία παθητική ετικέτα RFID (passive RFID tag) δε διαθέτει μπαταρία, η μονάδα ανάγνωσης RFID μπορεί να είναι ένα όργανο τροφοδοτούμενο από μπαταρία. Μία παθητική ετικέτα RFID (passive RFID tag) μπορεί να μεταδώσει μόνο απλές πληροφορίες, όπως είναι για παράδειγμα ένας αριθμός ταυτοποίησης ο οποίος αρκεί σε πολλές εφαρμογές διαχείρισης των δυνατοτήτων του δικτύου. Τα ενεργά RFIDs (active RFIDs), όπως είναι οι συσκευές ZigBee, τροφοδοτούνται



από μπαταρία και γενικότερα κοστίζουν ακριβότερα σε σύγκριση με τα παθητικά RFIDs (passive RFIDs). Το ZigBee, που έχει ως βάση τα ενεργά RFIDs (active RFIDs), παρουσιάζει μεγαλύτερη εμβέλεια σε σχέση με τα παθητικά RFIDs (passive RFIDs) και έχει τη δυνατότητα παροχής πρόσθετων υπηρεσιών, όπως για παράδειγμα η εκτίμηση της θέσης που βρίσκονται οι πόροι του δικτύου ή το προσωπικό. Το σκεπτικό, στο οποίο βασίζεται η εκτίμηση της θέσης, παρουσιάζεται στην επόμενη εικόνα όπου παρακολουθείται η θέση του προσωπικού στο εσωτερικό ενός κτηρίου με γραφεία και κλωβούς (cubes).



*Εικόνα 27 – Παρακολούθηση προσωπικού σε ένα κτήριο γραφείων με ZigBee ασύρματη δικτύωση. [23]*

Στο δίκτυο αυτό υπάρχουν τρεις σταθεροί κόμβοι ZigBee για τους οποίους είναι γνωστές οι τοποθεσίες στις οποίες βρίσκονται. Ο κινητός ZigBee κόμβος, ο οποίος μετακινείται από έναν υπάλληλο, εκπέμπει ένα σήμα το οποίο λαμβάνεται από τους τρεις σταθερούς κόμβους. Όσον πιο μακριά μεταδίδεται αυτό το σήμα τόσο περισσότερο εξασθενεί. Για αυτόν ακριβώς το λόγο, είναι πιθανό το πλάτος του σήματος που λαμβάνεται από κάθε έναν από τους τρεις σταθερούς κόμβους να είναι διαφορετικό. Η τοποθεσία του κινητού κόμβου υπολογίζεται κατά προσέγγιση με τη βοήθεια ειδικών αλγορίθμων. Οι αλγόριθμοι αυτοί μπορούν να πάρουν την ισχύ του σήματος που λαμβάνεται στους τρεις σταθερούς κόμβους και να υπολογίσουν κατά προσέγγιση την τοποθεσία του κινητού κόμβου. Όμως, ενδέχεται να υπάρχει μειωμένη ακρίβεια στην εκτίμηση της θέσης, καθώς οι αντανακλάσεις που παρουσιάζονται σε κλειστούς χώρους δημιουργούν συχνά εσφαλμένες μετρήσεις, οπότε και εκτιμήσεις θέσης. [23]

## Παρακολούθηση σε κτηνοτροφικές μονάδες

Στον κλάδο της κτηνοτροφίας τα ζώα παρουσιάζονται ιδιαίτερα ευάλωτα σε ασθένειες, για αυτό και είναι πολύ σημαντικό να παρακολουθούνται ώστε να εντοπίζεται κάθε άρρωστο ζώο γρήγορα. Η ταχύτερη αντιμετώπιση της νόσου μειώνει το πλήθος των παραγωγών που επηρεάζονται από το ξέσπασμα της νόσου ή άλλων καταστάσεων που επηρεάζουν την υγεία των ζώων. Οι παθητικές ετικέτες RFID (passive RFID tags) χρησιμοποιούνται ως μία ανέξοδη λύση για την παρακολούθηση των ζώων και μπορεί να αποδειχτούν επαρκείς για ορισμένες εφαρμογές. Οι ετικέτες αυτές χαρακτηρίζονται από περιορισμένη εμβέλεια μετάδοσης και μπορούν μοναχά να παρέχουν πληροφορίες οι οποίες έχουν προηγουμένως αποθηκευτεί όπως είναι για παράδειγμα ένας αριθμός ταυτοποίησης. Το πρότυπο IEEE 802.15.4 που βασίζεται σε ενεργές ετικέτες (active tags) μπορεί να κοστίζει περισσότερο από το αντίστοιχα παθητικά, ωστόσο μας προσφέρει μεγαλύτερη εμβέλεια μετάδοσης και είναι σε θέση να παρέχονται πληροφορίες πραγματικού χρόνου, όπως είναι για παράδειγμα ο χτύπος της καρδιάς των ζώων, θερμοκρασία του σώματος τους και η τοποθεσία στην οποία αυτά βρίσκονται (κατά προσέγγιση). Έτσι, είναι εύκολη η απομόνωση ενός άρρωστου ζώου και η αποφυγή γενικευμένης ασθένειας της κτηνοτροφικής μονάδας. [23]

Στην εικόνα που ακολουθεί παρουσιάζεται μία ασύρματη ZigBee συσκευή η οποία μετατρέπει τα σειριακά δεδομένα σε ασύρματη επικοινωνία και είναι ιδανική σε περιπτώσεις που πρέπει να αποφευχθούν τα καλώδια.

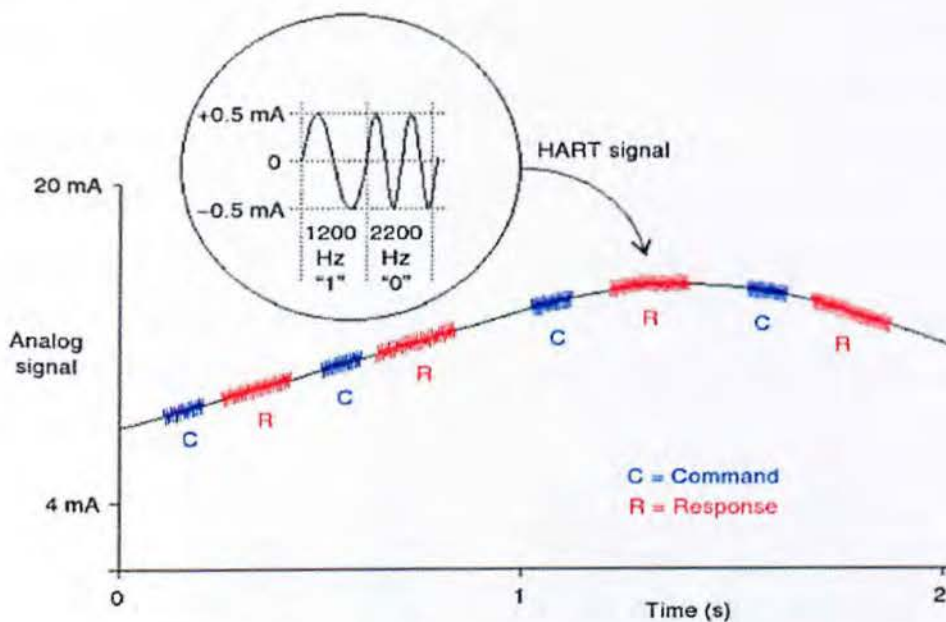


*Εικόνα 28 – Ασύρματη ZigBee συσκευή. [32]*



## 4.5 Wireless Hart

Το Hart είναι ένα ψηφιακό πρωτόκολλο για αμφίδρομη ενσύρματη επικοινωνία μεταξύ μίας κύριας εφαρμογής (host application) ή συσκευής και «έξυπνων» εργαλείων πεδίου, παρέχοντας έτσι πρόσβαση στα διαγνωστικά εργαλεία, σε ρυθμίσεις και στα δεδομένα των διεργασιών. Το παραδοσιακό πρωτόκολλο Hart καθόριζε ένα φυσικό επίπεδο στο οποίο χρησιμοποιούσε διαμόρφωση FSK (Frequency Shift Keying), ανταλλάσσοντας δεδομένα μεταξύ συσκευών «παράλληλα» από το αναλογικό σήμα ελέγχου (4-20 mA), χωρίς επιπλέον καλωδίωση. Σχηματικά, η μετάδοση των δεδομένων μέσω του αναλογικού σήματος ελέγχου φαίνεται στην παρακάτω εικόνα.



Εικόνα 29 – Hart σηματοδότηση (αναλογική και ψηφιακή). [24]

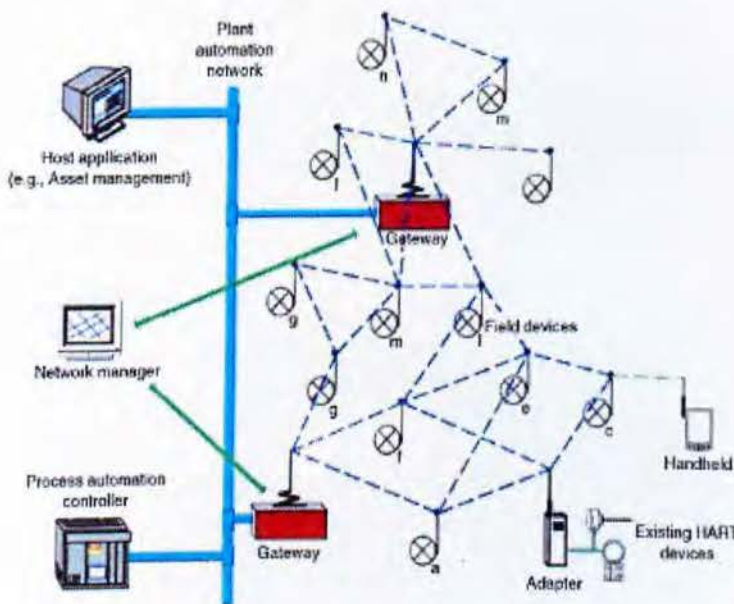
Από την έβδομη έκδοση, το Hart ενσωματώνει το πρότυπο IEEE 802.15.4, βασισμένο στο ασύρματο δίκτυο πλέγματος (mesh network), ως μία επιλογή του φυσικού επιπέδου. Αυτό συνήθως αναφέρεται ως Wireless Hart.

Το Wireless Hart έχει σχεδιαστεί με βάση μία σειρά από θεμελιώδεις προϋποθέσεις. Πρέπει να είναι απλό (εύκολο στη χρήση και στην ανάπτυξη), να χαρακτηρίζεται από αυτό-οργάνωση (self-organizing) και αυτό-ανάκαμψη (self-healing) σε περίπτωση σφάλματος, να είναι ευέλικτο (να υποστηρίζει πλήθος εφαρμογών), να είναι επεκτάσιμο (να ταιριάζει σε μικρές και μεγάλες μονάδες), να είναι αξιόπιστο, ασφαλές και να υποστηρίζει την υπάρχουσα τεχνολογία Hart (π.χ. εντολές Hart, ρυθμίσεις Hart, εργαλεία Hart). Το πρότυπο

Wireless HART χρησιμοποιεί πολλαπλή πρόσβαση με διαίρεση χρόνου (time division multiple access – TDMA). Όλες οι συσκευές είναι χρονικά συγχρονισμένες και επικοινωνούν με εκ των προτέρων προγραμματισμένες χρονοθυρίδες (time-slots) σταθερού μήκους. Η τεχνική πολλαπλής πρόσβασης TDMA ελαχιστοποιεί τις συγκρούσεις και μειώνει την κατανάλωση ισχύος από την πλευρά των συσκευών. [22]

#### 4.5.1 Αρχιτεκτονική του Wireless HART

Το Wireless HART είναι το πρώτο ανοιχτό και διαλειτουργικό ασύρματο πρότυπο επικοινωνίας. Έχει σχεδιαστεί ώστε να αντιμετωπίσει τις κυριότερες ανάγκες των βιομηχανικών διεργασιών και προσφέρει αξιόπιστη, σταθερή και ασφαλή ασύρματη επικοινωνία. Ένα δίκτυο Wireless HART αποτελείται από Wireless HART συσκευές πεδίου, τουλάχιστον μία Wireless HART πύλη (gateway) και από ένα Wireless HART διαχειριστή δικτύου (network manager). Αυτά τα στοιχεία συνδέονται και σχηματίζουν ένα ασύρματο δίκτυο πλέγματος (mesh), το οποίο υποστηρίζει αμφίδρομη επικοινωνία από την κεντρική μονάδα HART προς τις συσκευές πεδίου και αντίστροφα. Στην επόμενη εικόνα παρουσιάζεται η αρχιτεκτονική ενός Wireless HART δικτύου και οι κυριότερες συσκευές που το συγκροτούν.



Εικόνα 30 – Αρχιτεκτονική ενός Wireless HART δικτύου. [24]

Οι κυριότερες τοπολογίες Wireless HART δικτύων είναι η τοπολογία αστέρα (star network), πλέγματος (mesh network) και η τοπολογία αστέρα – πλέγματος (star – mesh

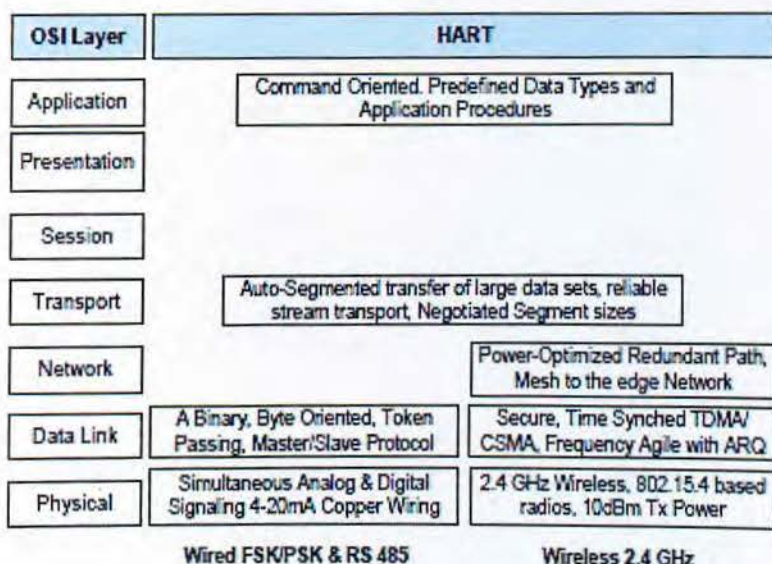


network), η οποία αποτελεί συνδυασμό των δύο προηγούμενων τοπολογιών. Ο διαχειριστής δικτύου (network manager) είναι η σημαντικότερη ίσως εφαρμογή ενός Wireless Hart δικτύου, αφού διαχειρίζεται το δίκτυο πλέγματος (mesh network) και τις συσκευές του δικτύου. Ο διαχειριστής δικτύου (network manager) εκτελεί ορισμένες ιδιαίτερα σημαντικές λειτουργίες.

- Διαμορφώνει το δίκτυο πλέγματος (mesh network).
- Επιτρέπει σε νέες συσκευές να συνδεθούν με το δίκτυο.
- Ορίζει το πρόγραμμα επικοινωνίας των συσκευών.
- Εγκαθιδρύει εφεδρικά μονοπάτια μετάδοσης δεδομένων για όλες τις επικοινωνίες.
- Παρακολουθεί το δίκτυο.

Η πύλη (gateway) συνδέει το δίκτυο πλέγματος (mesh network) με το αυτοματοποιημένο δίκτυο της βιομηχανικής μονάδας, επιτρέποντας τη διακίνηση δεδομένων μεταξύ των δύο αυτών δικτύων. Η πύλη (gate) παρέχει δυνατότητα πρόσβασης στις συσκευές του Wireless Hart, με κατάλληλο σύστημα που συνήθως διαθέτει ή με άλλες θεμελιώδεις εφαρμογές. [24]

Στην επόμενη εικόνα παρουσιάζεται η αρχιτεκτονική της στοίβας του πρωτοκόλλου Wireless Hart σύμφωνα με το OSI μοντέλο επικοινωνίας επτά επιπέδων.



*Εικόνα 3129 – Αρχιτεκτονική του Wireless Hart. [25]*

Όπως φαίνεται σε αυτή την εικόνα η στοίβα του πρωτοκόλλου αυτού περιλαμβάνει πέντε επίπεδα.

### **Το φυσικό επίπεδο (physical layer)**

Αυτό το επίπεδο του Wireless Hart βασίζεται κυρίως στο φυσικό επίπεδο IEEE STD 802.15.4-2006 2.4GHz DSSS. Αυτό το επίπεδο καθορίζει βασικά χαρακτηριστικά της ραδιοεπικοινωνίας, όπως είναι για παράδειγμα η μέθοδος σηματοδότησης, η ισχύος του σήματος και η ευαισθησία της συσκευής. Το Wireless Hart λειτουργεί όπως και το IEEE 802.15.4 στην ελεύθερη ISM ζώνη συχνοτήτων 2400-2483.5 MHz με ρυθμό μετάδοσης δεδομένων έως και 250 kbits/sec. Τα κανάλια του αριθμούνται από το 11 έως και το 26 με κενό της τάξεως των 5 MHz μεταξύ δύο γειτονικών καναλιών.

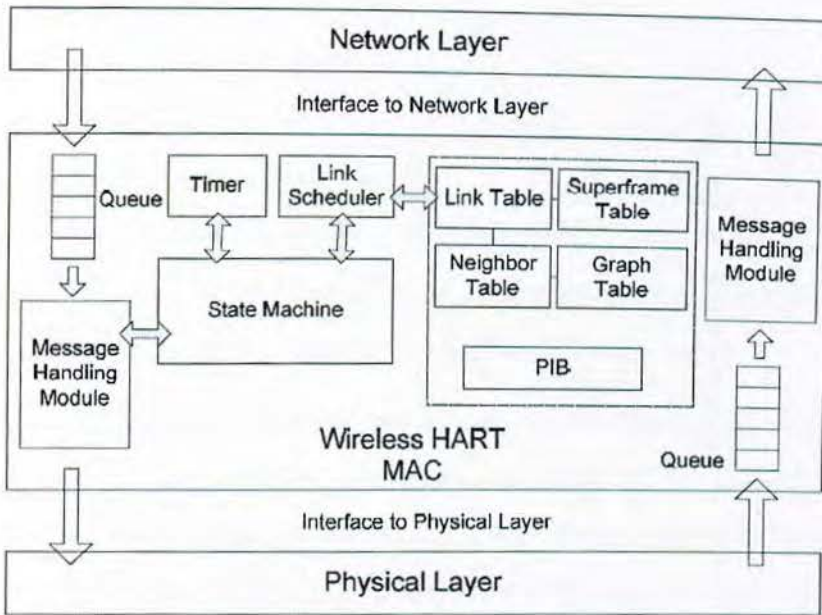
### **Το επίπεδο ζεύξης δεδομένων (data link layer)**

Το χρονικά συγχρονισμένο επίπεδο ζεύξης δεδομένων (data link layer), αποτελεί ένα ιδιαίτερο χαρακτηριστικό του Wireless Hart. Το Wireless Hart ορίζει μία χρονοθυρίδα (time-slot) η οποία είναι αυστηρά της τάξεως των 10 msec και χρησιμοποιεί τεχνολογία TDMA ώστε να παρέχει αιτιοκρατική (deterministic) επικοινωνία χωρίς συγκρούσεις. Η ιδέα του υπερπλασίου (superframe) εισάγεται ώστε να ομαδοποιήσει μία ακολουθία από συνεχόμενες χρονοθυρίδες (time-slots). Ένα υπερπλαίσιο (superframe) είναι περιοδικό, με περίοδο το συνολικό μήκος των θυρίδων (slots) που το απαρτίζουν. Όλα τα υπερπλαίσια (superframes) ενός δικτύου Wireless Hart ξεκινούν από τον απόλυτο αριθμό θυρίδας μηδέν (absolute slot number – ASN), όταν το δίκτυο δημιουργείται για πρώτη φορά. Στη συνέχεια κάθε υπερπλαίσιο (superframe) επαναλαμβάνεται με βάση την περίοδο του, με την πάροδο του χρόνου.

Για να ρυθμίσει με ακρίβεια τον τρόπο χρήσης των καναλιών, το Wireless Hart εισάγει την ιδέα της «μαύρης λίστας» καναλιών (channel blacklisting). Σε αυτή τη «μαύρη λίστα» (channel blacklisting) μπαίνουν τα κανάλια που επηρεάζονται από τακτικές παρεμβολές. Με αυτό τον τρόπο παρέχεται η δυνατότητα στο διαχειριστή του δικτύου να απενεργοποιήσει τη χρήση των καναλιών που βρίσκονται εντός της «μαύρης λίστας» (channel blacklisting).

Στην εικόνα που ακολουθεί παρουσιάζεται ο τρόπος σχεδίασης του επιπέδου ζεύξης δεδομένων (data link layer), το οποίο αποτελείται από έξι κύριες ενότητες.





Εικόνα 32 – Αρχιτεκτονική του επίπεδου ζεύξης δεδομένων (data link layer). [25]

Οι έξι αυτές ενότητες είναι:

- Οι διασυνδέσεις (Interfaces).
- Ο χρονιστής (Timer).
- Οι πίνακες επικοινωνίας (Communication Tables).
- Ο δρομολογητής συνδέσεων (Link Scheduler).
- Η μονάδα διαχείρισης μηνυμάτων (Message Handling Mode).
- Η μηχανή κατάστασης (State Machine).

### Το επίπεδο δικτύου (network layer) και το επίπεδο μεταφοράς (transport layer)

Το επίπεδο δικτύου (network layer) και το επίπεδο μεταφοράς (transport layer), συνεργάζονται με σκοπό την παροχή ασφαλούς και αξιόπιστης επικοινωνίας για τις συσκευές του δικτύου. Για την υποστήριξη της επικοινωνίας που βασίζεται στην τεχνολογία πλέγματος, κάθε Wireless Hart συσκευή πρέπει να είναι σε θέση να διαβιβάσει πακέτα για λογαριασμό των άλλων συσκευών. Έτσι στο Wireless Hart ορίζονται δύο πρωτόκολλα δρομολόγησης:

- **Δρομολόγηση γραφήματος (Graph Routing).** Το γράφημα είναι ένα σύνολο από μονοπάτια που συνδέουν τους κόμβους του δικτύου. Το μονοπάτι κάθε γραφήματος,

δημιουργούνται ρητά από το διαχειριστή του δικτύου (network manager) και λαμβάνονται από κάθε συσκευή το δικτύου. Για την αποστολή ενός πακέτου, η συσκευή αποστολής γράφει μία συγκεκριμένη ταυτότητα (ID) γραφήματος (προσδιορίζεται από τον προορισμό) στην επικεφαλίδα του δικτύου. Όλες οι συσκευές του δικτύου στο δρόμο προς τον προορισμό πρέπει να είναι εκ των προτέρων ρυθμισμένες με πληροφορίες γραφήματος που καθορίζουν τις γειτονικές συσκευές, μέσω των οποίων μπορούν να διαβιβαστούν τα πακέτα.

- **Δρομολόγηση πηγής (Source Routing).** Η δρομολόγηση πηγής αποτελεί συμπλήρωμα της δρομολόγησης γραφήματος, με στόχο τη διάγνωση του δικτύου. Για να σταλεί ένα πακέτο στον προορισμό του, η συσκευή αποστολής συμπεριλαμβάνει στην επικεφαλίδα μία λίστα από συσκευές μέσω των οποίων πρέπει να μεταδοθεί το πακέτο. Όταν το πακέτο δρομολογηθεί, κάθε συσκευή δρομολόγησης χρησιμοποιεί τη διεύθυνση της επόμενης συσκευής δικτύου που βρίσκεται στη λίστα, ώστε να έχει προσδιορίσει το επόμενο βήμα μέχρι να φτάσει το πακέτο στον προορισμό του.

#### **Το επίπεδο εφαρμογών (applications layer)**

Πρόκειται για το υψηλότερο επίπεδο του Wireless Hart. Ορίζει εντολές συσκευών, αποκρίσεις, τύπους δεδομένων και αναφορές κατάστασης. Στο Wireless Hart η επικοινωνία μεταξύ των συσκευών και της πύλης (gateway) βασίζεται σε εντολές και αποκρίσεις. Το επίπεδο εφαρμογών (application layer) είναι υπεύθυνο για την ανάλυση του περιεχομένου ενός μηνύματος, για την εξαγωγή του αριθμού της εντολής (command number), για την εκτέλεση της συγκεκριμένης εντολής και για τη δημιουργία αποκρίσεων. [25]

### **4.5.2 Τεχνικά Χαρακτηριστικά του Wireless Hart**

Το Wireless Hart χρησιμοποιεί διάφορους μηχανισμούς έτσι ώστε να συνυπάρξει με άλλες συσκευές στην κοινή ζώνη συχνοτήτων των 2.4 GHz ISM. Η τεχνική διαμόρφωσης διάχυτου φάσματος με μεταπηδήσεις συχνότητας (frequency hopping spread spectrum – FHSS) επιτρέπει στο Wireless Hart να μεταπηδά μεταξύ των 16 καναλιών που ορίζονται από το πρότυπο IEEE 802.15.4, προκειμένου να αποφευχθούν οι παρεμβολές. Η αξιολόγηση των καναλιών χωρίς παρεμβολές (clear channel assessment - CCA), αποτελεί μία προαιρετική λειτουργία η οποία μπορεί να εκτελεστεί πριν τη μετάδοση ενός μηνύματος. Επίσης η ισχύς



μετάδοσης μπορεί να ρυθμιστεί. Επιπρόσθετα παρέχεται ένας μηχανισμός ο οποίος απαγορεύει τη χρήση ορισμένων καναλιών, καθώς και η «μαύρη λίστα» καναλιών (channel blacklisting) όπως έχει ήδη αναφερθεί παραπάνω. Οι παραπάνω μηχανισμοί εξασφαλίζουν ότι το Wireless Hart δεν έρχεται σε αντίθεση με άλλα συνυπάρχοντα ασύρματα συστήματα που χαρακτηρίζονται από περιορισμούς πραγματικού χρόνου.

Το Wireless Hart παρέχει δύο διαφορετικούς μηχανισμούς για τη δρομολόγηση μηνυμάτων. Τον μηχανισμό του διαγράμματος δρομολόγησης (graph routing) και το μηχανισμό της πηγής δρομολόγησης (source routing). Ο μηχανισμός διαγράμματος δρομολόγησης (graph routing) χρησιμοποιεί προκαθορισμένα μονοπάτια ώστε να δρομολογήσει ένα μήνυμα από την πηγή προς τη συσκευή προορισμού. Το διάγραμμα δρομολόγησης αποτελείται από πολλά διαφορετικά μονοπάτια μεταξύ της πηγής και των συσκευών προορισμού, ώστε να μπορεί να χρησιμοποιεί και εφεδρικά μονοπάτια επικοινωνίας. Αυτός είναι ο προτιμώμενος τρόπος δρομολόγησης τόσο για τη λήψη όσο και για την αποστολή μηνυμάτων σε ένα Wireless Hart δίκτυο. Ο μηχανισμός δρομολόγησης πηγής (source routing) χρησιμοποιεί έτοιμες ad-hoc διαδρομές για τα μηνύματα και δεν παρέχει την παραμικρή ποικιλία μονοπατιών. Αυτή είναι και η αιτία, που αυτός ο μηχανισμός προορίζεται μόνο για διαγνωστικές διαδικασίες του δικτύου και όχι για διαδικασίες που αφορούν τα μηνύματα.

Συνοψίζοντας, πραγματοποιείται συγκεντρωτική παρουσίαση των τεχνικών χαρακτηριστικών του Wireless Hart στον επόμενο πίνακα.

IEEE προδιαγραφή	802.15.4
Ζώνη συχνότητας	2.4 GHz
Μέγιστος ρυθμός μετάδοσης σήματος (signal rate)	250 Kb/sec
Ονομαστικό εύρος μετάδοσης	>10m
Ονομαστική ισχύς εκπομπής	10 dBm
Πλήθος RF καναλιών	16
Εύρος ζώνης καναλιού	2 MHz
Τύπος διαμόρφωσης	O-QPSK
Μέθοδος διάδοσης (διασποράς)	DSSS
Μηχανισμός συνύπαρξης Μηχανισμός συνύπαρξης	«Μαύρη λίστα» καναλιών (channel blacklisting), ρυθμιζόμενη ισχύς μετάδοσης, μεταπηδήσεις καναλιών (channel hopping), αξιολόγηση καναλιών χωρίς παρεμβολές (clear channel assessment – CCA)
Βασική κυψέλη (cell)	Αστέρας (star)



Μέθοδος επέκτασης βασικής κυψέλης (cell)	Πλέγμα (mesh)
Μέγιστος αριθμός κόμβων κυψέλης (cell nodes)	>65000
Κρυπτογράφηση	AES μπλοκ κρυπτογράφησης (block cipher) με συμμετρικά κλειδιά
Πιστοποίηση (authentication)	Οι συσκευές δεν μπορούν να εισέλθουν στο δίκτυο χωρίς εξουσιοδότηση
Προστασία δεδομένων	128-bit CRC

**Πίνακας 5 – Τεχνικά χαρακτηριστικά του Wireless Hart. [25], [26]**

### 4.5.3 Ασφάλεια Συστημάτων με Wireless Hart

Η ασφάλεια είναι μία αναγκαία παράμετρος στο Wireless Hart για αυτό ακριβώς το λόγο δεν υπάρχει και επιλογή για την απενεργοποίηση της. Το Wireless Hart παρέχει από άκρη σε άκρη (end to end) και από άλμα σε άλμα (hop to hop) μέτρα ασφάλειας μέσω της κρυπτογράφησης του περιεχομένου των μηνυμάτων και της πιστοποίησης (authentication) των μηνυμάτων στο επίπεδο του δικτύου (network layer) και στο επίπεδο ζεύξης δεδομένων (data link layer). Ωστόσο τα μέτρα ασφάλειας είναι «διαφανή»(transparent) ως προς το επίπεδο εφαρμογών (applications layer). Το Wireless Hart χρησιμοποιεί τον CCM τρόπο λειτουργίας σε συνδυασμό με τον AES-128 αλγόριθμο κρυπτογράφησης. Επίσης, χρησιμοποιεί συμμετρικά κλειδιά για την πιστοποίηση (authentication) μηνυμάτων και την κρυπτογράφηση τους.

Μία σειρά από διαφορετικά κλειδιά ασφαλείας χρησιμοποιούνται για τη διασφάλιση της ασφαλούς επικοινωνίας. Πριν προσπαθήσει μία καινούργια συσκευή να εισχωρήσει στο ασύρματο δίκτυο, τροφοδοτείται με ένα κλειδί σύνδεσης (join key). Το κλειδί σύνδεσης (join key) χρησιμοποιείται για την πιστοποίηση (authentication) της συσκευής σε ένα συγκεκριμένο Wireless Hart δίκτυο. Όταν η συσκευή εισέλθει επιτυχώς στο δίκτυο, ο διαχειριστής δικτύου την τροφοδοτεί με ένα κατάλληλο κλειδί συνεδρίας (session key) και ένα κατάλληλο κλειδί δικτύου (network key) για περαιτέρω επικοινωνία. Στην ουσία, η παραγωγή κλειδιών και η διαχείριση τους πραγματοποιείται από ένα ευρύτερο διαχειριστή ασφάλειας (security manager) ο οποίος δεν καθορίζεται από το Wireless Hart. Τα κλειδιά όμως διανέμονται στις συσκευές του δικτύου από το διαχειριστή δικτύου (network manager). Ένα κλειδί συνεδρίας (session key) χρησιμοποιείται από το επίπεδο του δικτύου (network layer) για την πιστοποίηση (authentication) της από άκρη σε άκρη (end to end) επικοινωνίας μεταξύ δύο συσκευών (π.χ. μεταξύ μίας συσκευής πεδίου και της πύλης). Για κάθε ζευγάρι



επικοινωνίας (π.χ. συσκευή πεδίου με την πύλη, συσκευή πεδίου με το διαχειριστή δικτύου) χρησιμοποιούνται διαφορετικά κλειδιά συνεδρίας (session keys). Το επίπεδο ζεύξης δεδομένων (data link layer) χρησιμοποιεί ένα κλειδί δικτύου (network key) για την πιστοποίηση (authentication) μηνυμάτων σε βάση ενός άλματος. Όταν μία συσκευή επιχειρήσει να εισέλθει στο δίκτυο, χρησιμοποιείται ένα κλειδί δικτύου (network key) το οποίο είναι ευρύτερα γνωστό. Αυτό λαμβάνεται από τη συσκευή πριν αυτή λάβει ένα κατάλληλο κλειδί δικτύου (network key). Τα κλειδιά ανακυκλώνονται με βάση τις διαδικασίες ασφάλειας του διέπουν τη μονάδα αυτοματισμού διεργασιών. [22]

#### **4.5.4 Εφαρμογές του Wireless Hart στο Βιομηχανικό Αυτοματισμό και Οφέλη από τη Χρήση του**

Στο βιομηχανικό περιβάλλον το Wireless Hart καθιστά εφικτή την παρακολούθηση (monitoring) των επιμέρους τμημάτων μίας βιομηχανικής μονάδας και τη βελτιστοποίηση της λειτουργίας τους, εύκολα και με μικρό κόστος. Αυτό μπορεί να επιτευχθεί ακόμα και σε προσωρινές εγκαταστάσεις. Με τις πρόσθετες πληροφορίες που παρέχει το Wireless Hart, ο έλεγχος διεργασιών γίνεται πιο αποδοτικός με αποτέλεσμα να αυξάνεται η απόδοση της παραγωγής. Αυτό συμβαίνει διότι μειώνεται το ποσό της απαιτούμενης ενέργειας, με άμεση συνέπεια την αύξηση της ικανότητας διαβίβασης ή της ευελιξίας σε σχέση με την εναλλαγή των προϊόντων και παράλληλη συμμόρφωση στους κανονισμούς που αφορούν τη μείωση των εκπομπών RF.

Προσθέτοντας Wireless Hart συσκευές στα κρίσιμα σημεία μίας βιομηχανικής μονάδας, είναι εφικτή η λήψη πληροφοριών οι οποίες κανονικά δε θα ήταν διαθέσιμες στην αίθουσα ελέγχου, εξαιτίας περιορισμένης πρόσβασης ή εξαιτίας του κόστους καλωδίωσης. Η βελτίωση της ροής των δεδομένων και των μεθόδων διάγνωσης από τους αισθητήρες και τους επενεργητές βοηθά τη μετάβαση από μία καθαρά αιτιοκρατική (reactive) στρατηγική σε μία στρατηγική πρόγνωσης, όσον αφορά τη συντήρηση. Βέβαια οι δαπανηρές επισκευές και η διακοπή της λειτουργίας της βιομηχανικής μονάδας δεν γίνεται να αποφευχθούν πλήρως. Ωστόσο, αυξάνεται η αξιοπιστία της παραγωγής, η ασφάλεια των εργαζομένων και η προστασία του περιβάλλοντος.

Οι Wireless Hart συσκευές ως μέρος ενός ασύρματου συστήματος, μπορούν να πραγματοποιούν μετρήσεις της στάθμης ή της ροής του υλικού ανά τακτά χρονικά διαστήματα. Το σύστημα μεταδίδει της πληροφορίες που λαμβάνει σε ένα λογισμικό

SCADA (Supervisory Control and Data Acquisition) ή σε ένα λογισμικό καταγραφής και διαχείρισης ανάλογα με την εφαρμογή. Έπειτα τα δεδομένα αποστέλλονται σε ένα πληροφοριακό σύστημα. Αυτό έχει ως αποτέλεσμα τη μείωση του κόστους καταγραφής και την εξάλειψη των κενών που παρατηρούνται στις αλυσίδες εφοδιασμού. Σε επίπεδο χρηστών, αυτό μεταφράζεται σε διατήρηση της ανταγωνιστικότητας, σε ένα κόσμο στον οποίο αυξάνεται διαρκώς η απαίτηση για παγκοσμιοποίηση της παραγωγής. [33]

Επιπρόσθετα, η Wireless Hart τεχνολογία δίνει τη δυνατότητα προσθήκης μετρήσεων από σημεία που πριν ήταν φυσικά ή οικονομικά αδύνατο να ληφθούν. Ακόμα καθιστά εφικτή την παρακολούθηση ενεργειών και προσώπων. Συγκεντρωτικά, η Wireless Hart τεχνολογία υποστηρίζει όλο το φάσμα των εφαρμογών παρακολούθησης και ελέγχου, συμπεριλαμβάνοντας:

- Την παρακολούθηση του εξοπλισμού και των διεργασιών.
- Την παρακολούθηση του περιβάλλοντος, τη διαχείριση της ενέργειας, τη συμμόρφωση με τους κανονισμούς.
- Διαχείριση ενεργειών, προληπτική συντήρηση, εξειδικευμένες διαγνώσεις.
- Έλεγχο κλειστού βρόγχου ανάλογα με την περίπτωση. [27]

Στην εικόνα που ακολουθεί παρουσιάζεται ένας Wireless Hart πομπός για τη μέτρηση της θερμοκρασίας.



*Εικόνα 303 – Αισθητήρας Wireless Hart για τη μέτρηση της θερμοκρασίας. [34]*



## 5<sup>ο</sup> - ΚΕΦΑΛΑΙΟ

### “ΣΥΓΚΡΙΣΗ ΠΡΩΤΟΚΟΛΛΩΝ ΑΣΥΡΜΑΤΗΣ ΔΙΚΤΥΩΣΗΣ”

Σε αυτό το τμήμα της εργασίας θα πραγματοποιηθεί σύγκριση των χαρακτηριστικών των προαναφερθέντων πρωτοκόλλων ασύρματης δικτύωσης Wi-Fi, Bluetooth, ZigBee και Wireless Hart. Στον επόμενο πίνακα παρουσιάζονται συγκεντρωμένα τα κυριότερα χαρακτηριστικά των πρωτοκόλλων αυτών.

	Wi-Fi	Bluetooth	ZigBee	Wireless Hart
IEEE προδιαγραφή	802.11 a/b/g	802.15.1	802.15.4	802.15.4
Ζώνη συχνοτήτων	2.4 GHz και 5 GHz	2.4 GHz	868/915 MHz και 2.4 GHz	2.4 GHz
Μέγιστος ρυθμός μετάδοσης σήματος (signal rate)	54 Mb/sec	1 Mb/sec	250 Kb/sec	250 Kb/sec
Ονομαστικό εύρος μετάδοσης	100 m	10 m	10 – 100 m	>10m
Ονομαστική ισχύς εκπομπής	15 – 20 dBm	0 – 10 dBm	(-25) – 0 dBm	10 dBm
Πλήθος RF καναλιών	14 (2.4 GHz)	79	16	16
Εύρος ζώνης καναλιού	22 MHz	1 MHz	0.3/0.6 MHz και 2 MHz	2 MHz
Τύπος διαμόρφωσης	BPSK, QPSK, COFDM, CCK, M-QAM	GFSK	BPSK (+ASK) και O-QPSK	O-QPSK
Μέθοδος διάδοσης (διασποράς)	DSSS, CCK, OFDM	FHSS	DSSS	DSSS
Μηχανισμός συνύπαρξης	Δυναμική επιλογή συχνότητας, έλεγχος μεταδιδόμενης ισχύος (802.11 h)	Προσαρμοζόμενες μεταπηδήσεις συχνότητας (adaptive frequency hopping)	Δυναμική επιλογή συχνότητας (dynamic frequency selection)	«Μαύρη λίστα» καναλιών (channel blacklisting), ρυθμιζόμενη ισχύς μετάδοσης, μεταπηδήσεις καναλιών (channel hopping), αξιολόγηση καναλιών χωρίς παρεμβολές (clear channel assessment – CCA)
Βασική κυψέλη (cell)	BSS	Piconet	Αστέρας (Star)	Αστέρας (star)
Μέθοδος επέκτασης βασικής κυψέλης (cell)	ESS	Scatternet	Συστάδα δέντρων (cluster tree),	Πλέγμα (mesh)

			πλέγμα (mesh)	
Μέγιστος αριθμός κόμβων κυψέλης (cell nodes)	2007	8	>65000	>65000
Κρυπτογράφηση	RC4 κρυπτογράφηση ροής (stream cipher) (WEP), AES μπλοκ κρυπτογράφησης (block cipher)	E0 κρυπτογράφηση ροής (stream cipher)	AES μπλοκ κρυπτογράφησης (block cipher) (CTR, counter mode)	AES μπλοκ κρυπτογράφησης (block cipher) με συμμετρικά κλειδιά
Πιστοποίηση (authentication)	WPA2 (802.11i)	Κοινό μυστικό (shared secret)	CBC-MAC (επέκταση του CCM)	Οι συσκευές δεν μπορούν να εισέλθουν στο δίκτυο χωρίς εξουσιοδότηση
Προστασία δεδομένων	32-bit CRC	16-bit CRC	16-bit CRC	128-bit CRC

**Πίνακας 6 – Συγκριτικός πίνακας Wi-Fi, Bluetooth, ZigBee και Wireless Hart.**

Στη συνέχεια, τα πρωτόκολλα αξιολογούνται με βάση τα χαρακτηριστικά τους:

### Εμβέλεια

Το Bluetooth, το Wireless Hart και το ZigBee χρησιμοποιούνται για WPAN επικοινωνία (γύρω στα 10m απόσταση) με αποτέλεσμα να απαιτούν οπτική επαφή μεταξύ των συσκευών, ενώ το Wi-Fi χρησιμοποιείται για WLAN επικοινωνία (γύρω στα 100m απόσταση), όπου δεν απαιτείται οπτική επαφή. Το Bluetooth και το Wi-Fi προσφέρουν μεγάλο ρυθμό μετάδοσης δεδομένων, σε σχέση με το ZigBee και το Wireless Hart.

### Συχνότητα λειτουργίας

Όλα τα πρωτόκολλα χρησιμοποιούν τεχνικές διάχυτου φάσματος (spread spectrum) στη ζώνη συχνοτήτων των 2.4 GHz. Πιο συγκεκριμένα το Bluetooth χρησιμοποιεί την τεχνική διάχυτου φάσματος με μεταπηδήσεις συχνότητας (frequency hopping spread spectrum – FHSS), διαθέτει 79 κανάλια με εύρος ζώνης 1 MHz. Τα τρία υπόλοιπα πρότυπα χρησιμοποιούν την τεχνική διάχυτου φάσματος άμεσης ακολουθίας (direct sequence spread spectrum – DSSS). Το Wi-Fi διαθέτει 14 κανάλια εύρους 22 MHz. Το ZigBee και το Wireless Hart διαθέτουν 16 κανάλια εύρους 2 MHz. Συνεπώς το Bluetooth διαθέτει το μεγαλύτερο πλήθος καναλιών και παράλληλα το μικρότερο εύρος ζώνης ανά κανάλι. Αντίστοιχα το Wi-Fi παρουσιάζει το μεγαλύτερο εύρος ζώνης ανά κανάλι.



## Συνύπαρξη δικτύων

Από τη στιγμή που και τα τέσσερα παραπάνω πρωτόκολλα λειτουργούν στη ζώνη συχνοτήτων των 2.4 GHz, τίθεται το ζήτημα της ασφάλειας σε περίπτωση συνύπαρξης τους. Το Bluetooth παρέχει προσαρμοζόμενες μεταπηδήσεις συχνότητας (adaptive frequency hopping) ώστε να αποφεύγονται οι συγκρούσεις καναλιών. Το ZigBee χρησιμοποιεί τη δυναμική επιλογή συχνότητας (dynamic frequency selection). Αντίστοιχα το Wi-Fi χρησιμοποιεί τη δυναμική επιλογή συχνότητας (dynamic frequency selection) και τον έλεγχο της μεταδιδόμενης ισχύος. Το Wireless Hart διαθέτει «μαύρη λίστα» καναλιών (channel blacklisting), ρυθμιζόμενη ισχύ μετάδοσης, τις μεταπηδήσεις καναλιών (channel hopping) και την αξιολόγηση καναλιών χωρίς παρεμβολές (clear channel assessment – CCA). Όπως γίνεται αντιληπτό το Wireless Hart προσφέρει τους περισσότερους μηχανισμούς συνύπαρξης με αποτέλεσμα να είναι και ασφαλέστερη η συνύπαρξη του με άλλες συσκευές στον ίδιο χώρο. Πολύ καλός μηχανισμός συνύπαρξης είναι και αυτός που παρέχει το Bluetooth, αφού για να πραγματοποιηθεί παρεμβολή από κάποιο άλλο σήμα θα πρέπει να ταυτιστεί με το ρυθμό των συχνοτικών μεταπηδήσεων (frequency hopping), πράγμα πολύ δύσκολο.

## Πλήθος συσκευών ανά δίκτυο

Το μεγαλύτερο πλήθος συσκευών που ανήκουν σε μία κυψέλη (cell) του δικτύου είναι 8 για το Bluetooth και 2007 για το Wi-Fi. Για το Wireless Hart και το ZigBee το πλήθος των συσκευών σε μία κυψέλη (cell) του δικτύου ξεπερνά τις 65000. Συνεπώς το Wireless Hart και το ZigBee παρέχουν το μεγαλύτερο μέγεθος δικτύου, ενώ το Bluetooth το μικρότερο.

## Ασφάλεια

Στον τομέα της ασφάλειας όλα τα πρωτόκολλα παρέχουν μηχανισμούς κρυπτογράφησης και πιστοποίησης (authentication). Το Bluetooth χρησιμοποιεί την κρυπτογράφηση ροής (stream cipher) E0 και το «κοινό μυστικό» (shared secret) με 16-bit κυκλικό έλεγχο πλεονασμού (cyclic redundancy check – CRC). Το ZigBee και το Wireless Hart χρησιμοποιούν το προηγμένο πρότυπο κρυπτογράφησης (advanced encryption standard – AES). Το ZigBee χρησιμοποιεί κυκλικό έλεγχο πλεονασμού (cyclic redundancy check – CRC) 16 bit, ενώ το Wireless Hart κυκλικό έλεγχο πλεονασμού (cyclic redundancy check – CRC) 128-bit. Το Wi-Fi χρησιμοποιεί την κρυπτογράφηση ροής RC4 και την Wi-Fi

προστατευόμενη πρόσβαση 2 (Wi-Fi protected access 2 – WPA2) με κυκλικό έλεγχο πλεονασμού (cyclic redundancy check – CRC) 32-bit.

### **Πολυπλοκότητα**

Το πιο πολύπλοκο πρωτόκολλο από τα τέσσερα είναι το Bluetooth (188 θεμελιώδη στοιχεία τα οποία ορίζονται από το πρότυπο IEEE 802.15.1), ενώ τα λιγότερο πολύπλοκα είναι το ZigBee και το Wireless Hart (48 θεμελιώδη στοιχεία τα οποία ορίζονται από το πρότυπο IEEE 802.15.4). Μάλιστα η απλότητα τόσο του ZigBee όσο και του Wireless Hart τα κάνει κατάλληλα για εφαρμογές δικτύων αισθητήρων, αφού τα δίκτυα αυτού του είδους απαιτούν περιορισμένη μνήμη και καλή υπολογιστική ικανότητα. Το Wi-Fi είναι ενδιάμεσης πολυπλοκότητας σε σχέση με τα υπόλοιπα πρωτόκολλα (75 θεμελιώδη στοιχεία τα οποία ορίζονται από το πρότυπο IEEE 802.11 a/b/g).

### **Κατανάλωση ισχύος**

Όσον αφορά την κατανάλωση ισχύος, το Bluetooth, το Wireless Hart και το ZigBee προορίζονται για φορητές εφαρμογές, μικρής εμβέλειας και τροφοδοσία με μπαταρία περιορισμένης ισχύος. Προσφέρουν χαμηλή κατανάλωση ισχύος και σε αρκετές περιπτώσεις ο τρόπος λειτουργίας τους δεν επηρεάζει σημαντικά το χρόνο ζωής της μπαταρίας. Το Wi-Fi από την πλευρά του, έχει σχεδιαστεί για συνδέσεις μεγαλύτερων αποστάσεων και υποστηρίζει συσκευές που καταναλώνουν αρκετή ισχύ. Επίσης έχει αυξημένες απαιτήσεις σε υλικό (hardware) που οδηγεί σε αυξημένη κατανάλωση ενέργειας, πράγμα που περιορίζει τη διάρκεια της μπαταρίας ενός ασύρματου αισθητήρα. Συνεπώς το Bluetooth, το ZigBee και Wireless Hart είναι καταλληλότερα για εφαρμογές ασύρματων βιομηχανικών δικτύων (π.χ. κινητές συσκευές που λειτουργούν με μπαταρία ή δίκτυα αισθητήρων), επειδή χαρακτηρίζονται από χαμηλή κατανάλωση ισχύος η οποία οδηγεί σε αύξηση της αυτονομίας που αποτελεί ζήτημα ζωτικής σημασίας για ένα ασύρματο βιομηχανικό δίκτυο.



## 6<sup>ο</sup> - ΚΕΦΑΛΑΙΟ

### “ΣΥΝΟΨΗ - ΣΥΜΠΕΡΑΣΜΑΤΑ ”

Στην παρούσα πτυχιακή εργασία πραγματοποιήθηκε μία εκτενής παρουσίαση των ασύρματων δικτύων στο βιομηχανικό αυτοματισμό. Δόθηκε έμφαση στην παρουσίαση των ιδιαίτερων αναγκών που παρουσιάζουν τα βιομηχανικά συστήματα αυτοματισμού, καθώς και στις δυσκολίες που παρουσιάζει η ασύρματη δικτύωση στο βιομηχανικό περιβάλλον. Παρουσιάστηκαν οι πιο συνηθισμένες τοπολογίες ασύρματων δικτύων. Ιδιαίτερη αναφορά πραγματοποιήθηκε στα ασύρματα δίκτυα αισθητήρων, στον τρόπο σχεδίασης τους και παρουσιάστηκαν παραδείγματα χρήσης τους στο βιομηχανικό περιβάλλον. Το μεγαλύτερο μέρος της εργασίας αναλώθηκε στα πρωτόκολλα ασύρματης δικτύωσης. Το Wi-Fi, το Bluetooth, το ZigBee και το Wireless Hart. Ιδιαίτερο βάρος δόθηκε στη σύγκριση των τεσσάρων αυτών πρωτοκόλλων ασύρματης δικτύωσης, η οποία πραγματοποιήθηκε με βάση τα κυριότερα τεχνικά τους χαρακτηριστικά και τις κυριότερες εφαρμογές στις οποίες χρησιμοποιούνται.

Μέχρι πρότινος, το κόστος των βιομηχανικών ασύρματων δικτύων ήταν σχετικά υψηλό. Έτσι οι περισσότερες βιομηχανικές μονάδες βασίζονταν στη χρήση καλωδίων. Βέβαια οι καλωδιώσεις συνοδεύονται από οικονομικές επιβαρύνσεις οι οποίες είναι ιδιαίτερες σημαντικές όταν παρουσιαστεί η ανάγκη να αντικατασταθούν ή όταν χρειαστεί να μεταβληθεί η χωροταξία μίας μονάδας παραγωγής. Λαμβάνοντας υπόψη τις αυξημένες απαιτήσεις που υπάρχουν όσον αφορά την εγκατάσταση καλωδίωσης σε βιομηχανικές μονάδες, σε συνδυασμό με τη μείωση κόστους του ασύρματου εξοπλισμού, τα ασύρματα δίκτυα είναι σήμερα περισσότερο προσιτά, από ότι στο παρελθόν. Ο πιο σημαντικός ενδοιασμός σχετικά με την εγκατάσταση ασύρματων δικτύων σε μια βιομηχανική μονάδα, έχει να κάνει με την αξιοπιστία τους διότι δεν υπάρχει κανένα περιθώριο μη λειτουργίας τους. Βέβαια η ασύρματη δικτύωση είναι ευάλωτη στον ηλεκτρομαγνητικό θόρυβο, που υπάρχει στο βιομηχανικό περιβάλλον, και στις παρεμβολές οι οποίες αλλοιώνουν το σήμα. Τέτοιου είδους εμπόδια μπορούν να ξεπεραστούν χρησιμοποιώντας φάσμα ραδιοσυχνότητας (τεχνολογίες FHSS ή DHSS) ώστε να διασφαλιστεί η σταθερότητα λειτουργίας του δικτύου. Αντίστοιχα δεν πρέπει να ξεχνάμε ότι και οι καλωδιώσεις υφίστανται φθορές και η επισκευή τους αποτελεί μια ιδιαίτερα επίπονη και συχνά δαπανηρή διαδικασία σε περιπτώσεις παράλληλης λειτουργίας της βιομηχανικής μονάδας. Σε επίπεδο ασφάλειας οι ασύρματες



επικοινωνίες συνοδεύονται από τεχνικές κρυπτογράφησης που τις διασφαλίζουν ως ένα βαθμό ενάντια σε εξωτερικούς εισβολείς. Επίσης η μικρή εμβέλεια επικοινωνίας δεν διευκολύνει την υποκλοπή κρίσιμων πληροφοριών ή την εισαγωγή επικίνδυνων, για το δίκτυο, δεδομένων.

Τα ασύρματα δίκτυα προσφέρουν υψηλό βαθμό ευελιξίας από τη στιγμή που ο ασύρματος εξοπλισμός μπορεί να μετακινηθεί σε οποιοδήποτε σημείο εντός μίας βιομηχανικής μονάδας, υπό την προϋπόθεση να βρίσκεται εντός της ακτίνας κάλυψης του ασύρματου δικτύου. Επιπρόσθετα, οι ασύρματες επικοινωνίες διευκολύνουν την επεκτασιμότητα ενός δικτύου από τη στιγμή που τα πιο πολλά πρωτόκολλα ασύρματης δικτύωσης καθιστούν εφικτή τη σύνδεση πολλών χρηστών σε μία συσκευή, χωρίς να είναι απαραίτητη κάποια σύνθετη ρύθμιση των παραμέτρων ή διακοπή λειτουργίας της διεργασίας. Ο συνδυασμός αυτών των χαρακτηριστικών καθιστά τις ασύρματες επικοινωνίες οικονομικά συμφέρουσες, ελκυστικές, προσιτές και αξιόπιστες σε σύγκριση με τις ενσύρματες.

Όσον αφορά τα πρωτόκολλα ασύρματης δικτύωσης που υποστηρίζουν την επικοινωνία μεταξύ ασύρματων συσκευών, το Bluetooth, το Wireless Hart και το ZigBee απαιτούν οπτική επαφή, ενώ το Wi-Fi δεν απαιτεί. Το Wireless Hart και το ZigBee παρέχουν το μεγαλύτερο μέγεθος δικτύου, ενώ το Bluetooth το μικρότερο. Το πιο πολύπλοκο πρωτόκολλο από τα τέσσερα είναι το Bluetooth, ενώ τα λιγότερο πολύπλοκα είναι το ZigBee και το Wireless Hart. Μάλιστα η απλότητα τόσο του ZigBee όσο και του Wireless Hart τα κάνει κατάλληλα για εφαρμογές δικτύων αισθητήρων. Το Wi-Fi είναι ενδιάμεσης πολυπλοκότητας σε σχέση με τα υπόλοιπα πρωτόκολλα. Το Bluetooth, το ZigBee και Wireless Hart είναι καταλληλότερα για εφαρμογές χαμηλής κατανάλωσης ισχύος (π.χ. κινητές συσκευές που λειτουργούν με μπαταρία ή δίκτυα αισθητήρων).

Το Wireless Hart είναι πιο κατάλληλο για μεταφορά και απεικόνιση αναλογικών σημάτων και για συστήματα αυτόματου ελέγχου. Το Bluetooth είναι πιο κατάλληλο να χρησιμοποιείται ως αντικαταστάτης των σειριακών καλωδίων, αφού η χρήση του δεν απαιτεί τροποποιήσεις στο υπάρχον λογισμικό. Επιπρόσθετα χρησιμοποιείται για τη δημιουργία σημείων πρόσβασης συσκευών ή για τη διασύνδεση των PLCs με αισθητήρες και επενεργητές. Το ZigBee είναι κατάλληλο για τη διασύνδεση συσκευών ελέγχου με απομακρυσμένους αισθητήρες και ή επενεργητές. Το Wi-Fi είναι πιο κατάλληλο για τη διασύνδεση με απομακρυσμένους υπολογιστές και βιομηχανικά τερματικά, αλλά και για τη



μεταφορά δεδομένων μεγάλου όγκου από απομακρυσμένες εγκαταστάσεις (π.χ. εικόνα, ήχος).

Η επιλογή συγκεκριμένης τεχνολογίας, προκειμένου να υποστηριχθεί το σύνολο της επικοινωνίας σε μια βιομηχανική μονάδα, δεν αποτελεί εύκολη υπόθεση. Ο σχεδιασμός ενός βιομηχανικού δικτύου θα πρέπει να λαμβάνει υπ' όψιν τόσο τις απαιτήσεις των βιομηχανικών εφαρμογών, όσο και τους περιορισμούς που θέτει το βιομηχανικό περιβάλλον. Η πιο ρεαλιστική προσέγγιση είναι ο συνδυασμός της ασύρματης δικτύωσης με ενσύρματα δίκτυα, για τα κρίσιμότερα κομμάτια του δικτύου(π.χ. δίκτυα κορμού(backbone)). Για παράδειγμα, ασύρματα δίκτυα μπορούν να χρησιμοποιούνται για τη συλλογή μετρήσεων και τη σύνδεση των επενεργητών μιας διεργασίας σε access points, ενώ ένα ενσύρματο δίκτυο χρησιμοποιείται ως δίκτυο κορμού, για τη σύνδεση των access points με τον ελεγκτή της διεργασίας.

Από τη στιγμή που ο τρόπος εφαρμογής των παραπάνω πρωτοκόλλων ασύρματης δικτύωσης παρουσιάζει διαφορές, καλό θα ήταν η κάθε βιομηχανική μονάδα να κατανοήσει πρώτα πλήρως τις ανάγκες της, τόσο βραχυπρόθεσμα, όσο και μακροπρόθεσμα, και έπειτα να προχωρήσει στην επιλογή της ενδεδειγμένης για τη λειτουργία της λύσης. Ωστόσο, θεωρείται βέβαιο ότι τα ασύρματα δίκτυα διεκδικούν ισότιμη θέση με τα ενσύρματα δίκτυα, προσφέροντας νέες δυνατότητες στο πεδίο εφαρμογών των βιομηχανικών δικτύων.

## ΑΝΑΦΟΡΕΣ - ΒΙΒΛΙΟΓΡΑΦΙΑ

- [1] Wireless Communication in Process Automation: A Survey of Opportunities, Requirements, Concerns and Challenges. Waqas Ikram & Nina F. Thornhill
- [2] Wireless Networks for Industrial Automation. Second Edition. Dick Caro.
- [3] Wireless Technologies in Process Automation – Review and an Example to Follow. Marko Paavola. University of Oulu. Control Engineering Laboratory. 2007
- [4] Review of Existing Mobile MBWA Technologies. (IEEE 802.16 and IEEE 802.20). Thikrait Al Mosawi. November 2004.
- [5] Security Issues in Privacy and Key Management Protocols of IEEE 802.16. Xu Sen. Matthews Manton. Huang Chin-Cher. March 2006. Florida. USA.
- [6] Personal Area Networks PAN : Near-Field Intra-Body Communication. Thomas Guthrie Zimmerman.
- [7] Introduction to Bluetooth. L. Harte. Althos 2009.
- [8] Wireless Solutions for Automation Requirements. Carlos Cardeira. Armando W. Colombo. Ronald Schoop. IDMEC. Instituto Superior Técnico. Portugal. Schneider Electric GmbH. Germany
- [9] Can a Wireless Network Eliminate a Wired Network Completely?  
<http://www.excitingip.com/1879/can-a-wireless-network-eliminate-a-wired-network-completely/>
- [10] Wired or Wireless Local Area Networks?  
<http://www.broadbandinfo.com/cable/networking/wired-or-wireless-local-area-networks.html>
- [11] Βιομηχανική Πληροφορική. Robert E. King. Εκδόσεις Τζιόλα 2004.
- [12] Fundamentals of Wireless Sensor Networks. Theory and Practice. Walteneus Dargie. Christian Poellabauer. Wiley.
- [13] Wireless Sensor Networks. Technology, Protocols and Applications. K. Sohraby. D. Minoli. T. Znati.
- [14] Wireless Sensor Networks in Industrial Automation. Marko Paavola. Kauko Leiviska. University of Oulu. Control Engineering Laboratory. Finland.
- [15] <http://www.ni.com/labview/>
- [16] Wireless Ad-hoc Networks for Industrial Automation. Current Trends and Future Prospects. M. Mathiesen. G. Thonet. N. Aakvaag. ABB Corporate Research.. Bergerveien 12, 1375 Billingstad. Norway.



- [17] Guide to Wireless Ad-hoc Networks. S. Misra. I. Woungang. S. C. Misra.
- [18] A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. Jin-Shyan Lee. Yu-Wei Su. Chung-Chou Shen. Information & Communications Research Labs. Industrial Technology Research Institute (ITRI).
- [19] Industrial Use of Bluetooth. M. Andersson. CTO. ConnectBlue AB Sweden.  
<http://www.connectblue.se/>
- [20] Wi-Fi, Bluetooth, ZigBee and WiMax. H. Labiod. H. Afifi. C. De Santis. Springer.
- [21] Communication Techniques and Architectures for Bluetooth Networks in Industrial Scenarios. L. Lo Bello. O. Mirabella. University of Catania. Italy.
- [22] A Comparison of WirelessHART and ZigBee for Industrial Applications. T. Lennvall. S. Svensson. F. Hekland. ABB Corporate Research.
- [23] ZigBee Wireless Networks and Transceivers. S. Farahani.
- [24] Industrial Control Technology. A Handbook for Engineers and Researchers. P. Zhang
- [25] WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control. Jianping Song. Song Han. Aloysius K. Mok. Deji Chen. Mike Lucas. Mark Nixon. Wally Pratt. HART Communication Foundation 9390 Research Blvd. Suite I-350 Austin. TX 78759. USA.
- [26] Wireless Hart Technical Data Sheet. The Official Source for Hart Communication Technology.
- [27] Wireless Hart Applications.  
[http://www.hartcomm.org/protocol/wihart/wireless\\_applications.html](http://www.hartcomm.org/protocol/wihart/wireless_applications.html)
- [28] Wi-Fi... Why Now? Exploring New Wireless Technologies for Industrial Applications. Patrick McCardy, Ira Sharp, Phoenix Contact Inc., 2006  
[http://www.automation.com/pdf\\_articles/Wi-Fi-WhyNow.pdf](http://www.automation.com/pdf_articles/Wi-Fi-WhyNow.pdf)
- [29] Bluetooth in Industry. Snorre Kjesbu. Jan Endresen.
- [30] Control Engineering. Bluetooth for Industrial Applications.  
[http://www.controleng.com/index.php?id=483&cHash=081010&tx\\_ttnews\[tt\\_news\]=40636](http://www.controleng.com/index.php?id=483&cHash=081010&tx_ttnews[tt_news]=40636)
- [31] [http://www.bb-elec.com/product\\_multi\\_family.asp?multifamilyid=124](http://www.bb-elec.com/product_multi_family.asp?multifamilyid=124)
- [32] [http://www.icpdas-usa.com/zb\\_2550.html](http://www.icpdas-usa.com/zb_2550.html)
- [33] Wireless Hart Solutions.  
<http://www.endress.com/eh/home.nsf/#products/~process-automation-wireless-solutions-wirelesshart>
- [34] <http://www.hartcommproduct.com/inventory2/index.php?action=viewprod&num=1380>