ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

INTERNET OF THINGS 'ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ' ΣΕ ΥΠΗΡΕΣΙΕΣ ΥΓΕΙΑΣ ΜΕ ΕΜΦΑΣΗ ΣΤΗΝ ΚΑΤ' ΟΙΚΟΝ ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΑΣΘΕΝΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΤΣΙΡΜΠΑΣ Θ. ΧΑΡΑΛΑΜΠΟΣ

Επιβλέπων: Διονύσιος-Δημήτριος Κουτσούρης
Καθηγητής Ε.Μ.Π.

Αθήνα, Σεπτέμβριος 2009

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

INTERNET OF THINGS 'ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ' ΣΕ ΥΠΗΡΕΣΙΕΣ ΥΓΕΙΑΣ ΜΕ ΕΜΦΑΣΗ ΣΤΗΝ ΚΑΤ' ΟΙΚΟΝ ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΑΣΘΕΝΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΤΣΙΡΜΠΑΣ Θ. ΧΑΡΑΛΑΜΠΟΣ

Επιβλέπων: Διονύσιος-Δημήτριος Κουτσούρης
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 7η Σεπτεμβρίου 2009.

Διονύσιος-Δημήτριος Καθηγητής Ε.Μ.Π.	Κωνσταντίνα Νικήτα Καθηγήτρια Ε.Μ.Π.	Παναγιώτης Τσανάκας Καθηγητής Ε.Μ.Π.

Αθήνα, Σεπτέμβριος 2009

……

ΤΣΙΡΜΠΑΣ Θ. ΧΑΡΑΛΑΜΠΟΣ

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

Copyright © Τσίρμπας Θ. Χαράλαμπος, 2009

Με επιφύλαξη παντός δικαιώματος – All rights reserved

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου

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

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

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον καθηγητή κ. Κουτσούρη Δημήτριο-Διονύσιο για την εμπιστοσύνη που μου έδειξε στην ανάθεση αλλά και στην ανάπτυξη της παρούσας αυτής ενδιαφέρουσας εργασίας.

Επίσης θα ήθελα να ευχαριστήσω τον συνάδελφο και μέλος του Εργαστηρίου Βιοϊατρικής Τεχνολογίας του Ε.Μ.Π. κ. Κωσταντίνο Γκιόκα για τις πολύτιμες συμβουλές του.

Τέλος να ευχαριστήσω τη συνάδελφο και φίλη Αναστασία Φωτιάδη για τις συμβουλές, τον άπλετο χρόνο και την πολύτιμη βοήθεια που μου πρόσφερε στη συγγραφή της διπλωματικής μου.

Περίληψη

Η παρούσα διπλωματική έχει σαν στόχο να παρουσιάσει τις βασικές έννοιες του Διαδικτύου των πραγμάτων και πώς αυτό μπορεί να βρει χρήση στην υγειονομική περίθαλψη και συγκεκριμένα στην κατ' οίκον παρακολούθηση των ασθενών. Θα αναλυθούν οι βασικές αρχές που διέπουν το Διαδίκτυο των πραγμάτων, οι τεχνολογίες που εναρμονίζονται με αυτές και κατ' επέκταση οι απαιτήσεις που προκύπτουν κατά την εφαρμογή των τελευταίων όσο και οι προοπτικές που διαθέτουν. Δίνεται βαρύτητα στη δομή και στα χαρακτηριστικά του πρωτόκολλου του Διαδικτύου νέας γενιάς 'IPv6' και στο ρόλο που διαδραματίζουν η ασφάλεια και η διατήρηση της ιδιωτικότητας στη λειτουργία και στη βιωσιμότητα του Διαδικτύου των πραγμάτων. Με γνώμονα αυτά θα αναφερθούν λύσεις και αρχιτεκτονικές διασύνδεσης και διασφάλισης του απορρήτου.

Έπειτα από τον ορισμό των παραπάνω εννοιών γίνεται περιγραφή της ήδη υπάρχουσας εφαρμογής του Διαδικτύου των πραγμάτων στα νοσοκομεία και κατά πόσο αυτό είναι ευεργετικό για αυτά, τόσο για τη λειτουργία τους όσο και για τα οικονομικά τους. Στη συνέχεια αναζητείται λύση για την επέκταση και την τροποποίηση αυτού για την κατ' οίκον παρακολούθηση των ασθενών. Για το σκοπό αυτό έγινε μελέτη στην οποία αναλύθηκε το συνολικό σύστημα παρακολούθησης του ασθενούς αναφέροντας τα υπάρχοντα προβλήματα, τα πιθανά σενάρια χρήσης και προτάθηκαν λύσεις για την υλοποίηση του στο επίπεδο της δικτύωσης και της ασφάλειας. Τέλος επισημαίνονται θέματα για συζήτηση και τομείς που πρέπει να ερευνηθούν από την ακαδημαϊκή κοινότητα.

Λέξεις κλειδιά

Διαδίκτυο των πραγμάτων, υγειονομική περίθαλψη, κατ' οίκον περίθαλψη , ταυτοποίηση μέσω ραδιοσυχνοτήτων, ασφάλεια, ιδιωτικότητα, IPv6

Abstract

The present thesis, aims to present the basic significances of the Internet of things and how this can find use in healthcare and specifically in home care. We analyze the basic principles underlying the Internet of Things,the technologies that are harmonised with them and the requirements that are arisen from the implementation of last ones and the prospects that are available. It is very important to understand the structure and the characteristics of the new Internet protocol 'IPv6' and that the security and protection forms a basis for the survivability and dependability of the networks of the Internet of Things. So we will suggest some security architecture in order to protect privacy.

After analyzing the above, there is a description of an existing application on the Internet of Things in hospitals and if they have organisational and financial benefits. Afterwards solutions are sought for the extension and the modification of this for home monitoring of patients. For this purpose a study was made in which the total system of follow-up of patient is analyzed, indicating the existing problems, possible scripts of use, and solutions are proposed for its implementation at the level of networking and security. Finally issues for discussion are pointed and sectors that should be searched and developed from the academic community.

Key words

Internet of Things, healthcare, home care, Radio Frequency Identification, security, privacy, IPv6

Περιεχόμενα

Περίληψη ……...……..5

Abstract ……..……....6

Κεφάλαιο 1ο

Διαδίκτυο των Πραγμάτων……...14

1.1 Εισαγωγή …….15

1. 2 Υπάρχουσες Τεχνολογίες……..…17

1.3 Προοπτικές-Απαιτήσεις……..…….....20

1.3.1 Προοπτικές Συστήματος…….....20

1.3.2 Τεχνολογικές Απαιτήσεις ……...…23

1.3.3 Απαιτήσεις Δικτύωσης ...…….24

1.3.4 Απαιτήσεις ασφάλειας και ιδιωτικότητας …….....28

1.3.5 Απαιτήσεις Ραδιοκυμάτων ……...30

1.4 Προοπτικές εφαρμογής …….…32

1.4.1 Λίστα εφαρμογών…….....35

1.5 Ευρωπαϊκά έργα σχετικά με το Διαδίκτυο των πραγμάτων…….40

1. 6 Συμπεράσματα……...…40

1.7 Βιβλιογραφία……..……...41

Κεφάλαιο 2ο

IPv6…….…….42

2.1 Εισαγωγή για το IPv6 …….....43

2.1.1 Μορφή Πακέτου IPv6…….....43

2.1.2 Μετάβαση από το IPv4 στο IPv6……..47

2.2 Πλεονεκτήματα του IPv6 έναντι του IPv4 ……...51

2.2.1 Το IPv6 παρέχει μεγαλύτερο χώρο διευθύνσεων IP από το IPv4…….51

2.2.2 Το IPv6 παρέχει καλύτερη end-to-end σύνδεση από το IPv4……..…....52
2.2.3 Το IPv6 έχει καλύτερη δυνατότητα αυτορρύθμισης συσκευών από το IPv4……53
2.2.4 Το IPv6 παρέχει απλουστευμένες δομές επικεφαλίδας που οδηγούν σε ταχύτερη δρομόλογηση σε σύγκριση με το IPv4…….…55
2.2.5 Το IPv6 παρέχει μεγαλύτερη ασφάλεια σε σχέση με το IPv4 όσο αφορά τις εφαρμογές και τα δίκτυα…….….…56
2.2.6 Το IPv6 παρέχει καλύτερη ποιότητα υπηρεσιών (QoS) από το IPv4…....57
2.2.7 Το IPv6 παρέχει καλύτερες Multicast και Anycast ικανότητες σε σχέση με το IPv4…….…….59
2.2.8 Το IPv6 προσφέρει καλύτερες δυνατότητες φορητότητας από το IPv4……60
2.2.9 Το IPv6 προσφέρει μεγαλύτερη ευκολία στη διαχείριση σε σχέση με Το IPv4……..62
2.3 Μετρήσεις…….……..…..…64
2.3.1 Χαρακτηριστικά των μετρήσεων…….…....64
2.3.2 Συνδεσιμότητα…...……...…68
2.3.3 Υπολογισμός των hops…...……...68
2.3.4 RRT “Roynd-trip delay time”…..…….…....69
2.3.5 Ρυθμαπόδοση……..…..…….…....71
2.4 Συμπεράσματα..…….……..…..…73
2.5 Βιβλιογραφία…….……..…..…74

Κεφάλαιο 3ο

Ασφάλεια……...……...75
3.1 Παρουσίαση…….……...…..76
3.2 Ανάλυση της ασφάλειας και του απορρήτου……77
3.2.1 Κατηγοριοποίηση και ευαισθησία……...……77
3.3 Σημαντικά στοιχεία του Διαδικτύου των πραγμάτων……...88
3.3.1 Καθολικό ενδιάμεσο λογισμικό μεταξύ δικτύου-αισθητήρων……...…..89
3.3.2 RFID……90

3.3.2.1 Φυσικοί μηχανισμοί……...…..…….91
3.3.2.2 Πρωτόκολλα κρυπτογράφησης……...……...91
3.4 Έρευνα από άλλους τομείς……...…..92
3.4.1 Υπευθυνότητα πληροφοριών…….....……92
3.4.2 Κρυπτογραφημένα αναγνωριστικά…….……..93
3.4.3 Εξαγωγή κλειδιού από τα χαρακτηριστικά του ασύρματου καναλιού…….94
3.5 Συμπεράσματα…….…95
3.6 Βιβλιογραφία……...…95

Κεφάλαιο 4ο

Εφαρμογή του Διαδικτύου των πραγμάτων στην Υγειονομική περίθαλψη…..……97
4.1 Παρουσίαση…….....……98
4.2 Τηλεϊατρική & Υπηρεσίες Υγείας……..……...……100
4.3 Τηλεφροντίδα…….....……..……103
4.4 Το 'Διαδίκτυο των πραγμάτων' στην υγεία……..105
4.4.1 Παρουσίαση……105
4.4.2 Μοντέλα RFID σε υπηρεσίες υγείας……..…107
4.4.3 Ιατρικές υπηρεσίες παρακολούθησης θέσης (Location-based Medicare Service (LBMS))……109
4.4.4 Το κόστος και τα οφέλη των RFID σε πραγματικές εφαρμογές……..……..113
4.5 Συμπεράσματα…….…..118
4.6 Βιβλιογραφία…….118

Κεφάλαιο 5ο

Μελέτη…….…..……..120
5.1 Παρουσίαση…….....……..121
5.2 Περιγραφή προβλήματος……...…….121
5.3 Σενάρια χρήσης…….....……..……..123
5.3.1 Παράδειγμα χρήσης……...……..125

5.4 Επισκόπηση Συστήματος……...127

5.4.1 Διαμόρφωση Δικτύου……..128

5.4.2 Internet…….128

5.4.3 Intranet…….130

5.4.4 Πως λειτουργεί το σύστημα……..135

5.4.5 Απαιτήσεις ασφάλειας……..….135

5.4.5.1 IPSec……...……..….135

5.4.5.2 NDP Πρωτόκολλο…….....137

5.4.5.3 Παραγωγή κρυπτογραφημένων διευθύνσεων……..…..138

5.4.5.4 SEND Πρωτόκολλο…….…..139

5.5 Συσκευές υγείας παρακολούθησης βιοσημάτων με ενσωματωμένες RFID ετικέτες για το σπίτι……..……...142

5.6 Συμπεράσματα……..…….145

5.7 Βιβλιογραφία……..……...146

Κεφάλαιο 6ο

Θέματα προς συζήτηση……..……147

6.1 Παρουσίαση……......……148

6.2 Έρευνα της ακαδημαϊκής κοινότητας….……...…..149

Ευρετήριο εικόνων

Εικόνα 1.1:Ετικέτα RFID …….…….18

Εικόνα 1.2:Συσκευή ανάγνωσης RFID ……..19

Εικόνα 2.1: Μορφή δεδομενογράμματος IPv6…..…….44

Εικόνα 2.2: Μορφή δεδομενογράμματος IPv4…….……..46

Εικόνα 2.3: Προσέγγιση διττής στοίβας…..……...…48

Εικόνα 2.4: Σήραγγα……..……...……..50

Εικόνα 2.5: Ποσοστά χώρου διευθύνσεων IPv4…….52

Εικόνα 2.6:Παράδειγμα end-to-end σύνδεσης……53

Εικόνα 2.7: Dynamic Host Configuration Protocol……54

Εικόνα 2.8: Δομή της ασφάλειας …...……56

Εικόνα 2.9: Υπηρεσίες……..……..58

Εικόνα 2.10: Multicast και Anycast τεχνικές……..…..……60

Εικόνα 2.11: Διάγραμμα συνδρομητών κινητής τηλεφωνίας ανά 100 κατοίκους ……...…….61

Εικόνα 2.12: Συγχώνευση Δικτύων ……...……62

Εικόνα 2.13: IPv6/IPv4 dual-stack hosts and servers…….65

Εικόνα 2.14: Διαγράμματα μετρήσεων των hops…...……68

Εικόνα 2.15: Διαγράμματα μετρήσεων RTT……..70

Εικόνα 2.16:Διαγράμματα ρυθμαπόδοσης…….72

Εικόνα 3.1: Κατηγοριοποίηση θεμάτων και τεχνολογιών του Διαδικτύου των πραγμάτων…….79

Εικόνα 3.2: Επισκόπηση υψηλού επιπέδου της φάσης χειραψίας του SSL..…….82

Εικόνα 3.3: Onion Routing……...……..83

Εικόνα 3.4: Onion Routing ……...…....……..84

Εικόνα 3.5: DDOS attack…….....86

Εικόνα 4.1 Παραδείγματα Ιατρικής Τεχνολογίας……..…….98

Εικόνα 4.2: Μορφή συστήματος τηλεϊατρικής……....105

Εικόνα 4.3: Κύρια συστατικά του rfid…….108

Εικόνα 4.4:Η δομή του RFID στο Taipei Medical University Hospital…….….111

Εικόνα 4.5:Η αρχιτεκτονική δομή του LBMS……....111

Εικόνα 4.6: Η αλληλεπίδραση των ενοτήτων LBMS…….....112

Εικόνα 5.1: Διάγραμμα συστήματος κατ' οίκον ιατρικής παρακολούθησης ασθενών……...123

Εικόνα 5.2: Διάγραμμα ροής των πληροφοριών κατά την χρήση του συστήματος κατ' οίκον ιατρικής παρακολούθησης……...126

Εικόνα 5.3: Μοντέλο δικτύου…….…127

Εικόνα 5.4: Διάγραμμα διασύνδεσης με το Internet……...129

Εικόνα 5.5: Dual stack Ipv6/Ipv4……...130

Εικόνα 5.6: Δομή του intranet δικτύου……...131

Εικόνα 5.7: IPv6 πρωτόκολλο με χώρο διευθύνσεων 128 bit……....133

Εικόνα 5.8: Δομή RFID μηνύματος……133

Εικόνα 5.9: Δομή IPv6……..134

Εικόνα 5.10: Ενσωμάτωση RFID στο IPv6……134

Εικόνα 5.11: NDP μήνυμα……..……138

Εικόνα 5.12:Hash function…….139

Εικόνα 5.13: Μορφή της επιλογής CGA……140

Εικόνα 5.14: Μορφή της RSA υπογραφής……...……..140

Εικόνα 5.15: Μορφή της επιλογής Timestamp……...141

Εικόνα 5.16: Μορφή της επιλογής Nonce…….…….141

Ευρετήριο πινάκων

Πίνακας 2.1: Συγκεντρωτικός πίνακας διαφορών IPv6- IPv4…...…….63

Πίνακας 2.2: Πίνακας διαθέσιμων δικτύων……..……..64

Πίνακας 2.3: Dual-stack sites…...…….…….65

Πίνακας 3.1: Η ευαισθησία των θεμάτων ασφάλειας……..……...79

Πίνακας 3.2: Κατάσταση της έρευνας για εξαιρετικά ευαίσθητες ιδιότητες…….88

Πίνακας 5.1: Είδη και χαρακτηριστικά των ετικετών RFID……..132

Κεφάλαιο 1ο

Διαδίκτυο των πραγμάτων

1.1 Εισαγωγή

Υπάρχουν πάνω από 2 δισεκατομμύρια κινητά τερματικά που χρησιμοποιούνται σήμερα και πάνω από 1 δισεκατομμύριο χρήστες του Internet παγκοσμίως. Ασύρματες, κινητές και δικτυακές τεχνολογίες έδωσαν σε πρώτη φάση τη δυνατότητα διάχυτης επικοινωνίας μεταξύ συστημάτων και εφαρμογών και δημιούργησαν πολύ σημαντικές οικονομικές ευκαιρίες. Ωστόσο, αυτό μπορεί να είναι μόνο η αρχή: εξελισσόμενες τεχνολογίες δικτύωσης , όπως η *ταυτοποίηση μέσω* ραδιοσυχνοτήτων (RFID tags), ενδεχομένως θα μπορούν να αναπτυχθούν σε εκατοντάδες δισεκατομμύρια , για μια σχεδόν απεριόριστη γκάμα εφαρμογών.

Πιο μακροπρόθεσμα, αναμένεται απλές ετικέτες του σήμερα να εξελιχθούν σε ευφυέστερα δικτυωμένα αντικείμενα με αυξημένη αποθήκευση, επεξεργασία, καθώς και δυνατότητα προσθήκης αισθητήρων. Αυτό με τη σειρά του θα ανοίξει ένα εντελώς νέο φάσμα σε δικτυακές εφαρμογές, όπως M2M ” Man-to-Machine, Machine-to-Man, Machine -to-Mobile and Mobile-to-Machine ” και context-aware επικοινωνίες.

Το “Διαδίκτυο των πραγμάτων” είναι ένα δίκτυο δισεκατομμυρίων ή τρισεκατομμυρίων μηχανών οι οποίες επικοινωνούν μεταξύ τους. Είναι πολύ σημαντικό και κυρίαρχο θέμα για την εξέλιξη των πληροφοριών και των επικοινωνιών τις επόμενες δεκαετίες, καθώς η απλούστερη μορφή αυτού είναι ήδη σε χρήση. Υπάρχουν 1,3 δισεκατομμύρια ταυτοποιήσεις μέσω ραδιοσυχνοτήτων (RFID) και δύο δισεκατομμύρια χρήστες κινητών υπηρεσιών, σε όλο τον κόσμο.

Η ιδέα έχει διευρυνθεί από προηγμένες έννοιες τα τελευταία είκοσι χρόνια:

• ubiquitous communications
• pervasive computing
• ambient intelligence

Από μια γενική σκοπιά, μπορεί να συναχθεί το συμπέρασμα ότι η τάση για τον όλο και μεγαλύτερο αριθμό συνδεδεμένων ευφυών αντικειμένων είναι αμετάκλητη, διότι η οικονομική αξία ενός συστήματος αντικειμένων και συσκευών είναι άμεσα συνδεδεμένη με το γεγονός ότι είναι «δικτυωμένες».
Το Διαδίκτυο των πραγμάτων θα επιτρέψει μέσω της πληροφορικής την υποστήριξη των οικονομικών, της υγείας, της κοινωνικότητας αλλά και της ιδιωτικότητας.

Παρακάτω αναφέρονται τρία απλά παραδείγματα:

Διαχείριση περιουσιακών στοιχείων. Ηλεκτρονική σήμανση και παρακολούθηση της θέσης των αποσκευών σε έναν αερολιμένα, ή των εμπορευμάτων στο πλαίσιο μιας διαδικασίας παραγωγής στο εργοστάσιο.

Υγειονομική περίθαλψη. Αισθητήρες για αρτηριακή πίεση και καρδιακή συχνότητα, τακτικές μετρήσεις από το σπίτι του ασθενούς θα μπορούν να στέλνονται σε κάποιο κέντρο παρακολούθησης. Ένας υπολογιστής θα εντοπίζει τυχόν ανεπιθύμητες κινήσεις ή σήματα και θα ειδοποιεί τον υπεύθυνο γιατρό να ελέγξει τον ασθενή.

Παρακολούθηση περιβάλλοντος. Ένα δίκτυο αισθητήρων θα είναι σε θέση να παρακολουθεί το ύψος του ποταμού και των βροχοπτώσεων, θα μπορεί να επιτευχθεί πρόβλεψη των πλημμυρών και στήριξη των μέτρων διαχείρισης των υδάτων για την ανακούφιση από τυχόν πλημμύρες.

Οι πιθανές εφαρμογές της διαδεδομένης δικτύωσης είναι απεριόριστες. Μερικές εφαρμογές φαίνονται απαραίτητες, για παράδειγμα ο εντοπισμός ανθρώπων σε ένα πιθανό σενάριο καταστροφής, όπως φωτιά σε κάποιο τούνελ. Άλλες εφαρμογές μπορεί εκ πρώτης όψεως να φαίνονται μη ρεαλιστικές. Για να θεωρηθεί ότι αυτή η τεχνολογία πραγματικά αξίζει τον κόπο, υπάρχει ανάγκη για αντιμετώπιση του μεγάλου όγκου των εφαρμογών προκειμένου να κατανοηθούν καλύτερα οι διάφορες απαιτήσεις (π.χ. πραγματικός χρόνος, η ποιότητα των υπηρεσιών), που θα οδηγήσουν τελικά στην απαραίτητη "γενική" τεχνολογική εξέλιξη.

Τα θέματα που θεωρείται ότι παρουσιάζουν ενδιαφέρον όσο αφορά το Διαδίκτυο των πραγμάτων είναι τα εξής:

• Η προοπτική του συστήματος για το πώς τα δικτυωμένα συστήματα είναι πιθανό να εξελιχθούν.
• Οι επιπτώσεις της διασυνδεσιμότητας της συσκευής για τις μελλοντικές αρχιτεκτονικές δικτύου και των νέων τεχνολογιών.
• Συγκεκριμένη ασφάλεια και προστασία της ιδιωτικότητας.
• Η αρχιτεκτονική που απαιτείται για την υποστήριξη των αιτήσεων των τρισε-κατομμυρίων συσκευών που συνδέονται.
• Η σύνθεση των υπηρεσιών.
• Ο ρόλος των "ανοικτών" (λογισμικών) μοντέλων.
• Ο ρόλος των ασύρματων τεχνολογιών.

Αυτά καθιερώθηκαν σαν ερωτήσεις που πρέπει να απαντηθούν προκειμένου να κατανοηθούν οι απαιτήσεις για το παγκόσμιο δίκτυο του αύριο, για το πώς μπορεί να οικοδομηθεί και για το πώς θα είναι.

1.2 Υπάρχουσες τεχνολογίες

Το διαδίκτυο έχει καταστεί η πλατφόρμα ώστε να ξεκινήσουν Information Technology (IT) υπηρεσίες για όλα τα είδη των βιομηχανιών. Το Δίκτυα και οι υπηρεσίες λογισμικού συνδέονται μεταξύ τους με κάθε τρόπο. Οι αρχιτεκτονικές αρχές για τη δημιουργία προϊόντων λογισμικού και υπηρεσιών έχουν εξελιχθεί. Αρχιτεκτονικές αρχές όπως REpresentational State Transfer (REST), Event Driven Architecture (EDA), and Service Oriented Architecture (SOA) χρησιμοποιούνται για τη δημιουργία υπηρεσιών λογισμικού που χρησιμοποιούνται από εκατομμύρια ανθρώπους και επιχειρήσεις σε όλο τον κόσμο. Για παράδειγμα, το REST έχει αποδείξει τη χρησιμότητά του ως μια επιτυχημένη αρχή σχεδιασμού αφού όλο το World Wide Web (WWW) έχει σχεδιαστεί με βάση αυτό. Το SOA χρησιμοποιείται ευρέως για τη δημιουργία centric και web εφαρμογών επιχειρήσεων και υπηρεσιών. Έχει εξελιχθεί σε ένα νέο ώριμο επίπεδο, σε σύγκριση με άλλες τεχνολογίες που είναι διαθέσιμες στο παρελθόν για την παροχή γρήγορων υπηρεσιών. Όλες αυτές οι αρχές αρχιτεκτονικής συμπληρώνουν επίσης η μία την άλλη για το σχεδιασμό νέων υπηρεσιών.

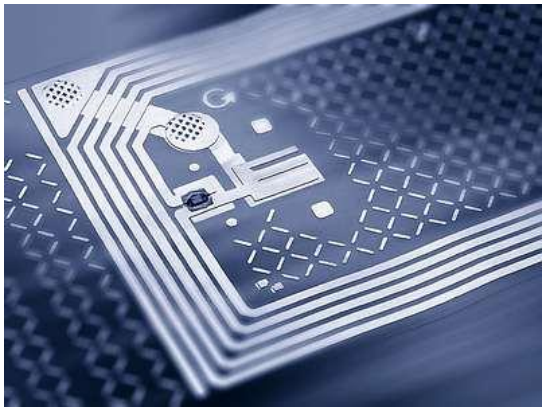
Αυτή η παράγραφος παρέχει τεχνικές πληροφορίες σχετικά με τα συστήματα RFID που είναι μία βασική τεχνολογία του Διαδικτύου των πραγμάτων.

RFID Systems

Μία από τις πιθανές τεχνολογίες αναγνώρισης που προτείνεται στην έκθεση της ITU είναι η Radio Frequency Identification (RFID). Η RFID είναι μια αυτόματη μέθοδος αναγνώρισης που χρησιμοποιεί τα ραδιοκύματα για να εντοπίσει σηματοδοτημένα στοιχεία όπως ανθρώπους, ζώα ή αντικείμενα Είναι παρόμοιο με το bar code , αλλά χρησιμοποιεί ένα μικροτσίπ μαζί με ραδιοκύματα. Μια ετικέτα RFID, επίσης είναι γνωστή και ως electronic label," "transponder" ή "code plate" η οποία αποτελείται από ένα τσιπ RFID που συνδέεται με μία κεραία. Οι ετικέτες μπορούν να διαβαστούν από πολλά μέτρα μακριά και χωρίς να χρειάζεται οπτική επαφή. Η πιο κοινή μέθοδος αναγνώρισης είναι να φυλάσσεται ο αύξοντα αριθμός που προσδιορίζει κάποιο άτομο ή κάποιο αντικείμενο, αλλά μια RFID ετικέτα μπορεί επιπλέον να αποθηκεύσει και άλλες πρόσθετες πληροφορίες. Τα συστήματα RFID χρησιμοποιούν ετικέτες RFID Που αποτελούν τη σημαντικότερη και αποδοτικότερη μέχρι στιγμής τεχνολογία για τις υπηρεσίες αναγνώρισης στοιχείου όσο αφορά το IOT «Internet Of Things».

Τα συστήματα RFID αποτελούνται από τρία κύρια στοιχεία : ετικέτες RFID, αναγνώστες RFID, και RFID λογισμικό.

Μια ετικέτα RFID ή αναμεταδότης μεταφέρει τα στοιχεία ταυτότητας που μπορεί να είναι μια μοναδική συμβολοσειρά ή ένας κωδικός. Επιπλέον, η ετικέτα μπορεί να αποθηκεύσει πληροφορίες ανάλογα με το μέγεθος της μνήμης της. Μια ετικέτα επισυνάπτεται φυσικά στο αντικείμενο που πρέπει να εντοπιστεί. Πρόκειται για μία ηλεκτρική συσκευή σχεδιασμένη ώστε να λαμβάνει ένα ειδικό σήμα και να στέλνει αυτόματα μια συγκεκριμένη απάντηση. Αποτελείται από ένα στοιχείο σύνδεσης (όπως ένα πηνίο, ή μια κεραία μικροκυμάτων) και ένα ηλεκτρονικό μικροτσίπ (λιγότερο από το 1 / 3 του χιλιοστού σε μέγεθος). Μπορεί να είναι παθητική, ημι-παθητική ή ενεργητική, με βάση την πηγή τροφοδοσίας της και τον τρόπο χρησιμοποίησής τους, και μπορεί να είναι μόνο ανάγνωσης, ανάγνωσης ή εγγραφής και ανάγνωσης / εγγραφής και αναδιατύπωσης, ανάλογα με το πώς τα δεδομένα είναι κωδικοποιημένα. Οι παθητικές ετικέτες RFID λαμβάνουν την ενέργεια από το ηλεκτρομαγνητικό πεδίο που εκπέμπεται από τους αναγνώστες. Οι ετικέτες χρησιμοποιούν συχνότητες εκπομπής που κυμαίνονται στα kilohertz, megahertz, και gigahertz.



Εικόνα 1.1: Ετικέτα RFID

Ένας RFID αναγνώστης είναι μία συσκευή που χρησιμοποιείται για να διαβάσει τα δεδομένα που στέλνονται από την ετικέτα. Για ανάγνωση παθητικών ετικετών RFID, ο αναγνώστης πρέπει να χρησιμοποιήσει επιπλέον ενέργεια σε ηλεκτρομαγνητική μορφή. Η συσκευή ανάγνωσης αποτελείται από μια διπολική κεραία και ένα μικροεπεξεργαστή. Η διπολική κεραία χρησιμοποιείται για τη μετάδοση των σημάτων και την τροφοδότηση της ετικέτας. Ο μικροεπεξεργαστής ελέγχει και διευθύνει όλες τις σχετικές διεργασίες της συσκευής ανάγνωσης . Ο αναγνώστης μπορεί να είναι είτε μια ειδική συσκευή χειρός είτε να είναι ενσωματωμένος σε μια κινητή συσκευή ή μπορεί ακόμα να ενταχθεί σε ένα τοίχο (σταθερές συσκευές ανάγνωσης). Σε σύγκριση με τις ετικέτες, οι συσκευές ανάγνωσης είναι μεγαλύτερες, πιο ακριβές, και καταναλώνουν περισσότερη ενέργεια

ανάλογα με την ιδιότητά τους. Η συσκευή ανάγνωσης πρέπει να έχει επίσης τη δυνατότητα επικοινωνίας (ενσύρματη ή ασύρματη).

Εικόνα 1.2: Συσκευή ανάγνωσης RFID

Το RFID λογισμικό είναι ένα υλικολογισμικό που τρέχει για τη συσκευή ανάγνωσης RFID. Υπάρχουν διάφορες υπηρεσίες που περιλαμβάνονται σε αυτό. Υπηρεσίες όπως η ανάγνωση, το κλείδωμα, η εγγραφή, και η διαγραφή μιας ετικέτας περιλαμβάνονται στο βασικό σύνολο λειτουργιών. Επιπλέον, το φιλτράρισμα, το άθροισμα, η αναζήτηση, η καταγραφή συμβάντων, και οι υπηρεσίες ασφαλείας περιλαμβάνονται και αυτά στο λογισμικό. Το υλικολογισμικό επίσης χρειάζεται για να επικοινωνεί η συσκευή ανάγνωσης με το δίκτυο, η οποία θα πρέπει να επεξεργάζεται και τις εντολές που λαμβάνει από ένα απομακρυσμένο σύστημα ελέγχου.

Υπάρχουν δύο τύποι RFID: κοντινού πεδίου RFID και μακρινού πεδίου RFID. Με Near Field Communication (NFC) RFID είναι εξοπλισμένα πολλά τηλέφωνα τα τελευταία χρόνια και πολλές NFC υπηρεσίες είναι διαθέσιμες ήδη για NFC τηλέφωνα. Οι NFC συσκευές ανάγνωσης διαβάζουν την ετικέτα εντός εμβέλειας 5 cm ή μερικές φορές χρειάζεται ένα άγγιγμα. Μακρινού πεδίου RFID καλύπτουν απόσταση μεταξύ τριών και έξι μέτρων από σταθερές συσκευές ανάγνωσης.

1.3 Προοπτικές-Απαιτήσεις

1.3.1 Προοπτικές Συστήματος

Το Διαδίκτυο των πραγμάτων είναι ένα δίκτυο επικοινωνίας συσκευών με τέσσερις βαθμούς πολυπλοκότητας:

• Καθαρά παθητικές συσκευές (RFID) που δίνουν σταθερά δεδομένα μετά από ερώτηση εξ' αποστάσεως.

• Συσκευές με μέτρια επεξεργαστική ισχύ οι οποίες διαμορφώνουν το μήνυμα, το οποίο ίσως να μεταβάλλεται με το χρόνο και θέση.

• Τηλεπισκοπικές συσκευές που παράγουν και στέλνουν πληροφορίες σχετικά με το περιβάλλον τους, όπως για παράδειγμα πίεση, θερμοκρασία, επίπεδο του φωτός, τοποθεσία.

•Συσκευές με μεγαλύτερη επεξεργαστική ισχύ που μπορεί να αποφασίσουν, χωρίς ανθρώπινη παρέμβαση και δεν χρειάζεται πρώτα να ερωτηθούν, για να επικοινωνήσουν με κάποια άλλη συσκευή. Το τελικό αυτό στάδιο κάνει "Proactive Computing", δηλαδή αυτές οι συσκευές έχοντας επίγνωση του φυσικού τους περιβάλλοντος, απαντούν σε αυτό το πλαίσιο με κάποια μορφή αντίδρασης που πιθανό να προκαλέσει και την αλλαγή του πλαισίου.

Η δύναμη του Διάδικτυο των πραγμάτων και των εφαρμογών που υποστηρίζει οφείλεται στο γεγονός ότι οι συσκευές συνδέονται μεταξύ τους. Οι συσκευές αυτές ορισμένες φορές αποκαλούνται "έξυπνες συσκευές", αν και ομάδες συσκευών δεν χρειάζεται να είναι το ίδιο έξυπνες. Μια gateway device μπορεί να απορρίπτει, να αθροίζει και να ελέγχει τη μορφή των δεδομένων από μια ομάδα απλών αισθητήρων πριν τα στείλει κάπου αλλού. Αυτό είναι ιδίως σημαντικό σε σχέση με την ασύρματη πρόσβαση και την επιλογή της κατάλληλης αρχιτεκτονικής, η οποία μπορεί να ποικίλλει ανάλογα με τις απαιτήσεις της εκάστοτε εφαρμογής.

Η ασύρματη επικοινωνία είναι ζωτικής σημασίας για το Διαδίκτυο των πραγμάτων. Πρώτον είναι προφανές, ότι πρέπει να υποστηρίζεται παντού ώστε να υπάρχει δυνατότητα φορητότητας αφού οι συσκευές, μπορούν να κυκλοφορούν και να μεταφέρονται οπουδήποτε. Δεύτερον, πρέπει να υπάρχει ευελιξία κάτι που δεν είναι δυνατό με τις ενσύρματες επικοινωνίες. Μία νέα συσκευή θα πρέπει να μπορεί να μετακινηθεί σε μια υπάρχουσα ομάδα, έτσι ώστε να αυξηθεί ο αριθμός πραγμάτων και η επεξεργαστική ισχύς της ομάδας και στη συνέχεια θα πρέπει να μπορεί να την εγκαταλείψει ξανά.

Οι διαφορετικές απαιτήσεις που ίσως έχει η κάθε συσκευή, έχει σαν αποτέλεσμα να οδηγήσει όπως ειπώθηκε σε διαφορετικές αρχιτεκτονικές επιλογές εφόσον η κάθε

συσκευή ενδέχεται να χρειάζεται να επικοινωνήσει με άλλες σε οποιαδήποτε απόσταση και με διαφορετικό μέσο επικοινωνίας.
Υπάρχουν συγκεκριμένες τεχνολογίες που είναι κατάλληλες για τις ακόλουθες κατηγορίες.

• κατά μερικά cm (Body Area Network, BAN)
• μερικά m (Personal Area Network, PAN)
• 10 έως 100 m (Local Area Network, LAN)
• μερικά km (Metropolitan Area Network, MAN)
• 10 έως 100 του km (Wide Area Network, WAN)
• 1000 km (Global Area Network)

Η επικοινωνία σε πολύ μακρινή απόσταση, κατά πάσα πιθανότητα θα συνεχίσει να χρησιμοποιεί ένα φορέα παροχής υπηρεσιών, για παράδειγμα ένα κινητό 3G, ή να εκμεταλλεύεται κάποιο σταθερό δίκτυο.
Το Διαδίκτυο των πραγμάτων όπως φαίνεται επιβάλλει μια νέα τάξη δικτύου, που παρουσιάστηκε ως Capillary Networks. Αυτά τα μικρών- αποστάσεων δίκτυα αιχμής είναι η επέκταση των υπαρχόντων δικτύων και υπηρεσιών σε όλες τις συσκευές που είναι εξοπλισμένες με αισθητήρες και ενεργοποιητές.
Στα Capillary Networks ανήκουν τα BAN, PAN και ενδεχομένως τα LAN περιβάλλοντα, με gateway devices που παρέχουν διεπαφή μεταξύ των επιπέδων όπου αυτή χρειάζεται.
Τα Capillary Networks είναι αυτόνομα και αυτό-οργανώνονται λόγω της ευελιξίας τους και της οικονομίας τους. Τα μικρά αυτά δίκτυα δεν πρέπει να επιβαρύνονται με το κόστος διαμόρφωσης, διαχείρισης και συντήρησης τους, ως εκ τούτου το Διάδικτυο των πραγμάτων θα πρέπει να λειτουργεί όπως ακριβώς απαιτεί το "plug and play" με τους ενσύρματους υπολογιστές. Οι γειτονικές συσκευές θα πρέπει να ανταλλάσσουν μηνύματα για να ανακαλύψουν η μία την άλλη και να ρυθμίσουν οι ίδιες την καλύτερη τοπολογία για την ανταλλαγή και την αποστολή μηνυμάτων προς, από και διαμέσω της μιας και της άλλης.
Με τον τρόπο αυτό, το δίκτυο θα μπορεί να αντιδράσει, όταν μια συσκευή φθάνει, φεύγει ή κινείται και θα μπορεί να διατηρηθεί, όταν πρόκειται να υπάρξει παρέμβαση ή διατάραξη των διαύλων επικοινωνίας. Η αυτό-οργάνωση και η δυνατότητα δυναμικής δρομολόγησης αποτελούν βάση για τη βιωσιμότητα και την αξιοπιστία των δικτύων του Διαδικτύου των πραγμάτων.

Η ανάγκη επικοινωνίας των συσκευών στο Διαδίκτυο των πραγμάτων μεταξύ τους οπουδήποτε και αν είναι αυτές εγκατεστημένες στον κόσμο, συνεπάγεται τη σπουδαιότητα της ονοματοδοσίας και της διευθυνσιοδότησης, οι οποίες θα προκύψουν μέσα από κατάλληλη έρευνα και επεξεργασία. Μέσω αυτών θα βρεθεί αν η επιθυμητή συσκευή υπάρχει, πού βρίσκεται, και ποιοι δίαυλοι επικοινωνίας απαιτούνται για τη

μεταξύ των συσκευών επικοινωνία. Επιπλέον οι πληροφορίες που παρέχονται από τις συσκευές αυτές μπορεί τελικά να συγκεντρώνονται και να χρησιμοποιούνται μαζί με τις υπόλοιπες πληροφορίες σε ένα κοινό web server. Το γεγονός αυτό σημαίνει ότι οι συσκευές μπορούν να συνδέονται με μια μοναδική ταυτότητα (μέσω της ονοματοδοσίας και της διευθυνσιοδότησης), η οποία δημιουργεί την επιτακτική ανάγκη για προστασία των προσωπικών δεδομένων και ασφαλή ανταλλαγή πληροφοριών.

Το Διαδίκτυο των πραγμάτων πρέπει να είναι σύμφωνο με τα πρότυπα και τις πρότυπες μεθόδους λειτουργίας. Ενώ η κάθε μεμονωμένη εφαρμογή πρέπει να έχει την δυνατότητα να χρησιμοποιεί τη δικές της ειδικές συσκευές, τα δικά της πρωτόκολλα και τους δικούς του τρόπους λειτουργίας, είναι συμφέρον όταν είναι άμεσα διαθέσιμες συνήθεις διαλειτουργικές πλατφόρμες να χρησιμοποιούνται αυτές.

Πρέπει να εξελιχθούν οι υπηρεσίες πλατφορμών πέρα από την τρέχουσα "στατική" διαμόρφωση υπηρεσιών και να προχωρήσουν προς την κατεύθυνση της παροχής υπηρεσιών σε προσανατολισμένες αρχιτεκτονικές. Σήμερα, οι υπηρεσίες είναι προγραμματισμένες και δεν μπορούν να προσαρμοστούν δυναμικά στις μεταβαλλόμενες απαιτήσεις και στα πλαίσια εφαρμογής. Η διαλειτουργικότητα εξακολουθεί να απαιτεί από τους χρήστες να γνωρίζουν τις δυνατότητες που προσφέρονται από τους παρόχους και τις αντίστοιχες υπηρεσίες τους από πριν. Αυτή η "closedworld" προσέγγιση συνεπάγεται ότι όλες οι client υπηρεσίες και τα χαρακτηριστικά αυτών είναι γνωστά εκ των προτέρων. Από την άλλη, η σημασιολογική μοντελοποίηση θα πρέπει να καταστεί δυνατό για τους service requestors να μπορούν να καταλάβουν ποια υπηρεσία και ποιοι πάροχοι μπορούν να προσφερθούν. Αυτό αποτελεί βασικό ζήτημα για την πορεία προς μια "open-world" προσέγγιση, όπου νέα, άγνωστα ή τροποποιημένα προϊόντα-υπηρεσίες μπορεί να εμφανιστούν σε οποιαδήποτε χρονική στιγμή. Αυτό έχει σαν συνέπεια να υπάρξουν ενδιάμεσες απαιτήσεις, όπως αυτές που χρειάζονται για τη διασύνδεση μεταξύ των συσκευών. Αυτό είναι ένα βασικό στοιχείο για την πρόοδο των δικτυακών συσκευών που τις καθιστά ικανές να προσαρμόζονται δυναμικά στις αλλαγές του πλαισίου που μπορεί να επιβληθούν από τα σενάρια εφαρμογής (π.χ. μετάβαση από την παρακολούθηση της λειτουργίας σε κατάσταση συναγερμού με σκοπό την επαγρύπνηση το οποίο μπορεί να συνεπάγεται διαφορετικές υπηρεσίες καθώς και την εφαρμογή διαφορετικών συμπεριφορών).

Το Διαδίκτυο των πραγμάτων πρέπει να είναι αξιόπιστο για την αντιμετώπιση πιθανής δυσλειτουργίας της συσκευής, κατεστραμμένης κίνησης δεδομένων ή κακόβουλης επίθεσης. Θα πρέπει οι πολιτικές διασφάλισης όσον αφορά την ιδιοκτησία των πληροφοριών και την δικαιοδοσία πρόσβασης στην συσκευή, να είναι έτσι θεσμοθετημένες ώστε να σέβονται το δικαίωμα του ανθρώπου στην ιδιωτικότητα.

1.3.2 Τεχνολογικές απαιτήσεις

Οι κύριες τεχνολογικές προκλήσεις εμφανίζονται και αναλύονται παρακάτω:

- Μέγεθος
- Κόστος
- Τροφοδοσία και ενεργειακή απόδοση
- Αισθητήρες
- Εγκατάσταση συσκευών
- Ειδικές συνθήκες περιβάλλοντος

Το μέγεθος των υφισταμένων RFID είναι περίπου:
10 cm x 4 cm για 900 MHz λειτουργία
6 cm x 1 cm για 2,45 GHz λειτουργία.

Έχει αναφερθεί ότι η Hitachi διαθέτει ένα ενσωματωμένο μικροτσίπ για το RFID με εμβαδό 0,15 mm^2 και πάχος 7,5 μm. Η πρόοδος όσον αφορά πολλές εφαρμογές, για παράδειγμα τις ηλεκτρονικές ταυτότητες, τα τραπεζογραμμάτια και τη σήμανση μικρών αντικειμένων θα εξαρτηθεί από τη μείωση του μεγέθους τους. Οι πραγματικά αόρατοι αισθητήρες που χρειάζονται σε ορισμένες περιπτώσεις δικτύωσης απαιτούν ακόμα πιο δραματική μείωση του μεγέθους τους. Η τεχνολογική κοινότητα μίλησε για μικρού μεγέθους συσκευές της τάξης των κόκκων άμμου ("smart sand") και για ακόμη μικρότερες ("smart dust"), αν και αυτά είναι φιλοδοξίες παρά προβλέψεις.

Το κόστος των RFID είναι της τάξης των € 0,50 για της κοινής χρήσης ετικέτες και τις εφαρμογές εντοπισμού προϊόντων, αλλά αυξάνονται δραματικά πέρα από € 25 για τις πιο εξελιγμένες συσκευές που χρησιμοποιούνται για παράδειγμα σε αυτοκινητόδρομο με διόδια. Η προσπάθεια για ευρύτερη εφαρμογή εξαρτάται πολύ από το χαμηλό κόστος. Το τυπωμένο κύκλωμα είναι μια πιθανή λύση και μια προσπάθεια να δοθεί σημαντική ώθηση στην πράξη, για την κατασκευή μικρότερης κλίμακας και όγκου ετικετών.

Η λειτουργικότητα πολλών εφαρμογών εξαρτάται από *την τροφοδοσία και την εξοικονόμηση ενέργειας* και από άλλες επιμέρους δυσκολίες. Οι συσκευές πρέπει να έχουν μακρά διάρκεια ζωής χωρίς να χρειάζεται αλλαγή των μπαταριών τους. Και αυτό γιατί οι καταναλωτές δεν θα αποδεχτούν συσκευές που απρόσμενα δε θα λειτουργούν ή θα έχουν την ανάγκη για αντικατάσταση της μπαταρίας τους. Σε άλλες εφαρμογές, όπως για παράδειγμα η παρακολούθηση των συνθηκών ενός χώρου, το ίδιο το κόστος πρόσβασης για αλλαγή των μπαταριών μπορεί να είναι από μόνο του απαγορευτικό.

Η τεχνολογία των αισθητήρων πρέπει να εξελιχθεί. Σε πολλές περιπτώσεις αισθητήρων πολύ μικρών διαστάσεων απαιτείται περαιτέρω έρευνα και ανάπτυξη (**R**esearch&**D**evelopment). Επιπλέον, οι αισθητήρες πρέπει να είναι εφοδιασμένοι με δυνατότητα επικοινωνίας αλλά και με τέτοια χαρακτηριστικά ώστε να καλύπτουν οποιαδήποτε ανάγκη. Αυτά τα ζητήματα είναι ακόμα στο πεδίο της R&D λόγω του ότι αυτές οι επικοινωνίες και τα χαρακτηριστικά αυτών των υπηρεσιών συγκριτικά με τις συσκευές έχουν σημαντική επίπτωση στο κόστος.

Η τοποθέτηση ετικετών και αισθητήρων δεν είναι πάντα εύκολη, οπότε χρειάζεται να αναπτυχθούν τρόποι για να γίνεται σταθερή σηματοδοσία σε ορισμένες εφαρμογές. Αυτό είναι σημαντικό ειδικά αν ένας αισθητήρας πρέπει να παραμείνει σε σταθερή επαφή με το υπό μελέτη αντικείμενο, όπως για παράδειγμα η μέτρηση θερμοκρασίας σε επιφάνεια. Έχει αναφερθεί ότι οι μέθοδοι της 3D εκτύπωσης,laser sintering και material deposition ως τεχνικές συγκόλλησης αισθητήρων σε επιφάνειες μπορεί να είναι κατάλληλες.

1.3.3 Απαιτήσεις Δικτύωσης

Η δικτύωση των συσκευών είναι ένα πολύπλευρο ζήτημα που έχει επιπτώσεις σε διάφορα στρώματα, τόσο στα περιφερειακά όσο και στο ίδιο το δίκτυο.

Οι προσδοκίες που υπάρχουν ως προς τη δικτύωση μπορούν να έρχονται σε σύγκρουση με τη φυσική πραγματικότητα των συσκευών. Θα ήταν προτιμότερο να χρησιμοποιηθούν έξυπνα πρωτόκολλα, για παράδειγμα για την αυτο-αναγνώριση του δικτύου και την προσαρμοστικότητα του συστήματος, αλλά αυτά έγκεινται στην επεξεργαστική ισχύ των συσκευών. Την ίδια στιγμή, όλα αυτά θα πρέπει να τρέχουν σε απειροελαχίστου μεγέθους συσκευές που δεν καταναλώνουν ενέργεια. Αυτό το σύνολο των αλληλοσυγκρουόμενων ζητημάτων απαιτεί έναν end-to-end σχεδιασμό του συστήματος και τη βελτιστοποίηση του. Μάλιστα, ορισμένες βασικές απαιτήσεις πρέπει να σχεδιαστούν από την αρχή. Σε αυτές συμπεριλαμβάνονται η προσαρμοστικότητα, η ικανότητα εξέλιξης, η ασφάλεια και η προστασία της ιδιωτικότητας. Η μεταγενέστερη εισαγωγή αυτών των χαρακτηριστικών δε θα είναι αποτελεσματική.

Τα κύρια ζητήματα όσο αφορά το Διαδίκτυο των πραγμάτων περιγράφονται παρακάτω:
• Ετερογενές Δίκτυο (Network heterogeneity)
• Πρότυπα (Standards)
• Πρωτόκολλα (Lightweight protocols)
• Protocol delayering (layers co-design)
•Αυτόνομα αυτό-οργάνωτα δίκτυα και προσαρμοστικότητα (Autonomous self-organising networks and adaptivity)

• Network discovery
• Dynamic routeing
• Βιωσιμότητα του δικτύου και αξιοπιστία (Network survivability and dependability)
• Εξελιξιμότητα (Network scalability)
• Στρατηγική ονοματοδοσίας και διευθυνσιοδότησης (Naming and addressing strategies)
• Δηλωτικός Προγραμματισμός (Declarative programming)
• Διεπαφές προγραμματισμού και εφαρμογών (Programming platforms and application program interfaces (APIs))
• Διαχείριση της κυκλοφορίας και της συμφόρησης (Traffic and congestion management)
• Πραγματικού χρόνου λύσεις και ανεκτικότητα καθυστέρησης (Real time resolution and delay tolerance)
• Διαχείριση σφάλματος: εντοπισμός και διόρθωση (Error detection and correction)

Το Διαδίκτυο των πραγμάτων θα πρέπει να είναι ένα ετερογενές δίκτυο, που θα απαρτίζεται από ομόσπονδα *ετερογενή* δίκτυα. Θα πρέπει να φιλοξενεί συσκευές:
• από διαφορετικούς κατασκευαστές
• διαφορετικών ημερομηνιών κατασκευής και επίσημων εκδόσεων
• διαφορετικών δυνατοτήτων και εξειδικεύσεων
• διαφορετικών ταχυτήτων
• που χρησιμοποιούν διαφορετικές τεχνικές διεπαφών
•με συγκλίνουσες διαφορετικές λειτουργίες

Οι συσκευές και οι πύλες θα πρέπει να αναγνωρίζουν αυτές τις διαφορές και να μεσολαβούν όπου είναι απαραίτητο. Για το λόγο αυτό, τα τεχνικά *πρότυπα* είναι απαραίτητα για μια ανοικτή, εξελισσόμενη πλατφόρμα.

Τα πρότυπα που απαιτούνται είναι:

• ενδοεπικοινωνία και διαλειτουργικότητα

• συντονισμός και επικοινωνία του αισθητήρα

• αυτο-οργάνωση και προσαρμοστικότητα

• περιγραφή υπηρεσιών και ικανότητα δήλωσης

• routeing and transport methods

• ραδιο-διεπαφές και πρόσβαση των μέσων

• εντοπισμός και συγχρονισμός

• δημοσίευση και εγγραφή συσκευών και πόρων

• διαχείριση και κράτηση των πόρων καθώς και έλεγχος αποδοχής

• ασφάλεια

• κρυπτογράφηση (end-to-end και hop-by-hop) και διανομή κλειδιών

• user interfaces

Τα πρότυπα πρέπει να είναι επεκτάσιμα, επιτρέποντας στις συσκευές να επικοινωνούν μεταξύ τους στο επίπεδο των κοινών τους λειτουργιών. Οι συσκευές πρέπει να συμπεριφέρονται προβλέψιμα, όταν τους παρουσιάζεται ένα μήνυμα που δεν μπορούν να κατανοήσουν. Για παράδειγμα οι συσκευές διέλευσης πρέπει να μεταδώσουν end-to-end μηνύματα, ακόμη και αν δεν μπορούν να κατανοήσουν ολόκληρο το περιεχόμενο.

Τα υπάρχοντα πρωτόκολλα μετάδοσης δεδομένων μπορεί να είναι ακατάλληλα για το Διαδίκτυο των πραγμάτων. Τα σημερινά πρωτόκολλα χρειάζονται συνήθως εκατοντάδες ή και περισσότερα kilobytes κώδικα (λογισμικού) για την εκτέλεσή τους. Αναφέρθηκε ότι ακόμη και το απλό πρωτόκολλο ZigBee το οποίο είναι κοινό σε εφαρμογές RFID απαιτεί 48 KB στοίβα, η οποία είναι υπερβολικά περίπλοκη για μικροσκοπικούς αισθητήρες. Το πρότυπο OSI, το μοντέλο επτά στρωμάτων έχει επηρεάσει μια ολόκληρη γενιά των τηλεπικοινωνιών και της τεχνολογίας των πρωτοκόλλων. Αυτή η τεχνολογία όμως στην συγκεκριμένη περίπτωση παρουσιάζει περιορισμούς με αποτέλεσμα η κυρίαρχη δικτύωση να απαιτεί νέες προσεγγίσεις. Απαιτούνται *ελαφρύτερα πρωτόκολλα* και ελαφρύτερες εφαρμογές που θα συμπιέσουν τα ρητά στρώματα πρωτοκόλλου σε μια ενιαία ενότητα.

Το Διαδίκτυο των πραγμάτων απαιτεί *αυτο-οργάνωση της δικτύωσης* ώστε να υπάρχει φορητότητα, οικονομία, ευελιξία καθώς επίσης και προσαρμοστικότητα του δικτύου. Η αυτο-οργάνωση της προσαρμοστικότητας είναι απαραίτητη ώστε να μπορεί να αντιμετωπίζει ένα απρόβλεπτο κόσμο, και πρέπει να εξεταστεί από την αρχή. Η αυτό-ανακάλυψη και η αυτο-οργάνωση των δικτύων πλέγματος παραμένουν υπό-ανάπτυξη ώστε να υπάρξουν μέθοδοι και *πρωτόκολλα* που έχουν ως αποτέλεσμα τη βέλτιστη ή έστω την επαρκώς εκτέλεση των δικτύων υπό τις προϋποθέσεις που θέτουν οι απαιτήσεις του Διαδικτύου το πραγμάτων. Τα αυτό-οργανωμένα δίκτυα πρέπει να προσαρμόζονται σε διαφορετικές απαιτήσεις για τις φυσικές και εικονικές τοπολογίες συνδέσμων. Η ανακάλυψη και η επαναχρησιμοποίηση υπηρεσιών από διαφορετικές εφαρμογές έχει πολύ μεγάλη σημασία. Διαφορετικές εφαρμογές μπορεί να απαιτούν διαφορετικές τοπολογίες όπως αστέρα, δαχτυλίδι ή πλήρη διασύνδεση. Η απαίτηση αυτών μπορεί να ποικίλλει ανάλογα με τον τρόπο λειτουργίας είτε αυτός είναι κανονικός, άγρυπνος συναγερμός, καταστροφής ή οποιοσδήποτε άλλος.

Το *dynamic routeing* είναι το αντίστοιχο της αυτο-οργάνωσης όπου τα δίκτυα αναλαμβάνουν νέες διαδρομές μετά την αρχική ανακάλυψη και οργάνωση τους. Αυτό ενδέχεται να προκύψει όταν μια νέα συσκευή φτάνει, μια καλύτερη πορεία κατέστη δυνατή (για παράδειγμα, όταν ένας κινητός κόμβος μετακινηθεί πιο κοντά σε μια πύλη) ή κάποιο πρόβλημα δημιουργηθεί όπως παρέμβασης, απώλειας μιας συσκευής ή ρήξης μιας διαδρομής.

Το Διαδίκτυο των πραγμάτων θα κλιμακωθεί ενδεχομένως σε πολύ μεγάλα δίκτυα πολλών αντικειμένων και συσκευών. Αυτό προϋποθέτει τις σωστές επιλογές σχεδιασμού, μία από αυτές είναι η εξελιξιμότητα. Με τον όρο αυτό υπονοείται η διανομή του επιπέδου ελέγχου και της επεξεργασίας των δεδομένων τα οποία επίσης συμβάλλουν στη *βιωσιμότητα και την ασφάλεια* του δικτύου.

Το Διαδίκτυο των πραγμάτων πρέπει να έχει τη *στρατηγική ονοματοδοσία και διευθυνσιοδότηση* μέσω των οποίων τα αντικείμενα θα μπορούν να προσδιοριστούν μόνα τους και θα μπορούν να εντοπίζουν άλλα αντικείμενα καθώς και τα μονοπάτια της επικοινωνίας τους. Επειδή το δίκτυο είναι ετερογενές, δηλαδή υποστηρίζει πολλές διαφορετικές συσκευές που προσφέρουν διαφορετικούς τύπους υπηρεσιών, θα χρειαστεί μία *δηλωτική διεπαφή*, όπως IDL ή XML. Αυτό θα επιτρέψει σε κάποια συσκευή ή σε κάποιο κόμβο να περιγράψει τι παρουσιάζει στα υπόλοιπα.

Ένα σύνολο από middleware που θα παρέχει *διεπαφές προγραμματισμού*, επικοινωνιών και άλλες υπηρεσίες για εφαρμογές, θα μπορεί απλοποιήσει τη δημιουργία των υπηρεσιών και των εφαρμογών. Οι υπηρεσίες προσέγγισης πρέπει να περάσουν από μια "στατική" προγραμματιζόμενη κατάσταση σε μία κατεύθυνση δυναμικής διαμόρφωσης και ικανότητας σύνθεσης.

Το Διαδίκτυο των πραγμάτων πρέπει να ενσωματώνει *τη διαχείριση της κυκλοφορίας και της συμφόρησης*. Έτσι θα αντιλαμβάνεται και θα διαχειρίζεται τη ροή πληροφορίας, θα ανιχνεύει πιθανές συνθήκες υπερχείλισης και θα εφαρμόζει διαφύλαξη των πόρων για timecritical και life-critical ροές δεδομένων. Σε αυτό το επίπεδο υπάρχουν πολλά περιθώρια εξέλιξης αφού δεν είναι γνωστά ακριβώς τα χαρακτηριστικά της κυκλοφορίας του Διαδίκτυο των πραγμάτων. Τα σχεδιαγράμματα ασυμμετρίας της κυκλοφορίας στα σημερινά δίκτυα που δημιουργούνται από τη διαδραστική χρήση μέσω της ευρυζωνικής πρόσβασης στο Διαδίκτυο ενδέχεται να αλλάξουν ριζικά στο μέλλον. Αυτό που θα μπορούσε να συμβεί στο μέλλον είναι η κίνηση του κύριου όγκου φορτίου δικτύων να μη συμβαίνει από το δίκτυο προς τα τερματικά (downstream), αλλά μάλλον αντίστροφα από τις συσκευές προς τα δίκτυα (upstream). Αυτό με τη σειρά του θα απαιτήσει ευφυείς στρατηγικές στο επίπεδο διαμόρφωσης της κυκλοφορίας και του φιλτραρίσματος και περαιτέρω δυνατότητες επεξεργασίας στην άκρη του δικτύου. Η ικανότητα δικτύωσης των άκρων αναμένεται επίσης να είναι ανάλογη της εφαρμογής, καθώς ορισμένες

κρίσιμες για την ασφάλεια εφαρμογές με πραγματικού χρόνου περιορισμούς, μπορεί να μην είναι συμβατές με την επιπρόσθετη καθυστέρηση που θα επιβάλλεται λόγω μιας τέτοιας επεξεργασίας.

Τα δίκτυα πρέπει να υποστηρίζουν *πραγματικού χρόνου λύσεις*. Για πολλές εφαρμογές η ακολουθία και ο συγχρονισμός των μηνυμάτων μπορεί να έχουν σημασία, παρόλο που η αυτο-οργάνωση των δικτύων και η επικοινωνία που βασίζεται στα πακέτα δεν εγγυώνται ούτε το χρόνο μετάδοσης ούτε και την ακολουθία των ληφθέντων μηνυμάτων.

Τέλος, το Διάδικτυο των πραγμάτων θα πρέπει να υποστηρίζει τη *διαχείριση σφάλματος*. Η διαχείριση μπορεί να καταπονεί την επεξεργαστική ισχύ, τον όγκο των δεδομένων και το χρόνο μετάδοσης. Από την άλλη πλευρά, όμως τα σφάλματα μπορεί να είναι μικρής ανησυχίας σε ορισμένες εφαρμογές αλλά πολύ απειλητικά για κάποιες άλλες.

1.3.4 Απαιτήσεις ασφάλειας και ιδιωτικότητας

Οι άνθρωποι θα αντισταθούν στο Διαδίκτυο των πραγμάτων εάν δεν υπάρχει καμία εμπιστοσύνη σε αυτό. Το Διαδίκτυο των πραγμάτων θα επηρεάσει και θα ελέγχει τα γεγονότα στον πραγματικό κόσμο καθώς θα περιέχει πληροφορίες αξίας. Για το λόγο αυτό είναι σίγουρο ότι θα προσελκύσει και την ανεπιθύμητη προσοχή. Το ψηφιακό έγκλημα γίνεται βιομηχανία από μόνο του και οι εγκληματίες είναι ήδη μέλη της. Όπου η κοινωνία δημιουργεί υψηλή εξάρτηση από κάποια κυρίαρχη τεχνολογική υποδομή, θα υπάρξουν μερικοί που θα θελήσουν να το εκμεταλλευτούν.

Οι δημόσιοι φόβοι είναι πιθανό να επικεντρωθούν σε ορισμένους τομείς της ασφάλειας και της ιδιωτικότητας όπως:

• Ευπάθεια στην επίθεση(Vulnerability to attack)
• Κλωνοποίηση ετικετών και κλοπή ταυτότητας(Tag cloning and identity theft)
• Δικαιώματα πρόσβασης σε δεδομένα(Access rights to data)
• Ποιότητα και ακεραιότητα (Quality and integrity)
• Δέσμευση των προσωπικών στοιχείων(Capture of personal data)
• Διατήρηση των προσωπικών στοιχείων(Retention of personal data)

Υπάρχουν διάφοροι τρόποι για να επιτεθούν στη λειτουργία ενός δικτύου:

• Με καταστροφή κόμβων

•Με εξασθένιση ή καταστροφή της μετάδοσης, παραδείγματος χάριν χρησιμοποιώντας σήματα παρεμβολής
•Με κατακλυσμό του δικτύου με πλαστά μηνύματα (επιθέσεις άρνησης παροχής υπηρεσιών)

Για να αντιμετωπιστούν τα παραπάνω θα πρέπει να αναπτυχθεί η ανθεκτικότητα η οποία μπορεί να κατασκευαστεί σε ένα δίκτυο χρησιμοποιώντας τις τεχνικές της εφαρμοσμένης μηχανικής δικτύων.
Η υπάρχουσα αρχιτεκτονική ασφάλειας θα πρέπει να αναπτυχθεί από την αρχή. Θα πρέπει να συμπεριληφθεί η ασφάλεια και οι κατανεμημένες αρχιτεκτονικές βάσεων δεδομένων και η φιλοσοφία δικτύων που επιτρέπει στις συσκευές να υποχωρούν σε αξιόπιστες συνδέσεις και κατασκευαστικά μέρη σε περίπτωση απειλής. Είναι απαραίτητο να κατανοηθεί και να διαμορφωθεί η λεπτομερής φύση των πιθανών απειλών, ώστε να είναι βέβαιο ότι τα δίκτυα θα είναι πράγματι βιώσιμα. Τα ακόλουθα είναι σχετικές τεχνικές προσεγγίσεις σε επίπεδο δικτύων.

• Dynamic routeing
• Διαχείριση σφαλμάτων
• Διαχείριση της κυκλοφορίας και του ελέγχου ροής των πληροφοριών
• Δυναμική επιλογή του ραδιο-καναλιού
• Diverse routeing
• Περιττή παροχή συσκευών, κόμβων και πόρων επεξεργασίας
•Αρχές σχεδιασμού δικτύων για την ακεραιότητα και την ποιότητα των υπηρεσιών
• Αρχιτεκτονική ασφάλειας και αξιοπιστίας
• Εργαλειοθήκη ασφάλειας και αξιοπιστίας
• Αξιοπιστία στοιχείων

Οι άνθρωποι και τα πράγματα μπορούν να προσποιηθούν για το τι είναι και τι δεν είναι. Για παράδειγμα, ένα πλαστό προϊόν μπορεί να αποκτήσει μια ετικέτα που μπορεί να χαρακτηριστεί ως γνήσια όμως ένα πρόσωπο μπορεί να επιχειρήσει να αποκτήσει την ταυτότητα κάποιου άλλου, γνωστό ως το φαινόμενο της *κλωνοποίησης ετικέτας*.

Μία λύση αποτελεί η μέθοδος δημιουργίας μιας ετικέτας που δεν θα μπορεί να κλωνοποιηθεί, με το να επιστρωθεί με κάποιο αδιαφανές υλικό που περιέχει μόρια υψηλού διηλεκτρικού περιορισμού. Το τυχαίο σχέδιο των μορίων δίνει στη συσκευή ένα "δακτυλικό αποτύπωμα" που είναι δύσκολο ή αδύνατο να αναπαραχθεί.

Η ασφάλεια είναι καλύτερη όταν βασίζεται σε ένα συνδυασμό στοιχείων αντί να βασιστεί σε ένα μόνο στοιχείο. Επίσης η αποτελεσματικότητα της ασφάλεια εξαρτάται από ένα προσανατολισμένο σύστημα που επιτρέπει πολλαπλές ταυτότητες σε διαφορετικά πλαίσια και χρόνους. Προσπάθειες για τη δημιουργία ασφάλειας με τη

χρήση μιας μεμονωμένης συνιστώσας, "μοναδικό κλειδί", μπορεί να αποτύχει και έτσι να γίνει περισσότερο κακό παρά καλό. Ένα παράδειγμα είναι τα βιομετρικά στοιχεία ταυτότητας τα οποία το άτομο δεν μπορεί να ανακαλέσει, σε περίπτωση που κάποιος βρει μια μέθοδο αντιγραφής αυτών θα υπάρξει πολύ μεγάλο πρόβλημα λόγω του ότι πολλά συστήματα στηρίζουν την ασφάλεια τους σε αυτή τη μεμονωμένη συνιστώσα.

Μερικές αρχές αποτελεσματικής ασφάλειας είναι οι εξής:

• Να μην υπάρχει ένα σταθερό αναγνωριστικό.
• Να μοιράζεται η ασφάλεια σε όλα στοιχεία του συστήματος.
• Να επιτρέπονται πολλαπλές μορφές της προσωπικής ταυτότητας.
•Να ποικίλουν οι απαιτούμενες μορφές της ταυτότητας είτε κατά την πάροδο του χρόνου, είτε κατά την ανταλλαγή μηνυμάτων σε κάθε πρόσβαση.
• Το κλείδωμα των στοιχείων ταυτότητας σε συγκεκριμένα πλαίσια.
• Το δικαίωμα του χρήστη να ανακαλέσει το κλείδωμα ταυτότητας.
• Έμφαση στην ασφάλεια και όχι απλή επιτήρηση.

Η προστασία της ιδιωτικότητας είναι ένα θέμα που απασχολεί πολλούς ανθρώπους. Το Διαδίκτυο των πραγμάτων θα συλλέξει πολλά στοιχεία σχετικά με προσωπικές κινήσεις, αγορές και ενέργειες. Με το κόστος αποθήκευσης κάτω από ένα νανο-ευρώ ανά byte, οι πληροφορίες μπορούν να διατηρηθούν επ’αόριστον.
Τα τεχνικά μέτρα για την προστασία της ιδιωτικότητας περιλαμβάνουν:
• κυριότητα των δεδομένων
• δικαιώματα πρόσβασης
• ιδιοκτησία των διαδικασιών
• άδεια για ενδοεπικοινωνία και διαλειτουργικότητα
• ικανότητα εξουδετέρωσης της ετικέτας (tag clipping)

Ωστόσο, τα τεχνικά μέτρα θα επιτύχουν πολύ λιγότερο αν τα κίνητρα είναι ευθυγραμμισμένα ή τα πραγματικά κίνητρα είναι κατά της ιδιωτικότητας.

1.3.5 Απαιτήσεις Ραδιοκυμάτων

Το ραδιοκύματα είναι θεμελιώδους σημασίας για το Διαδίκτυο των πραγμάτων. Πρόκειται για ένα ευέλικτο δίκτυο ασύρματα διασυνδεδεμένων συσκευών, όπου "τα ραδιοκύματα παρέχουν τη μαγεία" της "απανταχού κάλυψης". Θα ήταν σημαντικά περιορισμένο και δε θα μπορούσε να αναπτυχθεί αν όλες οι συνδέσεις ήταν ενσύρματες. Στις μέρες μας, υπάρχουν περίπου δύο δισεκατομμύρια χρήστες κινητών τηλεφώνων και

η συνολική αναλογία ραδιοδιαύλων-ανθρώπων είναι ένα προς ένα. Σύμφωνα με έκθεση της ITU, θα ξεκινήσει μια εποχή όπου το ποσοστό αυτό θα υπερβεί τα 1000 προς έναν.

Η αποδοτικότητα της χρήσης των ραδιοκυμάτων αποτελεί συγχρόνως μια απαίτηση και μια τάση. Επί του παρόντος, η κατάσταση που ισχύει είναι ένα με πέντε bits ανά δευτερόλεπτο ανά Hz ανά κελί.
Οι τεχνολογίες διεπαφών στον αέρα για το Διαδίκτυο των πραγμάτων, γνωστές ως εναλλακτικές ασύρματες τεχνολογίες (AWTs), παραμένουν κύριος στόχος ανάπτυξης. Οι υφιστάμενες τεχνολογίες που είναι πιθανό να αποτελέσουν τη βάση τους, είναι οι ακόλουθες:

• ZigBee (IEEE 802.15.4)
• WiMax (IEEE 802.16)
• WiFi (IEEE 802.11 παραλλαγές)
• Bluetooth (IEEE 802.15.1)
• UWB (IEEE 802.15.3a)
• Flash OFDM (IEEE 802,20)

Είναι πιθανό ότι το Διαδίκτυο των πραγμάτων, ή τουλάχιστον σημαντικά τμήματά του, θα χρησιμοποιήσουν ευρέος φάσματος τεχνολογίες κατά προτίμηση τις πιο παραδοσιακά τρέχουσες προσεγγίσεις μονής συχνότητας.
Η διάδοση του ευρέος φάσματος τεχνολογιών στέλνει το σήμα σε ένα ευρύ φάσμα συχνοτήτων, αλλά με πολύ χαμηλή ενέργεια σε κάθε μία ξεχωριστή μπάντα. Τα σήματα μοιάζουν με λευκό θόρυβο. Αυτό δε συμβαίνει όμως για δέκτες που είναι εξοπλισμένοι με κώδικες να τα αποκρυπτογραφούν. Οι λόγοι υπέρ των τεχνολογιών των ραδιοκυμάτων έχουν ως εξής:

• Είναι φασματικώς πιο αποτελεσματικές.
• Είναι λιγότερο ευάλωτες σε παρεμβολές από μονής συχνότητας σήματα. Αυτό θα μπορούσε να αποδειχθεί ζωτικής σημασίας για περιβάλλοντα, όπως αυτό του αυτοκινήτου.
• Είναι πιο ευπροσάρμοστες. Μπορούν να μεταφέρουν την ενέργεια του σήματος σε λιγότερο γεμάτες μπάντες.
Αυτό τους δίνει μεγαλύτερη ανοχή στην παρέμβαση, ενώ ταυτόχρονα τα ίδια προκαλούν λιγότερες παρεμβολές στους γειτονικούς χρήστες.

Το Διαδίκτυο των πραγμάτων απαιτεί σημαντικά βήματα προόδου στην τεχνολογία ραδιοφάσματος.

•Cognitive radio: τα ραδιοκύματα αντιλαμβάνονται τις μεταδόσεις που φθάνουν σε αυτούς καθώς και το επίπεδο των παρεμβολών.

• Gap finding: τα ραδιοκύματα βρίσκουν τις καλύτερες ζώνες συχνοτήτων για χρήση.
•Software defined radio: πομπός και δέκτης δεν είναι συνδεδεμένοι σε μία συχνότητα, σε ένα MAC πρωτόκολλο και σε μια μορφή μηνύματος, αλλά μπορεί να ποικίλλουν, όπως ορίζονται από κάποιο αποθηκευμένο πρότυπο.
• Smart antennae: εναέρια συστήματα μπορεί να διαφέρουν στη λήψη, στην κατεύθυνση και στο διάγραμμα ακτινοβολίας σύμφωνα με ένα αποθηκευμένο πρότυπο.

1.4 Προοπτικές εφαρμογής

Οι πιθανές χρήσεις της τεχνολογίας του Διαδίκτυο των πραγμάτων δεν έχουν όριο. Καλύπτουν πολλές ιδέες εφαρμογών, συμπεριλαμβανομένων των:

• τρεχουσών κερδοφόρων εφαρμογών

• εφαρμογών δοκιμής και επίδειξης

• προγραμματισμένων εφαρμογών

• υποθετικών εφαρμογών

Το Διαδίκτυο των πραγμάτων αποτελεί συγχώνευση του φυσικού και ψηφιακού κόσμου. Δημιουργεί ένα χάρτη του πραγματικού κόσμου μέσα στον εικονικό. Ο υπολογιστής αντιλαμβάνεται το φυσικό κόσμο, ανάλογα με τα χαρακτηριστικά του δικτύου αισθητήρων, με υψηλή χρονική και χωρική ανάλυση. Με άλλα λόγια, μπορεί να κατέχει πολλές αναλυτικές πληροφορίες. Ο υπολογιστής αντιλαμβάνεται τον πραγματικό κόσμο όχι όπως ακριβώς ο άνθρωπος, αλλά μπορεί να απαλλαγεί από τους περιορισμούς που επιβάλλονται από την ανθρώπινη κατανόηση.

Το Διαδίκτυο των πραγμάτων μπορεί να αντιδρά αυτόνομα στον πραγματικό κόσμο. Αυτό είναι γνωστό ως proactive computing. Το πώς αντιλαμβάνεται ένας υπολογιστή τον κόσμο του επιτρέπει να αλληλεπιδρά με το φυσικό κόσμο και να τον επηρεάζει. Μπορεί να τρέχει διαδικασίες χωρίς να χρειάζεται από τον άνθρωπο "να πατάει κάποιο κουμπί". Το Διαδίκτυο των πραγμάτων δεν είναι απλώς ένα εργαλείο για να επεκταθεί η ανθρώπινη ικανότητα. Γίνεται μέρος του περιβάλλοντος στο οποίο οι άνθρωποι ζουν και εργάζονται, και έτσι δημιουργεί ένα οικονομικά, κοινωνικά και προσωπικά καλύτερο περιβάλλον. Στον τομέα της βιομηχανίας και του εμπορίου, το Διαδίκτυο των πραγμάτων μπορεί να επιφέρει αλλαγή των επιχειρηματικών διαδικασιών.

Οι RFID εφαρμογές έχουν εγκατασταθεί και θα παραμείνουν ενώ τεχνικά πρότυπα αρχίζουν να προκύπτουν. Η πλειονότητα των επιτυχημένων εφαρμογών αυτή την περίοδο χρησιμοποιούν RFID στη διαδικασία της βιομηχανικής και εμπορικής

παρακολούθησης και στη διαχείριση περιουσιακών στοιχείων. Πιστεύεται ότι έχει επιτευχθεί απόδοση των επενδύσεων εντός 6-12 μηνών. Οι περισσότερες επιστροφές αναμένεται να γίνουν όταν η παρακολούθηση θα εφαρμόζεται σε υψηλής αξίας κινητά στοιχεία που μέχρι σήμερα δεν έχουν δομημένο χειρισμό. Η απόδοση είναι πιθανό να είναι λιγότερο σημαντική σε περιπτώσεις κατά τις οποίες τα RFID αντικαταστήσουν το δομημένο χειρισμό που βασίζεται σε παλαιότερες τεχνολογίες, για παράδειγμα barcodes ή χειροκίνητα συστήματα βασισμένα στο χαρτί.

Ο ανασχεδιασμός της επιχειρηματικής διαδικασίας δεν είναι απαραιτήτως απλός. Ορισμένες εφαρμογές μπορεί να λειτουργήσουν χωρίς ανθρώπινη εισαγωγή. Σε άλλες περιπτώσεις, η ανθρώπινη παρουσία και η συμμετοχή θα είναι δύσκολο να παραλειφθεί, ακόμη και στο απλούστερο επίπεδο του πατήματος του κουμπιού ώστε να ξεκινήσει η διαδικασία. Μερικές εφαρμογές μπορεί να αποσκοπούν στη συμπλήρωση, υποβοήθηση και στον εμπλουτισμό και όχι στην αντικατάσταση του ανθρώπινου ελέγχου της διαδικασίας.

Η αυτοκινητοβιομηχανία είναι πιθανόν να αποτελέσει σημαντικό χρήστη του Διαδικτύου των πραγμάτων. Αναμένεται ότι το ποσοστό των αυτοκινήτων που περιέχουν ενσωματωμένο σύστημα τηλεματικής θα αυξηθεί σε 43% το 2010. Τα κίνητρα για τη χρήση ραδιοκυμάτων στα αυτοκίνητα, παρά το γεγονός ότι πρόκειται για ένα δύσκολο ηλεκτρικά περιβάλλον για την ασύρματη μετάδοση, ήταν η παραμετροποίηση, η ευελιξία, τη καινοτομία και η απλούστευση της κατασκευής.

Η τηλεματική πλατφόρμα για αυτοκίνητο είναι υπό κατασκευή. Αυτή θα χρησιμοποιεί τις επικοινωνίες για:

• την παρακολούθηση των αυτοκινήτων

• τις υποδομές του αυτοκινήτου καθώς και τις υποδομές της επικοινωνίας μεταξύ των αυτοκινήτων

• τη συνεργασία οχήματος με όχημα

Οι κατασκευαστές μπορούν να χρησιμοποιούν την τεχνολογία αισθητήρων για τη δημιουργία επεκτάσιμων προϊόντων. Αυτό προσθέτει αξία στα φυσικά αγαθά παρέχοντας ένα στοιχείο υπηρεσίας. Η ρομποτική σήμερα συνήθως συνδέεται με τις κατασκευές και τις επιχειρήσεις, ωστόσο πιστεύεται πως η αγορά της ρομποτικής που σχετίζεται με το σπίτι μπορεί να υπερβεί τη βιομηχανική αγορά δέκα με είκοσι φορές.

Η εγχώρια αγορά κυρίως στον τομέα της υγειονομικής περίθαλψης, προσθέτει επιπλέον απαιτήσεις για ελαφριές και λειτουργικές συσκευές.

Η επιτυχής ανάπτυξη των εφαρμογών εξαρτάται από την ανάπτυξη των τεχνικών πλατφορμών και από τις κατάλληλες προδιαγραφές τους. Αυτές περιλαμβάνουν:

• Service object architecture (SOA)

• Ψηφιακή κατασκευή

• Ευέλικτη κατασκευή

• Έξυπνη κατασκευή

• Ανάσυρση δεδομένων

• Διαχείριση δεδομένων

•Manufacturing and user interfaces

• Δυνατότητα χρησιμοποίησης

• Product representations

• Μέσα εξατομίκευσης

Τα δίκτυα των αισθητήρων και οι κυρίαρχες προσεγγίσεις δικτύωσης παρουσιάζουν, επίσης, μεγάλο ενδιαφέρον για τη βιομηχανία κινητών. Το πλαίσιο εφαρμογής που χρησιμοποιούν οι κινητές συσκευές με διάφορες δυναμικά πλατφόρμες παροχής υπηρεσιών αποτελούν αντικείμενο έρευνας από φορείς εκμετάλλευσης της κινητής τηλεφωνίας. Πιλοτικά συστήματα υπάρχουν ήδη δείχνοντας τη δυνατότητα μιας φορητής συσκευής να αλληλεπιδρά με το περιβάλλον, π.χ. σε διάφορα πλαίσια των καταναλωτών. Ένας σημαντικός κατασκευαστής της ΕΕ έχει ξεκινήσει επίσης μια πρωτοβουλία που ονομάζεται "Sensor Planet", το οποίο αποτελείται από μια πλατφόρμα δοκιμής για την έρευνα κινητών-κεντρικών ασύρματων δικτύων αισθητήρων. Η συντριπτική πλειοψηφία της ερευνητικής πρόκλησης στο πλαίσιο των κινητών επικοινωνιών με τις συσκευές σχετίζεται με την πλατφόρμα παροχής υπηρεσιών και με την απαίτηση διάθεσης "ενήμερων υπηρεσιών" που θα μπορούν να αντιδράσουν δυναμικά και να προσαρμοστούν στο περιβάλλον.

1.4.1 Λίστα εφαρμογών

Παρακάτω ακολουθεί μια ταξινομημένη λίστα των εφαρμογών του Διαδικτύου των πραγμάτων. Η παρούσα έκθεση δεν σημαίνει ότι έχει συμπεριλάβει κάθε δυνατή εφαρμογή αυτής της τεχνολογίας. Ωστόσο, αυτό δίνει μια εικόνα του φάσματος των δυνατοτήτων της. Σημειώνεται ότι δεν υπάρχει καμία προφανής απειλητική εφαρμογή. Αυτός είναι ένας επιπλέον λόγος για τον οποίο το πρότυπο υποδομής αυτής είναι αναγκαίο.

Στρατιωτικές εφαρμογές

Βιομηχανία πετρελαίου και φυσικού αερίου

Βιομηχανία εξόρυξης

Έξυπνα κτήρια

- Αυτοματοποιημένη οικοδόμηση

Μεταφορές

- Παρακολούθηση της θερμοκρασίας που φέρουν τα σιδηροδρομικά οχήματα
- Πρόβλεψη μέσων συντήρησης
- Έγκαιρος έλεγχος της διάρκειας ζωής
- Διοικητικές μέριμνες μεταφορών
- Ναυτιλία
- Επικόλληση ετικετών και πληρωμή
- Κινητά τηλέφωνά που θα αλληλεπιδρούν με τα συστήματα πληρωμών

Αυτοκινητοβιομηχανία

- Ευφυή ελαστικά
- Ταυτότητα οχημάτων
- Σήματα αυτοκινητόδρομων

- Συνεταιριστική οδήγηση οχήματος με όχημα
- Εσωτερική αρχιτεκτονική ελέγχου οχημάτων
- Τηλεματική οχημάτων
- Υποδομές επικοινωνίας μεταξύ οχημάτων: οδικές υπηρεσίες πληροφοριών
- Ανακύκλωση των υλικών των οχημάτων
- Ανίχνευση: ζώνης ασφαλείας, άνοιγμα πόρτας, θερμοκρασίας, βροχής
- Αισθητήρα στάθμευσης

Έλεγχος περιβαλλοντικών συνθηκών

- Έλεγχος πληθυσμού πτηνών
- Μετεωρολογικός έλεγχος
- Ανίχνευση ακτινοβολίας
- Έλεγχος των κυμάτων και των ακτών
- Ανίχνευση τσουνάμι
- Παρακολούθηση του επίπεδου των ποταμών
- Έλεγχος ρύπανσης των υδάτων

Αλυσίδες εφοδιασμού και διαχείριση των προϊόντων

- Ολοκλήρωση της αλυσίδας εφοδιασμού
- Ολοκλήρωση κύκλου ζωής προϊόντος
- Διαχείριση απογραφής εμπορευμάτων
- Αποθήκευση ανταλλακτικών
- Διαχείριση αποθήκης
- Ποιοτικός έλεγχος
- Έλεγχος σειριακού αριθμού
- Διαχείριση υπηρεσιών τομέων

Κινητή διαχείριση ιδιόκτητων στοιχείων

- Ασφαλής εντοπισμός οχημάτων αερολιμένα
- Έλεγχος συντήρησης εργαλείων αεροπλάνων
- Χειρισμός απορριμμάτων
- Διαχείριση επικίνδυνων αποβλήτων
- Γεωλογία

Διαχείριση διαδικασιών

- Επεξεργασία κατασκευής ημιαγωγών, μετακινήσεις παρτίδας
- Βιομηχανική Ρομποτική
- Telerobotics (μακρινός έλεγχος ρομπότ)
- Τηλεπαρουσίαση: κάμερα / βίντεο εγγραφής
- Έλεγχος αγωγών υγραερίου

Έλεγχος δραστηριοτήτων συμμόρφωσης

- Πυρίμαχα παραθυρόφυλλα
- Πυρίμαχες θύρες
- Συναγερμοί καπνού
- Δρόμοι διαφυγής
- Εγκαταστάσεις καθαρισμού

Γεωργία

- Παρακολούθηση της αλυσίδας προσφοράς τροφίμων («από το χωράφι στο πιάτο")
- Παρακολούθηση των ζώων
- Φυτοπροστασία

Διαχείριση λιανικής

- Έλεγχος ραφιών
- Καλάθι αγορών / κατάλογος αγορών
- Εντοπισμός κατεύθυνσης εντός του καταστήματος
- Προβολή διαφημίσεων
- Αισθητήρας ελέγχου
- Μηχανές πώλησης
- Ετικέτες εμπορευμάτων
- Κινητά τηλέφωνα που θα αλληλεπιδρούν με τα συστήματα πληρωμών
- Μισθωμένο εξοπλισμό παρακολούθησης

Ασφάλεια

- Ανίχνευση πλαστών εμπορευμάτων
- Έλεγχος πρόσβασης
- Τραπεζογραμμάτια
- Διαβατήρια

Κυβέρνηση και δημόσιος τομέας

- Διαχείριση καταστροφών
- Διαχείριση πυρκαγιάς
- Υποστήριξη τουρισμού
- Εσωτερική ασφάλεια: ειδικός, πρόσθετος έλεγχος γεγονότων

Συστήματα πληροφόρησης

- Πινακίδες και σήματα

Σπίτι

- Απομακρυσμένη παρακολούθηση κλειδαριών
- Απομακρυσμένες οικιακές μέτρησεις
- Δίκτυο οικιακών συσκευών
- Οικιακή αυτοματοποίηση
- Οικιακή ρομποτική
- Βοηθός καθημερινότητας (βοηθά στο να βρίσκονται τα πράγματα)
- Τρόπος ζωής: επιλογή μουσικής, τηλεοπτικών προγραμμάτων
- Περιβάλλοντα ψυχαγωγίας
- Έλεγχος τροφίμων (" Διαδίκτυο-ψυγείο")
- Διαχείριση της ενέργειας
- Αυτόματα παραθυρόφυλλα

Ελεύθερος χρόνος και αναψυχή

- Αθλητικός εξοπλισμός: έλεγχος επιδόσεων χρηστών

Υγεία

- Παρακολούθηση ασθενών στο σπίτι
- Ταυτοποίηση και παρακολούθηση φαρμάκων
- Σύστημα παρακολούθησης: ΗΚΓ, σφυγμού, θερμοκρασίας, πίεσης του αίματος
- Παρακολούθηση της ζωής των ασθενών (εντατικής θεραπείας)

1.5 Ευρωπαϊκά έργα σχετικά με το Διαδίκτυο των πραγμάτων:

• PROMISE (6° πλαίσιο, ολοκληρωμένο έργο, 507100) Διαχείριση του κύκλου ζωής των προϊόντων και των πληροφοριών παρακολούθησης με χρήση έξυπνων ενσωματωμένων συστημάτων.

• EYES (5° πλαίσιο IST-2001-34734) Ενεργειακά αποτελεσματικά δίκτυα αισθητήρων

• e-SENSE (6° πλαίσιο, ολοκληρωμένο σχέδιο, 027227) Αποκόμιση περιβάλλουσας νοημοσύνης για κινητές επικοινωνίες μέσω ασύρματων δικτύων αισθητήρων

• MAGNET (6° πλαίσιο, ολοκληρωμένο έργο, 507102) Προσωπικά προσαρμόσιμα παγκόσμια δίκτυα

• Runes (6° πλαίσιο, ολοκληρωμένο σχέδιο, 004536) Αναδιαρθρώσιμα απανταχού δικτυωμένα ενσωματωμένα συστήματα

• UbiSec&Sens (6° πλαίσιο, ειδικά στοχοθετημένα ερευνητικά έργα, 506926) Απανταχού εξειδικευμένα δίκτυα με τη διασφάλιση της παροχής των υπηρεσιών, την πρόσβαση, την παράδοση και το περιεχόμενο τους

• CRUISE (6ο, δίκτυο αριστείας, 027738) Δημιουργία απανταχού ευφυών αισθητήρων περιβάλλοντος

1.6 Συμπεράσματα

Αρχικός στόχος του κεφαλαίου ήταν να γίνει προσέγγιση της ιδέα του Διαδικτύου των πραγμάτων και να αναλυθεί η υπάρχουσα τεχνολογία. Επίσης σύμφωνα με κάποιες αρχές που πρέπει να διέπουν το Διαδίκτυο των πραγμάτων, αναφέρθηκαν τεχνολογίες που θα μπορέσουν να αποτελέσουν την βάση για την περαιτέρω ανάπτυξη και εξέλιξη τους ώστε να μπορούν να εφαρμοστούν σε αυτό. Αναλύθηκαν επίσης οι απαιτήσεις συστήματος, δικτύωσης, ασφάλειας και ραδιοκυμάτων.

Συγχρόνως η ανάπτυξη του Διαδικτύου των πραγμάτων, που βασίζεται στο συνδυασμό διαφόρων επιστημονικών κλάδων και τεχνολογιών, δημιουργεί τεράστιες ευκαιρίες για τη βελτίωση της οικονομικής ανταγωνιστικότητας και της ποιότητας της ζωής των πολιτών, αλλά επίσης εγείρει περίπλοκα μη τεχνολογικά θέματα, ιδίως όσον αφορά την δεοντολογία, την ιδιωτικότητα, την ασφάλεια, τη διακυβέρνηση, το φάσμα, τη διαλειτουργικότητα, και άλλα, τα οποία αξίζουν τη μέγιστη προσοχή από τις δημόσιες αρχές, κατά προτίμηση στο πλαίσιο ενός σταθερού και καλά εστιασμένου διεθνούς διαλόγου.

1.7 Βιβλιογραφία

http://www.iot-visitthefuture.eu/

http://www.future-internet.eu/home.html

http://en.wikipedia.org/wiki/RFID

http://en.wikipedia.org/wiki/Internet_of_Things

http://www.ieee.com

http://www.itu.com

European Commission, Information Society and Media Directorate-General: From RFID to the Internet of Things, Pervasive networked systems, www.iot-visitthefuture.eu,2006

Communication from the commission to the European parliament, the council ,the European economic and social committee and the committee of the regions, early Early Challenges regarding the "Internet of Things",{COM(2008) aaa},{SEC(2008) bbb}

Maarten Botterman for the European Commission,Information Society and Media DirectorateGeneral:Internet of Things: an early reality of the Future Internet, Prague, http://ec.europa.eu/information_society/tl/policy/, 2009

Waldner, Jean-Baptiste . *Inventer l'Ordinateur du XXIeme Siècle*. London: Hermes Science. pp. p254. ISBN 2746215160, 2007

Waldner, Jean-Baptiste . *Nanocomputers and Swarm Intelligence*. London: ISTE. pp. p227-p231. ISBN 1847040020, 2008

Gérald Santucci. From Internet of Data to Internet of Things, Presented at International Conference on Future Trends of the Internet,2009

Κεφάλαιο 2ο

IPv6

2.1 Εισαγωγή για το IPv6

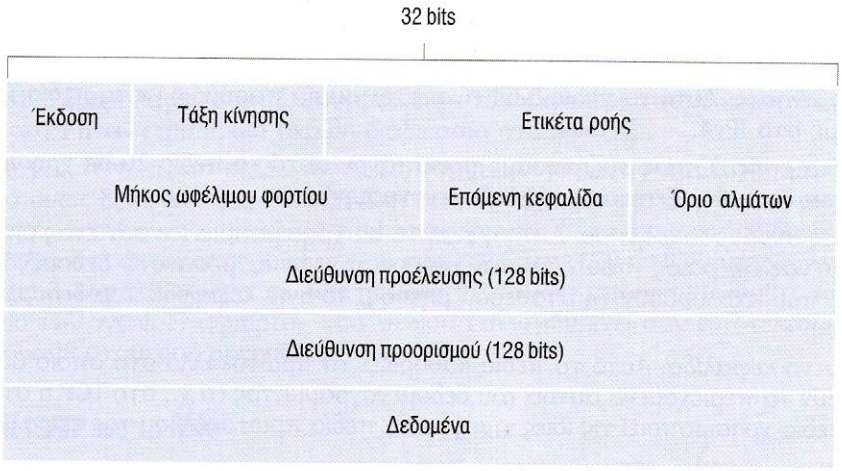
Στις αρχές της δεκαετίας του '90, η IETF ξεκίνησε μια προσπάθεια ανάπτυξης πρωτοκόλλου διάδοχου του IPv4. Ένα βασικό κίνητρο για αυτή την προσπάθεια είναι ότι ο χώρος διευθύνσεων IP 32-bit άρχισε να εξαντλείται, επειδή τα δίκτυα και οι κόμβοι IP συνδέονταν στο Διαδίκτυο (και έπαιρναν μοναδικές διευθύνσεις IP), με ταχύτατο ρυθμό. Για να ικανοποιηθεί η ανάγκη για ένα μεγάλο χώρο διευθύνσεων IP, αναπτύχθηκε ένα νέο πρωτόκολλο, το IPv6. Οι σχεδιαστές του IPv6 άρπαξαν επίσης την ευκαιρία να ρυθμίσουν και να επαυξήσουν και άλλα χαρακτηριστικά του IPv4, με βάση την εμπειρία λειτουργίας που είχαν με το IPv4.
Το χρονικό σημείο που οι διευθύνσεις IPv4 θα είχαν δεσμευθεί πλήρως (και κανένα νέο δίκτυο δεν θα μπορούσε να συνδεθεί στο Διαδίκτυο) ήταν το θέμα μεγάλης διαμάχης. Με βάση τις τρέχουσες τάσεις σε κατανομή διευθύνσεων, οι εκτιμήσεις των δύο αρχηγών της ομάδας εργασίας Address Lífetime Expectations της IETF ήταν ότι οι διευθύνσεις θα είχαν εξαντληθεί το 2008 και το 2018 αντίστοιχα [Solensky 1996, το Αμερικανικό Μητρώο για Αριθμούς Διαδικτύου (American Registry for Internet Numbers, ARIN) ανέφερε ότι όλες οι διευθύνσεις του IPv4 τάξης A είχαν εκχωρηθεί, το 62% των διευθύνσεων τάξης B είχαν εκχωρηθεί και το 37% των διευθύνσεων τάξης C είχαν εκχωρηθεί [ARIN 1996]. Αν και αυτές οι εκτιμήσεις και οι αριθμοί υπονοούσαν ότι μπορεί να έμενε αρκετός χρόνος μέχρι να εξαντληθεί ο χώρος διευθύνσεων IPv4, έγινε σαφές ότι θα χρειαζόταν αρκετός χρόνος για ανάπτυξη μιας νέας τεχνολογίας σε τέτοια εκτεταμένη κλίμακα και έτσι ξεκίνησε η προσπάθεια για IP νέας γενιάς (Next generation IP, IPng) [Bradner 1996, RFC 1752]. Το αποτέλεσμα αυτής της προσπάθειας ήταν η προδιαγραφή του IP έκδοση 6 (IPv6) [RFC 2460], που θα μελετηθεί παρακάτω. (Μια ερώτηση που γίνεται συχνά είναι, τι συνέβη στο IPv5. Αρχικά θεωρήθηκε ότι το πρωτόκολλο ST-2 θα γινόταν το IPv5, αλλά το ST-2 αργότερα απορρίφθηκε για χάρη του πρωτοκόλλου RSVP.)

2.1.1 Μορφή Πακέτου IPv6

Η μορφή του δεδομενογράμματος IPv6 φαίνεται στην εικόνα 2.1. Οι σημαντικότερες αλλαγές που εισήχθησαν στο IPv6 φαίνονται στη μορφή του δεδομενογράμματος:

- *Εκτεταμένες δυνατότητες διευθυνσιοδότησης*. Το IPv6 αυξάνει το μέγεθος της διεύθυνσης IP από 32 σε 128 bits. Έτσι καθίσταται πιο σίγουρο ότι δεν θα εξαντληθούν οι διευθύνσεις IP. Τώρα, όλα τα πράγματα στον πλανήτη θα μπορούν να διευθυνσιοδοτούνται με IP. Εκτός των διευθύνσεων μονοεκπομπής και πολυεκπομπής, το IPv6 έχει εισαγάγει ένα νέο τύπο διεύθυνσης, που καλείται διεύθυνση εκπομπής σε κάποιον από την ομάδα (anycast), η οποία επιτρέπει σε ένα

δεδομενόγραμμα που διευθυνσιοδοτείται για οποιαδήποτε εκπομπή να παραδίδεται σε οποιονδήποτε από μια ομάδα υπολογιστών υπηρεσίας. (Αυτό το χαρακτηριστικό μπορεί να χρησιμοποιηθεί, για παράδειγμα, για αποστολή μιας HTTP GET στον πλησιέστερο από μια σειρά κατοπτρικών ιστοχώρων, που περιέχουν ένα δεδομένο έγγραφο.)



Εικόνα 2.1: Μορφή δεδομενογράμματος IPv6

- *Μια απλοποιημένη επικεφαλίδα 40-byte.* Όπως αναφέρεται παρακάτω, ένας αριθμός πεδίων IPv4 έχουν απορριφθεί ή έχουν γίνει προαιρετικά. Η προκύπτουσα επικεφαλίδα σταθερού μήκους 40-byte επιτρέπει την ταχύτερη επεξεργασία του δεδομενοδιαγράμματος IP. Μια νέα κωδικοποίηση επιλογών επιτρέπει την πιο ευέλικτη επεξεργασία των επιλογών.

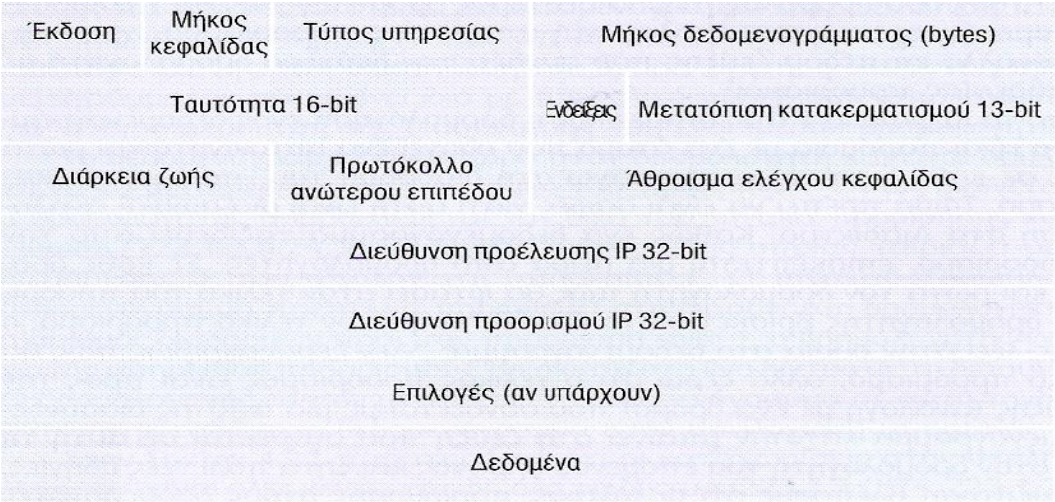
- *Ετικέτες ροής και προτεραιότητας.* Το IPv6 έχει έναν αφηρημένο ορισμό της ροής. Τα RFC 1752 και RFC 2460 δηλώνουν ότι αυτό επιτρέπει "τη σήμανση με ετικέτες πακέτων που ανήκουν σε συγκεκριμένες ροές, για τις οποίες ο αποστολέας ζητά ειδικό χειρισμό, όπως είναι η μη προεπιλεγμένη ποιότητα υπηρεσίας ή η υπηρεσία πραγματικού χρόνου". Για παράδειγμα, η μετάδοση ήχου και βίντεο μπορεί να θεωρηθεί σα ροή. Από την άλλη, οι πιο παραδοσιακές εφαρμογές, όπως η μεταφορά αρχείων και e-mail μπορούν να μην θεωρηθούν σαν ροές. Είναι δυνατό κίνηση που μεταφέρεται από ένα χρήστη υψηλής προτεραιότητας (για παράδειγμα, κάποιος που πληρώνει για καλύτερη υπηρεσία για την κίνησή του) να θεωρηθεί επίσης σαν ροή. Η επικεφαλίδα IPv6 έχει επίσης ένα πεδίο τάξης κίνησης 8-bit. Αυτό το πεδίο, σαν το πεδίο T0S στο IPv4, μπορεί να χρησιμοποιηθεί για να δώσει προτεραιότητα σε ορισμένα πακέτα μέσα σε μια ροή, ή μπορεί να χρησιμοποιηθεί για να δώσει προ-τεραιότητα σε δεδομε-νογράμματα από ορισμένες εφαρμογές (για παράδειγμα

πακέτα ICMP) σε σχέση με δεδομενογράμματα από άλλες εφαρμογές (για παράδειγμα, ειδήσεις δικτύου).

Τα παρακάτω πεδία ορίζονται στο IPv6:

- *Έκδοση.* Αυτό το πεδίο των 4-bit καθορίζει τον αριθμό έκδοσης του IP. Φυσικά, το IPv6 περιέχει τον αριθμό "6" σε αυτό το πεδίο. Σημειώνεται ότι αν βάλουμε ένα "4" σε αυτό το πεδίο, δε δημιουργείται ένα έγκυρο δεδομενόγραμμα IPv4. (Αν δημιουργείτο, η ζωή μας θα ήταν ευκολότερη)
- *Τάξη κίνησης.* Αυτό το πεδίο των 8-bit είναι στην ουσία παρόμοιο με το πεδίο T05 που έχει το IPv4.
- *Ετικέτα ροής.* Όπως αναφέρθηκε παραπάνω, αυτό το πεδίο των 20-bit χρησιμοποιείται για να καθορίζει μια "ροή" δεδομενογραμμάτων.
- *Μήκος ωφέλιμου φορτίου.* Αυτή η τιμή των 16-bit χρησιμοποιείται σαν ένας μη προσημασμένος ακέραιος, που δίνει τον αριθμό των bytes μέσα στο δεδομενόγραμμα IPv6, που ακολουθεί τη σταθερού μήκους, 40-byte επικεφαλίδα του δεδομενογράμματος.
- *Επόμενη επικεφαλίδα.* Αυτό το πεδίο καθορίζει το πρωτόκολλο στο οποίο θα παραδοθούν τα περιεχόμενα αυτού του δεδομενογράμματος (π.χ., στο TCP ή στο UDP). Το πεδίο αυτό χρησιμοποιεί τις ίδιες τιμές με το πεδίο πρωτοκόλλου της κεφαλίδας του IPv4.
- *Όριο αλμάτων.* Τα περιεχόμενα αυτού του πεδίου μειώνονται κατά ένα από κάθε δρομολογητή που προωθεί το δεδομενόγραμμα. Αν ο μετρητής ορίου αλμάτων φτάσει το μηδέν, τότε το δεδομενόγραμμα απορρίπτεται.
- *Διευθύνσεις προέλευσης και προορισμού.* Οι διάφορες μορφές της διεύθυνσης 128 bit IPv6 περιγράφονται στο RFC 2373.
- *Δεδομένα.* Αυτό είναι το τμήμα ωφέλιμου φορτίου του δεδομενογράμματος IPv6. Όταν το δεδομενόγραμμα φτάσει στον προορισμό του, το ωφέλιμο φορτίου θα αφαιρεθεί από το δεδομενόγραμμα IP και θα περάσει στο πρωτόκολλο που καθορίζεται στο πεδίο επόμενης επικεφαλίδας.

Τα παραπάνω προσδιόρισαν τον σκοπό των πεδίων που περιλαμβάνονται στο δεδομενόγραμμα IPv6. Συγκρίνοντας τη μορφή του δεδομενογράμματος IPv6 εικόνας 2.1 με τη μορφή του δεδομενογράμματος IPv4 που ακολουθεί στην εικόνα 2.2, φαίνεται ότι αρκετά πεδία που υπάρχουν στο δεδομενόγραμμα IPv4 δεν υπάρχουν πλέον στο δεδομενόγραμμα IPv6:



Εικόνα 2.2: Μορφή δεδομενογράμματος IPv4

- *Κατακερματισμός/Ανασύνθεση.* Το IPv6 δεν επιτρέπει τον κατακερματισμό και την ανασύνθεση σε ενδιάμεσους δρομολογητές. Αυτές οι λειτουργίες μπορούν να γίνουν μόνο στην προέλευση και στον προορισμό. Αν ένα δεδομενόγραμμα IPv6 που λαμβάνεται από ένα δρομολογητή είναι πολύ μεγάλο για να προωθηθεί επάνω σε μια εξερχόμενη ζεύξη, τότε ο δρομολογητής απλώς απορρίπτει το δεδομενόγραμμα και στέλνει ένα μήνυμα σφάλματος ICMP "Packet Too Big" (το πακέτο είναι πολύ μεγάλο) πίσω στον αποστολέα. Ο αποστολέας μπορεί κατόπιν να ξαναστείλει τα δεδομένα, χρησιμοποιώντας ένα μικρότερου μεγέθους δεδομενόγραμμα IP. Ο κατακερματισμός και η ανασύνθεση είναι μια χρονοβόρα διαδικασία. Η αφαίρεση αυτής της λειτουργίας από τους δρομολογητές και η τοποθέτησή της στα τερματικά συστήματα επιταχύνει κατά πολύ την προώθηση IP μέσα στο δίκτυο.

- *Άθροισμα ελέγχου επικεφαλίδας.* Επειδή τα πρωτόκολλα επιπέδου μεταφοράς (π.χ., TCP ή UDP) και ζεύξης δεδομένων (π.χ., Ethernet) στα επίπεδα του Διαδικτύου κάνουν τη λειτουργία αθροίσματος ελέγχου, οι σχεδιαστές του IP αισθάνθηκαν ότι αυτή η λειτουργία ήταν πλεονάζουσα στο επίπεδο δικτύου και θα μπορούσε να αφαιρεθεί. Πάλι, το κύριο ενδιαφέρον ήταν στην ταχεία επεξεργασία των πακέτων IP. Εφόσον η επικεφαλίδα IPv4 περιέχει ένα πεδίο TTL (παρόμοιο με το πεδίο ορίου αλμάτων στο IPv6), το άθροισμα ελέγχου επικεφαλίδας IPv4 θα έπρεπε να επανυπολογίζεται σε κάθε δρομολογητή. Όπως συμβαίνει με τον κατακερματισμό και την ανασύνθεση, αυτή ήταν επίσης μια ακριβής διαδικασία στο IPv4 .

- *Επιλογές.* Ένα πεδίο επιλογών δεν υπάρχει πλέον στην πρότυπη επικεφαλίδα IP. Αλλά όμως δεν έχει εξαφανιστεί. Αντί αυτού, το πεδίο επιλογών είναι μια από τις πιθανές "επόμενες επικεφαλίδες" που αναφέρονται μέσα στην επικεφαλίδα IPv6.

Αυτό σημαίνει ότι, όπως οι επικεφαλίδες των πρωτοκόλλων TCP ή UDP μπορούν να είναι η επόμενη επικεφαλίδα μέσα σε ένα πακέτο IP, το ίδιο μπορεί να συμβεί και με ένα πεδίο επιλογών. Η αφαίρεση του πεδίου επιλογών έχει σαν αποτέλεσμα μια επικεφαλίδα IP σταθερού μήκους 40-byte.

Το πρωτόκολλο ICMP χρησιμοποιείται από κόμβους IP για αναφορά συνθηκών σφάλματος και παροχή περιορισμένων πληροφοριών (για παράδειγμα, για απαντήσεις ηχούς σε ένα μήνυμα ping) προς ένα τερματικό σύστημα. Μια νέα έκδοση του ICMP έχει οριστεί για το IPv6 στο RFC 2463. Εκτός της αναδιοργάνωσης των υπαρχόντων ορισμών τύπου και κωδικών ICMP, το ICMPv6 έχει επίσης προσθέσει νέους τύπους και κωδικούς που απαιτούνται από τη νέα λειτουργικότητα του IPv6. Αυτοί περιλαμβάνουν τον τύπο "Packet Too Big" και έναν κωδικό σφάλματος "unrecognized IPv6 options" (άγνωστες επιλογές IPv6). Επίσης το ICMPv6 εντάσσει τη λειτουργικότητα του Πρωτοκόλλου Διαχείρισης Ομάδων Διαδικτύου (Internet Group Management Protocol, IGMP) το οποίο χρησιμοποιείται για διαχείριση της σύνδεσης και αποσύνδεσης ενός υπολογιστή υπηρεσίας στις ονομαζόμενες ομάδες πολυεκπομπής, που στο IPv4 ήταν ένα πρωτόκολλο ξεχωριστό από το ICMP.

2.1.2 Μετάβαση από το IPv4 στο IPv6

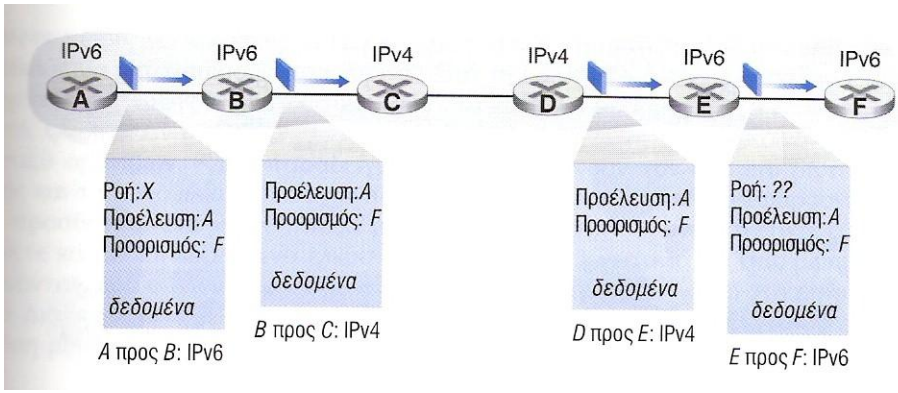
Τώρα προκύπτει ένα πρακτικό θέμα: πώς το δημόσιο Διαδίκτυο, που βασίζεται στο IPv4, θα μεταβεί στο IPv6. Το πρόβλημα είναι ότι ενώ τα νέα συστήματα με δυνατότητες IPv6 μπορούν να γίνουν καθοδικά συμβατά, δηλαδή μπορούν να στέλνουν, να δρομολογούν και να δέχονται δεδομενογράμματα IPv4, τα ήδη υπάρχοντα συστήματα με δυνατότητες IPv4 δεν είναι σε θέση να χειριστούν δεδομενογράμματα IPv6. Υπάρχουν αρκετές επιλογές.

Μια επιλογή θα είναι να ανακοινωθεί μια "ημερομηνία μετάβασης" - μια δεδομένη ημερομηνία και ώρα που οι μηχανές του Διαδικτύου θα σβήσουν και θα αναβαθμιστούν από IPv4 σε IPv6. Η τελευταία μεγάλη τεχνολογική μετάβαση (από τη χρήση του NCP στη χρήση του TCP) για υπηρεσία αξιόπιστης μεταφοράς έγινε σχεδόν πριν από 20 χρόνια. Ακόμη και τότε [RFC 801], που το Διαδίκτυο ήταν μικρό και το διαχειριζόταν μια μικρή ομάδων "μάγων", έγινε σαφές ότι μια τέτοια ημερομηνία μετάβασης δεν ήταν δυνατή. Μια ημερομηνία μετάβασης που να περιλαμβάνει εκατοντάδες εκατομμύρια μηχανές και εκατομμύρια διαχειριστές δικτύων και χρήστες είναι ακόμη πιο δύσκολη σήμερα. Το RFC 2893 περιγράφει δύο προσεγγίσεις (οι οποίες μπορούν να χρησιμοποιηθούν είτε μόνες ή μαζί) για βαθμιαία ενσωμάτωση υπολογιστών υπηρεσίας και δρομολογητών IPv6 σε έναν κόσμο IPv4 (με τον μακροχρόνιο βέβαια στόχο, να μεταβούν κάποτε όλοι οι κόμβοι IPv4 σε IPv6).

Ο πιο άμεσος πιθανώς τρόπος εισαγωγής κόμβων με δυνατότητες IPv6 είναι μια

προσέγγιση *διττής στοίβας (dual stack)*, όπου οι κόμβοι IPv6 θα έχουν επίσης πλήρη υλοποίηση IPv4. Ένας τέτοιος κόμβος, που αναφέρεται σαν κόμβος IPv6/IPv4 στο RFC 2893, έχει τη δυνατότητα να στέλνει και να λαμβάνει δεδομενογράμματα IPv4 και IPv6. Όταν διαλειτουργεί με έναν κόμβο IPv4, ένας κόμβος IPv6/IPv4 μπορεί να χρησιμοποιεί δεδομενογράμματα IPv4. Όταν διαλειτουργεί με έναν κόμβο IPv6, μπορεί να μιλήσει IPv6. Οι κόμβοι IPv6/IPv4 πρέπει να έχουν διευθύνσεις IPv6 και IPv4. Πρέπει να είναι επίσης σε θέση να προσδιορίσουν αν ένας άλλος κόμβος έχει δυνατότητες IPv6 ή έχει μόνο δυνατότητες IPv4. Αυτό το πρόβλημα μπορεί να λυθεί χρησιμοποιώντας το DNS το οποίο μπορεί να επιστρέψει μια διεύθυνση IPv6 αν το όνομα του κόμβου που μεταφράζεται έχει δυνατότητες IPv6 ή αλλιώς, να επιστρέψει μια διεύθυνση IPv4. Φυσικά, αν ο κόμβος που εκδίδει μια αίτηση DNS έχει μόνο δυνατότητες IPv4, τότε το DNS επιστρέφει μόνο μια διεύθυνση IPv4.

Στην προσέγγιση διττής στοίβας, αν ο αποστολέας ή ο δέκτης έχει μόνο δυνατότητες IPv4, πρέπει να χρησιμοποιηθεί ένα δεδομενόγραμμα IPv4. Σαν αποτέλεσμα, είναι πιθανό δύο κόμβοι με δυνατότητες IPv6 να καταλήξουν να ανταλλάσσουν δεδομένα IPv4 μεταξύ τους. Αυτό φαίνεται στην εικόνα 4.3. Υποθέστε ότι ο κόμβος A έχει δυνατότητες IPv6 και θέλει να στείλει ένα δεδομενόγραμμα IP στον κόμβο *F*, ο οποίος έχει επίσης δυνατότητες IPv6. Οι κόμβοι A και B μπορούν να ανταλλάσσουν δεδομενογράμματα IPv6. Αλλά όμως, ο κόμβος B πρέπει να δημιουργήσει ένα δεδομενόγραμμα IPv4 για να το στείλει στον C. Φυσικά το πεδίο δεδομένων του δεδομενογράμματος



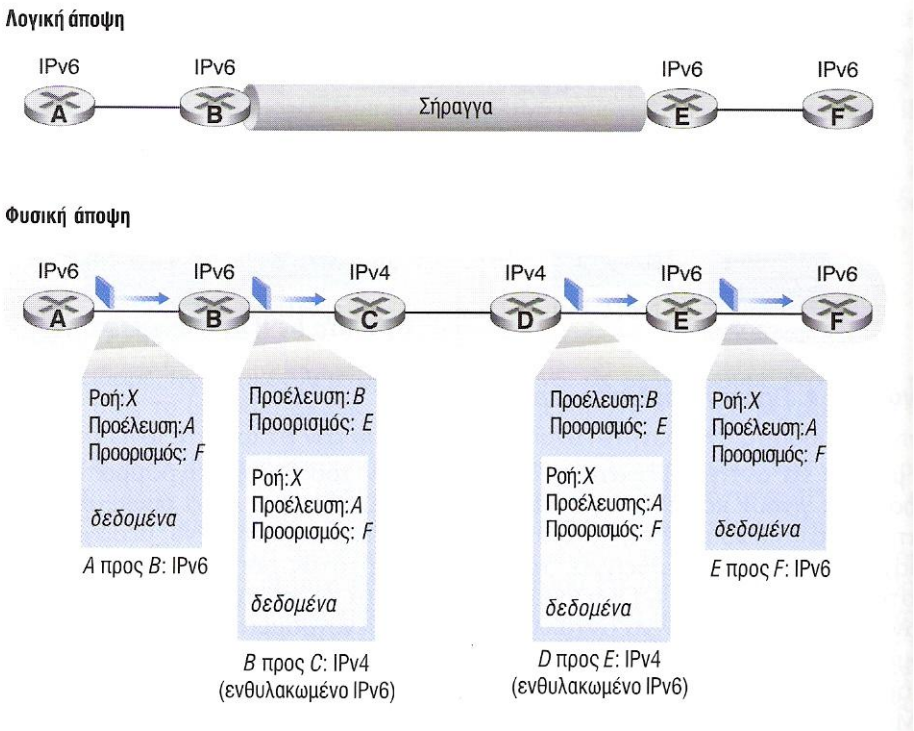
Εικόνα 2.3: Προσέγγιση διττής στοίβας

IPv6 μπορεί να αντιγραφεί στο πεδίο δεδομένων του δεδομενογράμματος IPv4 και μπορούν να γίνουν κατάλληλες αντιστοιχίσεις διευθύνσεων. Αλλά όμως, όταν γίνεται μετατροπή από IPv6 σε IPv4, θα υπάρχουν πεδία ειδικά για το IPv6, μέσα στο δεδομενόγραμμα IPv6 (για παράδειγμα, το πεδίο ταυτότητας ροής), τα οποία δεν έχουν αντίστοιχα πεδία στο IPv4. Οι πληροφορίες σε αυτά τα πεδία θα χαθούν. Έτσι, ακόμη και αν οι E και F μπορούν να ανταλλάσσουν δεδομενογράμματα IPv6, τα αφικνούμενα

δεδομενογράμματα IPv4 στον Ε από τον D δεν περιέχουν όλα τα πεδία που βρίσκονταν στο αρχικό δεδομενόγραμμα IPv6 που εστάλη από τον Α.

Μια εναλλακτική προσέγγιση, αντί της προσέγγισης διττής στοίβας, που συζητείται επίσης στο RFC 2893, είναι γνωστή σαν *σήραγγα* (tunneling). Η σήραγγα μπορεί να λύσει το πρόβλημα που αναφέρθηκε παραπάνω, επιτρέποντας, για παράδειγμα, τον Ε να λαμβάνει το δεδομενόγραμμα IPv6 που προέρχεται από τον Α. Η βασική ιδέα πίσω από την σήραγγα είναι η παρακάτω. Υποθέτοντας ότι δύο κόμβοι IPv6 (για παράδειγμα, οι Β και Ε στην εικόνα 4.3) θέλουν να διαλειτουργήσουν χρησιμοποιώντας δεδομενο-γράμματα IPv6, αλλά συνδέονται μεταξύ τους μέσω παρεμβαλλομένων δρομολογητών IPv4. Γίνεται αναφορά στους ενδιάμεσους δρομολογητές IPv4 που είναι μεταξύ των δρομολογητών IPv6, σαν μια *σήραγγα***,** όπως φαίνεται στην εικόνα 4.4. Με τη σήραγγα, ο κόμβος IPv6 στην πλευρά αποστολής της σήραγγας (για παράδειγμα, ο Β) παίρνει όλο το δεδομενόγραμμα IPv6 και το τοποθετεί μέσα στο πεδίο δεδομένων (ωφέλιμο φορτίο) ενός δεδομενογράμματος IPv4. Αυτό το δεδομενόγραμμα IPv4 απευθύνεται κατόπιν στον κόμβο IPv6 στην πλευρά λήψης της σήραγγqς (για παράδειγμα, στον Ε) και στέλνεται στον πρώτο κόμβο της σήραγγας (για παράδειγμα, στον C). Οι ενδιάμεσοι δρομολογητές IPv4 μέσα στη σήραγγα δρομολογούν αυτό το δεδομενόγραμμα IPv4 ανάμεσά τους, όπως θα δρομολογούσαν κάθε άλλο δεδομενόγραμμα, χωρίς να γνωρίζουν ότι το δεδομενόγραμμα IPv4 περιέχει ένα πλήρες δεδομενόγραμμα IPv6. Ο κόμβος IPv6 στην πλευρά λήψης της σήραγγας λαμβάνει τελικά το δεδομενόγραμμα IPv4 (είναι ο προορισμός του δεδομενογράμματος IPv4!), καθορίζει ότι το δεδομενόγραμμα IPv4 περιέχει ένα δεδομενόγραμμα IPv6, εξάγει το δεδομενόγραμμα IPv6 και μετά δρομολογεί το δεδομενόγραμμα IPv6 σαν να το είχε λάβει απευθείας από ένα γειτονικό του κόμβο IPv6.

Πρέπει να σημειωθεί ότι η υιοθέτηση του IPv6 προχωρεί αργά [Lawton 2001]. Εξ άλλου ένα από τα βασικά κίνητρα για το IPv6 ήταν η ελάττωση των διαθέσιμων διευθύνσεων IPv4. Εξελίξεις σαν τις διευθύνσεις IPv4 με βάση το ClDR, το DHCP και το NAT έχουν όλες συνεισφέρει προς τη λύση αυτού του προβλήματος, τουλάχιστον βραχυπρόθεσμα.



Εικόνα 2.4: Σήραγγα

Είναι όμως πιθανό, η εξάπλωση συσκευών, όπως είναι τα τηλέφωνα με δυνατότητες IP και άλλων φορητών συσκευών, να δώσει την αναγκαία ώθηση προς την ευρεία ανάπτυξη του IPv6. Η Ericsson είχε προγραμματίσει την έκδοση τηλεφώνων με δυνατότητες IPv6 το 2002 και το Ευρωπαϊκό Πρόγραμμα Third Generation Partnership Program [3GPP 2002] είχε καθορίσει το IPv6 σαν το πρότυπο σχήμα διευθυνσιοδότησης για κινητά πολυμέσα. Ακόμη και αν το IPv6 δεν έχει αναπτυχθεί πλήρως τα πρώτα επτά χρόνια της ζωής του, πρέπει να εξεταστεί η μακροχρόνια προοπτική του. Όπως το σημερινό σύστημα αριθμοδότησης τηλεφώνων που χρειάστηκε αρκετές δεκάδες χρόνια για να επικρατήσει, τώρα πλέον είναι εγκαταστημένο και δε δείχνει σημάδια ότι θα αλλάξει. Παρόμοια, μπορεί να χρειαστεί κάποιος χρόνος για να επικρατήσει το IPv6, αλλά όταν επικρατήσει θα κρατήσει για πολύ καιρό. Ο Brian Carpenter, πρώην πρόεδρος του Διαδικτύου Architecture Board [IAB 2002] και συγγραφέας αρκετών RFC που σχετίζονται με το IPv6 λέει "Θεώρησα το όλο εγχείρημα σαν ένα 15ετές έργο, που άρχισε το 1995" [Lawton 2001]. Σύμφωνα με τη λογική του Carpenter είμαστε ακόμη στη μέση του δρόμου!

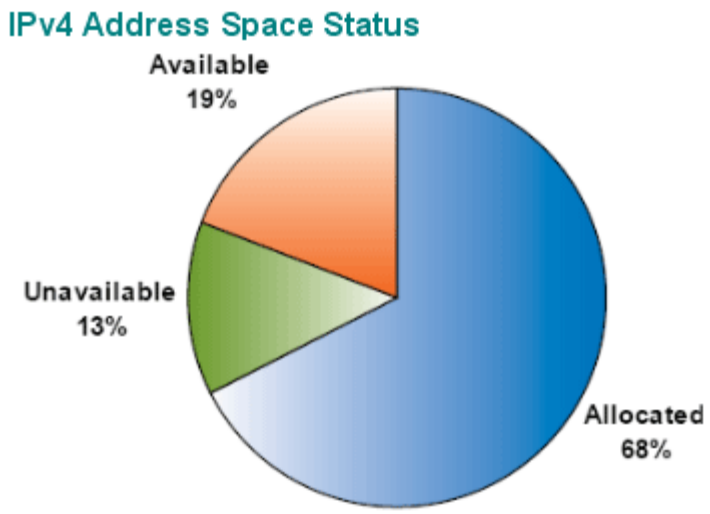
Αυτό που δείχνει το IPv6 είναι ότι είναι εξαιρετικά δύσκολο να αλλαχτούν τα πρωτόκολλα επιπέδου δικτύου. Από τις αρχές της δεκαετίας του '90 πολλά νέα πρωτόκολλα επιπέδου δικτύου έχουν διαφημιστεί σαν η επόμενη μεγάλη επανάσταση για το Διαδίκτυο, αλλά τα περισσότερα από αυτά είχαν περιορισμένη διείσδυση μέχρι σήμερα. Αυτά τα πρωτόκολλα περιλαμβάνουν το IPv6, τα πρωτόκολλα πολυεκπομπής

και πρωτόκολλα δέσμευσης πόρων. Πράγματι, η εισαγωγή νέων πρωτοκόλλων στο επίπεδο δικτύου είναι σαν να αντικαθίστανται τα θεμέλια ενός σπιτιού - είναι δύσκολο να γίνει χωρίς την κατεδάφιση όλου του σπιτιού, ή τουλάχιστον χωρίς να αναγκαστούν οι ένοικοι να μετακομίσουν προσωρινά. Από την άλλη, το Διαδίκτυο έχει γίνει μάρτυρας ταχείας ανάπτυξης νέων πρωτοκόλλων στο επίπεδο εφαρμογής. Τα κλασικά παραδείγματα, φυσικά, είναι το Web, η αποστολή άμεσων μηνυμάτων και η κοινή χρήση αρχείων Jεταξύ ομοτίμων. Άλλα παραδείγματα περιλαμβάνουν τον ήχο και βίντεο συνεχούς ροής και τη συνομιλία. Η εισαγωγή νέων πρωτοκόλλων επιπέδου εφαρμογής είναι σαν να προστίθεται ένα νέο επίπεδο μπογιάς σε ένα σπίτι - είναι σχετικά εύκολο να γίνει και αν επιλεχθεί μάλιστα ένα ελκυστικό χρώμα, όλη η γειτονιά θα το μιμηθεί. Στο μέλλον αναμένονται αλλαγές στο επίπεδο δικτύου του Διαδικτύου, αλλά αυτές οι αλλαγές θα συμβούν μάλλον με αργούς ρυθμούς, σε σχέση με τους ρυθμούς που συμβαίνουν οι αλλαγές στο επίπεδο εφαρμογής.

2.2 Πλεονεκτήματα του IPv6 έναντι του IPv4

2.2.1 Το IPv6 παρέχει ένα πολύ μεγαλύτερο χώρο διευθύνσεων IP από ότι το IPv4

Σε κάθε υπολογιστή ή κάθε συσκευή που χρειάζεται να συνδεθεί στο Διαδίκτυο απαιτείται μια παγκοσμίως μοναδική διεύθυνση IP. Το IPv4 χρησιμοποιεί 32 bit για μια διεύθυνση IP το οποίο μεταφράζεται σε περίπου 4 δισεκατομμύρια μοναδικές διευθύνσεις IP. Όταν το IPv4 εισήχθη στη δεκαετία του 1970 και έγινε αποδεκτό ως το πρωτόκολλο για το Διαδίκτυο, δεν είχε προβλεφθεί η σημερινή έκρηξη της δημοτικότητας αυτού. Κατά συνέπεια, φαινόταν λογικό ότι αυτά τα 4 δισεκατομμύρια διευθύνσεων θα επαρκούσαν για να καλύψουν οποιαδήποτε μελλοντική ανάπτυξη του Διαδικτύου.



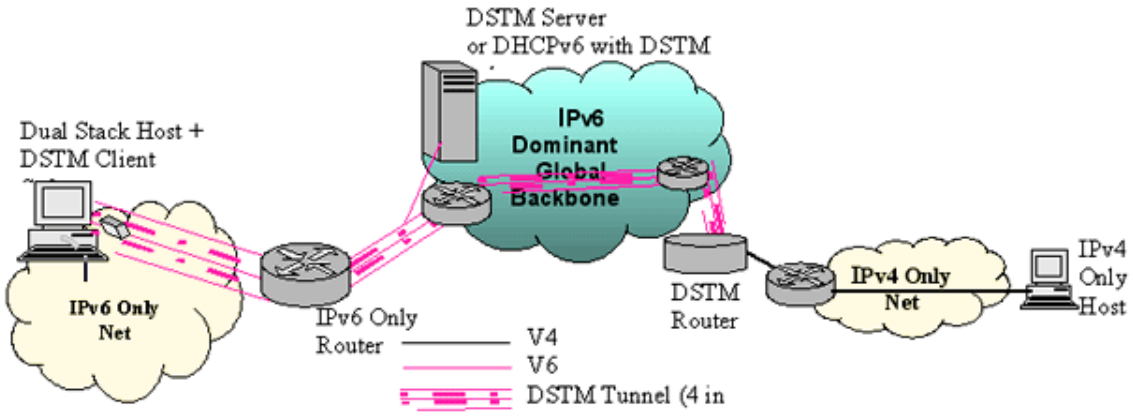
Εικόνα 2.5: Ποσοστά χώρου δευθύνσεων IPv4

Όπως φαίνεται και στο παραπάνω διάγραμμα σε λίγο καιρό και ιδίως με την έκταση που ενδέχεται να πάρει το Διαδίκτυο των πραγμάτων το IPv4 δεν θα μπορεί να ανταπεξέλθει στις ανάγκες που θα προκύψουν. Μία πιθανή λύση θα ήταν το Network Address Translation (NAT) το οποίο μεταφράζει μία μοναδική παγκόσμια IP σε πολλαπλές ιδιωτικές IP. Όμως αυτό θα προκαλούσε πολυπλοκότητα στο υλικό και στο λειτουργικό του δικτύου.

Σε αντίθεση το IPv6 χρησιμοποιεί 128 bits για μια διεύθυνση γεγονός που δημιουργεί 3.4×10^{38} μοναδικές διευθύνσεις. Για να γίνει κατανοητό το μέγεθος της κλίμακας, αν το σύνολο του χώρου του IPv4 περιέχεται σε ένα iPod, τότε ο νέος χώρος του IPv6 θα είναι όσο το μέγεθος της Γης. Έτσι μπορεί να θεωρηθεί ότι το IPv6, θα είναι σε θέση να παρέχει δισεκατομμύρια διευθύνσεις σε κάθε πρόσωπο και να διασφαλίσει ότι κάθε συσκευή που πρέπει να συνδεθεί με το Διαδίκτυο θα έχει μια μοναδική διεύθυνση IP.

2.2.2 Το IPv6 παρέχει καλύτερη end-to-end σύνδεση από το IPv4

Οι πιο διαδεδομένες εφαρμογές στις ημέρες μας είναι οι peer-to-peer εφαρμογές, όπως τα multi-player online παιχνίδια, η τηλεδιάσκεψη (streaming media), η κοινή χρήση αρχείων και το VoIP. Στα peer-to-peer δίκτυα, μια ομάδα από υπολογιστές μπορούν να επικοινωνούν απευθείας μεταξύ τους χωρίς να χρειάζονται έναν κεντρικό server. Οι peer-to-peer εφαρμογές απαιτούν end-to-end σύνδεση μεταξύ των μοναδικών τους διευθύνσεων IP.



Εικόνα 2.6: Παράδειγμα end–to–end διασύνδεσης

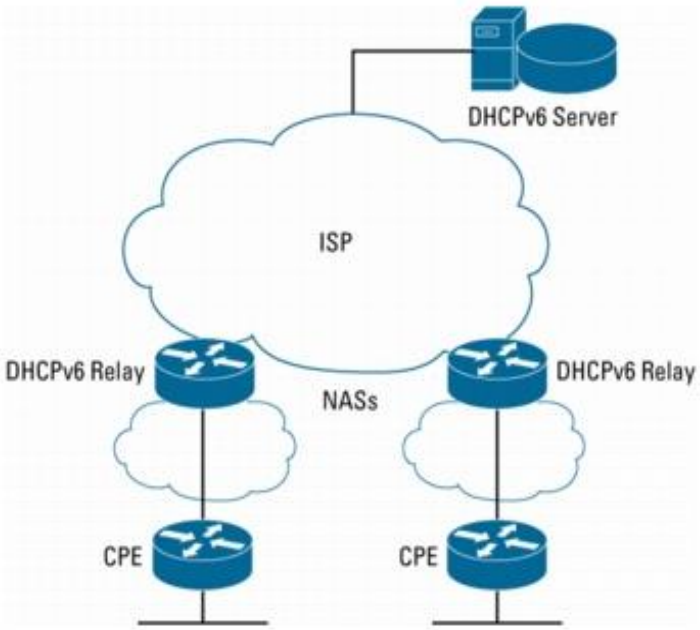
Όπως αναφέρθηκε προηγουμένως, η έλλειψη των διευθύνσεων που προκαλείται από IPv4 έχει ξεπεραστεί σε κάποιο βαθμό από τη χρήση NAT, το οποίο μεταφράζει ουσιαστικά μία μοναδική παγκόσμια διεύθυνση σε πολλαπλές ιδιωτικές διευθύνσεις. Η έλλειψη μοναδικών IP διευθύνσεων για κάθε σκοπό, έχει σαν αποτέλεσμα το NAT να δημιουργεί δυσκολίες στην εξασφάλιση της ορθής λειτουργίας των end-to-end υπηρεσιών. Η παρούσα λύση είναι η εφαρμογή ειδικών NAT τεχνικών ή η χρήση επιπλέον διακομιστών για την προσομοίωση της peer-to-peer επικοινωνίας.

Από την άλλη το IPv6, παρέχοντας μεγάλο χώρο διευθύνσεων δεν απαιτεί πλέον την χρήση NAT και μπορεί να εξασφαλίσει πραγματικές end-to-end διασυνδέσεις. Αυτό σημαίνει ότι οι peer-to-peer εφαρμογές όπως το VoIP ή το streaming media μπορούν να λειτουργήσουν πολύ πιο αποτελεσματικά και αποδοτικά με το IPv6.

2.2.3 Το IPv6 έχει καλύτερη δυνατότητα αυτορρύθμισης συσκευών από το IPv4

Κάθε φορά που κάποιος κόμβος θέλει να είναι μέρος ενός δικτύου, απαιτούνται πληροφορίες IP διεύθυνσης και πληροφορίες του δρομολογητή ώστε να ρυθμιστεί σωστά ο κόμβος. Στο παρελθόν, όπου υπήρχαν λιγότερες συσκευές και υπολογιστές σε ένα ενεργό IP δίκτυο, σχεδόν όλοι τους ήταν στατικά ρυθμισμένοι και οι διευθύνσεις IP ανατίθονταν χειροκίνητα. Ωστόσο, με την ταχεία διάδοση των προσωπικών υπολογιστών (PC) και των άλλων IP-enabled συσκευών, για την αποτελεσματική διαχείριση των συσκευών αυτών και την επαναχρησιμοποίηση των πόρων, κατέστη απολύτως αναγκαίο να εξεταστεί ένα είδος αυτορρύθμισης

Το IPv4 χρησιμοποιεί το stateful address autoconfiguration πρωτόκολλο, Dynamic Host Configuration Protocol (DHCP). Ο DHCP Server διατηρεί μια λίστα με τους χρήστες που φιλοξενεί καθώς και με τις διευθύνσεις που έχουν ανατεθεί στον κάθε χρήστη.



Εικόνα 2.7: Dynamic Host Configuration Protocol

Με την αύξηση των υπολογιστών και των συσκευών που χρησιμοποιούν IP, υπάρχει ανάγκη για ένα πρωτόκολλο IP που θα εξασφαλίζει εύκολη και αυτόματη ρύθμιση των συσκευών και των δρομολογητών. Οι νέες συσκευές που χρησιμοποιούν IP τώρα γίνονται όλο και πιο απλές όπως το 'Διαδίκτυο των πραγμάτων' και μπορούν να χρησιμοποιηθούν σε περιβάλλοντα όπου δεν θα απαιτείται εξάρτηση τους από τον διακομιστή.

Το IPv6 προσφέρει αυτόματη ρύθμιση και το πιο σημαντικό, απλούς μηχανισμούς διαμόρφωσης, γνωστούς και ως plug-and-play autoconfiguration. Οι δυνατότητες του IPv6 είναι πολύ περισσότερες από αυτές που προσφέρει σήμερα το IPv4. Το IPv6 προσφέρει dhcpv6, η οποία είναι αυτορρύθμιση παρόμοια με του IPv4 DHCP και προσφέρει stateful address autoconfiguration. Επιπλέον, το IPv6 προσφέρει stateless ή serverless address autoconfiguration.

Στην stateless αυτορρύθμιση, ο χρήστης μπορεί αυτόματα να διαμορφώσει τη δική του διεύθυνση IPv6 χωρίς να χρειάζεται καμία βοήθεια από ένα stateful address server. Ολόκληρα τα IPv6 προθέματα και όχι απλώς μια διεύθυνση παραδίδονται σε μια

συσκευή. Αυτό το ιδιαίτερο χαρακτηριστικό επιτρέπει στους δρομολογητές να απορυθμίζουν εύκολα τις διεπαφές τους γεγονός που μπορεί να χρησιμοποιηθεί πολύ αποτελεσματικά σε ευρυζωνικά δίκτυα πρόσβασης για την δυναμική παροχή πυλών στον χρήστη.

2.2.4 Το IPv6 περιέχει απλουστευμένες Δομές Επικεφαλίδας που οδηγούν σε ταχύτερη δρομολόγηση σε σύγκριση με το IPv4

Η παρούσα IP χρησιμοποιεί μια υπηρεσία διαγραμμάτων-δεδομένων για να μεταφέρει πακέτα δεδομένων σημείο προς σημείο χρησιμοποιώντας δρομολογητές. Η δομή της IPv4 επικεφαλίδας περιέχει 20 bytes δεδομένων, στα οποία περιέχονται όλες οι δυνατές επιλογές αναγκάζοντας έτσι τους ενδιάμεσους δρομολογητές να ελέγξουν κατά πόσον αυτές οι επιλογές υπάρχουν και αν υπάρχουν να τις επεξεργαστούν πριν τις προωθήσουν. Στην επικεφαλίδα των πακέτων IPv4, οι επιλογές αυτές έχουν κάποιο μέγιστο επιτρεπόμενο μέγεθος.

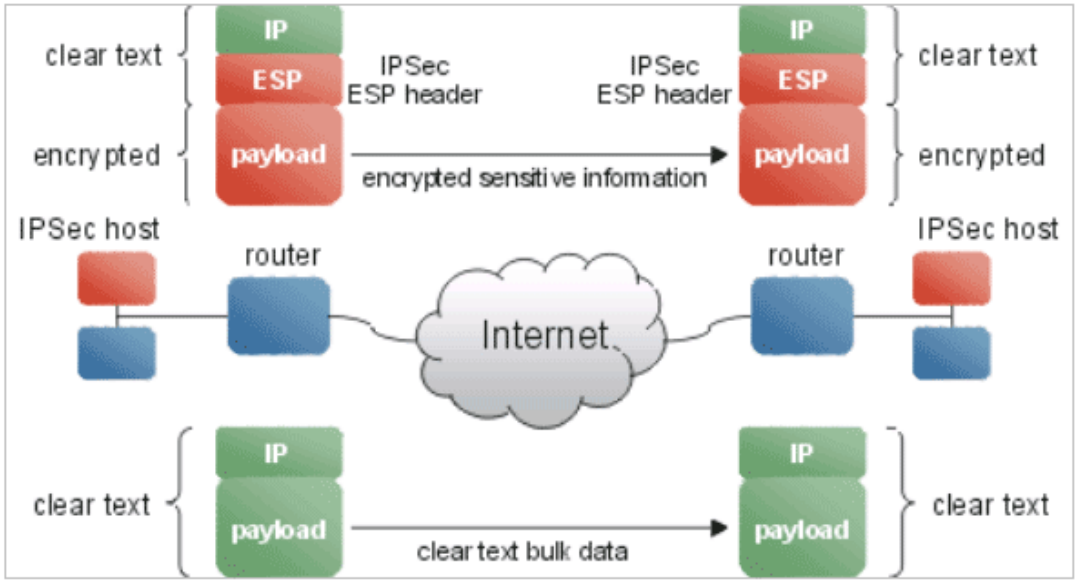
Η επικεφαλίδα του IPv4 έχει δύο κύρια προβλήματα που συμβάλλουν στην επιβράδυνση της ρυθμαπόδοσης, κάθε πακέτο πρέπει να υποβάλλεται σε επεξεργασία και checksum, καθώς και σε κάθε δρομολογητή ο οποίος διαχειρίζεται ένα πακέτο πρέπει να επεξεργάζεται το πεδίο της επιλογής του. Αυτό μπορεί να προκαλέσει μια σταδιακή υποβάθμιση των επιδόσεων κατά τη διαβίβαση των πακέτων IPv4.

Το IPv6 σε σύγκριση με το IPv4 έχει μια απλούστερη δομή επιγραφών πακέτων η οποία έχει σχεδιαστεί με στόχο κυρίως να ελαχιστοποιήσει το χρόνο και τις προσπάθειες που απαιτούνται κατά την επεξεργασία της επικεφαλίδας. Αυτό έχει επιτευχθεί με τη μετακίνηση των προαιρετικών πεδίων, καθώς οι τομείς που είναι εντελώς απαραίτητοι για την επέκταση των επικεφαλίδων διατίθενται μόνο μετά την επικεφαλίδα IPv6. Συνεπώς, οι IPv6 επιγραφές υποβάλλονται σε επεξεργασία αποτελεσματικότερα στους ενδιάμεσους δρομολογητές χωρίς να πρέπει να αναλύσουν μέσω των επιγραφών ή να επαναϋπολογίσουν τα checksums. Αυτή η αποδοτικότητα επιτρέπει την μείωση των γενικών εξόδων επεξεργασίας για τους δρομολογητές, καθιστά το υλικό λιγότερο σύνθετο και επιτρέπει στα πακέτα να υποβάλλονται σε πολύ γρηγορότερη επεξεργασία. Ένα άλλο χαρακτηριστικό της δομής της επικεφαλίδας του IPv6 είναι ότι η επέκταση της επικεφαλίδας επιτρέπει τις προσθήκες πρωτοκόλλου. Οι IPv6 επεκτάσεις επικεφαλίδας δεν έχουν περιορισμούς σχετικά με το μέγιστο μέγεθος, μπορούν να επεκταθούν για να φιλοξενήσουν οποιαδήποτε δεδομένα τόσα ώστε να υπάρξει αποτελεσματική επικοινωνία. Στην πραγματικότητα, ένα τυπικό πακέτο IPv6 δεν περιέχει επέκταση επικεφαλίδας. Μόνο αν στους ενδιάμεσους δρομολογητές ή στον προορισμό τους απαιτείται κάποια ειδική αντιμετώπιση, θα προστεθεί μία ή περισσότερες επικεφαλίδες επέκτασης ανάλογα με την απαίτηση. Αυτή η νέα επέκταση επικεφαλίδας κάνει το IPv6

πλήρως εξοπλισμένο ώστε να μπορεί να υποστηρίξει οποιαδήποτε μελλοντική ανάγκη ή δυνατότητα.

2.2.5 Το IPv6 παρέχει μεγαλύτερη ασφάλεια σε σχέση με το IPv4 όσο αφορά τις εφαρμογές και τα δίκτυα

Το Διαδίκτυο λειτουργεί τις τρεις τελευταίες δεκαετίες με το IPv4 ως βασικό πρωτόκολλο του. Ωστόσο, λόγω αυτού του end-to-end μοντέλου, το IPv4 σχεδι-άστηκε χωρίς να λαμβάνεται υπόψη η ασφάλεια, υποθέτοντας απλά ότι οι απαι-τούμενες εγγυήσεις θα παρέχονται στους τελικούς κόμβους. Για παράδειγμα, σε μια εφαρμογή όπως το ηλεκτρονικό μήνυμα που μπορεί να απαιτούνται υπηρεσίες κρυπτογράφησης - σύμφωνα με το IPv4, την ευθύνη την φέρει ο πελάτης του ηλεκτρονικού ταχυδρομείου στον τελικό κόμβο για την ομαλή παροχή των υπηρεσιών. Σήμερα, το Διαδίκτυο αντιμετωπίζει απειλές όπως η άρνηση εξυπηρέτησης, η διανομή κακόβουλου κώδικα, οι επιθέσεις Man-in-the-middle, οι επιθέσεις κατά-κερματισμού και οι επιθέσεις Reconnaissance



Εικόνα 2.8: Δομή της ασφάλειας

Τα Network Address Translation (NAT) και Port Network Address Translation (NAPT) στο IPv4 χρησιμοποιούνται για να παρέχουν κάποιο επίπεδο προστασίας από ορισμένες απειλές που αναφέρθηκαν παραπάνω με τη χρήση μεθόδων όπως τα firewalls. Επίσης, η εισαγωγή του πρωτοκόλλου IPSec, επιτρέπει στην επικοινωνία να είναι

κρυπτογραφημένη, αλλά η εφαρμογή του σε IPv4 είναι προαιρετική και όλη η ευθύνη για ασφαλή επικοινωνία εξακολουθεί να βαρύνει τους τελικούς κόμβους.

Στο IPv6, το IPSec είναι απαραίτητο πρωτόκολλο και είναι ένας από τους παράγοντες εξασφάλισης ότι το IPv6 παρέχει καλύτερη ασφάλεια από το IPv4. Το IPSec περιλαμβάνει ένα σύνολο κρυπτογραφικών πρωτοκόλλων με στόχο την ασφαλή επικοινωνία δεδομένων και τη ασφαλή ανταλλαγή κλειδιών. Τα κύρια πρωτόκολλα που χρησιμοποιούνται είναι:

1.Authentication Header (AH) πρωτόκολλο, το οποίο δίνει τη δυνατότητα ελέγχου της ταυτότητας και της ακεραιότητας των δεδομένων.

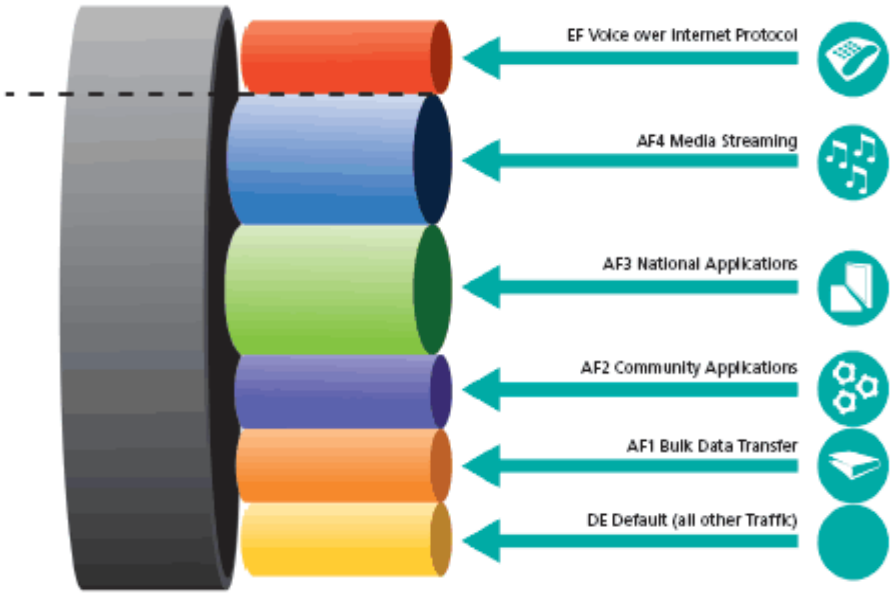
2.Encapsulating Security Payload (ESP) πρωτόκολλο, το οποίο διασφαλίζει τόσο την αυθεντικότητα όσο και την ακεραιότητα των δεδομένων, καθώς επίσης και την ιδιωτικότητα των δεδομένων.

3.Internet Key Exchange (IKE) πρωτόκολλο. Αυτή η οικογένεια πρωτοκόλλων βοηθά αρχικά στο να δημιουργηθούν και να διαπραγματευθούν οι παράμετροι της ασφάλειας μεταξύ δύο end points και έπειτα, παρακολουθεί τις εν λόγω πληροφορίες, έτσι ώστε να παραμένουν ασφαλείς μέχρι το τέλος.

Άρα το IPv6 διασφαλίζει ότι θα υπάρχουν end-to-end μηχανισμοί ασφάλειας που θα παρέχουν έλεγχο ταυτότητας και θα έχουν ικανότητες κρυπτογράφησης σε όλες τις αιτήσεις. Επίσης το ότι οι μηχανισμοί ασφάλειας είναι ίδιοι για όλες τις εφαρμογές έχει σαν αποτέλεσμα η δημιουργία και η διαχείριση των πολιτικών ασφαλείας να γίνεται πολύ απλούστερη. Το IPv6 επιτρέπει την πλήρη end-to-end ασφάλεια, παρέχοντας έτσι τη δυνατότητα ώστε μια νέα δέσμη εξατομικευμένων υπηρεσιών να αναπτυχθεί, όπως είναι οι κινητές υπηρεσίες ηλεκτρονικού εμπορίου που βασίζονται σε ασφαλείς συναλλαγές.

2.2.6 Το IPv6 παρέχει καλύτερη ποιότητα υπηρεσιών (QoS) από το IPv4

Στο IPv4, το πεδίο τύπος της υπηρεσίας ή Differentiated Services Code Point στην επικεφαλίδα του πακέτου έχουν συγκεκριμένο καθήκον στην ταξινόμηση των πακέτων και επίσης καθορίζουν το είδος των υπηρεσιών που αναμένονται από το πακέτο κατά την παράδοση του μέσα από τους δρομολογητές σε όλο το δίκτυο. Αυτό γίνεται συνήθως με συσκευές στο δίκτυο, οι οποίες θα ταξινομούν τα πακέτα με βάση τις ανάγκες της συγκεκριμένης εφαρμογής. Ωστόσο, αυτό σημαίνει επίσης ότι όλες οι QoS συσκευές δεν είναι απαραίτητο να είναι και μεταξύ τους συμβατές.



Εικόνα 2.9: Υπηρεσίες

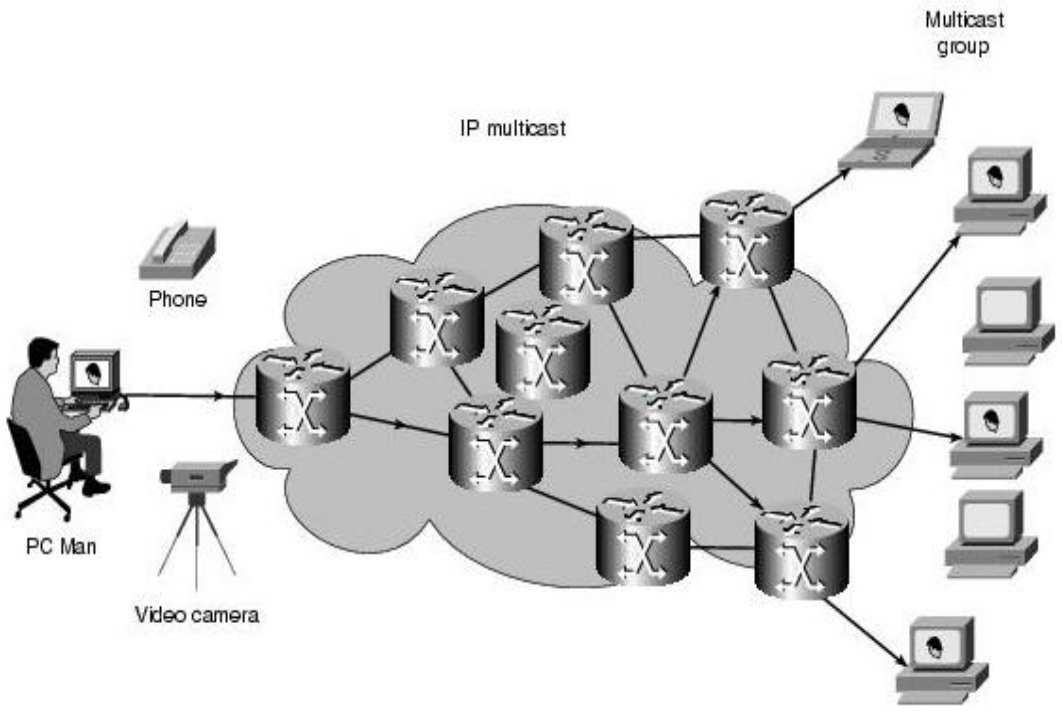
Στο QoS του IPv6 έχει δοθεί ιδιαίτερη ώθηση, με την επικεφαλίδα του IPv6 να περιέχει ένα νέο πεδίο, που ονομάζεται Flow Label πεδίο και το οποίο καθορίζει τον τρόπο που συγκεκριμένα πακέτα εντοπίζονται και αντιμετωπίζονται από τους δρομολογητές. Το πεδίο Flow Label επιτρέπει σε πακέτα που ανήκουν σε μια συγκεκριμένη ροή, με άλλα λόγια, που ξεκινούν από ένα συγκεκριμένο χρήστη προς ένα συγκεκριμένο προορισμό, να εντοπίζονται και να αντιμετωπίζονται γρήγορα και αποτελεσματικά από τους δρομολογητές. Το Flow Label Field, επομένως, δια-σφαλίζει ότι υπάρχει μία πιο αποτελεσματική παροχή πληροφοριών από το ένα άκρο στο άλλο χωρίς το ενδεχόμενο να έχει τροποποιηθεί η πληροφορία από ενδιάμεσα συστήματα. Αυτό εξασφαλίζει ένα υψηλό επίπεδο QoS ειδικά για peer-to-peer εφαρμογές όπως το VoIP και άλλες εφαρμογές πραγματικού χρόνου.

2.2.7 Το IPv6 παρέχει καλύτερες Multicast και Anycast ικανότητες σε σχέση με το IPv4

Στην τεχνική multicast ένα πακέτο αντιγράφεται από ένα στάδιο σε ένα κατώτερο , σε δομή ιεραρχικού δέντρου, αντί να στέλνεται απευθείας από την πηγή. Αυτό σημαίνει ότι υπάρχουν λιγότερα πακέτα στο δίκτυο και έτσι επιτυγχάνεται η βέλτιστη χρησιμοποίηση του εύρους ζώνης, αλλά και η μείωση των πόρων που απαιτούνται σε κάθε κόμβο του δικτύου. Αυτή η multicast τεχνική είναι ιδιαίτερα χρήσιμη όταν οι ροές των πληροφοριών πρέπει να διατεθούν σε μια μεγάλη ποικιλία συνδεδεμένων συσκευών και όχι μόνο σε ένα συγκεκριμένο προορισμό. Για παράδειγμα η τεχνική multicast χρησιμοποιείται για την αναμετάδοση των δεδομένων ήχου, βίντεο news feeds, οικονομικών data feeds και ούτω καθεξής.

Το μεγαλύτερο πρόβλημα με το multicast στο IPv4 είναι ότι είναι διαθέσιμο μόνο σε δευτερεύοντα δίκτυα ενώ οι περισσότεροι δρομολογητές στο Διαδίκτυο δεν είναι ρυθμισμένοι ώστε να υποστηρίζουν multicast. Για την αποτελεσματική χρήση των multimedia εφαρμογών, θα πρέπει να είναι δυνατή η διευθυνσιοδότηση των διαφόρων χρηστών, οι οποίοι ανήκουν σε διαφορετικά υποδίκτυα.

Το IPv6 επεκτείνει τις multicasting δυνατότητες του IPv4, προσφέροντας μια μεγάλη γκάμα διευθύνσεων πολλαπλής διανομής. Προφανώς, αυτό περιορίζει το βαθμό στον οποίο τα πακέτα πληροφοριών μπορούν τώρα να αναπαράγονται και βελτιώνουν σημαντικά την απόδοση του δικτύου. Επίσης το IPv6 βελτιώνει σημαντικά την έννοια των anycast υπηρεσιών, οι οποίες είναι διαθέσιμες και στο IPV4, αν και σε μια πολύ πιο απλούστερη μορφή. Στις anycast υπηρεσίες, τα πακέτα δεν αποστέλλονται σε όλους τους κόμβους του δικτύου, αλλά μόνο στον πλησιέστερα προσβάσιμο κόμβο. Μια τυπική εφαρμογή όπου η χρήση του anycast θα ήταν τεράστια είναι κατά την διάρκεια της ανακάλυψης ενός διακομιστή συγκεκριμένου τύπου, π.χ. ένος DNS server, ανάμεσα σε μια ομάδα διακομιστών. Θα παρέχει επίσης εναλλακτικές διαδρομές σε άλλους διακομιστές, έτσι ώστε αν για κάποιο λόγο, η διαδρομή προς το κύριο διακομιστή καταστεί μη διαθέσιμη, στην επόμενη σύνοδο, η σύνδεση θα πρέπει να υλοποιηθεί με τον επόμενο server της ομάδας.



Εικόνα 2.10: Multicast και Anycast τεχνικές

2.2.8 Το IPv6 προσφέρει καλύτερες δυνατότητες φορητότητας από το IPv4

Αν εξεταστούν τα χαρακτηριστικά φορητότητας του IP εξετάζονται ουσιαστικά τα χαρακτηριστικά που θα ήταν χρήσιμα για:

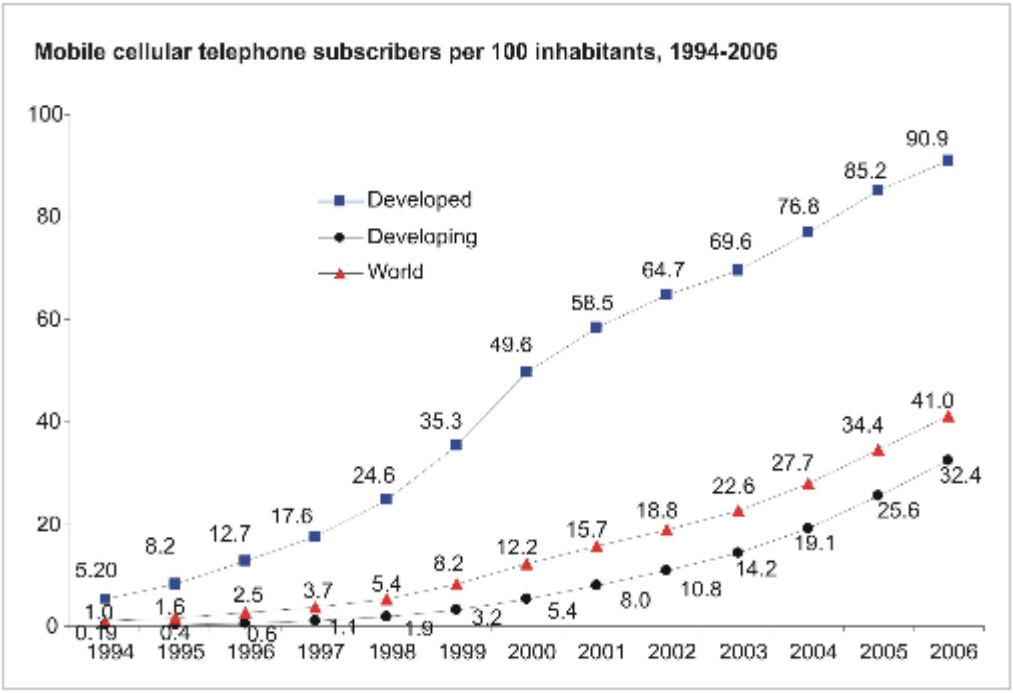
Κινητές συσκευές, οι οποίες μπορούν να αλλάξουν τη θέση τους, αλλά θα ήθελαν να διατηρήσουν τις υπάρχουσες συνδέσεις τους.

Δίκτυα κινητής τηλεφωνίας που προσφέρουν φορητότητα σε μια ομάδα συσκευών

Ad-hoc δικτύωση με την οποία ορισμένες από τις συσκευές παραμένουν συνδεδεμένες με το δίκτυο ή με μια περιοχή που γειτνιάζει με το δίκτυο μόνο για μικρής διάρκειας συνόδου επικοινωνίες

Όταν ένας κινητός κόμβος δεν είναι στο σπίτι, μεταδίδει πληροφορίες σχετικά με την τρέχουσα τοποθεσία του. Τώρα αν ένας κόμβος θέλει να επικοινωνήσει με αυτόν θα στείλει πρώτα τα πακέτα πληροφοριών στη διεύθυνση κατοικίας. Ο αντιπρόσωπος στο

σπίτι θα λάβει αυτά τα πακέτα και χρησιμοποιώντας έναν πίνακα, θα στείλει αυτά τα πακέτα στην τρέχουσα τοποθεσία του κινητού κόμβου.



Εικόνα 2.11: Διάγραμμα συνδρομητών κινητής τηλεφωνίας ανά 100 κατοίκους

Το κινητό IPv4 απαιτεί ειδικό δρομολογητή στη θέση του κινητού κόμβου ώστε να λαμβάνει τις κλήσεις σωστά. Επίσης, η βέλτιστη διαδρομή είναι διαθέσιμη προς κινητά IPv4 μόνο μέσα από ένα προαιρετικό σύνολο επεκτάσεων. Υπάρχει επίσης ένα πρόβλημα φιλτραρίσματος στο κινητό IPv4, δεδομένου ότι ο αντίστοιχος κόμβος χρησιμοποιεί τη διεύθυνση κατοικίας ως διεύθυνση προέλευσης του πακέτου και μπορεί έτσι να υπάρξει σύγχυση σχετικά με το ποιες διευθύνσεις IP πρέπει να το δεχτούν ή όχι

Στο IPv6 υποστηρίζεται υποχρεωτικά η φορητότητα με τη χρήση του MIPv6. Επίσης η εύρεση βέλτιστης διαδρομής είναι μια ενσωματωμένη δυνατότητα για κινητά IPv6. Επιπλέον, χαρακτηριστικά όπως το Neighbor Discovery και το Address Auto-configuration επιτρέπουν στους κινητούς κόμβους να λειτουργήσουν σε οποιαδήποτε θέση χωρίς να χρειάζονται οι υπηρεσίες των ειδικών δρομολογητών.

Το MIPv6 μπορεί να χρησιμοποιηθεί για να επιτευχθεί η απρόσκοπτη φορητότητα, επιτρέποντας μεταβιβάσεις μεταξύ των διαφόρων τεχνολογιών πρόσβασης π.χ. από ένα δίκτυο κινητής τηλεφωνίας σε ένα ασύρματο δίκτυο, με ελάχιστη διακοπή στις εν

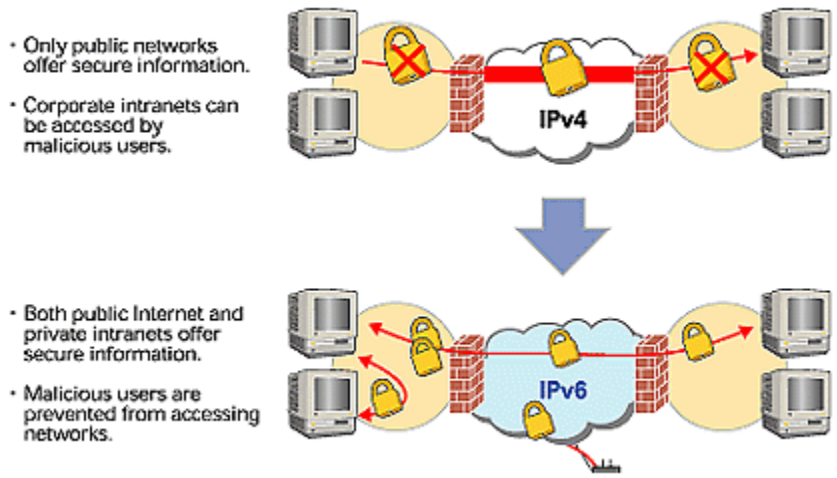
εξελίξει συνδέσεις. Δεν υπάρχει πρόβλημα φιλτραρίσματος στο Mobile IPv6 επειδή ο κόμβος ανταπόκρισης χρησιμοποιεί τη care-of address ως πηγή διεύθυνσης.

Οι συσκευές αυτές απαιτούν ολοένα και περισσότερο μεταφορά φωνής, βίντεο και δεδομένων, η οποία κατέστη δυνατή μέσω ενός προτύπου που ονομάζεται IP Multimedia Subsystem (IMS) πρότυπο. Ωστόσο, το IMS απαιτεί κάθε κινητή συσκευή να διαθέτει μια μοναδική διεύθυνση IP, η οποία θα είναι μια επίμονη διεύθυνση IP, προκειμένου να διασφαλιστούν οι πλήρως αμφίδρομες υπηρεσίες.

Το IPv6 μέσω του μεγάλου χώρου διευθύνσεων του εξασφαλίζει ότι κάθε κινητή συσκευή μπορεί να έχει τη δική της μοναδική διεύθυνση IP. Περαιτέρω, το Mobile IPv6 κάνει χρήση των επικεφαλίδων επέκτασης ώστε να προστεθούν και άλλες δυνατότητες όπως βελτιστοποίηση της διαδρομής μεταξύ των κινητών κόμβων κατά την περιαγωγή μεταξύ διαφορετικών δικτύων 3G.

2.2.9 Το IPv6 προσφέρει μεγαλύτερη ευκολία στη διαχείριση σε σχέση με το IPv4

Όταν σε ένα υπάρχον δίκτυο πρέπει να γίνει επέκταση, ή συγχώνευση δύο άλλων δικτύων ή αλλαγή παρόχων υπηρεσιών, τότε το δίκτυο πρέπει να μετατραπεί και να γίνει νέα ανάθεση συστήματος διευθυνσιοδότησης



Εικόνα 2.12: Συγχώνευση δικτύων

Με ένα δίκτυο IPv4, όλες οι εργασίες του δικτύου και η ανάθεση των νέων συστημάτων διεύθυνσης θα έπρεπε να γίνουν με το χέρι. ΣΕ αντίθεση το IPv6 παρέχει δυνατότητες ώστε η αναρίθμηση του δικτύου να μπορεί να συμβεί αυτόματα. Ένα άλλο χρήσιμο χαρακτηριστικό της διαχειριστικής ικανότητας του IPv6 είναι το multihoming. Με αυτό δύο ταυτόχρονες συνδέσεις είναι εγκατεστημένες σε δύο ISPS. Όταν μια υπηρεσία ISP έχει χαθεί, υπάρχει μια back-up σύνδεση στο Διαδίκτυο με τον άλλο ISP, με αυτό τον τρόπο εξασφαλίζεται πολύ μεγαλύτερη αξιοπιστία των υπηρεσιών, καθώς υπάρχουν περισσότερες από μία διαδρομές από τον χρήστη έως τον τελικό προορισμό.

Παρακάτω ακολουθεί πίνακας με τις βασικές διαφορές IPv4 και IPv6:

Subjects	IPv4	IPv6	IPv6 Advantages
Address Space	4 Billion Addresses	2^128	79 Octillion times the IPv4 address space
Configuration	Manual or use DHCP	Universal Plug and Play (UPnP) with or without DHCP	Lower Operation Expenses and reduce error
Broadcast / Multicast	Uses both	No broadcast and has different forms of multicast	Better bandwidth efficiency
Anycast support	Not part of the original protocol	Explicit support of anycast	Allows new applications in mobility, data center
Network Configuration	Mostly manual and labor intensive	Facilitate the re-numbering of hosts and routers	Lower operation expenses and facilitate migration
QoS support	ToS using DIFFServ	Flow classes and flow labels	More Granular control of QoS
Security	Uses IPsec for Data packet protection	IPsec becomes the key technology to protect data and control packets	Unified framework for security and more secure computing environment
Mobility	Uses Mobile IPv4	Mobile IPv6 provides fast handover, better router optimization and hierarchical mobility	Better efficiency and scalability; Work with latest 3G mobile technologies and beyond.

Πίνακας 2.1: Συγκεντρωτικός πίνακας διαφορών IPv6 – IPv4

2.3 Μετρήσεις

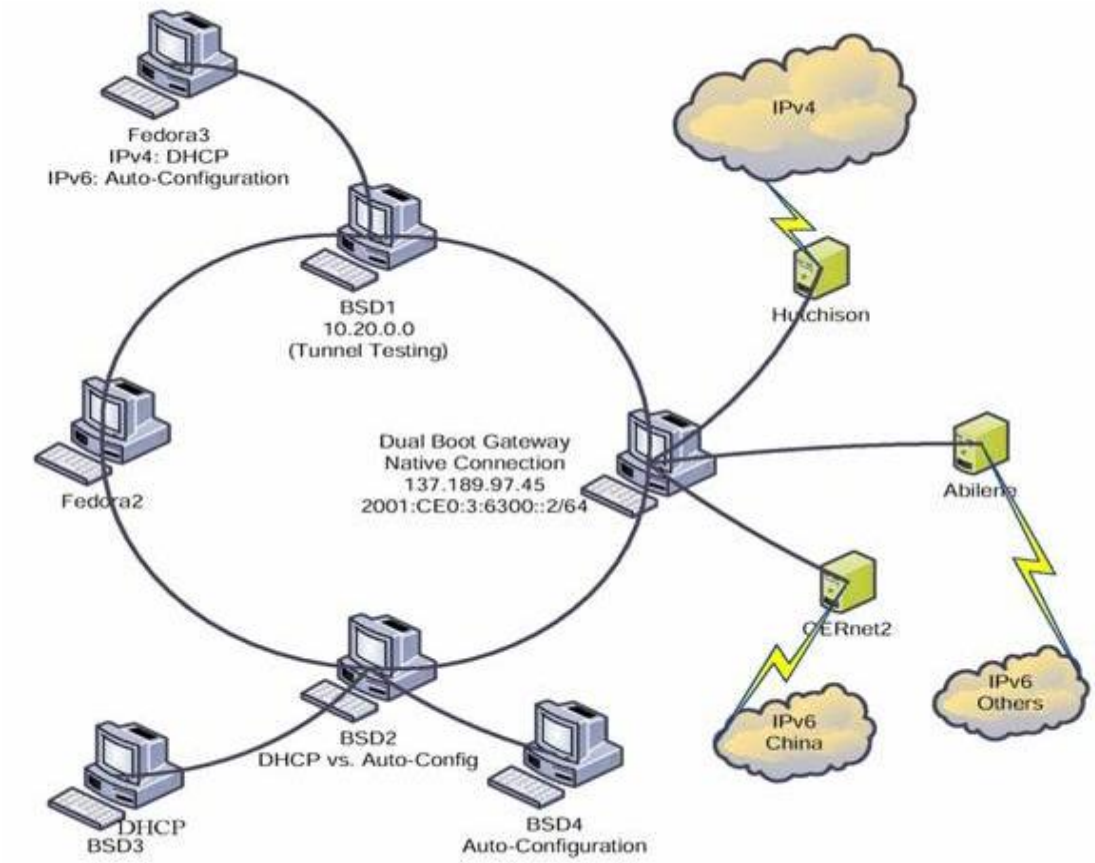
Για να μπορέσουμε να κατανοήσου από την μεριά του χρήστη τις διαφορές ως προς τις επιδόσεις του δικτύου περνώντας από το IPv4 στο IPv6 παραθέτουμε ορισμένες μετρήσεις. Για το σκοπό αυτό χρησιμοποιήθηκε probing traffic και δημιουργία κίνηση μέσω λήψεων αρχείων από πάνω από 2.000 dual-stack IPv6/IPv4.

2.3.1 Χαρακτηριστικά των μετρήσεων

Η μελέτη των μετρήσεων που αναφέρονται παρακάτω διεξήχθη από τα τέλη του 2006 μέχρι το πρώτο εξάμηνο του 2007.Για τις μετρήσεις χρησιμοποιήθηκαν επτά IPv6/IPv4 dual-stack μηχανήματα όπως φαίνεται στην εικόνα. Η πύλη μας είναι ένα dual-boot μηχάνημα, με Windows XP και Fedora Core 5. Τα μηχανήματα πελάτες ονομάζονται "BSD1-BSD4" και "Fedora2-Fedora3", τα BSD μηχανήματα τρέχουν FreeBSD 6.1 και τα μηχανήματα Fedora τρέχουν Fedora Core 5. Το δίκτυο των διεπαφών του κάθε μηχανήματος είναι συνδεδεμένο με μία δημόσια διεύθυνση IPv4 και μία διεύθυνση IPv6. Το υπο δοκιμή δίκτυο είναι συνδεδεμένο με μια σύνδεση 100Mbps στο IPv4 Internet μέσω του Hongkong Advanced Research Network (HARNET). Για το IPv6 υπάρχει μια σύνδεση 45Mbps με το HARNET, η οποία μοιράζεται με 7 άλλα πανεπιστήμια στο Χονγκ Κονγκ. Οι μετρήσεις είναι σχεδιασμένες για να διερευνηθούν οι διαφορές των επιδόσεων από dual-stack hosts που επιλέγουν μεταξύ IPv6 και IPv4. Κάθε μέτρηση επαναλήφθηκε 10 φορές κατά τη διάρκεια της ημέρας σε διαφορετικές ώρες και διαφορετικές μέρες της εβδομάδας.

		Pingable by IPv6	
		Yes	No
Pingable by IPv4	Yes	2014	7054
	No	208	1103

Πίνακας 2.2: Πίνακας διαθέσιμων δικτύων



Εικόνα 2.13: IPv6/IPv4 dual stack hosts and servers

<u>Παρακάτω γίνεται αναφορά ορισμένων Dual-Stack sites:</u>

Καθαρά IPv6 sites	Dual-Stack sites	Προσπελάσιμα Dual-Stack sites
alumni6.sjtu.edu.cn	03bm.vsix.net	03bm.vsix.net
amp-ipv6.cesnet.cz	052040.vsix.net	052040.vsix.net
analon.cns.ip6.vt.edu	0x2.org	0x2.org
apache.crihan.fr	1111.vsix.net	1111.vsix.net
ar.atwola.com.sixxs.org	40jaar.inzevenaar.nl	40jaar.inzevenaar.nl
as7684.bgp4.jp	6net.niif.hu	6net.niif.hu
atlantis.prolixium.com	6to4.nro.net	6to4.nro.net
audience.cnn.com.sixxs.org	a.tnh.jp	a.tnh.jp
batlabs.ipv6.enterzone.net	aaa.surfnet.nl	aaa.surfnet.nl
bonasses.blazing.de	aare.pri.ee	aare.pri.ee
boulder-inet6.tele.dk	abeceda.hvezdarna.cz	abeceda.hvezdarna.cz
cam.ipv6.switch.ch	adleman.dlitz.net	adleman.dlitz.net

cam01.6dns.org	admin.moonblade.net	admin.moonblade.net
camera2.cclipv6.itri.org.tw	ads.isoc.lu	ads.isoc.lu
chaz.ipv6.chaz6.com	afs94.pietermaritz.nl	afs94.pietermaritz.nl
cl-377.ams-01.nl.sixxs.net	albiero.astronomy.cz	albiero.astronomy.cz
Comclub-pt.tunnel.tserv1.fmt.ipv6.he.net	alexis.robertlan.eu.org	alexis.robertlan.eu.org
cpan.ipv6.elmundo.es	alphabet.ircnet.at	alphabet.ircnet.at
cucu.v6.mimora.com	alumni.mv.uni-kl.de	alumni.mv.uni-kl.de
cytosine6.bay13.net	alumni.su.lt	alumni.su.lt
d6.6dns.org	ameba.sc-uni.ktu.lt	ameba.sc-uni.ktu.lt
darkwing.ipv6.uoregon.edu	amiga.nvg.org	amiga.nvg.org
debian.ipv6.cesnet.cz	analyzer1.freebit.net	analyzer1.freebit.net
debian6.6dns.org	andre.cesnet.cz	andre.cesnet.cz
dino6.atoomnet.net	anstool.grnet.gr	anstool.grnet.gr
ed6.sjtu.edu.cn	apache.rhnet.is	apache.rhnet.is
felker.xs4all.nl.sixxs.org	apache.surfnet.nl	apache.surfnet.nl
files6.akl.lt	apo.astronomy.cz	apo.astronomy.cz
foundation6.sjtu.edu.cn	apocd.astronomy.cz	apocd.astronomy.cz
freebsd.ipv6.lostinspace.de	apt.conall.net	apt.conall.net
freesbee-inet6.wheel.dk	apt.uninett.no	apt.uninett.no
hdtv6.nm.gist.ac.kr	arabica.ecs.soton.ac.uk	arabica.ecs.soton.ac.uk
home.mahoroba.org	archive.spilsby.net	archive.spilsby.net
icae6.sjtu.edu.cn	asclepian.ie	03bm.vsix.net
imasd.ipv6.elmundo.es	a-select.surfnet.nl	052040.vsix.net
ipv6.6dns.org	03bm.vsix.net	0x2.org
ipv6.azet.org	052040.vsix.net	1111.vsix.net
ipv6.burcion.com	0x2.org	40jaar.inzevenaar.nl
ipv6.delouw.ch	1111.vsix.net	6net.niif.hu
audience.cnn.com.sixxs.org	40jaar.inzevenaar.nl	6to4.nro.net
batlabs.ipv6.enterzone.net	6net.niif.hu	a.tnh.jp
bonasses.blazing.de	6to4.nro.net	aaa.surfnet.nl
boulder-inet6.tele.dk	a.tnh.jp	aare.pri.ee
cam.ipv6.switch.ch	www.13thmonkey.org	abeceda.hvezdarna.cz
cam01.6dns.org	www.5minutesoffame.nl	adleman.dlitz.net
camera2.cclipv6.itri.org.tw	www.6diss.org	admin.moonblade.net
chaz.ipv6.chaz6.com	www.6gate.com	ads.isoc.lu
cl-377.ams-01.nl.sixxs.net	www.6journal.org	afs94.pietermaritz.nl
comclub-pt.tunnel.tserv1.fmt.ipv6.he.net	www.6net.org	albiero.astronomy.cz
cpan.ipv6.elmundo.es	www.6pack.org	www.ams-ix.net
cucu.v6.mimora.com	www.6win.dfn.de	www.amtek.nl
cytosine6.bay13.net	www.8823.net	www.anaka.jp
d6.6dns.org	www.aai.ee	www.analysis-of-patterns.net
darkwing.ipv6.uoregon.edu	www.aalca.uevora.pt	www.anltc.ie

debian.ipv6.cesnet.cz	www.aauug.dk	www.anst.uu.se
debian6.6dns.org	www.aboma.nl	www.antro.uu.se
dino6.atoomnet.net	www.abomafoon.nl	www.apan.net
ed6.sjtu.edu.cn	www.acad.bg	www.apnic.net
felker.xs4all.nl.sixxs.org	www.actae.uevora.pt	www.apops.net
files6.akl.lt	www.action-leonardo.net	www.apricot.net
foundation6.sjtu.edu.cn	www.ae.uevora.pt	www.arbmilj.uadm.uu.se
freebsd.ipv6.lostinspace.de	www.ae-osaka.co.jp	www.arbuz.dk
freesbee-inet6.wheel.dk	www.agentlink.org	www.arkeologi.uu.se
www.ipv6.siski.de	www.aitea.net	www.asahikawa.wide.ad.jp
www.ipv6.sixxs.net	www.akademihotellet.uu.se	www.asap.ecs.soton.ac.uk
www.ipv6.stack.nl	www.akademiskakapellet.uu.se	www.asia-bb.net
www.ipv6.vrijmoet.net	www.13thmonkey.org	www.asta.tu-clausthal.de
www.iua.ie	www.5minutesoffame.nl	www.ams-ix.net
www.jlu6.edu.cn	www.6diss.org	www.amtek.nl
www.microsoft.com.sixxs.org	www.6gate.com	www.anaka.jp
www.nasa.gov.sixxs.org	www.6journal.org	www.analysis-of-patterns.net
www.online-tutorials.net	www.6net.org	www.anltc.ie
www.playboy.com.sixxs.org	www.6pack.org	www.anst.uu.se
www.teameatme.com	www.6win.dfn.de	www.antro.uu.se
www.ttd.ipv6.elmundo.es	www.8823.net	www.apan.net
www.utrading.sk	www.aai.ee	www.apnic.net
www.v6.trueinternet.co.th	www.aalca.uevora.pt	www.apops.net
www.victoriassecret.com.sixxs.org	www.aauug.dk	www.apricot.net
www.volsec.ie	www.aboma.nl	www.arbmilj.uadm.uu.se
www.w3.org.sixxs.org	www.abomafoon.nl	www.arbuz.dk
www.ipv6.siski.de	www.acad.bg	www.arkeologi.uu.se
www.ipv6.sixxs.net	www.actae.uevora.pt	www.asahikawa.wide.ad.jp
www.ipv6.stack.nl	www.action-leonardo.net	www.asap.ecs.soton.ac.uk
www.ipv6.vrijmoet.net	www.ae.uevora.pt	www.asia-bb.net
www.iua.ie	www.ae-osaka.co.jp	www.asta.tu-clausthal.de

Πίνακας 2.3: Dual-Stack sites

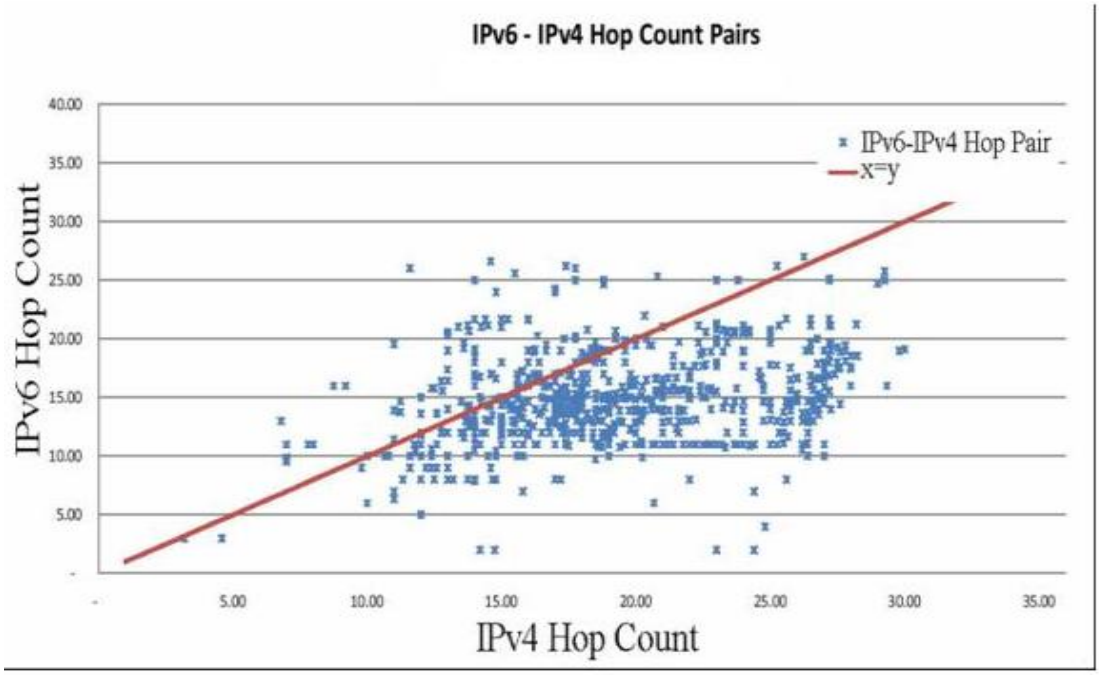
2.3.2 Συνδεσιμότητα

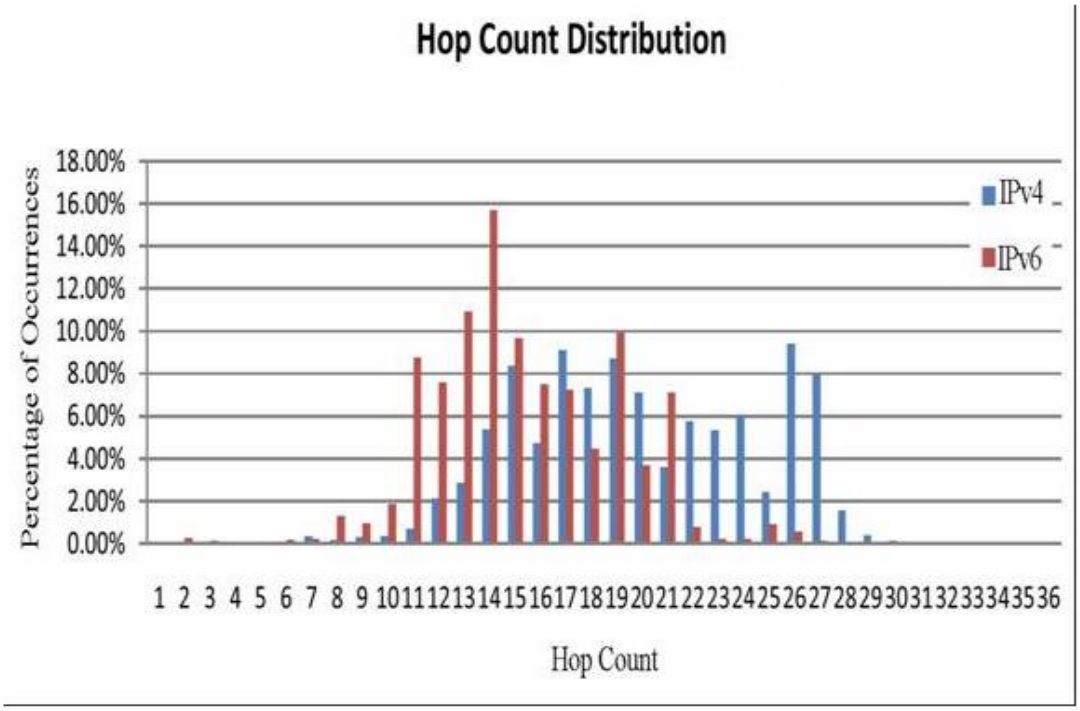
Στις μετρήσεις χρησιμοποιήθηκε ping και ping6 για τη διερεύνηση της σύνδεσης του IPv6, σε σύγκριση με το IPv4. Ο πίνακας δείχνει το μέσο ποσοστό των 2014 sites που είναι προσβάσιμα από IPv6/IPv4 κατά τη διάρκεια των μετρήσεων. Τα αποτελέσματα δείχνουν ότι πάνω από το 90% των τόπων είναι προσβάσιμο τόσο από το IPv6 και IPv4, με το IPv6 να έχει ποσοστό περισσότερο από 95% για σύνδεση με Dual-Stack sites. Τα αποτελέσματα δείχνουν ότι η σύνδεση κατά τις καθημερινές «εργάσιμες μέρες» και τα Σαββατοκύριακά δεν παρουσιάζουν σημαντικές διαφορές.

	Native IPv6	Native IPv4
Weekday	97.56%	90.74%
Weekend	96.57%	89.84%

2.3.3 Υπολογισμός των hops

Χρησιμοποιώντας traceroute και traceroute6, προσδιορίστηκε ο αριθμός των hops μεταξύ του κόμβου πηγής και του κόμβου προορισμού. Στις παρακάτω εικόνες παρουσιάζονται οι μετρήσεις των hop, τα μονοπάτια του IPv6 έχουν λιγότερα hop σε σύγκριση με τις διαδρομές του IPv4. Η μέση τιμή hop για τα IPv4 μονοπάτια και τις διαδρομές IPv6 είναι 19,81 hops και 15,22 hops αντίστοιχα. Αυτό μπορεί να οφείλεται στο γεγονός ότι υπάρχουν λιγότεροι IPv6 κόμβοι σε σύγκριση με τους IPv4 κόμβους στον κόσμο.

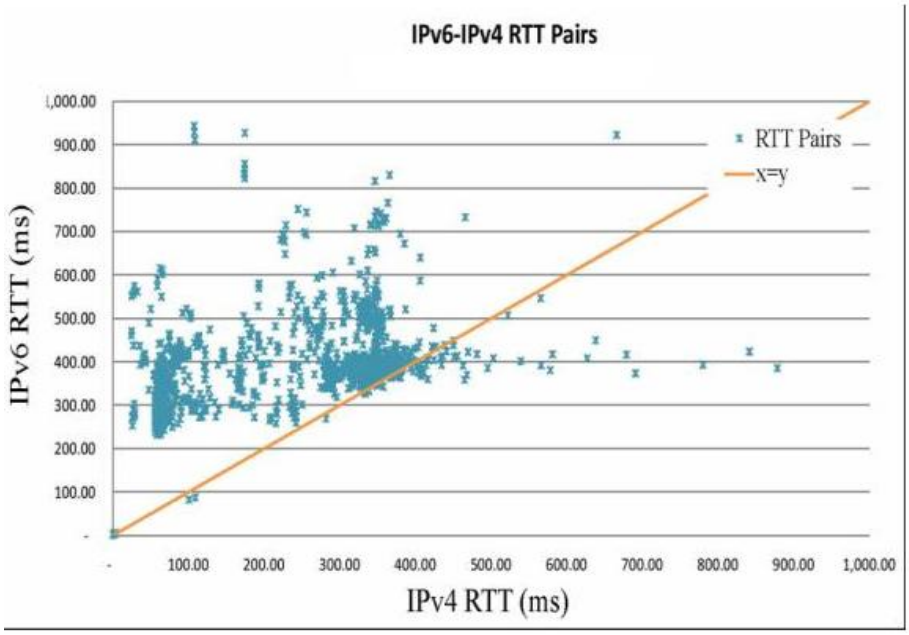


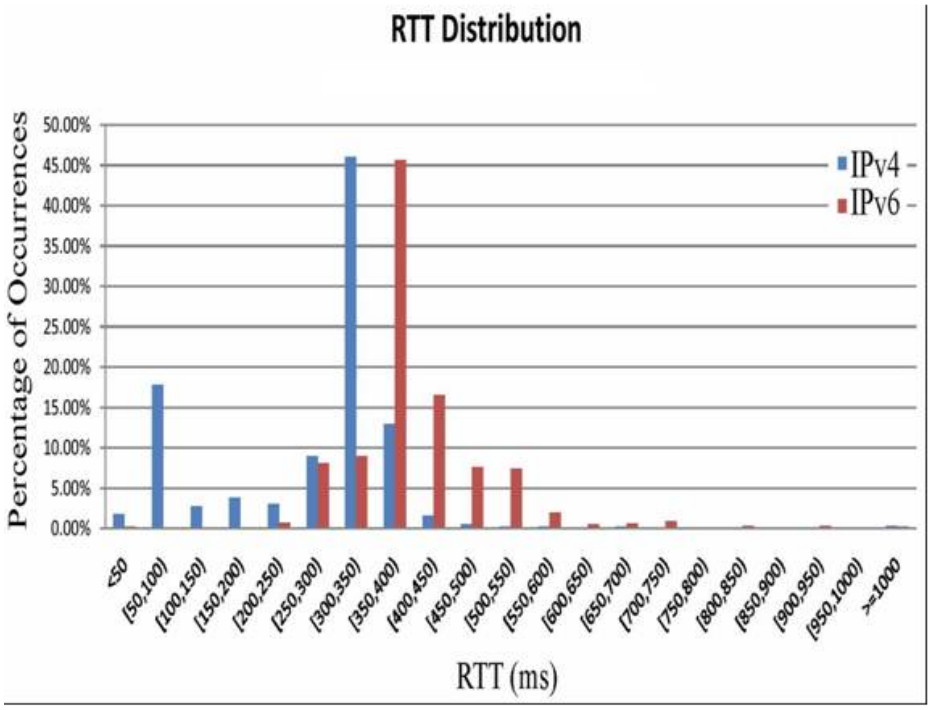


Εικόνα 2.14: Διαγράμματα μετρήσεων των hops

2.3.4 RTT "Round-trip delay time"

Η δοκιμή αυτή χρησιμοποιεί το ίδιο σύνολο των αποτελεσμάτων μετρήσεων της συνδεσιμότητας για να διερευνηθούν οι χρόνοι απόκρισης για τα πακέτα ping για διάφορους dual stack τοποθεσίες. Οι χρόνοι απόκρισης παρέχουν μια ένδειξη της ποιότητας της υπηρεσίας από την πλευρά των χρηστών στα δίκτυα IPv6/IPv4. Τα αποτελέσματά φαίνονται στην εικόνα και δείχνουν ότι τα IPv6 RTTs είναι υψηλότερα από τα RTTs IPv4. Οι μέσες τιμές των IPv6 και των IPv4 RTTs είναι 403.36ms και 272.78ms αντίστοιχα. Με την πρώτη ματιά, τα αποτελέσματα του RTT φαίνεται να έρχονται σε αντίθεση με τα αποτελέσματα από τον υπολογισμό των hops. Γενικά λιγότερα hops μεταφράζονται σε χαμηλότερα RTT για μια διαδρομή. Ωστόσο, λόγω του γεγονότος ότι ο αριθμός των κόμβων IPv6 και η συγκέντρωσή τους είναι μικρότερη και λιγότερο πυκνοί σε σχέση με τους κόμβους του IPv4, και ότι η άμεση διασύνδεσης των δικτύων IPv6 είναι χαμηλότερη σε σύγκριση με τα δίκτυα IPv4, υπάρχει μεγάλη πιθανότητα ότι τα IPv6 πακέτα να ταξιδεύουν σε μεγαλύτερη απόσταση μεταξύ των διαδοχικών hops σε σύγκριση με τα πακέτα IPv4 (οι διαδρομές του IPv6 είναι σημαντικά μεγαλύτερες σε σύγκριση με εκείνες των μονοπατιών του IPv4).



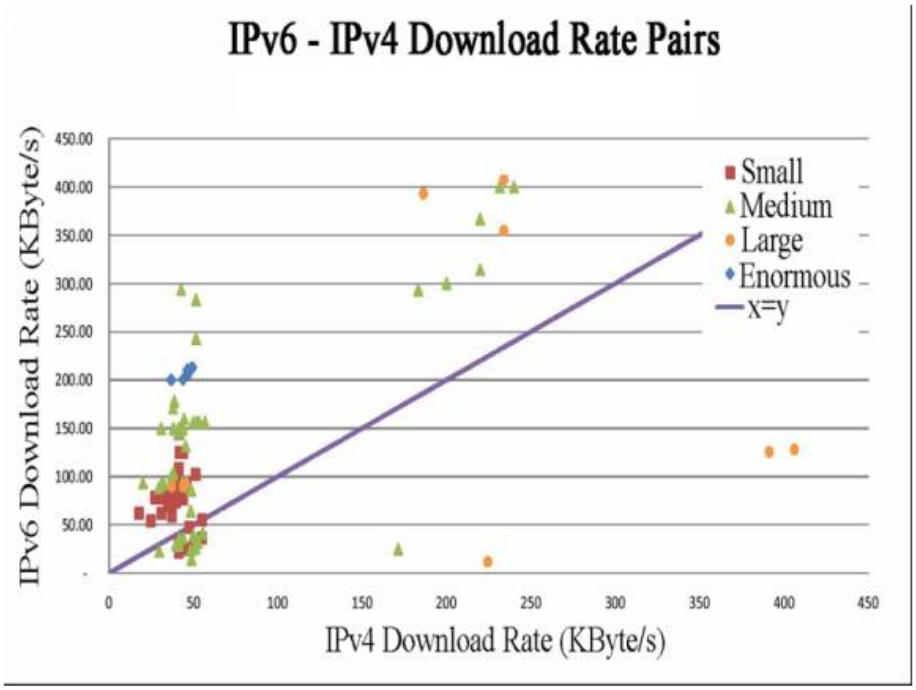


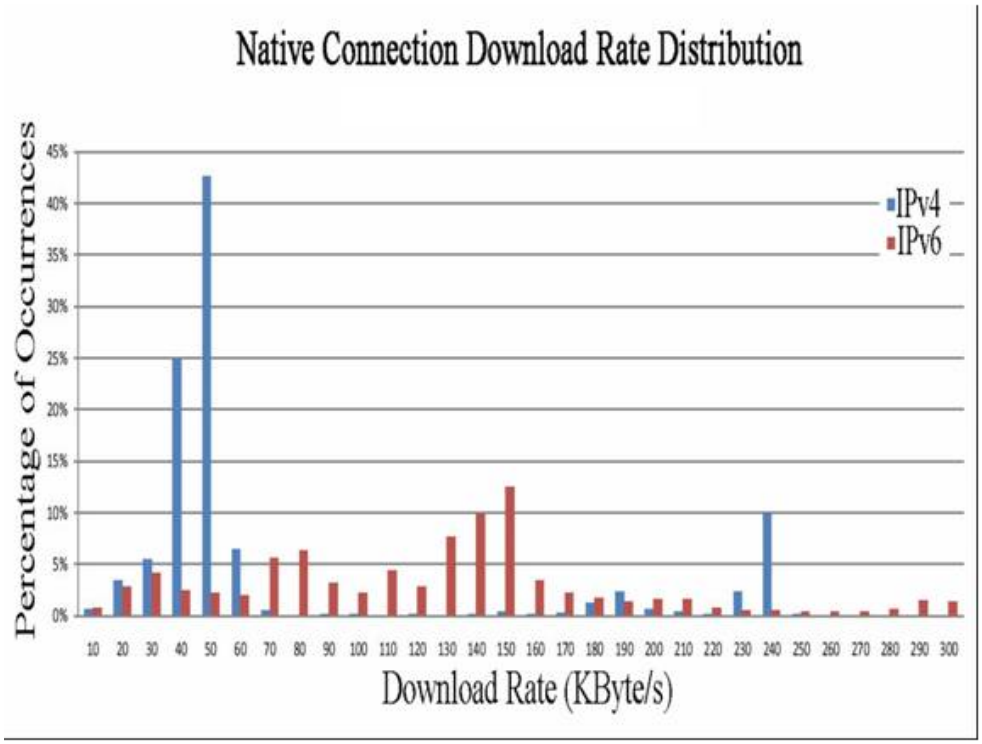
Εικόνα 2.15: Διαγράμματα μετρήσεων RTT

2.3.5 Ρυθμαπόδοση

Για αυτές τις μετρήσεις, χρησιμοποιήθηκαν wget και wget6 ώστε να κατέβουν αρχεία από τους dual stack διακομιστές, και στη συνέχεια αναλύθηκε η μέση απόδοση λήψης τους. Για να γίνει μια αμερόληπτη ανάλυση, κατέβηκαν αρχεία από τους διακομιστές με διαφορετικά λειτουργικά συστήματα, έτσι ώστε να μην επηρεάζεται από το είδος των Oses που χρησιμοποιούνται από αυτούς. Τα αρχεία που κατέβηκαν έχουν διάφορα μεγέθη που κυμαίνονται από 254KB σε 538MB. Σε αυτή τη δοκιμή, κατηγοριοποιήθηκαν τα αποτελέσματά με βάση το μέγεθος του αρχείου, δηλαδή κάτω του 1MB (μικρό), από 1MB έως 10MB (μεσαίο), από 10MB έως 100MB (μεγάλο) και πάνω από 100MB (τεράστιο).

Στις εικόνες φαίνεται ότι η ρυθμαπόδοση του IPv6 είναι υψηλότερη από αυτήν του IPv4, ιδίως για τις μεγάλα και τεράστια αρχεία. Η μέση ρυθμοαπόδοση του IPv6 είναι 107.75KB/s, ενώ στο IPv4 είναι 77.88KB/s. Αυτό μπορεί να εξηγηθεί από το γεγονός ότι το δίκτυο κορμού του IPv6έχει λιγότερη συμφόρηση, σε σύγκριση με το δίκτυο κορμού IPv4, και ως εκ τούτου, το ποσοστό κατεβάσματος στο IPv6 είναι υψηλότερο από αυτό του IPv4. Αν επικεντρωθούμε στην περιοχή με τα περισσότερα σημεία στην εικόνα. , βλέπουμε ότι η διακίνηση IPv6 για τεράστια μεγέθους αρχεία είναι περίπου 200KB/s. Για τα μεγάλου μεγέθους αρχεία, η διακίνηση IPv6 είναι περίπου 100KB/s, για τα μεσαίου μεγέθους αρχεία η διακίνηση IPv6 είναι περίπου 150KB/s και για τα μικρού μεγέθους αρχεία η ρυθμαπόδοση στο IPv6 κυμαίνεται από 50 έως 100KB/s. Τα αποτελέσματα αυτά δείχνουν ότι όσο μεγαλύτερο το μέγεθος του αρχείου, τόσο μεγαλύτερη είναι η ρυθμαπόδοση του IPv6.





Εικόνα 2.16: Διαγράμματα ρυθμαπόδοσης

2.4 Συμπεράσματα

Το IPv6 έχει ξεπεράσει πολλούς από τα περιορισμούς του IPv4 ενώ εισάγει νέα χαρακτηριστικά και λειτουργίες για να κάνει τη δουλειά του διαχειριστή του δικτύου ευκολότερη. Στις περιπτώσεις που το IPv6 είναι σημαντικά διαφορετικό από το IPv4, οι αλλαγές προορίζονται να ενισχύσουν την διαχειριστική ικανότητα. Οι ομοιότητες με το IPv4 , κάνουν το IPv6 να φαίνεται αισθάνεται γνώριμο.

Κατά την αντιμετώπιση των αδυναμιών του IPv4, το IPv6 έχει σημειώσει μεγάλη πρόοδο. Το πιο προφανές είναι ότι το IPv6 έχει ένα χώρο διευθύνσεων των 128 bits (έναντι 32 bits στο IPv4), η οποία επιτρέπει σε πολύ περισσότερες συσκευές να συνδεθούν σε ένα δίκτυο. Επιπλέον, το IPv6 βελτιώνει τις επιδόσεις του δρομολογητή μέσω της χρήσης πιο συνοπτικές επικεφαλίδων δικτύου, , τη μείωση εκπομπών του δικτύου, καθώς και την αποστολή κατακερματισμένων. Το IPv6 είναι ένα βασικό

βήμα για να καταστεί το Διαδίκτυο των πραγμάτων εφικτό. Αφού Διαδίκτυο των πραγμάτων προϋποθέτει ότι εκατομμύρια αντικείμενα-συσκευές θα είναι συνδεδεμένες μεταξύ τους. Αυτό σημαίνει ότι θα υπάρχει ανάγκη από εκατομμύρια διευθύνσεις τι οποίες μόνο το IPv6 μπορεί να καλύψει.

Το γεγονός ότι η τεχνολογία είναι νέα αντιπροσωπεύει σημαντικές προκλήσεις για αυτού που θέλουν την εφαρμόσουν. Ωστόσο, πολλές από τις προκλήσεις είναι επιφανειακές, διότι η βασική αρχιτεκτονική και οι αρχές του σχεδιασμού του δικτύου δεν έχουν αλλάξει. Έτσι, πολλές αλλαγές στο IPv6 είναι επιφανειακές. Για παράδειγμα, το IPv6 δεν χρησιμοποιεί πλέον "ιδιωτικές διευθύνσεις [RFC 1918]", αλλά αντίθετα χρησιμοποιεί δύο τύπους διευθύνσεων δικτύου που ονομάζεται "site-local" και "link-local" διευθύνσεις. Τα "Address Resolution Protocol" και "Router Discovery Protocol" έχουν αντικατασταθεί από το Neighbor Discovery Protocol. Το DHCP (Dynamic Host Configuration Protocol) δεν είναι απαραίτητο , οι χρήστες μπορούν να διαπραγματεύονται τις διευθύνσεις τους κατά την εκκίνηση.

Τέλος, η εφαρμογή τεχνικών εγχειρίδια που χρησιμοποιούνται για πολλά δίκτυα IPv4 είναι πολύ παρόμοια για τα IPv6 δίκτυα. Αυτό επιτρέπει στους IPv6 φορείς υλοποίησης να κάνουν χρήση της υπάρχουσας εμπειρογνωμοσύνη τους στην ανάπτυξη της επόμενης γενιάς δικτύων που χρησιμοποιούν το πλαίσιο IPv6.

2.5 Βιβλιογραφία

http://en.wikipedia.org/wiki/IPv6

http://www.ipv6.com

http://mobitec.ie.cuhk.edu.hk

http://www.networkdictionary.com/

http://www.ieee.com

James F. Kurose kai Keith W. Ross. Δικτύωση Υπολογιστών, 4nd edition, Addison Wesley, 2007.

Ιάκωβος Βενιέρης, Ευγενία Νικολούζου. Τεχνολογίες Διαδικτύου, 2η Έκδοση, Εκδόσεις Τζιόλα, 2006

Andrew S. Tanenbaum . Δίκτυα Υπολογιστών, Εκδόσεις Παπασωτηρίου, 2000

Χρ. Μπούρας.Εισαγωγή στην IPv6 τεχνολογία, http://www.6net.org/publications/,2006

Janos Mohacsi.IPv6 Security:Threats and solutions, NIIF/HUNGARNET IPv6 project,2005

Hayoung Oh Kijoon Chae . An Efficient Security Management in IPv6 Network via MCGA,www.ieee.com, 2004

Κεφάλαιο 3ο

Ασφάλεια

3.1 Παρουσίαση

Το Διαδίκτυο έχει υποστεί σοβαρές αλλαγές από την στιγμή της έναρξής του στα τέλη της δεκαετίας του 1960, λόγω του ARPANET (Advanced Research Projects Agency Network). Το αρχικό δίκτυο τεσσάρων κόμβων έχει αυξηθεί σε ένα άκρως διασυνδεδεμένο και αυτο-οργανωμένο δίκτυο στο οποίο στηρίζουν καθημερινά οι επιχειρήσεις την έρευνα και την οικονομία τους. Ο αριθμός των ανθρώπων που χρησιμοποιούν το παγκόσμιο δίκτυο έχει αναπτυχθεί με γεωμετρική πρόοδο περίπου στο 1,5 δισ., ποσοστό που επί του παρόντος αντιπροσωπεύει περίπου το 20% του παγκόσμιου πληθυσμού. Αυτός ο μεγάλος αριθμός τελικών χρηστών – ο οποίος δεν περιλαμβάνει τους διακομιστές και τους δρομολογητές στο εσωτερικό των δικτύων - έχει αλλάξει την καθημερινή μας ζωή και τις συνήθειες μας. Με την ελαχιστοποίηση των διαστάσεων των συσκευών, την αύξηση της υπολογιστικής δύναμης, και τη μείωση της κατανάλωσης ενέργειας, η τάση αυτή θα συνεχιστεί υπό την μορφή του Διαδικτύου των πραγμάτων.

Μία από τις μεγαλύτερες προκλήσεις σε ένα διασυνδεδεμένο κόσμο συστημάτων και αισθητήρων είναι η ασφάλεια και η προστασία της ιδιωτικότητας. Χωρίς διαβεβαιώσεις ότι η ασφάλεια των προσωπικών δεδομένων εξασφαλίζεται οι χρήστες δεν θα είναι πρόθυμοι να υιοθετήσουν αυτή τη νέα τεχνολογία που ενσωματώνεται αόρατα στο περιβάλλον της ζωής τους. Εκτός από τις τεχνικές λύσεις για την παροχή προστασίας της ιδιωτικότητας και της ασφάλειας, πρέπει να εφαρμόζονται και περαιτέρω μέτρα όπως κυβερνητικοί και ηθικοί θεσμοί. Κάθε φορά που κάποιο "πράγμα" συνδέεται με το παγκόσμιο Διαδικτύου και με άλλα «πράγματα», νέα προβλήματα ασφάλειας και προστασίας της ιδιωτικότητας προκύπτουν, ως προς την εμπιστευτικότητα, την αυθεντικότητα και την ακεραιότητα των δεδομένων που ανιχνεύονται και ανταλλάσσονται από αυτά. Η ιδιωτικότητα των ανθρώπων και των πραγμάτων πρέπει να διασφαλίζεται και επίσης να παρεμποδίζονται η ταυτοποίηση και η παρακολούθηση. Περαιτέρω, ακόμα και τα πιο αυτόνομα και ευφυή πράγματα έχουν προβλήματα όπως η προστασία της ταυτότητας και της ιδιωτικότητας των ιδίων. Μέχρι τώρα, αλλοιωμένα ψηφιακά συστήματα δεν είναι ως επί το πλείστον σε θέση να ενεργούν με το φυσικό κόσμο. Αυτό πιθανό να αλλάξει δραματικά σε ένα επικίνδυνο σενάριο όπου κατεστραμμένα ψηφιακά συστήματα θα μπορούν να λειτουργούν και να επηρεάζουν το φυσικό κόσμο.

Στη συνέχεια θα παρουσιαστεί «υποπαράγραφος 2» μια ανάλυση των στοιχείων του Διαδικτύου των πραγμάτων, της ευαισθησία τους όσο αφορά την ασφάλεια και την προστασία της ιδιωτικότητας, καθώς και μια ανάλυση της κατάστασης στον τομέα της έρευνας για θέματα που θεωρούνται ως εξαιρετικά ευαίσθητα. Επίσης θα αναφερθούν «υποπαράγραφος 3.4» δύο βασικές συνιστώσες του Διαδίκτυου των πραγμάτων - Global Sensor Networks και RFID – και εισάγονται λεπτομέρειες που αφορούν την ασφάλεια

και το έργο της ιδιωτικότητας. Αναλύονται τα αποτελέσματα ερευνών «υποπαράγραφος 4» από άλλους τομείς που αξίζουν να μελετηθούν για το Διαδίκτυο των πραγμάτων και τέλος «υποπαράγραφος 3.5 » παρατίθενται κάποιες παρατηρήσεις.

3.2 Ανάλυση της ασφάλειας και του απορρήτου

Καθώς το Διαδίκτυο των πραγμάτων είναι ένα μεγάλο πεδίο με χρήση διαφόρων τεχνολογιών, παρέχεται μια κατηγοριοποίηση των τεχνολογιών αυτών στην Ενότητα 2.1. Η κατηγοριοποίηση αυτή χρησιμεύει ως βάση για λεπτομέρειες σχετικά με την ασφάλεια και την ευαισθησία της ιδιωτικότητας στους αντίστοιχους τομείς. Στη συνέχεια, στο 2.2 εξετάζεται η κατάσταση της έρευνας στις καθορισμένες κατηγορίες και επισημαίνονται λεπτομέρειες σχετικά με θέματα που η έρευνα είναι ανεπαρκής.

3.2.1 Κατηγοριοποίηση και Ευαισθησία

Στην Εικόνα 3.1 φαίνεται μια κατηγοριοποίηση των θεμάτων - εσωτερικά στοιχεία - και των αντίστοιχων τεχνολογιών που χρησιμοποιούνται σε κάθε θέμα - εξωτερικά στοιχεία - που απαρτίζουν το Διαδίκτυο των πραγμάτων. Το Διαδίκτυο των πραγμάτων μπορεί να ταξινομηθεί σε οκτώ θεματικές ενότητες:

• Επικοινωνίες που επιτρέπουν την ανταλλαγή πληροφοριών μεταξύ των συσκευών

• Αισθητήρες για την καταγραφή και την αντιστοίχιση του φυσικού κόσμου στον ψηφιακό.

• Μετατροπείς ώστε να εκτελούνται ενέργειες στον φυσικό κόσμο, οι οποίες προκλήθηκαν από τον ψηφιακό.

• Αποθηκευτικός χώρος για τη συλλογή στοιχείων από αισθητήρες, την ταυτοποίηση και την παρακολούθηση των συστημάτων

• Συσκευές για την αλληλεπίδραση με τους ανθρώπους στον φυσικό κόσμο

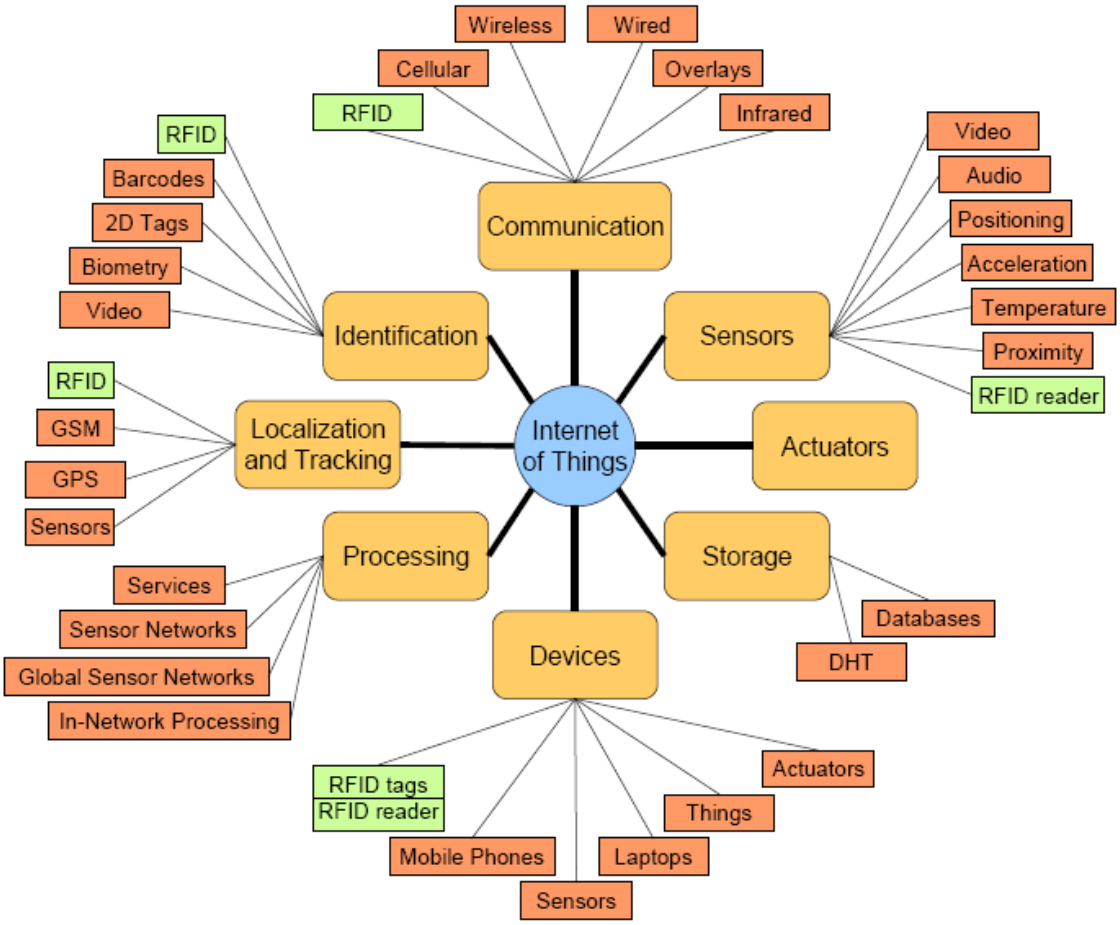
• Επεξεργασία για την παροχή δεδομένων και υπηρεσιών

• Εντοπισμός και παρακολούθηση

• Αναγνώριση για την παροχή μοναδικής ταυτότητας ενός φυσικού αντικειμένου στον ψηφιακό κόσμο.

Το κάθε θέμα χρησιμοποιεί διαφορετικές τεχνολογίες. Η κατηγοριοποίηση που έγινε δεν είναι αυστηρά ιεραρχική από άποψη θεμάτων και τεχνολογιών. Για παράδειγμα η αναγνώριση στην πραγματικότητα είναι μια μορφή επεξεργασίας που προκύπτει από την χρήση των αισθητήρων, έχει έναν ειδικό ρόλο στο Διαδίκτυο των πραγμάτων που είναι ανεξάρτητη από τη φυσική έννοια της αίσθησης και θα αντιμετωπίζεται ως ξεχωριστό θέμα. Βασική τεχνολογία η οποία ήδη έχει αναφερθεί πολλές φορές είναι το RFID η οποία χρησιμοποιείται ως τεχνολογία επικοινωνίας, και επιπλέον παρέχει αναγνώριση, εντοπισμό και παρακολούθηση. Οι συσκευές ανάγνωσης RFID ενεργούν ως αισθητήρες ενώ τέλος οι ετικέτες RFID μαζί με τις συσκευές ανάγνωσης αποτελούν μέρη του Διαδικτύου των πραγμάτων.

Τα θέματα αναφέρονται ξανά στον πίνακα 3.1 όπου έχουν καθορισθεί με βάση τις ιδιότητες της ασφάλειας και της ιδιωτικότητας. Οι ιδιότητες είναι αυτές που λαμβάνονται από τη CIA Triad «confidentiality, integrity and availability, εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα» και το Parkerian Hexad «έξι στοιχεία της ασφάλειας πληροφοριών προτεινόμενα από τον Donn B. Parker». Για κάθε θέμα ο πίνακας περιέχει την ευαισθησία και την αντίστοιχη ιδιότητα. Όπως και παραπάνω η κατηγοριοποίηση δεν είναι αυστηρά ιεραρχική, η ευαισθησία του κάθε θέματος μερικές φορές εξαρτάται από την ευαισθησία των άλλων ιδιοτήτων.



Εικόνα 3.1: Κατηγοριοποίηση θεμάτων και τεχνολογίες του Διαδικτύου των πραγμάτων

Topic \ Property	Integrity	Authenticity	Confidentiality	Privacy	Availability	Regulation
Communication	+++	+++	+++	++	+++	+
Sensors	+++	++	+	+++	+	+++
Actuators	+	+	+		+	++
Storage	+++	++	+++	+++	+	+++
Devices	+++	+	+	++	++	++
Processing	++	+	+	+++	+	+++
Localization/Tracking	+	+	+++	+++	+++	+++
Identification	++	+	+++	+++	+++	+++

Πίνακας 3.1: Η ευαισθησία των θεμάτων της ασφάλειας

Επικοινωνία: Έρευνες σε πρωτόκολλα επικοινωνίας έχουν καταλήξει σε λύσεις που παρέχουν ακεραιότητα, αυθεντικότητα και το απόρρητο αυτής. Τέτοιες είναι το TLS ή το SSL. Η προστασία της ιδιωτικότητας πρέπει να αντιμετωπιστεί από διάφορα συστήματα δρομολόγησης όπως η Onion δρομολόγηση ή η Freenet αλλά δυστυχώς και οι δύο δεν είναι σε ευρεία χρήση. Ανοικτό θέμα παραμένει η ύπαρξη DDoS επιθέσεων.

Το Επίπεδο Ασφαλών Sockets, *Secure sockets layer (SSL),* που αρχικά αναπτύχθηκε από την Netscape, είναι ένα πρωτόκολλο σχεδιασμένο ώστε να παρέχει κρυπτογράφηση και πιστοποίηση δεδομένων ανάμεσα σε έναν πελάτη Web και σε έναν εξυπηρετητή Web. Το πρωτόκολλο αρχίζει με μια φάση χειραψίας που διαπραγματεύεται έναν αλγόριθμο κρυπτογράφησης (π.χ., DES ή IDEA) και κλειδιά και πιστοποιεί τον εξυπηρετητή. στον πελάτη. Προαιρετικά, ο πελάτης μπορεί επίσης να πιστοποιηθεί από τον εξυπηρετητή. Όταν ολοκληρωθεί η χειραψία και αρχίσει η μετάδοση των δεδομένων της εφαρμογής, όλα τα δεδομένα κρυπτογραφούνται χρησιμοποιώντας κλειδιά συνόδου, για τα οποία έχει γίνει διαπραγμάτευση κατά τη φάση χειραψίας. Το SSL χρησιμοποιείται ευρέως στο ηλεκτρονικό εμπόριο και υλοποιείται σε σχεδόν όλα τα δημοφιλή προγράμματα περιήγησης και σε εξυπηρετητές Web. Ακόμη, είναι επίσης η βάση για το πρωτόκολλο Ασφάλειας Επιπέδου Μεταφοράς (Transport Layer Security, TLS) [RFC 2246].

Τα SSL και TLS δεν περιορίζονται στην εφαρμογή Web. Για παράδειγμα, μπορούν να χρησιμοποιηθούν παρόμοια για πιστοποίηση και για κρυπτογράφηση δεδομένων για προσπέλαση ταχυδρομείου IMAP (lnternet Mail Access Protocol). Το SSL μπορεί να θεωρηθεί σαν ένα επίπεδο που βρίσκεται ανάμεσα στο επίπεδο εφαρμογής και στο επίπεδο μεταφοράς. Στην πλευρά αποστολής, το SSL δέχεται δεδομένα (όπως ένα μήνυμα HΠP ή IMAP από μια εφαρμογή), κρυπτογραφεί τα δεδομένα και κατευθύνει τα κρυπτογραφημένα-δεδομένα σε μια TCP socket. Στην πλευρά λήψης, το SSL διαβάζει από την TCP socket, αποκρυπτογραφεί τα δεδομένα και τα κατευθύνει στην εφαρμογή. Αν και το SSL μπορεί να χρησιμοποιηθεί με πολλές εφαρμογές Διαδικτύου, θα το συζητήσουμε στο περιβάλλον Web, όπου χρησιμοποιείται κυρίως σήμερα για ηλεκτρονικό εμπόριο.

Το SSL παρέχει τα παρακάτω χαρακτηριστικά:

- Πιστοποίηση εξυπηρέτη SSL, που επιτρέπει σε ένα χρήστη να επιβεβαιώσει την ταυτότητα ενός εξυπηρέτη. Ένα πρόγραμμα περιήγησης με δυνατότητες SSL διατηρεί μια λίστα έμπιστων αρχών πιστοποίησης (CA) μαζί με τα δημόσια κλειδιά των CA. Όταν το πρόγραμμα περιήγησης θέλει να συνεργαστεί με έναν εξυπηρέτη Web με δυνατότητες SSL, το πρόγραμμα περιήγησης παίρνει ένα πιστοποιητικό από τον εξυπηρέτη, που περιέχει το δημόσιο κλειδί του εξυπηρέτη. Το πιστοποιητικό εκδίδεται (δηλαδή, υπογράφεται ψηφιακά) από μια CA, που αναφέρεται στη λίστα των έμπιστων CA του πελάτη. Αυτό το χαρακτηριστικό επιτρέπει στο πρόγραμμα περιήγησης να πιστοποιήσει τον εξυπηρέτη πριν ο χρήστης να υποβάλει έναν αριθμό κάρτας πληρωμών. Στο περιβάλλον του προηγούμενου παρα-δείγματος, αυτή η πιστοποίηση εξυπηρέτη επιτρέπει στον

Bob να επαληθεύσει ότι στέλνει πράγματι τον αριθμό της κάρτας πληρωμών του στην Alice Incorporated και όχι σε κάποιον άλλο, που ίσως να υποδύεται την Alice Incorporated .

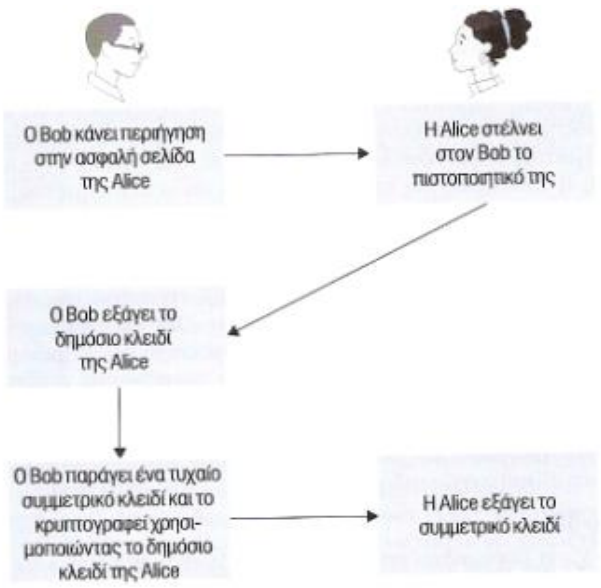
- Πιστοποίηση πελάτη SSL, που επιτρέπει σε έναν εξυπηρέτη να επιβεβαιώσει την ταυτότητα ενός χρήστη. Ανάλογα με την πιστοποίηση εξυπηρέτη, η πιστοποίηση πελάτη χρησιμοποιεί πιστοποιητικά πελατών, τα οποία έχουν εκδοθεί επίσης από CA. Αυτή η πιστοποίηση είναι σημαντική αν ο εξυπηρέτης, για παράδειγμα, είναι μια τράπεζα που στέλνει εμπιστευτικές οικονομικές πληροφορίες σε έναν πελάτη και θέλει να ελέγξει την ταυτότητα του παραλήπτη. Η πιστοποίηση πε-λάτη, αν και υποστηρίζεται από το SSL, είναι προαιρετική. Για να κρατήσουμε τη συζήτησή μας εστιασμένη στο θέμα μας, θα την αγνοήσουμε .
- Μια κρυπτογραφημένη σύνοδο SSL, στην οποία όλες οι πληροφορίες που στέλνο-νται ανάμεσα στο πρόγραμμα περιήγησης και στον εξυπηρέτη κρυπτογραφού-νται από το λογισμικό αποστολής (πρόγραμμα περιήγησης ή εξυπηρέτη Web) και αποκρυπτογραφούνται από το λογισμικό λήψης (πρόγραμμα περιήγησης ή εξυπηρέτη Web). Αυτή η εμπιστευτικότητα μπορεί να είναι σημαντική τόσο για τον πελάτη, όσο και για τον έμπορο. Επίσης, το SSL παρέχει ένα μηχανισμό για ανί-χνευση της επέμβασης στις πληροφορίες από έναν εισβολέα.

Πώς λειτουργεί το SSL

Ένας χρήστης, π.χ., ο Bob, κάνει περιήγηση στο Web και κάνει κλικ σε μια σύνδεση, που τον μεταφέρει σε μια ασφαλή σελίδα, η οποία βρίσκεται μέσα στον εξυπηρέτη με δυνατότητες SSL της Alice. Το τμήμα πρωτοκόλλου του URL για αυτή τη σελίδα είναι "https" και όχι το γνωστό "http". Το πρόγραμμα περιήγησης και ο εξυπηρέτης εκτελούν κατόπιν το πρωτόκολλο χειραψίας SSL, το οποίο (1) πιστοποιεί τον εξυπηρέτη (2) παράγει ένα διαμοιρασμένο συμμετρικό κλειδί. Και οι δύο αυτές εργασίες χρησιμοποιούν την τεχνολογία δημόσιου κλειδιού RSA. Η κύρια ροή των γεγονότων κατ φάση χειραψίας φαίνεται στην εικόνα 3.2. Κατά την διάρκεια αυτής της φάσης η Alice στέλνει στον Bob το πιστοποιητικό της, από το οποίο ο Bob παίρνει το δημόσιο κλειδί της Alice. Ο Bob κατόπιν δημιουργεί ένα τυχαίο συμμετρικό κλειδί, το κρυπτογραφεί με το δημόσιο κλειδί της Alice και στέλνει το κρυπτογραφημένο κλειδί Alice. Ο Bob και η Alice μοιράζονται τώρα ένα συμμετρικό κλειδί συνόδου. Όταν ολοκληρωθεί το πρωτόκολλο χειραψίας, όλα τα δεδομένα που στέλνονται ανάμεσα πρόγραμμα περιήγησης και στον εξυπηρέτη (επάνω σε συνδέσεις TCP) κρυπτογραφούνται χρησιμοποιώντας το συμμετρικό κλειδί συνόδου.

Αφού κάναμε μια επισκόπηση υψηλού επιπέδου του SSL, ας εξετάσουμε ανα αναλυτικότερα μερικές από τις πιο σημαντικές λεπτομέρειες. Η χειραψία SSL κάνει τα παρακάτω βήματα:

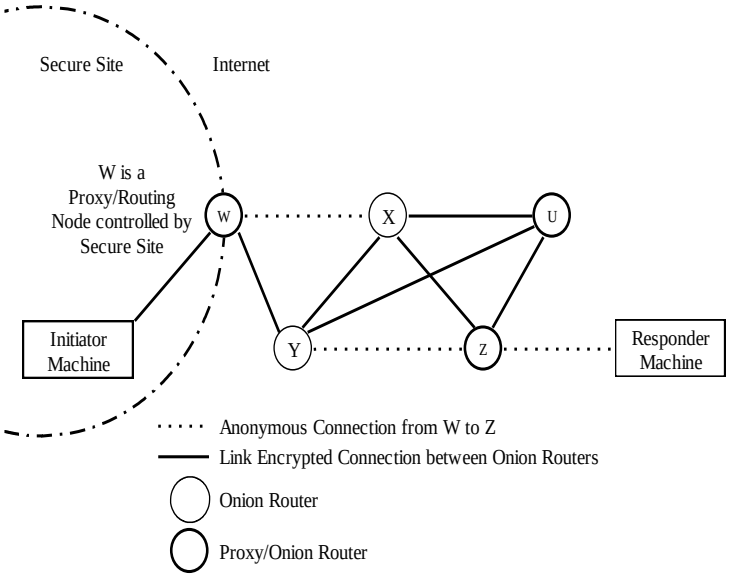
1. Το πρόγραμμα περιήγησης στέλνει στον εξυπηρέτη τον αριθμό έκδοσης SSL τις προτιμήσεις κρυπτογράφησης του προγράμματος περιήγησης. Το πρόγραμμα περιήγησης στέλνει τις προτιμήσεις κρυπτογράφησης, επειδή αυτό και ο εξυπηρέτης διαπραγματεύονται τον αλγόριθμο συμμετρικού κλειδιού που πρόκειτα να χρησιμοποιήσουν.
2. Ο εξυπηρέτης στέλνει στο πρόγραμμα περιήγησης τον αριθμό έκδοσης SSL, τις προτιμήσεις κρυπτογράφησης και το πιστοποιητικό του. Θυμηθείτε ότι το πιστοποιητικό περιλαμβάνει το δημόσιο κλειδί RSA του εξυπηρέτη και πιστοποιείται από κάποια: Αυτό σημαίνει ότι το πιστοποιητικό έχει υπογραφεί με το ιδιωτικό κλειδί της CA.
3. Το πρόγραμμα περιήγησης έχει μια λίστα έμπιστων CA και ένα δημόσιο κλειδί κάθε CA μέσα στη λίστα. Όταν το πρόγραμμα περιήγησης δεχθεί το πιστοποιητικό.



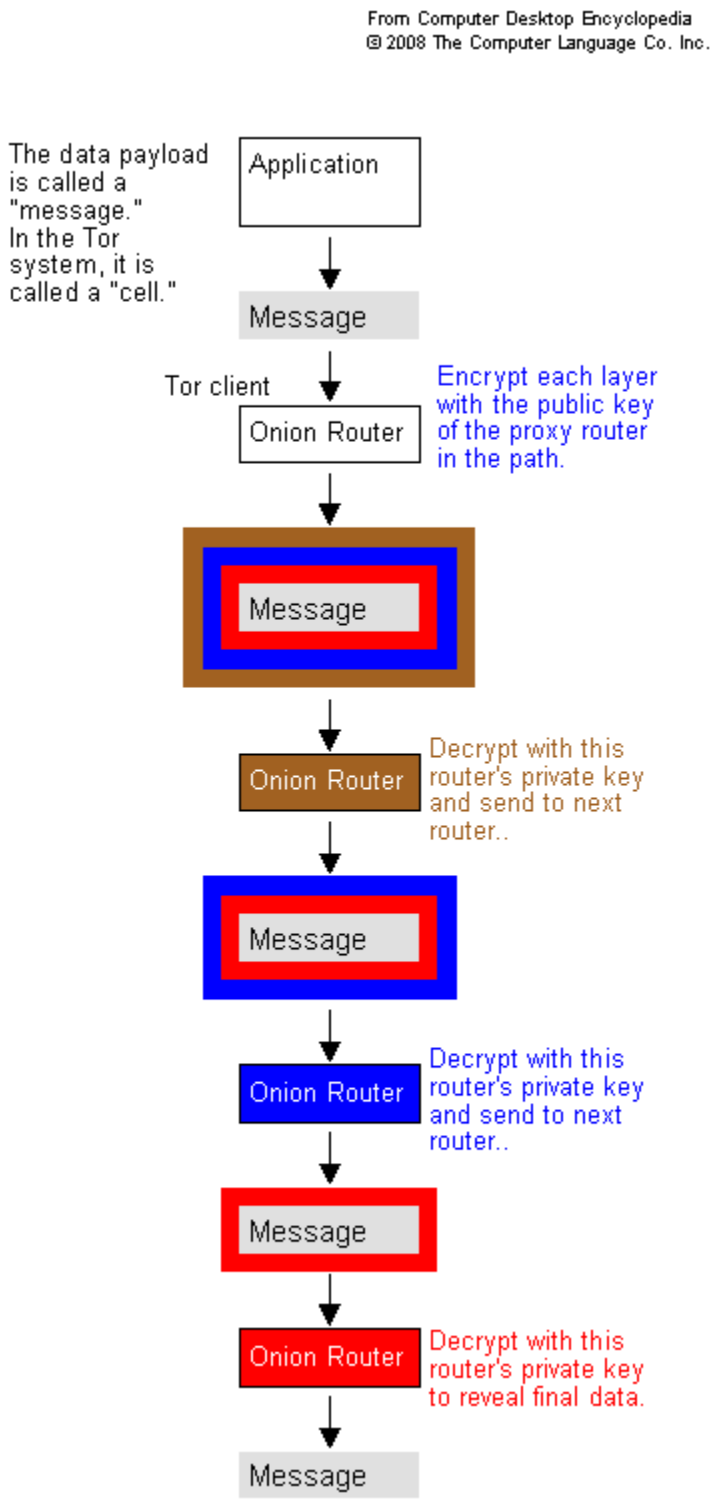
Εικόνα 3.2: Επισκόπηση υψηλού επιπέδου της φάσης χειραψίας του SSL

4. από τον εξυπηρέτη, ελέγχει για να δει αν η CA βρίσκεται μέσα στη λίστα. Αν όχι, η χρήστης προειδοποιείται για το πρόβλημα και πληροφορείται ότι δεν μπορεί να καθορισθεί μια κρυπτογραφημένη και πιστοποιημένη σύνδεση. Αν η CA βρίσκεται στην λίστα, το πρόγραμμα περιήγησης χρησιμοποιεί το δημόσιο κλειδί της CA για να επαληθεύσει το πιστοποιητικό και να πάρει το δημόσιο κλειδί του εξυπηρέτη

Το δίκτυο του Onion Routing αποτελείται από τους Onion Routers και τους Onion Proxies. Οι Onion Routers συνδέονται στο δημόσιο δίκτυο αλλά έχουν αποκαταστήσει μία και μοναδική σύνδεση με καθέναν από τους γειτονικούς Onion Routers. Οι Onion Proxies μεταφράζουν τα δεδομένα σε μορφή ανεξάρτητη της εκάστοτε εφαρμογής, η οποία θα γίνεται αποδεκτή και κατανοητή από το δίκτυο των Onion Routers. Ο Onion Proxy στην πλευρά του ιδρυτή επιλέγει ένα μονοπάτι μέχρι τον παραλήπτη. Για κάθε Router στο μονοπάτι, δημιουργείται ένα στρώμα με ένα πακέτο, που περιλαμβάνει την IP του επόμενου Router και τις πληροφορίες για τη δημιουργία του κλειδιού κρυπτο-γράφησης για την επικοινωνία με τον επόμενο. Όπως προωθείται το πακέτο στο μονοπάτι των Onion Routers, τα επίπεδα ξετυλίγονται και το Onion συμπληρώνεται (padding) για να μην μπορεί να αποκαλυφθεί το συνολικό μήκος. Όλες οι αιτήσεις από τον ιδρυτή αποστέλλονται από το ίδιο μονοπάτι των Onion routers. Οι απαντήσεις αποστέλλονται από τον τελευταίο Onion Router μέσω του ίδιου μονοπατιού. Μόλις τερματιστεί η σύνδεση, οι Onion Router χάνουν όλη την πληροφορία σχετικά με τη σύνδεση.



Εικόνα 3.3: Onion Routing

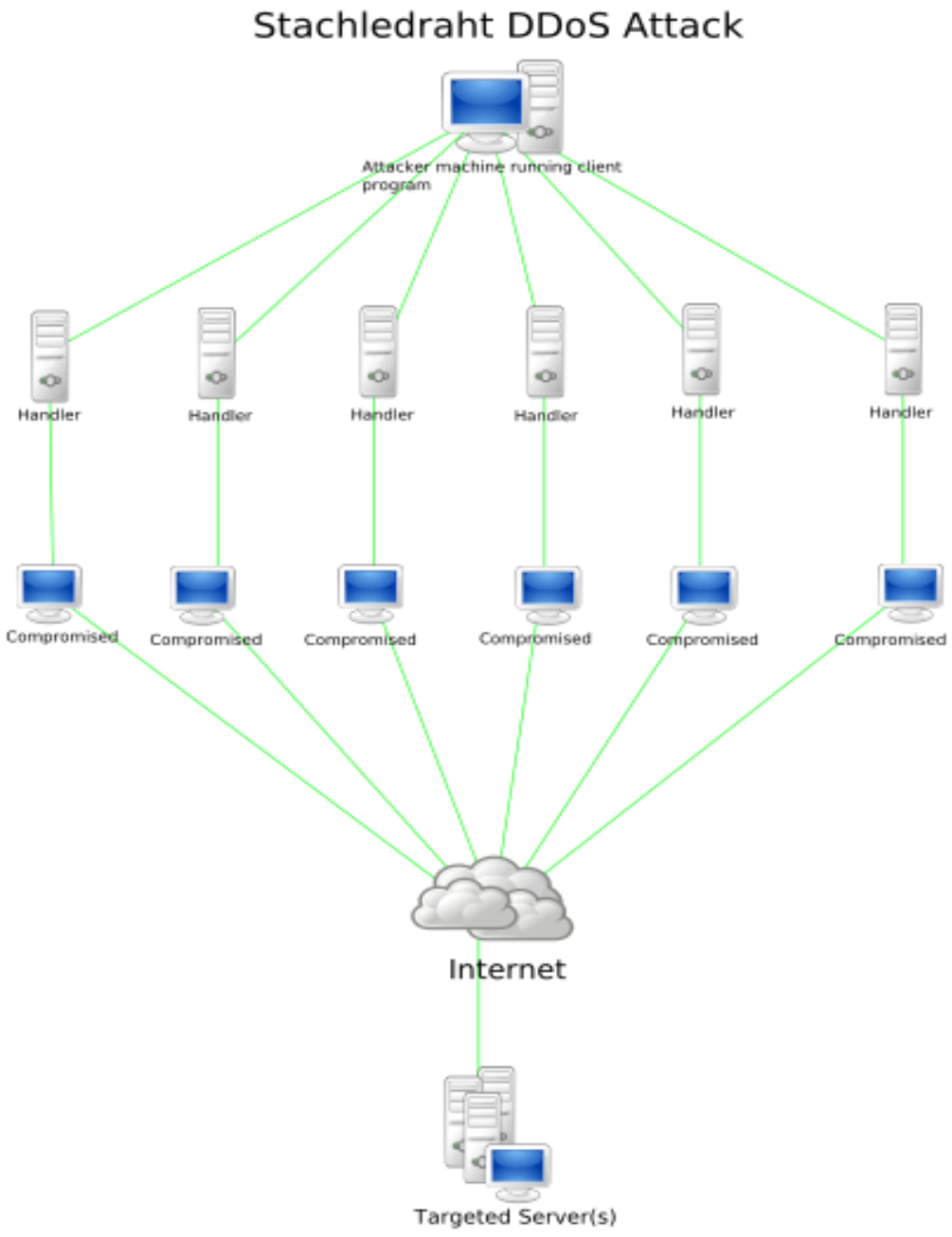


Εικόνα 3.4: Onion Routing

Το Freenet σχεδιάστηκε από τον Ian Clarke και έχει ως στόχο να παρέχει την ελευθερία της έκφρασης μέσω peer-to-peer δίκτυα διατηρώντας ισχυρή προστασία της ανωνυμίας. Το Freenet είναι ελεύθερο λογισμικό και συμβάλλει ώστε οι χρήστες να δημοσιεύουν ανώνυμα δεδομένα σε χώρους αποθήκευσης και να ανακτούν από αυτούς διάφορα είδη πληροφοριών. Το Freenet βρίσκεται υπό συνεχή ανάπτυξη από το 2000.

Μια *denial-of-service attack (επίθεση DoS)* ή αλλιώς μια *distributed denial-of-service attack (DDoS επίθεση)* αποτελεί ένα τρόπο ώστε κάποιος υπολογιστής να γίνει μη διαθέσιμος στους χρήστες που τον χρησιμοποιούν. Αν και τα μέσα για τη διεξαγωγή, τα κίνητρα και οι στόχοι μιας επίθεσης DoS μπορεί να ποικίλλουν, αποτελούνται συνήθως από τις συντονισμένες προσπάθειες ενός ατόμου ή ατόμων να εμποδίσουν μια ιστοσελίδα στο Διαδίκτυο ή μια υπηρεσία να λειτουργήσει αποτελεσματικά, προσωρινά ή επ' αόριστον. Στόχοι των επιθέσεων DoS συνήθως είναι οι web τοποθεσίες ή οι υπηρεσίες που φιλοξενούνται σε διακομιστές web με υψηλή κίνηση, όπως τράπεζες, σελίδες για πληρωμή με πιστωτική κάρτα ακόμη και nameservers.

Μια κοινή μέθοδος επίθεσης είναι η πρόκληση κορεσμού στου στόχο (θύμα) από εξωτερικές ανάγκες επικοινωνίας, τέτοιες ώστε αυτός να μην μπορεί να ανταποκριθεί στην κανονική κυκλοφορία ή να ανταποκρίνεται τόσο αργά ώστε να καταστεί μη διαθέσιμος. Σε γενικές γραμμές, οι επιθέσεις DoS υλοποιούνται είτε αναγκάζοντας το στοχοθετημένο υπολογιστή (ες) σε επανεκκίνηση έτσι ώστε να μην μπορεί πλέον να παρέχει υπηρεσίες σε αυτούς που προορίζονται είτε παρεμποδίζοντας τα μέσα επικοινωνίας μεταξύ του θύματος και των χρηστών ώστε να μην μπορούν αυτοί να επικοινωνήσουν επαρκώς.



Εικόνα 3.5: DDOS attack

Αισθητήρες : Ένα σημαντικό πρόβλημα των αισθητήρων είναι η ιδιωτικότητα. Αυτό προκαλείται κατά κύριο λόγο από άτομα που δεν γνωρίζουν ότι ανιχνεύονται. Ο Marc Langheinric στην εργασία του «Privacy by Design - Principles of Privacy-aware Ubiquitous Systems. In Proceedings of Ubicomp. Pp. 273–291. Oct. 2001» καθορίζει διάφορες κατευθυντήριες γραμμές για το χειρισμό αυτού του προβλήματος στη φάση του σχεδιασμού. Πρώτον οι χρήστες πρέπει να γνωρίζουν αν έχουν ανιχνευτεί «ειδοποίηση», δεύτερον πρέπει να είναι σε θέση να επιλέξουν πότε θα ανιχνευθούν και αν το θελήσουν να το διακόψουν και τρίτον θα πρέπει να μπορούν να διατηρήσουν την ανωνυμία τους «ανωνυμία και ψευδωνυμία».

Αποθηκευτικός χώρος: Ενώ υπάρχουν ειδικοί αποθηκευτικοί χώροι για την ακεραιότητα και την εμπιστευτικότητα, δυστυχώς συχνά αυτοί είναι απασχολημένοι . Συχνά, πάρα πολλές πληροφορίες οι οποίες δεν είναι αναγκαίες αποθηκεύονται, με αποτέλεσμα να προκαλείται υπερφόρτωση στο ίδιο το σύστημα. Στους χώρους αποθήκευσης θα πρέπει να δρουν μηχανισμοί ανωνυμοποίησης και ψευδωνυμίας ώστε να διασφαλίζεται ότι τα δεδομένα που περιέχουν ευαίσθητες πληροφορίες για την προστασία της ιδιωτικότητας δε θα είναι προσβάσιμα σε μη εξουσιοδοτημένους χρήστες.

Συσκευές: Η ακεραιότητα των συσκευών που είναι κάτι «παραδεκτό» αποτελεί ένα άλυτο ζήτημα. Η έρευνα στο Trusted Platform Computing αποσκοπεί στην προστασία της ακεραιότητας των συσκευών, παρόλο που το TPM «Trusted Platform Module» έχει ήδη ενσωματωθεί σε φορητούς υπολογιστές, δεν υπάρχουν πλήρως συμβατά λειτουργικά συστήματα με το TPM.

Επεξεργασία : Πρέπει να υπάρχουν μηχανισμοί για την επεξεργασία δεδομένων οι οποίοι θα διαβεβαιώνουν ότι οι ευαίσθητες επεξεργασμένες πληροφορίες δε θα διαβιβάζονται στις μη ασφαλείς συσκευές και αποθηκευτικούς χώρους. Πρέπει να καθοριστούν τυποποιημένοι κανονισμοί που θα διέπουν του μηχανισμούς αυτούς ώστε να διασφαλίζεται η ιδιωτικότητα.

Εντοπισμός, παρακολούθηση, καθώς και ταυτοποίηση: Για τον εντοπισμό, την παρακολούθηση, καθώς και την ταυτοποίηση ισχύουν οι ίδιες απαιτήσεις όπως και στα προηγούμενα, δηλαδή προστασία της ιδιωτικότητας των χρηστών που εντοπίστηκαν, ταυτοποιήθηκαν και παρακολουθήθηκαν. Σε όλες τις περιπτώσεις, ο χρήστης πρέπει να είναι σε θέση να ενημερωθεί για όλη την διαδικασία και να μπορεί να την διακόψει. Αυτό έχει οριστεί όπως έχει αναφερθεί και παραπάνω από τον Marc Langheinrich ως «επιλογή και συναίνεση».

Συνοψίζοντας, είναι φανερό ότι υπάρχει ανάγκη για περαιτέρω ανάπτυξη όσον αφορά τη διαθεσιμότητα της επικοινωνίας η οποία περιορίζεται λόγω του DDoS και όσον αφορά τη βελτίωση των υπηρεσιών που παρέχει το IP. Επιπλέον, βελτίωση χρειάζονται τα spyware ή rootkits ώστε να διασφαλίζεται η ακεραιότητα των συσκευών δηλαδή να βεβαιώνεται ότι αυτές είναι απαλλαγμένες από κακόβουλο λογισμικό. Τέλος, σχεδόν σε όλους τους τομείς λείπει η εφαρμογή μηχανισμών για την προστασία της ιδιωτικότητας στο Διαδίκτυο των πραγμάτων.

Οι κατευθυντήριες γραμμές που αναφέρθηκαν από τον Langheinrich είναι πολύ χρήσιμες για τους σχεδιαστές του συστήματος, αλλά επίσης πρέπει να ισχύουν τα εξής: πρώτον οι κανονισμοί να εξασφαλίζουν ότι τα συστήματα ακολουθούν αυτές τις κατευθυντήριες γραμμές και δεύτερον να αναπτυχθούν μηχανισμοί μέσω των οποίων οι ίδιοι οι χρήστες να έχουν τη δυνατότητα να ενεργούν υπέρ της προστασίας της ιδιωτικότητας τους, αντί να βασίζονται μόνο στα συστήματα του Διαδικτύου των πραγμάτων.

Topic \ Property	Integrity	Authenticity	Confidentiality	Privacy	Availability
Communication	2	2	3		1
Sensors	2			1	
Actuators					
Storage	3		3	1	
Devices	1				
Processing				1	
Localization/Tracking			3	1	2
Identification			3	1	2

Πίνακας 3.2: Κατάσταση της έρευνας για εξαιρετικά ευαίσθητες ιδιότητες

3.3 Σημαντικά στοιχεία του Διαδικτύου των πραγμάτων

Παρακάτω θα αναφερθεί το GSN «Global Sensor Networks» Middleware και θα αναλυθεί σε βάθος η τεχνολογία RFID. Εκτός από την τεχνολογική αναδρομή στο RFID, θα αναπτυχθούν ζητήματα ασφάλειας τόσο για το RFID όσο και για το GSN.

3.3.1 Καθολικό ενδιάμεσο λογισμικό μεταξύ δικτύου- αισθητήρων

Μεγάλη πρόοδος έχει πραγματοποιηθεί τα τελευταία χρόνια σχετικά με τις αρχιτεκτονικές ενδιάμεσου λογισμικού που συνδέουν του αισθητήρες και τα δίκτυα αισθητήρων στην παγκόσμια υποδομή του Διαδικτύου. Κατά την ανάπτυξη του 'middleware' υλικολογισμικού προκύπτουν προβλήματα ασφάλειας που οφείλονται ως επί το πλείστον από την ανάγκη σύνδεσης πολλαπλών ετερογενών δικτύων μέσω του Διαδικτύου « θέμα επικοινωνίας όπως αναφέρθηκε παραπάνω στην κατηγοριοποίηση ». Ωστόσο, τα νέα θέματα ασφάλειας και προστασίας της ιδιωτικότητας που προκύπτουν κατά την ενσωμάτωση του φυσικού κόσμου στον ψηφιακό του Διαδικτύου των πραγμάτων πρέπει να μελετηθούν περεταίρω.

IrisNet: Η IrisNet Αρχιτεκτονική χρησιμοποιεί Webcams ως αισθητήρες. Η ασφάλεια βασίζεται στην παραδοχή ότι ολόκληρο το παγκόσμιο δίκτυο αισθητήρων διοικείται από μια ενιαία, αξιόπιστη καθολική αρχή. Ως εκ τούτου, μπορεί να εξασφαλιστεί με την χρήση μηχανισμών ασφάλειας επικοινωνίας. Έτσι για να αντιμετωπίσει τις ανησυχίες της ιδιωτικότητας η IrisNet στο βίντεο υλοποιεί παραμόρφωση στα πρόσωπα. Ένα σενάριο χρήσης του IrisNet είναι η παρακολούθηση των χώρων δωρεάν στάθμευσης, που αποτελεί ένα καλό παράδειγμα στο οποίο η δημιουργία ανωνυμίας δεν περιορίζει απαραίτητα τα στοιχεία της λειτουργικότητας.

HiFi : Η HiFi καθορίζει μια ιεραρχική δομή επίπεδων. Δεδομένα διαβιβάζονται από το χαμηλότερο επίπεδο «τα πραγματικά στοιχεία» - αισθητήρες, όπως RFID ή δίκτυα αισθητήρων – μέσω των ενδιάμεσων επιπέδων προς ανώτερα. Το κάθε επίπεδο εκτελεί ειδικά καθήκοντα. Το χαμηλότερο επίπεδο καθαρίζει τα δεδομένα και προωθεί μόνο τα δεδομένα που ανταποκρίνονται σε ένα συγκεκριμένο πρότυπο ποιότητας (όπως η ισχύς του σήματος RFID). Τα υψηλότερα επίπεδα επικυρώνουν αυτά δεδομένα. Η προστασία της ιδιωτικότητας και ο έλεγχος πρόσβασης υλοποιούνται με την χρήση SQL για τον προσδιορισμό της πολιτικής αδειών.

ETRI Ubiquitous Sensor Network.: Μερικές απαιτήσεις ασφαλείας προκύπτουν είτε από τις απειλές προς διάφορες εφαρμογές από αναρμόδιους χρήστες που αποκτούν στοιχεία του αισθητήρα, είτε από αιτήσεις που προκαλούν την αναδιαμόρφωση των κόμβων του δικτύου των αισθητήρων διαταράσσοντας τη λειτουργία του αισθητήρα, είτε από την επίδοση Denial-of-Service επιθέσεων μέσω μεγάλου αριθμού αιτήσεων στον αισθητήρα. Επίσης υπάρχουν απειλές από κατεστραμμένα δίκτυα αισθητήρων που παρέχουν μη έγκυρα στοιχεία και στρεβλώνουν τα σωστά αποτελέσματα, προκύπτουν ακόμη απειλές και από εξωτερικά αντικείμενα όπως είναι η συνακρόαση. Τέλος, οι replay επιθέσεις και οι man-in-the-middle επιθέσεις είναι εφικτές όταν ο εισβολέας βρίσκεται μεταξύ της εφαρμογής και ενός στρώματος του υλικολοσμικού συστήματος.

3.3.2 RFID

Μια ετικέτα RFID είναι ένα μικρό ολοκληρωμένο κύκλωμα με ένα μοναδικό αναγνωριστικό που προσδιορίζει το αντικείμενο στο οποίο βρίσκεται - δεν είναι μόνο για ομάδα στοιχείων όπως ισχύει με τα barcodes. Οι RFID συσκευές ανάγνωσης μπορούν να ρωτούν τις ετικέτες και να λαμβάνουν το μοναδικό αναγνωριστικό στοιχείο, το οποίο στη συνέχεια καταχωρείται σε μια βάση δεδομένων που μπορεί να περιέχει και πρόσθετες πληροφορίες σχετικά με το θέμα. Συχνά, το αναγνωριστικό στοιχείο είναι δομημένο σε μια ιεραρχική μορφή που περιέχει πληροφορίες για τον κατασκευαστή, την τάξη της ομάδας που ανήκει το αντικείμενο και το ID του αντικειμένου. Η αγορά RFID αυξάνεται με ταχείς ρυθμούς με 1,02 δισ. ετικέτες να πωλούνται μόνο το 2006, και 5,20 δολάρια δισ. το 2008. Οι αριθμοί αυτοί για τις ετικέτες RFID, που παρουσιάζουν μια σημαντική τεχνολογία του Διαδικτύου των πραγμάτων προβλέπεται να αυξηθούν. Οι ετικέτες RFID στο άμεσο μέλλον θα ενσωματώνουν προηγμένη ανίχνευση και δυνατότητες επικοινωνίας, και επίσης το τμήμα του αισθητήρα θα είναι στην ίδια την ετικέτα RFID.
Το ότι οι ετικέτες RFID προσδιορίζουν μοναδικά τα αντικείμενα, προκαλούν ζητήματα προστασίας της ιδιωτικότητας. Αυτό προκύπτει από το ότι η παρακολούθηση των αντικειμένων συνεπάγεται και παρακολούθηση του προσώπου που τα κουβαλάει, τα φοράει ή που του έχουν εμφυτευθεί. Συνεπώς, πρέπει να προταθούν διαφορετικές τεχνικές κρυπτογράφησης ώστε να επιτραπεί μόνο σε πιστοποιημένα μέρη να αποκαλύψουν την πραγματική ταυτότητα της ετικέτας. Καθώς υπάρχουν διαφορετικές ετικέτες RFID (π.χ. ενεργητική, παθητική, ημι-ενεργή) με διαφορετικές υπολογιστικές δυνατότητες, υπάρχουν και διάφοροι μηχανισμοί για την ασφάλεια και την προστασία της ιδιωτικότητας. Η ασφάλεια και η ιδιωτικότητα σε συστήματα RFID έχουν οριστεί ως εξής :

• Ασφάλεια είναι η ικανότητα του συστήματος RFID να διατηρεί τις πληροφορίες που μεταδίδονται μεταξύ ετικέτας και συσκευής ανάγνωσης από μη ασφαλείς αποδέκτες.

• Ιδιωτικότητα στο RFID είναι η ικανότητα του συστήματος να κρατήσει την έννοια των πληροφοριών που διαβιβάζονται μεταξύ της ετικέτας και του αναγνώστη από μη ασφαλή-αποδέκτες.

Οι ετικέτες RFID έχουν την ικανότητα να εκτελούν βασικές λειτουργίες όπως XOR, hashing, υπολογισμό PRFs «Pseudorandom Functions ψευδοτυχαίων συναρτήσεων» και να συμμετέχουν στα πρωτόκολλα 'πρόκληση-απάντηση'. Υπάρχουν αρκετά πρωτόκολλα που υπακούν στο πρωτόκολλο 'πρόκληση-απάντηση' και τα οποία έχουν προταθεί για την επικοινωνία μεταξύ RFID tag και RFID reader. Μία συσκευή ανάγνωσης RFID έχει πρόσβαση σε ένα σύστημα βάσης δεδομένων που περιλαμβάνει όλα τα αναγνωριστικά

tag καθώς και πρόσθετες πληροφορίες, ανάλογα με το πρωτόκολλο. Οι φυσικοί μηχανισμοί για τη διατήρηση απόρρητου και της ιδιωτικότητας στα RFID αναφέρονται λεπτομερώς στην ενότητα 3.3.2.1 και τα RFID πρωτόκολλα κρυπτογράφησης στην ενότητα 3.3.2.2.

3.3.2.1 Φυσικοί μηχανισμοί

Kill Codes : Το Kill Codes απενεργοποιεί μόνιμα την ετικέτα και ως εκ τούτου εμποδίζει την ανάγνωση και την παρακολούθηση. Αυτό είναι ιδιαίτερα χρήσιμο για τα αντικείμενα που χρειάζονται παρακολούθηση στην αλυσίδα εφοδιασμού και όχι μετά την αγορά τους από τον πελάτη.

Faraday Cage : Με το να τοποθετηθεί μία RFID ετικέτα σε ένα κλουβί Faraday καθίσταται αδύνατο το διάβασμα της ετικέτας. Επιτρέπεται όμως στον χρήστη να αποφασίσει αν θα είναι δυνατή ή όχι η ανάγνωση της . Ένα κλουβί Faraday καθιστά αδύνατη την απανταχού κάλυψη.

Blocker Tag: Το Blocker Tag εκτελεί παρεμβολές προκαλώντας σύγχυση στους μη εξουσιοδοτημένους αναγνώστες οι οποίοι βλέπουν ότι υπάρχει μεγάλος αριθμός διαφορετικών ετικετών RFID. Μια ετικέτα blocker τοποθετείται συγχρόνως με την πραγματική ετικέτα RFID, ως εκ τούτου όσο εύκολα μπορεί να εφαρμοστεί το ίδιο εύκολα μπορεί και να απομακρυνθεί.

3.3.2.2 Πρωτόκολλα κρυπτογράφησης

Randomized Hash-Lock Protocol : Μια βάση δεδομένων περιέχει τις ταυτότητες όλων των ετικετών IDi, το i ανήκει στο {0. . .n}.Η συσκευή ανάγνωσης RFID στέλνει queries ερωτήσεις για να ξεκινήσει το πρωτόκολλο. Η ετικέτα υπολογίζει x = h(IDa|r) χρησιμοποιώντας hash συνάρτηση h(x), το ID του IDa, έναν τυχαίο αριθμό r, και μεταδίδει τα {x, r}στο διακομιστή.

Καθώς ο διακομιστής γνωρίζει τις ταυτότητες όλων των κλειδιών IDi, μπορεί και υπολογίζει το y = h(IDi|r) για κάθε i και συγκρίνει αν x =? y. Αν τα x και y ταιριάζουν τότε βρέθηκε το σωστό ID του IDa. Δεδομένου ότι το πρωτόκολλο τρέχει σε O(n) πολυπλοκότητα μπορεί να θέσει σε βαρύ φορτίο επεξεργασίας τον διακομιστή.

Hash Chain based Protocols : Το YA-TRAP πρωτόκολλο απαιτεί χρονικό συγχρονισμό μεταξύ του διακομιστή και των συσκευών ανάγνωσης, οι ετικέτες δεν απαιτείται να

έχουν ρολόγια. Στην έναρξη σε κάθε ετικέτα i αποδίδεται μια τριπλέτα (Ki, T_0, Tmax), Ki είναι για την ετικέτα ένα ειδικό-αναγνωριστικό που χρησιμοποιείται ως ετικέτα ταυτότητας και κρυπτογραφικό κλειδί, T_0 είναι μία αρχική χρονική στιγμή, π.χ. η στιγμή της κατασκευής, και Tmax είναι η μέγιστη τιμή του χρόνου που αντιστοιχεί στη μέγιστη διάρκεια ζωής της ετικέτας. Σε κάθε χρονική στιγμή Tr με το r να ανήκει στο {0. ..max } προκύπτει ένα hashtable HASHTABLEr, το οποίο δημιουργήθηκε στη βάση δεδομένων του διακομιστή. Για κάθε ετικέτα i οι τιμές των HMACKi(Tr) εισάγονται σε πίνακες HASHTABLEr, για παράδειγμα, για κάθε ετικέτα i με το κλειδί Ki, κάθε hashvalue κάθε χρονική στιγμή Tr υπολογίζεται και αποθηκεύεται.
Το πρωτόκολλο συνεχίζει ως εξής: ο αναγνώστης στέλνει το τρέχον Tr στην ετικέτα. Η ετικέτα θυμάται την τρέχουσα χρονική στιγμή ως Tt = Tr, υπολογίζει το Hr=HMACKi(Tt) και στέλνει πίσω το Hr στον αναγνώστη. Ο server γνωρίζει τώρα το Tr και το Hr της συγκεκριμένη χρονικής στιγμής και την hashvalue για την ετικέτα την ίδια χρονική στιγμή. Εξετάζει το hashtable HASHTABLEr που περιέχει όλα τα hashes για την τρέχουσα χρονική στιγμή Tr. Ρωτώντας το Hr της HASHTABLEr ο διακομιστής μπορεί να ανακτήσει το Ki το οποίο αντιστοιχεί στο αναγνωριστικό της ετικέτας i.

3.4 Έρευνα από άλλους τομείς

Το σημερινό Διαδίκτυο έχει αποτύχει με πολλούς τρόπους στην παροχή επαρκούς ασφάλειας και προστασίας. Στην ενότητα αυτή παρουσιάζονται τρία αποτελέσματα από έρευνα που έγινε σχετικά με το Διαδίκτυο των πραγμάτων.

3.4.1 Υπευθυνότητα πληροφοριών

Από την πρώτη στιγμή που δημιουργήθηκαν τα συστήματα πληροφοριών και το Web έχει τον τρόπο του να φθάσει σε εκατομμύρια ανθρώπους, το δίλημμα της ιδιωτικότητας στον ψηφιακό κόσμο έχει ξεκινήσει. Χρησιμοποιώντας τις ίδιες τεχνικές για προστασία της ιδιωτικότητας των ανθρώπων - και ίσως της ιδιωτικότητας των «πραγμάτων» στο Διαδίκτυο των πραγμάτων - θα παραχθούν ίσως στο τέλος τα ίδια αποτελέσματα δηλαδή μια ανεξέλεγκτη ροή πληροφοριών και μία μη προστατευόμενη ιδιωτικότητα. Οι τρέχουσες βάσεις δεδομένων ευρείας κλίμακας αποθήκευσης δεδομένων προσωπικού χαρακτήρα θα γεμίσουν ακόμη περισσότερο κατά τις ημέρες του Διαδικτύου των πραγμάτων. Όπως ο Schneier προειδοποιεί στη εργασία του [B. Schneier. The Future of Privacy. Presentation at RSA Conference Europe, Oct.2008.] δεν υπάρχει τρόπος να ελεγχεί η συλλογή και η χρήση των προσωπικών δεδομένων. Ακόμη χειρότερα, πολλά

δεδομένα συνδέονται με πολλά προσωπικά στοιχεία κάτι που στις περισσότερες των περιπτώσεων δεν είναι απαραίτητο. Όλα αυτά τα δεδομένα συλλέγονται και αποθηκεύονται, αλλά δεν διαγράφονται, το οποίο αναπόφευκτα θα οδηγήσει σε δεδομένα σκουπίδια .Ο Weitzner στην εργασία του (D. J. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler, G. J. Sussman.Information Accountability. Communications of the ACM 51(6):82–87, June2008.) παρουσιάζει μια νέα ιδέα για την προστασία της ιδιωτικότητας που την ονομάζει υπευθυνότητα πληροφοριών «Information Accountability». Η βασική αρχή του Information Accountability δεν είναι να προσπαθήσει να αποτρέψει τη διαρροή των δεδομένων αλλά να είναι σε θέση να ελέγχει τη χρήση των δεδομένων. Να είναι σε θέση να καλέσει τα πρόσωπα να απολογηθούν για την κακή χρήση των δεδομένων, κάτι που δεν μπορεί να γίνει με την τρέχουσα έννοια της προστασίας της ιδιωτικότητας η οποία στηρίζεται στο απόρρητο των πληροφοριών μυστικά.

3.4.2 Κρυπτογραφημένα αναγνωριστικά

Τα κρυπτογραφημένα αναγνωριστικά χρησιμοποιούνται σε πολλά νεότερα πρωτόκολλα δικτύωσης για να αποδείξουν την κυριότητα μιας διεύθυνσης. Το IPv6 Secure Neighbor Discovery (Αποστολή), π.χ., χρησιμοποιεί Cryptographically Generated Addresses ώστε να αποφεύγεται το address spoofing, κατά το δυνατόν περισσότερο στο Address Resolution Protocol (ARP) που χρησιμοποιείται σε τοπικά δίκτυα. Επιπλέον, λόγω του μεγάλου μεγέθους των Overlay identifiers, η χρήση των κρυπτογραφημένων αναγνωριστικών μπορεί να χρησιμεύσει στην απόδειξη της κυριότητας των αναγνωριστικών αυτών. Το Host Identity Protocol (HIP) π.χ., βασίζει την ασφάλειά του σε μεγάλο βαθμό στα κρυπτογραφημένα αναγνωριστικά, τα οποία λειτουργούν ως RFID ID, και έτσι οι ετικέτες μπορούν να αποδείξουν ότι ένα ID τους ανήκει. Με τις σημερινές λύσεις RFID κυρίως να έχουν αναπτυχθεί σε αυτοτελή συστήματα, έχει προκύψει η ανάγκη για απόδειξη της ιδιοκτησίας. Έχοντας δημόσιες βάσεις δεδομένων στις οποίες αποθηκεύονται όλες οι πληροφορίες σχετικά με τις ετικέτες οι οποίες είναι δημοσίως προσπελάσιμες, εμφανίζεται ο κίνδυνος πλαστογράφησης του ID της ετικέτας. Αυτό μπορεί να συμβεί γιατί καθώς συγκεντρώνονται πληροφορίες για τις ετικέτες από τη βάση δεδομένων στη συνέχεια μπορεί να δημιουργηθεί μια αντιγραμμένη-πλαστή ετικέτα η οποία θα λειτουργεί ως κάποια άλλη ετικέτα και θα εξαπατά τις υπόλοιπες. Σε αυτή την περίπτωση τα κρυπτογραφημένα αναγνωριστικά μπορούν να βοηθήσουν στον εντοπισμό των ετικετών που αντιγράφηκαν τα ID τους. Αυτό μπορεί να χρησιμοποιηθεί σε κόμβους αισθητήρων που λαμβάνουν μέρος σε ένα δίκτυο όπου τα αναγνωριστικά είναι αρκετά για να χρησιμοποιηθεί η μεθόδους αυτή. Οι κόμβοι θα ελέγχουν την κυριότητα του αναγνωριστικού, έτσι θα επιτυγχάνεται ο εντοπισμός των αντιγραμμένων

αισθητήρων οι οποίοι θα αναγνωρίζονταν σαν άλλες ετικέτες και πιθανόν να έδιναν εσφαλμένα δεδομένα.
Τα κρυπτογραφημένα αναγνωριστικά βασίζονται σε ασύμμετρου-κλειδιού κρυπτογράφηση και κατά συνέπεια έχουν μεγάλο πλεονέκτημα σε σύγκριση με τη συμμετρικού-κλειδιού κρυπτογράφηση όσον αφορά την υπολογιστική ισχύ και το μέγεθος του κλειδιού. Έχει αποδειχθεί ότι μπορεί να γίνει χρήση κρυπτογραφημένων αναγνωριστικών σε κόμβους αισθητήρων αφού αυτοί οι κόμβοι είναι σε θέση να εκτελέσουν μια ασύμμετρου-κλειδιού κρυπτογράφηση. Οι ετικέτες RFID δεν είναι μακριά από το να εκτελούν οι ίδιες ασύμμετρου-κλειδιού κρυπτογράφηση. Ως εκ τούτου, η χρήση RFID ετικετών ID σε συνδυασμό με κρυπτογραφημένα αναγνωριστικά θα έχει ενδιαφέροντα αποτελέσματα.

3.4.3 Εξαγωγή κλειδιού από τα χαρακτηριστικά του ασύρματου καναλιού

Όσο ένα μεγάλο μέρος της επικοινωνίας στο Διαδίκτυο των πραγμάτων θα πραγματοποιείται μέσω ασύρματων καναλιών τα οποία είναι ευαίσθητα στην συνακρόαση τόσο η εγκατάσταση ενός κλειδιού καθίσταται αναγκαία για την παροχή εμπιστευτικών επικοινωνιών. Η εργασία των Mathur et al. [S. Mathur, W. Trappe, N. Mandayam, C. Ye, A. Reznik. Radio-telepathy: Extractinga Secret Key from an Unauthenticated Wireless Channel. In Proceedings of MobiCom. Pp. 128–139. Sept. 2008.] προβλέπει τη δημιουργία ενός κοινού κρυπτογραφικού κλειδιού για δύο χρήστες, με βάση τα χαρακτηριστικά του ασύρματου καναλιού που χρησιμοποιούν. Καθώς τα χαρακτηριστικά του ασύρματου καναλιού στο πλαίσιο επικοινωνίας μεταξύ των A και B είναι τα ίδια μόνο για αυτούς (A και B), είναι δυνατό να χρησιμοποιηθούν για την εξαγωγή bits μέσω στοχαστικών διεργασιών. Αυτά τα bits μπορούν στη συνέχεια να χρησιμοποιηθούν για να σχηματιστεί ένα συμμετρικό κρυπτογραφικό κλειδί. Έτσι, οι A και B ανεξάρτητα μπορούν να υπολογίσουν το ίδιο συμμετρικό κλειδί για την επικοινωνία τους μόνο με το ότι ο A συνομιλεί με τον B και ο B συνομιλεί με τον A.
Αυτό το σύστημα φαίνεται πολλά υποσχόμενο, όταν πρόκειται για ασύρματη επικοινωνία στο Διαδίκτυο των πραγμάτων, πρώτον επειδή βασίζεται μόνο στη συμμετρικού-κλειδιού κρυπτογράφηση και δεύτερον επειδή δεν απαιτείται καθορισμός κλειδιών από την κατασκευή τους ή τη διανομή τους.

3.5 Συμπεράσματα

Η σταδιακή ανάπτυξη των τεχνολογιών που θα απαρτίζουν το Διαδίκτυο των πραγμάτων δεν θα πρέπει να αποτύχει σε αυτά διότι ήδη το Διαδίκτυο έχει αποτύχει στο να παρέχει επαρκή ασφάλεια και επαρκείς μηχανισμούς προστασίας της ιδιωτικότητας. Για παράδειγμα η βιαστική εισαγωγή των ηλεκτρονικών διαβατηρίων λόγω της πίεσης από την πολιτεία είχε σαν αποτέλεσμα την ανάπτυξη αυτών με ανεπαρκείς μηχανισμούς προστασίας της ιδιωτικότητας. Θα πρέπει να είναι βέβαιο ότι επαρκής ασφάλεια και προστασία της ιδιωτικότητας θα είναι διαθέσιμα πριν αυτή η τεχνολογία γίνει μέρος της καθημερινότητας.

Σε αυτό το κεφάλαιο, παρουσιάστηκε μια κατηγοριοποίηση των θεμάτων και των τεχνολογιών του Διαδικτύου των πραγμάτων και επισημάνθηκε η ευαισθησία και η κατάσταση στον τομέα της ασφάλειας και της ιδιωτικότητας. Σε αυτόν τον τομέα αναλύθηκαν ζητήματα για δύο βασικές τεχνολογίες του Διαδικτύου των πραγμάτων, το GSN και το RFID. Τέλος αναφέρθηκε έρευνα από άλλους τομείς της επιστήμης των υπολογιστών καθώς αξίζει να εξεταστεί η χρήση τους στο Διαδίκτυο των πραγμάτων.

3.6 Βιβλιογραφία

http://en.wikipedia.org/wiki

http://www.i-o-t.org/

http://magazine.digitalidworld.com

Christoph P. Mayer. Security and Privacy Challenges in the Internet of Things, Presented at Wissenschaftlichen Konferenz Kommunikation in Verteilten Systemen, 2009

Gérald Santucci. Networked enterprise &Radio Frequency Identification (RFID). Zurich ,2008.

Peter Schaar .Developments of the Privacy Debate in the Internet of Things, Presented at international conference for industry an academia, 2008.

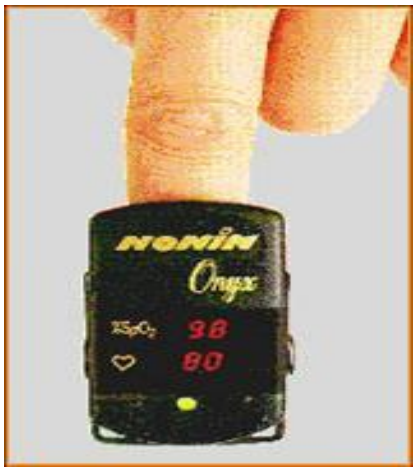
Κεφάλαιο 4ο

Εφαρμογή του Διαδικτύου των πραγμάτων στην Υγειονομική περίθαλψη

4.1 Παρουσίαση

Η ζωή του σύγχρονου ανθρώπου είναι συνυφασμένη με την αλματώδη πρόοδο της τεχνολογίας. Τα τεχνολογικά επιτεύγματα έχουν δώσει λύση σε προβλήματα που στο παρελθόν δυσχέραιναν τη διαβίωσή μας. Τα τελευταία μάλιστα χρόνια παρατηρούμε την άμεση εμπλοκή της τεχνολογίας με την ιατρική επιστήμη.

Η υγεία του ανθρώπου ιδίως όσον αφορά το μείζον ζήτημα της επιμήκυνσης της ζωής αποτελεί ούτως ή άλλως τον σημαντικότερο στόχο κάθε επιστήμης. Κάποιες από τις τεχνολογίες που εφαρμόζονται προσφέροντας σημαντική βοήθεια στο έργο της ιατρικής είναι τα τεχνητά όργανα και μέλη, τεχνητές αρθρώσεις, τεχνητοί καρδιακοί βηματοδότες, αυτοματοποιημένα εργαστήρια κ.α.



Εικόνα 4.1 Παραδείγματα Ιατρικής Τεχνολογίας

Ο στόχος της εποχής μας είναι να αξιοποιηθεί η τεχνολογία με τέτοιο τρόπο ώστε να δημιουργηθεί ένα σύστημα παροχής υπηρεσιών υγείας που να παρέχει βελτίωση της ποιότητας ζωής των ασθενών μέσω της μέγιστης δυνατής παρακολούθησής τους. Τούτο επιτυγχάνεται με την αποφυγή των περιττών μετακινήσεων δηλαδή σπίτι – νοσοκομείο ή εξεταστήριο, ειδικά των ασθενών με περιορισμένη κινητικότητα. Το τελευταίο μάλιστα έχει ως συνέπεια την ελαχιστοποίηση του κόστους τόσο σε χρήμα όσο και σε ταλαιπωρία για τον ασθενή.

Η παροχή υπηρεσιών υγείας περιλαμβάνει ένα πλήθος εμπλεκόμενων ατόμων, φορέων και διακινούμενης πληροφορίας.

- Οι ασθενείς που απαιτούν ποιοτικές υπηρεσίες και μειωμένο κόστος
- Το ιατρικό προσωπικό ήτοι ιατροί και νοσηλευτές
- Διαχειριστές υποδομών υγείας (νοσοκομείων, νοσηλευτηρίων, μέσων μεταφοράς κ.α.)
- Φαρμακευτικές εταιρίες
- Εταιρίες ιατρικού εξοπλισμού
- Εκπαίδευση στελεχών υγείας κλπ.

Τους παραπάνω εμπλεκόμενους φορείς συνδέει η πληροφορία η οποία πρέπει να διακινείται με ταχύτητα, ασφάλεια, ακρίβεια έτσι ώστε να επιτευχθεί η καλύτερη συνεργασία των παραπάνω φορέων και η χρήση της ορθότερης απόφασης.

Σήμερα η βελτίωση στην απόδοση των φορέων της υγείας είναι βασική προτεραιότητα για όλες τις χώρες του ΟΟΣΑ, αντικατοπτρίζοντας τις κοινές πιέσεις για μείωση του κόστους από την μία πλευρά και αύξηση της ικανοποίησης του αποδέκτη των υπηρεσιών υγείας από την άλλη.

Η δυνατότητα επικοινωνίας από παντού, η ικανότητα επεξεργασίας τεράστιων όγκων δεδομένων και η ευελιξία των σύγχρονων τερματικών συσκευών, θα δημιουργήσουν το απαραίτητο περιβάλλον για την ανάπτυξη ολοκληρωμένων, χρήσιμων και σε πολλές περιπτώσεις κρίσιμων εφαρμογών παροχής υπηρεσιών υγείας με ταυτόχρονη μείωση του κόστους.

Τα παραπάνω υλοποιούνται μέσω της εφαρμογής της πληροφορικής στις υπηρεσίες υγείας όπως είναι οι ακόλουθες:

- Συστήματα ψηφιακής επεξεργασίας βιολογικών σημάτων
- Ψηφιακή επεξεργασία ιατρικών εικόνων
- Εμπειρα συστήματα - νευρωνικά δίκτυα
- Αναγνώριση φωνής
- Συστήματα ιατρικής εκπαίδευσης
    - Evidence based medicine
    - Βάσεις δεδομένων
- Ενοποίηση υπηρεσιών υγείας:
    - Νοσοκομειακή Περίθαλψη - Ιατρεία - Κέντρα Υγείας
    - Τηλεϊατρική - Κατ' οίκον νοσηλεία
        - Τηλεδιάγνωση και τηλεσυμβουλευτική
            - Τηλεακτινολογία
            - Τηλεκαρδιολογία
            - Τηλεπαθολογία
            - Τηλεδερματολογία
        - Τηλεχειρουργική
        - Πρόληψη (διατροφή, ασθένειες, εμβόλια, συνθήκες διαβίωσης)
        - Τηλεσυνδιάσκεψη- Τηλεεκπαίδευση
        - Τηλεϊατρική για υποστήριξη διακομιστικών σταθμών
- Τήρηση Ηλεκτρονικού Φακέλου Ασθενούς σε κατανεμημένο περιβάλλον
- Προσπέλαση στοιχείων ασθενούς από διαφορετικά σημεία
- Εξυπηρέτηση επειγόντων περιστατικών - Ηλεκτρονική Κάρτας Υγείας
- Ασφάλεια - Προστασία Απορρήτου

4.2 Τηλεϊατρική & Υπηρεσίες Υγείας

Σε ότι αφορά το θέμα της παρακολούθησης και περίθαλψης των ασθενών, μία ιδιαίτερα ενδιαφέρουσα και συμφέρουσα προοπτική αποτελεί η τηλεϊατρική.

Με τον όρο τηλεϊατρική εννοούμε την χρησιμοποίηση των τεχνολογικών επιτευγμάτων του τομέα των τηλεπικοινωνιών και της ηλεκτρονικής επιστήμης (ένα σύνολο βιοαισθητήρων, συσκευών παρακολούθησης, πρωτοκόλλων μετάδοσης πληροφορίας κ.α.) με σκοπό την από απόσταση παρακολούθηση και περίθαλψη ασθενών και

ανήμπορων ανθρώπων. Η τηλεϊατρική στη δεκαετία του 90 χρησιμοποιήθηκε κυρίως από παροχείς ιατρικών υπηρεσιών έξω από γεωγραφικούς και χρονικούς περιορισμούς για παροχή δεύτερης ιατρικής γνώμης και συμβουλών από εξειδικευμένους γιατρούς. Γενικά η Τηλεϊατρική χρησιμοποιεί τηλεματικές τεχνολογίες, δηλαδή συνδυασμό υπολογιστών κι επικοινωνιών προκειμένου να υποστηριχτούν οι Ιατρικές υπηρεσίες Υγείας και Πρόνοιας.

Εύκολα συνάγει κανείς ότι πρόκειται για υποβοηθούσες τεχνολογίες και δεν πρόκειται για νέα μορφή ιατρικής. Ασφαλώς όμως η υιοθέτηση των τεχνολογιών αυτών έχει ως αποτέλεσμα την ανάγκη διαμορφώσεως νέων προτύπων οργάνωσης και παροχής των ιατρικών υπηρεσιών. Η καθημερινή πρακτική υποδεικνύει ότι δεν έχουν όλοι οι πολίτες ίση πρόσβαση σε υπηρεσίες οπουδήποτε περιεχομένου όπως υγεία, εκπαίδευση, άθληση, πολιτισμός, ενημέρωση κ.α. Οι λόγοι μπορεί να είναι πολλοί και διάφοροι όπως γεωγραφικοί, περιβαλλοντικοί, οικονομικοί, εκπαιδευτικοί, υγείας κ.α. Ορισμένες φορές οι ανισότητες μπορεί να είναι μεγάλες και συχνά ανυπέρβλητες. Οι προσπάθειες όλων των κοινωνιών σήμερα εστιάζονται στην «ενδυνάμωση του πολίτη» ώστε να έχει πρόσβαση και δυνατότητα αξιοποίησης όλων των ευκαιριών που εμφανίζονται και προσφέρονται.

Οι «τηλεματικές τεχνολογίες» λοιπόν αποτελούν το νέο σύμμαχο του ανθρώπου. Χάρη σε αυτές οι αποστάσεις εκμηδενίζονται και η διάθεση των υπηρεσιών μπορεί να γίνει οπουδήποτε κι αν βρίσκεται ο πολίτης ανεξάρτητα από την ώρα που τις επιζητεί. Εν τέλει η τηλεϊατρική μας παρέχει νέες δυνατότητες για περισσότερη δημοκρατία και δημοκρατικές διαδικασίες από οποιαδήποτε άλλη εποχή στον πλανήτη.

Όσο το βιοτικό επίπεδο μιας χώρας βελτιώνεται, αυξάνονται οι απαιτήσεις για ποιότητα στις υπηρεσίες, ενώ παράλληλα εντείνονται και οι πιέσεις για τη συνεχή βελτίωση της ποιότητάς τους. Σύμφωνα με τον ορισμό της «ποιότητας στις υπηρεσίες» του Διεθνή Οργανισμού Προτυποποιήσεως (ISO - International Standardization Organization) «ποιότητα είναι αυτό που ικανοποιεί τον πελάτη – χρήστη».

Οι υπηρεσίες υγείας έχουν και πρόσθετους ηθικούς, δεοντολογικούς, κοινωνικούς και νομικούς λόγους για να είναι αποδέκτης εγγυημένης ποιότητας. Στα πλαίσια του ΕΣΥ η διαθεσιμότητα των υπηρεσιών και η πρόσβαση σε αυτές φαίνεται ότι μειώνεται ραγδαία με την αύξηση της απόστασης κατοικίας και εργασίας από τις μεγάλες δευτεροβάθμιες ή τριτοβάθμιες μονάδες. Δυσκολεύεται συχνό από τις καιρικές συνθήκες κι από τις δυνατότητες μεταφοράς των ασθενούντων. Η διαθεσιμότητά τους επίσης είναι διαφορετική για τις διάφορες ώρες της ημέρας. Δυσκολεύεται έως και γίνεται αδύνατη από μια σειρά παραγόντων όπως η πυκνότητα κυκλοφορίας, οι μαζικές μετακινήσεις σε περιόδους διακοπών πάσης φύσεως κ.α.

Σε όλες τις περιπτώσεις, είναι εξαιρετικής σημασίας ο χρόνος απόκρισης σε συγκεκριμένο αίτημα, η ανταπόκριση από το ενδεδειγμένο επίπεδο του συστήματος και η

εγκυρότητα της απόκρισης. Δεδομένου ότι η Τηλεϊατρική δεν εξαρτάται από την απόσταση, ομάδες ειδικών μπορούν να επιληφθούν του περιστατικού, ακόμα κι αν οι ειδικοί βρίσκονται σε διαφορετικά σημεία. Οι χρόνοι επικοινωνίας δε, είναι εξαιρετικά μικροί κι ελεγχόμενοι. Εύλογα συνεπώς, η τηλεϊατρική συμβάλλει αποτελεσματικά στην ποιότητα των Υπηρεσιών Υγείας.

Η αύξηση του χρόνου ζωής – μέσος όρος 75 έτη για τις γυναίκες και 72 έτη για τους άντρες – υποστηρίζει την πεποίθηση ότι οι ανάγκες σε υπηρεσίες υγείας (ιατρικές) θα αυξάνονται με το χρόνο. Παράλληλα, επικρατούν νέες αντιλήψεις σχετικά με τις πλέον κατάλληλες συνθήκες θεραπείας ασθενών. Οι αντιλήψεις αυτές οφείλονται μερικώς και στις δυνατότητες που προσφέρουν οι νέες τεχνολογίες και οι επιστημονικές εξελίξεις.

Έτσι το σπίτι θεωρείται το πλέον κατάλληλο περιβάλλον για τον ασθενή και την αντιμετώπιση των προβλημάτων του (κατ' οίκον νοσηλεία), ακόμα και σε περιπτώσεις που κάτι τέτοιο ήταν προηγουμένως απαγορευτικό. Αρκεί βέβαια η παραμονή μακριά από τις ιατρικές μονάδες να συνδυαστεί με δυνατότητες διασύνδεσης, επισκεψιμότητας κ.α. Για το λόγο αυτό οι τηλεματικές τεχνολογίες βρίσκονται στο επίκεντρο του ενδιαφέροντος καθώς είναι οι καταλληλότερες για να αλλάξουν διαδικασίες και διεργασίες αντιμετώπισης προβλημάτων υγείας. Παλαιότερα έως και σήμερα, οι τράπεζες πληροφοριών ήταν τα βιβλία και οι βιβλιοθήκες. Στις αναπτυγμένες χώρες έχουν ουσιαστικά αντικατασταθεί από ηλεκτρονικές βιβλιοθήκες άμεσης πρόσβασης από οποιοδήποτε σημείο διαθέτει στοιχειώδη τηλεματική υποδομή. Παράλληλα, η αντιμετώπιση περιστατικών από ομάδες ειδικών είναι δυνατόν να αντικαταστήσουν τον ένα μόνο επαγγελματία υγείας, ο οποίος επιλαμβάνεται του περιστατικού, ειδικότερα σε περιβάλλοντα πρωτοβάθμιας φροντίδας υγείας. Η αντικατάσταση αυτή είναι σήμερα εφικτή χάρις στις δυνατότητες της τηλεσυνεδρίας.

Ειδικές μελέτες έχουν καταλήξει στο συμπέρασμα ότι παρά το υψηλό κόστος των σχετικών επενδύσεων, οι τηλεματικές τεχνολογίες προσφέρουν τις καλύτερες δυνατές λύσεις για τον έλεγχο των δαπανών. Δεν είναι λοιπόν περίεργο που σε όλες τις χώρες της Ευρωπαϊκής Ένωσης τα συστήματα Υγείας υποστηρίζονται πλέον από εκτεταμένα τηλεματικά δίκτυα και πληθώρα εφαρμογών. Οι τηλεματικές τεχνολογίες που επιστρατεύονται για την αντιμετώπιση ιατρικών προβλημάτων και των προβλημάτων υγείας, υποβοηθούν το έργο των επαγγελματιών υγείας. Έτσι, η ικανότητα αξιοποίησης των τεχνολογιών για την προσφορά υπηρεσιών στους ασθενείς, αλλά και στους επαγγελματίες υγείας, η ενασχόληση δηλαδή με την τηλεϊατρική ή την τηλεματική στην υγεία δεν αποτελεί «νέα ιατρική ειδικότητα». Αποτελεί ουσιαστικά υποχρέωση των επαγγελματιών υγείας να είναι σε θέση να χρησιμοποιούν τα τηλεματικά συστήματα προς όφελος των ασθενών και των ιδίων.

Ο έλεγχος των δαπανών μπορεί να γίνει μέσω των τηλεματικών τεχνολογιών, λαμβάνοντας υπόψη ότι όλες οι πληροφορίες και τα δεδομένα που παράγονται ή

αξιοποιούνται για την αντιμετώπιση ενός περιστατικού, καταγράφονται με ηλεκτρονικό τρόπο. Η καταγραφή επιτρέπει την ανάλυση και αξιολόγηση και κατά συνέπεια την αντιστοίχηση με δείκτες αποτελεσματικότητας και φυσικών δαπανών.Αν τέλος θυμηθούμε ότι η Τηλεϊατρική είναι ουσιαστικά «υποβοηθούσες τεχνολογίες» κι όχι ένας νέος κλάδος ιατρικής, τότε μπορούμε εύκολα να δεχτούμε ότι η οργάνωση και παροχή για παράδειγμα κατ' οίκον νοσηλείας, θα αποτελέσει αντικείμενο έντονου ανταγωνισμού μεταξύ δημοσίων και ιδιωτικών φορέων. Εξ' ίσου ανταγωνιστικό θα είναι και το περιβάλλον της πρωτοβάθμιας φροντίδας για την αντιμετώπιση εποχιακών αναγκών, με προεξέχουσα δραστηριότητα την κάλυψη των αναγκών των ατόμων που βρίσκονται σε διακοπές.

Το πρώτο σχέδιο ενός «τυπικού» Εγχειριδίου Τηλεϊατρικής, δημιουργήθηκε από το Εργαστήριο Ιατρικής Φυσικής την περίοδο 1995-97, όταν κατεβλήθη προσπάθεια να γίνει το Κέντρο Υγείας Νάξου πρότυπη μονάδα πρωτοβάθμιας Υγείας υποστηριζόμενη από υπηρεσίες Τηλεϊατρικής. Το Κέντρο Υγείας Νάξου είχε προταθεί στο Υπουργείο Υγείας να θεωρηθεί ως πρότυπο – πιλοτικό – δεδομένου ότι ήδη διέθετε τηλεματική υποδομή και σύστημα ηλεκτρονικών φακέλων υγείας. Όλη η υποδομή δημιουργήθηκε από το Εργαστήριο Ιατρικής Φυσικής στα πλαίσια ερευνητικών έργων. Συμπλήρωμα του Ε. Τ. μπορεί να είναι το «Εγχειρίδιο Ποιότητας», το οποίο εξακολουθεί να αποτελεί σημαντικό εργαλείο για την οργάνωση του φορέα ακόμα και κατά την νέα έκδοση προτύπων ποιότητας ISO 9000:2000. Πρότυπο Ε. Τ. γραμμένο στην Αγγλική είναι αυτό που έχει εκδώσει το Κέντρο Τηλεϊατρικής του Πανεπιστημίου Tromso της Νορβηγίας.Σε οποιαδήποτε περίπτωση είναι απαραίτητη η έγκριση του ασθενούς ή των οικείων του για τη χρήση των υπηρεσιών προκειμένου να αντιμετωπιστεί το πρόβλημα υγείας

4.3 Τηλεφροντίδα

Σήμερα όμως είναι εφικτή η εξ αποστάσεως παρακολούθηση η οποία συμβάλλει στην πρόληψη, έγκαιρη διάγνωση, θεραπεία και κατ' οίκον αποκατάσταση. Οφείλουμε όμως να δούμε τους λόγους για τους οποίους η εξ αποστάσεως παρακολούθηση, η τηλεφροντίδα γενικεύοντας είναι τόσο σημαντική καθώς και τις αιτίες που επέβαλλαν μια τέτοια μορφή υπηρεσιών υγείας.

- Είναι αδιαμφισβήτητο ότι η Γη είναι ένας πλανήτης που «γερνάει». Ειδικά στη χώρα μας το φαινόμενο της γήρανσης του πληθυσμού είναι έντονο. Αυτό έχει ως αποτέλεσμα την ύπαρξη περισσότερων αναλογικά γηραιών ανθρώπων που χρειάζονται περίθαλψη καθότι έχουν κινητικά και άλλα προβλήματα υγείας.

- Τα έξοδα υγείας – περίθαλψης δυστυχώς ακολουθούν τη ραγδαία ανάπτυξη της τεχνολογίας, με συνέπεια να καθίστανται αβάσταχτα ιδίως για τα μεσαία και κατώτερα οικονομικά στρώματα.
- Τα «οικογενειακά δίκτυα» έχουν κάνει την εμφάνισή τους, περισσότερο βέβαια στις δυτικές κοινωνίες οπότε η απαιτούμενη εξοικείωση με τον ηλεκτρονικό εξοπλισμό και τον κόσμο της πληροφορικής ήδη υπάρχει κι αναπτύσσεται διαρκώς.
- Μεγάλος αριθμός ασθενών κι ανήμπορων ανθρώπων σημαίνει αυτόματα μεγαλύτερες ανάγκες σε νοσοκομεία, εξεταστήρια, ιατρικό προσωπικό και ιατρικό εξοπλισμό. Για μια χώρα όπως η Ελλάδα με αυξανόμενο γηραιό πληθυσμό, με χαμηλό κατά κεφαλήν εισόδημα, δίχως βιομηχανία παραγωγής ηλεκτρονικών υπολογιστών και λοιπών ηλεκτρικών συσκευών, και με ασφαλιστικά ταμεία που συγχωνεύονται προκειμένου να επιβιώσουν καθώς συχνά αδυνατούν να καλύψουν τις ανάγκες ιατρικής περίθαλψης των ασφαλισμένων τους, αυτό αποτελεί σημαντικότατο πρόβλημα.

Το όραμα της τηλεϊατρικής είναι οι ηλικιωμένοι και ανήμποροι ασθενείς αντί να μετακινούνται προκειμένου να υποβληθούν σε εξετάσεις ή να παραμένουν σε νοσοκομεία προκειμένου να παρακολουθούνται, να έχουν τη δυνατότητα – προνόμιο να βρίσκονται στο σπίτι τους ή σε οικείο περιβάλλον με αποτέλεσμα:

Α) Βελτίωση της ποιότητας ζωής τους χωρίς να τίθεται θέμα ιατρικής ασφάλισης (ίδια ποιότητα υπηρεσιών ανεξαρτήτως ασφαλιστικού φορέα στον οποίο ανήκουν).

Β) Να υφίσταται έλεγχος και περιορισμός – ελαχιστοποίηση του σημαντικού κόστους των υπηρεσιών υγείας.

Γ) Καλύτερη λειτουργία των νοσοκομείων, εξεταστήριων κλπ λόγω μείωσης των ασθενών που πρέπει να παρακολουθούνται και να περιθάλπονται.

Επίσης σημαντικότατη βοήθεια μπορεί να προσφέρει η τηλεϊατρική σε απομακρυσμένες περιοχές όπως νησιά ή επαρχίες που δεν έχουν την απαιτούμενη ιατρική υποδομή. Με τη συμβολή της τεχνολογίας οι ασθενείς θα μπορούν να παρακολουθούνται από εξειδικευμένο προσωπικό χωρίς να χρειάζεται (εκτός από βαριές κι έκτακτες καταστάσεις) να μεταβούν στο νοσοκομείο που πιθανόν να βρίσκεται σε μεγάλη απόσταση.

Μία τέτοια τεχνολογία είναι το ‘Ίντερνετ των πραγμάτων’ η οποία αναλύθηκε στο πρώτο κεφάλαιο. Αυτή θα παρέχει στην τηλεϊατρική ευελιξία, καλύτερη και ευκολότερη διασυνδεσιμότητα μεταξύ τηλειατρικού σταθμού και ιατρικής συσκευής ‘ασθενής’ και μεγαλύτερη ασφάλεια απορρήτου.

Εικόνα 4.2: Μορφή συστήματος τηλεϊατρικής

4.4 Το ‘Διαδίκτυο των πραγμάτων’ στην υγεία

4.4.1 Παρουσίαση

Τα τελευταία χρόνια, σε όλες σχεδόν τις χώρες του κόσμου, έχουν διατεθεί σημαντικοί οικονομικοί πόροι για τον τομέα της υγειονομικής περίθαλψης. Η αγορά των αναπτυγμένων χωρών στηρίζεται σε μεσαίας και μεγαλύτερης ηλικίας ανθρώπους κατά κύριο λόγο. Η τάση αυτή έχει ως αποτέλεσμα να υπάρξει μια μεγαλύτερη ζήτηση για υγειονομική περίθαλψη που σχετίζεται με τις υπηρεσίες υγείας και ένας μεγαλύτερος ανταγωνισμός μεταξύ των παρόχων υγειονομικής περίθαλψης.

Η επίτευξη υψηλής επιχειρησιακής αποτελεσματικότητας στον τομέα της υγειονομικής φροντίδας αποτελεί βασικό στόχο για την οργανωτική αξιολόγηση των επιδόσεών της. Η αποδοτική χρήση θα πρέπει να θεωρείται ως ο κύριος δείκτης όσο αφορά τις επιδόσεις του νοσοκομείου. Από διαχειριστική άποψη, η κατανόηση της δομής του κόστους των νοσοκομείων και της αναποτελεσματικότητας στην αξιοποίηση των πόρων είναι ζωτικής

σημασίας για την πραγματοποίηση πολιτικών σχετικά με την υγειονομική περίθαλψη και τις αποφάσεις του προϋπολογισμού. Το κόστος των ιατρικών υπηρεσιών στα νοσοκομεία θα μπορούσε να ελεγχθεί από μεγαλύτερη λειτουργική αποτελεσματικότητα και να παρείχε περισσότερες επιλογές για οικονομικά προσιτή μέριμνα και βελτίωση της πρόσβασης στο δημόσιο.

Οι παροχές υγειονομικής περίθαλψης τα τελευταία χρόνια απαιτούν μια συντονισμένη προσπάθεια της τεχνολογίας της πληροφορίας ώστε να μειωθεί το κόστος της υγειονομικής περίθαλψης στο δυτικό κόσμο. Προκειμένου να μειωθεί το κόστος και να βελτιωθεί η αποτελεσματικότητα, η χρήση ευφυών συστημάτων θεωρείται επιβεβλημένη. Τα ευφυή συστήματα θα διαδραματίσουν σημαντικό ρόλο στην παροχή έξυπνης επεξεργασίας και εξατομικευμένων πληροφοριών από τους ασθενείς προς τους γιατρούς και το προσωπικού της υγειονομικής τους περίθαλψης (δηλαδή, νοσηλευτές).

Η διαχείριση της υγειονομικής περίθαλψης είναι πολύ πίσω σε σύγκριση με την υπηρεσία και την παρασκευή στις βιομηχανίες.

Υπάρχει αυξανόμενη ανησυχία σχετικά με την υγεία εξαιτίας της γήρανσης του πληθυσμού. Η κινητή τεχνολογία αισθητήρων αναμένεται να παρέχει πληροφορίες σε πραγματικό χρόνο για ζωτικά σημεία και για άλλους φυσιολογικούς δείκτες σχετικά με την υγεία και την φυσική κατάσταση ενός ατόμου. Αυτά τα συστήματα παρακολούθησης αναμένεται να βρουν μεγαλύτερη χρήση σε εφαρμογές όπως στα νοσοκομεία, σε συστήματα παρακολούθησης της υγείας στο σπίτι, στα γραφεία γιατρών, στη φροντίδα ηλικιωμένων, σε κέντρα φυσικής κατάστασης και σε ερευνητικές μελέτες για την υγεία.

Σε ένα πλαίσιο υγειονομικής περίθαλψης, θα μπορούσε να χρησιμοποιηθεί το Διαδίκτυο για την παροχή υπηρεσιών σε απομακρυσμένες περιοχές. Επίσης το κινητό εμπόριο μπορεί να χρησιμοποιηθεί για την αυτοματοποίηση της παράδοσης φαρμάκων. Μέχρι στιγμής, το Διαδίκτυο παρέχει ένα ολόκληρο φάσμα νέων τεχνολογιών στη διάθεση των νοσοκομείων ώστε να διευκολυνθεί η επικοινωνία και η οικοδόμηση σχέσεων με τους ασθενείς.

Η εφαρμογή των αρχών αυτών μπορεί να διευκολυνθεί από τη χρήση φορητής τεχνολογίας, όπως το Διαδίκτυο των πραγμάτων και όπως ήδη έχει αναφερθεί μια μορφή αυτού είναι το Radio Frequency Identification (RFID). Η σημερινή προηγμένη τεχνολογία είναι σε θέση να ενώσει τις έξυπνες ετικέτες (RFID) και την επεξεργασία δεδομένων σε ένα ενιαίο ολοκληρωμένο σύστημα. Το RFID είναι μια τεχνολογία που προσφέρει λύση στο ευρύ φάσμα των αναγκών των επιχειρήσεων συμπεριλαμβανομένου και του τομέα της υγειονομικής περίθαλψης. Παρατηρείται επίσης ότι ιατρικές εφαρμογές, όπως το Hospital Patient Management System (HPMS) βασισμένο σε RFID προσφέρει τεράστια πλεονεκτήματα σε σχέση με την διαχείριση των συστημάτων της υγειονομικής περίθαλψης.

4.4.2 Μοντέλα RFID σε υπηρεσίες υγείας

Στην παροχή ιατρικής περίθαλψης (δηλαδή, νοσοκομεία) παραδοσιακά χρησι-μοποιείται ένα σύστημα βασισμένο στο χαρτί "ένα διάγραμμα ροής», για να καταγράφονται οι πληροφορίες του ασθενούς κατά τη διάρκεια της εγγραφής, το οποίο ενημερώνεται από τη νοσοκόμα και παραδίδεται στο τέλος κάθε βάρδιας. Παρά το γεγονός ότι οι νοσοκόμες δαπανούν μεγάλο μέρος του χρόνου εργασίας τους για την ενημέρωση της καρτέλας του ασθενούς, αυτή μπορεί να μην είναι πάντα ακριβής, διότι είναι χειρόγραφη.

Οι νοσοκόμες διαδραματίζουν ζωτικό ρόλο στο σύστημα του νοσοκομείο και στην επιτυχία της ενδονοσοκομειακής και της εξωνοσοκομειακής περίθαλψης. Παίζουν επίσης ένα πολύ σημαντικό ρόλο με το να εκτελούν εντολές της κλινικής και να κοινοποιούν πληροφορίες μεταξύ του νοσοκομείου και του ασθενούς, το οποίο έχει σαν αποτέλεσμα να αξιολογηθεί η δυναμική της RFID (Radio Frequency Αναγνώρισης) τεχνολογίας σαν μέσο μεταβίβασης των πληροφοριών αυτών.

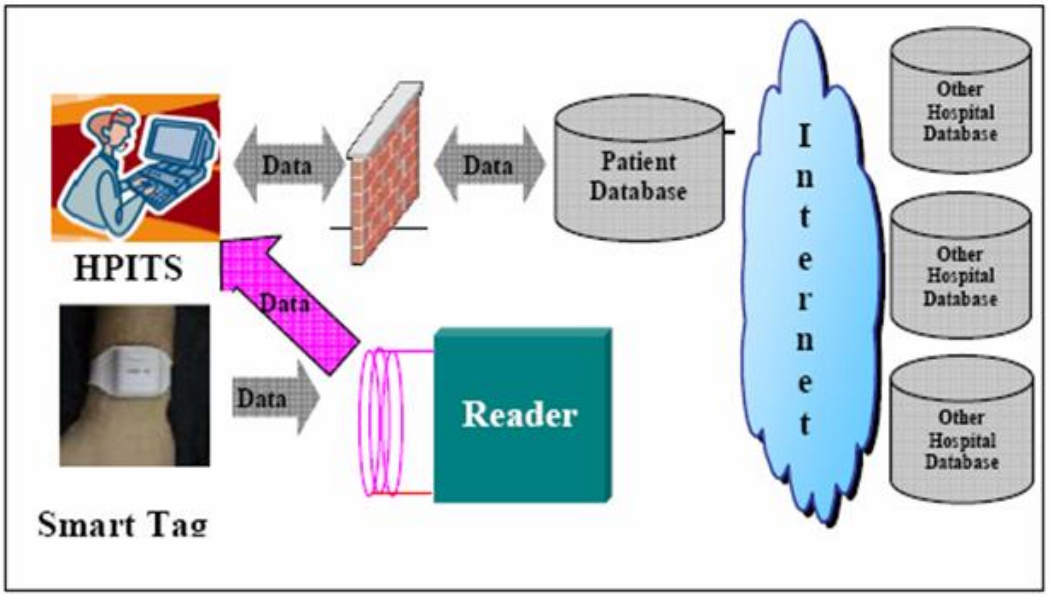
Το RFID είναι μία από τις ανερχόμενες τεχνολογίες, η οποία μπορεί να διευκολύνει την αυτοματοποίηση της ασφαλούς και ακριβής ταυτοποίησης των ασθενών, την παρακολούθηση και την επεξεργασία σημαντικών πληροφοριών σε θέματα υγείας στον τομέα της υγειονομικής περίθαλψης, όπως τα νοσοκομεία.

Κάθε ετικέτα RFID ‘η οποία μπορεί να είναι σε μορφή βραχιόλι’ αναγνωρίζεται από ένα μοναδικό Αριθμός Αναγνώρισης (UIN) που μπορεί να προγραμματιστεί είτε αυτόματα ή με το χέρι. Στη συνέχεια ο κωδικός αυτός προστατεύεται για να εξασφαλιστεί το υψηλό επίπεδο ασφαλείας.

Το RFID βραχιόλι θα δίνεται σε κάθε ασθενή, και στη συνέχεια μπορεί να χρησιμοποιηθεί για τον εντοπισμό των ασθενών καθ΄ όλη τη διάρκεια της νοσηλείας τους. Μπορεί επίσης να χρησιμοποιείται για την αποθήκευση των πιο σημαντικών στοιχείων των ασθενών (όπως όνομα ασθενή, ID, αλλεργίες σε φάρμακα, τα φάρμακα που χορηγήθηκαν στον ασθενή την τρέχουσα μέρα, η ομάδα αίματος του, και ούτω καθεξής) προκειμένου να ενημερώνεται δυναμικά το προσωπικό. Τα κωδικοποιημένα δεδομένα από το RFID βραχιόλι μπορούν να διαβαστούν ενώ οι ασθενείς κοιμούνται. Η τεχνολογία RFID παρέχει μια μέθοδο για τη διαβίβαση και τη λήψη των δεδομένων από έναν ασθενή για λογαριασμό του γιατρού ή του νοσηλευτικού προσωπικού χωρίς την ανθρώπινη παρέμβαση (δηλαδή μέσω ασύρματης επικοινωνίας). Είναι μια αυτό-ματοποιημένη τεχνολογία σύλληψης δεδομένων που μπορεί να χρησιμοποιηθεί για τον εντοπισμό και την αποθήκευση πληροφοριών σχετικά με τον ασθενή με ηλεκτρονικά μέσα τα οποία περιέχονται στο RFID βραχιόλι (δηλαδή τις έξυπνες ετικέτες). Οι γιατροί και το νοσηλευτικό προσωπικό θα μπορούν να έχουν πρόσβαση στις εγγραφές και κατ’ επέκταση στην ενημέρωση των ασθενών από απόσταση μέσω WiFi σύνδεση

χρησιμοποιώντας φορητές συσκευές όπως PDA (Personal Digital Assistant), φορητούς υπολογιστές και άλλες κινητές συσκευές. Το WiFi (wireless fidelity), είναι ένας ασύρματος τοπικός χώρος δικτύων (WLAN) που επιτρέπει στο φορέα παροχής υγειονομικής περίθαλψης (π.χ. νοσοκομεία) να αναπτύξει ένα δίκτυο πιο γρήγορα, σε χαμηλότερο κόστος και με μεγαλύτερη ευελιξία από ένα ενσύρματο σύστημα.

Η τεχνολογία RFID αποτελείται κυρίως από ένα αναμεταδότη (smart tag), και ένα αναγνώστη Healthcare Provider IT συστήματατος (HPITS), όπως φαίνεται στην ακόλουθη εικόνα. Κάθε ετικέτα επισυνάπτεται στον ασθενή σε μορφή βραχιόλι που περιέχει μία κεραία και ένα μικροσκοπικό μικροτσίπ μικρότερο και από έναν κόκκο άμμου.



Εικόνα 4.3: Κύρια συστατικά του rfid

Η κεραία λαμβάνει ραδιοκύματα ή ηλεκτρομαγνητικά κύματα ενέργειας που εκπέμπονται σε αυτό από μια συσκευή ανάγνωσης και επιτρέπει στο chip να διαβιβάσει από τους ασθενείς το μοναδικό αναγνωριστικό στην συσκευή ανάγνωσης, ώστε να εντοπίζεται ο ασθενής εξ αποστάσεως. Η συσκευή ανάγνωσης μετατρέπει τα ραδιοκύματα που αντανακλώνται πίσω από τον ασθενή σε ψηφιακές πληροφορίες που μπορούν στη συνέχεια να επεξεργαστούν από το HPITS.

Τα βασικά δεδομένα του ασθενούς (π.χ. ID, όνομα, ηλικία, τοποθεσία, κτλ), μπορούν να αποθηκευτούν σε μία βάση δεδομένων ή να συνδέονται μέσω του Διαδικτύου με βάσεις δεδομένων άλλων νοσοκομείων.

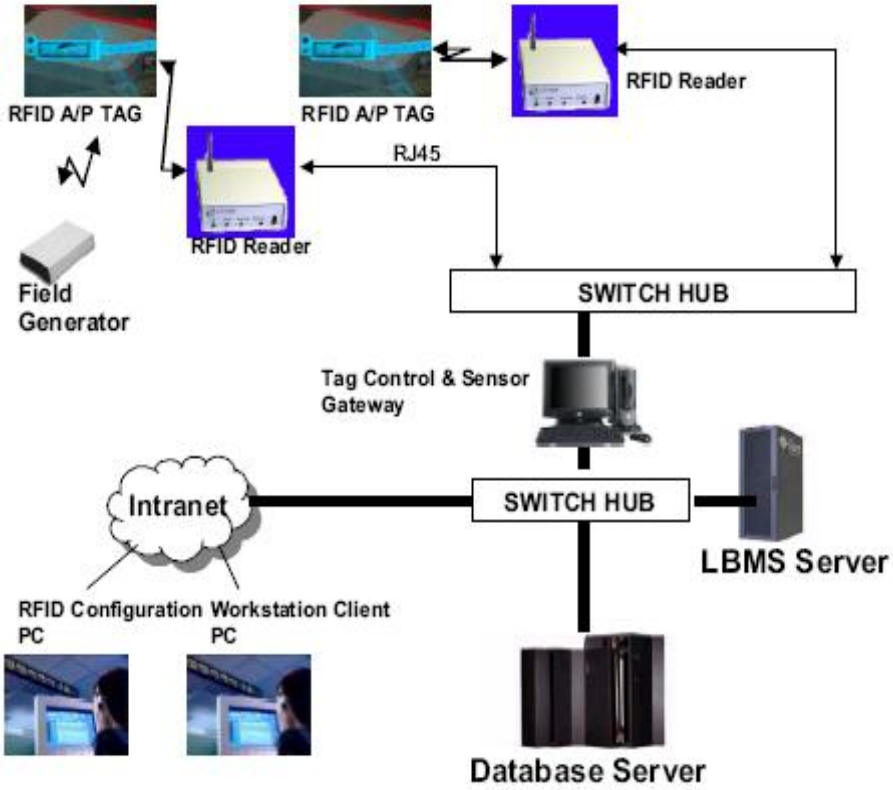
4.4.3 Ιατρικές υπηρεσίες παρακολούθησης θέσης (Location-based Medicare Service (LBMS))

Στις 12 Μαρτίου του 2003, η Παγκόσμια Οργάνωση Υγείας (ΠΟΥ) εξέδωσε μια παγκόσμια προειδοποίηση για την άτυπη πνευμονία, που ονομάστηκε σοβαρό οξύ αναπνευστικό σύνδρομο (SARS). Ο SARS είναι ιδιαίτερα μεταδοτικός ιός και γρήγορα αμφισβήτησε την αποτελεσματικότητα των μέτρων ελέγχου των λοιμώξεων στα νοσοκομεία. Ορισμένα νοσοκομεία έκλεισαν για εβδομάδες, σε μια προσπάθεια να προλάβουν την περαιτέρω εξάπλωση της νόσου. Όπως και συνέβη, η καταγραφή των φυσικών επαφών των ασθενών που είχαν προσβληθεί ήταν απαραίτητη για τον εντοπισμό και την ανίχνευση άλλων πιθανών προσβεβλημένων ατόμων. Χρειάστηκε χρόνος και προσπάθεια για την κατασκευή του ιστορικού των επαφών του ασθενούς με άλλους συνανθρώπους του, αλλά η ισχυρή, αυτόματη αναγνώριση και ο εντοπισμός των RFID φαινόταν να μπορούσε να συμβάλει τα μέγιστα στην παρούσα κατάσταση. Τον Μάιο του 2003, δύο νοσοκομεία της Σιγκαπούρης, Alexandra Hospital και National University Hospital, εφάρμοσαν πρώτα ένα σύστημα RFID το Hospital Movement Tracking System στο τμήμα των Ατυχημάτων και Επειγόντων Περιστατικών, για την παρακολούθηση των επισκεπτών, των ασθενών και του προσωπικού. Εμπνευσμένη από την πρωτοβουλία των δύο νοσοκομείων της Σιγκαπούρης, το TMUH 'Taipei Medical University Hospital ' άρχισε να εξετάζει ένα παρόμοιο σχέδιο.

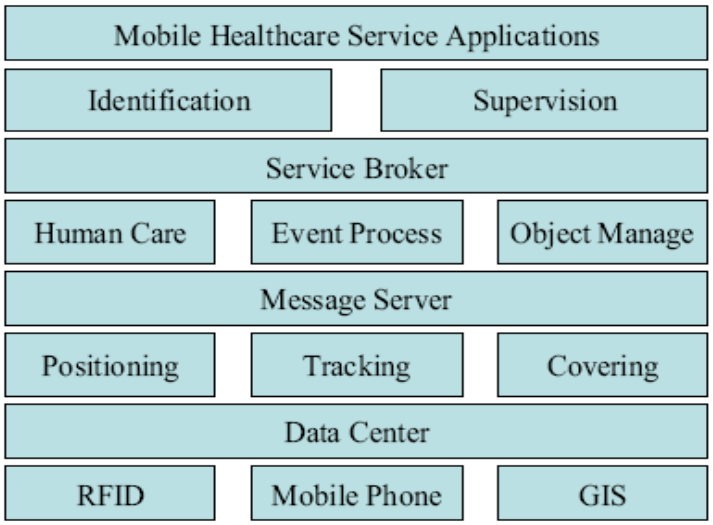
Τον Αύγουστο του 2003 το Taiwan Department of Industrial Technology (DoIT), Ministry of Economic Affairs (MOEA) ετοίμασε ένα σχέδιο επιδότησης για την ενθάρρυνση των εγχώριων επιχειρήσεων και των ιδρυμάτων για έρευνα και ανάπτυξη τεχνολογιών για την ανίχνευση, το οποίο θα συμπεριελάμβανε και τη θεραπεία του SARS. Το TMUH πρότεινε ένα χρονοδιάγραμμα ώσπου να αναπτύξει το Location-based Medicare Service (LBMS).

Μετά από μελέτη του τρόπου μετάδοσης του SARS, το νοσοκομείο αποφάσισε ότι το σύστημα θα έπρεπε να έχει την δυνατότητα σε πραγματικό χρόνο να παρακολουθεί καθώς και να λαμβάνει τη θερμοκρασία των tagged ασθενών. Μετά την εξέταση πολλών ειδών ετικετών, το TMUH επέλεξε τις 916,5 MHz UHF ενεργές ετικέτες. Αυτά τα ενεργά tag ήταν πολύ πιο ακριβά από τα παθητικά , αλλά είχαν μεγαλύτερη εμβέλεια ανάγνωσης καθώς και καλύτερη ταχύτητα ανάγνωσης, ώστε να είναι εφικτή η συνεχής παρακολούθηση του ασθενούς. Το νοσοκομείο αποφάσισε ότι οι ετικέτες για τους ασθενείς που είχαν προσβληθεί από το SARS θα έπρεπε να είχαν ενσωματωμένο θερμόμετρο. Μέσω της αυτόματης λήψης και της διαβίβασης της θερμοκρασίας, το σύστημα θα μπορούσε να συλλέξει δεδομένα σε πραγματικό χρόνο και να μειώσει τον κίνδυνο λοιμώξεων του προσωπικού λόγω της αναγκαίας επαφής τους με τους ασθενείς.

Ωστόσο, η ετικέτα δεν ήταν διαθέσιμη εκείνη την στιγμή, έτσι ένας RFID πωλητής κλήθηκε να υλοποιήσει μια τέτοια. Η συσκευή ανάγνωσης που χρησιμοποιήθηκε στο έργο αυτό έπρεπε να είχε σημαντικά χαρακτηριστικά συμπεριλαμβανομένων των εξής: 10 megabits μνήμη, δυνατότητα ανάγνωσης multi-tag, μία wakeup 433 MHz συχνότητα στις ετικέτες, και εύρος ανάγνωσης 3 εως 85 μέτρα. Επειδή οι συσκεύες ανάγνωσης είναι ακριβές, σε ορισμένα σημεία χρησιμοποιήθηκαν γεννήτριες πεδίων. Μια γεννήτρια πεδίου είναι μια μικρή, αποτελεσματική tag wake-up συσκευή που επικοινωνεί απευθείας με τον αναγνώστη. Η γεννήτρια ανοίγει περιοδικά και ζητάει ετικέτες για ένα καθορισμένο χρονικό διάστημα και μετά σβήνει. Μπορεί να ενεργοποιείται είτε από έναν αισθητήρα κίνησης είτε αν ο χρήστης καλέσει μια ειδική ετικέτα, ή όλες τις ετικέτες ανά πάσα στιγμή. Το κόστος μιας γεννήτριας πεδίου είναι πολύ μικρότερο από εκείνο του αναγνώστη. Προκειμένου να βελτιωθεί η ακρίβεια, οι γεννήτριες πεδίου χωρίζονται σε τρεις κατηγορίες: κανονική γεννήτρια, γεννήτρια ορόφου, και γεννήτρια περιοχής. Οι γεννήτριες ορόφου είχαν εγκατασταθεί στην περιοχή με τις σκάλες και οι γεννήτριες περιοχής εγκαταστάθηκαν στις διασυνδέσεις των γειτονικών περιοχών. Το εύρος ανίχνευσης των γεννητριών περιοχής και ορόφου θα έπρεπε να ελέγχεται για τις συντομότερες αποστάσεις, και η συχνότητα ανίχνευσης έπρεπε να είναι η συντομότερη δυνατή ώστε να εξασφαλιστεί ότι η ομαλή κυκλοφορία του κάθε tagged προσώπου ή αντικειμένου από μια περιοχή ή όροφο σε κάποιο άλλο. Μετά από πολλές δοκιμές και προσαρμογή, ένα νοσοκομείο με κάλυψη από RFID υποδομών (όπως απεικονίζονται στο σχεδιάγραμμα 4.4) ολοκληρώθηκε, συμπεριλαμβανομένων 163 γεννητριών πεδίου, 41 αναγνωστών RFID, 27 Yagi κεραιών, 15 σταθμών προγραμματισμού (SW) και ενός συστήματος API (SW). Η αρχιτεκτονική του συστήματος LBMS επίσης αναπτύχθηκε όπως απεικονίζεται στο σχήμα 4.5 η οποία δείχνει τον τρόπο με τον οποίο τα δεδομένα συλλέχθηκαν, επεξεργάστηκαν, αποθηκεύτηκαν και μετατράπηκαν σε χρήσιμες πληροφορίες για τις ιατρικές υπηρεσίες του νοσοκομείου.



Εικόνα 4.4:Η δομή του RFID στο Taipei Medical University Hospital

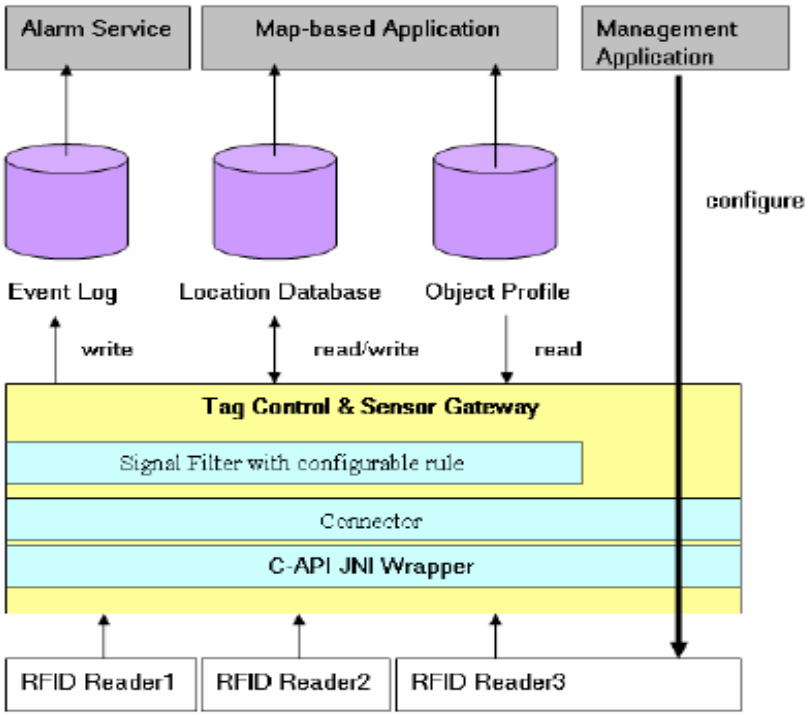


Εικόνα 4.5:Η αρχιτεκτονική δομή του LBMS

Υπήρξαν διαφορετικές ενότητες του συστήματος, συμπεριλαμβανομένων αυτών για τον έλεγχο των πινακίδων, την πύλη του αισθητήρα (RFID C-API, JNIwrapper, signal

dispatcher, signal filter), την ιατρική παρακολούθηση (ιατρική μεταφορά δεδομένων), και την εφαρμογή (υπηρεσία μηνυμάτων, υπηρεσία χαρτών, εντοπισμός υπηρεσιών).

Τα δεδομένα φιλτράρονται σύμφωνα με προκαθορισμένους κανόνες πριν από την διαβίβαση, και την αποθήκευση στη βάση δεδομένων θέσης και στις βάσεις για τις ζωτικής σημασίας πληροφορίες. Το σύστημα ανακτά αυτόματα τα ιατρικά αρχεία των ασθενών από πληροφοριακά συστήματα υγειονομικής περίθαλψης και δημιουργεί ένα Rulebase ώστε να κρίνει εάν υπήρχε λοιμώδης εκδήλωση. Το σύστημα LBMS είχε ένα γραφικό για τον χρήστη (GUI), το οποίο υιοθέτησε την προσέγγιση του web-service. Όταν το σύστημα ανίχνευε μια μεταδοτική περίπτωση, ειδοποιούσε με email και με SMS.



Εικόνα 4.6: Η αλληλεπίδραση των ενοτήτων LBMS

Η αλληλεπίδραση των ενοτήτων LBMS απεικονίζονται στο σχήμα 4.6. Το σύστημα μπορούσε επίσης να βοηθήσει στην επιβολή της καραντίνας μιας κοινότητας έξω από το νοσοκομείο μέσω συσκευή ανάγνωσης που θα κάλυπτε την περιοχή που είχε εκδηλωθεί η λοίμωξη.

Η διοίκηση του νοσοκομείου ήταν πολύ ικανοποιημένη με το σύστημα και σχεδίαζε να αναπτύξει και άλλες ιατρικές εφαρμογές που βασίζονται στο σύστημα LBMS, όπως είναι ο εντοπισμός πολύτιμου εξοπλισμού, ο ενδονοσοκομειακός ιατρικός έλεγχος και εντοπισμός του νεογνού και της μητέρας και τέλος ο νόμιμος έλεγχος των φαρμάκων.

4.4.4 Το κόστος και τα οφέλη των RFID σε πραγματικές εφαρμογές

- Treviglio Caravaggio Νοσοκομείο (Ιταλία): Εντοπισμός ασθενούς στα επείγοντα και ακτινολογικά τμήματα του ορθοπεδικού τομέα

Το Ospedale Treviglio-Caravaggio, είναι ένα νοσοκομείο με 440-κρεβάτια, βρίσκεται στο Treviglio, στην Ιταλία, και σε αυτό αναπτύχθηκε το RFID σύστημα για την παρακολούθηση των ασθενών του ορθοπεδικού τμήματος που νοσηλεύονται στην πτέρυγα έκτακτης ανάγκης του νοσοκομείου (ED) και οι οποίοι στη συνέχεια μετακινιούνται μεταξύ του ED και του ακτινολογικού τμήματος όπου λαμβάνουν ιατρικές υπηρεσίες.

Το ED, είναι μια νεόκτιστη εγκατάσταση, και δέχεται 55.000 ED ασθενείς ετησίως με τον όγκο των ασθενών να αυξάνεται κατά 10-12% ετησίως από το 2004. Από αυτούς, μόνο οι 200 ED ασθενείς αφορούν ορθοπεδικές περιπτώσεις κάθε μήνα. Αντιμετωπίζοντας ένα μεγάλο όγκο πληροφοριών από αιτήματα των μελών των οικογενειών των ασθενών, το 2004 το Ospedale Treviglio-Caravaggio ενέκρινε ένα ενεργό σύστημα RFID που θα εμφάνιζε τη θέση του κάθε ασθενούς που έχει ορθοπεδικά προβλήματα (οι οποίοι προσδιορίζονται από έναν αριθμητικό κωδικό) κατά τη διάρκεια της νοσηλείας του σε ένα διαδραστικό χάρτη που διατίθεται για την προβολή του σαλονιού των έκτακτων περιστατικών, καθώς και του χώρου του νοσηλευτικού προσωπικού.

Κόστος εφαρμογής

Λόγω της μη αποκάλυψης των συμφωνιών που υπογράφτηκαν από διάφορες κατηγορίες συμμετεχόντων σε αυτή τη μελέτη δεν μπορεί να υπάρξει ακριβής ποσοτικός προσδιορισμός των δαπανών. Ωστόσο, από συνεντεύξεις που πραγματοποιήθηκαν υπάρχει η δυνατότητα συλλογής συγκεκριμένων ποιοτικών στοιχείων κόστους, όπως η πάροδος του χρόνου του έργου και το κόστος υλικού RFID. Κατέστη δυνατό, συνεπώς,

να προσεγγιστεί ένα συνολικό κόστος το οποίο επικυρώθηκε κατά τη διάρκεια των συνεντεύξεων.

Το κόστος της εφαρμογής περιλαμβάνει το κόστος υλικού (€ 100.000) και το κόστος των δύο εκπροσώπων του προσωπικού του τομέα έκτακτης ανάγκης για περίπου 15 ημέρες για ολόκληρη την ανάπτυξη και τις φάσεις παράδοση του έργου. Στη συντήρηση και στο κόστος εργασίας περιλαμβάνεται ένα ελάχιστο κόστος για το χρόνο που απασχολήθηκε το προσωπικό για τη χρήση του συστήματος, όπως και ο χρόνος που διέθεσαν οι νοσοκόμες για την εγκατάσταση και το κατέβασμα των δεδομένων από τις ετικέτες RFID των ασθενών.

Πλεονεκτήματα της εφαρμογής:

Μια πλήρη οικονομική αξιολόγηση πρέπει να εξετάζει όλα τα αποτελέσματα (οφέλη) που προκύπτουν από την εφαρμογή όπως:

Αύξηση της αποδοτικότητας:

Αυτή εξαρτάται από τα κέρδη που συνδέονται με την αύξηση των ασθενών ανά βάρδια και το μειωμένο μέσο όρο χρόνου εξυπηρέτησης των ασθενών, το οποίο με τη σειρά του συνδέεται με τη βελτίωση της παραγωγικότητας του νοσηλευτικού προσωπικού.

Αυτή η εφαρμογή έχει συσχετισθεί με την εξοικονόμηση χρόνου των επειγόντων περιστατικών, το οποίο οφείλεται στο ότι η νοσοκόμα αποδεσμεύεται από την άμεση ανάγκη για ανταπόκριση σε αιτήματα σχετικά με το που βρίσκονται οι ασθενείς. Σύμφωνα με τους υπολογισμούς (είναι τα δύο σενάρια που προβλέπονται σε διάστημα πέντε ετών ως βέλτιστες πρακτικές, δείχνουν ότι αυτό είναι ο χρόνος ζωής ενός συστήματος πληροφορικής) η εισαγωγή του συστήματος RFID επιφέρει εξοικονόμηση πόρων ύψους € 37.183 περίπου μόνο από τη μείωση του χρόνου συνομιλίας μίας νοσοκόμας με ασθενείς με ορθοπεδικά προβλήματα. Η χρηματική αξία μπορεί να είναι υποθετική αλλά ο χρόνος που σώζεται μπορεί να μην οδηγήσει σε μείωση του αριθμού των απασχολούμενων. Περισσότερο σημαντικό είναι ο χρόνος που θα ελευθερωθεί να μπορεί διατεθεί για άλλες δραστηριότητες που βελτιώνουν τις υπηρεσίες υγείας και τη φροντίδα των ασθενών.

Άλλα κέρδη από την αύξηση της αποτελεσματικότητας περιλαμβάνουν τα εξής:

• στο ED αποτελεσματικότερη χρήση του χρόνου της νοσοκόμας που δαπανάται στους ασθενείς (κάτι που πρέπει να αποτιμηθεί σε χρηματική αξία σε σχέση με την ασφάλεια των ασθενών και των αποτελεσμάτων)

• βελτίωση της ικανότητας του προσωπικού για την ανίχνευση των ασθενών και την αποφυγή σύγχυσης στην εύρεση αυτών, καλύτερη προετοιμασία των διαδοχικών θεραπειών, και λιγότερος χρόνος απάντησης σε αιτήματα πληροφοριών σχετικά με την εισαγωγή των ασθενών στο ED ή το X-ray 'ακτινολογικό' τομέα.

Ποιητικά κέρδη:

• τρέχουσες, άμεσες προσβάσιμες πληροφορίες στην οικογένεια του σχετικά με το που βρίσκεται ο ασθενής στο ED με αποτέλεσμα τη βελτίωση της ποιότητας της φροντίδας και τη βελτίωση της ικανοποίησης των ασθενών

• επίδραση στην ικανοποίηση των ED νοσοκόμων .

• επίδραση των μοναδικών αναγνωριστικών για την εκτέλεση σωστών διαδικασιών στο ED και X-ray τμήμα (θα πρέπει να σημειωθεί ότι οι ετικέτες φέρουν μόνο έναν αριθμό και το όνομα του ασθενούς, και ότι κανένας ασθενής δεν καταγράφει ιατρικές πληροφορίες σχετικά με την υγεία του).

Άλλα οφέλη:

• καλύτερη κατανόηση του τρόπου λειτουργίας του ακτινολογικού τμήματος

➢ Birmingham Heartlands Νοσοκομείο (UK): Τεχνολογία λήψεων αποφάσεων σε Παθητικό χειρουργείο

Το Birmingham Heartlands Νοσοκομείο (BHH) έχει μία από τις υψηλότερες επιδόσεις στο Ηνωμένο Βασίλειο.Το νοσοκομείο αυτό εισήγαγε ένα RFID σύστημα σε δύο BHH χειρουργικές πτέρυγες και υλοποίησε ένα Safe Surgery System, "Ασφαλές Χειρουργικό Σύστημα". Σ΄αυτό οι ασθενείς και το προσωπικό διαμορφώνουν μία ροη εντοπισμού και

διαχείρισης του περιβάλλοντος. Πρωταρχικός στόχος είναι η βελτίωση της ασφάλειας του προσωπικού και των ασθενών, η βελτίωση της περίθαλψης, καθώς και η αυτοματοποίηση της συγκέντρωσης και της μεταφοράς δεδομένων, μέσω της χρήσης των PDAs και των ηλεκτρονικών αρχείων των ασθενών. Το Safe Surgery System περιλαμβάνει μια ψηφιακή λίστα λειτουργίας, η οποία ενεργοποιεί την αυτοματοποιημένη αναγνώριση των ασθενών, την πρόληψη λάθους στα χειρουργεία, την αύξηση της αποδοτικότητας του νοσοκομείου, και τη μείωση της έκθεσης του νοσοκομείου σε δικαστικά έξοδα. Είναι μια παθητική pre-OR 'pre Operating Room' τεχνολογία υποστήριξης λήψεων αποφάσεων (στη διαχείριση των διαδικασιών και στο σύστημα αναγνώρισης) που χρησιμοποιοεί RFID βραχιόλια και ψηφιακή ταυτότητα με φωτογραφία που συνδέεται με ένα ηλεκτρονικό pre-operative κατάλογο ελέγχου.

Κόστος εφαρμογής

Για λόγους εμπιστευτικότητας τόσο το κόστος εφαρμογής όσο και της συντήρησης των συστημάτων δεν θα μπορούσε να αποκαλυφθεί. Το συνολικό κόστος υλοποίησης είναι £ 100.000 για περίοδο 12 μηνών πιλοτικά σε 2 θαλάμους, και θεωρείται ότι περιλαμβάνει το υλικό, το λογισμικό, την εκπαίδευση και το κόστος του επανασχεδιασμού της διαδικασίας. Μία κάπως διαφορετική εκτίμηση της κατανομής του συνολικού (εφαρμογή και συντήρηση) κόστους του Safe Surgery System είναι £ 4 ανά ασθενή για περισσότερο από μία χρονική περίοδο των τριών χρόνων .Η τελευταία αυτή εκτίμηση περιλαμβάνει την υπηρεσία διαχείρισης του έργου, τη διαμόρφωση, την εγκατάσταση (λογισμικού), τον έλεγχο και την εκπαίδευση των χρηστών. Τέλος, το κόστος της θερμικής εκτύπωσης στα βραχιόλια ανά είδος ανά ασθενή είναι £ 1.

Πλεονεκτήματα της εφαρμογής

Τα οφέλη ου προκύπτουν είναι η βελτίωση της ποιότητας της περίθαλψης και η μείωση της οικονομικής επιβάρυνσης από σφάλματα σε ασθενείς για μεμονωμένα νοσοκομεία και γενικά για το σύστημα υγείας. Για παράδειγμα, εκτιμάται ότι οι κλινικές πληρωμές αμέλειας από το NHS "National Health System" στην Αγγλία αναμένεται να αυξηθούν κατά 80% το 2010 σε £ 713 εκατομμύρια. Χαρακτηριστικό είναι ότι το ποσοστό προσφυγών στο δικαστήριο μπορεί να αποτελέσει το 1-2% του συνολικού εισοδήματος του νοσοκομείου. Η επίτευξη της μείωσης των λαθών μπορεί να είναι σημαντική εξοικονόμηση από τη μείωση των αποζημιώσεων του νοσοκομείου κατά 30%. Σε εθνικό επίπεδο αυτό μπορεί να ένα £ 213 εκατομμύρια μείωση σε κλινικές πληρωμές αμέλειας. Επίσης υπάρχουν οφέλη στην ποιότητα της περίθαλψης τα οποία μπορεί να περιλαμβάνουν την αποφυγή της αναντιστοιχίας μεταξύ των ασθενών και τη φροντίδα τους (493 αναφορές από 45 εκθέσεις εντοπίστηκαν από την Εθνική Υπηρεσία

Ασφάλειας των ασθενών) και βελτίωση της πρόληψης κατά 19% του νοσοκομείου με βάση τα ανεπιθύμητα συμβάντα όσο αφορά ασφάλεια των ασθενών.

Αύξηση της αποδοτικότητας:

Τα οφέλη που Safe Surgery System περιλαμβάνουν:

• Αύξηση της εισροής των ασθενών: βελτίωσης κατά 12-24% (ανά περίοδο)

Άλλα κέρδη αποτελεσματικότητας που συνδέονται με το Safe Surgery System που δεν έχουν ποσοτικά αξία περιλαμβάνουν:

• αύξηση του χρόνου του νοσηλευτικού προσωπικού ο οποίος κερδίζεται απο:

-Τον εντοπισμό του καταλόγου λειτουργίας και τον έλεγχο των ασθενών

-Τα διοικητικά καθήκοντα, αφού το σύστημα αυτόματα κωδικοποιεί τις διαδικασίες

• ικανοποίηση των νοσοκόμων του OR ‘Operating Room’.

Ποιοτικά κέρδη:

• βελτίωση της ασφάλειας των ασθενών, καθώς οι πτέρυγες χρησιμοποιούν Safe Surgery System

• ικανότητα εκτύπωσης ετικετών με το ID των ασθενών για ανάλυση του δείγματος που λαμβάνεται κατά τη διάρκεια της χειρουργικής επέμβασης.

Άλλα οφέλη:

• επιπτώσεις από την αυτοματοποίηση των μετρήσεων για την καθημερινή -εβδομαδιαία ανάλυση έχουν ως αποτέλεσμα:

- Ενοποιημένη αναφορά και βελτιωμένες επιδόσεις

- Βελτίωση της κλινικής διακυβέρνησης και πρόοδο στην ικανότητα ελέγχου (το σύστημα με βάση την άδεια που έχει επεξεργάζεται τα δεδομένα των ασθενών και τον προεγχειρητικό κατάλογο)

4.5 Συμπεράσματα

Το RFID στην υγειονομική περίθαλψη έχει μεγάλες δυνατότητες όσο αφορά τη μείωση των λειτουργικών δαπανών, τη βελτίωση των ιατρικών υπηρεσιών και την ασφάλεια των ασθενών. Η εμπειρία των κατασκευαστών και των εμπόρων λιανικής πώλησης στην εφαρμογή των RFID χρησιμεύει σε συμβουλευτικό επίπεδο, αλλά δεν μπορεί να εφαρμοστεί σε νοσοκομεία. Η επιτυχία ενός σχεδίου RFID εξαρτάται από τη στρατηγική, τη διαδικασία υλοποίησης, τα χαρακτηριστικά της τεχνολογίας, το οργανωτικό πλαίσιο, και από τους ενδιαφερόμενους, στους οποίους σίγουρα περιλαμβάνονται ιατροί και νοσηλευτές. Τα παραδείγματα που αναφέρθηκαν δείχνουν πώς το RFID αναπτύχθηκε για να καλύψει τις πρακτικές ανάγκες των ιατρικών υπηρεσιών σε ένα νοσοκομείο. Με μία στρατηγική ανάπτυξης μπορούν να δημιουργηθούν με επιτυχία συνεργασίες, όπως ενός νοσοκομείου, με μία εταιρία πληροφορικής και μία συμβουλευτική ομάδας.

Η συμμετοχή και του ιατρικού προσωπικού είναι επίσης κρίσιμη. Η επιτυχία των RFID σε νοσοκομεία απαιτεί ομαδική προσπάθεια. Η χρήση του RFID σε ένα νοσοκομείο μπορεί να συμβάλει στην αποτελεσματικότερη λειτουργία, στην καλυτέρευση των ιατρικών υπηρεσιών και στην ασφάλεια των ασθενών. Το RFID θα πρέπει να θεωρείται ως μέρος του Διαδικτύου των πραγμάτων. Ως υποδομή παρέχει μια πραγματική επιλογή για το νοσοκομείο και μπορεί να φέρει την επανάσταση σε αυτό και στις ιατρικές πρακτικές, αλλά δεν μπορεί να προσφέρει αξία από μόνη της αυτόματα σε ένα νοσοκομείο. Τα νοσοκομεία θα πρέπει να σκεφτούν πώς το RFID - Ίντερνετ των πραγμάτων μπορεί να βοηθήσει και υπό ποιες μορφές, πριν λάβουν οποιαδήποτε απόφαση σχετικά με αυτό.

4.6 Βιβλιογραφία

http://www.biomed.ntua.gr

Δ. Κουτσούρης, Κ. Νικήτα, Σ. Παυλόπουλος. Ιατρικά Απεικονιστικά Συστήματα. Εκδόσεις Τζιόλα,2004

Περδικούρη Μ., Γιόβας Π., Παπαδογιάννης Δ. & Συνεργάτες. Τηλειατρική στην πράξη, Εκδόσεις Εν πλω , 2005

Shang-Wei Wanga, Wun-Hwa Chenb, Chorng-Shyong Onga, Li Liuc, Yun-Wen Chuangb a Department of Information Management, National Taiwan University b Department of Business Administration, National Taiwan University c Graduate Institute of Medical Informatics, Taipei Medical University. RFID applications in hospitals: a case study on a demonstration RFID project in a Taiwan hospital, Presented at Hawaii International Conference on System Sciences,2006

CONSTANTIJN VAN ORANJE,REBECCA SCHINDLER, LORENZO VALERI, ANNA MARIEVILAMOVSKA, EVI HATZIANDREU,ANNALIJN CONKLIN. Study on the requirements and options for Radio Frequency Identification (RFID) application in healthcare, www.ehealthserver.com,2009

Hongwei Du, Ben Bradford Rostam Assadi-Shehni. E-HEALTHCARE,www.ieee.com, 2003

Belal Chowdhury, Rajiv Khosla. RFID-based Hospital Real-time Patient Management System,www.3icare.com, 2005

Κεφάλαιο 5ο

Μελέτη

5.1 Παρουσίαση

Σ' αυτό το κεφάλαιο παρουσιάζεται μια μελέτη εφαρμογής της τεχνολογίας του Διαδικτύου των πραγμάτων σε συσκευές υγείας για την κατ' οίκον ιατρική παρακολούθηση των ασθενών. Χρησιμοποιήθηκαν συσκευές υγείας εξοπλισμένες με έξυπνες ετικέτες RFID και καθώς επίσης σταθεροί αναγνώστες RFID. Για το σχεδιασμό της αρχιτεκτονικής του συστήματος εφαρμόστηκαν οι αρχές που αναφέρθηκαν στα προηγούμενα κεφάλαια. Παρακάτω ακολουθεί περιγραφή του προβλήματος, απαρίθμηση σεναρίων χρήσης, λειτουργικών απαιτήσεων, χαρακτηριστικών ποιότητας, αρχιτεκτονικών δικτύου, εναλλακτικών λύσεων και προκλήσεων.

Το σύστημα αυτό έχει αναπτυχθεί για διαχείριση και παρακολούθηση. Παρέχει υπηρεσίες που ωφελούν τον υπό παρακολούθηση ασθενή στη συλλογή και στη μετάδοση ιατρικών δεδομένων, καθώς ενημερώνει το συνδρομητή (ιατρό) σχετικά με την κατάσταση της υγείας του ασθενούς. Επιπλέον αλληλεπιδρά με άλλα συστήματα με σκοπό την σύνταξη εκθέσεων και τη λήψη αποφάσεων σχετικά με την καταλληλότερη θεραπεία που θα πρέπει να ακολουθήσει ο ασθενής.

5.2 Περιγραφή προβλήματος

Ένα από τα βασικά προβλήματα κατά την παροχή της ιατρικής περίθαλψης είναι η συμφόρηση ασθενών στα νοσοκομεία τόσο στον τομέα των επειγόντων περιστατικών όσο και στον τομέα των κλινικών.

Ένας από τους κύριους λόγους που συμβαίνει αυτό είναι η ανάγκη να προταθεί από την ιατρό μία αποτελεσματική θεραπεία. Για να γίνει αυτό θα πρέπει ο ασθενής να παρακολουθηθείτε για ένα χρονικό διάστημα συνήθως κάποιων ημερών κατά το οποίο πρέπει να γίνονται και να καταγράφονται συχνά μετρήσεις ορισμένων βιοσημάτων όπως είναι η αρτηριακή πίεση, το ποσοστό γλυκόζης στο αίμα, η θερμομέτρηση και η οξυμέτρηση.

Ένας άλλος λόγος που συμβαίνει αυτό είναι ότι ασθενείς με χρόνιες παθήσεις που σχετίζονται με τα παραπάνω βιοσήματα είναι υποχρεωμένοι να νοσηλεύονται κάποιες μέρες το χρόνο για προγραμματισμένη παρακολούθηση της κατάστασης της υγείας τους.

Επίσης, σε κάποιες περιπτώσεις ορισμένοι ασθενείς από μια και μόνη μέτρηση των παραπάνω βιοσημάτων που είναι εκτός των φυσιολογικών ορίων, κάνοντας χρήση των προσωπικών τους συσκευών υγείας, και χωρίς να επαναλάβουν τις μετρήσεις για ένα διάστημα μερικών ωρών, ίσως και ημερών, σπεύδουν άμεσα στα εφημερεύοντα νοσοκομεία.

Όλη αυτή η μετακίνηση των ασθενών από το σπίτι τους στο εκάστοτε νοσοκομείο αυξάνει το κόστος τόσο των ασθενών όσο και των ίδιων των νοσοκομείων. Οι ασθενείς επιβαρύνονται με τα έξοδα των μετακινήσεων, της νοσηλείας τους καθώς επίσης και με το κόστος απουσίας τους από τις εργασίες τους. Από την άλλη τα νοσοκομεία επιβαρύνονται με την αγορά επιπρόσθετου εξοπλισμού και τη δημιουργία επιπρόσθετων εξεταστηρίων για την κάλυψη των αυξημένων αναγκών, καθώς και με το κόστος της συντήρησης των μηχανημάτων και της αναμενόμενης διάρκειας ζωής του εξοπλισμού. Επίσης απαιτείται αύξηση του χρόνου που πρέπει να αφιερώσει το ιατρικό-νοσηλευτικό προσωπικό στον κάθε ασθενή, το οποίο κατ' επέκταση υποβαθμίζει την ιατρική περί-θαλψη εφόσον δεν είναι δυνατό να δοθεί η απαραίτητη προσοχή στους πραγματικά έχοντες ανάγκη ασθενείς.

Από την άλλη μεριά σε μερικές περιπτώσεις που η μετακίνηση αυτή είναι θεμιτή και απαραίτητη δεν είναι πάντοτε εφικτή. Κάποιοι ασθενείς, δηλαδή ενώ πρέπει, δεν μπορούν να έχουν πρόσβαση στα νοσοκομεία είτε λόγω κινητικών προβλημάτων είτε λόγω απόστασης.

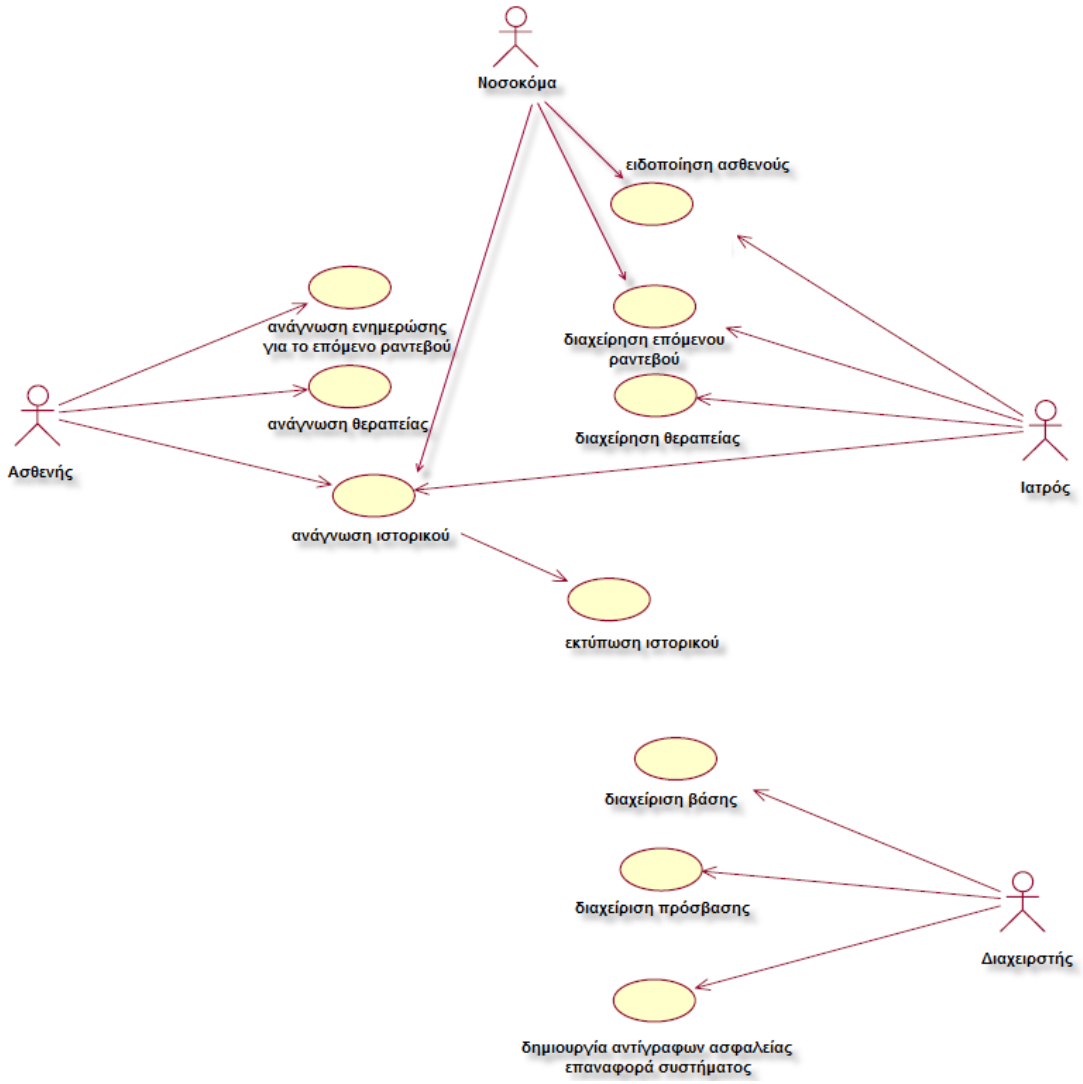
Ένα άλλο πρόβλημα της ιατρικής περίθαλψης είναι ότι ορισμένοι ασθενείς παραλείπουν ή δεν μπορούν να κρατήσουν ιστορικό με τα αποτελέσματα των μετρήσεων από τις προσωπικές τους συσκευές υγείας. Ακόμα κι αν αυτό επιτευχθεί το ιστορικό δίνεται και καταχωρείται μόνο από τον θεράποντα ιατρό τους και μόνο σε ένα συγκεκριμένο νοσοκομείο με αποτέλεσμα να μην είναι προσπελάσιμο από άλλους γιατρούς άλλων νοσοκομείων.

Υπάρχει επίσης μια κατηγορία ασθενών που παρόλο που της έχει δοθεί κάποια θεραπεία, η οποία όμως δεν έχει τα αναμενόμενα αποτελέσματα, (είτε γιατί οι ασθενείς δεν την ακολουθούν σωστά είτε γιατί δεν την ολοκληρώνουν) με αποτέλεσμα να είναι στάσιμη η πορεία της υγείας τους ή ακόμα και να χειροτερεύει, δεν ειδοποιεί το γιατρό της. Σε μερικές περιπτώσεις τα επίπεδα των βιοσημάτων των ασθενών αυτών φτάνουν σε κρίσιμα επίπεδα χωρίς οι ίδιοι να το αντιλαμβάνονται είτε λόγω άγνοιας των φυσιολογικών ορίων είτε λόγω αδιαφορίας. Μάλιστα σε ορισμένες περιπτώσεις αν είχε ενημερωθεί έγκαιρα ο γιατρός θα μπορούσε να αντιμετωπιστεί η κατάσταση χωρίς να χαθεί πολύτιμος χρόνος στη μετακίνηση από τον ίδιο τον ασθενή λαμβάνοντας κάποιο χάπι (πχ για την αυξημένη πίεση) ή κάνοντας κάποια ένεση (πχ ινσουλίνη).

Τέλος, ασθενείς που χρειάζονται παρακολούθηση από εξειδικευμένους γιατρούς αποφεύγουν τη νοσηλεία τους σε νοσοκομείο λόγω της ψυχολογικής φόρτισης (άγχος, φόβος) που τους προκαλεί η παραμονή τους σε αυτό. Ακόμα και αν νοσηλευτούν τις περισσότερες φορές δεν είναι συνεργάσιμοι με το ιατρικο-νοσηλευτικό προσωπικό.

5.3 Σενάρια χρήσης

Το παρακάτω διάγραμμα συντελεί στην παρουσίαση ολόκληρου του συστήματος της κατ' οίκον ιατρικής παρακολούθησης ασθενών καθώς επίσης και στην κατανόηση των προβλημάτων που προκύπτουν από αυτό. Πρέπει να τονιστεί ότι σε αυτή την ενότητα, δεν αναλύονται η εφαρμογή και οι σχετικές τεχνολογίες (η επιτυχία αυτών θα αναλυθεί σε επόμενα κεφάλαια). Οι ουσιαστικοί χρήστες του συστήματος είναι ο ασθενής, ο ιατρός, η νοσοκόμα και τέλος ο διαχειριστής.



Εικόνα 5.1: Διάγραμμα συστήματος κατ' οίκον ιατρικής παρακολούθησης ασθενών

Η όλη ιδέα του συστήματος βασίζεται στην ανάγκη τόσο ο ιατρός όσο και το νοσηλευτικό προσωπικό να μπορούν να παρακολουθούν ανά πάσα στιγμή το ιστορικό με τις μετρήσεις των βιοσημάτων του ασθενούς που ο ίδιος έχει λάβει σπίτι του με τις προσωπικές του συσκευές υγείας.

Οι ενδιαφερόμενοι χρήστες (ασθενής, ιατρός, νοσοκόμα και διαχειριστής) έχουν όλοι τη δυνατότητα να συνδεθούν στο πληροφοριακό σύστημα και να αποκτήσουν πρόσβαση σε αυτό, μέσω του τοπικού δκτύου του νοσοκομείου 'τοπικά' ή μέσω του διαδικτύου 'απομακρυσμένα', ο καθένας τους όμως σε διαφορετικό τομέα.

Ο ασθενής επιτρέπεται να δει από το πληροφοριακό σύστημα το ιστορικό με τις μετρήσεις του και να το εκτυπώσει ώστε να μπορεί να έχει και ο ίδιος μια γενική εικόνα της πορείας της υγείας του ανά πάσα στιγμή. Επίσης, μπορεί να διαβάσει τη θεραπεία που πιθανόν του έχει συντάξει ο θεράπων ιατρός του σύμφωνα με το ιστορικό του. Μια ακόμη δυνατότητα που έχει ο ασθενής είναι να ενημερωθεί από το σύστημα πότε έχει προγραμματιστεί το επόμενο ραντεβού του, ημερομηνία που θα ορίζει και πάλι ο γιατρός του σύμφωνα με το πόσο επείγει να εξετάσει τον ασθενή από κοντά, κρίνοντας πάντα από τα επίπεδα των βιοσημάτων του.

Ο ρόλος του γιατρού δε διαφέρει πολύ από τον συνηθισμένο. Η μόνη διαφορά έγκειται στο ότι δεν έρχεται σε άμεση επαφή με τον ασθενή. Παρόλα αυτά τον παρακολουθεί πολύ πιο συχνά και ενημερώνεται για τις μεταβολές της υγείας του. Ο γιατρός μέσω του πληροφοριακού συστήματος μπορεί να εκτυπώσει και αυτός το ιστορικό του ασθενή για να έχει μια πλήρη εικόνα γι΄αυτόν. Όταν το κρίνει απαραίτητο επεμβαίνει ηλεκτρονικά είτε προτείνοντας κάποια αλλαγή στη θεραπεία του ασθενούς είτε αντικατάστασή της με μια νέα πιο αποτελεσματική είτε ακόμα καλώντας τον ασθενή για εξέταση στο νοσοκομείο ορίζοντας του μέσω του συστήματος κάποιο ραντεβού.

Οι δυνατότητες πρόσβασης της νοσοκόμας στο σύστημα περιορίζονται πρώτον στην εκτύπωση του ιστορικού των βιοσημάτων του ασθενούς ώστε σε περίπτωση νοσηλείας του να μπορεί να ενσωματωθεί στον ιατρικό του φάκελο και δεύτερον στην ενημέρωση του ασθενούς για το επόμενο ραντεβού του με το γιατρό ή ακόμα και για πιθανή αλλαγή της ημερομηνίας. Τέλος, η νοσοκόμα μπορεί και με άλλους τρόπους επικοινωνίας (πχ μέσω κάποιου μηνύματος στο κινητό του ασθενούς) πέρα του πληροφοριακού συστήματος, ώστε να μην καθυστερήσει να δει ή να μην δει καθόλου, να ειδοποιήσει τον ασθενή σε περίπτωση άμεσης και έκτακτης νοσηλείας του στο νοσοκομείο. Αυτό μπορεί να το κάνει και ο γιατρός αλλά συνήθως αποτελεί δουλειά της νοσοκόμας.

Τέλος, το όλο σύστημα προκειμένου να διαχειριστεί σωστά από τεχνικής πλευράς, είναι απαραίτητος και ένας διαχειριστής. Αυτός είναι ο μόνος που θα μπορεί να διαχειρίζεται τη βάση δεδομένων του συστήματος, να κάνει backup και ανάκτηση των δεδομένων του ασθενούς και να ελέγχει την πρόσβαση των χρηστών σε διάφορες άλλες υπηρεσίες του συστήματος.

5.3.1 Παράδειγμα χρήσης

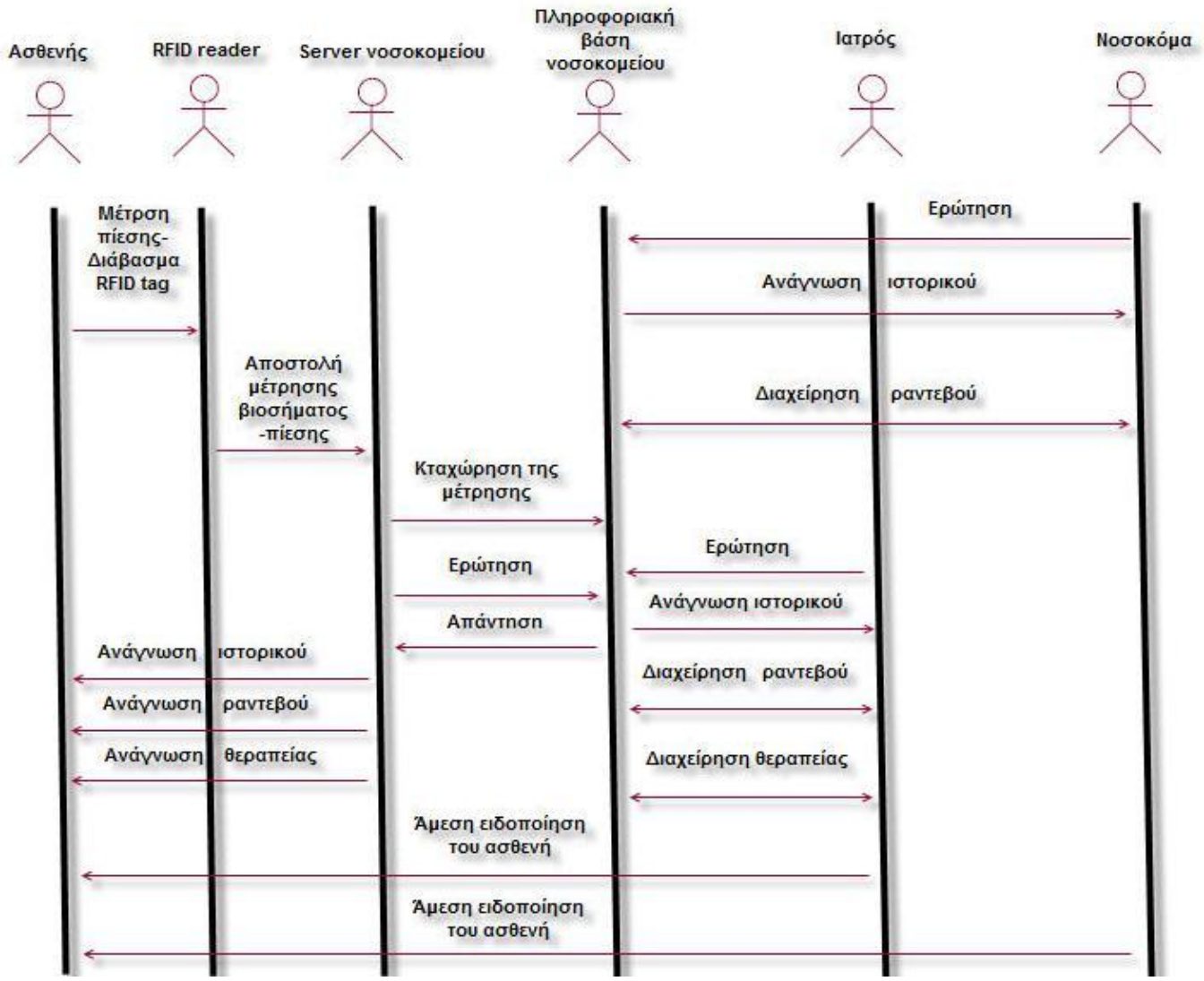
Ένα χαρακτηριστικό παράδειγμα χρήσης του παραπάνω συστήματος είναι από κάποιον ασθενή μεσαίας ηλικίας που πάσχει από χρόνια υψηλή αρτηριακή πίεση, μένει σε χωριό αρκετά μακριά από κάποιο νοσοκομείο που να έχει καρδιολόγο, γεγονός που τον περιορίζει όσον αφορά τις κατ' ιδίαν επισκέψεις για παρακολούθηση στον γιατρό, και επιπλέον δε διαθέτει ηλεκτρονικό υπολογιστή.

Ο ασθενής αυτός το μόνο που διαθέτει είναι ένα πιεσόμετρο εξοπλισμένο με RFID έξυπνες ετικέτες οπότε δε χρειάζεται να υποβάλλεται τόσο συχνά σε μετακινήσεις. (οι τεχνολογικές απαιτήσεις θα αναλυθούν σε επόμενη παράγραφο).

Το παρακάτω σχήμα δείχνει πλήρως την ροή των πληροφοριών κατά την χρήση του συστήματος από όλους τους παράγοντες. Αναλυτικότερα όταν ο ασθενής μετρήσει την πίεση του με την προσωπική συσκευή υγείας του τότε αυτόματα αυτή συγχρόνως διαβάζεται από μία συσκευή ανάγνωσης RFID. Η μέτρηση αυτή προωθείται στην συνέχεια στον server του νοσοκομείου όπου ανήκει ο θεράπων ιατρός του ασθενούς. Εκεί πλέον τοπικά καταχωρείται σε μία πληροφοριακή βάση του νοσοκομείου όπου ήδη υπάρχει μία εγγραφή του ασθενούς με τα στοιχεία του, προηγούμενες μετρήσεις του, παλιά του ραντεβού καθώς και με τη θεραπεία που ακολουθεί την τρέχουσα περίοδο. Από εκείνη την στιγμή και μετά η μέτρηση πλέον είναι στη διάθεση των αρμόδιων δηλαδή όσων έχουν πρόσβαση στο πληροφοριακό σύστημα.

Ο ιατρός, πιθανόν καρδιολόγος στην συγκεκριμένη περίπτωση, καθώς πραγματοποιεί τον προγραμματισμένο ιατρικό έλεγχο όσων ασθενών παρακολουθούνται από το σύστημα, ζητά από την βάση και ελέγχει το ιστορικό του συγκεκριμένου ασθενούς. Αν κατά την διάρκεια αυτού κριθεί ότι πρέπει επισπεύσει την ήδη προγραμματισμένη επίσκεψη του ασθενούς στο νοσοκομείο ή να οριστεί νέα τότε ο γιατρός μέσω του πληροφοριακού συστήματος επικοινωνεί πάλι με την βάση και διαχειρίζεται την ημερομηνία για το ραντεβού του ασθενούς του. Την διαχείριση αυτή μπορεί να την κάνει και κάποια νοσοκόμα κατόπιν εντολής του γιατρού.

Σε μια όμως τέτοια περίπτωση υπάρχει το εξής πρόβλημα· ο ασθενής του παραδείγματος όπως αναφέρθηκε και παραπάνω δεν έχει ηλεκτρονικό υπολογιστή άρα θα πρέπει να ενημερωθεί άμεσα μέσω κάποιου άλλου τρόπου επικοινωνίας όπως για παράδειγμα να τον καλέσουν στο τηλέφωνο και να τον ενημερώσουν για την αλλαγή ή για την ανάγκη δημιουργίας κάποιου νέου ραντεβού. Αυτή την ενημέρωση μπορεί να την κάνει είτε ο γιατρός είτε η νοσοκόμα.



Εικόνα 5.2: Διάγραμμα ροής των πληροφοριών κατά την χρήση του συστήματος κατ' οίκον ιατρικής παρακολούθησης

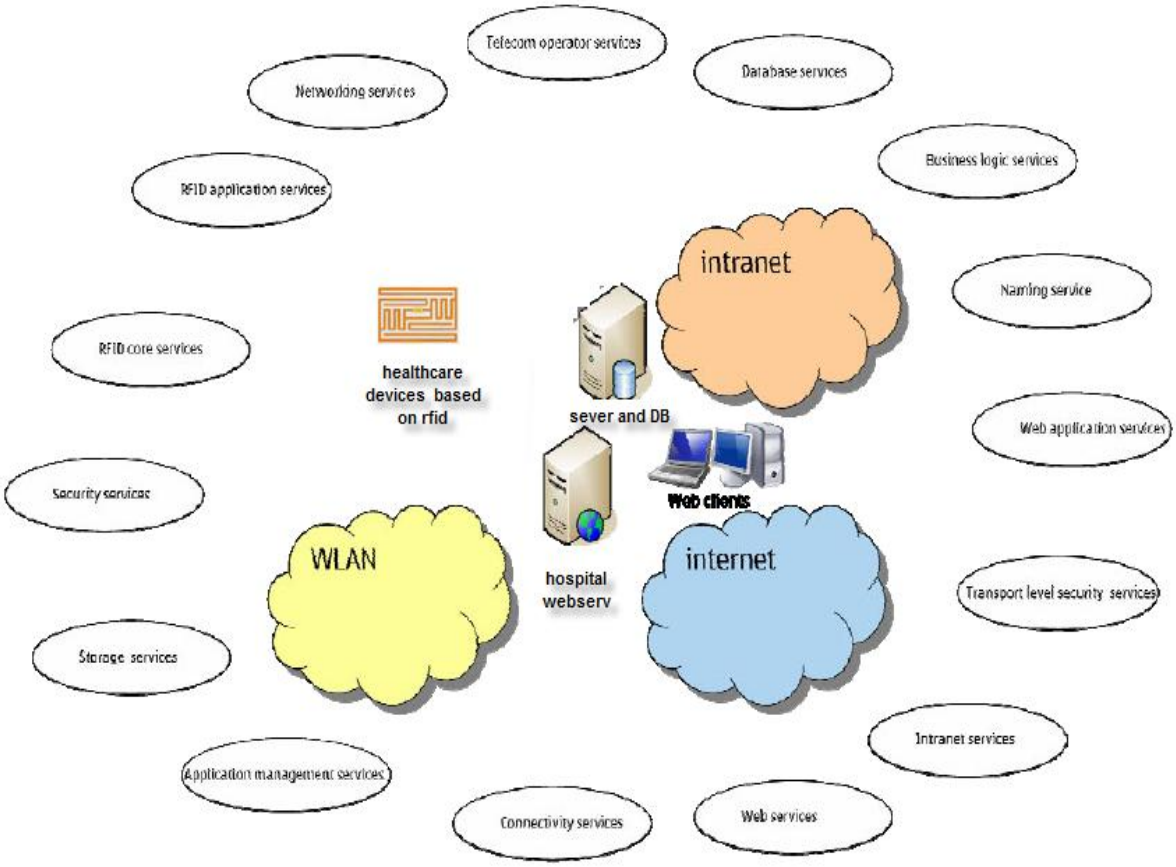
Επίσης υπάρχει περίπτωση η μέτρηση που θα ληφθεί από τον συγκεκριμένο ασθενή να είναι εκτός των φυσιολογικών ορίων, δηλαδή να παρουσιάσει πολύ αυξημένη αρτηριακή πίεση. Τότε κατά την καταχώρηση αυτής στη βάση δεδομένων ειδοποιείται άμεσα το νοσοκομείο.

Ο γιατρός που έχει πρόσβαση στη βάση δεδομένων σε μια τέτοια κατάσταση αντιμετωπίζει τον ασθενή σαν έκτακτο περιστατικό και ο ίδιος κρίνει πως θα το αντιμετωπίσει. Μπορεί να επικοινωνήσει με τον ασθενή και να του ζητήσει να πιει κάποιο χάπι το οποίο άμεσα και γρήγορα να του μειώσει την πίεση ώστε να μην χαθεί πολύτιμος χρόνος και όταν συνέλθει αν είναι σε θέση να πάει μόνος του στο νοσοκομείο για την περαιτέρω νοσηλεία του διαφορετικά να γίνει διακομιδή.

5.4 Επισκόπηση Συστήματος

Μέχρι τώρα έχουν αναφερθεί τα προβλήματα της υγειονομικής περίθαλψης και οι πιθανές χρήσεις του συστήματος. Το μοντέλο δικτύου που επιλέχτηκε γα το σύστημα παρουσιάζεται στο παρακάτω διάγραμμα. Αυτού του είδος η αρχιτεκτονική δίνει στο σύστημα την προοπτική της διαμόρφωσης του δικτύου.

Στο κέντρο του διαγράμματος βρίσκονται οι εξής συσκευές: συσκευές ανάγνωσης RFID, οι ετικέτες RFID, ο server με τις βάσεις δεδομένων, διάφοροι υπολογιστές φορητοί και μη, σταθμοί εργασίας-πελάτες. Αυτές συνδέονται με διάφορα δίκτυα όπως το internet, το intranet, το WLAN.



Εικόνα 5.3: Μοντέλο δικτύου

5.4.1 Διαμόρφωση Δικτύου

Το σύστημα πρέπει να χρησιμοποιεί ένα κατανεμημένο μοντέλο αρχιτεκτονικής υπηρεσιών, με τις υπηρεσίες σε διάφορα δίκτυα και γεωγραφικές τοποθεσίες.

Τα βασικά στοιχεία του δικτύου είναι:

backend server

server βάσεων δεδομένων

intranet

internet

έξυπνη συσκευή ανάγνωσης RFID

ετικέτες RFID

RFID gateway

lan gateway

local registry center

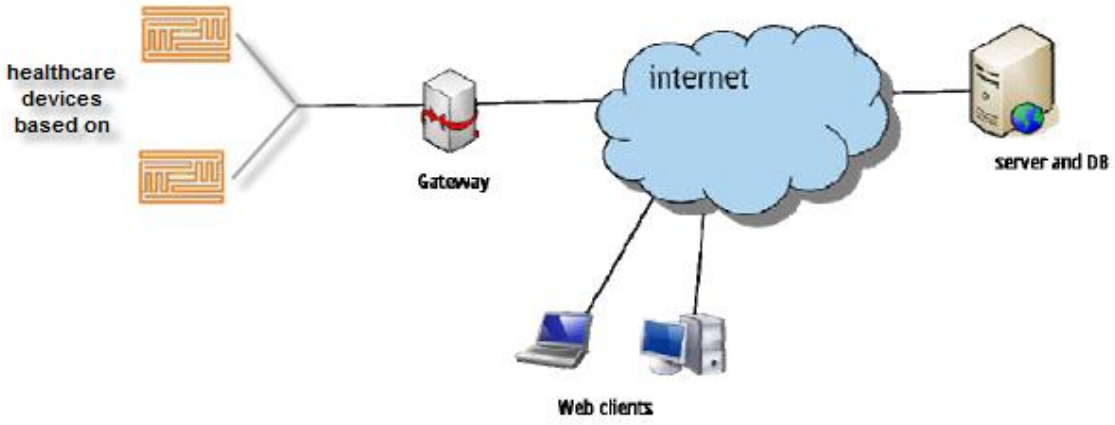
global registry center

Ένας backend server χρησιμοποιείται στο νοσοκομείο για να εκτελούνται backend εφαρμογές και υπηρεσίες web. Επίσης ένας server βάσης δεδομένων χρησιμοποιείται για να φιλοξενήσει τις αντίστοιχες υπηρεσίες. Το intranet παρέχει όλες τις υπηρεσίες της τοπικής επικοινωνίας είτε για επικοινωνία στο νοσοκομείο είτε στο σπίτι του ασθενούς. Στο νοσοκομείο είναι συνδεδεμένοι οι αρμόδιοι γιατροί και το νοσηλευτικό προσωπικό ενώ στον ασθενή συνδέονται οι συσκευές υγείας. Οι γιατροί μπορούν επίσης να αποκτήσουν πρόσβαση στις ενδοδικτυακές υπηρεσίες από το Διαδίκτυο μέσω VPN όταν βρίσκονται εκτός νοσοκομείου. Ενώ οι νοσοκόμες από το Διαδίκτυο δεν έχουν καθόλου πρόσβαση στο intranet για λόγους ασφαλείας.

5.4.2 Internet

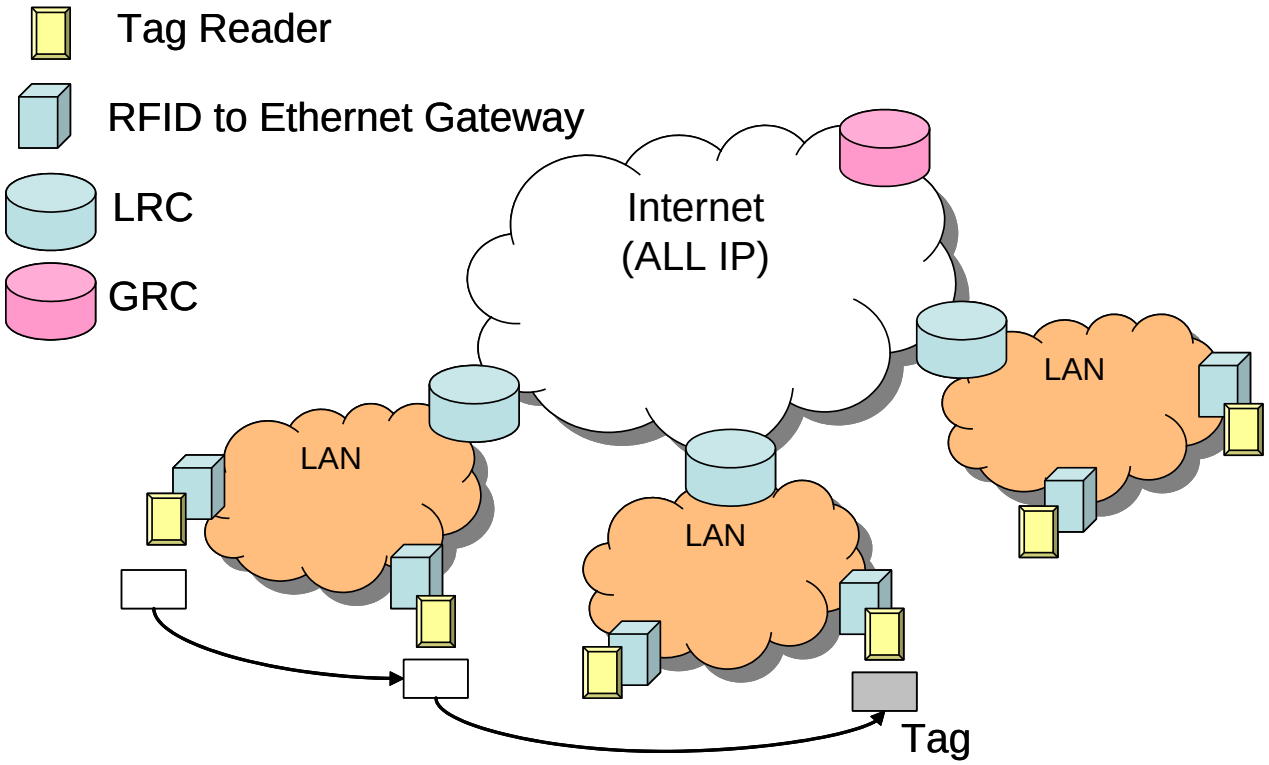
Ο server, η βάση δεδομένων του νοσοκομείου όσο και όλες οι συσκευές της υγειονομικής περίθαλψης είναι συνδεδεμένα με το δημόσιο διαδίκτυο. Επίσης συνδεδεμένοι με το δημόσιο διαδίκτυο είναι οι web clients και το Global Registration Center.

Η μορφή φαίνεται στο παρακάτω σχήμα:



Εικόνα 5.4: Διάγραμμα διασύνδεσης με το Internet

Το Global Registration Center είναι μια παγκόσμια βάση στην οποία καταχωρούνται όλα τα ID των RFID ετικετών. Επίσης όλα τα hosts είτε αυτά είναι στο νοσοκομείο είτε στον ασθενή είναι dual stack ipv6/ipv4 δηλαδή υποστηρίζουν και ipv6 και ipv4 με προτίμηση όμως στο πρώτο. Οι συσκευές υγείας συνδέονται με το διαδίκτυο μέσω ενός rfid gateway ενός lan gateway αλλά αυτό θα αναλυθεί καλύτερα στην επόμενη ενότητα το οποίο αναφέρεται στο intranet.



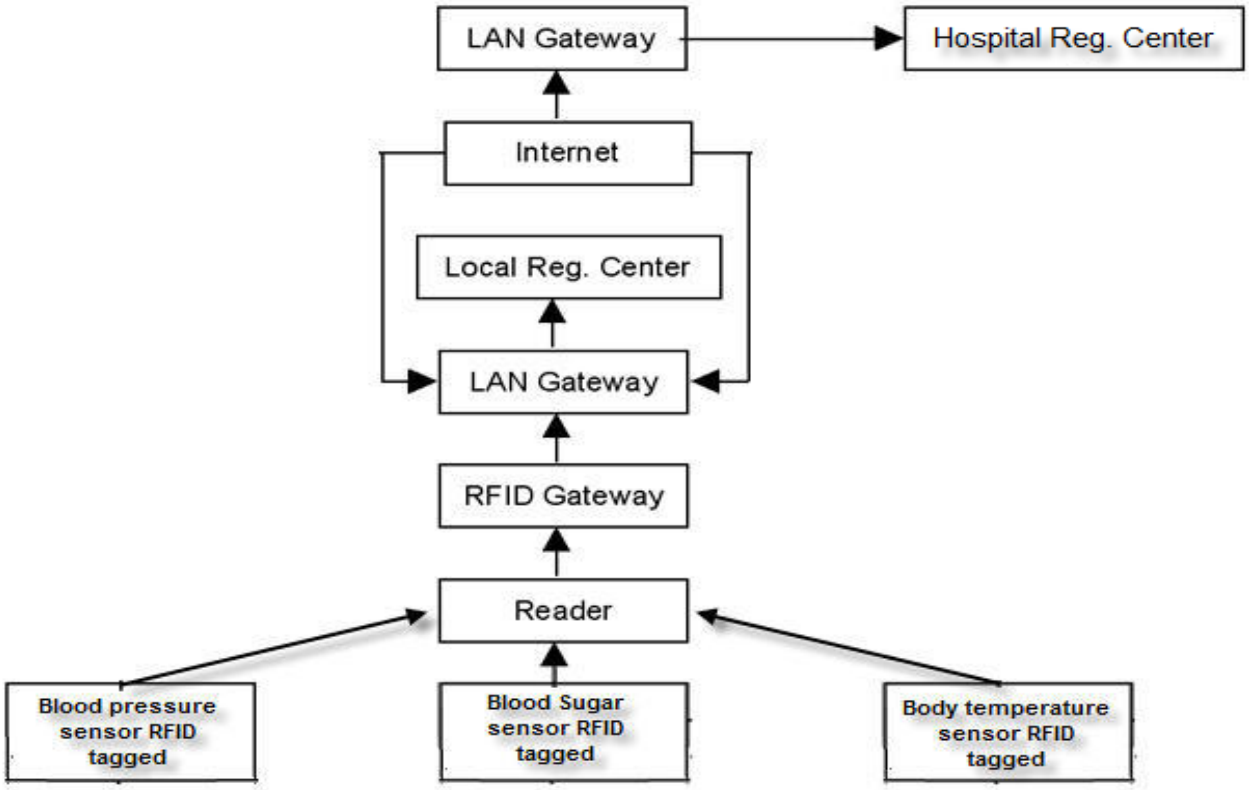
Εικόνα 5.5: Dual stack Ipv6/Ipv4

5.4.3 Intranet

Το τοπικό δίκτυο που έχει να αξία να αναλυθεί είναι αυτό στο σπίτι του ασθενούς το οποίο αποτελείται από τα εξής:

- Συσκευές υγείας εξοπλισμένες με RFID ετικέτες
- Συσκευή ανάγνωσης RFID
- Ένα RFID Gateway
- Ένα Lan Gateway
- Ένα Local Registration Center

Η δομή του intranet δικτύου του ασθενούς φαίνεται στο παρακάτω διάγραμμα:



Εικόνα 5.6: Δομή του intranet δικτύου

Επιλέχθηκε αυτή η δομή ώστε το σύστημα να μπορεί να εκμεταλλευτεί πλήρως τα πλεονεκτήματα του IPv6 και του RFID. Για να κατανοηθεί πλήρως πως αυτά μπορούν να συνδυαστούν και να αποδώσουν τα μέγιστα κρίνεται απαραίτητο να επαναληφθούν κάποια χαρακτηριστικά της δομής και της λειτουργίας τόσο του IPv6 όσο και του RFID.

Το RFID είναι μια ασύρματη τεχνολογία απομακρυσμένης αναγνώρισης η οποία μπορεί να ανακτά δεδομένα χρησιμοποιώντας ετικέτες RFID ή αναμεταδότες. Οι ετικέτες RFID κάνουν χρήση ολοκληρωμένων κυκλωμάτων και κεραιών για την παρακολούθηση αντικειμένων από απόσταση. Το ολοκληρωμένο κύκλωμα έχει ένα μοναδικό αναγνωριστικό για κάθε στοιχείο για την εξακρίβωση της ταυτότητας του μέσω ραδιοκυμάτων.

Το τσιπ δεν βοηθά μόνο στην αποθήκευση και επεξεργασία πληροφοριών, αλλά και τη διαφοροποίηση και την αποδιαμόρφωση των σημάτων RF. Η κεραία βοηθά στη λήψη

και μετάδοση των σημάτων. Ένας αναγνώστης RF μπορεί να διαβάσει κάθε ετικέτα εντός εμβέλειας.

Υπάρχουν τριών ειδών ετικέτες RFID: παθητικές, ενεργητικές, και ημιπαθητικές. Με βάση τα χαρακτηριστικά τους, αυτές χρησιμοποιούνται για ειδικούς σκοπούς παρακολούθησης. Στην περίπτωση του υπό μελέτη συστήματος επιλέχθηκαν ενεργητικές ετικέτες οι οποίες ήδη έχουν ενσωματωθεί στις συσκευές υγείας.

Tags and Features	Passive Tag	Active Tag	Semi Passive Tag
Internal Power Source	No	Yes	Yes
Signal by backscattering the carrier wave from the reader	Yes	No	Yes
Response	Weaker	Stronger	Stronger
Size	Small	Big	Medium
Cost	Less expensive	More expensive	Less
Potential Shell life	Longer	Shorter	Longer
Range	10 centimeters to few meters	Hundreds of meters	Hundreds of meters
Sensors	No	Yes	Yes

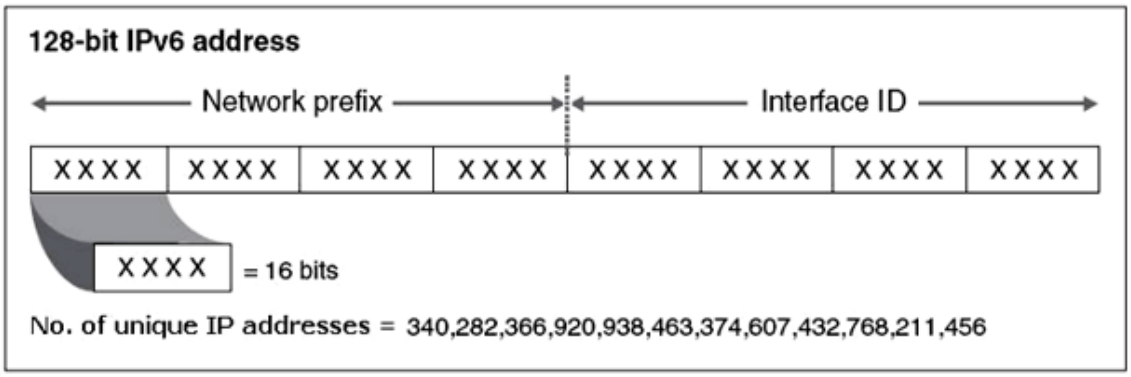
Πίνακας 5.1: Είδη και χαρακτηριστικά των ετικετών RFID

Μια ετικέτα RFID αντιπροσωπεύεται από ένα EPC (Electronic Product Code), που διαχειρίζεται σήμερα από το EPCglobal. Είναι είτε ένα 64-bit ή 96-bit αναγνωριστικό το οποίο είναι κατακερματισμένο σε τέσσερα τμήματα.

Header	EPC Manager	Object Class	Serial Number
36	28	24	36

- Header: Προσδιορίζει τον αριθμό έκδοσης EPC και επιτρέπει διαφορετικά μήκη ή είδη της EPC, όπως είναι Τύπος I, Τύπος II, Τύπος III, Τύπος IV.
- EPC Manager: Προσδιορίζει τον κατασκευαστή του προϊόντος του EPC.
- Object Class: Προσδιορίζει τον ακριβή τύπο του προϊόντος
- Serial Number: Προσδιορίζει το μοναδικό αναγνωριστικό του στοιχείου.

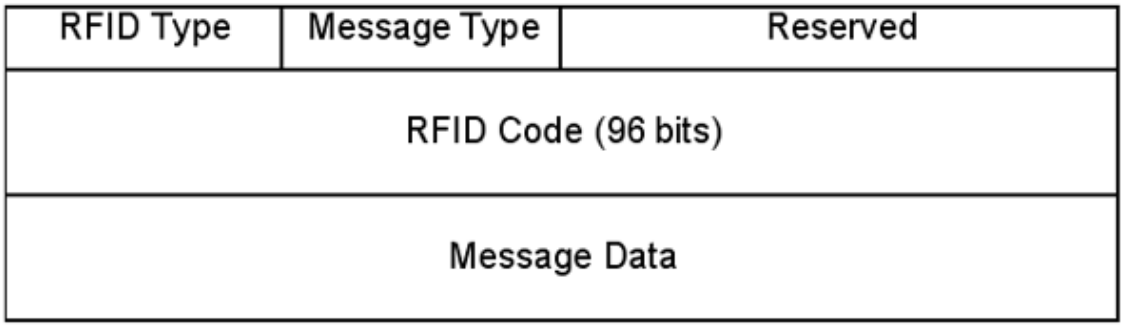
Το IPv6 είναι ένα πρωτόκολλο που παρέχει end-to-end σύνδεση με χώρο διευθύνσεων 128 bit. Βοηθά IP-δικτυωμένες συσκευές να επικοινωνούν μεταξύ τους με ασφάλεια και να δίνονται συγκεκριμένες διευθύνσεις σε κάθε μία από αυτές τις συσκευές. Το IPv6 εξασφαλίζει την αντιμετώπιση του προβλήματος της στενότητας των μελλοντικών δικτύων που θα βασιστούν σε αυτό.



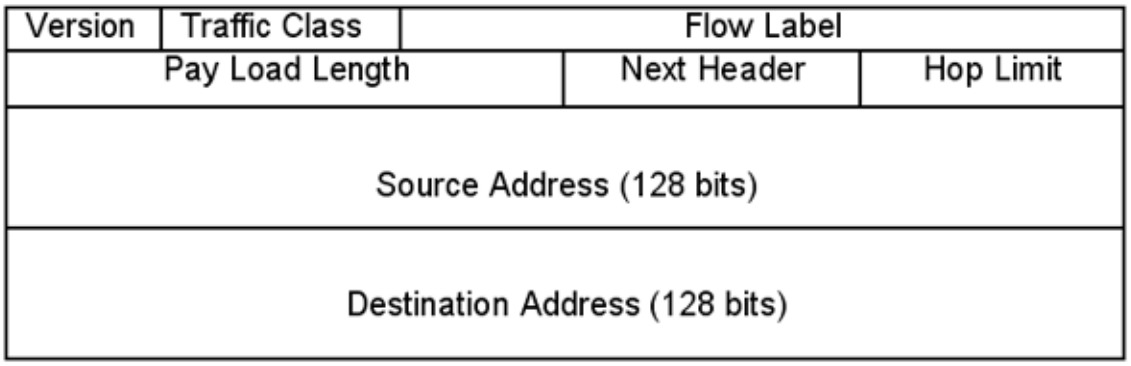
Εικόνα 5.7: IPv6 πρωτόκολλο με χώρο διευθύνσεων 128 bit.

Τα πρώτα 64 bits είναι για το υποδίκτυο και τα τελευταία 64 bits είναι για το interface ID. Στους τύπους των διευθύνσεων περιλαμβάνονται και οι Unicast, Multicast και Anycast τύποι. Οι Unicast τύποι ανατίθενται σε ενιαίο δίκτυο ενώ οι Multicast και Anycast καταχωρούνται σε δίκτυο που έχει πολλαπλές διασυνδέσεις.

Στα επόμενα διαγράμματα φαίνονται η δομή του RFID μηνύματος και του IPv6:

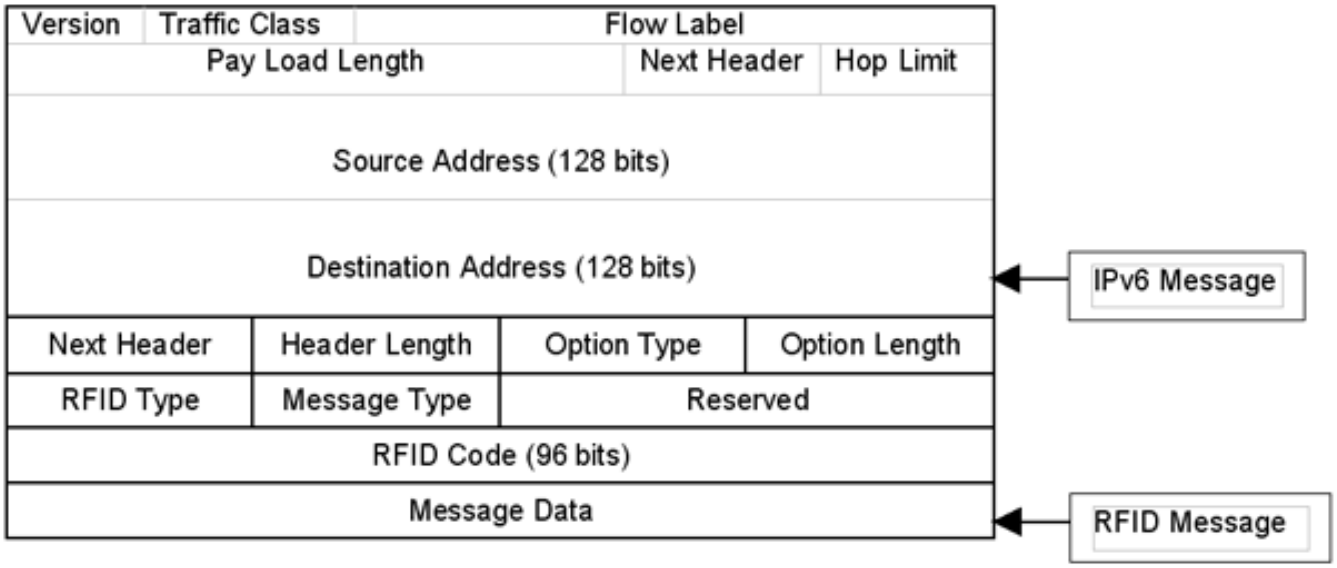


Εικόνα 5.8: Δομή RFID μηνύματος



Εικόνα 5.9: Δομή IPv6

Οι δομές των διευθύνσεων τους ταιριάζουν χωρίς καμία απώλεια λειτουργικότητας. Στο EPC, ο χώρος του RFID είναι 60 bits με 28 bits object class και 32 bits serial number, ενώ ένα υποδίκτυο IPv6 μπορεί να χωρέσει ολόκληρο τον χώρο αυτό. Με μια τέτοια συγχώνευση, το RFID Object Class και Serial Number γίνεται το IPv6 Interface ID. Με αυτό τον τρόπο κάθε ετικέτα RFID μπορεί να αντιπροσωπευθεί και να είναι προσπελάσιμη σε ένα δίκτυο IPv6. Με το συνδυασμό των τεχνολογιών RFID και IPv6, τα πάντα μπορούν να παρακολουθούνται.



Εικόνα 5.10: Ενσωμάτωση RFID στο IPv6

5.4.4 Πως λειτουργεί το σύστημα

Ο ασθενής μόλις μετρήσει κάποιο βιοσήμα με κάποια από τις προσωπικές συσκευές υγείας αυτό μεταδίδεται μέσω rf κυμάτων στο RFID reader. Αυτός με την σειρά του το προωθεί στο RFID Gateway όπου και επεξεργάζεται κατάλληλα.

Στο επόμενο επίπεδο υπάρχει το Lan Gateway όπου αναλαμβάνει να συνδέσει τα δεδομένα με το Local Registry Center και όλο το σύστημα με το Διαδίκτυο. Το Lan - RFID Gateway είναι ουσιαστικά επιφορτισμένο με την συγχώνευση του RFID στο IPv6 και κατ' επέκταση με τη διευθυνσιοδότηση όλων των συσκευών υγείας του ασθενούς.

5.4.5 Απαιτήσεις ασφάλειας

Η ασφάλεια στο σύστημα που αναλύθηκε είναι πρωταρχικός στόχος. Είναι φανερή η ανάγκη για διατήρηση του απορρήτου και της ακεραιότητας των δεδομένων που ανταλλάσσονται μεταξύ των ασθενών και του νοσοκομείου. Η φύση των δεδομένων είναι τέτοια που επιβάλλει την ανάλυση των απαιτήσεων του συστήματος όσο αφορά την διασφάλιση της ιδιωτικότητας του ασθενούς και την πρόταση κάποιων ενδεικνυόμενων λύσεων.

5.4.5.1 IPSec

Ολόκληρο το σύστημα βασίζεται στο πρωτόκολλο IPv6 άρα πρέπει να μελετηθεί κατά πόσο αυτό είναι διασφαλισμένο από πιθανές επιθέσεις οι οποίες μπορεί να έχουν σαν σκοπό την συνακρόαση ή ακόμη και την αλλοίωση των δεδομένων. Το IPv6 πρέπει να προστατεύεται από το IPSec. Το IPSec στο IPv6 έχει υλοποιηθεί με τη χρήση επικεφαλίδας ελέγχου ταυτότητας AH και επέκταση ESP επικεφαλίδας. Δεδομένου ότι επί του παρόντος, στο IPv4 το IPsec είναι διαθέσιμο σε όλους σχεδόν τους client και server, το IPv6 IPSec μπορεί να χρησιμοποιηθεί από διαχειριστές IT αμέσως, χωρίς να αλλάξουν οι εφαρμογές ή τα δίκτυα. Δεδομένου ότι το μοντέλο ασφαλείας IPsec απαιτείται, πρέπει να υποστηρίζεται από όλες τις εφαρμογές του συστήματος.

Το πρωτόκολλο Ασφάλειας IP (IP Security) ' IPsec', είναι μία οικογένεια πρωτοκόλλων που παρέχει ασφάλεια στο επίπεδο δικτύου. Το IPsec είναι ένα μάλλον περίπλοκο πρωτόκολλο και διάφορα τμήματά του περιγράφονται σε περισσότερα από δέκα RFC. Θα μελετηθεί το IPsec σε ένα συγκεκριμένο περιβάλλον, δηλαδή στο περιβάλλον όπου όλοι οι υπολογιστές υπηρεσίας μέσα στο Διαδίκτυο υποστηρίζουν το IPsec. Αν και αυτό το περιβάλλον δεν θα εμφανιστεί στο εγγύς μέλλον, το περιβάλλον θα απλοποιήσει τη

συζήτηση και θα βοηθήσει να κατανοηθούν τα βασικά χαρακτηριστικά του IPsec. Δύο κύρια RFC είναι τα RFC 2401, το οποίο περιγράφει τη συνολική αρχιτεκτονική ασφάλειας IP και το RFC 2411, το οποίο παρέχει μια επισκόπηση της οικογένειας πρωτοκόλλων IPsec και των εγγράφων που την περιγράφουν.

Για να αναλυθεί η παροχή ασφάλειας σε επίπεδο δικτύου πρέπει να αναλυθεί η παροχή εμπιστευτικότητας από το επίπεδο δικτύου, αν όλα τα δεδομένα που μεταφέρονταν από όλα τα δεδομενογράμματα IP ήταν κρυπτογραφημένα. Αυτό σημαίνει ότι όταν ένας υπολογιστής υπηρεσίας θέλει να στείλει ένα δεδομενόγραμμα, κρυπτογραφεί το πεδίο δεδομένων του δεδομενογράμματος πριν να το στείλει μέσα στο δίκτυο. Καταρχήν, η κρυπτογράφηση μπορεί να γίνει με κρυπτογράφηση συμμετρικού κλειδιού κρυπτογράφηση δημόσιου κλειδιού ή με κλειδιά συνόδου, για τα οποία γίνεται δια-πραγμάτευση χρησιμοποιώντας κρυπτογράφηση δημόσιου κλειδιού. Το πεδίο δεδομένων μπορεί να είναι ένα τμήμα TCP, ένα τμήμα UDP, ένα μήνυμα ICMP κλπ. Αν υπήρχε μια τέτοια υπηρεσία επιπέδου δικτύου, όλα τα δεδομένα που θα στέλνονταν από υπολογιστές υπηρεσίας -περιλαμβανομένων e-mail, ιστοσελίδων, μηνυμάτων ελέγχου, μηνυμάτων διαχείρισης (σαν τα ICMP και SNMP) - θα κρύβονταν από κάθε τρίτο, που παρακολουθούσε το δίκτυο. Έτσι, μια τέτοια υπηρεσία θα παρείχε μια καθολική κάλυψη για όλη την κίνηση Διαδικτύου, δίνοντας έτσι σε όλους μια αίσθηση ασφάλεια.

Εκτός της εμπιστευτικότητας, κάποιος μπορεί επίσης να θέλει το επίπεδο δικτύου να παρέχει πιστοποίηση προέλευσης. Όταν ένας υπολογιστής υπηρεσίας προορισμού δέχεται ένα δεδομενόγραμμα IP με μια συγκεκριμένη διεύθυνση προέλευσης IP, πιστοποιεί την προέλευση σιγουρεύοντας ότι το δεδομενόγραμμα IP παρήχθη πραγματικά με αυτή τη διεύθυνση προέλευσης IP. Μια τέτοια υπηρεσία αποτρέπει την πιστοποίηση δεδομενογραμμάτων με παραπλανητικές διευθύνσεις IP.

Στην οικογένεια πρωτοκόλλων IP υπάρχουν δύο κύρια πρωτόκολλα: το πρωτόκολλο Επιεφαλίδας Πιστοποίησης (Authentication Header, AH) και το πρωτόκολλο Ενθυλάκωσης Ωφέλιμου Φορτίου Ασφάλειας (Encapsulation Security Payload, ESP). Όταν ένας υπολογιστής υπηρεσίας προέλευσης στέλνει ασφαλή δεδομενογράμματα σε έναν υπολογιστή υπηρεσίας προορισμού, το κάνει είτε με το πρωτόκολλο AH, είτε με το πρωτόκολλο ESP. Το πρωτόκολλο AH παρέχει πιστοποίηση προέλευσης και ακε-ραιότητα δεδομένων αλλά δεν παρέχει εμπιστευτικότητα. Το πρωτόκολλο ESP παρέχει πιστοποίηση, ακεραιότητα δεδομένων και εμπιστευτικότητα. Παρέχοντας περισσότερες υπηρεσίες, το πρωτόκολλο ESP είναι φυσικά πιο περίπλοκο και απαιτεί περισσότερη επεξεργασία από το πρωτόκολλο AH.

Και στα δύο πρωτόκολλα, AH και ESP, πριν να σταλούν ασφαλή δεδομενογράμματα από έναν υπολογιστή υπηρεσίας προέλευσης σε έναν υπολογιστή υπηρεσίας προορισμού, οι υπολογιστές υπηρεσίας προέλευσης και δικτύου κάνουν χειραψία και δημιουργούν μια λογική σύνδεση επιπέδου δικτύου. Αυτό το λογικό κανάλι καλείται συσχέτιση ασφάλειας

(security association, SA). Έτσι, το IPsec μετασχηματίζει το παραδοσιακό ασυνδεσιστρεφές επίπεδο δικτύου του Διαδικτύου σε ένα επίπεδο με λογικές συνδέσεις! Η λογική σύνδεση που ορίζεται από μια SA είναι μια μονόδρομη σύνδεση. Αυτό σημαίνει ότι είναι μονοκατευθυντική. Αν και οι δύο υπολογιστές υπηρεσίας θέλουν να ανταλλάξουν δεδομενογράμματα μεταξύ τους, τότε δύο SA (δηλαδή λογικές συνδέσεις) πρέπει να καθοριστούν, μια προς κάθε κατεύθυνση. Μια SA προσδιορίζεται μοναδικά από μια τριάδα, η οποία αποτελείται από:

·Μια ταυτότητα πρωτοκόλλου ασφάλειας (AH ή ESP)

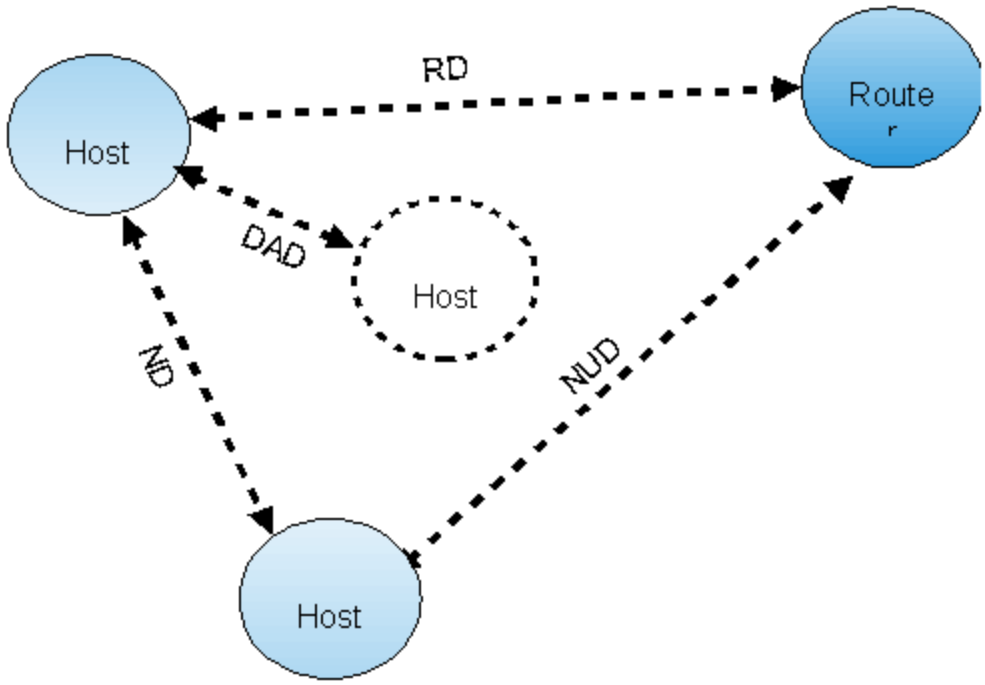
·Τη διεύθυνση προέλευσης IP για τη μονόδρομη σύνδεση

·Μια ταυτότητα σύνδεσης 32-bit, που καλείται Δείκτης Παραμέτρου Ασφάλειας (Security Parameter Index, SPI)

Για μια δεδομένη SA (δηλαδή, μια δεδομένη λογική σύνδεση από τον υπολογιστή υπηρεσίας προέλευσης προς τον υπολογιστή υπηρεσίας προορισμού), κάθε δεδομενόγραμμα IPsec θα έχει ένα ειδικό πεδίο για τον SPI. Όλα τα δεδομενογράμματα μέσα στην SA θα χρησιμοποιούν την ίδια τιμή SPI σε αυτό το πεδίο.

5.4.5.2 NDP πρωτόκολο

Επίσης το IPv6 διαθέτει μία επέκταση ασφάλειας που το καθιστά ακόμη πιο ασφαλή κατά την εφαρμογή του στο υπό μελέτη σύστημα. Η επέκταση αυτή είναι το NDP ‘Neighbor Discovery Protocol’ και ορίζεται στο RFCs 2461 και 2462. Έχει συγκεκριμένες λειτουργίες, όπως ανακάλυψη γείτονα ‘Neighbor Discovery (ND)’, αυτορύθμιση της διεύθυνσης ‘Address Auto-configuration, Router Discovery (RD)’, ανίχνευση μη διαθέσιμων γειτόνων ‘ Neighbor Un-reachability Detection (NUD)’, επίλυση διεύθυνσης ‘Address Resolution’, ανίχνευση διπλοκαταχωρημένης διεύθυνσης ‘Duplicate Address Detection (DAD)’, και άλλα.




```
<-----------NDP Message---------------->
*-------------------------------------------------------------*
| IPv6 Header       | ICMPv6    | ND Message- | ND Message    |
| Next Header = 58  | Header    | specific    | Options       |
| (ICMPv6)          |           | data        |               |
*-------------------------------------------------------------*
                <--NDP Message header-->
```

Εικόνα 5.11: NDP μήνυμα

Οι προδιαγραφές NDP τονίζουν τη χρήση του IPsec για την προστασία των NDP μηνυμάτων. Αλλά στα RFCS δεν περιγράφονται οδηγίες για το πώς θα χρησιμοποιείται το IPsec στα NDP. Τα IPsec AH μπορεί να χρησιμοποιηθούν στα NDP μηνύματα για την ενίσχυση της ασφάλειας.

Το IPsec μπορεί να εφαρμοστεί στα μηνύματα NDP μόνο με χειροκίνητη ρύθμιση του Security Associations (SA) και αυτό μπορεί να είναι μια κουραστική ή ανέφικτη αποστολή αν υπολογιστεί και ο όγκος των δεδομένων. Οι κύριοι λόγοι για τη χειροκίνητη ρύθμιση είναι οι εξής:

- SAs μπορούν να δημιουργηθούν μόνο μέσα από τη χρήση του Internet Key Exchange (IKE). Το IKE απαιτεί μία λειτουργία IP stack ώστε να λειτουργήσει αλλά αυτό έχει σαν αποτέλεσμα να προκαλείται κάποιο πρόβλημα εκκίνησης.

- Ακόμη και αν ήταν εγκατεστημένο το SAs, δεν είναι δυνατόν να εξακριβωθεί η κυριότητα των διευθύνσεων IP που δημιουργούνται δυναμικά.

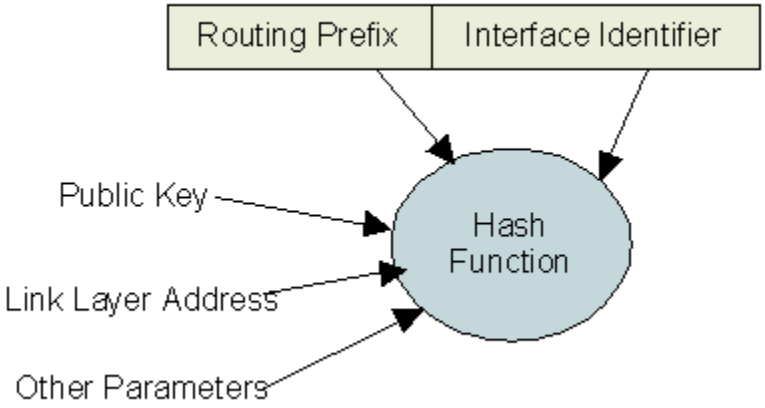
5.4.5.3 Παραγωγή κρυπτογραφημένων διευθύνσεων

Μία βασική λειτουργία του NDP είναι το CGA 'Cryptographic Generated Addresses', κατά το οποίο 62 bit χρησιμοποιούνται για την αποθήκευση ενός κρυπτογραφημένου hash δημόσιου κλειδιού.

host ID = HASH62(public_key)

Με την ενσωμάτωση παραμέτρων ασφαλείας, 'sec' στα δεξιότερα bits της 128-bit διεύθυνσης IPv6, το hash μήκος του κλειδιού μπορεί να αυξηθεί ώστε να υπάρξει ισχυρότερη ασφάλεια.

Hash = HASH(public_key)



Εικόνα 5.12:Hash function

5.4.5.4 SEND Πρωτόκολλο

Όταν το NDP χρησιμοποιείται και από τους χρήστες και από τους δρομολογητές είναι πιο ευάλωτο σε διάφορες επιθέσεις αν δεν προστατεύεται. Για να αντιμετωπίσει τις απειλές το NDP, έχει σχεδιαστεί το Secure Neighbor Discovery (SEND) πρωτόκολλο.

Οι διάφορες επιλογές του πρωτόκολλου δίνονται παρακάτω.

- Παραγωγή κρυπτογραφημένων διευθύνσεων

Η CGA διασφαλίζει ότι ο αποστολέας του μηνύματος NDP είναι και ο ιδιοκτήτης του. Πριν υποβληθεί αίτηση για μια διεύθυνση, κάθε κόμβος δημιουργεί ένα δημόσιο-ιδιωτικό κλειδί και η επιλογή CGA επαληθεύει αυτό το κλειδί.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |   Pad Length  |   Reserved    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                        CGA Parameters                         ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                           Padding                             ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Εικόνα 5.13: Μορφή της επιλογής CGA

- Επιλογή RSA υπογραφής

Οι υπογραφές του δημόσιου κλειδιού διατηρούν την ακεραιότητα των μηνυμάτων και την επικύρωση της ταυτότητας του αποστολέα. Η RSA υπογραφή προστατεύει τα μηνύματα απαιτώντας η υπογραφή του δημόσιου κλειδιού στο οποίο βασίζονται να επισυνάπτεται σε κάθε μήνυμα NDP.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |           Reserved            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                           Key Hash                            |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                       Digital Signature                       ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                           Padding                             ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Εικόνα 5.14: Μορφή της RSA υπογραφής

- Timestamp επιλογή

Η Timestamp επιλογή παρέχει replay προστασία και εξασφαλίζει ότι δεν έχουν αναπαραχθεί αυτόκλητα διαφημιστικά μηνύματα και ανακατευθύνσεις.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |          Reserved             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                           Timestamp                           +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Εικόνα 5.15: Μορφή της επιλογής Timestamp

- Nonce Επιλογή

Η επιλογή Nonce προστατεύει τα μηνύματα όταν χρησιμοποιούνται σε solicitation-advertisement pairs. Διασφαλίζει ότι μια διαφήμιση είναι μια νέα απάντηση σε μία παράκληση που έστειλε νωρίτερα ο κόμβος.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |  Nonce ...                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               |
|                                                               |
.                                                               .
.                                                               .
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Εικόνα 5.16: Μορφή της επιλογής Nonce

5.5 Συσκευές υγείας παρακολούθησης βιοσημάτων με ενσωματωμένες RFID ετικέτες για το σπίτι

Στο υπό μελέτη σύστημα προβλέπονται συσκευές υγείας με τις οποίες ο ασθενής θα έχει τη δυνατότητα να μετράει συγκεκριμένα βιοσήματα. Οι συσκευές αυτές πρέπει να έχουν συγκεκριμένα χαρακτηριστικά όπως για παράδειγμα να έχουν ενσωματωμένες RFID ετικέτες οποίες εκτός από το ID θα μεταφέρουν μέσω rf κυμάτων και άλλα δεδομένα όπως τις ιατρικές μετρήσεις.

Παρακάτω παραθέτονται κάποιες συσκευές που καλύπτουν τις συγκεκριμένες απαιτήσεις και είναι ήδη διαθέσιμες στην αγορά.

- 2.45G Medical Sensor (Blood Pressure)

Specifications (ODM/OEM welcome)	
This medical sensor is to be used with active reader, model: AR245M	
Blood Pressure Range	20~280 mmHg
Accuracy	±3 mmHg
Type	Arm measurement
Signal	RS232 I-O port Support RX, TX ,GROUND
Pulse Range	40 ~ 195/min ± 3%
Communication	2.45G, one direction (to AR245M)
Frequency	2.40~2.48GHz
LED Light	Indicates the reading status
Parameters	ID(1-255)
Working Distance	20M
*specification subject to change without notice	

- 2.45G Medical Sensor (Blood Sugar)

Specifications (ODM/OEM welcome)	
This medical sensor is to be used with active reader, model: AR245M	
Multi-key design, easy to use	
Large LCD display	
Minimum Blood Needed (0.7uL), reduce pain	
Quick measuring time (6 seconds only)	
Light weighted design, easy to carry	
Communication	2.45G, one direction (to AR245M)
Frequency	2.40~2.48GHz
LED Light	Indicates the reading status
Parameters	ID(1-255)
Working Distance	20M
*specification subject to change without notice	

- 2.45G Medical Sensor (Temperature)

Specifications (ODM/OEM welcome)	
This medical sensor is to be used with active reader, model: AR245M	
Temperature Range 30~43℃	
Accuracy ±0.3℃	
Signal (temperature) sent out every 10 seconds (EN12479 rule)	
Signal	RS232 I-O port Support RX, TX ,GROUND
Type	Wristband Type
Communication	2.45G, one direction (to AR245M)
Frequency	2.40~2.48GHz
LED Light	Indicates the reading status
Parameters	ID(1-255)
Working Distance	20M
*specification subject to change without notice	

- 2.45G Medical Sensor (Fall Detection)

Specifications (ODM/OEM welcome)	
This medical sensor is to be used with active reader, model: AR245M	
2G sensor technology (x/y axis)	
1.5G sensitivity (z axis)	
Panic button design	
Signal	RS232 I-O port Support RX, TX ,GROUND
Light weighted, easy to carry	
Communication	2.45G, one direction (to AR245M)
Frequency	2.40~2.48GHz
LED Light	Indicates the reading status
Parameters	ID(1-255)
Working Distance	20M
*specification subject to change without notice	

- 2.45G Medical Sensor (SPO2)

Specifications: (ODM/OEM welcome)	
This medical sensor is to be used with active reader, model: AR245M	
SPO_2 Range	35% -99%
Pulse Range	35% -99%
SPO_2 Accuracy	35% -99%
Pulse Accuracy	35% -99%
Large LCD design	
Signal	RS232 I-O port Support RX, TX ,GROUND
Communication	2.45G, one direction (to AR245M)
Frequency	2.40~2.48GHz
LED Light	Indicates the reading status
Parameters	ID(1-255)
Working Distance	20M
*specification subject to change without notice	

Επίσης από τον κατασκευαστή προτείνεται ο εξής RFID Reader:

- 2.45GHz Active RFID Reader/Writer

Specification	
Model no.	AR245M
Frequency range	2.4GHz-2.5M ISM Microwave band,125 channel, channel bandwidth 1MHz
Communication mode	dynamically encrypt mode
Asynchronism communication speed	9600Bps-115200Bps
Signal modulation mode	GFSK
Antenna polarizing	round polarization
Microwave message wrong-checked	CRC16 cycled redundance checkout
Receipting sensitivity	-90dbm
Recognizing mode	non-directional identification, reading card radii 3-15m round any angle
Identified distance	the farthest distance 80m
Recognized speed	80km/h
Anti- confliction	identify >100 cards at the same time
Wrong probability	one of ten million
Developing port	offer all types of port function
Sound indication	buzzer inside
Power adapter	AC190—235V/DC+12V
Operation temperaturer	-40°C~+85°C
Dimension	140*105*35mm
*Specification subject to change without notice	

5.6 Συμπεράσματα

Σε αυτή την ενότητα περιγράφτηκε ένα σενάριο παρακολούθησης ασθενών από το σπίτι τους κάνοντας χρήση της τεχνολογίας του Διαδικτύου των πραγμάτων. Αναλύθηκε πώς το υπό μελέτη σύστημα μπορεί να χρησιμοποιήσει την τεχνολογία του RFID και το πρωτόκολλο IPv6. Εξετάστηκε επίσης πως ένα τέτοιο σύστημα θα μπορούσε να σχεδιαστεί κατόπιν περιγραφής του προβλήματος και ανάλυσης των περιπτώσεων χρήσης του. Επιπλέον, παρουσιάστηκε η γενική εικόνα του συστήματος από την άποψη των υπηρεσιών. Αναφέρθηκαν πιθανές συνδέσεις του δικτύου και λύσεις για την υλοποίηση του. Προτάθηκαν λύσεις για πιθανά προβλήματα ασφάλειας που θα προκύψουν κατά την εφαρμογή.

Με τον τρόπο που υλοποιήθηκε το σύστημα παρακολούθησης των ασθενών δόθηκαν λύσεις σε μερικούς από τους προβληματισμούς που αναφέρθηκαν στην αρχή του κεφαλαίου αλλά δημιουργήθηκαν και καινούργιοι. Η παρακολούθηση από το σπίτι υπό αυτή την μορφή θα γίνει αποδεκτή από του ασθενείς και αυτό γιατί δεν αλλάζει σε τίποτα η καθημερινότητα του ασθενή λόγω του ότι ο τρόπος χρήσης των νέων συσκευών είναι ίδιος με τις ήδη ευρέως διαδεδομένες συσκευές υγείας ‘απλό πιεσόμετρο’. Αυτό θα έχει ευεργετικά αποτελέσματα τόσο για τους ασθενείς όσο και για το σύστημα περίθαλψης. Οι ασθενείς θα νιώθουν ασφάλεια πλέον γνωρίζοντας ότι ένας εξειδικευμένος γιατρός τους παρακολουθεί πολύ πιο συχνά και αποτελεσματικά από πριν χωρίς να χρειάζεται να μετακινηθούν στο νοσοκομεία. Το οποίο θα σήμαινε και έξοδα αλλά και ψυχολογική κατάπτωση των ασθενών λόγω του περιβάλλοντος του νοσοκομείου, δηλαδή θα επέφερε περαιτέρω επιβάρυνση της υγείας τους. Αναμένεται οι ασθενείς τρίτης ηλικίας, οι χρόνιοι παθόντες και οι ασθενείς που ζουν σε απομακρυσμένες περιοχές να επωφεληθούν περισσότερο από όλους τους άλλους. Αλλά και το νοσοκομείο θα επωφεληθεί από την μείωση της άσκοπης προσέλευσης ασθενών, με αποτέλεσμα ο εξοπλισμός του να είναι διαθέσιμος και λιγότερο επιβαρυμένος. Το προσωπικό του θα μπορεί να αξιοποιηθεί αποτελεσματικότερα σε θέσεις που θα υπάρχει πραγματική ανάγκη.

Από τη άλλη αυτή η μετάδοση ευαίσθητων προσωπικών δεδομένων όπως είναι τα ιατρικά δεδομένα ενός ασθενούς έχει σαν αποτέλεσμα να προκύψουν θέματα ηθικά αλλά και θέματα προστασίας της ιδιωτικότητας. Παρόλο που κατά την ανάλυση του συστήματος λήφθηκε σοβαρά υπόψη ο παράγοντας της ασφάλειας, δεν μπορεί να εγγυηθεί κανείς την απόλυτη προστασία της ιδωτικότητας του ασθενούς. Για το λόγο αυτό ο τομέας αυτός θα πρέπει να ερευνηθεί και να αναπτυχθεί περαιτέρω, αφού το απόρρητο θεωρείται ως το βασικό κριτήριο από τους ασθενείς για να υιοθετήσουν το παρόν ιατρικό σύστημα παρακολούθησης.

5.7 Βιβλιογραφία

http://www.ipv6.com/articles/applications/Using-RFID-and-IPv6.htm

http://www.summitco.com.tw

Yao-Chung Chang . Architecture Design and Performance Evaluation of RFID Object Tracking Systems, http://portal.acm.org,2007

Yu-Lee Choi, Seok-Man Kim , Sang-Hee Son , and Kyoung-Rok Cho. Design of the RFID for Storage of Biological Information, School of Business, La Trobe University, www.iiisci.org,2007

Martin Peter Michael. Architectural Solutions for Mobile RFID Services on Internet of Things, http://portal.acm.org, 2007.

Won Jay Song Son, S.H. Munkee Choi Minho Kang Dept. of Comput. Sci., Virginia Univ., Charlottesville, VA, USA. Privacy and security control architecture for ubiquitous RFID healthcaresystem in wireless sensor networks, Prepared for DG INFSO, H1,2009

Κεφάλαιο 6ο

Θέματα προς συζήτηση

6.1 Παρουσίαση

Καθώς το Διαδίκτυο των πραγμάτων θα γίνεται όλο και πιο πολύ μέρος της καθημερινότητας μας, θα παρατηρηθεί μία ραγδαία αύξηση του αριθμού και των τύπων των δικτυωμένων αντικειμένων, των ειδών της πληροφορίας που ανταλλάσσονται καθώς και του αριθμού και της πολυπλοκότητας των σχετικών τεχνολογιών. Οι προκλήσεις που θέτει η RFID τεχνολογία σήμερα σε εφαρμογές που βασίζονται σε αυτή θα παραμείνουν, και οι απαντήσεις σε αυτές θα πρέπει να αναθεωρηθούν για μεγαλύτερης κλίμακας εφαρμογή που είναι το Διαδίκτυο των πραγμάτων.

Η μετάβαση στο Διαδίκτυο των πραγμάτων δεν θα αλλάξει μόνο το μέγεθος αλλά και τη φύση του προβλήματος. Για παράδειγμα, τα ζητήματα της ιδιωτικότητας και της προστασίας των δεδομένων είναι πολύ πιο σημαντικά στο Διαδίκτυο των πραγμάτων. Για να επωφεληθούν οι πολίτες από την ευκολία που θα προσφέρεται, είναι πιθανόν να θέσουν όλο και περισσότερες συσκευές σε σύνδεση. Για να συνδυαστούν με ασφάλεια οι πληροφορίες από όλες αυτές τις συσκευές θα πρέπει να δημιουργηθεί μια κοινή πολιτική με την οποία αυτές θα πρέπει να συμμορφωθούν. Καθίσταται σημαντικό να διασφαλιστεί ότι τα θεμελιώδη δικαιώματα των ατόμων- πολιτών για την προστασία της ιδιωτικής τους ζωής και την προστασία των δεδομένων τους, όπως προβλέπονται στο ευρωπαϊκό δίκαιο, θα ληφθούν επαρκώς υπόψη στο σχεδιασμό και στη λειτουργία του Διαδικτύου των πραγμάτων. Αυτό γίνεται ακόμα πιο επιτακτικό όταν το Διαδίκτυο των πραγμάτων εφαρμόζεται στην υγεία και συγκεκριμένα στην κατ' οίκον παρακολούθηση ασθενών με τη βοήθεια διασυνδεδεμένων προσωπικών ιατρικών συσκευών. Ως εκ τούτου, είναι απαραίτητες κατάλληλες πολιτικές για τη στήριξη της ανάπτυξης του Διαδικτύου των πραγμάτων με την διασφάλιση των παραπάνω.

Σε αυτό το πλαίσιο θα ήταν σωστό να συζητηθούν τα εξής θέματα :

- Πώς θα ευαισθητοποιηθούν και θα ενεργοποιηθούν όλοι οι ενδιαφερόμενοι φορείς (καταναλωτές, επιχειρήσεις, κατασκευαστές ετικετών και συσκευών ανάγνωσης, προγραμματιστές, ερευνητές, τεχνικοί) οι οποίοι προτίθενται να κάνουν χρήση του Διαδικτύου των πραγμάτων.

- Πώς οι τεχνολογίες και οι υπηρεσίες του Διαδικτύου των πραγμάτων θα είναι κατανοητές και σε προσιτή τιμή, ιδίως για τα άτομα με ειδικές ανάγκες και μεγάλης ηλικίας.

- Πώς μπορούν να διασφαλιστούν τα θεμελιώδη δικαιώματα των ατόμων στην ιδιωτική ζωή, και τα προσωπικά τους δεδομένα, ιδίως αν αυτά είναι ιατρικά δεδομένα.

- Πώς η ανάπτυξη της τεχνολογίας, θα επιφέρει επιπλέον θέματα :

    - Θα καταστεί πρόβλημα στην ανακύκλωση με την ενσωμάτωση περισσότερων ηλεκτρονικών υλικών σε μια σειρά από αντικείμενα της καθημερινότητας τα οποία έως τώρα ήταν είτε βιοαποδομήσιμα είτε ανακυκλώσιμα.

    - Θα καταστεί πρόβλημα στην υγεία των χρηστών από την ακτινοβολία που θα λαμβάνουν λόγω της συνεχούς έκθεσης τους σε πολύ φορτωμένα ασύρματα δίκτυα.

6.2 Έρευνα της ακαδημαϊκής κοινότητας

Ένα άλλο θέμα προς συζήτηση είναι πώς η ακαδημαϊκή κοινότητα μέσω έρευνας θα μπορέσει να βοηθήσει στην ανάπτυξη του Διαδικτύου των πραγμάτων. Εκτιμώντας σε ποιο επίπεδο βρίσκονται οι τεχνολογίες του Διαδικτύου των πραγμάτων σήμερα συμπεραίνεται ότι με περαιτέρω μελέτη θα μπορούσαν να λειτουργήσουν καλύτερα, να γίνουν ευκολότερες και πιο προσιτές. Η κοινότητα θα πρέπει να συζητήσει και να ερευνήσει τα παρακάτω:

- Τη δημιουργία πρότυπων για τη διαλειτουργικότητα και τη διακυβέρνηση:

    - Για την υποδοχή περίπου 50.000 δισεκατομμυρίων διασυνδεδεμένων αντικείμενων και τις ανάγκες που θα προκύψουν από αυτό. Σε αυτά περιλαμβάνονται:

        - Διαχείριση δεδομένων, πληροφοριών και γνώσεων

        - Σημασιολογική μοντελοποίηση ώστε να κρατηθούν και να χρησιμοποιηθούν όλα τα δεδομένα που θα προκύψουν από το Διαδίκτυο των πραγμάτων στο σωστό τους πλαίσιο.

        - Ενασχόληση με την κλίμακα και τη χρονοεξάρτηση των δεδομένων, καθώς και με την αποθήκευση και αναζήτηση των δυναμικών πληροφοριών.

    - Για τις επικοινωνίες και την σύνδεση όσο αφορά τις ασύρματες τεχνολογίες και τη χρήση του ραδιοφάσματος

    - Για την αξιοποίηση των εξελίξεων στην πληροφορική και στα δίκτυα, όσο αφορά τις ανάγκες των ενσωματωμένων πλατφορμών νανοραδιοδιαύλων

και των πλατφορμών αισθητήρων και πώς όλα αυτά θα είναι διασυνδεμένα

- Για την παγκόσμια αναγνώριση και διαχείριση της σύνδεσης και της ενσωμάτωσης του εξελιγμένου Διαδικτύου δηλαδή του IPv6.
- Για την παροχή προσεγγίσεων και μοντέλων διακυβέρνησης για την αντιμετώπιση της πολυπλοκότητας και των κοινωνικών αξιών

❖ Την ασφάλεια και την ανθεκτικότητα των συστημάτων

- Ασφάλεια των δεδομένων και των συστημάτων από επιθέσεις, με την αύξηση της εξάρτησης τους από το περικλείον περιβάλλον και της χρήση πολλών τροπών διασύνδεσης.
- Αξιοπιστία και αντοχή των συστημάτων μέσω της αυτοδιάγνωσης , της χρήσης αισθητήρων και κέντρων ελέγχου.

❖ Ελεύθερη πληροφόρηση

- Συλλογή και διανομή της γνώσης μέσω μίας βάσης όπου θα καταγράφονται περιπτώσεις εφαρμογής του Διαδικτύου των πραγμάτων με στόχο την μελέτη αυτών για την εξέλιξη του.