ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΤΕΧΝΟΟΙΚΟΝΟΜΙΚΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΑΣΦΑΛΕΙΑ

ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΚΑΤΕΥΘΥΝΣΗ: ΤΕΧΝΟΟΙΚΟΝΟΜΙΚΗ ΔΙΟΙΚΗΣΗ

ΤΟ ΠΡΩΤΟΚΟΛΛΟ IPv6 ΚΑΙ ΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

Στυλιανός Κολοκυθάς

Αριθμός Μητρώου MTE/1151

Διπλωματική Εργασία υποβληθείσα στο Τμήμα Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς ως μέρος των απαιτήσεων για την απόκτηση Μεταπτυχιακού Διπλώματος Ειδίκευσης στην Τεχνοοικονομική Διοίκηση

Πειραιάς, Ιούνιος 2015

UNIVERSITY OF PIRAEUS

DEPARTMENT OF DIGITAL SYSTEMS

MASTER PROGRAM IN

TECHNO-ECONOMIC MANAGEMENT AND SECURITY OF DIGITAL SYSTEMS

FOLLOWING AREA: TECHNO-ECONOMIC MANAGEMENT

IPv6 PROTOCOL AND THE INTERNET OF THINGS

By
Stylianos Kolokuthas

Registration Number MTE/1151

Master Thesis submitted to the Department of Digital Systems of Piraeus in partial fulfillment of the requirements for the degree of Master in Techno-economic Management

Piraeus, Greece, June 2015

Αυτή η σελίδα αφήνεται σκόπιμα κενή

Αφιερώνεται στην οικογένειά μου

Αυτή η σελίδα αφήνεται σκόπιμα κενή

Ευχαριστίες

Θα ήθελα καταρχήν να ευχαριστήσω όλους όσους συνέβαλαν με οποιονδήποτε τρόπο στην επιτυχή εκπόνηση αυτής της διπλωματικής εργασίας. Οφείλω να ευχαριστήσω θερμά τον επιβλέποντα της διπλωματικής εργασίας μου, Δρα Λεωνίδα Κανέλλο, για την πολύτιμη βοήθεια και καθοδήγησή του κατά τη διάρκεια της δουλειάς μου. Το μεγαλύτερο ευχαριστώ το οφείλω στους γονείς μου, Στέφανο Κολοκυθά και Αναστασία Πρωτοπαπαδάκη για την ολόψυχη αγάπη και την υποστήριξή τους όλα αυτά τα χρόνια, καθώς και στον αδελφό μου Ιωάννη Κολοκυθά.

Αυτή η σελίδα αφήνεται σκόπιμα κενή

ΠΕΡΙΕΧΟΜΕΝΑ

Αυτή η σελίδα αφήνεται σκόπιμα κενή

Εισαγωγή

Ζούμε σε ένα συνδεδεμένο κόσμο. Είναι σπάνιο να περπατήσει κανείς στο δρόμο, να μπει σε οποιοδήποτε μέσο μαζικής μεταφοράς και να μη δει κάποιον να είναι απορροφημένος με το smartphone ή το tablet του. Αυτές οι συσκευές περιέχουν μια ποικιλία εφαρμογών λογισμικού που μπορεί να απαιτούν σύνδεση στο Διαδίκτυο. Οι εφαρμογές σε αυτές τις συσκευές μας βοηθούν να βλέπουμε την πρόγνωση του καιρού, να παρακολουθούμε τις τραπεζικές και χρηματιστηριακές συναλλαγές μας, να βλέπουμε τις πτήσεις της αεροπορικής εταιρίας μας, να διαβάζουμε ειδήσεις, να ακούμε ραδιόφωνο, ακόμα και να πληρώνουμε τον καφέ μας μέσω εφαρμογών ανέπαφων συναλλαγών.

Δεν είναι μόνο τα smartphone που είναι συνδεδεμένα, καθώς όλο και περισσότερες «έξυπνες» συσκευές κάθε τύπου, εξοπλισμένες με αισθητήρες, όπως οικιακός εξοπλισμός, οχήματα, μετρητικές συσκευές κατανάλωσης ενέργειας, θερμοκρασίας, ιατρικές συσκευές, συνδέονται δυναμικά στο Διαδίκτυο. Εκτός όμως από το να συνδέονται ευρυζωνικά με ικανοποιητική ταχύτητα στο διαδίκτυο οι συσκευές επικοινωνούν και μεταξύ τους μέσω της τεχνολογίας M2M (machine to machine). Πρόκειται για την τεχνολογία που επιτρέπει σε συσκευές ιδίων δυνατοτήτων να επικοινωνούν και να ανταλλάσσουν πληροφορίες μεταξύ τους, είτε ενσύρματα είτε ασύρματα, μέσω προηγμένων δικτύων τηλεπικοινωνιών επόμενης γενιάς (NGAs). Η ιδέα του «Διαδικτύου των πραγμάτων» (Internet of Things και σε συντομογραφία IoT), όρου που επινοήθηκε από τον Kevin Ashton το 2009, ξεκινά από δύο μείζονες τεχνολογικές εξελίξεις, πρώτον, την ψηφιοποίηση όλο και περισσότερων μηχανών και δεύτερον, την παραγωγή μεγάλου όγκου ψηφιακών δεδομένων (big data) που διακινούνται σε ένα παγκόσμιο κοινό μέσω πληθώρας διασυνδεδεμένων δικτύων.

Κάθε συσκευή, ηλεκτρονικός υπολογιστής, κινητό τηλέφωνο ή ταμπλέτα, συνδέεται στο διαδίκτυο με μια μοναδική διεύθυνση, που αποτελεί ένα αριθμό αποτελούμενο από συγκεκριμένο αριθμό bits, ο οποίος και αποτελεί την «ταυτότητα» της συσκευής. Με τον ολοένα αυξανόμενο αριθμό συσκευών που συνδέονται στο διαδίκτυο, παρουσιάστηκε η ανάγκη ύπαρξης και διάθεσης περισσοτέρων διευθύνσεων, από όσες μπορεί να παράσχει μέχρι σήμερα το IPv4, δηλαδή η τέταρτη έκδοση του ιντερνετικού πρωτοκόλλου IPv4. Όπως προβλέπεται από διεθνείς μελέτες και στατιστικές, μέχρι το 2020 θα μπορούσαν να υπάρχουν 30 δισεκατομμύρια συσκευές που θα συνδέονται ασύρματα στο Διαδίκτυο.[1] Σύμφωνα με έρευνες μεγάλων εταιριών στο χώρο των δικτύων[2], εκτιμάται ότι ο αριθμός αυτός θα μπορούσε να είναι ακόμα μεγαλύτερος, δηλαδή περίπου 50 δισεκατομμύρια συσκευές στο ίδιο χρονικό διάστημα.

Η αναμενόμενη έκρηξη του αριθμού διασυνδεδεμένων συσκευών καθιστά επιτακτική ανάγκη την άμεση μετάβαση των υποδομών του διαδικτύου από το μέχρι πρόσφατα χρησιμοποιούμενο πρωτόκολλο IPv4 στο σημαντικά μεγαλύτερης χωρητικότητας ιντερνετικό πρωτόκολλο IPv6. Μέσω του νέου πρωτοκόλλου μπορεί να αυξηθεί θεαματικά ο αριθμός των διευθύνσεων ώστε να καλύψει την εκθετική ζήτηση σύνδεσης συσκευών από τους οικιακούς και βιομηχανικούς χρήστες, και της μεταξύ τους αέναης ανταλλαγής πληροφοριών, κατά τη μετάβαση προς ένα «έξυπνο ψηφιακό οικοσύστημα». Το νέο αυτό πρότυπο διασυνδεδεμένης

---

1 ABIresearch. (2015). *Internet of Everything.* Retrieved 10/3/2015, from https://www.abiresearch.com/market-research/service/internet-of-everything/

2 http://www.ericsson.com/oss-bss/blog/iot-marketplace-looking-beyond-connected-devices/?gclid=CLjH_-ihu8YCFYrHtAodkc8LPw

οικονομίας και κοινωνίας θα έχει ως ραχοκοκαλιά το Διαδίκτυο των Πραγμάτων, γνωστό και ως Internet of Everything.

Πλην όμως, η μετάβαση αυτή της οικονομίας και της κοινωνίας σε ένα έξυπνο ψηφιακό οικοσύστημα θέτει ποικίλες προκλήσεις σε τεχνικό, επιχειρηματικό, νομικό και κοινωνικό επίπεδο ενώ δημιουργεί βαθιές ανατροπές σε καθιερωμένες ιδέες, πρότυπα κοινωνικής συμπεριφοράς, αντιλήψεις και τρόπους αλληλεπίδρασης.

Η παρούσα πρωτότυπη μελέτη αναλύει συνοπτικά τις τεχνικές και λειτουργικές παραμέτρους της διαδικασίας αυτής καθώς και τις επιχειρηματικές και κοινωνικές της επιπτώσεις, χωρίζεται δε σε δύο μέρη. Στο Πρώτο Μέρος αναλύονται συνοπτικά οι εφαρμογές του Διαδικτύου των Πραγμάτων στη βιομηχανία, στην παιδεία, στην παραγωγή, στις εργασιακές σχέσεις καθώς και το τεχνικό υπόβαθρο της μετάβασης μέσω του Πρωτοκόλλου IPv6, του οποίου αναλύονται τα τεχνικά χαρακτηριστικά και τα πλεονεκτήματα σε σχέση με το εφαρμοζόμενο μέχρι σήμερα πρωτόκολλο IPv4. Στο Δεύτερο Μέρος γίνεται μια συνοπτική επισκόπηση των κοινωνικών επιπτώσεων και του θεσμικού πλαισίου σε Ελλάδα και Ευρώπη, και εξετάζονται οι πολιτικές που απαιτούνται για την ομαλή μετάβαση οικονομίας και κοινωνίας σε ένα «έξυπνο» ψηφιακό οικοσύστημα..

ΠΡΩΤΟ ΜΕΡΟΣ
ΤΟ ΠΡΩΤΟΚΟΛΛΟ IpV6 ΚΑΙ Η ΜΕΤΑΒΑΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

Η μετάβαση στον ψηφιακό κόσμο του αύριο με την εισαγωγή των διασυνδεδεμένων συσκευών («connected devices»), της τρισδιάστατης εκτύπωσης (3D Printing), και του πανταχού παρόντος Διαδικτύου επιφέρει σημαντικές αλλαγές στην οικονομία και στην κοινωνία. Η διασυνδεσιμότητα αποτελεί πλέον στο δυτικό κόσμο βασική ανθρώπινη ανάγκη, όπως η πρόσβαση σε ηλεκτρισμό ή νερό.

Το πρωτόκολλο IPv6, που αποτελεί μετεξέλιξη του προηγούμενου πρωτοκόλλου IPv4, που έφτασε πια στα όριά του, αναμένεται να διευκολύνει τεχνικά αυτή τη σύνθετη διαδικασία, παρέχοντας τη δυνατότητα θεματικής αύξησης του αριθμού συσκευών που συνδέονται στα ευρυζωνικά δίκτυα τηλεπικοινωνιών.

ΚΕΦΑΛΑΙΟ 1
Εφαρμογές του Διαδικτύου των Πραγμάτων στην Οικονομία και στην Κοινωνία

Στις επόμενες σελίδες θα αναλύσουμε συνοπτικά τις κυριότερες εφαρμογές στην οικονομία και στην παραγωγική διαδικασία καθώς και τις κοινωνικές τους επιπτώσεις.

1.1 Εισαγωγή

Το Διαδίκτυο βρίσκεται στο μεταίχμιο μιας νέας εποχής. Σήμερα χαρακτηρίζεται από το πλήθος των υπηρεσιών που παρέχει στους χρήστες σε ανεπτυγμένο και

αναπτυσσόμενο κόσμο. Οι τελευταίοι καλούνται να χρησιμοποιήσουν τις διαθέσιμες πληροφορίες ώστε να εκτελέσουν πιο αποτελεσματικά κάθε παραγωγική διαδικασία και εργασία. Οι τεχνολογικές τάσεις όμως οδηγούν το διαδίκτυο και τους χρήστες του, σε μια νέα λογική αποδοτικότερης εκμετάλλευσης των διαθέσιμων πόρων. Σήμερα οι τεχνολογικά ανεπτυγμένες κοινωνίες είναι συχνά αναγκασμένες να προσαρμόζονται στις νέες εφαρμογές της τεχνολογίας και του διαδικτύου, με στόχο να εκμεταλλευτούν τα πλεονεκτήματα υιοθέτησής τους.

Το γεγονός αυτό δημιουργεί σημαντικές προκλήσεις στο κράτος, στους χρήστες, στους δημιουργούς εφαρμογών, στους διαχειριστές δικτύων και στους παρόχους υπηρεσιών κατά το διάστημα προσαρμογής στη νέα άυλη ψηφιακή οικονομία. Μεταξύ αυτών ανήκει η ανάγκη επανεκπαίδευσης των χρηστών στη χρήση των νέων συστημάτων, οι σημαντικές επενδύσεις που απαιτούνται για την δημιουργία και συντήρηση καινούριων υποδομών, καθώς και ανάγκη μετάβασης σε κοινά αποδεκτά τεχνικά και λειτουργικά πρότυπα που θα επιτρέπουν την συνέργεια όλων των εμπλεκόμενων μερών. Αποτελεί πλέον κοινοτυπία πως τα πιο επιτυχημένα τεχνολογικά επιτεύγματα είναι αυτά που παραμένουν αφανή και έχουν γίνει αδιάσπαστο κομμάτι της καθημερινότητας, δηλαδή η χρήση τους δηλαδή θεωρείται ως φυσιολογική λειτουργία στη ζωή. Χαρακτηριστικό παράδειγμα αποτελεί η κινητή τηλεφωνία που έχει εισχωρήσει στην καθημερινότητα των ανθρώπων και αποτελεί πλέον πολυχρηστικό εργαλείο με εφαρμογή σε όλες τις εκφάνσεις της επαγγελματικής και κοινωνικής ζωής.

Για το Διαδίκτυο παρόμοια εξέλιξη θα αποτελούσε η μετάβαση στην εποχή του IoT. Ειδικότερα, στο πλαίσιο αυτό κεντρικό ρόλο θα κατέχουν τα ξεχωριστά αντικείμενα του περιβάλλοντος, που θα είναι δικτυωμένα και θα αλληλεπιδρούν μεταξύ τους. Με το τρόπο αυτό οι χρήστες δεν θα χρειάζεται να αποτελούν το ενδιάμεσο μέλος που θα καλεί την υπηρεσία για να κάποιο συγκεκριμένο

αντικείμενο, αλλά το ίδιο το αντικείμενο θα αλληλεπιδρά με το Πληροφοριακό Σύστημα που χτίζεται γύρω του. Ο πρώτος που όρισε την έθεσε το πλαίσιο του «απανταχού υπολογίζειν» ήταν ο Marc Weiser[3], που θεωρεί την τάση αυτή ως το τρίτο τεχνολογικό κύμα στον κόσμο των υπολογιστών. Πρώτο ήταν η εποχή των κεντρικών υπολογιστών, που τους μοιράζονταν πολλοί χρήστες. Έπειτα περάσαμε στην εποχή των προσωπικών υπολογιστών. Τρίτο μεγάλο βήμα θα είναι η εποχή όπου η τεχνολογία θα βρίσκεται στο υπόβαθρο της καθημερινότητας, επηρεάζοντάς τη με τρόπο συνεχή και αδιάλειπτο.

1.2 Οι «έξυπνες» διασυνδεδεμένες συσκευές

Η μετάβαση στην εποχή του IoT με την ύπαρξη πληθώρας έξυπνων (smart) συσκευών αναμένεται να δημιουργήσει κινητήριες δυνάμεις ανάπτυξης, που θα προκαλέσουν την εξέλιξη των Πληροφοριακών Συστημάτων και την δημιουργία νέων εφαρμογών. Καθότι οι αλλαγές θα προκληθούν τόσο σε τεχνικό επίπεδο όσο και σε αυτό των διαδικασιών, είναι εύλογη η δημιουργία ευκαιριών για νέες επενδύσεις και υλοποιήσεις ιδεών, που θα μπορέσουν ενδεχομένως να μεταβάλλουν τον τρόπο που σήμερα αντιλαμβανόμαστε την αλληλεπίδραση του ανθρώπου με το τεχνικό περιβάλλον και με τους συνεργάτες του. Οι κλάδοι εφαρμογών, που μπορεί το IoT να επηρεάσει, περιλαμβάνουν σχεδόν το σύνολο των αγορών και των σημερινών υπηρεσιών. Στα επόμενα υποκεφάλαια ακολουθούν κάποιες από τις πιθανές κατηγορίες εφαρμογών που το IoT μπορεί να επηρεάσει. Μέσα από την ανάλυση που ακολουθεί θα γίνει επίσης εμφανές πως δεν πρόκειται τόσο για νέες εφαρμογές αλλά για αλλαγές στον τρόπο προσέγγισης παραδοσιακών διεργασιών, που σήμερα θεωρούμε ως δεδομένες. Αυτή η τεχνολογική εξέλιξη ενδέχεται να προκαλέσει ανακατατάξεις και να δώσει νέα

[3] https://en.wikipedia.org/wiki/Mark_Weiser

ώθηση παρέχοντας νέες ευκαιρίες και ανοίγοντας νέους ορίζοντες σε αγορές και παραγωγικούς τομείς που εδώ και καιρό θεωρούνται κορεσμένοι.

Μια βασική διαφορά των νέων αυτών εφαρμογών και κυρίως αυτών που θα διαδρούν με τον χρήστη και όχι μεταξύ συστημάτων, θα είναι η διαφοροποίηση της διεπαφής χρήσης. Ειδικότερα οι χρήστες θα μπορούν με μεγαλύτερη ευκολία να συνδέσουν τον πραγματικό κόσμο με τον εικονικό, επικοινωνώντας με φυσικότερο τρόπο τόσο με άλλους χρήστες όσο και με πολυμεσικές εφαρμογές. Παράδειγμα αποτελεί η χρήση κινητού τηλεφώνου εξοπλισμένου με κάμερα για την αναγνώριση αντικειμένων.

1.2.1 Μεταφορές

Οι μεταφορές αποτελούν βασικό κομμάτι του σύγχρονου πολιτισμού και αναγκαία υποδομή για την διακίνηση των αγαθών. Η βελτιστοποίησή τους λοιπόν θα συμπαρασύρει όλους τους τομείς της οικονομίας που εξαρτώνται από τις μεταφορές. Πιο συγκεκριμένα αλλαγές στον τρόπο διαχείρισης των μέσων σταθερής τροχίας (π.χ. σιδηρόδρομος) θα μπορούσε να αυξήσει την δυναμικότητα των γραμμών ώστε χωρίς επιπλέον επένδυση σε υλικές υποδομές, να υπάρξει αύξηση στην απόδοση, τόσο στον άξονα της ποσότητας όσο και σε αυτόν της ταχύτητας, αλλά χωρίς εκπτώσεις και συμβιβασμούς ασφάλειας ή άλλων κρίσιμων παραγόντων.

Παράλληλα η δυνατότητα που δίνεται στο πλαίσιο του Διαδικτύου των Πραγμάτων για σφαιρική πληροφόρηση, επιτρέπει την εξαγωγή γνώσης και συμπερασμάτων που μπορούν να αξιοποιηθούν ποικιλοτρόπως. Ειδικότερα θα ήταν εφικτός ο υπολογισμός του μέσου χρόνου μεταξύ βλαβών στα μέσα μεταφοράς (π.χ. λεωφορεία) ώστε να δημιουργηθεί ένα αξιόπιστο δίκτυο μεταφορών, ενώ

ταυτόχρονα θα ήταν δυνατή και η βέλτιστη διαχείριση του συστήματος επισκευών. Αυτό συνεπάγεται μικρότερα έξοδα σε ανταλλακτικά, ταχύτερη επισκευή, έγκαιρες παραγγελίες σε τμήματα με συχνές βλάβες ή αντικατάστασή τους με άλλα καλύτερης ποιότητας.

Στο χώρο των μαζικών μεταφορών θα μπορούσαμε να προβλέψουμε και νέα συστήματα τιμολόγησης χρήσης των υπηρεσιών. Τέτοιο παράδειγμα αποτελούν οι αυτόματες πληρωμές των εισιτηρίων με την είσοδο του καταναλωτή στο λεωφορείο ή στο τραίνο. Τέλος στα πλαίσια ενός σύνθετου συστήματος μεταφορών ανθρώπων ή και αγαθών, με την υιοθέτηση του Διαδικτύου των Πραγμάτων θα μπορούσε να δημιουργηθεί υποδομή συνολικής παρακολούθησης της πορείας των μεταφορών με σαφή προσανατολισμό την βελτιστοποίησή τους. Σήμερα υπάρχουν ήδη υλοποιημένες εφαρμογές, που παρότι δεν λειτουργούν σε ένα πλήρως ενοποιημένο περιβάλλον όπως προβλέπει το του Διαδίκτυο των Πραγμάτων, μας δίνουν την εικόνα μιας μελλοντικής αξιοποίησης τέτοιων τεχνολογιών. Ενδεικτικά παραδείγματα αποτελούν η αυτόματη διέλευση σε σταθμούς διοδίων (οδικοί άξονες), το σύστημα παρακολούθησης μεταφορών της εταιρείας DHL (μεταφορές), καθώς και το σύστημα αυτοματοποιημένης διανομής φαγητών (εστίαση).

1.2.2 Αυτοκίνηση

Πέρα από τις μαζικές μεταφορές εφαρμογές ενδέχεται να υπάρξουν και στο χώρο της αυτοκίνησης. Ήδη πολλές αυτοκινητοβιομηχανίες εξοπλίζουν τα οχήματά τους με καινοτόμα συστήματα που βοηθούν τους οδηγούς και τους επιβαίνοντες να έχουν πιο ασφαλείς και ποιοτικές διαδρομές. Το Σύστημα Ειδοποίησης Αλλαγής Λωρίδας το οποίο ενημερώνει τον οδηγό για ανεπιθύμητη αλλαγή λωρίδας με δονήσεις στο κάθισμα και το σύστημα αυτόματης επικοινωνίας μεταξύ οχημάτων

αποτελούν τα πρώτα παραδείγματα υλοποιήσεων τέτοιου είδους εφαρμογών. Ήδη συστήματα όπως η υποβοήθηση στάθμευσης, η αυτόματη ειδοποίηση για τις ζώνες ασφαλείας ή ανοικτές πόρτες, έχουν γίνει αναπόσπαστο κομμάτι της σύγχρονης αυτοκίνησης. Παράλληλα πιθανή εφαρμογή θα ήταν η διαχείριση της κυκλοφορίας με βάση την πληροφορία που συλλέγουν τα ίδια τα οχήματα από τα γύρω τους. Πιο συγκεκριμένα σε συνδυασμό με το σύστημα πλοήγησης το όχημα θα μπορούσε να προτείνει εναλλακτικές διαδρομές για κάποιον προορισμό, ή να ειδοποιεί τα άλλα οχήματα για ενδεχόμενο κίνδυνο ή για αυξημένη κίνηση. Επίσης η οδική σήμανση θα μπορούσε να μεταβάλλεται δυναμικά με στόχο την κυκλοφοριακή αποσυμφόρηση και ανάλογα με την πληροφορία που συλλέγεται από τα ίδια τα οχήματα της κάθε περιοχής.

1.2.3 Περιβάλλον

Στον τομέα της διαχείρισης πόρων του περιβάλλοντος και των οικολογικών δράσεων οι εφαρμογές του IoT θα μπορούσαν νε περιλαμβάνουν, την παρακολούθηση πληθυσμών απειλούμενων ζώων με στόχο την καλύτερη προστασία τους και την επίβλεψη δασικών οικοσυστημάτων για την πρόληψη πυρκαγιών. Ακόμη εφαρμογές με σημαντικότητα στον περιβαλλοντικό τομέα θα είναι αυτές που θα συμβάλλουν στην παρακολούθηση του φαινομένου του θερμοκηπίου. Ειδικότερα εξελιγμένα συστήματα μετεωρολογικής παρακολούθησης, θα δίνουν τη δυνατότητα για καλύτερα μοντέλα πρόβλεψης, ενώ ταυτόχρονα θα μπορούν να αλληλεπιδρούν με άλλα συστήματα που εξαρτώνται από τις καιρικές συνθήκες. Παράδειγμα αποτελεί η έγκαιρη ειδοποίηση σε αγροτικές περιοχές για έντονα καιρικά φαινόμενα που ίσως απειλούν τις καλλιέργειες. Μια ακόμη πιθανή εφαρμογή θα μπορούσε να προλαμβάνει ρύπανση του υδροφόρου ορίζοντα, ή να εξάγει συμπεράσματα για την καλύτερη αξιοποίηση των αποθεμάτων νερού.

1.2.4 Διαχείριση Εφοδιαστικής Αλυσίδας

Στο Διαδίκτυο των Πραγμάτων, ο τρόπος που γίνεται η διαχείριση των εφοδιαστικών αλυσίδων θα μπορέσει επίσης να αλλάξει. Η διάδοση της πληροφορίας από κάθε μέλος της αλυσίδας προς τα υπόλοιπα θα είναι άμεση και θα έχει ως αποτέλεσμα τη μείωση των μεταβολών ροών σ' ένα δικτυωμένο σύστημα (bullwhip effect). Παράλληλα η βελτιστοποίηση της εφοδιαστικής αλυσίδας θα δημιουργήσει το υπόβαθρο για την αντιμετώπιση και άλλων προβλημάτων όπως η μη διαθεσιμότητα προϊόντων στα ράφια του καταστήματος.

Οι νέες εφαρμογές θα μπορούσαν επίσης να έχουν ως προσανατολισμό την επίλυση παραδοσιακών προβλημάτων, των εφοδιαστικών αλυσίδων. Πέρα από τα ζητήματα που ήδη αναφέρθηκαν, λύσεις αναζητούνται για τον καλύτερο προσδιορισμό του κύκλου ζωής των προϊόντων και του χειρισμού τους στο πλαίσιο αυτό. Παράλληλα η διαχείριση του αποθέματος των κόμβων μιας εφοδιαστικής αλυσίδας αναμένεται να γίνει αποτελεσματικότερη, δεδομένης της αυξημένης πληροφόρησης που θα γίνει διαθέσιμη. Συστήματα που δείχνουν την τάση αυτή, έχουν ήδη υλοποιηθεί και λειτουργούν είτε σε ερευνητικό ή και σε επιχειρησιακό επίπεδο. Χαρακτηριστικό παράδειγματα αποτελεί το σύστημα της αλυσίδας λιανεμπορίου Walmart 6 που θεωρείται από τα πλέον ανεπτυγμένα στο χώρο.

1.2.5 Υπηρεσίες Υγείας

Ένας ακόμη κλάδος που αναμένεται να μεταβληθεί κατά τη μετάβαση στην εποχή του IoT, είναι αυτός των υπηρεσιών υγείας. Μια από τις πρώτες εφαρμογές που θα μπορούσαν να υλοποιηθούν είναι αυτή της παρακολούθησης των ασθενών σε ένα

ενοποιημένο σύστημα που θα μπορεί να συνδέει το ιστορικό, την φαρμακευτική αγωγή και την πορεία τους σε ενδονοσοκομειακό ή μη περιβάλλον. Τέτοιου τύπου εφαρμογές θα μπορούσαν να φανούν ιδιαίτερα χρήσιμες, όταν ο παράγοντας του χρόνου είναι κρίσιμος για την λήψη ιατρικών αποφάσεων. Ειδικότερα, ιατρικά δεδομένα που αφορούν τον ασθενή (αρτηριακή πίεση, σάκχαρο στο αίμα κλπ) θα είναι άμεσα προσβάσιμα σε πραγματικό χρόνο από τους θεράποντες ιατρούς σε περίπτωση ανάγκης. Το γεγονός αυτό θα μειώσει τον απαιτούμενο χρόνο διάγνωσης, ενώ θα μπορεί να προστατεύσει τους ασθενείς από έκτακτα συμπτώματα χρόνιων παθήσεων.

1.2.6 Παιδεία – Εκπαίδευση

Ώθηση και στον χώρο της εκπαίδευσης μπορούν να προσφέρουν εφαρμογές, που εκμεταλλεύονται τον πλούτο της διαθέσιμης πληροφορίας, για να προσφέρουν καλύτερης ποιότητας γνώση στους ενδιαφερόμενους. Παραδείγματα με πολυμεσικές εφαρμογές και έμπειρα συστήματα ήδη υπάρχουν και αποτελούν το πρώτο βήμα προς τη κατεύθυνση αυτή. Μια τεχνολογική εφαρμογή τέτοιου είδους είναι η συσκευή kindle 7 που αποτελεί το πρώτο «ηλεκτρονικό βιβλίο» ευρείας κατανάλωσης, με δυνατότητες να προτείνει αναγνώσματα στο χρήστη ανάλογα με τις επιθυμίες του ή άλλα κριτήρια που αυτός θέτει. Μελλοντικά τέτοια συστήματα με βάση τα κοινωνικά δίκτυα θα μπορούν να αναλάβουν διαδικασίες όπως η ξενάγηση σε μουσεία ή η «έξυπνη μαθητική τάξη» του ερευνητικού έργου POGO.

Συναφείς εφαρμογές θα είναι διαθέσιμες σε μαθητές με ειδικές ανάγκες (πχ κάρτες που θα αλλάζουν μέγεθος γραμμάτων σε υπολογιστές για μαθητές με προβλήματα όρασης), διδασκαλία εξ αποστάσεως, εξοικονόμηση ενέργειας στα σχολικά κτίρια, έλεγχος πρόσβασης και σχολική ασφάλεια, κινητές εφαρμογές για τη συνεχή υποστήριξη της μαθησιακής διαδικασίας κλπ.

1.2.7 Διακυβέρνηση

Εφαρμογές που θα κάνουν δυνατή την ταχύτερη εξυπηρέτηση των πολιτών από το κράτος, αλλά ταυτόχρονα θα επιτρέπουν και την συνέργεια μεταξύ διαφορετικών υπηρεσιών είναι ακόμη μια περίπτωση λύσεων που μπορούν να αναπτυχθούν. Τα συστήματα αυτά μπορούν να μειώσουν τα κόστη λειτουργίας των δημόσιων υπηρεσιών αυξάνοντας παράλληλα την παρεχόμενη ποιότητα. Έχουν ήδη αρχίσει να αναπτύσσονται και να αυτοματοποιούν κυρίως ενδοεπιχειρησιακές λειτουργίες.

Η εισαγωγή των έξυπνων δικτύων στις κρατικές λειτουργίες θα επιτρέπουν την από απόσταση διαχείριση του φωτισμού του οδικού δικτύου, το πότισμα των φυτών στα πάρκα και στιε πλατείες, την έξυπνη διαχείριση της κυκλοφορίας των φωτεινών σημετοδοτών, τις «έξυπνες» στάσεις λεωφορείων κλπ.

Μια πρόσφατη μελέτη (2014) της εταιρίας CISCO με τίτλο «Internet of Everything: A $4.6 Trillion Public-Sector Opportunity» [4], υπολογίζει τα συνολικά οφέλη εξοικονόμηση κόστους από την εφαρμογή του IoT για το δημόσιο τομέα στις ΗΠΑ σε 4,6 τρις δολλάρια μέχρι το 2020.

Τέτοια συστήματα έχουν ήδη εισαχθεί σε Ευρωπαικές χώρες όπως η Γερμανία, Η Σουηδία αλλά και εκτός Ευρώπης στην Ιαπωνία, η Ν. Κορέα και στις ΗΠΑ.

4 http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe_public_sector_vas_white%20paper_121913final.pdf

1.3 Επιχειρηματικές Ευκαιρίες

Όπως αναλύθηκε ήδη, υπάρχει ένα εύρος εφαρμογών οι οποίες μπορούν να αναπτυχθούν εκτενέστερα. Για την ανάπτυξη τους όμως και την τελική τους χρήση σε ευρεία κλίμακα, είναι αναγκαία η συμμετοχή και η συνεργασία αρκετών επιμέρους οργανισμών. Η ανάγκη αυτή αποτελεί ταυτόχρονα επιχειρηματική ευκαιρία για τους οργανισμούς αυτούς που θα κληθούν να επενδύσουν και να αξιοποιήσουν επενδύσεις. Μπορούμε να διακρίνουμε τρεις βασικούς «δράστες» στην διαδικασία μετάβασης στο περιβάλλον του IoT.

Οργανισμοί, πιο ειδικά ερευνητικά κέντρα, πανεπιστημιακοί οργανισμοί, τμήματα R&D εταιρειών. Οι παραπάνω θα κληθούν να δώσουν απαντήσεις και λύσεις στις προκλήσεις, που θα παρουσιάζονται στην πορεία υιοθέτησης κάθε επιμέρους τεχνολογίας και επιχειρηματικής προσέγγισης, που συνολικά θα οδηγήσουν σε ένα περιβάλλον IoT. Με δραστηριοποίηση στους τομείς αυτούς, οι παραπάνω δράστες θα μπορούσαν να διεκδικήσουν χρηματοδοτήσεις, από κρατικούς πόρους, ενδιαφερόμενες εταιρείες ή άλλους οργανισμούς με προθέσεις επενδύσεων σε αυτές τις τεχνολογίες.

Κατασκευαστές συσκευών και λογισμικού, προσδοκούν μια νέα πηγή εσόδων από τέτοιες δραστηριότητες. Τέτοιες εταιρείες μπορεί να είναι τηλεπικοινωνιακοί οργανισμοί, κατασκευαστές υλισμικού (δικτυακά προϊόντα, RFID) και εταιρείες ανάπτυξης εφαρμογών λογισμικού.

Χρήστες, τόσο σε ατομικό όσο και σε επίπεδο οργανισμών. Είναι όλοι αυτοί που θα κληθούν να υιοθετήσουν τα νέα δεδομένα και να αξιοποιήσουν τις δυνατότητες που τους προσφέρονται από τις νέες εφαρμογές. Οι χρήστες αυτοί θα μπορούν να βελτιστοποιήσουν τις διαδικασίες και τον τρόπο που χειρίζονται την πληροφορία ώστε να αποκομίσουν κέρδος. Το κέρδος αυτό μπορεί να είναι

χρηματικό ή και πρόσθετη καλύτερης ποιότητας, πληροφορία. Θα πρέπει να τονιστεί πως οι χρήστες παίζουν βασικό ρόλο στην εμπορευματοποίηση ενός συνόλου υπηρεσιών. Για αυτό το λόγο είναι κρίσιμη η συμμετοχή ενός χρήστη με ηγετικό ρόλο στην αγορά που θα συμπαρασύρει μικρότερους χρήστες στην υιοθέτηση της νέας προσέγγισης.

Τέτοιο παράδειγμα αποτελεί η εταιρεία λιανικής πώλησης Walmart που αποτελεί πρωτοπόρο στην υιοθέτηση ενός συστήματος βελτιστοποίησης της εφοδιαστικής αλυσίδας, που να ακολουθεί τις αρχές του IoT. Παράλληλα θα πρέπει να υπάρχει και πρωτοβουλία και σε κρατικό επίπεδο αφού ένα μεγάλο μέρος των εφαρμογών που θα μπορούσαν να υλοποιηθούν, αφορούν την ηλεκτρονική διακυβέρνηση και τον τρόπο με τον οποία αλληεπιδρά το κράτος τόσο με τους πολίτες όσο και με άλλους οργανισμούς ή κράτη. Πολλά κράτη χρηματοδοτούν έργα και έρευνες για εφαρμογές στο IoT.

Στην Ιαπωνία που με συλλογικές στρατηγικές, προσπαθεί να αναπτύξει τις χρήσεις των νέων τεχνολογιών και να παραμείνει στα πλέον προηγμένα τεχνολογικά κράτη. Η εφαμοζόμενη στρατηγική ονομάζεται Universal Communications (UNS) και στα πλαίσια της θα αναπτυχθούν κυρίως οι αισθητήρες και ετικέτες RFID.

- Πανταχού παρόντα (ubiquitous) ad-hoc δίκτυα
- Διαδραστικό λογισμικό, που να αναγνωρίζει τις προθέσεις των χρηστών.
- Πολλαπλά ευφυή λογισμικά ελέγχου
- Αυθεντικοποίηση με βιομετρικούς ελέγχους
- Βέλτιστη διαχείριση πνευματικών δικαιωμάτων σε ψηφιακά αγαθά
- Κατανεμημένη και συνεργατική λειτουργικότητα λογισμικού

- Προσαρμόσιμες διαδραστικές υπηρεσίες ανα τύπο χρήσης

Πιο συγκεκριμένες εφαρμογές αποτελούν:

- Η ιχνηλασιμότητα τροφίμων που αφορά την ικανότητα παρακολούθησης της διακίνησης ενός τροφίμου κατά τις φάσεις της παραγωγής, επεξεργασίας και διανομής.
- Το «έξυπνο» σπίτι.
- Οι "Έξυπνες Αστικές Κάρτες", με πρώτη χρήση τους σιδηροδρομικούς σταθμούς του Τόκυο.

Γίνεται λοιπόν εμφανές, πως τόσο κατά τη μετάβαση στο IoT όσο και μετά θα δημιουργηθούν οι κατάλληλες συνθήκες για ανάπτυξη. Σε πρώτη φάση οι ανάγκες λύσεις στην διαδικασία υλοποίησης, προκαλούν άμεσα την αύξηση της επιχειρηματικής δραστηριότητας με την ανάπτυξη νέων συστημάτων. Έπειτα υιοθετώντας τις νέες τεχνολογίες οι επιχειρήσεις, θα κληθούν να αναδιαμορφώσουν τις εσωτερικές τους διαδικασίες και να επαναπροσδιορίσουν την επιχειρηματική στρατηγική τους. Η αλλαγή αυτή είναι δυνατόν να οδηγήσει σε νέες ανάγκες, που θα αποτελέσουν αναπτυξιακές ευκαιρίες για νέες επιχειρήσεις.

1.4 Η σημασία της ασύρματης διασυνδεσιμότητας

Για την υλοποίηση των εφαρμογών που περιγράφηκαν στα προηγούμενα κεφάλαια, απαιτείται η ύπαρξη μιας καθολικά διαθέσιμης σταθερής ευρυζωνικής τεχνολογικής υποδομής που θα επιτρέπει στα αντικείμενα να αλληλεπιδρούν ασύρματα και ενσύρματα μεταξύ τους παρέχοντας στους χρήστες, συνεχώς και αδιάλειπτα, ένα σύνολο υπηρεσιών ανεξάρτητων από την επιμέρους υποδομή που την υποστηρίζει. Οι τεχνολογίες αυτές πρέπει να παρέχουν κάποια επίπεδα διαδικτύωσης στα αντικείμενα, ώστε να καταστεί δυνατή η επικοινωνία του

περιβάλλοντας με αυτά. Βασική τέτοια τεχνολογία είναι το RFID (Radio Frequency IDentification) ή «ταυτοποίηση μέσω ραδιοσυχνοτήτων».

1.4.1 Ταυτοποίηση αντικειμένων μέσω ραδιοσυχνοτήτων (RFID)

Η ταυτοποίηση μέσω ραδιοσυχνοτήτων, είναι μια μέθοδος αυτόματης αναγνώρισης αντικειμένων, που μπορεί να ανακτά πληροφορία ασύρματα από προϊόντα που είναι εφοδιασμένα με ετικέτες RFID. Το σύστημα λοιπόν αποτελείται από δύο βασικά μέρη, τον αναγνώστη και την ετικέτα. Ο αναγνώστης είναι η συσκευή που χρησιμοποιείται για την προσπέλαση των αντικειμένων. Είναι εφοδιασμένος με μια κεραία που εκπέμπει ραδιοκύματα στα οποία η ετικέτα ανταποκρίνεται. Η απάντηση λαμβάνεται μέσω της ίδιας κεραίας και προωθείται για επιπλέον επεξεργασία. Η εμβέλεια του αναγνώστη εξαρτάται από ένα αριθμό παραγόντων, όπως:

- Ο τύπος και το μέγεθος της κεραίας
- Η συχνότητα εκπομπής
- Η σχετική θέση μεταξύ κεραίας και ετικέτας
- Ενδεχόμενες παρεμβολές
- Φυσικά χαρακτηριστικά του αντικειμένου(απορροφητικότηταραδιοκυμάτων)
- Τύπος ετικετών

Οι ετικέτες είναι το τμήμα που προσαρμόζεται στο αντικείμενο ώστε να του δώσει τις στοιχειώδεις δυνατότητες δικτύωσης. Πρόκειται για κυκλώματα με δυνατότητα εκπομπής πληροφοριών, που είναι υλοποιημένα με τρόπο τέτοιο ώστε να προσαρμόζονται εύκολα σε αντικείμενα. Συνήθως είναι στη μορφή αυτοκόλλητων ή μικροσκοπικών κατασκευών που μπορούν είτε να κολλήσουν είτε να ενσωματωθούν στο αντικείμενο. Επίσης είναι δυνατή η εκτύπωση του κυκλώματος

πάνω στο σώμα του αντικειμένου με την τεχνολογία τρισδιάστατης εκτύπωσης. Το μέγεθός τους ποικίλει, αλλά η εξέλιξή τους τις κάνει όλο και μικρότερες. Μπορούμε να κατατάξουμε τις ετικέτες σε δύο βασικές κατηγορίες. Τις ενεργητικές και τις παθητικές. Οι ενεργητικές ετικέτες είναι αυτές που εξοπλίζονται και με μια δική τους πηγή ενέργειας. Κοινώς είναι εφοδιασμένες και με μια μπαταρία. Το χαρακτηριστικό αυτό τους δίνει κάποιες ιδιότητες, άλλες θετικές και άλλες αρνητικές. Στα θετικά μπορούμε να συμπεριλάβουμε:

- Την αυξημένη εμβέλεια της συσκευής.
- Την δυνατότητα να φέρει αισθητήρες η οποίοι θα τροφοδοτούνται από την μπαταρία και έτσι θα μπορούν να συλλέγουν πληροφορίες. (πχ. θερμοκρασία)
- Την ανθεκτικότητα σε παρεμβολές.

Στον αντίποδα έχουμε:

- Τον περιορισμένο χρόνο ζωής της ετικέτας, που εξαρτάται από τον χρόνο εξάντλησης των αποθεμάτων της μπαταρίας.
- Το μεγαλύτερο μέγεθος που έχει η συσκευή εξαιτίας της μπαταρίας.
- Το υψηλότερο κόστος της ετικέτας, τόσο όσον αφορά την αγορά όσο και για την συντήρηση, σε περίπτωση που η μπαταρίες αντικαθίστανται.

Οι παθητικές ετικέτες, δεν έχουν ενσωματωμένη πηγή ενέργειας, αλλά χρησιμοποιούν την εκπεμπόμενη ενέργεια από την κεραία του αναγνώστη για την απάντησή τους. Πιο συγκεκριμένα η ενσωματωμένη κεραία που υπάρχει στην ετικέτα δημιουργεί μαγνητικό πεδίο, όταν λαμβάνει ραδιοκύματα από τον αναγνώστη. Το πεδίο αυτό τροφοδοτεί το κύκλωμα της ετικέτας, ώστε αυτό να στείλει τηνπληροφορία στον αναγνώστη. Και ο τύπος αυτός, έχει πλεονεκτήματα και μειονεκτήματα.

Ως πλεονεκτήματα μπορούν να αναφερθούν τα εξής:

- Η μη εξάρτηση από κάποια πηγή ενέργειας δίνει πολύ μεγάλο χρόνο λειτουργίας στην ετικέτα, που πλέον εξαρτάται από την ταχύτητα φθοράς τους υλικού κατασκευής της.
- Το μέγεθος της συσκευής είναι περιορισμένο, καθώς διαθέτει μόνο το κύκλωμα και την ενσωματωμένη κεραία.
- Η ετικέτα είναι φθηνότερη στην κατασκευή της ενώ δεν χρειάζεται συντήρηση.

Από την άλλη πλευρά, στα μειονεκτήματα συγκαταλέγονται:

- Η μικρότερη εμβέλεια της ετικέτας, καθώς και η δυσκολία λειτουργίας σε περιβάλλον με παρεμβολές.
- Δεν είναι δυνατή η ενσωμάτωση αισθητήρων που έχουν ανάγκη από τροφοδοσία σε ηλεκτρική ενέργεια.
- Το γεγονός πως η ετικέτα δεν έχει περιορισμένο χρόνο ζωής, την κάνει ανιχνεύσιμη για πολλά χρόνια, γεγονός που εγείρει ζητήματα ασφάλειας και προστασίας δεδομένων.

Τέλος υπάρχει και μια υβριδική μορφή, οι ημιπαθητικές ετικέτες. Ο τύπος αυτός διαθέτει ενσωματωμένη πηγή ενέργειας η οποία όμως χρησιμοποιείται υπό συνθήκες. Πιο συγκεκριμένα, η ετικέτα χρησιμοποιεί την ενέργεια του αναγνώστη για να εκπέμψει, αλλά τροφοδοτεί από την μπαταρία πιθανούς αισθητήρες που είναι ενσωματωμένοι στη συσκευή ή άλλες εσωτερικές λειτουργίες. Επίσης μπορεί να ενισχύει το εκπεμπόμενο σήμα, σε απαιτητικά περιβάλλοντα όπου υπάρχουν παρεμβολές ή ο αναγνώστης είναι στα όρια της εμβέλειας. Οι ημιπαθητικές ετικέτες συνδυάζουν τα θετικά και τα αρνητικά στοιχεία των άλλων δύο τύπων. Η συχνότητες λειτουργίας του RFID εξοπλισμού, ανήκουν στη δέσμη των ελεύθερων συχνοτήτων ISM. Αυτό επιτρέπει στην χρήση της τεχνολογίας χωρίς την ανάγκη αδειοδότησης από τον υπεύθυνο φορέα. Φυσικά, παρότι η συχνότητα εκπομπής δεν είναι καθορισμένη, η χρήση του RFID πρέπει να υπακούει στους κανονισμούς

σχετικά με την ισχύ του σήματος όπως αυτοί ορίζονται από τον νόμο. Το χαρακτηριστικό αυτό συνεπάγεται δύο κύριες επιπτώσεις:

- Αυτή η περιοχή συχνοτήτων, είναι κορεσμένη γι' αυτό και υπάρχουν παρεμβολές.
- Στην ίδια περιοχή φάσματος λειτουργούν δύο πολύ διαδεδομένες τεχνολογίες, το wifi και το Bluetooth. Το γεγονός αυτό από τη μία ευθύνεται για παρεμβολές αλλά από την άλλη μπορεί να αποτελέσει τη βάση για κάποια συνέργεια μεταξύ των τεχνολογιών.

ΚΕΦΑΛΑΙΟ 2

Το τεχνολογικό υπόβαθρο του Διαδικτύου των Πραγμάτων

Για να επικοινωνήσουν μεταξύ τους οι διασυνδεδεμένες συσκευές χρειάζονται μια κοινή τεχνική γλώσσα, ένα κοινά αποδεκτό και κατανοητό πρωτόκολλο επικοινωνίας με επαρκή χωρητικότητα ώστε να υποστηρίξει συνεχώς και αποτελεσματικά τις πολλαπλές και κρίσιμες εφαρμογές σε βιομηχανία, οικονομία και κοινωνία.

2.1 Εισαγωγή

Το πρωτόκολλο επικοινωνίας που χρησιμοποιείται σήμερα ευρύτερα από κάθε άλλο είναι το IPv4. Αυτό μας παρέχει τη δυνατότητα να έχουμε στο Διαδίκτυο περίπου 4,3 δισεκατομμύρια διαφορετικές διευθύνσεις. Ο αριθμός ακούγεται σχετικά μεγάλος, αλλά δεν είναι στην πραγματικότητα αφού λάβουμε υπόψιν τα εξής στοιχεία :

- Το Διαδίκτυο αποκτά ολοένα και περισσότερους χρήστες, με πολυπληθείς χώρες όπως η Κίνα, να υιοθετούν ολοένα και ταχύτερα την πρόσβασή τους σε αυτό.

- Οι IP enabled συσκευές που πωλούνται διεθνώς ολοένα και αυξάνονται. Οι διαδικτυακές τηλεοράσεις, οι τρισδιάστατοι εκτυπωτές, τα ραδιόφωνα καθώς και οι ελεγχόμενες ηλεκτρικές συσκευές μέσω διαδικτύου γίνονται όλο και πιο δημοφιλείς.

- Πολλοί οικιακοί χρήστες πλέον τρέχουν ιδιωτικούς servers για να παρέχουν διάφορες υπηρεσίες στον κοινωνικό τους περίγυρο και όχι μόνο.

- Τα κινητά τηλέφωνα και οι προσωπικές ψηφιακές συσκευές μετατρέπονται από μεμονωμένες συσκευές σε εργαλεία πρόσβασης σε μία σειρά υπηρεσιών που παρέχονται μέσω Διαδικτύου.

- Η αυτοκινητοβιομηχανία θέλει να αποδίδει σε κάθε όχημα που κατασκευάζεται μία μοναδική διεύθυνση μέσω της οποίας θα μπορεί να ελέγχει την κατάσταση του οχήματος. Παρέχει online υπηρεσίες όπως η αναβάθμιση firmware και του ανασχεδιασμού των επιμέρους τμημάτων που το απαρτίζουν.

Με τα παραπάνω, γίνεται κατανοητό ότι οι διευθύνσεις που μας παρέχει το IPv4 πολύ σύντομα θα πληρωθούν και από ένα σημείο και μετά δεν θα υπάρχουν άλλες διαθέσιμες.

Το IPv6 δημιουργήθηκε με στόχο να επιλυθεί αυτό ακριβώς το πρόβλημα.Το IPv6 είναι το επόμενο επίπεδο των IP's. Από ότι φαίνεται η έκδοση 6, θα είναι κατά πάσα πιθανότητα το επόμενο ευρέως διαδεδομένο πρωτόκολλο Internet. Σε σύγκριση με το IPv4 το οποίο επιτρέπει μόνο 4.294.967.296 μοναδικές

διευθύνσεις, το IPv6 που χρησιμοποιεί ένα σύστημα 128-bit που θα μπορεί να δώσει 340 - ενδεκάκις εκατομμύρια [undecillion] (34, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000 , 000) Όπως ήταν αναμενόμενο, παρότι ο μοναδικός λόγος που ξεκίνησε η ανάπτυξή του ήταν ο παραπάνω, στην πορεία αποφασίστηκε ότι ήταν μια καλή ευκαιρία να γίνουν κάποιες βελτιώσεις σε επιμέρους ζητήματα όπου το IPv4 έχει επιδείξει κάποιες αδυναμίες.

2.2 Η Ιστορία του Internet Protocol

Το πρωτόκολλο Internet (Internet Protocol-IP) μπόρεσε να συνδέσει εκατομμύρια υπολογιστών και να φέρει μία καινούργια πραγματικότητα στην παροχή πρόσβασης στην πληροφορία. Το IP αναπτύχθηκε πριν είκοσι χρόνια σαν το πρωτόκολλο του network επιπέδου της αρχιτεκτονικής του Διαδικτύου (Internet) και μαζί με το πρωτόκολλο του transport επιπέδου TCP (Transmission Control Protocol) δημιούργησαν την οικογένεια πρωτοκόλλων TCP/IP. Στην αρχή το TCP/IP χρησιμοποιήθηκε για την διασύνδεση των διαφορετικών υπολογιστικών συστημάτων που χρησιμοποιούσε η κυβέρνηση των Η.Π.Α αλλά λόγω της εξαιρετικής του δύναμης εξαπλώθηκε παγκοσμίως νικώντας τις άλλες δικτυακές κατευθύνσεις και τεχνολογίες όπως: OSI, SNA, DECnet, NETware, κ.α. Το IP λοιπόν έγινε η βάση της δημιουργίας πάρα πολλών client-server ή peer-to-peer εφαρμογών και εκμεταλλεύεται έτσι την δυνατότητα της δικτυακής σύνδεσης. Το σημερινό Internet αποτελεί εξέλιξη του ARPANET, ενός δικτύου που άρχισε να αναπτύσσεται πειραματικά στα τέλη της δεκαετίας του 60 στις ΗΠΑ.

Σταδιακά όλο και περισσότερες χώρες συνδέονται στο NSFNET, μεταξύ των οποίων και η Ελλάδα το 1990. Το 1991, το εργαστήριο CERN στην Ελβετία παρουσιάζει το World Wide Web (WWW) (Παγκόσμιο Ιστό) που αναπτύχθηκε από τον Tim Berners-Lee. Πρόκειται για ένα σύστημα διασύνδεσης πληροφοριών

σε μορφή πολυμέσων (multimedia) που βρίσκονται αποθηκευμένες σε χιλιάδες υπολογιστές του Internet σε ολόκληρο τον κόσμο και παρουσίασής τους σε ηλεκτρονικές σελίδες, στις οποίες μπορεί να περιηγηθεί κανείς χρησιμοποιώντας το ποντίκι. Το γραφικό αυτό περιβάλλον έκανε την εξερεύνηση του Internet προσιτή στον απλό χρήστη. Παράλληλα, εμφανίζονται στο Internet διάφορα εμπορικά δίκτυα που ανήκουν σε εταιρίες παροχής υπηρεσιών Internet (Internet Service Providers - ISP) και προσφέρουν πρόσβαση στο Internet για όλους. Οποιοσδήποτε διαθέτει PC και modem μπορεί να συνδεθεί με το Internet σε τιμές που μειώνονται διαρκώς. Το 1995, το NSFNET καταργείται πλέον επίσημα και το φορτίο 11 του μεταφέρεται σε εμπορικά δίκτυα. Πλέον η απόκτηση domain names δεν είναι δωρεάν. Σαν αποτέλεσμα το έτος 1996, περίπου 10,000 εταιρίες χάνουν τα ονόματα χώρων τους καθώς δεν είχαν πληρώσει τέλη για αυτά.

2.3 Τεχνικά προβλήματα του IPv4

Όπως προναφέρθηκε, το Διαδίκτυο αυτήν τη στιγμή χρησιμοποιεί την έκδοση τέσσερα (4) του Internet πρωτοκόλλου, γνωστή συνοπτικά σαν IPv4. Πρόκειται αναμφίβολα για το πιο πετυχημένο πρωτόκολλο με χρήση του οποίου συνδέθηκαν χιλιάδες κόμβοι εκατοντάδων διαφορετικών δικτύων δημιουργώντας αυτό που σήμερα ονομάζουμε Διαδίκτυο. Αρκετές δεκάδες εκατομμυρίων υπολογιστών και εκατοντάδες εκατομμυρίων χρηστών είναι συνδεμένοι στο Διαδίκτυο.

Η πρώτη έκδοση του IP έγινε τα μέσα του 1970. Επομένως θα έλεγε κανείς ότι το IPv4 δουλεύει αρκετά καλά, ιδιαίτερα αν αναλογιστούμε την ηλικία του. Κάθε σύστημα στον κόσμο σήμερα χρησιμοποιεί IPv4 (εκτός από τα πειραματικά δίκτυα που χρησιμοποιούν από τώρα IPv6). Μιλάμε για ένα αριθμό συστημάτων της τάξης των 100 εκατομμυρίων, που χρησιμοποιούν διάφορες εκδόσεις δικτυακού λογισμικού για TCP/IP, που τρέχουν σε μια πληθώρα λειτουργικών συστημάτων

και υλικού. Αντιλαμβανόμαστε λοιπόν ότι μια πιθανή αναβάθμιση του πρωτοκόλλου θα επηρεάσει όλο το πιο πάνω αριθμό συστημάτων και οργανισμών αφού και αυτά πρέπει να αναβαθμιστούν ώστε να είναι συμβατά με το νέο πρωτόκολλο. Οι βασικοί λόγοι που απαιτείται η αναβάθμιση είναι οι παρακάτω:

- Θέματα έλλειψης διευθύνσεων: Αν και οι χρήστες πιστεύουν ότι αυτός εμφανίζεται σαν ο βασικότερος λόγος αναβάθμισης του IPv4, ουσιαστικά πρόκειται μόνο για ένα από τα προβλήματα που απασχολούν την κοινότητα του Διαδικτύου.

- Θέματα απόδοσης: Παρ' όλο που το IP λειτουργεί αποδοτικά τα 30 και πλέον χρόνια που χρησιμοποιείται, υπάρχουν πάρα πολλές βελτιώσεις που μπορούν να γίνουν. Οι διαχειριστές γνωρίζουν καλύτερα από όλους το κόστος διαχείρισης των routing entries εξαιτίας της έλλειψης επιπέδων ιεραρχίας στις IP διευθύνσεις. Επίσης αρκετές εφαρμογές απαιτούν υποστήριξη ποιότητας εξυπηρέτησης (QoS) από το IPv4 και προσπαθούν να ξεπεράσουν αυτή του την αδυναμία με χρήση άλλων πρωτοκόλλων σε υψηλότερα επίπεδα, μην πετυχαίνοντας όμως τα αναμενόμενα.

- Θέματα ασφάλειας: Μετά την τεράστια εξάπλωση που γνώρισε το Διαδίκτυο και τη χρήση του σε κάθε είδος οικονομικής συναλλαγής διαπιστώθηκε ότι η ασφάλεια δεν μπορεί να απασχολεί μόνο τις εφαρμογές, αλλά το ίδιο το IP θα πρέπει να έχει μηχανισμούς ασφάλειας.

- Θέματα αυτόματης ανάθεσης διεύθυνσης: Είναι γνωστό ότι οι ρυθμίσεις του IPv4 στους κόμβους είναι σχετικά πολύπλοκη διαδικασία. Οι χρήστες θα επιθυμούσαν μία λειτουργία "plug and play" με την έννοια του να μπορεί κάποιος να συνδέει τον υπολογιστή του στο δίκτυο IP και αυτός να μπορεί αυτόματα να βρίσκει τις ρυθμίσεις του. Οι ανάγκες των συνεχώς αυξανόμενων χρηστών που δεν

έχουν σταθερό χώρο εργασίας (mobile users) απαιτούν αυτόματες ρυθμίσεις ανεξάρτητα του δικτύου που χρησιμοποιούν κάθε φορά για να συνδεθούν.

2.4 Τεχνικές διαφορές μεταξύ IPv4 και IPv6

Εκτός από τις διαφορές που έχουν ήδη αναφερθεί υπάρχουν και άλλες διαφορές μεταξύ των δύο πρωτοκόλλων. Το IPv4 είχε κλάσεις διευθύνσεων: Η κλάση Α χρησιμοποιεί 7 bit για τα πιθανά υποδίκτυα και 24 bit για τις δικτυακές συσκευές που μπορούν να συνδεθούν στα υποδίκτυα. Η κλάση Β χρησιμοποιεί 14 bit για τον αριθμό των υποδικτύων και 16 bit για τους hosts. Η κλάση C χρησιμοποιεί 21 bit για τα δίκτυα και 8 bit για τους hosts.

Η κλάση Β αποδείχθηκε η πιο διάσημη γιατί οι περισσότερες επιχειρήσεις ήθελαν περισσότερες από 255 διευθύνσεις όμως συνήθως και πολύ λιγότερες από 65535. Στην αρχή όσοι είχαν ανάγκη για παραπάνω από 255 διευθύνσεις τους έδιναν μία κλάση Β. Στις αρχές του 1990, είχε γίνει προφανές ότι τελείωναν πολύ γρήγορα οι διευθύνσεις, και πολλές από αυτές ήταν αχρησιμοποίητες με αυτή τη μέθοδο, γι' αυτό άρχισαν να δίνονται και μέρη διευθύνσεων της κλάσης C αντί για μια ολόκληρη κλάση Β.

Το πρόβλημα βρήκε λύση το 1993 με την υιοθέτηση του CIDR (Classless Interdomain Routing). Με το CIDR η διάκριση σε κλάσεις δεν χρειαζόταν πια. Μια τιμή τώρα πια υποδείκνυε τη διάκριση σε bits που δείχνουν τα υποδίκτυα και τα bits που δείχνουν τις δικτυακές συσκευές στα υποδίκτυα. Το IPv6 και αυτό δεν έχει κλάσεις και χρησιμοποιεί τεχνική παρόμοια με αυτή του CIDR.

Στα δίκτυα IPv4 δεν υπήρχε καμία σχέση ανάμεσα στη διεύθυνση MAC ενός υπολογιστή σε ένα δίκτυο Ethernet με την IP που του είχε ανατεθεί. Έτσι υπήρχε ανάγκη για ένα πρωτόκολλο που να αντιστοίχιζε τις διευθύνσεις IP με τις διευθύνσεις MAC. Το πρωτόκολλο αυτό ονομάζεται ARP(Address Resolution

Protocol). Αρχικά όταν κάποιος θέλει να στείλει ένα μήνυμα σε μια διεύθυνση IP κάνει broadcast τη διεύθυνση στην οποία θέλει να στείλει το μήνυμα και ο υπολογιστής που την έχει απαντά. Έτσι μαθαίνει την διεύθυνση MAC που έχει ο υπολογιστής και σε ποια IP αντιστοιχεί.

Στο IPv6 πολλές φορές μπορεί να μην εμπεριέχεται η MAC διεύθυνση και γι' αυτό υπάρχει και εδώ ένας παρόμοιος μηχανισμός με το πρωτόκολλο ARP. Το ARP όμως χρησιμοποιεί broadcasts που το IPv6 δεν υποστηρίζει. Αντίθετα το IPv6 χρησιμοποιεί εκτενώς multicasts. Στο multicast τα πακέτα μεταδίδονται μόνο σε μια ορισμένη ομάδα δικτυακών συσκευών και όχι σε όλες. Στο IPv6 το αντίστοιχο πρωτόκολλο του ARP είναι το ND(Neighbor Discovery) και βασίζεται σε multicasts, είναι πιο γενικό από το ARP και όχι τόσο εξαρτώμενο από τα δίκτυα Ethernet. Στο IPv6 επίσης χρησιμοποιείται η τεχνολογία DAD(Duplicate Address Detection) δανεισμένη από το πρωτόκολλο AppleTalk και ανιχνεύει όπως λέει και το όνομά της αν υπάρχουν δικτυακές συσκευές που έχουν την ίδια IP ώστε να αποφευχθεί κάτι τέτοιο.

2.5 Πλεονεκτήματα και Μειονεκτήματα του IPv6 με το IPv4

Το πιο προφανές και με διαφορά πιο σημαντικό πλεονέκτημα της καινούριας έκδοσης του IP είναι ο πολύ μεγαλύτερος χώρος διευθύνσεων. Επίσης προσφέρει βαθύτερη ιεραρχία διευθυνσιοδότησης αλλά και απλούστερες ρυθμίσεις. Μια μέρα θα έχουμε ξεχάσει πως ήταν να έχουμε μια διεύθυνση των 32 Bytes.Οι διαχειριστές δικτύων θα αγαπήσουν τους μηχανισμούς αυτοδιαμόρφωσης που παρέχει το νέο πρωτόκολλο. Ακόμα και αν η αύξηση σε απαιτήσεις για χώρο διευθύνσεων διπλασιαζόταν κάθε 5 χρόνια όπως γινόταν για κάποιο χρονικό διάστημα, που είναι εκθετικός ρυθμός αύξησης, τότε οι διαθέσιμες διευθύνσεις θα τελείωναν το 2485. Ουσιαστικά δηλαδή, το νέο πρωτόκολλο αυξάνει τη

χωρητικότητα και επιλύει το πρόβλημα του περιορισμένου χώρου διευθύνσεων του IPv4.

- **Απλοποίηση της Επικεφαλίδας**: Στο IPv6 η επικεφαλίδα έχει μήκος 40 Bytes. Αυτό σημαίνει πως διαθέτουμε μόνο 8 Bytes για την επικεφαλίδα καθώς έχουμε και δύο IP διευθύνσεις, του αποστολέα και του παραλήπτη. Κάποια πεδία από την επικεφαλίδα του IPv4 έχουν αφαιρεθεί. Με αυτή την αλλαγή τα πακέτα γίνονται γρηγορότερα στη διαχείριση και σαν αποτέλεσμα έχουμε την μείωση του επεξεργαστικού κόστους.

- **Αυξημένη υποστήριξη για επεκτάσεις και επιλογές**: Στην IPv4 οι επιλογές ήταν ενσωματωμένες στην βασική επικεφαλίδα. Πλέον, ορίζονται οι επικεφαλίδες επέκτασης. Τα χαρακτηρίστηκα τους είναι ότι είναι προαιρετικές και εισάγονται πάντα ανάμεσα στην βασική επικεφαλίδα και στο φορτίο. Με αυτόν τον τρόπο τα πακέτα γίνονται πολύ ευέλικτα. Η δρομολόγηση των πακέτων γίνεται πολύ περισσότερο αποτελεσματική. Οι επιλογές μπορούν να εισαχθούν με ευκολία.

- Δ**υνατότητα αποτύπωσης των ροών κίνησης**: Τα πακέτα που ανήκουν στην ίδια ροή πακέτων απαιτούν ειδική διαχείριση και μπορουν να αποτυπωθούν από τον αποστολέα. Ένα παράδειγμα που εφαρμόζεται είναι οι υπηρεσίες πραγματικού χρόνου.

- **Καινοτομία:** Με την τεχνολογία NAT σήμερα συνεχίζεται η λειτουργία του IPv4. Η συγκεκριμένη τεχνολογία λύνει κάποια προβλήματα, σε κλασικές εφαρμογές client/server (π.χ email, web κλπ). Αντίθετα, σε άλλες εφαρμογές όμως, όπως VoIP, όπου κάθε Η/Υ πρέπει να είναι «διακριτός» και για όσους είναι έξω του δικτύου που χρησιμοποιεί NAT, η τεχνολογία NAT σίγουρα δυσκολεύει τη λειτουργία τους.

• **Αυτορύθμιση διεύθυνσης**: Στο IPv4 χρησιμοποιούνταν το πρωτόκολλο DHCP για να λάβει μία συσκευή αυτόματα IP διεύθυνση. Αυτό έχει 2 μεγάλα μειονεκτήματα:

1) Χρειάζεται 1 DHCP server.

2) Δεν υπάρχει εγγύηση ότι το ίδιο μηχάνημα θα λάβει την ίδια διεύθυνση (εκτός βέβαια και αν ρυθμιστεί ρητά με αντιστοίχηση της MAC διεύθυνσής του). Με το IPv6 υπάρχει μεν μια ανανεωμένη έκδοση του DHCP το DHCPv6 αλλά με το IPv6 υπάρχει και άλλη επιλογή για την αυτόματη ρύθμιση της διεύθυνσης, που ονομάζεται stateless autoconfiguration. Με αυτή την επιλογή κάθε δικτυακή συσκευή περιμένει να «ακούσει» ποια 64 bit να χρησιμοποιήσει για το πρώτο μέρος της IPv6 διεύθυνσης. Όσες συσκευές είναι μέρος του ίδιου δικτύου έχουν το ίδιο 64-bit πρόθεμα. Τα υπόλοιπα bit συμπληρώνονται από τη MAC διεύθυνση των συσκευών αυτών. Οι MAC διευθύνσεις είναι 48 bit συνεπώς τα υπόλοιπα 16 συμπληρώνονται κατά 1 προσυμφωνημένο τρόπο, συνήθως με 1. Με αυτόν τον τρόπο ο ίδιος Η/Υ παίρνει την ίδια IP κάθε φορά στο ίδιο δίκτυο και χωρίς την ανάγκη ύπαρξης DHCP server. Βέβαια οι δρομολογητές συνεχίζουν να «διαφημίζουν» στους Η/Υ ποιους δρομολογητές μπορούν να χρησιμοποιήσουν για να επικοινωνήσουν με το υπόλοιπο Internet.

• **Εύκολη αλλαγή διεύθυνσης**: Σύμφωνα με τον παραπάνω τρόπο αυτόματης ρύθμισης της διεύθυνσης, είναι πολύ εύκολο οι δικτυακές συσκευές ενός ολόκληρου δικτύου να αλλάξουν διεύθυνση. Απλά αλλάζει το 64-bit που διαφημίζεται με ένα καινούριο. Οι παλιές διευθύνσεις βέβαια παραμένουν σε ισχύ για τυχόν επικοινωνίες που είναι ήδη ανοιχτές ή δεν έχουν ενημερωθεί για την αλλαγή αλλά όσες καινούριες φτιάχνονται χρησιμοποιούν τις καινούριες, αλλαγμένες διευθύνσεις.

• **Ασφάλεια**: Ο πιο διαδεδομένος μύθος για το IPv6 είναι ότι θα είναι πιο ασφαλές από το IPv4 επειδή θα έχει «υποχρεωτική» υποστήριξη του IPSec. Το IPSec παρέχει κρυπτογράφηση και πιστοποίηση στο επίπεδο του IP προστατεύοντας έτσι τα δεδομένα μιας εφαρμογής από το να αλλαχθούν κατά τη μεταφορά τους. Στην πραγματικότητα όμως το IPSec είναι ήδη διαθέσιμο και για το IPv4 και το γεγονός ότι συμπεριλαμβάνεται στο IPv6 δε σημαίνει ότι δε χρειάζεται εκτενείς προσπάθειες για τη ρύθμιση και τη λειτουργία του.

Στο IPv4 βέβαια, είναι ακόμα πιο δύσκολη η ρύθμισή του, καθώς το NAT περιπλέκει τα πράγματα, επειδή υπάρχει «μετάφραση» στη μέση. Το IPv6 ωστόσο έχει ένα πλεονέκτημα ασφαλείας σε σχέση με το IPv4. Επειδή είναι μεγάλος ο χώρος διευθύνσεων, ένα worm είναι δύσκολο να «σκανάρει» όλο το υποδίκτυο. Στο IPv4, οι συσκευές ενός υποδικτύου το πολύ να είχαν μια 16 bit διεύθυνση, οπότε το worm μπορούσε συνήθως να κάνει port scanning σε όλους, ενώ με το IPv6, που ένα σύνηθες υποδίκτυο μπορεί να είναι ακόμα και 64 bit, είναι σχεδόν αδύνατο να το κάνει. Είναι σαν να «σκανάρει» ένα δίκτυο δύο φορές όσο το σημερινό IPv4 Internet.

• **Φορητότητα**: Με την χρήση του IPv4 για να επικοινωνήσει ένας φορητός κόμβος η διαδικασία ήταν η εξής: Τα πακέτα από τον φορητό κόμβο στέλνονται στον κεντρικό πάροχο και στην συνέχεια αυτός τα στέλνει στην τελική διεύθυνση και το ανάποδο. Με την χρήση του IPv6 η επικοινωνία μεταξύ του φορητού κόμβου και της διεύθυνσης επικοινωνίας είναι άμεση. Το πλεονέκτημα είναι ότι μπορεί έτσι να χρησιμοποιηθεί τι συντομότερο μονοπάτι μεταξύ των δύο. Τα πακέτα δεν χρειάζεται πλέον να περνούν από τον κεντρικό πάροχο. Αυτό μειώνει το φορτίο στο δίκτυο. Πράγμα πολύ σημαντικό, όταν μιλάμε για μεγάλους αριθμούς κινητών κόμβων που χρησιμοποιούν για παράδειγμα VoIP.

• **Ποιότητα Υπηρεσίας**: Το υπάρχον IP πρωτόκολλο διαχειρίζεται όλα τα

πακέτα με τον ίδιο τρόπο. Το πρώτο που έρχεται-πρώτο δρομολογείται. Τα QoS πρωτόκολλα έχουν την εργασία να παρέχουν διαφορετικές προτεραιότητες στα πακέτα όπως το εύρος ζώνης ή χρόνοι καθυστέρησης. Αυτή την στιγμή υπάρχουν δύο αρχιτεκτονικές. Η Integrated Services (IntServ) και οι Differential Services (Differv). Χρησιμοποιούνται για να κάνουν την δρομολόγηση σύμφωνα με συγκεκριμένα κριτήρια όπως για παράδειγμα αν υπάρχουν αρκετοί πόροι για να δρομολογηθούν τα δεδομένα. Επίσης μπορούν να ελέγξουν το κόστος εξαρτώμενα από διαφορετικά επίπεδα παροχής υπηρεσιών.

• **Αποδοτικότητα:** Μετά από δύο δεκαετίες εμπειρία χρήσης του IPv4 έχει αποκομιστεί αρκετή εμπειρία στο ποια χαρακτηριστικά είναι χρήσιμα και ποια όχι στο IPv4 και ποια λειτουργούν ως bottlenecks της ταχύτητας. Στο IPv6 έχουν ενσωματωθεί αυτές οι βελτιώσεις και πράγματι έχει πολύ καλύτερη απόδοση. Παρ' όλο που τώρα τα πεδία διευθύνσεων είναι 4 φορές μεγαλύτερα σε σχέση με το IPv4, η συνολική επικεφαλίδα είναι μόνο 40 bytes εν συγκρίσει με τα 20 bytes μιας τυπικής επικεφαλίδας IPv4.

Οι βελτιώσεις που υπάρχουν είναι οι εξής:

1) Η επικεφαλίδα του IPv6 έχει σταθερό μήκος
2) Η επικεφαλίδα του IPv6 είναι βελτιστοποιημένη για επεξεργασία 64 bit τη φορά σε σχέση με τα 32 bit του IPv4.
3) Το checksum της επικεφαλίδας IPv4 που υπολογίζεται κάθε φορά που 1 πακέτο περνά από 1 δρομολογητή, αφαιρέθηκε από το IPv6.
4) Οι δρομολογητές δεν είναι υποχρεωμένοι να χωρίζουν 1 μεγάλο πακέτο σε μικρότερα κομμάτια και μπορούν απλά να στείλουν σήμα να τους έρχονται μικρότερα πακέτα.
5) Το broadcast που χρησιμοποιούνταν ευρέως στο IPv4 αντικαταστάθηκε με τα multicast στο IPv6 με τα οποία δεν διακόπτονται όλες οι δικτυακές συσκευές για

να επεξεργαστούν το μήνυμα που έρχεται αλλά μόνο όσες «ακούνε» εκείνη τη στιγμή.

- Το κόστος της μετάβασης θα είναι υψηλό: Στις περιπτώσεις που το υλικό δεν είναι συμβατό, ή δεν μπορεί να αναβαθμιστεί ώστε να είναι συμβατό με IPv6, πράγματι η μετάβαση θα είναι ακριβή. Το μεγάλο πρόβλημα όμως παραμένει στους ISP(Internet Service Providers) και στις μεγάλες επιχειρήσεις που έχουν μεγάλους και ακριβούς δρομολογητές. Όμως οι «δρομολογητές αιχμής» έχουν σχετικά μικρή «οικονομική ζωή», και σε λίγα χρόνια το κόστος δε θα αποτελεί πρόβλημα εκτός και αν συνεχιστεί η αγορά υλικού συμβατού μόνο με IPv4. Για τις μικρότερες δικτυακές συσκευές που δεν μπορούν να αναβαθμιστούν, είτε είναι πολύ φθηνή η αγορά καινούριων είτε μπορούν να χρησιμοποιηθούν οι μηχανισμοί μετάβασης που συζητιούνται αργότερα. Το μόνο κόστος που απομένει είναι αυτό της εκπαίδευσης προσωπικού.

2.6 Το Πρωτόκολλο διασφάλισης του απορρήτου των επικοινωνιών IPSec

Η IPSec είναι ένα πρωτόκολλο ανοικτών προδιαγραφών για τη διασφάλιση του απορρήτου των επικοινωνιών. Είναι βασισμένο στις προδιαγραφές που ανέπτυξε η ομάδα εργασίας του Internet (IETF). Η IPSec διασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και την αυθεντικότητα των επικοινωνιών δεδομένων σε ένα IP δίκτυο. Η IPSec παρέχει τον απαραίτητο μηχανισμό για την ανάπτυξη ευκίνητων λύσεων ασφάλειας σε ένα δίκτυο. Έλεγχοι κρυπτογράφησης και πιστοποίησης ταυτότητας μπορούν να εφαρμοσθούν σε διάφορα επίπεδα στην δικτυακή υποδομή.

Πριν την άφιξη της IPSec στο προσκήνιο, εφαρμόζονταν αποσπασματικές λύσεις που αντιμετώπιζαν μέρος μόνο του προβλήματος. Για παράδειγμα, το

SSL(Secure Sockets Layer) παρέχει κρυπτογράφηση σε επίπεδο εφαρμογής για Web browsers και άλλες εφαρμογές. Το SSL προστατεύει την πιστότητα των δεδομένων που στέλνονται από κάθε εφαρμογή που το χρησιμοποιεί, αλλά δεν προστατεύει τα δεδομένα που αποστέλλονται από άλλες εφαρμογές. Κάθε σύστημα και εφαρμογή πρέπει να είναι προστατεμένη από το SSL για να του παρέχει το τελευταίο την προστασία.

Η IPSec υλοποιεί κρυπτογράφηση και πιστοποίηση επιπέδου δικτύου, παρέχοντας μια λύση ασφαλείας μέσα στην ίδια την αρχιτεκτονική του δικτύου. Έτσι τα συστήματα και οι εφαρμογές που βρίσκονται στις άκρες δεν χρειάζονται αλλαγές ή ρυθμίσεις για να έχουν το πλεονέκτημα της ισχυρής ασφάλειας. Επειδή τα κρυπτογραφημένα πακέτα μοιάζουν με κανονικά IP πακέτα μπορούν εύκολα να δρομολογηθούν μέσα από οποιοδήποτε IP δίκτυο, όπως το Internet, χωρίς καμία αλλαγή στον ενδιάμεσο δικτυακό εξοπλισμό. Οι μόνες συσκευές οι οποίες γνωρίζουν για την κρυπτογράφηση είναι αυτές στα ακραία σημεία. Αυτό το χαρακτηριστικό μειώνει δραστικά τόσο το κόστος της υλοποίησης όσο και το κόστος της διαχείρισης.

Η IPSec συνδυάζει τις παραπάνω τεχνολογίες ασφάλειας σε ένα ολοκληρωμένο σύστημα το οποίο παρέχει εμπιστευτικότητα, ακεραιότητα και πιστοποίηση της ταυτότητας των IP πακέτων. Η IPSec αναφέρεται και σε μια σειρά άλλων πρωτοκόλλων όπως ορίζεται στα RFC 1825-1829 και σε άλλες δημοσιεύσεις στο Internet.

Αυτές οι προδιαγραφές περιλαμβάνουν:

- **Κατάλληλο IP πρωτόκολλο ασφαλείας**. Ρόλος του είναι να καθορίζει την πληροφορία που πρέπει να προστεθεί σε ένα IP πακέτο για να ενεργοποιηθούν οι έλεγχοι πιστότητας, ακεραιότητας και πιστοποίησης ταυτότητας, όπως επίσης

καθορίζει και το πως πρέπει να γίνει η κρυπτογράφηση των δεδομένων του πακέτου.

• Δ**ιαχείριση κλειδιών**. Οι περισσότεροι από τους μηχανισμούς ασφαλείας που παρέχονται από την IPsec απαιτούν την χρήση κλειδιών κρυπτογράφησης. Ένα ξεχωριστό τμήμα τέτοιων μηχανισμών έχει δημιουργηθεί για διαχειρίζεται τα κλειδιά αυτά. Ο μηχανισμός αυτός ονομάζεται Internet Key Exchange (IKE). Δεν είναι απαραίτητο να χρησιμοποιηθεί το IKE, αλλά το να ρυθμιστούν χειροκίνητα οι συσχετισμοί ασφάλειας είναι μια δύσκολη και επίπονη διαδικασία. Το IKE πρέπει να χρησιμοποιείται στις περισσότερες εφαρμογές για να ενεργοποιεί ασφαλείς επικοινωνίες μεγάλης κλίμακας. Δημιουργεί ένα πιστοποιημένο και ασφαλές κανάλι μεταξύ δύο κόμβων και κατόπιν διαπραγματεύεται τους συσχετισμούς ασφάλειας για την IPSec. Αυτή η διαδικασία απαιτεί από τους δύο κόμβους να πιστοποιήσουν ο ένας τον άλλον και να μοιράσουν κλειδιά.

• **Πακέτα IPSec**. Η IPSec ορίζει ένα νέο σετ επικεφαλίδων το οποίο προστίθεται στα IP πακέτα. Αυτές οι νέες επικεφαλίδες τοποθετούνται μετά την επικεφαλίδα IP και πριν το πρωτόκολλο επιπέδου 4 (τυπικά το TCP ή το UDP).

Αυτές οι νέες επικεφαλίδες παρέχουν πληροφορίες για την ασφάλεια του φορτίου των IP πακέτων όπως αναλύεται παρακάτω:

• Η επικεφαλίδα πιστοποίησης ταυτότητας (AH - Authentication Header) διασφαλίζει την ακεραιότητα και την ταυτότητα των δεδομένων που διακινούνται. Δεν παρέχει ασφάλεια πιστότητας. Η επικεφαλίδα αυτή τοποθετείται μεταξύ της IPv6 επικεφαλίδας και επικεφαλίδων υψηλότερου στρώματος (π.χ. TCP, UDP).

• Φορτίο ασφαλείας ενθυλάκωσης (ESP-Encapsulating Security Payload). Προστατεύει την ακεραιότητα και την ταυτότητα των δεδομένων. Τοποθετείται μπροστά από την μετάδοση (π.χ. UDP, TCP), τον έλεγχο του δικτύου

(π.χ. ICMP) ή την επικεφαλίδα του πρωτοκόλλου δρομολόγησης.

Η IPSec παρέχει δυο καταστάσεις λειτουργίας, την transport και την tunnel:

• Στην κατάσταση transport, οι συσχετισμοί ασφάλειας γίνονται μεταξύ των δύο κόμβων που επικοινωνούν. Μόνο το IP φορτίο κρυπτογραφείται, ενώ οι αρχικές επικεφαλίδες μένουν ανέπαφες. Αυτή η κατάσταση λειτουργίας έχει το πλεονέκτημα της πρόσθεσης μόνο μερικών Bytes σε κάθε πακέτο. Επιπλέον, επιτρέπουν σε συσκευές στο δημόσιο δίκτυο να βλέπουν την τελική πηγή και τον προορισμό του πακέτου. Επιτρέπει ειδική επεξεργασία (για παράδειγμα QoS) στο ενδιάμεσο δίκτυο, βασισμένη στην πληροφορία που βρίσκεται στην IP επικεφαλίδα. Ωστόσο, η επικεφαλίδα θα κρυπτογραφηθεί περιορίζοντας τη δυνατότητα έρευνας των πακέτων.

• Στην κατάσταση λειτουργίας tunnel, οι συσχετισμοί ασφαλείας γίνονται μεταξύ δύο ασφαλών πυλών. Όλο το πακέτο κρυπτογραφείται, συμπεριλαμβανομένης και της βασικής επικεφαλίδας και γίνεται το φορτίο ενός καινούριου IP πακέτου το οποίο έχει κρυπτογραφηθεί και έχει προστεθεί σε αυτό μια καινούρια επικεφαλίδα. Αυτή είναι η αρχή λειτουργίας για ένα ιδιωτικό εικονικό δίκτυο (VPN). Αυτή η κατάσταση λειτουργίας επιτρέπει σε μια δικτυακή συσκευή, όπως ένας δρομολογητής, να ενεργήσει σαν ένας IPSec proxy. Αυτό σημαίνει ότι ο δρομολογητής πραγματοποιεί κρυπτογράφηση για λογαριασμό των υπολογιστών του δικτύου. Η πηγή του δρομολογητή κρυπτογραφεί τα πακέτα και τα προωθεί στο IPSec tunnel. Ο προορισμός του δρομολογητή αποκρυπτογραφεί το αρχικό IP διάγραμμα και το προωθεί στο σύστημα προορισμού του. Το βασικό πλεονέκτημα αυτής της κατάστασης λειτουργίας είναι ότι τα ακραία συστήματα δεν χρειάζεται να ρυθμιστούν για να επικαρπωθούν τα πλεονεκτήματα της IPSec. Η κατάσταση λειτουργίας tunnel προστατεύει επιπλέον το σύστημα από την διαδικασία της ανάλυσης κίνησης. Σε αυτή την κατάσταση λειτουργίας ο

επιτιθέμενος μπορεί να καθορίσει μόνο τα ακραία σημεία του tunnel και όχι την πραγματική πηγή και τον προορισμό των πακέτων που κυκλοφορούν μέσα σε αυτό, ακόμη και αν είναι τα ίδια με τα ακραία σημεία του tunnel.

Η κατάσταση λειτουργίας transport, μπορεί να χρησιμοποιηθεί μόνο όταν τόσο η πηγή, όσο και τα συστήματα προορισμού είναι συμβατά με την IPSec. Στις περισσότερες περιπτώσεις έχουμε όμως, έχουμε εφαρμογή της IPSec σε κατάσταση λειτουργίας tunnel. Έχουμε έτσι τη δυνατότητα να υλοποιήσουμε την IPSec στη δικτυακή υποδομή χωρίς να τροποποιήσουμε το λειτουργικό σύστημα ή οποιαδήποτε εφαρμογή στους servers και τους υπολογιστές του δικτύου.

2.7 Η χρησιμότητα του πρωτοκόλλου ασφαλείας IPSec

Το Internet αποτελεί αντικείμενο πολλών και διαφορετικών τύπων επιθέσεων συμπεριλαμβανομένων αυτών της απώλειας του απόρρητου, της ακεραιότητας των δεδομένων, της πλαστοπροσωπίας και της άρνησης παροχής υπηρεσιών. Ο στόχος της IPSec είναι η αντιμετώπιση όλων αυτών των προβλημάτων μέσα στην ίδια την υποδομή του δικτύου χωρίς να είναι αναγκαία η εγκατάσταση και η ρύθμιση ακριβών μηχανών και λογισμικού.

Η IPSec παρέχει κρυπτογράφηση στο επίπεδο του IP και για αυτό το λόγο αποτελεί ένα αξιοσημείωτο κομμάτι της συνολικής ασφάλειας. Οι προδιαγραφές της IPSec ορίζουν δύο νέους τύπους δεδομένων στα πακέτα: την επικεφαλίδα πιστοποίησης (AH-Authentication Header), για την παροχή υπηρεσίας ακεραιότητας δεδομένων και το φορτίο ενθυλάκωσης ασφάλειας (ESP-Encapsulating Security Payload) το οποίο παρέχει πιστοποίηση ταυτότητας και ακεραιότητα δεδομένων. Ορίζονται επίσης οι παράμετροι επικοινωνίας μεταξύ δύο συσκευών που είναι η διαχείριση των κλειδιών και η συσχετισμοί ασφάλειας (security associations).

Τα θέματα ασφαλείας που έχει να αντιμετωπίσει η IPsec περιγράφονται παρακάτω:

• Απώλεια του Απορρήτου (Loss of Privacy): Κάποιος που έχει καταφέρει να εισχωρήσει σε κάποιο δίκτυο έχει τη δυνατότητα να παρακολουθεί εμπιστευτικά δεδομένα κατά τη διακίνηση των τελευταίων στο Internet. Αυτή η δυνατότητα είναι ίσως ο μεγαλύτερος ανασταλτικός παράγοντας στις επικοινωνίες μεταξύ των επιχειρήσεων σήμερα. Χωρίς τη χρήση κρυπτογραφικών μεθόδων για κάθε πακέτο πληροφορίας υπάρχει η δυνατότητα ανάγνωσής του για όποιον έχει τα μέσα να το αιχμαλωτίσει. Το CERT (Computer Emergency Response Team Coordination Center) αναφέρεται στα προγράμματα «packet sniffers» ως την πιο συνηθισμένη περίπτωση επίθεσης από αυτές που συναντώνται.

• Απώλεια της Ακεραιότητας των Δεδομένων (Loss of Data Integrity): Ακόμα και για δεδομένα που δεν είναι εμπιστευτικά, πρέπει να λαμβάνονται μέτρα διασφάλισης της ακεραιότητάς τους. Μπορεί να μην μας ενδιαφέρει εάν κάποιος «δει» τη κίνηση ρουτίνας της δουλείας μας, αλλά σίγουρα θα μας προβλημάτιζε εάν αυτός αλλοίωνε κατά οποιοδήποτε τρόπο τα δεδομένα αυτά. Για παράδειγμα το να μπορεί κάποιος να πιστοποιεί με ασφάλεια τον εαυτό του στη τράπεζα κάνοντας χρήση ψηφιακών πιστοποιητικών δεν είναι αρκετό εάν η κύρια εργασία του στη τράπεζα θα μπορούσε να αλλοιωθεί με κάποιο τρόπο.

• Πλαστοπροσωπία (Identity Spoofing) : Εκτός της προστασίας των ίδιων των δεδομένων, θα πρέπει να παίρνουμε μέτρα ώστε να προστατεύεται και η ταυτότητά μας στο Internet. Ένας εισβολέας μπορεί να αποδειχθεί ικανός να κλέψει τη ταυτότητα κάποιου και έτσι να αποκτήσει πρόσβαση σε εμπιστευτικές πληροφορίες . Πολλά συστήματα ασφάλειας σήμερα, βασίζονται στην IP διεύθυνση για να αναγνωρίσουν μοναδικά τους χρήστες. Τα συστήματα αυτά είναι πολύ εύκολο να ξεγελαστούν και αυτό το γεγονός έχει οδηγήσει σε αναρίθμητες

επιθέσεις διαφόρων συστημάτων.

• Άρνηση Παροχής Υπηρεσιών (Denial-of-Service): Εφόσον κάποιος οργανισμός εκμεταλλεύεται το Internet, πρέπει να λάβει κάποια μέτρα ώστε να διασφαλίσει τη διαθεσιμότητα του συστήματός του σε αυτό. Τα τελευταία χρόνια διάφοροι hackers, έχουν βρει αδυναμίες στο πρωτόκολλο TCP/IP, που τους δίνει τη δυνατότητα να «ρίχνουν» τις μηχανές.

2.8 Το Mobile IPv6 και η λειτουργία του

Με το IPv4 αλλά και το IPv6, η μάσκα δικτύου αλλάζει κάθε φορά που αλλάζει το σημείο πρόσβασης στο δίκτυο. Όταν ένας κινητός κόμβος αλλάζει το σημείο πρόσβασής του, τότε αλλάζει και η IP διεύθυνσή του, πράγμα που διακόπτει τις TCP και UDP συνδέσεις του. Η χρήση του Mobile IP με το IPv4 έχει σοβαρούς περιορισμούς που το κάνουν ακατάλληλο για ένα παγκόσμιο δίκτυο. Ένας λόγος είναι ο περιορισμένος αριθμός διευθύνσεων. Αν φανταστούμε κάθε έξυπνο τηλέφωνο να έχει και από μία IP διεύθυνση τότε θα τελείωναν και οι τελευταίες διαθέσιμες διευθύνσεις άμεσα. Ο άλλος λόγος είναι ότι η IPv6 που διαθέτει επικεφαλίδες επέκτασης προσφέρει την δυνατότητα να τροποποιηθεί η δρομολόγηση σε ένα κόσμο με κινητά δίκτυα και αυτό είναι απαραίτητο αν θέλουμε να μιλάμε για δυνατότητα σύνδεσης σε τεράστιες μάζες συσκευών. Το γεγονός ότι το IPv6 χρησιμοποιεί το Neighbor Discovery κάνει το IPv6 πιο ανεξάρτητο στο στρώμα της δικτύωσης. Η Mobile IPv6 παίρνει την εμπειρία του IPv4 και τις ανώτερες δυνατότητες που προσφέρει το IPv6.

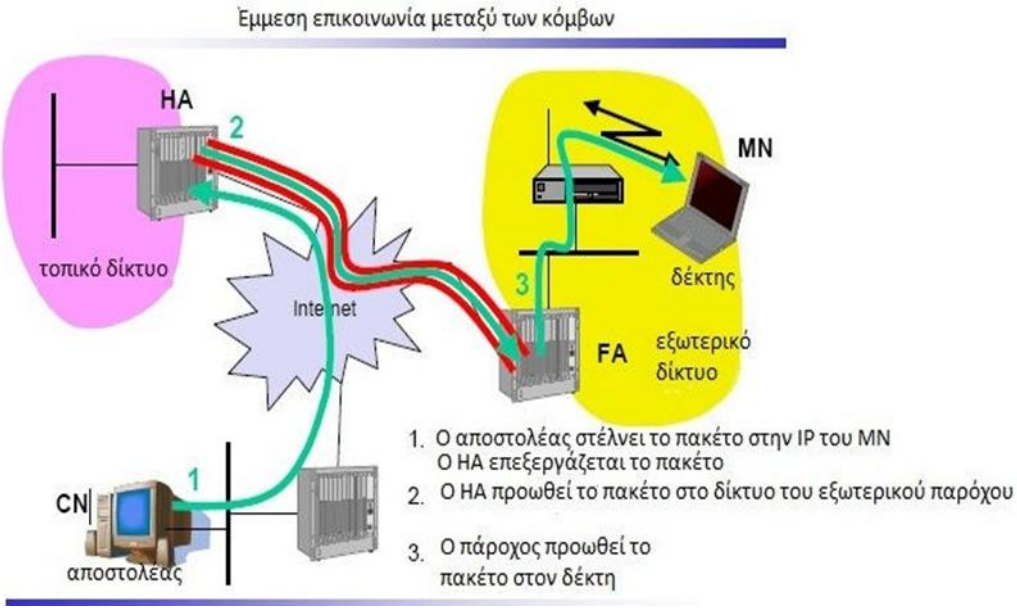
Η κεντρική διεύθυνση είναι η IPv6 διεύθυνση με το πρόθεμα της κεντρικής σύνδεσης ενός κινητού κόμβου (MN). Όσο ο κινητός κόμβος βρίσκεται σπίτι, δέχεται πακέτα μέσω των κανονικών IP μηχανισμών και συμπεριφέρεται σαν ένας

κλασσικός κόμβος. Όταν ο κόμβος είναι έξω από το σπίτι και συνδεμένος σε ένα ξένο δίκτυο, έχει την ανάλογη διεύθυνση. Δέχεται την διεύθυνση αυτή από τους IPv6 μηχανισμούς, όπως ο DHCPv6.

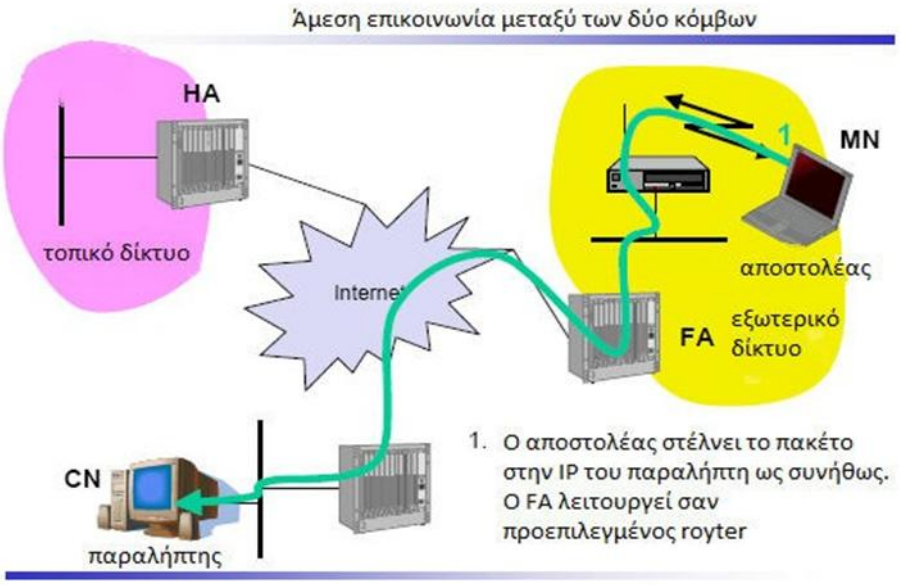
Ο συσχετισμός μιας κεντρικής διεύθυνσης (Home address - HA) και μιας εξωτερικής διεύθυνσης ονομάζεται binding. Μακριά από το σπίτι, ο κινητός κόμβος καταγράφει την εξωτερική του διεύθυνση στον router του κεντρικού του δικτύου. Για την καταγραφή της διεύθυνσης ο κόμβος στέλνει ένα μήνυμα στο κεντρικό router και στην συνέχεια αυτός απαντάει ότι πλέον γνωρίζει την νέα εξωτερική διεύθυνση. Κάθε κόμβος που επικοινωνεί με έναν κινητό κόμβο ονομάζεται κόμβος αλληλογραφίας (Correspondent Node-CN). Οι κινητοί κόμβοι μπορούν να κάνουν καταγραφή της εξωτερικής τους διεύθυνσης κατευθείαν στον κόμβο αλληλογραφίας. Ένας τέτοιος κόμβος δεν αποκλείεται να είναι και αυτός κινητός.

Υπάρχουν δύο τρόποι επικοινωνίας μεταξύ ενός κινητού και ενός κόμβου αλληλογραφίας:

- Έμμεση επικοινωνία: Τα πακέτα από τον κόμβο αλληλογραφίας στέλνονται στον κεντρικό πάροχο, αυτός τα μετατρέπει σε IPv6 και τα στέλνει στον κινητό κόμβο. Η αντίθετη διαδικασία γίνεται για να σταλούν πακέτα από τον κινητό κόμβο στον κόμβο αλληλογραφίας. Αυτή η διαδικασία δεν προϋποθέτει την χρήση του Mobile IPv6.



• Άμεση επικοινωνία: Η επικοινωνία μεταξύ των δύο κόμβων μπορεί να είναι άμεση χωρίς να γίνεται μέσω του κεντρικού παρόχου. Αυτό είναι και το βασικό πλεονέκτημα της Mobile IPv6 έναντι της Mobile IPv4. Η επιτυχία της σύνδεσης στηρίζεται στην καταχώρηση της εξωτερικής διεύθυνσης του κινητού κόμβου στον κόμβο αλληλογραφίας και η απάντηση από τον δεύτερο ότι τον έχει καταγράψει. Πλεονέκτημα αυτής της επικοινωνίας είναι ότι μπορεί να χρησιμοποιηθεί το συντομότερο μονοπάτι μεταξύ των δύο κόμβων. Σε περίπτωση αλλαγής της διεύθυνσης του κεντρικού παρόχου, ο κινητός κόμβος μπορεί να ενημερωθεί γι' αυτό με την χρήση της Dynamic Home Agent Prefix Discovery.



2.9 Πλεονεκτήματα του Mobile IPv6

Η υποστήριξη κινητικότητας για τις συσκευές του διαδικτύου είναι δυνατή και προτυποποιημένη και για τις δύο εκδόσεις του πρωτοκόλλου IP, IPv4 και IPv6, αλλά λόγω της διευρυμένης λειτουργικότητας και του μεταγενέστερου σχεδιασμού του IPv6 μερικά χαρακτηριστικά, τα οποία αφορούν την υποστήριξη κινητικότητας έχουν ενσωματωθεί πιο αποτελεσματικά στο Mobile IPv6 σε σχέση με το Mobile IPv4. Ακολουθούν επιγραμματικά τα κύρια πλεονεκτήματα του Mobile IPv6 :

- Το Mobile IP πρέπει να αναθέτει global IP διευθύνσεις σε έναν φορητό κόμβο σε κάθε σημείο στο οποίο ατός συνδέεται με το διαδίκτυο. Σε ζεύξεις οι οποίες εξυπηρετούν φορητούς κόμβους πρέπει να δεσμευθεί ένα σύνολο IP διευθύνσεων (τουλάχιστο μία), οι οποίες θα ανατεθούν ως care-of διευθύνσεις των φορητών κόμβων. Λόγω της έλλειψης IP διευθύνσεων στο πρωτόκολλο IPv4 μπορεί να υπάρξουν προβλήματα ανικανότητας δέσμευσης αρκετών global IPv4 διευθύνσεων σε ορισμένες ζεύξεις. Στο πρωτόκολλο IPv6 υπάρχουν αρκετές

διαθέσιμες διευθύνσεις.

- Το IPv6 χρησιμοποιώντας διευθύνσεις τύπου anycast επιτρέπει σε έναν κόμβο να στέλνει ένα πακέτο σε κάποιο από τα πολλά συστήματα τα οποία έχουν ανατεθειμένη αυτήν την anycast διεύθυνση σε κάποιο από τα interface τους. Το Mobile IPv6 κάνει αποτελεσματική χρήση αυτού του μηχανισμού, στο μηχανισμό Δυναμικής Ανακάλυψης home agent στέλνοντας ένα Binding Update στην anycast διεύθυνση των home agents και λαμβάνοντας απάντηση από ακριβώς έναν από τους πολλούς home agents. Το IPv4 δεν παρέχει μια τέτοια δυνατότητα.

- Χρησιμοποιώντας μηχανισμούς όπως το stateless address autoconfiguration και το Neighbor Discovery για τη ρύθμιση των παραμέτρων του, το Mobile IPv6 δεν χρειάζεται ούτε το πρωτόκολλο DHCP ούτε foreign agents στις απομακρυσμένες ζεύξεις ώστε να ρυθμιστούν οι care-of διευθύνσεις των φορητών κόμβων του.

- Το Mobile IPv6 μπορεί να χρησιμοποιήσει το IPsec για όλες τις απαιτήσεις ασφάλειας όπως η πιστοποίηση αυθεντικότητας και η προστασία ακεραιότητας δεδομένων.

- Για να αποφύγει τη σπατάλη εύρους ζώνης, λόγω της δρομολόγησης τριγώνου, το Mobile IP καθορίζει μηχανισμούς βελτιστοποίησης διαδρομής (route optimization). Ενώ η βελτιστοποίηση διαδρομής αποτελεί μία επιπρόσθετη λειτουργικότητα για το Mobile IPv4, αποτελεί ένα ενσωματωμένο χαρακτηριστικό στο Mobile IPv6.

Υπάρχουν πολλοί δρομολογητές στο Διαδίκτυο οι οποίοι εκτελούν το λεγόμενο ingress-filtering για τα πακέτα τα οποία πρόκειται να προωθηθούν από αυτούς. Αυτό σημαίνει ότι ελέγχουν αν η διεύθυνση πηγής ενός πακέτου είναι προσβάσιμη

από το interface από το οποίο ελήφθη το πακέτο. Το Mobile IPv6 μπορεί να συνυπάρχει με το ingress-filtering χωρίς προβλήματα. Ένας σε μία απομακρυσμένη ζεύξη χρησιμοποιεί την care-of διεύθυνσή του σαν διεύθυνση πηγής των πακέτων του και συμπεριλαμβάνει την home διεύθυνσή του στην επιλογή Home Address. Επειδή η care-of διεύθυνση αποτελεί μια έγκυρη διεύθυνση στην απομακρυσμένη ζεύξη (foreign link) το πακέτο θα περάσει από το μηχανισμό του ingress-filtering χωρίς κανένα πρόβλημα.

ΔΕΥΤΕΡΟ ΜΕΡΟΣ
ΚΟΙΝΩΝΙΚΟ ΚΑΙ ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

Η βαθμιαία εισαγωγή της νέας τεχνολογίας σε οικονομία και κοινωνία επιφέρει σημαντικές αλλαγές σε κοινωνικό και θεσμικό επίπεδο. Παράλληλα, η μετάβαση στο IoT με τη βοήθεια του IpV6 συνεπάγεται κινδύνους και απειλές που πρέπει να αντιμετωπιστούν επαρκώς από κράτη, ρυθμιστικές και εποπτικές αρχές προστασίας ασφάλειας και ιδιωτικότητας, και τις κοινωνίες συνολικά προς όφελος των πολιτών και των επιχειρήσεων.

ΚΕΦΑΛΑΙΟ 3
Κοινωνικές Επιπτώσεις του Διαδικτύου των Πραγμάτων

Στις επόμενες σελίδες αναλύονται συνοπτικά οι κοινωνικές επιπτώσεις της τεχνολογικής επανάστασης που μεταμορφώνει την παραγωγή, την οικονομία και την κοινωνία κατά την πορεία προς το νέο ψηφιακό οικοσύστημα.

3.1 Κίνδυνοι προσβολής ιδιωτικότητας

Η αυξημένη συνδεσιμότητα στο Διαδίκτυο συχνά συνεπάγεται σημαντικά αυξημένο κίνδυνο για την ασφάλεια, λόγω της ποσότητας των δεδομένων που συλλέγονται από αυτούς τους αισθητήρες και τις δυνατότητες ευρείας κοινής χρήσης αυτών των δεδομένων. Υπάρχουν επίσης ερωτήματα σχετικά με το ποιος συλλέγει, κατέχει και επεξεργάζεται τα δεδομένα που δημιουργούνται, που και πως οι πληροφορίες που δημιουργούνται μεταφέρονται και αποθηκεύονται, και ποιό επίπεδο ασφάλειας είναι απαραίτητο για την προστασία της ιδιωτικής ζωής.

Ας δούμε ένα πρώιμο παράδειγμα για τα εγγενή προβλήματα με την συνδεδεμένη τεχνολογία: το Υπουργείο Εξωτερικών των ΗΠΑ για πρώτη φορά άρχισε να εκδίδει διαβατήρια με βιομετρικά στοιχεία τον Αύγουστο του 2007. Τα έγγραφα αυτά περιείχαν ένα τσιπ RFID που – όπως αποκαλύφθηκε – θα μπορούσε να διαβαστεί από απόσταση 10 μέτρων από συσκευές που θα μπορούσαν να αγοραστούν σε δικτυακούς τόπους τύπου eBay. Λίγο αργότερα το πρόβλημα αναγνωρίστηκε και τα διαβατήρια επαναδιαμορφώθηκαν για να ενσωματώσουν ένα πλέγμα αλουμινίου στα καλύμματα τους, ώστε να εμποδίσουν τέτοια ανάγνωση. Ακόμη και με αυτό το επίπεδο προστασίας ωστόσο, το chip RFID εξακολουθούσε να είναι αναγνώσιμο όταν το κάλυμμα ήταν ανοικτό για επιθεώρηση.

Ευπάθειες όπως αυτή είναι μόνο η κορυφή του παγόβουνου. Είμαστε ακόμα στην αρχή της επανάστασης του Internet of Things, αφού σχετικά λίγες μεμονωμένες συσκευές μπορούν να έχουν αισθητήρες. Η αύξηση του κινδύνου θα σημειωθεί όταν τα ίδια τα αντικείμενα θα μπορούν να αρχίζουν να αναλαμβάνουν δράση με βάση τις επιθυμίες του χρήστη. Για παράδειγμα, είναι πλέον εύκολο να ρυθμίσουμε τη θερμοκρασία του εσωτερικού χώρου του σπιτιού μας χρησιμοποιώντας το smartphone, το tablet ή τον υπολογιστή. Στο μέλλον, ένα σύστημα οικιακού αυτοματισμού θα είναι σε θέση να ρυθμίσει τη θερμοκρασία με βάση την εγγύτητα του ιδιοκτήτη. Όταν το σπίτι είναι ακατοίκητο το καλοκαίρι, η θερμοκρασία μπορεί να επιτραπεί να αυξηθεί, λόγω μη λειτουργίας του συστήματος ψύξης, με στόχο την εξοικονόμηση ενέργειας. Όταν ο ιδιοκτήτης του σπιτιού θα ανιχνεύεται ότι φεύγει από την εργασία, το σύστημα κλιματισμού θα ενεργοποιείται αυτόματα, έτσι ώστε το σπίτι να ψύχεται στην επιθυμητή θερμοκρασία. Τι θα συμβεί όμως αν ένας κακόβουλος εισβολέας ή ένας μεμονωμένος χάκερ θα προσπαθήσει να πάρει τον έλεγχο της θερμοκρασίας του σπιτιού, καθιστώντας αδύνατη την ψύξη το καλοκαίρι και ζέστη το χειμώνα; Και τι θα συμβεί αν η επίθεση είναι γενικευμένη και επηρεάσει μια ολόκληρη περιοχή;

Όταν τα ψυγεία γίνουν συνδεδεμένα, τα δεδομένα που συλλέγονται για συγκεκριμένες αγορές τροφίμων θα μπορούσαν να οδηγήσουν σε συμπεράσματα σχετικά με τις αγοραστικές συνήθειες, τις προτιμήσεις, το διαιτολόγιο, την εθνοτική ή θρησκευτική κατάσταση ενός ατόμου, ακόμα και αν υπάρχουν προβλήματα υγείας. Αν και τα δεδομένα θερμοκρασίας που αποκτήθηκαν από το ψυγείο είναι πιθανό να είναι αβλαβή, οι πληροφορίες που συλλέγονται από ιατρικούς αισθητήρες και διανέμονται, εκτός των γιατρών η των νοσοκομείων, σε μη εξουσιοδοτημένους τρίτους (φαρμακευτικές και ασφαλιστικές εταιρίες, κατασκευαστές ιατρικού εξοπλισμού κλπ) θα μπορούσαν να δημιουργήσουν «προφίλ» των χρηστών, ειδικά αν συνδυάζονται με άλλες πληροφορίες και προσωπικά δεδομένα από συναφείς πηγές (πληρωμές, αγορές, μετακινήσεις, καταναλωτικές συνήθειες κ.ο.κ).

Παραδείγματος χάριν, η σχετική εφαρμογή θα μας ειδοποιήσει για αυξημένες αγορές παγωτού που συνδέονται με μια αύξηση του σακχάρου στο αίμα μας, και οι εμφυτευμένοι ιατρικοί αισθητήρες θα ανιχνεύσουν την αύξηση του σωματικού βάρους. Από τη μία πλευρά, εμείς (και ο γιατρός μας) θα μπορούμε να προειδοποιηθούμε ότι πρέπει να ρυθμίσουμε τη διατροφή μας, προκειμένου να παραμείνουμε υγιείς. Από την άλλη πλευρά όμως, η ασφαλιστική εταιρεία μας μπορεί επίσης να να ενημερωθεί και να αυξήσει το ασφάλιστρο, λόγω του αυξημένου κινδύνου για την υγεία μας. Είναι επίσης πιθανό ότι το ψυγείο μας ή άλλες συνδεδεμένες στο Διαδίκτυο συσκευές να ενσωματώνουν ήδη αισθητήρες που δεν είναι ενεργοί, όπως ένα μικρόφωνο ή μία κάμερα. Τι θα συμβεί αν ένας χάκερ θα μπορούσε να επιτρέψει την ενεργοποίηση τους εξ αποστάσεως για να διαπιστώσει αν είμαστε στο σπίτι ή ακόμα και να ακούσει τις συνομιλίες μας;

Σχετικά ελαττώματα ασφαλείας για κάθε είδους συνδεδεμένες συσκευές έχουν ανακαλυφθεί πολλές φορές. Κάνοντας χρήση των υποδομών της Google είναι δυνατό να εντοπίσετε πολλές ακάλυπτες κάμερες σε όλο τον κόσμο. Επίσης έχουν

σχεδιαστεί μηχανές αναζήτησης για να βλέπουν ειδικά όλων των τύπων τις συνδεδεμένες συσκευές. Η δυνατότητα για τους χάκερ να είναι σε θέση να αποκτήσουν πρόσβαση σε έξυπνες συσκευές είναι πραγματική, και όχι απλώς θεωρητική απειλή, και αυτό δεν έχει σχέση μόνο με την ασφάλεια των συστημάτων, αλλά και με την άγνοια των χρηστών. Καθώς όλο και περισσότερες από αυτές τις συσκευές συνδέονται στο Internet, το πρόβλημα μπορεί να χειροτερέψει αν δεν εφαρμοσθούν τα κατάλληλα μέτρα ασφαλείας. Παραδείγματος χάριν, αν κάποιος αποκτούσε πρόσβαση στην οπτική ροή δεδομένων των γυαλιών του Google Glass θα μπορούσε να παρακολουθεί όλες τις δραστηριότητες του χρήστη. Ένα επιπλέον παράδειγμα θα μπορούσε να είναι η πρόσβαση σε ευαίσθητα προσωπικά δεδομένα που αποθηκεύονται στον αυτόματο διανομέα για το φάρμακο του ασθενούς, που σε κανονικές συνθήκες έχει σχεδιαστεί να απελευθερώνει το φάρμακο ανάλογα με έναν αισθητήρα σώματος που ανιχνεύει μια συγκεκριμένη κατάσταση.

Στην ίδια κατεύθυνση, οποιαδήποτε συσκευή με ασύρματη σύνδεση θα μπορούσε να είναι ευάλωτη στην πειρατεία. Το hacking στο ψυγείο μας θα μπορούσε να παραβιάζει την ιδιωτική ζωή μας, έχοντας τη δυνατότητα να εκμεταλλεύεται μια αδυναμία ασφάλειας σε μια συνδεδεμένη στο ίδιο δίκτυο κλειδαριά πόρτας, κάτι που θα μπορούσε να σημαίνει ότι χιλιάδες σπίτια θα γίνουν ευάλωτα σε διάρρηξη. Ακόμη και χωρίς απόλυτη πρόσβαση, απλά αναλύοντας εξ αποστάσεως δεδομένα κίνησης δικτύου, μπορεί κανείς να λάβει εν αγνοία μας και χωρίς να αντιληφθούμε τίποτα χρήσιμες πληροφορίες σχετικά με το αν το σπίτι μας είναι άδειο ή όχι.

3.2 Ασφάλεια

Τελευταία γίνεται συνεχής αναφορά σχετικά με την απίστευτα χαλαρή προστασία

της ιδιωτικής ζωής που χρησιμοποιείται στις περισσότερες (IoT) συσκευές, και πόσο ευάλωτες είναι στο να παραβιαστούν. Οι χρήστες επιτρέπουν όλο και περισσότερο σε δεδομένα που αφορούν την υγεία τους, το εμπόριο, κλπ να αποθηκεύονται σε συσκευές και το ενδεχόμενο των δεδομένων να παραβιαστούν και να υποστούν κατάχρηση είναι πάντα επίκαιρο. Μια στενά συνδεδεμένη, αλλά σαφής, ανησυχία σχετικά με τα δεδομένα που αφορούν τους εαυτούς μας σε αυτές τις συσκευές, είναι η ικανότητα των συσκευών IoT να συλλέγουν και να μεταδίδουν πληροφορίες σχετικά με εμάς κρυφά. Σχεδόν ο καθένας στη δυτική κοινωνία είναι ήδη σε γενικές γραμμές ενήμερος ότι οι CCTV κάμερες ασφαλείας μας παρακολουθούν περισσότερο ή λιγότερο παντού στους δημόσιους και ιδιωτικούς χώρους, στο δρόμο, στις τράπεζες, στα εστιατόρια και στα εμπορικά καταστήματα.

Αυτό που λιγότεροι άνθρωποι συνειδητοποιούν είναι το πόσο διασυνδεμένες είναι ήδη μεταξύ τους πολλές από αυτές τις κάμερες. Η διασύνδεση συσκευών χτίζει μια εκδοχή του «Πανοπτικού», που είναι το άγρυπνο μάτι του Μεγάλου Αδερφού που παρακολουθεί τους πάντες, που απεικονίζεται σε πολλές ταινίες δράσης-περιπέτειας και τηλεοπτικές εκπομπές με δυνατότητα εντοπισμού του οποιοδήποτε, οπουδήποτε, σε πραγματικό χρόνο. Κάθε βίντεο επικοινωνεί και τροφοδοτείται από ένα ενιαίο κέντρο ελέγχου στο όποιο πολλές από αυτές τις κάμερες, στην πραγματικότητα, είναι προσβάσιμες μέσω δικτύων συνδεδεμένων στο ίντερνετ (internet-connected networks). Θα πρέπει να προκαλέσει μικρή έκπληξη ότι τα τρισδιάστατα video δίκτυα που διαχειρίζονται από τους δήμους, τα αεροδρόμια, και άλλες δημόσιες αρχές συχνά δεν έχουν ισχυρή προστασία της ιδιωτικής ζωής. Ως αποτέλεσμα, σχεδόν ο καθένας θα μπορούσε να σας παρακολουθεί μέσα από μία από αυτές τις δημόσιες κάμερες. Ακόμα και οι κάμερες που επιλέγουμε να εγκαταστήσουμε μπορεί να ρυθμιστούν ώστε να μας κατασκοπεύουν όταν δεν θέλουμε να το κάνουν.

Τον Σεπτέμβριο του 2013, στις ΗΠΑ η Ομοσπονδιακή Αρχή Εμπορίου FTC επέβαλε κυρώσεις σχετικά με κατάχρηση πληροφοριών που συλλέγονται από το IOT. Η TRENDnet, μια εταιρεία που εμπορεύεται κάμερες σχεδιασμένες ώστε να επιτρέπουν στους καταναλωτές να παρακολουθούν τα σπίτια τους εξ αποστάσεως εδραίωσε τα FTC τέλη ότι η χαλαρή πρακτική ασφαλείας εκθέτει σε δημόσια προβολή στο διαδίκτυο την ιδιωτική ζωή εκατοντάδων καταναλωτών. Σύμφωνα με την FTC η εταιρία χαρακτήρισε τα αμέτρητα προϊόντα της ως «ασφαλή» όταν στην πραγματικότητα οι κάμερες είχαν ελαττωματικό λογισμικό που τις άφηνε ευάλωτες σε επιθέσεις των επιτήδειων αθέμιτων εισβολέων. Ο ισχυρισμός αυτός κατήγγειλε ακόμη, ότι τον Ιανουάριο του 2012 ένας χάκερ εκμεταλλεύτηκε αυτό το ελάττωμα και το δημοσιοποίησε και τελικά αναρτήθηκαν σύνδεσμοι με υλικό από σχεδόν 700 κάμερες . Το υλικό παρουσίαζε μωρά να κοιμούνται στις κούνιες τους, μικρά παιδιά να παίζουν και ενήλικες να διάγουν την καθημερινή τους ζωή. Μόλις η Trendnet έμαθε για αυτό το κενό ασφάλειας ανέβασε έναν κώδικα λογισμικού στην ιστοσελίδα της και προσπάθησε να ειδοποιήσει τους πελάτες της για την ανάγκη να επισκεφτούν την ιστοσελίδα , ώστε να ενημερώσουν τις κάμερες τους με το τελευταίο λογισμικό που έχει αναρτηθεί.

Η ικανότητα να εντοπίζονται τα άτομα μέσα από διασυνδεμένες συσκευές δεν επιτυγχάνεται μόνο μέσω της βιντεοσκόπησης. Όλο και περισσότεροι άνθρωποι χρησιμοποιούν τις δυνατότητες του IoT , και το εντάσσουν στη καθημερινή τους ζωή. Η ψηφιοποίηση των αντιδράσεων μας, θα δημιουργήσει ένα ψηφιακό αρχείο των κινήσεων και της τοποθεσίας μας , ένα αρχείο που ποτέ πριν δεν έχει υπάρξει. Για τους διαφημιστές και τους λιανέμπορους, αυτό θα είναι ένα χρυσωρυχείο, όπως ακριβός και τα μέσα κοινωνικής δικτύωσης ήταν πρωτύτερα. Ένας ολοκαίνουριος κόσμος προσωπικών δεδομένων που μπορεί να χρησιμοποιηθεί, για να διανέμει με ακόμη μεγαλύτερη ακρίβεια στοχευόμενες διαφημίσεις, χωρίς καμία αμφιβολία, αυτές οι παροχές του IoT , όχι μόνο θέλουν να αναγνωρίσουν ποιοι ήμαστε, αλλά να μας υπενθυμίσουν που ήμασταν. Και όπως κάνουμε τώρα online

πολλοί χρήστες θα συναινέσουν στο να συγκεντρώνονται οι πληροφορίες τους κάτω από αυτές τις συνθήκες.

Η νομοθεσία, κάνει ό,τι μπορεί, ώστε να ανιχνεύσει τις φυσικές κινήσεις ενός υπόπτου, είτε μέσω κινητών τηλεφώνων, IP διευθύνσεων ή στίγματα GPS που συνδέονται με IoT συσκευές.

3.3 Κοινωνικές Επιπτώσεις

Οι επιπτώσεις αυτής της τεχνολογίας στην κοινωνία θα είναι εξαιρετικά πολύπλοκες και πιθανώς απρόβλεπτες, ωστόσο, κάποια γενικά σημεία που αξίζουν ενδεικτικής αναφοράς είναι τα εξής:

• Οργανωτικές και θεσμικές καινοτομίες θα προκύψουν από IoT, που θα αλλάξει ριζικά τον τρόπο που κάνουμε τα πράγματα, που ζούμε και επικοινωνούμε.

• Θα προκύψουν ακόμα αλλαγές σε απόψεις, στάσεις και συμπεριφορές για την προστασία της ιδιωτικής ζωής, την προστασία των δεδομένων, τη δημόσια ασφάλεια, τη διαχείριση της ενέργειας με χαμηλότερο κόστος.

• Η υιοθέτηση του Ίντερνετ των πραγμάτων, θα μπορούσε να οδηγήσει σε συνδυασμό με τα τεχνολογικά συστήματα, σε μεγάλο βαθμό στη μείωση της ανθρώπινης παρέμβασης στην παραγωγική διαδικασία, προκειμένου να αυξηθεί η αξιοπιστία και ο αυτοματισμός των σχετικών διαδικασιών.

• Νέοι κίνδυνοι για τη ζωή και την περιουσία θα προκύψουν από την αθέμιτη εισβολή σε συστήματα και αλλοίωση δεδομένων από εγκληματίες και αθέμιτου3 εισβολείς.

• Το IoT θα οδηγήσει αναπόφευκτα σε μια υψηλότερη ποιότητα στην παροχή πολλών υπηρεσιών που ήταν προβληματικές.

3.4 IoT και Οικονομία

Η αυξανόμενη διαθεσιμότητα των δεδομένων υψηλής ποιότητας που συλλέγονται και διαβιβάζονται σε πραγματικό χρόνο θα οδηγήσει αναμφίβολα σε επιστημονική, τεχνική και εμπορική καινοτομία. Η βιομηχανία επενδύει σήμερα τεράστια χρηματικά ποσά σε IoT υποδομές, οι ευκαιρίες για τις επιχειρήσεις είναι τεράστιες όσον αφορά τη βελτίωσης της παραγωγικότητας, και τον έλεγχο των αλυσίδων εφοδιασμού που διανέμονται σε πραγματικό χρόνο. Το IoT είναι ένας δυναμικός κόσμος, και η τεχνολογία είναι πιθανό να αναπτυχθεί ταχύτερα από τον κανονικό. Αλλά πόσα ξέρουμε για το δυναμικό αυτών των τεχνολογιών; για την υποστήριξη της ανταγωνιστικότητας των επιχειρήσεων και της επιτυχίας; Τι είναι το αναμενόμενο οικονομικό όφελος; Και πώς θα αλλάξει το χώρο εργασίας;

Για να κατανοήσουμε τις επιπτώσεις του IoT για τις επιχειρήσεις όσο και για την ευρύτερη κοινωνία θα επικεντρώνουμε στην ικανότητα των εφαρμογών τους σχετικά με:

1. πληροφόρηση, όπως για παράδειγμα η συλλογή και η επεξεργασία πληροφοριών μέσω αισθητήρων.

2. αυτοματοποίηση και συνταγογράφηση δραστηριοτήτων, όπως για παράδειγμα με τη χορήγηση μιας λειτουργίας σε ένα σύστημα ή με την επίβλεψη της εκπλήρωσης μιας δραστηριότητας.

3. μετατροπή των δραστηριοτήτων, όπως για παράδειγμα με τον επανασχεδιασμό μιας επιχειρηματικής διαδικασίας. Καθώς οι εφαρμογές του IoT θα χρησιμοποιούνται ευρέως, πρέπει να καταλάβουμε πώς αλληλεπιδρούν μεταξύ τους με τις οργανώσεις και τους ανθρώπους, και πώς οι ενέργειές τους είναι πλήρως ενεργοποιημένες ή περιορισμένες.

Τα δεδομένα αισθητήρα που συγκεντρώθηκαν μπορεί να επιτρέψουν τεκμηριωμένη λήψη αποφάσεων από διαχειριστές, αλλά αυτομάτως θα μπορούσε επίσης να περιορίσουν την ελευθερία του ατόμου να ενεργεί με διαφορετικό τρόπο.

Οι αισθητήρες είναι μόνο ένα στοιχείο στο IoT. Η άλλη μεγάλη κατηγορία συσκευών είναι οι ελεγκτές. Πρόκειται για συσκευές όπως διακόπτες, βαλβίδες και ενεργοποιητές, που εκτελούν συγκεκριμένες ενέργειες, όπως η προσαρμογή των ρυθμίσεων σε εξοπλισμό για μεταβλητές όπως η ταχύτητα, η θερμοκρασία ή πίεση, η ενεργοποίηση ανεμιστήρων εξαερισμού, κ.α. Το Δεκέμβριο του 2012 κινεζική ομάδα hacking εντοπίστηκε και συνελήφθη ενώ προσπαθούσε να διεισδύσει στο σύστημα ελέγχου ροής ύδατος των ΗΠΑ.

Παρόμοια προβλήματα έχουν σημειωθεί σε αρκετές χώρες. Οι περισσότερες επιθέσεις προέρχονταν από τη Ρωσία και την Κίνα. Ο Kyle Wilhoit της Trend Micro, κατέληξε στο συμπέρασμα ότι εισβολείς θα μπορούσαν να πάρουν τον έλεγχο σε πολλά συστήματα επιχειρήσεων κοινής ωφέλειας σε ολόκληρο τον κόσμο και ότι είναι πιθανό οι μηχανικοί των εγκαταστάσεων να είναι απληροφόρητοι για το τι συμβαίνει.

Τον Οκτώβριο του 2012, ο πρώην υπουργός Άμυνας των ΗΠΑ Λέον Πανέτα προειδοποίησε για μια πιθανή επίθεση cyber-Pearl Harbor, που θα μπορούσε να καταστρέψει το δίκτυο ηλεκτρικής ενέργειας των ΗΠΑ και τα συστήματα οικονομικών μεταφορών. Η Cisco εντόπισε τον Μάιο του περασμένου έτους μια

σειρά έμμεσων επιθέσεων στον τομέα της ενέργειας και στις εταιρείες πετρελαίου. Γέφυρες, φράγματα, κτίρια, αγωγοί, αεροπλάνα. κ.α. μπορούν να παρακολουθούνται συνεχώς για τη δομική ακεραιότητα τους από κατάλληλα τοποθετημένους αισθητήρες. Οι δρόμοι ίσως γεμίσουν με αισθητήρες έτσι ώστε τα αυτοκίνητα που θα ενσωματώνουν τεχνολογία αυτόματου πιλότου θα γίνουν πραγματικότητα. Τα σπίτια μας με τη βοήθεια αισθητήρων θα προσπαθήσουν να περιορίσουν την κατανάλωση ενέργειας. Πλυντήρια ρούχων θα μπορούν να επικοινωνούν με έναν έξυπνο μετρητή της ΔΕΗ για να αρχίζουν να πλένουν μόνο όταν η χρέωση του ηλεκτρικού ρεύματος είναι στα χαμηλότερα επίπεδα.

3.5 Μετατροπές των Εργασιακών Διαδικασιών

Βελτίωση της επιχειρησιακής απόδοσης έχει διερευνηθεί ιδιαίτερα στον τομέα της διαχείρισης της εφοδιαστικής αλυσίδας, όπου τα αναμενόμενα οφέλη περιλαμβάνουν μείωση των σφαλμάτων στα εγχειρίδια χρήσης και τη βελτίωση του ελέγχου της διαχείρισης των αποθεμάτων. Το IoT αναπόφευκτα θα οδηγήσει σε ανασχεδιασμό των διαδικασιών εργασίας, όσο οι οργανωσιακές ευθύνες για τον έλεγχο και την υπευθυνότητα αλλάζουν και αναδιανέμονται.

Ένας υπάλληλος καταστήματος θα μπορούσε να καθίστανται υπεύθυνος για τη χρήση του συστήματος για να ελέγξει τη γνησιότητα ενός αντικειμένου με IoT χαρακτηριστικά και ένας επιτηρητής εξ αποστάσεως μπορεί να καταστεί υπεύθυνος για να παρέμβει στην περίπτωση που συμβεί ένα περιστατικό. Δυσκολίες μπορεί να προκύψουν, εάν υπάρχει έλλειψη ικανότητας του ελέγχου, για παράδειγμα, αν ένας επόπτης είναι πολύ μακριά για να παρέμβει γρήγορα, ή σε περίπτωση που προκύψει σύγκρουση μεταξύ των νέων και των υφιστάμενων ευθυνών. Ενώ ανάπτυξη του Διαδικτύου των πραγμάτων στο χώρο εργασίας μπορεί να οδηγήσει σε ανειδίκευση των εργαζομένων λόγω του αυτοματισμού, από

την άλλη μπορεί εξίσου να οδηγήσει στην εκτέλεση πιο προσανατολισμένων και υψηλότερου επιπέδου υπηρεσιών. Η χρήση σε βιβλιοπωλεία της αυτόματης εξυπηρέτησης της αγοράς βιβλίου με τη βοήθεια της χρήσης της τεχνολογίας RFID σημαίνει οι βιβλιοθηκονόμοι εκτελούν λιγότερες διαδικασίες ρουτίνας με τους πελάτες και έτσι γίνονται πιο διαδραστικοί. Τα άτομα μπορεί επίσης να καταλήγουν να αισθάνονται να χάνουν τον έλεγχο και να απογοητεύονται όταν χρησιμοποιούν παντού υπολογιστές ή εφαρμογές του IoT και αν δεν διαθέτουν την κατάλληλη γνώση για το πώς να αλληλεπιδρούν και να χρησιμοποιούν τις σχετικές υπηρεσίες.

3.6 Εφαρμογές του IoT στο χώρο εργασίας

Αν προχωρήσουμε προς νέες και πιο ευέλικτες μορφές ελέγχου που μας ακολουθούν και ό,τι μας ενδιαφέρει, όπου και να πάμε, η οργανωσιακή κουλτούρα θα μπορούσε να επηρεάσει την αντίληψη των εφαρμογών του IoT από τους εργαζομένους είτε ως εργαλεία επιτήρησης που επιτρέπουν την ανάπτυξη νέων συστημάτων ελέγχου και λογιστικού ελέγχου, ή ως ένα πολύτιμο εργαλείο υποστήριξης για τις εργασιακές τους δραστηριότητες και την ασφάλεια τους ή ακόμη και τα δύο ταυτόχρονα.

Δεν υπάρχουν πειστικές αποδείξεις ως προς την συγκέντρωση ή αποκέντρωση των επιπτώσεων των εφαρμογών IoT σχετικά με την οργανωτική δομή και δύναμη. Αυξημένες δυνατότητες για τον έλεγχο και τη διαχείριση ενισχύουν την εφαρμογή των κανόνων και ως εκ τούτου, ελέγχουν τη συμπεριφορά που μπορεί να συνεπάγεται τη λήψη αποφάσεων από διευθυντικά στελέχη και την αύξηση της δύναμής τους μέσα στους οργανισμούς. Ωστόσο, η αυξημένη συλλογή δεδομένων μπορεί να χρησιμοποιηθεί όχι μόνο από τη διοίκηση για να ασκεί αυξανόμενη εξουσία και έλεγχο στους υπαλλήλους. οι εργαζόμενοι θα μπορούν επίσης να

χρησιμοποιούν τα δεδομένα για να κρατήσουν τη διαχείριση σε ελεγχόμενα επίπεδα και να τεκμηριώσουν τα αιτήματα τους για περισσότερη ασφάλεια για παράδειγμα. Εν ολίγοις, το Ίντερνετ των πραγμάτων φαίνεται ότι θα επιτρέψει τον μετασχηματισμό στις επιχειρηματικές διαδικασίες. Τα σημερινά επίπεδα των επενδύσεων στον τομέα της τεχνολογίας δείχνουν ότι μια καλή απόδοση αναμένεται από τη βιομηχανία όσον αφορά την αποτελεσματικότητα και την παραγωγικότητα. Ωστόσο, οι εφαρμογές που έχουν υλοποιηθεί μέχρι σήμερα είναι ως επί το πλείστον τη βελτίωση της τρέχουσας επιχειρηματικής πρακτικής. Πολλοί οργανισμοί μπορεί να προτιμούν αυτό το εξελικτικό (και όχι επαναστατικό) μοντέλο της καινοτομίας, και μένει να δούμε πώς θα αντιδράσουν σε περισσότερο ραγδαίες και ριζοσπαστικές, αναδυόμενη, και ίσως καθοδηγούμενες από το χρήστη . Μια παρόμοια εξέλιξη παρατηρήθηκε σε εφαρμογές που αναπτύχθηκαν στις προηγούμενες γενιές του Internet.

3.7 Κτίζοντας Έξυπνες Πόλεις

Σε πολλές χώρες του κόσμου, μεταξύ των οποίων το Ενωμένο Βασίλειο οι πόλεις και οι δήμοι αντιμετωπίζουν την αντικρουόμενες προκλήσεις για την προώθηση της οικονομικής ανάπτυξης και την εξασφάλιση της βιώσιμης ανάπτυξης. Το IoT θεωρείται ευρέως ότι διαδραματίζει σημαντικό ρόλο στην επίτευξη αυτών των κερδών αποδοτικότητας, με προώθηση της ανάπτυξης και την επίτευξη των περιβαλλοντικών στόχων μέσω περιορισμού των εκπομπών αερίων, αποθαρρύνοντας επιβλαβείς για το περιβάλλον καταστάσεις, και προάγει της εξοικονόμηση ενέργειας. Πολλές πόλεις του Ηνωμένου Βασιλείου με σκοπό την μελλοντική εξοικονόμηση ενέργειας, αναπτύσσουν Διαδικτυακές Υποδομές για την ψηφιοποίηση των υφιστάμενων φυσικών υποδομών για την ενέργεια, το νερό και τις μεταφορές.

Η εφαρμογή του IoT σε επίπεδο πόλεων συχνά καθοδηγείται από την κρατική χρηματοδότηση και αφορά κοινοπραξίες του δημόσιου και του ιδιωτικού τομέα. Στην πραγματικότητα οι ψηφιακές επιχειρήσεις που ασχολούνται με το οικοσύστημα επικεντρώνονται γύρω από τις πόλεις. Υποστηρίζουν ένα σύστημα για την προώθηση και την επιβολή συμπεριφοράς και έτσι να τους προετοιμάσουν στην εισαγωγή του IoT μέσω της πληροφόρησης και στρατηγικών που χρησιμοποιούν. Επιπλέον, έχουν δημιουργήσει και μηχανισμούς ανταμοιβής για να «ωθήσουν» τους πολίτες να υιοθετήσουν τέτοιες συμπεριφορές και έτσι να έχουν τα επιθυμητά αποτελέσματα.

ΚΕΦΑΛΑΙΟ 4

Νομικά και Ρυθμιστικά Ζητήματα του Διαδικτύου των Πραγμάτων

Εκτός από τα κοινωνικά ζητήματα που αναλύθηκαν παραπάνω, η τεχνολογική μετάβαση στο Διαδίκτυο των πραγμάτων γεννά πλήθος νομικών και ρυθμιστικών προκλήσεων και ερωτημάτων. Παραδείγματος χάριν:

- Χρειάζεται να υπάρχει στο Διαδίκτυο, όπως το γνωρίζουμε σήμερα, μια λωρίδα ταχείας κυκλοφορίας δεδομένων με εγγυημένη ταχύτητα, δρομολόγηση και ποιότητα για κρίσιμες εφαρμογές IoT δημόσιας ασφάλειας ή υγείας ;
- Αν ναι, πως σχετίζεται η θεσμοθέτηση εγγυημένης ποιότητας σύνδεσης με το φλέγον θέμα της ρύθμισης της ουδετερότητας του Διαδικτύου, όπου όλη η κίνηση ψηφιακών δεδομένων πρέπει να αντιμετωπίζεται ισότιμα από τους παρόχους δικτύων ;
- Τα διασυνδεδεμένα αυτοκίνητα θα καταβάλλουν τέλη περιαγωγής όταν περνάνε τα εθνικά σύνορα και συδέονται με άλλα δίκτυα κινητής τηλεφωνίας στην Ευρώπη ;
- Σε ποιες συχνότητες και σε ποια εναρμονισμένα τεχνικά πρότυπα θα λειτουργούν οι συσκευές αυτές και ποιος θα τις αδειοδοτεί ;
- Ποιός θα επιβλέπει τη συμμόρφωση των κατασκευαστών συσκευών, των εμπόρων και των παρόχων με τη νομοθεσία περί τηλεπικοινωνιών, περί ασφάλειας και περί προστασίας της ιδιωτικότητας ;

4.1 Ο Ρόλος των Ρυθμιστικών αρχών

Ένα από τα σημαντικότερα θέματα που προκύπτουν στην εποχή του IoT είναι η πρόσβαση στους κατασκευαστές ασύρματων διασυνδεμένων συσκευών και στους

παρόχους στην απαιτούμενη για τη διασύνδεση ασύρματη δικτυακή χωρητικότητα με ισότιμους και ανταγωνιστικούς όρους. Η απροβλημάτιστη και χωρίς περιορισμούς κυκλοφορία δεδομένων μέσω δικτύων θα πρέπει να συνεπάγεται με τη συμβατότητα των δικτύων, ώστε να μπορούν να έχουν αμφίδρομη σύνδεση και να παρέχουν σε όλους του χρήστες ίδιου επιπέδου υπηρεσίες.

Η επάρκεια και η διαθεσιμότητα φάσματος συχνοτήτων καθώς και η αποτελεσματική και επωφελής διαχείρισή του αποτελεί ένα ακόμα φλέγον ζήτημα που πρέπει να ρυθμιστεί αποτελεσματικά σε εθνικό, ευρωπαϊκό και παγκόσμιο επίπεδο. Το φάσμα των συχνοτήτων και η ασύρματη χωρητικότητα δικτύων 4G, LTE, και σε μερικά χρόνια 5G, είναι ένας σημαντικός παράγοντας για την εξάπλωση του Internet των πραγμάτων.

Θα πρέπει να βρεθεί άμεσα λύση για το θέμα της ιδιωτικότητας, της εμπιστοσύνης και της ασφάλειας και αυτό μπορεί να γίνει με τη συνεργασία των Ρυθμιστικών Αρχών τηλεπικοινωνιών, ιδιωτικότητας και ασφάλειας (ΕΕΤΤ, ΑΠΔΠΧ, ΑΔΑΕ κλπ) που είναι αρμόδιες στην Ελλάδα. Το IoT θα πρέπει να στηθεί πάνω στις σωστές βάσεις ώστε να προσφέρει ασφάλεια και περιορισμούς πρόσβασης στα ευαίσθητα προσωπικά δεδομένα (εθνική η φυλετική προέλευση, θρησκεία, οικονομική κατάσταση, πολιτικές πεποιθήσεις, σεξουαλικές προτιμήσεις κλπ) των χρηστών (π.χ. κρυπτογράφηση δεδομένων).

Το Διαδίκτυο των πραγμάτων θα δημιουργήσει νέους ορίζοντες ως αφορά την αδειοδότηση, στη πώληση των προϊόντων και των υπηρεσιών. Έτσι για να προστατευτούν τα πνευματικά δικαιώματα θα πρέπει να υλοποιηθούν νέοι τρόποι προστασίας των δημιουργών. Σημαντικό ρόλο θα μπορούσε να παίξει το ίδιο το κράτος μέσω της στήριξης που προσφέρει στις εταιρείες ή στους οργανισμούς που χρησιμοποιούν το IoT. Ένα μεγάλο και σημαντικό ρόλο έχουν οι Εθνικές Ρυθμιστικές Αρχές Τηλεπικοινωνιών ώστε να μπορέσουν να κατανοήσουν και να

ιεραρχήσουν σωστά τις προκλήσεις που προαναφέρονται, δρομολογώντας ικανοποιητικές λύσεις για την αγορά, τους κατασκευαστές και τους παρόχους.

4.2 Ραδιοφάσμα και αδειοδότηση

Η σημασία του ραδιοφάσματος στις ασύρματες τεχνολογίες είναι κεφαλαιώδης. Οι ασύρματες τεχνολογίες γίνονται όλο και πιο διαδεδομένες, τα έξυπνα κινητά τηλέφωνα, οι προσωπικοί υπολογιστές και οι ταμπλέτες είναι μια τέτοια περίπτωση. Όλα εξαρτώνται από την ασύρματη συνδεσιμότητα που παρέχουν οι ασύρματες ευρυζωνικές επικοινωνίες. Ένα σχετικό παράδειγμα είναι η τεχνολογία Wi-Fi, και η διασύνδεση τέτοιων δικτύων μεταξύ τους που χρησιμοποιείται από εκατομμύρια ανθρώπους για την ευκολότερη πρόσβαση στο διαδίκτυο από το σπίτι, το δημόσιο χώρο και το γραφείο.

Ο συνολικός όγκος των υπηρεσιών ανάλογα με τη διαθεσιμότητα του ραδιοφάσματος εκτιμάται από την Επιτροπή ΕΕ ότι είναι αξίας 200 δις € τουλάχιστον ετησίως στην Ευρώπη. Πράγματι, όλο και περισσότεροι τομείς που χρησιμοποιούν διάφορες ασύρματες τεχνολογίες όπως το RFID για να συνδεθούν τα δίκτυα αισθητήρων ή για να αυτοματοποιήσουν τις διαδικασίες τα εργοστάσια. Επιπλέον, τα αυτοκίνητα μπορούν να έχουν ασύρματες τεχνολογίες για την αύξηση της οδικής ασφάλειας, και το ραδιοφάσμα είναι επίσης ζωτικής σημασίας στις επιστημονικές υπηρεσίες για σύνδεση των δορυφορικών επικοινωνιών.

Μια κοινή και εναρμονισμένη προσέγγιση για την ρύθμιση του ραδιοφάσματος στην Ευρώπη είναι απαραίτητη. Όλες οι ασύρματες τεχνολογίες πρέπει να μεταδίδουν και να λαμβάνουν πληροφορίες μέσω του ραδιοφάσματος. Τέτοιες μεταδόσεις μπορεί να χρησιμοποιηθούν για μια ποικιλία για διαφορετικούς σκοπούς. Ωστόσο, προκειμένου να διασφαλιστεί ότι οι υποψήφιοι που

διαγωνίζονται για το ραδιοφάσμα δεν παρεμβαίνουν ο ένας τις λειτουργίες του άλλου, είναι απαραίτητο να συντονίσουν τη χρήση των συχνοτήτων για τις εφαρμογές IoT τόσο σε εθνικό όσο και σε διεθνές επίπεδο.

Η μεγιστοποίηση του οικονομικού οφέλους της Ενιαίας Ευρωπαϊκής Αγοράς

Η μεγιστοποίηση των οικονομικών οφελών της Ενιαίας Ευρωπαϊκής Αγοράς ("Connected Continent") χρειάζεται συντονισμό σε Ευρωπαϊκό επίπεδο: εναρμόνιση των κανόνων πρόσβασης στο ραδιοφάσμα σε διασυνοριακό επίπεδο. Ο γενικός στόχος της πολιτικής για το ραδιοφάσμα της ΕΕ είναι, συνεπώς, να συντονίζει την προσέγγιση για τη διαχείριση του ραδιοφάσματος σε ολόκληρη την Ένωση, να προωθήσει τον εκσυγχρονισμό της διαχείρισης του ραδιοφάσματος, εξασφαλίζοντας στην Ευρώπη ότι αποκομίζει το μεγαλύτερο δυνατό όφελος από τη χρήση των περιορισμένων πόρων, τόσο σήμερα όσο και στο μέλλον.

Η Πολιτική Ραδιοφάσματος της ΕΕ

Δεδομένης της αυξανόμενης ζήτησης του ραδιοφάσματος ως ένα φυσικό πόρο για την Κοινωνία της Πληροφορίας, και με βάση την πρόοδο που έχει σημειωθεί στο πλαίσιο της απόφασης για το ραδιοφάσμα (676/2002/ΕΚ), το 2012 η Ευρωπαϊκή Ένωση θέσπισε ένα πρόγραμμα πολιτικής για το ραδιοφάσμα, να καθορίσει τους βασικούς στόχους της πολιτικής του και να δημιουργήσει τις γενικές αρχές για τη διαχείριση του ραδιοφάσματος στην Εσωτερική Αγορά. Αυτό το πρόγραμμα υποστηρίζει τους στόχους και τις βασικές δράσεις της πρωτοβουλίας της Ευρώπης και του Ψηφιακού Θεματολογίου 2020 για την Ευρώπη, και ιδίως επικεντρώνεται στην εξάλειψη του ψηφιακού χάσματος, την αποδοτική χρήση του φάσματος, την προώθηση των επενδύσεων, του ανταγωνισμού, της καινοτομίας και την προστασία των στόχων γενικού συμφέροντος, όπως η πολιτιστική πολυμορφία και η πολυφωνία των μέσων ενημέρωσης.

Προτάθηκε από την Ευρωπαϊκή Επιτροπή το 2010 και εγκρίθηκε από το Ευρωπαϊκό Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο στις 14 Μαρτίου του 2012, το πρόγραμμα Πολιτικής Ραδιοφάσματος καθορίζει επίσης έναν οδικό χάρτη για τα επόμενα βήματα στην πολιτική ραδιοφάσματος (Radio Spectrum Policy Group RSPP) της Ευρωπαϊκής Ένωσης. Η έκθεση επικεντρώνεται στις ανάγκες φάσματος για υψηλής ταχύτητας 4ης γενιάς (4G) ασύρματα ευρυζωνικά συστήματα ως βασική δράση στο πλαίσιο του Ψηφιακού Θεματολογίου για την Ευρώπη. Επίσης, λαμβάνονται οι απαιτήσεις των άλλων τομέων (όπως ο οπτικοακουστικός τομέας, οι μεταφορές, η έρευνα, η προστασία του περιβάλλοντος ή της ενέργειας) υπόψη από την RSPP, διασφαλίζοντας παράλληλα βασικές απαιτήσεις άμυνας, έκτακτης ανάγκης ή της παρατήρησης της γης. Με βάση τους στόχους της πολιτικής, όπως ορίζονται στην RSPP, η Ευρωπαϊκή Επιτροπή, σε συνεργασία με όλα τα κράτη μέλη θα εργαστούν για την ολοκλήρωση της εσωτερικής αγοράς ενισχύοντας την ασύρματη καινοτομία

Τρεις βασικοί στόχοι: εναρμόνιση, αποτελεσματικότητα, διαθεσιμότητα

Οι τρεις βασικοί στόχοι της πολιτικής για το ραδιοφάσμα της ΕΕ είναι η εναρμόνιση των όρων πρόσβασης στο ραδιοφάσμα που επιτρέπουν τη διαλειτουργικότητα στις οικονομίες για ασύρματο εξοπλισμό, να εργαστούν προς την κατεύθυνση μιας πιο αποτελεσματικής χρήσης του ραδιοφάσματος, καθώς και για τη βελτίωση της διαθεσιμότητας των πληροφοριών σχετικά με την τρέχουσα χρήση, όσο και για τα μελλοντικά σχέδια της χρήσης και της διαθεσιμότητας του ραδιοφάσματος. Με βάση το κανονιστικό πλαίσιο της ΕΕ για τις ηλεκτρονικές επικοινωνίες, ο εκσυγχρονισμός της διαχείρισης του ραδιοφάσματος με στόχο τη διευκόλυνση της πρόσβασης σε ραδιοφάσμα μέσω της μεγαλύτερης ευελιξίας στις συνθήκες χρήσης του στην αγορά, οδήγησε τη διαχείριση των δικαιωμάτων χρήσης του ραδιοφάσματος, όπως η εμπορία ραδιοφάσματος, καθώς και με την εισαγωγή

πιο αποδοτικών ή έξυπνων τεχνολογιών που μπορούν να μοιραστούν συχνότητες και η καλά στοχευμένη ανακατανομή της χρήσης του ραδιοφάσματος για την εσωτερική αγορά.

4.3 Ελεγκτικοί μηχανισμοί και Ευθύνη των εταιριών

Τώρα είμαστε σε θέση να διαχειριστούμε προηγούμενες απρόσιτες περιοχές μέσω της χρήσης της τεχνολογίας και περιμένουμε όλο και περισσότερο να έχουμε πρόσβαση σε οποιεσδήποτε πληροφορίες μας ενδιαφέρουν ανά τον κόσμο. Υποθέτουμε επίσης ότι οι πληροφορίες που βασίζονται σε ψηφιακά δεδομένα είναι αξιόπιστες, και χρησιμοποιούνται όλο και περισσότερο ως υποκατάστατο για άλλα είδη. Αυτή η ενημερωτική ικανότητα ταυτίζεται με τις κοινωνικές τάσεις για πιο ευέλικτο λογιστικό έλεγχο. Με την ικανότητά του να συλλέγει δεδομένα για τις εργασιακές δραστηριότητες και για τις θέσεις των στοιχείων του ενεργητικού, το IoT υπόσχεται αυξημένο έλεγχο των πολύπλοκων καταστάσεων. Οι εταιρείες επίσης βρίσκονται υπό πίεση από τους πελάτες, τις ασφαλιστικές εταιρείες και ρυθμιστικούς φορείς για να υπάρχει μεγαλύτερη διαφάνεια, και η τεχνολογία όλο και περισσότερο εισχωρεί στις βιομηχανίες για την προώθηση της υγείας και της ασφάλειας, την πρόληψη των κινδύνων αστικής ευθύνης, και να βελτιώσει τον έλεγχο και τη διαδικασία της επαλήθευσης των αποτελεσμάτων.

Σε περιπτώσεις περίπλοκων συμβολαίων και δημόσιων-ιδιωτικών συνεργασιών περιλαμβάνει το IoT μοιρασμένες ευθύνες για την εκτέλεση των διαδικασιών καθώς οι εταιρίες ολοένα και περισσότερο υποχρεούνται να παρέχουν αποδείξεις και να δώσουν λεπτομέρειες για το πότε, από ποιόν και υπό ποιες συνθήκες έχουν ολοκληρωθεί οι σχετικές διαδικασίες. Αισθητήρες που συλλέγουν ψηφιακά δεδομένα μπορούν να αναπτυχθούν σε χώρους όπου προηγουμένως ήταν πρόσβαση μόνο σε μη-ψηφιακή λήψη δεδομένων (π.χ. με βάση χειρόγραφο

έγγραφο), και έτσι ικανοποιείται η απαίτηση διαφάνειας και ελέγχου των πληροφοριών. Ο ρόλος της αστυνομίας, των διωκτικών αρχών, και των αρχών ασφαλείας κάθε κράτους και των ορίων πρόσβασης στα ψηφιακά δεδομένα του IoT που πρέπει να τεθούν νομοθετικά είναι επίσης σημαντικός σε αυτή τη διαδικασία.

4.4 Προστασία Προσωπικών Δεδομένων και Εμπιστοσύνη

Έχουν ακουστεί δικαίως πολλά για τις πιθανές επιπτώσεις στην ιδιωτική ζωή του Ίντερνετ των Πραγμάτων. Θέματα προστασίας της ιδιωτικής ζωής προκύπτουν ως αποτέλεσμα της κατάρτισης των ευαίσθητων δεδομένων σχετικά με την καταναλωτική συμπεριφορά των ατόμων, έτσι προκύπτει η επιτακτική ανάγκη δημιουργίας ενός μοντέλου μέσω του IoT που να προβλέπει τις ανάγκες αυτές. Δεν είναι δύσκολο να φανταστεί κανείς στο προσεχές μέλλον πόλεις να είναι καταχωρημένες σε ένα πληροφοριακό σύστημα που να ξέρει πού ζείτε, πότε είστε σπίτι και να μπορεί να προβλέψει πότε θα φύγετε, να ξέρει πότε και πόσο συχνά βλέπετε τηλεόραση ή χρησιμοποιείτε το πλυντήριό σας, πότε και πόσο συχνά χρησιμοποιείτε το αυτοκίνητό σας, μπορεί να προβλέψει το βέλτιστο δρόμο να οδηγήσετε ή ποια λεωφορείο θα έχετε την ευκαιρία να πάρετε το πρωί. Θα ήταν εύκολο να καταγραφούν από αισθητήρες στο σπίτι και το αυτοκίνητό σας, και τα ψηφιακή ίχνη που έχουν συλλεγεί από το ψηφιακό εισιτήριο σας. Η επιλογή από ένα τέτοιο σύστημα μπορεί να μην είναι εύκολη, γιατί αυτό σήμαινε μη διαθεσιμότητα βασικών υπηρεσιών, όπως η θέρμανση ή η μεταφορά.

Για να επιτύχουν, οι δημόσιες υποδομές του IoT απαιτούν ευρεία δημόσια υποστήριξη που μπορεί να είναι μόνο να επιτευχθεί μέσω της ευρείας εμπλοκής των πολιτών και να παρθούν μέτρα για να βοηθήσουν τους πολίτες να κατανοήσουν το σκοπό των προτεινόμενων εξελίξεων. Εάν αυτό δεν είναι γίνει

εγκαίρως, μπορούμε να αναμένουμε την αντίσταση από εκείνους που τελικά θα επηρεαστούν οι εξελίξεις καθώς θα αποτελούν τροχοπέδι αυτών. Πολλά σχέδια έξυπνης ενέργειας στις ΗΠΑ και την Ευρώπη έχουν ήδη εγκαταλειφθεί, επειδή οι καταναλωτές δεν εμπιστεύονται τις προθέσεις των εταιρειών ενέργειας κατά την εγκατάσταση έξυπνων μετρητών στο σπίτι. Ωστόσο, έχουμε δει με την ανάπτυξη των μεταφορών με την ταξιδιωτική κάρτα για παράδειγμα οι καταναλωτές έχουν κίνητρο να τη χρησιμοποιήσουν στις συναλλαγές τους και να μοιραστούν πληροφορίες για την ιδιωτικής τους ζωή σε ορισμένες υπηρεσίες, ιδίως αν έχουν εμπιστοσύνη στις οργανώσεις που τα διαχειρίζονται.

Παρά τις εύλογες ανησυχίες για την προστασία της ιδιωτικής ζωής, η δημοτικότητα δεν έχει ακόμα ρυθμιστεί ολοκληρωτικά, ούτε υπάρχει κάποια νομοθεσία που να έχει εφαρμοστεί καθολικά. Αντιθέτως η προστασία της ιδιωτικής ζωής επιδιώκεται στην Ευρώπη μέσα από ένα συνονθύλευμα εθνικών διατάξεων, που υιοθετούν τις σχετικές Οδηγίες της ΕΕ, που περιγράφονται κατωτέρω. Η ύπαρξη ετερογένειας τελικά αποτυγχάνει στο να δημιουργήσει και να εγγυηθεί ένα κοινό πλαίσιο εμπιστοσύνης για τους ανθρώπους και τις εταιρίες.

4.5 Εθνικές πρωτοβουλίες για την ομαλή μετάβαση στο IPv6

Πολλές χώρες στην προσπάθεια τους για ομαλή μετάβαση από το IPv4 στο IPv6 αποφάσισαν τη συγκρότηση ομάδων που να είναι υπεύθυνες για αυτό. Μια εκ των χώρων αυτών είναι και η Ελλάδα δημιουργώντας την Hellenic IPv6 Task Force**.** Απώτεροι στόχοι της ομάδας είναι:

- Παρακολούθηση των εξελίξεων στην Ευρωπαϊκή αγορά. Καταγραφή της υφιστάμενης κατάστασης στην αντίστοιχη ελληνική.

- Οργάνωση συναντήσεων και αναζήτηση μοντέλων συνεργασίας μεταξύ εταιριών, ερευνητικών φορέων και οργανισμών του Δημοσίου.

- Παρακολούθηση της χρήσης και παροχής υπηρεσιών με βάση την τεχνολογία IPv6.

- Ανάδειξη βέλτιστων πρακτικών χρήσης της τεχνολογίας και διάχυση τεχνικών πληροφοριών.

- Εκπόνηση προτάσεων προς την Ελληνική Πολιτεία και άλλους ενδιαφερόμενους φορείς.

Η συμμετοχή στην Ομάδα Δράσης Hellenic IPv6 Task Force είναι ελεύθερη για όλους τους φορείς, οργανισμούς και εταιρίες, που επιθυμούν να συνεισφέρουν εθελοντικά στην κοινή προσπάθεια και να συμβάλλουν ενεργά στην προετοιμασία της χώρας για την ομαλή μετάβαση στο νέο πρωτόκολλο.

Η μετάβαση στο πρωτόκολλο IPv6 έχει πολλά πλεονεκτήματα σε σύγκριση με το προκάτοχο του, υπάρχουν όμως νομικά θέματα και κανόνες που περιορίζουν την πλήρη λειτουργικότητα των πλεονεκτημάτων του IPv6 αν και κυρίως στόχος είναι η βελτίωση της ποιότητας ζωής των πολιτών για την εκμετάλλευση τους όμως απαιτούνται νέοι νόμοι καθώς και έργα για την ομαλή λειτουργιά του πρωτοκόλλου, καθώς η μια δημιουργία νέων νόμων μπορεί να το καθιστά αυτόματα παράνομο σε πολλές περιπτώσεις.

4.6 Ρυθμιστικές Πολιτικές και νομοθετικά μέτρα σε Ευρώπη και ΗΠΑ

Ανησυχίες για τις νομικές επιπτώσεις που μπορεί να προκληθούν από τη χρήση του IPv6 έχουν προκύψει από σχετική Δημόσια Διαβούλευση της Ευρωπαϊκής Ένωσης που δημοσιεύτηκε στις 28.2.2013 (http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation) με τίτλο «Conclusions on the Internet of Things public consultation», που σκοπό είχε να εκθέσει τις απόψεις για την ομαλή ανάπτυξη του IPv6 που κύριο μέλημα της ήταν η προστασία της ιδιωτικής ζωής. Μια άλλη μελέτη με τίτλο «Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination» που δημοσιεύτηκε στις 13.5.2015, (http://ec.europa.eu/digital-agenda/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination) εκφράζει τους προβληματισμούς της Επιτροπής για την ακολουθητέα πολιτική καθώς και τις προβλέψεις της για τη μελλοντική ανάπτυξη του IoT στα κράτη-μέλη, μεταξύ των οποίων και η Ελλάδα όπου προβλέπεται χαμηλή ανάπτυξη εφαρμογών IoT στο άμεσο μέλλον.

Δεδομένης της αυξανόμενης πολυπλοκότητας του IoT, θα πρέπει να απαντηθούν ικανοποιητικά τα ακόλουθα ερωτήματα:

Δεδομένα ιδιοκτησίας. Το πιο σημαντικό, ποια οντότητα είναι κάτοχος των πρωτογενών δεδομένων που συλλέγονται και των στοιχείων που αναλύονται; Εμπιστευτικές πληροφορίες είναι η ψυχή της κάθε οργάνωσης. Μπορεί ένας πάροχος υπηρεσιών να χρησιμοποιεί τα δεδομένα που συλλέγονται για την εξυπηρέτηση άλλων πελατών; Αν η επιχειρηματική σχέση μεταξύ του οργανισμού και τον πάροχο υπηρεσιών καταρρεύσει, μπορεί ο οργανισμός να έχει πρόσβαση στα δικά του ιστορικά στοιχεία;

Αστική Ευθύνη. εάν οι αισθητήρες ή οι ανακοινώσεις σε IoT εφαρμογή δυσλειτουργούν, και προκληθούν σωματικές βλάβες ή υλικές ζημιές ποιος είναι υπεύθυνος; Για παράδειγμα, οι πληροφορίες του ανιχνευτή καπνού μπορεί να μην μεταδοθούν σωστά και ένα σπίτι να καεί. Εάν μια ιατρική συσκευή βραχυκυκλώσει, ο ασθενής μπορεί να τραυματιστεί σοβαρά. Σε μια βιομηχανική εφαρμογή, τμήμα του ακριβού εξοπλισμού μπορεί να υπερθερμανθεί και να γίνει άχρηστο. Εάν υπάρχουν πάροχοι αισθητήρων, προγραμματιστής της διεπαφής, πομπός τηλεπικοινωνιών, απομακρυσμένος συλλέκτης δεδομένων, σε ποιον πρέπει να επιρρίψει οικονομικές ευθύνες η εταιρία που υπέστη βλάβη;

Αυτοματοποιημένες Συμβάσεις. Πολλές από τις άδειες χρήσης για το λογισμικό είναι αυτοματοποιημένες και ενσωματωμένες στην συσκευή μέσω μικροτσίπ. Οι συμβάσεις αυτές έχουν τους συνήθεις όρους των ρητρών της σύμβασης χρήσης, όπως την κυριότητα των δεδομένων, τον περιορισμό της ευθύνης και τον τόπο για την επίλυση διαφορών. Ανάλογα με τα δολάρια της συναλλαγής, οι αυτοματοποιημένες συμβάσεις μπορεί να είναι διαπραγματεύσιμες.

Συντήρηση. Πώς συντηρείται η συσκευή IoT ; Η συντήρηση περιλαμβάνεται σε μια τρέχουσα σύμβαση παροχής υπηρεσιών, ή πρέπει να υπογραφεί ξεχωριστή σύμβαση συντήρησης; Εάν το ζήτημα συντήρησης δεν έχει συζητηθεί πριν από την εφαρμογή, θα μπορούσε να έχει σημαντική οικονομική επίπτωση στον προϋπολογισμό του οικιακού η επιχειρηματικού χρήστη.

Κινητές εφαρμογές. Για τις καταναλωτικές όπως και τις βιομηχανικές εφαρμογές, οι κινητές εφαρμογές μπορεί να παίξουν μεγάλο ρόλο. Η κινητή εφαρμογή θα επηρεάσει την απόδοση και την ακρίβεια ; Όλα τα παραπάνω ερωτήματα υπαντούνται εν μέρη με τους νόμους-οδηγίες που έχουν θεσπίσει τα κράτη ανά τον κόσμο, η νομοθεσία σε πολλές περιπτώσεις είναι ίδια έχοντας

κοινές κατευθύνσεις σχεδόν σε όλα τα κράτη και σε άλλες περιπτώσεις διαφέρει αρκετά.

Σύγκριση νομοθεσίας της Ευρωπαϊκής ένωσης με την αντίστοιχη των ΗΠΑ για την προστασία των δεδομένων

Στην Ευρώπη, υπάρχει σειρά γενικών και τομεακών Οδηγιών της ΕΕ για την προστασία των δεδομένων στο χώρο των ηλεκτρονικών επικοινωνιών. Μεταξύ αυτών οι Οδηγίες 95/46/EC, 97/66/EC και από τις πιο πρόσφατες 2002/21/EC, 2009/140/EC), που θα αντικατασταθούν σύντομα με ένα Κανονισμό Προστασίας Δεδομένων, ενιαίας εφαρμογής σε όλα τα κράτη-μέλη. Θεμέλιος λίθος για τη σύννομη επεξεργασία δεδομένων στην Ευρώπη είναι η συναίνεση του χρήστη που πρέπει κατά κανόνα να είναι ρητή και έγγραφη. Πως θα εξασφαλιστεί όμως αυτή η συναίνεση, σε επίπεδο συσκευής, με την άδεια χρήσης, με την on line εγγραφή του χρήστη σε ένα δικτυακό τόπο του κατασκευαστή ;

Αντίθετα, οι ΗΠΑ δεν διαθέτουν ενιαία αλλά τομεακή νομοθεσία (Κανόνες Ασφαλούς Λιμένα – Safe Harbour) για την προστασία των δεδομένων, η οποία βασίζεται σε ένα συνδυασμό της νομοθεσίας-ρύθμισης και αυτορρύθμισης.

Η ετερογένεια της νομοθεσίας μεταξύ κρατών δεν ευνοεί την ανάπτυξη της αγοράς συσκευών σε παγκόσμια κλίμακα , άρα απαιτείται μεγαλύτερη εναρμόνιση.

Στην Ελλάδα υπάρχουν επίσης νόμοι περί προστασίας των προσωπικών δεδομένων, που κατά βάση εφαρμόζονται για την προστασία των προσωπικών δεδομένων του χρήστη στο Διαδίκτυο των πραγμάτων, όπως:

- **Ο Νόμος 2472/199 «**Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα»**.**

- **Ο Νόμος 3471/2006** «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν. 2472/97, όπως τροποποιήθηκε με τους Ν. 3783/2009, Ν. 3917/2011 και Ν. 4070/2012)»
- **Ο Νόμος 3783/2009** «Ταυτοποίηση των κατόχων και χρηστών εξοπλισμού και υπηρεσιών κινητής τηλεφωνίας και άλλες διατάξεις»
- **Ο Νόμος 3917/2011** «Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις».

4.7 Συμπεράσματα

Το Διαδίκτυο των Πραγμάτων βρίσκεται ακόμα στα σπάργανα, αλλά η γενικευμένη υιοθέτησή του αναμένεται να αλλάξει την οικονομία και την κοινωνία συνεπιφέροντας σημαντικές ανατροπές στην διακυβέρνηση, στην παραγωγική διαδικασία, στην οικονομία, στην επιχειρηματικότητα και στην επικοινωνία ανθρώπων και μηχανών (M2M).

Οι συσκευές που είναι εξοπλισμένες με αισθητήρες είναι ένα ελάχιστο μέρος της υφιστάμενης βάσης των πιθανών αντικειμένων που θα μπορούσαν να συνδεθούν μελλοντικά στο Διαδίκτυο. Τα δεδομένα που παράγονται από αισθητήρες είναι ακόμα κατακερματισμένα και συνήθως περιορίζονται στον κατασκευαστή της συσκευής.

Καθώς όμως αυτές οι «έξυπνες» καταναλωτικές συσκευές, αθλητικός και ιατρικός εξοπλισμός, ρούχα, ρολόγια, γυαλιά (fitness trackers, watches, smart smart meters κλπ), και τα δεδομένα που αυτές συλλέγουν και μεταδίδουν μέσω Διαδικτύου ευρυζωνικών δικτύων νέας γενιάς, σταθερών (FTTH, FTTC) και κινητών (4G, 5G) θα καθίστανται ευρέως διαθέσιμα, εκτός από τα σημαντικά οφέλη, οι κίνδυνοι για την ασφάλεια και ιδιωτικότητα των χρηστών θα αυξάνονται θεαματικά.

Με τις δυνατότητες εντοπισμού και παρακολούθησης τόσο οι νόμιμες εταιρείες και οργανισμοί, όσο και οι εγκληματίες θα θελήσουν να αποκτήσουν πρόσβαση σε προσωπικές πληροφορίες σχετικά με τη ζωή μας. Για το λόγο αυτό είναι σημαντικό να διασφαλιστεί με τις κατάλληλες πολιτικές και νομοθετικές πρωτοβουλίες η ομαλή και συντονισμένη μετάβαση στο νέο ψηφιακό οικοσύστημα στην Ευρώπη και στον πολιτισμένο κόσμο.

Εάν εφαρμοστεί σωστά, το IoT μπορεί να αλλάξει τον κόσμο με θετικό τρόπο, ακόμα περισσότερο από ότι μπορούμε να φανταστούμε, κάνοντας μας ασφαλέστερους και υγιέστερους, με καλύτερη διαχείριση της ενέργειας, των φυσικών πόρων, μειώνοντας τα απόβλητα, πετυχαίνοντας εξοικονόμηση χρημάτων και βελτίωση του περιβάλλοντος.

Πλην όμως, η ύπαρξη πληθώρας αισθητήρων που θα βρίσκονται σχεδόν παντού δεν είναι μόνο μια πρόκληση, αλλά και μία σοβαρή απειλή γενικευμένης παρακολούθησης των δραστηριοτήτων μας και της ζωής μας. Καθώς το Διαδίκτυο εξελίσσεται, πρέπει να καθοριστούν αυστηρά τα αντίστοιχα πρότυπα ασφάλειας.

Θα πρέπει να περιμένουμε για να δούμε πως οι κοινωνίες θα προσαρμοστούν, όχι μόνο για τη χρησιμότητα του, αλλά να πειστούν ότι θα εφαρμοστούν κατάλληλες διασφαλίσεις για να εξασφαλιστεί η προστασία της ιδιωτικής ζωής και της ασφάλειας μας. Επειδή δεν είναι δυνατό να υπάρξει μία Κεντρική Αρχή αρμόδια για να επιβλέπει συνολικά τη συμμόρφωση, αλλά πληθώρα επιμέρους αρχών, η εκπαίδευση των χρηστών σε πολιτικές ασφαλούς χρήσης και η ευαισθητοποίηση των καταναλωτών είναι σημαντικός παράγοντας επιτυχίας του όλου εγχειρήματος.

Σε ευρωπαϊκό και παγκόσμιο επίπεδο απαιτείται η διεθνής συνεργασία μεταξύ κρατών, των οργάνων της ΕΕ, και ρυθμιστικών αρχών, διαλειτουργικότητα δικτύων και εφαρμογών, εναρμονισμένα τεχνικά πρότυπα, συντονισμένες πολιτικές ανάπτυξης ευρυζωνικών δικτύων επόμενης γενιάς και πολιτικές ρασδιοφάσματος. Η ύπαρξη όλων των ανωτέρω συνεργειών αποτελεί όρο ομαλής και επιτυχούς μετάβασης στο ψηφιακό μας μέλλον.

Αυτή η σελίδα αφήνεται σκόπιμα κενή

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνική

1. Η Μετάβαση του διαδικτύου από το IPv4 στο IPv6 - Δρα Ν. Τσαρμπόπουλου Ενημερωτικό δελτίο της ΕΕΤΤ τεύχος Νο 17 Ιούλιος 2008
2. Σύγχρονα δίκτυα τηλεπικοινωνιών - Δρα Παπαχριστοφή Κωνσταντίνου Εκδότης: εκδόσεις νέων τεχνολογιών ΕΠΕ, Χρονολογία έκδοσης: 2001, Αθήνα
3. Το Πρωτόκολλο IPv6 και το Internet των Πραγμάτων, Χρήστος Ζώτος, μεταπτυχιακή εργασία, ΠΑΠΕΙ, Τμήμα Ψηφιακών Συστημάτων, 2013.

Ξένη

1. IPv6 Essentials - Silvia Hagen, Second edition (May 24, 2006) , Geneva
2. Understanding IPv6 Edition – Joseph Davies third edition (June 25, 2012),London
3. Deploying IPv6 Networks 2006 - Ciprian Popoviciu, Eric Levy-Abegnoli, Patrick Grossetete first edition (Feb. 10 2006),California
4. Building the Internet of Things with IPv6 and MIPv6: The Evolving World of M2M Communications-Daniel Minoli,August 2013,New York
5. The zero marginal cost society the internet of things, the collaborative commons and the eclipse of capitalism, Jeremy Rifkin, Palgrave Macmillan, New York 2014.

Διαδικτυακοί τόποι

1. Kanellos Leonidas - Regulation towards a smart digital ecosystem, EETT 8th International Conference, 16 May 2013 http://www.telecomexperts.eu/#!inteconf/c1xtt

2. Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination, 2015 http://ec.europa.eu/digital-agenda/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination
3. Internet of Everything ABI search https://www.abiresearch.com/market-research/service/internet-of-everything/
4. Hewlett Packard security IoT http://www.securityinsider.gr/hewlett-packard-most-home-security-systems-are-easily-hacked/
5. RFID Wikipedia https://el.wikipedia.org/wiki/RFID
6. https://www.samsung.com/
7. radio spectrum policy for EU https://ec.europa.eu/digital-agenda/en/what-radio-spectrum-policy
8. Mobile Cybersecurity and the Internet of Things Empowering M2M Communication http://www.ctia.org/docs/default-source/default-document-library/ctia-iot-white-paper.pdf
9. IPv6 protocol www.Ipv6.com
10. EETT http://www.eett.gr/
11. Techguide for windows forIPv6 http://www.zdnetasia.com/techguide/windows/0,39044904,62040433,00.htm
12. U.S. Federal Communications Commission https://en.wikipedia.org/wiki/U.S._Federal_Communications_Commission
13. ΟΔΗΓΙΑ 95/46/ΕΚ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31995L0046&from=EL
14. ΟΔΗΓΙΑ 2002/58/ΕΚ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:el:PDF
15. ΝΟΜΟΣ 2472/1997 ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΑΤΟΜΟΥ ΑΠΟ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΜΕ ΕΝΣΩΜΑΤΩΜΕΝΕΣ ΤΙΣ ΤΡΟΠΟΠΟΙΗΣΕΙΣhttp://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/

NOMOTHESIA%20PROSOPIKA%20DEDOMENA/FILES/2472_97_JUNE2013.PDF

16. Ελληνική Νομοθεσία για τα προσωπικά δεδομένα http://www.dpa.gr/portal/page?_pageid=33%2c123437&_dad=portal&_schema=PORTAL
17. European Union Agency for Network and Information Security https://www.enisa.europa.eu/media/press-releases/enisa-1st-eu-agency-with-ipv6
18. enisa http://www.eett.gr/opencms/export/sites/default/EETT/Electronic_Communications/Telecoms/NetIntegrity/Guidelines/technical-guideline-on-incident-reporting-v-2-0.pdf
19. Top 5 Legal Issues in the Internet of Things http://www.wassom.com/top-5-legal-issues-internet-things-part-2-data-collection-invasion-privacy.html
20. Data Protection Directive https://en.wikipedia.org/wiki/Data_Protection_Directive
21. The legal considerations of the internet of things http://www.computerweekly.com/opinion/The-legal-considerations-of-the-internet-of-things
22. Conclusions of the Internet of Things public consultation http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation
23. Επιμορφωτικά βίντεο από τον ιστότοπο YouTube που χρησιμοποιήθηκαν:

https://www.youtube.com/watch?v=GmnfBBEZCN8

https://www.youtube.com/watch?v=uphxFHnVv1E

https://www.youtube.com/watch?v=gT9nmXPmTXI

https://www.youtube.com/watch?v=oGwOP66eL6k

https://www.youtube.com/watch?v=iR8ve5tTWAA

https://www.youtube.com/watch?v=aor29pGhlFE

https://www.youtube.com/watch?v=8EQze2FJu-k

https://www.youtube.com/watch?v=h1X5dMb3dGo&list=PLsyYTl_JhwoPM_ZAV07S1hSVfB0d6fFIg

https://www.youtube.com/watch?v=h1X5dMb3dGo