ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΡΗΤΗΣ

Σχολή Εφαρμοσμένων Επιστημών
Τμήμα Ηλεκτρονικών Μηχανικών Τ.Ε.

Πτυχιακή Εργασία

Ενσύρματη και Ασύρματη Μετάδοση Πληροφοριών

Μάνος Πηγουνάκης

Επιβλέπων Καθηγητής Δρ. Εμμανουήλ Σκουνάκης, MSc, MSc.

Δεκέμβριος 2014

Αφιερώνεται στην οικογένειά μου

Περίληψη

Σκοπός αυτής της πτυχιακής εργασίας είναι η ανάλυση και επεξήγηση των μεθόδων επικοινωνίας ενσύρματα αλλά και ασύρματα, καθώς και η εξέλιξή τους με την πάροδο του χρόνου με τη συμβολή της τεχνολογίας, παρουσιάζοντας βέβαια θέματα ασφαλείας και κινδύνους που κρύβουν οι τεχνολογίες αυτές.

Πιο συγκεκριμένα, στο πρώτο κεφάλαιο γίνεται μία ιστορική αναδρομή των μεθόδων επικοινωνίας από τα αρχαία χρόνια μέχρι σήμερα, αλλά και πως εξελίχθηκε με τη βοήθεια της τεχνολογίας και του Διαδικτύου.

Στο δεύτερο κεφάλαιο γίνεται μία εκτενής αναφορά στις επικοινωνίες διά της ενσύρματης μετάδοσης, τους τρόπους που επιτυγχάνεται η μετάδοσης της πληροφορίας και ότι σχετίζεται με την ενσύρματη δικτύωση.

Το τρίτο κεφάλαιο αναφέρεται στην ανάπτυξη της ασύρματης επικοινωνίας αλλά και δικτύωσης, αναλύοντας τους τρόπους με τους οποίους επιτυγχάνεται η μετάδοση ασύρματα, καθώς και πως εξελίχθηκαν οι ασύρματες επικοινωνίες με το πέρας του χρόνου.

Στο τέταρτο κεφάλαιο γίνεται εκτενής αναφορά σε θέματα ασφαλείας που προκύπτουν με τη δικτύωση όπως είναι οι κακόβουλες επιθέσεις σε υπολογιστικό αλλά και προσωπικό επίπεδο καθώς και τρόποι με τους οποίους μπορούμε να προστατευτούμε.

Το πέμπτο και τελευταίο κεφάλαιο περιλαμβάνει μία συνοπτική σύγκριση μεταξύ της ενσύρματης και ασύρματης δικτύωσης. Επίσης θίγεται το θέμα των μέσων κοινωνικής δικτύωσης και με ποιον τρόπο έχουν επηρεάσει τις ζωές μας.

Τέλος παραθέτω κάποιες προτάσεις που θα μπορούσαν να μας εξασφαλίσουν μία ασφαλέστερη περιήγηση στο μέλλον.

Abstract

The aim of this Dissertation is to analyze and explain the methods of communication both wired and wireless, and their evolution over time with the help of technology, of course presenting safety issues and risks faced by these technologies.

More specifically, the first chapter is a flashback of communication methods from ancient times until today, and how these are evolved with the help of technology and the Internet.

The second chapter elaborates on communications by wire, the ways in which information transmission is achieved and information related to the wired networking.

The third chapter refers to the development of wireless communications and networking. An analyzing is being done about the ways in which data are transmitted wirelessly, and that wireless communications have evolved over time.

The fourth chapter is a detailed report on safety issues arising with networking such as malicious attacks on computer and personal level as well as ways in which we can protect ourselves.

The fifth and final chapter includes a brief comparison between the wired and wireless networking. It also addresses the issue of social media and how they have influenced our lives.

Finally I quote some suggestions that could provide us a more secure web surfing in the future.

Ευχαριστίες

Αρχικά θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στον επιβλέποντα καθηγητή της παρούσας πτυχιακής εργασίας Δρ. Σκουνάκη Εμμανουήλ για την εμπιστοσύνη που μου έδειξε προκειμένου να αναλάβω την εργασία που αποτελεί ένα από τα κεφάλαια που με ενδιαφέρουν αλλά και για την καθοδήγηση και την επίβλεψη που μου παρείχε ώστε να φέρω την εργασία εις πέρας.

Τέλος εκφράζω την ευγνωμοσύνη μου στους γονείς μου για την υποστήριξη και βοήθειά τους όλα αυτά τα χρόνια, ιδιαίτερα σε όλη τη διάρκεια των σπουδών μου.

Πίνακας Περιεχομένων

Κεφάλαιο 1: Εισαγωγή

1.1 **Ιστορική Αναδρομή**

Ο άνθρωπος ως κοινωνικό και πολυμήχανο ον πάντα προσπαθούσε να έρθει με κάθε δυνατό τρόπο σε επικοινωνία με τους συνανθρώπους του ξεκινώντας να επικοινωνεί με τη φωνή του, αλλά το πρόβλημα ήταν πώς θα βρισκόταν τρόπος να επικοινωνεί από απόσταση. Έτσι, όταν δεν υπήρχε η δυνατότητα επικοινωνίας λόγω της μακρινής απόστασης, εφεύρισκε διάφορους τρόπους ώστε να επιτευχθεί κάτι τέτοιο.

Υπάρχουν πολλά παραδείγματα από το παρελθόν που το αποδεικνύουν αυτό, όπως τα σήματα καπνού που έκαναν οι Ινδιάνοι, τα ταχυδρομικά περιστέρια, οι αγγελιοφόροι στην αρχαία Ελλάδα ή ακόμα και οι τεράστιες φωτιές που άναβαν από βουνό σε βουνό για να προειδοποιήσουν για τυχόν επερχόμενη απειλή κ.α.

Βέβαια όλα τα παραπάνω δεν μπορούν να χαρακτηριστούν ως αξιόπιστοι τρόποι επικοινωνίας, διότι η μετάδοση των πληροφοριών δεν ήταν ούτε γρήγορη, ούτε ακριβής, αλλά και πολλές φορές δεν γνώριζαν αν όντως υπήρχε το επιθυμητό αποτέλεσμα, δηλαδή αν ο παραλήπτης λάμβανε την πληροφορία **[1].**

Με το πέρασμα των ετών και την εφεύρεση του ηλεκτρισμού και αργότερα την αξιοποίηση των νόμων του ηλεκτρομαγνητισμού δημιουργήθηκαν νέοι τρόποι επικοινωνίας.

Με τις γνώσεις και τα μέσα που διέθετε τότε ο άνθρωπος, προσπαθούσε να εξαλείψει τα προβλήματα που υπήρχαν και να βελτιώσει τις συνθήκες της επικοινωνίας. Έτσι το 1838 ο Samuel Morse εφευρίσκει τον ηλεκτρικό τηλέγραφο **(εικόνα 1)** και όλα δείχνουν ότι η ποιότητα της απομακρυσμένης επικοινωνίας θα φτάσει σε πολύ υψηλότερα επίπεδα απ ότι ήταν μέχρι τότε, καθώς με τη χρήση του τηρείται η βασική αρχή της επικοινωνίας, που είναι η επιβεβαίωση της λήψης της πληροφορίας από τον παραλήπτη.

Εικόνα 1 Τηλέγραφος [2]

Ο ηλεκτρικός τηλέγραφος είναι μια διάταξη που με τη βοήθεια του ηλεκτρικού ρεύματος μεταδίδει γραπτά σημεία μεταξύ δύο σταθμών. Εκμεταλλευόμενος λοιπόν τα ρεύματα μικρής και μεγάλης διάρκειας που διέρρεαν το σύρμα του τηλέγραφου επινόησε ένα σύστημα κωδικοποίησης του αλφάβητου γνωστό σε όλους ως “σήματα Morse”. Ο τηλέγραφος χρησιμοποιείται ακόμα και σήμερα σε απομονωμένα από τον κόσμο εργοστάσια ή πλοία και αυτός είναι και ένας λόγος που ακόμα και σήμερα γίνονται συνεχείς προσπάθειες για την τελειοποίησή του [2].

Αργότερα, το 1876, ο Graham Bell εφηύρε το τηλέφωνο **(εικόνα 2)** το οποίο έχει τη δυνατότητα να μετατρέπει τις ηλεκτρικές ταλαντώσεις σε ηχητικές με τη βοήθεια ενός ηλεκτρομαγνήτη.

Φυσικό επακόλουθο ήταν η ανάπτυξη και εξέλιξη του τηλεφώνου, οπότε προέκυψε και η ανάγκη δημιουργίας τηλεφωνικών κέντρων για να καλυφθούν οι ανάγκες των ανθρώπων για επικοινωνία.

Έτσι ξεκίνησε η δημιουργία των πρώτων χειροκίνητων τηλεφωνικών κέντρων, τα οποία συναντάμε μέχρι και σήμερα με την πιο εξελιγμένη τους μορφή που είναι τα αυτόματα πλέον τηλεφωνικά κέντρα [3].

Εικόνα 2 Τηλέφωνο [4]

Μία καινούρια εποχή ανέτειλε για τον κόσμο της επικοινωνίας και μετάδοσης πληροφοριών όταν ο Ιταλός Γουλιέλμο Μαρκόνι το 1895 εφηύρε τον ασύρματο καταφέρνοντας να μεταδώσει πληροφορίες χωρίς καλώδια, αλλά με τη χρήση ηλεκτρομαγνητικών κυμάτων μέσω ενός πομπού κι ενός δέκτη.

Έτσι μπήκε και επίσημα στις ζωές μας ο όρος “Τηλεπικοινωνία”. Κανείς δε μπορούσε να φανταστεί τότε, πόσο οι τηλεπικοινωνίες θα έμπαιναν στις ζωές μας και το πόσο θα επηρέαζαν τον τρόπο ζωής μας [5].

1.2 **Η Ιστορία του Διαδικτύου**

Μετά την εφεύρεση του ασυρμάτου έχουμε μια σειρά από εφευρέσεις στον τομέα των τηλεπικοινωνιών όπως το ραδιόφωνο, την τηλεόραση, τον ηλεκτρονικό υπολογιστή, το κινητό τηλέφωνο, τις δορυφορικές επικοινωνίες κλπ. Όλες αυτές οι ανακαλύψεις συνέβαλαν αρκετά στην ανάπτυξη του πολιτισμού, καθώς η επικοινωνία μεταξύ των

ανθρώπων σε κάθε σημείο του πλανήτη βελτιώθηκε, καθώς μπορούσαν πλέον να ανταλλάξουν ιδέες και να αλληλοεπηρεαστούν σε πολλούς τομείς, όπως στον τομέα της τέχνης, των γραμμάτων, της επιστήμης και της τεχνολογίας.

Εικόνα 3 Ηλεκτρονικές συσκευές[6]

Οι άνθρωποι διαθέτοντας όλα αυτά τα νέα τεχνολογικά μέσα και με την κατασκευή του πρώτου προσωπικού ηλεκτρονικού υπολογιστή (Personal Computer - PC) το 1981 από την IBM [7], ήρθαν σε επαφή με μία νέα μορφή επικοινωνίας που είναι ευρέως γνωστή ως “διαδίκτυο”.

Το διαδίκτυο ή Internet όπως συνηθίζεται να το λέμε, είναι ένα παγκόσμιο επικοινωνιακό δίκτυο διασύνδεσης υπολογιστών, που έχει σκοπό την ανταλλαγή δεδομένων μεταξύ οποιουδήποτε ηλεκτρονικού υπολογιστικού συστήματος με δυνατότητα διασύνδεσης σε αυτό ενσύρματα ή ασύρματα.

Οι πρώτες προσπάθειες για την κατασκευή ενός επικοινωνιακού δικτύου έγιναν στις ΗΠΑ την περίοδο του ‘‘ψυχρού πολέμου’’. Οι Αμερικάνοι, με τον φόβο μιας ενδεχόμενης πυρηνικής επίθεσης από τους Ρώσους που είχαν ήδη στείλει στο διάστημα τον δορυφόρο ‘‘Σπούτνικ 1’’, δημιούργησαν την υπηρεσία προηγμένων αμυντικών ερευνών ‘‘ARPA’’ (Advanced Research Project Agency), που πλέον στις μέρες είναι γνωστή και ως ‘‘DARPA’’ (Defense Advanced Research Project Agency). Κεντρικός σκοπός της υπηρεσίας αυτής ήταν

η τεχνολογική ανάπτυξη και δημιουργία ενός επικοινωνιακού δικτύου που θα μπορούσε να επιβιώσει σε μία ενδεχόμενη πυρηνική επίθεση.

Έτσι δημιουργήθηκε το πρώτο είδος διαδικτύου γνωστό ως ARPANET το οποίο στηρίχθηκε σε τρείς θεωρίες. Η πρώτη θεωρία υποστήριξε την ύπαρξη ενός κοινού δικτύου διασυνδεμένων υπολογιστών, οι οποίοι θα είχαν τη δυνατότητα να ανταλλάξουν γρήγορα πληροφορίες και προγράμματα. Το άλλο πρόβλημα που προέκυψε ήταν θέμα ασφάλειας του δικτύου, αν δηλαδή ένας υπολογιστής δεχόταν επίθεση, να υπάρχει μία δικλείδα ασφαλείας ώστε να είναι δυνατή η επικοινωνία του με τους υπόλοιπους υπολογιστές του δικτύου.

Η λύση σε αυτό το πρόβλημα δόθηκε από τον Paul Baran που χρησιμοποιώντας ψηφιακή τεχνολογία σχεδίασε ένα κατανεμημένο δίκτυο επικοινωνίας. Τέλος σημαντικό ρόλο συνετέλεσε και η θεωρία ανταλλαγής πακέτων του Leonard Kleinrock, που υποστήριζε πως τα πακέτα πληροφοριών που θα περιείχαν την προέλευση και τον προορισμό τους θα μπορούσαν να σταλούν από τον ένα υπολογιστή στον άλλο.

Βασιζόμενο στις παραπάνω θεωρίες το 1969 εγκαταστάθηκε και λειτούργησε για πρώτη φορά το ARPANET μέσω του οποίου με 4 κόμβους και 4 μίνι υπολογιστές διασυνδέθηκαν τέσσερα Πανεπιστήμια. Έτσι επιτεύχθηκε η πρώτη dial-up σύνδεση μέσω τηλεφωνικών γραμμών με ταχύτητα που έφτανε τα 50 kbps. Τρία χρόνια αργότερα, δηλαδή το 1972, οι χρήστες του ARPANET είχαν φτάσει τους 23, όπου εφαρμόστηκε και για πρώτη φορά το σύστημα διαχείρισης ηλεκτρονικού ταχυδρομείου (e-mail).

Το πρωτόκολλο που χρησιμοποιούσε το ARPANET ήταν το NCP (Network Control Protocol), το μεγάλο του μειονέκτημα όμως ήταν, ότι λειτουργούσε μόνο με συγκεκριμένους τύπους υπολογιστών.

Η παράλληλη δημιουργία και άλλων δικτύων που χρησιμοποιούσαν διαφορετικά πρωτόκολλα και συνδέονταν με το ARPANET προκάλεσε την ανάγκη δημιουργίας ενός πρωτοκόλλου που θα ένωνε όλα τα δίκτυα που είχαν δημιουργηθεί μέχρι τότε.

Έτσι προέκυψε λοιπόν το πρωτόκολλο TCP (Transmission Control Protocol) όπου αργότερα το 1978 προστέθηκε και το Internet Protocol, έγινε δηλαδή TCP/IP και το 1983 εδραιώθηκε ως το μοναδικό πρωτόκολλο που χρησιμοποιούσε το ARPANET.

Το 1984 υλοποιείται ένα σύστημα στο οποίο καταγράφονται 1000 κεντρικοί κόμβοι, όπου οι υπολογιστές του διαδικτύου αναγνωρίζονται από διευθύνσεις κωδικοποιημένων αριθμών, το οποίο ήταν το DNS (Domain Name System).

Λίγο αργότερα - το 1989 - το Εθνικό Ίδρυμα Επιστημών (National science Foundation, NSF) των ΗΠΑ δημιούργησε την πρώτη πανεπιστημιακή ραχοκοκαλιά (backbone), το NSFNet. Έπειτα ενσωματώθηκαν κι άλλα σημαντικά δίκτυα όπως το Usenet, Fidonet και το Bitnet, οπότε για οποιοδήποτε δίκτυο που χρησιμοποιούσε το πρωτόκολλο TCP/IP το συνέδεσαν με τον όρο Διαδίκτυο (Internet).

Εικόνα 4 Παγκόσμια Δικτύωση Ψηφιακών Συσκευών [10]

Βέβαια, η τεράστια ανάπτυξη του Διαδικτύου ήρθε όταν το 1989 στο ερευνητικό ίδρυμα CERN ο Τιμ Μπέρνερς – Λι εφάρμοσε την υπηρεσία του ‘‘Παγκόσμιου Ιστού’’ (World Wide Web) όπου είναι ουσιαστικά μία πλατφόρμα, που κάνει πιο εύκολη την αναζήτηση πληροφοριών κάθε είδους και είναι στη μορφή που το γνωρίζουμε μέχρι και σήμερα [8].

Έτσι, με τον όρο “Παγκόσμιο Δίκτυο” εννοούμε ένα δίκτυο συνδεδεμένων υπολογιστών και άλλων ψηφιακών σήμερα συσκευών (netbooks, tablets, κινητών τηλεφώνων κα) σε παγκόσμια κλίμακα, το οποίο χρησιμοποιεί συγκεκριμένη ομάδα πρωτοκόλλων

επικοινωνίας, όπως είναι το http (HyperText Tranfer Protocol), το TCP/IP (Transfer Control Protocol/Internet Protocol), το FTP (File Transfer Protocol), κα.

Πιο συγκεκριμένα, στο Παγκόσμιο δίκτυο ανήκει μεγάλος αριθμός από υπο-δίκτυα με υπολογιστές και άλλες ψηφιακές συσκευές συνδεμένες σε τοπικό επίπεδο και όλα αυτά είναι διασυνδεμένα μεταξύ τους ενσύρματα ή ασύρματα (ακόμη και μέσω δορυφόρων).

Σε επόμενα κεφάλαια θα γίνει περαιτέρω ανάλυση των δικτύων αυτών βάση τον τρόπο διασύνδεσής τους και τα χαρακτηριστικά τους [9].

1.3 Σύγχρονες Μορφές Επικοινωνίας

Η ραγδαία εξέλιξη της τεχνολογίας επηρέασε σημαντικά και τον τομέα των τηλεπικοινωνιών. Με τη χρήση των υπολογιστών και του Διαδικτύου ο τρόπος επικοινωνίας έχει αλλάξει εντελώς σε σχέση με παλαιότερα, που όπως έχει ήδη αναφερθεί υπήρχαν πολλά προβλήματα ιδιαίτερα όταν υπήρχε ο παράγοντας απόσταση. Πλέον τα προβλήματα αυτά έχουν εξαλειφθεί αφού με την χρήση των νέων μέσων επικοινωνίας έχουν εκμηδενιστεί χρόνοι και αποστάσεις.

Μία από τις πιο γνωστές μορφές επικοινωνίας του Διαδικτύου είναι το ηλεκτρονικό ταχυδρομείο ή ‘‘e-mail’’, όπου μπορούμε να στείλουμε μήνυμα και να φτάσει στον παραλήπτη μόλις σε λίγα δευτερόλεπτα, όσο μακριά και αν βρίσκεται, γνωρίζοντας μόνο την ηλεκτρονική του διεύθυνση. Έτσι όταν ο παραλήπτης ελέγξει το λογαριασμό του e-mail του βλέπει το μήνυμα και μπορεί να απαντήσει άμεσα. Μία άλλη πιο διευρυμένη ασύγχρονη επικοινωνία είναι οι ομάδες ανοιχτών συζητήσεων τα γνωστά σε όλους ‘‘forums’’, όπου μας δίνεται η δυνατότητα επικοινωνίας με ανθρώπους απ’ όλο τον κόσμο, ώστε να συζητήσουμε για οποιοδήποτε θέμα μας ενδιαφέρει.

Πέρα από τις μορφές αυτές υπάρχει και η συνομιλία σε πραγματικό χρόνο το γνωστό ‘‘chat’’, όπου θεωρείται σύγχρονη μορφή επικοινωνίας, καθώς τα άτομα που βρίσκονται την ίδια στιγμή μπροστά στον υπολογιστή τους ανταλλάσουν μηνύματα, ή και να

πραγματοποιήσουν τηλεδιάσκεψη, αν υπάρχει η δυνατότητα αυτή, με τη χρήση μικροφώνου και κάμερας [10].

Η τεχνολογική εξέλιξη έφερε στο φως νέες ηλεκτρονικές υπηρεσίες, οι οποίες ενσωματώνουν πολλές από τις παραπάνω μορφές επικοινωνίας. Αυτές οι υπηρεσίες είναι διαδικτυακοί τόποι που παρέχουν τη δυνατότητα στους χρήστες της παραγωγής και της δημοσίευσης προσωπικού περιεχομένου. Πρόκειται για τα ‘‘Μέσα Κοινωνικής Δικτύωσης’’.

Τα Μέσα Κοινωνικής Δικτύωσης παρέχουν διάφορες υπηρεσίες στους χρήστες με στόχο την καλύτερη επικοινωνία μεταξύ τους. Οι υπηρεσίες αυτές στην πλειοψηφία τους έχουν σκοπό το διαμοιρασμό οποιασδήποτε πληροφορίας μεταξύ των χρηστών, κάνοντας ψηφιακούς φίλους με τους οποίους επικοινωνούν με ποικίλους τρόπους, ανταλλάσουν ψηφιακό περιεχόμενο οποιασδήποτε μορφής, όπως εικόνες, μουσική, βίντεο, ακόμα και διαδικτυακούς συνδέσμους.

Εικόνα 5 Μέσα Κοινωνικής Δικτύωσης [13]

Προφανώς, ότι ισχύει σε κάθε είδος ηλεκτρονικής επικοινωνίας, έτσι και στα Μέσα Κοινωνικής Δικτύωσης, η γνώση στοιχειωδών κανόνων ασφαλείας και η ανάπτυξη κριτικής

σκέψης παίζει μεγάλο ρόλο στην προστασία μας από τη διαφύλαξη των προσωπικών μας δεδομένων και από κακόβουλες επιθέσεις από άλλους χρήστες, ώστε να μπορέσουμε να εκμεταλλευτούμε στο έπακρο τις δυνατότητες επικοινωνίας και ψυχαγωγίας που μας παρέχουν [14].

Μία άλλη συσκευή που έχει αλλάξει ριζικά τον τρόπο επικοινωνίας μας είναι ένας απόγονος του ‘‘τηλεφώνου του Graham Bell’’, το κινητό τηλέφωνο . Ονομάζεται κινητό, διότι δεν εξαρτάται από τη φυσική καλωδιακή σύνδεση στο δίκτυο παροχής τηλεφωνίας, αλλά ούτε εξαρτάται και από κάποια τοπική ασύρματη συσκευή εκπομπής ραδιοφωνικού σήματος χαμηλής συχνότητας. Τα κινητά τηλέφωνα χρησιμοποιούν τεχνολογία κυψελών (cells) όπου εκπέμπουν σε υψηλές συχνότητες.

Βέβαια η κεραία του κινητού τηλεφώνου εξαρτάται πάντα από άλλες κεραίες (των τηλεπικοινωνιακών εταιριών) για να λειτουργήσει και να μεταβιβάσει τα σήματα με τη βοήθεια των ηλεκτρομαγνητικών κυμάτων.

Στην αρχή της δεκαετίας του ’90 τα κινητά τηλέφωνα γνωρίζουν μεγάλη άνθιση με την ψηφιοποίηση δικτύων και συσκευών. Στις αρχικές τους εκδόσεις ήταν μεγάλα και βαριά και σήμερα σε πιο εξελιγμένες εκδόσεις είναι πολύ πιο μικρά και ελαφριά. Με την αναβάθμιση των δικτύων τους τα κινητά τηλέφωνα δεύτερης γενιάς παρείχαν και άλλες ευκολίες, όπως η αποστολή και λήψη σύντομων γραπτών μηνυμάτων (SMS). Αργότερα προστέθηκε η δυνατότητα αποστολής και λήψης φωτογραφιών και γενικότερα στα κινητά τηλέφωνα τρίτης γενιάς ενσωματώθηκε η δυνατότητα χρήσης των πολυμέσων [10].

Εικόνα 6 Smartphones [11]

Σήμερα τα περισσότερα κινητά έχουν μετονομαστεί πλέον σε “Smartphones”, δηλαδή έξυπνα τηλέφωνα. Πήραν το όνομα αυτό, διότι δεν έχουν μόνο τις δυνατότητες ενός συμβατικού κινητού τηλεφώνου αλλά και πολλών άλλων ανεξάρτητων συσκευών. Τα πρώτα έξυπνα τηλέφωνα συνδύαζαν τις λειτουργίες ενός κινητού τηλεφώνου και ενός προσωπικού ψηφιακού βοηθού (PDA).

Αργότερα προστέθηκαν κι άλλες λειτουργίες από ανεξάρτητες συσκευές, όπως η ψηφιακή φωτογραφική μηχανή, η βιντεοκάμερα τσέπης, τα φορητά media players, η δορυφορική μονάδα πλοήγησης (GPS) κ.α.

Τέλος, με τα smartphones υπάρχει η δυνατότητα σύνδεσης στο Διαδίκτυο όπου πολλοί χρήστες αξιοποιούν αυτήν τη μορφή επικοινωνίας καθώς μπορούν ανά πάσα στιγμή να επικοινωνήσουν χρησιμοποιώντας υπηρεσίες του Διαδικτύου [12].

Κεφάλαιο 2: Ενσύρματη Επικοινωνία

2.1 Εισαγωγή

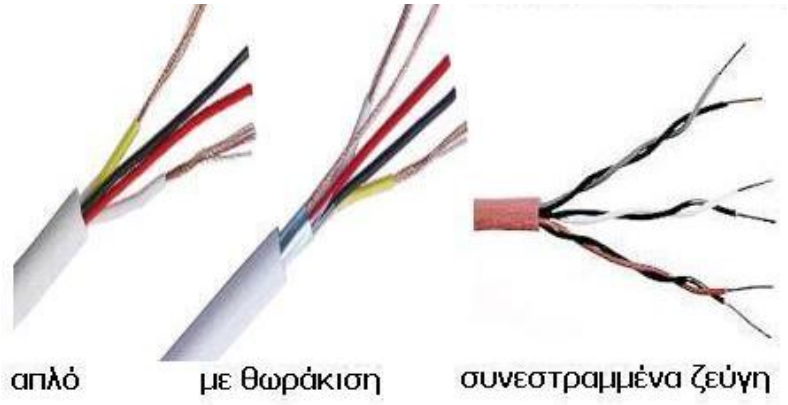
Η αναγκαιότητα της επικοινωνίας μεταξύ των ανθρώπων επηρέασε δραματικά τη ραγδαία ανάπτυξη του τομέα των τηλεπικοινωνιών. Αυτό είχε σαν αποτέλεσμα, την ανάγκη δικτύωσης στην πλειοψηφία των συσκευών που σχετίζονται με κάθε μορφή επικοινωνίας σε τοπικό αλλά και σε ευρύτερο επίπεδο. Βλέπουμε ότι στις μέρες μας σε όλους τους τομείς της κοινωνίας, όπως για παράδειγμα στην οικονομία, στην υγεία, στην παιδεία, οι εργαζόμενοι έχουν ως κύριο εφόδιο τους ηλεκτρονικούς υπολογιστές, τα κινητά τηλέφωνα, κ.α., ώστε η ανταλλαγή πληροφοριών ή η κοινή χρήση διαφόρων υπηρεσιών να γίνεται άμεσα και γρήγορα. Για να είναι εφικτό όμως αυτό, είναι απαραίτητη η εγκατάσταση κάποιας μορφής δικτύων.

Τα δίκτυα κατηγοριοποιούνται με βάση κάποια ειδικά χαρακτηριστικά τους, στα δημόσια και τα ιδιωτικά (ανάλογα με τον τρόπο πρόσβασης σε αυτά), και στα τοπικά, μητροπολιτικά, ευρείας κάλυψης και προσωπικά, όπου χωρίζονται ανάλογα με την γεωγραφική εμβέλεια που μπορούν να καλύψουν. Τέλος έχουμε τα ενσύρματα και ασύρματα, όπου η κατηγοριοποίηση γίνεται ανάλογα με το φυσικό μέσο διασύνδεσής τους [15].

Είναι προφανές ότι για να μεταδοθεί η κάθε πληροφορία από την πηγή στον προορισμό της απαιτείται κάποιο μέσο μετάδοσης που δίνει τη δυνατότητα να σταλεί το οποιοδήποτε σήμα. Τα ενσύρματα μέσα διάδοσης έβρισκαν αποκλειστική χρησιμότητα στα τηλεπικοινωνιακά δίκτυα, μέχρι να κάνουν την εμφάνιση τους τα ασύρματα μέσα μετάδοσης.

Ένα από τα πιο διαδεδομένα ενσύρματα μέσα μετάδοσης είναι το χάλκινο καλώδιο συνεστραμμένου ζεύγους (TP ή Twisted Pair). Το συναντάμε με ένα ή και περισσότερα ζεύγη που περιβάλλονται από μονωτικό υλικό και υπάρχει σε δύο μορφές, με αθωράκιστο ζεύγος (UTP ή Unshielded Twisted Pair) όπου χρησιμοποιείται κατά κόρων στα τηλεφωνικά δίκτυα και υπάρχει και με θωρακισμένο ζεύγος (STP ή Shielded Twisted Pair) όπου η

θωράκιση αυτή μας παρέχει προστασία από θορύβους και παρεμβολές . Ο τύπος UTP χωρίζεται σε κατηγορίες ανάλογα με το πόσο σφιχτό είναι το πλέξιμο των καλωδίων επειδή, όσο πιο σφιχτό είναι το πλέξιμο των καλωδίων τόσο γρηγορότερους ρυθμούς μετάδοσης και μείωση ηλεκτρικών αλληλεπιδράσεων θα υπάρχουν ανάμεσα σε κοντινά όμοια ζεύγη.

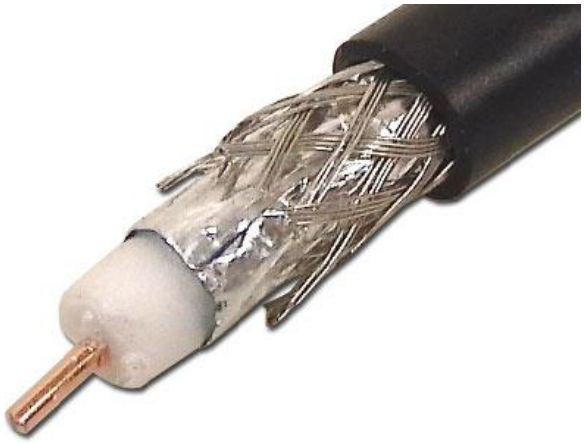


Εικόνα 7 Τύποι καλωδίων [16]

Το ομοαξονικό καλώδιο (coaxial cable) είναι ένα άλλο ενσύρματο μέσο διάδοσης. Αποτελείται από ένα εσωτερικό αγωγό περιβαλλόμενο από ένα εύκαμπτο μονωτικό στρώμα πλαστικού, το οποίο περιβάλλεται από ένα φύλλο αλουμινίου που λειτουργεί ως μόνωση και όλο αυτό περιβάλλεται από ένα συρμάτινο πλέγμα.

Με αυτό τον τρόπο ο εσωτερικός αγωγός παρουσιάζει πολύ μικρό ποσοστό θορύβου στη μετάδοση των σημάτων. Επίσης διαφέρει από τα άλλα θωρακισμένα καλώδια και χρησιμοποιείται για τη διέλευση ηλεκτρικών σημάτων μεγάλου εύρους συχνοτήτων, με αποτέλεσμα να έχουμε υψηλότερες ταχύτητες μετάδοσης από τα χάλκινα καλώδια.

Αυτός είναι ο κυριότερος λόγος που χρησιμοποιείται κυρίως στις υπεραστικές συνδέσεις του τηλεφωνικού δικτύου και στην καλωδιακή τηλεόραση.



Εικόνα 8 Ομοαξονικό καλώδιο [17]

Μία άλλη μορφή καλωδίου - η οποία πρόκειται να αντικαταστήσει στα σύγχρονα επικοινωνιακά συστήματα τις προαναφερθέντες μορφές καλωδίων - είναι η οπτική ίνα.

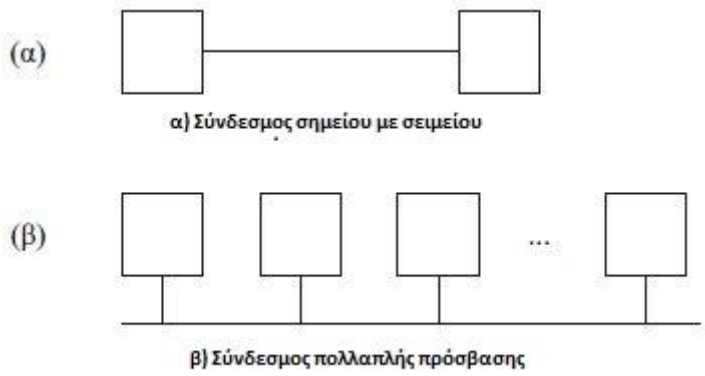
Το καλώδιο οπτικής ίνας αποτελείται από τον πυρήνα και ένα κυλινδρικό συνεχόμενο νήμα γυαλιού ή πλαστικό, απ΄ όπου γίνεται και η μετάδοση του φωτός. Ο πυρήνας περιβάλλεται από μια μονωτική επίστρωση και αυτή από ένα ειδικό προστατευτικό περίβλημα. Το καλώδιο αυτό αντί να μεταφέρει ηλεκτρική ενέργεια, μεταφέρει παλμούς φωτός. Είναι ένα πολύ καλύτερο μέσο διάδοσης, διότι το εύρος ζώνης είναι αρκετά μεγαλύτερο από των άλλων καλωδίων και δεν είναι τόσο ευαίσθητο σε παρεμβολές και θορύβους, επιτυγχάνοντας έτσι μεγαλύτερη ταχύτητα μετάδοσης δεδομένων και υψηλότερη ποιότητα, καθώς το σήμα που μεταδίδεται είναι ψηφιακό [16].

Εικόνα 9 Οπτική Ίνα [18]

2.2 Δικτύωση Η/Υ

Δίκτυο Η/Υ είναι μια ομάδα υπολογιστικών συστημάτων διασυνδεμένων μεταξύ τους με σκοπό το διαμοιρασμό πληροφοριών, εφαρμογών και περιφερειακών συσκευών. Η απλούστερη μορφή σύνδεσης ενός ενσύρματου δικτύου είναι η απευθείας σύνδεση υπολογιστών χρησιμοποιώντας ένα φυσικό μέσο όπως, καλώδιο χαλκού ή οπτικής ίνας. Το φυσικό αυτό μέσο ονομάζεται σύνδεσμος (link) και οι υπολογιστές του δικτύου ονομάζονται κόμβοι (nodes).

Υπάρχουν σύνδεσμοι σημείου με σημείο (point to point) όπου συνδέονται μόνο δύο κόμβοι και οι σύνδεσμοι πολλαπλής πρόσβασης (multiple-access) με δύο ή και περισσότερους κόμβους [16].

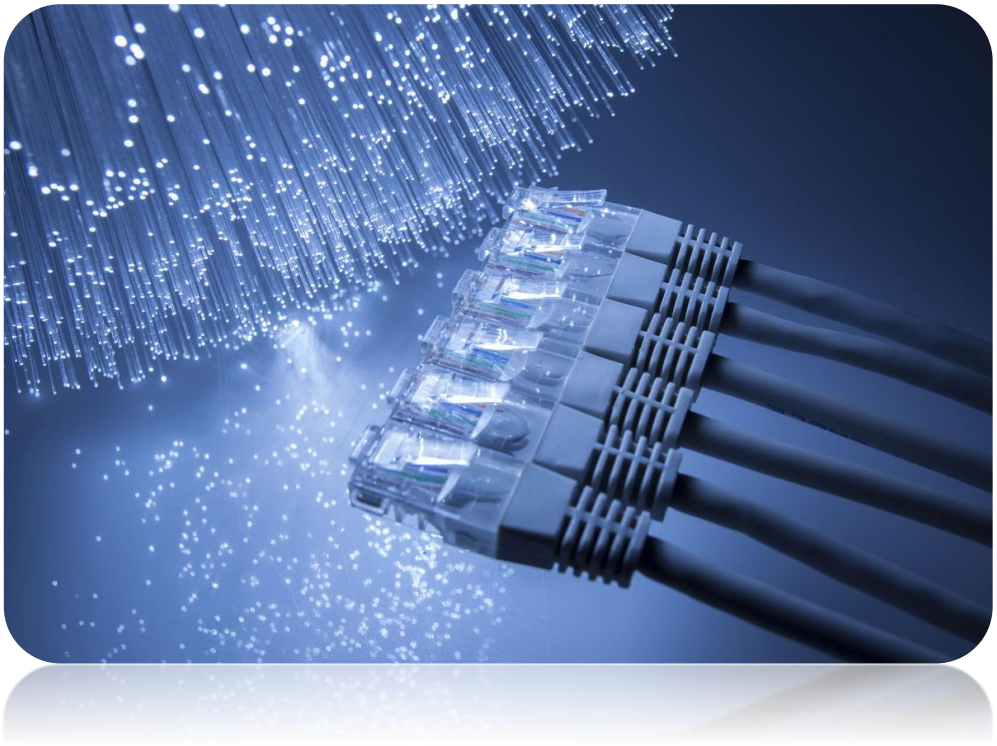


Εικόνα 10 Κόμβοι Δικτύωσης [16]

Τα ενσύρματα δίκτυα χωρίζονται σε δύο κατηγορίες, σε Δίκτυο Τοπικής Εμβέλειας (LAN – Local Area Network), και σε Δίκτυο Εκτεταμένης Εμβέλειας (WAN – Wide Area Network).

Το τοπικό δίκτυο (LAN) συντελείτε από μία μικρή ομάδα υπολογιστών, οι οποίοι είναι συνδεδεμένοι με ειδικά καλώδια δικτύου, τα γνωστά UTP (Unshielded Twisted Pair) και έχουν περιορισμένη γεωγραφική εμβέλεια λειτουργίας. Τα δίκτυα αυτά είναι ιδιωτικά και χρησιμοποιούνται κυρίως για να συνδέσουν προσωπικούς υπολογιστές με σκοπό την ανταλλαγή πληροφοριών ή την κοινή χρήση συσκευών, για παράδειγμα εκτυπωτών.

Τα κλασσικά LAN λειτουργούν συνήθως σε ταχύτητες των 10 έως 100 Mbps και παρουσιάζουν πολύ καλή πιστότητα στη μετάδοση πληροφορίας. Τα πιο προηγμένα LAN έχουν τη δυνατότητα να λειτουργήσουν σε υψηλότερες ταχύτητες καθώς έχουν βελτιωθεί τα μέσα μετάδοσής τους [16].



Εικόνα 11 Καλώδιο UTP [20]

Για την ευρύτερη ενσύρματη τοπική δικτύωση LAN χρησιμοποιείται το πρότυπο 802.3 ή Ethernet και χωρίζεται σε τρείς κατηγορίες, ανάλογα με την ταχύτητα μετάδοσης δεδομένων, και είναι οι ακόλουθες :

- Ethernet με ταχύτητα μετάδοσης 10 Mbps, όπου για τις συνδέσεις με χαλκό χρησιμοποιείται το πρότυπο 10BASE-T και για τις οπτικές ίνες το πρότυπο 10BASE-F(L).
- Fast Ethernet με ταχύτητα μετάδοσης 100 Mbps, όπου για τις συνδέσεις με χαλκό έχει επικρατήσει το πρότυπο 100BASE-TX. Το αντίστοιχο πρότυπο για τις οπτικές ίνες είναι το 100BASE-FX.

- Gigabit Ethernet με ταχύτητα μετάδοσης 1 Gbps, όπου για τις συνδέσεις με χαλκό έχει επικρατήσει το πρότυπο 1000BASE-T και το αντίστοιχο πρότυπο για τις οπτικές ίνες είναι τα 1000BASE-FX.

Τα 10Mbps του Ethernet αρκούν για το μοίρασμα μιας DSL (Digital Subscriber Line) σύνδεσης και την μεταφορά αρχείων πολυμέσων σε μικρό χρονικό διάστημα. Το Fast Ethernet προσφέρει δυνατότητες επεξεργασίας μεγάλων εφαρμογών σε μικρό χρόνο, όπως το κατέβασμα υψηλής ανάλυσης ταινιών και ταυτόχρονης επεξεργασίας αρχείων και βιντεοπαιχνιδιών.

Όσον αφορά το Gigabit Ethernet προσφέρει πολύ υψηλές ταχύτητες αλλά είναι αρκετά ακριβό. Το Νοέμβριο του 2007, αναπτύχθηκαν από την ομάδα IEEE P802.3ba Ethernet Task Force τα πρότυπα 40-100 Gigabit Ethernet (40-100 Gbps). Όπως συμβαίνει σε κάθε τεχνολογικό επίτευγμα, έτσι κι εδώ σκοπός είναι η βελτίωση και ανάπτυξη, για να επεκταθεί το 802.3 πρωτόκολλο λειτουργίας σε ταχύτητες 40 Gbps και 100 Gbps, ώστε να παρέχουν μια σημαντική αύξηση του εύρους ζώνης, διατηρώντας συνάμα τη μέγιστη συμβατότητα με το πρωτόκολλο 802.3 [1].

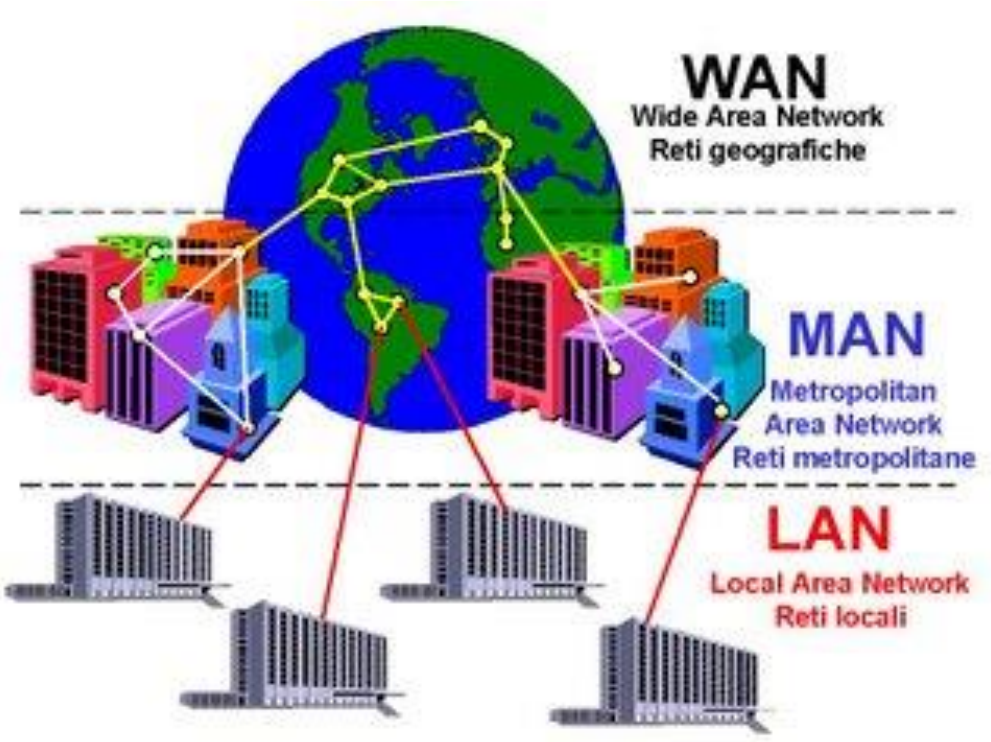
Ένα τοπικό δίκτυο αποτελείται από τον Διακομιστή (Server) και τους Πελάτες (Clients). Σαν διακομιστής χρησιμοποιείται ένας υπολογιστής ισχυρών τεχνικών χαρακτηριστικών, επειδή ουσιαστικά είναι ο εγκέφαλος του δικτύου. Πιο συγκεκριμένα, σε αυτόν είναι συνδεδεμένες όλες οι συσκευές που απαρτίζουν το εκάστοτε δίκτυο, είναι εγκατεστημένες όλες οι εφαρμογές και τα προγράμματα που χρησιμοποιούνται στο δίκτυο, όπως και είναι και αποθηκευμένα όλα τα αρχεία του δικτύου.

Ένας server συνήθως δουλεύει αδιάκοπα, ώστε να βρίσκεται ανά πάσα στιγμή στη θέση να εξυπηρετήσει τους Clients. Γι αυτό το λόγο είναι τοποθετημένος σε ένα ειδικό μεταλλικό κουτί, το Rack, το οποίο διαθέτει πολύ καλή παροχή εξαερισμού και ψύξης. Τέλος είναι συνδεδεμένος πάντα σε μια συσκευή αδιάλειπτης παροχής ρεύματος, το UPS, ώστε να είναι σε θέση να εξυπηρετήσει σε περίπτωση διακοπής ρεύματος.

Οι πελάτες είναι υπολογιστές ανεξαρτήτου ισχύος και απόδοσης και συνδέονται με τον Server για να τρέξουν προγράμματα, να μεταφέρουν αρχεία, για σύνδεση στο Διαδίκτυο και για όποιο άλλο λόγο χρειαστούν.

Το τοπικό δίκτυο LAN όπως είδαμε είναι ένα δίκτυο όπου η εμβέλεια του είναι περιορισμένη, έτσι για δικτύωση μεγαλύτερης εμβέλειας χρησιμοποιείται το Δίκτυο Ευρείας Περιοχής (WAN - Wide Area Network). Το δίκτυο αυτό έχει τη δυνατότητα να καλύψει μια αρκετά μεγάλη γεωγραφική περιοχή, όπως για παράδειγμα μια χώρα ή και ήπειρο και χρησιμοποιούνται συνήθως από μεγάλες επιχειρήσεις μέχρι και πολυεθνικές, που έχουν παραρτήματα σε διαφορετικές πόλεις ή ακόμα και σε διαφορετικές χώρες.

Στα περισσότερα WAN το κάθε υποδίκτυό τους αποτελείται από τις γραμμές μετάδοσης και τα στοιχεία μεταγωγής. Τις γραμμές μετάδοσης τις συναντάμε και ως ζεύξεις, διαύλους ή κυκλώματα, τα οποία μεταφέρουν την πληροφορία, δηλαδή τα bit μεταξύ των μηχανών.



Εικόνα 12 Τύποι Δικτύων [21]

Με τον όρο “στοιχεία μεταγωγής” εννοούμε εξειδικευμένους υπολογιστές που συνδέουν δύο ή περισσότερες γραμμές μετάδοσης. Πιο συγκεκριμένα, το στοιχείο μεταγωγής επιλέγει μια εξερχόμενη γραμμή για να προωθήσει τα δεδομένα που έχουν καταφθάσει σε μια εισερχόμενη γραμμή. Τους υπολογιστές αυτούς τους αποκαλούμε κόμβους μεταγωγής

πακέτων (packet switching nodes), κέντρα μεταγωγής δεδομένων (data switching exchanges) και ενδιάμεσα συστήματα (intermediate systems), διότι δεν υπάρχει κάποια τυποποιημένη ορολογία γι αυτούς, αν και σαν γενικότερο όρο για τους υπολογιστές μεταγωγής χρησιμοποιείται η λέξη δρομολογητής (router).

Συνοπτικά τα δίκτυα ευρείας περιοχής είναι μικρότερα επιμέρους δίκτυα, δηλαδή τοπικά, και υπολογιστές που είναι συνδεδεμένοι μεταξύ τους καλύπτοντας μία μεγάλη γεωγραφική περιοχή. Η μεταξύ τους επικοινωνία επιτυγχάνεται με τη χρήση καλωδίων υψηλών ταχυτήτων ή οπτικών ινών.

Μια υποκατηγορία των παραπάνω δικτύων είναι το MAN (Metropolitan Area Networks) ή Μητροπολιτικό Δίκτυο και αναφέρεται στο δίκτυο όπου δεν ξεπερνά τα σύνορα μιας πόλης, καλύπτοντας έτσι τις ανάγκες επικοινωνίας μέσα στην ίδια την πόλη και υπερισχύουν των τοπικών δικτύων σε σχέση με τους περιορισμούς απόστασης και ταχύτητας. Τέλος βασικό χαρακτηριστικό του MAN είναι ότι, έχει αρκετά απλοποιημένη σχεδίαση σε σχέση με τα υπόλοιπα, διότι με ένα φυσικό μέσο εκπομπής συνδέονται όλοι οι υπολογιστές του δικτύου [16].

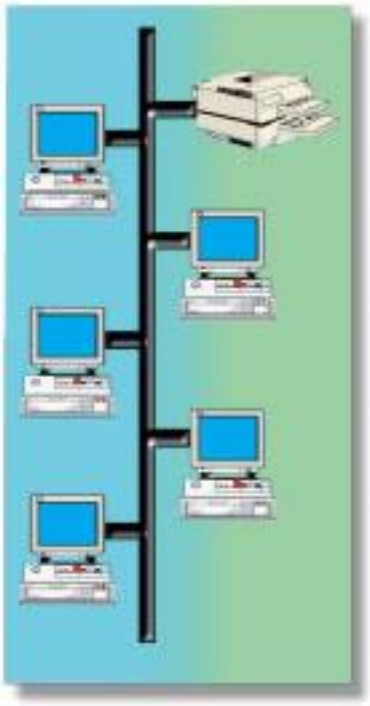
Σε όλα τα δίκτυα οι υπολογιστές και τα περιφερειακά μπορούν να συνδεθούν και να κατανεμηθούν από φυσική άποψη με διαφορετικούς τρόπους, από τους οποίους ο καθένας ονομάζεται τοπολογία δικτύου. Οι τοπολογίες είναι είτε φυσικές είτε λογικές.

Η φυσική τοπολογία του δικτύου είναι η φυσική διάταξη των κόμβων και των συνδέσμων ενός δικτύου. Αντίστοιχα, η λογική τοπολογία αποτυπώνει τον τρόπο με τον οποίο οργανώνονται οι κόμβοι του.

Η φυσική με την τοπική τοπολογία ενός δικτύου δεν ταυτίζονται πάντα. Διακρίνονται τέσσερις βασικές τοπολογίες τοπικών δικτύων, η αρτηρία, ο αστέρας, ο δακτύλιος και το δέντρο.

Στην τοπολογία αρτηρίας οι κόμβοι του δικτύου συνδέονται σε σειρά. Ένα βασικό χαρακτηριστικό αυτής της τοπολογίας είναι ότι τα μεταφερόμενα πλαίσια διασχίζουν όλο το μήκος του φυσικού μέσου και γι' αυτό λαμβάνονται απ' όλους τους κόμβους που διασυνδέονται στο τοπικό δίκτυο.

Τα πλεονεκτήματα αυτής της τοπολογίας είναι ότι είναι εύκολη στην εγκατάσταση και σχετικά φθηνή. Τα μειονεκτήματα είναι ότι αν σε ένα σημείο της αρτηρίας διακοπεί η επικοινωνία, τότε έχουμε κατάρρευση όλου του δικτύου και η βλάβη εντοπίζεται δύσκολα. Η τοπολογία αυτή εφαρμόζεται κυρίως σε τοπικά δίκτυα.



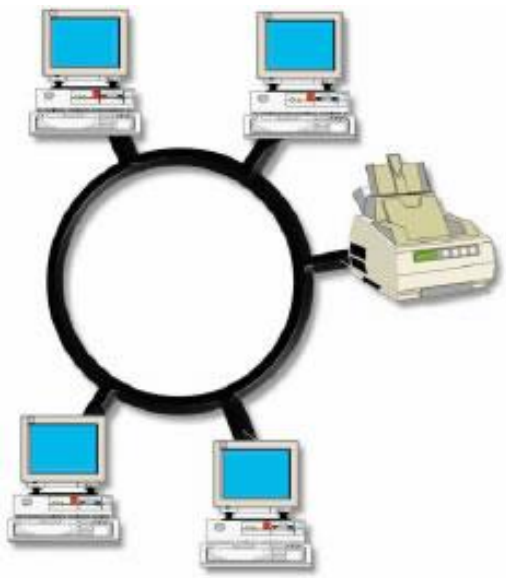
Εικόνα 13 Αρτηρία [16]

Στην τοπολογία αστέρα, όλοι οι κόμβοι του δικτύου συνδέονται απευθείας σ' ένα κεντρικό κόμβο, ο οποίος καλείται συγκεντρωτής ή ομφαλός επικοινωνίας. Αυτή η τοπολογία είναι εύκολη στην εγκατάσταση και διαχείρισή της αν εξαιρέσουμε ότι, μπορεί να εμφανιστούν κάποιες δυσχέρειες καθώς όλα τα στοιχεία πρέπει να περάσουν από τον κεντρικό κόμβο. Επίσης εύκολη είναι και η επέκταση του δικτύου καθώς απλά προστίθενται κι άλλοι κόμβοι χωρίς να χρειαστεί να σταματήσει να λειτουργεί. Το κόστος βέβαια είναι υψηλό για ένα τέτοιου είδους δίκτυο λόγο των καλωδίων και των συγκεντρωτών, αλλά το θετικό είναι πως δεν καταρρέει το δίκτυο σε περίπτωση βλάβης κάποιου κόμβου.

Εικόνα 14 (Αστέρας) [16]

Στην τοπολογία δακτυλίου, οι κόμβοι του δικτύου συνδέονται με τέτοιο τρόπο, ώστε να συνθέτουν ένα κλειστό βρόγχο. Αυτό έχει σαν αποτέλεσμα η μεταφορά δεδομένων σ' ένα δακτύλιο να γίνεται μόνο προς μία κατεύθυνση.

Αν κάποια συσκευή σταματήσει να λειτουργεί τότε καταρρέει όλο το δίκτυο και έχει και υψηλό κόστος διότι για τη δημιουργία του απαιτείται αγορά οπτικών ινών και αναλόγων καρτών δικτύου. Βέβαια, η τοπολογία αυτή χρησιμοποιείται σε δίκτυα τοπικά, αλλά και σε δίκτυα με πολλούς κόμβους, όπως ευρείας περιοχής όπου η υψηλή ταχύτητα είναι αναγκαία.



Εικόνα 15 Δακτύλιος [16]

Τέλος, μπορεί να συναντήσουμε συχνά συνδυασμό διαφορετικών τοπολογιών, όπως για παράδειγμα την τοπολογία δέντρου η οποία, συνδυάζει χαρακτηριστικά αρτηρίας και αστέρα.

Είναι μία υβριδική τοπολογία που αποτελείται από ομάδες υπολογιστών τοπολογίας αστέρα, οι οποίες με τη σειρά τους συνδέονται σε μία κεντρική αρτηρία [16].

Κεφάλαιο 3: Ασύρματη Επικοινωνία

3.1 Εισαγωγή

Η αλματώδης πρόοδος που έχει επιτευχθεί στον τομέα των τηλεπικοινωνιών και κυρίως στις ασύρματες επικοινωνίες, έχει δώσει νέες δυνατότητες στους τρόπους επικοινωνίας μας.

Μέχρι πρόσφατα, τα ενσύρματα μέσα μετάδοσης που αναφέρθηκαν και προηγουμένως, παρείχαν ικανές επιδόσεις αλλά περιόριζαν σημαντικά τη χρήση σε χώρους όπου δεν υπήρχε η κατάλληλη τηλεπικοινωνιακή υποδομή.

Έτσι έγιναν προσπάθειες ώστε να δημιουργηθούν ασύρματες ζεύξεις όπου θα επέτρεπαν στους χρήστες να συνδέονται και να ανταλλάζουν πληροφορίες χωρίς να δεσμεύονται από την ύπαρξη κάποιου φυσικού μέσου μετάδοσης.

Η ασύρματη μετάδοση προσφέρει τεράστιες δυνατότητες σε επίπεδο δικτύωσης και σε άλλες συσκευές εκτός των ηλεκτρονικών υπολογιστών.

Με τη δυνατότητα λοιπόν αυτής της ευελιξίας και με την ευκολία στην εγκατάσταση ενός ασυρμάτου δικτύου, οποιαδήποτε πλέον σύγχρονη ηλεκτρονική συσκευή μας παρέχει την δυνατότητα της ασύρματης μετάδοσης δεδομένων μέσω σύγχρονων ψηφιακών συσκευών όπως είναι για παράδειγμα τα κινητά τηλέφωνα, οι smart TVs, τα GPS, διάφορα περιφερειακά Η/Υ, κάμερες ασφαλείας, κα.

Εικόνα 16 Ασύρματη Δικτύωση [22]

3.2 Ασύρματη Δικτύωση

Ασύρματο δίκτυο καλείται ένα οποιοδήποτε τηλεπικοινωνιακό δίκτυο, το οποίο χρησιμοποιεί ραδιοκύματα ως φορείς πληροφορίας.

Η μετάδοση των δεδομένων επιτυγχάνεται μέσω ηλεκτρομαγνητικών κυμάτων με συχνότητα φέροντος, η οποία μεταβάλλεται ανάλογα από τον ρυθμό μετάδοσης δεδομένων που απαιτείται κάθε φορά από το αντίστοιχο δίκτυο. Πιο συγκεκριμένα, στα ασύρματα τοπικά δίκτυα η μετάδοση επιτυγχάνεται διαμέσου, των ραδιοφωνικών συχνοτήτων και είναι της τάξεως των 10^4 – 10^9 HZ, των μικροκυματικών συχνοτήτων με εύρος από 10^9 – 10^{12} HZ και τέλος των υπέρυθρων ακτινοβολιών που είναι από 10^{12} – 10^{14} HZ [22].

Ένα ασύρματο τοπικό δίκτυο μπορεί να είναι ήδη συνδεδεμένο σε ένα υπάρχον ενσύρματο τοπικό δίκτυο λειτουργώντας σαν επέκταση αυτού ή μπορεί να λειτουργεί και σαν ένα νέο δίκτυο. Παρόλο που τα ασύρματα δίκτυα εφαρμόζονται και σε εσωτερικούς και σε εξωτερικούς χώρους, τα ασύρματα τοπικά δίκτυα είναι ιδανικά για εσωτερικούς χώρους όπως γραφεία, ακαδημαϊκά ιδρύματα, ξενοδοχεία, νοσοκομεία κ.λ.π.

Η περιοχή όπου καλύπτει ένα ασύρματο τοπικό δίκτυο είναι η κυψέλη. Η κυψέλη είναι η περιοχή όπου λαμβάνει χώρα η ασύρματη επικοινωνία. Η περιοχή κάλυψης μιας κυψέλης εξαρτάται από την ισχύ του μεταδιδόμενου σήματος και του τύπου και της κατασκευής των τοίχων, των χωρισμάτων και άλλων φυσικών χαρακτηριστικών του εσωτερικού χώρου.

Όλοι οι ασύρματοι σταθμοί εργασίας μπορούν να μετακινούνται ελεύθερα μέσα στην κυψέλη.

Όπως αναφέραμε και σε προηγούμενο κεφάλαιο τα ενσύρματα δίκτυα κατηγοριοποιούνται ανάλογα με τον τρόπο διασύνδεσής τους ή με τη γεωγραφική κάλυψη. Το ίδιο ισχύει και με ασύρματα τοπικά δίκτυα ή WLAN (Wireless Local Area Networks), τα οποία καλύπτουν μια μικρή γεωγραφική περιοχή όπως για παράδειγμα ένα σπίτι ή ένα εργαστήριο υπολογιστών.

Υπάρχουν διάφορες τοπολογίες στα WLAN, όπου θα δούμε εκτενέστερα παρακάτω και διαφέρουν στον τρόπο με τον οποίο πραγματοποιείται η επικοινωνία. Ουσιαστικά οι συσκευές συνδέονται σε κάποιο κεντρικό διανομέα ο οποίος ονομάζεται access point χρησιμοποιώντας ασύρματες κάρτες δικτύου.

Τα ασύρματα μητροπολιτικά δίκτυα ή WMAN (Wireless Metropolitan Area Networks) αποτελούνται από την ασύρματη διασύνδεση σημείων τα οποία συνήθως απέχουν πολύ μεταξύ τους. Μερικά παραδείγματα μητροπολιτικών ασυρμάτων συνδέσεων είναι η σύνδεση δύο κτιρίων μιας εταιρείας στην ίδια πόλη ή και η διασύνδεση δύο σημείων σε διαφορετικές πόλεις. Η βασική διαφορά με τα τοπικά ασύρματα δίκτυα είναι το υλικό το οποίο χρησιμοποιείται στη διασύνδεση καθώς τυπικά η διασύνδεση γίνεται μεταξύ δύο σημείων (point to point) και η απόσταση είναι μεγαλύτερη.

Έτσι για την ασύρματη διασύνδεση δύο απομακρυσμένων σημείων θα πρέπει πιθανώς να χρησιμοποιηθεί μια κατευθυντική κεραία υψηλής ισχύος ώστε το σήμα να μην εξασθενεί και να μπορέσει να εστιάσει την ισχύ του στην απέναντι κεραία. Τα δίκτυα ευρείας περιοχής καλύπτουν πολύ μεγάλες γεωγραφικές περιοχές, για παράδειγμα, μπορούν να καλύψουν από τη σύνδεση διαφορετικών πόλεων μέχρι μιας ολόκληρης ηπείρου και μπορούν να συνδέσουν περισσότερα από ένα τοπικά δίκτυα ή και ομάδες τοπικών δικτύων.

Ο όρος ”Ασύρματα Προσωπικά Δίκτυα” (WPAN - Wireless Personal Area Networks) αναφέρεται στις σύγχρονες τεχνολογίες οι οποίες επιτρέπουν την ασύρματη διασύνδεση και επικοινωνία σε αποστάσεις λίγων μέτρων μεταξύ φορητών προσωπικών συσκευών όπως είναι τα κινητά τηλέφωνα, τα tablets κα.

Η επικοινωνία αυτή επιτρέπει στις συσκευές αυτές να παρέχουν υπηρεσίες όπως ανταλλαγή αρχείων, διαμοίραση εφαρμογών, άμεση επικοινωνία, ακόμα και διαμοιρασμό του Διαδικτύου [23].

Όπως είδαμε, τα δεδομένα μεταδίδονται μέσω ηλεκτρομαγνητικών κυμάτων και η κεραία είναι η συσκευή όπου συμβάλλει στην επίτευξη αυτού. Η μεταβαλλόμενη ηλεκτρική τάση, που μετατρέπεται σε ηλεκτρομαγνητικό κύμα, καταφθάνει στην κεραία με συγκεκριμένη συχνότητα όπου η συσκευή μετάδοσης/λήψης μεταφράζει σαν δεδομένα τα σήματα αυτά.

Τα βασικά χαρακτηριστικά μιας κεραίας είναι, κατά πόσο μπορεί να ενισχύσει το σήμα, ο τύπος της κεραίας και το εύρος της ακτινοβολίας της. Με βάση τα παραπάνω γίνεται η επιλογή της κεραίας για να καλυφθούν οι ξεχωριστές ανάγκες που έχει κάποιο ασύρματο δίκτυο.

Οι κεραίες χωρίζονται γενικότερα σε τρείς κατηγορίες με βάση τον τρόπο που ακτινοβολούν το σήμα μετάδοσής τους.

Έχουμε τις κατευθυντικές κεραίες όπου εκπέμπουν προ μία μόνο κατεύθυνση με μικρή συνήθως γωνία εκπομπής συγκεντρώνοντας την ισχύ του σήματος στη ζητούμενη κατεύθυνση. Εξαιτίας των χαρακτηριστικών αυτών χρησιμοποιούνται κυρίως για συνδέσεις point-to-point μεταξύ κτιρίων αλλά ακόμα και πόλεων.

Εικόνα 17 Κατευθυντική [26]

Υπάρχουν οι μη-κατευθυντικές κεραίες που ακτινοβολούν κυκλικά με βάση τον οριζόντιο άξονα και ενισχύουν το σήμα μειώνοντας την εκπομπή του σήματός τους στον κάθετο άξονα. Βρίσκουν εφαρμογή κυρίως σε τοπικά ασύρματα δίκτυα και σε τοπολογίες point-to-multipoint που είναι αναγκαία η κάλυψη ενός μεγάλου χώρου, όπως για παράδειγμα στον όροφο ενός κτηρίου.

Εικόνα 18

Μη-Κατευθυντική [27]

Τέλος οι κεραίες διπλής κατεύθυνσης εκπέμπουν σε γωνίες από 60 έως 120 μοίρες σε κάθε κατεύθυνση καθώς ακτινοβολούν προς δύο απέναντι κατευθύνσεις. Χρησιμοποιούνται για να καλύψουν χώρους όπως είναι διάδρομοι ή ακόμα και δρόμοι καθώς οι κεραίες αυτές, παρέχουν κάλυψη και στον κάθετο άξονα και έχουν και μεγαλύτερη ενίσχυση σήματος σε σχέση με τις μη-κατευθυντικές.

Εικόνα 19

Διπλής Κατεύθυνσης [28]

Η ενίσχυση σήματος της κάθε κεραίας που αναφερθήκαμε δηλώνει το βαθμό που μπορεί να ενισχύσει το σήμα της η κάθε κεραία προς την προτιμώμενη κατεύθυνση. Έχει μονάδα μέτρησης τα dBi. Κάποιες ενδεικτικές τιμές σε απλές εξωτερικές κεραίες είναι από 3 έως 7 dBi ενώ στις κατευθυντικές μπορεί να έχουμε και τιμές της τάξεως των 24 dBi. Ενώ η γωνία εκπομπής είναι ουσιαστικά το εύρος χώρου που καλύπτει το σήμα της κάθε κεραίας καθώς αν είμαστε εκτός της γωνίας αυτής το σήμα εκπομπής μειώνεται δραστικά. Βέβαια η ποιότητα και το εύρος κάλυψης της εκάστοτε κεραίας εξαρτάται και από τον σχεδιασμό της.

Η συσκευή εκπομπή και λήψης που έγινε αναφορά προηγουμένως είναι ουσιαστικά οι κάρτες δικτύου όπου μπορεί να έχουν εξωτερική ή ενσωματωμένη κεραία και διαφέρουν ως προς τον τρόπο διασύνδεσής τους όπως για παράδειγμα PCMCIA, PCI και USB όπως φαίνονται και στην παρακάτω εικόνα με τη σειρά που αναφέρθηκαν [25].

Εικόνα 20 Τύποι κεραιών [25]

Οι διαφορετικές συσκευές ενός ασυρμάτου δικτύου μπορούν να συνδεθούν μεταξύ τους είτε απ' ευθείας είτε με τη χρήση ενός κεντρικού διανομέα. Έτσι στα ασύρματα τοπικά δίκτυα έχουμε δύο βασικές τοπολογίες. Έχουμε τα ad-hoc όπου δε χρησιμοποιείται κεντρικός διανομέας για τη διασύνδεση των συσκευών καθώς υπάρχει άμεση επικοινωνία μεταξύ τους.

Επίσης έχουμε και την infrastructure τοπολογία όπου για τη διασύνδεση των συσκευών απαιτείται η χρήση ενός κεντρικού διανομέα (access point) ώστε να υπάρξει επικοινωνία μεταξύ των συσκευών. Να σημειωθεί βέβαια πως οι τοπολογίες που προαναφέρθηκαν στα ενσύρματα τοπικά δίκτυα ισχύουν και στα ασύρματα καθώς ακολουθείται η ίδια αρχιτεκτονική [29].

Βασική προϋπόθεση για κάθε συσκευή που χρειάζεται να συνδεθεί σε ασύρματα τοπικά δίκτυα είναι να διαθέτει ασύρματη κάρτα δικτύου που να βασίζεται στην οικογένεια προτύπων IEEE 802.11 ή όπως είναι και ευρέως γνωστή ως WiFi (Wireless Fidelity).

Η πιστοποίηση WiFi εξασφαλίζει τη σωστή επικοινωνία μεταξύ των ασύρματων συσκευών και τα διαφορετικά πρωτόκολλα που περιλαμβάνει διαφέρουν συνοπτικά, ως προς την ταχύτητα μετάδοσης δεδομένων και ως την μέγιστη απόσταση κάλυψής τους.

Το κάθε πρωτόκολλο που χρησιμοποιεί η κάθε συσκευή εξαρτάται κυρίως από την τεχνολογία της αλλά και το λόγο χρησιμότητας της. Με τις πολυχρηστικές βέβαια ηλεκτρονικές συσκευές που υπάρχουν πλέον είναι δεδομένη η υποστήριξη WiFi για την ασύρματη τοπική δικτύωση [30].

Τα παραπάνω πρωτόκολλα εκτός από τα ασύρματα τοπικά δίκτυα χρησιμοποιούνται και στα ασύρματα μητροπολιτικά δίκτυα (WMAN) με βασική διαφορά ότι στα μητροπολιτικά χρειάζεται ένας πιο ισχυρός πομποδέκτης και μια κατευθυντική κεραία υψηλής ισχύος, ώστε να μην έχουμε εξασθένηση σήματος καθώς η απόσταση εδώ τυπικά δύο σημείων είναι πολύ μεγαλύτερη από ένα τοπικό δίκτυο [29].

Με ένα παρόμοιο τρόπο όπως το WiFi λειτουργεί και η τεχνολογία ασύρματης δικτύωσης που καλείται WiMAX, αναφέρεται στα πρότυπα 802.16 και οι συνδέσεις αυτές μπορεί να είναι point-to-point ή κυψελοειδής όπως τα δίκτυα κινητής τηλεφωνίας. Παρέχουν υψηλές

ταχύτητες αλλά και πολύ μεγαλύτερη εμβέλεια, αφού έχει τη δυνατότητα κάλυψης 35 χιλιομέτρων και παραπάνω σε σχέση με τα 100 μέτρα που μπορεί να καλύψει το WiFi [31].

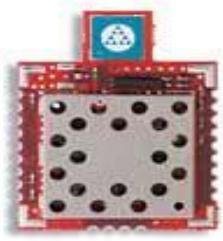
Τα ασύρματα προσωπικά δίκτυα WPAN δεν χρησιμοποιούν τα πρότυπα του WiFi αλλά ένα πρότυπο το οποίο ονομάζεται Bluetooth και χρησιμοποιείται για τη σύνδεση και επικοινωνία συσκευών με εμβέλεια περίπου 10 μέτρα. Χρησιμοποιεί την ίδια ραδιοσυχνότητα με το WiFi, δηλαδή τα 2.4 GHz αλλά χρησιμοποιεί πολύ μικρότερη ισχύ και χαμηλές ταχύτητες, ώστε να έχει χαμηλή κατανάλωση ρεύματος.

Έτσι, με το Bluetooth μπορούμε να συνδέσουμε το κινητό μας τηλέφωνο με το αυτοκίνητό μας (αν υπάρχει αυτή η δυνατότητα), επίσης επιτρέπει την επικοινωνία, σε πληκτρολόγια και ποντίκια Η/Υ που το υποστηρίζουν αλλά και σε οποιαδήποτε ηλεκτρονική συσκευή που διαθέτει πομποδέκτη τεχνολογίας Bluetooth (εικόνα 17) [25].

Εικόνα 21 Bluetooth Chip [25]

Τέλος, μία άλλη τεχνολογία που χρησιμοποιείται για τη χρήση ασύρματων προσωπικών δικτύων είναι η ZigBee η οποία χρησιμοποιείται για επικοινωνία ασύρματων συσκευών πολύ μικρού μεγέθους, κόστους και ισχύος και αναφέρεται στο πρότυπο IEEE 802.15.4.

Σκοπός αυτού του προτύπου είναι η αντικατάσταση του Bluetooth καθώς οι συσκευές που χρησιμοποιούν πομποδέκτη ZigBee (εικόνα 18) είναι αρκετά πιο φθηνές και έχουν και μεγαλύτερη ζωή μπαταρίας σε σχέση με τις Bluetooth [25].

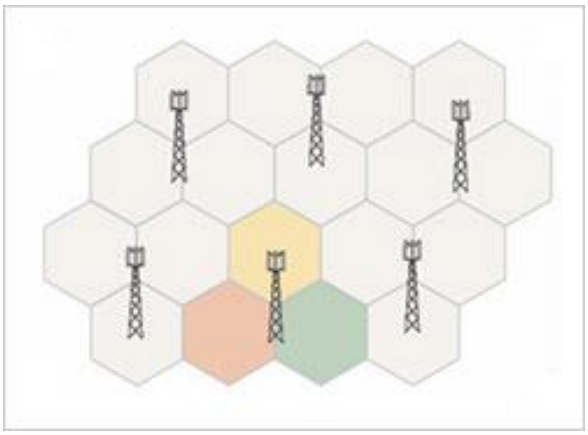


Εικόνα 22 (ZigBee Chip) [25]

Ένας άλλος τρόπος ασύρματης επικοινωνίας είναι τα κινητά τηλέφωνα που όπως ήδη έχουμε δει χρησιμοποιούν κυψελοειδή τεχνολογία. Το GSM είναι ένα ευρωπαϊκό σύστημα, που αργότερα υιοθετήθηκε και από άλλες χώρες εκτός Ευρώπης το οποίο, καθορίζει τις ζώνες εκπομπής συχνοτήτων αλλά και τα πρότυπα για τη μετάδοση του τηλεπικοινωνιακού σήματος κινητής τηλεφωνίας.

Η λειτουργία του GSM βασίζεται σε διαδοχικές όμοιες κεραίες οι οποίες ονομάζονται σταθμοί βάσης. Η διάταξη των βάσεων δημιουργεί περιοχές όπου η κάθε μία καλύπτεται από ένα σταθμό βάσης , δηλαδή κυψελοειδές σύστημα (εικόνα 19).

Οι εφαπτόμενες κυψέλες έχουν διαφορετικές συχνότητες για αποφυγή παρεμβολών. Ένα σημαντικό χαρακτηριστικό αυτών των συστημάτων είναι η μεταβαλλόμενη ισχύς, ώστε η επικοινωνία να γίνεται με επαρκές σήμα αλλά όχι απαραίτητα με υψηλή ισχύ που θα μπορούσε να προκαλέσει παρεμβολές σε γειτονικές κυψέλες.



Εικόνα 23 Κυψέλη [32]

Το GSM δίκτυο στη χώρα μας χρησιμοποιεί δύο ζώνες συχνοτήτων, με κεντρική τα 900 MHz και τα 1800 MHz . Έπειτα δημιουργήθηκε το δίκτυο 3^{ης} γενιάς (3G), το οποίο στηρίζεται στο επικοινωνιακό πρωτόκολλο UMTS με συχνότητα εκπομπής στα 2000 MHz και υποστηρίζει τη μετάδοση εικόνας και δορυφορική σύνδεση [33].

Πρόσφατα στη χώρα μας είναι διαθέσιμο και το δίκτυο LTE που είναι ο προάγγελος του δικτύου 4^{ης} γενιάς και είναι η εξέλιξη του UMTS.

Έτσι εκτός από τα πλεονεκτήματα των προκατόχων του με το LTE έχουμε τη δυνατότητα μετάδοσης εικόνας και βίντεο υψηλής ανάλυσης (HD) και γενικότερα πολύ υψηλή μετάδοση δεδομένων. Το δίκτυο LTE στην Ευρώπη λειτουργεί στα 800 MHz, 1.8 και 2.6 GHz [34].

Κεφάλαιο 4: Θέματα Ασφαλείας

4.1 Εισαγωγή

Ένα ζήτημα πολύ βασικό για τους τομείς της επικοινωνίας και ειδικότερα της δικτύωσης είναι το θέμα της ασφάλειας, αφού η ραγδαία τεχνολογική εξέλιξη των ηλεκτρονικών συσκευών που σχετίζονται αλλά και το Διαδίκτυο, αποτελούν πλέον αναπόσπαστα κομμάτια της καθημερινότητας της εποχής.

Η ασφάλεια σε κάθε είδους δικτύωση, αν αποδοθεί στην αγγλική γλώσσα θα δούμε ότι είναι μία πολυσήμαντη έννοια που περικλείει δύο όρους οι οποίοι είναι ‘‘security’’ και ‘‘safety’’. Με τον όρο ‘‘security’’ αναφερόμαστε στην ασφάλεια από ιούς, hackers και γενικότερα στην ασφάλεια του λογισμικού, ενώ με τον όρο ‘‘safety’’ αναφερόμαστε κυρίως το πόσο ασφαλείς είμαστε εμείς οι ίδιοι στους διάφορους κινδύνους όπως είναι, η προστασία της ιδιωτικής μας ζωής, οι απάτες μέσω του Internet κ.α..

Έτσι σε αυτό το κεφάλαιο θα γίνει μία εκτενείς αναφορά και διαχωρισμός αυτών των δύο όρων καθώς και πώς μπορεί ο κάθε χρήστης να προστατευτεί από τις απειλές αυτές [35].

4.2 Ασφάλεια και Διαδίκτυο

Όπως προλογίστηκε η έννοια του όρου ‘‘security’’ περιλαμβάνει διάφορες μορφές κακόβουλων επιθέσεων που μπορούν να επηρεάσουν το λογισμικό ή το εκάστοτε πρόγραμμα που έχουν στόχο.

Οι επιθέσεις αυτές προϋποθέτουν την ύπαρξη κακόβουλου λογισμικού (malicious software/malware software) όπου διαχωρίζεται σε δύο κατηγορίες, σε ιομορφικό λογισμικό, όπου περιλαμβάνει τα προγράμματα που έχουν τη δυνατότητα να αναπαραχθούν από μόνα τους, και μη ιομορφικό λογισμικό, όπου τα προγράμματα αναπαράγονται μόνο με την ανάμειξη του ανθρώπινου παράγοντα.

Μία ομάδα κακόβουλων προγραμμάτων που ανήκει στην κατηγορία των ιομορφικών λογισμικών ονομάζονται Ιοί καθώς είναι προγράμματα τα οποία, στόχος τους είναι να μολύνουν άλλα προγράμματα τροποποιώντας τα και είναι σχεδιασμένοι για να εκμεταλλεύονται τις αδυναμίες των άλλων προγραμμάτων.

Η μόνη διαφοροποίησή των ιών από τα «υγιή» προγράμματα είναι ότι, ενσωματώνονται σε αυτά και εκτελούνται κρυφά κατά τη διάρκεια της εκτέλεσης των προγραμμάτων-φορέων, εκτελώντας οποιαδήποτε λειτουργία είναι προγραμματισμένα.

Κάποιοι από τους βασικότερους τύπους ιών είναι οι εξής:

- **Παρασιτικοί** (parasitic), είναι από τους πιο διαδεδομένους τύπους, οι οποίοι προσαρτώνται σε εκτελέσιμα αρχεία (.exe) και αναπαράγονται κατά την εκτέλεση του μολυσμένου προγράμματος και επεκτείνονται και σε άλλα εκτελέσιμα αρχεία μολύνοντάς τα.
- **Παραμένοντες στη μνήμη** (memory-resident) , οι οποίοι εγκαθίστανται στην κύρια μνήμη του συστήματος και παραμένουν εκεί. Φαίνονται ως τμήματα προγραμμάτων και αναπαράγονται από τη στιγμή της εγκατάστασής τους καθώς μολύνουν κάθε πρόγραμμα που εκτελείται.
- **Τομέα εκκίνησης** (boot) και μολύνουν τον τομέα εκκίνησης του σκληρού δίσκου όπου είναι εγκατεστημένο το λειτουργικό σύστημα.
- **Δυσανιχνεύσιμοι** (stealth) που είναι ειδικά σχεδιασμένοι ώστε να μην ανιχνεύονται από τα ειδικά αντιβιοτικά λογισμικά.
- **Πολυμορφικοί** (polymorphic) οι οποίοι έχουν τη δυνατότητα να αλλάζουν την υπογραφή τους με κάθε μόλυνση καθιστώντας αδύνατη την ανίχνευσή τους μέσω αυτής.
- **Μακρο-ιοί** (macro-virus), θεωρούνται ιδιαίτερα επικίνδυνοι καθώς μολύνουν αρχεία κειμένου και όχι εκτελέσιμα προγράμματα, έτσι κάθε πλατφόρμα υλικού και λειτουργικό σύστημα που υποστηρίζει ‘‘Word’’ μπορεί να μολυνθεί. Μία συνηθισμένη μέθοδος διάδοσής τους είναι το ηλεκτρονικό ταχυδρομείο γι αυτό και η πλειοψηφία των κρουσμάτων ανήκει σε αυτή την κατηγορία.

Όπως διαπιστώνεται η καλύτερη λύση απέναντι στους ιούς θα ήταν με κάποιο τρόπο να μην μπορούσαν να εισαχθούν στο σύστημα, κάτι τέτοιο όμως είναι αδύνατο οπότε η καλύτερη αντιμετώπισή τους είναι η πρόληψη που μπορεί να μειώσει τις επιτυχείς επιθέσεις των ιών.

Έτσι οι επόμενες καλύτερες επιλογές που έχουμε είναι η ανίχνευση, δηλαδή να διαπιστωθεί η μόλυνση και να εντοπιστεί ο ιός, έπειτα αναγνώριση, δηλαδή να αναγνωριστεί ο συγκεκριμένος ιός που έχει μολύνει το σύστημα, αφού έχει γίνει η ανίχνευση και τέλος απομάκρυνση, όπου απομακρύνονται όλα τα ίχνη του ιού από το μολυσμένο πρόγραμμα, όπου αποκαθιστάται στην αρχική του κατάσταση, βέβαια απομακρύνεται και από όλα τα μολυσμένα συστήματα ώστε να προληφθεί τυχών εξάπλωσή του.

Όλες αυτές οι ενέργειες εκτελούνται από ειδικά λογισμικά, τα αντιβιοτικά, τα οποία με το πέρας του χρόνου εξελίσσονται σε πολυπλοκότητα καθώς το ίδιο ισχύει και για τους ιούς.

Έτσι τα λογισμικά προστασίας ή αντιβιοτικά διακρίνονται σε τέσσερις γενιές.

Στην πρώτη γενιά ανήκουν οι απλοί σαρωτές, στην δεύτερη οι ευρεστικοί σαρωτές, στην τρίτη οι παγίδες δραστηριότητας και στην τέταρτη η πλήρης προστασία.

Τα λογισμικά τέταρτης γενιάς περιλαμβάνουν τεχνικές των προηγούμενων γενεών αλλά επιπλέον παρέχουν και έλεγχο προσπέλασης όπου περιορίζει την ικανότητα των ιών να μολύνουν ένα σύστημα και να τροποποιήσει τυχών αρχεία.

Εικόνα 24 Μέρη Προγραμμάτων[40]

Πέρα από τα ιομορφικά λογισμικά που είδαμε, έχουμε και τη κατηγορία των μη ιομορφικών κακόβουλων λογισμικών. Τέτοιου είδους λογισμικά είναι οι λογικές βόμβες (logic bombs), οι κερκόπορτες (trapdoors), οι Δούριοι Ίπποι (Trojan Horses), τα βακτήρια (bacteria) και οι έλικες (worms).

Μία από τις παλιότερες μορφές κακόβουλου λογισμικού είναι η λογική βόμβα ή logic bomb, όπου είναι ένας κώδικας, ενσωματωμένος σε κάποια νόμιμη εφαρμογή, που είναι ρυθμισμένος να εκτελεστεί όταν εκπληρωθούν κάποιες προϋποθέσεις.

Η κερκόπορτα ή trapdoor είναι ένα μυστικό σημείο εισόδου ενός προγράμματος που επιτρέπει σε όποιον τη γνωρίζει να αποκτήσει δικαιώματα προσπέλασης στο σύστημα, παρακάμπτοντας τις συνήθεις διαδικασίες ελέγχου προσπέλασης.

Αν και χρησιμοποιήθηκαν αρχικά από τους προγραμματιστές για την εκσφαλμάτωση (debugging) και δοκιμή των προγραμμάτων, δηλαδή χρησιμοποιούνταν ως δικλείδες ασφαλείας, στην περίπτωση εκμετάλλευσής τους όμως από κακόβουλους

προγραμματιστές μεταβάλλονται σε απειλές αφού μπορούν να έχουν μη εξουσιοδοτημένη πρόσβαση στο σύστημα. Έτσι καθώς είναι δύσκολο να ελεγχθεί τέτοιου είδους απειλή , με την ανάπτυξη και συντήρηση του λογισμικού μπορούμε να αντιμετωπίσουμε τέτοιες απειλές.

Ο Δούρειος Ίππος (Trojan Horse) είναι ένα πρόγραμμα το οποίο περιέχει κρυμμένο κώδικα που όταν εκτελεστεί έχουμε κάποια ανεπιθύμητη ή επιβλαβή λειτουργία. Για παράδειγμα, μπορεί να αλλάξει τις παραμέτρους προστασίας των αρχείων ενός χρήστη έτσι ώστε τα αρχεία να είναι αναγνώσιμα απ όλους, να αποκαλύψει κωδικούς πρόσβασης του χρήστη ή ακόμα και να καταστρέψει σιωπηλά αρχεία του χρήστη.

Τα βακτήρια (bacteria) είναι προγράμματα που δεν καταστρέφουν εμφανώς αρχεία, αλλά έχουν μοναδικό σκοπό να πολλαπλασιάζονται εκθετικά με αποτέλεσμα να καταλαμβάνουν όλη τη χωρητικότητα του επεξεργαστή, της μνήμης ή του δίσκου, στερώντας ωφέλιμους πόρους του συστήματος από τους χρήστες.

Οι έλικες (worms), όπως είναι γνωστοί, εξαπλώνονται από σύστημα σε σύστημα μέσω δικτυακών συνδέσεων και με το που ενεργοποιείται μπορεί να συμπεριφερθεί ως ιός ως βακτήριο ακόμα και εισάγει Trojan Horses ώστε να εκτελεστή μία κακόβουλη ενέργεια. Μπορεί να μεταδοθεί μέσω της υπηρεσίας του ηλεκτρονικού ταχυδρομείου, ταχυδρομώντας ένα αντίγραφο του εαυτού του σε άλλα συστήματα. Μεταδίδεται με την υπηρεσία από απόσταση εκτέλεσης, δηλαδή εκτελεί ένα αντίγραφο του εαυτού του σε κάποιο άλλο σύστημα. Τέλος μεταδίδεται μέσω της υπηρεσίας από απόσταση σύνδεσης, όπου σε αυτή την περίπτωση ο έλικας έχει τη δυνατότητα να συνδεθεί με ένα απομακρυσμένο σύστημα ως χρήστης και με τη βοήθεια εντολών να αντιγράφει τον εαυτό του από το ένα σύστημα στο άλλο. Τέλος έχουν τα ίδια χαρακτηριστικά με τους ιούς, δηλαδή μια φάση ύπνωσης, μια φάση διάδοσης, μια φάση ενεργοποίησης και μια φάση εκτέλεσης [36].

Ένα πολύ μεγάλο ποσοστό των ηλεκτρονικών μηνυμάτων που διακινούνται στο Διαδίκτυο είναι ανεπιθύμητα ή spam, όπως συνηθίζεται να τα ακούμε. Τα spam αν και συχνά μεταφέρουν κακόβουλο λογισμικό, συνηθέστερη περίπτωση είναι να εμπεριέχουν μηνύματα σχετικά με πορνογραφία, φαρμακευτικά προϊόντα, αμφιλεγόμενες οικονομικές συναλλαγές αλλά και πολλά άλλα.

Οι εμπλεκόμενοι τέτοιων δραστηριοτήτων εδρεύουν συνήθως σε χώρες όπου δεν υπάρχει κατάλληλη νομοθεσία έτσι δρουν ελεύθερα. Το μεγάλο αυτό ποσοστό των spam οφείλεται στην αλόγιστη έκθεση της ηλεκτρονικής μας διεύθυνσης στο Διαδίκτυο μέσω διαφόρων ιστοτόπων όπως, τσατ, φόρουμ, από τις διάφορες υπηρεσίες των μέσων κοινωνικής δικτύωσης ακόμα και από τη συμπλήρωση κάποιας ηλεκτρονικής φόρμας.

Λόγο του μεγάλου αριθμού ηλεκτρονικών μηνυμάτων που διακινούνται καθημερινά στο Διαδίκτυο υπάρχει και μεγάλος κίνδυνος να δεχθούμε κάποια επίθεση μέσω του ηλεκτρονικού ταχυδρομείου.

Έτσι ένα άλλο είδος τέτοιας απάτης ονομάζεται ransomware, όπου το θύμα δέχεται ένα ηλεκτρονικό μήνυμα το οποίο μόλις το ανοίξει ξεκινάει μία διαδικασία κρυπτογράφησης των αρχείων που είναι αποθηκευμένα στον υπολογιστή του και κλειδώνονται. Οι δράστες εξηγούν στο θύμα ότι πρέπει να καταβάλει ένα χρηματικό ποσό ώστε να του αποσταλεί ο κωδικός πρόσβασης για την ανάκτηση των αρχείων.

Πρόκειται ουσιαστικά για μία ηλεκτρονική απαγωγή των αρχείων μας και γενικότερα τέτοιου είδους απάτες είναι γνωστές με τον όρο scam. Για την καταπολέμησή τους, ο κάθε πάροχος προσφέρει κάποιες επιλογές στους χρήστες του για να μπορεί να προστατευτεί με τα φίλτρα spam αλλά υπάρχει και η επιπλέον δυνατότητα να προσαρμόσει ο κάθε χρήστης τη συμπεριφορά του φίλτρου ανεπιθύμητης αλληλογραφίας αλλά πλέον υπάρχει ενσωματωμένη η προστασία αυτή και στα πλήρη πακέτα των αντιβιοτικών λογισμικών. Έτσι πρέπει να δίνεται ιδιαίτερη προσοχή στο άνοιγμα κάθε μηνύματος που δεν γνωρίζουμε τον αποστολέα ή δεν μας δίνονται επαρκή στοιχεία από το θέμα του μηνύματος [37].

Ένα άλλο είδος προστασίας ανεπιθύμητων ενεργειών είναι το τείχος προστασίας ή firewall και χρησιμοποιείται για να δηλώσει με ποια πόρτα του δικτύου επικοινωνεί ένα πρόγραμμα ή μία συσκευή έτσι ώστε να επιτρέπει ή να απορρίπτει την επικοινωνία στο διαδίκτυο ή με κάποια άλλη δικτυωμένη συσκευή. Προϋπόθεση για την αντιμετώπιση και πρόληψη των δικτυακών επιθέσεων είναι η σωστή ρύθμιση του firewall από τον εκάστοτε χρήστη.

Βέβαια για τη σωστή ρύθμιση ο διαχειριστής κάθε δικτύου θα πρέπει να έχει μία ολοκληρωμένη εικόνα του δικτύου του αλλά και των απαιτήσεών του, έτσι ώστε να μπορεί

να πράξει αναλόγως για καθετί που ζητάει επικοινωνία στο δίκτυο. Όλα αυτά προφανώς απαιτούν από το διαχειριστή να διαθέτει πολύ καλές γνώσεις πάνω στα δίκτυα των υπολογιστών πράγμα που δεν ισχύει δυστυχώς για ένα μεγάλο αριθμό χρηστών, διότι αφήνουν τα firewall στις προτεινόμενες ρυθμίσεις, καθιστώντας έτσι το δίκτυο ευάλωτο σε επιθέσεις από εξωτερικούς χρήστες, καθώς το κάθε δίκτυο έχει διαφορετικές απαιτήσεις προστασίας. Πλέον τα τείχη προστασίας έχουν ενσωματωθεί στα σύγχρονα ολοκληρωμένα πακέτα αντιβιοτικών, αλλά υπάρχουν και σαν αυτόνομα λογισμικά τα οποία έχουν τη δυνατότητα συνεργασίας με άλλα λογισμικά προστασίας [38].

Εικόνα 25 Firewall [41]

Όπως προαναφέρθηκε στην κατηγορία των μη ιομορφικών λογισμικών, τα προγράμματα αναπαράγονται μόνο με την ανάμειξη του ανθρώπινου παράγοντα.

Οι χρήστες που εμπλέκονται σε τέτοιες δραστηριότητες ονομάζονται hackers, οι οποίοι είναι έμπειροι χειριστές υπολογιστών με κατάλληλες γνώσεις αλλά και ικανότητες, όπου εισέρχονται σε ξένα υπολογιστικά συστήματα χωρίς άδεια χρήσης, έχοντας σκοπό να αποκαλύψουν τις αδυναμίες ασφαλείας χωρίς να υπάρχει πρόθεση για πρόκληση κάποιας ζημιάς στο σύστημα.

Αυτή είναι και η διαφοροποίησή τους από τους crackers, οι οποίοι έχουν και αυτοί σκοπό την παράνομη πρόσβαση σε ένα σύστημα και στα δεδομένα του, αλλά απώτερος σκοπός τους είναι να προκαλέσουν κάποια οικονομική ή κάποιου άλλου είδους ζημιά και την κλοπή πληροφοριών.

Επίσης δραστηριοποιούνται είτε μόνοι τους είτε σε ομάδες και κατηγοριοποιούνται σύμφωνα με τον τρόπο δράσης τους αλλά και το λόγο για τον οποίο δρουν. Κατά καιρούς οι ενέργειες τους έχουν δημιουργήσει πρόβλημα σε πολλούς τομείς (κοινωνικό, πολιτικό, οικονομικό, επιχειρησιακό). Κάθε συμβατικός χρήστης οφείλει να κάνει κάποιες απαραίτητες ενέργειες ώστε να θωρακίσει την ασφάλεια του συστήματός του και είναι η εγκατάσταση, ενός antivirus, ενός τοίχου προστασίας, προγράμματος anti-spam και ενημέρωση του λειτουργικού συστήματος σε πιθανές βελτιώσεις του [39].

Ένας άλλος κίνδυνος που παραμονεύει στο διαδίκτυο ονομάζεται pharming, που έχει σκοπό να παραπλανεί το χρήστη πιστεύοντας ότι σερφάρει σε μια γνήσια ιστοσελίδα με το σωστό URL, αλλά στην πραγματικότητα έχει παραπεμφθεί σε μία ψεύτικη. Ο απώτερος σκοπός των δραστών είναι η οικονομική εξαπάτηση, καθώς εκτρέπουν τη ροή των επισκεπτών σε άλλο ιστοχώρο, όπου τα στοιχεία από οποιαδήποτε συναλλαγή καταχωρούνται.

Μία άλλη παρόμοια μορφή παραπλάνησης είναι και το phising, όπου ο χρήστης παραπλανάται δίνοντας προσωπικές πληροφορίες συμπληρώνοντας μία ψεύτικη φόρμα στο Διαδίκτυο. Έτσι θα επιτρέψει σε έναν cracker να υποκλέψει ή να πλαστογραφήσει τα στοιχεία του υποψήφιου θύματος και να κερδίσει παράνομη πρόσβαση σε δεδομένα όπως, προσωπικούς λογαριασμούς, e-mail, κωδικούς PIN, ή οποιοδήποτε άλλο δεδομένα θελήσει.

Άλλη μορφή phising είναι και το spear phising, όπου είναι στοχευμένα μηνύματα τα οποία μπορούν να θεωρηθούν αυθεντικά από μια ομάδα ανθρώπων. Για παράδειγμα οι υπάλληλοι μιας εταιρίας δέχονται μήνυμα με φαινομενικό αποστολέα τον εργοδότη τους και τους ζητούνται όνομα χρήστη και κωδικό πρόσβασης αποσπώντας έτσι οι δράστες πολύτιμες πληροφορίες και συχνά απόρρητες. Κάτι παρόμοιο συμβαίνει και στις ιστοσελίδες κοινωνικής δικτύωσης και ονομάζεται social networking phising. Μία άλλη εκδοχή του phising είναι και το vishing, στην οποία για να γίνει πειστικότερος ο δράστης,

δίνεται στο θύμα ένας τηλεφωνικός αριθμός εξυπηρέτησης ή ζητείται το δικό του τηλέφωνο, ώστε να υπάρξει επικοινωνία. Άλλες μορφές είναι το spoofing, όπου ένα άτομο ή πρόγραμμα αποκτά πρόσβαση σε δεδομένα τρίτων χρησιμοποιώντας πλαστά στοιχεία [37].

Στην αρχή του κεφαλαίου έγινε μία αναφορά στους αγγλικούς όρους ‘‘security’’ και ‘‘safety’’, όπου έγινε ανάλυση του πρώτου όρου και είδαμε τους κινδύνους που κρύβει το Διαδίκτυο μέσω των κακόβουλων επιθέσεων και τρόπους προστασίας των υπολογιστικών μας συστημάτων.

Όσον αφορά τον όρο safety, όπου εννοούμε την ασφάλεια της ιδιωτικής μας ζωής, θα δούμε τους τρόπους που μπορεί να εκτεθούμε στο Διαδίκτυο όπως και τι πρέπει να προσέξουμε ώστε να αποφύγουμε κακόβουλές επιθέσεις που αφορούν την προσωπική μας ζωή. Οι περισσότεροι χρήστες θεωρούν τον κόσμο του Διαδικτύου ακίνδυνο καθώς δεν είναι κάτι απτό οπότε διαφέρει από τον πραγματικό κόσμο, ενώ στην ουσία αν και εικονικός κόσμος είναι πολύ πιο επικίνδυνος, καθώς μας δίνεται η δυνατότητα να ξεπεράσουμε τα όρια της πόλης που ζούμε και να «ταξιδέψουμε», να αγοράσουμε και να επικοινωνήσουμε με όλο τον κόσμο. Έτσι οι χρήστες δρουν πολλές φορές απερίσκεπτα καθώς μπορεί να δώσουν πληροφορίες για τη ζωή τους, τη διεύθυνση του σπιτιού τους, ακόμα και να λογομαχήσουν με κάποιο άγνωστο χωρίς να σκέφτονται πως η κάθε κίνησή τους στο Διαδίκτυο αφήνει ίχνη.

Τα cookies είναι οι υπαίτιοι για τα ίχνη που αφήνει ο κάθε χρήστης αφού πρόκειται για μικρά αρχεία που δημιουργούνται αυτόματα στον σκληρό δίσκο κάθε συστήματος χωρίς την έγκρισή μας όταν επισκεπτόμαστε κάποιες ιστοσελίδες. Έτσι εάν επισκεφτούμε ξανά κάποια άλλη στιγμή μία ιστοσελίδα μέσω του cookie θα γίνει η αναγνώρισή μας από τον διακομιστή. Τέτοιου είδους αρχεία συνήθως περιέχουν πληροφορίες όπως ποιες ιστοσελίδες επισκεφθήκαμε πόσο χρόνο αφιερώσαμε σε μία σελίδα και γενικότερα κάνουν μία σκιαγράφηση των συνηθειών μας στο Διαδίκτυο. Βέβαια υπάρχει πάντα η δυνατότητα απενεργοποίησής τους μέσω των επιλογών απορρήτου του εκάστοτε browser που χρησιμοποιούμε.

Υπάρχουν προγράμματα που εκμεταλλεύονται τα cookies αλλά και αρχεία που κατεβάζουμε από το Διαδίκτυο και ονομάζονται spywares. Ένα τέτοιο πρόγραμμα μπορεί

να προσκολληθεί κρυφά στα προαναφερθέντα και μετά να ξεκινήσει αμέσως την παρακολούθηση των δραστηριοτήτων μας. Έπειτα οι πληροφορίες που καταγράφει αποστέλλονται σε τρίτους που τις περισσότερες φορές βέβαια είναι εταιρίες που ξεκινούν να μας στέλνουν διαφημιστικό ή άλλο υλικό, ανάλογα με τις προτιμήσεις και τα ενδιαφέροντά μας.

Η αποθήκευση της στοχευμένης αυτής σκιαγράφησης μπορεί να αποφευχθεί με τη χρήση κατάλληλων προγραμμάτων που είναι γνωστά ως cleaners και σβήνουν τα αρχεία που δίνουν πληροφορίες και ότι άλλο μπορεί να προδώσει τις δραστηριότητές μας.

Ένας άλλος τρόπος είναι το «σερφάρισμα» μέσω proxy server όπου σημαίνει διακομιστής διαμεσολάβησης. Πρόκειται για ένα πρόγραμμα το οποίο παρεμβάλλεται μεταξύ ενός διακομιστή και του πελάτη, δηλαδή του χρήστη. Οπότε με ένα proxy server μπορούμε να κινούμαστε στο Διαδίκτυο χωρίς να συλλέγονται πληροφορίες για εμάς καθώς, για κάθε Δικτυακό τόπο που επισκεπτόμαστε φαίνεται σα να έχει γίνει επίσκεψη από τον proxy server [37].

Τέλος μία άλλη μέθοδος για να μην αφήνουμε ίχνη κατά την περιήγησή μας στο Διαδίκτυο είναι μία λειτουργία η οποία λέγεται Ιδιωτική Περιήγηση (InPrivate) και είναι διαθέσιμη σε όλους τους φυλλομετρητές ή browsers. Η λειτουργία αυτή είναι πολύ χρήσιμη κυρίως όταν χρησιμοποιούμε ένα κοινόχρηστο υπολογιστή, καθώς μας επιτρέπει να περιηγηθούμε χωρίς να αποθηκεύονται πληροφορίες σχετικές με τις σελίδες που επισκεφθήκαμε, αφού με τον τερματισμό της λειτουργίας αυτής σβήνονται αυτόματα, προσωρινά αρχεία, ιστορικό και cookies. Σε καμία περίπτωση βέβαια η ιδιωτική περιήγηση δεν μας κάνει ανώνυμους στο Διαδίκτυο, καθώς ο πάροχος ή οι σελίδες που επισκεφτήκαμε μπορούν να δουν την ηλεκτρονική μας διεύθυνση. Επίσης στην περίπτωση εγκατάστασης κάποιου κακόβουλου λογισμικού κατά τη λειτουργία αυτή παραμένουμε εκτεθειμένοι και μετά τον τερματισμό του browser [42].

Βλέπουμε ότι χρειάζεται ιδιαίτερη προσοχή κατά την περιήγησή μας στο Διαδίκτυο καθώς οι κίνδυνοι είναι πολλοί. Όμως καθώς η ανάγκη του ανθρώπου για συνεχόμενη δικτύωση ανά πάσα ώρα και μέρος γίνεται όλο και πιο επιτακτική πρέπει να δώσουμε και ιδιαίτερη προσοχή στα ασύρματα δίκτυα όπου συνδεόμαστε, καθώς είναι γνωστό πως τα ασύρματα δίκτυα υστερούν στον τομέα της ασφάλειας λόγω της φύσεώς τους.

Έτσι θα δούμε κάποιες βασικά βήματα ώστε να διαφυλάξουμε την ασφάλεια του ασυρμάτου δικτύου μας από τρίτους. Το router το οποίο εκπέμπει το σήμα του ασυρμάτου δικτύου μας είναι ο μόνος μεσάζοντας μεταξύ του συστήματός μας και του Διαδικτύου, έτσι πρέπει να ρυθμίσουμε κάποιες παραμέτρους του router, ώστε να διασφαλίσουμε ότι υπάρχει ασφάλεια στο δίκτυο μας από ανεπιθύμητους χρήστες.

Αρχικά για να συνδεθούμε με τη διαχείρηση του router μας πρέπει μέσω ενός φυλλομετρητή να πληκτρολογήσουμε τη διεύθυνση του router και μετά να πληκτρολογήσουμε ένα username κι ένα password ώστε να εισέλθουμε στο γραφικό περιβάλλον του. Καλό θα είναι μετά από αυτά τα βήματα να αλλάξουμε το default password με κάποιο της αρεσκείας μας, αφού τα περισσότερα router έχουν στάνταρ κωδικούς.

Έπειτα αλλάζουμε τον εργοστασιακό κωδικό και ορίζουμε πάλι δικό μας κωδικό όσο το δυνατόν πιο σύνθετος και ορίζουμε και ως επίπεδο κρυπτογράφησης του κωδικού ότι πιο σύγχρονο έχει στη διάθεσή του κάθε router.

Επίσης ρυθμίζουμε αργότερα και την ισχύ του εκπεμπόμενου σήματος σύμφωνα με την έκταση του χώρου που θέλουμε να εκπέμπεται το σήμα. Τέλος έχουν και τα router ειδικά φίλτρα για ασφάλεια όπου ελέγχουν την MAC ADDRESS, που είναι ουσιαστικά το όνομα της κάθε συσκευής που διαθέτει ασύρματη κάρτα δικτύου, και ρυθμίζουμε ποιες θέλουμε να έχουν πρόσβαση και ποιες όχι. Με αυτές τις ρυθμίσεις βοηθάμε στο να μειωθούν σημαντικά οι πιθανότητες παραβίασης του ασύρματου δικτύου μας [43].

Κεφάλαιο 5: Συμπεράσματα – Προτάσεις για το Μέλλον

Συμπερασματικά είδαμε πως ξεκίνησε η επικοινωνία μεταξύ των ανθρώπων, πως εξελίχθηκε μέχρι σήμερα και κατά πόσο βοήθησε η ραγδαία ανάπτυξη της τεχνολογίας. Αναλύσαμε θέματα σχετικά τόσο με την ενσύρματη όσο και την ασύρματη επικοινωνία.

Σε αυτό το σημείο θα ήταν ενδιαφέρουσα μία σύγκριση μεταξύ των δύο αυτών τρόπων επικοινωνίας συνοψίζοντας τα πλεονεκτήματα και τα μειονεκτήματά τους.

Έτσι, όπως είδαμε, η ασύρματη επικοινωνία εν αντιθέσει της ενσύρματης δεν χρησιμοποιεί ως μέσο μετάδοσης κάποιο τύπο καλωδίου και αυτό έχει σαν αποτέλεσμα η ενσύρματη σύνδεση να είναι ταχύτερη από την ασύρματη και να προσφέρει αρκετά καλύτερη απόδοση και αξιοπιστία.

Βέβαια το μεγαλύτερο μειονέκτημα της ενσύρματης τεχνολογίας είναι η απαραίτητη καλωδίωση για να επιτευχθεί σύνδεση μεταξύ των συσκευών. Το μεγαλύτερο πλεονέκτημα της ασύρματης επικοινωνίας είναι η ευελιξία που προσφέρει στο χρήστη, καθώς μπορεί να κινείται χωρίς περιορισμούς στην περιοχή εμβέλειας οποιουδήποτε δικτύου είναι συνδεδεμένος.

Επίσης με την ασύρματη τεχνολογία δεν έχουμε το κόστος που θα είχαμε για παράδειγμα σε μια μεγάλη επιχείρηση που θα χρειάζονταν αρκετά μέτρα καλωδίων για τη δικτύωση των υπολογιστών ή ακόμα και στην περίπτωση που θα χρειαζόταν μία απλή επέκταση του δικτύου.

Πέραν από το κόστος που προαναφέρθηκε, η εγκατάσταση ενός ασυρμάτου δικτύου μπορεί να γίνει εύκολα, γρήγορα και ευέλικτα, χωρίς τα προβλήματα της καλωδίωσης που απαιτείται σε αντίθετη περίπτωση. Οπότε όσον αφορά τον τομέα της ευελιξίας τα ασύρματα υπερισχύουν κατά κράτος καθώς, μπορούν να υποστηρίξουν μια μεγάλη ποικιλία τοπολογιών προκειμένου να ανταποκριθούν στις ανάγκες της κάθε περίστασης.

Οι τοπολογίες αυτές μπορούν εύκολα να αλλάξουν και περιλαμβάνουν, από απλά ισότιμα δίκτυα κατάλληλα για μικρό αριθμό χρηστών, έως πλήρως εκτεταμένα δίκτυα με

δυνατότητες περιαγωγής που μπορούν να εξυπηρετήσουν χιλιάδες χρήστες σε μεγάλες αποστάσεις.

Απ' όσα προαναφέρθηκαν ένα ασύρματο δίκτυο φαντάζει ιδανικό για κάθε περίπτωση και ανάγκη, όμως πέραν από τη μειωμένη απόδοση και την ταχύτητα, υπάρχει και μεγάλος κίνδυνος στο θέμα της ασφάλειας. Η ασφάλεια είναι ένας πολύ σημαντικός τομέας στην μετάδοση πληροφοριών-δεδομένων, αφού η μη σωστή εγκατάσταση ενός ασυρμάτου δικτύου ή δίκτυο με χαμηλή ασφάλεια το καθιστά ευάλωτο σε παρεμβολές και επιθέσεις.

Τα ασύρματα δίκτυα είναι επίσης ευάλωτα σε παρεμβολές. Εάν ένας ισχυρός αναμεταδότης που λειτουργεί στην ίδια ραδιοσυχνότητα με ένα ασύρματο δίκτυο βρίσκεται κοντά σε αυτό, τότε το δίκτυο μπορεί να καταστεί άχρηστο. Αυτό φυσικά μπορεί να γίνει και με κακόβουλη πρόθεση από κάποιον ο οποίος θέλει να εξαπολύσει μια επίθεση προς το δίκτυο.

Τα ασύρματα δίκτυα είναι ευάλωτα σε επιθέσεις από τη στιγμή που το ασύρματο μέσο είναι κοινόχρηστο. Όλοι οι ασύρματοι σταθμοί εργασίας μπορούν να «δουν» όλη την κίνηση που διασχίζει το μέσο, ακριβώς με τον ίδιο τρόπο που ισχύει στους διασυνδεδεμένους με καλώδιο σε σταθμούς εργασίας σε ένα Ethernet δίκτυο.

Εάν δεν ληφθούν κάποια μέτρα για την προστασία των δεδομένων που μεταδίδονται στο μέσο τότε αυτά μπορούν να διαβαστούν από εξωτερικούς ή εσωτερικούς κακόβουλους χρήστες. Μια πολιτική ασφαλείας είναι απαραίτητη σε κάθε εγκατάσταση ασύρματου δικτύου. Τα ασύρματα δίκτυα δεν είναι ασφαλή εξ' ορισμού. Πρέπει να ληφθεί υπόψη η ασφάλιση του δικτύου σε πολλά επίπεδα όπως, του ποιος έχει πρόσβαση στο μέσο καθώς και της παράνομης υποκλοπής δεδομένων [44].

Έπειτα από αυτές τις δύο μορφές μετάδοσης δεδομένων αναφερθήκαμε και στην ασφάλεια και προστασία τόσο των υπολογιστικών συστημάτων όσο και της προσωπικής μας ζωής από το Διαδίκτυο.

Είναι κοινή παραδοχή ότι κάποια διαδραστικά μέσα όπως το Διαδίκτυο και το κινητό τηλέφωνο αποτελούν μεγάλο κομμάτι της καθημερινότητάς μας καθώς είναι αξιοσημείωτα χρηστικά εργαλεία, επικοινωνίας, μάθησης, δημιουργίας, διασκέδασης και εργασίας.

Το λάθος βέβαια της πλειοψηφίας των χρηστών σήμερα, είναι ότι όχι μόνο δε λαμβάνουν στα σοβαρά όλους αυτούς τους κινδύνους που προαναφέρθηκαν αλλά δεν έχουν και το κατάλληλο γνωστικό υπόβαθρο πάνω στο θέμα αυτό.

Ένας ενήλικας ή γνώστης του θέματος είναι σε θέση να διακρίνει πολλούς από τους κινδύνους που κρύβει το Διαδίκτυο. Ένα παιδί όμως είναι ευάλωτο σε τέτοιου είδους κινδύνους και πολλές φορές βλέπουμε πως και οι ίδιοι οι γονείς δεν είναι τόσο επαρκής γνώστες του θέματος απ' όσο πιστεύουν, με αποτέλεσμα να πέφτει σε διάφορες παγίδες εκθέτοντας πολλές φορές τον εαυτό του άλλα και τον περίγυρό του.

Ένα άλλο πρόβλημα με την ανεξέλεγκτη χρήση του Διαδικτύου είναι και η παρενόχληση (bullying) που τη συναντάμε σε πολλές μορφές και τα παιδιά που γίνονται συνήθως αντικείμενο παρενόχλησης αντιμετωπίζουν δυσκολίες στο να υπερασπιστούν τον εαυτό τους. Τον τελευταίο καιρό έχει παρατηρηθεί αύξηση στα κρούσματα ρατσιστικών παρενοχλήσεων και πολλές φορές η έντονη παρενόχληση έχει οδηγήσει σε τρομερές συνέπειες όπως η αυτοκτονία παιδιών. Πολύ πιθανό αίτιο όλων αυτών βέβαια είναι και η αυξημένη επιρροή που ασκούν στις νεαρές ηλικίες κυρίως τα μέσα κοινωνικής δικτύωσης αλλά και η αλόγιστη χρήση τους.

Οι υπηρεσίες των μέσων κοινωνικής δικτύωσης βασίζονται στη δημιουργία προφίλ όπου καταχωρούμε προσωπικά μας δεδομένα όπως όνομα, e-mail, αλλά και ότι άλλες προαιρετικές πληροφορίες θέλουμε να δώσουμε για την προσωπική μας ζωή. Έτσι με τη δημοσιοποίηση προσωπικών δεδομένων υπάρχει πάντα ο κίνδυνος να διαβαστούν από κακόβουλους χρήστες. Γι αυτό το λόγο πρέπει να είμαστε πολύ προσεχτικοί πριν δημοσιοποιήσουμε κάποια πληροφορία για εμάς ή ακόμα και μια φωτογραφία ή βίντεο, καθώς δεν είναι λίγα τα κρούσματα παραβίασης προσωπικών δεδομένων αλλά και παραποίησης πληροφοριών [37].

Ευελπιστώ πως στο μέλλον θα αρχίσουν οι χρήστες του Διαδικτύου να το εκμεταλλεύονται ορθά, χρησιμοποιώντας το ως μία ατέρμονη πηγή πληροφόρησης, εκμάθησης αλλά και για την ψυχαγωγίας τους. Ο μόνος τρόπος για να μειωθούν δραστικά οι κακόβουλες επιθέσεις, σε υπολογιστικό αλλά και προσωπικό επίπεδο, είναι να μάθουμε να διακρίνουμε τους κινδύνους που τυχών μπορεί να συναντήσουμε.

Κάτι τέτοιο επιτυγχάνεται αν ξεκινήσουν όλοι και ενημερώνονται για τους κινδύνους που είδαμε αλλά και να υπάρχει επαρκής ενημέρωση από το σχολικό και οικογενειακό περιβάλλον, καθώς έτσι όπως εφοδιαζόμαστε για να μπορέσουμε να ανταπεξέλθουμε στις απαιτήσεις της πραγματικής ζωής έτσι πρέπει να εφοδιαστούμε και για τον πλασματικό κόσμο του Διαδικτύου καθώς έχει μεγάλο αντίκτυπο στην πραγματικότητα που ζούμε.

Έτσι αν υπάρχει παιδεία και ανεπτυγμένη κριτική σκέψη θα καταφέρουμε να έχουμε ένα ασφαλές Internet για εμάς και τα παιδιά μας που είναι το μέλλον αυτού του κόσμου.

Αναφορές

Βιβλιογραφία

[1] Ξ. Αικατερίνη, «Η τεχνολογία τοπικής δικτύωσης ethernet και οι τομείς εφαρμογής της,» [Ηλεκτρονικό]. Available: http://conta.uom.gr/conta/ekpaideysh/metaptyxiaka/technologies_diktywn/ergasies/2012/. [2012]

[2] Θ. ΓΕΩΡΓΙΟΥ, Ι. ΚΑΠΠΟΣ, Α. ΛΑΔΙΑΣ, Α. ΜΙΚΡΟΠΟΥΛΟΣ, Α. ΤΖΙΜΟΓΙΑΝΝΗΣ και Κ. ΧΑΛΚΙΑ, Πολυμέσα - Δίκτυα, ΑΘΗΝΑ: ΟΡΓΑΝΙΣΜΟΣ ΕΚΔΟΣΕΩΝ ΔΙΔΑΚΤΙΚΩΝ ΒΙΒΛΙΩΝ. [2008]

[3] «Βικιπαίδεια,» [Ηλεκτρονικό]. Available: http://el.wikipedia.org/wiki/Τηλέγραφος. [2014]

[4] «Βικιπαίδεια,» [Ηλεκτρονικό]. Available: http://el.wikipedia.org/wiki/Τηλέφωνο. [2014]

[5] [Ηλεκτρονικό]. Available: http://www.tercumeburolarimiz.com/servis/id/13. [2014]

[6] «Βικιπαίδεια,» [Ηλεκτρονικό]. Available: http://el.wikipedia.org/wiki/Γουλιέλμο_Μαρκόνι. [2014]

[7] [Ηλεκτρονικό]. Available: http://embeddedlounge.blogspot.gr/2009/11/phome-new-generation-home-phone.html. [2009]

[8] [Ηλεκτρονικό]. Available: http://el.wikipedia.org/wiki/Ιστορία_των_υπολογιστών.[2014]

[9] [Ηλεκτρονικό]. Available: http://el.wikipedia.org/wiki/Διαδίκτυο. [2014]

[10] [Ηλεκτρονικό]. Available: http://el.wikipedia.org/wiki/Παγκόσμιος_Ιστός. [2014]

[11] Τ. Ελένη, «slideshare,» [Ηλεκτρονικό]. Available: http://www.slideshare.net/elenti/ss-12735058. [2014[

[12] [Ηλεκτρονικό]. Available: http://www.gizmag.com/smartphone-comparison-2014-1/31787/. [2014]

[13] [Ηλεκτρονικό]. Available: http://el.wikipedia.org/wiki/Έξυπνο_τηλέφωνο. [2014]

[14] [Ηλεκτρονικό]. Available: http://echodiastasis.gr/τα-μέσα-κοινωνικής-δικτύωσης-και-η-δια/. [2014]

[15] Α. Τζικόπουλος, «Κέντρο Δια Βίου Μάθησης,» [Ηλεκτρονικό]. Available: kdvm.gr/Media/Default/Pdf%20enotites/3.5.pdf. [2013]

[16] «Αρχιτεκτονική Δικτύων,» [Ηλεκτρονικό]. Available: http://users.sch.gr/pepoudi/site/pages/intro.html. [2014]

[17] [Ηλεκτρονικό]. Available: http://www.computercablestore.com/1000ft_RG_6u_Dual_Shielde_PID62.aspx. [2014]

[18] [Ηλεκτρονικό]. Available: http://en.wikipedia.org/wiki/Optical_fiber. [2014]

[19] [Ηλεκτρονικό]. Available: http://ebooks.edu.gr/modules/ebook/show.php/DSGL-C127/577/3749,16441/. [2014]

[20] [Ηλεκτρονικό]. Available: http://www.bandwidthplace.com/wp-content/uploads/2013/05/ethernet.jpg. [2013]

[21] [Ηλεκτρονικό]. Available: http://worldinfo4u.com/wp-content/uploads/2014/01/lan-man-wan.jpg. [2014]

[22] «Ασύρματα Δίκτυα,» [Ηλεκτρονικό]. Available: isa.teipir.gr/files/projects/wireless_nets.ppt. [2014]

[23] [Ηλεκτρονικό].Available:http://conta.uom.gr/conta/ekpaideysh/metaptyxiaka/technologies_diktywn/teaching_m/WirelessNetworks-Web/TOC.html#TOC. [2014]

[24] [Ηλεκτρονικό]. Available:

http://2.bp.blogspot.com/-Z91adkKL8Bc/Tz5vch8WiOI/AAAAAAAAD2I/LiVPfnWbMw8/s1600/Nirkabel.jpg. [2014]

[25] [Ηλεκτρονικό]. Available: de.teikav.edu.gr/telematics/pdf/3o_Meros_Asyrmata_thlematikh.pdf. [2007]

[26] [Ηλεκτρονικό].Available:
http://i01.i.aliimg.com/photo/v0/109358947/Antenna_5_8GHz_directional_Grid_24dBi.jpg. [2014]

[27] [Ηλεκτρονικό]. Available: www.signifimobile.ca. [2014]

[28] [Ηλεκτρονικό]. Available: http://www.inbuildingprojects.com/wp-content/uploads/2010/11/

bi-directional-antenna.jpg. [2014]

[29] [Ηλεκτρονικό]. Available: http://users.sch.gr/angnikolou/tech_v/wireless.htm. [2014]

[30] «ΒΙΚΙΠΑΙΔΕΙΑ,» [Ηλεκτρονικό]. Available: http://el.wikipedia.org/wiki/IEEE_802.11. [2014]

[31] «ΒΙΚΙΠΑΙΔΕΙΑ,» [Ηλεκτρονικό]. Available: http://el.wikipedia.org/wiki/WiMAX. [2014]

[32] [Ηλεκτρονικό].Available:
http://www.vodafone.gr/portal/resources/media/AboutUs/CorporateResponsibility/keraies.jpg. [2014]

[33] «ΒΙΚΙΠΑΙΔΕΙΑ,»[Ηλεκτρονικό].Available:
http://el.wikipedia.org/wiki/Global_System_for_Mobile_Communications. [2014]

[34] «ΒΙΚΙΠΑΙΔΕΙΑ,» [Ηλεκτρονικό]. Available: http://el.wikipedia.org/wiki/LTE. [2014]

[35] [Ηλεκτρονικό]. Available: http://www.chiosjobs.gr/car031008-deltio2.asp. [2012]

[36] Σ. ΚΑΤΣΙΚΑΣ, ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ, ΕΛΛΗΝΙΚΟ ΑΝΟΙΧΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ, 2001. [2001]

[37] [Ηλεκτρονικό]. Available: http://www.saferinternet.org. [2008]

[38] «Βικιπαίδεια,» [Ηλεκτρονικό]. Available: http://el.wikipedia.org/wiki/Firewall. [2014]

[39] «Βικιπαίδεια,» [Ηλεκτρονικό]. Available: http://el.wikipedia.org/wiki/Χάκερ. [2014]

[40] [Ηλεκτρονικό]. Available: http://galleryhip.com/virus-malware.html. [2014.]

[41] [Ηλεκτρονικό]. Available: http://www.thewindowsclub.com. [2014]

[42] «Ορθή και Ασφαλής Χρήση των Νέων Τεχνολογιών,» [Ηλεκτρονικό].
Available: http://plinet.kas.sch.gr/saferinternet/index.php/asfaleia-se-asyrmata-diktya-wi-fi. [2014]

[43] «Πλήρης οδηγός για πλήρη ασφάλεια του ασύρματου δικτύου σας,» [Ηλεκτρονικό].
Available: http://www.pcsteps.gr/575-how-to-guide-wireless-network-security/. [2010]

[44] « Δίκτυα-Ενσύρματα και Ασύρματα,» [Ηλεκτρονικό]. Available: www.moec.gov.cy. [2014]