ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ
ΜΕΣΟΛΟΓΓΙΟΥ

ΤΜΗΜΑ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΚΑΙ ΔΙΚΤΥΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

‘ Θ Ε Μ Α ’

ΑΡΧΕΣ ΛΕΙΤΟΥΡΓΙΑΣ, ΕΦΑΡΜΟΓΕΣ ΚΑΙ ΠΡΟΣΟΜΟΙΩΣΗ ΣΥΣΤΗΜΑΤΟΣ ΕΠΙΚΟΙΝΩΝΙΑΣ ΚΟΝΤΙΝΗΣ ΕΜΒΕΛΕΙΑΣ (NFC)

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:

Δρ.Παρασκευάς Μιχάλης

Επίκουρος Καθηγητής Τμήματος ΤΕΣΥΔ ΤΕΙ Μεσολογγίου

ΦΟΙΤΗΤΡΙΑ:

Ζησιμοπούλου Ιωάννα

ΕΥΧΑΡΙΣΤΙΕΣ

Κλείνοντας την σύντομη περίληψη θα ήθελα να ευχαριστήσω τους γονείς μου που με στήριξαν, τον άντρα μου Γιάννη και τα παιδιά μου Παναγιώτη και Χρήστο, που ανέχτηκαν τις ατέλειωτες ώρες απουσίας μου. Ιδιαίτερα θα ήθελα να ευχαριστήσω τον Επίκουρο Καθηγητή κ. Παρασκευά Μιχάλη, επιβλέποντα Καθηγητή της πτυχιακής μου εργασίας, για την άριστη συνεργασία μας και την πολύτιμη βοήθεια του. Φυσικά δεν θα παραλείψω να ευχαριστήσω όλους τους καθηγητές του τμήματος Τηλεπικοινωνιακών Συστημάτων και Δικτύων που επιβράβευσαν την προσπάθεια μου.

Πίνακας περιεχομένων

ΠΕΡΙΛΗΨΗ

Η συγκεκριμένη εργασία σαν κύριο στόχο έχει την λεπτομερή περιγραφή της νέας αυτής τεχνολογίας σε επίπεδο συστήματος και εφαρμογών, εστιάζοντας ταυτόχρονα σε τέσσερα κύρια σημεία: εφαρμογές, ιδιωτικότητα, ασφάλεια, σύγκριση με υπάρχοντα ασύρματα συστήματα Η προσομοίωση του συστήματος καθώς και η λειτουργία του θα πραγματοποιηθεί σε περιβάλλον Matlab Simulink.

Συγκεκριμένα, γίνεται μία σύντομη εισαγωγή η οποία περιλαμβάνει τις βασικές έννοιες, τα ιδιαίτερα χαρακτηριστικά και τον τρόπο λειτουργίας των συστημάτων NFC καθώς και τις εφαρμογές που μπορεί να υλοποιήσει η τεχνολογία.

Κατόπιν, αναλύονται τα τμήματα ενός NFC συστήματος, οι οργανισμοί και τα πρότυπα αναγνώρισης της NFC τεχνολογίας και η εφαρμογή αυτής στην καθημερινότητα μας.

Ακολούθως, περιγράφονται θέματα ασφάλειας και ιδιωτικότητας των συστημάτων και τα θέματα ασφάλειας και υγείας των χρηστών, καθώς και οι πιθανές μελλοντικές χρήσεις της τεχνολογίας NFC. Στο τελευταίο μέρος της εργασίας υπάρχει η προσομοίωση ενός τέτοιου συστήματος σε Matlab Simulink.

Λέξεις Κλειδιά: Ασύρματα Δίκτυα, Αναγνώριση Ραδιοσυχνότητας Επικοινωνία Κοντινού Πεδίου, Έξυπνες Κάρτες, Ενεργητικές Και Παθητικές Ετικέτες, 13,56 MHz, 106 Kbit/s – 424 Kbit/s, ISO 14443, Διαμόρφωση Μετατόπισης Πλάτους.

ABSTRACT

This report has as main objective the detailed description of this new technology in both systemic and applications level, while focusing on four main areas: applications, comparison with existing wireless networks, privacy and security. Specifically, there is a brief introduction which includes basic concepts, characteristics and operation of NFC systems and applications that can be implemented by the technology.

Then, follows the analyzing of the parts of a NFC system, the agencies and the standards for the recognition of NFC technology as well as its implementation in the supply chain and in our daily lives.

Next, are described subjects of security and privacy of systems, and subjects of health and the user's safety, as also the possible future uses of the NFC technology In the last part of this work the simulation of such a system in Matlab Simulink is included.

Keywords: Wireless Networks, RFID (Radio-Frequency IDentification), NFC (Near Field Communications), Smarts Cards, Active and Passive Tags, 13,56, 106 Kbit/s – 424 Kbit/s, ISO 14443, A S K(Amplitude Shift Keying)

ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ

ΠΙΝΑΚΑΣ ΓΡΑΦΗΜΑΤΩΝ

ΑΚΡΟΝΥΜΙΑ

3G 3rd generation of mobile telecommunications technology

3GPP 3rd Generation Partnership Project

ASIC application-specific integrated circuit

ASK Amplitude Shift Keying

BER Bit Error Rate

CPU central processing unit

ETSI European Telecommunications Standards Institute

FSK Frequency-shift keying

GSM Global System for Mobile

GSMA GSM Association

HF High frequency

I2C Inter-Integrated Circuit

ID IDentification

IEEE Institute of Electrical and Electronics Engineers

ISO International Organization for Standardization

LF Low Frequency

LLCP Logical Link Control Protocol

MNOS Mobile Network Operators

NFCIP Near Field Communication Interface and Protocol

NDEF NFC Data Exchange Format

NFC Near Field Communication

OQPSK Offset Quadrature Phase-shift Keying

PCF Point Coordination Faction

PDAs Personal digital assistant

PSK Phase Shift Keying

QPSK Quadrature Phase Shift Keying

RF Radio Frequency

RFID Radio Frequency

RTD Record Type Definition

SE Secure Element

SER Symbol Error Rate

SIM Subscriber Identity Module

SNEP Simple NDEF Exchange Protocol

SNR Signal to Noise Ratio

TETRA Terrestrial Trunked Radio

UART Universal Mobile Telecommunications System

UHF Ultra-High Frequency

UMTS Uniform Subscriber Identify

URI Uniform Resource Identifier

URL Uniform Resource Locator

USIM Universal Subscriber Identity

WIFI Wireless Fidelity

WLAN Wireless Local Area Network

ΚΕΦΑΛΑΙΟ 1

1. ΕΙΣΑΓΩΓΗ

1.1 Πρόλογος

Το NFC είναι μια μορφή του RFID, σύστημα ασύρματης αναγνώρισης που αντικατέστησε το σύστημα οπτικής αναγνώρισης Bar Code, αλλά έχει ένα συγκεκριμένο σύνολο προτύπων που διέπουν τη λειτουργία του, interfaces, κλπ. Αυτό σημαίνει ότι ο NFC εξοπλισμός, και τα στοιχεία από διάφορους κατασκευαστές μπορούν να χρησιμοποιηθούν μαζί. Τα NFC πρότυπα δεν καθορίζουν μόνο το λειτουργικό περιβάλλον των εφαρμογών αλλά και τις μορφές δεδομένων και τις ταχύτητες μεταφοράς δεδομένων.

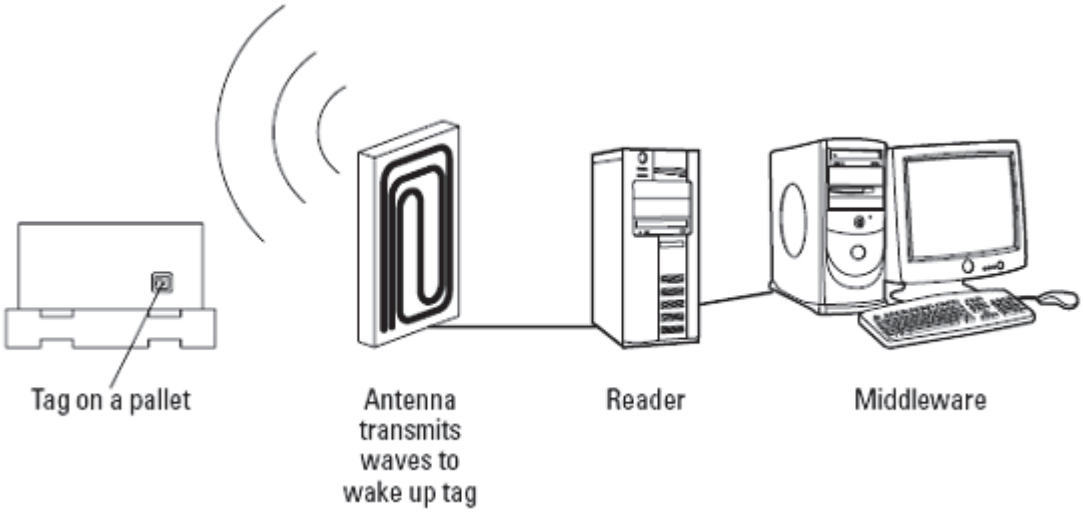
Ο όρος RFID προέρχεται από τα αρχικά των λέξεων **Radio Frequency IDentification**, δηλαδή «**ταυτοποίηση μέσω ραδιοσυχνοτήτων**». Η αναγνώριση μέσω ραδιοσυχνοτήτων είναι μία μέθοδος αναγνώρισης που στηρίζεται στην αποθήκευση και εξ' αποστάσεως ανάκτηση δεδομένων από ειδικά καρτελάκια, τα οποία διαθέτουν μηχανισμούς ραδιοεντοπισμού.

Σε ένα βασικό σύστημα NFC, απαιτούνται τέσσερα βασικά συστατικά για να επιτευχθεί η μετάδοση των δεδομένων:

- Ο transponder (που καλείται και απλά tag - ετικέτα) το οποίο προγραμματίζεται με πληροφορία που το αναγνωρίζει μοναδικά, καθορίζοντας έτσι το concept του "automatic identification".
- Ο transceiver (που καλείται κυρίως και reader - αναγνώστης) που χειρίζεται τη ραδιοεπικοινωνία μεταξύ των κεραιών και περνά την πληροφορία της ετικέτας στον εξωτερικό κόσμο.
- Μία κεραία που προσκολλάται στον αναγνώστη για να επικοινωνεί με τις ετικέτες.
- Το reader interface layer, ή αλλιώς middleware, το οποίο συμπιέζει χιλιάδες σήματα ετικετών σε μια συγκεκριμένη αναγνώριση και επίσης,δρα σαν κανάλι μεταφοράς μεταξύ των στοιχείων NFC hardware και των συστημάτων

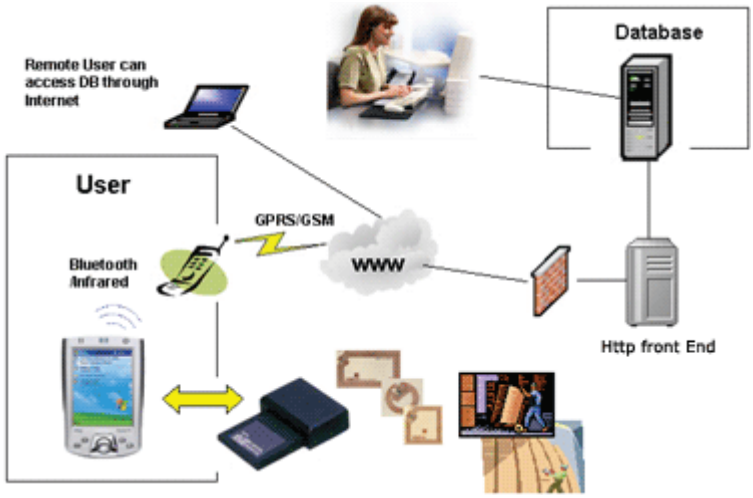
software της εφαρμογής του πελάτη, όπως το απόθεμα, η παραλαβή και τα logistics.

Η επόμενη εικόνα δείχνει τα βασικά του πώς ένα απλό σύστημα N F C λειτουργεί και τα τέσσερα κύρια συστατικά του συστήματος αυτού.[1]



Εικόνα 1:Τα κύρια συστατικά του R F I D

RFID και NFC προσφέρουν τους τρόπους να προσδιοριστούν ηλεκτρονικά οι άνθρωποι, οι θέσεις και τα πράγματα. Τα συγκροτήματα ηλεκτρονικών υπολογιστών μπορούν να ξέρουν το χώρο των πραγμάτων στον πραγματικό κόσμο, όπου συλλέγονται πληροφορίες: όπως από που είναι, το πώς χρησιμοποιούνται και εάν χρειάζονται προσοχή. Αυτές οι τεχνολογίες μειώνουν τις δαπάνες της συλλογής πληροφοριών και βελτιώνουν την ακρίβειά της. Μπορούν να βοηθήσουν να αυτοματοποιηθούν οι διαδικασίες που εξαρτώνται σήμερα από το μολύβι και το χαρτί ή τη χειρωνακτική εισαγωγή δεδομένων.[2]



Εικόνα 2:Λειτουργία συστήματος RFID

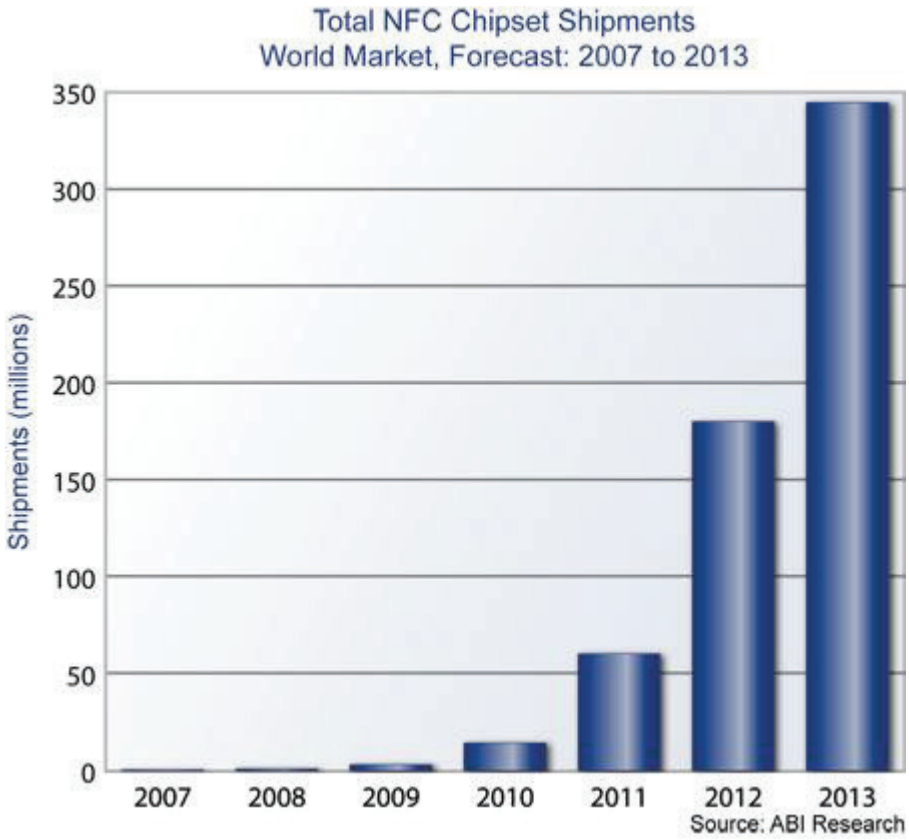
1.2 Ιστορική ανασκόπηση

Η Sony και η Philips οδηγούν καινοτόμοι το N F C σήμερα, αλλά οι ρίζες του ασύρματου προτύπου πάνε πίσω στο 2003, όταν εγκρίθηκε ς πρότυπο το ISO/IEC.Το 2004 Nokia Sony και Philips δημιουργούν το http://www.nfc-forum.org. Το forum έχει σήμερα περισσότερα από 200 μέλη συμπεριλαμβανομένων των κατασκευαστών, προγραμματιστές, και τα χρηματοπιστωτικά ιδρύματα των υπηρεσιών.

Το 2006, το φόρουμ NFC τεκμηρίωσε την τεχνολογία και δημιούργησε τον πρώτο οδικό χάρτη του. Διάφορες δοκιμές της τεχνολογίας πραγματοποιήθηκαν το 2007 και το 2008, αλλά δεν απογειώθηκε πραγματικά λόγω της έλλειψης υποστήριξης από τους μεταφορείς και τις τράπεζες. Το NFC είναι ισορροπημένο για να απογειωθεί, δεδομένου ότι οι σημαντικότεροι κατασκευαστές κινητών τηλεφώνων περιλαμβάνουν την τεχνολογία αυτή στα προϊόντα τους. Το 2011 θα μπορούσε να είναι το έτος των Επικοινωνιών Κοντινού Πεδίου. Αυτήν την περίοδο, η τεχνολογία NFC είναι πιο κοινή στην Ασία, την Ιαπωνία, και την Ευρώπη.

Εντούτοις οι ΗΠΑ αρχίζουν να καλύπτουν την διαφορά και αυτό γιατί, η GSMA, η διεθνής επαγγελματική οργάνωση για την ασύρματη βιομηχανία, ανακοίνωσε ότι 45 φορείς εκμετάλλευσης κινητών δικτύων (MNOS) από όλο τον κόσμο έχουν δεσμευτεί για την υποστήριξη κάρτας SIM, τεχνολογίας NFC. Μεταξύ των MNOS που υποστηρίζουν την προσέγγιση είναι η China Mobile και China Unicom, του Καναδά, Rogers Communications, Vodaphone Group και ISIS, η

αμερικανική κοινοπραξία μεταξύ της AT & T Mobility, η T-Mobile USA και η Verizon Wireless, όπως αναφέρεται στην ανακοίνωση.[3]



Εικόνα 3: Η εξέλιξη της τεχνολογίας NFC

ΚΕΦΑΛΑΙΟ 2

2.ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ ΚΑΙ ΣΥΣΤΑΤΙΚΑ NFC

2.1 Φυσικό επίπεδο στο NFC

Η Επικοινωνία κοντινού Πεδίου (**NFC-Near Field Communication**) είναι μια περιορισμένου φάσματος ασύρματη τεχνολογία συνδεσιμότητας (επίσης γνωστή ως ISO 18092) Interface and Protocol (NFCIP - 1) **σε αποστάσεις έως 10 εκατοστά (συνήθως < 5 cm)**. Επιτρέπει την γρήγορη ανάγνωση/εγγραφή δεδομένων (σχετικά λίγων- ενδεικτικά 48Bytes – 9kB) και εκλαμβάνεται ως απόδειξη φυσική παρουσίας. **Η ταχύτητα διαμεταγωγής δεδομένων μπορεί να είναι 106 kbps, 212 kbps ή 424 kbps.**

Επίσης, μπορεί να ενεργοποιήσει εύκολα υπηρεσίες. Αξιοποιείται μέσω κινητών συσκευών και smartphones, όπως ενδεικτικά τα Nokia 6212, C7, N9, τα Samsung Galaxy S II, (Google) Nexus S, S5230, Blackberry Bold 9900, Sagem (Mobiwire) Cosy με περισσότερα smartphones αλλά και tablets να αναμένονται εντός του 2011.

Εκτός από τα κινητά όμως υπάρχουν και NFC ετικέτες και κάρτες (εσωτερικού ή εξωτερικού χώρου, σε μπρελόκ, αυτοκόλλητα, μινιατούρες, κ.λπ.) με διαφορετική χωρητικότητα ή υπό μορφή έξυπνων καρτών σε σχήμα πιστωτικής ή σε άλλες υποδομές contactless (Contactless POS, Ticketing stands, Kiosks, κ.ά.)

Το πρωτόκολλο επικοινωνίας που επιλέχτηκε ήταν η συχνότητα 13.56MHz (στην οποία λειτουργεί και το RFID).

Το NFC πληροί τις προδιαγραφές των στάνταρτ ISO/IEC 14443 A & B, και Felica (ISO 18092).

Η τεχνολογία αναπτύσσεται και προωθείται κυρίως από το NFC Forum στο οποίο συμμετέχουν 140 εταιρίες και από άλλους οργανισμούς, όπως GSMA, GlobalPlatform και EMVCoH ταχύτητα διαμεταγωγής δεδομένων μπορεί να είναι 106 kbps, 212 kbps ή 424 kbps.

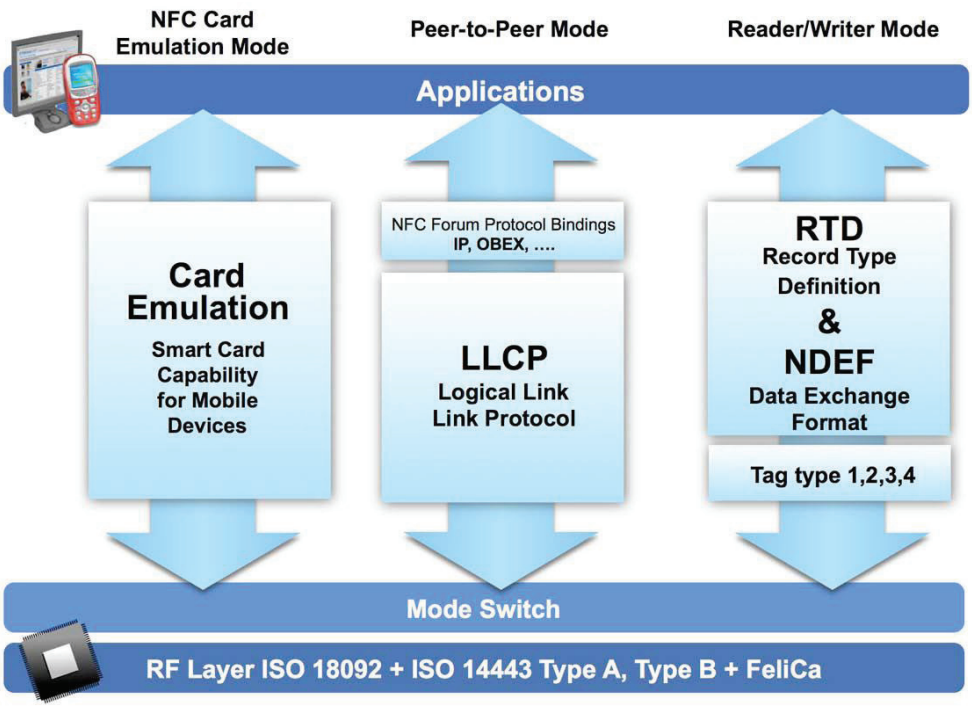
2.2 Αρχιτεκτονική NFC

Σε ένα NFC σύστημα πάντα υπάρχει ένας αποστολέας και ένας δέκτης. Ο αποστολέας ενεργά δημιουργεί ένα πεδίο ραδιοσυχνότητας όπου μπορεί να τροφοδοτήσει έναν παθητικό στόχο. Το σύστημα μπορεί να βρίσκεται σε 3+1 διαφορετικές καταστάσεις λειτουργίας, είτε αφορά επικοινωνία Reader/Writer (το ένα Active και το άλλο Passive),είτε οι δύο συσκευές να έχουν ομότιμη σχέση (Pear to Pear, αμφότερα active, όπως για παράδειγμα μεταξύ δύο κινητών τηλεφώνων με NFC chip), είτε Card Emulation (η συσκευή είναι Active αλλά υποδύεται το ρόλο π.χ. μιας κάρτας ως Passive.

Το μοντέλο peer-to-peer χρησιμοποιείται για τη μεταφορά δεδομένων μεταξύ συσκευών ορίζεται δηλαδή για επικοινωνία από συσκευή σε συσκευή σε επίπεδο σύνδεσης. Διαβιβάζονται έτσι τα προσωπικά στοιχεία επικοινωνίας μιας ηλεκτρονικής επαγγελματικής κάρτας από μια συσκευή σε μια άλλη, για παράδειγμα, μεταξύ ενός NFC-enabled κινητό τηλέφωνο και ένα NFC-enabled υπολογιστή. ¶ Μπορεί επίσης να χρησιμοποιηθεί αυτή η λειτουργία για την αρχική αντιστοίχιση, ή τη σύνδεση, δύο συσκευών που μπορούν στη συνέχεια να επικοινωνήσουν μέσω Bluetooth ή άλλο πρωτόκολλο.

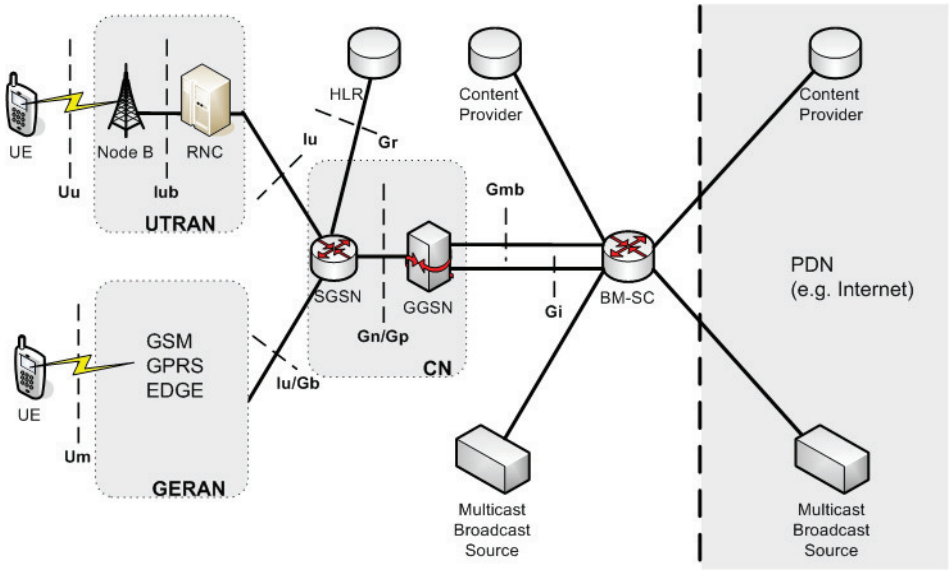
Με τη Reader/Writer λειτουργία, μια συσκευή NFC-enabled μπορεί να έχει πρόσβαση στα δεδομένα από ένα RFID-enabled αντικείμενο, όπως μια "έξυπνη κάρτα" με ενσωματωμένη ετικέτα RFID και επιτρέπει στους χρήστες να κατεβάζουν ένα URL για ένα trailer μιας ταινίας. ¶

Στο Emulation mode, μια NFC-enabled συσκευή συμπεριφέρεται σαν μια έξυπνη κάρτα. Η εξωτερική συσκευή αναγνώρισης καρτών έχει πρόσβαση στα ασφαλή στοιχεία της συσκευής όπως η USIM(Universal Subscriber Identify Module) αντίστοιχη της κάρτας SIM.



Εικόνα 4:Αρχιτεκτονική NFC

Η USIM κάρτα υποστηρίζει ταχύτερα δίκτυα από το δίκτυο GSM, όπως 3G /UMTS,δίκτυα που ξεχωρίζουν για τους αυξημένους ρυθμούς μετάδοσης των δεδομένων και την ταυτόχρονη υποστήριξη μεγαλύτερου όγκου δεδομένων και φωνής. Πιο συγκεκριμένα, το UMTS δίκτυο στην αρχική του φάση, θεωρητικά προσφέρει ρυθμούς μετάδοσης δεδομένων έως και 384 kbps σε περιπτώσεις όπου παρατηρείται αυξημένη κινητικότητα του χρήστη. Αντίθετα, όταν ο χρήστης παραμένει ακίνητος οι ρυθμοί μετάδοσης αυξάνουν κατά πολύ φθάνοντας την τιμή των 2 Mbps. Στην συνέχεια παρουσιάζεται ενδεικτικά η αρχιτεκτονική ενός UMTS δικτύου[4]



Εικόνα 5: Αρχιτεκτονική δικτύου UMTS

2.3 Ανάλυση συστήματος NFC

2.3.1 Λειτουργικές προδιαγραφές συστήματος NFC

Στην **εικόνα 4** εμφανίζεται η αρχιτεκτονική ενός συστήματος NFC Στη βάση κάθε τέτοιου τύπου συστήματος υπάρχουν οι προδιαγραφές της αναλογικής μετάδοσης (Analogue Specifications)οι οποίες καθορίζουν τα χαρακτηριστικά ραδιοσυχνότητας των συσκευών, όπως τη μορφή και τη δύναμη των πεδίων RF καθώς και τη λειτουργούσα σειρά των συσκευών. Το NFC βασίζεται στην επαγωγική ζεύξη, όπου τα αόριστα συνδεδεμένα επαγωγικά κυκλώματα μπορούν να χρησιμοποιηθούν για να μοιράζουν ενέργεια και δεδομένα ανάμεσα σε δύο συσκευές σε πολύ μικρή απόσταση

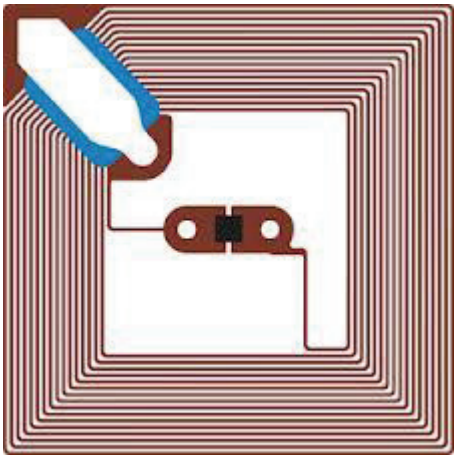
Τα ψηφιακά δεδομένα ακολουθούν τα πρότυπα ISO / IEC 18092 και ISO / IEC 14443.τα οποία καθορίζουν τα δομικά στοιχεία για την επικοινωνία. (Digital Protocol Specifications)

Στις προδιαγραφές δραστηριοτήτων (Activities Specifications),καθορίζονται οι δραστηριότητες που απαιτούνται για να δημιουργηθεί επικοινωνία με διαλειτουργικό τρόπο, βάση των προδιαγραφών του πρωτοκόλλου., η ανίχνευση σύγκρουσης πραγματοποιείτε με Polling Cycles (Δημοσκόπηση κύκλου είναι ο συνολικός χρόνος που απαιτείται από τον υπολογιστή ή την ηλεκτρονική συσκευή για να εκτελέσει μια πλήρη σταθμοσκόπηση όλων των αναγκαίων συνδέσεων.)

Επίσης, υπάρχει και κάτι που δεν φαίνεται με την πρώτη ματιά ,αλλά είναι προφανώς αναπόσπαστο κομμάτι των ασύρματων τεχνολογιών, το ενδιάμεσο λογισμικό (Middleware), το οποίο λειτουργεί ως «γέφυρα» επικοινωνίας μεταξύ του αναγνώστη και του πληροφοριακού συστήματος.

2.3.2:Ετικέτες NFC

Είναι ένα μικρό ηλεκτρονικό κύκλωμα που η βασική του λειτουργία είναι να αποθηκεύει και να μεταδίδει δεδομένα στον αναγνώστη.
Τοποθετείται στο υπό αναγνώριση αντικείμενο όπου αποθηκεύει έναν σειριακό αριθμό αναγνώρισης καθώς και ορισμένες άλλες πληροφορίες που αφορούν το αντικείμενο στο οποίο χρησιμοποιείτε.
Στην πιο βασική του μορφή του αποτελείτε από ένα ηλεκτρονικό τσιπάκι και μια κεραία τοποθετημένα σε ένα πακέτο ώστε να σχηματίσουν μια ετικέτα. Επίσης ορισμένες ετικέτες περιέχουν μπαταρίες και αυτό τις διαχωρίζει σε ενεργές και παθητικές ετικέτες όπως θα δούμε παρακάτω.



Εικόνα 6:NFC Tag

2.3.3:Η κεραία (antenna)

Είναι η συσκευή μέσω της οποίας γίνεται η συλλογή / μετάδοση της πληροφορίας από και προς τα tags. Χρησιμοποιούνται τόσο στις ετικέτες όσο και στους, αναγνώστες και κατηγοριοποιούνται,ανάλογα με τα χαρακτηριστικά τους .Το μέγεθος τους ποικίλει από μερικά τετραγωνικά εκατοστά, έως τετραγωνικά μέτρα. Σε ένα BlackBerry 9900 smartphone, για παράδειγμα, η κεραία NFC είναι

ενσωματωμένη στην πόρτα που καλύπτει το διαμέρισμα των μπαταριών

2.3.4: Ο αναγνώστης (reader/interrogatorr)

Ο αναγνώστης /ανακριτής είναι μια ενεργή συσκευή, που υπάρχει στα NFC/RFID συστήματα, και δημιουργεί ένα ρεύμα ραδιοσυχνότητας για να επικοινωνήσει μια ενεργή συσκευή με μια άλλη συμβατή συσκευή NFC, η μια μικρή ετικέτα NFC, η οποία έχει τις πληροφορίες που ο αναγνώστης θέλει.

Παθητικές συσκευές, όπως η ετικέτα NFC σε έξυπνες αφίσες, αποθηκεύουν πληροφορίες για να επικοινωνούν με τον αναγνώστη, αλλά δεν μπορούν να διαβάσουν άλλες ενεργές συσκευές.

Οι βασικές του λειτουργίες είναι:

- Να διαβάζει τα δεδομένα από τις NFC ετικέτες.
- Να γράφει δεδομένα στις NFC ετικέτες (στην περίπτωση που είναι έξυπνες ετικέτες).
- Να αναμεταδίδει δεδομένα από και προς τον ελεγκτή.
- Να τροφοδοτεί την ετικέτα(στην περίπτωση παθητικής ετικέτας)

Οι **NFC/RFID** αναγνώστες βασικά είναι μικροί υπολογιστές οι οποίοι αποτελούνται από 3 περίπου μέλη: Μια κεραία, ένα ηλεκτρονικό εξάρτημα RF που είναι υπεύθυνο για την επικοινωνία με την NFC ετικέτα και τον ελεγκτή.

Εκτός τις τέσσερις βασικές λειτουργίες ποιο σύνθετοι NFC/RFID αναγνώστες μπορούν να εκτελέσουν τρεις ποιο σημαντικές λειτουργίες:

- Εφαρμογή μέτρων για την αποτροπή συγκρούσεων ώστε να εξασφαλιστεί η ταυτόχρονη επικοινωνία με πολλές ετικέτες.
- Εξακρίβωση της γνησιότητας των ετικετών για την πρόληψη απάτης ή μη εξουσιοδοτημένης πρόσβασης στο σύστημα.
- Κρυπτογράφηση δεδομένων για την προστασία της ακεραιότητας των δεδομένων.

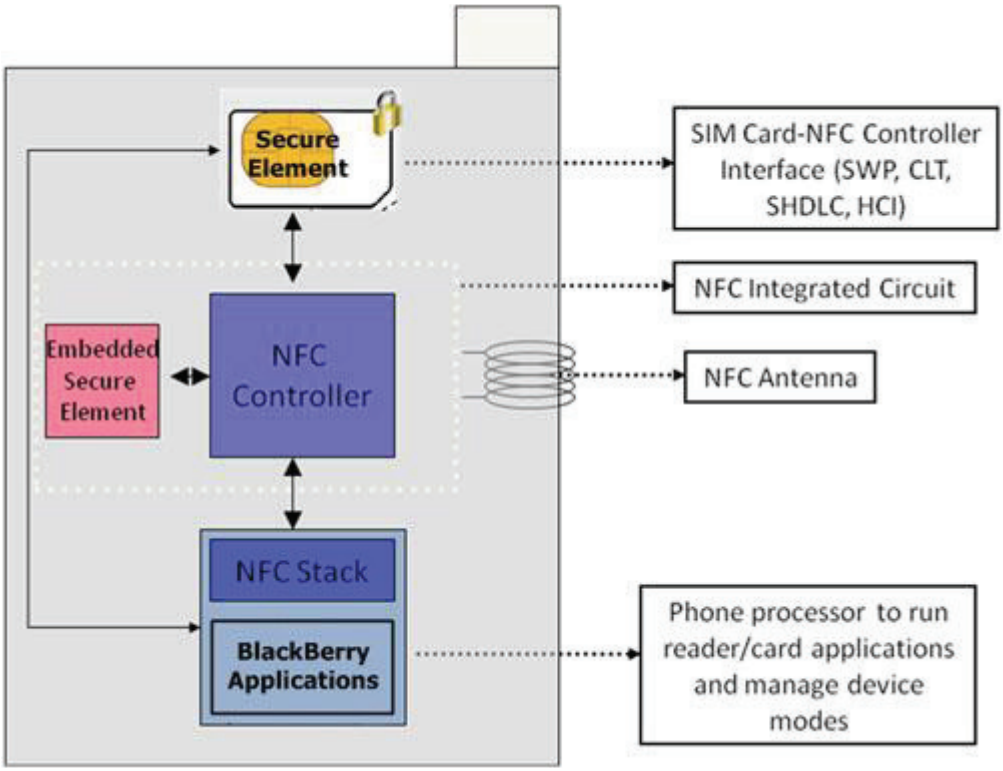
Εικόνα 7:NFC Reader

2 3.5: Ελεγκτής N F C

Οι ελεγκτές NFC είναι το ‘μυαλό’ σε κάθε NFC σύστημα. Χρησιμοποιούνται για να δικτυώσουν πολλαπλούς αναγνώστες NFC μαζί για την κεντρική επεξεργασία πληροφοριών.

Το φόρουμ NFC έχει δημιουργήσει την προδιαγραφή NFC Interface Controller (NCI), η οποία καθορίζει μια τυποποιημένη διεπαφή μέσα σε μία NFC συσκευή μεταξύ του ελεγκτή (NCI)και του κεντρικού επεξεργαστή εφαρμογών της συσκευής NFC.

Βασικά ο ελεγκτής NFC - αποτελείται από μια διεπαφή ελεγκτών υλικού NFC ("HCI") και ένα modem NFC. Αυτό το συστατικό διασυνδέεται με την κεραία NFC και επαναπροσανατολίζει την επικοινωνία RF (ραδιοσυχνότητα) στο επιλεγμένο SE (ασφαλές στοιχείο). Είναι το βασικό κομμάτι του υλικού που δίνει σε μια enabled NFC συσκευή όλες τις δυνατότητές της.[5]



Εικόνα 8:Λειτουργία NCI από κινητό με ενσωματωμένο NFC chip

Με τη νέα προδιαγραφή, οι κατασκευαστές συσκευών μπορούν να ενσωματώσουν εύκολα chipsets από διάφορους κατασκευαστές τσιπ. Η προδιαγραφή ορίζει επίσης ένα κοινό επίπεδο της λειτουργικότητας και της διαλειτουργικότητας μεταξύ των στοιχείων που περιλαμβάνονται μέσα σε μια NFC-enabled συσκευή.

Προηγουμένως, οι κατασκευαστές hardware έπρεπε να δημιουργήσουν τη δική τους, συγκεκριμένη συσκευή, ελεγκτής διεπαφής, για τη διαχείριση των αλληλεπιδράσεων μεταξύ της CPU της συσκευής και του NFC τσιπ. Η σημασία των προδιαγραφών NCI είναι: ότι οι κατασκευαστές θα έχουν πρόσβαση σε μια τυποποιημένη διεπαφή που μπορεί να εφαρμοστεί σε οποιοδήποτε είδος NFC-enabled συσκευής που κατασκευάζουν, είτε πρόκειται για κινητά τηλέφωνα, υπολογιστές, ταμπλέτες, εκτυπωτές, ηλεκτρονικά είδη ευρείας κατανάλωσης ή συσκευές.

Η οικοδόμηση σε καθολικά πρότυπα θα επιτρέψει επίσης στους κατασκευαστές να φέρουν τα NFC προϊόντα στην αγορά γρηγορότερα από πριν. Η προδιαγραφή NCI επιτρέπει τον έλεγχο και τη διαχείριση της λειτουργίας που

προσφέρονται από τον NFC ελεγκτή μιας συσκευής κάτι που υλοποιείται σύμφωνα με τις αντίστοιχες προδιαγραφές του NFC Forum.

Η νέα NCI παρέχει στους χρήστες μια λογική διεπαφή που υποστηρίζει μια σειρά από διαφορετικές φυσικές μεταφορές συμπεριλαμβανομένης της UART, SPI και I_2C. Η NCI υποστηρίζει επίσης τη δρομολόγηση της κυκλοφορίας σε άλλα ασφαλή στοιχεία στο εσωτερικό της συσκευής, όπως ETSI-HCI ή ISO / IEC 7816.

2.3.6: Ενδιάμεσο λογισμικό (middleware)

Όπως στον κόσμο του RFID έτσι και στο NFC, ο όρος αυτός συνήθως χρησιμοποιείται για να δηλώσει το λογισμικό που βρίσκεται σε ένα διακομιστή ανάμεσα στους αναγνώστες και τις εταιρικές εφαρμογές. Το ενδιάμεσο λογισμικό χρησιμοποιείται για να φιλτράρει τα δεδομένα και να περνά μόνο τις χρήσιμες πληροφορίες για τις εταιρικές εφαρμογές. Μερικά middleware μπορεί επίσης να χρησιμοποιηθούν για τη διαχείριση των αναγνωστών σε ένα δίκτυο.

2.4: Βασικά χαρακτηριστικά των NFC συστημάτων

2.4.1: Τύποι ετικετών NFC ανάλογα με την πηγή ενέργειά τους

Οι **ετικέτες** χωρίζονται σε τρεις κατηγορίες, **τις παθητικές** και τις **ενεργητικές**, ανάλογα με την κατασκευή τους. Επίσης, λόγω της κατασκευής τους κατηγοριοποιούνται ξεχωριστά μια ακόμα μορφή ετικέτας, η οποία είναι ενδιάμεση των δύο παραπάνω κατηγοριών, οι **Ημιπαθητικές ετικέτες**.

2.4.1.1: Παθητικές ετικέτες

Οι παθητικές ετικέτες (passive tags) αποτελούνται από ένα μικροτσίπ και μία κεραία. Ο αναγνώστης στέλνει ραδιοκύματα τα οποία μέσω της κεραίας μεταδίδουν ηλεκτρικό ρεύμα στο μικροκύκλωμα που περιλαμβάνει η ετικέτα. Αυτή στέλνει με τον τρόπο αυτό τα δεδομένα τα οποία έχουν αποθηκευτεί στο μικροτσίπ ως απάντηση. Οι παθητικές ετικέτες λόγω της ικανότητάς τους να λειτουργούν δίχως να τροφοδοτούνται με ηλεκτρικό ρεύμα από δική τους πηγή, είναι σημαντικά

φθηνότερες και πολύ πιο μικρές σε μέγεθος, με αποτέλεσμα να βρίσκουν εφαρμογή σε πολλά προϊόντα. Ωστόσο, η έλλειψη τροφοδοσίας περιορίζει και την εμβέλεια λειτουργίας τους που φτάνει μέχρι και τα πέντε μέτρα, αλλά και το εύρος των δεδομένων τα οποία μπορεί να αποθηκεύσουν και να αναμεταδώσουν.

2.4.1.2: Ενεργητικές ετικέτες

Οι ενεργές ετικέτες (active tags) λειτουργούν με τον ίδιο ακριβώς τρόπο που λειτουργούν οι παθητικές. Η διαφορά τους έγκειται στην τροφοδοσία του κυκλώματος που προκαλεί την αναμετάδοση των δεδομένων. Οι ενεργές ετικέτες διαθέτουν μπαταρίες και μπορούν μόνες τους να τροφοδοτήσουν την αναμετάδοση. Η χρήση της μπαταρίας, όμως, προκαλεί μεγαλύτερο κόστος παραγωγής, άρα και διάθεσης, ενώ ο όγκος επίσης αυξάνεται. Από την άλλη πλευρά, αυξάνονται και το μέγεθος των αποθηκευμένων στο μικροτσίπ δεδομένων αλλά και η εμβέλεια αναμετάδοσης που φθάνει τις μερικές δεκάδες μέτρα, δυνατότητες που καθιστούν τις ενεργές ετικέτες τις επικρατέστερες στο μέλλον, με μόνη προϋπόθεση την μείωση του κόστους και του όγκου.

2.4.1.3: Ημιπαθητικές ετικέτες

Οι ημιπαθητικές ετικέτες στην κατασκευή τους και στον τρόπο επικοινωνίας τους είναι ίδιες με τις παθητικές ετικέτες. Αυτό που τις κάνει να διαφέρουν είναι η μπαταρία που διαθέτουν, όπως και η ενεργητικές. ωστόσο η διαφορά τους παρουσιάζεται στο ότι η πηγή ενέργειας θέτει σε λειτουργία το ολοκληρωμένο κύκλωμα και όχι τη μετάδοση του σήματος στον αναγνώστη, από όπου και απορροφούν ενέργεια. Τέλος, οι ετικέτες αχρηστεύονται όταν τελειώσει η μπαταρία που διαθέτουν.

2.4.2: Κατηγορίες ετικετών NFC αναλόγως της δυνατότητας ανάγνωσης-εγγραφής

Επίσης, οι ετικέτες NFC διαχωρίζονται σύμφωνα με τον τύπο των μικροεπεξεργαστών που χρησιμοποιούν και τις προδιαγραφές του NFC Forum σε:

- **NFC Forum Type 1 Tag**

Οι ετικέτες Τύπου 1 βασίζονται στο πρότυπο ISO / IEC 14443A. Οι ετικέτες είναι σε θέσει διαβάσουν και να γράψουν εκ νέου Οι χρήστες μπορούν να ρυθμίσουν μια ετικέτα έτσι ώστε να γίνει μόνο για ανάγνωση. Η Διαθεσιμότητα μνήμης είναι 96 bytes και επεκτάσιμη έως 2 Kbyte.

- **NFC Forum Type 2 Tag**

Οι ετικέτες Τύπου 2 βασίζεται στο πρότυπο ISO / IEC 14443A. Οι ετικέτες είναι σε θέσει να διαβάσουν και να γράψουν εκ νέου Οι χρήστες μπορούν να ρυθμίσουν μια ετικέτα ώστε να γίνει μόνο για ανάγνωση. Η διαθεσιμότητα μνήμης είναι 48 bytes και επεκτάσιμη έως 2 Kbyte.

- **NFC Forum Type 3 Tag**

Οι ετικέτες τύπου 3 είναι βασισμένες στο Ιαπωνικό Βιομηχανικό Πρότυπο (JIS) X 6319-4, επίσης γνωστό ως Felica. Οι ετικέτες είναι προ-ρυθμισμένες κατά την κατασκευή τους είτε να διαβάζουν, είτε να είναι επανεγγράψιμες είτε να είναι μόνο για ανάγνωση. Η διαθεσιμότητα μνήμης είναι μεταβλητή, το θεωρητικό όριο μνήμης είναι 1MBytes ανά υπηρεσία.

- **NFC Forum Type 4 Tag**

Οι ετικέτες τύπου 3 είναι βασισμένες στο Ιαπωνικό Βιομηχανικό Πρότυπο ISO / IEC 14443. Οι ετικέτες είναι προ-ρυθμισμένες κατά την κατασκευή τους είτε να διαβάζουν, είτε να είναι επανεγγράψιμες είτε να είναι μόνο για ανάγνωση. Η διαθεσιμότητα μνήμης είναι μεταβλητή, 32Kbytes ανά υπηρεσία. η διεπαφή επικοινωνίας είναι συμβατή ή με τον τύπου A ή με τον τύπο B

- **NFC Forum Mifare Classic**

Οι ετικέτες αυτές είναι συμβατές με το πρότυπο ISO 14443A.Είναι και αυτή ουσιαστικά μια συσκευή αποθήκευσης όπως και οι προηγούμενες ετικέτες ,όπου η μνήμη είναι χωρισμένη σε μπλοκ ,με απλούς μηχανισμούς ασφαλείας για τον έλεγχο της πρόσβασης. Είναι βασισμένη σε ASIC και έχει περιορισμένη υπολογιστική ισχύς. Χάρη στην αξιοπιστία της και στο χαμηλό κόστος αυτή η ετικέτα χρησιμοποιείται ευρέως για εφαρμογές, όπως ηλεκτρονικό πορτοφόλι, έλεγχο πρόσβασης, εταιρικές ταυτότητες, μεταφορές ή ακόμα και ως εισιτήριο γηπέδου.

Πίνακας 1:Type Tags[6]

ΤΥΠΟΣ	ΠΡΟΙΟΝΤΑ	ΧΩΡΗΤΙΚΟΤΗΤΑ
Type 1	Innovision Topaz	96 Bytes
Type 2	NXP MIFARE Ultralight (C)	48-144 Bytes
Type 3	Sony Felica	1,4,9 Kbytes
Type 4	NXP DESFire	2,4,8 Kbytes
MIFARE	NXP MIFARE Classic	1,4 Kbytes

2.4.3: Λειτουργία ετικετών

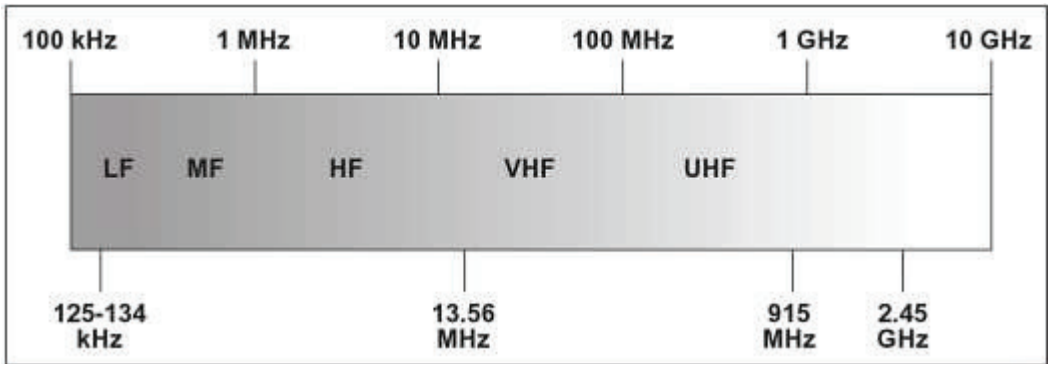
Οι NFC ετικέτες λειτουργούν με μια ενεργή συσκευή (συνήθως ένα κινητό τηλέφωνο) δημιουργώντας ένα μαγνητικό πεδίο που επάγει ένα ηλεκτρικό ρεύμα στην κεραία της παθητικής συσκευή (το Tag NFC) που εκκινεί το NFC Chip. Το NFC Tag τότε δημιουργεί ένα περαιτέρω μαγνητικό πεδίο το οποίο μπορεί σε αντάλλαγμα να διαβαστεί από την ενεργό συσκευή (το τηλέφωνο) και επιτρέπει δεδομένα που πρέπει να μεταφερθούν.

Εικόνα 9 :Παράδειγμα λειτουργίας Tag

2.4.4: Συχνότητες εκπομπής ετικετών NFC

Οι ετικέτες και οι αναγνώστες, θα πρέπει να ρυθμιστούν στην ίδια συχνότητα, ώστε να επικοινωνήσουν μεταξύ τους Το NFC λειτουργεί σε συχνότητα 13,56MHz (ενδεικτικά, ένα ασύρματο τηλέφωνο λειτουργεί σε συχνότητες κοντά στα 2Ghz)

Εικόνα 10:Πίνακας φάσματος Ραδιοσυχνοτήτων



2.4.4.1:Χαρακτηριστικά συχνοτήτων HF (Height Frequency)

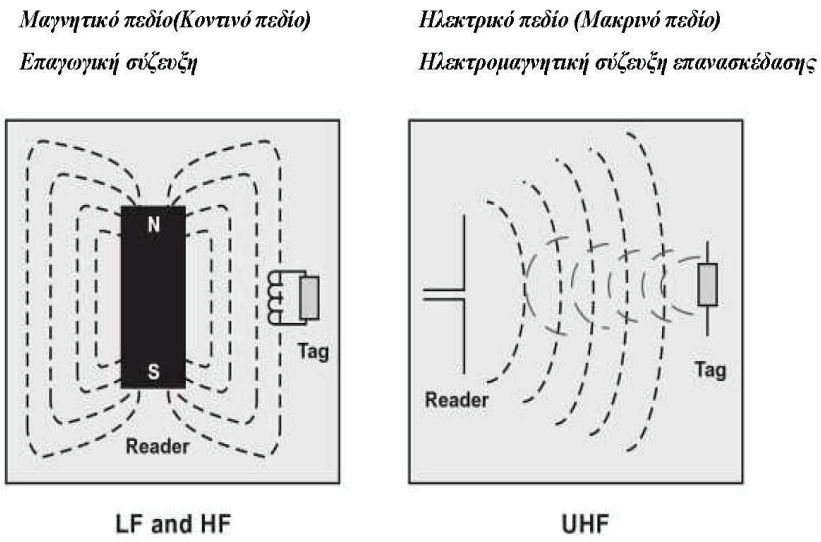
Τα συστήματα υψηλής συχνότητας λειτουργούν μεταξύ 10-15 MHz,αλλά τα 13,56 MHz είναι αυτά που χρησιμοποιούνται συχνότερα, έχουν μεγαλύτερο εύρος ζώνης και μεγαλύτερες ταχύτητες ανάγνωσης σε σχέση με τα συστήματα χαμηλής συχνότητας. Το κόστος των συστημάτων αυτών δεν είναι πολύ υψηλό παρόλο που είναι μεγαλύτερο από αυτό των συστημάτων χαμηλής συχνότητας. Έτσι τα συστήματα αυτά θεωρούνται φθηνά /οικονομικά και συνήθως χρησιμοποιούνται στον έλεγχο πρόσβασης (access control) και στις έξυπνες κάρτες Επίσης, ένα σύστημα NFC, που είναι ένα τυπικό σύστημα υψηλής συχνότητας (HF), χρησιμοποιεί παθητικές ετικέτες και η ταχύτητα μετάδοσης των δεδομένων από την ετικέτα στον αναγνώστη είναι χαμηλή.

Οι ετικέτες υψηλής συχνότητας δεν λειτουργούν καλά όταν βρίσκονται πάνω σε αντικείμενα που είναι φτιαγμένα από μέταλλα μπορούν να λειτουργήσουν όμως καλά σε αγαθά με υψηλή περιεκτικότητα σε νερό. Έχουν μέγιστη ταχύτητα ανάγνωσης 3 feet(1 μέτρο).

2.4.5:Μέγεθος και τύπος κεραίας

Λόγο του μεγάλου μήκους κύματος της χαμηλής συχνότητας ραδιοσυχνοτήτων, οι κεραίες των συστημάτων LF και HF πρέπει να κατασκευάζονται πολύ μεγαλύτερες από τις κεραίες UHF και μικροκυμάτων προκειμένου να επιτύχουν συγκρίσιμη λήψη σήματος. Αυτό παρ' όλα αυτά έρχεται σε σύγκρουση με τον στόχο του να κατασκευάζονται οι ετικέτες NFC μικρές και φτηνές .Οι περισσότεροι σχεδιαστές συστημάτων παραβλέπουν το κέρδος της κεραίας προκειμένου να ελέγξουν το κόστος, με τελικό αποτέλεσμα την χαμηλή εμβέλεια ανάγνωσης για τα συστήματα LF και HF.

Υπάρχει ένα κατώτατο όριο στο πόσο μικρές μπορούν να κατασκευαστούν οι κεραίες LF και HF, με αποτέλεσμα οι ετικέτες LF και HF να είναι συνήθως μεγαλύτερες από τις ετικέτες των UHF και των μικροκυμάτων. Η συχνότητα χρίσης θα καθορίσει τον τύπο της κεραίας που θα χρησιμοποιηθεί σε ένα σύστημα RF. Στα LF και HF χρησιμοποιούνται επαγωγικές κεραίες που συνήθως είναι τύπου βρόχου, ενώ στις συχνότητες UHF και μικροκυμάτων υπάρχει χωρητική σύζευξη και οι κεραίες είναι διπολικού τύπου.



Εικόνα 11:Διάγραμμα κεραίας/σύζευξη ετικετών

2.4.6: Μηδενισμοί κεραίας και προβλήματα προσανατολισμού

Οι επαγωγικές κεραίες, όπως αυτές που χρησιμοποιούνται στα LF και HF, λειτουργούν 'πλημυρίζοντας' μια ζώνη ανάγνωσης με ακτινοβολία RF. Πέρα από τα μεγάλα μήκη κύματος των LF και HF, αυτό λειτουργεί ώστε να κατακλύζει την ζώνη ανάγνωσης ενός αναγνώστη με ένα ομοιόμορφο σήμα το οποίο δεν θα διαφέρει σε ισχύ από το ένα άκρο στο άλλο. Οι διπολικές κεραίες αφετέρου ,όπως αυτές που χρησιμοποιούνται στις συχνότητες των UHF και των μικροκυμάτων, λειτουργούν εντοπίζοντας τα ακτινοβόλα σήματα από τον πομπό στον δέκτη. Αυτό πέρα από τα σχετικά μικρά μήκη κύματος της υψηλής συχνότητας των UHF και των

μικροκυματικών σημάτων, δημιουργεί μικρές διακυμάνσεις στη ζώνη ανάγνωσης στη ζώνη ανάγνωσης ενός αναγνώστη UHF μικροκυμάτων. Έτσι η ισχύς σήματος δεν θα είναι ομοιόμορφή από το ένα άκρο της ζώνης ανάγνωσης στο άλλο και ακόμη σε κάποια σημεία θα πέσει στο μηδέν δημιουργώντας 'μηδενισμούς' ή αόρατα σημεία Οι ετικέτες NFC που τοποθετούνται στα σημεία μηδενισμού καθιστούνε ουσιαστικά αόρατες σε έναν αναγνώστη RF , το οποίο προφανώς μπορεί να δημιουργήσει προβλήματα στα συστήματα UHF και μικροκυμάτων.

Επίσης τα σημεία μηδενισμού μπορούν να προκύψουν από τον αποσυντονισμό των ετικετών , που προκύπτει όταν δύο ετικέτες τοποθετούνται η μία κοντά στην άλλη, ή κοντά σε υγρά, μέταλλα και άλλα υλικά με υψηλή διηλεκτρική διαπερατότητα.

Οι επαγωγικές κεραίες έχουν ελάχιστο κατευθυντικό κέρδος εννοώντας ότι η ισχύς σήματος σε μια δεδομένη απόσταση είναι ίδια πάνω, κάτω, μπροστά και πίσω από την κεραία. Οι διπολικές κεραίες έχουν αρκετά υψηλότερο κατευθυντικό κέρδος, και σημαντικές διαφορές στην ισχύ πεδίου θα υπάρχουν σε μια δεδομένη απόσταση ανάμεσα σε σημεία μπροστά από την κεραία και πάνω από αυτή. Για τις ετικέτες UHF και μικροκυμάτων οι οποίες βρίσκονται πάνω από τον αναγνώστη, η ισχύς σήματος μπορεί να μην είναι αρκετά ισχυρή μεταξύ τους ώστε να επιτρέψει την επικοινωνία τους.

Όλα αυτά τα φαινόμενα απαιτούν τα συστήματα **UHF** και **RFID** να χρησιμοποιούν μια πιο περίπλοκη μορφή διαμόρφωσης, αποκαλούμενη διαμόρφωση μεταπήδησης συχνοτήτων,(Frequency Hopping: Διασπορά φάσματος με εναλλαγή συχνοτήτων **FHSS**) ώστε να ξεπεράσουν τα παραπάνω προβλήματα.

2.4.7: Παράγοντες που επηρεάζουν την ανάγνωση

Όπως είδαμε και παραπάνω κάθε συχνότητα λειτουργεί διαφορετικά αναλόγως των συνθηκών που τις επηρεάζουν. Για αυτό η δημιουργία ενός δικτύου αναγνώρισης ραδιοσυχνοτήτων, πρέπει να στηρίζεται σε ελέγχους που έχουν γίνει σχετικά με τους παράγοντες που επηρεάζουν την ανάγνωση των δεδομένων τα οποία θέλουμε να συλλέξουμε.

Τέσσερις είναι οι βασικοί παράγοντες που επηρεάζουν την ανάγνωση των ετικετών

από τους αναγνώστες και έχουν ως εξής:

Η απόσταση ανάγνωσης: Κάθε αναγνώστης εκπέμπει σήματα σε διαφορετικές συχνότητες, ενώ κάθε συχνότητα έχει διαφορετική εμβέλεια. Παράλληλα, κάθε αναγνώστης επικοινωνεί με συγκεκριμένο είδος ετικέτας. Για παράδειγμα, εάν γνωρίζουμε ότι η απόσταση ανάγνωσης στο υπό μελέτη δίκτυο μας θα είναι μικρή, τότε θα πρέπει να προσανατολιστούμε προς την επιλογή αναγνωστών που λειτουργούν σε χαμηλές συχνότητες και την τοποθέτηση παθητικών ετικετών

Το υλικό εφαρμογής των ετικετών: Λόγω της ικανότητας κάποιων υλικών, όπως το νερό, να απορροφούν τα ραδιοκύματα και κάποιων άλλων, όπως τα μέταλλα, να τα αντανακλούν, η τοποθέτηση ετικετών σε αυτά πρέπει να γίνει μετά από μελέτη και δοκιμές. Να ελέγχεται η απόσταση της ετικέτας από το μέταλλο, ή και να ελέγχεται το είδος της ετικέτας που μπορούμε να τοποθετήσουμε και αντίστοιχα και ο αναγνώστης που θα συμπληρώσει το δίκτυο.

Η γεωμετρία ανάγνωσης: Ο προσανατολισμός της κεραίας της ετικέτας θα κρίνει αν το σήμα το οποίο εκπέμπεται από τον αναγνώστη θα γίνει αποδεκτό. Έτσι, εάν η κεραία είναι παράλληλα τοποθετημένη σε σχέση με τον αναγνώστη, η επικοινωνία δεν θα είναι εφικτή. Για τον λόγο αυτό, οι κατασκευαστές οδηγούνται στην κατασκευή κυκλικών κεραιών, οι οποίες έχουν την ικανότητα να διαβάζουν σήματα ανεξαρτήτως της γωνίας εκπομπής. ωστόσο, οι γραμμικές κεραίες έχουν την ικανότητα να διαβάζουν σήματα σε μεγαλύτερες αποστάσεις.

Περιβαλλοντικές συνθήκες: Ένας ακόμη παράγοντας ο οποίος μπορεί μόνο με ελέγχους και δοκιμές να ξεπεραστεί, είναι ο χώρος στον οποίο θα γίνεται η ανάγνωση. Όπως προαναφέρθηκε, τα ραδιοκύματα ανακλώνται από άλλα υλικά και απορροφώνται από άλλα, ενώ την ίδια συμπεριφορά έχουν και όταν αλληλεπιδρούν με άλλα ραδιοκύματα. Σε ένα περιβάλλον στο οποίο διάφορα υλικά υπάρχουν, για παράδειγμα, σωληνώσεις, ράφια αποθήκευσης και επικρατεί υγρασία, η μετάδοση σημάτων από τους αναγνώστες ενδέχεται να δεχθεί παρεμβολές και η ανάγνωση να αποτύχει.

2.4.7.1: Κωδικοποίηση δεδομένων

Το NFC χρησιμοποιεί δύο διαφορετικές κωδικοποιήσεις για τη μεταφορά δεδομένων. Εάν μια συσκευή είναι σε active mode κατά τη μεταφορά δεδομένων

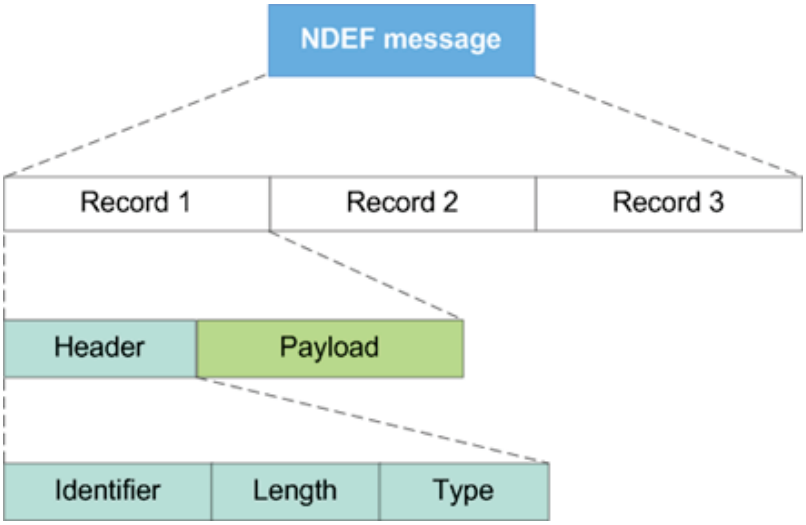
της σε 106 kbit/s, χρησιμοποιείται. μια τροποποιημένη κωδικοποίηση Miller με λόγο διαμόρφωσης 100% Σε όλες τις άλλες περιπτώσεις χρησιμοποιείται Manchester κωδικοποίηση με λόγο διαμόρφωσης 10%.

2.4.8: Μηνύματα που ανταλλάσσονται(NDEF)

Τα μηνύματα τα οποία μεταδίδονται ονομάζονται μηνύματα **NDEF** και είναι τα εξής:

- Smart Poster (για την ανάγνωση επιπλέον πληροφορίας από διαφημιστικά πόστερ)
- Handover (για παράδειγμα, την άμεση σύνδεση δύο συσκευών bluetooth με το άγγιγμά τους)
- vCard (μεταφορά στοιχείων επαφών υπό μορφή vCard)
- URL (παραπομπή σε ιστοσελίδα)
- SMS
- Call Request

Αναλυτικότερα, το υπόδειγμα ανταλλαγής δεδομένων NFC (NDEF) καθορίζει ένα σχήμα ενθυλάκωσης μηνυμάτων για την ανταλλαγή πληροφοριών, π.χ. μεταξύ μιας συσκευής NFC και μιας άλλης συσκευής NFC ή μιας ετικέτας NFC. Το NFC Data Exchange Format (NDEF) είναι μια τυποποιημένη μορφή δεδομένων που μπορούν να χρησιμοποιηθούν για την ανταλλαγή πληροφοριών μεταξύ οποιαδήποτε συμβατή συσκευή NFC και μια άλλη συσκευή ή NFC ετικέτα. Η μορφή των δεδομένων αποτελείται από μηνύματα NDEF και NDEF εγγραφές. Ένα μήνυμα NDEF αποτελείται από μία ή περισσότερες εγγραφές NDEF. Μπορούν να υπάρξουν πολλαπλάσιες εγγραφές σε ένα μήνυμα NDEF. Βασικά το μήνυμα NDEF είναι σειρά εγγραφών NDEF. Πόσα εγγραφές μπορούμε να ενθυλακώσουμε σε ένα μήνυμα NDEF εξαρτάται από την αίτησή μας και τον τύπο ετικετών.



Εικόνα 12:Δομή μηνύματος NDEF

Στην αμφίδρομη επικοινωνία ενός κινητού τηλεφώνου με NFC Reader και μιας NFC Tag για να διαβαστούν και να γραφούν δεδομένα για παράδειγμα ένα URL όπως (http://nokia.com), διαβιβάζεται ουσιαστικά ο παρακάτω κώδικας στο δεκαεξαδικό σύστημα.

03 0e d1 01 0a 55 03 6e 6f 6b 69 61 2e 63 6f 6d fe

- 03-Αυτό είναι το byte που καθορίζει τον τύπο της εγγραφής Μια εγγραφή NDEF εκπροσωπείται από το byte 03 στο δεκαεξαδικό.
- 0e-Αυτό είναι ένα byte που ενημερώνει πόσα bytes είναι το ωφέλιμο φορτίο της εγγραφής.
- d1-Με αυτό το byte δηλώνονται τα NDEF αρχεία που είναι εγγραφές μεταβλητού μήκους με ένα κοινό σχήμα που απεικονίζεται στο παρακάτω σχήμα.

2.4.8.1: NDEF Record

NDEF εγγραφές περιέχουν ένα ειδικό ωφέλιμο φορτίο, και έχουν την ακόλουθη δομή που προσδιορίζει τα περιεχόμενα και το μέγεθος της εγγραφής:

Bit 7 6 5 4 3 2 1 0

------ ------ ------ ------ ------ ------ ------ ------

[MB] [ME] [CF] [SR] [IL] [TNF]

[TYPE LENGTH]

[PAYLOAD LENGTH]

[ID LENGTH]

[RECORD TYPE]

[ID]

[PAYLOAD]

Header Record (Byte 0)

Η κεφαλίδα εγγραφής περιέχει μια σειρά από σημαντικούς τομείς, συμπεριλαμβανομένου ενός 3-bit πεδίου που προσδιορίζει τον τύπο του αρχείου που ακολουθεί (TNF):

TNF: Type Name Format Field

Ο τομέας TNF μιας εγγραφής NDEF είναι ένας 3-bits αριθμός ,ο οποίος περιγράφει τον τύπο της εγγραφής και προσδιορίζει πιθανώς την δομή και το περιεχόμενο του υπολοίπου της εγγραφής.

IL: ID LENGTH Field

Το flag IL δείχνει αν το πεδίο ID LENGTH υπάρχει ή όχι. Αν αυτό έχει οριστεί σε 0, τότε το πεδίο ID LENGTH παραλείπεται από την εγγραφή.

SR: Short Record Bit

Το flag SR έχει οριστεί σε 1 εάν το μήκος του πεδίου που περιλαμβάνει το ωφέλιμο φορτίο (PAYLOAND) είναι 1 byte (8 bits/0-255) ή λιγότερο. Αυτό επιτρέπει περισσότερο συμπαγή εγγραφές.

CF: Chunk Flag

Το flag CF δείχνει αν αυτό είναι το πρώτο κομμάτι εγγραφής ή ένα μεσαίο κομμάτι εγγραφής.

ME: Message End

Το flag δείχνει ότι αυτή είναι η τελευταία εγγραφή του μηνύματος NDEF.

MB: Message Begin

Το flag δείχνει ότι αυτή η εγγραφή είναι ή πρώτη του μηνύματος NDEF.

Type Length

Δείχνει το μήκος σε (bytes) του πεδίου RECORD TYPE .Αυτή η τιμή είναι πάντα 0 για ορισμένους τύπους εγγραφών που ορίζονται από το πεδίο TNF, το οποίο περιγράφεται παραπάνω.

Payload Length

Δείχνει το μήκος σε (bytes) του πεδίου PAYLOAND.Αν το SR έχει οριστεί σε 1 στην κεφαλίδα ,αυτή η τιμή θα είναι ένα byte μεγαλύτερη για (PAYLOAND μήκους 0-255 bytes).Αν το πεδίο SR είναι 0, η τιμή αυτή θα είναι μια 32-bits τιμή που καταλαμβάνει 4 Bytes.

ID Length

Δείχνει το μήκος σε Bytes του ID. Αυτό το πεδίο υπάρχει μόνο όταν το flag US είναι 1στην κεφαλίδα

Record Type

Η τιμή αυτή περιγράφει τον τύπο της εγγραφής που ακολουθεί. Οι τιμές του πεδίου τις συγκεκριμένης εγγραφής πρέπει να ανταποκρίνονται στην αξία των bits που έχουν καταχωρηθεί στην κεφαλίδα.

Record ID

Δείχνει την τιμή στο πεδίο ID εάν το ID συμπεριλαμβάνεται (το bit IL στην κεφαλίδα της εγγραφής έχει οριστεί 1).Εάν το IL είναι 0 το πεδίο παραλείπεται

Payload

Το ωφέλιμο φορτίο της εγγραφής, το οποίο θα είναι ακριβώς ο αριθμός των bytes που περιγράφονται στο πεδίο Payload Length νωρίτερα.

ΚΕΦΑΛΑΙΟ 3

3: ΠΡΟΤΥΠΑ ΚΑΙ ΚΑΤΑΣΚΕΥΑΣΤΕΣ ΤΕΧΝΟΛΟΓΙΑΣ NFC

3.1: Οργανισμοί και Πρότυπα Αναγνώρισης Ραδιοσυχνοτήτων

Η τεχνολογία NFC χρησιμοποιεί τις ραδιοσυχνότητες και για το λόγο αυτό απαιτούνται πρότυπα που θα καθορίζουν ποιο κομμάτι του φάσματος συχνοτήτων θα δεσμεύει, τα επίπεδα εκπομπής και θέματα παρεμβολών με άλλες ραδιουπηρεσίες.

Επιπρόσθετα, το γεγονός ότι υπάρχουν πολλοί κατασκευαστές –προμηθευτές της τεχνολογίας NFC, δημιουργεί πρόβλημα στον καταναλωτή που καλείται να επικοινωνήσει με διαφορετικά NFC συστήματα άλλων εταιριών. Ενώ, τέλος, το όραμα της αγοράς για ένα ανοικτό και παγκόσμιο σύστημα διαχείρισης της εφοδιαστικής αλυσίδας, με χρήση της τεχνολογίας NFC, απαιτεί πρότυπα προκειμένου αυτό να γίνει πραγματικότητα.

Για τους παραπάνω λόγους αναπτύχθηκαν μια σειρά από πρότυπα από συγκεκριμένους οργανισμούς κάποιοι από αυτούς είναι:

- **Παγκόσμιος Οργανισμός Προτυποποίησης** (ISO, International Organization for Standardization)
- **Παγκόσμιο Ηλεκτροτεχνικό Συμβούλιο** (IEC, International Electro technical Council)
- **Ευρωπαϊκό Ινστιτούτο Προτύπων Τηλεπικοινωνιών** (ETSI, European Telecommunications Standards Institute)
- **EPC global** (Electronic Product Code)
- **EMVCo** Υπεύθυνοι για τις επιπτώσεις σχετικά με τις αιτήσεις πληρωμής **EMV.**

3.2:Πρωτόκολλα

Τα πρότυπα του NFC καλύπτουν πρωτόκολλα επικοινωνίας και μορφές ανταλλαγής δεδομένων, και βασίζονται σε πρότυπα αναγνώρισης υφιστάμενων ραδιοσυχνοτήτων (RFID), συμπεριλαμβανομένων των ISO / IEC 14443 και FeliCa. Τα πρότυπα περιλαμβάνουν το ISO / IEC 18092 και εκείνα που καθορίζονται από το

NFC Forum, το οποίο προωθεί την τεχνολογία NFC και πιστοποιεί τη συμμόρφωση της συσκευής.

Πίνακας 2: Standards HF 13,56 MHz

	HF 13,56 MHz +/-7KHz	
ISO	**ISO 18092/ECMA 340**	it standardizes communication between two NFC devices
	ISO 21481/ECMA 352	This defines selection mechanism between different contactless technologies that operates on the same frequency 13.56Mhz.
	ISO/IEC 14443	Identification cards Contactless integrated circuit(s) cards. **Proximity cards** • Part 1: Physical characteristics • Part 2: Radio frequency power

ISO		and signal interface • Part 3:Initialization and Anti-collision • Part 4Transmission Protocol
	ISO/IEC 15693	Identification cards Contactless integrated circuit(s) cards **Vicinity cards** • Part 1: Physical characteristics • Part 2: Air interface and initialization • Part 3: Anti-collision and transmission protocol
	ISO/IEC 18000-3	Information Technology AIDC Techniques-RFID for Item Management Air Interface: • 18000-1 Part 1 – Generic Parameters for the Air Interface for Globally Accepted Frequencies

ISO		• 18000-2 Part 2 – Parameters for Air Interface Communications below 135 kHz • 18000-3 Part 3 – Parameters for Air Interface Communications at 13.56 MHz

3.3: NFC Forum Protocol stack

Η Stollmann NFC στοίβα πρωτοκόλλων "NFC Stack +" περιλαμβάνει το πλήρη ενδιάμεσο λογισμικό middleware για τα κύτταρα κινητής τηλεφωνίας, τα ενσωματωμένα προϊόντα και άλλες πλατφόρμες. Ως μια από τις πρώτες παγκοσμίως στοίβες πρωτόκολλων, υποστηρίζει όλες τις λειτουργίες που βασίζονται σε πρότυπα για τις προδιαγραφές NFC φόρουμ. Η λειτουργικότητα περιλαμβάνει επίσης συμβατότητα με έξυπνες κάρτες και ετικέτες με βάση τα Felica, MIFARE και ISO 14443:

- NFC LLCP (Logical Link Control Protocol)

Καθορίζει ένα στρώμα OSI-2 του πρωτοκόλλου για την υποστήριξη peer-to-peer επικοινωνίας μεταξύ δύο NFC-enabled συσκευών, η οποία είναι απαραίτητη για τις NFC εφαρμογές που περιλαμβάνουν αμφίδρομης επικοινωνίας. Η προδιαγραφή ορίζει δύο τύπους υπηρεσιών: **χωρίς σύνδεση** και **σύνδεση με προσανατολισμό**, που οργανώνονται σε τρεις κατηγορίες υπηρεσιών συνδέσεων:
σύνδεση χωρίς υπηρεσία, σύνδεση προσανατολισμένη προς τη υπηρεσία και **χωρίς υπηρεσία και προσανατολισμένη προς την υπηρεσία.σύνδεση**
Η Τρίτη κατηγορία είναι συνδυασμός των δύο πρώτων.

Η υπηρεσία χωρίς σύνδεση προσφέρει ελάχιστη ρύθμιση χωρίς εγγυήσεις αξιοπιστίας ή έλεγχο ροής (αναβάλλοντας αυτά τα ζητήματα στις εφαρμογές και στις

εγγυήσεις αξιοπιστίας που προσφέρονται από τα στρώματα της MAC του ISO/IEC 18092 και του ISO/IEC 14443).Η σύνδεση προσανατολισμένη προς την υπηρεσία προσθέτει την αίτηση την αξιόπιστη παράδοση, τον έλεγχο ροής και βασίζεται στην αρχή της πολυπλεξίας(multiplexing).

Το LLCP είναι ένα συμπαγές πρωτόκολλο, με βάση το βιομηχανικό πρότυπο IEEE 802.2, έχει σχεδιαστεί για να υποστηρίζει μικρές εφαρμογές με περιορισμένες απαιτήσεις μεταφοράς δεδομένων, όπως μικρές μεταφορές αρχείων ή δικτυακά πρωτόκολλα, όπως OBEX και TCP / IP, τα οποία με τη σειρά τους παρέχουν ένα πιο εύρωστο περιβάλλον για την εξυπηρέτηση των αιτήσεων. Το NFC LLCP προσφέρει μια σταθερή βάση για peer-to-peer εφαρμογές, ενισχύοντας τις βασικές λειτουργίες που προσφέρονται από το πρότυπο ISO / IEC 18092, χωρίς όμως να επηρεάζει τη διαλειτουργικότητα των εφαρμογών κληρονομιάς chipsets ή NFC.

- NFC HCI (under development)

Ο Host Controller Interface είναι μια λογική διεπαφή που επιτρέπει στην πρόσοψη μιας NFC συσκευής να επικοινωνεί άμεσα με έναν επεξεργαστή εφαρμογής και πολλαπλάσια ασφαλή στοιχεία στις διάφορες ηλεκτρονικές συσκευές όπως κύτταρα κινητής τηλεφωνίας, ή περιφερειακές μονάδες PDAs και PC, επιτρέποντας τη γρηγορότερη ολοκλήρωση της λειτουργίας NFC.

- NFC Data Exchange Format (NDEF) 1.0

Το απλό πρωτόκολλο ανταλλαγής NDEF εφαρμόζει το (SNEP) και επιτρέπει σε μια NFC συσκευή να ανταλλάξει μηνύματα τύπου(NDEF) με μια άλλη συσκευή NFC κατά τη λειτουργία του μοντέλου Peer to Peer

Το πρωτόκολλο χρησιμοποιεί τον τρόπο ελέγχου λογικών συνδέσεων του πρωτοκόλλου (LLCP) προσανατολισμένο προς τη σύνδεση για να παρέχει μια αξιόπιστη ανταλλαγή στοιχείων.

- NFC Record Type Definition (RTD 1.0)

Καθορίζει τη μορφή και τους κανόνες για τις τυποποιημένες εξ' ορισμού NFC εγγραφές αλλά και τις εφαρμογές τρίτων που είναι βασισμένες στη φόρμα NDEF. Η προδιαγραφή RTD παρέχει έναν τρόπο για να καθοριστούν αποτελεσματικά οι μορφές των εγγραφών για τις νέες εφαρμογές και δίνει στους χρήστες τη δυνατότητα να δημιουργήσουν τις δικές τους εφαρμογές με βάση τις προδιαγραφές NFC Forum.

- NFC Text Record Type Definition (RTD-Text 1.0)

Παρέχει έναν αποδοτικό τρόπο να αποθηκευτούν οι σειρές κειμένων σε πολλές γλώσσες με τη χρησιμοποίηση του μηχανισμού RDT και του σχήματος NDEF. Ένα παράδειγμα από τη χρήση αυτής της προδιαγραφής περιλαμβάνεται στο Smart Poster RTD

- NFC URI Record Type Definition (RTD-URI 1.0)

Παρέχει έναν αποτελεσματικό τρόπο για την αποθήκευση Uniform Resource Identifiers (URI), χρησιμοποιώντας τον μηχανισμό RTD και τη μορφή NDEF. Ένα παράδειγμα από τη χρήση αυτής της προδιαγραφής περιλαμβάνεται στο Smart Poster RTD.

- NFC Smart Poster Record Type Definition SPR 1.1

Καθορίζει ένα γνωστό τύπο στο NFC Forum για να θέτονται οι διευθύνσεις URL, τα γραπτά μηνύματα ή οι αριθμοί τηλεφώνων σε μία ετικέτα NFC, και τον τρόπο να μεταφέροντα μεταξύ των συσκευών. Το Smart Poster RTD βασίζεται στον μηχανισμό RTD και τη μορφή NDEF και χρησιμοποιεί το URI RTD και Κείμενο RTD ως δομικά στοιχεία.

- Card Emulation

Με τη λειτουργία που ονομάζεται «εξομοίωση κάρτας», μια συσκευή NFC μπορεί να επικοινωνεί με μια συσκευή ανάγνωσης RFID, διότι λειτουργεί ως μια κάρτα RFID.

Βασικά μια κάρτα RFID είναι παράδειγμα προς μίμηση από ένα MIDlet Java χρησιμοποιώντας Contactless API (JSR 257). Είναι σε θέση να έχουν πρόσβαση στο χώρο (είτε μιας κάρτα SIM, είτε μιας έξυπνης κάρτας, είτε μιας ασφαλής εσωτερικής μνήμη, ή μιας ασφαλής εξωτερικής μνήμη), όπου οι πληροφορίες αποθηκεύονται

3.4: Οργανισμοί τεχνολογίας NFC/RFID

3.4.1: NFC Forum/NFC Ecosystem

Το **NFC Forum** είναι μια μη κερδοσκοπική οργάνωση που ιδρύθηκε στις 18 Μαρτίου 2004 από την NXP Semiconductors, τη Sony και τη Nokia για την προώθηση της χρήσης του NFC Επικοινωνία Κοντινού Πεδίου Το φόρουμ NFC προωθεί την εφαρμογή και την τυποποίηση της τεχνολογίας NFC για να εξασφαλιστεί η διαλειτουργικότητα μεταξύ συσκευών και υπηρεσιών.

3.4.2 ISO

Ο **Διεθνής Οργανισμός Τυποποίησης** (**International Organization for Standardization**), είναι μια διεθνής οργάνωση δημιουργίας και έκδοσης προτύπων που αποτελείται από αντιπροσώπους των εθνικών οργανισμών τυποποίησης. Ο οργανισμός ιδρύθηκε στις 23 Φεβρουαρίου του 1947 και παράγει τα παγκόσμια βιομηχανικά και εμπορικά πρότυπα, τα επονομαζόμενα πρότυπα ISO.

Ενώ ο Διεθνής Οργανισμός Τυποποίησης ορίζεται από τον ίδιο ως μη κυβερνητική οργάνωση, η ικανότητα του να θέτει πρότυπα τα οποία αργότερα κυβερνήσεις αποφασίζουν πως πρέπει να τηρούνται δια νόμων ή συνθηκών, τον καθιστά πιο ισχυρό από άλλες μη κυβερνητικές οργανώσεις και στην πράξη λειτουργεί σαν μια κοινοπραξία με ισχυρούς συνδέσμους με κυβερνήσεις.
Μεταξύ αυτών που συμμετέχουν στον ISO, συγκαταλέγονται μεγάλες εταιρίες και τουλάχιστον ένα σωματείο προτυποποίησης από κάθε κράτος μέλος .Ο Διεθνής Οργανισμός Τυποποίησης συνεργάζεται στενά με την Διεθνή Ηλεκτροτεχνική Επιτροπή (International Electrotechnical Commission, IEC), η οποία είναι υπεύθυνη για την προτυποποίηση των ηλεκτρικών συσκευών

Η ISO/IEC Κοινή Τεχνική Επιτροπή
Για να αντιμετωπιστούν οι συνέπειες των ουσιαστικών αλληλοεπικαλύψεων σε θέματα προτυποποίησης και εργασίας σχετικά με την τεχνολογία της πληροφορίας, ο ISO και η Διεθνής Ηλεκτροτεχνική Επιτροπή (IEC) δημιούργησαν μία κοινή τεχνική επιτροπή γνωστή σαν ISO/IEC Κοινή Τεχνική Επιτροπή 1 (ISO/IEC Joint Technical Committee 1 -ISO/IEC JTC1). Ήταν η πρώτη επιτροπή τέτοιου είδους και ως σήμερα παραμένει η μόνη.
Οι αρμοδιότητές της, σύμφωνα με την επίσημη περιγραφή της, είναι η ανάπτυξη, συντήρηση, προώθηση και διευκόλυνση (διάδοσης) των προτύπων της Τεχνολογίας της Πληροφορίας (ΤΠ) που απαιτούνται εκεί όπου οι παγκόσμιες αγορές συναντούν τις επιχειρήσεις και τις απαιτήσεις των χρηστών και σχετίζονται με:

- και ανάπτυξη συστημάτων ΤΠ και εργαλείων.
- και ποιότητα των προϊόντων και συστημάτων ΤΠ.
- Ασφάλεια των συστημάτων ΤΠ και των πληροφοριών.
- Δυνατότητα μεταφοράς των προγραμμάτων εφαρμογών
- Διαλειτουργικότητα των προϊόντων και συστημάτων ΤΠ.

- Ενοποίηση των εργαλείων και περιβαλλόντων
- Εναρμόνιση λεξικού ΤΠ.
- Φιλικές προς τον χρήστη και εργονομικά σχεδιασμένες επαφές χρηστών (*user interface*)

3.4.3: EPC Global

Η EPC Global είναι μια μη κερδοσκοπική κοινοπραξία που ιδρύθηκε από το Uniform Code Council, αποτελείται από πολλούς διαφορετικούς φορείς και έχει στόχο την εμπορευματοποίηση των τεχνολογιών των ηλεκτρονικών προϊόντικών κωδικών (***Electronic Product Code -EPC***) και την ανάπτυξη προτύπων της τεχνολογίας RFID ώστε να βελτιωθεί η αποτελεσματικότητα και να περιορισθούν τα λάθη στην λειτουργία της εφοδιαστικής αλυσίδας.

Αυτό θα καταστεί δυνατό με την αυτοματοποίηση του εντοπισμού προϊόντων με την βοήθεια της τεχνολογίας RFID μέσω ενός παγκόσμιου δικτύου ανταλλαγής πληροφοριών. Η EPC global παρέλαβε την τεχνολογία του EPC από το Auto-ID Center, ένα κέντρο του MIT (Massachusetts Institute of Technology, Ινστιτούτο Τεχνολογίας της Μασαχουσέτης), που άρχισε από το 1999 να χρηματοδοτείται από το Uniform Code Council, την EAN International και κάποιες εταιρίες όπως η Gillette και η Procter & Gamble, με στόχο την ανάπτυξη ετικετών EPC μαζικής παραγωγής και χαμηλού κόστους.

EPC Global Network

Το EPC Global έχει ένα δίκτυο το οποίο επιτρέπει την αυτόματη αναγνώριση, σε πραγματικό χρόνο, αντικειμένων σε όλα τα στάδια της εφοδιαστικής αλυσίδας, ανεξαιρέτως κατασκευάστριας εταιρείας, οικονομικού τομέα και τοποθεσίας παγκοσμίως. Το EPC Global Network αποτελείται από:

1) Τον **Ηλεκτρονικό Κωδικό Προϊόντος (EPC): αποτελούμενος από 64-256 bits,** ο EPC είναι ένας μοναδικός αριθμός ταυτοποίησης προϊόντος σε επίπεδο τεμαχίου.

2) Το **Σύστημα Αναγνώρισης (ID System): αποτελούμενο από παθητικές RFID** ετικέτες που περιέχουν το EPC. Αυτό διαβάζεται από τους αναγνώστες NFC, και αποστέλλεται στα τοπικά πληροφοριακά συστήματα της

επιχείρησης μέσω του EPC λογισμικού (middleware).

3) Το **Λογισμικό EPC (EPC middleware): διαχειρίζεται γεγονότα ανάγνωσης** πραγματικού χρόνου και μεταβιβάζει τα δεδομένα που δέχεται στις Υπηρεσίες Πληροφοριών EPC και στα τοπικά πληροφοριακά συστήματα της επιχείρησης.

4) **Υπηρεσίες Πληροφοριών EPC (EPC Information Services): Οι Υπηρεσίες** Πληροφοριών EPC επιτρέπουν σε χρήστες την ανταλλαγή EPC δεδομένων με εμπορικούς συνεργάτες μέσω του EPC Global Network.

5) **Υπηρεσίες Ανακάλυψης (Discovery Services): Οι Υπηρεσίες Ανακάλυψης** επιτρέπουν σε χρήστες να αναζητήσουν παγκοσμίως και να αποκτήσουν πρόσβαση σε δεδομένα σχετικά με έναν συγκεκριμένο κωδικό EPC.

3.4.4 ETSI

Το **ευρωπαϊκό ινστιτούτο τηλεπικοινωνιακών προτύπων** (*European Telecommunications Standards Institute*) είναι ένας ανεξάρτητος αφιλοκερδής οργανισμός δημιουργίας και έκδοσης προτύπων στην βιομηχανία τηλεπικοινωνιών (κατασκευαστές εξοπλισμού και χείριστες δικτύων) στην Ευρώπη .Το ETSI πέτυχε στην προτυποποίηση του συστήματος κινητού τηλεφώνου (GSM) και του επαγγελματικού ραδιοσυστήματος (TETRA) επίσης ενέπνευσε την δημιουργία και είναι συνεργάτης στο 3 GPP.

Σημαντικά σώματα προτυποποίησης του ETSI, περιλαμβάνουν το: TISPAN (για σταθερά δίκτυα και σύγκλιση διαδικτύου) και το M2M (για επικοινωνία μηχανή προς μηχανή).Το ETSI δημιουργήθηκε το 1988 και αναγνωρίζεται επίσημα από την ευρωπαϊκή επιτροπή και την γραμματεία του EFTA. Με έδρα στην Sophia Antipolis (Γαλλία), είναι επίσημα υπεύθυνο για την προτυποποίηση τεχνολογιών πληροφορίας και επικοινωνιών (ICT) μέσα στην Ευρώπη.

Αυτές οι τεχνολογίες περιλαμβάνουν τηλεπικοινωνίες, αναμεταδόσεις και σχετικά πεδία, όπως τις μεταφορές πληροφοριών και τα ηλεκτρονικά ιατρικά. Το ETSI έχει 740 μέλη από 62 χώρες μέσα και έξω από την Ευρώπη και περιλαμβάνει κατασκευαστές, χειριστές δικτύων, διαχειριστές, παροχής υπηρεσιών ,ερευνητικά σώματα και χρηστές.

3.4.5 IEC

Η **διεθνής ηλεκτροτεχνική επιτροπή** είναι ένας μη κερδοσκοπικός, μη κυβερνητικός, οργανισμός διεθνών προτύπων, που προετοιμάζει και δημοσιεύει τα διεθνή πρότυπα για όλες τις ηλεκτρικές – ηλεκτρονικές και σχετικές τεχνολογίες .

Τα πρότυπα του IEC καλύπτουν ένα ευρύ φάσμα τεχνολογιών από την παραγωγή ισχύος, αναμεταδόσεις και διανομή σε οικιακές χρήσεις και εξοπλισμό γραφείου, ημιαγωγούς, οπτικές ίνες, μπαταριές ,ηλιακή ενέργεια, νανοτεχνολογία και πολλά άλλα.

Το IEC επίσης διαχειρίζεται τρία παγκόσμια συστήματα αξιολόγησης που πιστοποιούν το εάν ο εξοπλισμός, τα συστήματα, ή τα μέλη συμμορφώνονται με τα διεθνή πρότυπα. Το καταστατικό του IEC περιλαμβάνει όλες τις ηλεκτροτεχνολογίες, όπως την παράγωγη και διανομή ενέργειας, τις τηλεπικοινωνίες και τους γενικούς σχετικούς κλάδους, όπως η ορολογία και οι συμβολισμοί , η ηλεκτρομαγνητική συμβατότητα , η μέτρηση και η απόδοση, η αξιοπιστία και άλλα.

IEC ΠΡΟΤΥΠΑ

Τα IEC πρότυπα έχουν αριθμούς στην περιοχή 60000-79999 και οι τίτλοι τους παίρνουν μορφές όπως: IEC 60417. Η IEC συνεργάζεται στενά με τον Διεθνή Οργανισμό Τυποποίησης (ISO) και τη Διεθνή Ένωση Τηλεπικοινωνιών (ITU). Επιπλέον, συνεργάζεται με διάφορους μεγάλους οργανισμούς ανάπτυξης προτύπων, συμπεριλαμβανομένης της IEEE με την οποία υπέγραψε συμφωνία συνεργασίας το 2002, που τροποποιήθηκε το 2008 ώστε να συμπεριλάβει από κοινού εργασίες ανάπτυξης.

Πρότυπα που έχουν αναπτυχθεί από κοινού με το πρότυπο ISO όπως το ISO / IEC 26300, το Open Document Format για εφαρμογές του Office (Open Document) v1.0 φέρουν το ακρωνύμιο και των δύο οργανισμών.

Η χρήση του προθέματος ISO / IEC καλύπτει εκδόσεις από την Κοινή Τεχνική Επιτροπή ISO / IEC πάνω στην τεχνολογία πληροφόρησης, καθώς και τα πρότυπα αξιολόγησης της συμμόρφωσης που αναπτύχθηκαν από την ISO και την CASCO.

Σε άλλα πρότυπα που έχουν αναπτυχθεί σε συνεργασία μεταξύ της IEC και της ISO έχουν ανατεθεί αριθμοί της σειράς 80000, όπως το IEC 82045-1.Τα πρότυπα της IEC επίσης έχουν εγκριθεί ως εναρμονισμένα πρότυπα από άλλους οργανισμούς

πιστοποίησης, όπως η BSI (Μεγάλη Βρετανία), η CSA (Καναδάς), η UL & ANSI / INCITS (ΗΠΑ), η SABS (Νότια Αφρική), η οργάνωση SAI (Αυστραλία), SPC / GB (Κίνα) και η DIN (Γερμανία).

3.5: Κατασκευαστές της τεχνολογίας NFC

Οι περισσότεροι από τους κατασκευαστές της τεχνολογίας NFC είναι μέλη του NFC Forum η αλλιώς του NFC Ecosystem.Το NFC Ecosystem πρωτοεμφανίστηκε το 2004,ως ιδρυτικά μέλη αναφέρονται οι εταιρίες NXP Semiconductors, Philips, Nokia και Sony .Στις μέρες μας τοNFC Ecosystem αριθμοί πάνω από 150 μέλη-εταιρίες από όλο τον κόσμο. Τα μέλη χωρίζονται στις εξής κατηγορίες:**Sponsor Members, Principal Members, Associate Members, Non Profit Members[7]**

Εικόνα 13:Sponsor Members

Εικόνα 14:Principal Members

Εικόνα 15:Non-Profit Members

Εικόνα 16:Associate Members

ΚΕΦΑΛΑΙΟ 4

4: ΧΡΗΣΙΜΟΤΗΤΑ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ NFC-ΕΦΑΡΜΟΓΕΣ

4.1:Γενικά για τις εφαρμογές

Το NFC έχει πολύ μεγάλη χρησιμότητα στην καθημερινότητα και εφαρμόζεται σε πάρα πολλούς τομείς. Ο διαμοιρασμός αρχείων γίνεται με πάρα πολύ εύκολο τρόπο απλά ακουμπώντας την μια συσκευή με την άλλη. Η πληρωμή ενός λογαριασμού γίνεται εξίσου εύκολα ακουμπώντας τις συσκευές και πληκτρολογώντας το ποσό. Η σύνδεση multiplayer ανάμεσα σε δυο συσκευές εδραιώνεται πιο γρήγορα από ποτέ απλά ακουμπώντας τις δυο συσκευές. Υπάρχει η δυνατότητα να φέρουμε δυο συσκευές σε επαφή και οι χρήστες τους να γίνουν φίλοι στο Facebook ή να μοιραστούν κάτι κοινό ή την τοποθεσία όπου βρίσκονται. Ακόμη, μπορεί να χρησιμοποιηθεί στα μέσα μαζικής μεταφοράς, όπου θα υπάρχουν συστήματα πληρωμής με την τεχνολογία NFC και οι χρήστες θα περνάνε απλά τις συσκευές τους και θα αγοράζουν άμεσα και εύκολα το εισιτήριο. Επίσης μπορεί να χρησιμοποιηθεί για την άμεση σύνδεση δυο συσκευών όπως για παράδειγμα το Bluetooth και αντί να πρέπει να κάνουμε αναζήτηση να βρούμε την συσκευή που θέλουμε και να βάλουμε τον κωδικό απλά ακουμπάμε τις δυο συσκευές και κατευθείαν γίνεται η αποστολή του αρχείου. Όλο και περισσότερες διαδικασίες αξιοποιούν την τεχνολογία του NFC.[8]

4.2: Security NFC

Το σύστημα αποτελείται από τρία βασικά σημεία:

- NFC τηλέφωνο - συσκευές για τον έλεγχο της παρουσίας
- NFC ετικέτα - το σημείο ελέγχου για την εξακρίβωση της παρουσίας
- Λογισμικό για διαχείριση του συστήματος

Το λογισμικό για τη διαχείριση του συστήματος μπορεί να χρησιμοποιηθεί ως εφαρμογή web ή από το γραφείο. Έχει όλα τα εργαλεία για τη διαχείριση του συστήματος (ετικέτα, περιοχές, φρουροί, οδό και λειτουργία), καθώς και το έντυπο

για την επεξεργασία των δεδομένων και των εκθέσεων. Υπάρχουν δύο εκδόσεις (Basic και Pro).

Τα πλεονεκτήματα του:

- Το σύστημα λειτουργεί on-line (μεταφορά δεδομένων)
- Οι λειτουργίες του προγράμματος παρέχουν επιπλέον χαρακτηριστικά
- Κατεύθυνση (δρομολόγηση) των φρουρών μεταξύ των σημείων ελέγχου
- Καταγραφή των γεγονότων με επί τόπου φωτογραφίες και μηνυμάτων κειμένου (οπτική εξέταση)
- Την αλλαγή της ετικέτας NFC που υπάρχουν σε κάθε σημείο
- Κουμπί "άνθρωπος στο πάτωμα"
- Χρήση παρόμοιων εφαρμογών NFC στο ίδιο τηλέφωνο όπως η διαχείριση των παρουσιών
- Πολυλειτουργικότητα της συσκευής
- Τηλέφωνο, SMS, MMS
- Εγγραφή εικόνων, βίντεο και ήχων
- Χαμηλό κόστος συσκευής NFC
- Χαμηλό κόστος ετικετών NFC (περισσότερα σημεία ελέγχου)
- Απλότητα τοποθέτησης στα σημεία ελέγχου (αυτοκόλλητα)
- Αποτελεσματικό σύστημα back-office
- Ασφαλή πρόσβαση δεδομένων προστατευμένος με προηγμένα συστήματα

4.3:Ανίχνευση παρουσιών

Η τεχνολογία NFC προσφέρει μια νέα προσέγγιση για την καταχώρηση και τη διαχείριση της παρουσίας στο χώρο εργασίας. Οι εργαζόμενοι μπορούν να επιβεβαιώσουν την παρουσία τους στο χώρο εργασίας μέσα από ένα Tag NFC με τη βοήθεια ενός κινητού NFC. Το τηλέφωνο NFC μπορεί να χρησιμοποιηθεί ως τερματικός σταθμός για την ανίχνευση της παρουσίας, όταν οι εργαζόμενοι φτάνουν στο χώρο της δουλειά τους χρησιμοποιούν το τηλέφωνο NFC για την επικύρωση της ταυτότητας τους με το σήμα της τεχνολογίας NFC.

Πλεονεκτήματα:

- Χαμηλό κόστος εξοπλισμού
- Κινητικότητα του συστήματος
- Ο χρήστης έχει ένα σύστημα "με το κλειδί στο χέρι "
- Δυνατότητα συνεργασίας με απεριόριστο αριθμό πολύ μικρών περιοχών για την ανίχνευση παρουσιών
- Πλήρης αυτοματοποίηση του συστήματος χωρίς επιπλέον κόστος
- Δεν υπάρχουν έξοδα συντήρησης[9]

4.4: Ηλεκτρονικά εισιτήρια

Σε λειτουργία έχει τεθεί ήδη το σύστημα ηλεκτρονικής αγοράς και επικύρωσης εισιτηρίων στα χαρακτηριστικά, κόκκινα και διώροφα, λεωφορεία του Λονδίνου. Οι επιβάτες στα περίπου 8.500 λεωφορεία της βρετανικής πρωτεύουσας μπορούν πλέον να αγοράζουν και να επικυρώνουν εισιτήρια, χρησιμοποιώντας τις πιστωτικές και χρεωστικές τους κάρτες. Έξυπνες συσκευές κινητής τηλεφωνίας, που μπορούν να "μιμηθούν" με τη χρήση barcodes τη λειτουργία πιστωτικών και χρεωστικών καρτών, θα γίνονται επίσης δεκτές από το σύστημα. Ωστόσο, οι επιβάτες που διαθέτουν στο πορτοφόλι τους περισσότερες από μια κάρτες NFC, οφείλουν να προσέχουν κατά τη διάρκεια της ηλεκτρονικής "ανάγνωσης" από τα μηχανήματα. Ο λόγος είναι ότι λογικά το σύστημα θα απορρίψει και τις δύο κάρτες, αδυνατώντας να «διαβάσει» καθαρά κάποια από αυτές.

4.5: NFC και εκπαίδευση

Πρόκειται για τον αυτοματισμό των διαδικασιών σε σχολικά ή ακαδημαϊκά συγκροτήματα με στόχο τη βελτίωση της ασφάλειας, την καταγραφή των κινήσεων μαθητών και προσωπικού και τη διευκόλυνση κάθε μορφής καθημερινών λειτουργιών.

Ο τρόπος λειτουργίας της είναι απλός. Οι μαθητές και το προσωπικό λαμβάνουν τα προσωπικά NFC "SofTouch" Tags (π.χ. σε μορφή κάρτας ή ειδικό βραχιόλι). Ακουμπώντας την κάρτα ή το βραχιόλι σε μία συσκευή NFC κινητού τηλεφώνου ή άλλον αναγνώστη, οι μαθητές δηλώνουν την παρουσία τους στο μάθημα, την επιβίβασή τους στο σχολικό, εγγράφονται σε μαθήματα, λαμβάνουν πρόσβαση σε χώρους ή παρεχόμενες υπηρεσίες εντός του συγκροτήματος και δηλώνουν την ταυτότητά τους στο προσωπικό ασφαλείας κατά τη διάρκεια ελέγχων. Κατά τον ίδιο τρόπο, το προσωπικό του ιδρύματος δηλώνει την παρουσία του και αποκτά πρόσβαση σε ελεγχόμενους χώρους.

Οι κάτοχοι των συγκεκριμένων καρτών (μαθητές, καθηγητές, προσωπικό) μπορούν προαιρετικά να συμμετέχουν και σε ένα σύστημα «ηλεκτρονικού πορτοφολιού», μέσω του οποίου μεταφέρουν μικροποσά στην "SofTouch" κάρτα τους και μπορούν κατόπιν να τη χρησιμοποιήσουν για πληρωμές χωρίς μετρητά σε σημεία πώλησης εντός του συγκροτήματος. Το σύστημα ηλεκτρονικών συναλλαγών αυτών βελτιώνει την ασφάλεια στις συναλλαγές και διασφαλίζει ότι τα χρήματα θα ξοδευτούν μόνο σε καθορισμένα προϊόντα ή υπηρεσίες που παρέχονται εντός του ελεγχόμενου περιβάλλοντος του συγκροτήματος.

Στις δυνατότητες του συστήματος περιλαμβάνονται η έκδοση ή ανανέωση καρτών (π.χ. κατά την εγγραφή σε κάθε ακαδημαϊκό έτος), η καταγραφή παρουσίας καθηγητών και μαθητών, ο έλεγχος ασφαλείας σε όλο το συγκρότημα και σε περιοχές περιορισμένης πρόσβασης, η ευκολία στην πρόσβαση και καταγραφή χρήσης των υπηρεσιών και παροχών (π.χ. βιβλιοθήκη, αθλητικές εγκαταστάσεις κ.λπ.). Ακόμη προβλέπεται δυνατότητα πρόσβασης σε προσωποποιημένη πληροφόρηση και υπηρεσίες μέσω info-kiosks, ηλεκτρονικό πορτοφόλι (e-Purse) με χρήση των καρτών

ως μέσο πληρωμής σε διάφορα σημεία πώλησης, Online παρακολούθηση δραστηριότητας των μαθητών, σε πραγματικό χρόνο, πλήρης Στατιστική ανάλυση και παραγωγή αναφορών on-line και άμεση ειδοποίηση υπευθύνων ασφαλείας και γονέων, σε περίπτωση έκτακτης ανάγκης[10]

4.6:Ηλεκτρονικη ταυτότητα

Πρόκειται για την ανάπτυξη και εγκατάσταση μιας πληθώρας λύσεων διαχείρισης μητρώων για ιδιωτικούς και δημόσιους οργανισμούς βασισμένων στην τεχνολογία NFC.

Οι **τομείς εφαρμογής** των λύσεων ταυτότητας που παρέχονται περιλαμβάνουν:

- Οργανισμούς δημοσίου τομέα (π.χ. μητρώα πολιτών, μητρώα πρόνοιας)
- Επιχειρησιακό περιβάλλον (π.χ. μητρώα εργαζομένων, ανθρώπινο δυναμικό, πελατειακές λίστες)
- Τομείς υγείας και ασφάλισης (π.χ. μητρώα ασθενών, προσωπικές κάρτας ασφάλισης)
- Συλλόγους και Σωματεία (π.χ. μέλη αθλητικών σωματείων και ομοσπονδιών)
- Marketing, πελατειακή πίστη, προώθηση προϊόντων και υπηρεσιών (π.χ. μέλη προγραμμάτων loyalty, λίστες επικοινωνίας.

Οι λύσεις ταυτότητας που παρέχονται διακρίνονται για τα ακόλουθα **χαρακτηριστικά**:

- Ευέλικτη, επεκτάσιμη σχεδίαση βάσης δεδομένων, με αξιοποίηση του γενικού υποσυστήματος 'Identity Management module'
- Δικτυακές διεπαφές χρηστών, για άμεση εγκατάσταση και ευκολία στη χρήση
- Προσωποποιημένες contact και contactless κάρτες ταυτότητας (Smart Cards), tokens και fobs, ανάλογα με την εφαρμογή
- Μηχανισμοί καταγραφής και παρακολούθησης παρουσίας και συναλλαγών, μέσω ταυτοποίησης προσωποποιημένων μέσων αναγνώρισης (ID media) από σταθερούς ή φορητούς αναγνώστες

- Ασφαλής μεταφορά και αποθήκευση ευαίσθητων πληροφοριών από άκρη σε άκρη, από το σύστημα διαχείρισης βάσεων δεδομένων μέχρι το μέσο ταυτοποίησης του ατόμου.
- Διαλειτουργικότητα με σταθερά τερματικά, POS, και φορητές συσκευές, σε συμφωνία με τα διεθνή πρότυπα.[11]

ΚΕΦΑΛΑΙΟ 5

5: ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΣΕ NFC ΣΥΣΤΗΜΑΤΑ

5.1:Γενικα περί ασφάλειας

Μιας και ένα σύστημα NFC ανήκει στο γενικότερο πλαίσιο των RFID συστημάτων θα γίνει εκτενής αναφορά σε θέματα ιδιωτικότητας και ασφάλειας στην RFID τεχνολογία. Τα θέματα αυτά αναδεικνύονται από το γεγονός ότι οι άνθρωποι δεν μπορούν να αντιληφθούν την RF ακτινοβολία που χρησιμοποιείται για την ανάγνωση των tags και επιπλέον τα tags δεν κρατούν ιστορικό του τι διαβάστηκε και από ποιόν. Ως αποτέλεσμα, τα tags μπορούν να διαβαστούν από οντότητες διαφορετικές από αυτές των κατόχων τους και χωρίς οι κάτοχοι τους να έχουν επίγνωση.

Πιο συγκεκριμένα, το θέμα της ασφάλειας των συστημάτων και της αυθεντικοποίησης στο RFID, αφορά το πρόβλημα καλώς συμπεριφερόμενων readers τα οποία διαβάζουν πληροφορίες κακόβουλων tags, ειδικότερα πλαστών. Μέχρι πρόσφατα δεν διαφαινόταν να υπάρχει κίνδυνος αντιγραφής ενός tag αλλά ειδικοί απέδειξαν σημαντικές αδυναμίες ασφάλειας όπως η αντιγραφή ενός διαβατηρίου νέας γενιάς ή ενός συστήματος immobilizer με μη εξειδικευμένο χαμηλού κόστους εξοπλισμό.

Από την άλλη, η ιδιωτικότητα στο RFID αφορά το πρόβλημα κακόβουλων readers που διαβάζουν πληροφορίες από tags στα οποία δεν έχουν εξουσιοδότηση. Οι περισσότεροι κίνδυνοι παραβίασης της προσωπικής ζωής των πολιτών προκύπτουν από το γεγονός ότι τα tags με τη μοναδικότητα του σειριακού αριθμού τους, μπορούν εύκολα να συσχετιστούν με τη ταυτότητα ενός ατόμου.

5.2:Κίνδυνοι

Κίνδυνος παρακολούθησης των κινήσεων ενός ατόμου. Μπορεί να βγει ένα συμπέρασμα για τη συμπεριφορά ενός ατόμου με βάση τα δεδομένα που λαμβάνεται από μια ομάδα tags

Κίνδυνος συσχέτισης. Όταν ένας πελάτης αγοράσει ένα προϊόν το οποίο φέρει ένα tag, η ταυτότητα αυτού του ατόμου μπορεί να συσχετιστεί με τον ηλεκτρονικό σειριακό αριθμό του αντικειμένου.

Κίνδυνος αποκάλυψης θέσης. Άτομα τα οποία φέρουν ένα tag μοναδικού σειριακού αριθμού μπορεί να παρακολουθούνται στο χώρο και η τοποθεσία τους να φανερώνεται, με την προϋπόθεση αυτός που κάνει την παρακολούθηση να γνωρίζει την αντιστοιχία ατόμου με tag.

Κίνδυνος αποκάλυψης προτιμήσεων. Επιπλέον το tag σε ένα αντικείμενο φανερώνει τον κατασκευαστή, τον τύπο του, την μοναδική ταυτότητα του αλλά και την τιμή του. Αυτό αποκαλύπτει τις προτιμήσεις του πελάτη σε ανταγωνιστικές εταιρίες ή άλλα αδιάκριτα άτομα.

Κίνδυνος κατηγοριοποίησης ανθρώπων. Κάποιοι μπορούν να κατηγοριοποιήσουν τα άτομα σε διάφορες ομάδες με βάση τα tags που φέρουν, και να τα εντοπίσουν χωρίς καν να γνωρίζουν την ταυτότητα τους.

Κίνδυνος αποκάλυψης συναλλαγών. Όταν ένα αντικείμενο που φέρει tag αλλάξει ομάδα μπορεί κάποιος να συμπεράνει μια συναλλαγή μεταξύ των ατόμων που συσχετίζονται με αυτές τις ομάδες.

Κίνδυνος απαρχαιωμένων στοιχείων. Οι καταχωρήσεις που αφορούν ένα άτομο σε μια βάση δεδομένων δεν ενημερώνονται όταν το άτομο αποκόπτεται από το προϊόν που φέρει το tag άλλα το συσχετίζουν εφόρου ζωής με αυτόν με αποτέλεσμα σε πολλές περιπτώσεις να εξάγονται λάθος συμπεράσματα για το άτομο αυτό.

5.3 Τεχνικές επιθέσεων

Ακολουθούν μερικές από τις **τεχνικές επιθέσεων**, που μέχρι σήμερα έχουν εντοπισθεί, κατά των συγκεκριμένων συστημάτων και οι οποίες έχουν ως αποτέλεσμα τη δημιουργία προβλημάτων ασφάλειας και ιδιωτικότητας

5.3.1: Υποκλοπές (Eavesdropping)

Επειδή το NFC είναι σύστημα ασύρματης επικοινωνίας είναι προφανές ότι οι υποκλοπές είναι ένα σημαντικό ζήτημα. Όταν δύο συσκευές επικοινωνούν μέσω NFC χρησιμοποιούν RF κύματα για να μιλήσουν ο ένας στον άλλο. Ένας εισβολέας μπορεί φυσικά να χρησιμοποιήσει μια κεραία για να λάβει επίσης τα μεταδιδόμενα σήματα. Είτε με πειραματισμό είτε με βιβλιογραφική έρευνα, ο εισβολέας μπορεί να έχει τις απαιτούμενες γνώσεις για το πώς να εξαγάγει τα δεδομένα που μεταδίδονται από το λαμβανόμενο σήμα RF. Επίσης, ο εξοπλισμός που απαιτείται για να λάβει το σήμα RF, καθώς και ο εξοπλισμός για να αποκωδικοποιήσει το σήμα RF, πρέπει να θεωρούνται ότι είναι διαθέσιμα σε έναν εισβολέα, καθώς δεν είναι απαραίτητος κάποιος εξειδικευμένος τεχνικός

Η επικοινωνία NFC γίνεται συνήθως μεταξύ δύο συσκευών σε στενή γειτνίαση. Αυτό σημαίνει ότι δεν είναι περισσότερο από 10 cm (τυπικά λιγότερο) μακριά ο ένας από τον άλλο. Το βασικό ερώτημα είναι πόσο κοντά ένας εισβολέας θα πρέπει να είναι για να είναι σε θέση να ανακτήσει ένα χρησιμοποιήσιμο σήμα RF. Δυστυχώς, δεν υπάρχει σωστή απάντηση στο ερώτημα αυτό. Ο λόγος για αυτό είναι ο τεράστιος αριθμός των παραμέτρων που καθορίζουν την απάντηση. Για παράδειγμα, η απόσταση εξαρτάται από τις ακόλουθες παραμέτρους, και υπάρχουν πολλά περισσότερα.

- Το RF αρχειοθετεί το χαρακτηριστικό της δεδομένης συσκευής αποστολέων (δηλ. γεωμετρία κεραιών, που προστατεύει από την επίδραση της παραπάνω περίπτωσης, το PCB, το περιβάλλον
- Χαρακτηριστικό της κεραίας του επιτιθεμένου (δηλ. γεωμετρία κεραιών, δυνατότητα να αλλαχτεί η θέση και σε στις 3 διαστάσεις)
- Ποιότητα του δέκτη του επιτιθεμένου
- Ποιότητα του αποκωδικοποιητή σημάτων RF του επιτιθεμένου
- Οργάνωση της θέσης από όπου η επίθεση εκτελείται (π.χ. εμπόδια όπως τοίχοι ή μέταλλα, επίπεδο θορύβου)
- Η ισχύς που στέλνεται από την συσκευή NFC

Επομένως οποιοσδήποτε ακριβής αριθμός δίνεται ισχύει μόνο για ένα ορισμένο σύνολο των ανωτέρω δεδομένων παραμέτρων και δεν μπορεί να χρησιμοποιηθεί για να παραγάγει τις γενικές οδηγίες ασφάλειας.

Επιπλέον, μείζονος σημασίας θέμα είναι σε ποιο τρόπο ο αποστολέας των στοιχείων λειτουργεί. Αυτό σημαίνει εάν ο αποστολέας δημιουργεί το δικό του πεδίο RF (Active Mode) ή εάν ο αποστολέας χρησιμοποιεί τον τομέα RF που παράγεται από μια άλλη συσκευή (Passive Mode). Και οι δύο περιπτώσεις χρησιμοποιούν έναν διαφορετικό τρόπο για τα στοιχεία και είναι πολύ πιο δύσκολο να υποκλαπούν οι συσκευές που στέλνουν τα στοιχεία στον παθητικό τρόπο.

5.3.2:Αλλοίωση δεδομένων (Data Corruption)

Ένας επιτιθέμενος μπορεί επίσης να προσπαθήσει να τροποποιήσει το στοιχείο που διαβιβάζεται μέσω της διεπαφής NFC. Στην απλούστερη περίπτωση ο επιτιθέμενος θέλει ακριβώς να ενοχλήσει την επικοινωνία έτσι ώστε ο δέκτης να μην είναι ικανός να καταλάβει τα στοιχεία που στέλνονται από την άλλη συσκευή. Η δωροδοκία στοιχείων μπορεί να επιτευχθεί με τη διαβίβαση των έγκυρων συχνοτήτων του φάσματος στοιχείων σε έναν σωστό χρόνο. Ο σωστός χρόνος μπορεί να υπολογιστεί εάν ο επιτιθέμενος έχει μια καλή κατανόηση του χρησιμοποιημένου σχεδίου διαμόρφωσης και την κωδικοποίηση. Αυτή η επίθεση δεν είναι πάρα πολύ περίπλοκη, αλλά δεν επιτρέπει στον επιτιθέμενο να χειριστεί τα πραγματικά στοιχεία. Είναι βασικά μια άρνησης υπηρεσιών (Denial of Service attack.

5.3.3: Τροποποίηση δεδομένων (Data modification)

Στην τεχνική αυτή ο επιτιθέμενος θέλει ο δέκτης να λάβει τροποποιημένα στοιχεία και όχι τα πραγματικά στοιχεία που μεταδόθηκαν από τον αποστολέα.

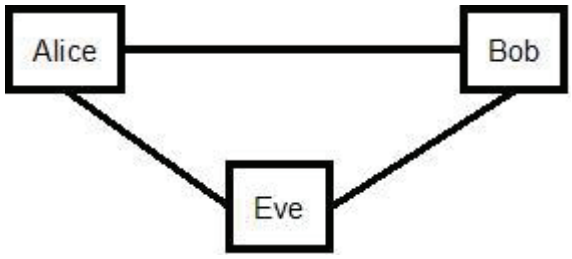
Η δυνατότητα πραγματοποίησης αυτής της επίθεσης εξαρτάται ιδιαίτερα από τη δύναμη της εφαρμοσμένη διαμόρφωσης εύρους. Αυτό είναι επειδή η αποκωδικοποίηση του σήματος είναι διαφορετική για τη διαμόρφωση 100% και 10%.

5.3.4: Εισαγωγή δεδομένων

Αυτό σημαίνει ότι ο επιτιθέμενος παρεμβάλλει τα μηνύματα στην ανταλλαγή στοιχείων μεταξύ δύο συσκευών. Αλλά αυτό είναι μόνο δυνατό, σε περίπτωση που η συσκευή δέκτης χρειάζεται πολύ χρόνο για να απαντήσει. Ο επιτιθέμενος θα μπορούσε να στείλει τα στοιχεία του νωρίτερα από τον έγκυρο δέκτη. Η εισαγωγή θα είναι επιτυχής, μόνο, αν τα εισαχθέντα δεδομένα μεταδοθούν, πριν από η αρχική συσκευή ξεκινήσει την απάντηση. Αν συμπίπτουν οι δύο ροές δεδομένων, τα δεδομένα θα καταστραφούν.

5.3.5: Man-in-the-Middle-Attack (Ενδιάμεσος)

Στην κλασική Man-in-the-Middle Attack, δύο άτομα που θέλουν να μιλήσουν ο ένας στον άλλο, πχ Alice και Bob, παρασύρθηκαν σε τριμελή συζήτηση με την Εύα εισβολέα.



Εικόνα 17: Man-in the Middle Attact

Η Alice και ο Bob δεν είναι ενήμεροι για το γεγονός ότι δεν μιλάμε ο ένας στον άλλο, και πως και οι δύο δέχονται δεδομένα από την Εύα. Μια τέτοια επίθεση είναι η κλασική απειλή χωρίς έλεγχο ταυτότητας σε βασικά πρωτόκολλα συμφωνίας, όπως Diffie-Hellmann. Η Alice και ο Bob θέλουν να συμφωνήσουν σχετικά με ένα μυστικό κλειδί, το οποίο στη συνέχεια χρησιμοποιούν για ένα ασφαλές κανάλι. Ωστόσο, όπως η Εύα είναι στη μέση, είναι δυνατόν για την Εύα να δημιουργήσει ένα κλειδί για την Αλίκη και ένα άλλο κλειδί για τον Bob. Όταν η Alice και ο Bob χρησιμοποιούν αργότερα το κλειδί τους για την εξασφάλιση δεδομένων, η Εύα είναι σε θέση να παρακολουθεί την επικοινωνία και την διαχείριση των δεδομένων που μεταφέρονται.

Πώς θα λειτουργήσει όταν η σχέση μεταξύ της Alice και του Bob είναι μια NFC σύνδεση; Αν υποθέσουμε ότι η Alice χρησιμοποιεί ενεργή λειτουργία και ο Bob

είναι σε παθητική κατάσταση, έχουμε την εξής κατάσταση. Η Alice δημιουργεί το RF πεδίο και στέλνει δεδομένα στον Bob. Σε περίπτωση που η Εύα είναι αρκετά κοντά, μπορεί να αφουγκράζομαι τα δεδομένα που αποστέλλονται από την Alice. Επιπλέον, η Εύα πρέπει να διαταράξει ενεργά τη μετάδοση της Αλίκης για να βεβαιωθεί ότι ο Bob δεν λαμβάνει τα δεδομένα. Αυτό είναι δυνατό για την Εύα, αλλά μπορεί να ανιχνευθεί από την Alice. Σε περίπτωση που η Alice ανιχνεύει τη διαταραχή, μπορεί να σταματήσει το βασικό πρωτόκολλο συμφωνίας. Ας υποθέσουμε Αλίκη δεν ανιχνεύει τη διαταραχή και έτσι το πρωτόκολλο μπορεί να συνεχιστεί. Στο επόμενο βήμα θα πρέπει η Εύα να στείλει δεδομένα στον Bob. Αυτό είναι ήδη ένα πρόβλημα, επειδή το RF πεδίο που παράγεται από την Alice είναι ακόμα εκεί, και έτσι η Εύα πρέπει να δημιουργήσει ένα δεύτερο πεδίο RF. Αυτό ωστόσο, προκαλεί δύο πεδία RF να είναι ενεργά την ίδια στιγμή. Είναι πρακτικά αδύνατο να ευθυγραμμίζονται πλήρως αυτά τα δύο πεδία ραδιοσυχνοτήτων. Έτσι, είναι σχεδόν ακατόρθωτο για τον Bob να κατανοήσει τα δεδομένα που αποστέλλονται από την Εύα. Γι 'αυτό και η δυνατότητα της Alice για την ανίχνευση της επίθεσης πολύ νωρίτερα καταλήγοντας στο συμπέρασμα ότι σε αυτό το σκηνικό μια Man-in-the-Middle επίθεση είναι πρακτικά αδύνατη.

Η μόνη άλλη περίπτωση είναι ότι η Alice είναι σε Active Mode λειτουργία και Bob επίσης Σε αυτή την περίπτωση Alice στέλνει κάποια δεδομένα στον Bob. Η Εύα μπορεί να απαριθμήσει και πάλι τα στοιχεία και πρέπει πάλι να διαταράξει τη μετάδοση της Alice για να βεβαιωθεί ότι ο Bob δεν λαμβάνει τα δεδομένα. Σε αυτό το σημείο θα μπορούσε να ανιχνεύσει η Alice τη διαταραχή που ήδη γίνεται από την Εύα και να σταματήσει το πρωτόκολλο.

Και πάλι, ας υποθέσουμε ότι η Alice δεν κάνει αυτόν τον έλεγχο και το πρωτόκολλο συνεχίζει. Στο επόμενο βήμα Εύα θα πρέπει να στείλει τα δεδομένα στον Bob. Εκ πρώτης όψεως αυτό φαίνεται καλύτερα τώρα, λόγω μοντέλου της δραστικής ενεργής επικοινωνίας η Alice έχει απενεργοποιήσει το RF πεδίο. Τώρα Εύα γυρίζει στο πεδίο RF και μπορεί να στείλει τα δεδομένα. Το πρόβλημα είναι ότι τώρα επίσης η Alice ακούει δεδομένου ότι αναμένει μια απάντηση από τον Bob. Αντί αυτού θα λάβει τα δεδομένα που αποστέλλονται από την Εύα και πάλι μπορεί να ανιχνεύσει ένα πρόβλημα στο πρωτόκολλο και να σταματήσει το πρωτόκολλο. Είναι αδύνατο σε αυτό το σκηνικό για την Εύα να στείλει τα δεδομένα είτε σε Alice ή Bob και να

διασφαλίσουμε ότι αυτά τα δεδομένα δεν λαμβάνονται από Bob ή Alice αντίστοιχα.[12]

5.4 Τρόποι επίλυσης προβλημάτων

Για τα προβλήματα και τους κινδύνους των συστημάτων RFID γενικά έχουν προταθεί διάφοροι τρόποι επίλυσής τους:

- **Καταστροφή των tags** κατά την αγορά τους, μέσω ενός kill command, ή αφαίρεση της ετικέτας χειροκίνητα όπου αυτό επιτρέπεται. Σαν μέτρο αποφυγής κακόβουλων kill commands απαιτείται ο reader που θα αποστείλει το kill command να έχει μεταδώσει και συγκεκριμένο PIN, το οποίο θα επαληθεύσει την ενέργεια αυτή. Η πρόταση της καταστροφή των tags, εξαλείφει όλα τα πλεονεκτήματα του RFID που μπορεί να αξιοποιήσει ο καταναλωτής. Για τα επαναχρησιμοποιήσιμα tags μία πρόταση είναι η απενεργοποίηση τους μέσω κάποιας sleep command και η ενεργοποίηση τους με κάποια wake up command, κάτι που όμως περικλείει προβλήματα αυθεντικοποίησης των readers ή διαχείρισης κωδικών.

- Η ασφάλεια των tags μπορεί ακόμα να επιτευχθεί με χρήση απλών υλικών από μέταλλο τα οποία μπλοκάρουν και διαχέουν την RF ακτινοβολία, για παράδειγμα μια κονσέρβα ή 27mm περιτύλιγμα με αλουμινόχαρτο είναι ικανά να θωρακίσουν το tag. Επίσης υλικά με υγρότητα απορροφούν τα RFID σήματα, για παράδειγμα 1mm περίβλημα θαλασσινού νερού έχει το ίδιο αποτέλεσμα. Ακόμα και τα πλαστικά αλλά και κάθε αγώγιμο υλικό έχει σαν αποτέλεσμα την αποδυνάμωση του σήματος της κεραίας, για παράδειγμα ένα tag μέσα σε μια ανθρώπινη γροθιά θα μπορούσε ίσως να αποτρέψει την ικανότητα ανάγνωσης του. Τέλος μπορεί να αποτραπεί πλήρως η λήψη ενέργειας από ένα tag αν απλώς τοποθετηθεί μέσα σε ένα κλωβό

Faraday ενώ παρομοίως μπορεί να αποτραπεί η επιτυχής αποστολής σημάτων από έναν reader αν αυτός τοποθετηθεί σε μία τέτοιου είδους περίφραξη η οποία εμποδίζει τα ηλεκτρομαγνητικά κύματα, όπως είναι ο κλωβός Faraday.[13]

- **Χρήση κρυπτογράφησης** κατά την επικοινωνία μεταξύ tag και reader. Σε αυτή την περίπτωση υφίσταται το πρόβλημα της διαχείρισης των κλειδιών καθώς και της κατακόρυφης αύξησης του κόστους των tags, προκειμένου αυτά να εκτελούν δυναμικές λειτουργίες κρυπτογράφησης

- **Χρήση κωδικών πρόσβασης** στο tag για την εξουσιοδοτημένη χρήση του. Απαραίτητη είναι η επίλυση του προβλήματος της διαχείρισης των κωδικών. Επιπλέον παράδοξο για κάποιες περιπτώσεις εφαρμογών είναι το γεγονός ότι ο reader συνήθως δε ξέρει ποιον κωδικό να μεταδώσει σε κάποιο tag παρά μόνο εάν ξέρει την ταυτότητα του.

- **Χρήση πολλών εναλλασσόμενων ψευδωνύμων** με σκοπό την αντικατάσταση της παρουσίας ενός μοναδικού σειριακού αριθμού του tag με άλλους τυχαίους ή μη ανιχνεύσιμους αριθμούς.
- **Χρήση blocker tags**, τα οποία μπλοκάρουν τους μη εξουσιοδοτημένους readers προσομοιώνοντας πολλά tags ταυτόχρονα. Ο κίνδυνος εξελιγμένοι readers να είναι ικανοί να φιλτράρουν επιτυχώς τα σήματα του blocker tag είναι υπαρκτός

- **Χρησιμοποιώντας ένα επιπλέον κύκλωμα**, ένα tag μπορεί να κάνει μια (σήμα προς θόρυβο) ανάλυση, ώστε να προσδιορίσει την απόσταση του reader και ανάλογα να ορίσει τη συμπεριφορά του. Η τεχνική αυτή δεν είναι επαρκής για να εγγυηθεί κάτι, αλλά είναι συμπληρωματική των προαναφερθέντων τεχνικών

- **Proxying προσέγγιση**. Χρήση προσωπικών συσκευών αυτοπροστασίας από αναγνώστες RFID για διαφύλαξη της ιδιωτικότητας, όπως για παράδειγμα το "Watchdog Tag", μία συσκευή παρακολούθησης και ελέγχου της RFID δραστηριότητας ή το "RFID

Guardian", μία συσκευή που λειτουργεί σαν κάποιο είδος RFID firewall.[14]

ΚΕΦΑΛΑΙΟ 6

6:ΣΥΓΚΡΙΣΗ ΤΟΥ NFC ΜΕ ΤΑ ΗΔΗ ΥΠΑΡΧΟΝΤΑ ΑΣΎΡΜΑΤΑ ΣΥΣΤΗΜΑΤΑ

6.1:Σύγκριση με Bluetooth

Το NFC και το Bluetooth είναι τεχνολογίες υψηλής συχνότητας ασύρματης επικοινωνίας μικρής εμβέλειας που περιλαμβάνονται σε ηλεκτρονικές συσκευές για εύκολη και ασφαλή αλληλεπίδραση ανάμεσα σε δύο ηλεκτρονικές συσκευές. Το NFC είναι μία τεχνολογία ασύρματης σύνδεσης η οποία μπορεί να χρησιμοποιηθεί για μια αμφίδρομη αλληλεπίδραση ανάμεσα σε ηλεκτρονικές συσκευές εντός κάποιων εκατοστών. Το Bluetooth είναι επίσης μία ασύρματη τεχνολογία η οποία σχεδιάστηκε για την αλληλεπίδραση μεταξύ των συσκευών επικοινωνίας εντός 10 μέτρων εμβέλειας χωρίς φυσική σύνδεση.

Το NFC εδραιώνει μια σύνδεση πιο γρήγορα από το κανονικό Bluetooth, αλλά όχι πιο γρήγορα από το Bluetooth χαμηλής ενέργειας. Αυτό συμβαίνει διότι το NFC εδραιώνει αυτόματα μια σύνδεση ανάμεσα σε δυο συσκευές σε λιγότερο από ένα δέκατο του δευτερολέπτου. Ο μέγιστος ρυθμός μεταφοράς δεδομένων για το NFC είναι 424 Kbit/s, και είναι πολύ ποιο αργό από το Bluetooth που στις πρώτες του εκδόσεις ήταν 2,1 Mbit/s.

Το NFC απαιτεί ωστόσο λιγότερη ενέργεια υπό κανονικές συνθήκες, ενώ όταν δουλεύει με μία μη τροφοδοτούμενη με ρεύμα συσκευή όπως για παράδειγμα μια έξυπνη πιστωτική κάρτα, τότε η κατανάλωση ενέργειας ανεβαίνει. Το NFC βασίζεται στην επαγωγική ζεύξη, όπου τα αόριστα συνδεδεμένα επαγωγικά κυκλώματα μπορούν να χρησιμοποιηθούν για να μοιράζουν ενέργεια και δεδομένα ανάμεσα σε δύο συσκευές σε πολύ μικρή απόσταση. Το Bluetooth είναι ένα ιδιόκτητο πρωτόκολλο για μικρής εμβέλειας επικοινωνία με υψηλό επίπεδο ασφαλείας. Αναπτύχθηκε από την Telecom Vendor Ericsson. Λειτουργεί στη συχνότητα ISM (2,4 GHz)[12].

	NFC	Bluetooth	Bluetooth Low Energy
Συμβατό με RFID	ISO/18000-3	Ενεργό	Ενεργό
Οργανισμός Τυποποίησης	ISO/IEC	Bluetooth SIG	Bluetooth SIG
Πρότυπο Δικτύου	ISO 13157	IEE 802.15.1	IEE 802.15.1
Τύπος Δικτύου	Point to Point	WPAN	WPAN
Κρυπτογράφηση	Όχι με το RFID	Διαθέσιμη	Διαθέσιμη
Εμβέλεια	<0,2m	~10 m (Κλάση2)	~100 m
Συχνότητα	13,56 MHz	2,4-2,5 GHz	2,4-2,5 GHz
Ρυθμός Δεδομένων(Bits/Sec)	424 Kbit/sec	2,1 Mbit/sec	~1,0 Mbit/sec
Χρόνος Προετοιμασίας	<0,1.sec	<6 sec	<0,006 sec
Κατανάλωση Ενέργειας	<15mA Ανάγνωση	Εξαρτάται από την Κλάση	<15mA Ανάγνωση

Εικόνα 18:Πίνακας-Σύγκριση NFC-Bluetooth

6.2: Σύγκριση με ZigBee

Το **ZigBee** είναι μια αξιόπιστη, αποτελεσματική ως προς το κόστος, ασύρματη τεχνολογία επικοινωνιών, σχετικά χαμηλή σε κατανάλωση ισχύος, ρυθμούς μετάδοσης δεδομένων, κόστος εφαρμογής και πολυπλοκότητα. Είναι ιδανική τεχνολογία για έξυπνο φωτισμό, παρακολούθηση της ενέργειας, οικιακό αυτοματισμό κλπ. Το ZigBee και το ZigBee Smart Energy Profile (SEP) έχουν αναγνωριστεί ως τα πιο κατάλληλα πρότυπα για εφαρμογές έξυπνου δικτύου στον οικιακό τομέα. Λειτουργεί στη μη αδειοδοτημένη ζώνη των 868MHz στην Ευρώπη, 915MHz στην Βόρεια Αμερική και 2.4GHz παγκοσμίως. Στη ζώνη των 2.4GHz, που λειτουργούν πιο συχνά οι πομποδέκτες, έχει 16 κανάλια εύρους 5MHz το καθένα και χρησιμοποιεί την OQPSK τεχνική διαμόρφωσης. Επιλέγεται αυτό το σχήμα, που είναι μια παραλλαγή της κλασσικής QPSK, επειδή απαιτεί λιγότερη ισχύ συγκριτικά με παρόμοια σχέδια διαμόρφωσης, ενώ επιτυγχάνει την ίδια ή καλύτερη απόδοση

(throughput). Το ZigBee προσφέρει ρυθμούς δεδομένων 20-250Kbps και κάλυψη 10-100m.

Θεωρείται πολύ καλή επιλογή για μετρήσεις (metering) και διαχείριση ενέργειας και είναι ιδανικό για εφαρμογές έξυπνων δικτύων χάρη στην απλότητα, την κινητικότητα που παρέχει, την ευρωστία, τις χαμηλές απαιτήσεις εύρους ζώνης, τη λειτουργία του σε μη αδειοδοτημένο φάσμα και την ευκολία εφαρμογής του.

Υπάρχουν, όμως, κάποιοι περιορισμοί στη χρήση του ZigBee σε πρακτικές εφαρμογές, όπως οι μικρές ικανότητες επεξεργασίας, το μικρό μέγεθος μνήμης, οι μικρές απαιτήσεις καθυστέρησης και οι παρεμβολές από άλλες συσκευές που μοιράζονται το ίδιο μέσο μετάδοσης.

6.3: Σύγκριση με 802.11(WiFi)

Το **IEEE 802.11** είναι μια οικογένεια προτύπων της IEEE για ασύρματα τοπικά δίκτυα (WLAN) που είχαν ως σκοπό να επεκτείνουν το 802.3 (Ethernet, το συνηθέστερο πρωτόκολλο ενσύρματης δικτύωσης υπολογιστών) στην ασύρματη περιοχή. Τα πρότυπα 802.11 είναι ευρύτερα γνωστά ως «WiFi» επειδή η WiFi Alliance, ένας οργανισμός ανεξάρτητος της IEEE, παρέχει την πιστοποίηση για τα προϊόντα που υπακούν στις προδιαγραφές του 802.11. Αυτή η οικογένεια πρωτοκόλλων αποτελεί το καθιερωμένο πρότυπο της βιομηχανίας στο χώρο των ασύρματων τοπικών δικτύων.

Ο όρος **WiFi** (**Wi**reless **Fi**delity, κατά την ορολογία **Hi**gh **Fi**delity η οποία αφορά την εγγραφή ήχου) χρησιμοποιείται για να προσδιορίσει τις συσκευές που βασίζονται στην προδιαγραφή IEEE 802.11 b/g/n και εκπέμπουν σε συχνότητες 2.4GHz. Ωστόσο το WiFi («ασύρματη πιστότητα» στα ελληνικά) έχει επικρατήσει και ως όρος αναφερόμενος συνολικά στα ασύρματα τοπικά δίκτυα. Συνήθεις εφαρμογές του είναι η παροχή ασύρματων δυνατοτήτων πρόσβασης στο Internet, τηλεφωνίας μέσω διαδικτύου (VoIP) και διασύνδεσης μεταξύ ηλεκτρονικών συσκευών όπως τηλεοράσεις, ψηφιακές κάμερες, DVD Player και ηλεκτρονικοί υπολογιστές. Σε φορητές ηλεκτρονικές συσκευές το 802.11 βρίσκει εφαρμογές ασύρματης μετάδοσης, όπως π.χ. στη μεταφορά φωτογραφιών από ψηφιακές κάμερες σε υπολογιστές για περαιτέρω επεξεργασία και εκτύπωση, αν και σε αυτόν τον τομέα

έχει υποσκελιστεί από το πρωτόκολλο Bluetooth για τα πολύ μικρότερης εμβέλειας ασύρματα προσωπικά δίκτυα.

Το 802.11 υποστηρίζει δύο τρόπους λειτουργίας: ομότιμα, όπου δεν υπάρχει κάποιος κεντρικός σταθμός βάσης-σημείο πρόσβασης, οι κόμβοι είναι ισότιμοι και η πρόσβαση στο κοινό μέσο (τον κενό χώρο) ρυθμίζεται από κάποιο κατανεμημένο πρωτόκολλο όπως το CSMA (έτσι λειτουργούν τα ad hoc WLAN), και με σημείο πρόσβασης, έναν κεντρικό κόμβο του τοπικού δικτύου δηλαδή -συνήθως συνδεδεμένο σε ενσύρματο δίκτυο κορμού (π.χ. στο Internet ή σε κάποιο μεγάλο Ethernet LAN)- ο οποίος αναλαμβάνει τον έλεγχο πρόσβασης στο κοινό μέσο και δρα ως αμφίδρομος επαναλήπτης. Τα WLAN με σημείο πρόσβασης ονομάζονται δίκτυα υποδομής ή δομημένα (infrastructure). Το σύνηθες μοντέλο που περιγράφει τέτοια δίκτυα είναι το εξής: υπάρχει ένα ενσύρματο δίκτυο κορμού (σύστημα κατανομής, DS) στο οποίο συνδέονται τα σημεία πρόσβασης (AP). Μία ομάδα κοινών κόμβων (STA) που επικοινωνούν ασύρματα με ένα συγκεκριμένο AP σε συγκεκριμένη συχνότητα ονομάζεται Βασικό Σύνολο Υπηρεσιών (BSS). Τα BSS διασυνδέονται μεταξύ τους μέσω του DS. Ας σημειωθεί ότι μπορεί τα STA ενός BSS να μην είναι όλα στην εμβέλεια όλων αλλά πρέπει οπωσδήποτε όλα να είναι στην εμβέλεια του σημείου πρόσβασης.

Όλα τα πρωτόκολλα 802.11x έχουν κοινό υποεπίπεδο MAC και διαφέρουν στο φυσικό μέσο. Το υποεπίπεδο LLC, που αναλαμβάνει τον έλεγχο ροής, τον έλεγχο σφαλμάτων και τη διασύνδεση προς το επίπεδο δικτύου, ταυτίζεται με το καθιερωμένο κοινό πρωτόκολλο 802.2 που χρησιμοποιείται και στο Ethernet και στα περισσότερα ενσύρματα τοπικά δίκτυα -με αποτέλεσμα την άμεση και χωρίς ανάγκη μετατροπών συνδεσιμότητα ενός 802.11 WLAN με το Internet ή άλλα WAN/διαδίκτυα που χρησιμοποιούν το IP ως πρωτόκολλο δικτύου. Το βασικό πρωτόκολλο MAC του 802.11 είναι το **DCF**, το οποίο βασίζεται στη μέθοδο CSMA/CA, ενώ στα δομημένα WLAN πάνω από το DCF τρέχει επιπλέον το πρωτόκολλο **PCF** το οποίο, αξιοποιώντας το AP, προσφέρει στα τερματικά όταν χρειάζεται πρόσβαση στο κοινό μέσο χωρίς ανταγωνισμό και συγκρούσεις.

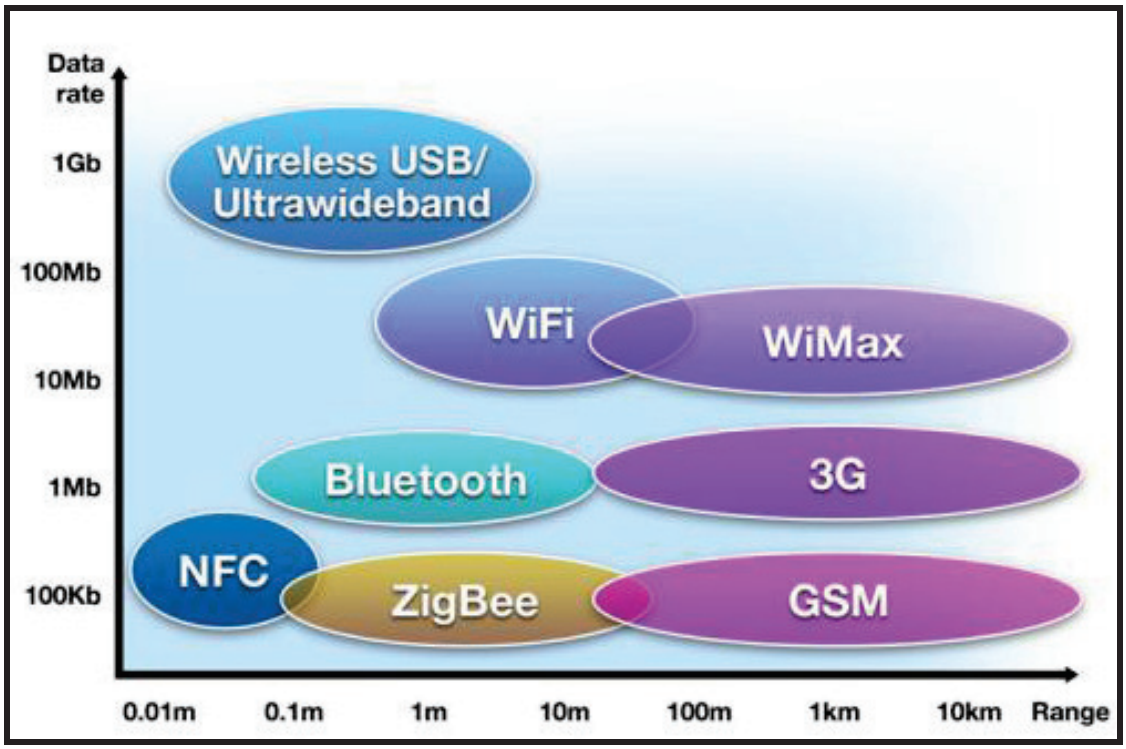
Ο ρυθμός μετάδοσης δεδομένων στο 802.11 εξαρτάται από την απόσταση μεταξύ των κόμβων. Όσο πιο μακριά βρίσκεται η ασύρματη συσκευή από το σημείο πρόσβασης,

τόσο χαμηλότερη είναι η ταχύτητα. Επίσης, λόγω της χρήσης του CSMA/CA αντί του CSMA/CD, η πραγματική διαμεταγωγή δεν υπερβαίνει το ήμισυ της ονομαστικής ταχύτητας: τα 54 Mbps του φυσικού επιπέδου στην πραγματικότητα δεν υπερβαίνουν ποτέ τα 27 Mbps στο LLC. Επιπλέον τα σημεία πρόσβασης που υποστηρίζουν ένα μεικτό δίκτυο b και g ρίχνουν τη διαμεταγωγή σε 18 Mbps, αρχικά, για να καταλήξουν σε περίπου 6 έως 9 Mbps όταν εκπέμπουν οι πελάτες.[15]

Πρωτόκολλα 802.11 τα οποία έχουν εμφανιστεί στην αγορά:

Πίνακας 3: Πρότυπα 802.11

Έκδοση	Ημερ/νια	Ζώνη συχν/των	Συνήθης ρυθμ μετάδ.	Ονομ./κος ρυθμ.μετάδ	Μέθοδ. μετάδ.	Εμβέλεια εσωτ. χώρων	Σχόλιο
802.11	1997	2,4GHz	0,9Mbit/sec	2Mbit/sec	IR/FHSS/DSSS	~20m	Το κλασικό πρότυπο, τώρα σε αχρηστία
802.11b	1999	2,4GHz	4,3Mbit/sec	11Mbit/sec	DSSS	~38m	Το πλέον επιτυχές εμπορικά, καθιέρωσε αρχικά τον όρο WiFi
802.11a	1999	5GHz	23Mbit/sec	54Mbit/sec	OFDM	~35m	Άγνωστη εμπορική πορεία λόγω ασυμβατότητας με το 802.11b
802.11g	2003	2,4GHz	19Mbit/sec	54Mbit/sec	OFDM	~38m	Αντικαταστάτης του 802.11b με επιτυχία



Εικόνα 19:Σύγκριση παρόμοιων ασύρματων τεχνολογιών

ΚΕΦΑΛΑΙΟ_7

7: ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΕΝΝΟΙΑ ΤΗΣ ΚΩΔΙΚΟΠΟΙΗΣΗΣ[18]

7.1: Κωδικοποίηση / αποκωδικοποίηση πηγής

Είσοδος: Μια αλυσίδα από σύμβολα, που φθάνουν με ρυθμός symbol/sec

Έξοδος: Δυαδική ακολουθία από 1 και 0, που δημιουργούν καθορισμένες λέξεις ανά λαμβανόμενο σύμβολο ή πακέτο (block) συμβόλων.

Μήκος λέξης(L, bits/symbol): Σταθερό ή μεταβλητό

Ρυθμός εξόδου: mn(opqr/sec) = st (ruvowxr/sec) y z (opqr/ruvowx)

Άριστος Κωδικοποιητής: Όταν ο ρυθμός δεδομένων εξόδου είναι ίσος με τον ρυθμό παροχής της πηγής (mn = m)

Παράμετροι κωδικοποιητή:
• Μήκος πακέτου (block size)
• Μήκη κωδικών λέξεων
• Μέσος ρυθμός ψηφιακών δεδομένων (data rate)
• Απόδοση κωδικοποιητή, δηλ. το πηλίκο m/mn

Αποκωδικοποιητής: Μετατρέπει μία δυαδική ακολουθία σε ακολουθία συμβόλων

• **Απλός**: οι κωδικές λέξεις είναι **σταθερού μήκους**

• **Πολύπλοκος:** οι κωδικές λέξεις είναι **μεταβλητού μήκους**

7.2:Διαμορφωτής

Είσοδος: Μια ακολουθία δυαδικών συμβόλων

Έξοδος: Μια κυματομορφή κατάλληλη για μετάδοση μέσω του καναλιού

Διαμόρφωση: Ισχυρό εργαλείο που χρησιμοποιείται για:

- Τη μείωση των επιπτώσεων του θορύβου του καναλιού.
- Την προσαρμογή του φάσματος συχνοτήτων του σήματος, με τα χαρακτηριστικά του καναλιού.
- Να δώσει δυνατότητα πολυπλεξίας πολλών σημάτων μαζί.
- Να υπερνικηθούν περιορισμοί των συσκευών.

Σημαντικές παράμετροι διαμορφωτή:

1. Τύπος κυματομορφής που χρησιμοποιεί
2. Διάρκεια κυματομορφών
3. Στάθμη ισχύος
4. Εύρος ζώνης συχνοτήτων που χρησιμοποιεί

Αύξηση των 2, 3, 4, οδηγεί σε μείωση του θορύβου.

7.3: Αποδιαμορφωτής

Αποδιαμόρφωση: Διαδικασία ανάκτησης του μηνύματος που φέρει η κυματομορφή η οποία παράγεται από τον διαμορφωτή.
Για δοσμένο τύπο διαμορφωτή, το σπουδαιότερο χαρακτηριστικό είναι η μέθοδος αποδιαμόρφωσης.
Υπάρχει μεγάλη ποικιλία διαθέσιμων τεχνικών αποδιαμόρφωσης.
Μπορούμε να συνάγουμε σχέσεις μεταξύ του ρυθμού ψηφιακών δεδομένων, απαιτήσεων σε ισχύ και εύρος ζώνης, αν γνωρίζουμε:

- Τον τύπο και τη διάρκεια της κυματομορφής που παράγει ο διαμορφωτής
- Τα φυσικά χαρακτηριστικά του καναλιού και του θορύβου του
- Τον τύπο της αποδιαμόρφωσης

Τα χαρακτηριστικά διαμορφωτή / αποδιαμορφωτή ορίζουν τον μέσο ρυθμό

σφαλμάτων.

7.4:Κωδικοποιητής/Αποκωδικοποιητής καναλιού

Κωδικοποιητής Καναλιού: Χρησιμοποιείται για τη μετάδοση υψηλής απόδοσης και αξιοπιστίας.

Συνήθως επιλέγονται λίγα, π.χ. δύο, αναλογικά σήματα για την μετάδοση μέσα από το κανάλι.

Πρόσθετα bits ελέγχου χρησιμοποιούνται για την ανίχνευση και διόρθωση λαθών.

Μέθοδοι κωδικοποίησης:

- Κατά μπλοκ : k bits πληροφορίας + r bits ελέγχου
- Συγκεραστική : bits πληροφορίας + bits ελέγχου αναμιγνύονται

Σημαντικά χαρακτηριστικά κωδικοποιητή καναλιού :

- Μέθοδος κωδικοποίησης
- Απόδοση κώδικα (= ρυθμός δεδομένων εισόδου / ρυθμός δεδομένων εξόδου)
- Ικανότητα για έλεγχο του σφάλματος
- Πολυπλοκότητα

Αποκωδικοποιητής καναλιού: ξαναβρίσκει τα bits που μεταφέρουν την πληροφορία από την κωδικοποιημένη δυαδική ακολουθία.

Σημαντικά χαρακτηριστικά αποκωδικοποιητή καναλιού:

- Πολυπλοκότητα
- Χρόνος καθυστέρησης

7.5:Κανάλια επικοινωνίας

Κανάλι Επικοινωνίας: το ηλεκτρικό μέσο, μεταξύ πηγής και προορισμού.

Χαρακτηριστικά καναλιού:

- Περιορισμένο εύρος ζώνης συχνοτήτων (φάσμα, Hz) – Χωρητικότητα C [απαιτείται C > R]
- Απόσβεση(απώλειες, εξασθένιση) (Signal to Noise Ratio – S/N)
- Παραμόρφωση πλάτους και φάσης

- Εισαγωγή θορύβου(Θερμικός προσθετικός λευκός θόρυβος, κρουστικός θόρυβος, παρεμβολές)– Δεν αφαιρείται σε όλες τις περιπτώσεις
- Πολυδιάδρομη όδευση(για ασύρματα κανάλια)
- Χρονικές μεταβολές

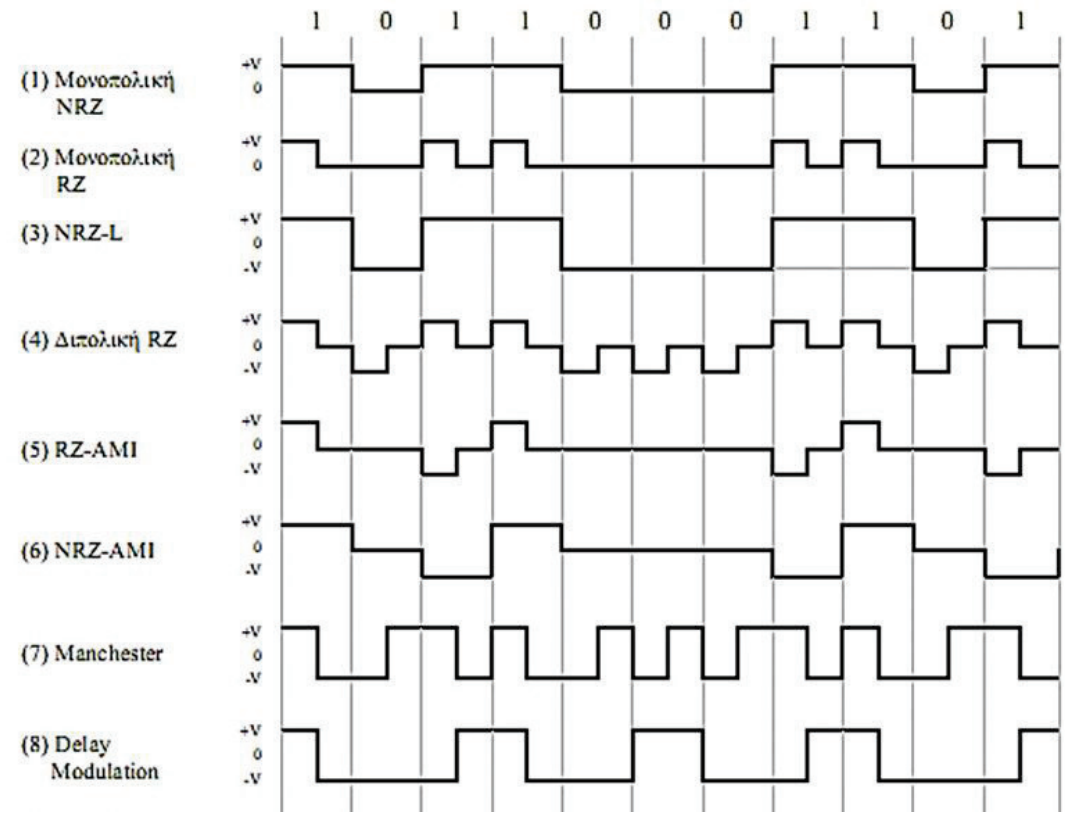
Είδη καναλιών:

Κανάλια καθοδηγούμενης μετάδοσης [συνεστραμμένα ζεύγη συρμάτων, [(τηλεφωνία, xDSL), ομοαξονικά καλώδια (CATV), οπτικές ίνες (2 x 10.□Hz)]

Κανάλια ελεύθερης μετάδοσης [ραδιομετάδοση (radio, TV, WLAN), κινητές επικοινωνίες (GSM, UMTS), δορυφορικά]

7.6: Κωδικοποιήσεις γραμμής

Οι συνήθης κωδικοποιήσεις γραμμής εμφανίζονται στην παρακάτω εικόνα:



Εικόνα 20: Κωδικοποίηση Manchester

Σε αυτήν την κωδικοποίηση, το δυαδικό 1 παριστάνεται με ένα παλμό που έχει θετική τάση στο πρώτο μισό της διάρκειας του bit και αρνητική τάση στο δεύτερο

Μισό της διάρκειας του bit. Το δυαδικό 0 παριστάνεται με ένα παλμό που έχει αρνητική τάση στο πρώτο μισό της διάρκειας του bit και θετική τάση στο δεύτερο μισό της διάρκειας του bit. Η μετάβαση στο μέσο του bit από θετική τάση σε αρνητική και από αρνητική σε θετική δηλώνει ένα 1 ή ένα 0 αντίστοιχα. Αυτή κωδικοποίηση χρησιμοποιείται σε τοπικά Ethernet δίκτυα. Η φασματική πυκνότητα ισχύος αυτού του σήματος για ισοπίθανα σύμβολα δίνεται από τη σχέση:

$$P(f) = V^2 T_b \left(\frac{\sin \pi \, f \, T_b / 2}{\pi \, f \, T_b / 2} \right)^2 \sin^2 \pi \, f \, T_b / 2$$

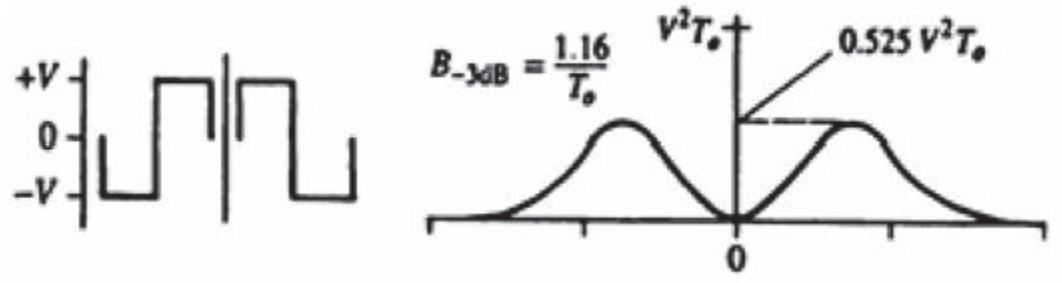
Εξίσωση 1

Το εύρος ζώνης κατά Nyquist της κυματομορφής είναι ίσο με *R* Hz.

Η πιθανότητα λήψης εσφαλμένου bit παρουσία AWGN θορύβου για ισοπίθανα σύμβολα, δίνεται από την σχέση:

$$P_B = (1/2)\mathrm{erfc}(E_b/N_0)$$

Εξίσωση 2



Εικόνα 21:Κωδικοποίηση Manchester

Στην παραπάνω εικόνα το 1 είναι θετικός παλμός στο πρώτο μισό, και αρνητικός στο δεύτερο μισό ενώ το 0 είναι διαμετρικά αντίθετος.

ΚΕΦΑΛΑΙΟ 8

8. ΜΟΝΤΕΛΑ ΔΙΑΜΟΡΦΩΣΗΣ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΟΥΝΤΑΙ NFC[18]

8.1: Ο όρος διαμόρφωση

Διαμόρφωση: Η συστηματική μεταβολή κάποιου χαρακτηριστικού της φέρουσας κυματομορφής, όπως π.χ. πλάτος, συχνότητα, φάση, σύμφωνα με μία συνάρτηση του πληροφοριακού σήματος (μήνυμα).

Βασικά χαρακτηριστικά

- Εύκολη ακτινοβολία: Για την αποτελεσματική εκπομπή της ηλεκτρομαγνητικής ακτινοβολίας στον ελεύθερο χώρο, οι διαστάσεις της κεραίας πρέπει να είναι συγκρίσιμες με το μήκος κύματος (λ) του σήματος.

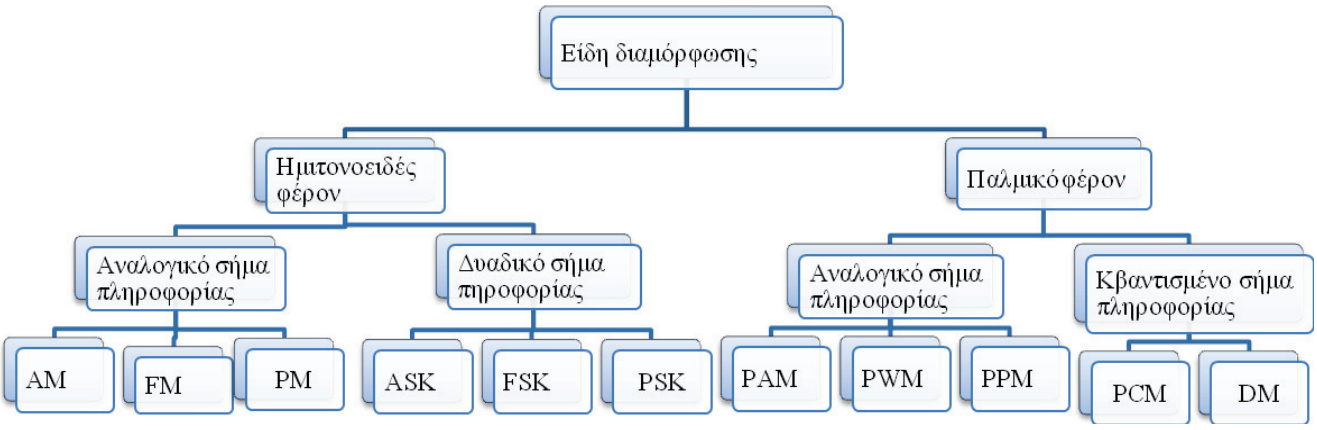
Ισχύει $\lambda = {}^{c}\!/_{f}$ όπου $c = 3.10^{8}$ m/sec

Άρα για $f = 300\text{Hz} \Rightarrow (\lambda = 10^{6}\text{ m})$ ενώ για $f = 300\text{MHz} \Rightarrow \lambda = 1\text{m}$

- πολυπλεξία: για τη μεταφορά των φασμάτων πολλών σημάτων σε διαφορετικές φασματικές περιοχές και την ταυτόχρονη μετάδοσή τους μέσα από το ίδιο κανάλι.
- Υπέρβαση περιορισμών από τις διατάξεις: μεταφέροντας το φάσμα του σήματος σε φασματική περιοχή που προσφέρει ευνοϊκότερες συνθήκες σχεδίασης των διατάξεων.
- Εκχώρηση συχνότητας: για την ραδιοφωνική ή τηλεοπτική εκπομπή σε συγκεκριμένη

φασματική περιοχή ανά σταθμό.

- Περιορισμό θορύβου και παρεμβολών : Μπορούμε να επιτύχουμε περιορισμό του θορύβου μετάδοσης ανταλλάσσοντας ευρύτερο φάσμα.



Εικόνα 22: Είδη διαμόρφωσης

8.2: Διαμόρφωση με Ημιτονοειδές Φέρον

Ψηφιακή διαμόρφωση συνεχούς κύματος ή ψηφιακή διαμόρφωση φέροντος

Σήμα πληροφορίας- . ακολουθία παλμών Ημιτονοειδές φέρον $x(t) = A\cos\omega_c t$

– Ψηφιακή διαμόρφωση πλάτους ή κλείδωμα μεταλλαγής πλάτους (ASK)

– Ψηφιακή διαμόρφωση συχνότητας ή κλείδωμα μεταλλαγής συχνότητας (FSK)

– Ψηφιακή διαμόρφωση φάσης ή κλείδωμα μεταλλαγής φάσης (PSK)

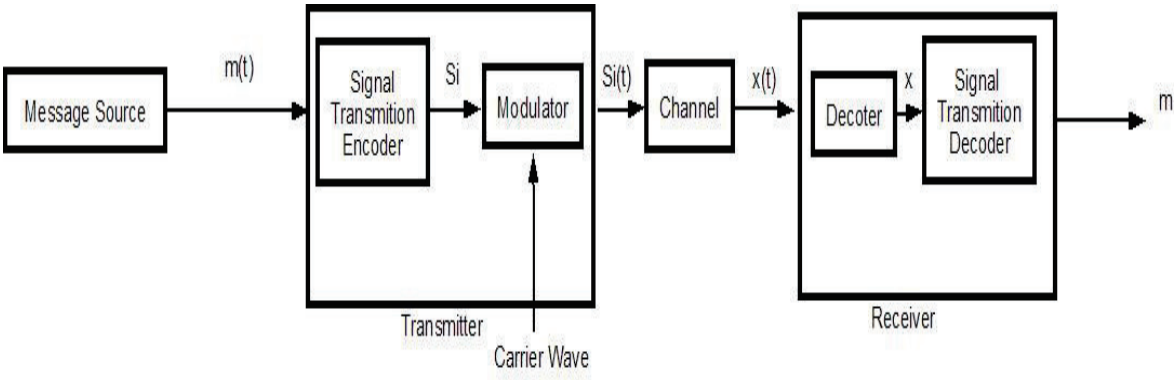
Η Ψηφιακή Διαμόρφωση χρησιμοποιείται για την μετάδοση ενός πληροφοριακού σήματος m(t) ακολουθίας παλμών (ψηφιακό) μέσα από ένα δοσμένο κανάλι επικοινωνίας.

Μπορούμε να χρησιμοποιήσουμε μετάδοση βασικής ζώνης, αλλά τα περισσότερα κανάλια έχουν φτωχή απόκριση στις χαμηλές συχνότητες.

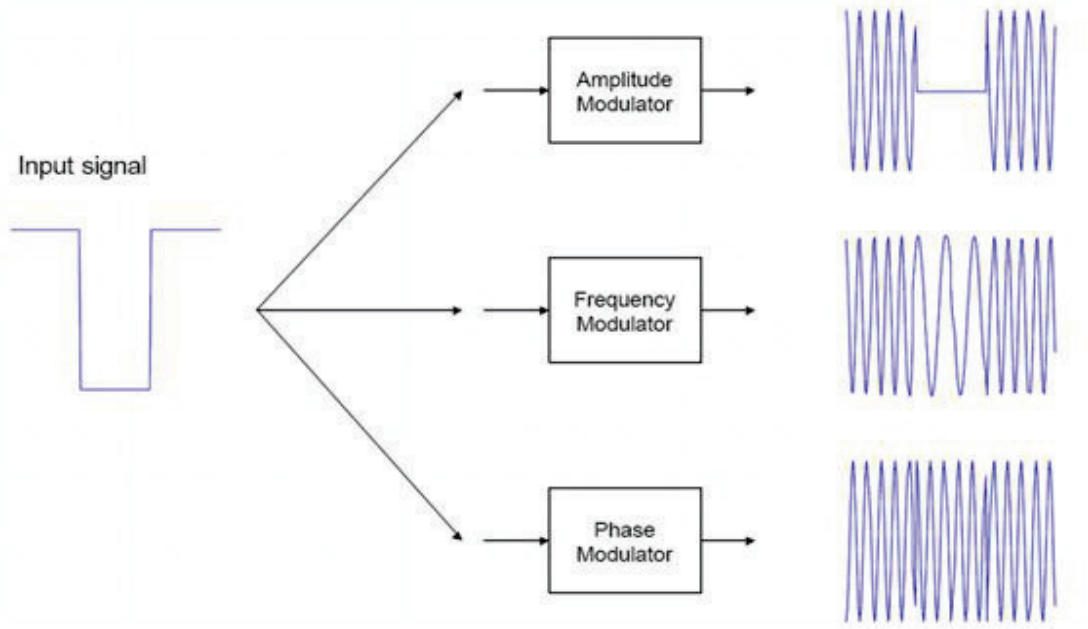
Επομένως, διαμορφώνουμε κατάλληλα το ψηφιακό σήμα $m(t)$ ώστε να το μεταφέρουμε στην επιθυμητή ζώνη διέλευσης συχνοτήτων του καναλιού. Η ψηφιακή πληροφορία m(t) μπορεί να μεταβάλλει το πλάτος, τη φάση ή τη συχνότητα του φέροντος.

Σήμα πληροφορίας $m(t)$ ακολουθία παλμών

Ημιτονοειδές φέρον $x(t) = A\cos\omega_c t$



Εικόνα 23: Ψηφιακή διαμόρφωση



Εικόνα 24: Μέθοδοι ψηφιακής διαμόρφωσης

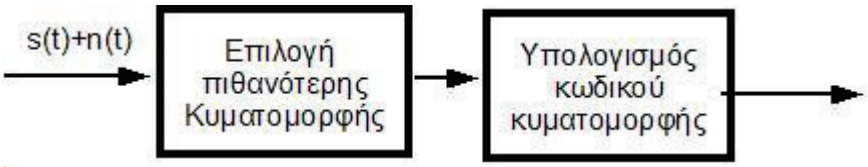
Στην ψηφιακή διαμόρφωση στέλνουμε bits με τη χρήση ενός υψίσυχνου φέροντος σήματος $x(t) = A\cos\omega_c t$.

κάθε bit διαρκεί T και ο ρυθμός μετάδοσης είναι $r = 1/T$

8.3: Αποδιαμορφωτες για ASK FSK PSK

Οι αποδιαμορφωτές για ASK, FSK και PSK:

- Αποφασίζουν για ποιά από τις M δυνατές κυματομορφές έχει μεταδοθεί
- Έχουν σαν έξοδο τον κωδικό της κυματομορφής αυτής
- Κριτήριο επιτυχίας = η μικρή πιθανότητα σφάλματος



$$\mathbf{b}_{\text{out}} = \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{\log_2(M)-1} \end{bmatrix} \qquad P(E) = \Pr\{\mathbf{b}_{\text{out}} \neq \mathbf{b}_{\text{transmitted}}\}$$

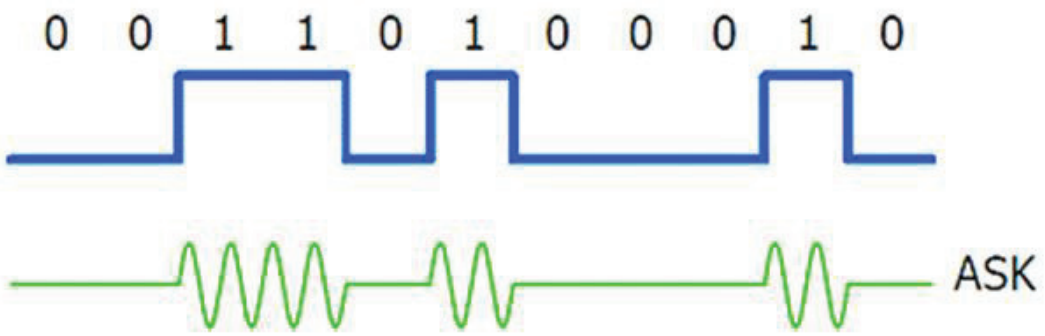
Εικόνα 25: Αποδιαμορφωτής

8.4Ειδικά η Διαμόρφωση ASK

Στην ASK το πλάτος του φέροντος μεταπηδά (switched) μεταξύ δύο (ή περισσότερων) επιπέδων, ανάλογα με την ψηφιακή πληροφορία.

Συγκεκριμένα:

- Για bit = 1 στέλνουμε επί χρόνο T το σήμα $x(t) = A\cos\omega_c t$
- Για bit = 0 στέλνουμε επί χρόνο T το μηδέν

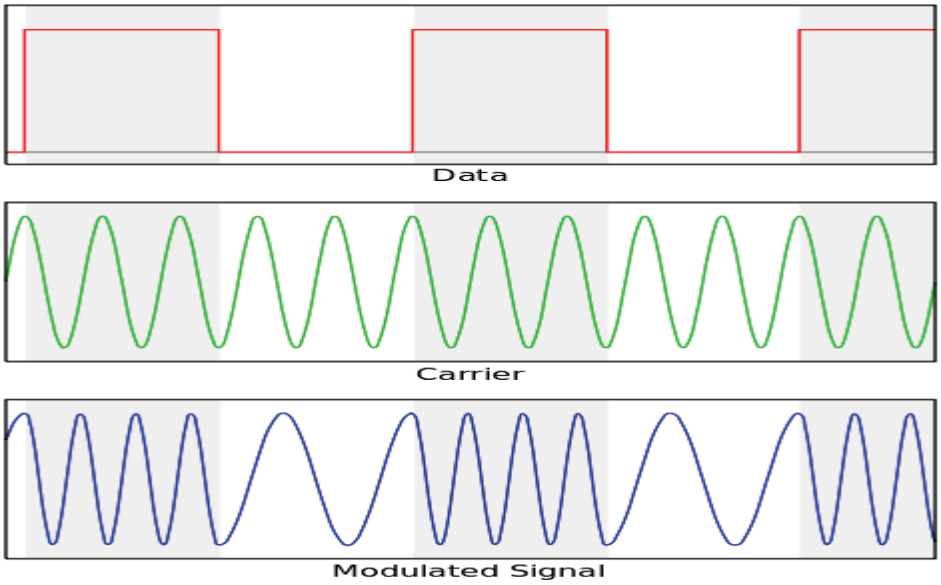


Εικόνα 26: Διαμόρφωση ASK

8.5:FSK διαμόρφωση

Διαμόρφωση μετατόπισης συχνότητας (Frequency-Shift Keying - FSK**)** ονομάζεται ο τύπος διαμόρφωσης σήματος όπου ψηφιακά δεδομένα παρουσιάζονται ως αλλαγές στη συχνότητα ενός φέροντος σήματος.

Τα περισσότερα από τα πρώτα μοντέλα modem χρησιμοποιούσαν διαμόρφωση FSK για να στείλουν και να λάβουν δεδομένα με ρυθμούς μέχρι 300, 600 ή 1200 bits το δευτερόλεπτο (συστάσεις I.T.U. V21 και V.23). Μερικοί μικρο-υπολογιστές χρησιμοποιούσαν μια ειδική μορφή διαμόρφωσης FSK, το πρότυπο Kansas City, για αποθήκευση δεδομένων σε κασέτες ήχου. Η διαμόρφωση FSK χρησιμοποιείται ακόμη στο ερασιτεχνικό ραδιόφωνο γιατί επιτρέπει μεταφορά δεδομένων από μη τροποποιημένο εξοπλισμό για μετάδοση φωνής.



Εικόνα 27: FSK Διαμόρφωση

8.5.1:FSK/ASK και θόρυβος

Η διαμόρφωση FSK εμφανίζει μεγαλύτερη αντοχή στο θόρυβο σε σχέση με την ASK, ενώ έχει εύρος ζώνης

$$B_{RF} = \text{baud rate} + f_2 - f_1$$

Εξίσωση 3

Όπου f1 και f2 οι δύο τιμές που παίρνει η συχνότητα του ημιτονικού φέροντος ανάλογα με το εάν μεταδίδεται 0 ή 1 (f2 η μεγαλύτερη τιμή πάντα).Στην περίπτωση δυαδικής FSK, bit rate και baud rate συμπίπτουν οπότε η σχέση 3.1.1 γράφεται αλλιώς $B_{RF} = R_B + F_2 - F_1$

Για την ψηφιακή διαμόρφωση θεωρητικά το BER για κάθε σήμα διαμόρφωσης μπορεί να εκφραστεί

$$BER_{BPSK} = Q\left(2\sqrt{\frac{2E_b}{N_0}}\right)$$

Εξίσωση 4

$$BER_{ASK,FSK} = Q\left(\sqrt{\frac{E_b}{N_0}}\right)$$

Εξίσωση 5

$$BER_{ASK} = \frac{1}{2}e^{-\frac{E_b}{N_0}} + \frac{1}{2}Q\left(\sqrt{\frac{E_b}{N_0}}\right)$$

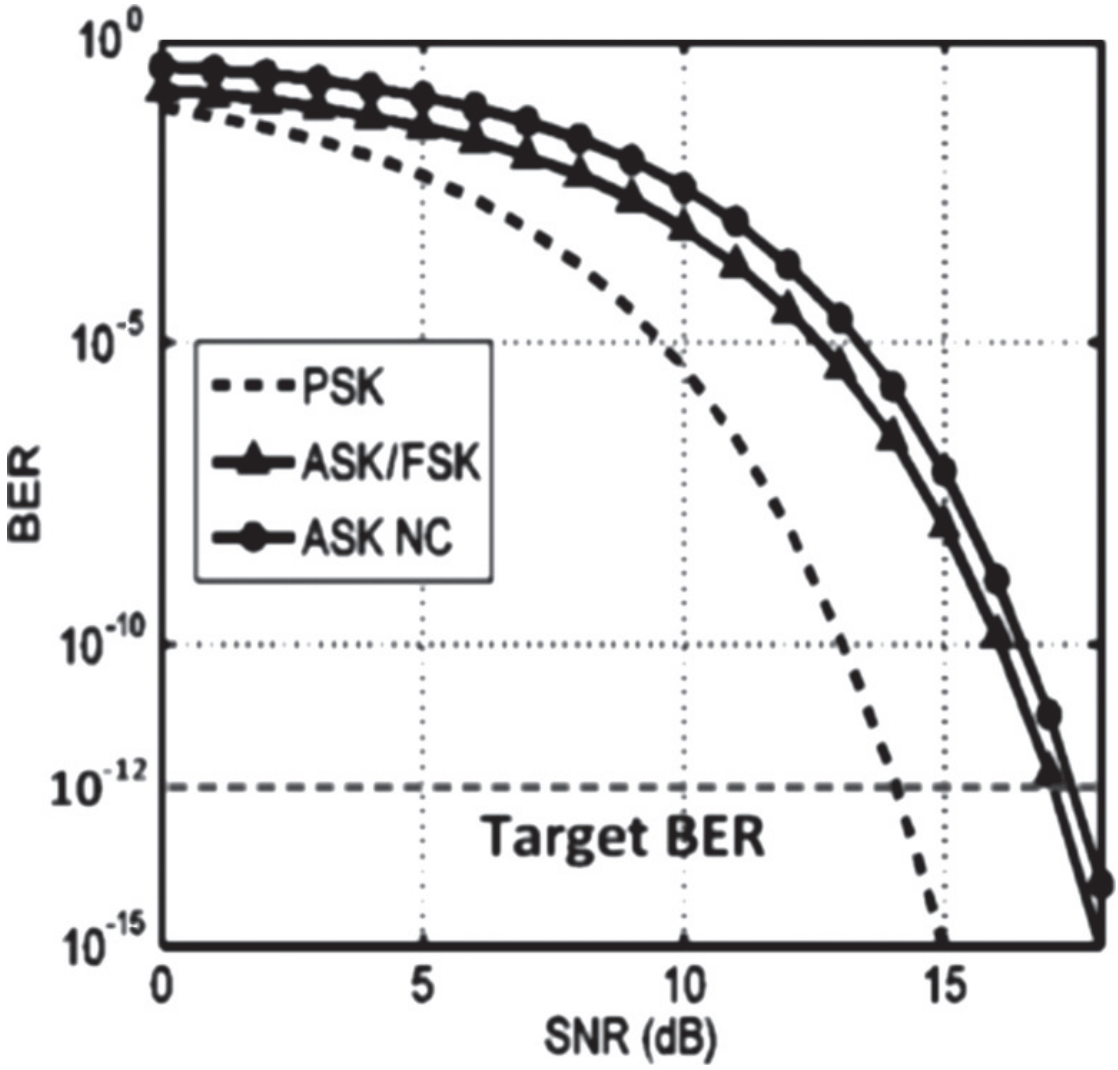
Εξίσωση 6

- E_b είναι η μέση ενέργεια bit
- N_0 είναι ο θόρυβος φασματική πυκνότητα ισχύος σε AWGN κανάλι

Δεδομένου ότι κάθε bit αντιπροσωπεύει ένα σύμβολο ό λόγος ενέργειας του bit προς τον θόρυβο ισχύος μεταφράζεται ως **SNR.**

Οι σχέσεις 1 και 2 δείχνουν ότι ASK και FSK διαμορφώσεις απαιτούν διπλάσια ισχύς σήματος από την BPSK για να επιτευχθεί το ίδιο BER.

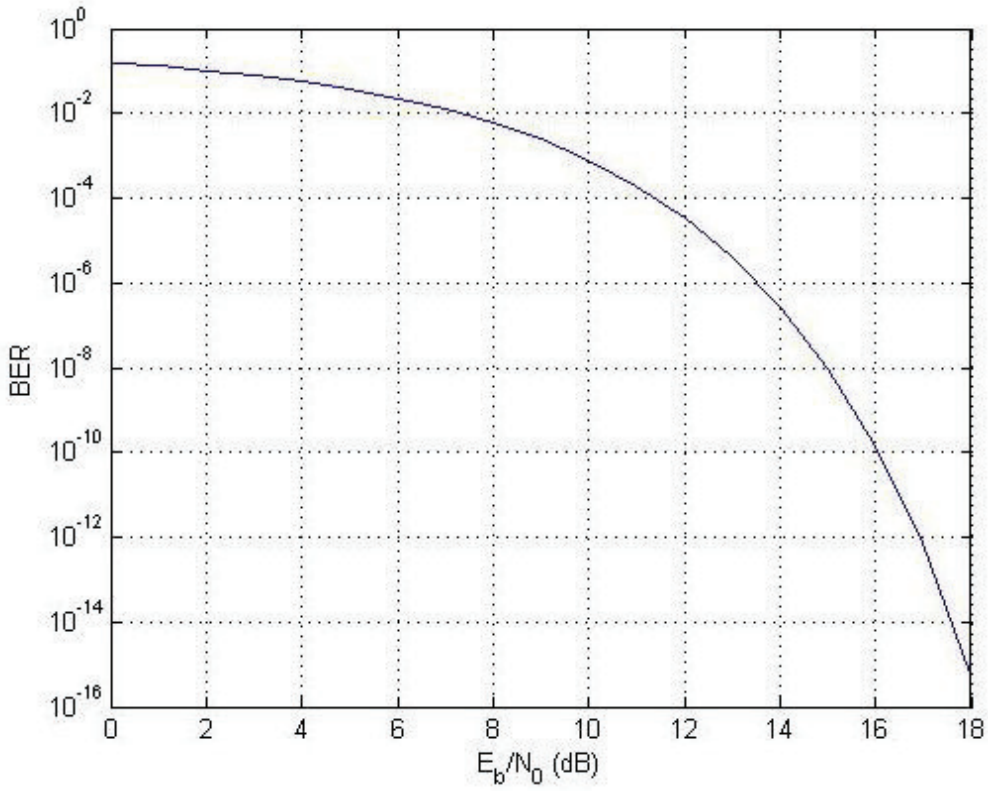
Η εικόνα 32 δείχνει ότι η μη συνεκτική διαμόρφωση ASK χρειάζεται περίπου 1dB υψηλότερο SNR για το ίδιο BER. Για ελάχιστο BER πρέπει στις BPSK,FSK/ASK,ASK να εφαρμόζεται SNR 14,1 και 18.



Εικόνα 28: Σύγκριση BER For BPSK,ASK/FSK,ASK

8.5.2 Matlab Editor BER for ASK

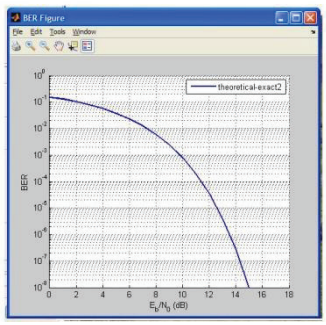
```
SNR = (0:1:18);
BER = berawgn (SNR, 'ask', 2, 'coherent');
figure;
semilogy(SNR, BER);
grid on;
xlabel('E_b/N_0 (dB)');
ylabel('BER');
```



Γράφημα 1 BER / ASK

8.5.3: Matlab Simulink BER FSK for AWGN Channel

Μέσα από το BERTool του Matlab Simulink εκτελούμε την προσομοίωση της διαμόρφωσης με SNR 18.



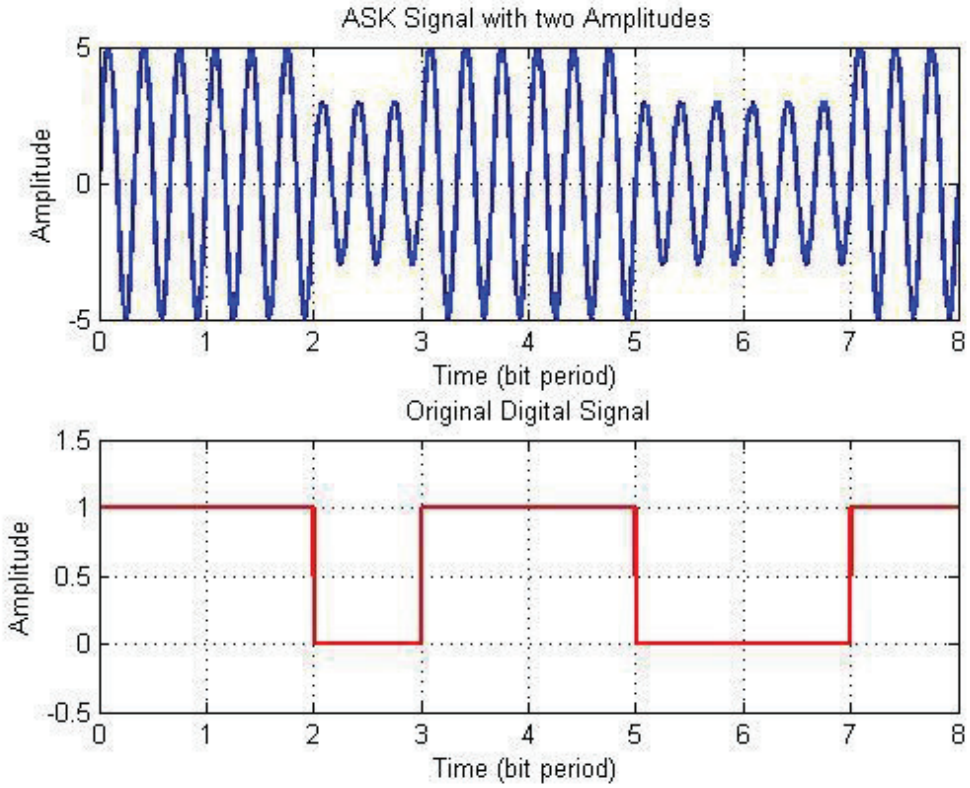
Γράφημα 2: BER FSK Simulink

8.5.4: Κώδικας Δυαδικής ASK (BASK) σε Matlab Editor

```
format long;
clear all;
close all;
N = 8; %Στάθμες κβαντοποίησης
bit_stream = round(rand(1,N)); %Γεννήτρια παραγωγής
τυχαίων Bit ομοιόμορφη κατανομή
A1 = 3; %Πλάτος για bit 0
A2 = 5; %Πλάτος για bit 1
f = 3; %Μέγιστη συχνότητα
fs = 100; %Συχνότητα δειγματοληψίας (θεώρημα Nyquist)
t = 0: 1/fs: 1; %Χρόνος εκτέλεσης από 0 έως 1 Bit με
περίοδο T = 1/fs Περίοδος δειγματοληψίας
%Μεταβλητές που αντιστοιχούν σε πίνακες μόνο για το plot
time = [];
ASK_signal = [];
Digital_signal = [];

for ii = 1: 1: length(bit_stream)
ASK_signal = [ASK_signal
(bit_stream(ii)==0)*A1*sin(2*pi*f*t)+...
(bit_stream(ii)==1)*A2*sin(2*pi*f*t)];
Digital_signal = [Digital_signal (bit_stream(ii)==0)*...
zeros(1,length(t)) +
(bit_stream(ii)==1)*ones(1,length(t))];
time = [time t];
t = t + 1;
end
subplot(2,1,1);
plot(time,ASK_signal,'LineWidth',2);
xlabel('Time (bit period)');
ylabel('Amplitude');
```

```
title('ASK Signal with two Amplitudes');
%Πίνακας ([0 time (end) 1.5 1.5]);
grid on;
subplot(2,1,2);
plot(time,Digital_signal,'r','LineWidth',2);
xlabel ('Time (bit period)');
ylabel ('Amplitude');
title ('Original Digital Signal');
axis ([0 time(end) -0.5 1.5]);
grid on;
```



Γράφημα 3: BASK

8.6: Θεώρημα δειγματοληψίας (Nyquist)

Το θεώρημα δειγματοληψίας ορίζει πως για να μην υπάρχει αλλοίωση στο περιεχόμενο ενός σήματος, πρέπει η συχνότητα με την οποία θα γίνει η

δειγματοληψία να είναι τουλάχιστον διπλάσια από την μέγιστη συχνότητα η οποία μπορεί να περιέχεται στο σήμα. Διαφορετικά θα έχουμε αναδίπλωση φάσματος ή αλλιώς φαινόμενο επικάλυψης – Aliasing.

Αναλυτικότερα, έστω η $f\max$ ενός αναλογικού σήματος $x_a($ τότε το $x_a($ μπορεί ανακτηθεί από τα δείγματα

$$x(= x_a(nTs)$$

Εξίσωση 7

αν

$$fs > 2f\max$$

Εξίσωση 8

ΚΕΦΑΛΑΙΟ 9

9: ΠΛΕΟΝΕΚΤΗΜΑΤΑ NFC

9.1: Πλεονεκτήματα

- Οι NFC αλληλεπιδράσεις είναι εύκολες και απλές καθώς δεν χρειάζεται παρά μόνο ένα απλό άγγιγμα.
- Η χρήση NFC είναι ιδανική για το ευρύτερο φάσμα των επιχειρήσεων καθώς είναι εύκολη στη χρήση, βελτιώνει την επικοινωνία μεταξύ των μελών της επιχείρησης.
- Η NFC τεχνολογία διευκολύνει την απλή και γρήγορη εγκατάσταση των ασύρματων τεχνολογιών όπως το Bluetooth και το WiFi.
- Είναι εγγενώς ασφαλής η χρήση καθώς οι μεταδόσεις είναι μικρής εμβέλειας (από ένα άγγιγμα σε μόλις λίγα εκατοστά). Επίσης σημαντικό χαρακτηριστικό είναι ότι δεν μπορεί να γίνει υποκλοπή δεδομένων ασύρματα.
- Βρίσκει εφαρμογή σε πολλές χρήσεις όπως στις πληρωμές, στα εισιτήρια, στη διαφήμιση, στις έξυπνες κάρτες, στην ανταλλαγή δεδομένων, στην κρυπτογράφηση παρουσίας και στον έλεγχο πρόσβασης.
- Αξιοποιεί τα κινητά τηλέφωνα ως μέσο αλληλεπίδρασης. Είναι ευρέως διαδεδομένα και τα κουβαλάμε πάντα μαζί μας, έχουν επεξεργαστή, έχουν συνήθως πρόσβαση στο διαδίκτυο, είναι διαδραστικά (πληκτρολόγιο, οθόνη αφής) και διαθέτουν ώριμα λειτουργικά συστήματα.

9.2: Μειονεκτήματα NFC

- Τα συστήματα NFC είναι εύκολο να υποκλαπούν. Οποιοσδήποτε είναι σε θέση να κλέψει τις προσωπικές πληροφορίες του καθενός πολύ εύκολα και αυτό γιατί δεν υπάρχει κάποιο αυστηρό μέτρο ασφαλείας. Μια προσθήκη θα μπορούσε να είναι ένα σύστημα αναγνώρισης προσώπου ή αναγνώρισης δακτυλικών αποτυπωμάτων.
- Η χρήση του NFC εκπέμπει ακτινοβολία.
- Ένα άλλο θέμα είναι ότι επειδή η λειτουργία του NFC γίνεται εξ αποστάσεως υπάρχει ο κίνδυνος απώλειας των δεδομένων.

ΚΕΦΑΛΑΙΟ 10

10: ΜΕΛΛΟΝΤΙΚΗ ΕΞΕΛΙΞΗ

Λόγω της ραγδαίας εξέλιξης, η χρήση των συστημάτων NFC εκτιμάται ότι θα φτάσει στο 1.2 εκατομμύρια μέχρι το 2015. Οι λιανοπωλητές αναμένεται να ξεκινήσουν πιλοτικά προγράμματα μέσα στο 2012 όπου θα ενσωματώνουν έξυπνες αφίσες στις πινακίδες των μαγαζιών τους και θα αναπτύξουν διάφορες στρατηγικές διαφήμισης εξωτερικού χώρου. Επίσης μια άλλη εξέλιξη είναι οι πληρωμές μέσω κινητού τηλεφώνου. Μέσα σε 4 χρόνια, το 50% των έξυπνων κινητών θα υποστηρίζουν το συγκεκριμένο σύστημα NFC.

Μια καινοτομία που πρόκειται να λάβει δράση είναι στο καινούργιο προϊόν "angry birds magic" όπου θα φέρει το παιχνίδι στον πραγματικό κόσμο με τη χρήση του NFC και GPS. Άλλες εφαρμογές που συζητούνται είναι εφαρμογές που αφορούν την παρακολούθηση της υγείας, όπως επίσης και τρόπους ώστε να εφοδιάσουν τα «έξυπνα σπίτια» με πόρτες που όχι μόνο ξεκλειδώνουν μέσω ενός NFC συστήματος, αλλά μπορούν επίσης να επικοινωνήσουν με άλλα αντικείμενα στο σπίτι.

Ένα δημοσίευμα των Digitimes αναφέρει ότι η Apple αναμένεται να συμπεριλάβει NFC (Near Field Communication) δυνατότητες στο iPhone μέσα στο 2012 με την επόμενη μεγάλη αναβάθμιση στη συσκευή. Οι πληροφορίες, μάλιστα, για την προσθήκη NFC στο iPhone υπήρχαν εδώ και πολλούς μήνες αλλά τελικά το iPhone 4S δεν περιέλαβε την τεχνολογία. Το δημοσίευμα αναφέρει ότι και η Apple θα εισέλθει σε αυτό το χώρο με τις NFC συσκευές μέσα στο 2012 συμμετέχοντας στην ραγδαία ανάπτυξη της τεχνολογίας από το 10% στο 50% μέσα στα επόμενα χρόνια.

ΚΕΦΑΛΑΙΟ 11

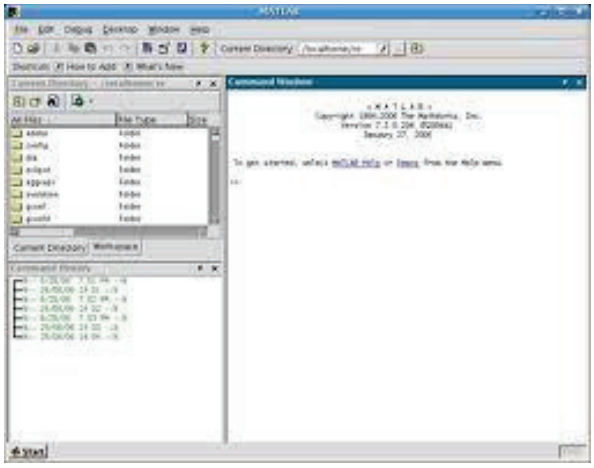
11: ΠΡΟΣΟΜΟΙΩΣΗ ΣΥΣΤΗΜΑΤΟΣ

11.1:Γενικά για το Matlab

Το Matlab είναι μια υψηλού επιπέδου γλώσσα τεχνικού προγραμματισμού και ένα αλληλεπιδραστικό περιβάλλον για την ανάλυση στοιχείων και την ανάπτυξη αλγορίθμων και εφαρμογών. Οι τελευταίες εκδόσεις τουMatlab (Matlab R2010α) μας δίνουν την δυνατότητα να χρησιμοποιήσουμε ένα σημαντικό εργαλείο (Toolbox) το Simulink,με το οποίο μπορούμε να συνθέσουμε μια διεργασία ή ένα σύστημα χρησιμοποιώντας εργαλεία τα οποία στηρίζονται στις ιδιότητες της γλώσσας προγραμματισμού G

11.2: Επεξήγηση παραθύρων του Matlab

- **Command Window** (Παράθυρο εντολών): Είναι το βασικό παράθυρο και χαρακτηρίζεται από το σύμβολο **>> (Command prompt).** Πληκτρολογούμε τις εντολές δίπλα από το >> και για να πάρουμε τα αποτελέσματα πατάμε Enter.
- **Command Directory** (Τρέχων κατάλογος): Εμφανίζονται τα περιεχόμενα του τρέχοντος καταλόγου π.χ. C:\MATLAB όπου και αποθηκεύονται τα αρχεία.
- **Workspace** (Χώρος εργασίας): Εμφανίζονται οι μεταβλητές που δημιουργούνται. Επιπλέον παίρνουμε πληροφορίες για τον τύπο και το μέγεθος της εκάστοτε μεταβλητής.
- **Command History** (Ιστορικό εντολών): Καταγράφονται όλες οι εντολές που εκτελούμε τώρα αλλά και εντολές που δόθηκαν κατά την εκτέλεση του προγράμματος προηγούμενες φορές.



Εικόνα 29:Περιβάλλον Matlab

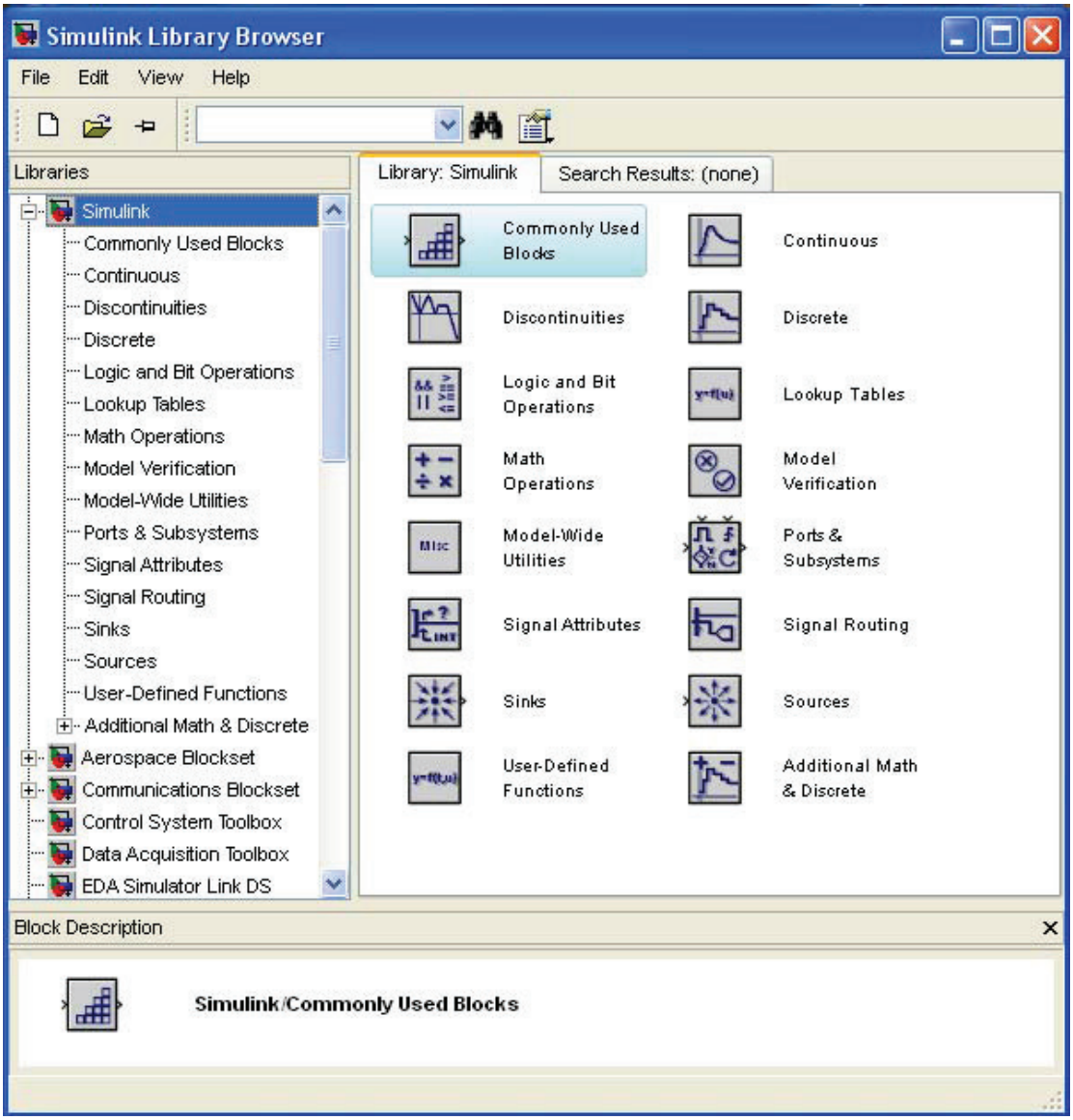
11.3: Εισαγωγή στο Matlab Simulink

Το Matlab μας δίνει τη δυνατότητα να χρησιμοποιήσουμε ένα σημαντικό εργαλείο (Toolbox) το Simulink, με το οποίο μπορεί να συνθέσει μία διεργασία ή ένα σύστημα χρησιμοποιώντας εργαλεία τα οποία στηρίζονται στις ιδιότητες της γλώσσας προγραμματισμού G. Δηλαδή το Simulink δίνει εργαλεία σε γραφικό περιβάλλον και με ευκολία στις ρυθμίσεις μπορεί να κάνει τη σύνθεση ενός συστήματος αποφεύγοντας έτσι τις εντολές ή τον προγραμματισμό που χρησιμοποιούμε στον editor.τουMatlab.

Μπορούμε να ενεργοποιήσουμε το Simulink είτε απευθείας από τη γραμμή εργαλείων του editor κάνοντας αριστερό κλικ από το ποντίκι πάνω στο αντίστοιχο εικονίδιο, είτε γράφοντας την εντολή Simulink στον editor του Matlab.Σε κάθε περίπτωση πάντως για να ενεργοποιήσουμε το Simulink libraries browser θα πρέπει η έκδοση του Matlab την οποία έχουμε εγκαταστημένη στο Η/Υ να έχει το Simulink.

Συστήματα που έχουμε δυνατότητα να συνθέσουμε με το Matlab Simulink είναι τα εξής:

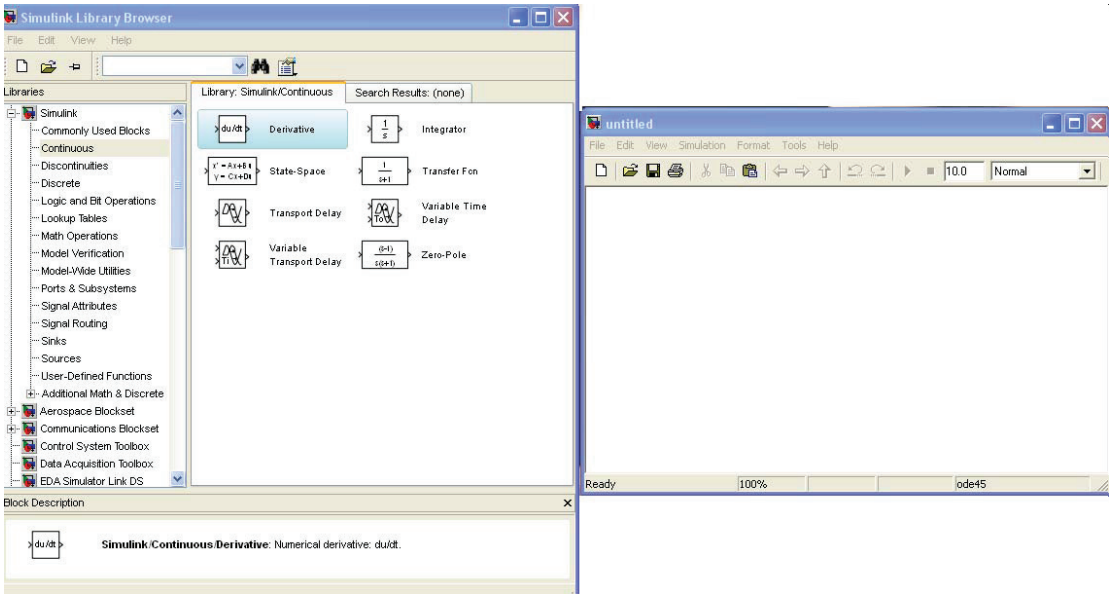
- Συστήματα αυτόματου ελέγχου γραμμικά
- Συστήματα αυτόματου ελέγχου μη γραμμικά
- Συστήματα για Real Time Control
- Ανάλυση συστημάτων
- Νευρωνικά δίκτυα.[16]



Εικόνα 30:Simulink library

Επιλέγοντας "**File→New→Model**" ανοίγει ένα νέο κενό αρχείο με το όνομα untitled στο οποίο θα δημιουργηθεί το σύστημα.

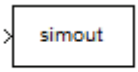
Πατώντας μια φορά σε οποιοδήποτε κατηγορία, μια λίστα από διαγράμματα (blocks) θα εμφανισθεί σε ξεχωριστό παράθυρο. Αυτά τα διαγράμματα μπορούν να εισαχθούν στο αρχείο untitled όπου θα πραγματοποιηθεί η προσομοίωση. Η εισαγωγή τους μπορεί να γίνει είτε με αντιγραφή – επικόλληση είτε με απλό σύρσιμο τους στο αρχείο. Στην εικόνα 23 φαίνονται τα blocks που αντιστοιχούν στην κατηγορία ***Continuous*** μαζί με το αρχείο untitled



Εικόνα 31: Αντιπροσωπευτικά διαγράμματα και αρχείο προσομοίωσης

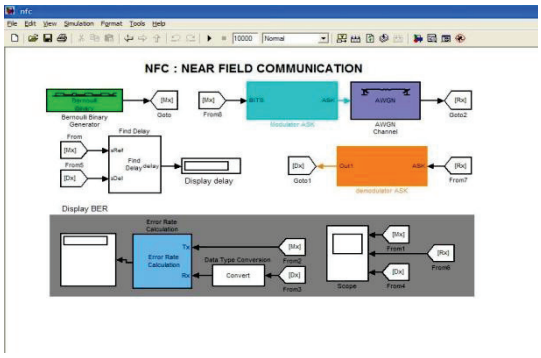
Πίνακας 4:Βασικά διαγράμματα Simulink

Κατηγορία	**Continuous**		
	Όνομα	**Σχήμα**	**Λειτουργία**
	Transfer Function	1/(s+1) Transfer Fcn	Περιγραφή Συστήματος με Συνάρτηση Μεταφοράς
	State Space	x' = Ax+Bu, y = Cx+Du State-Space	Περιγραφή Συστήματος στον Χώρο Κατάστασης
	Integrator	1/s Integrator	Ολοκλήρωση Σήματος Εισόδου
	Derivative	du/dt Derivative	Παραγώγιση Σήματος Εισόδου
Κατηγορία	**Sources**		
	Όνομα	**Σχήμα**	**Λειτουργία**

	Step		Βηματική Είσοδος
	Ramp		Αναρριχητική Είσοδος
	Clock		Εισαγωγή Χρόνου Προσομοίωσης
Κατηγορία	**Sinks**		
	Όνομα	**Σχήμα**	**Λειτουργία**
	Scope		Απεικόνιση του Σήματος Εισόδου Συναρτήσει του Χρόνου
	To Workspace		Αποθήκευση Τιμών του Σήματος Εισόδου στον Χώρο Εργασίας
Κατηγορία	**Math operations**		
	Όνομα	**Σχήμα**	**Λειτουργία**
	Gain		Πολλαπλασιασμός Σήματος Εισόδου με μια Σταθερά
	Sum		Άθροιση Σημάτων Εισόδου

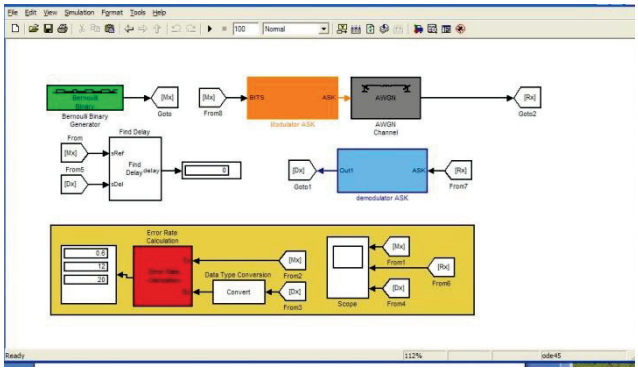
ΚΕΦΑΛΑΙΟ 12

12: ΣΥΝΘΕΣΗ ΣΥΣΤΗΜΑΤΟΣ



Εικόνα 32: Screen short 1 NFC Model

12.1: Εκτέλεση προσομοίωσης 100 time simulation stop



Εικόνα 33: Screen Short NFC1

12.2: Δομικά στοιχεία συστήματος

- **Start time /Stop time (100):** Στο λογισμικό Simulink, ο χρόνος και όλες οι σχετικές παράμετροι (όπως δείγμα/ φορές) είναι έμμεσα σε δευτερόλεπτα. Αν επιλέξουμε να χρησιμοποιήσουμε μια διαφορετική μονάδα του χρόνου, θα πρέπει να κλιμακωθούν όλες οι παράμετροι ανάλογα.

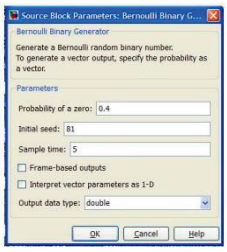
  Σημείωση: Ο χρόνος προσομοίωσης η πραγματική ώρα του ρολογιού δεν είναι η ίδια. Για παράδειγμα, εάν εκτελείται μια προσομοίωση για 10 sec

συνήθως δεν λαμβάνει 10 sec όπως μετράται σε ένα ρολόι. Ο χρόνος που χρειάζεται πραγματικά για να τρέξει μια προσομοίωση εξαρτάται από πολλούς παράγοντες συμπεριλαμβανομένης και της πολυπλοκότητας του μοντέλου, το μεγέθη βήματος, και την ταχύτητα του υπολογιστή.

- **Bernoulli binary:** Γεννήτρια τυχαίων δυαδικών αριθμών σύμφωνα με την κατανομή **Bernoulli.** Η **κατανομή Μπερνούλλι** είναι μια διακριτή συνάρτηση κατανομής τυχαίας μεταβλητής. Περιγράφει ένα τυχαίο πείραμα με δυο πιθανά αποτελέσματα (επιτυχία - αποτυχία) και πιθανότητα επιτυχίας p.

Θεωρούμε την τυχαία μεταβλητή X που παίρνει τιμές 0 ή 1, $X^{\in\{0,1\}}$. Για X=1 έχουμε επιτυχία και για X=0 αποτυχία. Η κατανομή Μπερνούλλι παίρνει τις εξής τιμές: $P(X=1)=p$ και $P(X=0)=q=1-p$

Παράθυρο διαλόγου-εισαγωγή παραμέτρων:



Εικόνα 34:Source Block parameters Benoulli Generator

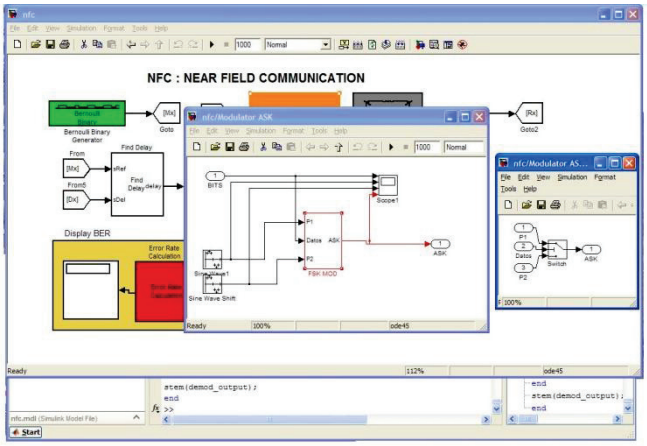
1. **Probability of a zero:** Η πιθανότητα να είναι η ακολουθία μηδενική
2. **Initial seed:** Αρχική τιμή της γεννήτριας **-σπόρος**.
3. **Sample time:** Περίοδος γεννήτριας ο χρόνος που θα περάσει μέχρι να ξαναεμφανιστεί ο σπόρος δηλ. η αρχική τιμή της γεννήτριας.

- **Goto Block:** Το goto μπλοκ διαβιβάζει σε άλλες συστοιχίες μπλοκ. Πραγματοποιούν δηλ. το Signal Routing .Η είσοδος μπορεί να είναι ένα πραγματικό ή μιγαδικό σήμα ή οποιουδήποτε τύπος δεδομένων. Το μπλοκ

Goto επιτρέπει να περάσει ένα σήμα από ένα τετράγωνο στο άλλο, χωρίς στην πραγματικότητα να τα συνδέει.

Ένα μπλοκ Goto μπορεί να περάσει το σήμα εισόδου του σε περισσότερες από μία συστοιχίες από μπλοκ, αν και ένα μπλοκ μπορεί να λάβει ένα σήμα από ένα μόνο Goto μπλοκ. Η έξοδος του Goto γίνεται Πολλαπλές είσοδοι From, From 8, 2, 1.Τα Goto μπορεί να είναι Transmitter(**Goto)**, Receiver(**from)** η και τα δυο.

- **BASK Modulation:** Δυαδική ASK Το μπλοκ της διαμόρφωσης περιλαμβάνει τα εξής δομικά στοιχεία:



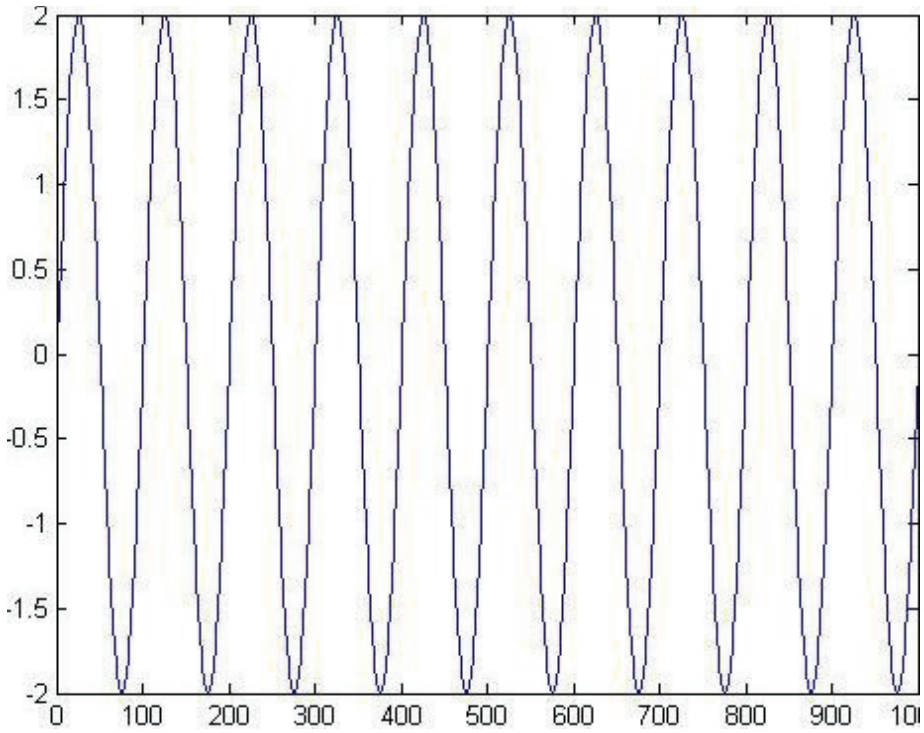
Εικόνα 35: Screen short BASK(ΜΠΛΟΚ)

Είσοδοι συστήματος:

1. **Bits:** Ακολουθία bits
2. **Sine wave:** Με αυτήν την πηγή εισάγουμε ημιτονοειδές σήμα. Το εργαλείο πηγής ημιτονοειδούς συνάρτησης (Sine Wave) βρίσκεται στο Sources

Κώδικας Sine wave Matlab Editor

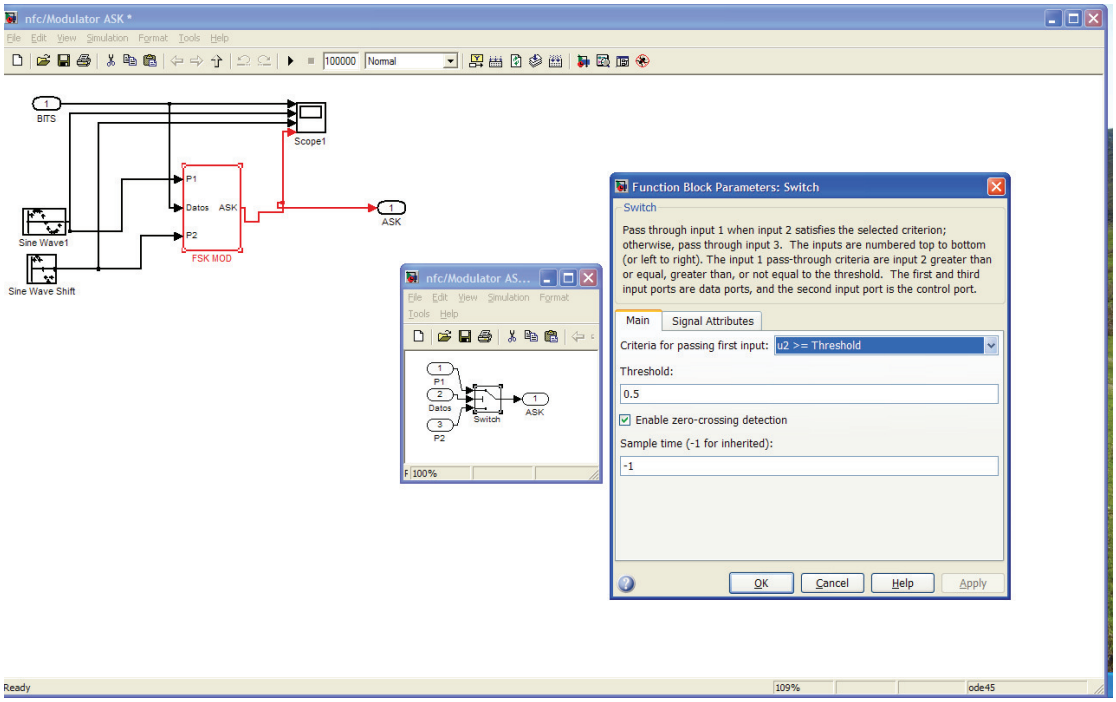
```
hsin1 = signalblks.SineWave (2, 10);
 hsin1.SamplesPerFrame = 1000;
 y = step (hsin1);
 plot (y);
```



Γράφημα 4:Σήμα διακριτού χρόνου Sine Wave

Πώς λειτουργεί το block Bask εξηγείται σε προηγούμενη ενότητα.

FSK Mod: Περιλαμβάνει ηλεκτρικό κύκλωμα που αποτελείται από ένα Switch που ενυπάρχει στη βιβλιοθήκη Signal Routing και έχει τα εξής χαρακτηριστικά: Το μπλοκ Switch διέρχεται διαμέσου της πρώτης εισόδου ή της τρίτης εισόδου με βάση την τιμή της δεύτερης εισόδου. Η πρώτη και η τρίτη συνάρτηση ονομάζονται είσοδοι δεδομένων. Η δεύτερη είσοδος ονομάζεται η είσοδος ελέγχου

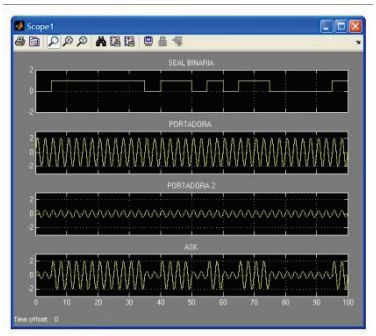


Εικόνα 36:Block Switch

1. **Default u2 >= Threshold:** Ελέγχει αν η τιμή στην είσοδο ελέγχου είναι μεγαλύτερη ή ίση με την τιμή κατωφλίου. Το κατώφλι Αντιστοιχίζει το όριο διακόπτη που καθορίζει ποια είσοδο του μπλοκ περνά στην έξοδο.
2. **Zero-Crossing Detection:** Βηματικός Αναμεταδότης ορίζει την τιμή μιας μεταβλητής, προσαρμόζει δυναμικά το μέγεθος του βήματος του χρόνου, με αποτέλεσμα να αυξάνεται όταν μια μεταβλητή αλλάζει αργά και να μειώνεται όταν μια μεταβλητά αλλάζει ραγδαία. Αυτή η συμπεριφορά του βηματοδότη προκαλεί πολλά μικρά βήματα στην περιοχή μιας ασυνέχειας, επειδή η μεταβλητή αλλάζει γρήγορα σε αυτή την περιοχή. Αυτό βελτιώνει την ακρίβεια, αλλά μπορεί να οδηγήσει σε υπερβολή στο χρόνο προσομοίωσης.

   Το λογισμικό Simulink χρησιμοποιεί την τεχνική που είναι γνωστή ως **Zero-Crossing Detection** διέλευση ανίχνευσης για να εντοπίσει με ακρίβεια μια ασυνέχεια χωρίς την προσφυγή σε υπερβολικά μικρά χρονικά βήματα. Συνήθως αυτή η τεχνική βελτιώνει την προσομοίωση όσο αφορά το χρόνο εκτέλεσης, αλλά μπορεί να σταματήσει κάποιες προσομοιώσεις πριν από την προβλεπόμενη ώρα ολοκλήρωσης τους. Άρα **Default:** On που σημαίνει ενεργοποίηση του **Zero crossing detection**

- **Scope 1 :**Πίνακας 4:Βασικά διαγράμματα Simulink



Γράφημα 5: Modulation ASK

- **AWGN Channel:** Κανάλι λευκού προσθετικού θορύβου

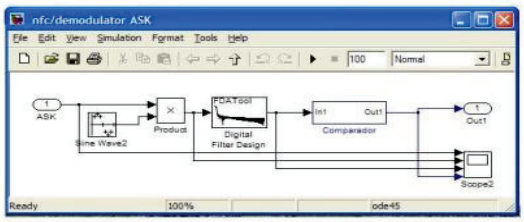
Αυτό το μπλοκ υποστηρίζει πολυκάναλα σήματα εισόδου και εξόδου, καθώς και το πλαίσιο με βάση την επεξεργασία. Τα σήματα εισόδου και εξόδου μπορεί να είναι πραγματική ή σύμπλοκο Όταν χρησιμοποιείτε με πολλαπλές εισόδους, οι τιμές διακύμανσης είναι ίσες μεταξύ πραγματικών και φανταστικών συνιστωσών του σήματος εισόδου. Παράμετροι:

1. Initial Seed: Αρχικός σπόρος, αρχική τιμή(67)
2. Mode: Τη μέτρηση θέλουμε να πάρουμε (Signal to noise ratio)
3. SNR: Η τιμή του SNR(18Db)
4. Input signal power, referenced to 1 ohm (watts): Ισχύς σήματος εισόδου(1 Watt)

- **Goto 2:** Το Goto2 γίνεται είσοδος για **From** 7,6
- **From/From 5:** Είναι σήματα εισόδου στο Block Find delay
- **Block Find delay:** Το μπλοκ **Find delay** βρίσκει την καθυστέρηση μεταξύ ενός σήματος και μιας καθυστερημένης, και ενδεχομένως διαστρεβλωμένης, εκδοχής του εαυτού του. Το συγκρότημα είναι ιδιαίτερα χρήσιμο όταν θέλουμε να συγκρίνουμε και να μεταδώσουμε λαμβανόμενο σήμα για να βρούμε το ποσοστό σφάλματος bit, όταν δεν ξέρουμε την καθυστέρηση στο λαμβανόμενο σήμα. Η θύρα εισόδου σημασμένο sRef λαμβάνει το αρχικό σήμα, ενώ η θύρα εισόδου επισημασμένο SDEL λαμβάνει την καθυστερημένη έκδοση του σήματος. Τα δύο σήματα εισόδου πρέπει να έχουν τους ίδιους χρόνους δείγματος.

- **Display delay:** Εργαλείο σύνθεσης από το μέτρο και τη φάση ενός μιγαδικού. Με το Display μπορούμε να πάρουμε αριθμητικά αποτελέσματα από ένα σύστημα. Το εργαλείο Display βρίσκεται στο Sinks.
- **Goto 1:** Είναι σήμα εισόδου για **From** 5, 4,
- **Demodulator ASK:**

  Δέχεται το σήμα **From 7** που είναι ή έξοδος του **AWGN** και εξάγει το σήμα Goto 1 που είναι οι τα αντίστοιχα σήματα εισόδων **From 5, From 4, From 3.**

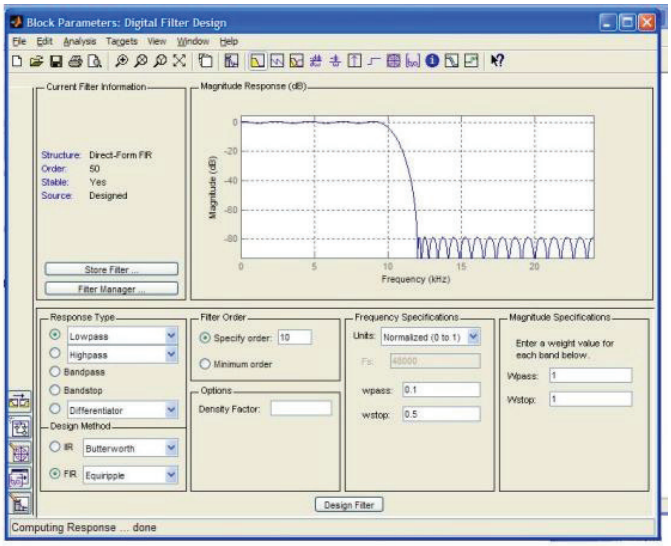


1. **ASK:** Παρέχει μια θύρα εισόδου για ένα υποσύστημα ή μοντέλο, εδώ παράγει την τιμή της εισόδου υποσυστήματος κατά το προηγούμενο χρονικό βήμα.
2. **Sine wave 2** : Πηγή τριγωνομετρικής συνάρτησης δείτε **Sine wave 2** : Πηγή τριγωνομετρικής συνάρτησης
3. **Block Product** : Πολλαπλασιάζει τις τιμές δύο εισόδων

- **Multiplication:** Element-wise (.*)
- **Number of inputs:** 2

4. **Digital filter design –Block Parameters**

Στην επεξεργασία σήματος, η λειτουργία ενός φίλτρου απομακρύνει τα ανεπιθύμητα μέρη ενός σήματος, όπως έναν τυχαίο θόρυβο, ή εξάγει χρήσιμα κομμάτια ενός σήματος, όπως οι συνιστώσες που βρίσκονται σε μια συγκεκριμένη περιοχή συχνοτήτων.



Εικόνα 37: Filter FIR

Τα κουμπιά κάτω από την λίστα filters ανοίγουν παράθυρα ένα με τα οποίο μπορούμε να επεξεργαστούμε η να δημιουργήσουμε φίλτρα. Το FTool είναι ένα εργαλείο απεικόνισης φίλτρων και βοηθά τον χρήστη στην ανάλυση των αποκρίσεων του φίλτρου που έχουμε επιλέξει. Στην παρούσα προσομοίωση έχουμε χρησιμοποιήσει ένα ψηφιακό low pass (χαμηλοδιαβατό) και FIR filter (συνέλιξη με κρουστική απόκριση φίλτρου Kernel filter)

Οι επιλογές απεικόνισης μας δίνουν τα εξής:

1. Magnitude response-Απόκριση Κέρδους φίλτρου
2. Phase response-Απόκριση φάσης φίλτρου
3. Magnitude and Phase response–Απόκριση κέρδους / φάσης του φίλτρου
4. Group delay response
5. Phase delay-καθυστέρηση φάσης
6. Impulse response-κρουστική απόκριση του φίλτρου
7. Polo /zero plot-χάρτης πόλων και μηδενικών
8. Filter coefficients-συντελεστές του παρανομαστή και του αριθμητή
9. Filter information-πληροφορίες για το φίλτρο (τάξη, δομή, τύπος, ευστάθεια, γραμμικότητα φάσης)
10. Magnitude response estimate

11. Round–off noise power spectrum-φάσμα θορύβου

Επιλέξαμε από τις υπάρχουσες λίστες για την προσομοίωση τα:

Response type→Low pass

Design method →FIR

Filter order→Specify order 127

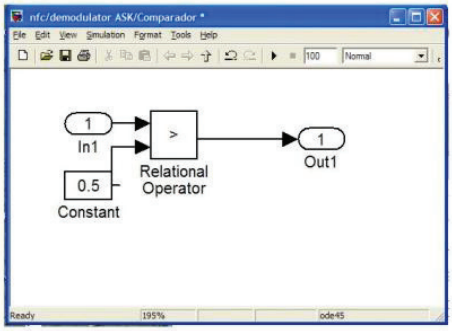
Frequency specification→Normalized (0 to 1)

Wpass→0.1

Wstop→0.5

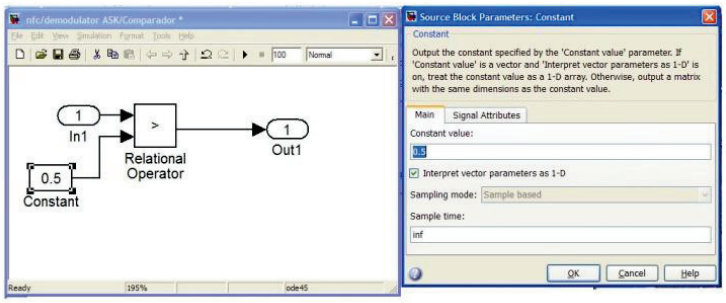
Magnitude specification→ Wpass.1, Wstop.1

5. ASK Comparator



Εικόνα 38: ASK Comparator

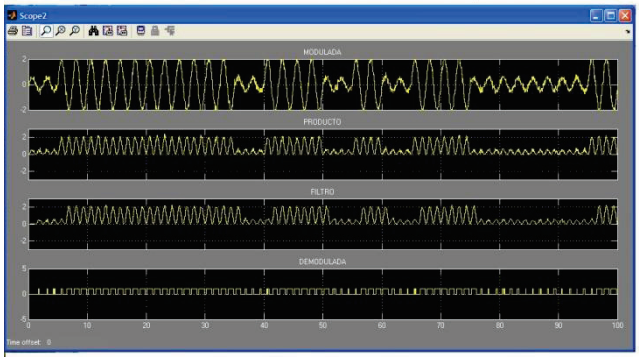
Ηλεκτρικό κύκλωμα που εκτελεί σχεσιακές πράξεις <,>, <=,> =, ==, και ~ =. Οι σχεσιακοί φορείς εκτελούν στοιχείο-προς-στοιχείο συγκρίσεις ανάμεσα σε δύο πίνακες. Επιστρέφουν μια λογική σειρά του ίδιου μεγέθους, με στοιχεία που στο λογικό 1 είναι (αληθής), όπου η σχέση είναι αληθινή, και στοιχεία (ψευδή) στο λογικό 0 όπου η σχέση δεν είναι αληθινή.



Εικόνα 39: Block constant parameters

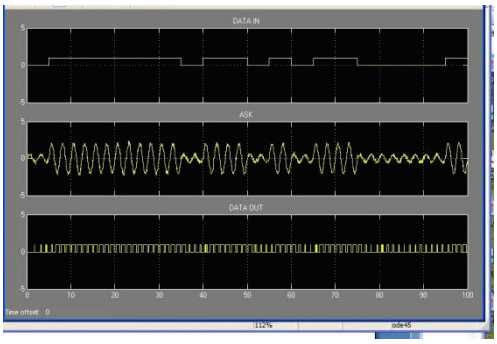
1. **In 1:** Είσοδος 1
2. **O,5:** Καθορίσουμε ένα διάνυσμα για αυτή την παράμετρο, και θέλουμε το μπλοκ να το ερμηνεύσει ως ένα φορέα, επιλέγουμε το διάνυσμα παραμέτρων και την 1-D παράμετρο

6. **Scope2:** Πίνακας 4:Βασικά διαγράμματα Simulink



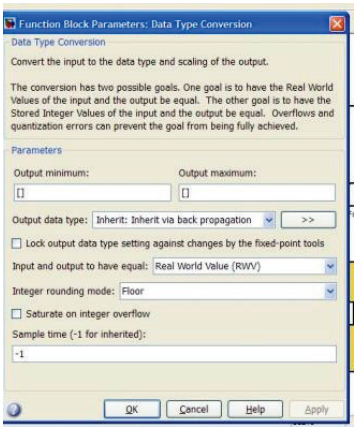
Γράφημα 6: Demodulation ASK

- **Scope:** Έχει σαν εισόδους τα σήματα **From1, From6, From3** που προέρχονται από **From1-Goto1, From6-Goto2, From4-Goto1**



Γράφημα 7:Scope1

- **Convert**



Εικόνα 40: Block Parameters Data Type Conversion

Το μπλοκ μετατροπής τύπου δεδομένων μετατρέπει τα στοιχεία για το είδος των δεδομένων και την κλιμάκωση που έχουμε ορίσει για ένα σήμα εισόδου οποιουδήποτε τύπου Η είσοδος μπορεί να είναι οποιοδήποτε πραγματικό ή μιγαδικό σήμα. Αν η είσοδος είναι πραγματική, η έξοδος είναι πραγματική. Αν η είσοδος είναι πολύπλοκη, η έξοδος είναι πολύπλοκη.

1. **Default: Off**

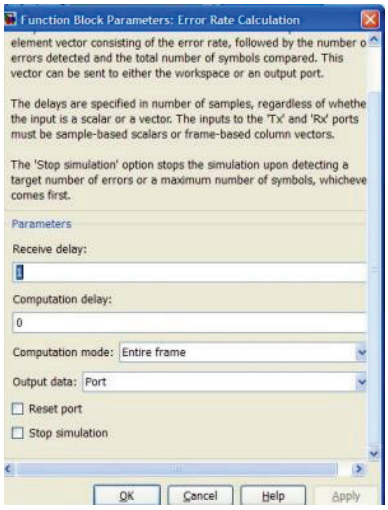
2. **Default: Inherit: Inherit via back propagation**
3. **Specify which type of input and output should be equal**.

Default: Real World Value (RWV): Καθορίζει το στόχο να καταστεί η τιμή World (RWV) της εισόδου να είναι ίδια ισούται με την τιμή World (RWV) της εξόδου.

4. **Specify the rounding mode for fixed-point operations:** Στρογγυλοποίηση

Default: Floor

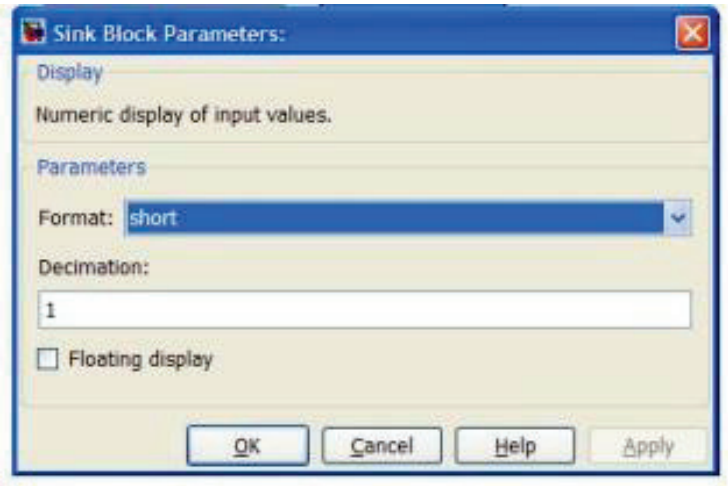
Error rate calculation: Επειδή οι είσοδοι είναι bits, το μπλοκ υπολογίζει το ποσοστό σφάλματος bit.



Εικόνα 41:Error Rate Calculation

Δέχεται τρείς εισόδους (σήματα) **From2 Receiver Goto** και το **From3 Receiver Goto1** που περνά μέσα από το **Convert**

- **Display:** Εμφανίζει τα αποτελέσματα της προσομοίωσης του NFC συστήματος για **SNR=18dB, ASK Modulation,FIR,Delay**
-



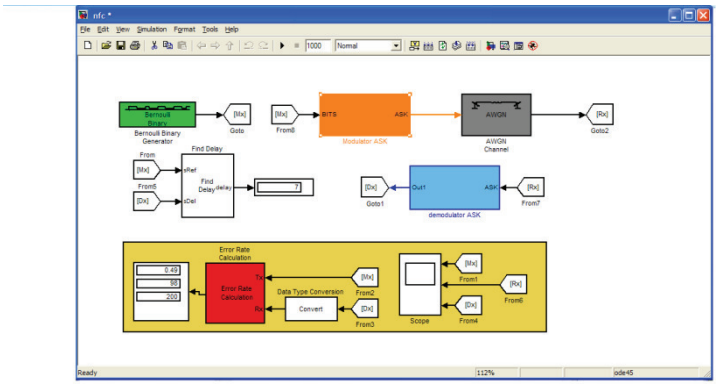
Εικόνα 42: Display parameters

12.3: Αποτελέσματα Προσομοίωσης

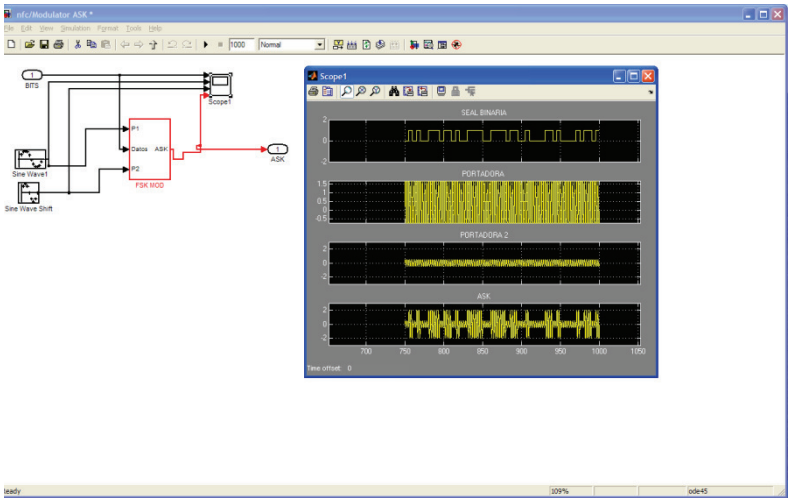
0,6	BER
12	ο συνολικός αριθμός σφαλμάτων, δηλαδή, οι συγκρίσεις μεταξύ άνισων στοιχείων
20	Ο συνολικός αριθμός των συγκρίσεων που γίνονται στο Block
0	Delay

Εικόνα 43: Αποτελέσματα 1

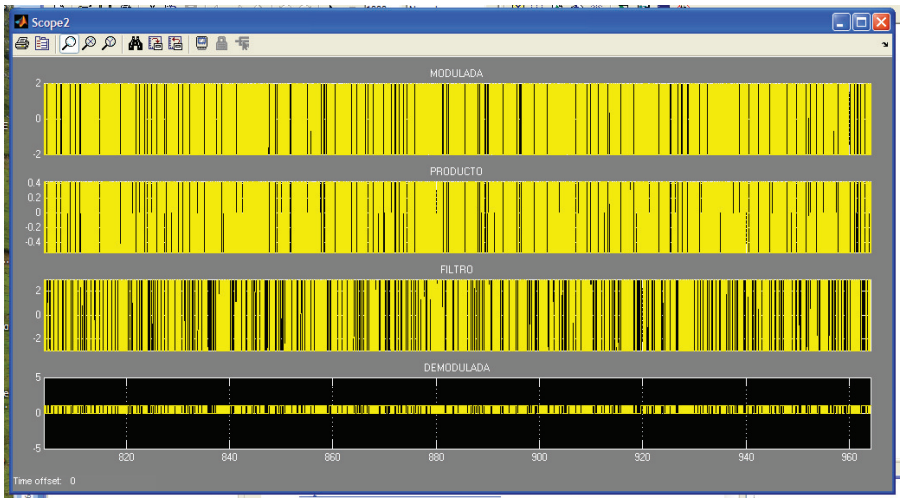
12.4: Εκτέλεση Προσομοίωσης 1000 time simulation stop



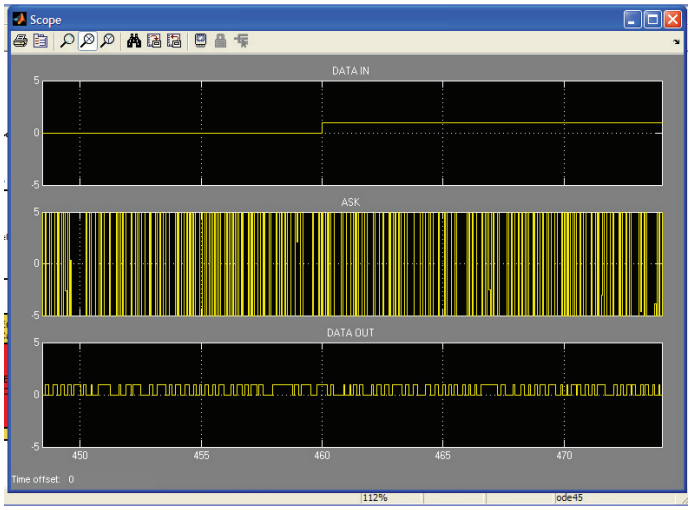
Εικόνα 44: Screen Short NFC2



Γράφημα 8: Modulation ASK



Γράφημα 9: Demodulation Ask



Γράφημα 10: Scope2

Display: Εμφανίζει τα αποτελέσματα της προσομοίωσης του NFC συστήματος για **SNR=-35dB, ASK Modulation,FIR,Delay**

12.5: Αποτελέσματα προσομοίωσης

0,49	BER
98	ο συνολικός αριθμός σφαλμάτων, δηλαδή, οι συγκρίσεις μεταξύ άνισων στοιχείων
200	Ο συνολικός αριθμός των συγκρίσεων που γίνονται στο Block
7	Delay

Εικόνα 45: Αποτελέσματα 2

ΚΕΦΑΛΑΙΟ 13

Βιβλιογραφία –Αναφορές

[1] http://eleftheroiellines.blogspot.gr/2012/10/rfid-rfid-chip

[2] CoreRfid$_{LTD,}$ Richard Harrison, Munzi Ali, Terry Allern

[3] Mobile Payments Today GSMA announces worldwide support for SIM-based NFC

[4] http://broadband.cti.gr/el/index.php

Υπηρεσίες Προώθησης Ευρυζωνικότητας

[5] http://supportforums.blackberry.com/t5/Java-Development/NFC-Primer-for-Developers/ta-p/1334857

[6] http://tech.in.gr/short-news/?aid=1231116834

[7] Gerhard_Romen_NFC_Forum_Transport.pdf

[8] http://el.wikipedia.org/wiki/NFC

[9] http://www.samacards.gr

[10]http://www.hotech.gr/index.php/el/what-we-do-el/solutions/nfc-solutions/nfc-campus

[11] http://www.hotech.gr/index.php/el/what-we-do-el/solutions/identity

[12] http://ece.wpi.edu/~dchasaki/papers/Security in NFC.pdf

[13] http://eleftheroiellines.blogspot.gr/2012/10/rfid-chip-rfid-chip.html

[14] ΑΡΧΕΣ ΛΕΙΤΟΥΡΓΙΑΣ ΚΑΙ ΕΦΑΡΜΟΓΕΣ

ΣΥΣΤΗΜΑΤΩΝ ΡΑΔΙΟΤΑΥΤΟΠΟΙΗΣΗΣ-RFID(Lyrarakis 2011)

[15] IEEE 802.11-Βικιπαίδεια

[16] Matlab για επιστήμονες και μηχανικούς

ΕΥΑΓΓΕΛΟΣ Β. ΧΑΤΖΙΚΟΣ Εκδόσεις ΤΖΙΟΛΑ

[17] Εγχειρίδιο Matlab Simulink Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Μηχανολόγων Μηχανικών

[18] Τηλεπικοινωνιακά συστήματα ΙΙ (Τεχνικές ψηφιακής διαμόρφωσης –Σεμινάριο ΙΕΕΕ)

Δρ.Μιχάλης Παρασκευάς Επίκ.Καθηγητής ΤΕΣΥΔ/ΤΕΙΜΕΣ