ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ ΜΕ ΘΕΜΑ :

JAMMING (Ο ΗΛΕΚΤΡΟΝΙΚΟΣ ΠΟΛΕΜΟΣ)

Της σπουδάστριας :

ΚΟΛΙΟΥ- ΒΕΡΓΟΥ ΑΦΡΟΔΙΤΗ
Α.Μ.: 5105
Ζ' ΕΞΑΜΗΝΟ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ
ΛΑΜΠΡΟΣ ΝΙΚ. ΣΑΚΚΑΣ

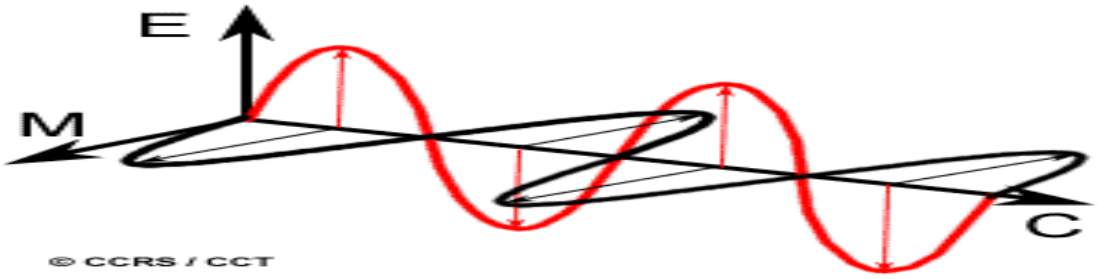
ΑΦΙΕΡΩΝΕΤΑΙ ΣΤΑ ΠΑΙΔΙΑ ΜΟΥ ,
ΤΟΝ ΣΠΥΡΟ
και
ΤΗΝ ΚΩΝΣΤΑΝΤΙΝΑ – ΔΗΜΗΤΡΑ ,
ΤΟΝ ΑΝΔΡΑ ΜΟΥ ,
ΣΤΟΥΣ ΓΟΝΕΙΣ ΜΟΥ
ΚΑΙ ΤΟΝ ΑΔΕΡΦΟ ΜΟΥ ,ΓΙΑΝΝΗ

ΕΥΧΑΡΙΣΤΩ ΘΕΡΜΑ
ΤΗΝ ΟΙΚΟΓΕΝΕΙΑ ΜΟΥ
ΓΙΑ ΤΗΝ ΗΘΙΚΗ ,
ΥΛΙΚΗ
& ΨΥΧΙΚΗ
ΣΥΜΠΑΡΑΣΤΑΣΗ
ΚΑΙ ΣΤΗΡΙΞΗ

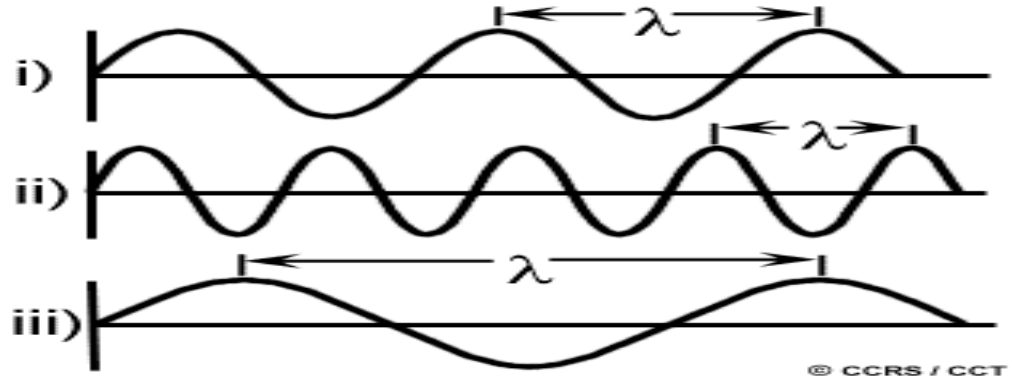
ΠΕΡΙΕΧΟΜΕΝΑ

Γενικά

Τα τελευταία χρόνια παρατηρούμε μια απότομη και ραγδαία ανάπτυξη της τεχνολογίας .Ιδιαίτερη ανάπτυξη γνώρισαν οι τομείς της πληροφορικής και των τηλεπικοινωνιών . Χάρη αυτών των επιστημών οι άνθρωποι κατασκεύασαν πολλές ηλεκτρικές και ηλεκτρονικές συσκευές , ζουν καλύτερα και ανετότερα σε σχέση με τα προηγούμενα χρόνια. Έχουν πολλές ευκολίες και ελευθερίες ,σε σημείο εξάρτησης ορισμένες φορές από αυτές ,που έχουν μπει στην ζωή μας και μας την ελέγχουν .
Οι περισσότεροι άνθρωποι στις ανεπτυγμένες χώρες έχουν ένα κινητό τηλέφωνο ,ένα ραδιόφωνο και μια τηλεόραση . Τα πάντα τα εντοπίζουν γρήγορα με τα ραντάρ . Επικοινωνούν και εξυπηρετούνται γρήγορα και απλά μέσω ηλεκτρονικών υπολογιστών .Βλέπουν και ακούν άμεσα τι γίνεται στον κόσμο και ότι τους ενδιαφέρει λες και είναι παρόντες. Όλοι έχουν πρόσβαση στους υπολογιστές από τους μικρούς ως τους μεγάλους και από τους μαθητές σχολείου ως το διάστημα .
Έχουμε δυο τρόπους επικοινωνίας των ηλεκτρονικών υπολογιστών και γενικότερα των δικτύων , τον ενσύρματο και τον ασύρματο.
Ο ενσύρματος τρόπος σύνδεσης γίνεται με την χρήση καλωδίων ενώ ο ασύρματος τρόπος γίνεται κυρίως με την χρήση κεραιών και χωρίς την χρήση καλωδίων. Ανάμεσα στις κεραίες δημιουργείται ένα ηλεκτρομαγνητικό πεδίο
(βλέπε στο σχήμα)



Η ηλεκτρομαγνητική ακτινοβολία έχει χαρακτηριστικά που προκύπτουν από την θεωρία των εξισώσεων Maxwell. Το ηλεκτρικό και το μαγνητικό πεδίο ενός ηλεκτρομαγνητικού κύματος είναι κάθετα μεταξύ τους και επίσης προς την διεύθυνση διάδοσης του κύματος.

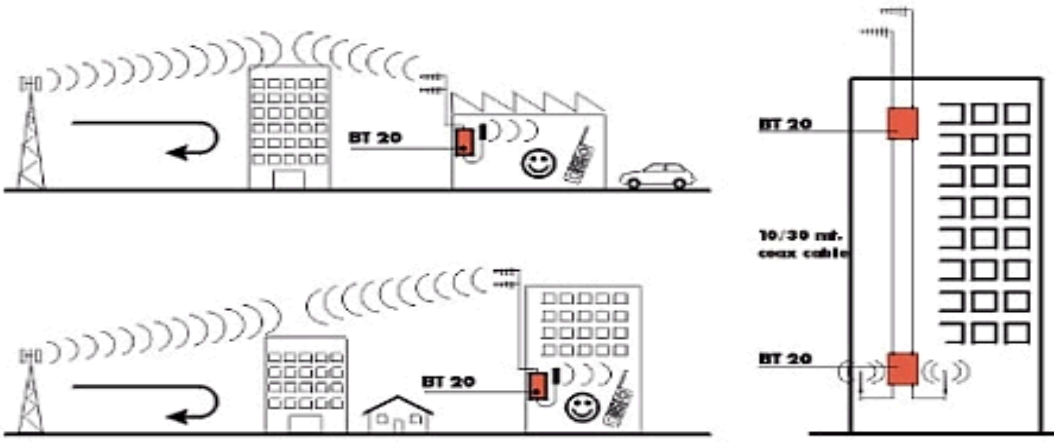


Η χωρική απόσταση ανάμεσα σε δύο μέγιστα ή ελάχιστα για τα δύο πεδία (τα οποία είναι σε συμφωνία φάσης σε ένα επίπεδο κύμα) ονομάζεται **μήκος κύματος λ**.(όπως φαίνεται στο παραπάνω σχήμα) [Γ', 8]

ΕΙΣΑΓΩΓΗ

Στον ενσύρματο τρόπο μετάδοσης μπορούμε με καταστροφή των καλωδίων να καταστρέψουμε την επικοινωνία .Στον ασύρματο τρόπο επικοινωνίας οι ηλεκτρομαγνητικές παρεμβολές προέρχονται από α) άμεση ή κοντινή κεραυνική εκκένωση (LEMP – Lightning Electromagnetic Impulse) . β)μεταγωγές φορτίων στο σύστημα μεταφοράς και διανομής ηλεκτρικής ενέργειας (SEMP-Switching Electromagnetic Discharges) γ) διαταραχές του επιπέδου τάσης των γραμμών μεταφοράς ηλεκτρικής ενέργειας δ) ηλεκτροστατικές κενώσεις ESD-Electrostatic Discharges) ε) παρεμβολές από πομπούς υψηλής ισχύος στο ραδιοηλεκτρικό τμήμα του φάσματος στ) ηλεκτρομαγνητικοί παλμοί από πυρηνικές εκρήξεις (NEMP-Nuclear electromagnetic Impulse)

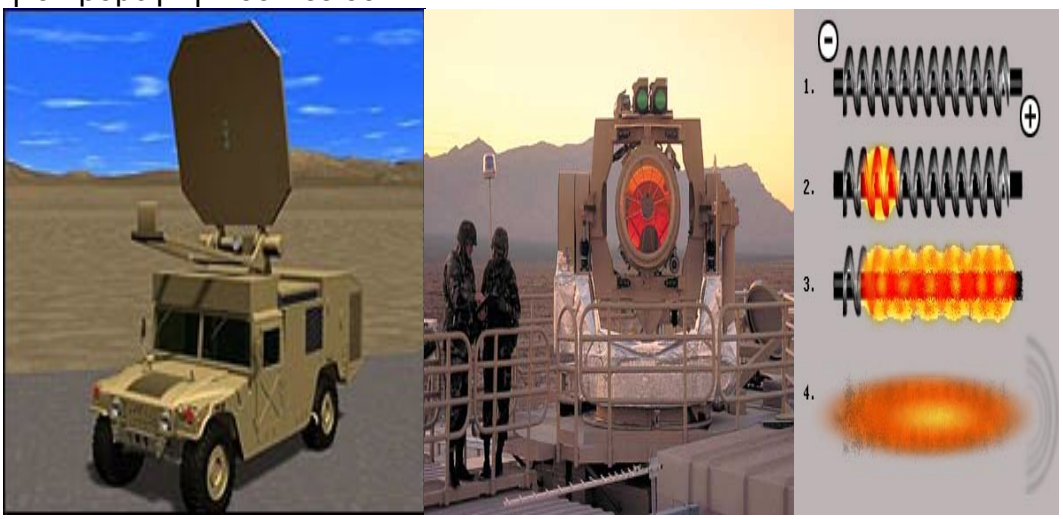
.



(Στο σχήμα βλέπουμε ένα υψηλό κτίριο μπορεί να δημιουργήσει προβλήματα στις επικοινωνίες γι' αυτό ο δέκτης πρέπει να είναι σε υψηλότερο σημείο από το κτίριο ή να υπάρχει ενδιαμέσος πομπός ,πάνω στο κτίριο) .

Προβλήματα ασφάλειας

Εκτός από τους παραπάνω φυσικούς και τεχνικής τρόπους μπορούμε να παρέμβουμε όπως αναφέραμε ορισμένες φορές εσκεμμένα και να παρεμποδίσουμε την επικοινωνία με την χρήση ηλεκτρομαγνητικού κύματος .
Στα παρακάτω σχήματα βλέπουμε <<όπλα >> που χρησιμοποιούνται σε ηλεκτρονικό πόλεμο με αποτέλεσμα να νεκρώνουν όλες οι ηλεκτρομαγνητικές συσκευές και ηλεκτρομαγνητικές επικοινωνίες και για αυτό ονομάζονται ε-βόμβες ή ηλεκτρομαγνητικές βόμβες .
.Στο αριστερό σχήμα βλέπουμε μια φορητή κεραία παρεμβολής , στο κεντρικό σχήμα βλέπουμε ακτίνες λέιζερ που καταστρέφουν τις κεραίες επικοινωνίας και στο δεξιό σχήμα βλέπουμε τον εσωτερικό τρόπο παραγωγής ηλεκτρομαγνητικού πεδίου .



ΣΧΗΜΑ ΗΛΕΚΤΡΟΜΑΓΝΗΤΙΚΑ ΟΠΛΑ [Γ’ ,18]

Με άλλα λόγια έτσι γίνεται το jamming ή αλλιώς ο ηλεκτρονικός πόλεμος .

- Το jamming ή ηλεκτρομαγνητικός πόλεμος σύμφωνα με την ψηφιακή βιβλιοθήκη είναι μια αμυντική δραστηριότητα που στηρίζεται στη χρήση ηλεκτρονικών μέσων, με σκοπό την παρεμπόδιση ή τον αποκλεισμό του εχθρού από τις επιθετικές δυνατότητες που προσφέρει η χρήση του ηλεκτρομαγνητικού φάσματος. Για τις ανάγκες του ηλεκτρονικού πολέμου χρησιμοποιούνται, όπως είναι φυσικό, ποικίλες συσκευές, από τον πιο απλό ασύρματο έως τον πιο σύγχρονο αναγνωριστικό δορυφόρο.
- Η παρεμβολή (**jamming**) είναι εσκεμμένα παραγόμενη παρεμβολή, συνήθως σε περιπτώσεις πολεμικών αεροπλάνων για αποπροσανατολισμό του radar.

Ο Ηλεκτρονικός Πόλεμος επίσης θεωρείται κλάδος ***του Πληροφοριακού Πολέμου (IW: Information Warfare).*** Η δημιουργία των τηλεπικοινωνιακών δικτύων συστήματος Πληροφοριών , Διοίκησης ,Επικοινωνιών , Ελέγχου και Επιτήρησης [(***Command, Control, Communications, Consultation & Intelligence (C^4I),***] απαιτεί να υπάρχει μια διαθεσιμότητα και συνεργασία όλων των υπηρεσιών ,διοικήσεων ,επιτελείων και μονάδων στρατού και όλες οι ανταλλαγές πληροφοριών(Audio, Video, Text, Data) γίνονται σε πραγματικό χρόνο με πολύ υψηλές ταχύτητες δεδομένων και εκεί υπεισέρχονται οι ιδιαίτερες απαιτήσεις του Ηλεκτρονικού Πολέμου όσον αφορά το φυσικό στρώμα ενός Δικτύου Ηλεκτρονικών Υπολογιστών (Computer Network Physical Layer). Τα συστήματα ***C^4I(σι φορ άι)***

προέρχονται κατευθείαν από τις βαριές στρατιωτικές εφαρμογές με την ονομασία C^3I (Command, Control, Communications & Intelligence) στην εποχή του Ψυχρού Πολέμου αλλά στην εποχή μας τα χρησιμοποιούν παντού και έχοντας ως κάλυμμα της προστασίας από την τρομοκρατία πρόσθεσαν και το 4 C (Consultation) και από C^3I έγινε C^4I.Ένα από τα υποσυστήματα του C^4I ,είναι το δίκτυο επικοινωνιών TETRA ,επίγειο συγκαναλικό ραδιοδίκτυο , σύμφωνα με την επίσημη ονομασία του). Ο ΟΤΕ είχε ήδη εγκαταστήσει ένα δίκτυο TETRA ,που στα τέλη του 2002 κάλυπτε μόνον το λεκανοπέδιο της Αττικής , τον Αργοσαρωνικό ,και τέσσερις μεγάλες πόλεις (Θεσσαλονίκη , Ηράκλειο Κρήτης , Πάτρα , Βόλο) καθώς και τον κορμό του εθνικού οδικού δικτύου. Οι απαιτήσεις αυτές δεν συνίστανται μόνον στην πολιτική εκπομπών με τη συμβατική της έννοια (εκπέμπω ή δεν εκπέμπω) αλλά συμπεριλαμβάνουν την έννοια της πληροφορίας ως σύνολο, σε κάθε της διάσταση και διαμέσου κάθε δυνατού μέσου διάδοσης, όπως διαμέσου ξηράς, διαστήματος (ασύρματη επικοινωνία), υποθαλάσσιος και κυβερνοχώρου. [Γ',65]

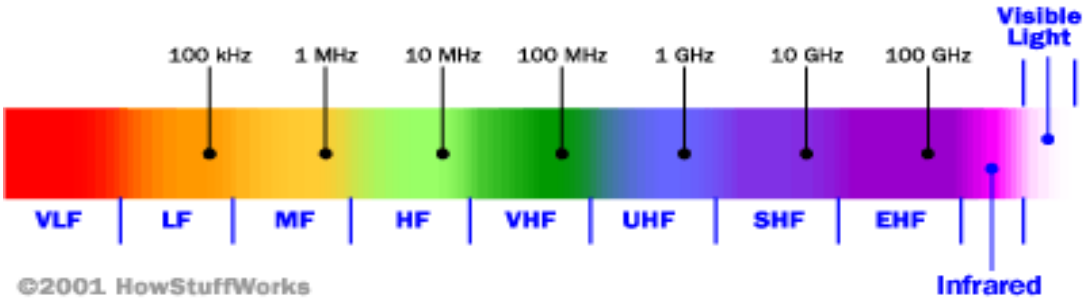
Σε τελική ανάλυση ο πόλεμος των κρατών γίνεται σύμφωνα με τον ΚΩΝ/ΝΟ ΓΕΡΟΚΩΣΤΟΠΟΥΛΟΣ (ΔΝΤΗΣ ΣΤ΄ΚΛΑΔΟΥ ΓΕΕΘΑ) ΣΤΗΝ ΕΡΓΑΣΊΑ ΤΟΥ ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΣΤΡΑΤΟΥ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ στο συνέδριο για την προστασία της κρίσιμης υποδομής της χώρας , σε πέντε διαστάσεις. Με άλλα λόγια η μεγαλύτερη μάχη γίνεται στον κυβερνόχωρο ,και μάλιστα ο πληροφοριακός πόλεμος. .

Στην εργασία θα αναφερθούμε πως ξεκίνησε ,πόσο αποτελεσματικός είναι , που, πως και με ποιον τρόπο γίνεται ο ηλεκτρονικός πόλεμος κυρίως στα ραντάρ και στο GSM (κινητή τηλεφωνία). Θα μιλήσουμε και ποια είναι τα βασικότερα είδη jamming ,αλλά και για τις τεχνικές που μπορούμε να χρησιμοποιήσουμε για να τον αποφύγουμε (anti-jamming) .Θα εξηγήσουμε και για την << ΑΡΝΗΣΗ ΕΞΥΠΗΡΕΤΗΣΗΣ >>(Denial Of Service-DOS) στα δίκτυα δηλαδή όταν στους εξουσιοδοτημένους χρήστες δεν παρέχεται η απαιτούμενη υπηρεσία μέσα σε μια καθορισμένη μέγιστη χρονική διάρκεια.
Πιθανότατα η πρώτη DOS Επίθεση που χρησιμοποιήθηκε στις ηλεκτρονικές επικοινωνίες ήταν το jamming στις ραδιοσυχνότητες των ενόπλων δυνάμεων . Στους στρατιωτικούς όρους το jamming είναι ο «απαλός θάνατος» (“soft killer “) από μια ηλεκτρονική επίθεση.Στην σημερινή εποχή μπορούμε να συναντήσουμε να κάνουν ηλεκτρονικό πόλεμο από έναν απλό πολίτη ,μια επιχείρηση ,έναν οργανισμό μέχρι και κανονικό πόλεμο ανάμεσα στα κράτη. (όπως ο ηλεκτρονικός πόλεμος στον κόλπο) .Το jamming το χρησιμοποιούν οι ανταγωνιστικές εταιρείες στην αγορά (με μορφή υποκλοπών) , οι μυστικές υπηρεσίες (ηλεκτρονική κατασκοπεία) ,οι κυβερνήσεις σε καταστάσεις υψηλού κίνδυνου (πόλεμος, τρομοκρατία ,παρακολούθησης με μορφή συνακρόασης) και αλλού.

ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

Για να δούμε πως ξεκίνησε το jamming θα πρέπει να επεξηγήσουμε τους όρους ραντάρ , GSM ,TETRA , GPS , 3G/UMTS,WCDMA και ραδιοκύματα .

Τα ραδιοκύματα είναι το φυσικό μέσο στο οποίο βασίζονται όλες οι ασύρματες τεχνολογίες (GSM ,Wi-Fi , Bluetooth) .Χαρακτηρίζονται από μεγάλη ευελιξία και ταχύτητες μεταφοράς δεδομένων , αλλά είναι επιρρεπείς σε παρεμβολές ,ενώ παράλληλα ανακύπτουν ζητήματα ασφαλείας .[Α',30].
Οι ραδιοσυχνότητες περιγράφουν το τμήμα ηλεκτρομαγνητικού φάσματος που αντιστοιχεί στην περιοχή από 10 KHz ως 300 GHz.Το τμήμα μετξύ 300MHz και 300 GHz συνήθως καλείται μικροκύματα (microwaves,MW) ενώ συχνά χρησιμοποιείται και ο όρος χιλιοστομετρικά κύματα (millimeter,mmW) για την περιοχή 30-300 GHz.[Γ',37]



Η Διεθνής Ένωση Τηλεπικοινωνιών (ITU, International Telecommunications Union) καθόρισε τον παρακάτω τρόπο χωρισμού της ζώνης Ραδιοσυχνοτήτων:

ELF	Extremely Low Freq.	30-300Hz	1-10Mm
VF	Voice Freq.	300-3000Hz	100-1000Km
VLF	Very Low Freq.	3-30KHz	10-100Km
LF	Low Freq.	30-300KHz	1-10Km
MF	Medium Freq.	300-3000KHz	100-1000m
HF	High Freq.	3-30MHz	10-100m
VHF	Very High Freq.	30-300MHz	1-10m
UHF	Ultra High Freq.	300-3000MHz	10-100cm
SHF	Super High Freq.	3-30GHz	1-10cm
EHF	Extremely High Freq.	30-300GHz	1-10mm
	Sub millimeter	300-3000GHz	100-1000μm

Οι τελευταίες τέσσερις υποδιαιρέσεις (δηλ. UHF, SHF, EHF, submillimeter) αποτελούν τα λεγόμενα **μικροκύματα.** Το μήκος κύματός τους βρίσκεται στην ζώνη 1m-1mm.
Ας αναφέρουμε τώρα κάποιες τυπικές εφαρμογές που εμπίπτουν στην ζώνη λειτουργίας των Ραδιοσυχνοτήτων:
Η ραδιοφωνία AM εμπίπτει στην ζώνη 535-1700KHz (MF)

Η ζώνη υψηλής συχνότητας (HF) χρησιμοποιείται στην ραδιοφωνία μικρού μήκους κύματος (βραχέα), στην ναυσιπλοία, και στις ερασιτεχνικές CB επικοινωνίες.
Η ραδιοφωνία FM εμπίπτει στην ζώνη 88-108MHz.
Η ζώνη VHF χρησιμοποιείται για συνήθεις τηλεοπτικές εφαρμογές (TV), περιέχει ζώνες χρησιμοποιούμενες από την αστυνομία, σε εφαρμογές walkie-talkie, κ.α.
Στην ζώνη UHF εμπίπτουν τα κυψελικά τηλέφωνα (cell phones), προσωπικά συστήματα επικοινωνιών (PCS), ασύρματα τηλέφωνα (cordless phones), global positioning systems (GPS), συστήματα ταυτοποίησης μέσω ραδιοσυχνοτήτων (RF identification systems), UHF-TV κανάλια, μικροκυματικούς φούρνους και ραντάρ κατόπτευσης μακρινών αποστάσεων (Long-range surveillance radar).
Η μικροκυματική ζώνη SHF χρησιμοποιείται σε ραντάρ ελέγχου κυκλοφορίας, και επόπτευσης πορείας (track surveillance), οδήγησης πυραύλων-βλημάτων (missile guidance), όπως και σε ραντάρ χαρτογράφησης και πρόβλεψης καιρού, καθώς και δορυφορικές επικοινωνίες.
Βιομηχανικές, επιστημονικές και ιατρικές εφαρμογές εμπίπτουν στην ζώνη UHF καθώς και στην χαμηλή ζώνη SHF, περίπου στην περιοχή των 900 MHz. Σαν παράδειγμα η Ραδιοαστρονομία χρησιμοποιεί την UHF ζώνη και τις περιοχές L-W της μικροκυματικής περιοχής.
Οπτικές επικοινωνίες με χρήση οπτικών ινών χρησιμοποιούν φως Laser στην περιοχή των 1-20μm λόγω των μικρών απωλειών που παρουσιάζουν οι οπτικές ίνες στην περιοχή αυτή. Πέρα από τις ραδιοσυχνότητες (RF) έχουμε την υπέρυθρη (IR) ακτινοβολία που εκτείνεται στην περιοχή 100-1μm (ή ισοδύναμα στην περιοχή συχνοτήτων 3-300THz, 1THz=$10^{12}\,Hz$)[Γ', 8]

Το *ραντάρ* (radar = Radio Detection And Ranging ή επίσης Radio Angle Detection And Ranging) είναι ένα ηλεκτρομαγνητικό σύστημα , που χρησιμοποιείται στον εντοπισμό και ανίχνευση αντικειμένων. Η λειτουργία του ραντάρ βασίζεται στην εκπομπή ηλεκτρομαγνητικών κυμάτων(μιας ημιτονοειδούς κυματομορφής) και στην ανάκλαση των ηλεκτρομαγνητικών κυμάτων, που όταν προσπέσουν σε κάποιο σώμα, επιστρέφουν πίσω στην πηγή που τα έστειλε. Το ραντάρ αποτελείται από έναν πομπό, ο οποίος είναι συνήθως μια κατευθυντική κεραία παραβολικού σχήματος, από ένα δέκτη, που τις περισσότερες φορές είναι η ίδια η κεραία και από μια οθόνη απεικόνισης, και έτσι βγάζουν τα αντίστοιχα συμπεράσματα. Έχουν πολλές εφαρμογές προπάντων στο στρατό (εντοπισμό εχθρικών αεροπλάνων και κίνδυνων ,πλοίων ,υποβρυχίων) ,στα συστήματα εθνικής ασφάλειας ,στην αεροπορία ,στην μετεωρολογία και σε παρά πολλούς άλλους τομείς έρευνας , αναγνώρισης και εντοπισμού στοιχείων. Το ραντάρ αποτελεί τον κύριο στόχο των συσκευών ηλεκτρονικού πολέμου που προσπαθούν να αφαιρέσουν από τον αντίπαλο τη δυνατότητα της έγκαιρης προειδοποίησης.
Παρακάτω βλέπουμε τις συχνότητες και χρήσεις ραντάρ (για τις πλέον σημαντικές εφαρμογές σύμφωνα με τα πρακτικά του 7^{ου} πανελλήνιο συνέδριο ΄φυσικής και το 6^{ο} κοινό συνέδριο Ένωσης ελλήνων φυσικών και ένωσης Κυπρίων φοιτητών [Γ', 23]

ΣΥΧΝΟΤΗΤΕΣ & ΧΡΗΣΕΙΣ ΤΩΝ RADAR (για τις πλέον σημαντικές εφαρμογές)			
Σύμβολο Ζώνης	*Ζώνη Συχνοτήτων F (GHz)*	*Μήκη Κύματος λ (cm)*	*Τύπος Radar (εφαρμογές)*
L	1,35 - 1,40	22,2 - 21,4	διάφορα στρατιωτικά Radar
S	2,45 - 2,69	12,3 - 11,2	Radar για πολιτικές χρήσεις
S	2,70 - 2,90	11,1 - 10,4	επιτήρηση στρατιωτικών αεροδρομίων
S	2,90 - 3,10	10,4 - 9,7	Radar για τη ναυσιπλοϊα
S	2,90 - 3,70	10,4 - 8,1	Radar για ποικίλες χρήσεις
C	4,2 - 4,4	7,1 - 6,8	διάφορα υψομετρικά Radar
C	5,35 - 5,47	5,6 - 5,5	Radar καιρού (μετεωρολογικά)
C	5,25 - 5,925	5,7 - 5,1	Radar για ποικίλες χρήσεις
X	8,5 - 10,55	3,53 - 2,84	Radar για ποικίλες χρήσεις
X	9,0 - 9,2	3,33 - 3,26	Radar για προσέγγιση ακριβείας
X	9,3 - 9,5	3,23 - 3,16	Radar καιρού και ναυσιπλοΐας
X	10,525	2,85	Radar για την αστυνομία
X	8,5 - 10,55	3,53 - 2,84	Radar για ποικίλες χρήσεις
Ku	15,7 - 17,7	1,91 - 1,70	Radar για ποικίλες χρήσεις
K	24,15	1,24	Radar για την αστυνομία
K	24,25 - 25,25	1,24 - 1,19	Radar για την αεροπλοΐα
Ka	31,8 - 33,4	0,94 - 0,90	Radar για την αεροπλοΐα
Ka	33,4 - 36,0	0,90 - 0,83	Radar για ποικίλες χρήσεις
V	43,0 - 48,0	0,70 - 0,63	Radar για ποικίλες χρήσεις

Η ηλεκτρομαγνητική παρεμβολή (Electro-Magnetic Interference, EMI) του Radar έχει επιτρεπτά όρια ανοχής τα 1~2 KV/m για τις στρατιωτικές διατάξεις & αυτοκίνητα, 10~200 V/m για τις εμπορικές συσκευές κλπ.Αν η ακτινοβολία του Radar υπερβεί το όριο ανοχής, τότε δημιουργούνται προβλήματα λειτουργίας στα παρεμβάλλομένα συστήματα.Η κεραία του Radar περιβάλλεται από μια ζώνη ραδιοεπιδράσεων (Radio-Frequency Interference, RFI), δηλαδή από μια περιοχή με ακτίνα R_{EMI}, στην οποία θα υπάρχουν λειτουργικές επιπτώσεις που ίσως εξελιχθούν σε επικινδυνότητα, δεδομένου ότι οι τιμές κορυφής του πεδίου E_{peak} ή/και H_{peak} θα υπερβαίνουν τα επιτρεπτά ‘όρια E_{EMC} ή/και H_{EMC} ,, $E_{EMC} = E_{PEAK}$ ή $H_{PEAK} = H_{EMC}$ Η R_{EMI} στο απόμακρο πεδίο ενός Radar προσδιορίζεται από τις: $R_{EMI} = \sqrt{\frac{Z_o P_{rad}(\theta,\varphi)}{4\pi E_{EMC}^2}}$ ή $R_{EMI} = \sqrt{\frac{P_{rad}(\theta,\varphi)}{4\pi Z_o H_{EMC}^2}}$

Στον επόμενο πίνακα δίδονται παραδείγματα της R_{EMI} για ραδιοπαρεμβολές από την ακτινοβολία που χρησιμοποιεί το Radar για ραδιοανίχνευση (in band EMI).

ΑΚΤΙΝΑ R_{EMI} ΤΗΣ ΖΩΝΗΣ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ ΑΠΟ ΠΑΡΕΜΒΟΛΕΣμέσα στη ζώνη (in band EMI) με παράμετρο την E_{EMC} = 10V/m, 100V/m & 1KV/m						
Τύπος	*Χαρακτη-*	*Ζώνη &*	*$P_{rad}(\theta,\varphi)$*	*R_{EMI} (m)*		
Radar	*ριστικά*	*Συχνότητα*	*KWp*	*E_{EMC}=10V/m*	*E_{EMC}=100V/m*	*E_{EMC}=1KV/m*
στρατιωτικό	Pulsed 500KWp G=36db	S (SHF)3GHz	2 000	24 437	2 444	244
πολιτικής αεροπορίας	Pulsed 200KWp G=41db	X (SHF) 9GHz	2 517 851	27 484	2 748	275
επιβατηγό πλοίο	Pulsed 15KWp G=29db	S (SHF) 3GHz	12 000	1 891	189	19
επιβατηγό πλοίο	Pulsed 10KWp G=36db	X (SHF)9,3GHz	40 000	3 456	346	35
τροχαίας	CW 0,2 Wp κεραία 23db	K (SHF)24,15GHz	40 W	110	11	1

Η ακτίνα R_{EMI} στην οποία υπάρχουν ραδιοπαρεμβολές απότηνπαρασιτικήακτινοβολία $P_{EMI}(\theta,\varphi)$ του Radar (out of band EMI) είναι μικρότερη και προκύπτει από την αντίστοιχη τιμή του πίνακα πολλαπλασιασμένη με τον παράγοντα

$$a = \sqrt{\frac{P_{EMI}(\theta,\varphi)}{P_{rad}(\theta,\varphi)}}$$

ΡΑΝΤΑΡ ΑΝΙΧΝΕΥΣΗΣ ΚΙΝΗΣΕΩΝ ΕΠΙΦΑΝΕΙΑΣ Surface Movement Radar (SMR) του Διεθνούς Αερολιμένα Αθηνών ,Ελ. Βενιζέλος του Γιώργου Χατζηπανάγου

Το Radome της κεραίας του Ραντάρ Κινήσεων Επιφανείας στην κορυφή του Πύργου Ελέγχου

Πομπός (Transmitter)

Το GSM (Global System for Mobile Communications) είναι ένα πρότυπο ψηφιακής επικοινωνίας που επικρατεί σήμερα στην Ευρώπη και χρησιμοποιείται τόσο στην τηλεφωνία (κυρίως κινητής τηλεφωνίας) όσο και στην μεταφορά πακέτων –δεδομένων και μηνυμάτων .Διαθέτει όλα τα γενικά πλεονεκτήματα των ψηφιακών συστημάτων όπως καλύτερη ποιότητα, υπηρεσίες ,αξιοπιστία και εξασφάλιση του απόρρητου μέσου της κρυπτογράφησης του σήματος. Ένα μεγάλο τμήμα των τωρινών δικτύων λειτουργούν στην μπάντα των UHF (συχνότητες δηλαδή από 300 MHz ως 3 GHz.)

3G/UMTS (Universal Mobile Telecommunication System). [Γ' ,81]

Το σύστημα UMTS κατευθύνει την πορεία των τηλεπικοινωνιών προς την τρίτη γενιά ασύρματων τηλεπικοινωνιακών δικτύων. Έχει τη δυνατότητα να ανταποκριθεί στη συνεχώς αυξανόμενη ζήτηση των εφαρμογών του διαδικτύου και στη συνεχόμενη ζήτηση για νέα χωρητικότητα στα συνωστισμένα ασύρματα δίκτυα. Το νέο δίκτυο μπορεί να καλύψει ταχύτητες μέχρι και 2Mbps ανά χρήστη και θέτει νέα πρότυπα γενικής περιαγωγής.
Το σύστημα UMTS (συχνά αναφέρεται W-CDMA: wideband code division multiple access) είναι μία από τις πιο σημαντικές καινοτομίες στην τάση προς τα δίκτυα 3ης γενιάς. Επιτρέπει πολλές εφαρμογές να χρησιμοποιηθούν από πολλούς χρήστες και είναι μια γέφυρα ανάμεσα στα πολλαπλά κυψελοειδή συστήματα που υπάρχουν σήμερα και στο παγκόσμιο πρότυπο για τις κινητές τηλεπικοινωνίες, το International Mobile Telecommunications – 2000 (IMT 2000).
Τα κύρια χαρακτηριστικά των συστημάτων 3ης γενιάς, είναι μια οικογένεια όμοιων προτύπων που έχουν τα ακόλουθα χαρακτηριστικά:

- Παγκόσμια κοινή χρήση
- Χρήση σε όλα τις εφαρμογές κινητής τηλεπικοινωνίας
- Υποστήριξη τόσο μεταγωγής πακέτων (Packet Switching) όσο και μεταγωγής κυκλώματος (Circuit Switching).
- Υψηλές ταχύτητες μέχρι 2 Mbps.
- Αποδοτικότερη χρήση του φάσματος.

WCDMA (Wideband Code Division Multiple Access).

Το Wideband CDMA είναι το σύστημα που προτιμάται από πολλούς διαχειριστές δικτύων με σκοπό την απόκτηση επιπλέον φάσματος. Έχει σχεδιαστεί ώστε να επιτρέπει μεταγωγή σε σύστημα GSM. Τα δίκτυα GSM δε μπορούν να αναβαθμιστούν σε δίκτυα WCDMA αλλά ορισμένα στοιχεία από αυτά όπως είναι η υποδομή του GPRS μπορούν να ξαναχρησιμοποιηθούν.
Ο ορισμός «ευρύ φάσμα» αναφέρεται σε κανάλι με φάσμα 5 MHz. Αυτό είναι τέσσερις φορές μεγαλύτερο από το CDMA-one και 25 φορές μεγαλύτερο από

το GSM. Το μεγαλύτερο φάσμα επιλέχθηκε να επιτρέπει μεγαλύτερες ταχύτητες, μόνο όμως σε περιοχές με καλή ποιότητα λήψης του σήματος. Αντίθετα με το CDMA-one, που στέλνει ένα bit πληροφορίας αυτόματα 64 φορές, το WCDMA τροποποιεί το κέρδος ανάλογα με την ισχύ του σήματος. Κάθε bit στέλνεται από 4 μέχρι 128 φορές, ώστε μεγαλύτερο φάσμα να είναι διαθέσιμο σε περιοχές με πιο δυνατό σήμα. [Γ' ,81]

GPS

Το GPS (Global Positioning System) ,που βασίζεται σε δορυφορικό και επίγειο δίκτυο .Το σύστημα **GPS** στηρίζει την λειτουργία του σε 24 γεωστατικούς δορυφόρους που διαθέτουν ρολόγια υψηλής ακρίβειας (ατομικά ρολόγια) και εκπέμπουν ανά τακτά χρονικά διαστήματα την ώρα καθώς και την θέση που βρίσκονται .Ο υπολογισμός του στίγματος από μια συσκευή GPS γίνεται με βάση τα σήματα που λαμβάνουν από τους δορυφόρους καθώς και του εσωτερικού ρολογιού που διαθέτει ..Συγκεκριμένα υπολογίζεται ο χρόνος ανάμεσα σε δύο διαδοχικά σήματα που λαμβάνει η συσκευή GPS από ένα γεωστατικό δορυφόρο .Έτσι η συσκευή είναι σε θέση να γνωρίζει την απόσταση που απέχει από ένα δορυφόρο .Ο συνδυασμός τριών σημάτων από δορυφόρους ή και περισσότερους δίνει με πολύ ακρίβεια το στίγμα πάνω στην γη.

ΤΕΤΡΑ *[Α',51]*

Είναι ένα ανοιχτό πρότυπο ψηφιακού συγκαναλικού ραδιοσυστήματος επικοινωνιών ,που προδιαγράφεται από το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακής Τυποποίησης (ETSI).Αποτελεί την πιο καλή λύση στα επίγεια συγκαναλικά ραδιοσυστήματα , για χρήση ως Κινητό Ραδιοσύστημα Δημόσιας Πρόσβασης (PAMR) ή Κινητό Ραδιοσύστημα Ιδιωτικής Χρήσης (PMR) ,έχοντας πολλά θετικά και σημαντικά στοιχεία που δεν μπορούν να προσφερθούν από άλλα κυψελοειδή δίκτυα ,όπως της κινητής τηλεφωνίας GSM.Οι δυνατότητες του ,που το κάνουν να ξεχωρίζει είναι :

- Ομαδική κλήση (ένας προς πολλούς)
- Δυνατότητα διεκπεραιωτή ,κρυπτοφώνηση /κρυπτογράφηση στη Ραδιοεπαφή ,
- Κρυπτοφώνηση /κρυπτογράφηση από άκρο σε άκρο ,
- Ταυτόχρονη ραδιοεπικοινωνία φωνής και δεδομένων
- Αμεσότροπη λειτουργία (Walkie talkie),

Όπως και δυνατότητες διαχείρισης δικτύου και τιμολόγησης .
Τα ΤΕΤΡΑ περιλαμβάνει εκτεταμένη σειρά προϊόντων ,όπως σταθμούς βάσης ,κέντρα μεταγωγής ,εργαλεία διαχείρισης και λειτουργίας ,κινητά , φορητά τερματικά και διακομιστές .Όλα έχουν την ικανότητα να επαναπρογραμματιστούν απλά και εύκολα ,όποτε υπάρχει αναβάθμιση του συστήματος ή για ικανοποίηση μελλοντικών απαιτήσεων , καθώς αναπτύσσεται νέα τεχνολογία .Οι τερματικές συσκευές(πομποδέκτες) τόσο του ΤΕΤΡΑ, όσο και του GSM ακολουθούν τη δομή του θεμελιώδους ψηφιακού συστήματος επικοινωνιών, βασίζονται στην ιδέα της κυψελοειδούς κάλυψης , είναι ψηφιακά συστήματα που διέπονται από τις ίδιες αρχές λειτουργίας και ο τρόπος διαχείρισης των σταθμών βάσης είναι πανομοιότυπος . Οι επιμέρους διαφορές τους εντοπίζονται στο είδος των

κωδικοποιητών , στο τρόπο συγκρότησης της ψηφιακής πληροφορίας , στην κρυπτογράφηση (αν υπάρχει) και στην διαμόρφωση του φέροντος .Τα βασικά πλεονεκτήματα ενός συστήματος TETPA :

1. Η μελλοντική αναβάθμιση και επέκταση του συστήματος γίνεται χωρίς να διακοπεί η λειτουργία του δικτύου, καθώς οι λειτουργίες του συστήματος εκτελούνται από software.
2. Τα συστήματα TETPA μπορούν να εξυπηρετήσουν διαφορετικές ομάδες χρηστών με τους ίδιους πόρους .Αυτές οι ομάδες ,μπορούν να έχουν το δικό τους Ιδεατό Ιδιωτικό Δίκτυο , με δικό τους διακομιστή και λειτουργίες διαχείρισης δικτύου .Καθώς θα καταλαμβάνουν μέρη του ίδιου φυσικού δικτύου ,τα Ιδεατά Ιδιωτικά Δίκτυα είναι αθέατα και μη προσβάσιμα σε άλλους χρήστες του δικτύου .

Τα κύρια τεχνικά χαρακτηριστικά του συστήματος TETPA ,είναι :

- Εύρος ζώνης συχνοτήτων : 380-430 MHz
- Διαφορά συχνότητας :10 MHz
- Διαυλοποίηση :25 MHz
- Διαμόρφωση :π/4DQPSK
- Ρυθμός μετάδοσης φωνής κα δεδομένων χωρίς προστασία :7,2 kbps/s
- Ρυθμός μετάδοσης φωνής κα δεδομένων χωρίς προστασία :4,8 kbps/s
- Πολυπλεξία ραδιοσυστήματος :TDMA ,4 χρονοθυρίδες
- Χρόνος αποκατάστασης κλήσεως:< 300 msec
- Ισχύς εξόδου σταθμού βάσης (antenna port) :μέχρι 25 W (44 dBm) ανά πομποδέκτη .

Το σύστημα TETPA περιλαμβάνει πλήθος υπηρεσιών φωνής και δεδομένων , καθώς και συμπληρωματικών υπηρεσιών ,όπως :

Υπηρεσίες Φωνής

- Ομαδική κλήση (group call)
- Ευρυεκπομπή (multiselect, multigroup)
- Ατομική κλήση (private call)
- Κλήση επίγουσας ανάγκης (High priority)
- Κλήση από / προς PABX,PSTN,GSM
- Υπηρεσίες δεδομένων
- Κλήση κατάστασης (status message)
- Κλήση επείγουσας ανάγκης
- Κλήση βράχεων δεδομένων (SDS)
- Κλήση αλφαριθμητικού κειμένου (ATS)
- Κλήση δεδομένων (Packet Data)
- Συμπληρωματικές Υπηρεσίες
- Κλήση προτεραιότητας (Priority call)
- Όψιμη είσοδος (Late Entry)
- Αναγνώριση ομιλούντος (TPI)
- Δυναμική Εκχώρηση Αριθμού Ομάδας (Dynamic Group Number Assignment)
- Φραγή εισερχόμενων κλήσεων
- Φραγή εξερχόμενων κλήσεων .

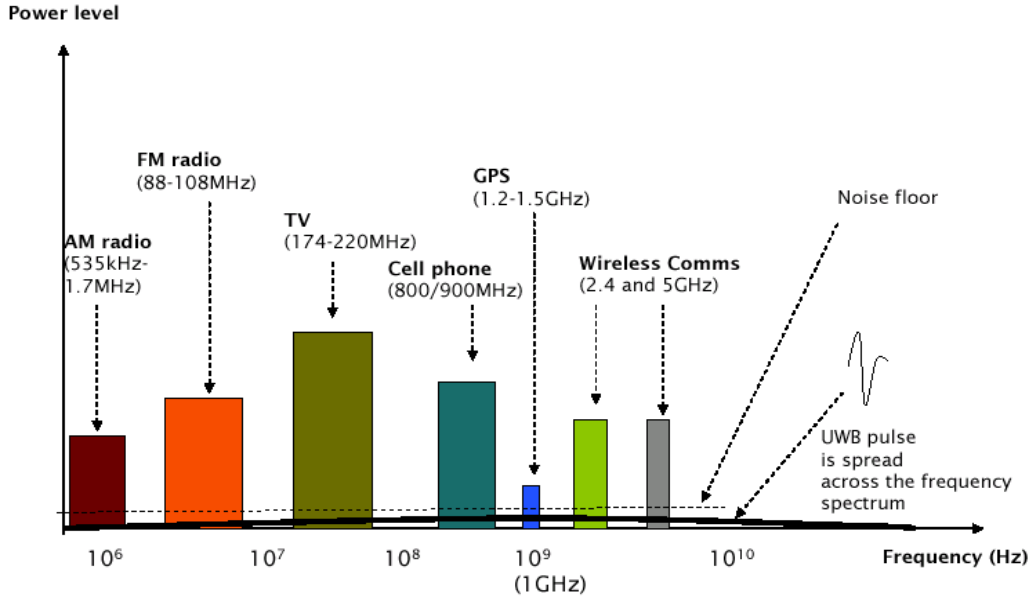


Figure 1.4: Power levels

Στο σχήμα παρατηρούμε το εύρος των ραδιοσυχνότητων και που χρησιμοποιούνται . [Γ',9]

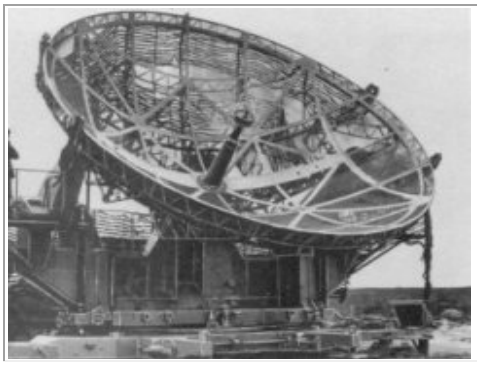
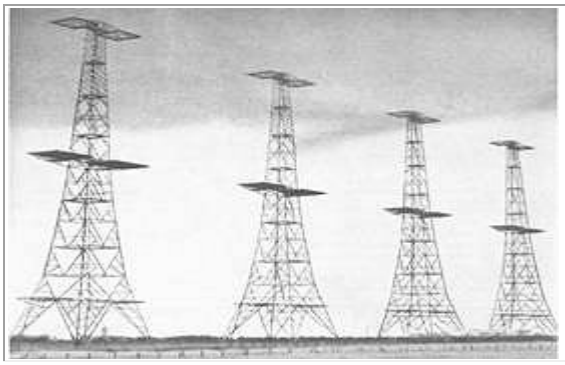
ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

Το 1864 ο Maxwell δημοσίευσε τις εξισώσεις της Ηλεκτρομαγνητικής Θεωρίας .
Ο **Heinrich Rudolf Hertz** με έρευνα επιβεβαίωσε πειραματικά την Ηλεκτρομαγνητική Θεωρία και την ύπαρξη *ηλεκτρομαγνητικών κυμάτων*.
Το 1895 ο Guglielmo Marconi πραγματοποίησε τις πρώτες ασύρματες εκπομπές σημάτων Μορς ,έβαλε την αρχή της *ασύρματης επικοινωνίας* και το 1898 είχε διαπιστώσει ότι η εμβέλεια ενός πομπού μεγάλωνε σημαντικά, όταν πομπός και δέκτης ήταν συντονισμένοι στην ίδια συχνότητα. Το 1901 πέτυχε ασύρματη ανταλλαγή μηνυμάτων μεταξύ Αγγλίας και της ανατολικής ακτής της Αμερικής Η κεραία είχε επινοηθεί από τον Ρώσο Αλέξανδρο Ποπώφ (1859-1905). Ο Χέβισάιτ συνέβαλε σημαντικά στη διάδοση των ηλεκτρομαγνητικών μελετών, εισάγοντας τη διανυσματική ανάλυση και τους τελεστές στην Ηλεκτρομαγνητική Θεωρία. Το 1904, όταν ο Reginald Fessenden μετέδωσε ασύρματα φωνή και μουσική και χρησιμοποίησε στα πειράματά του ένα μικρόφωνο άνθρακα. Το 1907 κατάφερε Χέβισάιτ να κατασκευάσει δύο πομπούς με διαμόρφωση πλάτους, οι οποίοι είχαν εμβέλεια περί τα 450 km.

ΓΙΑ ΤΑ ΡΑΝΤΑΡ

Η παρεμβολή (**jamming**) είναι εσκεμμένα παραγόμενη παρεμβολή, συνήθως σε περιπτώσεις πολεμικών αεροπλάνων για αποπροσανατολισμό του radar.

Το 1939 οι Γερμανοί είχαν εγκαταστήσει μια από τις πρώτες συσκευές εναέριας ανίχνευσης RED (Radio Direction Finding –2.1-2.6m) ,το σύστημα “FREY “,το οποίο είχε την δυνατότητα να μπορεί να εντοπίζει τα Αγγλικά βομβαρδιστικά από απόσταση 180 χιλιομέτρων .Οι πιο φημισμένες εγκαταστάσεις ήταν το “Chimney ή Καμινάδα ”και το “ Hoarding ή Φράχτης “.
Η ιδέα της εναέριας κατασκοπείας (συλλογή εναέριας πληροφορίας) ,γεννήθηκε ταυτόχρονα με την πρώτη πτήση των αδερφών Ράιτ το 1902.
Τον Απρίλιο 1904 ο HULSMEYER από το DUSSELDORF της Γερμανίας για πρώτη φορά κατέθεσε αίτηση καταχώρησης (US patent No. 810.150) για συσκευή ραντάρ αντανάκλασης ραδιοσημάτων εμβέλειας 1000 μέτρων.
Το Αύγουστο του 1907 στην Αμερική δημιουργείται ένα τμήμα αεροναυτικών βάσεων και υπηρεσιών στο τμήμα του στρατού, που το 1916 μετονομάζεται ως $1^{η}$ Αεροπορική Μοίρα με υπεύθυνο τον στρατηγό John Pershing.
Το 1914 ,στον Δεύτερο Παγκόσμιο πόλεμο έχουμε κατασκοπία αεροφωτογράφησης και υποκλοπή ραδιοσημάτων .
Το 1939 είναι γνώστες της τεχνογνωσίας του ραντάρ εκτός από την Γερμανία ,η Γαλλία ,η Πολωνία ,η Αγγλία ,Η.Π.Α. , και η Ρωσία .
Η γερμανική αεροπορία χρησιμοποίησε στις επιθέσεις της στην Αγγλία δύο αξιόπιστα δίκτυα ραντάρ .Το ένα δίκτυο , Chain Home ,είχε καλή εμβέλεια αλλά δεν μπορούσε να εντοπίσει αεροπλάνα που πετούσαν χαμηλά, ενώ το δεύτερο δίκτυο , Chain Home Low, είχε εμβέλεια 80 km και συχνότητα εκπομπής 200 MHz.

Αριστερα: Το γερμανικό ραντάρ Wuerzburg-Riese, *Δεξιά:* Οι κεραίες του δικτύου Chain Home

[Γ ‘ ,20]

Το 1940 ανακαλύπτεται η λυχνία μάγνητρου από τους άγγλους ,που χρησιμοποιήθηκε στο σύστημα “H2S” (συχνότητα λειτουργίας 10εκ.) και έγινε ο εφοδιασμός των αεροπλάνων με μικρά ραντάρ το 1943.

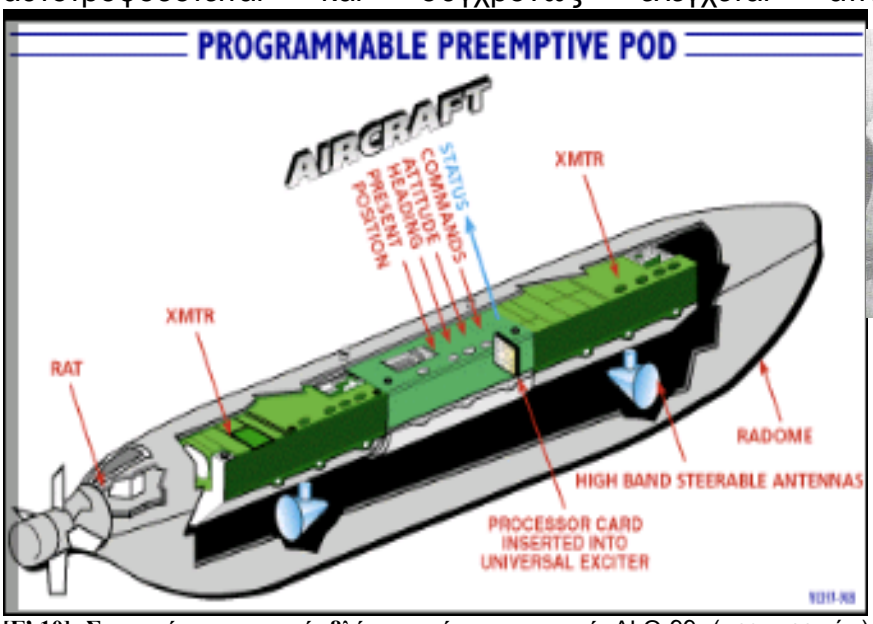
Στο δεύτερο παγκόσμιο πόλεμο χρησιμοποιήθηκαν τεχνικές παρεμβολών στα εχθρικά ραντάρ. Μια τέτοια τεχνική ήταν η ρίψη μεγάλων ποσοτήτων μικρών ταινιών από staniol. Κατά τις επιθέσεις των βρετανικών βομβαρδιστικών στην περιοχή του Αμβούργου, επί 2 συνεχείς ημέρες στο τέλος Ιανουαρίου 1943, ρίχτηκαν για παρενόχληση των γερμανικών ραντάρ περίπου 92 εκατομμύρια ταινίες μεγέθους ίσο με το μισό μήκος κύματος των εκπεμπόμενων ραδιοκυμάτων. Το συνολικό βάρος των ταινιών staniol ήταν της τάξης των 40 τόνων. [Γ’20]

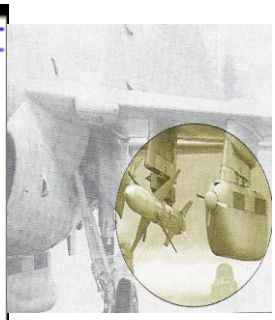
Αριστερά: Εργάτρια παρασκευάζει ταινίες staniol,
Δεξιά: Βρετανικά αεροπλάνα ρίχνουν τις ταινίες.

Ένα από τα πρώτα συστήματα παρεμβολής που χρησιμοποιήθηκε από το $3^{ο}$ Ράιχ για να κάνει παρεμβολές στις αγγλικές αεροπορικές επικοινωνίες ,ήταν το παρεμβολικό σύστημα” CARUSO “ με ισχύ 30-40 kW στα 3 μέτρα .Το σύστημα λειτούργησε σε παλμική διαμόρφωση “ Delta “ ,σαρώνοντας δύο ζεύγη συχνοτήτων από 2.5-2.7 και 2.7 –3.0 Hz . Ακολούθησαν το σύστημα “Heinrich “ 1&2 στα 4 και 14 μέτρα αντίστοιχα καθώς και το “ Karl “ 1&2 και παρά πολλά άλλα. [Α΄,45].

Στο δεύτερο παγκόσμιο πόλεμο χρησιμοποιήθηκε από την Αμερική στο ναυτικό το πρώτο εναέριο ραντάρ ανίχνευσης (το APS –20) .Ο ίδιος μηχανισμός αργότερα τοποθετήθηκε και στα αεροπλάνα. Αναβαθμίστηκε αρκετές φορές και το ραντάρ APS 95-103 χρησιμοποιήθηκε στο μοντέλο AWACS EC-121H (Airborne Warning and Control Systems) .Το 1977 παρουσιάζεται ο νέος τύπος AWACS E-3 (μοντέλο Boeing),με περιστρεφόμενη κεραία κυκλικής σάρωσης εντοπισμού 360^{0} μοιρών, που

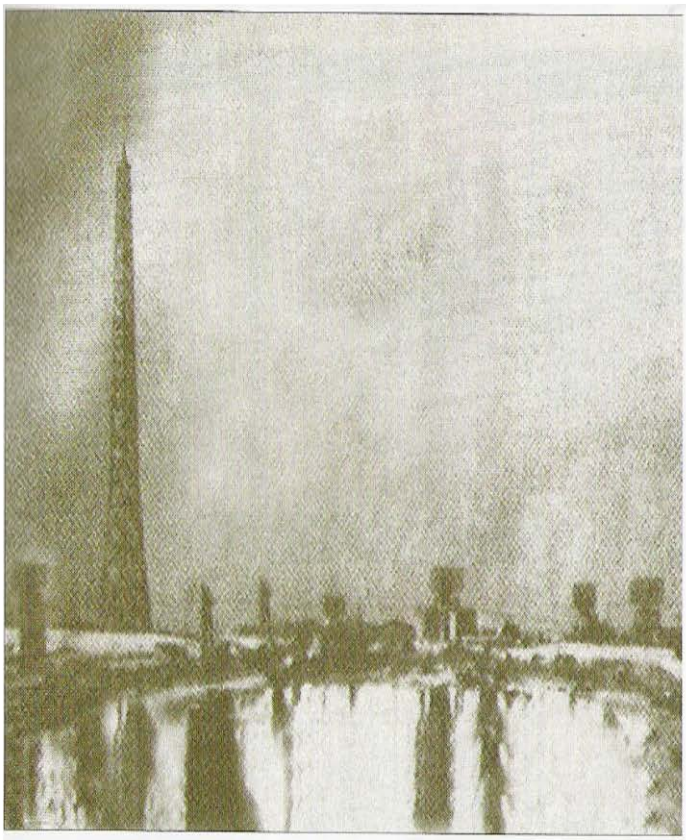
ανιχνεύει σε σύνολο 200.000 τετραγωνικά χιλιόμετρα οποιαδήποτε ιπτάμενα ή επίγεια κινούμενα αντικείμενα και αναγνωρίζονται αυτόματα με ηλεκτρονική επεξεργασία (αν είναι φιλικά ή εχθρικά) . [Α' ,34].
Στα μέσα της δεκαετίας του 1960 στην Αμερική , το εργοστάσιο μαχητικών αεροπλάνων "NORTHROP GRAMMAR AEROSPACE CORP. με κρατικές οικονομικές ενισχύσεις ,ξεκίνησε την σχεδίαση και κατασκευή αεροπλάνων με υψηλές για την εποχή προδιαγραφές στο χώρο των ραντάρ και του ηλεκτρονικού πόλεμου ,όπως το αεροπλάνο A-6 A (INTRUDER) ,που ονομάστηκε EA- 6 B PROWLER (είχε αρχική ονομασία YA-2 FI BUNO 147864) .Το EA- 6 B PROWLER,είναι ένας ιπτάμενος παρεμβολές ,που με τα 5 σούπερ "TOP SECRET " παρεμβολικά συστήματα ,νεκρώνει όλα τα αμυντικά και επιθετικά επίγεια συστήματα ,που χρησιμοποιούν τα ηλεκτρομαγνητικά κύματα και γενικά το ραδιοφάσμα. Έχει 5 αποσπώμενους μηχανισμούς παρεμβολής ,τα λεγόμενα "POD'S",Τ τύπου AN/ALQ-99(δύο σε κάθε φτερό και μια στο σημείο της κοιλιάς του αεροπλάνου) καθένας έχει δύο ισχυρότατους πομπούς παρεμβολής ,ικανοί στο σύνολο τους να καλύψουν ή να νεκρώσουν 7 διαφορετικές μπάντες επικοινωνίας φωνής ή ραντάρ. Ο πομπός AN/ALQ-99(Tactical Jamming System –TJS) αυτοτροφοδοτείται και συγχρόνως ελέγχεται από τον Η/Υ.

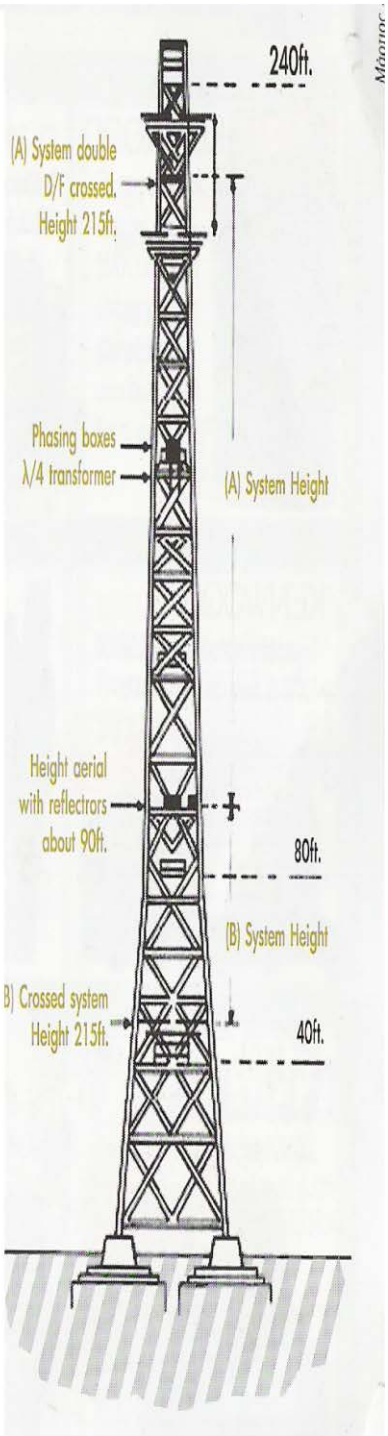




[Γ',10] Στο σχήμα αριστερά βλέπουμε ένα μηχανισμό ALQ-99 (εσωτερικά) και στο δεξί σχήμα παρατηρούμε ένα πολεμικό αεροπλάνο ,που δείχνει σε ποιο σημείο ακριβώς βρίσκονται αυτοί οι μηχανισμοί ALQ-99.

Υπάρχει ένας άλλος μηχανισμός ,ο ALQ-99 (On –board System –OBS) ,που συλλέγει και καταγράφει διάφορα πολεμικά δεδομένα ,τα οποία μπορούν να χρησιμοποιηθούν εν πτήση ή να αναλυθούν και να επεξεργαστούν αργότερα ή ακόμα χρησιμοποιώντας το σύστημα TEPRES (Tactical Electronic Processing & Evaluation System),να λάβουν εν πτήση νέες οδηγίες – και από AWACS – σε μορφή συμπιεσμένων δεδομένων για πιθανόν αλλαγές σε επιχείρηση εν εξέλιξη[Α' ,45].





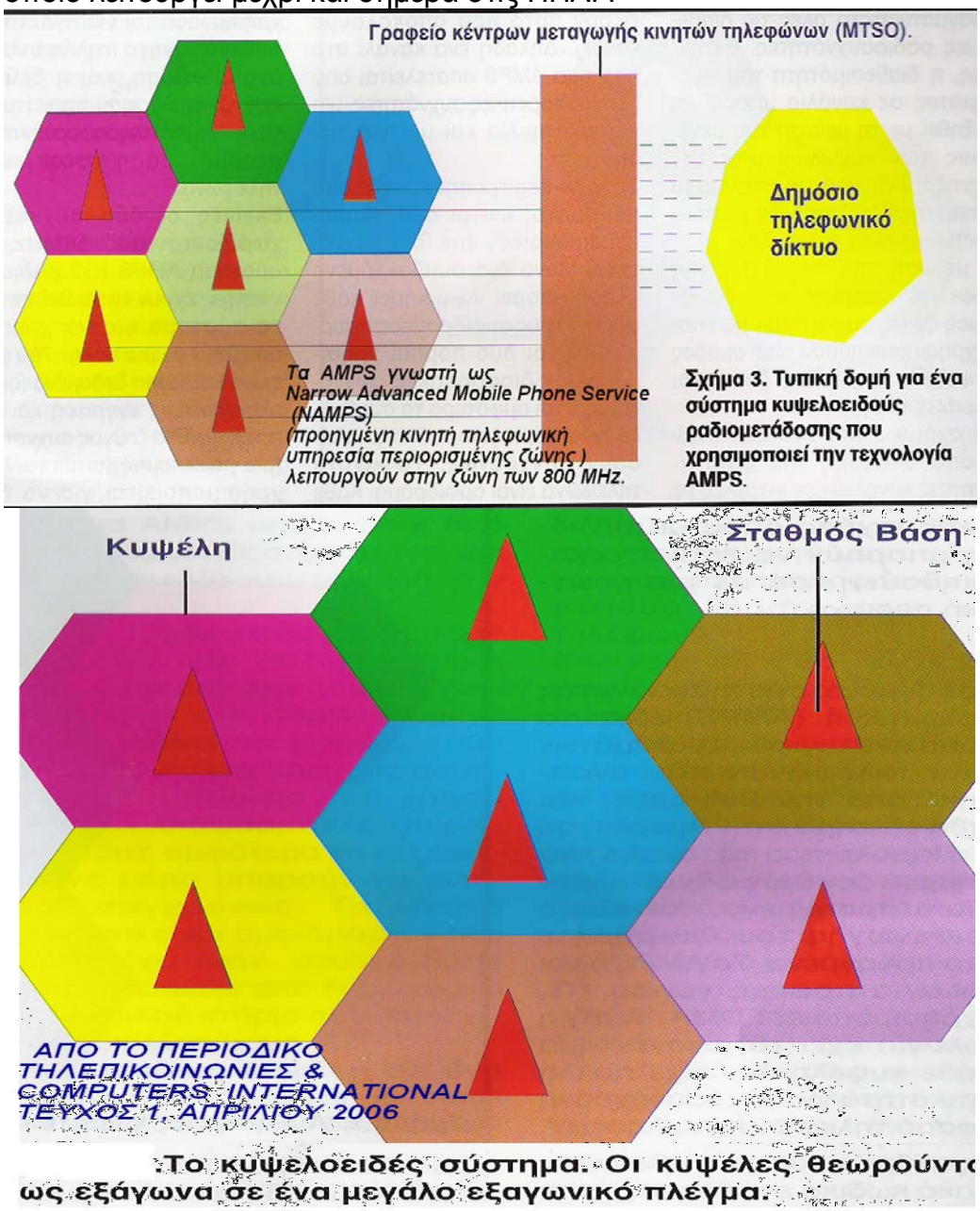
Φωτογραφία Αγγλικής ακτής του 1940 καθώς και γραμμικό σχήμα του ραντάρ "CHAIN HOME" το οποίο εγκατεστάθη στα τέλη του 1939.
Αριστερά διακρίνεται ο μεταλλικός πύργος εκπομπής, ύψους 101 μέτρων (CH-RDF) καθώς και οι αλυσιδωτές κεραίες λήψης (CHL CD=Costal Defence) οι οποίες είναι τοποθετημένες πάνω σε ξύλινους πύργους ύψους 74 μέτρων, έτσι ώστε να αλλοιώνεται στο ελάχιστο το επιστρεφόμενο ανακλώμενο σήμα.


ηλεκτρονικός βομβαρδισμός
E-2C HAWKEYE
EA-6B PROWLER
Πύραυλοι SAM

ΚΙΝΗΤΑ

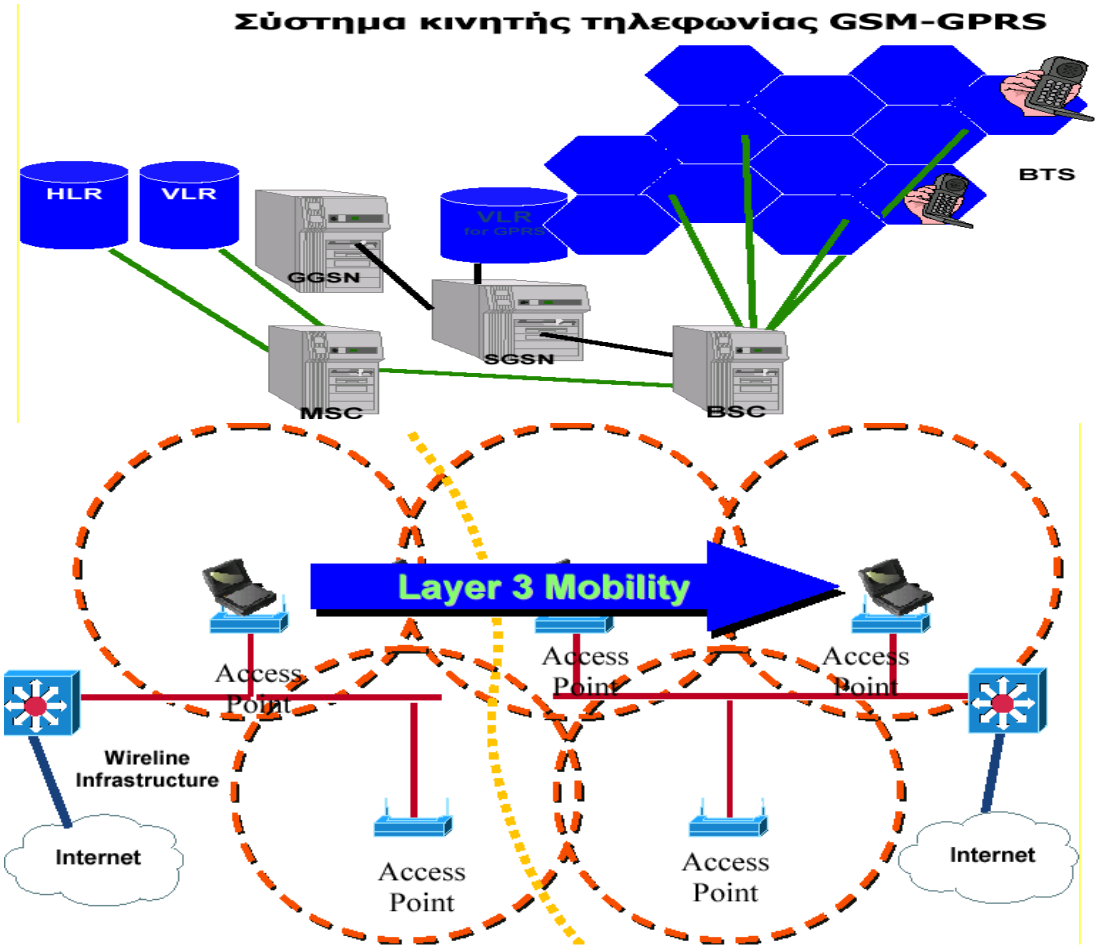
Τα συστήματα κινητής τηλεφωνίας πρώτης γενιάς μελετήθηκαν, υλοποιήθηκαν και λειτούργησαν από το 1970 μέχρι το 1990 . Βασίστηκαν στην κυτταρική δομή και είχαν αναλογικά χαρακτηριστικά
Η Κυτταρική ιδέα (Cellular Concept) για την ηλεκτρομαγνητική κάλυψη συγκεκριμένων γεωγραφικών περιοχών άρχισε να θεμελιώνεται μετά τον δεύτερο παγκόσμιο πόλεμο στα εργαστήρια BELL (Bell Telephone Laboratory – BTL) .
Το 1940 εμφανίστηκαν οι πρώτες κινητές επικοινωνίες (ραδιοτηλεφωνα),οι χρήστες των ραδιοτηλεφώνων πατώντας ένα κουμπί είχαν την δυνατότητα να μιλήσουν και να ανταλλάξουν πληροφορίες .Η χρήση όμως είναι περιορισμένη για συγκεκριμένες εφαρμογές (στρατιωτικές ,επικοινωνίες πλοίων , αεροσκαφών) .
Το 1961 το παράρτημα της σουηδικής εταιρείας Ericsson με την επωνυμία Svenska Radio Aktiebolaget (SRA)παρήγαγε για πρώτη φορά διεθνώς τον εξοπλισμό κινητών επικοινωνιών για εμπορική χρήση , απευθυνόμενο στο ευρύτερο κοινό .
Το 1962-1964 καταγράφεται διεθνώς το πρώτο διεθνές δίκτυο κινητών επικοινωνιών και το ανέπτυξε η εταιρεία Bell Systems ,στην περιοχή της Πενσυλβανία των ΗΠΑ και έδωσε την ονομασία Improved Mobile Telephone Service (IMTS) . Το δίκτυο ήταν το πρώτο στον κόσμο που επέτρεπε την αμφίδρομη επικοινωνία και οι συνομιλητές δεν πιέζουν πλήκτρα στο τερματικό τους για να μπορούν να μιλούν. Το σύστημα αυτό αναπτύχθηκε στις ΗΠΑ και στον Καναδά ,παρέχοντας τηλεπικοινωνιακές υπηρεσίες μέχρι και τα μέσα της δεκαετίας του 1980.
Το 1958 –1968 η εταιρεία AT& T έδωσε στην FCC επιστημονικά εναύσματα για την υλοποίηση υψηλής χωρητικότητας κυψελοειδούς συστήματος κινητής τηλεφωνίας (αναλογικά)και το 1968 οδήγησαν την FCC στην έκδοση της αντίστοιχης απόφασης (DOCKET) ,που στόχευε στην αντιμετώπιση του προβλήματος της κινητής επικοινωνιακής συμφόρησης και είχε αύξοντα αριθμό 18262.[Γ’,48]
Στη Ιαπωνία το 1967 η εταιρεία Nippon Telegraph and Telephone company (NTT) αναπτύσσει σε όλη την Ιαπωνία δίκτυο σε συχνότητες στην περιοχή των 800 MHz. Το 1969 η εταιρεία Bell Systems παρείχε δίκτυο κινητών επικοινωνιών στο ευρύ κοινό ,που λειτουργούσε σε συχνότητες στα 450 MHz και με δυνατότητα πραγματοποίησης μεταπομπών (HANDOVERS) για πρώτη φορά. Το δίκτυο αυτό είναι βασισμένο στο πρωτόκολλο IMTS.
Το 1970 , η FCC καταχώρησε 75 MHz στην ζώνη από 800 MHz ως 900 MHz για την χρήση των συστημάτων υψηλής χωρητικότητας .
Το Δεκέμβριο του 1971 , η AT& T κατέθεσε ολοκληρωμένη τεχνική πρόταση για την υλοποίηση ενός κυτταρικού συστήματος υψηλής χωρητικότητας. [Β’,6]
Τις 17 Οκτωβρίου του 1973 η εταιρεία Motorola παρουσίασε το πρώτο κινητό τηλέφωνο που μπορούσε να κρατηθεί με το ένα χέρι , να λειτουργεί αυτοτελώς χωρίς να χρειάζεται ξεχωριστά συστήματα τροφοδοσίας και έπαιξε καθοριστικό ρόλο στην μετέπειτα εξέλιξη των κινητών επικοινωνιών.
Το 1974 ,η FCC καταχώρησε επιπλέον 40 MHz, για την κινητή τηλεφωνία .
Το 1978 πραγματοποιήθηκε η εγκατάσταση του συστήματος σε πειραματική βάση .Τόσο η AT& T(όπως μετονομάστηκε η Bell South), όσο και η εταιρεία Bahrain telephone Company ,ανέπτυξαν και λειτούργησαν εμπορικά δίκτυα

κινητών επικοινωνιών βασισμένα στο πρότυπο Advanced Mobile Phone Service (AMPS) που είναι ένα αναλογικό σύστημα κινητών επικοινωνιών και πρόδρομος του Digital Advanced Mobile Phone Service (D-AMPS) και το οποίο λειτουργεί μέχρι και σήμερα στις ΗΠΑ. .



Στις δεκαετίες του 1980 αρκετές ευρωπαϊκές χώρες (Νορβηγία , Σουηδία , Φιλανδία , Βέλγιο , Ολλανδία , Μεγάλη Βρετανία ,ΕΙΠΕ) είχαν αναπτύξει δίκτυα κινητών επικοινωνιών βασισμένα σε πρότυπα αναλογικών επικοινωνιών (NMT 450 ΚΑΙ 900) τα οποία είναι μη συμβατά μεταξύ τους.
Από το 1990 ως το 2000 ,αναβαθμίστηκε η τεχνολογία συστημάτων της πρώτης γενιάς με αποτέλεσμα να λειτουργήσουν τα οργανωμένα κυτταρικά συστήματα κινητής τηλεφωνίας (Cellular mobile radio communication systems) δεύτερης γενιάς και χρησιμοποιούν για αποτελεσματική εκμετάλλευση του υπάρχοντος εύρους ζώνης τα ψηφιακά συστήματα .
Το 1982 η CERT(ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΤΑΧΥΔΡΟΜΕΙΩΝ) αποφάσισε την ίδρυση μιας ομάδας ειδικών (Group

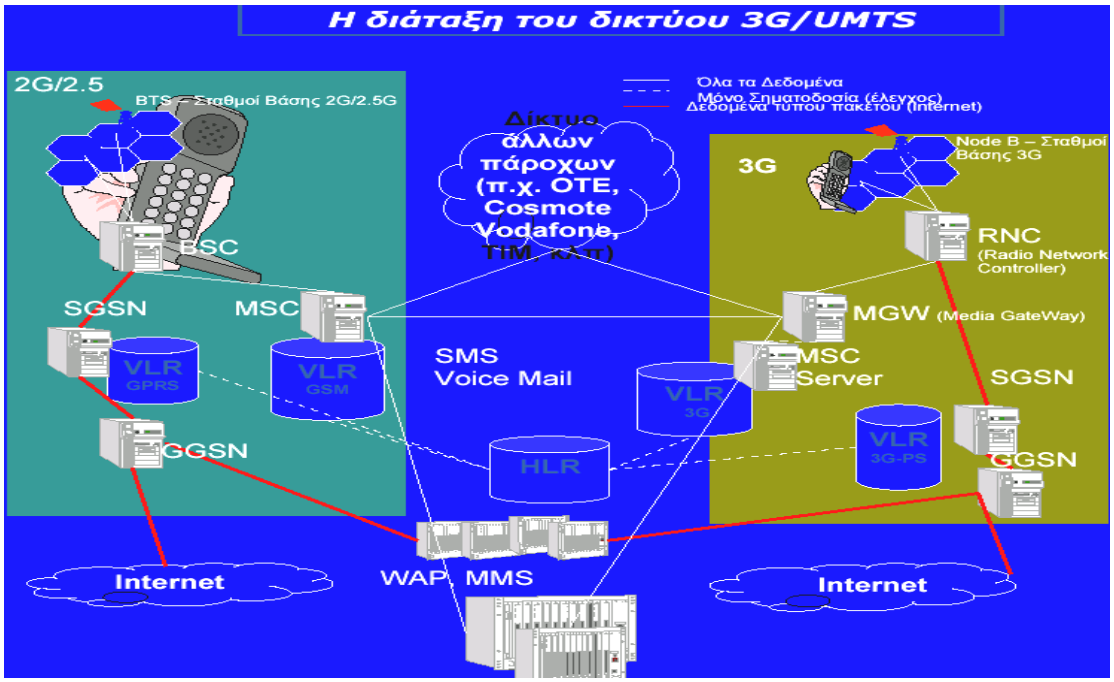
Special Mobile) για την ανάπτυξη του συνόλου κοινών προδιαγραφών ενός μελλοντικού πανευρωπαϊκού δικτύου κυψελωτών κινητών επικοινωνιών .
Το 1987 υπογράφεται το Μνημόνιο Συνεργασίας (MOU) από τηλεπικοινωνιακούς οργανισμούς (παρόχους) 12 χωρών .
Το 1988 γίνονται οι πρώτες αξιολογήσεις και δοκιμές (της ασύρματης διεπαφής κυρίως) και δείχνουν ότι το "GSM 900 " θα λειτουργήσει . Το "GSM 900 "λειτουργεί στην περιοχή των 900 MHz.
Το 1988-1992 ιδρύεται ο ETSI και η ομάδα GSM υπάγεται σε αυτόν σαν μια από τις τεχνικές του επιτροπές .Μετά την έγκριση τους οι προδιαγραφές της ομάδας θα γίνουν Πανευρωπαϊκά Τηλεπικοινωνιακά Πρότυπα (ETS) .
Το 1990 προδιαγραφές του GSM για την ζώνη των 900 MHz εφαρμόζονται και σε ένα Ψηφιακό Κυψελωτό Σύστημα στους 1800 MHz (DCS- 1800).
Τ ο 1991 οι προδιαγραφές του GSM καταλαμβάνουν πάνω από 5000 σελίδες σε 30 έγγραφα. Αναβάλλεται για το 1992 η προγραμματισμένη έναρξη του νέου συστήματος λόγω έλλειψης εγκεκριμένων τερματικών (GSM = God Send Terminals).
Το 1992 γίνεται η επίσημη έναρξη (God Has Send Terminals).
Το 1992 ενδιαφέρθηκαν οι Αυστραλοί παρόχοι να αναπτύξουν το νέο σύστημα και στην ίδια περιοχή αναπτύχθηκε το σύστημα PCS στις Η.Π.Α. ,που αποτελεί σύστημα συμβατό (μερικώς) με το GSM.
Από το 2001 άρχισε η ανάπτυξη δικτύων τρίτης γενιάς (3G/UMTS) ,που παρέχουν νέες και βελτιωμένες υπηρεσίες όπως βιντεοκλήση (video call)και εφαρμογές ροοθήκευσης βίντεο (video streaming) , πρόσβαση των δεδομένων σε υπηρεσίες δεδομένων (από 384 kbps μέχρι 14 Mbps με χρήση ειδικού χαρακτηριστικού HSDPA) και βασίζονται σε τεχνολογία Wide Code Division Multiple Access (WCDMA).Στα δίκτυα $3^{ης}$ γενιάς περιοριστικός παράγοντας παροχής υπηρεσίας στα δίκτυα είναι η στάθμη παρεμβολής στο δίκτυο ,που προέρχεται τόσο από τους χρήστες κινητών όσο από τους σταθμούς βάσης που υπάρχουν σε κάθε περιοχή . οι γειτονικές κυψέλες χρησιμοποιούν την ίδια φέρουσα συχνότητα (carrier) ,και μπορούν να επαναχρησιμοποιηθούν και διαφοροποιούνται μεταξύ τους με την χρήση διαφορετικών κωδίκων ανά κυψέλη ,που ονομάζονται κώδικες scrambling (Scrambling code) και θα αναφερθούμε παρακάτω. Στα δίκτυα UMTS ο κάθε χρήστης χρησιμοποιεί τον δικό του κωδικό και έτσι το δίκτυο τον διακρίνει από τους χρήστες. Τα δίκτυα $3^{ης}$ γενιάς λειτουργούν σε υψηλότερα συχνότητες από τα GSM (2100 MHz συγκριτικά με το 900/1800 MHz του GSM και έτσι τα ραδιοκύματα που εκπέμπουν καλύπτουν συγκριτικά μικρότερες αποστάσεις στο χώρο. Τα τελευταία χρόνια στα δίκτυα κινητών επικοινωνιών $3^{ης}$ γενιάς αναπτύχθηκαν νέες τεχνολογίες ασύρματης μετάδοσης όπως η τεχνολογία WLAN (Wireless Local Area Network =ασύρματο δίκτυο τοπικής πρόσβασης) ή η τεχνολογία Bluetooth για γρήγορη πρόσβαση στο διαδίκτυο κ.λ.π..Οι τεχνολογίες αυτές έχουν χαμηλή ισχύ αναμεταδότη που δεν ξεπερνά τα 150 m w Για την σύνδεση και επικοινωνία τα συστήματα WLANχρησιμοποιούν ραδιοκύματα συχνότητας 2,4 GHz ή 5 GHz. ,η ακτίνα λειτουργίας είναι μικρότερη των 300 μέτρων ,η ισχύς των ασύρματων σημείων πρόσβασης δεν υπερβαίνουν τα 100 m w και οι ρυθμοί μετάδοσης τους μεταξύ 2 ως 54 Mbps

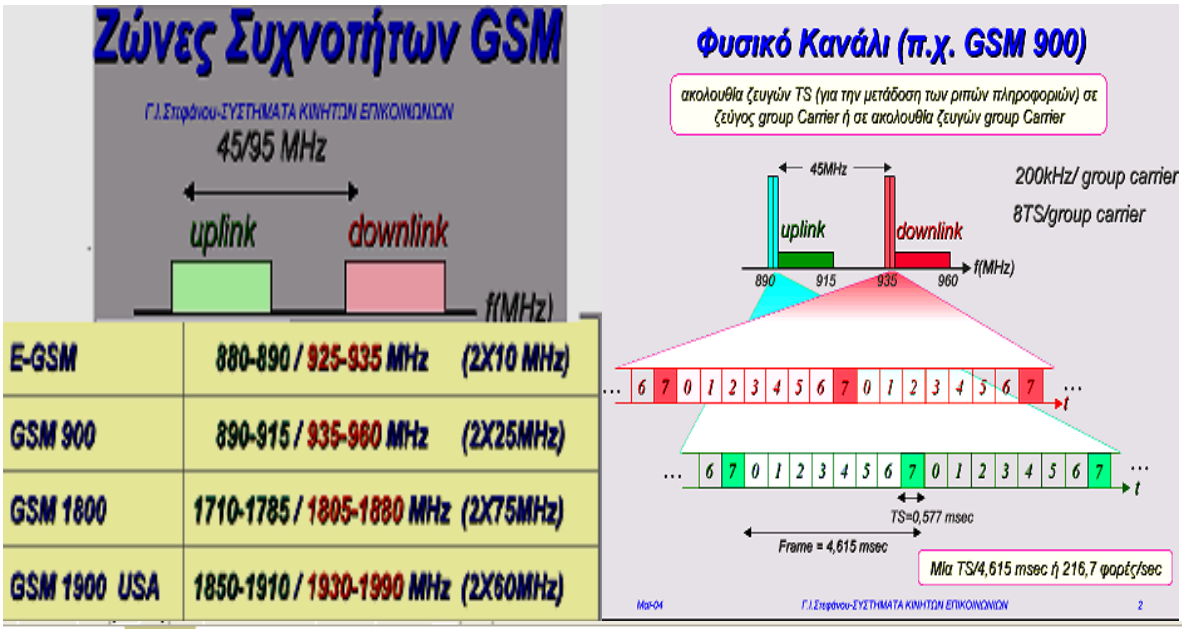


Όπως φαίνεται στο σχήμα 5, το δίκτυο WLAN αποτελείται από ασύρματα σημεία πρόσβασης (Access Points), τα οποία συνδέονται μέσω δρομολογητών (routers) και κατάλληλων εξυπηρετητών (servers), προς το διαδίκτυο (Internet) ή /και προς το εσωτερικό εταιρικό δίκτυο (intranet) του κατόχου τους. Οι χρήστες για να συνδεθούν στο δίκτυο αυτό τοποθετούν στις φορητές τους διατάξεις (laptops, PDA's, κινητά τηλέφωνα) κατάλληλες κάρτες WLAN, που επικοινωνούν ασύρματα με τη δικτυακή υποδομή. Οι τελευταίου τύπου φορητές διατάξεις διαθέτουν ενσωματωμένους προσαρμογείς WLAN.

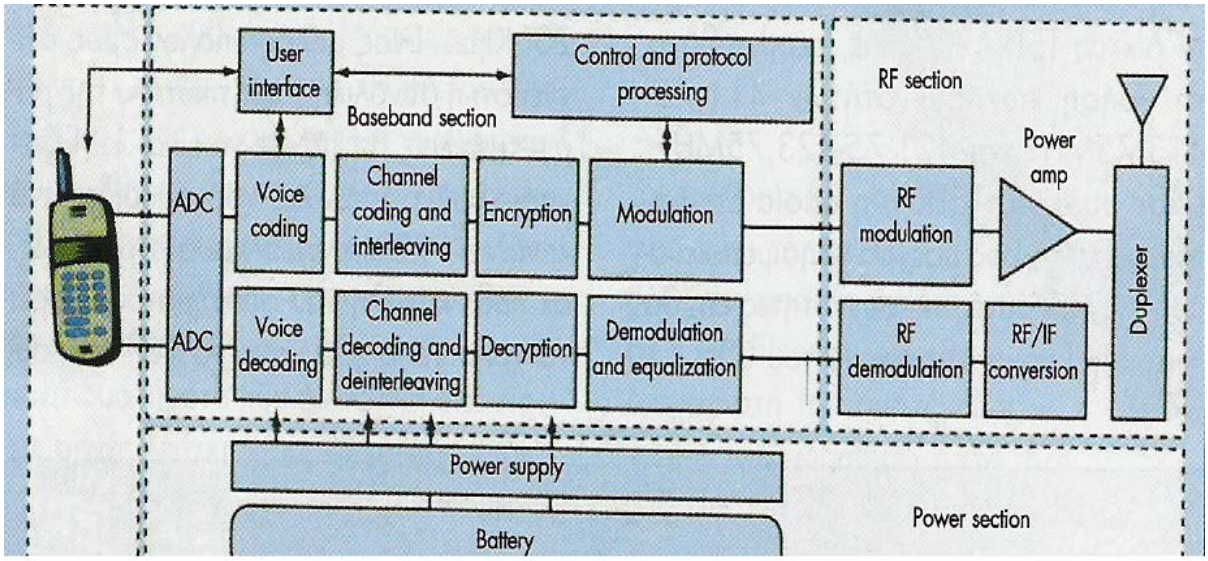
ΤΟΠΟΛΟΓΙΑ ΔΙΚΤΥΟΥ WLAN

Διάταξη δικτύου UMTS – 3G συγκριτικά με δίκτυο GSM/GPRS

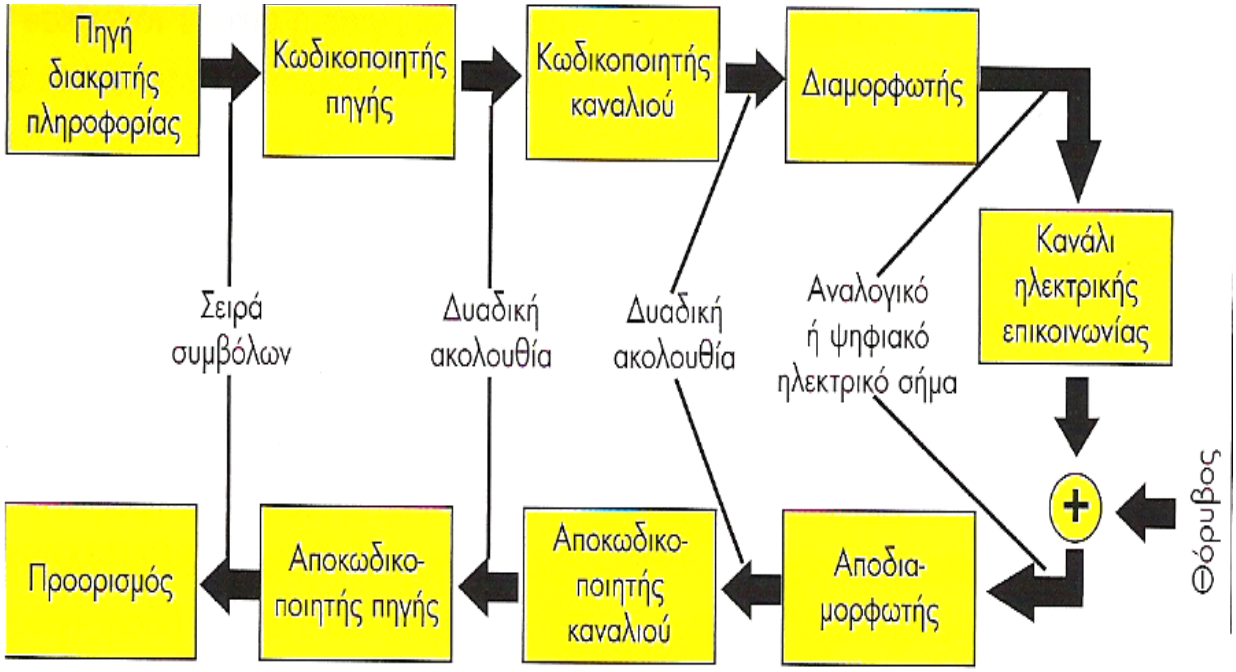



Ζώνες Συχνοτήτων GSM
Γ.Ι.Στεφάνου-ΣΥΣΤΗΜΑΤΑ ΚΙΝΗΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ
45/95 MHz
uplink
downlink
f(MHz)
E-GSM 880-890 / 925-935 MHz (2X10 MHz)
GSM 900 890-915 / 935-960 MHz (2X25MHz)
GSM 1800 1710-1785 / 1805-1880 MHz (2X75MHz)
GSM 1900 USA 1850-1910 / 1930-1990 MHz (2X60MHz)
Φυσικό Κανάλι (π.χ. GSM 900)
ακολουθία ζευγών TS (για την μετάδοση των ριπών πληροφοριών) σε ζεύγος group Carrier ή σε ακολουθία ζευγών group Carrier
45MHz
200kHz/ group carrier
8TS/group carrier
uplink
downlink
890
915
935
960
f(MHz)
TS=0,577 msec
Frame = 4,615 msec
Μία TS/4,615 msec ή 216,7 φορές/sec
Μαϊ-04
Γ.Ι.Στεφάνου-ΣΥΣΤΗΜΑΤΑ ΚΙΝΗΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ
2


Διάγραμμα Λειτουργίας Ενός Πομποδέκτη
Βασική Ζώνη
Ζώνη RF
DAC
ADC
Από-κωδικοποίηση φωνής
Από-κωδικοποίηση καναλιού & από-διαφύλλωση
Αποκρυπτο-γράφηση
Από-διαμόρφωση & Εξισορρόπηση
ADC
DAC
Κωδικοποίηση φωνής
Κωδικοποίηση καναλιού & διαφύλλωση
Κρυπτο-γράφηση
Διαμόρφωση
RF – Από-διαμόρφωση
RF – Μετα-τροπέας
RF – Διαμόρφωση
Παροχή Ισχύος
Μπαταρία
Υπομονάδα Ισχύος


User interface
Baseband section
Control and protocol processing
RF section
ADC
ADC
Voice coding
Voice decoding
Channel coding and interleaving
Channel decoding and deinterleaving
Encryption
Decryption
Modulation
Demodulation and equalization
RF modulation
RF demodulation
Power amp
RF/IF conversion
Duplexer
Power supply
Battery
Power section

Δομή ενός ψηφιακού πομποδέκτη. Η ουσιώδης διαφορά του από τους κλασικούς πομποδέκτες αναλογικής τεχνολογίας βρίσκεται στη βαθμίδα της ψηφιακής επεξεργασίας του σήματος (digital signal processing, DSP) (baseband section). Εκεί διεκπεραιώνονται όλες οι σύνθετες λειτουργίες, από την κρυπτογράφηση έως τη χρονικά κατομεριομένη εκπομπή και λήψη. Περιλαμβάνει τους ψηφιοαναλογικούς μετατροπείς της φωνής (ADC, DAC), τους κωδικοποιητές φωνής και καναλιού, τον ελεγκτή διεμπλοκής και χρονομερισμού της συχνότητας (channel coding & inteleaving), τη βαθμίδα κρυπτογράφησης και αποκρυπτογράφησης (encryption/decryption) και τους διαμορφωτές ψηφιακού σήματος I,Q. Η κατασκευή τέτοιων κυκλωμάτων πριν λίγα χρόνια, ήταν θέμα προχωρημένης επιστημονικής φαντασίας. Σήμερα πρόκειται για κοινή πρακτική, που προφέρεται όμως από πολύ λίγες εταιρείες, που κρατούν στα χέρια τους την παγκόσμια αγορά. Δεν θα δείτε συχνά τα ονόματά τους στην πρόσοψη των συσκευών, αλλά όπως γίνεται συνήθως, αυτοί που κινούν τα νήματα δεν βρίσκονται στο προσκήνιο. Οι βαθμίδες RF και IF είναι ενσωματωμένες στο ίδιο «κουτάκι» (RF section) και περιλαμβάνουν τον ενισχυτή ισχύος (power amplifier), τον ενισχυτή και μετατροπέα μέσης συχνότητας (IF conversion), όπως και το μεταλλάκτη κεραίας (duplexer). Το κύκλωμα αυτού του μικρού «ψηφιακού τέρατος» συμπληρώνεται με τα κυκλώματα ελέγχου των διαδικασιών (μικροϋπολογιστής, control & protocol processing), τον ελεγκτή πληκτρολογίου (user interface) και το σύστημα τροφοδοσίας (power supply & battery). Οι τερματικές συσκευές (πομποδέκτες) τόσο του TETRA, όσο και του GSM ακολουθούν τη δομή του θεμελιώδους ψηφιακού συστήματος επικοινωνιών. Οι επί μέρους διαφορές τους, εντοπίζονται στο είδος των κωδικοποιητών, στον τρόπο συγκρότησης της ψηφιακής πληροφορίας, στην κρυπτογράφηση (αν υπάρχει) και στη διαμόρφωση του φέροντος.



[01] **Βασικές μονάδες ενός συστήματος ψηφιακών επικοινωνιών.** Η απόδοσή του χαρακτηρίζεται από την ακρίβεια εκπομπής και εκφράζεται με το ρυθμό εκπομπής εσφαλμένων bits (BER). Στόχος του κωδικοποιητή πηγής είναι η μείωση του όγκου της «ψηφιακής πληροφορίας» που θα μεταδοθεί. Ο κωδικοποιητής καναλιού αποσκοπεί στον περιορισμό των σφαλμάτων μετάδοσης.

ΤΙ ΕΙΝΑΙ Ο ΗΛΕΚΤΡΟΝΙΚΟΣ ΠΟΛΕΜΟΣ

Ο ηλεκτρονικός πόλεμος (Electronic Warfare - EW),θεωρείται η τύφλωση καταστροφή των ενσύρματων / ασύρματων επικοινωνιών, είτε με ηλεκτρομαγνητικά κύματα (που δεν επιδρούν όμως στις οπτικές ζεύξεις) είτε με φυσική καταστροφή (χρήση όπλων).Στον ηλεκτρονικό πόλεμο γίνεται εσκεμμένη εκπομπή ηλεκτρομαγνητικής ακτινοβολίας ώστε να μειωθεί ή να απαγορευθεί η χρήση μίας ζώνης του ηλεκτρομαγνητικού φάσματος από τον εχθρό. Οι τεχνικές Jamming χωρίζονται γενικά σε δύο κατηγορίες του θορύβου και της παραπλάνησης όπως θα τις αναφέρουμε παρακάτω.
Οι παρεμβολείς (jammers)στα ραντάρ διακρίνονται επίσης σε σημειακούς (stand-off), συνοδευτικής προστασίας και αυτο-προστασίας.Το jamming γίνεται στην κεραία λήψης ενός τηλεπικοινωνιακού συστήματος ,που λαμβάνει το σήμα παρεμβολής στην ίδια περιοχή ή υποπεριοχή συχνοτήτων στην οποία εκπέμπει και ο πομπός του συστήματος . Ο ηλεκτρονικός πόλεμος γίνεται κυρίως στον δέκτη ,χωρίς αυτό να σημαίνει ότι δεν μπορεί να γίνει και στον πομπό . Οι πομποί ,που μπορούν να βρεθούν από τη διεύθυνση τους , ή μπορεί να καταστραφεί ο εξοπλισμός τους ή να δεχτούν μεγάλης ισχύος μικροκύματα και να υποστούν σοβαρές βλάβες.
Για να γίνει μια επιτυχημένη επίθεση jamming θα πρέπει μετά από ερεύνα (search)και παρακολούθηση (track) ,να μετρηθεί η ισχύ του σήματος του δέκτη και να γίνει εκπομπή του σήματος jammer(υποκλοπέας) με ισχύς ίδια ή μεγαλύτερη από την ισχύ του σήματος του δέκτη. Δηλαδή πρώτα ο υποκλοπέας μαθαίνει τα χαρακτηριστικά του <<εχθρικού σήματος >>και μετά επαναεκπέμπει με κατάλληλη διαμόρφωση πλάτους ,φάσεως και πολώσεως. Με αυτό τον τρόπο είναι σαν να γίνεται μια παραπλάνηση του δέκτη για αυτό η τεχνική αυτή λέγεται και jamming παραπλάνησης.
Η αποτελεσματικότητα του υποκλοπέα εξαρτάται από το λόγο J/S (JAMMING –to – Signal ratio) από την περιοχή συχνοτήτων λειτουργίας , από την δυνατότητα μεταπήδησης της συχνότητας ,από την κωδικοποίηση του καναλιού και την διαπλοκή του συστήματος του στόχου, από την ισχύ εκπομπής ,από το εύρος και διαμόρφωση του εύρους παλμού ,από την ομαδοποίηση ,συχνότητα και διαμόρφωση παλμών , από χαρακτηριστικά λοβών και πόλωσης της κεραίας , από τους μεθόδους συντονισμού με άλλα (παράλληλα συστήματα όπως δίκτυα).Αν πρόκειται για ραντάρ επίσης λαμβάνεται υπόψη η θέση του παρεμβολέα στο διάγραμμα ακτινοβολίας της κεραίας του ραντάρ ,ο συντελεστής διάδοσης για τη διαδρομή παρεμβολέα προς ραντάρ, η απόσταση του παρεμβολέα από το ραντάρ, η ατμοσφαιρική εξασθένιση στη διαδρομή .ενώ αν πρόκειται για πυραύλους ο υποκλοπέας εξαρτάται και από την μέθοδο τηλεκατεύθυνσης , τα χαρακτηριστικά πυροσωλήνα ,και από τις μεθόδους ECCM .
Ο λόγος J/S (JAMMING –to – Signal ratio) υπολογίζεται από την παρακάτω σχέση :

$$\frac{J}{S} = \frac{P_j G_{jr} G_{rj} R^2_{tr} L_r B_r}{P_t G_{tr} G_{rt} R^2_{jr} L_j B_j}$$

Όπου

P_j = Ισχύς του jammer

G_{jr} =κέρδος κεραίας από τον jammer στο δέκτη επικοινωνίας

G_{rj}= κέρδος κεραίας από τον δέκτη στο jammer επικοινωνίας

R_{jr} = ακτίνα μεταξύ του jammer και του δέκτη συστήματος επικοινωνίας

B_j= εύρος ζώνης του πομπού του jammer

L_j = απώλεια σήματος του jammer

P_t = Ισχύς του εκπομπού επικοινωνίας

G_{rt} = κέρδος κεραίας από τον δέκτη στο πομπό επικοινωνίας

B_r=εύρος ζώνης του δέκτη επικοινωνίας

R_{tr} =ακτίνα μεταξύ του εκπομπού και του δέκτη συστήματος επικοινωνίας

L_r=απώλεια σήματος στο σύστημα επικοινωνίας

Από την εξίσωση παρατηρούμε ότι για να έχουμε την μέγιστη αποδοτικότητα στον ηλεκτρονικό πόλεμο θα πρέπει η Ενεργή Εκπεμπόμενη Ισχύς ERP (Effective Radiated Power)του jammer ,που είναι αποτέλεσμα του κέρδους της κεραίας και της ισχύς εξόδου ,να είναι υψηλή . Παρατηρούμε ότι η απόσταση jammer-δέκτη (**R_{jr}**) διπλασιαστεί τότε θα πρέπει η ισχύ να τετραπλασιαστεί (**P_j**) για να ισχύει η ισότητα και να συνεχίσει ο jammer να έχει το ίδιο αποτέλεσμα .Αντίθετα αν θα θέλαμε να εμποδίζαμε ένα jamming τότε το κέρδος της κεραίας προς τον δέκτη επικοινωνίας να είναι όσο τον δυνατόν μεγαλύτερο ενώ το κέρδος προς το jammer να είναι όσο γίνεται πιο μικρό.

Ο λόγος της συνδυασμένης παρεμβολής προς θόρυβο προκύπτει από τον τύπο

$$I_o / N_o = \frac{N_o + J_o + C_o}{N_o}$$

Οι ηλεκτρονικές παρεμβολές γίνονται πιο εύκολα σε τηλεπικοινωνιακά συστήματα που μεταξύ των τηλεπικοινωνιακών συσκευών εκπέμπεται ένα σήμα συγχρονισμού γιατί έτσι και χαθεί ο συγχρονισμός διακόπτεται η μετάδοση .Είναι δύσκολο για τον jammer να ξέρει πότε έχει χαθεί ο συγχρονισμός.

ΚΑΤΗΓΟΡΙΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΠΟΛΕΜΟΥ

Σύμφωνα με τον Αίθωνα Ναρλή,Δρ. Ηλεκτρονικού Μηχανικού διακρίνουμε τις παρακάτω κατηγορίες ηλεκτρονικού πόλεμου:

ELINT:

Προέρχεται από τα αρχικά ELectronic INTelligence και έχει σκοπό την ανάλυση των μη τηλεπικοινωνιακών ηλεκτρομαγνητικών και των ακουστικών σημάτων, εκπεμπόμενων από μη πυρηνικές πηγές. Κεντρικός όμως σκοπός είναι η αναγνώριση και καταγραφή των παραμέτρων εκπομπής των ραντάρ. Χωρίς αυτά τα δεδομένα η αποτελεσματική αναγνώριση και παραπλάνηση των εχθρικών ραντάρ είναι επισφαλής.

ESM:

Προέρχεται από τα αρχικά του όρου Electronic Support Measures. Ασχολείται με τις δραστηριότητες ανίχνευσης, εντοπισμού και ταχείας αναγνώρισης των εκπομπών ραντάρ για άμεση αναγνώριση κινδύνου . Με την χρήση παθητικών αισθητήρων γίνεται η υποκλοπή της ηλεκτρομαγνητικής δραστηριότητας του αντιπάλου .Έτσι δίδεται η δυνατότητα ταυτοποίησης της υποκλοπής με φορέα , άμεσης και ταχείας εμπλοκής δραστηριοτήτων αντιμέτρων, αποφυγής και σκόπευσης.

ECM:

Προέρχεται από τα αρχικά Electronic Counter Measures. Σκοπό έχει να προκαλεί δυσχέρειες ή και να απαγορεύει τη χρήση του ηλεκτρομαγνητικού φάσματος από τον εχθρό. Κάνουν διακοπή λειτουργίας και παραπλάνησης των αισθητήρων και επικοινωνιών των αντιπάλων .

ECCM :

Προέρχεται από τον όρο Electronic Counter Measures έχει σκοπό να κάνει ασφαλή τη μεταχείριση του ηλεκτρομαγνητικού φάσματος από φίλιες δυνάμεις ,να τις προστατεύει από τα εχθρικά αντίμετρα και να κάνουν τα ηλεκτρομαγνητικά συστήματα απρόσβλητα από τις επιθέσεις του ηλεκτρονικού πόλεμου . Οι τεχνικές ECM και ECCM είναι παρόμοιες και για τα επικοινωνιακά συστήματα.

.

COMINT:

Ο όρος αυτός προέρχεται από τα αρχικά του COMmunication INTelligence .Έχει σκοπό την ανάλυση των τεχνικών χαρακτηριστικών των επικοινωνιακών σημάτων, τον εντοπισμό των πηγών εκπομπής, την πυκνότητα των αναμεταδόσεων και τις υποκλοπές τηλεπικοινωνιών .

SIGNIT:

Είναι τα αρχικά από τον όρο SIGNal InTelligence. Οι αρμοδιότητες του καλύπτουν όχι μόνο αυτών του ELINT και του COMINT αλλά και οποιασδήποτε φύσεως εκπομπής συμπεριλαμβανομένων και των ηλεκτρομαγνητικών εκπομπών, είτε σεισμικών που προέρχονται από πυρηνικές εκρήξεις.

ΕΙΔΗ JAMMING

Ο πιο συνηθισμένος τρόπος για να γίνει ένα JAMMING είναι να γίνει εκπομπή περιορισμένου εύρους θορύβου (barrage jamming ,denial jamming) , με αποτέλεσμα από την εισβολή του σήματος παρεμβολής στην συχνότητα επικοινωνίας να κατακλυστεί το πραγματικό σήμα από το αυτό. Επίσης μπορούν να χρησιμοποιηθούν διαφορές κυματομορφές που είναι πολύ αποτελεσματικές στον ηλεκτρονικό πόλεμο όπως FM διαμορφωμένος θόρυβος ,«ριπές» Θορύβου .CW τόνοι (Constant Wave) που δημιουργεί το spot jamming και τα σήματα που σαρώνουν όλο το φάσμα (swept –spot jamming) .Οι παρεμβολές θορύβου στις τηλεπικοινωνίες δεν γίνονται πάντοτε αντιληπτές ως παρεμβολή. Ας δούμε αναλυτικά ορισμένες από τις μέθοδοι παρεμβολής που χρησιμοποιούνται γενικά και κυρίως στα ραντάρ και ραντάρ αεροπλάνων

Βασικές μέθοδοι παρεμβολής

Spot Noise (σημείου)είναι η πιο απλούστερη μέθοδος, όπου εκπέμπεται μια κυματομορφή (ένας θόρυβος) με την μέγιστη ισχύ σε πολύ μικρό εύρος συχνοτήτων ή σε ένα κανάλι λειτουργίας του εχθρικού πομπού. Ωστόσο, παρόλο που υπάρχει δυνατότητα παρεμβολής ραντάρ με ευελιξία συχνότητας (frequency agile), τα αποτελέσματα δεν ικανοποιούν. Με την τεχνική Noise Jammer δεν απαιτείται να ξέρει κάποιος λεπτομερείς πληροφορίες για χαρακτηριστικά του εχθρικού συστήματος είναι όμως ευάλωτη σε συστήματα ευρέσεως διοπτεύσεως (DF) εχθρικού P/E, θέτουν σε κίνδυνο το φορέα τους (Anti-Radiation Missile).
Σημείωση 1: Το ανωτέρω μειονέκτημα αφορά απλές τεχνικές παρεμβολής θορύβου σε εχθρικά P/E και όχι τεχνικές “Noise Cover Pulse”.

Barrage Noise (φραγμού)εδώ παρεμβάλλεται θόρυβος ταυτόχρονα σε όλη τη σχετική μπάντα (σε ένα μεγάλο συχνοτήτων) , αλλά απαιτείται υψηλότερη ισχύς εκπομπής για το ίδιο αποτέλεσμα .Αυτό το πετυχαίνουμε ή όταν ένας jammer εκπέμπει σε όλο το εύρος συχνοτήτων (κυρίως σήμα λευκού θορύβου) ή έχοντας έναν μεγάλο αριθμό από jammers σε γειτονικές συχνότητες ,ώστε να καλύπτει όλο το εύρος .

Swept-spot Noise (σάρωσης): Ανιχνεύεται συνεχώς μια μπάντα συχνοτήτων(συνήθως θόρυβος μικρού εύρους) και αφού ανιχνευτούν οι χρησιμοποιούμενες, εκτελείται παρεμβολή στην περιοχή που ορίζεται από τη χαμηλότερη και την υψηλότερη συχνότητα εκπομπής. Ο σχεδιαστής του ECM πρέπει να προσδώσει ευελιξία στην ταχύτητα σάρωσης του παρεμβολέα, ώστε να υπάρχει βέλτιστη προσαρμογή. Θα πρέπει να σαρώνει επανειλημμένα όλη την ευρεία περιοχή και ο ρυθμός σάρωσης να είναι τέτοιος ώστε σε κάθε περιοχή συχνοτήτων να παραμένει για αρκετό χρόνο για να

διακοπεί η επικοινωνία μεταξύ πομπού και δέκτη. Γι' αυτόν το λόγο μπορεί να τροποποιηθεί αυτός ο παράγοντας λειτουργίας σε δύο παρεμβολείς επί του ίδιου φορέα. Το Swept-spot Noise (ή Sweep jamming) συνδυάζει τα πλεονεκτήματα του Barrage και του Spot jamming γιατί σαρώνει πολύ γρήγορα σε μια στενή ζώνη συχνοτήτων ,εξοικονομώντας ενέργεια.

Οι παρεμβολές ***Spot Noise, Swept-spot Noise ,Noise Barrage Noise*** είναι τεχνικές θόρυβου. Με την απλή τεχνική Noise Jammer((όχι την "Noise Cover Pulse")δεν απαιτείται να ξέρει κάποιος λεπτομερείς πληροφορίες για τα χαρακτηριστικά του εχθρικού συστήματος, είναι όμως ευάλωτη σε συστήματα ευρέσεως διοπτεύσεως (DF) εχθρικού P/E και θέτουν σε κίνδυνο το φορέα τους (Anti-Radiation Missile).Η παρεμβολή θορύβου στις τηλεπικοινωνίες δεν γίνεται πάντοτε αντιληπτή ως παρεμβολή.

Στα ραντάρ έχουμε επίσης και τις παρακάτω ***<u>τεχνικές παρεμβολής:</u>***

<u>JITTER PRF Pulsed Jammer</u> .

Είναι μια παραλλαγή όπου ο jammer μεταπηδά διαδοχικά σε καταστάσεις ON/OFF.

Range-Gate Pull Off (RGPO ή Range Gate Stealing) (μετακίνηση ή «κλοπή» πύλης)

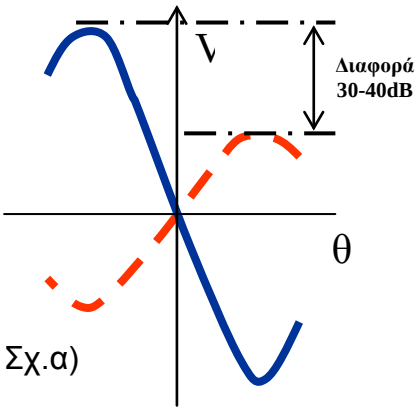
Τα ραντάρ ιχνηλάτησης συγκεντρώνονται σε ένα στόχο. Αυτό γίνεται με μια διαδικασία γνωστή ως gating και δίνει μια ευκαιρία στο σχεδιαστή ECM να προκαλέσει σύγχυση. Από τη στιγμή που επιλεγεί ο στόχος, το ραντάρ δεν «ακούει» συνεχώς μεταξύ των παλμών εξόδου από την ηχώ του ραντάρ, αλλά μόνο τη στιγμή περίπου που αναμένεται η ανάκλαση. Καθώς ο στόχος αυξάνει ή μειώνει την απόστασή του, η gate (πύλη) μετακινείται ανάλογα. Το διάστημα χρόνου μεταξύ του παλμού εξόδου του ραντάρ και την απάντηση gated που λαμβάνεται χρησιμοποιείται για την εξαγωγή της απόστασης του στόχου. Η πύλη ανάλογα ακολουθεί το σήμα επιστροφής, με τα σήματα εκτός αυτής να απορρίπτονται. Με τη μέθοδο RGPO η πύλη αποσπάται από την ηχώ του ραντάρ. Οι παλμοί ραντάρ που φτάνουν στον παρεμβολέα ενισχύονται και επανεκπέμπονται, ώστε να προκαλέσει την αυτόματη μείωση κέρδους των κυκλωμάτων λήψης του ραντάρ, όπως θα έκανε ο καθένας μας αν ξαφνικά το ραδιόφωνο αύξανε την έντασή του από μόνο του που θα μείωνε την έντασή του. Αν τα κυκλώματα του ραντάρ δεν μπορούν να διακρίνουν την αυθεντικότητα του σήματος, τότε το ραντάρ θα αρχίσει να «απαντά» στο λάθος σήμα, οπότε η πύλη έχει «κλαπεί». Με καθυστέρηση του σήματος (αλλαγή φάσης), ο παρεμβολέας πείθει το ραντάρ (την πύλη) πως ο στόχος απομακρύνεται έως ότου το πραγματικό σήμα επιστροφής βρεθεί εκτός πύλης και πλέον αγνοείται. Αν τώρα ο παρεμβολέας σταματήσει την εκπομπή, ο στόχος θα μοιάζει να έχει εξαφανιστεί μιας και η πύλη μένει κενή. Αυτή η μέθοδος αποδίδει ιδιαίτερα εναντίον των ραντάρ που εκτελούν TWS, τα οποία υπερφορτώνονται από αποθηκευμένες και εισερχόμενες πληροφορίες.

(VGRO) ΑΠΟΣΠΑΣΗΣ ΘΥΡΑΣ ΤΑΧΥΤΗΤΑΣ .

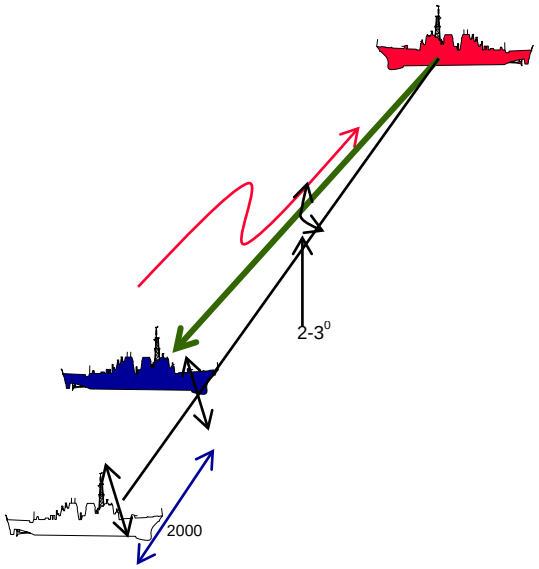
Η τεχνική VGPO μοιάζει με την παρουσιάζει RGPO έχει ειδικό ενδιαφέρον για την αντιμετώπιση PD Radar που χρησιμοποιούν φίλτρα στενής περιοχής συχνότητας, τα οποία εκτελούν πρόσκτηση της μετατόπισης συχνότητας Doppler του στόχου και ιχνηλατούν τη μεταβολή της τότε ο παρεμβολέας αναπαράγει και εκπέμπει το λαμβανόμενο σήμα με παραποιημένη ή μηδενική μετατόπιση Doppler ώστε το εχθρικό ραντάρ να εξάγει ταχύτητα στόχου διαφορετική της πραγματικής ή να θεωρηθεί ο στόχος ακίνητος, με συνέπεια να διακοπεί η πρόσκτηση.

ΠΑΡΑΠΛΑΝΗΣΗ ΜΟΝΟΠΑΛΜΙΚΟΥ P/E ΚΑΤΑ ΔΙΟΠΤΕΥΣΗ ΜΕ ΤΕΧΝΙΚΗ CROSS – POLARIZATION

όπου απαιτείται ισχύς παρεμβολής υπερέχουσα της ισχύος του εχθρικού P/E κατά 30-40dB(σχ.α)



Σχ.α)



Σχ.β)

Σχ.β) Παρατηρούμε ότι η συσκευή προκαλεί σφάλμα αποστάσεως 2000 yards και σφάλμα διοπτεύσεως $2\text{-}3^0$. Ο ερυθρός διατηρεί τον εγκλωβισμό αλλά αυτός είναι λάθος Όπως παρατηρούμε ότι πιο αποτελεσματικός είναι ο συνδυασμός των τεχνικών RGPO ΚΑΙ CROSS POLARIZATION .

Velocity track breaking (αποδέσμευση ίχνους ταχύτητας):

Παρόμοια με την RPGO, με ειδίκευση σε παλμικά ραντάρ doppler και Συνεχούς Κύματος. Το εκπεμπόμενο σήμα έχει ελαφρώς διαφορετική συχνότητα, την οποία το ραντάρ την εκλαμβάνει ως μεταβολή της ταχύτητας του στόχου.

Inverse amplitude modulation (ανάστροφη διαμόρφωση πλάτους):

Χρησιμοποιείται εναντίον ραντάρ κωνικής σάρωσης, τα οποία σαρώνουν μια περιοχή γύρω από το στόχο, οπότε ανάλογα με την ισχύ του σήματος και τη συχνότητα των σημάτων επιστροφής στην περιοχή ανίχνευσης μπορεί να κεντράρει επάνω στο στόχο. Αν αυτός βρίσκεται στο κέντρο, το σήμα επιστροφής θα εξαρτάται μόνο από σποραδικές μεταβολές που προκαλούνται από αλλαγή στάσης. Όποιες μεταβολές παρουσιάζουν την ίδια συχνότητα με το ρυθμό σάρωσης του ραντάρ σημαίνει ότι προκαλούνται από την έκκεντρη θέση του στόχου, δίνοντας έτσι ισχυρότερη επιστροφή σε ένα μόνο σημείο της περιοχής σάρωσης. Ο παρεμβολέας επομένως μπορεί να στείλει τέτοια σήματα που να προκαλέσουν τη μετατόπιση της κεραίας για διόρθωση. Πολλά παλαιά σοβιετικά ραντάρ, αλλά και μερικά νέα, είναι διστατικά (bistatic), δηλαδή έχουν διακριτές κεραίες λήψης και εκπομπής. Στην περίπτωση αυτή μόνο η κεραία λήψης χρησιμοποιεί κωνική σάρωση. Ως αποτέλεσμα, δεν μπορεί να ανακαλυφθεί ο ρυθμός σάρωσης με τις κλασικές μεθόδους ELINT από τη στιγμή που η μέθοδος είναι παθητική. Αυτά τα ραντάρ αντιμετωπίζονται μόνο με μεταβολή του ρυθμού διαμόρφωσης του παρεμβολέα εντός ενός πεδίου πιθανών τιμών, οπότε να αποδίδει σε τακτά

χρονικά διαστήματα. Τα μονοπαλμικά ραντάρ ιχνηλατήσεις δεν επηρεάζονται από αυτή τη μέθοδο, μιας και τέτοιες κεραίες εκπέμπουν τέσσερις (συνήθως) ακτίνες και λαμβάνουν τα σήματα λάθους από σύγκριση των αντίθετων ζευγαριών ακτινών. Τα σήματα αυτά λαμβάνονται με ηλεκτρονική και όχι μηχανική σάρωση, περιπλέκοντας περισσότερο το θέμα της παρεμβολής.

Inverse gain jamming (παρεμβολή ανάστροφου κέρδους):

Αποσκοπεί στην παρεμβολή ραντάρ έρευνας και πρόσκτησης. Καθώς αρχίζει ο φωτισμός του στόχου (του αεροσκάφους που φέρει τον εξοπλισμό ECM) ο παρεμβολέας λαμβάνει το σήμα και το επανεκπέμπει σε υψηλότερη στάθμη ισχύος. Καθώς τώρα επικεντρώνεται η ακτινοβόληση, ο παρεμβολέας συνεχίζει την εκπομπή αλλά σε πολύ μικρότερη στάθμη. Από τη στιγμή που τα κυκλώματα επεξεργασίας του ραντάρ υποθέτουν πως το ισχυρότερο σήμα έρχεται από το «κέντρο» του αεροσκάφους, εισάγεται σφάλμα αζυμουθίου ή ύψους.

False target generation (δημιουργία ψευδούς στόχου)

Ό,τι και προηγουμένως, αλλά για τα άκρα. Δημιουργεί επιπλέον στόχους καθώς «περνά» η ακτίνα του ραντάρ. Αν η ισχύς είναι αρκετή, η ένδειξη στην οθόνη του ραντάρ μοιάζει με τόξο και, αν η λειτουργία του παρεμβολέα είναι διακοπτόμενη, εμφανίζονται πολλαπλοί στόχοι. Ανάλογα με τη διαμόρφωση των παρεμβολών στην οθόνη εμφανίζονται σφάλματα κάθε είδους, ακόμη και το να εμφανίζεται ότι οι στόχοι κινούνται διαφορετικά!

Buddy Mode

Απαιτούνται δύο αεροσκάφη. Αν πετούν και τα δύο «εντός» της ακτίνας σάρωσης του εχθρικού ραντάρ και εκπέμπουν σήματα παρεμβολής της ίδιας συχνότητας και παρόμοιου πλάτους, μεταξύ των οποίων το ραντάρ δεν μπορεί να διακρίνει απόσταση και γωνία, δημιουργούνται σφάλματα έως και μισού γωνιακού διαχωρισμού από αυτόν μεταξύ των αεροσκαφών. Παρόμοιο αποτέλεσμα γίνεται και με ένα αεροσκάφος που πετά χαμηλά, με το δεύτερο σήμα να προέρχεται από την ανάκλαση του πρωτότυπου στο έδαφος. Το ζήτημα είναι πως ο παρεμβολέας θα πρέπει να αποστείλει περισσότερη ενέργεια προς το έδαφος (αν υπάρχει σχετική δυνατότητα με κεραία διάταξης φάσης) ώστε να αντιμετωπιστούν οι απώλειες διασποράς ή η πιθανή λήψη από πλευρικό λοβό του ραντάρ.

Cross Eye (στραβισμός)

Παρόμοια περίπτωση, μόνο που εδώ χρησιμοποιούνται δύο πηγές σήματος. Ένα ζεύγος κεραιών απέχει όσο το δυνατόν περισσότερο. Τα σήματα ραντάρ λαμβάνονται από τη μια και ενισχυμένα εκπέμπονται από τη δεύτερη και τα σήματα που λαμβάνονται από αυτή εκπέμπονται από την άλλη με διαφορά φάσης 180 μοίρες. Αν το σύστημα δουλεύει γρήγορα και με ακρίβεια, δημιουργείται πολύ μεγάλη σύγχυση στο ραντάρ.

Μία ενδιαφέρουσα όπως και φθηνή μέθοδος παραπλάνησης και παρεμβολής των ραντάρ είναι τα παθητικά δολώματα ***(passive decoys).*** Η συσκευή αυτή είναι ένας ανακλαστήρας ακτινοβολίας ραντάρ αποτελούμενος από «φακούς Luneberg» όμοιους σε λειτουργία με τα πλαστικά σήματα στα ποδήλατα, στα σήματα οδικής κυκλοφορίας κ.λπ. που ανακλούν το φως των προβολέων των αυτοκινήτων.

Άρα σε γενικές γραμμές οι παρεμβολείς (jammers) στα ραντάρ διακρίνονται σε σημειακούς (stand-off), συνοδευτικής προστασίας και αυτο-προστασίας.
Η πυκνότητα ισχύος του παρεμβολέα στα ραντάρ υπολογίζεται λαμβάνοντας υπόψη
α) τη θέση του παρεμβολέα στο διάγραμμα ακτινοβολίας της κεραίας του ραντάρ και το συντελεστή διάδοσης για τη διαδρομή παρεμβολέα προς ραντάρ ,
β) την απόσταση του παρεμβολέα από το ραντάρ και την ατμοσφαιρική εξασθένιση στη διαδρομή.
Η συνολική ισχύς παρεμβολής είναι το άθροισμα του θερμικού θορύβου και των εξωτερικών παρεμβολών. Όμως όταν ο στόχος που ανιχνεύεται από ένα ραντάρ είναι ένα πολεμικό αεροσκάφος, είναι δυνατή η παραπλάνηση του ραντάρ, με την απελευθέρωση ενός μεγάλου αριθμού μεταλλικών νημάτων από το αεροσκάφος και αυτή η τεχνική παραπλάνησης λέγεται μοντέλο Μεταλλικών Νημάτων (CHAFF) .

Mitigation Paths for Free-Space GPS Jamming

Matt Boggs
Kenea C. Maraffio
GPS/INS Systems Section, Naval Air Warfare Center Weapons Division (NAWCWPNS)/China Lake

STEALTH

Υπάρχουν αρκετοί τρόποι που καθιστούν δύσκολο τον εντοπισμό στόχου από τα ραντάρ, με εντυπωσιακότερο όλων την «μυστικότητα» (Stealth), ο οποίος επηρεάζει την αντανακλαστικότητα (RCS) του στόχου. Το RCS ενός αεροσκάφους ή άλλου οχήματος εξαρτάται από διάφορους παράγοντες, συμπεριλαμβανομένου του μεγέθους, τα υλικά από τα οποία κατασκευάστηκε, (τα μέταλλα π.χ., παρέχουν ένα υψηλό RCS) , και η μορφή, όπου καθιστώντας τις γωνίες αιχμηρές , διασκορπίζεται το σήμα επιστροφής, αυξάνοντας έτσι το RCS. Επίσης όσο λιγότερες γωνίες έχει ένα αεροσκάφος τόσο δυσκολότερο είναι να εντοπιστεί γιατί αντανακλά λιγότερο τα ηλεκτρομαγνητικά κύματα . Η «μυστικότητα» ενός αεροσκάφους Stealth βελτιστοποιείται, από την μπροστινή κάτω όψη, αυτή ακριβώς την όψη που βλέπει το Ραντάρ .Είναι δύσκολο να κατασταθεί ένα αεροσκάφος «αόρατο» από όλες τις πλευρές. Κατά ενδιαφέρον τρόπο, τα χαμηλής συχνότητας ραντάρ έχουν περισσότερες πιθανότητες, να εντοπίσουν τα Stealth αεροσκάφη, από τα υψηλής συχνότητας ραντάρ.
Επιπλέον, εάν ένα ραντάρ που λειτουργεί σε μια μεγάλη υψομετρικά πλατφόρμα ανιχνεύσει ένα αεροσκάφος Stealth που πετά σε χαμηλό ύψος, θα είναι σε θέση να το απεικονίσει ως "τρύπα" στις επιστροφές ραντάρ.

ΤΕΧΝΙΚΕΣ ΑΠΟΦΥΓΗΣ JAMMING (anti-jamming) [Γ΄,64]

Για το jamming υπάρχουν τεχνικές αποφυγής αλλά και συσκευές με ενσωματωμένες τις τεχνικές αποφυγής(ECM) ,που χρησιμοποιούνται κυρίως σε στρατιωτικές εφαρμογές και στις επικοινωνίες .Το κόστος των συσκευών δεν θα πρέπει να είναι υπερβολικά υψηλό. Βέβαια όλα εξαρτούνται από την από το μέγεθος και το είδος της απειλής του jammer , τις δυνατότητες και τις ικανότητες του .

Οι τεχνικές anti-jamming είναι :

LPD (Low Probability of Detection)

Σύμφωνα με την τεχνική αυτή η ηλεκτρομαγνητική επικοινωνία έχει τέτοια στοιχεία ,που δεν ανιχνεύεται από τον εχθρό .φαίνεται ότι δεν υπάρχει ,καμουφλάρεται από τον θόρυβο και έτσι ο jammer δεν μπορεί να παρεμβάλλει σε ένα για αυτόν ανύπαρκτο σήμα .

LPI (Low Probability of Intercept)

Εδώ ο jammer δυσκολεύεται στην παρεμβολή του Το ηλεκτρομαγνητικό σήμα επικοινωνίας έχει τέτοια στοιχεία ,που ο jammer δυσκολεύεται στην παρεμβολή του.

Ο συνδυασμός και των δύο τεχνικών(Low Probability of Detection και της Low Probability of Intercept)είαναι πολύ αποτελεσματικές στο jamming .

Άλλα κυκλώματα ***anti-jamming*** είναι

ISU (Interference Suppression Unit)

Απορρίπτει ασύγχρονες-ως προς PRF-παρεμβολές και σήματα θορύβου

PAD (Pulse Amplitude Discrimination)

Απορρίπτει όλους τους παλμούς οι οποίοι έχουν πλάτος μεγαλύτερο από το αναμενόμενο πλάτος της ηχούς του στόχου .

PC (Pulse Compression)

Διαμορφώνουμε κομμάτια του παλμού.
Έτσι κωδικοποιούμε το σήμα, και το P/E απορρίπτει τους μη κωδικοποιημένους παλμούς παρεμβολής .

PLD (Pulse Length Discrimination)

Απορρίπτει όλους τους λαμβανόμενους παλμούς που είναι μικρότερης ή μεγαλύτερης διάρκειας από τον εκπεμπόμενο παλμό .

STC (Sensitivity Time Control)

Ανάλογα με την απόσταση αυξάνει η ευαισθησία του δέκτη. Έτσι έχουμε μικρή ευαισθησία στις μικρές αποστάσεις, εκεί όπου οι στόχοι δίνουν ισχυρά σήματα.

AGC (Automatic Gain Control)

Αυτό είναι αποτελεσματικό ενάντια σε παρεμβολή μεταβαλλόμενου πλάτους γιατί περιορίζει τα σήματα μεγάλου εύρους και μακράς διαρκείας.

Pol. Can (Polarization Cancellation)

Απορρίπτονται ηλεκτρομαγνητικές ακτινοβολίες ανεπιθύμητης πολώσεως.

VC (Video Corellation)

Επειδή οι πραγματικοί στόχοι έχουν το ίδιο πλάτος και θέση από σάρωση σε σάρωση, αυτό το κύκλωμα συσχετίζει τις διαδοχικές εκπομπές της συσκευής.

Λογαριθμικός Ενισχυτής

Ενισχύει γραμμικώς τα ασθενή σήματα και λογαριθμικός τα ισχυρά.
Jitter PRF .Εξαφανίζει παρεμβολές με το να μεταβάλλει το PRF από παλμό σε παλμό ώστε να μην μπορούν να συγχρονισθούν οι Jammers στο PRF του P/E. Ψευδείς στόχοι που προέρχονται από παρεμβολές εμφανίζονται μετατοπιζόμενοι κατά απόσταση και διακρίνονται εύκολα Είναι η πλέον αποτελεσματική τεχνική σε ECM παραπλανήσεως.

Τεχνική Frequency Agility

Το P/E κατέχει συγκεκριμένο αριθμό καναλιών/ εκπεμπόμενων συχνοτήτων. Εάν ο χειριστής διαπιστώσει παρεμβολή, χρησιμοποιεί άλλο κανάλι εκπομπής. Η αποτελεσματικότητά της εξαρτάται από την εκπαίδευση του χειριστή.

Τεχνικές διευρυμένου φάσματος (spread spectrum)

Στις επικοινωνίες διευρυμένου φάσματος το σήμα εξαπλώνεται επίτηδες σύμφωνα με μια ψευδοτυχαία σειρά, σε μια περιοχή συχνοτήτων πολύ μεγαλύτερου εύρους από αυτό που χρειάζεται να μεταδοθεί το σήμα έτσι ώστε να απορριφθούν σχεδόν όλες οι παρεμβολές που οφείλονται σε Jammer .

1.ΤΕΧΝΙΚΕΣ ΔΙΕΥΡΥΜΕΝΟΥ ΦΑΣΜΑΤΟΣ (spread spectrum)

Οι τεχνικές διευρυμένου φάσματος είναι μια τεχνολογία ,που δυσκολεύει τον εντοπισμό ,την υποκλοπή και το jamming .Στις επικοινωνίες διευρυμένου φάσματος το σήμα εξαπλώνεται επίτηδες σύμφωνα με μια ψευδοτυχαία σειρά, σε μια περιοχή συχνοτήτων πολύ μεγαλύτερου εύρους από αυτό που χρειάζεται να μεταδοθεί το σήμα έτσι ώστε να απορριφθούν σχεδόν όλες οι παρεμβολές που οφείλονται σε Jammer. Η ψευδοτυχαία σειρά, αποτελεί τον κώδικα διεύρυνσης του σήματος (spreading code) και με αυτόν τον τρόπο το σήμα αποκτά σαν ένα είδος <<ανοσία>> σε διάφορους τύπους θορύβου και στη παρεμβολή πολλαπλών διαδρομών .Επίσης μπορεί να χρησιμοποιηθεί για την απόκρυψη και κρυπτογράφηση των σημάτων .Ο πομπός και ο δέκτης θα πρέπει να έχουν την ίδια ψευδοτυχαία σειρά και να είναι σε απόλυτο συγχρονισμό , ώστε να μπορεί να ανακτηθεί σωστά το σήμα στον δέκτη. Τα σήματα των χρηστών διαχωρίζονται στον δέκτη χρησιμοποιώντας τις ιδιότητες του κώδικα και η παρεμβολή μεταξύ των χρηστών περιορίζεται από την ετεροσυσχέτιση των κωδικών. Η ετεροσυσχέτιση (Cross correlation)είναι η σύγκριση μεταξύ δύο ακολουθιών που προέρχονται από διαφορετικές πηγές .Όταν λέμε σύγκριση δηλαδή συσχέτιση (Correlation) τότε βλέπουμε πόσο όμοια είναι τα δύο σύνολα δεδομένων μεταξύ τους και παίρνουν τιμές από (–1 ως 1) .Αν οι τιμές είναι (1) τότε οι δύο ακολουθίες είναι όμοιες , αν είναι (0) τότε δεν υπάρχει σχέση μεταξύ τους και αν είναι (-1) η μία ακολουθία είναι κατοπτρική της άλλης. Υπάρχει και η έννοια της αυτοσυσχέτιση (Auto correlation)που θα χρησιμοποιήσουμε παρακάτω και είναι η σύγκριση μιας ακολουθίας με ένα μετατοπισμένο στο χρόνο αντίγραφό της.Με την διαμόρφωση διευρυμένου φάσματος μειώνονται οι πολλαπλές διαδρομές και πολλοί χρήστες μπορούν να μοιράζονται το ίδιο κανάλι χωρίς να χρειάζεται εξωτερικός μηχανισμός συγχρονισμού δηλαδή επικοινωνία πολλαπλής πρόσβασης. Έτσι πολλαπλοί χρήστες μπορούν να χρησιμοποιήσουν το ίδιο κανάλι ευρέως φάσματος με πολύ μικρή παρεμβολή
Η πολλαπλή πρόσβαση με διαίρεση κώδικα που λέγεται CDMA λέγεται και μετάδοση διευρυμένου φάσματος.
.Οι κατηγορίες ακολουθιών διεύρυνσης (spreading codes) είναι οι
α) PN ακολουθίες.
και β) οι Ορθογώνιοι κώδικες .
Μια PN γεννήτρια παράγει ακολουθία που φαίνεται να είναι τυχαία αλλά δεν είναι στατικά τυχαία γιατί περνάει πολλά τεστ τυχαιότητας .Οι PN ακολουθίες παράγονται από έναν αλγόριθμο χρησιμοποιώντας μια αρχική τιμή (seed). Αν δεν είναι γνωστά ο αλγόριθμος και η αρχική τιμή, είναι πρακτικά αδύνατο να προβλεφθεί η ακολουθία . Οι PN ακολουθίες με μεγάλη πιθανότητα έχουν χαμηλές ετεροσυσχέτισεις (cross-correlation) και αυτοσυσχετίσεις (autocorrelation) .Οι Ορθογώνιοι κώδικες είναι σχεδιασμένοι ώστε όλες οι ετεροσυσχέτισεις μεταξύ διαφορετικών κωδικών να είναι μηδενικές (και όλες οι αυτοσυσχέτισεις autocorrelations να είναι χαμηλά). Οι ορθογώνιες ακολουθίες μεταβλητού παράγοντα διάχυσης (OSVD-code)lλέγονται και κωδικοί καναλοποίησης ή βραχείς κώδικες (Channelisation Codes) και το μήκος τους εξαρτάται από τον παράγοντα SF (ή GF),διακρίνουν τα

διαφορετικά κανάλια μιας εκπομπής .όσο αφορά τα κινητά είναι ίδιοι για όλες τις κυψέλες /κινητά ,όμως χρειάζονται πρόσθετοι κώδικες(scrambling codes).Για κάθε κυψέλη είναι ειδικοί οι κωδικοί περίπλεξης .Οι κώδικες scrambling ή μακρύ κώδικες είναι μεγάλου μήκους (π,χ, 38400 chips),υπάρχουν σε μεγάλο πλήθος ,στο uplink διαχωρίζουν τα διάφορα κινητά (πηγές) και στο Downlink διαχωρίζουν τις διάφορες κυψέλες ανά τομείς (πηγές) .Με τον συνδιασμό των δυο κωδικών κατασκευάζονται οι χρησιμοποιούμενοι κωδικοί στο WCDMA (κινητά) που είναι ψευδοτυχαίες ακολουθίες (ΣΤΕΦΆΝΟΥ)

Η έννοια του διευρυμένου φάσματος είναι σχετική. Ένα σήμα που μεταφέρει πληροφορία με ρυθμό διαμεταγωγής R =100 Mbits / sec απαιτεί εύρος φάσματος B =100MH z και φυσικά δεν μπορεί να θεωρηθεί σήμα διασποράς φάσματος. Αντίθετα σήμα που μεταφέρει πληροφορία με ρυθμό R =100 bits / sec και «απλώνεται» σε εύρος B=100MH z , είναι, προφανώς σήμα διασποράς φάσματος, και μάλιστα ο λόγος κέρδους της διαδικασίας (processing gain) είναι της τάξεως B/ R $=10^6$, ή 60 dB .

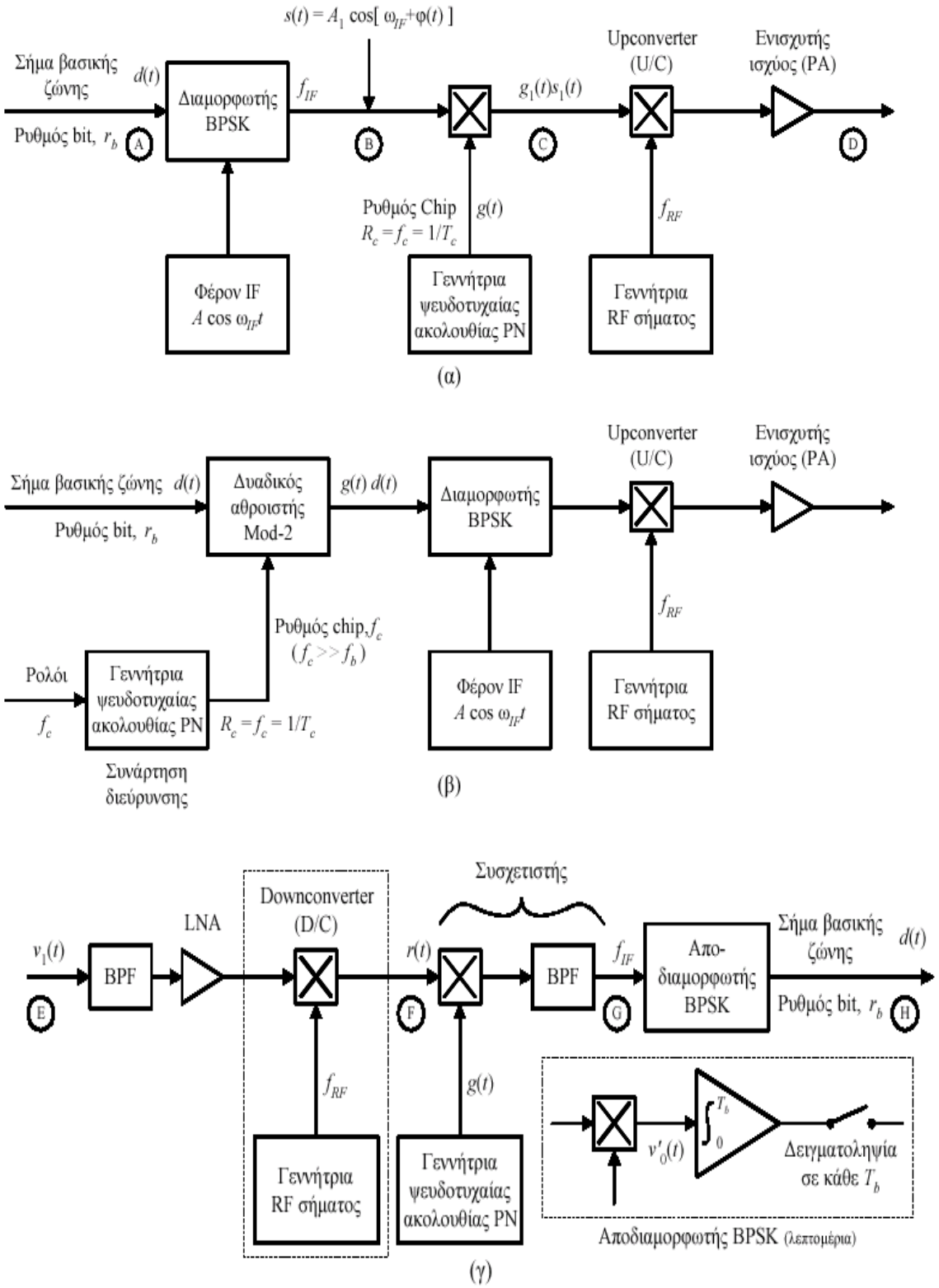
Ας συγκρίνουμε ένα σήμα «στενής ζώνης» με ένα σήμα διεσπαρμένου φάσματος. Παρατηρούμε ότι καθώς η ενέργεια του σήματος απλώνεται, η μέγιστη ισχύς μειώνεται με τέτοιο τρόπο, ώστε πολλές φορές να γίνεται μικρότερη ακόμη και από το κατώφλι θορύβου. Αλλά ακόμη και αν τα σήματα «χαθούν» μέσα στο θόρυβο μπορούν να επαναπροσδιορισθούν (αναδυθούν μέσα από το θόρυβο), με τη βοήθεια μιας μαθηματικής διαδικασίας συσχέτισης του κώδικα, ο οποίος έχει εγγραφεί στο σήμα πριν την εκπομπή του. Με τον τρόπο αυτό τα σήματα γίνονται «αόρατα» από τα κοινά συστήματα ηλεκτρονικής παρακολούθησης .

Υπάρχουν τρεις τρόποι για να «διευρύνουμε» το φάσμα. Ο πρώτος είναι απλός, μεταβάλλουμε συνεχώς, μεταξύ δύο ορίων, τη συχνότητα του φέροντος . Είναι τα γνωστά σήματα chirp (από τον ήχο τιτιβίσματος που ακούγεται στο δέκτη), που στην εποχή του Ψυχρού Πολέμου χρησιμοποιήθηκαν στα ραντάρ μεγάλης εμβέλειας για τη έγκαιρη προειδοποίηση πυρηνικής επίθεσης (early warning) . Ένα ισχυρότατο τέτοιο σήμα ήταν ακουστό, παλαιότερα, και στην Ελλάδα. Προερχόταν από το τεράστιας ισχύος ραντάρ επιτήρησης που είχαν οι Σοβιετικοί στα Ουράλια Όρη. Τα ραντάρ «πέραν του ορίζοντος», όπως λέγονται, λειτουργούν καλύτερα με τέτοια σήματα σάρωσης. Η τεχνολογία αυτή είναι πλέον ξεπερασμένη, αφού τον ίδιο ρόλο επιτελούν τώρα καλύτερα τα αεροπλάνα συνεχούς επιτήρησης (AWACS). Τώρα χρησιμοποιούνται κυρίως οι δύο παρακάτω συνηθισμένες τεχνικές .

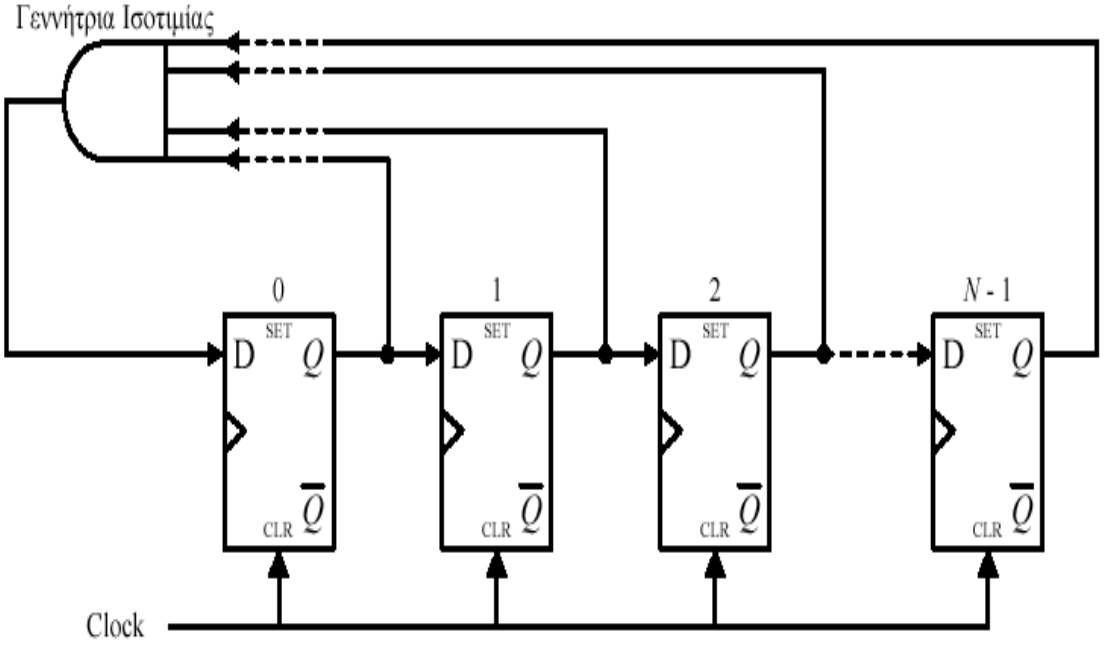
Οι πιο συνηθισμένες τεχνικές του διευρυμένου φάσματος είναι :

α) η άμεση ακολουθία (Direct Sequence –DS) (π.χ. WCDMA ,IS-95)

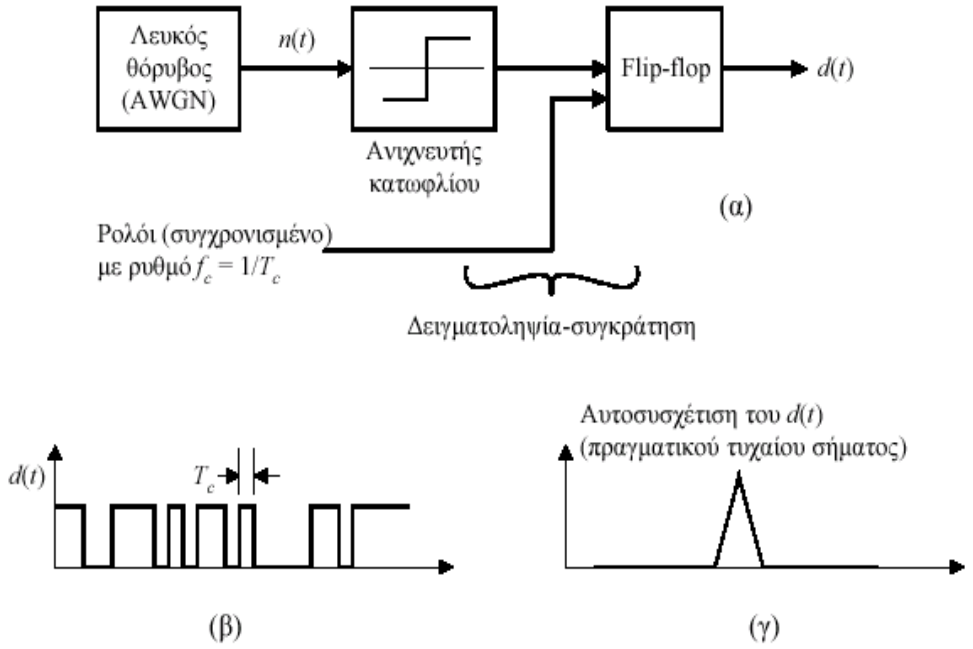
και β) η Αναπήδηση συχνότητας(Frequency Hoping – FH)(π.χ. GSM)



Σύστημα πομπού-δέκτη DS-CDMA. (α) Πομπός με διαμόρφωση BPSK ακολουθούμενη από διεύρυνση φάσματος (spreading). (β) Ισοδύναμος πομπός με τον (α) αλλά με τη διεύρυνση φάσματος στη βασική ζώνη. (γ) Ο αντίστοιχος δέκτης. Η αποδιαμόρφωση μπορεί και να προηγηθεί της απόδιεύρυνσης (de-spreading).



Γεννήτρια ψευδοτυχαίας ακολουθίας.



Παραγωγή τυχαίας ακολουθίας δυαδικών δεδομένων. (α) Γεννήτρια. (β) Χρονική απόκριση τραγματικού τυχαίου σήματος. (γ) Αυτοσυσχέτιση πραγματικού τυχαίου σήματος.

(του ΔΗΜΗΤΡΗ ΨΙΧΟΥΔΑΚΗ
ΣΧΕΔΙΑΣΗ ΕΠΙΓΕΙΟΥ ΣΤΑΘΜΟΥ ΣΤΑ 120 Mbps)

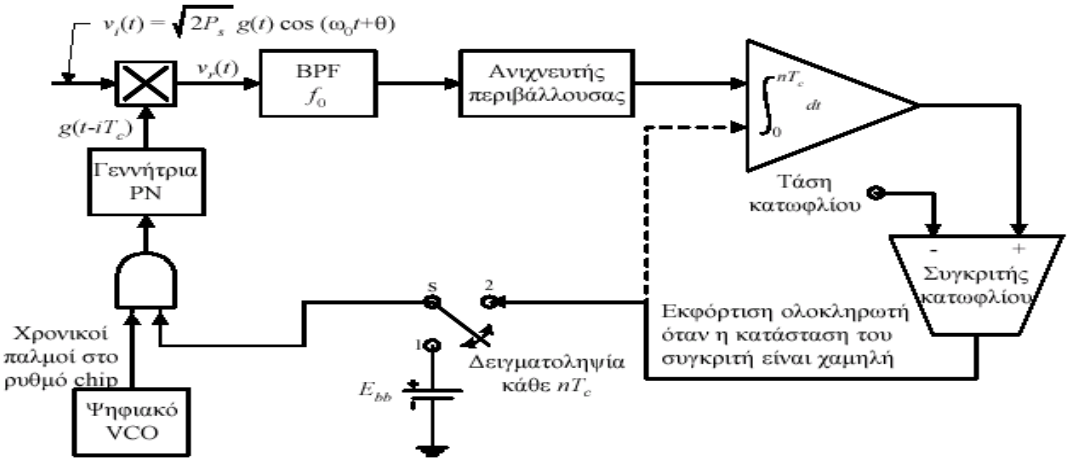
ΣΥΓΧΡΟΝΙΣΜΟΣ ΣΥΣΤΗΜΑΤΩΝ ΔΙΕΥΡΥΜΕΝΟΥ ΦΑΣΜΑΤΟΣ

Ο συγχρονισμός ενός δέκτη συστήματος διευρυμένου φάσματος απαιτεί τρία είδη συγχρονισμού:

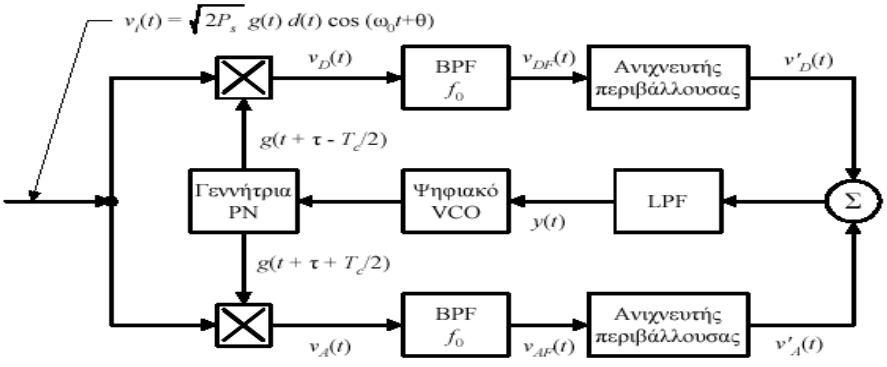
1) Συγχρονισμό φέροντος και φάσης (ανάκτηση φέροντος).
2) Συγχρονισμό bit και πλαισίου.
3) Συγχρονισμό chip ή ψευδοτυχαίας ακολουθίας.

Η ανάκτηση χρονισμού chip για τα DS-SS συστήματα γίνεται σε δύο φάσεις:

1) Ανάκτηση (acquisition) ή χονδρικός συγχρονισμός.
2) Ιχνηλάτηση (tracking) ή ακριβής συγχρονισμός.



Κύκλωμα ανάκτησης CDMA σήματος και σήματος διευρυμένου φάσματος.



Κλειδωμένος βρόχος καθυστέρησης (delay-locked loop, DLL) για ιχνηλάτηση (tracking) σημάτων DS-CDMA.

1.α)Η τεχνική άμεσης ακολουθίας διευρυμένου φάσματος (Direct Sequence Spread spectrum)

Στην τεχνική άμεσης ακολουθίας τα bits του κάθε χρήστη κωδικοποιούνται με μια δυαδική ακολουθία (=κωδικός). Ο ρυθμός του σήματος των δεδομένων (data rate) συμβολίζεται με D. Τα bits του κωδικού καλούνται chips δηλαδή έχουμε διάσπαση του κάθε bit σε *k chip. Άρα* τα chip είναι μια σταθερή ακολουθία, συγκεκριμένη για κάθε χρήστη και ο ρυθμός δεδομένων των chip στο νέο κανάλι είναι *kD (*chip rate) , που συμβολίζεται με W . Ο ρυθμός των chips (W)είναι τυπικά πολύ μεγαλύτερος από τον ρυθμό των bits(R).

Ο παράγων διάχυσης (SF) =

(SF) = (#chips/bit) = ρυθμός chips W / ρυθμός bit καναλιού R

Κέρδος επεξεργασίας (Processing Gain) (G) =10 log SF, db

Έτσι το κάθε bit στο αρχικό σήμα αναπαρίσταται με πολλαπλά chips στο μεταδιδόμενο σήμα Ο κώδικας απλώνει το σήμα σε μια ευρύτερη περιοχή συχνοτήτων και η διεύρυνση είναι ανάλογη με τον αριθμό chips που χρησιμοποιούνται .
Κυρίως υπάρχουν ***δυο τεχνικές*** που συνδυάσουν την ακολουθία πληροφορίας με τον κώδικα διεύρυνσης , η μια τεχνική είναι χρησιμοποιώντας XOR και η άλλη τεχνική αναπαριστά τα bits με +1 and -1 και χρησιμοποιεί πολλαπλασιασμό .
Η αποκλειστική πύλη OR(exclusive –OR) χρησιμοποιείται στην τεχνική αυτή κυρίως για την συνένωση ομάδα ψηφιακών σημάτων με ένα << τυχαίο >>θόρυβο ο οποίος έχει όλες τις συχνότητες του συγκεκριμένου φάσματος . Τα αποτέλεσμα είναι το φάσμα των συχνοτήτων να διαχέεται σε ένα εύρος ζώνης που είναι διπλάσιο του κωδικού. Αυτός ο τυχαίος κωδικός λέγεται Spreading Code ή Spreading Sequence .Όσο μεγαλύτερος είναι αυτός ο κωδικός τόσο μεγαλύτερο είναι το Processing Gain αλλά και τόσο μικρότερη είναι η καθαρή ροή των δεδομένων .Ας τον παρουσιάσουμε τον Spreading Code ως κωδικό κρυπτογράφησης που όσο μεγαλώνει ο κωδικός τόσο ασφαλέστερα κρυπτογραφούνται τα δεδομένα αλλά τόσο μεγαλύτερη επεξεργαστική ισχύς θα χρειαστεί. Στην πραγματικότητα η τεχνική αυτή δημιουργεί ένα << χάος μέσα από τάξη >> . Το πλεονέκτημα αυτή της τεχνικής είναι αν πολλαπλασιαστεί το διαμορφούμενο σήμα με τον αρχικό θόρυβο αυτό που θα προκύψει είναι το πρωτογενές σήμα. Αυτή η λειτουργία λέγεται correlation και λειτουργεί μόνο αν οι ψευδοτυχαίου κωδικοί είναι οι ίδιοι και απόλυτα συγχρονισμένοι με το ρολόι του κωδικού.

Τα βασικά πλεονεκτήματα της Direct Sequence Spread spectrum είναι :

Χαμηλή πυκνότητα ισχύος στον αέρα .
Η εκπομπή του Direct Sequence Spread spectrum)είναι συνεχής (δεν υπάρχουν hops , όπως θα δούμε παρακάτω) και η διασπορά(spreading) είναι του σήματος (πλάτος καναλιού) .Η ισχύς των 100 m V διαχέεται σε όλο το φάσμα συχνοτήτων και άρα ισχύς / Hz είναι τελικά πολύ χαμηλότερη των 100 MHz .Το σήμα του Direct Sequence Spread spectrum) καταλαμβάνει μεγαλύτερο πλάτος και μικρότερο ύψος , έτσι ώστε το συνολικό εμβαδόν να είναι ίδιο με την τεχνική FHSS, που θα δούμε παρακάτω. Το σήμα συνεπώς είναι πολύ κοντά στο επίπεδο θορύβου του περιβάλλοντος του σήματος

Απορρόφηση παρεμβολών .
Το σήμα του DSSS δεν επηρεάζεται από παρεμβολές . Για να πετύχει ο δέκτης την αποδιαμόρφωση θα πρέπει ο δέκτης να κάνει τον ίδιο πολλαπλασιασμό δηλαδή να πολλαπλασιάσει το σήμα με τον <<τυχαίο >> θόρυβο και αν υπάρχει και παρεμβολή θα πολλαπλασιαστεί και αυτή μαζί με τα άλλα. Μετά από αυτόν τον πολλαπλασιασμό στο δέκτη , αυτό που επιτυγχάνεται είναι να αποδιαμορφωθεί το επιθυμητό σήμα και να διαμορφωθεί κατά DSSS η παρεμβολή (με άλλα λόγια διαχέεται η παρεμβολή).

Παράλληλη χρήση του ίδιου καναλιού (Πολλαπλή Πρόσβαση) .
Για να πετύχουμε αποδιαμόρφωση , πρέπει ο δέκτης να κάνει ακριβώς τον ίδιο πολλαπλασιασμό με τον<< τυχαίο θόρυβο >> (Spreading Code) τότε έχουμε DSSS.Αν ο δέκτης δεν έχει αποθηκευμένο τον ίδιο <<τυχαίο θόρυβο >> τότε αυτό που θα πετύχει είναι να διασπείρει ακόμη περισσότερο το λαμβανόμενο σήμα δηλαδή να το ξαναδιαμορφώσει δηλαδή (άρα θα το εξασθενίσει) .Στηριζόμενοι σε αυτή την ιδιαιτερότητα μπορούμε σε κάθε κανάλι να βάλουμε συστήματα με διαφορετικά Spreading Code, χωρίς να υπάρχει σημαντική επιρροή . Το αποτέλεσμα που προκύπτει είναι ένα εκτεμένου εύρους φάσμα σε σύγκριση με την καθαρή πληροφορία και δημιουργείται το **Direct Sequence ευρέως φάσματος .**

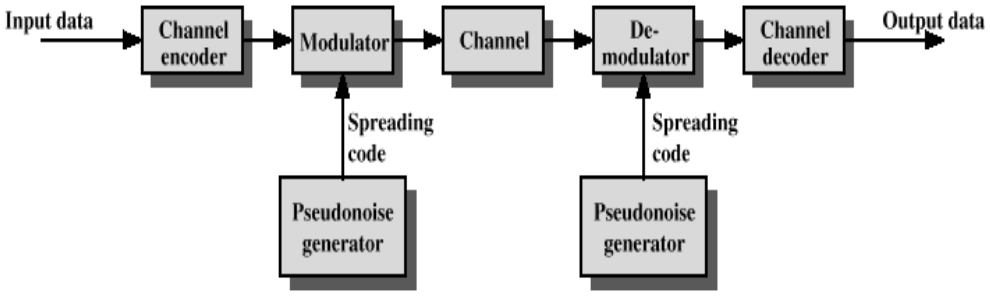
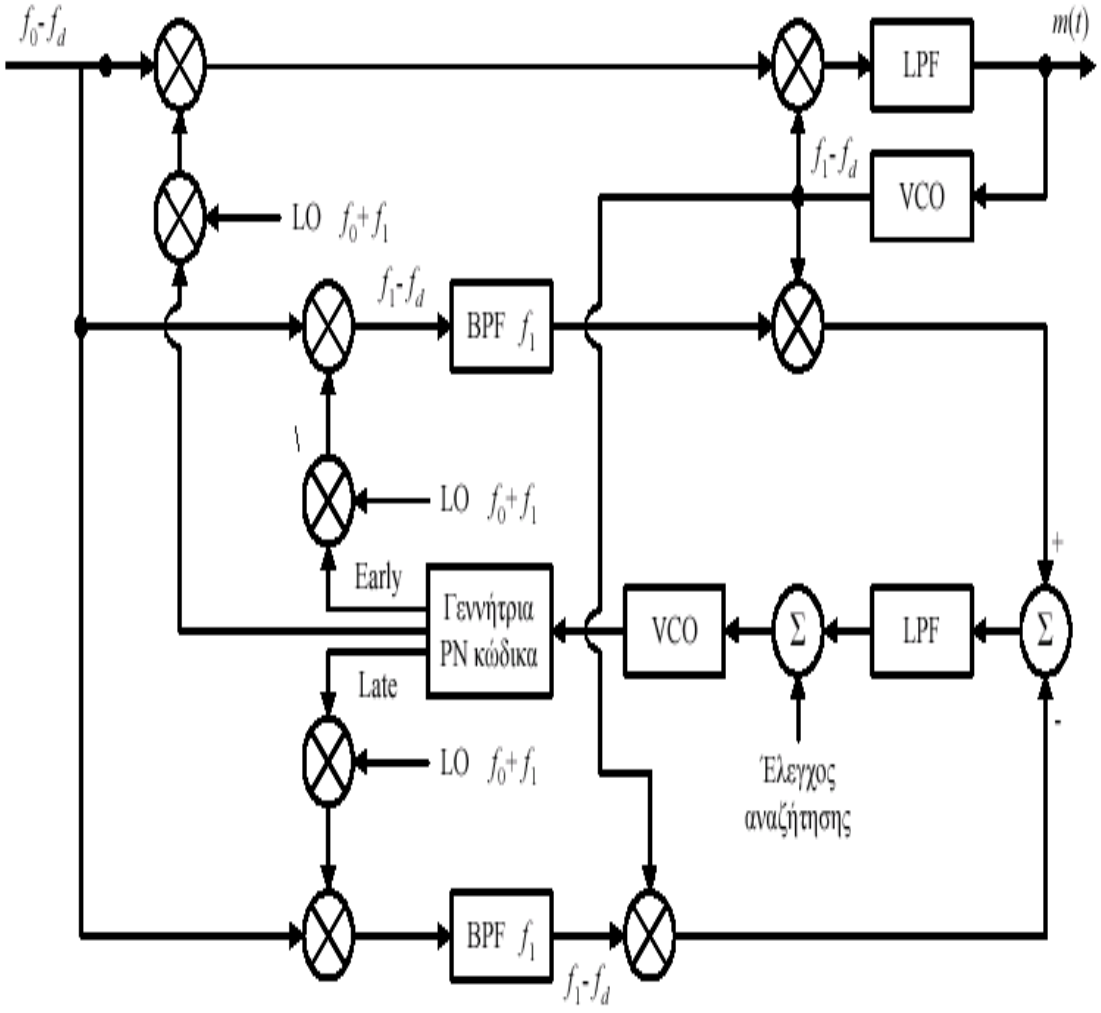


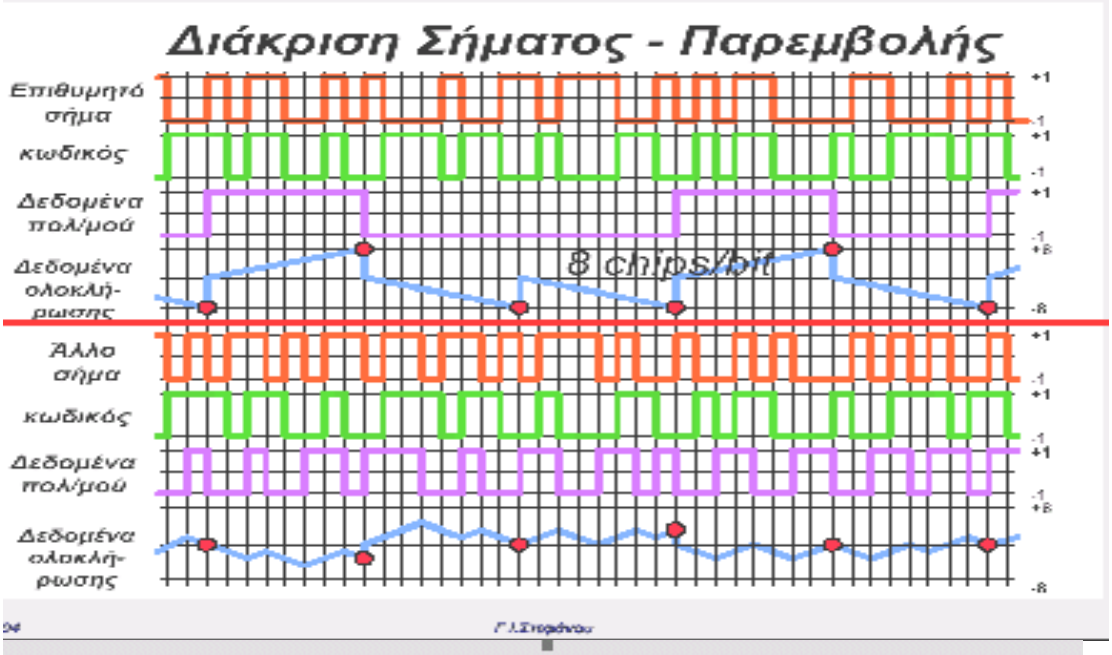
Figure 7.1 General Model of Spread Spectrum Digital Communication System

σχ.7.1Γενικό μοντέλο ψηφιακού επικοινωνιακού συστήματος διευρυμένου φάσματος

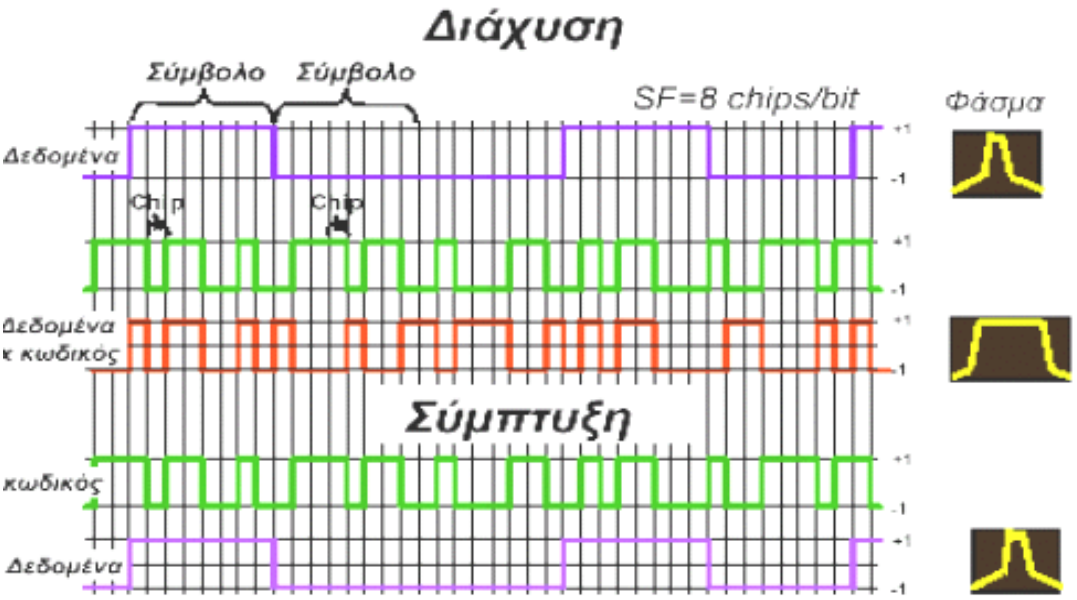


Σύμφωνος δέκτης σήματος ευθείας ακολουθίας διευρυμένου φάσματος.

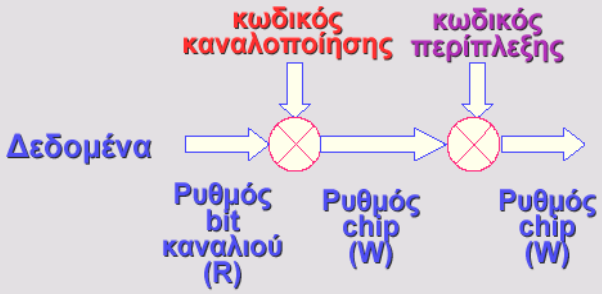
Παράδειγμα Άμεσης Ακολουθίας-Συσχετιστής (Correlator)



Παράδειγμα Άμεσης Ακολουθίας



Διάχυση Φάσματος

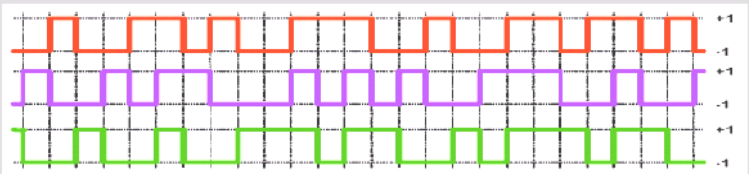


Κωδικός διάχυσης = κωδικός καναλοποίησης x κωδικός περίπλεξης

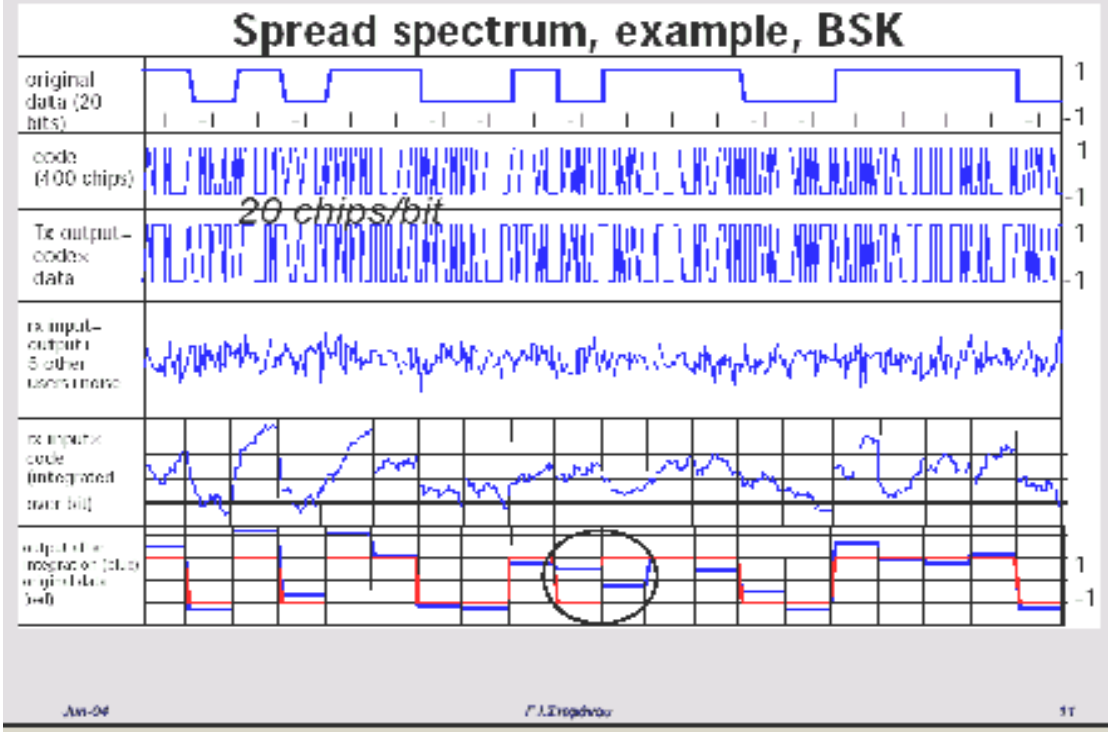
Κωδικός καναλοποίησης

Κωδικός περίπλεξης

Κωδικός διάχυσης



Τεχνική Διάχυτου Φάσματος



ΚΩΔΙΚΟΠΟΙΗΣΗ

Η θεωρία της κωδικοποίησης ή θεωρία κωδικών (coding theory) είναι ένας κλάδος των μαθηματικών ,που ασχολείται με τους τρόπους αξιόπιστης μετάδοσης των δεδομένων ,σε ενθόρυβα κανάλια επικοινωνίας. Ερευνά τους μαθηματικούς αλγόριθμους ,που ανιχνεύουν τα λάθη στην μετάδοση της πληροφορίας ,που προκαλούνται από τον θόρυβο στο κανάλι .Ο θόρυβος στο κανάλι αποτελεί την μάστιγα των επικοινωνιών και είναι γενικά ανεπιθύμητος .Ο όρος κωδικοποίηση ,χρησιμοποιείται ,χρησιμοποιείται για να περιγράψει πολλές και διαφορετικές λειτουργίες σε ένα κανάλι επικοινωνιών .Περιλαμβάνει την **κωδικοποίηση πηγής** (source coding) , όπου η πληροφορία της αναλογικής ή ψηφιακής πηγής <<συμπιέζεται>>για να γίνει η κατάλληλη εκπομπή ,με όσο το δυνατό μικρότερη σπατάλη εύρους ζώνης και ισχύος .Αναφέρεται επιπλέον και στην κωδικοποίηση καναλιού (channel coding) ,όπου προστίθεται στην πληροφορία πηγής ,επιπλέον ψηφία ελέγχου (πλεονασμός),ώστε να είναι δυνατή η ανίχνευση και η διόρθωση των σφαλμάτων ,που θα προκύψουν κατά την μετάδοση .Πρόκειται επομένως για την αντίθετη διαδικασία από αυτή της πηγής .Η μια πασχίζει για την ελάττωση του μεγέθους ,ενώ η άλλη αναζητεί έξυπνους τρόπους αύξησης .Εδώ σημαντικό ρόλο έχουν οι κώδικες έλεγχου σφάλματος (Error Control Codes ,ECC).Τέλος ο όρος κωδικοποίηση αναφέρεται και στην κωδικοποίηση διαμόρφωσης (modulation coding) ,που περιλαμβάνει τις τεχνικές ψηφιακής διαμόρφωσης των σημάτων .Ο Hamming ,θεωρείται ο μεγάλος δάσκαλος της θεωρίας των κωδικών .Αυτός σχεδίασε έναν κώδικα ,στον οποίο ,ανά τέσσερα bit μηνύματος ακολουθούσαν τρία bit ελέγχου ,με αποτέλεσμα όχι μόνο τον εντοπισμό των λαθών κατά την μετάδοση ,αλλά και τη διόρθωση τους .Τα τηλεπικοινωνιακά κανάλια θεωρούνται <<δυαδικά συμμετρικά κανάλια >>(Binary Symmetric Channel ,BSC) .Δυαδικά γιατί τα μοναδικά σύμβολα που διακινούνται είναι τα ψηφία 0 και 1 ,ενώ λέγονται συμμετρικό γιατί οι πιθανότητες εσφαλμένης λήψης κάθε συμβόλου είναι ίσες ,ανεξάρτητα από την θέση του μέσα στην ψηφιοσειρά .

Στις περισσότερες περιπτώσεις η πληροφορία μεταδίδεται σαν μια ακολουθία παλμών (0 και 1) ,που λέγονται ψηφία .Τα δυαδικά ψηφία είναι γνωστά ως δυφία ή bits(binary digits).

Μήκος μιας λέξης είναι ο αριθμός των ψηφίων που την αποτελούν .Το κανάλι που διαβιβάζει μια τέτοια πληροφορία ,ονομάζεται δυαδικό .

Για παράδειγμα ,ο κώδικας που αποτελείται από όλες τις λέξεις μήκους 2 ,είναι ο C={00,10,01,11}.Μπλοκ κώδικας είναι αυτός που όλες οι λέξεις έχουν το ίδιο μήκος .Οι λέξεις που ανήκουν σε συγκεκριμένο κώδικα λέγονται κωδικολέξεις .Βάρος μιας κωδικολέξης ονομάζεται το πλήθος εμφανίσεων του ψηφίου 1,σε αυτή .Βαθμός πληροφορίας G ενός δυαδικού κώδικα με μήκος κωδικολέξης n ,είναι η ποσότητα $G=1/n*\log_2(C)$,όπου C των κωδικολέξεων .Κάθε δυαδικός κωδικός ,με μήκος κωδικολέξης n ,περιλαμβάνει 2^n κωδικολέξεις .Άρα ισχύει $1<C<2^n$ και ο βαθμός παίρνει τιμές από 0 ως 1.Κώδικας με βαθμό πληροφορίας μεγαλύτερο από 0,8 θεωρείται πολύ καλός .

Κατά την μεταφορά μιας λέξης μέσου του δυαδικού συμμετρικού τηλεπικοινωνιακού καναλιού (BSC) ,δεν χάνονται ούτε προστίθενται ψηφία. Επομένως η κωδικολέξη θα φτάσει με το ίδιο μήκος ,αλλά λόγω των παρεμβολών να είναι διαφορετική .Για παράδειγμα ,αν ληφθεί η ψηφιοσειρά

(011011001)και ο κώδικας έχει μήκος 3 ,τότε ξέρουμε ότι λάβαμε τις εξής τρεις λέξεις : 011 , 011 , 001. Όλες οι πληροφορίες που θα λάβουμε θα πρέπει να είναι πολλαπλάσιες του 3 .Όταν λέμε κωδικοποίηση σημαίνει ότι η λέξη που ελήφθηκε θα συγκριθεί με κάποιο σύνολο λεξικό από κωδικολέξεις. .Αν από την σύγκριση δεν βρεθούν όμοια τότε έχουν υπεισέλθει λάθη ,σε διαφορετική περίπτωση αν ληφθεί γνωστή κωδικολέξη ,τότε όλα έχουν ληφθεί σωστά.(σχ.2)

Παράδειγμα

Στον κώδικα $C_{1=}$ {00,10,01,11} κάθε λέξη δυο ψηφίων είναι μια κωδικολέξη ,δεν μπορεί να ανακαλυφθεί κάποια λάθος ,αφού όλες είναι δεκτές. Στον επαναληπτικό κώδικα C_2 ={000000 , 101010 , 010101 , 111111}, κάθε κωδικολέξη του $C_{1=}$ {00,10,01,11} επαναλαμβάνεται τρεις φορές. Αν ληφθεί έστω μια λέξη που είναι λάθος όπως 110101 τότε από την σύγκριση θα φανεί ότι αυτή η κωδικολέξη δεν είναι στο σύνολο , άρα υπάρχει ένα λάθος .
(σχ.3) Αν υπάρχει ένα λάθος σε κάθε κωδικολέξη ,τότε δυο από τις 3 επαναλήψεις θα είναι σωστές .Τώρα ο βαθμός πληροφορίας μειώθηκε από 1 σε 1/3 .Αλλάζουμε το $C_{1=}$ {00,10,01,11}προσθέτοντας στο τέλος της κωδικολέξης το 0 ή το 1 , ώστε το πλήθος των ψηφίων να είναι άρτιο,
$C_{3=}${000 ,101 ,011 ,110}.Το επιπλέον ψηφίο λέγεται**<<ψηφίο έλεγχου της ισοτιμίας >> (parity check bit).** Αν ληφθεί 010, που δεν είναι κωδικολέξη τότε θα ανακαλυφθεί το λάθος .Θα γίνει μια προσπάθεια διόρθωσης του λάθους με την αλλαγή όσο των δυνατόν λιγότερων ψηφίων ,ώστε να προκύψει η σωστή κωδικολέξη .Οι κώδικες πρέπει να σχεδιάζονται με λογικούς βαθμούς πληροφορίας ,χαμηλό κόστος κωδικοποίησης και με κάποιες ικανότητες αυτοανίχνευσης και αυτοδιόρθωσης λαθών ,ώστε να μην απαιτείται επανάληψη της διαδικασίας μετάδοσης .

Με το **<<ψηφίο έλεγχου της ισοτιμίας >> (parity check bit),** (με την εισαγωγή ενός επιπλέον ψηφίου) ,ελλατώνεται επιπλέον η πιθανότητα διαβίβασης λανθασμένης λέξης .Γενικά η πιο σίγουρη μέθοδος για την μείωση των λαθών στην μετάδοση είναι η χρήση επιπλέον ψηφίων. Ο πιο απλούστερος κώδικας μετάδοσης με λίγα λάθη είναι η πολλαπλή επανάληψη. Υπάρχουν δυο βασικές τεχνικές για τον έλεγχο σφαλμάτων .

Η πρώτη τεχνική αναφέρεται σαν αίτηση αυτόματης επανάληψης (Automatic Repeat request ,ARQ) ,όπου επιτυγχάνεται ανίχνευση και όχι διόρθωση σφαλμάτων .Όταν ανιχνευτεί σφάλμα στην λήψη , η ψηφιοσειρά επαναλαμβάνεται μετά από αίτηση επανάληψη της αποστολής ,που πραγματοποιείται με την ύπαρξη σε ένα ARQ σύστημα ενός βρόγχου ανάδρασης.

Η τεχνική αυτή έχει τρεις διαφορετικές μορφές :
1)ARQ στάσης και αναμονής ,
2)ARQ υπαναχώρησης N βημάτων
και 3) ARQ επιλεκτικής επανάληψης .

Η δεύτερη τεχνική για τον έλεγχο των σφαλμάτων είναι η πρόσω διόρθωση σφάλματος (Forward Error Correction ,FEC) ,σύμφωνα με την οποία επιτυγχάνεται τόσο ανίχνευση όσο και διόρθωση των σφαλμάτων με την εισαγωγή καταλλήλων πλεοναζόντων ψηφίων ελέγχου .Με την τεχνική αυτή που λέγεται και αλγεβρική κωδικοποίηση , δεν χρειάζεται επανεκπομπή της εσφαλμένης ακολουθίας δεδομένων .

Η αλγεβρική κωδικοποίηση έχει δυο μορφές :
1)τη κωδικοποίηση σε ομάδες (block coding)
και την 2) συνελικτική κωδικοποίηση (convolutional coding) .

ΚΩΔΙΚΟΠΟΙΗΣΗ BLOCK

Η εισερχόμενη ακολουθία δεδομένων ,οργανώνονται αρχικά σε ομάδες (μπλοκ) ,που θεωρούνται ως ένα σύνολο **k** συμβόλων ,που πρέπει να οργανωθούν σε μια ανώτερη ομάδα ,που αποτελείται από **n** σύμβολα .Τ ο αποτέλεσμα είναι ότι ο αποκωδικοποιητής μπορεί να ανιχνεύει και να διορθώνει πλήρη , εσφαλμένα <<κομμάτια >> του μηνύματος όταν φτάνει στον δέκτη .Οι κώδικες λέγονται και (**k,n) αλγεβρικοί κώδικες** και χαρακτηρίζονται από τον ρυθμό τους $\mathbf{R_C}$ **=k/n.(σχ.3)** Χαμηλός ρυθμός κωδικοποίησης ,σημαίνει μεγάλος πλεονασμός ,άρα μικρότερη πιθανότητα σφάλματος .

Οι πιο γνωστοί αλγεβρικοί κώδικες είναι οι κώδικες Hamming , οι κώδικες Reed-Muller, οι κώδικες Golay, οι κυκλικοί κώδικες BCH και οι κώδικες Reed-Solomon.Οι κώδικες Reed-Solomonχρησιμοποιούνται κυρίως στα cd players, ενώ οι κυκλικοί κώδικες BCH χρησιμοποιούνται κυρίως σε πολύ κρίσιμες εφαρμογές ,όπου η επικοινωνία χωρίς λάθη είναι ζωτικής σημασίας ,όπως η ραδιοκαθοδήγηση των διηπειρωτικών βαλλιστικών πύραυλων με πυρηνικές κεφαλές ή εντολές τηλεχειρισμού των διαστημικών σκαφών ,χρησιμοποιείται ο κώδικας BCH (1023,11) ,που μπορεί να διορθώσει ένα καταπληκτικό αριθμό σφαλμάτων (255) ,αλλά χρειάζεται ένα υψηλό πλεόνασμα σε bit . (σχ8)

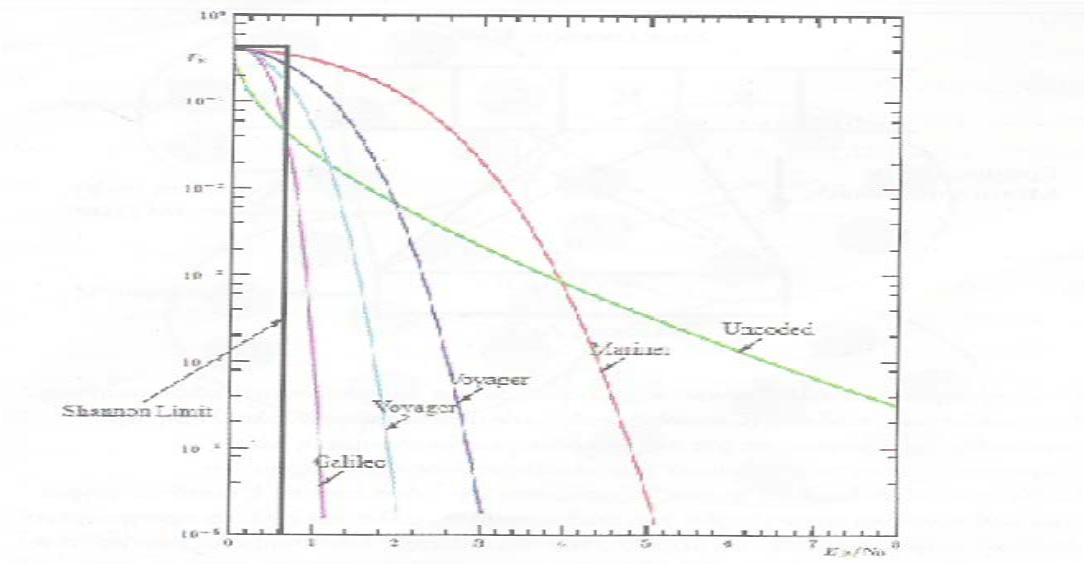
Το μπλοκ των δεδομένων εισόδου(μηχανικό ανάλογο της κωδικοποίησης)μπορούν να θεωρηθούν ως μικρά σφαιρίδια διαφορετικών διαστάσεων .Το σύστημα κωδικοποίησης δίνει διαφορετικά χρώματα στα σφαιρίδια ,ανάλογα με το μέγεθος τους και ο αποκωδικοποιητής ρυθμίζεται έτσι ώστε να ελέγχει το μέγεθος και το χρώμα των σφαιριδίων . Αν κάποιο σφαιρίδιο συγκεκριμένου μεγέθους ,έχει διαφορετικό χρώμα από το αναμενόμενο ,τότε ανίχνευσε σφάλμα και αν έχει επιπλέον πληροφορίες για τις σωστές διαστάσεις και τα αντίστοιχα χρώματα,θα μπορεί να τα διορθώσει. Αν όμως τα σφάλματα στο κανάλι είναι πολλά που να παραμορφώνουν και να αλλοιώνουν το σφαιρίδιο από διαστάσεις και από χρώμα ,και το μεταμορφώσουν σε άλλο διαφορετικό σφαιρίδιο ,τότε το σφάλμα δεν θα εντοπιστεί ,ούτε θα διορθωθεί.

Η πιο γνωστή μορφή κωδικών μπλοκ είναι του κώδικα Hamming .(σχ.4).Στο πίνακα βλέπουμε ένα κώδικα Hamming με ρυθμό 4 / 7 ,όπου τα 16 πιθανά μπλοκ εισόδου τεσσάρων bit κωδικοποιούνται και εμφανίζονται στην έξοδο ,ως μπλοκ των 7 bit.Αυτό το σύνολο των 16 μπλοκ εξόδου ,έχει επιλεγεί κατάλληλα από τους 128 (=2^{7}) δυνατούς συνδυασμούς ,ώστε να είναι οι πλέον ανόμοιοι μεταξύ τους και κάθε μπλοκ να διαφέρει από οποιοδήποτε άλλο ,κατά τουλάχιστον τρία bit.Εάν κατά την εκπομπή κάποιου από αυτά συμβούν ένα ή δυο σφάλματα ,ο ανιχνευτής θα αντιληφθεί ότι αυτό που έλαβε δεν είναι έγκυρο και θα το σημειώσει ως σφάλμα .Αν το σφάλμα είναι μόνο ένα ,ο δέκτης μπορεί να προσδιορίσει το έγκυρο μπλοκ που είναι κοντά στο εσφαλμένο και να το διορθώσει .(σχ.5).Ενώ όταν συμβούν τρία σφάλματα κατά την μετάδοση του μπλοκ ,τότε το αρχικό θα μετατραπεί σε κάποιο άλλο έγκυρο , όποτε τα σφάλματα δεν θα γίνουν αντιληπτά. Η απόσταση

HAMMING είναι μια ιδιότητα του κώδικα ,που δείχνει το πλήθος των bit ,που διαφέρουν δυο οποιοδήποτε κώδικες λέξεις (ή μπλοκ)(σχ.3) .Όσο μεγαλύτερη είναι η απόσταση αυτή ,τόσο μεγαλύτερη είναι η δυνατότητα ανίχνευσης ή διόρθωσης των εμφανιζόμενων σφαλμάτων .Ένας κώδικας μπλοκ ,με απόσταση HAMMING ίση με p,μπορεί να ανιχνεύσει ως p-1 και να διορθώσει ως (p-1)/2 σφάλματα σε κάθε μπλοκ . Όσο αυξάνεται το μήκος του κώδικα του μπλοκ προκύπτουν δυο προβλήματα που είναι 1) της καθυστέρησης και 2) της πολυπλοκότητας .Οι συνελεκτικοί κώδικες (convolutional codes) χρησιμοποιώντας το μηχανισμό του ολισθαίνοντας παραθύρου μετατρέπουν ολόκληρη την ακολουθία δεδομένων , σε μια και μοναδική κωδικοποιημένη λέξη (σχ.6).Τα κωδικοποιημένα δυαδικά ψηφία εξαρτώνται όχι μόνο από τα k δυαδικά ψηφία ,που μπαίνουν στο κωδικοποιητή , αλλά και από τα προηγούμενα δυαδικά ψηφία εισόδου .Τ ο μέγεθος του παραθύρου , που συμβολίζεται με το n ,αποτελείται από το πλαίσιο εισόδου k συμβολών , και από τον αποθηκευμένο στην μνήμη του κωδικοποιητή αριθμό συμβόλων .

Σε αντίθεση με τους κώδικες μπλοκ , οι συνελεκτικοί κώδικες (convolutional codes) εφαρμόζονται στην εισερχόμενη σειριακή ακολουθία δεδομένων , σε επίπεδο bit.Ο κωδικοποιητής έχει μνήμη και εκτελεί ένα αλγόριθμο , που χρησιμοποιεί έναν ορισμένο αριθμό από τα πλέον πρόσφατα bit , για να σχηματίσει την κωδικοποιημένη ακολουθία δεδομένων εξόδου. Η διαδικασία αποκωδικοποίησης είναι κυρίως μια σειριακή διαδικασία ,που στηρίζεται στο παρών και το προηγούμενο bit, (ή σύμβολα) , που έχουν ληφθεί και χρησιμοποιούν τις βαθμίδες αναδρομικής επεξεργασίας ,με πιο γνωστή τον αποκωδικοποιητή Viterbi. Υπάρχουν πολλών ειδών αποκωδικοποιητές όπως αυτοί της αυστηρής απόφασης ,που δεν παρέχεται στον αποκωδικοποιητή καμιά πληροφορία ,για το πόσο κοντά βρίσκεται το συγκεκριμένο σύμβολο ,στο όριο λήψης απόφασης , ενώ οι αποκωδικοποιητές χαλαρής απόφασης (soft decision decoding) ,που δίνονται στον αποκωδικοποιητή σημαντικές , παράπλευρες πληροφορίες για την εγκυρότητα των συμβόλων .Τα συστήματα αποκωδικοποίησης χαλαρής απόφασης ,έχουν μεγαλύτερη ικανότητα ανίχνευσης και διόρθωσης σφαλμάτων από αυτή της αυστηρής.Το κέρδος αποκωδικοποίησης είναι 3 db για κώδικα ίδιου μήκους .

Το μειονέκτημα που έχουν όλες οι ***μέθοδοι κωδικοποίησης*** είναι ότι αυξάνουν τον αριθμό των δεδομένων που πρέπει να μεταδοθούν και έτσι απαιτούν είτα αυξημένο εύρος ζώνης είτε μειωμένο ρυθμό εκπομπής . Υπάρχει όμως τρόπος να αντισταθμιστεί οποιαδήποτε μείωση του ρυθμού εκπομπής και αυτή είναι η αύξηση των αριθμών των καταστάσεων των συμβόλων ,κατά την διάρκεια της διαμόρφωσης κάτι που επιβαρύνει όμως το λόγο Eb /No.



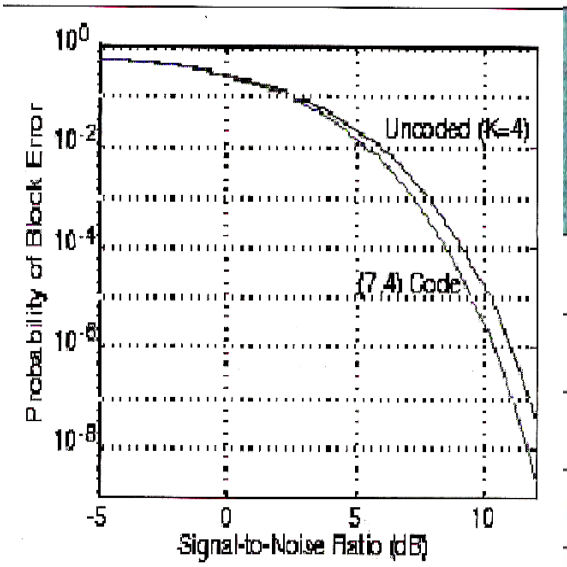
Οι αλγόριθμοι κωδικοποίησης αξιολογούνται με τη βοήθεια του διαγράμματος Εσφαλμένα bit, σε σχέση με το λόγο σήματος προς θόρυβο (ή, διαφορετικά, ενέργεια ανά bit (Eb)/στάθμη θορύβου (No). Στο διάγραμμα φαίνεται η πρόοδος που έχει επιτευχθεί από το 1960 μέχρι σήμερα. Οι πρώτες διαστημικές επικοινωνίες δεν χρησιμοποιούσαν κωδικοποίηση (πράσινη καμπύλη, uncoded). Η πρώτη αποστολή, στην οποία χρησιμοποιήθηκε κωδικοποίηση, ήταν η εξερεύνηση του Άρη από το σκάφος Mariner 6, στην οποία χρησιμοποιήθηκε κωδικοποίηση RS/Reed-Solomon (κόκκινη καμπύλη, Mariner). Στις επόμενες αποστολές των Voyager, που συνεχίζουν την επικοινωνία τους μέχρι σήμερα, που έχουν φτάσει στα όρια της ηλιόπαυσης, χρησιμοποιήθηκαν βελτιωμένοι κώδικες RS. Στη συνέχεια, αναπτύχθηκε και εφαρμόστηκε εκτενώς η κωδικοποίηση Golay, για να φτάσουμε σήμερα στην αποστολή του «Γαλιλαίου» και του Cassini, στα οποία γίνεται ευρεία χρήση των Turbo Codes.

σχ.2 ΚΩΔΙΚΕΣ HAMMING ΣΧ.3 ΑΠΟΣΤΑΣΗ HAMMING

Αριθμός ομάδων (block)	Δεδομένα block εισόδου	Δεδομένα block εξόδου
0	0000	0000+000
1	1000	1000+110
2	0100	0100+101
3	1100	1100+011
4	0010	0010+111
5	1010	1010+001
6	0110	0110+010
7	1110	1110+100
8	0001	0001+011
9	1001	1001+101
10	0101	0101+110
11	1101	1101+000
12	0011	0011+100
13	1011	1011+010
14	0111	0111+001
15	1111	1111+111

4	0010	111+0010
5	1010	001+1010
6	0110	100+0110
7	1110	010+1110
8	0001	101+0001

k	n	R = k/n
4	7	0,57
11	15	0,73
26	31	0,84
57	63	0,91
120	127	0,94
247	255	0,968
502	511	0,982

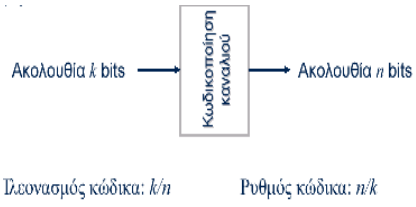


Ρυθμός ανίχνευσης εσφαλμένων bit σε ένα κώδικα Hamming (7,4). Οι καμπύλες της πιθανότητας εμφάνισης σφάλματος, για την περίπτωση της μη κωδικοποιημένης διαμόρφωσης BPSK και της BPSK κωδικοποιημένης με κώδικα Hamming (7, 4). Τα μαθηματικά που απαιτούνται για τον υπολογισμό της απόδοσης μερικών κωδίκων τέτοιας μορφής είναι εξαιρετικά πολύπλοκα και συχνά είναι δυνατός μόνον ο προσεγγιστικός προσδιορισμός. Η βελτίωση που προκύπτει μεταξύ των κωδικοποιημένων και των μη κωδικοποιημένων συστημάτων, για συγκεκριμένη τιμή της πιθανότητας εμφάνισης σφάλματος, ονομάζεται κέρδος της κωδικοποίησης (coding gain).

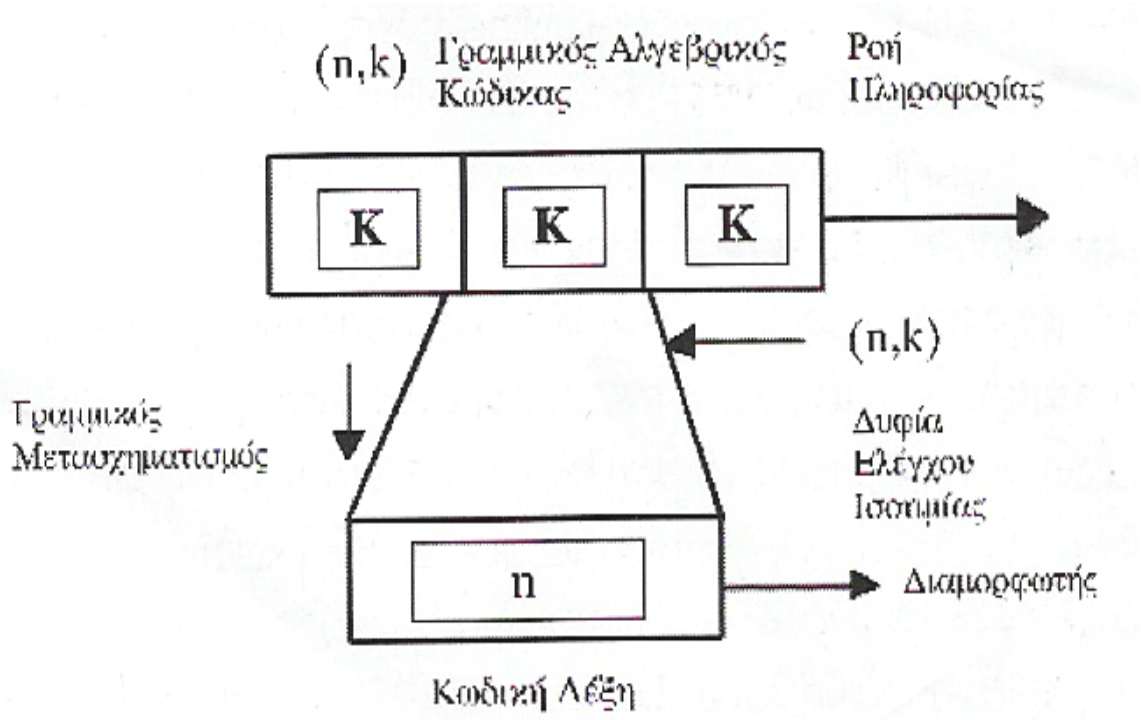
(σχ.4)

k	n	Απόδοση Κώδικα R = k/n	Είδος κώδικα	Αριθμός διορθωτέων bit
4	7	0,57	Hamming	1
5	15	0,33	BCH	3
24	63	0,84	BCH	7
64	127	0,50	BCH	10
171	255	0,0,67	BCH	11
247	255	0,968	Hamming	1
502	511	0,982	Hamming	2
11	1023	0,01	BCH	255 !

(σχ.5)

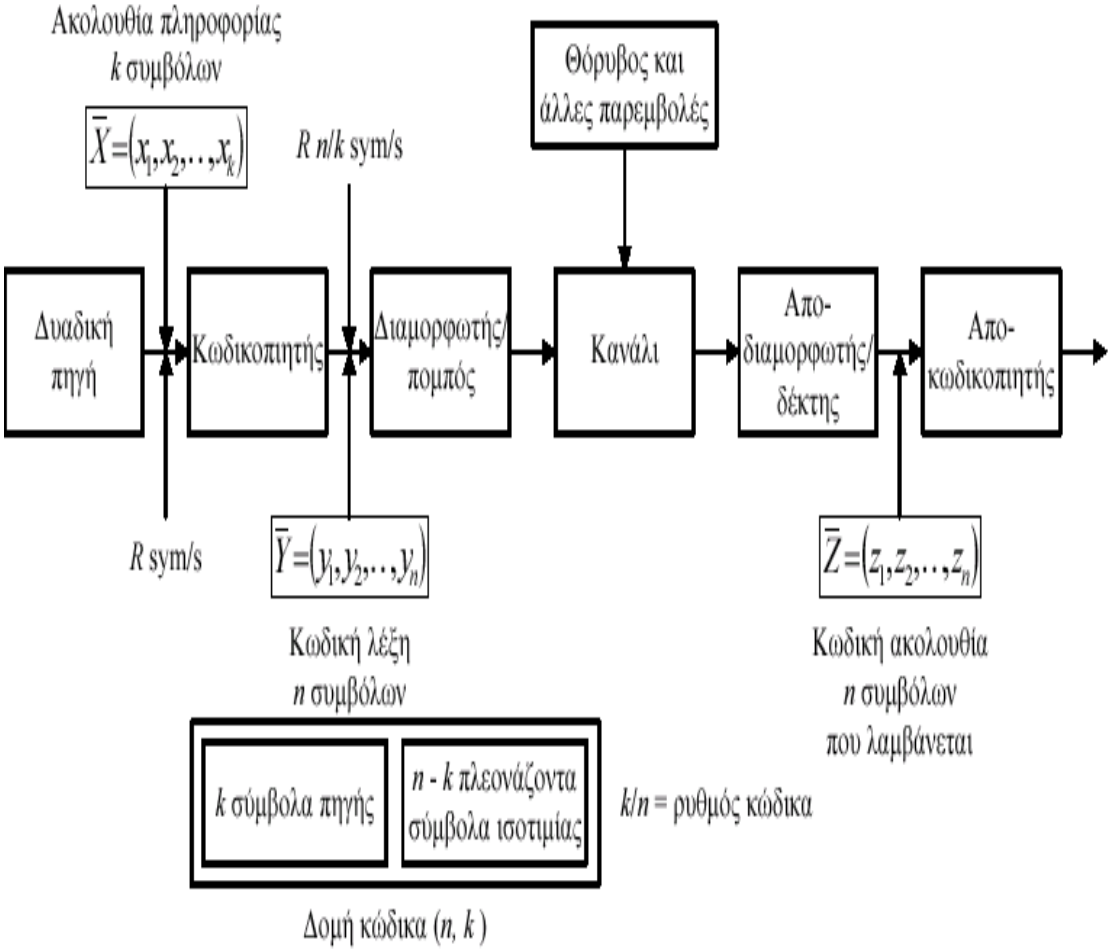


Όπως αναφέραμε παραπάνω όταν λέμε κωδικοποίηση καναλιού εννοούμε ότι εισάγουμε μια περίσσεια πληροφορία (κώδικες) για να αντιμετωπίσουμε τον θόρυβο και τις παρεμβολές στο κανάλι .Η απλούστερη μορφή κωδικοποιητή καναλιού είναι η επανάληψη κάθε bit γίνεται m φορές όπως φαίνεται στο διπλανό σχήμα .



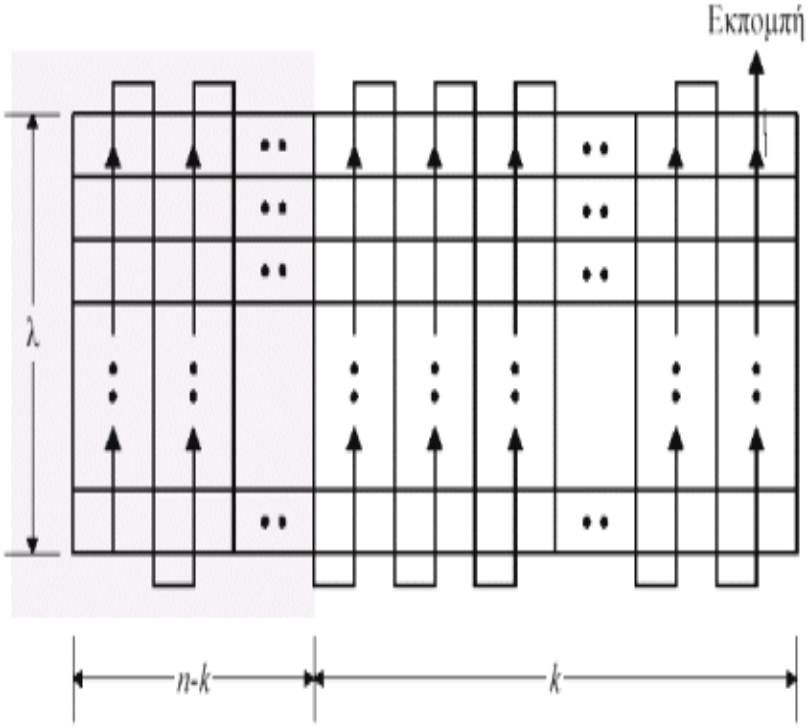
Η μέθοδος αλγεβρικής κωδικοποίησης block. Το μήνυμα χωρίζεται σε ένα πλήθος ισομηκών λέξεων, μήκους k δυφίων η καθεμία, οι οποίες προσάγονται στην είσοδο του κωδικοποιητή, που παράγει στην έξοδό του μια ομάδα (block) από n κωδικοποιημένα δυαδικά ψηφία. Προστίθενται, σύμφωνα με διάφορους κανόνες, n–k πλεονάζοντα δυαδικά ψηφία σε k δυαδικά ψηφία πληροφορίας, για να σχηματίσουν τα n κωδικοποιημένα δυαδικά ψηφία. Συνήθως, αυτοί οι κώδικες αναφέρονται ως (n, k) αλγεβρικοί κώδικες. Οι πιο γνωστοί, εν χρήσει, αλγεβρικοί κώδικες που χρησιμοποιούνται είναι οι κώδικες Hamming, οι κώδικες Golay, οι κυκλικοί κώδικες BCH και οι κυκλικοί μη-δυαδικοί κώδικες Reed-Solomon.

(σχ.6)



Κωδικοποίηση και αποκωδικοποίηση.

Το παραπάνω σχήμα δείχνει την διαδικασία της κωδικοποίησης και της αποκωδικοποίησης .



Εκπομπή κώδικα με block διαπλοκή. Κάθε κωδική λέξη έχει μήκος n σύμβολα (k bit πληροφορίας και $n - k$ πλεονάζοντα bit). Ο ορθογώνιος πίνακας περιέχει λ κωδικές λέξεις. Η παράμετρος λ ονομάζεται *βαθμός διαπλοκής*.

Το παραπάνω σχήμα δείχνει την εκπομπή κώδικα (συνελεκτικούς κώδικες) με block διαπλοκή.

ΠΑΡΑΜΕΤΡΟΙ ΚΩΔΙΚΑ BCH. Μήκος κώδικα n, αριθμός συμβόλων πληροφορίας ανά κωδική λέξη k και αριθμός διορθώσιμων σφαλμάτων e για κώδικα BCH μήκους 7 έως 255.

n	k	e	n	k	e	n	k	e	n	k	e
7	4	1									
15	11	1		10	13		8	31		115	21
	7	2		7	15	255	247	1		107	22
			127	120	1		239	2		99	23
31	26	1		113	2		231	3		91	25
	21	2		106	3		223	4		87	26
	16	3		99	4		215	5		79	27
	11	5		92	5		207	6		71	29
				85	6		199	7		63	30
63	57	1		78	7		191	8		55	31
	51	2		71	9		187	9		47	42
	45	3		64	10		179	10		45	43
	39	4		57	11		171	11		37	45
	36	5		50	13		163	12		29	47

(σχ.8)

1.β)Η τεχνική Αναπήδηση συχνότητας διευρυμένου φάσματος (Frequency Hopping Spread spectrum)

Στην τεχνολογία Αναπήδησης συχνότητας (FH) ,το σήμα μεταπηδά (hops) από κανάλι σε κανάλι μεταφέροντας μικρές <<ριπές >> της πληροφορίας σε κάθε κανάλι για καθορισμένη χρονική διάρκεια. Η εκπομπή του σήματος στο τηλεπικοινωνιακό δίκτυο δεν γίνεται με σταθερό φέρον αλλά με περιοδικές <<τυχαίες >>εναλλαγές . Αυτή η εναλλαγή συχνότητας φέροντος ονομάζεται ``*Hopping* . Είναι η πιο αποτελεσματική τεχνική EPM. Ο σκοπός της είναι να αναγκάσει του Jammer να δουλέψει σαν Barrage Jammer (μεγάλου εύρους σήμα jamming) ή σαν **Spot** Jammer(σε μικρό εύρος σήμα jamming) και να παρεμβάλλει σε όλες τις συχνότητες , με αποτέλεσμα να διασπείρει την συνολική ισχύ του σ` ένα πολύ μεγάλο εύρος ζώνης (σε κάθε περιοχή συχνοτήτων), έτσι ώστε η ισχύς ανά μονάδα συχνότητας (Watts/Hz) να ελαχιστοποιηθεί .Αν ο παρεμβολέας διασπείρει την ενέργεια του σε όλο το φάσμα συχνοτήτων ,που λειτουργεί το τηλεπικοινωνιακό σύστημα ,τότε τα συστήματα ,που λειτουργούν με τεχνολογία Αναπήδησης συχνότητας (FH) έχουν processing gain **(G_P)** ίσο με :

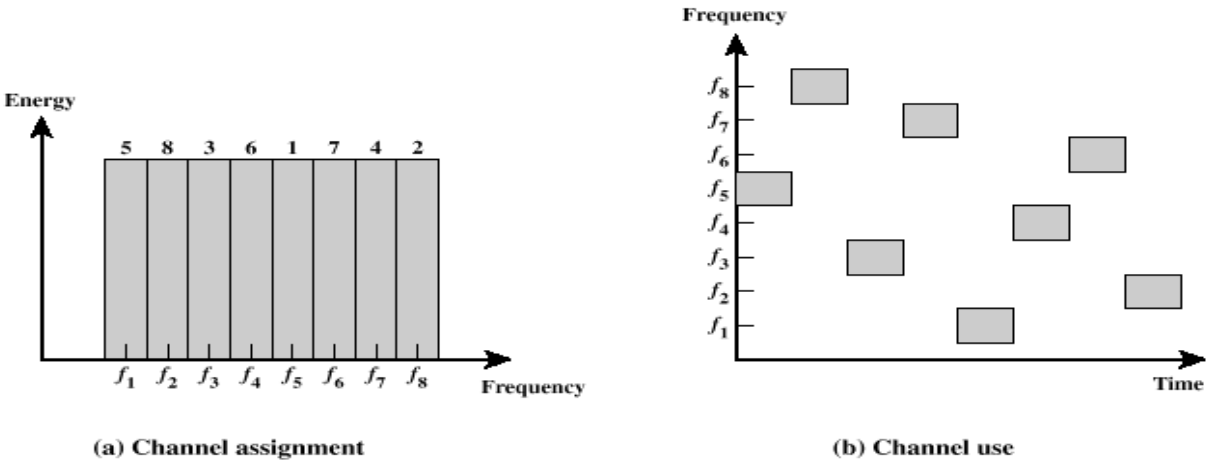
$$G_P = \frac{\beta_n}{\beta_m}$$

όπου ο β_n είναι η μπάντα συχνοτήτων πάνω στην οποία έχουμε *Hopping και ο* β_m είναι το εύρος ζώνης του μηνύματος.
Υπάρχουν δύο ειδών τρόποι αναπήδησης ,οι αργοί και οι γρήγοροι hoppers. Οι αργοί hoppers αλλάζουν τη συχνότητα τους με ένα ρυθμό από 50 έως 500 hops ανά δευτερόλεπτο . Ενώ οι γρήγοροι hoppers, που ο αριθμός των Hops είναι όσο γίνεται μεγαλύτερος και απαιτούν hop rate περίπου 10000 hops ανά δευτερόλεπτο για να προστατευτούν απέναντι στα υπερσύγχρονα fast –follower στρατιωτικά jammers. Η τεχνική των γρήγορων hoppers λέγεται ``Fast Frequency Hopping``και ο Jammer θα πρέπει να είναι πολύ ``γρήγορος``, θα πρέπει να προπορεύεται (follow-on jamming) ,ώστε να ανιχνεύσει μία στιγμιαία εκπομπή και στη συνέχεια να συνεχίσει την έρευνά του σε άλλη συχνότητα.

Όταν φτάσει στον δέκτη, συμπιέζεται η εκπομπή και επανακτάται ο αρχικός παλμός, αλλά ταυτόχρονα διασπείρεται η παρεμβολή θορύβου και έτσι μειώνεται η αποτελεσματικότητά του. .Οι ωτακουστές ακούνε μόνο ανούσια κομμάτια σήματος και κάθε προσπάθεια που γίνεται για παρεμβολή σήματος σε μια συχνότητα έχει σαν αποτέλεσμα να καταστρέψουν μόνο μερικά bit.

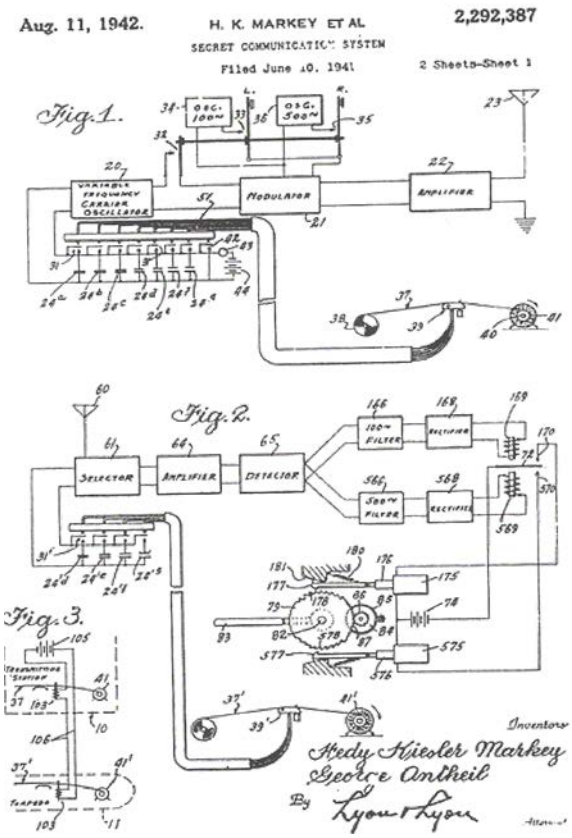
Η τεχνική της αναπήδησης συχνότητας εφευρέθηκε από την ηθοποιό HEADY LAMAR και τον μουσικό το 1941 GEORGE ANTHEIL και το σύστημα πρωτοεμφανίζεται στις μονοκάναλες επικοινωνίες VHF Αέρος και εδάφους ,το γνωστό SINCGARS –SINgle =Channel Ground & Airborne Radio ,όπου το διαμορφωμένο σήμα αναπηδά –τέλεια συγχρονισμένο σε πομπό και δέκτη – πολλαπλές φορές το δευτερόλεπτο από συχνότητα σε συχνότητα ,πετυχαίνοντας έτσι τηλεπικοινωνιακά αντίμετρα παρεμβολών ,αλλά και θωράκιση παρεμβολής .Αν και θεωρητικά η αναπήδηση της συχνότητας

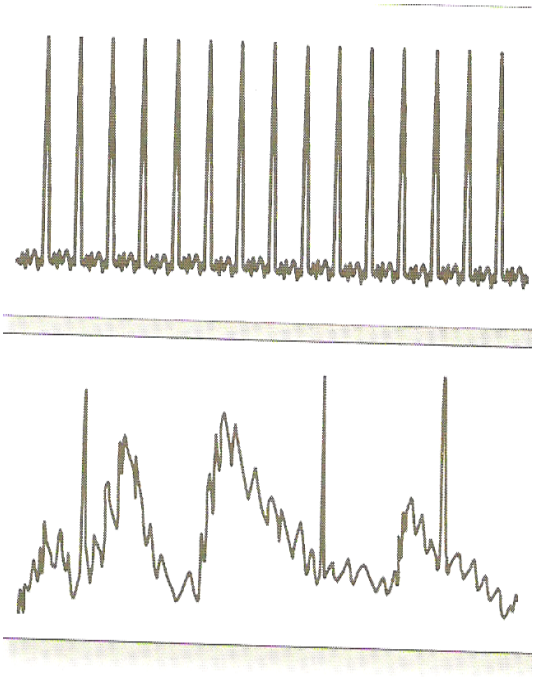
μπορεί να εφαρμοστεί σε όλο το φάσμα ,εντούτοις οι πρώτες στρατιωτικές συσκευές λειτούργησαν στα VHFκαι αργότερα στα HF , λόγω του περιοριστικού φαινομένου διάδοσης που έχουν τα HF κύματα. Ένα τηλεπικοινωνιακό δίκτυο με Frequency Hopping, περιλαμβάνει τον επίγειο σταθμό ,που τις περισσότερες φορές λέγεται ‘’Master station “ ,καθώς και τους παρελκυόμενους σταθμούς του δικτύου “Slave” ,που μπορεί να είναι κινητοί έως και φορητοί. Ο συγχρονισμός αναπήδησης στα πρώτα μοντέλα έπρεπε να είναι γνωστός και προγραμματισμένος εκ των προτέρων σε όλο το δίκτυο πομποδεκτών ,προκείμενου να υπάρξει σωστή επικοινωνία και συγχρονισμός αποκωδικοποίησης του σήματος . Αργότερα παρουσιάστηκε μια αναβαθμισμένη εφαρμογή αναπήδησης , η << Smart Hopping- Έξυπνη αναπήδηση >> ,που εκτός του ότι μπλοκάρει αυτόματα τις χρησιμοποιούμενες συχνότητες –αυξάνοντας έτσι την ταχύτητα αναπήδησης-, ταυτόχρονα έχει την δυνατότητα με το υποφέρον σήμα να αλλάξει και να ξανά προγραμματίζει τον συγχρονιστικό αλγόριθμο ανά πάσα στιγμή εξ’ αποστάσεως Επίσης κατασκευάστηκε ένας νέος ψηφιακός συνδυασμός “PSK-Phase Shift Keying – Διαμόρφωση μετατόπισης φάσης ” με “FSK-Frequency Shift Keying - Διαμόρφωση μετατόπισης συχνότητας ”.Στο πόλεμο της Βοσνίας πολλοί ραδιοερασιτεχνικοί πομποδέκτες μάρκας Icom ,Yaesu,Kenwood, χρησιμοποιήθηκαν με επιτυχία ως αντίμετρα παρεμβολών Hopping στα HF.
Η τεχνική διευρυμένου φάσματος με αναπήδηση συχνότητας στα συστήματα GSM έχει ως σκοπό τη μείωση των γρήγορων διαλείψεων που προκαλούνται λόγω της κίνησης των συνδρομητών του δικτύου .Η ακολουθία hopping μπορεί να χρησιμοποιεί ως και 64 διαφορετικές συχνότητες .Ο υποκλοπέας μπορεί να ακούσει το BCCH και να πάρει εκ των προτέρων την ακολουθία hopping ,που η ταχύτητα του στο GSM είναι περίπου 200hops /sec. Έτσι παρατηρούμε ότι η τεχνική αναπήδηση της συχνότητας στο σύστημα GSM δεν παρέχει μεγάλη προστασία ,παρόλο που γίνεται δύσκολα ο εντοπισμός του MS , γιατί ο MS στέλνει σε κάθε κανάλι και μόνο σε μια timeslot ,δηλαδή μόνο για 577 μs κάθε φορά .Η κατεύθυνση του MS μπορεί να εντοπιστεί με ακρίβεια μόνο με συσκευές που έχουν τη δυνατότητα κατευθυντικής ανίχνευσης (Directional Finder Equipment –DF) και μπορούν να προσδιορίσουν την κατεύθυνση σε χρόνο λιγότερο από 577 μs ή ακολουθώντας τη συχνότητα μεταπήδησης.



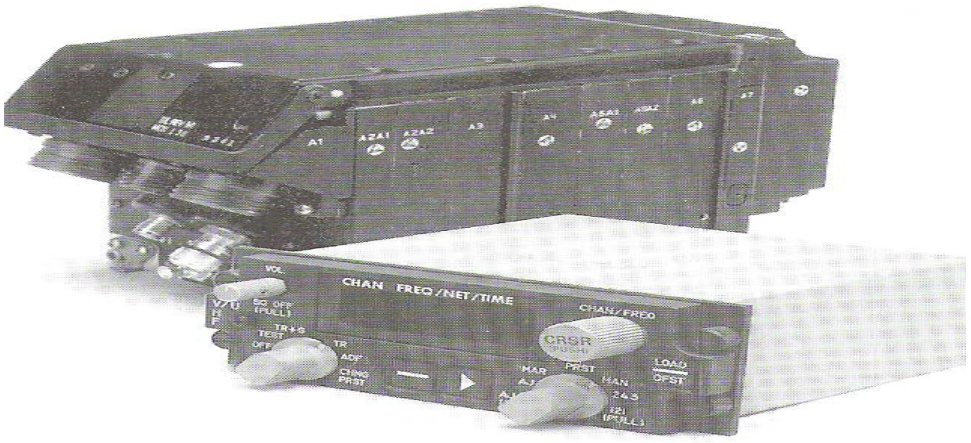
(a) Channel assignment (b) Channel use

Figure 7.2 Frequency Hopping Example





Σχήμα 1. Κυματομορφή του παλμού σήματος φωνής με ψηφιακή αναπήδηση στα HF. Σχήμα 2. Κυματομορφή του παλμού σήματος φωνής με ψηφιακή αναπήδηση στα HF/SSB χρησιμοποιώντας παλμοριπή συγχρονισμού FSK.



Μερικά από τα μοντέλα πομποδεκτών με σύστημα Hopping και Have Quick, είναι το HF-90 της εταιρείας Q-MAC, η σειρά 4400 της εταιρείας Rohde & Schwarz, το μοντέλο AN/ARC210 της γνωστής Rockwell Collins κ.π.α.

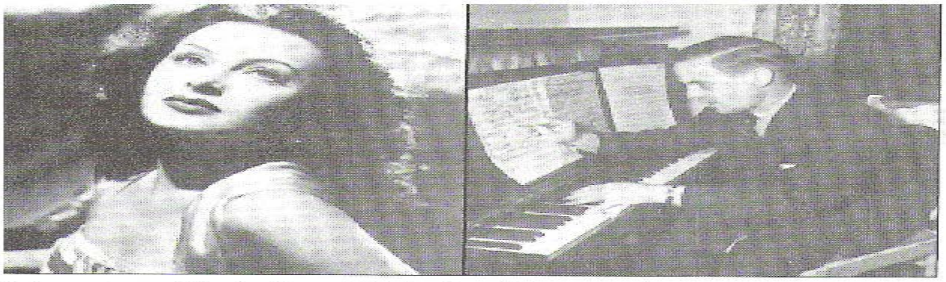
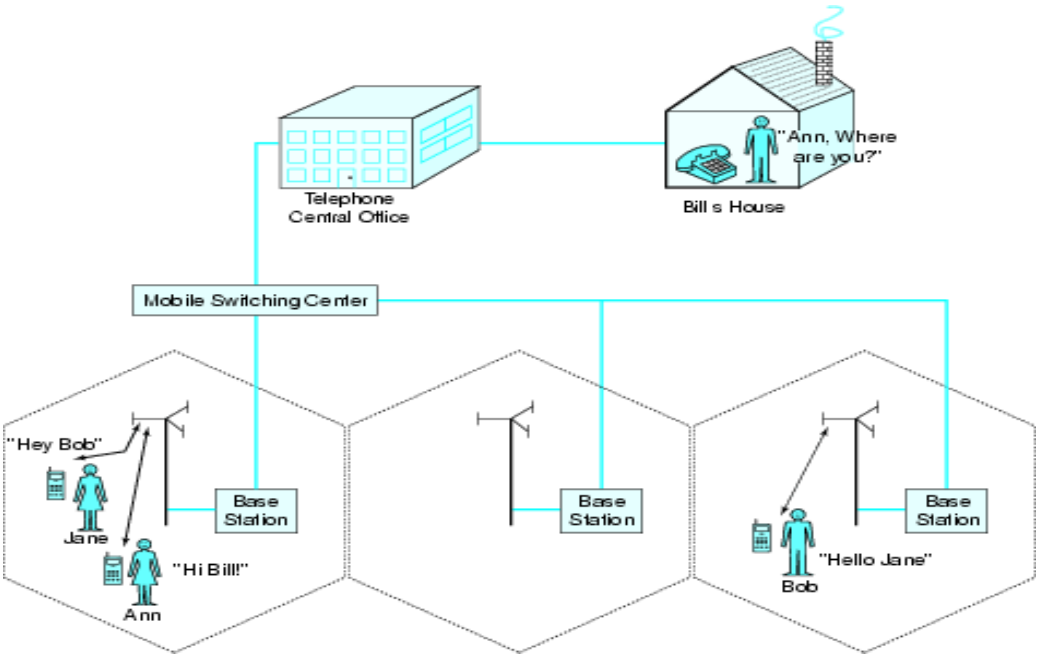


Photo courtesy: of the Academy of Motion Arts & Sciences & the Estate of George Antheil.

ΚΙΝΗΤΗ ΤΗΛΕΦΩΝΙΑ και το jamming σε αυτή

Για να ασχοληθούμε με το jamming στην κινητή ,τηλεφωνική επικοινωνία θα πρέπει να αναφερθούμε πρώτα στα χαρακτηριστικά της .Τα δίκτυα κινητής τηλεφωνίας χωρίζονται σε γεωγραφικές περιοχές που ονομάζεται κυψέλες,η καθεμιά από τις οποίες εξυπηρετείται από ένα σταθμό βάσης .(σχήμα 1) .Τα κινητά τηλέφωνα (mobile phone or cellular phone) αποτελούν τον σύνδεσμο του χρήστη με το δίκτυο με άλλα λόγια το κινητό τηλέφωνο αποτελεί το συνδυασμό τηλεφώνου του πομπού με τον δέκτη ασύρματης επικοινωνίας . Είναι έτσι σχεδιασμένο το σύστημα ώστε να εξασφαλίζει τη διατήρηση της σύνδεσης των κινητών τηλεφώνων με το δίκτυο, καθώς οι χρήστες μετακινούνται από την μια κυψέλη στην άλλη. Τα κινητά τηλέφωνα για να επικοινωνήσουν με τους σταθμούς της βάσης ανταλλάσσουν ραδιοκύματα και χρησιμοποιούν ραδιοσυχνότητες . Δίνεται η δυνατότητα τηλεφωνικής επικοινωνίας παντού και πάντα με τον ίδιο αριθμό κλήσης .
Η καινοτομία της κινητής τηλεφωνίας είναι ότι :
α)γίνεται διαχωρισμός μίας πόλης σε μικρά κύτταρα ή κυψέλες (cellular) για αυτό το σύστημα λέγεται κυψελοειδής, κυτταροειδής. Μία μεγάλη πόλη μπορεί να έχει εκατοντάδες κύτταρα
β)επιτρέπει να χρησιμοποιούνται οι ίδιες ραδιοσυχνότητες από διάφορους χρήστες σε μία πόλη και έτσι δίνεται η δυνατότητα να εξυπηρετούνται περισσότεροι χρήστες
και γ) επιτρέπει ευελιξία στην ανάπτυξη του δικτύου.
Μέσα σε κάθε κύτταρο οι ραδιοσυχνότητες είναι πάλι περιορισμένες αλλά είναι και ο χώρος περιορισμένος . Βάση της κινητής τηλεφωνίας είναι ένα δίκτυο που αποτελείται από κυψέλες και ονομάζεται κυψελοειδές ή Κυψελωτό δίκτυο τηλεφώνου (cell telephone system)Σε κάθε κυψέλη υπάρχει ένας σταθμός Βάσης (base station) που επικοινωνεί με τα κινητά τηλέφωνα στην κυψέλη του Με άλλα λόγια αντί να υπάρχει ένας μεγάλος σταθμός για μία πόλη, υπάρχουν πολλοί μικροί σταθμοί. Ένας σταθμός Βάσης αποτελείται από αρκετές κεραίες εκπομπής και λήψης, που συνήθως είναι στερεωμένες σε έναν ιστό ,από μια μονάδα ελέγχου σε ένα κτίριο με τεχνολογία ασύρματης επικοινωνίας. Οι σταθμοί Βάσης συνδέονται με ένα κέντρο με συνηθισμένα τηλεφωνικά καλώδια ,διαβιβάζουν στο κέντρο τις συνομιλίες που διενεργούνται από κάποιο κινητό τηλέφωνο στην κυψέλη τους και λαμβάνουν από το κέντρο τις συνομιλίες που πρέπει να διαβιβάσουν σε κάποιο κινητό τηλέφωνο στην κυψέλη τους . Το κέντρο μεταγωγής κινητού τηλεφώνου (Mobile Switching Center ή Mobile Telephone Switching Office - MTSO) ελέγχει όλους τους σταθμούς Βάσης και ενώνει όλες τις κλήσεις στο σταθερό σύστημα τηλεφώνου Κάθε κινητό τηλέφωνο χρησιμοποιεί 2 συχνότητες για αμφίδρομη επικοινωνία . Υπάρχουν 832 ραδιοσυχνότητες για μία πόλη: 790 για φωνή και 42 για δεδομένα δηλαδή υπάρχουν 395 κανάλια συνομιλίας .Το ραδιοσήμα του σταθμού Βάσης δεν είναι υπερβολικά ισχυρό για να μην δημιουργεί παρεμβολές στα σήματα της επόμενης κυψέλης.
Κάθε κυψέλη έχει 6 γείτονες .Στα αναλογικά συστήματα κάθε κυψέλη έχει 395 / 7 = 56 κανάλια ενώ στα ψηφιακά συστήματα κάθε κυψέλη έχει 168 κανάλια .

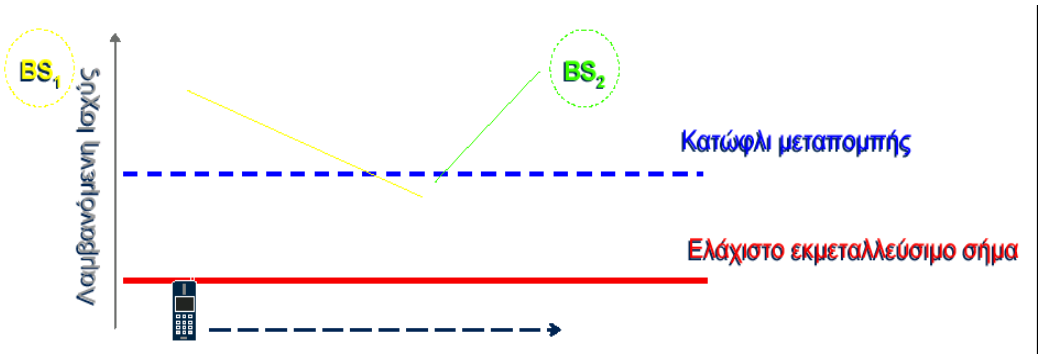
Το μέγεθος της κυψέλης ορίζεται από τον αναμενόμενο αριθμό χρηστών κινητών τηλεφώνων και καθορίζεται κατά το σχεδιασμό του δικτύου. Τυπικό μέγεθος της κυψέλης στις ΗΠΑ είναι 26 km^2 ενώ εδώ στην Ευρώπη μπορεί να είναι 1 έως 4 km^2 ή και μικρότερο στο κέντρο κάποιας μεγαλούπολης
Αν κάποιο κινητό τηλέφωνο απομακρυνθεί από την κυψέλη, τότε η σύνδεση μεταβιβάζεται αυτόματα στην επόμενη κυψέλη. Αν σε κάποια κυψέλη χρησιμοποιούνται όλο και περισσότερα κινητά τηλέφωνα τότε έχουμε υπερφόρτωση του σταθμού Βάσης .Για να αποφευχθεί αυτό μπορεί να γίνει υποδιαίρεση της κυψέλης δηλαδή εγκαθίστανται αναγκαστικά πρόσθετοι σταθμοί Βάσης που με μικρότερη ισχύ εκπομπής εξυπηρετούν τις μικρότερες κυψέλες τους και έτσι έχουμε ευελιξία στην δομή και λειτουργία της κινητής τηλεφωνίας .Το κινητό τηλέφωνο χρησιμοποιεί κωδικούς για να επικοινωνήσει και να λάβει κλήσεις αυτοί είναι α) ο Electronic Serial Number (ESN) που είναι ο προγραμματισμένος αριθμός (32 bits) από την κατασκευάστρια βιομηχανία β) ο Mobile Identification Number (MIN) που είναι αριθμός (10 bits) που βασίζεται στον αριθμό τηλεφώνου του κινητού και γ) ο System Identification Number (SID) που είναι μοναδικός αριθμός (5 bits) και καθορίζεται σε κάθε φορέα της κινητής τηλεφωνίας . Όταν ένας χρήστης ανάψει το κινητό του, το τηλέφωνο πρώτα λαμβάνει ένα SID από τον σταθμό Βάσης σε μία ειδική συχνότητα (control channel) . Αν το κινητό δεν βρίσκει το control channel τότε είναι out of range και γράφει το μήνυμα “no service” , ενώ αν λάβει το SID τότε το συγκρίνει με το SID που έχει προγραμματισμένο και αν ταιριάζει ξέρει ότι επικοινωνεί με το δικό του σύστημα (home system). Διαφορετικά ξέρει ότι κάνει περιαγωγή (roaming) δηλαδή ότι χρησιμοποιεί ένα διαφορετικό σύστημα από εκείνο στο οποίο ο χρήστης έχει συνδρομή . Μαζί με το SID το κινητό στέλλει και ένα “registration request” το οποίο φυλάγεται σε βάση δεδομένων στο MTSO για να εντοπισμό του κινητό όταν καλείται από άλλα τηλέφωνα . Όταν το κινητό ενός χρήστη καλείται τότε το MTSO λαμβάνει την κλήση και πρώτα εντοπίζει το κινητό και μετά το MTSO διαλέγει τις 2 συχνότητες για την κλήση και τις στέλλει στο κινητό μέσω του control channel. Όταν το κινητό και ο σταθμός Βάσης αλλάξουν σε αυτές τις συχνότητες, τότε η κλήση ενώνεται και μπορεί να γίνει η συνομιλία .Όταν ο χρήστης κινείται προς την άκρη της κυψέλης του ο σταθμός Βάσης αντιλαμβάνεται ότι η ισχύς του σήματος του κινητού ελαττώνεται ενώ ταυτόχρονα οι γειτονικοί σταθμοί της Βάσης αντιλαμβάνονται ότι ο χρήστης κινείται προς την κυψέλη τους από την αύξηση της ισχύς του σήματος. Σε κάποια στιγμή, σε συνεργασία με το MTSO ο ένας σταθμός Βάσης δίνει (hands off) την κλήση στον άλλο σταθμό και το κινητό λαμβάνει νέες συχνότητες μέσω του control channel για να αλλάξει κυψέλη. Αυτή η διαδικασία όπου το δίκτυο μεταφέρει την κλήση από ένα σταθμό σε άλλον κατά την διάρκεια της μετακίνησης και της συνομιλίας λέγεται μεταβίβαση ή μεταπομπή (handover) και συμβαίνει αδιάλειπτα ,χωρίς να αντιληφθεί την αλλαγή ο χρήστης του κινητού που συνομιλεί. (σχήμα 1)



(σχήμα 1.Το σύστημα λειτουργίας ενός κυψελωτού δικτύου κινητής τηλεφωνίας .)

Το GSM είναι σχεδιασμένο ώστε να αντιστέκεται σε ξαφνικές διακοπές που γίνονται στο κανάλι κίνησης (Traffic Channel –TCH) και προκαλούνται εξαιτίας των απωλειών από μεγάλα αντικείμενα ,όπως τούνελ κτλ. Ή αν κατά την διάρκεια της συνομιλίας όταν ο χρήστης αποσυνδέσει την μπαταρία .
Μια άλλη κυψέλη θα μπορούσε να συνεχίσει την επικοινωνία αν ο αρχικός σταθμός BTS χάσει την επαφή του με το MS . Η σχεδίαση του GSM προβλέπει δύο λύσεις:1) τη μεταπομπή (handover),που αναφέραμε παραπάνω , χρησιμοποιείται όταν η σύνδεση μπορεί να επανέλθει και εξαρτάται από την ποιότητα της μετάδοσης και τις μετρήσεις των λαμβανόμενων σημάτων από τον MS και των BTS .2) τη αποκατάσταση κλήσης ,όταν η αρχική σύνδεση έχει χαθεί ολοκληρωτικά. Η μεταπομπή είναι η διαδικασία μιας κλήσης από την δικαιοδοσία ενός σταθμού βάσης στην δικαιοδοσία ενός άλλου , έχει προτεραιότητα ως προς τις νέες κλήσεις και πρέπει να εκτελείται όσο το δυνατόν πιο σπάνια .Η μεταπομπή ξεκινά όταν η ισχύς του λαμβανόμενου σήματος πέσει σε μια προκαθορισμένη τιμή πάνω από το ελάχιστο σήμα λήψης . Η ισχύς μεταπομπής είναι ίση με την εκμεταλλεύσιμη ισχύ και το δ . Η εκμεταλλεύσιμη ισχύ είναι ίση με –90 με –100 dBm όπου το dBm είναι μονάδα μέτρησης και είναι ίση με 10 log 10 (C /1m W).Αν το δ :

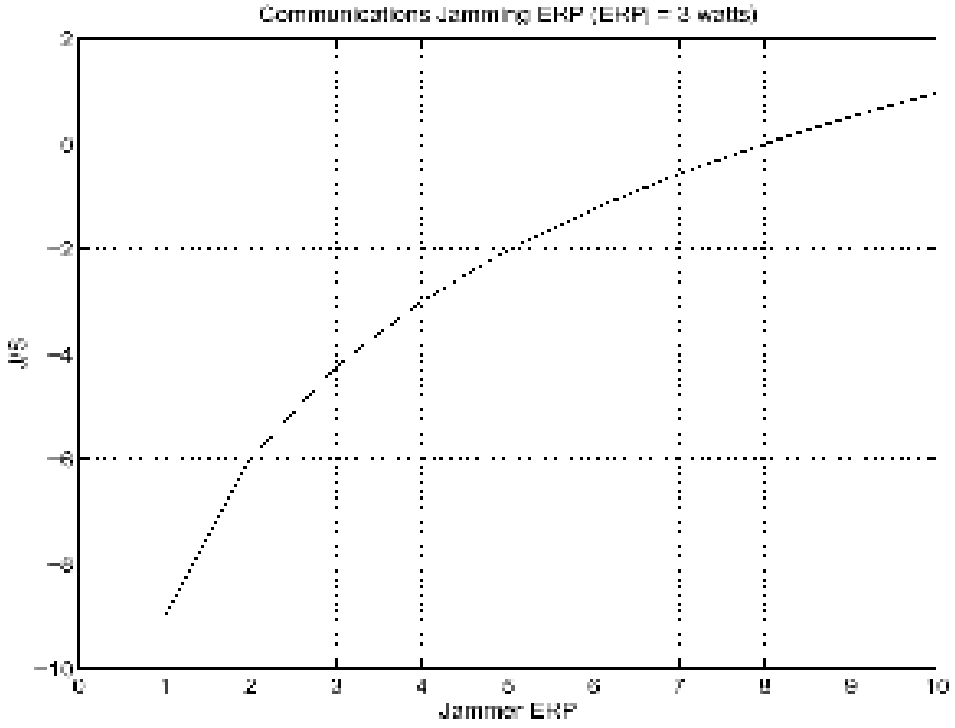
1. είναι πολύ μεγάλο τότε υπάρχει ο κίνδυνος μη αναγκαίας μεταπομπής,
2. ενώ αν το δ είναι πολύ μικρό τότε υπάρχει κίνδυνος απώλειας της κλήσης .(σχήμα 2).



(σχήμα 2. Διαδικασία μεταπομπής)

Στην μεταπομπή θα πρέπει να εξασφαλιστεί ότι πτώση του σήματος δεν οφείλεται σε διαλείψεις , διακοπές ,για αυτό υπάρχει ανάγκη διαρκούς παρακολούθησης της ισχύος .Στα συστήματα 1ης γενιάς ,κάθε BS παρακολουθούσε την ισχύ όλων των κινητών (MS) . Εκτός από την παρακολούθηση της ένδειξης έντασης του ραδιοσήματος (RSSI) [Radio Signal Strength Indication : RSSI] των κλήσεων που είναι σε εξέλιξη , ένας δέκτης εντοπισμού παρακολουθούσε την ένταση του σήματος στις γειτονικές κυψέλες .Όλη αυτή η πληροφορία διοχετευόταν στο MSC ,που αποφάσιζε για το πότε θα γίνει μεταπομπή. Στα συστήματα 2ης γενιάς έχουμε μεταπομπή υποβοηθούμενη από το κινητό (Mobile Assisted Hand-Off –MAHO).Εδώ το κινητό μετρά την ισχύ του BS και η μεταπομπή γίνεται όταν ο γειτονικός σταθμός BS είναι ισχυρότερος . Αυτή η κατανεμημένη λειτουργία βοηθά στην απλοποίηση της δομής του MSC.Όταν το κινητό κινείται μεταξύ κυψελοειδών συστημάτων τότε προκύπτουν θέματα περιαγωγής (roaming) και συμβατότητας .Για να εξασφαλιστούν διαθέσιμα κανάλια υπάρχουν 1) κανάλια ασφαλείας (Guard Channels) ,που είναι εφεδρικά μόνο για μεταπομπές και 2) Ουρά αναμονής (Queuing) όπου το περιθώριο σχεδίασης δ είναι αρκετά μεγάλο έτσι ώστε να υπάρχει αρκετός χρόνος μετά την αίτηση μεταπομπή πριν χαθεί το σήμα .Η μεταπομπή της 1ης γενιάς είχε διάρκεια 10 seconds και το δ ήταν περίπου ίσο με 6-10 dB.Η μεταπομπή της 2ης γενιάς (GSM) υποβοηθούμενη από το κινητό είναι ταχύτερη και είναι 1-2 seconds ενώ το δ είναι ίσο περίπου με 6dB .Σε όλα τα πιο πάνω παραδείγματα έχουμε <<σκληρή μεταπομπή >> (hard handoff).Ενώ η μαλακή μεταπομπή (soft handoff)είναι μια ιδιαιτερότητα του CDMA .Επιτρέπει στον ισχυρό BS να χειριστεί μια κλήση . Όλοι οι BS χρησιμοποιούν τις ίδιες συχνότητες ,απλά με διαφορετικούς κώδικες .(ΒΟΥΓΙΟΥΚΑΣ ,ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΕΠΙΚΟΙΝΩΝΙΩΝ)
Συνήθως όταν γίνεται jamming το δίκτυο θα χρησιμοποιήσει την διαδικασία της αποκατάστασης της κλήσης .
Θα πρέπει να αναφέρουμε ενημερωτικά ότι το ύψος της αντένας (κεραίας) υπολογίζεται με βάση το εμβαδών της κυψελίδας, όσο πιο μεγάλη είναι η κυψελίδα τόσο πιο ψιλά θα μπει και η αντένα. Δεν βάζουμε όλες τις αντένες ψιλά για να μην φτάνει το σήμα από μια κυψελίδα σε μια άλλη, η οποία να μην είναι γειτονική της και επομένως να υπάρχει περίπτωση να χρησιμοποιούν την ίδια συχνότητα.
Επειδή όμως οι κεραίες των σταθμών βάσης είναι συνήθως σε ψηλά μέρη, jamming γίνεται πιο εύκολα στο downlink από ότι στο uplink . Είναι πιο οικονομικό στο jammer να εξουδετερώσει την σχετικά μικρή ισχύ εξόδου του MS.Αν θέλει να μπλοκάρει έναν MS,πρέπει να διακρίνει πιο σήμα έρχεται από αυτόν και να τον μπλοκάρει . Αν χρησιμοποιεί την τεχνική της μεταπήδησης

της συχνότητας, θα πρέπει να μπορεί να ακολουθήσει την συχνότητα εκπομπής του MS , να είναι πιο γρήγορος και να εκπέμπει σήμα με μεγαλύτερη ισχύ .Το uplink jamming εμποδίζεται στο TCH εμποδίζεται από τις μεταβάσεις και την αποκατάσταση της κλήσης . Για να έχουμε πιθανότητα μετάβασης θα πρέπει πέρα από TCH , θα πρέπει όλα τα κανάλια ελέγχου RACH όλων των BTS στην περιοχή να μπλοκαριστούν για ορισμένο χρονικό διάστημα με μεγαλύτερη ισχύ από αυτή του σήματος , για να διακοπεί η μετάδοση . Μια υπάρχουσα κλήση μπορεί να διακοπεί με μερικά λεπτά αποτελεσματικού jamming.
Μια άλλη εκδοχή είναι ο jammer να στοχεύει τα RACH κανάλια ελέγχου .Με αυτόν τον τρόπο θα εμπόδιζε όλους τους MS να ζητούν οποιαδήποτε υπηρεσία από την συγκεκριμένη κυψέλη .Αλλά σε ορισμένες περιπτώσεις είναι αναποτελεσματικός επειδή δεν διακόπτει τις ενεργές κλήσεις.
Στο παρακάτω σχήμα φαίνεται η απαιτούμενη ισχύ για RACH jamming.



σχημα. Παράδειγμα αποτελεσματικότητας του RACH jamming υπολογισμένο με την παρακάτω εξίσωση

$$\frac{J}{S} = \frac{P_j G_{jr} G_{rj} R^2_{tr} L_r B_r}{P_t G_{tr} G_{rt} R^2_{jr} L_j B_j}$$

Το κέρδος της κεραίας προς το MS και τον jammer είναι 12 dBi .Το κέρδος της κεραίας είναι 12 dBi. Ο MS έχει μέγιστη ισχύ εξόδου 2 W .Η απόσταση jammer- BTS είναι διπλάσια από την απόσταση MS- BTS. Καθώς ο απαραίτητος λόγος J/ S για GSM jamming είναι –5 dBi η απαραίτητη ERP (οριζόντιος άξονας) φαίνεται από το γράφημα (2,5 W)
[Γ',9]

Η τυχαία πρόσβαση GSM RACH γίνεται ως εξής :όταν δεν δοθεί απάντηση σε ένα αίτημα , τότε ο MS θα επαναλάβει το αίτημα του μετά από κάποιο χρονικό διάστημα. Ο μέγιστος αριθμός των επαναλήψεων και ο χρόνος μεταξύ τους γνωστοποιείται στο BCCH.Εφόσον ο MS δεν εξυπηρετηθεί από το RACH μπορεί να ζητήσει υπηρεσία από κάποια άλλη κυψέλη. Για το λόγο αυτό τα RACH κανάλια όλων των BTS στην περιοχή πρέπει να μπλοκαριστούν .
Από την αρχιτεκτονική των καναλιών στο GSM παρατηρούμε ότι τα Control Channels (FCCH , SCH και BCCH) στο downlink θα πρέπει να είναι στόχος αν η ύπαρξη μιας κυψέλης πρέπει να κρυφτεί από το jamming . Αυτά τα κανάλια είναι εύκολο να αναγνωριστούν και να χρησιμοποιήσουν μια σταθερή ισχύ εξόδου. Μπλοκάροντας τις πληροφορίες συγχρονισμού είναι δυνατό να εμποδίσουμε τον MS να αναγνωρίσει ένα δίκτυο GSM.
Το GSM έχει ένα χαρακτηριστικό που διευκολύνει περισσότερο το jamming: το σύστημα ανατροφοδοτεί το jammer για την αποτελεσματικότητα του αυξάνοντας γρήγορα την ισχύ των καναλιών όταν το jamming είναι επιτυχημένο , κάτι που είναι πιο εύκολο για έναν έξυπνο jammer να βελτιώσει τη χρήση της ισχύς του .Συνήθως η αποτελεσματικότητα μιας επίθεσης jamming είναι δύσκολο να καθοριστεί και αφήνει αμφιβολίες στο jammer .
Μια αποτελεσματική επίθεση jamming στο GSM (άρνηση εξυπηρέτησης υπηρεσίας) ,που στηρίζεται σε κυκλώματα μεταγωγής φωνητικών επικοινωνιών ,θεωρείται και αν ένα τηλεφώνημα διακόπτεται κάθε 5 δευτερόλεπτα .Ολοκληρωτική άρνηση εξυπηρέτηση υπηρεσίας (DOS) έχουμε αν ο MS δεν μπορούσε να ζητήσει καμιά υπηρεσία ,ούτε sms .
Το GSM έχει ένα πολύ αποδοτικό interleaving και forward error correction (FEC). Η διασύνδεση GSM είναι ανθεκτική στην παρεμβολή (interference) συγκρινόμενη με τα άλλα δίκτυα κινητών επικοινωνιών και αυτή εξαρτάται σε μεγάλο βαθμό από την αρχιτεκτονική των καναλιών του. Τα κανάλια είναι εύκολο να απομονωθούν και να υποστούν jamming. Για να μπλοκαριστεί η λήψη ενός MS είναι δύσκολο γιατί δεν εντοπίζεται εύκολα η θέση του και για αυτό οι επιθέσεις jamming θα πρέπει να επικεντρωθούν στο uplink και κυρίως στο RACH κανάλια ελέγχου στο uplink . Καθώς οι BTS βρίσκονται σε υψηλά σημεία , το jamming στα uplink είναι ο καλύτερος τρόπος για το GSM.
Υπάρχουσες συνδέσεις μπορούν να διακοπούν μπλοκάροντας τα Traffic Channels (TCH) που χρησιμοποιούνται από την σύνδεση και μπλοκάροντας επίσης Random Access Channels (RACH) όλων των άλλων κελιών στην περιοχή . Αυτό θα αποτρέψει το σύστημα από την αποκατάσταση της κλήσης μέσω άλλων BS . Αυτού του είδους jamming πρέπει να διατηρηθεί μέχρι το δίκτυο να σταματήσει την προσπάθεια για αποκατάσταση της χαμένης σύνδεσης και αυτό χρειάζεται μερικά δευτερόλεπτα .Τα αποτελέσματα του jamming μπορούν να ελαττωθούν χρησιμοποιώντας κατευθυντικές κεραίες στους BTS.Το μέγεθος των κυψελών πρέπει να είναι όσο γίνεται μικρότερο για να γίνει χρήση της μέγιστης ισχύος της συσκευής του MS και με αυτό τον τρόπο να αυξηθεί ο αριθμός των πιθανών κελιών αποκατάστασης κλήσεων .
Επίσης τα τηλέφωνα GSM πρέπει να έχουν κατευθυντικές κεραίες ,αλλά αυτό θα επιδρούσε αρνητικά στην ευκινησία τους . Η τεχνική αναπήδηση της συχνότητας στο GSM είναι πολύ αργή για να μειώσει τις επιδράσεις του jamming.

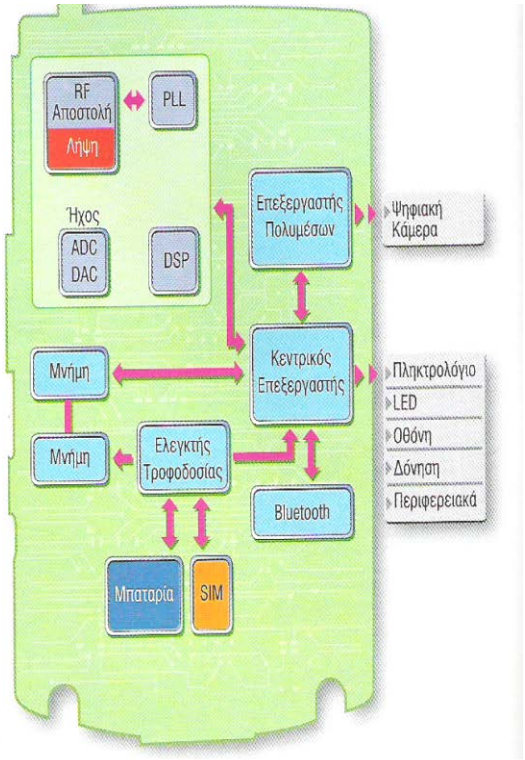
ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΚΙΝΗΤΟΥ ΤΗΛΕΦΩΝΟΥ/SMARTPHONE

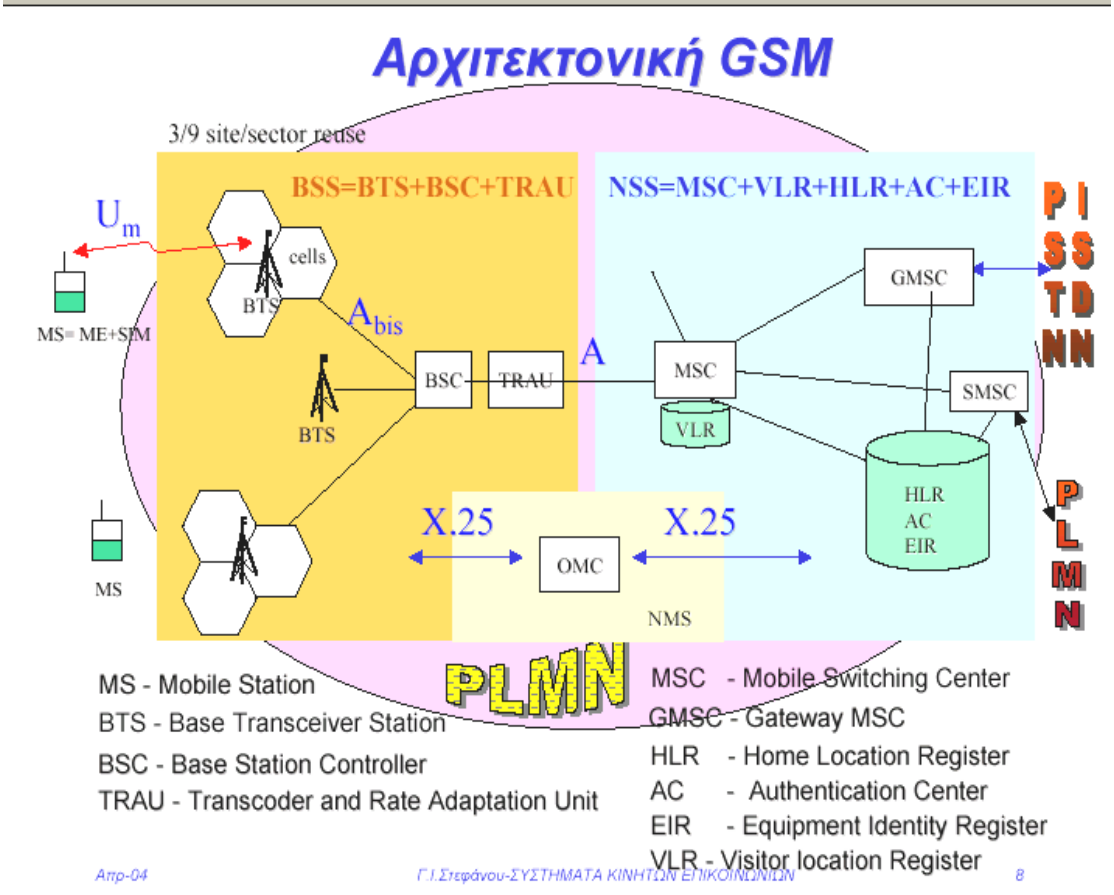
Ένα κινητό τηλέφωνο/Smartphone αποτελείται στην ουσία από τρία ολοκληρωμένα κυκλώματα. Το κέντρο είναι ο επεξεργαστής, ο οποίος ενσωματώνει τους ελεγκτές για τη μνήμη, το πληκτρολόγιο, την οθόνη, τα LED, τις διάφορες θύρες, το Bluetooth και τα περιφερειακά. Επίσης αναλαμβάνει την εκτέλεση των εφαρμογών (Java κ.ά.) και του λογισμικού ελέγχου της συσκευής το οποίο είναι μόνιμα αποθηκευμένο στη μνήμη Flash. Ακόμα είναι υπεύθυνος για την επικοινωνία με το δίκτυο GSM , για τον καθορισμό των ραδιοσυχνοτήτων και των σημάτων ελέγχου, ενώ ασχολείται και με την οργάνωση όλων των υπόλοιπων ολοκληρωμένων. Τα ολοκληρωμένα κυκλώματα ασύρματης επικοινωνίας (RF) είναι υπεύθυνα για την αποστολή και τη λήψη των ραδιοκυμάτων, ενώ εκεί πραγματοποιούνται οι μετατροπές της φωνής από αναλογική μορφή σε ψηφιακή και το αντίστροφο. Ο ισχυρός επεξεργαστής ψηφιακού σήματος (DSP) αναλαμβάνει διάφορες ειδικευμένες εργασίες αναφορικά με την επικοινωνία του κινητού με τον έξω κόσμο.

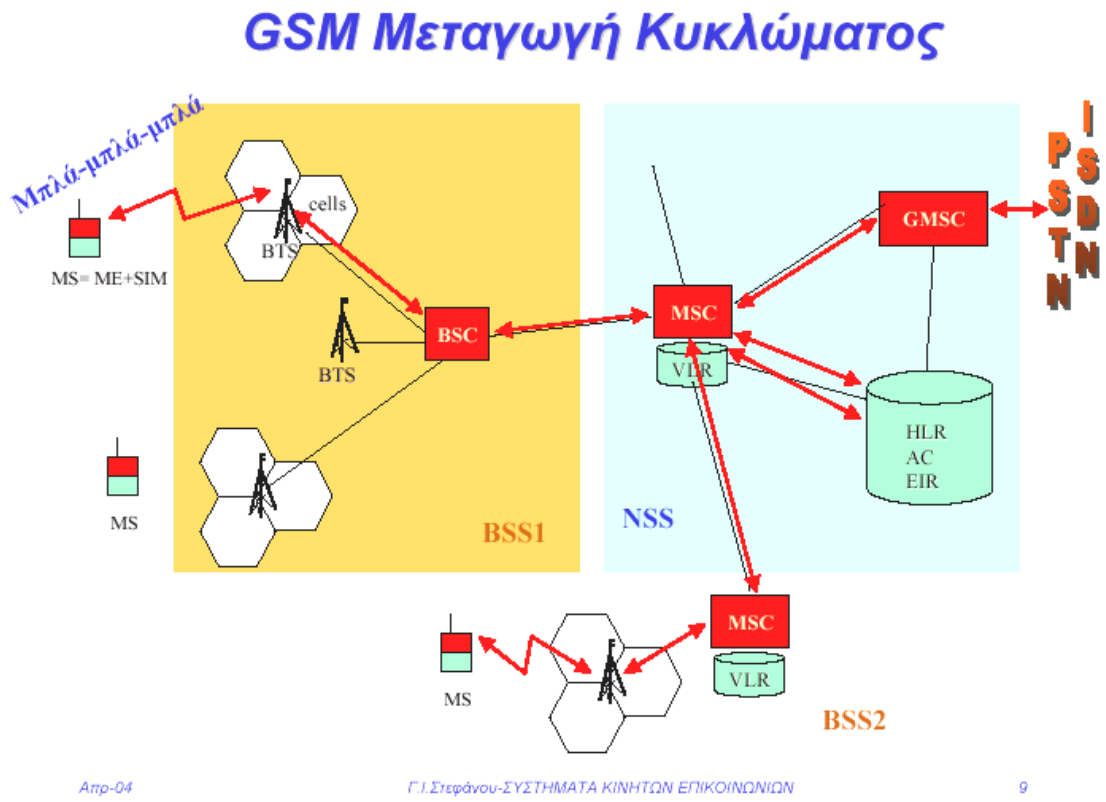
Τέλος το ολοκληρωμένο κύκλωμα τροφοδοσίας ασχολείται με την σωστή τροφοδοσία ρεύματος από τις μπαταρίες στα διάφορα μέρη του κινητού τηλεφώνου.

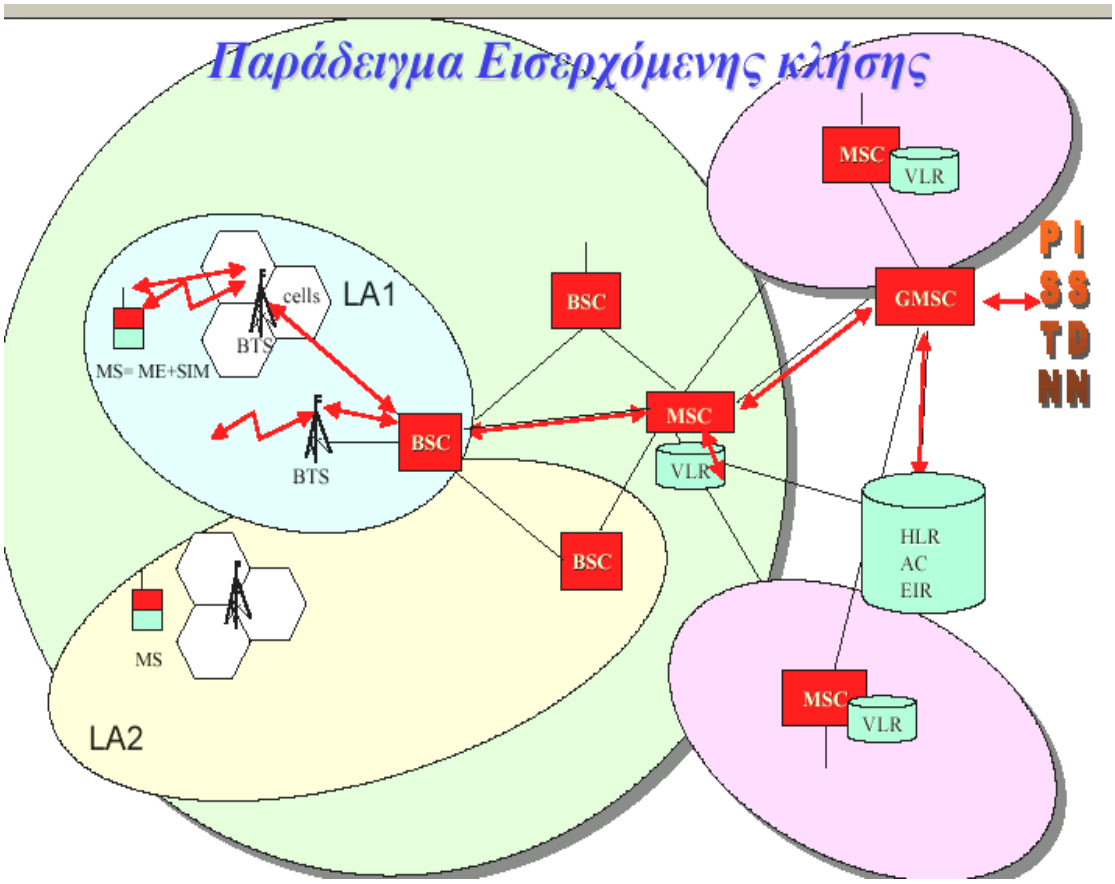
Στη σχεδίαση Smartphone συνήθως ο κεντρικός επεξεργαστής έχει μεγαλύτερη ισχύ από τα «απλά» κινητά τηλέφωνα ενώ δέχεται σημαντική βοήθεια από τον επεξεργαστή πολυμέσων σε ό,τι αφορά τα γραφικά, τη διαχείριση video, τον έλεγχο της ψηφιακής κάμερα κ.ά. Επιπλέον, το λογισμικό ελέγχου έχει περισσότερες δυνατότητες από τα «απλά» κινητά τηλέφωνα.

Η σχεδίαση Smartphone τείνει να γίνει το πρότυπο των κινητών του κοντινού μέλλοντος, ενώ είναι πιθανόν να υπάρχουν μικρές διαφοροποιήσεις στη σχεδίαση του εκάστοτε κατασκευαστή.

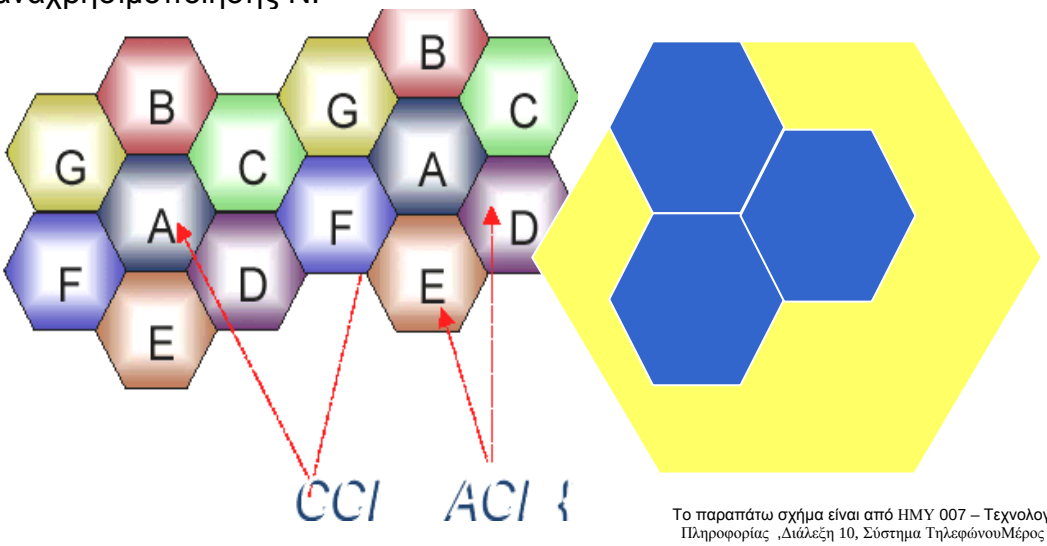





GSM Μεταγωγή Κυκλώματος
Μπλά-μπλά-μπλά
MS= ME+SIM
cells
BTS
BSC
BTS
MS
BSS1
MSC
VLR
GMSC
HLR
AC
EIR
NSS
PSTN
ISDN
MSC
VLR
MS
BSS2
Απρ-04
Γ.Ι.Στεφάνου-ΣΥΣΤΗΜΑΤΑ ΚΙΝΗΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ
9


Παράδειγμα Εισερχόμενης κλήσης
MSC
VLR
GMSC
PSTN
ISDN
LA1
cells
BTS
MS= ME+SIM
BSC
BSC
MSC
VLR
BTS
BSC
HLR
AC
EIR
MS
LA2
MSC
VLR

Στα συστήματα GSM έχουμε ενδοκαναλική παρεμβολή και η σχέση σήματος προς θόρυβο λέγεται SNR , (Signal –to – Noise Ratio).
Ενδοκαναλική παρεμβολή (Co – Channel Interference: CCI) είναι η παρεμβολή ή από τους χρήστες ή από τον BS μιας κοντινής κυψέλης με το ίδιο σύνολο συχνοτήτων.
Ενώ η παρεμβολή του γειτονικού καναλιού είναι η παρεμβολή από άλλη κυψέλη που έχει σύνολο γειτονικών συχνοτήτων (Adjacent Channel Interference: ACI)
Η παρεμβολή γειτονικού καναλιού εξαρτάται από την απόσταση των δυο πομποδεκτών και την ποιότητα των φίλτρων απόρριψης των συχνοτήτων .Η ενδοκαναλική παρεμβολή εξαρτάται κυρίως από τον συντελεστή επαναχρησιμοποίησης N.



Το παραπάτω σχήμα είναι από ΗΜΥ 007 – Τεχνολογία Πληροφορίας ,Διάλεξη 10, Σύστημα ΤηλεφώνουΜέρος Β.

Όταν περιορίσουν την ακτίνα της κυψέλης εντός των ορίων μιας κυψέλης ,το ίδιο σύνολο καναλιών που χρησιμοποιήσαμε σε αυτήν μπορεί να ξαναχρησιμοποιηθεί κάπου μακρύτερα. Η διαδικασία σχεδιασμού , επιλογής και διανομής καναλιών σε όλους τους κυψελοειδείς σταθμούς βάσης ενός συστήματος ονομάζεται επαναχρησιμοποίηση συχνότητας ,(frequency reuse)
Η σχέση του σήματος προς το θόρυβο (signal –to –noise ratio SNR) μπορεί να βελτιωθεί αν αυξηθεί η ισχύ εκπομπής .Όμως αυξάνοντας την ισχύ εκπομπής όλων των χρηστών ο λόγος σήματος προς παρεμβολή signal –to –interference =SIR) ,για να βελτιωθεί ο SIR πρέπει να αυξηθεί ο λόγος (q=D/R)
Παρατηρούμε μεγαλώνοντας το q , το N μεγαλώνει άρα μικραίνουμε την χωρητικότητα του συστήματος .
Τον SIR ή αλλιώς carrier to interference (C/I) στον σταθμό βάσης της κεντρικής κυψέλης σαν συνάρτηση των αποστάσεων είναι ο τύπος

$$C/I = SIR = \frac{R^{-n}}{\sum_{k=1}^{6} D_k^{-n}}$$

Από τον παραπάνω τύπο,ο παρονομαστής αναφέρεται σε χρήστες σε κυψέλες των γειτονικών ομοκαναλικών ομάδων .Αν θεωρήσουμε ότι $D_k = D$ τότε παίρνουμε την παρακάτω σχέση

$$C/I = \frac{(D/R)^n}{6} = \frac{(\sqrt{3N})^n}{6}$$

και παρατηρούμε ότι ο λόγος φέροντος προς παρεμβολή είναι ανάλογος με το N και βελτιώνεται με αύξηση του N.

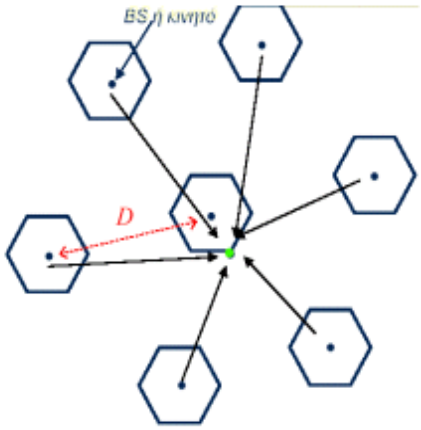
Ο λόγος σήματος προς παρεμβολή προς παρεμβολή (SIR) γίνεται

$$SIR = \frac{S}{\sum_{k=1}^{6} I_k}$$

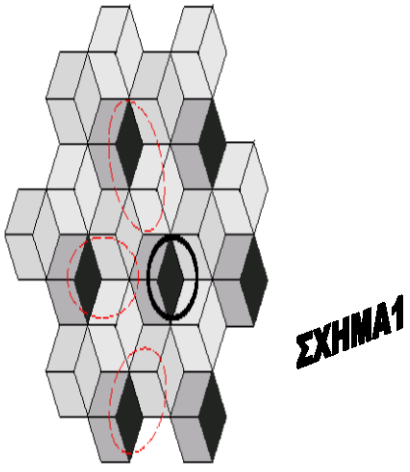
Όπου:

S είναι η ισχύς του σήματος ενδιαφέροντος [*Signal of Interest: SoI*] και

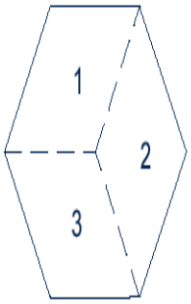
I_k είναι η ισχύς μίας παρεμβολής



Ένας τρόπος μείωσης της παρεμβολής από ομοιοκαναλικές κυψέλες είναι η τομεοποίηση , που αναφέρεται στην χρήση κατευθυντικών κεραιών αντί ισοτροπικών γιατί μειώνεται η παρεμβολή στις άλλες κυψέλες .Με ην τομεοποίηση ,κάθε τομέας είναι απλά μια κυψέλη και χρειάζεται μεταπομπή μεταξύ των τομέων .Οι τρεις κεραίες των τομέων λαμβάνουν σήματα που λαμβάνει ένα κινητό .Στο παράδειγμα φαίνονται τρεις τομείς των 120^o,ενώ οι κατευθυντικές κεραίες των BS τοποθετούνται στις παρυφές των κυψελών και χρησιμοποιείται η κεραία με την καλύτερη λήψη για να εκπέμψει το σήμα . (ΣΧΗΜΑ1)



ΣΧΗΜΑ1



(ΣΧΗΜΑ 2)

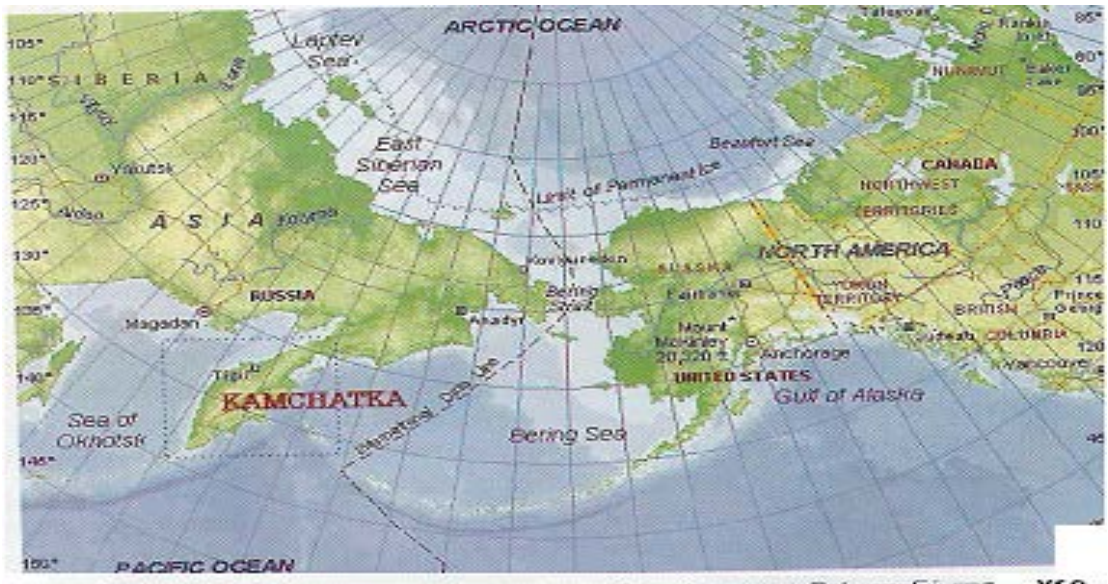
Ορισμένες φορές στο GSM συναντούμε το φαινόμενο του << προσωρινού δανεισμού >> συχνοτήτων από κυψέλες μικρής κυκλοφορίας σε κυψέλες με μεγάλη κυκλοφορίας και μόλις ολοκληρωθεί και τελειώσει η κλήση τότε τις επιστρέφει .Όλη αυτή την διάρκεια που δανείζουν τις συχνότητες δεν μπορούν να χρησιμοποιηθούν τα κανάλια από τις γειτονικές κυψέλες .
Αν οι χρήστες είναι πολλοί μπορούν να διαχωριστούν τις κυψέλες σε μικρότερα μέρη με μειωμένη ακτίνα κάλυψης και έτσι να αυξηθεί η χωρητικότητα των κυψελών.(ΣΧΗΜΑ 2)

Νόμιμη συνακρόαση

ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

Το τελευταίο χρονικό διάστημα ακούγεται στα μέσα μαζικής ενημέρωσης για τις υποκλοπές τηλεφωνικών επικοινωνιών της εταιρείας Vodafone .Όμως αυτές οι υποκλοπές με την μορφή της συνακρόασης υπήρχαν από πολύ παλιά.
Σύμφωνα με το άρθρο για τις υποκλοπές [Γ',48] το 1970 ξεκίνησε μια επιχείρηση ,από μια ιδέα του Bradley J. και του Henry Kissinger ,ενός πλοίαρχου του αμερικανικού ναυτικού και ενός σχεδιαστή όλης της επιχείρησης ,για να γίνει από τους Αμερικάνους υποκλοπή όλων των τηλεφωνικών επικοινωνιών μεταξύ του σοβιετικού αρχηγείου στόλου και της Μόσχας .Αυτή η υποκλοπή έγινε από το υποθαλάσσιο καλώδιο τηλεφωνικής ζεύξης μεταξύ της χερσονήσου της Καμτσάτκα (Kamchatka)και της ανατολικής ακτής της Ρωσίας , βορείως της Ιαπωνίας στην Οκχοτσική (Okhotsk) θάλασσα .Το καλώδιο βρισκόταν έξω από το μεγαλύτερο ναύσταθμο πυρηνικών υποβρυχίων της πρώην ΕΣΣΔ, στο Πετροπαβλόσκ ,σε βάθος 200 μέτρα. Συσκευές υποκλοπής τοποθετήθηκαν και στα υπόλοιπα υποβρύχια καλώδια τηλεφωνικών διόδευσεων ,κυρίως στην παγωμένη θάλασσα του Μπόρενς , στον Αρκτικό Ωκεανό .Οι υποκλοπές διάρκεσαν πάνω από 15 χρόνια ,όπου τους έκλεβαν πολλές κρατικές μυστικές πληροφορίες και κυρίως για τις ατέλειες των βαλλιστικών πυραύλων . Έγινε με την μεταφορά ενός αμερικανικού πυρηνοκίνητου υποβρύχιου ,του UUS Halibut , που είχε εγκατεστημένο τον ισχυρότερο υπολογιστή της εποχής εκείνης τον Univax και είχε εξοπλισμό τέτοιο, που με 'ένα ειδικό σύστημα επαγωγικής λήψης και καταγραφής παγίδεψε το καλώδιο των Ρώσων .Κάθε έξι μήνες ανέβαινε και αντικαθιστούσε τις μαγνοταινείες με τις υποκλαπείσες πληροφορίες με καινούριες και ξαναβυθιζόταν .Οι μαγνοταινείες μεταφέρονταν στο οχυρό Meade , στο Μέριλαντ ,στο αρχηγείο της υπηρεσίας ασφαλείας (NSA) και κορυφαίοι κρυπτογράφοι ανέλυσαν τους κώδικες και 1200 μεταφραστές και αναλυτές εξέτασαν εξονυχιστικά όλες τις καταγραφές .οι πληροφορίες ήταν ανεκτίμητες. Όμως ένα μέρος της δράσης αποκαλύφθηκε στους Ρώσους από την καταγραφή ύποπτων κινήσεων στην υποκλεμμένη περιοχή μέσω δορυφόρων το 1980.

Το βρυλικό υποβρύχιο USS Halibut, το οποίο ανέλαβε όλη τη «βρώμικη δουλειά» της τοποθέτησης της συσκευής υποκλοπής πάνω στο υποβρύχιο καλώδιο και την απλογή των μαγνητοταινιών.)



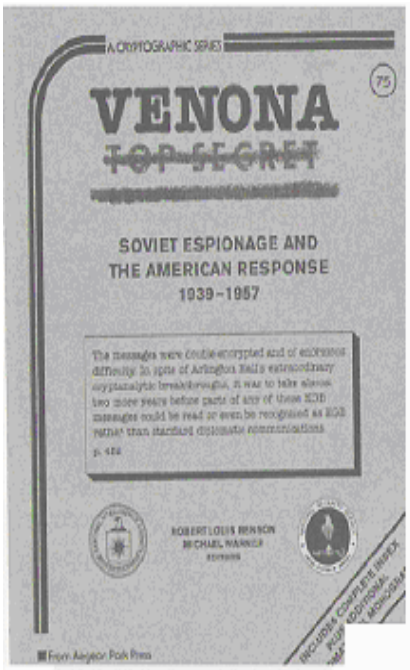
Το υποθαλάσσιο καλώδιο τηλεπικοινωνιακής σύνδεσης είχε πληγεί μεταξύ της χερσονήσου της Καμτσάτκα (Kamchatka) και της ανατολικής ακτής της Ρωσίας στην θάλασσα του Οχότσκ (Okhotsk).

Ένα άλλο πρόγραμμα το<< Programm >> έχει ως αντικείμενο την οργάνωση της παρακολούθησης εκατομμυρίων τηλεφωνικών συνομιλιών και ηλεκτρονικών μηνυμάτων ,όχι μόνο στην Αμερική ,αλλά σε όλο τον κόσμο. Αυτό το εγχείρημα παρακολούθησης, σύμφωνα με την συνέντευξη το 2005 του δημοσιογράφου της Ταιμς , Τζειμς Ρίσεν , το έθεσε με απόλυτη μυστικότητα η κυβέρνηση Μπους μετά την δολοφονική επίθεση της 11^{ης} Σεπτεμβρίου 2001 .Η φιλοσοφία του <<Προγράμματος >> είναι να δίδεται χωρίς όρους ,κάθε νομική και τεχνική διευκόλυνση στις μυστικές υπηρεσίες των Η.Π.Α. να παρακολουθούν όποιο τηλέφωνο θέλουν ασχέτως σε ποιον ανήκει ,ποιο αξίωμα έχει και ανεξαρτήτως της χώρας που βρίσκεται .
Μια άλλη επιχείρηση υποκλοπής τηλεφωνικών επικοινωνιών ήταν η επιχείρηση Gold ,το 1954.Σε μια συνδυασμένη ενέργεια , η CIA και η βρετανική MI 6 έσκαψαν ένα τούνελ μήκους 650 μέτρων ,(από τα οποία τα 400 μέτρα σε σοβιετικό τομέα ,σε βάθος 6 μέτρων) ,κάτω Από την καλύτερη επιτηρούμενη περιοχή του Ανατολικού Βερολίνου , δίπλα στο περίφημο φυλάκιο Charlie . Αυτό ήταν το κομβικό σημείο που συγκεντρώνονταν όλες οι τηλεπικοινωνιακές γραμμές στρατιωτικών επικοινωνιών μεταξύ της Ανατολικής Γερμανίας και της Μόσχας. Μέσα στο τούνελ στήθηκε ολόκληρο εργαστήριο υψηλής τεχνολογίας. Επειδή δεν μπορούσαν να σπάσουν τον κώδικα κρυπτογράφησης σε απευθείας τηλεφωνική ροή ,χρησιμοποιούσαν την καταγραφή του ανακλώμενου ήχου (echo) , που για κάποιο ανεξήγητο λόγο διέρρεε από τις συσκευές και δεν ήταν κρυπτογραφημένες .Όλα αυτά γινόταν εν γνώσει των Σοβιετικών και του σοβιετικού πράκτορα που δούλευε μέσα στην Βρετανική υπηρεσία Πληροφοριών ,ο George Blake ,που συμμετείχε μάλιστα και στον σχεδιασμό της σήραγγας . Με άλλα οι δυτικοί έπεσαν στην παγίδα των Σοβιετικών και του George Blake,τους κατασκεύασαν την σήραγγα του Βερολίνου και οι Σοβιετικοί την χρησιμοποιούσαν την επιχείρηση ως εφαλτήριο παραπληροφόρησης και ηθελημένης προώθησης αλλοιωμένων πληροφοριών .

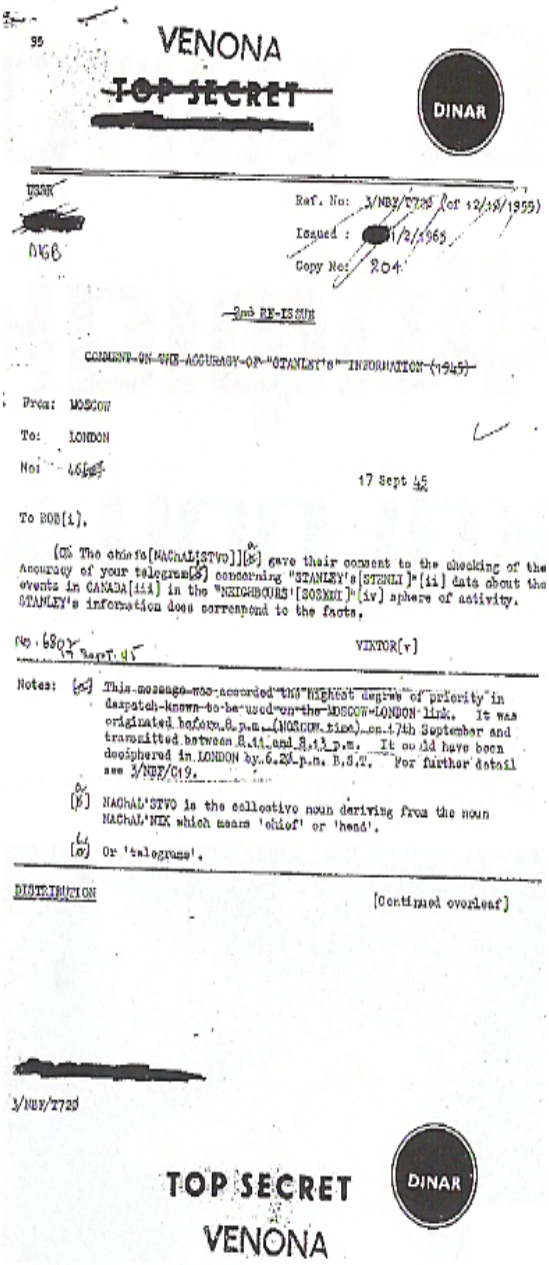
Μία από τις ελάχιστες φωτογραφίες που δείχνουν μέρος της σήραγγας του Βερολίνου.

Όμως οι Αμερικανοί έσκαψαν σήραγγα στην Μόσχα κάτω από το νέο κτίριο του κέντρου επικοινωνιών της KGB.Εγκατέστησαν συστήματα υποκλοπής πάνω σε όλες τις γραμμές και η επιχείρηση έδωσε πλήρη πρόσβαση στις πλέον απόρρητες επικοινωνίες της KGB.
Τηλεπικοινωνιακές , τηλεφωνικές υποκλοπές έγιναν και μέσα στο αρχηγείο της Ευρωπαϊκής Ένωσης ,στο κτίριο Justus ,στην καρδιά των Βρυξελλών .Το Μάρτιο του 2003 , λίγο πριν την διάσκεψη Κορυφής των πρωθυπουργών των χωρών της Ε.Ε. ,που θα συζητούσαν την επικείμενη εισβολή στο Ιράκ, ανακοινώθηκαν ότι βρέθηκαν τόσο στις αίθουσες συσκέψεων ,τόσο και στο τηλεφωνικό δίκτυο ,συσκευές υποκλοπής .Οι ίδιες συσκευές βρέθηκαν μετά από ένα χρόνο και στο κτίριο την Ηνωμένων Εθνών στην Γενεύη .
Μια άλλη επιχείρηση σχετικά με τις υποκλοπές ήταν το σχέδιο Venona .Το πρόγραμμα Venona ήταν ένα πρόγραμμα για την λήψη και την εκμετάλλευση των κρυπτογραφημένων σοβιετικών διπλωματικών επικοινωνιών της εποχής του 1939-1955 και σχεδιάστηκε το 1943 από την Υπηρεσία Πληροφοριών του Αμερικανικού Στρατού (ASIS) , πρόγονο της NSA και είναι γνωστή ως Arlington Hall ,επειδή εκεί γίνονταν η ανάλυση κειμένων.

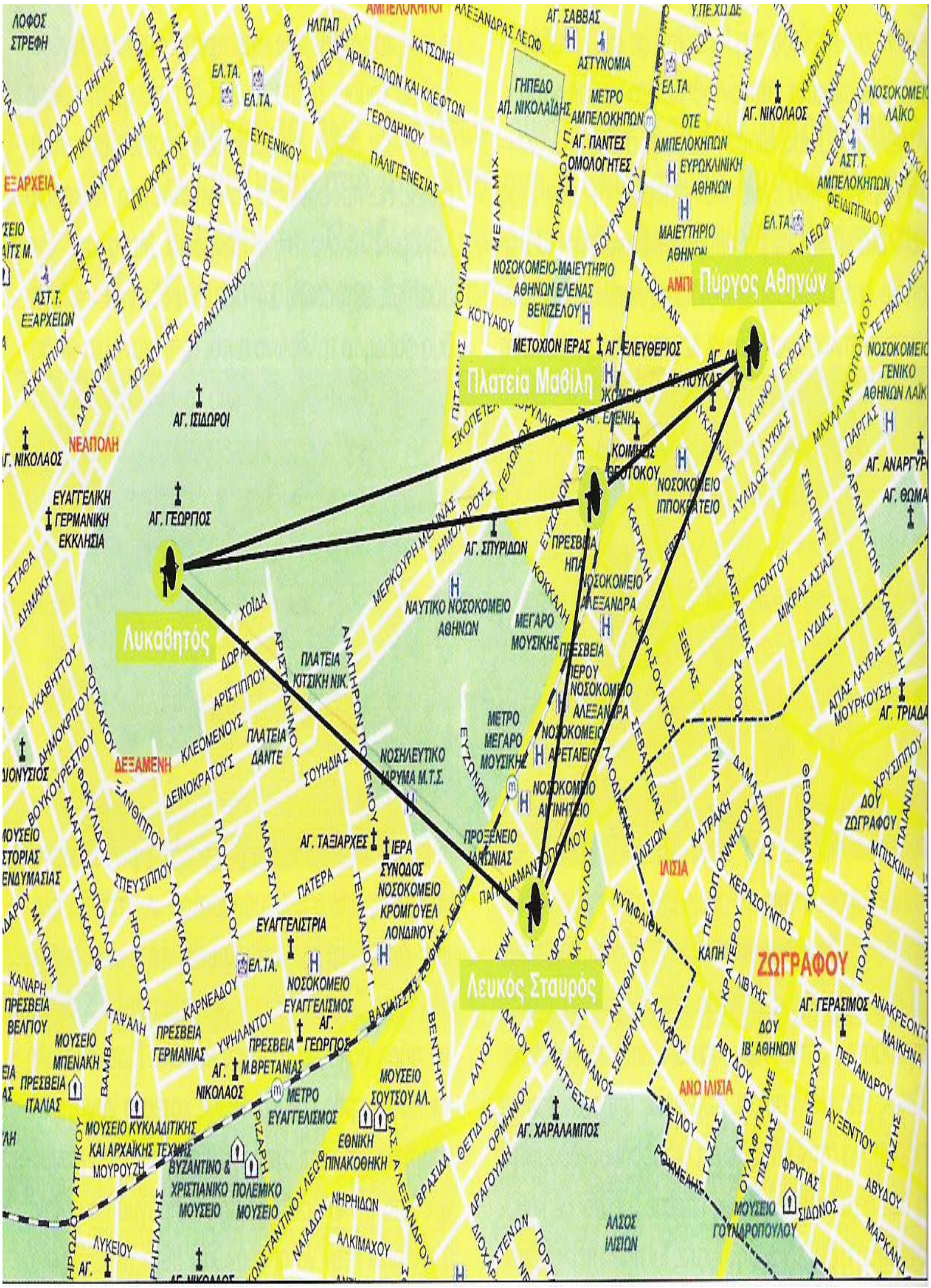
Ήδη από το 1939 είχαν συσσωρευτεί χιλιάδες κρυπτογραφημένα σοβιετικά τηλεγραφήματα ,με ισχυρότατο κώδικα κρυπτογράφησης , που είναι γνωστός σαν σημειωματάριο μιας χρήσης (one – time – pad) και ο οποίος είναι αδύνατον να αναλυθεί. Όμως το 1944 , η δασκάλα Meredith Gardner , μια από τις αναλύτριες του σχεδίου κατόρθωσε να διαβάσει δυό μηνύματα της KGB ,που αποκάλυπταν ότι κάποιος από το επιτελείο του αμερικανικού Υπουργείου Πολέμου μετέδιδε απόρρητες πληροφορίες στους Σοβιετικούς , όπως διαρροή πληροφοριών των μυστικών σχεδίων της ατομικής βόμβας , από τα απόρρητα εργαστήρια της Los Alamos .Αυτό είχε ως συνέπεια να αποκαλύπτουν οι πράκτορες που δούλευαν για την Ρωσία και να φυλακιστούν ή να πεθάνουν στην ηλεκτρική καρέκλα .



Το σχέδιο Venona ήταν ένα πρόγραμμα για τη λήψη και την εκμετάλλευση των κρυπτογραφημένων σοβιετικών διπλωματικών επικοινωνιών της εποχής 1939-1955. Οι αποκρυπτογραφήσεις τού σχεδίου Venona αποκάλυψαν 200 ονόματα ή ψευδώνυμα ατόμων που βρίσκονταν στις ΗΠΑ και αναφέρονταν σε μηνύματα των Σοβιετικών ως συνεργάτες ή πληροφοριοδότες. Τα μηνύματα αποκάλυψαν τη δραστηριότητα των Julius και Ethel Rosenberg, Klaus Fucks και άλλων, που είχαν αναμιχθεί σε υποθέσεις κατασκοπίας σχετικές με την κατασκευή της ατομικής βόμβας. Συνεπήρθησαν σχεδόν όλοι και μερικοί εκτελέστηκαν. Η επιχείρηση Venona αποτελεί την πλέον ένδοξη σελίδα στον κατάλογο των επιτυχιών της αμερικανικής αντικατασκοπίας. Όλες οι λεπτομέρειες της επιχείρησης αναλύονται στο κείμενο «Venona, Top Secret», το οποίο υπάρχει και στο Internet στη διεύθυνση kvlatos@tellas.gr

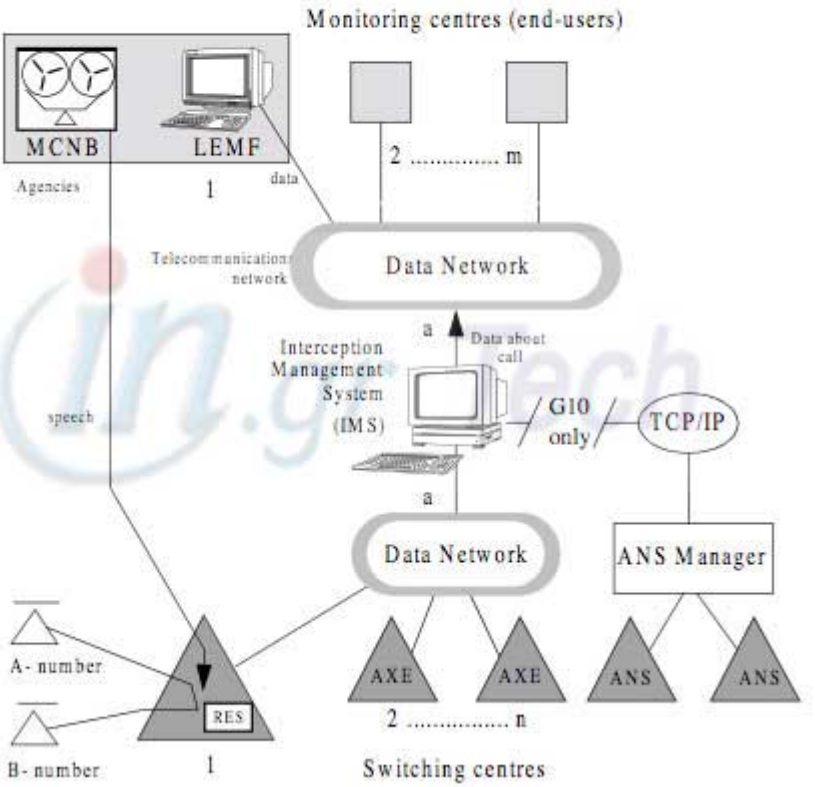


Ένα από τα άκρως απόρρητα αποκρυπτογραφημένα τηλεγραφήματα της επιχείρησης Venona. Μόνον το 1995 έγινε η άρση του απορρήτου για την επιχείρηση και δημοσιεύτηκαν τα πρώτα κείμενα.



Από της 4 Μαρτίου 2005 , ημέρα Παρασκευή η Ericsson ανίχνευσε σε δύο κόμβους της εταιρείας Vodafone – Panafon ειδικό κωδικό που μπορεί να σχετίζεται με υποκλοπές τηλεφώνων , τις 3 Φεβρουαρίου 2006 ανακοινώθηκε επίσημα στο κοινό και άρχισαν οι διώξεις .Με την χρήση και τη βοήθεια των κεραιών που φαίνονται στο σχήμα έγιναν οι υποκλοπές(συνακρόαση) . Παρακάτω θα δούμε πως έγινε η υποκλοπή το 2005/06 στην Ελλάδα [Γ',6].

Figure 1.1 Telecommunication interception model



[Γ',6]

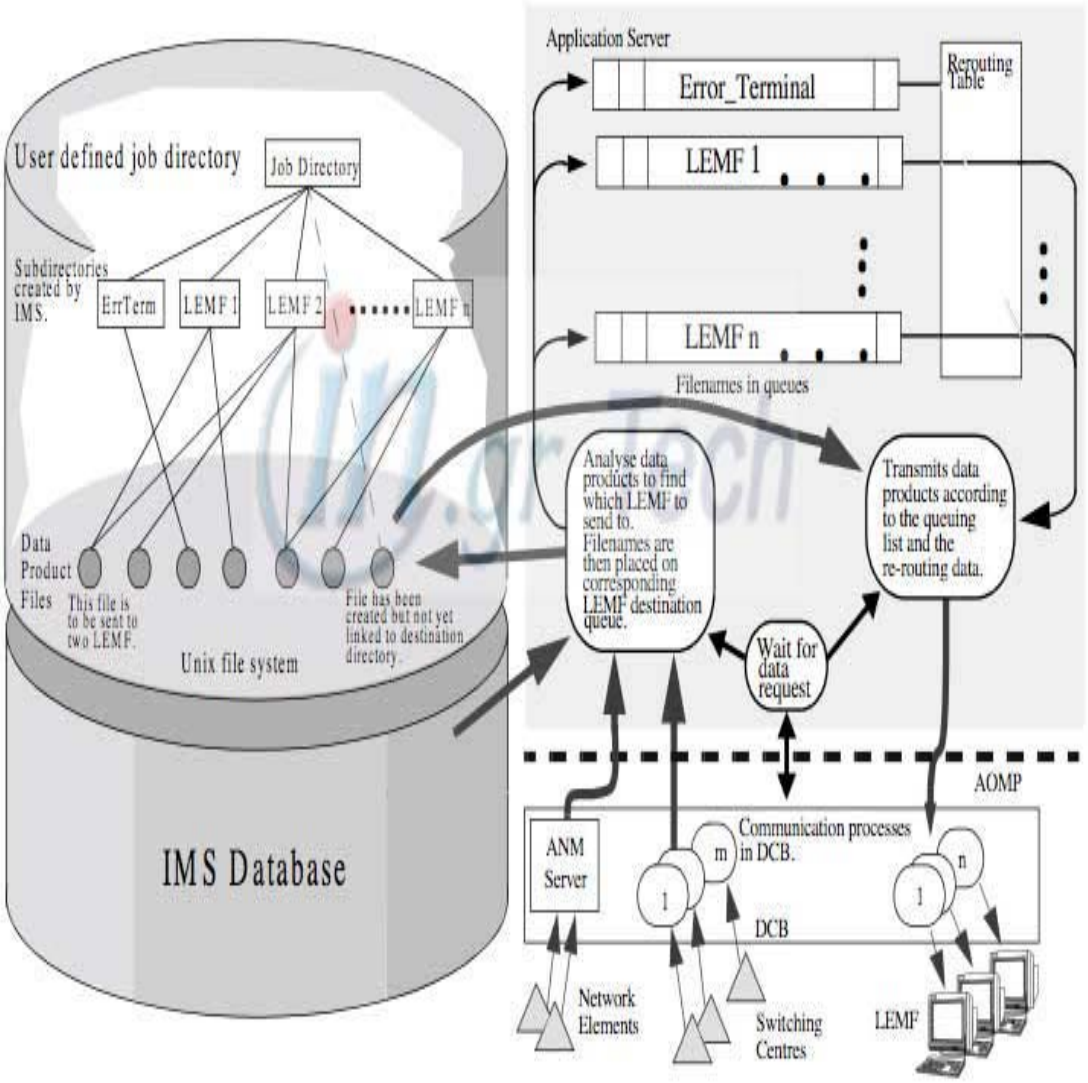
Όπως θα παρατηρήσετε στο σχήμα που ακολουθεί, κατά την έναρξη λειτουργίας του συστήματος συνακρόασης, μπορεί να ενεργοποιηθεί ξεχωριστή χρέωση μέσω συγκεκριμένης εντολής. Επίσης, όταν το σύστημα τίθεται σε λειτουργία, στέλνει συναγερμό (alert) σε οπτικό σύστημα (φωτάκι) και ενημερώνει τα αρχεία καταγραφής και τους τεχνικούς βάρδιας.

Οι χειριστές και οι διαχειριστές του συστήματος έχουν γραφικό περιβάλλον εργασίας, στο οποίο φαίνονται όλες οι δραστηριότητες και ρυθμίζονται οι παράμετροι λειτουργίας, έτσι ώστε οι ενδείξεις έναρξης λειτουργίας του συστήματος συνακρόασης θα γινόντουσαν αμέσως αντιληπτές

Στη εικόνα που ακολουθεί φαίνεται το τηλεπικοινωνιακό μοντέλο του IMS (Interception Management System, Συστήματος Διαχείρισης Συνακροάσεων). Σύμφωνα με το σχήμα που ακολουθεί, το σύστημα δίδει την δυνατότητα στον -παράνομο στην περίπτωσή μας- χειριστή να παρακολουθήσει δυνάμει άπειρα τηλέφωνα και να ανακατευθύνει τα δεδομένα που συλλέγονται στους σταθμούς καταγραφής , παρακολούθησης. Όπως φαίνεται στο σχήμα που ακολουθεί στην καρδιά του συστήματος υπάρχει το λειτουργικό σύστημα Unix το οποίο αρχειοθετεί τοποθετώντας σε "ουρά" (queue) τα αρχεία καταγραφής των συνομιλιών των -δυνάμει απείρων- προς παρακολούθηση κινητών.

Η βάση δεδομένων του συστήματος δέχεται αυτά τα αρχεία καταγραφής όλων των σταθμών-κινητών που παρακολουθούνται .

Figure 1.3 Server functions implementation model



[Γ',6]

ΠΩΣ ΓΙΝΕΤΑΙ Η ΠΑΡΕΜΒΟΛΗ ΜΕ ΤΗΝ ΜΟΡΦΗ ΤΗΣ ΣΥΝΑΚΡΟΑΣΗΣ .

Το γενικό πλαίσιο που ακολουθείται κατά την σχεδίαση ενός σύγχρονου συστήματος όπως της κινητής επικοινωνίας είναι ότι πρέπει να είναι ασφαλές σε ότι αφορά την παραβίαση του από ερασιτεχνικές ή ημιεπαγγελματικές επιθέσεις , αλλά θα πρέπει να προσφέρει την δυνατότητα νόμιμης άρσης του απορρήτου , όταν αυτό κριθεί σκόπιμο .

Υπάρχουν τρία επίπεδα ασφάλειας στις τηλεπικοινωνίες .

Το πρώτο επίπεδο ασφαλείας περιλαμβάνει τους μηχανισμούς πιστοποίησης και ελέγχου πρόσβασης ,που στοχεύουν στην διατήρηση της ασφάλειας μέσω του ελέγχου της πρόσβασης στο σύστημα .Αναφέρεται στη διαδικασία εξουσιοδότησης << εισόδου και χρήσης >> και πιστοποίησης (authentication) , δηλαδή στον έλεγχο της ταυτότητας του χρήστη ,που μοιάζει με τα passwords των υπολογιστών .
Το δεύτερο επίπεδο της διαχείρισης και ελέγχου των διαδικασιών διατήρησης του απόρρητου ,περιλαμβάνει τους μηχανισμούς διαχείρισης και καλής λειτουργίας των συστημάτων .Ελέγχεται η λειτουργία σύμφωνα με τις προδιαγραφές και προκαλείται η διακοπή των επικοινωνιών ,όταν κάτι δεν λειτουργήσει με τα προβλεπόμενα .Αφορά στο γενικό διαχειριστικό έλεγχο της καλής (από απόψεως κρυπτογράφησης) λειτουργίας του συστήματος .
Το τρίτο επίπεδο είναι <<των ασφαλών αλγόριθμων >>(cryptographic algorithms) ,αναφέρεται στους μαθηματικούς αλγόριθμους ,που σε συνδυασμό με τα <<κλειδιά >>,προσδίδουν στο σύστημα το επιθυμητό επίπεδο ασφαλείας .Ταυτόχρονα πρέπει να υπάρχει και το επίπεδο της << σύννομης υποκλοπής >>(lawful interception mechanisms) δηλαδή η δυνατότητα της ηθελημένης παραβίασης του απόρρητου, όταν προκύπτει η ανάγκη,από εξουσιοδοτημένους μηχανισμούς .Όλα τα συστήματα έχουν σχεδιαστεί να υπάρχει αν απαιτηθεί η άρση του απόρρητου.

Οι επικοινωνίες μέσω των κινητών τηλεφώνων δεν υποκλέπτονται κατά την εναέρια διαδρομή του σήματος από το κινητό τηλέφωνο μέχρι το σταθμό λήψης δηλαδή την πλησιέστερη κεραία γιατί είναι κρυπτογραφημένη , εκτός και αν γίνει άρση της κρυπτογράφησης για διάφορους άλλους λόγους .
Η άρση της κρυπτογράφησης **,που είναι μια υποκλοπή ,*θα γίνει με δυο τρόπους.***

Η πρώτη μορφή υποκλοπής για την άρση της κρυπτογράφησης είναι η κινητοποίηση κάποιου εξειδικευμένου κλιμακίου υποκλοπών ,που θα έχει εξαιρετικά εξελιγμένη τεχνολογική υποδομή και ικανότητες και θα επιχειρήσει λήψη και κρυπτανάλυση του κρυπτογραφημένου σήματος ,όμως αυτό εκτός που είναι δύσκολο και απαγορευμένο χρησιμοποιείται κυρίως σε πολεμικές επιχειρήσεις .

Η δεύτερη μορφή υποκλοπής για την άρση της κρυπτογράφησης είναι << η παραπλάνηση >> του κινητού τηλεφώνου μέσω αντικατάσταση της κεραίας λήψης της τηλεφωνικής εταιρείας με άλλη ,που θα βρίσκεται συνεχώς κοντά στο τηλέφωνο και θα παίζει το ρόλο του <<ψεύτικου σταθμού βάσης >> .Η τεχνική αυτή μοιάζει με την φυσική παρακολούθηση και λέγεται και <<ISMI catcher >> ,που έχει όμως ένα μειονέκτημα .Θα πρέπει ο σταθμός λήψεως να βρίσκεται συνεχώς κοντά στο τηλέφωνο – στόχο , σε απόσταση μικρότερη από αυτή που βρίσκεται η κάθε κεραία και να το ακολουθεί κατά βήμα ,κάτι που εκτός του ότι μπορεί να γίνει εύκολα αντιληπτή χρειάζεται τις κατάλληλες υποδομές και το κατάλληλο προσωπικό.
Από τεχνικής φύσεως είναι εύκολο να γίνει αν σε ένα φορτηγάκι ,που πηγαίνει έξω από το σπίτι στόχος ,φορτωθεί ένας σταθμό βάσεως (υποκλοπέας) και ρυθμιστεί να εκπέμπει πιο δυνατό σήμα από αυτό που δίνουν στην περιοχή οι εταιρείες κινητής τηλεφωνίας . Τότε το κινητό τηλέφωνο που συνδέεται πάντα με πιο ισχυρό σήμα θα βλέπει σαν κοντινή κυψέλη το σταθμό –υποκλοπέα και αν ο χρήστης του κινητού θελήσει να συνδεθεί στο δίκτυο , θα επιλεχθεί άθελα του αυτός ο σταθμός – μαϊμού (υποκλοπέας) και θα του δώσει **το IMSI του κινητού του χρήστη .**Στην συνέχεια εκείνος ο σταθμός – μαϊμού λειτουργεί ως κινητό και το μεταβιβάζει στο πραγματικό σταθμό κινητής τηλεφωνίας και λαμβάνει τον αριθμό ***RAND ,*** τον οποίο αναμεταδίδει στο κινητό τηλέφωνο του χρήστη και γίνεται η υποκλοπή και η συνακρόαση . Με άλλα λόγια ο σταθμός – μαϊμού λειτουργεί σαν ενδιάμεσος σταθμός ,που παρακολουθεί τη συνομιλία και γνωρίζει όλα τα στοιχεία ταυτότητας του κινητού σταθμού .Αυτή η τεχνική είναι μια παραλλαγή της γνωστής κρυπταναλυτικής επίθεσης , που είναι γνωστή ως τεχνική **man –in – the –middle** και χρησιμοποιείται σήμερα ευρύτερα.
Το σύστημα της κινητής τηλεφωνίας GSM αποτέλεσε μια πραγματική επανάσταση στην εξέλιξη των τηλεπικοινωνιών , σε σημείο που να διακρίνεται η εποχή των κινητών επικοινωνιών σε προ- GSM περίοδο και μετά- GSM περίοδο . Η ταυτόχρονη χρήση φασματικής πολυπλεξίας (**TDMA**) , αλλαγής συχνότητας κατά την διάρκεια της επικοινωνίας (frequency hopping) ,ψηφιοποίησης και κρυπτογράφησης δεδομένων και φωνής , η διαδικασία πιστοποίησης πριν την αποκατάσταση της επικοινωνίας (authentication) κάνουν το σύστημα GSM θεωρητικά απρόσβλητο .Η πραγματικότητα όμως είναι διαφορετική .**Υπάρχουν ήδη συστήματα ,που μπορούν να συλλάβουν (capture) <<on air >> την εκπομπή των κινητών τηλεφώνων , να παρακολουθούν τις αλλαγές συχνοτήτων (tracking) , και να αποδιαμορφώνουν το σήμα** .
Όσο αφορά την αποκρυπτογράφηση είναι λίγο πιο δύσκολα τα πράγματα . Όταν σχεδιάστηκε το σύστημα GSM ,στις αρχές της δεκαετίας του 1990 ,αναπτύχθηκε ειδικός αλγόριθμος κρυπτογράφησης ,που λέγεται A5 και ακόμα και σήμερα είναι δύσκολο να σπάσει . Χρησιμοποιούσε κρυπτογράφηση ψευδοτυχαίο κώδικα , με μήκος 64 bits ,ο οποίος , με τα μέτρα της προηγούμενης δεκαετίας , ήταν ανθεκτικός ακόμα και σε σοβαρή <<κρυπταναλυτική επίθεση>>. Λιγότεροι ισχυροί κρυπτοκώδικες που χρησιμοποιούνταν για την κρυπτογράφηση των δεδομένων του ηλεκτρονικού ταχυδρομείου με μήκος 52 bits π.χ. του προγράμματος PGP,θεωρήθηκαν από την αμερικανική κυβέρνηση ως πολεμικά όπλα ,που είχε απαγορεύσει την εξαγωγή τους .

Μετά από αυτό οι Ευρωπαίοι σχεδιαστές της κινητής τηλεφωνίας υποβάθμισαν την ισχύ του κρυπτοαλγόριθμου .Αντικατέστησαν το Α5 με τους εξής ειδικά σχεδιασμένους αλγόριθμους :
Για την ευρωπαϊκή αγορά (χώρες CERT) τον Α5/1 ,με κρυπτογραφική ισχύ 52 bits.

Για τις περιφερειακές χώρες της Ευρώπης και την Ρωσία ο Α5/2 , με ισχύ 40 bits.

Για όλες τις υπόλοιπές χώρες (τριτοκοσμικές) ο Α5 / 0 , που είναι χωρίς κρυπτογράφηση .Θα φανεί περίεργο αλλά και η Γαλλία χρησιμοποιεί το Α5 / 0,που γι αυτό τον λόγο λέγεται και << French mode >>.
Για τα δίκτυα τρίτης γενιάς 3 G σχεδιάστηκε ένας ακόμα αλγόριθμος ο << Α5 /3 >> ,που χρησιμοποιούν π.χ. όπως τα κινητά Nokia με ενεργοποιημένη την λειτουργία Net Monitor.
Αυτές οι κρυπταναλυτικές επιθέσεις εναντίον του αλγόριθμου Α5 , χρησιμοποιούνται όταν γίνει υποκλοπή σήματος κατά την εναέρια διαδρομή .
Όταν όμως ο υποκλοπέας έχει πρόσβαση στους σταθμούς των εταιρειών της κινητής τηλεφωνίας είναι εντελώς διαφορετική η περίπτωση γιατί μετά τις κεραίες λήψεως του σταθμού βάσεως ,δεν υπάρχει κρυπτογράφηση και η διαδικασία υποκλοπής είναι απλή και ανάλογη με αυτής της σταθερής τηλεφωνίας .

Το σύστημα ασφάλειας ασύρματων επικοινωνιώνGSM εξαρτάται από δυο διαδικασίες :

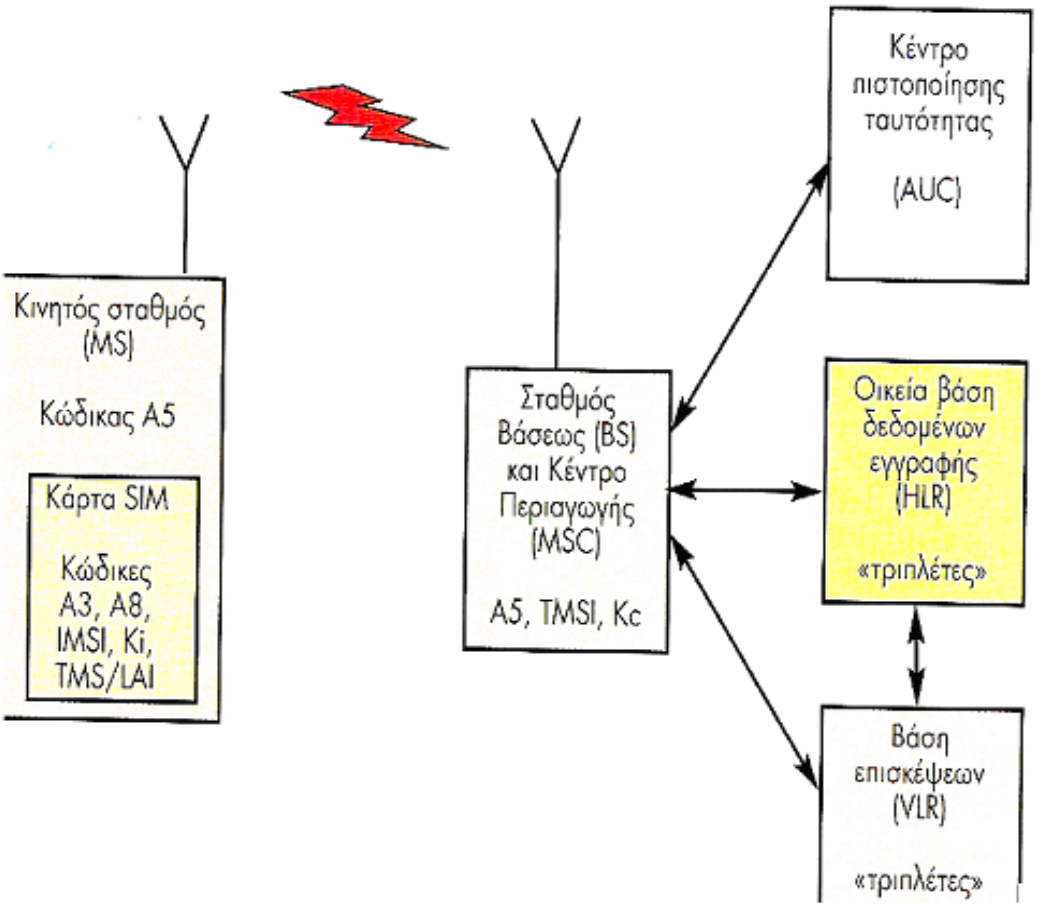
- ***<u>την διαδικασία πιστοποίησης</u>***

- ***<u>και την διαδικασία κρυπτογράφησης φωνής .</u>***

Στις διαδικασίες αυτές συμμετέχουν τρεις αλγόριθμοι .
Στην διαδικασία πιστοποίησης και ελεύθερης πρόσβασης στο σταθμό βάσης στηρίζεται στους αλγόριθμους Α3 και Α8 .Πολλές φορές στα δίκτυα κινητής τηλεφωνίας οι δύο αλγόριθμοι ενοποιούνται σε ένα όπως είναι ο αλγόριθμος COMP 128 της AEG.Μια νεότερη έκδοση του είναι ο COMP 128 –2 ,που έχει απλή δομή και μικρή υπολογιστική ισχύ και βρίσκεται στην κάρτα SIM και όχι στο τηλέφωνο .
Η δεύτερη διαδικασία ασφαλείας της κρυπτογράφησης της φωνής χρησιμοποιεί τον αλγόριθμο Α5 ,που χρειάζεται μεγάλη υπολογιστική ισχύ και για αυτό βρίσκεται στην μονάδα DSP του τηλεφώνου. Η δράση του αλγόριθμου Α5 στηρίζεται στην παραγωγή της << κλείδας κρυπτογράφησης φωνής K_C >> ,μεγέθους 64 bits και από αυτά μόνο τα πρώτα 54 bits χρησιμοποιούνται ενώ τα υπόλοιπα 10 bits αντικαθίστανται με μηδενικά .Αυτή η μείωση του μήκος από 64 σε 54 bit ,μειώνει δραστικά την ισχύ κρυπτογράφησης του αλγόριθμου φωνής Α5 .Το μήκος της κλείδας δεν μπορεί να αυξηθεί με εξωτερική επέμβαση ,κάτι που ισχύει σε όλους τους αλγόριθμους ,που θα χρησιμοποιηθούν στην θέση του Α8 .

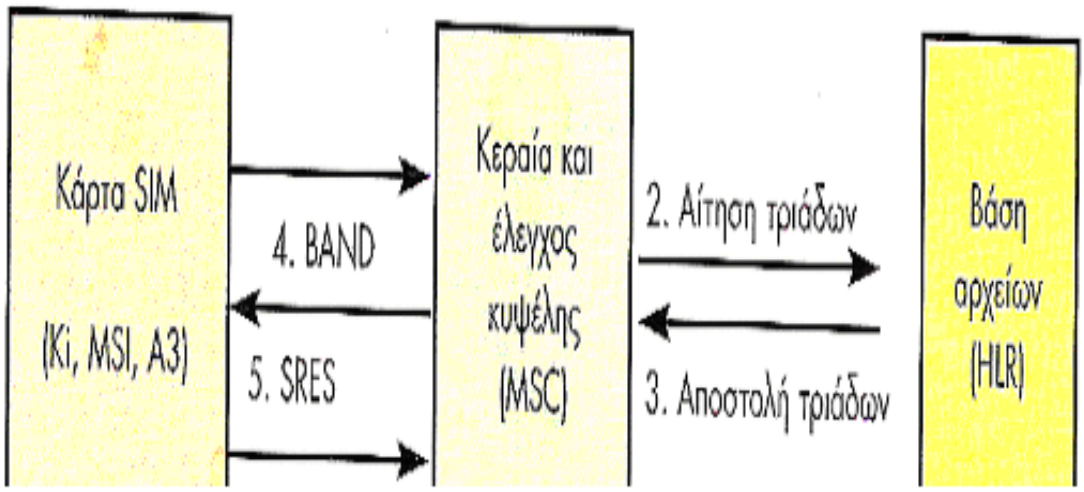
ΑΡΧΙΚΗ ΕΓΓΡΑΦΗ ΤΟΥ ΚΙΝΗΤΟΥ ΣΤΟ ΣΥΣΤΗΜΑ

Μόλις ο κινητός σταθμός μπει σε λειτουργία ,σαρώνει τις συχνότητες εκπομπής συνεχούς πληροφορίας του δικτύου (BCH /CCCH) .Όταν ο κινητός σταθμός μπει για πρώτη φορά στο σύστημα ή μετά από μεγάλη παύση , το κέντρο μεταγωγής (Mobile Services Switching Center ,MSC) και η βάση επισκέψεως (Visitor Location Register ,VLR) δεν γνωρίζουν τίποτα για αυτόν. Ο κινητός σταθμός πρέπει να τους ενημερώσει για τα στοιχεία του ,που θα πρέπει να διασταυρωθούν μέσω της οικείας βάσης δεδομένων του δικτύου (Home Location Register ,HLR) (σχήμα 1) .Ο κινητός σταθμός αρχίζει την ενημέρωση του συστήματος ,στέλνοντας τον αριθμό IMSI (Διεθνής Ταυτότητα Συνδρομητή , International Mobile Subscriber Identity) ανακοινώνοντας ότι ένας είναι ένας νέος στην περιοχή ,Η ταυτότητα IMSI είναι καταχωρημένη στην κάρτα SIM και προσδιορίζει τον συνδρομητή , δεν ταυτίζεται με τον αριθμό κλήσης του ,θεωρείται μη ανακοινώσιμο στοιχείο , που δεν το γνωρίζει ούτε ο συνδρομητής και αποτελείται από 15 το πολύ αλφαριθμητικούς χαρακτήρες .Για λόγους διασφάλισης του απόρρητου της ταυτότητας IMSI(για να μην γίνεται συχνή εκπομπή του σε κάθε κλήση) το δίκτυο ορίζει ένα προσωρινό IMSI ή TMSI (Temporary Mobile Subscriber Identity) .Αυτός έχει περιορισμένη ,τοπική σημασία μέσα στην περιοχή μιας βάσης επισκέψεως (Visitor Location Register ,VLR) και το μέγιστο μέγεθος του είναι τέσσερα bytes.Η βάση επισκέψεως πριν ορίσει σε έναν συνδρομητή ένα TMSI ,πρέπει να τον αναγνωρίσει ,ζητώντας εκπομπή του IMSI .Παράλληλα , ανταλλάσσεται η ταυτότητα της περιοχής εντοπισμού (Location Area Identification ,LAI) που προσδιορίζει μια συγκεκριμένη περιοχή του δικτύου ,μέσα στην οποία λειτουργεί ο κινητός σταθμός .Από τότε ,το σύστημα το θεωρεί συνδεδεμένο (attached) και καταγράφει την ταυτότητα IMSI στα αρχεία επισκέψεως ,χρησιμοποιώντας για τις μετέπειτα επικοινωνίες τον TMSI . Η βάση επισκέψεως ενημερώνει συστηματικά και την οικεία βάση δεδομένων του δικτύου (Home Location Register ,HLR) , όπου καταγράφονται όλα τα δεδομένα που αφορούν στο σύνολο των κινητών σταθμών που ανήκουν στο δίκτυο .



Κατομερισμός αρμοδιοτήτων και εξουσιοδοτήσεις ασφαλείας για την εγγραφή και χρήση στο δίκτυο κινητής τηλεφωνίας.

σχήμα 1



Διαδικασία αναγγελίας του κινητού σταθμού (MS) στην κυψέλη και αλληλουχία των ενεργειών που απαιτούνται για την «έκδοση» των τριάδων.

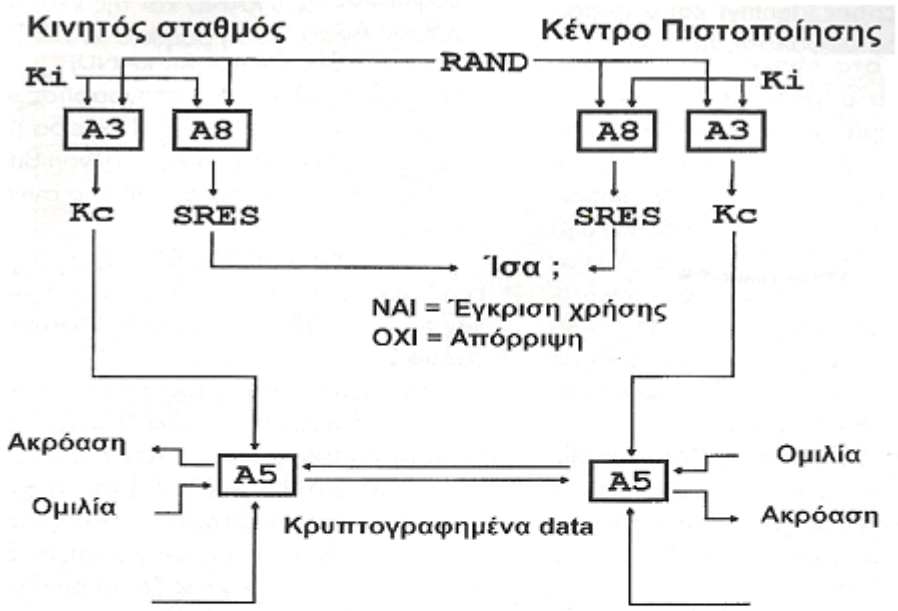
ΔΙΑΔΙΚΑΣΙΑ ΕΞΟΥΣΙΟΔΟΤΗΣΗΣ ΓΙΑ ΤΗ ΧΡΗΣΗ ΤΟΥ ΔΙΚΤΥΟΥ

Η εξουσιοδότηση χρήσης τηλεφωνικής συσκευής ,γίνεται με εισαγωγή και αναγνώριση από το κινητό του τετραψήφιου αριθμού PIN (Personal Identity Number) ,που αντιστοιχεί στην κάρτα SIM (Subscriber Identity Module) . Πρόκειται για την γνωστή διαδικασία CHV1 (Card Holder Verification 1 ,πρώτη επαλήθευση ταυτότητας) ,που επαναλαμβάνουν καθημερινά εκατομμύρια χρήστες κινητών τηλεφώνων. Αν γίνει λανθασμένη εισαγωγή του αριθμού τρεις διαδοχικές φορές ,τότε η κάρτα μπλοκάρεται και απαιτείται η εισαγωγή του οκταψήφιου κωδικού επαναλειτουργίας PUK (personal unblocking key) .Αν γίνει εισαγωγή λανθασμένου PUK επί δέκα συνεχείς φορές ,η κάρτα αχρηστεύεται . Στην συνέχεια ,χρησιμοποιείται ένα πολύπλοκο σύστημα πιστοποίησης της ταυτότητας και εξουσιοδότησης του συνδρομητή, για την χρήση δικτύου ,που συντονίζεται από το κέντρο ελέγχου της τηλεφωνικής εταιρείας (Φορέας) .Η πιστοποίηση της ταυτότητας του συνδρομητή και η εξουσιοδότηση χρήσης του δικτύου GSM γίνονται από το κέντρο πιστοποίησης ταυτότητας του συνδρομητή (Authentication Center, AUC) καθώς και από το κέντρο τεκμηρίωσης κινητού σταθμού (Equipment Identity Register ,EIR) και είναι διαδικασίες ανεξάρτητες .Η διαδικασία εξασφαλίζει στον φορέα της υπηρεσίας κινητής τηλεφωνίας από την παράνομη χρήση τρίτων ,όσο και το συνδρομητή από την κλοπή της συσκευής ή της κάρτας SIM. Η ασφαλής χρήση του κινητού τηλεφώνου στηρίζεται κατά ένα μέρος στην <<ταυτότητα του >>,που περιέχεται σε δυο κωδικούς αριθμούς ,που έχουν γραφεί στην κάρτα SIM ,έναν άγνωστο και ένα απόρρητο ,που έχουν γραφεί πάνω στην κάρτα SIM.Ο άγνωστος είναι ο αριθμός IMSI (International Mobile Subscriber Identity) και ο απόρρητος η κλείδα ασφαλείας Ki , που είναι μοναδική και φυλάσσεται τόσο στην κάρτα όσο και στο κέντρο πιστοποίησης (AUC).Πρόκειται για το λεγόμενο κοινό μυστικό (shared secret). Η κλείδα ασφαλείας Ki έχει μέγεθος 128 bit ,δεν είναι γνωστή στον κάτοχο του της συσκευής , δεν μπορεί να υπολογιστεί ή να αποσπαστεί εύκολα από την κάρτα και αποτελεί το ***ακρογωνιαίο λίθο*** για την συνολική ασφάλεια των επικοινωνιών κινητής τηλεφωνίας GSM.Δεν μεταδίδεται ποτέ από τον αέρα και δεν μπορεί θεωρητικά να εξαχθεί από την κάρτα . Όταν ο κινητός σταθμός (MS, Mobile Station) αναγγείλει την παρουσία του σε κάποια κυψέλη του δικτύου (Κέντρο λήψης και μεταγωγής , (MSC ,Mobile Services Switching Center),τότε ειδοποιείται η οικεία βάση δεδομένων εγγραφής (HLR,Home Location Register) ,που στέλνει μια πεντάδα τριών αριθμών (<<τριπλέτες >> , triples).Αν ο σταθμός βρίσκεται σε περιαγωγή (σε άλλη χώρα) ,τότε η ανταλλαγή στοιχείων γίνεται μέσω της Βάσεως επισκέψεως (VLR) ,η οποία δεν παράγει δικές της τριπλέτες ,αλλά τις ζητάει από την οικεία βάση δεδομένων της χώρας εγγραφής του κινητού .Οι τριπλέτες είναι << τριάδες >> κωδικών ,μιας χρήσεως ,διαφορετικές για κάθε συνδρομή και αποτελείται από :

Ένα τυχαίο αριθμό RAND (RANDom number) που παράγεται από το δίκτυο
Μια ενυπογραφη απάντηση SRES(Signed RESponse) ,που δημιοργείται από τον αριθμό RAND και της κλείδας ασφαλείας Ki, με την βόηθεια του αλγόριθμου A3.
SRES =A3 (Ki,RAND)

Μια ειδική κλείδα κρυπτογράφησης φωνής (Ciphering key-Kc).Η κλείδα Kc θα χρησιμοποιηθεί από τον αλγόριθμο A5 για την κρυπτογράφηση της συνομιλίας
Kc = A8 (Ki ,RAND).

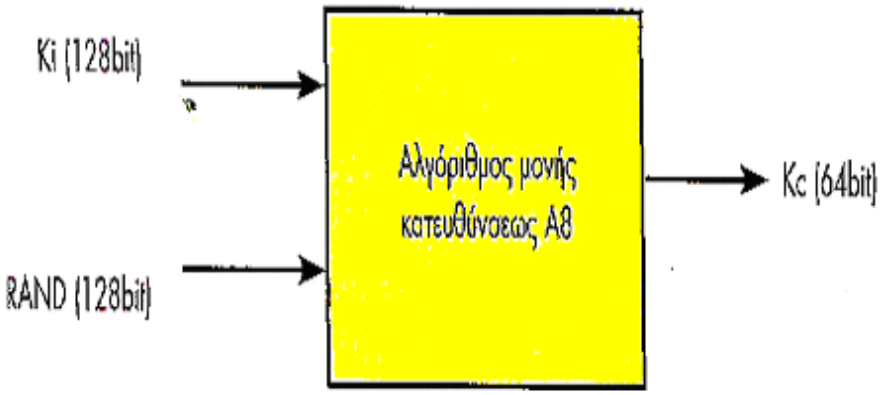
Η αλληλουχία των ενεργειών για την λήψη των τριάδων απεικονίζεται στο **σχήμα 2.**
Σε περίπτωση του κινητού τηλεφώνου σε διαφορετική χώρα (περιαγωγή) το ξένο δίκτυο ζητάει εκ των προτέρων μία τριάδα (SRES , Kc,RAND)και τη χρησιμοποιεί όταν το ζητήσει ο φιλοξενούμενος σταθμός . Έτσι ακόμα και το δίκτυο φιλοξενίας δεν γνωρίζει τον συνδυασμό A3 /A8 / Ki του φιλοξενουμένου.
Οι αλγόριθμοι A3 , A5 , A8.
Η μοναδικότητα τόσο των κλειδιών Ki αλλά και οι τιμές των τυχαίων αριθμών SRES και RAND ,εξασφαλίζουν την ύπαρξη άπειρων κλειδιών Kc .Με αυτόν τον τρόπο ο συνδρομητής διαθέτει συνεχώς νέους κωδικούς κρυπτογράφησης , για να μιλάει με ασφάλεια με άλλους συνδρομητές του δικτύου. Μία τουλάχιστον <<νέα >> τριάδα πρέπει να είναι διαθέσιμη κάθε στιγμή ,ανά συνδρομητή ,μέσα στην βάση ,για να χρησιμοποιηθεί μόλις ζητηθεί. Η πιστοποίηση του κινητού τηλεφώνου με το δίκτυο γίνεται ως εξής :
Όταν ο κινητός σταθμός αιτηθεί σύνδεση με την βάση , του αποστέλλεται από το κέντρο ελέγχου ο αριθμός RAND. Με την βοήθεια του αλγόριθμου A3 υπολογίζεται (στο κινητό τηλέφωνο) από τους Ki (128 bit) και RAND(128 bit) ,ο αριθμός SRES(32 bit). Αν ο αριθμός SRES είναι ο ίδιος με αυτόν που ήδη έχει υπολογίσει το κέντρο πιστοποίησης , τότε η σύνδεση προχωρεί. Από τους ίδιους αριθμούς Ki και RAND ο αλγόριθμος A8 υπολογίζει την κλείδα κρυπτογράφησης φωνής Kc (64 bit).Από τα 64 bitπου παράγει χρησιμοποιεί τα πρώτα 54 . Τα υπόλοιπα 10 αντικαθίστανται με μηδενικά .Η μείωση του μεγέθους από 64 σε 54 έχει δραματικές συνέπειες στην ισχύ του αλγορίθμου κρυπτογράφησης φωνής α5 και προβλέπεται σε όλους τους αλγόριθμους, που πιθανόν να χρησιμοποιηθούν στην θέση του A8. Αποτελεί μια από τις απαιτήσεις του συστήματος .Στην πράξη έχουν ενοποιηθεί οι δυο αλγόριθμοι σε έναν αλγόριθμο διπλής λειτουργίας ,που λέγεται A3 / A8 ή COMP 128,που παράγει μια ακολουθία 128 bit,που τα 36 πρώτα αποτελούν τον αριθμό SRES , ενώ τα τελευταία 54 σχηματίζουν την κλείδα Kc,ενώ τα ενδιάμεσα ψηφία δεν χρησιμοποιούνται . Οι λεπτομέρειες της δομής του COMP 128 δεν είναι δημοσίως γνωστές αλλά με επίμονη διαδικασία ανάλυσης πάνω σε κάρτες SIM(ανάστροφη αποδόμηση , reserve engineering) αναλύθηκε πλήρως . **(σχήμα 3)**



Διαδικασία πιστοποίησης του κινητού τηλεφώνου στο δίκτυο. Στο κέντρο πιστοποίησης (AUC) του φορέα παροχής υπηρεσιών κινητής τηλεφωνίας, φυλάσσονται οι κλείδες ασφαλείας Ki όλων των συνδρομητών. Η ίδια κλείδα φυλάσσεται και στη συσκευή του συνδρομητή, μέσα στην κάρτα SIM. Το AUC παράγει μία τριάδα κωδικών που περιέχουν:

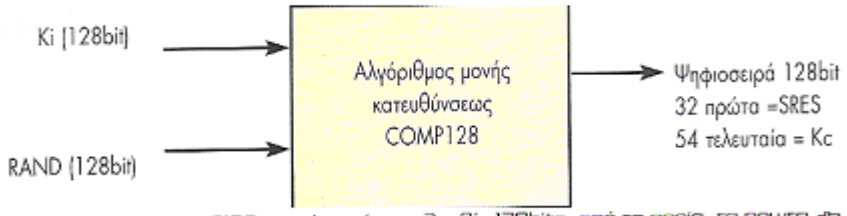
- ένα τυχαίο αριθμό RAND,
- το αποτέλεσμα SRES του αλγόριθμου (A3, Ki)
- το αποτέλεσμα Kc του αλγόριθμου πιστοποίησης A8.

Κάθε τέτοια τριάδα υπάρχει στο φορέα και είναι διαθέσιμη όταν τη ζητήσει ο συνδρομητής. Μόλις ο κινητός σταθμός αιτηθεί σύνδεση, του αποστέλλεται από το κέντρο ο αριθμός RAND. Η συσκευή του συνδρομητή υπολογίζει το SRES με τη βοήθεια των Ki, A8. Αν το SRES είναι το ίδιο με αυτό που έχει ήδη υπολογίσει το κέντρο πιστοποίησης, τότε η σύνδεση προχωρεί, αν όχι, η αίτηση απορρίπτεται. Η σύνδεση ολοκληρώνεται και αρχίζει η μεταβίβαση των δεδομένων που κρυπτογραφούνται με τον αλγόριθμο A5.



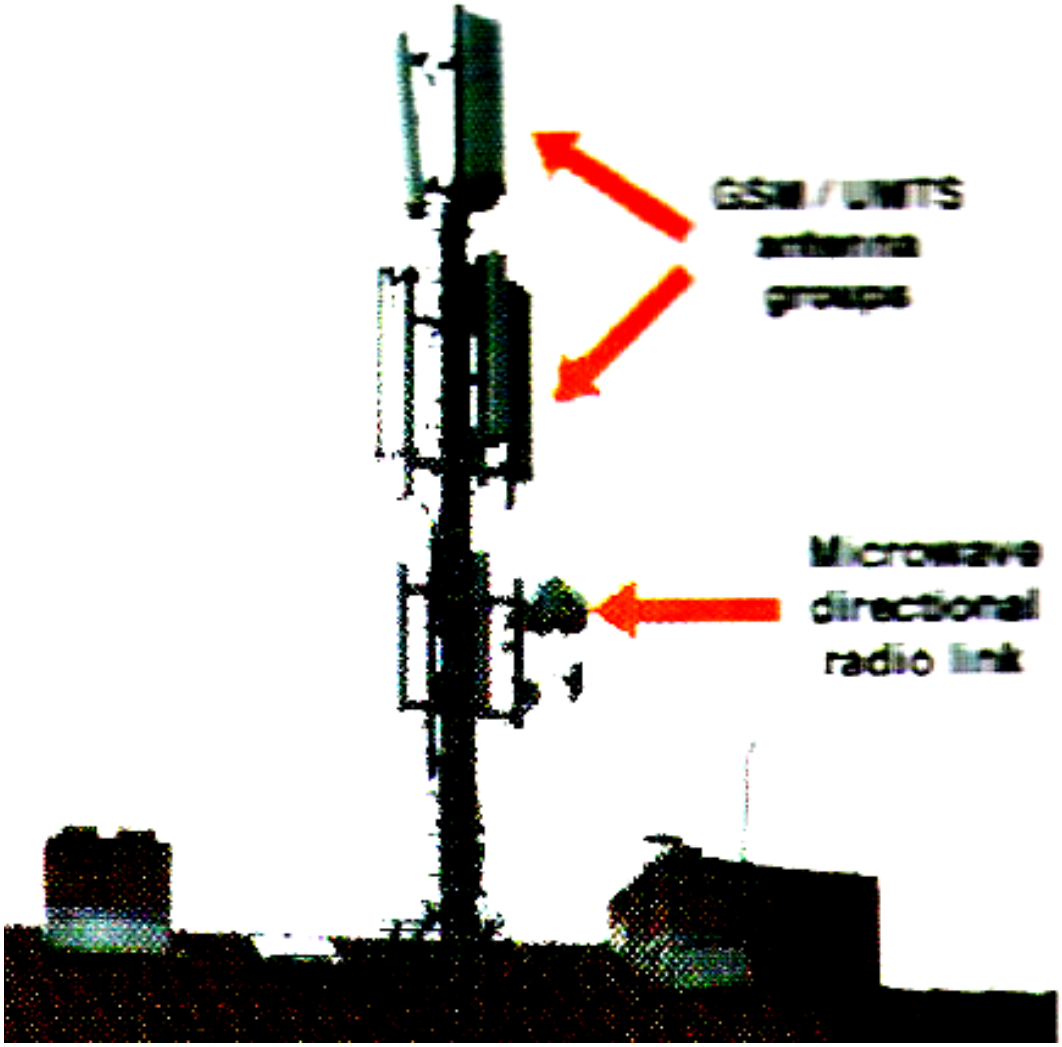
Παραγωγή της κλείδας κρυπτογράφησης φωνής Kc (64bit) από την κλείδα Ki (128bit) και τον τυχαίο αριθμό RAND (128bit), μέσω της μονόδρομης συνάρτησης A8. Η κλείδα Kc παραμένει η ίδια για όλες τις συνομιλίες, όσο ο κινητός σταθμός διατηρεί τη σύνδεσή του με το σταθμό βάσης. Αλλάζει μόνον όταν ο σταθμός αιτήσει νέα πιστοποίηση ταυτότητας. Από τα 64 bit που παράγει ο κώδικας, χρησιμοποιούνται μόνο τα πρώτα 54. Τα υπόλοιπα 10 ανακαθίστανται με μηδενικά.

σχήμα 2



Ο αλγόριθμος COMP128 παράγει μία ακολουθία 128bits, από το οποίο, τα πρώτα 32 αποτελούν τον αριθμό SRES, ενώ τα τελευταία 54 αχημοτίζουν την κλείδα Kc. Η κλείδα Kc θα έπρεπε να έχει μέγεθος 64bits, αλλά πιέσεις για περιορισμό της ισχύος κρυπτογράφησης «ανάγκασαν» τους σχεδιαστές του συστήματος να απλόξουν τις αρχικές απαιτήσεις τους. Το ενδιάμεσο ψηφίο δεν χρησιμοποιούνται. Όταν προτάθηκε από τη γερμανική εταιρεία AEG, τα περισσότερα δίκτυα το δέχθηκαν σαν τον «από μηχανής θεό», αφού δεν προβλέπεται από την αρχική σχεδίαση του συστήματος GSM. Είναι άγνωστο πόσο δίκτυο δεν χρησιμοποιούν αυτόν τον αλγόριθμο και έχουν αναπτύξει κάποιο δικό τους. Πιθανολογείται ότι είναι ελάχιστα. Υπάρχουν ενδείξεις ότι λόγω των προβλημάτων ασφαλείας, υπάρχει πρόταση αντικατάστασης του COMP128 με μία νεώτερη έκδοση COMP128-2, για την οποία υπάρχουν ελάχιστα γνωστά στοιχεία.

σχήμα 3

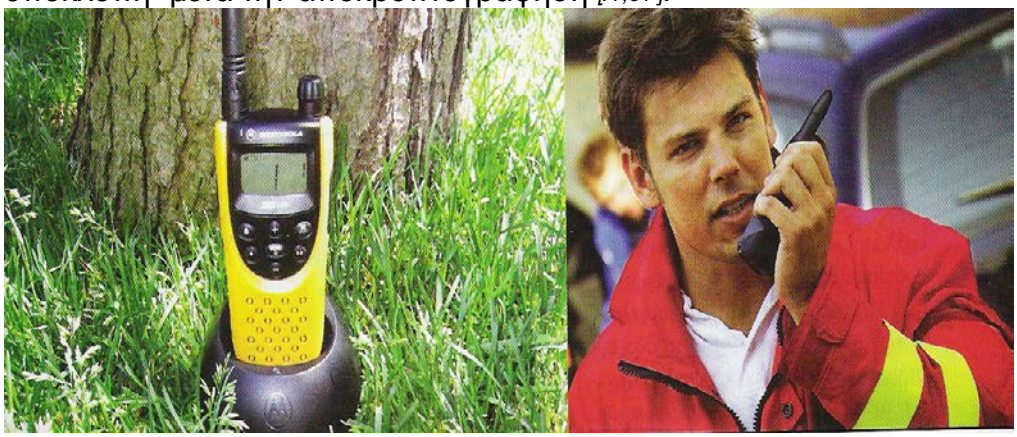


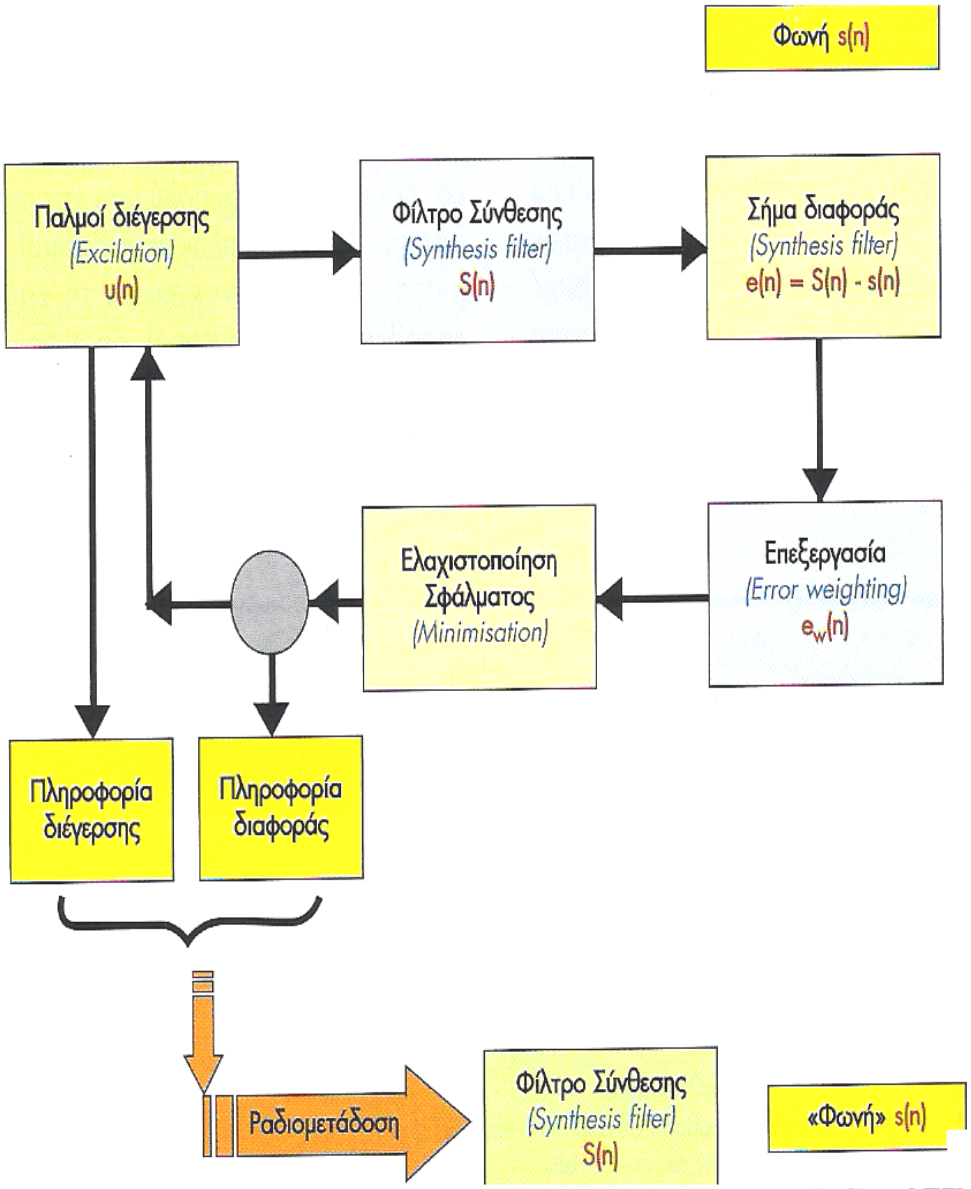
ΣΧΗΜΑ 4[Β',9]

Όσοι δεν έχουν πρόσβαση στο λογισμικό της νόμιμης συνακρόασης μπορούν να χρησιμοποιήσουν εναλλακτικές μεθόδους .Σύμφωνα με την εφημερίδα The Sunday Times του Λονδίνου κάποια εταιρεία που ειδικεύεται στην πώληση συσκευών υποκλοπής σημάτων GSM,στην τιμή των 250.008 ευρώ. Στην πραγματικότητα η συσκευή αυτή δεν υποκλέπτει τις απευθείας συνδέσεις των κινητών τηλεφώνων αλλά παρακολουθεί την μικροκυματική ζεύξη μεταξύ των σταθμών βάσεως και του κεντρικού δικτύου.(Microwave directional radio link),η οποία μεταφέρει πολλές τηλεφωνικές διοδεύσεις ,με την γνωστή τεχνική παλμοκωδικής διαμόρφωσης .(PCM) .Οι διοδεύσεις αυτές μπορεί να είναι ψηφιακές και πολυπλεγμένες φασματικά , δεν είναι όμως κρυπτογραφημένες .Οι μικροκυματικές ζεύξεις χρησιμοποιούν συχνότητες στην περιοχή των 236 Hz ή 386 Hz .(ΣΧΗΜΑ 4)
Και δέκτες για τέτοιες συχνότητες δύσκολα βρίσκονται στην αγορά. Παράλληλα οι εκπομπές είναι εξαιρετικά κατευθυνόμενες και ο δέκτης θα πρέπει να βρίσκεται μέσα στο λοβό εκπομπής – λήψης . [Β',9]

Ανασφάλειες στο σύστημα TETPA , οι διαδικασίες του και σχηματικές παραστάσεις του συστήματος. *[Α',51]*

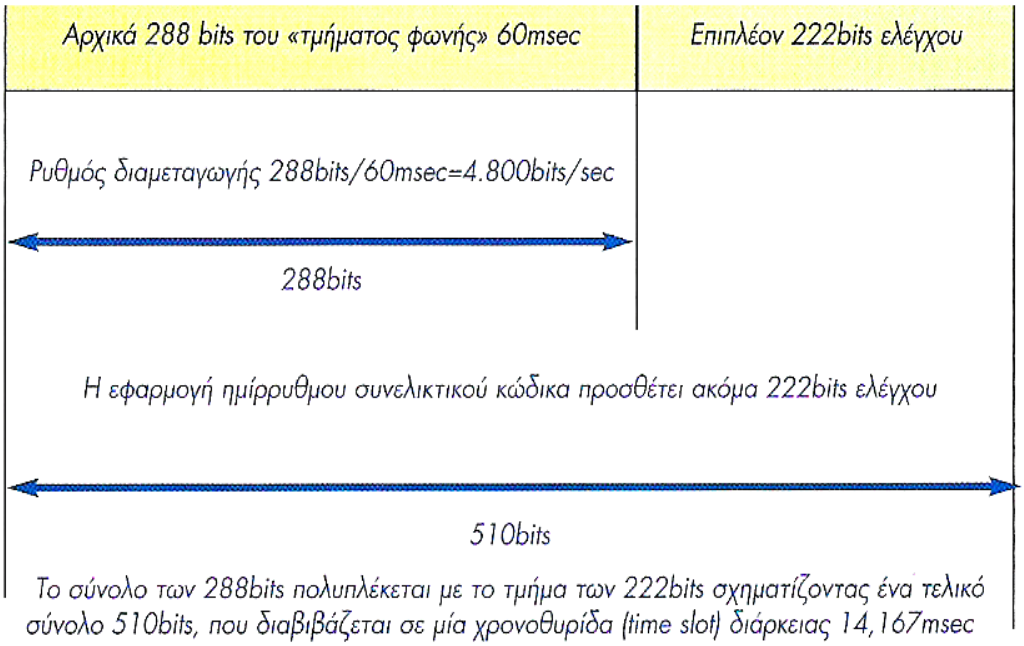
Τα TETPA είναι ένα πολύ ασφαλές σύστημα επικοινωνιών και δεν υπάρχει πρόβλημα εσωτερικής υποκλοπής κατά την ώρα της μεταφοράς .Όμως στο σύστημα TETPA οι κλείδες με τις οποίες γίνεται η αποδοχή ενός τερματικού στο σύστημα βρίσκονται στην εξουσία του προμηθευτή . Η δυναμική κρυπτογράφηση των επικοινωνιών (αυτόματη αλλαγή κωδικού με κάθε χρήση) ελέγχεται από το υπουργείο Εσωτερικών της Ολλανδίας ,που είναι για αυτό εξουσιοδοτημένο από την Ε.Ε , καθώς τα συστήματα TETPA έχουν αναπτυχθεί πανευρωπαϊκά στο πλαίσιο εφαρμογής της συνθήκης Σέγκεν . Ο αλγόριθμος , με βάση τον οποίο γίνεται η κρυπτογράφηση του συστήματος και η αυτόματη αλλαγή των κωδικών , δεν καθορίζεται από τις ελληνικές αρχές , γιατί δεν υπάρχει εξειδικευμένη επιστημονική ομάδα και τα <<κλειδιά >> τα διαχειρίζεται η προμηθεύτρια αμερικανική εταιρεία SAIC. Σύμφωνα με το υπουργείο Δημοσίας Τάξης , η SAIC, ενώ ήταν υποχρεωμένη να προμηθεύσει την κυβέρνηση με συσκευές υψηλής ασφάλειας με κρυπτοφώνηση <<security class 3 >> , της παρέδωσε τελικά το << security class 1 >>χωρίς κρυπτοφώνηση .Από αυτά συμπεράνουμε ότι ενώ τα συστήματα είναι ασφαλές από υποκλοπές από εξωγενείς παράγοντες, αν τα κλειδιά της διαχείρισης ,ασφάλειας έχουν παραδοθεί σε τρίτους για διαφόρους λόγους τότε δεν υπάρχει ασφάλεια από την συνακρόαση , υποκλοπή μετά την αποκρυπτογράφηση *[Α',51]*.



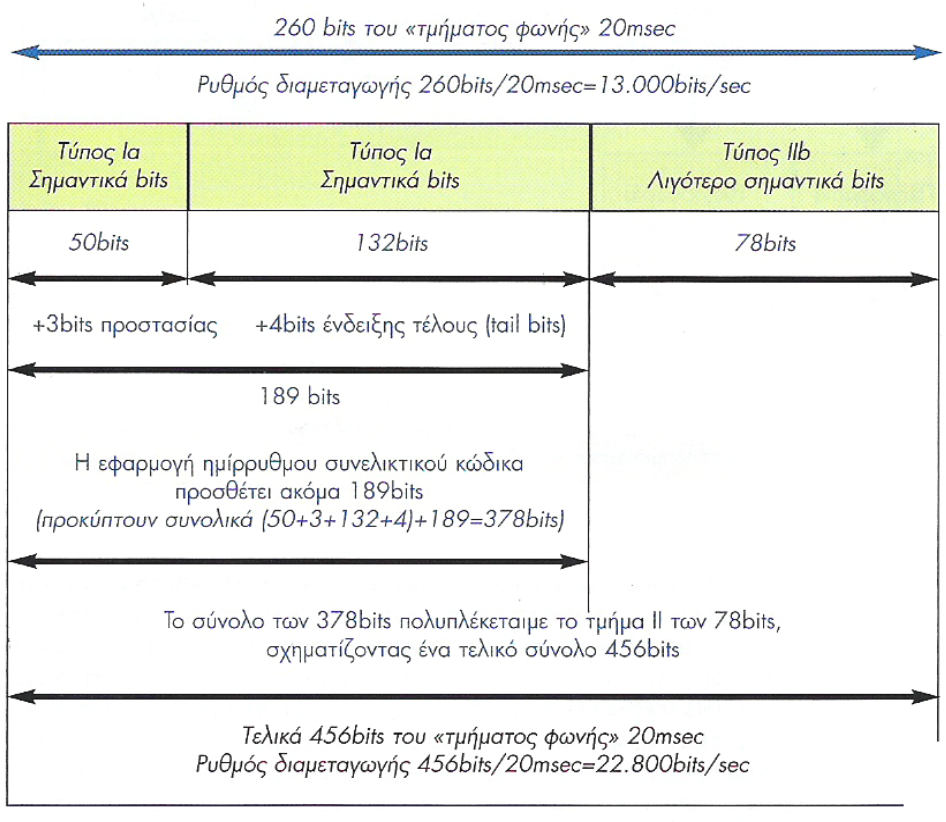


Κωδικοποίηση φωνής με γραμμική πρόβλεψη (Linear Predictive Coding, LPC):

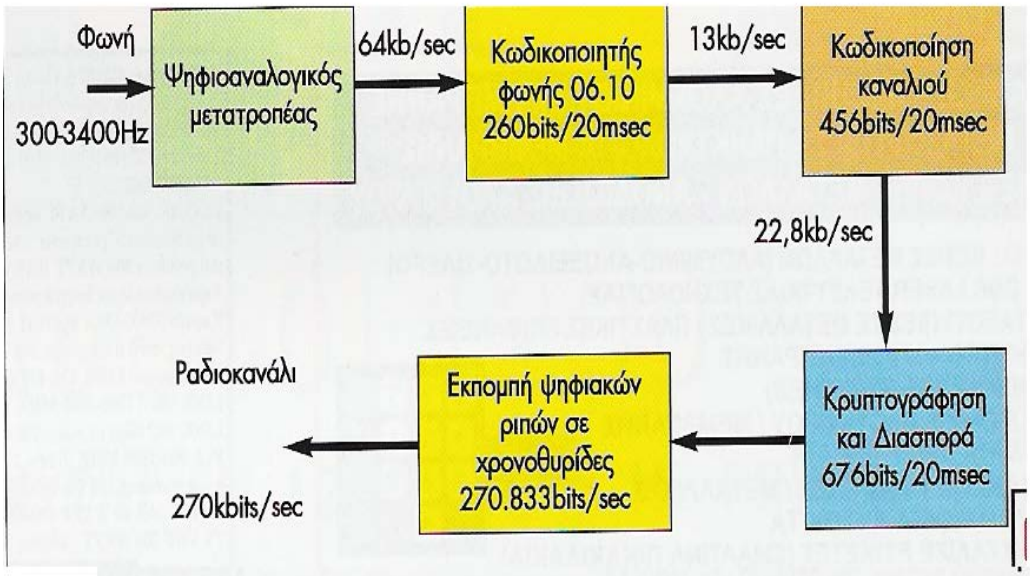
Το σήμα φωνής s(n) «σπάει» σε πλαίσια (frames) με τυπική διάρκεια 20msec. Την ίδια στιγμή παράγεται από ένα ειδικό κύκλωμα που λέγεται «διεγέρτης» (exciter), μία ακολουθία παλμών u(n), η οποία οδηγείται στο φίλτρο σύνθεσης. Το φίλτρο «επιλέγει» μία σειρά από παραμέτρους, από μία «βιβλιοθήκη έτοιμων παραμέτρων» και προσπαθεί να μετατρέψει την ακολουθία παλμών σε σήμα S(n), που να μοιάζει με το «κομμάτι» της φωνής. Αυτό γίνεται με μία διαδικασία δοκιμής και απόρριψης, μέχρις ότου η διαφορά σφάλματος e(n) των δύο σημάτων να ελαχιστοποιηθεί. Ο κωδικοποιητής (encoder) αναλύει το εισερχόμενο σήμα φωνής, συνθέτοντας πολλές διαφορετικές προσεγγίσεις, μέχρι να βρεθεί αυτή που ταιριάζει περισσότερο. Όταν βρεθεί η βέλτιστη, οι παράμετροι του φίλτρου και οι πληροφορίες για την ακολουθία παλμών διέγερσης διαβιβάζονται στον αποκωδικοποιητή (decoder), ο οποίος ανασυνθέτει το συγκεκριμένο τμήμα του σήματος φωνής.



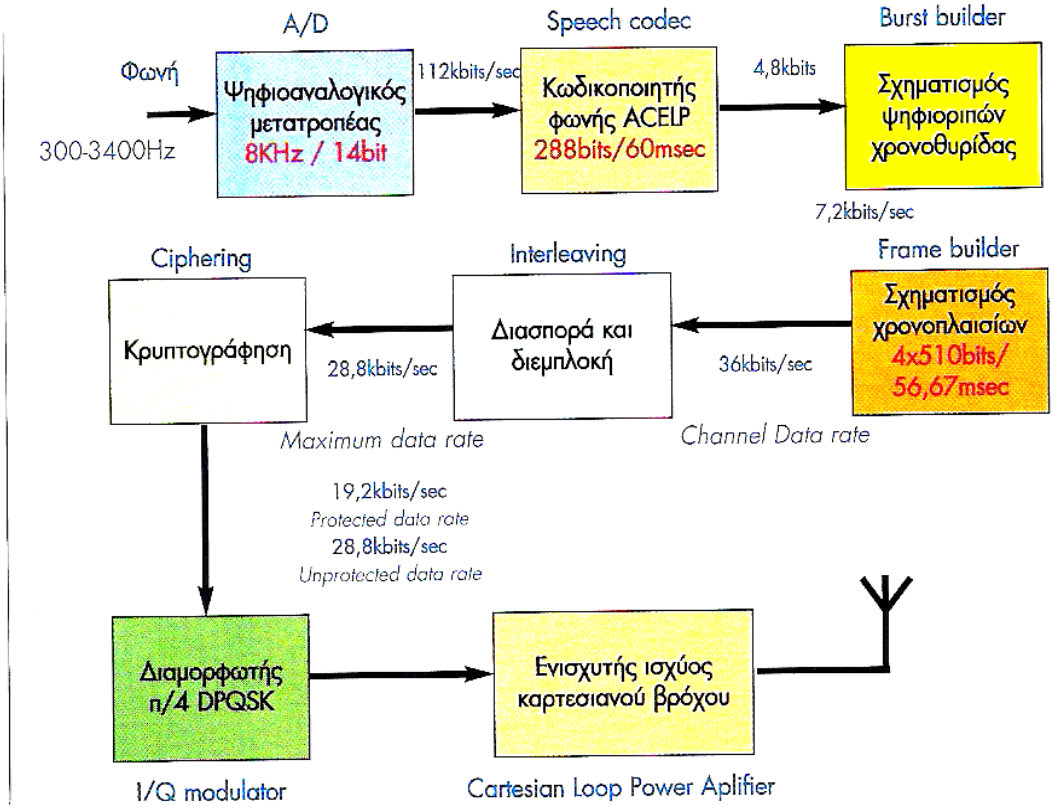
Codec ACELP (TETRA). Δομή του τμήματος (πλαισίου-frame) των 510bits ανά ακουστικό «δείγμα» διάρκειας 60msec, από το αρχικό δείγμα 288bits, που παράγει ψηφιοσειρά με ταχύτητα 4.8kbps και οδηγεί σε ταχύτητα μετάδοσης του ψηφιακού συστήματος 28.8kbps



Codec LPC 06.10 (GSM). Δομή του τμήματος (πλαισίου-frame) των 260bits ανά ακουστικό «δείγμα» διάρκειας 20msec, που παράγει ψηφιοσειρά με ταχύτητα 13kbps και οδηγεί σε ταχύτητα μετάδοσης του ψηφιακού συστήματος 23.8kbps



Βασικές βαθμίδες και αλληλουχία των ρυθμών που ακολουθούν τα δυαδικά ψηφία, κατά την αύξηση του ρυθμού διαμεταγωγής από βαθμίδα σε βαθμίδα, του τμήματος εκπομπής ενός κινητού τηλεφώνου.

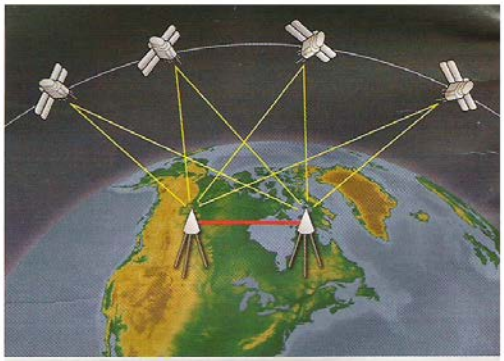


Βασικές βαθμίδες του πομποδέκτη TETRA. Απεικονίζονται παράλληλα οι ταχύτητες διαμεταγωγής της ψηφιακής πληροφορίας, από βαθμίδα σε βαθμίδα, για το τμήμα εκπομπής. Για το τμήμα λήψης, είναι η ακριβώς αντίστροφη. Πρόκειται για ένα ολοκληρωμένο «ψηφιακό εργοστάσιο». Δεν θυμίζει σε τίποτα την κλασική δομή ενός πομπού VHF.

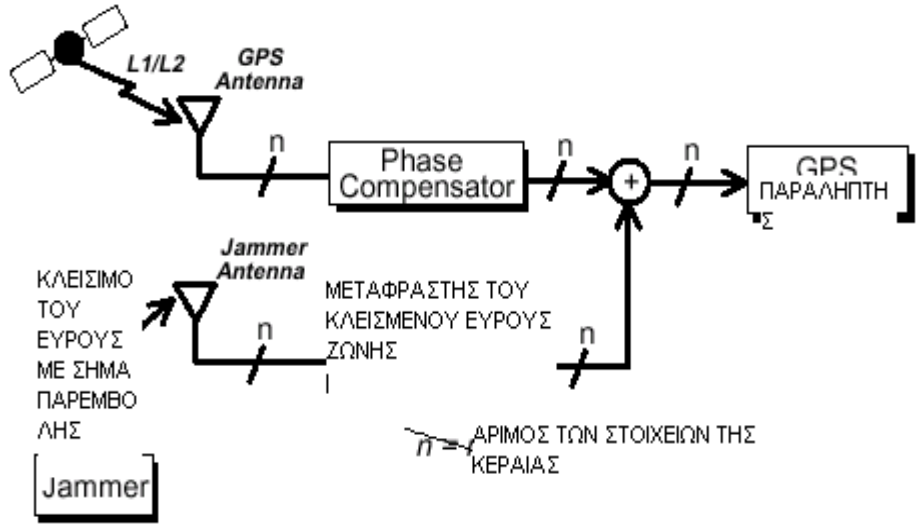
GPS και jamming

Τα τελευταία χρόνια αναπτύχθηκε ένα σύστημα εντοπισμού και πλοήγησης, το GPS (Global Positioning System) ,που βασίζεται σε δορυφορικό και επίγειο δίκτυο και έχει πολλές εφαρμογές σε πολλούς τομείς της ζωής μας. Εφόσον η μετάδοση σημάτων στο GPS γίνεται με ηλεκτρομαγνητικά κύματα και μέσο μετάδοσης είναι ο αέρας ,γίνεται να κάνουν jamming και σε αυτό το σύστημα με παρόμοιους τρόπους με αυτούς που κάνουν στο GSM και WLAN, με ορισμένες διαφοροποιήσεις .Επειδή το GPS (Global Positioning System) έχει πολλές εφαρμογές στην πλοήγηση πλοίων ,αεροπλάνων και σε άλλες περιπτώσεις το jamming σε αυτό είναι πολύ επικίνδυνο.

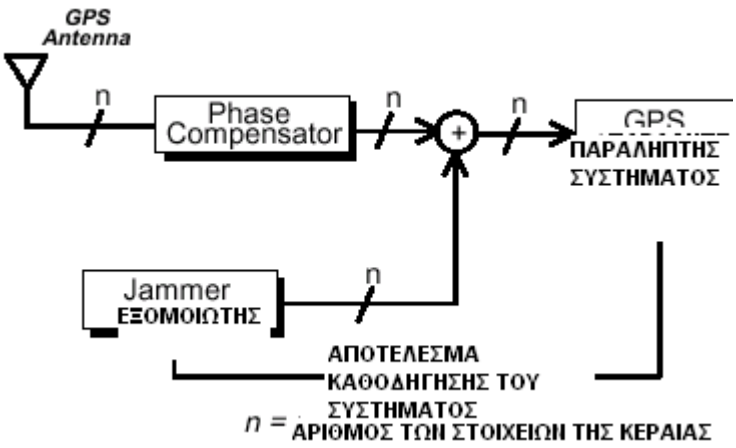
Οι πρώτες εφαρμογές της τεχνολογίας GPS αφορούσαν στη ναυτιλία και την αεροπλοΐα. Στις φωτογραφίες διακρίνεται το εντυπωσιακό εσωτερικό δύο μικρών αεροσκαφών τύπου Cessna.



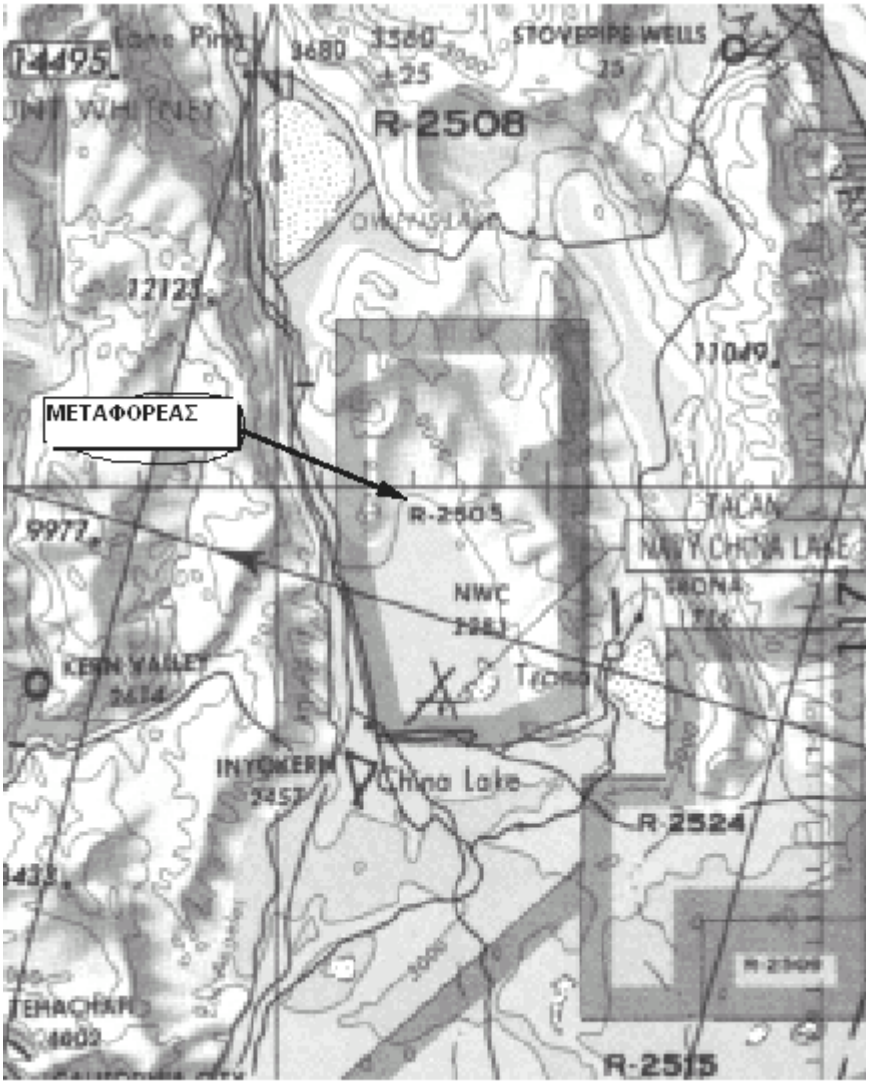
Το σύστημα GPS στηρίζεται στη χρήση δορυφόρων και αντίστοιχων επίγειων σταθμών επικοινωνίας, οι οποίοι συνδυάζουν τα στίγματα κάθε πομπού, υπολογίζοντας την ακριβή θέση του. Όσο περισσότεροι είναι οι δορυφόροι με τους οποίους συνδέεται ταυτόχρονα ένα σύστημα GPS, τόσο πιο ακριβείς είναι οι πληροφορίες που το χαρακτηρίζουν.



ΜΕΤΑΦΡΑΣΤΗΣ ΣΥΧΝΟΤΗΤΑΣ GPS ΠΟΥ ΔΕΧΤΗΚΕ JAMMING

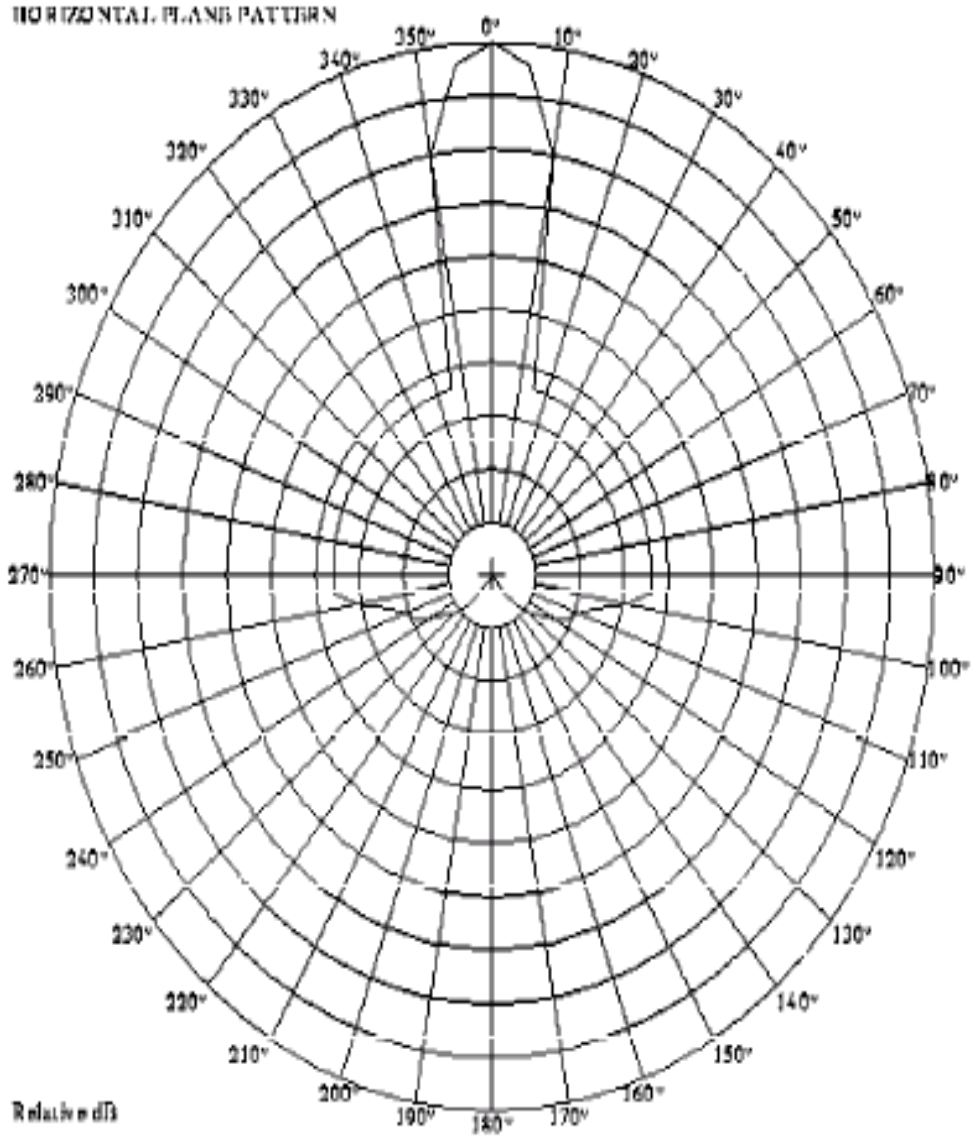


ΕΝΑ ΣΥΣΤΗΜΑ ΕΞΟΜΟΙΩΣΗΣ GPS ΠΟΥ ΔΕΧΤΗΚΕ JAMMING



ΠΑΡΑΔΕΙΓΜΑ ΔΗΜΙΟΥΡΓΙΑΣ (ΤΟΠΟΘΕΤΗΣΗΣ) ΕΝΟΣ JAMMER

Για να τοποθετηθεί ένας jammer και για να είναι αποτελεσματικό το jamming του θα πρέπει να γίνουν ορισμένες ρυθμίσεις και κυρίως στην κεραία εκπομπής του.Η πρώτη ρύθμιση για 10 k W ERP ενός άμεσου jammer είναι να χρησιμοποιεί μια κεραία με 20 – βαθμούς κάθετα και οριζόντια ακτίνα εύρους όπως απεικονίζεται στο παρακάτω σχήμα .Το σύστημα κεραίας έχει κατεύθυνση 40 –βαθμούς νοτιοανατολικά .

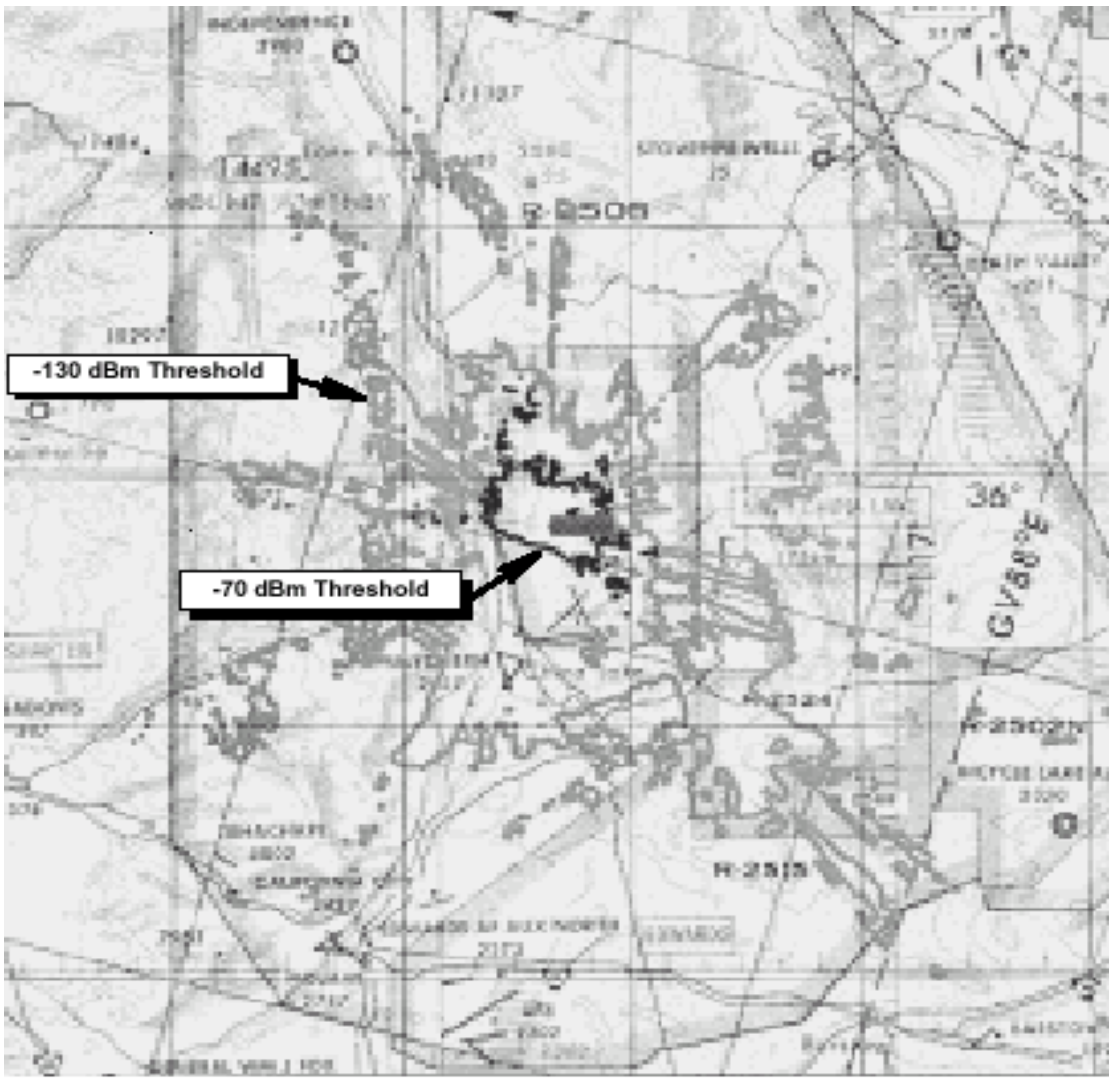


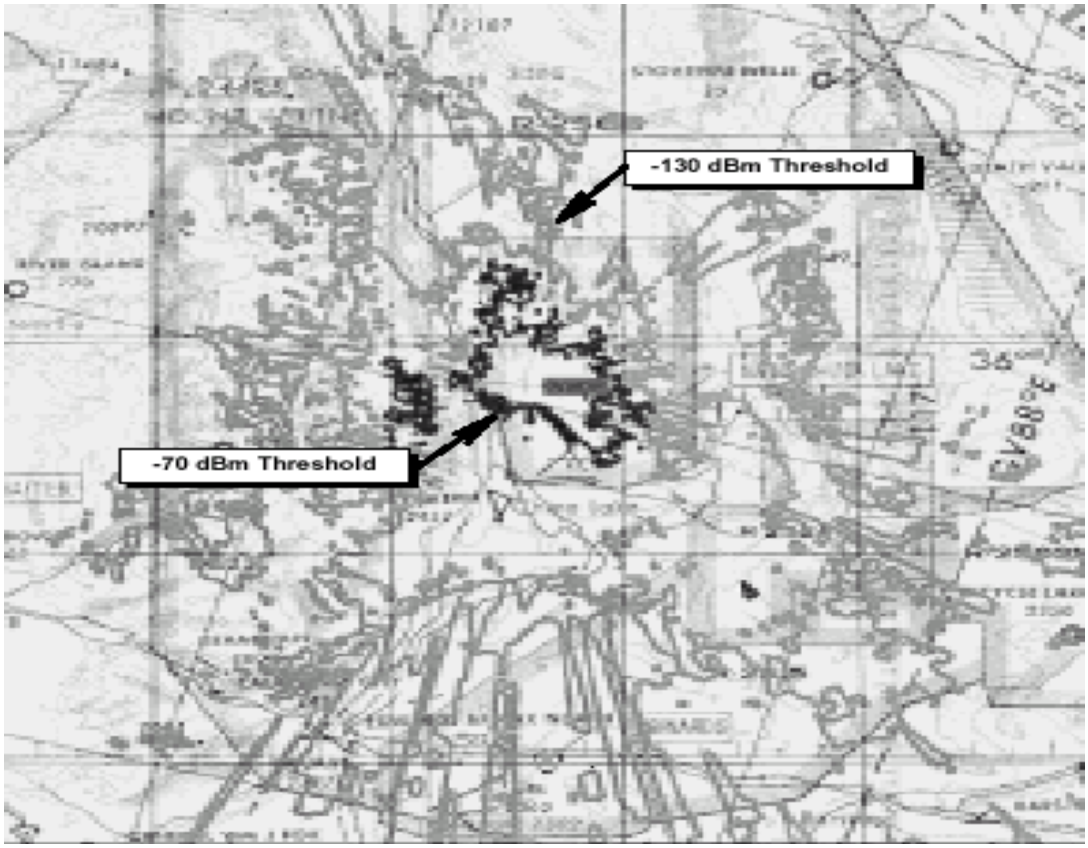
ΟΡΙΖΟΝΤΙΟ (ΡΑΔΙΟΓΡΑΜΜΑ) ΣΧΗΜΑ ΓΙΑ ΑΜΕΣΟ JAMMER

ΓΕΩΓΡΑΦΙΚΗ ΘΕΣΗ ΤΟΥ *Jammer*	N35° 54' 6.50" W117° 43' 0.30"
ΙΣΧΥΣ	10 kW ERP
ΚΕΡΑΙΑ *Elevation*	2361.5' MSL (ΠΑΤΩΜΑ ΚΟΙΛΑΔΑΣ)
ΚΕΡΑΙΑ ΛΗΨΗΣ	ΙΣΟΤΡΟΠΙΚΗ
ΚΕΡΑΙΑ ΛΗΨΗΣ *Elevation*	100.0' AGL
ΣΥΧΝΟΤΗΤΑ	L1 (1575.42 MHz)
ΠΡΟΒΛΕΨΗ ΕΜΠΙΣΤΟΣΥΝΗΣ	0.0 dB
ΑΤΜΟΣΦΑΙΡΙΚΗ ΑΠΟΡΡΟΦΗΣΗ	ΔΕΝ ΥΠΑΡΧΕΙ
K ΠΑΡΑΓΟΝΤΑΣ	1.33
ΤΥΠΟΣ ΜΕΛΕΤΗΣ	50% ΧΡΟΝΟΣ ; 50% ΓΕΩΓΡΑΦΙΚΗ ΘΕΣΗ

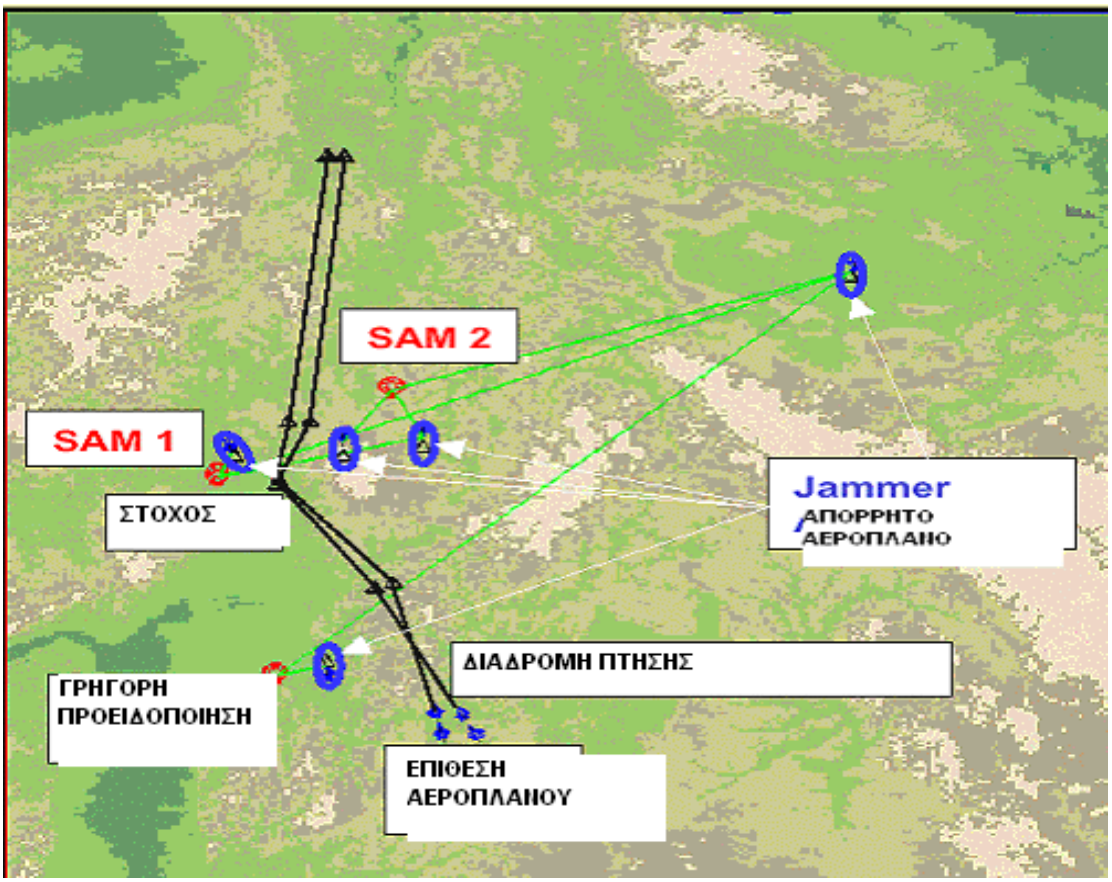
Table 1 *TIREM Propagation Model Parameters*

Στο παρακάτω σχήμα απεικονίζονται οι επιδράσεις μιας απευθείας παρεμβολής στις κεραίες ,μας δείχνει ότι η τοποθεσία (στόχος) είναι διαφορετική από την πραγματική.



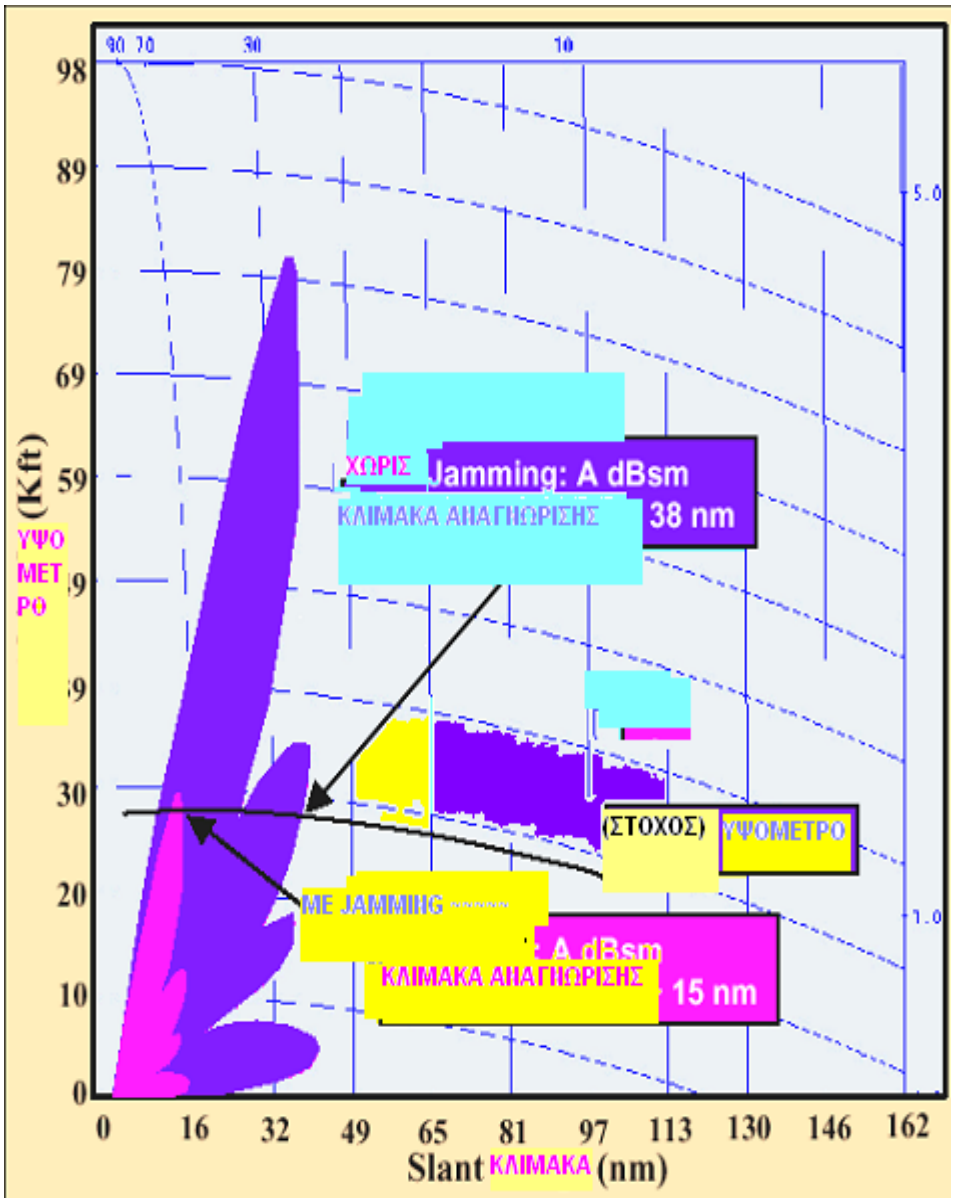


σχημα . βλέπουμε το γεωγραφικό σχέδιο πως απεικονίζεται αν έχει υποστεί jamming 10 k W και αν όχι . Παρατηρούμε ότι η γεωγραφική θέση μετά το jamming είναι εσφαλμένη .



Χαρακτηριστικά της επίθεσης.
Μπλε συστήματα
τέσσερις επιθέσεις αεροπλάνου (αερομαχίες)
ταχύτητα 350 knots
υψόμετρο =~ 27 K ft
διαδρομή πτήσης = από νότια σε βόρεια
επτά επιθέσεις jammer αεροπλάνων
υψόμετρο =~ 27 K ft με χαμηλή πτήση

ΜΟΝΤΕΛΟ ΕΝΟΣ ΡΑΝΤΑΡ ΣΤΟ EAD SIM(ΕΞΟΜΟΙΩΤΗ) .Βασικοί παράμετροι είναι η συχνότητα , ακτίνα δράσης , παραμέτρους σάρωσης , ισχύς , κ.λ.π. Υπάρχει ικανότητα συνδυασμού μιας κεραίας που έχει σχεδιαστεί για να προσδιορίζει ένα ραντάρ ακριβώς .



[Γ ’,70]
Οι πληροφορίες για το GPS πάρθηκαν από το

ΑΣΦΑΛΗ ΜΕΤΑΔΟΣΗ ΠΛΗΡΟΦΟΡΙΩΝ

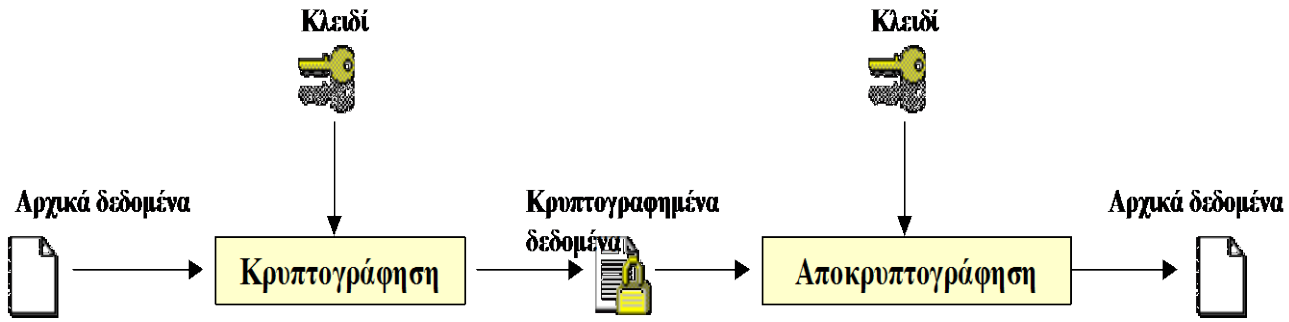
Α) ΤΙ ΕΙΝΑΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΚΑΙ ΤΙ ΚΡΥΠΤΑΝΑΛΥΣΗ

Ένα κρυπτογραφικό σύστημα που μεταδίδει δεδομένα κρύβοντάς τα μέσα σε χάος δοκιμάστηκε για πρώτη φορά υπό πραγματικές συνθήκες σε μητροπολιτικό δίκτυο οπτικών της Αθήνας, στο πλαίσιο ευρωπαϊκού ερευνητικού προγράμματος. Η έρευνα, που περιγράφεται στο έγκριτο περιοδικό Nature και μάλιστα έγινε εξώφυλλο στο περιοδικό New Scientist, βασίζεται σε έναν οπτικό πομπό λέιζερ, ο οποίος εκπέμπει χαοτική ακτινοβολία μέσα στην οποία κωδικοποιείται η προς μετάδοση πληροφορία. Στην άλλη άκρη της οπτικής ίνας, μια πανομοιότυπη συσκευή αντιστρέφει τη διαδικασία και αναλαμβάνει να διαχωρίσει το χάος από την πληροφορία, εξηγεί στο in.gr/news ο καθηγητής Δημήτρης Συβρίδης του Τμήματος Πληροφορικής και Τηλεπικοινωνιών του Πανεπιστημίου Αθηνών, επικεφαλής της ομάδας. Η δεύτερη αυτή συσκευή είναι ουσιαστικά το κλειδί για την αποκρυπτογράφηση, καθώς η λειτουργία της εξαρτάται από τα μοναδικά φυσικά της χαρακτηριστικά. Ακόμα και αν κάποιος ωτακουστής κατάφερνε να υποκλέψει τη μετάδοση, χωρίς το κλειδί το μόνο που θα μπορούσε να διαβάσει θα ήταν χάος. Αν και η τεχνολογία αυτή είχε φανεί υποσχόμενη σε θεωρητικό επίπεδο, το πείραμα στην Αθήνα επιβεβαιώνει για πρώτη φορά ότι είναι δυνατή η εφαρμογή της σε εμπορικά δίκτυα οπτικών ινών.Η μετάδοση έγινε στο μητροπολιτικό δίκτυο οπτικών ινών της «Αττικές Τηλεπικοινωνίες ΑΕ». Το σήμα ξεκίνησε από το εργαστήριο των ερευνητών στην Πανεπιστημιούπολη Ζωγράφου και κατέληξε πάλι εκεί έχοντας διανύσει συνολική απόσταση 120 χιλιομέτρων.

Χαοτικός ταλαντωτής

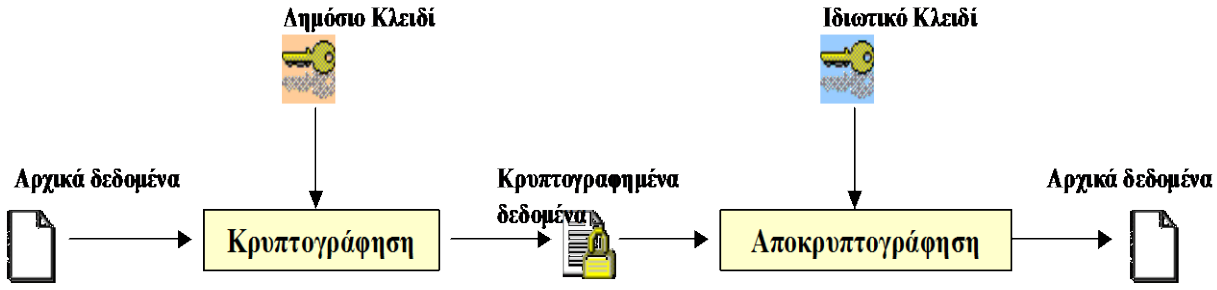
Τα λέιζερ, που χρησιμοποιούνται ως οπτικοί πομποί στις τηλεπικοινωνίες, κανονικά είναι αρμονικοί ταλαντωτές, δηλαδή παράγουν ένα σύμφωνο, μονοχρωματικό ηλεκτρομαγνητικό κύμα. Κάτω από κατάλληλες ειδικές συνθήκες, το λέιζερ μπορεί να γίνει ασταθές και να μετατραπεί σε χαοτικό ταλαντωτή, ο οποίος παράγει ηλεκτρομαγνητική ακτινοβολία μεγάλου φασματικού εύρους. Στην τελευταία έρευνα οι επιστήμονες μπόρεσαν να κρύψουν την πληροφορία μέσα σε αυτή την χαοτική ταλάντωση, αξιοποιώντας ένα πολύ μικρό, δυσδιάκριτο τμήμα του φάσματός της.Τα δεδομένα δεν χάνονται, καθώς το χάος εμπεριέχει οργάνωση και δεν είναι θόρυβος. Το λέιζερ-δέκτης αντιστρέφει τη διαδικασία και έτσι ο παραλήπτης του μηνύματος μπορεί να αφαιρέσει το χάος από το σήμα και να ανακτήσει την αρχική πληροφορία. Το τελευταίο πείραμα έδειξε ότι η διάταξη είναι αποτελεσματική στην αξιόπιστη μετάδοση δεδομένων με ταχύτητες έως και 2,4 gigabit/sec. «Τα αποτελέσματά μας δείχνουν ότι πληροφορία μπορεί να μεταδοθεί σε υψηλούς ρυθμούς χρησιμοποιώντας ντετερμινιστικό χάος» αναφέρει η δημοσίευση, με πρώτο συγγραφέα τον υποψήφιο διδάκτορα Απόστολο Αργύρη.

Με τον όρο *κρυπτογράφηση δεδομένων* εννοούμε τη διαδικασία μετατροπής των δεδομένων σε μία μορφή στη οποία θα αποκρύπτεται το περιεχόμενο τους. Η αντίστροφη διαδικασία ανάκτησης των αρχικών δεδομένων από κρυπτογραφημένο κείμενο ονομάζεται *αποκρυπτογράφηση*. Η κρυπτογράφηση πραγματοποιείται με τη χρήση ενός *κρυπτογραφικού αλγορίθμου* και ενός *κλειδιού*. Ο κρυπτογραφικός αλγόριθμος είναι μία μαθηματική συνάρτηση που παίρνει ως είσοδο τα δεδομένα της κρυπτογράφησης ή της αποκρυπτογράφησης και με τη χρήση του κλειδιού (που λειτουργεί ως παράμετρος) παράγει ως έξοδο τα κρυπτογραφημένα ή αποκρυπτογραφημένα δεδομένα αντίστοιχα.Υπάρχουν δύο τύποι κρυπτογραφικών αλγορίθμων, οι *συμμετρικοί* και οι *ασύμμετροι*, και δύο αντίστοιχοι τύποι μηχανισμών κρυπτογράφησης: η *συμμετρική* και η *ασύμμετρη*. Η τελευταία είναι γνωστή και ως *κρυπτογράφηση δημόσιου κλειδιού*. Κατά τη συμμετρική κρυπτογράφηση, χρησιμοποιείται το ίδιο κλειδί τόσο κατά τη κρυπτογράφηση όσο και κατά την αποκρυπτογράφηση των δεδομένων. Αυτό σημαίνει ότι κατά τη ανταλλαγή κρυπτογραφημένων δεδομένων μεταξύ δύο οντοτήτων, πρέπει και οι δύο οντότητες να γνωρίζουν το κοινό κλειδί, ώστε να μπορούν αντίστοιχα να «κλειδώνουν» και να «ξεκλειδώνουν» τα δεδομένα, όπως φαίνεται στο επόμενο Σχήμα.



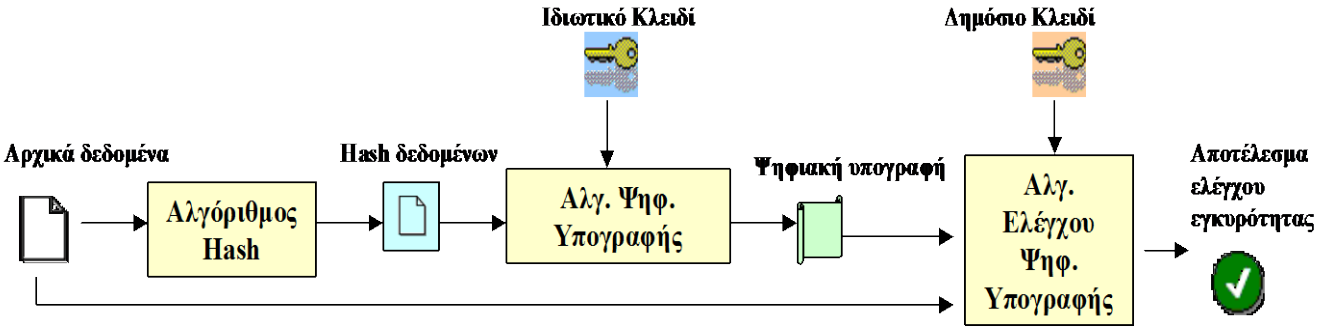
Σχήμα 5.1: Συμμετρική κρυπτογράφηση – αποκρυπτογράφηση

Η ιδιότητα της ασύμμετρης κρυπτογράφησης είναι ότι όταν τα δεδομένα είναι κρυπτογραφημένα με το ένα από τα δύο κλειδιά μπορεί να αποκρυπτογραφηθούν μόνο με το άλλο. Έτσι, στη περίπτωση που μια οντότητα Α θέλει να στείλει κρυπτογραφημένα δεδομένα σε μια οντότητα Β, κρυπτογραφεί με το δημόσιο κλειδί της Β (που είναι προσβάσιμο από όλους). Στη συνέχεια η Β αποκρυπτογραφεί με το ιδιωτικό της κλειδί (που είναι προσβάσιμο μόνο από αυτή).



Σχήμα 5.2: Ασύμμετρη κρυπτογράφηση – αποκρυπτογράφηση

Κατά την ασύμμετρη κρυπτογράφηση χρησιμοποιούνται δύο διαφορετικά κλειδιά (ή αλλιώς ένα *ζεύγος κλειδιών*). Το πρώτο κλειδί καλείται *«δημόσιο»* και είναι διαθέσιμο σε όλες τις ενδιαφερόμενες οντότητες. Το δεύτερο κλειδί καλείται *«ιδιωτικό»* και πρέπει να είναι διαθέσιμο μόνο στον κάτοχο του. Ένας σημαντικός μηχανισμός που στηρίζεται στη ασύμμετρη κρυπτογράφηση είναι ο μηχανισμός της *ψηφιακής υπογραφής*. Ως ψηφιακή υπογραφή ορίζεται «ένας κρυπτογραφικός μετασχηματισμός που επιτρέπει στον αποδέκτη των δεδομένων να εξακριβώσει τη πηγή και την ακεραιότητα τους και επομένως να προστατευτεί από πλαστοπροσωπία, π.χ. του αποστολέα». Με άλλα λόγια η ψηφιακή υπογραφή είναι το «ηλεκτρονικό» υποκατάστατο της συμβατής υπογραφής του αποστολέα και είναι απαραίτητη ως απόδειξη της ταυτότητας του σε κάθε ηλεκτρονική συναλλαγή. Η ψηφιακή υπογραφή παράγεται με μηχανισμούς ασύμμετρης κρυπτογράφησης, κατά τους οποίους δημιουργείται αρχικά ένα *hash* των δεδομένων, που στη συνέχεια αποτελεί είσοδο σε έναν κρυπτογραφικό αλγόριθμο ψηφιακής υπογραφής βάσει του ιδιωτικού κλειδιού του υπογράφοντος. Το hash είναι το αποτέλεσμα μίας μονόδρομης μαθηματικής συνάρτησης (αλγόριθμος hash ή Message Digest) από το οποίο είναι υπολογιστικά αδύνατο να εξαχθεί η είσοδος, δηλαδή τα αρχικά δεδομένα. Ο έλεγχος εγκυρότητας της ψηφιακής υπογραφής γίνεται με χρήση του κατάλληλου αλγορίθμου και του δημόσιου κλειδιού του υπογράφοντος. Ως είσοδος δίνονται τα δεδομένα και η ψηφιακή υπογραφή, ενώ η έξοδος είναι μία τιμή που καθορίζει το αν η ψηφιακή υπογραφή είναι έγκυρη ή όχι.

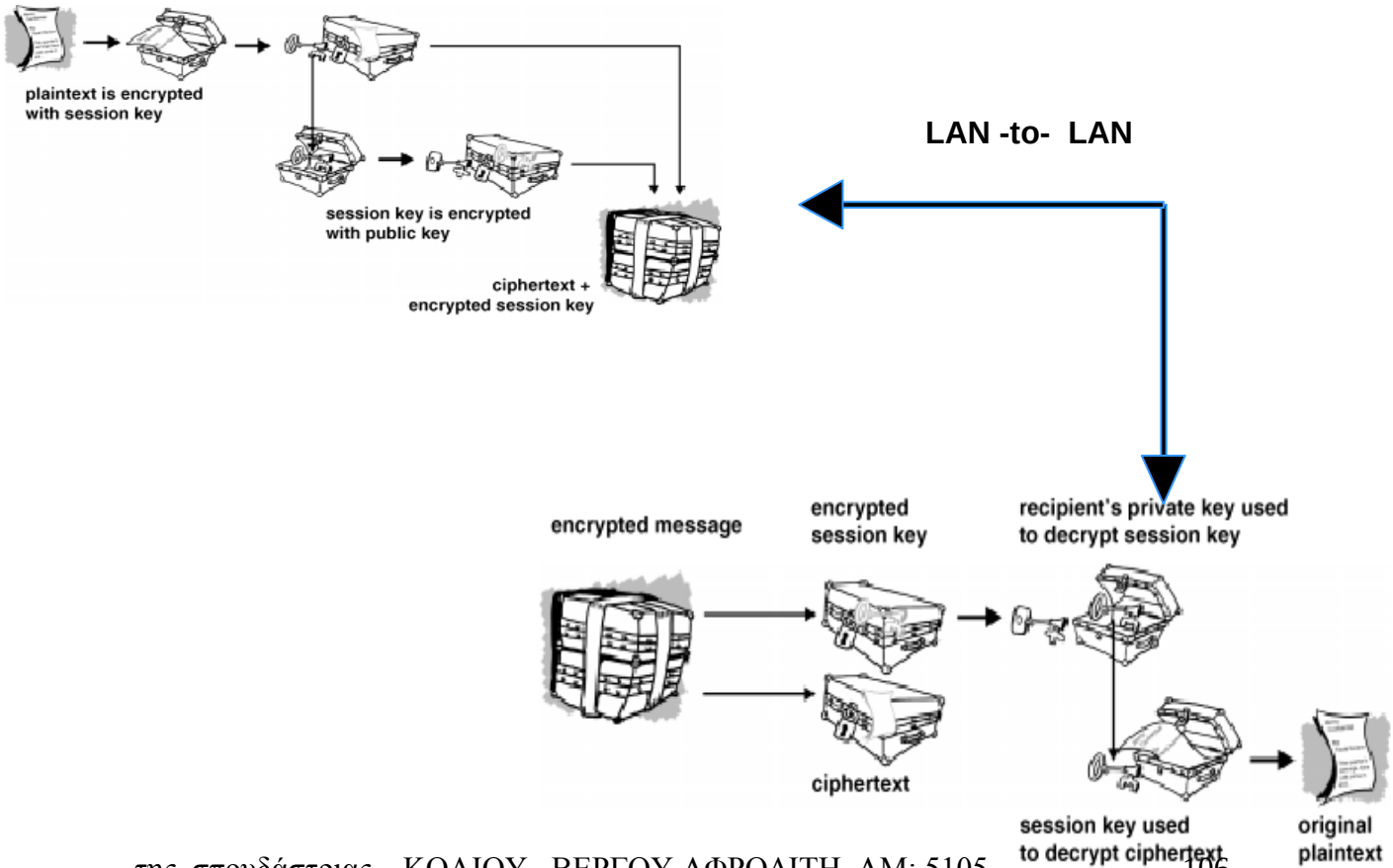


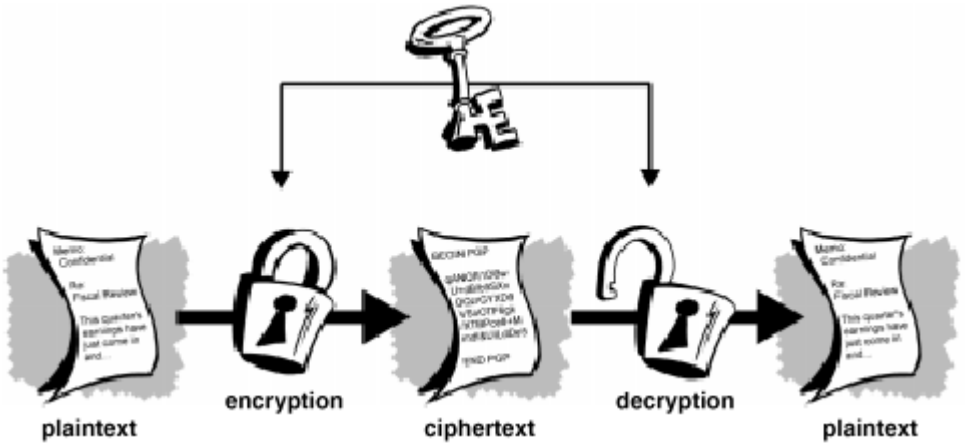
Σχήμα 5.3: Διαδικασία ψηφιακής υπογραφής δεδομένων και ελέγχου εγκυρότητας

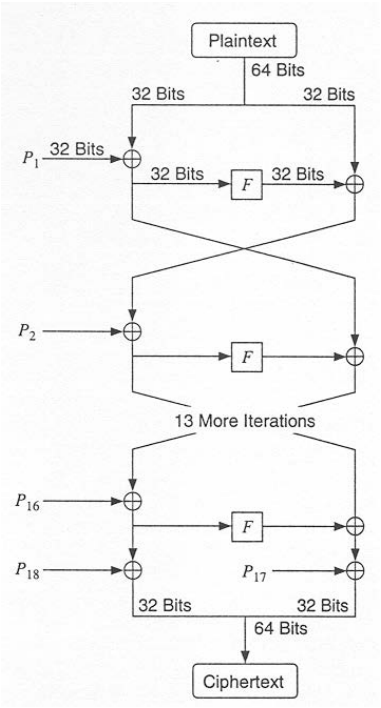
Η νομική ισχύς της ψηφιακής υπογραφής έχει κατοχυρωθεί από την Ευρωπαϊκή Κοινότητα με την Οδηγία 1999/93/ΕΚ, η οποία έχει ενσωματωθεί και στο εθνικό δίκαιο με το Προεδρικό Διάταγμα 150/201 που εποπτεύεται από την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ).
Ο άλλος αναπόσπαστος κλάδος της κρυπτογραφίας είναι η κρυπτανάλυση. Στην κρυπτανάλυση έχουμε τις προσπάθειες να σπάσουμε έναν κωδικό ή να μας δοθεί η δυνατότητα να πλαστογραφήσουμε την αυθεντικότητα μιας πληροφορίας δημιουργώντας μια αποδεκτή ψηφιακή υπογραφή. Υπάρχουν οι λεγόμενες “κρυπταναλυτικές επιθέσεις”, κατά τις οποίες γίνονται οι εξής προσπάθειες : η πρώτη είναι η επίθεση κατά την οποία έχουμε το κρυπτοκείμενο (ciphertext) και το κείμενο (plaintext) και προσπαθούμε να συμπεράνουμε τον κωδικό πρόσβασης (password). Μια άλλη είναι το να έχουμε τον κωδικό πρόσβασης, το κρυπτοκείμενο και το κείμενο και να προσπαθούμε να συμπεράνουμε τις διαδικασίες του αλγόριθμου. Αυτή η

τεχνική είναι συνήθως αναγκαία όταν ο στόχος χρησιμοποιεί μυστικό αλγόριθμο συμμετρικής κρυπτογράφησης.

Μια άλλη συνήθης τεχνική είναι το να έχουμε τον αλγόριθμο και έναν αριθμό από υπογεγραμμένα κείμενα και να προσπαθούμε να βρούμε τρόπο να παραγάγουμε μια αποδεκτή υπογραφή, με σκοπό το κείμενό μας να γίνει αποδεκτό ως προερχόμενο από έμπιστη οντότητα (με τον όρο οντότητα εννοούμε ένα χρήστη, έναν υπολογιστή, μια τράπεζα κτλ.). Στην κρυπτανάλυση, όταν αναλύουμε έναν αλγόριθμο, θεωρητικά προσπαθούμε να περιορίσουμε το ποσοστό τυχαιότητας που αυτός προσδίδει στο κρυπτοκείμενο και έτσι με λιγότερες δοκιμές να έχουμε την αποκρυπτογράφηση του μηνύματος. Μεγάλο ρόλο παίζουν και οι επιστήμες των πιθανοτήτων και της συνδυαστικής. Η κρυπτανάλυση τέλος είναι απολύτως αναγκαία για την αξιολόγηση ενός αλγόριθμου και κατά συνέπεια για τον προσδιορισμό του βαθμού ασφαλείας που προσφέρει.
Πολλές φορές ακούμε πως ένα πρόγραμμα είναι ασφαλές λόγω του ότι χρησιμοποιεί έναν “ασφαλή” αλγόριθμο. Αυτό δεν είναι πάντα αλήθεια. Στην κρυπτανάλυση μετράνε πολύ αυτά που αποκαλούμε “μειονεκτήματα πρωτοκόλλου”, δηλαδή μπορεί στα μαθηματικά ο αλγόριθμος να προσφέρει μεγάλο βαθμό ασφάλειας, αλλά, αν το πρόγραμμα που τον εφαρμόζει δεν είναι σχεδιασμένο σωστά, τότε δίνεται πολλές φορές η δυνατότητα να σπάσει ο κωδικός, πράγμα που συμβαίνει κυρίως στα συστήματα αυθεντικοποίησης, όταν δε χρησιμοποιούνται σωστά οι λεγόμενες hash functions, δηλαδή οι συναρτήσεις μέσω των οποίων παράγονται τα κλειδιάΌμως τα κρυπτογραφημένα συστήματα είναι ευάλωτα σε επίθεση τύπου “man in the middle”,υπάρχει όμως η λύση με την χρήση πιστοποιητικών (certificates)..Υπάρχει και η απαίτηση συμβατότητας με X.509 για την προοπτική της υλοποίησης.





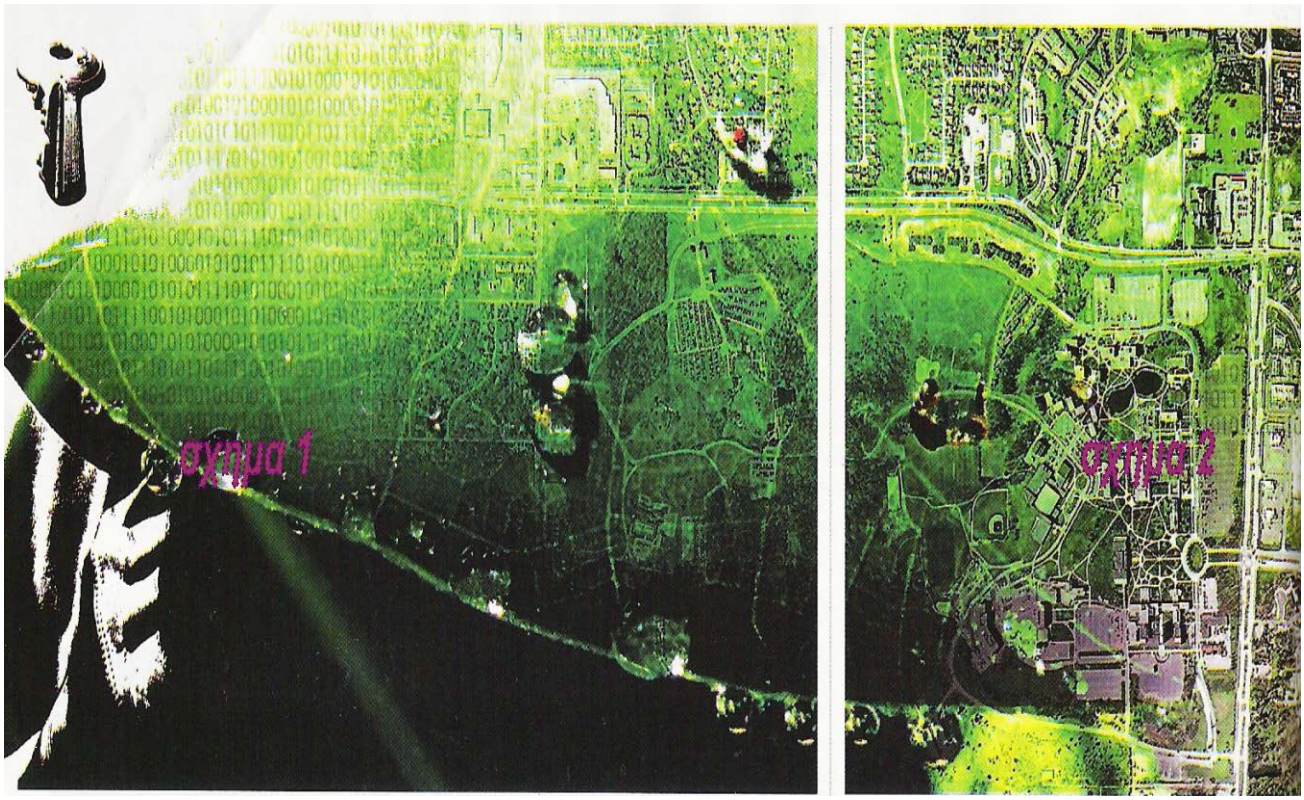


Plaintext: αρχικό μήνυμα, είσοδος στο cipher
Encryption:μέθοδος διαχωρισμού plaintext με τέτοιο τρόπο προκειμένου να κρύβονται τα στοιχεία που το αποτελούν
Ciphertext: το encryption του plaintext
Decryption:μετατροπή ciphertext σε plaintext
Κλειδί: κομμάτι δεδομένων που χρησιμοποιείται από τον αλγόριθμο κρυπτογράφησης για παραγωγή ciphertext (ΕΊΝΑΙ ΑΡΙΘΜΟΣ!!)
Μήκος :512,768,1024,2048 bits
Κατηγορίες:
•Public:μπορεί να χρησιμοποιηθεί από όλους•Secret:μόνο αυτός που το έφτιαξε πρέπει να το χρησιμοποιεί για decryption

Στη διάρκεια του Β' Παγκόσμιου Πολέμου, οι γερμανικές τακτικές επικοινωνίες, χρησιμοποιούσαν μια «κατώτερη» κρυπτομηχανή, τη θρυλική **«Αίνιγμα»**. Για την κρυπτανάλυσή της, είχε σχεδιαστεί μια ad hoc «υπολογιστική» μηχανή, η **«Βόμβα»**. Την έλεγαν «**Bombe»,,** λόγω του φοβερού θορύβου που έκανε όταν λειτουργούσε! Χρησιμοποιούσε ηλεκτρομηχανική τεχνολογία, με διακόπτες και ηλεκτρονόμους. Αντίθετα, οι στρατηγικές επικοινωνίες μεταξύ της ανώτατης διοίκησης, δηλαδή του ίδιου του Χίτλερ και των στρατηγών του, διεξάγονταν με τη βοήθεια μιας πολύ εξελιγμένης μηχανής κρυπτογράφησης, της **Lorenz SZ40**. Αυτή η κορωνίδα της γερμανικής τεχνολογίας, ήταν ουσιαστικά, ένα τηλέτυπο, που μπορούσε ταυτόχρονα να κρυπτογραφήσει και να διαβιβάσει το κείμενο, επιτυγχάνοντας μεγάλη οικονομία χρόνου και κόπου. Μπορεί να θεωρηθεί και ως η **πρώτη on-line κρυπτομηχανή**.

Άλλοι εναλλακτικοί τρόποι ασφαλείας

Τα υδατογραφήματα επιτρέπουν την ύπαρξη κρυμμένων πληροφοριών στα ψηφιακά μέσα, έτσι ώστε το υδατογράφημα να είναι δυσδιάκριτο και δύσκολο να αφαιρεθεί. Η κρυπτογραφία και το υδατογράφημα είναι επιστημονικοί ερευνητικοί τομείς με έναν υψηλό στρατηγικό αντίκτυπο για την ευρωπαϊκή βιομηχανία και για την κοινωνία. Είναι ένα θεμελιώδες μέσο για την ασφάλεια, τη μυστικότητα και την αξιοπιστία στην κοινωνία των πληροφοριών για την ψηφιακή διαχείριση στοιχείων.
Επίσης στα ασύρματα δίκτυα μπορεί να χρησιμοποιηθεί και η **στεγανογραφία** όπου μέσα σε ένα μήνυμα π.χ μια φωτογραφία όπως στο σχήμα 2 μπορεί να κρυφτεί ένα ολόκληρο κρυπτογραφημένο μήνυμα χωρίς συμπίεση όπως φαίνεται στο σχήμα 1 .Αυτό παρέχει μεγαλύτερη ασφάλεια στις επικοινωνίες των χρηστών .



ΤΟ ΑΣΦΑΛΕΣ ΚΙΝΗΤΟ ΤΗΛΕΦΩΝΟ ΣΥΝΟΜΙΛΙΩΝ <<talk secure >>

Μια λύση στο πρόβλημα των καταναλωτών για ασφάλεια στις συνομιλίες τους αποτελούν τα προϊόντα General Dynamics , που διαφημίζονται στο περιοδικό Mobile.Το talk secure είναι ένα τηλέφωνο ,που πετυχαίνει ύψιστη ασφάλεια κατά την μετάδοση φωνής και δεδομένων σε εμπορικά δίκτυα GSM,που λειτουργούν στις συχνότητες 900/1800/1900 MHz, και έχει τα ίδια χαρακτηριστικά του .Για την κρυπτογράφηση κατά την μετάδοση των δεδομένων χρησιμοποιεί τον αλγόριθμο AES (advanced Encryption Standard), που αντικατέστησε τον αλγόριθμο DES(Data Encryption Standard) και προστατεύει από θέματα δημόσιας ασφάλειας , επαγγελματικά μυστικά , πνευματική ιδιοκτησία και οικονομικά θέματα.

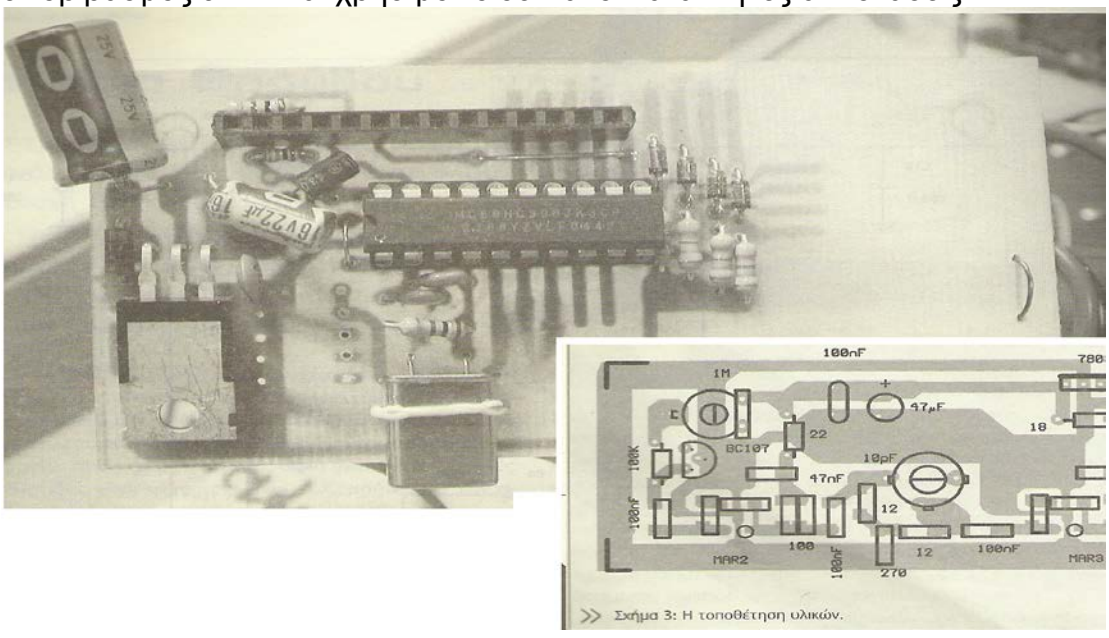
ΓΕΝΝΗΤΡΙΑ ΘΟΡΥΒΟΥ

Ο θόρυβος ,το γνωστό φύσημα των ενισχυτών και των ραδιοφώνων , είναι ένα από τα χειρότερα μειονεκτήματα στα ηλεκτρονικά συστήματα και κυρίως στα συστήματα τηλεπικοινωνιών .
Για την παραγωγή του ,χρησιμοποιείται δύο μεθόδους :

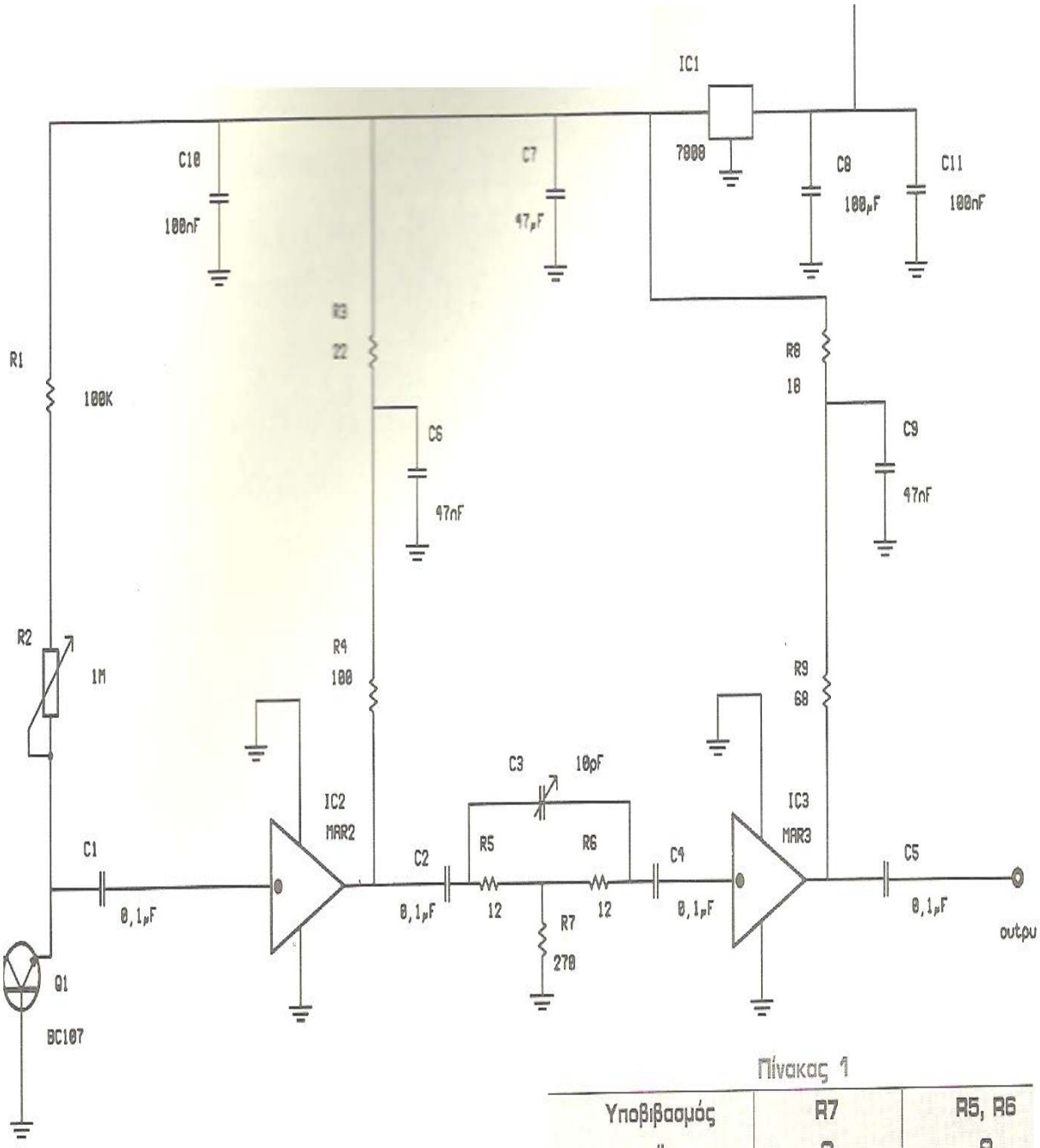
- .την θερμική μέθοδο ,όπου πολώνουν μια λυχνία ή μια κρυσταλλοδίοδο και το σήμα που παράγεται , ακολούθως , ενισχύεται από ενισχυτές ευρέως φάσματος.

- Την ψηφιακή μέθοδο με απαριθμητές .

Με την μέθοδο αυτή , ο θόρυβος παράγεται με κυκλώματα που παράγουν ψευδοτυχαίες ακολουθίες συμβάντων. Η γεννήτρια θορύβου είναι μια διάταξη που παράγει θόρυβο τυχαίου πλάτους και συχνότητα δηλαδή η γεννήτρια παράγει συχνότητες σε τυχαία σειρά και σε μη σταθερό πλάτος .Τα σήματα που παράγονται από τέτοια κυκλώματα μπορούν να χρησιμοποιηθούν σε οποιαδήποτε τομέα της ηλεκτρονικής ,π.χ . στην τηλεφωνία . Μορφή τέτοιων σημάτων είναι ο λευκός θόρυβος είτε αυτός είναι ακουστικής είτα αυτός είναι ραδιοφωνικής συχνότητας . Με κατάλληλο φιλτράρισμα , ο τυχαίος θόρυβος αντικαθιστά την ομιλία (ήχο) ή τα επιμέρους στοιχεία , ως προς την φυσικότητα και την πολυπλοκότητα.
Η παρακάτω γεννήτρια θορύβου παράγει θόρυβο σε όλη την περιοχή των VHF, των UHF και στην περιοχή της δορυφορικής τηλεόρασης. Η στάθμη εξόδου είναι αρκετή για να ελεγχθούν τα φίλτρα και η ευαισθησία του δέκτη.[Α΄,53] Στα παρακάτω σχήματα βλέπουμε πως είναι εσωτερικά μια γεννήτρια θορύβου , ένα σχεδιάγραμμα τοποθέτησης των υλικών και το θεωρητικό διάγραμμα κατασκευής .Όπως επίσης βλέπουμε στο σχήμα ανάλογα με την χρήση της γεννήτριας θορύβου γίνεται ο κατάλληλος υποβιβασμός d Bm και χρησιμοποιούνται οι κατάλληλες αντιστάσεις.



Σχήμα 3: Η τοποθέτηση υλικών.



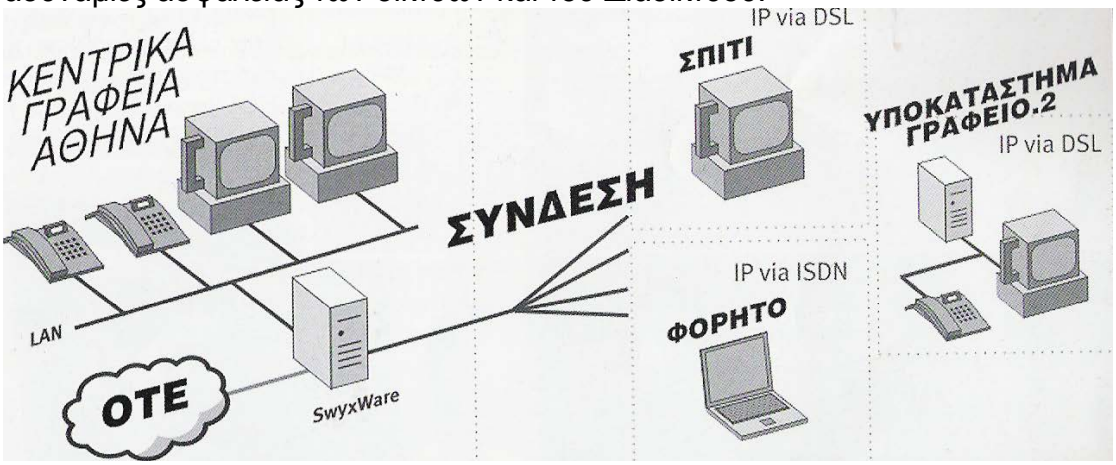
Σχήμα 1: Το θεωρητικό διάγραμμα της κατασκευής.

Πίνακας 1

Υποβιβασμός db	R7 Ω	R5, R6 Ω
1	870.0	5.8
3	292.0	11.6
6	150.5	37.3
9	105.0	61.6
10	96.2	71.2
20	61.0	247.5

Τα ασύρματα επιχειρηματικά δίκτυα και η ασφάλεια

Σε ένα όμως επιχειρηματικό δίκτυο που περιλαμβάνει ένα ασύρματο δίκτυο (WLAN ή WWAN ή WATM), οι πιστοποιημένοι χρήστες και η εμπιστευτική επικοινωνία είναι περισσότερο προβληματικοί σε σχέση με ένα ενσύρματο δίκτυο. Καθώς τα κινητά δίκτυα αναπτύσσονται, τα κινητά τηλέφωνα όπως και κάθε άλλη κινητή συσκευή, εκτίθεται όλο και περισσότερο σε θέματα ασφάλειας του Διαδικτύου και κυρίως τώρα που τα σύγχρονα συστήματα επικοινωνιών βασίζονται στην τεχνολογία Voice Over IP (VoiP) ,που επιτρέπουν την ενοποίηση των απομακρυσμένων χώρων σε έναν μεγάλο , εικονικό χώρο , μέσα στον οποίο υπάρχει επικοινωνία των υπολογιστών αλλά και των τηλεφώνων. Μ ε την νέα όμως τεχνολογία κληρονομούν και τις αδυναμίες ασφαλείας των δικτύων και του Διαδικτύου.



Η ΤΕΧΝΟΛΟΓΙΑ ΤΩΝ ΣΥΓΧΡΟΝΩΝ ΣΥΣΤΗΜΑΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ
Voice Over IP
(VoiP)

Οι απειλές ασφάλειας που παρουσιάζονται είναι οι ακόλουθες:

Παρεμβολές και αξιοπιστία

Οι παρεμβολές στις ασύρματες επικοινωνίες μπορεί να προέλθουν από ταυτόχρονες εκπομπές δύο ή περισσοτέρων πηγών που μοιράζονται την ίδια ζώνη συχνοτήτων. Όταν πολλοί σταθμοί που περιμένουν να απελευθερωθεί ο δίαυλος και να αρχίζουν να εκπέμπουν, εμφανίζονται συγκρούσεις. Συγκρούσεις εμφανίζονται λόγω του προβλήματος του 'κρυμμένου τερματικού', όπου κάποιος σταθμός, πιστεύοντας ότι ο δίαυλος είναι ελεύθερος, αρχίζει την εκπομπή χωρίς να ανιχνεύει επιτυχώς την ήδη ευρισκόμενη σε εξέλιξη μετάδοση. Παρεμβολές επίσης εμφανίζονται από τις διαλείψεις πολλαπλών διαδρομών, που χαρακτηρίζονται από τυχαίες διακυμάνσεις του πλάτους και της φάσης στη λήψη. Η αξιοπιστία ενός διαύλου επικοινωνιών μετριέται συνήθως με τον μέσο ρυθμό εσφαλμένων bit (BER). Η αυτόματη αναμετάδοση και η διόρθωση λαθών χρησιμοποιούνται για την αύξηση της αξιοπιστίας.

Ασφάλεια επικοινωνίας

Στα ενσύρματα δίκτυα, το μέσο μετάδοσης μπορεί να παρέχει φυσική ασφάλεια και η πρόσβαση στο δίκτυο ελέγχεται εύκολα. Στα ασύρματα δίκτυα, η ασφάλεια επικοινωνίας είναι δυσκολότερο να ελεγχθεί, καθότι το μέσο μετάδοσης είναι ανοιχτό σε οποιονδήποτε βρίσκεται στη ραδιοκάλυψη ενός πομπού. Η ασφάλεια των δεδομένων στο ασύρματο τμήμα επιτυγχάνεται με κρυπτογράφηση. Ωστόσο, η διαδικασία της κρυπτογράφησης αυξάνει το κόστος του συστήματος και μειώνει την επίδοσή του.

Άρνηση Εξυπηρέτησης -Denial of service (DOS/DDOS)

Αποτελεί επίθεση κατά την οποία ο εισβολέας προσπαθεί να διακόψει κάθε υπηρεσία που παρέχεται στους νόμιμους χρήστες. Το DDOS είναι μια εξαπλωμένη μορφή αυτής της επίθεσης, όπου οι εισβολείς κάνουν ταυτόχρονες ‘επιθέσεις’ για να επιτύχουν πιο ολοκληρωμένη εισβολή.

Spoofing

Αποτελεί τεχνική για επιτυχημένη, μη εξουσιοδοτημένη πρόσβαση στους υπολογιστές. Καταρχάς πρέπει ο εισβολέας να βρει μια διεύθυνση IP ενός έμπιστου κόμβου. Μόλις η πληροφορία ληφθεί, ο εισβολέας μπορεί να την χρησιμοποιήσει για να πείσει τον δέκτη ότι ο ίδιος ο εισβολέας είναι ο αποστολέας που μπορεί να εμπιστευτεί.

Man in the Middle

Επίθεση κατά την οποία ο εισβολέας προσπαθεί να τοποθετήσει τον εαυτό του στην ‘μέση’ μιας συζήτησης. Αυτές οι επιθέσεις πραγματοποιούνται από κακεντρεχείς εισβολείς, που ξεγελούν και τα 2 μέλη της συζήτησης οι οποίοι έχουν την εντύπωση πως είναι μόνοι τους ενώ στην ουσία παρακολουθούνται. Έπειτα ο εισβολέας μπορεί εκτός από παρακολούθηση των πληροφοριών που ανταλλάσσονται να επιτύχει την διαστρέβλωση τους ή ακόμα και να εμφυτεύσει δικές του πληροφορίες. Τα ασύρματα δίκτυα είναι πολύ ‘ευαίσθητα’ σε τέτοιου είδους επιθέσεις.
Επιθέσεις man in the middle μπορούν να γίνουν κυρίως κατά την κρυπτογράφηση στο δίκτυο GSM, που τότε δέχεται τις επιθέσεις. Σε ορισμένες χώρες απαγορεύεται η κρυπτογράφηση για αυτό στο GSM standard υπάρχει ως επιλογή . Αυτό το μειονέκτημα δεν είναι επικίνδυνο από μόνο του , αλλά επειδή ο MS δεν πιστοποιεί την αυθεντικότητα του BTS , αυτό θα μπορεί να χρησιμοποιηθεί για να κρυφακούσει .Ο εχθρός μπορεί να προμηθευτεί τον εξοπλισμό ενός σταθμού Βάσης και να εγκαταστήσει ένα δικό του BTS με ανενεργή κρυπτογράφηση. Ο MS θα συνδεθεί με το BTS του επιτιθέμενου ,αν έχει τα χαρακτηριστικά του διαχειριστή και καλύτερο σήμα από τον πραγματικό σταθμό βάσης. Ο ψεύτικος σταθμός που βρίσκεται ανάμεσα MS και το BTS παρακολουθώντας , κρυφακούγοντας , παρεμβάλλοντας ένα δικό του σήμα παραπλάνησης , ή στέλνοντας ένα σήμα ότι είναι κατειλημμένο στο MS κάθε φορά που αυτός θέλει να πραγματοποιήσει μια κλήση και όλα αυτά γίνονται εν αγνοία των άλλων ,που δεν γνωρίζουν την ύπαρξη του.

Replay

Επίθεση κατά την οποία ο εισβολέας αποκτά μέρη των καλωδίων του δικτύου. Αφού τα αποκτήσει μπορεί να αποσπάσει πληροφορίες από αυτά όπως κωδικοί πρόσβασης και γενικές πληροφορίες εξουσιοδότησης. Ακόμη αφού τα χρησιμοποιήσει μπορεί να τα τοποθετήσει πίσω στην θέση τους στο δίκτυο.

TCP/IP Hijacking

Λέγεται και υφαρπαγή συνόδου(Session Hijacking). Ο εισβολέας μπορεί να πάρει τον έλεγχο σε έναν TCP τομέα ανάμεσα σε δύο μηχανήματα. Μία διαδεδομένη μέθοδος είναι αυτή κατά την οποία χρησιμοποιούνται πακέτα IP καλά εδραιωμένων πηγών (source-routed IP packets).

DNS Poisoning

Επίθεση κατά την οποία τα DNS αρχεία μας 'μολύνονται' με λάθος πληροφορίες. Έτσι αν υποθέσουμε ότι έχουμε μια εγγραφή η οποία 'δείχνει' σε έναν έμπιστο κόμβο, τότε ο εισβολέας μπορεί να την αλλάξει και η εγγραφή μας πια να 'δείχνει' σε μια λάθος κατεύθυνση.

Weak Keys

Επίθεση κατά την οποία ο εισβολέας ανακαλύπτει κάποια μυστικά κλειδιά με κάποια συγκεκριμένη αξία στην κρυπτογράφηση που έχει ήδη γίνει. Μερικές φορές ευθύνεται και η χαμηλής πιστότητας κρυπτογράφηση που έχει πραγματοποιηθεί.

Mathematical

Οι μαθηματικές και αλγεβρικές επιθέσεις στηρίζουν την επιτυχία τους στα κρυπτογραφημένα κομμάτια κώδικα του συστήματος τα οποία παρουσιάζουν σε μεγάλο βαθμό μαθηματική δομή.

Social Engineering

Πολλές φορές οι εισβολείς πραγματοποιούν επιθέσεις μόνο και μόνο για να εκμεταλλευτούν τις αδυναμίες των ίδιων των συστημάτων. Επιθέσεις αυτού του τύπου πραγματοποιούνται κυρίως σε τερματικά τελικών χρηστών.

Brute Force

Αποτελεί μια μορφή 'σπασίματος' κωδικών πρόσβασης. Οι Brute Force επιθέσεις δοκιμάζουν κάθε πιθανή ακολουθία χαρακτήρων μέχρι να πετύχουν το σωστό συνδυασμό. Η μόνη προστασία που μπορούμε να έχουμε απέναντι σε αυτές τις επιθέσεις είναι μεγάλο μήκος κωδικών ή/και την αλλαγή των κωδικών μας τακτικά.

Software Exploitation

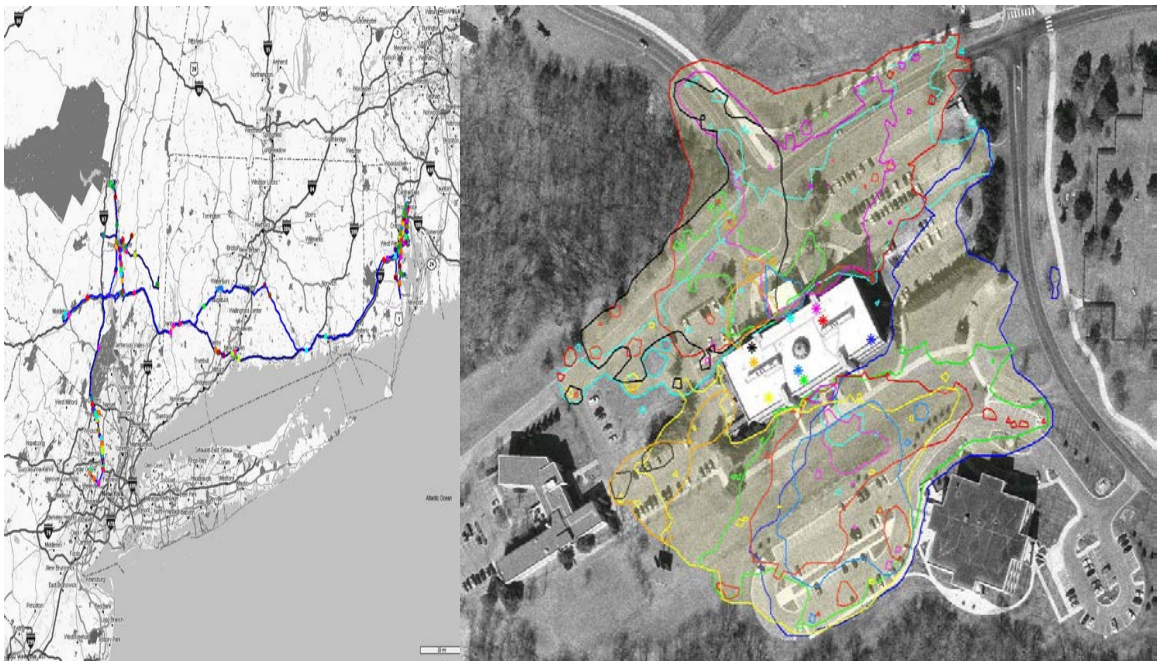
Επιθέσεις κατά 'λαθών' του συστήματος και 'αδύναμων' σημείων του κώδικα. Η προστασία μας απέναντι σε αυτές τις επιθέσεις είναι οι συχνές ανανεώσεις του λογισμικού με τις απαραίτητες διορθώσεις.

War Dialling

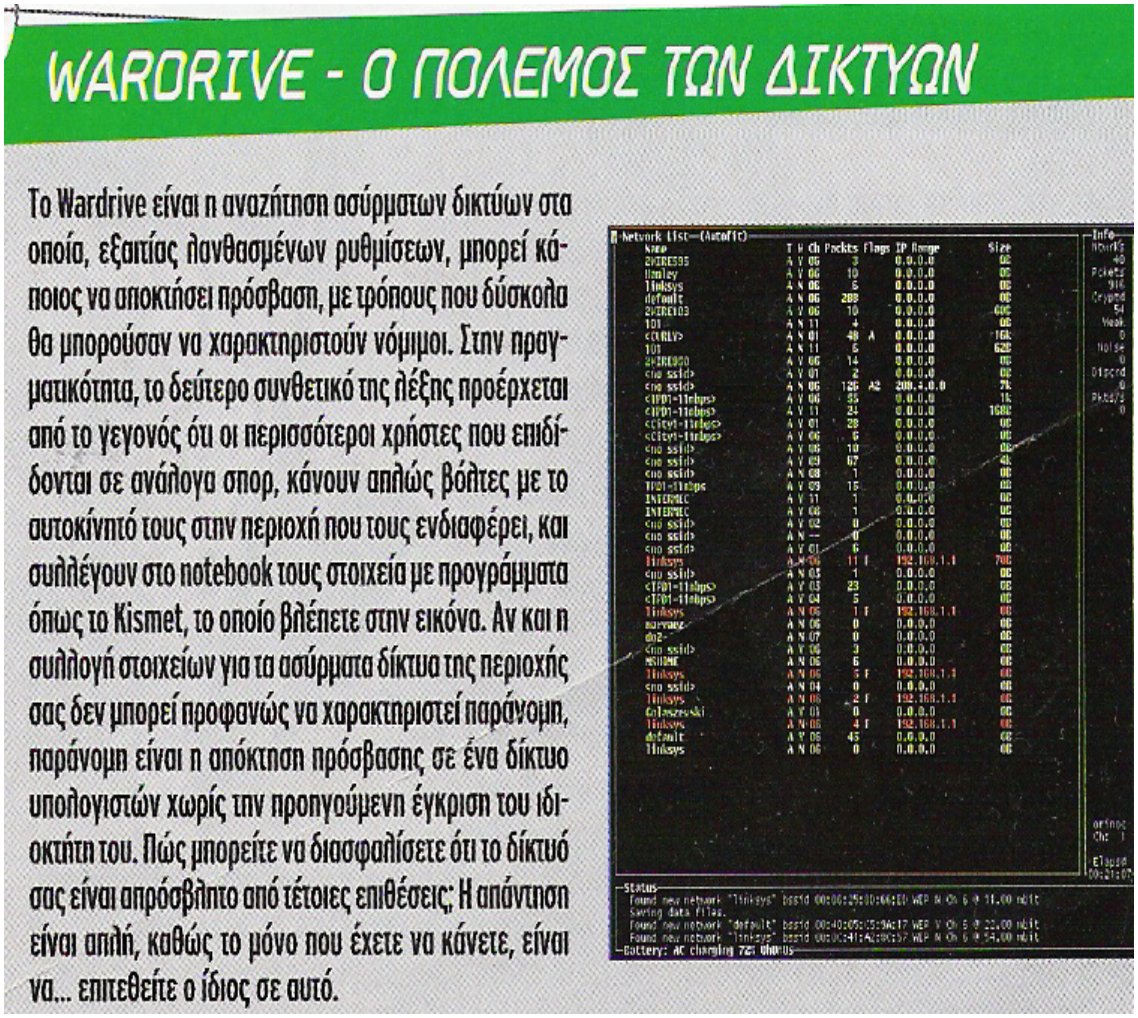
Αποτελεί την διαδικασία χρησιμοποίησης εργαλείων ανίχνευσης στα dial up modems. Τα εργαλεία αυτά είναι προγράμματα υπολογιστή που χρησιμοποιούνται για την αναγνώριση των τηλεφωνικών αριθμών που μπορούν επιτυχώς να συνδεθούν με ένα modem. Το πρόγραμμα καλεί μια σειρά αριθμών και καταγράφει τις αποτυχημένες και τις επιτυχημένες κλήσεις.

War Driving

Επίθεση κατά την οποία χρησιμοποιείται ένα εργαλείο για την εισβολή σε ασύρματα συστήματα από εξωτερικό παράγοντα. Για την συγκεκριμένη επίθεση απαιτείται μια κάρτα Ethernet ασύρματου δικτύου και επίσης χρειάζεται μια πολύ δυνατή κεραία εφόσον ο εισβολέας σκοπεύει να παραμείνει σε μεγάλη απόσταση από το σύστημα. Το War Driving είναι η πιο συνηθισμένη μέθοδος αναζήτησης ασύρματων δικτύων . Ο επίδοξος εισβολέας οδηγεί σε περιοχές που υπάρχουν ασύρματα δίκτυα και χρησιμοποιώντας ένα φορητό Η/Υ ή PDA με το κατάλληλο software, τα ανακαλύπτει και συνδέεται σε αυτά. Υπάρχουν πολλά προγράμματα διαθέσιμα στο internet για το «σπάσιμο» ασύρματων δικτύων. Συχνά χρησιμοποιούνται αρκετά ανορθόδοξα μέσα, όπως η συσκευασία γνωστής μάρκας με πατατάκια ή οποία είναι ίσως ο καλύτερος ενισχυτής σήματος στην αγορά σήμερα.



Αναφορικά με την ασφάλεια ενός ασύρματου δικτύου πρέπει να πούμε ότι εκτός από τα προβλήματα που οφείλονται στην τεχνολογία μετάδοσης, συνεχίζουμε να έχουμε και τα προβλήματα ενός ενσύρματου δικτύου. Εδώ βλέπουμε πόσο εύκολο είναι για κάποιον ο οποίος βρίσκεται στο δρόμο, χρησιμοποιώντας τον κατάλληλο εξοπλισμό, να συνδεθεί στο ασύρματο δίκτυο από απόσταση ασφαλείας και ενδεχομένως να αποκτήσει πρόσβαση σε ολόκληρο το εταιρικό δίκτυο. Αρκεί ένας φορητός ή ένα PDA.



WARDRIVE - Ο ΠΟΛΕΜΟΣ ΤΩΝ ΔΙΚΤΥΩΝ

Το Wardrive είναι η αναζήτηση ασύρματων δικτύων στα οποία, εξαιτίας λανθασμένων ρυθμίσεων, μπορεί κάποιος να αποκτήσει πρόσβαση, με τρόπους που δύσκολα θα μπορούσαν να χαρακτηριστούν νόμιμοι. Στην πραγματικότητα, το δεύτερο συνθετικό της λέξης προέρχεται από το γεγονός ότι οι περισσότεροι χρήστες που επιδίδονται σε ανάλογα σπορ, κάνουν απλώς βόλτες με το αυτοκίνητό τους στην περιοχή που τους ενδιαφέρει, και συλλέγουν στο notebook τους στοιχεία με προγράμματα όπως το Kismet, το οποίο βλέπετε στην εικόνα. Αν και η συλλογή στοιχείων για τα ασύρματα δίκτυα της περιοχής σας δεν μπορεί προφανώς να χαρακτηριστεί παράνομη, παράνομη είναι η απόκτηση πρόσβασης σε ένα δίκτυο υπολογιστών χωρίς την προηγούμενη έγκριση του ιδιοκτήτη του. Πώς μπορείτε να διασφαλίσετε ότι το δίκτυό σας είναι απρόσβλητο από τέτοιες επιθέσεις; Η απάντηση είναι απλή, καθώς το μόνο που έχετε να κάνετε, είναι να... επιτεθείτε ο ίδιος σε αυτό.

Buffer Overflow

Επίθεση κατά την οποία ο εισβολέας εκμεταλλεύεται την χαμηλή ποιότητα του γραμμένου κώδικα. Εάν ο κώδικας δεν ελέγχει το μήκος των μεταβλητών, τότε το σύστημα θα είναι ευαίσθητο σε τέτοιου είδους επιθέσεις.

SYN flood

Είναι επιθέσεις που εκμεταλλεύονται τις αδυναμίες του πρωτοκόλλου TCP/IP. Ένας μεγάλος αριθμός από μισάνοιχτες συνδέσεις χρησιμοποιείται για να αποτρέψει την σύνδεση των νόμιμων χρηστών.

Port Scanning

Χρησιμοποιείται ‘τρέχοντας’ έναν ανιχνευτή τρωτότητας στο σύστημα που έχει την δυνατότητα να ‘βλέπει’ ποιες θύρες είναι ανοιχτές.

Αντίμετρα

Το Διαδίκτυο είχε προβλήματα ασφάλειας ακόμα και τότε που βρισκόταν σε πειραματικό στάδιο. Σήμερα που έχει γιγαντωθεί, οι κίνδυνοι είναι ακόμα περισσότεροι. Αυτό οφείλεται γιατί το Διαδίκτυο χρησιμοποιείται για έναν σκοπό εντελώς ξένο προς τον αρχικό σχεδιασμό, που είναι κυρίως το εμπόριο. Είναι σχεδόν παράλογο ότι ενώ το Διαδίκτυο είχε αρχικά δημιουργηθεί με σκοπό να είναι απρόσβλητο(bullet-proof) σε εχθρικές επιθέσεις, και κυρίως σε DOS – ΕΠΙΘΕΣΕΙΣ , τώρα είναι εξαιρετικά τρωτό ακόμα και από άτομα μικρής ηλικίας χωρίς ιδιαίτερες τεχνικές γνώσεις.
Τα οικονομικά ιδρύματα επικεντρώνουν το ενδιαφέρον τους στην ασφάλεια των ηλεκτρονικών υπηρεσιών σε σχέση με τα ασύρματα δίκτυα.

Μερικές από τις πιο γνωστές λύσεις στα προβλήματα της ασφάλειας των ασύρματων δικτύων είναι οι ακόλουθες:

WEP (Wired Equivalent Privacy)

Δεδομένου ότι η ασύρματη επικοινωνία χρησιμοποιεί ένα ‘ανοικτότερο’ μέσο επικοινωνίας σε σύγκριση με το συνδεδεμένο με καλώδιο LAN, οι σχεδιαστές του IEEE 802.11 προτύπου περιέλαβαν στη προδιαγραφή ένα διαμοιραζόμενο μηχανισμό κρυπτογράφησης. Όπως φανερώνει και το όνομα του, στόχος του προτύπου WEP είναι να δοθεί ένα επίπεδο μυστικότητας ισοδύναμο με αυτό ενός μη-ασφαλή ενσύρματου τοπικού δικτύου. Ένα WLAN δίκτυο πρέπει να περιλαμβάνει το πρότυπο WEP, προκειμένου να αποκτήσει τη σφραγίδα έγκρισης Wi-Fi. Έτσι, αν και το WEP είναι προαιρετικό μέρος της 802.11 προδιαγραφής, όλοι οι προμηθευτές θα πρέπει να την περιλαμβάνουν προκειμένου να εξασφαλίσουν πιστοποίηση ταυτότητας και εμπιστευτικότητα.
Μιλώντας γενικά, το WEP στηρίζεται σε ένα προκαθορισμένο σύνολο κλειδιών που μοιράζονται μεταξύ των ασύρματων συσκευών – όπως φορητοί Η/Υ με ασύρματους προσαρμογής LAN – και των ασύρματων σημείων πρόσβασης (AP). Ο χρήστης που διαθέτει το σωστό κλειδί, μπορεί να επικοινωνήσει με οποιοδήποτε σημείο πρόσβασης στο ασύρματο δίκτυο. Χωρίς το κλειδί η Link Level σύνδεση αίτησης απορρίπτεται. Ο αλγόριθμος κρυπτογράφησης που χρησιμοποιείται στο πρότυπο WEP είναι ο RC4. Το σχέδιο στηρίζεται σε ένα κλειδί 40 δυαδικών ψηφίων για την κρυπτογράφηση του ωφέλιμου φορτίου των πλαισίων δεδομένων. Η ομάδα εργασίας επέλεξε το συγκεκριμένο αλγόριθμο εν μέρει επειδή η κυβέρνηση των Ηνωμένων Πολιτειών δεν απαγορεύει την εξαγωγή προϊόντων που χρησιμοποιούν την RC4 μέθοδο κρυπτογράφησης. Αντίθετα άλλοι αλγόριθμοι όπως ο DES μπορούν να εξαχθούν σε μερικές μόνο συγκεκριμένες εφαρμογές. Επιπλέον οι δοκιμές

από τα μέλη της IEEE 802.11 απέδειξαν ότι ο αλγόριθμος RC4 εξασφαλίζει ασφάλεια που φτάνει ή ακόμα και ξεπερνάει την ασφάλεια που προσφέρουν τα συνδεδεμένα με καλώδιο πρότυπα Ethernet. Πρέπει βέβαια να σημειώσουμε ότι όσο διατίθενται ασύρματα 'sniffers', η μεγαλύτερη ασφάλεια και η εύρεση αποτελεσματικότερων τρόπων εξασφάλισης της θα είναι αναγκαία.
Δυστυχώς πολλοί προμηθευτές στις μέρες μας δεν έχουν εφαρμόσει ακόμα το χαρακτηριστικό γνώρισμα WEP στα προϊόντα τους.

Χρήση της Κρυπτογραφίας Δημοσίου Κλειδιού στα Ασύρματα Δίκτυα

Οι τεχνικές δημοσίου κλειδιού έχουν υιοθετηθεί σε πολλού τομείς της τεχνολογίας πληροφοριών, συμπεριλαμβανόμενης της ασφάλειας δικτύων, της ασφάλειας λειτουργικών συστημάτων , της ασφάλειας δεδομένων εφαρμογών και της διαχείρισης των ψηφιακών δικαιωμάτων. Τα κυψελοειδή standard έχουν ήδη υιοθετήσει την κρυπτογραφία δημοσίου κλειδιού ως ένα θεμελιακό στοιχείο στην συγκρότηση ενός ασφαλούς ασύρματου περιβάλλοντος .

Ασφαλής περιήγηση.

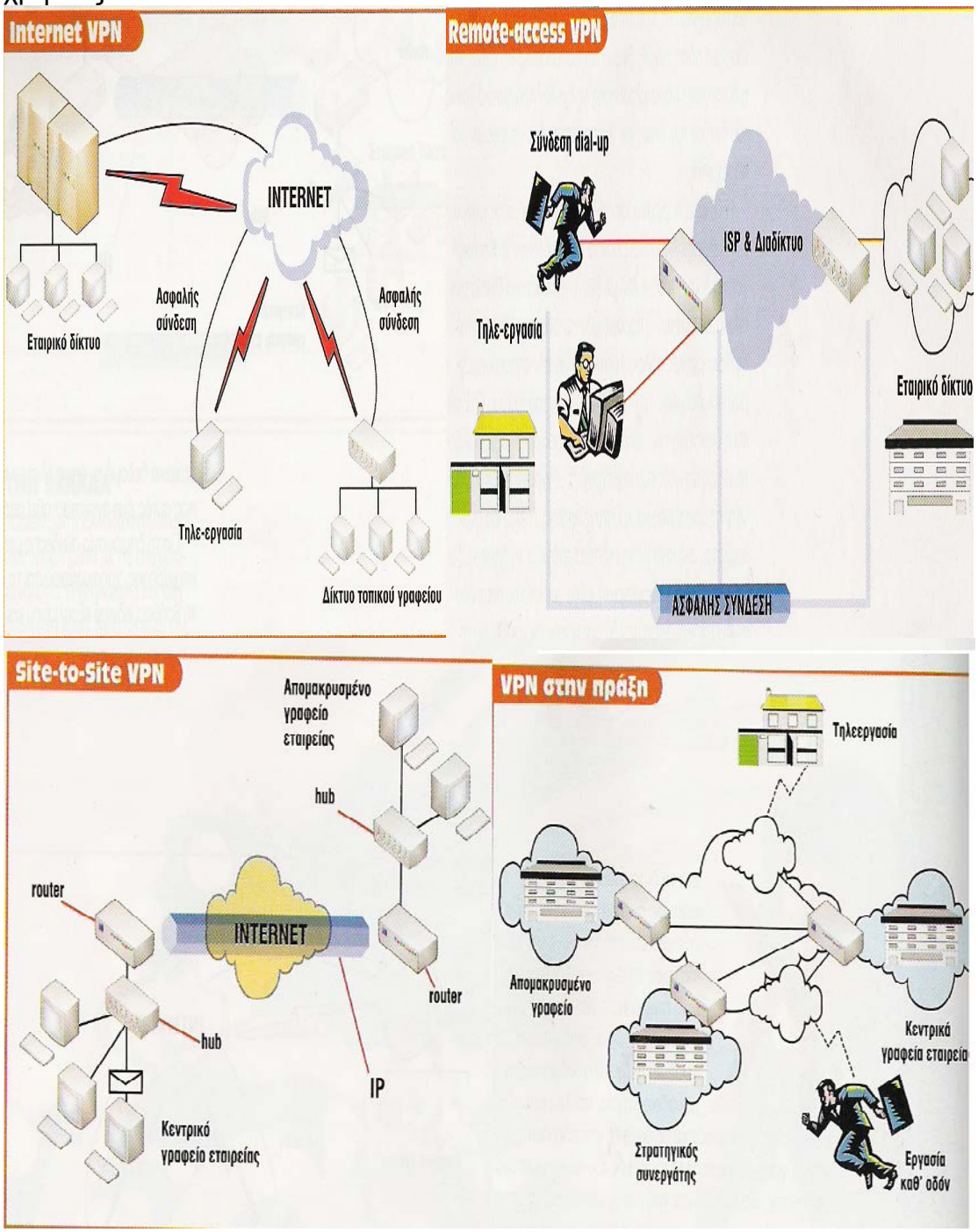
Τα πρωτόκολλα ασφάλειας στο Διαδίκτυο είναι οι πιο συχνές εφαρμογές των μεθολογιών του δημοσίου κλειδιού στις ασύρματες συσκευές. Αντίστοιχα με το γνωστό πρωτόκολλο TLS (Transport Layer Security) έχει αναπτυχθεί και η ασύρματη εκδοχή του, γνωστή ως WTLS (Wireless Transport Layer Security). Το WTLS δημιουργήθηκε για να παρέχει μια ασφαλή δίοδο μεταξύ του κινητού τηλεφώνου και μιας εξόδου WAP. Παρόλα αυτά δεν ικανοποίησε την απαίτηση για απόλυτη ασφάλεια στα δεδομένα. Μια μετέπειτα έκδοση του WAP (2.0) υιοθετήθηκε από το TLS πρωτόκολλο και επιτρέπει την πραγματική απόλυτη ασφάλεια καθόλη την περιήγηση μας στο διαδίκτυο. Αυτό πραγματοποιείται με τους εξής τρόπους :1) Επιτρέποντας σε έναν εξυπηρετητή δικτύου και σε έναν πελάτη (στην περίπτωσή μας –μια κινητή συσκευή) να αυθεντικοποιήσει κάθε έναν και να δημιουργήσει μια κρυπτογραφημένη σύνδεση. Στην αυθεντικοποίηση, η κρυπτογράφηση δημοσίου κλειδιού χρησιμοποιείται για να παρέχεται αμοιβαία αυθεντικοποίηση και συμφωνία κοινού κλειδιού. 2) Μόλις το πρώτο στάδιο ολοκληρωθεί, τα δεδομένα των εφαρμογών ανταλλάσσονται πλέον με ασφάλεια με την βοήθεια της συμμετρικής κρυπτογράφησης χρησιμοποιώντας το κοινό κλειδί.

Πρόσβαση στα Δίκτυα Επιχειρήσεων.

Τα 2.5G και 3G ασύρματα δίκτυα ενεργοποιούν τις κινητές συσκευές στο να έχουν πρόσβαση να εκτελούν εφαρμογές, όπως αποστολή e-mail, μεταφορά αρχείων, CRM και άλλα. Αυτό αυξάνει την ανάγκη για εικονικό ιδιωτικό δίκτυο (VPN) το οποίο θα παρέχει δικτυακή ασφάλεια μεταξύ της συσκευής του τηλεφώνου και του εξυπηρετητή. Οι πελάτες VPN μπορεί να έχουν εισχωρήσει σε πολλά στρώματα όπου η βασική εισχώρηση είναι στο πρωτόκολλο Διαδικτύου (IP) χρησιμοποιώντας το IETF Internet Protocol Security (Ipsec). Το IPsec προστατεύει τις ανταλλαγές στο δικτυακό στρώμα,

παρέχοντας ακεραιότητα και αυθεντικότητα δεδομένων , εμπιστευτικότητα πληροφοριών και προστασία επανάληψης. Το IPsec χρησιμοποιεί κρυπτογράφηση δημοσίου κλειδιού ως μέρος της δικτυακής ανταλλαγής κλειδιών (IKE) το οποίο χρησιμοποιεί διαχείριση αυτόματων κλειδιών. Το IKE διαχειρίζεται την ανταλλαγή των παραμέτρων ασφαλείας, όπως επίσης επιτρέπει σε έναν VPN εξυπηρετητή να αυθεντικοποιήσει μια κινητή συσκευή χρησιμοποιώντας διεύθυνση διαπιστευμένη. Το VPN είναι ήδη ένα ισχυρό κίνητρο για επιχειρήσεις ώστε να αναπτύσσουν δομές δημοσίου κλειδιού δημιουργώντας το έδαφος για ανάπτυξη των ψηφιακών υπογραφών.

Μόλις αυτή η δομή είναι έτοιμη να χρησιμοποιηθεί από απομακρυσμένους χρήστες, θα μπορεί να εξυπηρετήσει και ασύρματους απομακρυσμένους χρήστες.



Κινητή Αυθεντικοποίηση Πληρωμής.

Η κρυπτογραφία δημοσίου κλειδιού θεωρείται σαν μια προτιμώμενη αρχιτεκτονική για κινητό εμπόριο και κινητές τραπεζικές συναλλαγές. Το πιο αξιοσημείωτο χαρακτηριστικό είναι το Visa Three Domain Secure (3-D Secure). Η αρχιτεκτονική του βασίζεται στην ικανότητα να αυθεντικοποιεί έναν απομακρυσμένο κάτοχο κάρτας με ένα προκαθορισμένο μηχανισμό όπου τα απαραίτητα δεδομένα μπορούν να συλλεχτούν κατά την διάρκεια της τρέχουσας διαδικασίας. Το συγκεκριμένο πρωτόκολλο παρέχει μεθόδους αυθεντικοποίησης όπως το κοινό μυστικό, η υπογραφή και η βιομετρική.

Το πιο ασφαλές σενάριο είναι αυτό της υπογραφής το οποίο στηρίζεται στην κρυπτογραφία δημοσίου κλειδιού. Οι τοπικές δοσοληψίες θεωρούνται επίσης σαν μελλοντικές εφαρμογές των ασύρματων τηλεφώνων.

Έλεγχος Πρόσβασης .

Μία κινητή συσκευή με δυνατότητες κρυπτογράφησης δημοσίου κλειδιού μπορεί ακόμα να χρησιμοποιηθεί ως ένα μέσο αυθεντικοποίησης για πρόσβαση σε συστήματα ελέγχου, βασισμένο στους μηχανισμούς ανάκλησης-απάντησης, όπου το τηλέφωνο δέχεται μια πρόκληση από τον εξυπηρετητή και παράγει μια απάντηση. Ο μηχανισμός μπορεί να βασίζεται στην χρήση συμμετρικού ή ασύμμετρου αλγόριθμου. Οι συμμετρικοί αλγόριθμοι απαιτούν αρχικοποίηση της κινητής συσκευής με ένα μυστικό κλειδί, μοναδικό για κάθε εφαρμογή το οποίο συχνά είναι πολύ δύσκολο να εφαρμοστεί. Αντίθετα με τους ασύμμετρους αλγόριθμους που απαιτούν μόνο από τον εξυπηρετητή να επιτύχει την αυθεντικοποίηση της υπογραφής. Το Mobile Electronic Transactions (MeT) group λειτουργεί σε ένα τοπικό πρωτόκολλο αυθεντικοποίησης το οποίο ονομάζεται Personal Transaction Protocol (PTP) το οποίο θα επιτρέπει στους χρήστες να αυθεντικοποιούν τους εαυτούς τους από διάφορες θέσεις χρησιμοποιώντας τα κινητά τους τηλέφωνα.

Ψηφιακές Υπογραφές στις Κινητές Δοσοληψίες.

Οι ψηφιακές υπογραφές γίνονται με την κρυπτογραφία δημοσίου κλειδιού, το πιο πρακτικό εργαλείο στις καθημερινές εφαρμογές. Οι ψηφιακές υπογραφές αναμένεται να γίνουν ένα θεμελιώδες στοιχείο για εφαρμογές κινητών συσκευών καθώς ήδη χρησιμοποιούνται για την υπογραφή δοσοληψιών σε τραπεζικές και εμπορικές συναλλαγές στο Διαδίκτυο. Μια νέα έννοια για τις κινητές δοσοληψίες είναι οι ειδοποιήσεις (actionable alerts) που δημιουργούνται από τον πάροχο της υπηρεσίας ο οποίος στέλνει ένα μήνυμα στον χρήστη του κινητού και ο χρήστης απαντά. Μια ασφαλής εκδοχή των εφαρμογών αυτών, βασισμένη στις ψηφιακές υπογραφές και στην κρυπτογράφηση, επιτρέπει στις τράπεζες να υιοθετήσουν κινητές πλατφόρμες για να ασφαλίσουν τις τραπεζικές τους συναλλαγές.

Αυθεντικοποίηση Περιεχομένων.

Η υπογραφή κωδικών είναι μια βασική τεχνολογία για κινητές συσκευές που ενεργοποιούν αποθήκευση εφαρμογών όπως τα Java Applets. Είναι

απαραίτητο για τέτοιες συσκευές να μπορούν να διασφαλίσουν την ασφάλεια του κωδικού που αποθηκεύουν. Ο παροχέας του κωδικού μπορεί να παρέχει αυτή την ασφάλεια υπογράφοντας ψηφιακά το κωδικό με μια XML ψηφιακή υπογραφή ή Java API. Το τηλέφωνο κρατά ένα ασφαλές αντίγραφο του δημοσίου κλειδιού του υπογράφοντος, για να επιβεβαιώσει την υπογραφή του κωδικού πριν τον χρησιμοποιήσει. Η υπογραφή κωδικού όμως από μόνη της δεν βεβαιώνει την ασφάλεια του κωδικού αλλά σιγουρεύει ότι ο κωδικός δεν αλλοιώθηκε από τρίτους.
Ψηφιακά Πιστοποιητικά Ένα ψηφιακό πιστοποιητικό χαρακτηρίζει τον κάτοχο του για διάφορους σκοπούς, όπως είναι το δίπλωμα οδήγησης, η ασφάλεια υγείας κλπ.

Τα ψηφιακά πιστοποιητικά εισάγονται με την μορφή διαπιστευμάτων του χρήστη. Τα ψηφιακά πιστοποιητικά δημιουργούνται και υπογράφονται ψηφιακά από την σχετική αρχή ανάλογα με τον σκοπό τους. Όταν χρησιμοποιούνται σε ασύρματες συσκευές, τα ψηφιακα πιστοποιητικά βρίσκονται πάνω στην συσκευή και μπορούν να μεταφερθούν χρησιμοποιώντας κάποια έξυπνη κάρτα [Γ',80].

ΕΠΙΛΟΓΟΣ – ΣΥΜΠΕΡΑΣΜΑΤΑ

Τα τελευταία χρόνια οι τηλεπικοινωνίες ,τα δίκτυα και οι ηλεκτρονικές υπολογιστές μπαίνουν δυναμικά σχεδόν σε όλους τους τομείς στην ζωή μας . Η εποχή μας χαρακτηρίζεται από την σύγκλιση των τεχνολογιών πληροφορικής και τηλεπικοινωνιών .Η ζωή μας σαν άτομο αλλά και σαν κράτος έχει πολλές ευκολίες , ανέσεις και ευημερίες. Όλες σχεδόν οι πληροφορίες είτε επικοινωνιακές (τηλέφωνα) ,είτε επιχειρηματικές , είτε ιατρικές , είτε στρατιωτικές , είτε κρατικές ,είτε διεθνές έχουν μετατραπεί σε πληροφορίες ηλεκτρονικής μορφής. Όπως αναφέραμε στην εργασία ότι για αυτό το λόγο δημιουργήθηκε ένα σύστημα τηλεπικοινωνιακών δικτύων το (C^4I), ,που είναι ο συνδυασμός Πληροφοριών , Διοίκησης ,Επικοινωνιών , Ελέγχου και Επιτήρησης [(Command, Control, Communications, Consultation & Intelligence (C^4I),] Το σύστημα (C^4I) απαιτεί να υπάρχει μια διαθεσιμότητα και συνεργασία όλων των υπηρεσιών ,διοικήσεων ,επιτελείων και μονάδων στρατού και όλες οι ανταλλαγές πληροφοριών(Audio, Video, Text, Data) να γίνονται σε πραγματικό χρόνο με πολύ υψηλές ταχύτητες δεδομένων .

[A',63]

Η ιστορία του ανθρωπινού γένους μας έχει διδάξει πως ότι δημιουργείται από τον άνθρωπο και είναι προς όφελος του , σχεδόν πάντα υπάρχει ένα τρωτό σημείο,(όπως στην περίπτωση μας η παρεμβολή και ο ηλεκτρονικός πόλεμος- jamming) , που μπορεί να του δημιουργήσει πρόβλημα . Το jamming, με μορφή των επιθέσεων , των ηλεκτρομαγνητικών παρεμβολών και των συνδυασμένων απειλών στα δίκτυα και τηλεπικοινωνιακά συστήματα , το χρησιμοποιούν άλλοι για πλάκα ή για προσωπικούς στόχους , οι ανταγωνιστικές εταιρείες στην αγορά (με μορφή υποκλοπών) , οι μυστικές υπηρεσίες (ηλεκτρονική κατασκοπεία) ,οι κυβερνήσεις σε καταστάσεις υψηλού κίνδυνου (πόλεμος, τρομοκρατία ,παρακολούθησης με μορφή συνακρόασης) και αλλού με άσχημα ως καταστροφικά αποτελέσματα τόσο σαν άτομο , όσο σαν επιχείρηση ή και σαν κράτος ,κράτη (τρομοκρατία) ορισμένες φορές . Οι επιδιώξεις του εισβολέα (jammer) είναι πολλές και διάφορες ,όπως από ένα αστείο ή προσωπικό όφελος , από παράνομο οικονομικό κέρδος , από καταστροφή των συστημάτων των ανταγωνιστών και από επιθέσεις (ηλεκτρονικές) στην κρίσιμη υποδομή της χώρας από τρομοκρατικές ομάδες ή από αντίπαλα – εχθρικά κράτη. Όπως αναφέραμε στην εργασία οι τρόποι και οι μορφές jamming αλλά και anti-jamming είναι πολλοί και διάφοροι .Το φαινόμενο μπορεί να είναι κάποιο ειδικό ,συγκεκριμένο ,εξατομικευμένο αλλά και γενικό γιατί όπως είπαμε ο χώρος << μάχης >> επεκτείνεται τόσο στον απλό πολίτη όσο στον κυβερνόχωρο και θα είναι κυψελοειδούς μορφής και πολυδιάστατος . Η κυριαρχία της πληροφορίας θα αποτελεί τον κυρίως θεμελιώδη στρατιωτικό αντικειμενικό σκοπό .Συμπερασματικά θα πρέπει να προσθέσουμε ότι θα πρέπει να υπάρχει αλληλοενημέρωση των εμπλεκόμενων υπηρεσιών σε ιδιωτικό , εθνικό και διεθνές επίπεδο ως μοναδικό μέσο αποτροπής των κινδύνων και οποιασδήποτε μορφής επιθέσεων και παρεμβολών γιατί όπως αναφέραμε στην εργασία οι παρεμβολές γίνονται κυρίως από ειδικευμένο τεχνικό προσωπικό , με ακριβά τεχνικά μέσα και κυρίως σε υπηρεσίες αυξημένου ενδιαφέροντος (κράτος). Γι'αυτό οι υπεύθυνοι των τηλεπικοινωνιών και κυρίως το κράτος και σε συνεργασία με άλλα κράτη αν γίνεται ,θα πρέπει σύμφωνα με τον Γιάννη Καλογήρου (Ειδικό Γραμματέα ΚτΠ & υπουργείο Οικονομίας και Οικονομικών) στην εργασία του για τα δίκτυα και τις κρίσιμες υπηρεσίες στον πολίτη (13/5/2003), να γίνει :

- Ανάλυση υπαρχόντων και αναδυόμενων κινδύνων
- Παροχή τεχνικής υποστήριξης
- Προώθηση ανταλλαγής βέλτιστων πρακτικών
- Ανάπτυξη συνεργασιών
- Παρακολούθηση τήρησης προδιαγραφών
- Διερεύνηση ανάπτυξης νέων απαιτούμενων προδιαγραφών ασφαλείας
- Προώθηση εκτίμησης ρίσκου σε επιχειρήσεις και οργανισμούς
- Συνεργασία με τρίτες χώρες,που χρησιμοποιούνται ορισμένες φορές ως ενδιάμεσοι σταθμοί ηλεκτρομαγνητικών επιθέσεων και γενικώς όλων των μορφών επιθέσεων λόγω έλλειψη ασφαλείας και έλεγχου του κρατικού μηχανισμού .Ενθάρρυνση των χωρών αυτών για δημιουργία μιας κοινής προσέγγισης για την διασφάλιση της ασφάλειας .

Και θα πρέπει να είμαστε πολλοί επιφυλακτικοί γιατί όπως δείχνει το παρακάτω πολυσήμαντο σχήμα του Γιώργου Λέκατη ότι η αλήθεια είναι ότι γενικώς ας υπάρχει ένας γενικός υπαρκτός κίνδυνος ,ένα μέρος αυτού είναι γνωστός αλλά εμείς μόνο ένα πολύ μικρό μέρος κινδύνου ελέγχουμε.

ΠΑΡΑΡΤΗΜΑ

ΒΑΣΙΚΑ ΠΡΟΤΥΠΑ ΚΑΙ ΕΝΝΟΙΕΣ ΑΠΑΡΑΙΤΗΤΕΣ ΣΤΑ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

S-BLUETOOTH.

Η ασύρματη τεχνολογία Bluetooth επέφερε μια επανάσταση στον τομέα της σύνδεσης σε προσωπικό επίπεδο, παρέχοντας ελευθερία στις καλωδιακές συνδέσεις. Επιτρέπει τη σύνδεση ανάμεσα σε φορητούς υπολογιστές, κινητά τηλέφωνα, φορητές συσκευές χειρός καθώς και τη σύνδεση στο Internet.
Αντίθετα με άλλα ασύρματα πρότυπα, το Bluetooth περιλαμβάνει ορισμούς και για το επίπεδο σύνδεσης (Link layer) αλλά και το επίπεδο εφαρμογής (Application layer). Λειτουργεί στα 2.4 GHz διασφαλίζοντας συμβατή επικοινωνία σε παγκόσμιο επίπεδο. Τα χαρακτηριστικά της τεχνολογία Bluetooth είναι τα εξής:
Διαιρεί το εύρος συχνοτήτων. Αυτός ο διαχωρισμός χρησιμοποιείται για την αναπήδηση από το ένα κανάλι σε άλλο, χαρακτηριστικό το οποίο προσθέτει ένα ισχυρό επίπεδο ασφάλειας.
Μπορεί να συνδέσει μμέχρι και 8 συσκευές.
Υποστηρίζει σύγχρονες αλλά και ασύγχρονες εφαρμογές.
Περιλαμβάνει επίσης ένα ειδικό λογισμικό ελέγχου και κωδικοποίησης ταυτότητας ώστε να μμπορούν να επικοινωνήσουν μόνο οι συσκευές που έχουν οριστεί από τους ιδιοκτήτες τους.

Τεχνική προδιαγραφή Bluetooth

Η τεχνολογία είναι σχεδιασμένη για να λειτουργήσει σε εξαιρετικά δυσμενές περιβάλλον ράδιο-θορύβου. Η ευέλικτη σχεδίαση στηρίζεται στη ραδιομετάδοση σε πολλαπλές συχνότητες με αυτόματη και πολύ γρήγορη μεταλλαγή (αναπήδηση συχνότητας σύμφωνα με την επικρατούσα αδόκιμη απόδοση του όρου frequency hopping). Το σύστημα εκτελεί 1600 αλλαγές συχνότητας το δευτερόλεπτο. Πρόκειται για εντυπωσιακή ταχύτητα, αν λάβετε υπόψη σας, ότι πριν 5-6 χρόνια τέτοιες επιδόσεις ήταν απόρρητα στρατιωτικά μυστικά και κόστιζαν εκατομμύρια δολάρια. Τ ο πρωτόκολλο που ενσωματώνει η τεχνολογία Bluetooth στηρίζεται στη μεταγωγή «ψηφιακών πακέτων πληροφορίας». Κάθε πακέτο μεταδίδεται σε διαφορετική συχνότητα, ενώ συνήθως καταλαμβάνει μόνο μία χρονοθυρίδα (time slot) μετάδοσης, χωρίς όμως να περιορίζεται σ' αυτή, δεδομένου ότι –εφ' όσον απαιτηθεί- μπορούν να καταληφθούν έως και 5 χρονοθυρίδες. Χρησιμοποιείται και εδώ η τεχνική της χρονικής πολυπλεξίας, δηλαδή της ταυτόχρονης χρήσης μίας συχνότητας από πολλά διαφορετικά σήματα που είναι χρονικά καταμερισμένα (Time Division Multiple Access , TDMA). Η τεχνική πρωτοεφαρμόστηκε εμπορικά στη κινητή τηλεφωνία GSM και μέσα σε 5 χρόνια αντικατέστησε όλα τα παλαιότερα συστήματα ραδιομετάδοσης σε κάθε σύγχρονη εφαρμογή τηλεπικοινωνιών .Η μετάδοση της πληροφορίας γίνεται στη περιοχή των μικροκυμάτων. Χρησιμοποιείται η ζώνη συχνοτήτων των 2,45 GHz , που έχει αποδοθεί σε ελεύθερη χρήση διεθνώς και λέγεται «ζώνη συχνοτήτων για βιομηχανική, επιστημονική και ιατρική χρήση» (Industrial , Scientific and Medical Band , ISM Band).

Κάθε πακέτο πληροφορίας μεταβιβάζεται σε διαφορετική συχνότητα. Χρησιμοποιείται ένα είδος διαμορφώσεως τονικής εναλλαγής (2 FSK).

CDMA I (Multiband Synchronous Dierct Sequence CDMA I).

Το σύστημα CDMA one είναι ένα πλήρες ασύρματο σύστημα πολλαπλής πρόσβασης που βασίζεται στα πρωτόκολλα IS-95A και IS-95B. Εκπροσωπεί ασύρματα συστήματα και εφαρμογές από-άκρο-σε-άκρο και όλες τις απαραίτητες προδιαγραφές που περιβάλλουν τη λειτουργία του. Το CDMA one όταν χρησιμοποιηθεί μπορεί να:

- Αυξήσει τη χωρητικότητα από 8 μέχρι 10 φορές σε ένα αναλογικό σύστημα AMPS και 4 με 5 φορές σε ένα κυψελωτό δίκτυο GSM,

Δώσει καλύτερη ποιότητα ομιλίας σε σχέση με τα υπάρχοντα αναλογικά δίκτυα,

- Απλοποιήσει τη διαδικασία σχεδιασμού του δικτύου γιατί γίνεται χρήση μιας συχνότητας για όλο το δίκτυο,
- Αυξήσει την προστασία των δεδομένων και των κλήσεων
- Δώσει βελτιωμένα χαρακτηριστικά κάλυψης γιατί μπορεί να υλοποιηθεί με λιγότερους σταθμούς,
- Αυξήσει το χρόνο ομιλίας χρησιμοποιώντας λιγότερη ενέργεια για τη λειτουργία του
- Δώσει εύρος ζώνης ανάλογο της ζήτησης (bandwidth on demand)
-

MMAC (Multimedia Mobile Access Communication).

Το σύστημα MMAC αποτελεί την τηλεπικοινωνιακή τεχνολογία που μπορεί να δώσει στους χρήστες πολύ μεγάλες ταχύτητες δεδομένων με απώτερο στόχο την κάλυψη ποιότητας στις εφαρμογές πολυμέσων κάνοντας χρήση συνδέσεων σε δακτυλίους οπτικών ινών. Ο χρόνος έναρξης της εφαρμογής είναι το έτος 2002 και συνοπτικά οι δυνατότητες του συστήματος είναι:

Υψηλές ταχύτητες δεδομένων μέχρι 30Mbps για ασύρματη χρήση όπως για παράδειγμα το ασύρματο τηλέφωνο ποθ υποστηρίζει και video

Ασύρματα τοπικά δίκτυα με ταχύτητες μέχρι 156Mbps που μπορούν να ικανοποιήσουν και απαιτήσεις εικονοσύσκεψης.

Πρόσβαση ATM για ασύρματα τοπικά δίκτυα με εύρος ζώνης μέχρι 5MHz που μπορεί να δώσει ταχύτητες 20-25Mbps.

IMT-2000.

Ο όρος IMT-2000 αναφέρεται σε μια υπηρεσία κινητής επικοινωνίας, η οποία παρέχει μια μεγάλη ποικιλία ασύρματων υπηρεσιών, με δυνατότητα μετάδοσης πολυμεσικών υπηρεσιών σε υψηλές ταχύτητες. Η κινητή επικοινωνία έχει εξελιχθεί από πρώτης γενιάς (αναλογική), σε δεύτερης γενιάς (ψηφιακή), και τελικά στην τρίτης γενιάς που είναι η τεχνολογία IMT-2000.

Η τεχνολογία IMT-2000 επιτρέπει στους χρήστες την μετάδοση φωνής, δεδομένων ακόμη και κινούμενων εικόνων. Για την επίτευξη αυτών των υπηρεσιών, η ταχύτητα μετάδοσης των δεδομένων κυμαίνεται από 144kbps έως και 2Mbps.

Η IMT-2000 χρησιμοποιεί το παγκοσμίως κοινό εύρος συχνότητας των 2GHZ, ενώ επιλέγει από 5 έως 20MHz για την παροχή των πολυμεσικών υπηρεσιών. Κάτω από τις τρέχουσες συνθήκες, η ταχύτητα μετάδοσης των δεδομένων κυμαίνεται από 64kbps έως 384kbps, ενώ αναμένεται το 2005, η ταχύτητα αυτή να φτάνει τα 2Mbps.

Το πρότυπο IEEE 802.11

Ένα ασύρματο τοπικό δίκτυο είναι αυτό στο οποίο ένας κινούμενος χρήστης μπορεί να συνδεθεί σε ένα τοπικό δίκτυο μέσω μια ασύρματης σύνδεσης. Το πρότυπο IEEE 802.11 περιγράφει τις τεχνολογίες που χρησιμοποιούνται στα ασύρματα τοπικά δίκτυα.

Το 802.11 είναι μια οικογένεια προδιαγραφών για ασύρματα τοπικά δίκτυα που αναπτύχθηκαν από ομάδες εργασίας του ινστιτούτου ηλεκτρολόγων και ηλεκτρονικών μηχανικών, το γνωστό institute of electrical and electronics engineers (IEEE).

Όλα τα πρότυπα που περιλαμβάνει το 802.11, χρησιμοποιούν το πρωτόκολλο ethernet και μέθοδο πολλαπλής πρόσβασης με ανίχνευση φέροντος και αποφυγή συγκρούσεων, το carrier sense multiple access with collision avoidance (csma/ca). Η μέθοδος διαμόρφωσης που χρησιμοποιήθηκε αρχικά ήταν το κλείδωμα μεταλλαγής φάσης ή διαμόρφωση διακριτής φάσης, phase-shift keying (psk). Σε νεότερες προδιαγραφές όμως, χρησιμοποιούνται και άλλα σχήματα ψηφιακής διαμόρφωσης, όπως το complementary code keying (cck). Οι νεότερες μέθοδοι διαμόρφωσης παρέχουν μεγαλύτερους ρυθμούς μετάδοσης δεδομένων.

Αυτή τη στιγμή υπάρχουν 4 πρότυπα στην οικογένεια 802.11: 802.11, 802.11a, 802.11b, 802.11g και μέχρι το τέλος του έτους αναμένεται να εγκριθούν τα 802.11i και 802.11e. Και τα 4 χρησιμοποιούν το πρωτόκολλο ethernet και μέθοδο πολλαπλής πρόσβασης με ανίχνευση φέροντος και αποφυγή συγκρούσεων, το carrier sense multiple access with collision avoidance (csma/ca).

IEEE 802.11: εφαρμόζεται σε ασύρματα τοπικά δίκτυα και παρέχει ρυθμούς μετάδοσης 1 ή 2Mbps στη μπάντα των 2.4GHz.

IEEE 802.11a: είναι μια επέκταση του 802.11 που εφαρμόζεται σε ασύρματα τοπικά δίκτυα και παρέχει ρυθμούς μετάδοσης έως 54Mbps στη μπάντα των 5GHz. Συνήθως όμως οι επικοινωνίες πραγματοποιούνται στα 6Mbps, 12Mbps ή στα 24Mbps και χρησιμοποιείται πολυπλεξία επιμερισμού συχνότητας. Χρησιμοποιείται σε ασύρματα δίκτυα ATM.

IEEE 802.11b: συνήθως το λέμε wi-fi και είναι συμβατό με το 802.11. Η μέθοδος διαμόρφωσης που χρησιμοποιήθηκε στο 802.11 ήταν το κλείδωμα μεταλλαγής φάσης ή διαμόρφωση διακριτής φάσης, phase-shift keying (psk). Η μέθοδος διαμόρφωσης που επιλέχθηκε για το 802.11b είναι γνωστή ως complementary code keying (cck) και παρέχει μεγαλύτερους ρυθμούς μετάδοσης δεδομένων.

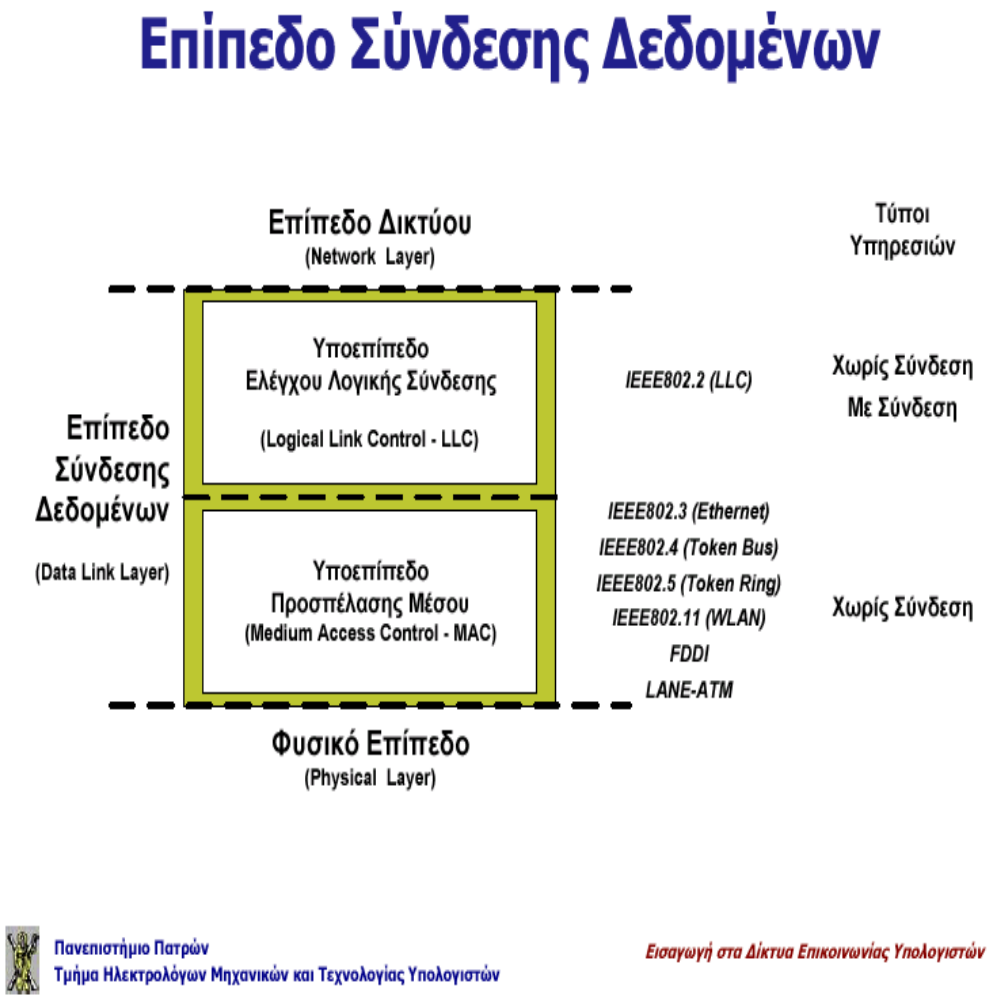
IEEE 802.11e: το πρώτο ασύρματο πρότυπο για οικιακό ή εταιρικό δικτυακό περιβάλλον. Παρέχει χαρακτηριστικά ποιότητας υπηρεσιών και υποστήριξη πολυμέσων στα υπάρχοντα ασύρματα πρότυπα IEEE 802.11a και IEEE 802.11b ενώ ταυτόχρονα είναι και συμβατό με αυτά. Η ποιότητα υπηρεσιών και υποστήριξη πολυμέσων είναι ένας κρίσιμος παράγοντας στα ασύρματα οικιακά δίκτυα που θέλουμε να παρέχουν φωνή, video και ήχο (video on demand, audio on demand, voice over ip, υψηλής ταχύτητας πρόσβαση στο internet).

IEEE 802.11g: εφαρμόζεται σε ασύρματα τοπικά δίκτυα και παρέχει ρυθμούς μετάδοσης άνω των 20mbps στη μπάντα των 2.4GHz. Αυτό είναι το πρότυπο που εγκρίθηκε πιο πρόσφατα και παρέχει ασύρματη μετάδοση σε σχετικά κοντινές αποστάσεις με ταχύτητες μέχρι και 54mbps συγκριτικά με τα 11mbps του πρότυπου 802.11b. Όπως και το 802.11b, το IEEE 802.11g λειτουργεί στη μπάντα των 2.4GHz οπότε είναι συμβατό με αυτό.

IEEE 802.11i: προσθέτει στο 802.11 πρότυπο ασύρματων τοπικών δικτύων, το πρωτόκολλο ασφάλειας advanced encryption standard (aes).

Ορθογώνια πολυπλεξία συχνότητας (Orthogonal Frequency Division Multiplexing-OFDM)

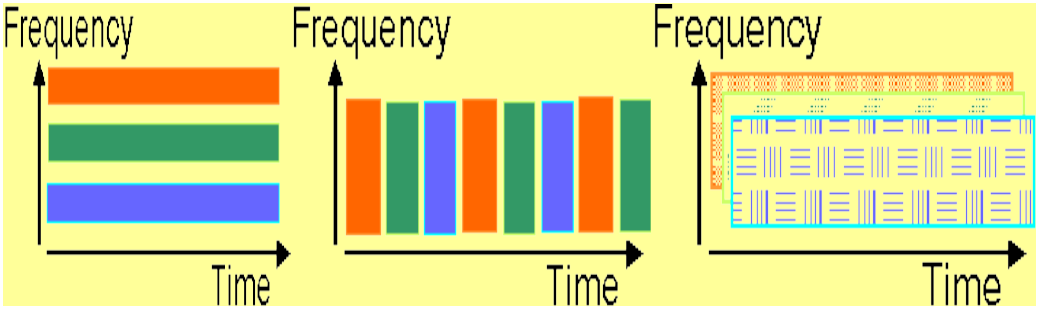
Η κωδικοποίηση OFDM, είναι μια μορφή διαμόρφωσης πολλών φερόντων σημάτων και διαφέρει από αυτήν της διασποράς φάσματος. Η τεχνική OFDM χωρίζει το σήμα σε πολλά μικρότερα υποσήματα, τα οποία και εκπέμπει σε διαφορετικές συχνότητες. Αυτό μειώνει τη διαφωνία (crosstalk) στις μεταδόσεις σημάτων, κάτι το οποίο καθιστά το OFDM πολύ χρήσιμο για τη μετάδοση υψίρρυθμων και ευρυζωνικών πληροφοριών. Επίσης, με τον τρόπο αυτό, η μετάδοση είναι πολύ ανθεκτική στις παρεμβολές. Η IEEE επέλεξε να χρησιμοποιήσει OFDM στο πρότυπο 802.11 a, με ταχύτητα μετάδοσης μέχρι 54Mbps. Η ίδια διαμόρφωση χρησιμοποιείται στην τεχνολογία ADSL, που πετυχαίνει υψηλότατες ταχύτητες στα κοινά τηλεφωνικά δίκτυα, αλλά και στην επερχόμενη ψηφιακή τηλεόραση. Είναι μια τεχνολογία, που ενώ είχε αναλυθεί σε θεωρητικό επίπεδο εδώ και χρόνια, έκανε ξαφνικά, δυναμική εμφάνιση στη σκηνή των ψηφιακών επικοινωνιών και κατέλαβε εξ εφόδου όλες τις νέες εφαρμογές.



ΠΟΛΥΠΛΕΞΙΑ

Πολυπλεξία είναι η **μετάδοση** πολλών σημάτων πληροφορίας μέσα από το ίδιο κανάλι (**πολυπλεξία**). Υπάρχουν 3 τρόποι πολυπλεξίας
•**Πολυπλεξία στην συχνότητα (FDM –** Frequency Division Multiplexing). Κάθε σήμα πληροφορίας χρησιμοποιεί διαφορετική ζώνη συχνοτήτων
•**Πολυπλεξία στον χρόνο (TDM –**Time Division Multiplexing**).** Κάθε σήμα πληροφορίας καταλαμβάνει διαφορετική χρονοσχισμη.
•**Πολυπλεξία με κώδικα (CDM** – Code Division Multiplexing). Κάθε σήμα πληροφορίας διακρίνεται από τα αλλά με ειδικό κώδικα
•**Πολυπλεξία με διαίρεση μήκους κύματος (WDM-** Wavelength Division Multiplexing). Μορφή του FDM με εφαρμογή στις οπτικές ίνες.

Η τεχνολογία διασποράς φάσματος –με τη μορφή του συστήματος κωδικομεριστικής πολυπλεξίας (Code Division Multiple Access , CDMA) , χρησιμοποιείται στη κινητή τηλεφωνία των ΗΠΑ, της Ιαπωνίας, της Κορέας και της Κίνας, παράλληλα με το γνωστό μας σύστημα GSM . Αν και ακόμη υπολείπεται σε διάδοση, το σύστημα CDMA και οι παραλλαγές του (CDMA - One , CDMA -2000, W - CDMA) είναι τόσο προηγμένο τεχνολογικά, που είναι βέβαιο ότι θα αποτελέσει το πρότυπο για τη κινητή τηλεφωνία τρίτης γενιάς. Χρησιμοποιείται, επιπλέον, σε όλα τα πρότυπα ασύρματης δικτύωσης των ηλεκτρονικών συσκευών (τοπικά ασύρματα δίκτυα Bluetooth , και Wi - Fi ή IEEE 802.11 x).



ΠΡΟΓΡΑΜΜΑΤΑ

SECUREPHONE: ***Secure contracts signed by telephone***
Χρηματοδοτημένο κάτω από το ***6th FWP*** (***Sixth Framework Programme***)
Γραμμή δράσης: Προς ένα σφαιρικό πλαίσιο αξιοπιστίας και ασφάλειας

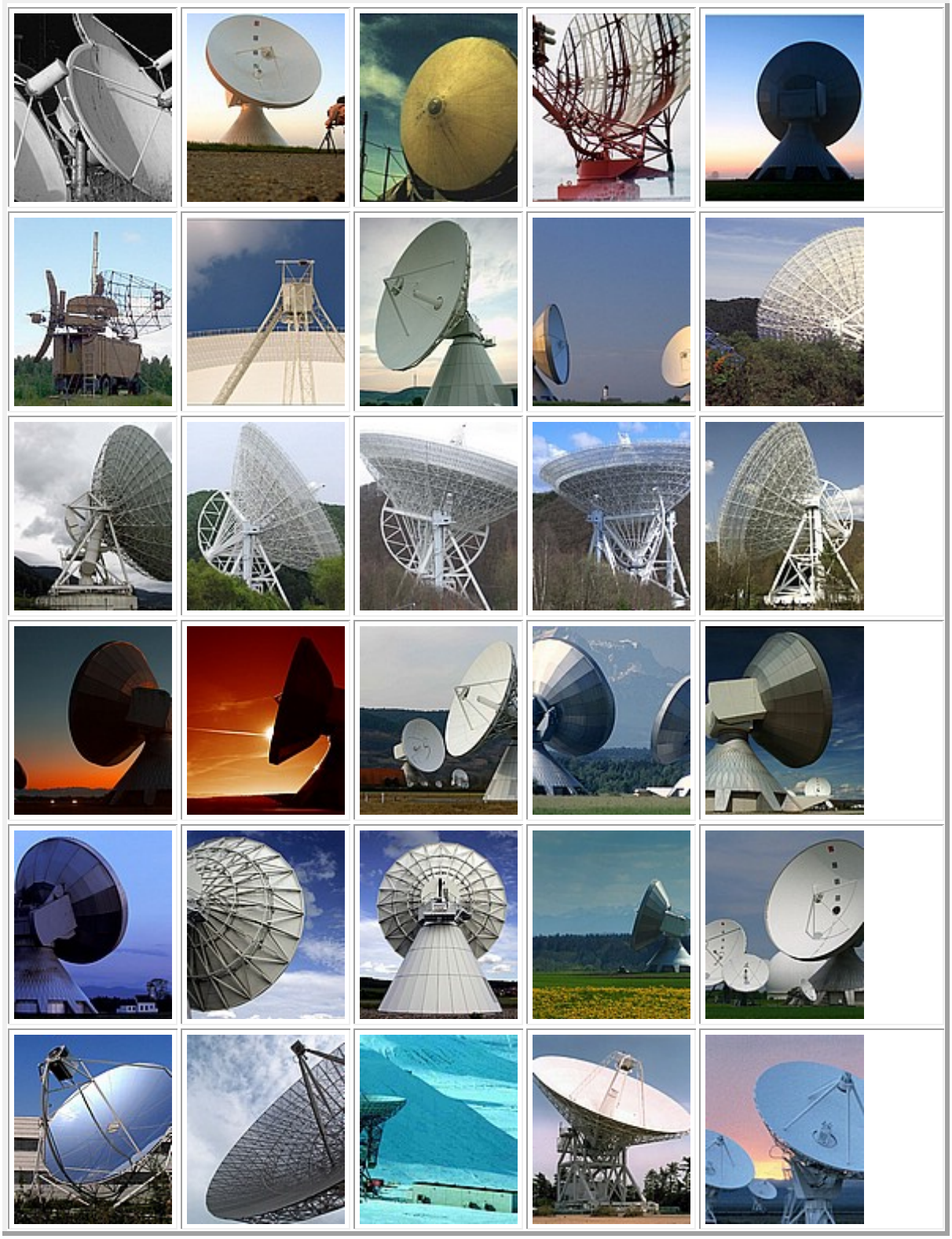
Το πρόγραμμα SecurePhone στοχεύει στην ανάπτυξη μιας νέας υποδομής για το σύστημα κινητής επικοινωνίας οι οποία θα εξασφαλίζει με έναν φιλικό τρόπο την αμοιβαία αναγνώριση των ομιλητών στο κινητό τηλέφωνο επιτρέποντάς τους να διαπραγματεύονται δεσμευτικά νόμιμα ηλεκτρονικά-συμβόλαια μέσα από μία κλήση από το κινητό τηλέφωνο. Η υπάρχουσα υποδομή επικοινωνίας, υστερεί στην αυστηρή αναγνώριση των χρηστών, δεν μπορεί να χρησιμοποιηθεί για δεσμευτικές νόμιμες συναλλαγές. Η λύση που προτείνεται από αυτό το πρόγραμμα είναι να πραγματοποιήσει ένα καινοτόμο πρωτότυπο 3G/B3G, επιτρέποντας την ενίσχυση του PDA με έναν "βιομετρικό

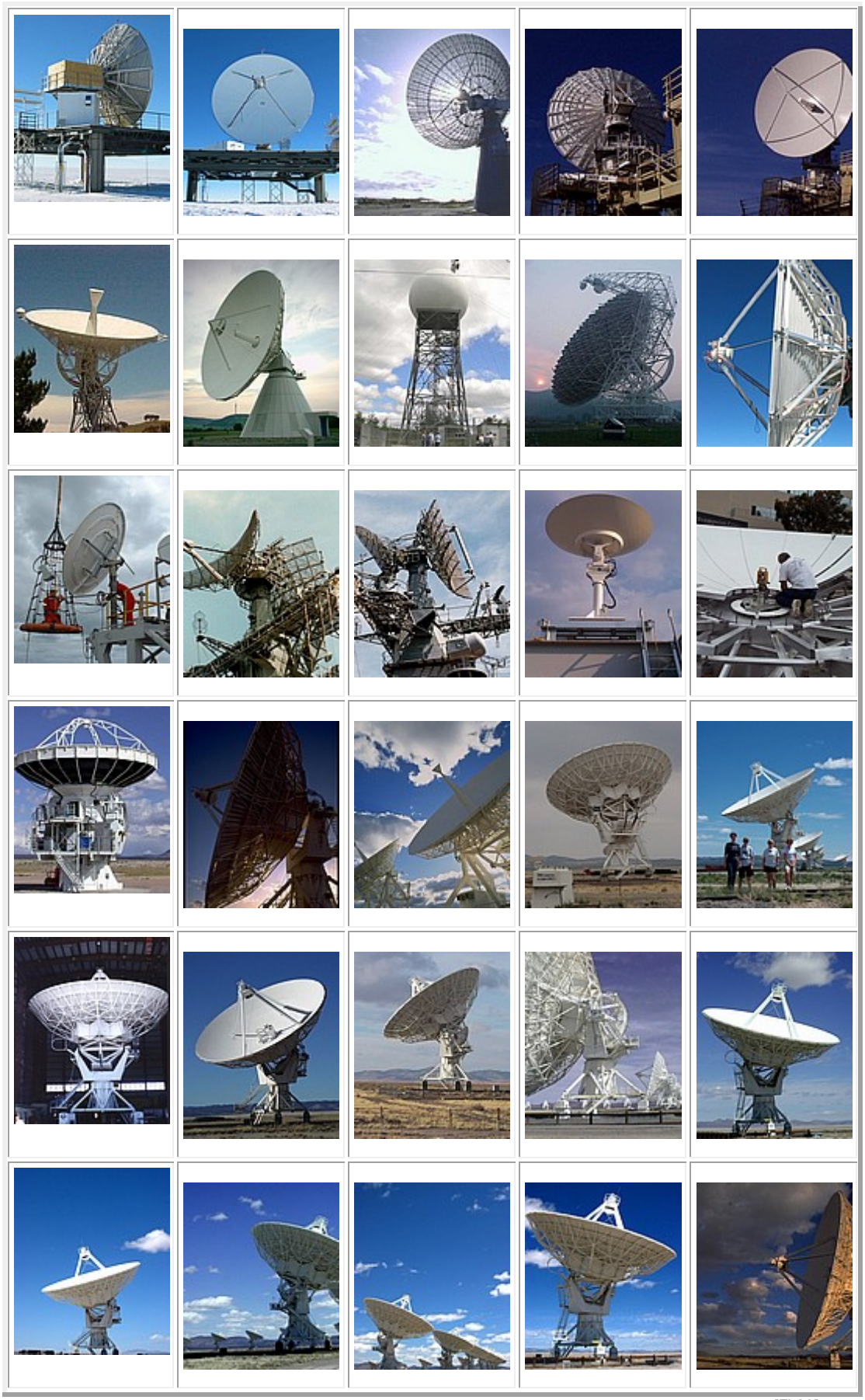
αναγνωριστή" προκειμένου να επιτραπεί στους χρήστες να αναγνωρίζουν αμοιβαία ο ένας τον άλλο και να επικυρώνονται με ασφάλεια. Το πρόγραμμα SecurePhone στη συνέχεια θα επιτρέψει στους χρήστες να ανταλλάσσουν και να τροποποιούν με ασφάλεια αρχεία ήχου, εικόνας ή/και κειμένου, και τελικά να τα υπογράφουν ηλεκτρονικά κατά τη διάρκεια ενός τηλεφωνήματος. Ειδικότερα, το πρόγραμμα SecurePhone θα επιτρέψει να γίνεται η ηλεκτρονική-υπογραφή φωνητικών δηλώσεων "on the fly".
Βιομετρικά αναγνωρισμένοι χρήστες θα έχουν πρόσβαση στις ενσωματωμένες ιδιαίτερες και καινοτόμες εγκαταστάσεις για ηλεκτρονική-υπογραφή της συσκευής. Το σύστημα θα επιτρέπει στους χρήστες, χωρίς την ανάγκη για είσοδο πρόσθετων αριθμητικών PIN, να υπογράφουν ηλεκτρονικά και να στέλνουν δεδομένα, ταυτόχρονα με τη φωνή, κατά τη διάρκεια ενός κανονικού τηλεφωνήματος, χρησιμοποιώντας την υποδομή PKI που βρίσκεται στην κάρτα SIM της συσκευής τους. Ειδικότερα, στους χρήστες θα δοθεί η ευκαιρία να επιλέγουν μεταξύ της διαβίβασης των κωδικοποιημένων ακουστικών αρχείων ή αρχείων κειμένου, που παράγονται αυτόματα μέσο μιας μετατροπής φωνής σε κείμενο (speech-to-text conversion).

Λεπτομέρειες προγράμματος

Αρκτικόλεξο προγράμματος: SECUREPHONE
Αναφορά προγράμματος: 506883
Διάρκεια: 30 μήνες
Κόστος προγράμματος: 3.30 εκατ. ευρώ
Χρηματοδότηση προγράμματος: 2.00 εκατ. ευρώ

ΕΙΔΗ ΡΑΝΤΑΡ





[Γ',20]

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΠΕΡΙΟΔΙΚΑ

1. *CHIP ΤΕΥΧΟΣ 21 ΟΚΤΩΒΡΙΟΣ 2004*
2. *CHIP ΤΕΥΧΟΣ 8 , ΑΥΓΟΥΣΤΟΣ 2006,*
3. *COMPUTER ACTIVE ΤΕΥΧΟΣ 8 ,8/2005*
4. *COMPUTER ACTIVE , ΤΕΥΧΟΣ 10 ΝΟΕΜΒΡΙΟΣ 2005*
5. *COMPUTER ACTIVE , ΤΕΥΧΟΣ 11 ΔΕΚΕΜΒΡΙΟΣ 2005*
6. *COMPUTER ACTIVE , ΤΕΥΧΟΣ 12 ΙΑΝΟΥΑΡΙΟΣ 2006,*
7. *COMPUTER ACTIVE , ΤΕΥΧΟΣ 14 ΜΑΡΤΙΟΣ 2006*
8. *COMPUTER ACTIVE , ΤΕΥΧΟΣ 15 ΑΠΡΙΛΙΟΣ 2006*
9. *COMPUTER ACTIVE , ΤΕΥΧΟΣ 16 ΜΑΙΟΣ 2006*
10. *COMPUTER ACTIVE , ΤΕΥΧΟΣ 17 ΙΟΥΝΙΟΣ 2006*
11. *COMPUTER ACTIVE , ΤΕΥΧΟΣ 18 ΙΟΥΛΙΟΣ 2006,*
12. *COMPUTER ACTIVE , ΤΕΥΧΟΣ 7 ΙΟΥΛΙΟΣ – ΑΥΓΟΥΣΤΟΣ 2005*
13. *COMPUTER ACTIVE , ΤΕΥΧΟΣ 8 ΣΕΠΤΕΜΒΡΙΟΣ 2005*
14. *COMPUTER ΓΙΑ ΟΛΟΥΣ , ΤΕΥΧΟΣ 237, ΜΑΙΟΣ 2004*
15. *COMPUTER ΓΙΑ ΟΛΟΥΣ , ΤΕΥΧΟΣ 244, ΔΕΚΕΜΒΡΙΟΣ 2004*
16. *COMPUTER ΓΙΑ ΟΛΟΥΣ , ΤΕΥΧΟΣ 263, ΙΟΥΛΙΟΣ 2006.*
17. *COMPUTER ΤΡΙΤΗ ,ΤΕΥΧΟΣ 10 , 9 ΜΑΙΟΥ 2006*
18. *COMPUTER ΤΡΙΤΗ ,ΤΕΥΧΟΣ 11 , 23 ΜΑΙΟΥ 2006*
19. *COMPUTER ΤΡΙΤΗ , ΤΕΥΧΟΣ 8 11 ΑΠΡΙΛΙΟΥ 2006*
20. *COMPUTER ΤΡΙΤΗ ΤΕΥΧΟΣ 9 25 ΑΠΡΙΛΙΟΥ 2006*
21. *DIGITAL TV SAT , ΤΕΥΧΟΣ 81, ΣΕΠΤΕΜΒΡΙΟ 2005*
22. *DIGITAL WORLD, ΤΕΥΧΟΣ 6 , 7/8/2005*
23. *MOBILE , ΤΕΥΧΟΣ 4, ΙΟΥΛΙΟΣ 2006*
24. *PC MAGAZINE, ΕΛ. .ΕΚΔΟΣΗ ,ΤΕΥΧΟΣ 2 , , (2/2006)*
25. *PC MAGAZINE ΕΛ. .ΕΚΔΟΣΗ , ΤΕΥΧΟΣ 3 , (3 / 2006)*
26. *PC MAGAZINE, ΕΛ. .ΕΚΔΟΣΗ , ΤΕΥΧΟΣ 4 , (4 / 2006)*
27. *PC MAGAZINE, ΕΛ. .ΕΚΔΟΣΗ , ΤΕΥΧΟΣ 7 , (7/2006)*
28. *PC WORLD , ΕΛ. ΕΚΔΟΣΗ , ΤΕΥΧΟΣ 16 , ΜΑΙΟΣ 2006*
29. *PC WORLD , ΕΛ. ΕΚΔΟΣΗ , ΤΕΥΧΟΣ 20 , ΣΕΠΤΕΜΒΡΙΟΣ 2006*
30. *RAM , ΤΕΥΧΟΣ 175, ΔΕΚΕΜΒΡΙΟ 2003*
31. *RAM , ΤΕΥΧΟΣ 202, ΜΑΙΟΣ 2006,*
32. *RAM , ΤΕΥΧΟΣ 203, ΙΟΥΝΙΟΣ 2006,*
33. *ΚΙΝΗΤΑ ΝΕΑ (100) ΜΑΡΤΙΟΣ 2006,*
34. *ΡΑΔΙΟΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ, ΤΕΥΧΟΣ 41, ΜΑΙΟΣ –ΙΟΥΝΙΟΣ 2002*
35. *ΡΑΔΙΟΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ , Τ ΕΥΧΟΣ 42 ,ΙΟΥΛΙΟ – ΑΥΓΟΥΣΤΟ 2002*
36. *ΡΑΔΙΟΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ, ΤΕΥΧΟΣ 51,ΙΑΝΟΥΑΡΙΟΣ-ΦΕΒΡΟΥΑΡΙΟΣ 2004*
37. *ΡΑΔΙΟΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ ,ΤΕΥΧΟΣ 56 ΝΟΕΜΒΡΙΟΣ- ΔΕΚΕΜΒΡΙΟΣ 2004*
38. *ΡΑΔΙΟΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ ,ΤΕΥΧΟΣ 57 ,ΙΑΝΟΥΑΡΙΟΣ-ΦΕΒΡΟΥΑΡΙΟΣ 2005*
39. *ΡΑΔΙΟΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ, ΤΕΥΧΟΣ 58 ,ΜΑΡΤΙΟΣ – ΑΠΡΙΛΙΟΣ 2005*
40. *ΡΑΔΙΟΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ, ΤΕΥΧΟΣ 59 ,ΜΑΙΟΣ –ΙΟΥΝΙΟΣ 2005*
41. *ΡΑΔΙΟΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ ,ΤΕΥΧΟΣ 61, ΣΕΠΤΕΜΒΡΗΣ – ΟΚΤΩΒΡΙΟΣ 2005*
42. *ΡΑΔΙΟΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ, ΤΕΥΧΟΣ 63, ΙΑΝΟΥΑΡΙΟΣ-ΦΕΒΡΟΥΑΡΙΟΣ 2006*
43. *ΡΑΔΙΟΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ,ΤΕΥΧΟΣ 63,ΙΑΝΟΥΑΡΙΟΣ-ΦΕΒΡΟΥΑΡΙΟΣ 2006*
44. *ΡΑΔΙΟΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ ,ΤΕΥΧΟΣ 65,ΜΑΙΟΣ – ΙΟΥΝΙΟΣ 2006*
45. *ΡΑΔΙΟΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ , ΤΕΥΧΟΣ 40, ΜΑΡΤΙΟΣ – ΑΠΡΙΛΙΟΣ 2002*
46. *ΤΕΧΝΙΚΗ ΕΚΛΟΓΗ ,ΤΕΥΧΟΣ 469 , ΜΑΡΤΙΟ 2006*
47. *ΤΕΧΝΙΚΗ ΕΚΛΟΓΗ , ΤΕΥΧΟΣ 470 , ΑΠΡΙΛΙΟ 2006*
48. *ΤΕΧΝΙΚΗ ΕΚΛΟΓΗ , ΤΕΥΧΟΣ 472 , ΙΟΥΝΙΟΣ 2006*
49. *ΤΕΧΝΙΚΗ ΕΚΛΟΓΗ , ΤΕΥΧΟΣ 462, ΙΟΥΛΙΟΣ – ΑΥΓΟΥΣΤΟΣ 2005*
50. *ΤΕΧΝΙΚΗ ΕΚΛΟΓΗ , ΤΕΥΧΟΣ 463 , ΣΕΠΤΕΜΒΡΙΟΣ 2006*
51. *ΤΕΧΝΙΚΗ ΕΚΛΟΓΗ , ΤΕΥΧΟΣ 473, ΙΟΥΛΙΟΣ – ΑΥΓΟΥΣΤΟΣ 2006*
52. *ΤΕΧΝΙΚΗ ΕΚΛΟΓΗ , ΤΕΥΧΟΣ 464 , ΟΚΤΩΒΡΙΟ 2005*
53. *ΤΕΧΝΙΚΗ ΕΚΛΟΓΗ , ΤΕΥΧΟΣ 467, ΙΑΝΟΥΑΡΙΟΣ 2006,*
54. *ΤΕΧΝΙΚΗ ΕΚΛΟΓΗ , ΤΕΥΧΟΣ 472 , ΙΟΥΝΙΟΣ 2006,*
55. *ΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ &COMPYTERS INTERNATIONAL ,τευχος 1 ,Απριλίου 2006*

ΒΙΒΛΙΟΓΡΑΦΙΑ [Β']
(ΒΙΒΛΙΑ)

1. ***DIGITAL COMMUNIKATION THIRD EDITION του JOHN R.BARRY , EDWARD A. LEE, DAVID G. MESSERSCHMITT,KLUWER ACADEMIC PUBLISHERS***
2. ***WIRELESS , COMMUNIKATIONS (PRINCIPLES AND PRACTICE) SECOND ENITION του THEODORE S. RAPPAPORT, (PRENTICE HALL COMMUNIKATION)ENGINEERING AND EMERGING TECHNOLOGIES SERIES , THEODORE S. RAPPAPORT ,SERIES EDITOR***
3. ***ΔΙΑΔΟΣΗ ΗΛΕΚΤΡΟΜΑΓΝΗΤΙΚΩΝ ΚΥΜΑΤΩΝ ΣΕ ΓΗΙΝΟ ΠΕΡΙΒΑΛΛΟΝ του Ι.Δ.ΚΑΝΕΛΛΟΠΟΥΛΟΣ (ΚΑΘΗΓΗΤΗΣ Ε.Μ.Π.) ΕΚΔΟΣΕΙΣ ΤΣΙΟΛΑ***
4. ***ΚΡΥΠΤΟΓΡΑΦΙΑ (Η επιστήμη της ασφαλούς επικοινωνίας) του Δημήτρη Μ. Πουλάκη , εκδόσεις ΖΗΤΗ ΘΕΣ/ΝΙΚΗ***
5. ***ΜΕΤΑΔΟΣΗ ΔΕΔΟΜΕΝΩΝ ΧΩΡΙΣ ΠΑΡΕΜΒΟΛΕΣ (HANS HEUBLEIN) ΕΚΔΟΣΕΙΣ ΤΣΙΟΛΑ***
6. ***ΣΗΜΕΙΩΣΕΙΣ ΔΙΑΛΕΞΗΣ του ΣΤΕΡΓΙΟΥ ΕΛΕΥΘΕΡΙΟΥ ,ΣΤΟ ΜΑΘΗΜΑ (ΤΟΥ Ε΄ΕΞΑΜΗΝΟΥ ΤΟΥ ΤΜΗΜΑΤΟΣ ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ)ΑΣΥΡΜΑΤΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ – ΔΙΚΤΥΑ , ΑΡΤΑ 2002-2003***
7. ***ΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ & COMPUTERS INTERNATIONAL, ΤΕΥΧΟΣ 1 , ΑΠΡΙΛΙΟΣ 2006,***
8. ***ΨΗΦΙΑΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ του ANDY BATEMAN , ΕΚΔΟΣΕΙΣ ΤΣΙΟΛΑ***
9. ***Scanner Busters2 . O.C.Poole , έκδοση Interproducts (μετάφραση Τεχνική εκλογή)***

ΒΙΒΛΙΟΓΡΑΦΙΑ
(ΗΛΕΚΤΡΟΝΙΚΗΣ ΜΟΡΦΗΣ –ΙΣΤΟΣΕΛΙΔΕΣ)

1. ΗΜΥ 007 – **Τεχνολογία Πληροφορίας**
   Διάλεξη 10,Σύστημα ΤηλεφώνουΜέρος Β, ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ,ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ ,ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ
4. ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ τεχνολογίας ΔΙΑΣΠΟΡΑΣ ΦΑΣΜΑΤΟΣ
5. TechTeam Community > Forums > Internet και Δίκτυα Ηλεκτρονικών Υπολογιστών > Wi-Fi (WLAN)WWW.TECHTEAM.GR/INDEX.PHP?
6. www.in.gr/tech /ims-ericsson .jpg
7. Ασύρματα δίκτυα Επικοινωνιών ,του ΔΡ. ΔΗΜΟΣΘΕΝΗΣ ΒΟΥΓΙΟΥΚΑΣ http://www.icsd.aegean.gr/lecturers/arouskas/courses/material/mps_wireless/3_1_boygioukas_wireless_transmission.pd
8. ΕΙΣΑΓΩΓΙΚΟ ΚΕΦΑΛΑΙΟ, ΓΕΝΙΚΗ ΠΟΙΟΤΙΚΗ ΠΑΡΟΥΣΙΑΣΗ, ΓΙΑ ΤΗΝ **ΡΑΔΙΟΚΥΜΑΤΙΚΗ ΤΗΛΕΠΙΣΚΟΠΗΣΗ,**Απόστολος Κουϊρουκίδης
9. Radio Jamming Attacks Two Poular Mobile Networks ,Mika Stahlberg,Helsinki University of Technology
10. http://www.defencenet.gr/defence/index.php?option=com_content&task=view&id=277&Itemid=4
11. http://courses.ece.uiuc.edu/ece445/projects/fall2005/project4_proposal.doc
12. http://www.neo.gr/website/ergasiamathiti/80.ht
13. htpp://sfr.ee.teiath.gr/historia/historia/selida620.h
14. http://info.awmn.net/users//index.php?option=com_simplefaq&task=display&Itemid=51&catid=13&PHPSESSID=6c6b84cb51255fed4b25c9051b05eacb
15. //Kermit.sda.t-online.de/3sat/hitec/microwellenkanone.rm
16. ΠΡΑΚΤΙΚΑ ΗΜΕΡΙΔΑΣ : **ΕΠΙΔΡΑΣΕΙΣ ΤΗΣ ΗΛΕΚΤΡΟΜΑΓΝΗΤΙΚΗΣ ΑΚΤΙΝΟΒΟΛΙΑΣ ΣΤΗΝ ΥΓΕΙΑ :**

(ΜΥΘΟΙ ΚΑΙ ΠΡΑΓΜΑΤΙΚΟΤΗΤΑ,Τετάρτη 1 η Ιουνίου , 2005,Αμφιθέατρο Εθνικού Ιδρύματος Ερευνών , **Βασικές αρχές λειτουργίας των δικτύων κινητών, επικοινωνιών (GSM/GPRS - UMTS), των κινητών τηλεφώνων και άλλων ασυρμάτων διατάξεων μικρής εμβέλειας,(Bluetooth, WLAN),Δρ . Κωνσταντίνος Ν . Χαλκιώτης,**Επιστημονικός Συνεργάτης Εργαστηρίου Ιατρικής Φυσικής ,Ιατρική Σχολή Πανεπιστημίου Αθηνών

17. **ΦΑΚΕΛΟΣ: ΗΛΕΚΤΡΟΝΙΚΟ ΠΕΔΙΟ ΜΑΧΗΣ ΠΑΡΕΜΒΟΛΕΣ του ΝΑΡΛΗ ΑΙΘΩΝΑ**
18. http://upload.wikimedia.org/de/46/GSM.netzwerk.org
19. http://www.gnosinet.gr/ez/ShowCategory.asp?Skip=120&CatID=28
20. http://sfr.ee.teiath.gr/historia/historia/selida607.htm#1
21. www.techline.gr/contents.html
22. http://de.wikipedia.org/wiki/Global_System_for_Mobile_Communications"

23. ΠΡΑΚΤΙΚΑ ΣΥΝΕΔΡΙΟΥ ΤΟΜΟΣ Α (7 Πανελλήνιο Συνέδριο Φυσικής & 6 Κοινό Συνέδριο Ένωσης Ελλήνων και Ένωσης Κυπρίων Φυσικών)
24. http://xanthippi.ceid.upatras.gr/courses/mobile/Presentations/Lecture4.ppt
25. ΝΤΑΣΗΣ ΕΥΘΥΜΙΟΣ ,ΣΧΕΔΙΑΣΜΟΣ RSA-Blowfish για κρυπτογράφηση δεδομένων & χρήση ηλεκτρονικής υπογραφής (maglarisrypt[1]και κρυπτογραφία
26. http://www.teiser.gr/icd/ptixiakes_parousiaseis/zampiti_andreadi.ppt
27. ΑΝΑΛΥΣΗ ΣΥΓΧΡΟΝΩΝ ΣΥΣΤΗΜΑΤΩΝ ΤΩΝ ΡΑΝΤΑΡ ΜΕ ΤΗΝ ΒΟΗΘΕΙΑ ΤΟΥ ΛΟΓΙΣΜΙΚΟΥ MRSA (του ΑΝΔΡΕΑΔΗ ΓΕΩΡΓΙΟ , ΖΑΜΠΙΤΗ ΠΕΤΡΟ) ΣΕΡΡΕΣ 2005
28. www.rtr.at/web.nsf/deutsch/telekommunikation.frequenzvergabe-specktrum-GSM.Spektrum?open. Document
29. www.salonicawirelless.network
30. **ΕΝΟΠΟΙΗΣΗ ΑΜΥΝΤΙΚΟΥ ΧΩΡΟΥ / ΝΕΕΣ ΤΕΧΝΟΛΟΓΙΕΣ του** Αίθωνα Ναρλή,Δρ. Ηλεκτρονικού Μηχανικού
31. library.techlink.gr/ptisi/article-main. asp?mag=2&issue=160&article=4076 - 104k –
32. WWW. http://library.techlink.gr/ptisi/article-main.asp?mag=2&issue=257&article=6382(ASPIS ΓΙΑ ΤΑ F-16C/D ΤΗΣ ΠΟΛΕΜΙΚΗΣ ΑΕΡΟΠΟΡΙΑΣ, Πάνου Ευαγγέλου)
33. Ασφάλεια σε Ασύρματα Τοπικά Δίκτυα IEEE 802.11, IEEE 802.11 WLAN Security",Μεταπτυχιακή Εργασία,Μαλατράς Απόστολος
36. {(εργασία **ΦΑΚΕΛΟΣ: ΗΛΕΚΤΡΟΝΙΚΟ ΠΕΔΙΟ ΜΑΧΗΣ) ΠΑΡΕΜΒΟΛΕΣ } του** Αίθωνα Ναρλή,Δρ. Ηλεκτρονικού Μηχανικού
37. Αλληλεπίδραση RF ηλεκτρομαγνητικών κυμάτων και βιολογικών ιστών (ΚΩΝ/ΝΑ ΝΙΚΗΤΑ ,Αναπλ.Καθ. Ε.Μ.Π.)
38. http://www.defencenet.gr/defence/index.php?option=com_content&task=view&id=277&Itemid=42
39. ΡΑΝΤΑΡ Α/Ο TPQ-36.
40. ECE 445 Senior Design Lab,Fall 2005,Ben Niemoeller,Larry Dietrick,Albert Rhee
41. htpp://europa.eu.int/comm./internal_market/en
42. http://eclass.di.uoa.gr/F15/document/%D0%E1%F1%EF%F5%F3%E9%DC%F3%E5%E9%F2/Techno-economics%20master.pdf
43. http://eclass.upatras.gr/EE658/document/Mathcad/MoM%20-%20Wire%20Antenna.pdf
44. http://www.uni-kassel.de/fb16/tet/marklein/lecturenotes/nftii/lectures/Lecture4.pdf
45. http://sfr.ee.teiath.gr/historia/historia/selida607.htm#1
46. Δρ.ΕΜΜΑΝΟΥΗΛ ΜΑΓΚΟΣ ΣΗΜΕΙΩΣΕΙΣ Γ' ΕΞΑΜΗΝΟΥ , (ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ – ΕΝΟΤΗΤΑ –Ε) (ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ,ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ,ΑΚΑΔ.ΕΤΟΣ 2005/06)
47. ΕΠΙΚΟΙΝΩΝΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΔΙΕΥΡΥΜΕΝΟΥ ΦΑΣΜΑΤΟΣ ΤΗΣ ΞΑΝΘΙΠΠΗΣ
48. ΔΙΚΤΥΑ ΚΑΙ ΚΡΙΣΙΜΕΣ ΥΠΗΡΕΣΙΕΣ ΣΤΟΝ ΠΟΛΙΤΗ του ΓΙΑΝΝΗ ΚΑΛΟΓΗΡΟΥ (ΕΙΔΙΚΟ ΓΡΑΜ. ΚτΠ,ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΟΙΚΟΝΟΜΙΚΩΝ 2003)
49. GSM (Group Special Mobile) – το ΠΑΜΕΥΡΩΠΑΙΚΟ ΣΥΣΤΗΜΑ ΚΙΝΗΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ ,ΨΗΦΙΑΚΟ ΚΥΨΕΛΩΤΟ ΣΥΣΤΗΜΑ $2^{Hς}$ ΓΕΝΙΑΣ (ΣΥΣΤΗΜΑΤΑ ΚΙΝΗΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ του Γ.Ι.ΣΤΕΦΑΝΟΥ)
50. Radio Wave Fundamentals
51. ΕΙΣΑΓΩΓΗ ΣΤΑ ΔΙΚΤΥΑ ΕΠΙΚΟΙΝΩΝΙΑΣ ΥΠΟΛΟΓΙΣΤΩΝ ,στο ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ , ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ & ΤΕΧΝΟΛΟΓΙΑΣ ΥΠΟΛΟΓΙΣΤΩΝ
52. DONALD C. COX (Wireless Personal Communikations , What is it?)
53. ΣΥΣΤΗΜΑΤΑ ΔΙΑΧΥΤΟΥ ΦΑΣΜΑΤΟΣ (Spead Spectrum) του Γ.Ι.ΣΤΕΦΑΝΟΥ(ΙΟΥΝΙΟΥ 2004)
54. www. Dotteam.gr / mobiles.php?(χαοτική κρυπτογραφία)
55. www.kybernografoi .gr/issues/nos/top.htm , (ΚΡΥΠΤΟΓΡΑΦΙΑ ΑΠΟ ΚΩΝ/ΝΟ ΜΠΟΝΙΚΟ)
56. ΣΧΕΔΙΑΣΗ ΕΠΙΓΕΙΟΥ ΔΟΡΥΦΟΡΙΚΟΥ ΣΤΑΘΜΟΥ ΤΩΝ 120 Mbps του ΔΗΜΗΤΡΗ ΨΥΧΟΥΔΑΚΗ (ΜΕΤΑΠΤΥΧΙΑΚΟ ΤΜΗΜΑ ΡΑΔΙΟΗΛΕΚΤΡΟΛΟΓΙΑΣ ΜΕ ΚΑΤΕΥΘΥΝΣΗ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ του ΑΡΙΣΤΟΤΕΛΕΙΟΥ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΘΕΣ/ΝΙΚΗΣ)
57. ΣΥΜΠΕΡΑΣΜΑΤΑ ΤΟΥ ΣΥΝΕΔΡΙΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ 2005 (MD5)
58. www.at-mix.de/
59. Η ΣΗΜΑΣΙΑ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ ΚΡΙΣΙΜΟΥ ΕΞΟΠΛΙΣΜΟΥ ΑΠΟ ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΑΡΕΜΒΟΛΕΣ του Δρ .ΚΩΣΤΑ ΣΑΜΑΡΑ ,(Raycap Α.Ε) (ΑΠΟ ΤΟ $1^{Ο}$ ΠΑΝΕΛΛΗΝΙΟ ΣΥΝΕΔΡΙΟ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΚΡΙΣΙΜΗΣ ΥΠΟΔΟΜΗΣ ΤΗΣ ΧΩΡΑΣ ,13-14 ΜΑΙΟΥ 2003, ΔΗΜΟΚΡΙΤΟΣ , Η ΕΞΑΡΤΗΣΗ ΑΠΟ ΤΑ ΥΠΟΛΟΓΙΣΤΙΚΑ & ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΑ ΔΙΚΤΥΑ
60. www. Islab.demokritos .gr
61. Code Division Multiple Access του Ashutosh Deepak Gore (EESA Lecture Series,2005,Wirelless Tecnologies Workshop)
62. ΣΥΣΤΗΜΑΤΑ ΚΙΝΗΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ ΤΟΥ Γ.Ι.ΣΤΕΦΑΝΟΥ , ΜΑΙΟΥ 2004
63. ΡΑΝΤΑΡ ΚΑΙ ΔΟΡΥΦΟΡΟΙ ΣΤΗΝ ΥΠΗΡΕΣΙΑ ΤΗΣ ΜΕΤΕΩΡΟΛΟΓΙΑΣ (National Observatory of Athens ,Institute for environmental Research)
64. Του ΓΙΩΡΓΟΥ ΚΩΝΣΤΑΝΤΟΠΟΥΛΟ (Πρόεδρο Ελλ. Φορέα Πρόληψης Τηλεπικοινωνιακής απάτης ,Διευθυντή ασφάλειας & πρόληψης Τηλεπικοινωνιακής απάτης, ΑΠΟ ΤΟ $1^{Ο}$

ΠΑΝΕΛΛΗΝΙΟ ΣΥΝΕΔΡΙΟ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΚΡΙΣΙΜΗΣ ΥΠΟΔΟΜΗΣ ΤΗΣ ΧΩΡΑΣ ,13-14 ΜΑΙΟΥ 2003)

65. www.di.uoa.gr)ΗΝ ΠΟΛΕΜΟΣ του Ν. ΝΙΚΗΤΑΚΟΣ (Αναπλ.Καθηγητής) ΠΛΟΙΑΡΧΟΣ Π.Ν εα
66. Η ΠΑΡΟΥΣΑ ΚΑΤΑΣΤΑΣΗ ΣΕ ΘΕΜΑΤΑ ΚΡΥΠΤΟΓΡΑΦΙΑΣ (ΚΩΝ/ΝΟΣ ΧΑΛΑΤΣΗΣ ,Τμ. Π& Τα, ΕΚΠΑ)
67. Htpp//axion.physiss.ubc.ca./crypt.html
68. Του Δρ. ΙΩΑΝΝΗ Α. ΠΑΠΑΖΟΓΛΟΥ ,ΑΣΦΑΛΕΙΑ ΥΠΟΔΟΜΩΝ & ΔΙΑΧΕΙΡΙΣΗΣ ΚΙΝΔΥΝΟΥ (ΕΡΓΑΣΤΗΡΙΟ ΑΞΙΟΠΙΣΤΙΑΣ ΣΥΣΤΗΜΑΤΩΝ ΒΙΟΜΗΧΑΝΙΚΗΣ ΑΣΦΑΛΕΙΑΣ) παρουσιάστηκε στο 1^{Ο} ΠΑΝΕΛΛΗΝΙΟ ΣΥΝΕΔΡΙΟ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΚΡΙΣΙΜΗΣ ΥΠΟΔΟΜΗΣ ΤΗΣ ΧΩΡΑΣ ,13-14 ΜΑΙΟΥ 2003)
69. 1 Kinita.pdf (ΔΙΑΦΟΡΕΣ ΥΠΗΡΕΣΙΕΣ) ΤΟΥ Γ.Ι.ΣΤΕΦΑΝΟΥ (ΜΑΙΟΣ 2005)
70. ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΚΡΥΠΤΟΓΡΑΦΙΑ (ΓΕΝΙΚΗ ΕΠΙΣΚΟΠΗΣΗ) lecture 1-Introduction (General _ Overview) [1]
71. A Methodology for Network – Centric Electronic Attack Evaluation του Paul Wang, Myron Green bam Mitchell Sparrow ,(ITT INDUSTRIES , AVIONICS DIVISION KEN Mckenzie ,Ami Patel (Modern Technology Solutions, (NDIA T& E SUMMIT) 2003 , CANADA
72. RAND , Project air Force
73. ΨΗΦΙΑΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ (ΔΙΑΜΟΡΦΩΣΗ)
74. ΚΕΦΑΛΑΙΟ 6 , ΜΙΚΤΕΣ
75. Μεταπτυχιακή εργασία της ΘΡΗΣΚΟΥ ΧΡΥΣΑΝΘΗΣ & ΜΗΛΙΟΥ ΑΙΚΑΤΕΡΙΝΗ (2002) , με τίτλο ΑΣΦΑΛΕΙΑ ΣΤΟ Η/Ε
76. Mitigation Paths for Free-Space GPS Jamming του Matt Boggs,Kenea C. Maraffio , GPS/INS System Section ,Naval Air Warfare Center Weapons Division (NAWWCWPNS) /China Lake
77. ΠΠΣ στην ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΤΙΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ , ΕΠΙΚΟΙΝΩΝΙΕΣ ΚΙΝΗΤΩΝ ΣΥΣΤΗΜΑΤΩΝ , Γ.Ι. ΣΤΕΦΑΝΟΥ (ΜΑΡΤΙΟΣ 2004)
78. ΧΩΡΗΤΙΚΟΤΗΤΑ ΚΥΨΕΛΗΣ του Γ.Ι.ΣΤΕΦΑΝΟΥ (ΑΠΡΙΛΙΟ 2004)
79. ΔΙΑΣΤΑΣΙΟΛΟΓΗΣΗ ΔΙΚΤΥΩΝ , του Γ.Ι.ΣΤΕΦΑΝΟΥ , (ΑΠΡΙΛΙΟ 2005)
80. http://www.google.gr/search?q=%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CE%B7+%CE%B5%CF%80%CE%B9%CE%B8%CE%B5%CF%83%CE%B7&hl=el&lr=&start=20&sa=N(ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ)
81. ***Εμπιστοσύνη και Ασφάλεια σε ένα κινητό και γρήγορο δικτυακό περιβάλλον», Ομάδα Εργασίας 'Στ-3', Δρ. Νινέτα Πολέμη(Πανεπιστήμιο Πειραιώς), Δρ.Δημήτρης Πεππές,(VODAFONE), Παναγιώτης Ηλιόπουλος (INTRACOM), Μιλτιάδης Λεωνίδου(Atos Arigin Hellas), Δρ. Αθηνά Μπούρκα(Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα), Πέγκη Μπούτση(EXPERTNET SA),[ebusinessforum)***
82. ***http://www.fas.org/man/dod-101/sys/ac/equip/an-alq-99.htm***
83. http://www.nokia.com.gr/nokia/0,,65909,00.html(5 Ιανουαρίου 2005 , ΑΣΦΑΛΕΙΑ ΣΤΑ BLUETOOTH , ΑΠΟ ΕΤΑΙΡΕΙΑ ΝΟΚΙΑ)
84. http://egnatia.ee.auth.gr/~aalexioy/bloutoot.htm(**ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ)**
85. http://ngia.rootforge.org/content/Tutorials/PlugMeIn/Channels.htm
86. http://egnatia.ee.auth.gr/~abaziako/kefalaio15.html
87. http://www.hitec.gr/lex/default.aspx
88. http://www.iit.demokritos.gr/cip-conf/presentations/2.4-Lekatis.pdf
89. http://egnatia.ee.auth.gr/~abaziako/atm.html
90. http://www.hcaa-eleng.gr/gr/systems/astre2000_gr.html, **1997-2005 Ένωση Ηλεκτρονικών Μηχανικών Ασφαλείας Εναερίου Κυκλοφορίας Υπηρεσίας Πολιτικής Αεροπορίας,**
91. http://66.102.9.104/PAGE/952/EL/1
92. www.izor.com/Page/1033/EL/1/+DOS+&hl=el&gl=gr&ct=clnk&cd=3&lr=lang_el
93. //gebiti.com
94. http://www.geocities.com/grphysics/news/scnews313.html
95. www.ece.rutgers.edu
96. http://vino.physics.uoc.gr/~gts/classes/reports05/xirou.doc
97. http://el.wikipedia.org/wiki/%CE%A1%CE%B1%CE%BD%CF%84%CE%AC%CF%81
98. Μιχάλης Σαμιωτάκης, σύμβουλος Ασφαλείας Πληροφοριακών και Τηλεπικοινωνιακών Συστημάτων της εταιρείας MD5 Α.Ε.,*Συνέντευξη στο Pathfinder και στη Ζέττα Καρφίδου* ,PATHFINDER
99. Ηλεκτρονικό Έγκλημα 2004: Δικτυοπειρατεία & Τηλεπικοινωνιακή Απάτη http://www.microsoft.com/hellas/press/2004b/md5.mspx
100. http://www.microsoft.com/hellas
101. http://www.hcaa-eleng.gr/gr/systems/astre2000_gr.html
102. http://sfr.ee.teiath.gr/historia/historia/graphics/instr/radar2.htm
103. http://www.go-online.gr/ebusiness/specials/article.html?article_id=368
104. Internet www.mmfai.org,July 2004, Diamant Building, ΦΟΡΟΥΜ ΚΑΤΑΣΚΕΥΑΣΤΩΝ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ
105. SyNET, **Systems & Networks, Experts in Technology,** –http://www.cisco.com/go/safe
106. europa.eu.int/information_society/programmes/eten/index_en.htm
107. http://www.eett.gr
108. http://www.ote.gr/efta
109. **http://www.fas.org/man/dod-101/sys/ac/equip/an-alq-99.htm**