



**ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ
ΜΕΣΟΛΟΓΓΙΟΥ**

Τμήμα Τηλεπικοινωνιακών Συστημάτων & Δικτύων

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Μελέτη Της Κωδικοποίησης Φωνητικής Πληροφορίας Στο Δίκτυο GSM

ΜΠΟΥΡΟΥ ΔΗΜΟΚΛΕΙΑ 0384

ΧΡΙΣΤΟΠΟΥΛΟΥ ΧΡΙΣΤΙΝΑ 0361

Επιβλέπων: Λούβρος Σπυρίδων

Ναύπακτος Νοέμβριος 2010

ΠΕΡΙΕΧΟΜΕΝΑ

1.ΕΙΣΑΓΩΓΗ.....	6
1.1 Τρόποι χρήσης και παροχής δικτύων κινητής τηλεφωνίας.....	6
1.2 Διάκριση γενιών κινητής τηλεφωνίας.....	7
2.ΤΟ ΠΑΓΚΟΣΜΙΟ ΔΙΚΤΥΟ GSM.....	9
2.1 Έννοια δικτύου GSM.....	9
2.2 Ζώνες συχνοτήτων.....	11
2.2.1 GSM 900MHz.....	11
2.2.2 GSM 1800MHz.....	11
2.2.3 GSM 1900MHz.....	12
2.2.4 E-GSM.....	12
2.3 Αρχιτεκτονική δικτύου GSM.....	13
3.ΔΙΑΧΩΡΙΣΜΟΣ GSM.....	15
3.1 Δημόσια GSM και Ιδιωτικά GSM	15
3.2. Δομή της ραδιοζεύξης.....	16
3.2.1. Περιγραφή των GSM GATEWAYS.....	18
3.2.2. Μειονεκτήματα τουGSM.....	20
4.ΚΩΔΙΚΟΠΟΙΗΣΗ ΦΩΝΗΣ.....	21
4.1 Η φωνή ως σήμα και το υπόβαθρο της.....	22
4.2 Κωδικοποίηση και αποκωδικοποίηση.....	23
4.2.1 Κωδικοποίηση στο δίκτυο GSM.....	23
4.2.2 Το σχήμα κωδικοποίησης.....	24
4.2.3 Κωδικοποίηση και διαμόρφωση καναλιών.....	25
5.ΤΕΧΝΙΚΕΣ ΚΩΔΙΚΟΠΟΙΗΣΗΣ.....	26

5.1 Waveform coding τεχνικές.....	27
5.1.1 Model based τεχνικές (vocoders).....	27
5.1.2 Το μοντέλο linear predictive coding	28
5.1.3 Αλγόριθμος LPC για αναγνώριση φωνής.....	29
6.VOICE OVER IP (IP ΤΗΛΕΦΩΝΙΑ).....	31
6.1 Πρωταρχικές λειτουργίες.....	33
6.2 Μέσα ασυρμάτου μετάδοσης	35
6.2.1 Τοπολογίες ασύρματης μετάδοσης.....	36
7.BLOCK INTERLEAVER.....	38
7.1 Block Κώδικες.....	41
7.1.1 Block Κώδικες και Πιθανότητες Σφαλμάτων.....	47.
7.1.2 Block Codes σε αντιστοιχία με απόσταση Hamming.....	50
7.2 Κωδικοποίηση πηγής και καναλιού.....	52
7.2.1 Κωδικοποίηση τμήματος (block coding).....	53
7.2.2 Γραμμικοί Μπλοκ Κώδικες.....	54
7.2.3 Κυκλικό Κώδικες.....	56
7.2.4. Παράδειγμα CRC κώδικα.....	59
7.2.5 Διαπλοκή block.....	60
8.ΚΩΔΙΚΕΣ BLOCK ΚΑΙ CONVOLUTIONAL.....	61
8.1 Χαρακτηριστικά συνελεκτικών κώδικων.....	62
8.1.1 Διαδικασία κωδικοποίησης δεδομένων(convolution).....	63
8.1.2 Αναπαράσταση με διανύσματα συνδέσεων.....	67
8.1.3. Παράδειγμα Convolution κώδικα.....	69
8.1.3 Διαφορές συνελεκτικών κώδικων και block.....	71
9.ΒΙΒΛΙΟΓΡΑΦΙΑ.....	72

ΕΥΡΕΤΗΡΙΟ ΣΧΗΜΑΤΩΝ

Σχήμα 1: GSM δίκτυο	13
Σχήμα 2: Δομή ραδιοζεύξης	17
Σχήμα 3: Διάγραμμα HAMMING	31
Σχήμα 4: Τοπολογία ασύρματων δικτύων	37
Σχήμα 5: Δεύτερο είδος τοπολογίας ασύρματων δικτύων	38
Σχήμα 6: Block διάγραμμα ενός στοιχειώδους συστήματος επικοινωνίας	40
Σχήμα 7: Πίνακας αποκωδικοποίησης για έναν δυαδικό κώδικα	42
Σχήμα 8: Το δυαδικό συμμετρικό κανάλι (BSC)	44
Σχήμα 9: Το δυαδικό erasure κανάλι	45
Σχήμα 10: Πίνακας πολυωνύμων	58
Σχήμα 11: Πίνακας αληθείας	64
Σχήμα 12: Convolutional κωδικοποιητής	65
Σχήμα 13: Χρονοδιάγραμμα	66
Σχήμα 14: Διαδικασία συνελκτικής κωδικοποίησης ακολουθίας πληροφορίας	68

1.ΕΙΣΑΓΩΓΗ

Τα κινητά τηλέφωνα αποτελούν αναπόσπαστο τμήμα της καθημερινής ζωής στον σύγχρονο κόσμο. Η κινητή τηλεφωνία άλλαξε ριζικά τη ζωή καθώς και τον τρόπο επικοινωνίας των ανθρώπων, με αποτέλεσμα ένα αίσθημα ασφάλειας και βεβαιότητας, που όμοιό του δεν είχε καταγραφεί μέχρι σήμερα στην ανθρώπινη ιστορία. Προοδευτικά η μετάβαση από την αναλογική στην ψηφιακή τεχνολογία ήταν αναπόφευκτη από τη στιγμή που τα ψηφιακά δίκτυα κινητής τηλεφωνίας φάνηκαν να ξεπερνούν τους σοβαρούς περιορισμούς χωρητικότητας των αντίστοιχων αναλογικών, ενώ εμφάνιζαν μεγαλύτερη πιστότητα ήχου, λόγω της αποτελεσματικότερης χρήσης των ραδιοσυχνοτήτων, υποστήριζαν επιπλέον λειτουργίες και παρείχαν τα εχέγγυα για μεγαλύτερη ασφάλεια στη μετάδοση των πληροφοριών. Τα νέα δίκτυα κινητής τηλεφωνίας παρέχουν εξάλλου τη δυνατότητα μόνιμης σύνδεσης, υψηλών ταχυτήτων (≥ 2 Mbps) και αύξησης των συσκευών που μπορούν να συνδεθούν ταυτόχρονα με χρήση ενός και μόνο κινητού τερματικού.

1.1. Τρόποι χρήσης και παροχής δικτύων κινητής τηλεφωνίας

Για να έχουμε την δυνατότητα χρήσης του κινητού τηλεφώνου είναι απαραίτητη η ύπαρξη ενός τουλάχιστον ασύρματου δικτύου κινητής τηλεφωνίας. Τα δίκτυα αυτά χρησιμοποιούν σταθμούς βάσης για να καλύψουν με ηλεκτρομαγνητικό σήμα τους χώρους που βρισκόμαστε. Όταν χρησιμοποιούμε το κινητό μας τηλέφωνο για να επικοινωνήσουμε, τότε αυτό στέλνει και λαμβάνει ηλεκτρομαγνητικά σήματα προς και από έναν σταθμό βάσης, ο οποίος στη συνέχεια επικοινωνεί ενσύρματα ή ασύρματα με κάποια κέντρα αναδιανεμόντας την πληροφορία, ώστε να μπορούμε να επικοινωνούμε με αυτούς που θέλουμε.

1.2. Διάκριση γενιών κινητής τηλεφωνίας

Μέσω των δικτύων κινητής τηλεφωνίας μπορούν να αποκτήσουν πρόσβαση στο Internet κινητά τηλέφωνα (smartphones), φορητοί υπολογιστές και υπολογιστές παλάμης. Ωστόσο, ο τρόπος πρόσβασης, όπως επίσης και η ποιότητά της, εξαρτώνται από το είδος κινητής τηλεφωνίας ή ακριβέστερα, από τη "γενιά" της. Ως γνωστόν, η κινητή τηλεφωνία διακρίνεται σε γενιές. Πρόκειται για διαφορετικές τεχνολογικές πλατφόρμες, που απεικονίζουν την εξέλιξη στην κινητή τηλεφωνία. Μολονότι συνήθως γίνεται λόγος για 3 γενιές, την πρώτη, τη δεύτερη και την τρίτη, τις οποίες για συντομία ονομάζουμε 1G, 2G και 3G στην πραγματικότητα και οι γενιές και οι τεχνολογικές υποδομές μέσω των οποίων εκφράζονται είναι περισσότερες των τριών. Είναι χαρακτηριστικό ότι μεταξύ δεύτερης και τρίτης γενιάς παρεμβάλλεται η γενιά 2.5 (2.5G), ενώ περισσότερες της μιας τεχνολογικές υποδομές στεγάζονται κάτω από την "ομπρέλα" μιας γενιάς, όπως θα δούμε και παρακάτω, ενώ κάλλιστα κάθε διαφορετική υποδομή θα μπορούσε να ταυτίζεται και με διαφορετική γενιά.

Η αρχή έγινε με την **1G**, που έκανε την εμφάνισή της πριν από το 1990 σε ορισμένες χώρες της Ευρώπης και στην Αμερική. Στην Ελλάδα δεν έφθασε ποτέ. Ογκώδεις συσκευές, χαμηλότερες ταχύτητες, χαμηλή ποιότητα και μετάδοση φωνής με αναλογικό τρόπο, αλλά και πολλά προβλήματα σύνδεσης ήταν τα χαρακτηριστικά της 1G.

Η δεύτερη γενιά κινητής τηλεφωνίας εισήχθη στο παγκόσμιο στερέωμα στις αρχές της δεκαετίας του '90, κυρίως μέσω των τεχνολογικών υποδομών **GSM** (Global System for Mobile Communications) με χρήση σε Ευρώπη, Αφρική, Ασία, **TDMA** (Time Division Multiple Access) με χρήση στις ΗΠΑ, **CDMA** (Code Division Multiple Access) σε ΗΠΑ και Ασία και **PDC** (Personal Digital Cellular) στην Ιαπωνία. Όλες οι παραπάνω τεχνολογικές πλατφόρμες εντάσσονται στη **2G**. Στην Ελλάδα, το πρότυπο 2G που χρησιμοποιείται είναι το GSM. Κύρια χαρακτηριστικά του είναι η ψηφιακή μετάδοση φωνής με καλή πιστότητα και η ψηφιακή μετάδοση

δεδομένων με χαμηλή ταχύτητα, μόλις 9,6 Kbps. Η πρώτη προσπάθεια σύνδεσης στο Internet μέσω των δικτύων της 2G έγινε πριν από μερικά χρόνια με την εμφάνιση του **WAP** (Wireless Applications Protocol). Οι χαμηλές όμως ταχύτητες μετάδοσης δεδομένων και η ανυπαρξία συσκευών που να υποστηρίζουν ικανοποιητική απεικόνιση των ιστοσελίδων οδήγησε το WAP σε αποτυχία.

Στη συνέχεια μία άλλη τεχνολογία, η **HSCSD** (High Speed Circuit Switched Data), ανέλαβε να υποστηρίξει τη γρήγορη μετάδοση δεδομένων μέσω του δικτύου GSM και πέτυχε να διπλασιάσει (και να τριπλασιάσει, ενίοτε) την ταχύτητα διαμεταγωγής δεδομένων, έναντι της ταχύτητας του GSM. Κάπου εδώ ολοκληρώνεται η πρώτη περίοδος των κινητών τεχνολογιών σύνδεσης με το Internet, που δεν στέφθηκε με επιτυχία, με εξαίρεση ορισμένες μόνο χώρες, στις οποίες δεν συγκαταλέγεται η Ελλάδα. Από εκείνο το σημείο και εφεξής τα δίκτυα κινητής τηλεφωνίας αρχίζουν να γίνονται πιο ελκυστικά για τους χρήστες που επιθυμούν να έχουν πρόσβαση στο Διαδίκτυο μέσω του κινητού τους ή άλλης φορητής συσκευής. Αυτό οφείλεται στο ότι οι γενιές που ακολούθησαν ήταν (και είναι) ασύγκριτα πιο γρήγορες, καθώς και στο ότι κυκλοφόρησαν στην αγορά οι "κατάλληλες" συσκευές (μεγάλες έγχρωμες οθόνες, με υποστήριξη πολυμέσων κ.λπ.). Έτσι, την αργή και χαμηλών δυνατοτήτων 2G ακολούθησε η γενιά 2.5. Τα τεχνολογικά πρότυπα της **2.5G** είναι το **GPRS** (General Packet Radio Service) και το **EDGE** (Enhanced Data rates for Global Evolution), με πιο διαδεδομένο το GPRS, το οποίο χρησιμοποιείται και στην Ελλάδα. Η 2.5G, εκτός από άριστη ποιότητα μετάδοσης φωνής, προσφέρει μετάδοση δεδομένων σε πολύ υψηλότερες ταχύτητες έναντι της 2G, και, θεωρητικά, μπορεί να φθάσει και τα 115Kbps για το GPRS και τα 384Kbps για το EDGE.

Η τρίτη γενιά κινητής τηλεφωνίας ενσωματώνει, αρκετά πρότυπα με πιο διαδεδομένα τα πρότυπα **UMTS** (Universal Mobile Telecommunications System) και **WCDMA** (Wideband Code Division Multiple Access). Η 3G είναι διαθέσιμη στην Ελλάδα και προσφέρει πολλές δυνατότητες υπηρεσιών πολυμέσων (λ.χ. παρακολούθηση τηλεοπτικών προγραμμάτων από το κινητό), συνεχή σύνδεση με το Διαδίκτυο και μετάδοση κάθε είδους δεδομένων σε πολύ υψηλές ταχύτητες, από 64Kbps έως 384Kbps σε πρώτο στάδιο, και μέχρι τα 2Mbps αργότερα.

Τέλος, η συνέχεια σε αυτή τη διαδοχή των γενιών θα δοθεί μετά το 2010, με το λανσάρισμα της τέταρτης γενιάς κινητής τηλεφωνίας (4G), που βρίσκεται ήδη σε στάδιο ανάπτυξης και εκτιμάται ότι θα ξεπερνά κατά πολύ όλες τις προηγούμενες.

2. ΤΟ ΠΑΓΚΟΣΜΙΟ ΔΙΚΤΥΟ GSM

2.1 Έννοια δικτύου GSM

(Global System for Mobile Communications: που σημαίνει παγκόσμιο σύστημα κινητών επικοινωνιών αρχικά από την *Groupe Special Mobile* είναι το πιο δημοφιλές πρότυπο για τα κινητά συστήματα τηλεφωνίας στον κόσμο. Η GSM Association οργάνωσε την προώθηση του εμπορίου των κατασκευαστών του κλάδου της κινητής τηλεφωνίας και υπολογίζει ότι το 80% της παγκόσμιας αγοράς κινητών χρησιμοποιεί το πρότυπο GSM. Το χρησιμοποιούν πάνω από 3 δισεκατομμύρια άνθρωποι σε περισσότερες από 212 χώρες και εδάφη. Η παρουσία του επιτρέπει στις διεθνείς συμφωνίες περιαγωγής μεταξύ των φορέων εκμετάλλευσης κινητής τηλεφωνίας να παρέχει στους συνδρομητές τη χρήση των τηλεφώνων τους σε πολλά μέρη του κόσμου. Το GSM τεχνολογιών διαφέρει από τον προκάτοχό του στο ότι και τα δύο κανάλια σηματοδότησης και η ομιλία είναι ψηφιακά και ως εκ τούτου θεωρείται GSM *δεύτερης γενιάς (2G)* συστήματος κινητής τηλεφωνίας. Αυτό διευκολύνει επίσης την ευρεία εφαρμογή και εξάπλωση των εφαρμογών επικοινωνίας δεδομένων στο σύστημα. Η πανταχού παρουσία της εφαρμογής του προτύπου GSM έχει ένα πλεονέκτημα τόσο στους καταναλωτές, οι οποίοι μπορούν να επωφεληθούν, αλλά και για τους φορείς εκμετάλλευσης δικτύων, οι οποίοι μπορούν να επιλέξουν εξοπλισμό από πολλούς προμηθευτές εξοπλισμού GSM. Το GSM επίσης είναι πρωτοπόρος χαμηλού κόστους εφαρμογής της υπηρεσίας σύντομων μηνυμάτων(SMS), που

ονομάζονται επίσης μηνύματα κειμένου. Το GSM χρησιμοποιεί μια ποικιλία κωδικοποιητών φωνής για συμπίεση ήχου 3,1 kHz στα μεταξύ 6,5 και 13 kbit / s. Αρχικά, δύο κωδικοποιητές, χρησιμοποιήθηκαν. Αυτοί χρησιμοποίησαν ένα σύστημα που βασίζεται σε γραμμική προγνωστική κωδικοποίηση (LPC). Εκτός του ότι είναι αποτελεσματικό με bitrates, αυτοί οι κωδικοποιητές κατέστησαν επίσης ευκολότερο τον εντοπισμό ήχου, που επιτρέπει τη διασύνδεση στρώμα αέρα για να δώσουν προτεραιότητα και στην καλύτερη προστασία των τμημάτων αυτών του σήματος. GSM ενισχύθηκε περαιτέρω το 1997 με το Enhanced Full Rate(EFR)codec, ένα 12,2 kbit / s codec που χρησιμοποιεί ένα πλήρες κανάλι. Στο σύστημα GSM η περιοχή συχνοτήτων που έχει εκχωρηθεί για την λειτουργία των δικτύων κινητής τηλεφωνίας υποδιαιρείται σε περισσότερες υποπεριοχές συχνοτήτων– κανάλια επικοινωνίας εύρους 200kHz. Κάθε κανάλι μπορεί να χρησιμοποιείται ταυτόχρονα από οκτώ το πολύ συνδρομητές, οι οποίοι χρησιμοποιούν διαδοχικά το κανάλι για λίγο χρόνο (περίπου 0,577 ms). Κάθε σταθμός βάσης επικοινωνεί με τα κινητά τηλέφωνα που βρίσκονται στη περιοχή, συνήθως με 6 έως 12 κανάλια συχνοτήτων. Τα κανάλια αυτά είναι διαφορετικά μεταξύ γειτονικών κυψελών, ώστε να ξεχωρίζουν μεταξύ τους. Επειδή ο αριθμός των καναλιών είναι περιορισμένος, τα ίδια κανάλια ξαναχρησιμοποιούνται σε διαφορετικές κυψέλες. Η σχεδίαση των δικτύων είναι τέτοια, ώστε οι κυψέλες που χρησιμοποιούν τα ίδια κανάλια να είναι όσο το δυνατόν μακρύτερα μεταξύ τους για την ελαχιστοποίηση των παρεμβολών της μιας στη λειτουργία της άλλης. Τα κινητά τηλέφωνα μετρούν το επίπεδο του σήματος που λαμβάνουν από τους πλησιέστερους σταθμούς βάσης και αν, καθώς μετακινούμαστε, το σήμα από έναν άλλο σταθμό βάσης γίνει καλύτερο από το σήμα του σταθμού που χρησιμοποιούμε, τότε το δίκτυο κινητής τηλεφωνίας μας μεταβιβάζει στην κυψέλη του σταθμού αυτού, χωρίς η μεταβίβαση να γίνεται αισθητή από μας. Το 1989 η ευθύνη του GSM ανατέθηκε στο Ευρωπαϊκό Τηλεπικοινωνιακό Ινστιτούτο Προτύπων (ETSI) και το 1990 ανακοινώθηκαν επίσημα για πρώτη φορά το πρότυπο και τα χαρακτηριστικά του GSM. Το 1991 άρχισε η εμπορική του διάθεση στην Ευρώπη, ενώ στην Ελλάδα το σύστημα χρησιμοποιήθηκε το 1993 από την WIND Hellas. Το πρότυπο GSM δεν είναι μόνο Ευρωπαϊκό πρότυπο, αφού υιοθετήθηκε από πολλές άλλες χώρες των άλλων Ηπείρων, εκμεταλλευόμενο διάφορες ζώνες συχνοτήτων.

2.2 Ζώνες συχνοτήτων

2.2.1. GSM 900MHz

Το 1990 άρχισαν να λειτουργούν τα πρώτα δίκτυα GSM στη ζώνη συχνοτήτων των 900 MHz. Η Διεθνής Ένωση Τηλεπικοινωνιών (ITU) παραχώρησε ένα ζεύγος συχνοτήτων, από τα 890 έως τα 915 MHz και από τα 935 έως τα 960 MHz. Η πρώτη περιοχή χρησιμοποιείται για την επικοινωνία του κινητού με τον σταθμό βάσης (Up link), ενώ η δεύτερη για την επικοινωνία του σταθμού βάσης με το κινητό (down link). Οι περιοχές (ζώνες) των 25MHz υποδιαιρούνται η καθεμία σε 124 + (1 ελεύθερο) κανάλια συχνότητας και κάθε κανάλι έχει εύρος ζώνης 200 KHz. Όλο αυτό το σύστημα ονομάστηκε GSM 900 ή Standard GSM.

2.2.2. GSM 1800MHz

Στη συνέχεια, το 1991, αναπτύχθηκε το σύστημα DCS 1800, στο οποίο διατηρείται η δομή ενός GSM 900 δικτύου αλλά χρησιμοποιούνται διαφορετικά ζεύγη συχνοτήτων, από τα 1710 έως τα 1785 MHz Up link και από τα 1805 έως τα 1880 MHz Down link. Οι περιοχές των 75MHz υποδιαιρούνται η καθεμία σε 374 (+ 1 ελεύθερο) κανάλια και κάθε κανάλι έχει εύρος ζώνης 200 KHz. Αυτή η αλλαγή στην ζώνη συχνοτήτων έγινε διότι οι ζώνες του GSM 900 στην Ευρώπη ήταν πιασμένες από άλλους παροχείς κινητής τηλεφωνίας. Όπως και στην χώρα μας, σήμερα, όλες οι εταιρίες κινητής τηλεφωνίας χρησιμοποιούν και τα δύο συστήματα(GSM 900/GSM 1800) στα δίκτυα τους αυξάνοντας αισθητά τη χωρητικότητά στα δίκτυα τους. Στα τέλη δεκαετίας του 1990 η GSM World Association αποφάσισε να μετονομάσει το DCS 1800 σε GSM 1800 για να φανεί η δυναμικότητα και η παγκοσμιότητα του GSM.

2.2.3. GSM 1900MHz

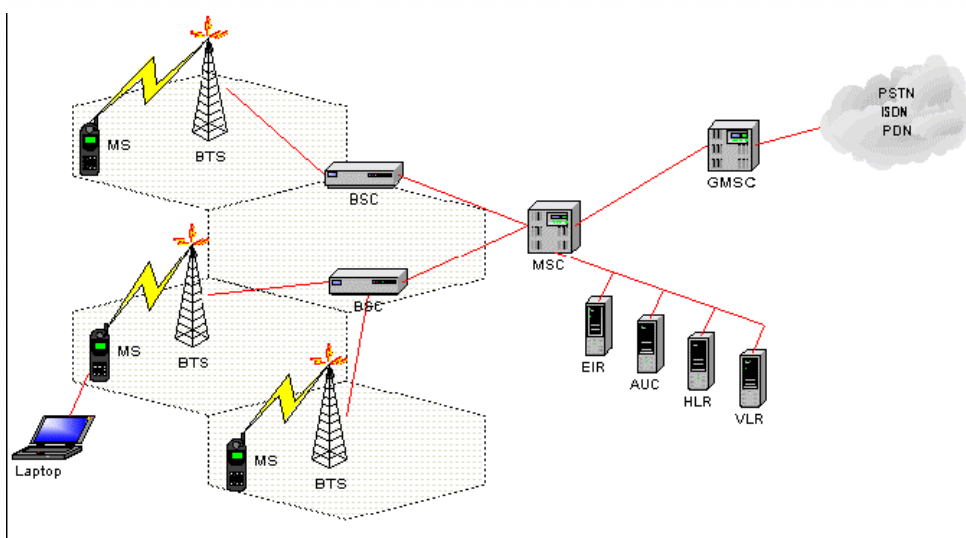
Στο GSM 1900 χρησιμοποιείται σε αρκετές χώρες της Αμερικής, διατηρείται και πάλι η δομή ενός GSM 900 δικτύου, αλλά χρησιμοποιούνται και εδώ διαφορετικά ζεύγη συχνοτήτων: Από τα 1850 έως τα 1910 MHz για Up link και από τα 1930 έως τα 1990 MHz για Down link. Οι περιοχές των 60MHz υποδιαιρούνται η καθεμία σε 299+ (1 ελεύθερο) κανάλια συχνότητας και κάθε κανάλι έχει εύρος ζώνης 200KHz. Στα τέλη δεκαετίας του 1990 η GSM World Association αποφάσισε να μετονομάσει το PCS 1900 που λεγότανε παλιότερα σε GSM 1900 για να φανεί η δυναμικότητα και η παγκοσμιότητα του GSM.

2.2.4. E-GSM / Extended-GSM 900 - Εκτεταμένη ζώνη GSM

Το E-GSM καθορίστηκε από την Ευρωπαϊκή Επιτροπή Ράδιο Επικοινωνιών στα τέλη της δεκαετίας του 1990 για να «αντικαταστήσει» το κλασικό GSM 900 διατηρώντας βέβαια την δομή του αυξάνοντας όμως τις περιοχές συχνοτήτων από 880 έως 915 MHz για Up link και 925 έως 960 MHz Down link. Έτσι επέτρεψε στα δίκτυα κινητής τηλεφωνίας να αυξήσουν τη χωρητικότητά τους και να καλύψουν τις ανάγκες από την αυξημένη κίνηση των πελατών τους.

2.3 Αρχιτεκτονική δικτύου GSM

Ένα δίκτυο GSM απαρτίζεται από αρκετές δικτυακές οντότητες, όπως φαίνεται και στο σχήμα , και χωρίζεται σε τρία μέρη: τον κινητό σταθμό, το υποσύστημα σταθμού βάσης και το υποσύστημα δικτύου.



Σχήμα 1: GSM δίκτυο

Ο Κινητός Σταθμός (Mobile Station – MS) είναι η τερματική συσκευή που έχει μαζί του ο χρήστης της κινητής τηλεφωνίας (κινητό τηλέφωνο, φορητός υπολογιστής συνδεδεμένος με το κινητό τηλέφωνο, κτλ). Το κινητό τηλέφωνο περιέχει μια «έξυπνη» κάρτα, που ονομάζεται SIM (Subscriber Identity Card) και περιέχει πληροφορίες για το συνδρομητή της κινητής τηλεφωνίας. Έτσι, ο χρήστης μπορεί να αλλάξει συσκευή αλλά να εξακολουθεί να χρησιμοποιεί την ίδια SIM κάρτα, διατηρώντας τον ίδιο αριθμό και την ίδια συνδρομή. Η SIM κάρτα περιέχει το Διεθνές Αναγνωριστικό Συνδρομητή Κινητής Τηλεφωνίας (International Mobile Subscriber Identity – IMSI), που είναι μοναδικό για κάθε συνδρομητή και χρησιμοποιείται για να γνωστοποιήσει στο σύστημα την ταυτότητα του χρήστη, καθώς και για διάφορες διαδικασίες αυθεντικοποίησης. Επιπλέον, κάθε τερματική συσκευή αναγνωρίζεται μοναδικά από το Διεθνές Αναγνωριστικό Ασύρματης Συσκευής (International Mobile

Equipment Identity – IMEI). Το Υποσύστημα Σταθμού Βάσης (Base Station Subsystem – BSS) απαρτίζεται από δύο οντότητες: τον Πομποδέκτη του Σταθμού Βάσης (Base Transceiver Station – BTS) και τον Ελεγκτή του Σταθμού Βάσης (Base Station Controller – BSC). Η λειτουργία του BTS είναι να λαμβάνει και να εκπέμπει ραδιοσήματα από και προς τους κινητούς σταθμούς, να επεξεργάζεται τα σήματα, να (απο)κωδικοποιεί τη φωνή και να προσαρμόζει τον ρυθμό μετάδοσης. Ένας BTS υλοποιεί μία κυψέλη του συστήματος GSM. Πολλοί BTSs ελέγχονται από έναν BSC. Ο BSC ευθύνεται για την διαχείριση των ασύρματων πόρων. Δηλαδή ασχολείται με την διανομή των καναλιών στους κινητούς σταθμούς, την άρση της διανομής, την αλλαγή συχνότητας και το χρονοισμό των ραδιοσημάτων. Η κεντρική μονάδα του υποσυστήματος δικτύου (Network Subsystem – NSS) είναι το Κέντρο Μεταγωγής (Mobile Switching Center – MSC). Οι ροές που προέρχονται από τους κινητούς σταθμούς στις αντίστοιχες κυψέλες, δρομολογούνται μέσω του MSC. Ο MSC παρέχει όλη τη λειτουργικότητα που χρειάζεται για την διαχείριση ενός χρήστη κινητής τηλεφωνίας, όπως εγγραφή στην υπηρεσία κινητής τηλεφωνίας, αυθεντικοποίηση, τοπολογική ενημέρωση και δρομολόγηση κλήσης για τους χρήστες που βρίσκονται εκτός αρχικού δικτύου. Οι ροές από και προς ένα σταθερό δίκτυο τηλεφωνίας (π.χ. PSTN, ISDN, PDN) διαχειρίζονται από ένα αφιερωμένο γι' αυτή τη δουλειά Κέντρο Μεταγωγής (Gateway Mobile Switching Center – GMSC). Τα GSM δίκτυα είναι ιεραρχικά δομημένα. Αποτελούνται από τουλάχιστον μία διοικητική περιοχή που ανατίθεται σε έναν MSC. Κάθε διοικητική περιοχή αποτελείται από τουλάχιστον μία τοπολογική περιοχή (Location Area – LA). Η κάθε τοπολογική περιοχή απαρτίζεται από πολλά σύνολα κυψελών. Κάθε σύνολο κυψελών ανατίθεται σε έναν BSC. Ένα σύνολο από βάσεις δεδομένων είναι διαθέσιμες για τον έλεγχο κλήσεων και τη διαχείριση δικτύου: το HLR (Home Location Register), το VLR (Visitor Location Register), το AUC (Authentication Center) και το EIR (Equipment Identity Register). Για όλους τους χρήστες που είναι συνδρομητές σε έναν παροχέα κινητής τηλεφωνίας, τα μόνιμα δεδομένα (όπως το προφίλ του χρήστη) καθώς και κάποια προσωρινά δεδομένα (όπως η τρέχουσα θέση του χρήστη) αποθηκεύονται στο HLR. Στην περίπτωση που υπάρχει κλήση για έναν χρήστη, το HLR είναι πάντα η πρώτη βάση που ρωτάται για την τρέχουσα τοποθεσία του χρήστη. Το VLR είναι υπεύθυνο για ένα

σύνολο τοπολογικών περιοχών και αποθηκεύει δεδομένα για τους χρήστες που είναι την τρέχουσα στιγμή μέσα στην περιοχή της δικαιοδοσίας του. Αυτό σημαίνει ότι και μέρος από τα μόνιμα δεδομένα ενός χρήστη μεταφέρονται από το HLR στο υπεύθυνο VLR για γρηγορότερη προσπέλαση. Παρόλα αυτά, και το VLR μπορεί να αποθηκεύσει προσωρινά δεδομένα για δική του χρήση. Τα άλλα δύο μητρώα, το AUC και το EIR χρησιμοποιούνται για θέματα ασφάλειας και αυθεντικοποίησης. Το AUC είναι μια προστατευμένη βάση δεδομένων που αποθηκεύει ένα αντίγραφο του μυστικού κλειδιού της SIM κάρτας κάθε συνδρομητή, το οποίο χρησιμοποιείται για αυθεντικοποίηση και κρυπτογράφηση πάνω από το ασύρματο κανάλι. Το EIR είναι μια βάση που περιέχει μια λίστα με όλα τις έγκυρες συσκευές κινητής τηλεφωνίας του δικτύου. Κάθε κινητός σταθμός αποθηκεύεται στη βάση με το αντίστοιχο αναγνωριστικό του (IMEI). Ένας κινητός σταθμός μπορεί να θεωρηθεί άκυρος αν το κινητό έχει δηλωθεί ως κλεμμένο ή αν δεν είναι συμβατού τύπου.

3. Διαχωρισμός GSM

Στο σημείο αυτό κρίνεται αναγκαίος ο διαχωρισμός των GSM σε Δημόσια και Ιδιωτικά:

3.1 Δημόσια GSM και Ιδιωτικά

Ως Δημόσια χαρακτηρίζονται τα GSM που χρησιμοποιούνται προκειμένου να δρομολογήσουν τις κλήσεις των συνδρομητών στο δίκτυο των παροχών κινητής τηλεφωνίας. Οι κάρτες SIM τοποθετούνται σε ειδικές τερματικές διατάξεις (Fixed Cellular Terminals). Η χρήση δημόσιων GSM συνιστά εμπορική εκμετάλλευση των κατ'αποκλειστικότητα συχνοτήτων στους παρόχους κινητής τηλεφωνίας. Σημειώνεται πως η εμπορική εκμετάλλευση του φάσματος επιτρέπεται στις εταιρίες που δρομολογούν κλήσεις στα δίκτυα κινητής τηλεφωνίας.

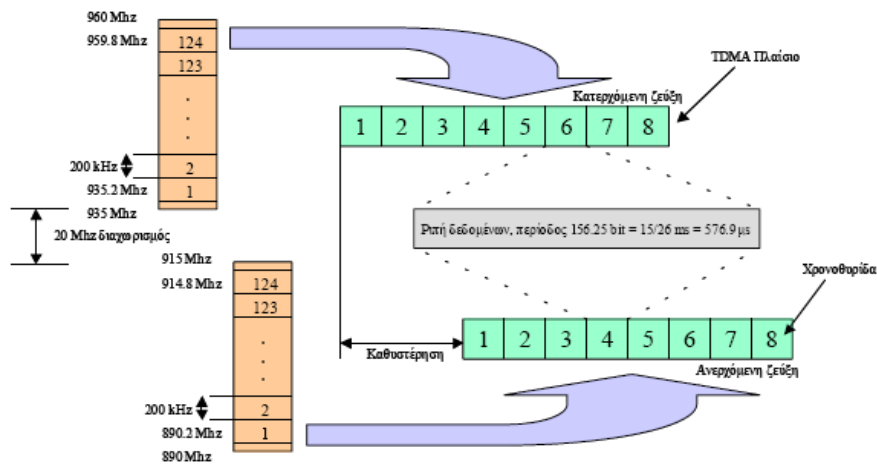
Ιδιωτικά GSM

Ως Ιδιωτικά χαρακτηρίζονται τα GSM που χρησιμοποιούνται από φυσικά ή νομικά πρόσωπα προκειμένου να επιτύχουν διασύνδεση με το δίκτυο και να δρομολογήσουν αποκλειστικά τις κλήσεις τους από σταθερό προς κινητό. Στην περίπτωση αυτή το GSM εγκαθίσταται στο PABX (Private Automatic Branch Exchange) του συνδρομητή. Η χρήση ιδιωτικών GSM, σε αντίθεση με τη χρήση των Δημοσίων, δεν αποτελεί εμπορική εκμετάλλευση απονεμηθείσας συχνότητας αλλά μεταπώληση αερόχρονου, εφόσον εξυπηρετεί αποκλειστικά τις ίδιες ανάγκες φυσικών ή νομικών προσώπων.

3.2. Δομή της ραδιοζεύξης

Η διεπαφή της ραδιοζεύξης χωρίζεται σε ένα πλήθος από κανάλια: κανάλια από τα οποία περνάει η φωνή και τα προς μετάδοση δεδομένα, καθώς και κανάλια που χρησιμοποιούνται για μηνύματα διαχείρισης και για διεργασίες διαχείρισης του φόρτου των καναλιών. Δύο μπάντες συχνοτήτων των 25 Mhz διατέθηκαν από τον διεθνή οργανισμό ITU για το GSM σύστημα. Έτσι, η μπάντα 890-915 Mhz δόθηκε στην ανερχόμενη ζεύξη (από τον κινητό σταθμό προς το BSS), ενώ η μπάντα 935-960 Mhz δόθηκε στην κατερχόμενη ζεύξη (από το BSS προς τον κινητό σταθμό). Για να γίνει δυνατή η ταυτόχρονη μετάδοση από κινητούς σταθμούς σε διαφορετικές, πιθανόν, κυμέλες χρησιμοποιήθηκε συνδυασμός των τεχνικών πολύπλεξης σε επίπεδο συχνότητας (FDMA) και σε επίπεδο χρόνου (TDMA). Έτσι κάθε μπάντα των 25 Mhz χωρίστηκε σε 124 φέρουσες συχνότητες των 200 kHz η καθεμία. Ένα πλήθος τέτοιων συχνοτήτων ανατίθεται σε ένα BTS, ορίζοντας με αυτό τον τρόπο ποιες συχνότητες

εξυπηρετούνται από μία κυψέλη. Επιπλέον, κάθε φέρουσα συχνότητα περιέχει οκτώ TDMA κανάλια. Αυτό προκύπτει χωρίζοντας τη φέρουσα συχνότητα σε οκτώ χρονοθυρίδες (time slots) απαρτίζουν ένα TDMA πλαίσιο. Κάθε χρονοθυρίδα διαρκεί για περίοδο 156,25 bits ή αλλιώς για $15/26 \text{ ms} = 576,9 \mu\text{s}$. Κατά συνέπεια ένα TDMA πλαίσιο διαρκεί 4,613 ms. Ένας κινητός σταθμός χρησιμοποιεί τις ίδιες χρονοθυρίδες τόσο στην ανερχόμενη όσο και στην κατερχόμενη ζεύξη.



Σχήμα 0-2: Δομή ραδιοζεύξης

3.2.1 Περιγραφή των GSM Gateways

Οι πύλες GSM είναι συσκευές των οποίων αρχικός σκοπός ήταν να επιτραπούν σε κλήσεις που εκκινούν από ένα δίκτυο σταθερής τηλεφωνίας να διασυνδέονται με τα κινητά δίκτυα τηλεπικοινωνιών. Τα τηλέφωνα σταθερής τηλεφωνίας συνδέονται με τη συσκευή που περιέχει ένα ή περισσότερα GSM SIMs. Η πύλη GSM συνδέει έπειτα τις κλήσεις που γίνονται με τα τηλέφωνα σταθερής τηλεφωνίας με το δίκτυο GSM χρησιμοποιώντας το SIMs που περιλαμβάνεται μέσα σε αυτά. η διαδικασία κλήσης χωρίς την χρήση GSM Gateways. Μια κλήση η οποία εκκινεί από σταθερό δίκτυο προς ένα κινητό αποδέκτη κατευθύνεται στο G-MSC (Gateway mobile switching center). Κινητό κέντρο μετατροπής με μια πρόσθετη λειτουργία που επιτρέπει σε ένα δίκτυο GSM να διασυνδέεται με άλλα δίκτυα από εκεί στο BSC (Base station controller) και από εκεί παραδίδεται στον κινητό αποδέκτη μέσω του BTS (Base transceiver station) του κινητού παρόχου. Αυτός είναι ο κλασσικός τρόπος κλήσης που μεγιστοποιεί την αποτελεσματικότητα των δικτύων και την ποιότητα κλήσης μέσω τυποποιημένων διεπαφών και διαδικασιών από την βιομηχανία και τους διεθνείς τηλεπικοινωνιακούς οργανισμούς (ETSI, ITU κλπ). Είναι επίσης σύμφωνο με τις ευρωπαϊκές και εθνικές ρυθμιστικές υποχρεώσεις σχετικά με τη διασύνδεση δικτύων. Έστω μια κλήση που εκκινεί από ένα σταθερό δίκτυο με τελικό προορισμό ένα παραλήπτη κινητού δικτύου, με την χρήση GSM Gateways η πορεία που θα ακολουθηθεί είναι η εξής: από τον καλούντα η κλήση θα δρομολογηθεί προς το Gateway, η οποία περιέχει τις Subscriber Identity Modules (SIMs), διάφορα δίκτυα κινητής τηλεφωνίας .

Όταν η κλήση φτάσει στην Gateway αναγνωρίζει το κινητό δίκτυο του καλούμενου, επιλέγει την κατάλληλη SIM και δημιουργεί μια νέα κλήση προς αυτό, χρησιμοποιώντας το δίκτυο κινητής στο οποίο ανήκει αυτός (on-net κλήση) , ή όταν αυτό δεν είναι διαθέσιμο δίκτυο άλλης εταιρείας κινητής τηλεφωνίας η οποία σε αυτή την περίπτωση λειτουργεί ως transit network (off-net κλήση). Όταν αυτός ανταποκριθεί συνδέει τον καλούμενο με τον καλούντα. Η παραπάνω διαδικασία εξασφαλίζει οικονομικό κέρδος στον καλούντα διότι εκμεταλλεύεται τις χαμηλότερες

χρεώσεις από κινητό σε κινητό ίδιου η διαφορετικού παρόχου οι οποίες είναι συγκριτικά χαμηλότερες από τις αντίστοιχες από κινητό σε σταθερό και το ανάποδο. Από την έως τώρα χρήση των Gateways μπορούμε να αναγνωρίσουμε δύο ομάδες χρηστών οι οποίοι επωφελούνται από την χρήση των Gateways. Οι ομάδες αυτές είναι: Οι τελικοί χρήστες: Η κατηγορία αυτή μπορεί να διακριθεί σε δύο υποκατηγορίες, στους οικιακούς και στους εταιρικούς. Οι οικιακοί διαθέτουν Gateways μικρών δυνατοτήτων με σκοπό την εξυπηρέτηση των ατομικών αναγκών τους. Οι εταιρικοί διαθέτουν μεγάλων δυνατοτήτων Gateways τα οποία είναι συνδεδεμένα στα αυτόματα τηλεφωνικά κέντρα των εταιριών (PABX) . Τα εταιρικά Gateways έχουν δυνατότητες προγραμματισμού και παραμετροποίησης σύμφωνα με τις ανάγκες του χρήστη και περιέχουν αρκετή υπολογιστική ισχύ και ευφυΐα. Οι Εναλλακτικοί πάροχοι σταθερής τηλεφωνίας:

Η κατηγορία αυτή χρηστών χρησιμοποιούν τα Gateways προκειμένου να δρομολογήσουν κλήσεις που προέρχονται από το δίκτυό τους, προς το δίκτυο των παρόχων κινητής τηλεφωνίας. Για τον σκοπό αυτό τα Gateways συνδέονται με τα κέντρα μεταγωγής των εναλλακτικών τα οποία προγραμματίζονται κατάλληλα ώστε να δρομολογούν όλες τις κλήσεις που κατευθύνονται σε συνδρομητές κινητής τηλεφωνίας μέσω των αυτών. Στις παραγράφους που ακολουθούν θα γίνει παρουσίαση των επιπτώσεων από την χρήση των Gateways από όλες τις προαναφερθείσες ομάδες χρηστών. Πιθανά προβλήματα από τη λειτουργία των GSM-Gateways (GSM-gws) Υπάρχουν τέσσερις περιοχές στις οποίες μπορούμε να εστιάσουμε την προσοχή μας όσον αφορά πιθανά προβλήματα από την χρήση των τερματικών διατάξεων που καλούνται GSM-gws:

A) Προβλήματα που σχετίζονται με την διαχείριση του φάσματος συχνοτήτων και με θέματα σχεδιασμού και λειτουργίας των δικτύων.

B) Ζημίες στον καταναλωτή ως αποτέλεσμα της διακοπής ή της αδυναμίας παροχής της ζητούμενης υπηρεσίας (προβλήματα στην ποιότητα των παρεχόμενων υπηρεσιών).

Γ) Θέματα ασφάλειας που σχετίζονται και με νομικές υποχρεώσεις των παρόχων.

Δ) Διάφορα νομικά θέματα.

3.2.2. Μειονεκτήματα του GSM

Ενώ το GSM είναι κατάλληλο για τη μετάδοση φωνής κατά τη διάρκεια μιας τηλεφωνικής κλήσης, προβλήματα εμφανίζονται όταν πρόκειται για μετάδοση δεδομένων κατά τη διάρκεια μιας συνόδου. Πιο συγκεκριμένα, η ανάθεση των καναλιών στην ανερχόμενη και κατερχόμενη ζεύξη είναι η ίδια για όλη τη διάρκεια της συνόδου, με αποτέλεσμα ο χρήστης να πληρώνει για τη χρονική διάρκεια της συνόδου και όχι για τον όγκο των δεδομένων που μετέδωσε (ή/και έλαβε). Έτσι, ο χρήστης μπορεί να πληρώνει και για τη χρονική διάρκεια που περίμενε να λάβει ή να μεταδώσει κάποια δεδομένα, χωρίς ουσιαστικά να μεταδίδει ή να λαμβάνει τίποτα. Ένα άλλο μειονέκτημα είναι ο μεγάλος χρόνος που απαιτείται για την εγκαθίδρυση της σύνδεσης (20 με 25 δευτερόλεπτα) σε συνδυασμό με την από-άκρη-σε-άκρη καθυστέρηση (round-trip delay) που υπολογίζεται γύρω στα 400 με 500 ms. Ο ρυθμός μετάδοσης φτάνει τα 9,6 kbps που είναι αρκετά μικρός σε σύγκριση με τους σημερινούς ρυθμούς μετάδοσης στο Διαδίκτυο. Επίσης, σε κάθε χρήση ανατίθεται μία χρονοθυρίδα, που σημαίνει ότι ο μέγιστος αριθμός χρηστών που μπορούν να εξυπηρετηθούν ταυτόχρονα από μια φέρουσα συχνότητα είναι οκτώ. Αν αυτό συνδυαστεί με το γεγονός ότι και ο πιο ενεργός χρήστης χρησιμοποιεί πλήρως μόνο την μία κατεύθυνση ζεύξης (ανερχόμενη ή κατερχόμενη) τότε είναι φανερό ότι υπάρχει ένα ποσοστό 50% σπατάλης των ασύρματων πόρων. Τα παραπάνω προβλήματα που παρουσίαζε το GSM για τη μετάδοση δεδομένων οδήγησαν στη δημιουργία μιας νέας υπηρεσίας του GSM που θα αφορούσε αποκλειστικά τη μετάδοση δεδομένων πάνω από το GSM, χρησιμοποιώντας όμως τεχνικές μεταγωγής πακέτου και όχι κυκλώματος όπως χρησιμοποιούνταν μέχρι τότε τόσο για μετάδοση φωνής όσο και για μετάδοση δεδομένων. Το προσφερόμενο ηλεκτρομαγνητικό φάσμα το οποίο διατίθεται για τηλεπικοινωνιακή χρήση είναι ένας πεπερασμένος πόρος και η Εθνική Επιτροπή Τηλεπικοινωνιών (εφεξής EET) είναι αρμόδια για την εξασφάλιση

ότι χρησιμοποιείται αποτελεσματικά ώστε να ικανοποιεί τις τρέχουσες και μελλοντικές απαιτήσεις με γνώμονα το εθνικό και κοινοτικό δίκαιο και την προστασία των καταναλωτών. Αυτές οι ευθύνες οδήγησαν την ΕΕΤ στην έναρξη δημόσιας διαβούλευσης, με θέμα «Λειτουργία και χρήση των GSM-Gateways στην Ελληνική Αγορά Τηλεπικοινωνιών». Αυτές οι συσκευές αναφέρονται συνήθως ως Mobile Gateways ή GSM Gateways ή και SIM Boxes και η βασική λειτουργία τους είναι να επιτρέπουν στα σταθερά τηλεφωνικά δίκτυα να συνδέονται άμεσα με τα κινητά δίκτυα μέσω μιας σύνδεσης κινητής τηλεφωνίας. Το παρών έγγραφο παρέχει λεπτομέρειες για την πιθανή χρήση των πυλών GSM από τους τελικούς χρήστες ή από τους παρόχους τηλεπικοινωνιακών υπηρεσιών και παρουσιάζει τις ευρείες επιπτώσεις της χρήσης τους και στις δύο καταστάσεις. Το έγγραφο διευκρινίζει πρόσθετα το ρυθμιστικό περιβάλλον για αυτές τις συσκευές με την παρουσίαση της θέσης ΕΕΤ σε σχέση με τη χρήση αυτών των συσκευών και στα δύο σενάρια.

4. ΚΩΔΙΚΟΠΟΙΗΣΗ ΦΩΝΗΣ

Η φωνή δειγματοληπτείται με ρυθμό 8000 δείγματα ανά sec. Κάθε δείγμα ψηφιοποιείται σε 13 bits (ο κωδικοποιητής κωδικοποιεί με 16 bit ανά δείγμα, αλλά το GSM αγνοεί 3 bit). Άρα, ο ρυθμός είναι 104 Kbit/sec. Στην είσοδο του κωδικοποιητή, 160 ομάδες των 13 bit φτάνουν μέσα σε ένα διάστημα 20 msec. Ο κωδικοποιητής συμπιέζει τα δεδομένα αυτά, μετατρέποντάς τα σε μπλοκ των 260 bit (άρα, ρυθμός 13 kbit/sec). Έχουμε λοιπόν μία συμπίεση της τάξης 1:8. Η συμπίεση γίνεται με τον αλγόριθμο που λέγεται Regular Pulse Excitation - Long term Prediction - Linear Predictive Coder (RPELTP).

Βασίζεται στο ότι χρησιμοποιούνται προηγούμενα δείγματα για την πρόβλεψη των επομένων, λόγω του ότι σε πολύ μικρό χρονικό διάστημα η πληροφορία αλλάζει ελάχιστα. Στην ουσία, δεν ψηφιοποιείται το δείγμα αυτό κάθε αυτό, αλλά η διαφορά του από το προηγούμενο δείγμα (κάτι που απαιτεί πολύ λιγότερα bit).

4.1. Η φωνή ως σήμα και το υπόβαθρο της

Οι φωνητικοί ήχοι είναι η απήχηση των ταλαντώσεων της πίεσης του αέρα που εκπνέεται από τους πνεύμονες και διαμορφώνονται (Modulated) και προσαρμόζονται (shaped) σε σχήμα από τις ταλαντώσεις των φωνητικών χορδών (glottal chords) καθώς και την αντήχηση ή συντονισμό (resonance) του φωνητικού σωλήνα καθώς ο αέρας πιέζεται μέσω των χειλιών και της μύτης. Η φωνή είναι πολύ πλούσιο σήμα σε πληροφορία το οποίο εκμεταλλεύεται την διαμόρφωση σε συχνότητα (Frequency-modulated), διαμόρφωση σε πλάτος (amplitude-modulated) και σε φέρων διαμορφωμένο στο χρόνο (and time-modulated carriers) π.χ. αρμονικές και θόρυβος, διάρκεια ισχύος, κυματισμός του pitch, μετακινήσεις της αντήχησης κτλ, για να μεταφέρει πληροφορία σχετικά με λέξεις, την ταυτότητα του ομιλητή, προφορά, συναισθηματική κατάσταση, αλλά και κατάσταση υγείας του. Από μία τηλεπικοινωνιακή σκοπιά όλη αυτή η πληροφορία μπορεί να εκμαιευθεί από το παραδοσιακό τηλέφωνο με εύρος 4KHz, η ενέργεια της φωνής πάνω από αυτό το εύρος μπορεί να μεταφέρει πληροφορία για την ποιότητα του ήχου, αλλά και την αίσθηση (sensation).

4.2. Κωδικοποίηση και αποκωδικοποίηση.

Η κωδικοποίηση και αποκωδικοποίηση της φωνής εξασφαλίζει τις απαραίτητες μετατροπές που πρέπει να εφαρμοστούν στα –αναλογικής μορφής– ηχητικά κύματα, ώστε αυτά να μεταφερθούν μέσα από το ψηφιακό δίκτυο IP. Τη λειτουργία της μετατροπής του αναλογικού σήματος σε ψηφιακό αναλαμβάνει ένα κύκλωμα που λέγεται encoder (κωδικοποιητής), ενώ την ακριβώς αντίστροφη διαδικασία, δηλαδή την επαναφορά του σε αναλογική μορφή κατανοητή από τον συνομιλητή μας, αναλαμβάνει ο decoder (αποκωδικοποιητής). Ο encoder και ο decoder ονομάζονται, χάριν συντομίας με μία λέξη codec. Εκτός από την ψηφιοποίηση και από-ψηφιοποίηση του σήματος, ο codec συχνά εφαρμόζει και μια συμπίεση των πληροφοριών, ώστε να εξοικονομηθούν σημαντικοί πόροι του δικτύου. Είναι χαρακτηριστικό ότι αν το σήμα παρέμενε ασυμπίεστο, θα απαιτούνταν γραμμές αρκετών Mbps για την αποπεράτωση μίας και μόνο συνομιλίας. Αντίθετα, χάρη στη συμπίεση, η ανθρώπινη φωνή μπορεί να μεταφερθεί και από μια γραμμή δεδομένων ταχύτητας λίγων Kbps χωρίς καμία αλλοίωση της ποιότητας και κυρίως χωρίς διακοπές.

4.2.1. Κωδικοποίηση στο δίκτυο GSM

Το GSM, είναι ένα καθαρά ψηφιακό δίκτυο, οπότε τα αναλογικά σήματα ήχου, θα πρέπει να περάσουν από την διαδικασία της ψηφιοποίησης. Η μέθοδος που χρησιμοποιείται από το ISDN και τα υπάρχοντα τηλεφωνικά δίκτυα είναι η PCM η οποία όμως βγάζει σαν αποτέλεσμα, ροή 64Kbps, αρκετά υψηλή για να μεταφερθεί με ραδιοζεύξη. Το GSM τελικά κατέληξε στην χρήση ενός διαφορετικού πρωτόκολλου του **RPE-LPC**, το οποίο παίρνει τις πληροφορίες από τα προηγούμενα δείγματα φωνής, τα οποία δεν αλλάζουν αρκετά γρήγορα και προβλέπει την τρέχον

δειγματοληψία. Η φωνή, χωρίζεται σε δείγματα των 20 millisecond, κωδικοποιημένα στα 260bits, δίνοντας συνολική ροή δεδομένων 13Kbps.

4.2.2. Το σχήμα κωδικοποίησης

Ο front-end μηχανισμός παράγει τα ακουστικά διανύσματα με τους 13 ή 39 MFCC συντελεστές για κάθε frame (δηλαδή διάστημα 10 msec), με αποτέλεσμα ο ρυθμός πληροφορίας να είναι 1300 (ή 3900) συντελεστές αντίστοιχα ανά second. Αφού κάθε συντελεστής αντιπροσωπεύεται από μια float μεταβλητή απαιτούνται $1300 \text{ ή } 3900 * 32 \text{ bits/sec}$, δηλαδή 41,6 ή 124.8 kbps αντίστοιχα. Αυτός ο ρυθμός είναι μικρότερος σε σχέση με αυτό της αρχικής πηγής πληροφορίας (δειγματοληπτημένη κυματομορφή σε 8 ή 16Khz και με 16bits ανά σύμβολο) και σκοπός μας είναι να τον μειώσουμε ακόμα περισσότερο , χρησιμοποιώντας τεχνικές κβαντισμού.

Θυμίζουμε ότι με τον κβαντισμό, ουσιαστικά περιορίζουμε τον αριθμό συμβόλων εξόδου, σε ένα μικρό σύνολο προτύπων συμβόλων εξόδου, καταφέροντας να συμπιέσουμε από τη μια το σήμα αλλά και δυστυχώς να εισάγουμε θόρυβο από την άλλη. Στην εισαγωγή αυτού του κεφαλαίου, τονίσαμε ότι επειδή στόχος μας δεν είναι η όσο πιο πιστή αναπαραγωγή του σήματος, αλλά η καλλίτερη δυνατή αναγνώριση, την απώλεια πληροφορίας που έχουμε με τον κβαντισμό, τη μετράμε με βάση τα αποτελέσματα της αναγνώρισης. Αυτό μας βοηθάει πρακτικά στο να αξιολογήσουμε τα διάφορα σχήματα κωδικοποίησης.

4.2.3. Κωδικοποίηση και διαμόρφωση καναλιών

Λόγω των ηλεκτρομαγνητικών παρεμβολών, η κωδικοποιημένη φωνή και τα δεδομένα που μεταφέρονται μέσω ραδιοκυμάτων, θα πρέπει να προστατευθούν. Μετά από αντικειμενικές δοκιμές, βρέθηκε ότι κάποια συγκεκριμένα bits ήταν και τα πιο σημαντικά για την διατήρηση της ποιότητας του ήχου. Αυτά τα bits, χωρίστηκαν σε 3 κλάσεις :

- Κλάση Ia 50 bits - μεγαλύτερη ευαισθησία σε λάθη των bit
- Κλάση Ib 132 bits - μέτρια ευαισθησία σε λάθη των bit
- Κλάση II 78 bits - μικρή ευαισθησία σε λάθη των bit

Τα ψηφία της κλάσης Ia, έχουν ένα 3ψήφιο πλεονάζον κυκλικό κώδικα, ο οποίος έχει προστεθεί για την διόρθωση των λαθών. Αν βρεθεί κάποιο λάθος, το πλαίσιο κρίνεται φθαρμένο για μεταφορά και απορρίπτεται. Αντικαταστίεται από μια εξασθετισμένη έκδοση του προηγούμενου σωστού πλαισίου. Τα 53 αυτά ψηφία, μαζί με τα 132 ψηφία της κλάσης Ib και 4 ψηφία για το κλείσιμο της ακολουθίας, δίνονται σε έναν κωδικοποιητή και κάθε ψηφίο μετατρέπεται σε 2, βασισμένο σε συνδυασμό των 4 προηγούμενων ψηφίων. Ο κωδικοποιητής έχει σαν αποτέλεσμα 378 ψηφία, τα οποία προστίθενται στα απομένοντα ψηφία της κλάσης II. Έτσι κάθε 20 ms ομιλίας κωδικοποιούνται σε 456bits, δίνοντας ροή δεδομένων 22.8kbps. Τα 456 αυτά ψηφία χωρίζονται σε 8 μπλόκ των 57 ψηφίων και το καθένα από αυτά διανέμετε σε μια μονάδα χρόνου. Αφού κάθε μονάδα χρόνου μπορεί να μεταφέρει δύο μπλοκ των 57 ψηφίων, μεταφέρονται δύο διαφορετικά δείγματα φωνής.

Το ψηφιακό σήμα διαμορφώνεται σε αναλογικές συχνότητες με εύρος φάσματος 200KHz, χρησιμοποιώντας ψηφιακή διαμόρφωση GMSK (Gaussian-filtered Minimum Shift Keying). Το GMSK επιλέχθηκε, καθώς αποτελεί ένα πολύ καλό συμβιβασμό μεταξύ εξοικονόμησης φάσματος, πολυπλοκότητα του πομπού και περιορισμένες ανεπιθύμητες παρεμβολές σε γειτονικά κανάλια, ώστε να μπορεί να συνυπάρχει με τα αναλογικά δίκτυα.

Στους 900MHz τα ραδιοκύματα ανακλούνται σε φυσικά εμπόδια, όπως κτίρια, αμάξια, φυσικά εμπόδια κ.α. Έτσι δημιουργούνται πολλά αντανακλώμενα σήματα, που φτάνουν στην κεραία με διαφορετική φάση και μέσα από τα οποία πρέπει να ανακτηθεί το σωστό σήμα της ομιλίας. Έτσι στην μέση κάθε πλαισίου το GSM αποστέλλει ένα καθορισμένο 26bit σήμα και με διάφορους αλγορίθμους επεξεργάζεται το σήμα, ώστε να είναι όσο το δυνατόν ποιο σωστό γίνεται.

Για να αυξηθεί η απόδοση του συστήματος και επίσης για να μην υπάρχουν αρκετές παρεμβολές στις συχνότητες, χρησιμοποιείται η μη συνεχόμενη μετάδοση δεδομένων (DTX). Το DTX εκμεταλλεύεται τα κενά που υπάρχουν στην ομιλία, κλείνοντας σε εκείνες τις περιόδους τον πομπό, εξοικονομώντας παράλληλα ενέργεια στην κινητή μονάδα.

5. ΤΕΧΝΙΚΕΣ ΚΩΔΙΚΟΠΟΙΗΣΗΣ ΦΩΝΗΣ

- WAVEFORM CODING
- MODEL-BASED
- HYBRID

Σε κάθε μια από τις παραπάνω κατηγορίες συναντάμε τεχνικές που παρέχουν διαφορετικούς ρυθμούς μετάδοσης, ακρίβεια αναπαράστασης της πληροφορίας, απόδοση παρουσία θορύβου και πολυπλοκότητα υλοποίησης. Κάθε κατηγορία εξυπηρετεί λοιπόν διαφορετικές ανάγκες.

5.1. Waveform Coding τεχνικές

Οι τεχνικές αυτής της κατηγορίας, είναι στη πλειοψηφία τους σχετικά απλές. Σκοπός είναι η πιστή αναπαραγωγή του σήματος της φωνής στο δέκτη. Κωδικοποιητές (coders) κυματομορφής έχουν σχεδιαστεί τόσο στο πεδίο του χρόνου όσο και στο πεδίο της συχνότητας και είναι αρκετά γρήγοροι λόγω ακριβώς της σχετικά απλής λειτουργίας τους.

5.1.1. Model based τεχνικές (Vocoders)

Σε αντίθεση με τις τεχνικές της προηγούμενης κατηγορίας που βασίζονται σε μία δείγμα προς δείγμα ή frames ανά frames αναπαράσταση της κυματομορφής (πεδίο της χρόνου/συχνότητας), οι τεχνικές αυτής της κατηγορίας βασίζονται στο μοντέλο παραγωγής φωνής. Έτσι χρησιμοποιώντας τη γνώση μας για την διαδικασία παραγωγής φωνής, οι τεχνικές αυτές καταφέρνουν να αναπαριστούν το σήμα της φωνής με πολύ μικρότερο bandwidth και τέτοιες είναι και οι εφαρμογές στις οποίες χρησιμοποιούνται. Ουσιαστικά γίνεται εξαγωγή παραμέτρων που αντιστοιχούν στις χρονικά μεταβαλλόμενες παραμέτρους του φωνητικού σωλήνα.

Υπάρχουν 2 δυνατές πηγές, η πρώτη πηγή αντιστοιχεί στον ήχο χωρίς φωνή και η δεύτερη σε αυτόν με φωνή (unvoiced & voiced sounds). Στην 2η πηγή η φωνή παράγεται όταν οι φωνητικές χορδές πάλλονται σε κάποια βασική συχνότητα f_0 . Μια πηγή κάθε χρονική στιγμή διεγείρει το φίλτρο που αναπαριστάνει το φωνητικό σωλήνα και έτσι παράγεται το σήμα της φωνής. Η παραγωγή των παραμέτρων του φωνητικού σωλήνα γίνεται με χρήση γραμμικής πρόβλεψης (linear prediction coding). Το σύνολο των παραμέτρων που προκύπτουν περιλαμβάνουν τους συντελεστές πρόβλεψης, το κέρδος (gain) του σήματος, το είδος εισόδου που έχουμε και τη συχνότητα f_0 , εφόσον η είσοδος είναι voiced. Οι παραπάνω παράμετροι μεταδίδονται στον δέκτη όπου χρησιμοποιώντας το ίδιο μοντέλο ανακατασκευάζεται το αρχικό σήμα (για αυτό το λόγο οι τεχνικές αυτές ονομάζονται επίσης analysis by synthesis τεχνικές). Από αυτές τις παραμέτρους και με κατάλληλους μετασχηματισμούς μπορούν να προκύψουν ακουστικά διανύσματα, τα οποία βέβαια μπορούν επίσης να χρησιμοποιηθούν για αναγνώριση. Άρα η μέθοδος αυτή αποτελεί

ουσιαστικά ένα εναλλακτικό front-end μηχανισμό. Αποτελεί φυσικά και μέθοδο κωδικοποίησης φωνής, αφού από το αρχικό σήμα φωνής έχει ήδη προκύψει μια ακολουθία ακουστικών διανυσμάτων.

Βασικό χαρακτηριστικό των vocoders είναι οι χαμηλοί ρυθμοί μετάδοσης αλλά και η χαμηλή ποιότητα. Υπάρχουν πολλές υλοποιήσεις vocoders με πιο διαδεδομένους όσους στηρίζονται σε τεχνικές γραμμικής πρόβλεψης, σαν αυτή που μόλις περιγράφηκε. Οι υβριδικοί κωδικοποιητές (επίσης vocoders), προσπαθούν να χρησιμοποιήσουν μια πιο σύνθετη διέγερση από τους LPC vocoders, καταφέροντας έτσι καλή ποιότητα για χαμηλούς-μέσους ρυθμούς μετάδοσης. Υλοποιήσεις vocoders (υβριδικών και μη) είναι οι channel, phase, cepstral & formant vocoders, καθώς και οι RELP, CELP & VSELP vocoders. Μάλιστα η κωδικοποίηση GSM στη κινητή τηλεφωνία δευτέρας γενεάς, βασίζεται σε RPE-LTP υβριδικό κωδικοποιητή, ενώ οι CELP αποτελούν το πρότυπο για κινητή τηλεφωνία στην Βόρειο Αμερική.

5.1.2. Το μοντέλο linear predictive coding

Η θεωρία του LPC (Linear Predictive Coding) όπως εφαρμόζεται στην αναγνώριση φωνής είναι γνωστή αρκετά χρόνια. Η μέθοδος αυτή είναι ευρέως ιαδεδομένη κυρίως για τους εξής λόγους:

1. Η θεωρία LPC παρέχει ένα καλό μοντέλο του σήματος φωνής ειδικά για τα φαινομενικά σταθερής κατάστασης μέρη του σήματος που περιέχουν ήχο στα οποία δίνει μια καλή προσέγγιση της φωνητικής οδού. Σε unvoiced (άηχα) μέρη του σήματος και σε μεταβατικά στάδια το LPC μοντέλο είναι λιγότερο αποτελεσματικό.

2. Ο τρόπος που η LPC εφαρμόζεται στην ανάλυση του σήματος δίνει έναν καλό διαχωρισμό της πηγής με την φωνητική οδό με αποτέλεσμα να έχουμε συμπίεση των χαρακτηριστικών του σήματος.

3. Το LPC είναι ένα βολικό μοντέλο. Η μέθοδος είναι μαθηματικά ακριβής και απλή στην εφαρμογή είτε σε hardware είτε σε software. Το υπολογιστικό κόστος είναι συγκριτικά μικρότερο από μεθόδους όπως η Filterbank.

4. Πειραματικά το LPC μοντέλο λειτουργεί καλά στην αναγνώριση φωνής.

Βασική θεωρία του LPC μοντέλου

Η βασική ιδέα του LPC είναι ότι μια τιμή (sample) ενός σήματος στο χρόνο, $s(n)$ την χρονική στιγμή n μπορεί να προσεγγισθεί ως γραμμικός συνδυασμός των προηγούμενων p δειγμάτων (samples) σύμφωνα με την σχέση:

$s(n) \sim a_1 s(n-1) + a_2 s(n-2) + \dots + a_p s(n-p)$ όπου οι συντελεστές a_1, a_2, \dots, a_p , είναι σταθεροί στο πλαίσιο (frame) του σήματος που γίνεται η ανάλυση.

5.1.3. Αλγόριθμος LPC για αναγνώριση φωνής.

Σε αυτό το κομμάτι θα περιγράψουμε τις λεπτομέρειες της LPC frontend επεξεργασίας χωρίζοντάς την σε στάδια επεξεργασίας για ευκολία.

Τα στάδια είναι τα εξής:

1. Προέμφαση (Preemphasis) – Το ψηφιοποιημένο σήμα, $s(n)$, περνά μέσα από ένα πρώτου βαθμού FIR φίλτρο για να το κάνουμε πιο ανθεκτικό σε θέματα ακρίβειας στην πορεία της επεξεργασίας του. Το πιο συνηθισμένο σύστημα προέμφασης είναι το φίλτρο πρώτου βαθμού: $H(z) = 1 - az^{-1}$

Η έξοδος του συστήματος σχετίζεται με την είσοδο με τη εξίσωση:

$$S(n) = S(n) - aS(n-1)$$

με ποιο κοινή τιμή για το a να είναι το 0.95.

2. Frame blocking – Σε αυτό το στάδιο ορίζουμε ένα πλαίσιο (frame) των N δειγμάτων (samples). Μέσα σε αυτό το πλαίσιο γίνεται η LPC ανάλυση. Το

πλαίσιο αυτό ‘κυλάει’ ανατρέχοντας όλο το σήμα. Μόλις γίνει η ανάλυση στο πρώτο πλαίσιο τότε μετακινείται κατά M δείγματα του σήματος και γίνεται ανάλυση στα επόμενα N samples. Έτσι το πρώτο frame αποτελείται από N samples. Το δεύτερο frame ξεκινά M samples από το σημείο αρχής του πρώτου και επικαλύπτει το πρώτο frame κατά $N - M$ samples. Έτσι και το τρίτο αρχίζει $2M$ samples μετά το πρώτο και το επικαλύπτει κατά $N - 2M$ ή κατά $N - M$ το δεύτερο. Δηλαδή, το πρώτο frame θα αποτελείται από τις τιμές του σήματος $s(0), s(1), \dots, s(N-1)$, το δεύτερο frame από τις τιμές $s(M), s(M+1), \dots, s(M+N-1)$ και το l th frame από τις τιμές $s(M(L-1)), s(M(L-1)+1), \dots, s(M(L-1)+N-1)$. Η τιμή του M επιλέγεται συνήθως ώστε να είναι $M = 1/3 N$. Αν το $M \ll N$ τότε το LPC φάσμα θα είναι ομαλό ενώ αν το $M > N$ τότε δεν υπάρχει επικάλυψη των frames και κάποιο από το σήμα μας θα χαθεί και η σχέση μεταξύ των τιμών του LPC φάσματος θα είναι θορυβώδης.

3. Windowing – Εδώ επιβάλλουμε σε κάθε frame ένα ‘παράθυρο’ έτσι ώστε να μειώσουμε τις ασυνέχειες του σήματος στην αρχή και στο τέλος κάθε frame. Αυτό γίνεται όπως προαναφέραμε σε προηγούμενο κεφάλαιο για να κάνουμε το σήμα μας μηδέν στην αρχή και τέλος του κάθε frame. Αν ορίσουμε ένα ‘παράθυρο’ ως $w(n)$, $0 \leq n \leq N-1$ τότε το αποτέλεσμα αυτής της διαδικασίας θα είναι :

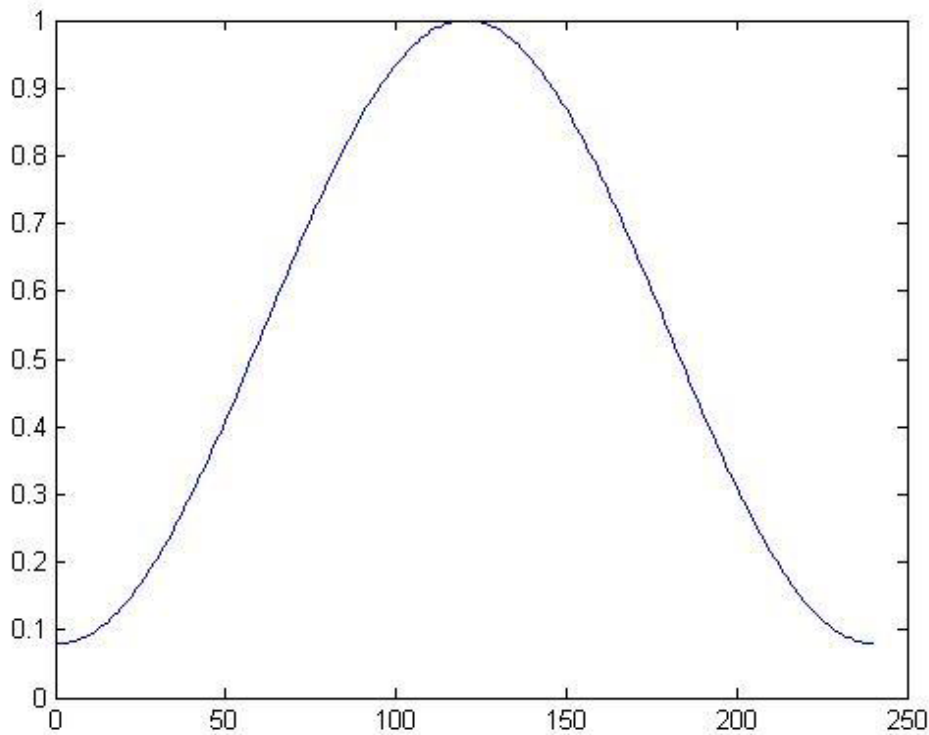
$$X_l(n) = X_l(n)W(n)$$

το subscript l δείχνει το l th frame. Συνήθως στην autocorrelation

χρησιμοποιούμε το Hamming ‘παράθυρο’:

$$W(n) = 0.54 - 0.46 \cos(2\pi n / (N-1)) \quad 0 \leq n \leq N-1$$

Η γραφική παράσταση ενός Hamming παραθύρου 240 τιμών φαίνεται παρακάτω και μπορούμε να καταλάβουμε γιατί μηδενίζει τις τιμές στα άκρα του πλαισίου



Σχήμα 3: Διάγραμμα Hamming

6. VOICE OVER IP (IP Τηλεφωνία)

Τεχνολογία που χρησιμοποιεί ως βάση της το πρωτόκολλο TCP/IP, για την πραγματοποίηση τηλεφωνικών κλήσεων. Τα αρχικά του TCP/IP προέρχονται από τις λέξεις Transmission Control Protocol/Internet Protocol, ή σε ελεύθερη μετάφραση στα ελληνικά: πρωτόκολλο ελέγχου αποστολής δεδομένων/πρωτόκολλο διαδικτύου.

Η ιδέα της χρήσης του TCP/IP για τη μετάδοση φωνητικής πληροφορίας, παλαιότερα έμοιαζε με άπιαστο όνειρο, καθώς οι ρυθμοί μετάδοσης δεδομένων μεταξύ των δικτύων ήταν πολύ χαμηλοί, ενώ αντίθετα η μετάδοση ήχου ήταν ιδιαίτερα απαιτητική σε ταχύτητες. Σήμερα όμως τα πράγματα έχουν αλλάξει ριζικά. Οι συνδέσεις γίνονται όλο και γρηγορότερες, επιτρέποντας την ποιοτική μετάδοση ήχου ή ακόμα και εικόνας σε πραγματικό χρόνο (ροή εικόνας και ήχου ή audio/video

streaming). Παράλληλα, ανακαλύφθηκε ότι η κυματομορφή της ανθρώπινης φωνής μπορεί να συμπιεστεί σε πολύ μεγάλο ποσοστό, χωρίς να υποστεί σχεδόν καμία απώλεια όσον αφορά την ποιότητα και τη χροιά. Έτσι, μετά την αύξηση της χωρητικότητας των γραμμών, ήρθε και η μείωση των απαιτήσεων μιας φωνητικής συνομιλίας σε bandwidth, να κάνει ακόμα πιο προσιτή και εύκολη τη χρήση του TCP/IP για τη διεξαγωγή τηλεφωνικών κλήσεων.

Η τεχνολογία Voice over IP προσφέρει τα πλεονεκτήματά της τόσο στους παρόχους σταθερής τηλεφωνίας, όσο και στους απλούς συνδρομητές. Οι εταιρείες σταθερής τηλεφωνίας τώρα διαθέτουν πολύ υψηλότερη χωρητικότητα δικτύου, έχοντας την ευχέρεια έτσι να εξυπηρετήσουν περισσότερους συνδρομητές με μικρότερο κόστος. Μέσα από μια γραμμή μπορούν να μεταβιβάζονται τα δεδομένα πολλών τηλεφωνικών κλήσεων. Αντίθετα, χωρίς το Voice over IP, κάθε τηλεφωνική γραμμή μπορούσε να φέρει σε πέρας μόνο μια συνομιλία. Έπρεπε δηλαδή κάθε συνδρομητής να διαθέτει μια αποκλειστική γραμμή που συνδέει τον χώρο του με το τηλεφωνικό κέντρο του παρόχου του. Το Voice over IP επιτρέπει τη χρήση μιας γραμμής υψηλής ταχύτητας δεδομένων ώστε να εξυπηρετηθούν οι συνδρομητές μιας ολόκληρης περιοχής. Τα δεδομένα διαφορετικών συνομιλιών δεν υπάρχει καμία περίπτωση να αναμιχθούν μεταξύ τους, κάτι για το οποίο μεριμνεί το πρωτόκολλο TCP/IP. Στο PSTN δίκτυο σταθερής τηλεφωνίας, μια γραμμή παραμένει μόνιμα κατειλημμένη ακόμα και τα δευτερόλεπτα εκείνα που δεν μεταδίδεται φωνή. Αντίθετα, με το Voice over IP καταναλώνονται πόροι από το δίκτυο, ή bandwidth, όπως συνηθίζουμε να λέμε, μόνο κατά τις στιγμές που μεταδίδεται φωνή. Αυτό εξασφαλίζει καλύτερη αξιοποίηση των γραμμών, μικρότερο φόρτο αλλά και κόστος.

Οι επιχειρήσεις, μπορούν με τη σειρά τους να επωφεληθούν από το γεγονός ότι μια γραμμή δεδομένων μπορεί να μεταφέρει και το σήμα τηλεφωνικής συνομιλίας. Αν κάποια εταιρεία διαθέτει πολλά παραρτήματα, καθένα εκ των οποίων χρησιμοποιεί μια μισθωμένη γραμμή Internet ή ενδοδίκτυο, αυτή μπορεί να χρησιμοποιηθεί και για τη μετάδοση φωνής. Γίνεται έτσι περιττή η χρήση μιας γραμμής του δημόσιου σταθερού τηλεφωνικού δικτύου και αποφεύγεται η χρονοχρέωση των συνομιλιών.

Άλλο ένα πλεονέκτημα είναι η δυνατότητα παροχής νέων υπηρεσιών, προστιθέμενης ή μη αξίας, από τα δίκτυα σταθερής τηλεφωνίας προς τους συνδρομητές. Υπηρεσίες όπως η βίντεο-τηλεφωνία ή η αποστολή αρχείων από τον ένα συνομιλητή προς τον άλλο κατά τη διάρκεια της κλήσης, όπως επίσης και η τηλεδιάσκεψη μεταξύ απεριόριστου αριθμού ατόμων, είναι μόνο κάποιες από τις νέες ευκολίες που μπορεί να προσφέρει η τεχνολογία Voice over IP. Επίσης υπηρεσίες unified messaging μπορούν να υλοποιηθούν με ιδιαίτερα απλό τρόπο, επιτρέποντας έτσι τη συμβατότητα μεταξύ διαφορετικών μορφών μηνυμάτων. Για παράδειγμα, θα είναι εφικτή ακόμα και η ακρόαση του κειμένου ενός e-mail, δηλαδή η μετατροπή του σε φωνητικό μήνυμα που θα «ταξιδεύει» μέσω της τηλεφωνίας Voice over IP. Έμμεσο πλεονέκτημα μπορούν να αποκομίσουν και οι απλοί ιδιώτες. Το μικρότερο κόστος που έχουν οι γραμμές μεταφοράς δεδομένων για τους παρόχους σταθερής τηλεφωνίας, θα επιτρέψουν την προσφορά υπηρεσιών με χαμηλότερο κόστος, κάτι που φυσικά θα ωφελήσει τον απλό ιδιώτη, περισσότερο από οποιονδήποτε άλλο.

6.1. Οι πρωταρχικές λειτουργίες που εκτελεί ένα δίκτυο Voice over IP είναι οι εξής:

(1). Σηματοδότηση. Είναι μια από τις πιο σημαντικές διαδικασίες, καθώς πρόκειται ουσιαστικά για τον συντονισμό και σωστή συνεργασία όλων των μερών του δικτύου για την πραγματοποίηση μιας κλήσης. Τον ρόλο της σηματοδότησης αναλαμβάνει ειδικός εξοπλισμός που λέγεται Gatekeeper

(2). Διαχείριση αριθμών και συνδρομητικών στοιχείων. Η διαχείριση της αριθμοδότησης αναλαμβάνει την καταχώρηση των αριθμών των συνδρομητών, οι οποίοι στην περίπτωση της τηλεφωνίας μέσω IP είναι ειδικές διευθύνσεις δικτύου, γνωστές σαν IP addresses. Το ίδιο τμήμα αναλαμβάνει επίσης τη σύνδεση ενός αναλογικού δικτύου PSTN με ένα δίκτυο Voice over IP, κάνοντας τις απαραίτητες μετατροπές, ώστε να είναι εφικτή η επικοινωνία μεταξύ των συνδρομητών τους. Ο εξοπλισμός που αναλαμβάνει τη διασύνδεση και την κατάλληλη μετατροπή των

πληροφοριών μεταξύ διαφορετικών δικτύων και πρωτοκόλλων ονομάζεται Gateway.

(3). Δρομολόγηση κλήσεων. Το τμήμα διαχείρισης κλήσεων έχει σαν κύριο σκοπό τον έλεγχο της έναρξης και του τερματισμού της επικοινωνίας μεταξύ των συνδρομητών. Όταν μια κλήση τερματίζεται, απελευθερώνονται και οι ανάλογοι πόροι του δικτύου, ώστε να γίνουν αξιοποιήσιμοι από άλλους συνδρομητές που ίσως τους χρειαστούν. Παρόλο που αρχικά κάθε κατασκευαστής παρουσίαζε τη δική του αρχιτεκτονική δικτύου όσον αφορά την πραγματοποίηση των κλήσεων, το τελευταίο διάστημα κάθε δίκτυο Voice over IP τείνει να ακολουθήσει τα πρότυπα H.323 και SIP, που έχουν σχεδιαστεί από την ITU (International Telecommunications Union) και τον IETF αντίστοιχα. Αυτό εξασφαλίζει συμβατότητες μεταξύ διαφορετικών δικτύων, αλλά και συσκευών τηλεφωνίας IP.

(4). Κωδικοποίηση και αποκωδικοποίηση. Η κωδικοποίηση και αποκωδικοποίηση της φωνής εξασφαλίζει τις απαραίτητες μετατροπές που πρέπει να εφαρμοστούν στα – αναλογικής μορφής- ηχητικά κύματα, ώστε αυτά να μεταφερθούν μέσα από το ψηφιακό δίκτυο IP. Τη λειτουργία της μετατροπής του αναλογικού σήματος σε ψηφιακό αναλαμβάνει ένα κύκλωμα που λέγεται encoder (κωδικοποιητής), ενώ την ακριβώς αντίστροφη διαδικασία, δηλαδή την επαναφορά του σε αναλογική μορφή κατανοητή από τον συνομιλητή μας, αναλαμβάνει ο decoder (αποκωδικοποιητής). Ο encoder και ο decoder ονομάζονται, χάριν συντομίας με μία λέξη codec. Εκτός από την ψηφιοποίηση και από-ψηφιοποίηση του σήματος, ο codec συχνά εφαρμόζει και μια συμπίεση των πληροφοριών, ώστε να εξοικονομηθούν σημαντικοί πόροι του δικτύου. Είναι χαρακτηριστικό ότι αν το σήμα παρέμενε ασυμπίεστο, θα απαιτούνταν γραμμές αρκετών Mbps για την αποπεράτωση μίας και μόνο συνομιλίας. Αντίθετα, χάρη στη συμπίεση, η ανθρώπινη φωνή μπορεί να μεταφερθεί και από μια γραμμή δεδομένων ταχύτητας λίγων Kbps χωρίς καμία αλλοίωση της ποιότητας και κυρίως χωρίς διακοπές.

6.2. ΜΕΣΑ ΑΣΥΡΜΑΤΟΥ ΜΕΤΑΔΟΣΗΣ

Τα μέσα μετάδοσης που χρησιμοποιούνται στα ασύρματα τοπικά δίκτυα υπολογιστών, είναι οι διάφορες μορφές ηλεκτρομαγνητικής ακτινοβολίας, οι οποίες εντοπίζονται κυρίως στο φάσμα των ραδιοφωνικών συχνοτήτων (στο εύρος των 104 έως 109 Hz), στο φάσμα των μικροκομματικών συχνοτήτων (στο εύρος των 109 έως 1012 Hz) καθώς επίσης και στο φάσμα των υπέρυθρων ακτινοβολιών (στο εύρος των 1012 έως και 1014 Hz του ηλεκτρομαγνητικού φάσματος συχνοτήτων). Πιο αναλυτικά, η χρήση αυτών των μέσων στα τοπικά δίκτυα υπολογιστών, έχει ως εξής :

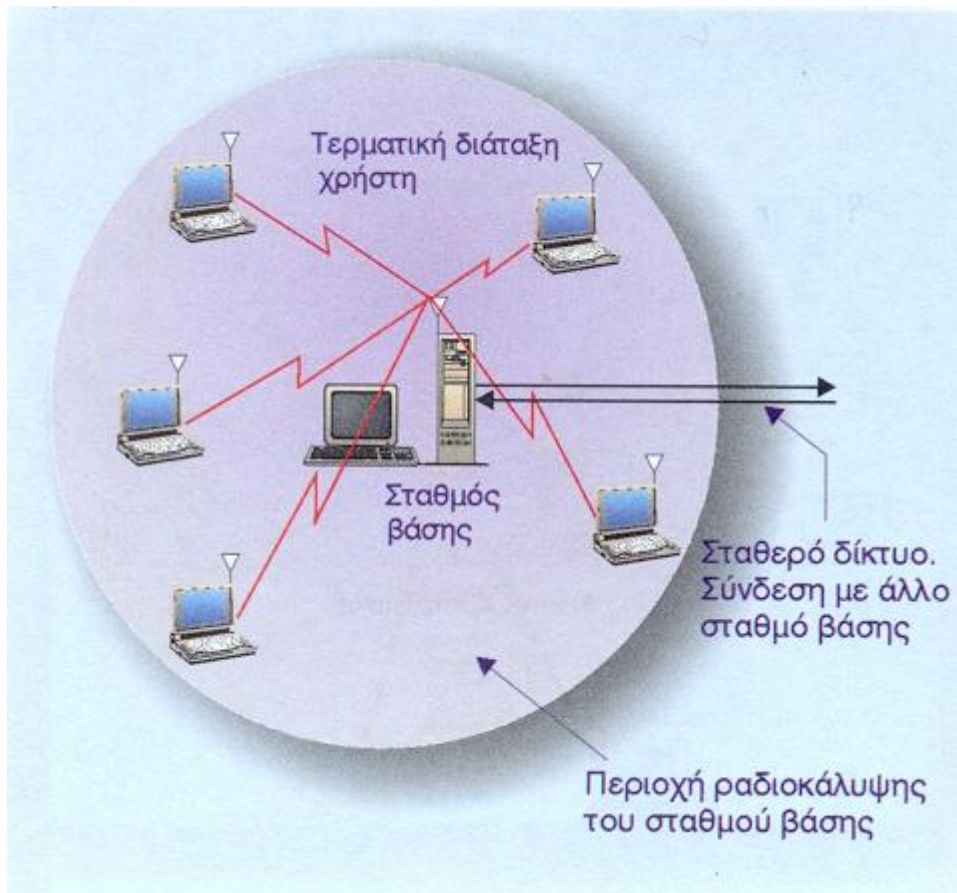
Οι ραδιοσυχνότητες χρησιμοποιούνται κυρίως στις ραδιοφωνικές και τηλεοπτικές εκπομπές καθώς επίσης και στα κυτταρικά τηλεφωνικά δίκτυα. Το βασικό μειονέκτημα αυτού του τύπου επικοινωνίας, είναι η επικάλυψη των διαφόρων περιοχών συχνοτήτων του ηλεκτρομαγνητικού φάσματος, γεγονός που οδηγεί στον καθορισμό μιας συγκεκριμένης ζώνης συχνοτήτων για κάθε εφαρμογή. Από την άλλη πλευρά, η επικοινωνία δια της χρήσης μικροκομματικής ακτινοβολίας, χρησιμοποιείται κυρίως σε περιπτώσεις στις οποίες η φυσική επικοινωνία είναι σχετικά δύσκολη (με χαρακτηριστικό παράδειγμα την επικοινωνία κόμβων που είναι εγκατεστημένοι σε δύσβατες περιοχές). Μια αντιπροσωπευτική εφαρμογή της επικοινωνίας κόμβων δια της χρήσης μικροκυμάτων είναι η περίπτωση επικοινωνίας από σημείο σε σημείο με τα δύο σημεία να είναι σταθερά ή να μεταβάλλεται το ένα σε σχέση με το άλλο. Τέλος είναι σημαντικό να σημειωθεί ότι λόγω των φυσικών ιδιοτήτων που χαρακτηρίζουν τη μικροκομματική ακτινοβολία, οι κεραιές του πομπού και του δέκτη θα πρέπει να βρίσκονται σε συνεχή οπτική επαφή.

Τα ασύρματα δίκτυα ανοικτής ακρόασης χρησιμοποιούν συνδέσεις εκπομπής και μπορούν να υλοποιηθούν χρησιμοποιώντας τρία βασικά σχήματα τοπολογιών. Στην πρώτη από αυτές τις τοπολογίες που είναι και η πιο παλιά, χρησιμοποιείται ένας κεντρικός κόμβος επικοινωνίας που είναι γνωστός ως σταθμός βάσης. Αυτός ο κόμβος συνδέεται με ένα πλήθος τερματικών σταθμών που βρίσκονται κατανεμημένοι σε μικρή περιοχή γύρω από αυτόν, δια της χρήσης ραδιοκυμάτων χαμηλής

συχνότητας. Επεκτείνοντας την τοπολογία αυτή σε μια πολύ μεγαλύτερη γεωγραφική περιοχή, μπορούμε να ομαδοποιήσουμε τους τερματικούς σταθμούς σε κυψέλες, κάθε μια εκ των οποίων, διαθέτει το δικό της σταθμό βάσης. Όλοι αυτοί οι σταθμοί βάσης συνδέονται μεταξύ τους δια μέσου ενός ενσύρματου δικτύου, προκειμένου τελικά να γίνει σωστός καταμερισμός της χωρητικότητας του δικτύου, σε όλους τους χρήστες που συνδέονται σε αυτό. Η μετάδοση της πληροφορίας κρατείται σε χαμηλά επίπεδα ισχύος έτσι ώστε να ελαχιστοποιείται η διακίνηση σε γειτονικές κυψέλες και να είναι δυνατή η επαναχρησιμοποίηση της ίδιας ζώνης συχνοτήτων από διαφορετικές κυψέλες, οι οποίες δεν είναι γειτονικές μεταξύ τους.

6.2.1 Τοπολογίες ασύρματης μετάδοσης

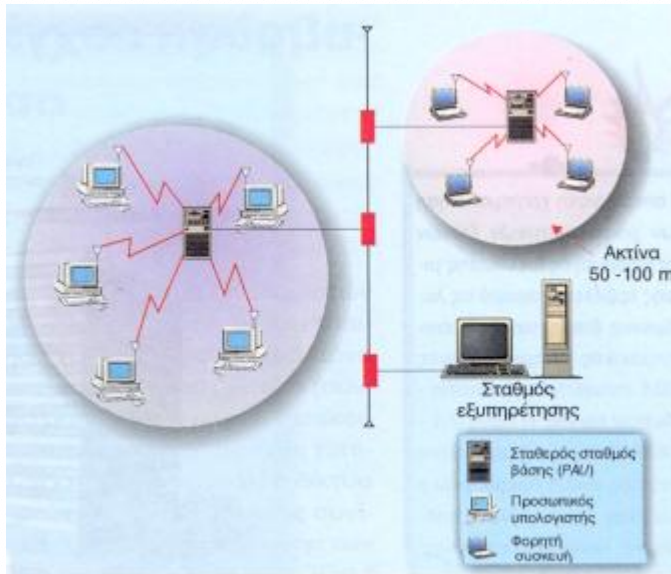
Τα ασύρματα δίκτυα ανοικτής ακρόασης χρησιμοποιούν συνδέσεις εκπομπής και μπορούν να υλοποιηθούν χρησιμοποιώντας τρία βασικά σχήματα τοπολογιών. Στην πρώτη από αυτές τις τοπολογίες που είναι και η πιο παλιά, χρησιμοποιείται ένας κεντρικός κόμβος επικοινωνίας που είναι γνωστός ως σταθμός βάσης. Αυτός ο κόμβος συνδέεται με ένα πλήθος τερματικών σταθμών που βρίσκονται κατανεμημένοι σε μικρή περιοχή γύρω από αυτόν, δια της χρήσης ραδιοκυμάτων χαμηλής συχνότητας. Επεκτείνοντας την τοπολογία αυτή σε μια πολύ μεγαλύτερη γεωγραφική περιοχή, μπορούμε να ομαδοποιήσουμε τους τερματικούς σταθμούς σε κυψέλες, κάθε μια εκ των οποίων, διαθέτει το δικό της σταθμό βάσης. Όλοι αυτοί οι σταθμοί βάσης συνδέονται μεταξύ τους δια μέσου ενός ενσύρματου δικτύου, προκειμένου τελικά να γίνει σωστός καταμερισμός της χωρητικότητας του δικτύου, σε όλους τους χρήστες που συνδέονται σε αυτό. Η μετάδοση της πληροφορίας κρατείται σε χαμηλά επίπεδα ισχύος έτσι ώστε να ελαχιστοποιείται η διακίνηση σε γειτονικές κυψέλες και να είναι δυνατή η επαναχρησιμοποίηση της ίδιας ζώνης συχνοτήτων από διαφορετικές κυψέλες, οι οποίες δεν είναι γειτονικές μεταξύ τους.



Σχήμα 4: Τοπολογία ασυρμάτων δικτύων

Το δεύτερο είδος τοπολογίας ασύρματων τοπικών δικτύων, περιλαμβάνει ένα πλήθος κατανεμημένων τερματικών διατάξεων (Portable Devices, PD), στις οποίες, οι χρήστες του δικτύου, συνδέονται, δια μέσου κατάλληλα σχεδιασμένων μονάδων πρόσβασης (Portable Access Unit, PAU). Οι ίδιες οι τερματικές διατάξεις, συνδέονται

σε ένα κεντρικό σταθμό βάσης, δια μέσου ενσύρματης γραμμής επικοινωνίας. Οι αποστάσεις των τερματικών διατάξεων από το σταθμό βάσης, εξαρτώνται από την ισχύ του σταθμού, το τυπικό εύρος του οποίου κυμαίνεται από 50 έως 100 μέτρα



Σχήμα 5: Δεύτερο είδος τοπολογίας ασυρμάτου δικτύου

Τέλος, η τρίτη περίπτωση αφορά την άμεση ασύρματη σύνδεση κάποιων τερματικών διατάξεων που βρίσκονται εγκατεστημένες σε ένα μικρό χώρο, όπως είναι ένας χώρος συνεδρίων και συσκευέσεων ή ένα αεροδρόμιο.

7. BLOCK INTERLEAVER

Για την επίτευξη διαφορεικής λήψης (diversity) χρησιμοποιείται διαπλέκτης (interleaver). Το interleaving στοχεύει στο να διανείμει τα μεταδιδόμενα bit σε χρόνο ή και συχνότητα για να επιτύχει την επιθυμητή διανομή εσφαλμένων bit μετά την αναδιαμόρφωση. Αυτό που αποτελεί μια επιθυμητή διανομή σφάλματος εξαρτάται από τον κώδικα FEC που χρησιμοποιείται. Το ποιο είδος interleaving απαιτείται

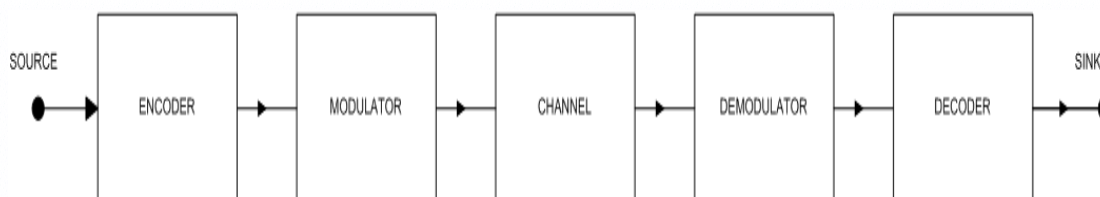
εξαρτάται από τα χαρακτηριστικά των καναλιών. Εάν το σύστημα λειτουργεί σε ένα καθαρά AWGN (Additive Wave Noise) περιβάλλον δεν απαιτείται interleaving, επειδή η διανομή σφάλματος δεν μπορεί να αλλάξει από επανεντοπισμό των bits. Το interleaving ουσιαστικά αφορά ένα στάδιο όπου τα ψηφία παραλλάσσονται με έναν καθορισμένο τρόπο. Η παραλλαγή αυτή εκτελείται από έναν block interleaver με μέγεθος που αντιστοιχεί στον αριθμό των bits μέσα σε ένα σύμβολο OFDM σε δυο στάδια.

Το block interleaving λειτουργεί σε ένα block από bits κάθε φορά. Ο αριθμός bits στο block καλείται βάθος interleaving (interleaving depth), και καθορίζει την καθυστέρηση που εισάγει το interleaving. Ένα block interleaving μπορεί να περιγραφεί ως μήτρα στην οποία τα δεδομένα γράφονται στις στήλες και διαβάζονται στις σειρές ή και αντίστροφα. Ο block interleaving είναι απλός στο να υλοποιηθεί χρησιμοποιώντας μνήμη τυχαίας πρόσβασης (RAM) στα ψηφιακά κυκλώματα. Στο πρώτο στάδιο διαδοχικά ψηφία παραλλάσσονται ώστε να αντιστοιχούν σε μη διαδοχικά φέροντα μέσα στο OFDM σύμβολο, ενώ στο δεύτερο στάδιο επιτυγχάνεται η αντιστοίχιση διαδοχικών ψηφίων σε λιγότερο και περισσότερο αξιόπιστα ψηφία πάνω στον αστερισμό του σχήματος διαμόρφωσης, ώστε να αποφεύγονται επιμήκεις ακολουθίες αναξιόπιστων συμβόλων. Το interleaving εισάγει αναγκαστικά καθυστέρηση στο σύστημα επειδή τα bits δεν λαμβάνονται στην ίδια σειρά όπως τα μεταδίδει η πηγή της πληροφορίας. Ολόκληρο το επικοινωνιακό σύστημα συνήθως υπαγορεύει κάποια μέγιστη καθυστέρηση που το σύστημα συνήθως μπορεί να ανεχτεί περιορίζοντας ως εκ τούτου το μέγεθος interleaving που μπορεί να χρησιμοποιηθεί. Όλα τα κωδικοποιημένα bits δεδομένων θα γίνουν interleaved από μια ομάδα δεδομένων interleaver με ένα μέγεθος ομάδας δεδομένων που αντιστοιχεί στον αριθμό δυαδικών ψηφίων σε ένα ενιαίο OFDM ΣΥΜΒΟΛΟ. Το interlaver καθορίζεται από μια μετατροπή βημάτων. Το πρώτο εξασφαλίζει ότι τα παρακείμενα κωδικοποιημένα bits χαρτογραφούνται εναλλακτικά σε μη-παρακείμενα υπό-φέροντα. Η δεύτερη μετατροπή εξασφαλίζει ότι τα παρακείμενα κωδικοποιημένα bits χαρτογραφούνται εναλλακτικά πάνω σε λιγότερο και περισσότερο σημαντικά bits του αστερισμού και από αυτό αποφεύγονται μακρές εκτελέσεις από χαμηλής αξιοπιστίας bits.

7.1. Block Κώδικες

Με την ραγδαία αύξηση του πλήθους και της πολυπλοκότητας των τηλεπικοινωνιακών διατάξεων, καθώς και λόγω της ανάγκης μετάδοσης της πληροφορίας σε μεγάλες αποστάσεις και σε έντονα "θορυβώδες" περιβάλλον, παρουσιάστηκε η ταυτόχρονη ανάγκη για αύξηση της πιθανότητας μετάδοσής της. Ακόμη, η εγγενής κρισιμότητα της φύσης της πληροφορίας (π.χ. ιατρικό σήμα) απαίτησε την χρησιμοποίηση είτε υπηρεσιών οι οποίες στερούνται λαθών είτε κάποιων ειδών αλγορίθμων, οι οποίοι εντοπίζουν τα λάθη ή ακόμη καλύτερα έχουν την δυνατότητα να τα διορθώσουν. Οι τελευταίοι, αποτελούν βέβαια και την καλύτερη λύση, αφού συνδυάζουν τον εντοπισμό με την διόρθωση λαθών, η επιλογή, όμως, του αλγορίθμου που θα χρησιμοποιηθεί είναι ένας συμβιβασμός ανάμεσα στην πολυπλοκότητα του, και συνεπώς και στην απαίτησή του σε χρονική διάρκεια, και στην αποτελεσματικότητά του.

Το block διάγραμμα, ενός στοιχειώδους ψηφιακού συστήματος επικοινωνίας, φαίνεται στην παρακάτω εικόνα. Η πηγή πληροφορίας παρέχει δυαδικά ψηφία. Ο κωδικοποιητής μετατρέπει αυτά τα ψηφία και στη συνέχεια ο διαμορφωτής τα μετασχηματίζει σε σήματα τα οποία είναι ικανά να μεταδοθούν στο κανάλι. Εισερχόμενα στο κανάλι τα σήματα αυτά διαταράσσονται από το θόρυβο και στη συνέχεια εισέρχονται στον αποδιαμορφωτή, αναδιαμορφώνονται και περνούν στον αποκωδικοποιητή, ο οποίος και παίρνει την απόφαση σχετικά με το ποίο σήμα στάλθηκε και το προωθεί στην έξοδό του.



Σχήμα 6: Block διάγραμμα ενός στοιχειώδους συστήματος επικοινωνίας

Οι block κώδικες ομαδοποιούν τη συνεχόμενη ακολουθία των bits της πληροφορίας, τα οποία εισέρχονται στον κωδικοποιητή, σε κομμάτια ή block k συμβόλων. Στη συνέχεια, λειτουργούν, ανάλογα με τον κώδικα, πάνω σε αυτά τα block ξεχωριστά. Σε κάθε πιθανό block πληροφορίας k συμβόλων αντιστοιχίζεται ένα block το οποίο αποτελείται από n κώδικα σύμβολα, όπου $n > k$. Το αποτέλεσμα, το οποίο από εδώ και στο εξής θα ονομάζεται κωδική λέξη, μεταβάλλεται από τον θόρυβο και αποκωδικοποιείται στον δέκτη ανεξάρτητα από όλες τις άλλες κωδικές λέξεις. Το n ονομάζεται μήκος του κώδικα ή αλλιώς block length .

Όπως αναφέραμε και πιο πάνω, οι block κώδικες ομαδοποιούν τη συνεχόμενη ακολουθία των bits της πληροφορίας, τα οποία εισέρχονται στον κωδικοποιητή, σε block k συμβόλων. Block κώδικας, ονομάζεται ένα σύνολο από M ακολουθίες συμβόλων μήκους n . Έστω q , ο αριθμός των διακριτών συμβόλων πληροφορίας(στην περίπτωση της δυαδικής μετάδοσης πληροφορίας $q=2$). Οι ακολουθίες αυτές, συμβόλων μήκους n , q διακριτών συμβόλων, ονομάζονται κώδικες λέξεις του κώδικα. Ο αριθμός των κωδικών λέξεων είναι μια δύναμη του q , είναι δηλαδή $M=q^n$.

Στον δέκτη, ακολούθως, λαμβάνεται μια απόφαση, με βάση την πληροφορία από το ληφθέν n διαστατό πολυώνυμο, σχετικά με την κωδική λέξη που μεταδόθηκε. Αυτή η απόφαση είναι μια στατιστική απόφαση, είναι μια απόφαση που από την φύση της χρησιμοποιεί ως βάση την πληροφορία που είναι διαθέσιμη και κατά συνέπεια δεν μπορεί να είναι αλάνθαστη. Με την χρήση του κατάλληλου κώδικα, η πιθανότητα μιας λανθασμένης απόφασης είναι συνήθως πολύ μικρότερη από την πιθανότητα που υπήρχε αρχικά, στα σύμβολα εισόδου στο κανάλι, να αναπαραχθούν χωρίς λάθος στην έξοδο του καναλιού. Η διαδικασία απόφασης, μπορεί να οριστεί μαθηματικά από έναν πίνακα αποκωδικοποίησης, όπως τον πίνακα που βλέπουμε πιο κάτω. Οι κωδικές λέξεις αποτελούν την πρώτη σειρά του πίνακα. Όταν λαμβάνεται μια κωδική λέξη, είναι λογικό να θεωρούμε ότι η ίδια κωδική λέξη είναι και αυτή που στάλθηκε. Η απόφαση του δέκτη για άλλες πιθανές ληφθείσες λέξεις περιγράφεται παραθέτοντας κάτω από κάθε μια κωδική λέξη, τις ληφθείσες λέξεις οι οποίες θα αποκωδικοποιηθούν σε αυτήν. Έτσι κάθε μια από τις πιθανές να ληφθούν λέξεις, εμφανίζεται μόνο μια φορά στον πίνακα αποκωδικοποίησης. Για

παράδειγμα, ας υποθέσουμε ότι υπάρχουν τέσσερα πιθανά μηνύματα a, b, c και d και ότι το μήνυμα μεταδίδεται χρησιμοποιώντας έναν δυαδικό block κώδικα με μήκος πέντε. Στη συνέχεια, τέσσερις κωδικές λέξεις πρέπει να επιλεγούν, έστω 11000 για το a, 00110 για το b, 10011 για το c και 01101 για το d. Η απόφαση του δέκτη πρέπει να περιγραφεί για κάθε μια από τις $2^5=32$ πιθανές ληφθείσες λέξεις. Ένα παράδειγμα για το πώς μπορεί να γίνει αυτό φαίνεται στον παρακάτω πίνακα.

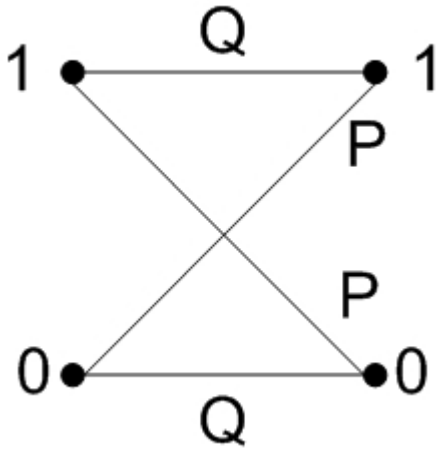
Κωδικές Λέξεις	<u>1 1 0 0 0 0 0 1 1 0 1 0 0 1 1 0 1 1 0 1</u>
	1 1 0 0 1 0 0 1 1 1 1 0 0 1 0 0 1 1 0 0
Άλλες	1 1 0 1 0 0 0 1 0 0 1 0 0 0 1 0 1 1 1 1
Ληφθήσες	1 1 1 0 0 0 0 0 1 0 1 0 1 1 1 0 1 0 0 1
Λέξεις	1 0 0 0 0 0 1 1 1 0 1 1 0 1 1 0 0 1 0 1
	<u>0 1 0 0 0 1 0 1 1 0 0 0 0 1 1 1 1 1 0 1</u>
	1 1 1 1 0 0 0 0 0 0 0 1 0 1 1 1 0 1 0 1
	0 1 0 1 0 1 0 1 0 0 1 1 1 1 1 0 0 0 0 1

Σχήμα 7: Πίνακας αποκωδικοποίησης για έναν δυαδικό κώδικα με $q=k=2$ και $n=5$

Οι κανόνες κωδικοποίησης και αποκωδικοποίησης, οι οποίοι φαίνονται στον πίνακα, αποκωδικοποιούν σωστά μια λέξη η οποία δεν θα έχει περισσότερα από ένα λάθη, δηλαδή περισσότερα από ένα αλλαγμένα σύμβολα, μια και κάθε μια από τις πέντε λέξεις οι οποίες θα είχαν ως αποτέλεσμα ένα μοναδικό λάθος βρίσκονται κάτω από κάθε μια κωδική λέξη (ανάμεσα στην συνεχόμενη και την διακεκομμένη γραμμή). Όμως, δεν αποκωδικοποιούνται σωστά όλα τα μοτίβα λαθών. Για παράδειγμα, εάν μεταδοθεί το 11000 και συμβούν δύο λάθη οδηγώντας έστω στο 11110 η λέξη θα αποκωδικοποιηθεί σωστά γιατί το 11110 είναι στην στήλη κάτω από το 11000 στον πίνακα. Όμως, αν σε άλλη περίπτωση τα δύο λάθη έχουν σαν αποτέλεσμα να λάβουμε την 11011, θα αποκωδικοποιηθεί λανθασμένα σε 10011, επειδή το 11011 είναι στην στήλη κάτω από το 10011.

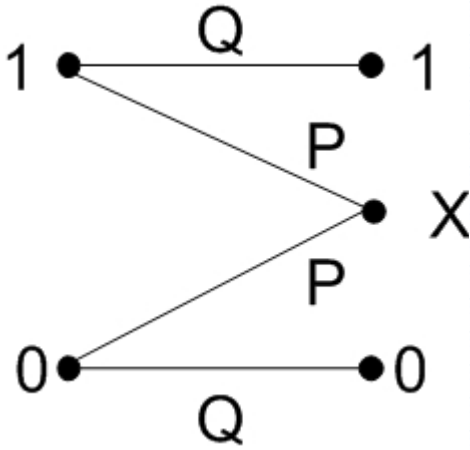
Σε μερικές περιπτώσεις, είναι δυνατό ο αποκωδικοποιητής να είναι σε θέση να δηλώσει απλά ότι υπάρχει λάθος στην κωδική λέξη που λήφθηκε χωρίς όμως να μπορεί να υποδείξει ποια ήταν η κωδική λέξη που εστάλη. Αυτό μπορεί να πάρει την μορφή ενός συστήματος εντοπισμού λαθών, στο οποίο ο αποκωδικοποιητής δίνει το σήμα ότι υπάρχει λάθος αλλά δεν πράττει τίποτε πιο πέρα εκτός και αν ληφθεί μια κωδική λέξη. Επιπρόσθετα, όπως αναφέρθηκε και προηγουμένως, μπορεί να συνδυαστεί ο εντοπισμός λάθους με την διόρθωση σφαλμάτων. Για παράδειγμα, για τον κώδικα ο οποίος φαίνεται στον πίνακα, κάθε ληφθείσα λέξη πάνω από την διακεκομμένη γραμμή μπορεί να αποκωδικοποιηθεί στην κωδική λέξη στην κορυφή της στήλης, αλλά ο αποκωδικοποιητής δεν θα μπορέσει να εντοπίσει λάθη για τις λέξεις που λαμβάνονται κάτω από αυτή τη γραμμή. Αυτό αντιστοιχεί σε διόρθωση μοναδικού λάθους με εντοπισμό μερικών συνδυασμών δύο ή περισσότερων λαθών.

Θέλοντας να προβλέψουμε την απόδοση ενός κώδικα, είναι απαραίτητο να έχουμε ακριβείς πληροφορίες σχετικά με το κανάλι. Αν και τα περισσότερα πραγματικά τηλεπικοινωνιακά κανάλια δεν μπορούν να παρασταθούν με ακρίβεια από το δυαδικό συμμετρικό κανάλι (Binary Symmetric Channel, BSC) το οποίο φαίνεται στην εικόνα , αυτή είναι η θεώρηση του καναλιού που χρησιμοποιείται ευρέως. Για αυτό το δυαδικό συμμετρικό κανάλι, η πιθανότητα να ληφθεί το ίδιο σύμβολο με αυτό που στάλθηκε είναι Q . Υποτίθεται ότι $Q > P$ και ότι το κάθε σύμβολο είναι ανεξάρτητο από όλα τα άλλα (ένα τέτοιο κανάλι λέγεται κανάλι δίχως μνήμη). Εννοείται ότι ένα τέτοιο κανάλι συμπεριλαμβάνει και τον διαμορφωτή και τον αποδιαμορφωτή ενός τυπικού επικοινωνιακού συστήματος το οποίο είδαμε προηγουμένως.



Σχήμα 8: Το δυαδικό συμμετρικό κανάλι (BSC)

Ένα άλλο ιδανικό κανάλι, το οποίο έχει μελετηθεί ευρέως, είναι το δυαδικό erasure κανάλι το οποίο φαίνεται στην παρακάτω εικόνα . Για αυτό το κανάλι, η πιθανότητα να ληφθεί το ίδιο δυαδικό ψηφίο το οποίο στάλθηκε είναι Q . Η πιθανότητα να σβηστεί ένα σύμβολο που μεταδόθηκε είναι $P=1-Q$. (Το σβήσιμο συμβολίζεται με το X). Τα δυαδικά σύμβολα θεωρούνται ότι επηρεάζονται ανεξάρτητα. Σημειώστε ότι με αυτό το κανάλι, οι τοποθεσίες των αλλαγμένων συμβόλων είναι γνωστές, και αυτό το γεγονός κάνει τις διορθώσεις των σβησιμάτων πιο εύκολες από τις διορθώσεις των λαθών. Γενικεύσεις αυτού του erasure καναλιού περιλαμβάνουν ένα μη δυαδικό erasure κανάλι και ένα κανάλι και με σβησίματα και με λάθη. Το erasure κανάλι είναι μια εξιδανίκευση ενός συστήματος στο οποίο ο αποδιαμορφωτής της προηγούμενης εικόνας είναι σχεδιασμένος ώστε να παραδίδει ένα σύμβολο σβησίματος (X) παρά ένα 1 ή 0 σε περιπτώσεις αμφισβήτησης.



Σχήμα 9: Το δυαδικό erasure κανάλι

Τώρα, ας θεωρήσουμε ένα δυαδικό συμμετρικό κανάλι και ότι μεταδίδεται σε αυτό μια συγκεκριμένη δυαδική κωδική λέξη. Η πιθανότητα ώστε να μην συμβεί κάποιο σφάλμα είναι Q^n . Η πιθανότητα να συμβεί ένα λάθος σε μια συγκεκριμένη θέση είναι PQ^{n-1} . Η πιθανότητα μιας συγκεκριμένης λέξης που λήφθηκε να διαφέρει από την λέξη που μεταδόθηκε σε i θέσεις είναι $P^i Q^{n-i}$. Μια και $Q > P$, το ληφθέν block έχει τις περισσότερες πιθανότητες να μην έχει λάθη. Οποιαδήποτε ληφθείσα λέξη με ένα λάθος είναι πολύ πιο πιθανή από μια λέξη η οποία θα έχει δύο ή περισσότερα λάθη, και ούτω καθεξής. Σε αυτή την περίπτωση, με την υπόθεση ότι όλες οι κωδικές λέξεις είναι εξίσου πιθανό να μεταδοθούν, η καλύτερη απόφαση στον δέκτη θα είναι πάντα να αποκωδικοποιεί την κάθε λέξη που λαμβάνει στην κωδική λέξη η οποία διαφέρει στις λιγότερες θέσεις με την ληφθείσα. Αυτή η αποκωδικοποίηση μέγιστης πιθανοφάνειας, όπως αυτή καλείται, μπορεί να γενικευτεί σε μη δυαδικό κανάλι χωρίς μνήμη. Με την προϋπόθεση ότι έχουμε ένα δυαδικό συμμετρικό κανάλι, η πιθανότητα της σωστής αποκωδικοποίησης μπορεί να υπολογιστεί με τον ακόλουθο τρόπο για τον κώδικα του πίνακα . Έστω ότι στάλθηκε η λέξη 11000. Θα αποκωδικοποιηθεί σωστά αν ληφθεί οποιαδήποτε λέξη στην στήλη της. Μια από αυτές τις λέξεις δεν διαφέρει σε καμία θέση, πέντε από αυτές διαφέρουν σε μια θέση και δύο από αυτές διαφέρουν σε δύο θέσεις. Η πιθανότητα σωστής αποκωδικοποίησης είναι:

$$P(\text{σωστής αποκωδικοποίησης})=1P0Q5+5P1Q4+2P2Q3$$

Παρόμοιοι υπολογισμοί μπορούν να γίνουν και για τις άλλες κωδικές λέξεις.

Εάν αυτός ο κώδικας χρησιμοποιείται μόνο για εντοπισμό σφάλματος, η πιθανότητα σωστής λήψης είναι Q^5 . Η πιθανότητα ενός μη αντιληπτού λάθους, στην περίπτωση που έχει μεταδοθεί το 11000 είναι η πιθανότητα να ληφθεί μια άλλη κωδική λέξη όταν έχει αποσταλεί η λέξη 11000. Μια και μια κωδική λέξη διαφέρει σε τέσσερις θέσεις και οι άλλες δύο σε τρεις θέσεις η κάθε μια,

$$P(\text{μη αντιληπτό λάθος})=1P4Q+2P3Q2$$

Η έννοια της απόστασης Hamming είναι χρήσιμη στην μελέτη της ικανότητας διόρθωσης σφαλμάτων των κωδικών. Η απόσταση Hamming, ανάμεσα σε δύο λέξεις, ορίζεται ως ο αριθμός των θέσεων στις οποίες διαφέρουν οι δύο λέξεις. Έτσι, ένα μοναδικό σφάλμα αντιστοιχεί σε απόσταση Hamming ίση με 1 ανάμεσα στην λέξη που στάλθηκε και στην λέξη που λήφθηκε. Αν ένας κώδικας χρησιμοποιείται μόνο για εντοπισμό λαθών και πρέπει να εντοπίζει όλα τα μοτίβα $d-1$ ή λιγότερων λαθών, είναι απαραίτητο και επαρκεί η ελάχιστη απόσταση Hamming ανάμεσα στις κωδικές λέξεις να είναι d . Γιατί, εάν η ελάχιστη απόσταση είναι d , κανένα μοτίβο με $d-1$ λάθη δεν μπορεί να αλλάξει μια κωδική λέξη σε μια άλλη, ενώ εάν η ελάχιστη απόσταση Hamming είναι $d-1$ ή μικρότερη, υπάρχει κάποιο ζευγάρι λέξεων με απόσταση μικρότερη από d μεταξύ τους και υπάρχει ένα μοτίβο με λιγότερα από d λάθη το οποίο θα μπορεί να οδηγήσει από την μια στην άλλη.

Παρομοίως, είναι πιθανό να αποκωδικοποιήσουμε με τέτοιο τρόπο ώστε να μπορούμε να διορθώσουμε όλα τα μοτίβα με t ή λιγότερα λάθη αν και μόνο αν η ελάχιστη απόσταση ανάμεσα στις κωδικές λέξεις είναι τουλάχιστο $2t+1$. Τότε οποιαδήποτε ληφθείσα λέξη, με $t' \leq t$ λάθη, διαφέρει από την κωδική λέξη που μεταδόθηκε σε t' σύμβολα, αλλά από οποιαδήποτε άλλη κωδική λέξη σε τουλάχιστο $2t+1-t' > t'$ σύμβολα. Στον αντίποδα, εάν η ελάχιστη απόσταση είναι μικρότερη, υπάρχει τουλάχιστον μια περίπτωση όπου ένα σφάλμα μήκους t , έχει ως αποτέλεσμα μια ληφθείσα λέξη τουλάχιστο τόσο κοντά σε μια κωδική λέξη όσο και η κωδική λέξη που μεταδόθηκε. Τέλος, μπορεί ναδειχθεί ότι είναι πιθανό να αποκωδικοποιήσουμε με έναν τέτοιο τρόπο ώστε να διορθώσουμε όλους τους

συνδυασμούς από t ή λιγότερα λάθη και ταυτόχρονα να εντοπίσουμε όλους τους συνδυασμούς από d ή λιγότερα λάθη ($d \geq t$) αν και μόνο αν η ελάχιστη απόσταση ανάμεσα στις κωδικές λέξεις είναι $t+d+1$.

Έκτος από την εφαρμογή τους σε τηλεπικοινωνιακά συστήματα, οι block κώδικες βρίσκουν εφαρμογή και σε αρκετές άλλες επιστημονικές περιοχές. Αποτελούν την βάση για τον πίνακα μεταγωγής καταμερισμού φορτίου, ο οποίος δεν είναι απλώς πιο αποδοτικός από τα συμβατικά συστήματα διευθυνσιοδότησης μνήμης, αλλά κάνει και κάποια αυτόματη διόρθωση σε περιπτώσεις βλαβών των εξαρτημάτων. Έχουν, επίσης, προταθεί για χρήση σε συστήματα ανάκτησης εγγράφων, για συμπίεση δεδομένων και κατασκευή υπολογιστών ανθεκτικών σε σφάλματα.

7.1.1. Block Κώδικες και Πιθανότητες Σφαλμάτων

Η δυαδική πηγή θεωρούμε ότι παράγει μια ακολουθία συμβόλων με ρυθμό R σύμβολα/s. Τα σύμβολα αυτά ομαδοποιούνται σε block των k συμβόλων. Σε κάθε block k συμβόλων προσθέτουμε $n - k$ πλεονάζοντα σύμβολα για να παραχθεί μια κωδική λέξη μήκους n συμβόλων. Τα $n-k$ πλεονάζοντα σύμβολα ονομάζονται σύμβολα ισοτιμίας. Το αποτέλεσμα αναφέρεται ως κώδικας block (n, k) . Εφόσον κάθε κωδική λέξη μεταφέρει k bit πληροφορίας, ο ρυθμός πληροφορίας στην έξοδο του κωδικοποιητή θα είναι k/n bit ανά σύμβολο. Έτσι το k/n αναφέρεται ως ο *ρυθμός του κώδικα*.

Υπάρχει το πρόβλημα όπου λόγω του αποσβενύμενου καναλιού, όλοι οι subcarriers θα φτάσουν στο δέκτη με διαφορετικό πλάτος. Τότε, παρότι οι περισσότεροι θα φτάνουν χωρίς πρόβλημα, θα υπάρχουν μερικοί με πολύ χαμηλό πλάτος οι οποίοι θα καταστρέφουν το σήμα φέρνοντας το bit error ratio (BER) κοντά στο 0.5. Για την αποφυγή της κυριαρχίας του καναλιού από τα πολύ ασθενή σύμβολα, χρησιμοποιούμε κωδικοποίηση εμπρόσθιας διόρθωσης σφάλματος (forward error correction coding) Τότε τα λάθη των ασθενών subcarriers θα διορθώνονται και το κανάλι θα εξαρτάται από το μέσο όρο των subcarriers, αντί μόνο από τους ασθενείς. Υπάρχουν δύο είδη

κωδικοποίησης, οι block codes και οι convolutional codes. Αν όλες οι μεταδιδόμενες λέξεις είναι εξίσου πιθανές, και το κανάλι δεν έχει μνήμη, τότε το παραπάνω επιτυγχάνεται επιλέγοντας ως πιο πιθανή κωδική λέξη τη κωδική λέξη με τη μικρότερη απόσταση Hamming από την λαμβανόμενη κωδική λέξη. Η απόσταση Hamming μεταξύ των ακολουθιών Y και Z ορίζεται ως το βάρος (το πλήθος των μονάδων) στο άθροισμα Mod-2 των Y και Z . Η άθροιση Mod-2 συμβολίζεται με το \oplus και έχει την εξής ιδιότητα:

$$b_1 \oplus b_2 = \int_0^1 -1$$

$$b_1 = b_2$$

$$b_1 \neq b_2$$

όπου τα b_1 και b_2 είναι αυθαίρετα δυαδικά ψηφία. Αφού τα Y και Z είναι διανύσματα το άθροισμα Mod-2 λαμβάνεται ανά συνιστώσα. Σε συνήθεις εφαρμογές, η κωδικοποίηση χρησιμοποιείται σε περιβάλλοντα όπου η εκπεμπόμενη ισχύς είναι περιορισμένη. Επίσης, οι κωδικές λέξεις n συμβόλων πρέπει να εκπεμφθούν στο ίδιο χρονικό διάστημα που παράγονται τα k σύμβολα πληροφορίας της πηγής. Αν οι συνθήκες αυτές δεν ισχύουν, τότε υπάρχει μικρή ανάγκη για κωδικοποίηση. Η αύξηση της ισχύος εκπομπής βελτιώνει, σχεδόν πάντα, την απόδοση του συστήματος σε περιβάλλον περιορισμένου θορύβου. Ομοίως, αν η ακολουθία δεδομένων μπορεί να αποθηκευτεί σε έναν καταχωρητή και να διαβασθεί με αργότερο ρυθμό, τότε η απόδοση του συστήματος αυξάνει επειδή αυξάνει η ενέργεια ανά σύμβολο.

Ας θεωρήσουμε ότι η ισχύς του πομπού είναι S watt και τα k σύμβολα εξέρχονται από τη πηγή σε συνολικό χρόνο T δευτερόλεπτων. Έτσι η διαθέσιμη ενέργεια για κάθε κωδική λέξη είναι $w = ST$. Η λαμβανόμενη ενέργεια ανά σύμβολο είναι ST/k χωρίς κωδικοποίηση. Με κωδικοποίηση, η ενέργεια κατανέμεται στη κωδική λέξη n συμβόλων, οπότε η λαμβανόμενη ενέργεια ανά σύμβολο, με κωδικοποίηση, είναι ST/n . Εφόσον $n > k$, η ενέργεια ανά σύμβολο μειώνεται με τη κωδικοποίηση, επομένως η πιθανότητα σφάλματος συμβόλου με κωδικοποίηση είναι μεγαλύτερη από ότι χωρίς κωδικοποίηση. Αν ο κώδικας σχεδιασθεί σωστά, ο πλεονασμός που εισάγεται με τα $n - k$ σύμβολα ισοτιμίας επιτρέπει επαρκή δυνατότητα διόρθωσης σφάλματος έτσι ώστε το σύστημα να έχει μια ολική βελτίωση της απόδοσης.

Ένα μέτρο της αποτελεσματικότητας της κωδικοποίησης αποκτάται με τη σύγκριση της πιθανότητας σφάλματος λέξης με κωδικοποίηση $wec P$ με τη σύγκριση της πιθανότητας σφάλματος λέξης χωρίς κωδικοποίηση $wcu P$. Οι πιθανότητες σφάλματος συμβόλου με και χωρίς κωδικοποίηση είναι $c q$ και $w q$, αντίστοιχα. Η πιθανότητα σφάλματος λέξης χωρίς κωδικοποίηση είναι 1 μείον τη πιθανότητα όλα τα σύμβολα πληροφορίας να ληφθούν σωστά. Αυτό δίνει: $Pwcu = 1(1 - qu)^k$ Η πιθανότητα σφάλματος λέξης με κωδικοποίηση είναι κάπως πιο πολύπλοκη. Ας θεωρήσουμε ότι ο κώδικας έχει ελάχιστη απόσταση $\min d$ έτσι ώστε e σφάλματα μπορούν να διορθωθούν, όπου:

$$e = \frac{1}{2}(d \min - 1)$$

Αν περισσότερα από e σφάλματα σε μια κωδική λέξη οδηγούν πάντα σε σφάλμα στη λέξη, τότε η πιθανότητα σφάλματος λέξης είναι:

$$Pwcu \leq \sum_{i=e+1}^n \frac{n}{i} qc(1 - qc)^{n-1}$$

όπου

$$\frac{n}{i} = \frac{n!}{i!(n-i)!} = \frac{n(n-1)\dots\dots(n-i+1)}{i!}$$

δηλώνει τον αριθμό όλων των συνδυασμών n αντικειμένων από τα οποία λαμβάνονται i τη φορά. Δηλαδή αναπαριστάνει το πλήθος όλων πιθανών i σφαλμάτων σε κωδική λέξη n συμβόλων. Το $c q$ δηλώνει την πιθανότητα σφάλματος συμβόλου με κωδικοποίηση. Οι κώδικες για τους οποίους ισχύει η ισότητα λέγονται *τέλειοι κώδικες*. Οι μόνοι τέλειοι κώδικες είναι ο κώδικας *Hamming* που διορθώνει ένα σφάλμα και ο κώδικας *Golay*. Για άλλους κώδικες υπάρχουν συγκεκριμένες κωδικές λέξεις για τις οποίες μπορούμε να έχουμε σωστή αποκωδικοποίηση με περισσότερα από e σφάλματα. Για τους κώδικες αυτούς η σχέση αποτελεί ένα χρήσιμο άνω όριο.

7.1.2. Block Codes σε αντιστοιχία με απόσταση Hamming

Ένας block code κωδικοποιεί ένα μπλοκ από k σύμβολα εισόδου σε n σύμβολα εξόδου, όπου n μεγαλύτερο από το k . Ο σκοπός των επιπλέον $n-k$ συμβόλων είναι η αύξηση της ελάχιστης απόστασης Hamming, δηλαδή ο ελάχιστος αριθμός των διαφορετικών συμβόλων μεταξύ κάθε ζεύγους κωδικοποιημένων λέξεων [9]. Για μια απόσταση d_{\min} , η κωδικοποίηση αυτή μπορεί να σφάλματα όπου t δίνεται από τον τύπο:

$$t \leq \text{floor}\left(\frac{d_{\min}-1}{2}\right)$$

Η ελάχιστη απόσταση Hamming εξαρτάται από τον αριθμό των επιπλέον συμβόλων ως εξής:

$$d_{\min} \leq n - k + 1$$

Μια κατηγορία κωδικοποιήσεων η οποία φτάνει το παραπάνω όριο στην απόσταση Hamming είναι οι Reed-Salomon codes. Λόγω της καλής απόστασης και της δυνατότητας αποτελεσματικής κωδικοποίησης και αποκωδικοποίησης που έχουν, είναι από τους πιο διαδεδομένους αλγορίθμους που χρησιμοποιούνται σε block codes. Καθορίζονται για μπλοκ με σύμβολα που αποτελούνται από m bits ανά σύμβολο, όπου ο αριθμός n των συμβόλων που κωδικοποιούνται σχετίζεται με το m ως: $n = 2^m - 1$

Ο αριθμός των συμβόλων εισόδου τότε θα είναι:

$$k = 2^{m-d_{\min}}$$

Όπως φαίνεται από την σχέση, δεν υπάρχει μεγάλη δυνατότητα τροποποίησης στο μέγεθος της κωδικοποίησης. Παρόλα αυτά, μπορούμε να προσαρμόσουμε την κωδικοποίηση στα δικά μας δεδομένα, αφήνοντας ένα τμήμα της εισόδου ίσο με μηδέν, και

αφαιρώντας τον ίδιο αριθμό bits από την έξοδο. Επιπλέον, γίνεται να αυξήσουμε το μήκος της κωδικοποίησης σε μία δύναμη του 2, αν προσθέσουμε και ένα parity bit.

Σύμφωνα με τις σχέσεις, η Reed Salomon κωδικοποίηση μπορεί να διορθώσει μέχρι $\text{floor}((n-k)/2)$ σύμβολα που περιέχουν σφάλματα. Επειδή κάθε σύμβολο περιέχει m bits, μπορούν να διορθωθούν έως $m \cdot \text{floor}((n-k)/2)$ bits. Αυτός ο αριθμός είναι ο μέγιστος αριθμός σφαλμάτων που μπορούν να διορθωθούν, καθώς πρέπει να ικανοποιείται παράλληλα και ο μέγιστος αριθμός των συμβόλων που είναι δυνατόν να διορθωθούν. Αυτό το χαρακτηριστικό κάνει την Reed Salomon κωδικοποίηση ιδιαίτερα καλή στην OFDM μετάδοση σε multipath κανάλι (όπως το PLC) καθώς τα σφάλματα σε τέτοια κανάλια συγκεντρώνονται σε περιορισμένους subcarriers που βρίσκονται σε συχνότητες με μεγάλη εξασθένηση.

Στην περίπτωση των μπλοκ κωδίκων, όπου η ακολουθία των *bit* της πηγής πληροφορίας (*source bits*) χωρίζεται σε μπλοκ των k bit, που ονομάζονται *bit δεδομένων* (*data bits* ή *information bits*) ή *bit μηνύματος* (*message bits*). Κάθε μπλοκ παριστάνει ένα από τα $2k$ διακριτά μηνύματα. Ο κωδικοποιητής μετατρέπει κάθε μπλοκ των k bit, σε μεγαλύτερο μπλοκ των n bit, τα οποία ονομάζονται *bit κώδικα* (*code bits*) ή *σύμβολα καναλιού* (*channel symbols*), όπως αναφέρθηκε και πιο πάνω συνιστούν μια κωδικοποιημένη λέξη των n bit. Υπάρχουν επομένως $2n$ δυνατές κωδικοποιημένες λέξεις (*code words*), ενώ ο αριθμός των δυνατών μηνυμάτων είναι $2k$. Κατά συνέπεια υπάρχουν $2n-2k$ δυνατές λέξεις των n bit που δεν συνιστούν δυνατά μηνύματα. Οι $2k$ κωδικοποιημένες λέξεις των n bit αποτελούν το αλφάβητο του κώδικα.

Τα $(n-k)$ bit που προσθέτει ο κωδικοποιητής σε κάθε μπλοκ δεδομένων των k bit, ονομάζονται *πλεονάζοντα bit* (*redundant bits*) ή *bit ισοτιμίας* (*parity bits*) ή *bit ελέγχου* (*check bits*). Τα bit αυτά δεν μεταφέρουν καινούρια πληροφορία. Ένας τέτοιος κώδικας αναφέρεται ως ένας (n, k) γραμμικός κώδικας μπλοκ. Ο λόγος των πλεοναζόντων bit προς τα bit δεδομένων, $(n-k)/k$, ονομάζεται *πλεόνασμα* (*redundancy*) του κώδικα, και ο λόγος των bit δεδομένων προς το συνολικό αριθμό των bit, k/n , ονομάζεται *ρυθμός του κώδικα* (*code rate*). Ο ρυθμός του κώδικα μπορεί να θεωρηθεί ως το κλάσμα ενός bit καναλιού που

μεταφέρει πληροφορία. Για παράδειγμα, σε ένα κώδικα με ρυθμό $1/2$, κάθε bit καναλιού μεταφέρει $1/2$ bit πληροφορίας. Στους κώδικες που θα εξεταστούν στο παρόν κεφάλαιο θεωρείται ότι η κωδικοποιημένη λέξη των n bit μεταδίδεται στον ίδιο χρόνο που θα μεταδιδόταν η (μη κωδικοποιημένη) λέξη των k bit. Συνεπώς, αυτό σημαίνει ότι απαιτείται επιπλέον εύρος ζώνης για την μετάδοση. Για παράδειγμα, για ένα κώδικα με ρυθμό $1/2$ (100% πλεόνασμα) απαιτείται διπλάσιο εύρος ζώνης σε σχέση με την κωδικοποιημένη μορφή. Ωστόσο, για ένα κώδικα με ρυθμό $3/4$ το πλεόνασμα είναι 33% και το εύρος ζώνης αυξάνεται κατά έναν παράγοντα ίσο με $4/3$ μόνο.

7.2 Κωδικοποίηση Πηγής και καναλιού Block Coding

Η ακολουθία εξόδου της πηγής είναι ψηφιακή, οπότε θέλουμε να την αναπαραστήσουμε με όσο λιγότερα bits γίνεται. Απορρίπτουμε λοιπόν την περιττή πληροφορία. Μεγάλο μέρος της πληροφορίας που μεταδίδεται σε ασύρματα δίκτυα είναι φωνή, οπότε θα δώσουμε ιδιαίτερο βάρος σε αυτήν.

Κωδικοποίηση Καναλιού , (block coding) .

Εισάγεται πλεονάζουσα πληροφορία με ελεγχόμενο και συστηματικό τρόπο. Τα bits αυτά δε μεταφέρουν πληροφορία , αλλά δίνουν τη δυνατότητα στον αποκωδικοποιητή να διορθώνει λάθη.

Block κώδικες:

- Block bits πληροφορίας αντιστοιχούνται σε n bits ($n > k$)
- Το μέγεθος πλεονάζουσας πληροφορίας μετράται από το λόγο n/k .

Π.χ. **Hamming**, Hadamard, Golay, Cyclic Codes, BCH, Reed-Solomon

7.2.1. Κωδικοποίηση τμήματος (block coding)

Σε αυτό το είδος κωδικοποίησης ο κωδικοποιητής προσαρτά r πλεονάζοντα bits σε κάθε τμήμα των k bits πληροφορίας. Με αυτόν τον τρόπο σχηματίζονται κωδικές λέξεις μήκους $n = k + r$ bits και για το λόγο αυτό οι αντίστοιχοι κώδικες αναφέρονται ως (n, k) κώδικες.

Το χαρακτηριστικό στοιχείο αυτού του τύπου κωδικοποίησης είναι ότι κάθε τμήμα των k bits πληροφορίας κωδικοποιείται ανεξάρτητα από προηγούμενα τμήματα του ρεύματος των bits της πληροφορίας. Οι χρησιμοποιούμενοι κώδικες ονομάζονται συμπαγείς και η πιο σημαντική τους παράμετρος είναι η ελάχιστη απόσταση d_{\min} , η οποία καθορίζει τη δυνατότητα που παρέχει ο κώδικας για ανίχνευση και διόρθωση λαθών. Για την ακρίβεια, η ελάχιστη απόσταση ενός κώδικα ισούται με τον αριθμό των θέσεων στις οποίες δύο κωδικοποιημένες λέξεις διαφέρουν και, μάλιστα, ο αριθμός των λαθών που μπορούν να ανιχνευτούν και να διορθωθούν σε κάθε λαμβανόμενη κωδικοποιημένη λέξη είναι ανάλογος του μεγέθους αυτού.

Οι συχνότερα χρησιμοποιούμενοι στην πράξη κώδικες τμήματος είναι οι γραμμικοί, ειδική κατηγορία των οποίων αποτελούν οι κυκλικοί κώδικες. Γραμμικοί κώδικες είναι οι κώδικες Hamming και οι κώδικες Colay. Οι γνωστότεροι κυκλικοί κώδικες είναι οι κώδικες Reed-Solomon και οι κώδικες BCH.

7.2.2. Γραμμικοί Μπλοκ Κώδικες

Ένας δυαδικός μπλοκ κώδικας (n, k) , ορίζεται πλήρως από $M=2k$ δυαδικές ακολουθίες μήκους n που ονομάζονται κωδικές λέξεις. Ένας κώδικας C , συνίσταται από M κωδικές λέξεις c_i με $1 \leq i \leq 2k$.

$$C = \{c_1, c_2, \dots, c_M\}$$

όπου c_i είναι μια ακολουθία μήκους n με όρους που παίρνουν τιμές 0 ή 1.

Ορισμός 1.1 Ένας μπλοκ κώδικας είναι γραμμικός, αν κάθε γραμμικός συνδυασμός δύο κωδικών λέξεων είναι επίσης μια κωδική λέξη. Στη δυαδική περίπτωση αυτή η απαίτηση σημαίνει ότι αν c_i και c_j είναι κωδικές λέξεις τότε $c_i \oplus c_j$ είναι επίσης μια κωδική λέξη, όπου \oplus συμβολίζει πρόσθεση modulo-2 των συντεταγμένων των δύο διανυσμάτων.

Με τον ορισμό αυτό, βλέπουμε ότι ένας γραμμικός κώδικας είναι ένας k -διάστατος υποχώρος του n -διαστατού χώρου. Είναι ακόμη προφανές ότι, η ακολουθία 0, που όλες οι συντεταγμένες της είναι μηδέν, είναι κωδική λέξη κάθε γραμμικού κώδικα γιατί για κάθε κωδική λέξη c_i ισχύει $c_i \oplus c_i = 0$. Σημειώστε ότι σύμφωνα με τον πιο πάνω ορισμό η γραμμικότητα ενός κώδικα εξαρτάται μόνο από τις κωδικές λέξεις και όχι από τον τρόπο με τον οποίο οι ακολουθίες πληροφορίας αντιστοιχίζονται στις κωδικές λέξεις. Αλλά είναι φυσικό να υποθέσουμε ότι αν η ακολουθία πληροφορίας u_1 (μήκους k) αντιστοιχίζεται στην κωδική λέξη c_1 (μήκους n) και η ακολουθία πληροφορίας u_2 αντιστοιχίζεται στην κωδική λέξη c_2 , τότε η $u_1 \oplus u_2$ αντιστοιχίζεται στην $c_1 \oplus c_2$. Στο εξής, θα υποθέτουμε ότι οι γραμμικοί κώδικες που μελετούμε έχουν την ιδιότητα αυτή.

Σαν παράδειγμα μπορούμε να αναφέρουμε έναν κώδικα ο οποίος ορίζεται ως εξής

$$C = (00000, 10100, 01011, 11111)$$

Είναι πολύ εύκολο να δούμε ότι ο κώδικας αυτός είναι γραμμικός. Αν η αντιστοιχία μεταξύ των ακολουθιών πληροφορίας και κωδικών λέξεων είναι

$$00 \rightarrow 00000$$

01→10100

10→01111

11→11111

η ιδιότητα που συζητήσαμε προηγουμένως ισχύει. Αν η αντιστοιχία είναι

00→10100

01→11111

10→00000

11→01011

η ιδιότητα δεν ισχύει. Αλλά, και στις δύο περιπτώσεις ο κώδικας είναι γραμμικός. Τώρα θα ορίσουμε τις βασικές παραμέτρους που χαρακτηρίζουν έναν κώδικα.

Ορισμός 1.2 Η απόσταση Hamming μεταξύ δύο κωδικών λέξεων, c_i και c_j , είναι ο αριθμός των συντεταγμένων στις οποίες οι δύο κωδικές λέξεις διαφέρουν και συμβολίζεται με $d(c_i, c_j)$.

Ορισμός 1.3 Το βάρος Hamming ή απλά βάρος μιας κωδικής λέξης c_i , είναι ο αριθμός των μη μηδενικών στοιχείων μιας κωδικής λέξης και συμβολίζεται με $w(c_i)$.

Ορισμός 1.4 Η ελάχιστη απόσταση ενός κώδικα, είναι η ελάχιστη απόσταση μεταξύ δύο οποιονδήποτε διαφορετικών κωδικών λέξεων, δηλαδή, $d_{\min} = \min\{d(c_i, c_j)\}$, όπου $i \neq j$, $\oplus c_i, c_j$

Ορισμός 1.5 Το ελάχιστο βάρος ενός κώδικα, είναι το ελάχιστο βάρος των κωδικών λέξεων με εξαίρεση την κωδική λέξη 0, $w_{\min} = \min\{w(c_i)\}$, όπου $c_i \neq 0$

Ορισμός 1.6 Σε κάθε γραμμικό κώδικα, $d_{\min} = w_{\min}$

Ένας κώδικας είναι μία διαδικασία μονοσήμαντης απεικόνισης στοιχείων από ένα σύνολο A σε ένα σύνολο B . Στην περίπτωση της κωδικοποίησης καναλιού και των κωδικών που χρησιμοποιούνται για αυτήν, τα στοιχεία του συνόλου A ονομάζονται **λέξεις πληροφορίας u_i** ($i= 1,2,\dots,M$), ενώ εκείνα του συνόλου B , στα οποία και αντιστοιχίζονται, ονομάζονται **κωδικές λέξεις, ή codewords, c_i** . Το M ισούται με τους δυνατούς συνδυασμούς των ακολουθιών k δυαδικών ψηφίων, δηλαδή $M=2^k$. Δυαδικός ονομάζεται ένας κώδικας όταν τα στοιχεία και των δύο συνόλων είναι ακολουθίες δυαδικών ψηφίων (0 ή 1). Εφόσον μιλάμε για μονοσήμαντη απεικόνιση δεν μπορεί το πλήθος των στοιχείων των δύο συνόλων να διαφέρει.

Μια από τις κατηγορίες κωδικών καναλιού είναι οι γραμμικοί κώδικες μπλοκ. Ένας κώδικας μπλοκ είναι γραμμικός αν κάθε γραμμικός συνδυασμός δύο κωδικών του λέξεων είναι επίσης κωδική του λέξη. Στην περίπτωση δυαδικού κώδικα αυτό σημαίνει πως το αποτέλεσμα της συνιστώσας-προς-συνιστώσα XOR λογικής πράξης μεταξύ δύο κωδικών του λέξεων, είναι επίσης κωδική λέξη.

7.2.3. Κυκλικοί κώδικες

Ένας γραμμικός κώδικας C καλείται κυκλικός, αν η κυκλική μετατόπιση κάθε κωδικής λέξης είναι και αυτή κωδική λέξη.

Αναφορικά με τη συνάρτηση κυκλικής μετατόπισης $k(\cdot)$, ισχύουν τα ακόλουθα: $k(x+y) = k(x)+k(y)$ και $k(ax) = ak(x)$. Η λέξη x που απαρτίζει μαζί με τις $(n-1)$ κυκλικές της μετατοπίσεις το S , γραμμικό ανάπτυγμα του οποίου είναι ο κώδικας C , ονομάζεται γεννήτορας του κυκλικού κώδικα C . Κάθε κώδικας μπορεί να έχει πολλούς γεννήτορες.

Αρχικά θα πρέπει να σκεφτόμαστε οποιαδήποτε ακολουθία n bits ως ένα πολυώνυμο $n-1$ βαθμού. Ο συντελεστής του κάθε όρου του πολυώνυμου λαμβάνει την τιμή του αντίστοιχου bit της ακολουθίας. Για παράδειγμα, η ακολουθία 1001110101 αντιστοιχεί τον πολυώνυμο: $M(x)=x^9+x^6+x^5+x^4+x^2+1$. Τόσο στον αποστολέα

κόμβο όσο και στον παραλήπτη είναι γνωστή εκ των προτέρων μια ειδική ακολουθία, η οποία ονομάζεται πολυώνυμο γεννήτορας και συμβολίζεται με $G(x)$. Ο αλγόριθμος CRC συνοψίζεται στα ακόλουθα βήματα..

Αποστολέας Κόμβος

1. Πολλαπλασιασμός του $M(x)$ με τον συντελεστή x^k , όπου k είναι ο βαθμός του προκαθορισμένου πολυωνύμου $G(x)$. Αυτό ουσιαστικά αντιστοιχεί σε αύξηση του μήκους των δεδομένων κατά k bits με αριστερή ολίσθηση κατά k των αρχικών bits και ταυτόχρονη πλήρωση των κενών θέσεων με μηδενικά.

1. Διαίρεση του $M(x)x^k$ με το $G(x)$. Από αυτή τη διαίρεση προκύπτει το πηλίκο $Q(x)$

και το υπόλοιπο $R(x)$.

2. Σύνθεση του μηνύματος $T(x)$, το οποίο θα αποστείλει προς το δίκτυο το ακόλουθο μήνυμα: $T(x)=M(x)x^k+R(x)$

Αποστολέας Κόμβος

1. Διαίρεση του μηνύματος $Z(x)$ με το $G(x)$. Από αυτή τη διαίρεση προκύπτουν το πηλίκο $Q(x)$ και το πηλίκο $R'(x)$. Εάν $R'(x)=0$, τότε δεν υπάρχει σφάλμα μεταφοράς.

Αν θεωρήσουμε ότι στη μεταφερόμενη ακολουθία $Z(x)$ προστίθεται ο θόρυβος $E(x)$, τότε ο παραλήπτης θα λάβει την ακολουθία $Z(x)=T(x)+E(x)$. Κανείς δεν μπορεί να αποκλείσει την περίπτωση, η μορφή του θορύβου να είναι τέτοια έτσι ώστε η λαμβανόμενη ακολουθία να διαιρείται ακριβώς από το πολυώνυμο γεννήτορας. Σε αυτή την περίπτωση όμως ο παραλήπτης θα βγάλει το (λανθασμένο) συμπέρασμα ότι στη ληφθείσα ακολουθία δεν υπάρχει σφάλμα μεταφοράς. Η επιλογή του πολυωνύμου είναι κρίσιμος παράγοντας στον έλεγχο κυκλικού πλεονασμού. Τα κριτήρια επιλογής του πολυωνύμου είναι σύνθετα. Στη πράξη έχουν επικρατήσει να χρησιμοποιούνται τα πολυώνυμα του ακόλουθου πίνακα.

Διακριτικός Τίτλος	G(x)
CRC-8	x^8+x^2+x+1
CRC-10	$x^{10}+x^9+x^5+x^4+x+1$
CRC-ITU-T	$x^{16}+x^{12}+x^5+1$
CRC-32	$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$

Σχήμα 10: Πίνακας πολυωνύμων

Σε γενικές γραμμές μπορεί να αποδειχθεί ότι οι κώδικες CRC μήκους k bits έχουν τις ακόλουθες δυνατότητες εντοπισμού σφαλμάτων μεταφοράς.

1. Όλα τα σφάλματα μονού bit, αρκεί οι όροι x^k και x^0 να έχουν μη μηδενικούς συντελεστές
2. Όλα τα σφάλματα διπλού bit, αρκεί το πολυώνυμο να περιέχει τρεις τουλάχιστον όρους.
3. Όλα τα σφάλματα περιττού πλήθους αρκεί το πολυώνυμο να περιέχει τον όρο $(x+1)$.
4. Όλα τα σφάλματα σε δέσμη bits με μήκος μικρότερο από k bits. Όπου ως δέσμη ονομάζουμε ένα πλήθος από διαδοχικά bits. Επίσης, εντοπίζονται τα περισσότερα από τα σφάλματα μεταφοράς σε δέσμες με μήκος μεγαλύτερο από k bits.

7.2.4 Παράδειγμα Block(CRC) κώδικα

Κατά την κωδικοποίηση block εισάγεται πλεονάζουσα πληροφορία με ελεγχόμενο και συστηματικό τρόπο. Τα bits αυτά δεν μεταφέρουν πληροφορία, αλλά δίνουν τη δυνατότητα στον αποκωδικοποιητή να διορθώνει λάθη.

Έστω λοιπόν ότι στον κώδικά μας έχουμε ως μεταβλητές $Q=8$ δηλαδή είσοδο 8 bit (π.χ 11010011) και $G=5$ (π.χ 10011) το πολυώνυμο/γεννήτορας. Οι συναρτήσεις `re_flip` είναι overloaded και εμφανίζουν ανάποδα τα bit ώστε να μη μπερδευτεί κάποιος που διαβάζει τα bit ανάποδα. Με τις εντολές `ifstream/ ofstream` δημιουργώ ροή εισόδου / εξόδου αντίστοιχα. Με τις εντολές `instream.open/ ostream.open` εφόσον βρεθεί, ανοίγει το αρχείο.

Έστω λοιπόν η είσοδος 11010011 και το πολυώνυμο x^4+x+1 . Παρατηρώ ότι $k=4$ άρα προσθέτω στην παλμοσειρά k μηδενικά. Άρα έχω: 000011010011 (σύνολο 12 στοιχεία/ αντίστοιχα στον κώδικα η εντολή `const int mxk_length-Q+(G-1)`). Στη συνέχεια κάνω αριστερή ολίσθηση κατά k ($mxk \leq G-1$) και προκύπτει: 110100110000. Κατά την εντολή `temp_mxk[i]=mxk[i+(mxk_length-G)]` Απομονώνω τα τελευταία G ψηφία του `mxk` με σκοπό να αρχίσω την crc κωδικοποίηση. Ακολουθεί η διαδικασία crc κατά την οποία κάνω XOR την είσοδο με το πολυώνυμο:110100110000

```
xor  10011
      01001
```

Στο αποτέλεσμα που προκύπτει διαγράφω το πρώτο στοιχείο (το 0) και κατεβάζω ένα στοιχείο τη φορά από το bit εισόδου. Αν το πρώτο στοιχείο του αποτελέσματος είναι 1 κάνω XOR την είσοδο με το πολυώνυμο. Αν το πρώτο στοιχείο του αποτελέσματος είναι 0 κάνω XOR με τόσα μηδενικά όσα τα ψηφία του πολυωνύμου.

Τα παραπάνω φανερώνονται στον κώδικα μας με την εντολή `if`.

Τέλος δημιουργούμε ένα `bitset` μεγέθους 12 θέσεων και με την εντολή `for` κάνουμε την πρόσθεση του μηνύματος (`mxk`) με το υπόλοιπο(`temp_mxk`). Τέλος του κώδικα.

7.2.6. Διαπλοκή block

Μια σημαντική τεχνική η οποία είναι αποτελεσματική για την αντιμετώπιση των σφαλμάτων κατά συστάδες είναι η *διαπλοκή*. Πριν εφαρμοστεί η ακολουθία δεδομένων στο κανάλι, αυτό οδεύει σε μια διαδικασία διαπλοκής και κωδικοποίησης για διόρθωση σφαλμάτων. Στο άκρο λήψης τα δεδομένα αποκωδικοποιούνται, δηλαδή τα bit των δεδομένων αποτιμώνται κατά τέτοιο τρόπο ώστε να υπάρχει το πλεονέκτημα της διόρθωσης σφαλμάτων και της ανίχνευσης των βασικών χαρακτηριστικών τα οποία προκύπτουν από την κωδικοποίηση και η διαδικασία της διαπλοκής εξαλείφεται. Όπως διαπιστώνεται, μια ομάδα δεδομένων που απαρτίζεται από kl bit φορτώνεται σε ένα καταχωρητή μετατόπισης ο οποίος είναι οργανωμένος σε k γραμμές με l bit ανά γραμμή. Η ακολουθία των δεδομένων εισάγεται στο στοιχείο αποθήκευσης $a11$. Σε κάθε μετατόπιση κάθε bit κινείται μια θέση προς τα δεξιά, ενώ το bit που βρίσκεται στην πιο ακραία δεξιά θέση του στοιχείου αποθήκευσης μετατοπίζεται στην πιο αριστερή θέση της επόμενης γραμμής. Έτσι, για παράδειγμα, όπως δηλώνεται και από το βέλος, το περιεχόμενο της θέσης $a11$ μετατοπίζεται στην $a21$. Όταν έχουν εισαχθεί και τα kl bit, ο καταχωρητής είναι πλήρης, με το πρώτο bit να είναι στην akl και το τελευταίο στην $a11$.

Στο σημείο αυτό η ακολουθία των δεδομένων παροχετεύεται σε έναν δεύτερο παρόμοιο καταχωρητή και μια διαδικασία κωδικοποίησης εφαρμόζεται στα δεδομένα που κρατήθηκαν αποθηκευμένα στον πρώτο καταχωρητή. Σε αυτή τη διαδικασία κωδικοποίησης, τα bit πληροφορίας μιας στήλης (δηλαδή $a11, a21, \dots, akl$) αντιμετωπίζονται σαν τα bit μιας μη κωδικοποιημένης λέξης στην οποία θα πρέπει να προστεθούν bit ισοτιμίας. Έτσι διαμορφώνεται η κωδικοποιημένη λέξη $a11a21\dots aklc11c21\dots crl$ και ως εκ τούτου παράγεται μια κωδικοποιημένη λέξη με k bit πληροφορίας και r bit ισοτιμίας. Ας σημειωθεί ότι σε αυτήν την κωδικοποιημένη λέξη τα bit πληροφορίας βρίσκονταν l bit μακρύτερα στη «γνήσια» ακολουθία των δεδομένων.

Όταν ολοκληρωθεί η κωδικοποίηση, το συνολικό περιεχόμενο του $k \times l$ καταχωρητή πληροφορίας καθώς επίσης και τα $r \times l$ bit ισοτιμίας μεταδίδονται μέσω του καναλιού. Γενικά, η bit προς bit σειριακή μετάδοση εξάγεται υπό τη μορφή γραμμή προς

γραμμή, δηλαδή υπό τη μορφή $crl \dots crl \dots cll \dots cllakl \dots ak1 \dots a2l \dots a2lall \dots a12all$ Ας σημειωθεί ότι τα δεδομένα μεταδίδονται με την ίδια ακριβώς σειρά με την οποία εισήχθησαν στον καταχωρητή, με τη διαφορά ότι τώρα μεταδίδονται και τα bit ισοτιμίας. Τα δεδομένα που λαμβάνονται αποθηκεύονται και πάλι με την ίδια σειρά όπως στον πομπό και πραγματοποιείται η αποκωδικοποίηση διόρθωσης σφαλμάτων. Τότε τα bit ισοτιμίας απορρίπτονται και τα bit των δεδομένων μετατοπίζονται εκτός του καταχωρητή. Για να γίνει κατανοητός ο τρόπος με τον οποίο η διαπλοκή επηρεάζει τις συστάδες των σφαλμάτων, ας θεωρηθεί ότι ο κώδικας που ενσωματώνεται σε μια κωδικοποιημένη λέξη επαρκεί για διόρθωση ενός απλού σφάλματος. Ας υποθεθεί στη συνέχεια ότι στη μεταδιδόμενη ακολουθία δεδομένων λαμβάνει χώρα μια συστάδα θορύβου που διαρκεί για l συνεχόμενα κωδικοποιημένα bit. Τότε εξαιτίας της δομής που παρουσιάστηκε, είναι φανερό ότι μόνο ένα σφάλμα θα εμφανιστεί σε κάθε στήλη και αυτό το απλό σφάλμα θα διορθωθεί. Αν υπάρχουν $l + 1$ συνεχόμενα σφάλματα, τότε μια στήλη θα έχει δύο σφάλματα και η διόρθωση δεν είναι εξασφαλισμένη

8. ΚΩΔΙΚΕΣ CONVOLUTIONAL

Οι συνελκτικοί κώδικες εισήχθησαν από τον Elias το 1955 ως εναλλακτική επιλογή έναντι των μπλοκ κωδίκων. Οι συνελκτικοί κώδικες μεταχειρίζονται τα δεδομένα εισόδου σαν μια συνεχή ακολουθία δεδομένων, σε αντίθεση με τους κώδικες block που συγκεντρώνουν τα εισερχόμενα bits σε ομάδες (blocks), και παράγουν μεγαλύτερες ομάδες σε n έξοδο τους. Το κύριο χαρακτηριστικό τους είναι ότι διαθέτουν μνήμη κατά τη διαδικασία κωδικοποίησης. Λίγο αργότερα, οι Wozencraft και Reiffen πρότειναν την ακολουθιακή αποκωδικοποίηση ως αποδοτική μέθοδο αποκωδικοποίησης συνελκτικών κωδίκων με μεγάλα μήκη εξαναγκασμού και σύντομα έκαναν την εμφάνισή τους πειραματικές μελέτες. Το 1963 ο Massey πρότεινε μια λιγότερο αποδοτική αλλά ευκολότερα υλοποιήσιμη μέθοδο αποκωδικοποίησης, την καλούμενη αποκωδικοποίηση κατωφλίου (threshold

decoding). Αυτή η εξέλιξη αποτέλεσε αφορμή για μια σειρά από πρακτικές εφαρμογές των συνελκτικών κωδίκων στην ψηφιακή μετάδοση σε τηλεφωνικά, δορυφορικά και ασύρματα κανάλια. Αργότερα, το 1967, ο Viterbi πρότεινε έναν αλγόριθμο αποκωδικοποίησης μέγιστης πιθανοφάνειας (maximum likelihood, ML), σχετικά εύκολα υλοποιήσιμο για αποκωδικοποιητή soft-απόφασης συνελκτικών κωδίκων με μικρά μήκη εξαναγκασμού. Ο αλγόριθμος Viterbi παράλληλα με εκδοχές soft-απόφασης της ακολουθιακής αποκωδικοποίησης οδήγησαν στην εφαρμογή των συνελκτικών κωδίκων σε διαστημικά και δορυφορικά συστήματα επικοινωνιών τη δεκαετία του '70. Το 1974 οι Bahl, Cocke, Jelinek και Raviv (BCJR) εισήγαγαν έναν αλγόριθμο αποκωδικοποίησης μέγιστης εκ των υστέρων πιθανότητας (maximum a posteriori probability, MAP) για συνελκτικούς κώδικες με άνισες εκ των προτέρων (a priori) πιθανότητες για τα bits πληροφορίας. Ο αλγόριθμος BCJR έχει βρει εφαρμογή πρόσφατα σε σχήματα αποκωδικοποίησης soft-απόφασης όπου οι εκ των προτέρων πιθανότητες των bits πληροφορίας μεταβάλλονται από υλοποίηση σε υλοποίηση.

8.1 Χαρακτηριστικά συνελκτικών κωδίκων

Οι κώδικες της κατηγορίας αυτής δημιουργούνται σχηματίζοντας τη συνέλιξη των ψηφίων πληροφορίας με την “κρουστική” απόκριση ενός καταχωρητή ολίσθησης, η οποία ορίζεται ως η απόκριση του κωδικοποιητή για είσοδο την ακολουθία ψηφίων “10”. Το χαρακτηριστικό γνώρισμα των συνελκτικών κωδίκων είναι η σειριακή επεξεργασία ολόκληρου του ρεύματος των ψηφίων πληροφορίας και η ύπαρξη μνήμης όπου αποθηκεύονται προηγούμενα ψηφία, δηλαδή η έξοδος του κωδικοποιητή κάθε στιγμή εξαρτάται δραστικά και από εισόδους προηγούμενων χρονικών στιγμών. Γίνεται αντιληπτή, λοιπόν, η διαφορά σε σχέση με τους συμπαγείς κώδικες όπου η επεξεργασία πραγματοποιείται ανά τμήματα και ανεξάρτητα από bits που ανήκουν σε άλλα τμήματα. Οι αλγόριθμοι συνελκτικής κωδικοποίησης βρίσκουν

μεγάλη εφαρμογή κυρίως σε εμπορικές εφαρμογές και στρατιωτικά συστήματα, όπου απαιτείται μεγάλη ασφάλεια.

Ένας συνελκτικός κώδικας ορίζεται από τρεις παραμέτρους: n k K Ένας (n, k, K) κώδικας επεξεργάζεται κάθε φορά k ψηφία πληροφορίας εισόδου και παράγει μία έξοδο n ψηφίων για κάθε k εισερχόμενα ψηφία. Η μνήμη των κωδικών χαρακτηρίζεται από τον περιοριστικό παράγοντα K που ονομάζεται μήκος εξαναγκασμού (*constraint factor*). Στην ουσία, τρέχουσα έξοδος n ψηφίων ενός (n, k, K) κώδικα εξαρτάται όχι μόνο από την τιμή του τρέχοντος συνόλου k ψηφίων εισόδου αλλά και από τα προηγούμενα $1 - K$ σύνολα των k ψηφίων εισόδου. Έτσι, έξοδος είναι μία συναρτήσεων τελευταίων $1 - K$ ψηφίων εισόδου. Αφού για κάθε k bits εισόδου έχουμε n bits εξόδου, ο κωδικός ρυθμός θα είναι: $R_c = k/n$. Οι παράμετροι k και n παίρνουν συνήθως τιμές από 1 ως 8 κι ο κωδικός ρυθμός c R μεταξύ 1/8 και 7/8. Η επιλογή του μήκους εξαναγκασμού K γίνεται με βάση το επιθυμητό κέρδος κωδικοποίησης (εδώ χρησιμοποιήσαμε μήκη με τιμή από 2 ως 9).

8.1.1. Διαδικασία κωδικοποίησης δεδομένων (convolution)

Η κωδικοποίηση δεδομένων με τρόπο συνελκτικό επιτυγχάνεται με τη χρήση ενός καταχωρητή ολίσθησης και σχετίζεται με τη συνδυαστική λογική modulo-two πράξεων. Ένας καταχωρητής ολίσθησης είναι απλώς ένα ζεύγος flip-flops όπου η έξοδος του νιοστού flip-flop είναι συνδεδεμένη με την είσοδο του (νιοστού+1) flip-flop.

Κάθε στιγμή που η τιμή του ρολογιού αλλάζει καθορισμένη κατεύθυνση (από 0 σε 1) τα δεδομένα ολισθαίνουν κατά ένα στάδιο. Η συνδυαστική λογική εμφανίζεται με τη μορφή αποκλειστικών OR πυλών (XOR). Ως υπενθύμιση οι πύλες XOR είναι δυο εισόδων και μιας εξόδου και αναπαριστώνται με το παρακάτω λογικό σύμβολο



το οποίο εφαρμόζει τον ακόλουθο πίνακα αληθείας

ΕΙΣΟΔΟ A	ΕΙΣΟΔΟ B	ΕΞΟΔΟΣ (A XOR B)
0	0	0
0	1	1
1	0	1
1	1	0

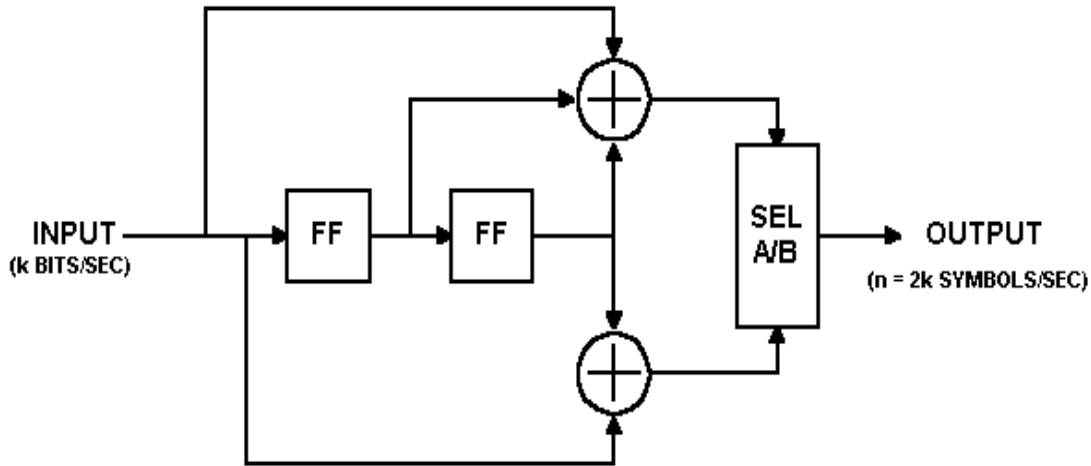
Σχήμα 11: Πίνακας αληθείας

Οι πύλες XOR εκτελούν modulo-two πράξεις. Αν κλιμακώσεις q πύλες XOR δυο εισόδων, με την έξοδο της πρώτης συνδεδεμένη στην είσοδο της δεύτερης, την έξοδο της δεύτερης συνδεδεμένη στην είσοδο της τρίτης κτλ, η αλυσίδα που έχει δημιουργηθεί είναι το modulo-two άθροισμα $q+1$ εισόδων.

Ένας πιο διαδομένος τρόπος αναπαράστασης XOR πυλών είναι ο ακόλουθος:



Πλέον έχουμε δυο βασικά χαρακτηριστικά ενός convolutional κωδικοποιητή (flip-flops τα οποία περιλαμβάνουν το καταχωρητή ολίσθησης και αποκλειστικές OR πύλες και προσομοιώνουν ένα modulo-two αθροιστή. Παρακάτω παρατίθεται μια εικόνα ενός convolutional κωδικοποιητή ρυθμού $\frac{1}{2}$, $K=3$ και $m=2$.



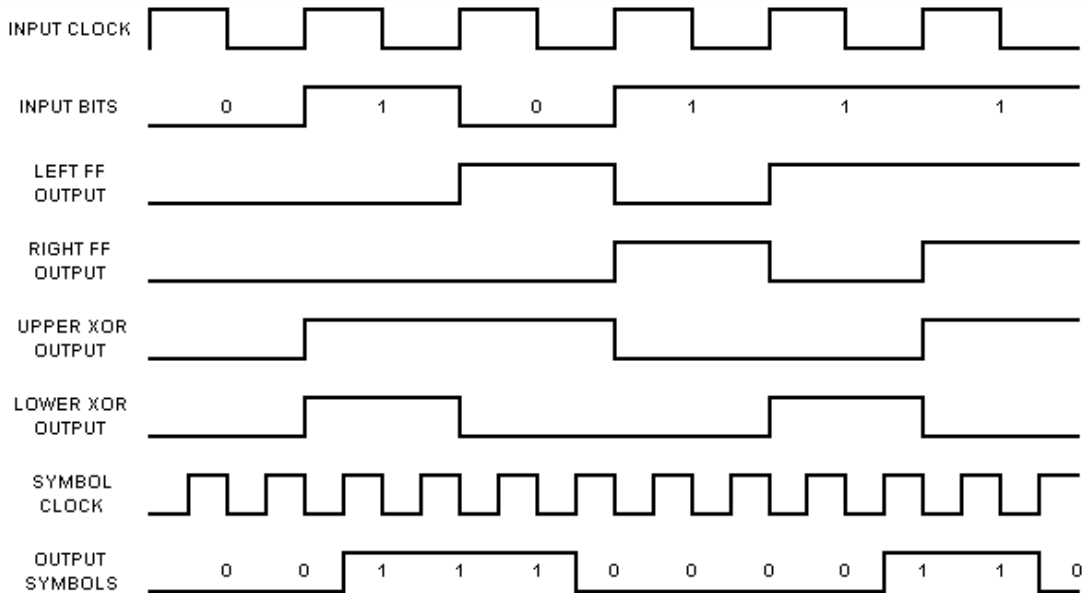
Σχήμα 12: Convolutional κωδικοποιητής

Ο κωδικοποιητής ξεκινά μόλις η ακμή του ρολογιού γίνει θετική. Έπειτα η έξοδος του αριστερού flip-flop συγχρονίζεται προς το δεξιό flip-flop, το προηγούμενο bit εισόδου συγχρονίζεται στο αριστερό flip-flop και έτσι ένα νέο bit εισόδου γίνεται διαθέσιμο. Ο selector A/B επιλέγει και προωθεί τη πρώτη χρονική στιγμή την έξοδο ανώτερου αθροιστή και την επόμενη χρονική στιγμή την έξοδο του κατώτερου αθροιστή.

Έστω είσοδος 010111001010001.

Αρχικά οι έξοδοι των flip-flop είναι 0. Στο πρώτο κύκλο ρολογιού η είσοδος στο κωδικοποιητή είναι 0, οι έξοδοι των flip-flop είναι 0 οπότε είσοδοι των αθροιστών είναι 0, άρα οι έξοδοι είναι 00. Στο δεύτερο κύκλο ρολογιού η έξοδος του αριστερού flip-flop είναι 0 αφού 0 ήταν η είσοδος στο πρώτο κύκλο όπως επίσης και η έξοδος του δεξιού flip-flop είναι 0 επειδή 0 ήταν η έξοδος του αριστερού flip-flop στο προηγούμενο κύκλο. Πλέον οι είσοδοι στο πάνω αθροιστή είναι 100 ενώ στο κάτω 10, οπότε έξοδος 11. Στο τρίτο κύκλο ρολογιού η έξοδος του αριστερού flip-flop είναι 1 αφού 1 ήταν η είσοδος στο πρώτο κύκλο, επίσης η έξοδος του δεξιού flip-flop είναι 0 επειδή 0 ήταν η έξοδος του αριστερού flip-flop στο προηγούμενο κύκλο. Πλέον οι είσοδοι στο πάνω αθροιστή είναι 010 ενώ στο κάτω 00, οπότε έξοδος 10 κτλ κτλ.

Το χρονοδιάγραμμα παρακάτω απεικονίζει τη διαδικασία.



Σχήμα 13:Χρονοδιάγραμμα

Καθώς όλα τα bit εισαχθούν στον κωδικοποιητή, η τελική έξοδος είναι η εξής 00 11 10 00 01 10 01 11 11 10 00 10 11 00 11. Είναι φανερό ότι για $K=3$ και ρυθμό $\frac{1}{2}$ κάθε είσοδος επηρεάζει άρδεις το αποτέλεσμα εξόδου. Για αυτό το λόγο ο convolutional κωδικοποιητής χρησιμοποιείται για επιδιόρθωση λαθών.

Για αυτό το λόγο τρέχουμε τη παραπάνω διαδικασία $m=2$ φορές έχοντας ως είσοδο μηδέν ώστε στο τελευταίο στάδιο τα flip flop να έχουν ως έξοδο μόνο μηδέν. Η νέα έξοδος θα είναι 00 11 10 00 01 10 01 11 11 10 00 10 11 00 11 10 11 και αυτό το κάνουμε γιατί ο αποκωδικοποιητής πρέπει να αρχίζει σε μια γνωστή κατάσταση και να τελειώνει επίσης σε γνωστή, γεγονός που βοηθά πολύ στη διαδικασία αποκωδικοποίησης. Αν δεν κάναμε flushing τα τελευταία m bits θα είχαν μικρότερη πιθανότητα πρόβλεψης ενός λάθους σε σχέση με τα υπόλοιπα.

8.1.2. Αναπαράσταση με διανύσματα συνδέσεων

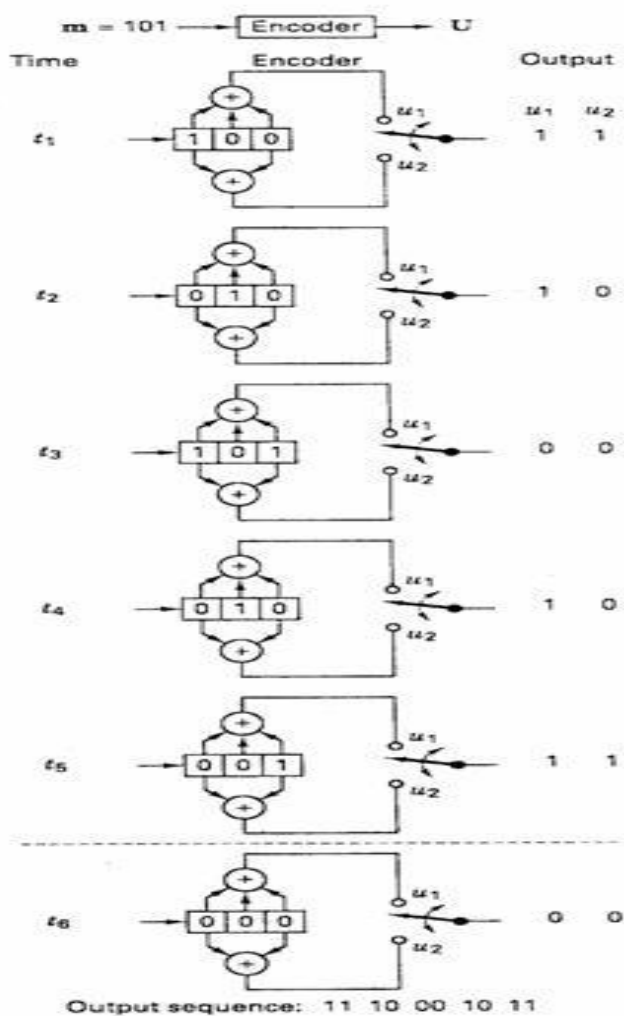
Ένας τρόπος αναπαράστασης του κωδικοποιητή είναι μέσω μιας ομάδας 2^k διανυσμάτων συνδέσεων, ενός για κάθε modulo-2 αθροιστή. Κάθε διάνυσμα έχει διάσταση K και περιγράφει τη σύνδεση του καταχωρητή με τον εν λόγω αθροιστή. Μια μονάδα στην i -στη θέση του διανύσματος υποδεικνύει ότι η αντίστοιχη βαθμίδα του καταχωρητή ολίσθησης είναι συνδεδεμένη στον αθροιστή, ενώ ένα μηδενικό υποδεικνύει ότι δεν υπάρχει σύνδεση της θέσης αυτής του καταχωρητή με τον αθροιστή. Για τον κωδικοποιητή του παραδείγματος μπορούμε να γράψουμε

$$\mathbf{E}_1 = 1\ 1\ 1$$

$$\mathbf{E}_2 = 1\ 0\ 1$$

Ας υποθέσουμε τώρα ότι η ακολουθία πληροφορίας $\mathbf{m} = 1\ 0\ 1$ εισέρχεται στον κωδικοποιητή του παραδείγματος. Στο σχήμα 3 φαίνεται η διαδικασία της κωδικοποίησης της ακολουθίας αυτής. Όπως βλέπουμε, τις χρονικές στιγμές t_1 , t_2 και t_3 εισέρχονται διαδοχικά στον καταχωρητή, ένα κάθε φορά, τα bits πληροφορίας. Στη συνέχεια, τις χρονικές στιγμές t_4 και t_5 εισέρχονται $K-1=2$ μηδενικά για τον καθαρισμό του καταχωρητή, εξασφαλίζοντας έτσι ότι και το τελευταίο bit πληροφορίας θα περάσει από όλες τις βαθμίδες του καταχωρητή. Η ακολουθία εξόδου είναι η 1 1 1 0 0 1 0 1 1, όπου το αριστερότερο σύμβολο αντιστοιχεί στην πρώτη χρονικά εκπομπή. Ολόκληρη η ακολουθία εξόδου είναι απαραίτητη για την αποκωδικοποίηση του μηνύματος, ακόμη και τα κώδικα σύμβολα που προέκυψαν από τη διαδικασία του καθαρισμού.

Μπορούμε να προσεγγίσουμε τη λειτουργία του κωδικοποιητή μέσα από την έννοια της κρουστικής απόκρισης, της απόκρισης δηλαδή του κωδικοποιητή σε ένα και μοναδικό bit που μετακινείται στις βαθμίδες του. Στον παρακάτω πίνακα βλέπουμε τις εξόδους του κωδικοποιητή του παραδείγματος, καθώς μετακινείται μέσα του μια μονάδα. Η κρουστική απόκριση του κωδικοποιητή είναι λοιπόν η 11 10 11. Γνωρίζοντας την κρουστική απόκριση ενός κωδικοποιητή, μπορεί κανείς να βρει την ακολουθία εξόδου για μια συγκεκριμένη ακολουθία εισόδου μέσω γραμμικού αθροίσματος μετατοπισμένων κρουστικών αποκρίσεων



Σχήμα 14: Διαδικασία συνελκτικής κωδικοποίησης ακολουθίας πληροφορίας

8.1.3. Παράδειγμα για Convolutional code

Έστω ότι έχω στον κώδικά μου τρεις καταχωρητές ($K=3$) και την είσοδο 4^{ov} bit ($M=4$) Έχοντας λοιπόν είσοδο 1011 σημαίνει ότι το λιγότερο σημαντικό ψηφίο είναι ο τελευταίος άσσος και το μεγαλύτερο ο πρώτος άσσος άρα ο αριθμός είναι $2^0*1+2^1*0+2^2*1+2^3*1$. Στη `++/bitset` αν θελήσουμε να εισάγουμε τα παραπάνω ψηφία θα πρέπει να πληκτρολογήσουμε με την ανάποδη σειρά σε ένα αρχείο. Επίσης δεν μπορούμε να κάνουμε `dynamic` αλλαγή στο μέγεθος του vector αυτό το λόγω βάλουμε δύο `#define` στην αρχή. Επίσης οι συναρτήσεις `re_flip` είναι `overloaded` και εμφανίζουν ανάποδα τα bit ώστε να μη μπερδευτεί κάποιος που διαβάζει τα bit ανάποδα. Με τις εντολές `ifstream/ ofstream` δημιουργώ ροή εισόδου / εξόδου αντίστοιχα. Εφόσον βρει και ανοίξει το αρχείο(εντολές `ifstream.open/ ofstream.open`) δημιουργώ μια συμβολοσειρά `s` η οποία είναι και η είσοδος μας δηλαδή το 1011. Στη συνέχεια δημιουργώ τον πίνακα `b1` με τα στοιχεία του `s`

1	0	1	1
---	---	---	---

Και εκτυπώνω το `b1` σαν 1101.

Στη συνέχεια δημιουργώ vector `sum` και λόγω φλιπ φλοπ πρέπει να είναι 000. Επιπλέον δημιουργώ δύο μονοδιάστατους πίνακες για να εισαχθούν τα αποτελέσματα των XOR τόσο για την είσοδο, όσο για την έξοδο.

Μέσα σε μια εντολή `for` δηλώνουμε το μέγεθος του `s` (`size=4`) και επειδή η μεταβλητή `i` που δηλώσαμε νωρίτερα επιστρέφει `unsigned` κάνουμε `cast` για να γίνει `signed`. Αρχικά για `i=0` έχω

1	0	0
---	---	---

Για την XOR `u1: 1^0^0=1`

Για την XOR `u2: 1^0=1`

Εκτυπώνει το `sum` τα αποτελέσματα των δύο XOR και τα εισάγει στο αρχείο `output.txt`. Στη συνέχεια κάνει δεξιά ολίσθηση κατά 1 και προκύπτει

0	1	0
---	---	---

Συνεχίζουμε για $i=1$ και έχω

1	1	0
---	---	---

Για την XOR u1: $1^1=0$

Για την XOR u2: $0^1=1$

Εκτυπώνει το sum τα αποτελέσματα των δύο XOR και τα εισάγει στο αρχείο output.txt. Στη συνέχεια κάνει δεξιά ολίσθηση κατά 1 και προκύπτει

0	1	1
---	---	---

Συνεχίζουμε με τον ίδιο τρόπο για $i=2$ και $i=3$

Πρέπει στο τέλος να αδειάσουμε (flush) και τον καταχωρητή δηλαδή τα φλιπ φλοπ. Για αυτό το λόγο τρέχουμε την παραπάνω διαδικασία έχοντας είσοδο 0 ώστε στο τελευταίο στάδιο τα φλιπ φλοπ να έχουν έξοδο μόνο 0 και αυτό το κάνουμε γιατί ο αποκωδικοποιητής πρέπει να αρχίζει σε μια και να τελειώνει σε μια γνωστή κατάσταση, γεγονός που βοηθά πολύ στην διαδικασία της αποκωδικοποίησης. Αν δεν κάναμε flushing τα τελευταία bits θα είχαν μικρότερη πιθανότητα πρόβλεψης ενός λάθους σε σχέση με τα υπόλοιπα.

Έτσι λοιπόν και στον κώδικά μας έχουμε την εντολή while η οποία όταν το sum γεμίσει με μηδέν σταματά να εκτελείται. Τότε λοιπόν κλείνουμε τις δύο ροές εισόδου και τελειώνει ο κώδικας.

8.1.4. Διαφορές συνελεκτικών κωδικών και block

Οι συνελεκτικοί κώδικες διαφέρουν από τους μπλοκ κώδικες στο ότι ο κωδικοποιητής διαθέτει μνήμη και οι έξοδοί του σε κάποια χρονική στιγμή δεν εξαρτώνται μόνο από τις εισόδους του εκείνη τη χρονική στιγμή, αλλά και από έναν αριθμό προηγούμενων εισόδων. Ένας συνελεκτικός κωδικοποιητής ρυθμού $R = k/n$ με τάξη μνήμης V μπορεί να υλοποιηθεί ως ένα γραμμικό ακολουθιακό κύκλωμα k εισόδων και n εξόδων με μνήμη εισόδου V . Αυτό σημαίνει ότι οι εισοδοί παραμένουν στον κωδικοποιητή για V επιπλέον χρονικές στιγμές αφότου εισέλθουν σ' αυτόν. Συνήθως τα n και k παίρνουν μικρές τιμές, η ακολουθία πληροφορίας διαιρείται σε μπλοκ μήκους k και η κωδική λέξη σε μπλοκ μήκους n . Στη σημαντική ειδική περίπτωση όπου $k=1$, η ακολουθία πληροφορίας δε διαιρείται σε μπλοκ και υπόκειται συνεχή επεξεργασία. Σε αντίθεση με τους μπλοκ κώδικες, μεγάλες ελάχιστες αποστάσεις κωδικών λέξεων και μικρές πιθανότητες σφάλματος δεν επιτυγχάνονται με αύξηση των k και n , αλλά με αύξηση της τάξης μνήμης V .

9. ΒΙΒΛΙΟΓΡΑΦΙΑ

- [1]. Embedded Microprocessor Systems: Real World Design (Third Edition) –
Newnes
- [2]. Designing embedded systems with PIC microcontrollers – Newnes
- [3]. Hardware firmware and software design – O G Pora
- [4]. GSM Modules software user guide – Telit
- [5]. *Practical Approaches to Speech Coding*”, P. Papamichalis, Prentice-Hall, 1987 (Βιβλιοθήκη ΤΜ.Η.Υ.Π.)
- [6]. <http://www.umts-forum.org>
- [7]. ΜΟΤΟ-ΟΤΕ και ΕΛΟΤ. Γενική και Ειδική Τηλεπικοινωνιακή Ορολογία. Αθήνα Ελλάδα, 10η έκδοση, Ιούνιος 2001
- [8]. M. Abramowitz και I. A. Stegun. Handbook of Mathematical Functions, with Formulas, Graphs, and Mathematical Tables. Dover, New York, 9η έκδοση, 1972
- [9]. S. Haykin. Communications Systems. John Wiley & Sons, New York, 1994.
- [10]. A. A. Huurdeman. The Worldwide History of Telecommunications. John Wiley & Sons, Hoboken, New Jersey, 2η έκδοση, 2003.
- [11]. M. C. Mallik. Chronology of developments of wireless communication and electronics. IETE Technical Review, 3(9):479–522, Σεπτέμβριος 1986.
- [12]. B. Sklar. Rayleigh fading channels in mobile digital communications systems part II:Mitigation. IEEE Communications Magazine, 35(9):148–155, Σεπτέμβριος 1997
- [13]. E. Shannon, “A Mathematical Theory of Communication,” *Bell Syst. Tech. J.*,27, pp. 379-423 (Part I), 623-656 (Part II), July 1948.
- [14]. M. Chiani, A. Conti, and V. Tralli. Further Results on Convolutional Code Search for Block-Fading Channels. IEEE Trans. Inform. Theory, June 2004.

- [15]. Sarma Vangala and Hossein Pishro-Nik. A Highly Reliable FSO/RF Communication System Using Efficient Codes. *IEEE Trans Wireless Commun.*
- [16]. <http://almasmmu.blogspot.com/2007/06/channel-coding-for-wireless.html>, Channel Coding for Wireless Communication Systems.
- [17]. <http://www.wikipedia.org/>, Wikipedia.
- [18]. John G. Proakis, “Digital Communications”, Fourth Edition
- [19]. Sarah S. Johnson “Introducing Low-Density Parity-Check Codes”
- [20]. Γεώργιος Κων. Κοκκινάκης, “Εισαγωγή στις Επικοινωνίες”, 2004
- [21]. A . Dholakia, M . Vouk, and D . Bitzer, “ Table based decoding of rate one – half convolutional codes, ” *IEEE Transactions. on Communications*, vol . 43, no . 2 – 4, pp . 681 – 686, 1995.
- [22]. Thuan Nguyen, Ferit Yegenoglu, Agatino Sciuto, COMSAT Laboratories, Ravi Subbarayan, Lockheed Martin Global Communications- Voice over IP Service and Performance in Satellite Networks-pdf.
- [23]. Analysis of IP voice conferencing over EuroSkyWay satellite system Cruickshank, H.; Sun, Z.; Carducci, F.; Sanchez, A.; *IEEE Proceedings Communications*, Volume: 148 Issue: 4 , Aug 2001 Page(s): 202 -206.
- [24]. Uyles Black- Voice Over IP (Second Edition). Prentice Hall Series.
- [25]. Daniel Minoli-Emma Minoli.-Delivering Voice over IP Networks. Wiley.
- [26]. ITU-T Rec. G.711, “Pulse Code Modulation (PCM) of Voice Frequencies,” 1988.
- [27]. “Channel Coding in Communication Networks: From Theory to Turbocodes”, p. 272, edited by A. Glavieux, ISTE Ltd., 2007
- [28]. E. Biglieri, “Coding and Modulation for a Horrible Channel”, *IEEE Communications Magazine*, May 2003
- [29]. “Digital Communications”, John Proakis, McGraw-Hill, 4th edition, 2000
- [30]. I. Kim, B. McArthur, and E. Korevaar. Comparison of Laser Beam Propagation at 785 nm and 1550 nm in Fog and Haze for Optical Wireless Communications. In *roc. SPIE*, 2001.

ΠΑΡΑΡΤΗΜΑ

Για την υλοποίηση της τυχαίας παλμοσειράς σε block και convolutional κώδικα χρησιμοποιήσαμε κώδικα γραμμένο στη Γλώσσα C.

ΚΩΔΙΚΑΣ CRC

```
#include <iostream>

#include <fstream>

#include <string>

#include <bitset>

#include <vector>

#include <math.h>

#define Q 50

#define G 11

using namespace std;

void re_flip(bitset<Q>);

int main(int argc, char *argv[])

{

    ifstream inStream;

    ifstream inStream2;

    inStream.open("C:/input_crc.txt");

    inStream2.open("C:/qX.txt");

    string input;

    string input2;

    inStream>>input;
```

```

inStream2>>input2;
bitset<Q> m(input);
bitset<G> g(input2);
cout<<"M(x) " <<m<<endl<<"G(x) " <<g<<endl;
const int mxk_length=Q+(G-1);
int i;
bitset<mxk_length> mxk(input);
mxk<<=G-1;
cout<<"M(x)*X^" <<G-1<<" " <<mxk<<endl;
bitset<G> temp_g(input2);
bitset<G> temp_mxk;
bitset<G> zeros;
for(i=0;i<G;i++)
{
    temp_mxk[i]=mxk[i+(mxk_length-G)];
}
cout<<"Xor prakseis " <<endl;
for(i=0;i<(mxk_length-G);i++)
{
    if(temp_mxk[G-1]==1)
    {
        cout<<temp_mxk<<"^" <<g;
        temp_mxk=g^temp_mxk;
        temp_mxk<<=1;
    }
}

```

```

        temp_mxk[0]=mxk[(mxk_length-G)-(i+1)];
        cout<<"=" <<temp_mxk<<endl;

    }
    else
    {

        cout<<temp_mxk<<"^"<<zeros;
        temp_mxk=zeros^temp_mxk;
        temp_mxk<<=1;
        temp_mxk[0]=mxk[(mxk_length-G)-(i+1)];
        cout<<"=" <<temp_mxk<<endl;

    }
}

bitset<mxk_length> t;
for(i=0;i<mxk_length;i++)
{
    t[i]=mxk[i]|temp_mxk[i];
}

cout<<"Ara tha metadsw :"<<mxk<<"+"<<temp_mxk<<"="<<t<<endl;
system("pause");

return 0;
}

```



```

void re_flip(bitset<Q> temp)
{
    int i;
    for (i=0;i<Q;i++)
    {
        cout<<temp[i];
    }
    cout<<endl;
}

```

ΑΠΟΤΕΛΕΣΜΑ

M(x) 11010011010011101010011100010111100010101010110001

G(x) 000000000000

M(x)*X¹⁰

110100110100111010100111000101111000101010101100010000000000

Xor prakseis

11010011010¹⁰^000000000000= 10100110100

10100110100¹⁰^000000000000= 01001101001

01001101001¹⁰^000000000000= 10011010011

10011010011¹⁰^000000000000= 00110100111

00110100111¹⁰^000000000000= 01101001110

01101001110¹⁰^000000000000= 11010011101

11010011101¹⁰^000000000000= 10100111010

10100111010¹⁰^000000000000= 01001110101

01001110101¹⁰^000000000000= 10011101010

1001101010^0000000000= 00111010100
00111010100^0000000000= 01110101001
01110101001^0000000000= 11101010011
11101010011^0000000000= 11010100111
11010100111^0000000000= 10101001110
10101001110^0000000000= 01010011100
01010011100^0000000000= 10100111000
10100111000^0000000000= 01001110001
01001110001^0000000000= 10011100010
10011100010^0000000000= 00111000101
00111000101^0000000000= 01110001011
01110001011^0000000000= 11100010111
11100010111^0000000000= 11000101111
11000101111^0000000000= 10001011110
10001011110^0000000000= 00010111100
00010111100^0000000000= 00101111000
00101111000^0000000000= 01011110001
01011110001^0000000000= 10111100010
10111100010^0000000000= 01111000101
01111000101^0000000000= 11110001010
11110001010^0000000000= 11100010101
11100010101^0000000000= 11000101010
11000101010^0000000000= 10001010101
10001010101^0000000000= 00010101010
00010101010^0000000000= 00101010101

00101010101^00000000000= 01010101011
01010101011^00000000000= 10101010110
10101010110^00000000000= 01010101100
01010101100^00000000000= 10101011000
10101011000^00000000000= 01010110001
01010110001^00000000000= 10101100010
10101100010^00000000000= 01011000100
01011000100^00000000000= 10110001000
10110001000^00000000000= 01100010000
01100010000^00000000000= 11000100000
11000100000^00000000000= 10001000000
10001000000^00000000000= 00010000000
00010000000^00000000000= 00100000000
00100000000^00000000000= 01000000000
01000000000^00000000000= 10000000000

Ara tha metadwsw

:110100110100111010100111000101111000101010101100010000000000+
1

0000000000=110100110100111011100111000101111000101010101100010
000000000

Πιέστε ένα πλήκτρο για συνέχεια. . .

ΚΩΔΙΚΑΣ CONVOLUTION

```
#include <iostream>

#include <fstream>

#include <string>

#include <bitset>

#include <vector>

#define K 3

#define M 50

using namespace std;

void re_flip(bitset<K>);

void re_flip(bitset<M>);

int main()

{

    cout<<"Convolution encoder k=1, n=2, K=3, r=1/2"<<endl;

        ifstream inStream;

        ofstream outStream;

        inStream.open("C:/input.txt");

        outStream.open("C:/output.txt");

        string s;

        inStream>>s;

        bitset<M> b1(s);
```

```

cout<<b1<<endl;

re_flip(b1);

bitset<K> sum(string("000"));

bitset<1> u1;

bitset<1> u2;

int i;

for(i=0;i<signed(s.size());i++)

{

    sum[2]=b1[i];

    u1=(sum[0]^sum[1]^sum[2]);

    u2=sum[0]^sum[2];

    cout<<sum<<". ";

    cout<<u1<<u2<<endl;

    ostream<<u1;

    ostream<<u2;

    sum>>=1;

}

cout<<"Katharismos Kataxwrhth\n";

while(!sum.none())

{

```



```

        u1=(sum[0]^sum[1]^sum[2];

        u2=sum[0]^sum[2];

        cout<<sum<<". ";

        cout<<u1<<u2<<endl;

        sum>>=1;

        outStream<<u1;

        outStream<<u2;

    }

    outStream.close();

    inStream.close();

    system("PAUSE");

    return 0;

}

void re_flip(bitset<K> temp)

{

    int i;

    for (i=0;i<K;i++)

    {

        cout<<temp[i];

    }

    cout<<endl;

```

```

}

void re_flip(bitset<M> temp)

{
    int i;

    for (i=0;i<M;i++)

    {

        cout<<temp[i];

    }

    cout<<endl;

}

```

ΑΠΟΤΕΛΕΣΜΑ

Convolution encoder $k=1$, $n=2$, $K=3$, $r=1/2$

10001010011101010101110000110101100110101001110110

01101110010101100110101100001110101010111001010001

000.00

100.11

110.01

011.01

101.00

110.01

111.10

011.01

001.11

100.11

010.10

101.00

010.10

101.00

110.01

011.01

001.11

100.11

110.01

011.01

101.00

010.10

101.00

110.01

011.01

001.11

000.00

000.00

100.11

110.01

111.10

011.01

101.00

010.10

101.00

010.10

101.00

010.10

101.00

110.01

111.10

011.01

001.11

100.11

010.10

101.00

010.10

001.11

000.00

100.11

Καθαρισμος Kataxwrhth

010.10

001.11

Πιέστε ένα πλήκτρο για συνέχεια. . .