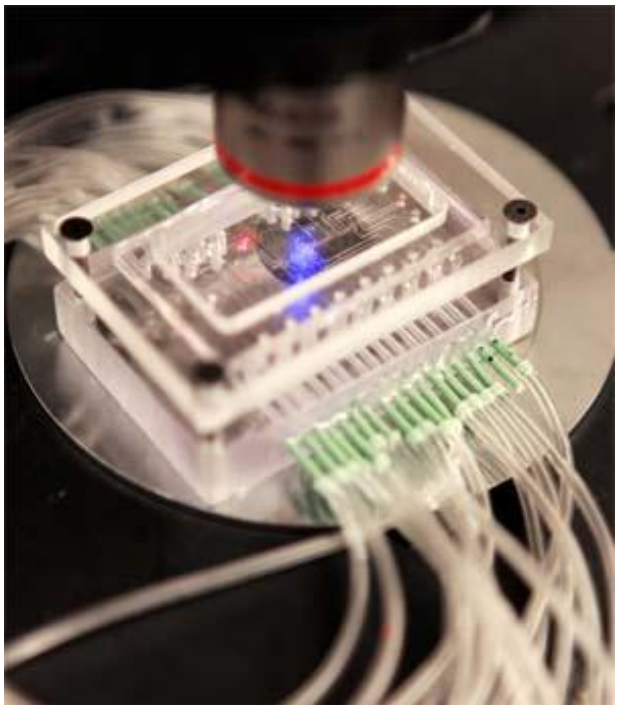
ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Κίνδυνοι και Ασφάλεια Δορυφορικών Συστημάτων Πρόσβασης Υπό Όρους

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Γεωργίου Νίκος



Επιβλέπων: Χρήστος Καψάλης
Καθηγητής Ε.Μ.Π

Αθήνα, Οκτώβριος 2009

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Κίνδυνοι και Ασφάλεια Δορυφορικών Συστημάτων Πρόσβασης Υπό Όρους

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Γεωργίου Νίκος

Επιβλέπων: Χρήστος Καψάλης
Καθηγητής Ε.Μ.Π

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

……..	……..	……..
Χ. Καψάλης	Π. Κωττής	Φ. Κωνσταντίνου
Καθηγητής Ε.Μ.Π	Καθηγητής Ε.Μ.Π	Καθηγητής Ε.Μ.Π

Αθήνα, Οκτώβριος 2009

.....
Γεωργίου Νίκος
Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π

Περίληψη

Η διπλωματική εργασία ασχολείται με τις μεθόδους παράκαμψης της ασφάλειας των δορυφορικών συστημάτων πρόσβασης υπό όρους. Τα δορυφορικά συστήματα με πρόσβαση υπό όρους είναι τα συστήματα εκείνα στα όποια, πρόσβαση δικαιούται αυτός που έχει καταβάλει (στον πάροχο του συστήματος) το κατάλληλο τίμημα. Έτσι του διατίθεται ο κατάλληλος εξοπλισμός που του επιτρέπει να έχει πρόσβαση στις υπηρεσίες που παρέχει ο πάροχος (ταινίες, αθλητικοί αγώνες, teletext και άλλα). Αν δεν έχει καταβληθεί η συνδρομή, αλλά επιτυγχάνεται πρόσβαση στις υπηρεσίες με τεχνητά μέσα, τότε έχουμε άρση της ασφάλειας και πραγματοποιείται το φαινόμενο της πειρατείας. Στα επτά κεφάλαια η διπλωματική αναλύει το δορυφορικό σύστημα (εκπομπή και λήψη), τη χρήση της κρυπτογραφίας για έλεγχο πρόσβασης, όπως και τους τρόπους πειρατείας και τα αντίμετρα που λαμβάνονται από τις εταιρείες.

Στο Πρώτο εισαγωγικό Κεφάλαιο της εργασίας εξηγούνται τα παραπάνω.

Στο Δεύτερο Κεφάλαιο παρουσιάζεται μια αναδρομή των συστημάτων πρόσβασης υπό όρους στα αναλογικά, μετά στα υβριδικά και τέλος στα σημερινά ψηφιακά σήματα.

Στο Τρίτο, και ενδιαφέρον, Κεφάλαιο εξηγείται το δορυφορικό σύστημα εκπομπής και λήψης. Συγκεκριμένα αναλύεται το πρότυπο DVB που είναι το ευρωπαϊκό (και όχι μόνο) τηλεοπτικό πρότυπο εκπομπής, με έμφαση φυσικά στη δορυφορική του εκδοχή DVB-S, καθώς και η συμπίεση MPEG. Ακόμα εξηγείται πως το σήμα κωδικοποιείται και διαμορφώνεται στον εκπομπό όπως και πως λαμβάνεται στο δέκτη του τελικού χρήστη.

Στο Τέταρτο περιγράφεται ο μηχανισμός κρυπτογράφησης του σήματος από τον πάροχο και ο μηχανισμός αποκρυπτογράφησης με τη χρήση της έξυπνης κάρτας στο δορυφορικό δέκτη του συνδρομητή.

Τέλος στο Πέμπτο, Έκτο και Έβδομο Κεφάλαιο που είναι και το κύριο μέρος αναλύονται οι τρεις πιο διαδεδομένοι τρόποι άρσης της ασφάλειας των συστημάτων πρόσβασης. Με τη σειρά που αναλύονται, αυτά είναι ο διαμοιρασμός κάρτας (card sharing), η κλωνοποίηση κάρτας και το video streaming.

Λέξεις Κλειδιά

DVB, DVB-S, DVB-S2, CAS, CSA, CAM, EMM, ECM, CW, QPSK, DES, AES, RSA, MD-5, MPEG, εξομοιωτής, διαμόρφωση, πάροχος, δέκτης, πειρατεία, έξυπνη κάρτα, διαμοιρασμός κάρτας, κλωνοποίηση κάρτας, εκπομπή, λήψη, κρυπτογράφηση

Abstract

This thesis deals with bypass methods of the safety of conditional access satellite systems. Satellite systems with conditional access, are those systems in which everyone who has paid the provider's subscription has access. The subscriber is been provided with the appropriate equipment (smart card and receiver) that allows him to have access to the provided services (movies, sporting events, teletext and more). If there is access to the services with illegal equipment and without subscription, then we have security breach and the phenomenon of piracy takes place. In seven chapters performs the analysis of the satellite system (transmission and reception), the use of cryptography for access control, and the different ways of piracy and the security measures taken by the companies.

In the first introductory chapter of the thesis we explain the above.

In the second chapter we show the conditional access mechanism historically from analog signal to hybrid and finally to digital signals that been used in latest satellite technology.

In the third chapter we explain the satellite systems mechanism (transmission and reception of signal). Specifically we analyze DVB protocol which is the European (and not only) TV broadcast standard, with an emphasis of course on satellite version DVB-S, as well as MPEG compression. Moreover we explain how the signal is encoded and transmitted and recieved.

In the fourth we explain encryption mechanism in the provider's transmission system, and the mechanism of decryption, using the smart card, in the satellite receiver of the Subscriber.

Finally in the fifth, sixth and seventh chapter which are the main part of thesis, we analyze the three most widespread methods for satellite piracy. By the order they came along these are: card sharing, cloning card and video streaming.

Keywords

DVB, DVB-S, DVB-S2, CAS, CSA, CAM, EMM, ECM, CW, QPSK, DES, AES, RSA, MD-5, MPEG, emulator, receiver, piracy, smart card, card sharing, cloning card, encryption

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον καθηγητή της σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών κύριο Χρήστο Καψάλη για την αποδοχή του να αναλάβω το συγκεκριμένο θέμα της εργασίας.

Τους πρώην συμφοιτητές μου και νυν συναδέλφους Ηλεκτρολόγους Μηχανικούς : Σκούτα Κατερίνα, Καλιακούδη Δημήτρη και Δημητρίου Παύλο για την πολύτιμη βοήθεια τους.

Το Ζώτο Γεώργιο, ηλεκτρονικό, για τις διορθώσεις και υποδείξεις του.

Όπως και την οικογένεια μου που με στήριξε και με στηρίζει όλα αυτά τα χρόνια.

Επικοινωνία για διατύπωση απορίων, διευκρινήσεων, διορθώσεων ή οτιδήποτε άλλο στο email, nikoscyp@gmail.com.

στους καθηγητές

και εκπαιδευτικούς

Λουγκρίδη Χαράλαμπο

και Ασπρομάλλη Γεώργιο

για το ‘’Ευ Ζην’’

Κεφάλαιο 1 : Εισαγωγή

1.1 Λόγοι διπλωματικής

- Η εξερεύνηση του πεδίου κρυπτογραφίας δορυφορικών εκπομπών
- Δεν υπάρχει κάτι παρόμοιο και είναι μια κατατοπιστική αρχή για κάποιον που θέλει:
    - να κατανοήσει την κρυπτογράφηση στις δορυφορικές τηλεπικοινωνίες
    - να βρει αντίμετρα κατά της πειρατείας ή νέες τεχνικές κρυπτογράφησης
- Η δορυφορική κρυπτογράφηση αποτελεί αιχμή της τεχνολογίας και είναι ένα πεδίο που θέλω να ασχοληθώ επαγγελματικά
- Ενδιαφέρον και χόμπι για τα δορυφορικά δρώμενα

Το θέμα της διπλωματικής αναλύει τη μεθοδολογία και τους τρόπους πειρατείας των δορυφορικών εκπομπών-λήψεων στα συστήματα πρόσβασης υπό όρους.

1.2 Τι είναι όμως δορυφορική εκπομπή-λήψη ;

Για να κατανοήσουμε τι σημαίνει δορυφορική εκπομπή-λήψη εξηγούμε πρώτα τους όρους, πάροχος και συνδρομητής που θα συναντήσουμε κατά κόρον στη διπλωματική. Ο πάροχος ονομάζεται το φυσικό πρόσωπο ή εταιρεία η οποία διαθέτει τον κατάλληλο εξοπλισμό, άδεια, προσωπικό για να εκπέμπει οπτικοακουστικό υλικό(ο.υ.)σε συγκεκριμένη ομάδα ατόμων που έχουν συνάψει συμβόλαιο μαζί του και ονομάζονται συνδρομητές.

1.2.1 Δορυφορική εκπομπή

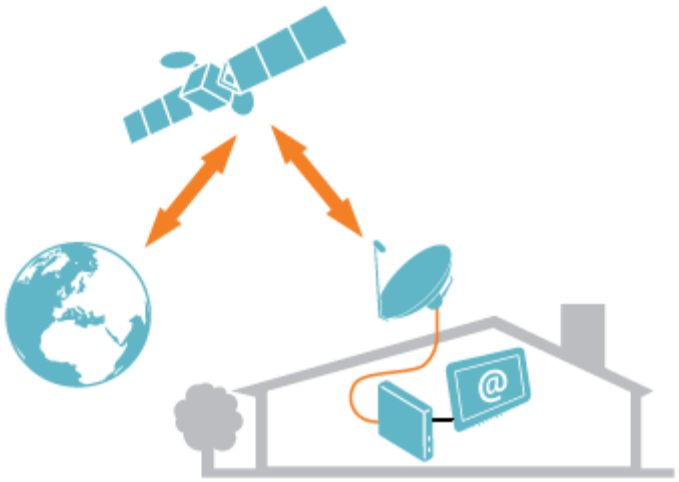
Η εκπομπή γίνετε με αποστολή του ο.υ. μέσω ηλεκτρομαγνητικών κυμάτων από τα κεντρικά γραφεία του παροχου σε ένα δορυφόρο(για Ελλάδα Hotbird 13ο ή/και HellasSat 21ο).Η όλη εκπομπή-λήψη γίνεται σε μορφή DVB* ,το όποιο θα αναλύσουμε εκτενώς στο Κεφάλαιο 3.

1.2.2 Δορυφορική λήψη

Αντίστοιχα δορυφορική λήψη είναι η λήψη τους σήματος (που στέλνει ο πάροχος) από το συνδρομητή-πελάτη του. Αυτό γίνεται ως εξής:
Το σήμα λαμβάνετε από ένα κίλο κάτοπτρο προσανατολισμένο προς το δορυφόρο. Με την αρχή της οπτικής, παράλληλες ακτίνες από το άπειρο συγκλίνουν στην εστιακή απόσταση του κατόπτρου όπου ευρίσκεται το LNB(Low Noise Block Downconverter, μεταλλάκτης χαμηλού θορύβου).
Τα LNB ή αλλιώς μάτι όπως συνηθίζουν να το λένε πολλοί είναι αυτό που λαμβάνει το σήμα από τον δορυφόρο (η κεραία δηλαδή). Το σήμα αντανακλάτε από το κάτοπτρο στο LNB όπου υποβαθμίζει τη συχνότητα του για να περιοριστούν οι απώλειες μεταφοράς, το ενισχύει και διαχωρίζει τις πολώσεις*.

**Το σήμα προς πληροφορία διαμορφώνεται και στις δύο πολώσεις (κάθετη, οριζόντια) του ηλεκτρομαγνητικού φέροντος κύματος για καλύτερη εκμετάλλευση του ηλεκτρομαγνητικού φάσματος συχνοτήτων .Έτσι ανά συχνότητα υπάρχουν δύο σήματα (κανάλια) ανάλογα με την τάση που δέχεται από το δέκτη το LNB (13V για κατακόρυφη ή 18V για οριζόντια) επιλέγει ποιά από τις δύο θα τροφοδοτήσει το δορυφορικό δέκτη.*

Από το μάτι περνά με το ομοαξονικό καλώδιο στο ψηφιακό δορυφορικό δέκτη όπου αφού τύχει επεξεργασίας (αποκρυπτογραφηθεί αν είναι κρυπτογραφημένο) διοχετεύεται στις οπτικές εξόδους (scart, rca, hdmi) στην τηλεόραση του τηλεθεατή/συνδρομητή. Το όλο σύστημα εκπομπής-λήψης αναλύεται στο κεφάλαιο 3 της παρούσας εργασίας.



Σχήμα 1 : αποστολή και λήψη δορυφορικού σήματος στον πελάτη ,το σήμα στέλνεται από επίγειο σταθμό στο δορυφόρο όπου αντανακλάται ενισχύεται και αποστέλλεται πίσω στη γη για λήψη από τον πελάτη

Εδώ κάνουμε παύση και εξηγούμε τι είναι ο ψηφιακός δέκτης

Σχήμα 2: ψηφιακός δορυφορικός δέκτης

1.3 Τι είναι ο ψηφιακός δέκτης;

Οι δορυφορικές μεταδόσεις των τηλεοπτικών καναλιών έχουν ξεκινήσει εδώ και χρόνια να γίνονται ψηφιακά σε σχέση με τις επίγειες που ακόμα οι πλείστες είναι αναλογικές. Η τηλεόραση διαθέτει ειδική βαθμίδα για τη λήψη των αναλογικών επίγειων τηλεοπτικών μεταδόσεων. Τέτοια βαθμίδα όμως είτε λόγω κόστους ,είτε λόγω τεχνογνωσίας ,είτε άλλων συμφερόντων-παραγόντων δεν υπάρχει για λήψη δορυφορικών μεταδόσεων στις πλείστες τηλεοράσεις. Έτσι είναι αναγκαία η ύπαρξη εξωτερικής βαθμίδας που λαμβάνει το δορυφορικό σήμα το επεξεργάζεται και το μετατρέπει σε video-audio σήμα ικανό να αναπαραχθεί στην τηλεόραση όπως κάνει και ένα εξωτερικό dvd-player.

Αυτές οι βαθμίδες επειδή λαμβάνουν δορυφορικό σήμα καλούνται διεθνώς «Receivers» και λόγω λήψης ψηφιακών μεταδόσεων, ονομάζονται Digital Receivers ή όπως αποδίδεται στην γλώσσα μας, «ψηφιακοί δέκτες».

1.3.1 Οι δορυφορικοί ψηφιακοί δέκτες και οι κατηγορίες τους

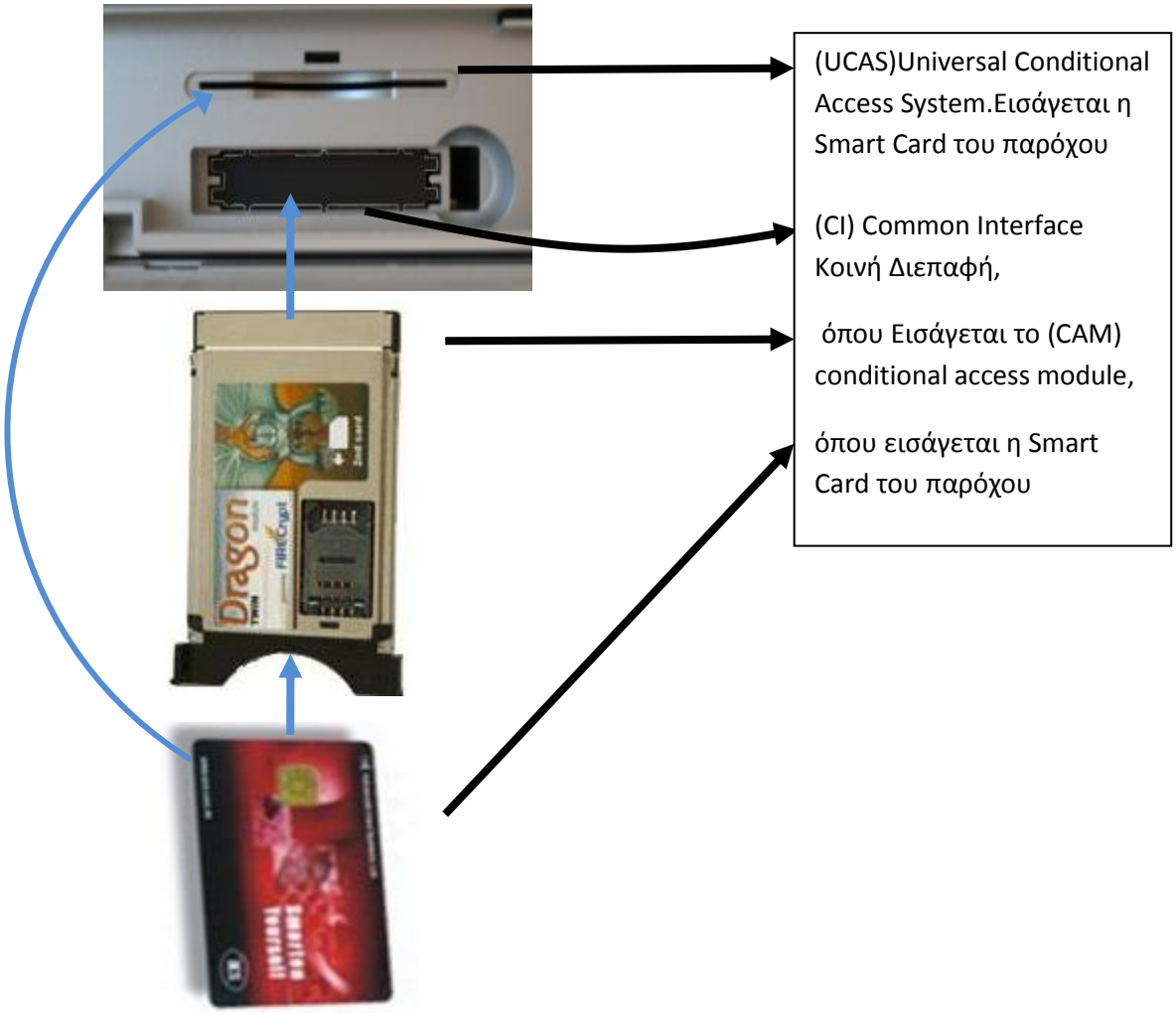
Οι δορυφορικοί ψηφιακοί δέκτες έχουν με τα χρόνια εξελιχθεί και έχουν δημιουργήσει αρκετές υποκατηγορίες.

1.3.1.1 Free To Air δέκτες

Η πρώτη υποκατηγορία είναι οι δέκτες Free To Air, ή αλλιώς F.T.A. Είναι η απλούστερη μορφή ψηφιακών δορυφορικών δεκτών και μπορούν και λαμβάνουν τα κανάλια που εκ-πέμπουν ελεύθερα στους δορυφόρους.

1.3.1.2 Δέκτες με δυνατότητα αποκρυπτογράφησης

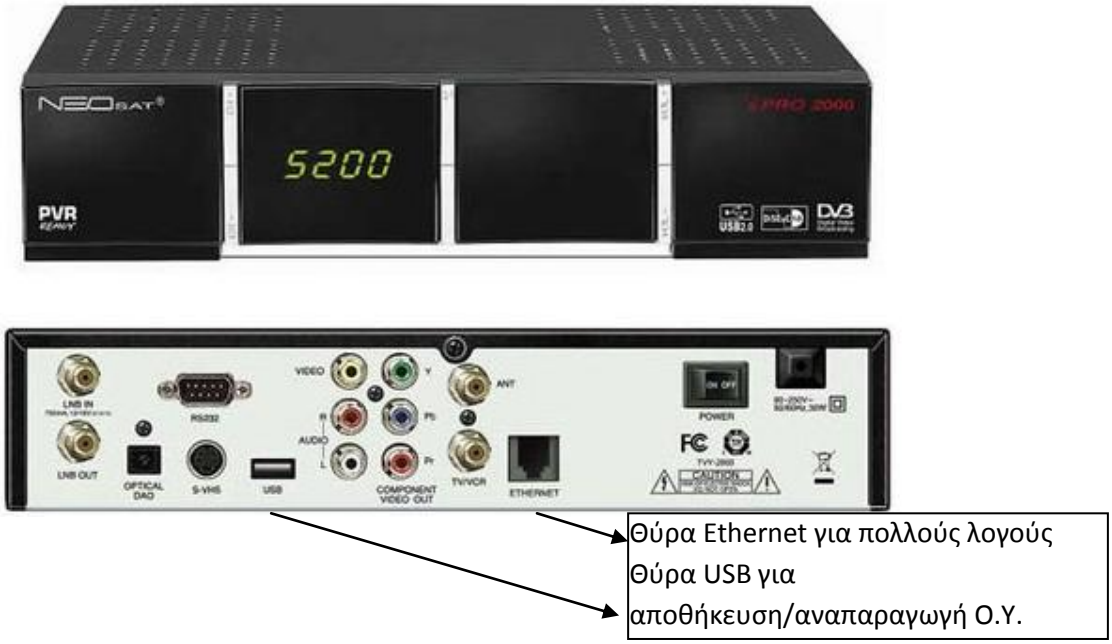
Η δεύτερη υποκατηγορία είναι οι δέκτες με ένα ή περισσότερα Common Interface (C.I.) η και (UCAS) Universal Conditional Access System. Είναι η πλέον δημοφιλής κατηγορία δεκτών στην Ευρώπη, καθώς επιτρέπει τη λήψη εκτός των ελεύθερων δορυφορικών καναλιών και κάποιων συνδρομητικών, υπό προϋποθέσεις. Συγκεκριμένα, πρέπει να τοποθετηθεί στο C.I. του δέκτη ένα επιπρόσθετο εξάρτημα που ονομάζεται Common Access Module ή CAM. Το εξάρτημα αυτό επιτρέπει τη συνεργασία του δέκτη με συνδρομητικές κάρτες ψηφιακών δορυφορικών πακέτων, και κατ' επέκταση την τηλεθέαση κωδικοποιημένων καναλιών. Ενώ η θύρα UCAS διαθέτει ενσωματωμένο CAM οπότε εισάγεται απευθείας στη σχισμή η συνδρομητική κάρτα. Στο σχήμα 3 φαίνονται οι δύο τρόποι εισαγωγής έξυπνης κάρτας στο δέκτη(UCAS και CI με εξωτερικό CAM).



Σχήμα 3: Μέρη Κρυπτογράφησης ενός ψηφιακού δορυφορικού δέκτη

1.3.1.3 Δέκτες με σύνδεση στο διαδίκτυο

Τρίτη μεγάλη κατηγορία είναι αυτή των δικτυωμένων δεκτών, που συνδέονται μέσω θυρών «Ethernet» σε ένα οικιακό δίκτυο ή και στο Διαδίκτυο. Οι δέκτες αυτοί είναι ιδιαίτερα δημοφιλείς στους χρήστες υπολογιστών, καθότι επιτρέπουν την αξιοποίηση των δορυφορικών μεταδόσεων με ποικίλους τρόπους. Συνήθως, αξιοποιούνται και ως «Multimedia Terminal», για την αναπαραγωγή αρχείων ήχου και εικόνας, σε διάφορες μορφές και από διάφορες πηγές.



Σχήμα 4: Δέκτης με θύρα Ethernet

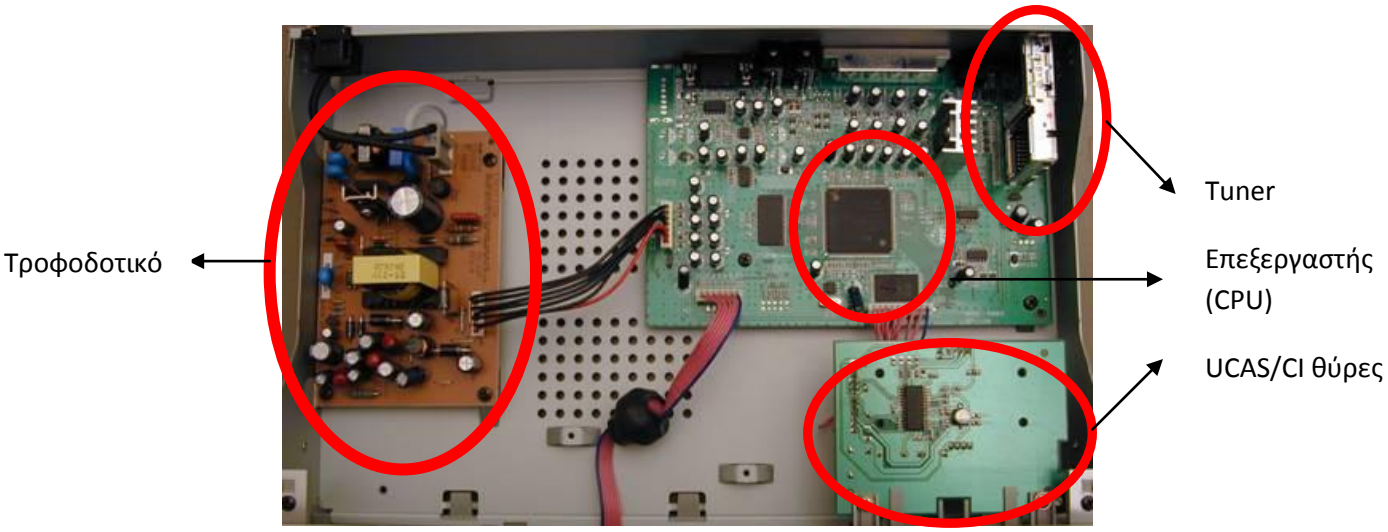
Υποκατηγορία αυτών έχουν ισχυρό επεξεργαστή/μνήμη και σκληρό δίσκο όπου τρέχουν εφαρμογές Linux (συμπεριφέρονται δηλαδή σαν ηλεκτρονικοί υπολογιστές).Με αυτή τη δυνατότητα μπορούν να εξομοιώνουν κρυπτογραφικά συστήματα και αλγορίθμους να επικοινωνούν στο internet να ανταλλάζουν πληροφορίες με το δίκτυο και άλλα. Γνωστός και πρωτοπόρος εκπρόσωπος αυτής της κατηγορίας είναι η εταιρία Dreambox Multimedia

Σχήμα 5: Το τελευταίο μοντέλο της Dreambox Multimedia ο DM 8000 HD RVR με χαρακτηριστικά:

- 400 MHz MIPS Processor
- Linux Operating System
- Twin DVB-S2 Tuner -(δες Κεφάλαιο 3)
- 2 x Plug&Play Tuner Module sockets (DVB-S, DVB-C, DVB-T) -(δες Κεφάλαιο 3)
- 4 x DVB Common-Interface Slots
- 2 x Smartcard-Reader (Dreamcrypt)
- integrated Compact Flash and SD Card slot
- 128 MByte Flash, 256 MByte RAM
- prepared for WLAN (slot and antenna)
- 10/100Mbit Ethernet Interface
- 3 x USB2.0 (1x Front, 2 x Back)
- 2 x SAT

1.3.2 Μέρη ενός κοινού ψηφιακού δέκτη :

- Όπως οι πλείστες οικιακές συσκευές οι ψηφιακοί δέκτες λειτουργούν με dc-τάση οπότε διαθέτουν τροφοδοτικό που είναι μετατροπέας ac-dc.
- Διαθέτουν το τμήμα αποκρυπτογράφησης (UCAS/CI θύρες) που είδαμε πιο πριν.
- Διαθέτουν το tuner που φιλτράρει τη συχνότητα του καναλιού που επιθυμεί ο χρήστης να δει.
- Και διαθέτει τον επεξεργαστή που ελέγχει τις διεργασίες που γίνονται για να εξαχτεί το σήμα.



Σχήμα 6 :Το εσωτερικό ενός δέκτη με τα μέρη που το αποτελούν

Γιατί όμως είπες ότι το σήμα είναι κρυπτογραφημένο και γιατί οι πάροχοι το κρυπτογραφούν και οι πελάτες συνάπτουν συμβόλαιο και πληρώνουν συνδρομή; Πριν δούμε γιατί κρυπτογραφεί ο πρώτος (πάροχος) και πληρώνει ο δεύτερος (συνδρομητής) ας δούμε τι σημαίνει κρυπτογράφηση.

1.4 Κρυπτογράφηση καναλιού

Κρυπτογράφηση δορυφορικού σήματος είναι η τεχνική με την οποία η εικόνα και ο ήχος παραμορφώνονται σε βαθμό που να μην είναι κατανοητές. Για να μπορέσει ο πελάτης να δει το σήμα πρέπει να ζητήσει από τον πάροχο να του δώσει τον κατάλληλο εξοπλισμό (έξυπνη κάρτα) που μόνο αυτός διαθέτει, για την αποκρυπτογράφηση του σήματος καταβάλλοντας πάντα το κατάλληλο αντίτιμο (συνδρομή).

1.4.1 Γιατί όμως γίνεται κρυπτογράφηση;

Οι δορυφορικές συνδρομητικές εκπομπές εμφανίζουν πολλά πλεονεκτήματα σε σύγκριση με τις ελεύθερες αναλογικές ή ψηφιακές εκπομπές αυτές είναι:

- Οι συνδρομητικές δορυφορικές τηλεοπτικές εκπομπές συνήθως δεν περιέχουν αρκετές διαφημίσεις και στηρίζονται στο αμερικανικό μοντέλο που θέλει οι συνδρομητές να πληρώνουν τα κόστη του παροχου αντί οι διαφημιζόμενοι.
- Ο πάροχος συνδρομητικού δορυφορικού σήματος περιέχει στο πρόγραμμα του τελευταίας κυκλοφορίας ταινίες, μεγάλα αθλητικά γεγονότα (champion league κ.α.), ντοκιμαντέρ όπως και κοσμικές εκδηλώσεις (βραβεία Oscar). Όλα αυτά έχουν ακριβά δικαιώματα και ο αγοραστής(πάροχος) θα πρέπει να βγάλει αυτά τα λεφτά.
- Συνήθως ο πάροχος συμπεριλαμβάνει τεχνολογίες- υπηρεσίες άγνωστες οι πιο πολλές στην αναλογική τηλεόραση όπως αλλαγή γλώσσας εκφωνητή σε αθλητικό αγώνα ή ταινία, αλλαγή γλώσσας γραμματοσειράς σε ταινία, επιλογή γωνιάς λήψης σε αθλητικό αγώνα ,περίληψη προγραμμάτων (EPG) και άλλες υπηρεσίες .

Όλα αυτά χρειάζονται χρήμα και το χρήμα από διαφημίσεις δεν αρκεί όπως και το γεγονός όσο πιο πολλές διαφημίσεις τόσο πιο πολύ πέφτει η ποιότητα της υπηρεσίας. Έτσι με τη συνδρομή ο πάροχος βρίσκει τα χρήματα και ο συνδρομητής απολαμβάνει καλύτερες και ποιοτικότερες υπηρεσίες. Εδώ βρίσκεται και ο λόγος που ο πάροχος κρυπτογραφεί το σήμα του, οποίος πληρώσει βλέπει και εδώ έρχεται και ο πειρατής. Το κάθε δορυφορικό σύστημα από τη στιγμή που εισάγει κρυπτογραφία για να κάνει επιλεκτική τν πρόσβαση των υπηρεσιών του καλείται Σύστημα Πρόσβασης Υπό Όρους.

1.5 Πειρατής- Πειρατεία

Πειρατής στα δορυφορικά δρώμενα ονομάζετε αυτός που έχει πρόσβαση σε αποκρυπτογραφημένο οπτικοακουστικό υλικό για το όποιο δεν έχει πληρώσει δικαιώματα– συνδρομή στον ανάλογο πάροχο που ανήκουν τα δικαιώματα εκπομπής. Ο όρος έχει ενδιαφέρουσα ιστορία προέρχεται από την εποχή των πρώτων παράνομων ερασιτεχνικών ραδιοεκπομπών. Οι παράνομοι ερασιτέχνες εξέπεμπαν τις παράνομες ραδιοφωνικές εκπομπές τους από πλοία στα όποια είχαν ασυλία έτσι η χώρα στην όποια εξέπεμπαν παράνομα αδυνατούσε να τους συλλάβει. Η χρήση του πλοίου και η παρόμοια παράνομη συμπεριφορά τους έδωσε το συνώνυμο του πειρατή που επικράτησε και στις δορυφορικές λήψεις.

Η πειρατεία δεν είναι κάτι άγνωστο στις συνδρομητικές τηλεοπτικές υπηρεσίες αλλά όπως θα δούμε και στο επόμενο κεφάλαιο προϋπήρχε από καταβολής των συνδρομητικών καναλιών. Το εύκολο και γρήγορο κέρδος, η πρόκληση για σπάσιμο των κωδικών κρυπτογράφησης, η μανία για αθλητικά ή αλλά κανάλια υψηλής τηλεθέασης, ο ανταγωνισμός των εταιρειών είναι μόνο λίγοι λόγοι που συντηρούν και χρηματοδοτούν την ύπαρξη της. Βέβαια τα πρώτα χρόνια η γνώση ήταν προνόμιο των λίγων και οι κρυπτογραφήσεις ασθενείς ,η έλευση του διαδικτύου και η ανταλλαγή γνώσης και πληροφορίας έφερε ισχυρές και δαπανηρές κρυπτογραφήσεις από την πλευρά των παρόχων αναγκάζοντας και τους πειρατές να καταφύγουν και αυτοί σε ευφυή δίκτυα ευρείας ζώνης (κεφάλαιο 5) ή σε ηλεκτρονικά μικροσκοπία και αντίστροφη μηχανική(κεφάλαιο 6).Το σίγουρο είναι ότι ο πόθος των πειρατών για κατάλυση των αλγορίθμων κρυπτογράφησης δε θα σταματήσει ποτέ και οι πάροχοι είναι αναγκασμένοι να επενδύσουν άψυχο (πιο εξελιγμένα συστήματα προστασίας) αλλά και έμψυχο(καλούς μηχανικούς και κρυπτογράφους) υλικό.

Το θέμα τις πειρατείας στις δορυφορικές επικοινωνίες είναι πολύ σοβαρό και φτάνει να απασχολεί ακόμα και την Ευρωπαϊκή Ένωση. Η Ε.Ε στις 20 Νοέμβριου του 1998 εξέδωσε την οδηγία 98/84/ΕΚ για την νομική προστασία των υπηρεσιών που βασίζονται σε συστήματα πρόσβασης υπό όρους. Ενώ το 2003 και 2008 εξέδωσε δύο εκθέσεις σε συνέχεια της οδηγίας, βάση των οποίων η πειρατεία ,συστημάτων πρόσβασης υπό όρους, θεωρείται ως έγκλημα στο κυβερνοχώρο.

Επιπλέον σε ξεχωριστή έκθεση της Satelite TV Platforms: World Survey and Prospects to 2017 αναφέρεται ότι συνολικά το 1997 δαπανήθηκαν για πειρατικό εξοπλισμό 200 εκατομμύρια ευρώ σε όλη την Ευρώπη, ενώ το 2007 το ποσό έφτασε το 1 δισεκατομμύριο.

1.5.1 Τρόποι δορυφορικής πειρατείας

Η δορυφορική πειρατεία έχει πολλούς τρόπους κατάλυσης της προστασίας πρόσβασης από τρίτους. Οι πιο γνωστοί τρόποι αναφέρονται επιγραμματικά κάτωθι και αναλύονται εκτενώς στη διπλωματική οι τρεις πιο κύριοι και ζημιογόνοι για ένα πάροχο.

1.5.1.1 Διαμοιρασμός της εικόνας και ήχου(content redistribution)

1) Ο απλός και κλασσικός τρόπος διαμοιράσματος της εικόνας και ήχου από την έξοδο του ψηφιακού δορυφορικού δέκτη. Αφού το σήμα/ήχος αποκρυπτογραφηθεί από ένα νόμιμο δέκτη οδηγείται με διαχωριστή (splitter) σε άνω των 1 τηλεοράσεων. Έτσι έχουμε κοινή θέαση καναλιού σε όλο το σπίτι ή και σε ολόκληρη την πολυκατοικία. Τον καιρό που μεσουρανούσε το αναλογικό πακέτο filmnet/supersport ο τρόπος αυτός ευδοκιμούσε στις πολυκατοικίες. Οι ένοικοι έβαζαν δύο αποκωδικοποιητές στην ταράτσα μιας πολυκατοικίας και τραβούσαν έξοδο από κάθε δεκτή σε όλα τα διαμερίσματα, έτσι κάθε ένοικος ανάλογα αν ήθελε filmnet/supersport συντόνιζε την τηλεόραση του στο ένα ή στον άλλο δέκτη. Στην ίδια κατηγορία υπάγονται τα video sender, τα οποία εκπέμπουν σε ραδιοκύματα το ο.υ. Αν και ο τρόπος αυτός αποτελεί εν μέρη πειρατεία δεν μπορεί να εξυπηρετήσει μεγάλο αριθμό χρηστών και δεν αναλύεται.

Στα συν : ο φτηνός και απλός τρόπος.
Στα πλην: περιορισμένου βεληνεκούς, δεν μπορεί ο καθένας να επιλέξει τι θα δει

1.5.1.2 Με video streaming

2) Με video streaming : αναβαθμισμένη σύγχρονη τεχνική του προηγούμενου τρόπου. Με την έλευση του adsl και των ευρυζωνικών γρήγορων συνδέσεων, ολόκληρο δορυφορικό κανάλι ακόμα και transponder (αναμεταδότης που περιέχει πακέτο καναλιών) μεταφέρεται αφού αποκρυπτογραφηθεί από νόμιμο δέκτη μέσω του internet. Πως γίνεται αυτό: το κανάλι αφού βγει από το δέκτη μέσω software υπολογιστή ή αυτόνομων συσκευών (converter) μετατρέπεται σε συμπιεσμένη οικονομική μορφή ιδανική για μεταφορά στο internet. Έτσι με τα πρωτοκολλά multicast του διαδικτύου μπορεί ένας χρήστης να στέλνει σε πολλούς χρήστες ο.υ μέσω διαδικτύου. Ο τρόπος αναλύεται στο κεφάλαιο 7.

Στα συν : περισσότεροι χρήστες, μεγαλύτερη εμβέλεια
Στα πλην: αναγκαστική χρήση internet και γρήγορων συνδέσεων , χαμηλότερη ποιότητα αφού υποβαθμίζεται για να μπορεί να σταλθεί μέσω ίντερνετ.

1.5.1.3 Card Sharing

3) Με περιβόητο card sharing : Ο τρόπος που ανθεί και αποτελεί το μεγάλο πλήγμα των παρόχων , αναλύεται διεξοδικά στο 5ο κεφάλαιο. Περιληπτικά: ο πειρατής παίρνει κρυπτογραφημένο σήμα από το δορυφορικό του πιάτο. Για να αποκρυπτογραφηθεί χρειάζεται τα λεγόμενα κλειδιά. Αυτά τα κλειδιά (cw – control words) δίνονται από ένα server ο οποίος είναι ενωμένος με ένα δέκτη ο οποίος έχει νόμιμη κάρτα και συνδρομή.

Στα συν : ο χρήστης έχει επιλογή προγράμματος, καλή ποιότητα εικόνας – ήχου, μεγάλη εμβέλεια
Στα πλην : τις πλείστες φορές χρειάζεται σύνδεση internet

1.5.1.4 Με κλωνοποίηση κάρτας

4) Με κάρτα σωσία αυθεντικής πληρωμένης κάρτας: Άδεια ειδική κάρτα φορτώνεται με αρχεία που βρίσκει κάποιος στο ίντερνετ και εξομοιώνει τη λειτουργία γνήσιας πληρωμένης με συνδρομή κάρτα. Αυτές οι κάρτες δεν είναι κάτι νέο, απλά εξαφανίζονται με την έλευση νέου ή αναβαθμισμένου συστήματος κρυπτογράφησης από τις εταιρίες και εμφανίζονται αφού οι αρχιπειρατές σπάσουν (ανακαλύψουν) τον πλήρη αλγόριθμό κρυπτογράφησης με αντίστροφη μηχανική (reverse engineering). Το θέμα μελετάται στο κεφάλαιο 6.

Στα συν : Δε χρειάζεται ίντερνετ, καλή ποιότητα ήχου, εικόνας
Στα πλην: Αβέβαιο μέλλον, με μικροαλλαγές του συστήματος κρυπτογράφησης από τον πάροχο δεν μπορούν να δουλέψουν και αναγκαστική αγορά άλλης

1.6 Σύστημα Πρόσβασης υπό Όρους στην Ελλάδα

Αφού είδαμε τους συνηθέστερους τρόπους πειρατείας δορυφορικού σήματος, θα δούμε μια ιστορική αναδρομή στην Ελλάδα της εξέλιξης της πειρατείας στην αναλογική/ δορυφορική τηλεόραση.

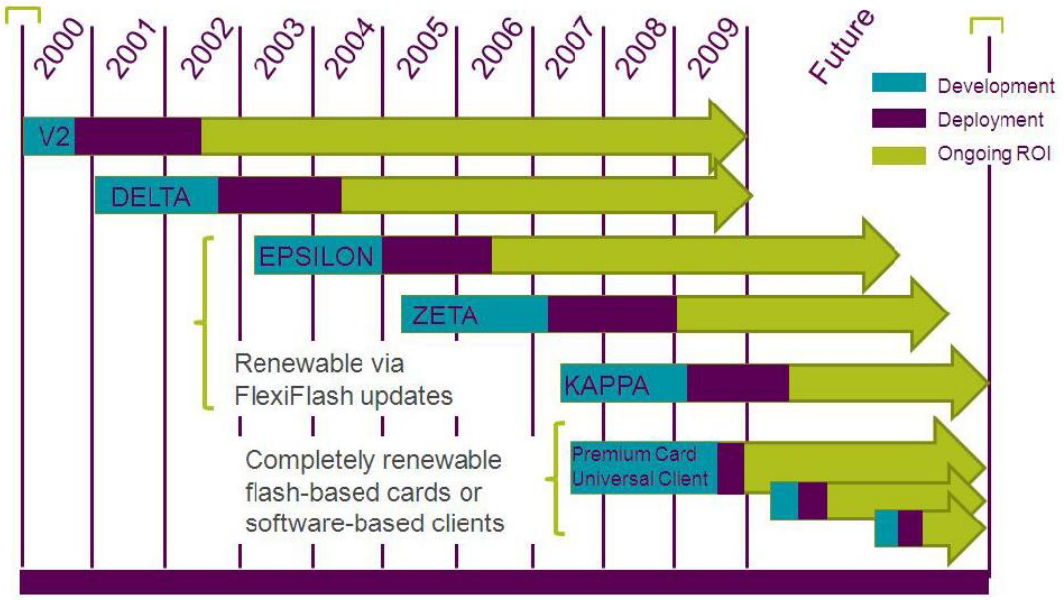
Στην αναλογική εποχή η Multichoice Hellas εξέπεμπε (ακόμα εκπέμπει) 2 κανάλια : τα filmnet (ταινίες πρώτης προβολής) και supersport (αθλητικά). Η πειρατεία γινόταν με τον πρώτο τρόπο ή με τον τρόπο επέμβασης στο δέκτη και τροποποίησης του κυκλώματος. Με την έλευση της δορυφορικής ψηφιακής εποχής , 2 ψηφιακά πακέτα εμφανίστηκαν : το nova και ο alpha digital. Ο δεύτερος σύντομα χρεοκόπησε αφού έκανε υπερβολικές δαπάνες χωρίς πλάνο. Δεν υπάρχει πληροφορία για το σύστημά του. Πέρασαν 10 χρόνια και από τότε μόλις τώρα (τέλη 2009) ετοιμάζετε δεύτερος πάροχος να εκπέμψει (OTE –ConnX) με άγνωστο σύστημα κρυπτογράφησης. Έτσι εξετάζουμε μόνο την περίπτωση της Nova(ή Νόβα) που εκπέμπει στο σύστημα irdeto.

Το σύστημα πρόσβασης Irdeto είναι ολλανδικής προέλευσης και ανήκει σήμερα στον όμιλο Naspers που ελέγχει και αρκετά συνδρομητικά πακέτα. Ιδρύθηκε το 1969 από ένα μηχανικό τον Pieter den Toonder στο Dordrecht της Ολλανδίας. Υπήρξε από τα πρώτα συστήματα που χρησιμοποιήθηκαν στην Ευρώπη, παλαιότερα μάλιστα η διάδοση του ήταν αρκετά μεγαλύτερη, καθώς εκτός του ελληνικού πακέτου υποστήριζε αρκετά ευρωπαϊκά. Αριθμεί σήμερα 900 υπαλλήλους και έχει συνάψει συμφωνίες με κορυφαίους παρόχους κινητών, δορυφορικών και IPTV σε Ευρώπη Ασία και Αφρική. Το Irdeto ήταν το πρώτο ψηφιακό κλείδωμα που έσπασε, από τις αρχές του 1999! Η πειράτευση έγινε με τις πρώτες εμπορικού τύπου κάρτες, που ονομάζονταν Hornet (υπήρχαν και άλλες λιγότερο γνωστές) και οι οποίες πωλούνταν σε εκδόσεις με 1 έως 3 πακέτα Irdeto (διαφορετικού κόστους εννοείται). Με τις κάρτες αυτές, ήταν ορατή και η Nova πάνω από ένα χρόνο πριν από την εμπορική της λειτουργία κατά την περίοδο των δοκιμών.

Όμως, τα πακέτα άρχισαν να παίρνουν αντίμετρα, αλλάζοντας κωδικούς και γύρω στα μέσα του 1999 σταμάτησε η υποστήριξη των καρτών, που συνέχισαν να δείχνουν για λίγο ακόμη μόνο τα πακέτα που δεν άλλαζαν κωδικούς. Στα μέσα του 1999 αρχίζουν να εμφανίζονται στο διαδίκτυο ιστοσελίδες ή φόρουμ που παρέχουν πληροφορίες για το σύστημα Irdeto και όσοι διαθέτουν μία ληγμένη κάρτα Irdeto μπορούν να την απενεργοποιήσουν.

Η Nova ξεκινά την εμπορική της λειτουργία στα τέλη του 1999 αλλά στις αρχές του 2000 η απλή επανενεργοποίηση γνήσιων ληγμένων καρτών (mosc) εξελίσσεται σε ...κλωνοποίηση άλλων γνήσιων καρτών, που έχουν συνδρομή, με αποτέλεσμα και οι αλλαγές κωδικών να μην είναι αρκετές για να κλείσουν τις κοινοποιημένες πλέον κάρτες ούτε καν προσωρινά, ενώ από τα μέσα περίπου του 2000 η διαδικασία της κλωνοποίησης είναι εφικτή και σε πάμφθηνες goldwafer cards, οι οποίες εκτός από το πακέτο της Νόβα μπορούν και να λειτουργήσουν με περισσότερα πακέτα Irdeto! Η ελληνική αγορά πλημμυρίζει από τέτοιες κάρτες και οποιοσδήποτε κατέχει ένα υπολογιστή, μπορεί να φτιάξει τέτοιες κάρτες με αρχεία που θα βρει στο διαδίκτυο ή που θα «διαβάσει» απλά από μία γνήσια συνδρομητική κάρτα, κάνοντας ένα hexmasterkey extraction(είναι το user key που θα δούμε στο κεφάλαιο με τις έξυπνες κάρτες).

Οι κάρτες αυτές κυκλοφορούν επί ένα χρόνο και κάτι, στην Ελλάδα και στο εξωτερικό , και η Nova, όπως και τα άλλα πακέτα σε Irdeto, έχουν μεγάλο πρόβλημα (οι πρώτες τέτοιες κάρτες λειτούργησαν αδιάλειπτα για 16 περίπου μήνες). Η μόνη λύση που είχαν τα πακέτα και η Irdeto ήταν η ολική αλλαγή του συστήματος CAS. Αυτό ήταν το Irdeto2 το οποίο αναγκαστικά για να λειτουργήσει απαιτήθηκε αλλαγή όλων των καρτών των συνδρομητών. Η Nova ολοκλήρωσε την αλλαγή αυτή τον Οκτώβριο του 2001. Από τότε το σύστημα έχει παραμείνει το Irdeto2, ενώ έχουν παρουσιαστεί νέες εκδόσεις καρτών οι οποίες φαίνονται στο σχήμα 7 από το site της Irdeto.



Σχήμα 7: Όλες οι εκδόσεις καρτών του συστήματος CAS της Irdeto

Στο σχήμα φαίνονται οι δύο πρώτες εκδόσεις 2 και 4 που υπάρχουν ακόμα στη Νόβα όπως και οι Ζήτα και Κάπα (Ελληνικά ονόματα μάλλον κάποιος David Canellos που βρίσκεται στους επικεφαλείς θα τα πρότεινε).Οι κάπα είναι οι πιο νέες που παρουσιαστήκαν στη Νόβα και μπορούν(όπως και οι Έψιλον και Ζήτα) να αναβαθμίσουν το λογισμικό τους από το δορυφορικό σήμα(FlexiFlash) χωρίς να αλλαχτεί η κάρτα όπως παλιά. Από τον Οκτώβριο του 2009 η Νόβα άρχισε να αναβαθμίζει μέσω αυτής της τεχνολογίας την ασφάλεια αυτών των καρτών. Επιπλέον οι Κάπα είναι οι πρώτες κάρτες που χρησιμοποιούν την τεχνολογία παντρέματος κάρτας με δέκτη (SS=Secure Silicon) για αντιμετώπιση της card sharing πειρατείας που θα δούμε πιο κάτω.

Τέλος του Αυγούστου του 2009 παρουσιάζεται από την Irdeto το CAS Irdeto3 με σκοπό την καλύτερη ασφάλεια της επένδυσης των παρόχων , ήδη ανακοινώθηκε στο τέλος του 2009 οι πρώτες μετατροπές παρόχων στην τρίτη έκδοση. Στη Νόβα δεν υπάρχει οποιαδήποτε ενημέρωση ακόμα (Οκτώβριος 2009) για αλλαγή σε Irdeto3.

1.7 Βιβλιογραφία

Digital TelevisionSatellite, Cable, Terrestrial,IPTV, Mobile TV in theDVB Framework
Third Edition: Hervι Benoit

Digital Video and Audio Broadcasting Technology A Practical Engineering Guide Second Edition: Walter Fischer

Περιοδικό ‘’tv sat’’ έκδοση Ιανουάριος 2007
Περιοδικό ‘’Δορυφορικά Νέα’’ έκδοση Ιανουάριος 2008

www.wikipedia.org
www.irdeto.com

Κεφάλαιο 2 : Δομή εικόνας –κρυπτογραφία σήματος

2.1 Εισαγωγή

Αν θέλαμε να κάνουμε μια ιστορική ανάδρομη στην τεχνολογία της κρυπτογράφησης εικόνας-ήχου θα χωρίζαμε την ιστορία στις τρεις ακόλουθες φάσεις :

- αναλογική τηλεόραση
- στα ημιψηφιακά συστήματα
- πλήρη ψηφιακά συστήματα

Μια ιστορική ανάδρομη για τα τρία συστήματα με λεπτομέρειες για τον καθένα μας δίνει το άρθρο του περιοδικού Δορυφορικά Νέα Νοέμβριος 2007

Στην αναλογική τηλεόραση εφαρμόστηκαν ανώριμες λύσεις, που συχνά κατέληξαν σε δημόσιο εξευτελισμό και γελοιοποίηση των «ειδικών». Χρησιμοποιήθηκε κάθε λογής κόλπα πάνω στο αναλογικό τηλεοπτικό σήμα ώστε να το κάνει ακατάληπτο. Αναστροφή του φασματικού περιεχομένου, αλλαγή, αλλοίωση και αναδιάταξη της σειράς εκπομπής των γραμμών του ράστερ εικόνας, εξαφάνιση των παλμών συγχρονισμού, ανάμιξη με σήματα παρεμβολής... σε κάθε περίπτωση πάντως, η κύρια ιδέα ήταν το «ανακάτεμα», η «αναδόμηση» και το «μπέρδεμα» των παραμέτρων του τηλεοπτικού σήματος. Γι' αυτό και όλες αυτές οι τεχνικές ονομάστηκαν συλλήβδην «video scrambling». Η αναλογική κρυπτογράφηση δεν πέτυχε πάντως σπουδαία αποτελέσματα! Ούτε η τελική εικόνα -μετά την αποκρυπτογράφηση- ήταν ικανοποιητική ούτε η ασφάλεια της μετάδοσης υψηλή. Τη μια μέρα έμπαινε το σύστημα σε εμπορική εκμετάλλευση και την άλλη είχαν δημοσιευθεί οι λεπτομέρειες της αποκωδικοποίησης! Η κατάσταση είχε εξελιχθεί σχεδόν σε πόλεμο εκ του συστάδην. Πολλοί είχαν ως χόμπι το «σπάσιμο» των νέων τηλεοπτικών συστημάτων κρυπτογραφίας. Είχαν οργανωθεί μάλιστα και «λέσχες των hackers του Χ συστήματος». Τότε το Internet ήταν ακόμη στα σπάργανα και οι «ανακοινώσεις» γίνονταν κυρίως μεταξύ ομάδων από «επαΐοντες», είτε μέσα από ειδικευμένα περιοδικά είτε από στόμα σε στόμα για αυτό και απέπνεαν το άρωμα του «τεχνολογικού μυστικισμού».

Το πρώτο τηλεοπτικό ευρωπαϊκό κανάλι που χρησιμοποίησε «σοβαρή» κρυπτογραφία, ήταν το γαλλικό Canal+ το 1984 Ήταν μια αναλογική λύση, που έκρυβε ψήγματα ψηφιακής τεχνολογίας. Εισήγαγε «τεχνητή καθυστέρηση» στις γραμμές σάρωσης του ράστερ (Horizontal Line Delay). Κάθε γραμμή υφίσταται διαφορετική ψευδοκαθυστέρηση με τη χρήση ειδικών κυκλωμάτων, που ονομάζονται delay lines και είχαν ήδη χρησιμοποιηθεί στο σύστημα SECAM. Για την κρυπτογράφηση του ήχου χρησιμοποιήθηκε απλή αναστροφή του φασματικού περιεχομένου (spectrum inversion), τεχνική που είχε τις ρίζες της στα στρατιωτικά συστήματα των αρχών της δεκαετίας του 1950. Μέσα σε ένα μήνα το περιοδικό Radio Plans είχε δημοσιεύσει έναν «πειραματικό» αποκωδικοποιητή, που τον έδινε μάλιστα και συναρμολογημένο. Η γελοιοποίηση του πρώτου κρυπτογραφικού εγχειρήματος μεγάλης πνοής, έκοψε την ορμή της τεχνολογίας και λίγο έλειψε να οδηγήσει το Canal+ σε χρεοκοπία. Πιο επαγγελματική προσπάθεια έγινε από το ολλανδικό FilmNet το 1986, το οποίο εισήγαγε το σύστημα κρυπτογράφησης VideoCipher και την τεχνική της απαλοιφής των παλμών συγχρονισμού έκανε όμως το «λάθος» να προβάλει ταινίες

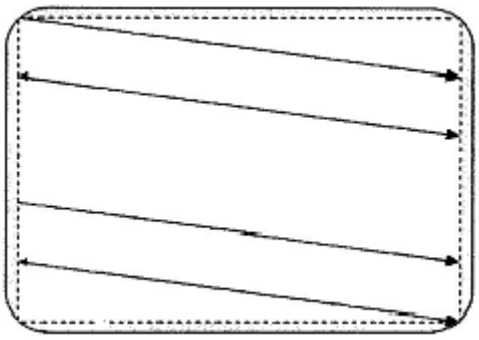
προχωρημένου πορνογραφικού περιεχομένου, κάτι σπάνιο για εκείνη την εποχή. Αυτή η «πρωτοποριακή» προσφορά λειτούργησε σαν μαγνήτης για όλους τους hackers, οι οποίοι θεώρησαν θέμα τιμής την άλωση του καινοφανούς κρυπτοσυστήματος .

Οι καλύτεροι «κρυπτοπειρατές» της Ευρώπης εργάστηκαν νυχθημερόν με ζήλο και αυταπάρνηση και το σύστημα κατέρρευσε μέσα στα επόμενα δύο χρόνια. Έκτοτε συνεχίστηκε αυτό το παιχνίδι με συνεχείς αναγγελίες νέων συστημάτων και ισάριθμες τεχνολογικές ήττες. Η αναλογική τεχνολογία ήταν κρυπτογραφικά θνησιγενής.

Η κατάσταση, όμως έγινε πολύ δυσκολότερη με την εμφάνιση της ψηφιακής τεχνολογίας. Τα αστεία τελείωσαν και η πειρατική αγορά πάγωσε (καταρχήν). Το «σπάσιμο» ακόμη και του πιο απλού συστήματος ψηφιακής κρυπτογράφησης απαιτούσε πολλά χρόνια σπουδών, βαθιά γνώση και ειδίκευση, σοβαρές υποδομές και άφθονους πόρους. Η επιχείρηση έγινε ασύμφορη και όσες περιπτώσεις κρυπτανάλυσης ψηφιακών τηλεοπτικών συστημάτων αναγγέλλονται κατά καιρούς, δεν οφείλονταν σε ερασιτέχνες πειρατές ή χομπίστες αλλά είτε σε λάθος σχεδιασμένα συστήματα, είτε σε στρατηγικές marketing, των εταιρειών για δωρεάν θέαση ,είτε σε αντίπαλες εταιρείες (Μέρτοχ και NDS κατά MediaGuard),είτε σε επαγγελματίες πειρατές που δαπανούν πολύ χρήμα με σκοπό την απόσβεση και το κέρδος. Δυστυχώς ή ευτυχώς, η ψηφιακή τεχνολογία είναι πολύ ισχυρή κρυπτογραφικά

2.2 Δομή της τηλεοπτικής εικόνας

Η κρυπτογράφηση αναλογικού σήματος είναι ‘’απλή’’ υπόθεση αντίθετα .Αντίθετα, είναι δύσκολη η σωστή αποκρυπτογράφηση, γιατί υποβαθμίζει την ποιότητα και αφήνει στην αρχική εικόνα διάφορα «κουσούρια». Το μάτι είναι εξαιρετικά απαιτητικό, αναλυτικό και ευαίσθητο οπτικό όργανο ακριβείας. Μπορεί να εντοπίσει ασήμαντες χρωματικές και γεωμετρικές αλλοιώσεις της εικόνας. Επομένως, όλα τα λάθη κατά τον επανασχηματισμό της, γίνονται αντιληπτά και δεν κρύβονται. Αυτός είναι και ένας από τους λόγους της βραδείας εξέλιξης των συστημάτων κρυπτογράφησης εικόνας. Για να γίνουν κατανοητές οι τεχνικές της αναλογικής τηλεοπτικής κρυπτογράφησης, πρέπει να αναφερθεί τόσο ο τρόπος σχηματισμού της τηλεοπτικής εικόνας που ονομάζεται «ράστερ», όσο και ο τρόπος μετάδοσης του έγχρωμου τηλεοπτικού αναλογικού σήματος. Για τη σάρωση της εικόνας, η ηλεκτρονική δέσμη εκτελεί ταυτόχρονα δύο κινήσεις, μία οριζόντια από αριστερά προς τα δεξιά και μία κατακόρυφη, από πάνω προς τα κάτω. Το ευρωπαϊκό πρότυπο τηλεόρασης προβλέπει ότι η εικόνα αναλύεται σε 625 οριζόντιες γραμμές σάρωσης. Επομένως, στο χρόνο που χρειάζεται να σαρωθεί η εικόνα μια φορά από πάνω προς τα κάτω. πρέπει να σαρωθεί 625 φορές από αριστερά προς τα δεξιά όλα αυτά πρέπει να επαναλαμβάνονται 25 φορές το δευτερόλεπτο. Με τον τρόπο αυτό, η σάρωση δημιουργεί ένα γεωμετρικό σχήμα από παράλληλες γραμμές, με ελαφρά κλίση προς τα κάτω δεξιά, το οποίο ονομάζεται **ράστερ.** Η συχνότητα γραμμών είναι 25 χ 625=15.625Hz. ενώ η περίοδος γραμμών είναι 1/15625=64psec. Για να αναπαράγεται μια τηλεοπτική εικόνα σταθερά και σωστά στην οθόνη, πρέπει οι κινήσεις της δέσμης να εξελίσσονται ταυτόχρονα στον πομπό και στον τηλεοπτικό δέκτη. Η συνθήκη αυτή ονομάζεται **συγχρονισμός** και εξασφαλίζεται με την εκπομπή μιας σειράς παλμών, οι οποίοι ονομάζονται **παλμοί συγχρονισμού.**



Το **ράστερ τ**ης τηλεοπτικής εικόνας σχηματίζεται από τις δύο ταυτόχρονες κινήσεις που εκτελεί η ηλεκτρονική δέσμη, μία οριζόντια από αριστερά προς τα δεξιά και μία κατακόρυφη από πάνω προς τα κάτω. Όσο χρόνο η ηλεκτρονική δέσμη κινείται από αριστερά προς τα δεξιά, κινείται ελάχιστα και προς τα κάτω. Όταν επιστρέφει στο αριστερό άκρο. επαναλαμβάνει την ίδια κίνηση, αρχίζοντας από ελαφρά χαμηλότερη θέση. Μία κατηγορία τεχνικών αναλογικής κρυπτογράφησης της τηλεοπτικής εικόνας, βασίζεται στο «μπέρδεμα» (scrambling) αυτών των κινήσεων της δέσμης. Στην **«αναστροφή γραμμής»** (Line Inversion) η δέσμη κινείται με την αντίθετη φορά. Στην **«αναδιάταξη γραμμών»** (Line Shuffle) οι γραμμές της δέσμης ανακατεύονται και χάνεται η αρχική σειρά. Η καλύτερη και πιο πολύπλοκη μέθοδος ονομάζεται **«κοπή και αλλαγή»** (Cut and Rotate). Οι γραμμές σάρωσης «κόβονται» στα δύο. σε 256 προκαθορισμένα σημεία και τα κομμάτια επανασυνδέονται μεταξύ τους. φτιάχνοντας μια αναδομημένη γραμμή σάρωσης. Αυτό επαναλαμβάνεται σε όλες τις γραμμές και το τελικό αποτέλεσμα παράγει μια εντελώς ασαφή εικόνα. Το σύστημα αποτελεί μια επιτυχημένη στιγμή της αναλογικής κρυπτογράφησης και χρησιμοποιήθηκε μέχρι πρόσφατα με την εμπορική ονομασία **VideoCrypt** Μπορείτε να φανταστείτε κάποια άλλη μορφή αλλοίωσης των γραμμών, που να είναι όμως, αναστρέψιμη και να αποδίδει μετά την αποκατάσταση την αρχική εικόνα; Αν σκεφτείτε κάτι που δεν ανακαλύφθηκε τα προηγούμενα χρόνια, ίσως να βρήκατε το νέο σύστημα κρυπτογράφησης, που θα σας κάνει πλούσιους. Αν και καλύτερα να στρέψετε τις προσπάθειες σας στην ψηφιακή κρυπτογραφία εικόνας, που υπόσχεται καλύτερα αποτελέσματα.

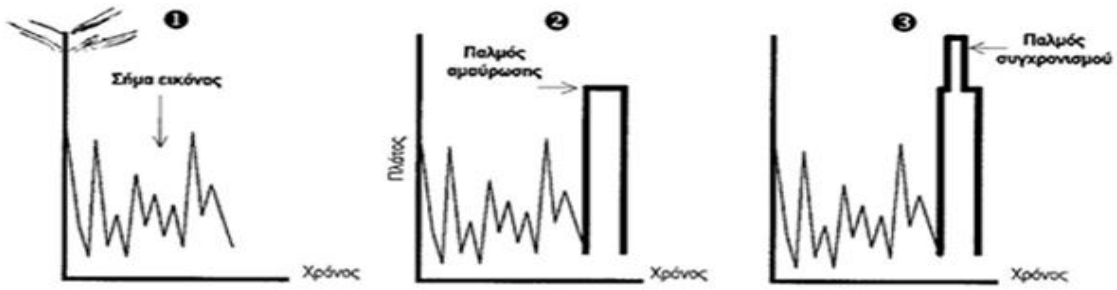
2.2.1 Συνιστώσες τηλεοπτικού σήματος

Το τηλεοπτικό σήμα αποτελείται από συνδυασμό τριών ξεχωριστών συνιστωσών:

- Το **σήμα εικόνας** με τις πληροφορίες φωτεινότητας και χρωματικότητας της εικόνας. Η μορφή του είναι σχεδόν τυχαία, αλλά το πλάτος του κυμαίνεται πάντοτε μεταξύ του 10% (απόλυτα λευκό) και του 75% (απόλυτα μαύρο) του ολικού πλάτους.

- Τους **παλμούς αμαύρωσης,** που κάνουν αόρατες τις γραμμές επιστροφής των σαρώσεων. Οι παλμοί αμαύρωσης ξεκινούν λίγο πριν την έναρξη κάθε επιστροφής της δέσμης σάρωσης και διαρκούν μέχρι την αρχή της επόμενης σάρωσης. Υπάρχουν παλμοί αμαύρωσης γραμμών που καλύπτουν τις οριζόντιες επιστροφές της δέσμης και παλμοί αμαύρωσης πεδίων, που καλύπτουν τις κατακόρυφες επιστροφές.

- Τους **παλμούς συγχρονισμού,** που συγχρονίζουν τη σάρωση στον πομπό και στο δέκτη. Οι παλμοί αυτοί έχουν ειδική θέση μέσα στο τηλεοπτικό σήμα. γιατί τοποθετούνται πάντοτε στην οροφή των παλμών αμαύρωσης. Υψώνονται μέχρι το 100% του πλάτους του τελικού σήματος και γι' αυτό αντιπροσωπεύουν σήμα «πιο μαύρο από το μαύρο». Το γεγονός αυτό βοηθάει τα κυκλώματα του δέκτη να τους ξεχωρίζουν εύκολα από το υπόλοιπο τηλεοπτικό σήμα.



Οι τρεις συνιστώσες του σύνθετου τηλεοπτικού σήματος: Παρατηρήστε ότι στο σχήμα οι παλμοί συγχρονισμού έχουν το μέγιστο προς τα πάνω (θετική πολικότητα). σε αντίθεση με την πραγματικότητα, όπου οι παλμοί έχουν αντίθετη φορά (αρνητική πολικότητα). Μία απλοϊκή τεχνική κρυπτογράφησης αντιστρέφει την **«πολικότητα»** (video polarity inversion) όλου του σήματος. Το αποτέλεσμα είναι, στο δέκτη, η εικόνα να φαίνεται όπως το αρνητικό φιλμ της φωτογραφίας. Αυτή η τεχνική υποφέρει από χαμηλή αφάνεια (obscurity), δηλαδή είναι εύκολα αναγνώσιμη. Σε προβολές προγράμματος με ειδικό ενδιαφέρον και χαμηλή απαίτηση ευκρίνειας- όπως συμβαίνει για παράδειγμα στις αισθησιακές ταινίες- αυτή η ιδιομορφία παραβλέπεται. Παλαιότερα υπήρχε σημαντικό τμήμα διψασμένου τηλεοπτικού κοινού, που δεν το πτοούσαν τέτοιες «επουσιώδεις λεπτομέρειες».

2.3 Συστήματα αναλογικής κρυπτογράφησης

Ιδιαίτερο χαρακτηριστικό των αναλογικών συστημάτων κρυπτογράφησης ήταν ότι δεν απαιτούσαν κλειδί αποκρυπτογράφησης. Όλη η απαραίτητη πληροφορία λήψης υπήρχε έτοιμη μέσα στους αποκωδικοποιητές που προσέφεραν οι εταιρείες και ο τηλεθεατής απλώς τους συνέδεε στην τηλεόραση. Γι' αυτό και η διαδικασία ονομαζόταν **scrambling,** δηλαδή αναδιάταξη των παραμέτρων του σήματος με τη βοήθεια κάποιου σταθερού αλγόριθμου, που ήταν εξαρχής γνωστός στον αποκωδικοποιητή. Δεν άλλαζε, ήταν μυστικός και τον περιείχε ένα ειδικό μικροκύκλωμα EPROM όμως, κρυπτογράφηση με μυστικό αλγόριθμο είναι εξαρχής καταδικασμένη σε αποτυχία. Σύμφωνα με τη βασική αρχή της Κρυπτογραφίας, που λέγεται και αρχή του Kircoff, η ισχύς πρέπει να περιέχεται στο κρυπτογραφικό κλειδί και όχι στον κρυπτοαλγόριθμο, ο οποίος οφείλει να είναι γνωστός και δημόσια ανακοινωμένος. Η λέξη scrambling δεν αποδόθηκε ποτέ με κατάλληλη ελληνική μετάφραση, επειδή εκείνη την εποχή, από το 1985-1995 αυτή η κρυπτοτεχνολογία δεν χρησιμοποιήθηκε στη χώρα μας, αλλά μόνον στα καλωδιακά δίκτυα της Αμερικής και της Βόρειας Ευρώπης. Τότε η δορυφορική λήψη ήταν ακόμη στα σπάργανα, είχε υψηλό κόστος υποδομών και μικρή διείσδυση στο τηλεοπτικό κοινό. Η λέξη **encryption** (κρυπτογράφηση), η οποία αναφέρεται στη διαδικασία μεταφοράς της κρυπτογραφικής κλείδας, χρησιμοποιήθηκε σπάνια. Η κρυπτογραφική κλείδα αποτελεί εφεύρημα της ψηφιακής τεχνολογίας και περιέχεται στην κάρτα πρόσβασης, τη smart card.

Μερικές από τις τεχνικές κρυπτογράφησης εικόνας που χρησιμοποιήθηκαν την αθώα εποχή της αναλογικής τηλεόρασης, πριν την ψηφιακή επέλαση, είναι:

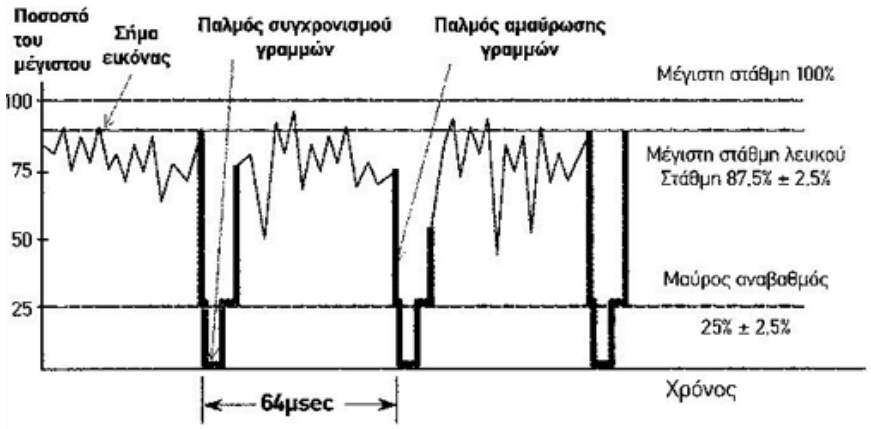
- Η **«αναστροφή γραμμής»** (Line Inversion Video Scrambling), κατά την οποία η δέσμη σάρωσης του ράστερ κινείται με την αντίθετη από την κανονική φορά. Πρόκειται για απλή και φτηνή μέθοδο - είναι και η πρώτη που μπήκε σε εμπορική εκμετάλλευση- που δίνει χαμηλή ποιότητα κρυπτογραφικής εικόνας, χαμηλή κρυπτοασφάλεια και μεγάλη αναγνωσιμότητα της κρυπτοεικόνας. Ένα από σοβαρά μειονεκτήματα των αναλογικών μεθόδων είναι η χαμηλή αφάνεια (obscurity), δηλαδή το γεγονός ότι η εικόνα είναι εύκολα αναγνώσιμη.

- Παρόμοια πλεονεκτήματα και μειονεκτήματα είχε και η **«αναστροφή της πολικότητας»** του τηλεοπτικού σήματος (video polarity inversion). Το αποτέλεσμα είναι ότι στο δέκτη η εικόνα φαίνεται όπως το αρνητικό φιλμ της φωτογραφίας. Σε προβολές προγράμματος με ειδικό ενδιαφέρον και χαμηλή απαίτηση ευκρίνειας- όπως συμβαίνει για παράδειγμα στις αισθησιακές ταινίες- αυτή η ιδιομορφία παραβλέπεται και υπήρχε σημαντικό τμήμα ειδικού τηλεοπτικού κοινού, που δεν το πτοούσαν τέτοιες «επουσιώδεις λεπτομέρειες». Κάποια εποχή μάλιστα, η παρακολούθηση τέτοιων ταινιών με ανεστραμμένο video είχε αποκτήσει cult χαρακτήρα!

- Στην **«αναδιάταξη γραμμών»** (Line Shuffle Video Scrambling) οι γραμμές του ράστερ ανακατεύονται, αναδιατάσσονται και χάνεται η αρχική σειρά. Δίνει καλή τελική εικόνα και έχει υψηλή αφάνεια. Απαιτεί όμως κύκλωμα μνήμης και δημιουργεί αστάθεια στο συγχρονισμό των κυκλωμάτων. Η σειρά αναδιάταξης είναι συγκεκριμένη και γνωστή στον αποκωδικοποιητή. Προσφέρθηκε στην αγορά με την εμπορική ονομασία **View Guard** και χρησιμοποιήθηκε στα καλωδιακά δίκτυα της Αμερικής ABC και FOX. Ένα παρόμοιο σύστημα, με την εμπορική ονομασία VideoCipher, σχεδιάστηκε από τη Linkabit Systems και χρησιμοποιούσε σαν αλγόριθμο αλλαγής της σειράς των γραμμών σάρωσης, τον άσπαστο τότε κρυπτοαλγόριθμο DES. Χρησιμοποιήθηκε από το δίκτυο CBS μέχρι το 1998. αλλά και στον πρώτο τηλεοπτικό δορυφόρο Telstar 301, το 1995.

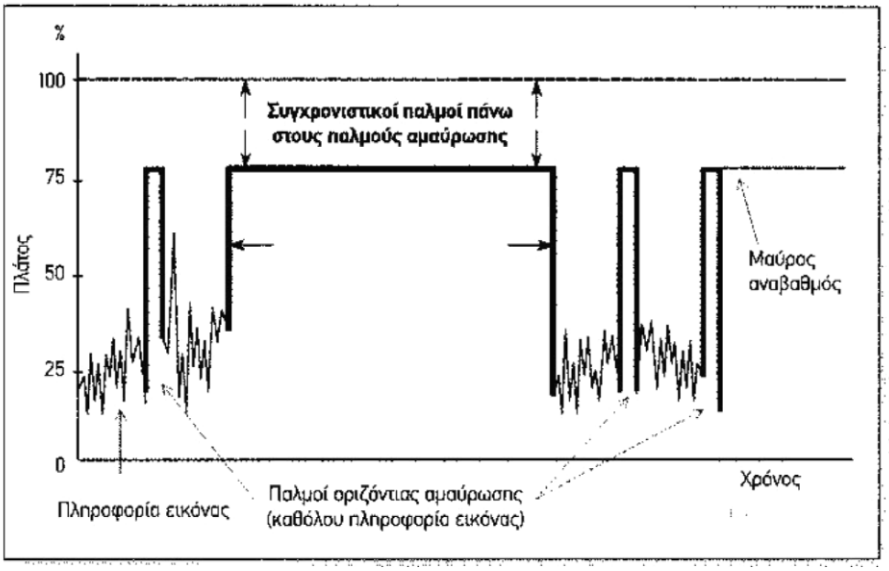
- Μία έξυπνη και ικανοποιητική μέθοδος αναλογικής κρυπτογράφησης, ονομάζεται **«κοπή και αλλαγή»** των γραμμών του ράστερ (Cut and Rotate). Οι γραμμές σάρωσης «κόβονται» στα δύο, σε 256 προκαθορισμένα σημεία και τα κομμάτια αναδιατάσσονται μεταξύ τους. φτιάχνοντας μια νέα αναδομημένη γραμμή σάρωσης. Αυτό επαναλαμβάνεται σε όλες τις γραμμές και το τελικό αποτέλεσμα αποδίδει μια εντελώς ασαφή εικόνα, που μοιάζει σαν να ξεχειλώνει ή να συμπιέζεται περιοδικά. Αποτελεί μία από τις καλύτερες στιγμές των αναλογικών συστημάτων κρυπτογράφησης. Προσφέρθηκε στην αγορά με την εμπορική ονομασία **VideoCrypt** Χρησιμοποιήθηκε μέχρι το 1990 από όλα τα μεγάλα εμπορικά ευρωπαϊκά δίκτυα, κυρίως το British Sky Broadcasting (BSB). χωρίς κρυπτογράφηση ήχου. Στο σύστημα αυτό χρησιμοποιήθηκε για πρώτη φορά «κάρτα πρόσβασης», που περιείχε τον αλγόριθμο αλλαγής των σημείων κοπής των γραμμών σάρωσης. Η κάρτα περιείχε επίσης για πρώτη φορά, έλεγχο πιστοποίησης της γνησιότητας και απόρριψης από τον αποκωδικοποιητή, αν βρισκόταν πλαστή.

- Η **τεχνική «συμπίεσης ή απόκρυψης των παλμών συγχρονισμού»** (Sync Suppression) τους εξαφανίζει ή τους αλλάζει θέση, ώστε να μην μπορούν να τους βρουν τα κυκλώματα αποδιαμόρφωσης του δέκτη. Χωρίς αυτήν την πληροφορία, ο δέκτης ρολάρει την εικόνα σε βαθμό που κάνει την παρακολούθηση αδύνατη. Οι παλμοί συγχρονισμού μεταδίδονται με άλλον τρόπο, κρυμμένοι σε κάποιο άλλο σημείο του σήματος ή αναδημιουργούνται στο δέκτη με τη βοήθεια παράπλευρης πληροφορίας. Είναι φτηνή και αξιόπιστη μέθοδος, με ικανοποιητικά αποτελέσματα, αλλά προκαλεί προβλήματα συμβατότητας στο σύστημα **Secam**. Αυτήν την τεχνική εφάρμοσε το ολλανδικό **FiimNet.** το 1986, στο σύστημα κρυπτογράφησης **SatPac,** το οποίο εξελίχθηκε στη συνέχεια στο **VideoCypher.** Οι εξαφανισμένοι παλμοί συγχρονισμού επανασχηματίζονταν στο δέκτη, με τη χρήση ειδικού υποφέροντος σήματος συγχρονισμού, που χρησιμοποιούσε κυκλώματα κλειδώματος φάσης (Phase Locked Loop, PLL). Τότε αποτελούσε πρωτοποριακή τεχνολογία, αλλά η προσφορά στο εμπόριο των κυκλωμάτων PLL τα επόμενα χρόνια, εξαφάνισε το πλεονέκτημα και έκανε το σύστημα ευάλωτο και διάτρητο, μέχρις ότου εγκαταλείφθηκε. Το 1992. το FilmNet άλλαξε το σύστημα κρυπτογράφησης στο ημιψηφιακό και αδικοχαμένο (!) **D2-Mac** ή **EuroCrypt**



Σύνθετο αναλογικό τηλεοπτικό σήμα. Η συχνότητα επανάληψης των γραμμών είναι 25 χ 625=15.625Hζ. ενώ ο χρόνος διάρκειας κάθε γραμμής είναι 1/15625=64 μ*sec.* Για να αναπαράγεται μια τηλεοπτική εικόνα σταθερά και σωστά στην οθόνη, πρέπει οι κινήσεις της δέσμης να εξελίσσονται συγχρονισμένα στον πομπό και στον τηλεοπτικό δέκτη. Η συνθήκη αυτή εξασφαλίζεται με την εκπομπή μιας σειράς παλμών συγχρονισμού. Μια κατηγορία τεχνικών αναλογικής κρυπτογράφησης της τηλεοπτικής εικόνας, βασίζεται στη **«συμπίεση» ή «απόκρυψη» των παλμών συγχρονισμού** (Sync Suppression). Χωρίς αυτήν την πληροφορία, ο δέκτης ρολάρει την εικόνα σε βαθμό που κάνει την παρακολούθηση αδύνατη. Οι παλμοί συγχρονισμού μεταδίδονται με άλλο τρόπο, κρυμμένοι σε κάποιο διαφορετικό σημείο του σήματος ή αναδημιουργούνται στο δέκτη με τη βοήθεια παράπλευρης πληροφορίας. Αυτήν την τεχνική εφάρμοσε το ολλανδικό **FilmNet.** το 1986, στο σύστημα κρυπτογράφησης SatPac, το οποίο εξελίχθηκε στη συνέχεια στο VideoCipher. Οι εξαφανισμένοι παλμοί συγχρονισμού επανασχηματίζονται στο δέκτη, με τη χρήση ειδικού υποφέροντος σήματος (subcarrier) συγχρονισμού και κυκλωμάτων κλειδώματος φάσης (Phase Locked Loop. PLL). Τότε αποτελούσε πρωτοποριακή τεχνολογία, αλλά η προσφορά στο εμπόριο των κυκλωμάτων PLL εξαφάνισε το πλεονέκτημα και έκανε το σύστημα ευάλωτο και διάτρητο, μέχρις ότου εγκαταλείφθηκε. Το 1992. το FilmNet άλλαξε το σύστημα κρυπτογράφησης στο D2-Mac ή EuroCrypt.

Μετά τη σάρωση όλων των γραμμών ενός πεδίου, ακολουθεί ένας παλμός αμαύρωσης πεδίων. Αυτός ο παλμός έχει πολύ μεγαλύτερη διάρκεια από τους παλμούς συγχρονισμού γραμμών και προσφέρεται σαν ιδανικό σημείο ένθεσης διάφορων «μυστήριων» σημάτων κρυπτογράφησης. Σε μια «προηγμένη» τεχνική αναλογικής κρυπτογράφησης, τοποθετούμε μέσα στον παλμό συγχρονισμού πεδίων ένα σήμα με συχνότητα 93.750kHz. που είναι εξαπλάσια από τη συχνότητα ανανέωσης γραμμών. Το σήμα αυτό **«πολυπλέκεται»** με το αρχικό σήμα, το μπερδεύει και «τρελαίνει» τα κυκλώματα αποδιαμόρφωσης του δέκτη, που δεν μπορούν να ξεχωρίσουν το σήμα παρεμβολής από την αυθεντική πληροφορία (Sine multiplex). Αυτό το σύστημα αναλογικής κρυπτογράφησης προσφέρθηκε με την εμπορική ονομασία **Tetease** ή **Sat Tel.** χρησιμοποιήθηκε μέχρι πρόσφατα από το BBC World Service και το κινηματογραφικό κανάλι Premiere. Αποτέλεσε το τελευταίο εναπομείναν αναλογικό κρυπτογραφικό κατάλοιπο στο σημερινό ψηφιακό κόσμο.



Μια αναλογική λύση που κρύβει ψήγματα ψηφιακής τεχνολογίας, είναι η δημιουργία «τεχνητής χρονικής καθυστέρησης», διάρκειας από 900 έως 1800 nsec, στις γραμμές σάρωσης του ράστερ (Horizontal Line Delay). Κάθε γραμμή υφίσταται διαφορετική ψευδοκαθυστέρηση, με τη χρήση ειδικών κυκλωμάτων, που ονομάζονται delay lines και χρησιμοποιήθηκαν στο σύστημα Secam που χρησιμοποιεί παρόμοια τεχνολογία. Προσφέρθηκε στην αγορά με το όνομα **Discet** και χρησιμοποιήθηκε από το γαλλικό **Canal+,** το 1984. Αν και ήταν πολύ προηγμένη τεχνολογία για την εποχή της. βρέθηκε -άγνωστο γιατί- στο στόχαστρο των επιστημόνων hackers της εποχής. Το περιοδικό Radio Plans δημοσίευσε έναν «πειραματικό» αποκωδικοποιητή και το αποτέλεσμα λίγο έλειψε να οδηγήσει το δίκτυο στη χρεοκοπία.

Όταν όλες οι επιμέρους τεχνολογίες δοκιμασθούν και αποτύχουν, τότε το μόνο που απομένει είναι ο συνδυασμός τους. Έτσι έγινε και με το σύστημα **PayView,** που χρησιμοποιήθηκε από το γερμανικό κανάλι TeleClub, στις αρχές της δεκαετίας του 1990. Χρησιμοποίησε ταυτόχρονα αναστροφή video, μετατόπιση των παλμών συγχρονισμού και τεχνητή καθυστέρηση στη διάρκεια των παλμών σάρωσης. Δεν σημείωσε ιδιαίτερη επιτυχία και μετά από πέντε χρόνια παραχώρησε τη θέση του στην ψηφιακή τεχνολογία.

Όλα αυτά τα συστήματα απαιτούσαν ειδικά, ακριβά και πολύπλοκα για το τηλεοπτικό σήμα ήταν ασθενές, δεν λειτουργούσαν καθόλου, δημιουργώντας μεγάλα προβλήματα στους παροχείς της υπηρεσίας. Έτσι εφαρμόστηκαν με επιτυχία μόνο στις χώρες που λειτουργούσαν καλωδιακά δίκτυα και δημιούργησαν ένα τηλεοπτικό χάσμα, χωρίζοντας τις χώρες σε προηγμένο τηλεοπτικό Βορρά και τριτοκοσμικό Νότο. Στις χώρες με καλωδιακή τηλεοπτική υποδομή προσφέρονταν κινηματογραφικές ταινίες τελευταίας παραγωγής και ακριβές παραγωγές υψηλής ποιότητας, ενώ δημιουργήθηκαν και ειδικά κανάλια θεματικού περιεχομένου, όπως για παράδειγμα, τα γνωστά Discovery, Animal Planet, National Geographic κ.ά. Οι υπόλοιποι έμειναν με τηλεοπτικό περιεχόμενο χαμηλού επιπέδου και χαμηλού κόστους. διάφορες σκουπιδοπαραγωγές. που εντέλει ζημίωσαν την αντίληψη για την τηλεόραση και τη μετέτρεψαν σε «χαζοκούτι». Έτσι, επί πολλά χρόνια, η κρυπτογράφηση των τηλεοπτικών προγραμμάτων καρκινοβατούσε και δεν μπορούσε να αξιωθεί εμπορική επιτυχία και να συμπαρασύρει και την ποιότητα των προγραμμάτων Έπρεπε να έρθει η εποχή της ψηφιακής τεχνολογίας για να αλλάξει το σκηνικό.

2.4 Ημιψηφιακά συστήματα και έξυπνες κάρτες

Στις αρχές της δεκαετίας του 1990 έγινε μια πολύ σημαντική αλλαγή στα συστήματα κρυπτογράφησης τηλεοπτικής εικόνας. Εγκαταλείφθηκαν οι απλοϊκές αναλογικές τεχνολογίες και άρχισαν να χρησιμοποιούνται τα ημιψηφιακά (quasi-digital) συστήματα. Η ημιψηφιακή τεχνολογία δεν μεταβάλλει τη γνωστή μορφή του τηλεοπτικού σήματος. Αυτό έγινε αργότερα με την τεχνολογία DVB (Κεφάλαιο 3) η οποία χρησιμοποίησε το πρότυπο MPEG-2 (Κεφάλαιο 3), για να ψηφιοποιήσει και να αλλάξει εντελώς την τεχνολογία μετάδοσης από αναλογική σε ψηφιακή. Απλώς, πάνω στην αναλογική τεχνολογία χρησιμοποίησε ψηφιακές τεχνικές ελέγχου της μετάδοσης, εισάγοντας την πρώτη εκδοχή του CAM (Conditional Access Module).Η χρήση της «έξυπνης κάρτας πρόσβασης» (CA smart card), η οποία ελέγχει τα δικαιώματα στη λήψη , αποτελούσε καινοτομία όχι μόνον τεχνολογικά, αλλά και στο στιλ! Έδινε στους δέκτες περισσότερο «επαγγελματική» (professional) μορφή και απέτρεπε τους περιστασιακούς τζαμπατζήδες και ερασιτέχνες χάκερς από «πειρα(μα)τικούς τυχοδιωκτισμούς». Ιδιαίτερο χαρακτηριστικό των απλών αναλογικών συστημάτων κρυπτογράφησης, ήταν ότι δεν απαιτούσαν κλειδί αποκρυπτογράφησης. Όλη η απαραίτητη πληροφορία λήψης υπήρχε έτοιμη μέσα στους αποκωδικοποιητές που προσέφεραν οι εταιρείες και ο τηλεθεατής απλώς τους συνέδεε στην τηλεόραση. Η διαδικασία κρυπτογράφησης δεν άλλαζε, ήταν μυστική και την περιείχε ένα ειδικό μικροκύκλωμα. Όμως κρυπτογράφηση με μυστικό αλγόριθμο, είναι εξαρχής καταδικασμένη σε αποτυχία. Σύμφωνα με τη βασική αρχή της Κρυπτογραφίας, η ισχύς πρέπει να περιέχεται στο κρυπτογραφικό κλειδί και όχι στον αλγόριθμο, ο οποίος οφείλει να είναι γνωστός και δημόσια ανακοινωμένος. Τα συστήματα που δεν χρησιμοποιούν κρυπτοκλειδί, αναφέρονται με το γενικό όρο «scrambling systems». Η κρυπτογραφική κλείδα αποτελεί «κατάκτηση» της ψηφιακής τεχνολογίας και περιέχεται στη smart card (Κεφάλαιο6), την κάρτα πρόσβασης. Τα συστήματα αυτά αναφέρονται σαν «encryption systems». Στα ημιψηφιακά συστήματα, ο αλγόριθμος κρυπτογράφησης επεμβαίνει στη σειρά εμφάνισης των γραμμών του ράστερ και είτε απλώς τις αναδιατάσσει είτε τις κόβει και τις επανασυνδέει διαφορετικά. Στην πρώτη περίπτωση, την «αναδιάταξη γραμμών» (Line Shuffle), οι γραμμές του ράστερ ανακατεύονται, αναδιατάσσονται και χάνεται η αρχική σειρά. Δίνει καλή τελική εικόνα και έχει υψηλή αφάνεια. Απαιτεί όμως κύκλωμα μνήμης και δημιουργεί αστάθεια στο συγχρονισμό των κυκλωμάτων. Ο αλγόριθμος μεταβολής της σειράς ήταν μια απλή παραλλαγή του DES και το κλειδί της διαδικασίας ήταν ενσωματωμένο στην κάρτα πρόσβασης. Προσφέρθηκε στην αγορά με την εμπορική ονομασία MediaGuard. την άτυχη κατάληξη του οποίου αναφέραμε στην αρχή. Ένα παρόμοιο σύστημα με την εμπορική ονομασία VideoCipher, σχεδιάστηκε από τη Linkabit Systems και χρησιμοποιούσε σαν αλγόριθμο αλλαγής της σειράς των γραμμών σάρωσης, τον άσπαστο τότε, κρυπτοαλγόριθμο DES(Κεφάλαιο 6). Χρησιμοποιήθηκε από το δίκτυο CBS μέχρι το 1998, αλλά και στον πρώτο τηλεοπτικό δορυφόρο Telstar 301, το 1995. Στη δεύτερη περίπτωση, την «κοπή και αλλαγή» των γραμμών του ράστερ (Cut and Rotate), οι γραμμές σάρωσης «κόβονται» στα δύο, σε 256 προκαθορισμένα σημεία και τα κομμάτια αναδιατάσσονται μεταξύ τους, φτιάχνοντας μια νέα αναδομημένη γραμμή σάρωσης. Αυτό επαναλαμβάνεται σε όλες τις γραμμές και το τελικό αποτέλεσμα αποδίδει μια εντελώς ασαφή εικόνα, που μοιάζει σαν να ξεχειλώνει ή να συμπιέζεται περιοδικά. Προσφέρθηκε στην αγορά με την εμπορική ονομασία VideoCrypt, την επιτυχημένη πορεία του οποίου επίσης αναφέραμε και χρησιμοποιήθηκε μέχρι το 1999 από μεγάλα ευρωπαϊκά δίκτυα,

κυρίως το British Sky Broadcasting (BSB). Το VideoCrypt χρησιμοποιούσε μια ισχυρότερη μορφή του αλγόριθμου DES, τον τριπλό DES (3DES). Η κάρτα πρόσβασης περιείχε τόσο τον αλγόριθμο αλλαγής των σημείων κοπής των γραμμών σάρωσης. όσο και το κλειδί της διαδικασίας, που άλλαζε σε τακτικά χρονικά διαστήματα και δινόταν στους χρήστες από το δορυφορικό σήμα. Η κάρτα περιείχε επίσης για πρώτη φορά έλεγχο πιστοποίησης της γνησιότητας και απόρριψης από τον αποκωδικοποιητή, αν βρισκόταν πλαστή. Όταν πρωτοξεκίνησαν όλα τα αυτά τα ψευδό-ψηφιακά συστήματα, στις αρχές της δεκαετίας του 1990 επικράτησε ενθουσιασμός, θεωρήθηκαν ασφαλή και οριστική λύση του προβλήματος της μετάδοσης κρυπτογραφημένης τηλεοπτικής εικόνας. Όμως, ο ενθουσιασμός κράτησε λίγο. Ήταν σειρά του επιτυχημένου VideoCrypt να αρχίσει να αμφισβητείται και να δέχεται κρυπταναλυτικές επιθέσεις. Οι πρώτες κάρτες χρησιμοποιούσαν ενσωματωμένο μικροελεγκτή (microcontroller), που περιείχε το λογισμικό και μπορούσε «εύκολα» να αποδομηθεί με αντίστροφη μηχανική, ώστε να χρησιμοποιηθεί με κατάλληλες τροποποιήσεις σε άλλους μικροελεγκτές. Μετά τις πειρατικές επιθέσεις, το λογισμικό εγκαταστάθηκε σε κυκλώματα ASIC (Application Specific Integrated Circuits), τα οποία επέτρεπαν αλλαγή τόσο της κλείδας, όσο και του αλγόριθμου, μέσω λήψης από το δέκτη (διαδικασία «κατεβάσματος»). Με τον τρόπο αυτό οι πειρατικές επιτυχίες μειώθηκαν. Όμως. αργότερα εμφανίστηκαν στην αγορά απενεργοποιημένες κάρτες, που μπορούσαν να επαναχρησιμοποιηθούν και να λειτουργήσουν ως αυθεντικές και η ασφάλεια του συστήματος εξουδετερώθηκε έγινε αντιληπτό ότι ήταν δυνατόν να χρησιμοποιηθεί το ίδιο κλειδί αποκρυπτογράφησης με αυτό που είχαν οι νόμιμοι χρήστες του συστήματος. Έτσι μόλις ένα τέτοιο κλειδί γινόταν γνωστό, «κυκλοφορούσε» στο internet και η ασφάλεια ήταν παρελθόν. Έπρεπε να γίνει διανομή νέας κλείδας και η διαδικασία «γάτας - ποντικού» άρχιζε από την αρχή. Θύμα αυτής της τακτικής ήταν το σύστημα NagraSyster του ομίλου Kudelski,του τρίτου παγκόσμιου κολοσσού ΜΜΕ. Όταν εμφανίστηκε το προηγμένο σύστημα DirecTV, η τακτική των πειρατών άλλαξε. Αναλύονταν τα σήματα επικοινωνίας (Bus signals) μεταξύ της κάρτας και του δέκτη. Στη συνέχεια, σχεδιάστηκαν κυκλώματα, στα οποία η βάση χρόνου ήταν ελάχιστα αλλοιωμένη ως προς την αυθεντική και με προσεκτική ρύθμιση της διαδικασίας χρονισμού (ένα εκατομμυριοστό του δευτερολέπτου!), γινόταν άρση του παλμού πιστοποίησης της γνησιότητας της κάρτας. Η τελευταία καινοτομία εναντίον των θνησιγενών ημιψηφιακών συστημάτων, ήταν η κλωνοποίηση. Χρησιμοποιούσαν τον ίδιο αριθμό σειράς σε πολλούς διαφορετικούς δέκτες ή κάρτες. Χρησιμοποιήθηκε παράλληλα με τεχνικές άρνησης της κωδικολέξης προστασίας, ώστε να μην είναι δυνατή η αδρανοποίηση της κάρτας μέσω σήματος από τον παροχέα της υπηρεσίας. Αυτή η «επίθεση» ονομάστηκε «ανάλυση McCormac», από το όνομα του διάσημου θεωρητικού της κρυπτανάλυσης των smart cards. Η βελτιωμένη σημερινή του εκδοχή, ονομάζεται «διανομή κάρτας» (Card Sharing) και αποτελεί θανάσιμο κίνδυνο για τους παροχείς συνδρομητικής τηλεόρασης, αφού δεν λειτουργεί σε επίπεδο κρυπτανάλυσης και αλγορίθμων και κλειδιών και όλων αυτών των δύσκολων θεμάτων, αλλά σε απλό επίπεδο διανομής της ίδιας υπηρεσίας σε πολλούς αποδέκτες. Όλα αυτά τα συστήματα απαιτούσαν ειδικά, ακριβά και πολύπλοκα για εκείνη την εποχή ηλεκτρονικά. Εφαρμόστηκαν στις χώρες που λειτουργούσαν καλωδιακά ή δορυφορικά δίκτυα και δημιούργησαν χάσμα, ανάμεσα στις τηλεοπτικά προηγμένες χώρες και στις καθυστερημένες. Στις πρώτες προσφέρονταν ποιοτικές και ακριβές παραγωγές, ενώ στις δεύτερες υποτυπώδεις παράγωγες.

2.5 Πλήρη Ψηφιακά συστήματα και έξυπνες κάρτες

Για τον τρόπο πληρωμής και τους περιορισμούς φροντίζει η τεχνολογία, αφού η «ελεγχόμενη πρόσβαση» (Conditional Access, CA) θεωρείται μία από τις πλέον προηγμένες τεχνολογίες. Απασχολεί χιλιάδες «ειδικούς» και κρυπτογράφους, που έχουν στόχο το πορτοφόλι του τηλεθεατή. Η τεχνολογία είχε δύσκολη και συχνά αδιέξοδη διαδρομή μέχρι να φτάσει στο σημερινό επίπεδο ωριμότητας. Ξεκίνησε από την αναλογική τηλεόραση, στην οποία εφαρμόστηκαν ευφάνταστες λύσεις που συχνά κατέληγαν σε δημόσιο εξευτελισμό και γελοιοποίηση των «ειδικών». Η κατάσταση άλλαξε με την εμφάνιση της ψηφιακής τεχνολογίας. Οι ανώριμες τεχνολογίες παραμερίσθηκαν και το «σπάσιμο» ακόμη και του πιο απλού ψηφιακού συστήματος απαιτούσε βαθιά γνώση, σοβαρές υποδομές και άφθονους πόρους. Η επιχείρηση έγινε ασύμφορη και όσες περιπτώσεις κρυπτανάλυσης ψηφιακών τηλεοπτικών συστημάτων αναγγέλλονταν, οφείλονταν σε τρεις αιτίες; είτε σε λάθος σχεδιασμένα συστήματα, είτε σε στρατηγικές marketing, είτε σε τυχαία δυσλειτουργία. Η εμφάνιση της ψηφιακής τηλοψίας (Digital Video Broadcasting, DVB), έφερε τη μεγάλη ανατροπή και επέβαλε την τεχνολογία του «ελεγκτή πρόσβασης» (CAM, Conditional Access Module).Ο ελεγκτής «δέχεται» και υποστηρίζει την «έξυπνη κάρτα πρόσβασης» (smart card). Στο πρώτο στάδιο, η ενσωμάτωση της smart card είχε περισσότερο ψυχολογική παρά ουσιαστική επίδραση, αφού έφερε κλίμα υψηλής τεχνολογίας, που απέτρεπε τους «πειραματικούς πειρασμούς». Σήμερα, η χρήση της σε κάθε σοβαρό σύστημα δορυφορικής τηλεόρασης είναι απαραίτητη. Η ιδιοφυής σχεδίαση του DVB πρόβλεψε ότι η μονάδα ελέγχου της πρόσβασης δεν θα πρέπει να είναι κλειστή στις προδιαγραφές, αλλά να επιτρέπει την ενσωμάτωση διαφορετικών τεχνολογιών κρυπτογράφησης. Έτσι, το πρότυπο προτείνει δύο επιλογές: την πρόσβαση μέσω κοινού συστήματος κρυπτογράφησης (simulcrypt) και την πρόσβαση μέσω διαφορετικών κρυπτοσυστημάτων (multicrypt ή CI=common interface). Στην πρώτη περίπτωση, τα δίκτυα τηλεόρασης χρησιμοποιούν διαφορετικά συστήματα ελεγχόμενης πρόσβασης, αλλά τον ίδιο αλγόριθμο κρυπτογράφησης, που ονομάζεται «κοινός κρυπτοαλγόριθμος» (CSA, Common Scrambling Algorithm). Στη δεύτερη επιλογή, όλες οι λειτουργίες ελεγχόμενης πρόσβασης περιλαμβάνονται σε μια εξωτερική μονάδα (συνήθως πρόκειται για την κάρτα πρόσβασης), η οποία παρεμβάλλεται στη ροή των δεδομένων. Αυτό επιτυγχάνεται με τη χρήση κοινής υποδοχής (CI, Common Interface) για διαφορετικές «κάρτες». Με τον τρόπο αυτό, τα τηλεοπτικά δίκτυα χρησιμοποιούν τα «δικά τους» συστήματα πρόσβασης. Η τεχνική αυτή έχει το πλεονέκτημα ότι δεν απαιτεί συμφωνίες μεταξύ των δικτύων, αλλά έχει υψηλό κόστος. Μέσα στην ψηφιακή ροή των δεδομένων εικόνας (DVB transport stream) περιλαμβάνεται ο χάρτης προγράμματος (PMT,Program Map Table), ένα από τα στοιχεία του οποίου είναι ο πίνακας ελεγχόμενης πρόσβασης (CAT,Conditional Access Table),που λέγεται συνήθως και «πίνακας κλειδιών» και ο οποίος καθορίζει τα δικαιώματα στη λήψη(Κεφάλαιο 3). Οι πίνακες αυτοί περιέχονται στο λογισμικό της κάρτας και πρέπει να αλλάζουν συχνά. Οι περισσότερες δορυφορικές κάρτες των επίσημων πακέτων καναλιών κάνουν αναβαθμίσεις του λογισμικού μέσω δορυφόρου. Αν λήξει η συνδρομή, τότε η εταιρεία διακόπτει την ενημέρωση της κάρτας, κάνοντας αδύνατη την αποκρυπτογράφηση του «συνδρομητικού πακέτου».

2.6 Σύνοψη Συστημάτων

2.6.1 Αναλογικά Συστήματα

- Αναλογικό σήμα
- Η κρυπτογραφία υφίσταται στο εσωτερικό του αποκωδικοποιητή
- Κρυπτογραφία δεν είναι ουσιώδες μέρος της διαδικασίας αποκωδικοποίησης

2.6.2 Υβριδικά Συστήματα

- Αναλογικό σήμα πάλι ,το σήμα προς μετάδοση είναι σύμφωνο προς πρότυπο αναλογικής τηλεόρασης (PAL, D2MAC, NTSC, SECAM)
- Αναλογικό σήμα κωδικοποιημένα με ψηφιακή framebuffer χρησιμοποιώντας κρυπτογραφημένη κλείδα έλεγχου
- Πλήρως κρυπτογραφική διαχείρισης με τη χρήση έξυπνων καρτών εγγραφής παραδείγματα: VideoCrypt, EuroCrypt (EN 50094), Syster Nagravision

2.6.3 Πλήρη Ψηφιακά Συστήματα

- Ψηφιακό διαμορφωμένο σήμα, κρυπτογραφημένο και πολυπλεγμένο MPEG-2 με ροή δεδομένων ήχου και βίντεο.
- Κρυπτογραφική εγγραφή διαχείρισης με τη χρήση έξυπνων καρτών, όπως τα υβριδικά συστήματα
- Παραδείγματα: DVB, DSS / VideoGuard

2.7 Βιβλιογραφία

Digital Television Satellite, Cable, Terrestrial,IPTV, Mobile TV in theDVB Framework
Third Edition: Hervι Benoit

Τ.Ε.Ι. ΚΡΗΤΗΣ ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΠΟΛΥΜΕΣΩΝ
«Ψηφιακή τηλεόραση-βίντεο» ΣΗΜΕΙΩΣΕΙΣ ΜΑΘΗΜΑΤΟΣ : Γιώργος Σ. Κακαβιάτος

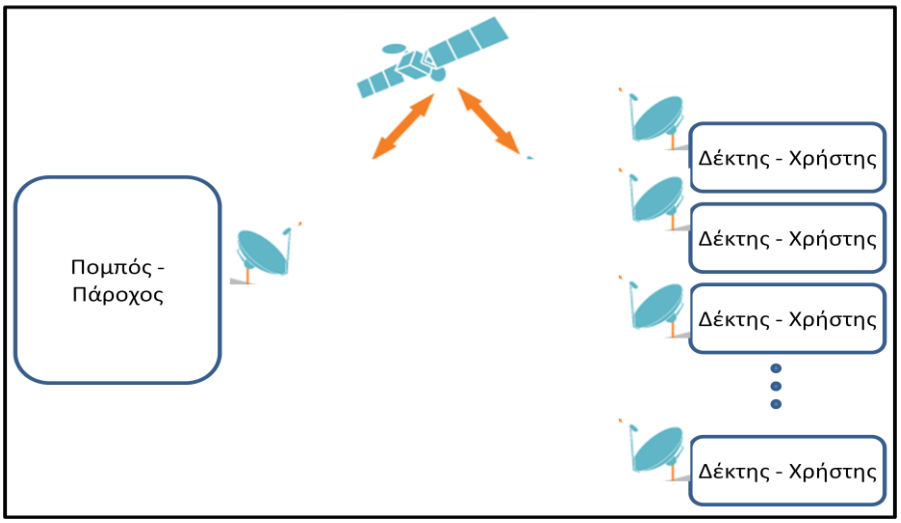
Περιοδικό Δορυφορικά Νέα τεύχος Απρίλιος 2007
Περιοδικό Δορυφορικά Νέα τεύχος Μάιος 2007

Κεφάλαιο 3 Κωδικοποίηση,διαμόρφωση αποστολή και λήψη σήματος

3.1 Εισαγωγή

Στο κεφάλαιο αυτό εξετάζουμε τη διαδικασία εκπομπής και λήψης του δορυφορικού σήματος. Η διαδικασία αυτή όπως είπαμε και πιο πριν χωρίζεται σε τρεις διακριτές φάσεις:

- Η πρώτη αρχίζει με το φορέα παροχής υπηρεσιών και την κρυπτογράφηση του σήματος στον πομπό κατά την εκπομπή.
- Η δεύτερη με το δορυφόρο που ενισχύει και ανακατευθύνει το σήμα στους χρήστες-συνδρομητές.
- Και η τρίτη όταν ο συνδρομητής χρησιμοποιεί τον απαραίτητο εξοπλισμό, Lnb-δέκτη (STB) , δηλαδή για λήψη και αποκρυπτογράφηση, αν χρειάζεται, του σήματος.



Σχήμα 1 εκπομπή - λήψη δορυφορικού σήματος

Η όλη εκπομπή γίνεται στον περίφημο ραδιοτηλεοπτικό και όχι μόνο πρότυπο DVB (Digital Video Broadcasting) . Το πρόγραμμα DVB είναι μια διεθνής κοινοπραξία βιομηχανίας με περισσότερα από 280 μέλη, κατασκευαστών, χειριστών δικτύων, υπεύθυνων για την ανάπτυξη λογισμικού, ρυθμιστικών οργανισμών και άλλων σε πάνω από 35 χώρες. Σκοπός τους είναι ο σχεδιασμός ανοικτών διαλειτουργικών προτύπων για την καθολική παράδοση των ψηφιακών υπηρεσιών. Τα πρότυπα δημοσιεύονται από τη μικτή Τεχνική Επιτροπή (JTC) που απαρτίζεται από τις:

- European Telecommunications Standards Institute (ETSI) ,
- European Committee for Electrotechnical Standardization (CENELEC) και
- European Broadcasting Union (EBU), γνωστή από τη Eurovision.

Ιστορικά ο DVB οργανισμός ξεκίνησε σαν άγνωστος φορέας το Σεπτέμβριο του 1993 με το λεγόμενο ‘ DVB Project’ μέσα σε δύσκολες και αβέβαιες τεχνολογικά εποχές. Το πρότυπο DVB ήρθε να λύσει τεχνολογικές δυσκολίες και προβλήματα στη μετάδοση οπτικοακουστικού υλικού εφαρμόζοντας πρωτοποριακές τεχνολογίες.

Αν και θα εξηγηθούν παρακάτω αναφέρουμε ενδεικτικά : εφάρμοσε πρώτος (ο DVB οργανισμός) την αλυσιδωτή κωδικοποίηση (concatenated coding) στις δορυφορικές επικοινωνίες, και περιέλαβε στο DVB-S2 (πρότυπο δορυφορικής μετάδοσης δεύτερης γενιάς) άλλη πρωτοπορία, τους θεωρητικά εφαρμόσιμους, μέχρι πρότινος κώδικες BCH (Bose, Chaudhuri and Hocquenghem) κώδικες, μαζί με APSK κωδικοποίηση. Με αυτές τις τεχνικές έλυσε το πρόβλημα της ανίχνευσης και διόρθωσης λαθών στο δέκτη και έκανε προσιτή τη δορυφορική ψηφιακή επικοινωνία.

Έτσι ο φορέας DVB θεωρείται πλέον αυθεντία στο χώρο της ραδιοτηλεόρασης και καμία τεχνολογική εξέλιξη δεν προχωρεί αν δε λάβει την έγκριση του γραφείου της EBU στη Γενεύη.

Ο φορέας ξεκίνησε κατανέμοντας τις ραδιοτηλεοπτικές μεταδόσεις σε τρία διαφορετικά συστήματα :

- Δορυφορική μετάδοση (DVB-S), που θα την αναλύσουμε παρακάτω
- Καλωδιακή τηλεόραση (DVB-C)
- Επίγεια ψηφιακή εκπομπή (DVB-T)

οπού και καθιέρωσε τα ανάλογα πρότυπα.
Από τότε όμως ασχολήθηκε έκτος τα πρότυπα εκπομπής και με αλλά πρότυπα. Αυτά είναι ανά κατηγορία:
Conditional Access (ελεγχόμενη πρόσβαση οπτικοακουστικού υλικού)
DVB-CSA DVB-SIM

Interactivity (διαδραστικότητα)
DVB-NIP DVB-RCC DVB-RCCS DVB-RCD DVB-RCG DVB-RCL DVB-RCP DVB-RCS DVB-RCT

Interfacing (διασύνδεση)
DVB-ATM DVB-CI DVB-HAN DVB-HLN DVB-IRDI DVB-PDH DVB-PI DVB-SDH

Internet Protocol
DVB-IPDC DVB-IPTV

Measurement (μετρήσεις)
DVB-M

MHP - Multimedia Home Platform (πλατφόρμα διαδραστικής τηλεόρασης)
DVB-GEM DVB-MHP DVB-PCF

Multiplexing (πολυπλεξία)
DVB-DATA DVB-MPEG DVB-SI DVB-SSU DVB-TVA DVB-TXT DVB-VBI

Subtitling (υποτιτλισμός)
DVB-SUB

Transmission (εκπομπή) που όπως είπαμε ήταν και τα πρώτα πρότυπα του φορέα
DVB-C DVB-DSNG DVB-H DVB-MC DVB-MS DVB-MT DVB-S DVB-S2 DVB-SH DVB-SMATV DVB-T

Ενώ για τα (DVB-S) και (DVB-T) αναπτύχθηκαν τα πιο εξελιγμένα (DVB-S2) και (DVB-T2)

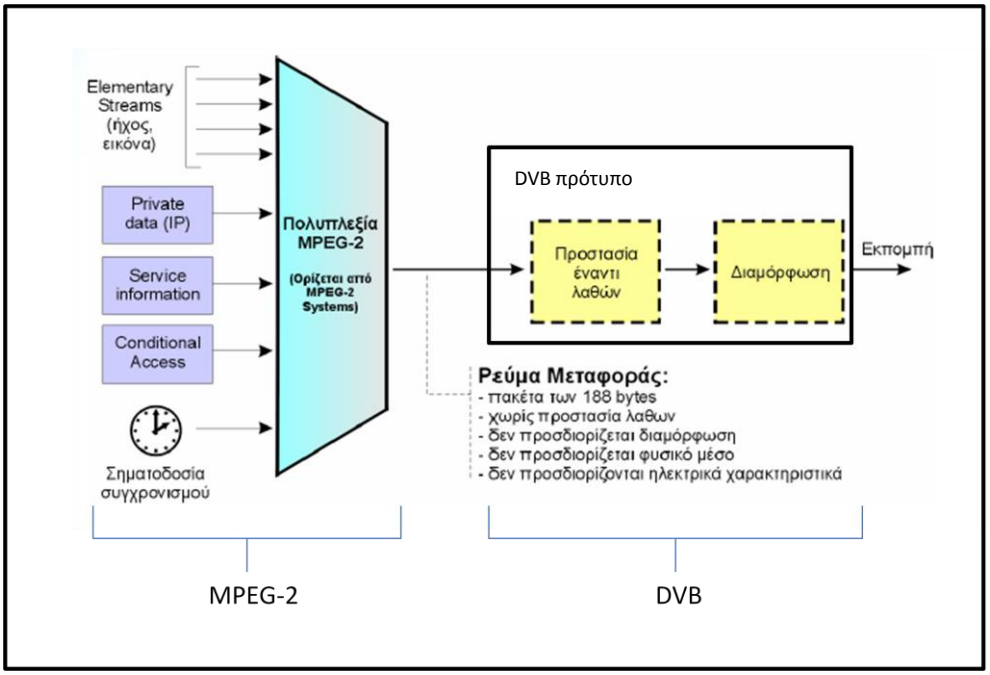
3.2 ΕΚΠΟΜΠΗ

Από όλα αυτά εμείς θα σταθούμε στην κατηγορία των εκπομπών (transmission) και στα δύο πρότυπα που ενδιαφέρουν τις δορυφορικές επικοινωνίες. Αυτά είναι το DVB-S και DVB-S2. Θα εξετάσουμε εκτενώς το DVB-S ανά στάδιο. Αναφέρουμε ότι η διάταξη και τα σταδία που ακολουθούν αναφέρονται μονό για το DVB-S. Το DVB-S2 έχει πιο εξελιγμένη δομη με αρκετές διαφορές από το DVB-S2. Στην ανάλυση όμως του DVB-S αναφέρονται και οι διαφορές που παρουσιάζουν ανά δομή τα δύο πρότυπα.

Το DVB-S αναπτύχτηκε το 1993, χρησιμοποίησε την ήδη αναπτυγμένη και επιτυχημένη συνταγή συμπίεσης MPEG για το οπτικοακουστικό υλικό και εφάρμοσε πάνω της το πρότυπο DVB που περιέχει :

- Μηχανισμό προστασίας λαθών και ανοχής στο θόρυβο διαύλου (αέρας) ,
- Διαμόρφωση για κατάλληλη εκπομπή στο δίαυλο (αέρας)

Σχηματικά αυτό που αναφέραμε φαίνεται κάτωθι :



Σχήμα 2 : Το πρότυπο DVB-S που αποτελείται από δύο σταδία MPEG επεξεργασία και DVB τροποποίηση.

Δηλαδή το αναλογικό σήμα υφίσταται στην πλευρά του παρόχου MPEG επεξεργασία και τροποποίηση κατά DVB έτσι ώστε να μπορεί να αποσταλεί κατά DVB-S μέσω της δορυφορικής δέσμης στον τελικό χρήστη.

3.2.1 Πρότυπο συμπίεσης εικόνας ήχου αλλά και δεδομένων MPEG

Το πρώτο στάδιο που θα εξετάσουμε είναι η επεξεργασία MPEG:

Το MPEG είναι ακρωνύμιο του Moving Pictures Experts Group, και έχει συσταθεί από τον Διεθνή Οργανισμό Τυποποίηση (**International Organization for Standardization**, διακριτική ονομασία: **ISO**). Σκοπός του είναι η δημιουργία πρότυπων για εκπομπή και συμπίεση οπτικοακουστικού υλικού (εικόνας, ήχου, video). Ανάλογα με την εφαρμογή, την τεχνολογία, το κόστος και άλλους παράγοντες το MPEG έχει παρουσιάσει και συνεχίζει να αναπτύσσει διάφορα πρότυπα.

Αυτά είναι :

MPEG-1: MPEG-1, το πρώτο βίντεο εικόνας και ήχου με πρότυπο συμπίεσης, υποστηρίζει βίντεο 352x240 με ρυθμό 30 fps (καρέ ανά δευτερόλεπτο) . Ωστόσο, η ποιότητα του βίντεο MPEG-1 είναι ελαφρώς χαμηλότερη από την ποιότητα του βίντεο που προσφέρεται από ένα κανονικό βίντεο.

MPEG-2: MPEG-2 μπορεί να υποστηρίξει τα συστήματα του βίντεο 720x480 και 1280x720 στα 60 καρέ ανά δευτερόλεπτο, με ποιότητα ήχου ίση με συμβατικού CD ήχου. Είναι κατάλληλο για όλα σχεδόν τα τηλεοπτικά πρότυπα, συμπεριλαμβανομένων PAL, NTSC και HDTV. Το MPEG-2 έχει την ικανότητα να μειώσει αρχείο δίωρης ταινίας σε λίγα gigabytes δεδομένων. Χρησιμοποιείται επίσης για την αποθήκευση δεδομένων σε DVD.

MPEG-3: Το MPEG-3 ήταν προσανατολισμένο στην τεχνολογία της **Τηλεόρασης Υψηλής Ευκρίνειας** (HDTV - High Definition TV) αλλά εγκαταλείφθηκε αφού διαπιστώθηκε ότι το MPEG-2 μπορεί με κάποιες αλλαγές στη σύνταξη των προδιαγραφών να χρησιμοποιηθεί το ίδιο καλά στη HDTV. 'Ετσι η δουλειά που είχε γίνει πάνω στο MPEG-3 ενσωματώθηκε στο MPEG-2.

MPEG-4: Δημιουργήθηκε στα τέλη του 1998, έχει σαν βάση τα MPEG-1, MPEG-2, Apple QuickTime. Είναι σχεδιασμένο έτσι ώστε να μεταδώσει εικόνες και βίντεο, με τη χρήση του μικρότερου εύρους ζώνης δικτύου από όλα τα προηγούμενα πρότυπα. Χρησιμοποιείται στο internet, video-streaming, ψηφιακή τηλεόραση και αλλού. Συμπεριλαμβάνει το πρότυπο συμπίεσης MPEG-4 H. 264/AVC.

MPEG-5, MPEG-6: Δεν υπάρχουν αυτά τα πρότυπα και ο λόγος όσο παράξενος και αν ακούγεται είναι διότι οι κατασκευαστές αποφάσισαν να μη κάνουν το αναμενόμενο και μετά το MPEG-4 αντί του 5 και 6 να μεταπηδήσουν στο MPEG- 7.

MPEG-7: MPEG-7 δημιουργήθηκε το 2001 και είναι πρότυπο για αναζήτηση και απεικόνιση ανάμεσα σε περιεχόμενο πολυμέσων(δε θα μας απασχολήσει).

MPEG-21: Το MPEG21 σε αντίθεση με τα προηγούμενα MPEG-1, MPEG-2, MPEG-4 και MPEG-7 δεν προτείνει τρόπους για την κωδικοποίηση, επεξεργασία ή περιγραφή πολυμέσων αλλά στοχεύει κυρίως στον τρόπο με τον οποίο θα γίνει η διάθεση. Το όραμα που υπάρχει πίσω από την δημιουργία του είναι η απρόσκοπτη πρόσβαση σε διαφόρων ειδών πολυμέσα, από διαφορετικές τερματικές συσκευές και διαμέσου ετερογενών δικτύων.

Τα παραπάνω από αυτά συνεχίζουν να αναπτύσσονται ενώ στα σκαριά υπάρχουν και αλλά ενδεικτικά τα MPEG-B, MPEG-C, MPEG-D MPEG-M MPEG-V και άλλα που δεν είναι επί του παρόντος.

Τα πρότυπα MPEG αποτελούνται από τα **Parts (**διαφορετικά μέρη). Κάθε **Part** (μέρος) καλύπτει μια ορισμένη πτυχή ολόκληρης της προδιαγραφής. Κάθε κατασκευαστής μπορεί να απομονώσει όποιο ή όποια **Parts** θέλει ανάλογα με την εφαρμογή που θέλει. Τα πιο παλιά είναι τα :

Part 1---Systems
Part 2---Video
Part 3---Audio
Part 4---Conformance:
Part 5---Software Simulation

που βρίσκονται στο MPEG-1, στο MPEG-2 αυξάνονται και φτάνουν τα 9, ενώ στο MPEG-4 μέχρι στιγμής αριθμούν 23.

Από όλα αυτά εμείς ξεχωρίζουμε το Part10 του MPEG-4 που είναι το AVC (Advanced Video Coding) γνωστό και ως H.264 . Παρουσιάστηκε το Μάιο του 2003 και αποτελεί την καλύτερη συμπίεση /ποιότητα για οπτικοακουστικό υλικό από όλα τα πρότυπα. Χρησιμοποιείται στη High Definition (HD) τηλεόραση (δορυφορική, επίγεια και καλωδιακή) , όπως και στους ψηφιακούς δίσκους blue-ray όπου οι ταινίες αποθηκεύονται με αυξημένη ποιότητα.

Κάθε πρότυπο τώρα έχει τα λεγόμενα Profile και Levels. Αρχίζουμε από το εύκολο που είναι τα Levels. Αυτά είναι τα διαφορετικά επίπεδα ανάλυσης (σε pixels) του οπτικοακουστικού υλικού. Ανάλογα με την εφαρμογή ξεκινούν από 128x96 pixels και φτάνουν 4096x2304 pixels (για σύγκριση η Full High Definition ανάλυση των τηλεοράσεων είναι 1920x1080).

Τα Profiles είναι διαφορετικά προφίλ δειγματοληψίας και τρόπου συμπίεσης των κινούμενων εικόνων. Κάθε Profile συνδυάζεται ανεξάρτητα με κάθε Level και έτσι δίνει τη δυνατότητα στον κατασκευαστή να διαλέξει τον κατάλληλο συνδυασμό για την εφαρμογή του (εγγραφή ταινίας σε blue-ray, video-conference, video-streaming και αλλά).

Αφού τελειώσαμε με τα θεωρητικά ας μπούμε στα πιο πρακτικά του MPEG. Γενικά θα ασχοληθούμε με τα πρότυπα MPEG-2 και MPEG-4 τα οποία χρησιμοποιούνται στις δορυφορικές επικοινωνίες και μας αφορούν άμεσα.

Το MPEG-2 όπως αναφέραμε πιο πάνω κάνει:

- **συμπίεση**,

δηλαδή μείωση του όγκου της ψηφιακής πληροφορίας εικόνας και ήχου. Με τη χρήση του αλγόριθμου συμπίεσης MPEG-2 με τεχνικές που δε καλύπτονται από αυτό το σύγγραμμα επιτυγχάνεται μείωση της τηλεοπτικής εικόνας του ψηφιοποιημένου PAL κατά 97%, δηλαδή βελτίωση της τάξης του 33:1 . Ο ρυθμός μετάδοσης μειώνεται από 216Mbps (αναλογικό) σε 6 έως 8 Mbps. Αναφέρουμε ότι η συμπίεση είναι πρώτιστη ανάγκη στις δορυφορικές επικοινωνίες αφού το εύρος ζώνης στοιχίζει αρκετά και είναι περιορισμένο. Αλλά και την καταπληκτική ιδέα που ακούει στο όνομα

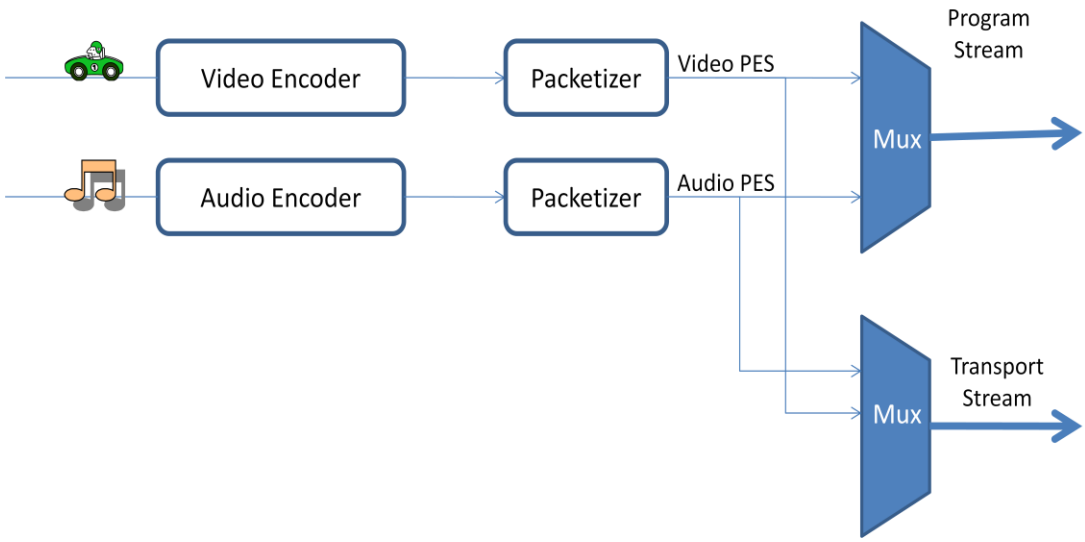
- **πολυπλεξία**,

δηλαδή η ταυτόχρονη μετάδοση πολλών τηλεοπτικών καναλιών από μία συχνότητα. Παλαιότερα, η αναλογική τεχνολογία απαιτούσε εύρος ζώνης 36MHz και έναν αναμεταδότη (transponder) του δορυφόρου για τη μετάδοση ενός και μόνο τηλεοπτικού προγράμματος (τεχνολογία SCPC. Single Carrier Per Channel) .

Με την τεχνολογία DVB-S μεταδίδονται από το ίδιο εύρος συχνοτήτων και από τον ίδιο πομπό μέχρι δέκα διαφορετικά τηλεοπτικά προγράμματα (σε κανονική ανάλυση). Η εντυπωσιακή βελτίωση οφείλεται στη χρήση πολυπλεξίας (multiplexing) , μιας τεχνικής που χωρίζει την ψηφιακή παλμοσειρά σε τμήματα, μοιράζοντας σε κάθε κανάλι ίσο «χώρο» μετάδοσης. Αυτή η τεχνολογία - που λέγεται MCPC (Multiple Channel Per Carrier) - έχει καθιερώσει και νέους όρους, όπως «ψηφιακό μπουκέτο» ή «πακέτο καναλιών». Όταν λοιπόν αναφερόμαστε στο μπουκέτο της Nova στο δορυφόρο Hot Bird, στη συχνότητα 11,823GHz εννοούμε ότι σ' αυτήν τη συχνότητα και με εύρος ζώνης 36MHz μεταδίδονται μέχρι δέκα διαφορετικά τηλεοπτικά προγράμματα.

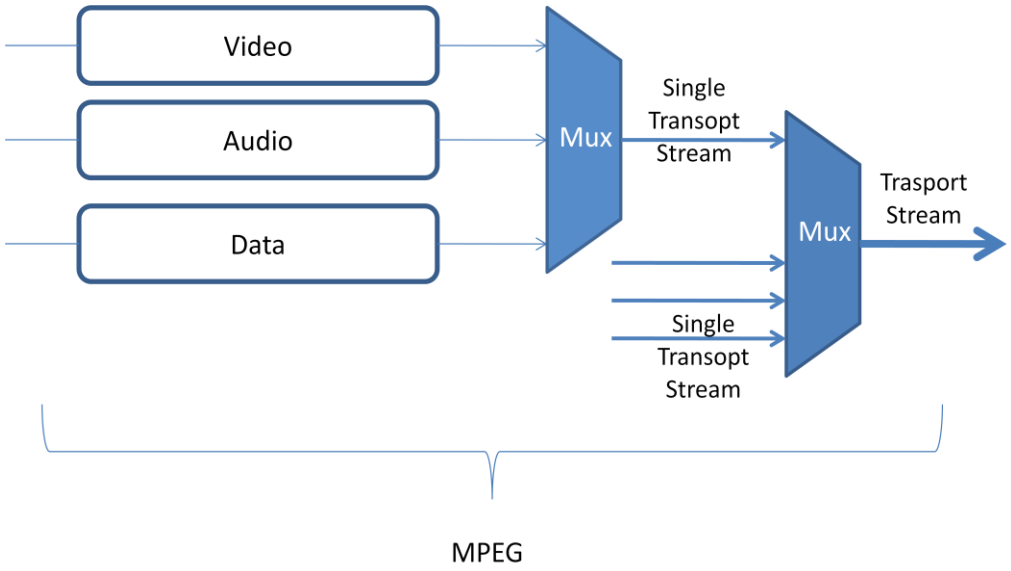
3.2.1.1 Trasport Stream (ροή μεταφοράς)

Το MPEG όπως και τα δίκτυα ηλεκτρονικών υπολογιστών αλλά και το Internet χρησιμοποιεί την τεχνολογία «μεταγωγής πακέτων δεδομένων» (data packets). Το οπτικοακουστικό υλικό με τη μέθοδο της δειγματοληψίας ψηφιοποιείται και επεξεργάζεται στους κωδικοποιητές (audio,video).Αφού ψηφιοποιηθούν τεμαχίζονται σε μικρά πακέτα (για πιο αποτελεσματικό μηχανισμό διόρθωσης λαθών) και δημιουργούν ανεξάρτητες ροές για κάθε κανάλι (στοιχειώδεις ροές- Elementary Stream). Αυτές οι ροές μαζί με τη ροή των πληροφοριών (περιέχει πληροφορίες για συγχρονισμό των ανεξάρτητων ροών) με πολυπλεξία (τοποθέτηση όλων των πακέτων σε μια ροή) σχηματίζουν ανά πρόγραμμα ροή μεταφοράς (SPTS Single Program **Transport Stream**). Πολλές από αυτές τις ροές από πολλά προγράμματα (τηλεοπτικά κανάλια) σχηματίζουν με πολυπλεξία την τελική μας ροή που είναι και αυτή που μεταδίδεται στο δίαυλο μας και ονομάζεται ροή μεταφοράς (**Transport Stream**). Η ροή μεταφοράς **Transport Stream** δεν πρέπει να ταυτίζεται ή να θεωρείται υπερσύνολο της ροής προγράμματος **Program Stream.** Πολλοί φοιτητές στις μελέτες τους αλλά και πολλοί συγγραφείς θεωρούν εσφαλμένα ότι πρώτα υφίσταται ανά τηλεοπτικό κανάλι η **Program Stream** και μετά πολυπλέκεται στην **Transport Stream**. Η αλήθεια είναι η εξής :Το MPEG ανάλογα με τη εφαρμογή έχει δύο επιλογές να παράγει **Program Stream** ή **Transport Stream**. Αυτό φαίνεται στο σχήμα που ακολουθεί :



Σχήμα 3 : η παράγωγη program ή transport stream ανάλογα με την εφαρμογή

Η **Program Stream** αποτελείται από μεγάλα πακέτα για μετάδοση σε ασφαλές μέσο με λίγα λάθη (πχ. στους δίσκους CD ή σε εφαρμογές PC) ενώ η **Transport Stream** αποτελείται από πακέτα μικρού μήκους (εδώ 188 bytes). Το μικρό μήκος των πακέτων κάνει τον μηχανισμό διόρθωσης λαθών πιο αποτελεσματικό. Έτσι χρησιμοποιείται για μετάδοση όπου το μέσο είναι επιρρεπές σε λάθη όπως οι δορυφορικές επικοινωνίες.

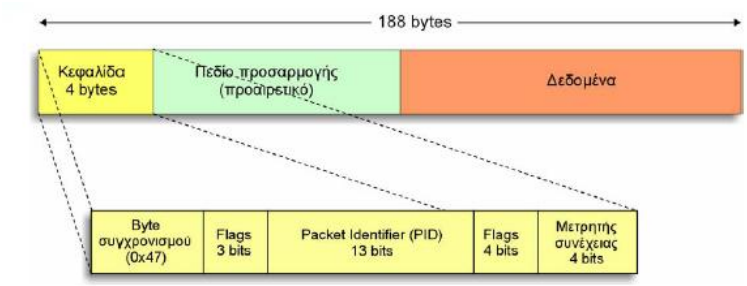


Σχήμα 4 : Η παράγωγη transport stream με πολυπλεξία πολλών καναλιών (single trasport stream)

Αυτές οι ροές θα πρέπει να συνδυαστούν με οργανωμένο τρόπο και να συμπληρωθούν με επιπλέον πληροφορίες. Αυτές είναι πληροφορίες κρυπτογράφησης (EMM,ECM θα τα δούμε πιο μετά), πληροφορίες οι οποίες θα επιτρέψουν το διαχωρισμό τους από τον ψηφιακό αποκωδικοποιητή (Set Top Box-STB) , πληροφορίες για το συγχρονισμό των πακέτων αλλά και της εικόνας με τον ήχο, όπως και επιπρόσθετες υπηρεσίες ή πληροφορίες που επιθυμεί να εντάξει ο πάροχος. Παρακάτω αναλύεται το πακέτο που αποτελεί τη trasport stream και πως ανακατευθύνεται ανά ομάδα για να δημιουργήσει το αρχικό κανάλι στο δορυφορικό δέκτη του χρήστη.

3.2.1.2 Κατευθύνοντας μια πολυπλεξία MPEG-2 - Το πακέτο PES

Κάθε πακεταρισμένη στοιχειώδη ροή ή αλλιώς πακέτο PES, έχει αρχικά μέγεθος 188bytes και «αρχίζει» με την επικεφαλίδα (header) 4 bytes, η οποία ακολουθείται από τα δεδομένα της στοιχειώδους ροής 184 bytes.



Τα 4 bytes του header ή 32 bits διανέμονται ως εξής

Byte συγχρονισμού	8 bits
Flags –Σημαίες	3 bits
Packet Identifier (PID)	13 bits
Flags –Σημαίες	4 bits
Μετρητής Συνέχειας	4 bits
Σύνολο bits :	32 bits

Αυτό το πεδίο μας ενδιαφέρει

Σχήμα 5: Τα bits της επικεφαλίδας ενός πακέτου PES (packetarized elementary stream)

Προσπερνούμε τη χρησιμότητα των παραπάνω bits και στεκόμαστε μόνο στο πεδίο Packet Identifier (PID) . Αυτό ονομάζεται ταυτότητα αναγνώρισης (packet identity) και είναι μια διεύθυνση του πακέτου. Το PID είναι αυτό που κατευθύνει το δεκτή του τελικού χρήστη στη εύρεση των πληροφοριών που θέλει ο χρήστης. Δηλαδή αν θέλει συγκεκριμένο κανάλι (πχ. ΝΕΤ) ή αν θέλει αλλαγή γλώσσας υπότιτλων κ.α., μέσω του PID θα καταφέρει ο δέκτης να ξεχωρίσει τις συγκεκριμένες υπηρεσίες στο πλήθος τις πολυπλεγμένης ροής και να τις παρουσιάσει στο χρήστη. Πως γίνεται όμως αυτό;

Στο ρεύμα ροής υπάρχουν επιπλέον πληροφορίες που χωρίζονται σε δύο κύριες κατηγορίες:

- Τηλεοπτικά προγράμματα (Program Specific Information- **PSI**). Δεν καθορίζονται από το MPEG.
- Πληροφορίες Υπηρεσίας (Service Information- **SI**). Δεν καθορίζονται από το MPEG αλλά από το DVB.

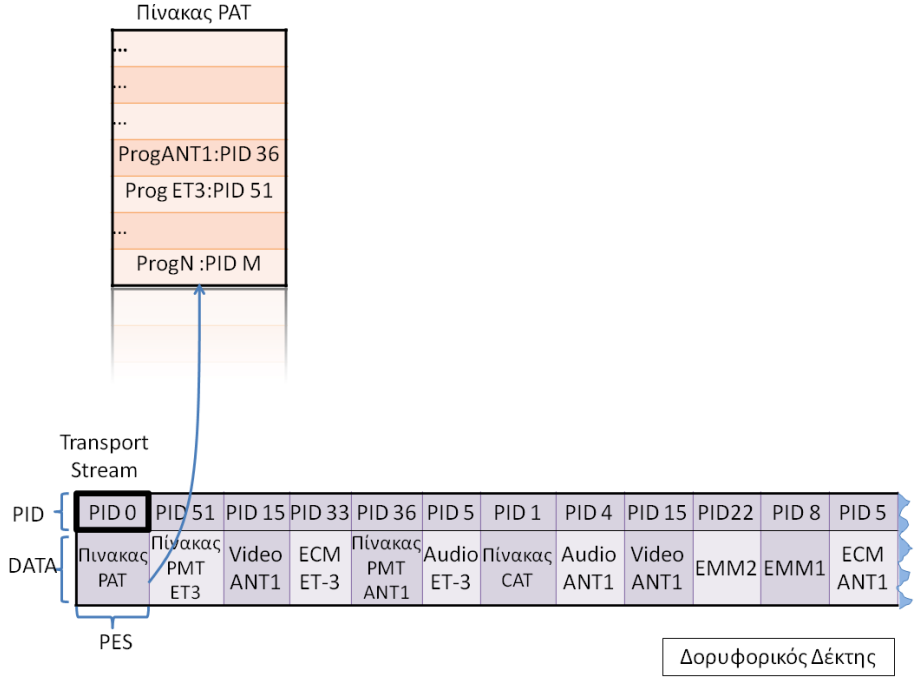
Τα PSI αποτελούνται από δεδομένα που επιτρέπουν σε έναν αποκωδικοποιητή την αποπολυπλεξία μιας επιλογής του χρήστη από τη ροή, ενώ τα SI είναι δεδομένα που παρέχουν πληροφορίες σχετικές με το σύνολο της υπηρεσίας που παρέχει ο πάροχος (π.χ. αριθμός καναλιών, ώρα, συχνότητες κ.α.). Δε θα σταθούμε σε αυτές τις πληροφορίες γιατί

δεν είναι αυστηρά καθορισμένες, εξαρτώνται ανά πάροχο αλλά και γιατί δεν έχουν άμεση σχέση με την κρυπτογραφία όπως έχουν τα PSI δεδομένα.
Τα PSI δεδομένα χωρίζονται σε 4 πίνακες

- Program Association Table (**PAT**)
- TS Program Map Table (**PMT**)
- Conditional Access Table (**CAT**)
- Network Information Table (**NIT**)

3.2.1.2.1 Πίνακας PAT

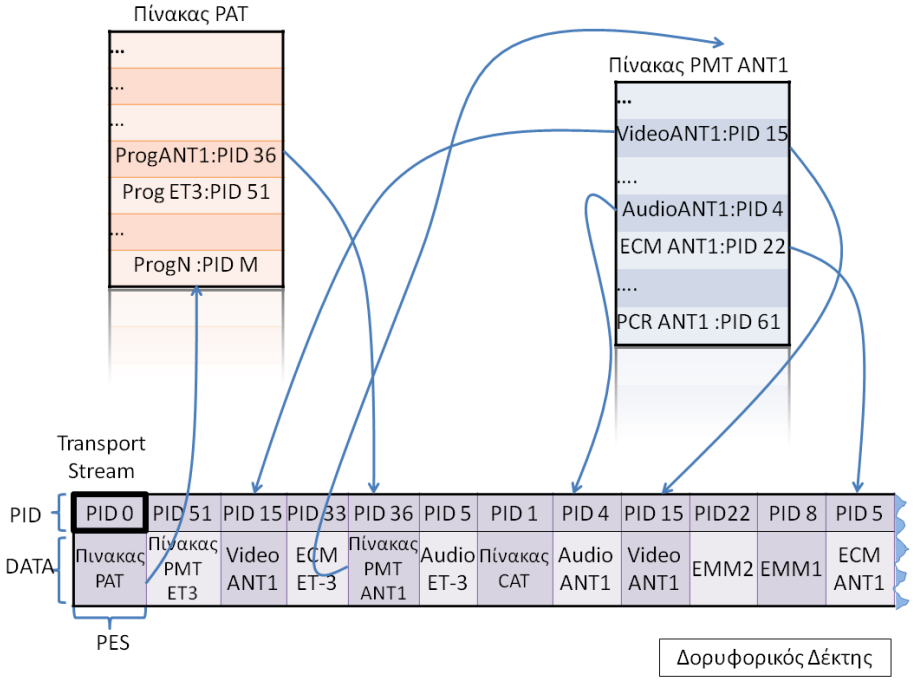
Περιέχεται στα πακέτα της ροής που έχει σαν PID 0000 (δηλαδή όλα τα bits του 0) . Αναγνωρίζεται από το δορυφορικό δέκτη μας και υπάρχει πάντα στην ψηφιακή ροή. Ο πίνακας **PAT** απλώς μας λέει σε ποιό **PID** βρίσκεται ο **PMT** πίνακας κάθε καναλιού-υπηρεσίας που μας παρέχει ο πάροχος (πχ. σε ποιό **PID** βρίσκεται ο **PMT** πίνακας του καναλιού ANT1 (δηλαδή **PMT**$_{ANT1}$).



Σχήμα 6: εύρεση πινάκα PAT από PID 0

3.2.1.2.2 Πίνακας PMT

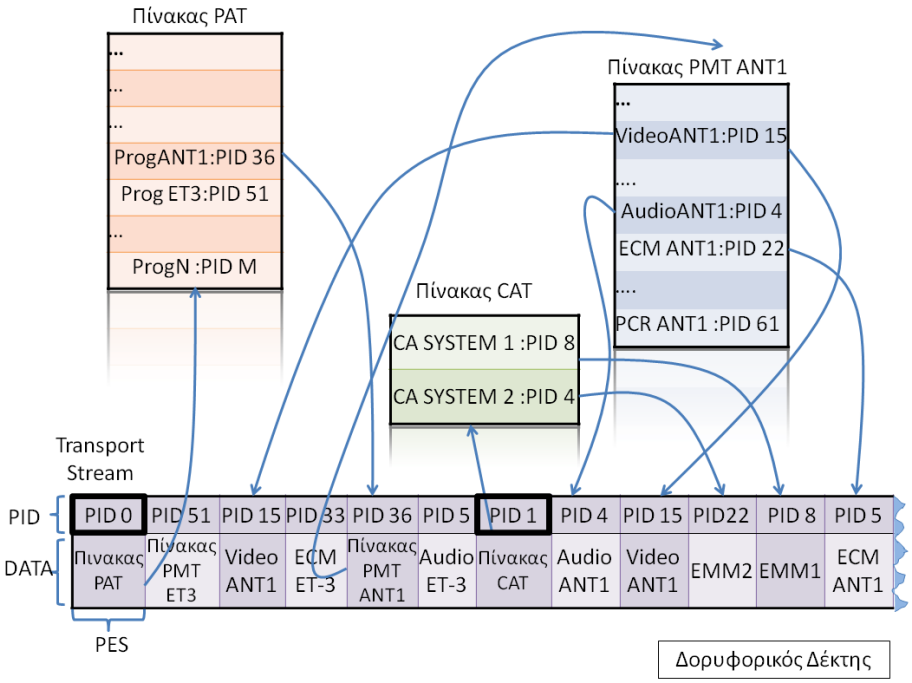
Ο πίνακας **PMT** τώρα δεν είναι τίποτα άλλο από τον πινάκα που μας λέει σε ποια διαφορετικά **PID** βρίσκονται οι ατομικές πληροφορίες που συνθέτουν το κανάλι που ανήκει ο πίνακας. Δηλαδή στο παράδειγμα μας ο πίνακας $\mathbf{PMT}_{ANT1}$ μας λέει σε ποιά **PID** βρίσκονται η εικόνα, ο ήχος, οι υπότιτλοι, το ECM μήνυμα αν το κανάλι ANT1 είναι κρυπτογραφημένο (θα εξηγήσουμε έπειτα τι είναι ECM) και αλλά. Αρά άμα θέλουμε να δούμε ANT1 ο δέκτης ψάχνει τον πινάκα **PAT** και βρίσκει με το **PID** του ANT1 το $\mathbf{PMT}_{ANT1}$, από αυτό βρίσκει τα **PID** των πληροφοριών που απαρτίζουν αυτό το κανάλι. Στηριζόμενος ο δέκτης σε αυτές τις πληροφορίες συνθέτει το κανάλι και το απεικονίζει στην τηλεόραση.



Σχήμα 7: εύρεση πινάκα PAT

3.2.1.2.3 Πίνακας CAT

Ο πίνακας CAT αναφέρει το PID (διεύθυνση) του EMM (θα εξηγήσουμε αναλυτικά τα EMM και ECM στο επόμενο κεφάλαιο) που είναι απαραίτητο αν υπάρχουν κρυπτογραφημένα κανάλια. Αν υπάρχουν πάνω από ένα συστήματα κρυπτογράφησης παρέχεται και η διεύθυνση των EMM των υπολοίπων συστημάτων.



Σχήμα 8: Εύρεση στοιχειωδών ροών που απαρτίζουν το κανάλι από πινάκα PAT

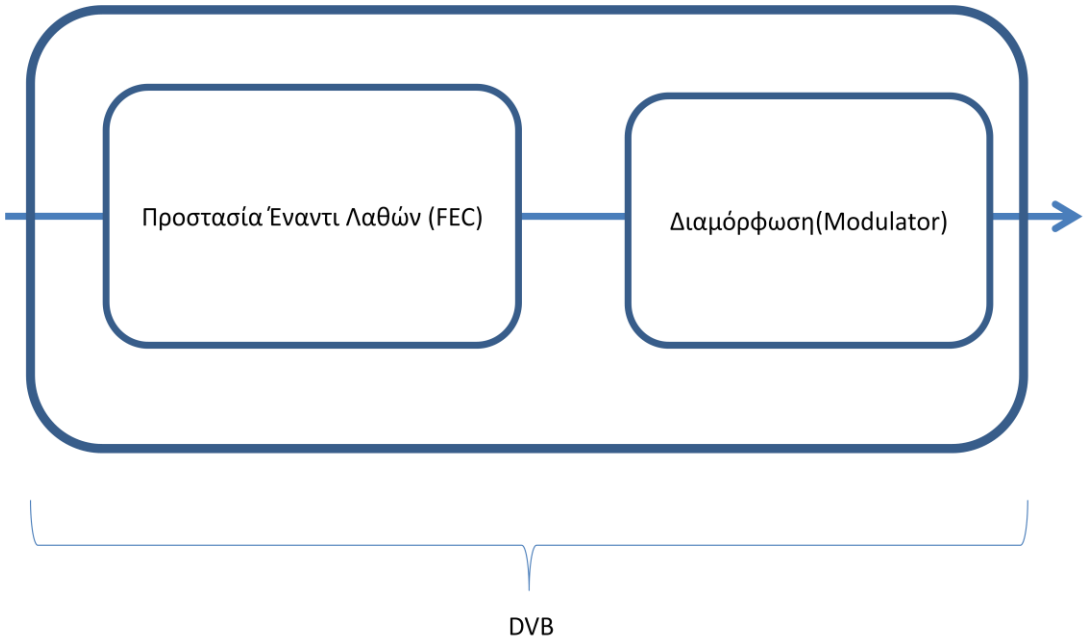
3.2.1.2.4 Πίνακας NIT

Τέλος ο NIT πίνακας περιέχει ιδιωτικές πληροφορίες του παρόχου που δεν καθορίζονται από το πρότυπο DVB οπότε κάθε πάροχος είναι ελεύθερος να περιλάβει ό,τι θέλει. Σε γενικές γραμμές, περιέχει κανάλια συχνοτήτων, αριθμούς δορυφορικού αναμεταδότη, χαρακτηριστικά διαμόρφωσης του σήματος κλπ.

3.2.2 DVB επεξεργασία

Μετά την επεξεργασία κατά MPEG έχουμε το δεύτερο στάδιο αυτό της επεξεργασία κατά DVB.

Το πολυπλεγμένο σήμα όπως δείχνει το σχεδιάγραμμα υποβάλλεται σε προστασία έναντι λαθών (FEC) και σε διαμόρφωση (κατάλληλη διαφοροποίηση για να μπορεί να αποσταλεί το σήμα μας μέσω του δορυφορικού δίαυλου).



Σχήμα 9 :Τα δύο κυρία σταδία της DVB επεξεργασίας κατά DVB-S

3.2.2.1 Κωδικοποίηση Καναλιού, FEC (Forward Error Correction)

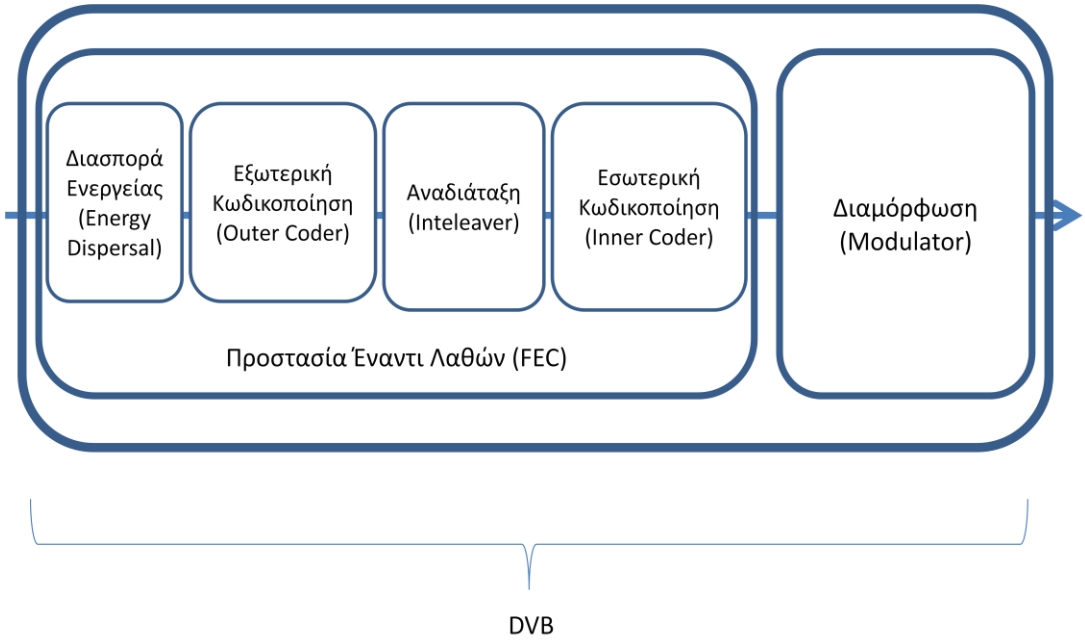
Τι εννοούμε όμως με τον όρο FEC (Forward Error Correction) ;

Το δορυφορικό σήμα κατά την εκπομπή και λήψη του εμφανίζει σφάλματα μετάδοσης. Αυτό γιατί ο δορυφορικός δίαυλος είναι επιρρεπής σε λάθη. Για να λυθεί αυτό το πρόβλημα αρχικά υλοποιήθηκε ο τρόπος που χρησιμοποιείται στο διαδίκτυο (σε εφαρμογές TCP) και είναι ο ARQ (Automatic Repeat request) . Δηλαδή το σήμα τεμαχιζόταν σε κομμάτια και στελνόταν κομμάτι κομμάτι. Ανά κομμάτι ο λήπτης απαντούσε στον αποστολέα ότι έλαβε το κομμάτι καλά και έστελνε εντολή ‘’προχώρα στο επόμενο’’ ή ότι δεν έλαβε καλά γράφοντας ‘’ξαναστείλε το κομμάτι’’. Κάτι τέτοιο όμως απαιτούσε χρόνο, αμφίπλευρη επικοινωνία και μπορεί να οδηγούσε σε ατέρμονους κύκλους. Έτσι η λύση του FEC ή αλλιώς μονομερής διόρθωση λαθών προτάθηκε στις δορυφορικές επικοινωνίες για να λύσει αυτά τα προβλήματα. Κατά FEC η διόρθωση λαθών γίνεται μόνο στο δέκτη του τελικού χρήστη χωρίς να χρειάζεται αμφίπλευρη επικοινωνία, τμηματική και με καθυστέρηση. Το κόλπο ήταν η προσθήκη ψηφίων στο σήμα τα οποία βοηθούν το δέκτη να καταλάβει ποιο είναι το αρχικό σήμα χωρίς άλλη πληροφορία. Είναι δυνατόν όμως χωρίς να ξέρουμε το αρχικό σήμα να βρούμε που έχει λάθη ;

Ένα παράδειγμα για να κατανοήσουμε τη διαδικασία είναι το έξης.

Έστω ότι έχω τη ροή 1, 2, 3, 4 για αποστολή από τον πομπό στο δέκτη. Για να προστατεύω το σήμα μου από αλλοίωση, τετραπλασιάζω το πλήθος των ψηφίων ώστε η ροή μου να

γίνει 1111, 2222, 3333, 4444. Άμα ο δέκτης λάβει 1101, 2252, 3333, 4442, αφού ξέρει ότι κάθε πακέτο περιέχει το ίδιο ψηφίο τα μεταφράζει σαν 1111, 2222, 3333, 4444 και αφού αφαιρέσει τα επιπλέον ψηφία λαμβάνει το αρχικό σήμα 1, 2, 3, 4. Έτσι ενώ υπάρχουν 3 λάθη ο δέκτης αυτοδιορθώνεται. Βέβαια αυτό είναι ένα υπεραπλουστευμένο παράδειγμα. Η μαθηματική θεωρία που περιέχεται είναι πεπερασμένα πεδία και άλλα προχωρημένα μαθηματικά. Η τιμή FEC ορίζεται ως το πηλίκο του σήματος /σήματος με επιπλέον bits-διόρθωσης. Όσο πιο μικρό είναι το FEC τόσο περισσότερα bits-διόρθωσης προστίθενται και τόσο πιο πολλά λάθη διορθώνονται (με κόστος βεβαία μεγαλύτερο εύρος ζώνης). Η διαδικασία FEC στο DVB-S αναλύεται σε τέσσερα σταδία που φαίνονται στο σχήμα 10 και αναλύονται παρακάτω:



Σχήμα 10 :Ανάλυση διαδικασιών που γίνονται στη FEC επεξεργασία

3.2.2.1.1 Διασπορά Ενεργείας (Energy Dispersal)

Η ψηφιακή ροή αφού περάσει από τον MPEG πολυπλέκτη μπαίνει στην πρώτη βαθμίδα του FEC που είναι η διασπορά ενέργειας. Η διαδικασία αυτή, που οδηγεί σε διασπορά της ενέργειας του σήματος γίνεται για λόγους συμμόρφωσης με τους κανονισμούς της αρχής ραδιοσυχνοτήτων για την κατάληψη του φάσματος. Μακριές σειρές bits από 0 ή 1 δημιουργούν μια DC συνιστώσα στο σήμα (αφού το 0 και 1 ξεχωρίζονται από διαφορά τάσης) έτσι συγκέντρωση ισχύς σε μια μικρή ζώνη συχνοτήτων δημιουργεί προβλήματα π.χ. παρεμβολές στα παρακείμενα κανάλια. Για αυτή τη δουλειά χρησιμοποιείται ο αλγόριθμος PRBS (Pseudo Random Binary Sequence).

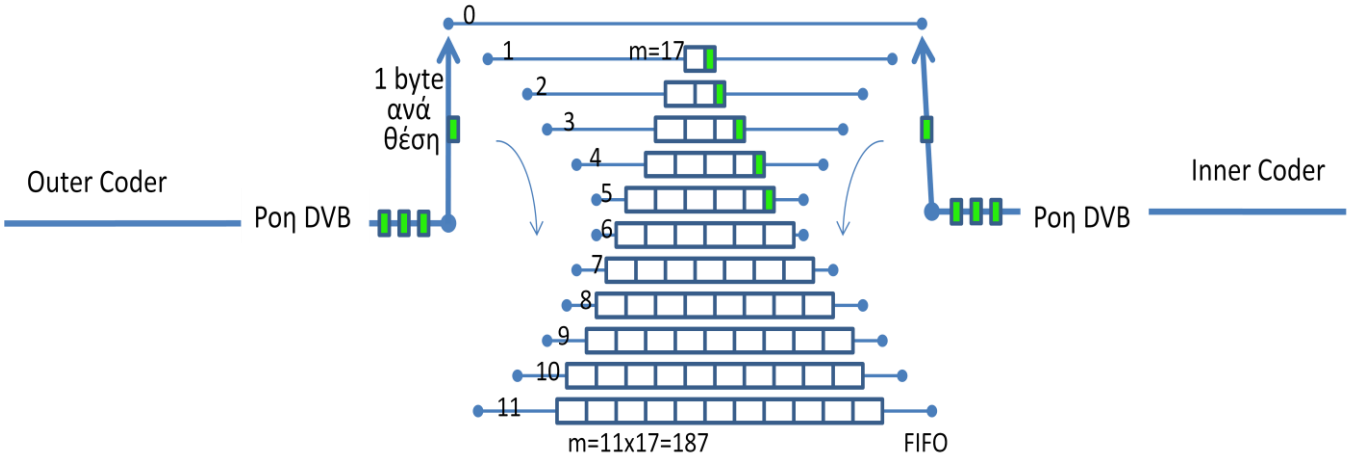
3.2.2.1.2 Εξωτερική Κωδικοποίηση (Outer Coder)

Εδώ γίνεται η πρώτη προσθήκη επιπλέον bytes για κωδικοποίηση. Στο DVB-S χρησιμοποιείται μια πιο μικρή έκδοση του κώδικα RS (Reed-Solomon). Ο RS ανακαλύφθηκε το 1960 από τους Irving Reed και Gustave Solomon ερευνητές του MIT. Όπως είπαμε ο κώδικας προσθέτει επιπλέον bytes στη ροή έτσι ώστε ο δέκτης να μπορεί να καταλαβαίνει που υπάρχει λάθος. Η κωδικοποίηση RS εφαρμόζεται στα CD και στις διαστημικές μεταδόσεις, όπως και στο ADSL. Έχει το πλεονέκτημα της μικρής προσθήκης byte-διόρθωσης, της χαμηλής απαίτησης σε υπολογιστική ισχύ, όπως και της καλής απόδοσης. Ενώ η αρχική έκδοση του αλγορίθμου του είναι η RS (255, 239, t = 8) στο DVB-S χρησιμοποιείται η έκδοση RS (204, 188, t = 8) δηλαδή 188 bytes μπαίνουν 204 βγαίνουν και μέγιστος αριθμός λαθών που ανιχνεύονται είναι 8. Για να γίνει αυτή η κοντύτερη έκδοση απλώς προστίθενται 51 μηδενικά bytes στην είσοδο του κωδικοποιητή (255, 239) δηλαδή 188+51=239 bytes. Αφού βγουν από τον κωδικοποιητή (255, 239) γίνονται 239 bytes, από τα οποία αφαιρούνται τα 51 μηδενικά και περνούμε τα 255-51 = 204 bytes που προβλέπονται από την μικρότερη έκδοση. Στο πιο πρόσφατο πρότυπο το DVB-S2 χρησιμοποιείται η κωδικοποίηση BCH (Bose Chaudhuri Hocquenghem) . Στην ουσία ο BCH αποτελεί οικογένεια κωδικών μέρος της οποίας ανήκει και ο RS (Reed- Solomon) . Αν και ο RS έχει ικανότητα για διόρθωση μέχρι 8 σφάλματα ο BCH έχει μεταβλητό βαθμό διόρθωσης που μπορεί να φτάσει και 255 σφάλματα με το BCH (1023, 11) με αύξηση βεβαία του πλεονάσματος σε bytes-διόρθωσης. Σημειώνουμε ότι ο κώδικας που εφαρμόζεται εδώ ονομάζεται τμηματικός διότι ομαδοποιεί ανά τμήματα τα bytes δίνοντας τους σύμβολα και στα σύμβολα άλλα σύμβολα, πχ. το 01→ α, το 00→ β ενώ το αβ → Α.

3.2.2.1.3 Αναδιάταξη (Inteleaver)

Η ακολουθία των δεδομένων αναδιοργανώνεται ώστε να αποφεύγονται μεγάλες ακολουθίες λαθών. Η αναδιάταξη εφαρμόστηκε με επιτυχία στα CD (compact disk-πηκτικός δίσκος). Όταν το CD εμφάνιζε γδάρσιμο σε ένα σημείο υπήρχε η μαζική απώλεια συνεχόμενων bits και η ακρόαση τραγουδιού για λίγα δευτερόλεπτα γινόταν ανέφικτη. Άμα όμως ανακατώσουμε τα δεδομένα (αναδιάταξη) τα βάλουμε στο CD και αυτό εμφανίσει απώλεια σε ένα κομμάτι (γδάρσιμο) ,τότε χάνουμε μικρό κομμάτι από όλες τις πληροφορίες του CD και όχι ένα κομμάτι συνεχομένων bits. Έτσι τα περιεχόμενα του CD (τραγούδια) μπορούν να αναπαραχθούν χωρίς να γίνει αντιληπτή η απώλεια των bits. Έτσι και το DVB εφαρμόζει αυτή την τεχνική για να έχουμε μικρή συνολική απώλεια πληροφορίας σε σημειακή αποκοπή της ροής. Η όλη αναδιάταξη γίνεται με απλούς τρόπους. Ένας από αυτούς είναι το γέμισμα ενός πίνακα με τη ροή ανά γραμμή και άδειασμα του πίνακα ανά στήλη έτσι η τελική ροή που λαμβάνεται είναι πλήρως ανακατεμένη.

Εδώ για το ανακάτωμα αυτό χρησιμοποιείται ο αλγόριθμος Forney, ο οποίος προβλέπει την εξής διάταξη:



Σχήμα 11 :Αναδιατάκτης-Interleaver

12 ουρές FIFO (first in first out) με μεταβλητό μέγεθος από 0 bytes έως 17X11 = 187bytes με βήμα αύξησης 17bytes, δηλαδή έχουν μέγεθος 0, 17, 34…. 187. Το βήμα δεν είναι τυχαίο αυτό γιατί θέλουμε να ανακατέψουμε το πακέτο PES που εξέρχεται από το RS coder και έχει μέγεθος 204 bytes για 12 ουρές αρά 204/12 =17 και προκύπτει το βήμα του μεταβλητού μεγέθους των FIFOs. Μεταφέρονται 1 byte σε κάθε ουρά με ταυτόχρονη μετακίνηση του δείκτη στην επομένη FIFO ουρά και μεταφορά εκεί του επομένου byte. Τα bytes από τις FIFO ουρές με δεύτερο δείκτη (συγχρονισμένο με τον πρώτο) αφαιρούνται από τις ουρές και η ροή ξανασχηματίζεται με ανακατωμένη όμως κατάσταση.

3.2.2.1.4 Εσωτερική Κωδικοποίηση (Inner Coder)

Μετά το ανακάτεμα χρησιμοποιείται ο συνελικτικός ή πιθανοκρατικός κώδικας. Γιατί χρησιμοποιείται όμως ο συνελικτικός κώδικας επιπλέον του τμηματικού; Αποδείχτηκε ότι η χρησιμοποίηση τόσο συνελικτικών όσο και τμηματικών κωδικών ανεξάρτητα δε μας δίνει ικανοποιητικό βαθμό αντίστασης κατά των λαθών και ότι μόνο συνδυασμός τους δίνει τα βέλτιστα αποτελέσματα. Στο DVB-S ο συνελικτικός κώδικας που χρησιμοποιείται είναι ο Viterdi (ο οποίος ζει και είναι διευθύνων σύμβουλος στη Qualcomm που είναι η μεγαλύτερη εταιρία κινητής τηλεφωνίας στον κόσμο). Οι συνελικτικοί κώδικες δεν επεξεργάζονται ανά τμήμα τη ροή αλλά δουλεύουν πάνω σε όλη τη ροή την οποία ‘’ανακατευθύνουν’’ με δικό τους μονοσήμαντο τρόπο. Έτσι ξέροντας το δρομολόγιο της νέας ροής (σκεφτείτε δρομολόγιο πάνω στο χάρτη) ο δέκτης μπορεί μια λάθος παράκαμψη στο δρομολόγιο της ροής (λόγου σφάλματος) να την εντοπίσει και να τη διορθώσει. Με τον συνελικτικό κώδικα η ροή διπλασιάζεται αφού δημιουργούνται δύο ροές εξόδου με μέγεθος η καθεμιά ίσο με αυτό της εισερχομένης ροής. Για να έχει ευχέρεια ο εκπομπός μπορεί να διαλέξει να έχει λιγότερη αξιοπιστία κάνοντας οικονομία στην εκπεμπόμενη ροή. Γι αυτό το λόγο το DVB-S προέβλεψε κόψιμο bits σε συγκεκριμένες θέσεις στη διπλή ροή που εξέρχεται από τον συνελικτικό κώδικα. Οι ροές εξέρχονται με κλάσματα (ή FEC εσωτερικού κώδικα) 1/2, 2/3, 3/4, 5/6, 7/8 ως προς τη ροή εισόδου. Το 1/2 σημαίνει μπαίνει 1 bit διπλασιάζεται και βγαίνουν 2 bits αφού η ροή διπλασιάζεται (και αρά δε κόβεται κανένα bits όποτε βέλτιστη αντοχή λαθών). Ενώ το 7/8 πχ σημαίνει μπαίνουν 7 bits

διπλασιάζονται γίνονται 14 bits και βγαίνουν στο τέλος 8 bits αρά κόπηκαν για οικονομία εύρους ζώνης 6 bits.

Το σύγχρονο πρότυπο DVB-S2 χρησιμοποιεί τους κώδικες LDPC (Low Density Parity Check) και στα ελληνικά κωδικοποίηση έλεγχου ισοτιμίας ήπιας μορφής. Ανακαλύφθηκαν το 1962 από τον R.Gallager, έχουν απλή αλγεβρική κατασκευή και εύκολο αλγόριθμο αποκωδικοποίησης (ο αποκωδικοποιητής βρίσκεται στο δέκτη του χρήστη), κύριο ατού (πλεονέκτημα) τους όμως είναι ότι η υλοποίηση τους αποκλίνει από το απαράβατο, από τη φύση, όριο του Shannon κατά 0, 6 έως 1, 2 db.

Είναι η πρώτη πρακτική εφαρμογή του θεωρητικού κώδικα LDPC και αυξάνει τις τιμές του FEC σε 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 5/6, 8/9, 9/10.

Το τελικό FEC του κάθε συστήματος κωδικοποίησης ισούται με το γινόμενο των FEC της εξωτερικής και εσωτερικής κωδικοποίησης. Για παράδειγμα για το DVB-S, είναι το γινόμενο του FEC του RS που είναι 188/204 **επί** το FEC του συνελικτικού κώδικα πχ. 3/4, άρα 188/204*3/4=47/68.

Αν και η διαμόρφωση ακόμα δεν έχει γίνει, οι δύο ροές που σχηματίζονται από το συνελικτικό κώδικα προετοιμάζονται για τη διαδικασία της διαμόρφωσης. Αυτή η προετοιμασία αναφέρεται ως mapping (χαρτογράφηση) κατά την οποία οι 2 ροές ομαδοποιούνται σε bits και δημιουργούν τα σύμβολα (symbol mapping) τα οποία μεταφράζονται σαν σημεία ‘’ψηφιακές θέσεις ‘’ στο συναστρικό διάγραμμα (Constellation diagramm) της διαμόρφωσης που χρησιμοποιείται. Αναλυτική ερμηνεία αυτών των όρων γίνεται κάτωθι στη διαδικασία διαμόρφωσης.

3.2.2.2 Διαμόρφωση

Η επομένη και τελική διαδικασία που υποβάλλεται η ψηφιακή ροή είναι η διαμόρφωση. Η διαμόρφωση στην ουσία είναι η μετατροπή της ψηφιακής ροής σε αναλογική μορφή με τρόπο τέτοιο που στη λήψη της αναλογικής ροής να μπορεί να γίνει η μετατροπή πίσω στην αρχική ψηφιακή.

Για να εξηγήσουμε όμως τα συναστρικά διαγράμματα πρέπει να εξηγήσουμε την διαδικασία της διαμόρφωσης.

Λόγω μέσου μετάδοσης (αέρας) οι δορυφορικές επικοινωνίες χρησιμοποιούν τις αναλογικές μεταδόσεις (η ψηφιακή μετάδοση λόγω θορύβου και διαλείψεων δε μπορεί να χρησιμοποιηθεί) . Η αναλογική μετάδοση γίνεται με σήμα της μορφής

$$C(t) = A(t)\,\text{συν}(\omega\psi)$$

Όπου

C (t) :το σήμα ή καλύτερα το φέρον, αφού '' φέρει'' την πληροφορία

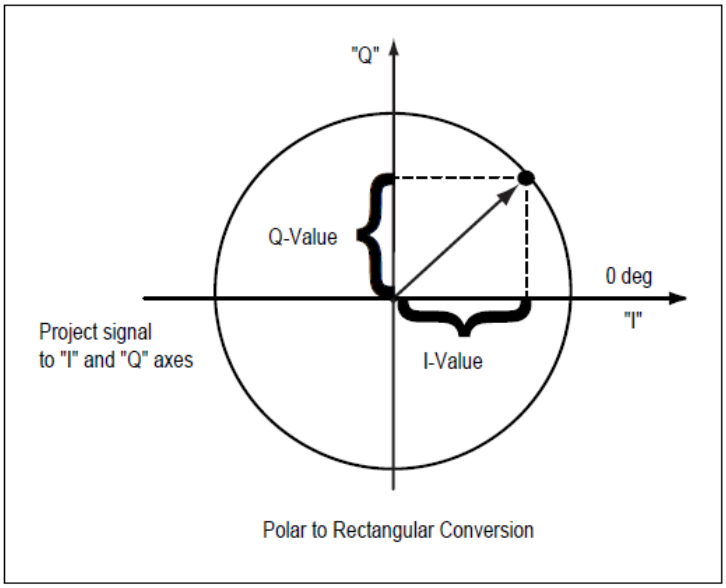
A (t) :μέτρο του σήματος

ω:η συχνότητα του περιστρεφόμενου διανύσματος(αν αναλύσουμε το σήμα σαν διάνυσμα)

ψ:η φάση του διανύσματος (η γωνία του διανύσματος για συχνότητα ω=0)

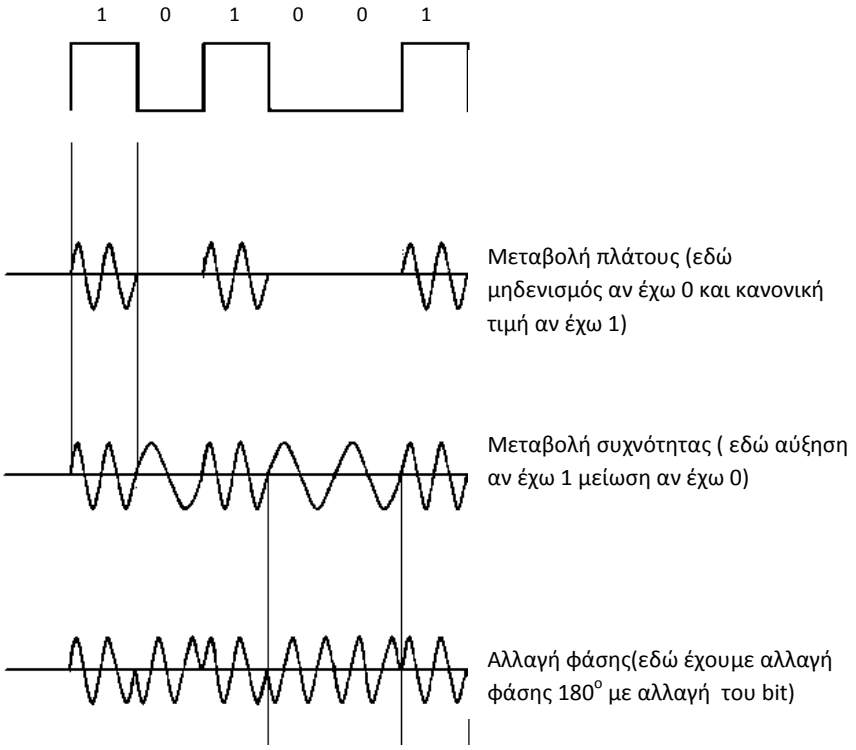
Το σήμα αυτό αναλύεται γεωμετρικά (με τριγωνομετρία) σε δύο ορθογώνιες συνιστώσες (για ψ=0) όπως δείχνει γραφικά το σχήμα 12 και λαμβάνουμε την συμφασική ή μιγαδική συνιστώσα I (In Phase) όπου $I = A(t)\,\text{συν}\omega t$ και την ορθογώνια ή πραγματική συνιστώσα Q (Quadrate) όπου $Q = A(t)\,\eta\mu\omega t$.

Τα δύο σήματα (I, Q) αποτελούν το φέρον σήμα που ανάλογα με το σήμα πληροφορίας διαμορφώνεται (αλλάζουν τα χαρακτηριστικά του)



Σχήμα 12 : Η ανάλυση του φέροντος σε I και Q συνιστώσα. Η γνώση της τιμής του I και Q μας δίνει πληροφορίες ποιά bits περιέχονται στο σήμα.

Στις ψηφιακές επικοινωνίες η πληροφορία είναι τα bits (0 ή 10. Για να μεταφερθούν τα bits στο φέρον και για να γίνουν αντιληπτά στο δέκτη απλώς μεταβάλλουμε μια από τις 3 παραμέτρους του φέροντος σήματος. Αυτές είναι το **μέτρο** οπότε έχουμε την ASK (Amplitude-shift keying) διαμόρφωση, τη **συχνότητα** με την FSK (Frequency-shift keying), τη **φάση** με την PSK (Phase-shift keying). Οι τρεις παράμετροι φαίνονται στο σχήμα 13:



Σχήμα 13: Σχηματικά οι τρεις μεταβολές παραμέτρων (μέτρο, συχνότητα, φάση)

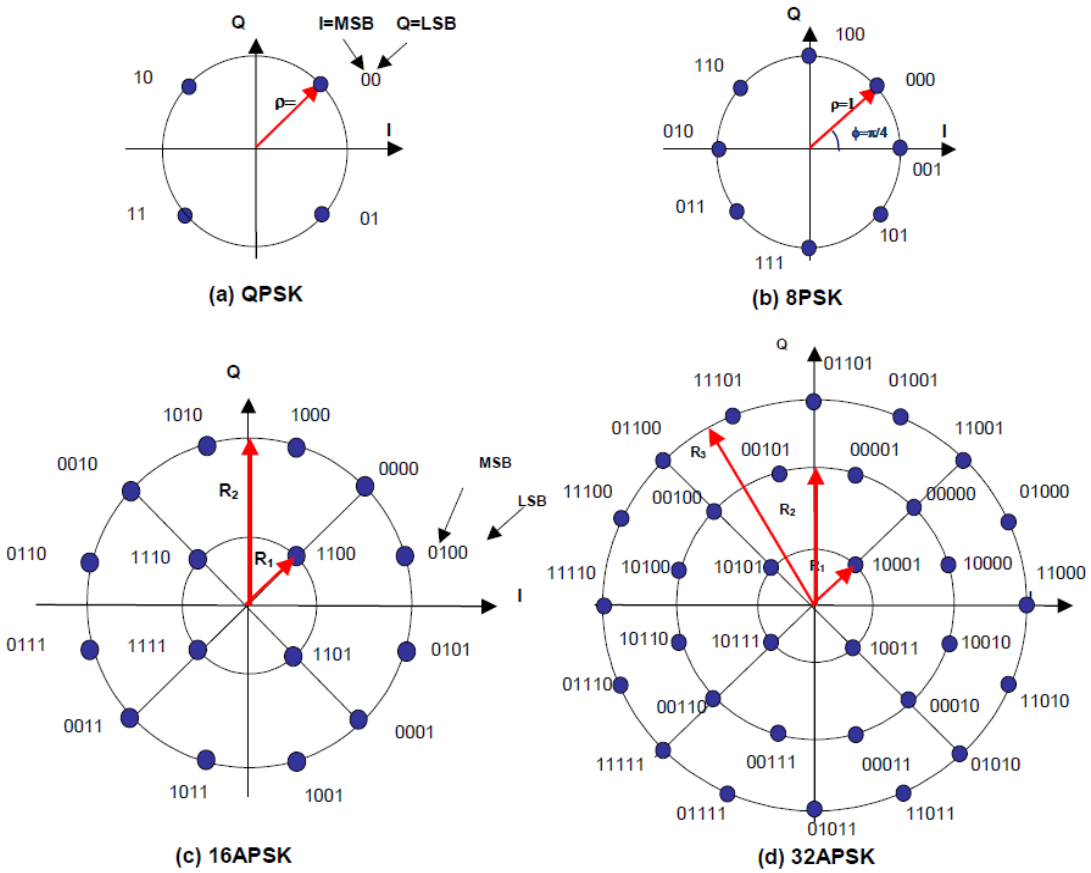
Αυτές οι διαμορφώσεις είναι για δυική μεταβολή κάποιας παραμέτρου, για επιπλέον εξοικονόμηση εύρους ζώνης ή για αποστολή μεγαλυτέρου ρυθμού bits στο ίδιο εύρος υπάρχουν οι Μ-διαμορφώσεις, όπως π.χ. η QPSK (quatre-Phase-shift keying) με 4 διαφορετικές φάσεις, η 8PSK (8-Phase-shift keying) με 8 διαφορετικές φάσεις, η ή 4ASK (4-Amplitude-shift keying) με 4 διαφορετικά πλάτη.

Ενώ τέλος με τη ανάπτυξη της μικροηλεκτρονικής δημιουργηθήκαν κυκλώματα που επιτρέπουν το συνδυασμό παραμέτρων με εκπληκτικά αποτελέσματα στην αύξηση του ρυθμού μετάδοσης των bits. Αυτές είναι η 16 ή 32APSK (Amplitude and Phase-shift keying) οπού μεταβάλλονται και η φάση και το πλάτος του φέροντος ταυτόχρονα και με πολλές διαφορετικές στάθμες (Σχήμα 14).

Γενικά όσες παραπάνω διαφορετικές μεταβολές(σε αριθμό και τρόπο) υποβάλουμε το φέρον τόσους παραπάνω συνδυασμούς-καταστάσεις μπορούμε να κάνουμε (άρα παραπάνω πληροφορία να μεταδώσουμε). Σύμβολο ονομάζουμε τον αριθμό των bits πληροφορίας που αποστέλλονται σε κάθε διαμόρφωση(π.χ. 2 ή 3 bits), ενώ οι καταστάσεις είναι ο αριθμός $2^{(\text{bits συμβόλου})}$ πχ 2^2=4 ή 2^3=8 και δείχνει πόσους διαφορετικούς συνδυασμούς bits μπορούμε να έχουμε με ένα συγκεκριμένο αριθμό συμβόλου .Έτσι με σύμβολο 1 bit μπορούμε να έχουμε δύο συνδυασμούς (0 ή 1) ενώ με 2 bits (πχ PSK) μπορούμε να έχουμε 4 συνδυασμούς (00, 01, 10, 11) ενώ με την 32APSK έχουμε 32 καταστάσεις, με σύμβολο των 5bits (πχ 01001) . Επειδή ο ρυθμός μετάδοσης συμβόλου είναι σχεδόν σταθερός ανά διαμόρφωση αφού είναι ένα στιγμιότυπο του φέροντος γίνεται

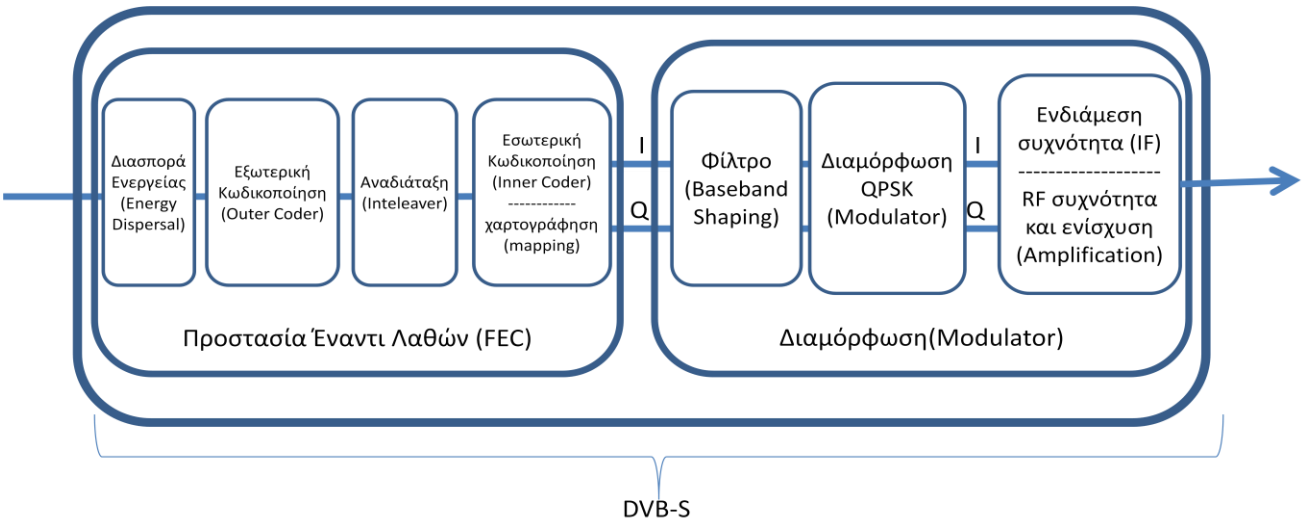
εύκολα αντιληπτό ότι αύξηση του αριθμού των bits ανά σύμβολο προκαλεί αύξηση της ροής των bits.

Κάθε διαμόρφωση όπως είδαμε ανάλογα με τις διαφορετικές μεταβολές που μπορεί να υποστεί το φέρον της, τόσους συνδυασμούς μπορεί να μεταδώσει. Όμως χρειάζεται μια αντιστοίχηση των συνδυασμών των bits (που αποτελείται από 0 και 1) με τις τιμές των συνιστωσών **I** και **Q** (που αποτελείται από μετρό και φάση)**.** Αυτή την αντιστοίχηση ή mapping στην τεχνική ορολογία, μας την παρέχει ο mapping table (πίνακας χαρτογράφησης- σχήμα 19 για QPSK). Ο πίνακας χαρτογράφησης ανάλογα με τα bits εισόδου δίνει τις κατάλληλες εξόδους **I** και **Q** οι όποιες με τη σειρά τους εισέρχονται στον διαμορφωτή και ενσωματώνονται στο φέρον. Η αναπαράσταση του συνδυασμού των bits στην αναλογική μετατροπή τους γίνεται με τα συναστρικά διαγράμματα κάθε διαμόρφωσης. Αυτά δείχνουν για κάθε τιμή των **I** και **Q** συνιστωσών τον ανάλογο συνδυασμό των bits που αντιστοιχεί έτσι ώστε να μπορεί ο δέκτης ξερώντας τον πίνακα χαρτογράφησης και το συναστρικό διάγραμμα να μπορεί να καταλάβει ποια bits ήθελε ο πομπός να εκπέμψει. Παρακάτω φαίνονται τα διαγράμματα των QPSK (a) , 8PSK (b) , 16APSK (c) και 32APSK (d) :



Σχήμα 14: τα συναστρικά διαγράμματα των QPSK (a) , 8PSK (b) , 16APSK (c) και 32APSK (d) , οπού R1, R2, R3 τα διαφορετικά πλάτη διαμόρφωσης (σε Volts), ενώ MSB:most significant bit, LSB:less significant bit. Το MSB εξέρχεται πρώτο από τη ροή και τελευταίο βγαίνει το LSB (δηλαδή ο συνδυασμός των bits αντιστρέφεται κατά την έξοδο). Παρατηρούμε ότι όσο αυξάνονται οι στάθμες των I και Q τιμών τα bits ανά σύμβολο (συνδυασμό) αυξάνονται από 2bits στην QPSK σε 5bits στην 32APSK.

Επανερχόμαστε τώρα στη διαδικασία της διαμόρφωσης του DVB-S παρουσιάζοντας το block-διάγραμμα



Σχήμα 15 : Τα στάδια της διαμόρφωσης

Δημιουργία σύμβολου – Χαρτογράφηση (mapping)

Όπως είπαμε στο τελευταίο στάδιο του FEC (εσωτερική κωδικοποίηση) σχηματίζονται δύο ροές, αυτές υφίστανται το symbol mapping δηλαδή χωρίζονται σε σύμβολα. Στο DVB-S η μόνη και αυτή διαμόρφωση που χρησιμοποιείται είναι η QPSK ενώ στη DVB-S2 που θα συζητηθεί παρακάτω είναι η QPSK, 8PSK, 16APSK και 32APSK. Η QPSK έχει ανά σύμβολο 2 bits διότι έχει 4 διαφορετικές καταστάσεις για τα I και Q (αφού δέχεται 4 διαφορετικές τιμές φάσης), γενικά αν M οι διαφορετικές καταστάσεις της διαμόρφωσης τότε τα bits **n** που χρησιμοποιούνται ανά σύμβολο είναι $n=\log_2 M$. Έτσι τα bits σε DVB-S χωρίζονται ανά δύο και οδηγούνται στο QPSK table mapping που φαίνεται εδώ

Bit 1	Bit 0	I σε Volts (V)	Q σε Volts (V)
0	0	+1	+1
1	0	-1	-1
0	1	-1	+1
1	1	+1	-1

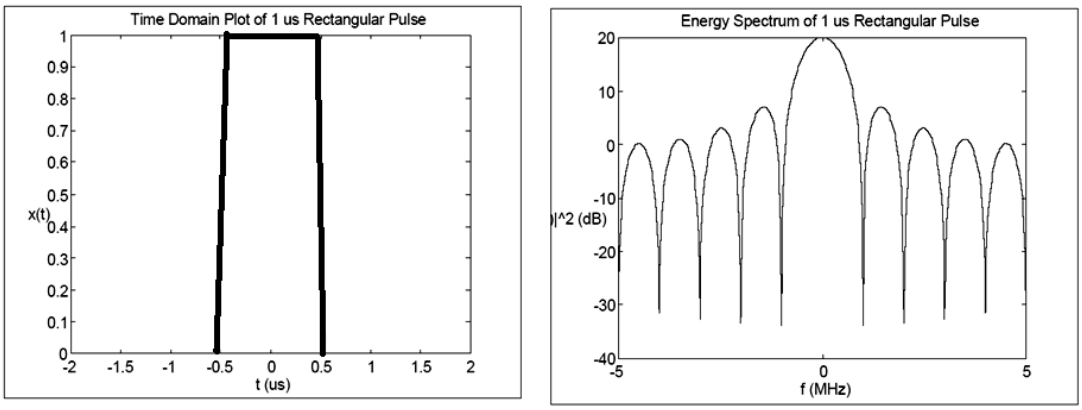
Σχήμα 16:Πινακας αντιστοίχισης των bits της QPSK σε I και Q ροές

όπου και αντιστοιχίζονται (κωδικοποιούνται στην ουσία) σε I και Q ροές. Η αντιστοίχηση-κωδικοποίηση (διαφορετική με την κωδικοποίηση FEC) είναι απευθείας κωδικοποίηση δηλαδή κάθε σύμβολο (κωδικό λέξη ή κατάσταση) λαμβάνει μια τιμή φέροντος. Ενώ υπάρχει και η διαφορική κωδικοποίηση που δεν αποστέλλονται τα ψηφία πληροφορίας απευθείας αλλά νέα ψηφία που δημιουργούνται από διαφορικό κωδικοποιητή με συγκεκριμένο κανόνα κάθε φορά. Συνήθως ο κανόνας είναι να αποστέλλονται συγκεκριμένα bits κατά τη μετάβαση του προηγούμενου σύμβολου με το επόμενο (δηλαδή σε ένα πίνακα υπάρχουν όλες οι πιθανές μεταβιβάσεις και όλα τα αντίστοιχα bits ή κώδικες λέξης που αποστέλλονται).

Στο DVB-S2 χρησιμοποιείτο εκτός από την QPSK οι: 8QPSK, 16APSK, 32 APSK. Αυτές έχουν αντίστοιχα μέγεθος σύμβολου 3, 4, 5 bits. Στο DVB-S2 εφαρμόζεται bit interleaver μετά το συνελικτικό κώδικα (όχι πριν) και δημιουργείται το σύμβολο από τη ροη. Κάθε σύμβολο μπαίνει σε ένα μετατροπέα και εξέρχεται ανάλογα με την τιμή των bits που το απαρτίζουν σε ροές I και Q.

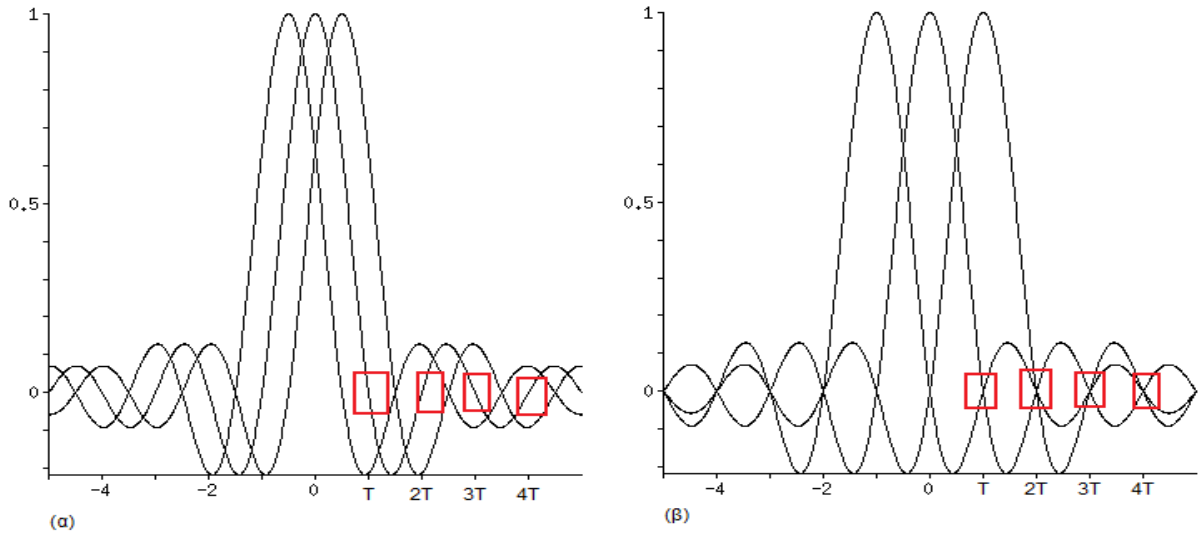
3.2.2.2.1 Φίλτρο

Οι δύο ροές εισέρχονται όπως δείχνει και το σχήμα 14 στο φίλτρο. Γιατί όμως χρειάζεται φίλτρο; Οι ροές αποτελούνται από σύμβολα ψηφιών που αποτελούν ορθογωνίους παλμούς NRZ (από 0 έως 1). Από την ανάλυση Fourier γνωρίζουμε ότι το εύρος ζώνης ενός ιδανικού ορθογώνιου παλμού είναι άπειρο (βλέπε σχήμα 17) .



Σχήμα 17: (α) χρονική περιγραφή ορθογώνιου παλμού (β) φασματική περιγραφή (το φάσμα ορθογώνιου παλμού δείχνει ότι έχει μεγάλο ανεπιθύμητο εύρος ζώνης)

Καθότι οι διάφορες τηλεπικοινωνιακές διατάξεις όπως και το μέσο μετάδοσης έχουν ένα συγκεκριμένο εύρος ζώνης είναι επόμενο οι ιδανικοί ορθογώνιοι παλμοί να φιλτράρονται καθώς η πληροφορία διαδίδεται από τον πομπό στο δέκτη. Το αποτέλεσμα αυτού του απλού φιλτραρίσματος είναι η διασπορά των συμβόλων που χρησιμοποιούνται για τη μετάδοση δεδομένων. Η διασπορά (λόγω του πεπερασμένου εύρους ζώνης είτε του μέσου διάδοσης) των διαδοχικών συμβόλων έχει ως αποτέλεσμα την επικάλυψη μέρους της ενέργειας του ενός με τα γειτονικά του προκαλώντας έτσι το λεγόμενο πρόβλημα της διασυμβολικής παρεμβολής (ISI-intersymbol interference) σχήμα 18(α). Η διασυμβολική παρεμβολή είναι ένα πρόβλημα για το δέκτη αφού λόγω παρεμβολής δε μπορεί να διαχωρίσει το τρέχον σύμβολο από τα γειτονικά του. Έτσι, ακόμη και στην περίπτωση που δεν έχουμε θόρυβο σε ένα κανάλι επικοινωνίας, η διασυμβολική παρεμβολή μπορεί να οδηγήσει στην λανθασμένη ανίχνευση συμβόλων στο δέκτη μας, έχοντας ως αποτέλεσμα τον αναπόφευκτο ρυθμό σφαλμάτων. Το φαινόμενο της διασυμβολικής παρεμβολής είναι δυνατόν να περιοριστεί σε τέτοιο βαθμό, ώστε να μην υποβαθμίζει την ποιότητα της ζεύξης αναφορικά με τον παρατηρούμενο ρυθμό εμφάνισης σφαλμάτων χρησιμοποιώντας συγκεκριμένα φίλτρα. Για να εξαλειφτεί η επίδραση ISI πρέπει το σύστημα μας να σχεδιαστεί έτσι ώστε οι επικαλυπτόμενοι παλμοί να μην δημιουργούν πρόβλημα στην ορθή εκτίμηση ενός δυαδικού σύμβολου. Αυτό γίνεται αν έχουν μηδενική τιμή την στιγμή που κάνουμε δειγματοληψία (λήψη απόφασης) του λαμβανομένου σήματος (τετραγωνάκια στο σχήμα 18(α)). Δηλαδή αν αντί το σχήμα 18(α) τριών παλμών με επικάλυψη να έχουμε το 18(β) χωρίς επικάλυψη στους χρόνους δειγματοληψίας από το δέκτη.



Σχημα18:(α) τρεις παλμοί με επικάλυψη ISI στους χρόνους δειγματοληψίας (β) χωρίς επικάλυψη στους χρόνους δειγματοληψίας (τετραγωνάκια) από το δέκτη, με φίλτρο Nyquist

Με μαθηματικούς όρους, θέλουμε ο παλμός να ικανοποιεί την σχέση

$$x(kT)=\begin{cases}1, & k=0\\ 0, & k\neq 0\end{cases}$$

όπου k είναι ακέραιος και T η χρονική απόσταση του σύμβολου κωδικοποίησης. Δηλαδή ο παλμός να μηδενίζεται για ακέραιους πολλαπλασίους χρόνους T **στους όποιους γίνεται η δειγματοληψία** από το δέκτη και το σήμα μας θέλουμε **εκείνη και μόνο εκείνη** τη στιγμή να μην έχει ISI. Τα σημεία αυτά φαίνονται όπως προαναφέραμε με τετραγωνάκια στο σχήμα 18(β).

Ικανή και αναγκαία συνθήκη για να ισχύει η πιο πάνω σχέση είναι η συνθήκη Nyquist:

$$\sum_{m=-\infty}^{\infty} X\left(f+\frac{m}{T}\right)=T$$

Στο DVB-S χρησιμοποιούμε το φίλτρο Nyquist ανυψωμένου συνημίτονου με φασματικά χαρακτηριστικά:

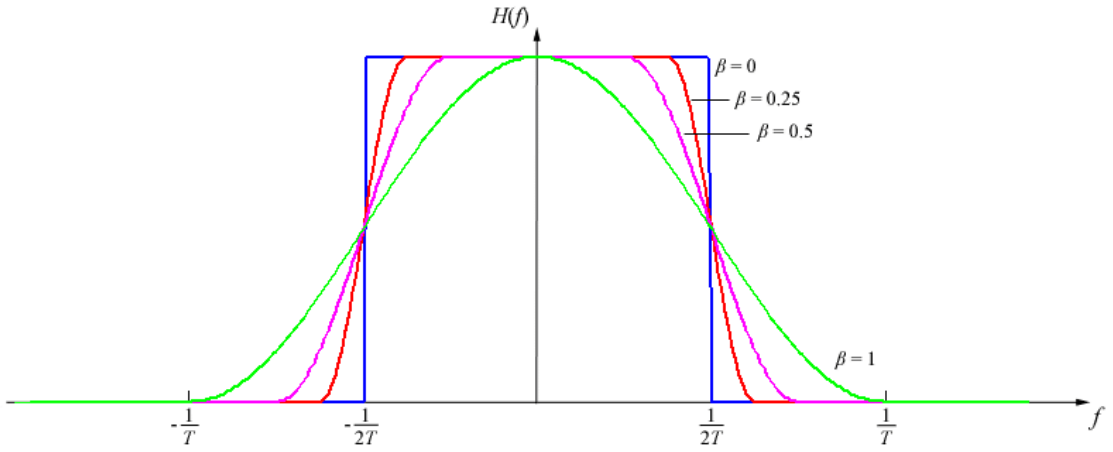
$$H(f)=\begin{cases}T, & |f|\le \frac{1-\beta}{2T}\\ \frac{T}{2}\left[1+\cos\left(\frac{\pi T}{\beta}\left[|f|-\frac{1-\beta}{2T}\right]\right)\right], & \frac{1-\beta}{2T}<|f|\le\frac{1+\beta}{2T}\\ 0, & |f|\ge\frac{1-\beta}{2T}\end{cases}$$

H (f) είναι ο Fourier μετασχηματισμός της **h (t)** , όπου h (t) είναι η κρουστική απόκριση

$\mathbf{f_N}$ =1 / 2T=R_S/2 είναι η συχνότητα Nyquist

T : είναι η διάρκεια συμβόλου

β : ο παράγοντας εξασθένισης (roll-off factor**)** και λαμβάνει τιμές από 0 έως 1 ($0\le\beta\le1$) και είναι ανάλογος του πρόσθετο εύρους ζώνης που καταλαμβάνει το σήμα μετά της συχνότητας Nyquist (1 / 2T)

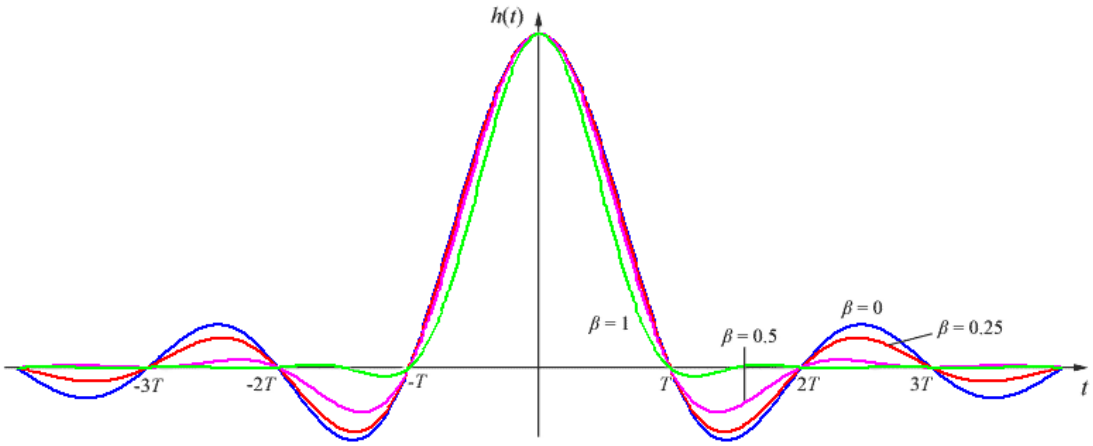


Σχήμα 18.1 : φάσμα παλμού

Ενώ το φάσμα του H (f) είναι

$$h(t) = \mathrm{sinc}\left(\frac{t}{T}\right)\frac{\cos\left(\frac{\pi\beta t}{T}\right)}{1-\frac{4\beta^2 t^2}{T^2}}$$

όπου φυσικά sinc (t/T) =sin (πt/T) / (πt/T)



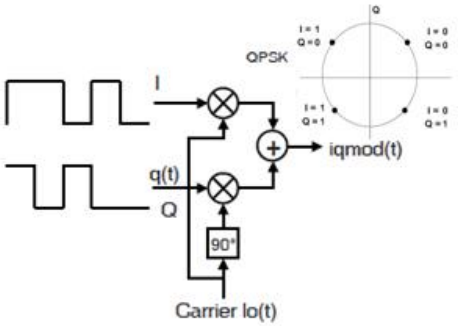
Σχήμα 18.2 :παλμός ανυψωμένου συνημίτονου σε χρονική περιγραφή για β={0. 25, 0. 5, 1}

Από τη γραφική παράσταση της χρονικής απόκρισης παρατηρούμε τη θεωρητική συνθήκη Nyquist που πρέπει να ικανοποιεί το φίλτρο και είναι :η χρονική απόκριση να παρουσιάζει μηδενικά σε περιόδους πολλαπλάσιους της περιόδου **T** των συμβόλων. Το φίλτρο είναι όπως είπαμε ένα αυξημένο φίλτρο συνημίτονου και προκειμένου να βελτιστοποιηθούν το εύρους ζώνης και η αναλογία σήματος προς θόρυβο, το φιλτράρισμα μοιράζεται εξίσου μεταξύ του πομπού και του δέκτη, κάθε ένας από τους οποίους περιλαμβάνει ένα φίλτρο που ονομάζεται τετραγωνικής ρίζας ανυψωμένο συνημίτονο. Γινόμενο τον δύο φίλτρων δίνει το ανυψωμένο.

Το DVB-S έχει β=0. 35 ενώ το DVB-S2 έχει μεταβλητό β για ποιο μεγάλη ευελιξία και παίρνει τις τιμές β={ 0. 35, 0. 25, 0. 20}.

3.2.2.2.2 Διαμόρφωση QPSK

Αφού οι I και Q ροές εξέλθουν του φίλτρο μετατρέπονται σε αναλογική μορφή και ανάγονται σε συχνότητα IF (ενδιάμεση συχνότητα). Στο DVB-S όπως αναφέραμε η διαμόρφωση είναι η QPSK δηλαδή υπάρχουν 4 καταστάσεις σύμβολου (00, 01, 11, 10) και με 2 bits ανά σύμβολο (1 bit από την I και 1 bit από την Q) . Όπως φαίνεται στο σχήμα 19 ένας τοπικός ταλαντωτής με φέρον συχνότητας IF διαμορφώνουν με $\sin\omega_0 t$ την Q συνιστώσα του διαγράμματος και με $\cos\omega_0 t$ τη συνιστώσα I. Η υπέρθεση των δύο δίνει σαν έξοδο ένα από τους 4 συνδυασμούς.



$p_i(t)$	Bit	$p_q(t)$	Bit	QPSK
1 V	(1)	1 V	(1)	$\cos\omega_0 t - \sin\omega_0 t = \sqrt{2}\cos(\omega_0 t + 45°)$
1 V	(1)	−1 V	(0)	$\cos\omega_0 t + \sin\omega_0 t = \sqrt{2}\cos(\omega_0 t - 45°)$
−1 V	(0)	1 V	(1)	$-\cos\omega_0 t - \sin\omega_0 t = \sqrt{2}\cos(\omega_0 t + 135°)$
−1 V	(0)	−1 V	(0)	$-\cos\omega_0 t + \sin\omega_0 t = \sqrt{2}\cos(\omega_0 t - 135°)$

Digital Video and Audio Broadcasting Technology
W. Fischer
ISBN 978-3-540-76357-4

Σχήμα 19: διαμόρφωση I και Q ροών σε συχνότητα IF μαζί με το mapping table (QPSK)

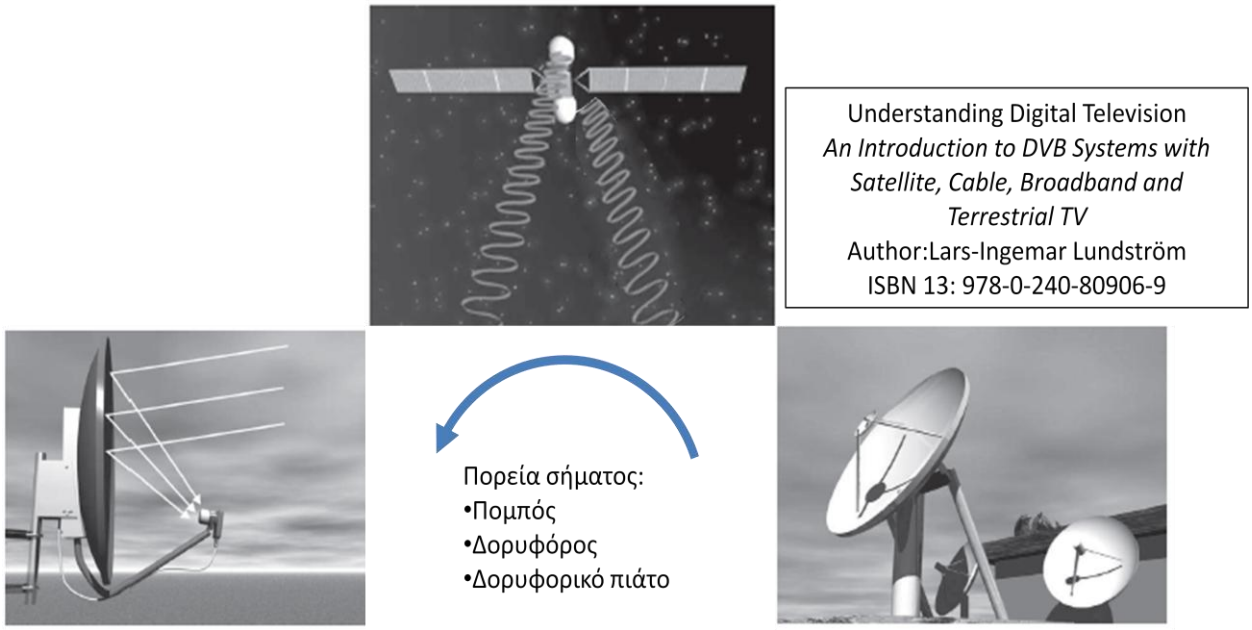
Αξίζει να αναφερθεί ότι τα ηλεκτρομαγνητικά κύματα διαθέτουν στην ίδια συχνότητα δύο πολώσεις (κάθετη – οριζόντια).Αυτή τη φυσική ιδιότητα εκμεταλλεύονται οι τηλεπικοινωνίες και χρησιμοποιούν και τις δύο για αποστολή διαφορετικής πληροφορίας σε κάθε πόλωση. Έτσι γίνεται μέγιστη εκμετάλλευση του εύρους ζώνης. Εννοείται ότι η συσκευή λήψης(LNB) όπως θα δούμε και πιο κάτω είναι σε θέση να ξεχωρίσει και να αποδώσει στο δέκτη τις δύο πολώσεις .

3.2.2.2.3 Ενίσχυση και εκπομπή

Η διαμορφωμένη έξοδος υφίσταται ανύψωση της συχνότητας του φέροντος από την IF στην RF(συχνότητα εκπομπής). Το ανορθωμένο σήμα ενισχύεται με ενισχυτή ισχύος HPA που του προσδίνει την τελική ισχύ εκπομπής και οδηγείται στη διάταξη σύζευξης για εκπομπή που είναι η κεραία. Η όχι απευθείας διαμόρφωση στην RF (14-18GHz) συχνότητα αλλά διαμόρφωση στη IF (70-140MHz) και μετά άνω μετατροπή στην RF, οφείλεται στο γεγονός ότι οι διαμορφωτές σε συχνότητες RF είναι δαπανηροί και δύσκολα εφαρμόσιμοι.

3.3 ΔΟΡΥΦΟΡΟΣ -ΕΠΑΝΑΛΗΠΤΗΣ

Η διάταξη εκπομπής είναι μεγάλα παραβολικά κάτοπτρα προσανατολισμένα στον εκάστοτε δορυφόρο που έχει ναυλώσει ο κάθε πάροχος. Αφού το κάτοπτρο προσανατολιστεί με το δορυφόρο εκπέμπεται με τη μορφή λεπτής και ισχυρής δέσμης στο δορυφόρο. Η δέσμη αυτή ονομάζεται uplink δέσμη. Ο δορυφόρος λαμβάνει το σήμα και αφού το επεξεργαστεί το κατευθύνει προς τη γη και προς τις περιοχές που έχει καθοριστεί από τον πάροχο. Οι διεργασίες που γίνονται πάνω στο σήμα είναι η ενίσχυση του (κατά 50-100 Watt) αφού ώσπου να φτάσει στο δορυφόρο έχει εξασθενίσει όπως και η μείωση της συχνότητας του για να διαφέρει το σήμα ανόδου (uplink) από το σήμα που φεύγει από το δορυφόρο – καθόδου (downlink). Η πορεία του σήματος φαίνεται στο σχήμα 20. Ο δορυφόρος για τέτοια διάταξη εννοείται ότι είναι γεωστατικός.



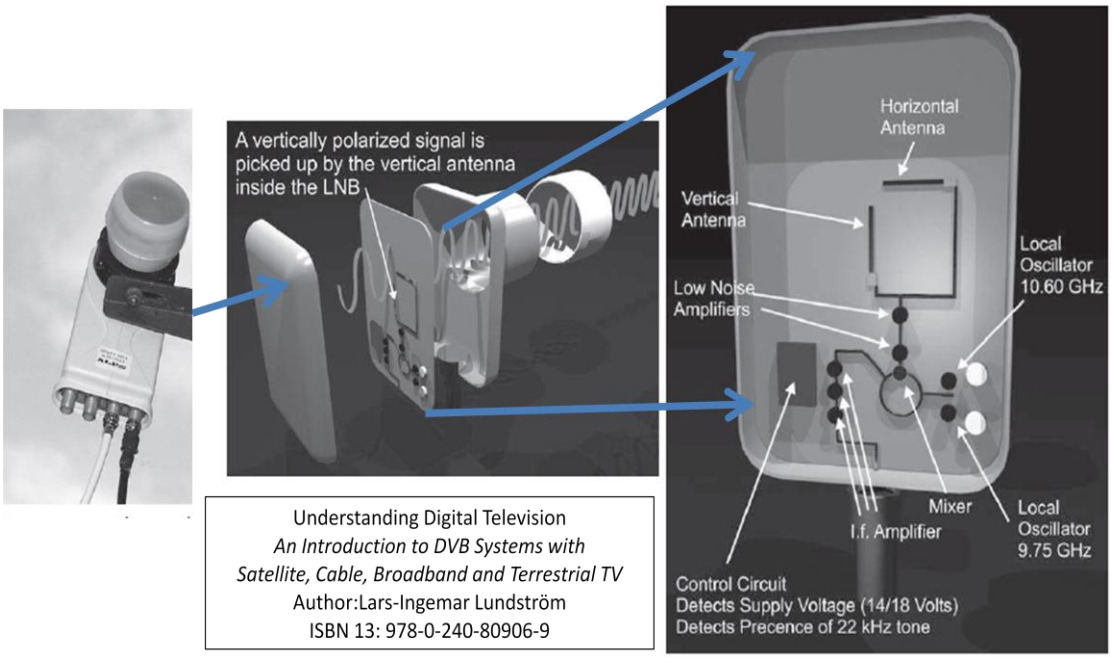
Σχήμα 20 : Η πορεία του σήματος από τον πομπό στο δέκτη μέσω του δορυφόρου.

3.4 ΛΗΨΗ

Το σήμα καθόδου συγκεντρώνεται και κατευθύνεται από το παραβολικό κάτοπτρο του χρήστη στο LNB (Low Noise Block) βλέπε σχήμα 20, και μέσω του LNB και καλωδίου τροφοδοτεί το δέκτη που κάνει ανάκτηση του σήματος.

3.4.1 LNB

Το LNB λαμβάνει το RF σήμα με δύο κεραίες (κάθετη και οριζόντια, σχήμα 21) έτσι ώστε να εντοπίσει τις δύο πολώσεις που αναφέραμε πριν. Μετά εφαρμόζει μέσω του LNA (Low Noise Ampification) ενίσχυση στο ταλαιπωρημένο και εξασθενημένο σήμα. Μετά λαμβάνει χώρα η κάτω μετατροπή από την RF συχνότητα στην IF με ένα ταλαντωτή που έχει συχνότητα ή 10.60GHz ή 9.75GHz. Η συχνότητα που θα χρησιμοποιηθεί εξαρτάται από το σήμα και ελέγχεται από το κύκλωμα ελέγχου του LNB (εκπέμπει σήμα 22Khz). Τέλος το σήμα μας ενισχύεται σαν συχνότητα IF πλέον και μέσω καλωδίου μικρής αντίστασης αποστέλλεται στο δορυφορικό δέκτη του συνδρομητή.

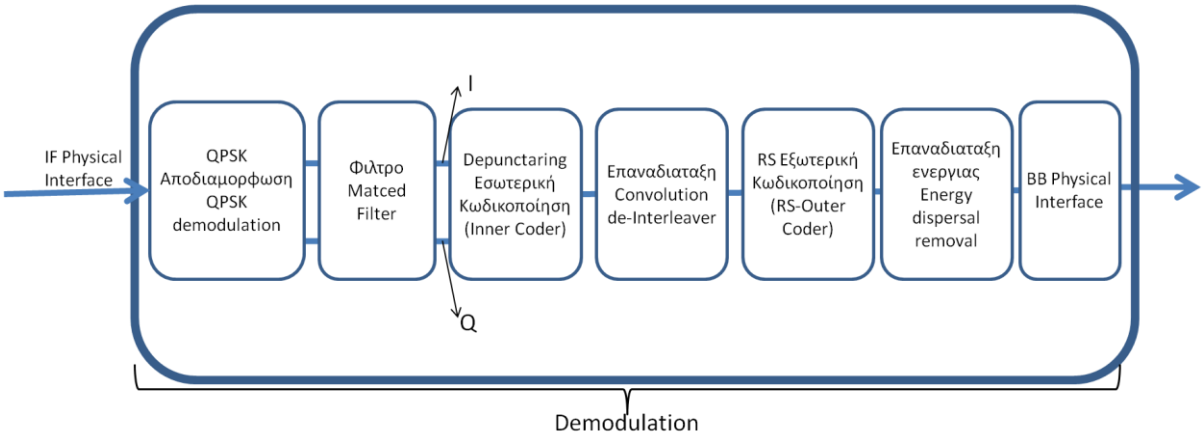


Σχήμα 21: το LNB και το εσωτερικό του

3.4.2 Δορυφορικός Δέκτης

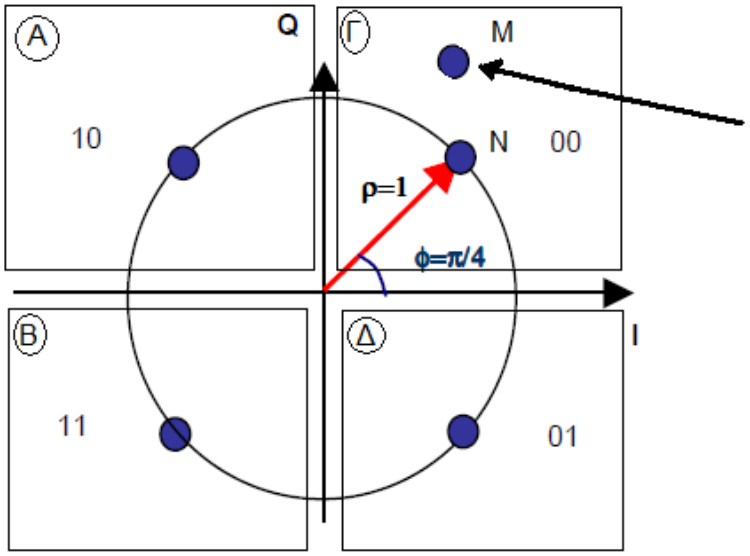
3.4.2.1 Αποδιαμόρφωσης

Εδώ γίνεται η αντίστροφη διαδικασία από τον πομπό. Αυτή φαίνεται σχηματικά στο σχήμα 22.



Σχήμα 22:Αντιστροφη διαδικασία ανάκτησης ροής πληροφορίας δέκτη

Το σήμα σε συχνότητα IF αναλύεται στις δύο αναλογικές συνιστώσες σε I και Q. Γίνεται η αντίθετη διαδικασία που γίνεται στον εκπομπό. Βάσει του συναστρικού διαγράμματος προβάλλεται το σήμα στο συναστρικό διάγραμμα και κάθε σημείο του σήματος που λαμβάνεται, μέσω χαλαρής απόφασης αποφασίζεται σε ποιά περιοχή από όλες (πχ 00, 01, 10, 11 για QPSK) ανήκει.



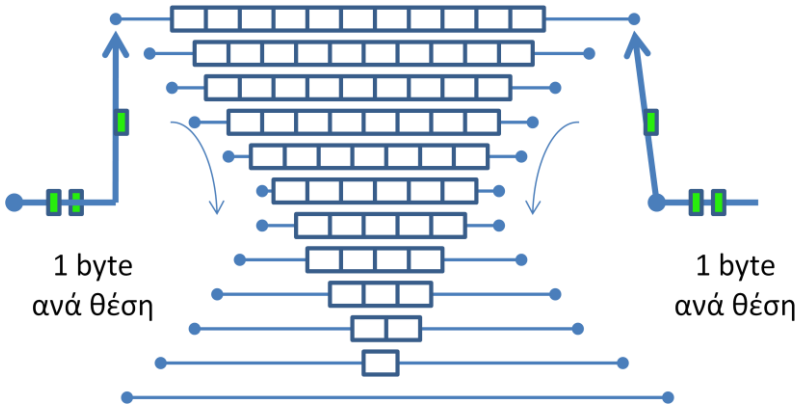
Σχήμα 23: Χαλαρή απόφαση επιλογής κατάστασης
(εκπομπή Μ λήψη Ν αρά επιλογή 00 κατάστασης)

Επειδή το σήμα έχει υποστεί αλλοίωση δεν εντοπίζεται ακριβώς στην συντεταγμένη I και Q θέση που επιλέχτηκε και εκπέμφθηκε. Έτσι μέσω της χαλαρής απόφασης συμφώνα με την οποία το αποτύπωμα που αφήνει το σήμα στο συναστρικό διάγραμμα λήψης αντιστοιχίζεται με το σημείο (πχ 00, 01, 10, 11 για QPSK) που είναι πιο κοντά στο διάγραμμα κατά ευκλείδεια απόσταση. Αυτό φαίνεται στο παράδειγμα του σχήματος 12 ο πομπός έκπεμψε το σημείο 00 με το σημείο Ν με συνιστώσες $\sqrt{V}\cos(\omega_0 t + 45°)$ οπου V η τάση. Ο δέκτης έλαβε $\sqrt{V'}\cos(\omega_0 t + 73°)$ δηλαδη με μεγαλυτερη φαση και μεγαλυτερη ταση και φαίνεται στο σχήμα σαν Μ. Ο αποδιαμορφωτής έχει χωρίσει το διάγραμμα

ισόμερος σε 4 περιοχές (Α, Β, Γ, Δ για τα 10, 11, 00, 01 αντίστοιχα) και παρατηρεί ότι το Μ είναι στην περιοχή Γ και το αναγνωρίζει σαν 01. Αν ο θόρυβος και η εξασθένιση είναι μεγάλη μπορεί ο αδιαμόρφωτης να εκτιμήσει λάθος την κατάσταση σύμβολου με μια γειτονική. Δηλαδή το Μ να βρεθεί σε περιοχή έκτος τη Γ π.χ. την Α (αν έχει φάση πάνω από 90^{o}) και να εκτιμηθεί σαν 10. Για να μειωθεί η επίδραση αυτού του λάθους τα συναστρικά διαγράμματα σχεδιάζονται κατά κώδικα Grey. Συμφώνα με το κώδικα Grey οι γειτονικές περιοχές του σχεδιαγράμματος διαφέρουν μόλις κατά ένα bit έτσι ώστε αν γίνει λάθος εκτίμηση αυτή να είναι της τάξης του ενός bit μόλις. Έτσι τα αναλογικά σήματα μετατρέπονται σε ψηφιακά.

Μετά τον αποδιαμορφωτή QPSK έχουμε το φίλτρο Nyquist που είναι η δεύτερη τετραγωνική ρίζα ,του ανυψωμένου συνημίτονου φίλτρου, που αναλύθηκε εκτενώς πριν.

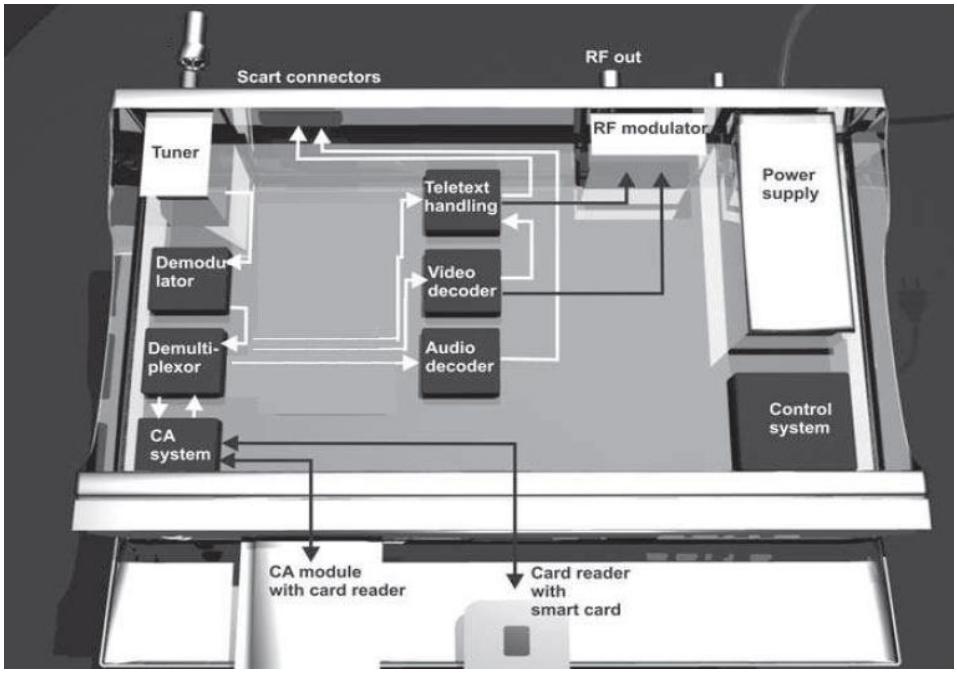
Ακολουθεί ο αποκωδικοποιητής Viterdi που είναι ο αποκωδικοποιητής του συνελικτικού κώδικα. Έπειτα η αναδιάταξη που φαίνεται στο σχήμα 24 και είναι ακριβώς αντίθετη της αναδιάταξης στον πομπό (σχήμα 11).



Σχήμα 24: Αντίστροφος Αναδιατάκτης

Έπειτα το σήμα αποκωδικοποιείται κατά Reed Solomon κωδικοποίηση και επανέρχεται στην αρχική του κατανομή αφού αφαιρεθεί το τυχαίο ανακάτωμα της διασποράς ενεργείας. Το σήμα έχει μετατραπεί στην αρχική πλέον ροή των 188bytes της Transport Stream και είναι έτοιμο για επεξεργασία αποκρυπτογράφησης ή απευθείας προβολή στο τερματικό (τηλεόραση) του χρήστη αν δε φέρει κρυπτογράφηση.

Η όλη διαδικασία που περιγράφηκε ήταν η αποδιαμόρφωση. Έπειτα ακολουθεί ο αποπολυπλέκτης κατά MPEG. Για να υπάρχει μια πρακτική απεικόνιση των σταδίων στο δορυφορικό δέκτη δίνεται ένα ενδεικτικό σχήμα ενός δορυφορικού δέκτη κατά DVB-S:



Σχήμα 25 : Εσωτερικό δορυφορικού δέκτη με τα στάδια λήψης

Το σήμα φτάνει από το LNB στο tuner το οποίο στην ουσία ασκεί το ρόλο του φίλτρου αφού αφήνει να περάσει μόνο η συχνότητα (ή ομάδα καναλιών, αφού ανά συχνότητα συνυπάρχουν 8-10 κανάλια κατά DVB-S) που επιλεγεί ο χρήστης με το τηλεχειριστήριο του. Το φιλτραρισμένο σήμα προωθεί στο Demodulator (αποδιαμορφωτή) που περιγράφηκε πριν και από εκεί μεταφέρεται στο Demultiplexor (αποπολυπλέκτη) που θα μελετηθεί τώρα. Αν το κανάλι έχει κρυπτογράφηση λαμβάνει τις πληροφορίες για αποκρυπτογράφηση από το CASS (Conditional Access Sub-system) , αν δεν έχει προχωρεί κατευθείαν στο διαχωρισμό σε ήχο-εικόνα και εξαγωγή μέσω Scart, ή άλλων εξόδων(HDMI) στην τηλεόραση (σχήμα25).

Θυμίζουμε επιγραμματικά πως επιλέγεται από τη ροή το κάθε κανάλι.

1. Ο χρήστης διαλέγει κανάλι με το τηλεχειριστήριο
2. Ο Δέκτης:

(α) φιλτράρει τα πακέτα με PID Ο και λαμβάνει τις ενότητες PAT

(β) κατασκευάζει τον πίνακα PAT από τα δεδομένα των ενοτήτων

(γ) φιλτράρει το PID που αντιστοιχεί στο PMT (ανάλογα με το PAT πίνακα) αυτού του προγράμματος

(δ) κατασκευάζει τον PMT πίνακα από τις σχετικές ενότητες

(ε) Βρίσκει τις ενότητες συγχρονισμού εικόνας, ήχου, κρυπτογράφησης και τις προωθεί στους αποκωδικοποιητές ήχου και εικόνας οι οποίοι αποστέλλουν το οπτικοακουστικό πλέον σήμα στην τηλεόραση.

Η παρουσία όμως κρυπτογραφημένου καναλιού προϋποθέτει μια επιπλέον διαδικασία στο στάδιο εκπομπής τη διαδικασία κρυπτογράφησης που προσπεράστηκε σε αυτό το κεφάλαιο δια το λόγο ότι αναλύεται ενδελεχώς στο επόμενο κεφάλαιο.

3.5 Βιβλιογραφία

A Comparison between satellite DVB conditional access and secure IP multicast:
H. Cruickshank, M.P. Howarth, S.Iyengar, Z. Sun

H.264 and MPEG-4 VideoCompression Video Coding for Next-generation Multimedia:
Iain E. G. Richardson

UnderstandingMPEG-4: Klaus Diepold, Sebastian Moeritz

Technologies and Services on Digital Broadcasting Overview of MPEG-2 Systems
Broadcast Technology no.11, Summer 2002

COMMUNICATION SYSTEMS ENGINEERING: John G. Proakis, Masoud Salehi

Digital Television Satellite, Cable, Terrestrial, IPTV, Mobile TV in the DVB Framework
Third Edition: Hervι Benoit

Understanding Digital Television An Introduction to DVB Systems with
Satellite, Cable, Broadband and Terrestrial TV: Lars-Ingemar Lundstrm

DIGITAL SATELLITE COMMUNICATIONSGiovanni E. Corazza

Satellite Communications: Dennis Roddy
Digital Video and Audio Broadcasting Technology A Practical Engineering Guide
Second Edition: Walter Fischer

DVB Fact Sheet – April 2008 by DVB Project Office
DVB Fact Sheet – June 2008by DVB Project Office
EN 300 421 V1.1.2 (1997-08)
European Standard (Telecommunications series)
ETSI EN 302 307 V1.1.2 (2006-06)
European Standard (Telecommunications series)
ETSI TR 102 376 V1.1.1 (2005-02)
Technical Report
ETSI TS 102 441 V1.1.1 (2005-10)
Technical Specification
TR 101 198 V1.1.1 (1997-09)
Technical Report

Επίγεια και Δορυφορική Τηλεόραση Ευρείας Εκπομπής
ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ: Δημήτριος Κ.Γαλάνης

Simulation Βελτίωσης Ραδιοκάλυψης DVB-T με βοήθεια Smart Antennas
ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ: Λαμπίρης Δ.Χαράλαμπος

Τα πρότυπα DVB-S2 / RCS για κινητές δορυφορικές επικοινωνίες. Εφαρμογή σε γρήγορα τρένα και πλοία. ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ: Μαρία – Άννα Γ. Γαϊτάνη,Φραγκίσκος Σ.Δεμένεγας

Το Νέο Δορυφορικό Πρότυπο ΕκπομπήςDVB-S2: Θέματα Ενθυλάκωσης, Σηματοδοσίας και Συμβατότητας ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ :Ηλίας Γ. Τσαγκλής

Image and Video Encryption From Digital Rights Management to Secured Personal Communication: Andreas Uhl, Andreas Pommer

Δορυφορικές Επικοινωνίες: Χ.Καψάλης, Π.Κωττής
Κεραίες Ασύρματες Ζεύξεις: Χ.Καψάλης, Π.Κωττής
Διαμόρφωση και Μετάδοση Σημάτων: Π.Κωττής

Κεφάλαιο 4:Μηχανισμός κρυπτογράφησης-αποκρυπτογράφησης σήματος

Όπως είπαμε στο 2^{ο} κεφάλαιο, για να προστατεύσει η δορυφορική βιομηχανία την επένδυσή της , θέσπισε την κρυπτογράφηση. Αν και υπάρχουν πολλά συστήματα και αλγόριθμοι κρυπτογράφησης το DVB για τις μεταδόσεις του χρησιμοποιεί σαν βάση τον αλγόριθμο Common Scrambling Algorithm (CSA) που θα αναλυθεί πιο κάτω. Ο αλγόριθμος CSA κρυπτογραφεί κατά τη διάρκεια εκπομπής , την πολυπλεγμένη κατά MPEG ροή με μια κλείδα(ή κλειδί) το λεγόμενο Control Word (CW) που αποτελείται από 32 bytes. Το DVB πρωτόκολλο και ο CSA αλγόριθμος , προβλέπουν ένα σύστημα κρυπτογράφησης που αναλύεται πιο κάτω αλλά δεν προβλέπουν και δεν τυποποιούν τον τρόπο εξαγωγής του CW(control worlds) από τη ροή στο δεκτή. Δηλαδή παρέχει τον αλγόριθμο κρυπτογράφησης αλλά δε τυποποιεί τον τρόπο αποστολής και διασφάλισης της μυστικότητας του κλειδιού.

Ο τρόπος αποστολής και η ασφάλεια του CW εξαρτάται από το σύστημα CAS(Conditional Access System) που θα διαλέξει ο πάροχος από τα διαθέσιμα που υπάρχουν στην αγορά. Όπως συμβαίνει και με όλα τα προϊόντα και υπηρεσίες όσο πιο ακριβό είναι κάθε CAS συνήθως τόσο πιο ασφαλές είναι.

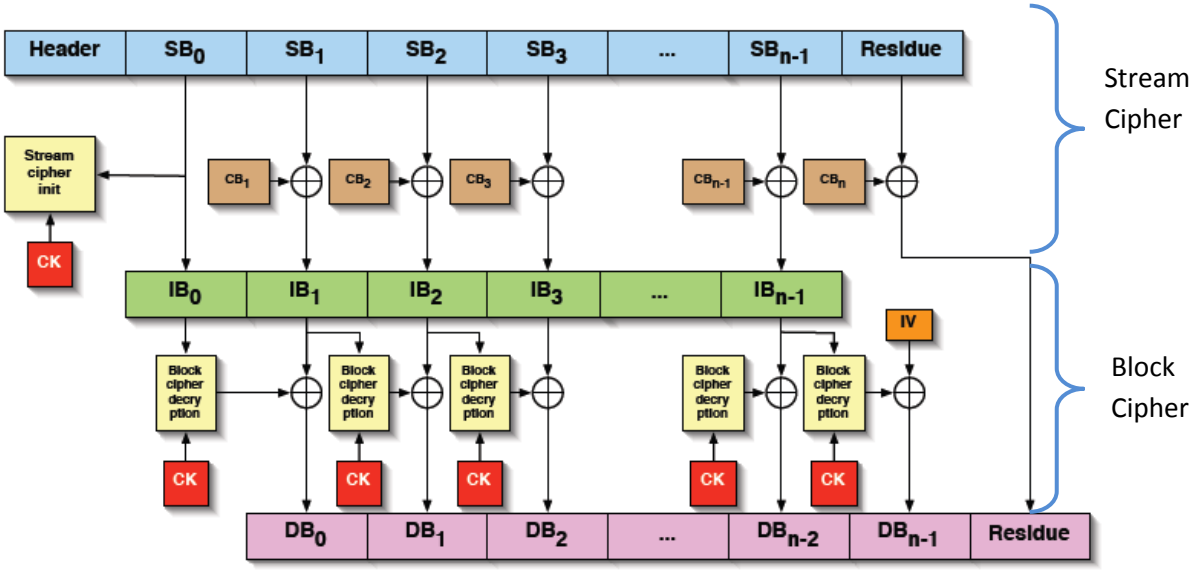
Γιατί όμως επιλέγει αυτός ο τρόπος μη τυποποίησης της κρυπτογράφησης του CW και η ύπαρξη πολλών CAS;

- Σίγουρα για να δραστηριοποιηθούν ανεξάρτητα εταιρίες έτσι ώστε να υπάρξει επένδυση και ερεύνα στον τομέα της κρυπτογράφησης ο.υ.
- Τυχούσας κατάρρευσης ενός CAS συστήματος από πειρατές να μην επηρεάζονται τα άλλα συστήματα CAS αφού είναι ανεξάρτητα.
- Οι πειρατές δεν επικεντρώνονται στο ‘’σπάσιμο’’ του CSA αλγορίθμου αλλά στο CAS του παρόχου που τους ενδιαφέρει.

Παρακάτω αναλύεται ο αλγόριθμος CSA.

4.1 CSA αλγόριθμος (Common Scrambling Algorithm)

Ο αλγόριθμος CSA παρουσιάστηκε αρχικά από το (ETSI) Electronical Telecommunication Standards Institute και υιοθετήθηκε από το DVB το Μάιο του 1994. Η επιτροπή κρατάει ακόμα και σήμερα τις λεπτομέρειες της υλοποίησης μυστικές, με συμφωνίες που υπογράφονται από το κάθε μέλος της οργάνωσης και απαγορεύει την υλοποίηση των αλγορίθμων σε επίπεδο λογισμικού. Σκοπός του είναι η κρυπτογράφηση της MPEG ροής πριν την εκπομπή της και η αποκρυπτογράφηση της κατά τη λήψη. Για αυτό το σκοπό χρησιμοποιεί συνδυασμό δύο cipher (κρυπτογραφημάτων στα ελληνικά) του block cipher (μπλοκ κρυπτογράφησης) και του stream cipher (κρυπτογράφημα ρεύματος). Ωστόσο αυτά τα δύο cipher μοιράζονται ένα κοινό κλειδί 64 bit (control word-CW) και το αποτέλεσμα του πρώτου δίνεται ως είσοδος στον cipher ρεύματος (σχήμα 1). Οπότε η εξαγωγή του κλειδιού από ένα από τα δύο chiper καταλύει και τον αλγόριθμο κρυπτογράφησης.



Σχήμα 1:Τα δύο chiper ,stream και block που αποτελούν το CSA

Μέχρι το 2002, ο αλγόριθμος ήταν διαθέσιμος μόνο στο πλαίσιο μιας συμφωνίας μη κοινολόγησης (Non-Disclosure Agreement-NDA) από το θεματοφύλακα ETSI. Αυτό που αρνήθηκε το NDS και εξακολουθεί να απαγορεύει στους δικαιοδόχους ,όπως είπαμε, είναι η υλοποίηση του αλγορίθμου σε λογισμικό για λόγους ασφαλείας. Οι λίγες πληροφορίες που υπήρχαν τότε στη διάθεση του κοινού περιέχεται σε Τεχνική έκθεση ETSI European Telecommunications Standards Institute.

ETSI Technical Report289: Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems, 1996.

και των αιτήσεων για διπλώματα ευρεσιτεχνίας:

Simon Bewick. Descrambling DVB data according to ETSI common scrambling specification. UK Patent Applications GB2322994A / GB2322995A,1998 .

Davies Donald Watts, Rix Simon Paul Ashley, and Kuehn Gideon Jacobus. System and apparatus for blockwise encryption and decryption of data. USPatent Application US5799089 , 1998.

Αν και το CSA αρχικά θα εφαρμοζόταν μόνο σε υλικό, πράγμα δύσκολο για να αντιστραφεί και να αποκαλυφθεί ο αλγόριθμος ,προς έκπληξη όλων το 2002 κυκλοφορεί το FreeDec, ένα πρόγραμμα των Windows για το CSA σε μορφή λογισμικού. Αν και κυκλοφόρησε μόνο ως δυαδική μορφή (assembly) ,η αποσυναρμολόγηση του αποκάλυψε τα ελλείποντα στοιχεία από τα προηγούμενα γραπτά και επέτρεψε την επαναδόμηση του αλγορίθμου σε υψηλότερο επίπεδο γλωσσών προγραμματισμού(πχ C++). Με το CSA τώρα δημοσίως γνωστά στο σύνολό του, οι κρυπταναλυτές άρχισαν να ψάχνουν για κρυπταναλυτικές αδυναμίες. Όπως και σε άλλους αλγόριθμους κρυπτογράφησης, ένα ασθενές προβλέψιμο τμήμα μπορεί να σπάσει ολόκληρο τον αλγόριθμο. Το ασθενές αυτό σημείο προκύπτει από το γεγονός ότι τμήματα του μηνύματος είναι γνωστά ή τουλάχιστον εύκολα προβλέψιμα, όπως οι MPEG κεφαλίδες. Το μήκος κλειδιού του είναι 64 bits, μήκος το όποιο επιτρέπει πολλές διαφορετικές δυνατότητες της κρυπτογράφησης. Μια επίθεση λαμβάνοντας 1 μs για κάθε προσπάθεια, μέσα από όλες τις πιθανές λέξεις-κλειδιά, θα θέλει περίπου 300. 000 χρόνια, κατά μέσο όρο για να ερευνήσει όλο το πεδίο ορισμού. Αυτό μπορεί να μειωθεί με τη χρήση του προβλέψιμου μέρους του κρυπτογραφημένου μήνυμα και να αποκλείσει δυνητικά κλειδιά. Έτσι ενώ ο CSA αλγόριθμος χρησιμοποιεί 64-bit κλειδιά, στην πραγματικότητα, μόνο 48 bits από τα βασικά είναι άγνωστα, αφού τα bytes 3

και 7 χρησιμοποιούνται ως checksum byte, και να μπορούν εύκολα να υπολογιστούν εκ νέου. Εργασία: Ralf-Phillip Weinmann and Kai Wirt. ‘’Analysis of the dvb common scrambling algorithm’’
Ενώ με την εργασία του Kai Wirt: ‘’Fault Attack on the DVB Common Scrambling Algorithm’’ η οποία εισάγει σφάλματα στο κρυπτογραφημένο ρεύμα και μελέτη του αποτελέσματος της αποκρυπτογράφησης, περιορίζονται περισσότερο οι πιθανοί συνδυασμοί.

Αν και με εξαντλητική αναζήτηση μπορεί να βρεθεί κλειδί, αυτό δε επηρεάζει ακόμα την ύπαρξη του αλγορίθμου αφού το κλειδί αλλάζει πολύ συχνά (2-10sec) και ο χρόνος υπολογισμού κάθε κλειδιού είναι ανέφικτος με τα τωρινά κρυπταναλυτικά ευρήματα. Όμως αν και δεν έχει δημοσιευτεί ικανή επίθεση που να καταλύει άμεσα τον αλγόριθμο, δε φαντάζει απίθανο να έχει βρεθεί κρυφά ή να βρεθεί στο σύντομο μέλλον.

4.2 CAS (Common Access System) - Σύστημα κοινής πρόσβασης

Αν ο αλγόριθμος CSA μας δίνει το σύστημα κρυπτογράφησης με το κλειδί CW το CAS μας δίνει τον τρόπο δημιουργίας ασφάλειας και εξαγωγής του CW από το δέκτη. Με λίγα λογία το CSA μας δίνει την κλειδαριά με το κλειδί και το CAS πόσο καλά κρυμμένο είναι το κλειδί.

Αποτελείται από το **κύριο σύστημα** του CAS που βρίσκεται στα γραφεία του παρόχου και το **υπό-σύστημα** του CASS (Conditional Access Sub System) που είναι στο δεκτή του συνδρομητή.

Το κύριο μέρος του CAS αποτελείται από τα:

- SMS(Subscriber Management System) -σύστημα διαχείρισης
- SAS (Subscriber Authorization System) σύστημα αδειοδότησης

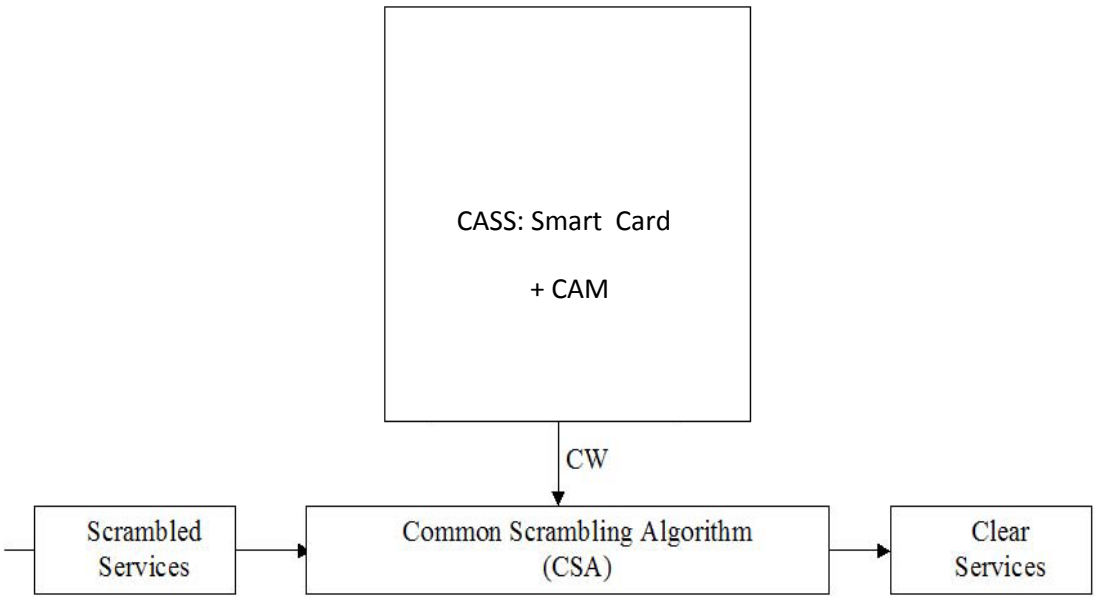
Το SMS έχει ως σκοπό την παραγωγή συνδρομητικών καρτών, αποστολή λογαριασμών, λήψη πληρωμών (ακόμα και με απευθείας σύνδεση με τράπεζες και τραπεζικούς λογαριασμούς) από τους συνδρομητές και διακοπή παροχών σε απλήρωτους λογαριασμούς. Είναι σε σύνδεση με το SAS το οποίο ενημερώνει ποιοί πελάτες έχουν ταχτοποιήσει τις οφειλές τους και έχουν δικαίωμα θέασης.
Το SAS λαμβάνει τις αδειοδοτήσεις από το SMS και τις μετατρέπει σε μηνύματα που ενθυλακώνει στη ροή MPEG πριν την εκπομπή της. Στην ουσία λειτούργει σαν εκτελεστής των εντολών του SMS αφού παράγει και αποστέλλει τα δύο κύρια μηνύματα κρυπτογράφησης EMM και ECM που θα αναλυθούν πιο κάτω.

Το υποσύστημα CASS (Conditional Access Sub System) αποτελείται από το CAM + συνδρομητική κάρτα και ευρίσκονται στην πλευρά του πελάτη -συνδρομητή. Η κάρτα είναι η γνωστή συνδρομητική κάρτα που μας δίνει ο πάροχος με τη συνδρομή(αναλυτικά στο κεφάλαιο 6). Το CAM είναι υλικό τοποθετημένο στον STB που παρέχει ο κάθε πάροχος και είναι εξειδικευμένο και προσαρμοσμένο στο κρυπτογραφικό σύστημα κάθε παρόχου. Αν και το CAM αποτελεί hardware (υλικό) οι πειρατές σχεδόν όλα τα CAS κατάφεραν να το εξομοιώσουν σε λογισμικά και να το εισάγουν σε OSTB. Επιπλέον το CAM σαν υλικό μπορεί να αγοραστεί σε PCMCIA μορφή σκέτο και νόμιμο και να εισαχθεί σε CI (common interface) θύρα STB που δε περιλαμβάνει ενσωματωμένο CAM (εξηγήθηκε στο $1^{ο}$ κεφάλαιο).

Σκοπός του είναι η εξαγωγή του CW από τη ροή με τη βοήθεια των EMM και ECM αφού έχει εξασφαλίσει μέσω της συνδρομητικής κάρτας ότι ο συγκεκριμένος δέκτης έχει δικαίωμα θέασης.

Κάθε πάροχος επιλεγεί το δικό του CAS (σύστημα πρόσβασης) πληρώνοντας τα ανάλογα δικαιώματα στην εταιρία που ανήκει .Τα επικρατέστερα CAS της Ευρώπης είναι:

- BISS
- Conax
- Cryptoworks
- Philips
- Digicipher
- Irdeto
- KeyFly
- Nagravision
- Kudelski
- NDS Videoguard NDS
- PowerVu
- RAS
- SECA Mediaguard Canal+
- Viaccess Viaccess CA



Σχήμα 2: Το CASS εξάγει το CW από τη ροή MPEG και μέσω αυτού ο CSA ξεκλειδώνει το σήμα.

4.3 Διαδικασία της κρυπτογράφησης-αποκρυπτογράφησης

4.3.1 Εισαγωγή

Η όλη διαδικασία κρυπτογράφησης-αποκρυπτογράφησης στηρίζεται σε κλειδιά , όπως και για να ανοίξεις μια πόρτα θέλεις ένα απλό κλειδί έτσι και εδώ θες ένα ραβασάκι που άμα το ξέρεις μπορείς να αποκρυπτογραφήσεις ή αλλιώς να ξεκλειδώσεις τις υπηρεσίες του παρόχου. Τα κλειδιά είναι ψηφιακά πακέτα μεγέθους 8 εως 32 bytes συνήως.

Αυτό το κλειδί στην ουσία είναι όπως αναφέραμε το:

- **CW** Control Word (κλείδα ελέγχου) ένας 8-byte συνήθως αριθμός ο οποίος εξάγεται από τον αλγόριθμο CSA χρησιμοποιώντας δύο ψηφιακά πακέτα γνωστά ως ‘’μηνύματα’’, αφού περάσει από πολλούς υπολογισμούς και ελέγχους.

Τα δύο ‘’μηνύματα’’ που δημιουργούνται ,ενθυλακώνονται (πολυπλέκονται) στη ψηφιακή ροή του DVB κατά τη διαδικασία MPEG και αποστέλλονται από τον πάροχο για να βοηθήσουν την πιστοποίηση του δέκτη σαν νόμιμος δέκτης και για να εξάγουν το CW από τη ροή είναι:

- **ECM** μηνύματα ελέγχου (entitlement control messages) τα οποία πρωτοείδαμε στους πίνακες PMT.

- **EMM** μηνύματα διαχείρισης (entitlement management messages) που είδαμε στους πίνακες CAT του προηγούμενου κεφαλαίου.

Τα μηνύματα αυτά διαθέτουν «ψηφιακές υπογραφές» που τα πιστοποιούν και δεν επιτρέπουν «ύποπτες αλλαγές».

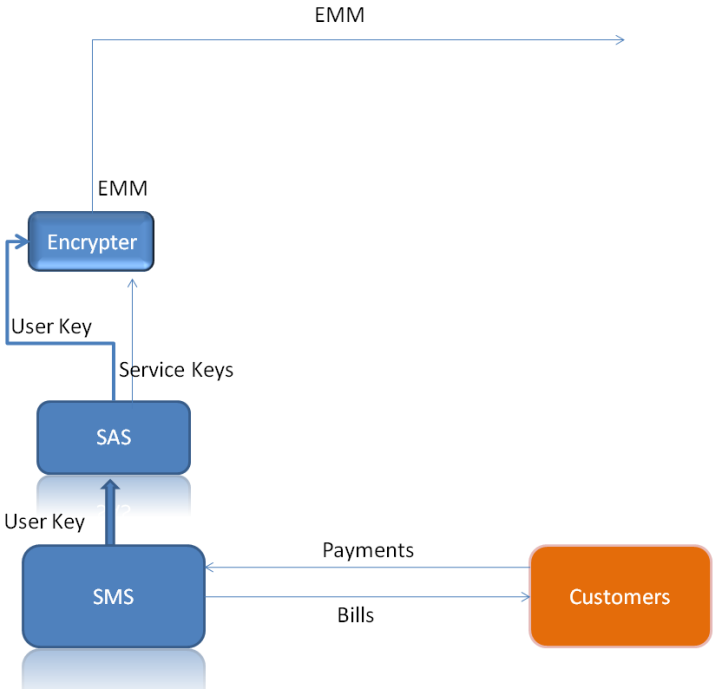
Το ECM εμπεριέχει το περίφημο CW (control word) για να εξαχθεί όμως το CW από το ECM χρειάζεται τη βοήθεια ,όπως θα δούμε πιο κάτω , του EMM και της συνδρομητικής κάρτας (στην ουσία του **user key -UK** που εμπεριέχει η κάρτα). Τα ECM εκπέμπονται και αλλάζουν κάθε 1-10 sec για μέγιστη ασφάλεια οπότε και το CW ισχύει για μόλις 1-10 sec.

Το EMM δίνει τα απαραίτητα στοιχειά για να εξαχθεί το CW από το ECM (αυτό είναι το **Service key – SK**) είναι υπεύθυνο για την διακοπή της συνδρομής αν είναι απλήρωτη, όπως και είναι υπεύθυνο για τα ποιά κανάλια (αριθμό) από όλα θα δει ο συνδρομητής (ανάλογα ποσά έχει πληρώσει).Τα EMM Εκπέμπονται κάθε 10 sec αλλά συνήθως το service key αλλάζει κάθε μήνα και είναι το ίδιο για όλους(εκπέμπονται τόσο συχνά για να γίνουν αντιληπτά από όλους τους συνδρομητές)

Αυτά για εισαγωγή θα δούμε τώρα αναλυτικά τις δύο διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης

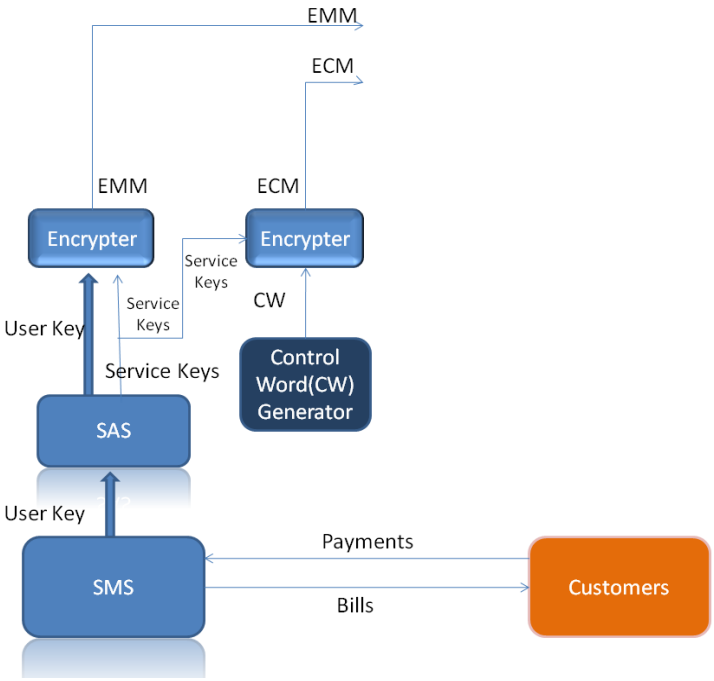
4.3.2 Διαδικασία κρυπτογράφησης

Η κρυπτογράφηση πραγματοποιείται στις εγκαταστάσεις του παρόχου εκεί όπως είπαμε υπάρχει το SMS το όποιο διαχειρίζεται της πληρωμές των συνδρομητών. Έχει μια βάση με τους συνδρομητές που έχουν πληρώσει τη μηνιαία συνδρομή και δικαιούνται πρόσβαση στην υπηρεσία. Έτσι αποστέλλει στο SAS τα user key των χρηστών που πρέπει να έχουν πρόσβαση. Το user Key είναι ένας μονοσήμαντος αριθμός που προσδιορίζει κάθε χρήστη και εμπεριέχεται στη συνδρομητική του κάρτα. Το SAS λαμβάνει αυτό τα user Keys και κρυπτογραφεί μέσω αυτών ένα άλλο κλειδί το Service Key ,δίνοντας το EMM, οπότε για να εξαχθεί το **Service Key** χρειάζεται κάποιος να έχει ένα από τα user Key που έστειλε το SMS. Το service key είναι κοινό για όλους τους χρήστες και αλλάζει συνήθως κάθε μήνα. Η κρυπτογράφηση του Service Key με το user key μας δίνει το EMM μήνυμα(σχήμα 3).



Σχήμα 3: Δημιουργία EMM από τα User Keys των συνδρομητών που πλήρωσαν

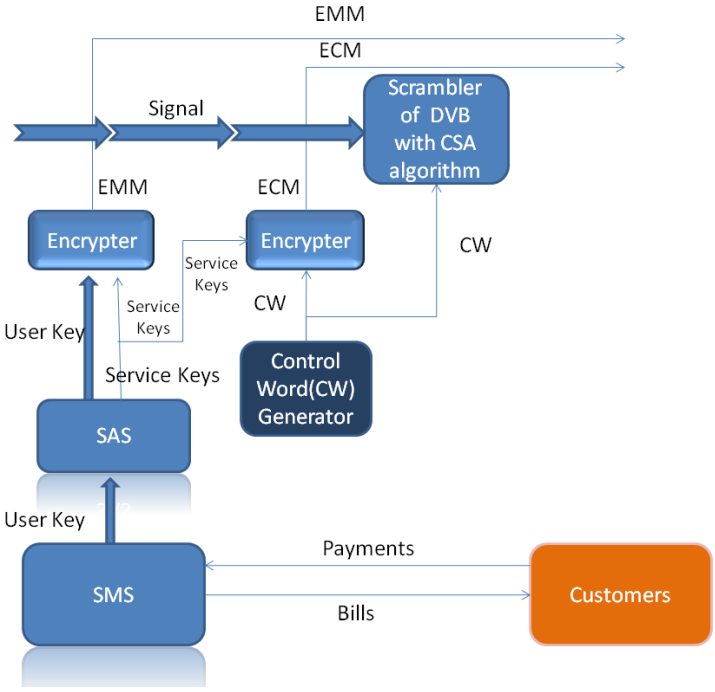
Εκτός όμως του EMM το SAS δημιουργεί και το ECM. Μια τυχαία γεννήτρια control words (CW) , των κλειδιών δηλαδή που ξεκλειδώνουν την υπηρεσία μέσω του CSA αλγορίθμου , παράγει CW κλειδιά τα οποία το SAS τα κρυπτογραφεί με το Service Key τώρα (το όποιο θυμίζουμε έχει κρυπτογραφηθεί με το user key της κάρτας). Η κρυπτογράφηση αυτή αποτελεί το ECM μήνυμα.



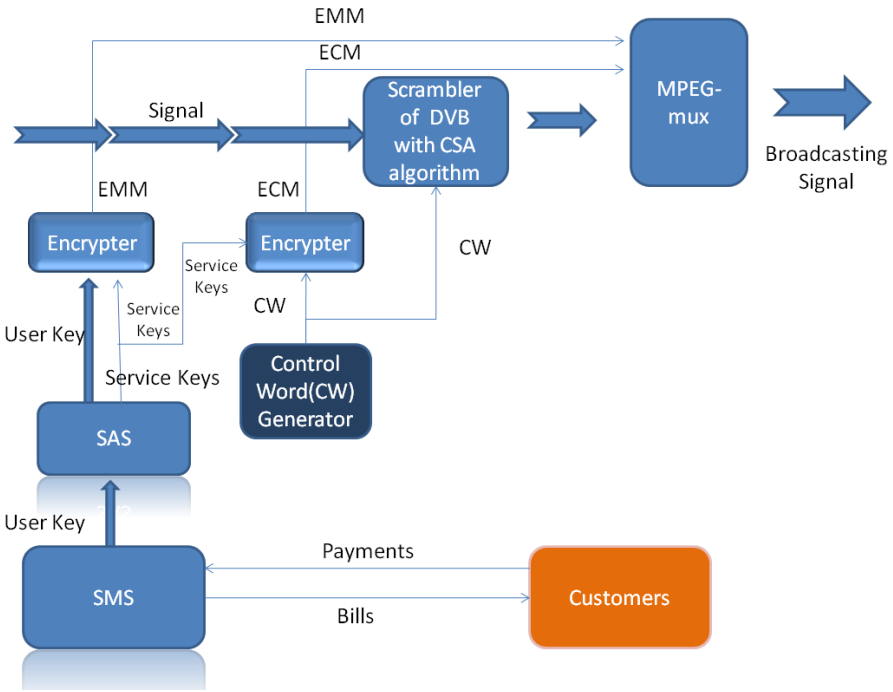
Σχήμα 4: Δημιουργία ECM κρυπτογραφημένα με το service ley

Ταυτόχρονα ένα αντίγραφο του κλειδιού CW κρυπτογραφεί το οπτικοακουστικό σήμα (σχήμα 5α) του παρόχου με τον αλγόριθμο CSA (σχήμα 3). Έπειτα ενθυλακώνεται και πολυπλέκεται μαζί με τα μηνύματα EMM και ECM. Βλέπουμε και από το σχήμα 3 ότι το ‘’κλειδωμένο’’ με το κλειδί CW **σήμα** αποστέλλεται **ταυτόχρονα** στη ροή μαζί με το **κλειδί**(ECM) με το οποίο είναι κλειδωμένο.

Το σήμα μετά την κρυπτογράφηση κατά CSA υποβάλλεται σε FEC, διαμορφώνεται δηλαδή (δες κεφάλαιο 3) και αποστέλλεται μέσω του δορυφορικού δίαυλου στους χρήστες (σχήμα5β).



Σχήμα 5α:Κρυπτογράφηση σήματος με το CW(control word)



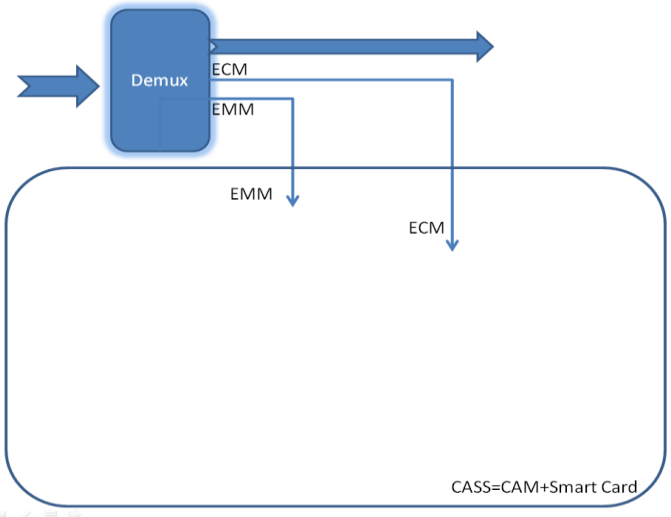
Σχήμα 5β: Πολυπλεξία του κρυπτογραφημένου σήματος μαζί με το EMM-ECM και αποστολή του στο δορυφορικό δίαυλο

4.3.3 Αποκρυπτογράφηση

Το σήμα αφού αποσταλεί από τον πομπό του παρόχου διανέμεται μέσω του δορυφόρου στους χρήστες. Το σήμα όπως αναφέραμε συγκεντρώνεται με το δορυφορικό πιάτο και λαμβάνεται με το LNB. Αφού γίνει υποβιβασμός συχνότητας στέλνεται στο δεκτή οπού γίνεται η δημιουργία της αρχικής ροής που χρειάζεται όμως αποκρυπτογράφηση για να μπορέσει ο νόμιμος χρήστης να την παρακολουθήσει.

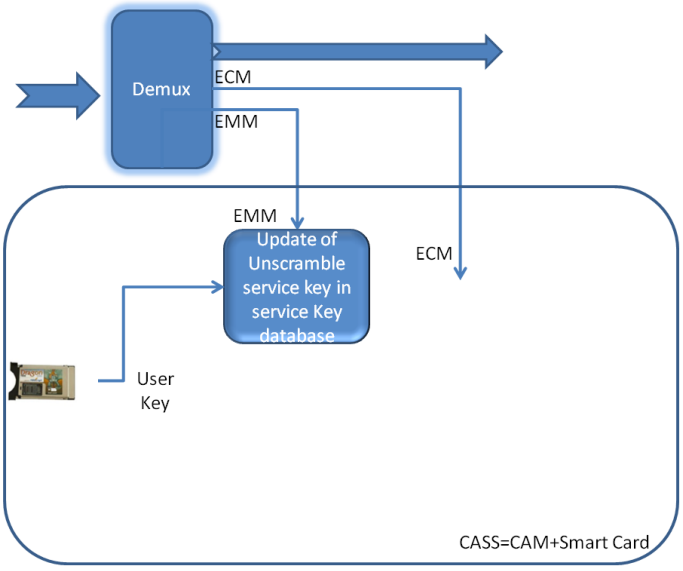
Η αποκρυπτογράφηση γίνεται ως εξής:

Τα EMM ECM εξάγονται από τη ροή DVB και οδηγούνται στο CAM. Το CAM (Common Access Module) όπως αναφέραμε είναι υλικό (hardware) οπού γίνονται όλες οι πράξεις και οι υπολογισμοί για την εξαγωγή του CW. Εμπεριέχεται σε αυτό η smart card και μαζί αποτελούν το CASS(Conditional Access Sub System) που είναι διαφορετικό κάθε εταιρίας που παρέχει υπηρεσίες κρυπτογράφησης. Αυτό φαίνεται στο σχήμα 6.



Σχήμα 6:Εξαγωγη EMM και ECM από τη ροή και αποστολή τους στο CASS

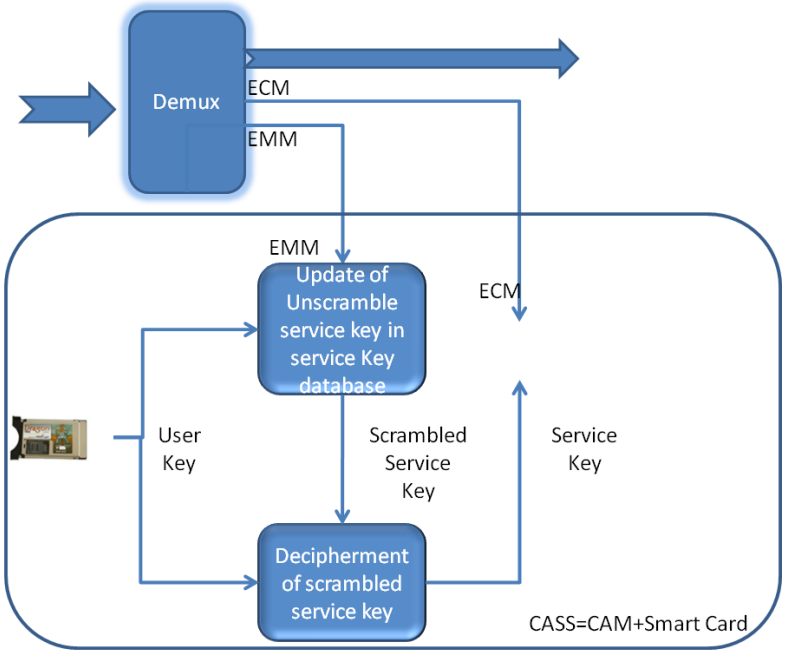
Το EMM όπως είπαμε περιέχει το service key(κρυπτογραφημένο πάντα με το user key της κάρτας). Το σύστημα αποστέλλει σε κάθε συνδρομητή διαφορετικό EMM που περιέχει το user key του (εφόσον έχει πληρώσει αν δεν έχει πληρώσει δεν αποστέλλετε EMM στο χρήστη αυτό και έτσι διακόπτεται η συνδρομή του).



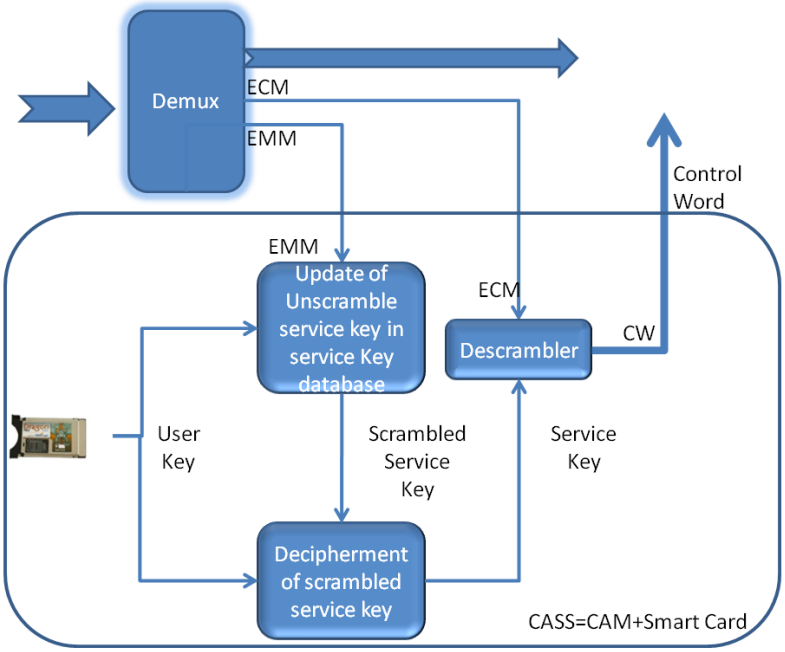
Σχήμα 7:Ανανεωση service key μετά από έλεγχο ότι η κάρτα είναι έγκυρη

Το CASS αφού πιστοποιήσει ότι η κάρτα έχει δικαίωμα λήψης του EMM (δηλαδή είναι ενεργή και έχει πληρωμένη συνδρομή)λαμβάνει το EMM και εξάγει το service key. Για να εξάξει και να αποκρυπτογραφήσει το service key το CASS εφαρμόζει πάνω του το user key(μάλλον με RSA ασύμμετρη κρυπτογράφηση γίνεται, κάτι που θα δούμε στο 6 κεφάλαιο) και λαμβάνει σαν έξοδο το service key (σχήμα 8) το οποίο αποθηκεύει (περίπου ένα μήνα). Θυμίζουμε ότι το EMM από καταβολής του στο SAS περιέχει το service key κρυπτογραφημένο με το user key(σχήμα 3).

Το service key έπειτα εφαρμόζεται στο ECM και αποκρυπτογραφεί το CW (σχήμα 9). Θυμίζουμε το CW είναι κρυπτογραφημένο με το service key (σχήμα 4).

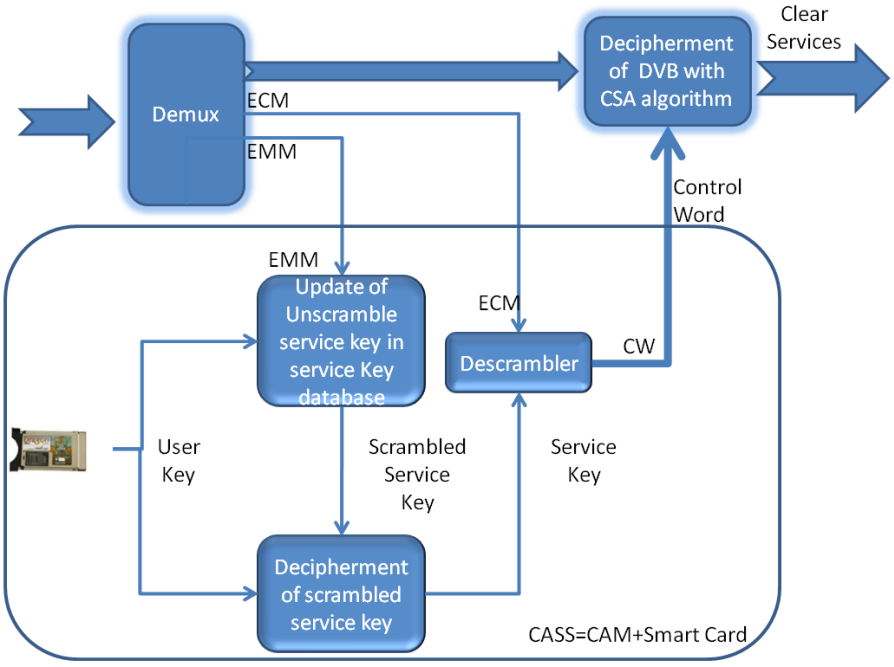


Σχήμα 8: Η ανάκτηση του service key με το user key της κάρτας



Σχήμα 9: Η εξαγωγή του control word από το ECM με το service key που ανακτήθηκε πιο πριν από το EMM

Μέσω τώρα του CSA αλγορίθμου του DVB γίνεται η τελική αποκρυπτογράφηση του οπτικοακουστικού υλικού το οποίο μπορεί να γίνει ορατό και αναγνωρίσιμο από το συνδρομητή. Σε κάθε πάροχο οι μετατροπές είναι οι ίδιες:
EMM->service-key->ECM->Control Word, η φιλοσοφία (οι πράξεις ή αλλιώς οι κρυπτογραφήσεις για να γίνει η μετατροπή μεταξύ EMM, ECM, service key) είναι διαφορετική.



Σχήμα 10: Η αποκρυπτογράφηση της ροής με το control word μέσω του αλγόριθμου CSA

Σύνοψη –Περίληψη του όλου συστήματος :

Στον πομπό

- Το service key (ίδιο για ένα μήνα για όλους) κρυπτογραφείται με το user Key(μοναδικό ανά χρήστη και μόνιμο) όσων χρηστών πλήρωσαν δημιουργώντας το EMM.

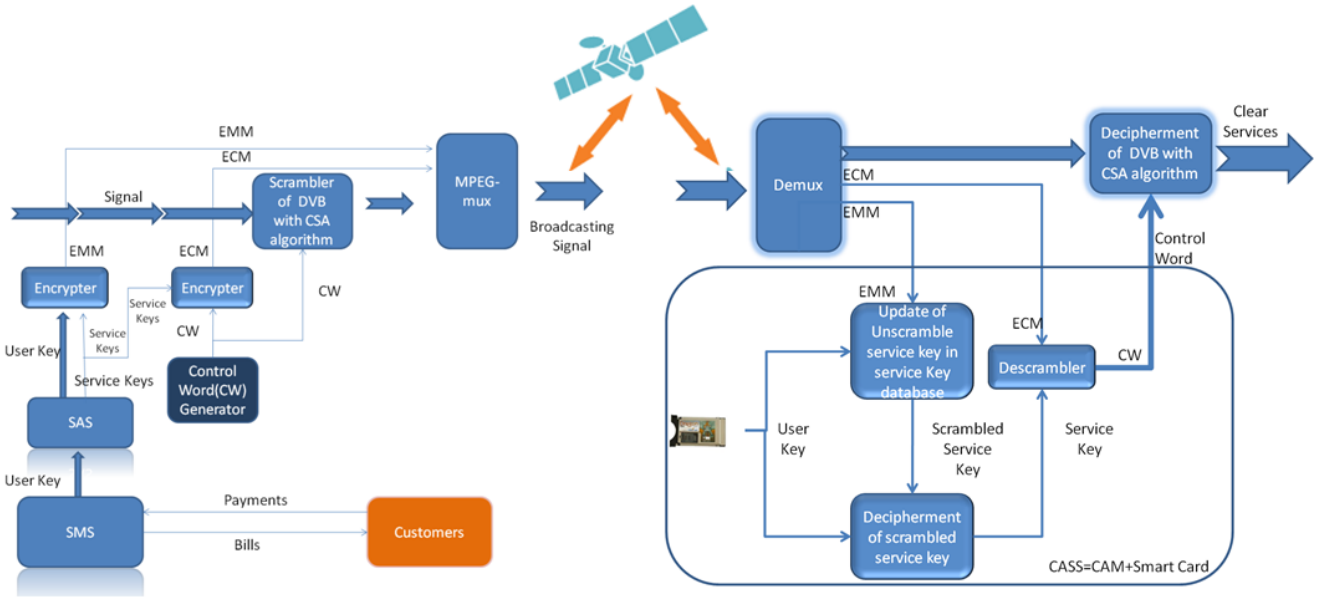
- Το Control word(αλλάζει κάθε 10 sec) που φέρει το γενικό πρόσταγμα αποκρυπτογράφησης, κρυπτογραφείται με το Service key(ίδιο για ένα μήνα για όλους) και δημιουργούν το ECM (άρα απαιτείται η παρουσία service key στο δεκτή για αποκρυπτογράφηση). Ταυτόχρονα το σήμα μας κρυπτογραφείται από αντίγραφο του Control Word.

Στο δέκτη

- Γίνεται έλεγχος αν στο EMM μήνυμα εμπεριέχεται το user key του δέκτη του οποίου ευρίσκεται (δηλαδή στην κάρτα που έχει ο δέκτης), αν ναι προχωρεί στην αποκρυπτογράφηση του Service key με αυτό το user key.

- Το ECM λαμβάνει το service key από το προηγούμενο μήνυμα (EMM) και αποκρυπτογραφεί το Control Word.

- Το Control Word στέλνεται στον αποκρυπτογράφο του CSA και αποκρυπτογραφείται το οπτικοακουστικό υλικό μας.



Σχήμα 11: Η όλη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης

Βιβλιογραφία

2005 Conditional Access in Mobile Systems: Securing the Application
Eimear Gallery, Allan Tomlinson,

Protection of DVB Systems by Trusted Computing: Nicolai Kuntze Andreas U. Schmidt

Functional model of aconditional access system EBU Project Group B/CA

Enhancing the Conditional Access Module Security in Light of Smart Card Sharing Attacks:
Konstantinos Markantonakis, Michael Tunstall, Keith Mayes

INTERNATIONAL STANDARD ISO/IEC13818-1

Fault Attack on the DVB Common Scrambling Algorithm: Kai Wirt

Analysis of the DVB Common Scrambling Algorithm: Ralf-Philipp Weinmann, Kai Wirt

Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications EN 50221

Conditional Access Concepts and Principles: David W. Kravitz and David M. Goldschlag

Technologies and Services on Digital Broadcasting Scrambling (Conditional Access System)
Broadcast Technology no.12, Autumn 2002

Security Architectures in Mobile Integrated Pay-TV Conditional Access System:
Hamidreza Shirazi

Digital Video Broadcasting (DVB),Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems,ETR 289

Soft Conditional Access for Digital Television: Dominika Olczak

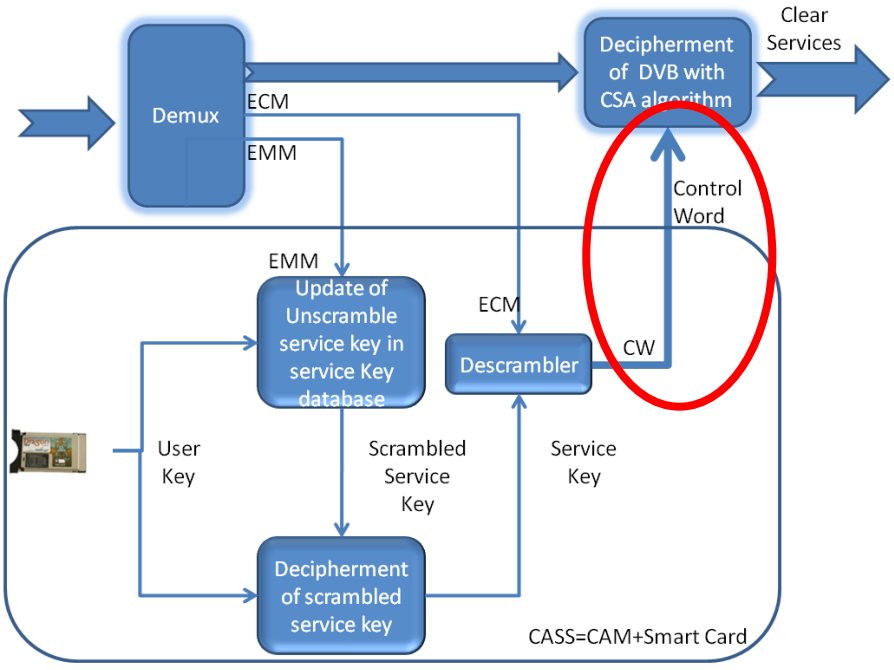
Inhibiting Card Sharing Attacks:
Michael Tunstall, Konstantinos Markantonakis, and Keith Mayes

Countermeasures for Attacks on Satellite TV Cards using Open Receivers:
Lishoy Francis, William G. Sirett, Keith Mayes, Konstantinos Markantonakis

Κεφάλαιο 5 : Πειρατεία με διαμοιρασμό κάρτας

5.1 Εισαγωγή στο Card Sharing (Διαμοιρασμό Κάρτας)

Οι πειρατές δεν άργησαν να βρουν την αχίλλειο φτέρνα του κρυπτογραφικού συστήματος DVB. Όπως και στην αρχαιότητα όλοι οι ισχυροί είχαν ένα αδύνατο σημείο ,στο σύστημα DVB αυτό είναι ο δίαυλος επικοινωνίας του CASS με τον CSA αλγόριθμο. Η επικοινωνία των δύο γίνεται χωρίς πιστοποίηση και χωρίς κρυπτογράφηση τις πλείστες φορές οπότε η εξαγωγή του CW από το δεκτή και η μεταφορά του σε άλλο η άλλους δέκτες δεν γίνεται αντιληπτή ούτε εμποδίζεται με κανένα μηχανισμό (σχήμα 1).Ενώ σε όποια συστήματα υπάρχει κρυπτογράφηση του διαύλου, αυτή παρακάμπτεται με τη χρήση λογισμικών – εξομοιωτών(emulators)που δύναται να εξάγουν το CW χωρίς κρυπτογράφηση. Έτσι ένας δεύτερος δέκτης μπορεί να τροφοδοτηθεί με control words χωρίς να εμπεριέχεται σε αυτόν οποιαδήποτε smart card και να αποκρυπτογραφεί το κρυπτογραφημένο σήμα που ούτως ή άλλως λαμβάνει. Το εκπληκτικό είναι ότι οι συνηθισμένες ‘’έξυπνες κάρτες’’ απαντούν-επιστρέφουν control words σε κάθε ECM χωρίς να ελέγχουν πόσα control words τροφοδοτούν και άρα να καταλάβουν ότι υπερλειτουργούν για ένα δέκτη και ότι τροφοδοτούν με κλείδες (CW) και άλλους δέκτες. (Οι τελευταίας τεχνολογίας κάρτες που θα δούμε πιο μετά δεν έχουν μηχανισμό που καταλαβαίνουν την υπολειτουργία και σταματούν την κάρτα).



Σχήμα 1: Ο επίμαχος ανασφαλής δίαυλος.

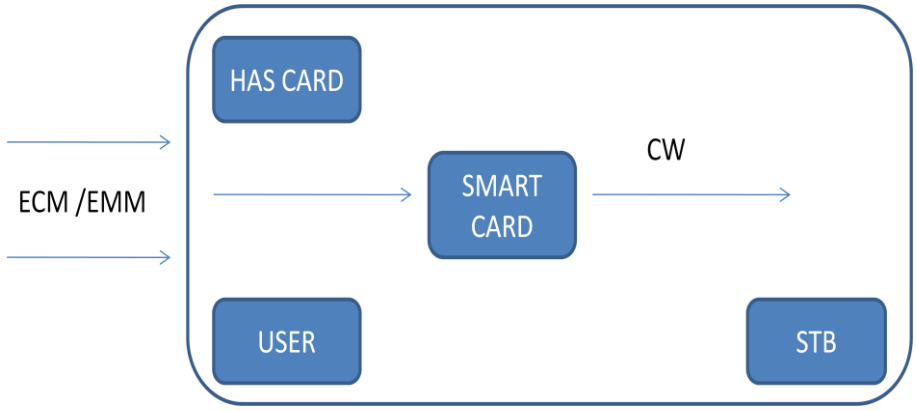
Ο πρώτος εμπνευστής της μεθόδου είναι ο κρυπταναλυτής McCormac ο όποιος κατά τη δεκαετία του 80’ στο σύστημα Videocrypt χρησιμοποιώντας βιντεοκασέτα κατέγραφε τη ροή των κλειδιών από την κάρτα στο δέκτη. Ταυτόχρονα όσοι δεν είχαν την κάρτα βιντεογραφούσαν το κρυπτογραφημένο κανάλι. Η κασέτα με τα κλειδιά μπορούσε άνετα να αντιγραφεί και να δημιουργηθούν αρκετά όμοια αντίγραφα ,έτσι όσοι είχαν βιντεογραφήσει το κανάλι αφού προμηθευόντουσαν τη δεύτερη κασέτα με τη ροή των

κλειδιών μπορούσαν σε μεταγενέστερο χρόνο να συνδυάσουν τις δύο κασέτες και να δουν το κανάλι αποκρυπτογραφημένο. Το αξιοσημείωτο με την ιστορία είναι ότι ο εμπνευστής θεώρησε ότι αν και καλή η μέθοδος δε θα μπορούσε να χρησιμοποιηθεί για ταυτόχρονη αποκρυπτογράφηση αλλά για μεταγενέστερη. Η έλευση του γρήγορου ίντερνετ όμως άλλαξε αυτή τη θεώρηση και επέτρεψε την εξαγωγή και διάδοση των κλειδιών με ταυτόχρονη αποκρυπτογράφηση τους σήματος από χρήστες χωρίς κάρτα.

Το νόμιμο μοντέλο

Το νόμιμο μοντέλο που ισχύει για κάθε συνδρομητή που έχει πληρωμένη συνδρομή και εξηγήθηκε στο προηγούμενο κεφάλαιο είναι το εξής:

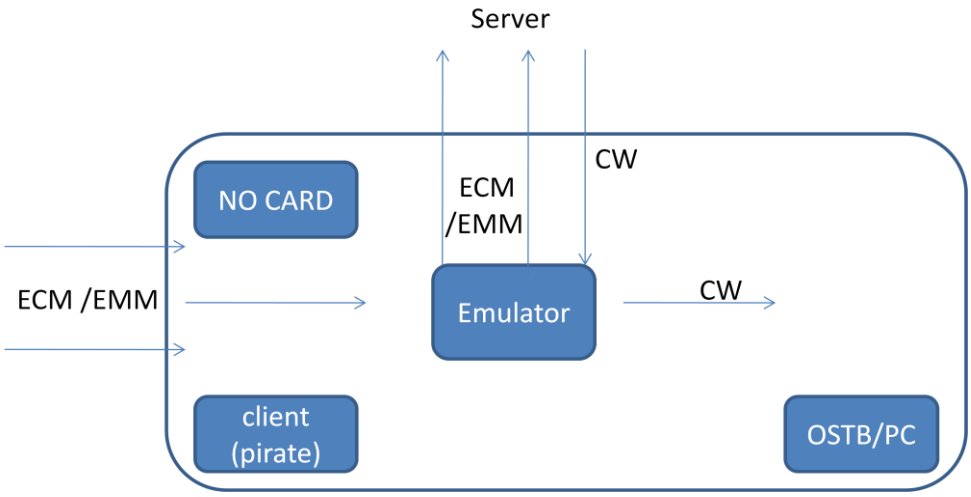
Ο νόμιμος χρήστης με δίκη του κάρτα όπως το σχήμα 2 λαμβάνει ECM/EMM με το πιάτο του τα προωθεί στην κάρτα του και παίρνει το CW που χρησιμοποιεί στο **δέκτη του.**



Σχήμα 2: Νόμιμος χρήστης (έχει κάρτα)

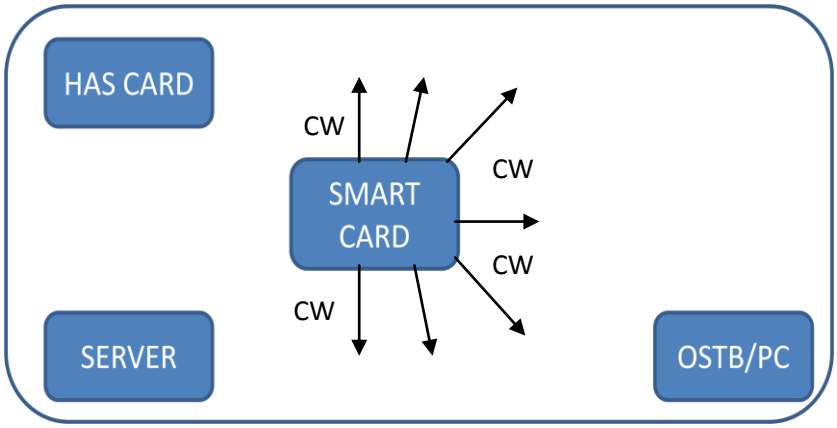
Πειρατεία μέσω Card Sharing (μοίρασμα control words)

Ο παράνομος χρήστης τώρα δεν έχει κάρτα στο δέκτη του όμως χρειάζεται CW(Control Words) για να αποκρυπτογραφήσει το σήμα του. Αυτά τα λαμβάνει μέσω δικτύου από άλλη κάρτα η οποία εμπεριέχεται σε server, σχήμα 3 (ο server αναλύεται στην επομένη παράγραφο).



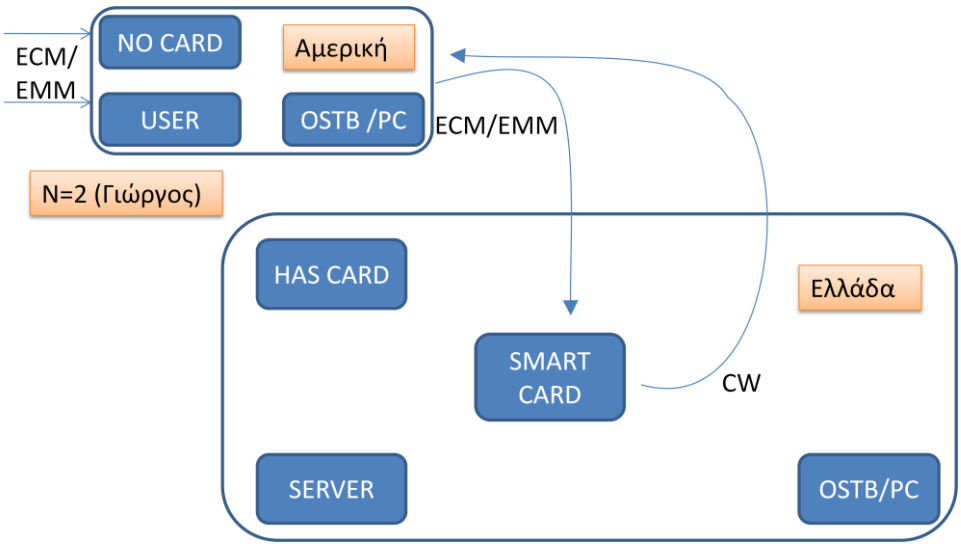
Σχήμα 3:Παράνομος χρήστης (δεν έχει κάρτα)

Ο server τώρα είναι ένας κεντρικός OSTB (open STB) δηλαδή ένας δορυφορικός ψηφιακός αποκωδικοποιητής που τρέχει ανοιχτό λογισμικό (Linux) ή ένας ηλεκτρονικός υπολογιστής που δέχεται δορυφορικό σήμα μέσω DVB – PIC card. Αυτός αποτελεί το ρόλο του **Server** και είναι υπεύθυνος να διαθέτει τα CW στους χρήστες που είναι ενωμένοι μαζί του και ονομάζονται **Clients**.



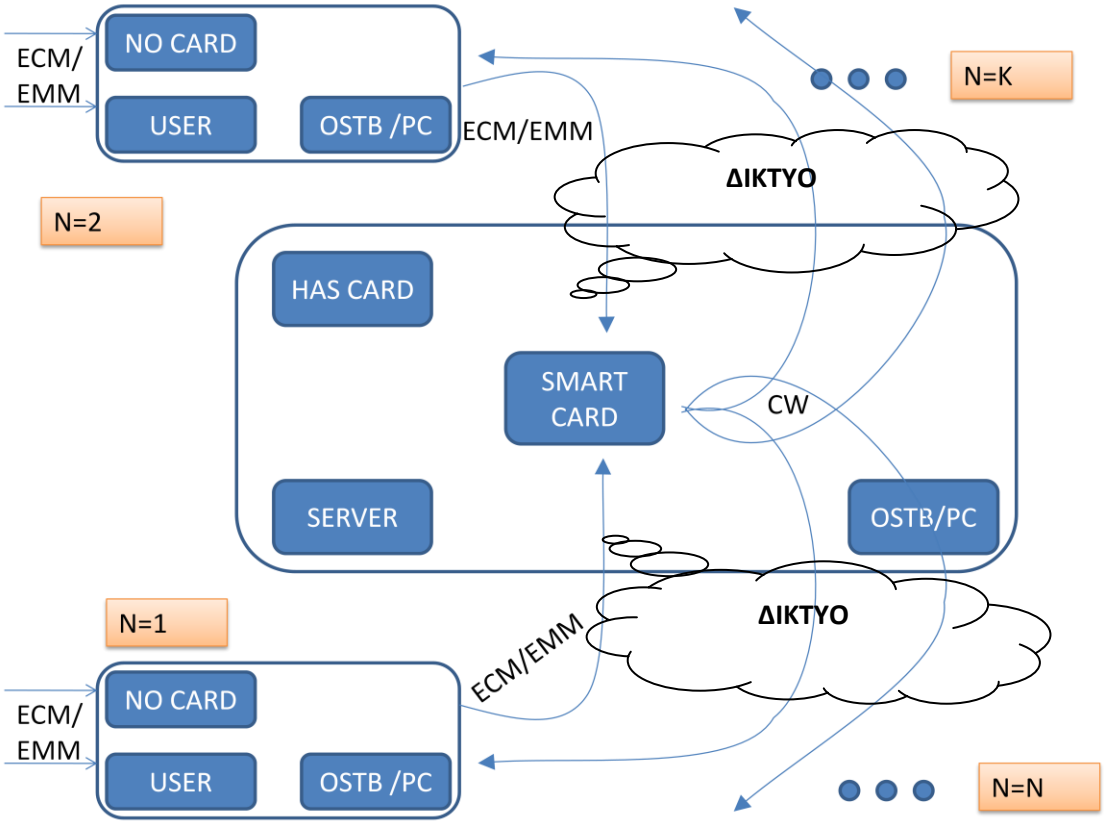
Σχήμα4:Ο server (διαμοιραστής) έχει κάρτα και διαμοιράζει τα κλειδιά στους παράνομους πελάτες

Ο Server δεν λαμβάνει συνήθως ECM/EMM από το πιάτο του (μπορεί να μην έχει καν πιάτο). Λαμβάνει μέσω δικτύου όποιο και αν είναι αυτό (internet,wifi,ενσύρματο κ.α.) τα ECM και EMM από χρήστες (clients) του δικτύου. Αυτοί δεν έχουν κάρτα και δεν έχουν το user key και το service key για να αποκρυπτογραφήσουν το σήμα οπότε αφού λάβουν τα ECM και EMM από το πιάτο τους τα διοχετεύουν στον Server για εξαγωγή του control word και αποστολή του πίσω σε αυτούς. Ο server αφού ρωτήσει την κάρτα, παίρνει τα CW, τα προωθεί σε όποιο τα ζήτησε και ξεκλειδώνει το σήμα του. Οπότε έχουμε το σχήμα όπου ο Γιώργος βρίσκεται Αμερική και ο server Ελλάδα. Ο Γιώργος λαμβάνει σήμα από το πιάτο του στην Αμερική εξάγει από το σήμα του τα EMM/ECM. Τα στέλνει στο server στην Ελλάδα μέσω ίντερνετ και ο server άπαντα στο ECM με το CW. (Το EMM χρειάζεται για να γίνονται update service keys στον server κάθε μηνά). Ο Γιώργος λαμβάνει τα control words και αποκρυπτογραφεί το σήμα του χωρίς να έχει ούτε συνδρομή με τον πάροχο ούτε κάρτα(σχήμα 5).



Σχήμα 5:Μεσω διαδικτύου είναι εφικτή η μεταφορά control word από την Ελλάδα στην Αμερική και η άρση των περιορισμών που θέτει ο πάροχος

Και επειδή όπως είπαμε η κάρτα μπορεί να άπαντα σε μεγάλο αριθμό αιτήσεων (ανάλογα με κάρτα μπορεί και N=30) μπορούν στο κόλπο να ενταχθούν και άλλοι χρήστες και να πάρουμε το διάγραμμα:



Σχήμα 6 : Μια και μόνο κάρτα και ένας OSTB (πχ Dreambox)μπορεί ανάλογα με την κάρτα να τροφοδοτήσει μέχρι και 30 χρήστες ,ενώ με άλλες τεχνικές πολλούς παραπάνω

Πριν προχωρήσουμε όμως στην ανάλυση του μοντέλου server-client θα δούμε τις διαφορετικές μορφές που μπορεί να πάρει το δίκτυο στο σχήμα 6.

5.2 Μορφές δικτύου Card Sharing

Αν και το internet σαν δίκτυο είναι αυτό που θα αναλύσουμε εκτενώς και είναι το πιο βρώμικο και επικερδές υπάρχουν και άλλες μορφές δικτύου. Μορφές που μας δίνουν και διαφορετικούς τρόπους card-sharing που πολλές φόρες χρειάζονται άλλες γνώσεις εξοπλισμό και φαντασία αφού τα όρια δεν έχουν τέλος όπως θα δούμε.
Σε όλες τις περιπτώσεις χρειάζεται ένας server και ένας ή περισσότεροι clients.

5.2.1 Περίπτωση 1 δίκτυο: ηλεκτρικές γραμμές σπιτιού

Ο διαμοιρασμός των απαντήσεων της κάρτας γίνεται συνήθως σε τοπικό δίκτυο (σπίτι πολυκατοικία).Το δίκτυο υλοποιείται ενσύρματα μέσω ηλεκτρικής γραμμής. Οι πληροφορίες (κλειδιά)μεταφέρονται με UTP καλώδιο από το server σε ειδικά PLC (power line converter) τα οποία συνδέονται στις ηλεκτρικές πρίζες του σπιτιού (σχήμα 7)και αποστέλλουν τα κλειδιά σε όλες τις πρίζες του σπιτιού. Άλλο PLC σε άλλη πρίζα εξάγει την πληροφορία από τη γραμμή του ρεύματος και με UTP καλώδιο μεταφέρει τα κλειδιά στο client .Ανάλογος μετατροπέας υπάρχει και για RF γραμμές όπου η πληροφορία μεταδίδεται μέσω των καλωδίων της κεραίας.

Σχήμα 7: Αποστολή control words μέσω ανταπτόρων και δικτύου ηλεκτρικού ρεύματος

5.2.2 Περίπτωση 2 δίκτυο: ομοαξονικό καλώδιο

5.2.2.1 μέσω rs-232 θύρας

Ο διαμοιρασμός των απαντήσεων της κάρτας γίνεται συνήθως σε τοπικό δίκτυο (σπίτι πολυκατοικία). Το δίκτυο υλοποιείται ενσύρματα μέσω ομοαξονική γραμμής χρησιμοποιείται η rs-232 θύρα του δέκτη (σειριακή θύρα για αναβάθμιση λογισμικού συνήθως) τόσο στο server όσο και στο client

5.2.2.2 μέσω card splitters

Το ρόλο server παίζει μικρή συσκευή-card splitter (όχι δέκτης άλλα απλός αναγνώστης κάρτας) με εξόδους για καλώδιο για ενσύρματη επικοινωνία. Οι clients έχουν κατάλληλους converter (μετατροπείς) που καταλήγουν στη UCAS θύρα - card reader του δέκτη (κεφαλαίο 1 αν δε θυμάστε τι είναι) και δίνουν τα κλειδιά στο δέκτη-client.

Πρόκειται για προϊόντα που πωλούνται νόμιμα, η χρήση τους όμως μπορεί να είναι νόμιμη ή παράνομη, ανάλογα με το αν περιορίζεται εντός της οικίας ή φεύγει και έξω από αυτήν.

5.2.3 Περίπτωση 3 δίκτυο: ασύρματα

5.2.3.1 μέσω rs-232 θύρας (ασύρματα)

Όπως πριν με διαφορά ότι το δίκτυο υλοποιείται ασύρματα μέσω ειδικών adaptor (προσαρμογέων) με κεραία που συνδέονται τόσο στο server όσο και στο client μέσω της rs-232 θύρας. Η κεραία μπορεί να ενωθεί με εξωτερική κεραία (ιδιοκατασκευή) και να εκπέμπει όσο μακριά επιθυμεί ο χρήστης (εννοείται παράνομα).

Σχήμα 8: Θύρα RS-232 και αντάπτορας για ασύρματη αποστολή control words

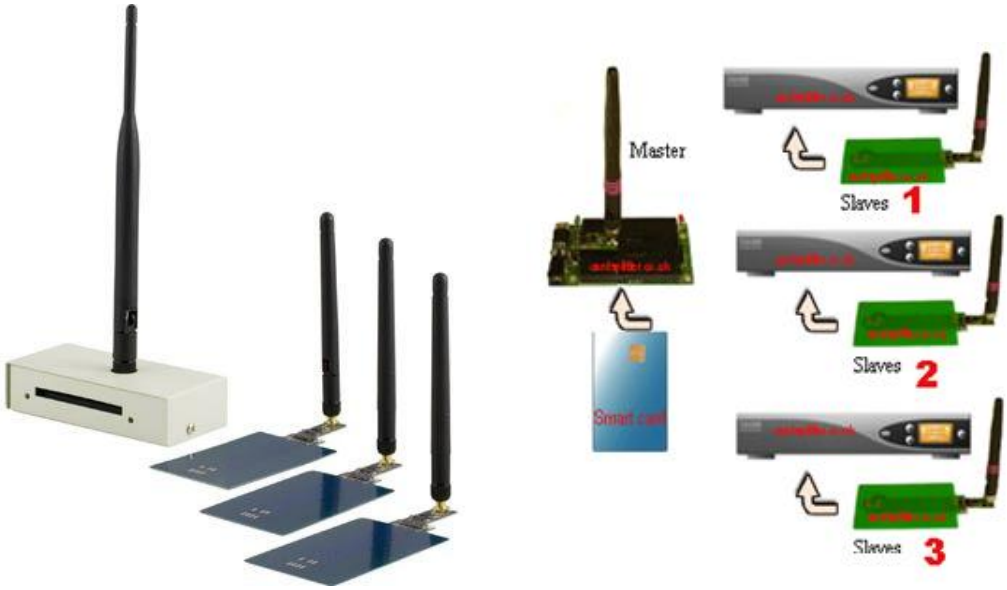
5.2.3.2 μέσω card splitters (ασύρματα)

Το ρόλο server παίζει πάλι η μικρή συσκευή-card splitter (όχι δέκτης άλλα απλός αναγνώστης κάρτας) και έχει είτε wifi ή radio frequency κεραία για αποστολή-λήψη ECM και control word.

Οι clients έχουν καταλλήλους converters που καταλήγουν στη UCAS θύρα - card reader του δέκτη (κεφάλαιο 1 αν δε θυμάστε τι είναι) και δίνουν τα κλειδιά.

Είναι προφανές ότι το σήμα μπορεί να περάσει τα όρια της οικίας, οπότε και η νομιμότητα ή η παρανομία είναι οριακά διακριτές.

Η εμβέλεια ποικίλλει ανάλογα και με τα εμπόδια. Σε ειδικές περιπτώσεις μπορεί να γίνει και ενίσχυση σήματος και να χρησιμοποιηθούν ακόμη και ενδιάμεσοι αναμεταδότες. Δηλαδή τοποθετούνται κεραίες σε ταράτσες και ολόκληρη γειτονιά συμμετέχει στην παρανόμια αν θέλει.



Σχήμα 9: Card splitters ,το κεντρικό χρησιμεύει για να μπαίνει η κάρτα ενώ τα υπόλοιπα (3 εδώ) τοποθετούνται στις υποδοχές των δεκτών-πελατών για ασύρματη αποστολή των control word

5.2.3.3 μέσω VHF συχνότητας και απευθείας λήψη από τηλεόραση

Περίπτωση καταγεγραμμένη σε ελληνικό χωρίο. Τοποθετημένος σε εκκλησία χωριού δορυφορικός δέκτης έστελνε εικόνα και ήχο σε πομπό όπου διαμορφωνόταν σε VHF συχνότητα. Οι κάτοικοι του χωρίου αφού προσανατόλιζαν την κεραία τους στην εκκλησία συντόνιζαν την τηλεόραση με τη συχνότητα VHF που έστελνε ο πομπός και παρακολουθούσαν χωρίς συνδρομή τα συνδρομητικά κανάλια. Αν και ο τρόπος δεν περιλάμβανε αποστολή κλειδιών αλλά μονό εικόνας-ήχου λόγω της ιδιομορφίας καταγράφεται.

5.2.4 Περίπτωση 4 δίκτυο: Το επίσημο PVR της Nova

Ο Panasat PVR 3001 αποτελεί την επίσημη πρόταση της Nova για διαμοιρασμό της συνδρομητικής κάρτας σε τρία ξεχωριστά τερματικά ταυτόχρονα. Ο κάτοχος αυτού του δέκτη μπορεί να έχει ταυτόχρονη παρακολούθηση διαφορετικού καναλιού σε δεύτερη τηλεόραση ενώ μπορεί να κάνει εγγραφή ενός τρίτου καναλιού.

Σχήμα 10 :Ο Panasat PVR 3001 με δύο τηλεχειριστήρια για θέαση σε δύο τηλεοράσεις με μια συνδρομή

5.2.5 Περίπτωση 5 δίκτυο : internet

Οι server και clients είναι συνδεδεμένοι στο Internet και ανταλλάζουν μέσω της Ethernet θύρας τις απαραίτητες πληροφορίες. Αποτελεί το μαζικότερο τρόπο πειρατείας και την σοβαρότερη μαζί με τη gamma card (που θα δούμε στο επόμενο κεφάλαιο)μέθοδο πειρατείας και αναλύεται πιο κάτω.

5.3 Card Sharing μέσω Internet

Μια γρήγορη σύνοψη για να θυμηθούμε τι είναι Card Sharing. Σε ένα δίκτυο Card Sharing (για χάρη συντομίας CS) όλοι οι δέκτες λαμβάνουν δορυφορικό σήμα. Έτσι λοιπόν, συντονίζουν στην επιθυμητή συχνότητα και λαμβάνουν τη transport stream με το επιθυμητό οπτικοακουστικό περιεχόμενο στο δέκτη τους, μόνο που είναι κρυπτογραφημένο. Τα κλειδιά (control words) για να ανοίξουν το κανάλι, εφόσον δεν διαθέτουν τη smart card του provider, τα λαμβάνουν μέσω του δικτύου CS από ένα δέκτη (ή υπολογιστή) που είναι εξοπλισμένος με τη νόμιμη smart card (μπορεί και όχι νόμιμη δες επόμενο κεφάλαιο). Η πηγή (δέκτης ή υπολογιστής) που διαθέτει τη smart card, ονομάζεται Server και οι συσκευές που λαμβάνουν τις απαραίτητες πληροφορίες από αυτόν, ονομάζονται Clients.Με την πληροφορία αυτή, οι Clients, παρότι δεν διαθέτουν τη smart card, μπορούν να αποκρυπτογραφήσουν το transport stream που ήδη λαμβάνουν στα tuner τους(φυσικά με το αζημίωτο καταβάλλοντας στο διαχειριστή του server το αντίτιμο που αναλογεί).

Με ποιο τρόπο όμως ξέρουν πού θα κοιτάξουν για τα Control Words και τι συμβαίνει με το CAM του συστήματος κρυπτογράφησης, που πλέον δεν υφίσταται; Εδώ έρχονται οι λεγόμενοι emulators...

Στους πελατειακούς δορυφορικούς δέκτες (clients) όπως είδαμε δεν υπάρχουν κάρτες ούτε ενεργοί αναγνώστες καρτών (CI-common interface ή UCAS -1^{ο} κεφάλαιο). Το ρόλο του CAM (hardware) έρχονται να τον αντικαταστήσουν οι Emulators ή Emu που είναι λογισμικά (software) που προσομοιώνουν τη λειτουργία του CAM ενός δέκτη. Δηλαδή έγινε αντιγραφή του υλικού και του τρόπου εξαγωγής των CW από τα ECM μέσω λογισμικού που φορτώνεται (αντιγράφεται) στην EEPROM **:** **E**lectrically **E**rasable **P**rogrammable **R**ead-**O**nly **M**emory του δέκτη του client. Εννοείται ότι ο Server τρέχει ξεχωριστό δικό του emulator (**server emulator**) που εκτός των υπολογισμών και αποστολής των CW είναι και υπεύθυνος ποιός πελάτης θα συνδεθεί μαζί του (αν έχει πληρώσει την πειρατική του συνδρομή). Επιπλέον το emulator πραγματοποιεί τη σύνδεση του server με άλλους server άλλων παρόχων εμπλουτίζοντας τα CW του δικτύου. Με την ιδία λογική ο client ‘’τρέχει’’ το δικό του emulator το : **client emulator**.

5.3.1 Πρωτοκόλλα επικοινωνίας :

Το emulator όμως σαν software εμπεριέχει και χρειάζεται για να δουλέψει το λεγόμενο πρωτόκολλο επικοινωνίας. Αφού εφαρμόζεται λογική δικτύων με κεντρικό διακομιστή (server) και πελάτες (clients) είναι λογικό να πρέπει να υπάρχουν κανόνες επικοινωνίας (ποιος ζητά, που στέλνω κλπ) αλλά και κανόνες έλεγχου (είναι ο τάδε εξουσιοδοτημένος για σύνδεση με το server;). Όλα αυτά ελέγχονται από τα πρωτοκολλά επικοινωνίας. Κάθε emulator έχει συνήθως το δικό του πρωτόκολλο αλλά μπορεί να επικοινωνεί και με πρωτοκολλά άλλων emulators. Από το τεύχος ‘’Δορυφορικών Νέων’’ Μάιος 2007 περνούμε την ιστορία και λειτουργιά των δύο πιο διαδεδομένων πρωτοκόλλων:

- **Radegast**
- **Newcamd & mgcamd**

5.3.1.1 Radegast

Το radegast είναι ουσιαστικά το πρώτο πρωτόκολλο που εφευρέθηκε για το δικτυακό sharing (διαμοιρασμό) καρτών. Οι φήμες λένε ότι η όλη ιδέα ξεκίνησε από έναν Έλληνα του εξωτερικού, ο οποίος την ημέρα (μάλλον το βράδυ) των γενεθλίων του, είχε μαζέψει μερικούς φίλους σε κάποιο σπίτι για να το γιορτάσουν. Ποτό στο ποτό, κουβέντα στην κουβέντα, ξεπήδησε και η ιδέα του να φτιάξουν ένα πρόγραμμα card sharing. Κάπως έτσι λοιπόν φημολογείται ότι δημιουργήθηκε το radegast.

Το radegast είναι πολύ απλό στη χρήση και η απλότητα του το κάνει και το πιο γρήγορο από όλα τα αντίστοιχα πρωτόκολλα. Η λειτουργία του βασίζεται σε ένα τμήμα που διαχειρίζεται τις κάρτες και σε ένα τμήμα που αναλαμβάνει το διαμοιρασμό. Ο διαμοιρασμός γίνεται μέσα από κάποια πόρτα(port) που ορίζουμε εμείς. Οι πελάτες- δέκτες μέσω αυτής της μοναδικής πόρτας, ζητάνε και παίρνουνε τα κλειδιά CW όλων των καρτών που διαχειρίζεται ο server. Δεν υπάρχει κάποιου είδους κωδικοποίηση ή κρυπτογράφηση και στην πραγματικότητα δεν υπάρχει και κάποιος έλεγχος για το ποιος ζητάει τα κλειδιά, δηλαδή μπορεί ο κάθε ένας που γνωρίζει το IP και την πόρτα του server, να ζητήσει κλειδιά από αυτόν (σχετικά πρόσφατα αυτό άλλαξε). Τα πλεονεκτήματα του είναι:

- Απλός κώδικας.
- Κώδικας που έχει δοθεί στη δημοσιότητα.
- Δυνατότητα διαμοιρασμού πολλών καρτών από το ίδιο IP και πόρτα.
- Γρήγορη απόκριση.

Αυτά τα πλεονεκτήματα έκαναν το radegast να εμφανιστεί και σε μηχανήματα που έχουν πολύ χαμηλή υπολογιστική ισχύ, όπως το inet(σχήμα 12), αλλά και σε δέκτες που δεν τρέχουν Linux,με μειωμένη επεξεργαστική ισχύ και περιορισμένη μνήμη. Όμως. έχει 2 βασικά μειονεκτήματα:

- Δεν κάνει ενημέρωση EMM (με απλά λόγια δεν ενημερώνει τα βασικά κλειδιά της κάρτας και δεν διαχειρίζεται εντολές που αφορούν στη συνδρομή, όπως ενεργοποίηση, απενεργοποίηση κλπ.).
- Δεν ελέγχει ποιος ζητάει κλειδιά. Έτσι. δεν είναι εύκολο να διαχειριστείς τους πελάτες και να περιορίσεις ποιος θα κάνει χρήση της υπηρεσίας και ποιος όχι. Για να λυθούν τα προβλήματα αυτά, δημιουργήθηκαν κάποια πρόσθετα προγράμματα (π. χ. Netpilot).

5.3.1.2 Newcamd & mgcamd

Το newcamd ήρθε με όλα τα πλεονεκτήματα του radegast. αλλά χωρίς τα μειονεκτήματα του. Το newcamd στην πραγματικότητα υπάρχει σε 2 μορφές, στην παλιά και στη νέα. Η νέα μορφή ξεκινά από την έκδοση 5. 25 και πάνω ενώ η τρέχουσα είναι 6. 10. Το newcamd ενσωματώνει κωδικοποίηση 3DES (δες κεφάλαιο 6), τόσο κατά τη διάρκεια της διαδικασίας σύνδεσης των πελατών (logon procedure) , όσο και κατά την επικοινωνία μεταξύ server και πελατών (clients). Το γεγονός ότι το 3DES είναι αρκετά ισχυρό και απαιτεί μεγάλη υπολογιστική ισχύ δεν επιτρέπει την ενσωμάτωση του σε συσκευές όπως το με μικρή επεξεργαστική ισχύ inet. Ακόμα, ο κώδικας του δεν είναι ελεύθερος, όμως κυκλοφορεί εδώ και καιρό ένα αρχείο, που εξηγεί τα βασικά σημεία για το πώς να συνδεθεί κάποιος σε ένα server newcamd (περιγραφή του πρωτοκόλλου). Αυτό επέτρεψε σε εταιρείες να ενσωματώσουν στους δέκτες τους και δυνατότητα σύνδεσης σε server τύπου newcamd. Επειδή όμως δεν έχει δημοσιευθεί το πλήρες πρωτόκολλο, αλλά τμήματα του, δεν επιτυγχάνεται 100% προσομοίωση σε δέκτες που δεν τρέχουν Linux. Παρόλα αυτά, μέχρι στιγμής δεν φαίνεται να υπάρχει κάποιο πρόβλημα με αυτούς τους δέκτες, αλλά ακόμη και αν βρεθεί, το πιθανότερο είναι να λυθεί άμεσα, με κάποια αναβάθμιση. Η αλήθεια είναι ότι στους δέκτες αυτούς έχει ενσωματωθεί το mgcamd (δες παρακάτω). Το newcamd γράφτηκε από Γερμανούς... έτσι από χόμπι. Για να μη γίνει όμως το πρόγραμμα τους αντικείμενο πειρατείας, δηλαδή για να μη χρησιμοποιηθεί από κάποιους που θα πουλάνε πειρατικές συνδρομές, ενσωμάτωσαν εκούσια δύο μειονεκτήματα και αυτά δεν είναι άλλα από τη μη υποστήριξη καρτών Premiere Word και NDS (Sky UK & Sky Italia).

Μια άλλη ομάδα, που δεν είχε τέτοιους προβληματισμούς, δημιούργησε το mgcamd, το οποίο είναι ίδιο με το newcamd , χωρίς φυσικά τα μειονεκτήματα του. Ακόμη και σήμερα, όταν μιλάμε για σύνδεση newcamd, στην πραγματικότητα εννοούμε mgcamd. Το newcamd απαιτεί εκτός από την πόρτα επικοινωνίας και μερικές άλλες παραμέτρους για να μπορέσει κάποιος πελάτης να συνδεθεί και να ζητήσει κλειδιά. Αυτές είναι το Login credentials, που είναι το όνομα χρήστη (login) και το συνθηματικό (password) και το Encryption key. που αποτελεί το κλειδί DES για την κωδικοποίηση της επικοινωνίας. Με αυτόν τον τρόπο, μόνο όποιος έχει τα σωστά παραπάνω στοιχεία μπορεί να συνδεθεί με το Server. Οι συνδέσεις newcamd επιτρέπουν την ενημέρωση κλειδιών από τους πελάτες, ενώ υπάρχει και ειδική εντολή που καθορίζει σε ποιους από αυτούς θα επιτρέπεται κάτι τέτοιο. Με άλλα λόγια, ο διαχειριστής του server φτιάχνει μια λίστα με πελάτες που επιτρέπεται "να συνδεθούν και αν αυτοί θα έχουν δυνατότητα ενημέρωσης κλειδιών. Για κάθε έναν από αυτούς, εκδίδει ένα όνομα χρήστη και ένα συνθηματικό (login / password).

Υπάρχει τουλάχιστον ένας λόγος να μην επιτρέπεται σε όλους τους πελάτες να κάνουν ενημέρωση κλειδιών. Αυτός είναι ότι ο πελάτης για να κάνει κάτι τέτοιο, θα πρέπει να έχει πρόσβαση σε όλα τα στοιχεία της κάρτας που διαμοιράζεται, συμπεριλαμβανομένου και του αριθμού σειράς. Αυτό επιτρέπει σε κάποιο να δει ποια κάρτα έχει ο server και να την ακυρώσει αν ο server είναι παράνομος. Άλλος λόγος είναι για να περιοριστεί ο όγκος των δεδομένων (traffic) που διακινείται στο δίκτυο και έτσι να μπορούν περισσότεροι πελάτες να συνδεθούν.

Να αναφέρω εδώ, ότι στις περισσότερες περιπτώσεις ο newcamd server διαχειρίζεται μία κάρτα ανά πόρτα. Έτσι. αν ο server έχει 2 κάρτες, πρέπει ο πελάτης να κάνει 2 φορές

σύνδεση σε διαφορετική πόρτα, μία για κάθε κάρτα, σε αντίθεση με το radegast που επιτρέπει το πέρασμα ECM πολλών καρτών από την ίδια πόρτα. Επίσης, αυτό που αναφέρω παραπάνω απλοϊκά ως ενημέρωση κλειδιών", στην πραγματικότητα είναι ενημέρωση EMM.

Εκτός αυτών γνωστά είναι και τα

5.3.1.3 CCcam

- συνήθως για Dreambox δέκτες/Linux Pc με θετικά και αρνητικά τα εξής:

+ Υποστηρίζεται ακόμα(δηλαδή βγαίνουν συνεχώς νέες εκδόσεις)
+Πολλοί χρήστες
+/- Όχι αρκετά γρήγορο.
- Δημιουργεί μεγάλο φόρτο κίνησης.
- Ακόμα δεν υποστηρίζεται από όλα τα tuner (SH4 etc.)

5.3.1.4 Gbox

- για Linux Pc/Windows Pc με θετικά και αρνητικά τα εξής:

+ Γρήγορο
+ Καταναλώνει λίγους πόρους δικτύου(δε δημιουργεί μεγάλο φόρτο).
- Δεν αναπτύσσεται πλέον
- Δεν υποστηρίζεται από όλα τα tuner της αγοράς

Τέλος υπάρχουν και τα emulator Evocamd , Mgcamd, Camd3 αλλά και αρκετά άλλα πειραματικά ή για ειδικά κανάλια. Όλα όμως με τον ίδιο σκοπό.

Επειδή όμως τα emulators και τα πρωτόκολλα σχεδιάστηκαν από διαφορετικές ομάδες παρουσιάζουν ασυμβατότητες μεταξύ τους μια συσχέτιση κάποιων φαίνεται στον πίνακα που ακολουθεί :

Emulator	Λειτουργία	Σύνδεση με Server	Σύνδεση με Emulator
NewCS	Server	-	MGcamd/Evocamd /Camd3/CCcam κ. ά.
MGcamd	Client	NewCS	-
Evocamd	Client	NewCS	-
Camd3	Server + Client	-	Camd3
CCcam	Server + Client	-	CCcam

Σχήμα 11: Οι emulators και οι συνδυασμοί που μπορούν να γίνουν μεταξύ τους

5.3.2 Τρόποι Card Sharing μέσω διαδικτύου.

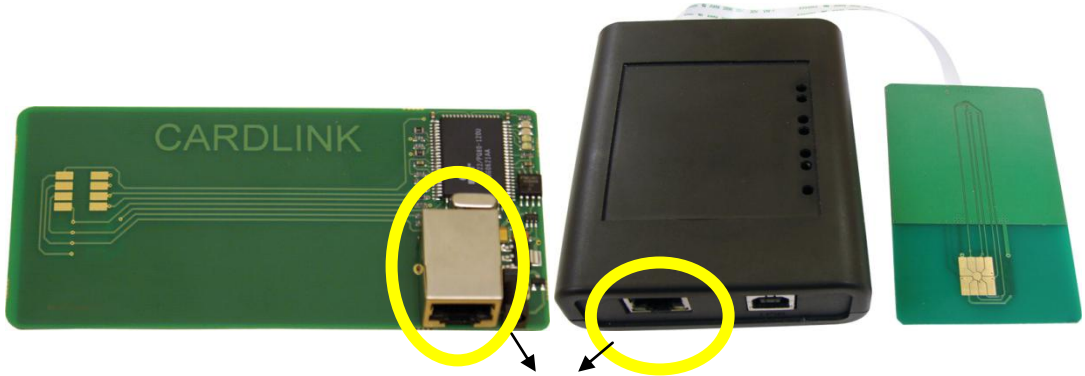
Αν και το δίκτυο είναι ένα και το αυτό οι τρόποι είναι διάφοροι και πολλοί.

5.3.2.1 Διαδικτυακό μοίρασμα από την RS-232 δεκτών

Ειδικό λογισμικό (για ορισμένους δέκτες) το οποίο τρέχει σε ανοιχτό υπολογιστή, επιτρέπει στο δέκτη που είναι συνδεδεμένος σειριακά με τον υπολογιστή, να συμμετέχει (υπό προϋποθέσεις) σε ορισμένα δίκτυα. Στην πράξη, έχουμε εδώ μία πλέον σύγχρονη επιστροφή στις ρίζες, αφού το πρώτο μοίρασμα κάρτας έγινε μέσω υπολογιστή και σειριακής θύρας, με τη χρήση season interface που έμπαινε στο CAM ή card reader του δέκτη και έδινε τις σωστές απαντήσεις για το άνοιγμα καναλιών

5.3.2.2 i-net season interface - Cardlink Ethernet smart card

Δίνουν Ethernet Interface σε ένα απλό STB (δορυφορικό δέκτη) για να επικοινωνεί στο internet για card sharing. Έχουν eprom και μπορούν να ''φορτωθούν'' με emulators για να επικοινωνούν με server.

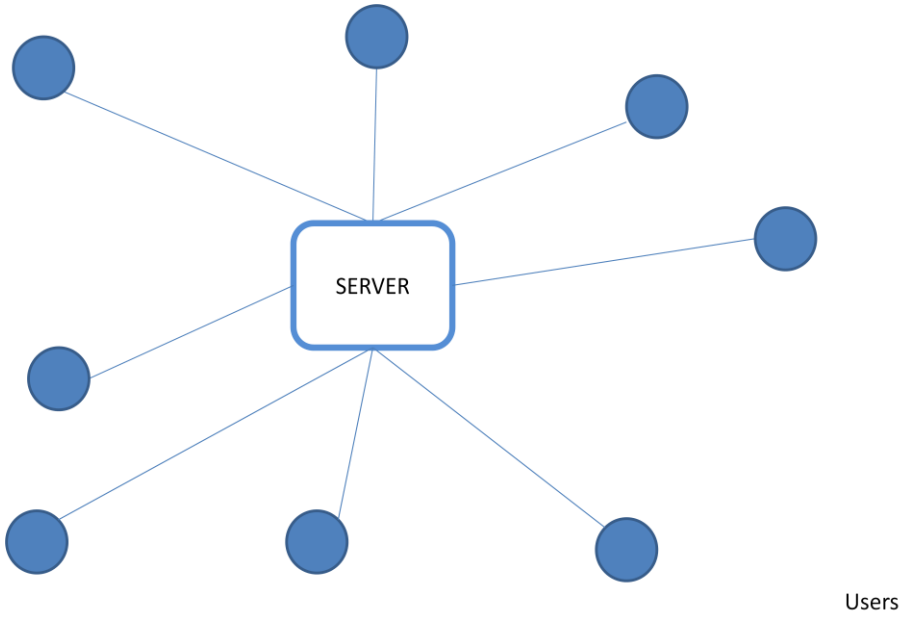


Σχήμα 12:Συσκευές που μετατρέπουν την CI υποδοχή του δέκτη σε Ethernet Interface,του δίνουν δηλαδή δυνατότητες να ενώνεται με το διαδίκτυο και server για ανταλλαγή κλειδιών

5.3.2.3 Δέκτες /pc με Ethernet-linux και ανεπίσημο λογισμικό- ΙΔΙΟΚΤΗΤΟΙ

Αυτό είναι σήμερα το πλέον διαδεδομένο card sharing. Αν αυτό γίνεται στα όρια του εσωτερικού σας δικτύου (LAN) , είναι σαφώς νόμιμο, αν όμως επεκτείνεται στο διαδίκτυο (WAN) , τότε είναι σαφώς παράνομο!

Σε πολύ γενικές γραμμές, η προς διανομή κάρτα μπαίνει στο card reader του δέκτη- server. ο οποίος και τη διαβάζει με τη βοήθεια κάποιου ειδικού emulator. Εφόσον οι κατάλληλες ρυθμίσεις για τη διανομή, οι απαντήσεις της κάρτας μεταβιβάζονται και στο υπόλοιπο δίκτυο, μέσω της θύρας Ethernet του δέκτη και καταλήγουν σε έναν ή περισσότερους δέκτες-πελάτες που χρησιμοποιούν τη συνεργαζόμενη εκδοχή-πελάτη του emulator που χρησιμοποίησε ο server (εφόσον βέβαια έχουν... αδειοδοτηθεί κατάλληλα). Όλες οι παραπάνω λειτουργίες επιτυγχάνονται συνήθως σε δέκτες με Linux (Dreambox) και ανεπίσημα λογισμικά. Έτσι server γίνονται άνετα από ένα ερασιτέχνη και μπορεί να αποδώσει κέρδη έως και 10000 ευρώ το μηνά (τιμές για 2009). Αυτό γιατί η μηνιαία πειρατική συνδρομή κυμαίνεται από 5-20 ευρώ (χρεώνει ο έχων το server, πληρώνει ο πελάτης) και οι πελάτες φτάνουν μέχρι και 500.



Σχήμα 13: Ο server και οι πελάτες (παράνομοι πελάτες πάντα)

Πιο επαγγελματική λύση είναι η υλοποίηση σε υπολογιστή. Ένας αναγνώστης καρτών συνδέεται με τη σειριακή θύρα του υπολογιστή που κάνει το ρόλο του server. Όπως είναι γνωστό το κάθε τι στο internet μπορεί να καταγραφεί και να ανιχνευθεί και αργά ή γρήγορα να βρεθεί η τοποθεσία του, έτσι οι πειρατές σκέφτηκαν τρόπους να μην αφήνουν ίχνη σε περίπτωση που ανακαλυφθεί ο server (proxy server).

Οι server λοιπόν τρέχουν secure – encrypted linux σε μηχανήματα που δεν έχουν σκληρούς δίσκους. Δηλαδή το μηχάνημα εκκινά από CD-ROM και όλο το λειτουργικό τρέχει στην μνήμη RAM. Το CD-ROM αφαιρείται από το μηχάνημα και έτσι ο server, αν κάποιος τον βρει, να μην έχει καταγεγραμμένα στοιχεία ούτε για το πρόγραμμα που τρέχει ούτε για τους πελάτες που είναι κείνη την ώρα επάνω. Ως γνωστό ότι τρέχει στην RAM χάνεται μόλις διακοπεί το ρεύμα. Έτσι δεν υπάρχουν στοιχειά εναντίον κανενός στο δικαστήριο (κάτι παρόμοιο γίνεται και στα internet cafe που τρέχουν τα φρουτάκια στη μνήμη RAM , μόλις έρθει η αστυνομία ο υπολογιστής σβήνει και όλα εξαφανίζονται).

Οι server αυτοί κρατάνε πολλές φορές μέχρι και 8 επίσημες συνδρομητικές κάρτες, που θα μπορούσαν να αποτελέσουν αποδεικτικά στοιχεία (αφού έχει σειριακό αριθμό που είναι συνδεδεμένος με αυτόν που αγόρασε την κάρτα). Για να μην βρεθούν οι κάτοχοι αυτών των καρτών, αυτές κόβονται ώστε να μην φαίνονται τα στοιχεία από το πλαστικό της κάρτας και τα τσιπάκια (ολοκληρωμένα) τοποθετούνται σε μία ειδική βάση που τα καταστρέφει περνώντας υψηλή τάση αν κάποιος παραβιάζει την πόρτα του server.(Οι πληροφοριες λήφθησαν από το www.zotos.biz)

Για να υπάρχει η μυστικότητα και η εχεμύθεια με σκοπό την προστασία και του πειρατή αλλά και του πελάτη, τα χρήματα αυτά περνάνε από χέρι σε χέρι χωρίς καταθέσεις σε λογαριασμούς τραπεζών ή άλλων ηλεκτρονικών συναλλαγών που μπορούν να ανιχνευθούν. Οι συνδρομές κυμαίνονται από 5 έως 20 ευρώ το μηνά ενώ οι νόμιμες συνδρομές έχουν συνήθως 40-60 ευρώ (τιμές 2009). Έτσι εκτός του ότι χάνει ο πάροχος έσοδα χάνει και το κράτος από το μαύρο αφορολόγητο χρήμα που ανταλλάσσεται.

Ο διαχειριστής του server δίνει πρόσβαση σε οποίον έχει πληρώσει την πειρατική του συνδρομή. Σε κάθε client δίνει ένα user name ,password,όπως και την ip του server. Έτσι ο χρήστης μπορεί να έχει μοναδική πρόσβαση από οποίο τερματικό θέλει αλλά κάνοντας login μονό μια φόρα. Δηλαδή η ταυτόχρονη πρόσβαση με τον ίδιο κωδικό είναι ανέφικτη και δε μπορούν ταυτόχρονα να μπουν δύο client στο δίκτυο με τα ιδία στοιχειά. Το σύστημα αν και πειρατικό αυτοπροστατεύεται δηλαδή από εσωτερικούς πειρατές.

Οι server -δέκτες συνήθως ‘’στήνονται ‘’ στην Ελλάδα και γι’αυτό και η αστυνομία έχει βρει πολλά από αυτά τα δίκτυα. Οι server υπολογιστές όμως συνήθως βρίσκονται σε γειτονικές ή πιο μακρινές χώρες κάνοντας δύσκολο τον εντοπισμό τους.

5.3.2.4 Server για δέκτες με Ethernet και ανεπίσημο λογισμικό-ΕΤΑΙΡΙΚΟΙ

Εδώ έχουμε τη δεύτερη πιο διαδεδομένη πρακτική σήμερα, που είναι βέβαια και η πλέον παράνομη! Ορισμένοι δέκτες με θύρα Ethernet και ειδικό ανεπίσημο λογισμικό, με το που θα συνδεθούν στο διαδίκτυο εντοπίζουν ειδικούς σερβιτόρους που έγιναν για λογαριασμό τους και μόνο και τροφοδοτούνται από αυτούς, με όλα τα χρειαζούμενα για το άνοιγμα αρκετών πακέτων. Οι ειδικοί αυτοί server υφίστανται σε χώρες που είναι δύσκολο να κλείσουν νομικά (δες Κίνα, Βόρειος Κορέα και κάτι νησιά στους ωκεανούς).

Οι δέκτες κάνουν login (σύνδεση) στο server της εταιρίας που λανσάρει τους δέκτες με τη MAC address και ένα serial number που διαθέτουν. Έτσι η πρόσβαση δεν είναι εφικτή για δέκτες που δεν υπάρχουν στο database του server.Πολλές δεν υφίσταται μηνιαία συνδρομή (η συνδρομή είναι για όσο ζήσει ο server δηλ. μήνες έως χρόνια). Το κέρδος όμως βγαίνει από την τρελή πώληση των ιδιόκτητων δεκτών (με τιμή περίπου 250 – 300 ευρώ) που φαίνεται να είναι επικερδής για να υφίστανται ακόμα έτσι server.

Τέτοιοι δέκτες στην ελληνική αγορά είναι οι nanox (ή κοντός στα forum) ,tecview, vissionet, protek. Εξαίρεση αποτελεί ο vissionet, ο όποιος αν και δούλευε χρονιά σαν non-pay server όπως οι άλλοι έχει μια μικρή ετήσια συνδρομή. Αύτη ενεργοποιείται με ένα κωδικό που βρίσκει κάποιος σε ειδικά ξυστά στη μαύρη αγορά, δηλαδή Ομόνοια.

Οι δέκτες παρέχουν ανεπίσημο forum (δεν παραδέχονται ότι είναι δικό τους δηλαδή) για την υποστήριξη αλλά και φερεγγυότητα της δουλείας τους (δηλαδή αγόρασε το δεκτή μας και δεν θα εξαφανιστούμε). Εκεί οι χρήστες δηλώνουν κανάλια που επιθυμούν να ενταχτούν στο server ,αναφέρουν βλάβες του server, πληροφορίες εγκατάστασης του δεκτή κ.α. Οι ιδιόκτητοι αυτοί δέκτες όπως και οι Dreambox πωλούνταν καθαροί’’ ,δηλαδή σαν απλοί δέκτες χωρίς παράνομο λογισμικό για σύνδεση στο δίκτυο. Έτσι παρέχεται πλήρης νομική κάλυψη στον προμηθευτή που δεν είναι υπεύθυνος για το τι θα εγκαταστήσει ο χρήστης πάνω. Ο χρήστης τώρα αφού πάει σπίτι του εγκαθιστά μέσω διαδικτύου (με τη βοήθεια των forum) το παράνομο λογισμικό σύνδεσης με το server (που είναι και αυτό τις κατασκευάστριας εταιρίας) και καταφέρνει τη σύνδεση με το server. Είναι σχεδόν αυτονόητο να αναφέρουμε ότι οι κατασκευαστές των δεκτών δεν παραδέχονται την ύπαρξη από μέρους τους, των ειδικών αυτών free-pay server.

Απόσπασμα από forum ενός από τους δέκτες αναφέρει-προδίδει το μέγεθος τους.

''…I notice something very disturbing that has nothing to do with the number of people on the net. 11823 server had only about 550 to 600 people which is nothing compared to the 65k which is the limit. Some other transponders on Astra for example had 3 times the above.

I will report this, in the mean time I had to take offline 2 servers…. ''

Ο τεχνικός μιλά για ένα πρόβλημα που υπάρχει στον ένα από τους 5 server που παρέχουν κλειδιά στους χρήστες για νόβα. Η νόβα έχει σαν εταιρεία ενοικίαση 5 συχνότητες στο Hotbird δορυφόρο 10930H,11240H,11823H,11938H,12169H, (υπάρχει και η 12245 που έχει όμως ένα κανάλι) Σε κάθε συχνότητα (transponder=αναμεταδότη) μπορεί να στριμώξει με επίπτωση στην ποιότητα όσα κανάλια θέλει συνήθως έχει έως 10. Ανά συχνότητα τοποθετείται ένας server, απ'ότι βλέπουμε κάθε server ''σηκώνει'' 65000 χρήστες οπού 65000*5=325000 ταυτόχρονα. Αυτό το νούμερο είναι για τη μεγίστη ΤΑΥΤΟΧΡΟΝΗ σύνδεση χρηστών στο server οπότε οι συνολικοί κάτοχοι αυτών των δεκτών μπορεί να είναι παραπάνω.

Στο παρελθόν όμως δεν είναι λίγες οι φόρες που τρίτοι πειρατές κατάφεραν να συνδεθούν στους ιδιόκτητους server κάνοντας login από υπολογιστές ή Linux δέκτες (Dreambox) χωρίς την αγορά του ιδιόκτητου server. Δηλαδή και μεταξύ των πειρατών υφίσταται πειρατεία

5.3.3 Μεγάλα δίκτυα πως υλοποιούνται

Εδώ όμως είπαμε ότι η τάξη μεγέθους χωρητικότητας αυτών των server φτάνει το O (100000) δηλαδή είναι της τάξης των εκατοντάδων χιλιάδων. Όμως κάθε κάρτα μπορεί λόγω επεξεργαστικής ισχύς να απάντα σε ερωτήσεις ECM σε CW σε μέγεθος το πολύ 20-30 χρήστες. Αυτό γιατί ο μέσος χρόνος αλλαγής CW άρα και αποστολής ECM στην κάρτα είναι 9-10sec δηλαδή περίπου 10000ms. Ο μέσος χρόνος επεξεργασίας και εξαγωγής του CW από το νέο ECM είναι 200-500ms άρα άμα όλοι οι χρήστες στο δίκτυο βλέπουν κανάλι διαφορετικού ECM και θέλουν ξεχωριστό CW φτάνουμε στο 10000ms/350ms=28 χρήστες. Αν και οι χρόνοι μεταβάλλονται ανάλογα με τον πάροχο, την κάρτα και τον αριθμό καναλιών (άρα και διαφορετικά ECM), ο αριθμός χρηστών σπανία μπορεί να ξεπεράσει χωρίς άλλη τεχνική τους 30.

Μιλήσαμε όμως για τάξη μεγέθους δικτύου O(10000) πως φτάνουμε σε αυτά τα νούμερα;

Οι τεχνικές που εφαρμόζονται είναι τεχνολογικά ανεπτυγμένες πράγμα που δείχνει και το κέρδος που παρουσιάζουν όπως και το κενό που παρουσιάζουν τα υφιστάμενα κρυπτογραφικά δορυφορικά συστήματα.

Μια τεχνική είναι ο υπερχρονισμός (over clock) της συνδρομητικής κάρτας με αυτό το τρόπο ο χρόνος επεξεργασίας ενός ECM μειώνεται και αυξάνονται οι χρήστες. Αυτός ο τρόπος καταστρέφει με τον καιρό την κάρτα αλλά και δεν αυξάνει σε μεγάλο βαθμό τους χρήστες όσο η επομένη τεχνική.

Η κύρια τεχνική είναι το caching ή buffering (προσωρινή αποθήκευση) των control words και αποστολή στους χρήστες.

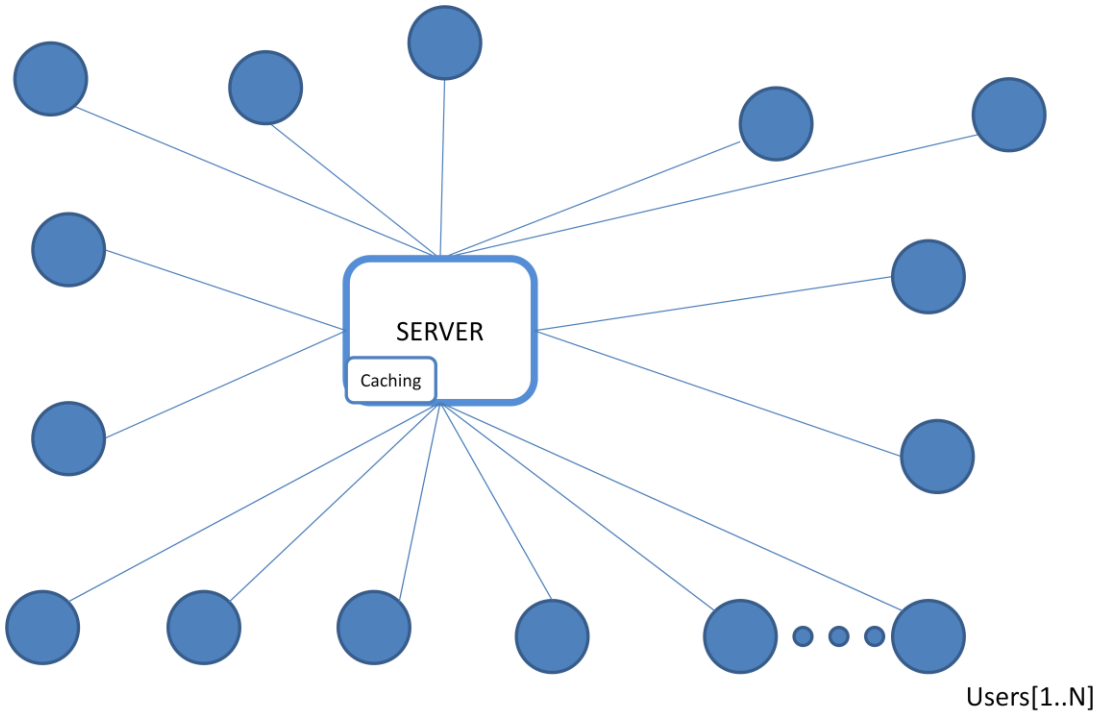
Μέσω του caching των control words η κάρτα για το ίδιο control word δεν ξαναρωτιέται. Δηλαδή ο server διατηρεί ένα πινάκα control words και ecm

ECM	Control Word

Σχήμα 14: Πίνακας αντιστοιχίας ECM και control word

Με το που φτάνει από κάποιο χρήστη ένα ερώτημα ECM ο server ψάχνει τον πίνακα ,αν δεν υπάρχει το ECM ρωτά την κάρτα παίρνει την απόκριση του Control Word καταγράφει το ζεύγος στον πινάκα και στέλνει το control word σε αυτόν που το ζήτησε. Αν τώρα έρθει ένα ECM ερώτημα που εμπεριέχεται στον πινάκα ο server δε ρωτά την κάρτα αλλά κάνει αντίγραφο του Control word που αντιστοιχεί στο ECM και το στέλνει στον αιτούντα. Έτσι με αυτή την τεχνική δε καταπονείται η κάρτα και μπορούν με την ίδια κάρτα να εξυπηρετηθούν πολλοί περισσότεροι παράνομοι πελάτες. Όπως αναφέραμε όμως η διάρκεια των ECM είναι περίπου 10 sec έτσι ο πίνακας διαγράφει μετά από μια λογική πάροδο χρόνου (πχ 30 sec)τις πιο παλιές εγγραφές αφού ο πάροχος δεν θα ξαναστείλει το ίδιο ECM σε σύντομο χρόνο.

Σε όλα τα παρακάτω μοντέλα που θα ακολουθήσουν υποστηρίζεται η τεχνική caching και γι'αυτό δε θα αναφέρεται.

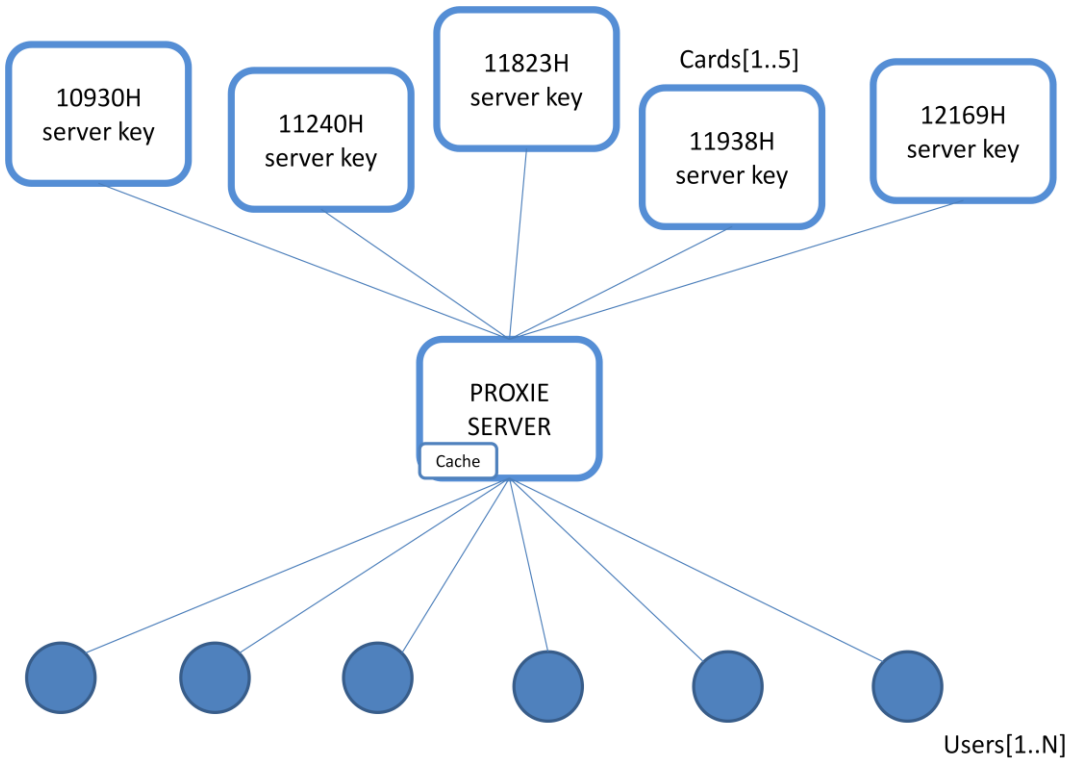


Σχήμα 15: Με τη μέθοδο Caching οι πελάτες που μπορούν να εξυπηρετηθούν αυξάνονται

Αφού έφτασε και αυτή η τεχνική στα όριά της χρησιμοποιήθηκε η τεχνική της τοποθέτησης νόμιμης συνδρομητικής κάρτας ανά συχνότητα μαζί με αυτόματη εξαγωγή control words. Αυτό γίνεται δια το λόγο ότι όπως αναφέραμε ανά συχνότητα εμπεριέχονται στην transport stream πάνω από ένα κανάλι (συνήθως 8-10 με DVB-S και mpeg-2),έτσι η εναλλαγή καναλιών στην ίδια συχνότητα είναι πιο οικονομική σε χρόνο παρά την εναλλαγή καναλιών σε διαφορετική συχνότητα. Η εξοικονόμηση χρόνου, δηλαδή με το που δημιουργεί ο πάροχος το control word να μπαίνει στο δίκτυο, είναι καίριο σημείο για τη σωστή λειτουργία του δικτύου. Γι αυτό και οι πάροχοι προσπαθούν να χτυπήσουν αυτά τα δίκτυα στη ρίζα τους στην αυτόματη αλλαγή των καναλιών δηλαδή. Έτσι η irdeto παρουσίασε την τεχνολογία ''Surf Locking'' που κλειδώνει την κάρτα αν αυτή κάνει συνεχόμενο και για πολλή ώρα zapping (αλλαγή καναλιού).

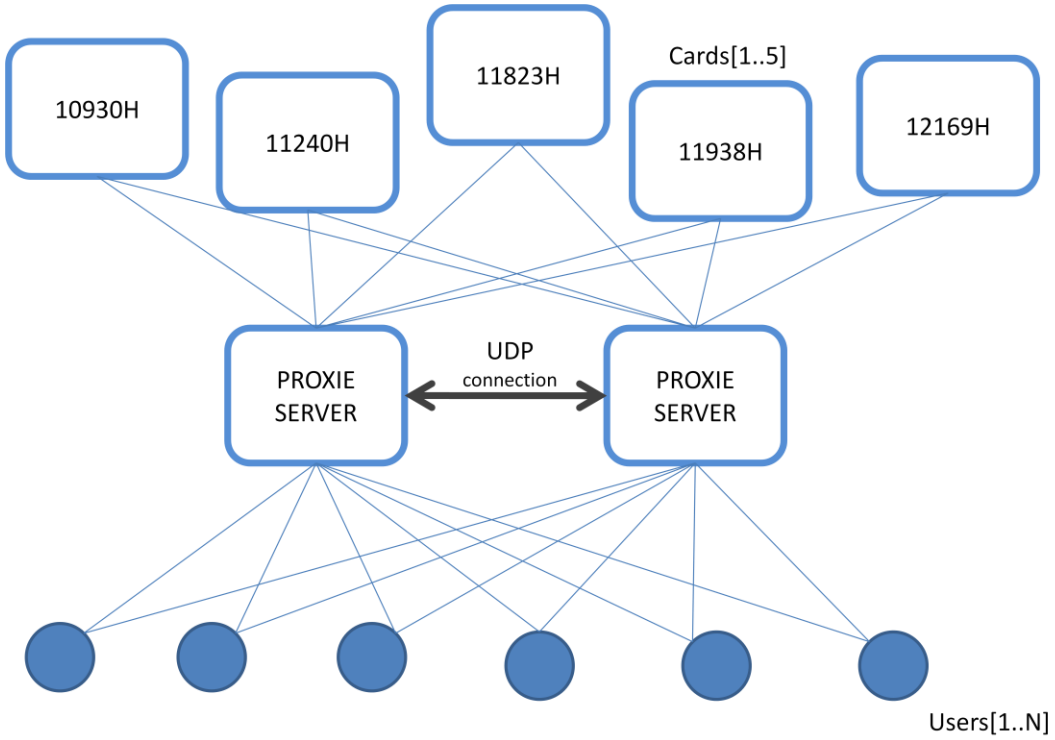
Κάθε κάρτα που ''διαμοιράζεται'' τοποθετείται ή σε υπολογιστή ή σε ειδικό δέκτη (ονομάζονται **server key**) ο οποίος κάνει αυτόματη και συνεχή εναλλαγή καναλιών στην ίδια συχνότητα οπότε στέλνονται ECM στην κάρτα και λαμβάνονται τα CW κλειδιά τα οποία εξάγονται στο κεντρικό server όσο πιο γρήγορα γίνεται(σχήμα 16). Η αυτόματη εναλλαγή καναλιών ,αν και θα μπορούσε να υλοποιηθεί με κάποιο να κρατά το χειριστήριο και να αλλάζει κανάλια συνεχεία, γίνεται με μικρά προγράμματα script. Τα κλειδιά στέλνονται στον κεντρικό server και αποθηκεύονται στην προσωρινή μνήμη (cache) σε πίνακα(σχήμα 14) όπου έρχονται τα ECM ερωτήματα των πελατών. Αξίζει να αναφέρουμε ότι οι **server Key** δεν ερωτούνται ή περιμένουν ECM από κάποιο χρήστη τα script προγράμματα είναι υπεύθυνα γι' αυτά. Οι χρήστες απλός ερωτάνε τον κεντρικό server στέλνοντας τις ερωτήσεις ECM. Ο server εδώ απλός λαμβάνει τα αιτήματα από τους πελάτες βρίσκει

στους πίνακες τους το control word που ζητείται βάσει του ECM που έστειλε ο πελάτης και κάνει ένα αντίγραφο το οποίο το στέλνει στον αιτούντα (έξυπνο!).Έτσι η κάρτα δε καταπονείται (που είναι και το ζητούμενο) και το δίκτυο τροφοδοτείται με CW.



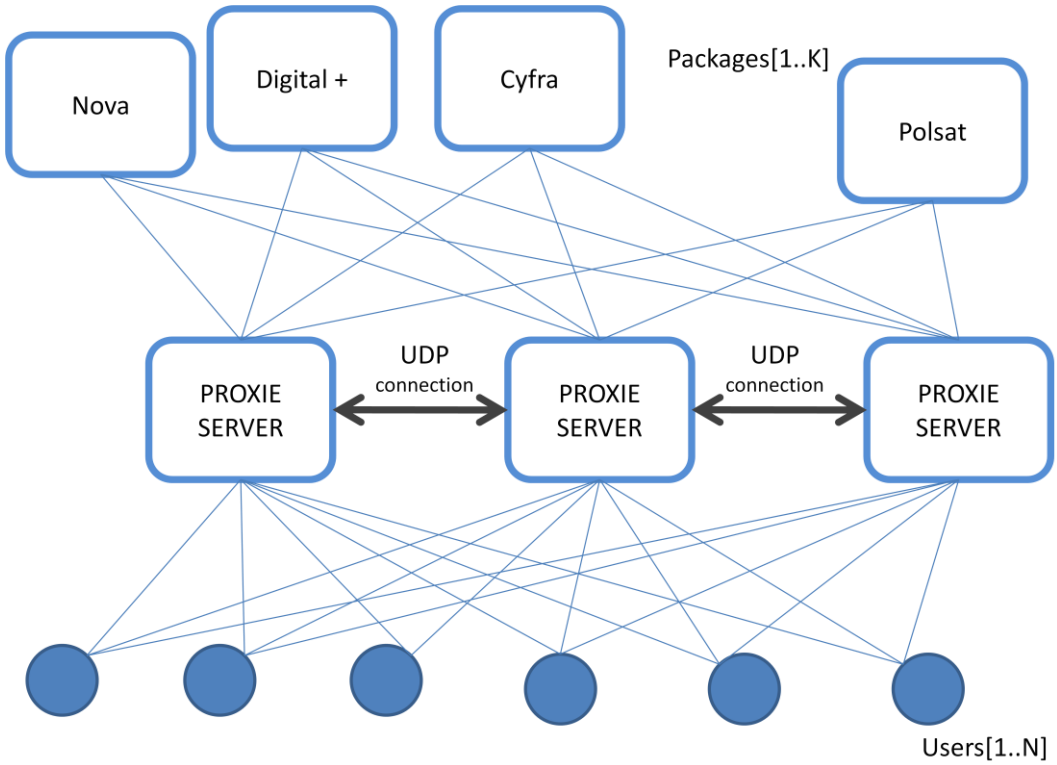
Σχήμα 16 :Server ενωμένος με δέκτες (server key) συντονισμένους σε καθορισμένη συχνότητα για άμεση εξαγωγή των control words

Επειδή σε όλα τα συστήματα που λειτουργούν σε έτσι μέγεθος χρηστών (εκατοντάδες χιλιάδες) υπάρχουν και backup server έτσι και εδώ βλέπουμε συστήματα με δύο server ή και παραπάνω για back up αλλά και εξισορρόπηση φορτίου (σχήμα 17).



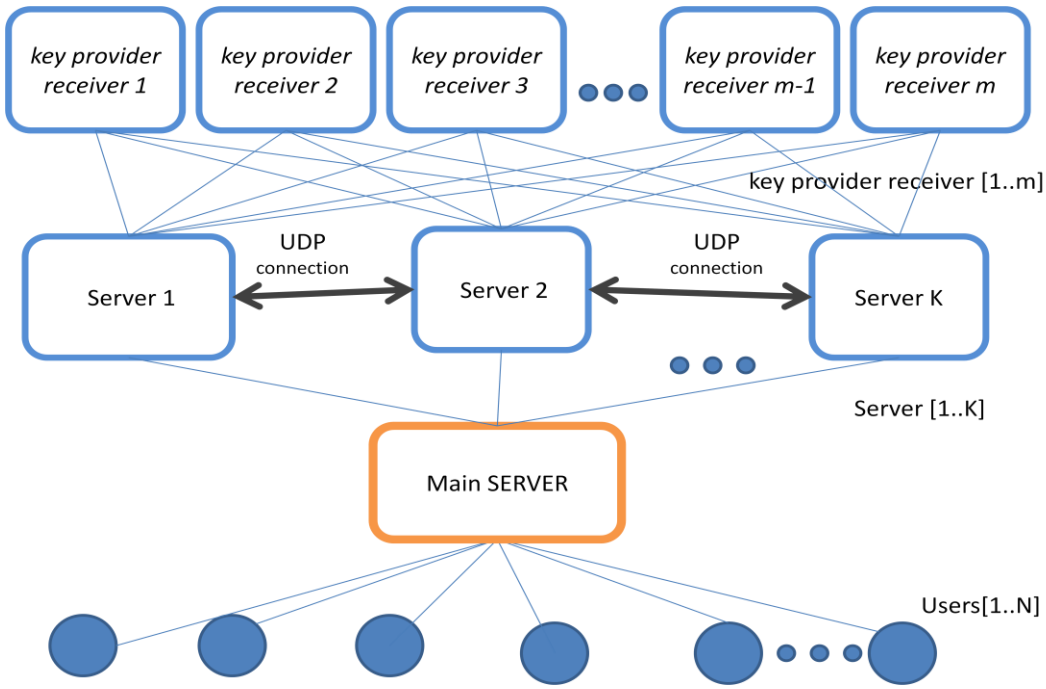
Σχήμα 17:Server ενωμένος με άλλο server για εξισορρόπηση φορτίου αλλά και για back up

Το μοντέλο δε περιορίζεται φυσικά σε έναν πάροχο και είναι επεκτάσιμο και μπορεί να συνεργαστεί και με άλλους παρόχους. Οπότε ένα πειρατικό δίκτυο μπορεί και να προσφέρει control words και άλλων παρόχων (σχήμα 18).



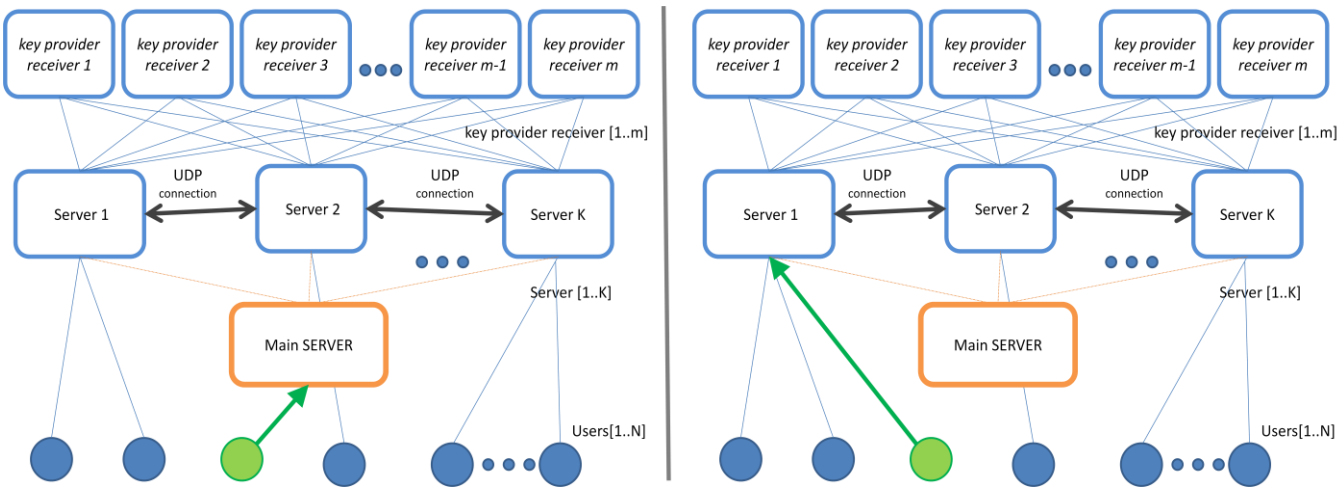
Σχήμα 18:Η προσθήκη άλλων μπουκέτων (εκτός πχ Nova) γίνεται με εύκολο τρόπο και κάνει το server πιο ελκυστικό για παράνομους χρήστες

Ενώ αν το δίκτυο είναι αρκετά μεγάλο αλλά και αν θέλουμε να είναι εύκολα επεκτάσιμο χρησιμοποιούνται πολλοί server οργανωμένοι από έναν κύριο server ,τον main server, (σχήμα 19).



Σχήμα 19: Οργάνωση του συστήματος από ένα Main Server

Σύμφωνα με αυτό το μοντέλο ένας νέος πελάτης(πράσινη κουκίδα) ρωτά το main server που να συνδεθεί, αυτός του δίνει σύνδεση με ένα server και ο πελάτης επικοινωνεί κατευθείαν με το server. Οι server επικοινωνούν τακτικά με το main ανταλλάζουν πληροφορίες κίνησης και χωρητικότητας έτσι ώστε ο main server να ξέρει που να στείλει ανά πάσα στιγμή κάθε νέο πελάτη. Έτσι οι πελάτες, τα τερματικά δηλαδή, πρέπει να ξέρουν μόνο την IP του main server που πρέπει να είναι σταθερή. Ενώ η προσθήκη/κατάργηση ενός server γίνεται εύκολα με απλή δήλωση/διαγράφη του server στο main server. Οπότε το σύστημα είναι επεκτάσιμο .



Σχήμα 20: Η λειτουργία του Main Server

Για ακόμα γρηγορότερη απόκριση και λιγότερη καθυστέρηση οι πελάτες αφού συνδεθούν σε ένα server δεν στέλνουν στο server το EMC (8-32 bytes) αλλά απλώς τον αριθμό του καναλιού που επιθυμεί να δει ο πελάτης. Ο κάθε server ξέρει ότι όταν δει τον αριθμό καναλιού απαντά με το τρέχων control word που έχει για το κανάλι αυτό. Έτσι γίνεται οικονομία στο bandwith του δικτύου αφού οι 8 bytes EMC πληροφορίες αντικαθιστώνται με λίγα bits. Επίσης ο client μπορεί να στείλει τη συχνότητα του καναλιού του βλέπει και το δίκτυο να του στείλει όλα τα κλειδιά (CW) των καναλιών που υπάρχουν σε αυτή τη συχνότητα. Ενώ άλλη λύση είναι η αποστολή όλων των κλειδιών στον πελάτη χωρίς να ενδιαφέρεται ο server πιο κανάλι θέλει να δει ο client. Κάτι τέτοιο καταπονεί το δίκτυο αλλά είναι πιο εύκολο. Αυτή την τεχνική χρησιμοποιούν και οι δορυφορικοί server που αναλύονται στην κάτωθι παράγραφο.
Η αρχιτεκτονική αυτών των πειρατικών δικτύων δεν είναι συγκεκριμένη και τυποποιημένη αφού είναι παράνομη και εξαρτώνται ανάλογα με τους πελάτες που εξυπηρετεί ,τα χρήματα που διατίθενται αλλά και την τεχνογνωσία αλλά και ευφυΐα που διαθέτουν οι σχεδιαστές του.
Ένα άλλο δίκτυο που δεν αναφέρθηκε και χρησιμοποιείται ανά διαστήματα είναι η αποστολή των control words μέσω δορυφόρου από το server και λήψη τους από τους πελάτες. Το όλο δίκτυο είναι ο δορυφόρος, δεν υπάρχει internet και επειδή δεν υπάρχει κανάλι επιστροφής από τους πελάτες στο server (οι πελάτες δέχονται πληροφορίες και σήμα από το δορυφόρο δε μπορούν να στείλουν πίσω)ο δεύτερος αποστέλλει όλα τα control words όλων των καναλιών του παρόχου (ανεξάρτητα πιο θέλει ο χρήστης).Το κρυπτογραφημένο σήμα φτάνει πάντα από τον πάροχο, τα κλειδιά όμως από τον παράνομο server. Έτσι είναι προφανές ότι πρέπει να υπάρξει δεύτερο tuner (που θα λαμβάνει μόνο τα κλειδιά). Τα control words φτάνουν στο δέκτη του πελάτη και ο δέκτης μέσω ειδικού λογισμικού διαλέγει το control word που επιθυμεί. Πως μπορεί κάποιος να αποστέλλει μέσω δορυφόρου control words έτσι εύκολα; Η απάντηση είναι ότι αυτά αποστέλλονται μέσω δορυφορικού internet κρυμμένα μέσα σε πακέτα IP .Ένας χρήστης κάνει συνδρομή για δορυφορικό internet και κατεβάζει από μια σελίδα στο internet αρχείο κειμένου πχ που δεν είναι κείμενο αλλά τα control words. Άλλος τρόπος είναι η επισύναψη και αποστολή των κλειδιών μαζί με τις πληροφορίες teletext σε δορυφορικά κανάλια διαφημίσεων ή τηλεγνωριμιών. Εννοείται ότι οι δέκτες που χρησιμοποιούν αυτό το δίκτυο πρέπει να είναι δέκτες της εταιρίας που αποστέλλει τα control words αφού μονό αυτοί έχουν το κατάλληλο λογισμικό για να εξάγουν τα control words από το δεύτερο tuner.

Τα αντιμετρά που παίρνουν οι πάροχοι σε αυτά τα φαινόμενα είναι σε πρώτο στάδιο η μείωση όσο γίνεται του χρόνου αλλαγής του control word ανά κανάλι. Μεγάλη μείωση όμως προκαλεί προβλήματα σε πολλούς νόμιμους χρήστες οι οποίοι αν και διαθέτουν επίσημη συνδρομητική κάρτα αδυνατούν ο δέκτες τους να ακολουθήσουν τον γρήγορο ρυθμό αλλαγής των control words. Επιπλέον αύξηση αποστολής ECM προκαλεί μείωση αριθμού των EMM κάτι πάλι που δυσκολεύει την ευελιξία του παροχου.

Επίσης αξίζει να αναφερθεί ότι όλα τα πειρατικα μοντέλα ισχύουν και για DVB-T εκπομπή (επίγεια ψηφιακή) ή DVB-C εκπομπή(καλωδιακή) αφού οι κρυπτογραφήσεις και εκεί ακολουθούν την ιδία τακτική και σχεδίαση με το DVB-S. Το φαινόμενο του card-sharing σε DVB-T αναφέρεται ότι γίνεται στη Κύπρο στο συνδρομητικό πάροχο που χρησιμοποιεί DVB-T εκπομπή.

5.3.4 Μέτρα κατά του Card Sharing

Το ένα μέτρο που αναφέραμε είναι το ‘’Surf Locking’’ της Irdeto με το οποίο η κάρτα κλειδώνει αν υπάρχει συνεχόμενη αλλαγή καναλιού. Ενώ το άμεσα εφαρμόσιμο από την νόβα μέτρο είναι το πάντρεμα του δορυφορικού δέκτη με τη δορυφορική κάρτα. Σύμφωνα με αυτό κάθε κάρτα απαντά σε ερωτήσεις ECM μόνο από ένα δορυφορικό δεκτή που έχει κατοχυρωθεί να συνεργάζεται. Το λεγόμενο πάντρεμα δεν επιτρέπει τη λειτουργία της κάρτας σε άλλο δορυφορικό δέκτη έτσι άμα μπει μέσα σε δίκτυο και ρωτηθεί με ECM από άλλους δέκτες δε θα αποκριθεί με το CW.Η δε εξαγωγή του CW είναι θεωρητικά αδύνατη αφού χρησιμοποιείται η τεχνολογία Secure Silicon. Βάσει αυτής της τεχνολογίας τα CW κρυπτογραφούνται κατά τη διάρκεια κρυπτογράφησης και αποκρυπτογραφούνται μόνο από ειδικό επεξεργαστή που ευρίσκεται στο συγκεκριμένο δέκτη Το μέτρο άρχισε και στην Ελλάδα να εμφανίζεται αλλά θα απαιτηθεί καιρός και χρήμα μέχρι να αλλαχτούν όλες οι κάρτες. Το μέτρο είναι καινούργιο και η ανθεκτικότητα του θα κριθεί σε βάθος χρόνου.

5.4 Βιβλιογραφία

Attacks on Pay-TV Access Control Systems
Markus G. Kuhn

Countermeasures for Attacks on Satellite TV Cards using Open Receivers:
Lishoy Francis, William G. Sirett, Keith Mayes, Konstantinos Markantonakis

Inhibiting Card Sharing Attacks:
Michael Tunstall, Konstantinos Markantonakis, and Keith Mayes

Enhancing the Conditional Access Module Security in Light of Smart Card Sharing Attacks:
Konstantinos Markantonakis, Michael Tunstall, Keith Mayes

Περιοδικο ''Δορυφορικά Νεα'' τεύχος Μαιος 2007
Περιοδικο ''Δορυφορικά Νεα'' τεύχος Μαρτιος 2007
Περιοδικο ''Δορυφορικά Νεα'' τεύχος Μαρτιος 2008
Περιοδικο ''Δορυφορικά Νεα'' τεύχος Φεβρουάριος 2008
Περιοδικο ''Δορυφορικά Νεα'' τεύχος Ιουλιος 2008
Περιοδικο ''Satellite Home'' τεύχος 1

www.zotos.biz
www.wikipedia.com
www.cardsharing.biz
www.cardserver.org
www.eurocardsharing.com
www.cardsharingforum.com/
και άλλα ....

ΚΕΦΑΛΑΙΟ 6 : Πειρατεία με κλωνοποίηση έξυπνης κάρτας

Στο κεφάλαιο 4 αναπτύξαμε το μοντέλο κρυπτογράφησης αποκρυπτογράφησης σύμφωνα με το οποίο πραγματοποιούνται κρυπτογραφήσεις και αποκρυπτογραφήσεις κλειδιών για τη διασφάλιση της πρόσβασης στο οπτικοακουστικό υλικό μόνο στους χρήστες που είναι εγκεκριμένοι από τον πάροχο. Στο στάδιο κρυπτογράφησης όλες οι διεργασίες γίνονται σε ασφαλές χώρο (γραφεία παρόχου) με έλεγχο πρόσβασης στο χώρο αυτό. Στη δε αποκρυπτογράφηση όμως που γίνεται στο δορυφορικό δεκτή του πελάτη, υπάρχει πλήρης πρόσβαση στον εξοπλισμό από τους επίδοξους πειρατές. Έτσι το σύστημα αποκρυπτογράφησης μαζί με τα κλειδιά πρέπει να φυλάσσεται κατά το δυνατό καλύτερο τρόπο. Γι'αυτό το λόγο χρησιμοποιούνται οι έξυπνες κάρτες (smart card) οι όποιες αποθηκεύουν τα κλειδιά και ταυτόχρονα κάνουν τις ενδιάμεσες αποκρυπτογραφήσεις δίνοντας το τελικό CW πίσω στο δέκτη για πλήρη αποκρυπτογράφηση μέσω του CSA. Οι έξυπνες κάρτες αποτελούν την αιχμή της τεχνολογίας ολοκληρωμένων τόσο στον τομέα ασφάλειας όσο και στον τομέα τεχνολογίας.

6.1 Εισαγωγή-Ιστορική αναδρομή

Με απλούς όρους, η έξυπνη κάρτα είναι ένας μικροσκοπικός υπολογιστής με πολύ σημαντικές δυνατότητες τοποθετημένος σε πλαστική κάρτα. Ο μικροσκοπικός αυτός υπολογιστής, αλλιώς καλούμενος μικροτσίπ, είναι ένα ολοκληρωμένο κύκλωμα με ηλεκτρικές επαφές ή με δυνατότητες ασύρματης επικοινωνίας που συνδυαζόμενος με την κατάλληλη συσκευή υποδοχής καρτών έχει τη δυνατότητα αποθήκευσης και μεταφοράς χιλιάδων bits πληροφορίας καθώς και επεξεργασίας αυτών των δεδομένων για την εξυπηρέτηση ποικίλων εφαρμογών. Κύρια χαρακτηριστικά των έξυπνων καρτών είναι ότι παρέχουν ασφάλεια δεδομένων και συνδιαλλαγών, ταχύτητα και ευκολία χρήσης καθώς επίσης αντοχή στην καταπόνηση και κακή χρήση με μεγάλο διάστημα "ζωής".

Θα μπορούσαμε να πούμε ότι οι έξυπνες κάρτες είναι το αποτέλεσμα της ταυτόχρονης βελτίωσης των μαγνητικών πλαστικών καρτών και των microchip. Το 1968 οι Jurgen Dethloff και τον Helmut Grotrupp στη Γερμανία δημοσιεύουν πατέντα για ενσωμάτωση μικροκυκλώματος σε πλαστικές κάρτες. Το 1969 παρουσιάζεται στη Γαλλία, από τον δημοσιογράφο Roland Moreno, μία ιδέα για μία κάρτα με ενσωματωμένο κύκλωμα. Ενώ το 1970 στην Ιαπωνία ο Kunitaka Arimura καταθέτει πατέντα και αυτός για ενσωματωμένο chip (ολοκληρωμένο) σε πλαστικές κάρτες. Το 1970 η μικροηλεκτρονική προοδεύει αρκετά ώστε να δημιουργήσει εργαστηριακά ολοκληρωμένα κυκλώματα που ενσωματώνουν μνήμη και επεξεργαστή. Έτσι οι θεωρητικές εργασίες άρχισαν να τυχαίνουν τις πρώτες εργαστηριακές δόκιμες. Ήταν όμως το 1974 χρονιά που ο Γάλλος Roland Monero κατάθεσε την πατέντα των έξυπνων καρτών στη Γαλλία και υπήρξε εκεί πραγματική ανάπτυξη της τεχνολογίας αυτής. Τη δεκαετία του '70 Γαλλία και Γερμανία σαν πρωτοστάτες της τεχνολογίας ανάλαβαν τόσο την εξέλιξη των έξυπνων καρτών όσο και τη διάδοση τους αρχίζοντας τις πρώτες εμπορικές εφαρμογές τη δεκαετία του '80 (τηλεφωνικούς θαλάμους, κινητές τηλεπικοινωνίες, τράπεζες κ. α.).

Η πρώτη έξυπνη κάρτα κατασκευάστηκε τελικά το 1977 από την Motorola και την Bull ενώ συγχρόνως 3 εμπορικοί κατασκευαστές, η Bull, η SGS Thomson και η Schlumberger ξεκίνησαν να αναπτύσσουν εφαρμογές πάνω στη νέα τεχνολογία. Η πρώτη αυτή κάρτα περιείχε δύο μικροτσίπ, δηλαδή ένα μικροελεγκτή και μία ξεχωριστή συσκευή μνήμης. Το

1984 η ένωση γαλλικών ταχυδρομείων και τηλεπικοινωνιών (Frence PPT) αρχίζουν εκτεταμένες δοκιμές έξυπνων καρτών για δημόσιους τηλεφωνικούς θαλάμους. Οι τηλεκάρτες αυτές ενθουσιάζουν και κερδίζουν τον κόσμο. Τον επόμενο χρόνο (1985) οι Γερμανοί κάνουν και αυτοί δοκιμές για την επομένη γενιάς τηλεκάρτα για τηλεφωνικούς θαλάμους και αναδεικνύουν την τηλεκάρτα με μικροκύκλωμα την καλύτερη μεταξύ των μαγνητικών και καρτών ολογράμματος. Τα πειράματα για τηλεκάρτες με chip συνεχίζονται αμείωτα και το 1986 αφού λύνονται τεχνολογικά και κατασκευαστικά εμπόδια, κυκλοφορούν για χρήση οι πρώτες τηλεκάρτες αριθμώντας εκατομμύρια κομμάτια. Το 1990 αριθμούν τα 60.000.000 κομμάτια και το 1997 σχεδόν μισό δισεκατομμύριο τηλεκάρτες.

Η Γερμανία εμφανίζει παρόμοια νούμερα με διαφορά όμως τρία χρόνια πιο αργά λόγω κυρίως τη χρησιμοποίησης της πιο εξελιγμένης και ακριβής μνήμη EEPROM* σε σχέση με την ERROM που χρησιμοποίησαν οι Γάλλοι. Η πρώτη δεν απαιτεί εξωτερική τάση προγραμματισμού και είναι επανεγγράψιμη. Έτσι οι δύο χώρες σέρνουν πρώτες το χορό της ενσωμάτωσης των έξυπνων καρτών στους δημοσίους τηλεφωνικούς θαλάμους πουλώντας και προωθώντας αυτή τη τεχνολογία και σε άλλες χώρες.

Στις κινητές τηλεπικοινωνίες τώρα πρωτοπόρησαν οι Γερμανοί με την εταιρία C-Netz που εφάρμοσε τις έξυπνες κάρτες στα αναλογικά κινητά λόγω κυρίως ότι οι μαγνητικές κάρτες που χρησιμοποιούσε τότε δεν ήταν απόλυτα ασφαλείς. Επειδή όμως το αναλογικό σύστημα κινητών κατασκευαστικά δεν μπορούσε να εξυπηρετήσει μεγάλη αγορά (λόγω έλλειψης συχνοτήτων στη Γερμανία μόλις 1.000.000 χρήστες μπορούσαν να υπάρχουν) δεν υπήρξε μαζική παραγωγή. Τη τεχνολογία και τεχνογνωσία όμως αυτή εκμεταλλεύτηκε το ευρωπαϊκό σύστημα κινητών ψηφιακής τεχνολογίας GSM και εφάρμοσε τις έξυπνες κάρτες στα κινητά (κάρτες SIM) με αποτέλεσμα σήμερα να υπάρχουν σχεδόν ένα δισεκατομμύριο χρήστες σε 180 χώρες.

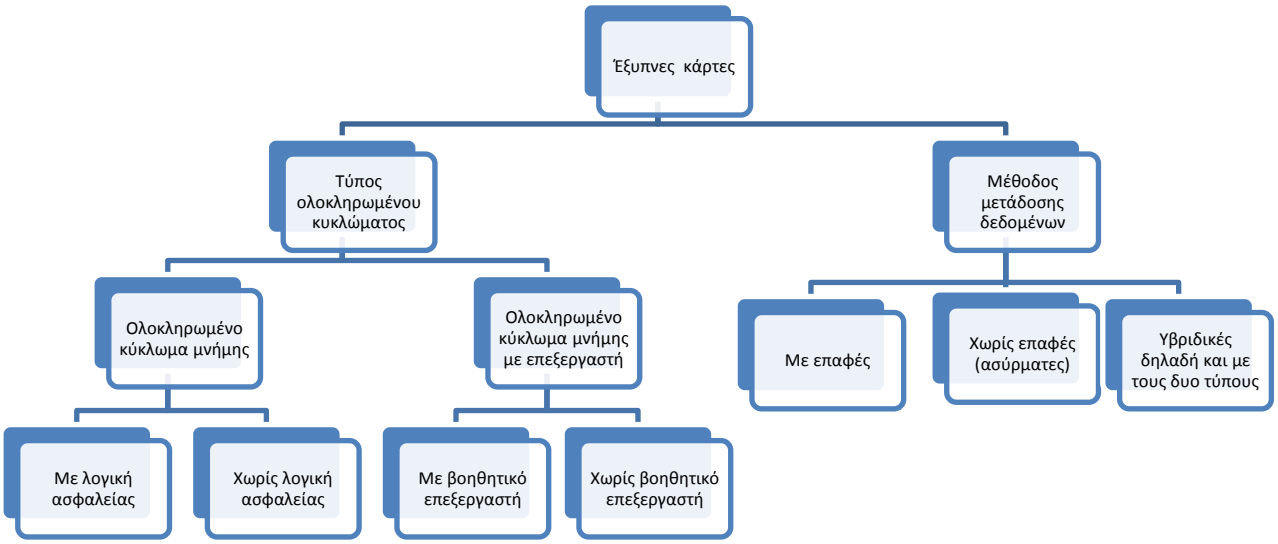
Στον τραπεζικό τομέα τώρα αν και η φορητότητα-ευχρηστία των έξυπνων καρτών αποτελούσαν τέλειο μέσο συναλλαγών άργησαν να ενταθούν στον τραπεζικό σύστημα. Αυτό οφείλεται κυρίως στην αυξημένη ασφάλεια που απαιτείται να έχουν οι έξυπνες κάρτες για αυτές τις εφαρμογές. Η ανάπτυξη όμως της μοντέρνας κρυπτογραφίας σε συνδυασμό με την ανάπτυξη ημιαγωγών και μικροηλεκτρονικής βοήθησε την ενσωμάτωση τελικά των έξυπνων καρτών και στις τραπεζικές συναλλαγές. Οι Γαλλικές τράπεζες το 1982-1983 κάνουν τις πρώτες δόκιμες σε τραπεζικές συναλλαγές με 60.000 έξυπνες κάρτες, με το εγχείρημα να στέφεται με επιτυχία. Έτσι το 1984 παρουσιάζεται και επίσημα για χρήση στη Γαλλία. Μέσα σε 10 χρόνια όλες οι τράπεζες υιοθετούν την τεχνολογία έξυπνων καρτών στις συναλλαγές τους και το γαλλικό χρηματοπιστωτικό σύστημα περνά σε άλλο επίπεδο. Πάρα την ενσωμάτωση των έξυπνων καρτών στα κινητά τηλεφωνά, μόλις το 1996 εμφανίζονται στη Γερμάνια οι έξυπνες κάρτες στις τράπεζες, ενώ σε μόλις ένα χρόνο (το 1997) όλες οι τράπεζες ενθουσιάζονται προσφέροντας στους πελάτες τους συναλλαγές με αυτές.

*EEPROM

Η EEPROM (Electrically Erasable Programmable Read-Only Memory) είναι μνήμη ROM που μπορεί να μεταβληθεί από τον χρήστη, δηλαδή μπορεί να σβηστεί και να επαναπρογραμματιστεί με την εφαρμογή υψηλότερης από την κανονική τάσης. Το κύριο χαρακτηριστικό της είναι ότι δεν μπορεί να σβηστεί και να προγραμματιστεί σε κομμάτια αλλά μόνο στην ολότητά της, και αυτό μπορεί να γίνει χωρίς να μετακινηθεί από τον υπολογιστή. Έχει περιορισμένη διάρκεια ζωής αφού επιτρέπει περιορισμένο αριθμό επαναπρογραμματισμών ο οποίος φτάνει σε δεκάδες ή εκατοντάδες χιλιάδες φορές.

Αξιοσημείωτη αναφορά, στον τομέα τραπεζικών συναλλαγών, είναι το έτος 1994 οπού οι Europay, MasterCard και Visa ενώνονται και παρουσιάζουν το πρότυπο EMV που απευθύνεται σε πιστωτικές κάρτες που κατακλύζουν μέχρι σήμερα την αγορά.
Η ενσωμάτωση των έξυπνων καρτών σε αυτούς τους τομείς (τηλεπικοινωνίες, τράπεζες, κινητά), το μικρό κόστος τους, η μεγάλη ασφάλεια και η φορητότητα τους, έχει σαν αποτέλεσμα τη χρησιμοποίηση τους σε όλους σχεδόν τους τομείς της καθημερινότητας μας. Οι έξυπνες κάρτες σήμερα χρησιμοποιούνται στις δημοσιές συγκοινωνίες, στα νοσοκομεία για καταγραφή ιατρικών στοιχείων, στις ταυτότητες, εκλογικά βιβλιάρια, άδειες οδηγού, πρόσβαση σε χώρους ή υπηρεσίες (πχ φωτοτυπίες) και οπού γενικά απαιτείται έλεγχος αυθεντικότητας. Ασφαλώς και οι δορυφορικές συνδρομητικές υπηρεσίες δε θα μπορούσαν να μην υιοθετήσουν τη χρήση έξυπνων καρτών στα συστήματα πρόσβασης ώστε να αποτελούν τη δικλίδα ασφάλειας για την παροχή υπηρεσιών μονό στους εγκεκριμένους χρήστες.

6.2 Κατηγορίες έξυπνων καρτών :



Σχήμα 1: Κατηγορίες έξυπνων καρτών

Βάσει του διαγράμματος οι σημερινές έξυπνες κάρτες χωρίζονται ανάλογα με τον τύπο ολοκληρωμένου σε δύο κατηγορίες ενώ ανάλογα, με τον τύπο διασύνδεσης με το τερματικό, σε τρεις .

6.2.1 Τύπος ολοκληρωμένου κυκλώματος

Με το πρώτο κριτήριο, διακρίνουμε δύο κατηγορίες έξυπνων καρτών:

- **Κάρτες μνήμης** – κάρτες αποθήκευσης πληροφοριών (memory cards) . Οι κάρτες αυτές περιέχουν ολοκληρωμένο κύκλωμα μνήμης και λογική σε υλικό (hardware logic), η οποία μπορεί να θέσει ή να διαγράψει τιμές στη μνήμη. Διαθέτουν δύο υποκατηγορίες οι κάρτες που διαθέτουν λογική ασφάλειας και αυτές που δεν έχουν.
- Έξυπνες κάρτες με κύκλωμα μικροεπεξεργαστή. Ο επεξεργαστής τους, πέρα από την αποθήκευση και ασφάλιση πληροφοριών, μπορεί να λαμβάνει αποφάσεις που ορίζονται στις προδιαγραφές του έργου για το οποίο θα χρησιμοποιηθούν. Διαθέτουν και αυτές δύο υποκατηγορίες αυτές που έχουν βοηθητικό επεξεργαστή και αυτές που στερούνται αυτό το δεύτερο επεξεργαστή.

6.2.2 Μέθοδος μετάδοσης δεδομένων

Με βάση το δεύτερο κριτήριο, διακρίνουμε τρεις κατηγορίες έξυπνων καρτών:

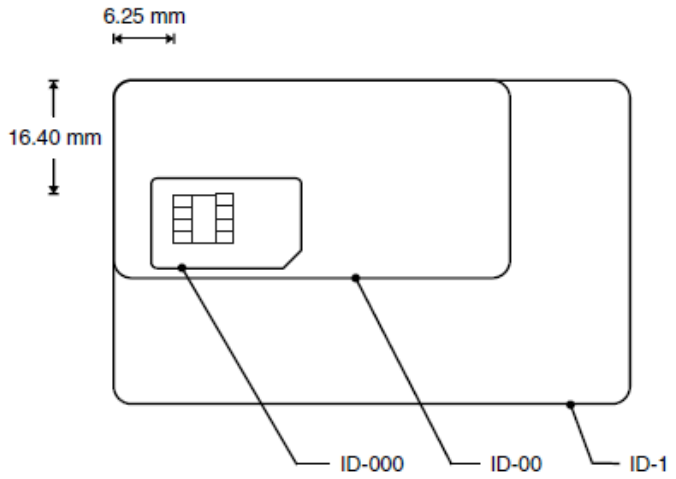
- Έξυπνες κάρτες με επαφές (Contact Cards). Οι κάρτες αυτές επικοινωνούν με ηλεκτρικές επαφές και πρέπει να εισαχθούν σε μία συσκευή ανάγνωσης προκειμένου να διαβαστούν ή να εισαχθούν πληροφορίες.

- Ασύρματες έξυπνες κάρτες (Contactless Cards). Οι κάρτες αυτές έχουν ενσωματωμένη εσωτερικά μικροσκοπική κεραία και μπορούν να επικοινωνούν με κεραία λήψης χωρίς τη φυσική τους επαφή με κάποια συσκευή ανάγνωσης προκειμένου οι πληροφορίες να ανανεωθούν,- να αλλάξουν ή να υποβληθούν σε επεξεργασία.

- Υβριδικές κάρτες και συνδυασμένες κάρτες (Hybrid και Combination Cards). Οι κάρτες αυτές ενσωματώνουν και τους δύο τρόπους μετάδοσης και συνεπώς μπορούν να επικοινωνήσουν κατά περίπτωση είτε με ενσύρματο είτε με ασύρματο τρόπο.

6.3 Χαρακτηριστικά έξυπνων καρτών

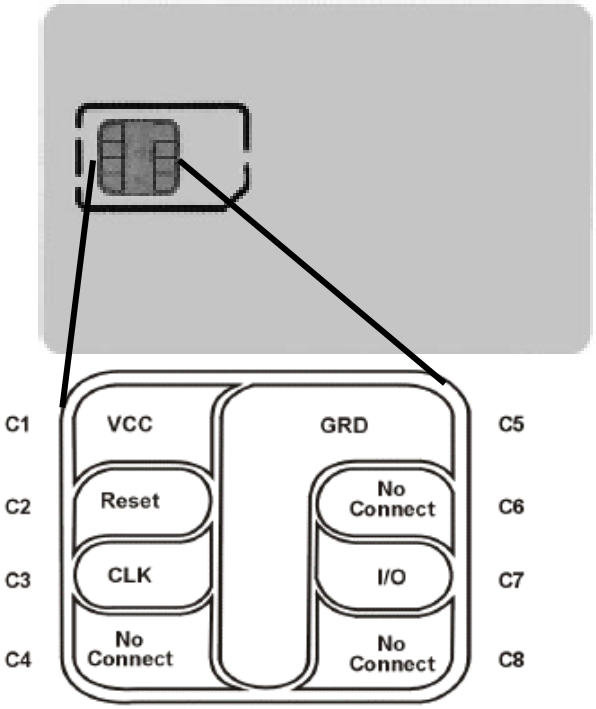
Οι διαστάσεις των έξυπνων καρτών ορίζονται στο ISO 7810. Οι δύο κύριες είναι η ID-1 που είναι το μέγεθος των πιστωτικών καρτών και το ID-000 που είναι το μέγεθος της κάρτες SIM που χρησιμοποιείται στα κινητά. Η μορφή ID-1 έχει πλάτος 85, 6 mm, ύψος 54 mm, ακτίνα γωνίας 3, 18 ± 0, 30 mm και πάχος 0, 76 ± 0, 08 mm. Οι τηλεφωνικές συσκευές GSM απαιτούν έξυπνες κάρτες μικρότερου μεγέθους έτσι οι διαστάσεις της ID-000 είναι: πλάτος 25 mm, ύψος 15 mm, ακτίνα γωνίας 1 ± 0, 10 mm και πάχος 0, 76 ± 0, 08 mm. Η κάτω δεξιά γωνία της κάρτας είναι κομμένη σε γωνία 45° και έτσι υποδεικνύει τον σωστό τρόπο εισαγωγής της κάρτας. Τέλος, η μορφή ID-00 βρίσκεται, από άποψη μεγέθους, μεταξύ των ID-1 και ID-000. Έχει πλάτος 66 mm, ύψος 33 mm, ακτίνα γωνίας 3, 18 ± 0, 30 mm και πάχος 0, 76 ± 0, 08 mm.



Σχήμα 2:Τα διαφορετικά μεγέθη έξυπνων καρτών

Στα συστήματα ελεγχόμενης πρόσβασης (CAS) των δορυφορικών επικοινωνιών χρησιμοποιούνται οι έξυπνες κάρτες με επαφές με επεξεργαστή, ο όποιος διαθέτει και μικροεπεξεργαστή. Η ανάταξη των επεξεργαστών τα τελευταία χρόνια όμως έχει κάνει ικανή την ύπαρξη και μονό επεξεργαστή κάνοντας τον μικροεπεξεργαστή περιττό. Είναι συνήθως μεγέθους ID-1 αλλά υπάρχουν και υλοποιήσεις σε ID-000.

Οι επαφές των έξυπνων καρτών καθορίζονται από το πρότυπο ISO-7812, βάσει του οποίου οι επαφές κατανέμονται όπως φαίνονται στο σχήμα 3.



C1	Vcc	Τροφοδοσία, από 3 έως 5 Volt
C2	RST	Είσοδος επαναφοράς (Reset Input)
C3	CLK	Είσοδος ρολογιού (Clock input)
C4		Δεσμευμένη για μελλοντική χρήση
C5	GND	Γείωση (Ground)
C6	Vpp	Τάση προγραμματισμού (δεν χρησιμοποιείται πια) . Σε παλαιότερες κάρτες προγραμμάτιζε τη μνήμη EEPR0M.
C7	I/O	Σειριακή είσοδος/έξοδος
C8		Δεσμευμένη για μελλοντική χρήση

Σχήμα 3: Οι επαφές των έξυπνων καρτών

Σύμφωνα με την προδιαγραφή ISO/IEC 7816, οι έξυπνες κάρτες έχουν οκτώ ηλεκτρικές επαφές C1 έως C8 με τη C6 να μην χρησιμοποιείται πλέον. Ενώ η C4 και C8 ορίζονται σαν AUX1, AUX2 (βοηθητικές) για μελλοντικές χρήσης (όπως αμφίδρομη επικοινωνία με USB interface).

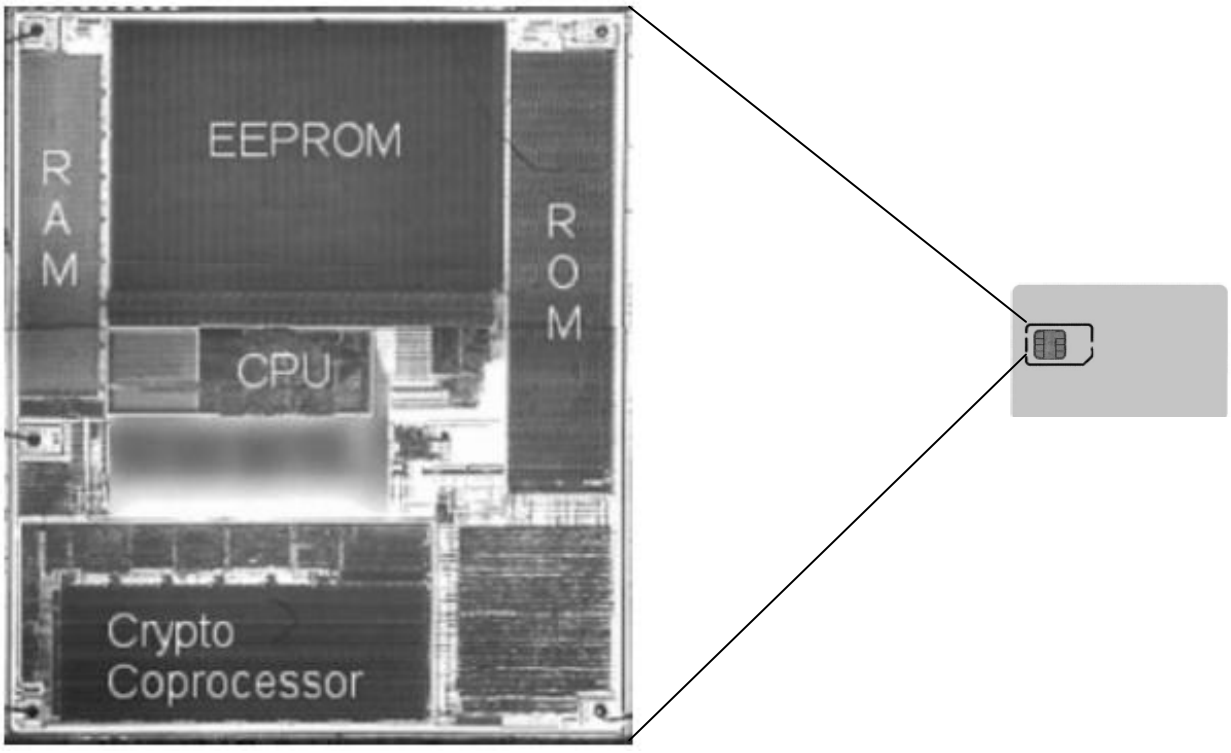
6.3.1 Επικοινωνία με τον εξωτερικό κόσμο

Η επικοινωνία μεταξύ έξυπνης κάρτας και συσκευής ανάγνωσης γίνεται από μία και μοναδική επαφή (C7). Εξαιτίας αυτού του περιορισμού, η επικοινωνία είναι μονόδρομη (half-duplex), δηλαδή κάρτα και συσκευή ανάγνωσης χρησιμοποιούν εναλλάξ τη γραμμή εισόδου/εξόδου για την αποστολή δεδομένων. Η επικοινωνία ξεκινάει πάντοτε με αίτηση της συσκευής ανάγνωσης και η κάρτα απαντά στις αιτήσεις αυτές. Η κάρτα δεν στέλνει ποτέ δεδομένα, αν δεν έχουν ζητηθεί από τη συσκευή ανάγνωσης. Συνεπώς, η σχέση μεταξύ κάρτας και συσκευής ανάγνωσης είναι σχέση master-slave, με τη συσκευή ανάγνωσης να είναι ανώτερη ιεραρχικά. Η κάρτα κατά την είσοδο της στη συσκευή ανάγνωσης λαμβάνει την εντολή «Ενεργοποίηση και Λειτουργία εξ αρχής» (PR = Power and Reset) και απαντά με το σήμα «Έναρξης Λειτουργίας» (ATR = Answer to Reset) στη συσκευή ανάγνωσης. Το σήμα ATR περιέχει πληροφορίες σχετικά με τα στοιχεία της κάρτας και το πρωτόκολλο μετάδοσης. Η συσκευή ανάγνωσης «προσαρμόζεται» στις παραμέτρους και στέλνει την πρώτη εντολή. Η κάρτα επεξεργάζεται την εντολή και δίνει την κατάλληλη απάντηση στη

συσκευή ανάγνωσης. Αυτός ο τρόπος λειτουργίας συνεχίζεται μέχρι την ολοκλήρωση της διαδικασίας.
Υπάρχει μια οικογένεια από διαφορετικά πρωτόκολλα για την ανταλλαγή δεδομένων κατά τη διάρκεια της επικοινωνίας. Τα πιο κοινά πρωτόκολλα για τις κάρτες με επαφές και μικροεπεξεργαστή είναι το T=0 (Ασύγχρονη, half-duplex, ανά byte επικοινωνία) και το T=1 (Ασύγχρονη, half-duplex, ανά block επικοινωνία).

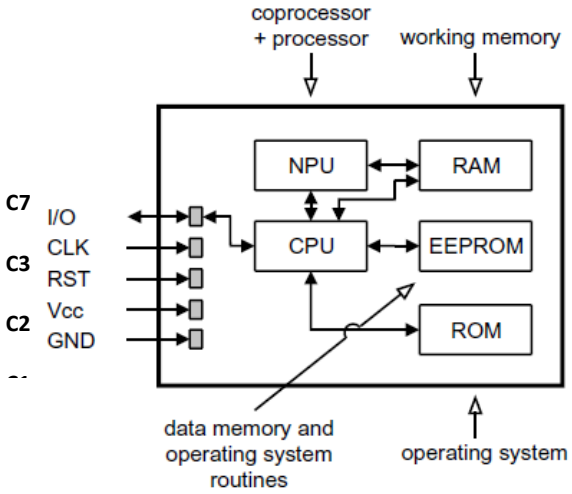
Μπορούμε να πούμε ότι το T=0 είναι το παλαιότερο εκ των δύο πρωτοκόλλων. Η SIM κάρτα του GSM είναι η σημαντικότερη εφαρμογή αυτού του πρωτοκόλλου. Το σημαντικό του πλεονέκτημα είναι ότι είναι απλό και οι υλοποιήσεις του πολύ αποδοτικές σε θέματα χωρητικότητας. Το τίμημα αυτών των πλεονεκτημάτων είναι η ανεπαρκής διαφοροποίηση του στρώματος μεταφοράς από το ανώτερο στρώμα. Για την εξαγωγή δεδομένων από την κάρτα είναι απαραίτητο να γίνουν δύο ανταλλαγές εντολών. Στον πρώτο κύκλο εντολών ο host στέλνει την εντολή και η έξυπνη κάρτα επιστέφει το μήκος της απάντησης που θα ακολουθήσει. Στον δεύτερο κύκλο εντολών ο host ζητάει τον αναμενόμενο αριθμό των bytes της απάντησης και η κάρτα του τα στέλνει.
Στο T=1 πρωτόκολλο ο host μπορεί να στείλει μια εντολή και να λάβει απάντηση αμέσως. Επίσης, το πρωτόκολλο αυτό διαφοροποιεί πλήρως το επίπεδο εφαρμογής από το επίπεδο μεταφοράς και είναι κατάλληλο για ασφαλή αποστολή μηνυμάτων μεταξύ του host και της κάρτας.

6.3.2 Μέρη ολοκληρωμένου Έξυπνης κάρτας:



Σχήμα 4: Τα επιμέρους συστήματα του μικροτσίπ της έξυπνης κάρτας σε μεγεθυμένη φωτογραφία (Φώτο: Infineon Technologies)

Το τσιπάκι με διαστάσεις 5x5 χιλιοστά του μέτρου, που βρίσκεται πάνω στην έξυπνη κάρτα περιλαμβάνει ένα ολόκληρο ηλεκτρονικό υπολογιστή σε σμίκρυνση. Διαθέτει επεξεργαστή (CPU), προσπελάσιμη μνήμη (RAM), μόνιμη μνήμη (ROM), ελεγχόμενη επανεγγράψιμη μνήμη (EEPROM) και τα κατάλληλα κυκλώματα ελέγχου και επικοινωνίας με τον εξωτερικό κόσμο (Control Logic). Η διαδικασία κατασκευής του αν και με απλή με τα σημερινά δεδομένα εν τούτοις απαιτεί εξειδικευμένη υποδομή και προχωρημένη τεχνολογία. Η σύνθεση του ολοκληρωμένου φαίνεται πάνω στο σχήμα 4 ενώ η λειτουργία κάθε ενός σταδίου απεικονίζεται κάτω στο σχήμα 5 και εξηγείται πιο κάτω.



Σχήμα 5: Τα επιμέρους συστήματα του μικροτσίπ της έξυπνης κάρτας

6.3.2.1 RAM

RAM (Random Access Memory - Μνήμη Τυχαίας Προσπέλασης) είναι μνήμη που περιέχεται σε ένα ή περισσότερα μικροτσίπ κοντά στον μικροεπεξεργαστή, έχει μικρό φυσικό μέγεθος και μικρή γενικά χωρητικότητα σε σχέση με άλλα αποθηκευτικά μέσα. Είναι όμως πολύ γρήγορη και υπάρχει άμεση πρόσβαση στα δεδομένα της, ενώ οι διαδικασίες ανάγνωσης και εγγραφής γίνονται τάχιστα (χρόνος πρόσβασης σε τάξη nanoseconds). Τα όποια δεδομένα και στοιχεία συστήματος αποθηκεύονται στη RAM, βρίσκονται εκεί μόνο όσο ο μίκρο-υπολογιστής λειτουργεί και χάνονται όταν το ρεύμα αφαιρεθεί. Ο όρος “τυχαία προσπέλαση” αναφέρεται στο ότι η πρόσβαση σε αποθηκευμένη πληροφορία δεν γίνεται ακολουθιακά αλλά άμεσα.

6.3.2.2 ROM

Η ROM (Read Only Memory - Μνήμη Μόνο Ανάγνωσης) είναι μνήμη στην οποία δεν μπορούν να γίνουν εγγραφές, αλλά μόνο ανάγνωση. Η ROM περιέχει τα στοιχεία προγραμματισμού (στην ουσία το λειτουργικό) που επιτρέπουν σε ένα υπολογιστή να ξεκινήσει και δεν χάνει τα δεδομένα της όταν ο υπολογιστής κλείσει.

6.3.2.3 EEPROM

Η EEPROM (Electrically Erasable Programmable Read-Only Memory) είναι μνήμη ROM που μπορεί να μεταβληθεί από τον χρήστη, δηλαδή μπορεί να σβηστεί και να επαναπρογραμματιστεί με την εφαρμογή υψηλότερης από την κανονική τάσης. Το κύριο χαρακτηριστικό της είναι ότι δεν μπορεί να σβηστεί και να προγραμματιστεί σε κομμάτια αλλά μόνο στην ολότητά της, και αυτό μπορεί να γίνει χωρίς να μετακινηθεί από τον υπολογιστή. Έχει περιορισμένη διάρκεια ζωής αφού επιτρέπει περιορισμένο αριθμό

επαναπρογραμματισμών ο οποίος φτάνει σε δεκάδες ή εκατοντάδες χιλιάδες φορές. Εδώ γράφονται τα διάφορα προγράμματα που εκτελούνται από τη CPU (βάση του λειτουργικού της ROM) χρησιμοποιώντας ως άμεσο και προσπελάσιμο χώρο για τις ενδιάμεσες πράξεις τη μνήμη RAM.

6.3.2.4 Μικροεπεξεργαστής (CPU)

Ο μικροεπεξεργαστής είναι ένας επεξεργαστής υπολογιστή σε μικροτσίπ. Μερικές φορές καλείται "λογικό τσιπ". Είναι σχεδιασμένος για να εκτελεί αριθμητικές και λογικές διεργασίες που χρησιμοποιούν μικρές περιοχές καταγραφής αριθμών που καλούνται καταχωρητές. Τυπικές τέτοιες διεργασίες είναι η πρόσθεση, η αφαίρεση η σύγκριση δύο αριθμών ή η μεταφορά αριθμών από μία περιοχή σε άλλη. Αυτές οι διεργασίες είναι αποτέλεσμα ενός συνόλου εντολών που αποτελούν μέρος του σχεδιασμού του μικροεπεξεργαστή. Άρχισε να παράγεται σε 8-bit λειτουργία ενώ σήμερα έχει φτάσει τα 32-bit.

6.3.3 Λογισμικό Έξυπνων καρτών

Σαν μικροί υπολογιστές οι έξυπνες κάρτες διαθέτουν λογισμικό και προγράμματα για έλεγχο ασφάλεια και λειτουργία της κάρτας. Τα μέρη του λογισμικού είναι:

6.3.3.1 Λειτουργικό σύστημα

Αφού η έξυπνη κάρτα έχει δομή ηλεκτρονικού υπολογιστή, θα πρέπει να «ελέγχεται» και από κάποιο ενσωματωμένο λειτουργικό σύστημα. Είναι το ανάλογο των Windows και Linux στους υπολογιστές.

6.3.3.2 Εντολές

Μία εντολή είναι μία διαταγή που δίνεται σε ένα επεξεργαστή από ένα υπολογιστικό πρόγραμμα που βρίσκεται στην EEPROM. Στις έξυπνες κάρτες των δορυφορικών συστημάτων οι περισσότερες εντολές έχουν να κάνουν με ανταλλαγή και επεξεργασία κλειδιών χρησιμοποιώντας κρυπτογραφικούς αλγόριθμους που εξηγούνται πιο κάτω.

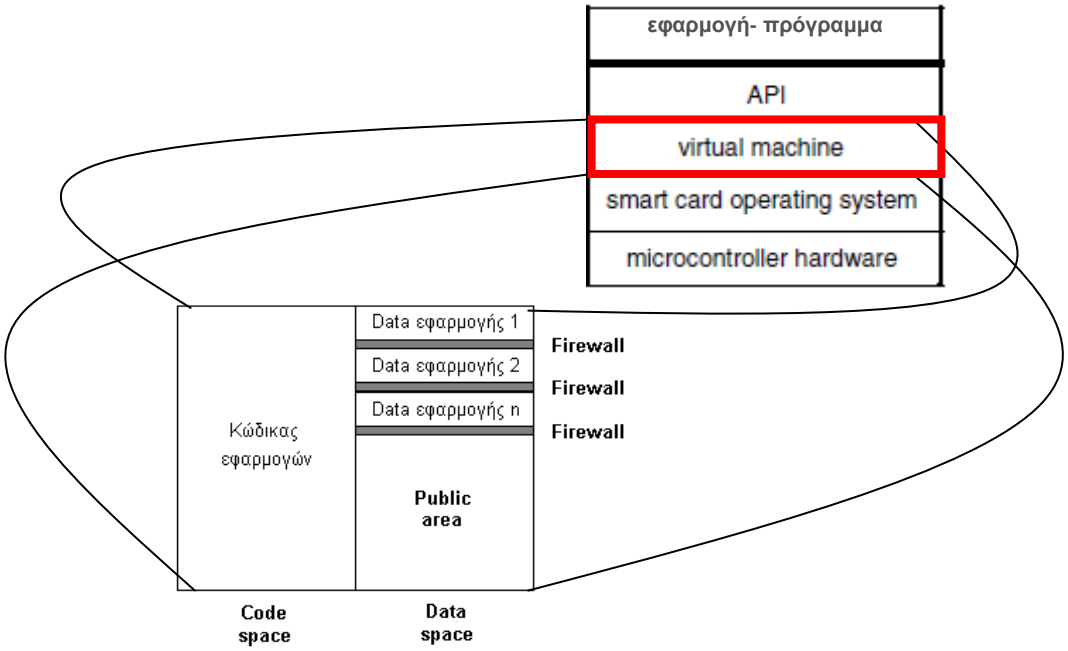
6.3.3.3 Application Programming Interface (API)

Το API ή στα ελληνικά διεπαφή προγραμματισμού εφαρμογών είναι λογισμικό το οποίο δρα σαν μεσάζων προγράμματος και λογισμικού. Στην ουσία διατυπώνει το σύνολο των λειτουργιών-υπηρεσιών που μπορεί να παρέχει το λειτουργικό σύστημα στα προγράμματα χωρίς να γίνεται κάποια αναφορά στον κώδικα που υλοποιεί αυτές τις υπηρεσίες(δηλαδή αποκρύπτει για ασφάλεια το λειτουργικό).

Για να γίνει εύκολα αντιληπτό αυτό, δίνεται το κλασσικό παράδειγμα για εξήγηση της API, αυτό του ταχυδρομείου. Το ταχυδρομείο παρέχει την υπηρεσία της αποστολής γραμμάτων. Η υπηρεσία αυτή αναφέρει τους κανόνες που θα ακολουθήσεις για να κάνεις το αίτημά σου (φορμάτ διεύθυνσης παραλαβής, γραμματόσημο, κ.λ.π.). Το πώς θα υλοποιηθεί αυτό σου το αίτημα είναι δουλειά ενός ολόκληρου μηχανισμού ανθρώπων και υλικού αθέατα στον χρήστη της υπηρεσίας. Δηλαδή στο παράδειγμα του ταχυδρομείου η διεπαφή είναι οι υπηρεσίες που παρέχει στους πελάτες και οι οποίες είναι γραμμένες συνήθως σε ένα φυλλάδιο. Το φυλλάδιο αυτό είναι η διεπαφή του ταχυδρομείου προς τους πελάτες.

6.3.3.4 Virtual Machine

Μια εικονική μηχανή είναι ένα απομονωμένο τμήμα λογισμικού που μπορεί να τρέξει το λειτουργικό σύστημα της κάρτας σαν ήταν ο κεντρικός επεξεργαστής(στην ουσία το προσομοιώνει-emulates). Η εξολοκλήρου κατασκευή της από λογισμικό δηλαδή (δεν περιέχει κανένα τμήμα υλικού) της προσφέρει διάφορα ευδιάκριτα πλεονεκτήματα. Αυτά είναι συμβατότητα, απομόνωση, φορητότητα, και ανεξαρτησία υλικού(hardware). Συγκεκριμένα για την απομόνωση δίνεται το σχήμα 6, που εξηγεί το διαχωρισμό των εφαρμογών μεταξύ τους. Κάθε εφαρμογή έχει τον ιδιωτικό της χώρο μνήμης, ο οποίος καθίσταται απροσπέλαστος για τις υπόλοιπες εφαρμογές, με χρήση firewalls. Δηλαδή οι εφαρμογές διαχωρίζονται και δεν υπάρχει πρόσβαση μεταξύ τους για ασφάλεια (σχήμα 6 virtual machine Multos OS).



Σχήμα 6: Τα επίπεδα του λογισμικού της έξυπνης κάρτας μαζί με μεγέθυνση της εικονικής μηχανής (virtual machine)

Οι κυρίαρχες υλοποιήσεις λογισμικού είναι η Java Card και η Multos.

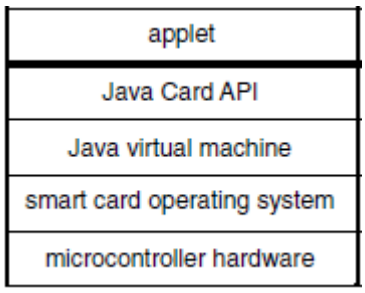
6.3.4 Multos

Η κοινοπραξία Multos δημιουργήθηκε το 1997 με στόχο τον ορισμό ενός προτύπου για έξυπνες κάρτες πολλαπλών εφαρμογών (multi-application smart cards) . Η συμμετοχή στην κοινοπραξία είναι ανοικτή σε όλους, όσοι είναι πρόθυμοι να καταβάλλουν την ετήσια συνδρομή. Το αποτέλεσμα του έργου της κοινοπραξίας ήταν η δημιουργία του Multos, του πρώτου ανοικτού, υψηλής ασφάλειας λειτουργικού συστήματος για έξυπνες κάρτες πολλαπλών εφαρμογών. Με το Multos, διαφορετικές ομάδες προγραμματιστών αναπτύσσουν εφαρμογές, οι οποίες μπορούν να συνυπάρχουν στην ίδια έξυπνη κάρτα, ανεξάρτητα και απομονωμένες μεταξύ τους με ασφάλεια.

Η Multos αποτελεί **Operating System** έξυπνης κάρτας. Η εικονική μηχανή (virtual machine) του Multos λέγεται Application Abstract Machine (AAM) και δεν «εμφανίζεται» ούτε στη διαδικασία της επικοινωνίας με τη μηχανή ανάγνωσης, ούτε εμπλέκεται στις εφαρμογές της κάρτας. Για λόγους ασφαλείας και μυστικότητας λειτουργεί απομονωμένα και «κρυφά».
Στη θέση του λειτουργικού συστήματος, όπως προαναφέραμε, εμφανίζεται μια διεπαφή API (Application Programming Interface) με όνομα MEL. Οι συναρτήσεις του Multos παρέχουν κρυπτογράφηση και αποκρυπτογράφηση DES, 3DES, RSA, SHA-1 hashing, γεννήτρια τυχαίων αριθμών και άλλα (θα εξηγηθούν κάτωθι στην κρυπτογραφία). Με την εικονική μηχανή του Multos, επιτυγχάνεται η φορητότητα (portability) των εφαρμογών μεταξύ καρτών με διαφορετικούς μικροεπεξεργαστές, αρκεί για κάθε επεξεργαστή να υπάρχει υλοποίηση Multos. Οι εφαρμογές γράφονται σε κάποια γλώσσα προγραμματισμού υψηλού επιπέδου (C, Java) και στη συνέχεια, με χρήση compiler, μετατρέπονται σε MEL (Multos Executable Language) byte code. Είναι επίσης δυνατή η συγγραφή εφαρμογών απευθείας σε MEL.

6.3.5 Java Card

Η δεύτερη μεγάλη υλοποίηση ακούει στο όνομα Java Card
Για τη δημιουργία εφαρμογών έξυπνων καρτών σε Java Card, δεν απαιτείται η γνώση των εντολών που υποστηρίζει το λειτουργικό σύστημα της κάρτας του κάθε κατασκευαστή. Γι'αυτό και η Java Card δεν αποτελεί λειτουργικό όπως σφαλμένα διατυπώνεται σε εργασίες και βιβλία, αλλά πλατφόρμα. Υπάρχουν λειτουργικά που δημιουργούνται για Java Card πλατφόρμα, η οποία αποτελείται μονό από τον API-Java Card και τη εικονική μηχανή Java Virtual Machine(δεν εμπεριέχεται δηλαδή και λειτουργικό στη JavaCard). Η Java Card είναι πρόταση της Sun Microsystems για προγραμματισμό σε έξυπνων καρτών. Οι εφαρμογές που είναι γραμμένες σε γλώσσα Java Card είναι κατάλληλες για υλοποίηση σε έξυπνες κάρτες αλλά και άλλες συσκευές με περιορισμένη δυνατότητα μνήμης και ισχύος. Τα βασικά συστατικά της μέρη φαίνονται στο σχήμα 7.Αυτα είναι οι εφαρμογές(applet), το API που είναι το Java Card API εδώ και η εικονική μηχανή η Java Virtual Machine. Αναφέρεται ότι και εδώ η εικονική μηχανή εφαρμόζει firewalls μεταξύ των applets (εφαρμογών) για περισσότερη ασφάλεια.



Σχήμα 7 : Τα στρώματα κάρτας με Java πλατφόρμα

Η Java Card διαθέτει λόγω Javas μεγάλη ευχρηστία ,ενώ η παραμετροποίηση της τυγχάνει ανάλογης ασφάλειας με τη Multos ή τη GlobalPlatform (που αναφέρεται πιο κάτω). Χρησιμοποιείται για καθημερινές εφαρμογές αλλά και τραπεζικές και εφαρμογές κινητής τηλεφωνίας.

6.3.6 GlobalPlatform

Σημαντικό μερίδιο αγοράς επίσης έχει και η πλατφόρμα GlobalPlatform η οποία αναπτύχθηκε αρχικά από τη Visa σαν Visa Open Platform και μετά εξελίχτηκε σε OpenPlatform όπου το 1999 πηρέ την τελική ονομασία GlobalPlatform. Σήμερα αποτελείται εκτός τη Visa και από 20 πλήρη μέλη, με ισχυρά ονόματα όπως της IBM, Hitachi, France Telecom, MasterCard και άλλες. Η πλατφόρμα γνωρίζει απήχηση στα GSM και στις εφαρμογές που μπορούν να φορτωθούν στις GSM κάρτες από τον πάροχο μέσω του δικτύου. Ενώ λόγω Visa έχει μεγάλο μερίδιο στις τραπεζικές συναλλαγές.
Η microsoft παρουσίασε τη δική της εκδοχή σε OS με το Windows for Smart cards (WfSC) και αν και επένδυσε πολλά λεφτά στη ανάπτυξη και προβολή του λειτουργικού της δεν έτυχε αποδοχής και εγκαταλείφτηκε. Τελικά δε γίνεται να είμαστε καλοί σε όλα.

6.3.7 Άλλες πλατφόρμες-λειτουργικά

Για να κλείσουμε την αναφορά των OS και πλατφορμών αναφέρουμε εντελώς πληροφοριακά την ύπαρξη των ‘’SmartCard.NET’’ και ‘’BasicCard’ (σε γλώσσα Basic) πλατφορμών. Ακόμη την αναμενόμενη έλευση του λειτουργικού Linux στις έξυπνες κάρτες αφού τόσο οι 32-bit μικροεπεξεργαστές όσο και η ανοιχτή κοινότητα υποστηρίζει αυτό το εγχείρημα.

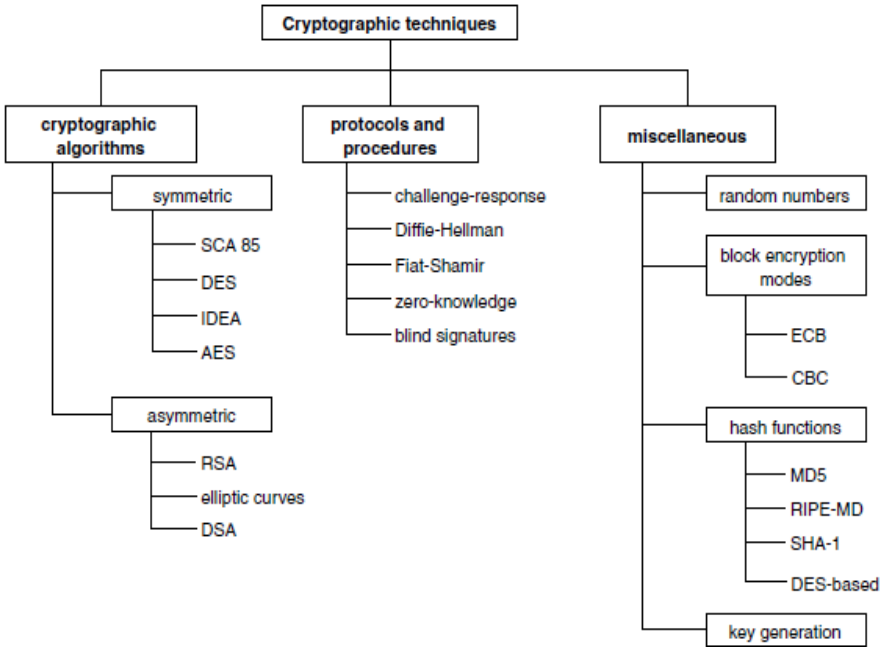
Τα operating systems και οι πλατφόρμες στις έξυπνες κάρτες δίνουν τον ίδιο αγώνα με τα ανάλογα OS των επιτραπέζιων υπολογιστών. Οι επενδύσεις που γίνονται στον τομέα είναι τεράστιες διότι και τα κέρδη είναι ανάλογα. Συμφώνα με τις προβλέψεις δε θα επιβιώσουν όλα, αλλά ποία θα εξαρτηθεί από το μέλλον.

6.4 Κρυπτογραφία

Οι έξυπνες κάρτες παρέχουν ως επί των πλείστων πρόσβαση σε Υπό Όρους Συστήματα (τραπεζικά, τηλεπικοινωνιακά, δορυφορικά κ.α.). Έτσι ο χρήστης πρέπει να πιστοποιεί στο σύστημα ότι είναι ο πραγματικός χρήστης και δικαιούται πρόσβαση σε αυτό.

Γι'αυτό το λόγο οι έξυπνες κάρτες χρησιμοποιούν στην πράξη τη θεωρία της κρυπτογραφίας. Όλες οι πληροφορίες κρυπτογραφούνται με κλειδιά που ευρίσκονται μόνο στην έξυπνη κάρτα του χρήστη και χρησιμεύουν για να αποκρυπτογραφούν τα εισερχόμενα μηνύματα από τον πάροχο στην κάρτα, αλλά και να κρυπτογραφούν τα μηνύματα από την κάρτα στον πάροχο.

Η πρώτη μέθοδος κρυπτογραφίας αναφέρεται στην εποχή των Σπαρτιατών με τη διάσημη μέθοδο της σκυτάλης. Από τότε τα πράγματα έχουν αλλάξει ριζικά, τα τεχνάσματα και οι έξυπνοι τρόποι έχουν αντικατασταθεί από αλγόριθμους που στηρίζονται σε άλυτα μαθηματικά προβλήματα ή σε συνδυασμούς που ούτε όλοι οι σημερινοί υπολογιστές μπορούν να υπολογίσουν. Μια σύνοψη των σημερινών αλγορίθμων και τεχνικών κρυπτογράφησης που χρησιμοποιούνται στις έξυπνες κάρτες δίνεται στο σχήμα 8 που ακολουθεί.



Σχήμα 8: Οι τεχνικές κρυπτογραφίας που εμφανίζονται και υποστηρίζονται από τους μικροεπεξεργαστές των έξυπνων καρτών

Από αυτές τις τεχνικές στεκόμαστε στους αλγορίθμους κρυπτογράφησης που αποτελούνται από τους συμμετρικούς και τους ασύμμετρους και στις συναρτήσεις hash.

6.4.1 Συμμετρικοί αλγόριθμοι

Οι συμμετρικοί αλγόριθμοι κρυπτογράφησης είναι η κλασική κρυπτογράφηση όπου κάθε μέλος του συστήματος διαθέτει το μυστικό κλειδί. Αν ο Α (πχ ο πάροχος) θέλει να στείλει ένα μήνυμα στο Β (συνδρομητής - έξυπνη κάρτα), κρυπτογραφεί το μήνυμα με το κοινό μυστικό κλειδί, ο Β λαμβάνει το σήμα και το αποκρυπτογραφεί με το ίδιο κλειδί μυστικό κλειδί που έχει και αυτός.

Τέτοιοι αλγόριθμοι όπως φαίνεται από το σχήμα 8 είναι ο DES, ο AES, ο IDEA ο SCA 85 και άλλοι. Οι πιο κύριοι είναι ο DES και ο AES.

6.4.1.1 DES

Ο DES τέθηκε σε ισχύ το 1977 και αποτελούσε για καιρό τον κύριο συμμετρικό αλγόριθμο με μήκος κλειδιού (56 bits) . Η αύξηση της επεξεργαστικής ισχύς των υπολογιστών έκανε την άρση του αλγορίθμου εύκολη με τη μέθοδο της εξαντλητικής αναζήτησης. Μια λύση δόθηκε με τον 3DES που αποτελεί μια παραλλαγή του DES που χρησιμοποιεί τρία DES κλειδιά σε σειρά (τα δύο συνήθως είναι τα ιδία). Ο 3DES αν και είναι κατά 2-3 φόρες πιο αργός από το DES παρέχει καλύτερη προστασία. Φημολογείται η ύπαρξη trapdoor(ή backdoor = πίσω πόρτα) στον αλγόριθμο γνωστή σε λίγους και εκλεκτούς (κυβερνήσεις), βάσει της όποιας ο αλγόριθμος καταλύεται άμεσα. Την υπόθεση ενισχύει το γεγονός ότι η IBM (σχεδιαστής DES) δεν αποκαλύπτει τις σχεδιαστικές αρχές των κουτιών κρυπτογράφησης (block-chip).

6.4.1.2 AES

Ο AES επιλέχτηκε το Μάιο του 2002 από το αμερικανικό Υπουργείο Εμπορίου σαν μια εξέλιξη του DES, το μήκος κλειδιού μπορεί να είναι 128 bits (16 bytes), 192 bits (24 bytes) ή ακόμα και 256bits (32 bytes). Εκτός του διαφορετικού μήκους κλειδιού από τον DES πληροφοριακά αναφέρεται ότι ο AES δε χρησιμοποιεί δίκτυα Fiestel όπως ο DES.

Πλεονεκτήματα της συμμετρικής κρυπτογραφίας είναι :

- Οι περιορισμένες ανάγκες σε υπολογιστική ισχύ
- Η ταχύτητα της μεθόδου
- Η συρρίκνωση του κρυπτογραφημένου κειμένου σε σχέση με το αρχικό

Μειονεκτήματα

- Ανάγκη για ασφαλή μετάδοση του κλειδιού μεταξύ των μελών (οπότε χρειαζόμαστε οπωσδήποτε απόλυτα αξιόπιστο κανάλι ή άμεση ανταλλαγή κλειδιού)
- Μειωμένη ασφάλεια σε σχέση με τους ασύμμετρους αλγορίθμους

6.4.2 Ασύμμετροι αλγόριθμοι

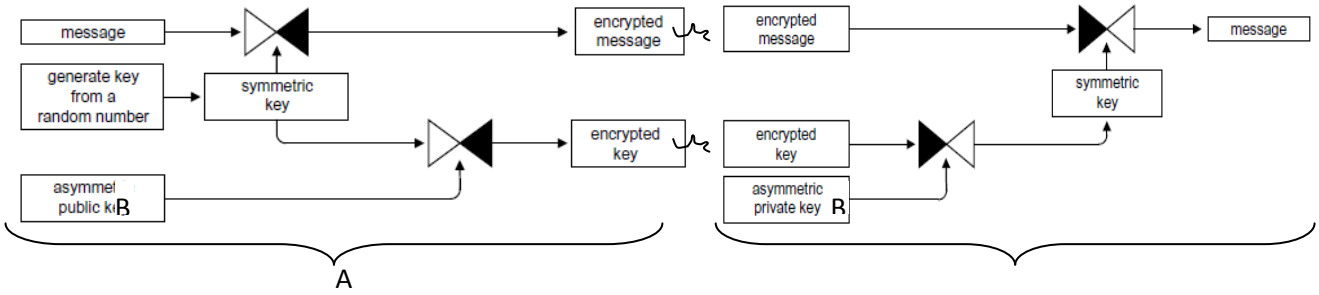
Οι ασύμμετροι αλγόριθμοι είναι οι αλγόριθμοι που χρησιμοποιούν δύο κλειδιά, το δημόσιο και το ιδιωτικό κλειδί. Κάθε χρήστης του δικτύου διαθέτει ένα ζευγάρι δημόσιου και ιδιωτικού κλειδιού. Το δημόσιο κλειδί το διαδίδει ελευθέρα χωρίς προστασία για να κρυπτογραφήσουν όσοι θέλουν μηνύματα σε αυτόν. Για παράδειγμα αν ο Α θέλει να στείλει στο Β ένα μήνυμα, έχουμε την εξής διαδικασία. Ο Α βρίσκει το δημόσιο και ελεύθερο κλειδί του Β και κρυπτογραφεί το μήνυμα, το οποίο ο Β το αποκρυπτογραφεί με το ιδιωτικό κρυφό του κλειδί. Μόνο το ιδιωτικό κλειδί του Β μπορεί να αποκρυπτογραφήσει το μήνυμα που είναι κρυπτογραφημένο με το δημόσιο του Β. Το εκπληκτικό είναι ότι η δημοσιοποίηση του δημόσιου κλειδιού δε δίνει ικανοποιητική βοήθεια για την εύρεση του ιδιωτικού κλειδιού που είναι κρυφό (συναρτήσεις μονής κατεύθυνσης).

Με αυτόν τον τρόπο όμως, ο Β δε ξέρει αν το μήνυμα ήρθε από τον Α αφού όλοι έχουν το δημόσιο κλειδί. Το μόνο που ξέρει ο Β είναι ότι μόνο αυτός μπορεί να αποκρυπτογραφήσει το μήνυμα. (Ούτε καν ο αποστολέας μπορεί αφού δεν έχει το ιδιωτικό κλειδί του παραλήπτη). Για το πρόβλημα πιστοποίησης χρησιμοποιούνται οι ψηφιακές υπογραφές που αναφέρονται πιο κάτω.

Το κρυπτογραφικό μοντέλο λειτουργεί και αντίθετα. Δηλαδή αν ο Α στέλνει το μήνυμα στο Β και θέλει να πιστοποιήσει ότι είναι ο Α, κρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί($A_{\text{ιδιωτικό}}$). Ο Β τώρα αποκρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του Α οπότε άμα αποκρυπτογραφηθεί το μήνυμα με το κλειδί αυτό ξέρει σίγουρα (100%) ότι το έστειλε ο Α. Το μειονέκτημα είναι ότι αφού το δημόσιο του Α είναι ελεύθερο και γνωστό σε όλους μπορούν όλοι να αποκρυπτογραφήσουν το μήνυμα και όχι μόνο ο Β. (Άρα αυτή η μέθοδος χρησιμοποιείται για επιβεβαίωση αποστολέα σε μη ασφαλή μηνύματα).

Κύριοι ασύμμετροι αλγόριθμοι που χρησιμοποιούνται στις έξυπνες κάρτες (γιατί υπάρχει πλειάδα ασύμμετρων αλγορίθμων για άλλες χρήσεις πχ.internet) είναι οι RSA, DSA, και ο αλγόριθμος ελλειπτικών καμπύλων.

Επειδή οι ασύμμετροι αλγόριθμοι είναι απαιτητικοί σε ισχύ και χρόνο, δε χρησιμοποιούνται συνήθως για κρυπτογράφηση του μηνύματος, αλλά το κείμενο κρυπτογραφείται με συμμετρικό αλγόριθμο (3DES, AES) και μόνο το κλειδί κρυπτογραφείται και αποστέλλεται με τον ασύμμετρο αλγόριθμο. Σχήμα 9:



Σχήμα 9 : Κρυπτογράφηση μόνο του συμμετρικού κλειδιού με ασύμμετρο αλγόριθμο

6.4.2.1 RSA

Ο RSA προτάθηκε από τους Ron Rivest, Adi Shamir και Len Adleman το 1978. Βέβαια φημολογείται (και γιατί όχι) ότι παρόμοιες εργασίες έγιναν από ερευνητές στο Β΄ παγκόσμιο πόλεμο, στο ψυχρό πόλεμο και στις μυστικές Βρετανικές υπηρεσίες τη δεκαετία 70. Όμως, λόγω του μη ανθρωπιστικού έργου αυτών των ερευνών και της μυστικοπάθειας οι τότε πιθανοί πρωτοπόροι ερευνητές έμειναν άγνωστοι. Αποτελεί τον πιο συνηθισμένο αλγόριθμο ασύμμετρης κρυπτογράφησης μαζί με τις ελλειπτικές καμπύλες. Βασίζεται στις αρχές της θεωρίας αριθμών και στη μεγάλη πολυπλοκότητα του παραγοντισμού του γινομένου δύο μεγάλων πρώτων αριθμών.

6.4.2.1 DSA

Ο DSA προτάθηκε το 1991 από το NIST (US National Institute of Standards and Technology) . Πηρέ το όνομα του από τις λέξεις Digital Signature Algorithm (DSA) διότι χρησιμοποιείται για τη ψηφιακή υπογραφή εγγράφων με τον αλγόριθμο κατακερματισμού SHA-1 (θα τα εξηγήσουμε πιο κάτω). Ο αλγόριθμος αποτελεί τροποποίηση του κρυπτοσυστήματος ElGamal και στηρίζεται στη δυσκολία του προβλήματος Diffie-Hellman και όχι στο πρόβλημα διακριτού λογάριθμου όπως πολλοί φοιτητές και συγγραφείς παρουσιάζουν στις εργασίες τους. Ο λογάριθμος λόγω της μεγαλύτερης από άλλους επεξεργαστικής ισχύς που απαιτεί αλλά και της ύποπτης για trapdoor μυστικής εκδοχής (λόγω χωράς προέλευσης) δε διαδόθηκε αρκετά.

6.4.2.3 Αλγόριθμος ελλειπτικών καμπυλών

Ο αλγόριθμος ελλειπτικών καμπυλών παρουσιάστηκε το 1985 ανεξάρτητα(;) από Victor Miller και Neal Koblitz, η μαθηματική του υποδομή δεν είναι απλή και ξεφεύγει από τους στόχους του συγγράμματος. Οι αλγόριθμοι αυτοί αποτελούν τους λιγότερο απαιτητικούς σε υπολογιστική ισχύ και παρέχουν για το ίδιο μήκος κλειδιού μεγαλύτερη ασφάλεια από τους δύο προαναφερθείσας αλγορίθμους. Γι’αυτό το λόγο πιστεύεται ότι θα κυριαρχήσουν στο μέλλον.

Πλεονεκτήματα ασύμμετρων η αλγορίθμων δημόσιου κλειδιού είναι:

- Η μεγάλη τους ασφάλεια σε σχέση με τους συμμετρικούς, αφού δε χρειάζονται αξιόπιστο κανάλι επικοινωνίας.
- Η μεγάλη τους υπολογιστική απροσιμότητα (δηλαδή με τα σημερινά τεχνολογικά μέσα και με εξαντλητική αναζήτηση κλειδιού δε μπορούν να αρθούν,(στο μέλλον ίσως)).

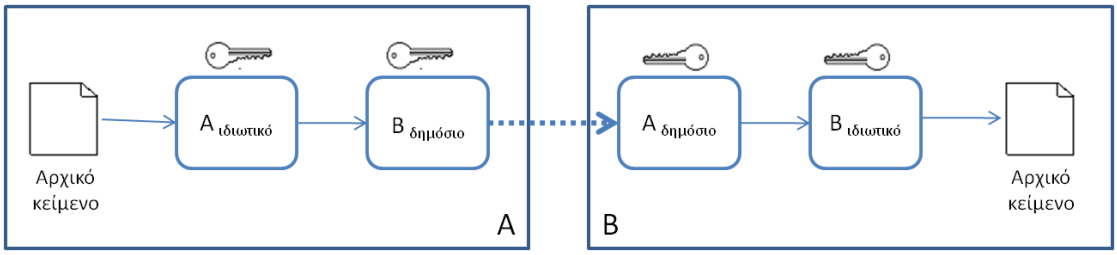
Μειονεκτήματα

- Στηρίζονται σε μαθηματικά προβλήματα που μπορεί μια μέρα να βρεθεί σύντομος πολυωνιμικός χρόνος επίλυσης τους και να καταλυθούν οι αλγόριθμοι.
- Απαιτούν μεγάλη υπολογιστική ισχύ και εμφανίζουν πολύ μεγαλύτερη καθυστέρηση στην κρυπτογράφηση – αποκρυπτογράφηση σε σχέση με τους συμμετρικούς. Γι΄αυτό το λόγο χρησιμοποιούνται συνήθως για να κρυπτογραφήσουν μονό το συμμετρικό κλειδί που κρυπτογράφησε το κείμενο ή/και να κρυπτογραφήσουν τη ψηφιακή υπογραφή που εξηγείται παρακάτω.

6.4.3 Ψηφιακές υπόγραφες

Οι ψηφιακές υπόγραφες αποτελούν ό,τι και η κανονική υπογραφή εγγράφων. Πιστοποιούν δηλαδή την αυθεντικότητα του αποστολέα, την αυθεντικότητα του μηνύματος (υπογραφή δημόσιου κλειδιού) και σε συνδυασμό με τη συνάρτηση κατακερματισμού και την ακεραιότητα του έγγραφου (υπογραφή σύνοψης). Οι ψηφιακές υπογραφές χρησιμοποιούν το ζεύγος κλειδιών (ιδιωτικό και δημόσιο) των ασύμμετρων αλγορίθμων για να πιστοποιούν την ταυτότητα του αποστολέα.

Στην υπογραφή δημόσιου κλειδιού χωρίς σύνοψη όλο το κείμενο κρυπτογραφείται με ασύμμετρο αλγόριθμο. Αν ο Α θέλει να στείλει στο Β δε κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του Β μόνο αλλά το υπογράφει πρώτα. Δηλαδή ο Α πρώτα κρυπτογραφεί το μήνυμα που θέλει να στείλει με το ιδιωτικό του κλειδί $A_{ιδιωτικο}$ και μετά με το δημόσιο κλειδί του Β ($B_{δημοσιο}$). Έπειτα στέλνει ο Α το μήνυμα και το λαμβάνει ο Β. Ο Β τώρα χρησιμοποιεί το δημόσιο κλειδί του Α, $A_{δημοσιο}$ (άρα στάλθηκε από τον Α) και μετά εφαρμόζει το ιδιωτικό κλειδί του πάνω σε αυτό $B_{ιδιωτικο}$ και εξάγει το αρχικό μήνυμα. Έτσι ο Β ξέρει ότι το μήνυμα το έστειλε πράγματι ο Α και το έχει υπογράψει κιόλας ο Α και δε μπορεί να αρνηθεί την αυθεντικότητα της υπογραφής του αφού, μονό αυτός έχει το $A_{ιδιωτικο}$ κλειδί.



Σχήμα 10: Υπογραφή δημοσίου κλειδιού χωρίς σύνοψη

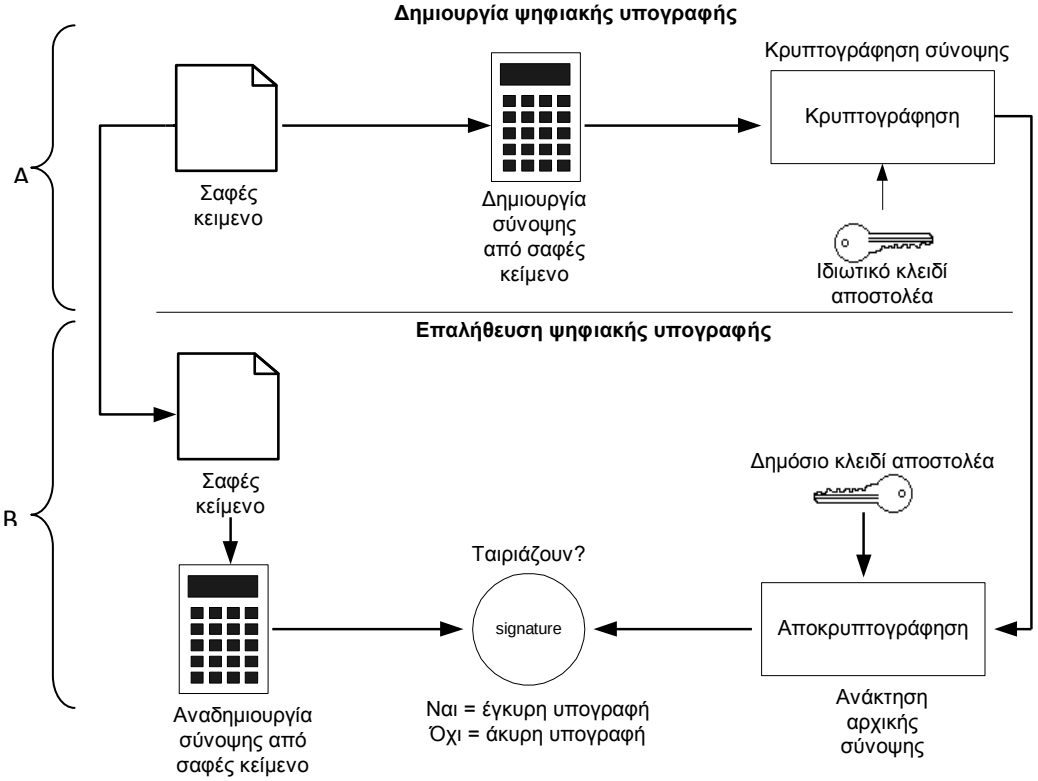
6.4.3.1 Ο αλγόριθμος σύνοψης- hash algorithm

Πριν πούμε την υπογραφή με σύνοψη μηνύματος θα εξηγήσουμε τον αλγόριθμο σύνοψης ή αλλιώς κατακερματισμού γνωστό στην αγγλική ορολογία ως hash algorithm. Ο αλγόριθμος σύνοψης είναι ένας αλγόριθμος που παίρνει σαν είσοδο ένα μήνυμα απροσδιόριστου μεγέθους και δίνει σαν έξοδο μια μονοσήμαντη περίληψη ή σύνοψη συγκεκριμένου μεγέθους (πολύ μικρότερου του αρχικού κειμένου) . Ο αλγόριθμος σύνοψης παράγει μοναδική σύνοψη για κάθε κείμενο και έστω και ένα γράμμα από το κείμενο να αλλάξει ριζικά όλη η σύνοψη. Η σύνοψη είναι μονοσήμαντη δηλαδή δε μπορεί κάποιος από τη σύνοψη να βρει το αρχικό μήνυμα (κάτι τέτοιο θα ήταν η τελεία συμπίεση και κρυπτογράφηση μαζί). Στις έξυπνες κάρτες χρησιμοποιούνται κυρίως οι αλγόριθμοι MD5, SHA-1 αλλά και οι SHA-256, DES-based και RIPR-MD.

Ο MD5 αποτελεί τη $5^{η}$ έκδοση αλγορίθμου που σχεδίασε ο Ronald Rivest (συνιδρυτής του RSA και δεινός κρυπταναλυτής) το 1992. Παράγει σύνοψη των 128 bits.

Ο SHA-1 αναπτύχθηκε από την έμπιστη (;) αρχή NSA (National Security Agency of USA) το 1993, δημιουργεί σύνοψη των 160 bits ενώ οι νέες εκδόσεις του επιτρέπουν 256, 384 και 512 bits.

Χρησιμοποιώντας τώρα τους αλγορίθμους σύνοψης (hash algorithms) δημιουργούμε τις ψηφιακές υπογραφές. Επανερχόμαστε στο σχήμα όπου ο Α στέλνει στο Β ένα μήνυμα και το υπογράφει. Ο Α κάνει μέσω του αλγορίθμου σύνοψης μια σύνοψη του μηνύματος και το κρυπτογραφεί (το υπογράφει) με το ιδιωτικό του κλειδί $A_{ιδιωτικό}$, ταυτόχρονα στέλνει την υπογραφή αυτή και το κείμενο αυτούσιο στο Β. Ο Β λαμβάνει την υπογραφή και εφαρμόζει πάνω της το δημόσιο κλειδί του Α, το $A_{δημόσιο,}$ όποτε παίρνει τη μια σύνοψη. Από το κείμενο που έλαβε αυτούσιο από τον Α (χωρίς κρυπτογράφηση) εφαρμόζει αλγόριθμο σύνοψης και παίρνει την άλλη σύνοψη, συγκρίνει τις δύο συνόψεις και αν είναι οι ίδιες ξέρει ότι το μήνυμα το έστειλε ο Α και δεν το έχει αλλάξει κανείς.

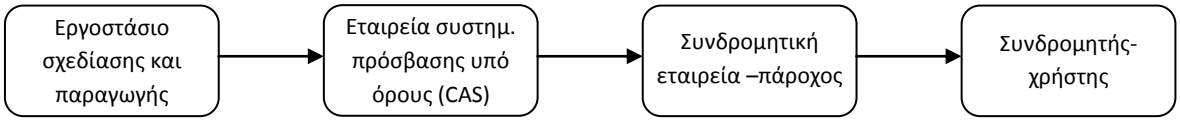


Σχήμα 10

Βέβαια με αυτό το μοντέλο, το μήνυμα στέλνεται αυτούσιο, οπότε μόνο η ακεραιότητά του και η προέλευσή του πιστοποιείται, όχι όμως και το απόρρητό του αφού στέλνεται αυτούσιο. Για να έχουμε και απόρρητο χρησιμοποιούμε υπογραφή δημοσίου κλειδιού που αναφέραμε πριν ,με κόστος μεγαλύτερο χρόνο και υπολογιστική ισχύ.

Τα πλείστα μοντέλα κρυπτογράφησης που αναλύθηκαν παραπάνω χρησιμοποιούν και οι πάροχοι στα συστήματα πρόσβασης υπό όρους. Αν και κάθε εταιρεία έχει τα δικά της ,συστήματα και συνδυασμούς, αλγορίθμων συνήθως τα μηνύματα EMM και ECM κρυπτογραφούνται τα μεν πρώτα με ασύμμετρο αλγόριθμο και τα δε δεύτερα με συμμετρικό (για ταχύτητα). Το δε ιδιωτικό κλειδί του ασύμμετρου αλγόριθμου(όποιου ή όποιων χρησιμοποιούνται)φυλάσσεται στην έξυπνη κάρτα του πελάτη ενώ το κλειδί του ασύμμετρου αποστέλλεται με τα EMM μηνύματα. Τόσο το EMM όσο και το ECM χρησιμοποιούν υπογραφές σύνοψης για πιστοποίηση της αυθεντικότητας τους αλλά και για διασφάλιση της ακεραιότητας τους.

Έκτος όμως από την υπολογιστική ισχύ της κρυπτογραφίας και της ισχύς τους κατά της κρυπτανάλυσης, οι έξυπνες κάρτες πρέπει να προφυλάσσονται και από τεχνικές και υλικές επιθέσεις σε όλα τα στάδια τους. Δηλαδή στο στάδιο σχεδίασης, γραμμής παραγωγής, στον προγραμματισμό τους από τον πάροχο και στο στάδιο χρήσης από τον τελικό αποδέκτη-πελάτη(σχήμα 13).



Σχήμα 13: Πορεία έξυπνης κάρτας

Και στα τέσσερα στάδια πρέπει να λαμβάνονται μέτρα προστασίας τόσο από πειρατές όσο και από φιλόδοξους υπαλλήλους, ανταγωνιστές ή άλλους. Στα πρώτα στάδια ειδικά αν διαρρεύσουν σχέδια υλοποίησης κατά το σχεδιασμό ή παραγωγή μπορεί να αποδειχτεί μοιραίο για όλο το σύστημα (που μπορεί να αριθμεί εκατομμύρια συνδρομητικές κάρτες).

Στο δεύτερο στάδιο η εταιρία συστημάτων πρόσβασης αφού λάβει τις κάρτες τοποθετεί μέσα τους αλγορίθμους κρυπτογράφησης διαλέγοντας από μια γκάμα ασύμμετρων συμμετρικών, ψηφιακών υπογράφων με αλγόριθμο hash, αλγορίθμων τυχαίων αριθμών που δε δημοσιοποιεί ή αναφέρει πουθενά.

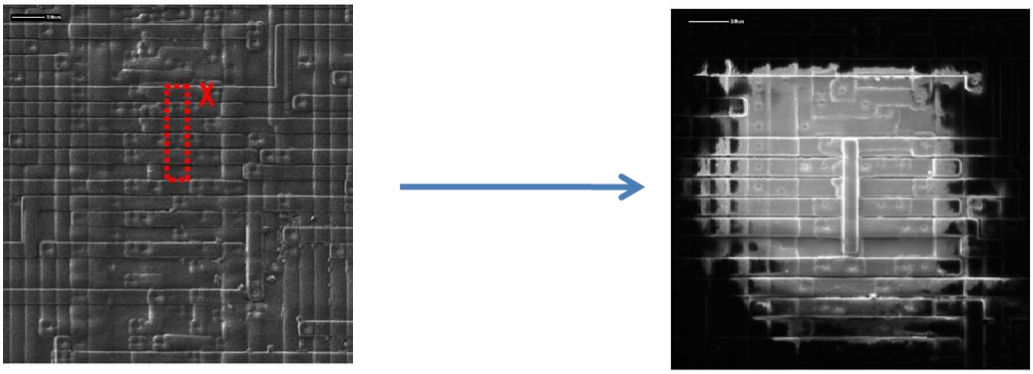
Στο τρίτο στάδιο η εταιρία CAS (στην Ελλάδα η irdeto) παραδίδει στον πάροχο (Nova) τις έξυπνες κάρτες με το σχήμα κρυπτογράφησης που δημιούργησε (irdeto2 σήμερα) που χειρίζεται συμφώνα με το μοντέλο που δείξαμε στο κεφάλαιο 4. Η νόβα τοποθετεί και χειρίζεται τα user key των καρτών μέσω των SMS και SAS.

Στο τέταρτο στάδιο η κάρτα παραδίδεται στον πελάτη και από εκεί και πέρα ο τελικός χρήστης έχει πλήρη πρόσβαση στην κάρτα για να πειραματιστεί και να προσπαθήσει να παραβιάσει την ασφάλεια της.

Κατά το παρελθόν αν και στις έξυπνες κάρτες χρησιμοποιήθηκαν δυσπρόσιτοι υπολογιστικά αλγόριθμοι οι πειρατές κατάφεραν να εξάγουν τα επιθυμητά κλειδιά από αυτές. Αυτό οφείλεται κυρίως στο ότι ο πειρατής έχει στην κατοχή του την έξυπνη κάρτα και μπορεί να πειραματιστεί πάνω της. Έτσι βασιζόμενος στην ευρηματικότητα του, στην εξέλιξη της τεχνολογίας, στις ακαδημαϊκές εργασίες, στις παραβλέψεις - λάθη των κατασκευαστών, μπορεί να έχει πλαγιά πρόσβαση στην άρση των συστημάτων ασφαλείας των έξυπνων καρτών.

Παραδείγματα φαίνονται στις δύο εικόνες κάτωθι:

Σχήμα 11: Παρατήρηση ηλεκτρομαγνητικών αποκρίσεων της έξυπνης κάρτας σε επιλεγμένες εισόδους



Michael Tunstall
Attacks on Smart Cards - Copyright Gemplus Ltd 2003

Σχήμα 12 : Προσθήκη γραμμών στους διαύλους του επεξεργαστή για ανταλλαγή –εξαγωγή ψηφίων με απώτερο σκοπό την κατάλυση της ασφάλειας

Άλλες τεχνικές είναι η επήρεια των bits της κάρτας σε UV ακτινοβολία, σε ακτίνες laser, σε ηλεκτρομαγνητικούς παλμούς και άλλους εξωτερικούς παράγοντες. Με αυτό τον τρόπο ο πειρατής αλλάζει τα bits και παρακολουθεί τις αλλαγές στις εξόδους της κρυπτογράφησης. Δίνοντας πχ όλο 0 σαν είσοδο σε DES, ο DES είναι σαν να παρακάμπτεται. Άλλο είναι το πάγωμα της RAM και η εξέταση της αφού τα κλειδιά για να υπολογίσουν πράξεις στιγμιαία εξάγονται στη RAM.

Από παράβλεψη του κατασκευαστή της Γερμανικής τράπεζας το 1997 οι πειρατές περιόρισαν το πεδίο των πιθανών αριθμών συνδυασμών των τετραψήφιων PIN (Personal identification number) από 10^4 (10*10*10*10) σε μόλις 450 συνδυασμούς, λαμβάνοντας υπόψη ότι το σύστημα της τράπεζας δε δημιουργούσε τυχαία PIN αλλά PIN με περισσότερη συμμετοχή του 0 και του 5 παρά του 6 και 9 ενώ το 0 σχεδόν ποτέ δεν έμπαινε σαν πρώτο ψηφίο. Από τότε μελετήθηκαν και αναπτύχτηκαν αλγόριθμοι παραγωγής τυχαίων αριθμών (σχήμα 8 –random number) οι οποίοι χρησιμοποιούνται στην παραγωγή τυχαίων κλειδιών.

6.5 Η έξυπνη κάρτα Gamma

Στην Ελλάδα τώρα και στο σύστημα της Irdeto που χρησιμοποιεί η συνδρομητή δορυφορική τηλεόραση Nova, αν και η δεύτερη έκδοση του περίφημου Irdeto CAS (Irdeto2) δε γνώρισε για πολλά χρόνια (έξη) παραβίαση στο επίπεδο των έξυπνων καρτών. Τον Ιανουάριο του 2007 εμφανίστηκε μια κάρτα λεγόμενη Gamma Card η οποία υποσχόταν συνεχή παράνομη θέαση με τη χρησιμοποίηση της. Αυτό ακούστηκε σαν ένα εμπορικό τρικ αφού κατά καιρούς, κυκλοφορούν κάρτες που έχουν κάποια μηνιαία κλειδιά όπου μόλις περάσει ο μήνας σταματούν να δουλεύουν χωρίς να ανανεώνουν τα κλειδιά που περιέχουν.
Με την πάροδο του καιρού όμως αποδείχτηκε ότι η gamma κάρτα δεχόταν τα νέα service key, δεν απέρριπτε δηλαδή την ανανέωση και συμπεριφερόταν σαν κανονική συνδρομητική κάρτα χωρίς να έχει παραχθεί από την Irdeto και χωρίς να πληρώνεται η μηναία συνδρομή στη Nova.
Η αγορά της κάρτας κυμαίνεται σε 60-100 ευρώ και απαιτεί ένα προγραμματιστή κάρτας που ενώνεται σε ένα υπολογιστή για να φορτωθεί το κατάλληλο πρόγραμμα και να αρχίσει να ξεκλειδώνει το σήμα χωρίς να απαιτείται τίποτα άλλο. Το όλο εγχείρημα βέβαια κρυπτογραφείται εκ νέου από τον αρχιπειρατή παραγωγό των καρτών έτσι ώστε ένας αντίπαλος πειρατής να μη μπορεί να παράγει και αυτός έτσι κλωνοποιημένη κάρτα. Δηλαδή οι πειρατές προστατεύονται από άλλους πειρατές και μερικές φορές το κάνουν με καλύτερο τρόπο από ότι ο πάροχος. Η συγκεκριμένη μέθοδος πειρατείας αποτελεί το μεγαλύτερο πλήγμα για ένα πάροχο αφού είναι απλή μέθοδος πειρατείας (μια κάρτα και τελειώνεις) χωρίς ρυθμίσεις δικτύου και δεκτών όπως το Card Sharing, ενώ η μη έγκυρη πάταξη του φαινομένου οδηγεί συνήθως σε αλλαγή κρυπτογράφησης από τον πάροχο.
Η Gamma Card πωλείται από τους παράνομους εμπόρους χωρίς να μπορεί να ξεκλειδώσει τις συνδρομητικές υπηρεσίες. Η πώληση γίνεται από χέρι σε χέρι ή από ηλεκτρονικές ιστοσελίδες με χωρά προέλευσης εκτός Ευρωπαϊκής Ένωσης όπου το ευρωπαϊκό δίκαιο δεν έχει ισχύ και δε μπορεί να κλείσει κάποιος αυτά τα ηλεκτρονικά καταστήματα. Για να μπορέσει η κάρτα να υποδυθεί την αυθεντική πρέπει να προγραμματιστεί ‘’φορτωθεί’’ με κατάλληλους κωδικούς - εντολές που έχει δημιουργήσει ο παράνομος εφευρέτης της κάρτας και τις δημοσιοποιεί επί πληρωμή ή ελεύθερα στο διαδίκτυο. Η μη τοποθέτηση των κωδικών από τον παραγωγό γίνεται για τρεις λόγους κυρίως.

- Να μην αποτελεί παράνομο υλικό αν πιαστεί στα χέρια του εμπόρου αφού δε μπορεί να ανοίξει συνδρομητικό κανάλι η κενή κάρτα.
- Να απαιτείται τακτική ανανέωση των κωδικών όποτε είναι ανούσιο οποιοδήποτε λογισμικό αφού έως να πουληθεί θα θέλει άλλο.
- Να μπορεί ο αρχή-πειρατής να βγάζει επιπλέον χρήματα πουλώντας το λογισμικό ανεξάρτητα από την κάρτα.

Πως γίνεται όμως η κάρτα να συμπεριφέρεται ως κανονική;
Οι πειρατές κατάφεραν να κάνουν τις κάρτες να λειτουργούν με παρόμοιο τρόπο (εξομοίωση) με τις αυθεντικές, δηλαδή να δίνουν τις ίδιες αποκρίσεις στα ECM και EMM κλειδιά χωρίς κατά ανάγκη να ξέρουν πως λειτουργούν οι αυθεντικές κάρτες (μπορεί και να ξέρουν αλλά είναι δύσκολο χωρίς ενημέρωση από τους κατασκευαστές). Έτσι το μόνο που τους μένει είναι να ξέρουν ενεργά User key κάρτας ή καρτών για να τα τοποθετήσουν στις παράνομες κάρτες τους. Ο τρόπος εύρεσης των User Key γινόταν παλιά εύκολα με ένα

προγραμματιστή καρτών και ειδικά προγράμματα. Κάτι τέτοιο δεν ισχύει σήμερα αφού το User Key πλέον κρύβεται καλά από τους κατασκευαστές. Έτσι η δυσκολία εύρεσης του User Key όσο και ο μεγάλος αριθμός κατοχής User Key από τους αρχιπειρατές (όπως θα δούμε πιο κάτω) κάνουν δύσκολη τη θεώρηση εξαγωγής αφού σημαίνει ότι οι αρχιπειρατές θα έχουν πρόσβαση σε πολλές συνδρομητικές κάρτες (πράγμα δύσκολο). Οπότε οι αρχιπειρατές της gamma βρήκαν τόσα user key, είτε μέσω παρατήρησης και αποκρυπτογράφησης της ροής του παρόχου, είτε με πληροφορίες από τους υπολογιστές του συστήματος πρόσβασης, είτε με ατελείωτες δοκιμές για ενεργά user key μέσω υπολογιστών (μάλλον απίθανο).

Με ένα μόλις User key από μια πληρωμένη συνδρομή μπορούν να δημιουργηθούν όσα αντίγραφα θέλουμε. Το σύστημα αποκρυπτογράφησης που χρησιμοποιεί το DVB-S όπως είδαμε δε παρέχει κανάλι επιστροφής, έτσι ο πάροχος δεν είναι σε θέση να ξέρει ότι υπάρχουν 10000 πχ συνδρομητές με το ίδιο User Key. Η έλλειψη καναλιού επιστροφής είναι ένα πρόβλημα που μειώνει την ασφάλεια του DVB και διάφορες λύσεις προτείνονται (πχ χρησιμοποίηση modem ή τηλεφώνου για κανάλι επιστροφής). Έτσι ένας τρόπος ανακάλυψης της διαρροής από τον πάροχο είναι η αγορά κλωνοποιημένης κάρτας και η ανακάλυψη του user-key που διέρρευσε. Ξέροντας αυτή την πληροφορία ο πάροχος μπορεί άμεσα να διακόψει τη λειτουργιάς της αυθεντικής κάρτας και όλων των κλωνοποιημένων.
Για να το παρακάμψουν εν μέρει αυτό οι κατασκευαστές των gamma card παρατηρήθηκε ότι δημιούργησαν πολλά λογισμικά με πολλά user key (πχ. 500)ανά λογισμικό. Κάθε κενή κάρτα μετά την εγκατάσταση του λογισμικού από το χρήστη κλειδώνει σε ένα user key ανάλογα με τον σειριακό αριθμό της ή με άλλο παράγοντα **και μόνο αυτό** το User Key μπορεί να ανιχνευθεί από ένα τρίτο(όχι τα υπόλοιπα αφού είναι κρυπτογραφημένα με αλγόριθμο των πειρατών στο λογισμικό). Έτσι ο πάροχος δεν καταφέρνει να ανακαλύψει όλα τα user key που κατέχουν οι πειρατές απλά μέρος αυτών, με αποτέλεσμα κάποιες κάρτες να συνεχίζουν να παίζουν. Για να τα ανακαλύψει όλα πρέπει να αγοράσει αρκετές κάρτες και να είναι τυχερός να φανερωθούν όλα τα user key. Αλλά και να βρεθούν όλα τα user key που διέρρευσαν δεν είναι σε θέση να διασφαλίσει κανένας ότι δε θα εμφανιστούν άλλα.

Όλα αυτά που αναφέρουμε είναι συμπεράσματα και παρατηρήσεις από τη λειτουργία των gamma στα δύο χρόνια ζωής τους. Ο ακριβής τρόπος λειτουργίας των gamma είναι μυστικός και γνωστός μόνο από τους κατασκευαστές για ασφάλεια της επένδυσης τους. Έτσι μπορεί η πραγματική λειτουργιά τους να μην είναι 100% έτσι όπως περιγράφηκε.

Η nova-irdeto δεν αντέδρασαν άμεσα στην παρουσία αυτής της κάρτας που παρουσίασε εκπληκτική αντοχή δύο ετών συνεχής λειτουργίας. Αυτό, λόγο του ότι δε μπορούσε να βρει τα user key που διαρρεύσαν αλλά κυρίως στο γεγονός ότι ο πάροχος μπορεί, με το κλείσιμο ενός user key που διέρρευσε, να επηρεάσει τη λειτουργία άλλων νόμιμων καρτών αφού τα user key αποστέλλονται από τα EMM ανά ομάδες. Έτσι έπρεπε να βρεθεί μια λύση που να απενεργοποιεί την ανανέωση των service keys των καρτών αυτών αλλά και να μην επηρεάζει τις αυθεντικές ταυτόχρονα. Φαίνεται ότι βρέθηκε τέτοια λύση και από τον Ιούλιο του 2009 άρχισαν οι κάρτες να σταματούν και να απαιτούν νέα αρχεία για να ξαναδουλέψουν και τα οποία δε δίνουν πολλές μέρες δωρεάν θέασης.

Η irdeto στα πλαίσια της αναβάθμισης της ασφαλείας της παρουσίασε τη λύση που προσφέρουν όλο και περισσότερες εταιρίες παροχής συνδρομητικών υπηρεσιών. Αυτή είναι η ανανέωση και αναβάθμιση του λογισμικού ασφαλείας (αλλαγή ιδιωτικών κλειδιών ή αλλαγή αλγορίθμων κρυπτογράφησης) στον ‘’αέρα’’. Δηλαδή δυναμικά ο πάροχος μέσω των EMM στις νέες κάρτες μπορεί χωρίς να χρειάζεται αλλαγή κάρτας να κάνει αλλαγές στο σύστημα ασφαλείας-κρυπτογράφησης της κάρτας. Η irdeto ονόμασε την τεχνολογία όπως είπαμε και πριν (Κεφάλαιο 1) Flash-Flexi. Έτσι με το που εντοπίζονται κλωνοποιημένες κάρτες μπορεί με μια εντολή ο πάροχος να εισάγει στις υπάρχουσες κάρτες, εντολές για αλλαγές στο σύστημα κρυπτογράφησης και να αχρηστεύσει τις παράνομες .Έτσι ο πάροχος δε χάνει χρήμα για αλλαγή καρτών, δε χάνει χρόνο(αφού γίνεται άμεσα η αλλαγή) και δεν χρειάζεται να αλλάξει δέκτες στους νόμιμους συνδρομητές όπως γινόταν πολλές φορές.

Επιπλέων χρησιμοποιείται η δεύτερη τεχνολογία η SS (δηλαδή η Secure Silicon), που είδαμε και στο Card Sharing, βάσει της οποίας η συνδρομητική κάρτα παντρεύεται με το δορυφορικό αποκωδικοποιητή. Έτσι η κάρτα επιστρέφει τα Control Words σε ένα συγκεκριμένο δέκτη με τον οποίο έχει συμφωνήσει η κάρτα. Η κάρτα πλέων γνωρίζει πότε και που θα στείλει τα CW ,ενώ όταν τα στέλνει αυτά είναι κρυπτογραφημένα. Με αυτή τη τεχνολογία θα είναι ακόμα πιο δύσκολα να πραγματοποιηθούν κλωνοποιημένες κάρτες αφού και να γίνουν θα δουλεύουν μόνο στο δέκτη που είναι ‘’παντρεμένες’’ άρα θα πρέπει να κλωνοποιηθεί και ο δέκτης.

Με αυτές τις τεχνολογίες η Irdeto ισχυρίζεται ότι θα πατάξει τόσο το Card Sharing όσο και την κλωνοποίηση καρτών. Η ασφάλεια ή όχι του εγχειρήματος δε μπορεί να ειπωθεί αν είναι μεγάλη ή όχι (αν και φαίνεται ελπιδοφόρα για τους παρόχους). Από τον καιρό όμως της αναλογικής δορυφορικής συνδρομητικής τηλεόρασης οι εταιρίες (τόσο κρυπτογράφησης όσο και εκπομπής) διαφημίζουν συστήματα τα οποία επικαλούνται να είναι άρρηκτα και απόρθητα (φυσιολογικό για να τα πουλήσουν) και μετά από λίγο καιρό να πειρατεύονται. Αναφέρονται ήδη στο εξωτερικό σε περιπτώσεις που η κάρτα ‘’ξεπαντρεύεται’’ και δουλεύει εκτός του δέκτη που ‘’παντρεύτηκε’’.

Ο Markus G.Kuhn (καθηγητής Cambridge με εργασίες κρυπτανάλυσης συστημάτων πρόσβασης) πάντως είπε το 1978: ‘’Every security microcontroller and ASIC will be reverse engineered within weeks if pirates see a chance to make a million dollars profit from doing it’’. Που σημαίνει αν υπάρχει περιθώριο κέρδους όλα γίνονται και ο κανόνας μέχρι σήμερα (Οκτώβριο 2009)ισχύει.

6.6 Βιβλιογραφία

Attacks on Smart Cards: Michael Tunstall (πολύ καλό βιβλίο)

Smart Card Security and Applications Second Edition: Mike Hendry

Smart Card Applications Design Models for using and programming smart cards:
Wolfgang Rankl, translated by Kenneth Cox

Smart Card Handbook Third Edition:
Wolfgang Rankl and Wolfgang Effing, translated by Kenneth Cox

Smart Card Evolution: Fernando Ferreira

Smart Cards, Tokens,Security and Applications:
Keith E. Mayes and Konstantinos Markantonakis

Attacks on Pay-TV Access Control Systems :Markus G. Kuhn

Analysis of the Nagravision Video Scrambling Method Markus G. Kuhn

Smart Card & Security Basics CardLogix, Inc.

Περιοδικό ‘’Δορυφορικά Νέα’’ Δεκέμβριος 2008

Επέκταση περιηγητή για διαχείριση πιστοποιητικών σε τεχνολογία έξυπνων καρτών
ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ: Χρυσούλα Π. Σκλιά

Έξυπνες Κάρτες σε Εφαρμογές Ηλεκτρονικής Διακυβέρνησης
ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ: Αλέξανδρος Κ. Σφάγγος

Ανάπτυξη Εφαρμογών Σε Έξυπνες Κάρτες
ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ: Αθανασία Κ.Δημητράκη

INTERNATIONAL STANDARD : ISO/IEC7816-1
INTERNATIONAL STANDARD : ISO/IEC7816-2
INTERNATIONAL STANDARD : ISO/IEC7816-3
INTERNATIONAL STANDARD : ISO/IEC7816-4
INTERNATIONAL STANDARD : ISO/IEC7816-5
INTERNATIONAL STANDARD : ISO/IEC7816-6
INTERNATIONAL STANDARD ISO/IEC 7816-15:2004
INTERNATIONAL STANDARD : ISO14443

http://www.sat-television.com
http://www.irdeto.com
http://www.maldiviandigital.com/smartcard-file-section
http://www.etsi.org
http://board.satportal.to/gamma-card-ellada-kypros

Κεφάλαιο 7 Πειρατεία μέσω Video Streaming

7.1 Εισαγωγή

Το video steaming(βίντεο συνεχούς ροής) μέσω διαδικτύου αποτελεί μια πλάγια μέθοδο δορυφορικής πειρατείας που αναπτύσσεται με ταχύς ρυθμούς και αποτελεί ανερχόμενη απειλή για τους παρόχους.

Το Video Streaming χρησιμοποίει όπως και το Card Sharing το διαδίκτυο σαν κύριο δίκτυο με τη διαφορά ότι εδώ δεν ανταλλάζει κλειδιά αλλά ολόκληρο το οπτικοακουστικό υλικό. Ο επίδοξος πειρατής αφού αποκρυπτογραφήσει με νόμιμο ή παράνομο τρόπο το δορυφορικό σήμα του δε το τροφοδοτεί στην τηλεόραση αλλά το διανέμει στο διαδίκτυο. Άλλοι χρήστες είτε με μικρή συνδρομή είτε δωρεάν παρακολουθούν χωρίς να έχουν πληρώσει δικαιώματα στον πάροχο τις υπηρεσίες του. Η αύξηση των ευρυζωνικών συνδέσεων και ταχυτήτων σε συνδυασμό με τη μείωση των τιμών των συνδέσεων κατέστησαν τη μέθοδο προσιτή για κάθε επίδοξο που δεν επιθυμεί να πληρώσει συνδρομή στον πάροχο.

Πριν μιλήσουμε για τη μέθοδο και τους διαφορετικούς τρόπους Video Streaming θα μιλήσουμε για τα μοντέλα αποστολής αρχείων στο διαδίκτυο.

7.2 Συστήματα εκπομπής διαδικτύου:

Το διαδίκτυο παρουσιάζει και υποστηρίζει τέσσερα διαφορετικά συστήματα εκπομπής αυτά είναι :

- unicast
- broadcast
- multicast
- anycast

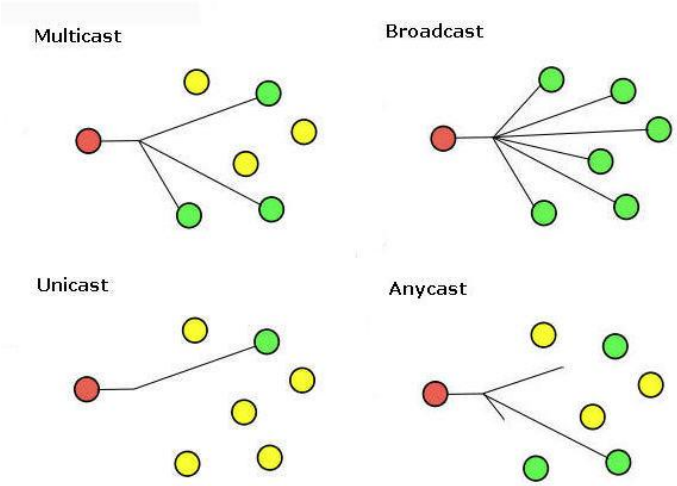
Τα συστήματα φαίνονται στο σχήμα 1 και εξηγούνται κάτωθι :

Το unicast υποστηρίζει παράδοση πληροφορίας(βίντεο εδώ) από τον αποστολέα(κόκκινη κουκίδα) σε ένα μόνο τερματικό(πράσινη κουκίδα).

Το broadcast υποστηρίζει αποστολή σε όλους ανεξαρτήτως τους χρήστες του δικτύου.

Το multicast (που μας ενδιαφέρει και στα ελληνικά είναι πολυδιανομή) υποστηρίζει αποστολή της πληροφορίας από τον αποστολέα σε μια ομάδα χρηστών (όχι όλους τους χρήστες αλλά αρκετούς).

Ενώ τέλος κατά το anycast μοντέλο η παράδοση της πληροφορίας γίνεται από το αποστολέα σε ένα κόμβο μιας ομάδας χωρίς συγκεκριμένα κριτήρια(συνήθως τον πιο κοντινό).

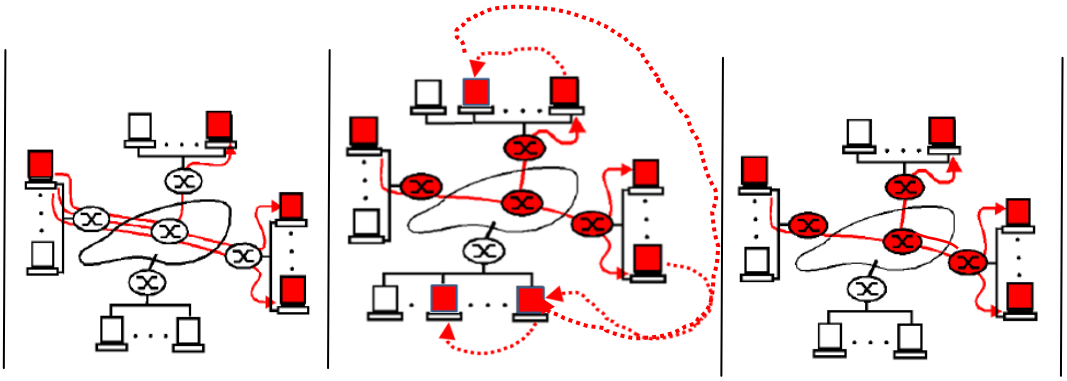


Σχήμα 1 : Συστήματα εκπομπής που υποστηρίζει το διαδίκτυο

7.2.1 Multicast

Το multicast μοντέλο αποστολής πληροφοριών (video, ήχου, τιμές μετοχών ,αλλαγές στη βάση δεδομένων κτλ) χρησιμοποιείται για δορυφορική πειρατεία. Για να εξηγήσουμε πως χρησιμοποιείται αυτό το σύστημα εκπομπής για πειρατεία πρέπει πρώτα να αναλύσουμε τους τρεις τρόπους εκπομπής του multicast. Αυτοί είναι:

- Μονοεκπομπή ένας προς όλους(multi-unicast)
- Ρητή Πολυεκπομπή (multicast)
- Πολυεκπομπή επιπέδου εφαρμογής (application multicast)



(α) Μονοεκπομπή ένας προς όλους

(β) Πολυεκπομπή επιπέδου εφαρμογής

(γ) Ρητή Πολυεκπομπή

Σχήμα 2 : Τα διαφορετικά σχήματα δρομολόγησης στο διαδίκτυο

Μονοεκπομπή ένας προς όλους: Όπως φαίνεται και στο σχήμα 2(α) ο αποστολέας εγκαθιδρύει ξεχωριστή unicast σύνδεση με τον κάθε έναν τελικό χρήστη και αφού ανακατασκευάσει την πληροφορία τόσες φορές όσοι και οι χρήστες τη στέλνει στους χρήστες. Κάτι τέτοιο επιβαρύνει το δίκτυο, τον επεξεργαστή του αποστολέα και έχει άνω όριο χρηστών όσο και το upload bandwith αποστολέα.

Η Ρητή Πολυεκπομπή όπως φαίνεται στο σχήμα 2(γ) υποστηρίζει μια εκπομπή από τον αποστολέα οπότε δεν καταπονείται το δίκτυο. Η ροή λαμβάνεται από τους ενδιάμεσους δρομολογητές αντιγράφεται και προωθείται κατάλληλα σε όσους χρήστες έκαναν αίτηση

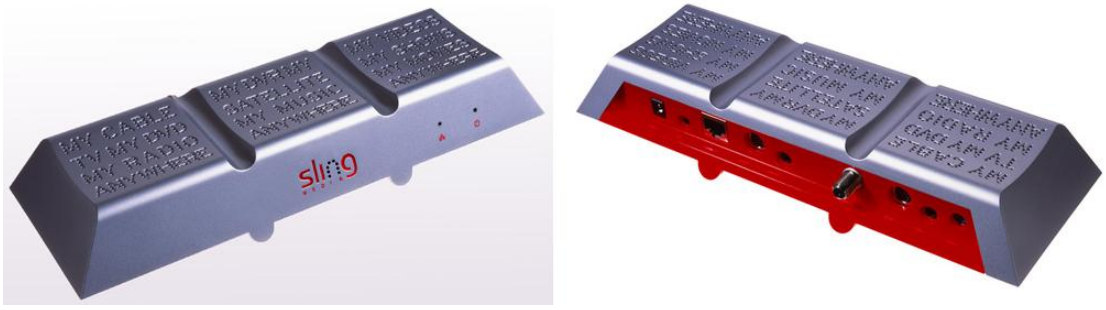
για πρόσβαση. Αποτελεί τη βέλτιστη λύση για εξοικονόμηση bandwith και πόρων δικτύου αλλά απαιτεί κατάλληλη υποδομή και υποστήριξη σε επίπεδο δικτύου. Δηλαδή επαφίεται στον πάροχο του διαδικτύου η υλοποίηση ή όχι αυτής της υποδομής. Στην Ελλάδα οι ιδιωτικές εταιρίες παροχής ευρυζωνικών συνδέσεων δεν επιτρέπουν ακόμα τέτοια υλοποίηση δικτύου και μόνο το ΕΔΕΤ(Εθνικό Δίκτυο Έρευνας και Τεχνολογίας) προσφέρει αυτήν την υπηρεσία στο ακαδημαϊκό δίκτυο του.

Πολυεκπομπή επιπέδου εφαρμογής (σχήμα 2β) όπου ο αποστολέας στέλνει τη ροή σε ένα ή λίγους χρήστες και αυτή μέσω εφαρμογής και σύνδεσης P2P (peer to peer, θα εξηγηθεί πιο κάτω) αντιγράφουν και προωθούν πακέτα πληροφορίας της ροής σε άλλους χρήστες. Έτσι δεν καταπονείται ο αποστολέας (που μπορεί να είναι ένας απλός χρήστης που θέλει να εκπέμψει ένα ποδοσφαιρικό αγώνα)και αναλαμβάνουν οι υπόλοιποι με κατανεμημένη υπολογιστική επεξεργασία να αλληλοτροφοδοτούν τη ροή στο δίκτυο.

7.2.1.1 Μονοεκπομπή ένας προς όλους

Η Μονοεκπομπή ένας προς όλους χρησιμοποιείται σχεδόν από τον καθένα μας καθημερινά. Αποτελεί τη μέθοδο που συνομιλούν δύο χρήστες με βίντεο -συνδιάσκεψη(video conference) στα προγράμματα κοινωνικές δικτύωσης(skype,msn,oovoo-που επιτρέπει μέχρι και 8 συνδέσεις ταυτόχρονα) και αλλά. Ο αποστολέας αποτελείται από το PC του κάθε χρήστη που θέλει να εκπέμψει. Το PC αναλαμβάνει να κάνει τα αντίγραφα βίντεο και να εκπέμψει σε όσους χρήστες επιθυμούν να δουν και ακούσουν το χρήστη. Η μέθοδος τόσο καιρό γινόταν μόνο μέσω υπολογιστή και αυτό λόγο της ανάγκης μετατροπής(transcoding) του video σε μορφή με μεγαλύτερη συμπίεση και λιγότερο bandwith από το αρχικό. Το οπτικοακουστικό υλικό που λαμβάνεται από τους δορυφορικούς δέκτες είναι σε μορφή MPEG-2 με εύρος 3-4 Mbps μια τέτοια upload εκπομπή αποτελεί προνόμιο λίγων και γι'αυτο πρέπει να γίνει μετατροπή σε αλγόριθμο με καλύτερη συμπίεση (συνήθως MPEG-4 με H.264).Στην πειρατεία τέτοια συμπίεση πραγματοποιεί ο υπολογιστής ,αυτός συνδέεται με το δορυφορικό δέκτη και ‘’τραβά’’ το αποκρυπτογραφημένο σήμα στην έξοδο του πριν την τηλεόραση ,το μετατρέπει σε H.264 κωδικοποίηση με εύρος από 300Kbps-1000Kbps το οποίο απαιτεί upload ταχύτητες 1MByte (που είναι οι πλείστες συνδέσεις upload στην Ελλάδα). Έτσι εφαρμογές όπως το VLCplayer χρησιμοποιούνται για να λάβουν κωδικοποιήσουν και αποστείλουν ένα δορυφορικό κανάλι (πχ ποδοσφαιρικό αγώνα) σε μικρή ομάδα φίλων.

Η ανάπτυξη ολοκληρωμένων για transcoding και η μείωση των τιμών τους επέτρεψε αυτή τη διαδικασία(λήψη, transcoding και εκπομπή) να γίνεται και από αυτόνομη συσκευή χωρίς ανάγκη υπολογιστή. Πρωτοπόρος αυτής της τεχνολογίας ήταν η συσκευή sling box με το περίεργο σχήμα σοκολάτας, αυτή φαίνεται στο σχήμα 3



Σχήμα 3 : sling box

Η συσκευή διαθέτει είσοδος σήματος εικόνας και ήχου και έξοδο ethernet θύρας. Η συσκευή λαμβάνει το σήμα και το διανέμει στο internet ,μέσω λογισμικού της εταιρίας που εγκαθιστά ο χρήστης στον υπολογιστή, στο κινητό ή στο PDA(personal digital assistant) συνδέεται με τη συσκευή και βλέπει μέσω Streaming το βίντεο που εκπέμπεται. Μέσω του ειδικού λογισμικού ο χρήστης μπορεί να αλλάζει κανάλια στη δορυφορική ή επίγεια τηλεόραση να δυναμώνει ή να χαμηλώνει τη φωνή ή ακόμα να ενεργοποιεί ή να απενεργοποιεί το δέκτη/τηλεόραση ενώ είναι μίλια μακριά. Αυτή η τεχνολογία έφερε νέους όρους στο προσκήνιο ένας από αυτός είναι του place shifting. Η μεταφορά δηλαδή της συνδρομής μέσω internet όπου θέλει ο χρήστης. Αυτές οι συσκευές (sling box και όμοιες) και λόγω επεξεργαστικής ισχύς, και λόγω δικαιωμάτων αλλά και λόγω Upload bandwidth εκπέμπουν ταυτόχρονα το πολύ σε δύο χρήστες στο internet. Έτσι αυτή η τεχνολογία δεν επηρεάζει οικονομικά τους παρόχους συνδρομητικής τηλεόρασης αλλά πολλοί πάροχοι όπως η Libery Media και Echostar προσφέρουν συσκευές place shifting για να προσελκύσουν πελάτες προβάλλοντας την επιλογή για μεταφορά συνδρομής στις τους διακοπές σαν επιπλέον ατού της εταιρίας τους. Πανάκριβες συσκευές όμως μπορούν να εκπέμπουν ταυτόχρονα σε πολλούς παράνομους χρήστες αν είναι συνδεδεμένοι σε εσωτερικό δίκτυο LAN (όχι WAN-internet). Αυτό γιατί οι ταχύτητες φτάνουν τα 1Gbps (συνήθως είναι 100Mbps) και η ανακάλυψη αυτών των δικτύων είναι ανέφικτη από το διαδίκτυο. Κάτι τέτοιο δε συναντιέται όμως στην Ελλάδα αλλά σε μεγάλα οικιστικά συγκροτήματα και σε ξενοδοχεία στην Ασία.

7.2.1.2 Πολυεκπομπή επιπέδου εφαρμογής

Στην Πολυεκπομπή ή πολυδιαμονή (multicast) με εφαρμογή όπως είπαμε και πριν , ειδικό λογισμικό για P2P συνδέσεις εγκαθίσταται ή χρησιμοποιείται από τους χρήστες του δικτύου, έτσι ο αρχικός κόμβος προωθεί την οπτικοακουστική ροή (βίντεο) και οι υπόλοιποι χρήστες το αναπαράγουν και ταυτόχρονα το αναδιανέμουν σε άλλους. Έτσι δεν υπάρχει ο κεντρικός server αλλά ένα ολόκληρο δίκτυο που χρησιμοποίει τους πόρους όλων των τερματικών που είναι στο δίκτυο.

Το λογισμικό ή οι συνδέσεις P2P έγιναν γνωστές με την υπηρεσία του Napster. Οι χρήστες αντάλλαζαν αρχεία μουσικής στην αρχή λόγω ταχυτήτων την τότε εποχή μέσω της εφαρμογής Napster. Η Napster είχε ένα server ο οποίος λάμβανε την IP και τους τίτλους των τραγουδιών που είχε ο κάθε χρήστης για διανομή με τη σύνδεση του στο πρόγραμμα. Η συλλογή όλων αυτών των πληροφοριών δημιουργούσε μια μεγάλη βάση τίτλων τραγουδιών και IPs ,έτσι με αναζήτηση στη βάση, κάθε χρήστης μπορούσε να βρει ποιοί χρήστες μοιράζουν το αρχείο που θέλει και κατεβάζοντας κομμάτι κομμάτι από τον κάθε χρήστη-δότη να λάβει όλο το αρχείο μουσικής σε γρήγορο χρόνο. Αυτό το μοντέλο όμως της κεντρικής διαχείρισης δημιούργησε συμφόρηση αφού με αύξηση χρηστών αυξανόντουσαν οι ερωτήσεις στο server. Η διακοπή όμως του Napster δεν ήρθε από την συμφόρηση αλλά από τα νομικά προβλήματα που πρόεκυψαν από τη λειτουργία του. Συγκεκριμένα οι εταιρείες της μουσικής βιομηχανίας βλέποντας τους χρήστες να ανταλλάζουν αρχεία μουσικής παρά να τα αγοράζουν κινήθηκαν νομικά κατά του server και πέτυχαν το κλείσιμο του (λειτούργει επί πληρωμή τώρα με άλλους διαχειριστές)και μεγάλες αποζημιώσεις. Αν και κέρδισαν οι εταιρίες μια μάχη δε κέρδισαν τον πόλεμο (στην ουσία τον έχασαν)με τη έλευση παρόμοιων εφαρμογών(torrents,Kazza,Emule,gnutella,κα). Η δεύτερης γενιάς P2P εφαρμογές μεταφέρουν τη διαχείριση της βάσης στους χρήστες και υπάρχει απουσία

κεντρικού server έτσι είναι αδύνατον πρακτικά η μουσική βιομηχανία ή όποια άλλη βιομηχανία (πχ δορυφορική) να επέμβει. Οι τρόποι που χρησιμοποιούνται είναι η κατανομή της βάσης των αρχείων του δικτύου στα τερματικά που χρησιμοποιούν την εφαρμογή ή την καθόλου χρήση βάσης δεδομένων των αρχείων. Στην πρώτη περίπτωση οι χρήστες χωρίζονται ανά ομάδες με αρχηγό ομάδας ο οποίος είναι απλός χρήστης όπου στον υπολογιστή του διατηρεί βάση για τα αρχεία που διαθέτει η ομάδα του και μιλά με τους άλλους αρχηγούς. Οποίος χρήστης θέλει ένα αρχείο επικοινωνεί με τον αρχηγό ομάδας που ψάχνει το αρχείο μέσα στην ομάδα του πρώτα και μετά μέσω των αρχηγών των άλλων ομάδων στις άλλες ομάδες. Με το δεύτερο τρόπο κάθε χρήστης επικοινωνεί με το διπλανό του και του θέτει το ερώτημα για ένα αρχείο οι διπλανοί κόμβοι μεταφέρουν το ερώτημα στους διπλανούς τους και ούτω καθεξής έως να βρεθούν χρήστες που έχουν το αρχείο του ερωτήματος και να αρχίσει η αποστολή κομματιών από καθένα από αυτούς.

Με αυτό τον τρόπο τώρα των P2P συνδέσεων παρουσιαστήκαν εφαρμογές για live streaming. Ένας χρήστης ανεβάζει στο δίκτυο P2P ένα αρχείο βίντεο και αυτό διαμοιράζεται όπως διαμοιράζονται τα αρχεία στα P2P δίκτυα. Έτσι η θέαση των αθλητικών αγώνων των όποιων έχει αγοράσει τα δικαιώματα πανάκριβα ο πάροχος γίνεται μόνο με τη χρήση υπολογιστή σύνδεση στο internet και προγραμμάτων P2P live streaming όπως το ppstream,streamview,ustream και άλλα.

Αυτό το είδος multicast αποτελεί την πρωταρχική μέθοδο πειρατείας μέσω live streaming και αποτελεί τη μεγαλύτερη απειλή για τον πάροχο. Η ραγδαία αύξηση του internet έχει κάνει εντελώς απλό και εύκολο το ανέβασμα και τη θέαση μέσω του internet όλων των αθλητικών γεγονότων. Τα μέτρα που προσπαθούν να πάρουν οι πάροχοι είναι το water mark ,το SVP όπως και τα νομικά μέτρα κατά ιστοσελίδων που δημοσιεύουν links streaming αγώνων. Ξεκινώντας από το τρίτο δύσκολα θα αποτραπεί η live streaming πειρατεία αφού η παγκοσμιοποίηση του internet αποτελεί δικλίδα ασφαλείας για τους πειρατές. Το SVP (Secure Video Processor) ή άλλες τεχνολογίες υποστηρίζουν την τελική αποκρυπτογράφηση της εικόνας και του ήχου να μη γίνεται στο δέκτη αλλά στο εσωτερικό της τηλεόρασης με ειδικά κυκλώματα. Έτσι ένας χρήστης δε θα μπορεί να εξάγει το σήμα από την τηλεόραση και να το διοχετεύσει στο διαδίκτυο. Κάτι τέτοιο βέβαια απαιτεί την αναβάθμιση των τερματικών των χρηστών (τηλεοράσεις) με άλλες που εμπεριέχουν τα ειδικά αυτά κυκλώματα. Κάτι τέτοιο απαιτεί χρήματα και χρόνο και δεν είναι βέβαιο ότι η επένδυση αυτή θα αποδώσει. Έτσι το μόνο μέτρο που θεωρώ και το πιο ισχυρό όπλο των παρόχων είναι το Watermark. Αυτό υποστηρίζει υπογραφή της εικόνας με τα στοιχειά της συνδρομητικής κάρτας που παρέχει το κλειδί για αποκρυπτογράφηση του σήματος. Η σφραγίδα αποθηκεύεται στο σήμα και δε μπορεί να εξαχθεί έστω και αν αυτό αντιγραφεί ή αποθηκευθεί. Έτσι με το που παρουσιάζεται ένας αγώνας στο διαδίκτυο ο πάροχος μπορεί να βρει από ποιό συνδρομητή εκπέμφθηκε (παράνομα) και να διακόψει τη συνδρομή του ανάλογου χρήστη και συνάμα το live streaming που προβάλλεται στο internet. Η μέθοδος υπήρχε από παλιά αλλά οι πειρατές τοποθετούσαν ένα logo(έμβλημα να το πω;) πάνω από τα στοιχειά της κάρτας κατά την εκπομπή για να μη φαίνονται τα στοιχεία της κάρτας στην τηλεόραση αλλά το logo. Οι πάροχοι επανήλθαν με νέα Watermark τα οποία δεν είναι αντιληπτά από το μάτι (μικρές κουκίδες) αλλά ειδικές συσκευές των αντιλαμβάνονται το Watermark και καταλαβαίνουν τα στοιχεία της κάρτας. Στην Ελλάδα ανακοινώθηκε ότι αυτή η μέθοδος θα χρησιμοποιηθεί για να εντοπιστούν οι καφετέριες και τα μπαρ που δεν πληρώνουν την ακριβή συνδρομή καφετέριας αλλά τη φτηνή οικιακή συνδρομή.

7.2.1.3 Ρητή Πολυεκπομπή

Η ρητή εκπομπή είναι η βέλτιστη μέθοδος multicast μετάδοσης στο internet. Ο αποστολέας αποστέλλει στο δίκτυο ένα αντίγραφο της ροής και οι δρομολογητές με τα κατάλληλα πρωτόκολλα είναι αυτοί που αναλαμβάνουν να δημιουργήσουν τον κατάλληλο αριθμό αντιγράφων και να το διανέμουν στους χρήστες που ζητούν τη μετάδοση. Έτσι ούτε ο αποστολέας καταπονείται ούτε το δίκτυο αφού όπως δείχνει και το σχήμα 2(γ) δεν εμφανίζει το δίκτυο πουθενά πάνω από μια ροή πληροφορίας στην ίδια γραμμή. Τα πρωτόκολλα που χρησιμοποιούνται είναι το IGMP(internet group managment protocol, πρωτόκολλο διαχείρισης ομάδων διαδικτύου). Ενώ οι αλγόριθμοι δρομολόγησης Πολυεκπομπή επιπέδου δικτύου (PIM,DVRP,MOSPF) συντονίζουν τους δρομολογητές πολυεκπομπής. Όπως αναφέραμε μόνο το ΕΔΕΤ προσφέρει αυτές τις υπηρεσίες στην Ελλάδα και αν υπάρξει η υποστήριξη και από τους παρόχους θα είναι βέβαιο ότι η πειρατεία video streaming θα γνωρίσει αποθέωση.

7.3 Βιβλιογραφία

Computer Networking and the Internet, fifth edition: Fred Halsall

The Technology of Video and Audio Streaming, Second Edition: David Austerberry

Δικτύωση Υπολογιστών, Kurose & Ross, Εκδόσεις Μ. Γκιούρδας

Δίκτυα Υπολογιστών, Andrew Tanenbaum, Εκδόσεις Κλειδάριθμος

Τεχνολογίες-Διαδικτύου, Ι. Βενιέρης, Ε. Νικολούζου, Εκδόσεις Τζιόλας

Περιοδικό ''Δορυφορικά Νέα'' τεύχος Μάιος 2008
Περιοδικό ''Δορυφορικά Νέα'' τεύχος Νοέμβριος 2006

www.wikipedia.org