ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΔΙΔΑΚΤΙΚΗΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ
&ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών
«Διδακτική της Τεχνολογίας και Ψηφιακών Συστημάτων»

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ

ΑΝΑΛΥΣΗ ΤΗΣ ΓΡΗΓΟΡΗΣ ΔΙΑΔΙΚΑΣΙΑΣ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ ΣΤΑ ΕΤΕΡΟΓΕΝΗ ΔΙΚΤΥΑ 3G-WLAN

ΑΓΓΕΛΟΣ ΖΕΝΕΤΟΣ ΜΕ/0655

Υπεύθυνος Καθηγητής
ΧΡΙΣΤΟΣ ΞΕΝΑΚΗΣ

ΠΕΙΡΑΙΑΣ
Οκτώβριος 2008

Περίληψη

Οι ασύρματες επικοινωνίες είναι, από οποιαδήποτε άποψη, το ταχύτερο αναπτυσσόμενο τμήμα της βιομηχανίας επικοινωνιών. Τα κυψελοειδή συστήματα έχουν γνωρίσει εκθετική αύξηση κατά τη διάρκεια της τελευταίας δεκαετίας και υπάρχουν αυτήν την περίοδο περίπου δύο δισεκατομμύριο χρήστες παγκοσμίως. Πράγματι, τα κινητά τηλέφωνα έχουν γίνει ένα κρίσιμα επιχειρησιακό εργαλείο και ένα μέρος της καθημερινής ζωής στις περισσότερες αναπτυγμένες χώρες, και αντικαθιστούν γρήγορα τα απαρχαιωμένα συστήματα καλωδιώσεων σε πολλές αναπτυσσόμενες χώρες.

Επιπλέον, τα ασύρματα δίκτυα τοπικής περιοχής(WLAN) συμπληρώνουν αυτήν την περίοδο ή αντικαθιστούν τα καλωδιωμένα δίκτυα σε πολλές σπίτια, επιχειρήσεις, και πανεπιστημιουπόλεις. Πολλές νέες εφαρμογές , συμπεριλαμβανομένων των ασύρματων δικτύων αισθητήρων, τα έξυπνα σπίτια και συσκευές, και την απομακρυσμένη τηλεϊατρική, προκύπτουν από ερευνητικές ιδέες βασισμένες στα συγκεκριμένα συστήματα.

Η εκρηκτική ανάπτυξη των ασύρματων συστημάτων σε συνδυασμό με τον πολλαπλασιασμό των υπολογιστών παλάμης lap-tops και palmtops συστήνουν ένα φωτεινό μέλλον για τα ασύρματα δίκτυα, και ως αυτόνομα συστήματα αλλά και ως τμήμα της μεγαλύτερης υποδομής δικτύωσης.

Ωστόσο, πολλές τεχνικές προκλήσεις παραμένουν στο σχεδιασμό των στιβαρών ασύρματων δικτύων προκειμένου να παρέχουν την απαιτούμενη απόδοση ώστε να υποστηρίζουν τις αναδυόμενες εφαρμογές.

Τα τελευταία 30 χρόνια, οι βιομηχανίες τεχνολογίας πληροφοριών (IT) έχουν βιώσει δύο μεγάλα κύματα της επανάστασης, το ένα είναι η εφεύρεση του Διαδικτύου, και το άλλο οι ευρείες εφαρμογές των ασύρματων τεχνολογιών. Οι τεχνολογίες Διαδικτύου για πρώτη φορά στη ιστορία της ανθρωπότητας παρέχουν σε μας μια υποδομή παροχής ταχύτατων πληροφοριών μέσω των παγκόσμιων ιστών οπτικής ίνας που καλύπτουν ουσιαστικά κάθε γωνία του κόσμου. Επιπλέον, η δυνατότητα της διπλής κατεύθυνσης ανταλλαγής πληροφοριών στο διαδίκτυο έχει προκαλέσει θεμελιώδεις αλλαγές σε πολλούς τομείς της ζωής μας. Για παράδειγμα, τα διηπειρωτικά τηλεφωνήματα δεν θεωρούνται πλέον οικονομική πολυτέλεια. Πολύ σύντομα σε καθέναν θα δίνεται το προνόμιο όλα τα τηλεφωνήματα φωνής (είτε εντός χώρας είτε διεθνή) να είναι δωρεάν, χάρη στην ευρεία δυνατότητα πρόσβασης του διαδικτύου σε όλο τον κόσμο. Ο πίνακας 1.1 παρουσιάζει κορυφαίες 20 χώρες με τους περισσότερους συνδρομητές Διαδικτύου στον κόσμο όπως καταγράφεται σε 2005.

Πίνακας 1-1 Κορυφαίες 20 χώρες με τους περισσότερους συνδρομητές Διαδικτύου στον κόσμο όπως καταγράφεται το 2005.

Country or region	Number of subscribers	Population in 2005	Penetration rate (%)	World percentage (%)
United States	202,888,307	296,208,476	68.5	21.6
China	103,000,000	1,282,198,289	7.9	11.0
Japan	78,050,000	128,137,485	60.9	8.3
Germany	47,127,725	82,726,188	57.0	5.0
India	39,200,000	1,094,870,677	3.6	4.2
United Kingdom	35,807,929	59,889,407	59.8	3.8
South Korea	31,600,000	49,929,293	63.3	3.4
Italy	28,610,000	58,608,565	48.8	3.0
France	25,614,899	60,619,718	42.3	2.7
Brazil	22,320,000	181,823,645	12.3	2.4
Russia	22,300,000	144,003,901	15.5	2.4
Canada	20,450,000	32,050,369	63.8	2.2
Spain	15,565,138	43,435,136	35.8	1.7
Indonesia	15,300,000	219,307,147	7.0	1.6
Mexico	14,901,687	103,872,328	14.3	1.6
Taiwan	13,800,000	22,794,795	60.5	1.5
Australia	13,784,966	20,507,264	67.2	1.5
Netherlands	10,806,328	16,316,019	66.2	1.2
Poland	10,600,000	38,133,891	27.8	1.1
Malaysia	9,513,100	26,500,699	37.9	1.1
Rest of the World	176,943,950	2,444,250,712	7.2	18.8
World total	938,710,929	6,420,102,722	14.6	100.0

Τα ασύρματα συστήματα έχουν επιτύχει πρωτοφανή διείσδυση στον χώρο των τηλεπικοινωνιών και συναγωνίζονται τις ενσύρματες σταθερές τηλεπικοινωνίες. Οι νέες εφαρμογές που απαιτούν υψηλό εύρος, έχουν θέσει νέες κατευθύνσεις σχετικά με το τι αναμένεται από τις ασύρματες επικοινωνίες τα επόμενα χρόνια. Με βάση αυτές τις νέες τάσεις η ζήτηση για συμπληρωματικότητα των συστημάτων δεύτερης γενιάς όπως τα GSM, PDC, DECT και άλλα, κρίνεται απαραίτητη. Το UMTS κατά συνέπεια έχει αναπτυχθεί ως μία κοινή προσπάθεια πολλών εταιριών και διαχειριστών επικοινωνιών. Το UMTS είναι μία απόδειξη της συνένωσης των συστημάτων μεταγωγής πακέτου και κυκλώματος παρέχοντας στους χρήστες μεγαλύτερη ευελιξία. Όλες αυτές οι αλλαγές, απαιτούν αυξημένα χαρακτηριστικά ασφάλειας τα οποία να είναι ικανοποιητικά και πρακτικά.

Η ανάγκη για ασφαλής λύσεις διατηρώντας την ακεραιότητα, την εμπιστευτικότητα και την προστασία κατά της απάτης κρίνεται απαραίτητη. Ειδικά μιας και το UMTS έχει γίνει παγκοσμίως διαδεδομένο. Όμως τέτοιες λύσης ασφάλειας πρέπει να έχουν την δυνατότητα αναβάθμισης ώστε να είναι συμβατές με την μελλοντική υπολογιστική δύναμη, η οποία ενδεχομένως μπορεί να χρησιμοποιηθεί για να σπάσει τους σημερινούς αλγορίθμους.

Στη παρούσα εργασία στο πρώτο κεφάλαιο γίνεται αναφορά στην εξέλιξη των ασύρματων δικτύων τηλεπικοινωνιών και στην μελλοντική ανάπτυξη τους.

Στο δεύτερο κεφάλαιο εξετάζεται το ασύρματο δίκτυο κινητών επικοινωνιών UMTS, η αρχιτεκτονική του και τα μέλη από τα οποία αποτελείται.

Στο τρίτο κεφάλαιο αναλύεται το ασύρματο LAN δίκτυο, ο αρχιτεκτονικός σχεδιασμός του καθώς και τα πρωτόκολλα που έχουν αναπτυχθεί παρέχοντας ποικιλομορφία στις δυνατότητες των ασύρματων LAN δικτύων.

Στο τέταρτο κεφάλαιο γίνεται αναφορά στα σύγχρονα ασύρματα δίκτυα κινητών επικοινωνιών, όπως το B3G δίκτυο. Αναλύεται η αρχιτεκτονική του δικτύου καθώς και τα δικτυακά μέρη που το απαρτίζουν. Αποτελείται κατά κύριο λόγω από το UMTS δίκτυο και την WLAN τεχνολογία επιτρέποντας στους χρήστες να μετακινούνται ελεύθερα στα δύο δίκτυα.

Στο πέμπτο κεφάλαιο αναλύεται η διαδικασία AKA, όπου είναι η βασικότερη διαδικασία αυθεντικοποίησης του χρήστη στο δίκτυο και του δικτύου στο χρήστη. Αποτελεί αναπόσπαστο κομμάτι των ασύρματων επικοινωνιών μιας και καμία παρεχόμενη υπηρεσία δεν μπορεί να εκτελεστεί εάν δεν έχει πραγματοποιηθεί προηγουμένως η διαδικασία AKA.

Στο έκτο κεφάλαιο παρουσιάζονται τα αποτελέσματα της προσομοίωσης και η γραφική παράσταση που προέκυψε από τις διάφορες τιμές εισόδου. Αναλύεται επίσης η μέθοδος discrete event simulation (προσομοίωση διακριτών γεγονότων) πάνω στην οποία βασίστηκε ο κώδικας της προσομοίωσης.

Πίνακας Περιεχομένων

Πίνακας Εικόνων-Πινάκων

1. ΕΙΣΑΓΩΓΗ

Η εντυπωσιακή εξέλιξη των δικτύων κινητής τηλεφωνίας και οι δυνατότητες των ασύρματων πολυμέσων επικοινωνίας δημιουργούν πολλά ερωτηματικά στους διαχειριστές, κατασκευαστές και επιστήμονες που εργάζονται σε αυτόν τον τομέα. Το μελλοντικό σενάριο είναι ανοιχτό σε πολλές εναλλακτικές λύσεις: σκέψεις, προτάσεις, και δραστηριότητες του κοντινού μέλλοντος μπορούν να παρέχουν απάντηση σε πολλά ανοικτά σημεία και να υπαγορεύσουν τις μελλοντικές τάσεις του ασύρματου κόσμου.

Το μέλλον στις ασύρματες επικοινωνίες βασίζεται στο να παρέχουν και να υποστηρίζουν όλες τις υπηρεσιών πολυμέσων, όπως δεδομένα, γραφικά, ήχο, εικόνες και βίντεο, για διαφορετικές κατηγορίες χρηστών: (1) οι χρήστες δεν συνδέονται ενσύρματα στο δίκτυο. (2) χρήστες μπορούν να έχουν πρόσβαση στο δίκτυο από πολλές τοποθεσίες (δηλαδή, νομαδικούς χρήστες) και (3) οι χρήστες μπορούν να έχουν πρόσβαση στο δίκτυο, ενώ μετακινούνται συνεχώς μέσα σε αυτό. (δηλαδή, χρηστών κινητής τηλεφωνίας).

Το 2008-2010 η αγορά των υπηρεσιών πολυμέσων, θα αντιμετωπίσει μια μεγάλη αύξηση, με κινητήριο μοχλό της υπηρεσίες δεδομένων που παρέχονται από το διαδίκτυο(Internet). Η προοπτική της σημερινής κοινωνίας της πληροφορίας απαιτεί μια πολλαπλότητα των συσκευών, συμπεριλαμβανομένου των Internet Protocol (IP)-enabled οικιακών συσκευών, αυτοκίνητα, τους προσωπικούς υπολογιστές, αισθητήρες, ενεργοποιητές, που όλα πρέπει να είναι ολικώς συνδεδεμένα. Τα τρέχοντα κινητά και ασύρματα συστήματα και οι αρχιτεκτονικές έννοιες πρέπει να εξελιχθούν ώστε να αντιμετωπισθούν αυτές οι περίπλοκες απαιτήσεις συνδεσιμότητας. Η επιστημονική έρευνα σε αυτόν τον πραγματικά διεπιστημονικό τομέα αυξάνεται με ταχείς ρυθμούς. Νέες τεχνολογίες, νέες αρχιτεκτονικές έννοιες, και νέες προκλήσεις εμφανίζονται. Ένα μεγαλύτερο εύρος γνώσης, που θα κυμαίνεται στα διαφορετικά επίπεδα της στοίβας του πρωτοκόλλου, απαιτείται από όλους τους εμπειρογνώμονες που συμμετέχουν στην έρευνα, στη σχεδίαση, στη ανάπτυξη και στις πτυχές των μελλοντικών ασύρματων δικτύων.

Η σχεδίαση δικτύων, χρησιμοποιώντας την αρχιτεκτονική των ανοιχτών συστημάτων διασύνδεσης(Open Systems Interconnection – OSI) έχει μια ικανοποιητική προσέγγιση για ενσύρματα δίκτυα κυρίως όταν οι τηλεπικοινωνιακές συνδέσεις που εγκαθίστανται καλούνται να παράγουν ρυθμούς δεδομένων gigabit-ανά-δευτερόλεπτο (Gbps) και ρυθμούς σφάλματος (BERs) τάξης 10^{-12}. Τα ασύρματα κανάλια συνήθως έχουν πολύ χαμηλότερους ρυθμούς δεδομένων (της τάξης μερικών Mbps), υψηλότερο BERs (της τάξη10^{-2} έως 10^{-6}), και επιδεικνύουν σποραδικά σφάλματα και διαλείπουσα συνδεσιμότητα. Αυτά τα χαρακτηριστικά επίδοσης μεταβάλλονται ανάλογα την τοπολογία του δικτύου και την συμφόρηση των χρηστών επίσης διαφέρουν από χρόνο σε χρόνο. Κατά συνέπεια, καλές επιδόσεις του ασύρματου δικτύου δεν μπορούν να πραγματοποιηθούν χωρίς μια πραγματικά βελτιστοποιημένη, ολοκληρωμένη και προσαρμοστική σχεδίαση δικτύου. Κάθε επίπεδο της στοίβας πρωτοκόλλου θα πρέπει να προσαρμόζεται στις παραλλαγές της ασύρματης σύνδεσης με κατάλληλο τρόπο λαμβάνοντας υπ' όψιν της προσαρμοστικές στρατηγικές των άλλων επιπέδων προκειμένου να βελτιστοποιηθεί η απόδοση του δικτύου. Σε αυτό το εισαγωγικό κεφάλαιο περιγράφονται τα βασικά στάδια της εξέλιξης από το τρέχοντα ετερογενή ασύρματα δίκτυα προς τις μελλοντικές ολοκληρωμένες διαδικτυακές υπηρεσίες πολυμέσων δικτύου.

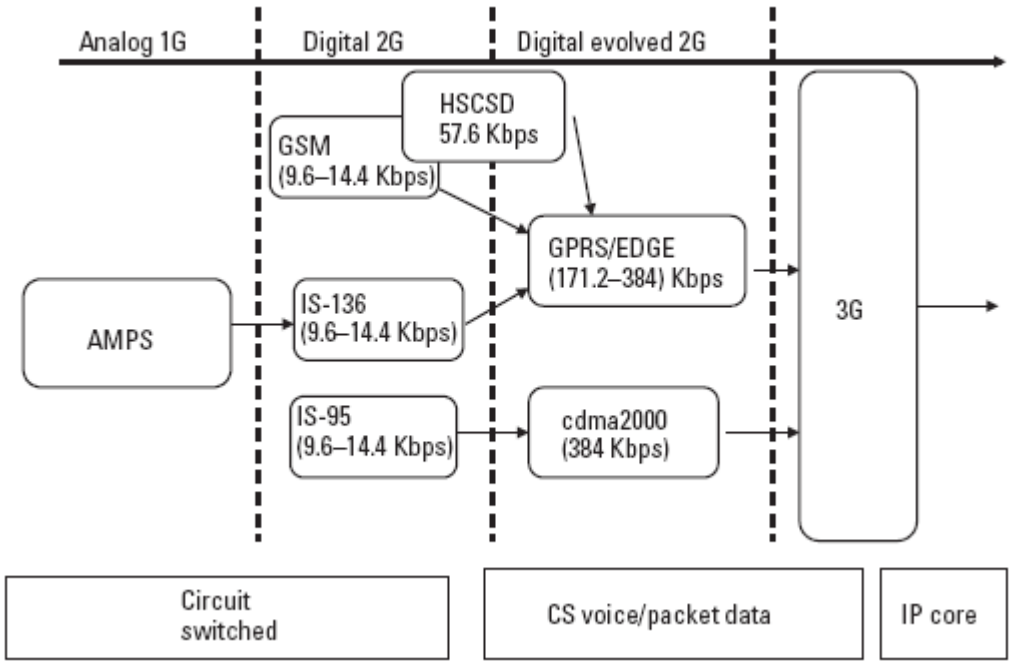
1.1 Επανάσταση των κινητών δικτύων

Τα κύρια επιτεύγματα στην εξέλιξη των δικτύων κινητής τηλεφωνίας, από τα δεύτερης γενιάς (2G) συστήματα προς αυτά της τρίτης γενιάς (3G) μέσω του λεγόμενου "εξελιγμένο" (evolved) 2G, επισημαίνονται στις παραγράφους που ακολουθούν. Η μετάβαση από γενιά σε γενιά δεν χαρακτηρίζεται μόνο από αύξηση στους ρυθμούς δεδομένων, αλλά και από τη μετάβαση από τα circuit-switched(CS) συστήματα στα CS-voice/packed δεδομένα και στα συστήματα που βασίζονται στο πρωτόκολλο IP, όπως επισημαίνεται και στην Εικόνα 1.1.

1.1.1 2ης Γενιάς εξελιγμένα συστήματα

Η δεύτερη γενιά συστημάτων αποτελεί ένα ορόσημο στο κινητό κόσμο, που αντιστοιχεί με την εισαγωγή των ψηφιακών κυψελωτών επικοινωνιών. Η εξέλιξη από την πρώτη γενιά (1G) των αναλογικών συστημάτων σήμαινε το πέρασμα σε ένα νέο σύστημα, διατηρώντας παράλληλα την ίδια προσφερόμενη υπηρεσία: φωνή.

Η επιτυχία των συστημάτων 2G, η οποία επεκτείνει το παραδοσιακό δημόσιο τηλεφωνικό δίκτυο (PSTN) ή το ψηφιακό δίκτυο ενοποιημένων υπηρεσιών (ISDN) και επιτρέπουν την πανεθνική ή ακόμη και σε παγκόσμιο επίπεδο και αδιάκοπη περιαγωγή με την ίδια κινητή συσκευή, είναι τεράστια.



Εικόνα 1-1 Επανάσταση των κυψελοειδών επικοινωνιών από τα 2G στα 3G συστήματα

Σήμερα το πιο επιτυχημένο κινητό ψηφιακό κυψελωτό σύστημα είναι το παγκόσμιο σύστημα για κινητές επικοινωνίες (GSM) με χρήστες σε περισσότερες από 174 χώρες. Το 2001 έχουν αναφερθεί περισσότεροι από 600 εκατ. συνδρομητές, και οι προβλέψεις δίνουν ότι ο αριθμός των συνδρομών θα υπερβαίνει το 1,5 δισ. ευρώ μέχρι το 2009. Το GSM είναι το μοναδικό ψηφιακό σύστημα στην Ευρώπη, με πάνω από 320 εκατομμύρια χρήστες.
Στην Ιαπωνία λειτουργεί το Προσωπικό Ψηφιακό Κυψελοειδές Σύστημα (PDC). Στην Ηνωμένες Πολιτείες η ψηφιακή αγορά χωρίζεται σε πολλά συστήματα, το σύστημα που

χρησιμοποιεί πολυπλεξία διαίρεσης χρόνου (TDMA) , το σύστημα που χρησιμοποιεί πολυπλεξία διαίρεσης κώδικα (CDMA). και το σύστημα GSM. Αυτός ο κατακερματισμός έχει οδηγήσει σε σοβαρά προβλήματα όσον αφορά την κάλυψη και την διαθεσιμότητα των υπηρεσιών. Το 32% των συνδρομητών κινητών στις Ηνωμένες Πολιτείες και στον Καναδά, εξακολουθούν να χρησιμοποιούν το αναλογικό σύστημα προηγμένων υπηρεσιών κινητής τηλεφωνίας (AMPS).

Τα 2G κινητά συστήματα εξακολουθούν να χρησιμοποιούνται κατά κύριο λόγο για φωνητική κίνηση. Οι βασικές εκδόσεις τυπικά εφαρμόζουν ένα κύκλωμα μεταγωγής υπηρεσίας, που εστιάζεται στις υπηρεσίες φωνής, και προσφέρουν χαμηλό ρυθμό δεδομένων (9.6-14.4 Kbps).

Οι μεταβατικές τεχνολογίες μεταξύ των 2G και 3G συστημάτων έχουν προταθεί για να επιτύχουν ταχύτερο ρυθμό δεδομένων και με χαμηλότερο κόστος απ 'ό, τι τα συστήματα τρίτης γενιάς. Τα εξελιγμένα συστήματα χαρακτηρίζονται από υψηλότερους ρυθμούς δεδομένων (64-384 Kbps) και τα δεδομένα παρέχονται σε μορφή πακέτων.

Στη συνέχεια, τονίζονται μερικές από τις μεγαλύτερες εξελιγμένες τεχνολογίες των συστημάτων 2G προκειμένου να παραστεί η εξελικτική διαδρομή των κινητών δικτύων προς την εποχή των πολυμέσων.

1.1.1.1 High-Speed Circuit-Switched Data

Εντός του πλαισίου της 2G τεχνολογίας το κύκλωμα μεταγωγής δεδομένων υψηλών ταχυτήτων (HSCSD) προέρχεται από την ανάγκη να επιλυθούν προβλήματα που σχετίζονται με την καθυστέρηση του δικτύου GSM στη μετάδοση δεδομένων.

Στην πραγματικότητα, το GSM υποστηρίζει μετάδοση δεδομένων με ρυθμό δεδομένων πάνω απο 9,6 έως 14,4 Kbps στη λειτουργία μεταγωγής κυκλώματος και τη μεταφορά καναλιών σηματοδοσίας με πακέτα μικρού μήκους (μέχρι 160 χαρακτήρες).

Το HSCSD είχε προταθεί από το ETSI στις αρχές του 1997. Η βασική ιδέα είναι να αξιοποιηθούν περισσότερες από μία χρονοθυρίδες παράλληλα, ανάμεσα από τις οκτώ διαθέσιμες χρονοθυρίδες, με ανάλογη επαύξηση των ρυθμών δεδομένων. Το HSCSD επιτρέπει στο χρήστη να έχει πρόσβαση, για παράδειγμα, στο LAN μιας εταιρίας, να στέλνει και να λαμβάνει e-mail και να έχει πρόσβαση στο Internet, ενώ βρίσκεται εν κινήσει. Προς το παρόν είναι διαθέσιμο σε 90 εκατομμύρια συνδρομητές σε 25 χώρες.

Από την άλλη πλευρά, η HSCSD υπηρεσία δεν εκμεταλλεύεται αποτελεσματικά την κατά ριπάς φύση της κίνησης των δεδομένων (π.χ.,περιήγηση στο Web, e-mail, WAP). Τα κανάλια είναι δεσμευμένα κατά τη διάρκεια της σύνδεσης. Επιπλέον, η εκμετάλλευση περισσότερων χρονοθυρίδων ανά χρήστη σε ένα κύκλωμα μεταγωγής πακέτων οδηγεί σε δραστική μείωση των διαθέσιμων καναλιών για τους χρήστες φωνητικών υπηρεσιών. Για παράδειγμα, τέσσερις HSCSD χρήστες, με τέσσερις διαθέσιμες χρονοθυρίδες ο καθένας, αποτρέπουν 16 χρήστες φωνητικών υπηρεσιών να έχουν πρόσβαση στο δίκτυο.

Συνεπώς, υπάρχει ανάγκη για ένα δίκτυο μεταγωγής πακέτου που θα παρέχει μία πιο αποδοτική εκμετάλλευση των πόρων.

Η υπηρεσία HSCSD μπορεί να θεωρηθεί ως ένα πρώτο βήμα προς τη μεταβατική τεχνολογία μεταξύ των 2G συστημάτων και των εξελιγμένων (evolved) 2G συστημάτων.(Εικόνα 1.1).

1.1.1.2 I - MODE

Μια μεγάλη επιτυχία στην Ιαπωνία έχει επιτευχθεί από τις υπηρεσίες i-mode, που καθιερώθηκε στις αρχές του 1999, οι οποίες παρέχονται από το PDC σύστημα. Το i-mode, ως εκ τούτου, αντιπροσωπεύει ένα μεταβατικό βήμα από το PDC προς την κατεύθυνση των 3G συστημάτων.

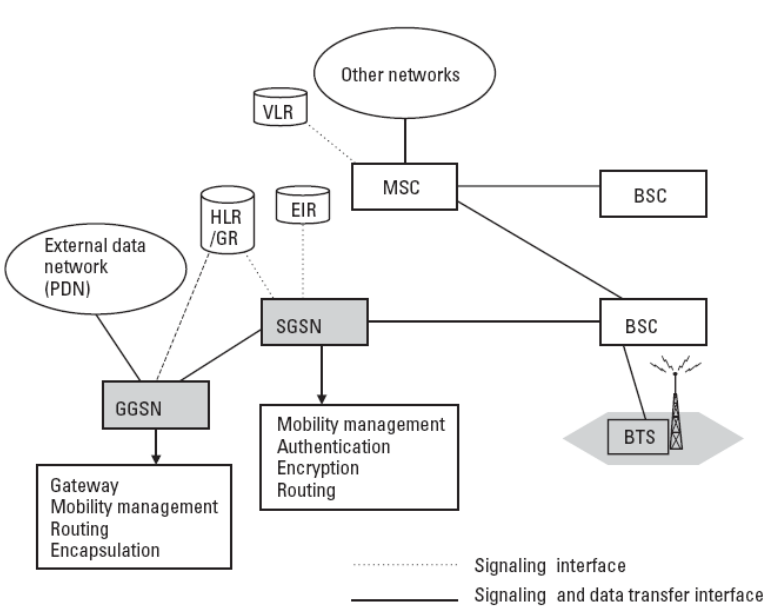
Η υπηρεσία i-mode χρησιμοποιεί το συμπαγές πρωτόκολλο HTML, διευκολύνοντας έτσι τη διασύνδεση με το Internet. Οι συνδρομητές μπορούν να στέλνουν και να λαμβάνουν e-mail και να έχουν πρόσβαση σε μια μεγάλη ποικιλία συναλλαγών, σε ψυχαγωγικές υπηρεσίες,

περιήγηση σε Web sites και σελίδες. Η υπηρεσία i-mode είναι πολύ φιλική προς το χρήστη και όλες οι οδηγίες μπορούν να διαχειρίζονται μόνο από 10 πλήκτρα.

1.1.1.3 General Packet Radio Service and Enhanced Data Rates for GSM Evolution

Η υπηρεσία General Packet Radio Service (GPRS) και η Enhanced Data Rates for GSM Evolution(EDGE) έχουν εισαχθεί ως μεταβατικές τεχνολογίες για την εξέλιξη του δικτύου GSM.

Παρέχονται υψηλοί ρυθμοί δεδομένων, δεδομένου ότι οι GPRS χρήστες μπορούν να εκμεταλλευτούν περισσότερες από μία χρονοθυρίδες παράλληλα, αντίθετα με την τεχνολογία HSCSD, και ο αριθμός των χρονοθυρίδων που ανατίθενται σε ένα χρήστη ποικίλη (π.χ., μπορεί να μειωθούν σε περίπτωση ανεπάρκειας των πόρων για τη φωνητική υπηρεσία). Ο μέγιστος θεωρητικά ρυθμός bit του GPRS είναι 171,2 Kbps (με χρήση οκτώ χρονοθυρίδων). Τρέχουσες τιμές αιχμής είναι 20/30 Kbps. Μία διαφορά με το GSM, εντοπίζεται στο multiframe. Ενώ στο GSM το multiframe αποτελείται από 51 frames(1 TDMA frame περιέχει 8 tsl), στο GPRS το multiframe αποτελείται από 52 frames. Κάθε τέτοιο multiframe αποτελείται από 12 radio blocks των 4 TDMA radio frames, 2 κενά frames και 2 frames για το PTCCH. ΄Ενα radio block (20 ms) αντιπροσωπεύει τον ελάχιστο χρόνο που ανατίθεται σε ένα χρήστη. Αν ο χρήστης μεταδίδει ή λαμβάνει μεγάλα διαγράμματα δεδομένων, μπορεί να του δοθεί περισσότερα από ένα radio block. Το σύνολο αυτών των μπλοκ λαμβάνονται / μεταδίδονται από το κινητό του τερματικού σταθμού κατά τη διάρκεια λήψης / μετάδοσης της προσωρινής ροής δεδομένων (TBF), η οποία διατηρείται μόνο κατά τη διάρκεια της μεταφοράς δεδομένων. Μια σύνοδος μπορεί να αποτελείται από ένα ή περισσότερα TBFs τα οποία ενεργοποιούνται κατά τη διάρκεια της φάσης μετάδοσης / λήψης. Σε κάθε TBF αποδίδεται μια προσωρινή ταυτότητα (TFI) από το δίκτυο, η οποία είναι μοναδική και για τις δύο κατευθύνσεις. Για παράδειγμα, κατά τη διάρκεια της λήψης, κάθε κινητό τερματικό ακούει σε όλα τα radio blocks που υπάρχουν στο κεντρικό κανάλι, αλλά συλλέγει μόνο εκείνα με την κατάλληλη ετικέτα (π.χ., TFI). Αυτός ο μηχανισμός απλοποιεί τη διαχείριση των πόρων σε point-to-multipoint μεταδόσεις, όπως στο downlink (σταθμός βάσης-κινητό τερματικό), δεδομένου ότι κάθε σταθμός που λαμβάνει μπορεί να δεχθεί τα σωστά blocks. Αντίθετα προς το GSM, η GPRS υπηρεσία μπορεί να χειριστεί με ευελιξία ασύμμετρες υπηρεσίες, δεσμεύοντας διαφορετικό αριθμό χρονοθυρίδων στο uplink και στο downlink. Στην εικόνα 1.2 παρατίθεται το αρχιτεκτονικό μοντέλο GPRS.



Εικόνα 1-2 Το GSM – GPRS αρχιτεκτονικό μοντέλο.

1.1.2 Συστήματα 3ης Γενιάς (3G Systems) .

Η εξέλιξη από τα 2G συστήματα στα 3G χαρακτηρίζεται από μια επαναστατική αλλαγή από την εστίαση στη φωνή σε κινητές υπηρεσίες πολυμέσων, με την ταυτόχρονη υποστήριξη αρκετών τάξεων QoS σε μία μόνο ασύρματη διεπαφή.

Τα συστήματα τρίτης γενιάς μπορούν να προσφέρουν υψηλότερο ρυθμό δεδομένων, επιτρέποντας με τον τρόπο αυτό την ενεργοποίηση ενός πολύ ευρύτερου φάσματος υπηρεσιών. Έχουν εντοπιστεί τα ακόλουθα είδη υπηρεσιών.:

- Βασικές και ενισχυμένες υπηρεσίες φωνής, συμπεριλαμβανομένων εφαρμογών, όπως audio conferencing και voice mail.
- Υπηρεσίες χαμηλού ρυθμού δεδομένων, όπως μηνύματα, e-mail, φαξ.
- Υπηρεσίες μέτριου ρυθμού δεδομένων για τη μεταφορά αρχείων και την πρόσβαση στο Internet σε ποσοστά επί της τάξης των 64 Kbps έως 144 Kbps.
- Υπηρεσίες υψηλής ταχύτητας δεδομένων για την υποστήριξη high-speed packet and circuit-based πρόσβασης στο δίκτυο, καθώς και υποστήριξη υψηλής ποιότητας video conferencing με ρυθμούς
  υψηλότερους από 64 Kbps.
- Υπηρεσίες πολυμέσων, που παρέχουν ταυτόχρονες υπηρεσίες βίντεο, ήχου και δεδομένων για την υποστήριξη προηγμένων διαδραστικών εφαρμογών.
- Υπηρεσιών πολυμέσων, επίσης, ικανές να στηρίξουν διαφορετική ποιότητα απαιτούμενων υπηρεσιών για διαφορετικές εφαρμογές.

Το 1985 η Διεθνής Ένωση Τηλεπικοινωνιών (ITU) όρισε το όραμα για ένα 3G κυψελωτό σύστημα, όπου αρχικά ονομάστηκε Future Public Land MobileTelecommunications System (FPLMTS) και αργότερα μετονομάστηκε σε Διεθνής Κινητές Τηλεπικοινωνίες-2000 (IMT-2000). Το ITU έχει δύο μεγάλους στόχους για τα 3G ασύρματα συστήματα: παγκόσμια περιαγωγή και υπηρεσίες πολυμέσων. Η Παγκόσμια Διοικητική διάσκεψη ραδιοεπικοινωνιών (WARC'92) εντόπισε τις 1885 έως 2025 και 2110 έως 2200 MHz, ζώνες συχνοτήτων που πρέπει να διατίθενται σε όλο τον κόσμο για τα νέα συστήματα IMT-2000. Οι ζώνες αυτές θα διατεθούν με διάφορους τρόπους σε διάφορες περιοχές και χώρες. Μια κοινή φασματική κατανομή μαζί με μια κοινή διεπαφή αέρος και το πρωτόκολλο περιαγωγής, σχεδιασμένο για όλο τον κόσμο, μπορεί να ολοκληρώσει την παγκόσμια ικανότητα περιαγωγής. Για να υποστηρίξει ταυτόχρονα νέες υπηρεσίες πολυμέσων που απαιτούν πολύ υψηλότερο ρυθμό δεδομένων και καλύτερο QoS από τις υπηρεσίες γωνής, το 3G wireless σύστημα προβλέπει:

- Υψηλότερους ρυθμούς μετάδοσης δεδομένων υπηρεσιών: μέχρι 384 Kbps για κινητούς χρήστες και 2 Mbps για προκαθορισμένους χρήστες, με αύξηση έως 20 Mbps.
- Ευέλικτες διεπαφές αέρος, καθώς και πιο ευέλικτη διαχείριση των πόρων.

Η συμβατότητα με τα 2G συστήματα είναι επίσης ένας από τους κύριους στόχους των συστημάτων 3G. Διαφορετικές πρωτοβουλίες προσπάθησαν να ενοποιήσουν τις διαφορετικές προτάσεις που υποβλήθηκαν στο ITU το 1998 από το ETSI για την Ευρώπη, το Association of Radio Industries and Broadcasting (ARIB) και Telecommunications Technology Council (TTC) για την Ιαπωνία, και το American National Standard Institute (ANSI) για τις ΗνωμένεςΠολιτείες.

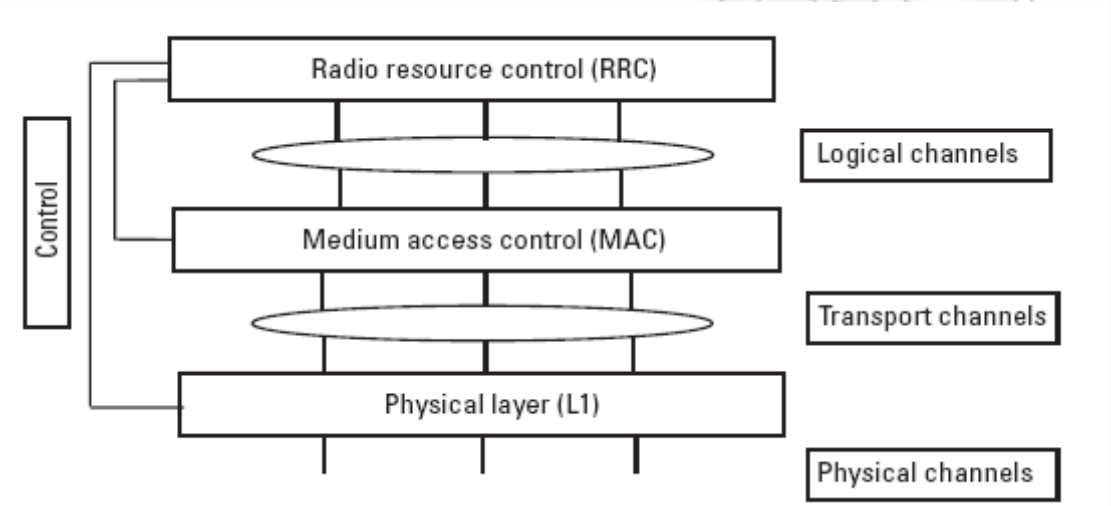
1.1.2.1 Universal Mobile Telecommunications System

Το Universal Mobile Telecommunications System (UMTS) είναι η Ευρωπαϊκή έκδοση του IMT-2000. Το UMTS Terrestrial Radio Access (UTRA) εγκρίθηκε από το ITU το Μάιο του 2000. Ένας τυπικός ρυθμός chip της τάξης των 3,84 Mcps χρησιμοποιείται για την κατανομή συχνότητας στα 5-MHz. Το Wideband CDMA(W-CDMA) το οποίο υποστηρίζεται από ομάδες της Ιαπωνίας(ARIB) και της Ευρώπης, και είναι συμβατό με το GSM, έχει επιλεγεί από το UTRA για αμφιδρόμηση με Διαίρεση Συχνότητας (Frequency Division DuplexFDD -

μονόδρομα υποκανάλια ,άλλο υποκανάλι για uplink και άλλο για downlink) ενώ το TD-έχει επιλεγεί από το UTRA για αμφιδρόμηση με διαίρεση Χρόνου (Time Division Duplex, TDD Αμφίδρομα Υποκανάλια το ίδιο υποκανάλι και για uplink και για downlink, και διαχωρισμός βάσει TDM).

Η εισαγωγή της λειτουργίας TDD είναι κυρίως λόγω των ασύμμετρων ζωνών συχνοτήτων που έχουν σχεδιαστεί από τον ITU. Επίσης, η ασύμμετρη φύση της κίνησης των δεδομένων σχετικά με τις αμφίδρομες συνδέσεις αναμένεται στην επόμενη γενιά των ασύρματων συστημάτων (π.χ., εφαρμογές Διαδικτύου) επομένως υποδηλώνει ότι η TDD λειτουργία θα μπορούσε να προτιμηθεί έναντι της FDD.

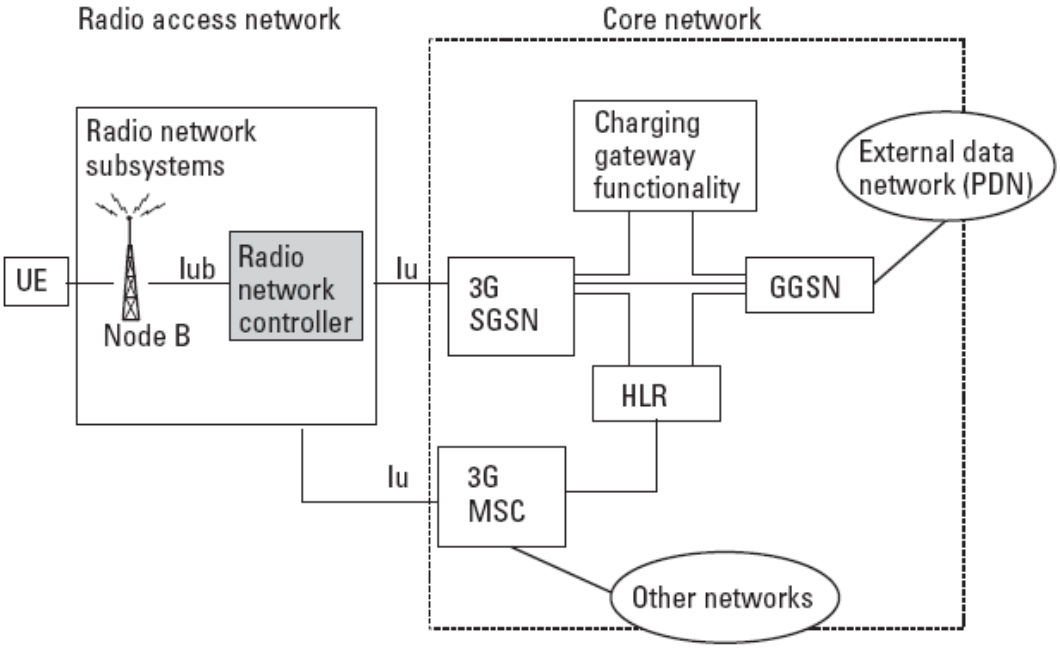
Η εικόνα 1.3 παρέχει μία ολική εικόνα για την αρχιτεκτονική των πρωτοκόλλων του UMTS Radio Access Network (UTRAN).



Εικόνα 1-3 Αρχιτεκτονική των πρωτοκόλλων ραδιοεπαφής στο UTRAN

Τα παραπάνω πρωτόκολλα (Εικόνα 1.3) μπορούν να χωριστούν σε τρία επίπεδα: το φυσικό στρώμα, το στρώμα σύνδεσης δεδομένων και το στρώμα δικτύου. Το στρώμα σύνδεσης δεδομένων χωρίζεται σε δύο υπο-στρώματα: Στο MAC και στο radio link control (RLC). Τα MAC πρωτόκολλα παρέχουν μια βελτιστοποιημένη πρόσβαση για την μετάδοση πακέτων δεδομένων μέσω της στατιστικής πολυπλεξίας ορισμένων χρηστών σχετικά με ένα σύνολο κοινών σταθμών. Έχουν ζωτική σημασία παρέχοντας την αποτελεσματικότερη αξιοποίηση των περιορισμένων ράδιο - πόρων. Τα πρωτόκολλα RLC παρέχουν αξιόπιστη μεταφορά πληροφοριών μέσω μηχανισμών αναμετάδοσης των σφαλμάτων. Το πρωτόκολλο RRC είναι μέρος του επιπέδου δικτύου και είναι υπεύθυνο για τη διαχείριση των πόρων.

Η εικόνα 1.4 παρουσιάζει την αρχιτεκτονική του UMTS δικτύου. Το UMTS αποτελείται από το δίκτυο πυρήνα (Core Network-CN) το οποίο συνδέεται με το UTRAN μέσω της διεπαφής I_u η οποία συγκεντρώνει όλη την κίνηση που προέρχεται από τους σταθμούς. Το UTRAN αποτελείται από ένα σύνολο ράδιο δικτυακών υποσυστημάτων (radio network sybsystems - RNS) που συνδέονται με το CN μέσω της διεπαφής I_u. Κάθε RNS είναι υπεύθυνο για τους πόρους των κυψελών του και κάθε κόμβος έχει μία ή περισσότερες κυψέλες. Το RNS είναι ανάλογο με το BSS στη GSM-GPRS αρχιτεκτονική, και αποτελείται από έναν radio network controller –RNC (κατά αντιστοιχία με το BSC) και από έναν η περισσότερους κόμβους B. Η εγκατάσταση ενός κόμβου B απαιτεί μια πλήρης αντικατάσταση των αναλογικών BTS, δεδομένου ότι πρέπει να χειρίζονται τις διαφορετικές διεπαφές αέρα που έχουν εισαχθεί στο W-CDMA. Ένας κόμβος B είναι συνδεδεμένος με το RNC μέσω της διεπαφής I_{ub}. Το RNC διαχωρίζει τη διαδικασία μεταγωγής κυκλώματος από τη μεταγωγή πακέτου και είναι υπεύθυνο για τη δρομολόγηση πρώτα στο 3G-MSC και ύστερα στο 3G-SGSN. Το 3G-MSC διαφοροποιείται από το GRPS-MSC για την αντιμετώπιση νέων αλγορίθμων συμπίεσης φωνής και κωδικοποίησης και επεξεργάζεται τη μεταγωγή κυκλώματος που διοχετεύεται σε αυτό από το RNC. Το MSC στη συνέχεια στέλνει τα δεδομένα στο PSTN και η πληροφορία δρομολογείται χρησιμοποιώντας το πρωτόκολλο IP-over-ATM. Το SGN τροποποιείται ώστε να διαχειριστεί την κίνηση από το AAL5 αλλά εκτελεί την ίδια λειτουργία με το GRPS.



Εικόνα 1-4 Αρχιτεκτονική δικτύου UMTS

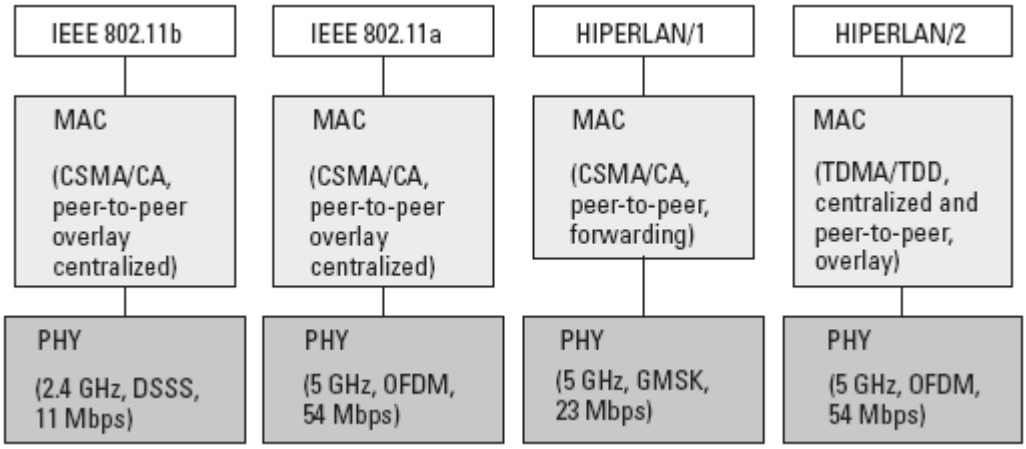
1.1.3 Ασύρματα δίκτυα τοπικής περιοχής (W-LANs) .

Μια άλλη σημαντική πτυχή της εξελικτικής πορείας των ασύρματων δικτύων αποτελούν τα ασύρματα τοπικά δίκτυα (WLANs). Η εξάπλωση των WLAN είναι εκρηκτική, με έρευνες να αναφέρουν ετήσια αύξηση 300%.

Τα WLAN συστήματα είναι μια τεχνολογία που μπορεί να προσφέρει εφαρμογές με πολύ υψηλό ποσοστό δεδομένων και μεμονωμένες συνδέσεις και αποτελεί ένα ελκυστικό τρόπο συγκρότησης δικτύων υπολογιστών σε περιβάλλοντα όπου η καλωδιακή εγκατάσταση είναι ακριβή ή δεν είναι εφικτή.

Τα WLAN συστήματα αντιπροσωπεύουν την ένωση δύο από τους ταχύτερα αναπτυσσόμενους κλάδους στη βιομηχανία των υπολογιστών: LANs και mobile computing, κεντρίζοντας έτσι την προσοχή των κατασκευαστών εξοπλισμού.

Ενώ στην αρχή των WLANs υπήρχαν αρκετά ιδιόκτητα προϊόντα, σήμερα είναι κυρίως συμβατά με το πρότυπο 802.11b(επίσης γνωστό ως Wi-Fi) όπως ορίζεται από το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE). Λειτουργεί σε συχνότητες 2.4 GHz στα 11 Mbps και αναμένεται να επεκταθεί για να φθάσει τα 20 Mbps. Μια περιγραφή της MAC μπορεί να βρεθεί στην εικόνα 1.5 η οποία απεικονίζει διαφορετικά πρότυπα WLAN.



Εικόνα 1-5 WLAN πρότυπα.

Στην Ευρώπη, ένα άλλο πρότυπο που ονομάζεται High Performance Local Area Network (HIPERLAN) έκανε χρήση του ελεύθερου (unlicensed) φάσματος των 5-GHz ,όπου είναι διαθέσιμο μεγαλύτερο εύρος ζώνης, παρέχοντας υψηλότερο ρυθμό μετάδοσης δεδομένων (HIPERLAN /1: 20 Mbps) και υψηλότερη ποιότητα συστημάτων πολυμέσων. Τα ασύρματα LAN επόμενης γενιάς, συμπεριλαμβανομένων των IEEE 802.11a και HIPERLAN / 2, προσφέρουν υψηλότερες επιδόσεις και μεγαλύτερο φάσμα ικανοτήτων.

Το HiperLAN (HIgh PErformance Radio LAN) είναι ένα Wireless LAN πρότυπο. Είναι μια ευρωπαϊκή εναλλακτική λύση για το πρότυπο IEEE 802,11. Η έννοια αυτή ορίζεται από το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων (ETSI). Στο ETSI τα πρότυπα ορίζονται από το έργο BRAN (Broadband Radio Access Networks). Το πρότυπο HiperLAN έχει τέσσερις διαφορετικές εκδόσεις. Επίσης λειτουργεί ως ένα οικιακό δίκτυο όπως το HiperLAN / 1. Το HiperLAN / 2 χρησιμοποιεί τη ζώνη των 5 GHz και ρυθμό δεδομένων πάνω από 54 Mbit / s.

Το πρότυπο HIPERLAN / 2 (54 Mbps), το οποίο επικυρώθηκε το 2000, διαφέρει από το IEEE 802.11a. Στην πραγματικότητα, τα HIPERLAN / 2 συστήματα χρησιμοποιούν ένα connection oriented πρωτόκολλο και προορίζονται για την υποστήριξη ποικιλίας υπηρεσιών φωνής, δεδομένων και πολυμέσων.

1.1.4 Ad Hoc δίκτυα και ασύρματα προσωπικά δίκτυα.

Πολλά WLANs του σήμερα χρειάζονται μια υποδομή δικτύου που θα παρέχει πρόσβαση σε άλλα δίκτυα και θα περιλαμβάνουν το MAC. Τα Ad hoc ασύρματα δίκτυα δεν χρειάζονται καμία υποδομή. Σε αυτά τα συστήματα οι κινητοί σταθμοί μπορεί να λειτουργήσουν ως ενδιάμεσοι κόμβοι σε ένα multihop περιβάλλον διάδοσης από κινητούς σταθμούς σε σταθμούς βάσης Οι Κινητοί σταθμοί έχουν τη δυνατότητα να υποστηρίξουν λειτουργίες των σταθμών βάσης.

Η οργάνωση του δικτύου βασίζεται σε μετρήσεις που λαμβάνονται από όλους τους κινητούς σταθμούς και τους σταθμούς βάσης για την αυτόματη και δυναμική οργάνωση του δικτύου σύμφωνα με την πραγματική παρέμβαση και με την τρέχουσα κατάσταση εκχώρησης του καναλιού προκειμένου να αξιολογηθούν οι νέες συνδέσεις για την βελτιστοποίηση της σύνδεσης.

Τα συστήματα αυτά θα παίξουν συμπληρωματικό ρόλο για την επέκταση της κάλυψης συστημάτων χαμηλής ισχύος και για τις εφαρμογές χωρίς άδεια. Μια κεντρική πρόκληση για το σχεδιασμό των ad hoc δικτύων είναι η ανάπτυξη ενός δυναμικού πρωτοκόλλου δρομολόγησης που να μπορεί να βρει αποτελεσματικά δρομολόγια επικοινωνίας μεταξύ δύο κόμβων. Μια Mobile Ad Hoc Networking (MANET) ομάδα εργασίας έχει συσταθεί στο πλαίσιο του Internet Engineering Task Force (IETF) ώστε να αναπτύξει ένα πλαίσιο δρομολόγησης που θα βασίζεται στο IP πρωτόκολλο στα ad hoc δίκτυα. Μια άλλη πρόκληση είναι η ορθή σχεδίαση του MAC πρωτόκολλου για multihop ad hoc δίκτυα.

2. ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΔΙΚΤΥΟΥ UMTS

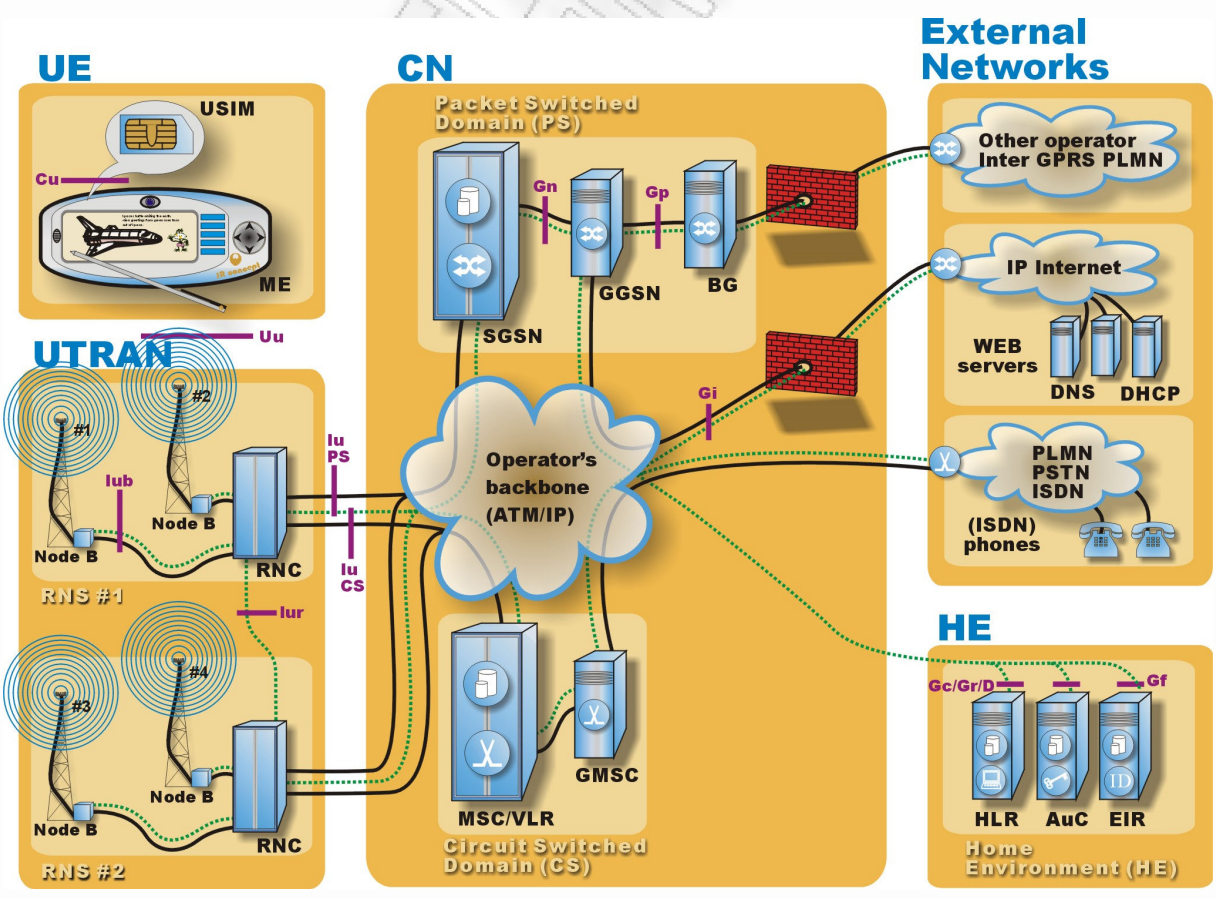
Το UMTS, Universal Mobile Telecommunications System είναι ένα σύστημα τρίτης γενιάς (3G) για το παγκόσμιο σύστημα κινητής επικοινωνίας. Από την πρώτη γενιά (αναλογική), συστήματα όπως το NMT μέσω συστημάτων δεύτερης γενιάς όπως το GSM, η βιομηχανία των κινητών επικοινωνιών , έχουν μεταφερθεί από τις απλές, χαμηλής ποιότητας υπηρεσίες φωνητικής τηλεφωνίας σε υψηλής ποιότητας καθώς και σε υπηρεσίες δεδομένων.

Το έργο έχει αναπτυχθεί μεταξύ άλλων από το ETSI, το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων και ξεκίνησε με την προοπτική να παράγει ρυθμούς μετάδοσης δεδομένων μεγαλύτερους από το GSM, να παρέχει νέες και περισσότερες υπηρεσίες προς τους τελικούς χρήστες και παρέχει ένα πραγματικά παγκόσμιο σύστημα. Το 3rd Generation Partnership Project(3GPP) είναι υπεύθυνο για την ανάπτυξη του συστήματος UMTS.

Το UMTS παρέχει τόσο μεταγωγή πακέτων όσο και μεταγωγή κυκλώματος, με την μεταγωγή πακέτων να παρέχει τον υψηλότερο ρυθμό δεδομένων, έως και 2Mbps ανά χρήστη.

Το κεφάλαιο αυτό παρέχει μια σύντομη εισαγωγή στο σύστημα UMTS και σε ενότητες όπως οι υπηρεσίες, οι κόμβους και οι διασυνδέσεις του δικτύου.

Στην εικόνα 2.1 παρουσιάζονται τα μέρη από τα οποία αποτελείται το UMTS σύστημα.



Εικόνα 2-1. Μέρη από τα οποία αποτελείται το UMTS σύστημα

2.1 Υπηρεσίες στο UMTS

Το UMTS προσφέρει συνδέσεις μεταγωγής πακέτων και κυκλώματος με ταχύτητες έως 384kbps στο CS και 2Mbps στο PS. Αυτό προσφέρει μια νέα σειρά υπηρεσιών προς τους κινούμενους χρήστες, όμοιες με αυτές που υπάρχουν σε δίκτυα σταθερής τηλεφωνίας και στο Internet. Οι υπηρεσίες αυτές περιλαμβάνουν βιντεοδιάσκεψη (video conferencing), υψηλότερες ταχύτητες μεταφοράς και υψηλή (CD) ποιότητα ήχου για το τερματικό. Ένα άλλο χαρακτηριστικό, το οποίο εισήχθη με την General Packet Radio Service (GPRS) είναι το να είναι «πάντα συνδεδεμένο» με το Internet.

2.2 Εξοπλισμός Χρήστη (UE)

Εξοπλισμός Χρήστη (UE) είναι το τελικό σημείο χρήσης του δικτύου UMTS. Η ανάπτυξη αυτού του τμήματος κατά κάποιο τρόπο καθοδηγεί τις εξελίξεις αναφορικά με το ποιες υπηρεσίες και εφαρμογές θα είναι διαθέσιμες στο χρήστη. Η τιμή πρέπει να είναι χαμηλή ταχύτητα ώστε να επιτρέψει στους χρήστες να αγοράσουν το νέο εξοπλισμό UMTS. Αυτό επιτυγχάνεται με την ενοποίηση των ραδιοφωνικών διεπαφών και την τοποθέτηση όλων των πληροφοριών του κάθε χρήστη σε έξυπνες κάρτες.

2.2.1 Τερματικά (Terminals)

Το σύγχρονο τηλέφωνο δεν είναι πλέον απλά ένα τηλέφωνο, με τα νέα δεδομένα υπηρεσιών που προσφέρονται, έχουν μετονομαστεί σε τερματικά. Οι μεγαλύτεροι κατασκευαστές έχουν παρουσιάσει διαφορετική έννοια των τερματικών σταθμών, αλλά λίγοι έχουν πράγματι προχωρήσει σε παραγωγή. Παρόλο που οι τερματικοί σταθμοί διαφέρουν σε μέγεθος και σχεδιασμό, όλοι τους έχουν μεγαλύτερες οθόνες και λιγότερα κουμπιά σε σύγκριση με τα 2G τηλέφωνα. Αυτό οφείλεται κυρίως στην αύξηση της χρήσης του τερματικού σταθμού, εξαιτίας τον όλο και περισσότερων υπηρεσιών δεδομένων που προσφέρονται και το τερματικό είναι έτσι συνδυασμούς από κινητό τηλέφωνο, μόντεμ και palmtop υπολογιστή.

Το τερματικό προσφέρει τρεις διασυνδέσεις. Οι δύο κύριες διασυνδέσεις είναι οι Uu διασυνδέσεις που ορίζουν το ραδιοφωνικό σύνδεσμο (Wideband Code Division multiple access interface). Φροντίζουν για όλες τις φυσικές συνδέσεις με το UMTS δίκτυο. Η Τρίτη είναι η Cu διασύνδεση ανάμεσα στο τερματικό και στην UMTS IC Card (UICC). Αυτή η διασύνδεση ακολουθεί την τυπική μορφή των έξυπνων καρτών.

Ακόμα και αν οι κατασκευαστές των τερματικών έχουν πολλές διαφορετικές ιδέες για το σχεδιασμό των τερματικών σταθμών, θα πρέπει να συμμορφωθούν με ένα ελάχιστο σύνολο συγκεκριμένων προτύπων, επιτρέποντας στους χρήστες να έχουν πρόσβαση σε ορισμένες βασικές λειτουργίες με τον ίδιο τρόπο, χρησιμοποιώντας διαφορετικά τερματικά

Τα πρότυπα αυτά περιλαμβάνουν :

- Τμήμα πληκτρολογίου (φυσικά ή εικονικά πλήκτρα οθόνης)
- Καταχώριση νέου κωδικού
- Η αλλαγή των κωδικών PIN
- Απεμπλοκή των PIN/PIN2
- Παρουσίαση του IMEI
- Χειρισμός των συμπληρωματικών υπηρεσιών
- Έλεγχος κλήσεων

Αφήνεται στους προγραμματιστές των τερματικών να αποφασίσουν για το υπόλοιπο υλοποίησης της διεπαφής του τερματικού σταθμού και ο χρήστης πιθανότατα θα επιλέξει το τερματικό που βασίζεται σε δύο κριτήρια, του σχεδιασμού και της διασύνδεσης. Η διασύνδεση

είναι ένας συνδυασμός του μεγέθους και των πληροφοριών που παρέχονται από την οθόνη (αφής) , τα κουμπιά και το μενού.

2.2.2 UICC

Η UMTS IC κάρτα είναι μία «έξυπνη» κάρτα και σαν υλικό παρουσιάζει μεγάλο ενδιαφέρων το πόση μνήμη και πόση επεξεργαστική ισχύ μπορεί να παρέχει. Στο UICC εκτελείται η εφαρμογή USIM.

2.2.3 USIM

Στο GSM σύστημα, η κάρτα SIM αποθηκεύει προσωπικές πληροφορίες (των συνδρομητών) κωδικοποιημένες «σκληρά» πάνω στην κάρτα. Αυτό έχει αλλάξει και στο UMTS, η UMTS Subscriber Identity Module (SIM) έχει τοποθετηθεί σαν εφαρμογή στο UICC. Αυτό επιτρέπει περισσότερες αιτήσεις ή / και κλειδιά / ηλεκτρονικών υπογραφών για άλλους σκοπούς που αποθηκεύονται στην USIM στο UICC (π.χ. κωδικούς πρόσβασης για ασφαλείς τραπεζικές συναλλαγές). Επίσης, δίνεται η δυνατότητα σε πολλές USIMs να συνυπάρχουν στην ίδια UICC, παρέχοντας έτσι την πρόσβαση σε πολλαπλά δίκτυα.

Η USIM περιέχει λειτουργίες και δεδομένα που απαιτούνται για την αναγνώριση και την αυθεντικοποίηση του συνδρομητή στο δίκτυο UMTS. Επίσης αντίγραφο του προφίλ των υπηρεσιών του συνδρομητή μπορεί να βρίσκεται αποθηκευμένο στην USIM.

Ο χρήστης θα πρέπει ο ίδιος να αυθεντικοποιεί τον εαυτό του στην USIM εισάγοντας ένα κωδικό PIN. Αυτό είναι για να βεβαιωθούμε ότι η πρόσβαση στο UMTS δίκτυο χορηγείται στον πραγματικό χρήστη. Το δίκτυο θα παρέχει υπηρεσίες σε όποιον χρησιμοποιεί το τερματικό με βάση την ταυτότητα USIM που ισχυρίστηκε, και όχι στον χρήστη.

2.3 UMTS Terrestrial Radio Access Network

Το UMTS Terrestrial Radio Access Network (UTRAN) αποτελεί τη σύνδεση ανάμεσα στο χρήστη και στο Core Network (CN). Αποτελείται από όλα τα στοιχεία για την παροχή UMTS επικοινωνιών στον αέρα και για τον έλεγχο αυτών. Το UTRAN είναι σήμερα το μοναδικό καθορισμένο Radio Access Network, αν και οι δορυφορικές επικοινωνίες έχουν συζητηθεί ως εναλλακτική λύση. Ένα άλλο πιθανό δίκτυο ραδιο πρόσβασης είναι το HIPERLAN, μια υψηλής ταχύτητας ασύρματη τεχνολογία LAN υπό ανάπτυξη.

Το UTRAN ορίζεται μεταξύ δύο διασυνδέσεων. Η Iu διεπαφή μεταξύ του UTRAN και CN, που χωρίζεται σε δύο μέρη, την PS Iu διεπαφή για τον τομέα μεταγωγής πακέτων και την Iu CS για το τομέα μεταγωγής κυκλώματος, και την Uu διεπαφή μεταξύ του UTRAN και εξοπλισμό των χρηστών.

Μεταξύ αυτών των διασυνδέσεων υπάρχουν δύο κόμβοι, οι RNC και οι σταθμοί βάσης Node B.

2.3.1 Radio Network Controller (RNC)

Ο Radio Network Controller (RNC) είναι υπεύθυνος για έναν ή περισσότερους σταθμούς βάσης Node B και ελέγχει τους ραδιοφωνικούς του πόρους. Είναι επίσης το σημείο παροχής υπηρεσιών για τις υπηρεσίες που παρέχει το UTRAN στο CN. Είναι συνδεδεμένο με το CN με δύο συνδέσεις, μία προς την τμήμα μεταγωγής πακέτων, το SGSN και μία προς το τμήμα μεταγωγής κυκλώματος, το MSC.

Ένα άλλο σημαντικό έργο των RNCs είναι η εμπιστευτική και ακέραια προστασία των δεδομένων. Μετά την αυθεντικοποίηση εφόσον οι διαδικασίες συμφωνίας κλειδιών έχουν πραγματοποιηθεί, τα κλειδια ακεραιότητας και εμπιστευτικότητας του συνδρομητή

τοποθετούνται στο RNC. Αυτά χρησιμοποιούνται στη συνέχεια μαζί στις λειτουργίες ασφάλειας, F8 και F9.

Ένα RNC μπορεί να έχει πολλαπλούς λογικούς ρόλους ανάλογα με το τι κόμβο εξυπηρετεί. Ο χρήστης συνδέεται με έναν Serving RNC. Όταν ο χρήστης μετακινείται και φτάνει σε ένα άλλο RNC ένα Drift RNC αναλαμβάνει τον έλεγχο των ραδιοφωνικών πόρων του χρήστη, αλλά το Serving RNC θα χειρίζεται ακόμα την σύνδεση με το CN. Ο τελευταίος ρόλος που ένα RNC μπορεί έχει είναι ο «Έλεγχος». Κάθε κόμβος Β ελέγχεται από ένα RNC που είναι υπεύθυνο για τους ραδιοφωνικούς του πόρους.

2.3.2 Node B

Οι σταθμοί βάσης έχουν ονομαστεί Node B στο UMTS και το έργο τους είναι να εκτελούν τις φυσικές ράδιο – συνδέσεις ανάμεσα στο τερματικό και στα ίδια. Δέχονται σήματα από την διασύνδεση Iub από το RNC και τα μετατρέπουν σε ράδιο σήματα με τη διασύνδεση Uu. Εκτελούν επίσης ορισμένες βασικές λειτουργίες διαχείρισης ράδιο – πόρων όπως ο «εσωτερικός βρόχος ελέγχου ισχύς». Αυτή είναι μια δυνατότητα για να αποτρέπεται το «near-far» πρόβλημα. Αυτό συμβαίνει όταν όλοι οι τερματικοί σταθμοί εκπέμπουν με την ίδια δύναμη, έτσι τα τερματικά που βρίσκεται πλησιέστερα προς τον κόμβο Β, θα καταπνίγουν το σήμα από τα τερματικά που βρίσκονται μακριά. Έτσι ο Node B ελέγχει την ισχύ που έλαβε από τους διάφορους τερματικούς σταθμούς και τους ενημερώνει για τη μείωση ή την αύξηση της ισχύς έτσι ώστε στον κόμβο Β να λαμβάνεται η ίδια ποσότητα ισχύος από κάθε τερματικό.

2.4 Core Network

Το Core Network (CN) χωρίζεται σε δύο μέρη, στον τομέα μεταγωγής πακέτων (PS) και στον τομέα μεταγωγής κυκλώματος (CS). Ο τομέας PS παρέχει υπηρεσίες δεδομένων στον χρήστη από τις συνδέσεις με το Διαδίκτυο και άλλα δίκτυα δεδομένων, και ο τομέας CS προσφέρει βασικές τηλεφωνικές υπηρεσίες σε όλα τηλεφωνικά δίκτυα
Οι κόμβοι του CN είναι διασυνδεδεμένοι με το δίκτυο κορμού του κάθε διαχειριστή και συνήθως συνδέονται με τεχνολογίες δικτύου υψηλής ταχύτητας, όπως το ATM.

2.4.1 SGSN

Ο Serving GPRS Support Node (SGSN) είναι ο κύριος κόμβος του δικτύου μεταγωγής πακέτων. Είναι συνδεδεμένο με το UTRAN μέσω της Iu PS διασύνδεσης και με το GGSN από την διεπαφή Gn. Το SGSN είναι υπεύθυνο για όλες τις συνδέσεις μεταγωγής πακέτων του συνδρομητή. Κατέχει δύο τύπους στοιχείων συνδρομητή, πληροφορίες συνδρομητή και πληροφορίες εντοπισμού θέσης.

Δεδομένα Συνδρομητή που αποθηκεύονται στο SGSN:

- Διεθνής ταυτότητα συνδρομητή κινητής τηλεφωνίας (IMSI)
- Προσωρινή ταυτότητες (P-TMSI διευθύνσεις)
- Διευθύνσεις Πρωτοκόλλων Πακέτων δεδομένων (PDP)

Δεδομένα Εντοπισμού Θέσης που αποθηκεύονται στο SGSN:

- Περιοχή δρομολόγησης του συνδρομητή
- Ο αριθμός VLR
- Οι διευθύνσεις GGSN από κάθε GGSN που έχουν ενεργές συνδέσεις

2.4.2 GGSN

Ο Gateway GPRS Support Node (GGSN) είναι ένα SGSN το οποίο είναι διασυνδεδεμένο με άλλα δίκτυα δεδομένων. Όλες οι επικοινωνίες δεδομένων περνούν μέσα από ένα GGSN μεταξύ του συνδρομητή και των εξωτερικών δικτύων. Όπως και με το SGSN κατέχει δύο είδη δεδομένων, πληροφορίες συνδρομητή και πληροφορίες εντοπισμού θέσης.

Δεδομένα Συνδρομητή που αποθηκεύονται στο GGSN:

- Διεθνής ταυτότητα συνδρομητή κινητής τηλεφωνίας(IMSI)
- Διευθύνσεις Πρωτοκόλλων Πακέτων δεδομένων (PDP)

Δεδομένα Εντοπισμού Θέσης που αποθηκεύονται στο SGSN:

- Διευθύνσεις από τα τρέχων SGSN όπου ο συνδρομητής είναι συνδεδεμένος

2.4.3 Border Gateway (BG)

Το Border Gateway (BG) είναι μια πύλη μεταξύ του τμήματος μεταγωγής πακέτων του δημόσιου κινητού δικτύου (PLMN) και των εξωτερικών δικτύων. Η λειτουργία αυτού του κόμβου είναι αρκετά όμοια με ένα τείχος προστασίας για το Internet, για τη διατήρηση της ασφάλειας του συνδρομητή από εξωτερικές επιθέσεις.

2.4.4 Visitor Location Register (VLR)

Ο Visitor Location Register (VLR) είναι ένα αντίγραφο από το Home Location Register του συνδρομητή. Τα δεδομένα του συνδρομητή που χρειάζονται για να του παρέχουν τις διάφορες υπηρεσίες αντιγράφονται από το HLR και αποθηκεύονται εδώ, Τόσο το MSC όσο και το SGSN έχουν VLRs που συνδέονται με αυτά.

Τα ακόλουθα δεδομένα είναι αποθηκευμένα στο VLR:

- Διεθνής ταυτότητα συνδρομητή κινητής τηλεφωνίας(IMSI)
- Mobile Station International ISDN Number (MSISDN)
- Προσωρινά Mobile Subscriber Identities (TMSI) εάν υπάρχουν
- Η τρέχουσα περιοχή θέσης (LA) του συνδρομητή
- Ο τρέχων SGSN κόμβος όπου ο συνδρομητής είναι συνδεδεμένος με αυτών

Επιπλέον, η VLR μπορεί να κατέχει περισσότερες πληροφορίες σχετικά με τις υπηρεσίες που έχουν εκχωρηθεί στο συνδρομητή.

Τόσο ο SGSN κόμβος όσο και ο MSC υλοποιούνται ως ένας φυσικός κόμβος με τον VLR και έτσι ονομάζεται VLR / SGSN και VLR / MSC.

2.4.5 Mobile-services Switching Centre (MSC)

Το Mobile-services Switching Centre (MSC) είναι υπεύθυνο για τις συνδέσεις μεταγωγής κυκλώματος ανάμεσα στα τερματικά και το δίκτυο. Εκτελεί όλες τις λειτουργίας μεταγωγής και σηματοδοσίας των συνδρομητών στην περιοχή κάλυψης τους. Η λειτουργικότητα της MSC στο UMTS είναι παρόμοια με τα καθήκοντα της MSC του GSM, αλλά με αυξημένες δυνατότητες.

Οι συνδέσεις μεταγωγής κυκλώματος μεταφέρονται μέσω της διεπαφής Iu CS ανάμεσα στο UTRAN και στο MSC. Από εκεί μεταφέρονται μέσω του GMSC σε εξωτερικά δίκτυα.

2.4.6 Gateway MSCs (GMSC).

Μερικά ή όλα τα MSCs μπορεί να Gateway MSCs (GMSC). Το GMSC είναι υπεύθυνο για την εκτέλεση των λειτουργιών δρομολόγησης της θέσης του κινητού εξοπλισμού. Όταν εξωτερικά δίκτυα προσπαθούν να συνδεθούν στο PLMN ενός παρόχου, ένα GMSC παραλαμβάνει την αίτηση εγκατάστασης σύνδεσης και ρωτά την HLR του τρέχοντος MSC του χρήστη. Στη συνέχεια δρομολογή την κλίση σε αυτή την MSC.

Όλες οι συνδέσεις μεταγωγής μέσω κυκλωμάτων που δεν έχουν ολοκληρωθεί εντός του ίδιου παρόχου συνδέονται μέσω του GMSC στα εξωτερικά δίκτυα.

2.5 Home Environment (HE).

Το οικιακό περιβάλλον (HE) κατέχει υπηρεσίες προφίλ των συνδρομητών του εκάστοτε παρόχου. Επίσης παρέχει και πληροφορίες τιμολόγησης που χρειάζονται για την αυθεντικοποίηση των χρηστών και την χρέωση τους για τις παρεχόμενες υπηρεσίες. Τόσο οι υπηρεσίες που προσφέρονται όσο και οι υπηρεσίες που μπλοκάρονται βρίσκονται αποθηκευμένες για κάθε χρήστη στο HE

2.5.1 Home Location Register (HLR)

Η Home Location Register (HLR) είναι μια βάση δεδομένων που είναι επιφορτισμένη με τη διαχείριση των κινητών συνδρομητών. Ένα κινητό δίκτυο μπορεί να αποτελείται από πολλές HLRs, ανάλογα με τον αριθμό των κινητών συνδρομητών, την ικανότητα του κάθε HLR και την εσωτερική οργάνωση του δικτύου.

Η βάση δεδομένων αποτελείται από το International Mobile Subscriber Identity, (IMSI) τουλάχιστον έναν Mobile Subscriber ISDN Number (MSISDN) και τουλάχιστον μίας PDP διεύθυνσης. Τόσο οι MSISDN όσο και οι MSI αριθμοί μπορούν να χρησιμοποιηθούν ως κλειδιά για την πρόσβαση σε άλλες αποθηκευμένες πληροφορίες. Η HLR για να είναι σε θέση να δρομολογεί και να χρεώνει τις κλήσεις κρατάει επίσης πληροφορίες σχετικά με το ποιό SGSN και VLR είναι καταχωρημένος ο κάθε συνδρομητής.

Άλλες υπηρεσίες που προσφέρονται, όπως η προώθηση κλήσεων, ο ρυθμός δεδομένων και το φωνητικού ταχυδρομείου είναι επίσης καταχωρημένες στο κατάλογο με τις περιορισμένες υπηρεσίες.

Η HLR και ο AUC είναι λογικοί δικτυακοί κόμβοι, αλλά συχνά εφαρμόζονται στον ίδιο φυσικό κόμβο. Η HLR κατέχει όλες τις πληροφορίες για το χρήστη και την συνδρομή. Δηλαδή πληροφορίες χρέωσης, ποιές υπηρεσίες προσφέρονται και ποιες απορρίπτονται αλλά και πληροφορίες σχετικά με την προώθηση κλήσεων Αλλά επίσης τη βασική πληροφορία σχετικά με το VLR και το SGSN όπου ο χρήστης είναι συνδεδεμένος.

2.5.2 AuC

Η AUC κατέχει όλα τα στοιχεία που απαιτούνται για την πιστοποίηση της ταυτότητας και της ακεραιότητας για κάθε χρήστη. Σχετίζονται με το HLR και εφαρμόζονται ως ένας φυσικός κόμβος. Αυτό διευκολύνει την ενσωμάτωση των βάσεων δεδομένων, αλλά θα πρέπει να διατηρούνται αυστηρά ξεχωριστές, και η AUC δεν πρέπει ποτέ να δώσει οποιαδήποτε πληροφορία στο HLR εκτός από τα AVs.

Το AUC αποθηκεύει το διαμοιραζόμενο μυστικό κλειδί K, για κάθε συνδρομητή. Παράγει τα AVs, σε πραγματικό χρόνο, όταν ζητηθεί από το SGSN / VLR.

2.5.3 Equipment Identity Register (EIR)

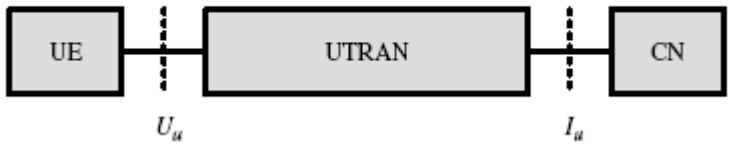
Ο Equipment Identity Register (EIR) είναι υπεύθυνος για τη φύλαξη του IMEI. Αυτό είναι μια μοναδική ταυτότητα για όλους τους τερματικούς σταθμούς. Η βάση δεδομένων για τους αριθμούς IMEI χωρίζεται σε τρία μέρη, λευκές, γκρι και μαύρες λίστες. Η λευκή λίστα περιέχει όλους τους IMEI αριθμούς που μπορούν να έχουν ολική πρόσβαση στο δίκτυο. Ένας τερματικός σταθμός βρίσκεται στη γκρίζα λίστα, όταν παρακολουθείται ή εντοπίζεται στο δίκτυο, και όταν επρόκειτο να αποκλειστεί εντελώς από την πρόσβαση, τότε τοποθετείται στη μαύρη λίστα. Όταν το τερματικό είναι δηλωθεί ως κλεμμένο, το IMEI τοποθετείται στο μαύρο κατάλογο και, συνεπώς απαγορεύεται η πρόσβαση του στο δίκτυο. Μπορεί επίσης να χρησιμοποιηθεί για να κρατήσει μια συγκεκριμένη σειρά τερματικών σταθμών έξω από το δίκτυο, εάν δεν λειτουργούν σύμφωνα με τις προδιαγραφές.

2.6 External Networks

Τα εξωτερικά δίκτυα δεν αποτελούν μέρος του ίδιου του συστήματος UMTS, αλλά είναι αναγκαίο να τους παρέχεται διασυνδεδεμένη επικοινωνιών. Τα εξωτερικά δίκτυα μπορεί να είναι είτε διαφορετικά τηλεφωνικά δίκτυα, όπως τα δημόσια κινητά δίκτυα (PLMN), τα δημόσια τηλεφωνικά δίκτυα μεταγωγής (PSTN) και τα ISDN, ή τα data-based δίκτυα, όπως το Internet. Η μεταγωγή πακέτων συνδέεται με τα δίκτυα δεδομένων, ενώ η μεταγωγή κυκλώματος συνδέεται με το τηλεφωνικό δίκτυο.

2.7 Interfaces

Οι ρόλοι των διαφόρων κόμβων του δικτύου, ορίζονται με τις διάφορες διασυνδέσεις. Αυτές οι διασυνδέσεις ορίζονται αυστηρά, έτσι ώστε διαφορετικοί κατασκευαστές να μπορούν να διασυνδέουν τα διαφορετικά υλικά μεταξύ τους. Στην εικόνα 2.2 παρουσιάζονται οι διεπαφές με τα τμήματα που συνδέουν.



Εικόνα 2-2 Utran Interfaces

2.7.1 Uu Interface

Η Uu διασύνδεση είναι η WCDMA, Wideband Code Division Multiple Access, ραδιο-διεπαφή η οποία ορίζεται στο UMTS. Η διεπαφή αυτή είναι ανάμεσα στον κόμβο Β και στο τερματικό.

2.7.2 Iu Interface

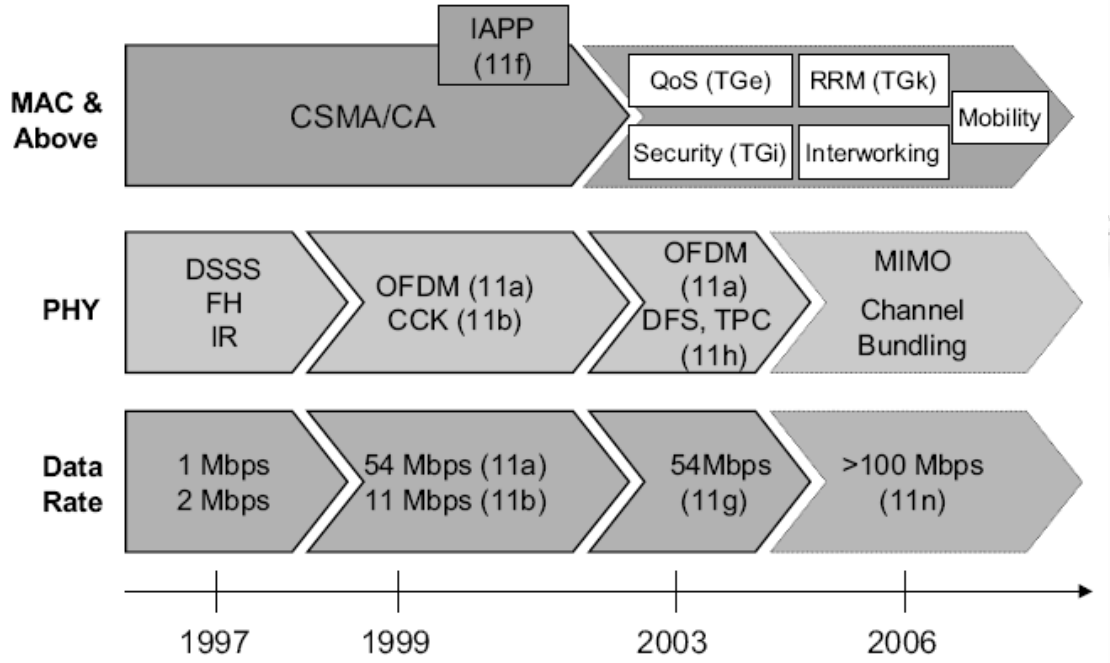
Η διασύνδεση Iu συνδέει το CN και το UTRAN. Αποτελείται από τρία μέρη, το
Iu PS για το τμήμα μεταγωγής πακέτων, το Iu CS για το τμήμα μεταγωγής κυκλώματος και το Iu BC για το τμήμα εκπομπής. Το CN μπορεί να συνδεθεί σε πολλά UTRANs και με Iu Ps και CS διεπαφές. Αλλά το UTRAN δεν μπορεί να συνδεθεί σε περισσότερα από ένα CN.

3. ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΔΕΔΟΜΕΝΩΝ WLAN

Η βιομηχανία των Ασύρματων Τοπικών Δικτύων (WLAN) έχει καταστεί ένας από τους ταχύτερα αναπτυσσόμενους τομείς της οικονομίας της επικοινωνίας. Οι αποστολές WLAN εξοπλισμού αυξήθηκαν σε σχεδόν 12 εκατομμύρια μονάδες το 2001 και η ζήτηση αναμένεται να συνεχιστεί να αναπτύσσεται κατά ένα ετήσιο ποσοστό 23% κατά την επόμενη πενταετία. Η αύξηση αυτή οφείλεται, σε μεγάλο βαθμό, από την εισαγωγή WLAN προϊόντων που βασίζονται σε πρότυπα. Η προσδοκία της συνεχόμενος αύξησης του WLAN προέρχεται από την υπόσχεση των νέων τυποποιημένων τεχνολογιών WLAN, από την βελτίωση της σχέσης κόστος/απόδοση των συστημάτων WLAN, και από την αυξανόμενη διαθεσιμότητα των λύσεων WLAN που παγιώνουν τη φωνή, τα δεδομένα, και τις λειτουργίες κινητικότητας. Αυτό, σε συνδυασμό με τις προβλέψεις της αγοράς που αναφέρουν ότι το WLAN θα γνωρίσει τεράστια ανάπτυξη τα επόμενα χρόνια, δείχνουν ότι οι τεχνολογίες WLAN θα παίξουν σημαντικό ρόλο στο μέλλον και θα έχουν σημαντικές επιπτώσεις στις επιχειρήσεις μας και την προσωπική μας ζωή.

Η IEEE 802.11 ομάδα εργασίας (ΟΕ) είναι ήδη εξελίξει πολλές πτυχές του δεσπόζων WLAN προτύπου, συμπεριλαμβανομένης της ασφάλειας, της ποιότητας των υπηρεσίων (QoS), και η συνύπαρξη με άλλες τεχνολογίες χωρίς άδεια. Το Σχήμα 4.1 δείχνει πώς τα WLAN πρότυπα έχουν αναπτυχθεί και συνεχίζουν να εξελίσσονται. Υπάρχουν πρόσθετες τεχνικές προκλήσεις που πρέπει να αντιμετωπιστούν για την επίλυση των προβλημάτων της υψηλής απόδοσης (HT), της κινητικότητας, της διασυνεργασίας του WLAN με άλλα εξωτερικά δίκτυα και την διαχείριση των ραδιοφωνικών πόρων.

Υψηλότερες ταχύτητες δεδομένων απαιτούν ευρείες ζώνες συχνοτήτων, και ικανοποιητική ευρυζωνική σύνδεση μπορεί να επιτευχθεί σε υψηλότερες ζώνες συχνοτήτων. Δεδομένου ότι η απώλεια διαδρομής (LOS) είναι ανάλογη με την φέρουσα συχνότητα, η απώλεια διάδοσης είναι αναπόφευκτη στην υψηλότερη μπάντα συχνοτήτων. Κατά συνέπεια, η περιοχή κάλυψης είναι μικρότερη σε σχέση με το τρέχων κυψελωτό σύστημα.



Εικόνα 3-1 Τρέχοντα και μελλοντικά MAC, PHY και ρυθμοί δεδομένων των WLAN πρότυπων

Τα WLAN και τα 3G συστήματα κινητής τηλεφωνίας μπορούν να παρέχουν ασύρματες συνδέσεις υψηλών ταχυτήτων, όπου οι παλαιότερες κυψελωτές τεχνολογίες δεν μπορούσαν να προσφέρουν. Τα WLANs είναι πιο κατάλληλα για HotSpot κάλυψη, δηλαδή, ασύρματη ευρυζωνική πρόσβαση με περιορισμένη κινητικότητα. Τα 3G συστήματα κινητής τηλεφωνίας, που έχουν φωνητική υποστήριξη, ευρεία κάλυψη και μεγάλη κινητικότητα, είναι πιο κατάλληλα στις περιοχές με μέτρια ή χαμηλή πυκνότητα απαιτήσεων για την ασύρματη χρήση που απαιτεί υψηλή κινητικότητα.

Στο μέλλον, τα διάφορα συμπληρωματικά δίκτυα ράδιο-πρόσβασης (RANs) θα χρησιμοποιηθούν σε συνδυασμό με τα 4G RANs για να παρέχουν υπηρεσίες ολικής κάλυψης. Το WLAN αναμένεται να είναι ένα από αυτά τα συμπληρωματικά RANs που θα χρησιμοποιηθεί για να επιτύχει την ευρυζωνική ασύρματη υπηρεσία με περιορισμένη κινητικότητα.

3.1 IEEE 802.11 πρότυπα για ασύρματες επικοινωνίες

Το IEEE αναπτύσσει και διατηρεί τεχνολογικά πρότυπα με βάση τις συστάσεις των συναλλασσόμενων με ειδικές γνώσεις στην τεχνολογία των προτύπων. Οι επιστήμονες, οι κατασκευαστές, και οι τελικοί χρήστες συμμετέχουν ενεργά στο ινστιτούτο παρέχοντας δεδομένα, με τα οποία έρχεται σε ομοφωνία σχετικά με τα πρότυπα που είναι κατάλληλα για μια συγκεκριμένη τεχνολογία.

Η χρήση κάθε IEEE προτύπου είναι πλήρως εθελοντική και η ύπαρξη ενός προτύπου IEEE δεν σημαίνει ότι δεν υπάρχουν άλλοι τρόποι για να παράγεις, να δοκιμάζεις, να κάνεις μετρήσεις, να αγοράζεις, ή να παρέχεις άλλα αγαθά και υπηρεσίες που να σχετίζονται με το πεδίο εφαρμογής του IEEE προτύπου. Η έρευνα των επιστημόνων, των κατασκευαστών, και οι τελικοί χρήστες όλοι επωφελούνται από όλα τις κοινές προδιαγραφές που περιέχονται στα πρότυπα. Όταν ο καθένας χρησιμοποιεί το πρότυπο, οι πελάτες μπορούν να χρησιμοποιούν εξοπλισμό από διαφορετικούς κατασκευαστές χωρίς προβλήματα ασυμβατότητας.

Το IEEE 802 σύνολο προτύπων έχει να κάνει με το φυσικό επίπεδο (PHY) και τα επίπεδα διασύνδεσης δεδομένων των τοπικώς και των μητροπολιτικών δικτύων (LAN και Mans). Αυτά είναι τα δύο στρώματα που βρίσκονται στο κάτω μέρος του ISO / OSI μοντέλου δικτύων, πολύ μακριά από το επίπεδο εφαρμογών, και ασχολούνται με την μετάδοση δεδομένων (και λήψη) μεταξύ υπολογιστών στα LANs και MANs. Η IEEE έχει διασπάσει το επίπεδο συνδέσμου δεδομένων σε δύο διαφορετικά υπο-επίπεδα: στον έλεγχο λογικής σύνδεση (LLC)

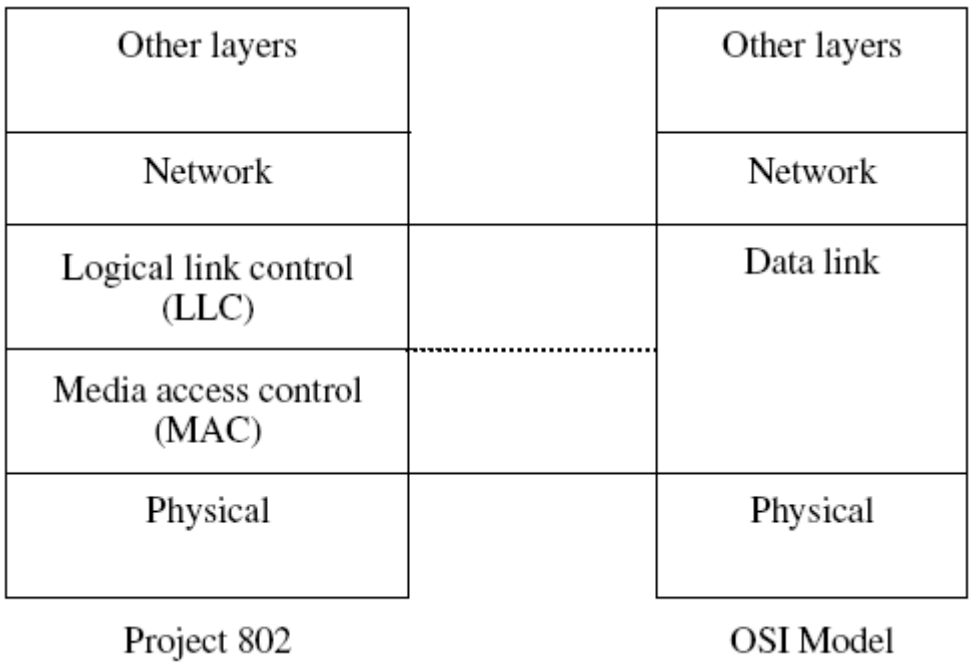
και στον έλεγχο πρόσβασης μέσων (MAC) (Εικόνα 4.2). Το πρωτόκολλο IEEE LLC αφορά την λογική διεύθυνση, έλεγχο πληροφοριών, δεδομένων και μερίσματα του τμήματος HDLC (έλεγχο συνδέσμου δεδομένων υψηλού επιπέδου), ενώ τα MAC πρωτόκολλα ασχολούνται με το συγχρονισμό, έλεγχο λαθών και τις φυσικές διευθύνσεις. Τα MAC πρωτόκολλα είναι ειδικά για τη χρήση σε LAN (Ethernet, Token Ring, Token Bus, κτλ).

Τα πρότυπα IEEE 802.3 ασχολούνται με τις Ethernet (ενσύρματες) επικοινωνίες. Αρχικά, υποστήριζαν 10-Mbps ρυθμούς δεδομένων, αλλά ως δίκτυο τερματικών έγιναν πιο γρήγορα και έτσι μπορούν να λειτουργούν εφαρμογές πολυμέσων. Επίσης η ανάγκη να μοιράζονται υψηλής ταχύτητας διακομιστές (Servers) ανάμεσα στα LANs τα έκανε ευρέως διαδεδομένα, και υψηλότεροι ρυθμοί δεδομένων περιλαμβάνονται στα νέα πρότυπα. Στα μέσα της δεκαετίας του 1990 ανανεώθηκαν ώστε να περιλαμβάνουν ρυθμούς μετάδοσης έως 100 Mbps, και στα τέλη του 1990 το Gigabit Ethernat εδραιώθηκε για το 802.3. Οι εμπειρογνώμονες βεβαιώνουν ότι οι δύο μεγάλες κινητήριες δυνάμεις της εν λόγω βιομηχανίας είχαν πάντα την ευκολία της εγκατάστασης και της αύξηση του ρυθμού μετάδοσης δεδομένων, δύο σημαντικά χαρακτηριστικά του Fast Ethernet και του Gigabit Ethernet. Έτσι, κυριαρχούν έναντι των άλλων Ethernet LAN 802,3 IEEE προτύπων (τα οποία ονομάζονται Token Ring και Token Bus).

Τα 802,4 και 802,5 πρότυπα αφορούν τα επίπεδα PHY και MAC για τις τοπολογίες Token Bus και Token Ring, αντίστοιχα. Τα πρότυπα του IEEE 802,6 αντιμετωπίζουν τις ανάγκες των MANs. Η οικογένεια 802,11 των προτύπων είναι αφιερωμένη στις απαιτήσεις των δύο χαμηλότερων στρωμάτων του ISO στα ασύρματα δίκτυα. Μία πλήρης λίστα των υπόλοιπων προτύπων παρουσιάζεται στον πίνακα 4.1.

Κατά ανάπτυξη των προτύπων για τα ασύρματα δίκτυα, η IEEE παρατήρησε τους κανονισμούς ραδιοσυχνότητας της αμερικανικής Επιτροπής Ομοσπονδιακής Επικοινωνίας (FCC), δεδομένου ότι τα ραδιοκύματα ήταν το μέσο μετάδοσης για την ασύρματη δικτύωση. Το 1985, η FCC σχεδίασε οριζόμενος συγκεκριμένες μερίδες από το φάσμα ραδιοσυχνοτήτων για τη βιομηχανία, την επιστήμη, και για ιατρική χρήση, και αυτές έγιναν γνωστές ως ISM ζώνες. Αυτές είναι: (1) 902-928 MHZ, ένα εύρος ζώνης 26 MHZ (2) 2.4-2.4835 Ghz, ένα εύρος ζώνης 83.5 MHZ, αποκαλούμενο συνήθως ζώνη 2.4-Ghz και (3) 5.725-5.850 Ghz, ένα εύρος ζώνης 125 MHZ, αποκαλούμενο συνήθως ζώνη 5-Ghz.

Μέσα σε ορισμένες κατευθυντήριες γραμμές, οι FCC κανονισμοί επιτρέπουν στους χρήστες να λειτουργούν ραδιόφωνα μέσα σε αυτές τις



Εικόνα 3-2 Διαχωρισμός MAC και LLC

ζώνες χωρίς FCC άδεια. ένα προφανές πλεονέκτημα για τους κατασκευαστές των τεχνολογιών ασύρματων δικτύων(και για τους χρήστες που δεν πρέπει να λαμβάνουν άδεια λειτουργίας τους κινητά τηλέφωνα).

Τα 802,11 πρότυπα έχουν εξελιχθεί με τον καιρό, και σήμερα ορίζονται στα 802,11 πρότυπα έξι μέθοδοι για την ασύρματη μετάδοση δεδομένων. Κάθε μέσο μετάδοσης αντιπροσωπεύει το δικό του PHY εντός 802.11. Τα πρώτα πρότυπα IEEE 802.11 ολοκληρώθηκαν το 1997, και τρία από αυτά ορίζονται για ταχύτητα μετάδοσης δεδομένων 1 - και 2 Mbps. Μια επισκόπηση αυτών των PHY παρέχονται στον πίνακα 4.2 και εξηγείται παρακάτω:

- Η Direct-Sequence Spread Spectrum (DSSS) PHY χρησιμοποιεί την ζώνη των 2.4-GHz και μπορεί να μεταδώσει δεδομένα σε ταχύτητες 1 ή 2 Mbps. Για πρώτη φορά χρησιμοποιήθηκε για στρατιωτικές επικοινωνίες. Για την πρόληψη παρεμβολών, τα ραδιόφωνα που χρησιμοποιούν DSSS διαβιβάζουν τα σήματά τους σε όλη τη διαθέσιμη ISM μπάντα με πολύ χαμηλή ενέργεια. Αυτό αποτρέπει παρεμβολές από σήματα στενής ζώνης και μειώνει την πιθανότητα μετάδοσης των σφαλμάτων. Όσοι παρακολουθούν το κανάλι με σκοπό να υποκλέψουν πληροφορίες μπορούν να ερμηνεύσουν αυτά τα μηνύματα, σαν θόρυβο.

- Η συχνότητα hopping Spread Spectrum (FHSS) PHY επίσης χρησιμοποιεί την ζώνη 2.4-GHz για μετάδοση σε 1 ή 2 Mbps, και επίσης αρχικά χρησιμοποιήθηκε σε στρατιωτικές εφαρμογές. Δύο ραδιόφωνα που επικοινωνούν χρησιμοποιώντας FHSS αλλάζουν συχνότητες σύμφωνα με ένα προκαθορισμένο ψευδοτυχαίο ρυθμό, και μόνο παραμένουν σε μια συγκεκριμένη συχνότητα για ένα κλάσμα του δευτερολέπτου (οι FCC κανονισμοί, απαιτούν η συχνότητα να μεταβάλλεται σε 400 ms ή λιγότερο). Η τεχνική αυτή ελαχιστοποιεί τις πιθανότητες ότι περισσότερες από μια ραδιοφωνικές συσκευή θα εκπέμπουν στην ίδια συχνότητα ταυτόχρονα.

- Η Diffused Infrared (DFIR) PHY χρησιμοποιεί σχεδόν ορατό φως στο 850-nm έως 950 nm- για σηματοδοσία. Ωστόσο, σε αντίθεση με τις υπέρυθρες (IR) του τηλεχειριστηρίου των τηλεοράσεων που χρειάζονται μια οπτική επαφή για να λειτουργήσουν, οι συσκευές που ακολουθούν τα 802,11 DFIR πρότυπα δεν απαιτείται να έχουν οπτική επαφή, γεγονός που επιτρέπει την οικοδόμηση ενός πραγματικού LAN. Όμως, δεν υπάρχουν προϊόντα ασύρματης δικτύωσης διαθέσιμα σήμερα που εφαρμόζουν αυτή την PHY.

- Το έκτο 802,11 PHY περιγράφεται αναλυτικά στο πρότυπο IEEE 802.11g και είναι συμβατή με το προγενέστερο 802.11b. Η πολυπλεξία OFDM επιτρέπει ρυθμούς δεδομένων μέχρι 54 Mbps στα 2.4-MHz. Η ταχύτητα μετάδοσης δεδομένου OFDM και COFDM είναι επαρκής για τη μεταφορά φωνής και εικόνας αρκετά γρήγορα για τους περισσότερους χρήστες.

802.1	Higher-layer LAN protocols
802.2	Logical link control
802.3	Ethernet (wired)
802.4	Token Bus
802.5	Token Ring
802.6	MAN
802.7	Broadband
802.8	Fiber optic
802.9	Isochronous LAN
802.10	LAN/MAN Security
802.11a	Wireless LAN: 5-GHz band
802.11b	Wireless LAN: 2.4-GHz band
802.11c	Wireless LAN: higher layers
802.11d	Wireless LAN: MAC
802.11e	Wireless LAN: MAC
802.11f	Higher layers
802.11g	Wireless LAN: higher rate 2.4-GHz band
802.11h	Wireless LAN: MAC
802.11i	Wireless LAN: MAC
802.12	Demand priority
802.13	Not used
802.14	Cable modem
802.15	Wireless PAN
802.16	Broadband wireless access
802.17	Resilient packet ring
802.18	Radio regulations
802.19	Coexistence
802.20	Mobile broadband wireless access

Πίνακας 3-1 Λίστα προτύπων 802.11

DSSS	2.4 GHz	1 or 2 Mbps
FHSS	2.4 GHz	1 or 2 Mbps
DFIR	850 to 950 nm (infrared)	None implemented
COFDM	5 GHz	54 Mbps
HR/DSSS	2.4 GHz	5.5 or 11 Mbps
OFDM	2.4 GHz	54 Mbps

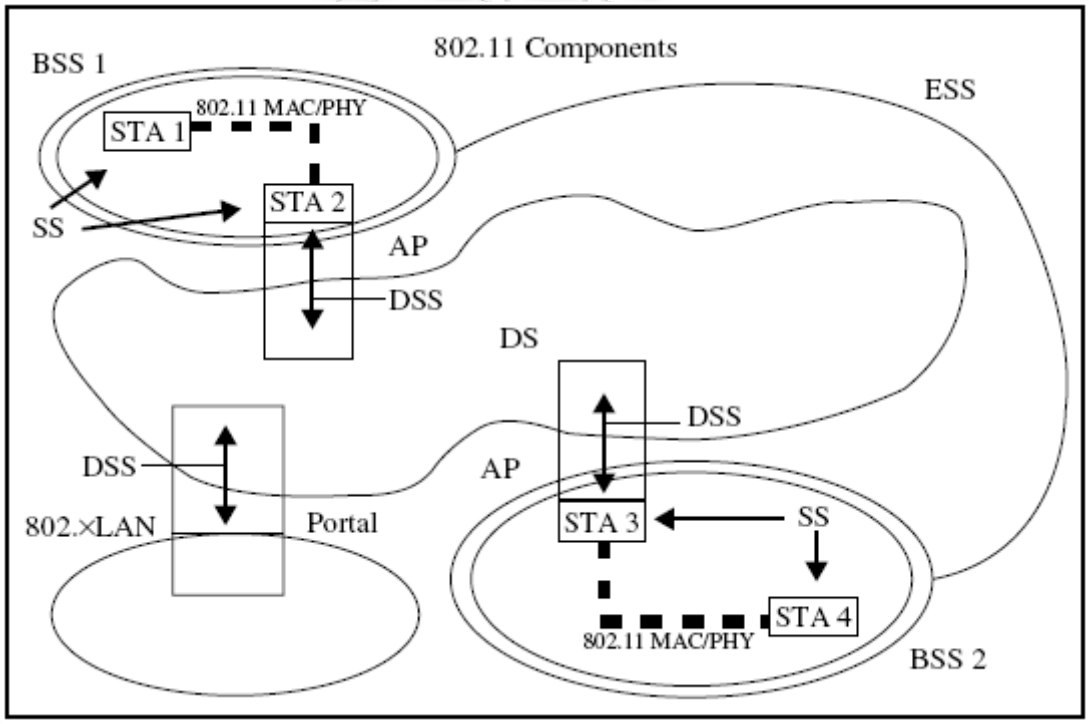
Πίνακας 3-23.1. 802.11 PHY Layers

3.1.1 Βασικές αρχές του IEEE 802.11

Τα Wireless LAN συστήματα είναι διαφορετικά από τα ενσύρματα LAN για διάφορους λόγους. Ενώ μπορεί κανείς να σχεδιάσει την αρχιτεκτονική ενός ενσύρματου LAN, για τα ασύρματα PHYs δεν υπάρχουν καθορισμένες περιοχές κάλυψης. Τα χαρακτηριστικά διάδοσης είναι δυναμικά και απρόβλεπτα (βλέπε σχήμα 4.3). Μικρές αλλαγές στην θέση ή την κατεύθυνση μπορεί να οδηγήσουν σε δραματικές διαφορές στην ισχύ του σήματος. Παρόμοια αποτελέσματα μπορεί να προκύψουν όταν ένας σταθμό (STA) είναι σταθερός ή κινητός. Τα σχήματα που χρησιμοποιούνται από τον IEEE για την σχεδίαση της αρχιτεκτονικής ενός WLAN υπάρχουν για λόγους ευκολίας. Στην πραγματικότητα, τα όρια των WLANs δεν είναι σαφώς καθορισμένα από τη μια στιγμή στην άλλη, κυρίως λόγω της κινητικότητας των κόμβων.

Στο IEEE 802.11 οι μονάδες που χαρακτηρίζονται από διευθύνσεις ονομάζονται STA. Το STA είναι ένα μήνυμα προορισμού, αλλά δεν ανήκει (εν γένει) σε μια συγκεκριμένη τοποθεσία, όπως θα συνέβαινε σε ένα ενσύρματο LAN. Τα MAC πλαίσια προσαρμόζονται ώστε να λάβουν υπ' όψιν αυτήν την αλλαγή. Το IEEE κάνει τις παρακάτω παρατηρήσεις σχετικά με τα 802,11 PHYs, επισημαίνοντας ότι (α) Χρησιμοποιούν ένα μέσο που δεν έχει ούτε απόλυτα ούτε εύκολα παρατηρήσιμα όρια εκτός των οποίων οι σταθμοί με PHY πομποδέκτες είναι ανίκανοι να λαμβάνουν δεδομένα, (β) είναι απροστάτευτοι από εξωτερικά σήματα (γ) επικοινωνούν δια μέσω ενός μέσου σημαντικά λιγότερο αξιόπιστο από τα ενσύρματα PHYs (δ) έχουν δυναμικές τοπολογίες (ε) υπάρχει έλλειψη πλήρης συνδεσιμότητας και ως εκ τούτου η υπόθεση ότι κάθε STA μπορεί να ακούσει κάθε άλλο STA είναι αβάσιμη (στ) είναι χρονικά μεταβαλλόμενα και έχουν ασύμμετρες ιδιότητες διάδοσης.

Τα αρχιτεκτονικά στοιχεία ενός 802,11 δικτύου αποτελούνται από τα STA, από τα BSSs, από τα distribution systems (DS) , από τα WM, από τα distribution systems media (DSM), από access points (AP) (γνωστά και ως σταθμοί βάσης-BS) από extended service sets (ESS), και από potals όπως φαίνεται στο σχήμα 4.3.



Εικόνα 3-3 Τα συστατικά του 802.11 WLAN

Οι σταθμοί είναι διευθυνσιοδοτημένες μονάδες σε ένα δίκτυο και μπορεί να είναι πελάτες ή διακομιστές. Ενώ είναι δυνατόν για δύο προσωπικούς υπολογιστές να επικοινωνούν μεταξύ τους απευθείας μέσω μιας ασύρματης σύνδεσης, σε ένα ασύρματου LAN ένας προσωπικός υπολογιστής είναι πιο πιθανό να συνδεθεί με το σταθμό βάσης (ή AP) για την πρόσβαση με το υπόλοιπο δίκτυο. Οι προσωπικοί υπολογιστές και οι προσωπικούς ψηφιακούς βοηθοί (PDAs) είναι οι πιο κοινοί τύποι σταθμών σε WLAN.

Το BSS είναι το βασικό σύνολο των συσκευών σε ένα δίκτυο WLAN, και μπορεί να περιλαμβάνει μόνο δύο σταθμούς. Το IEEE 802.11 documentation(1999) επίσης χρησιμοποιεί τον όρο BSS εννοώντας την περιοχή κάλυψης εντός της οποίας τα μέλη-σταθμοί του BSS μπορούν να παραμείνουν σε επικοινωνία, και ότι εάν κάποιος σταθμός κινηθεί "εκτός" του BSS, δεν μπορεί πλέον να επικοινωνεί απευθείας με τα άλλα μέλη του BSS. Ένα ανεξάρτητο σύνολο βασικών υπηρεσιών (IBSS) είναι πιθανό εάν οι σταθμοί μπορούν να επικοινωνούν απευθείας μεταξύ τους. Όταν ένα IBSS δημιουργείται δυναμικά, για προσωρινή χρήση, αναφέρεται και ως ad hoc δίκτυο. Αν ο σταθμός είναι μέλος της υποδομής ενός BSS τότε «συνδέεται» με το BSS με τη βοήθεια μιας υπηρεσίας συστημάτων διανομής (DSS), η οποία αναλύεται στην συνέχεια. Οι συνδέσεις επιτρέπεται να είναι δυναμικές, δεδομένου ότι οι σταθμοί εισέρχονται και εξέρχονται από το BSS.

Το DS (που δεν πρέπει να συγχέεται με DSS) είναι το αρχιτεκτονικό στοιχείο που χρησιμοποιείται για τη σύνδεση των BSSs μεταξύ τους.Τα DS χαρτογραφούν διευθύνσεις στους πραγματικούς προορισμούς για τις κινητές συσκευές με πολλαπλά BSSs. Σε αυτόν τον τύπο αρχιτεκτονικής τα BSS δεν είναι ανεξάρτητα αλλά είναι στοιχεία ενός μεγαλύτερου και εκτεταμένου δικτύου. Το DS χρησιμοποιεί το DSM ενώ το BSS χρησιμοποιεί αυτό που αναφέρεται ως WM. Οι όροι διατηρούνται διακριτοί διότι το DSM και το WM εκτελούν διαφορετικές εργασίες. Ωστόσο δεν υπάρχει κάποιος IEEE «κανόνας» που να λέει ότι το μέσο που χρησιμοποιείται πρέπει να είναι διαφορετικό εάν υιοθετείται ως DSM ή ως WM. Το documentation αναφέρει ρητά ότι η IEEE 802.11 LAN αρχιτεκτονική καθορίζεται ανεξάρτητα από τα φυσικά χαρακτηριστικά της κάθε συγκεκριμένης εφαρμογής.

Τα APs είναι σταθμοί που παρέχουν DS υπηρεσίες. Επειδή είναι σταθμοί χαρακτηρίζονται από διευθύνσεις. Τα APs συνδέουν τα STAs με το LAN. Οι διαχειριστές ορίζουν παραμέτρους για τα APs, συμπεριλαμβανομένου του ονόματος του ασύρματου δικτύου , του καναλιού που χρησιμοποιείται από το AP και ποιό Wired Equivalent Privacy Key χρησιμοποιείται από το δίκτυο για ασφάλεια. Τα ασύρματα δίκτυα χρησιμοποιούν κρυπτογράφηση για τη μεταφορά δεδομένων από εξωτερικούς εισβολείς και τα WEP κλειδιά είναι ένας τρόπος για την κρυπτογράφηση και αποκρυπτογράφηση. Εν ολίγοις τα δεδομένα μεταφέρονται από τους STAs των BSS μέσω των AP στα DS και αντιστρόφως.

Όταν χρησιμοποιείται ένα AP για να συνδυαστεί με ένα DS, ένα ή περισσότερα BSSs και ενδεχομένως ένα ή περισσότερα LANs τότε το δίκτυο που δημιουργείται ονομάζεται ESS. Τα 802.11 DS και BSS επιτρέπουν στο 802.11 τη δημιουργία ενός δικτύου αυθαίρετου μεγέθους και πολυπλοκότητας. Η βασική ιδέα είναι ότι το ESS δίκτυο εμφανίζεται το ίδιο στο LLC στρώμα με το IBSS δίκτυο και οι κινητοί σταθμοί μπορούν να κινούνται από ένα BSS σε άλλο του ίδιου ESS δικτύου.

Η τελευταία λογική αρχιτεκτονική μονάδα σε ένα IEEE WLAN είναι η πύλη (portal), που συνδέει ένα παραδοσιακό ενσύρματο LAN στο 802,11 WLAN. Η συσκευή που ενεργεί ως πύλη μπορεί επίσης να λειτουργήσει και ως AP. Σε πολύ απλά λόγια, μια πύλη είναι το σημείο όπου ένα καλώδιο από ένα ενσύρματο LAN συναντά μια συσκευή από το ασύρματο LAN που μπορεί να διαβάσει από την πύλη του σύρματος και να διαβιβάζει στην WLAN μέσω του ραδιοφώνου (ή το ασύρματο μέσο επιλογής). Εάν δεν υπάρχει συσκευή από το WLAN που να έχει συνδεθεί με καλώδιο σε ενσύρματο LAN, τότε η επικοινωνία μεταξύ των δύο δικτύων δεν θα πραγματοποιηθεί.

3.1.2 Αρχιτεκτονική και Λειτουργία του υπο- επιπέδου MAC

Υπενθυμίζεται ότι η οικογένεια προτύπων IEEE 802 έχει χωρίσει το επίπεδο δεδομένων του ISO / OSI σε δύο μέρη: Τα άνω υπόστρωμα είναι το υπόστρωμα LLC, και το χαμηλότερο είναι το MAC υπόστρωμα (ακριβώς πάνω από το PHY) (όπως φαίνεται στο σχήμα 4.2). Αυτό γίνεται προκειμένου να γίνει διάκριση μεταξύ της λειτουργικότητας της πρόσβασης στο μέσο

από άλλα θέματα σύνδεσης δεδομένων. Κάθε IEEE 802 PHY πρότυπο (Ethernet, Token Ring, Token Bus, και ούτω καθεξής) προδιαγράφει τόσο τις πτυχές PHY του πρωτοκόλλου, καθώς και τον τρόπο με τον οποίο η πρόσβαση πραγματοποιείται(όπως παρουσιάζεται στον πίνακα 3.3). Για παράδειγμα, το πρότυπο IEEE 802.3 (Ethernet) καθορίζει τους τύπους των μέσων που μπορούν να χρησιμοποιηθούν (αρμοδιότητα του PHY)- και καθορίζει τη

Standard	Medium access protocols
802.3	CSMA/CD
802.4	Token bus access
802.5	Token ring access
802.11	FHSS, DSSS, Infrared
802.11a	OFDM
802.11b	DSSS
802.11g	OFDM

Πίνακας 3-3.12 Πρότυπα και πρωτόκολλα πρόσβασης στο μέσο

χρήση του CSMA / CD πρωτόκολλου μεσαίας πρόσβασης (αρμοδιότητα του επιπέδου συνδέσμου δεδομένων και του υπο- επιπέδου MAC). Αντίθετα, το υπόστρωμα LLC καταφέρνει να παρέχει μία ενιαία διασύνδεση με το επίπεδο δικτύου για τις πολλές τοπολογίες φυσικού επιπέδου.. Αυτό περιλαμβάνει τον έλεγχο της σύνδεσης μεταξύ του υπολογιστή λήψης και λήψη ηλεκτρονικών υπολογιστών, και ελέγχει ότι τα πλαίσια μεταφέρονται χωρίς λάθη.

Μία από τις MAC υπηρεσίες, η ασύγχρονη υπηρεσία μεταφοράς δεδομένων, διαχειρίζεται την ανταλλαγή πακέτων δεδομένων, που ονομάζεται MSDUs, μεταξύ συσκευών Από τεχνική άποψη, τα MSDUs δεν μεταφέρονται από συσκευή σε συσκευή. Το MSDU είναι το πακέτο δεδομένων που κινείται ανάμεσα του λογισμικού του κεντρικού υπολογιστή και του MAC του ασύρματου LAN . Το MSDU τυπικά κατανέμεται σε μικρότερα τμήματα, όπου σε καθένα από αυτά προστίθεται μία MAC επικεφαλίδα, πριν από την κρυπτογράφηση και την μετάδοση. Αυτή η διαδικασία είναι γνωστή ως κατακερματισμός. Τα τμήματα της αρχικής MSDU είναι γνωστά ως MAC protocol Data Units (MPDUs). Τα MPDUs είναι πακέτα δεδομένων που μεταφέρονται μεταξύ του MAC και της κεραίας. Κατά τη διάρκεια μετάδοσης, τα MSDUs αποστέλλονται από το λειτουργικό σύστημα (OS) προς το υπό-επίπεδο MAC και μετατρέπονται σε MPDUs έτοιμες να αποσταλούν μέσω του ραδιοφώνου. Κατά τη διάρκεια λήψης τα MPDUs φθάνουν μέσω της κεραίας και μετατρέπονται σε MSDUs πριν παραδοθούν στο OS. Αν ένα MPDU χαθεί στη μετάδοση, μπορεί να επανεκπεμφθεί αντί να αποσταλθεί ξανά ένα ολόκληρο MSDU.

Όλα τα MAC τα πλαίσια έχουν τα ίδια βασικά χαρακτηριστικά: μια κεφαλίδα MAC για τον έλεγχο των πλαισίων, τη διάρκεια, διεύθυνση, πληροφορία για έλεγχο ακολουθίας, ένα πλαίσιο σώματος (το οποίο ποικίλλει ανάλογα με τον τύπο του πλαισίου), και ένα πλαίσιο ελέγχου ακολουθίας (FCS), το οποίο διαθέτει έναν IEEE 32-bit κυκλικό κώδικα πλεονασμού (CRC). Το FC πεδίο περιέχει την έκδοση του πρωτόκολλου, το είδος, την υποκατηγορία, το DS εκπομπής, το DS λήψης, επιπλέον τμήματα, διαχείριση ενέργειας, επιπλέον δεδομένα, WEP, και ταξινομημένα υποπεδία.

Το MAC 802,11 υποστηρίζει CSMA / CA, και εφαρμόζεται σε όλα τα STAs, ως θεμελιώδης διανεμημένη λειτουργία συντονισμού (DCF). Αυτό είναι σχεδόν το ίδιο DCF που χρησιμοποιείται στο IEEE 802.3 Ethernet LANs - CSMA / CD. Το CSMA είναι ένα "listen and talk" πρωτόκολλο: Τα STAs "ακούν" το μέσο μετάδοσης πριν από την αποστολή ενός μηνύματος. Εάν το μέσο αυτό είναι σε χρήση, χρησιμοποιούν έναν back-off αλγόριθμο για να προγραμματίσουν την επανεκπομπή τους σε μελλοντικό χρόνο, όταν το μέσο θα είναι διαθέσιμο. Δεν προλαμβάνονται όλες οι συγκρούσεις με αυτό το σχήμα. Εάν το STA A στέλνει ένα μήνυμα, αυτό θα χρειαστεί χρόνο (καθυστέρηση διάδοσης) πριν φθάσει στο STA B. Εν τω μεταξύ, το STA B μπορεί να ακροαστεί το μέσο, να μην ακούσει το μήνυμα του STA A και

να συμπεράνει ότι το μέσο είναι ελεύθερο, και στέλνει ένα μήνυμα το οποίο συγκρούεται με το πρώτο. (Σε ένα LAN με μια ασυνήθιστα μεγάλη περίοδο διάδοσης, ή σε ένα WAN, ο χρόνος διάδοσης μεταξύ των σταθμών μπορεί να είναι πολύ μεγάλος πράγμα θετικό για τον μεταφορέα που «ακούει» το μέσο.) Επιπλέον, υπάρχει το "πρόβλημα του κρυφού τερματικού." Σε ένα ασύρματο δίκτυο, το STA C μπορεί να εμποδίζεται φυσικά να «ακούσει» ότι το STA A εκπέμπει, και να υποθέσει ότι είναι ασφαλές να εκπέμψει στο STA B προκαλώντας αλλεπάλληλες συγκρούσεις. Σε ένα ενσύρματο LAN, οι συγκρούσεις ανιχνεύονται, για να βεβαιωθούν ότι τα μηνύματα που εμπλέκονται σε συγκρούσεις δεν χάνονται οριστικά, αλλά ο χρόνος χάνεται και το μέσο παραμένει άσκοπα δεσμευμένο. Τα ενσύρματα LAN μπορούν εύκολα να ανιχνεύουν συγκρούσεις ακούγοντας για μεταβολές στην τάση του μέσου μετάδοσης. Τα ασύρματα STAs δεν μπορεί να χρησιμοποιήσουν αυτή τη μέθοδο, επειδή το σήμα της διαβίβασης των STA υπερέχει έναντι όλων των άλλων σήματα, και τα ανταγωνιστικά σήματα δεν μπορούν να εντοπιστούν. Μία λύση θα ήταν να αναπτύξουν ακριβές κατευθυντικές κεραίες και front-end ενισχυτές σε κάθε STA, με ένα σετ για εκπομπή και ένα για λήψη, Αυτή η μέθοδος όμως δεν είναι βολική στα ραδιο - τερματικά εξαιτίας του υψηλού κόστους και και των επιπλέον απαιτούμενων υλικών. Η μέθοδος αποφυγής συγκρούσεων(CA) αναπτύχθηκε με σκοπό να εξυπηρέτηση το μηχανισμό CSMA στα ασύρματα δίκτυα και είναι η βασική μέθοδος πρόσβασης που υιοθετείται από το πρότυπα 802,11.

3.1.3 IEEE 802.11 Frequency Hopping Spread Spectrum

Αρχικά στο 802.11 υποστηρίζονταν δύο στρατηγικές μετάδοσης : η frequency hopping spread spectrum και η (FHSS) and direct-sequence spread spectrum (DSSS).

Η 802,11 FHSS PHY προορίστηκε να λειτουργεί στην ζώνη συχνοτήτων 2,4 GHz με ταχύτητα 1 ή 2 Mbps. Το FHSS σύστημα απορροφήθηκε από τα πρότυπα 802.11b αφού διαπιστώθηκε ότι εμπεριέχει δύο τεχνικές μετάδοσης και για ένα πρότυπο σήμαινε ότι ήταν απαραίτητα δύο είδη (ασυμβίβαστα) εξοπλισμού για την εφαρμογή του προτύπου, έτσι η DSSS αποδείχθηκε ότι ήταν η πιο αξιόπιστη τεχνική. Ο εξοπλισμός που κληρονομήθηκε από το 802,11 δεν είναι συμβατός με τα τρέχοντα πρότυπα. Ωστόσο, αναφέρεται μόνο και μόνο για να γίνει κατανοητό το γιατί προτιμήθηκε το DHSS για τα 802,11 δίκτυα.

Όταν χρησιμοποιείται η FHSS μέθοδος, ο πομπός μετατοπίζει την κεντρική συχνότητα αρκετές φορές το δευτερόλεπτο και τόσο ο πομπός όσο και ο δέκτης παραμένουν συγχρονισμένοι επειδή το κάθε «βήμα » πραγματοποιείτε σύμφωνα με έναν ψευδοτυχαίο κανονισμό τον οποίο γνωρίζει η κάθε συσκευή. Στις Ηνωμένες Πολιτείες, η FCC ορίζει ότι τουλάχιστον 75 διακριτές συχνότητες πρέπει να υιοθετηθούν για κάθε κανάλι μετάδοσης, και ότι ένα σήμα δεν μπορεί να παραμείνει σε οποιαδήποτε συγκεκριμένη συχνότητα για περισσότερο από 400ms. Στα 802.11, το μέγιστο μήκος ενός πακέτου είναι περίπου 30 ms, και τα «βήματα» απέχουν 1 MHZ το ένα από το άλλο. Το FHSS μπορεί να υιοθετηθεί και για τις αναλογικές και ψηφιακές επικοινωνίες, αλλά εφαρμόζεται αυτήν την περίοδο πρώτιστα για τις ψηφιακές μεταδόσεις. Εάν 75 παρακείμενες συχνότητες χρησιμοποιούνται, τότε το εύρος ζώνης που απαιτείται για μια μετάδοση είναι 75 φορές μεγαλύτερο από όταν χρησιμοποιείται μόνο μια συχνότητα - το φάσμα είναι εξαπλωμένο σε μια μεγαλύτερη μερίδα της ζώνης μετάδοσης (για αυτό και «Frequency Hopping Spread Spectrum». Το αρχικό κίνητρο για την ανάπτυξη αυτής της τεχνικής ήταν η επιθυμία να αποφευχθεί το εχθρικό μπλοκάρισμα ενός ραδιο σήματος. Εάν μια μετάδοση μεταπηδήσει σε μια φραγμένη συχνότητα, τα δεδομένα που αποστέλλονται μάταια σε αυτή την συχνότητα επανεκπέμπονται σε επόμενο βήμα. Για τα ασύρματα δίκτυα, η FHSS έχει μια επιθυμητή «παρενέργεια: » Ελαχιστοποιεί τις πιθανότητες ότι οι διαφορετικοί πομποί του δικτύου θα αντιμετωπίσουν την παρέμβαση οι μεν από τους δε, διαφορετικά το δίκτυο θα μπορούσε ενδεχομένως να τεθεί εκτός λειτουργίας.

3.1.4 IEEE 802.11 Direct Sequence Spread Spectrum

Η διαμόρφωση DSSS διαδίδει ένα σήμα πάνω από μία ευρεία ζώνη πολύ χαμηλής ισχύος. Τα αρχικά 802.11 πρότυπα υποστήριξαν DSSS ρυθμούς δεδομένων 1 και 2 Mbps στη ζώνη των 2.4-Ghz. Το ευρέως διαδεδομένο σήμα μπορεί να ανακτηθεί από έναν συμβατό δέκτη παρά την παρεμβολή στενής ζώνης , εντός του φάσματος και οι εξωτερικοί παράγοντες που «κρυφακούν» το δίκτυο μπορεί να ερμηνεύσουν κάποια από τα αδύναμα σήματα στενής ζώνης που παράγονται από την DSSS ότι είναι θόρυβος. Σύμφωνα με τα πρότυπα 802,11, οι DHSS πομποί διαδίδουν κάθε bit δεδομένων σε 11 μικρότερα τμήματα, που ονομάζεται chip, και αυτά τα chips, μεταδίδονται, και διαχέονται πάνω από ένα εκτεταμένο φάσμα, για την ανάκτηση και το "despreading" από το DHSS δέκτη. Αυτή η διαδικασία τεμαχισμού, αυξάνει την πιθανότητα ο παραλήπτης να ανακτήσει τα αρχικά δεδομένα με την πρώτη προσπάθεια. Αν κάποια μέρος του chip χαθεί, ο παραλήπτης μπορεί να χρησιμοποιήσει στατιστικές τεχνικές για να προσδιορίσει ποιό ήταν το αρχικό, χωρίς να επανεκπεμφθεί το chip. Το σήμα είναι αποτελεσματικά «δυνατότερο» από το να εκπέμπονταν τα δεδομένα ακατέργαστα. Με άλλα λόγια, αυτή η μέθοδος μετάδοσης είναι συμπαγή.

Η διαμόρφωση 802,11 DHSS χωρίζει την μπάντα των 2.4 GHz σε 14 κανάλια των 5 MHz, 11 εκ των οποίων είναι διαθέσιμα για χρήση στις Ηνωμένες Πολιτείες και τον Καναδά (δεν είναι όλα διαθέσιμα οπουδήποτε). Εξαιτίας της διάδοσης του σήματος, τα DHSS κανάλια που απέχουν 30 MHz το ένα από το άλλο την άλλη μπορεί να παρεμβάλλονται μεταξύ τους. Αυτό σημαίνει ότι μόνο τρεις WLANs θα πρέπει να λειτουργούν ταυτόχρονα στην ίδια περιοχή για να διαβεβαιώσουν μη απειλητική αξιοπιστία.

Τα αρχικά 802,11 πρότυπα χρησιμοποίησαν την μέθοδο differential binary phase-shift keying (DBPSK) για εκπομπή στα 1 Mbps και τη μέθοδο differential quadrature phase-shift keying (DQPSK) για εκπομπή στα 2 Mbps.

3.1.5 Ο λόγος επικράτησης του DSSS

Ενώ το FHSS διαβιβάζει πέρα από ένα ευρύ φάσμα σε πολυάριθμες περιορισμένης ζώνης συχνότητες, το εύρος ζώνης του DSSS είναι πάντα ευρύ. επομένως το FHSS χρειάζεται ένα πολύ πιό αργό ποσοστό δειγματοληψίας στην εφαρμογή του και μπορεί αναλόγως να εφαρμοστεί με τη λιγότερη δαπάνη. Ο αποφασιστικός παράγοντας, εντούτοις, είναι ότι τα συστήματα DSSS παρέχουν ένα γερό σήμα με καλύτερη περιοχή κάλυψης από τα FHSS. Αυτές οι ενισχύσεις είναι ακριβώς αυτό που τα WLANs απαιτούν.

3.1.6 3.1.6 IEEE 802.11 Προδιαγραφές για υπέρυθρες

Πολλές σκέψη και εργασία αφιερώθηκε στα 802.11 πρότυπα σχετικά με τη χρήση των σημάτων IR. Δυστυχώς με μικρό ώφελος. Η κατασκευή ενός WLAN που χρησιμοποιεί την τεχνολογία IR απαιτεί οι συσκευές να τοποθετούνται πιο κοντά από ότι στη χρησιμοποίηση των ραδιο σημάτων, και αυτό μπορεί να είχε αποτρέψει την εφαρμογή τους. Επιπλέον αν και τα 802.11 πρότυπα επιτρέπουν στις IR συσκευές να μην βρίσκονται στην ίδια ευθεία , υπάρχει μία κοινή αντίληψη ότι οι IR συσκευές πρέπει να «στοχεύουν» η μία την άλλη όπως μια TV με το τηλεχειριστήριο της. Ένα άλλο μειονέκτημα μπορεί να είναι ότι τα 802.11 LANs που βασίζονται σε υπέρυθρες προορίζονται να λειτουργούν μόνο σε εσωτερικούς χώρους, περιορισμένα από τους εξωτερικούς τοίχους. Σε κάθε περίπτωση, δεν υπάρχει κανένα ασύρματο προϊόν δικτύωσης διαθέσιμο σήμερα που να εφαρμόζει αυτό το IR PHY.

Τα 802,11 υπέρυθρα (IR) PHY ορίζουν ότι το φως στο 850 με 950 nm χρησιμοποιείται για σήματα και επιτρέπει την οικοδόμηση ενός πραγματικού LAN συστήματος. Το εύρος αυτών των σημάτων, με ευαίσθητους δέκτες είναι περίπου 20 m. Ωστόσο, σε ένα περιβάλλον χωρίς αντανακλαστικές επιφάνειες, το εύρος μπορεί να μειωθεί.

3.1.7 IEEE 802.11b Συμπληρωματικά πρότυπα στα 802.11 πρότυπα

Το IEEE 802.11b ,συμπλήρωμα των αρχικών 802,11 προτύπων, καθορίζεται σήμερα ως το πιο κοινό ασύρματο πρότυπο, Wireless Fidelity (Wi-Fi). Είναι επίσης γνωστό ως 802,11 High Rate, και υποστηρίζει ταχύτητες μέχρι 11 Mbps (συγκρίσιμη με την ταχύτητα των 10 Mbps του αρχικού 802,3 Ethernet προτύπου). Το 802.11b λειτουργεί στην ίδια ζώνη συχνοτήτων 2,4 GHz όπως και το 802.11. Μέχρι το 802.11b, τα IEEE 802.11 δίκτυα λειτουργούσαν σε ταχύτητες μόνο 1 ή 2 Mbps. Η ταχεία αύξηση της δημοτικότητάς του 802.11b οφείλεται λόγω της ταχύτερης μετάδοσης δεδομένων. Δεν ήταν πλέον η ασύρματη τεχνολογία πιο αργή σε σχέση με το πρότυπο Ethernet. Οι εργασίες τώρα πια σε ένα ασύρματο δίκτυο μπορούν να γίνουν περίπου στον ίδιο χρόνο, όπως και σε ένα ενσύρματο δίκτυο. Το 802.11b λόγω της εκτεταμένης εμπορικής διαφήμισης που είχε έγινε προσιτό στα οικιακά δίκτυα.

Είναι σημαντικό να συνειδητοποιήσουμε ότι μόνο το 802.11b ορίζει ένα νέο είδος PHY και MAC υπόστρωμα για τα 802.11, χωρίς να αποτελεί εξ ολοκλήρου νέα προσέγγιση στην ασύρματη επικοινωνία. Το LLC υπόστρωμα (του OSI επιπέδου δεδομένων) δεν χρειάζεται να αλλάξει για το 802.11b. Ωστόσο, το 802.11b παρουσιάζει δύο νέα δύο υπό-επίπεδα στο PHY: το υποεπίπεδο PLCP και το υπο-επίπεδο PMD. Το PMD παρέχει μεθόδους εκπομπής και λήψης δεδομένων μεσα από ένα ασύρματο μέσο ανάμεσα σε δύο ή και περισσότερους STAs, όπου ο καθένας χρησιμοποιεί ένα σύστημα υψηλων – ρυθμών μετάδοσης (11 Mbps). Το PLCP επιτρέπει στο MAC να λειτουργεί με ελάχιστη εξάρτηση από το PMD υπόστρωμα, διευκολύνοντας την παροχή των MAC υπηρεσιών (όπως ασύγχρονη μεταφορά δεδομένων).

Μια άλλη εμφανής βελτίωση που θεσπίστηκε με το 802.11b αφορά τις διαδικασίες εκπομπής δεδομένων. Τα πρωτότυπα 802,11 πρότυπα (1997) υποστήριζαν δύο εντελώς διαφορετικές μεθόδους κωδικοποίησης την FHSS και την DSSS - προκειμένου να χορηγήσουν κάποια ευελιξία στις εφαρμογές. Όπως αποδεικνύεται, αυτό οδήγησε σε σύγχυση και ασυμβατότητα μεταξύ του εξοπλισμού. Η αναβάθμιση του 802.11b μείωσε την χρήση του FHSS για χάρη του DSSS. Το DSSS έχει αποδειχθεί ότι είναι πιο αξιόπιστο από το FHSS, και θέτοντας μια μέθοδο κωδικοποίησης εξαλείφεται το πρόβλημα ύπαρξης ενός ενιαίου πρότυπου που περιλαμβάνει δύο είδη εξοπλισμού που δεν είναι συμβατά μεταξύ τους. Φεύγοντας από το FHSS, αυτό, σημαίνει ότι οι 802.11b συσκευές δεν είναι συμβατές με τις 802,11 συσκευές που χρησιμοποιούν το FHSS. Είναι συμβατές με τις συσκευές 802,11 που χρησιμοποιούν το DSSS, και επειδή τίποτα δεν έχει αλλάξει στο LLC υπόστρωμα, μπορούν να λειτουργούν σε αρμονία με το πρότυπο ενσύρματο Ethernet.

3.1.8 IEEE 802.11g Standard

Τα πρότυπα IEEE 802.11g τροποποιούν τα αρχικά 802,11 πρότυπα για να καταστεί δυνατός ο 54-Mbps ρυθμός δεδομένων με διάδοση στα 2.4-MHz. Τα πρότυπα 802.11g έχουν σχεδιαστεί ώστε να είναι συμβατά με πρότυπα 802.11b – και τα δύο μοιράζονται την ίδια ISM μπάντα. Το extended rate physical (ERP) στρώμα εισάγεται προκειμένου να ενεργοποιήσει υψηλότερους ρυθμούς μετάδοσης δεδομένων.

Η ανάδρομη συμβατότητα με το 802.11b σημαίνει ότι οι 802.11b STAs μπορούν να συνδεθούν με τα 802.11g APs, αν και μόνο σε 11-Mbps ρυθμούς, και ότι οι 802.11g STAs μπορούν να συνδεθούν με τα 802.11b APs, και πάλι στον χαμηλό ρυθμό. Αυτό σημαίνει ότι οι χρήστες μπορούν να αναπτύξουν το νέο εξοπλισμό 802.11g ένα κομμάτι τη φορά και όχι όλα με τη μία, χωρίς να χάσουν την λειτουργικότητα του δικτύου τους.

Το 802.11g χρησιμοποιεί την τεχνική OFDM, όπως το 802.11a, καθώς και το DSSS, όπως το 802.11b. Όλοι οι ρυθμοί δεδομένων που υποστηρίζονται στο 802.11a και 802.11b υποστηρίζονται και στο 802.11g. Ο Πίνακας 3.4 παραθέτει τους ρυθμούς δεδομένων για το 802.11g, τα είδη μετάδοσης και της διαμόρφωσης των συστημάτων.

Οι 802.11b συσκευές δεν μπορούν να εντοπίσουν σωστά αν το μέσο που θέλουν να χρησιμοποιήσουν είναι απασχολημένο, όταν τη 802.11g συσκευές το χρησιμοποιούν για

μετάδοση. Ως εκ τούτου, τα πρότυπα 802.11g παρέχουν μηχανισμούς προστασίας για τα 802.11g STAs λειτουργώντας τα σε ένα μικτό 802.11b/802.11g περιβάλλον, συμπεριλαμβανομένων RTS και CTS μηνυμάτων. Η 802.11g ρυθμαπόδοση είναι μεγαλύτερη από αυτήν του 802.11b για την ίδια απόσταση, με οποιονδήποτε από τους μηχανισμούς προστασίας. Υπάρχουν επίσης μηχανισμοί προστασίας για τα δίκτυα 802.11g που αναγνωρίζουν ότι κάποιο 802.11b δίκτυο λειτουργεί σε κοντινή απόσταση και αποτρέπουν την ύπαρξη παρεμβολών.

Data rate (Mbps)	Transmission type	Modulation scheme
54	OFDM	64 QAM
48	OFDM	64 QAM
36	OFDM	16 QAM
24	OFDM	16 QAM
18	OFDM	QPSK1
12	OFDM	QPSK
11	DSSS	CCK2
9	OFDM	BPSK3
6	OFDM	BPSK
5.5	DSSS	CCK
2	DSSS	QPSK
1	DSSS	BPSK

Πίνακας 3-3 Ρυθμοί μετάδοσης στο 802.11g, τύποι μετάδοσης, και σχήματα διαμόρφωσης.

3.1.9 IEEE 802.11a Συμπληρωματικά στα 802.11 Πρότυπα

Το IEEE 802.11a το συμπλήρωμα των αρχικών 802,11 προτύπων ορίζεί ένα νέο PHY για μεταδόσεις έως και 54 Mbps στη ζώνη των 5 GHz με χρήση COFDM. Το MAC υπόστρωμα παραμένει αμετάβλητο σε σχέση με την αρχική έκδοση 802,11. Η ζώνη των 5-GHz είναι επίσης γνωστή ως εθνική υποδομή πληροφοριών χωρίς άδεια (U-NII). Το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων (ETSI) HIPERLAN-2 WLANs χρησιμοποιεί επίσης το OFDM, μιας και είναι η πιο δημοφιλής τεχνική διαμόρφωσης για υψηλής ταχύτητας WLANs σε εσωτερικούς χώρους.

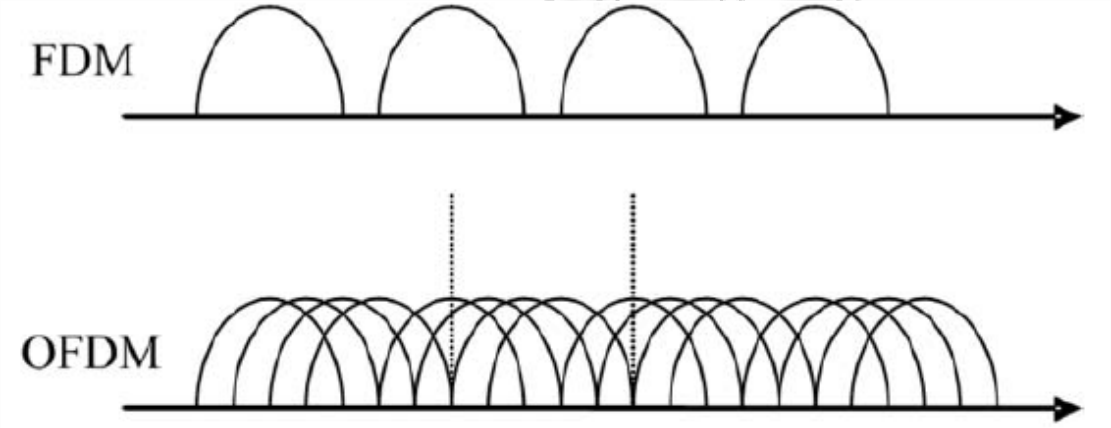
Το πρωτόκολλο COFDM καθορίζεται στα πρότυπα 802.11a. Χρησιμοποιεί υψηλότερες συχνότητες από το HR/DSSS (το πρωτόκολλο του 802.11b) και διάφορα σχέδια διαμόρφωσης, το COFDM παρέχει ρυθμούς δεδομένων 6, 9, 12, 18, 24, 36, 48, και 54 Mbps. Οι 802.11a συσκευές προσπαθούν να επικοινωνήσουν στον υψηλότερο ρυθμό μετάδοσης και μεταβαίνουν στον αμέσως χαμηλότερο στη περίπτωση που εμφανιστούν αρκετά λάθη μετάδοσης. Όσο πιο κοντά είναι οι συσκευές η μια με την άλλη τόσο πίο γρήγοτα επικοινωνούν μεταξύ τους εξαιτίας της υψηλής δύναμης του σήματος. Οι μικτότεροι ρυθμοί μετάδοσης μπορούν να καλύψουν αποστάσεις έως 100 μέτρα.

Τα πλεονεκτήματα του COFDM έναντι του HR/DSSS (802.11b) περιλαμβάνουν υψηλότερους ρυθμούς μετάδοσης, περίπου τέσσερις φορές περισσότερα διαθέσιμα κανάλια, λιγότερο κίνδυνο παρέμβασης από τις συσκευές Bluetooth και τα φορητά τηλέφωνα που

λειτουργούν στην ίδια ζώνη ISM, και μέχρι πέντε φορές μεγαλύτερη ρυθμαπόδοση σε μια λειτουργία γραφείου. Ένας διαχειριστής δικτύου 802.11a μπορεί να επιτύχει κέρδος ρυθμαπόδοσης με την ανάπτυξη APs με ίδιο κόστος με ένα δίκτυο 802.11b, ή μπορεί να κρατήσει τη ρυθμαπόδοση του 802.11b αναπτύσσοντας φθηνότερα APs.

Το OFDM είναι μια παραλλαγή της πολυπλεξίας συχνότητας (FDM). Και στα δύο το εύρος ζώνης χωρίζεται σε μικρότερους "Subcarriers" και τα subcarriers χρησιμοποιούνται ως κανάλια μετάδοσης δεδομένων. Το FDM χρησιμοποιήθηκε στην πρώτη γενιά κινητών τηλεφώνων, αλλά σπαταλιέται εύρος ζώνης αφήνοντας ένα αχρησιμοποίητο κανάλι μεταξύ των subcarriers σαν ασφάλεια για πιθανές παρεμβολές από το ένα τηλέφωνο στο άλλο. Αντίθετα το OFDM επιλέγει κανάλια που μπορούν να επικαλύπτονται χωρίς παρεμβάλλεται το ένα στο άλλο διατηρώντας το εύρος ζώνης.

OFDM κωδικοποιεί μια μονή μετάδοση σε πολλαπλούς "Subcarriers", αντίθετα μία άλλη αναδυόμενη τεχνική κωδικοποίησης, η τεχνική CDMA, η οποία χρησιμοποιεί μαθηματικά κατασκευάσματα πιο πολύπλοκα από του OFDM για να στείλουν πολλαπλές μεταδόσεις σε έναν μεταφορέα. Το πλεονέκτημα των λιγότερο περίπλοκων μαθηματικών του OFDM είναι αποταμίευση στην επεξεργασία αλγορίθμων όταν αποκωδικοποιούνται οι μεταδόσεις στο δέκτη. Στο OFDM, ένα ευρύ κανάλι συχνότητας διαιρείται σε υπο-κανάλια που κάθε ένα μεταφέρει δεδομένα και τα υπο-κανάλια είναι πολυπλεγμένα σε ένα μονό γρήγορο κανάλι μετάδοσης.



Εικόνα 3-4 FDM έναντι OFDM

Το OFDM επιτυγχάνει ένα κέρδος στη ρυθμαπόδοση έναντι του FDM εκμεταλλεύοντας την μαθηματική ορθογονικότητα. Στην ουσία, οι επικαλυπτόμενοι υπομεταφορείς ολισθαλινουν στο πεδίο συχνότητας όταν οι γειτονικοί υπομεταφορείς έχουν μηδενικό εύρος (σχήμα 4.7). Το OFDM παίρνει το κωδικοποιημένο σήμα για κάθε υπο-κανάλι και χρησιμοποιεί τον αντίστροφο γρήγορο μετασχηματισμό Φουριέ (IFFT) για να δημιουργήσει ένα σύνθετο κυματοειδές από τη δύναμη του κάθε subchannel. Οι δέκτες OFDM μπορούν έπειτα να εφαρμόσουν το FFT σε ένα λαμβανόμενο κυματοειδές για να εξαγάγουν το εύρος κάθε συστατικού.

4 .3GPP – WLAN Interworking

Interworking Architecture

4.1 Εισαγωγή

Τα πρώτα κυψελωτά τηλεφωνικά σύστημα (τα πρώτα ασύρματα δίκτυα) εισήχθησαν στα τέλη της δεκαετίας του 1970. Διαμορφώθηκαν μετά τα ενσύρματα δίκτυα και χρησιμοποιούσαν για μετάδοση αναλογικά δεδομένα πάνω από ένα κινητό δίκτυο. Αρχικά ονομάστηκαν ασύρματα συστήματα πρώτης γενιάς (1G) όταν η επόμενη γενεά των κυψελοειδών δικτύων επεκτάθηκε στη δεκαετία του '90. Αυτά τα δίκτυα «δεύτερης γενιάς» (2G) μετέδιδαν ψηφιακά φωνητικά δεδομένα στα κινητά δίκτυα. Οι συμπληρωματικές ασύρματες εφαρμογές όπως e-mail και Internet συχνά αναφέρονται και ως τεχνολογίες 2.5G . Αυτήν την περίοδο είναι σε λειτουργία η τρίτη γενιά (3G) της ασύρματης τεχνολογίας. Σχεδιάστηκε για εφαρμογές μεγάλων πολυμέσων με ρυθμούς μετάδοσης από 128 kbps εώς και 10 Mbps, και αναβαθμίζονται σε 100 Mbps για τα WLANs. Οι προσπάθειες έρευνας και ανάπτυξης στρέφονται τώρα στην επόμενη γενεά της ασύρματης τεχνολογίας, που αποκαλείται 4G ή B3G (Beyond 3G). Αυτά τα συστήματα μπορούν να επιτύχουν ρυθμούς μετάδοσης μέχρι 1Gbps με εύρος πάνω από 100MHz, Το έτος 2010 έχει τεθεί ως η προβλεπόμενη ημερομηνία για την εφαρμογή των B3G των συστημάτων (αλλά μερικές εφαρμογές θα επεκταθούν πιθανώς το 2006-2007). Η τεχνολογία B3G θα καταστήσει πιθανό να παρακολουθεί κάποιος ταινίες και τηλεόραση από ένα κινητό κυψελωτό τηλέφωνο. Για να συμβεί αυτό, θα πρέπει να αναβαθμιστούν πολλά τεχνολογικά σημεία των δικτύων, περιλαμβάνοντας βελτίωση των Ad Hoc κινητών δικτύων, των δορυφορικών συστημάτων, της κατανομής φάσματος, και των υψηλότερων ασύρματων ρυθμών μετάδοσης δεδομένων. Τα προτεινόμενα IEEE 802.20 πρότυπα θα συντονίσουν τις B3G προσπάθειες σχεδιασμού. Μια σημαντική πτυχή της διαδικασίας τυποποίησης θα είναι να παρέχει καθολική πρόσβαση στην ευρεία ποικιλία ασύρματων δικτύων που είναι ήδη σε χρήση. όπου το καθένα έχει το δικό τους εύρος , ρυθμό μετάδοσης και όρια κινητικότητας.

Πολλές ενδιαφέρουσες και χρήσιμες υπηρεσίες και εφαρμογές μπορούν να αναπτυχθούν, υποθέτοντας ότι η απανταχού και υψηλή B3G ασύρματη πρόσβαση είναι διαθέσιμη («πάντα συνδεδεμένη, παντού προσβάσιμη»). Μία από τις κύριες δυνάμεις πίσω από την ανάπτυξη του B3G είναι η απαίτηση για μεγαλύτερη απόδοση στα ποικίλα σενάρια. Οι σχεδιαστές του B3G περιλαμβάνουν κατασκευαστές τερματικού εξοπλισμού και υποδομής τους, ακαδημαϊκούς, επιχειρηματίες, φορείς παροχής υπηρεσιών, ρυθμιστικούς φορείς, και κυβερνητικούς οργανισμούς. Δεν θα πρέπει να αποτελεί έκπληξη το γεγονός ότι η εύρεση ενός καθολικού ορισμού της B3G/4G είναι ένα πολύ αόριστο έργο, ακόμη και μετά αρκετά χρόνια δραστηριότητας και πολλές προσπάθειες στη βιβλιογραφία.

Οι B3G σχεδιαστές στοχεύουν τους ακόλουθους τεχνικούς στόχους: (1) ρυθμούς μετάδοσης δεδομένων στα 100 Mbps και 1 Gbps σε μια τοπική περιοχή (2) δικτύωση IP (3) πανταχού παρούσες, κινητές επικοινωνίες (4) μικρότερη λανθάνουσα κατάσταση (5) καθυστερήσεις σύνδεσης λιγότερο από 500ms (6) καθυστερήσεις μετάδοσης λιγότερο από 50ms (7) δαπάνες ανά bit σημαντικά χαμηλότερες, ίσως 1/10th ή 1/100th χαμηλότερο από το 3G και (8) χαμηλότερο κόστος υποδομής, ίσως 1/10 χαμηλότερο από αυτό του 3G. (Εικόνα 4.1)

Data rates	100 Mbps in wide coverage, 1 Gbps in a local area
Networking	All-IP
Communications	Ubiquitous, mobile, seamless
Latency	Shorter than that of 3G
Connection delays	Less than 500 ms
Transmission delays	Less than 50 ms
Costs per bit	1/10 to 1/100 lower than that of 3G
Infrastructure cost	Lower, perhaps 1/10 lower than that of 3G

Εικόνα 4-1 Οι στόχοι των σχεδιαστών του B3G

Προβλέπεται ότι αυτός ο τύπος τεχνολογίας θα επιτρέψει την ενίσχυση του ηλεκτρονικού εμπορίου, θα προσθέσει στην παραγωγικότητα της εργασίας, και θα παρέχει τους τρόπους ώστε να βελτιωθεί ο προσωπικός ελεύθερος χρόνος. Η τεχνολογία B3G μπορεί μια μέρα να βρεθεί στα οχήματα, σε δημόσιους χώρους, την υγειονομική περίθαλψη, την εκπαίδευση, και στη βιομηχανία της διασκέδασης.

4.2 Network Elements

Παρακάτω περιγράφεται η αρχιτεκτονική διασύνδεσης και τα διαφορά δικτυακά στοιχεία που απαιτούνται προκειμένου να επιτευχθεί διασυνεργασία ανάμεσα στην τεχνολογία 3G και στα WLANs δίκτυα.

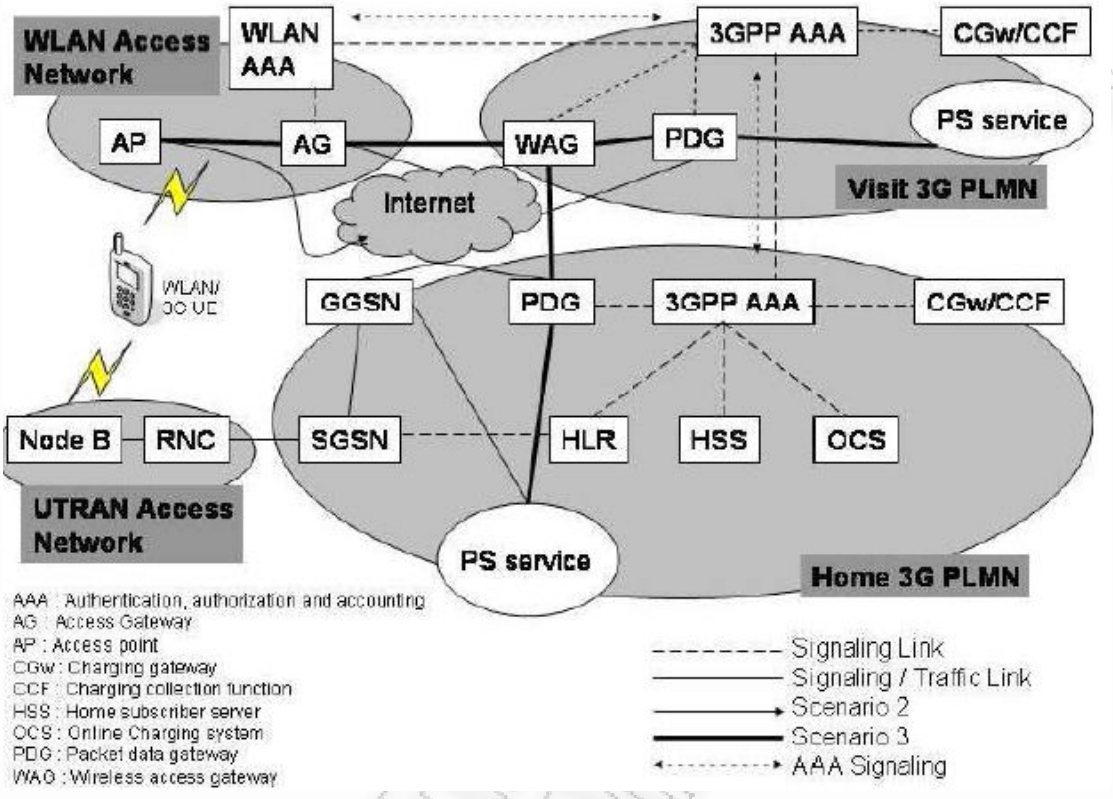
Τα κυριότερα συστατικά ανήκουν σε τρεις μεγάλες δικτυακές ενότητες όπου κάθε μία περιλαμβάνει διαφορετικά στοιχεία που συμβάλλουν στην ένωση των ενοτήτων μεταξύ τους, και περιγράφονται παρακάτω(Εικόνα 4.2) :

- Το *Home Environment (HE)* : Το HE περιλαμβάνει τον 3GPP Home AAA server και το PDG(Packet Data Gateway). Ο 3GPP home AAA Server βρίσκεται εντός του 3GPP δικτύου και ανακτά πληροφορίες αυθεντικοποίησης από το HLR/HSS του 3GPP Home Network του συνδρομητή. Επίσης είναι υπεύθυνο για την εκτέλεση της AKA διαδικασίας προς την κατεύθυνση του WLAN-UE. Το PDGW λειτουργεί ως πύλη εισόδου ενώ το UE έχει πρόσβαση στην υπηρεσία 3GPP packet data μέσω του WLAN.

- Το *Serving Network (SN)* : Στο SN ανήκουν το 3GPP AAA Proxy, το Access Point (AP) και το WAG (WLAN access gateway. Το AAA Proxy αντιπροσωπεύει μια λογική proxying λειτουργία, δηλαδή, όπου αναμεταδίδει τις AAA πληροφορίες μεταξύ του WLAN και του 3GPP Home AAA Server. Το AP είναι συσκευή υλικού όπου τερματίζει την ράδιο-σύνδεση που συνδέεται με ένα UE και λειτουργεί ως κόμβος επικοινωνίας για το UE προκειμένου να συνδεθεί με ένα ενσύρματο δίκτυο.

- Το *WLAN – UE :* Το WLAN-UE, μπορεί να είναι ένας φορητός προσωπικός υπολογιστής ή ένα PDA με μια WLAN κάρτα, και επιπλέον εξοπλισμένο με μια έξυπνη κάρτα UICC/USIM για την πρόσβαση στις WLAN διασυνεργαζόμενες υπηρεσίας.

Στις επόμενες ενότητες περιγράφονται τα επιμέρους συστατικά.



Εικόνα 4-2 Μοντέλο αναφοράς της διασυνεργασίας του 3GPP και του WLAN και η αρχιτεκτονική δικτύωσης.

4.2.1 WLAN UE

Το WLAN UE είναι ο εξοπλισμός των χρηστών που χρησιμοποιεί μια κάρτα UICC με την οποία ο κάθε 3GPP συνδρομητής μπορεί να έχει πρόσβαση στο WLAN AN με σκοπό την διασυνεργασία με το 3GPP. Το WLAN UE παρέχει τη δυνατότητα πρόσβασης μόνο στο WLAN, ή είναι ικανό να παρέχει ραδιο πρόσβαση και στο WLAN και στο 3GPP. Κάποια WLAN UE είναι ικανά να παρέχουν της ταυτόχρονης ραδιο πρόσβαση και στο WLAN και στο 3GPP. Ένα WLAN UE μπορεί να περιλαμβάνει διάφορους τερματικούς τύπους, των οποίων η ρύθμιση (π.χ. διεπαφή σε ένα UICC), η λειτουργία και το περιβάλλον λογισμικού δεν είναι υπό τον αποκλειστικό έλεγχο του 3GPP διαχειριστή , όπως ένας φορητός υπολογιστής, ή ένα PDA με WLAN κάρτα, αναγνώστη κάρτας UICC και κατάλληλες εφαρμογές λογισμικού.

Οι λειτουργίες του WLAN UE περιλαμβάνουν:

- Συσχέτιση με ένα I-WLAN
- αυθεντικοποίηση πρόσβασης σε WLAN βασισμένη σε EAP μεθόδους
- Επιλογή ενός κατάλληλου VPLMN για την περίπτωση roaming
- Κατασκευή κατάλληλου NAI

- Λήψη κατάλληλης IP. Εάν το WLAN UE προορίζεται για χρήση με το WLAN ANs υποστηριζόμενο IPV4 καθώς επίσης και με το IPV6, τότε θα πρέπει να είναι εξοπλισμένο με διπλή IP στοίβα.
- Εάν εφαρμόζονται μηχανισμοί QoS, το UE εφαρμόζει τους μηχανισμούς DiffServ μαρκάροντας το πεδίο DS των IP πακέτων σύμφωνα με τις QoS απαιτήσεις της εφαρμογής.
- Εάν οι μηχανισμοί QoS εφαρμόζονται το UE χαρτογραφεί το το DS πεδίο των IP πακέτων με συγκεκριμένες QoS παραμέτρους της WLAN τεχνολογίας.

Για WLAN 3GPP IP πρόσβαση το WLAN UE

- Χτίζει ένα κατάλληλο W-APN που χρησιμοποιείται για την επιλογή εξωτερικής IP δικτύου.
- Ζητά αίτηση για την επίλυση μιάς W-APN σε PDG διεύθυνση.
- Εάν οι IPv4 και IPv6 διευθύνσεις επιστρέφονται κατά τη διάρκεια της διαδικασίας ψηφίσματος, το WLAN UE θα επιλέξει τη διεύθυνση που έχει την ίδια μορφή με την δικιά του τοπική IP διεύθυνση (IPv4 ή IPv6).
- Καθιερώνει μια ασφαλή σήραγγα σε ένα PDG.
- Λαμβάνει μια απομακρυσμένη IP διεύθυνση.
- Επιτρέπει πρόσβαση στις υπηρεσίες που παρέχονται στην περιοχή PS των παρόχων.
- Επιτρέπει στους χρήστες να επιλέξουν τον τύπο πρόσβασης στο δίκτυο, δηλ. WLAN 3GPP IP Acces ή WLAN Direct IP Access.
- Δυνατότητα να υποδείξει εάν απαιτείται πολλαπλή αυθεντικοποίηση ή όχι κατά τη διαδικασία επικύρωσης tunnel. Αυτή η λειτουργία απαιτείται μόνο σε περίπτωση που συγκεκριμένο W-APN απαιτεί την επικύρωση και την έγκριση με τον εξωτερικό AAA server.

4.2.2 3GPP AAA Proxy

Το 3GPP AAA Proxy αποτελεί μία λειτουργία φιλτραρίσματος που κατοικεί στο Visited 3GPP δίκτυο. Η λειτουργία αυτή περιλαμβάνει.

- Αναμετάδοση των πληροφοριών AAA μεταξύ WLAN και του 3GPP AAA.
- Την επιβολή συγκεκριμένων κανόνων που προέρχονται από τις συμφωνίες περιαγωγής μεταξύ των 3GPP χειριστών και μεταξύ των WLAN χειριστών και των 3GPP χειριστών.
- Παρέχει τις πληροφορίες περιορισμού στο πεδίο πρόσβασης του WLAN που βασίζονται στις πληροφορίες έγκρισης από το εγχώριο δίκτυο.
- Υποβολή εκθέσεων σχετικά με τις πληροφορίες χρέωσης/λογιστικής ανά-χρηστών στο VPLMN σύστημα χρέωσης για τους χρήστες περιαγωγής.

Πρωτόκολλο μετατροπής όταν τα Wa και WD σημεία αναφοράς δεν χρησιμοποιούν το ίδιο πρωτόκολλο

Μόνο για 3GPP IP πρόσβαση.

- Λήψη ανά tunnel πληροφορίες τιμολόγησης με βάση το αναγνωριστικό του κάθε tunnel από το WAG και της χαρτογράφησης ενός αναγνωριστικού χρήστη και από το αναγνωριστικό ενός τούνελ από το PDG. Δημιουργία χρεωστικών εγγραφώ ανά χρήστη για τους χρήστες περιαγωγής.
- Λήψη των πληροφοριών έγκρισης που σχετίζονται με τα αιτήματα των συνδρομητών για τα W-APNs στο Home ή το Visited δίκτυο.
- Έγκριση της πρόσβασης στα W-APNs του Visited δίκτυο σύμφωνα με την τοπική πολιτική.
- Λήψη των κατάλληλων πληροφοριών πολιτικής επιβολής από τον AAA server και τις παρέχει στο WAG του VPLMN.

- Μπορεί να παρέχει τις κατάλληλες πληροφορίες δρομολόγησης σε ένα WLAN.

Οι 3GPP AAA Proxy λειτουργίες μπορούν να εμφανιστούν σε έναν ξεχωριστό φυσικό κόμβο δικτύων, μπορεί να εμφανιστούν στο 3GPP AAA Server ή σε οποιοδήποτε φυσικό κόμβο δικτύων.

4.2.3 3GPP AAA Server

Ο 3GPP AAA Server βρίσκεται εντός του 3GPP δικτύου. Υπάρχει μόνο ένας 3GPP AAA Server για οποιονδήποτε WLAN συνδρομητή που υπάγεται στο δίκτυο.:

Ο 3GPP AAA Server :

- Ανακτά τις πληροφορίες αυθεντικοποίησης και το προφίλ του κάθε συνδρομητή (συμπεριλαμβανομένων των πληροφοριών έγκρισης του συνδρομητή) από το HLR/HSS του 3GPP Home δικτύου του συνδρομητή.
- Αυθεντικοποιεί τον 3GPP συνδρομητή με βάση τις πληροφορίες επικύρωσης που ανακτώνται από το HLR/HSS. Το σήμα αυθεντικοποίησης μπορεί να περάσει μέσω των AAA proxies.
- Ενημερώνει τις πληροφορίες έγκρισης για πρόσβαση στο WLAN κάθε φορά που τροποποιείται η υπηρεσία συνδρομής του χρήστη, όταν ζητείται από HSS/HLR.
- Καταχωρεί (ο 3GPP AAA Server)κάθε διεύθυνση ή όνομά με το HLR/HSS για κάθε 3GPP συνδρομητή που επικυρώνεται και εξουσιοδοτείται.
- Κινεί τη διαδικασία εκκαθαρίσεων όταν ο 3GPP AAA Server διαγράφει τις πληροφορίες ενός συνδρομητή.
- Μπορεί να λειτουργεί επίσης και ως AAA Server.
- Διατηρεί την κατάσταση της σύνδεσης για το WLAN UE.
- Παρέχει την κατάσταση της σύνδεσης για το WLAN UE. σε άλλες οντότητες.
- Παράγει και εκθέτει τις πληροφορίες χρέωσης /λογιστικής ανά-χρήστη σχετικά με την άμεση WLAN IP πρόσβαση στο HPLMN σύστημα χρέωσης.
- Μεταφέρει την αυθεντικοποίηση ενός συνδρομητή σε έναν 3GPP AAA Server όταν ζητείται από το HSS/HLR.
- Εάν εφαρμόζονται οι μηχανισμοί QoS: ο 3GPP AAA Server εγκρίνει και αποθηκεύει το 3GPP WLAN QoS προφίλ. Το εξουσιοδοτημένο QoS προφίλ είναι βασισμένο στην πιο στενή αντιστοιχία του QoS προφίλ του συνδρομητή με τις οι ικανότητες/ πολιτικές του WLAN AN.

Για WLAN 3GPP IP πρόσβαση:

- Παρέχει στο PDG τη απομακρυσμένη διεύθυνση IP του WLAN UE, που παραλαμβάνεται από το HSS.
- Παρέχει στο AAA Proxy τις κατάλληλες πληροφορίες πολιτικής.
- Παρέχει τις απαραίτητες πολιτικές που επιβάλλονται, στο WAG στο HPLMN.
- Παρέχει τις απαραίτητες πληροφορίες δρομολόγησης στο WLAN AN.
- Εάν εφαρμόζονται οι μηχανισμοί QoS: ο 3GPP AAA Server εγκρίνει το 3GPP WLAN QoS προφίλ για τα tunnels. Το εξουσιοδοτημένο QoS προφίλ βασίζεται στο WLAN QoS προφίλ του συνδρομητή στις πληροφορίες συνδρομητή και αποθηκεύει το 3GPP WLAN QoS προφίλ για την WLAN 3GPP IP πρόσβαση όταν εκτελεστεί η διαδικασία αυθεντικοποίησης και έγκρισης

4.2.4 HLR/HSS

Το HLR/HSS εντοπίζεται μέσα στο 3GPP Home Network του συνδρομητή και είναι η οντότητα που περιέχει τα στοιχεία επικύρωσης και συνδρομής που απαιτούνται για τον 3GPP συνδρομητή για να έχει πρόσβαση στην διασυνεργαζόμενη υπηρεσία WLAN. Εκτός από άλλες πληροφορίες, το HSS περιέχει 3GPP WLAN QoS προφίλ, δεδομένα επικύρωσης και συνδρομής για τους 3GPP συνδρομητές.

Το HSS επίσης παρέχει πρόσβαση σε άλλες οντότητες στο WLAN UE's. Για αυτόν τον λόγο, το HSS πρέπει να αποθηκεύσει τη διεύθυνση IP του 3GPP AAA Server στον οποίον το WLAN UE είναι καταχωρημένο.

Όταν ένας 3GPP AAA Server εκτός από τον καταχωρημένο 3GPP AAA Server ενός συνδρομητή, ζητάει πληροφορίες αυθεντικοποίησης ή το προφίλ
του συνδρομητή, το HSS θα πρέπει να ζητήσει την μεταφορά της αυθεντικοποίησης στον καταχωρημένο 3GPP AAA Server παρέχοντας την διεύθυνση του 3GPP AAA Server σε αυτό.

4.2.5 WLAN Access Gateway (WAG)

Το WLAN Access Gateway εφαρμόζεται σε ένα σύστημα πρόσβασης με ενεργό το WLAN 3GPP IP. Το WLAN Access Gateway είναι μία πύλη μέσω της οποίας τα δεδομένα από και προς το WLAN δίκτυο πρόσβασης θα πρέπει να δρομολογούνται μέσω ενός PLMN για να παρέχουν ένα WLAN UE με 3G PS υπηρεσίες σε ένα WLAN 3GPP ενεργό σύστημα πρόσβασης.

Στην περίπτωση της περιαγωγής το WLAN Access Gateway εμφανίζεται στο VPLMN, ενώ στην περίπτωση μη-περιαγωγής στο HPLMN.

Το WLAN Access Gateway:

- Επιτρέπει στο VPLMN να παραγάγει τις πληροφορίες χρέωσης για τους χρήστες που έχουν πρόσβαση στο WLAN AN στην περίπτωση περιαγωγής.
- Επιβάλλει τη δρομολόγηση των πακέτων μέσω του PDG.
- Εκτελεί τη συλλογή πληροφοριών λογιστικής ανά tunnel, π.χ. αρίθμηση όγκου (αρίθμηση bytes) και υπολειπόμενου χρόνου, που χρησιμοποιούνται για τις τακτοποιήσεις των διά-χειριστών σε περίπτωση σεναρίου περιαγωγής όταν το σημείο αναφοράς Wu είναι μεταξύ του WLAN UE και του PDG στο εγχώριο δίκτυο. Οι πληροφορίες χρέωσης προωθούνται στο 3GPP AAA Proxy στο visited Network μέσω του σημείου αναφοράς Wg .

Τα πακέτα πρέπει μόνο να διαβιβάζονται όταν :

1. είναι μέρος μιας υπάρχουσας tunnel ή
2. είναι αναμενόμενα μηνύματα από το WLAN UEs. Αυτό περιλαμβάνει τα αιτήματα υπηρεσιών, και τα μηνύματα καθιερώσεων tunnels.

Εάν εφαρμόζονται οι μηχανισμοί QoS τότε υποστηρίζει το μηχανισμό DiffServ για uplink/downlink IP πακέτων.

Δεδομένου ότι το WAG δεν έχει μια πλήρη σχέση εμπιστοσύνης με το WLAN UE, δεν είναι ικανό να σταματήσει όλα τα μηνύματα. Εντούτοις, τα μηνύματα από μια άγνωστη διεύθυνση IP μπορούν εύκολα να απορριφθούν. Μπορούν να χρησιμοποιηθούν επίσης άλλες προσεγγίσεις. Πρόσθετοι τύποι μηνυμάτων φτάνουν στον έλεγχο των χειριστών. Επιπλέον, οι μεταφραστές διευθύνσεων δικτύων μέσα στο WLAN μπορούν να τροποποιήσουν τη διεύθυνση προέλευσης των πακέτων IP από το WLAN UEs. Η τροποποιημένη διεύθυνση πηγής μπορεί να συσχετιστεί σε ένα WLAN UE μέσω του PDG κατά τη διάρκεια της καθιέρωσης ενός tunnel και να παρέχεται στο WAG μέσω του 3GPP AAA Proxy/Server. Πριν από αυτό το σημείο, όλα τα πακέτα των tunnels θα δρομολογούνταν από WAG εκτός από

εκείνα που απορρίπτονται ενδεχομένως λόγω ορισμένων κανόνων FireWall που εφαρμόζονται στο WAG.

4.2.6 Packet Data Gateway (PDG)

Οι υπηρεσίες που βασίζονται σε 3GPP PS είναι προσπελάσιμες μέσω του Packet Data Gateway στο Home Network του χρήστη, ή στο PDG από το επιλεγμένο VPLMN. Η διαδικασία έγκρισης και επιλογής μιας υπηρεσίας (π.χ. W-APN επιλογής) και ο έλεγχος εγγραφής καθορίζει εάν μια υπηρεσία παρέχεται από το Home Network ή από το Visited Network. Αν η PDG προορίζεται να στηρίξει τις συνδέσεις από WLAN UES χρησιμοποιώντας IPv4 και IPv6 τοπικές διευθύνσεις, θα πρέπει να είναι εφοδιασμένο με μια διπλή στοίβα IP.

Η επιτυχής ενεργοποίηση μιας επιλεγμένης υπηρεσίας οδηγεί σε:

- Προσδιορισμός της IP διεύθυνσης του PDG που χρησιμοποιείται από το WLAN UE
- Εντοπισμός μιας WLAN UE απομακρυσμένης διεύθυνσης IP στο WLAN UE.
- Εγγραφή της WLAN UE τοπικής διεύθυνσης IP με το PDG και τη συσχέτιση αυτής της διεύθυνσης με τη WLAN UE. απομακρυσμένη IP διεύθυνση

Το Packet Data Gateway

- Περιλαμβάνει πληροφορίες δρομολόγησης των WLAN-3G συνδεδεμένων χρηστών.
- Δρομολογεί τα πακέτα δεδομένων που λαμβάνονται ή στέλνονται στους WLAN-3G συνδεδεμένους χρήστες.
- Εκτελεί μεταφράσεις και χαρτογραφήσεις διευθύνσεων.
- Εκτελεί ενθυλάκωση και από- θυλάκωση.
- Εγκρίνει ή απορρίπτει το ζητούμενο W-APN σύμφωνα με την απόφαση που λαμβάνεται από τον 3GPP AAA Server.
- Επιτρέπει εντοπισμό της WLAN UE απομακρυσμένης διεύθυνσης IP.

4.3 Reference Points

4.3.1 Wa reference point

Το σημείο αναφοράς Wa συνδέει το WLAN Access Network, ενδεχομένως μέσω ενδιάμεσων δικτύων, με το 3GPP Network (δηλαδή με το 3GPP AAA Proxy στην περίπτωση περιαγωγής και το 3GPP AAA server στην περίπτωση μη περιαγωγής). Πρωταρχικός σκοπός των πρωτοκόλλων που διέρχονται από αυτό το σημείο αναφοράς είναι η μεταφορά της αυθεντικοποίησης, της έγκρισης και των πληροφοριών χρέωσης με ασφαλή τρόπο. Επίσης η EAP αυθεντικοποίηση πρέπει να μεταφέρεται μέσω του Wa σημείου αναφοράς.

Η λειτουργία του σημείου αναφοράς είναι να μεταφέρει AAA πλαίσια:

- Μεταφέρει δεδομένα για σηματοδοσία αυθεντικοποίησης/έγκρισης ανάμεσα στο WLAN UE και στο 3GPP Network.
- Μεταφέρει δεδομένα χρέωσης για κάθε WLAN χρήστη για να ενεργοποιηθεί η online ή η offline χρέωση. Για να ελαχιστοποιηθούν οι απαιτήσεις του WLAN Access Network, η χρήση της online χρέωσης είναι προαιρετική και εξαρτάται από τη συμφωνία των διαχειριστών του WLAN AN και του 3GGP PLMN.
- Μεταφέρει κλειδιά με σκοπό την προστασία και την κωδικοποίηση της ραδιο-διεπαφής.

- Παρέχει στο WLAN πληροφορίες περιορισμένης πρόσβασης που βασίζονται στις εγκεκριμένες υπηρεσίες για τον κάθε χρήστη.

4.3.2 Wx reference point

Αυτό το σημείο αναφοράς βρίσκεται μεταξύ του 3GPP AAA Server και του HSS. Ο κύριος σκοπός των πρωτοκόλλων που διέρχονται από αυτό το σημείο αναφοράς είναι η επικοινωνία μεταξύ της WLAN AAA υποδομής και του HSS.

Η λειτουργία αυτού του σημείου αναφοράς είναι να ενεργοποιεί:

- Ανάκτηση των διανυσμάτων αυθεντικοποίησης, π.χ. για την επικύρωση USIM, από το HSS.
- Ανάκτηση πληροφοριών του συνδρομητή του WLAN AN από το HSS.
- Εγγραφή του 3GPP AAA Server ενός εξουσιοδοτημένου WLAN χρήστη στο HSS.
- Ένδειξη της αλλαγής του προφίλ των συνδρομητών μέσα στο HSS.
- Ανάκτηση των online/offline διαδικασιών χρέωσης από το HSS.
- Διαδικασία αποκατάστασης λαθών ανάμεσα στο HSS και στον 3GPP AAA Server.

4.3.3. D'/Gr' reference point

Αυτό το προαιρετικό σημείο αναφοράς βρίσκεται μεταξύ του 3GPP AAA Server και του HLR/HSS. Ο πρωταρχικός σκοπός του πρωτοκόλλου που διασχίζει αυτό το σημείο αναφοράς είναι επικοινωνία μεταξύ της WLAN AAA υποδομής και του HLR.

Όταν το HLR το καθιστά δυνατό η λειτουργία αυτού του σημείου αναφοράς είναι να επιτρέψει:

- Ανάκτηση των διανυσμάτων αυθεντικοποίησης, π.χ. για την επικύρωση USIM, από το HLR.
- Εγγραφή του 3GPP AAA Server ενός εξουσιοδοτημένου WLAN χρήστη στο HLR.
- Ένδειξη της αλλαγής του προφίλ των συνδρομητών μέσα στο HLR.
- Διαδικασία αποκατάστασης λαθών ανάμεσα στο HLR και στον 3GPP AAA Server.
- Ανάκτηση των online/offline διαδικασιών χρέωσης από το HLR.

Αν ο AAA 3GPP Server υποστηρίζει το D' σημείο αναφοράς, θα εμφανιστεί στην HLR / HSS ως VLR και πρέπει να συμπεριφέρεται σύμφωνα με την περιγραφή της συμπεριφοράς μιας VLR που υποστηρίζει το D σημείο αναφοράς.

Αν ο AAA 3GPP Server υποστηρίζει ο Gr' σημείο αναφοράς, θα εμφανιστεί στην HLR / HSS ως SGSN και πρέπει να συμπεριφέρεται σύμφωνα με την περιγραφή της συμπεριφοράς μιας SGSN που υποστηρίζει το Gr σημείο αναφοράς.

4.3.4. Wo reference point

Το Wo σημείο αναφοράς χρησιμοποιείται από τον 3GPP AAA Server για να επικοινωνεί με το 3GPP Online σύστημα χρέωσης (OCS). Ο κύριος σκοπός των πρωτοκόλλων που διέρχονται από αυτό το σημείο αναφοράς είναι η μεταφορά πληροφοριών online χρέωσης, ώστε να ασκεί έλεγχο πιστώσεων για την online χρέωση των συνδρομητών.

Η λειτουργία αυτού του σημείο αναφοράς είναι η μεταφορά:

- Δεδομένα Online χρέωσης.

Το Wo σημείο αναφοράς είναι παρόμοιο με την Ro διεπαφή που χρησιμοποιείται σήμερα στο 3GPP OCS.

4.3.5. Wf reference point

Το Wf σημείο αναφοράς εντοπίζεται ανάμεσα στον 3GPP AAA Proxy/Server και το 3GPP Offline σύστημα χρέωσης (OCS). Ο κύριος σκοπός των πρωτοκόλλων που διέρχονται από αυτό το σημείο αναφοράς είναι η μεταφορά πληροφοριών offline χρέωσης προς το 3GPP Offline σύστημα χρέωσης του διαχειριστή το οποίο εντοπίζεται στο Visited Network ή στο Home Network, ανάλογα με το που κατοικεί ο συνδρομητής.

Οι πληροφορίες που μεταφέρονται στο Offline σύστημα χρέωσης τυπικά χρησιμοποιούνται για :

- Την παραγωγή λογαριασμών για offline χρεώσεις συνδρομητών.
- Υπολογισμός της λογιστικής των διά-χειριστών από όλους τους χρήστες περιαγωγής. Αυτή η λογιστική χρησιμοποιείται για να κανονίσει τις πληρωμές μεταξύ του visited και home network διαχειριστή ή/και μεταξύ του home/visited δικτύου και του WLAN.

4.3.6. Wg reference point

Το σημείο αναφοράς WG ισχύει για την πρόσβαση στο WLAN 3GPP IP.
Αυτό είναι μια AAA διεπαφή ανάμεσα στον 3GPP AAA Server/Proxy και το WAG. Χρησιμοποιείται για :

- να παρέχει τις πληροφορίες που απαιτούνται από το WAG για να εκτελέσει τις λειτουργίες πολιτικής που επιβάλλονται στους εξουσιοδοτημένους χρήστες.
- να μεταφέρει πληροφορίες χρέωσης ανά tunnel από το WAG στον AAA proxy, μόνο για το σενάριο περιαγωγής.

4.3.7. Wn reference point

Το σημείο αναφοράς Wn εφαρμόζεται στην WLAN 3GPP IP πρόσβαση. Αυτό είναι το σημείο αναφοράς μεταξύ του δικτύου πρόσβασης WLAN και του WAG. Αυτή η διεπαφή χρησιμοποιείται για να αναγκάσει την κυκλοφορία σε μία WLAN UE σήραγγα να ταξιδέψει μέσω του WAG. Μπορούν να υπάρξουν διάφοροι διαφορετικοί τρόποι ώστε να εφαρμοστεί αυτή η διεπαφή. Η συγκεκριμένη μέθοδος για να εφαρμόσει αυτήν την διεπαφή υπόκειται στην τοπική συμφωνία μεταξύ του WLAN AN και του PLMN.

4.3.8. Wp reference point

Είναι το σημείο αναφοράς ανάμεσα στο WAG και στο PDG.

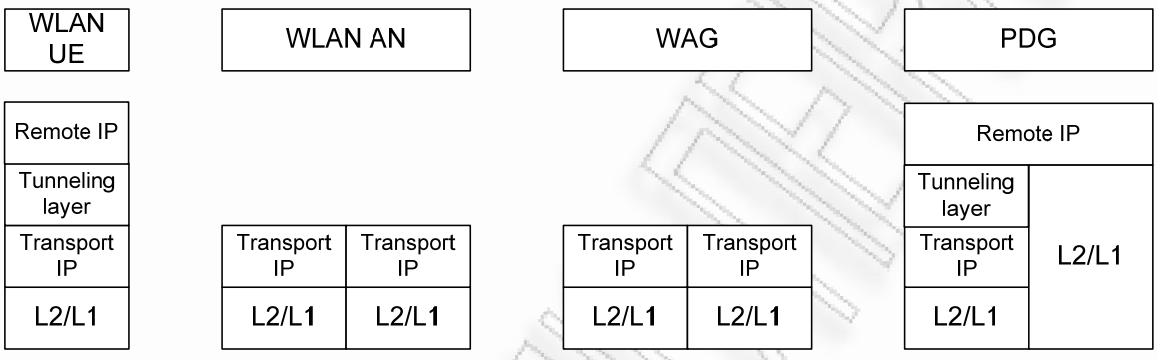
4.3.9. Wi reference point

Το Wi σημείο αναφοράς εφαρμόζεται στην WLAN 3GPP IP πρόσβαση. Αυτό είναι το σημείο αναφοράς μεταξύ του Packet Data Gateway και ενός δικτυού πακέτων δεδομένων. Το δίκτυο πακέτων δεδομένων μπορεί να είναι ένας εξωτερικός δημόσιος φορέας ή ιδιωτικό δίκτυο πακέτων δεδομένων.

Το Wi σημείο αναφοράς είναι παρόμοιο με το Gi σημείο αναφοράς που παρέχεται από το PS domain. Η διασύνδεση με δίκτυα πακέτων δεδομένων παρέχεται μέσω του Wi που βασίζεται σε IP. Τα κινητά τερματικά προσφέρουν υπηρεσίες μέσω του Wi σημείου αναφοράς.

4.4 Πρωτόκολλα

Η στοίβα πρωτοκόλλων ανάμεσα στο WLAN UE και στο PDG παρουσιάζεται στην παρακάτω εικόνα.



Εικόνα 4-3 Στοίβα πρωτοκόλλων ανάμεσα στο WLAN UE και στο PDG

4.4.1 Remote IP Layer

Το Remote IP επίπεδο χρησιμοποιείται από το WLAN UE ώστε να διευθυνσιοδοτήθει με το εξωτερικό δίκτυο πακέτων δεδομένων. Σε αυτό το επίπεδο, το WLAN UE διευθυνσιοδοτείται από την απομακρυσμένη διεύθυνση IP και τα πακέτα ανταλλάσσονται μεταξύ του WLAN UE και μια εξωτερικής οντότητας. Το PDG δρομολογεί τα remote IP πακέτα χωρίς να τα τροποποίηση.

4.4.2 Tunneling IP Layer

Το tunneling επίπεδο αποτελείται από την tunneling επικεφαλίδα, η οποία επιτρέπει ένα από άκρη σε άκρη tunneling μεταξύ του WLAN UE και του PDG. Χρησιμοποιείται για να ενθυλακώσει το remote IP layer στα IP πακέτα.

Όταν τα ενθυλακωμένα IP πακέτα κωδικοποιούνται ,η tunneling επικεφαλίδα περιέχει ένα πεδίο το οποίο χρησιμοποιείται για την αναγνώριση του peer και την αποκωδικοποίηση των πακέτων.

4.4.3 Transport IP Layer

Το επίπεδο Transport IP χρησιμοποιείται από ενδιάμεσα δίκτυα ή οντότητες και το WLAN AN με σκοπό τη μεταφορά των remote IP Layer πακέτων. Ανάμεσα στο WLAN UE και το WAG, το επίπεδο transport IP χρησιμοποιείται από το WLAN UE προκειμένου να αποκτήσει διεύθυνση όταν ανήκει στο WLAN AN, σε ενδιάμεσα δίκτυα και σε 3G δίκτυα.

Σε αυτό το επίπεδο το WLAN UE διευθυνσιοδοτείται από το την τοπική IP διεύθυνση.

Αυτή η τοπική διεύθυνση μπορεί να είναι :

- Μία ιδιωτική IPv4 διεύθυνση που εντοπίζεται από το WLAN AN, σε αυτή την περίπτωση απαιτείται το NAT στο WLAN AN και χρησιμοποιείται για να κάνει την τοπική IP διεύθυνση του WLAN UE ικανή να δρομολογηθεί στα ενδιάμεσα δίκτυα (εάν υπάρχουν) , στο VPLMN και στο HPLMN.
- Μία δημόσια (είτε IPv4 είτε IPv6) διεύθυνση που εντοπίζεται από το WLAN AN. Σε αυτήν την περίπτωση το NAT δεν χρειάζεται.

5. 3GPP – WLAN Security Architecture

5.1 Εισαγωγή.

Η αρχιτεκτονική ασφάλειας στα 3G δίκτυα βασίζεται σε τρεις βασικές αρχές ασφάλειας:

- Αυθεντικοποίηση (Επικύρωση)
- Εμπιστευτικότητα
- Ακεραιότητα

Αυθεντικοποίηση

Η αυθεντικοποίηση παρέχεται για να βεβαιώσει την ταυτότητα μιας οντότητας. Ένας κόμβος που θέλει να επικυρωθεί σε κάποιον πρέπει να παρουσιάσει την ταυτότητα του. Αυτό μπορεί να γίνει είτε με την γνωστοποίηση ενός μυστικού που μόνο οι κόμβοι που εμπλέκονται γνωρίζουν ή με να επιτρέψουν σε έναν τρίτο που και οι δύο κόμβοι εμπιστεύονται, να παρουσιάσει τις ταυτότητές τους.

Η χρήση της αυθεντικοποίησης είναι πολύ σημαντική σε μετάδοση στοιχείων όπου καμία ανθρώπινη συμμετοχή δεν εμπλέκεται, σε αντίθεση με την φωνητική τηλεφωνία, όπου η πραγματική φωνή ενός προσώπου μπορεί να είναι κάποιο είδος αυθεντικοποίησης.

Η αυθεντικοποίησης στα 3G δίκτυα χωρίζεται σε δύο μέρη:

- Αυθεντικοποίηση του χρήστη στο δίκτυο
- Αυθεντικοποίηση του δικτύου στο χρήστη

Και οι δύο αυτές οι διαδικασίες πραγματοποιούνται με την ίδια ανταλλαγή μηνυμάτων μεταξύ τους. Αυτό ονομάζεται «αυθεντικοποίηση με ένα πέρασμα» μειώνοντας τα μηνύματα που στέλνονται εκατέρωθεν. Μετά από αυτές τις διαδικασίες ο χρήστης θα είναι βέβαιος ότι το δίκτυο στο οποίο συνδέεται, εξυπηρετείται από το δικό του Home Network. Και το δίκτυο θα είναι σίγουρο ότι η ισχυριζόμενη ταυτότητα του χρήστη είναι αληθινή.

Η αυθεντικοποίηση σε αυτό το στρώμα απαιτείται για τους άλλους μηχανισμούς ασφάλειας όπως η εμπιστευτικότητα και η ακεραιότητα. Για το εξυπηρετούμενο δίκτυο είναι πολύ σημαντικό να γνωρίζει την πραγματική ταυτότητα του χρήστη έτσι να είναι βέβαιο ότι θα πληρωθεί για τις υπηρεσίες που προσφέρει. Ο χρήστης από την πλευρά του θέλει την επικύρωση για να σιγουρευτεί ότι οι υπηρεσίες που πληρώνει παραδίδονται σε αυτόν.

Εμπιστευτικότητα

Η εμπιστευτικότητα χρησιμοποιείται για να κρατήσει τις πληροφορίες ασφαλισμένες από τα ανεπιθύμητα συμβαλλόμενα μέρη. Με τους όλο και περισσότερους ανθρώπους να χρησιμοποιούν τα τερματικά και για προσωπική χρήση και για την επιχείρηση τους (π.χ. υπηρεσία online όπως τραπεζικές εργασίες) η ανάγκη για την ασφαλή επικοινωνία αυξάνεται γρήγορα.

Η εμπιστευτικότητα στα 3G δίκτυα επιτυγχάνεται με Ciphering στην επικοινωνία μεταξύ του συνδρομητή και του δικτύου και με αναφορά στο συνδρομητή από τις προσωρινές (τοπικές) ταυτότητες αντί της χρησιμοποίησης της σφαιρικής ταυτότητας, IMSI. Το Ciphering

πραγματοποιείται μεταξύ του συνδρομητή (USIM) και του RNC, και η εμπιστευτικότητα χρηστών είναι μεταξύ του συνδρομητή και του VLR/SGSN.

Οι πληροφορίες που πρέπει να είναι εμπιστευτικές είναι:

- Η ταυτότητα του συνδρομητή.
- Η τρέχουσα θέση του συνδρομητή.
- Τα δεδομένα του χρήστη (Τόσο η φωνή όσο και τα δεδομένα που μεταφέρονται πρέπει να διατηρούνται εμπιστευτικά)
- Τα δεδομένα σηματοδοσίας.

Ακεραιότητα

Μερικές φορές η προέλευση ή το περιεχόμενο ενός μηνύματος πρέπει να ελεγχθεί. Ακόμα κι αν έχει προέλθει από ένα προηγουμένως επικυρωμένο συμβαλλόμενο μέρος, το μήνυμα μπορεί να έχει αλλοιωθεί. Για να αποφευχθεί αυτό, είναι απαραίτητη η προστασία ακεραιότητας. Το ίδιο το μήνυμα μπορεί να μην είναι απαραίτητο να είναι εμπιστευτικό το σημαντικό πράγμα είναι η γνησιότητα του.

Η μέθοδος για την προστασία ακεραιότητας στα 3G δίκτυα είναι να παραχθούν ίχνη που προστίθενται στα μηνύματα. Τα ίχνη μπορούν μόνο να παραχθούν στους κόμβους που ξέρουν ότι τα κλειδιά παράγονται από το μυστικό κλειδί K. Αποθηκεύονται στο USIM και το AuC. Είναι πολύ σημαντικό να προσφερθεί η προστασία ακεραιότητας, ειδικά από τη στιγμή που το εξυπηρετούμενο δίκτυο συχνά χρησιμοποιείται από άλλον χειριστή από το χειριστή του συνδρομητή.

Η ιδιότητα που πρέπει να προστατευθεί ακέραια είναι τα μηνύματα σηματοδοσίας.

Στο φυσικό επίπεδο, τα bits ελέγχονται για την ακεραιότητα τους από το CRC checksum, αλλά αυτά τα μέτρα συμπεριλαμβάνονται μόνο για να επιτύχουν bit-error ελεύθερες μεταδόσεις στοιχείων μέσω του αέρα, και δεν είναι ισοδύναμα με την ακεραιότητα του επιπέδου μεταφοράς.

Το Authentication and Key Agreement (AKA) είναι από το πιο σημαντικά χαρακτηριστικά του 3G δίκτυο. Όλες οι άλλες υπηρεσίες εξαρτώνται από αυτά μιας και καμία higher-level δεν μπορεί να χρησιμοποιηθεί χωρίς την αυθεντικοποίηση του χρήστη.

Authentication:

- Αναγνώριση του χρήστη στο δίκτυο
- Αναγνώριση του δικτύου στο χρήστη

Key agreement:

- Παράγει το cipher key
- Παράγει το integrity key

Όταν εκτελείται το Authentication and Key Agreement:

- Ακέραια προστασία των μηνυμάτων
- Εμπιστευτική προστασία των δεδομένων σηματοδοσίας.
- Εμπιστευτική προστασία των δεδομένων του χρήση.

Οι διαδικασίες Authentication and Key Agreement λαμβάνουν χώρα στη USIM, στο SGSN/VLR και στο HLR/AuC. Μιας και το Serving Network διαιρείται στα τμήματα Packet Switched (PS) and Circuit Switched (CS), το VLR/SGSN σημαίνει είτε το SGSN/VLR κόμβο στο packet switched τμήμα ή το VLR/MSC κόμβο στο circuit switched τμήμα. Η διαδικασία αυθεντικοποίησης εκτελείται με τον ίδιο τρόπο και στα δύο τμήματα, οπότε δεν υπάρχει λόγος να γίνει διαχωρισμός των δυο διαδικασιών.

5.2 Μηχανισμοί Ασφάλειας.

Authentication and key agreement (AKA)

Το WLAN UE και ο AAA Server θα πρέπει να υποστηρίζουν και την EAP AKA αλλά και την EAP SIM μέθοδο. Ένα WLAN UE με καταχωρημένη μία USIM ή SIM πρέπει να ζητάει την διαδικασία αυθεντικοποίησης ανάλογα με την έξυπνη κάρτα που περιλαμβάνει. Η διαδικασία για την επιλογή της μεθόδου είναι η εξής :

1) Το WLAN UE πρέπει να στείλει ένα αναγνωριστικό (οτιδήποτε κ αν είναι , μόνιμο, ψευδόνυμο κτλ) στον AAA Server. Κατά την πρώτη αυθεντικοποίηση το αναγνωριστικό θα πρέπει να είναι το IMSI και το μήνυμα που περιλαμβάνει το αναγνωριστικό θα πρέπει επίσης να περιλαμβάνει και μία ένδειξη για την μέθοδο αυθεντικοποίησης που θα χρησιμοποιηθεί. Στις επόμενες αυθεντικοποιήσεις το αναγνωριστικό θα είναι μια προσωρινή ταυτότητα για την οποία ο AAA Server έχει ήδη μία ένδειξη για την σχετική μέθοδο αυθεντικοποίησης. Αυτή η μέθοδος δεν θα πρέπει να τροποποιείται από το WLAN UE.

2) Εάν ο AAA Server αναγνωρίσει την EAP μέθοδο αλλά όχι την ταυτότητα του χρήστη, πρέπει να ζητήσει νέο αναγνωριστικό χρησιμοποιώντας την EAP μέθοδο που αναγνωρίστηκε από το WLAN UE.

3) Εάν ο AAA Server αναγνωρίσει ταυτότητα του χρήστη, πρέπει να προσκομίσει τα AVs από το HSS. Εάν δεν ταιριάζουν με την λαμβανόμενη EAP μέθοδο, θα επικρατήσει η εγγραφή του χρήστη.

4) Εάν η ταυτότητα του χρήστη δεν αναγνωριστεί, ο AAA Server θα πρέπει να αποφασίσει ποια μέθοδο θα χρησιμοποιήσει(πρέπει να υπάρχει μια προκαθορισμένη μέθοδος για αυτήν την περίπτωση). Εάν αυτή η προκαθορισμένη μέθοδος δεν ταιριάζει με την εγγραφή του χρήστη, το WLAN UE απαντάει με ένα NACK στον AAA Server και στη συνέχεια ο AAA απαντάει με την άλλη μέθοδο μέχρι να ληφθεί κάποιο γνώριμο αναγνωριστικό.

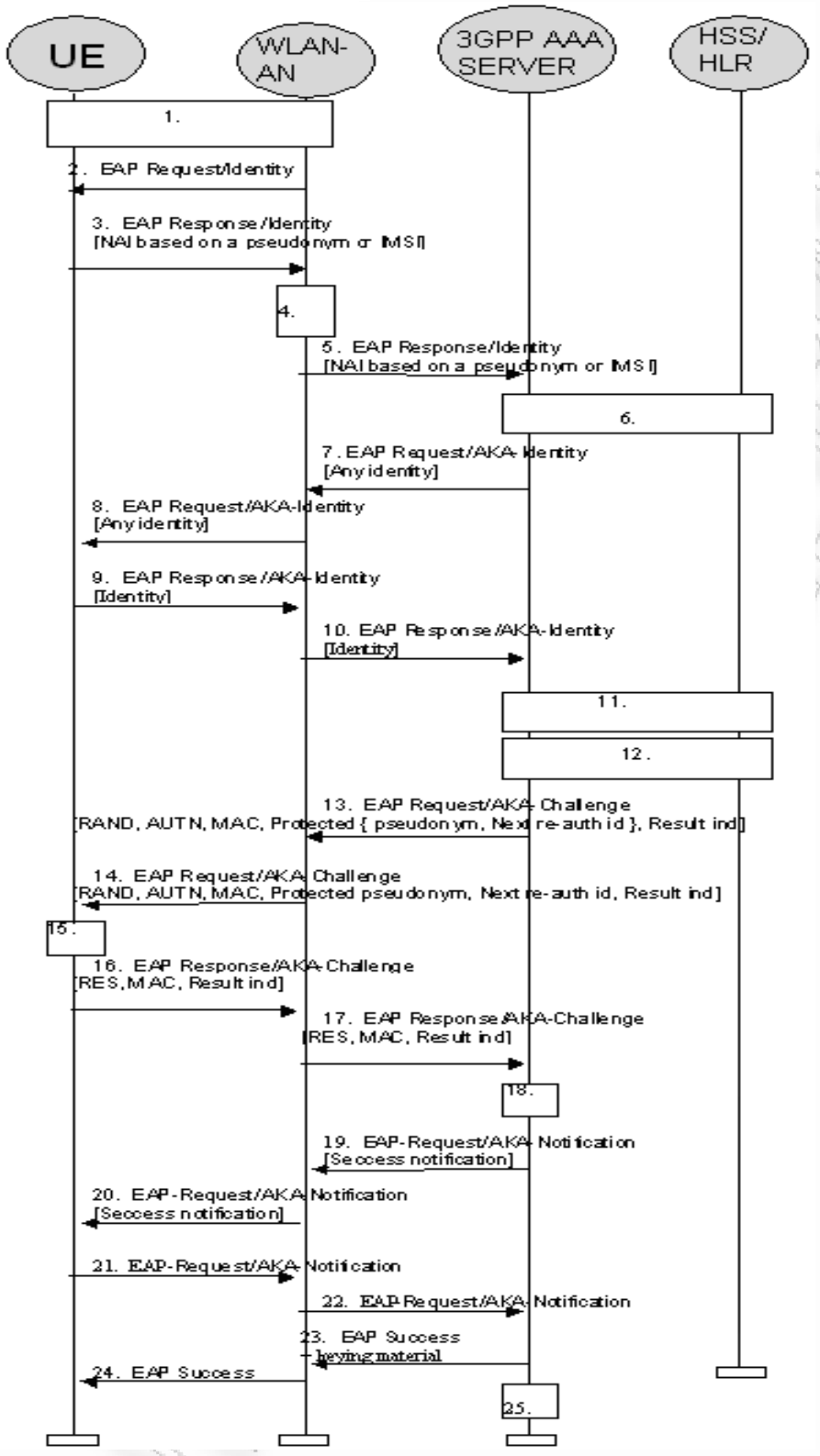
Το AKA θα πρέπει να αφιερωθεί μόνο για WLAN πρόσβαση, μιάς και τα κλειδιά που παρέχονται από τη SIM (Kc) ή τη USIM (CK,IK) κατά την διάρκεια του AKA πρέπει να αποθηκεύονται στην μνήμη του ME.

5.2.1 USIM-based WLAN Access Authentication

Η αυθεντικοποίηση βασισμένη στο USIM είναι μια αποδεδειγμένη λύση που ικανοποιεί τις απαιτήσεις επικύρωσης που προβλέπονται για τα 3G δίκτυα. Αυτή η μορφή αυθεντικοποίησης βασίζεται στο EAP-AKA

EAP/AKA Procedure

Στην παρακάτω εικόνα(5.1) περιγράφεται πως ο EAP/AKA μηχανισμός χρησιμοποιείται στο WLAN-3GPP σενάριο διασύνδεσης.



Εικόνα 5-1. Αυθεντικοποίηση βασισμένη στο EAP-AKA σχήμα

1) Μια σύνδεση καθιερώνεται μεταξύ του WLAN UE και του WLAN AN, χρησιμοποιώντας μια συγκεκριμένη διαδικασία τεχνολογίας ασύρματου LAN

2) Το WLAN AN στέλνει ένα EAP μήνυμα Request/ Identity στο WLAN UE.

3) Το WLAN UE στέλνει ένα EAP μήνυμα Response/ Identity. Το WLAN UE στέλνει το αναγνωριστικό του το οποίο συμμορφώνεται με την NAI μορφή. Το NAI περιέχει είτε ένα ψευδώνυμο το οποίο εντοπίζεται στο WLAN UE από προηγούμενη αυθεντικοποίηση ή στην περίπτωση της πρώτης αυθεντικοποίησης, περιέχει το IMSI.

4) Το μήνυμα δρομολογείται στον κατάλληλο 3GPP AAA Server που βασίζεται στο σφαιρικό τμήμα του NAI. Το σημείο της δρομολόγησης μπορεί να περιλαμβάνει έναν ή περισσότερους AAA proxies.

5) Ο 3GPP AAA Server λαμβάνει το πακέτο EAP Response/ Identity το οποίο περιλαμβάνει την ταυτότητα του συνδρομητή. Η ταυτότητα του WLAN ράδιο-δικτύου, η ταυτότητα του VPLMN και η MAC διεύθυνση του WLAN UE πρέπει επίσης να λαμβάνονται από τον 3GPP AAA Server στο ίδιο μήνυμα.

6) Ο 3GPP AAA Server αναγνωρίζει τον συνδρομητή ως υποψήφιο για αυθεντικοποίηση με το EAP-AKA, βασισμένο στη λαμβάνουσα ταυτότητα. Στη συνέχεια ο 3GPP AAA Server ελέγχει εάν υπάρχει διαθέσιμο κάποιο αχρησιμοποίητο διάνυσμα για αυτόν τον συνδρομητή. Εάν δεν υπάρχει λαμβάνει από το HSS/HLR ένα σύνολο νέων διανυσμάτων αυθεντικοποίησης. Επιπλέον ο 3GPP AAA Server ζητά διανύσματα αυθεντικοποίησης από το HSS/HLR και όταν εντοπίσει ότι το επιλεγμένο VPLMN από το χρήστη έχει αλλάξει.

Το HSS/ HLR ελέγχει εάν υπάρχει καταχωρημένος ήδη ένας 3GPP AAA Server για να εξυπηρετεί αυτόν τον συνδρομητή. Σε αυτήν την περίπτωση το HSS/ HLR πρέπει να παρέχει στον τρέχων 3GPP AAA Server την διεύθυνση του προηγούμενου καταχωρημένου 3GPP AAA Server. Τα σήματα αυθεντικοποίησης δρομολογούνται στον προηγούμενο 3GPP AAA Server μέσω συγκεκριμένων μηχανισμών.

7) Ο 3GPP AAA Server ζητάει ξανά την ταυτότητα του χρήστη χρησιμοποιώντας το μήνυμα EAP Request/ AKA Identity. Αυτό το αίτημα εκτελείται στην περίπτωση που οι ενδιάμεσοι κόμβοι μπορεί να έχουν αλλάξει ή να είχαν αντικαταστήσει την ταυτότητα των χρηστών. Εντούτοις, αυτό το νέο αίτημα της ταυτότητας χρηστών μπορεί να παραλειφθεί από τον Home Operator εάν υπάρχει η βεβαιότητα ότι την ταυτότητα των χρηστών δεν θα μπορούσε να αλλάξει ή να τροποποιηθεί με οποιαδήποτε μέσα στο μήνυμα EAP Response Identity.

8) Το WLAN AN προωθεί το EAP Request/ AKA Identity μήνυμα στο WLAN UE.

9) Το WLAN UE απαντάει με την ίδια ταυτότητα που χρησιμοποιήθηκε στο EAP Response Identity μήνυμα.

10) Το WLAN AN προωθεί το EAP Response/ AKA Identity μήνυμα στον 3GPP AAA Server. Η ταυτότητα που παραλαμβάνεται από αυτό το μήνυμα θα χρησιμοποιηθεί από τον 3GPP AAA Server για το υπόλοιπο της διαδικασίας αυθεντικοποίησης. Εάν βρεθεί μια ασυνέπεια μεταξύ των ταυτοτήτων που παραλαμβάνονται στα δύο μηνύματα (EAP Response/ Identity και EAP Response/ AKA Identity) έτσι ώστε τα διανύσματα αυθεντικοποίησης και το προφίλ του χρήστη που ανακτήθηκαν προηγουμένως από το HSS/HLR είναι άκυρα, αυτά τα στοιχεία θα ζητηθούν πάλι από το HSS/HLR.

11) Ο 3GPP AAA Server ελέγχει εάν είναι `διαθέσιμο το προφίλ του συνδρομητή για ασύρματη πρόσβαση στο WLAN. Εάν όχι το προφίλ ανακτάται από το HSS.

12) Νέο υλικό κλειδιών παραδίδεται από τα IK και CK. Αυτό το υλικό απαιτείται από το EAP-AKA για να διασφαλιστεί η ακεραιότητα και η εμπιστευτικότητα.

13) Ο 3GPP AAA Server στέλνει το RAND και το AUTN , ένα κωδικοποιημένο μήνυμα αυθεντικοποίησης (MAC) και δύο αναγνωριστικά χρήση: ένα προστατευμένο ψευδώνυμο και ένα re-authentication id στο WLAN-UE με ένα μήνυμα EPA Request-AKA Challenge. Η

αποστολή του re-authentication id εξαρτάται από τις ρυθμίσεις του Διαχειριστή του δικτύου ανάλογα με τον αν επιτρέπει fast-reauthentication ή όχι.

14) Το WLAN AN στέλνει το EAP Request-AKA Challenge μήνυμα στο WLAN UE.

15) Το WLAN UE εκτελεί έναν UMTS αλγόριθμο στην USIM. Το USIM ελέγχει ότι το AUTN είναι σωστό και με αυτό πιστοποιεί το δίκτυο. Εάν το AUTN είναι λάθος τότε το τερματικό απορρίπτει την αυθεντικοποίηση. Εάν ο αριθμός ακολουθίας είναι έξω από το synch, το τερματικό κινεί μια διαδικασία συγχρονισμού. Εάν το AUTN είναι σωστό, το USIM υπολογίζει το RES, IK και τα CK.

16) Το WLAN UE υπολογίζει μία νέα τιμή MAC που καλύπτει το EAP μήνυμα με υλικό από τα νέα κλειδιά. Στη συνέχεια στέλνει ένα EAP Response-AKA Challenge μήνυμα που περιέχει το υπολογισμένο RES και την νέα υπολογισμένη τιμή MAC στο WLAN AN.

17) Το WLAN AN στέλνει το EAP Response-AKA Challenge πακέτο στον 3GPP AAA Server.

18) Ο 3GPP AAA Server ελέγχει το λαμβανόμενο MAC και συγκρίνει το XRES με ταο λαμβανόμενο RES.

19) Εάν όλοι οι έλεγχοι του προηγούμενου βήματος είναι επιτυχείς, ο 3GPP AAA Server στέλνει το μήνυμα EAP Request-AKA Notification συνοδευόμενο από μήνυμα επιτυχίας.

20) Το WLAN AN προωθεί το μήνυμα στο WLAN UE.

21) Το WLAN UE στέλνει το μήνυμα EAP Response-AKA Notification.

22) Το WLAN AN προωθεί αυτό το μήνυμα στον 3GPP AAA Server και αυτός αγνοεί τα περιεχόμενα αυτού του μηνύματος.

23) Ο 3GPP AAA Server στέλνει το μήνυμα EAP Success στο WLAN AN.

24) Το WLAN AN ενημερώνει το WLAN UE σχετικά με την επιτυχημένη αυθεντικοποίηση με το EAP Success μήνυμα. Τώρα η ανταλλαγή EAP-AKA έχει ολοκληρωθεί επιτυχώς, και το WLAN UE και το WLAN μοιράζονται εκείνα τα κλειδιά που παρήχθησαν κατά τη διάρκεια αυτής της ανταλλαγής.

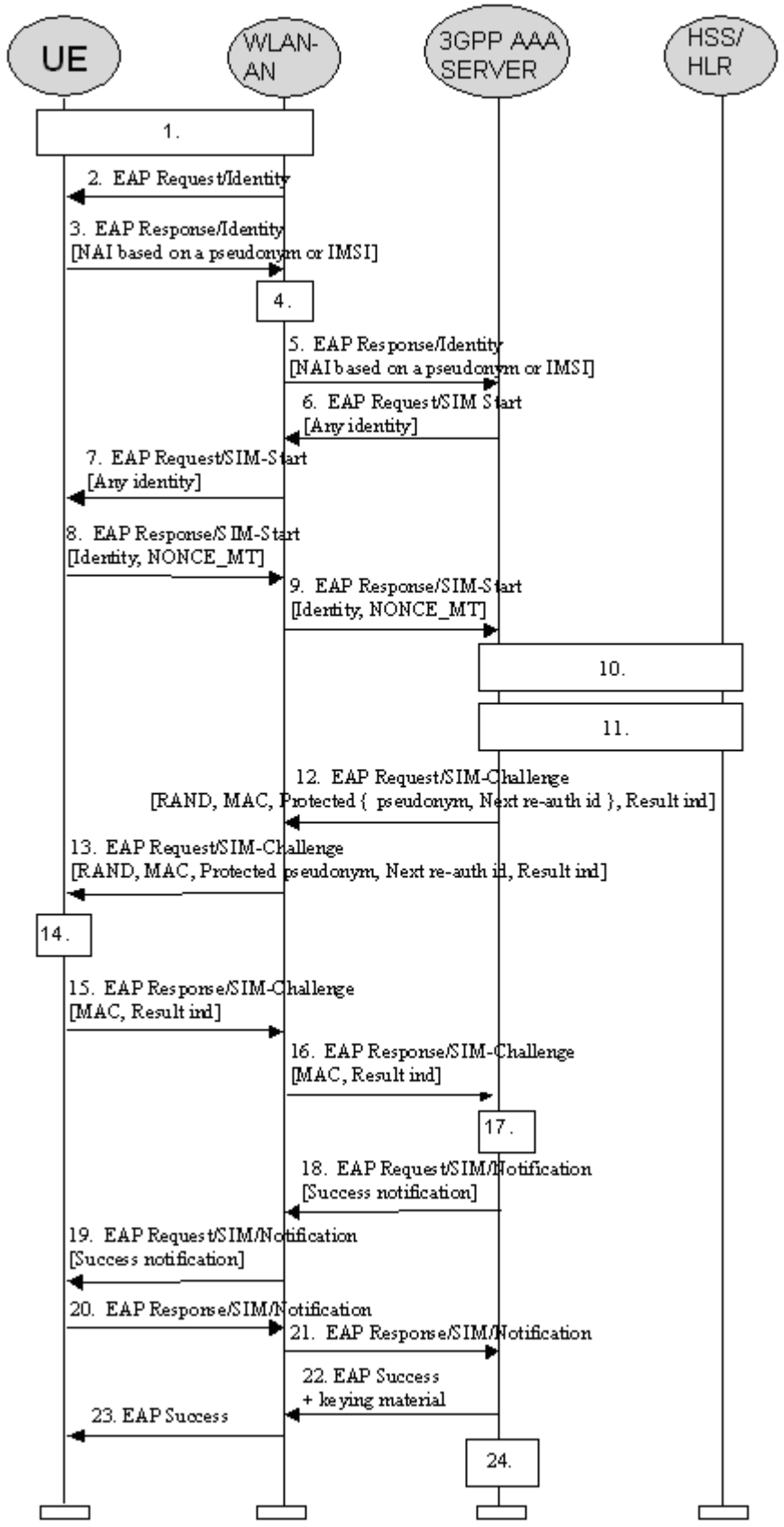
25) Εάν δεν υπάρχει καμία άλλη τρέχουσα σύνοδος WLAN πρόσβασης για το συνδρομητή που να ανιχνεύεται από το 3GPP AAA Server τότε ο 3GPP AAA Server ξεκινάει την WLAN καταχώρηση στο HSS/HLR.

5.2.2 GSM SIM-based WLAN Access Authentication

Η αυθεντικοποίηση βασισμένη στο SIM είναι χρήσιμη για GSM συνδρομητές οι οποίοι δεν έχουν UICC με USIM εφαρμογές. Η αυθεντικοποίηση βασίζεται στην διαδικασία EAP-SIM

EAP/SIM Procedure

Στην παρακάτω εικόνα(5.2) περιγράφεται πως ο EAP/SIM μηχανισμός χρησιμοποιείται στο WLAN-3GPP σενάριο διασύνδεσης.



Εικόνα 5-2 Αυθεντικοποίηση βασισμένη στο EAP-SIM σχήμα.

1) Μια σύνδεση καθιερώνεται μεταξύ του WLAN UE και του WLAN AN, χρησιμοποιώντας μια συγκεκριμένη διαδικασία τεχνολογίας ασύρματου LAN

2) Το WLAN AN στέλνει ένα EAP μήνυμα Request/ Identity στο WLAN UE.

3) Το WLAN UE στέλνει ένα EAP μήνυμα Response/ Identity. Το WLAN UE στέλνει το αναγνωριστικό του το οποίο συμμορφώνεται με την NAI μορφή. Το NAI περιέχει είτε ένα ψευδώνυμο το οποίο εντοπίζεται στο WLAN UE από προηγούμενη αυθεντικοποίηση ή στην περίπτωση της πρώτης αυθεντικοποίησης, περιέχει το IMSI.

4) Το μήνυμα δρομολογείται στον κατάλληλο 3GPP AAA Server που βασίζεται στο σφαιρικό τμήμα του NAI. Το σημείο της δρομολόγησης μπορεί να περιλαμβάνει έναν ή περισσότερους AAA proxies.

5) Ο 3GPP AAA Server λαμβάνει το πακέτο EAP Response/ Identity το οποίο περιλαμβάνει την ταυτότητα του συνδρομητή. Η ταυτότητα του WLAN ράδιο-δικτύου, η ταυτότητα του VPLMN και η MAC διεύθυνση του WLAN UE πρέπει επίσης να λαμβάνονται από τον 3GPP AAA Server στο ίδιο μήνυμα.

6) Ο 3GPP AAA Server αναγνωρίζει τον συνδρομητή ως υποψήφιο για αυθεντικοποίηση με το EAP-SIM, βασισμένο στη λαμβάνουσα ταυτότητα και στη συνέχεια στέλνει το EAP Request/SIM Start πακέτο στο WLAN AN. Ο 3GPP AAA Server ζητάει ξανα την ταυτότητα του χρήστη. Αυτό το αίτημα εκτελείται στην περίπτωση που οι ενδιάμεσοι κόμβοι μπορεί να έχουν αλλάξει ή να είχαν αντικαταστήσει την ταυτότητα των χρηστών. Εντούτοις, αυτό το νέο αίτημα της ταυτότητας χρηστών μπορεί να παραλειφθεί από τον Home Operator εάν υπάρχει η βεβαιότητα ότι την ταυτότητα των χρηστών δεν θα μπορούσε να αλλάξει ή να τροποποιηθεί με οποιαδήποτε μέσα στο μήνυμα EAP Response Identity.

7) Το WLAN AN στέλνει το EAP Request/SIM-Start πακέτο στο WLAN UE.

8) Το WLAN UE επιλέγει έναν νέο τυχαίο αριθμό NONCE_MT. Αυτός ο αριθμός χρησιμοποιείται για την αυθεντικοποίηση του δικτύου. Το WLAN UE περιλαμβάνει το ίδιο αναγνωριστικό που χρησιμοποιήθηκε στο μήνυμα EAP Response Identity. Το WLAN UE στέλνει το πακέτο EAP Response/SIM-Start, που περιέχει το NONCE_MT και το αναγνωριστικό του χρήση στο WLAN AN.

9) Το WLAN AN στέλνει το EAP Response/SIM-Start πακέτο στον 3GPP AAA Server. Το αναγνωριστικό που λαμβάνεται από αυτό το μήνυμα θα χρησιμοποιηθεί από τον 3GPP AAA Server για το υπόλοιπο της διαδικασίας αυθεντικοποίησης. Εάν διαπιστωθεί ασυμφωνία μεταξύ των ταυτοτήτων που λαμβάνονται από τα δύο μηνύματα (EAP Response Identity και EAP Response/SIM Start) έτσι ώστε όλα τα δεδομένα των χρηστών που ανακτήθηκαν προηγουμένως από το HSS/HLR να είναι λανθασμένα, αυτά τα δεδομένα θα ζητηθούν εκ νέου από το HSS/HLR.

10) Ο 3GPP AAA Server ελέγχει ότι έχει διαθέσιμα N αχρησιμοποίητα διανύσματα αυθεντικοποίησης για τον συνδρομητή. Απαιτούνται αρκετά GSM διανύσματα αυθεντικοποίησης προκειμένου να παραχθούν κλειδιά με ωφέλιμο μήκος ισοδύναμα με το EAP-AKA. Εάν δεν είναι διαθέσιμα N διανύσματα αυθεντικοποίησης ένα νέο σύνολο διανυσμάτων λαμβάνεται από το HSS/HLR. Ίσως απαιτείται αντιστοιχία μεταξύ του προσωρινού αναγνωριστικού με το IMSI. Επιπλέον ο 3GPP AAA Server θα ανακτήσει διανύσματα αυθεντικοποίησης από το HSS/HLR εάν εντοπίσει ότι το επιλεγμένο από το χρήστη VPLMN έχει μεταβληθεί.

Το HSS/ HLR ελέγχει εάν υπάρχει καταχωρημένος ήδη ένας 3GPP AAA Server για να εξυπηρετεί αυτόν τον συνδρομητή. Σε αυτήν την περίπτωση το HSS/ HLR πρέπει να παρέχει στον τρέχων 3GPP AAA Server την διεύθυνση του προηγούμενου καταχωρημένου 3GPP AAA Server. Τα σήματα αυθεντικοποίησης δρομολογούνται στον προηγούμενο 3GPP AAA Server μέσω συγκεκριμένων μηχανισμών

11) Ο 3GPP AAA Server ελέγχει ότι έχει διαθέσιμο το προφίλ για WLAN πρόσβαση του συνδρομητή. Εάν όχι, το προφίλ ανακτάται από το HSS/HLR. Ο 3GPP AAA Server πιστοποιεί ότι ο συνδρομητής είναι εξουσιοδοτημένος να χρησιμοποιήσει τις WLAN υπηρεσίες.
12) Νέο υλικό κλειδιών προέρχεται από το NONCE_MT και από τα N Kc κλειδιά. Αυτό το υλικό απαιτείται από το EAP-SIM για να διασφαλιστεί η ακεραιότητα και η εμπιστευτικότητα. Ένα νέο ψευδώνυμο και ένα re-authentication αναγνωριστικό επιλέγονται και προστατεύονται από τα κλειδιά που παρήχθησαν. Υπολογίζεται ένα Message Authentication Code (MAC), και αυτό χρησιμοποιείται ως τιμή αυθεντικοποίησης του δικτύου.

Ο 3GPP AAA Server στέλνει τα RAND, MAC, το προστατευμένο ψευδώνυμο και το re-authentication αναγνωριστικό στο WLAN AN με ένα EAP Request/SIM-Challenge μήνυμα.

13) Το WLAN AN στέλνει το EAP Request/SIM-Challenge μήνυμα στο WLAN UE.

14) Το WLAN UE τρέχει N φορές τους GSM A3/A8 αλγόριθμους στη SIM, μία φορά για κάθε RAND. Αυτός ο υπολογισμός δίνει N SRES και Kc τιμές. Το WLAN UE αντλεί επιπλέον υλικό κλειδιών από τα Nc κλειδιά και από το NONCE_MT.

15) Το WLAN UE στέλνει ένα EAP Response/SIM-Challenge που περιέχει το υπολογισμένο MAC, στο WLAN AN. Το WLAN UE θα περιλάβει σε αυτό το μήνυμα την ένδειξη αποτελέσματος εάν έλαβε την ίδια ένδειξη από το 3GPP AAA Server . Διαφορετικά, το WLAN UE θα παραλείψει αυτήν την ένδειξη.

16) Το WLAN AN στέλνει το EAP Response/SIM-Challenge πακέτο στο 3GPP AAA Server.

17) Ο 3GPP AAA Server συγκρίνει κάθε αντίγραφο από το απεσταλμένο MAC με το ληφθέν MAC.

18) Εάν η σύγκριση από το προηγούμενο βήμα είναι επιτυχείς ο 3GPP AAA Server πρέπει να στείλει το μήνυμα EAP Request/SIM/Notification πριν από το EAP Success μήνυμα.

19) Το WLAN AN προωθεί το μήνυμα στο WLAN UE.

20) Το WLAN UE στέλνει το EAP Response/SIM/Notification

21) Το WLAN AN προωθεί το EAP Response/SIM/Notification μήνυμα στο 3GPP AAA Server. Ο 3GPP AAA Server αγνοεί τα περιεχόμενα αυτού του μηνύματος.

22) Ο 3GPP AAA Server στέλνει το EAP Success μήνυμα στο WLAN AN. Εάν παραχθεί κάποιο επιπλέον υλικό κλειδιών για WLAN εμπιστευτικότητα και ακεραιότητα τότε ο 3GPP AAA Server συμπεριλαμβάνει αυτά τα κλειδιά στο AAA πρωτόκολλο.

23) Το WLAN AN πληροφορεί το WLAN UE σχετικά με την επιτυχημένη αυθεντικοποίηση με το EAP Success μήνυμα. Τώρα η EAP SIM ανταλλαγή έχει ολοκληρωθεί με επιτυχία, και το WLAN UE και το WLAN AN μπορούν να μοιραστούν το υλικό κλειδιών που παράχθηκε κατά τη διαδικασία της ανταλλαγής

24) Εάν δεν υπάρχει καμία άλλη τρέχουσα σύνοδος WLAN πρόσβασης για το συνδρομητή που να ανιχνεύεται από το 3GPP AAA Server τότε ο 3GPP AAA Server ξεκινάει την WLAN καταχώρηση στο HSS/HLR.

5.2.3 EAP support in Smart Cards

EAP-AKA Procedure

Θα πρέπει να είναι δυνατή ως εφαρμοζόμενη επιλογή, ο τερματισμός του EAP να πραγματοποιείται στο UICC. Για αυτό το λόγο όλα τα βήματα του EAP-AKA μηχανισμού

αυθεντικοποίησης όπως αυτός περιγράφτηκε προηγουμένως, ισχύουν, με εξαίρεση το βήμα 15 που αντικαθίσταται με τα εξής:

> Το WLAN-UE εκτελεί την EAP μέθοδο αυθεντικοποίησης στο UICC. Η USIMπιστοποιεί ότι το AUTN είναι σωστό και ως εκ τούτου αυθεντικοποιεί το δίκτυο. Εάν το AUTN είναι λανθασμένο, το UICC απορρίπτει την αυθεντικοποίηση. Εάν ο ακολουθιακός αριθμός είναι εκτός του synch, τότε το UICC αρχικοποιεί μία διαδικασία συγχρονισμού. Εάν ο AUTN είναι σωστός, το UICC υπολογίζει το Master Session Key και το Extended Master Session Key και ελέγχει το λαμβανόμενο MAC με το νέο παραγόμενο υλικό κλειδιών.
> Εάν ληφθεί ένα προσωρινό αναγνωριστικό (ψευδώνυμο ή/και re-authentication αναγνωριστικό) , τότε το UICC αποθηκεύει το προσωρινό αναγνωριστικό για την επόμενη πλήρη ή γρήγορη αυθεντικοποίηση. Αυτό το προσωρινό αναγνωριστικό πρέπει να διαγραφτεί μετά την επόμενη διαδικασία αυθεντικοποίησης.

EAP-SIM Procedure

Θα πρέπει να είναι δυνατή ως εφαρμοζόμενη επιλογή, ο τερματισμός του EAP να πραγματοποιείται στο UICC. Για το χειρισμό του EAP-SIM το UICC χρησιμοποιείτο GSM-AKA με την εφαρμογή των λειτουργιών μετατροπής c2 και c3. Για αυτό το λόγο όλα τα βήματα του EAP-SIM μηχανισμού αυθεντικοποίησης όπως αυτός περιγράφτηκε προηγουμένως, ισχύουν, με εξαίρεση το βήμα 14 που αντικαθίσταται με τα εξής:

> Το WLAN-UE εκτελεί την EAP μέθοδο αυθεντικοποίησης στο UICC. Το WLAN-UE συνεχίζει την διαδικασία μόνο όταν το MAC είναι σωστό.
> Εάν ληφθεί ένα προσωρινό αναγνωριστικό (ψευδώνυμο ή/και re-authentication αναγνωριστικό) , τότε το UICC αποθηκεύει το προσωρινό αναγνωριστικό για την επόμενη πλήρη ή γρήγορη αυθεντικοποίηση. Αυτό το προσωρινό αναγνωριστικό πρέπει να διαγραφτεί μετά την επόμενη διαδικασία αυθεντικοποίησης.

5.2.4 Fast re-authentication mechanisms in WLAN Access

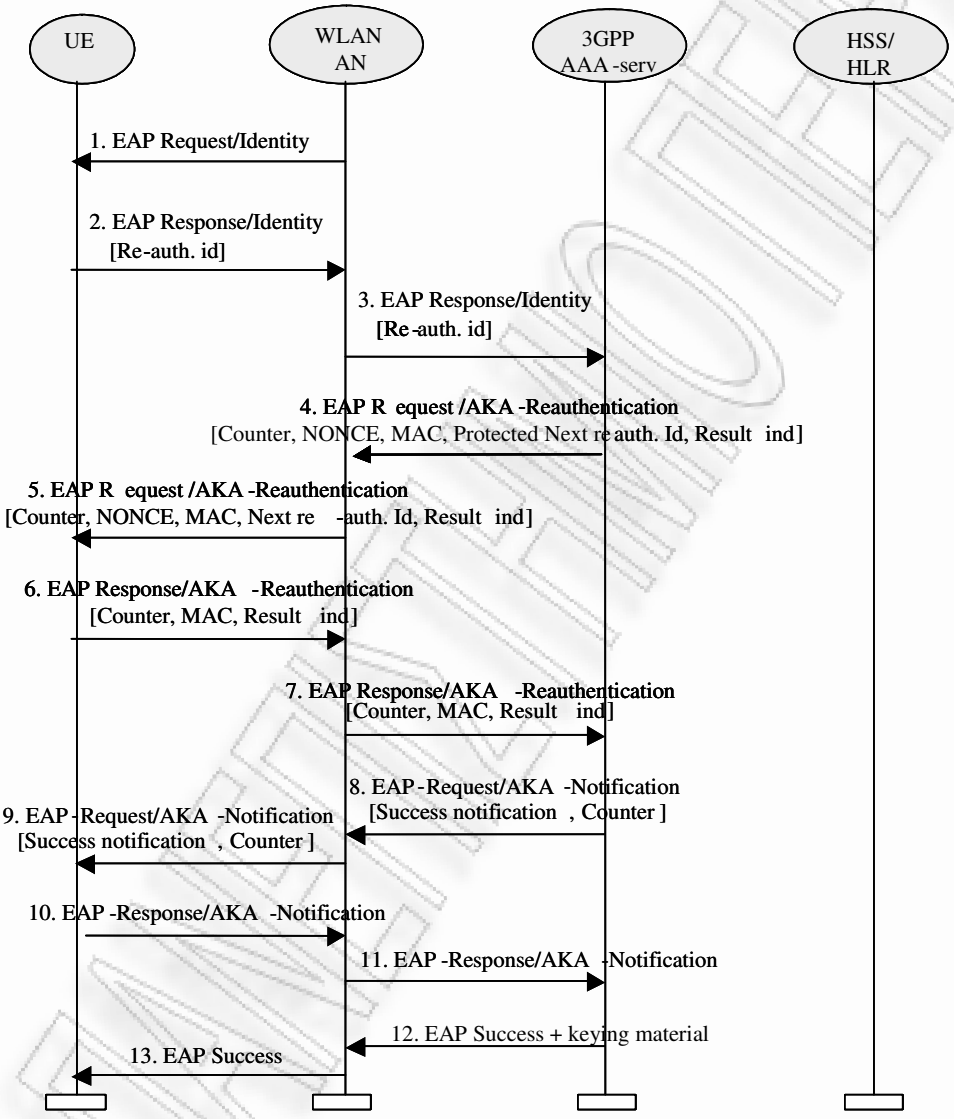
Όταν η διαδικασία αυθεντικοποίησης πρέπει να εκτελεστεί σε τακτά χρονικά διαστήματα, μπορεί να οδηγήσει σε υψηλό φόρτο δικτύου, ειδικά όταν το πλήθος των συνδεδεμένων χρηστών είναι υψηλό. Επομένως είναι περισσότερο αποδοτικό να εκτελείται η γρήγορη επαν-αυθεντικοποίηση. Έτσι η διαδικασία επαν-αυθεντικοποίησης επιτρέπει στο WLAN-AN να αυθεντικοποιεί έναν συγκεκριμένο χρήση με μία ελαφρύτερη διαδικασία από την πλήρη αυθεντικοποίηση, χάρη στην επαναχρησιμοποίηση τον παραγόμενων κλειδιών από την προηγούμενη αυθεντικοποίηση.

Η επαναχρησιμοποίηση κλειδιών από προηγούμενη αυθεντικοποίηση εκτελείται με τον ακόλουθο τρόπο: το «παλιό» master key εισάγεται μέσα σε μία ψευδο-τυχαία συνάρτηση(όπως και στην πλήρη αυθεντικοποίηση) για την παραγωγή ενός νέου Master Session Key (MSK) και ενός νέου Extended MSK. Σε αυτήν την διαδικασία παράγονται νέα Transient EAP Keys (TEKs) αλλά θα πρέπει να απορριφθούν. Τα TEKs που χρειάζονται για να προστατεύσουν τα EAP πακέτα πρέπει να είναι τα «παλιά». Έτσι τα EAP πακέτα πρέπει να προστατεύονται με τα ίδια κλειδιά με την προηγούμενη διαδικασία πλήρης αυθεντικοποίησης, αλλά το link layer key στο WLAN access network είναι ανανεωμένο μιάς και το MSK παράγεται ξανά.

Αυτή η διαδικασία υπονοεί ότι ο AAA Server μετά από μια πλήρη διαδικασία αυθεντικοποίησης όταν εκδοθεί ένα αναγνωριστικό επαν-αυθεντικοποίησης, θα αποθηκεύσει τα κλειδιά(MK, TEKs και Counter) που απαιτούνται σε περίπτωση που η επόμενη αυθεντικοποίηση είναι γρήγορη επαν- αυθεντικοποίηση. Όταν το WLAN UE ολοκληρώσει μία πλήρη αυθεντικοποίηση από την οποία παραλάβει το αναγνωριστικό της γρήγορης επαν-αυθεντικοποίησης, θα πρέπει να αποθηκεύσει τα ίδια δεδομένα με σκοπό να προετοιμαστεί για γρήγορη επαν-αυθεντικοποίηση.

EAP/AKA procedure

Η εφαρμογή του EAP/AKA πρέπει να περιλαμβάνει και τον μηχανισμό της γρήγορης επαν-αυθεντικοποίησης που περιγράφεται σε αυτήν την ενότητα, αν και η χρήση είναι προαιρετική και εξαρτάται από την πολιτική που εφαρμόζει ο κάθε διαχειριστής, και επιβάλλονται από τον AAA Server μέσο της αποστολής του αναγνωριστικού επαν-αυθεντικοποίησης σε κάθε διαδικασία αυθεντικοποίησης. Η ολοκληρωμένη διαδικασία περιγράφεται παρακάτω και εξηγεί πως αυτή λειτουργεί για την διασυνεργασία του WLAN-3GPP.



Εικόνα 5-3 EAP-AKA fast re-authentication

1. Το WLAN-AN στέλνει ένα EAP Request/Identity στο WLAN-UE.

2. Το WLAN-UE απαντάει με ένα EAP Response/Identity που περιλαμβάνει ένα re authentication identity (αυτό το αναγνωριστικό είχε ληφθεί προηγουμένως από τον AAA server κατά τη διάρκεια της πλήρης αυθεντικοποίησης).

3. Το WLAN-AN προωθεί το EAP Response/Identity στον AAA server.

4. Ο AAA server αρχικοποιεί τον Counter (όπου αρχικοποιήθηκε στην τιμή ένα στην διαδικασία της πλήρης αυθεντικοποίησης) και το στέλνει στο EAP Request message, μαζί με το NONCE, το MAC και ένα προστατευμένο re-authentication id για την επόμενη γρήγορη επαν-αυθεντικοποίηση. Εάν ο AAA server δεν είναι σε θέση να παραδώσει ένα re-authentication identity, την επόμενη φορά το WLAN-UE θα επιδιώξει την πλήρη αυθεντικοποίηση (για να αποφύγει την χρήση του re-authentication identity για παραπάνω από μία φορές).

Ο 3GPP AAA Server στέλνει επίσης ένα result indication στο WLAN-UE,με σκοπό να αναφέρει ότι επιθυμεί να προστατεύσει το success result μήνυμα στο τέλος της διαδικασίας. Η προστασία των result μηνυμάτων εξαρτάται από τις πολιτικές που εφαρμόζουν οι διαχειριστές των δικτύων..

5. Το WLAN-AN προωθεί το EAP Request μήνυμα στο WLAN-UE.

6. Το WLAN-UE πιστοποιεί ότι η τιμή του Counter είναι καινούργια και το MAC είναι σωστό, και στέλνει το EAP Response μήνυμα με την ίδια τιμή του Counter και το υπολογισμένο MAC. Το WLAN-UE πρέπει να περιλαμβάνει στο μήνυμα το result indication εάν έχει παραλάβει το ίδιο αναγνωριστικό από τον 3GPP AAA. Αλλιώς, το WLAN-UE πρέπει να παραλείψει αυτήν την ένδειξη.

7. Το WLAN-AN προωθεί την απάντηση στον AAA server.

8. Ο AAA server πιστοποιεί ότι η τιμή του Counter είναι η ίδια με αυτήν που στάλθηκε, και ότι το MAC είναι σωστό, και στέλνει το EAP Request/AKA-Notification μήνυμα, πριν από το EAP Success μήνυμα. Το EAP Request/AKA-Notification μήνυμα είναι MAC προστατευμένο, και περιλαμβάνει ένα κρυπτογραφημένο αντίγραφο του Counter που χρησιμοποιείται στην παρούσα διαδικασία επαν-αυθεντικοποίησης.

9. Το WLAN AN προωθεί το EAP Request/AKA-Notification μήνυμα στο WLAN-UE.

10. Το WLAN-UE στέλνει το EAP Response/AKA-Notification.

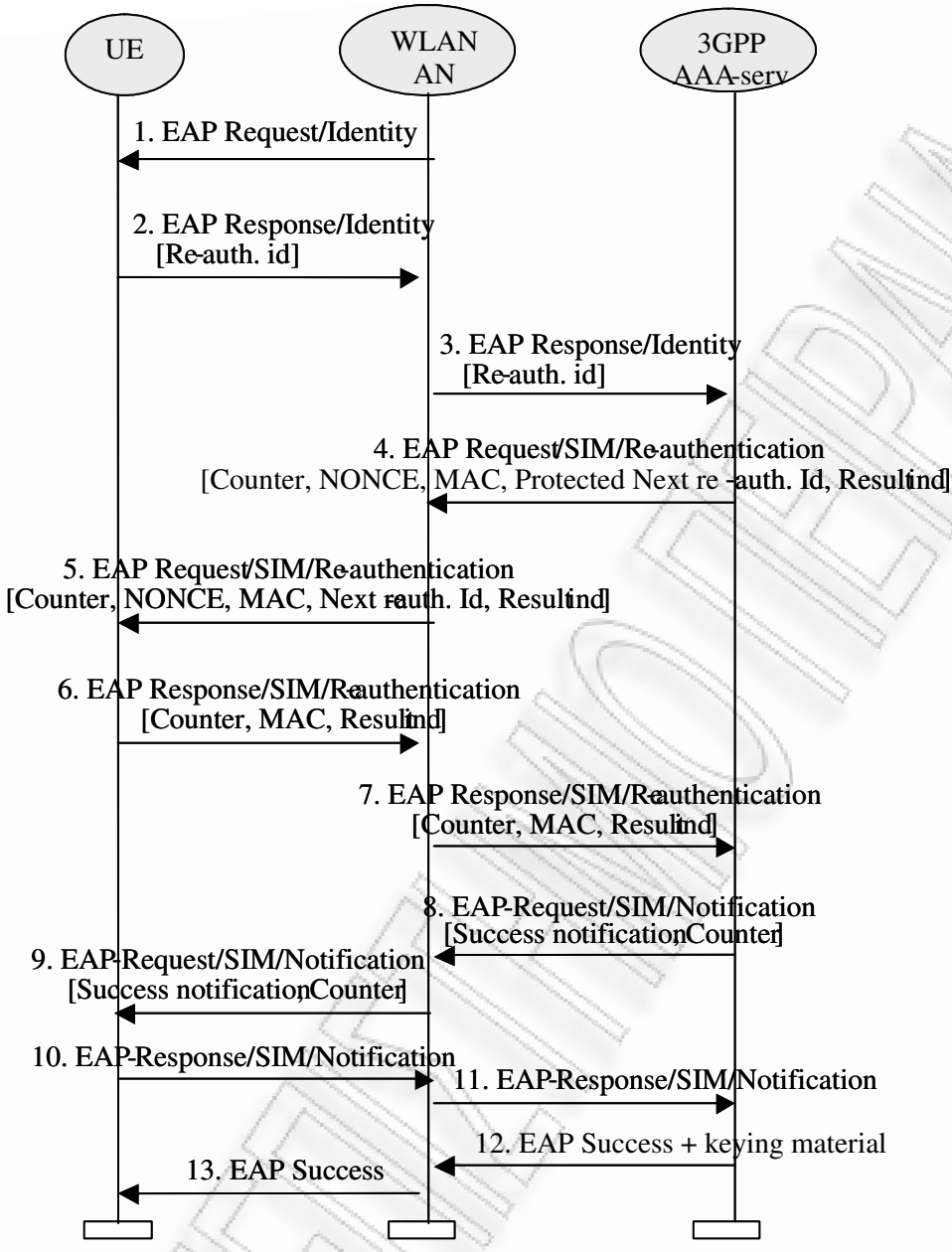
11.Το WLAN AN προωθεί το EAP Response/AKA-Notification μήνυμα στον 3GPP AAA server. Ο 3GPP AAA Server πρέπει να αγνοήσει τα περιεχόμενα του μηνύματος.

12. Ο AAA server στέλνει ένα EAP Success μήνυμα. Εάν παραχθεί κάποιο επιπλέον υλικό κλειδιών για WLAN εμπιστευτικότητα και ακεραιότητα τότε, ο 3GPP AAA Server θα περιελάμβανε αυτό το υλικό στο AAA πρωτόκολλο. Το WLAN-AN αποθηκεύει αυτό το υλικό κλειδιών για να χρησιμοποιηθεί για επικοινωνία με το αυθεντικοποιημένο WLAN-UE.

13. Το EAP Success μήνυμα προωθείται στο WLAN-UE.

EAP/SIM procedure

Η εφαρμογή του EAP/SIM πρέπει να περιλαμβάνει και τον μηχανισμό της γρήγορης επαν-αυθεντικοποίησης που περιγράφεται σε αυτήν την ενότητα, αν και η χρήση είναι προαιρετική και εξαρτάται από την πολιτική που εφαρμόζει ο κάθε διαχειριστής, και επιβάλλονται από τον AAA Server μέσο της αποστολής του αναγνωριστικού επαν-αυθεντικοποίησης σε κάθε διαδικασία αυθεντικοποίησης. Η ολοκληρωμένη διαδικασία περιγράφεται παρακάτω και εξηγεί πως αυτή λειτουργεί για την διασυνεργασία του WLAN-3GPP.



Εικόνα 5-4 EAP SIM Fast re-authentication

Η διαδικασία γρήγορης επαν-αυθεντικοποίησης είναι ίδια με την διαδικασία EAP-AKA fast re-authentication, όπως αυτή περιγράφτηκε προηγουμένως. Η μόνη διαφορά παρουσιάζεται στα βήματα 8,9,10 και 11 και αφορά τον τύπο των μηνυμάτων. Στην διαδικασία EAP-AKA έχουμε τα EAP Request/AKA-Notification και τα EAP Response /AKA-Notification μηνύματα ενώ στη διαδικασία EAP-SIM τα EAP Request/SIM-Notification και τα EAP Response /SIM-Notification.

Η διαδικασία γρήγορης επαν-αυθεντικοποίησης μπορεί να αποτύχει οποιαδήποτε στιγμή, για παράδειγμα εξαιτίας ανεπιτυχούς ελέγχου των MACs ή επειδή δεν υπάρχει απάντηση από το WLAN-UE μετά από δικτυακή αίτηση. Σε αυτήν την περίπτωση η διαδικασία EAP-AKA και EAP-SIM θα τερματίσουν και ένα αναγνωριστικό στέλνεται στο HSS/HLR.

5.2.5 Fallback to full authentication from fast re-authentication

Στην EAP SIM/AKA διαδικασία για πλήρη αυθεντικοποίηση, ο 3GPP AAA server στέλνει στο WLAN UE τα προσωρινά αναγνωριστικά ώστε να χρησιμοποιηθούν στην επόμενη διαδικασία αυθεντικοποίησης. Η επόμενη αυθεντικοποίηση μπορεί να είναι είτε μία πλήρης-αυθεντικοποίηση είτε μια διαδικασία γρήγορης επαν-αυθεντικοποίησης εξαρτάται από τον τύπο των προσωρινών αναγνωριστικών που παρελήφθησαν από το WLAN UE. Εάν το WLAN UE παραλάβει ένα fast re-authentication αναγνωριστικό, πρέπει να το χρησιμοποιήσει στην επόμενη αυθεντικοποίηση, ενημερώνοντας τον AAA server ότι πρέπει να εκτελεστεί μία γρήγορη επαν-αυθεντικοποίηση. Εάν το WLAN UE παραλάβει μόνο ένα ψευδώνυμο, το WLAN UE, πρέπει να το χρησιμοποιήσει στην επόμενη διαδικασία αυθεντικοποίησης και κατά συνέπεια πρέπει να ξεκινήσει μια πλήρης αυθεντικοποίηση.

Οποτεδήποτε παραλαμβάνεται ένα fast re-authentication αναγνωριστικό από το WLAN UE αυτό θα είναι το προσωρινό αναγνωριστικό που θα χρησιμοποιηθεί στην επόμενη διαδικασία αυθεντικοποίησης, ανεξάρτητα εάν έχει ληφθεί επίσης ένα ψευδώνυμο. Τα full authentication EAP Request/SIM Challenge and EAP Request/AKA Challenge μηνύματα επιτρέπουν την αποστολή και των δύο τύπων αναγνωριστικών. Ωστόσο, στα μηνύματα EAP Request/AKA Re-authentication και EAP Request/SIM Re-authentication είναι πιθανόν να στέλνονται μόνο re-authentication αναγνωριστικά.

Εάν το home network αποφασίσει να ξεκινήσει γρήγορες επαν-αυθεντικοποιήσεις, πρέπει να το αναφέρει στο WLAN UE, συμπεριλαμβάνοντας τα fast re-authentication αναγνωριστικά σε μία διαδικασία πλήρης αυθεντικοποίησης. Εάν αργότερα το home network αποφασίσει να εκτελέσει ξανά μία πλήρη αυθεντικοποίηση, ο the 3GPP AAA server πρέπει να το αναφέρει στο WLAN UE ζητώντας ένα ψευδώνυμο μετά την λήψη ενός fast re-authentication αναγνωριστικού. Για αυτό το λόγο ο AAA Server στέλνει ένα fast re-authentication αναγνωριστικό στο WLAN UE, περιλαμβάνοντας επίσης και ένα ψευδώνυμο, έτσι ώστε το WLAN UE να το διατηρήσει σε περίπτωση που ολισθήσει σε πλήρη αυθεντικοποίηση.

Στην περίπτωση του EAP-AKA, όταν ο AAA Server αποφασίσει να εκτελέσει πλήρη αυθεντικοποίηση ξανα, πρέπει να χρησιμοποιήσει το μήνυμα EAP Request/AKA Identity με την παράμετρο AT_FULLAUTH_ID_REQ. Το WLAN UE πρέπει στη συνέχεια να επιστρέψει ένα ψευδώνυμο.

Στην περίπτωση του EAP-SIM, όταν ο AAA Serve ραποφασίσει να εκτελέσει πλήρη αυθεντικοποίηση ξανα, πρέπει να χρησιμοποιήσει το μήνυμα EAP Request/SIM/Start με την παράμετρο AT_FULLAUTH_ID_REQ. Το WLAN UE πρέπει στη συνέχεια να επιστρέψει ένα ψευδώνυμο.

5.2 Πότε εκτελείται το AKA.

Το Authentication and Key Agreement εκτελείται όταν:
- Καταχωρείται ένας χρήστης σε ένα Serving Network.
- Μετά από αίτημα υπηρεσίας.
- Αίτηση ενημέρωσης θέσης.
- Αίτηση σύνδεσης.
- Αίτηση αποσύνδεσης.
- Αίτηση επαν-εγκαθίδρυσης της σύνδεσης.

5.3 Επαναχρησιμοποίηση των AVs .

Η επαναχρησιμοποίηση των AVs απορρίπτεται από τη USIM εξαιτίας του ελέγχου του ακολουθιακού αριθμού. Αυτό γίνεται για να αποτρέψει στο δίκτυο να εκτελέσει το Authentication and Key Agreement επαναλαμβανόμενα, χρησιμοποιώντας τα ίδια AVs.

Ωστόσο κάποιες φορές, η επαναχρησιμοποίηση των AVs είναι απαραίτητη. Όπως όταν το VLR/SGSN στέλνει ένα 'User authentication request' μήνυμα στη USIM, αλλά ποτέ δεν παίρνει απάντηση. Όταν ο χρόνος αναμονής για αυτήν την απάντηση παρέλθει, θα

προσπαθήσει να ξαναστείλει το ίδιο ζεύγος RAND||AUTN στην USIM ξανά. Εάν η USIM έχει παραλάβει το AV από την πρώτη φορά, αλλά η απάντηση δεν έφτασε ποτέ στο VLR/SGSN θα αντιληφθεί ότι ο ακολουθιακός αριθμός που παραλήφτηκε είναι εκτός ορίων. Για να αποφύγει την εκκίνηση της διαδικασίας resynchronisation σε αυτές τις περιπτώσεις, η USIM πάντα ξεκινάει συγκρίνοντας τον εισερχόμενο τυχαίο αριθμό με τον προηγούμενο που έλαβε. Εάν ταιριάζουν, θα στείλει μόνο την τελευταία αποθηκευμένη απάντηση. Για αυτό το λόγο όλες οι παράμετροι που παράγονται στην USIM πρέπει να αποθηκεύονται.

6. Περιγραφή προβλήματος – Σχολιασμός αποτελεσμάτων

6.1 Authentication Procedure and SQN Number.

Authentication Procedure

Η βασική διαδικασία αυθεντικοποίησης ανάμεσα σε ένα κινητό τερματικό και το δίκτυο παρουσιάζεται στην εικόνα 6.1. Ο μηχανισμός ασφάλειας έχει σχεδιαστεί με σκοπό να πετύχει αμοιβαία αυθεντικοποίηση ανάμεσα στον κινητό χρήστη και στο δίκτυο με τη βοήθεια του προ-διαμοιραζόμενου μυστικού κλειδιού «K» (128 bits) το οποίο μοιράζεται στην USIM και το AuC. Αυτή η διαδικασία αυθεντικοποίησης διπλής κατεύθυνσης επιτρέπει στο UMTS να αυξήσει την δικτυακή ασφάλεια σε σύγκριση με το GSM εξαλείφοντας προβλήματα λανθασμένων σταθμών βάσης.

Authentication Request

Η βασική διαδικασία αυθεντικοποίησης εκτελείται ανάμεσα στον εξοπλισμό του χρήστη (USIM, MS) και το core δίκτυο(VLS/SGSN και HLR/AuC). Οι συναλλαγές που αφορούν το χρήστη όπως η κλήση και η ενημέρωση θέσης, αρχικοποιούν την διαδικασία αυθεντικοποίησης. Ένα authentication data request στέλνεται από το VLR/SGSN στο HLR/AuC και το AuC παράγει διανύσματα αυθεντικοποίησης(AVs). Την ίδια στιγμή το AuC αυξάνει το SQN_{HE} και αποθηκεύει την τιμή στην βάση δεδομένων.

Authentication Response

Το κάθε AV αποτελείται από πέντε διανύσματα: ένα τυχαίο αριθμό (RAND) , μία αναμενόμενη απάντηση του χρήστη (XRES), ένα cipher Key (CK), ένα integrity key (IK), και ένα κουπόνι αυθεντικοποίησης για αυθεντικοποίηση δικτύου (AUTN). Μετά την λήψη αυτών των διανυσμάτων το VLR/SGSN στέλνει δύο διανύσματα (RAND και AUTN) στο κινητό τερματικό και πιστοποιεί την απάντηση του τερματικού.

Verification and Failure Report

Το κινητό τερματικό επίσης ελέγχει το MAC και το SQN με το AUTN προκειμένου να πιστοποιήσει το δίκτυο. Εάν η αυθεντικοποίηση αποτύχει στο κινητό τερματικό, ένα μήνυμα λάθους παράγεται και αποστέλλεται στο HLR/AuC. Αυτό το μήνυμα χρησιμοποιείται προκειμένου να αναλυθούν οι ψευδείς επικοινωνίες.

Re- Synchronization

Εάν το κινητό τερματικό αποτύχει να πιστοποιήσει το SQN που στάλθηκε από το HLR/AuC, μία διαδικασία Re- Synchronization αρχικοποιείται προκειμένου να ταιριάξει τον μετρητή ανάμεσα στο SQN_{HE} και SQN_{MS}. Μετά το Re- Synchronization, το HLR/AuC στέλνει ένα «Authentication Info Ack» στο VLR/SGSN με το οποίο ολοκληρώνεται η Re- Synchronization διαδικασία.

Network Authentication

Μετά τον έλεγχο του MAC και του SQN, το κινητό τερματικό υπολογίζει το RES και στέλνει το αποτέλεσμα στο VLR/SGSN, το οποίο συγκρίνει το RES με το XRES που παρέλαβε από το HLR/AuC και ολοκληρώνει την διαδικασία αυθεντικοποίησης. Εάν το RES διαφέρει από το XRES, το VLR/SGSN στέλνει ένα «authentication failure report» παρουσιάζοντας το λόγο της αποτυχίας. Εάν το RES είναι ίδιο με το XRES, το VLR/SGSN επιλέγει το CK και το IK για την εγκατάσταση της σύνδεσης. Το κινητό τερματικό υπολογίζει τα CK, IK και αποθηκεύει το SQN.

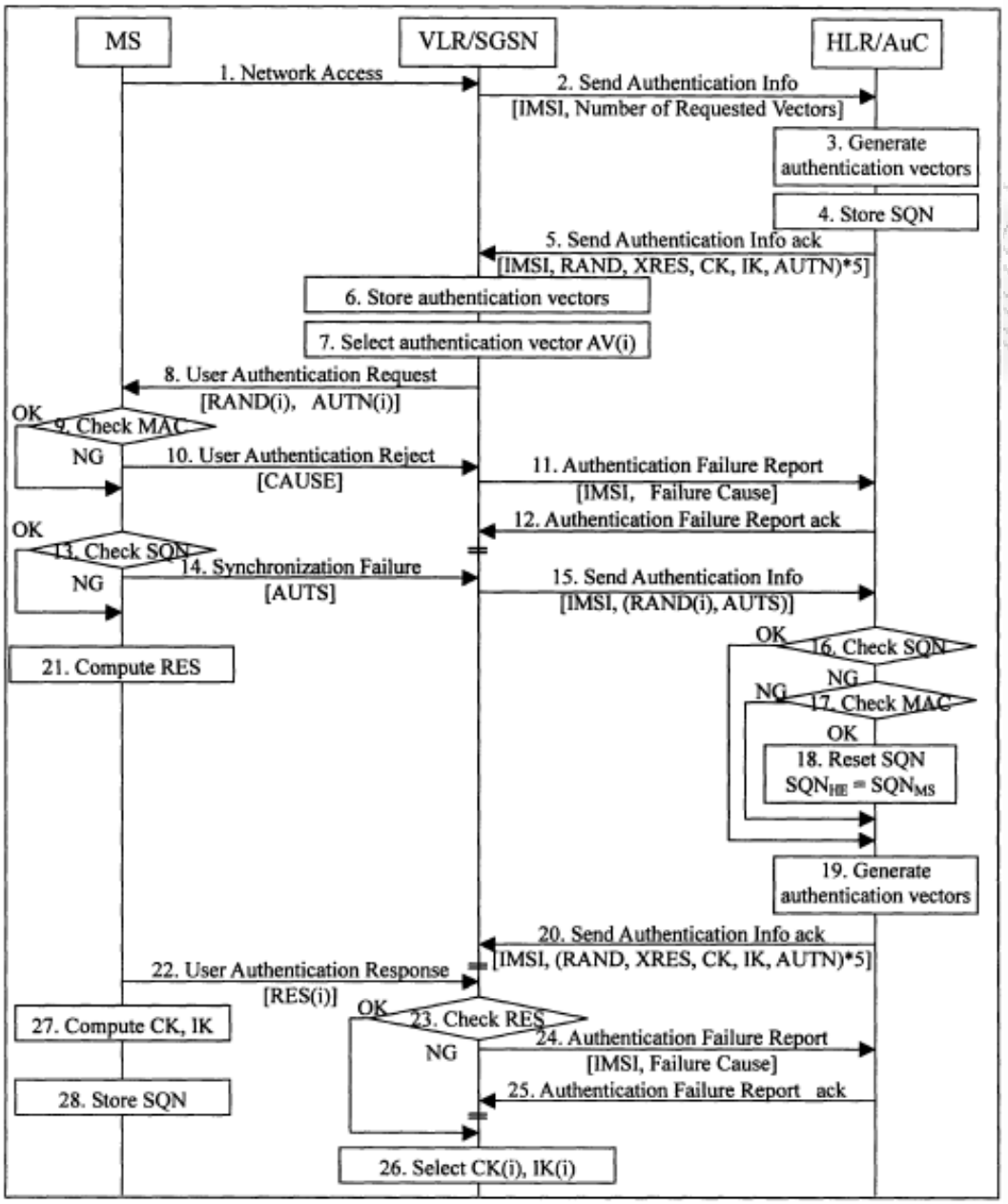
Πιστοποίηση του ακολουθιακού αριθμού (SQN) ενάντια των επιθέσεων επανάληψης.

Οι επιθέσεις επανάληψης είναι άγριες επιθέσεις στο σύστημα όπου διάφορα έγκυρα μηνύματα παρεμποδίζονται και επανεκπέμπονται αργότερα. Για να ξεπεραστεί αυτή η απειλή, οι τεχνικές προδιαγραφές του 3GPP περιγράφουν τη χρήση του ακολουθιακού αριθμού SQN. Ο SQN είναι ένας μετρητής (48bits) που διατίθεται και από την USIM και από το AuC για να διαβεβαιώσει την δικτυακή αυθεντικοποίηση. Ο ακολουθιακός αριθμός SQN_{HE} είναι ένας ανεξάρτητος μετρητής για κάθε χρήστη που αποθηκεύεται στο HLR/AuC και ο ακολουθιακός αριθμός SQN_{MS} δηλώνει τον μεγαλύτερο ακολουθιακό αριθμό όπου έχει αποδεχθεί η USIM από το δίκτυο. Κατά την διαδικασία αυθεντικοποίησης η USIM και το HLR/AuC παρακολουθούν τους μετρητές SQN_{HE} και SQN_{MS} αντίστοιχα και συγκρίνουν τα SQNs (πρέπει SQN_{HE} - SQN_{MS} <=D και SQN_{HE} > SQN_{MS}). Εάν το ληφθέν SQN είναι εκτός ορίων, η διαδικασία re- synchronization αρχικοποιείται προκείμένου να ταιριάξει τους δύο μετρητές.

Μόνο τα αληθινά USIM και HLR/AuC γνωρίζουν το σωστό SQN. Το SQN συνεχώς μεταβάλλεται με τις συναλλαγές των χρηστών και είναι σχεδόν απίθανο για εισβολείς να αντιγράψουν το SQN σε real-time συναλλαγές. Οποιαδήποτε αυθαίρετα άλματα στους ακολουθιακούς αριθμούς μπορεί να σημαίνουν ψευδή πρόσβαση.

Η διαχείριση του SQN αποτελεί πρόκληση για πολλούς παρόχους . Τόσο οι time-based όσο και οι non-time based λειτουργίες παραγωγής SQN απαιτούν πολύπλοκη ανάπτυξη λογισμικού. Το HLR/AuC πρέπει ν αποθηκεύει τα πιο πρόσφατα SQNs για κάθε συνδρομητή και να εφαρμόζουν real-time backup λειτουργίες για τους SQNs. Μία βλάβη στη βάση δεδομένων μπορεί να προκαλέσει τρομερό αριθμό εκτελέσεων της διαδικασίας Re-Synchronization, με αποτέλεσμα να οδηγήσει το δίκτυο σε βαριά συμφόρηση.

Αντίθετα, η διαδικασία Re- Synchronization πρέπει να εκτελείται κάθε φορά που η USIM εντοπίζει ότι ο ακολουθιακός αριθμός βρίσκεται εκτός ορίων. Αυτή η διαδικασία δεν θα πρέπει να λαμβάνει χώρα πολύ συχνά για λόγους απόδοσης. Η πιστοποίηση του ακολουθιακού αριθμού βοηθάει τους διαχειριστές των ασύρματων δικτύων να εντοπίζουν πιθανές απειλές κατά του συστήματος.



Εικόνα 6-1 Διαδικασία Αυθεντικοποίησης

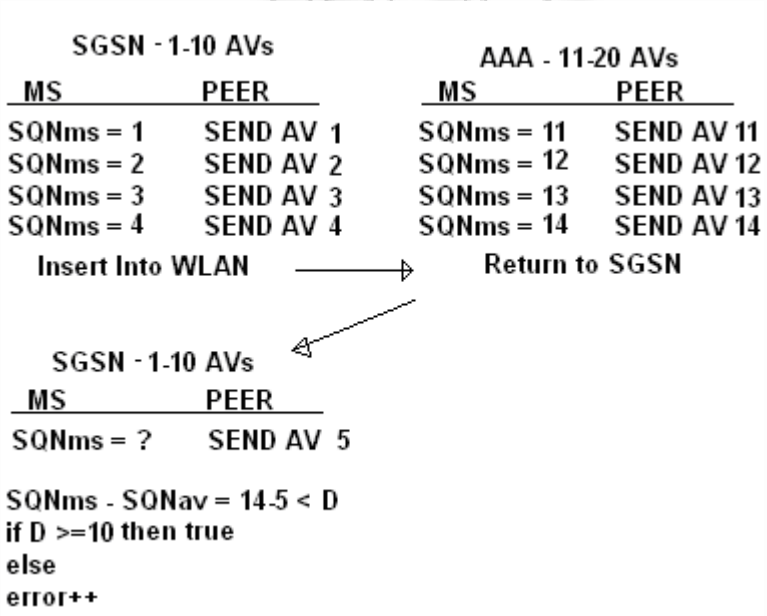
6.2 Ανάλυση Προσομοίωσης

Στην παρούσα εργασία μελετάται η κινητικότητα των χρηστών σε ένα 3G δίκτυο. Συγκεκριμένα ανάμεσα στο UTRAN κα σε ένα WLAN. Τα διάφορα γεγονότα που λαμβάνουν χώρα στο δίκτυο απεικονίζονται με μία λίστα γεγονότων και χωρίζονται σε τέσσερις κατηγορίες. Υπάρχει το SGSN event όπου κάθε φορά που εμφανίζεται στην κορυφή της λίστας υποθέτουμε ότι ο χρήστης μετακινείται στο UMTS δίκτυο, το AAA event όπου προσδιορίζει τη μετακίνηση του χρήστη στο WLAN δίκτυο, το AUTH event που εξυπηρετεί την ανάγκη αυθεντικοποίησης του χρήστη από την εκάστοτε οντότητα (AAA, SGSN) και το END_SIM event που σηματοδοτεί τον τερματισμό της προσομοίωσης. Αρχικά η λίστα γεγονότων αρχικοποιείται με τρία γεγονότα: Εισαγωγή στο UTRAN δίκτυο (SGSN), γεγονός αυθεντικοποίησης(AUTH) και τερματισμός της προσομοίωσης (END_SIM). Τα γεγονότα αυτά εκτελούνται σε τυχαίους χρόνους οι οποίοι παράγονται από μία εκθετική κατανομή με διαφορετικό λ (λάμδα) για κάθε event.

Οι τιμές των λ για την δημιουργία των χρόνων των events, των λ για την δημιουργία των χρόνων παραμονής στο κάθε δίκτυο, το πλήθος των διανυσμάτων αυθεντικοποίησης που παράγονται από το AuC καθώς και το D (επιτρεπτή τιμή διαφοράς ανάμεσα στο SQN_{HE} και το SQN_{MS}) εισάγονται παραμετρικά στην προσομοίωση από το αρχείο «input_parameters.txt».

Κάθε φορά που ο χρήστης κινείται σε διαφορετικό δίκτυο, από UTRAN σε WLAN ή από WLAN σε UTRAN, τότε απαιτείται η διαδικασία αυθεντικοποίησης. Επίσης απαιτείται κάθε φορά που στην κορυφή της λίστας υπάρχει το AUTH event. Ο κάθε Server δεσμεύει έναν συγκεκριμένο αριθμό διανυσμάτων αυθεντικοποίησης, όπως αυτός έχει οριστεί στο αρχείο παραμέτρων. Σε κάθε αυθεντικοποίηση ο SQSN ή ο AAA counter, αντίστοιχα αυξάνεται κατά ένα και ο SQN_{MS} εκχωρεί την SQN τιμή του διανύσματος που λαμβάνει από τον Server. Στην περίπτωση που το δίκτυο στείλει στο MS, SQN μικρότερο από αυτόν που έχει τότε υπάρχει κάποιο όριο ανοχής D που υποδηλώνει την διαφορά SQN_{MS} - SQN_{HE} Στην περίπτωση που η διαφορά αυτή είναι μεγαλύτερη από το D τότε αγνοείται η μικρότερη τιμή που στάλθηκε στο MS και το SQN_{MS} διατηρεί την προηγούμενη τιμή. Σε αντίθετη περίπτωση ένας μετρητής λάθους αυξάνεται κατά ένα, και παράγονται νέα διανύσματα αυθεντικοποίησης. Η επιλογή του D γίνεται συνήθως από τους διαχειριστές του δικτύου και μπορεί να διαφέρει από πάροχο σε πάροχο.

Σενάριο Εκτέλεσης



Εικόνα 6-2 Σενάριο Εκτέλεσης

Παρακάτω παρουσιάζονται ορισμένες τιμές των παραμέτρων και η Μέση τιμή λάθους όπως προκύπτει από την προσομοίωση. Οι τιμές αυτές είναι η μέγιστες που μπορούν να προκύψουν για αυτές τις παραμέτρους δεδομένου bound = 2, όπου είναι η ελάχιστη τιμή για το bound. Υπάρχει αναλογία μεταξύ bound και E[x]. Μεγάλο bound σημαίνει μικρό E[x] και αντίστροφα.

Input Parameters

**********Parameters **********
SEED / Auth In Sgsn / Auth in AA / Stay in Sgsn / Stay in AA / bound / NumVectorsSGSN1 / NumVectorsAP
****

		Errors/Num of Sims
1 1 4 6 8 2 5 5		E[x] = 0.051315
1 1 4 6 8 2 10 10		E[x] =0.053205
1 2 4 6 8 2 5 5		E[x] =0.079036
1 2 6 6 8 2 5 5		E[x] =0.084878
1 2 6 8 10 2 5 5		E[x] =0.075383
1 1 3 6 10 2 5 5		E[x] =0.046367
1 1 3 4 6 2 5 5		E[x] =0.057265
1 1 3 6 8 2 5 5		E[x] =0.049052
1 1 4 6 10 2 5 5		E[x] =0.048511

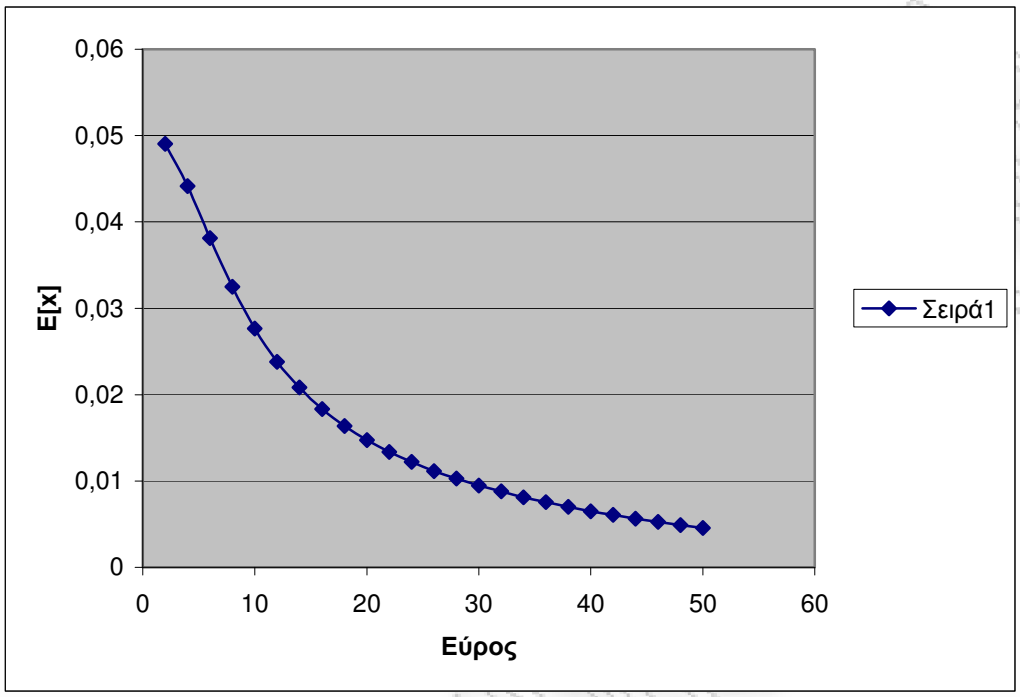
Πίνακας 6-1 Ενδεικτικές τιμές των παραμέτρων

Από τον παραπάνω πίνακα επιλέγουμε το σετ των παραμέτρων με το μικρότερο E[x] και εκτελούμε την προσομοίωση εικοσιπέντε φορές. Κάθε φορά διατηρούμε σταθερές όλες τις παραμέτρους και μεταβάλλουμε κατά +2 το bound, με αρχική τιμή το 2.

Τιμές Παραμέτρων		E[x]		Περιθώριο Λάθους
1 1 3 6 8 2 5 5		0,049052		2
2 1 3 6 8 4 5 5		0,044157		4
3 1 3 6 8 6 5 5		0,038134		6
4 1 3 6 8 8 5 5		0,032503		8
5 1 3 6 8 10 5 5		0,027656		10
6 1 3 6 8 12 5 5		0,023783		12
7 1 3 6 8 14 5 5		0,020837		14
8 1 3 6 8 16 5 5		0,018326		16
9 1 3 6 8 18 5 5		0,016369		18
10 1 3 6 8 20 5 5		0,014716		20
11 1 3 6 8 22 5 5		0,013374		22
12 1 3 6 8 24 5 5		0,0122		24
13 1 3 6 8 26 5 5		0,011145		26
14 1 3 6 8 28 5 5		0,010308		28
15 1 3 6 8 30 5 5		0,009482		30
16 1 3 6 8 32 5 5		0,008795		32
17 1 3 6 8 34 5 5		0,008124		34
18 1 3 6 8 36 5 5		0,007538		36
19 1 3 6 8 38 5 5		0,007001		38
20 1 3 6 8 40 5 5		0,006474		40
21 1 3 6 8 42 5 5		0,006055		42
22 1 3 6 8 44 5 5		0,005638		44
23 1 3 6 8 46 5 5		0,005265		46
24 1 3 6 8 48 5 5		0,004883		48
25 1 3 6 8 50 5 5		0,004567		50

Πίνακας 6-2 Αποτελέσματα προσομοίωσης.

Από τον παραπάνω πίνακα προκύπτει η εξής γραφική παράσταση:



Παρατηρούμε ότι είναι μία εκθετική κατανομή. Όσο μεγαλώνει το εύρος (bound) τόσο πιο πολύ μικραίνει εκθετικά η μέση τιμή του σφάλματος και σε πολύ μεγάλες τιμές >100 μηδενίζεται. Κάτι τέτοιο είναι αναμενόμενο μιας και πολύ μεγάλο D υποδηλώνει ότι η τιμή που στέλνει το δίκτυο στο MS μπορεί να διαφέρει αρκετά (πολύ μικρότερο) σε σχέση με την τιμή SQN_{ME}.

6.3 Discrete -event simulation

Στην προσομοίωση διακριτών γεγονότων, η λειτουργία ενός συστήματος εκφράζεται σαν μία χρονολογική σειρά γεγονότων. Κάθε γεγονός λαμβάνει χώρα σε ένα άμεσο χρονικό διάστημα και σηματοδοτεί μια αλλαγή στην κατάσταση του συστήματος. Η προσομοίωση διακριτών γεγονότων είναι μια ισχυρή υπολογιστική τεχνική για την κατανόηση της συμπεριφοράς των συστημάτων. Με τον όρο σύστημα, εννοούμε μια συλλογή από οντότητες (π.χ., άνθρωποι και μηχανές) που αλληλεπιδρούν με τον χρόνο και η σύνθεση των οντοτήτων εξαρτάται από τους στόχους της μελέτης. Η ιδιαίτερη φύση των συστημάτων και οι ιδιότητες που θέλουμε να κατανοήσουμε μπορεί να ποικίλλουν.

Σε γενικές γραμμές, για να προσδιορισθεί εάν το σύστημα πληροί μία ιδιότητα, θα πρέπει να καταλήξουμε σε ένα μαθηματικό μοντέλο του συστήματος. Στην προσομοίωση διακριτών γεγονότων, τα μοντέλα περιορίζονται στα λεγόμενα μοντέλα διακριτών γεγονότων. Εδώ, ένα σύνολο καταστάσεων χαρακτηρίζεται από το σύστημα και η εξέλιξη του συστήματος αποτυπώνεται σαν μία ακολουθία της μορφής:

$< s_0, (e_0, t_0), s_1, (e_1, t_1), s_2, \ldots >$

όπου τα si's είναι οι καταστάσεις του συστήματος, τα ei's τα γεγονότα και τα ti's θετικοί αριθμοί που αντιπροσωπεύουν τους χρόνους που παριστάνεται κάποιο γεγονός. Με τον όρο κατάσταση ορίζουμε το σύνολο των μεταβλητών που περιγράφουν το σύστημα μία στιγμή και η επιλογή τους εξαρτάται από τους στόχους της μελέτης.

Ανεπίσημα, η ανωτέρω ακολουθία σημαίνει ότι το σύστημα αρχίζει, για παράδειγμα στο χρόνο 0, στην κατάσταση s0 και το γεγονός e0 πραγματοποιείται την στιγμή t0 για να οδηγήσει το σύστημα στην κατάσταση s1 όπου το γεγονός e1 πραγματοποιείται την χρονική στιγμή t1 και ούτω καθεξής .

Λαμβάνοντας υπόψη την εξέλιξη ενός συστήματος, μπορούμε να καθορίσουμε τις ιδιότητές του και να αξιολογήσουμε τα κατάλληλα μέτρα απόδοσης. Κατά συνέπεια, ο στόχος μας είναι μια αποδοτική μέθοδος για να παραγάγει τις εξελίξεις και να αξιολογήσει τις ιδιότητες και τα μέτρα απόδοσης. Σε γενικές γραμμές, υπάρχει μια σειρά από παραμέτρους του συστήματος, που αναφέρονται ως παράμετροι εισόδου, και καθορίζουν την εξέλιξη του συστήματος και κατά συνέπεια, τις ιδιότητες και τα μέτρα επιδόσεις. Συνήθως, θέλουμε να περιγράφουμε τις παραμέτρους εισόδου ενός συστήματος, στοχαστικά αντί για ντετερμινιστικά και αυτό γιατί αντί να καθορίσουμε τις τιμές των παραμέτρων εισόδου ντετερμινιστικά, τις αφήνουμε να είναι τυχαίες μεταβλητές, που παίρνουν τις τιμές από κάποια περιοχή τιμών με κάποια κατανομή πιθανότητας. Έτσι κάθε σύνολο των παραμέτρων εισόδου οδηγεί σε μία μοναδική εξέλιξη του συστήματος. Ο στόχος είναι να ληφθούν τα μέτρα απόδοσης που υπολογίζονται από πολλές τέτοιες εξελίξεις.

Components of a Discrete-Event Simulation

Clock

Ο προσομοιωμένος χρόνος αποτελεί ένα σύνολο χρονικών στιγμών στις οποίες συμβαίνουν γεγονότα. Αποθηκεύεται σε μία σφαιρική (Global) μεταβλητή προκειμένου να είναι ορατός από όλες τις οντότητες του συστήματος και γενικά είναι διαφορετικός από το πραγματικό χρονικό διάστημα που διαρκεί η εκτέλεση της προσομοίωσης στον υπολογιστή.

Υπάρχουν δύο μηχανισμοί προώθησης του ρολογιού:
Ο μηχανισμός *σταθερής αύξησης*, όπου αυξάνει το ρολόι κατά μικρά χρονικά διαστήματα και ελέγχει αν υπάρχουν γεγονότα να συμβούν σε αυτό το διάστημα και ο *μηχανισμός επόμενου γεγονότος*, όπου αρχικοποιεί το ρολόι στην τιμή 0 και το αυξάνει κάθε φορά στη χρονική στιγμή του αμέσως επόμενου γεγονότος.

Events List

Η προσομοίωση υποστηρίζει τουλάχιστον μία λίστα γεγονότων προσομοίωσης. Αυτή η λίστα περιλαμβάνει γεγονότα τον οποίον η εκτέλεση εκκρεμεί, λόγο της εκτέλεσης κάποιου προγενέστερου γεγονότος. Ένα γεγονός περιγράφεται από τον χρόνο που πραγματοποιείται και από τον τύπο του, ό οποίος προσδιορίζει το κομμάτι του κώδικα που θα εκτελεστεί. Συνηθίζεται για το κάθε γεγονός, ο κωδικός να είναι παραμετροποιημένος, οπότε σε αυτήν την περίπτωση η περιγραφή του γεγονότος περιέχει επίσης παραμέτρους για τον κώδικα του γεγονότος.

Όταν τα γεγονότα είναι στιγμιαία, οι δραστηριότητες που επεκτείνονται με την πάροδο του χρόνου διαμορφώνονται ως ακολουθίες γεγονότων. Μερικά πλαίσια προσομοίωσης επιτρέπουν το χρόνο ενός γεγονότος να προσδιορίζεται σαν διάστημα, δίνοντας το χρόνο έναρξης και το χρόνο ολοκλήρωσης κάθε γεγονότος.

Η λίστα που περιέχει τα γεγονότα προς εκτέλεση διατηρεί μία ουρά προτεραιότητας ταξινομημένη με βάση τους χρόνους των γεγονότων. Επομένως ανεξάρτητα από την σειρά των γεγονότων που προστίθενται στη λίστα, αφαιρούνται αυστηρά με χρονολογική σειρά. Έχουν αποδειχθεί αποτελεσματικές πολλές δομές για την μοντελοποίηση τέτοιων συστημάτων με σημαντικότερες την ταξινομημένη συνδεδεμένη λίστα, πολλαπλές συνδεδεμένες λίστες, μία για κάθε χρονικό διάστημα Δt, Δέντρο με κάθε γεγονός σε διαφορετικό κόμβο.

Random-Number Generators

Η προσομοίωση πρέπει να παραγάγει τυχαίες μεταβλητές διάφορων ειδών, ανάλογα με το μοντέλο του συστήματος. Αυτό ολοκληρώνεται από μια ή περισσότερες ψευδοτυχαίες γεννήτριες αριθμών. Η χρήση των ψευδοτυχαίων αριθμών σε αντιδιαστολή με τους αληθινούς τυχαίους αριθμούς είναι ένα όφελος σε περίπτωση που χρειαστεί μια προσομοίωση μια επανάληψη με ακριβώς την ίδια συμπεριφορά.

Ένα από τα προβλήματα με τις κατανομές τυχαίων αριθμών που χρησιμοποιούνται στην προσομοίωση διακριτών γεγονότων είναι ότι οι κατανομές σταθερής κατάσταση των χρόνων των γεγονότων δεν μπορεί να είναι γνωστές εκ των προτέρων. Με αποτέλεσμα, το αρχικό σύνολο των γεγονότων που τοποθετείται στην λίστα γεγονότων δεν θα έχει χρόνους άφιξης που αντιπροσωπεύουν την κατανομή σταθερής κατάστασης. Αυτό το πρόβλημα επιλύεται με την έναρξη του μοντέλου της προσομοίωσης. Μόνο ένας περιορισμένος αριθμός προσπαθειών καταβάλλεται για να οριστούν ρεαλιστικές τιμές στο αρχικό σύνολο γεγονότων. Αυτά τα γεγονότα, ωστόσο , προγραμματίζουν επιπρόσθετα γεγονότα και με το πέρασμα του χρόνου η κατανομή των χρόνων των γεγονότων προσεγγίζει την κατάσταση ισορροπίας.

Πως δημιουργούμε όμως μια τυχαία μεταβλητή με συγκεκριμένη εκθετική κατανομή;
Έστω U τυχαία μεταβλητή ομοιόμορφα κατανεμημένη στο διάστημα [0,1]

$$f(u) = \begin{cases} 1, \text{αν } 0 \le u \le 1 \\ 0, \text{αλλιώς} \end{cases}$$

Τότε, η τυχαία μεταβλητή X=-β lnUείναι εκθετικά κατανεμημένη

$$\begin{aligned} F(x) &= P(X \le x) \\ &= P(-\beta \ln U \le x) \\ &= P(\ln U \ge -\frac{x}{\beta}) \\ &= P(e^{-x/\beta} \le U \le 1) \\ &= 1 - e^{-x/\beta} \end{aligned}$$

Statistics – Performance Indicators.

Η προσομοίωση παρακολουθεί τα χαρακτηριστικά των στατιστικών του συστήματος, οι οποίες εκφράζουν ποσοτικά διάφορα θέματα που μας ενδιαφέρουν για το σύστημα, όπως το

E[x] = #Errors/ #Runs , δηλαδή ο μέσος αριθμός σφαλμάτων που προκύπτει από τον αριθμό των λαθών όπως αυτός υπολογίζεται κατά την εκτέλεση όλων των εκτελέσεων του κώδικα, προς τον αριθμό αυτών των εκτελέσεων.

Ending Condition

Κατά τη διάρκεια εκτέλεσης της προσομοίωσης ο κώδικας παράγει συνεχώς νέα γεγονότα επομένως θεωρητικά μία προσομοίωση διακριτών γεγονότων θα εκτελείται για πάντα. Επομένως ο σχεδιαστής μιας προσομοίωσης πρέπει να αποφασίζει το πότε αυτή η προσομοίωση θα ολοκληρωθεί. Συνηθισμένες επιλογές είναι «μετα από χρόνο t» η «μετα την εκτέλεση n γεγονότων» ή πιο γενικά «όταν η στατιστική ποσότητα x αγγίξει την τιμή y».

Αλγόριθμος εκτέλεσης μίας προσομοίωσης διακριτών γεγονότων

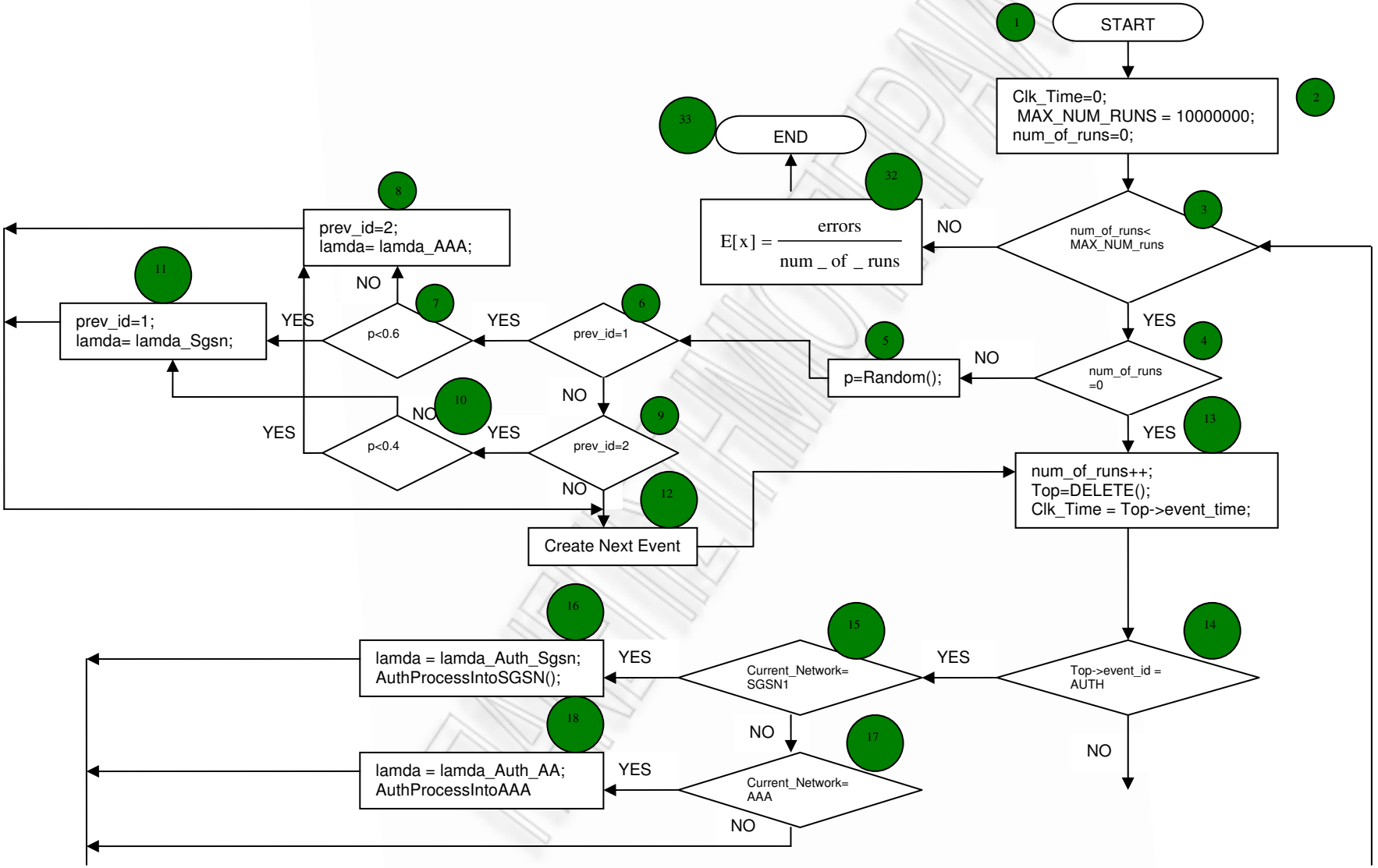
Ο βασικός βρόγχος της προσομοίωσης διακριτών γεγονότων ακολουθεί την παρακάτω μορφή:

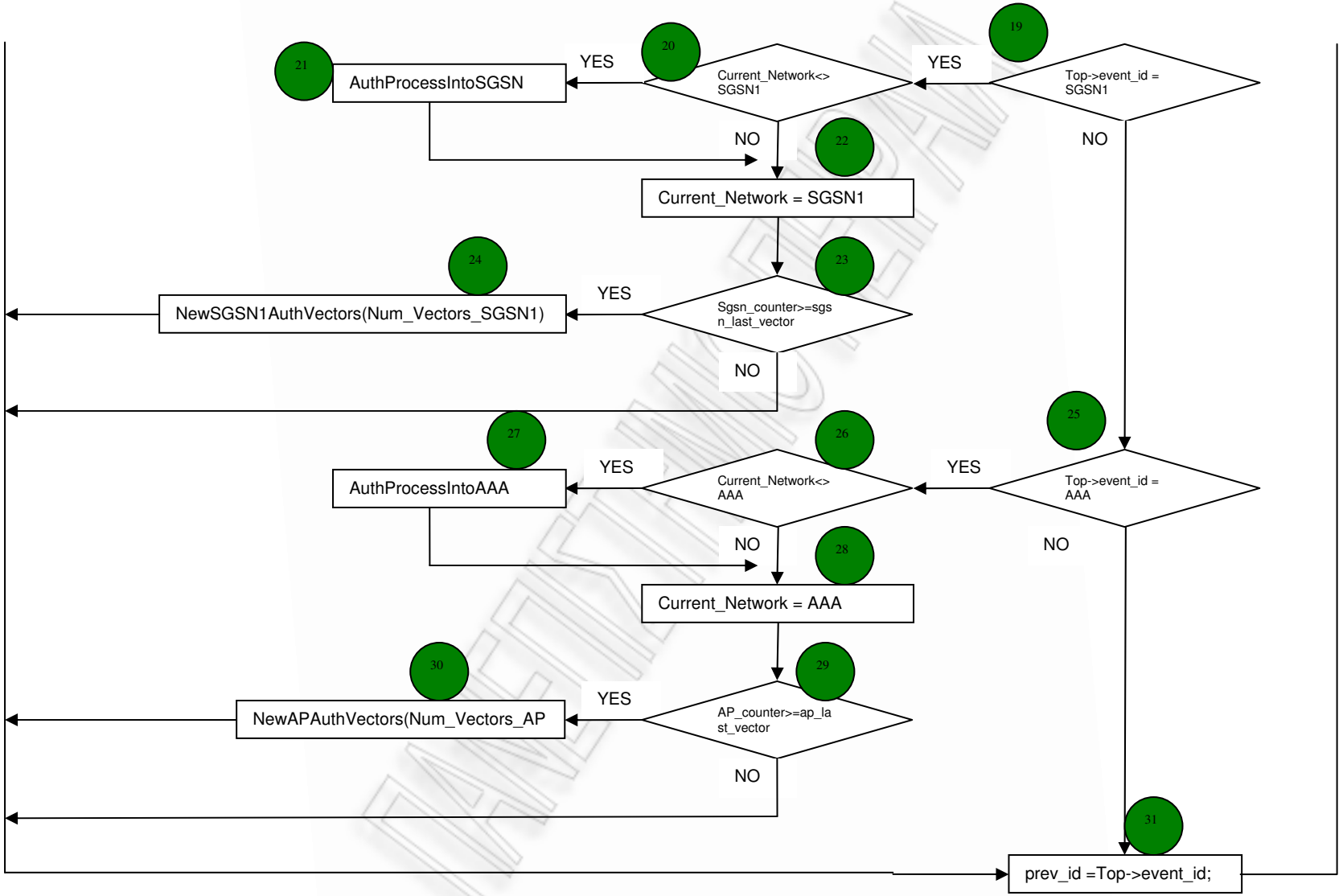
Έναρξη
- Αρχικοποίηση συνθήκης τερματισμού σε FALSE.
- Αρχικοποίηση των μεταβλητών του συστήματος.
- Αρχικοποίηση ρολογιού (Συνήθως αρχικοποιείται σε μηδέν).
- Προγραμματισμός των αρχικών γεγονότων (π.χ. εισαγωγή αρχικών γεγονότων στη λίστα).

Εκτέλεση βρόγχου
While (Ending Condition is FALSE) then do the following:
- Εκχώρηση του ρολογιού στον χρόνου του επόμενου γεγονότος..
- Εκτέλεσε το επόμενο γεγονός και διέγραψε το από την λίστα.
- Ενημέρωσε τους στατιστικούς δείκτες..

Τέλος
- Παραγωγή της έκθεσης στατιστικών και των μέτρων επίδοσης.

6.4 Διάγραμμα ροής προσομοίωσης


1
START
2
Clk_Time=0;
MAX_NUM_RUNS = 10000000;
num_of_runs=0;
3
num_of_runs< MAX_NUM_RUNS
YES
NO
4
num_of_runs =0
YES
NO
5
p=Random();
6
prev_id=1
YES
NO
7
p<0.6
YES
NO
8
prev_id=2;
lamda= lamda_AAA;
9
prev_id=2
YES
NO
10
p<0.4
YES
NO
11
prev_id=1;
lamda= lamda_Sgsn;
12
Create Next Event
13
num_of_runs++;
Top=DELETE();
Clk_Time = Top->event_time;
14
Top->event_id = AUTH
YES
NO
15
Current_Network= SGSN1
YES
NO
16
lamda = lamda_Auth_Sgsn;
AuthProcessIntoSGSN();
YES
17
Current_Network= AAA
YES
NO
18
lamda = lamda_Auth_AA;
AuthProcessIntoAAA
YES
32
E[x] = errors / num _ of _ runs
NO
33
END



Εικόνα 6-3 Διάγραμμα ροής προσομοίωσης.

Το διάγραμμα ροής της προσομοίωσης εμφανίζεται στην εικόνα 6.3 και τα βήματα της προσομοίωσης αναλύονται παρακάτω:

Βήμα 1: Έναρξη προσομοίωσης.
Βήμα 2 : Αρχικοποίηση μεταβλητών, ρολογιού προσομοίωσης και λίστας γεγονότων.
Βήμα 3 : Έλεγχος εάν η μεταβλητή num_of_runs είναι μικρότερη από max_num_runs.
Βήμα 4 : Εάν ναι, ελέγχουμε εάν το num_of_runs ισούται με μηδέν. Εάν δηλαδή είμαστε στην πρώτη επανάληψη.
Βήμα 5 : Εάν όχι υπολογίζουμε την πιθανότητα p.
Βήμα 6,7,8: Εάν το τελευταίο event της λίστας ήταν τύπου 1, τότε ελέγχουμε την τιμή της πιθανότητας p. Εάν είναι μικρότερη του 0.6 τότε ενημερώνουμε τις παρακάτω μεταβλητές
prev_id=1;
lamda= lamda_Sgsn;
αλλιώς
prev_id=2;
lamda= lamda_AAA;
που σημαίνει ότι το επόμενο event θα είναι ίδιο τύπου με το τελευταίο event που διαγράφτηκε από τη λίστα με πιθανότητα 0.6. Αλλιώς με πιθανότητα 0.4 δημιουργούμε event με διαφορετικό τύπο.
Βήμα 9,10,11: Εάν το τελευταίο event της λίστας ήταν τύπου 2, τότε ελέγχουμε την τιμή της πιθανότητας p. Εάν είναι μικρότερη του 0.4 τότε ενημερώνουμε τις παρακάτω μεταβλητές
prev_id=2;
lamda= lamda_AAA;
αλλιώς
prev_id=1;
lamda= lamda_Sgsn;
που σημαίνει ότι το επόμενο event θα είναι ίδιο τύπου με το τελευταίο event που διαγράφτηκε από τη λίστα με πιθανότητα 0.4. Αλλιώς με πιθανότητα 0.6 δημιουργούμε event με διαφορετικό τύπο.
Βήμα 12: Δημιουργούμε ένα νέο event με id και lamda όπως αυτά ενημερώθηκαν παραπάνω.
Βήμα 13: Αυξάνεται ο μετρητής των εκτελέσεων της προσομοίωσης, και διαγράφεται το κορυφαίο event από τη λίστα. Το ρολόι της προσομοίωσης ενημερώνεται με τον χρόνο του γεγονότος που μόλις διαγράφτηκε.
Βήμα 14-18: Ελέγχουμε τον τύπο του event που διαγράφτηκε. Εάν είναι τύπος AUTH τότε ελέγχουμε σε ποιό δίκτυο ανήκει ο χρήστης και επομένως σε ποιο δίκτυο θα πραγματοποιηθεί η νέα αυθεντικοποίηση. Εάν ανήκει στο δίκτυο με τύπο SGSN1 τότε καλείται η διαδικασία αυθεντικοποίησης AuthProcessIntoSGSN(), αλλίως αν ανήκει στο δίκτυο με τύπο AAA τότε καλείται η διαδικασία αυθεντικοποίησης AuthProcessIntoAAA(), ενημερώνοντας κάθε φορά τις απαραίτητες μεταβλητές.
Βήμα 19-22: Ελέγχουμε τον τύπο του event που διαγράφτηκε. Εάν είναι τύπος SGSN1 ελέγχουμε το δίκτυο που στο οποίο ανήκει ο χρήσης. Εάν είναι το ίδιο με το δίκτυο που το event ορίζει απλά ενημερώνουμε την μεταβλητή Current_Network = SGSN1 εννοώντας πως ο χρήστης παρέμεινε στο ίδιο δίκτυο, αλλιώς σημαίνει ότι ο χρήστης εισήλθε σε διαφορετικό δίκτυο επομένως επιβάλλεται η διαδικασία αυθεντικοποίησης. Επομένως καλείται ο συνάρτηση AuthProcessIntoSGSN(),
Βήμα 23,24: Εάν ο μετρητής των AVs είναι μεγαλύτερος από τον μέγιστο που έχει οριστεί για το τρέχων δίκτυο τότε το δίκτυο ζητάει νέα AV ενημερώνοντας κατάλληλα τους μετρητές του συστήματος με την συνάρτηση NewSGSN1AuthVectors.
Βήμα 25-30: Ακολουθείται ακριβώς η ίδια διαδικασία με τα βήματα 19-24, αλλά θεωρούμε σαν τρέχων δίκτυο το WLAN.
Βήμα 31: Αποθηκεύουμε στην μεταβλητή prev_id το event_id του event που διαγράψαμε από τη λίστα προκειμένου να τοποθετηθεί ξανά μέσα στη λίστα με νέο χρόνο μεγαλύτερο από το χρόνο του ρολογιού της προσομοίωσης.
Βήμα 32: Όταν η μεταβλητή num_of_runs φτάσει την τιμή max_num_runs τότε σηματοδοτείται ο τερματισμός της προσομοίωσης και υπολογίζεται η στατιστική μεταβλητή E[x] η οποία προκύπτει από το πλήθος των λαθών προς τον συνολικό αριθμό εκτέλεσης της προσομοίωσης.
Βήμα 33: Τερματισμός προσομοίωσης αποτύπωση στατιστικών μεταβλητών.

Συμπεράσματα - Ανακεφαλαίωση

Από τα παραπάνω συμπεραίνουμε πως οι ανάγκες των χρηστών για ταχύτερες επικοινωνίες, περισσότερες υπηρεσίες που θα καλύπτουν τις απαιτήσεις τους και η ανάγκη για αυξημένη κινητικότητα των χρηστών ανάμεσα σε ετερογενή δίκτυα, οδηγεί σε μία ραγδαία τεχνολογική εξέλιξη των υπαρχόντων δικτύων. Ήδη για αυτό το λόγο, τα ασύρματα δίκτυα υπερτερούν έναντι των παραδοσιακών ενσύρματων, και στο μέλλον αναμένεται εάν όχι η ολική αντικατάσταση τους, τουλάχιστον το μεγαλύτερο μέρος τους.

Ένα από τα σημαντικότερα μειονεκτήματα των ασύρματων επικοινωνιών είναι ότι γίνονται εύκολος στόχος από ανεπιθύμητους εισβολείς και για αυτό το λόγο πρωταρχικό ρόλο στην ανάπτυξη και εξέλιξη των ασύρματων δικτύων αποτελεί η ανάπτυξη ενός συστήματος ασφαλείας ικανό να αποτρέψει την πρόσβαση σε κακόβουλους χρήστες. Η διαδικασία αυθεντικοποίησης EAP-AKA (ή EAP-SIM για το GSM) αποτελεί ένα πάρα πολύ καλό εργαλείο αυθεντικοποίησης χρηστών στο δίκτυο, αλλά και του δικτύου στους χρήστες. Αυτή η αμοιβαία αυθεντικοποίηση εξασφαλίζει στο χρήστη ότι θα είναι προσβάσιμες οι υπηρεσίες που του αναλογούν και ότι το δίκτυο παρέχει εκείνες τις υπηρεσίες για τις οποίες ο χρήστης χρεώνεται.
Παρόλα αυτά η διαδικασία αυθεντικοποίησης είναι μια χρονοβόρα διαδικασία και για λόγους απόδοσης είναι προτιμότερο να παραλείπεται σε περιπτώσεις όπου αυτό είναι εφικτό.

Για αυτό το λόγο η χρήση των ακολουθιακών αριθμών SQN_{MS} και SQN_{HE} αποτρέπει την εφαρμογή της διαδικασίας της πλήρης αυθεντικοποίησης κάθε φορά που το δίκτυο το απαιτεί. Είδαμε όμως ότι η συχνότητα κατά την οποία εφαρμόζεται αυτή η διαδικασία εξαρτάται κατά μεγάλο βαθμό από το διάστημα(bound) D το οποίο εκφράζει το εύρος της διαφοράς που επιτρέπεται να έχουν αυτοί οι δύο ακολουθιακοί αριθμοί. Εάν η διαφορά τους είναι μεγαλύτερη από το διάστημα D τότε η διαδικασία Re- Synchronization εκτελείται προκειμένου να επαναφέρει τις αποδεκτές τιμές στο σύστημα. Στην περίπτωση που η διαφορά είναι μικρότερη, τότε δεν απαιτείται επαν-αυθεντικοποίηση του χρήστη στο δίκτυο και επομένως χρησιμοποιούνται τα κλειδιά που εφαρμόστηκαν στην τελευταία σωστή αυθεντικοποίηση.

Οι χρήστες με αυξημένοι κινητικότητα είναι πιο πιθανό να προκαλούν το «λάθος» που περιγράφτηκε παραπάνω. Μία αρκετά μεγάλη τιμή στη μεταβλητή D προφανώς θα απέτρεπε αυτή την κατάσταση λάθους, αλλά ταυτόχρονα θα αναιρούσε και την ύπαρξη της μεταβλητής D σαν εργαλείο προστασίας από επιθέσεις επανάληψης. Επομένως ένα πιο αποδοτικό δίκτυο ίσως οδηγούσε τελικά σε ένα πιο ευάλωτο δίκτυο. Αντιθέτως μία πολύ μικρή τιμή της ποσότητας D θα παρείχε μεγαλύτερη ασφάλεια στο δίκτυο αλλά θα έχανε την αποδοτικότητα του μίας και η διαδικασία Re-Synchronization θα εφαρμοζόταν πολύ συχνότερα. Ποιά είναι λοιπόν η καταλληλότερη τιμή της μεταβλητής D; Ο κάθε πάροχος ορίζει και μία διαφορετική τιμή με αποτέλεσμα να κρίνει ο καθένας διαφορετικά την σωστή τιμή για το δικό του δίκτυο.

Μία λύση θα ήταν να ενημερώνεται δυναμικά για κάθε χρήστη η τιμή D. Δηλαδή το δίκτυο να συλλέγει πληροφορίες σχετικά με την κινητικότητα του κάθε χρήστη, τις υπηρεσίες που χρησιμοποιεί, την συχνότητα των κλήσεων που λαμβάνει και πραγματοποιεί και γενικότερα πληροφορίες σχετικά με την συχνότητα που εκτελούνται διαδικασίες αυθεντικοποίησης στο δίκτυο εξαιτίας του. Έτσι το δίκτυο θα γνώριζε το προφίλ του κάθε χρήστη και η τιμή της μεταβλητής D θα μπορούσε να αυξηθεί ή να μειωθεί ανάλογα με την ημέρα, ώρα ή και το χρονικό διάστημα που ο κάθε χρήστης χρησιμοποιεί το δίκτυο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Prasad, R., M. Ruggieri, “Special Issue on the Future Strategy for the New Millenium Wireless World,” Wireless Personal Communications, Vol. 17, Nos. 2–3, June 2001.

[2] van Nobelen, R., et al., “An Adaptive Radio Link Protocol with Enhanced Data Rates for GSM Evolution,” IEEE Personal Communications, Vol. 6, No. 1, Feb. 1999, pp. 54–64.

[3] Prasad, R., W. Mohr, and W. Konhauser, Third-Generation Mobile Communication System, Norwood, MA: Artech House, 2000.

[4] IEEE 802.11, IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Nov. 1997.

[5] Crow, B. P., et al., “IEEE 802.11 Wireless Local Area Network,” IEEE Communications Magazine, Sept. 1997, pp. 116–126.

[6] Prasad, R., Wideband CDMA for Third-Generation Mobile Systems, Norwood, MA: Artech House, 1998.

[7] Cai, J., and D. J. Goodman, “General Packet Radio Service in GSM,” IEEE Communications Magazine, Oct. 1997.

[8] Ramjee Prasad and Marina Ruggieri .Technology Trends in Wireless Communications

[9] ETSI SAGE Task force for 3GPP, General report on the Design, Specification and Evaluation of The MILENAGE Algorithm Set: An Example Algorithm Set for the 3GPP Authentication and Key Generating Functions, Version 1.0, Internal document

[10] 3GPP, A Guide to 3rd Generation Security, 3G TR 33.900, v1.2.0 (2000-1)

[11] 3GPP system to Wireless Local Area Network (WLAN) interworking;
System description (Release 7).3GPP TS 23.234 V7.3.0 (2006-09) ,

[12] 3G Security; Wireless Local Area Network (WLAN) interworking security
(Release 7) 3GPP TS 33.234 V7.2.0 (2006-09).

[13] 3G and WLAN Interworking Security: Current Status and Key Issues. Chou-Chen Yang Kuan-Hao Chu, and Ya-Wen Yang.

[14] Security architectures for B3G mobile networks Christos Xenakis · Christoforos Ntantogian

[15] Security in third Generation Mobile Networks Christos Xenakis*, Lazaros Merakos

[16] Interworking between WLAN and 3G Cellular Networks: An IMS Based
Architecture Kumudu S. Munasinghe, Abbas Jamalipour and Branka Vucetic