

UMTS NETWORK

Η ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ
ΔΙΚΤΥΟΥ ΚΙΝΗΤΗΣ
ΤΗΛΕΦΩΝΙΑΣ UMTS



ΓΕΩΡΓΙΟΥ ΣΠΥΡΙΔΟΥΛΑ

ΚΟΥΜΟΥΝΔΟΥΡΟΥ ΑΛΚΗΣΗ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ



ΤΕΙ ΗΠΕΙΡΟΥ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ &
ΔΙΟΙΚΗΣΗΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ



ΔΙΚΤΥΟ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ ΤΡΙΤΗΣ ΓΕΝΝΙΑΣ

UMTS

Η ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΚΑΙ ΟΙ ΥΠΗΡΕΣΙΕΣ ΤΟΥ

Κουμουνδούρου Αλκηστη (Α.Μ. 456)

Γεωργίου Σπυριδούλα (Α.Μ. 347)

ΥΠΕΥΘΥΝΟΣ ΚΑΘΗΓΗΤΗΣ:

Στεργίου Ελευθέριος



-ΑΡΤΑ 2004-

Κεφάλαιο 1 Εισαγωγή

1.1 Υπάρχοντα Συστήματα Κινητών Τηλεπικοινωνιών.....	6
1.1.1 Ανάπτυξη 3 ^{ης} Γενιάς Συστημάτων Κινητών Τηλεπικοινωνιών.....	8
1.1.2 Προλειτουργικές φάσεις του UMTS: GPRS / EDGE.....	10
1.1.3 Πολλαπλές Τεχνικές Πολλαπλής Πρόσβασης Διαίρεσης. Κώδικα (CDMA) – Στάδια Τυποποίησης.....	10
1.2 Επίδραση των χαρακτηριστικών του συστήματος UMTS στη διαχείριση πόρων ραδιοδικτύου (RRM).....	12
1.2.1 Μεγάλο εύρος ζώνης.....	12
1.2.2 Πολλαπλές Προδιαγραφές QoS.....	12
1.2.3 Ασύμμετρη Κυκλοφορία.....	13

Κεφάλαιο 2 Η Εξέλιξη από το GSM στο UMTS

2.1 Τύποι Εξέλιξης.....	14
-------------------------	----

Κεφάλαιο 3 Βασικές πληροφορίες για το UMTS RADIO COMMUNICATION

3.1 Η επικοινωνία βασικών αρχών ραδιοεπικοινωνίας.....	19
3.2 Η κυψελοειδής αρχή ραδιοεπικοινωνιών.....	22
3.3 Πολλαπλάσιες τεχνικές πρόσβασης.....	27
3.4 Χαρακτηριστικά του ραδιομονοπατιού της 3ης Γενιάς.....	30
Οι βασικές έννοιες.....	32
3.4.1 Κανάλια WCDMA.....	35
3.4.2 Η Δομή των πλαισίων WCDMA.....	45

Κεφάλαιο 4 UMTS RADIO ACCESS NETWORK(UTRAN)

Εισαγωγή.....	46
4.1. Η Αρχιτεκτονική του UTRAN.....	47
4.2 Ο σταθμός βάσης.....	47
4.2.1 Εσωτερική δομή των Σταθμών Βάσεων (BS).....	48
4.2.2 Η μέθοδος διαμόρφωσης.....	49
4.2.3. Η Τεχνική του αποδέκτη.....	51
4.2.4 Δυναμικότητα κυψέλης.....	52
4.3 Ο ελεγκτής των ραδιο δικτύων.....	54
4.3.1 Η παράδοση ελέγχου (handover control).....	55
Λόγοι πίσω από το handover	56



Διαδικασία του Handover.....	57
Τύποι Handovers.....	59
4.3.2 Έλεγχος Ισχύος.....	66
Βασικές προσεγγίσεις του ελέγχου ισχύος.....	67
Μηχανισμοί Ελέγχου Ισχύος στο UTRAN (WCDMA-FDD).....	67
Open Loop Power Control (OLPC).....	68
Closed Loop Power Control (CLPC).....	69
Έλεγχος ισχύος σε ειδικές περιπτώσεις.....	70
4.3.3 Λειτουργίες Ελέγχου στο UTRAN.....	71
4.3.3.1 Μετάδοση Πληροφοριών Συστήματος.....	71
4.3.3.2 Αρχική Πρόσβαση και Διαχείριση της σύνδεσης για σηματοδότηση.....	72
4.3.3.3 Διαχείριση του ραδιο Bearer.....	74
4.3.3.4 Ασφάλεια στο UTRAN.....	74
4.3.3.5 Διαχείριση κινητικότητας στο επίπεδο UTRAN.....	75
4.3.3.6 Χειρισμός της Βάσης Δεδομένων.....	79
4.3.3.7 Θέση του UE.....	79

Κεφάλαιο 5 Ασύρματο Δίκτυο UMTS

Εισαγωγή.....	80
5.1 Αρχιτεκτονική του CN στο 3GPP R99.....	81
5.2 Διαχείριση Κινητικότητας (MM).....	84
5.2.1 Ταυτότητες και Διευθύνσεις των χρηστών και των τερματικών.....	85
5.2.2 Δομές Θέσεων και ταυτότητες τους.....	89
5.2.3 Μοντέλο Διαχείρισης Κινητικότητας.....	91
5.2.3.1 Καταστάσεις MM σε κόμβο μεταγωγής κυκλώματος.....	91
5.2.3.2 Καταστάσεις MM σε κόμβο μεταγωγής πακέτου.....	92
5.3. Διαχείριση Επικοινωνίας (CM).....	93
5.3.1. Διαχείριση σύνδεσης για την μεταγωγή κυκλώματος.....	93
5.3.1.1 Διαχείριση Σύνδεσης – Εσωτερική εργασία στο δίκτυο.....	95
5.3.1.2. Διαχείριση σύνδεσης – Χρέωση.....	96
5.4.Πτυχές Αρχιτεκτονικής στην 3GPP R4.....	98
5.5 Πτυχές Αρχιτεκτονικής στην 3GPP R5.....	99

Κεφάλαιο 6 Το Τερματικό UMTS

6.1 Η αρχιτεκτονική του τερματικού.....	100
6.2 Διαφορές των τερματικών.....	103
6.3 Ιδιότητες των UMTS τερματικών.....	108
6.4 Εγγραφή στο UMTS.....	109
6.5 Interface Χρήστη.....	111

Κεφάλαιο 7 Υπηρεσίες σε περιβάλλον UMTS

7.1 Οι υπηρεσίες και το commercial μοντέλο.....	113
7.2 Αρχιτεκτονική του QoS.....	114
7.2.1 Ταξινόμηση του QoS στο UMTS.....	115
UMTS QoS τάξεις.....	116
7.2.2 QoS Classes – a Provocative Approach.....	119
7.3 Δυνατότητες υπηρεσιών στην πλατφόρμα UMTS Service Platform.....	123
7.3.1 Service Capability – Wireless Application Protocol (WAP).....	126
7.3.2. Service Capability – Location Communication Services (LCS).....	126
7.3.2.1. Περίληψη των μεθόδων τοποθέτησης.....	128
Θέση της ταυτότητας της κυψέλης Cell ID.....	129
Round Trip Time (RTT) Based Positioning.....	130
Χρόνος Άφιξης - Time of Arrival (TOA) Positioning.....	131
Διαφορά χρόνου άφιξης - Time Difference of Arrival (TDOA) Positioning.....	132
Γωνία άφιξης - Angle of Arrival Positioning (AOA).....	134
Reference Node Based Positioning (RNBP).....	135
Παγκόσμιο Σύστημα Τοποθέτησης - Global Positioning System (GPS).....	136
7.3.2.2. Ακρίβεια θέσης - Positioning Accuracy.....	138
7.3.2.3 Χαρακτηριστικές μέθοδοι τοποθέτησης για το UMTS.....	140
Cell ID Based Positioning in UMTS.....	140
Observed Time Difference of Arrival-Idle Period Down Link (OTDOA-IPDL) in UMTS.....	143
Assisted GPS for UMTS.....	144
7.2.3.4 Αρχιτεκτονική της δομής του συστήματος UMTS για τις υπηρεσίες θέσης- Location Services (LCS).....	145
Λειτουργίες του LCS στο CN.....	147
Λειτουργίες του LCS στο UTRAN.....	149
Λειτουργίες του LCS στο UE.....	150
LCS πελάτης και GMLC περιβάλλον.....	151
Τα πλεονεκτήματα της αρχιτεκτονικής λύσης LCS στο UMTS.....	152
7.3.3 Η ικανότητα υπηρεσιών – Εκτέλεση της κινητης εφαρμογής στο περιβάλλον (MExE).....	153
7.3.4. Ικανότητα υπηρεσιών-Εφαρμογή του εγχειριδίου UMTS SIM (USAT).....	155
7.3.5 Ικανότητα υπηρεσιών CAMEL SCE.....	156
7.3.6 Παράδειγμα : Ικανότητες υπηρεσιών σε κτίρια.....	158
7.4 Υπηρεσίες UMTS και σχέδια υπηρεσιών.....	161
7.4.1. Υπηρεσίες και η υπο συζήτηση QoS Class.....	162
7.4.2. Services and Streaming QoS class.....	167
7.4.3. Services and Interactive/Background Class.....	170
7.4.4 Service Concept: Virtual Home Environment (VHE).....	170

Κεφάλαιο 8 Ασφάλεια στο περιβάλλον UMTS

Εισαγωγή.....	173
8.1. Ασφάλεια πρόσβασης στο UMTS.....	175
8.1.1. Legacy from 2G.....	176
8.1.2. Αμοιβαία εξακρίβωση.....	179
8.1.3. Κρυπτογράφηση για την εξακρίβωση.....	183
8.1.4. Προσωρινές ταυτότητες.....	188
8.1.5. Απόκρυψη του UTRAN.....	190
8.1.6. Προστασία της ακεραιότητας του σήματος του RRC.....	194
8.2 Πτυχές ασφάλειας στα επίπεδα Συστήματος και Δικτύου.....	199
8.2.1. Περίληψη τα ασφάλειας του 3GPP Release 5 Network Domain.....	199
8.2.2. IPSEC.....	201
8.2.3. MAPSEC.....	204
8.3. Προστασία των εφαρμογών και των υπηρεσιών.....	205

Κεφάλαιο 9 Πρωτόκολλα UMTS

9.1 Αναφορά στην Αρχιτεκτονική των Πρωτοκόλλων που χρησιμοποιούνται στη 3GPP R99.....	207
9.1.2 Μοντέλο αναφοράς των UTRAN Πρωτοκόλλων.....	209
9.1.3 Το Μοντέλο Αναφοράς Πρωτοκόλλων του CN.....	210
9.2 Αρχιτεκτονική των εσωτερικών πρωτοκόλλων του UMTS.....	213
9.3 Πρωτόκολλα μεταφοράς στο δίκτυο μέσα στο Uu Interface.....	218
9.3.1 Πρωτόκολλο Ελέγχου Μέσης Πρόσβασης (MAC).....	218
9.3.2 Πρωτόκολλο ελέγχου Δικτύου (RLC).....	221
9.3.3 Πρωτόκολλο Μεταφοράς ATM.....	226
9.3.4 IP Transport for User Data (GTP-U).....	230
9.4. Πρωτόκολλα ΡαδιοΔικτύου.....	234
9.4.1. Radio Network Control Plane.....	234
9.4.1.1 RANAP – Radio Access Network Application – Εφαρμογές Ραδιοπρόσβασης δικτύου.....	234
9.4.1.2. RNSAP – Radio Network Subsystem Application Protocol.....	236
9.4.1.3. NBAP – Node B Πρωτόκολλο Εφαρμογής.....	239
9.4.1.4. Πρωτόκολλο RRC (Radio Resource Control).....	243
9.4.2. ΡαδιοΔίκτυο.....	246
9.4.2.1 PDPC-Packet Data Convergence Protocol.....	246
9.4.2.2 UTRAN FRAME PROTOCOLS.....	248
Frame Protocols at Iu –Πρωτόκολλα πεδίου στο Iu.....	249
Frame Protocol for Dedicated Channels at Iur & Iub.....	250
Frame Protocol for Common Transport Channels at Iur και Iub.....	251
9.5 System Network Protocol-Πρωτόκολλο συστήματος.....	252
9.5.1 Non – Access Stratum Protocols.....	252

9.5.1.1. MM Πρωτόκολλο για το CS Domain.....	252
9.5.1.2 GPRS Mobility Management for Ps Domain (GMM).....	257

ΚΕΦΑΛΑΙΟ 10 Παραδείγματα εφαρμογών

10.1. Εισαγωγή.....	260
10.1.1 Paging – Σελιδοποίηση.....	262
10.1.2.Εγκατάσταση της σύνδεσης της RRC Connection.....	265
10.1.3.Transaction Reasoning.....	268
10.1.4.Έλεγχος εξακρίβωσης και ασφάλειας.....	269
10.1.5.Εγκατάσταση transaction με την Allocation του Radio Access Bearer (RAB).....	270
10.1.6 Transaction.....	274
10.1.7 Transaction Clearing και απελευθέρωση του RAB.....	274
10.1.8 RRC Connection Release.....	278
10.2 RRM Procedure Examples.....	279
10.2.1 Soft Handover – Link Addition and Link Deletion.....	280
10.2.2. SRNS Relocation – Circuit Switched.....	284
10.2.3 Inter – System Handover from UMTS to GSM – Circuit Switched.....	287
10.3 MM Procedure Examples.....	290
10.3.1 Cell update.....	291
10.3.2 URA Update.....	293
10.3.3 Location Update to the CN CS domain.....	293
10.3.4. Routing Area Update to the CN PS domain.....	296
10.4 CC Procedure Example.....	298
10.5 Packet Data Example.....	302

Κεφάλαιο 11 Η Εποχή της 3G στην Ελλάδα

Εισαγωγή.....	305
---------------	-----

UMTS – Παγκόσμιο Σύστημα Κινητών Τηλεπικοινωνιών

Κεφάλαιο 1 Εισαγωγή

1.1 Υπάρχοντα Συστήματα Κινητών Τηλεπικοινωνιών

Οι κινητές τηλεπικοινωνίες εξελίσσονται ταχύτατα σήμερα αλλά η τεχνολογία τους δεν είναι πρόσφατη. Πριν από 30 – 40 χρόνια έκαναν την εμφάνισή τους μεγάλοι κόστους κινητές διατάξεις τηλεπικοινωνιών. Σημαντικό βήμα για τις κινητές τηλεπικοινωνίες έγινε στις αρχές της δεκαετίας του '80 οπότε εμφανίστηκε η αναλογική κυψελοειδής τεχνολογία. Φτάνοντας στο τέλος της χιλιετίας, η κινητή τηλεφωνία έχει μετατραπεί σε μαζικό προϊόν στην αγορά των τηλεπικοινωνιών.

Το σύστημα GSM (Global System for Mobile Communications) που λειτουργεί σε συχνότητα 900MHz καθώς και το DCS1800 (Digital Cellular System=Ψηφιακό Κυψελοειδές Σύστημα) που λειτουργεί σε συχνότητα 1800GHz, αποτελούν την συμβολή της Ευρώπης στην εξέλιξη των κινητών τηλεπικοινωνιών. Τα συστήματα αυτά σχεδιάστηκαν κατά την δεκαετία του '80 και άρχισαν να εφαρμόζονται σε διάφορες ευρωπαϊκές χώρες κατά το 1992. Το σύστημα GSM είναι ένα ψηφιακό κυψελοειδές σύστημα το οποίο κατέκτησε την παγκόσμια αγορά παρόλο που αρχικά αναπτύχθηκε αποκλειστικά για τα ευρωπαϊκά δεδομένα. Διαθέτει πολλές προηγμένες υπηρεσίες, όπως την συμβατότητα με το ISDN (Integrated Services Digital Network=Ψηφιακό Σύστημα Ολοκληρωμένων Υπηρεσιών), καθώς και την δυνατότητα περιαγωγής(roaming) παγκοσμίως σε άλλα δίκτυα GSM.

Ωστόσο, ο αριθμός των συνδρομητών στο GSM εκτιμάται από το Forum UMTS μέχρι τις αρχές του 2002 σε 400 εκατομμύρια και αναμένεται να ξεπεράσουν τα 1800 εκατομμύρια ως το 2005. Η ολοένα αυξανόμενη

ζήτηση των κινητών επικοινωνιών έχει ήδη προβλεφθεί και αναμένεται ότι το 2010, περίπου το 60% των επικοινωνιών της Ευρώπης θα πραγματοποιούνται με πολυμεσικές εφαρμογές κινητών επικοινωνιών.

Μια ανάλογη αύξηση αναμένεται και παγκοσμίως, με ετήσιο ρυθμό γύρω στο 70%. Σημειώνεται, ότι οι χρήστες δεδομένων το 1998 έφταναν τα 3 εκατομμύρια ενώ το 2005 αναμένεται να είναι 77 εκατομμύρια. Οι προβλέψεις της αγοράς των κινητών ραδιοσυστημάτων δείχνει μια αυξανόμενη ζήτηση μεγάλης σειράς υπηρεσιών από υπηρεσίες φωνής και χαμηλόρυθμες υπηρεσίες μετάδοσης δεδομένων μέχρι υπηρεσίες μετάδοσης υψηλής ταχύτητας.

Προβλέπεται ότι θα απαιτούνται πιο προηγμένες υπηρεσίες από τις υπηρεσίες φωνής και τις χαμηλόρυθμες υπηρεσίες μετάδοσης σύμφωνα με τις παρακάτω τρεις κατηγορίες:

1. Ηλεκτρονικά δεδομένα με πρόσβαση στο διαδίκτυο, ηλεκτρονικό ταχυδρομίο, σύγχρονη μεταφορά εικόνων, μεταφορά αρχείων πολυμέσων, φορητοί υπολογιστές.

2. Κινητές τηλεπικοινωνίες, βιντεοσυνδιάσκεψη, υπηρεσίες GSM και ISDN, εικονοτηλεφωνία, υπηρεσίες ευρυζωνικών δεδομένων.

3. Δεδομένα εικόνας / ήχου με προαιρετική την εικόνα, αλληλεπιδραστικές υπηρεσίες εικόνας, infotainment, ηλεκτρονικά έντυπα, αγορές από απόσταση ή ηλεκτρονικό εμπόριο, υπηρεσίες διαδικτύου προστιθέμενης αξίας, συμβολή στο ραδιόφωνο και στην τηλεόραση.

Επιπλέον αναμένεται υψηλό επίπεδο ασυμμετρίας ανάμεσα στην κατερχόμενη και την ανερχόμενη ζεύξη για την μετάδοση των δεδομένων(π.χ. για πρόσβαση στο Διαδίκτυο), όπου απαιτείται μεγαλύτερη χωρητικότητα στην κατερχόμενη ζεύξη.

Από τα παραπάνω είναι φανερό ότι όχι μόνο έχει αυξηθεί ο αριθμός των χρηστών αλλά και οι κινητές επικοινωνίες έχουν γίνει πιο απαιτητικές σε εύρος ζώνης και πιο ασύμμετρες. Η στρατηγική που ακολουθείται από την βιομηχανία υπαγορεύει να συγκλίνουν οι υπάρχουσες προδιαγραφές

σε ένα μοναδικό παγκόσμιο πρότυπο προδιαγραφών. Τέλος, τα τρέχοντα κινητά συστήματα 2^{ης} γενιάς δεν μπορούν με κανένα τρόπο να ανταποκριθούν στις παραπάνω απαιτήσεις σε εύρος ζώνης και στην συμβατότητα.

Αναπόφευκτα, οι παραπάνω εφαρμογές παρουσιάζουν τεχνικές απαιτήσεις, οι οποίες μπορούν να ικανοποιηθούν μόνο με την ανάπτυξη μιας νέας βελτιωμένης γενιάς κινητών ραδιοσυστημάτων.

1.1.1 Ανάπτυξη 3^{ης} Γενιάς Συστημάτων Κινητών Τηλεπικοινωνιών

Η Τρίτη γενιά κινητών συστημάτων επικοινωνιών είναι γνωστή ως IMT – 2000 (International Mobile Telecommunications=Διεθνείς Κινητές Τηλεπικοινωνίες). Η σταδιακή μετάβαση από τα συστήματα 2^{ης} στα συστήματα 3^{ης} γενιάς ξεκίνησε με την αλλαγή του αιώνα. Υπάρχουν παγκόσμιοι φορείς τυποποίησης των οποίων έργο είναι ο σχεδιασμός και η ανάπτυξη των συστημάτων 3^{ης} γενιάς. Οι φορείς αυτοί είναι:

1. Για την Ευρώπη ο ETSI (European Telecommunications Standards Institute=Ευρωπαϊκό Ινστιτούτο Τυποποίησης των Τηλεπικοινωνιών).
2. Για τις ΗΠΑ ο TIA (Telecommunications Industry Association=Ένωση Βιομηχανιών Τηλεπικοινωνιών).
3. Για την Ιαπωνία ο ARIB (Association of Radio Industries and Businesses=Ένωση Βιομηχανιών&Επιχειρήσεων Ραδιοεπικοινωνιών).
4. Για την Ν. Κορέα ο TTA (Telecommunications Technology Association=Ένωση για τις Τεχνολογίες Τηλεπικοινωνιών).

Για να εξασφαλιστούν οι διεθνείς προδιαγραφές, αναπτύσσεται η 3GPP (3d Generation Partnership Project=Έργο 3^{ης} Γενιάς), η οποία είναι αποτέλεσμα συνεργασίας των παραπάνω φορέων. Το UMTS που έχει προταθεί από τον ETSI είναι η πρόταση της Ευρώπης για τα παγκόσμια συστήματα 3^{ης} γενιάς IMT – 2000.

Η εισαγωγή των κινητών συστημάτων 3^{ης} γενιάς ξεκίνησε μέσω ενός αριθμού προ-λειτουργικών και λειτουργικών φάσεων που θα υλοποιηθούν κατά τα έτη 2000 – 2005. Σκοπός αυτής της προσέγγισης είναι να μειωθεί ο κίνδυνος και το κόστος για τους χειριστές, να εξασφαλιστεί η γρήγορη αναγνώριση των υπηρεσιών από τους τελικούς χρήστες και να είναι εγγυημένη η επιτυχής εφαρμογή του κινητού συστήματος 3^{ης} γενιάς. Οι πρωταρχικές φάσεις ανάπτυξης του UMTS είναι οι ακόλουθες:

1. Αύξηση της χωρητικότητας του GSM έτσι ώστε να περιλαμβάνει πακέτα (GPRS) και λειτουργίες μεταφορές υψηλών ταχυτήτων (EDGE = Enhanced Data Rates for GSM=Βελτιωμένοι ρυθμοί δεδομένων για το Παγκόσμιο Σύστημα Κινητών Επικοινωνιών). Η φάση αυτή είναι γνωστή ως φάση GSM2+

2. Προ UMTS δοκιμασική φάση, κατά την οποία οι σταθμοί βάσης θα δοκιμάζονται είτε ως υποσύνολα είτε ως απομονωμένα δοκιμασικά δίκτυα πακέτου.

3. Βασική φάση ανάπτυξης, η οποία ξεκίνησε το 2002 και περιλαμβάνει την πρώτη ενσωμάτωση των σταθμών βλασης UTRA σε «ενεργά» δίκτυα και την προώθηση των δορυφορικών υπηρεσιών UMTS. Επίσης, θα περιλαμβάνει νέες υπηρεσίες βασισμένες εξολοκλήρου στις δυνατότητες του UMTS και υποστήριξη υπηρεσιών μικρού και μεγάλου εύρους ζώνης στις ίδιες διεπαφές UTRA (UMTS Terrestrial Access=UMTS Επίγειας Πρόσβασης).

4. Φάση εμπορευματοποίησης, η οποία έχει σχεδιαστεί να ξεκινήσει μέσα στο 2003 και αναμένεται να αποδώσει κατά το 2005, ενσωματώνοντας τις βελτιώσεις της απόδοσής του και εισάγοντας νέες πολύπλοκες υπηρεσίες UMTS.

1.1.2 Προλειτουργικές φάσεις του UMTS: GPRS / EDGE

Η παρούσα φάση των τηλεπικοινωνιών είναι η GSM 2+. Προκειμένου να ικανοποιηθούν οι ολοένα και αυξανόμενες απαιτήσεις των

χρηστών και να διαφυλαχθεί η ανταγωνιστικότητα, βασικό μέλημα κατά την ανάπτυξη της φάσης GSM 2+ από τον ETSI, ήταν ο προσδιορισμός μιας γενικής ραδιοπηρεσίας πακέτου (GPRS), η οποία παρέχει συνδέσεις υψηλού εύρους ζώνης. Το επόμενο βήμα μετά το GPRS είναι το σύστημα EDGE (Βελτιωμένοι ρυθμοί δεδομένων για το Παγκόσμιο Σύστημα Κινητών Επικοινωνιών), το οποίο εξασφαλίζει την ομαλή μετάβαση στην Τρίτη γενιά συστημάτων.

Η εισαγωγή του συστήματος UMTS θα πρέπει να πραγματοποιηθεί μέσα από μια σειρά προ-λειτουργικών φάσεων, κατά την πενταετία 2000-2005. Πρόκειται για την μετάβαση από την φάση GSM +2 προς την φάση 3, η οποία αφορά στην πλήρη ανάπτυξη και αξιοποίηση του συστήματος κινητών επικοινωνιών. Οι πρωταρχικές φάσεις ανάπτυξης του συστήματος UMTS είναι η επέκταση της χωρητικότητας του συστήματος GSM προκειμένου να περιλαμβάνει την τεχνολογία υψηλών ταχυτήτων GPRS και στην συνέχεια, η χρήση του συστήματος EDGE. Τα δύο συστήματα που αναφέρθηκαν θα προσφέρουν πολύτιμη εμπειρία και μπορούν να παρέχουν μια βάση για την ανάπτυξη υπηρεσιών διασυνεργασίας, διεπαφών παροχέα υπηρεσιών καθώς επίσης και ενός πυρήνα κινητών υπηρεσιών πολυμέσων.

1.1.3 Πολλαπλές Τεχνικές Πολλαπλής Πρόσβασης Διαίρεσης Κώδικα (CDMA) – Στάδια Τυποποίησης

Η Ευρωπαϊκή Επιτροπή χρηματοδοτεί σειρά ερευνητικών δραστηριοτήτων στο πλαίσιο Προηγμένων Τεχνολογιών και Υπηρεσιών Τηλεπικοινωνιών (ACTS), οι οποίες σχετίζονται με τα συστήματα κινητών επικοινωνιών, προκειμένου να υποστηριχθεί η διεθνής συναίνεση και τυποποίηση. Παλαιότερο ερευνητικό πρόγραμμα ήταν το πρόγραμμα Έρευνας Προηγμένων Τηλεπικοινωνιών στην Ευρώπη (RACE) I και II, το οποίο εστίαζε στη διερεύνηση προηγμένων ραδιοεπαφών προηγμένου

συστήματος Πολλαπλής Πρόσβασης Διαίρεσης Χρόνου (TDMA) και συστήματος CDMA.

Το Μελλοντικό Πολλαπλό Σύστημα Πρόσβασης Ραδιοσυχνοτήτων (FRAMES) ήταν το μόνο πρόγραμμα ACTS που ασχολήθηκε με το επίγειο τμήμα του συστήματος UMTS. Βασικός σκοπός του ήταν να αναπτυχθεί ένα μοντέλο – πρόταση ραδιοεπαφής, το οποίο θα πληρεί τις απαιτήσεις των επίγειων συστημάτων κινητών επικοινωνιών τρίτης γενιάς. Το αρχικό μοντέλο FRAMES πληρούσε τις προϋποθέσεις αυτές και λάμβανε υπόψη την παγκόσμια εμβέλεια του συστήματος GSM, σχετικά με τις συγκεκριμένες παραμέτρους και το δίκτυο πυρήνα GSM. Βασισμένο στις απαιτήσεις του συστήματος UMTS καθώς και τις δραστηριότητες και τις αποφάσεις που ελήφθησαν σε διάφορα μέρη του κόσμου, το έργο FMA αναπτύχθηκε αρχικά το 1996 συνδυάζοντας τεχνικές TDMA και CDMA σε μια εναρμονισμένη πλατφόρμα προκειμένου να είναι συμβατό με όλα τα πιθανά σενάρια του συστήματος UMTS και να μπορεί να προτείνει σφαιρικές τεχνικές λύσεις.

Τελικά, τον Ιανουάριο του 1998, μετά την αξιολόγηση μεγάλου αριθμού προτάσεων για το μοντέλο επίγειας ραδιοζεύξης με σύστημα UMTS, το Ευρωπαϊκό Ινστιτούτο Τυποποίησης των Τηλεπικοινωνιών αποφάσισε να θιοθετήσει το CDMA μεγάλου εύρους ζώνης και ένα υβρίδιο του TDMA/CDMA. Τα δύο μοντέλα πρόσβασης χρησιμοποιούνται για το μοντέλο Αμφίδρομης Διαιρεμένης Συχνότητας (FDD) του UTRA και το μοντέλο Χρονοδιαιρετικής Αμφίδρομης Επικοινωνίας.

1.2 Επίδραση των χαρακτηριστικών του συστήματος UMTS στη διαχείριση πόρων ραδιοδικτύου (RRM).

1.2.1 Μεγάλο εύρος ζώνης

Τα συστήματα του μέλλοντος αναμένεται να απαιτούν πολύ μεγαλύτερους ρυθμούς μετάδοσης δεδομένων από τα σημερινά αλλά θα

περιορίζονται από τις συνθήκες μετάδοσης, όπως η απώλεια λόγω απόστασης, και οι πολλαπλές διαδρομές. Επειδή η απαιτούμενη ισχύς του πομπού αυξάνει γραμμικά με το εύρος, δεν θα υπάρχει πρόσβαση υψηλής ταχύτητας σε μεγάλο εύρος. Αυτό θα αυξήσει την πολυπλοκότητα των μοντέλων διαχείρισης πόρων.

1.2.2 Πολλαπλές Προδιαγραφές QoS

Το εύρος ζώνης δεν είναι ιδιαίτερα σημαντικό για το σχεδιασμό και την απόδοση των μοντέλων διαχείρισης πόρων, σε αντίθεση με τα χαρακτηριστικά κυκλοφορίας που είναι σημαντικά. Τα βασικά προβλήματα διαχείρισης στα συστήματα πολυμέσων σχετίζονται με ρυθμούς μετάδοσης δεδομένων και τους μηχανισμούς πρόληψης καθυστερήσεων, όπως η κυκλοφορία σε μικρά περιβάλλοντα κελιών, θα παρουσιάσουν μεγάλες απαιτήσεις σε χωρητικότητα.

Οι χρήστες εφαρμογών video πιθανόν να απαιτήσουν σημαντικά τμήματα του φάσματος, το οποίο θα μοιράζονται, π.χ. με την κυκλοφορία των ηλεκτρονικών μηνυμάτων, η οποία δεν παρουσιάζει καμιά απαίτηση σε θέματα ταχύτητας. Η δυναμική κατανομή καναλιών παρέχει μεγάλη οικονομία σε χωρητικότητα από τις σημερινές διατάξεις κινητής τηλεφωνίας.

Τα συστήματα με ασυνεχή μετάδοση δεδομένων θα παρουσιάσουν ένα διαφορετικό είδος προβλήματος. Εφόσον δεν υπάρχει συνεχής μετάδοση δεν μπορεί να εξασφαλιστεί η καλή ποιότητα του συνδέσμου παρά μόνο κατά την στιγμή της πραγματοποίησης μιας μετάδοσης. Αυτό επηρεάζει όλες τις αποφάσεις διαχείρισης πόρων (κατανομή καναλιών, έλεγχος ισχύος, αποφάσεις μεταπομπής). Σε αυτές τις περιπτώσεις, οι αποφάσεις κατανομής καναλιών και ελέγχου ισχύος πρέπει να γίνουν με βάση τις εκτιμώμενες μετρήσεις ποιότητας του συνδέσμου κι όχι τόσο με τις στιγμιαίες τιμές. Ένας τρόπος είναι να διατηρηθεί τεχνητά ένας φυσικός

σύνδεσμος ακόμα και όταν δεν υπάρχουν δεδομένα, ορίζοντας ένα ελάχιστο επίπεδο αδράνειας.

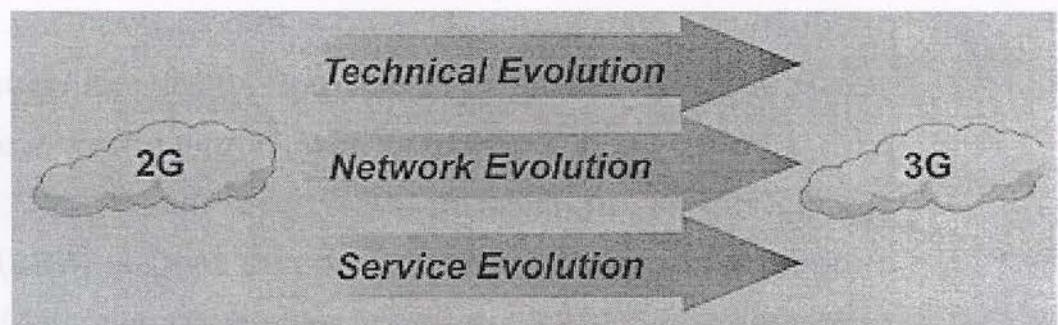
1.2.3 Ασύμμετρη Κυκλοφορία

Τα σημερινά συστήματα κινητής τηλεφωνίας είναι σχεδιασμένα κυρίως για την παροχή υπηρεσιών φωνής και λειτουργούν με συμμετρικό αμφίδρομο τρόπο. Οι ρυθμοί μετάδοσης δεδομένων και άλλες παράμετροι QoS στα συστήματα αυτά είναι ίδιες τόσο στην ανερχόμενη όσο και στην κατερχόμενη ζεύξη. Στα συστήματα τρίτης γενιάς, αναμένεται να επικρατήσει η κυκλοφορία δεδομένων που μεταδίδονται από IP εφαρμογές ανάκλησης πληροφοριών. Σε πολλές από τις εφαρμογές αυτές, η αυξανόμενη τιμή της συνολικά προσφερόμενης αναλογίας αναμένεται να επιβαρύνει το τμήμα κατερχόμενης ζεύξης του συστήματος.

Η παροχή υπηρεσιών πολυμέσων σε ασύσματα συστήματα παρουσιάζει μεγάλες απαιτήσεις αποτελεσματικής διαχείρισης πόρων ραδιοδικτύου.. Οι χρήστες θα χρειάζονται έναν αριθμό συνδέσμων με διάφορες ρυθμίσεις των παραμέτρων QoS. Για να χειριστεί αυτή την ποικιλία των υπηρεσιών χρήστη, του σύστημα UMTS θα παρέχει ένα εν δυνάμει μεγάλο αλλά πεπερασμένο σύνολο βασικών υπηρεσιών, κάθε μια από τις οποίες θα προσφέρει ένα συγκεκριμένο σύνολο παραμέτρων QoS.

Κεφάλαιο 2 Η Εξέλιξη από το GSM στο UMTS

Η εξέλιξη από το GSM στο UMTS καλύπτει όχι μόνο την **τεχνική εξέλιξη των στοιχείων δικτύου** αλλά και των **επεκτάσεων της δομής (αρχιτεκτονικής) του δικτύου** και των **υπηρεσιών δικτύου**. Όταν αυτοί οι τρεις τύποι εξέλιξης προσαρμόζονται μαζί, η ομαλή μετάβαση από τη δεύτερη γενιά (2G) στην Τρίτη γενιά (3G) θα είναι επιτυχής και θα επιφέρει κέρδη.



Εικόνα 1 Τύποι Εξέλιξης

2.1 Τύποι Εξέλιξης

Όταν μιλάμε για την τεχνική εξέλιξη εννοούμε το μονοπάτι ανάπτυξης, το πώς τα στοιχεία του δικτύου θα εφαρμοστούν και με ποια τεχνολογία. Αυτή είναι μια πολύ απλή ανάπτυξη και ακολουθεί αυστηρά τις γενικές, κοινές τάσεις εξελίξεων της τεχνολογίας. Σε αυτήν την φάση πρέπει να ληφθεί υπόψη ότι ένα δίκτυο είναι τόσο ισχυρό όσο το πιο αδύνατο στοιχείο του και εξαιτίας των ανοικτών interfaces που καθορίζονται στις προδιαγραφές, πολλά δίκτυα είναι συνδυασμοί που ο εξοπλισμός τους προέρχεται από πολλούς προμηθευτές.

Η βασική ιδέα πίσω από τις προδιαγραφές του **GSM** ήταν να καθοριστούν διάφορα ανοικτά interfaces, τα οποία καθορίζουν τα τυποποιημένα συστατικά του **GSM συστήματος**. Εξαιτίας της επέκτασης

των interfaces, ο χειριστής που διατηρεί το δίκτυο μπορεί να συμπεριλάβει διαφορετικά συστατικά του δικτύου από διαφορετικούς προμηθευτές δικτύων GSM. Επίσης, όταν ένα interface επεκτείνεται, καθορίζει αυστηρά πώς οι λειτουργίες του δικτύου προχωρούν στο interface και αυτό με τη σειρά του καθορίζει στη συνέχεια ποιες λειτουργίες αφήνονται για να εφαρμοστούν εσωτερικά από τα στοιχεία του δικτύου και στις δύο πλευρές του interface.

Όπως αποδείχθηκε κατά τη λειτουργία των αναλογικών κινητών δικτύων, η συγκεντρωμένη νοημοσύνη (**centralized intelligence**) παρήγαγε πολύ φορτίο στο σύστημα, παρόλο που μείωσε τη γενική απόδοση του συστήματος. Γι' αυτό η προδιαγραφή του GSM παρείχε σε γενικές γραμμές τα μέσα για να διανεμηθεί η νοημοσύνη σε όλο το δίκτυο.

Από την μεριά του δικτύου GSM, αυτή η αποκεντρωμένη νοημοσύνη εφαρμόζεται με τη διαίρεση ολόκληρου του δικτύου σε 4 ξεχωριστά υποσυστήματα που είναι το υποσυστήμα δικτύων (**NSS**), το υποσυστήμα σταθμών βάσεων (**BSS**), το υποσυστήμα διοίκησης δικτύων (**NMS**) και τον κινητό σταθμό (**MS**).

Το **BSS** είναι το μέρος του δικτύου το οποίο είναι αρμόδιο για το ραδιοέλεγχο διαδρομών. Κάθε κλήση συνδέεται μέσω του BSS. Το **NSS** είναι το μέρος του δικτύου το οποίο φροντίζει τις λειτουργίες ελέγχου κλήσης. Κάθε κλήση συνδέεται πάντα από και μέσω το NSS. Το **NMS** είναι το λειτουργικό τμήμα του δικτύου και αυτό που ασχολείται με την συντήρηση του δικτύου. Είναι επίσης απαραίτητο για ολόκληρο τον έλεγχό του. Ο χειριστής του δικτύου παρατηρεί και διατηρεί την ποιότητα και τις υπηρεσίες του δικτύου μέσω του NMS. Τα open interface σε αυτήν την περίπτωση βρίσκονται μεταξύ του **MS** και του **BSS** (interface Um) και μεταξύ του **BSS** και του **NSS** (interface A). Το interface μεταξύ του **NMS** και των **NSS/BSS** αναμενόταν να είναι ανοικτό, αλλά οι προδιαγραφές του δεν ήταν έτοιμες έγκαιρα και γι' αυτό κάθε κατασκευαστής εφαρμόζει τα interface NMS με τις δικές τους μεθόδους.

Το **MS** είναι ένας συνδυασμός ενός ιδεατού μοντέλου υπηρεσιών και του εξοπλισμού του τερματικού. Ο τελικός εξοπλισμός υπό αυτήν τη μορφή ο οποίος καλείται κινητός εξοπλισμός (**ME**) και τα στοιχεία του συνδρομητή καταχωρούνται σε ένα ξεχωριστό μοντέλο αποκαλούμενο μοντέλο ταυτότητας υπηρεσίας (**SIM**). Ως εκ τούτου,

$$\mathbf{ME + SIM = MS}$$

Η επόμενη τεχνολογία για την κινητή τηλεφωνία είναι το **GPRS**. Το GPRS έχει την δυνατότητα να χρησιμοποιεί ασύμμετρες συνδέσεις όταν χρειάζεται και έτσι οι πηγές του δικτύου χρησιμοποιούνται καλύτερα. Το GPRS είναι ένα μέσο το οποίο φέρνει την IP mobility και το Internet πιο κοντά στον ψηφιακό χρήστη αλλά και όχι μια ολοκληρωτική λύση για την IP mobility (κινητικότητα). Από την πλευρά των υπηρεσιών, το GPRS ξεκινά μια διαδρομή ανάπτυξης όπου όλο και περισσότερα παραδοσιακά κυκλώματα μεταγωγής υπηρεσιών μετατρέπονται για να χρησιμοποιηθούν πάνω στο GPRS επειδή αυτές οι υπηρεσίες ήταν από την αρχή πιο κατάλληλες για τις συνδέσεις μεταγωγής πακέτων. Ένα παράδειγμα γι' αυτό είναι το πρωτόκολλο WAP (ασύρματο πρωτόκολλο εφαρμογής), η δυνατότητα του οποίου ανακαλύπτεται κατά την χρησιμοποίηση του GPRS.

Όταν οι συνδέσεις μεταγωγής πακέτων χρησιμοποιούνται, η **ποιότητα της υπηρεσίας (QoS)** είναι ένα πολύ ουσιαστικό ζήτημα. Σε γενικές γραμμές το GPRS υποστηρίζει την έννοια **QoS** αλλά στην πράξη όχι. Ο λόγος εδώ είναι ότι η κίνηση του GPRS είναι δεύτερης προτεραιότητας κίνηση στο δίκτυο GSM: το GSM χρησιμοποιεί τις άλλες αχρησιμοποίητες πηγές του Um interface. Επειδή το μέγεθος των αχρησιμοποίητων πηγών δεν είναι ακριβώς γνωστό εκ των προτέρων, κανένας δεν μπορεί να εγγυηθεί ένα ορισμένο εύρος ζώνης συχνοτήτων για το GPRS άρα και για το QoS δεν μπορεί να υπάρξει εγγύηση.

Η **Τρίτη γεννιά κινητής υπηρεσίας, 3G**, εισάγει τη νέα μέθοδο ραδιο προσπέλασης, την **WCDMA**. Η WCDMA και οι παραλλαγές της

είναι παγκόσμιες, επομένως όλα τα δίκτυα τρίτης γεννιάς πρέπει να είναι σε θέση να αποδεχθούν την πρόσβαση από οποιονδήποτε συνδρομητή δικτύων τρίτης γεννιάς. Επιπρόσθετα, η WCDMA έχει μελετηθεί λεπτομερώς στις εργαστηριακές εγκαταστάσεις και έχει αναγνωρισθεί ότι έχει καλύτερα φασματικά αποτελέσματα από την **TDMA** (σε ορισμένες περιπτώσεις) και είναι καταλληλότερη για τη μεταφορά πακέτων από την μέθοδο TDMA βασισμένη στη ραδιο πρόσβαση. Η WCDMA και ο ραδιο εξοπλισμός πρόσβασης δεν είναι υπό αυτήν τη μορφή συμβατοί με τον εξοπλισμό GSM, και γι' αυτό έχοντας προσθέσει την WCDMA στο δίκτυο πρέπει να προστεθούν νέα στοιχεία: ο *ραδιο ελεγκτής δικτύων* (**RNC**) και ο *σταθμός βάσης* (**BS**).

Οι συνδέσεις μεταφοράς μέσα στο ραδιο δίκτυο πρόσβασης WCDMA εφαρμόζονται με τη χρησιμοποίηση του ATM πάνω στα μέσα των φυσικών μεταφορών (εφαρμογές της 3GPP R99). Σε μια προτυποποίηση (FRAMES (1996-1998)) συζητήθηκε πολύ αν θα πρέπει να χρησιμοποιηθεί το ATM στο δίκτυο ή όχι. Το τελικό συμπέρασμα ήταν να χρησιμοποιηθεί το ATM για **δύο λόγους**:

1) το μέγεθος του κελιού του ATM και το οφέλιμο φορτίο του είναι σχετικά μικρό. Το **πλεονέκτημα** εδώ είναι ότι η ανάγκη της αποθήκευσης πληροφοριών μειώνεται. Εάν έχουμε μεγάλη αποθήκευση, οι αναμενόμενες καθυστερήσεις θα αυξηθούν εύκολα και επίσης το στατικό φορτίο στον εξοπλισμό αποθήκευσης θα αυξηθεί. Θα πρέπει να ληφθεί υπόψη αυτή η αποθήκευση και έτσι οι υπάρχουσες καθυστερήσεις έχουν ένα αρνητικό αντίκτυπο στις απαιτήσεις του QoS πραγματικού χρόνου κίνησης.

2) Η άλλη εναλλακτική λύση, η IP και η έκδοσή της IPv4, έχει υπολογισθεί να χρησιμοποιηθεί επίσης αλλά η **IPv4 έχει μερικά σοβαρά μειονεκτήματα**. Είναι περιορισμένη στο περιβάλλον της και επιπλέον δεν υποστηρίζει το QoS. Από την άλλη μεριά, το ATM και το bit rate ταιριάζουν πολύ καλά με τις απαιτήσεις του QoS. Αυτό οδηγεί στο

συμπέρασμα ότι, όπου τα **ATM** και **IP** *συνδυάζονται* (για την κυκλοφορία πακέτων) το IP χρησιμοποιείται πάνω από το ATM. Αυτή η λύση συνδυάζει τα καλά σημεία και των δύο πρωτοκόλλων: το IP είναι κατάλληλο για τις συνδέσεις με τα άλλα δίκτυα και το ATM φροντίζει την ποιότητα και επίσης τη δρομολόγηση της σύνδεσης. Εξαιτίας των μειονεκτημάτων του IPv4 έχει γίνει ένας συμβιβασμός. Ορισμένα στοιχεία από την χρήση του δικτύου χρησιμοποιούν IPv4 τύπου διευθύνσεις αλλά η πραγματική κίνηση των τελικών χρηστών-συνδρομητών χρησιμοποιεί τις δυναμικές τροποποιημένες IPv6 διευθύνσεις οι οποίες είναι έγκυρες μέσα στο δίκτυο τρίτης γεννιάς. Για να προσαρμοστεί το δίκτυο 3G στα άλλα δίκτυα σε αυτήν την περίπτωση, η δομή του δικτύου 3G IP πρέπει να περιέχει δυνατότητα μετατροπής της διεύθυνσης IPv4 σε IPv6, επειδή τα εξωτερικά δίκτυα μπορεί να μην υποστηρίζουν απαραίτητως τις IPv6.

Κεφάλαιο 3 Βασικές πληροφορίες για το UMTS RADIO COMMUNICATION

Ο σκοπός αυτού του κεφαλαίου είναι να εισαχθούν εν συντομία δύο θεμελιώδη ζητήματα ραδιοεπικοινωνίας, Πρώτα, ο λόγος πίσω από τους περιορισμούς και επίσης για να αντιληφθούμε τη βασική δομή οποιουδήποτε ραδιοσυστήματος επικοινωνιών. Το δεύτερο ζήτημα είναι σχετικό με το πώς η ραδιοεπικοινωνία αντιμετωπίζεται συγκεκριμένα στο **UMTS**. Αυτό εξετάζεται με την περιγραφή των βασικών στοιχείων της τρίτης γενιάς (3G) και πιο συγκεκριμένα του WCDMA -FDD, παρέχοντας τους ουσιαστικούς μηχανισμούς και την ορολογία.

3.1 Η επικοινωνία βασικών αρχών ραδιοεπικοινωνίας

Η επικοινωνία είναι πάντα το ουσιαστικό μέρος κάθε είδους κοινωνίας και ειδικά ανθρώπινης κοινωνίας. Επειδή η κοινωνική εξέλιξη είναι ένα έμφυτο χαρακτηριστικό της συλλογικής ζωής με αποτέλεσμα τις περιπλοκότερες σχέσεις αλληλεπίδρασης, τα πιο προηγμένα μέσα απαιτείται πάντα να συναντήσουν τις απαιτήσεις της επικοινωνίας μεταξύ των μελών της κοινωνίας. Κατά τη διάρκεια της ιστορίας της ανθρώπινης ζωής, πολλές τεχνικές έχουν αναπτυχθεί με σκοπό την επικοινωνία. Μεταξύ τους, η ραδιοεπικοινωνία είναι, και θα είναι μια από τις σημαντικότερες τεχνικές που το άτομο έχει χρησιμοποιήσει ποτέ για να επικοινωνεί.

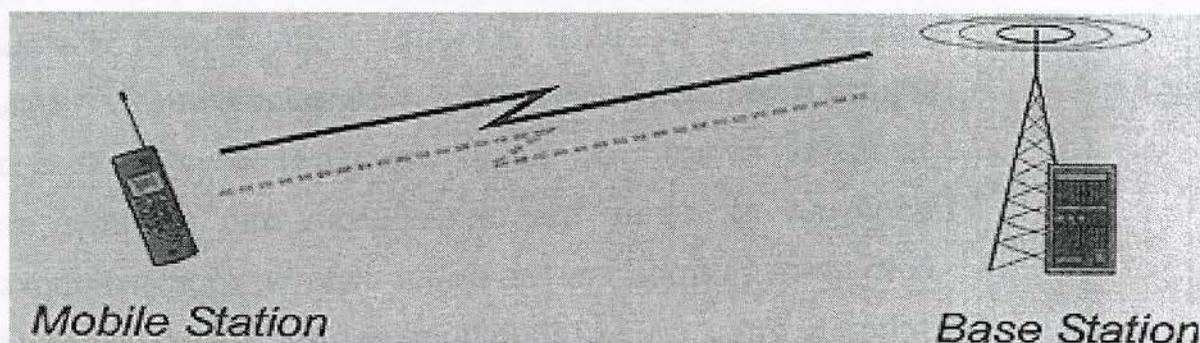
Η χρήση της ραδιοεπικοινωνίας έχει ανακαλυφθεί από τότε που ο Hertz εμφάνισε πειραματικά τη σχέση μεταξύ του φωτός και της ηλεκτρικής ενέργειας το 1887 αφού ο Maxwell είχε επεξηγήσει τις κύριες εξισώσεις των ηλεκτρομαγνητικών πεδίων το 1864. Κατόπιν, ο Marcony χρησιμοποίησε το " ερτζιανό " κύμα για να επικοινωνεί, κάνοντας την

εφεύρεση της ασύρματης τηλεγραφίας σε 1896. Εκμεταλλευόμενοι το ραδιο κύμα για τη διαβίβαση των πληροφοριών, αυτό το ραδιοκύμα είναι το βασικό μέρος κάθε είδους ραδιοεπικοινωνίας.

Η θεμελιώδης αρχή της ραδιοεπικοινωνίας είναι ότι χρησιμοποιεί τα ραδιο κύματα ως μέσο μεταφοράς. Σαν φυσικά φαινόμενα, τα ραδιο κύματα είναι μια συνέπεια των ηλεκτρομαγνητικών πεδίων. Κάτω από ορισμένες περιστάσεις, τα χρονικά εξαρτώμενα ηλεκτρομαγνητικά πεδία παράγουν τα κύματα που ακτινοβολούν από την πηγή στο περιβάλλον. Αυτή η πηγή μπορεί να είναι παραδείγματος χάριν μια συσκευή αποστολής σημάτων όπως έναν σταθμό βάσεων ή ένα κινητό μικροτηλέφωνο. Επειδή τα ραδιο κύματα γενικώς είναι βασισμένα στα ηλεκτρομαγνητικά πεδία, τα χαρακτηριστικά τους είναι αυστηρά εξαρτώμενα από το περιβάλλον όπου τα κύματα διαδίδονται. Σαν συνέπεια, ένα ραδιο κύμα βασισμένο σε σύστημα ραδιοεπικοινωνίας είναι τρωτό στους περιβαλλοντικούς παράγοντες, παραδείγματος χάριν, τα βουνά, τους λόφους, τεράστιους ανακλαστήρες όπως τα κτίρια, η ατμόσφαιρα, και άλλα.

Κάθε σύστημα επικοινωνίας αποτελείται από τουλάχιστον δύο στοιχεία, τα οποία είναι η **συσκευή αποστολής σημάτων** και ο **δέκτης**. Αυτά τα δύο στοιχεία μπορούν να ενσωματωθούν σε μια συσκευή (πομποδέκτης) έτσι ώστε να είναι ικανά να λειτουργούν και τα δύο ως συσκευή αποστολής σημάτων και συσκευή-δέκτης. Ένα παράδειγμα μιας τέτοιας συσκευής είναι ο *σταθμός βάσης* και το *κινητό μικροτηλέφωνο* σε οποιοδήποτε προηγμένο δημόσιο σύστημα κινητών επικοινωνιών. Η εικόνα 2 επεξηγεί το απλούστερο σύστημα ραδιοεπικοινωνίας, που αποτελείται από έναν σταθμό βάσης και ένα κινητό μικροτηλέφωνο. Υποθέστε ότι ο σταθμός βάσεων ενεργεί ως πηγή συσκευών αποστολής σημάτων για έναν συγκεκριμένο χρόνο με ορισμένες περιβαλλοντικές περιστάσεις. Κατόπιν το ραδιο σήμα ακολουθεί την πορεία από τον σταθμό βάσης στον κινητό σταθμό με την ταχύτητα του φωτός. Η λαμβάνουσα δύναμη σήματος στο μικροτηλέφωνο εξαρτάται από την

απόσταση από το σταθμό βάσης, το μήκος κύματος, και το περιβάλλον επικοινωνίας.



Εικόνα 2 Βασικά Στοιχεία ενός ραδιο συστήματος επικοινωνίας

Ο μηχανισμός διάδοσης ραδιο κυμάτων εξαρτάται πολύ από τα μήκη κύματος ή τις συχνότητες. Εκτός από αυτό, οποιοδήποτε προκαλούμενο από τον άνθρωπο ή φυσικό εμπόδιο όπως τα υψηλά κτίρια, την έκταση, τις καιρικές συνθήκες, κ.λπ. έχει επιπτώσεις στον τρόπο και το χρόνο της διάδοσης σημάτων μεταξύ της συσκευής αποστολής σημάτων (πομπού) και του δέκτη. Ομοίως, οι παράμετροι του συστήματος, παραδείγματος χάριν, ύψος κεραιών και κατεύθυνση ακτίνων έχουν φυσικά την επίδρασή τους στην απόσταση της διάδοσης, τον τρόπο, και την καθυστέρηση διάδοσης. Η φύση των ραδιοεπικοινωνιών επιφέρει εγγενώς μερικά ακανθώδη προβλήματα. Τα βασικά προβλήματα που κάθε σύστημα ραδιο επικοινωνίας αντιμετωπίζει είναι σαν τα ακόλουθα:

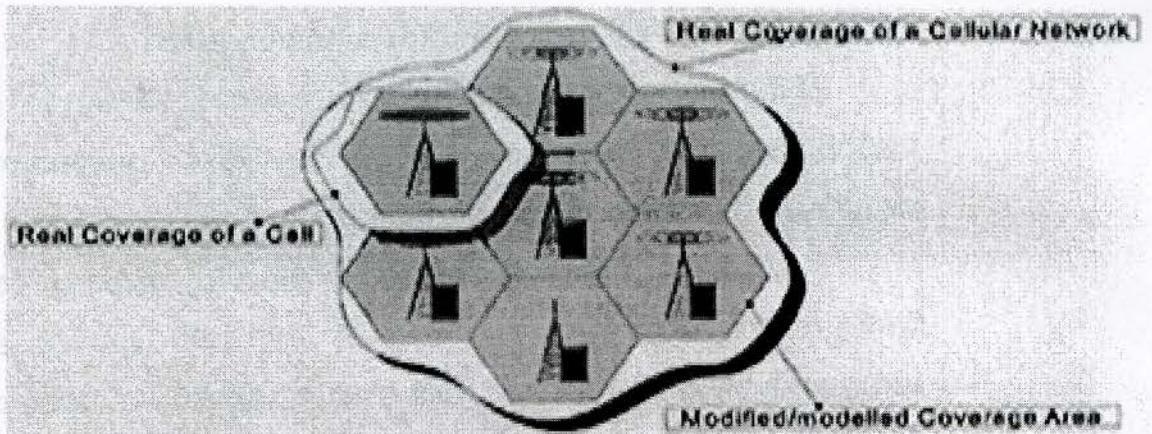
- 1) φαινόμενα διάδοσης πολλαπλών διαδρομών
- 2) φαινόμενα εξασθένισης πολλαπλών διαδρομών
- 3) έλλειψη ραδιοπηγών

3.2 Η κυψελοειδής αρχή ραδιοεπικοινωνιών

Η απλή ραδιοεπικοινωνία είναι ανίκανη να παρέχει την υπηρεσία πρόσβασης σε μεγάλο αριθμό τελικών συνδρομητών, δηλαδή αντιμετωπίζει περιορισμό δυναμικότητας.

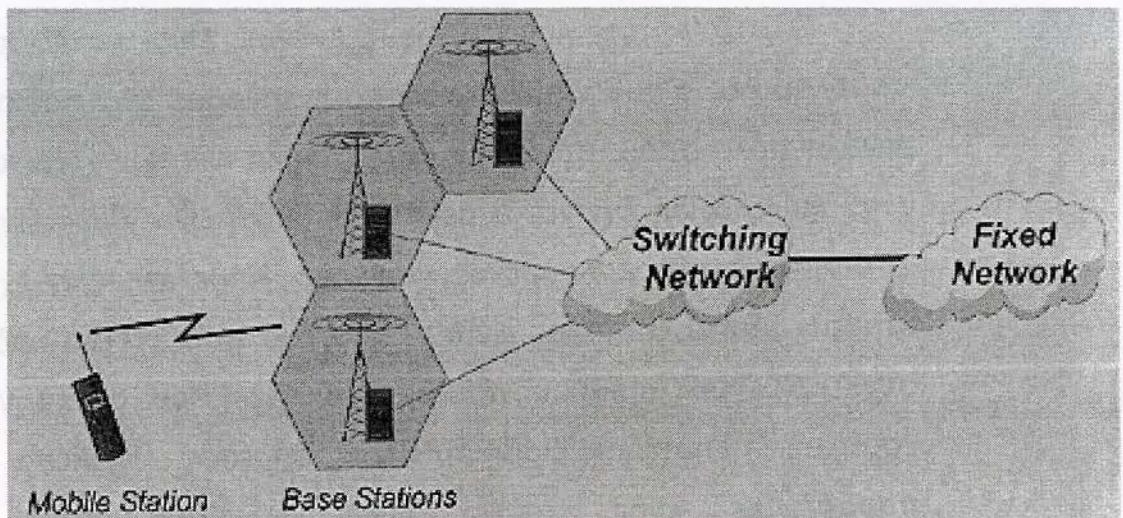
Αρχικά, οι δημόσιες ραδιοεπικοινωνίες πρέπει να προσφέρουν διπλή επικοινωνία για την παροχή της ταυτόχρονης επικοινωνίας 2 τρόπων (duplex). Επομένως, δεν είναι πρακτικό να προσφερθούν τέτοιες υπηρεσίες, για παράδειγμα, ραδιοφωνική μετάδοση πληροφοριών. Εκτός από αυτό, η δύναμη σημάτων στον δέκτη επιδεινώνεται καθώς η απόσταση μεταξύ του αποστολέα και του δέκτη αυξάνεται, με συνέπεια ένα απαράδεκτο QoS (**ποιότητα της υπηρεσίας**) στην περιοχή μακριά από τον αποστολέα σημάτων. Αφετέρου, κάθε αποστολέας σημάτων είναι ικανός να προσφέρει έναν περιορισμένο αριθμό ραδιο συνδέσεων/καναλιών στους τελικούς χρήστες-συνδρομητές που σκοπεύουν να καλέσουν ταυτόχρονα, με συνέπεια τον περιορισμό της δυναμικότητας. Επομένως, το φάσμα πρέπει να χρησιμοποιηθεί πιο αποτελεσματικά για να συναντήσει την απαιτούμενη ραδιο πρόσβαση.

Ο στόχος της κυψελοειδούς έννοιας είναι να εξεταστούν αυτά τα προβλήματα. Υποθέστε ότι προγραμματίζουμε ένα ραδιο δίκτυο για μια μεγάλη πόλη όπου υπάρχουν εκατομμύρια κινητών χρηστών. Βασιζόμενοι στην κυψελοειδή έννοια, η μεγάλη περιοχή είναι διαιρεμένη σε διάφορες υποπεριοχές αποκαλούμενες **κυψέλες**. Κάθε **κυψέλη** έχει τον δικό της σταθμό βάσης, ο οποίος είναι σε θέση να παρέχει μια ραδιο σύνδεση για συγκεκριμένους αριθμούς ταυτόχρονων χρηστών από την εκπομπή ενός χαμηλού – επιπέδου διαβιβασθέντος σήματος. Η εικόνα 3 επεξηγεί ένα παράδειγμα ενός τομέα επτά κυψελών ενός κυψελοειδούς δικτύου.



Εικόνα 3 Μια συλλογή από κυψέλες σε ένα κυψελλοειδές δίκτυο

Η φύση της ραδιοεπικοινωνίας και της κυψελοειδούς έννοιας είναι οι αρχικοί λόγοι γιατί η βασική αρχιτεκτονική των προηγμένων συστημάτων κινητών επικοινωνιών είναι αυτήν την περίοδο αυτή που είναι. Η εικόνα 4 επεξηγεί τη βασική αρχιτεκτονική ενός ραδιοσυστήματος βασισμένου στην κυψελλοειδής έννοια. Όπως εμφανίζεται, η βασική αρχιτεκτονική οποιουδήποτε προηγμένου κυψελοειδούς συστήματος αποτελείται από τους σταθμούς βάσης, ένα δίκτυο μετατροπής, και τη σταθερή λειτουργία δικτύων για την backbone μεταφορά.



Εικόνα 4 Βασική Δομή ενός κυψελλοειδούς συστήματος

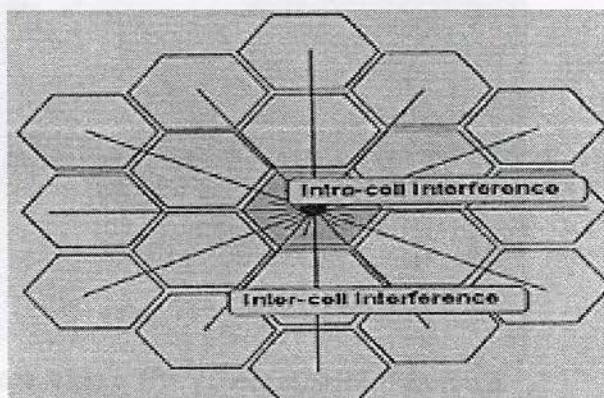
Η λύση της κυψελοειδούς έννοιας επιλύει τα βασικά προβλήματα των ραδιο συστημάτων από την άποψη της δυναμικότητας του ραδιοσυστήματος, αλλά συγχρόνως αντιμετωπίζει άλλα προβλήματα,

όπως:παρέμβαση που οφείλεται στην κυψελοειδή δομή, συμπεριλαμβανομένης της παρέμβασης από τις εσωτερικές και εξωτερικές κυψέλες, προβλήματα που οφείλονται στη κινητικότητα (mobility), έλλειψη ραδιοπηγών που είναι βασισμένες σε κυψέλες.

Ας υποθέσουμε ένα κυψελοειδές σύστημα με ασύγχρονους χρήστες οι οποίοι μοιράζονται το ίδιο ραδιο εύρος ζώνης συχνοτήτων και χρησιμοποιούν τον ίδιο ραδιο σταθμό βάσης σε κάθε περιοχή ή κυψέλη κάλυψης. Κάθε σταθμός βάσης όχι μόνο λαμβάνει την παρέμβαση από τα κινητά μικροτηλέφωνα στη βασική κυψέλη αλλά και από τα τερματικά και τους σταθμούς βάσης που βρίσκονται στις γειτονικές κυψέλες. Επομένως, ανάλογα με την πηγή παρέμβασης, μπορούν να ταξινομηθούν ως intra-cell / co-channel, inter-cell / adjacent cell, και παρέμβαση οφειλόμενη στο θερμικό θόρυβο.

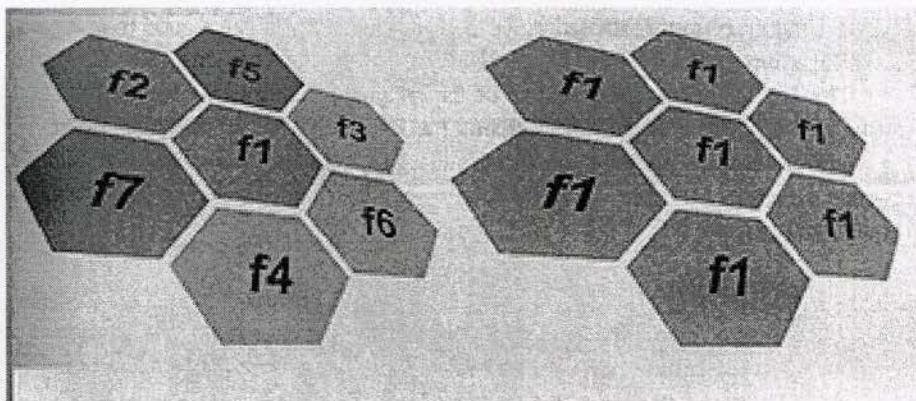
Όπως διευκρινίζεται στην εικόνα 5 προκειμένου να ανταπεξέλθει στη συνολική παρέμβαση που παραλαμβάνεται από τα τερματικά, η παρέμβαση μέσα στη βασική κυψέλη και στις γειτονικές κυψέλες πρέπει να ερευνηθεί.

Από την σκοπιά των κινητών σταθμών, η παρέμβαση των inter-cell προκαλείται από το σήμα των σταθμών βάσης ή των κινητών σταθμών των γειτονικών κυψελών της βασικής κυψέλης όπου ο κινητός σταθμός “στρατοπεδεύει”.



Εικόνα 5 Παρέμβαση INTER-CELL και INTRA-CELL σε ένα κυψελοειδές σύστημα

Σε ένα κυψελοειδές σύστημα, εάν η ίδια συχνότητα χρησιμοποιείται σε κάθε κυψέλη τότε ο κινητός σταθμός, ο οποίος συνδέεται με το ραδιο δίκτυο, αντιμετωπίζει το πρόβλημα της παρέμβασης καναλιών, συμπεριλαμβανομένης της παρέμβασης παρακείμενων (adjacent cell) καναλιών και την παρέμβαση του co-channel. Εκτός από αυτό, το περιβάλλον του δικτύου μπορεί να περιλαμβάνει βουνά, λόφους, και άλλα εμπόδια, προκαλώντας προβλήματα πολλαπλών διαδρομών και απώλειες διαδρομών. Αυτό λύνεται κυρίως με τη χρησιμοποίηση της **τεχνικής επαναχρησιμοποίησης συχνότητας**, δηλ. σε κάθε κυψέλη του προτύπου τομέων (cluster) χρησιμοποιείται μια διαφορετική συχνότητα. Έτσι, ο παράγοντας επαναχρησιμοποίησης συχνότητας είναι μια ουσιαστική παράμετρος για το προγραμματισμό ραδιο δικτύων σε οποιοδήποτε κυψελοειδές σύστημα, το οποίο λειτουργεί βασιζόμενο στις κοινόχρηστες αρχές της συχνότητας. Με τη βελτιστοποίηση του παράγοντα επαναχρησιμοποίησης συχνότητας τα προβλήματα – κίνδυνοι του (adjacent cell) παρακείμενου καναλιού και του co-channel μπορούν να μειωθούν αρκετά, με συνέπεια την αύξηση της δυναμικότητας, η οποία είναι κρίσιμη για τα δημόσια ραδιο συστήματα. Η εικόνα 6 εμφανίζει ένα παράδειγμα των προτύπων μιαςς-επτά (one-seven) και μιαςς-μιας (one-one) επαναχρησιμοποίησης συχνότητας, αντίστοιχα.



Εικόνα 6 FREQUENCY RE – USE PATTERN, FR=7 AND FR = 1

Η κυψελοειδής έννοια αυξάνει τη δυναμικότητα του ραδιο συστήματος ειδικά όταν χρησιμοποιούμε την επαναχρησιμοποίηση

συχνότητας. Όσο μικρότερες είναι οι κυψέλες, τόσο αποτελεσματικότερα χρησιμοποιείται το ραδιο φάσμα αλλά το κόστος του συστήματος αυξάνει συγχρόνως επειδή χρειάζονται περισσότεροι σταθμοί βάσης.

Η σχεδίαση ενός πολυστρωματικού δικτύου, που περιλαμβάνει macro-, micro- και pico- κυψέλες είναι ένα επόμενο βήμα για την παροχή λύσεων σχεδιασμού ενός προηγμένου συστήματος σε συνεργασία με την εννοια της επαναχρησιμοποίησης της συχνότητας για να αναπτυχθεί η δυναμικότητα του συστήματος. Είναι δουλειά του προγραμματισμού δικτύου να βελτιστοποιήσει τον συνδυασμό της δομής του δικτύου και της επαναχρησιμοποίησης της συχνότητας για να αυξήσει την δυναμικότητα του συστήματος αποτελεσματικά με βάση το κόστος, αποφεύγοντας την ανεπιθύμητη αύξηση στον αριθμό των απαιτούμενων σταθμών βάσης. Αυτές οι λύσεις, εντούτοις, θέτουν νέες απαιτήσεις για το σύστημα για να αντιμετωπιστεί η κινητικότητα των κινητών τηλεπικοινωνιών και η επιθυμητή απόδοση του συστήματος από την άποψη της ποιότητας των υπηρεσιών και του σήματος του φορτίου.

Αν και, η κινητικότητα (mobility) δίνει τη δυνατότητα του να είναι εφικτή οπουδήποτε και οποτεδήποτε για το τελικό συνδρομητή, εντούτοις, θέτει ακριβείς απαιτήσεις για το κυψελλοειδές σύστημα για να υποστηρίξει ένα τέτοιο χαρακτηριστικό γνώρισμα. Η διαχείριση της κινητικότητας του κινητού τερματικού είναι ένα από τα πιο ουσιαστικά μέρη οποιασδήποτε λειτουργίας του κυψελοειδούς συστήματος. Γενικά, σε ένα σύστημα ραδιοεπικοινωνίας, η σελιδοποίηση (paging), η ενημέρωση θέσης, και οι διαδικασίες παράδοσης παρέχουν την κινητικότητα χρηστών. Ο μηχανισμός παράδοσης εγγυάται ότι όποτε το κινητό τερματικό μετακινείται από την μια περιοχή/κυψέλη του σταθμού βάσης σε άλλη, το ραδιο σήμα παραδίδεται στο στόχο-σταθμό βάσης. Επιπλέον, η αναπροσαρμογή θέσης και οι μηχανισμοί σελιδοποίησης εγγυώνται ότι ο κινητός σταθμός μπορεί να αναγνωριστεί - πιαστεί ακόμα κι αν δεν υπάρχει καμία συνεχής ενεργή ραδιο σύνδεση μεταξύ του κινητού και του αντίστοιχου σταθμού

βάσης. Το δίκτυο αρχίζει πάντα το μηχανισμό σελιδοποίησης και ο κινητός σταθμός μονογράφει τη διαδικασία αναπροσαρμογών θέσης.

3.3 Τεχνικές πολλαπλής πρόσβασης

Η κυψελοειδής έννοια ελέγχει τον περιορισμό της δυναμικότητας από την άποψη της κάλυψης του συστήματος. Επομένως, δεν βοηθά μόνη τα όρια της δυναμικότητας σε κάθε κυψέλη όσο οι ταυτόχρονοι χρήστες είναι σε αμφισβήτηση (in question). Από τη σκοπιά του ραδιο φάσματος, είναι εξαιρετικά σημαντικό πώς οι ραδιοπηγές δεσμεύονται στους ταυτόχρονους χρήστες. Ο έλεγχος των ραδιο πηγών έχει γίνει ένας από τα πιο σημαντικά χαρακτηριστικά οποιουδήποτε ραδιοσυστήματος επικοινωνίας, ο οποίος παρέχει υπηρεσίες στον τεράστιο αριθμό υπηρεσιών που απαιτούνται.

Οι τεχνικές πολλαπλών προσβάσεων έχουν αναπτυχθεί για να καταπολεμήσουν το πρόβλημα της ταυτόχρονης ραδιο κατανομής πρόσβασης στους αιτούντες για πρόσβαση χρήστες. Η βασική πτυχή οποιουδήποτε πολλαπλάσιου σχεδίου πρόσβασης είναι πώς η διαθέσιμη περιοχή συχνότητας δεσμεύεται. Τα αρχικά προβλήματα που αντιμετωπίζονται από τις λύσεις πολλαπλών προσβάσεων είναι σχετικά με τα εγγενή χαρακτηριστικά των ραδιο συστημάτων: Περιορισμός εύρους ζώνης συχνοτήτων, εξασθένηση πολλαπλών διαδρομών της ραδιο σύνδεσης και παρεμβολή από άλλους χρήστες στο κυψελοειδές περιβάλλον όπου η κυψελοειδής έννοια και η επαναχρησιμοποίηση της συχνότητας έχει χρησιμοποιηθεί. Το βασικό ζήτημα για την αποτελεσματική χρήση της συχνότητας είναι η πολλαπλή πρόσβαση. Δηλαδή, πρέπει να υπάρχουν τόσοι πολλοί χρήστες όσο είναι δυνατόν, οι οποίοι να χρησιμοποιούν την επιδιορθωμένη πηγή, σε αυτήν την περίπτωση, την συχνότητα.

Η μέθοδος πολλαπλής πρόσβασης χρησιμοποιείται στα αναλογικά κυψελοειδή δίκτυα και ονομάζεται FDMA (πολλαπλάσια

πρόσβαση τμήματος συχνότητας) όπου κάθε χρήστης χρησιμοποιεί την δικιά του συχνότητα (ή ζευγάρι των συχνοτήτων).

Στην περίπτωση της FDMA, η κατοχή της προσωπικής συχνότητας ή του εύρους ζώνης συχνοτήτων προσδιορίζει το ραδιο κανάλι. Κατά την εξέταση του αριθμού των ραδιο συνδέσεων, αυτό σημαίνει **μια συχνότητα = ένας χρήστης = ένα κανάλι**. Αυτή η τεχνική πολλαπλής πρόσβασης, εντούτοις, δεν είναι ένας αποδοτικός τρόπος για να διαμοιραστούν οι περιορισμένες ραδιοπηγές σε ένα δημόσιο σύστημα κινητών επικοινωνιών. Επομένως, ένας αποτελεσματικότερος τρόπος να χρησιμοποιηθούν οι πηγές συχνότητας που επιτρέπει σε μια αύξηση στη δυναμικότητα του συστήματος, ονομάζεται **TDMA (χρονικό τμήμα πολλαπλής πρόσβασης)** το οποίο αναπτύχθηκε κατά την πρόωρη φάση των συστημάτων κινητής ραδιοεπικοινωνίας. Το TDMA είναι η πιο κοινή μέθοδος πολλαπλής προσπέλασης που χρησιμοποιείται στα κυψελοειδή συστήματα δεύτερης γενιάς όπως στο GSM. Επίσης, τα συστήματα μεταφορών τα οποία βασίζονται στο TDMA χρησιμοποιούνται ευρέως. Ίσως το πιο γνωστό σύστημα είναι η προδιαγραφή του G.703 το οποίο βασίζεται στο PCM (διαμόρφωση κώδικα σήματος).

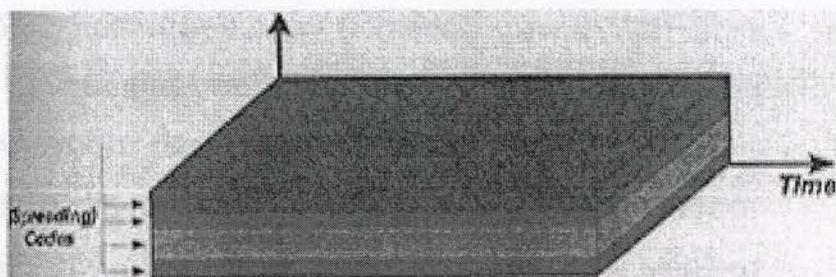
Στο GSM σύστημα Um interface οι χρήστες μιας δεδομένης συχνότητας τη διαιρούν με βάση τον χρόνο: κάθε χρήστης έχει μια μικρή φέτα του χρόνου (timeslot) για διαφορετικές διαδικασίες. Αυτό το timeslot επαναλαμβάνεται συχνά και αυτό δημιουργεί μια εντύπωση συνεχούς σύνδεσης. Αυτό το σύστημα το καθιστά πιθανό να έχει πολλούς χρήστες – τόσους πολλούς όσοι είναι και οι αριθμοί timeslots, τα οποία είναι οκτώ για το GSM – και χρησιμοποιούν ταυτόχρονα την ίδια συχνότητα

Ο κώδικας τμηματοποίησης της πολλαπλής πρόσβασης (CDMA) είναι μια άλλη τεχνική πολλαπλής πρόσβασης που έχει χρησιμοποιηθεί για παρόμοιους σκοπούς όπως για το FDMA και για το TDMA. Εντούτοις, αυτό προσπελαύνει το ίδιο πρόβλημα από τη χρησιμοποίηση μιας συνολικά διαφορετικής στρατηγικής. Καθώς μια

διάδοση - φάσματος βασισμένη στο σχέδιο ραδιο πρόσβασης, το CDMA είναι ένα από τα περιπλοκότερα, η οποία έχει χρησιμοποιηθεί σε διαφορετικές εφαρμογές. Αντίθετα από τα TDMA και τα FDMA, οι ραδιοπηγές δεσμεύονται βασισμένες στους κώδικες του σχεδίου CDMA. Κατά συνέπεια όλοι οι ταυτόχρονοι χρήστες μπορούν να απασχολήσουν το ίδιο εύρος ζώνης συχνοτήτων συγχρόνως. Σε κάθε χρήστη ανατίθεται ένας κώδικας/οι κώδικες που ποικίλλουν ανά συναλλαγή και εκείνοι οι κώδικες χρησιμοποιούνται για τη κυψέλη, το κανάλι και το διαχωρισμό των χρηστών. Κάθε χρήστης χρησιμοποιεί την ίδια περιοχή συχνότητας ταυτόχρονα και ως εκ τούτου δεν υπάρχει καμία "χρονική αυλάκωση" ή κατανομή συχνότητας όπως στα TDMA και FDMA σύστημα, αντίστοιχα.

1) Αν το δημιουργημένο ποσοστό δυαδικών ψηφίων είναι χαμηλό, μπορεί να διαδοθεί καλά και έτσι η ισχύς που απαιτείται για την μεταφορά θα είναι μικρή. Αυτό το είδος περίπτωσης μπορεί να φανεί ως λεπτό στρώμα στον εικόνα 7.

2) Αν το δημιουργημένο ποσοστό δυαδικών ψηφίων είναι υψηλό αυτό μπορεί να διαδοθεί επίσης και έτσι η ισχύς που απαιτείται για την μεταφορά θα είναι υψηλότερη. Αυτό το είδος περίπτωσης μπορεί να φανεί ως παχύ στρώμα στην εικόνα 7.



Εικόνα 7 CDMA (CODE DIVISION MULTIPLE ACCESS)

Αντίθετα από το εύρος ζώνης συχνοτήτων - περιορισμένης πολλαπλής πρόσβασης (FDMA και TDMA) το οποίο υποφέρει κυρίως από την παρέμβαση του co-channel μέσω της υψηλής απόδοσης της

επαναχρησιμοποίησης της συχνότητας, η παρέμβαση του εσωτερικού χρήστη κατά το uplink είναι ο κρισιμότερος τύπος παρέμβασης από την άποψη του δυναμικού μονάδας και του QoS στο σύστημα CDMA. Ο λόγος είναι ότι η παρέμβαση του εσωτερικού χρήστη κατά το uplink αυξάνεται σε μια βάση ισχύος, και η απόδοση κάθε χρήστη γίνεται φτωχότερη καθώς ο αριθμός ταυτόχρονων χρηστών αυξάνεται σε ένα ενιαίο κελί.

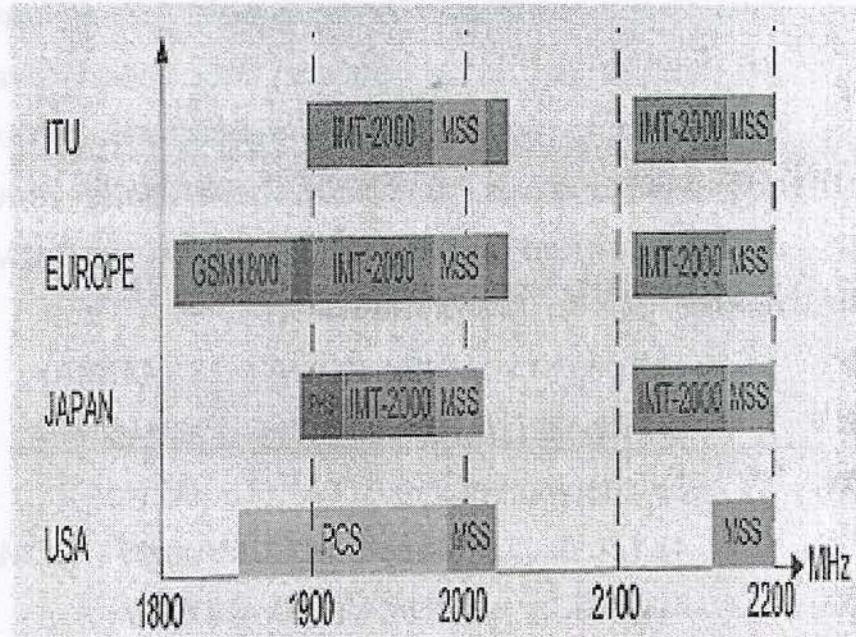
Ανάλογα με το διαδιδόμενο σήμα που χρησιμοποιείται στη διαμόρφωση, το σχέδιο CDMA μπορεί να ταξινομηθεί στις ακόλουθες ομάδες:

- 1) Άμεση ακολουθία CDMA (DS - CDMA)
- 2) Hopping συχνότητας (FH – CDMA)
- 3) Hopping χρόνου CDMA (TH - CDMA)
- 4) Υβριδική διαμόρφωση CDMA (HM - CDMA)
- 5) MultiCarrier CDMA (MC - CDMA)

3.4 Χαρακτηριστικά του ραδιομονοπατιού της 3^{ης} Γενιάς

Η κατανομή του φάσματος της Τρίτης Γενιάς είναι ένα καυτό θέμα για συζήτηση κατά τη διάρκεια των τελευταίων ετών παγκοσμίως. Περιλαμβάνει πολλά σημαντικά θέματα, τα οποία ποικίλλουν πολύ μεταξύ των χωρών και των χειριστών. Αρχικά, το απαιτούμενο δωμάτιο φάσματος για την Τρίτη Γενιά δεν είναι διαθέσιμο με τον ίδιο τρόπο στις διαφορες χώρες. Αυτό οφείλεται βασικά εξαιτίας της μερίδας φάσματος που καταλήφθηκε ήδη από άλλα συστήματα στη χρήση ή τις περιοχές φρουράς που απαιτούνται για τα συστήματα, οι οποίες λειτουργούν στις παρακείμενες περιοχές συχνότητας. Αφετέρου, οι πολιτικές προσπελάσης για τη χορήγηση αδειών φάσματος ποικίλλουν επίσης από χώρα σε χώρα. Φυσικά, οι χειριστές που περιλαμβάνονται στα συστήματα Δεύτερης Γενιάς είναι πρόθυμοι να έχουν την τεχνολογία των ακρών με τη συμμετοχή στην εργασία ανάπτυξης της Τρίτης Γενιάς. Επομένως, οι απαιτήσεις του περιβάλλοντος κανονικοποίησης του φάσματος της Τρίτης

Γεννιάς κλείνουν τη διεθνή και εθνική συνεργασία προκειμένου να εναρμονιστεί η κατανομή φάσματος παγκοσμίως και να την διαχειριστούν αποτελεσματικά μέσα στις χώρες (Εικόνα 8).



Εικόνα 8 To 3G System Spectrum

Από την πλευρά της Τρίτης Γεννιάς, έχει αποφασιστεί (στα μέσα του 1999 απ ο την ΟΗΓ) ότι θα υπάρξουν **τρεις παραλλαγές CDMA** σε χρήση. Αυτοί είναι:

DS - WCDMA - FDD: Άμεση ακολουθία - Ευρείας ζώνης Διαχωρισμού Κώδικα Πολλαπλής πρόσβασης – Διπλός Διαχωρισμός Συχνότητας

DS - WCDMA - TDD: Άμεση ακολουθία - Ευρείας ζώνης Διαχωρισμού Κώδικα Πολλαπλής πρόσβασης – Διπλός Διαχωρισμός Χρόνου

MC - CDMA: Πολυ μεταφορέας - Διαχωρισμός Κώδικα Πολλαπλής πρόσβασης.

Σε αυτούς τους όρους, το πρώτο μέρος περιγράφει την μέθοδο διάδοσης πληροφοριών μέσω του φάσματος συχνότητας, το δεύτερο μέρος δείχνει το σχέδιο πολλαπλής πρόσβασης και το τελευταίο μέρος εκφράζει πώς οι διαφορετικές κατευθύνσεις μεταφορών (uplink και downlink) είναι χωρισμένες.

Οι βασικές έννοιες

Στο WCDMA, το ρεύμα στοιχείων (data stream) του αποστολέα σημάτων του σταθμού βάσης χειρίζεται τα στοιχεία στην κατεύθυνση downlink συνδέσεων που αντιπροσωπεύει την κυκλοφορία από το δίκτυο στο τερματικό. Αυτή η κυκλοφορία χρησιμοποιεί διάφορα κανάλια στο Uu interface. Στο Uu interface το αποτελεσματικό εύρος ζώνης συχνοτήτων για το WCDMA είναι 3,84 MHz και με τις περιοχές φρουράς το απαιτούμενο εύρος ζώνης συχνοτήτων είναι 5 MHz.

Προκειμένου να αποκτηθεί μια καλύτερη κατανόηση του θέματος, θα συζητήσουμε εν συντομία τη θεωρία πληροφοριών (Information Theory).

Η Information Theory είναι ένα μαθηματικό μοντέλο που εξηγεί τις αρχές της μεταφοράς σημάτων. Αυτή η θεωρία δεν κάνει οποιαδήποτε διαφορά μεταξύ των διαφορετικών τεχνολογιών που περιλαμβάνονται επειδή τα βασικά μαθηματικά είναι πάντα τα ίδια. Σε αυτό το πλαίσιο, υπάρχουν διάφορες απλουστευμένες αρχές, οι οποίες μπορούν να εξαχθούν από τη Information Theory:

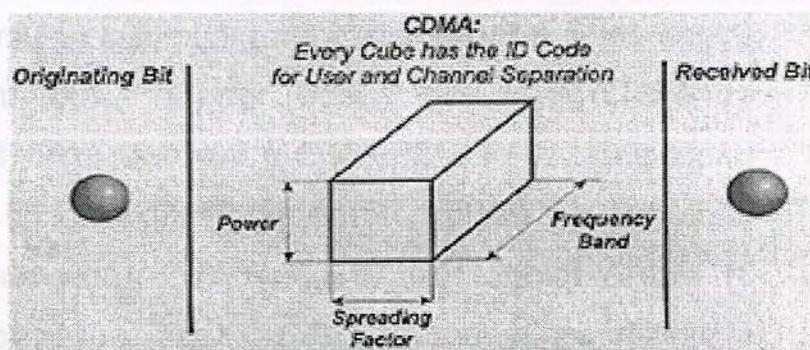
- 1) οι πληροφορίες που μεταφέρονται παρουσιάζουν ορισμένη ισχύ, ονομαζόμενη P_{inf}
- 2) όσο ευρύτερη η περιοχή για τη μεταφορά πληροφοριών, τόσο μικρότερη είναι η ισχύς που προέρχεται-παρουσιάζει τις μεταφερόμενες πληροφορίες σε ένα αφιερωμένο (μικρό) σημείο μέσα στην περιοχή μεταφοράς πληροφοριών. Με άλλα λόγια, η συνολική ισχύς P_{inf} είναι ένα ολοκλήρωμα πέρα από την περιοχή μεταφοράς πληροφοριών σε αυτήν την περίπτωση
- 3) όσο περισσότερες πληροφορίες πρόκειται να μεταφερθούν, τόσο περισσότερη ισχύς απαιτείται. Κατά συνέπεια, όταν αυξάνεται προς στιγμήν η ισχύς η P_{inf} αυξάνεται, επίσης. Σε αυτό το πλαίσιο, όσο υψηλότερο το αρχικό ποσοστό δυαδικών ψηφίων που μεταφέρεται, τόσο περισσότερη ισχύς απαιτείται.

Εάν παίρνουμε αυτό στον απολογισμό και συνδυάζουμε τις πληροφορίες που παρουσιάζονται στην εικόνα 7, είμαστε σε θέση να επεξηγήσουμε πώς το WCDMA μεταχειρίζεται ένα ενιαίο δημιουργμένο κομμάτι των στοιχείων των χρηστών αποκαλούμενο bit.

Στο air interface του WCDMA, κάθε δημιουργημένο δυαδικό ψηφίο(bit) πληροφοριών είναι όπως ένα "κιβώτιο" το οποίο έχει σταθερή τιμή αλλά οι μεταβολές του "κιβώτιου" αλλάζουν ανάλογα με την περίπτωση. Αναφερόμενοι στην εικόνα 9, το βάθος του "κιβωτίου" (περιοχή συχνότητας) είναι σταθερό στο WCDMA. Οι άλλες δύο διαστάσεις, η ισχύς και ο διαδίδομενος παράγοντας εξαρτώνται από την αλλαγή. Βασισμένα σε αυτό τα ακόλουθα συμπεράσματα μπορούν να γίνουν:

1) όσο καλύτερα μπορεί να διαδοθεί το σήμα, τόσο μικρότερη είναι η απαιτούμενη ενέργεια ανά δυαδικό ψηφίο (ισχύς). Αυτό μπορεί να εφαρμοστεί εάν το δημιουργμένο ποσοστό δυαδικών ψηφίων είναι χαμηλό. Με άλλα λόγια, ο διαδίδομενος παράγοντας αυξάνει και η ισχύς μειώνεται.

2)όσο μικρότερος είναι ο διαδίδομενος παράγοντας, τόσο περισσότερη ενέργεια απαιτείται ανά δυαδικό ψηφίο (ισχύς). Αυτό εφαρμόζεται όταν το δημιουργημένο ποσοστό δυαδικών ψηφίων είναι υψηλό. Με άλλα λόγια, ο διαδίδομενος παράγοντας αυξάνεται και η ισχύς μειώνεται.



Εικόνα 9 WCDMA AIR INTERFACE AND BIT TREATMENT

Ένα περίπλοκο ζήτημα με το WCDMA είναι ότι ένα "bit" δεν είναι ένα "bit" σε όλες τις περιπτώσεις. Ο όρος - bit - αναφέρεται στο bit

πληροφοριών, το οποίο είναι ένα bit που εμφανίζεται στην αρχική ροή στοιχείων των χρηστών. Το δυαδικό ψηφίο που αναφέρεται στον κώδικα που χρησιμοποιείται για τη διάδοση καλείται chip. Βασισμένοι σε αυτόν τον καθορισμό, είμαστε σε θέση να παρουσιάσουμε μερικά βασικά αναγκαία θέματα που χρειάζονται στο WCDMA.

Το bit rate του κώδικα που χρησιμοποιείται για την αρχική διάδοση σημάτων είναι, όπως καθορίζεται, 3,84. Mb/s. Αυτή η αξία είναι σταθερή για όλες τις παραλλαγές WCDMA που χρησιμοποιούνται στα δίκτυα 3^{ης} Γενιάς. Αυτό καλείται ως System Chip Rate και εκφράζεται ως 3,84. Mcps (μεγα chips ανα sec). Με αυτό το System Chip Rate το μέγεθος του ενός chip είναι

$$1/3\ 840.000 = 0.00000026041s.$$

Πως μπορούμε να κάνουμε το επιθυμητό σήμα να πιαστεί από την πλευρά του αποδέκτη; Κάθε χρήστης χρησιμοποιεί μοναδικό κώδικα για να πάρει το επιθυμητό σήμα. Το λαμβανόμενο σήμα πολλαπλασιάζεται από τον συγκεκριμένο κώδικα του αποδέκτη σαν αποτέλεσμα των πολλαπλασιαζόμενων πληροφοριών. Αν ο σωστός κώδικας και το επιθυμητό σήμα που λάβαμε είναι πολλαπλασιασμένα, το αποτέλεσμα θα είναι τα δεδομένα που έχουν αναβαθμιστεί με τις καθαρές peaks πάνω στο σήμα, διαφορετικά αυτά τα δεδομένα δεν θα περιλαμβάνουν τις καθαρές peaks πάνω στο σήμα για να προχωρήσουν πιο πέρα. Ο συντελεστής εξάπλωσης είναι ένας πολλαπλασιαστής που περιγράφει τον αριθμό πολλών chips χρησιμοποιείται στο ραδιο μονοπάτι WCDMA για 1 symbol.

$$K = 2^k, \text{ όπου } k = 0,1,2,3,\dots,8$$

Παράδειγμα για $k=6$ $K=64$, δηλαδή 1 symbol χρησιμοποιεί 64 chips στο WCDMA στην uplink κατεύθυνση (ανάλογα με τους πίνακες 3,1 και 3,2).

ντί για συντελεστή εξάπλωσης το ονομάζουμε και processing gain(G_p) και μπορεί να εκφραστεί ως:

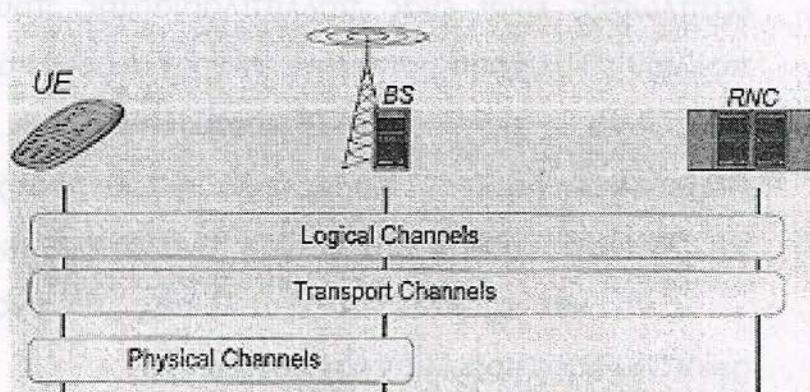
$G_p = B_{Uu} / B_{Bearer} = \text{System chip rate} / \text{Bearer bit rate} = \text{Spreading factor}$

B_{Uu} = Bandwidth του Uu interface

B_{Bearer} = Bandwidth του rate – matched baseband data(rate – matched baseband data (λαμβάνει ήδη πολύ σημαντικές πληροφορίες όπως η κωδικοποίηση του καναλιού και πληροφορίες προστασίας από λάθη).

3.4.1 Κανάλια WCDMA

Η ραδιο πρόσβαση WCDMA δεσμεύει το εύρος ζώνης συχνοτήτων για τους χρήστες και το δεσμευμένο εύρος ζώνης συχνοτήτων και οι ελέγχομενες λειτουργίες του αντιμετωπίζονται με τον όρο "κανάλι". Η λειτουργία που εφαρμόζεται μέσω του WCDMA καθορίζει ποια είδη καναλιών απαιτούνται και πώς οργανώνονται. Η οργάνωση καναλιών που χρησιμοποιεί το WCDMA είναι τριών επιπέδων. Υπάρχουν **λογικά κανάλια**, **κανάλια μεταφοράς** και **φυσικά κανάλια**. Από αυτά, τα λογικά κανάλια περιγράφουν τους τύπους πληροφοριών που μεταδίδονται, τα κανάλια μεταφορών περιγράφουν πώς τα λογικά κανάλια πρόκειται να μεταφερθούν και τα φυσικά κανάλια είναι τα "μέσα μετάδοσης" παρέχοντας τη ραδιο πλατφόρμα μέσω της οποίας οι πληροφορίες μεταφέρονται πραγματικά (Εικόνα 10).



Εικόνα 10 Τύποι καναλιών και η θέση τους στο UTRAN

Σχετικά με τα λογικά κανάλια, το UE και το δίκτυο έχουν διαφορετικές στοιχειώδεις εργασίες να κάνουν. Κατά συνέπεια, οι λογικές, οι μεταφερόμενες και φυσικές δομές καναλιών είναι λίγο διαφορετικές σε καθεμία κατεύθυνση. Κατά προσέγγιση, το δίκτυο έχει τις ακόλουθες στοιχειώδεις εργασίες να εκτελέσει:

- το δίκτυο πρέπει να ενημερώσει το UE για το ραδιο περιβάλλον. Αυτές οι πληροφορίες αποτελούνται από, παραδείγματος χάριν, την τιμή ή τις τιμές του κώδικα που χρησιμοποιείται στο κελί(κυψέλη) και στις γειτονικές κυψέλες, που επιτρέπονται τα επίπεδα ισχύος, κ.λ.π. Αυτό το είδος πληροφοριών το δίκτυο εξασφαλίζει για το UE μέσω του λογικού καναλιού αποκαλούμενου **κανάλι ελέγχου ραδιοφωνικής μετάδοσης Broadcast Control Channel (BCCH)**.

- όταν υπάρχει μια ανάγκη να επιτευχθεί το UE για την επικοινωνία (παραδείγματος χάριν, μια κινητή ολοκληρωμένη κλήση) το UE πρέπει να σελιδοποιηθεί προκειμένου να βρεθεί η ακριβής θέση του. Αυτό το αίτημα δικτύων παραδίδεται στο λογικό κανάλι αποκαλούμενο **κανάλι ελέγχου σελιδοποίησης Paging Control Channel (PCCH)**.

- το δίκτυο μπορεί να έχει ορισμένες στοιχειώδεις εργασίες να κάνει, οι οποίες είναι ή μπορεί να είναι κοινές για όλο το UE το οποίο είναι εγκατεστημένο στο κελί. Για αυτόν το λόγο το δίκτυο χρησιμοποιεί το λογικό κανάλι αποκαλούμενο **κοινό κανάλι ελέγχου Common Control Channel (CCCH)**. Δεδομένου ότι μπορεί να υπάρξουν πολυάριθμα UE που χρησιμοποιούν το CCCH ταυτόχρονα, το UE πρέπει να χρησιμοποιήσει το U-RNTI (ραδιο προσωρινή ταυτότητα δικτύων UTRAN) για τους σκοπούς προσδιορισμού. Με την έρευνα του λαμβανόμενου U-RNTI η UTRAN μπορεί να περάσει τα λαμβανόμενα μηνύματα στις σωστές υπηρεσίες RNC. Το U-RNTI συζητείται αργότερα.

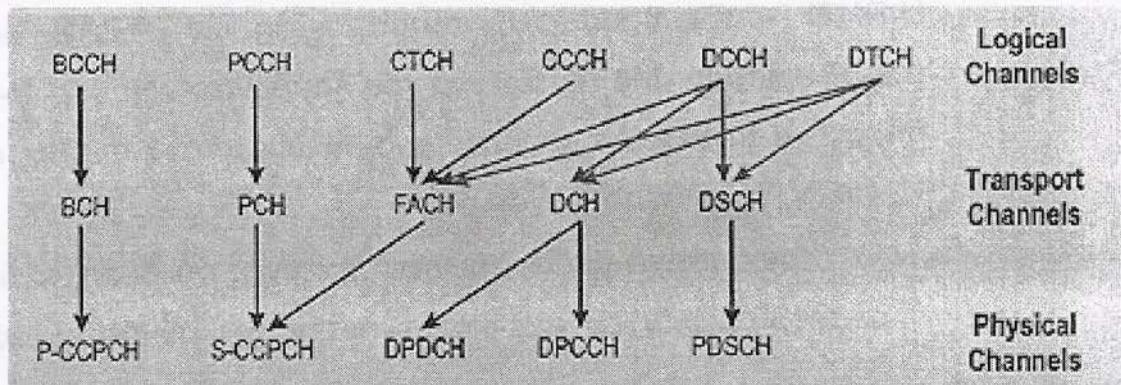
- όταν υπάρχει μια αφιερωμένη, ενεργός σύνδεση, το δίκτυο στέλνει τις πληροφορίες ελέγχου σχετικά με αυτήν την σύνδεση μέσω του λογικού

καναλιού το οποίο καλείται **αφιερωμένο κανάλι ελέγχου Dedicated Control Channel (DCCH)**.

- αφιερωμένη κυκλοφορία: η αφιερωμένη κυκλοφορία χρηστών για την υπηρεσία ενός χρήστη στην downlink κατεύθυνση στέλνεται μέσω του λογικού αφιερωμένου καναλιού το οποίο καλείται **αφιερωμένο κανάλι κυκλοφορίας Dedicated Traffic Channel (DTCH)**.

- το **κοινό κανάλι κυκλοφορίας Common Traffic Channel (CTCH)** είναι ένα ομοιοκατευθυνόμενο κανάλι που υπάρχει μόνο στην κατεύθυνση downlink και χρησιμοποιείται κατά τη διαβίβαση των πληροφοριών είτε σε όλα τα UE ή σε μια συγκεκριμένη ομάδα UE μέσα στο κελί.

Τα κανάλια μεταφοράς που εμφανίζονται στην εικόνα 11 εκτός από ένα είναι όλα υποχρεωτικά. Τα **υποχρεωτικά κανάλια μεταφοράς** είναι το κανάλι ραδιοφωνικής μετάδοσης Broadcast Channel (BCH), το κανάλι σελιδοποίησης Paging Channel (PCH), το προσωπικό κανάλι πρόσβασης Forward Access Channel (FACH) και το αφιερωμένο κανάλι Dedicated Channel (DCH). Εκτός από αυτά, ο χειριστής μπορεί να διαμορφώσει το UTRAN για να χρησιμοποιήσει την κοινή κατιούσα σύνδεση καναλιού Downlink Shared Channel (DSCH). Σε αυτά τα κανάλια μεταφορών, το **μόνο αφιερωμένο κανάλι μεταφορών** είναι το **DCH**. Τα άλλα είναι κοινά. Σε αυτό το σημείο ο όρος "dedicated" σημαίνει ότι το UTRAN έχει δεσμεύσει το κανάλι που χρησιμοποιείται μεταξύ αυτού και σημαντικών τερματικών. Ο όρος "common" σημαίνει ότι διάφορα τερματικά θα μπορούσαν να χρησιμοποιήσουν το κανάλι ταυτόχρονα.



Εικόνα 11 Τοποθέτηση των λογικών, φυσικών καναλιών και των καναλιών μεταφοράς στην DOWNLINK κατεύθυνση

Το **BCH** φέρει το περιεχόμενο του BCCH, π.χ. τις συγκεκριμένες πληροφορίες UTRA που παραδίδονται στο κελί. Αυτές οι πληροφορίες αποτελούνται από, παραδείγματος χάριν, τους τυχαίους κώδικες πρόσβασης, τις πληροφορίες αυλακώσεων πρόσβασης και τις πληροφορίες για τα γειτονικά κελιά. Το UE πρέπει να είναι σε θέση να αποκωδικοποιήσει το BCH προκειμένου να καταχωρηθεί στο δίκτυο. Το BCH διαβιβάζεται με σχετικά υψηλή ισχύ επειδή κάθε τερματικό στην προοριζόμενη περιοχή κάλυψης κελιών πρέπει να είναι ικανό να το "ακούει".

Το **PCH** χρησιμοποιείται όταν το δίκτυο επιθυμεί να αρχίσει μια σύνδεση με κάποιο UE.

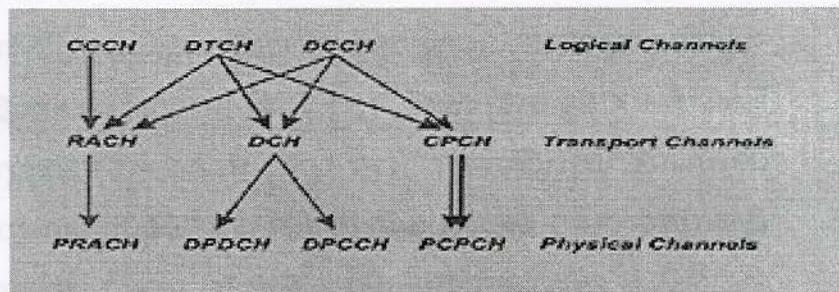
Το **FACH** φέρνει τις πληροφορίες ελέγχου στο UE που είναι γνωστό ότι είναι στο κελί. Για παράδειγμα, όταν το RNC λαμβάνει ένα μήνυμα τυχαίας προσπέλασης από το τερματικό, η απάντηση παραδίδεται μέσω του FACH. Εκτός από αυτό, το FACH μπορεί να κουβαλά κίνηση πακέτων στην downlink κατεύθυνση. Ένα κελί μπορεί να περιέχει πολυάριθμα FACH αλλά ένα από αυτά διαμορφώνεται πάντα με τέτοιο τρόπο (με χαμηλό ποσοστό δυαδικών ψηφίων) έτσι ώστε όλα τα τερματικά που εδρεύουν στην περιοχή κελιών να είναι σε θέση να το λάβουν.

Το **DCH** φέρνει τις αφιερωμένες πληροφορίες κυκλοφορίας και ελέγχου, δηλ. το **DCCH** και **DTCH**. Πρέπει να σημειωθεί ότι ένα DCH μπορεί να φέρει αρκετά DTCH ανάλογα με την περίπτωση. Παραδείγματος χάριν, ένας χρήστης μπορεί να έχει μια ταυτόχρονη κλήση φωνής και την τηλεοπτική κλήση ενεργές. Η κλήση φωνής χρησιμοποιεί ένα λογικό κανάλι DTCH και η τηλεοπτική κλήση απαιτεί ένα άλλο λογικό κανάλι DTCH. Και οι δύο, εντούτοις, χρησιμοποιούν το ίδιο κανάλι DCH.

Από την άποψη δυναμικού μονάδας(capacity) της UTRA, ο στόχος είναι να χρησιμοποιηθούν τα κοινά κανάλια μεταφοράς όσο το δυνατόν περισσότερο, δεδομένου ότι τα αφιερωμένα κανάλια θα καταλάβουν τα

ραδιο κελιά συμπεριφοράς. Το προαιρετικό DSCH είναι ένας στόχος αυξανόμενου ενδιαφέροντος. Φέρει τις αφιερωμένες πληροφορίες χρηστών (DTCH και DCCH) για την κυκλοφορία πακέτων και διάφοροι χρήστες μπορούν να τις μοιραστούν. Από αυτή την άποψη είναι καλύτερο από το DCH, δεδομένου ότι σώζει πηγές που αφορούν το δίκτυο σχετικά με την κίνηση των πακέτων στην **downlink κατεύθυνση**. Ένα άλλο σημείο είναι ότι το μέγιστο ποσοστό δυαδικών ψηφίων (bit rate) για το DSCH μπορεί να αλλάξει γρηγορότερα από ό,τι στο DCH. Η αναμενόμενη ευρεία χρήση των υπηρεσιών παράγει τα περιστασιακά καμένα πακέτα, όπως παραδείγματος χάριν το web surfing, έτσι έχει αυξήσει το ενδιαφέρον για το DSCH.

Στη **uplink κατεύθυνση** το ποσό των λογικών καναλιών που απαιτείται είναι μικρότερο. Υπάρχουν μόνο τρία λογικά κανάλια, τα **CCCH**, **DTCH** και **DCCH** που είναι ίδια όπως στην downlink κατεύθυνση (εικόνα 12).



Εικόνα 12 Τοποθέτηση των λογικών, φυσικών καναλιών και των καναλιών μεταφοράς στην UPLINK κατεύθυνση

Υπάρχουν 3 υποχρεωτικά κανάλια μεταφοράς στη uplink κατεύθυνση που είναι το τυχαίο κανάλι πρόσβασης RACH, DCH και το κοινό κανάλι πακέτων (CPCH).

Το **RACH** φέρνει τις πληροφορίες ελέγχου από το UE στο UTRAN, όπως παραδείγματος χάριν, αίτηση για εγκατάσταση σύνδεσης.

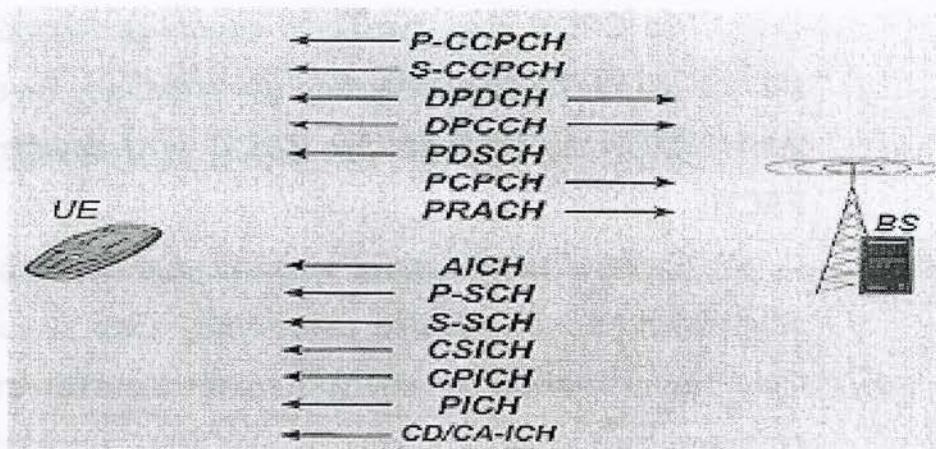
Το **DCH** είναι ίδιο όπως και στην downlink κατεύθυνση, π.χ. η αφιερωμένη μεταφορά καναλιών κουβαλά τις πληροφορίες για τα DCCH και DTCH.

Το **CPCH** είναι ένα κοινό κανάλι μεταφοράς που χρησιμοποιείται για την μεταφορά των στοιχείων των πακέτων. Είναι ένα είδος επέκτασης για το RACH και το αντίστοιχο CPCH στην downlink κατεύθυνση είναι το FACH.

Όταν οι πληροφορίες που συλλέγονται από τα λογικά κανάλια και οργανώνονται στα κανάλια μεταφοράς, είναι έτοιμα για να μεταδοθούν. Πρίν την μεταφορά τα κανάλια τακτοποιούνται στα φυσικά κανάλια. Η επισκόπηση του φυσικού καναλιού WCDMA παρέχεται στην εικόνα 13.

Τα φυσικά κανάλια χρησιμοποιούνται μεταξύ του τερματικού και του σταθμού βάσης. Η φυσική πρόσβαση (δηλ. τα φυσικά κανάλια) είναι χωρισμένη από άλλα στρώματα. Αυτή η ρύθμιση το καθιστά πιθανό να ανταλλάξει το φυσικό ραδιο μέσο πρόσβασης κάτω από τα άλλα στρώματα, στη θεωρία. Στην πράξη η μέση αλλαγή της ραδιο πρόσβασης θα απεικονιστεί στα υψηλότερα στρώματα αλλά αυτή η ρύθμιση ελαχιστοποιεί αυτές τις αλλαγές.

Το **αρχικό κοινό φυσικό κανάλι ελέγχου (P - CCPCH)** φέρει το BCH στην downlink κατεύθυνση. Το P - CCPCH είναι διαθέσιμο με έναν τέτοιο τρόπο έτσι ώστε όλα τα τερματικά που εδρεύουν μέσα στην περιοχή κάλυψης των κελιών είναι σε θέση να αποδιαμορφώσουν το περιεχόμενό τους. Λόγω αυτής της απαίτησης, το P - CCPCH έχει μερικά χαρακτηριστικά, τα οποία είναι πραγματικά περιορισμοί όταν συγκρίνονται με τα άλλα φυσικά κανάλια σε αυτό το σύστημα. Το P - CCPCH χρησιμοποιεί ένα σταθερό κώδικα διοχέτευσης και έτσι ο διαδιδόμενος κώδικας του καθορίζεται, επίσης. Αυτό είναι ανάγκη επειδή διαφορετικά τα τερματικά δεν θα είναι ικανά "να δουν" και να αποδιαμορφώσουν το P - CCPCH. Το bit rate του P - CCPCH είναι 30kb/s με μια διαδιδόμενη τιμή 256. Το bit rate πρέπει να είναι χαμηλό επειδή αυτό το κανάλι διαβιβάζεται με σχετικά υψηλή ισχύ. Εάν χρησιμοποιήσουμε υψηλότερο bit rates, η παρέμβαση αρχίζει να αυξάνει εφόσον περιορίζεται έτσι το δυναμικό(ισχύς)του συστήματος.

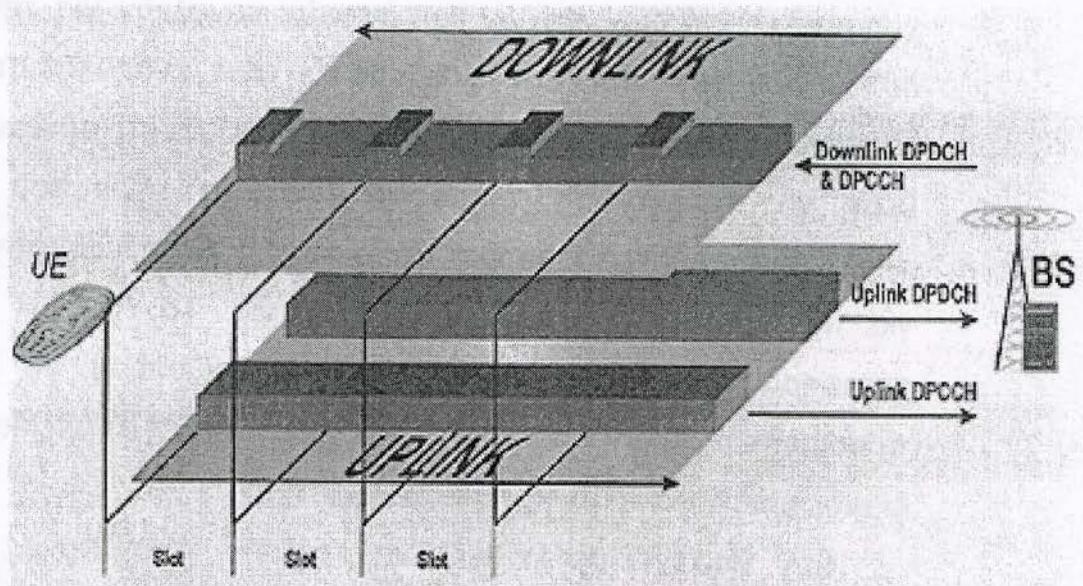


Εικόνα 13 WCDMA Φυσικά Κανάλια

Το δευτεροβάθμιο κοινό φυσικό κανάλι ελέγχου (S - CCPCH) φέρει δύο κανάλια μεταφοράς σε αυτό: Το **Κανάλι σελιδοποίησης (PCH)** και το **προωστικό κανάλι πρόσβασης (FACH)**. Αυτά τα κανάλια μεταφοράς μπορούν να χρησιμοποιήσουν το ίδιο ή διαφορετικό S -CCPCH, κατά συνέπεια ένα κελί περιέχει πάντα τουλάχιστον ένα S-CCPCH. Το bit rate του S - CCPCH είναι σταθερό και σχετικά χαμηλό οφειλόμενο στους ίδιους λόγους σχετικά με το P -CCPCH. Σε μια μετέπειτα φάση το bit rate του S-CCPCH μπορεί να αυξηθεί με την αλλαγή των καθορισμών του συστήματος. Η διαμόρφωση του S -CCPCH είναι μεταβλητή: ανάλογα με την περίπτωση, το S -CCPCH μπορεί να διαμορφωθεί διαφορετικά προκειμένου να βελτιστοποιηθεί η απόδοση του συστήματος. Όσον αφορά στις μεταβλητές εναλλακτικές λύσεις διαμόρφωσης του S -CCPCH, μια εναλλακτική λύση για να αυξηθεί η απόδοση του συστήματος πρέπει να πολλαπλασιάσουμε τις πληροφορίες PCH μαζί με το FACH στο S -CCPCH και οι σχετικές PCH ενδείξεις σελιδοποίησης σε ένα διαφορετικό φυσικό κανάλι το οποίο καλείται **κανάλι δεικτών σελιδοποίησης (PICH)**.

Το **αφιερωμένο φυσικό κανάλι στοιχείων (DPDCH)** φέρει την αφιερωμένη κυκλοφορία χρηστών. Το μέγεθος του DPDCH είναι μεταβλητό και μπορεί να φέρει διάφορες κλήσεις/συνδέσεις μέσα σε αυτό. Όπως το όνομα λέει, είναι ένα αφιερωμένο κανάλι, το οποίο σημαίνει ότι χρησιμοποιείται μεταξύ του δικτύου και του ενός χρήστη. Τα αφιερωμένα

φυσικά κανάλια δεσμεύονται πάντα ως ζευγάρια για τη μια σύνδεση: ένα κανάλι για τη μεταφορά πληροφοριών ελέγχου και άλλο ένα για την πραγματική κυκλοφορία. Το DPCCH μεταφέρει τις πληροφορίες ελέγχου κατά τη διάρκεια της αφιερωμένης σύνδεσης. Η εικόνα 14 εμφανίζει πώς το DPDCH και το DPCCH αντιμετωπίζονται και στην uplink και στην downlink κατεύθυνση.



Εικόνα 14 DPDCH AND DPCCH στην UPLINK και DOWNLINK κατεύθυνση

Στην downlink κατεύθυνση το DPDCH (φέρνοντας στοιχεία χρηστών) και το DPCCH (που φέρνει παραδείγματος χάριν τις πληροφορίες ποσοστού στοιχείων ελέγχου ισχύος) πολλαπλασιάζονται χρονικά. Εάν δεν υπάρχει τίποτα για να φέρει το DPDCH το διαβιβασθέν σήμα είναι παλμικό και προκαλεί τις διαταραχές του τύπου EMC, αυτό δεν είναι ένα πρόβλημα στην downlink κατεύθυνση. Στη uplink κατεύθυνση το DPDCH και το DPCCH, είναι μη παλμικό και δεν υπάρχουν διαταραχές. Η έκβαση της διαμόρφωσης του I/Q στο UE είναι στην πραγματικότητα ένα κανάλι αλλά κουβαλά 2 διακλαδωμένες πληροφορίες (βλ. Εικόνα 14) και οι δύο από τις διακλαδωμένες πληροφορίες καταναλώνουν μια πηγή κώδικα.

Μαζί, το DPCCH και το DPDCH φέρουν το περιεχόμενο του καναλιού μεταφοράς DCH. Όταν η αφιερωμένη σύνδεση χρησιμοποιεί μια

υψηλή αιχμή bit rate το σύστημα αρχίζει εύκολα να υποφέρει από την έλλειψη κωδίκων διοχέτευσης στο κελί. Σε αυτήν την περίπτωση, υπάρχουν 2 δυνατότητες: είτε να προσθέσουν έναν νέο κώδικα scrambling ανακατώματος στο κελί ή να χρησιμοποιήσει κοινά κανάλια για την αφιερωμένη μεταφορά πληροφοριών. Η προσθήκη των κωδίκων ανακατώματος δεν συστήνεται επειδή η ορθότητα χάνεται. Αντ' αυτού, η χρησιμοποίηση των πηγών των κοινών καναλιών για την μεταφορά των δεδομένων των πακέτων φαίνεται να είναι ένας καλύτερος τρόπος να αυξηθεί το δυναμικό μονάδας (ισχύς). Η κατιούσα σύνδεση DCH είναι σε θέση να παρέχει τις πληροφορίες εάν η λήψη του UE πρέπει να αποκωδικοποιήσει το φυσικό κοινό κανάλι κατιούσας σύνδεσης (PD-SCH) για τις πρόσθετες πληροφορίες χρηστών. Το **PD-SCH** φέρει το κανάλι μεταφοράς DSCH και όπως εξηγήθηκε νωρίτερα, το DSCH είναι ένα προαιρετικό χαρακτηριστικό γνώρισμα που ο χειριστής μπορεί να διαμορφώσει για το αν χρησιμοποιηθεί ή όχι.

Εάν υπάρχει μια ανάγκη να σταλούν τα δεδομένα πακέτων σε μια uplink κατεύθυνση και το δυναμικό μονάδας μεταφοράς πακέτων RACH δεν είναι αρκετό, το UE μπορεί να χρησιμοποιήσει το CPCH (uplink κοινό κανάλι πακέτων). Το αντίστοιχο φυσικό κανάλι στη uplink κατεύθυνση είναι το PCPCH (φυσικό (uplink) κοινό κανάλι πακέτων). Το αντίστοιχο του CPCH στην κατεύθυνση κατιουσών συνδέσεων είναι το DPCCCH.

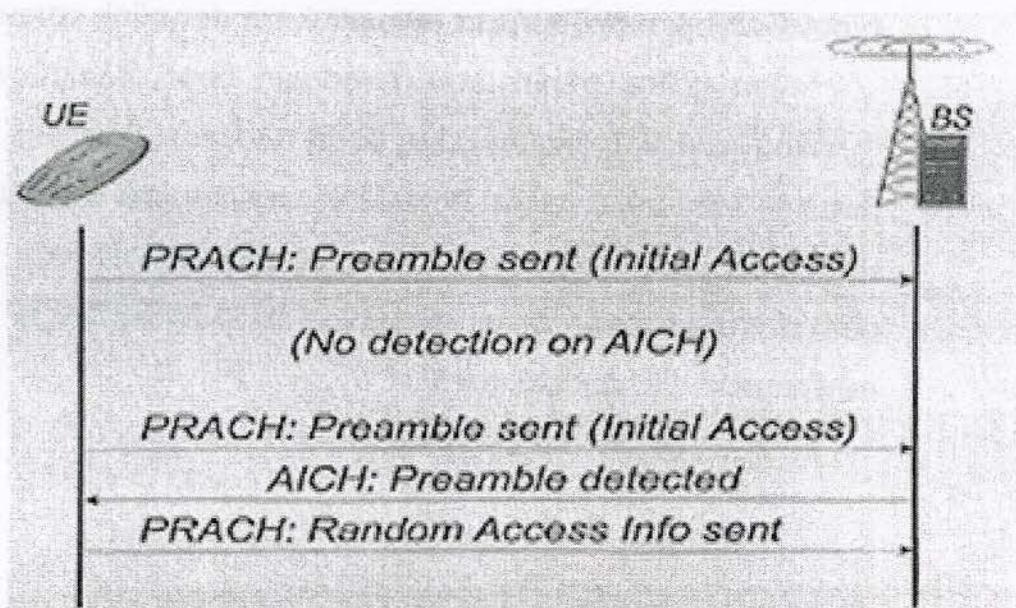
Το **PRACH** φέρει πληροφορίες σχετικές με την τυχαία διαδικασία πρόσβασης (εικόνα 15). Με αυτήν την διαδικασία οι τελικές προσβάσεις στο δίκτυο και επίσης μικρά ποσά δεδομένων μπορούν να μεταφερθούν. Η τυχαία διαδικασία πρόσβασης έχει τις ακόλουθες φάσεις:

1. Το UE αποκωδικοποιεί τις πληροφορίες της BCH για το P - CCPCH και βρίσκει ότι οι αυλακώσεις του RACH είναι διαθέσιμες όπως και ο κώδικας ή οι κώδικες ανακατώματος (scrambling codes).
2. Το UE επιλέγει τυχαία μια αυλάκωση RACH για να χρησιμοποιηθεί.

3. Το UE θέτει το αρχικό επίπεδο ισχύος που χρησιμοποιείται (αυτό είναι βασισμένο στο λαμβανόμενο επίπεδο ισχύος κατιουσών συνδέσεων) και στέλνει τον αποκαλούμενο πρόλογο στο δίκτυο.

4. Το τερματικό αποκωδικοποιεί το AICH (κανάλι ένδειξης αποκτήσεων) για να βρεί εάν το δίκτυο ειδοποίησε το σταλμένο πρόλογο. Εάν δεν ήταν το UE στέλνει τον πρόλογο πάλι αλλά με ένα υψηλότερο επίπεδο ισχύος bit.

5. Όταν το AICH δείχνει ότι το δίκτυο ειδοποίησε τον πρόλογο, το UE στέλνει τις πληροφορίες RACH στο PRACH. Το μήκος των πληροφοριών RACH που στέλνονται είναι είτε ένα είτε δύο πλαίσια WCDMA, χρονικά αυτό παίρνει είτε 10 είτε 20 ms.



Εικόνα 15 Random Accesses

3.4.2 Η Δομή των πλαισίων WCDMA

Για να μπορέσει να χειριστεί η ραδιο πρόσβαση τις ενέργειες ελέγχου όπως το συγχρονισμό, τις ρυθμίσεις συγχρονισμού, τη διαβεβαίωση των μεταφορών, κ.λπ. μεταξύ του δικτύου και του κινητού σταθμού που τα δεδομένα έκρηξης πρέπει να δομηθούν με έναν καθορισμένο με σαφήνεια τρόπο. Επομένως, το WCDMA περιέχει μια δομή πλαισίων, που είναι

διαίρεμένη σε 15 αυλακώσεις, κάθε μια από αυτές έχει μήκος $2/3$ ms και έτσι το μήκος πλαισίων είναι 10 ms.

Βασιζόμενοι σε αυτό, ένα WCDMA πλαίσιο είναι ικανό να χειριστεί

$$0,010 \text{ s} / 0.00000026041 \text{ s} \approx 38400 \text{ Chips}$$

Μια αυλάκωση στο WCDMA πλαίσιο περιέχει:

$$38400 \text{ Chips} / 15 \text{ Slots} = 2560 \text{ Chips.}$$

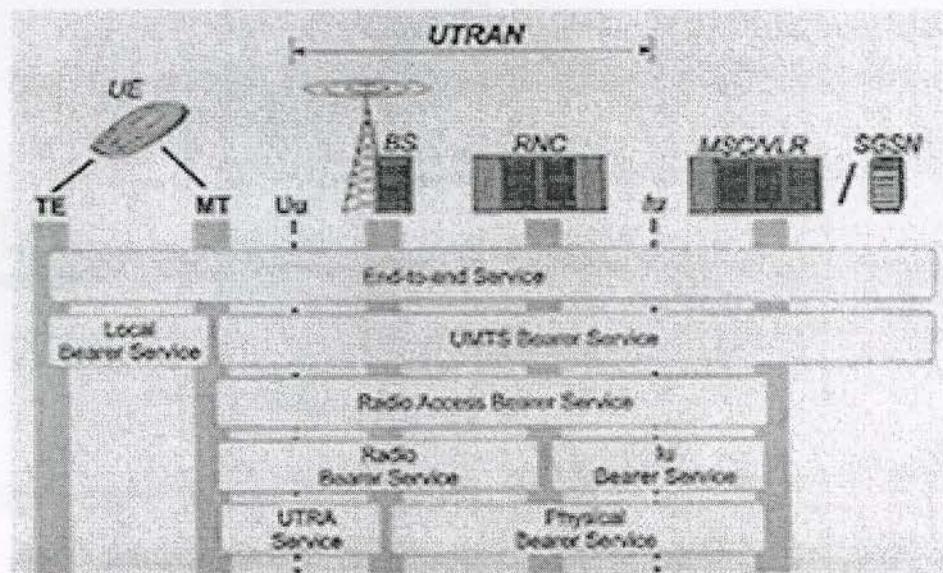
Αντίθετα με το GSM, το WCDMA δεν περιέχει καθόλου super-, hyper-, ή με πολλά πλαίσια δομές. Αντίθετα, τα πλαίσια WCDMA είναι αριθμημένα από τον SFN (Αριθμός πλαισίων του Συστήματος). Ένα SFN χρησιμοποιείται για τον εσωτερικό συγχρονισμό του UTRAN και χρονομετρά τις πληροφορίες μεταφοράς του BCCH. Τα αφιερωμένα φυσικά κανάλια έχουν διαφορετική δομή για την uplink και downlink κατευθυνση.

Στη uplink περίπτωση, η βασική δομή πλαισίων του αφιερωμένου φυσικού καναλιού ακολουθεί τη δομή πλαισίων downlink συνδέσεων, αλλά η βασική διαφορά είναι ότι τα uplink αφιερωμένα κανάλια δεν μπορούν να θεωρηθούν ως χρόνος πολυπλεξίας του DPDCH και του DPCCH. Αυτό οδηγεί στο γεγονός ότι η λειτουργία πολλών κωδικών είναι πιθανή για τα αφιερωμένα UL φυσικά κανάλια.

Κεφάλαιο 4 UMTS RADIO ACCESS NETWORK (UTRAN)

Εισαγωγή

Η βασική ιδέα του UTRAN είναι να δημιουργηθούν και να διατηρηθούν οι ραδιο φορείς πρόσβασης (RAB) για τις επικοινωνίες μεταξύ του εξοπλισμού των χρηστών (UE) και το ασύρματο Δίκτυο (CN). Με το RAB τα στοιχεία του ασύρματου δικτύου δίνουν μια ψευδαίσθηση για ένα σταθερό μονοπάτι επικοινωνίας με το UE, αφού τα απελευθερώνουμε από την ανάγκη να φροντιστούν τις πτυχές της ραδιοεπικοινωνίας. Το UTRAN πραγματοποιεί ορισμένα μέρη της ποιότητας της υπηρεσίας (QoS) ανεξάρτητα της αρχιτεκτονικής (Εικόνα 16).



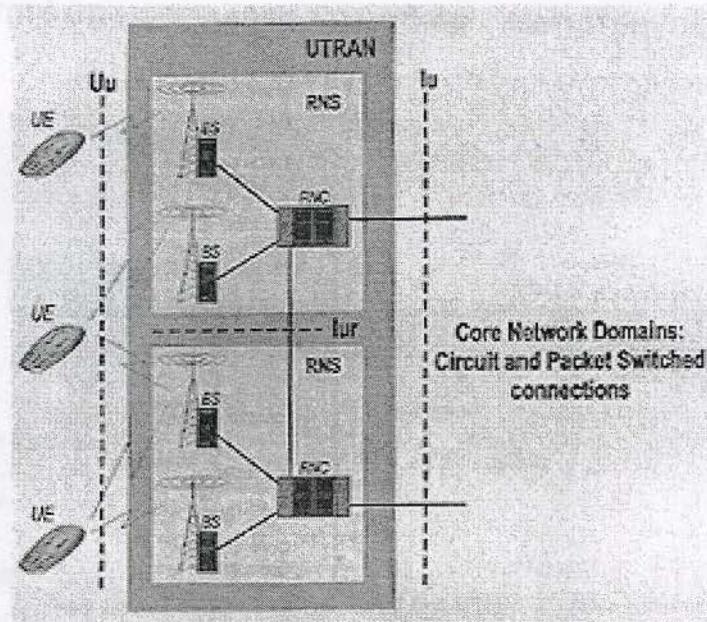
Εικόνα 16 BEARER / QoS αρχιτεκτονική στο UTRAN

Το UTRAN βρίσκεται μεταξύ δύο ανοικτών διαπροσωπειών που είναι το **Uu** και το **Iu**. Από την άποψη αρχιτεκτονικής φορέων, η βασική στοιχειώδης εργασία του UTRAN είναι να παρασχεθεί η υπηρεσία φορέων πέρα από αυτές τις διαπροσωπείες. Από αυτή την άποψη το UTRAN ελέγχει το Uu interface και μέσα στο Iu interface η παροχή υπηρεσίας φορέων γίνεται σε συνεργασία με το ασύρματο δίκτυο.

4.1.Η Αρχιτεκτονική του UTRAN

Η εικόνα 17 παρουσιάζει την αρχιτεκτονική του UTRAN στο επίπεδο στοιχείων του δικτύου. Το UTRAN αποτελείται από τα Ραδιο Υποσυστήματα του Δικτύου (**RNS**) και κάθε RNS περιέχει πολλά σύνολα από σταθμούς Βάσης (**BS**, ή επίσημα Κόμβος B) που καταλαμβάνουν το Uu interface και ένα RNC.

Τα RNS είναι διαχωρισμένα το ένα από το άλλο με το interface UMTS μεταξύ των σύνδέσεων του interface των RNC (Iur) ανάμεσα σε δύο RNC. Το Iur, το οποίο αναγνωρίστηκε σαν ένα ανοικτό interface, κουβαλα και τις πληροφορίες σήματοδότησης και τις πληροφορίες της κίνησης.



Εικόνα 17 UTRAN αρχιτεκτονική

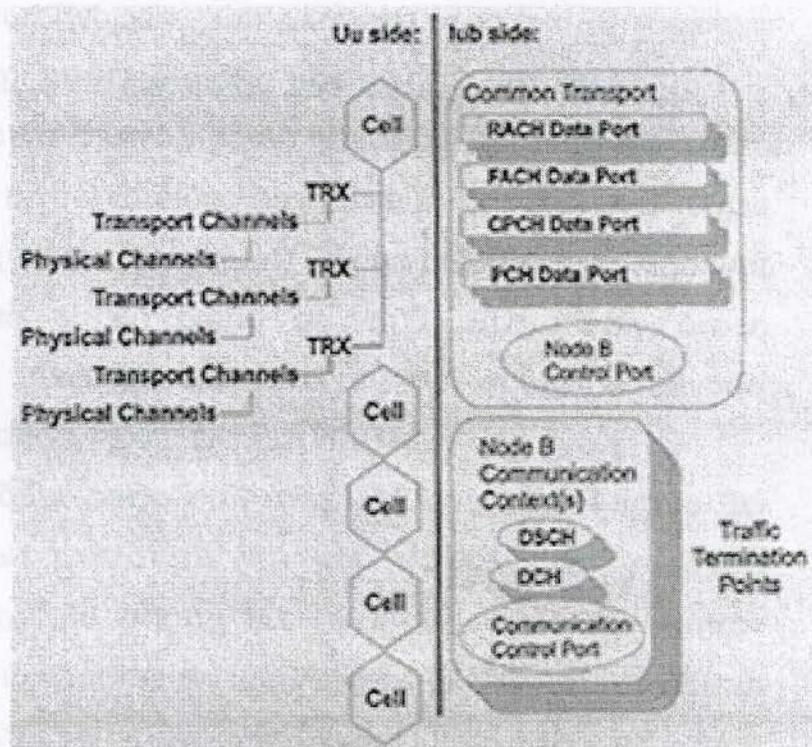
4.2 Ο σταθμός βάσης

Ο σταθμός βάσης (BS) βρίσκεται μεταξύ του Uu και του UMTS interface μεταξύ του RNC και του σταθμού βάσης (Iub) interface. Οι βασικές στοιχειώδεις εργασίες του πρόκειται να καθιερώσουν τη φυσική εφαρμογή του Uu interface και, προς το δίκτυο, είναι η εφαρμογή του Iub interface με τη χρησιμοποίηση των πρωτοκόλλων που ειδικά χρησιμοποιούνται για αυτά τα interfaces. Για να καταλάβουμε το Uu

interface εννοούμε τον Σταθμό Βάσης (BS) που εφαρμόζει τα ραδιοφυσικά κανάλια πρόσβασης WCDMA τα οποία μεταφέρουν τις πληροφορίες από τα κανάλια μεταφοράς στα φυσικά κανάλια που βασίζονται στη ρύθμιση που καθορίζεται από το RNC.

4.2.1 Εσωτερική δομή των Σταθμών Βάσεων (BS)

Από την άποψη του δικτύου, οι BS μπορούν να διαιρεθούν σε διάφορες λογικές οντότητες όπως φαίνεται στην εικόνα 18.



Εικόνα 18 Λογική Δομή του Σταθμού Βάσης BS

Στη πλευρά Iub, ο BS είναι μια συλλογή δύο οντοτήτων, **κοινή μεταφορά** και ένας **αριθμός Σημείων Λήξης Κυκλοφορίας (TTP)**. Η **κοινή μεταφορά** αντιπροσωπεύει εκείνα τα κανάλια μεταφορών που είναι κοινά για όλα τα UE στη κυψέλη και εκείνα που χρησιμοποιούνται για την αρχική πρόσβαση. Η κοινή οντότητα μεταφοράς περιέχει επίσης μια θύρα Ελέγχου ενός Κόμβου B που χρησιμοποιείται για τους σκοπούς λειτουργίας και συντήρησης (O&M). Ένας **TTP** αποτελείται από διάφορα *Πλαίσια*

Επικοινωνίας κόμβων B. Το **Πλαίσιο Επικοινωνίας κόμβων B** αποτελείται, στη συνέχεια, από όλες τις αφιερωμένες πηγές συμπεριφοράς που απαιτούνται όταν το UE είναι σε αφιερωμένο τρόπο (dedicated mode). Κατά συνέπεια, τα πλαίσια μιας επικοινωνίας κόμβων B μπορούν να περιέχουν τουλάχιστον ένα αφιερωμένο κανάλι, για παράδειγμα το (DCH). Από την άποψη των υποδομών δικτύων UMTS, οι BS μπορούν να θεωρηθούν ότι είναι μια λογική O&M οντότητα, η οποία είναι υπαγόμενη στις διοικητικές διαδικασίες δικτύων. Με άλλα λόγια, αυτός ο όρος περιγράφει τους φυσικούς BS και τις περιστάσεις τους, περιοχή των BS.

Από την άποψη του ραδιο δικτύου και του ελέγχου του οι BS αποτελούνται από διάφορες άλλες λογικές οντότητες αποκαλούμενες τα **κελιά**. Ένα κελί είναι η μικρότερη ραδιο οντότητα δικτύων που έχει τον δικό του αριθμό προσδιορισμού (ταυτότητα κελιών), το οποίο είναι δημόσια ορατό για το UE. Όταν το ραδιο δίκτυο διαμορφώνεται, είναι στην πραγματικότητα το κελί ή τα κελιά που αλλάζουν.

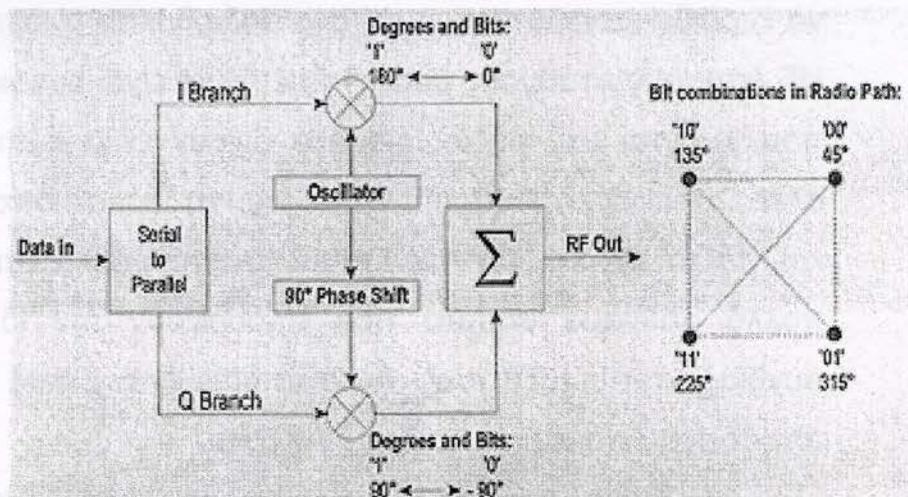
Κάθε κελί έχει έναν κώδικα ανακατώματος (scrambling code), **το UE αναγνωρίζει ένα κελί από δύο αξίες, κώδικας scrambling (κατά την σύνδεση σε ένα κελί) και την ταυτότητα των κελιών (για τη ραδιο τοπολογία δικτύων)**. Ένα κελί μπορεί να έχει διάφορους αποστολείς-αποδέκτες (οι TRXs, αποκαλούμενοι επίσης και ως μεταφορείς) κάτω από αυτό. Το TRX του κελιού παραδίδει τις πληροφορίες ραδιοφωνικής μετάδοσης μέσω του UE.

4.2.2 Η μέθοδος διαμόρφωσης

Από την άποψη του συστήματος, η χρησιμοποιημένη μέθοδος διαμόρφωσης βρίσκεται κάτω από κάποιο ενδιαφέρον δεδομένου ότι έχει μια στενή σχέση με την γενική δυναμικότητα του συστήματος και της απόδοσης τους. Το WCDMA χρησιμοποιεί τη QPSK ως μέθοδο διαμόρφωσής του στην κατεύθυνση κατιουσών συνδέσεων. Για να τον καταστήσουμε απλό, αυτή η μέθοδος διαμόρφωσης εκφράζει λίγο και τη

θέση του με μια διαφορετική φάση από τον μεταφορέα. Τα δυαδικά ψηφία bits στη διαδικασία διαμόρφωσης αντιμετωπίζονται ως ζευγάρια και έτσι, αυτό παράγει τέσσερις πιθανούς δύο -bit- συνδυασμούς που υποδεικνύονται.

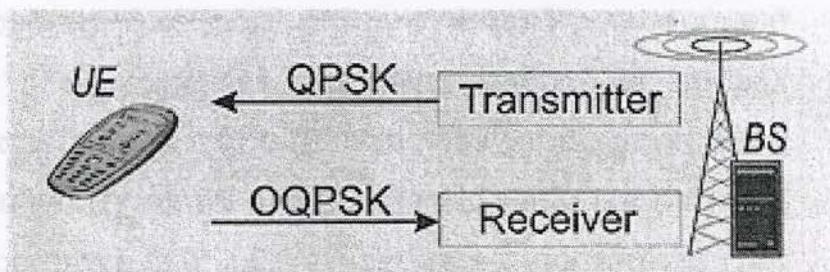
Στη διαδικασία διαμόρφωσης, το ρεύμα δεδομένων που διαμορφώνεται, π.χ. τα φυσικά κανάλια μετατρέπονται αρχικά από σειριακή σε παράλληλη μορφή. Μετά από αυτήν την μετατροπή, η διαδικασία διαμόρφωσης διαιρεί το ρεύμα δεδομένων σε δύο κλάδους, I και Q. Στον κλάδο I το δυαδικό ψηφίο που έχει την αξία "1" αντιπροσωπεύει + 180° μετατόπιση φάσης και η αξία "0" σημαίνει ότι η φάση του μεταφορέα δεν έχει μετατοπιστεί. Στο κλάδο του Q το bit που έχει την αξία "1" αντιπροσωπεύει + 90° μετατόπιση φάσης και η αξία "0" αντιπροσωπεύει -90° μετατόπιση φάσης. Όταν το εισερχόμενο ρεύμα δεδομένων συνδυάζεται με την έξοδο ταλαντωτών, οι δύο - bit - συνδυασμοί (ένα bit από το I και ένα bit από τον κλάδο Q) αντιπροσωπεύουν τη μετατόπιση φάσης που εμφανίζεται στη δεξιά πλευρά της εικόνας 19 που οι λεπτές γραμμές στο τετράγωνο δείχνουν τα "μονοπάτια" όπου το σύστημα μπορεί να μεταφερθεί το ίδιο από μια φάση σε άλλη.



Εικόνα 19 Αρχές Διαδικασίας διαχείρισης του QPSK

Αυτό το σύστημα εργάζεται πολύ καλά, αλλά ορισμένοι δύο - bit - συνδυασμοί είναι δυσκολότερο να χειριστούν. Παραδείγματος χάριν, όταν

αλλάζουν οι τιμές bit από "00" "σε 11" σημαίνει 180° μετατόπιση φάσης που μπορεί να φανεί ως πολύ αξιοπρόσεκτη αλλαγή εύρους. Οι πολύ μεγάλες αλλαγές εύρους προκαλούν τα προβλήματα ειδικά εάν το εύρος ζώνης συχνοτήτων που χρησιμοποιείται στη ραδιο σύνδεση είναι ευρύ. Σε αυτήν την περίπτωση οι BS πρέπει να έχουν τους γραμμικούς ενισχυτές προκειμένου να εγγυηθούν ότι οι αλλαγές εύρους αντιπροσωπεύονται σωστά σε όλο το χρησιμοποιημένο εύρος ζώνης συχνοτήτων.



Εικόνα 20 Χρησιμοποιημένες μέθοδοι μορφοποίησης και οι κατευθύνσεις τους

4.2.3. Η Τεχνική του αποδέκτη

Το WCDMA χρησιμοποιεί πολλαπλές διαδρομές. Οι διαδρομές αυτές μεταφέρουν το μεταδιδόμενο σήμα σε πολλούς διαφορετικούς προορισμούς από τον μεταφορέα στον αποδέκτη. Απ'την άλλη πλευρά για να κερδιθεί μεγαλύτερη ισχύς στο ραδιοδύκτιο η ισχύς μεταφοράς από το UE (και τους σταθμούς βάσης) πρέπει να είναι σχετικά μικρές. Οι μειώσεις που γίνονται στο ραδιο interface δίνουν επίσης περισσότερο χώρο για άλλες μεταφορές. Αυτό οδηγεί σε μια κατάσταση όπου είναι πολύ χρήσιμο και για το UE και για τον Σταθμό Βάσης γιατί είναι ικανά να συλλέγουν πολλά αδύναμα σήματα που προορίζουν την ίδια μεταφορά και να συνδιάζονται μεταξύ τους. Αυτό απαιτεί έναν ειδικό τύπο αποδέκτη. Ένα παράδειγμα αποδέκτη λέγεται RAKE.

Έχοντας χρησιμοποιήσει τον αποδέκτη RAKE και μέσα στο UE και μέσα στους BS το καθιστά πιθανό να συλλάβει και να συνδυάσει τους διαφορετικούς κλάδους του επιθυμητού σήματος και να βελτιώσει την ποιότητα του τελευταίου ρεύματος σημάτων ή δεδομένων που υποβάλλεται σε επεξεργασία περαιτέρω.

4.2.4 Δυναμικότητα κυψέλης

Στα πρώτα συστήματα του UMTS, το UTRAN θα χρησιμοποιήσει τη παραλλαγή WCDMA -FDD. Σε αυτήν την παραλλαγή, οι κατευθύνσεις μεταφοράς του Uu interface χρησιμοποιούν χωριστές περιοχές συχνότητας. Μια από τις πιο ενδιαφέρουσες ερωτήσεις (και ένα από τα συγγέοντα αντικείμενα) για τους ανθρώπους είναι το δυναμικό μονάδας του WCDMA TRX. Στο παγκόσμιο σύστημα των κινητών επικοινωνιών (GSM) ο υπολογισμός δυναμικού μονάδας του TRX είναι μια πολύ απλή διαδικασία, αλλά επειδή μέσα στο WCDMA το ραδιο interface αντιμετωπίζεται διαφορετικά και το δυναμικό μονάδας του συστήματος περιορίζεται από τους μεταβλητούς παράγοντες, το δυναμικό μονάδας του WCDMA TRX δεν είναι πολύ εύκολο να καθοριστεί.

Το ακόλουθο κείμενο παρουσιάζει μια ιδέα πώς να υπολογίσει κανείς κατά προσέγγιση το δυναμικό μονάδας WCDMA TRX θεωρητικά και βασισμένος στους όρους του ραδιο συστήματος. Προκειμένου να απλοποιηθεί το ζήτημα, πρέπει να κάνουμε μερικές υποθέσεις:

- όλοι οι συνδρομητές κάτω από την περιοχή κάλυψης TRX διανέμονται εξίσου έτσι ώστε να έχουν ίσες αποστάσεις από την TRX κεραία
- το επίπεδο ισχύος που χρησιμοποιούν είναι ίδιο και έτσι η παρέμβαση που προκαλούν είναι στο ίδιο επίπεδο
- αυτοί που βρίσκονται κάτω από το TRX χρησιμοποιούν το ίδιο ποσοστό bits ευραίους ζώνης, π.χ. επίσης τα ίδια ποσοστά συμβόλων.

Κάτω από αυτές τις περιστάσεις μια αξία αποκαλούμενη κέρδος επεξεργασίας (GP) μπορεί να καθοριστεί. Η επεξεργασία του κέρδους είναι ένας σχετικός δείκτης που μας ενημερώνει ποια είναι η σχέση μεταξύ ολόκληρου του διαθέσιμου εύρους ζώνης συχνοτήτων (BRF) και το ποσοστό bits ευραίους ζώνης περιοχών (Binformation).

$$GP = BRF / \text{Binformation}$$

Υπάρχει ένας άλλος τρόπος να εκφραστεί ο GP χρησιμοποιώντας ποσοστά bits και δεδομένων:

GP = chiprate/datarate

Και οι δύο τρόποι (όταν αναγγέλλονται σε τιμές dB) δίνει κατά συνέπεια τη βελτίωση της αναλογίας σήματος/ διαταραχής (**S/N**) μεταξύ του λαμβανόμενου σήματος και της εξόδου του δέκτη.

Παράδειγμα

Bit rate = 30 kb/s spreading factor=?

$G_p = 3840000 / 30000 = 128 = \text{Spreading Factor}$

Η ισχύς **P** = $E_b * \text{Baseband Datarate}$

Ο θόρυβος σ'ένα κανάλι (N_{Channel}) χροισιμοποιεί τμηματικά ολόκληρο το ευρος ζώνης B_{rf} :

$$N_{\text{Channel}} = B_{\text{RF}} * N_o$$

όπου N_o είναι W / Hz

έτσι,

$$S / N = P / N_{\text{Channel}} = E_b * \text{Baseband Datarate} / B_{\text{RF}} * N_o = (E_b / N_o) / G_p$$

Αν υποθέσουμε ότι έχουμε X χρήστες κάτω απο το TRX θεωρούμε X-1 χρήστες να προκαλούν παρέμβαση σ'ένα χρηστή:

$$S / N = P / P * (X-1) = 1 / X-1 \approx 1 / X$$

$$\text{Οπότε, } (E_b / N_o) / G_p \approx 1 / X \Rightarrow X \approx G_p / (E_b / N_o)$$

Παράδειγμα

Υποθέτουμε ότι ο spreading factor στο κελί είναι 128 και γι' αυτές τις μεταβολές το E_b / N_o είναι 3dB. Πόσους χρήστες μπορεί ένα κελί να περιλαμβάνει αν υποθέσουμε ότι υπάρχει 1 TRX διαθέσιμο;

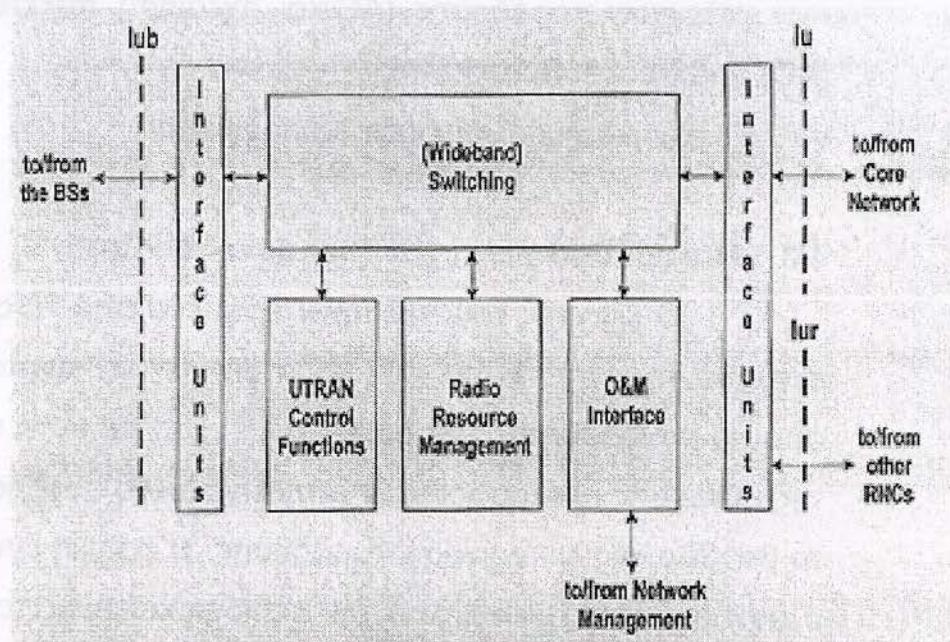
$$X \approx G_p / (E_b / N_o) = 128 / 3\text{dB} \approx 128 / 2 = 64 \text{ χρήστες}$$

Αυτό είναι το μέγιστο ποσό χρηστών που το TRX είναι σε θέση να χειριστεί, στη θεωρία λαμβάνοντας υπόψη την παρέμβαση των intracell. Στην πραγματικότητα τα γειτονικά κελιά προκαλούν παρέμβαση intercell. Εάν υποθέσουμε ότι η παρέμβαση intercell είναι ίδια με την παρέμβαση intracell έπειτα το ποσό χρηστών χωρίζεται σε 32 ($64/2 = 32$).

- το N_0 είναι μια τοπική μεταβλητή, η οποία περιλαμβάνει επίσης μερικές ειδικές τιμές του αποδέκτη
- το E_b είναι μια μεταβαλλόμενη φυσική μεταβλητή και οι εξαρτήσεις του αναφέρονται στις επόμενες κουκίδες
- Απόκτηση κέρδους / spreading factor (διαδιδόμενος παράγοντας): όσο μεγαλύτερη είναι τιμή του διαδιδόμενου παράγοντα, τόσο μικρότερο είναι το E_b
- όσο υψηλότερο είναι το ποσοστό εύρος ζώνης που χρησιμοποιείται, τόσο μεγαλύτερο θα είναι το E_b (αυτό είναι μια άμεση συνέπεια από το προηγούμενο σημείο).
- απόσταση μεταξύ του τερματικού και του αποδέκτη των BS: όσο μεγαλύτερη είναι η απόσταση, τόσο μεγαλύτερη θα είναι το E_b .
- ταχύτητα κίνησης του τερματικού: όσο μεγαλύτερη είναι η ταχύτητα που χρησιμοποιείται, τόσο μεγαλύτερο θα είναι το E_b .

4.3 Ο ελεγκτής των ραδιο δικτύων

Το RNC είναι το στοιχείο ελέγχου και μεταστροφής του UTRAN. Το RNC βρίσκεται μεταξύ του Iub και του Iu interface. Έχει επίσης το τρίτο interface το αποκαλούμενο Iur για εσωτερικές διά - συνδέσεις RNS.



Εικόνα 21 Λογική Δομή του RNC

Το RNC βλέπει τους BS ως δύο οντότητες που είναι κοινά πλαίσια επικοινωνίας μεταφοράς και συλλογής των κόμβων B. Το RNC που ελέγχει αυτούς τους κόμβους για έναν BS καλείται ο **RNC ελέγχου (CRNC)**.

Το RNC είναι ένα σημείο μετατροπής μεταξύ του φορέα Iu και του φορέα RB ή των φορέων RBs.

Ολόκληρη η λειτουργία του RNC μπορεί να ταξινομηθεί σε δύο μέρη, στη Διαχείριση των ΡαδιοΠηγών της UTRAN (RRM) και στις λειτουργίες ελέγχου. Το **RRM** είναι μια συλλογή των αλγορίθμων που χρησιμοποιούνται για να εγγυηθούν τη σταθερότητα του ραδιο μονοπατιού και το QoS της ραδιο σύνδεσης με την αποδοτική διανομή και τη διαχείριση των ραδιο πηγών. Οι **λειτουργίες ελέγχου** του UTRAN περιλαμβάνουν όλες αυτές τις λειτουργίες που αφορούν το set-up, τη συντήρηση και την έκδοση των RBs συμπεριλαμβανομένων των λειτουργιών υποστήριξης για τους αλγορίθμους RRM.

Οι αλγόριθμοι RRM που παρουσιάζονται σύντομα εδώ είναι:

- έλεγχος αποδοχής(handover control)
- ισχύς ελέγχου(Power Control)
- έλεγχος παράδοσης (AC)και σχεδίαση πακέτου (Admission Control (AC) and Packet Scheduling)
- διαχείριση κώδικα(Code Management)

4.3.1 Η παράδοση ελέγχου (handover control)

Ο έλεγχος του handover είναι ένα από τα ουσιαστικά μέσα για να εγγυηθεί τη κινητικότητα των χρηστών σε ένα κινητό δίκτυο επικοινωνιών, όπου ο συνδρομητής μπορεί να είναι μέσα σε αυτό το δίκτυο. Η διατήρηση της σύνδεσης κυκλοφορίας με έναν κινούμενο συνδρομητή γίνεται πιθανή με τη βοήθεια της λειτουργίας παράδοσης. Η βασική έννοια είναι απλή: όταν ο συνδρομητής κινείται από την περιοχή κάλυψης του ενός κελιού σε άλλο, μια νέα σύνδεση με το κελί-στόχο πρέπει να εγκατασταθεί και η σύνδεση με

το παλαιό κελί μπορεί να αφηθεί. Ο έλεγχος των μηχανισμών παράδοσης είναι εντούτοις, αρκετά περίπλοκο ζήτημα στα κυψελοειδή συστήματα και στα ειδικά συστήματα πολλαπλής Πρόσβασης Τμηματοποίησης του Κώδικα (CDMA) προσθέτει μερικά ενδιαφέροντα συστατικά σε αυτό.

Λόγοι πίσω από το handover

Ο βασικός λόγος πίσω από ένα handover είναι ότι η σύνδεση του interface δεν εκπληρώνει τα επιθυμητά κριτήρια που τίθενται για το άλλο και έτσι είτε το UE ή το UTRAN αρχίζει τις ενέργειες προκειμένου να βελτιωθεί η σύνδεση.

Στην περίπτωση των κλήσεων μεταγωγής πακέτων, τα handovers επιτυγχάνονται κυρίως όταν ούτε το δίκτυο ούτε το UE δεν έχουν οποιαδήποτε δραστηριότητα μεταφοράς πακέτων.

Τα κριτήρια εκτέλεσης του handover εξαρτώνται κυρίως στη στρατηγική του handover που εφαρμόζεται στο σύστημα. Εντούτοις, τα περισσότερα κριτήρια πίσω από το handover που ενεργοποιούν το υπόλοιπο στην ποιότητα σημάτων, την κινητικότητα χρηστών, την διανομή κυκλοφορίας, το εύρος ζώνης συχνοτήτων, και άλλα.

Το handover που οφείλεται στην ποιότητα σημάτων εμφανίζεται όταν πέφτει η ποιότητα ή η δύναμη του ραδιο σήματος κάτω από ορισμένες παραμέτρους που προσδιορίζονται στο RNC. Η επιδείνωση του σήματος ανιχνεύεται από τις σταθερές μετρήσεις σημάτων που πραγματοποιούνται και από το UE και από τους BS. Το handover της ποιότητας σημάτων μπορεί να εφαρμοστεί και για τις uplink και για τις downlink ραδιο συνδέσεις.

Τα handovers που οφείλονται στην κίνηση εμφανίζονται όταν το δυναμικό μονάδας κίνησης ενός κελιού έχει φθάσει στο maximum ή το πλησιάζει. Σε αυτήν την περίπτωση, το UE κοντά στις άκρες του κελιού με υψηλό φορτίο, μπορεί να παραδοθεί στα γειτονικά κελιά με το λιγότερο φορτίο κυκλοφορίας. Με τη χρησιμοποίηση αυτού του είδους του handover το φορτίο του συστήματος μπορεί να διανεμηθεί πιο ομοιόμορφα και η

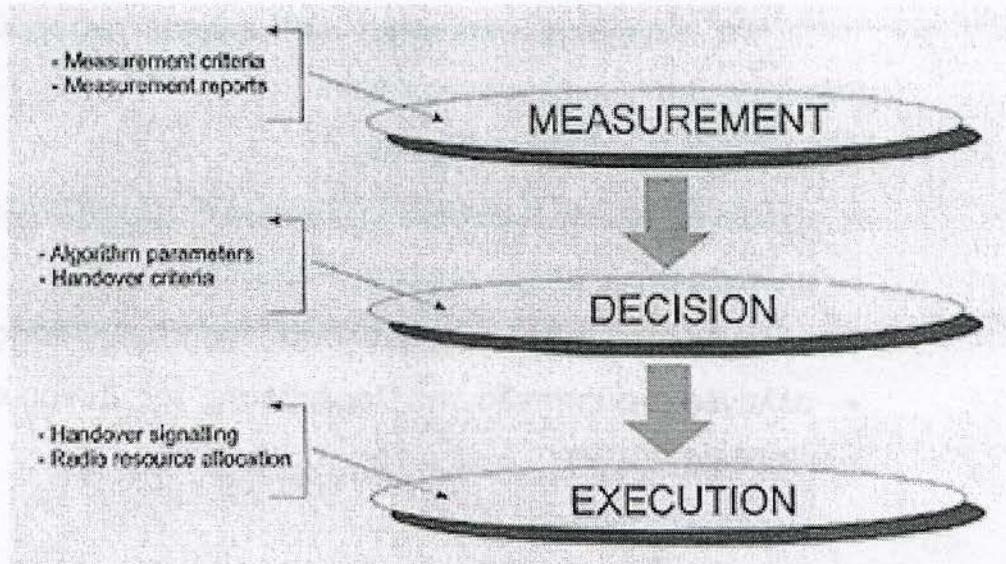
αναγκαία κάλυψη και το δυναμικό μονάδας μπορούν να προσαρμοστούν αποτελεσματικά για να συναντήσουν την απαιτούμενη κυκλοφορία μέσα στο δίκτυο.

Ο αριθμός των handovers είναι απευθείας εξαρτώμενος από το βαθμό κινητικότητας του UE. Εάν υποθέσουμε ότι το UE συνεχίζει να κινείται στην ίδια κατεύθυνση, τότε μπορεί να ειπωθεί ότι όσο γρηγορότερα το UE κινείται τόσο περισσότερα handovers προκαλούνται στο UTRAN. Για να αποφύγουμε τα ανεπιθύμητα handovers το UE με υψηλή ταχύτητα κίνησης μπορεί να παραδοθεί, παραδείγματος χάριν, από τις μικροκυψέλες (micro-cells) στις υπερκυψέλες (macro-cells). Σε περίπτωση που το UE κινείται αργά, από την άλλη μεριά, μπορεί να παραδοθεί από τα macro-cells στα micro-cells για να βελτιωθεί η δύναμη των ραδιο σημάτων και να αποφύγει την κατανάλωση της μπαταρίας του.

Η απόφαση να εκτελεσθεί ένα handover γίνεται πάντα από το RNC, που εξυπηρετεί αυτήν την περίοδο το συνδρομητή, εκτός από το handover που οφείλεται στην κίνηση. Στην τελευταία περίπτωση το κινητό κέντρο μετατροπής (MSC) μπορεί επίσης να πάρει την απόφαση. Εκτός από τον ανωτέρω λόγο, πολλοί άλλοι λόγοι, παραδείγματος χάριν, η αλλαγή των υπηρεσιών μπορεί επίσης να είναι μια βάση για την εκτέλεση του handover.

Διαδικασία του Handover

Η εικόνα 22 επεξηγεί, μια βασική διαδικασία handover αποτελούμενη από τρεις βασικές φάσεις, συμπεριλαμβανομένης της φάσης μέτρησης, της φάσης απόφασης, και της φάσης εκτέλεσης. Η γενική διαδικασία του handover που συζητείται εδώ είναι συγκεκριμένα σχετική με το σύστημα WCDMA.



Εικόνα 22 Διαδικασία Handover

Σύμφωνα με την τεχνική προδιαγραφή της 3GPP (TS) 25.331, οι μετρήσεις του UE μπορούν να ομαδοποιηθούν σε διαφορετικές κατηγορίες, ανάλογα με αυτό που το UE πρέπει να μετρήσει. Οι διαφορετικοί τύποι μετρήσεων είναι:

- μετρήσεις εσωτερικής συχνότητας: περιλαμβάνουν μετρήσεις με βάση τα φυσικά κανάλια downlink κατεύθυνσης για σήματα με τις ίδιες συχνότητες
- μετρήσεις εσωτερικής συχνότητας: περιλαμβάνουν τις μετρήσεις με βάση τα φυσικά κανάλια downlink κατεύθυνσης για τα σήματα με διαφορετικές συχνότητες
- μετρήσεις εσωτερικής συχνότητας: καλύπτουν μετρήσεις με βάση φυσικά κανάλια downlink συνδέσεων τα οποία ανήκουν σε ένα άλλο σύστημα ραδιο πρόσβασης από το UTRAN, για παράδειγμα το GSM
- μετρήσεις κίνησης: περιλαμβάνουν την δυνατότητα κίνησης στην uplink κατεύθυνση
- μετρήσεις ποιότητας: περιλαμβάνουν μετρήσεις για παραμέτρους ποιότητας, για παράδειγμα τα ποσοστά λάθους μεταφοράς
- εσωτερικές μετρήσεις: περιλαμβάνουν μετρήσεις για την δυνατότητα μεταφοράς του UE και το ποσοστό λαμβανομένων σημάτων του UE

Τα γεγονότα μέτρησης, αφ' ετέρου, μπορούν να προκληθούν βασιζόμενα στα ακόλουθα κριτήρια:

- αλλαγή του καλύτερου κελιού
- αλλαγές στο Πρωτεύον Κοινό Πιλοτικό Κανάλι (CPICH) επίπεδο σήματος
- αλλαγές στο επίπεδο σήματος P-CCPCH
- αλλαγές στο επίπεδο της αναλογίας της παρέμβασης του σήματος(SIR)
- αλλαγές στο επίπεδο της Παρέμβασης της Δυναμικότητας του Σήματος του Κώδικα (ISCP)
- Περιοδική αναφορά
- Χρόνος έκθεσης

Όσο η λήψη της απόφασης για το handover μας απασχολεί, υπάρχουν δύο κύριοι τύποι handover:

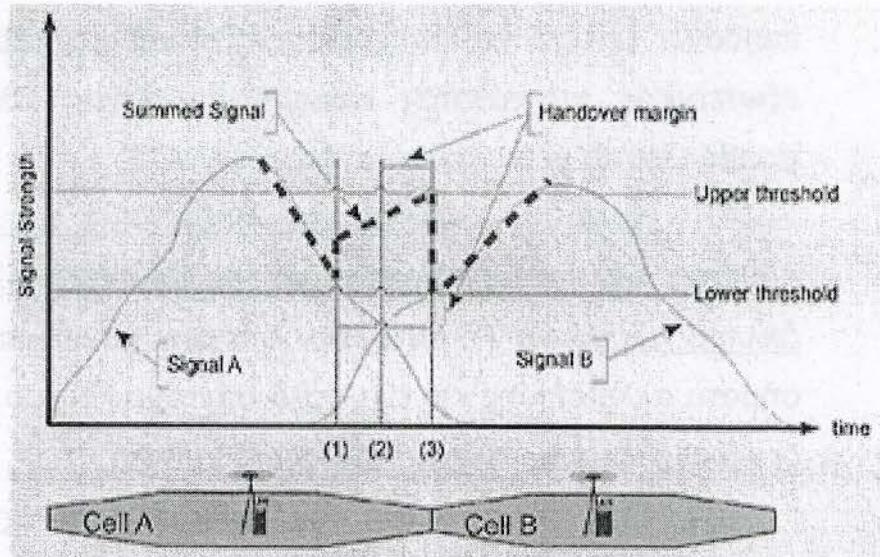
- ***Αξιολογημένο Δίκτυο Handover (NEHO)***
- ***Αξιολογημένο Κινητό Handover (MEHO)***

Στην περίπτωση της διαδικασίας NEHO, το δίκτυο SRNC παίρνει την απόφαση του handover, καθώς στη προοπτική MEHO το UE προετοιμάζει κυρίως την απόφαση handover. Στην περίπτωση των συνδιασμένων τύπων handover NEHO και MEHO, η απόφαση που παίρνεται είναι σε συνεργασία με το SRNC και το UE.

Ακόμα και στο MEHO handover η τελική απόφαση σχετικά με την εκτέλεση του handover παίρνεται από το SRNC. Ο λόγος είναι ότι το RNC είναι υπεύθυνο για το ολικό PPM του συστήματος.

Η απόφαση για την επίλυση του handover βασίζεται στις μετρήσεις που αναφέρονται από το UE και τον σταθμό βάσης όπως τα κριτήρια θέτονται από τους αλγόριθμους του Handover.

Οι βασικές αρχές ενός αλγορίθμου handover παρουσιάζονται στην εικόνα 23. Σε αυτό το παράδειγμα υποθέτουμε ότι τα κριτήρια της λήψης της απόφασης του αλγορίθμου βασίζονται στην πιλοτική ισχύς του σήματος έτσι όπως αναφέρεται από το UE.



Εικόνα 23 Γενικές αρχές των αλγορίθμων των handovers

Οι ακόλουθες παράμετροι χρησιμοποιούνται σε αυτό το παράδειγμα αλγορίθμου handover:

- **Upper threshold:** είναι το επίπεδο στο οποίο η δύναμη του σήματος για την σύνδεση είναι στο μεγαλύτερο αποδεκτό επίπεδο σε σεβασμό με αυτά που απαιτεί το QoS.
- **Lower threshold:** είναι το επίπεδο στο οποίο η δύναμη του σήματος για την σύνδεση είναι στο μικρότερο αποδεκτό επίπεδο που ικανοποιεί αυτά που απαιτεί το QoS. Έτσι, η δύναμη του σήματος για την σύνδεση δε θα πρέπει να πέσει κάτω από αυτό.
- **Handover margin:** είναι μια προκαθορισμένη παράμετρος, η οποία ορίζεται στο σημείο που η ισχύς του σήματος του γειτονικού κελιού (B) έχει ξεκινήσει να φτάνει την ισχύ του σήματος του τρέχοντος κελιού (A) με ένα συγκεκριμένο σύνολο και / ή για μια συγκεκριμένη στιγμή.
- **Active Set:** είναι μια λίστα από σήματα των κλάδων (κελιών) μέσω της οποίας το UE έχει μόνιμη σύνδεση με το UTRAN.

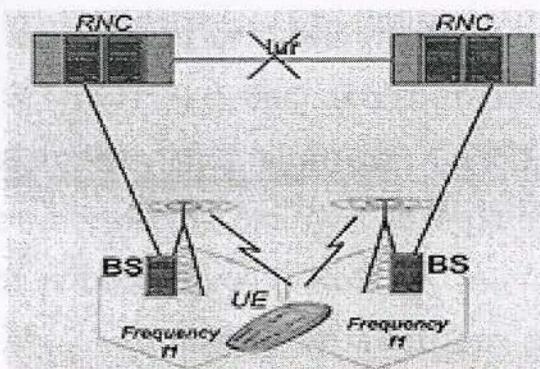
Τύποι Handovers

Τα handovers μπορούν να κατηγοριοποιηθούν σαν σκληρό handover, μαλακό handover και πιο μαλακό handover. Το σκληρό

handover μπορεί να κατηγοριοποιηθεί και περαιτέρω σε **εσωτερικής και εξωτερικής συχνότητας σκληρό handover**. Όλοι αυτοί οι μηχανισμοί προβάλλονται μέσω του συστήματος UMTS.

Κατά την διάρκεια της διαδικασίας του handover, αν η παλιά σύνδεση έχει αφαιρεθεί πριν κάνουμε την καινούρια σύνδεση τότε αυτό καλείται σκληρό handover. Γι' αυτό, δεν υπάρχει μόνο μια σειρά από ταυτόχρονα σήματα αλλά επίσης και ένα πολύ σύντομο κόψιμο στην σύνδεση, το οποίο δεν διακρίνεται εύκολα για τον κινητό χρήστη.

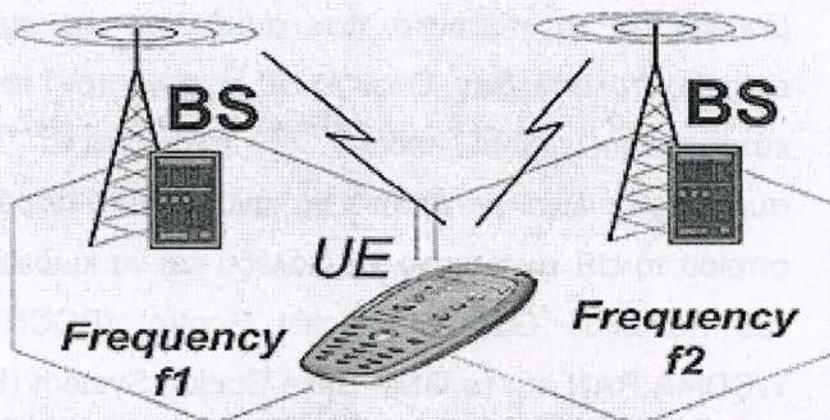
Στην περίπτωση του *inter-συχνότητας σκληρό handover* η μεταφερόμενη συχνότητα της νέας ραδιο πρόσβασης είναι διαφορετική από την παλιά με το UE που είχε συνδεθεί. Από την άλλη μεριά, αν ο νέος μεταφορέας στον οποίο το UE είχε πρόσβαση μετά την διαδικασία handover είναι ίδιος με αυτόν που είχε ο αρχικός μεταφορέας, τότε έχουμε σκληρό handover intra-frequency.



Εικόνα 24 INTRA-FREQUENCY HARD HANDOVER

Στην εικόνα 24, το RNC που γειτονεύει δεν είναι συνδεδεμένο με το Iur interface εξαιτίας της στρατηγικής- σχεδίου του ραδιο δικτύου ή σε λόγους μεταφοράς κι έτσι το inter-RNC soft handover δεν είναι δυνατό να γίνει. Έτσι, το μόνο handover που μπορεί να υπάρξει σε αυτήν την περίπτωση είναι το intra-frequency hard handover για να υποστηρίξει την ραδιο πρόσβαση στο δίκτυο που δεν φαίνεται και την κινητικότητα του χρήστη από τον παλιό BS στον καινούριο. Στην πραγματικότητα, αυτό

οδηγεί σε ένα inter RNC handover γεγονός στο οποίο το MSC επίσης εμπλέκεται.



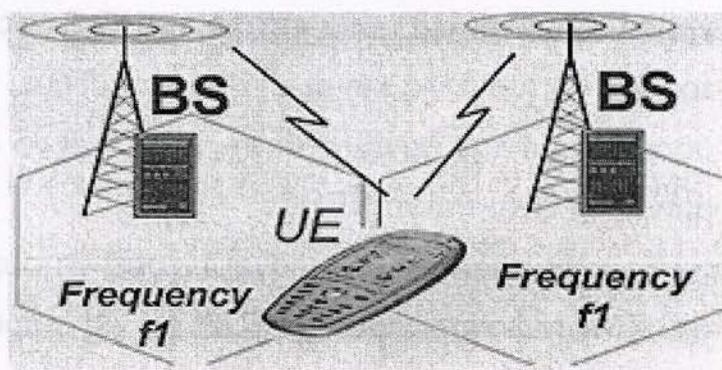
Εικόνα 25 INTER-FREQUENCY HARD HANDOVER

Το **inter-frequency handover** χρησιμοποιείται επίσης και στο δίκτυο με Ιεραρχική Δομή Κελιού (HCS) μεταξύ των χωρισμένων επιπέδων κελιών, για παράδειγμα μεταξύ των υπερκυψελών και των μικροκυψελών, τα οποία χρησιμοποιούν διαφορετικές συχνότητες μεταφοράς μέσα στην περιοχή κάλυψης. Σε αυτήν την περίπτωση το inter-frequency handover χρησιμοποιείται όχι μόνο επειδή το UE διαφορετικά θα χάσει την σύνδεση του στο δίκτυο αλλά και με σκοπό να αυξήσει την απόδοση του συστήματος όσον αφορά την δυναμικότητα- ισχύς και το QoS. Το inter-frequency hard handover είναι πάντα NEHO.

Το inter-frequency handover μπορεί να συμβεί μεταξύ δύο διαφορετικών δικτύων ραδιο πρόσβασης (RAN's), για παράδειγμα, μεταξύ του GSM και του WCDMA. Σε αυτό το σημείο μπορεί να ονομαστεί και inter-system handover (Εικόνα 26). Ένα inter-system handover είναι πάντα ένας τύπος της inter-frequency, αφού διαφορετικές συχνότητες χρησιμοποιούνται σε διαφορετικά συστήματα.

Η πιθανότητα να αποδώσει ένα inter-system handover είναι ικανή στο WCDMA με έναν ειδικό τρόπο τον Compressed Mode (ή Slotted Mode). Το Slotted Mode μπορούμε να το επιτύχουμε μειώνοντας τον ρυθμό δεδομένων χρησιμοποιώντας το υψηλότερο επίπεδο ελέγχου και επίσης μειώνοντας το ποσοστό των συμβόλων σε συνεργασία με το φυσικό επίπεδο πολυπλεξίας. Όταν το UE χρησιμοποιεί το Uu interface σε αυτή την κατάσταση (slotted mode) τα περιεχόμενα του WCDMA πλαισίου συμπιέζεται λίγο με σκοπό να ανοίξει ένα παράθυρο χρόνου μέσω του οποίου το UE είναι ικανό να διαλέξει και να κωδικοποιήσει τις πληροφορίες του Καναλιού GSM Broadcast Control (BCCH). Επιπρόσθετα, και το WCDMA RAN και το GSM Base Station System (BSS) πρέπει να μπορούν να στέλνουν τις πληροφορίες ταυτότητας τους ο καθένας στο BCCH έτσι ώστε το UE να μπορεί να αποδώσει την κωδικοποίηση κατάλληλα.

Αντίθετα από το hard handover, **εάν μια νέα σύνδεση καθιερώνεται προτού να εκδοθεί η παλαιά σύνδεση τότε το handover καλείται soft handover.** Στο WCDMA, η πλειοψηφία των handovers είναι intra-frequency soft handover. Όπως διευκρινίζεται στην εικόνα 26, στο **soft handover** οι γειτονικοί BS περιελάμβαναν στο γεγονός των μεταφορών του handover την ίδια συχνότητα.

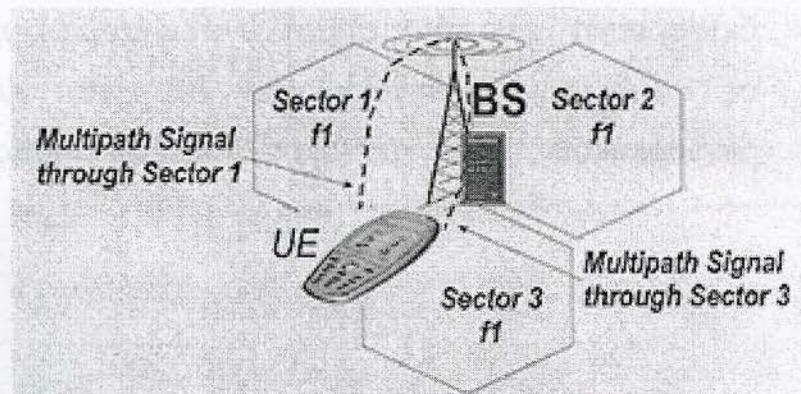


Εικόνα 26 Intra – frequency soft handover

Το **soft handover** εκτελείται μεταξύ δύο κελιών που ανήκουν σε διαφορετικό BS αλλά όχι απαραίτητως στο ίδιο RNC. Εν πάση περιπτώσει το RNC που περιλαμβάνεται στο soft handover πρέπει να συντονίσει την

εκτέλεση του soft handover πάνω από το Iur interface. Σε ένα γεγονός soft handover η πηγή και οι στόχοι των κελιών έχουν την ίδια συχνότητα. Σε περίπτωση κυκλώματος μεταστρεφόμενης κλήσης, το τερματικό εκτελεί πραγματικά τα soft handover σχεδόν όλη την ώρα εάν το περιβάλλον των ραδιο δικτύων έχει μικρά κελιά. Υπάρχουν διάφορες παραλλαγές του soft handover, συμπεριλαμβανομένου του softer και του soft-softer handovers.

Ένα **softer handover** είναι ένα handover από το οποίο ένα νέο σήμα είτε προστίθεται είτε διαγράφεται από το ενεργό σύνολο, είτε αντικαθίσταται από ένα ισχυρότερο σήμα μέσα στους διαφορετικούς τομείς, οι οποίοι είναι κάτω από τους ίδιους BS (εικόνα 27).



Εικόνα 27 INTRA – Frequency softer Handover

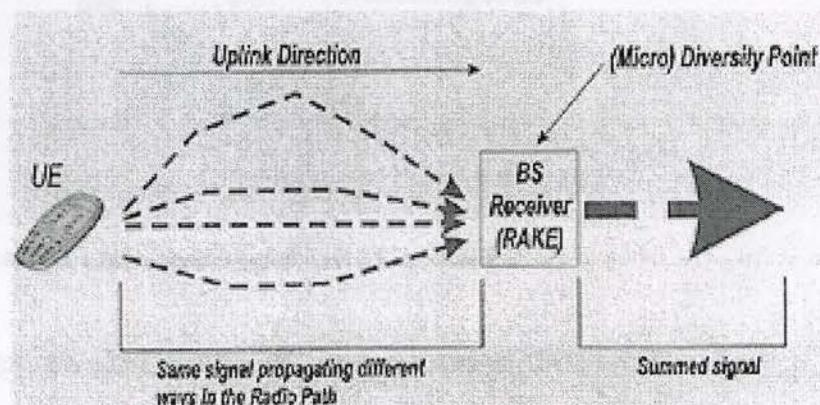
Στο soft handover, οι BS διαβιβάζουν μέσω του ενός τομέα αλλά λαμβάνουν από περισσότερο από έναν τομέα. Σε αυτήν την περίπτωση το UE έχει ενεργές τις uplink ραδιο συνδέσεις με το δίκτυο μέσω περισσότερους από έναν τομέα ο οποίος επικοινωνεί με τον ίδιο BS.

Όταν τα soft και softer handovers εμφανίζονται ταυτόχρονα, ο όρος soft-softer handover χρησιμοποιείται συνήθως. Ένα soft-softer handover μπορεί να εμφανιστεί, παραδείγματος χάριν, σε συνδυασμό με inter-RNC handover, ενώ ένα σήμα inter-sector προστίθεται στο ενεργό σύνολο του UE μαζί με την προσθήκη ενός νέου σήματος μέσω ενός άλλου κελιού που ελέγχεται από ένα άλλο RNC.

Αναφερόμενοι στο soft handover και το ενεργό σύνολο, υπάρχουν δύο όροι που περιγράφουν το χειρισμό των συστατικών των πολλαπλών διαδρομών. Αυτοί είναι **microdiversity** και **macrodiversity**.

Η **microdiversity** σημαίνει την κατάσταση όπου τα πολλαπλών διαδρομών συστατικά διάδοσης συνδυάζονται στους BS όπως φαίνεται στην εικόνα 28. Το WCDMA χρησιμοποιεί την διάδοση πολλαπλών διαδρομών. Αυτό σημαίνει ότι ο αποδέκτης BS RAKE είναι σε θέση να καθορίσει, να διαφοροποιήσει και να συνοψίσει διάφορα σήματα λαμβανόμενα από το ραδιο μονοπάτι.

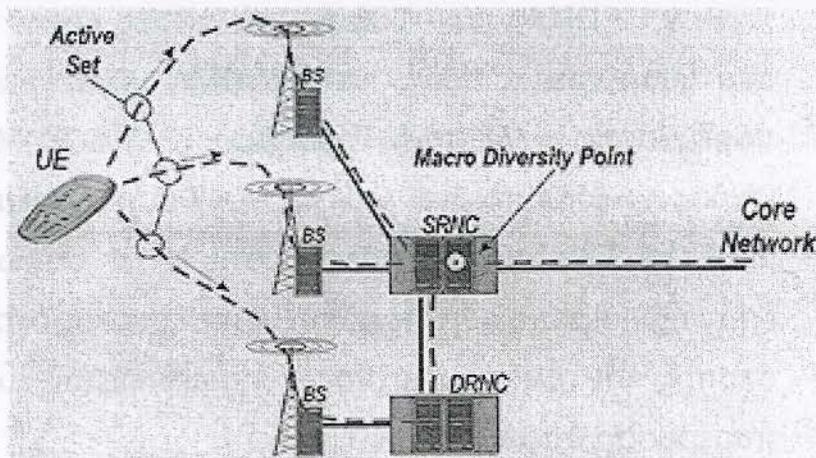
Η λειτουργία της **microdiversity** στο επίπεδο των BS συνδυάζει τα διαφορετικά μονοπάτια σημάτων που παραλαμβάνονται από ένα κελί, και σε αυτήν την περίπτωση των BS ανά τομείς, η έκβαση από τους διαφορετικούς τομείς, η οποία αναφέρεται επίσης ως softer handover.



Εικόνα 28 Η **micro diversity** στο BS

Επειδή το UE μπορεί να χρησιμοποιεί κελιά που ανήκουν σε διαφορετικό BS ή ακόμα και σε διαφορετικό RNC η λειτουργία της **macrodiversity** υπάρχει επίσης και στο επίπεδο RNC. Ωστόσο, ο τρόπος συνδιασμού των σημάτων είναι αρκετά διαφορετικός από την περίπτωση της **microdiversity** στον BS επειδή δεν υπάρχει κανένας RAKE αποδέκτης στο RNC. Έτσι, άλλες περιπτώσεις όπως η ποιότητα ροής δεδομένων μπορεί να χρησιμοποιούνται για να συνδιαστούν ή να επιλέξουν την επιθυμητή data stream. Η εικόνα 29 παρουσιάζει μια περίπτωση στην οποία το UE έχει ένα Active Set τριών κελιών σε χρήση και ένα από αυτά τα κελιά

είναι συνδεδεμένο σε ένα άλλο RNC. Σε αυτήν την περίπτωση, ο BS αρχικά αθροίζει το άθροισμα των σημάτων που απασχολούν τα ραδιομονοπατία μόνο του και το τελικό άθροισμα του data stream γίνεται στο επίπεδο RNC.



Εικόνα 29 Macro diversity στο BS

Από την πλευρά την αρχιτεκτονικής δομής του συστήματος, το δίκτυο UMTS υποστηρίζει τους ακόλουθους τύπους των handovers:

- Intra Bs/inter-cell handover (softer handover)
- Inter BS handover, που περιλαμβάνει τα hard και soft Handovers
- Inter RNC handover, που περιλαμβάνει τα hard, soft, soft-Softer handovers
- Inter MSC handover
- Inter Serving GPRS Support Node (SGSN) handover
- Inter system handover

4.3.2 Έλεγχος Ισχύς

Ο έλεγχος της ισχύος είναι ένα πολύ σημαντικό χαρακτηριστικό οποιουδήποτε κυψελλοειδούς συστήματος CDMA. Αν δεν έχουμε υπολογίσει τον απαραίτητο μηχανισμό ελέγχου της ισχύος, αυτά τα συστήματα δεν μπορούν να λειτουργήσουν.

Οι σημαντικότεροι λόγοι για τα προβλήματα που παρουσιάζονται κατά τον έλεγχο ισχύος είναι η παρεμβαλλόμενη εξαρτημένη δυναμικότητα του WCDMA και η περιορισμένη πηγή ισχύος του UE. Αντίθετα με τις τεχνικές FDMA και TDMA, οι οποίες είναι πολλαπλές προσβάσεις περιορισμένου εύρους, το WCDMA είναι μια τεχνική περιορισμένης παρέμβασης πολλαπλής πρόσβασης. Στα FDMA και TDMA, ο έλεγχος ισχύος χρησιμοποιείται για να μειωθεί η παρέμβαση των μικροκυψελών μέσα σε ένα κυψελλοειδές σύστημα το οποίο αναπτύσσεται από την επαναχρησιμοποίηση της συχνότητας ενώ στα συστήματα WCDMA ο σκοπός του ελέγχου ισχύος χρησιμοποιείται κυρίως για να μειώσει την παρέμβαση από τις υπερκυψέλες.

Βασικές προσεγγίσεις του ελέγχου ισχύος

Είναι εύκολο να καταλάβει κανείς ότι στην περίπτωση της uplink η βασική κατάσταση για τον αποδέκτη BS είναι ότι η ισχύς που αντιπροσωπεύει ένα UE σήμα είναι πάντα ίδιο όταν συγκρίνεται με τα άλλα UE σήματα ανεξάρτητα από την απόστασή τους από τον BS. Στην πραγματικότητα ωστόσο, το ραδιοκανάλι είναι εξαιρετικά μη σταθερό, όπως και οι απαιτούμενες ραδιοπηρεσίες διαφέρουν για τους διάφορους χρήστες και ακόμα και στον ίδιο χρήστη και κατά την διάρκεια μιας ραδιοσύνδεσης. Γι' αυτό η ισχύς μεταφοράς του UE θα πρέπει να ελέγχεται πολύ προσεκτικά με την χρησιμοποίηση αποδοτικών μηχανισμών.

Μηχανισμοί Ελέγχου Ισχύος στο UTRAN (WCDMA-FDD)

Στο WCDMA, ο έλεγχος ισχύος γίνεται και στην uplink και στην downlink κατεύθυνση. Στην downlink κατεύθυνση ο έλεγχος ισχύος χρησιμοποιείται για να μειωθεί η παρέμβαση σε άλλα κελιά. Όμως δεν είναι ζωτικής σημασίας όπως στην uplink κατεύθυνση για την εφαρμογή της μεταφερόμενης ισχύος. Προηγείται της downlink κατεύθυνσης γιατί βελτιώνει την απόδοση του συστήματος ελέγχοντας την παρέμβαση σε άλλα κελιά. Ο

κύριος σκοπός του ελέγχου ισχύος είναι (στην uplink) να διαχειριστεί το near-far πρόβλημα κάνοντας το επίπεδο της μεταφερόμενης ισχύος που λαμβάνεται από όλα τα τερματικά όσο μπορεί ίδιο όσο είναι δυνατόν στο κελί-βάση για το ίδιο QoS.

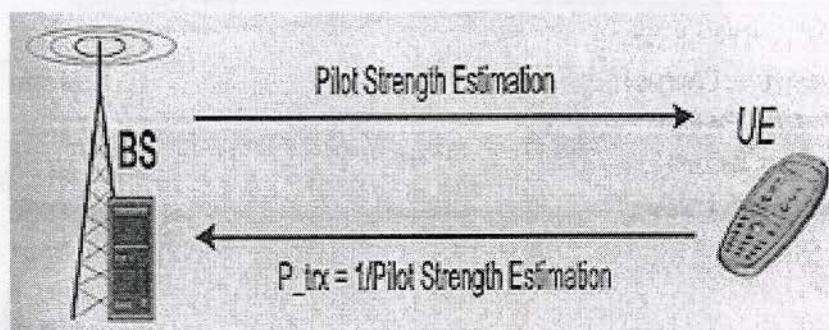
Στο GSM ο έλεγχος ισχύος χρησιμοποιείται για την σύνδεση μια ή δυο φορές το sec, αλλά εξαιτίας της κριτικής φύσης του WCDMA ο έλεγχος ισχύος χρησιμοποιείται στην σύνδεση 1500 φορές το sec. Έτσι στο WCDMA τα βήματα εφαρμογής ισχύος είναι αρκετά πιο γρήγορα από ότι στο GSM.

Στο WCDMA, το σύστημα χρησιμοποιεί δυο διαφορετικούς μηχανισμούς ελέγχου ισχύος:

- Open Loop Power Control (OLPC)
- Closed Loop Power Control (CLPC)

Open Loop Power Control (OLPC)

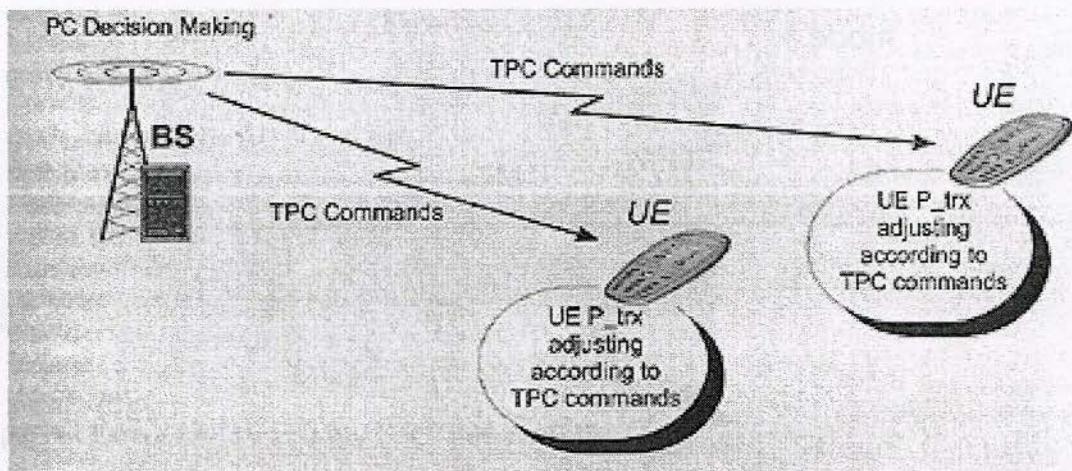
Στο OLPC που χρησιμοποιείται κυρίως στην uplink κατεύθυνση το σήμα UE εφαρμόζει την δύναμη μεταφοράς του σε ένα συγκεκριμένο επίπεδο του λαμβανόμενου σήματος από τον BS CPICH όταν το UE είναι σε idle mode και πρωταρχική μεταφορά στο Κανάλι φυσικής προσπέλασης (PRACH). Επιπρόσθετα το UE λαμβάνει πληροφορίες σχετικά με τις επιτρεπόμενες παραμέτρους ισχύος από το κελί BCCH όταν είναι σε idle mode.



Εικόνα 30 OLPC για την uplink κατεύθυνση

Closed Loop Power Control (CLPC)

Το CLPC χρησιμοποιείται για να εφαρμόσει την ταχύτητα ισχύος όταν η ραδιο σύνδεση έχει ήδη εγκατασταθεί. Σαν βασικός στόχος είναι να compensate το φαινόμενο των άμεσων αλλαγών στην ραδιο-ισχύ του σήματος και έτσι αυτό θα πρέπει να είναι αρκετά πιο γρήγορο για να ανταποκρίνεται σε αυτές τις αλλαγές. Η εικόνα 31 παρουσιάζει τον βασικό uplink μηχανισμό CLPC ο οποίος είναι ειδικός για το WCDMA. Ο BS διατάσει το UE να αυξάνει ή να μειώνει την ταχύτητα μεταφοράς με έναν κύκλο των 1.5 kHz (1500 φορές το sec) με 1,2, ή 3 dB step-sizes. Η απόφαση του αν θα μειωθεί ή θα αυξηθεί η ισχύς βασίζεται στο λαμβανόμενο SIR το οποίο έχει καθοριστεί από τον BS. Όταν ο BS λαμβάνει το σήμα UE, συγκρίνει την ισχύ του σήματος με την προκαθορισμένη αξία στον BS. Αν είναι το ίδιο ο BS στέλνει μια διαταγή TPC στο UE για να μειώσει την ισχύ του σήματος. Αν το λαμβανόμενο σήμα είναι χαμηλότερο από τον threshold στόχο ο BS στέλνει μια διαταγή στο UE να αυξήσει την ταχύτητα μεταφοράς. Θα πρέπει να σημειωθεί ότι υπάρχουν διάφορες μεταβλητές παράμετροι όπως το SIR (signal strength), FER (Frame Error Ratio) and BER (Bit Error Ratio) μπορούν να χρησιμοποιηθούν για να συγκριθεί η ποιότητα που λαμβάνουμε και για να πάρουμε την απόφαση για να ελέγξουμε την ισχύ μεταφοράς.

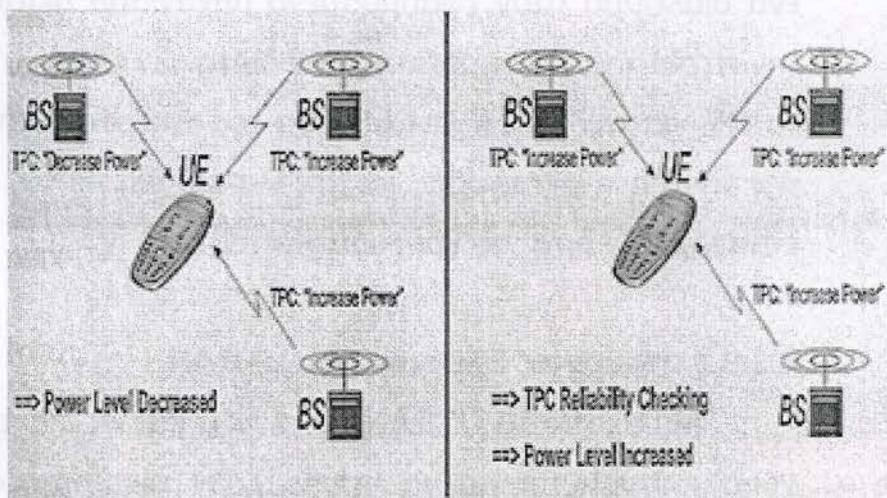


Εικόνα 31 Βασικός μηχανισμός CLPC στην uplink κατεύθυνση

Έλεγχος ισχύος σε ειδικές περιπτώσεις

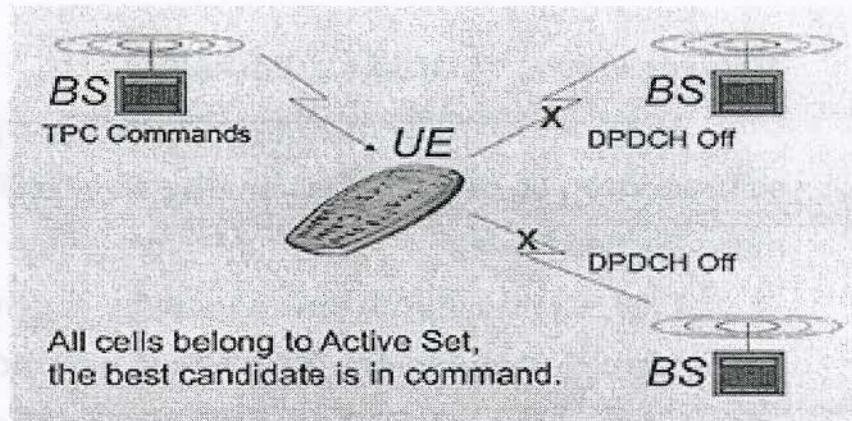
Αυτές οι περιπτώσεις είναι για τον έλεγχο ισχύος που σχετίζεται με το soft handover, με το Site Selection Diversity (SSDT), και με το compressed mode (Slotted Mode).

Στην περίπτωση του **soft handover**, η μεταφερόμενη ισχύς του UE εφαρμόζεται βασιζόμενο στην επιλογή της πιο κατάλληλης διαταγής ελέγχου ισχύος από εκείνα τα TPC τα οποία λαμβάνει από διαφορετικό BS στο οποίο αυτό έχει εγκατεστημένα radio links (Εικόνα 32). Σε αυτήν την περίπτωση επειδή το UE λαμβάνει περισσότερα από ένα TPC commands απο διαφορετικούς BS, οι TPC commands μπορεί να διαφέρουν μεταξύ τους. Αυτό έχει σαν αποτέλεσμα, ότι αυτές οι διαταγές δεν προστατεύονται απέναντι σε λάθη ή απλά μπορεί να προκύπτουν από το περιβάλλον του δικτύου.



Εικόνα 32 Έλεγχος ισχύος σε συνεργασία με το soft handover

Στην περίπτωση του **SSDT**, ο BS με το ισχυρότερο σήμα είναι δυναμικά επιλεγμένος σαν ο μοναδικός BS μεταφοράς (Εικόνα 33). Έπειτα, οι άλλοι BS με τους οποίους το UE έχει ήδη συνδεθεί, κλείνουν τα Dedicated Physical Data Channels (DPDCH). Αυτή η μέθοδος μειώνει την downlink παρέμβαση καθώς το UE είναι σε soft handover.



Εικόνα 33 Site Selection Diversity (SSDT)

Στο **compressed mode**, η μεταφορά και η αποδοχή του BS και του UE καθορίζονται για μια προκαθορισμένη περίοδο να κάνουν χώρο για να παρουσιαστούν οι μετρήσεις εσωτερικής συχνότητας, για παράδειγμα σε σχέση με το γεγονός του inter system handover. Σαν αποτέλεσμα, υπάρχει ένα διάλειμμα στον εφαρμοσμένο μηχανισμό μεταφοράς ισχύος. Σε αυτήν την περίπτωση ο αποδέκτης των διαταγών ελέγχου ισχύος, για παράδειγμα, το UE για την uplink κατεύθυνση του επιτρέπεται να αυξήσει ή να μειώσει την ταχύτητα μεταφοράς με μεγάλα step-sizes για να φτάσει το επιθυμητό επίπεδο SIR όσο πιο γρήγορα γίνεται.

4.3.3 Λειτουργίες Ελέγχου στο UTRAN

Με σκοπό το UTRAN να ελέγξει και να διαχειριστεί τα RBs, τα οποία χρησιμοποιούνται για να προβάλλουν την υπηρεσία RAB, θα πρέπει να παρουσιάσουμε μερικές άλλες λειτουργίες σε συνδιασμό με τους αλγορίθμους RRM. Ταξινομούνται ως εξής:

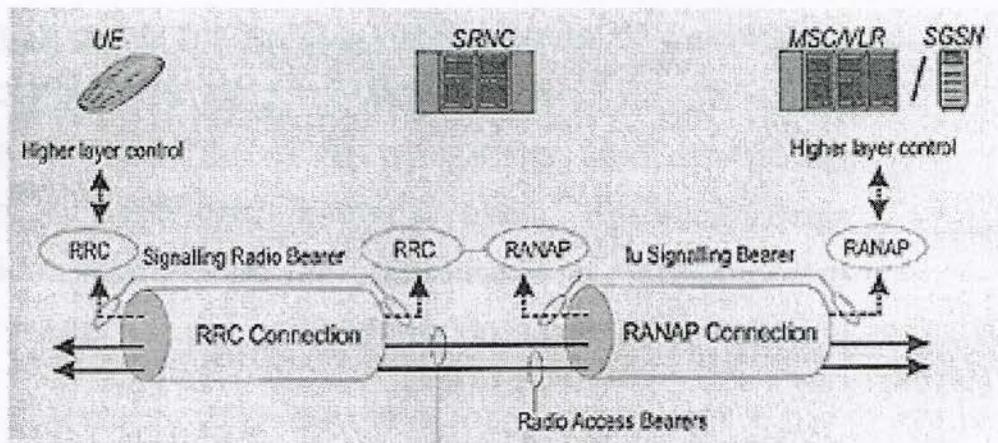
4.3.3.1 Μετάδοση Πληροφοριών Συστήματος

Μια σημαντική λειτουργία του RNC είναι να διαχειρίζεται τις πληροφορίες του συστήματος. Αυτές χρησιμοποιούνται για να καθορίσουν και τις δυο ραδιο συνδέσεις μεταξύ του UTRAN και του UE και επίσης για να ελέγχουν την συνολική λειτουργία του UTRAN. Το RNC μεταδίδει τα

στοιχεία των πληροφοριών του συστήματος για να βοηθήσει το UTRAN να ελέγξει τις λειτουργίες προβάλλοντας το UE με σημαντικά στοιχεία που χρειάζονται όταν επικοινωνεί με το UTRAN. Για παράδειγμα, για να προβληθούν τα ραδιο κριτήρια μέτρησης, ο προσδιορισμός της σελιδοποίησης, οι πληροφορίες του ραδιο μονοπατιού, τα δεδομένα που βοηθούν τις περιπτώσεις τοποθέτησης, κ.α.

4.3.3.2 Αρχική Πρόσβαση και Διαχείριση της σύνδεσης για σηματοδοσία

Πριν το RNC τοποθετήσει όλα τα RABs τα οποία έχουν ζητηθεί στο RB, χρειάζεται να δημιουργήσει την σύνδεση σηματοδοσίας μεταξύ του UE και του CN. Η 3GPP specification Technical Report (TR) 25.990 καθορίζει την σύνδεση σηματοδοσίας σαν μια (όχι γνωστή) ένωση μεταξύ του UE και του CN για να μεταφέρουν υψηλότερου επιπέδου πληροφορίες μεταξύ των οντοτήτων στην Non Access Stratum (NAS). Για να το κάνει αυτό το RNC χρησιμοποιεί τις υπηρεσίες της σύνδεσης RRC στον σχεδιασμό του Signalling Radio Bearer (SRB) μεταξύ του UE και του UTRAN για να προβάλει τις υπηρεσίες μεταφοράς για την σύνδεση σηματοδοσίας. Όταν το RNC έχει δημιουργήσει το SRB χρησιμοποιεί το πρώτο RLC RBs για να μετατρέψει και να μεταφέρει την σύνδεση σηματοδοσίας μέσω του UTRAN στο UE. Το RB έχει καθοριστεί σαν οι υπηρεσίες που παρέχουν μέσω του RLC επιπέδου για τη μεταφορά των δεδομένων του χρήστη μεταξύ του UE και του RNC. Ωστόσο, καθορίζει ότι τα πρωτεύον RBs χρησιμοποιούνται επίσης και για τους σκοπούς της σύνδεσης σηματοδοσίας (Εικόνα 34).



Εικόνα 34 Σχέση μεταξύ των SRB, RB, signalling connection, RANAP and the role of RNC

Η όλη διαδικασία ξεκινά όταν το UE μπαίνει σε idle mode αυξάνοντας την ισχύ τους. Αφού αυξηθεί, το UE προσπαθεί να συνδεθεί με το UTRAN. Το UE ψάχνει για ένα κατάλληλο κελί στο UTRAN και διαλέγει το κελί για να προβάλει τις διαθέσιμες υπηρεσίες. Αυτή η επιλογή είναι γνωστή ως **“κατασκήνώνοντας στο κελί”**. Η κατασκήνωση περιλαμβάνει μια έρευνα κελιού, όπου το UE ψάχνει για ένα κελί καθορίζει τον κώδικα για την downlink κατεύθυνση και συγχρονισμό πλαισίων αυτού του κελιού. Η έρευνα γίνεται με διαφορετικά βήματα.

Κατά το πρώτο βήμα το UE χρησιμοποιεί τον πρωταρχικό κώδικα συγχρονισμού του κανάλιου συγχρονισμού (SCH), ο οποίος είναι κοινός για όλα τα κελιά.

Στο δεύτερο βήμα το UE χρησιμοποιεί τον δευτερεύον κώδικα συγχρονισμού του SDH για να βρει τον συγχρονισμό πλαισίων και αναγνωρίζει τον ομαδοποιημένο κώδικα του κελιού που έχει βρεθεί από το πρώτο βήμα.

Στο τρίτο και τελευταίο βήμα, το UE καθορίζει τον ακριβή πρωτεύον κώδικα που χρησιμοποιείται από το κελί και τον οποίο τον βρίσκουμε μέσα στο UTRAN. Αν το UE αναγνωρίσει τον πρωταρχικό κώδικα τότε το P-CCPH μπορεί να βρεθεί και οι ειδικές πληροφορίες

ευρείας επέκτασης τόσο του συστήματος αλλά και του κελιού που έχουν καθοριστεί από το RNC μπορούν να διαβαστούν.

4.3.3.3 Διαχείριση του ραδιο Bearer

Όταν το RB εγκαθίσταται μεταξύ του ραδιο δικτύου και το UE είναι καιρός για το RNC να τοποθετήσει το RAB(s) που έχει ζητηθεί στο RB για μεταφορά μεταξύ του UTRAN και του UE. Σε αυτήν την περίπτωση το RNC δημιουργεί την ψευδαίσθηση ενός φτιαγμένου bearer μεταξύ του CN και του UE.

Αφού αυτά τα RAB έχουν διαπραγματευθεί μεταξύ του UE και του CN μέσω της σύνδεσης σηματοδότησης, προωθείται στο RNC για τις περαιτέρω ενέργειες. Η κύρια λειτουργία του RNC είναι να αναλύει τις συμπεριφορές των απαιτούμενων RABs, αξιοποιεί τις ραδιο πηγές που χρειάζονται για αυτά, ενεργοποιεί τα ραδιο κανάλια χρησιμοποιώντας το κατώτερο επίπεδο υπηρεσιών και τοποθετεί τα απαιτούμενα RABs στον RB. Γι' αυτό το RNC καλύπτει όλες τις λειτουργίες ελέγχου που σχετίζονται με τα RABs που υποστηρίζονται.

Όπως φαίνεται στην εικόνα 34, το RAB κουβαλά την σύνδεση RRC μεταξύ του RNC και του UE μέσω του radio interface και μαζί με την σύνδεση που βασίζεται στο πρωτόκολλο RANAP μεταξύ του RNC και του CN πάνω στο Iu interface. Σε αυτήν την περίπτωση το RNC λειτουργεί σαν μετατροπέας πρωτοκόλλου μεταξύ του RAN και του CN. Το RNC τοποθετεί τα RABs που απαιτούνται στον RBs χρησιμοποιώντας τις τρέχουσες ραδιο πηγές πληροφοριών και ελέγχει το κατώτερο επίπεδο υπηρεσιών.

4.3.3.4 Ασφάλεια στο UTRAN

Η ασφάλεια του UTRAN είναι μια ακόμα λειτουργία που διαχειρίζεται το RNC. Ο κανόνας που χρησιμοποιείται για να προστατευθεί η σύνδεση σηματοδότησης μεταξύ του UE και του UTRAN μέσω του radio

interface και αργότερα χρησιμοποιείται για να προστατέψει τα δεδομένα των χρηστών που μεταφέρονται μεταξύ του UE και του UTRAN.

Το RNC αλλάζει την σηματοδοσία και τα δεδομένα των χρηστών χρησιμοποιώντας τους καθορισμένους integrity και ciphering αλγόριθμους. Σε αυτήν την περίπτωση χρειάζεται να καθορίσουμε random αριθμούς και να καθορίζουμε τις μετρήσεις ενός εξαρτημένου μετρητή χρόνου για τον έλεγχο της integrity των μηνυμάτων σηματοδοσίας. Επίσης εξασφαλίζει τα λαμβανόμενα μηνύματα χρησιμοποιώντας αυτούς τους αλγόριθμους.

4.3.3.5 Διαχείριση κινητικότητας στο επίπεδο UTRAN

Το UTRAN level Mobility Management (MM) αναφέρεται σε εκείνες τις λειτουργίες, τις οποίες το RNC διαχειρίζεται με σκοπό να κρατήσει το UE σε επαφή με τα κελιά του UTRAN, λαμβάνοντας υπόψη την κινητικότητα του χρήστη μέσα στο UTRAN και τον τύπο της κίνησης ή των RAB(s) που αυτό χρησιμοποιεί.

Η φύση της κίνησης στο UMTS δίκτυο είναι διαφορετική από τον παραδοσιακό τύπο της κίνησης της μεταγωγής κυκλώματος. Αυτό σημαίνει ότι το UTRAN είναι ικανό να μοιράσει τις ραδιο πηγές για τα RABs που έχουν διαφορετικό QoS.

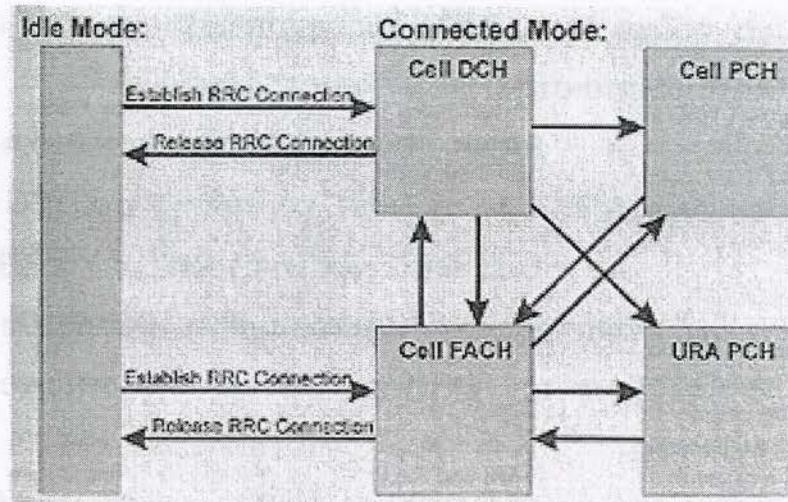
Ο ακρογωνιαίος λίθος του UTRAN level mobility βασίζεται στο κελί, UTRAN Registration Area(URA), Radio Network Temporary Identifier(U-RNTI) και το RRC model. Ένα **URA** καθορίζεται σαν μια περιοχή που καλύπτεται από έναν αριθμό κελιών. Είναι μόνο εσωτερικά γνωστό στο UTRAN και δεν είναι ορατό από το CN. Αυτό σημαίνει ότι όποτε το UE έχει μια σύνδεση RRC η θέση του είναι γνωστή από το UTRAN στο επίπεδο ενός URA. Κάθε φορά που το UE μπαίνει σε ένα νέο URA πρέπει να εκτελέσει μια procedure αναβάθμισης URA.

Βασιζόμενοι στην 3GPP TS 25.401 Radio Network Temporary Identities(RNTI) που χρησιμοποιούν οι UE χρήστες στο UTRAN, θα πρέπει

να πούμε ότι η **RNTI** χρησιμοποιείται για να διαχειρίζεται την εσωτερική κινητικότητα στο UTRAN και περιλαμβάνει:

- SRNC RNTI (S-RNTI): τοποθετείται σε συνεργασία με την σύνδεση RRC από το SRNC και επίσης το SRNC μπορεί να φτάσει το UE.
- Drift RNC RNTI (D-RNTI): τοποθετείται από το DRNC σε συνεργασία με την εγκατεστημένη βάση και χρησιμοποιείται για να διαχειρίζεται την σύνδεση UE και την υπάρχουσα βάση πάνω στο Iur interface.
- Cell RNTI (C-RNTI): τοποθετείται όταν το UE έχει πρόσβαση σε ένα νέο κελί, είναι ένας CRNC ειδικός ανιχνευτής και χρησιμοποιείται για να αναγνωρίσει το CRNC σε ποιο το UE έχει την σύνδεση RRC. Έτσι το UE μπορεί να αναγνωρίσει τον εαυτό του στο CRNC και επίσης το CRNC μπορεί να έχει πρόσβαση στο UE. Αυτός ο ανιχνευτής χρησιμοποιείται όταν το UE είναι στο κανάλι (FACH).
- UTRAN RNTI (U-RNTI): τοποθετείται σε ένα UE που έχει μια σύνδεση RRC και αναγνωρίζει το UE μέσα στο UTRAN. Χρησιμοποιείται σαν ένας ανιχνευτής UE για το πρώτο κελί πρόσβασης όταν μια σύνδεση RRC υπάρχει για αυτό το UE.

Έχοντας καθορίσει τους ρόλους του RNC, των UE ανιχνευτών και του σκεπτικού του URA, η ερώτηση που προκύπτει είναι πώς να το συνδιάσουμε με την κατάσταση transition με σκοπό να διαχειριστεί την εσωτερική κίνηση του UTRAN και του RRM. Οι βασικές αρχές του τρόπου με τον οποίο θα διαχειριζόμαστε τις καταστάσεις transition του RRC φαίνονται στην εικόνα 35 και είναι οι εξής:



Εικόνα 35 Κατάσταση αυτοματισμού του RRC

- **Καμία ραδιο σύνδεση:** η τοποθεσία του UE είναι γνωστή μόνο από το CN. Αυτό σημαίνει ότι οι πληροφορίες τοποθεσίας αποθηκεύονται στο δίκτυο βασιζόμενες στην τελευταία ενέργεια MM που το UE έχει εκτελέσει μαζί με το CN.
- **Ραδιο σύνδεση μέσω κοινών καναλιών:** αν οι ραδιοσυνδέσεις χρησιμοποιούν κοινά κανάλια, για παράδειγμα, τα FACH και CPCH, η τοποθεσία του UE είναι γνωστή σε σχέση με το κελί. Ο τρόπος με τον οποίο αυτές οι πληροφορίες τοποθεσίας ανανεώνονται λέγεται Cell Update Procedure. Αυτή η κατάσταση μπορεί να χρησιμοποιηθεί όταν υπάρχει χαμηλό bit rate data για να μεταφερθεί μεταξύ του UTRAN και του UE.
- **Ραδιο σύνδεση μέσω καναλιών DCHs:** σε αυτήν την περίπτωση το UTRAN έχει τοποθετήσει αφιερωμένες πηγές για την σύνδεση (DPDCH) και τα αφιερωμένα κανάλια φυσικού ελέγχου (DPCCH). Η τοποθεσία του UE είναι γνωστή στο επίπεδο του κελιού. Εξαρτώμενη από τον τύπο της σύνδεσης, διαφορετικές RRC procedures μπορούν να παρουσιαστούν. Αν η αφιερωμένη σύνδεση χρησιμοποιείται για να κουβαλήσει μια υπηρεσία χρησιμοποιώντας την υψηλότερη κλάση QoS (για παράδειγμα φωνητική κλήση μεταγωγής κυκλώματος) το UTRAN και το UE παράγουν handovers. Αν η υπηρεσία που κουβαλά η ραδιο σύνδεση

χρησιμοποιεί την χαμηλότερη κλάση QoS (για παράδειγμα web surfing, allowing buffering and delays) τα handovers μπορεί να μην ολοκληρώνονται έτσι. Αντίθετα, το UE χρησιμοποιεί την procedure Cell Update για να ενημερώσει το UTRAN σχετικά με την τοποθεσία του για παράδειγμα το μέρος όπου πρέπει να μεταφερθούν τα δεδομένα μέσω της ραδιοσύνδεσης.

- **Ραδιοσύνδεση στην κυψέλη PCH:** Όταν το UE είναι στο κελί FACH ή το κελί PCH αλλά δεν υπάρχουν data για να μεταφερθούν, η κατάσταση του UE αλλάζει στο κελί PCH στο οποίο μπορεί να δει τις περιπτώσεις σελιδοποίησης βασισμένες στους καθορισμένους κύκλους Discontinuous Reception (DRX) και έτσι ακούν το κανάλι σελιδοποίησης. Σε αυτήν την περίπτωση η τοποθεσία του UE είναι γνωστή στο accuracy ενός μονού καναλιού και μερικές φορές καλείται κελί βάσης.

- **Ραδιοσύνδεση στη κατάσταση URA PCH:** Όταν το UE είναι στο κελί FACH ή στο κελί DCH και δεν υπάρχουν δεδομένα να μεταφερθούν μεταξύ του UE και του UTRAN ή η κινητικότητα στο UE είναι υψηλή τότε το UE μπορεί να μεταφερθεί στο URA PCH με σκοπό να αποφευχθεί η περιοδική αναβάθμιση του κελιού και για να απελευθερώσει τις αφιερωμένες πηγές. Σε αυτήν την περίπτωση η τοποθεσία του UE είναι γνωστή μόνο σε ένα επίπεδο URA κι έτσι με σκοπό να κρατηθεί η θέση του κελιού το UE πρέπει να σελιδοποιηθεί από το UTRAN/RNC. Μια τέτοια περίπτωση είναι όταν χρησιμοποιείται η μέθοδος τοποθέτησης με βάση το κελί.

- **Idle mode:** Όταν το UE και το UTRAN δεν έχουν καμία ραδιοσύνδεση για παράδειγμα όταν το UE είναι κλειστό. Σε αυτήν την περίπτωση RRC το δίκτυο δεν έχει κανένα είδος πληροφοριών που να αφορούν την τοποθεσία του UE.

4.3.3.6 Χειρισμός της Βάσης Δεδομένων

Οι πληροφορίες σε μια βάση δεδομένων ενός ραδιοδικτύου μπορούν να κατηγοριοποιηθούν ως εξής:

- **Πληροφορίες Αναγνώρισης του κελιού:** Κωδικοί, αριθμός ID του κελιού, Περιοχή θέσης του ID του κελιού και Περιοχή Routing ID του κελιού.
- **Πληροφορίες Ελέγχου Ισχύος:** επιτρεπόμενα επίπεδα ισχύος στις κατευθύνσεις uplink και downlink μέσα στην περιοχή κάλυψης του κελιού.
- **Πληροφορίες σχετικά με τα Handovers:** η ποιότητα της σύνδεσης και οι παράμετροι που σχετίζονται με την κίνηση που εμποδίζουν την πρόοδο του handover για το UE.
- **Πληροφορίες Περιβάλλοντος:** οι πληροφορίες για τα γειτονικά κελιά (και στο GSM και στο WCDMA). Αυτές οι λίστες κελιών μεταφέρονται στο UE και το UE κάνει τις μετρήσεις για το ραδιο περιβάλλον σαν μια πρωταρχική δουλειά για τα handovers.

4.3.3.7 Θέση του UE

Μια άλλη σημαντική λειτουργία που διαχειρίζεται το RNC είναι να ελέγχει το μηχανισμό τοποθέτησης του UE στο UTRAN. Επιλέγει την κατάλληλη μέθοδο τοποθέτησης και ελέγχει πως η μέθοδος τοποθέτησης εκτελείται μέσα στο UTRAN και μέσα στο UE. Επίσης, επαναδιοργανώνει τις πηγές του UTRAN που περιλαμβάνονται στην τοποθεσία που βρίσκεται το UE.

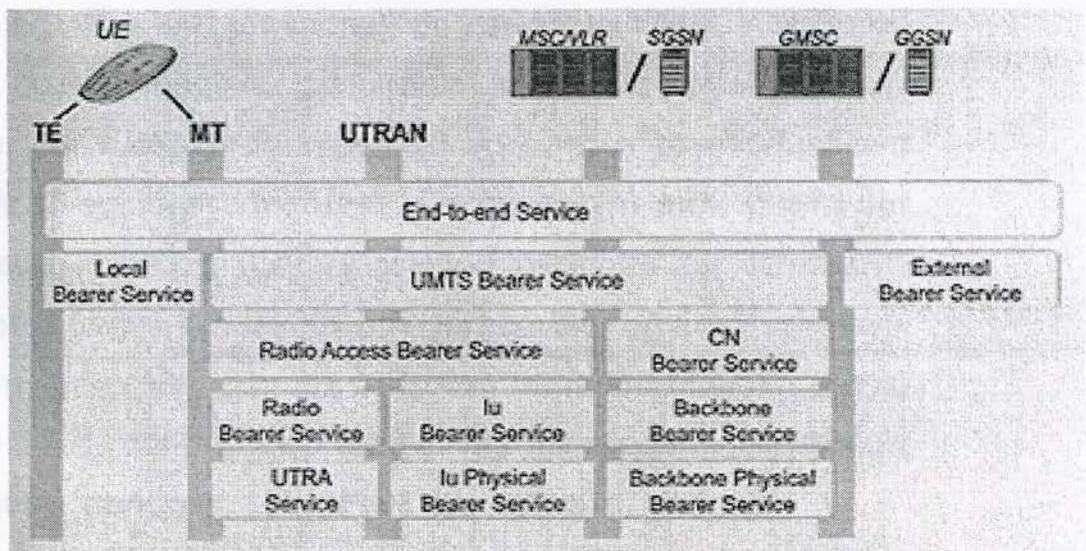
Στις μεθόδους τοποθέτησης που βασίζονται στο δίκτυο το RNC υπολογίζει την θέση και δείχνει την accuracy που έχει επιτευχθεί. Επίσης ελέγχει ένα αριθμό από τις θέσεις και τις Μονάδες Μέτρησεις/BSs (LMUs/BSs) με σκοπό τον καθορισμό των ραδιο μετρήσεων για να τοποθετηθεί ή να βοηθήσει να βρει την θέση του το UE.

Κεφάλαιο 5 Ασύρματο Δίκτυο UMTS

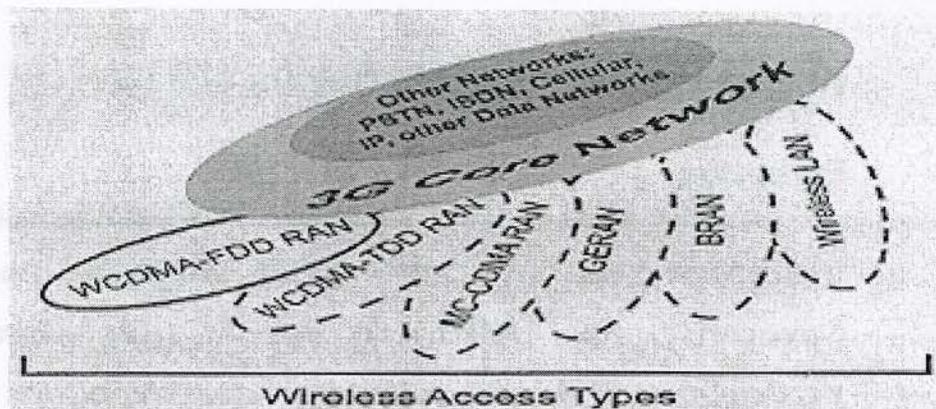
Εισαγωγή

Το UMTS Core Network (CN) μπορεί να θεωρηθεί ως η πλατφόρμα όλων των επικοινωνιακών υπηρεσιών που παρέχονται στους διαχειριστές του UMTS. Οι βασικές τηλεπικοινωνιακές υπηρεσίες περιλαμβάνουν κλήσεις μεταγωγής κυκλώματος και routing δεδομένων πακέτου.

Το CN τοποθετεί τις απαιτήσεις της end-to-end Ποιότητας της Υπηρεσίας(QoS) στην bearer υπηρεσία του UMTS. Όταν οι απαιτήσεις QoS συνδέονται εσωτερικά με τα άλλα δίκτυα χρειάζεται επίσης να τοποθετηθούν πανω στο διαθέσιμη εξωτερική bearer υπηρεσία. Αυτός ο ρόλος της πύλης του UMTS CN φαίνεται στην εικόνα 36.



Εικόνα 36 Αρχιτεκτονική του Bearer and του QoS architecture στο CN

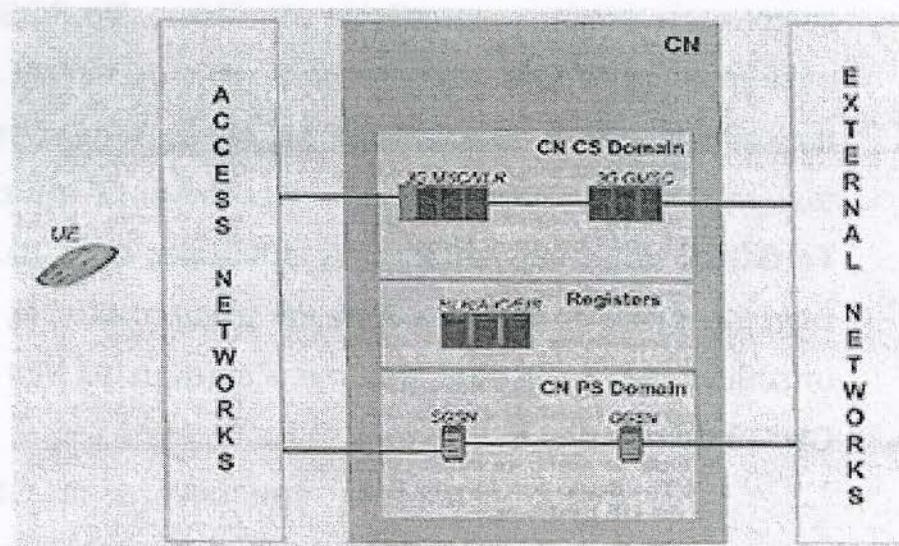


Εικόνα 37 Παγκόσμιο Δίκτυο για ασύρματη πρόσβαση

5.1 Αρχιτεκτονική του CN στο 3GPP R99

Η πρώτη version των προδιαγραφών του UMTS, η 3GPP R99, μας παρουσιάζει ένα σύστημα το οποίο έχει μια ραδιο πρόσβαση ευρείας μετάδοσης και το CN συμπεριλαμβάνεται και στο GSM. Αυτό σημαίνει, ότι η αρχική πλατφόρμα GSM με προεκτάσεις GPRS για υπηρεσίες δεδομένων πακέτων πρέπει να χρησιμοποιείται όσο πιο αποτελεσματικά γίνεται. Αυτή είναι μια προφανής εκτίμηση αφού κάθε κομμάτι περιλαμβάνει τα κόστη που θα πραγματοποιηθούν για την εγκατάσταση του UMTS. Από την στιγμή που το υποσύστημα του δικτύου GSM/GPRS είναι ικανό να παράσχει βασικές υπηρεσίες επικοινωνίας τόσο για την κίνηση μεταγωγής κυκλώματος όσο και για την κίνηση μεταγωγής πακέτου με ένα πλούσιο προμηθευτικό υλικό και προστιθέμενες υπηρεσίες, και έτσι προκύπτει μια προφανής επιλογή για την βάση του UMTS CN.

Επίσης, στο CN της 3GPP R99 η κίνηση μπορεί να είναι είτε μεταγωγής κυκλώματος είτε μεταγωγής πακέτου. Και οι δυο τύποι κίνησης απαιτούν μερικές συγκεκριμένες ρυθμίσεις και αυτό γίνεται γιατί το CN είναι εξαρχής διαιρεμένο σε δυο βάσεις, την βάση της μεταγωγής κυκλώματος (CS domain) και βάση μεταγωγής πακέτου (PS domain). Η CN αρχιτεκτονική φαίνεται στην εικόνα 38.



Εικόνα 38 Αρχιτεκτονική του CN

Το CN CS Domain έχει δυο βασικά δικτυακά στοιχεία που μπορούν να συνδιαστούν: το Mobile Switching Centre/Visitor Location Register (MSC/VLR) και το Gateway Mobile Switching Centre (GMSC). Το πρώτο στοιχείο είναι υπεύθυνο για την διαχείριση των ενεργειών της σύνδεσης μεταγωγής κυκλώματος για την διαχείριση της κινητικότητας (MM) που σχετίζεται με θέματα όπως η αναβάθμιση της θέσης, η εγκατάσταση της θέσης, η σελιδοποίηση και οι λειτουργίες ασφάλειας. Το δεύτερο στοιχείο αναλαμβάνει τις εισερχόμενες και εξερχόμενες συνδέσεις προς και από άλλα δίκτυα. Από την άποψη της διαχείρισης της σύνδεσης, το GMSC εγκαθιστά ένα μονοπάτι κλήσης προς το παρεχόμενο MSC/VLR κάτω από το οποίο θα βρεθεί ο διευθετημένος πάροχος. Από την άποψη του MM, το GSMC καθορίζει μια procedure για ανίχνευση θέσης η οποία έχει σκοπό να βρει το σωστό MSC/VLR για την σύνδεση της κλήσης.

Το **MSC/VLR** περιλαμβάνει τους μετατροπείς που απαιτούνται για την μετατροπή του κώδικα ομιλίας. Η καταπληκτική διαφορά εδώ είναι ότι οι προδιαγραφές του GSM οι μετατροπείς κώδικα θεωρούνται σαν ένα κομμάτι του ραδιο δικτύου, στη 3G είναι ένα κομμάτι του CN.

Το **CN PS domain** έχει επίσης δυο βασικά στοιχεία του δικτύου κινητής τηλεφωνίας, τα Serving GPRS Support Node (SGSN) και το Gateway GPRS Support Node (GGSN). Το **SGSN node** υποστηρίζει την

επικοινωνία πακέτων κατευθείαν στο δίκτυο. Το SGSN node είναι κυρίως υπεύθυνο για θέματα σχετιζόμενα κυρίως με το MM όπως η αναβάθμιση της routing area, η εγκατάσταση της θέσης, η σελιδοποίηση και ο έλεγχος των μηχανισμών ασφάλειας που σχετίζονται με την επικοινωνία πακέτων. Το **GGSN node** περιλαμβάνει τις συνδέσεις προς άλλα δίκτυα μεταγωγής πακέτων όπως το Internet. Από την πλευρά του CN, το GGSN node είναι υπεύθυνο για τα θέματα που σχετίζονται με το MM όπως το GMSC στο CN CS domain.

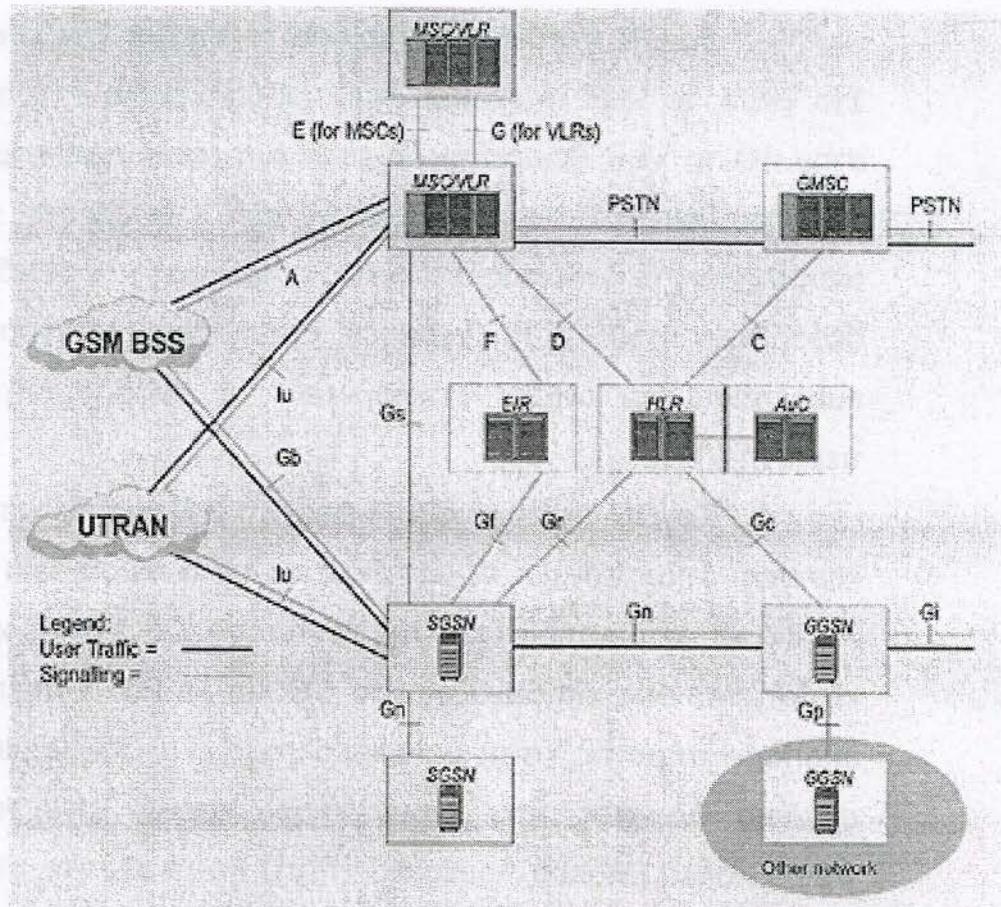
Το δίκτυο μεταφοράς που συνδέει τα GSNs μαζί λέγεται IP backbone ή Intranet. Γι' αυτό το λόγο το IP backbone διαχωρίζεται από τα άλλα δίκτυα με την λειτουργία των firewalls. Για το IP backbone το PS domain πρέπει επίσης να περιέχει ένα Domain Name Server(DNS). Έτσι, τα SGSN και GGSN είναι ικανά να παράγουν routing και επίσης αυτά μπορεί να ανήκουν σε διαφορετικά δίκτυα.

Στην εικόνα 38 οι Registers περιλαμβάνουν το Home Location Registry (HLR), το Authentication Centre (AuC) και το Equipment Identity Register (EIR). Αυτό το κομμάτι του CN δεν παραδίδει κίνηση. Αντίθετα περιλαμβάνει τις πληροφορίες διεύθυνσης και ταυτότητας και για το CS και για το PS domain το οποίο απαιτείται για παράδειγμα στις procedures που είναι σχετικές με το MM. Το **HLR** περιλαμβάνει προσωρινά δεδομένα του παροχέα. Ένας παροχέας μπορεί πάντα να συνδεθεί με ένα μόνο HLR. Το HLR είναι υπεύθυνο για τις procedures που σχετίζονται με το MM.

Το **AuC** είναι μια βάση δεδομένων δημιουργημένη από τους Authenticated Vectors. Αυτοί περιέχουν τις παραμέτρους ασφαλείας τη χρήση των VLR και SGSN για λειτουργίες ασφαλείας που εκτελούνται στο lu interface. Δουλεύει μαζί με το HLR και χρησιμοποιούν το ίδιο πρωτόκολλο MAP για τη μεταφορά των πληροφοριών. Η ασφάλεια είναι ένα κομμάτι του MM. Το EIR περιλαμβάνει πληροφορίες αναγνώρισης που σχετίζονται με το hardware της συσκευής UE.

Το CN περιλαμβάνει ακόμα το **Visitor Location Register(VLR)**. Στο GSM, το VLR το έχουμε χειριστεί ξεχωριστά στις προδιαγραφές αλλά στην 3G το VLR θεωρείται ότι είναι ένα εσωτερικό κομμάτι του MSC. Το VLR συμμετέχει στις procedures που σχετίζονται με το MM όπως αναβάθμιση τοποθεσίας, ενέργειες ασφάλειας και σελιδοποίησης. Η βάση δεδομένων του VLR περιέχει προσωρινά αντίγραφα των ενεργών subscribers, οι οποίοι εκτελούνται στην αναβάθμιση τοποθεσίας στην περιοχή VLR.

Το CN περιέχει δυο διαφορετικά domains για την μεταφορά της κίνησης, όπως είπαμε παραπάνω, και αυτά τα domain λαμβάνουν υπόψη τα ειδικά χαρακτηριστικά της κίνησης. Τα ειδικά χαρακτηριστικά της κίνησης επίσης επηρεάζουν το CS και το PS domain και περαιτέρω τα interface σήματος και η μεταφορά τους. Το CS domain χρησιμοποιεί τα σενάρια σήματος που έχουν κληρονομηθεί από το GSM στο MAP πρωτόκολλο (Mobile Application Part) που καλύπτει οποιοδήποτε add-ins στο UMTS που φέρεται στο σύστημα. Στην εικόνα 39 αυτά τα κληρονομηθέντα interfaces είναι σημειωμένα με κεφαλαία σύμφωνα με τους κανόνες του MAP interface. Αυτά τα interfaces ακολουθούν τις ίδιες αρχές που χρησιμοποιούνται ήδη στο σύστημα GSM.



Εικόνα 39 Το interface του CN στην 3GPP R99

5.2 Διαχείριση Κινητικότητας (MM)

Η κατανόηση της σημασίας της κινητικότητας κάνει τον σχεδιασμό των δικτύων κινητικότητας αρκετά δύσκολο από τις ήδη υπάρχουσες τηλεπικοινωνίες και δημιουργεί πολλές ελπίδες για εντελώς διαφορετικές υπηρεσίες για τους τελικούς χρήστες.

Ας ξεχωρίσουμε την διαφορά μεταξύ των δυο βασικών εννοιών που σχετίζονται με την κινητικότητα των χρηστών:

- **Location:** χρησιμοποιείται για να αναφερθεί στην τοποθεσία του τελικού χρήστη (και του τερματικού του) μέσω της λογικής δομής του δικτύου. Τα στοιχεία αναγνώρισης μέσα στα οποία είναι η λογική δομή είναι τα κελιά και οι περιοχές των ομάδων-κελιών. Με τον όρο περιοχή δεν εννοούμε απαραίτητα τον γεωγραφικό τόπο των κελιών που γειτονεύουν

αλλά συμπεριλαμβάνει τον διαχειριστή δικτύου για τις περιπτώσεις διαχείρισης του δικτύου.

- **Position:** αναφέρεται στη γεωγραφική θέση του τελικού χρήστη (και του τερματικού του) μέσα στην περιοχή κάλυψης του δικτύου. Η γεωγραφική θέση δίνεται σαν ένα ζευγάρι συγκεκριμένων συντεταγμένων. Όταν δεν μπορεί να βρεθεί η γεωγραφική θέση η θέση μπορεί να δίνεται, σαν μια ταυτότητα ενός κελιού, από το οποίο η θέση μπορεί να καθοριστεί, για παράδειγμα οι γεωγραφικές συντεταγμένες του BS που ελέγχει το συγκεκριμένο κελί.

5.2.1 Ταυτότητες και Διευθύνσεις των χρηστών και των τερματικών

Οι σκοποί των διαφορετικών ταυτοτήτων που χρησιμοποιούν οι χρήστες του UMTS μπορούν να περιληφθούν στα εξής:

- **Μοναδική Ταυτότητα:** χρησιμοποιείται για να προβάλει μια παγκόσμια μοναδική ταυτότητα για τον χρήστη. Αυτή η τιμή λειτουργεί σαν πρωταρχικό κλειδί για όλους τους χρήστες δίνοντας σημασία στις πληροφορίες των χρηστών και επίσης χρησιμοποιείται σαν βάση για περιπτώσεις χρέωσης.

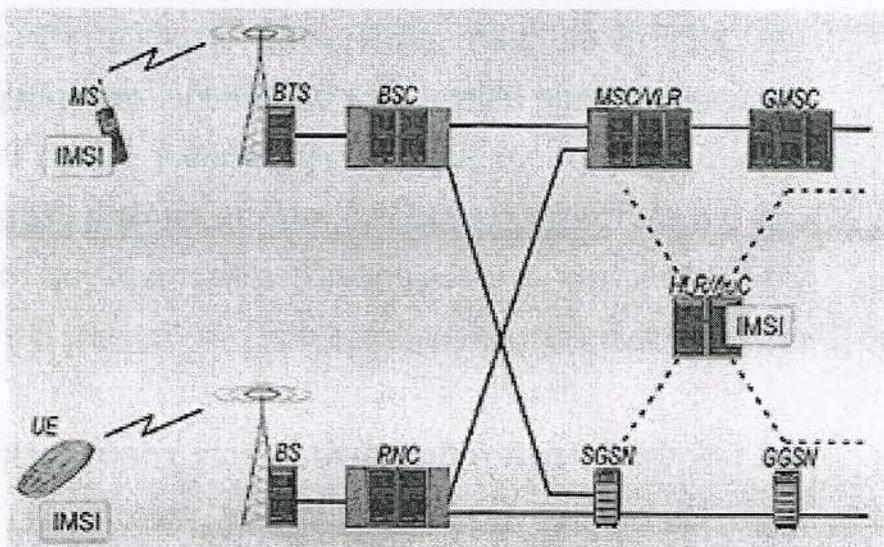
- **Διαχωρισμός Υπηρεσιών:** χρησιμοποιείται ειδικά στις περιπτώσεις των μεταβολών (transaction) του τερματικού-κινητού ή υπηρεσίας που θα χρησιμοποιείται και θα πρέπει να αναγνωρισθεί. Αυτό γίνεται χρησιμοποιώντας μια ταυτότητα που έχει σχέση με την μοναδική ταυτότητα του χρήστη.

- **Σκοποί routing:** μερικοί ειδικοί κανονισμοί απαιτούνται με σκοπό να παρουσιάζουν transaction routing το οποίο δεν ταιριάζει σε κανένα άλλο δίκτυο.

- **Ασφάλεια:** είναι ένα πολύ σημαντικό ζήτημα για το κυψελοειδές σύστημα και αυτό γιατί προσαρμόζονται επιπλέον ταυτότητες για να βελτιώσουν την ατομικότητα των χρηστών. Αυτές οι ταυτότητες είναι προαιρετικές αλλά είναι καλύτερα να τις χρησιμοποιούμε πάντα.

Αυτή η μοναδική ταυτότητα του χρήστη-κινητού τηλεφώνου ονομάζεται International Mobile Subscriber Identity (IMSI).

$$\text{IMSI} = \text{MCC} + \text{MNC} + \text{MSN}$$



Εικόνα 40 Παγκόσμιες Ταυτότητες Χρηστών Κινητής Τηλεφωνίας (IMSI)

Το MSC είναι κωδικός χώρας για τα κινητά (3 ψηφία)

Το MNC είναι κωδικός δικτύου για τα κινητά (2-3 ψηφία)

Το MSN είναι ο αριθμός του χρήστη (9-10 ψηφία). Αυτός ο αριθμός αποθηκεύεται στην κάρτα SIM (USIM).

Το **IMSI** λειτουργεί σαν ένα πρωταρχικό κλειδί σε μια βάση δεδομένων στο HLR, VLR, AuC, SGSN. Αυτός ο αριθμός ακολουθεί τις προδιαγραφές της ITU-T με αριθμό E.214. Ο αριθμός IMSI χρησιμοποιείται για την ακριβή αναγνώριση του χρήστη. Όταν ο χρήστης κάνει roaming έξω από το δίκτυο βάση, το νέο δίκτυο είναι ικανό να αναγνωρίζει το δίκτυο-βάση ζητώντας από το UE να προβάλλει αυτόν τον αριθμό.

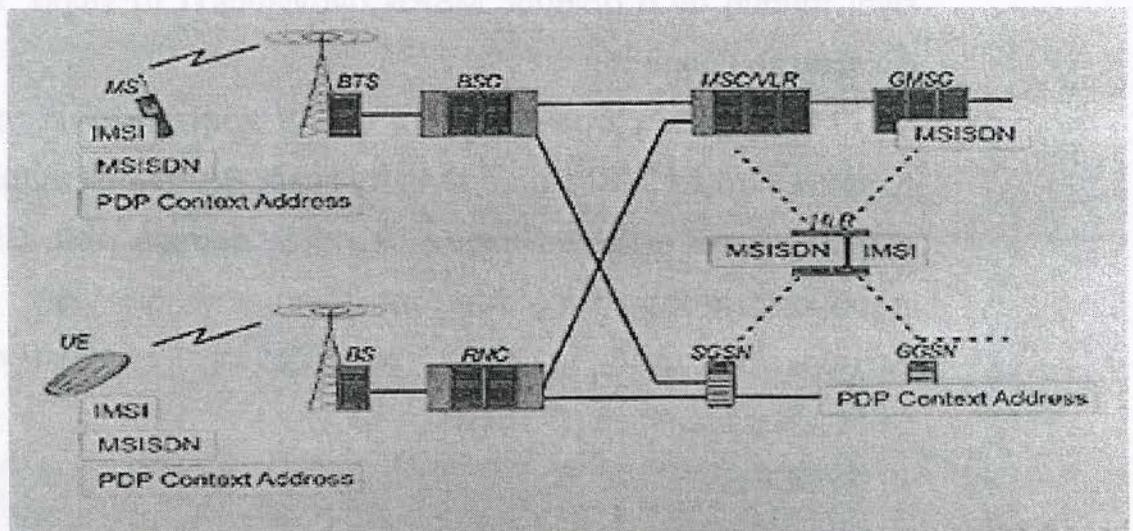
Το **MSISDN** χρησιμοποιείται για των διαχωρισμό των υπηρεσιών. Επειδή ένας χρήστης μπορεί να έχει ενεργοποιήσει πολλές φορές την ίδια υπηρεσία ο αριθμός αυτός λειτουργεί σαν ένα διαχωριστικό μεταξύ αυτών των υπηρεσιών. Για παράδειγμα, ο χρήστης κινητής τηλεφωνίας μπορεί να

έχει ένα μόνο MSISDN αριθμό για την υπηρεσία ομιλίας, έναν άλλο αριθμό για κάποια άλλη υπηρεσία και συνεχίζεται. Το MSISDN αποτελείται από τρία κομμάτια:

$$\text{MSISDN} = \text{CC} + \text{NDC} + \text{SN}$$

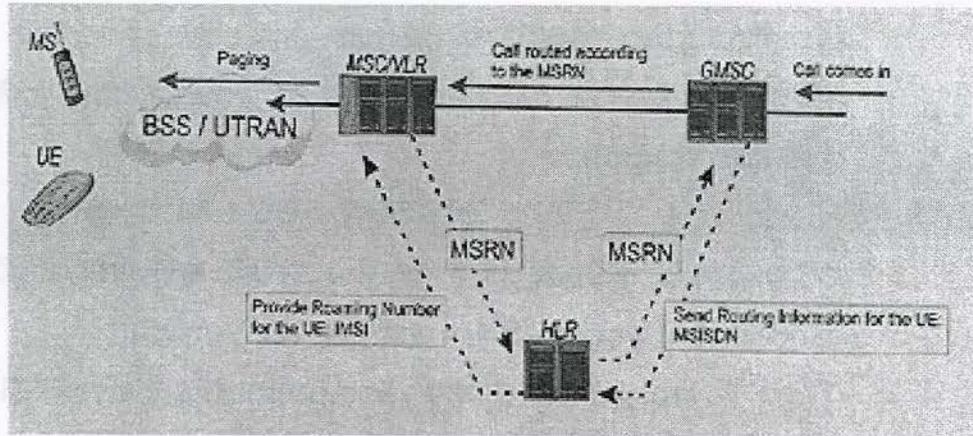
CC=κώδικος χώρας (1-3 ψηφία), **NDC** =εθνικός κωδικός κατάληξης της κλήσης (1-3 ψηφία), **SN** = αριθμός του χρήστη

Το πρωτόκολλο που χρησιμοποιείται για το MSISDN είναι το Packet Data Protocol (PDP) το οποίο είναι μια IP διεύθυνση για το χρήστη κινητής τηλεφωνίας. Η διεύθυνση PDP μπορεί να είναι είτε δυναμική είτε στατική. Αν είναι δυναμική, δημιουργείται όταν θα δημιουργηθεί μια ακολουθία πακέτων ενώ αν είναι στατική καθορίζεται από το HLR.



Εικόνα 41 Αριθμός ISDN του χρήστη κινητής τηλεφωνίας (MSISDN)

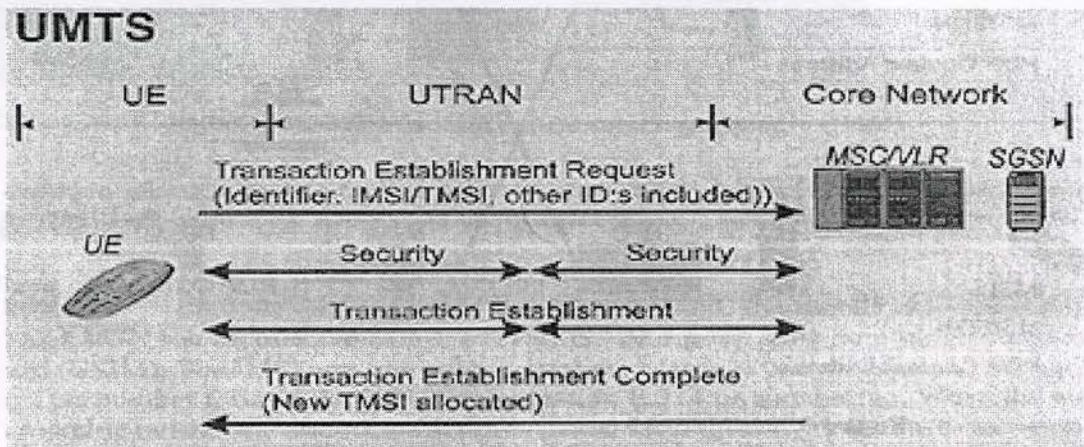
Ο Mobile Subscriber Roaming Number (MSRN) χρησιμοποιείται για τις κλήσεις routing (ΕΙΚΟΝΑ 42). Ο τύπος του MSRN είναι ίδιος με αυτόν του MSISDN, αποτελείται από τρία κομμάτια CC, NDC, SN και ακολουθεί τις προδιαγραφές E.164.



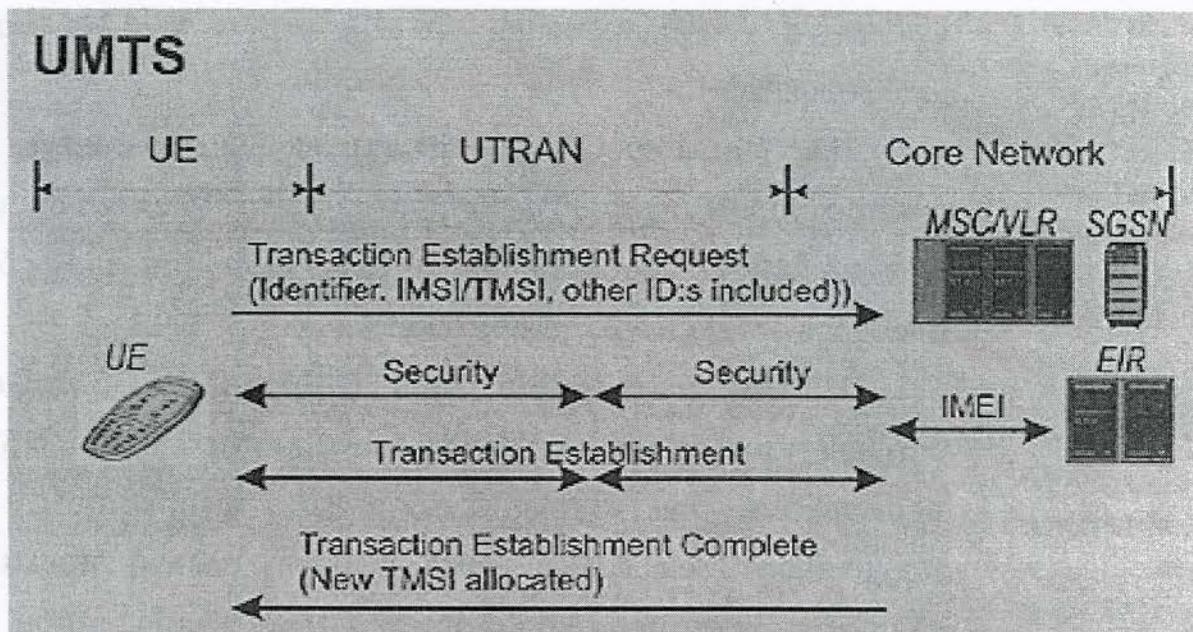
Εικόνα 42 Αριθμός Roaming για τον χρήστη κινητής τηλεφωνίας (MSRN)

Το MSRN χρησιμοποιείται για την σύνδεση του κινητού τερματικού για την κλήση μεταξύ της πύλης MSC και των MSC/VLR. Αυτή η σύνδεση είναι πιθανή αν ο αριθμός MSRN αναγνωρίζει τη χώρα, το δίκτυο και τα στοιχεία του δικτύου.

Για λόγους ασφαλείας το UMTS χρησιμοποιεί το TMSI αντι για το IMSI γιατί το IMSI για να είναι ασφαλές θα πρέπει να μετακινείται πολύ γρήγορα στο ciphered mode. Το PS domain του CN χρησιμοποιεί παρόμοιες προσωρινές ταυτότητες για τον ίδιο λόγο. Με σκοπό να διαχωριστούν από το TMSI, ονομάζονται Packet Temporary Mobile Subscriber Identities (P-TMSIs).



Εικόνα 43 Θέση της ταυτότητας του προσωρινού χρήστη κινητής τηλεφωνίας (TMSI)



Εικόνα 44 Παγκόσμια ταυτότητα εξοπλισμού κινητής τηλεφωνίας (IMEI)

5.2.2 Δομές Θέσεων και ταυτότητες τους.

Το MM απαιτεί μια λογική δόμηση του δικτύου UMTS. Η λογική δομή αντιπροσωπεύεται με λογικά κομμάτια του τρέχοντος δικτύου. Αυτές οι λογικές οντότητες συμπεριφέρονται σαν ένας χάρτης για τις procedures MM. Το UMTS συμπεριλαμβάνει τέσσερα επίπεδα λογικών καθορισμών τα οποία είναι:

- Location Area (LA)
- Routing Area (RA)
- UTRAN Registration Area (URA)
- Cell

LA: είναι μια περιοχή όπου το UE μπορεί να κινείται χωρίς να εκτελείται η procedure location. Το LA αποτελείται από κελιά, το ελάχιστο είναι ένα κελί και το μεγαλύτερο είναι όλα τα κελιά κάτω από ένα VLR. Ένα RNC μπορεί να έχει πολλά LA ή ένα LA το οποίο μπορεί να καλύπτει πολλά RNCs. Κάθε LA αναγνωρίζεται από το Location Area Identity (LAI).

$$\text{LAI} = \text{MCC} + \text{MNC} + \text{LAcod}e$$

Τα MNC, MCC είναι ίδια με τον αριθμό IMSI. Ο αριθμός LAI είναι ένας αριθμός μοναδικός παγκοσμίως και μέσα στο ίδιο δίκτυο το ίδιο LA δεν

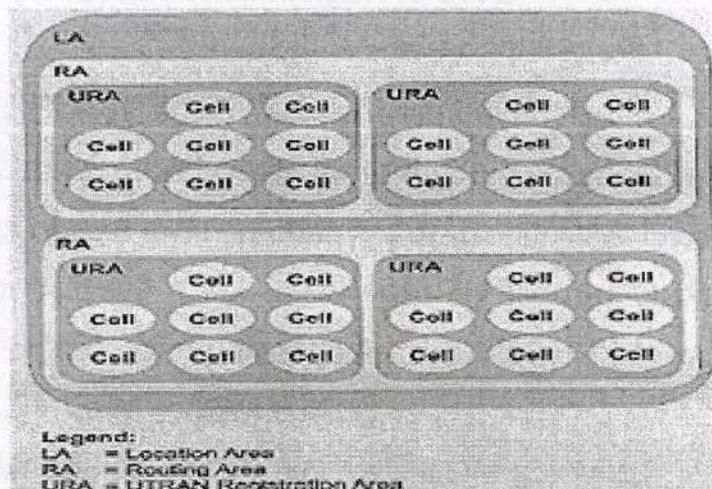
πρέπει να επαναλαμβάνεται. Το UE ακούει το LAIs από το κανάλι μεταφοράς BCH.

RA: Όπως το CN CS domain, το PS domain έχει την δική του εγκατάσταση θέσης που βασίζεται στο RA. Το RA είναι παρόμοιο με το LA. Ένα LA μπορεί να έχει πολλά RAs μέσα του αλλά δεν ισχύει το αντίστροφο. Ένα RA ανήκει σε δύο LA.

UTRAN Registration Area (URA): Στο GSM δίκτυο το MM διαχειρίζεται ολοκληρωτικά μεταξύ του τερματικού και του NSS. Το UTRAN περιλαμβάνει την τοπική εγκατάσταση κινητικότητας, μια UTRAN Registration Area (URA). Αυτή η μικρή αλλαγή προκαλεί αξιόλογες αλλαγές στην εσωτερική δομή του SGSN και εξαιτίας αυτού, το 3^{ης} γεννιάς SGSN περιλαμβάνει την λειτουργικότητα και της 2^{ης} και της 3^{ης} γεννιάς SGSN.

Cell: Το μικρότερο τμήμα που χρησιμοποιείται για την εσωτερική οντότητα το MM είναι ένα κελί-κυψέλη. Η κυψέλη στην domain access είναι η μικρότερη οντότητα που έχει την δική του ορατή από όλους ταυτότητα που λέγεται Cell ID (CI). Όπως ο κωδικός του LA όσο και το CI είναι ένας αριθμός, ο οποίος πρέπει να είναι μοναδικός μέσα στο δίκτυο. Για να διαχωριστούν τελείως τα κελιά μεταξύ τους, η ταυτότητα που πρέπει να χρησιμοποιηθεί ονομάζεται Cell Global Identity (CGI).

$$\text{CGI} = \text{MNC} + \text{MCC} + \text{LAcod}e + \text{CI}$$



Εικόνα 45 MM λογικές οντότητες και οι σχέσεις τους

5.2.3 Μοντέλο Διαχείρισης Κινητικότητας

5.2.3.1. Καταστάσεις MM σε κόμβο μεταγωγής κυκλώματος

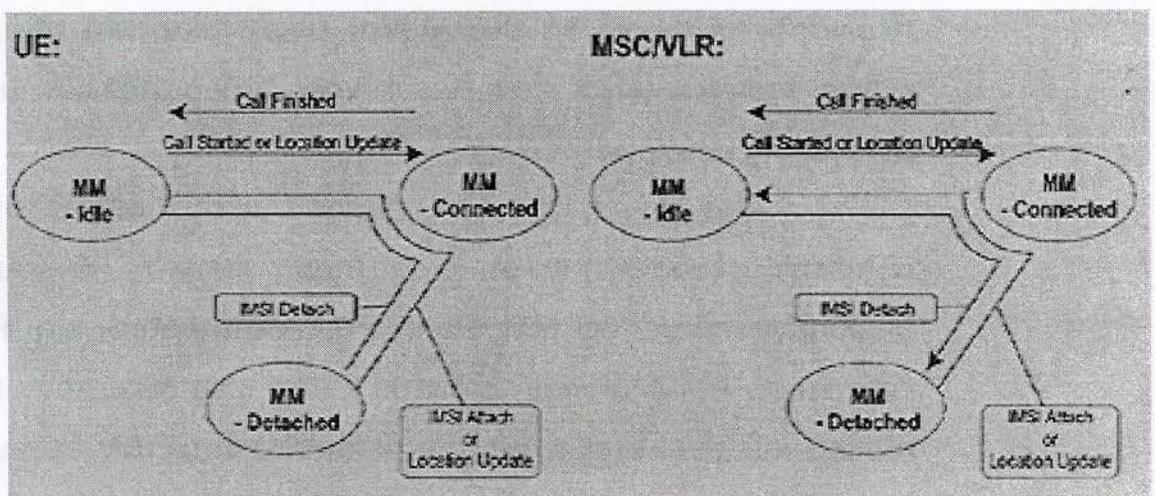
Από την πλευρά του MM, ένα τερματικό μπορεί να έχει 3 καταστάσεις: το MM-detached, το MM-idle και το MM-connected. Αυτές οι καταστάσεις δείχνουν πως η θέση του τερματικού είναι γνωστή όταν συγκρίνεται με την λογική δομή που παρουσιάζεται στην εικόνα 45.

MM-detached state: το δίκτυο δεν ενδιαφέρεται για το τερματικό και τον χρήστη καθόλου. Χρησιμοποιούμε την κατάσταση αυτή ,π.χ. όταν το τερματικό είναι κλειστό.

MM-idle state: το δίκτυο γνωρίζει την θέση του τερματικού-χρήστη με την βοήθεια του LA.

MM-connected state: το δίκτυο γνωρίζει την θέση του τερματικού με την βοήθεια του κελιού.

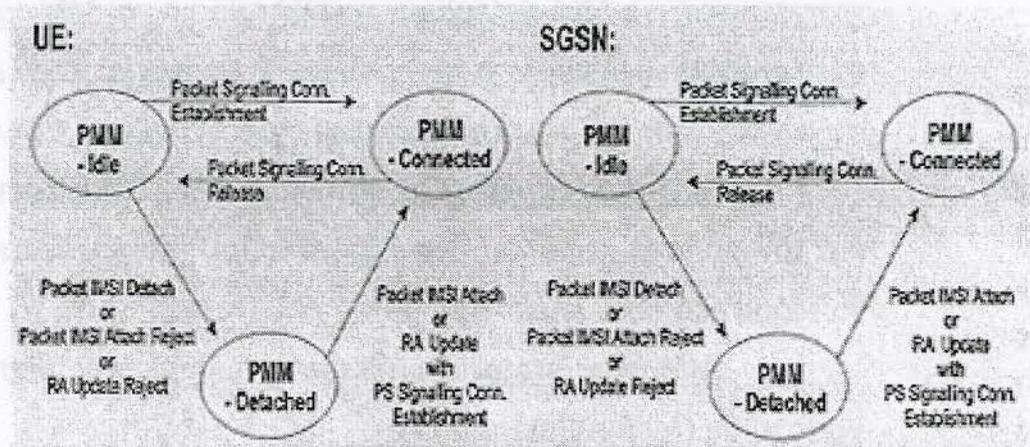
Οι καταστάσεις αυτές είναι ίδιες τόσο για το GSM NSS όσο και στο UMTS CS domain ακολουθώντας τις προδιαγραφές της 3GPP R99. Η MM state αλλάζει ως εξής: **MM-detached** → **MM-connected** → **MM-idle**. Όταν ένας χρήστης είναι ενεργός, το τερματικό είναι ανοικτό, τότε η MM state βρίσκεται ανάμεσα στις καταστάσεις MM-connected και MM-idle ανάλογα με την χρήση του κινητού: όταν η κλήση ξεκινά η MM state πηγαίνει ως εξής: MM-idle → MM-connected και όταν η κλήση τελειώνει η MM state είναι: MM-connected → MM-idle.



Εικόνα 46 Μοντέλο MM σε μεταγωγή κυκλώματος (MM)

5.2.3.2 Καταστάσεις MM σε κόμβο μεταγωγής πακέτου

Οι καταστάσεις PMM (Packet Mobility Management) είναι ίδιες με πριν αλλά αλλάζει η κίνηση από μια κατάσταση στην άλλη.



Εικόνα 47 Μοντέλο MM σε μεταγωγή πακέτου (PMM)

PMM-detached: το δίκτυο δεν είναι πληροφορημένο για την σύνδεση μεταγωγής πακέτων

PMM-connected: τα δεδομένα μπορούν να μεταφερθούν μεταξύ του τερματικού και του δικτύου. Το SGSN γνωρίζει τις πληροφορίες για την μεταφορά πακέτων με την συνεργασία της routing διεύθυνσης του RNC.

PMM-idle: η θέση είναι γνωστή με την συνεργασία της ταυτότητας της routing περιοχής. Η διαδικασία σελιδοποίησης χρειάζεται με σκοπό να φτάσει το τερματικό, π.χ. η σηματοδότηση.

Από την πλευρά του χρήστη, η σύνδεση μεταγωγής πακέτων περιγράφεται συχνά να είναι πάντα ενεργή και από την άλλη μεριά, μια κλήση πακέτων είναι σαν ένα σύνολο πάρα πολλών μικρών κλήσεων μεταγωγής κυκλώματος.

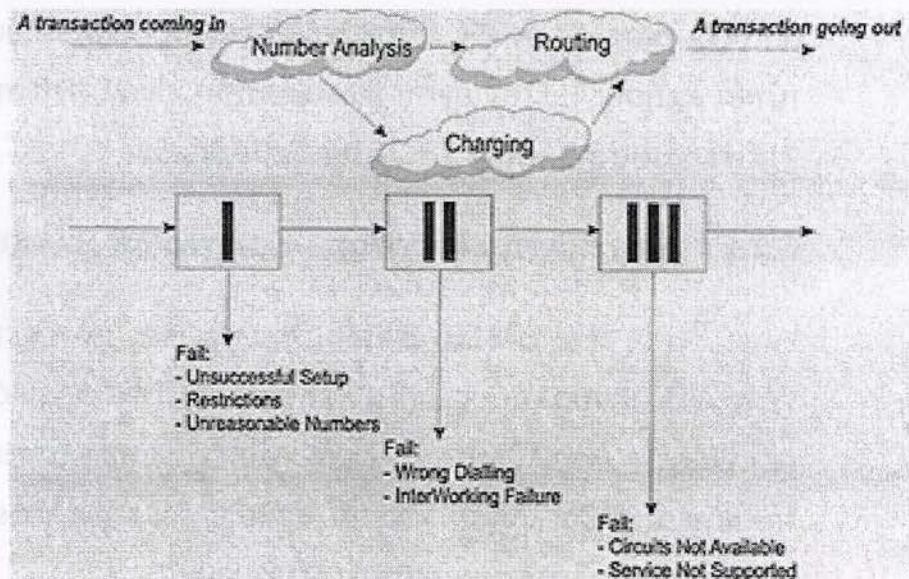
Από την πλευρά του δικτύου, η σύνδεση μεταγωγής πακέτων δίνει την ψευδαίσθηση ότι είναι πάντα ανοικτή. Η ψευδαίσθηση αυτή δημιουργείται με τις MM states: **PMM-connected** και **PMM-idle**. Στην κατάσταση PMM-idle και το δίκτυο και το κινητό κρατούν την πληροφορία routing και είναι έτοιμα για την μεταφορά πακέτων δεδομένων αλλά δεν είναι ικανά να μεταφέρουν πακέτα σε αυτήν την κατάσταση αφού δεν υπάρχει οποιαδήποτε σύνδεση μέσω της πρόσβασης δικτύου.

Όταν ο χρήστης κλείνει το τερματικό του, η MM κατάσταση επιστρέφει στην PMM-detached και οι πληροφορίες routing που παρουσιάζονται στους κόμβους δικτύου δεν είναι έγκυρες πια. Αν για κάποιους λόγους παρουσιαστεί κάποιο λάθος στο περιεχόμενο της σύνδεσης IMSI πακέτων ή στην RA αναβάθμιση.

5.3. Διαχείριση Επικοινωνίας (CM)

5.3.1. Διαχείριση σύνδεσης για την μεταγωγή κυκλώματος

Η διαχείριση της σύνδεσης είναι μια υψηλής ποιότητας λειτουργία που περιγράφει τις λειτουργίες που απαιτούνται για την εισερχόμενη και εξερχόμενη κίνηση μέσα σε ένα switch. Το switch πρέπει να εκτελεί 3 λειτουργίες: την number analysis, την routing και την χρέωση.



Εικόνα 48 Αρχικό διάγραμμα διαχείρισης σύνδεσης μεταγωγής κυκλώματος

Η **Number analysis** είναι μια συλλογή κανόνων για το πως πρέπει να χειριστεί το δίκτυο την μετετροπή. Αυτή ψάχνει να βρεί από τους δυο αριθμούς, τον καλούντα και τον καλούμενο και παίρνει αποφάσεις που βασίζονται στους καθορισμένους κανόνες. Στην Φάση I το switch ελέγχει αν ο αριθμός που καλεί είναι λογικός και αν οποιοσδήποτε περιορισμός όπως η call barring χρησιμοποιείται με τον καλούντα αριθμό.(ΕΙΚΟΝΑ 47). Στην Φάση II το σύστημα επικεντρώνεται στον αριθμό που καλέσθηκε. Η

φύση της επαφής ανιχνεύεται :αν είναι διεθνής ή εθνική κλήση και υπάρχει κανένας routing κανόνας που έχει καθοριστεί για τον καλούμενο αριθμό. Επιπλέον ελέγχει αν η συγκεκριμένη επαφή απαιτεί κάποιο συγκεκριμένο εξοπλισμό (όπως το modem) για να συνδεθεί ή η επαφή είναι χρεώσιμη ή όχι. Επιπλέον γίνονται και οι έλεγχοι για τις στατιστικές σε αυτή την φάση.

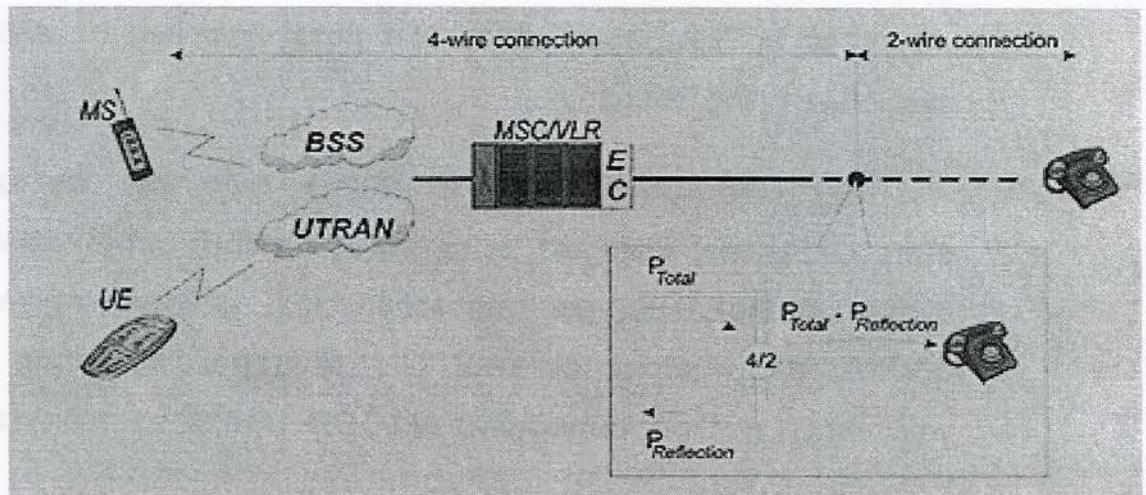
Κατά την διάρκεια της επαφής το switch αποθηκεύει τις πληροφορίες σχετικά με την επαφή και την σύνδεση της και συλλέγει πληροφορίες χρέωσης αν η επαφή έχει κριθεί να είναι χρεώσιμη. Όταν η επαφή τελειώσει η Φάση II αναλαμβάνει να απελευθερώσει όλες τις πηγές που σχετίζονται με την επαφή αυτή.

Ο έλεγχος κλήσης αναγνωρίζει τον τύπο της κλήσης και βασιζόμενος σε αυτόν αποφασίζει για τις περαιτέρω ενέργειες. Οι βασικοί τύποι κλήσης μεταγωγής κυκλώματος είναι: **1)Κανονική κλήση (φωνή)**
2)Επείγουσα κλήση **3)Κλήση δεδομένων**

5.3.1.1 Διαχείριση Σύνδεσης – Εσωτερική εργασία στο δίκτυο

Το UMTS δίκτυο πρέπει να συνδέεται με τα υπάρχοντα γειτονικά δίκτυα όπως το PSTN και το ISDN. Αρχικά, οι κλήσεις δεδομένων μεταγωγής κυκλώματος είναι αυτές που απαιτούν εφαρμογή αλλά πρακτικά κάθε κλήση γίνεται καθώς το κυψελλοειδές δίκτυο απαιτεί να χρησιμοποιούνται εσωτερικές λειτουργίες.

Σήμερα και στο άμεσο μέλλον η κύρια λειτουργία στα κυψελλοειδή δίκτυα είναι ακόμα η φωνή καθώς το κομμάτι της κίνησης που χρησιμοποιείται αναμένεται να μειωθεί. Η φωνή είναι μια απαιτητική υπηρεσία και ο κατάλληλος χειρισμός της απαιτεί μερικές ειδικές ενέργειες όπως η εξαφάνιση της ηχούς. Αυτή απαιτείται κυρίως από τις κλήσεις που έχουν γίνει από το κυψελλοειδές δίκτυο και καταλήγουν στο PSTN. Η εικόνα 48 δείχνει τι γίνεται στο PSTN.



Εικόνα 48 Η δύναμη ανάκλασης και από που προέρχεται αυτή

5.3.1.2. Διαχείριση σύνδεσης - Χρέωση

Το UMTS σύστημα δημιουργεί κάποιες νέες απαιτήσεις που αφορούν την χρέωση. Αυτές οι αλλαγές είναι οι παρακάτω:

- Σύμφωνα με τις αλλαγές στο commercial mode, το σύστημα χρέωσης πρέπει να είναι ικανό να παράγει λεπτομερείς πληροφορίες σε όλο το commercial μοντέλο, π.χ. η χρέωση γίνεται μεταξύ του χρήστη και του δικτύου, το δίκτυο και ο παροχέας των υπηρεσιών και ακόμα μεταξύ του παροχέα υπηρεσίας και του παροχέα content.
- Μηχανισμοί ελέγχου προστίθενται και βελτιώνονται μεταξύ του δικτύου που παρέχει τις υπηρεσίες και του βασικού δικτύου.
- Το κομμάτι χρέωσης μπορεί να ελέγχει τα κόστη. Σημειώνεται ότι έχει ήδη εφαρμοστεί στα αναπτυσσόμενα δίκτυα 2^{ης} γενιάς αλλά στα UMTS δίκτυα θα είναι μια πρωταρχική λειτουργία.
- Ατομικός λογαριασμός πρέπει να είναι διαθέσιμος για κάθε χρήστη και σε κάθε δραστηριότητα. Σημείωση: μια ανοικτή ερώτηση είναι

για το αν θα χρεώσουμε ή όχι μια pure signalling transaction όπως η αναβάθμιση της θέσης.

Το **Call Detail Record (CDR)** είναι μια λεπτομερής λίστα transactions που σχετίζεται με τις πηγές και αυτή παράγεται από το UMTS δίκτυο. Φυσιολογικά, μια transaction, π.χ. η φωνητική κλήση παράγει αρκετές πληροφορίες σε κάθε CN. Η παρακάτω κλήση σκοπεύει να περιγράψει τι είδους αντικείμενα ένα CDR μπορεί να περιέχει:

- Ατομική ταυτότητα χρέωσης: αυτός ο αριθμός IMSI αναγνωρίζει τον χρήστη. Καθορίζει επίσης τα λεγόμενα περιβάλλοντα βάσης. Ο αριθμός IMSI περιέχει την mobile country και τις portion δικτύων.
- Ταυτότητα του τερματικού και κλάση: η ταυτότητα του τερματικού είναι IMEI και η κλάση περιγράφεται στην classmark του κινητού σταθμού. Η classmark του κινητού σταθμού προσδιορίζει την υπηρεσία που χρησιμοποιείται πάνω στο UMTS δίκτυο.
- Καλούμενη Διεύθυνση: ονομάζεται και B αριθμός και προσδιορίζει τον προορισμό και στην περίπτωση του PSTN/ISDN προσδιορίζει την υπηρεσία που χρησιμοποιείται πάνω στο δίκτυο UMTS.
- Χρησιμοποιημένες πηγές 3ης γενιάς: ο bearer και τα χαρακτηριστικά του όπως το εύρος, η ταυτότητα και ο τύπος υπηρεσίας (connection oriented / connectionless).
- Παράμετροι QoS: ειδικά στο CN PS domain η τιμή της υπηρεσίας βασίζεται στο προσφερόμενο QoS. Πρακτικά, το QoS καθορίζει τον τύπο καθυστέρησης και την τιμή που χρησιμοποιείται στην σύνδεση.
- Υπηρεσίες 3G δικτύου και στοιχεία της ταυτότητας του δικτύου: για το UMTS δίκτυο, το MCC και το MNC είναι μοναδικές ταυτότητες και

για τα στοιχεία του δικτύου οι ταυτότητες αυτές μπορεί να είναι διευθύνσεις επιπέδου SCCP ή στατικές IP.

- Time stamps: όταν η σύνδεση έχει ξεκινήσει και όταν έχει τελειώσει
- Πληροφορίες MM: αυτό καλύπτει τις ταυτότητες της θέσης και της routing περιοχής καθώς και τις ταυτότητες κλήσεων. Χρησιμοποιείται συνήθως στις υπηρεσίες που βασίζονται στο context της location.
- Ταυτότητα του CDR: κάθε CDR πρέπει να ονομαστεί έτσι ώστε να μπορεί να αναγνωριστεί κατά την διάρκεια μιας περιόδου 3 μηνών τουλάχιστον.

Στο UMTS το roaming μεταξύ των δικτύων αναμένεται να είναι αυτόματο, σε ορισμένες περιπτώσεις ακόμα και σε εθνικό επίπεδο. Αυτό θέτει τις απαιτήσεις ότι οι διαδικασίες λογαριασμού πρέπει να είναι αυτόματες, επίσης. Οι τρόποι για να επιτευχθεί αυτό το ερίδος της λειτουργίας είναι κυρίως:

- CDR automatic forwarding: οι πληροφορίες χρέωσης μεταφέρονται μεταξύ των δικτύων. Κάτι τέτοιο χρησιμοποιείται σε μερικές χώρες μεταξύ διαφόρων δικτύων. Ένα καλό παράδειγμα μπορεί να είναι η Φιλανδία, όπου οι πληροφορίες χρέωσης μεταφέρονται μεταξύ του PSTN και των κυψελλοειδών δικτύων. Στα πρωτόκολλα, μερικά από αυτά περιέχουν μηχανισμούς για να μεταφέρουν πληροφορίες χρέωσης. Ένα από τα πρωτόκολλα που μπορεί να το κάνει αυτό είναι το ISUP.
- Αλγόριθμος χρέωσης: αυτός ο αλγόριθμος περιέχει πληροφορίες σχετικά με την χρέωση του χρήστη και κατεβάζετε από το δίκτυο –βάση του χρήστη. Όταν ο χρήστης είναι ενεργός σε ένα δίκτυο που επισκέπτεται, ο αλγόριθμος κατεβάζεται από το δίκτυο –βάση και η

χρέωση γίνεται για να ελέγξει αυτόν τον αλγόριθμο. Αυτή η μέθοδος λέγεται και delegation χρέωσης.

Οι αλγόριθμοι που περιγράφηκαν είναι ένας από τους λόγους γιατί το CAMEL (Common Application for Mobile Networks – Enhanced Logics) είναι πρακτικά μια κύρια λειτουργία στα UMTS δίκτυα.

5.4. Πτυχές Αρχιτεκτονικής στην 3GPP R4

Στη 3GPP R99 οι κύριες αλλαγές στοχεύουν στο κομμάτι πρόσβασης του δικτύου. Το κύριο θέμα που παρουσιάστηκε είναι η νέα ευρείας ραδιοπρόσβαση, UTRAN. Στη πλευρά του ασύρματου δικτύου ο σκοπός ήταν να ελαχιστοποιηθούν οι αλλαγές και χρησιμοποιούν τα υπάρχοντα GSM / GPRS στοιχεία δικτύου όσον το δυνατόν περισσότερο. Στη 3GPP R4 η στρατηγική είναι κάπως αντίθετη: η πρόσβαση δικτύου δεν έχει εμπειρία σε τόσες αλλαγές αλλά το CN επεκτείνεται απίστευτα.

Τελικά, η 3GPP R4 περιέχει όλες τις πιθανότητες όσον αφορά τη συμπεριφορά της κίνησης. Αν η transaction που έρχεται από την πρόσβαση δικτύου, είναι μεταγωγής πακέτου, μπορεί να βασίζεται σε ένα εξωτερικό δίκτυο είτε είναι μεταγωγής πακέτων είτε είναι μεταγωγής κυκλώματος. Επίσης, αν η transaction έρχεται από πρόσβαση δικτύου μεταγωγής κυκλώματος μπορεί να πάει στο εξωτερικό δίκτυο είτε μεταγωγής κυκλώματος είτε μεταγωγής πακέτων. Στη 3GPP R99 η φύση της σύνδεσης (κυκλώματος / πακέτων) παραμένει η ίδια μέσω του δικτύου.

5.5 Πτυχές Αρχιτεκτονικής στην 3GPP R5

Τα βασικά θέματα στην 3GPP R5 είναι GSM / EDGE RAN (GERAN) και IP μεταφορά μέσα στην πρόσβαση του δικτύου. Στη 3GPP R5 η κίνηση είναι πάντα μεταγωγής πακέτων. Δεν γνωρίζουμε όμως αν είναι πραγματικού ή μη πραγματικού χρόνου.

Οι διαφορές που παρουσιάζονται μεταξύ των R4 και R5 δεν είναι ορατή στους τελικούς χρήστες. Το ραδιομονοπάτι του UTRAN δουλεύει ακόμα όπως δουλεύει μέχρι τώρα. Επίσης, τα τερματικά που χρησιμοποιούνται μέχρι τώρα χρησιμοποιούνται και σε αυτήν την περίοδο. Μέσα στο δίκτυο πρόσβασης η τεχνολογία μεταφοράς μπορεί να είναι IP αντί για ATM αλλά αυτό είναι επιλογή του διαχειριστή.

Κεφάλαιο 6 Το Τερματικό UMTS

6.1 Η αρχιτεκτονική του τερματικού

Η κύρια λειτουργία του UMTS τερματικού σχετίζεται κυρίως στην αλληλεπίδραση μεταξύ του τερματικού και του δικτύου. Οι ακόλουθες λειτουργίες θεωρούνται κύριες για όλα τα UMTS τερματικά:

- Ένα interface σε μια integrated κάρτα κυκλώματος για εισαγωγή του Universal Subscriber Identity Module (USIM).
- Παροχέας Υπηρεσιών και εγκατάσταση - απεγκατάσταση δικτύου.
- Αναβάθμιση της θέσης.
- Κανονικοποίηση και απόκτηση και των δύο, connection-oriented και connectionless υπηρεσιών.
- Αναγνώριση ενός εξοπλισμού (IMEI)
- Βασικές ταυτότητες αναγνώρισης των δυνατοτήτων των τερματικών.
- Το τερματικό πρέπει να είναι ικανό να υποστηρίζει επείγουσες κλήσεις χωρίς ένα USIM.
- Υποστηρίζει την εκτέλεση των αλγορίθμων που απαιτούνται για την αυθεντικότητα και την κωδικοποίηση.

Το UMTS τερματικό πρέπει να υποστηρίζει τις ακόλουθες επιπρόσθετες λειτουργίες για να αντιμετωπίζει μελλοντικές «εξεγέρσεις»:

- Μια δυνατότητα Application Programming Interface (API).
- Έναν μηχανισμό για να κατεβαίνουν πληροφορίες σχετικά με τις υπηρεσίες (παράμετροι, κείμενα ή ακόμα και software), νέα πρωτόκολλα, άλλες λειτουργίες και ακόμα νέα APIs μέσα στο τερματικό.

- Κυριαρχία του Virtual Home Environment (VHE) που χρησιμοποιούν το ίδιο user interface και / ή άλλα interfaces καθώς γίνεται roaming.
- Προαιρετική εισαγωγή πολλών IC καρτών.

Το UE αποτελείται από τα **ME, TE, USIM**.

USIM: είναι το ανεξάρτητο κομμάτι του χρήστη στο UE. Το USIM είναι βασικά μια λογική σκέψη και εφαρμόζεται φυσικά σε μια integrated κυκλώματος κάρτα. Αυτή η κάρτα, που περιέχει εφαρμογές software ή πολλαπλά USIMs, λέγεται συχνά Universal Integrated Circuit Card (UICC). Ο χειριστής με τον οποίο οι χρήστες κάνουν την subscription, θα προβάλλει τις πληροφορίες για τα USIMs. Το USIM συνδέεται περισσότερο με τα προφίλ των υπηρεσιών παρά με ένα συγκεκριμένο προφίλ χρήστη.

ME: είναι το ανεξάρτητο κομμάτι από το UE του χρήστη, το οποίο περιέχει διάφορα μοντέλα.

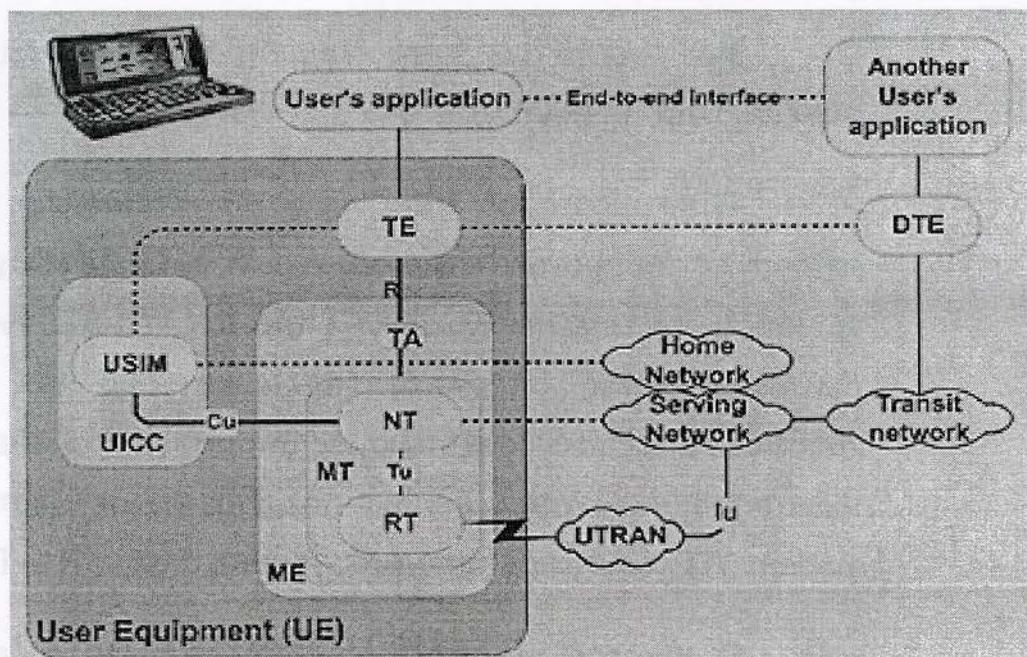
TE: κομμάτι του UE είναι ο εξοπλισμός που χρησιμοποιούν οι λειτουργίες εφαρμογών του τελικού χρήστη. Ο εξοπλισμός του τερματικού τερματίζει την τηλεπικοινωνιακή υπηρεσία. Το TE γνωρίζει τις πιθανές τηλεπικοινωνιακές υπηρεσίες για λογαριασμό των εφαρμογών των χρηστών. Ο τερματικός εξοπλισμός μπορεί, για παράδειγμα, να ελέγχει το τερματισμό του κινητού χρησιμοποιώντας το σετ διαταγών ελέγχου του modem (AT commands) που καθορίζονται από το ITU-T.

Ο **κινητός τερματισμός (MT)** από την άλλη πλευρά είναι το κομμάτι του εξοπλισμού του χρήστη, το οποίο τερματίζει την ραδιομεταφορά προς και από το δίκτυο και εφαρμόζει τις δυνατότητες του τερματικού εξοπλισμού σε αυτές τις ραδιομεταφορές. Από την άποψη του κινητού συστήματος, το MT είναι βασικά η πραγματική τερματική συσκευή. Το MT έχει την δυνατότητα να αλλάζει την τοποθεσία του μέσα στη

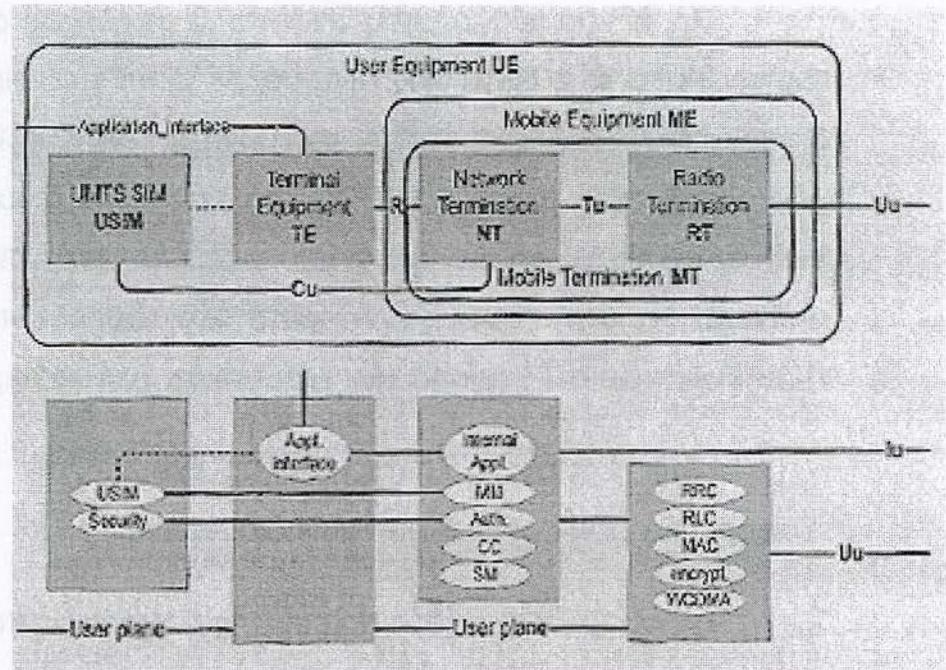
πρόσβαση δικτύου ή να κινείται στην περιοχή κάλυψης ενός άλλου δικτύου. Το MT τερματίζει και τις υπηρεσίες του UMTS δικτύου.

Το **NT (Network Termination)** είναι το κομμάτι του ασύρματου δικτύου που εξαρτάται από το MT. Το NT χρησιμοποιεί πρωτόκολλα stratum μη πρόσβασης για την διαχείριση κινητικότητας (MM / GMM) και διαχείριση επικοινωνίας (CC / SM). Γι αυτό το NT μπορεί να φαίνεται σαν τερματικό από την άλλη πλευρά του απλού ασύρματου δικτύου.

Το **RTC (Radio Termination)** είναι μια λειτουργική ομάδα του MT που σχετίζεται με το δίκτυο ραδιοπρόσβασης μόνο. Τερματίζει τις υπηρεσίες UTRAN. Χρησιμοποιούν πρωτόκολλα RRC, MAC, RLC στην κορυφή της φυσικής ραδιοσύνδεσης. Αυτά τα πρωτόκολλα αναλύονται αργότερα.



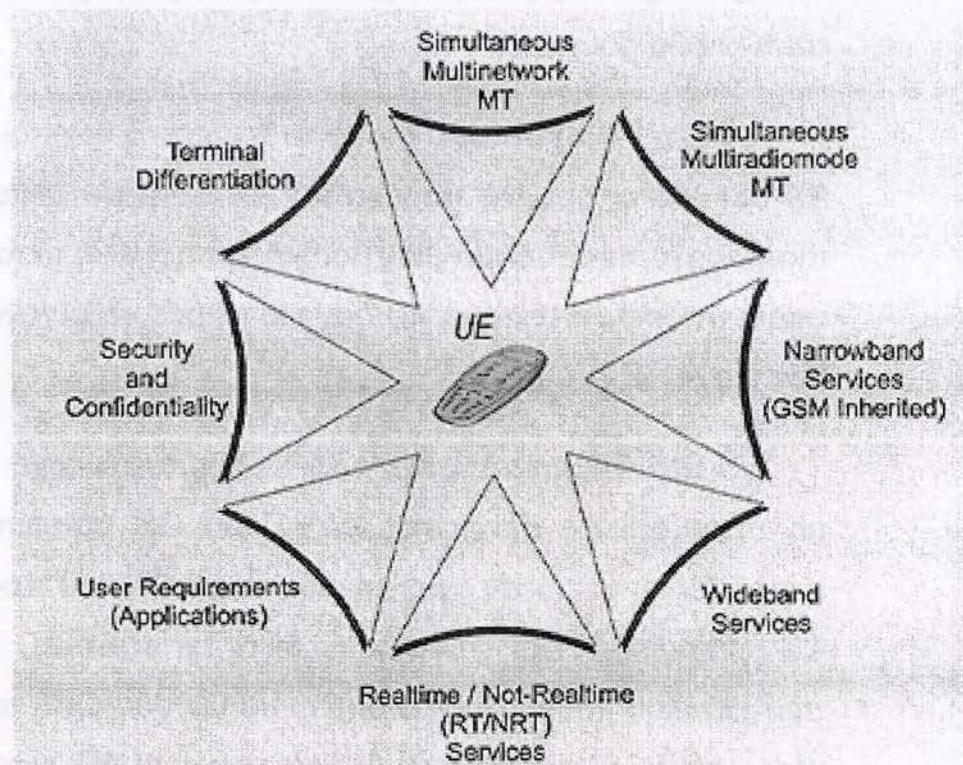
Εικόνα 49 Ο εξοπλισμός του χρήστη σε σχέση με την αρχιτεκτονική



Εικόνα 50 Θέση των κύριων οντοτήτων σε ένα UE

6.2 Διαφορές των τερματικών

Οι παράγοντες που επηρεάζουν το UE φαίνονται στην εικόνα 51.



Εικόνα 51 Παράγοντες που επηρεάζουν το UE

Η Αρχιτεκτονική δικτύου κινητής τηλεφωνίας UMTS

Αν η τιμή του κινητού είναι πολύ υψηλή αυτό αυξάνει με τη σειρά του τα ρίσκα στις δικτυακές εφαρμογές. Αυτά μαζί με άλλους παράγοντες δημιουργούν διαφορετικότητα στα κινητά. Αυτή η διαφορετικότητα είναι ήδη ορατή στην αγορά του GSM, όπου κάποια τερματικά είναι φτιαγμένα για τον καταναλωτή και άλλα για τους επαγγελματίες καταναλωτές, κ.α. Φαίνεται ότι στην Τρίτη Γεννιά αυτή η διαφορετικότητα θα δημιουργήσει διστακτικότητα στην αγορά των τερματικών ακόμα περισσότερο.

Στα τερματικά Τρίτης Γεννιάς έχουν στην βασική δομή τους 2 διαφορετικά είδη network domains διαθέσιμα:

- Packet Switched (PS) domain για υπηρεσίες πακέτων
- Circuit Switched (CS) domain για υπηρεσίες κυκλωμάτων

Στο **PS/CS operation mode** το τερματικό έχει επαφή και με το PS και το CS domain και το τερματικό είναι ικανό να προβάλλει ταυτόχρονα και τις υπηρεσίες μεταγωγής κυκλώματος και μεταγωγής πακέτων μέσω και των δύο domains.

Στο **PS operation mode** το τερματικό έρχεται σε επαφή μόνο με το PS domain μπορεί να παρέχει υπηρεσίες μόνο μέσα στο PS domain. Το πιο γνωστό παράδειγμα μιας βασικής υπηρεσίας μεταγωγής κυκλώματος η οποία μπορεί να εφαρμοστεί σαν μια υπηρεσία μεταγωγής πακέτων είναι η Voice over IP (VoIP).

Στο **CS operation mode** το τερματικό έρχεται σε επαφή μόνο με τις παρεχόμενες υπηρεσίες μέσω του CS domain. Ωστόσο, αυτό δεν εμποδίζει τις υπηρεσίες μεταγωγής πακέτων που προσφέρονται μέσω του CS domain. Είναι πιθανό μερικές υπηρεσίες μεταγωγής πακέτων πραγματικού χρόνου ειδικά αυτές με υψηλές QoS απαιτήσεις παρέχονται μέσω του CS domain με τοπικό constant bit rate παρόλο που αυτές βρίσκεται σε εξωτερικά δίκτυα.

Στο **PS/CS operation mode** το τερματικό μπορεί να έχει μια ευκαιρία να καθορίζει τις location update procedures αν το δίκτυο υποστηρίζει το προαιρετικό Gs interface μεταξύ του MSC/VLR και του SGSN γι' αυτό το σκοπό. Σε αυτή την περίπτωση το τερματικό μπορεί να επιλέξει σύμφωνα με τις δυνατότητες του αν θα χρησιμοποιήσει συνδιασμένες ή ξεχωριστά τις procedures αναβάθμισης.

Ο διαχωρισμός των λειτουργιών του τερματισμού δικτύου στον εξοπλισμό του κινητού επιτρέπει την ταξινόμηση του εξοπλισμού του χρήστη σύμφωνα με τις ικανότητες του MT να χρησιμοποιήσει τεχνολογίες πολλαπλής πρόσβασης και τεχνολογίες ασύρματου δικτύου. Τα ακόλουθα παρουσιάζουν βασικές εναλλακτικές, οι οποίες θεωρητικά είναι πιθανές.

- Single radiomode MT: μπορεί να χρησιμοποιήσει μόνο ένα τύπο ραδιο interface για την κίνηση των χρηστών. Στο UMTS, το προτεινόμενο ραδιο interface τουλάχιστον στην αρχή είναι το WCDMA – FDD, το οποίο είναι ένα τυπικό παράδειγμα ενός μόνο radiomode MT.
- Multi radiomode MT: μπορεί να χρησιμοποιήσει πολλούς τύπους ραδιο interface για την κίνηση των χρηστών. Μια ενδιαφέρουσα περίπτωση σε αυτή την κατηγορία είναι ένα dualmode τερματικό GSM/UMTS, για το οποίο το inter-operation είναι καλά καθορισμένο στις προδιαγραφές της 3GPP.
- Single network MT: μπορεί να χρησιμοποιήσει ένα τύπο ασύρματου δικτύου. Ένα UMTS τερματικό, το οποίο είναι ικανό να χρησιμοποιήσει τουλάχιστον ένα από τους operation modes: PS, CS ή PS/CS είναι ένα παράδειγμα για ένα μόνο δίκτυο MT.
- Multinetwork MT: είναι ικανό να χρησιμοποιήσει πολλά διαφορετικά ασύρματα δίκτυα. Μέσα στο UMTS ασύρματο δίκτυο ένα τυπικό τερματικό αυτού του είδους υποστηρίζει επίσης GSM NSS.

Βασιζόμενοι στους χρήστες και στις ανάγκες τους και λαμβάνοντας υπόψη τις δυνατότητες που προσφέρει η ευρείας μετάδοση ραδιο πρόσβαση κάποιος μπορεί να διακρίνει 4 κύρια χαρακτηριστικά που περιγράφουν τους χρήστες, τις ανάγκες και τις σχετιζόμενες υπηρεσίες.

- **Κλασικό τερματικό:** είναι παρόμοιο με τα υπάρχοντα κυψελλοειδή τηλέφωνα. Είναι φτιαγμένο έτσι ώστε να είναι φθηνό κι έτσι περιέχει περιορισμένες δυνατότητες όπως μεταγωγή πρόσβασης φωνής και περιορισμένη πρόσβαση δεδομένων με κυριώς χαμηλής ροής δεδομένων, τα οποία είναι καλύτερα από τα σημερινά GSM και GPRS. Αυτό το τερματικό είναι ικανό να διαχειριστεί την ραδιο πρόσβαση στο GSM και στο WCDMA αλλά όχι απαραίτητα ταυτόχρονα. Με άλλα λόγια, εφαρμόζει “τα επιλεγόμενα multinetwork MT”. Αυτό το είδος του τερματικού μπορεί να θεωρηθεί ότι είναι ένα είδος “επέκταση GSM”, η αξία της χρήσης του βασίζεται στα υπάρχοντα GSM δίκτυα και η πρόσβαση στο WCDMA χρησιμοποιείται περιστασιακά, κυρίως για τις συνδέσεις μεταγωγής πακέτων.

- **Dual mode:** αυτός ο τύπος του τερματικού περιέχει και τις δύο προσβάσεις, GSM και WCDMA και μπορεί αυτόματα να επιλέξει τη μέθοδο πρόσβασης σε μια διαθέσιμη υπηρεσία που ζητήθηκε. Για παράδειγμα, κλήσεις φωνής συνδέονται τυπικά μέσω του GSM, αλλά οι υπηρεσίες δεδομένων και πολυμέσων συνδέονται τυπικά μέσω του GSM, αλλά οι υπηρεσίες δεδομένων και πολυμέσων συνδέονται μέσω του WCDMA. Αυτός ο τύπος του τερματικού μπορεί να χρησιμοποιήσει τα πλεονεκτήματα και των δυο προσβάσεων και μπορεί να παρουσιάζει inter-system handover και στις δυο κατευθύνσεις. Στην περίπτωση του inter-system handover η υπηρεσία που χρησιμοποιείται εφαρμόζει στη ραδιο πρόσβαση όποτε είναι δυνατόν. Έτσι, αυτό το τερματικό εφαρμόζει “ταυτόχρονο multinetwork MT”. Όταν τα UMTS δίκτυα χρησιμοποιούνται

για παγκόσμια χρήση, αυτά τα τερματικά πιθανόν να δοαμορφώνουν το μεγαλύτερο μέρος της αγοράς.

- **Multimedia terminal:** αυτό είναι σαν το προηγούμενο τερματικό αλλά είναι πιο ευφυές από την πλευρά του δικτύου. Τα τερματικά Dual mode δεν χειρίζονται απαραίτητα τους UTRAN ραδιο bearers με τον καλύτερο τρόπο αλλά το multimedia τερματικό μπορεί να παράγει "optimal multiplexing" των bearers που χρησιμοποιούνται για multimedia κλήσεις. Η δυνατότητα αποθήκευσης είναι ένα πολύ σημαντικό ζήτημα όταν το UMTS δίκτυο ανακατεύεται. Το multimedia τερματικό δεν είναι απαραίτητα για την συνολική αγορά, αλλά για επιχειρηματίες χρήστες, τουλάχιστον στην αρχή τους. Τα multimedia τερματικά είναι ένα είδος συνδιασμού των κυψελλοειδών τηλεφώνων και των laptop και palmtop computers. Περιέχουν πολλές εφαρμογές που χειρίζονται τις multimedia συνδέσεις και υπηρεσίες.

- **Special terminals:** αυτά τα τερματικά δεν έχουν απαραίτητα μια "τηλεφωνική παρουσία" όπως τα προηγούμενα. Αυτά τα τερματικά παρέχουν ειδικές περιπτώσεις και μπορούν να συνδιαστούν μαζί με άλλους εξοπλισμούς. Αυτό το τερματικό μπορεί, για παράδειγμα, να τοποθετηθεί σε ένα αυτοκίνητο και μπορεί να δουλέψει σε συνεργασία με ένα vehicle computer. Αν το αυτοκίνητο κλαπεί, αυτού του είδους το τερματικό μπορεί να "ξυπνήσει" και μεταφέρει τις πληροφορίες για την θέση του οχήματος σχετικά με την διεύθυνση του δρόμου χρησιμοποιώντας GPS και τις πληροφορίες του vehicle computer. Χρησιμοποιεί PS operation mode μόνο και οι περιοχές στις οποίες εφαρμόζεται μπορούν να είναι πολύ διαφορετικές. Υπάρχουν πολλά οράματα σχετικά με τα "έξυπνα σπίτια" όπως το υλικό refrigerator που μπορεί να παραγγείλει φαγητό όταν απαιτηθεί. Αυτό το τερματικό μπορεί να είναι ο intergrated επικοινωνιακός εξοπλισμός που εγκαθιστά την σύνδεση σε αυτή τη περίπτωση.

6.3 Ιδιότητες των UMTS τερματικών

Επειδή ο κύκλος ζωής των UMTS δικτύων αναμένεται να διαρκέσει αρκετές δεκαετίες θα υπάρξουν αρκετά είδη τέτοιων τερματικών με διάφορα είδη δυνατοτήτων.

Οι βασικές πληροφορίες σχετικά με την δυνατότητα ενός UE ονομάζονται mobile station classmark. Στο UMTS υπάρχουν 2 classmark. Η classmark 2 που ονομάζεται CN classmark και η classmark 3 που ονομάζεται RAN classmark.

Πληροφορίες σχετικά με τις βασικές δυνατότητες του UE στον κινητό σταθμό classmark 3 είναι:

- Διαθέσιμοι WCDMA κόμβοι όπως οι FDD και οι TDD
- Δυνατότητες dual mode, π.χ. υποστηρίζει διάφορες μεταβλητές των GSM συστημάτων με υποστηριζόμενες ζώνες συχνότητας και άλλα χαρακτηριστικά
- Διαθέσιμοι αλγόριθμοι κρυπτογράφησης
- Ιδιότητες λειτουργίας μέτρησης στο UE, όπως διαθεσιμότητα των επεκτεινόμενων δυνατοτήτων μετρήσεως και διαθέσιμος χρόνος για το MT για να αλλαχθεί από ένα ραδιο κανάλι σε άλλο για να γίνουν οι μετρήσεις ενός γειτονικού κελιού.
- Δυνατότητα να χρησιμοποιεί μεθόδους τοποθέτησης και διάφορα είδη μεθόδων τοποθέτησης υποστηρίζονται.
- Δυνατότητα να χρησιμοποιεί παγκόσμιες συλλογές χαρακτήρων, π.χ. 16 bit κωδικοποίηση χαρακτήρων, που είναι γνωστή ως ISO / IEC 10646 ή Unicode, αντίθετα για την βασική την 7-bit GSM συλλογή χαρακτήρων σε υπηρεσίες μικρών μηνυμάτων.

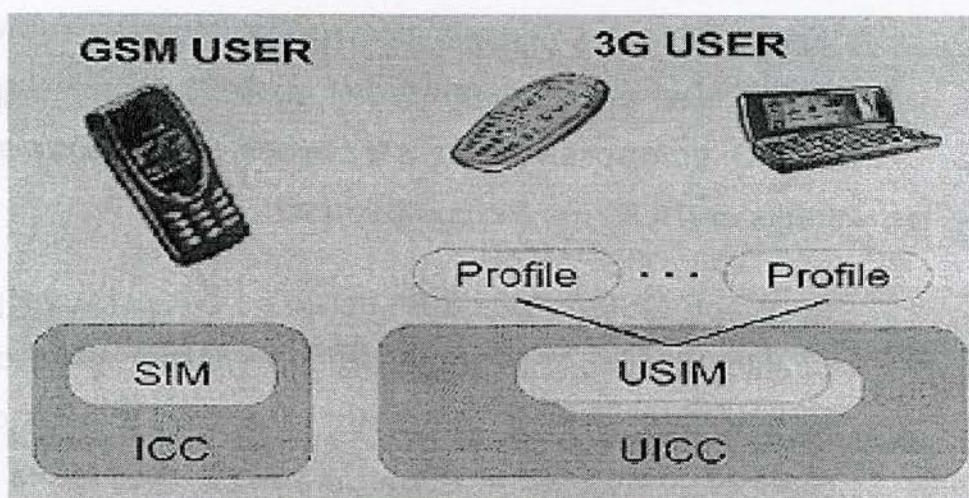
6.4 Εγγραφή στο UMTS

Όπως το GSM, έτσι και το UMTS διαχωρίζει την subscription από το ME. Οι συγκεκριμένες πληροφορίες για την subscription ονομάζονται USIM (Εικόνα 52). Οι USIM ονομάζονται και “Μοντέλο Ταυτότητας-Αναγνώρισης Υπηρεσιών” επειδή οι υπηρεσίες ακολουθούν τις πληροφορίες της κάρτας SIM. Οι ανταποκρινόμενες πληροφορίες αποθηκεύονται στο Home Location Register (HLR) του δικτύου-βάση του χρήστη.

Στο GSM, η κάρτα SIM είναι σε ένα μετακινούμενο ICC (Integrated Circuit Card) και εκεί αποθηκεύει ο χρήστης αλλά αποθηκεύονται και οι πληροφορίες για τις υπηρεσίες. Στο UMTS η μετακινούμενη αποθήκη δεδομένων είναι το UICC και αυτό περιέχει το USIM με τις ταυτότητες και τις πληροφορίες υπηρεσιών. Το USIM αποτελείται από πολλά προφίλ τα οποία είναι “φίλτρα” που καθορίζουν πως, για παράδειγμα, οι αποθηκευμένες πληροφορίες φαίνονται στον χρήστη. Αυτά τα προφίλ μπορούν να αλλάζουν: ο χρήστης μπορεί να αλλάζει τις ρυθμίσεις των προφίλ και το δίκτυο μπορεί να κάνει αλλαγές στις πληροφορίες του προφίλ.

Ένα USIM μπορεί να περιέχει πολλά προφίλ τα οποία λειτουργούν με συγκεκριμένο σκοπό. Ας υποθέσουμε ότι ένας χρήστης έχει 2 τερματικά. Ένα από αυτά είναι σε “κλασικό τύπο” (help in Section 6.2) και το άλλο είναι multimedia τερματικό. Όταν ο χρήστης εισάγει το USIM στα τερματικά του η subscription είναι η ίδια αλλά το τερματικό παρουσιάζει τις πληροφορίες με ένα διαφορετικό τρόπο. Ένα διαφορετικό προφίλ χρησιμοποιεί για την ίδια subscription ανάλογα με το TE που χρησιμοποιείται. Για παράδειγμα, μέσω του multimedia τερματικού ο χρήστης είναι σε θέση να έχει πρόσβαση στις πληροφορίες (π.χ.picture archive), οι οποίες δεν είναι διαθέσιμες με το κλασικό τερματικό.

Τελικά, η διαφορά μεταξύ μιας κάρτας GSM SIM και μιας USIM είναι ότι η USIM είναι ικανή να κατεβάζει από το δίκτυο και οι πληροφορίες της είναι προσβάσιμες και ανανεώσιμες μέσω του ραδιο μονοπατιού.



Εικόνα 52 Ταυτότητα των μοντέλων των χρηστών στο GSM και στην 3G

Η USIM περιλαμβάνει 5 βασικούς τύπους δεδομένων:

- **Administrative:** αυτός είναι ένας τύπος δεδομένων ο οποίος προσδιορίζει από τον κατασκευαστή της USIM και τον παροχέα των υπηρεσιών και λειτουργεί σαν τιμή-κλειδί για ασφαλείς αλγορίθμους IMSI και πληροφοριών πρόσβασης.
- **Temporary network data:** είναι κυρίως πληροφορίες διαχείρισης όπως η προσφερόμενη περιοχή θέσης ID, TMSI και οι τιμές-κλειδιά που υπολογίζουν το ciphering.
- **Service related data:** αυτό περιέχει πληροφορίες σχετικά με την διαθεσιμότητα ή την αδειοδότηση διαφόρων υπηρεσιών, και των εσωτερικών δεδομένων τους. Μια υπηρεσία είναι διαθέσιμη όταν η subscription έχει την δυνατότητα να υποστηρίζει την υπηρεσία. Όταν μια υπηρεσία δεν είναι διαθέσιμη σημαίνει ότι η υπηρεσία δεν πρέπει να χρησιμοποιείται από το USIM χρήστη, ακόμα και αν το UE έχει την

δυνατότητα να υποστηρίζει την υπηρεσία. Για παράδειγμα, το USIM μπορεί να περιέχει, αν ο διαχειριστής το επιτρέπει, υπηρεσίες όπως ένας τοπικός κατάλογος τηλεφώνων για τον χρήστη, mobile subscriber ISDN number, fixed dialling numbers, πληροφορίες εισερχόμενων και εξερχόμενων κλήσεων, αποθήκευση, αναφορές κατάστασης και παράμετροι υπηρεσιών για μικρά μηνύματα (SMS), πληροφορίες χρέωσης, επιλογέας PLMN που ελέγχεται από χρήστη και διαχειριστή με τεχνολογία πρόσβασης, λίστα συνεργαζόμενων δικτύων, κ.τ.λ.

- **Applications:** Το USIM αποθηκεύει μικρές εφαρμογές που χρειάζεται για συγκεκριμένες υπηρεσίες. Αυτές χρησιμοποιούν για παράδειγμα όπως είναι οι Applets Java οι οποίες μπορούν να κατασκευαστούν και να αποθηκευθούν στο USIM για αξιοποίηση τους αργότερα μέσα στο UE.

- **Personal:** Αυτό καλύπτει τα δεδομένα τα οποία αποθηκεύει ο χρήστης στην κάρτα SIM για παράδειγμα μικρά μηνύματα και αναπάντητες κλήσεις.

6.5 Interface Χρήστη

Το user interface του UMTS τερματικού μπορεί να ακολουθεί ή όχι τον παραδοσιακό τρόπο όπως στα GSM τερματικά. Η χρήση του user interface εξαρτάται ολοκληρωτικά από τον κατασκευαστή του τερματικού. Είναι ωστόσο, πολύ πιθανό ότι κάτι παρόμοιο θα παρουσιάζεται με τον ένα τρόπο ή τον άλλο όπως σε ένα κανονικό αριθμημένο keypad..

Υπάρχουν κάποιες λειτουργίες που το τερματικό πρέπει να έχει, όπως το "Accept", "Select", "Send", "Indication", "End". Αυτές οι λειτουργίες είναι σημαντικές με σκοπό να χειριστούν την αρχή και την λήξη των κλήσεων και των επιπλέον υπηρεσιών. Ο χρήστης θα πρέπει να έχει πρόσβαση σε όλες αυτές τις λειτουργίες.

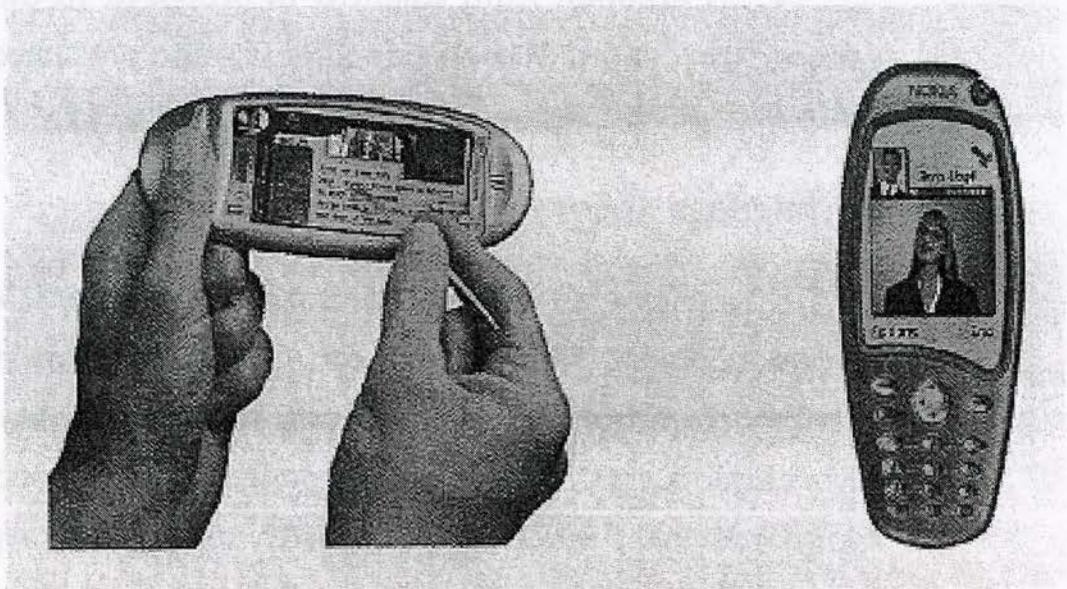
Accept: χρησιμοποιείται για να αποδεχθούμε μια κλήση

Select: χρησιμοποιείται για να εισάγουμε πληροφορίες. Ο φυσικός τρόπος για να εισάγουμε τους χαρακτήρες 09, +, * μπορεί να είναι ένα πληκτρολόγιο, μια μηχανή αναγνώρισης φωνής, ένας εξοπλισμός δεδομένων ή άλλα.

Send: αναλαμβάνει την αποστολή των πληροφοριών που έχουν εισαχθεί (ο αριθμός του χρήστη) στο δίκτυο.

Indication: χρησιμοποιείται για να δώσει όλα τα είδη των πληροφοριών για την κλήση.

End: χρησιμοποιείται για να τερματίσει ή να αποσυνδεθεί από μια κλήση. Και τα δυο μέρη μιας κλήσης μπορούν να χρησιμοποιήσουν την λειτουργία End ή ακόμα και για το δίκτυο.



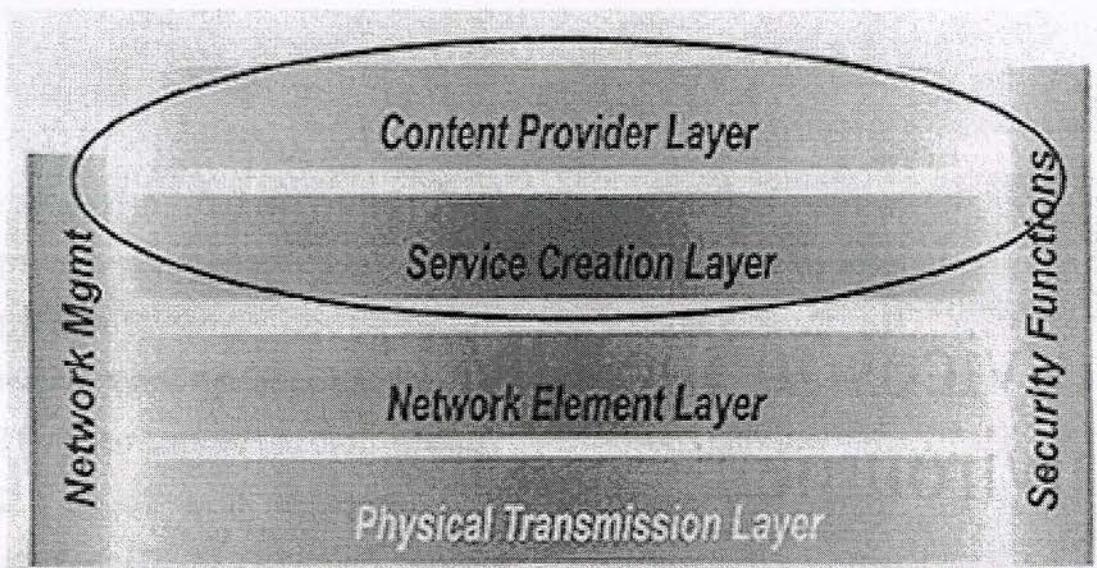
Εικόνα 53 Conceptual UMTS τερματικά

Κεφάλαιο 7 Υπηρεσίες σε περιβάλλον UMTS

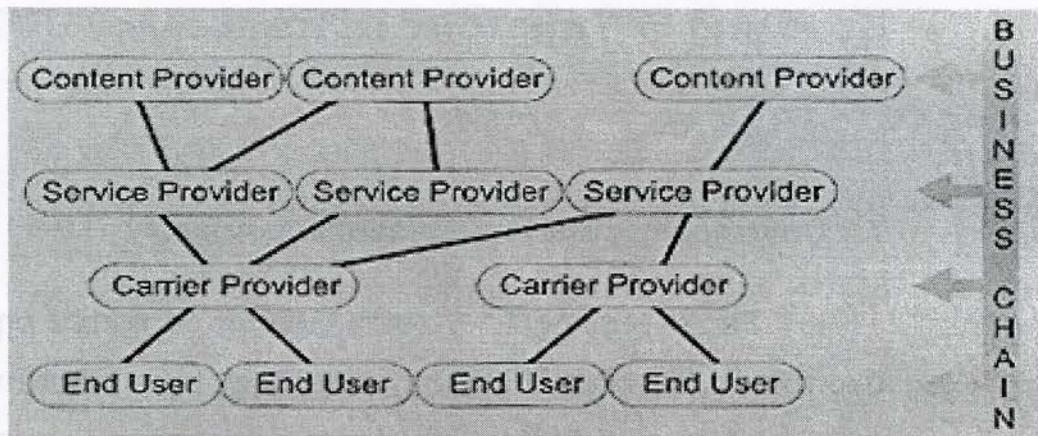
7.1 Οι υπηρεσίες και το commercial μοντέλο

Στις μέρες της 1^{ης} γεννιάς δικτύων τα δίκτυα δημιουργήθηκαν με σκοπό να προσφέρουν μια υπηρεσία, της ομιλίας. Αυτά τα συστήματα δεν υποστηρίζουν την ιδέα του να έχουν περισσότερες υπηρεσίες. Με της 2^{ης} γεννιάς δίκτυα υπήρξε μια διάθεση για εξέλιξη και κάποια commercial «σώματα» που εστιάζουν την δουλειά τους σε υπηρεσίες και content provision που ήρθαν στην αγορά.

Η εικόνα 54 παρουσιάζει πως οι υπηρεσίες, η δημιουργία τους και η content provision τοποθετούνται στο UMTS. Η πιο σημαντική είναι η ασφάλεια και η διαχείρισή της. Το commercial μοντέλο του UMTS δίνει πιθανότητες να διαχωριστούν κάποιοι commercial ρόλοι. Τα σώματα που χρησιμοποιούνται σε αυτούς τους ρόλους πρέπει να μεταφέρουν κάποιες ευαίσθητες πληροφορίες μέσω αυτών και αυτό έχει ένα καταπληκτικό αποτέλεσμα στους μηχανισμούς ασφάλειας.



Εικόνα 54 Οι υπηρεσίες στο UMTS και οι θέσεις τους στο δίκτυο



Εικόνα 55 Οι υπηρεσίες 3^{ης} γενιάς και η επιχειρηματική αλυσίδα

Circuit switched bit rate (kb/s)	Packet switched bit rate	Coverage type
144 kb/s	144 kb/s (peak)	Basic coverage, rural/suburban, fast moving vehicles, outdoor
384 kb/s	384 kb/s (peak)	Extended coverage, urban, moving vehicles, outdoor
2 Mb/s	2 Mb/s (peak)	Hot spot areas, urban, centre, walking speeds, indoor

Εικόνα 56 Ο πίνακας με τα bit rates του UMTS

7.2 Αρχιτεκτονική του QoS

Από την πλευρά του τελικού χρήστη, το UMTS δίκτυο είναι ένα δίκτυο για υπηρεσίες. Σε αυτή την περίπτωση, η τεχνολογία μόνη της δεν είναι το πιο σημαντικό αλλά είναι ένας παράγοντας που προβάλλει το QoS έτσι ώστε ο τελικός χρήστης να μπορεί να ικανοποιηθεί με τις υπηρεσίες που χρησιμοποιεί. Για να το εκφράσουμε αυτό τεχνολογικά, οι υπηρεσίες που προσφέρονται στον χρήστη μεταφέρονται στο UMTS δίκτυο με τους bearers. Ο bearer είναι μια υπηρεσία που παρέχει QoS μεταξύ δυο καθορισμένων σημείων. Αφού η δομή του UMTS δικτύου περιέχει πολλά επίπεδα συστήματος, που έχουν τις δικές του ιδιότητες QoS (π.χ.

ραδιομονοπάτι), το QoS χειρίζεται από πολλά επίπεδα λαμβάνοντας υπόψη τα ειδικά χαρακτηριστικά που σχετίζονται με αυτό το επίπεδο.

Το κομμάτι QoS καλύπτει και τον έλεγχο της σύνδεσης και την ροή δεδομένων των χρηστών. Τα προβλήματα με το QoS μπορεί πιθανότατα να σχετιστούν με την εξωτερική bearer υπηρεσία, που έχει σαν σκοπό να καλύπτει το QoS στις συνδέσεις με τα άλλα δίκτυα. Οι μηχανισμοί QoS έξω από το UMTS δίκτυο δεν είναι μέσα στις προδιαγραφές της 3GPP και από αυτή την άποψη μερικά προβλήματα παρουσιάζονται.

7.2.1 Ταξινόμηση του QoS στο UMTS

Η ταξινόμηση των απαιτήσεων QoS του UMTS (γνωστές και σαν ταξινομήσεις κίνησης) καθορίζονται έχοντας υπόψη ότι η ταξινόμηση πρέπει να είναι απλή.

Οι επόμενες 4 αρχές είναι:

- Οι τάξεις QoS πρέπει να επιτρέπουν την αποδοτική χρήση της ραδιο δυνατότητας (UMTS Terrestrial Radio Access (UTRA) Service).
- Το CN και το UTRAN πρέπει να είναι ικανά να εμπεριέχουν ανεξάρτητα τον διαχωρισμό της υπηρεσίας bearer και της lu bearer υπηρεσίας.
- Το δίκτυο UMTS πρέπει να λειτουργεί ανεξάρτητα από τα γειτονικά του δίκτυα. Από την άλλη πλευρά, οι μηχανισμοί συμβατικότητας πρέπει να παρουσιάζονται (bearer υπηρεσία UMTS και διαχωρισμός των εξωτερικών bearer υπηρεσιών).
- Ο διαχειριστής πρέπει να μπορεί να χρησιμοποιήσει την υπάρχουσα τεχνολογία μεταφοράς μέσα στο UMTS σύστημα με έναν τρόπο οικονομικό από πλευρά κόστους (φυσική και backbone bearer υπηρεσία).

Οι UMTS QoS τάξεις είναι :

- **Conversational Class:** ελάχιστη δυνατή καθυστέρηση, όχι buffering, συμμετρική κίνηση, εγγυημένο bit rate.
- **Streaming Class:** ελάχιστη δυνατή καθυστέρηση, επιτρεπόμενο buffering, ασύμμετρη κίνηση, εγγυημένο bit rate.
- **Interactive Class:** μέτρια δυνατή καθυστέρηση, επιτρεπόμενο buffering, ασύμμετρη κίνηση, όχι εγγυημένο bit rate.
- **Background Class:** μεγάλη δυνατή καθυστέρηση, επιτρεπόμενο buffering, ασύμμετρη κίνηση, όχι εγγυημένο bit rate.

Η **Conversational Class** είναι η πιο απαιτητική QoS class για πραγματικού χρόνου κίνηση (RT), για παράδειγμα φωνητική κλήση. Όλες οι υπηρεσίες που χρησιμοποιούνται στο CN CS domain έχουν Conversational Class στο επίπεδο bearer υπηρεσιών στο UMTS. Στο επίπεδο των υπηρεσιών για το τελικό χρήστη, ο χρήστης μπορεί να συναντά προβλήματα ποιότητας στην εξωτερική bearer υπηρεσία και το άλλο άκρο της σύνδεσης δε θα είναι ικανό να εγγυηθεί το QoS.

Όταν ο χρήστης θέλει να κάνει surfing στο Internet μέσω της σύνδεσης μεταγωγής κυκλώματος χρησιμοποιεί την Conversational Class. Αυτή η σύνδεση από μόνη της μπορεί να έχει συνεχόμενη συμμετρική ροή bit μέσω του UMTS δικτύου. Το QoS που χρησιμοποιείται για web surfing μπορεί να μην ικανοποιήσει τον χρήστη, αφού η ροή πληροφοριών δεν είναι πραγματικού χρόνου για να μην υπερφορτωθεί ο web server ή τα εξωτερικά δίκτυα που συμμετέχουν.

Σαν συμπέρασμα, σε αυτή την περίπτωση ο τελικός χρήστης έχει QoS Conversational Class υπηρεσία σε χρήση στο επίπεδο της bearer

υπηρεσίας του UMTS, αλλά η τελική υπηρεσία προς τον χρήστη είναι κάτι άλλο από αυτό.

Η **streaming class** δεν θέλει τόσο αυστηρά όρια για την καθυστέρηση. Η καθυστέρηση μπορεί να ποικίλει κατά την διάρκεια της σύνδεσης κι έτσι οι πληροφορίες μπορεί να φορτώνονται μέσα στο δίκτυο. Οι τυπικές υπηρεσίες της streaming class θα είναι ασύμμετρης κίνησης. Για παράδειγμα, ο χρήστης μπορεί να “κατεβάζει” μουσική από το δίκτυο.

Οι **interactive** και **background classes** δεν είναι ευαίσθητες στην καθυστέρηση για τις τελικές υπηρεσίες. Μια τυπική interactive class μπορεί να είναι, για παράδειγμα, Wireless Application Protocol (WAP) υπηρεσία. Ο χρήστης στέλνει ένα αίτημα και το δίκτυο απαντά όταν υπάρχουν ελεύθερες πηγές απάντησης. Αυτή η καθυστέρηση μεταξύ του response – request μπορεί να ποικίλλει και οι πληροφορίες που είναι για να μεταφερθούν στον χρήστη μπορεί να είναι buffered με σκοπό να καθορίσουν την αποδοτικότητα και την δυναμικότητα του δικτύου.

Οι πιο σημαντικοί παράγοντες QoS στο UMTS είναι:

- Μέγιστο bit rate (kb/s)
- Εγγυημένο bit rate (kb/s)
- Επιτρεπόμενη καθυστέρηση μεταφοράς (ms)
- Αν η ζητούμενη QoS class είναι διαπραγματεύσιμη ή όχι.

Το **μέγιστο bit rate** καθορίζει το μέγιστο bit rate που το UMTS bearer μπορεί να χρησιμοποιήσει για να μεταφέρει πληροφορίες μεταξύ των δυο άκρων του UMTS bearer.

Το **εγγυημένο bit rate** καθορίζει το bit rate που το UMTS bearer πρέπει να μεταφέρει μεταξύ των δυο άκρων του UMTS bearer.

Η **καθυστέρηση μεταφοράς** είναι ο πιο σημαντικός παράγοντας μεταξύ των UMTS QoS classes. Οι απαιτήσεις των QoS classes για την τελική υπηρεσία μπορεί να είναι διαπραγματεύσιμη ή όχι. Για παράδειγμα, σε μια περίπτωση κλήσης ομιλίας μεταγωγής κυκλώματος η QoS class πρέπει να είναι conversational και δεν μπορεί να το διαπραγματευθεί αυτό. Από την άλλη πλευρά οι υπηρεσίες μεταγωγής πακέτων πρέπει να χρησιμοποιούνται με διάφορες QoS classes.

	Conversational	Streaming	Interactive	Background
Maximum bit rate (kb/s)	Less than 2048	Less than 2048	Less than 2048	Less than 2048
Guaranteed bit rate (kb/s)	Less than 2048	Less than 2048	N/A	N/A
Symmetry	Symmetric	Asymmetric	Asymmetric	Asymmetric
Transfer delay (ms)	100-250	250-seconds	N/A	N/A

Πίνακας 57 Χαρακτηριστικά του UMTS bearer service (partial and indicatory)

	Conversational	Streaming	Interactive	Background
Maximum bit rate (kb/s)	Less than 2048	Less than 2048	Less than 2048	Less than 2048
Guaranteed bit rate (kb/s)	Less than 2048	Less than 2048	N/A	N/A
Symmetry	Symmetric	Asymmetric	Asymmetric	Asymmetric
Transfer delay (ms)	80-250	250-seconds	N/A	N/A

Πίνακας 58 Χαρακτηριστικά του UMTS radio access bearer service (partial and indicatory)

Οι κυριότεροι bearers είναι ο UMTS bearer και η RAB υπηρεσία. Όμως, μέσα στο CN ο CN bearer και ο Iu bearer έχουν μεγάλο ενδιαφέρον. Αυτές οι bearer υπηρεσίες περιγράφουν προσεκτικά το

φυσικό μέσο που θα χρησιμοποιηθεί για τον UMTS bearer και υπάρχουν 3 περιπτώσεις για να εγγραφούμε το QoS σε αυτό το επίπεδο:

1. Αν το δίκτυο μεταφοράς συνδέει τους CN κόμβους και το UTRAN μαζί χρησιμοποιώντας Asynchronous Transfer Mode (ATM) σαν μεταφορά, οι συμπεριφορές των υπηρεσιών των CN bearer τοποθετούνται στις ATM classes κίνησης. Αυτό είναι το σίγουρο δεδομένο στις προδιαγραφές της 3GPP R99 του UMTS. Καθώς περνά ο καιρός και το δίκτυο συμπεριλαμβάνεται στην 3GPP R4/5 το πρωτόκολλο IP θα χρησιμοποιείται για την μεταφορά.

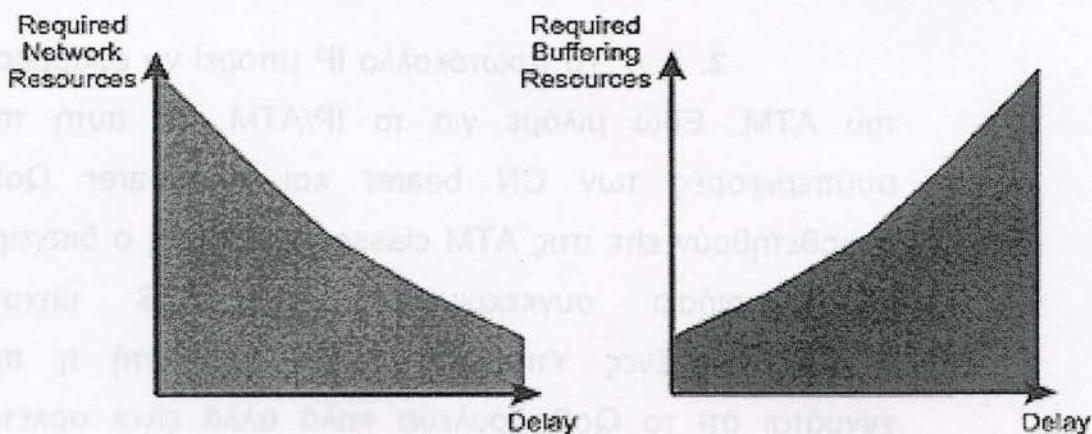
2. Το πρωτόκολλο IP μπορεί να εφαρμοστεί στην κορυφή του ATM. Εδώ μιλάμε για το IP/ATM. Σε αυτή τη περίπτωση οι συμπεριφορές των CN bearer και lu bearer QoS μπορούν να τοποθετηθούν είτε στις ATM classes κίνησης ή ο διαχειριστής μπορεί να χρησιμοποιήσει συγκεκριμένους IP QoS μηχανισμούς όπως Διαφοροποιημένες Υπηρεσίες (DiffServ). Αυτή η πρωτότυπη λύση εγγυάται ότι το QoS δουλεύει καλά αλλά είναι αρκετά περίπλοκο να διαχειριστεί από τη στιγμή που διάφορα πρωτόκολλα σε διαφορετικά επίπεδα χρησιμοποιούνται από τη διαχείριση του QoS.

3. Η Τρίτη περίπτωση είναι να χρησιμοποιηθεί το πρωτόκολλο IP σαν μεταφορά μέσω φυσικών μέσων προσφέροντας αρκετό εύρος ζώνης. Σε αυτήν την περίπτωση οι συμπεριφορές των CN και lu bearer χειρίζονται με τους ειδικούς μηχανισμούς IP QoS όπως την Diff Serv.

7.2.2 QoS Classes – a Provocative Approach

Στα δίκτυα 1^{ης} γεννιάς και της 2^{ης} γεννιάς η σύνδεση ήταν μέχρι τώρα **μεταγωγής κυκλώματος**. Αυτό είχε τα πλεονεκτήματα και τα μειονεκτήματα του. Ένα πλεονέκτημα είναι ότι η σύνδεση μεταγωγής κυκλώματος είναι σταθερή όταν τοποθετείται χρησιμοποιώντας fixed bit

rates και στις δυο κατευθύνσεις είναι συμμετρική και προβάλλει σταθερό μέσο για οποιαδήποτε υπηρεσία χρησιμοποιώντας την σύνδεση. Ένα μειονέκτημα, είναι ότι εύκολα χαλαρίζει τις ραδιο πηγές αν η υπηρεσία που χρησιμοποιείται στην σύνδεση δεν απαιτεί fixed bit rate και σύνδεση συμμετρικού τύπου. **Στο UMTS η πλειοψηφία της κίνησης αναμένεται να είναι μεταγωγής πακέτου και η σύνδεση μεταγωγής πακέτου φέρνει νέες παραμέτρους σε αυτήν την εικόνα.** Οι συνδέσεις δεν χρησιμοποιούν απαραίτητα fixed bit rate πια, και επιπρόσθετα τα bit rates μπορεί να διαφέρουν σύμφωνα με την κατεύθυνση μεταφοράς.



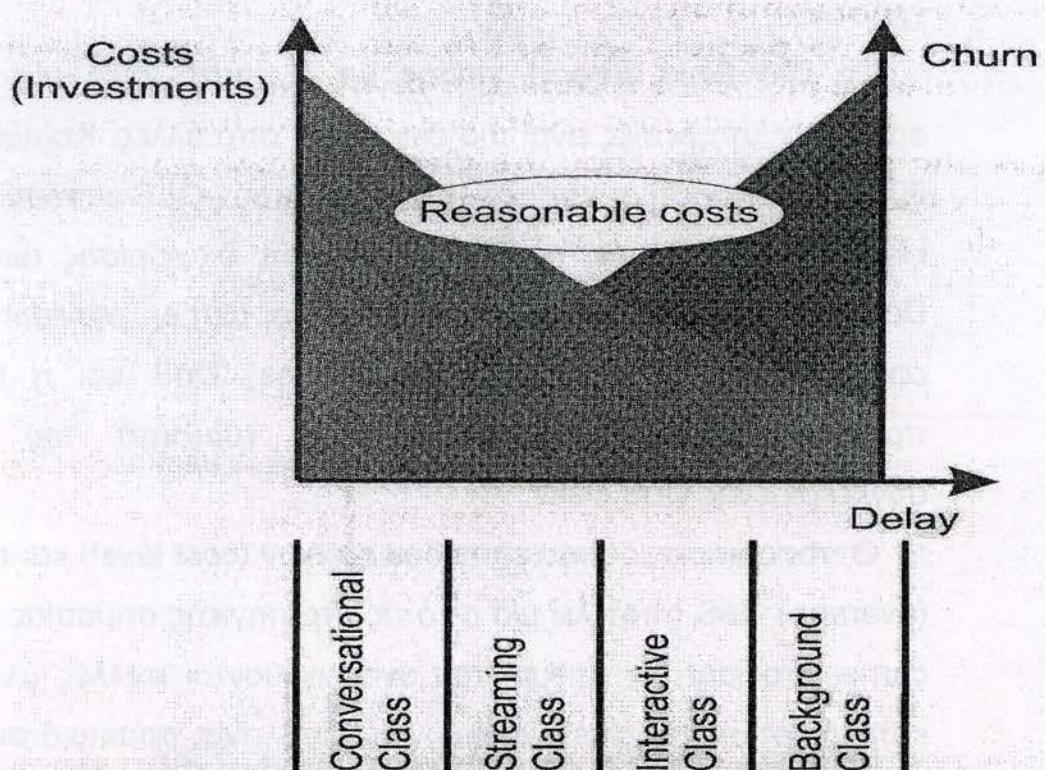
Εικόνα 59 Παράγοντες που επηρεάζουν το QoS (provocative)

Το QoS είναι ένα θέμα πολύ σημαντικό επειδή περιγράφει τον ανθρώπινο παράγοντα να ενδιαφέρεται για την ποιότητα της σύνδεσης. Εξαιτίας αυτού, το βασικό θέμα στο QoS είναι η καθυστέρηση. Στο QoS είναι καλύτερα να είναι μικρότερη η καθυστέρηση της σύνδεσης. Αυτό δημιουργεί την εντύπωση μιας καλής ποιότητας σύνδεσης όσο ενδιαφέρει τους χρήστες.

Το QoS από την άλλη πλευρά του δικτύου έχει πολλούς άλλους παράγοντες που το επηρεάζουν (Εικόνα 59). Καταρχήν, η ελάττωση της καθυστέρησης απαιτεί αρκετές πηγές δικτύου. Σε αυτήν την περίπτωση οι πηγές δικτύου σημαίνουν για παράδειγμα το εύρος ζώνης μεταφοράς που τοποθετείται στην σύνδεση. Όσο μεγαλύτερη είναι η καθυστέρηση τόσο

λιγότερες πηγές δικτύου σε σύνολο απαιτούνται. Αυτό φαίνεται στο αριστερό γράφημα της Εικόνας 59.

Μία άλλη εκδοχή, είναι η προσωρινή αποθήκευση (buffering) των δεδομένων (bit streams) ή των πακέτων πληροφοριών. Με μια πρώτη ματιά, το buffering δείχνει να είναι καλή ιδέα: με την προσωρινή αποθήκευση της ροής των πληροφοριών εντός του δικτύου, η χρήση ορισμένων πολύτιμων πόρων δικτύου μπορεί να ελαχιστοποιηθεί. Αυτό ισχύει, αλλά αν η καθυστέρηση στο δίκτυο είναι μεγάλη, η ποσότητα των προσωρινά αποθηκευμένων (buffered) πληροφοριών διογκώνεται. Έτσι, η ανάγκη για πόρους buffering αυξάνεται ως αντίδραση στην καθυστέρηση. Επίσης, ο τελικός χρήστης μπορεί να μην είναι ικανοποιημένος από την ποιότητα του δικτύου και να οδηγηθεί στον τερματισμό της συνδρομής του. Ακολουθεί ένα σχεδιάγραμμα για αυτή τη περίπτωση.



Εικόνα 60 Κατάσταση του κόστους δικτύων και του QoS (provocative)

Ο κοινός παράγοντας για τις ανάγκες τόσο των πόρων δικτύου όσο και του buffering είναι τα χρήματα δηλαδή το κόστος και οι επενδύσεις. Αν

αυτοί οι παράγοντες εξεταστούν ως αποτέλεσμα της καθυστέρησης, μια αιχμηρή παρουσίαση μπορείτε να δείτε στην εικόνα 60. Η καθυστέρηση αυτή κατηγοριοποιείται (classified) μέσω του QoS που αποδεικνύεται σχετικά ακριβή επιλογή. Το παρεχόμενο QoS αποτελεί ένα τμήμα των δικτύων UMTS που προορίζεται για βελτιστοποίηση.

Ένα δίκτυο υψηλής ποιότητας κοστίζει από την πλευρά των επενδύσεων, μπορεί όμως να προσφέρει ανάλογη ποιότητα. Ένα δίκτυο κακής ποιότητας έχει εν μέρει έξοδα από την πλευρά των επενδύσεων και απώλειες συνδρομών. Μεταξύ των δύο αυτών απόλυτων και ακραίων περιπτώσεων, η προσφερόμενη ποιότητα είναι αρκετά καλή και οι συνδρομές δεν χάνονται στα πλαίσια του ανταγωνισμού. Αυτός ο συνδιασμός ελαχιστοποιεί τις ενδότερες επενδύσεις συγκριτικά με τα επερχόμενα οφέλη. Η ιδανική αυτή κατάσταση ποικίλει ανάλογα με τον operator και τη χώρα που ανταποκρίνεται στις προσδοκίες του τελικού χρήστη.

Το ίδιο θέμα μπορεί επίσης να εξεταστεί από μία άλλη πλευρά: ορισμένες υπηρεσίες είναι πιο επικερδείς από άλλες. Κοιτώντας την εικόνα 60 διαφαίνεται ότι οι υπηρεσίες που απαιτούν QoS streaming ή interactive class είναι ως έχουν, λόγω της βέλτιστης διαχείρισης των επενδύσεων. Παρ' όλ' αυτά, στην πραγματικότητα, ο carrier provider χρειάζεται να εφαρμόσει όλες τις κατηγορίες (classes) QoS και η βελτιστοποίηση πραγματοποιείται αφού εκτιμηθεί η ευρύτητα της χρήσης μίας συγκεκριμένης QoS class.

Ο προσδιορισμός του επιπέδου εξόδων (cost level) και του μέσου όρου (average) QoS αποτελεί μία από τις στρατηγικής σημασίας αποφάσεις του carrier provider, τη στιγμή που αναμειγνύονται πολλές άλλες εκδοχές. Η κατηγοριοποίηση (classification) του QoS είναι πρακτικά ασήμαντη για τις circuit switched connections, γεγονός που καθιστά τις προσφερόμενες υπηρεσίες packet switched κατά την έναρξη της βελτιστοποίησης του κόστους. Αυτό το σκεπτικό, αποτελεί τη βασική αιτία που οδηγεί στην

προσπάθεια για γρήγορη μετατροπή όσο το δυνατόν περισσότερων υπηρεσιών circuit switched σε packet switched. Για παράδειγμα, η Voice over IP (VOIP) αποτελεί μία πολύ ενδιαφέρουσα περίπτωση λόγω των δυνατοτήτων μείωσης κόστους των δαπανών που προσφέρει σε ευρεία μετάδοση (transmission bandwidth).

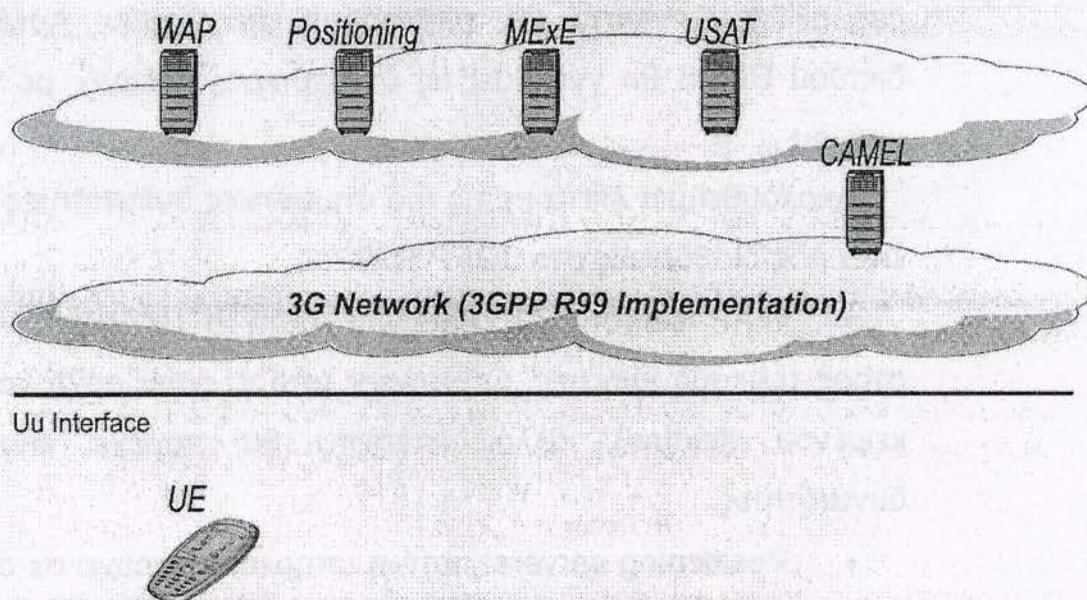
7.3 Δυνατότητες υπηρεσιών στην πλατφόρμα UMTS Service Platform

Μία από τις βασικές αρχές στο UMTS είναι ότι το δίκτυο που πραγματοποιεί τις συνδέσεις διαχωρίζεται όσο το δυνατόν περισσότερο από τα μέρη του δικτύου που διατηρούν τις υπηρεσίες. Η διαφοροποίηση αυτή δημιουργεί διαφημιστική προοπτική και ευελιξία στην αγορά. Για να εφαρμοστεί αυτή η ιδέα, το 3GPP R99 παρέχει τμήματα δικτύου (network components) επονομαζόμενα ως δυνατότητες υπηρεσιών (service capabilities), γνωστά ως πλατφόρμα υπηρεσιών. Αυτό το τμήμα του δικτύου UMTS θα γνωρίσει τις μεγαλύτερες αλλαγές με το πέρασμα του χρόνου.

Ακολουθεί μία λίστα με τις πιο σημαντικές δυνατότητες υπηρεσιών που είναι ήδη διαθέσιμες στο 3GPP R99.

- WAP server/WAP gateway: αυτή η υπηρεσία παρέχει browser στους τελικούς χρήστες. Ο browser μπορεί στην αρχή να είναι σε μορφή κειμένου (textual), αλλά μετέπειτα θα παρέχει πιο εξειδικευμένες δυνατότητες.
- Positioning servers: αυτή η υπηρεσία παρέχει σε άλλες υπηρεσίες, πληροφορίες σχετικά με τη θέση (position) του UE. Γι' αυτόν τον λόγο, οι υπηρεσίες αυτές αναφέρονται συχνά ως υπηρεσίες βασισμένες στη θέση (location based services).
- Περιβάλλον εκτέλεσης εφαρμογών φορητού/κινητού σταθμού: Αυτή η υπηρεσία παρέχει σε άλλες υπηρεσίες, πληροφορίες σχετικά με τις δυνατότητες του τερματικού σε σχέση με τη διαχείριση πληροφοριών.

- UMTS SIM Application Toolkit (USAT): Η υπηρεσία αυτή παρέχει τα εργαλεία/μέσα (tools) που είναι απαραίτητα για τον χειρισμό της κάρτας SIM (SIM card handling)
- Customised Application for Mobile network Enhanced Logic (CAMEL): Αυτή η υπηρεσία συμπεριλαμβάνει επιμέρους δυνατότητες υπηρεσιών και προορίζεται για τον τελικό χρήστη π.χ. αποτελεί μία συνηθισμένη πλατφόρμα για όλα τα είδη υπηρεσιών που χρησιμοποιούνται από τους συνδρομητές. Με την εξέλιξη του δικτύου UMTS από 3GPP R99 σε 3GPP R4, ο ρόλος του CAMEL αναβαθμίζεται και εξελίσσεται σε "service interconnection point". Θα αποτελεί σταθμό στην διεκπεραίωση υπηρεσιών. Χαρακτηριστικό παράδειγμα αυτής της περίπτωσης αποτελεί το Virtual Home Environment (VHE), το οποίο περιγράφεται αργότερα.

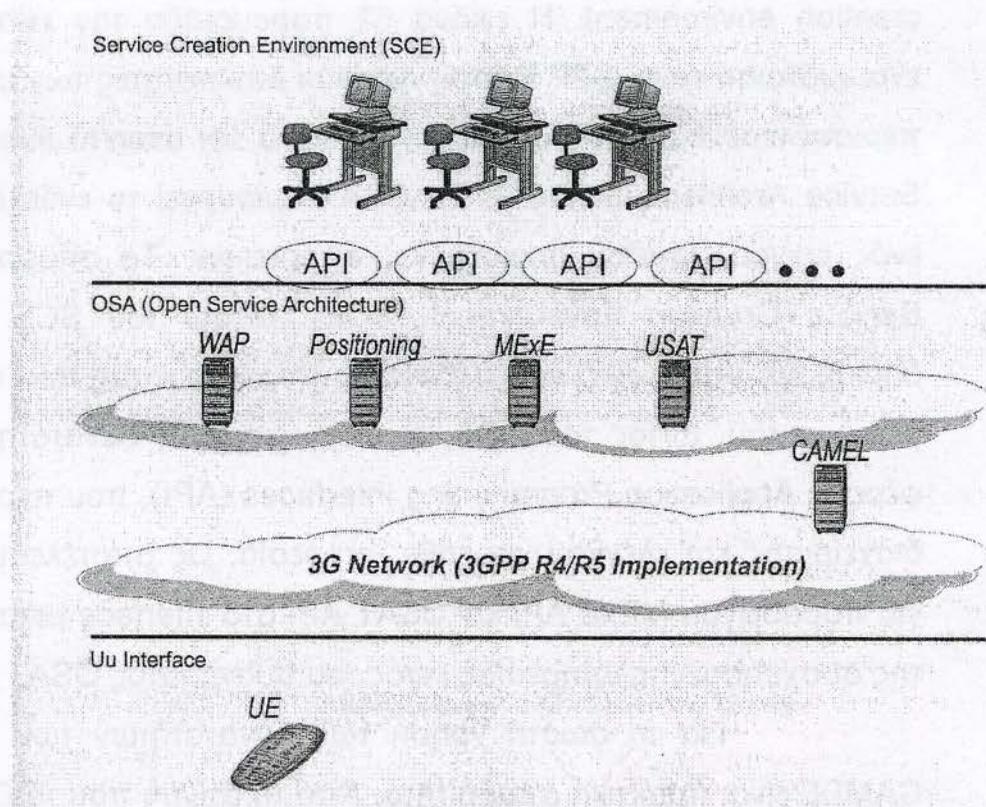


Εικόνα 61 Δυνατότητες υπηρεσιών στην εφαρμογή 3GPP R99

Στην ενσωμάτωση του 3GPP, οι δυνατότητες των υπηρεσιών είναι κατά κάποιον τρόπο σημαντικές και γι' αυτό μπορεί να είναι εν μέρει vendor-dependent. Δεν υπόκεινται σε απόλυτο και κοινόχρηστο και πολύπλευρο έλεγχο, γεγονός που οδηγεί στην απουσία universal service

creation environment. Η εικόνα 62 παρουσιάζει την εφαρμογή και την ενσωμάτωση του 3GPP R4/R5, όπου οι δυνατότητες των υπηρεσιών είναι περισσότερο ομοιογενείς: διατηρούν κοινό και ανοιχτό interface, το Open Service Architecture (OSA). Το OSA δημιουργεί το ενδεχόμενο ύπαρξης ενός κοινού σημείου δημιουργίας υπηρεσιών. Το σημείο αυτό καλείται Service Creation Environment (SCE). Μέσω του SCE οποιοσδήποτε δημιουργεί υπηρεσίες, έχει πρόσβαση στις υπηρεσίες που είναι διαθέσιμες μέσω αυτού. Εντός του OSA, οι διαχωρισμένες δυνατότητες υπηρεσιών φέρουν Application Programming Interfaces (API), που περιέχουν στοιχεία διαχείρισης και ελέγχου για κάθε υπηρεσία. Ως αποτέλεσμα, θα υπάρχει για παράδειγμα MExE API και USAT API στο interface μεταξύ του SCE και της συσχετισμένης υπηρεσίας εντός του συστήματος OSA.

Για τη σωστή χρήση των δυνατοτήτων των υπηρεσιών, το CAMEL είναι πρακτικά απαραίτητο. Από τη στιγμή που το CAMEL παρέχει open protocol interfaces, είναι πιθανό να εσωκλείει δημιουργία υπηρεσιών και content provision από το CN. Όπως περιγράφηκε πρωτύτερα στην αλυσίδα αξιών (value chain) που παρουσιάζεται στο σχήμα 61, η δομή αυτή διαμορφώνει ένα επίπεδο δημιουργίας υπηρεσιών (service creation layer) το οποίο μπορεί από μόνο του να αποτελέσει ένα commercial body: από τη στιγμή που διατηρεί ανοιχτό interface(s) προς το CN, δεν έχει σημασία σε ποιο CN(s) είναι εφαρμοσμένο. Το γεγονός αυτό αποτελεί ουσιαστική διαφορά σε σύγκριση με το GSM: στο GSM η δημιουργία υπηρεσιών με βάση Intelligent Network (IN) (Intelligent Network based service creation) ήταν διαθέσιμη και έγκυρη μόνο σε οικιακά δίκτυα. Στο UMTS, οι υπηρεσίες είναι διαθέσιμες σε κάθε δίκτυο UMTS αν είναι διαθέσιμη η σύνδεση μέσω CAMEL και οι carrier και service providers έχουν συμφωνήσει από κοινού για τις υπηρεσίες που προορίζονται για χρήση μεταξύ των δικτύων.



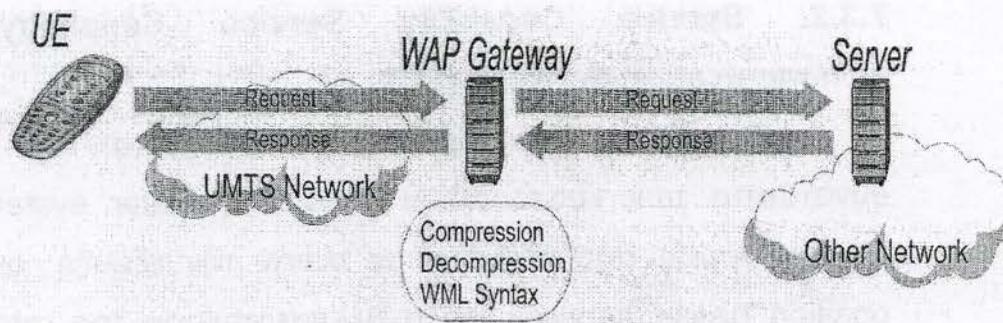
Εικόνα 62 Δυνατότητες υπηρεσιών στην εφαρμογή 3GPP R4/R5

Οι ακόλουθες υποενότητες παρουσιάζουν τις ικανότητες υπηρεσιών.

7.3.1 Service Capability – Wireless Application Protocol (WAP)

Κατά κύριο λόγο, το WAP είναι ένας τρόπος παροχής (web) browser προς τον τελικό χρήστη (63). Η εφαρμογή του browser βρίσκεται στο τερματικό και ανάλογα με τις απαιτήσεις του χρήστη ανατρέχει στις πληροφορίες που προορίζονται για download από το δίκτυο.

Όταν το WAP είναι ενσωματωμένο σε δίκτυο UMTS, η HTML που χρησιμοποιείται στο Internet δεν είναι κατάλληλη για το φορητό/κινητό περιβάλλον (mobile environment) καθώς ο τύπος της HTML δεν είναι επαρκώς ακριβής, γεγονός που μπορεί να οδηγήσει σε σύγχυση όσον αφορά τα τερματικά και τις λειτουργίες του browser.



Εικόνα 63 Διάλογος στο WAP – ιδεώδες διάγραμμα

Αντί της HTML, το WAP χρησιμοποιεί Wireless Markup Language (WML), η οποία είναι πιο ακριβής στον τύπο και τη σύνταξη. Οι σελίδες WML μπορούν να αποθηκευτούν σε έναν κανονικό Internet server αλλά δεν είναι προσπελάσιμες μέσω ενός κοινού Internet browser.

Ο πυρήνας των υπηρεσιών WAP είναι μία WAP gateway. Ένας server λαμβάνει τις εντολές των χρηστών και τις μετατρέπει σε HyperText Transfer Protocol (http) εντολές, και το αντίστροφο. Λόγω του τρέχοντος bandwidth, που αποτελεί θεμελιώδους σημασίας τομέα στα φορητά δίκτυα, η WAP gateway αναλαμβάνει το πακετάρισμα και τη συμπίεση των δεδομένων (data packaging και compression) προς τα τερματικά. Το WAP αποτελεί την κατάλληλη δυνατότητα υπηρεσίας για τις υπηρεσίες που χρησιμοποιούν interactive QoS class βασισμένες στο μοντέλο ανταπόκρισης αίτησης (request-response model). Η καθυστέρηση της σύνδεσης δεν αποτελεί θέμα, καθώς η έναρξή της είναι σχετικά γρήγορη.

Το WAP υπό αυτήν τη μορφή δεν συμπεριλαμβάνεται στις προδιαγραφές 3GPP. Για περισσότερες λεπτομέρειες σχετικά με το WAP, για τις τρέχουσες και τις μελλοντικές εφαρμογές του, μπορείτε να ανατρέξετε στη δικτυακή διεύθυνση <http://www.wapforum.org>

7.3.2. Service Capability Service Capability – Location Communication Services (LCS)

Το mobile positioning εξελίσσεται σε μία ελπιδοφόρα δυνατότητα των κυψελοειδών δικτύων (cellular system). Δύο είναι οι βασικοί τομείς που οδηγούν σε αυτήν την εξέλιξη: οι αναβαθμισμένες position based services και η βελτιστοποίηση της απόδοσης του radio system με τη χρήση βοηθητικών δεδομένων position assistance data. Παραδείγματα εφαρμογών βασισμένων σε commercial position αποτελούν η διαχείριση fleet, η διαχείριση ροής πληροφοριών, η μεταφορά, οι πλησιέστερες υπηρεσίες, οι έκτακτες υπηρεσίες, οι υπηρεσίες καθοδήγησης κ.τ.λ. Από την άλλη πλευρά, τα position assistance data μπορούν να χρησιμοποιηθούν για τη βελτιστοποίηση της απόδοσης του συστήματος ρυθμίζοντάς το για σχεδίαση δικτύων, RRM, Mobility Management (MM) κ.α.

Έως τώρα, η κυψελοειδής τεχνολογία ωθεί τον χρήστη στην κατάργηση της χρήσης ενσύρματης επικοινωνίας υποστηρίζοντας τη φορητότητα του χρήστη και ποικίλες υπηρεσίες επικοινωνίας ανεξάρτητα από τη θέση του. Παρά το γεγονός ότι η φορητότητα των κυψελοειδών τερματικών προκαλεί περιπλοκές και φορτώνει το δίκτυο, εξελίσσεται σε μία σημαντική ευκαιρία σε συνδυασμό με τη δυνατότητα positioning των κυψελοειδών συστημάτων.

Σε αυτό το σκέλος, αρχικά περιγράφουμε τις βασικές αρχές διαφορετικών μεθόδων positioning που έχουν αναπτυχθεί έως τώρα για τα φορητά δίκτυα. Έπειτα αναφερόμαστε στις τεχνικές positioning που προορίζονται για το UMTS. Γίνεται επίσης λόγος για την αρχιτεκτονική positioning του UMTS και τις λειτουργίες positioning που εντοπίζονται σε διαφορετικούς τομείς των δικτύων.

Για να διατηρηθεί ο παραλληλισμός με την ορολογία των προδιαγραφών 3GPP, χρησιμοποιούμε τον όρο “position” με την

γενικότερη έννοια, αλλά με τον όρο “location” αναφερόμαστε στις προδιαγραφές 3GPP όπου αυτή η λειτουργία συστήματος λέγεται LCS.

7.3.2.1. Περίληψη των μεθόδων τοποθέτησης

Οι μέθοδοι ποικίλουν για τον προσδιορισμό της γεωγραφικής θέσης ενός κυψελοειδούς τερματικού. Οι πιο σημαντικές είναι οι ακόλουθες:

- Cell ID based positioning
- Round-Trip Time (RTT) positioning
- Time-of-Arrival (TOA) positioning
- Time Difference of Arrival (TDOA) positioning
- Angle of Arrival (AOA) positioning
- Reference Node Based Positioning (RNBP)
- Global Positioning System (GPS)

Οι βασικές αρχές χρήσης αυτών των μεθόδων για το UE positioning περιγράφονται παρακάτω. Έπειτα, ακολουθεί μία συνοπτική περιγραφή για την ακρίβεια των διάφορων μεθόδων πριν γίνει λόγος για τις μεθόδους positioning που ορίζονται από το UMTS.

Θέση της ταυτότητας της κυψέλης Cell ID

Η θέση του τερματικού μπορεί να προσδιοριστεί με τη χρήση πληροφοριών για το radio cell στο οποίο βρίσκεται ή πρόσφατα βρισκόταν. Οι πληροφορίες σχετικά με τη θέση του cell αποτελείται είτε από cell ID είτε από cell coverage co-ordinates. Με τη χρήση της cell ID ή των cell coverage co-ordinates της γνωστής θέσης του serving BS, εκτιμάται η θέση του τερματικού.

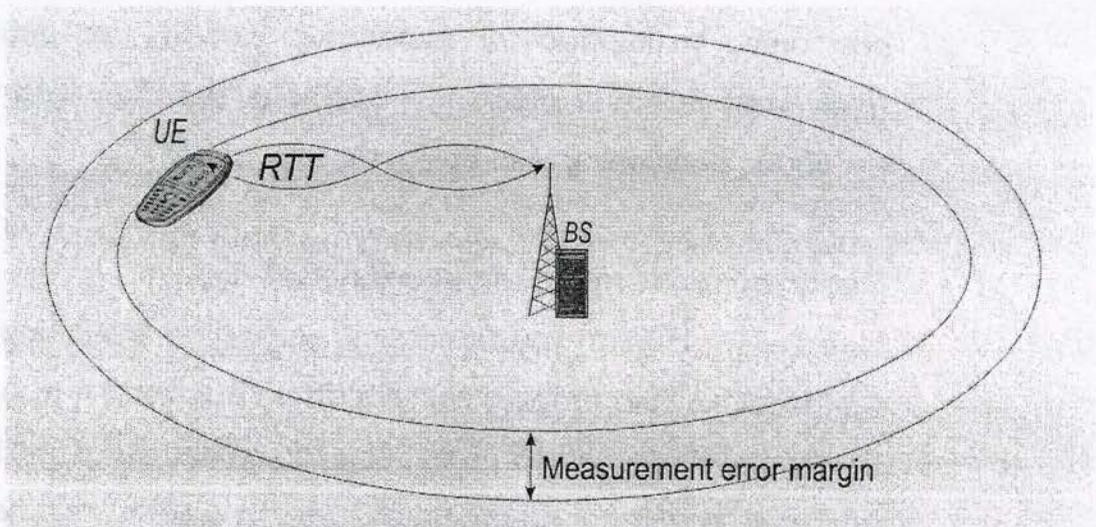
Σύμφωνα με τις προδιαγραφές 3G, η cell ID παρουσιάζεται ως radio information κι έτσι υπάρχει η περίπτωση να μη μεταφερθεί στο CN. Αντιθέτως, η cell ID προσκολλάται στην “service area identification” και μπορεί να αποσταλεί στο CN.

Round Trip Time (RTT) Based Positioning

Το RTT του radio signal μπορεί επίσης να χρησιμοποιηθεί για την ενδυνάμωση της ακρίβειας κατά την εκτίμηση της θέσης. Ο υπολογισμός της θέσης του τερματικού μπορεί να χρησιμοποιήσει τις μετρήσεις RTT των σημάτων από πολυάριθμα BSs σχήμα (64). Το RTT αποτελεί τον χρόνο propagation καθυστέρησης της μετάδοσης του signal από το BS και αντίστροφα. Γι' αυτόν τον λόγο, η απόσταση μεταξύ του τερματικού και του BS μπορεί να αποκομιστεί με βάση τον χρόνο t και την εμβέλεια του ραδιοφωνικού/ασύρματου κύματος. Σύμφωνα με τα παραπάνω έχουμε:

$$D = (RTT/2) \cdot c + \epsilon$$

Όπου το D είναι η απόσταση μεταξύ τερματικού και BS, c η ταχύτητα του ηλεκτρομαγνητικού κύματος η οποία είναι ίση με την ταχύτητα του φωτός (3×10^8 m/s). Το RTT είναι round trip time και το ϵ είναι η απόκλιση μέτρησης.



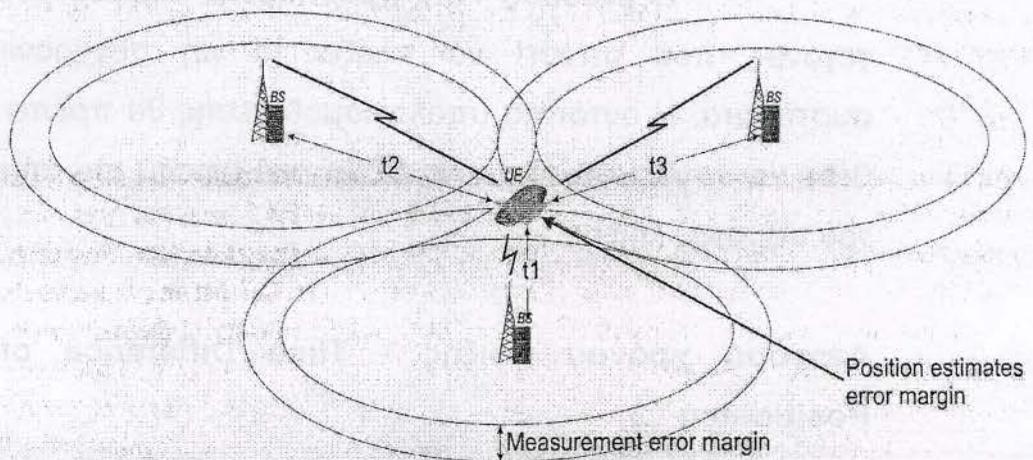
Εικόνα 64 Round Trip Time (RRT) positioning

Θα πρέπει να σημειωθεί ότι η απόσταση D είναι στην πραγματικότητα η ακτίνα ενός κύκλου που περιβάλλει το BS. Έτσι, για πιο ακριβείς εκτιμήσεις η θέση του φορητού τερματικού μπορεί να προσδιοριστεί με τη χρήση επιπρόσθετων μετρήσεων RTT από γειτονικά BSs, εάν αυτές είναι διαθέσιμες. Έπειτα, ο προσδιορισμός της θέσης

βρίσκεται εντός των τριών περιβάλλοντων κύκλων στο κέντρο των οποίων βρίσκεται το BS. Η ακρίβεια της αποδοθείσας εκτίμησης της θέσης εξαρτάται από τις ανακρίβειες των μετρήσεων RTT.

Χρόνος Άφιξης - Time of Arrival (TOA) Positioning

Κατά τη μέθοδο TOA ο υπολογισμός της θέσης βασίζεται στην καθυστέρηση propagation του radio signal από τον πομπό στον δέκτη. Όταν είναι διαθέσιμες τουλάχιστον τρεις μετρήσεις TOA, η θέση του τερματικού μπορεί να προσδιοριστεί με τη χρήση μίας τριγωνομετρικής τεχνικής, ελαχιστοποιώντας τις λιγότερο τετραγωνισμένες αποστάσεις μεταξύ του τερματικού και των corresponding κύκλων TOA. Στο 65 παρουσιάζονται οι αρχές προσδιορισμού της θέσης του τερματικού με τη μέτρηση του TOA τριών γειτονικών BS.



Εικόνα 65 Time of arrival (TOA) positoning

Στη μέθοδο TOA η απόσταση από το τερματικό μέχρι το BS είναι proportional στο propagation time, t_1 . Ως επόμενο, αν υπάρχει Line-of-Sight (LOS) μεταξύ του handset και του BS, η απόσταση μεταξύ τους προκύπτει ως εξής:

$$D_i = ct_i$$

Όπου c είναι η ταχύτητα του ηλεκτρομαγνητικού κύματος και t_1 ο χρόνος καθυστέρησης κατά τη μετάδοση του signal από ένα BS στο

τερματικό ή αντίστροφα. Παρ' όλ' αυτά, πρακτικά πάντα εμφανίζεται λάθος στις μετρήσεις TOA λόγω του Non-Line-of-Sight (NLOS), αδύναμο signal, αντανakλάσεις και shadowing. Γι' αυτόν τον λόγο, ένα margin λάθους μετρήσεως θα πρέπει πάντα να υπολογίζεται κατά την εκτίμηση της ακρίβειας του TOA positioning.

Για την προσκόμιση εκτίμησης μοναδικής θέσης του φορητού τερματικού, είναι απαραίτητο το TOA τουλάχιστον τριών BS. Έπειτα, η θέση του handset μπορεί να εκτιμηθεί με τον υπολογισμό της απόστασης μεταξύ του τερματικού και ποικίλων BSs (κύκλοι TOA). Δηλαδή:

$$D_i = \sqrt{[(X_i - x_m)^2 + (Y_i - y_m)^2 + (Z_i - z_m)^2]} + \varepsilon$$

Όπου (x_i, y_i, z_i) είναι οι συντεταγμένες των γειτονικών BSs που αποτελούν μέρος της διαδικασίας positioning και (x_m, y_m, z_m) οι συντεταγμένες του τερματικού που προορίζεται για τοποθέτηση.

Η μέθοδος TOA προϋποθέτει ακριβέστατο συγχρονισμό BS, γεγονός που μπορεί να πλήξει τα μη συγχρονισμένα κυψελοειδή συστήματα. Η οντότητα υπολογισμού θέσης θα πρέπει επίσης να είναι σε θέση να υπολογίζει τη χρονική διαφορά μεταξύ του σήματος εκπομπής και του σήματος λήψης.

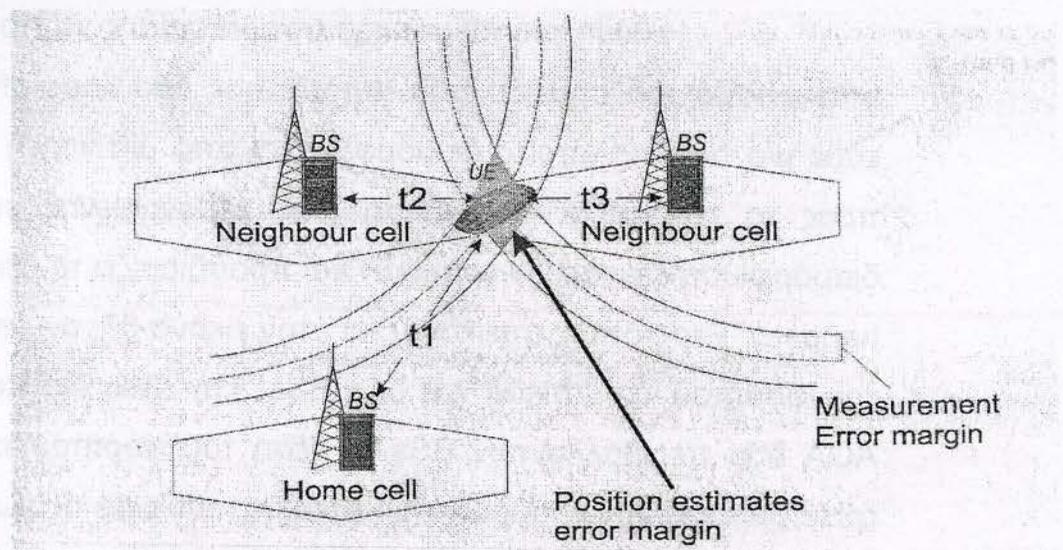
Διαφορά χρόνου άφιξης - Time Difference of Arrival (TDOA) Positioning

Η βασική αρχή της μεθόδου TDOA διαφέρει από εκείνη που ακολουθείται στην περίπτωση της TOA. Εδώ, το τερματικό παρατηρεί το TDOA των radio signals από τα περιβάλλοντα BSs. Η μη προσδιορισμένη θέση του τερματικού εκτιμάται με την επεξεργασία των μετρήσεων TDOA μεταξύ του τερματικού και τουλάχιστον τριών BSs των οποίων οι συντεταγμένες είναι ήδη γνωστές. Το TDOA που έχει υπολογιστεί από το τερματικό αποτελείται από τα εξής:

$$\text{TDOA} = \text{RTD} + \text{GTD}$$

Όπου η Γεωμετρική Χρονική Διαφορά (Geometric Time Difference – GTD) προέρχεται από τη γεωμετρία, για παράδειγμα οι διαφορές propagation delay μεταξύ του handset και των δύο BSs. Το GTD αποτελεί την ποσότητα πληροφοριών που έχουν να κάνουν με τη θέση του handset, καθώς ορίζει ένα hyperbola μεταξύ των δύο BSs. Επιπρόσθετα, σε ένα σύστημα όπως το WCDMA, όπου τα BSs δεν είναι συγχρονισμένα, η Σχετική Χρονική Διαφορά (Relative Time Difference – RTD) πρέπει να είναι γνωστή. Το RTD είναι η διαφορά μετάδοσης μεταξύ των σημάτων των γειτονικών BSs.

Στην εικόνα 66 διαφάνονται οι αρχές της μεθόδου TDOA positioning. Η θέση του τερματικού υπολογίζεται με βάση το TDOA μεταξύ του serving BS και των περιβάλλοντων BSs, που συνθέτουν μία hyperbola, το foci της οποίας συμπίπτει με την κεραία του πομπού του ανταποκρινόμενου BS. Η θέση του τερματικού μπορεί να υπολογιστεί με την τροποποίηση των αποστάσεων του τερματικού στις hyperbolas αν είναι διαθέσιμες περισσότερες από δύο τιμές TDOA.



Εικόνα 66 Time Difference of Arrival (TDOA) positioning

Γι' αυτόν τον λόγο, στη μέθοδο TDOA, η βασική ιδέα είναι ο καθορισμός της σχετικής θέσης του τερματικού εξετάζοντας τη χρονική διαφορά στην οποία καταφτάνει το σήμα στον στόχο (το τερματικό ή το

BS) αντί την απόλυτη χρονική στιγμή άφιξής του. Ως επόμενο, αν είναι διαθέσιμη η χρονική διαφορά μεταξύ του φορητού τερματικού και των περιβάλλοντων BSs και υπάρχει LOS μεταξύ τους, το φορητό τερματικό βρίσκεται εντός hyperbola:

$$D_i - D_3 = c\Delta t = c * \text{GTD} = \sqrt{[(X_i - x_m)^2 + (Y_i - y_m)^2 + (Z_i - z_m)^2]}$$

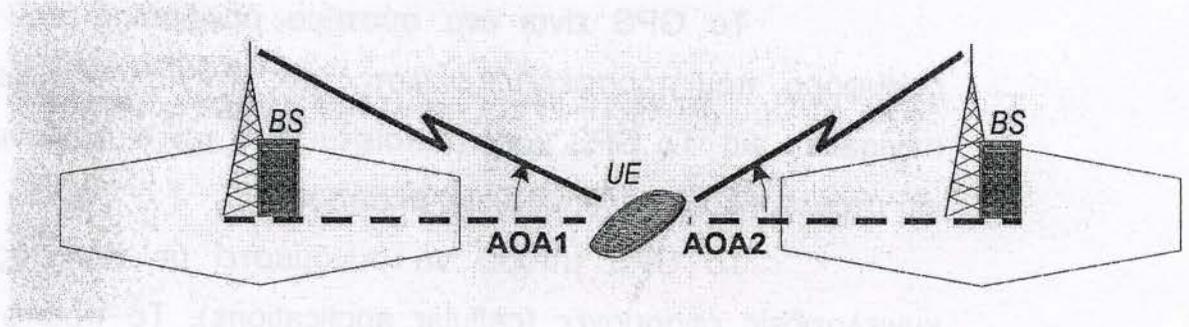
Όπου D_1 είναι η απόσταση από το φορητό handset στα περιβάλλοντα BSs και c η ταχύτητα του φωτός, Δt η χρονική διαφορά της άφιξης του signal από τα περιβάλλοντα BSs, X_i , Y_i και Z_i οι συντεταγμένες των BSs, και (x_m, y_m, z_m) οι συντεταγμένες του φορητού τερματικού. Όπως απεικονίζεται στο 66, με τον υπολογισμό δύο TDOA από τρία διαφορετικά BSs μπορεί να εκτιμηθεί η θέση του τερματικού στα κοινά σημεία αυτών των hyperbolas. Παρ' όλ' αυτά, για την προσκόμιση μοναδικής και πιο συγκεκριμένης εκτίμησης είναι απαραίτητες οι μετρήσεις τουλάχιστον τριών BS.

Γωνία άφιξης - Angle of Arrival Positioning (AOA)

Η θέση του τερματικού μπορεί επίσης να προσδιοριστεί με τον υπολογισμό του σημείου που συμπίπτουν δύο lines of pilot branches, η κάθε μία από τις οποίες διαμορφώνεται από μία νοητή γωνία από το BS προς το τερματικό. Η μέτρηση μίας μεμονωμένης γωνίας οδηγεί στη διαμόρφωση ζευγαριών γραμμών και προσδιορίζει τη θέση του επιθυμητού handset. Έτσι, όπως απεικονίζεται στην εικόνα 67, αν υπάρχει LOS μεταξύ του φορητού τερματικού και δύο BSs, και είναι διαθέσιμες οι μετρήσεις AOA δύο περιβάλλοντων BSs, η θέση του φορητού τερματικού ορίζεται από την τομή των γραμμών που προκύπτουν από τις γωνίες της άφιξης.

Παραπλήσια με τις μεθόδους TOA και TDOA, η ακρίβεια της μεθόδου AOA μπορεί να βελτιωθεί με τη χρήση περισσότερων από δύο μετρήσεων. Παρ' όλ' αυτά, το φαινόμενο reflection και diffraction προκαλούν σημαντικά σφάλματα, όταν η AOA χρησιμοποιείται σε ανοιχτό (urban) περιβάλλον. Υπό κανονικές συνθήκες το φορητό τερματικό δεν σε

θέση να καθορίσει το AOA από μόνο του και ως επόμενο, πρακτικά, το AOA πρέπει να υπολογίζεται στα BSs. Το implement του AOA είναι περίπλοκο και έχει μεγάλο κόστος, καθώς είναι απαραίτητες μεγάλες κεραιές στις εγκαταστάσεις λήψης. Από την άλλη πλευρά, είναι δυνατή η χρήση υπάρχουσας κεραιάς που αναλαμβάνει την αναμετάδοση του σήματος.



Εικόνα 67 Angle of Arrival (AOA) positioning

Reference Node Based Positioning (RNBP)

Η μέθοδος RNBP έχει ως βασική αρχή την επιλογή ενός κόμβου αναφοράς για να παρέχει στη φορητή συσκευή μετρήσεις auxiliary positioning. Ο κόμβος αναφοράς μπορεί να είναι κινητός ή εγκατεστημένος και να υποστηρίζει λειτουργίες relay ή repeater(αναμεταδότης). Μπορεί επίσης να αποτελεί συσκευή υπηρεσίας positioning, δέκτη GPS ή οποιουδήποτε είδους συσκευή γνωστής θέσης που μπορεί να χρησιμοποιηθεί ως σημείο αναφοράς κατά τον προσδιορισμό της θέσης των τερματικών.

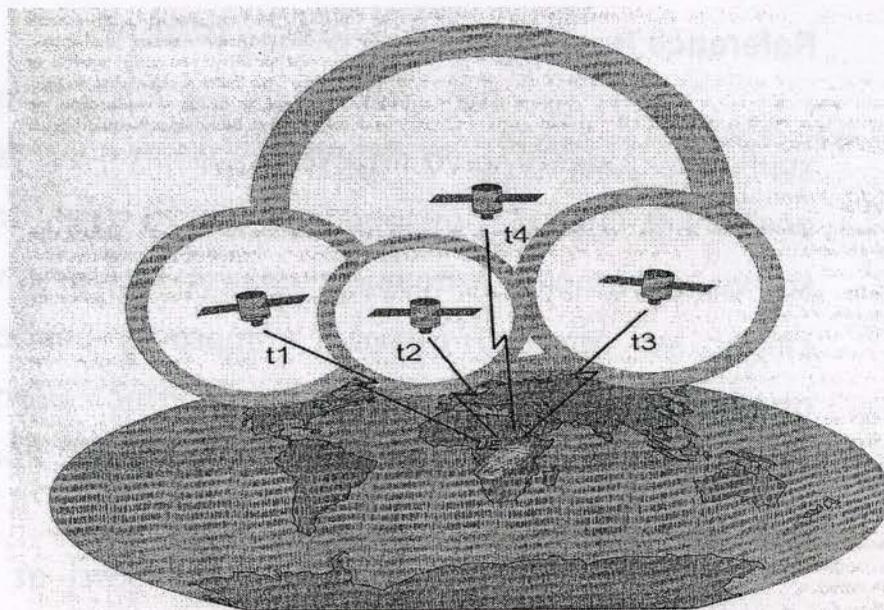
Το RNBP μπορεί να εφαρμοστεί σε οποιαδήποτε μέθοδο όπως TDOA, TOA ή AOA. Βασικό σημείο αποτελεί το γεγονός ότι το RNBP μπορεί να παρέχει enhanced positioning χρησιμοποιώντας επιπρόσθετες συσκευές αναφοράς στο δίκτυο. Από την άλλη πλευρά, το κόστος αυξάνεται καθώς τα RNBPs θα χρειαζόταν να τοποθετηθούν σε εγκαταστάσεις BS ή άλλες παρόμοιας φύσης, ενώ θα ήταν απαραίτητη η προσθήκη επιπλέον κεραιών. Πάντως, το επιπλέον κόστος μπορεί να

αντισταθμιστεί με τη χρήση αναμεταδοτών στα ραδιοφωνικά δίκτυα από υπάρχουσες εγκαταστάσεις δικτύου. Σε κάθε περίπτωση είναι σημαντική η σχεδίαση των δικτύων έτσι ώστε να αποφευχθούν τα αυξημένα επίπεδα παρεμβολών αναμετάδοσης.

Παγκόσμιο Σύστημα Τοποθέτησης - Global Positioning System (GPS)

Το GPS είναι ένα σύστημα positioning που βασίζεται σε δορυφόρο, που προσφέρει ποικιλοτρόπως την καλύτερη διαθέσιμη radio navigation aid. Το GPS χρησιμοποιείται από την Αμερικάνικη κυβέρνηση για στρατιωτικούς και δημόσιους σκοπούς.

Το GPS μπορεί να συνδυαστεί με πολλούς τρόπους με κυψελοειδείς εφαρμογές (cellular applications). Το πρώτο βήμα είναι η implement ενός GPS στο τερματικό, το οποίο προσφέρει τα ίδια πλεονεκτήματα με έναν ανεξάρτητο δέκτη GPS.



Εικόνα 68 GPS positioning

Η ακρίβεια και η ταχύτητα του δέκτη GPS μπορεί να βελτιωθεί σημαντικά με την αποστολή GPS assistance data στο τερματικό. Τα βοηθητικά δεδομένα δημιουργούνται χρησιμοποιώντας δέκτη αναφοράς GPS στο κυψελοειδές δίκτυο.

Η βασική αρχή που κρύβεται πίσω από το GPS είναι ότι έχει ως βάση τη μέθοδο TOA αλλά λόγω του ακριβή συγχρονισμού η εφαρμογή του GPS γίνεται περίπλοκη.

Το GPS προϋποθέτει τον ακριβή συγχρονισμό από ένα σύνολο δορυφόρων που συμμετέχουν στη διαδικασία positioning οι οποίοι μεταδίδουν/εκπέμπουν ένα spread (διάχυτο) spectrum signal στη Γη μέσω L-band. Ένα ακριβές ρολόι στον δέκτη υπολογίζει τη χρονική καθυστέρηση του σήματος μεταξύ των δορυφόρων και του δέκτη. Αυτό καθιστά δυνατό τον υπολογισμό της απόστασης του δέκτη από κάθε δορυφόρο. Στην περίπτωση που ο δέκτης παρατηρεί τρεις δορυφόρους, η θέση του μπορεί να προσδιοριστεί με τριγωνομετρική προσέγγιση. Σε πρακτικό επίπεδο, το ρολόι του δέκτη δεν χρειάζεται να είναι τόσο ακριβές αν τα signals από έναν τέταρτο δορυφόρο συμβάλλουν στη διόρθωση των σφαλμάτων του χρονομετρητή του δέκτη. Οι σφαιρικές επιφάνειες που περιβάλλουν τους δορυφόρους μπορούν να διαμορφωθούν με βάση τον χρόνο μετάδοσης του σήματος (signals' traveling time).

Έχοντας ορίσει τρεις σφαίρες, η θέση του δέκτη υπολογίζεται με το κοινό σημείο τους, παρέχοντας γεωγραφικές συντεταγμένες. Στο 68 απεικονίζεται η εκτίμηση θέσης με βάση το GPS.

Το GPS positioning αποτελεί το πλέον ακριβές σύστημα positioning, ειδικότερα όταν χρησιμοποιεί Differential GPS (DGPS) assistance. Παρ' όλ' αυτά, οι δέκτες GPS θα παρουσιάζουν υπό φυσιολογικές συνθήκες LOS στην περίπτωση τεσσάρων δορυφόρων, γεγονός που οδηγεί σε προβλήματα ειδικά σε κλειστούς χώρους. Επιπρόσθετα, ο δέκτης GPS διαθέτει αποκλειστική δορυφορική κεραία η οποία είναι συγκριτικά μεγάλου μεγέθους και μπορεί να προκαλέσει παρεμβολές με τις κυψελοειδής δραστηριότητες. Ο δέκτης GPS διογκώνει το κόστος κατασκευής και κατανάλωσης ενέργειας του φορητού τερματικού. Για να ξεπεραστεί ή τουλάχιστον να μειωθεί η έκταση αυτού

του προβλήματος, το GPS positioning και η GPS assistance υποστηρίζονται τόσο από GSM όσο και UMTS δίκτυα.

7.3.2.2. Ακρίβεια θέσης - Positioning Accuracy

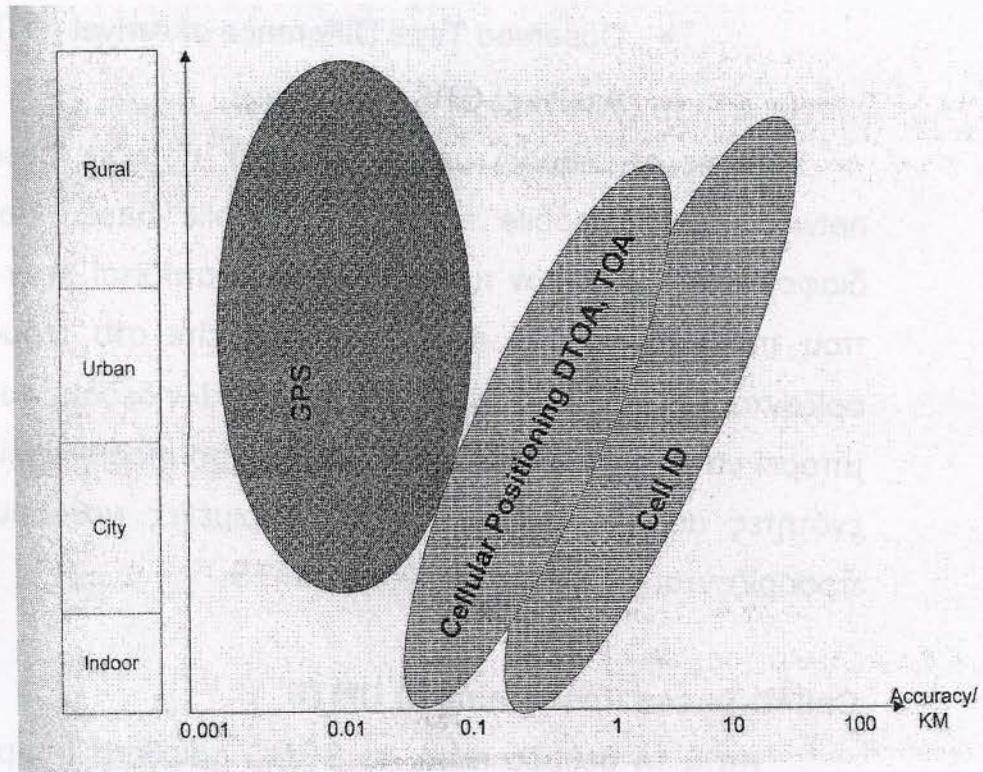
Όπως περιγράφηκε νωρίτερα, οι βασικές αρχές οποιασδήποτε μεθόδου positioning, εκτός από την cell-information based μέθοδο, βασίζονται στα χαρακτηριστικά του radio signal propagation που δεν είναι εύκολα προβλέψιμα. Με αυτόν τον τρόπο, η ακρίβεια των μεθόδων cellular positioning εξαρτώνται αυστηρά από το περιβάλλον (cellular environment), την διαθεσιμότητα LOS, τις μετρήσεις signal, τα χαρακτηριστικά του δέκτη, καθώς επίσης και από την προσέγγιση του εκάστοτε εφαρμοσμένου υπολογισμού.

Η ακρίβεια της μεθόδου που έχει ως βάση τη cell ID εξαρτάται από τη δομή cell του radio network. Σε μία δομή δικτύου με macro-cells η ακρίβεια θέσης ποικίλει από μερικά χιλιόμετρα μέχρι δεκάδες. Σε περιβάλλον pico-cell και micro-cell επίπεδο ακρίβειας κυμαίνεται μεταξύ λίγων έως δεκάδων μέτρων.

Η ακρίβεια της μεθόδου TOA εξαρτάται από το signal fading, το shadowing και τον αριθμό των μετρήσεων των signal branches που είναι διαθέσιμα για διαφορετικά BSs. Είναι θεμελιώδους σημασίας να υπάρχει LOS σε BSs έτσι ώστε να προσκομισθεί ακριβής εκτίμηση της θέσης του φορητού τερματικού. Δυστυχώς, αυτή η συνθήκη αντιπαράκειται στις αρχές σχεδιασμού κανονικού cellular network, και ως επόμενο δεν είναι εφικτή η απόλυτη/βέλτιστη ακρίβεια εντός των cellular networks.

Όπως και στη μέθοδο TOA, η ακρίβεια της μεθόδου TDOA υπόκειται στα χαρακτηριστικά του radio signal εντός του περιβάλλοντος του cellular network και στον αριθμό των διαθέσιμων μετρήσεων, ειδικά στις περιπτώσεις NLOS. Παρ' όλ' αυτά, κατά τη χρήση TDOA, από τη στιγμή που υπολογίζονται μόνο χρονικές διαφορές, είναι σύνηθες

φαινόμενο η παρουσίαση σφαλμάτων σε όλα τα BSs, γεγονός που οδηγεί στην ακύρωση της διαδικασίας positioning. Ως αποτέλεσμα, οι μέθοδοι που βασίζονται στο TDOA προσφέρουν καλύτερα αποτελέσματα από τις αντίστοιχες που βασίζονται στο TOA, ενώ κατά τα άλλα οι συνθήκες παραμένουν παραπλήσιες.



Εικόνα 69 GPS positioning

Συνοπτικά, δεν είναι δυνατή η γενίκευση της ακρίβειας διαφορετικών μεθόδων positioning, καθώς δεν υφίστανται απόλυτα λογικά κριτήρια, κι έτσι η ακρίβεια του positioning θα πρέπει να εξετάζεται και να εκτιμάται για κάθε περίπτωση ξεχωριστά. Παρ' όλ' αυτά, ο βαθμός ακρίβειας διαφορετικών μεθόδων μπορεί χονδρικά να αποδοθεί όπως απεικονίζεται στο 69.

7.3.2.3 Χαρακτηριστικές μέθοδοι τοποθέτησης για το UMTS

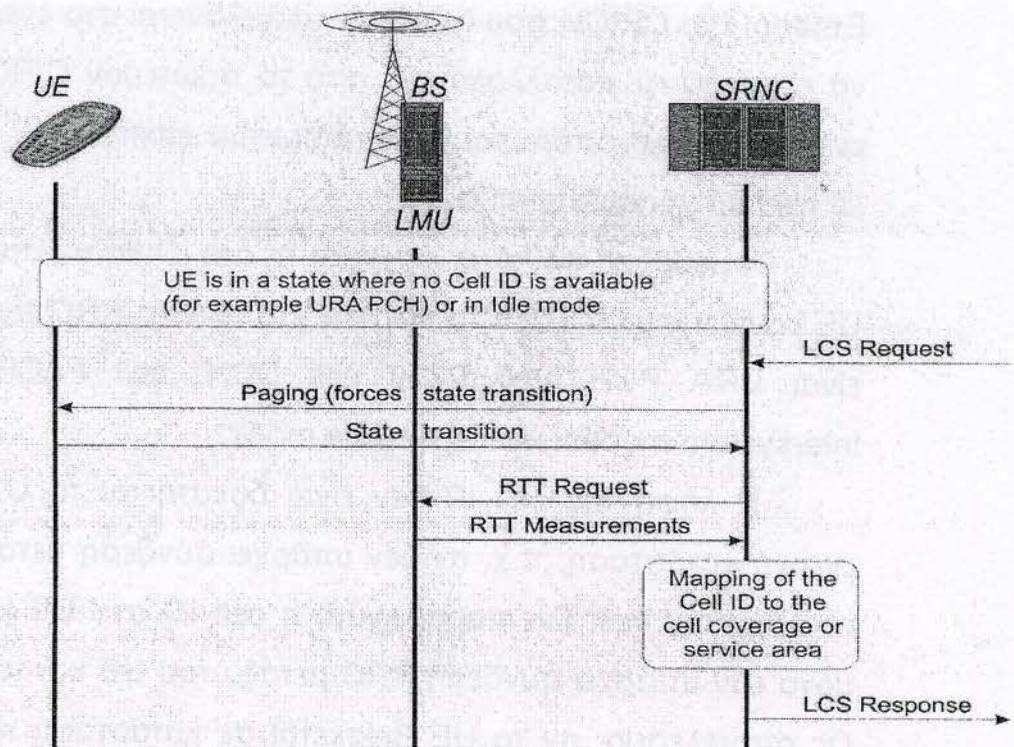
Όλες οι μέθοδοι positioning που περιγράφηκαν παραπάνω, εξετάστηκαν στη 3GPP από μία γενικευμένη/κατηγοριοποιημένη άποψη. Ως αποτέλεσμα, επιλέχθηκαν τρεις μέθοδοι για τα δίκτυα UMTS:

- Cell ID based positioning
- Observed Time Difference of Arrival (OTDOA)
- Assisted GPS positioning

Αυτές οι μέθοδοι μπορεί να είναι network based, mobile based, network based mobile assisted ή mobile based network assisted. Η διαφορά μεταξύ αυτών των προτύπων ενοπίζεται στον υπολογισμό θέσης που πραγματοποιείται είτε στο δίκτυο είτε στο τερματικό. Άλλοι τύποι ορίζονται από τη δημιουργία των βοηθητικών δεδομένων, οπότε η μέθοδος μπορεί να είναι τόσο network assisted όσο mobile assisted. Οι παρακάτω ενότητες ασχολούνται με τις συγκεκριμένες μεθόδους positioning που προορίζονται για χρήση σε δίκτυα UMTS.

Cell ID Based Positioning in UMTS

Κατά τη μέθοδο αυτή, το SRNC οριοθετεί (maps) την cell ID στον προκαθορισμένο Service Area Identifier (SAI). Υπάρχει η πιθανότητα να χρειαστούν επιπρόσθετες λειτουργίες αν το UE βρίσκεται σε κατάσταση soft handover ή σε κατάσταση RRC, κατά τις οποίες το cell δεν είναι προσδιορισμένο



Εικόνα 70 Cell ID based positioning, general procedure

Σε κατάσταση soft handover, το UE μπορεί να έχει συνδεδεμένα διαφορετικά signal branches σε διαφορετικά cells, δηλώνοντας διαφορετικές cell Ids. Σε αυτήν περίπτωση η εκτίμηση της θέσης βασίζεται στην απόκρυψη του cell (cell coverage based position estimate) και μπορεί να βελτιωθεί με τον συνδυασμό όλων των διαθέσιμων πληροφοριών στο SRNC.

Φυσιολογικά, η επιλογή της cell ID βασίζεται στις παραμέτρους που ορίζουν την ποιότητα των ληφθέντων signal branches. Έτσι, το SRNC επιλέγει τη cell ID με το ισχυρότερο signal branch ως αναφορά για τον προσδιορισμό της θέσης του UE. Διαφορετικά, η πρώτη cell ID που δημιουργήθηκε με την έναρξη της σύνδεσης μπορεί να επιλεγεί ως cell προσδιορισμού θέσης. Επιπρόσθετα σε αυτούς τους συνηθισμένους μηχανισμούς, λαμβάνονται υπόψη και άλλα κριτήρια επιλογής της cell ID κατά το handover.

Η cell ID μπορεί να καθοριστεί σύμφωνα με το primary common pilot channel (CPICH) στο ενεργό σύνολο BSs που έχει λάβει το τερματικό.

Επίσης, ένα CPICH που δε συμπεριλαμβάνεται στο ενεργό σύνολο μπορεί να εξελιχθεί σε καταλληλότερο από το πρωτεύον CPICH που ανήκει στο ενεργό σύνολο οπότε και χρησιμοποιείται έπειτα στον καθορισμό της cell ID που θα χρησιμοποιηθεί.

Η μέθοδος που έχει ως βάση τη cell ID θα πρέπει να υποστηρίζει το UE positioning ανεξάρτητα από την κατάσταση RRC της σύνδεσης η οποία είναι URA PCH, cell PCH, cell DCH, cell FACH, cell reselection, intersystem modes, καθώς και idle mode.

Η λήψη της cell ID δεν είναι δυνατή αν το UE δεν βρίσκεται σε ενεργή κατάσταση, π.χ. αν δεν υπάρχει σύνδεση μεταξύ του UE και ενός τουλάχιστον cell. Για παράδειγμα, η cell ID στο UE μπορεί να υφίσταται μόνο εάν υπάρχει σύνδεση RRC μεταξύ του UE και τουλάχιστον ενός BS. Ως αποτέλεσμα, αν το UE βρίσκεται σε κατάσταση κατά την οποία είναι αδύνατη η παροχή cell identifier, το UE αλλάζει αναγκαστικά σε κατάσταση που την επιτρέπει. Για παράδειγμα, σε κατάσταση URA PCH η cell ID μπορεί να μην είναι διαθέσιμη, οπότε το UE γυρνάει σε αναγκαστική αλλαγή κατάστασης καναλιού η οποία περιέχει τη cell ID, π.χ. κυψέλη FACH, έτσι ώστε να καθορίσει τον cell identifier. Το δίκτυο μπορεί επίσης να αποτρέψει το UE από το να διεισδύσει στην κατάσταση αναβάθμισης URA έτσι ώστε να προσκομίσει cell id updates όταν το UE επιλέγει ένα νέο cell. Όταν το UE βρίσκεται σε κατάσταση idle ή URA PCH, είναι απαραίτητο να καθοδηγηθεί για σκοπούς positioning από το CN ή το UTRAN.

Στο UMTS, τα πιθανά UTRAN θα πρέπει να μην γνωστοποιούνται στο CN. Ως αποτέλεσμα, ο cell identifier οδηγείται (mapped) στον service area identifier, που με τη σειρά του αποστέλεται από το UTRAN στο CN μέσω του Iu interface. Η περιοχή υπηρεσιών (service area) μπορεί να περιέχει περισσότερα του ενός cell, όμως προς το παρόν ισχύει αμφίδρομη συνεργασία (one-to-one relationship) μεταξύ της cell ID και του service area identifier εντός του UTRAN.

Observed Time Difference of Arrival-Idle Period Down Link (OTDOA-IPDL) in UMTS

Η δεύτερη μέθοδος UMTS positioning OTDOA-IPDL αποτελείται από δύο μέρη. Κατ' αρχάς, από το OTDOA, το οποίο είναι θεωρητικά παραπλήσιο με το TDOA που περιγράφηκε νωρίτερα. Παρ' όλ' αυτά, σε αυτό το σκέλος δίνεται έμφαση στο ότι το UE υπολογίζει τις ληφθείσες χρονικές διαφορές μεταξύ των περιβάλλοντων BSs με σκοπό την εκτίμηση της θέσης του UE.

Η μέτρηση των OTDOA και RTD δεν είναι απολύτως άμεση/δρομολογίσιμη, εξαιτίας των παρακάτω λόγων:

- Σε ορισμένες περιπτώσεις ένας επαρκής αριθμός downlink pilot signals μπορεί να μην είναι διαθέσιμος προς μέτρηση από το UE. Αυτό μπορεί να συμβαίνει όταν το UE βρίσκεται τόσο κοντά στο serving BS που ο δέκτης μπλοκάρεται από την ισχύ της μετάδοσης/εκπομπής. Η περίπτωση αυτή αναφέρεται ως "hearability effect".

- Τα BSs συνήθως δεν είναι συγχρονισμένα εντός WCDMA-FDD, οπότε η διαφορά συγχρονισμού μεταξύ των BSs, η RTD, θα πρέπει να γνωστοποιηθεί ή να μετρηθεί πριν γίνει εφικτός ο υπολογισμός της θέσης του τερματικού.

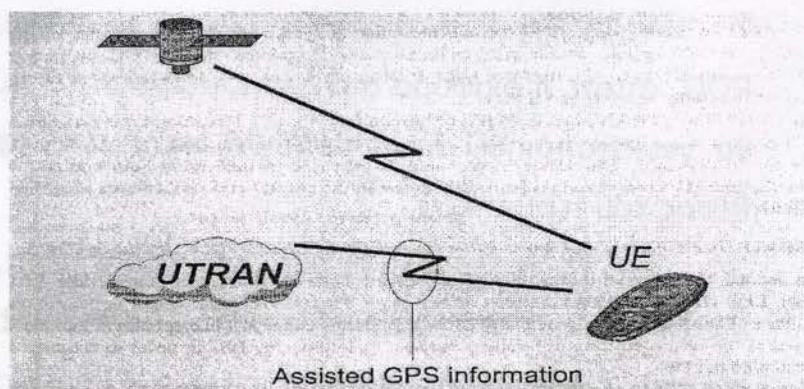
Για να ξεπεραστούν αυτά τα προβλήματα, εξετάστηκαν δύο πιθανές λύσεις, πρώτα στα Ιαπωνέζικα standardization bodies κι έπειτα στο 3GPP για την ενεργοποίηση υποστήριξης UE positioning σε δίκτυα WCDMA-FDD.

Κατά την πρώτη εκδοχή, θα γινόταν προσωρινή αύξηση της ισχύος μετάδοσης των περιβάλλοντων BSs, έτσι ώστε να ξεκινήσει μετρήσεις το UE. Παρ' όλ' αυτά, καθώς το WCDMA-FDD, όπως και κάθε άλλη CDMA based radio technology είναι interference-limited, η προσέγγιση αυτή δεν μπορεί να είναι εφικτή καθώς τελικά, θα οδηγούσε σε διόγκωση των επιπέδων παρεμβολών στο δίκτυο.

Η άλλη λύση προτείνει την παύση μετάδοσης από το serving BS για μικρά χρονικά διαστήματα έτσι ώστε να μειωθεί το πρόβλημα του hearability. Η μέθοδος αυτή ονομάζεται "Idle Period Down-Link" (IPDL). Κατά τη διάρκεια μίας idle period του serving BS, το UE μπορεί να μετρήσει τα signals των περιβάλλοντων BSs. Επίσης, κατά τις περιόδους αυτές, οι RTDs μπορούν να υπολογιστούν με περισσότερη ακρίβεια. Οι μονάδες μετρήσεων που χρησιμοποιούνται για αυτόν τον σκοπό μπορούν να τοποθετηθούν εντός ή κοντά σε BS sites (εγκαταστάσεις BS) κατά τη χρήση IPDL.

Assisted GPS for UMTS

Υπάρχουν δύο βασικοί τύποι assisted GPS, ονομαστικά οι UE based και UE-assisted, οι οποίοι διαφέρουν στο σημείο διεξαγωγής του υπολογισμού θέσης. Πρέπει να σημειωθεί ότι το UE είναι επίσης πιθανό να λάβει GPS assistance data από το δίκτυο κατά τη μέθοδο UE-assisted GPS



Εικόνα 71 Assisted GPS

Κατά τη περίπτωση UE based assisted GPS το UE περιέχει έναν ολοκληρωμένο δέκτη GPS και ο υπολογισμός της θέσης πραγματοποιείται από το UE. Τα GPS assistance data που αποστέλλονται από το δίκτυο στο UE συμπεριλαμβάνουν:

- Βοηθητικά δεδομένα μετρήσεων (Measurement assistance data), όπως είναι ο χρόνος αναφοράς, η λίστα ορατών δορυφόρων, το

satellite signal Doppler και το code phase search window. Τα δεδομένα αυτά παραμένουν έγκυρα για 2 έως 4 ώρες.

- Βοηθητικά δεδομένα για υπολογισμό θέσης (Assistance data for position calculation) που είναι η θέση/τόπος αναφοράς, η satellite ephemeris και τα clock corrections. Τα δεδομένα αυτά παραμένουν έγκυρα για 4 ώρες.

Κατά τη χρήση διαφοροποιημένων GPS αποστέλλονται επίσης διαφοροποιημένα διορθωτικά δεδομένα (correction data) στο τερματικό. Αυτός ο τύπος assistance data είναι έγκυρος για περίπου 30s, καλύπτει όμως μία σχετικά μεγάλη γεωγραφική περιοχή. Ως επόμενο, είναι δυνατή η δημιουργία βοηθητικών δεδομένων με τη χρήση ενός μόνο κεντρικά τοποθετημένου δέκτη αναφοράς (centrally located reference receiver).

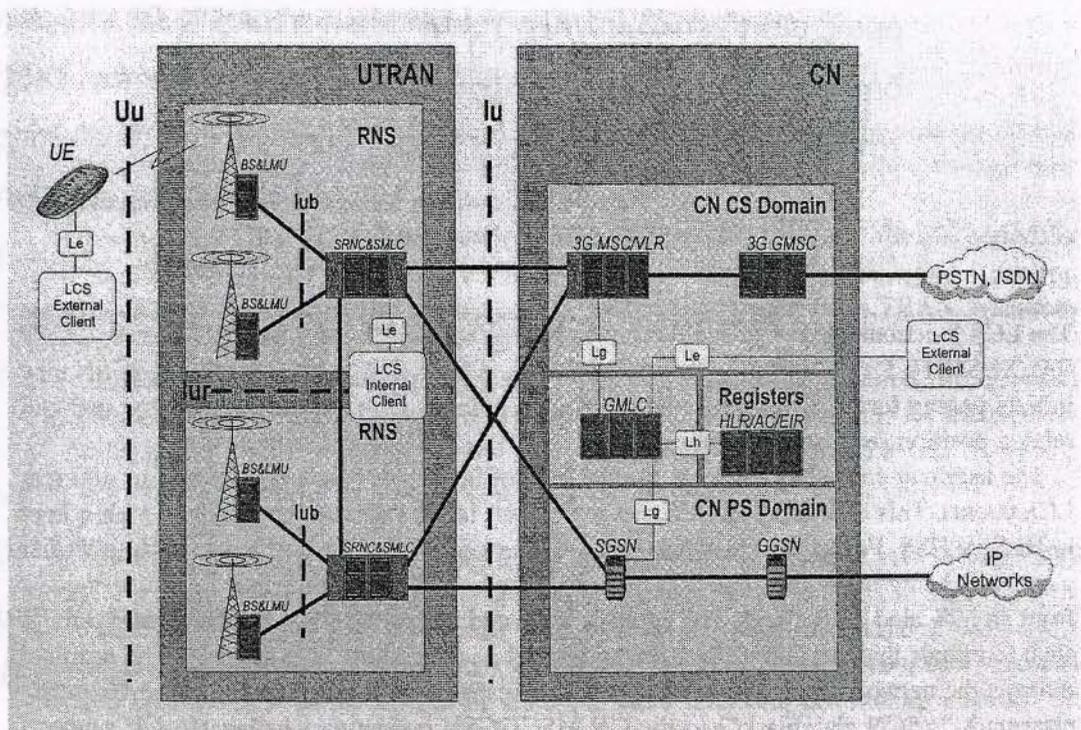
Κατά την network based UE-assisted GPS solution, το UE διαθέτει έναν μειωμένης ισχύος δέκτη GPS. Με τη χρήση αυτού του δέκτη το UE πραγματοποιεί μετρήσεις ψευδούς απόστασης (pseudorange measurements) τα αποτελέσματα των οποίων μεταδίδει σε μια υπολογιστική μονάδα του δικτύου η οποία διεκπεραιώνει το υπόλοιπο της λειτουργίας GPS. Κατά την εκδοχή αυτή, το δίκτυο στέλνει περιορισμένα βοηθητικά δεδομένα στο UE, το οποίο από την άλλη πλευρά πρέπει να στείλει μέσω uplink τα αποτελέσματα όλων των μετρήσεων. Ο χρόνος αναφοράς (reference time) πρέπει να είναι πιο ακριβής κατά το UE-assisted mode παρά κατά το UE based mode.

7.2.3.4 Αρχιτεκτονική της δομής του συστήματος UMTS για τις υπηρεσίες θέσης- Location Services (LCS)

Η λειτουργία τοπικών υπηρεσιών (Location Services functionality – LCS) στο UMTS διανέμεται σε υπάρχουσα μέρη του δικτύου κατά κύριο λόγο με τον ίδιο τρόπο όπως στο GSM. Ένα βασικό νέο στοιχείο/τμήμα δικτύου, το Gateway Mobile Location Centre (GMLC), προστίθεται στη

γενική/συνολική αρχιτεκτονική του συστήματος με σκοπό την υποστήριξη των τοπικών υπηρεσιών τόσο σε GSM όσο και UMTS.

Στην εικόνα 72 απεικονίζεται η συνολική αρχιτεκτονική του LCS στο UMTS. Ο εξοπλισμός και η λειτουργία του LCS βρίσκεται τόσο στο CN όσο και στο UTRAN. Το UTRAN περιέχει λειτουργίες για υπολογισμό θέσης με βάση τις παραπάνω μεθόδους και το σύνολο/συλλογή δεδομένων positioning. Στο CN το GMLC λειτουργεί ως σημείο σύνδεσης μέσω του οποίου μεταφέρονται τα positioning data σε άλλες δυνατότητες υπηρεσιών ή εφαρμογές πελατών.



Εικόνα 72 General LCS architecture in UMTS

Στο GSM, το Serving Mobile Location Centre (SMLC) μπορεί να αποτελεί ένα αυτόνομο φυσικό τμήμα/στοιχείο δικτύου ή να είναι ενσωματωμένο στο BSC. Στο UMTS η λειτουργία SMLC βρίσκεται ενσωματωμένη στο RNC ακολουθώντας τις αρχικές προδιαγραφές, όμως ένα ανεξάρτητο SMLC για υποβοηθούμενα GPS κατηγοριοποιείται.

Το SMLC εντός GSM και το serving RNC στο UTRAN επιλέγουν τη μέθοδο positioning, ελέγχουν τις μετρήσεις positioning και υπολογίζουν τη θέση του επιθυμητού τερματικού χρησιμοποιώντας τα αποτελέσματα των

που μπορούν να τη χειριστούν και να την αναδείξουν στον χρήστη. Το τερματικό ενημερώνει το δίκτυο σχετικά με αυτή τη δυνατότητα μέσω UE classmark. Το UE στέλνει στο CN MSC/SGSN classmark 2 (CN classmark) που γνωστοποιεί εάν το UE υποστηρίζει privacy verification ή όχι (LCS value added capability).

Το UE στέλνει επίσης classmark 3 (RAN classmark) στο RNC (και στο BSC + MSC στην περίπτωση του GSM) αναδεικνύοντας τις υποστηριζόμενες μεθόδους LCS. Αυτές οι πληροφορίες δεν είναι απαραίτητες στο CN. Στο PS domain οι ανταποκρινόμενες οντότητες πληροφοριών είναι η υπηρεσία UE και η δυνατότητα UE radio access.

Τα MSC και SGSN διαχειρίζονται τα charging και billing που συσχετίζονται με το LCS. Αυτό συμπεριλαμβάνει charging και billing τόσο για clients όσο και συνδρομητές μέσα στους οποίους είναι και οι home και roaming subscribers(συνδρομητές) από άλλα PLMNs. Τα MSC και SGSN δίνουν έγκριση για το provision της υπηρεσίας positioning για ένα συγκεκριμένο UE με τρόπο ίδιο όπως σε άλλες cellular services. Το MSC/VLR διαχειρίζεται το LCS εντός του CN PS domain ενώ το SGSN υποστηρίζει LCS στο CN PS domain.

Η υποστήριξη HLR για LCS συμπεριλαμβάνεται στον ρόλο του, σύμφωνα με τον οποίο περιέχει τα δεδομένα συνδρομής και τα προσωπικά προφίλ των συνδρομητών όπως επίσης και πληροφορίες σχετικά με το σε ποιο VLR και/ή SGSN είναι τώρα εγγεγραμμένο το φορητό τερματικό. Το GMLC αιτεί πληροφορίες δρομολόγησης (routing information), όπως είναι για παράδειγμα το VLR και/ή SGSN στο οποίο είναι εγγεγραμμένο το mobile, από το HLR μέσω ενός Mobile Application Part (MAP) based interface.

Το GMLC λαμβάνει τις αιτήσεις υπηρεσιών από εξωτερικούς LCS clients (ή από το ίδιο το φορητό τερματικό) και προωθεί την αίτηση positioning στο MSC/VLR ή στο SGSN σύμφωνα με το HLR. Πρέπει να σημειωθεί ότι το GMLC ουσιαστικά αποτελεί οντότητα gateway, η οποία

ενεργοποιεί μία σύνδεση μεταξύ του δικτύου και οποιοδήποτε εξωτερικού client.

Το GMLC αναγνωρίζει τον LCS client εντός του UMTS PLMN ανατρέχοντας σε προσδιορισμό του client (client verification) και έγκριση από το HLR, π.χ. βεβαιώνει ότι ο LCS client έχει τη δυνατότητα να πραγματοποιήσει positioning του συνδρομητή. Το GMLC καθορίζει αν η εκτίμηση της θέσης που έχει αποσταλεί από το δίκτυο συντρέχει με την αίτηση QoS που έχει οριστεί από τον LCS client. Το GMLC επίσης παρέχει έλεγχο ροής όσον αφορά τις αιτήσεις positioning κατά τη διάρκεια ταυτόχρονων αιτημάτων και μπορεί να μετατρέψει τις ληφθείσες πληροφορίες θέσης από το δίκτυο σε τοπικές συντεταγμένες. Το GMLC μπορεί να δημιουργήσει δικά του δεδομένα σχετικά με charging και billing για το LCS.

Λειτουργίες του LCS στο UTRAN

Το serving RNC στο UTRAN (ή το SMLC στο GSM) επιλέγει την κατάλληλη μέθοδο positioning με τη οποία επιτυγχάνεται το επιθυμητό QoS level για το αίτημα θέσης. Το SRNC επίσης ελέγχει τον τρόπο διεκπεραίωσης της μεθόδου positioning στο UE και στο UTRAN.

Κατά τη χρήση της μεθόδου OTDOA-IPDL, το SRNC ελέγχει και καθορίζει τις περιόδους idle σε διαφορετικά BSs με σκοπό την ελαχιστοποίηση της επίδρασης στην απόδοση του UTRAN. Αυτό πραγματοποιείται είτε σύμφωνα με προκαθορισμένες ρυθμίσεις είτε on-demand. Το RNC επίσης συγχρονίζει τους πόρους UTRAN που συμπεριλαμβάνονται στο positioning του τερματικού.

Στις network based μεθόδους positioning το SRNC υπολογίζει την εκτίμηση θέσης και αναδεικνύει την ληφθείσα ακρίβεια. Ελέγχει επίσης έναν αριθμό LMUs σε BSs με σκοπό την προσκόμιση ραδιοφωνικών μετρήσεων που κρίνονται απαραίτητες για την ανάδειξη της θέσης ή για να συμβάλλουν σε αυτή. Το signaling μεταξύ SRNC και LMU μεταφέρεται

μέσω του Iub interface και σε μερικές περιπτώσεις soft handover μέσω του Iur interface.

Στο UMTS, το LMU συνήθως ενσωματώνεται σε BS και το αυτόνομο/ανεξάρτητο LMU πιθανότατα θα παραμείνει απροσδιόριστο. Οι βασικές λειτουργίες του LMU έχουν να κάνουν με τη μέτρηση της RTD μεταξύ διαφορετικών BSs, τις Absolute Time Differences (ATD) σε ρολί αναφοράς, ή οποιοδήποτε είδος μέτρησης radio interface timing των σημάτων που έχουν μεταδοθεί από τα BSs. Μερικά αποτελέσματα μετρήσεων που επιστράφηκαν από το LMU στο SRNC μπορούν να χρησιμοποιηθούν σε περισσότερες από μία μεθόδους positioning. Όλες οι μετρήσεις θέσης και οι βοηθητικές μετρήσεις που έχει προσκομίσει ένα LMU αποστέλλονται μόνο στο SRNC που είναι συσχετισμένο με το ανταποκρινόμενο BS. Το SRNC ελέγχει τον συγχρονισμό οποιασδήποτε periodicity των μετρήσεων του LMU εντός BS, είτε άμεσα είτε βάση προκαθορισμένων ρυθμίσεων.

Λειτουργίες του LCS στο UE

Ανάλογα με τη μέθοδο positioning, το UE μπορεί να λαμβάνει μέρος στις διαδικασίες positioning ποικιλοτρόπως. Για παράδειγμα, σε μία network based μέθοδο positioning, το UE δεν υπολογίζει τη θέση, τη στιγμή που μία mobile based μέθοδος positioning μπορεί. Επίσης, το UE μπορεί να είναι εξοπλισμένο με δέκτη GPS, ο οποίος ενεργοποιεί τον ανεξάρτητο/αυτόνομο προσδιορισμό της θέσης. Η λειτουργία GPS εντός του UE μπορεί να βελτιωθεί από το δίκτυο με την αποστολή βοηθητικών πληροφοριών GPS στο φορητό. Σύμφωνα με μία εκδοχή μεθόδου assisted GPS η θέση του UE που φέρει δέκτη GPS καθορίζεται στο δίκτυο με βάση τα αποτελέσματα των μετρήσεων GPS από το UE.

Το φορητό τερματικό μπορεί να ζητήσει από το δίκτυο να καθορίσει τη θέση του (network assisted positioning) ή το ίδιο το τερματικό μπορεί να προσδιορίσει τη θέση του μετρώντας τον συγχρονισμό των σημάτων και

χρησιμοποιώντας τα αποτελέσματα των μετρήσεων και βοηθητικά δεδομένα από το δίκτυο. Το UE μπορεί επίσης να περιέχει μία εφαρμογή LCS, η οποία λειτουργεί σαν LCS client.

Η χρήση IPDL προϋποθέτει τη δυνατότητα του UE να κάνει μετρήσεις και να αποθηκεύει τις radio signal timing idle periods, και να correlate διαφορετικούς κώδικες BCH με διαφορετικές idle period patterns. Το UE χρειάζεται να καθορίσει τον χρόνο/στιγμή άφιξης του πρώτου ανιχνευμένου path, τόσο για το serving BS όσο και για τα υπόλοιπα BSs που ανιχνεύει. Θα πρέπει επίσης να είναι σε θέση να αποστέλει τα αποτελέσματα πίσω στο SRNC.

LCS πελάτης και GMLC περιβάλλον

Ο LCS client παρέχει υπηρεσίες βασιζόμενες σε πληροφορίες θέσης και μπορεί να ερμηνευτεί σαν οντότητα λογικής λειτουργίας (logical functional entity) που αιτεί πληροφορίες θέσης από το κυψελοειδές δίκτυο (cellular network) για ένα ή περισσότερα επιθυμητά (target) τερματικά. Το αίτημα μπορεί να περιέχει ένα καθορισμένο σετ/σύνολο παραμέτρων που ορίζουν το αιτούμενο QoS και τον χρόνο απόκρισης. Ο LCS client μπορεί να reside σε μια οντότητα/στοιχείο (συμπεριλαμβανομένου του UE) εντός του PLMN ή σε μία οντότητα εκτός PLMN.

Παράλληλα με την υποστήριξη του LCS από βασικά interfaces του UMTS, όπως είναι τα Uu, Iub, Iur και Iu, τα ακόλουθα νέα LCS interfaces ορίζονται για GMLC:

- Το interface μεταξύ LCS client και GMLC καλείται Le και απεικονίζεται στην εικόνα 73. LCS client αποστέλλει το αίτημα θέσης (position request) στο συγκεκριμένο interface και το GMLC στέλνει τα ανάλογα αποτελέσματα πίσω στον LCS client.
- Το Lh αποτελεί ένα νέο interface μεταξύ του GMLC και του HLR (HSS) όπως απεικονίζεται στην εικόνα 73. Το GMLC χρησιμοποιεί

αυτό το interface για να προσκομίσει τα routing information data τόσο για CS όσο και για PS domain από το HLR.

- Το GMLC (στο οικιακό PLMN ή άλλο PLMN) είναι συνδεδεμένο με το MSC/VLR μέσω του Lg interface. Το Lg interface χρησιμοποιείται επίσης μεταξύ GMLC και SGSN. Το GMLC προωθεί το αίτημα θέσης για ένα συγκεκριμένο τερματικό (target terminal) στο σωστό MSC/VLR ή SGSN χρησιμοποιώντας το Lg interface και το MSC/VLR και SGSN επιστρέφουν το αποτέλεσμα στο GMLC.

Τόσο το Lh όσο και το Lg interface έχουν ως βάση το πρωτόκολλο MAP.

Τα πλεονεκτήματα της αρχιτεκτονικής λύσης LCS στο UMTS

Η αρχιτεκτονική του συστήματος UMTS LCS είναι παρόμοια με εκείνη του LCS στο GSM, αλλά ορισμένες μη απαραίτητες λύσεις δικτύου (optional network solutions) δεσμεύτηκαν στο UMTS LCS έτσι ώστε να μειωθεί η πολυπλοκότητα αυτής της λύσης/πρότασης. Σε σύγκριση με το GSM LCS, το UTRAN που έχει ως βάση το WCDMA-FDD παρουσιάζει τα πλεονεκτήματα και τους περιορισμούς όσον αφορά τις εφαρμογές cellular positioning, οι οποίες σχετίζονται κατά κύριο λόγο με την νέα τεχνολογία ασύρματης πρόσβασης.

Στο UMTS, το SRNC παίζει βασικό ρόλο στον έλεγχο της ασύρματης πρόσβασης, συμπεριλαμβάνοντας τη διαχείριση ασύρματων πόρων (radio resource management). Οι μετρήσεις radio link, συμπεριλαμβανομένων των μετρήσεων soft handover, τερματίζονται και ελέγχονται στο SRNC. Από τη στιγμή που ένα ποσοστό 30 - 40% των κλήσεων είναι πιθανό να συμπεριλαμβάνεται σε soft handover, το SRNC θα έχει σε πολλές περιπτώσεις πρόσβαση σε αποτελέσματα μετρήσεων που προορίζονται για θέματα/σκοπούς positioning. Είναι λογική λοιπόν η εκμετάλλευση αυτού του προτερήματος του WCDMA-FDD όταν αναφερόμαστε στην

αρχιτεκτονική LCS στο UMTS. Ως αποτέλεσμα, οι λειτουργίες που καλούνται/ανταποκρίνονται στο SMLC εντός GSM εντοπίζονται στο SRNC εντός του UMTS.

Είναι επίσης πιθανό, να χρησιμοποιηθούν βοηθητικά δεδομένα LCS (LCS assistance data) κατά τη βελτιστοποίηση της απόδοσης του συστήματος σε συνδυασμό με τη διαχείριση ραδιοφωνικών πόρων (radio resources management) γεγονός το οποίο ενισχύει την τοποθέτηση λειτουργιών LCS στο SRNC. Η κοινή αρχιτεκτονική για το LCS και το radio resource management στο RNC, προσδίδει προνόμια στην βελτιστοποίηση της χρήσης (ασύρματων πόρων) radio resources, signaling load (φόρτωση σημάτων) και μηχανισμών positioning, γεγονός που οδηγεί σε αυξημένη/βελτιωμένη απόδοση του συστήματος.

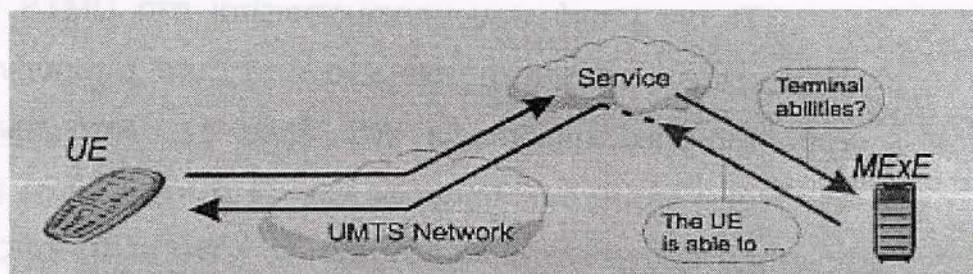
Τα επιπρόσθετα προνόμια που προσφέρει αυτή η λύση αρχιτεκτονικής αποτελούν τις απλοποιημένες προδιαγραφές signaling στα lu, lur και Uu interfaces σε σύγκριση με το εύρος επιλογών στο GSM. Στο UMTS βασική αρχή αποτελεί ο διαχωρισμός των radio related aspects από τα CN aspects κατάσταση που ισχύει και για το LCS.

7.3.3 Η ικανότητα υπηρεσιών – Εκτέλεση της κινητής εφαρμογής στο περιβάλλον (MExE)

Το τερματικό που χρησιμοποιείται στο UMTS δεν ακολουθεί ένα συγκεκριμένο πρότυπο: ορισμένα από αυτά μπορούν να παρουσιάσουν χαρακτηριστικά multimedia ενώ άλλα όχι. Από την άλλη πλευρά, οι υπηρεσίες παρέχουν πληροφορίες σε συγκεκριμένη μορφή (format). Το ερώτημα που γεννάται λοιπόν, έχει να κάνει με το πώς θα παρουσιαστούν στην κατάλληλη μορφή (format) στο τερματικό οι πληροφορίες που παρέχουν οι υπηρεσίες. Ως λύση του προβλήματος αυτού, οι προδιαγραφές 3GPP παρουσιάζουν το Mobile Application Execution Environment (MExE).

Οι πληροφορίες που χειρίζεται το MExE είναι MExE classmark, η οποία παρέχεται από τα τερματικά που υποστηρίζουν αυτό το περιβάλλον. Υπάρχουν δύο τύποι MExE classmark, οι classmark 1 και 2. Τα τερματικά που υποστηρίζουν input και output τύπου WAP παρέχουν MExE classmark 1: το αριθμητικό πληκτρολόγιο και το περιορισμένο μέγεθος οθόνης με καθορισμένο αριθμό χαρακτήρων, αποτελούν τις βασικές ενδείξεις για αυτήν την κατηγορία. Η MExE classmark 2 προέρχεται από το τερματικό εάν εκείνο υποστηρίζει Java οπότε χειρίζεται πιο ευέλικτες εκδοχές user interface: το χρώμα της οθόνης, πλήρες πληκτρολόγιο και πιο ισχυρές εφαρμογές, που αποτελούν τις βασικές ενδείξεις αυτής της περίπτωσης.

Υπό το πρίσμα του MExE, το συννεφάκι που καλείται "service" όπως απεικονίζεται στο 74, μπορεί να αποκαλείται MExE Service Environment (MSE). Το MSE δεν υπόκειται σε κάποια συγκεκριμένη παραμετροποίηση/ρύθμιση, καθώς η τελευταία εξαρτάται από τις υπηρεσίες που παρέχει στους τελικούς χρήστες ο service provider/carrier. Κατά κύριο λόγο, το MExE ως σύλληψη συνεργάζεται και με δίκτυα 2G, αλλά το δίκτυο UMTS αποτελεί την πρώτη βαθμίδα πλήρους υποστήριξής του. Εντός MSE και μεταξύ του τερματικού και του MSE οι πληροφορίες θα πρέπει να μεταφέρονται μέσω HTTP.

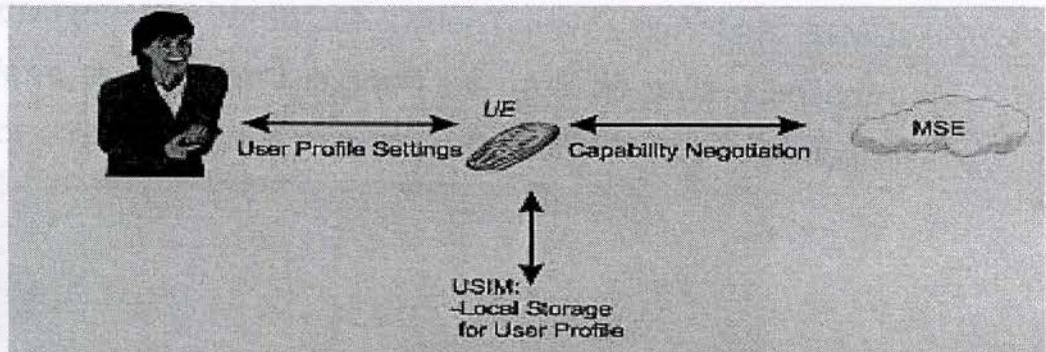


Εικόνα 74 Αρχές του MExE

Άλλη μία πλευρά σχετικά με το MExE αποτελεί το environment enabling personalization. Πολλοί παροχείς υπηρεσιών Internet παρέχουν τη δυνατότητα κατηγοριοποίησης (personalize) για παράδειγμα της αρχικής σελίδας σύμφωνα με τις προτιμήσεις του χρήστη. Το MExE κάνει

το ίδιο και για τις υπηρεσίες ή για να είμαστε πιο συγκεκριμένοι, για τη μορφή παρουσίασης των πληροφοριών (information presentation format).

Ο τελικός χρήστης μπορεί να φέρει τις ρυθμίσεις του τερματικού στα μέτρα του και αυτές οι πληροφορίες αποθηκεύονται τοπικά στο USIM. Ο τύπος του τερματικού και οι προκαθορισμένες ρυθμίσεις του καθορίζουν τις δυνατότητες του τερματικού και το MExE διαχειρίζεται εκείνες που έχουν να κάνουν με το δίκτυο.



Εικόνα 75 Profiles των χρηστών

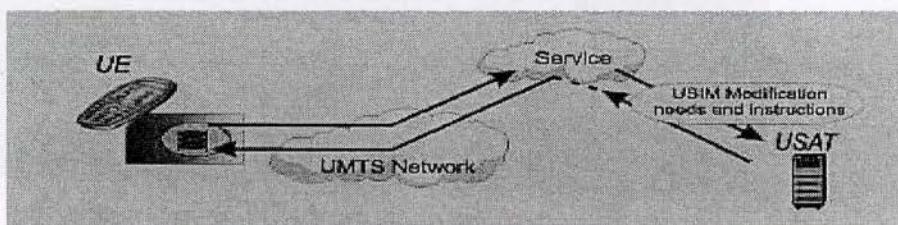
Το τελικό output που λαμβάνει ο χρήστης είναι το αποτέλεσμα της διαδικασίας κατά την οποία οι επιθυμητές πληροφορίες φιλτράρονται: πρώτα εξετάζονται οι δυνατότητες του τερματικού και έπειτα το προφίλ του χρήστη (75). Για παράδειγμα, η MExE classmark ενημερώνει το δίκτυο ότι το τερματικό μπορεί να διαχειριστεί WAP (classmark 1). Ο χρήστης έχει ορίσει πως θα έπρεπε να εμφανίζονται οι ληφθείσες πληροφορίες WAP (χαρακτήρες ανά γραμμή, αριθμός γραμμών κ.τ.λ.). Το MExE διαμορφώνει (format) τις πληροφορίες προς αποστολή σύμφωνα με τις παραπάνω οδηγίες.

7.3.4. Ικανότητα υπηρεσιών-Εφαρμογή του εγχειριδίου UMTS SIM (USAT)

Φυσιολογικά, η κάρτα UMTS SIM (USIM) είναι παρόμοια με την GSM SIM, αλλά υποστηρίζει πιο σύγχρονες λειτουργίες. Η USIM έχει περισσότερη μνήμη, μεγαλύτερη υπολογιστική ισχύ και είναι διαθέσιμη για

download. Αυτό δημιουργεί προοπτική για νέα είδη υπηρεσιών που δεν είναι απαραίτητο να συναντώνται και στα δίκτυα GSM. Πρέπει να σημειωθεί ότι η USIM είναι backward compatible με την GSM SIM αλλά αυτή η συμβατότητα δεν ισχύει κάτω από όλες τις συνθήκες.

Όπως απεικονίζεται στην εικόνα 76, ο μηχανισμός παραμετροποίησης / διαχείρισης της USIM (USIM manipulation facility) εφαρμόζεται με ξεχωριστή/ανεξάρτητη δυνατότητα υπηρεσίας, την USAT (UMTS SIM Application Toolkit). Με αυτόν τον μηχανισμό ο παροχέας υπηρεσιών είναι σε θέση να παρέχει υπηρεσίες οι οποίες μπορούν για παράδειγμα να παραμετροποιήσουν τη δομή των μενού του τερματικού.



Εικόνα 76 Αρχές του USAT

Με αυτόν τον τρόπο, ο παροχέας υπηρεσιών μπορεί να αναπτύξει εύκολη “one-click-type” πρόσβαση WAP, η οποία παρέχει τώρα περισσότερες υπηρεσίες από τον ίδιο service provider.

Το USAT αποτελεί ένα πολύ ισχυρό εργαλείο και όσον αφορά αυτήν την υπηρεσία ή carrier provider, μπορεί να επιφέρει σημαντικές αλλαγές στις παραμέτρους συνδρομής (subscription parameters) όπως είναι ο αριθμός IMSI. Αυτό μπορεί να κριθεί απαραίτητο σε μερικές υπηρεσίες που είναι implemented με το CAMEL, αλλά δε συνιστάται λόγω μεγάλου ρίσκου.

7.3.5. Ικανότητα υπηρεσιών CAMEL SCE

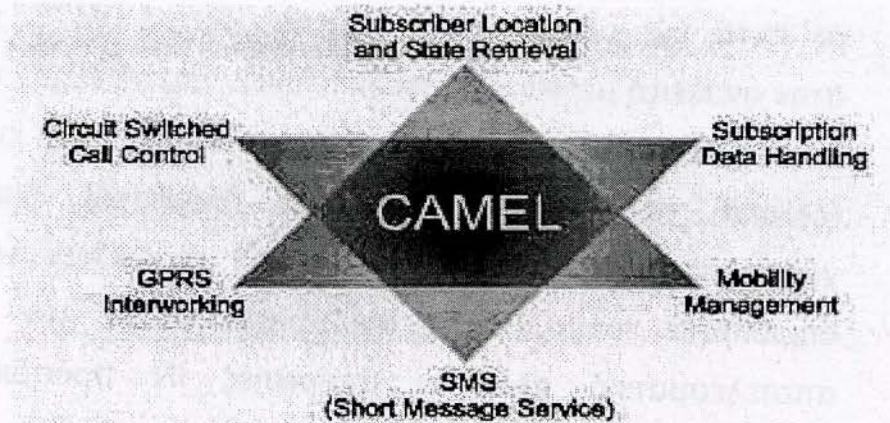
Το CAMEL από μόνο του αποτελεί μία πολύ μεγάλη οντότητα (entity) και δεν αποτελεί θέμα σε αυτό το βιβλίο με αυτήν την ιδιότητα. Παρ’

όλ' αυτά, έχει αξιοσημείωτο ρόλο στα δίκτυα UMTS, γεγονός που οδηγεί στην ανάδειξη μερικών βασικών πτυχών του σε αυτήν την ενότητα.

Όπως περιγράφηκε νωρίτερα, η εξέλιξη των κυψελοειδών δικτύων (cellular networks) περιέχει IN (Intelligent Network), το οποίο χρησιμοποιείται κατά κύριο λόγο για εξειδικευμένες υπηρεσίες και τη δημιουργία τους. Το IN implements αυτόν τον μηχανισμό (facility) αποτελεσματικά αλλά οι υπηρεσίες IN προσδιορίζονται από τον service/carrier provider. Οι υπηρεσίες IN αδυνατούν να μεταφέρονται μεταξύ δικτύων. Από την άλλη πλευρά, μία από τις βασικές προϋποθέσεις του UMTS είναι το αυτόματο roaming με πλήρες πακέτο υπηρεσιών. Η διαδικασία της τοποθέτησης τέτοιου είδους φορητότητας και ευκολίας υπηρεσιών πέρα από το IN καλείται CAMEL. Αν το αυτόματο roaming και το Service Creation Environment (SCE) χρησιμοποιούνται σε δίκτυα UMTS, κάθε συνδρομητής του δικτύου UMTS έχει επίσης εγγραφή CAMEL.

Όπως στην περίπτωση του IN, το CAMEL φροντίζει για τον έλεγχο της circuit switched connection. Έχει τις ίδιες ιδιότητες με το IN και μπορεί να αποδώσει το ίδιο ή περισσότερο αποτελεσματικά. Αντίθετα απ' το IN, το CAMEL μπορεί να εκτελέσει interworking με packet switched connections. Αυτό το τμήμα χρήσης του CAMEL δεν είναι πλήρως προσδιορισμένο και αναμένονται αξιοσημείωτες αλλαγές προς αυτήν την κατεύθυνση. Το CAMEL μπορεί να interoperate με όλες τις υπηρεσίες που χρησιμοποιούνται στο GSM και το SMS αποτελεί μία από αυτές.

Το MM αποτελεί μία εκδοχή που δεν υποστηρίζεται από το IN αλλά το CAMEL είναι ικανό να μεταφέρει πληροφορίες MM εντός και μεταξύ των δικτύων. Επίσης, interoperates με τις λειτουργίες συνδρομής σε δίκτυο UMTS (UMTS network register functions), π.χ. το HLR και το VLR μπορούν για αυτόν τον λόγο να διαχειριστούν δεδομένα συνδρομής (subscription data).



Εικόνα 77 Περιβάλλον λειτουργίας του CAMEL

Επιπρόσθετα στο MM, το CAMEL διατηρεί άμεσα interfaces με το LCS, οπότε έχει τη δυνατότητα να χρησιμοποιήσει/προσκομίσει πληροφορίες positioning διαθέσιμες μέσω του LCS. Τα σημεία επαφής του CAMEL με το LCS φαίνονται στο 7.23. Το CAMEL interface στο GSM τείνει στο gsmSCF (Lc) και για το UMTS προς το CSCF (Le).

7.3.6 Παράδειγμα : Ικανότητες υπηρεσιών σε κτίρια

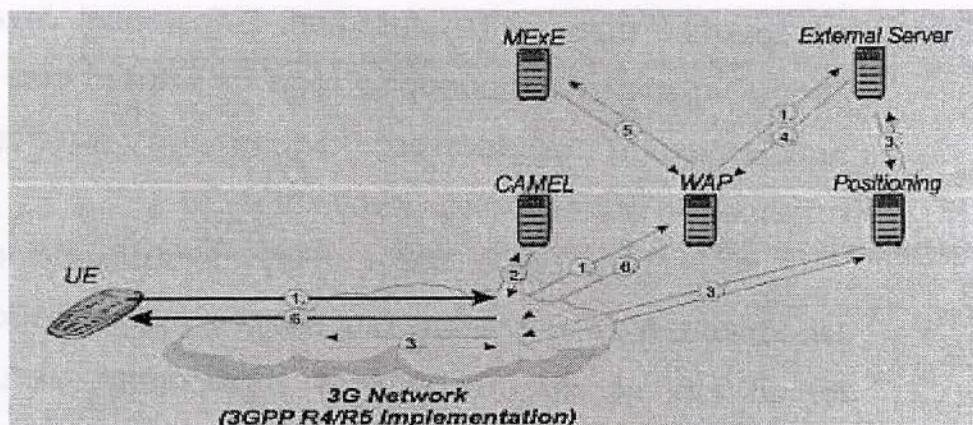
Το παράδειγμα αυτό σχετικά με την ταυτόχρονη χρήση διαφορετικών υπηρεσιών είναι καθαρά υποθετικό, αλλά στοχεύει στην ανάδειξη του τρόπου με τον οποίο μία υπηρεσία end-to-end χρησιμοποιεί δυνατότητες υπηρεσιών ως building blocks κατά την εφαρμογή του στο 3GPP R4/R5.

Ας υποθέσουμε ότι ένας συνδρομητής έχει στην κατοχή του ένα τερματικό που μπορεί να λάβει και να χειριστεί κείμενο, φωτογραφίες, multimedia, δηλαδή χρησιμοποιεί MExE classmark 2. Η συνδρομή που χρησιμοποιείται σε αυτήν την περίπτωση είναι προπληρωμένη, δηλαδή προϋπάρχει ένας λογαριασμός για κάθε transaction, ανεξάρτητα απ' το αν η τελευταία είναι circuit ή packet switched.

Οι υπηρεσίες που χρησιμοποιεί εδώ ο χρήστης θα μπορούσαν να βαφτιστούν ως “local entertainment” (τοπική διασκέδαση). Αυτή η υπηρεσία παρέχει πληροφορίες σχετικά με εστιατόρια, clubs κ.τ.λ. εντός της περιοχής, για παράδειγμα, στην οποία διαμένει ο χρήστης. Στην εικόνα 78 περιγράφεται η πιθανή ροή πληροφοριών.

Ο χρήστης χρησιμοποιεί την υπηρεσία “local entertainment” μέσω του web portal ενός provider. Αυτό οδήγησε τον service provider στο να στείλει το ανάλογο λογισμικό (software) στο USIM. Σ’ αυτήν την ενότητα, χρησιμοποιήθηκε το USAT και χρησιμοποιήθηκε για παράδειγμα ένα menu item για να εκκινήσει το “local entertainment” που προστέθηκε στο προφίλ του χρήστη στο USIM. Τώρα πλέον, ο χρήστης έχει όλα τα μέσα διαθέσιμα έτσι ώστε να κάνει χρήση της υπηρεσίας όταν το επιθυμεί.

1) Ο χρήστης ενεργοποιεί την υπηρεσία “local entertainment” με τη αποστολή μηνύματος σχετικά με τα κοντινά εστιατόρια. Αυτό το αίτημα διαμορφώνεται μέσω ενός browser παρόμοιου με εκείνον του WAP εντός του τερματικού που αποστέλλεται μέσω WAP gateway. Η WAP gateway αποστέλλει έπειτα το αίτημα σε έναν εξωτερικό server που περιέχει πληροφορίες που είναι απαραίτητες για την υπηρεσία “local entertainment”.



Εικόνα 78 Παράδειγμα για τις ικανότητες των υπηρεσιών

2) Κατά την πραγματοποίηση της σύνδεσης, το δίκτυο επιβεβαιώνει ότι η συγκεκριμένη συνδρομή είναι προπληρωμένου τύπου (pre-paid type) και ο λογαριασμός του συνδρομητή είναι έχει επιβεβαιωθεί από το CAMEL.

3) Ο εξωτερικός server χρειάζεται τις πληροφορίες positioning του συνδρομητή έτσι ώστε να προχωρήσει στην παροχή σχετικών πληροφοριών. Αιτεί τις πληροφορίες position από το GMLC, το οποίο με τη σειρά του ξεκινά διαδικασίες positioning εντός του δικτύου. Το GMLC διεκπεραιώνει το positioning του χρήστη χρησιμοποιώντας τις μεθόδους που περιγράφηκαν νωρίτερα. Το GMLC επιστρέφει τις πληροφορίες positioning του συνδρομητή στον εξωτερικό server, ο οποίος καθορίζει μέσω του λογισμικού εφαρμογών (application software) (directory, database κ.τ.λ.) ποιες είναι οι κατάλληλες πληροφορίες για κάθε περίπτωση.

4) Μετά τη λήψη των πληροφοριών, οι πληροφορίες επιστρέφονται στην WAP gateway ως ανταπόκριση στο αίτημα του συνδρομητή.

5) Η WAP gateway αιτεί οδηγίες παρουσίασης και πληροφορίες για το προφίλ του συνδρομητή από το MExE. Υποθετικά: αν το τερματικό υποστηρίζει classmark 1, η WAP gateway στέλνει τις πληροφορίες σε μορφή κειμένου σύμφωνα με τις δυνατότητες του τερματικού (μέγεθος απεικόνισης, αριθμός σειρών, αριθμός χαρακτήρων ανά σειρά κ.τ.λ.). Αν το τερματικό υποστηρίζει classmark 2 (personal Java) η WAP gateway μπορεί να στείλει πληροφορίες τόσο σε κείμενο όσο και γραφικά και να παρέχει ακόμα περισσότερες πληροφορίες, για παράδειγμα λογότυπα εστιατορίων, φωτογραφίες, μενού κ.τ.λ.

6) Όταν έχουν πλέον αναγνωρισθεί/λυθεί οι δυνατότητες του τερματικού, η WAP gateway διαμορφώνει τις πληροφορίες στο κατάλληλο format και τις αποστέλλει στον συνδρομητή μέσω του δικτύου. Το τερματικό ενημερώνει τον συνδρομητή, για παράδειγμα σχετικά με τη λίστα των εστιατορίων στο τρέχον cell. Η ακρίβεια του positioning εξαρτάται από την τεχνολογία positioning.

Αυτή η περιγραφή ενός παραδείγματος υπηρεσίας οδηγεί στο τέλος της αναφοράς μας στο δίκτυο UMTS ως μία ισχυρή πλατφόρμα για το στήσιμο value-added υπηρεσιών προς τους χρήστες 3G. Ο χρόνος θα δείξει τα όρια ανάπτυξης νέων υπηρεσιών που βασίζονται στις δυνατότητες υπηρεσιών που παρέχει η πλατφόρμα δικτύου UMTS.

7.4 Υπηρεσίες UMTS και σχέδια υπηρεσιών

Σε αυτήν την ενότητα αναδεικνύουμε μερικά αντικείμενα (items) που είναι συνδεδεμένα με τις υπηρεσίες end-to-end στο UMTS. Εντός του δικτύου UMTS βρίσκεται ένα δίκτυο για υπηρεσίες, για το οποίο κανείς δε μπορεί να προσδιορίσει το είδος των υπηρεσιών που θα χρησιμοποιούνται στα επόμενα χρόνια. Στην εφαρμογή των 3GPP R99 τα δίκτυα UMTS παρέχουν τις ίδιες αν όχι περισσότερες υπηρεσίες σε σχέση με το GSM. Αυτό σημαίνει ότι από την πλευρά του χρήστη, αυτές οι υπηρεσίες λειτουργούν με παρόμοιο τρόπο αλλά η implementation τους σε δίκτυο είναι πολλές φορές διαφορετική.

Η εξέλιξη από GSM σε UMTS, δεν αφήνει ανεπηρέαστη την εξέλιξη των υπηρεσιών. Το γεγονός αυτό δεν πέφτει στην αντίληψη του χρήστη αλλά επιφέρει σημαντικές αλλαγές στο δίκτυο. Αν μελετήσουμε την εξέλιξη αυτή εν αντιθέσει με τις προδιαγραφές 3GPP διαφάνεται πως ορισμένες εκδόσεις προδιαγραφών επικεντρώνονται σε συγκεκριμένα μέρη του δικτύου. Οι προδιαγραφές 3GPP R99 επικεντρώνονται στην wideband radio access στο δίκτυο και το CN υιοθετείται από το GSM με ασήμαντες αλλαγές. Οι προδιαγραφές 3GPP R4 αντιθέτως, επικεντρώνονται στο CN και παρουσιάζουν νέους μηχανισμούς όπως το IP Multimedia Subsystem (IMS). Σε αυτήν την περίπτωση αλλάζει επίσης η διαχείριση των υπηρεσιών του δικτύου. Για παράδειγμα, οι circuit switched voice calls θα μπορούσαν να παραδίδονται μέσω του IMS ως VoIP calls. Σύμφωνα με το 3GPP R5 θα υπάρξουν και πάλι αλλαγές όσον αφορά την πλευρά

πρόσβασης του δικτύου, με το CN να εξελίσσεται παραπέρα. Στον ακόλουθο πίνακα παρουσιάζεται η πλειοψηφία των υπηρεσιών GSM

Service(s)	Circuit Switched Domain R99	Packet Switched Domain R99
Speech (voice)	Supported	N/A (VoIP could be used in theory)
Facsimile	Supported	N/A (application level implementation like IP fax)
Alternate fax and speech	Supported	N/A
Circuit switched data bearer services	Supported	N/A
Supplementary services	Supported	N/A
USSD (unstructured supplementary service data)	Supported	N/A

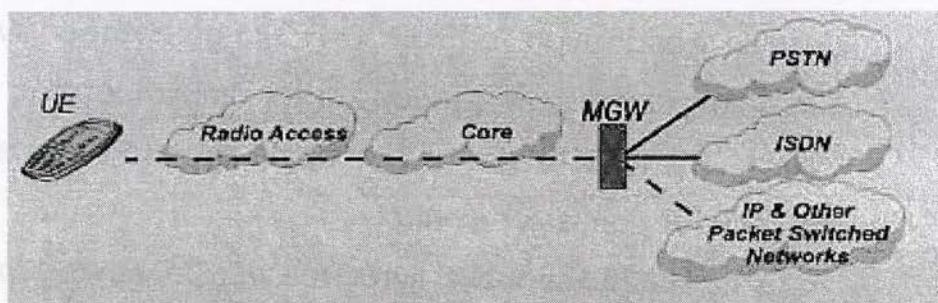
Πίνακας 79 Υπηρεσίες που κληρονομούνται από το GSM και η μεταχείρισή τους στο 3GPP R99

7.4.1. Υπηρεσίες και η υπο συζήτηση QoS Class

Στην πρώιμη φάση του UMTS η πιο συνηθισμένη υπηρεσία που θα χρησιμοποιεί conversational QoS class θα παραμείνει η υπηρεσία speech. Αν η τελευταία εφαρμογή εφαρμοστεί χρησιμοποιώντας το CN CS domain που μεταδόθηκε από το GSM, το QoS δεν θα αποτελεί πλέον θέμα. Τα στοιχεία του CS domain έχουν ήδη ενσωματωμένα QoS στον εξοπλισμό τους. Εξετάζοντας το θέμα από την πλευρά του UMTS, η κατάσταση είναι λίγο πιο περίπλοκη καθώς οι αλγόριθμοι κωδικοποίησης speech (speech coding algorithms) που χρησιμοποιούνται στο GSM και UMTS είναι διαφορετικοί. Το UMTS, παρ' όλ' αυτά, δίνει έμφαση στην interoperability μεταξύ του ίδιου και του GSM. Ως αποτέλεσμα της implemented interoperability με inter-system handovers η μέθοδος κωδικοποίησης speech μεταβάλλεται κατά τη διάρκεια της κλήσης (call). Για να διατηρηθεί η ποιότητα της σύνδεσης το σύστημα μπορεί προσωρινά/περιστασιακά να κάνει buffer στο bit stream representing speech.

Η λύση σε αυτό το δίλλημα είναι η χρήση μίας AMR (Adaptive Multi-Rate) τεχνικής κωδικοποίησης σύμφωνα με τις προδιαγραφές 3GPP. Ο AMR codec μπορεί να αναπαράγει ποικίλα source bit rates: 12.2, 10.2, 7.95, 7.40, 6.70, 5.90, 5.15 και 4.75 kb/s. Από αυτούς τους ρυθμούς, το 12.2 kb/s stream ανταποκρίνεται στο GSM-EFR (Enhanced Full Rate) που ισούται με τον GSM EFR codec. Μερικά από τα άλλα bit rates είναι επίσης συμβατά με άλλα 2G ψηφιακά συστήματα όπως το US-TDMA και το Ιαπωνικό PDC. Όσον αφορά την υπηρεσία speech, η λειτουργία του AMR speech codec μπορεί να ερμηνευτεί ως «μετατροπέας QoS» μεταξύ διαφορετικών τεχνολογιών ασύρματης πρόσβασης.

Το επόμενο βήμα είναι η μετατροπή της κοινής υπηρεσίας speech σε υπηρεσία packet switched, VoIP. Σύμφωνα με τις προδιαγραφές 3GPP R99, η υπηρεσία speech εξακολουθεί να χρησιμοποιείται με τον κλασικό τρόπο, π.χ. μέσω circuit switched connections. Οι προδιαγραφές 3GPP R4/R5 παρουσιάζουν τελείως διαφορετικές, universal δομές προς όφελος του packet switching. Αν το δίκτυο UMTS εφαρμόζεται σύμφωνα με το 3GPP R4/R5, η υπηρεσία speech μεταφέρεται ως packet switched από το τερματικό στη Media Gateway (MGW) μέσω του δικτύου.



Εικόνα 80 VoIP και δίκτυα

Η MGW φέρει όλους τους απαιτούμενους και σχετικούς μηχανισμούς για διαφορετικές περιπτώσεις μετατροπών, για παράδειγμα το AMR είναι μεταξύ αυτών. Καθώς τα περιβάλλοντα δίκτυα είναι κατά κανόνα circuit switched όπως το PSTN (Public Switched Telephony Network) και ISDN (Integrated Services Digital Network), το MGW περιέχει επίσης μερικούς μηχανισμούς μετατροπών (conversion mechanisms) για τα παραπάνω. Θα

πρέπει να σημειωθεί ότι αυτοί οι μηχανισμοί υπόκεινται σε περιορισμούς όσον αφορά τη ροή πληροφοριών, και πρέπει να φροντίζουν για την μετατροπή του signaling μεταξύ διαφορετικών δικτύων. Σχετικά με το VoIP, κυριαρχούν δύο εναλλακτικές για το call control signaling, η προδιαγραφή H.323 και το SIP (Session Initiation Protocol).

Το H.323 από το ITU-T μπορεί να χαρακτηριστεί ως “umbrella standard” καθώς περιέχει όλα τα σχετικά standards που απαιτούνται για τον καθορισμό μεταφοράς multimedia ροής (multimedia traffic delivery) σε τέτοιου είδους δίκτυα, που δεν είναι απαραίτητο να εγγυώνται για το QoS.

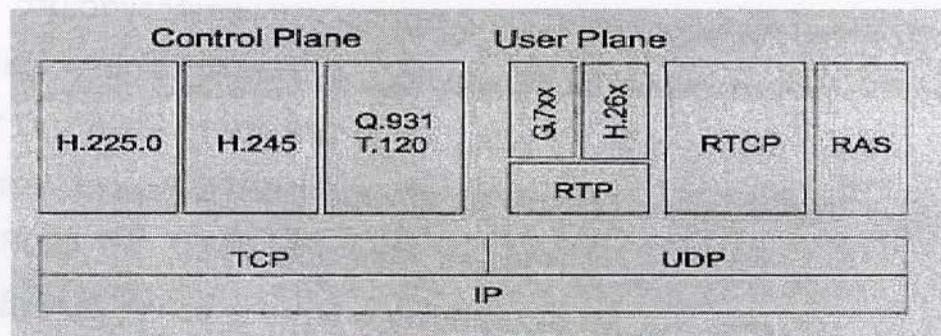
Το H.323 ορίζει τέσσερα στοιχεία δικτύου, τα terminal, gateway, gatekeeper και Multipoint Control Unit (MCU). Στα δίκτυα UMTS αυτά τα στοιχεία μπορούν να ερμηνευτούν ως λειτουργίες και διαχωρίζονται σε στοιχεία δικτύου: το τερματικό H.323 αποτελεί εφαρμογή του UE, η H.323 gateway είναι εν μέρει λειτουργία του MGW, ο H.323 gatekeeper προορίζεται ισομερώς για ποικίλες λειτουργίες load control σε UTRAN και CN nodes και η MCU αποτελεί ξεχωριστή λειτουργία του CN.

Η βασική λειτουργία της H.323 gateway είναι η ανάθεση συνδέσεων σε άλλα δίκτυα χρησιμοποιώντας διαφορετικές εκδοχές signaling, όπως είναι για παράδειγμα το ISUP. Ο H.323 gatekeeper είναι υπεύθυνος για τη διαχείριση των πόρων δικτύου και της διαθεσιμότητάς τους. Από αυτήν την άποψη, για παράδειγμα, η λειτουργία του H.323 gatekeeper εφαρμόζεται στο UTRAN admission control.

Το H.323 λειτουργεί εντός του περιβάλλοντος του πρωτοκόλλου που περιγράφηκε στο 81 και μεταφέρεται (carried) μέσω του IP stack. Στην περίπτωση signaling χρησιμοποιείται το TCP καθώς είναι πιο αξιόπιστο, αν και πιο αργό. Το UDP layer χρησιμοποιείται για δεδομένα χρήστη. Υπάρχει η περίπτωση σφάλματος όμως η ταχύτητα είναι πιο βαρυσήμαντη. Επιπλέον, το H.323 καλύπτει ποικίλα standards για διάφορους σκοπούς.

Control plane:

- H.225.0: αυτό το standard διαχειρίζεται το session management, data multiplexing και connection quality observation aspects.
- H.245: διαμορφώνει ένα κανάλι ελέγχου (control channel) που χρησιμοποιείται για μεταφορά δεδομένων σχετικά με τα υποστηριζόμενα audio και video coding formats, channel management και τον έλεγχο ροής (flow control) της σύνδεσης. Το H.245 είναι πολύ συχνά implemented με περιορισμένες δραστηριότητες (facilities).
- Q.931, T.120: ο H.323 gatekeeper μπορεί να εφαρμοστεί ποικίλα standards για την επίτευξη σύνδεσης. Η πιο σημαντική είναι η Q.931 που ορίζει τον ISDN-type του call set-up. Οι υπόλοιπες όπως η T.120 δεν είναι σημαντικές όσον αφορά τις συνδέσεις δεδομένων.



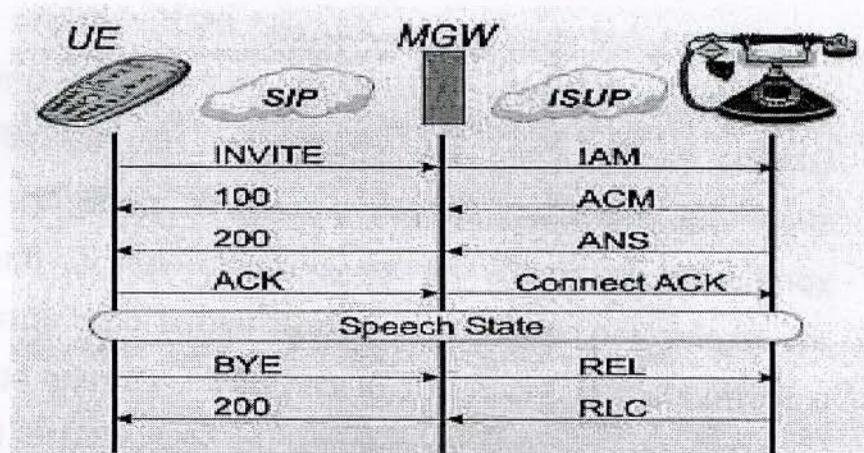
Εικόνα 81 το περιβάλλον του H.323 πρωτοκόλλου

Το H.323 user plane προορίζεται για audio και video transfer. Για τη μεταφορά αυτή, το H.323 ορίζει το αποκαλούμενο Real-time Transport Protocol (RTP) που προσδιορίζει frame structures και ελέγχει θέματα συγχρονισμού. Το RTP χρησιμοποιείται από διαφορετικούς αλγόριθμους συμπίεσης (codecs) οι περισσότεροι από τους οποίους δεν είναι θεμελιώδεις. Ο μοναδικός θεμελιώδης σημασίας codec είναι ο G.711 που είναι απαραίτητος για την εδραίωση κλασικού 64 ή 56 kb/s PCM coding για voice connections. Τα υπόλοιπα πρωτόκολλα, RTCP (Real-time Control Protocol) και RAS (Registration, Admission and Status) χρησιμοποιούνται για τον ποιοτικό έλεγχο της σύνδεσης, τον έλεγχο bandwidth και τη μεταφορά πληροφοριών κατάστασης (status information transfer).

Όπως είναι φανερό, η H.323 implementation του VoIP και άλλων υπηρεσιών πραγματικού χρόνου (real-time services) μέσω packet switched σύνδεσης μπορεί να εξελιχθεί σε σχετικά δύσκολη. Άλλη μία εναλλακτική πρόταση όσον αφορά ειδικότερα το VoIP είναι το πρωτόκολλο Session Initiation Protocol (SIP), το οποίο αποτελεί ένα "Internet world counterpart" για το H.323, που στοχεύει στην διεκπεραίωση των ίδιων εργασιών με την περίπτωση του H.323 με τη διαφορά να εντοπίζεται στο ότι είναι implemented έχοντας ως βάση ένα IP. Το προτέρημα του SIP σε σύγκριση με το H.323 είναι ότι είναι πιο απλό, καθώς η πραγματοποίηση της σύνδεσης δεν απαιτεί τόσα πολλά μηνύματα άρα απαιτεί λιγότερο χρόνο. Το SIP συμπεριλαμβάνεται στο IMS αλλά οι προδιαγραφές 3GPP που αναφέρονται σε αυτό παραμένουν επεξεργάσιμες.

Η εικόνα 82 παρουσιάζει ένα απλοποιημένο δείγμα του τρόπου με τον οποίο το MGW χειρίζεται το SIP και το ISUP στα πλαίσια του VoIP. Η VoIP session ξεκινάει με μήνυμα INVITE (πρόσκλησης) ως ανταπόκριση στο ISUP Initial Address Message (IAM). Το ISUP Address Complete Message (ACM) εκλαμβάνεται ως μία θετική επιβεβαίωση στην πλευρά του SIP κ.ο.κ. Η βασική ιδέα είναι ότι κάθε μήνυμα SIP έχει ένα αντίστοιχο τμήμα (counterpart) στην πλευρά του ISUP και το αντίθετο. Αν το H.323 χρησιμοποιείται υπό παρόμοια μέθοδο, μπορεί από την πλευρά του να χρησιμοποιήσει δεκάδες μηνύματα για τη δημιουργία ενός μηνύματος ISUP προς το άλλο δίκτυο. Αυτό το είδος χρονικής καθυστέρησης θα μπορούσε να αποβεί μοιραίο σε ορισμένες περιπτώσεις.

Ως συμπέρασμα, το SIP αποτελεί καλύτερη εναλλακτική συγκριτικά με το VoIP και για περισσότερες multimedia sessions. Από την άλλη πλευρά, το H.323 (επειδή αποτελεί παλαιότερο standard) τυγχάνει καλύτερης υποστήριξης (product support) και διαθεσιμότητας τερματικών (terminal availability).

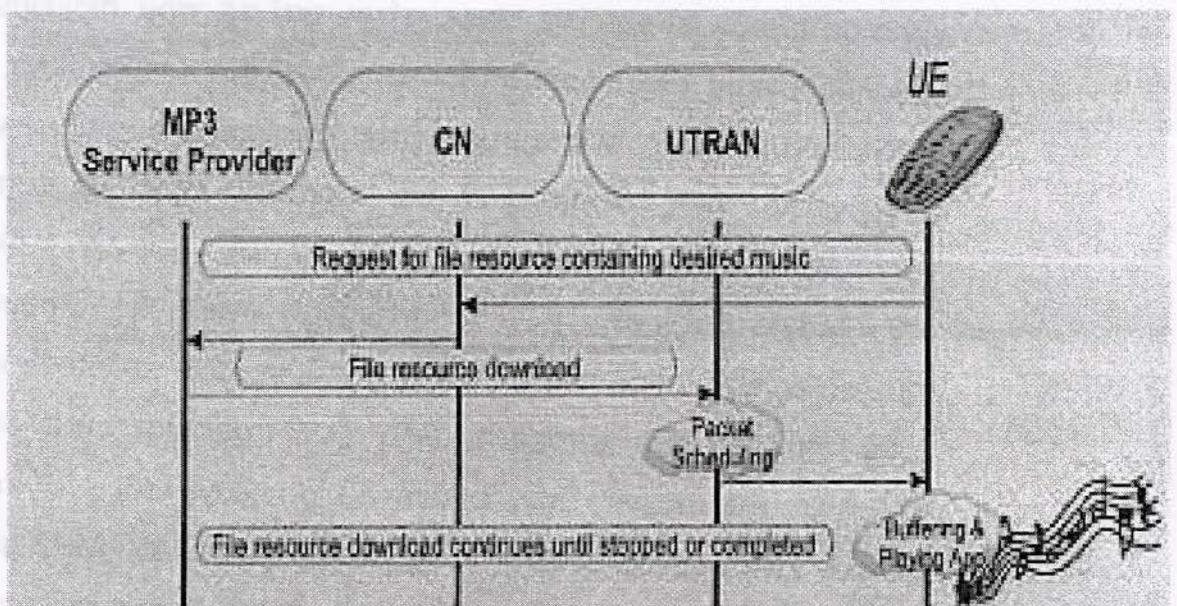


Εικόνα 82 Η συνομιλία σηματοδοσίας με παράδειγμα το SIP και ISUP

7.4.2. Services and Streaming QoS class

Αν μία υπηρεσία χρησιμοποιεί conversational QoS class δεν αναλαμβάνει τη μεταφορά αρχείων. Η πρώτη QoS class που διαχειρίζεται τη μεταφορά δεδομένων διαμέσου της σύνδεσης είναι η streaming class. Από τη στιγμή που η ολοκλήρωση του (file) download αρχείων απαιτεί χρόνο οπότε και επιφέρει χρονική καθυστέρηση, είναι απαραίτητη η ύπαρξη μηχανισμών για το άνοιγμα και τη διαχείριση των αρχείων όταν δεν έχουν μεταφερθεί πλήρως από την πηγή στον προορισμό τους. Αυτόν τον τομέα καλύπτει η QoS class. Οι τυπικές υπηρεσίες ή εφαρμογές που χρησιμοποιούν streaming class, είναι εκείνες που διαχειρίζονται αρχεία μεγάλου όγκου αλλά μακροπρόθεσμα παίζουν μικρό ρόλο σε αυτήν την διαδικασία. Επίσης, οι υπηρεσίες που προσφέρουν multicast (ταυτόχρονη συνεργασία ενός αποστολέα και πολλών ληπτών) τύπο υπηρεσίας χρησιμοποιούν streaming class αν δεν υπάρχει χρονική καθυστέρηση. Για την ελαχιστοποίηση των επιπτώσεων πιθανής καθυστέρησης, οι υπηρεσίες streaming class είναι κατά κύριο λόγο unidirectional. Η χρονική καθυστέρηση είναι υπαρκτή αλλά δεν προκαλεί επιπλοκές λόγω της απουσίας interactivity. Στην εικόνα 83 απεικονίζεται ένα παράδειγμα του τρόπου επίτευξης ακρόασης ενός μουσικού αρχείου MP3 μέσω streaming QoS class. Η εντός UE εφαρμογή στέλνει στο δίκτυο το αίτημα του χρήστη

που αφορά ένα συγκεκριμένο αρχείο MP3 κι έπειτα το αίτημα καταλήγει στον επιθυμητό service provider. Ως επιβεβαίωση, ο παροχέας υπηρεσιών ξεκινάει το download του επιθυμητού αρχείου MP3. Κατά τη χρήση streaming QoS class ολόκληρο το MP3 αρχείο δεν είναι απαραίτητο να χρησιμοποιηθεί το UE την ίδια χρονική στιγμή. Το βασικό σημείο σε αυτήν την περίπτωση, είναι ότι τα packet format data καταφτάνουν στο UE με ικανοποιητικό ρυθμό και με σωστή σειρά. Το data stream γίνεται buffered σε δύο μέρη για δύο διαφορετικούς λόγους: στο UTRAN τα δεδομένα γίνονται buffered με σκοπό τον έλεγχο της πρόσβασης στο radio interface και της φόρτωσής (load) του, και στο UE η εφαρμογή streaming class κατασκευάζει buffers από το data stream έτσι ώστε να παρουσιάσει τα δεδομένα στον χρήστη σε μορφή “real-time-like”, δηλαδή συνεχόμενα χωρίς εμπλοκές και διακοπές. Όταν η εφαρμογή στο UE έχει κάνει buffer σε αρκετά δεδομένα έτσι ώστε να ξεκινήσει playback, τα δεδομένα παρουσιάζονται/παίζονται στον χρήστη μέσω της επιλεγμένης εφαρμογής. Παράλληλα, η εφαρμογή streaming class συνεχίζει το download δεδομένων από τον παροχέα υπηρεσιών. Το data download συνεχίζεται μέχρι την ολοκλήρωση/πλήρωση του αρχείου ή μέχρι να διακόψει τη διαδικασία ο χρήστης.



Εικόνα 83 παράδειγμα για τη χρήση της πηγής MP3

Οι υπηρεσίες streaming class θα μπορούσαν να εφαρμοστούν με το H.323 protocol stack, αλλά η εφαρμογή τους θα ήταν περίπλοκη. Από την άλλη πλευρά, οι υπηρεσίες streaming class έχουν εξελιχθεί πολύ στο περιβάλλον του Internet. Το Internet προσφέρει πολύ περιορισμένο bandwidth στους κοινούς χρήστες γεγονός που έχει οδηγήσει στην ανάπτυξη διαφορετικών τεχνικών streaming για εξαλείψουν αυτό το περιορισμό. Οι τεχνικές streaming που χρησιμοποιούνται σε περιβάλλον Internet έχουν ως βάση τη νοοτροπία του “client-server”. Ο τελικός χρήστης χρησιμοποιεί μία εφαρμογή για τη διαχείριση της streaming bit flow, έτσι ώστε να μπορεί να την αποθηκεύσει και να τη διαχειριστεί όταν χρειαστεί. Η “client-server” πλευρά αυτού του είδους streaming εμφανίζεται όταν ο χρήστης επιθυμεί να βλέπει/ακούει/διαχειρίζεται το bit stream, οπότε η εφαρμογή ξεκινάει το data buffering και ανοίγει το interface στον τελικό χρήστη. Με άλλα λόγια, στο Internet-type-of-streaming, το streaming γίνεται στην πραγματικότητα από την εφαρμογή που είναι εγκατεστημένη στο τερματικό του χρήστη, ενώ στην περίπτωση του H.323 based streaming το streaming γίνεται εντός του δικτύου και ο τελικός χρήστης αναλαμβάνει τη διαχείριση της streaming bit flow μόνο μέσω του interface με έναν προκαθορισμένο τρόπο.

Και οι δύο αυτοί τύποι θα χρησιμοποιούνται επειδή διαφορετικές υπηρεσίες που χρησιμοποιούν streaming QoS class θέτουν τις δικές τους απαιτήσεις. Από την άλλη πλευρά, ο στόχος είναι η βελτίωση (utilize) του Internet-type-of-streaming καθώς καθιστά την δικτυακή implementation απλούστερη οπότε και λιγότερο δαπανηρή.

7.4.3. Services and Interactive/Background Class

Η interactive class μπορεί να υποστεί θεαματικές και ποικίλες καθυστερήσεις. Οι υπηρεσίες που utilize αυτήν την QoS class είναι κατά κύριο λόγο request-response-type υπηρεσιών όπως είναι το web surfing

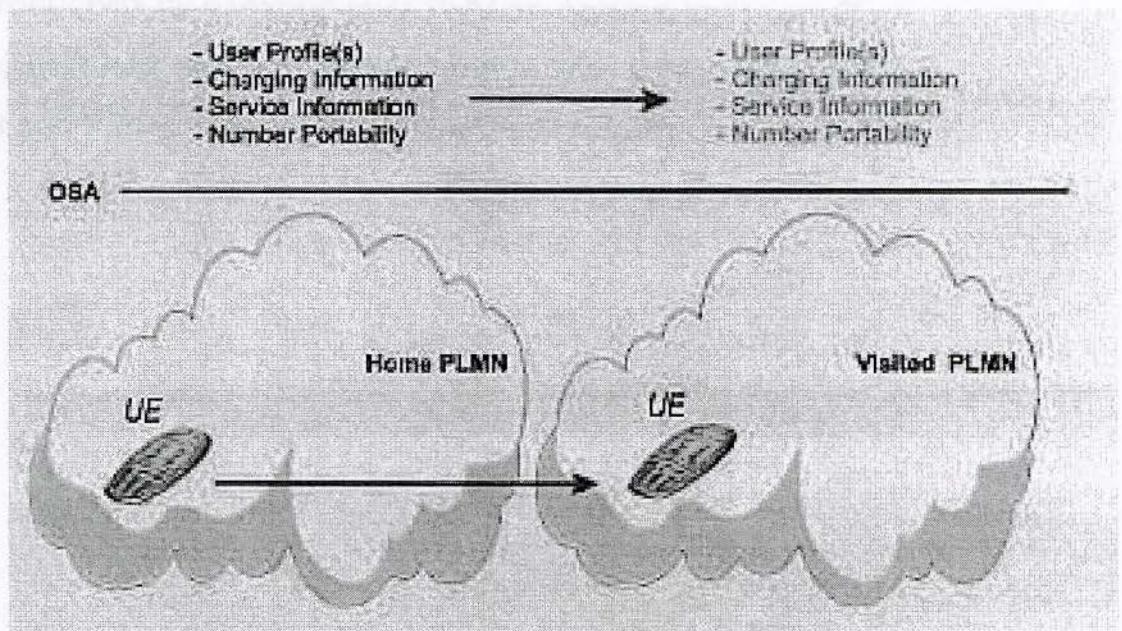
(αίτημα (request): η URL διεύθυνση μίας επιθυμητής web page, ανταπόκριση (response): τα περιεχόμενα αυτής της σελίδας), οι υπηρεσίες WAP (ακολουθείται η παραπάνω λογική) και άλλες υπηρεσίες που προϋποθέτουν άνοιγμα server connections. Ένα νέο σύνολο υπηρεσιών που καλούνται location based services utilize αυτήν την QoS class. Οι μηχανισμοί αυτών των υπηρεσιών προϋποθέτουν αισθητή συμμετοχή του δικτύου UMTS.

Η background QoS class παρέχει το βασικό connectivity level, όπου η καθυστέρηση και το Bit Error Rate (BER) είναι σε πρακτικό επίπεδο ασήμαντα αν το δίκτυο διαθέτει λειτουργία διόρθωσης σφαλμάτων (error correction functionality). Οι υπηρεσίες που utilize αυτήν την QoS class αποτελούν διάφορες διαδικασίες που συμπεριλαμβάνουν file downloads. Για παράδειγμα, η λήψη e-mail αποτελεί μία από αυτές.

7.4.4 Service Concept: Virtual Home Environment (VHE)

Με μια πρώτη ματιά, η σύλληψη του VHE φαίνεται απλή: ο χρήστης πρέπει πάντα να διατηρεί το ίδιο, προσωπικά διαμορφωμένο, ξεχωριστό interface στο τερματικό του, ανεξάρτητα από το δίκτυο στο οποίο βρίσκεται.

Στην εικόνα 84 απεικονίζεται την ιεραρχία στο VHE. Αν και αυτή η υπηρεσία είναι πολύ απλή όταν εξετάζεται από την πλευρά του συνδρομητή, θέτει υψηλές απαιτήσεις στα αναμειγνυόμενα δίκτυα.



Εικόνα 84 Οι αρχές του VHE

Κατά κύριο λόγο, το VHE ασχολείται με τα προφίλ του συνδρομητή, τις πληροφορίες charging, τις πληροφορίες των υπηρεσιών και πληροφορίες numbering για έναν συγκεκριμένο συνδρομητή, είτε αυτές μεταφέρονται, είτε είναι διαθέσιμες μεταξύ των δικτύων. Τα προηγούμενα αποτελούν πολύπλοκα θέματα κατά τη διαχείρισή τους μεταξύ δικτύων. Ο κοινός παρανομαστής και το βασικό κλειδί για τη διεκπεραίωση του θέματος αυτού είναι το CAMEL και το VHE προϋποθέτει την παρουσία του σε κάθε δίκτυο UMTS που φέρει VHE. Οι δυνατότητες των υπηρεσιών είναι προσβάσιμες μέσω του CAMEL. Έτσι:

- Τα προφίλ των συνδρομητών (subscriber profiles) διαχειρίζονται στο MSE
- Οι πληροφορίες υπηρεσιών που έχουν ως βάση την θέση (location based services information) μπορούν να μεταφερθούν μεταξύ των δικτύων διαμέσου του CAMEL
- Άλλες πληροφορίες υπηρεσιών (provisioned services και πληροφορίες χρήσης/χρησιμότητάς τους) μεταφέρονται μεταξύ των δικτύων διαμέσου του CAMEL
- Είναι εφικτή η number portability διαμέσου CAMEL

Όπως είναι φανερό, το VHE είναι δύσκολο να εφαρμοστεί και από τα παραπάνω σημεία η τελευταία αναφορά (number portability) είναι ίσως η πιο δύσκολη περίπτωση λόγω των διαφορετικών numbering schemes που χρησιμοποιούνται ανά τον κόσμο.



Εικόνα 84 Οι αρχές του VHE

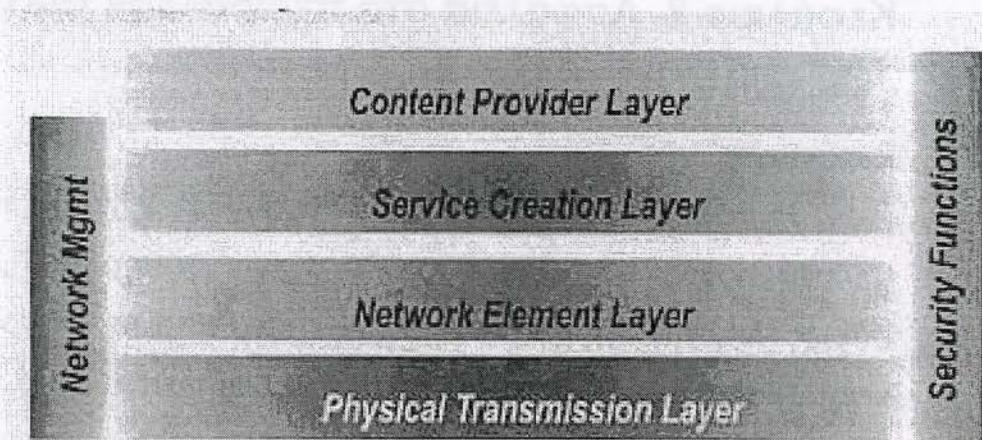
Κεφάλαιο 8 Ασφάλεια στο περιβάλλον UMTS

Εισαγωγή

Η ασφάλεια ήταν πάντα άμεσα συνδεδεμένη με τα φορητά δίκτυα (mobile networks) λόγω της φύσης των ασύρματων επικοινωνιών, οι οποίες είναι εύκολα προσβάσιμες όχι μόνο από τους υποψήφιους χρήστες κινητών τηλεφώνων αλλά και από οποιονδήποτε πιθανό υπόκλοπέα. Παρ' όλ' αυτά, η ασφάλεια αποτελεί ένα πολύ ευρύτερο θέμα, οι τομείς του οποίου πρέπει να ληφθούν υπόψη από όλους τους σχετιζόμενους (players) στον τομέα της κινητής επικοινωνίας. Θα εξετάσουμε τόσο την πλευρά των παροχών υπηρεσιών (carrier/service providers) όσο και την πλευρά των τελικών χρηστών (end users). Επίσης, θα εξετάσουμε τη νομική παρέμβαση (lawful interception), η οποία αποτελεί πτυχή των φορητών μέσων επικοινωνίας, ως μέρος της σύγχρονης κοινωνίας.

Τα αναλογικά κινητά δίκτυα πρώτης γενιάς (first generation -1G-mobile networks) δεν διέθεταν πολλές δυνατότητες σχετικά με την ασφάλεια, και εκείνο τον καιρό οι συνδρομητές δεν είχαν κατανοήσει τη σημασία των ασφαλών συνδέσεων (secure connections). Απ' την άλλη πλευρά, ο ραδιοφωνικός δίαυλος (radio path) (ο οποίος μεταξύ άλλων υστερεί στον τομέα της ασφάλειας αποτελεί το πιο απροστάτευτο μέρος του συστήματος) μπορεί να ασφαλιστεί πολύ αποτελεσματικά, αλλά αυτή η διεργασία έχει τόσο πλεονεκτήματα όσο και μειονεκτήματα. Αν η ασύρματη σύνδεση (radio connection) είναι τύπου point-to-point (μεταξύ δύο χρηστών), μπορεί να χρησιμοποιηθεί μία αποκλειστική ρύθμιση ασφάλειας. Με αυτόν τον τρόπο επιτυγχάνονται οι ασφαλείς στρατιωτικές radio connections. Στα δημόσια κυψελοειδή δίκτυα (public cellular networks) το radio path είναι πάντα point-to-multipoint, δηλαδή το ίδιο σήμα εκπομπής καταφτάνει σε πολλά τερματικά κι ως επόμενο

οποιοδήποτε αποκλειστικό σύστημα ασφάλειας στο radio path δεν χρησιμοποιείται υπό αυτήν τη μορφή



Εικόνα 85 Η ασφάλεια και ο ρόλος της στη 3G

Στο βασικό GSM, ο τομέας της ασφάλειας επικεντρώνεται στην ασφάλεια του ραδιοφωνικού διαύλου (radio path), δηλαδή τον τομέα των δικτύων πρόσβασης. Στα δίκτυα UMTS η ασφάλεια αποτελεί ευρύτερο θέμα. Η σύνδεση δικτύου πρόσβασης (access network connection) πρέπει να ασφαλιστεί και επιπρόσθετα να ληφθούν υπόψη πολλές άλλες πτυχές. Η αλυσίδα του διαφημιστικού μοντέλου που θα δούμε παρακάτω, οδηγεί στην κατάσταση όπου μερικές φορές, ορισμένες πολύ ευαίσθητες πληροφορίες μεταφέρονται μεταξύ διαφορετικών ομάδων και δικτύων (parties and networks). Από την πλευρά της ασφάλειας αυτό μπορεί να ερμηνευτεί ως σοβαρό ρίσκο ασφάλειας. Επίσης, διεθνείς και τοπικές αρχές θέτουν τις προτεραιότητες τους όσον αφορά αυτό το τομέα. Το UMTS συνεχίζει να συνδιάζει την τηλεπικοινωνία (telecommunication) και την επικοινωνία δεδομένων (data communication), γεγονός που δημιουργεί απειλή για τον τομέα της ασφάλειας. Στον κόσμο του IP, η ασφάλεια υπήρξε ένα θέμα για πολλά χρόνια, καθώς έχουν εντοπιστεί ποικίλες απειλές ασφάλειας και έχουν αναπτυχθεί πολλοί αμυντικοί μηχανισμοί.

8.1. Ασφάλεια πρόσβασης στο UMTS

Η τεχνολογία ασύρματης πρόσβασης (radio access technology) θα αλλάξει από TDMA σε WCDMA με την θεμελίωση των κινητών δικτύων τρίτης γενιάς (3G). Παρά την αλλαγή αυτή, οι απαιτήσεις για την ασφάλεια πρόσβασης (access security) δε θα αλλάξουν. Στο UMTS παραμένει απαραίτητη η πιστοποίηση ταυτότητας (authentication) των τελικών χρηστών (end users), δηλαδή η ταυτότητα (identity) κάθε συνδρομητή ελέγχεται – έτσι αποτρέπεται η χρέωση κλήσεων που προέρχονται από ψευδείς χρήστες.

Στο δίκτυο ραδιοφωνικής/ασύρματης πρόσβασης (radio access network) προστατεύεται η εμπιστευτικότητα (confidentiality) των φωνητικών κλήσεων (voice calls) όπως επίσης και εκείνη των δεδομένων χρήστη που μεταδίδονται. Αυτό σημαίνει ότι ο χρήστης έχει έλεγχο όσον αφορά την επιλογή των συνόλων (parties) με τις οποίες επιθυμεί να επικοινωνήσει. Οι χρήστες θέλουν επίσης να ξέρουν ότι η προστασία εμπιστευτικότητας (confidentiality protection) που πραγματικά εφαρμόζεται: η διαφάνεια (visibility) των εφαρμοσμένων μηχανισμών ασφάλειας είναι απαραίτητη. Η προσωπική απόκρυψη (privacy) των δραστηριοτήτων του χρήστη εκτιμάται. Στις περισσότερες περιπτώσεις, ο μέσος πολίτης δεν ενδιαφέρεται αν κάποιος μπορεί να εντοπίσει τη θέση του. Όμως, σε περίπτωση που ο εντοπισμός (tracking) είναι επίμονος, ο χρήστης ίσως ενοχληθεί. Σε σχέση με αυτό, συγκεκριμένες πληροφορίες σχετικά με τη θέση/στοιχεία των χρηστών μπορεί να φανούν χρήσιμες π.χ. για επίδοξους διαρρήκτες. Επίσης, η προσωπική απόκρυψη (privacy) των δεδομένων του χρήστη αποτελεί κρίσιμο θέμα όταν τα δεδομένα μεταφέρονται μέσα στο δίκτυο. Η προσωπική απόκρυψη και η εχεμύθεια (privacy and confidentiality) είναι όροι σχεδόν συνώνυμοι σε αυτήν την παρουσίαση.

Η διαθεσιμότητα της πρόσβασης στο UMTS είναι πολύ σημαντική για τον συνδρομητή που πληρώνει για τον σκοπό αυτό. Οι διαχειριστές

δικτύου (network operators) θεωρούν σημαντική την σταθερότητα (reliability) της λειτουργικότητας του δικτύου: θέλουν να διατηρούν τον έλεγχο εντός του δικτύου για την αποτελεσματική λειτουργία του. Αυτό επιτυγχάνεται μέσω της ακεραιότητας όλων των εκπομπών σήματος των ασύρματων (radio network signaling). Γίνεται έλεγχος για το αν όλα τα μηνύματα ελέγχου (control messages) έχουν δημιουργηθεί από εγκεκριμένα στοιχεία (authorized elements) του δικτύου. Σε γενικές γραμμές, ο έλεγχος ακεραιότητας (integrity checking) προστατεύει τα μηνύματα από μεταβολές (manipulation) όπως είναι π.χ. η εισαγωγή, διαγραφή ή αλλαγή (insertion, deletion or substitution).

Το πιο σημαντικό χαρακτηριστικό κατά την παροχή ασφάλειας στους διαχειριστές δικτύου (network operators) και τους συνδρομητές, είναι η κρυπτογραφία, η οποία απαρτίζεται από ποικίλες τεχνικές που έχουν τις ρίζες τους στην επιστήμη και την τέχνη της μυστικής γραφής (secret writing). Μερικές φορές είναι χρήσιμη η εκ προθέσεως δυσνόητη επικοινωνία, δηλαδή η επικοινωνία μέσω κρυπτογράφησης. Αυτή είναι η πιο αποτελεσματική μέθοδος προστασίας της επικοινωνίας ενάντια σε κακοήθεις σκοπιμότητες.

8.1.1. Legacy from 2G

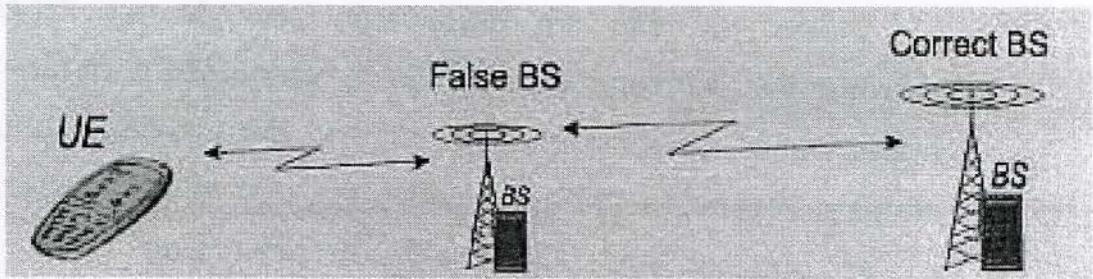
Η μεταπήδηση από τα αναλογικά συστήματα πρώτης γενιάς (1G) στα ψηφιακά συστήματα δεύτερης γενιάς (2Generation systems), έκανε δυνατή την ανάπτυξη εξελιγμένων κρυπτογραφικών μεθόδων. Τα πιο σημαντικά χαρακτηριστικά/λειτουργίες ασφάλειας στο σύστημα GSM είναι:

- Η εξακρίβωση των στοιχείων του χρήστη (authentication of the user)
- Κρυπτογράφηση της επικοινωνίας στο ασύρματο interface (encryption of communication in the radio interface)
- Χρήση προσωρινών διακριτικών χαρακτηριστικών (use of temporary identities)

Κατά την όλο και μεγαλύτερη επιτυχία του GSM και άλλων συστημάτων δεύτερης γενιάς (2G), η χρησιμότητα αυτών των βασικών παραμέτρων ασφάλειας έγινε επίσης θεμελιώδους σημασίας. Ήταν επόμενο λοιπόν, το UMTS να υιοθετήσει αυτά τα χαρακτηριστικά (features) στο νέο σύστημα όσον αφορά τα θέματα ασφάλειας.

Η επιτυχία του GSM οδήγησε στη συνειδητοποίηση των περιορισμών της ασφάλειάς του. Μία δημοφιλής τεχνολογία είναι δελεαστική για τους απατεώνες (fraudsters). Οι ιδιότητες (properties) του GSM που δέχτηκαν την περισσότερη κριτική από πλευράς ασφάλειας, είναι οι ακόλουθες:

- Οι ενεργές επιθέσεις κατά του δικτύου είναι εφικτές: αυτό έχει να κάνει με κάποιον που διαθέτει τον απαιτούμενο εξοπλισμό έτσι ώστε να παρουσιαστεί ως γνήσιο στοιχείο του δικτύου (legitimate network element) ή χρήστης τερματικού 86.
- Σχολαστικός έλεγχος δεδομένων, π.χ. κλειδιά (keys) που χρησιμοποιούνται κατά την κρυπτογράφηση radio interface, αποστέλλονται μεταξύ διαφορετικών δικτύων χωρίς κρυπτογράφηση (ciphering).
- Μερικά μέρη της αρχιτεκτονικής ασφάλειας παραμένουν κρυφά, π.χ. κρυπτογραφικοί αλγόριθμοι: σε τελική ανάλυση δεν είναι άξιοι εμπιστοσύνης καθώς δεν είναι ευρέως διαθέσιμοι για ανάλυση και απ' την άλλη πλευρά, ευρύτερα μυστικά έχουν την τάση να αποκαλύπτονται αργά ή γρήγορα.
- Τα κλειδιά (keys) που χρησιμοποιούνται για την κρυπτογράφηση του radio interface γίνονται μακροπρόθεσμα επιρρεπή σε επιθέσεις κατά τις οποίες ως απώτερος σκοπός είναι ο εντοπισμός του κατάλληλου κλειδιού.



Εικόνα 86 Ενεργή επίθεση

Αυτοί οι περιορισμοί παρέμειναν σκόπιμα στο σύστημα GSM. Η απειλή που δημιουργήθηκε εξαιτίας τους εκτιμήθηκε ως μηδαμινή (inferior) σε σύγκριση με το επιπρόσθετο κόστος που θα προέκυπτε από την προσπάθεια απαλοιφής της. Παρ' όλ' αυτά, με την εξέλιξη της τεχνολογίας, οι επιτιθέμενοι έχουν πρόσβαση σε αποτελεσματικότερα εργαλεία. Γι' αυτόν τον λόγο, το αποτέλεσμα της σύγκρισης μεταξύ κόστους και ασφάλειας οδήγησε σε διαφορετικό συμπέρασμα στην περίπτωση της 3G.

Στο UMTS, τα αντίμετρα για τις αδυναμίες στο GSM έχουν εξελιχθεί. Αυτή είναι άλλη μία σημαντική αρχή που οδήγησε στο σχεδιασμό της αρχιτεκτονικής ασφάλειας τρίτης γενιάς (3G). Τα πιο σημαντικά χαρακτηριστικά ασφάλειας σχετικά με την ασφάλεια πρόσβασης του UMTS είναι τα ακόλουθα:

- Αμοιβαία εξακρίβωση ταυτότητας του χρήστη και του δικτύου (mutual authentication of the user and the network)
- Χρήση προσωρινών ταυτοτήτων (use of temporary identities)
- Κρυπτογράφηση ασύρματης πρόσβασης δικτύου (radio access network encryption)
- Προστασία της ακεραιότητας εκπομπής σημάτων εντός UTRAN (protection of signaling inside UTRAN).

Αυτοί οι περιορισμοί αφέθηκαν στο σύστημα GSM. Η απειλή που επιβλήθηκε υπολογίστηκε κατώτερη σε σύγκριση με το προστιθέμενο κόστος να τους παρακάμψει. Εντούτοις, καθώς η τεχνολογία προωθεί, οι επιτιθέμενοι αποκτούν πρόσβαση στα καλύτερα εργαλεία. Γι' αυτό η

έκβαση μιας παρόμοιας σύγκρισης μεταξύ του κόστους και της ασφάλειας οδήγησε σε ένα διαφορετικό συμπέρασμα στη 3G περίπτωση.

8.1.2. Αμοιβαία εξακρίβωση

Υπάρχουν τρεις οντότητες που συμπεριλαμβάνονται στον μηχανισμό εξακρίβωσης του συστήματος UMTS:

- Οικιακό δίκτυο (home network)
- Δίκτυο υπηρεσιών (serving network – SN)
- Τερματικό, πιο συγκεκριμένα USIM (smart card)

Η βασική ιδέα είναι ότι το SN ελέγχει την ταυτότητα του συνδρομητή (όπως στο GSM) με μία τεχνική πρόκλησης-ανταπόκρισης (challenge-and-response technique) ενώ το τερματικό ελέγχει αν το Serving Network έχει εγκριθεί γι' αυτό από το home network. Το τελευταίο σκέλος είναι μία νέα λειτουργία στο UMTS (σε σύγκριση με το GSM) και μέσω αυτής, το τερματικό μπορεί να ελέγξει εάν είναι συνδεδεμένο με ένα έγκυρο δίκτυο.

Το πρωτόκολλο αμοιβαίας εξακρίβωσης ταυτότητας από μόνο του δεν αποτρέπει το σενάριο του σχήματος 86, αλλά (σε συνδιασμό με άλλους μηχανισμούς ασφάλειας) εγγυάται ότι ο επιτιθέμενος δεν μπορεί να επωφεληθεί πραγματικά από αυτήν την κατάσταση. Το μόνο πιθανό όφελος για τον επιτιθέμενο είναι ότι βρίσκεται σε θέση να παρενοχλήσει τη σύνδεση, τη στιγμή που δεν υπάρχουν μέθοδοι πρωτοκόλλου ικανές να αποτρέψουν ολοκληρωτικά αυτόν τον τύπο επίθεσης. Για παράδειγμα, ένας επιτιθέμενος μπορεί να χρησιμοποιήσει τη μέθοδο της ραδιοφωνικής παρεμβολής (radio jamming).

Ο ακρογωνιαίος λίθος του μηχανισμού πιστοποίησης ταυτότητας είναι το πρωταρχικό κλειδί -K- (master key) που μοιράζεται μεταξύ του USIM του χρήστη και της βάσης δεδομένων του οικιακού δικτύου (home network database). Αυτό, είναι μονίμως κρυφό με μέγεθος 128 χαρακτήρων/bits. Το κλειδί -K- δε μεταφέρεται ποτέ έξω απ' τα

προαναφερθέντα. Για παράδειγμα, ο χρήστης δεν έχει γνώση για το master key του.

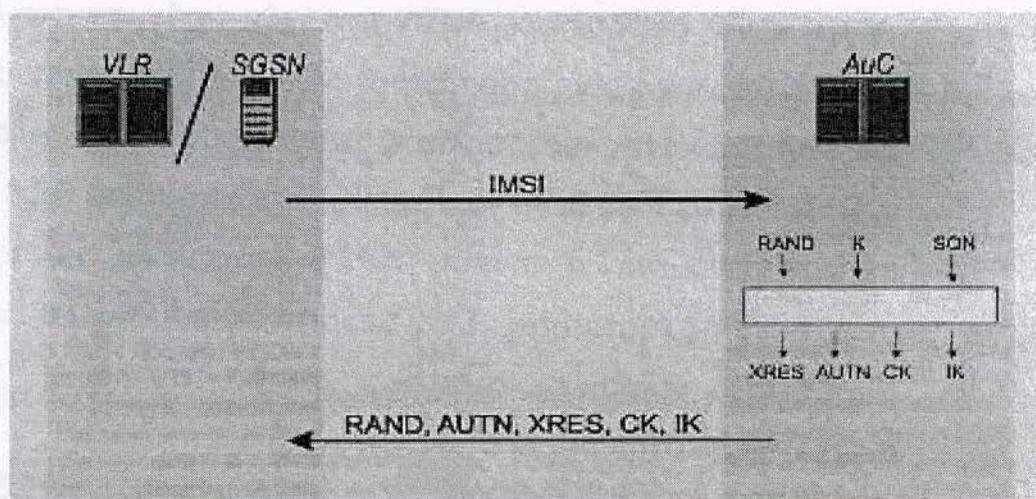
Παράλληλα με την αμοιβαία πιστοποίηση ταυτότητας, παρέχονται κλειδιά κρυπτογράφησης και ελέγχου ακεραιότητας, τα οποία είναι προσωρινά και μεγέθους 128 bits. Από το μόνιμο κλειδί -K- αποσπώνται νέα κλειδιά κατά τη διάρκεια κάθε διεργασίας εξακρίβωσης ταυτότητας (authentication event). Ο περιορισμός στο ελάχιστο της χρήσης ενός μόνιμου κλειδιού, αποτελεί βασική αρχή στην κρυπτογραφία, όπως είναι η δημιουργία προσωρινών κλειδιών για την προστασία των δεδομένων η ανάλυση υπηρεσιών με τις νέες μεθόδους και, αφ' ετέρου, τα σφαιρικά μυστικά τείνουν να αποκαλυφθούν πιο σύντομα ή τα πιο πρόσφατα πλήκτρα που χρησιμοποιούνται για το ραδιο λογαριασμό διαπροσωπειών γίνονται τελικά τρωτά στις ογκώδεις ζωώδεις επιθέσεις δύναμης όπου κάποιος δοκιμάζει όλα τα πιθανά πλήκτρα έως ότου ταιριάζει με κάποια.

Ο ακρογωνιαίος λίθος του μηχανισμού πιστοποίησης ταυτότητας είναι ένα κύριο βασικό **K** που μοιράζεται μεταξύ του USIM του χρήστη και της βάσης δεδομένων βασικών δικτύων. Αυτό είναι ένα μόνιμο μυστικό με ένα μήκος 128 bits. Το βασικό **K** δεν μεταφέρεται ποτέ έξω από τις δύο θέσεις. Παραδείγματος χάριν, ο χρήστης δεν έχει καμία γνώση του κύριου πλήκτρου της/του.

Συγχρόνως με την αμοιβαία πιστοποίηση ταυτότητας, τα πλήκτρα για την κρυπτογράφηση και τον έλεγχο ακεραιότητας παράγονται. Αυτά είναι προσωρινά πλήκτρα με το ίδιο μήκος 128 bits. Τα νέα πλήκτρα παράγονται από το μόνιμο βασικό **K** κατά τη διάρκεια κάθε γεγονότος πιστοποίησης ταυτότητας. Είναι η βασική αρχή στο σύστημα κρυπτογραφία για να περιορίσει τη χρήση ενός μόνιμου πλήκτρου στο ελάχιστο και να παραγάγει αντ' αυτού τα προσωρινά πλήκτρα για την προστασία των μαζικών στοιχείων. Περιγράφουμε τώρα την πιστοποίηση ταυτότητας και το βασικό μηχανισμό συμφωνίας (AKA) σε ένα γενικό επίπεδο. Τη διαδικασία πιστοποίησης ταυτότητας μπορεί να αρχίσουν

αφότου προσδιορίζεται ο χρήστης στο εξυπηρετώντας δίκτυο. Ο προσδιορισμός εμφανίζεται όταν διαβιβαστεί η ταυτότητα του χρήστη, δηλ. μόνιμη ταυτότητα IMSI ή προσωρινή ταυτότητα TMSI, σε VLR ή SGSN. Κατόπιν VLR ή SGSN στέλνει ένα αίτημα στοιχείων πιστοποίησης ταυτότητας στο κέντρο πιστοποίησης ταυτότητας (AuC) στο βασικό δίκτυο.

Το AuC περιέχει τα κύρια πλήκτρα των χρηστών και βασισμένος στη γνώση IMSI που το AuC είναι σε θέση να παραγάγει τα διανύσματα πιστοποίησης ταυτότητας για το χρήστη. Η διαδικασία παραγωγής περιέχει τις εκτελέσεις διάφορων κρυπτογραφικών αλγορίθμων, οι οποίοι περιγράφονται αργότερα λεπτομερέστερα. Τα παραγμένα διανύσματα στέλνονται πίσω σε VLR/SGSN στην απάντηση στοιχείων πιστοποίησης ταυτότητας. Αυτή η διαδικασία απεικονίζεται στην εικόνα 87. Αυτά τα μηνύματα λέγχου μεταφέρονται στο πρωτόκολλο MAP.



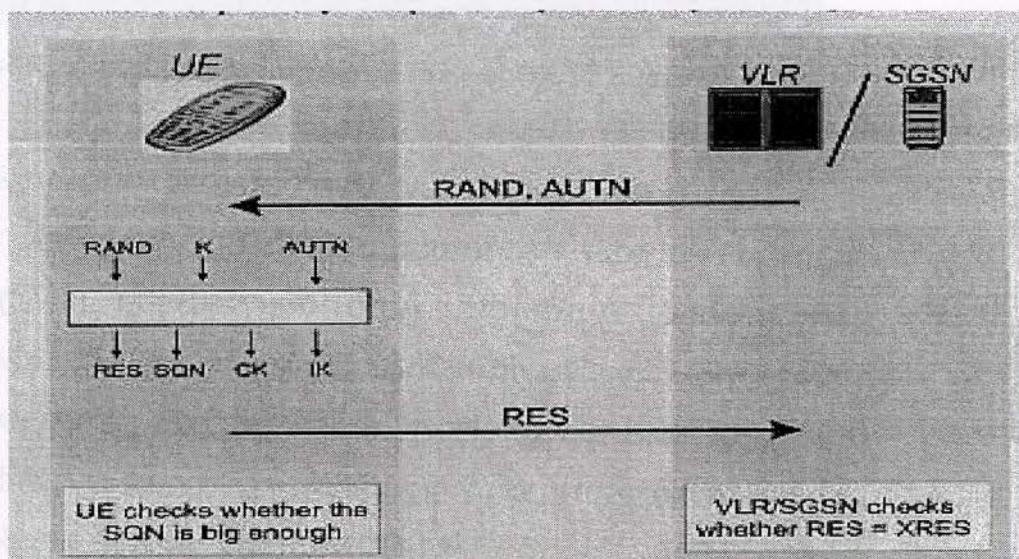
Εικόνα 87 Αίτηση και απάντηση εξακρίβωσης δεδομένων

Στο δίκτυο υπηρεσιών, ένα στοιχείο πιστοποίησης ταυτότητας απαιτείται για κάθε περίπτωση αυθεντικοποίησης δηλ. για κάθε εκτέλεση πιστοποίησης ταυτότητας. Αυτό σημαίνει ότι (ενδεχομένως μεγάλης απόστασης) επικοινωνία μεταξύ SN και το AuC δεν είναι απαραίτητη για κάθε διαδικασία πιστοποίησης ταυτότητας και μπορεί σε γενικές γραμμές να γίνει ανεξάρτητα από τις ενέργειες χρηστών μετά από την αρχική εγγραφή. Πράγματι, το VLR/SGSN μπορεί να προσκομίσει τα νέα στοιχεία

πιστοποίησης ταυτότητας από AuC πολύ πριν από την εξάντληση των καταχωρημένων στοιχείων.

Το δίκτυο (VLR ή SGSN) στέλνει αίτηση πιστοποίησης ταυτότητας χρηστών στο τερματικό. Αυτό το μήνυμα περιέχει δύο παραμέτρους από το στοιχείο πιστοποίησης ταυτότητας, το RAND και AUTN. Αυτές οι παράμετροι μεταφέρονται στο USIM που υπάρχει μέσα σε ένα απροσπέλαστο περιβάλλον, δηλ. στην κάρτα UMTS IC (UICC). Το USIM περιέχει το βασικό κλειδί **K**, και η χρησιμοποίησή του με τις παραμέτρους RAND και AUTN ως καταχωρήσεις, USIM πραγματοποιεί έναν υπολογισμό που παραπέμπει στη δημιουργία στοιχείων πιστοποίησης ταυτότητας στο AuC. Αυτή η διαδικασία περιέχει επίσης την εκτέλεση ποικίλων αλγόριθμων όπως στη περίπτωση του υπολογισμού AuC.

Ως αποτέλεσμα αυτού του υπολογισμού το USIM είναι σε θέση να ελέγξει εάν η παράμετρος AUTN παρήχθη πράγματι στο AuC και αν αυτό ισχυεί η υπολογισμένη παράμετρος RES στέλνεται πίσω σε VLR/SGSN με την ανταπόκριση πιστοποίησης ταυτότητας των χρηστών. Τώρα το VLR/SGSN είναι σε θέση να συγκρίνει την απάντηση RES των χρηστών με την αναμενόμενη απάντηση XRES που είναι μέρος του στοιχείου πιστοποίησης ταυτότητας. Στην περίπτωση που ταιριάζουν η πιστοποίηση ταυτότητας τελειώνει επιτυχώς. Αυτό το μέρος της διαδικασίας απεικονίζεται στην παρακάτω εικόνα

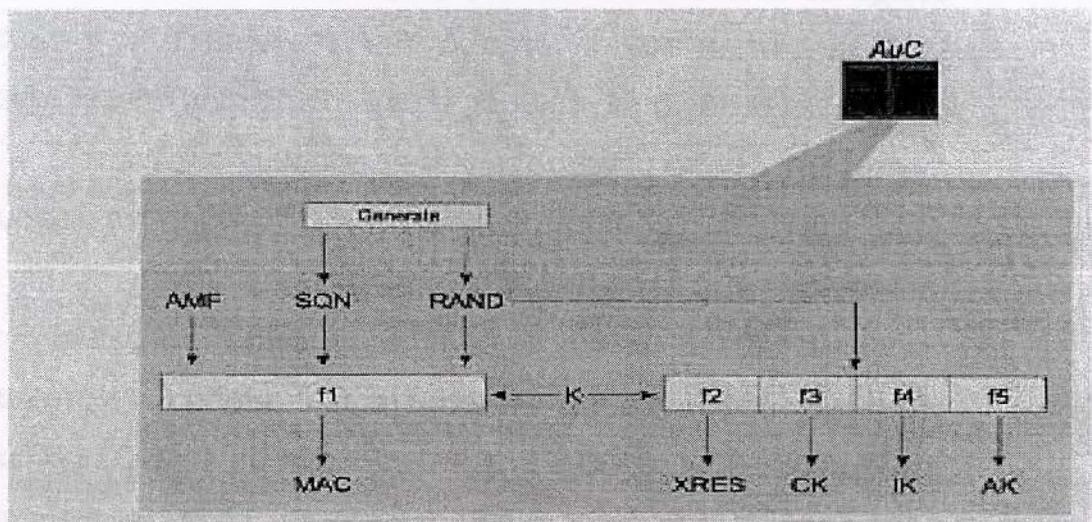


Εικόνα 88 Αίτηση και απάντηση εξακρίβωσης χρήστη

Τα κλειδιά για τη δικτυακή κρυπτογράφηση radio access και την προστασία ακεραιότητας, δηλαδή CK και IK, δημιουργούνται ως υποπροϊόν στη διαδικασία πιστοποίησης ταυτότητας. Αυτά τα προσωρινά κλειδιά συμπεριλαμβάνονται στο στοιχείο πιστοποίησης ταυτότητας και κατά συνέπεια, μεταφέρονται στο VLR/ SGSN. Αυτά τα κλειδιά μεταφέρονται αργότερα στο RNC εντός του radio access network κατά την εκκίνηση κρυπτογράφησης και προστασίας ακεραιότητας. Από την άλλη πλευρά, το USIM είναι σε θέση να υπολογίσει τα CK και IK αφού έχει λάβει το RAND (και αφού το έχει επιβεβαιώσει μέσω του AUTN). Τα προσωρινά κλειδιά μεταφέρονται στη συνέχεια από το USIM στο φορητό εξοπλισμό όπου εφαρμόζονται οι αλγόριθμοι κρυπτογράφησης και προστασίας ακεραιότητας.

8.1.3. Κρυπτογράφηση για την εξακρίβωση

Έπειτα ρίχνουμε μια πιο κοντινή ματιά στην παραγωγή των στοιχείων πιστοποίησης ταυτότητας στο AuC. Μια πιο λεπτομερής απεικόνιση της διαδικασίας δίνεται στη παράκατω εικόνα



Εικόνα 89 Γεννιά του φορέα εξακρίβωσης

Η διαδικασία ξεκινάει από την επιλογή μιας σωστής ακολουθίας αριθμών SQN. Χοντρικά αυτό που απαιτείται είναι η ακολουθία αριθμών, να επιλέγεται από μια αύξουσα κατάταξη. Ο σκοπός του αριθμού ακολουθίας είναι να αποδείξει αργότερα στο χρήστη ότι το στοιχείο πιστοποίησης ταυτότητας είναι νέο, δηλ. δεν έχει ξαναχρησιμοποιηθεί. Παράλληλα με την επιλογή του αριθμού ακολουθίας, δημιουργείται ένα τυχαίο bit string RAND μεγέθους 128bits. Αυτό είναι μια δύσκολη και ταυτόχρονα σημαντική διεργασία αλλά σε αυτή την παρουσίαση υποθέτουμε ότι μια ψευδοτυχαία κρυπτογραφική γεννήτρια είναι σε χρήση, η οποία παράγει μεγάλες ποσότητες απρόβλεπτων δυαδικών ψηφίων όταν είναι διαθέσιμη μια αξιόπιστη τυχαία φυσική πηγή.

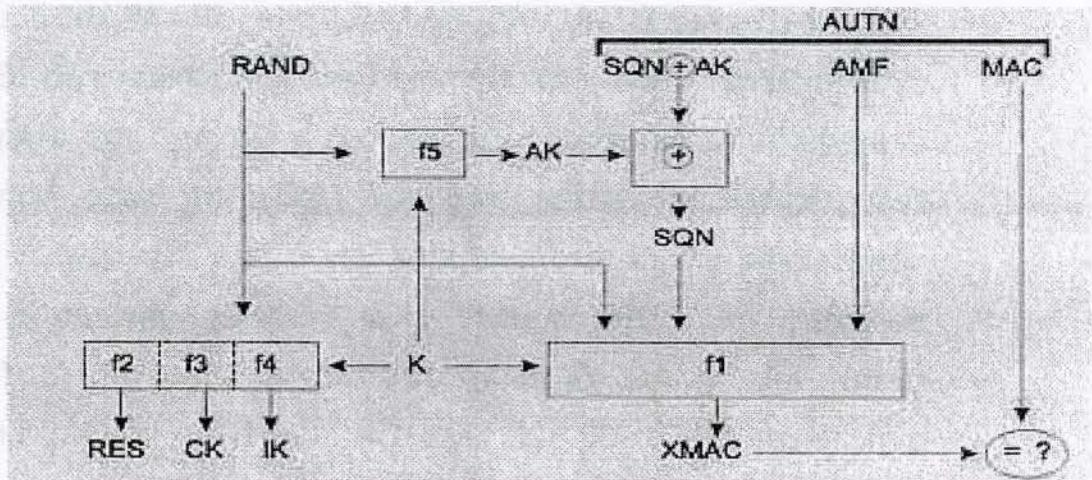
Η βασική έννοια κατά τον υπολογισμό στοιχείου πιστοποίησης ταυτότητας είναι μια μονόδρομη λειτουργία. Αυτό είναι μια μαθηματική λειτουργία, η οποία είναι σχετικά εύκολο να υπολογιστεί αλλά πρακτικά αδύνατο να αντιστραφεί. Με άλλα λόγια, αν το αποτέλεσμα γνωστοποιηθεί δεν υπάρχει αποτελεσματικός αλγόριθμος για να απομονώσει οποιαδήποτε εισαγωγή στοιχείων που θα οδηγούσε στην παραγωγή του αποτελέσματος. Φυσικά, για τον εντοπισμό των σωστών εισαχθέντων στοιχείων από έναν απλό αλγόριθμο είναι η δοκιμή όλων των πιθανών επιλογών μέχρι τον εντοπισμό του επιθυμητού αποτελέσματος. Είναι φανερό ότι αυτός ο αλγόριθμος εξαντλητικής αναζήτησης γίνεται εξαιρετικά ανεπαρκής όσο το μέγεθος των πληροφοριών αυξάνεται.

Συνολικά χρησιμοποιούνται πέντε μονόδρομες λειτουργίες για τον υπολογισμό του στοιχείου πιστοποίησης ταυτότητας. Αυτές οι λειτουργίες είναι οι f1, f2, f3, f4 και f5. Η f1 λειτουργία διαφέρει από τις υπόλοιπες τέσσερις στον αριθμό παραμέτρων εισόδου. Καταχωρεί τέσσερις παραμέτρους: κύριο κλειδί **K**, τυχαίο αριθμό RAND, αριθμό ακολουθίας SQN και τέλος ένα πεδίο διαχείρισης πιστοποίησης ταυτότητας AMF (Authentication Management Field). Όλες οι άλλες λειτουργίες από το f2 έως την f5 καταχωρούν μόνο το κλειδί **K** και το RAND. Η μονόδρομη

ιδιότητα είναι κοινή για όλες τις λειτουργίες f1 - f5 και όλες μπορούν να αναπτυχθούν γύρω από την ίδια θεμελιώδη λειτουργία. Εντούτοις, είναι σημαντικό να διαφέρουν μεταξύ τους η μια από την άλλη λειτουργία με έναν θεμελιώδη τρόπο: από την έξοδο της μιας λειτουργίας καμία πληροφορία για τα αποτελέσματα των άλλων λειτουργιών δεν μπορεί να συναχθεί. Η έξοδος του f1 είναι κώδικας μηνύματος πιστοποίησης ταυτότητας (MAC, 64 bits), αποτελέσματα του f2, f3, f4 και f5 είναι, αντίστοιχα, XRES (32-128 bits), CK (128 bits), IK (128 bits) και AK (64 bits).

Το στοιχείο πιστοποίησης ταυτότητας αποτελείται από τις παραμέτρους RAND, XRES, CK, IK και AUTN. Η τελευταία λαμβάνεται από τη σύνδεση τριών διαφορετικών παραμέτρων: Η SQN προστέθηκε bit-by-bit στην AK, AMF και τη MAC.

Τώρα εξετάζουμε το χειρισμό της πιστοποίησης ταυτότητας από την πλευρά του USIM. Αυτό απεικονίζεται στην εικόνα 90. Οι ίδιες λειτουργίες f1 - f5 συναντιούνται και σ'αυτή τη περίπτωση αλλά σε μια ελαφρώς διαφορετική κατάταξη. Η λειτουργία f5 πρέπει να υπολογιστεί πριν από τη λειτουργία f1 δεδομένου ότι f5 χρησιμοποιείται για να κρύψει SQN. Αυτή η απόκρυψη είναι απαραίτητη έτσι ώστε να αποφευχθεί η υποκλοπή πληροφοριών σχετικά με την ταυτότητα του χρήστη εντός του SQN. Το αποτέλεσμα της λειτουργία f1 παρουσιάζεται στο χρήστη ως XMAC. Αυτό συγκρίνεται με τη MAC που παραλαμβάνεται από το δίκτυο ως τμήμα της παραμέτρου AUTN. Εάν υπάρχει αντιστοιχία σημαίνει ότι η RAND και AUTN έχει δημιουργηθεί από κάποια οντότητα που γνωρίζει το κλειδί K, για παράδειγμα από το AuC του οικιακού δικτύου του χρήστη.



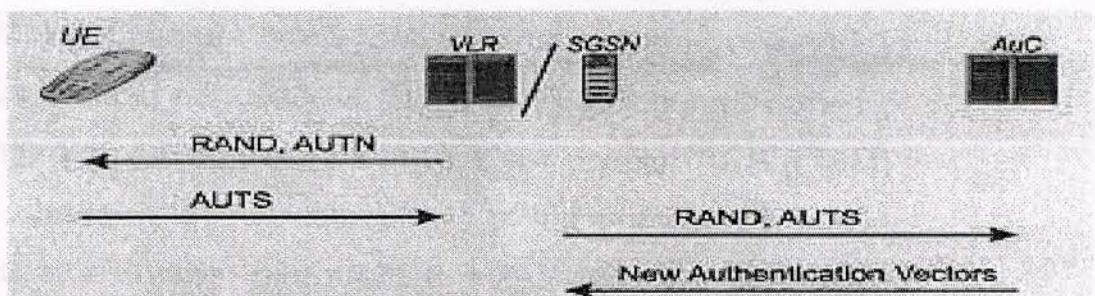
Εικόνα 90 Χειρισμός της εξακρίβωσης στο USIM

Παρόλα αυτά υπάρχει η πιθανότητα κάποιος επιτιθέμενος που έχει καταγράψει ένα πιά πρόωρο γεγονός πιστοποίησης ταυτότητας επαναλαμβάνει το ζευγάρι της RAND και AUTN. Όπως αναφέρεται ανωτέρω, ο αριθμός ακολουθίας προστατεύει ενάντια σε αυτήν την απειλή. Το USIM θα πρέπει απλά να ελέγξει ότι δεν έχει ξαναδει το ίδιο SQN. Ο ευκολότερος τρόπος να ελεγχθεί αυτό είναι η εμφάνιση των αριθμών ακολουθίας σε αύξουσα κατάταξη. Είναι επίσης πιθανό ότι το USIM επιτρέπει ορισμένα SQNs να φτάσουν καθυστερημένα και σε λάθος σειρά εάν διατηρεί για παράδειγμα μικρή λίστα από τους μεγαλύτερους αριθμούς ακολουθίας που έχουν ληφθεί ως τώρα. Δεδομένου ότι η μεταφορά των στοιχείων πιστοποίησης ταυτότητας από το AuC και η πραγματική χρήση αυτών των στοιχείων για την πιστοποίηση ταυτότητας γίνονται εν μέρη ανεξάρτητα, είναι πιθανή η χρήση των στοιχείων αυτών σε διαφορετική σειρά από την αρχικά διαμορφωμένη. Ο προφανέστερος λόγος για αυτή τη περίπτωση είναι συνέπεια της ανεξαρτησίας των λειτουργιών που έχουν να κάνουν με διαχείριση για το CS και PS domain. Αυτό υποδεικνύει ότι τα στοιχεία πιστοποίησης ταυτότητας προσκομίζονται σε VLR και SGSN ανεξάρτητα το ένα από το άλλο και χρησιμοποιούνται επίσης ανεξάρτητα.

Η επιλογή των αλγορίθμων f1 - f5 ορίζεται κατά κύριο λόγο από το operator. Αυτό συμβαίνει επειδή χρησιμοποιούνται μόνο στο AuC και στο USIM και ο ίδιος home operator τα ελέγχει και τα δύο. Ένα παράδειγμα

συνόλων αλγορίθμων (MILENAGE) υπάρχει στη 3GPP προδιαγραφή TS 35.206. Η διαχείριση του αριθμού ακολουθίας ορίζεται επίσης από τον operator. Υπάρχουν δύο βασικές μέθοδοι στη δημιουργία αριθμών ακολουθίας: κάθε χρήστης μπορεί να έχει έναν μεμονωμένο αριθμό ακολουθίας ή μια παραγωγή αριθμού ακολουθίας που μπορεί να έχει σαν βάση έναν global counter, π.χ. universal time. Ο συνδυασμός αυτών των δύο μεθόδων είναι επίσης πιθανός: παραδείγματος χάριν, το σημαντικό μέρος του SQN ορίζεται από τον χρήστη ενώ το λιγότερο έχει σαν βάση έναν global counter.

Ο μηχανισμός αμοιβαίας πιστοποίησης ταυτότητας βασίζεται σε δύο παραμέτρους που είναι καταχωρημένες τόσο στο AuC όσο και στο USIM: ένα αμετάβλητο βασικό κλειδί **K** και ένας δυναμικός αριθμός ακολουθίας SQN. Είναι ζωτικής σημασίας ότι αυτές οι παράμετροι διατηρούνται και στις δυο πλευρές με έναν συγχρονισμένο τρόπο. Για το αμετάβλητο κλειδί **K** αυτό είναι εύκολο αλλά είναι πιθανό ότι οι δυναμικές πληροφορίες σχετικά με τους αριθμούς ακολουθίας απομένουν από το συγχρονισμό για οποιοδήποτε λόγο. Ως συνέπεια, η πιστοποίηση ταυτότητας θα αποτύγχανε. Μια συγκεκριμένη διαδικασία επαν-συγχρονισμού χρησιμοποιείται σε αυτήν την περίπτωση στην εικόνα 91. Με τη χρησιμοποίηση του βασικού κλειδιού **K** ως βάση για την ασφαλή επικοινωνία, το USIM ενημερώνει το AuC για το τρέχον SQN.



Εικόνα 91 Επαναληπτική Διαδικασία συγχρονισμού

Μια παράμετρος AUTS παραδίδεται κατά τη διάρκεια του επαν-συγχρονισμού. Περιέχει δύο μέρη: τον αριθμό ακολουθίας του USIM που

καλύπτεται από το AK και ένα μήνυμα πιστοποίησης ταυτότητας κώδικα MAC-S που υπολογίζεται από μια άλλη μονόδρομη λειτουργία f1 από τις εισαγόμενες παραμέτρους SQN, K, RAND και AMF. Οι τελευταίες δύο παράμετροι λαμβάνονται από το αποτυχημένο γεγονός πιστοποίησης ταυτότητας. Η μονόδρομη λειτουργία f1* πρέπει να διαφέρει από την f1 γιατί σε διαφορετική περίπτωση οι κατεγεγραμμένες παράμετροι AUTN θα να μπορούσαν να είναι αποδεκτές ως έγκυρες παράμετροι AUTS κατά τον επανασυγχρονισμό και ένας επιτιθέμενος θα μπορούσε να εισβάλει στο μηχανισμό αυθεντικοποίησης.

8.1.4. Προσωρινές ταυτότητες

Η μόνιμη ταυτότητα του χρήστη στο UMTS είναι IMSI όπως στη περίπτωση επίσης του GSM. Εντούτοις, ο προσδιορισμός του χρήστη σε UTRAN γίνεται σε όλες σχεδόν τις περιπτώσεις από προσωρινές ταυτότητες, με την TMSI στο CS domain ή P-TMSI στο PS domain. Αυτό δείχνει ότι η εχεμύθεια της ταυτότητας χρηστών προστατεύεται σχεδόν πάντα έναντι στους επιτιθέμενους. Η αρχική συνδρομή είναι μια εξαιρετική περίπτωση όπου η προσωρινή ταυτότητα δεν μπορεί να χρησιμοποιηθεί δεδομένου ότι το δίκτυο δεν γνωρίζει ακόμα τη μόνιμη ταυτότητα του χρήστη. Μετά από αυτό είναι δυνατή η χρήση προσωρινών ταυτοτήτων.

Ο μηχανισμός λειτουργεί ως εξής. Υποθέτουμε ότι ο χρήστης έχει ήδη αναγνωριστεί από την IMSI εντός του δικτύου υπηρεσιών. Έπειτα το δίκτυο υπηρεσιών (VLR ή SGSN) δεσμεύει μια προσωρινή ταυτότητα (TMSI ή P - Tmsi) για τον χρήστη και διατηρεί τον συσχετισμό μεταξύ της μόνιμης ταυτότητας και της προσωρινής. Το τελευταίο είναι σημαντικό μόνο τοπικά και κάθε VLR ή SGSN απλά φροντίζει να μην δεσμεύσει το ίδια TMSI/P-Tmsi σε δύο διαφορετικούς χρήστες ταυτόχρονα. Η δεσμευμένη προσωρινή ταυτότητα μεταφέρεται στο χρήστη την έναρξη κρυπτογράφησης. Αυτή η ταυτότητα χρησιμοποιείται έπειτα τόσο για uplink όσο και downlink signaling μέχρι μια νέα TMSI (ή P-Tmsi) δεσμευτεί από

το δίκτυο. Η δέσμευση μιας νέας προσωρινής ταυτότητας αναγνωρίζεται από το τερματικό και μετά από αυτό η παλαιά προσωρινή ταυτότητα αφαιρείται από το VLR (ή SGSN). Αν η επιβεβαίωση της δέσμευσης δεν φτάσει στο VLR/SGSN θα κρατήσει τόσο την παλαιά όσο και την νέα (P-)TMSI και θα δεχτεί τη μια από αυτές κατά το uplink signaling. Κατά το downlink signaling η IMSI πρέπει να χρησιμοποιηθεί επειδή το δίκτυο δεν γνωρίζει ποια προσωρινή ταυτότητα είναι αυτή τη στιγμή αποθηκευμένη στο τερματικό. Σε αυτήν την περίπτωση, VLR/SGSN δίνει εντολή στο τερματικό να σβήσει οποιαδήποτε αποθηκευμένη TMSI/P-TMSI και ακολουθεί μια νέα επανατοποθέτηση.

Παραμένει παρόλα αυτά ένα πρόβλημα. Πως το δίκτυο υπηρεσιών αποκομίζει την IMSI. Από τη στιγμή που προσωρινή ταυτότητα έχει υπόσταση μόνο τοπικά η ταυτότητα σε τοπικό επίπεδο πρέπει να επισυναφθεί προκειμένου να ληφθεί μια σαφής ταυτότητα για το χρήστη. Αυτό σημαίνει ότι η Location Area Identity (LAI) επισυνάπτεται στο SI και Routing Area Identity (RAI) επισυνάπτεται στην P-Tmsi.

Αν το UE φθάσει σε μια νέα περιοχή τότε η ένωση μεταξύ IMSI και (P-)TMSI μπορεί να προσκομιστεί από την παλαιά θέση ή από τη Routing Area αν η διεύθυνσή της είναι γνωστή στη νέα περιοχή (που βασίζεται σε LAI ή RAI). Αν η διεύθυνση δεν είναι γνωστή ή μια σύνδεση στην παλαιά περιοχή δεν είναι εφικτή τότε UE αναζητά IMSI.

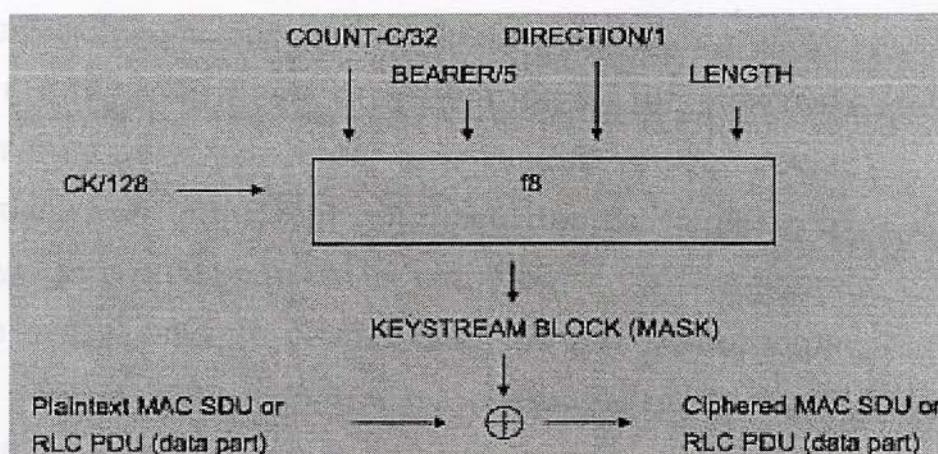
Υπάρχουν μερικά συγκεκριμένα μέρη, π.χ. αερολιμένες όπου πολλά IMSIs μπορούν να διαβιβαστούν μέσω του radio interface αφού πολλοί ανοίγουν τα κινητά τους μετά την πτήση. Από την άλλη πλευρά ο εντοπισμό των ατόμων είναι πιο δύσκολος σε αυτά τα μέρη. Συνολικά, ο μηχανισμός εμπιστευτικότητας ταυτότητας των χρηστών στο UMTS δεν παρέχει 100% προστασία αλλά προσφέρει ένα σχετικά καλό επίπεδο προστασίας. Η προστασία ενάντια σε έναν ενεργό επιτιθέμενο δεν είναι πολύ καλή δεδομένου ότι ο επιτιθέμενος μπορεί να προσποιηθεί ότι παρέχει ένα δίκτυο υπηρεσιών στο οποίο ο χρήστης αποκαλύπτει τη

μόνιμη ταυτότητά. Ο μηχανισμός αμοιβαίας πιστοποίησης ταυτότητας δεν βοηθά σ'αυτή τη περίπτωση καθώς ο χρήστης πρέπει να προσδιοριστεί προτού να μπορέσει να επικυρωθεί.

8.1.5. Απόκρυψη του UTRAN

Από τη στιγμή που ο χρήστης και το δίκτυο έχουν αμοιβαία αναγνώριση μπορούν να ξεκινήσουν ασφαλείς επικοινωνίες. Όπως περιγράφηκε νωρίτερα cipher key CK μοιράζεται μεταξύ του βασικού δικτύου και του τερματικού μετά από ένα επιτυχές γεγονός πιστοποίησης ταυτότητας. Προτού να μπορέσει να αρχίσει η κρυπτογράφηση, τα επικοινωνιώντας συμβαλλόμενα μέρη πρέπει να συμφωνήσουν σχετικά με τον αλγόριθμο κρυπτογράφησης. Ευτυχώς, στο UMTS που εφαρμόζεται σύμφωνα με 3GPP R99, μόνο ένας αλγόριθμος καθορίζεται. Η κρυπτογράφηση/αποκρυπτογράφηση πραγματοποιείται στο τερματικό και στο RNC από του δικτύου. Αυτό σημαίνει ότι cipher key CK πρέπει να μεταφερθεί από τη CN στο radio access network. Αυτό γίνεται σε ένα συγκεκριμένο μήνυμα RANAP, το *Security Mode Command*. Αφού το RNC έχει λάβει το CK μπορεί να ξεκινήσει την κρυπτογράφηση στέλνοντας στο τερματικό RRC Security Mode Command.

Ο μηχανισμός κρυπτογράφησης UMTS είναι βασισμένος σε ένα stream cipher όπως απεικονίζεται στο 92.



Εικόνα 92 Αλλαγή ροής στο UMTS

Αυτό σημαίνει ότι τα δεδομένα plaintext προστίθενται bit-by-bit to random-looking mask data, τα οποία δημιουργούνται βασισμένα στο cipher key CK και μερικές άλλες παραμέτρους. Αυτός ο τύπος κρυπτογράφησης έχει το πλεονέκτημα ότι τα mask data μπορούν να παραχθούν πριν γνωστοποιηθεί το plaintext. Έπειτα η τελική κρυπτογράφηση είναι μια πολύ γρήγορη λειτουργία. Η αποκρυπτογράφηση στη λαμβάνουσα πλευρά γίνεται με ακριβώς τον ίδιο τρόπο καθώς η πρόσθεση mask bits δυο φορές έχει το ίδιο αποτέλεσμα με την προσθήκη μηδενικών.

Κάθως τα mask data δεν εξαρτώνται καθόλου από το plaintext είναι απαραίτητη η ύπαρξη άλλης μιας παραμέτρου εισόδου η οποία αλλάζει με κάθε δημιουργία καινούργιας mask. Διαφορετικά, δύο διαφορετικά plaintexts, για παράδειγμα το P1 και το P2 θα προστατεύονταν από την ίδια mask. Έπειτα θα συνέβαινε το ακόλουθο ανεπιθύμητο φαινόμενο: αν προσθέσουμε bit-by-bit το P1 και το P2 και κάνουμε το ίδιο με τα κρυπτογραφημένα μέρη τους, τότε το bit string που θα προέκυπτε θα ήταν το ίδιο και στις δυο περιπτώσεις. Αυτό συμβαίνει διότι δυο πανομοιότυπες masks ακυρώνει η μια την άλλη κατά την διαδικασία προσθήκης bit-by-bit. Ως αποτέλεσμα το bit-by-bit άθροισμα των P1 και P2 θα γινόταν γνωστό σε οποιοδήποτε θα προσπαθούσε να εισβάλει στα κρυπτογραφημένα μηνύματα στο radio interface. Χαρακτηριστικά, εάν δύο bit strings σημαντικών στοιχείων προστεθούν το ένα στο άλλο bit-by-bit, και τα δύο μπορούν να αποκαλυφθούν πλήρως από το bits string που θα προκύψει. Έτσι αυτό θα αναδείκνυε μια διαροή στη κρυπτογράφηση για τα δυο μηνύματα P1 και P2.

Η κρυπτογράφηση εμφανίζεται είτε στο medium access control layer(MAC) είτε στο radio link control layer (RLC). Και στις δύο περιπτώσεις, υπάρχει ένας μετρητής που αλλάζει για κάθε PDU. Στη MAC αυτό είναι connection frame number (CFN) και στο RLC ένα συγκεκριμένο αριθμός ακολουθίας(sequence number) RLC-SN. Αν αυτοί οι μετρητές χρησιμοποιούνται υπό αυτήν τη μορφή ως είσοδος για την παραγωγή

mask το πρόβλημα θα που εξηγήθηκε στη προηγούμενη παράγραφο θα εμφανιζόταν ακόμα δεδομένου ότι αυτοί οι μετρητές μηδενίζονται γρήγορα. Γί αυτό εισάγεται ένας μεγαλύτερος μετρητής που ονομάζεται hyperframe number (HFN). Αυξάνεται όποτε ο μικρός μετρητής (CFN στο MAC και RLC-SN στο RLC) μηδενίζεται. Ο συνδυασμός του HFN και του μικρότερου μετρητή ονομάζεται count-c και χρησιμοποιείται ως μια συνεχώς μεταβαλλόμενη είσοδος στην παραγωγή mask μέσα στο μηχανισμό κρυπτογράφησης.

Κατά κύριο λόγο ο μεγαλύτερος μετρητής HFN θα μπορούσε επίσης να μηδενιστεί. Ευτυχώς, είναι τα γεγονότα πιστοποίησης ταυτότητας συμβαίνουν αρκετά συχνά έτσι ώστε να μηδενιστεί η πιθανότητα εμφάνισης HFN wrap-around.

Η ταυτότητα BEARER του radio bearer είναι επίσης απαραίτητη για τον αλγόριθμο κρυπτογράφησης καθώς οι μετρητές για διαφορετικούς radio bearers διατηρούν ανεξαρτησία μεταξύ τους. Αν ο input bearer δεν προοριζόταν για χρήση τότε θα οδηγούμασταν στη κατάσταση που το ίδιο σύνολο input parameters θα συμπεριλαμβάνονταν στον αλγόριθμο και η ίδια mask θα αναπαραγόταν περισσότερες από μια φορές. Ως συνέπεια θα συνέβαινε το πρόβλημα που περιγράφηκε παραπάνω και τα μηνύματα(αυτή τη φορά σε διαφορετικούς radio bearers) που έχουν κρυπτογραφηθεί με την ίδια mask θα ήταν εκτεθημένα στον επιτιθέμενο.

Ο πυρήνας του μηχανισμού κρυπτογράφησης είναι ο αλγόριθμος παραγωγής mask που έχει αντιστοιχηθεί με την λειτουργία F8. Η προδιαγραφεί είναι δημόσια διαθέσιμη ως αυτήν 3GPP TS 35.201 και βασίζεται σε ένα block cipher το επονομαζόμενο KASUMI(για το οποίο ισχύει μια άλλη προδιαγραφή 3GPP TS 35.202). Αυτό το block cipher μετατρέπει το 64 bit input σε 64bit output. Η μετατροπή ελέγχεται από το 128 bit cipher key CK. Αν το CK δεν είναι γνωστό τότε δεν υπάρχουν αποτελεσματικοί αλγόριθμοι για τον υπολογισμό του output από το input ή

το αντίθετο. Η μετατροπή αυτή μπορεί να γίνει αν ισχύει ένα από τα ακόλουθα:

- όλα τα πιθανά κλειδιά δοκιμάζονται μέχρι να εντοπιστεί το σωστό
- συλλέγεται ένας τεράστιος πίνακας από όλα τα ζευγάρια 2^{64} input-output

Και οι δύο προσεγγίσεις είναι πρακτικά αδύνατες.

Είναι πιθανό η πιστοποίηση ταυτότητας να μην εκτελείται κατά την έναρξη της σύνδεσης. Σε αυτήν την περίπτωση χρησιμοποιείται το προηγούμενο cipher key για την κρυπτογράφηση. Το κλειδί καταχωρείται στο USIM μεταξύ των συνδέσεων. Επίσης, το σημαντικότερο μέρος του μεγαλύτερου HFN που χρησιμοποιείται μέχρι τώρα καταχωρείται στο USIM. Για την επόμενη σύνδεση, η καταχωρημένη τιμή αυξάνεται κατά ένα και χρησιμοποιείται ως αρχική τιμή για το σημαντικότερο μέρος του HFN.

Ένας δείκτης cipher χρησιμοποιείται στα τερματικά για να εμφανίσει στο χρήστη εάν η κρυπτογράφηση εφαρμόζεται ή όχι, παρέχοντας κατά συνέπεια κάποια διαφάνεια των μηχανισμών ασφάλειας. Σημειώστε ότι παρόλο που συνιστάται η χρήση ciphering παραμένει προαιρετική για τα δίκτυα UMTS.

8.1.6. Προστασία της ακεραιότητας του σήματος του RRC

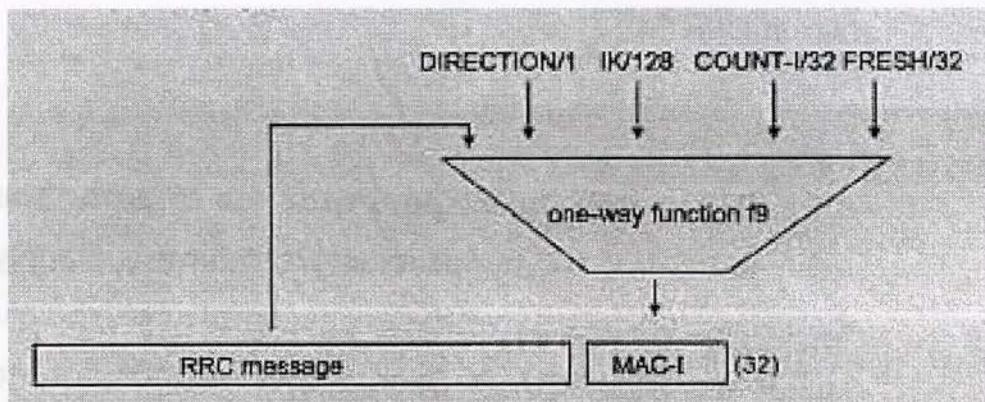
Ο σκοπός της προστασίας ακεραιότητας(Integrity Protection) είναι η αυθεντικοποίηση μεμονομένων μηνύματων ελέγχου. Αυτό είναι σημαντικό καθώς μια ξεχωριστή διαδικασία αυθεντικοποίησης παρέχει διαβεβαίωση σχετικά με τις ταυτότητες (identities) των επικοινωνούντων πλευρών μόνο κατά τη διάρκεια της. Στην εικόνα 86 απεικονίζεται το παραπάνω θέμα: ένα ψευδές BS λειτουργεί ως ένας απλός σύνδεσμος και παραδίδει όλα τα μηνύματα στη σωστή μορφή τους μέχρι την ολοκλήρωση της διαδικασίας αυθεντικοποίησης. Έπειτα το ψευδές BS μπορεί να ξεκινήσει την

μεταποίηση των μηνυμάτων. Εντούτοις, εάν τα μηνύματα είναι προστατευμένα χωριστά, ο σκόπιμος χειρισμός των μηνυμάτων μπορεί να παρατηρηθεί και τα ψεύτικα μηνύματα μπορούν να απορριφθούν.

Η προστασία ακεραιότητας εφαρμόζεται στο στρώμα RRC. Κατά συνέπεια, χρησιμοποιείται μεταξύ του τερματικού και του RNC, ακριβώς όπως την κρυπτογράφηση. Η κλειδί ακεραιότητας IK παράγεται κατά τη διάρκεια της πιστοποίησης ταυτότητας και της βασικής διαδικασίας συμφωνίας, πάλι παρόμοια με το κλειδί cipher. Επίσης, το IK μεταφέρεται στο RNC μαζί με τα CK στην εντολή κατάσταση ασφαλείας.

Ο μηχανισμός προστασίας ακεραιότητας είναι βασισμένος στην έννοια ενός κώδικα πιστοποίησης ταυτότητας μηνυμάτων. Αυτό είναι μια μονόδρομη λειτουργία, η οποία ελέγχεται από το μυστικό κλειδί IK.

Η λειτουργία ενεργοποιείται με το f9 και έχει ως output το MAC-I, το οποίο αποτελεί ένα φαινομενικά τυχαίο (random-looking) bit string. Το MAC-I προσκολλάται σε κάθε μήνυμα RRC ενώ παράλληλα δημιουργείται και ελέγχεται από την πλευρά λήψης. Επηρεάζεται από κάθε αλλαγή στις παραμέτρους με έναν απρόβλεπτο τρόπο. Η λειτουργία f9 απεικονίζεται στο 93.



Εικόνα 93 Κωδικός εξακρύβωσης μηνύματος

Ως inputs είναι τα ακόλουθα: IK, το μήνυμα RRC, ένας μετρητής COUNT-I, το (direction bit) bit κατεύθυνσης (uplink/downlink) και ένας τυχαίος αριθμός FRESH. Η παράμετρος COUNT-I προσδιορίζει τον ανταποκρινόμενο μετρητή (counter) για την κρυπτογράφηση. Το πιο

χαρακτηριστικό τμήμα είναι ένα HFN και τα τέσσερα λιγότερο σημαντικά bits από τον αριθμό ακολουθίας RRC (RRC sequence number). Εν ολίγης, το COUNT-I αποτρέπει την επανάληψη μηνυμάτων ελέγχου: εγγυάται ότι το σύνολο των τιμών για τις παραμέτρους εισόδου (input parameters) είναι διαφορετικό για κάθε εκτέλεση της λειτουργίας προστασίας ακεραιότητας f 9.

Η παράμετρος FRESH επιλέγεται από το RNC και εκπέμπεται στο UE. Στο σημείο αυτό, είναι απαραίτητη η προστασία του δικτύου ενάντια σε μία εσφαλμένη (maliciously chosen) αρχική τιμή για το COUNT-I. Το πιο σημαντικό μέρος του HFN αποθηκεύεται στο USIM μεταξύ των συνδέσεων. Ένας επιτιθέμενος θα μπορούσε να παρουσιαστεί ως USIM και να στείλει στο δίκτυο μία εσφαλμένη τιμή, καθιστώντας έτσι την αρχική τιμή του HFN πολύ χαμηλή/μικρή. Στην περίπτωση που δεν εκτελείται η διαδικασία αυθεντικοποίησης χρησιμοποιείται η παλιά IK. Το γεγονός αυτό θα έδινε την ευκαιρία στον επιτιθέμενο να επαναλάβει μηνύματα RRC signaling από προηγούμενες συνδέσεις με καταχωρημένες τιμές MAC-I με την προϋπόθεση απουσίας της παραμέτρου FRESH. Με την τυχαία επιλογή της FRESH, το RNC προστατεύεται από τέτοιου είδους επιθέσεις, οι οποίες βασίζονται στην καταχώρηση προηγούμενων συνδέσεων. Όπως έχει ήδη γίνει γνωστό, ο συνεχώς αυξανόμενος μετρητής COUNT-I προστατεύει ενάντια σε επιθέσεις επανάληψης (replay attacks) που έχουν ως βάση την καταχώρηση κατά τη διάρκεια κοινής σύνδεσης καθώς η FRESH παραμένει ίδια. Θα πρέπει να σημειωθεί ότι η ταυτότητα (identity) του radio bearer δεν χρησιμοποιείται ως παράμετρος εισόδου για τον αλγόριθμο ακεραιότητας, αντίθετα από την περίπτωση του αλγορίθμου κρυπτογράφησης. Καθώς είναι πιθανή η ύπαρξη αρκετών radio bearers παράλληλα για το control plane, είναι εφικτή η επανάληψη μηνυμάτων ελέγχου (control messages) που καταχωρήθηκαν εντός της ίδιας σύνδεσης RRC αλλά σε διαφορετικό radio bearer. Παρ' όλ' αυτά, δεν είναι αυτό το θέμα που μας απασχολεί, καθώς η radio bearer identity ενσωματώνεται

στο μήνυμα μετά τον υπολογισμό του κωδικού αυθεντικοποίησης μηνύματος (message authentication code) (παρά του ότι δεν μεταδίδεται με το μήνυμα). Για αυτόν τον λόγο, η ταυτότητα του radio bearer επιδρά στην τιμή του MAC-I και έχουμε προστασία ενάντια σε επιθέσεις επανάληψης που έχουν ως βάση εγγραφές σε διαφορετικούς radio bearers.

Είναι εμφανές ότι υπάρχουν μερικά μηνύματα ελέγχου RRC των οποίων η ακεραιότητα δεν μπορεί να προστατευτεί από τον μηχανισμό. Στην πραγματικότητα, τα μηνύματα που αποστέλλονται πριν την ενσωμάτωση του κλειδιού ακεραιότητας IK (integrity key IK) δεν μπορούν να προστατευτούν. Τυπικό παράδειγμα αποτελεί το μήνυμα αίτησης σύνδεσης RRC (RRC connection request message).

Το Social engineering δεν αναγνωρίζεται συνήθως ως κίνδυνος ασφάλειας από τον μέσο συνδρομητή παρά το γεγονός ότι παίζει σημαντικό ρόλο σε πολλές περιπτώσεις επιθέσεων. Όσον αφορά τους συνδρομητές, το social engineering αποτελεί, για παράδειγμα, τους τρόπους πρόσβασης σε ένα τερματικό με την ανάκτηση του PIN. Ο συνδρομητής έχει τη δυνατότητα να προστατευτεί έναντι του social engineering καθιστώντας ενεργή την απόκρυψη του PIN και διατηρώντας το παράλληλα διαχωρισμένο από το τερματικό. Το social engineering δρα με παραπλήσιο τρόπο και από πλευράς δικτύου: εκείνοι που εργάζονται με στοιχεία δικτύου δέχονται περίεργες κλήσεις και ζητούνται να δώσουν user ID και password σε έναν μη διαθέσιμο καλούντα. Συχνά αυτές οι κλήσεις αποτελούν social engineering όπου ασφαλείς πληροφορίες μπορεί να καταλήξουν σε λάθος χέρια. Στην πραγματικότητα με αυτόν τον τρόπο ξεκινάει την προσπάθειά του ένας hacker. Ως αποτέλεσμα, το social engineering μπορεί να παρέχει πρόσβαση σε στοιχεία δικτύου ζωτικής ή μη σημασίας. Στον χώρο του IP, το social engineering είναι σχετικά παρόμοιο αλλά στον τομέα των τηλεπικοινωνιών δεν χρησιμοποιείται

ευρέως καθώς ο εξοπλισμός δεν υπόκειται σε δημόσια πρόσβαση και το προσωπικό διαχείρισης του έχει συνέπεια της ευθύνης του.

Με το sniffing, ο hacker στοχεύει, για παράδειγμα, στην περισυλλογή πληροφοριών user ID και password. Δυστυχώς, τα προγράμματα sniffing είναι ευρέως διαθέσιμα για download μέσω Internet. Ένα πρόγραμμα sniffing αποτελεί εργαλείο όταν βρίσκεται στα κατάλληλα χέρια και χρησιμοποιείται για παρακολούθηση δικτύων και εντοπισμό πιθανών σφαλμάτων. Όταν όμως βρίσκεται στα λάθος χέρια, αποτελεί ένα ισχυρό μέσο για τον hacker κατά την διακριτική παρακολούθηση πολυάριθμων συνδέσεων στο Internet.

Οι πληροφορίες που έχουν συγκεντρωθεί με το sniffing, μπορούν να utilized στο επόμενο στάδιο με τη μέθοδο hacking spoofing. Το spoofing είναι η μέθοδος κατά την οποία ο hacker χρησιμοποιεί την διεύθυνση IP κάποιου άλλου χρήστη και δέχεται πακέτα από άλλους χρήστες. Με άλλα λόγια, ο hacker αντικαθιστά τον σωστό δέκτη στη σύνδεση.

Ασφαλώς ο hacker θα μπορούσε να επιχειρήσει να ανοίξει μία σύνδεση με την IP address κάποιου άλλου, αλλά είναι πιο δύσκολο και σε πολλές περιπτώσεις αυτού του είδους οι μονόδρομες λειτουργίες (one way traffic) είναι επίσης χρήσιμες για σκοπούς hacking. Σήμερα, το γεγονός ότι οι χρήστες πραγματοποιούν πολλές εργασίες από το σπίτι, αποτελεί έναν τρόπο απόκτησης πρόσβασης σε πληροφορίες της εκάστοτε εταιρίας καθώς εργοδότης και υπάλληλος ανταλλάσσουν δεδομένα μέσω Internet.

Αν ο επιτιθέμενος θελήσει να περάσει στο επόμενο στάδιο, προχωράει στο session hijacking με σκοπό την κατάληψη μίας σύνδεσης. Όπως αναφέρθηκε πρωτίτερα, ακόμα και ένας ισχυρός μηχανισμός αυθεντικοποίησης ταυτότητας κατά την έναρξη της σύνδεσης δεν παρέχει προστασία σε μετέπειτα hijacking. Είναι απαραίτητη η ύπαρξη προστασίας ακεραιότητας για ολόκληρη τη session.

Κατά την (επίθεση) Denial of Service (DoS) attack ο hacker δεν στοχεύει στην συλλογή πληροφοριών, αλλά στο να προκαλέσει ζημιές και προβλήματα σε άλλους χρήστες και service providers.

Σε μία τυπική επίθεση DoS, ο hacker δημιουργεί προβληματική ροή (disturbing traffic) η οποία στην χειρότερη περίπτωση μπλοκάρει τον επιθυμητό server με τέτοιο τρόπο ώστε να μη μπορεί να παρέχει πλέον υπηρεσίες. Το σκεπτικό είναι, για παράδειγμα, είναι η πλήρωση του server από αιτήματα (requests) και η παράλειψη των επιβεβαιώσεων (acknowledgements) που αποστέλλει ο server. Ως συνέπεια, ο server δεσμεύει πόρους για την επερχόμενη σύνδεση, η οποία τελικά δεν πραγματοποιείται. Με τη λήξη των μετρητών της σύνδεσης απελευθερώνονται οι πόροι για την εξυπηρέτηση άλλης σύνδεσης. Όταν οι προσπάθειες σύνδεσης που περιέχουν buffer δέχονται συνεχώς νέα αιτήματα οπότε και γεμίζουν, ο server κολλάει και δεν μπορεί να παρέχει «πραγματική» υπηρεσία.

Υπάρχουν και πιο εξειδικευμένες επιθέσεις DoS και πολυάριθμα εργαλεία για αυτόν τον σκοπό στο διαδίκτυο. Συνοπτικά, η προστασία ενάντια σε DoS είναι πολύ δύσκολο αντικείμενο.

Μία βελτιωμένη επίθεση DoS μπορεί να έχει ενσωματωμένες και άλλες μεθόδους από εκείνες που περιγράφηκαν νωρίτερα. Για παράδειγμα, η DoS ξεκινάει από κλεμμένες διευθύνσεις IP με έναν τρόπο όπου μπορεί να παρευρίσκονται εκατοντάδες υπολογιστές. Η DoS αποτελεί μία πολύ ισχυρή και επικίνδυνη επίθεση και προκαλεί με χαρακτηριστική ευκολία μεγάλες οικονομικές απώλειες. Τον Φεβρουάριο του 2000, δύο μεγάλες εταιρίες Internet, δέχτηκαν σοβαρές επιθέσεις DoS και οι συνδέσεις τους δεν ήταν σε θέση να παρέχουν υπηρεσίες κατά τη διάρκειά της.

Άλλο ένα παράδειγμα επίθεσης τύπου DoS είναι η στόχευση σε μηχανές αναζήτησης του διαδικτύου (Internet search engines) που υπερφορτώνονται με δεδομένα ανακριβών αιτημάτων. Το παραπάνω,

αποτελεί έναν «φτηνό» όσο και απλό τρόπο για να κρεμάσει ένας search engine server.

Το παραπάνω κείμενο περιέγραψε συνοπτικά τις πιο συνηθισμένες επιθέσεις ασφάλειας, οι οποίες αποτελούν απειλή που δεν πρέπει να αγνοούνται σε καμία περίπτωση καθώς τα εργαλεία πραγματοποίησής τους είναι δωρεάν διαθέσιμα στο Internet. Πώς πρέπει λοιπόν να πράξουμε; Το θέμα της ασφάλειας πρέπει να λαμβάνεται υπόψη ως αλυσίδα, όπου ολόκληρο το σύστημα (ασφάλεια επικοινωνίας (communication security), ασφάλεια δεδομένων (data security) και ασφάλεια μετάδοσης (signaling security) να είναι τόσο ισχυρό όσο και ο πιο αδύναμος κρίκος. Με άλλα λόγια, όλα πρέπει να είναι ασφαλή: οι αλγόριθμοι, τα πρωτόκολλα, οι σύνδεσμοι (links), οι εφαρμογές κ.τ.λ.

8.2 Πτυχές ασφάλειας στα επίπεδα Συστήματος και Δικτύου

8.2.1. Περίληψη της ασφάλειας του 3GPP Release 5 Network Domain

Αναφέρθηκε νωρίτερα, ότι μία από τις αδυναμίες της αρχιτεκτονικής ασφάλειας στο GSM προέρχεται από το γεγονός ότι τα δεδομένα αυθεντικοποίησης ταυτότητας μεταδίδονται απροστάτευτα μεταξύ διαφορετικών δικτύων. Για παράδειγμα, τα κλειδιά cipher χρησιμοποιούνται για την προστασία της ροής (traffic) στο radio interface ενώ τα ίδια μεταφέρονται ελεύθερα μεταξύ δικτύων. Ο λόγος που οδηγεί σε αυτήν την κατάσταση οφείλεται στην κλειστή φύση των δικτύων SS7: μόνο ένας μικρός αριθμός μεγάλων ιδρυμάτων έχει πρόσβαση σε αυτά. Στο UMTS Release 99 η δομή του κεντρικού δικτύου (core network structure) είναι παρόμοια με εκείνη του GSM και γι' αυτό δεν επήλθαν σημαντικές βελτιώσεις στον τομέα της ασφάλειας ροής μεταξύ των CNs.

Στις επερχόμενες εκδόσεις του UMTS η κατάσταση αλλάζει: η δομή του κεντρικού δικτύου εξελίσσεται και η IP γίνεται το κυρίαρχο πρωτόκολλο σχετικά με το στρώμα δικτύων (network layer). Το signaling μεταξύ διαφορετικών κεντρικών δικτύων θα γινόταν μέσω ανοιχτών συνδέσεων.

Υπάρχει μια εμφανής τάση έναντι στην ευκολότερη πρόσβαση στη ροή των κεντρικών δικτύων. Υπάρχουν πολύ περισσότεροι φορείς που περιλαμβάνονται καθώς και μια κοινότητα χάκερ που είναι επιδέξιοι στα ζητήματα IP.

Το βασικό εργαλείο στην προστασία της κυκλοφορίας των δεδομένων των δικτύων είναι το πρωτόκολλο IPSEC. Παρέχει την εμπιστευτικότητα και την ακεραιότητα της επικοινωνίας στο στρώμα IP. Επίσης, τα επικοινωνώντας συμβαλλόμενα μέρη μπορούν να επικυρώσουν το ένα το άλλο χρησιμοποιώντας IPSEC. Το κρίσιμο ζήτημα είναι η βασική διαχείριση: πώς να παράγει, να ανταλλάξει και να διανείμει ποικίλα κλειδιά που απαιτούνται στους αλγορίθμους που χρησιμοποιούνται για να παρέχουν την προστασία εμπιστευτικότητας και ακεραιότητας. Ακολουθεί μια συνοπτική παρουσίαση στο πρωτόκολλο IPSEC.

Επιπρόσθετα στην προστασία των IP-based δικτύων, η ασφάλεια των SS7-based δικτύων ενισχύεται στην έκδοση 5 UMTS. Ενας συγκεκριμένος μηχανισμός ασφάλειας έχει αναπτυχθεί για το πρωτόκολλο MAP. Αυτό καλείται MAPSEC και παρέχει την προστασία εμπιστευτικότητας και ακεραιότητας. Η βασική διαχείριση υποστήριξης MAPSEC περιέχει παρόμοιες τεχνικές με εκείνες που χρησιμοποιούνται για την υποστήριξη IPSEC.

8.2.2. IPSEC

Η IP ασφάλεια τυποποιείται από IETF (Internet Engineering Task Force). Αποτελείται από μια δωδεκάδα RFCs και είναι ένα αναπόσπαστο μέρος IPv6. Στο IPv4 IPSEC μπορεί να χρησιμοποιηθεί ως προαιρετικός "πρόσθετος" μηχανισμός για να παρέχει την ασφάλεια στο στρώμα IP. Τα βασικά συστατικά IPSEC είναι τα ακόλουθα:

- Authentication Header (AH)
- Encapsulation Security Payload (ESP)
- Internet key Exchange (IKE)

Ο σκοπός IPSEC είναι να προστατευθούν τα πακέτα IP: αυτό γίνεται με ESP και/ή AH. Εν ολίγοις, το ESP παρέχει τόσο την προστασία εμπιστευτικότητας όσο και ακεραιότητας ενώ το AH παρέχει μόνο τη τελευταία. Υπάρχουν περισσότερες λεπτές διαφορές μεταξύ των δύο αλλά σαφώς ESP και AH αποτελούν θεμελιώδεις μηχανισμούς. Ένας από τους λόγους για αυτό το είδος πλεονασμού στα πρότυπα IPSEC είναι έλεγχος εξαγωγής: έχουν υπάρξει αυστηροί περιορισμοί στην εξαγωγή των μηχανισμών προστασίας εμπιστευτικότητας στις περισσότερες χώρες, ενώ οι μηχανισμοί προστασίας ακεραιότητας είναι χαρακτηριστικά ελεύθεροι από τους περιορισμούς. Αυτήν την περίοδο τέτοιοι περιορισμοί εξαγωγής καταργούνται και ως συνέπεια η σημασία AH σε σύγκριση με ESP υποβαθμίζεται.

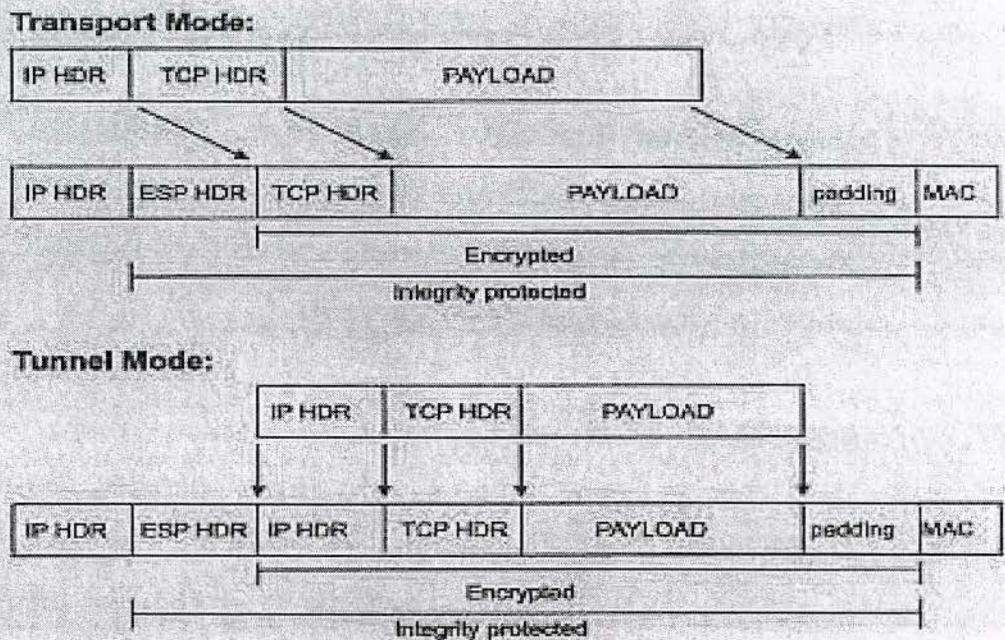
Τόσο το ESP όσο και το AH χρειάζονται κλειδιά. Γενικότερα, μια έννοια μιας ένωσης ασφάλειας Security Association(SA) είναι ουσιαστική στο IPSEC. Εκτός από την κρυπτογράφηση και τα κλειδιά πιστοποίησης, το SA περιέχει πληροφορίες σχετικά με το χρησιμοποιημένο αλγόριθμο, τη διάρκεια ζωής των κλειδιών και το SA το ίδιο, έναν αριθμό ακολουθίας που προστατεύει ενάντια στις επιθέσεις επανάληψης, κ.λ.π.

Οι ενώσεις ασφάλειας πρέπει να συζητηθούν πριν από την χρήση ESP ή AH, ένα για κάθε κατεύθυνση επικοινωνίας. Αυτό επιτυγχάνεται με έναν ασφαλή τρόπο με το πρωτόκολλο IKE. Υπάρχουν διάφοροι τρόποι του IKE αλλά η ιδέα είναι σαφής: τα επικοινωνώντας συμβαλλόμενα μέρη είναι σε θέση να παραγάγουν τα "working keys" και τα SAs, τα οποία χρησιμοποιούνται στην προστασία της επόμενης επικοινωνίας. Το IKE είναι βασισμένο στην έξυπνη ιδέα του δημόσιου βασικού συστήματος κρυπτογραφίας όπου τα μυστικά κλειδιά για την ασφαλή επικοινωνία μπορούν να ανταλλαχθούν μέσω ενός μη ασφαλούς καναλιού. Εντούτοις, η πιστοποίηση ταυτότητας των συμβαλλόμενων μερών που χρησιμοποιούν το IKE δεν μπορεί να πραγματοποιηθεί χωρίς τη χρήση

μακροπρόθεσμων κλειδιών. Αυτά συνήθως βασίζονται είτε σε μια χειροκίνητη συναλλαγή ενός γνωστοποιημένου μυστικού είτε Public Key Infrastructure (PKI) και των πιστοποιητικών. Και οι δύο λύσεις είναι σαφώς σημαντικές: η πρώτη απαιτεί τα μέρη της προσπάθειας διαμόρφωσης ενώ η δεύτερη υπονοεί τα αφιερωμένα στοιχεία υποδομής με την ειδική λειτουργία.

Η διαπραγμάτευση του SAs όπως από IKE είναι ανεξάρτητη από το σκοπό για τον οποίον χρησιμοποιούνται αυτά τα SAs. Γι αυτό το λόγο το IKE μπορεί να χρησιμοποιηθεί για τη διαπραγμάτευση των κλειδιών και των SAs που χρησιμοποιούνται, π.χ. MAPSEC.

Ολοκληρώνουμε με την περαιτέρω περιγραφή του ESP. Υπάρχουν δύο καταστάσεις ESP σε transport mode και tunnel mode. Το transport mode λειτουργεί κατά κύριο λόγο ως εξής: αποκρύπτονται όλα τα στοιχεία του πακέτου IP εκτός από την IP header. Κατόπιν μια νέα ESP header προστίθεται μεταξύ της IP header και του κρυπτογραφημένου μέρους: αυτό περιέχει, π.χ. τις πληροφορίες σχετικά με το SA που χρησιμοποιείται. Επίσης, η κρυπτογράφηση προσθέτει μερικά δυαδικά ψηφία(bits) στο τέλος του πακέτου. Τέλος Message Authentication Code(MAC) υπολογίζεται πέρα από όλα εκτός από την IP header και επισυνάπτεται στο τέλος του πακέτου. Στο τέλος από την πλευρά λήψης ελέγχεται πρώτα η ακεραιότητα. Αυτό γίνεται με την αφαίρεση της IP header από την αρχή του πακέτου και τη MAC από το τέλος του πακέτου, κι έπειτα ακολουθεί η εκτέλεση της λειτουργίας MAC (που βασίζεται στις πληροφορίες της ESP header) και η σύγκριση του αποτελέσματος με τη MAC του πακέτου. Εάν η έκβαση του ελέγχου ακεραιότητας είναι θετική, αφαιρείται η ESP header και τα υπόλοιπα μέρη αποκρυπτογραφούνται (πάλι με βάση τις πληροφορίες στην ESP header). Στην εικόνα 94 απεικονίζεται το παραπάνω.



Εικόνα 94 Encapsulation Security Payload (ESP)

Το tunnel mode διαφέρει από το transport mode κατά τον ακόλουθο τρόπο. Μια νέα IP header προστίθεται στην αρχή του πακέτου. Έπειτα οι ίδιες διαδικασίες όπως στο transport mode πραγματοποιούνται για το νέο πακέτο. Αυτό σημαίνει ότι η IP header του αρχικού πακέτου είναι προστατευμένη, όπως απεικονίζεται στο 95.

Η κατάσταση μεταφοράς είναι η βασική χρήση του ESP μεταξύ δύο σημείων end points. Εντούτοις, όταν εφαρμόζεται στα δίκτυα UMTS υπάρχουν δύο προβλήματα: τα στοιχεία των επικοινωνούντων δικτύων πρέπει:

- Know the IP address of each other;
- Implement all the ISPEC functionality.

Η τυπική χρήση της κατάστασης tunnel σχετίζεται με την έννοια ενός εικονικού ιδιωτικού δικτύου Virtual Private Network (VPN). Το IPSEC χρησιμοποιείται μεταξύ δύο κόμβων (security gateways) και η (end-to-end) προστασία παρέχεται εχέμυθα καθώς το συνολικό πακέτο μέσα στο πακέτο που είναι προστατευμένο μεταξύ των gateways. Σαφώς, σε αυτό το

σενάριο κάθε στοιχείο πρέπει να εμπιστευθεί την αντίστοιχη gateway. Επίσης, το τμήμα από το στοιχείο μέχρι το gateway πρέπει να προστατεύεται με άλλα μέσα π.χ. εφαρμόζεται σε ένα φυσικά προστατευμένο περιβάλλον. Η μέθοδος που προτιμάται για τον έλεγχο των μηνυμάτων του κεντρικού δικτύου UMTS είναι η χρήση ESP σε κατάσταση tunnel μεταξύ των security gateways.

8.2.3. MAPSEC

Τώρα εξετάζουμε εν συντομία μερικές βασικές ιδιότητες του MAPSEC. Η ιδέα είναι να προστατευθεί η εμπιστευτικότητα και η ακεραιότητα των λειτουργιών MAP. Στη δεύτερη κατάσταση προστασίας του MAPSEC, τόσο η εμπιστευτικότητα όσο και η ακεραιότητα είναι προστατευμένες ενώ στην πρώτη κατάσταση προστασίας, μόνο η ακεραιότητα προστατεύεται. Στην κατάσταση προστασίας 0 δεν υπάρχει καμία προστασία.

Για την εμπιστευτικότητα, το φορτίο της αρχικής λειτουργίας MAP είναι κρυπτογραφείται. Ένας security header προστίθεται για να δείξει τον τρόπο που πρέπει να γίνει η αποκρυπτογράφηση και σε γενικές γραμμές να παρέχει ασφάλεια στο MAPSEC. Για την ακεραιότητα, υπολογίζεται ένα MAC πέρα από το cleartext φορτίο της αρχικής λειτουργίας MAP και του security header. Μια παράμετρος συνεχώς μεταβαλλόμενου χρόνου χρησιμοποιείται για την προστασία ενάντια στις επιθέσεις επανάληψης.

Οι συσχετισμοί ασφάλειας για το MAPSEC δημιουργούνται χρησιμοποιώντας το πρωτόκολλο IKE. Αυτό γίνεται με στοιχεία διαχείρισης αποκλειστικού κλειδιού, τα καλούμενα Key Administration Centers(KAC) τα οποία διαπραγματεύονται κλειδιά εκ μέρους όλων των υπόλοιπων στοιχείων CN στο ίδιο δίκτυο. Αυτό οδηγεί σε μερικές βελτιώσεις εντός του IKE, οι οποίες δεν οριστικοποιήθηκαν ακόμα στο IETF του 2001.

8.3. Προστασία των εφαρμογών και των υπηρεσιών

Η ασφάλεια στο δίκτυο εφαρμόζεται σύμφωνα με το μοντέλο OSI (Open System Interconnection) δηλ. κάθε OSI στρώμα έχει τα μέσα του για τους σκοπούς ασφάλειας (εικόνα 95). Για να απλοποιηθούν αυτό, υπάρχουν δύο βασικοί κλάδοι, οι οποίοι είναι link-to-link ασφάλεια και end-to-end ασφάλεια.

Application Layer	S-MIME PGP SET
Presentation Layer	
Session Layer	SSL SOCKS RADIUS
Transaction Layer	
Network Layer	IPSec
Link Layer	
Physical Layer	

Εικόνα 95 Πρωτόκολλα ασφαλείας σε διαφορετικά OSI επίπεδα

Στη link-to-link ασφάλεια η ιδέα είναι ότι μια σύνδεση (path) διαμορφώνεται από links επικοινωνίας. Οτιδήποτε περνάει από το συγκεκριμένο link προστατεύεται από π.χ. την κρυπτογράφηση, και εάν αυτό γίνεται για κάθε link σε κάθε σύνδεση ολόκληρη η σύνδεση είναι ασφαλής. Το μειονέκτημα σε αυτή τη περίπτωση είναι ότι είναι ότι αν η ροή των δεδομένων ακολουθήσει εσφαλμένη πορεία τότε τα περιεχόμενα του link μπορεί να εκτεθούν χωρίς να είναι βέβαιο ότι θα το αντιληφθεί ο τελικός χρήστης.

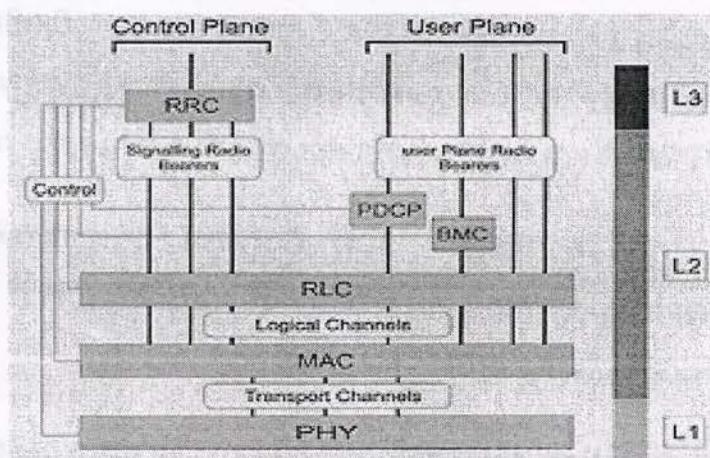
Εάν η ασφάλεια εφαρμοστεί στα υψηλότερα στρώματα του OSI, τότε μιλάμε για τη end-to-end ασφάλεια. Σε αυτήν την περίπτωση τα δεδομένα παραμένουν προστατευμένα, για παράδειγμα, είναι κρυπτογραφημένα μέχρι να φτάσουν στον προορισμό τους. Τα δεδομένα που έχουν αποσταλεί είναι καλά ασφαλισμένα, υπάρχει όμως τώρα η πιθανότητα να πραγματοποιηθεί traffic analysis: μπορεί κάποιος να βρει για παράδειγμα

ποιος τα έστειλε, ποιος τα έλαβε, πότε έγινε η μετάδοση και τη συχνότητα της. Εάν μια συνολική λύση ασφάλειας δικτύων εφαρμόζεται, μια πρέπει να συνδυάσει και την link-to-link και τους end-to-end μηχανισμούς ασφάλειας. Η κρυπτογράφηση κάθε σύνδεσης καθιστά οποιαδήποτε ανάλυση των πληροφοριών δρομολόγησης αδύνατη, ενώ η end-to-end κρυπτογράφηση μειώνει την απειλή τα στοιχεία στους διάφορους κόμβους στο δίκτυο. Σε ορισμένες περιπτώσεις, όπως το κυψελοειδές δίκτυο, η πιστοποίηση ταυτότητας στρώματος συνδέσεων απαιτείται προκειμένου να ελεγχθεί η πρόσβαση στο κυψελοειδές δίκτυο. Στο 3G δίκτυο, οι διαδικασίες ασφάλειας επιπέδων πρόσβασης φροντίζουν την κρυπτογράφηση επιπέδων συνδέσεων και την προστασία ακεραιότητας μέσα στο δίκτυο πρόσβασης. Μέσα στη CN και στις συνδέσεις στο άλλο δίκτυο οι διάφορες μέθοδοι μπορούν να χρησιμοποιηθούν συμπεριλαμβανομένων εκείνων που συζητούνται στο προηγούμενο τμήμα.

Κεφάλαιο 9 Πρωτόκολλα UMTS

9.1 Αναφορά στην Αρχιτεκτονική των Πρωτοκόλλων που χρησιμοποιούνται στη 3GPP R99.

Το interfaces του UTRAN βασίζεται στην ραδιοτεχνολογία του WCDMA, το οποίο έχει κάποιες βασικές διαφορές αν συγκριθεί με την τεχνολογία της 2^{ης} γεννιάς κινητής τηλεφωνίας. Η πλευρά η οποία ελέγχεται από τα πρωτόκολλα του interface είναι πολύπλοκη από τις ροές κίνησης διαφορετικών ειδών και διαφορετικών origins. Για να είναι σίγουρος και αποτελεσματικός ο έλεγχος της πολυπλεξίας η επιπεδοποίηση των καθκόντων έχει εφαρμοστεί. Έτσι, αυτό έχει σαν αποτέλεσμα ένα μοντέλο αναφοράς 3 επιπέδων που παρουσιάζεται στην Εικόνα 60.



Εικόνα 96 Μοντέλο αναφοράς των πρωτοκόλλων του ραδιο interface

Τα επίπεδα ονομάζονται ανάλογα με την θέση στην αρχιτεκτονική του interface: επίπεδο 1, επίπεδο 2, επίπεδο 3. Αν και οι γνωστές αρχές επιπέδων του OSI έχουν εφαρμοστεί στο σχεδιασμό, αυτά τα 3 επίπεδα

δεν μπορούν θεωρηθούν σαν τα 3 κατώτερα επίπεδα του OSI μοντέλου. Τα επίπεδα έχουν καλά καθορισμένες υπευθυνότητες και interfaces μεταξύ τους, το οποίο κάνει δυνατό να ονομαστούν ως ακολούθως:

L1-φυσικό επίπεδο L2-επίπεδο συνδέσεων L3-επίπεδο δικτύου

Στο φυσικό επίπεδο (L1) παρέχονται οι υπηρεσίες σαν ένα σετ καναλιών μεταφοράς του WCDMA. Έτσι, το φυσικό επίπεδο είναι υπεύθυνο για την πρώτη πολλαπλή λειτουργία: να τοποθετήσει τις ροές από τα κανάλια μεταφοράς σε φυσικά WCDMA κανάλια και αντίστροφα.

Το επίπεδο σύνδεσης (L2) κάνει μια σημαντική λειτουργία: δυναμικό διαμορισμό της ισχύς στο WCDMA interface. Αντίθετα από την μεγάλη ποικιλία των καναλιών μεταφοράς στο L1 από το επίπεδο επιτρέπει στο ανώτερο επίπεδο να βλέπει μόνο ένα σετ των radio bearers τα οποία μπορούν να μεταφερθούν μέσω του radio.

Το **Medium Access Control ημιεπίπεδο (MAC)** ελέγχει την χρήση της μεταφορόμενης ισχύς έχοντας διαβεβαιώσει τις αποφάσεις για την θέση της δυναμικότητας-ισχύς (που έχουν γίνει από την πλευρά του UTRAN) και εκτελούνται και στις δυο πλευρές του radio interface.

Το **Radio Link Control ημιεπίπεδο (RLC)** προσθέτει την λειτουργία του επιπέδου σύνδεσης πάνω στα λογικά κανάλια και προβάλλεται από το ημιεπίπεδο MAC.

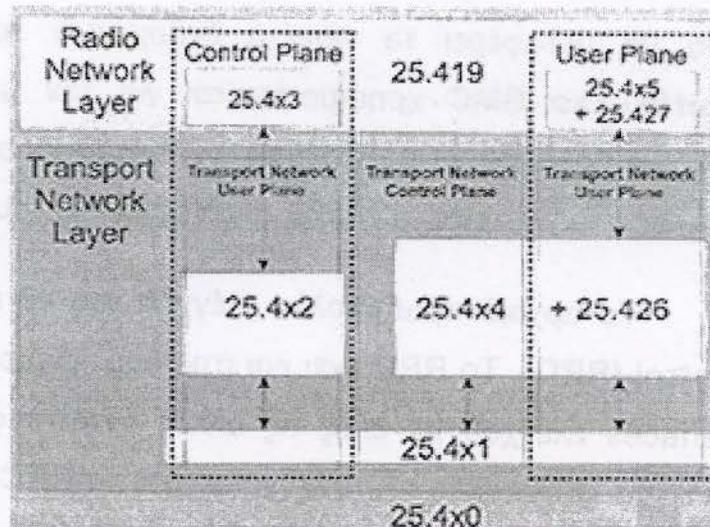
Για το επίπεδο L3 τα πρωτόκολλα ελέγχου (σηματοδοσίας) προϋποθέτουν την υπηρεσία RLX να είναι αρκετά διαθέσιμη. Για τα δεδομένα του CN domain (π.χ. κωδικοποιημένη ομιλία) η λειτουργία μετατροπής είναι μηδενική, αλλά για το PS domain χρειάζεται ένα επιπρόσθετο ημιεπίπεδο κάλυψης. Το **Packet Data Convergence Protocol (PDCP)** ημιεπίπεδο δημιουργεί το radio interface του UMTS

ικανό να μεταφέρει τα πακέτα δεδομένων του πρωτοκόλλου IP. Το **πρωτόκολλο BMC** χρησιμοποιείται για την μετάδοση δεδομένων και multicast domains. Ο σχεδιασμός και η παράδοση μηνυμάτων από κελιά-κυψέλες στα Ues είναι ο κύριος σκοπός αυτού του πρωτοκόλλου.

Το αρχικό πρωτόκολλο ελέγχου του L3 είναι το **Radio Resource Control (RRC)**. Το RRC έχει και στις δυο πλευρές (UE και UTRAN side) interfaces ελέγχου με όλες τις άλλες οντότητες πρωτοκόλλων. Παρόλα αυτά το πρωτόκολλο που ελέγχεται από το RRC τοποθετείται σε ένα άλλο UTRAN δίκτυο και υπάρχει ανάγκη να υποστηριχθεί ο μηχανισμός ελέγχου με τα υπάρχοντα standard πρωτόκολλα.

9.1.2 Μοντέλο αναφοράς των UTRAN Πρωτοκόλλων

Το δίκτυο πρόσβασης, το UTRAN, έχει την πλήρη ευθύνη των ραδιο πηγών του WCDMA. Το UTRAN μεταφέρει τις ραδιοπηγές διαχείρισης και ελέγχου διαμέσου των στοιχείων του δικτύου και δημιουργεί τους radio bearers πρόσβασης για να επιτρέπουν την επικοινωνία μεταξύ των UEs και του Ασύρματου Δικτύου (CN) μέσω ολόκληρου των infrastucture του UTRAN. Αυτή η επικοινωνία δομείται σύμφωνα με το γενικό πρωτόκολλο του UTRAN που παρουσιάζεται στην Εικόνα 97.



Εικόνα 97 Γενικό μονέλο UTRAN (Αναφερόμενοι στις προδιαγραφές της 3GPP: $x=1$ lu protocol; $x=2$ lur protocols; $x=3$ lub protocols)

Τα βασικά στοιχεία της δομής του πρωτοκόλλου του UTRAN είναι επίπεδα και planes. Η βασική αρχή των επιπέδων χρησιμοποιείται στο σχεδιασμό του UTRAN για να διαχωρίζει αρχικά μεταξύ των 2 βασικών κομματιών του protocol stack αντί να προχωρά μέσα σε εξατομικευμένα επίπεδα. Γι' αυτό όλα τα κατώτερα επίπεδα των πρωτοκόλλων συνθέτουν μαζί ένα σύνολο που καλείται επίπεδο μεταφοράς δικτύου του UTRAN. Ο όρος μεταφοράς χρησιμοποιείται με την έννοια του OSI μοντέλου, π.χ. να καλύπτει των σετ των πρωτοκόλλων που επιτρέπουν μη – adjacent κόμβους δικτύου για να επικοινωνούν κατά μήκος ενός συνδισμένου internetwork πολλών πιθανών διαφορετικών ειδών υποδικτύων. Μια άλλη πτυχή σχεδίασης είναι ότι το περιλαμβάνουν στο επίπεδο μεταφοράς δικτύου όλα εκείνα τα πρωτόκολλα, τα οποία επιλέγονται από τα υπάρχοντα πρωτόκολλα αντί να χρειαστεί να σχεδιαστούν ειδικά πρωτόκολλα ειδικά για τις περιπτώσεις UMTS.

Το άλλο σετ των πρωτοκόλλων στην κορυφή των επιπέδων μεταφοράς ονομάζεται επίπεδο ραδιοδικτύου. Αυτά τα πρωτόκολλα έχουν σχεδιαστεί προσεκτικά για το UMTS σύστημα και η χρήση τους είναι να

ελέγχουν την διαχείριση και χρήση των radio bearers πρόσβασης κατά μήκος των διαφόρων UTRAN interfaces.

9.1.3 Το Μοντέλο Αναφοράς Πρωτοκόλλων του CN

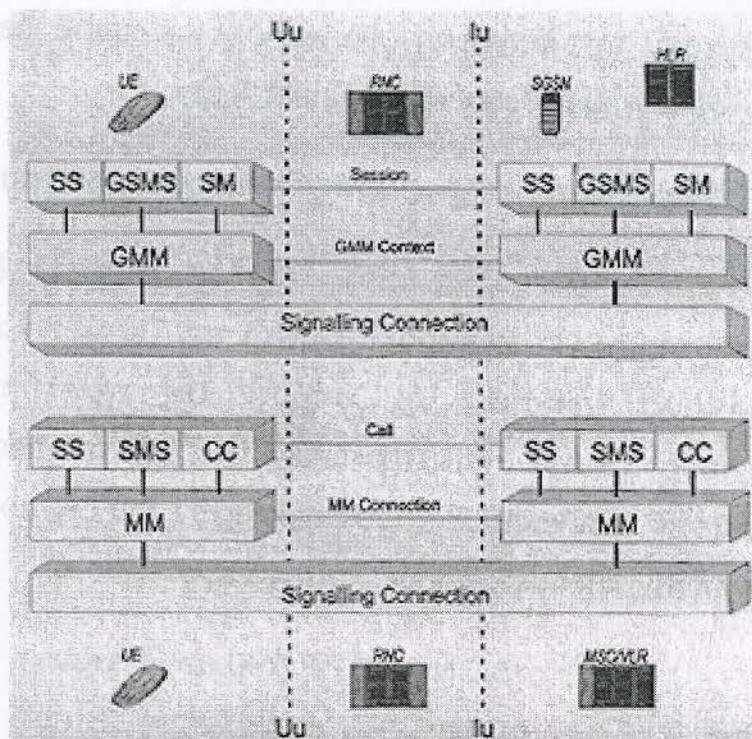
Το CN αποτελείται από τα στοιχεία δικτύου που παρέχουν υποστήριξη για τα χαρακτηριστικά του δικτύου και τις υπηρεσίες για τους τελικούς χρήστες. Η υποστήριξη που παρέχεται περιλαμβάνει λειτουργικότητα όπως την διαχείριση των πληροφοριών για την θέση του χρήστη, έλεγχος των χαρακτηριστικών του δικτύου και των υπηρεσιών και οι μηχανισμοί μεταφοράς για την σηματοδότηση.

Μέσα στο CN η 3GPP R99 αρχιτεκτονική πρωτοκόλλου διακρίνεται από αυτή του GSM/GPRS συστήματος. Έτσι 5 κύρια σει πρωτοκόλλων μπορούν να διακριθούν:

- Πρωτόκολλα μη πρόσβασης μεταξύ των UEs και του CN
- Πρωτόκολλα ελέγχου σηματοδότησης δικτύου μεταξύ του δικτύου-βάσης και του δικτύου που εξυπηρετεί
- Πρωτόκολλα βασικού δικτύου δεδομένων πακέτων
- Πρωτόκολλα ελέγχου transit του δικτύου
- Πρωτόκολλα ελέγχου υπηρεσιών

Το UMTS CN τερματίζει τα πρωτόκολλα μη πρόσβασης από τα UEs. Πέρα από αυτά το GSM/GPRS background είναι πολύ αποδεκτό. Αυτό αντανakλάται από τις προδιαγραφές της 3GPP TS 24008, οι οποίες είναι μια version του διάσημου “ancestor” GSM 04.8.

Τα πρωτόκολλα μη πρόσβασης εμφανίζονται στην Εικόνα 62



Εικόνα 98 Τα πρωτόκολλα μη προσπέλασης του UMTS

- **Session Management (SM) πρωτόκολλο:** περιλαμβάνει την εγκατάσταση και απελευθερώνει την session μεταφορά πακέτων δεδομένων ή τα περιοχόμενα του Packet Data Protocol (PDP) στο CN domain.
- **Call Control (CC) πρωτόκολλο:** ελέγχει την εγκατάσταση και την απελευθέρωση των κλήσεων μεταγωγής κυκλώματος στο CN CS domain.
- **Supplementary Service (SS) πρωτόκολλο:** ελέγχει την ενεργοποίηση και απενεργοποίηση των διαφόρων υποστηριζόμενων υπηρεσιών που σχετίζονται με τις κλήσεις ή όχι.
- **Short message Service (GSM/SMS) πρωτόκολλο:** ελέγχει την παράδοση των μικρών μηνυμάτων από και προς στα UEs.

Η σηματοδότηση ελέγχου του δικτύου μεταξύ του βασικού δικτύου και το δίκτυο που εξυπηρετεί, χρησιμοποιεί τις υπηρεσίες στη μεταγωγή κυκλώματος. Με την γνωριμία των υπηρεσιών πακέτων με το υποσύστημα GPRS έγινε αναγκαίο να εξαπλωθεί το πρωτόκολλο MAP στα interfaces μεταξύ των GPRS κόμβων υποστήριξης και των κόμβων του δικτύου – βάσης. Από την πλευρά του 3G CN interface τα ακόλουθα ελεγχονται από της Τρίτης Γενιάς το πρωτόκολλο MAP:

- Interfaces C,D, E, F και G, τα οποία αρχικοποιούνται από το GSM σύστημα
- Interfaces Gc, Gr, Gf και Gs, τα οποία αρχικοποιούνται από το GPRS σύστημα.

Αυτό σημαίνει ότι φυσιολογικά και το SGSN και το GGSN πρέπει να είναι εξοπλισμένα με την εφαρμογή του πρωτοκόλλου MAP για λόγους ελέγχου.

9.2 Αρχιτεκτονική των εσωτερικών πρωτοκόλλων του UMTS

Τα UTRAN και τα CN πρωτόκολλα, έχουν γίνει γνωστά με 2 κύριες πτυχές πρωτοκόλλων:

- Διαχωρισμός των πτυχών γενικής μεταφοράς από τις UMTS ειδικευμένες πτυχές των κινητών τηλεπικοινωνιών δικτύων χρησιμοποιώντας την επιπεδοποίηση.
- Διαχωρισμός των πτυχών ελέγχου του δικτύου από τα δεδομένα των χρηστών με planes.

Τα **δύο βασικά σχέδια πρωτοκόλλων** στην παγκόσμια αρχιτεκτονική πρωτοκόλλων είναι:

- Τα εσωτερικής λειτουργίας πρωτόκολλα

- Τα πρωτόκολλα τερματισμού

Τα **πρωτόκολλα εσωτερικής λειτουργίας** έχουν να κάνουν με τα πρωτόκολλα, τα οποία ανήκουν στο ίδιο επίπεδο αλλά εξαπλώνονται κατά μήκος των στοιχείων των πολύπλοκων δικτύων και γι' αυτό συνθέτουν ένα σετ από πρωτόκολλα, τα οποία χρησιμοποιούνται για την εκτέλεση μιας κοινής λειτουργίας παγκόσμιου συστήματος. Σαν παραδείγματα τέτοιων λειτουργιών μπορεί κάποιος να θεωρήσει την εγκατάσταση των bearer πρόσβασης ή την αναβάθμιση της τοποθεσίας του χρήστη. Το πρώτο απαιτεί εσωτερική εργασία από το Ue στο CN στοιχείο και συνδιάζει τις λειτουργίες από το RRC πρωτόκολλο και τα AP πρωτόκολλα μέσα στην UTRAN. Για την αναβάθμιση της τοποθεσίας, η αλυσίδα των πρωτοκόλλων εσωτερικής λειτουργίας αποτελείται από το πρωτόκολλο MM (μεταξύ του UE και του CN) και το MAP πρωτόκολλο μεταξύ των CN κόμβων. Μια τέτοια αλυσίδα καλείται ως μια διαδικασία συστημάτων σύμφωνα με τους σχεδιαστές των πρωτοκόλλων.

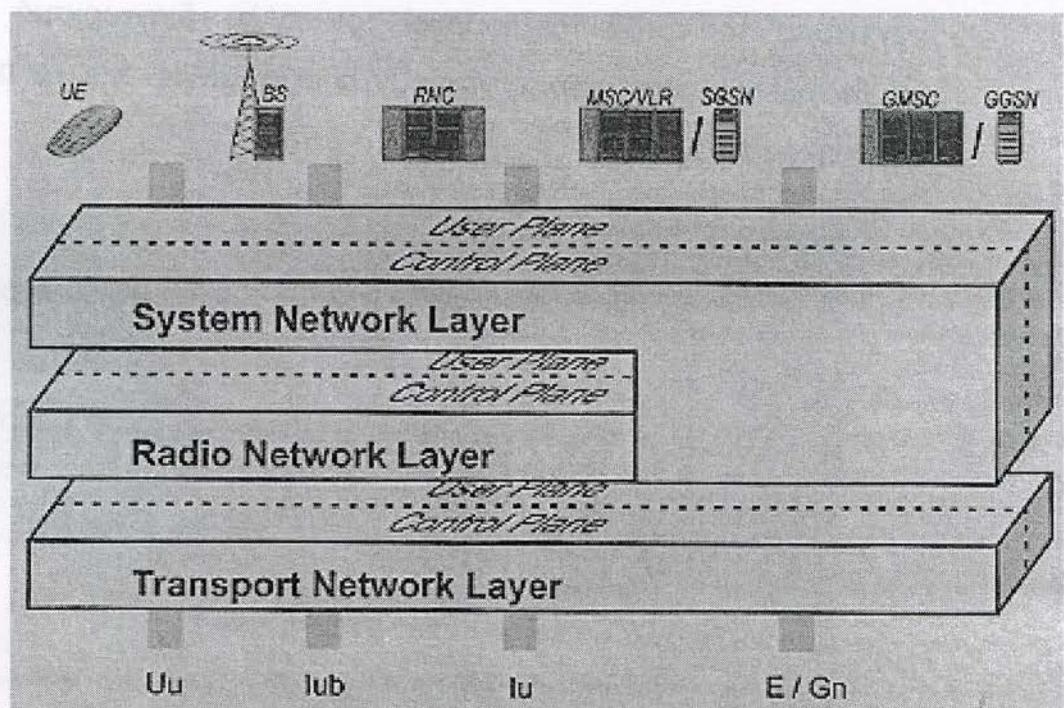
Τα **πρωτόκολλα τερματισμού** μπορεί να θεωρηθούν σαν το τέλος μιας αλυσίδας πρωτοκόλλων τα οποία εργάζονται εσωτερικά με τον τρόπο που περιγράφηκε πιο πάνω. Μέσα σε ένα στοιχείο του δικτύου, όπου ένα πρωτόκολλο τερματίζει, μια λειτουργία του συστήματος ή ένας αλγόριθμος μπορεί να αναγνωριστεί σαν την πηγή των δεδομένων ή των διαταγών. Για τα πρωτόκολλα MM που περιγράφηκαν πιο πάνω, στο παράδειγμα αναβάθμισης της τοποθεσίας, σημεία τερματισμού είναι το UE και το HLR. Ο τερματισμός συζητείται μερικές φορές με σεβασμό σε ένα μόνο πρωτόκολλο, αλλά μετά τα σημεία τερματισμού είναι απλά τα δυο άκρα του peer-to-peer πρωτοκόλλου. Γι' αυτό από την πλευρά της αρχιτεκτονικής του παγκόσμιου συστήματος πρωτοκόλλων, ο τερματισμός ενός σετ εσωτερικών πρωτοκόλλων είναι πιο σημαντικός.

Το UMTS πρωτόκολλο μπορεί να διαχωριστεί – σε οριζόντιο διαχωρισμό- σε δυο επίπεδα. Τα πρωτόκολλα μέσα σε κάθε επίπεδο

λειτουργούν κατά μήκος πολλαπλών interfaces και ανήκουν μαζί στα πρωτόκολλα εσωτερικής λειτουργίας.

Τρία επίπεδα μπορούν να διαχωριστούν όπως φαίνονται στην εικόνα 99.

- Επίπεδο μεταφοράς δικτύου
- Επίπεδο ραδιο δικτύου
- Επίπεδο συστήματος δικτύου

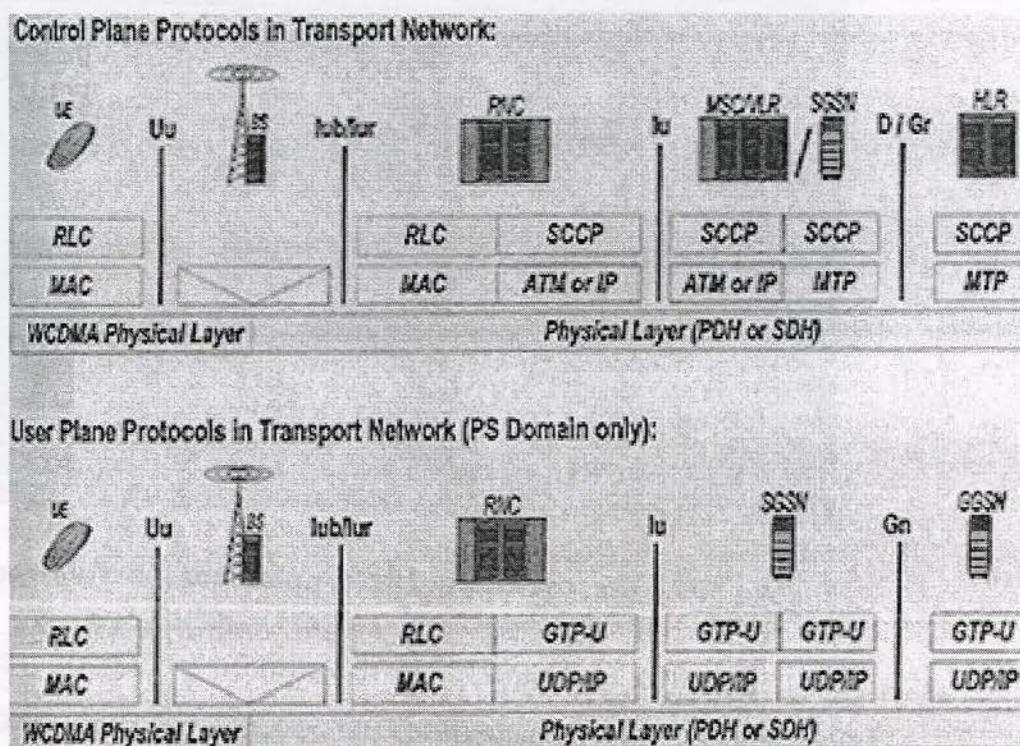


Εικόνα 99 Αρχιτεκτονική των UMTS πρωτοκόλλων εσωτερικής λειτουργίας

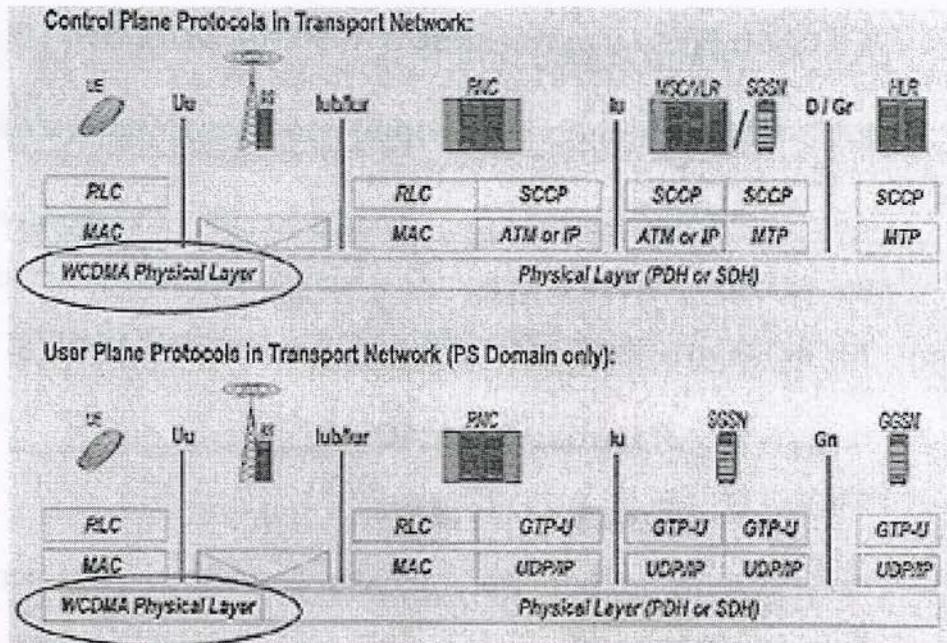
Σε αυτό το διαχωρισμό το επίπεδο μεταφοράς είναι υπεύθυνο για την παροχή μιας υπηρεσίας μεταφοράς γενικού σκοπού για όλα τα στοιχεία του UMTS δικτύου έτσι ώστε να το κάνουν ικανό να επικοινωνήσουν κατά μήκος όλων των interfaces που περιγράφηκαν πιο πάνω. Η λειτουργικότητα του UMTS δικτύου διαχωρίζεται κατά μήκος των στοιχείων του δικτύου χρησιμοποιώντας τα πρωτόκολλα μέσα στα επίπεδα

δικτύου και συστήματος, τα οποία εξ ορισμού είναι ιδιαίτερα στο UMTS. Τα πρωτόκολλα του επιπέδου δικτύου κάνουν σίγουρη την εσωτερική λειτουργία μεταξύ του UEs και του CN πάνω σε όλους τους radio bearers πρόσβασης. Τα πρωτόκολλα που χρησιμοποιούνται στο επίπεδο συστήματος εξαπλώνονται από το UE μέχρι την άκρη transit του δικτύου του UMTS CN. Αυτά κάνουν σίγουρη την εσωτερική λειτουργία στις υπηρεσίες επικοινωνίας του UMTS.

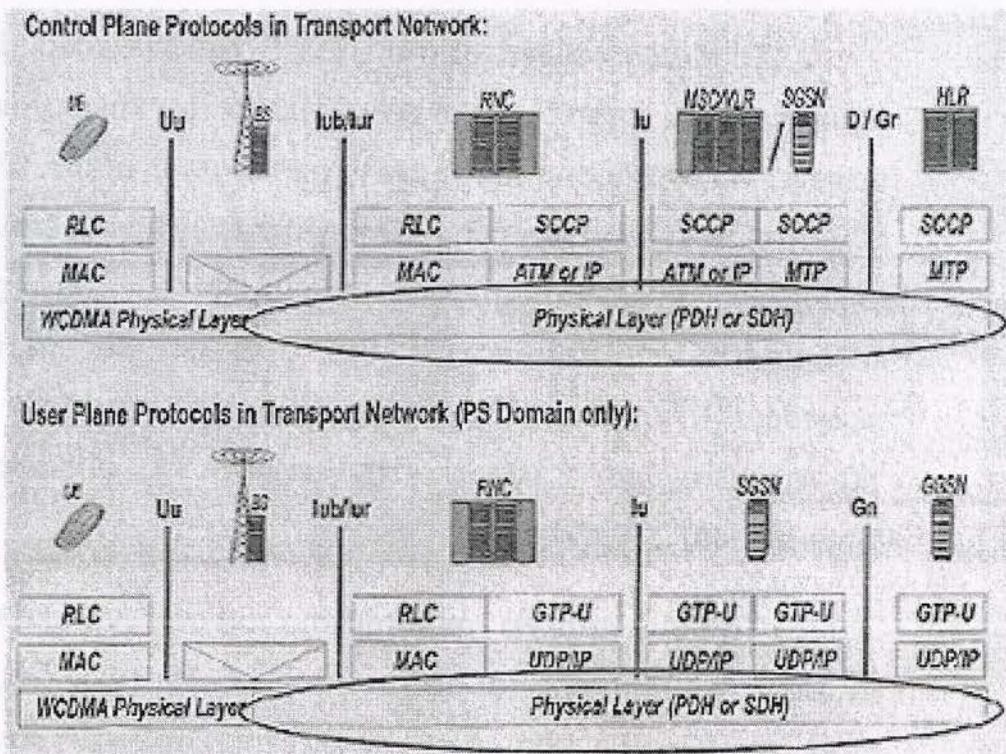
Μέσα σε αυτά τα επίπεδα μπορεί να γίνεται διαχωρισμός μεταξύ των πτυχών ελέγχου και των πτυχών μεταφοράς των δεδομένων των χρηστών, το οποίο δημιουργεί τον άλλο διαχωρισμό του μοντέλου πρωτοκόλλων που χρησιμοποιούνται στο UMTS και τα οποία φαίνονται στην εικόνα 100.



Εικόνα 100 Τα πρωτόκολλα δικτύου μεταφοράς στο 3GPP R99



Εικόνα 101 Το φυσικό επίπεδο στο Uu interface



Εικόνα 102 Το φυσικό επίπεδο σε άλλα interfaces

9.3 Πρωτόκολλα μεταφοράς στο δίκτυο μέσα στο Uu Interface

9.3.3.1 Πρωτόκολλα μεταφοράς στο δίκτυο μέσα στο Uu Interface

Τα πρωτόκολλα μεταφοράς τα οποία ελέγχουν την σηματοδοσία και τα δεδομένα των χρηστών – και για την μεταγωγή κυκλώματος και για την μεταγωγή πακέτων – μέσα στο Uu interface είναι:

- **Πρωτόκολλο MAC**
- **Πρωτόκολλο RNC**

Αυτά τα δυο πρωτόκολλα δουλεύουν μαζί σαν ραδιοένωση του δικτύου μεταφοράς.

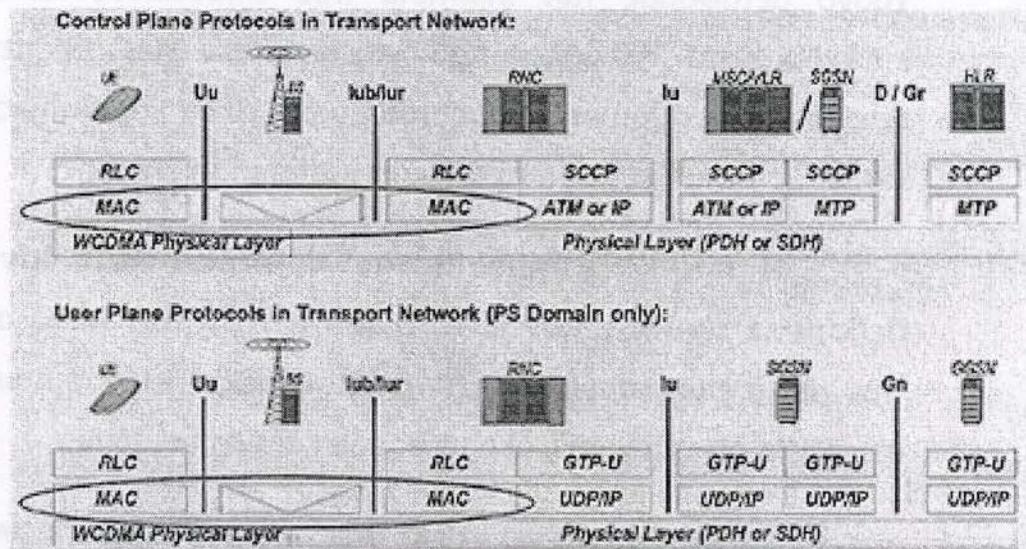
9.3.1. Πρωτόκολλο Ελέγχου Μέσης Πρόσβασης (MAC)

Το MAC είναι ενεργό στα UE, BS, RNC (Εικόνα 103). Το MAC είναι πρωτόκολλο 2 επιπέδων και σαν κομμάτι του κοινου δικτύου μεταφοράς παρέχει και στα δύο επίπεδα **ελέγχου** και **user plane**. Στο σχεδιασμό του MAC πρωτοκόλλου και στην κίνηση μεταγωγής πακέτου και στην κίνηση μεταγωγής κυκλώματος, σαν σηματοδοσία κίνησης έχει μπει σε λογαριασμό από την αρχή. Αυτή είναι μια βασική διαφορά από τα πρωτόκολλα πακέτων 2^{ης} γεννιάς, τα οποία μπορεί να θεωρηθούν μόνο για την μεταγωγή πακέτων στην κορυφή του φυσιολογικού μεταφορέα (time-slotted) 2^{ης} γεννιάς.

Το MAC παρέχει την υπηρεσία του σαν ένα σετ λογικών καναλιών, τα οποία χαρακτηρίζονται από τον τύπο δεδομένων που μεταφέρονται σε αυτά. Υπάρχουν 4 είδη καναλιών ελέγχου και 2 είδη καναλιών μεταφοράς κατά μήκος των λογικών καναλιών.

Το MAC έχει την υπευθυνότητα του ελέγχου των επικοινωνιών πάνω στα WCDMA κανάλια μεταφοράς που παρέχονται από το φυσικό επίπεδο. Με σκοπό να είναι ικανό να μοιραστεί την ισχύ των καναλιών

μεταφοράς κατά μήκος του σετ των χρηστών, το MAC χρησιμοποιεί blocks μεταφοράς σαν μονάδα μεταφοράς. Το πιθανό μέγεθος των blocks για κάθε κανάλι μεταφοράς προσφέρεται στο MAC από το φυσικό επίπεδο του WCDMA σαν ένα κομμάτι του σετ των καθορισμών της μεταφοράς.



Εικόνα 103 Δίκτυο μεταφοράς – Μέσης πρόσβασης έλεγχος

Το MAC πρωτόκολλο είναι ικανό να περιπλέκει τα PDM από τα υψηλότερα επίπεδα σε σετ blocks μεταφοράς που μεταφέρονται μέσω κοινών καναλιών μεταφοράς. Η αναγνώριση των Ues σε κοινά κανάλια μεταφοράς γίνεται με προσωρινή ταυτότητα (τοποθετημένη στο RNC) που μπορεί να είναι είτε Cell-Radio Network Temporary Identity (C-RNTI, 16bits) ή UTRAN Radio Network Temporary Identity (U-RNTI, 32bits).

Στα αφοσιωμένα κανάλια μεταφοράς το MAC είναι ικανό να πολυπλέκει κανοντας ένωση στα στα σετς blocks από το υψηλότερο επίπεδο PDUs. Σε αυτήν την περίπτωση όλα τα blocks στο σετ πρέπει να ανήκουν σε ένα μόνο UE για το οποίο το κανάλι μεταφοράς είναι αφοσιωμένο και η δημιουργία πολυπλεξίας είναι πιθανή μόνο αν οι

παράμετροι QoS είναι ιδανικό για τις υπηρεσίες που υποστηρίζονται από το αφοσιωμένο κανάλι.

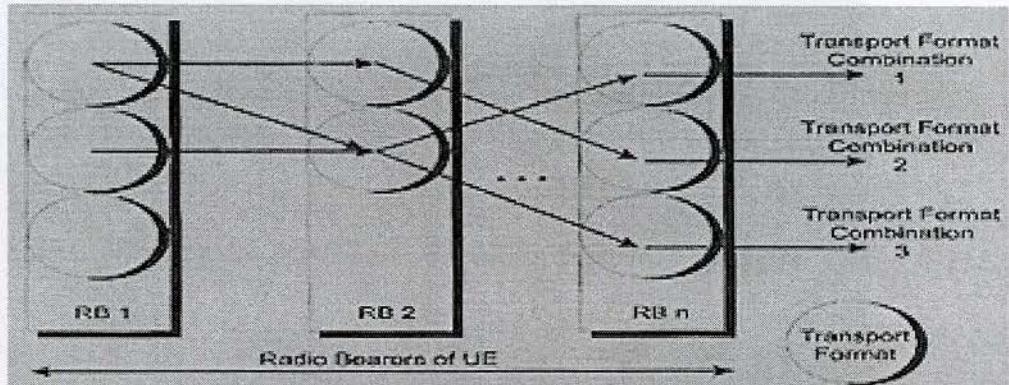
Το MAC είναι ένα πρωτόκολλο πραγματικού χρόνου. Πρέπει να "συναντήσει" τις απαιτήσεις χρόνου φυσικού επιπέδου. Το MAC πρέπει να είναι έτοιμο να στείλει ένα νέο σετ μεταφερόμενων blocks σύμφωνα με τον χρόνο μεταφοράς των internets που υποδεικνύονται από το φυσικό επίπεδο. Κατά τη διάρκεια που ένα εσωτερικό MAC πρέπει να επιλέξει τον αρχικό σχεδιασμό μεταφοράς που βασίζεται σε χαρακτηριστικά δεδομένων για να μεταφερθούν στη πρόσφατη κατάσταση κίνησης.

Η βασική υπηρεσία του επιπέδου MAC είναι να παρέχει δεδομένα κίνησης των MAC SDUs μεταξύ των MAC οντοτήτων. Από την μεριά των ανωτέρων επιπέδων αξίζει να σημειωθεί ότι αυτή η υπηρεσία δίνεται χωρίς acknowledges και segmentation.

Το MAC συλλέγει στατιστικές πληροφορίες σχετικά με την κίνηση που χρησιμοποιείται από το επίπεδο RRC. Αυτές οι πληροφορίες MAC περιλαμβάνουν τοπικές μετρήσεις όπως buffer occupancy, variance και coverage. Επίσης δείχνει την underflow και overflow που ανιχνεύονται σε κάθε κανάλι μεταφοράς.

Το επίπεδο MAC προσφέρει έναν αλγόριθμο ciphering του κόμβου μεταφοράς RLC. Οι MAC SDUs στέλνουν στα αφιερωμένα λογικά κανάλια DCCH και DTCH τον αλγόριθμο αυτόν με ένα ειδικό κλειδί για το UE χρησιμοποιώντας τον block cipher αλγόριθμο KASUMI.

Το MAC έχει μόνο ένα PDU που ονομάζεται data-PDU, και αποτελείται από ένα MAC SDU και μια επικεφαλίδα πρωτοκόλλου MAC. Η επικεφαλίδα είναι φτιαγμένη σύμφωνα με το κανάλι που χρησιμοποιείται. Σε ορισμένες περιπτώσεις, π.χ., όταν το UE έχει μόνο ένα αφιερωμένο κανάλι, η επικεφαλίδα MAC μπορεί να απουσιάζει.

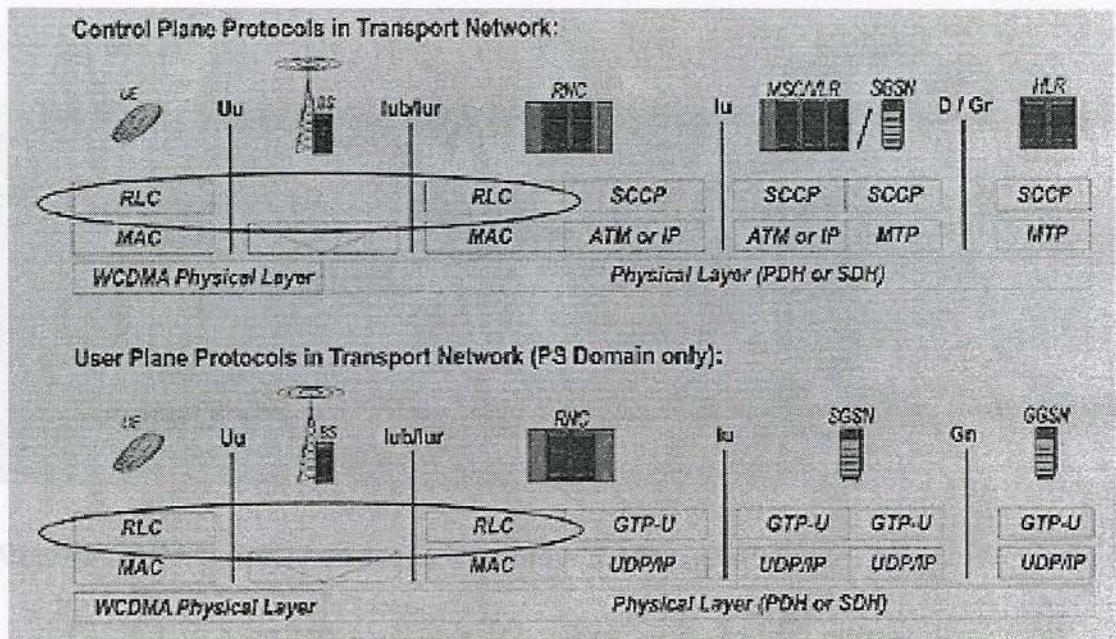


Εικόνα 104 Συνδιασμοί μεταφοράς στο MAC πρωτόκολλο

9.3.2. Πρωτόκολλο ελέγχου Δικτύου (RLC)

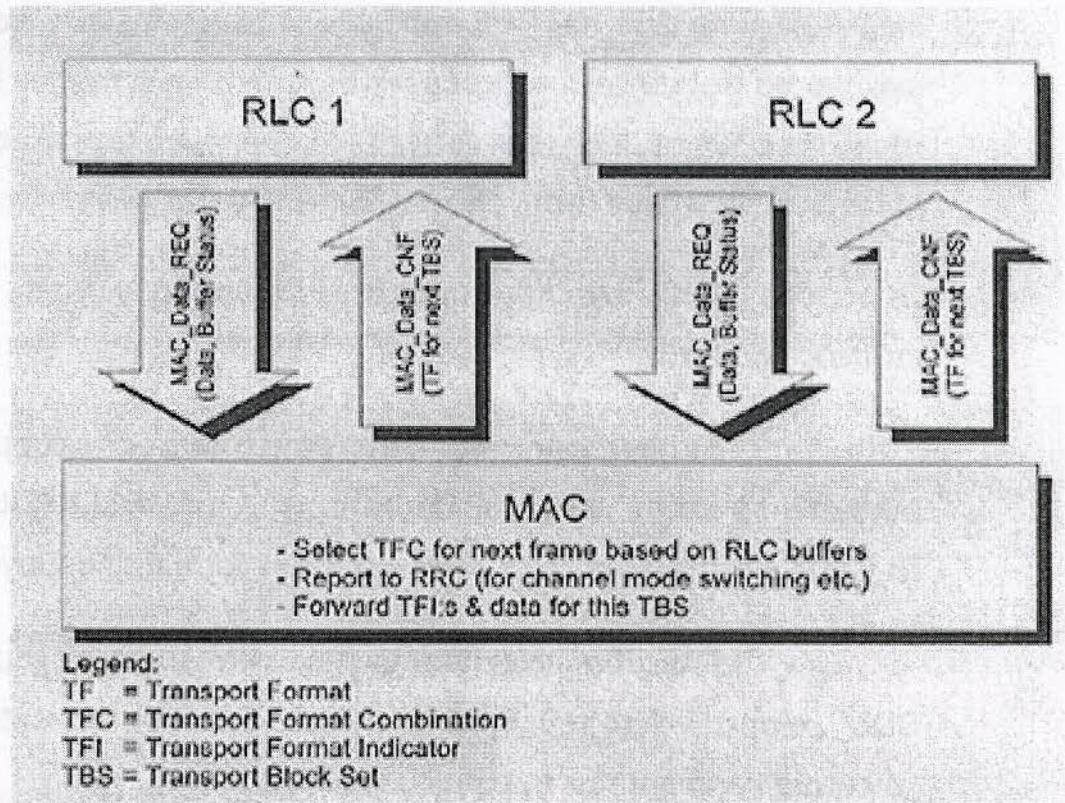
Το RLC πρωτόκολλο τρέχει και στο RNC και στο UE και εφαρμόζει την λειτουργία του κανονικού επιπέδου δικτύου στο WCDMA interface (Εικόνα 105). Το RLC είναι ενεργό και στο plane ελέγχου και στο plane χρήστη και παρέχει υπηρεσίες δικτύου και για συνδέσεις μεταγωγής κυκλώματος και για συνδέσεις μεταγωγής πακέτων.

Το λειτουργικό περιβάλλον του RLC εξαρτάται στο σχεδιασμό που έχει συζητηθεί. Στην περίπτωση του user plane το RLC χρησιμοποιείται από το PDCP πρωτόκολλο και στην περίπτωση του control plane το RLC χρησιμοποιείται από το RRC πρωτόκολλο. Το χαμηλότερο επίπεδο πρωτοκόλλου για το RLC είναι το MAC, το οποίο παρέχει υπηρεσίες μεταφοράς δεδομένων όπως το MAC SDUs μέσω λογικών καναλιών.



Εικόνα 105 Μεταφορά δικτύου – έλεγχος ραδιοένωσης

Επειδή ο κόμβος μεταφοράς δεδομένων MAC είναι άγνωστος, το RLC γίνεται υπεύθυνο για την παράδοση των υψηλότερων επιπέδων PDUs, των οποίων η αξιοπιστία είναι απαραίτητη. Επίσης, το επίπεδο MAC δεν είναι ικανό να ενώσει μεγαλύτερα SDUs σύμφωνα με τα format μεταφοράς που είναι διαθέσιμα, το RLC αναλαμβάνει τέτοια λειτουργία. Έτσι, τα formats μεταφοράς είναι ορατά στο RLC επίπεδο όπως φαίνεται στην εικόνα 106.



Εικόνα 106 Εσωτερική οργάνωση του RLC με τη βοήθεια του MAC στα αφοσιωμένα κανάλια

Το RLC παρέχει τις υπηρεσίες μεταφοράς δεδομένων υψηλότερων επιπέδων PDUs όπως RLC SDUs. Αυτή η υπηρεσία καλείται υπηρεσία radio bearer. Τρεις κόμβοι της λειτουργίας έχουν καθοριστεί για το RLC: **transparent (Tr)**, **unacknowledged (UM)** και **acknowledged (AM)**.

Στον **διαφανή κόμβο (transparent mode)** το RLC μεταφέρει SDUs χωρίς να προσθέτει οποιαδήποτε πληροφορία πρωτοκόλλου. Αυτός ο κόμβος χρησιμοποιείται, π.χ. για streaming υπηρεσιών. Στον **κόμβο μη αναγνωρισιμότητας (unacknowledged mode)** το RLC μεταφέρει SDUs χωρίς να εγγυάται την παράδοση στην peer οντότητα. Αυτός ο κόμβος χρησιμοποιείται από κάποιες RRC εφαρμογές, όπου η αναγνωρισιμότητα ελέγχεται από το RRC πρωτόκολλο. Στον **κόμβο αναγνωρισιμότητας (acknowledged mode)** το RLC μεταφέρει SDUs και εγγυάται την παράδοση στις peer οντότητες του. Η εγγυημένη παράδοση

διαβεβαιώνεται από την επαναμεταφορά. Σε περίπτωση που το RLC είναι ανίκανο να παραδώσει τα δεδομένα σωστά, ο χρήστης του RLC στο μέρος της μεταφοράς σημειώνεται. Αυτός ο κόμβος χρησιμοποιείται για μεταφορά μεταγωγής πακέτων μέσω αφιερωμένων λογικών καναλιών.

Το RNC έχει πολυάριθμες λειτουργίες για να παράγουν στο επίπεδο του όπως:

- **Διαχωρισμός και Επανασχεδιασμός:** εφαρμογή των PDUs υψηλότερου επιπέδου μεταβλητών προς / από RLC PDUs. Το μέγεθος RLC PDU εφαρμόζεται στο φυσικό σετ των format εφαρμογών.
- **Αλυσίδα:** χρησιμοποιείται όταν τα περιεχόμενα ενός RLC SDU μπορεί να τοποθετηθεί στο RLC PDU σε concatenation με την τελευταία segment του τελευταίου RLC SDU.
- **Γέμισμα από κάποιο υλικό:** Όταν το γέμισμα από κάποιο υλικό δεν εφαρμόζεται και τα δεδομένα που παραμένουν για να μεταφερθούν δεν ολοκληρώνει ένα ολόκληρο RLC PDU δοσμένου μεγέθους, τα εναπομείναντα πεδία δεδομένων πρέπει να γεμιστούν με padding bits. Το μπορεί να αντικατασταθεί από την κρατούμενη κατάσταση πληροφοριών για την αντίθετη σύνδεση.
- **Διόρθωση Λαθών:** Πολλές λειτουργίες του RLC έχουν να κάνουν με την ανίχνευση και την διόρθωση λαθών. Τα bits λαθών μπορούν στην πραγματικότητα να ανιχνευθούν από τον έλεγχο του φυσικού επιπέδου CRC, αλλά το RLC επίπεδο είναι υπεύθυνο για την ανάκαμψη από τα λάθη. Η πιο αποδοτική ανάκαμψη λαθών παρέχεται από την μεταφορά στα αναγνωρισμένα δεδομένα του κόμβου μεταφοράς.
- **Μεταφορά των SDUs στην εσωτερική ακολουθία:** Το RLC πρωτόκολλο μπορεί να είναι σχεδιασμένο από το RRC για να υπακούει σε

διαφορετικά σχήματα επαναμεταφοράς, π.χ. Επιλεγόμενη Επανάληψη, Πηγαίνε Πίσω N και Stop και Wait.

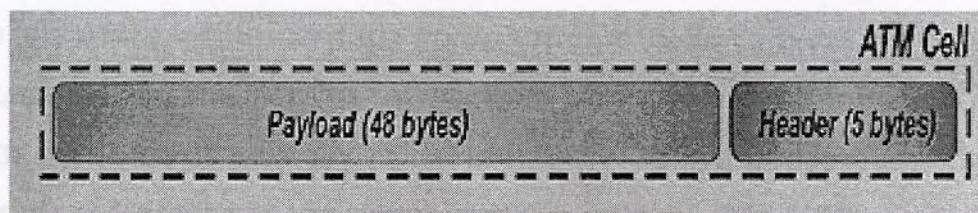
- **Διπλή ανίχνευση:** Το RLC είναι ικανό να ανιχνεύσει τα διπλότυπα των λαμβανόμενων RLC PDUs και μπορεί να επιβεβαιώσει ότι το resultant υψηλότερο επίπεδο PDU παραδίδεται μόνο μια φορά στο ανώτερο επίπεδο.
- **Έλεγχος ροής:** Επιτρέπει έναν RLC αποδοχέα να ελέγξει το ρυθμό κατά τον οποίο η peer RLC οντότητα μπορεί να στείλει πληροφορίες.
- **Ακολουθία ελέγχου αριθμών:** Μπορεί να χρησιμοποιηθεί στον κόμβο μη αναγνωρισιμότητας για να εγγραφεί την integrity των reassembled PDUs. Παρέχει έναν μηχανισμό για την ανίχνευση των λανθασμένων RLC SDUs μέσω του ελέγχου του αριθμού ακολουθίας στο RLC PDUs όταν αυτοί (οι SDUs) μοιάζουν μέσα στο RLC SDU. Ένα λανθασμένο RLC PDU θα απορριφθεί.
- **Ανίχνευση λάθους πρωτοκόλλου και διόρθωση του:** Ο έλεγχος λαθών πρωτοκόλλου και η λειτουργικότητα της ανάκαμψης ψάχνει και καλύπτει για τα λάθη στην λειτουργία του RLC πρωτοκόλλου. Η reset procedure RLC χρησιμοποιείται για να επανακάμψει από μια κατάσταση λάθους. Σε περίπτωση που υπάρχει λάθος που δεν μπορεί να διορθωθεί η RLC οντότητα “τονίζει” το RRC επίπεδο.
- **Λειτουργία Αποβολής / Επανάληψης:** Με το RLC μπορεί να αποβληθεί και να επαναληφθεί η μεταφορά δεδομένων κάτω από την αίτηση από το RRC.
- **Απόρριψη της SDU:** Η λειτουργία αυτή επιτρέπει την απόρριψη του εναπομείνοντος RLC PDUs αυτού του SDU από το buffer ον της πλευράς του μεταφορέα, όταν η μεταφορά ενός RLC PDU δεν

επιτυγχάνει για πολύ καιρό. Αυτή η λειτουργία επιτρέπει το buffer overflow. Υπάρχουν πολλοί εναλλακτικοί κόμβοι της λειτουργίας απόρριψης του RLC SDU.

- **Chiphering:** Η λειτουργία αυτή εκτελείται στο επίπεδο RLC για εκείνους τους radio bearers που είναι σε κόμβο unacknowledged (μη αναγνωρισιμότητας) ή ackknnowledged (αναγνωρισιμότητας). Η chiphering γίνεται μέσα σε ένα ειδικό κλειδί του UE χρησιμοποιώντας τον αλγόριθμο blockchipher KASUMI.

9.3.3. Πρωτόκολλο Μεταφοράς ATM

Η βασική ιδέα στο ATM είναι να διαχωρίζει την ροή πληροφοριών που μπορεί να μεταφέρεται σε μικρά κομμάτια (πακέτα), να βάζει tags (επικεφαλίδες) διευθύνσεων σε εκείνα τα πακέτα και στην συνέχεια να μεταφέρει τα πακέτα μέσω φυσικών μονοπατιών μεταφοράς. Η άκρη που λαμβάνει, συλλέγει τα λαμβανόμενα πακέτα και τις αρχικές πληροφορίες ροής από τα συστατικά των πακέτων. Οι πληροφορίες μεταφοράς περιλαμβάνονται στο πακέτο και το πακέτο αυτό ονομάζεται ATM cell.



Εικόνα 107 Δομή του ATM cell

Η επικεφαλίδα ενός ATM cell περιλαμβάνει μερικές πληροφορίες διεύθυνσης όπως φαίνονται στην εικόνα 69. Τα πιο σημαντικά θέματα είναι:

- **VPI (Virtual Path Identifier):** αυτός που αναγνωρίζει ένα Virtual Path (VP), ή περισσότερο γενικά, ένας αναγνωριστής για μια πρόσφατη εγκατεστημένη ημιμόνιμη σύνδεση.

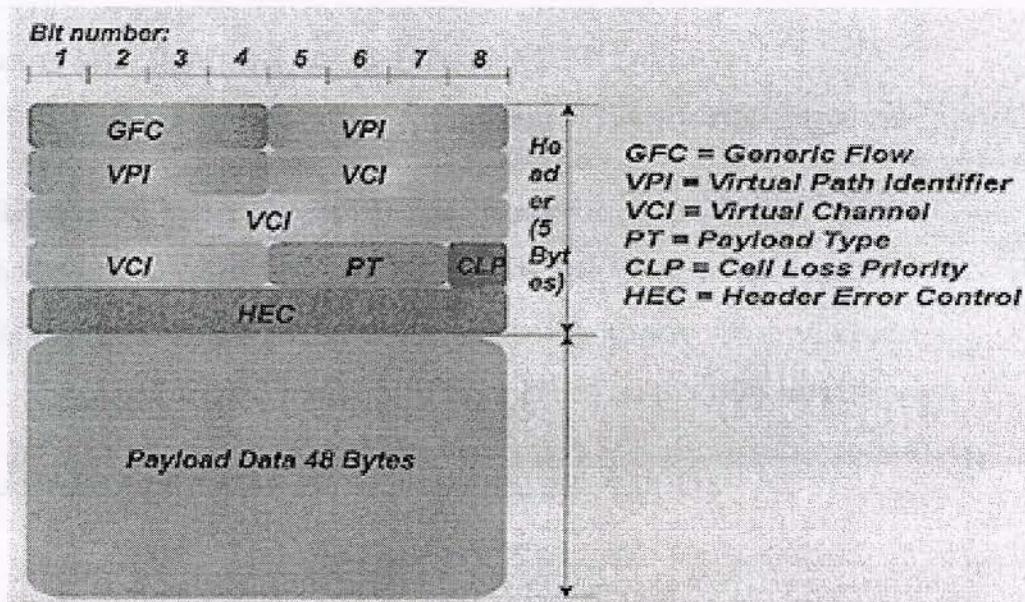
- **VCI (Virtual Channel Identifier):** ένας αναγνωριστής για ένα Virtual Circuit (VC). Αυτό το πεδίο είναι μεγάλο επειδή μπορεί να υπάρχουν χιλιάδες από κανάλια για να αναγνωριστούν μέσα σε ένα VP. Για παράδειγμα, εφαρμογές multimedia μπορεί να απαιτούν πολλά VCIs, ένα VC για κάθε συστατικό multimedia.
- **PT (Payload Type):** αυτό δείχνει αν το πεδίο πληρωμής των 48 bytes μεταφέρει δεδομένα χρηστών ή δεδομένα ελέγχου.
- **CLP (Cell Loss Priority):** αυτό είναι μια σημαία που δείχνει αν το ATM Cell είναι σημαντικό ή λιγότερο σημαντικό. Αν CLP=1 (χαμηλή προτεραιότητα / λιγότερο σημαντικό) το σύστημα μπορεί να χάσει αυτό το ATM cell αν χρειαστεί.
- **HEC (Header Error Control):** στο πρωτόκολλο ATM, η επικεφαλίδα του ATM cell προστατεύεται από λάθη.
- **Reason:** μια αποτυχία στην επικεφαλίδα του ATM cell μπορεί να παραδοθεί σε λάθος διεύθυνση, για παράδειγμα η διόρθωση λαθών που χρησιμοποιείται είναι ικανή να ανιχνεύει όλα τα λάθη στην επικεφαλίδα και μια αποτυχία μπορεί να διορθωθεί.

Οι κλάσεις υπηρεσιών του ATM πρωτοκόλλου είναι:

- Constant Bit Rate Υπηρεσίες (CBR)
- Unspecified Bit Rate Υπηρεσίες (UBR)
- Available Bit Rate Υπηρεσίες (ABR)
- Variable Bit Rate Υπηρεσίες (VBR)

Τα επίπεδα εφαρμογής για το ATM είναι τα ακόλουθα:

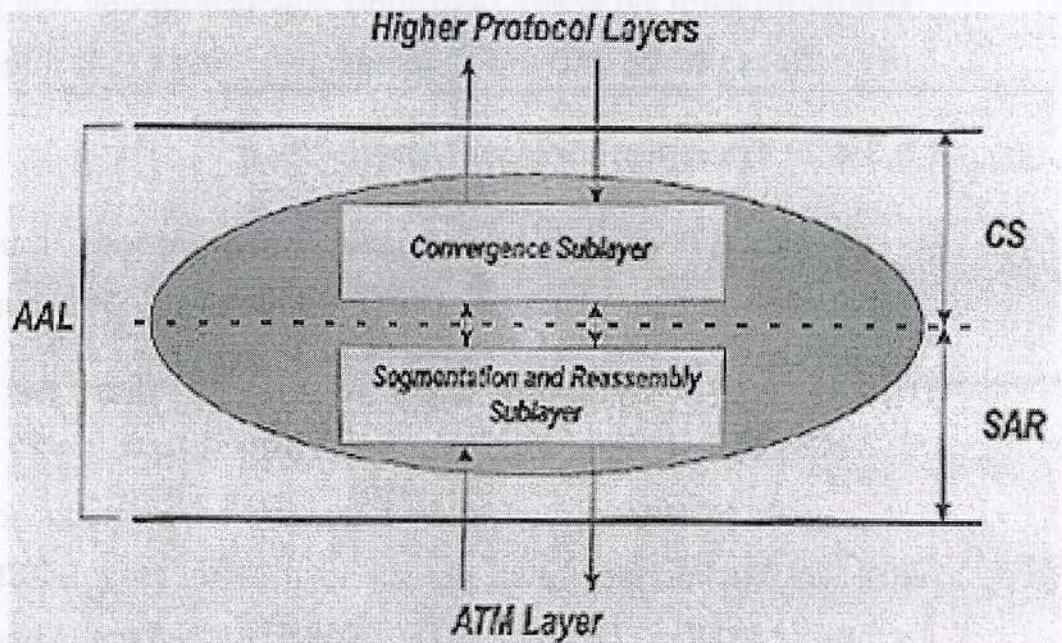
- **AAL1:** προσφέρει σύγχρονους κόμβους, σύνδεση περιορισμένης σύνδεσης και constant bit rate για υπηρεσίες που απαιτούν τέτοια είδους εφαρμογή
- **AAL2:** προσφέρει σύγχρονους κόμβους, σύνδεση περιορισμένης σύνδεσης με μεταβλητό bit rate για υπηρεσίες που χρησιμοποιούν αυτήν την εφαρμογή
- **AAL3/4:** προσφέρει connectionless και ασύγχρονη σύνδεση με μεταβλητό bit rate
- **AAL5:** προσφέρει ασύγχρονους κόμβους, σύνδεση περιορισμένης σύνδεσης με μεταβλητό bit rate



Εικόνα 108 Η δομή των επικεφαλίδων των ATM κυψελών

Στην Εικόνα 109, το AAL χωρίζεται σε δύο ημιεπίπεδα, το Convergence Ημιεπίπεδο (CS) και το Segmentation And Re-assembly (SAR) ημιεπίπεδο. Το CS ημιεπίπεδο εφαρμόζει το AAL στο ανώτερο επίπεδο πρωτοκόλλων και το SAR χωρίζει τα δεδομένα που μεταφέρονται σε κατάλληλα payload κομμάτια και στην κατεύθυνση αποδοχής τα συλλέγει και τα κάνει ίδια με αυτά που είναι πίσω στα αρχικά dataflow.

Ανάλογα με την περίπτωση, το CS ημιεπίπεδο μπορεί να χωριστεί σε περισσότερα μικρότερα κομμάτια.



Εικόνα 109 Γενική Δομή του AAL

Από την πλευρά του UMTS, τα AAL2 και AAL5 είναι οι πιο σημαντικές εναλλακτικές. Το AAL2 φαίνεται η πιο κατάλληλη επιλογή για συνδέσεις user plane μεταγωγής κυκλώματος και το AAL5 φαίνεται η πιο κατάλληλη επιλογή για ανταλλαγές ελέγχου του πρωτοκόλλου. Μια πιο λεπτομερή λίστα αυτών των AAL μεταβλητών σε διαφορετικά UTRAN interfaces πρωτοκόλλων δίνονται στον πίνακα Πίνακα 110.

AAL5	Iu: CS C-plane, PS C/U-plane, internal C-plane of the transport network Iur: C-plane, internal C-plane of the transport network Iub: C-plane, internal C-plane of the transport network
AAL2	Iu: CS U-plane Iur: U-plane Iub: U-plane

ΠΙΝΑΚΑΣ 110 Πίπεδα εφαρμογής του ATM τα οποία χρησιμοποιούνται στα UTRAN interfaces

Με το UTRAN το επίπεδο εφαρμογής, στο ATM, AAL5 χρησιμοποιείται για να μεταφέρει όλα τα πρωτόκολλα ελέγχου. Το AAL2 χρησιμοποιείται για κοινές μεταφορές των δεδομένων των χρηστών σε όλα τα interfaces εκτός από τα PS domain user data στο Iu interface.

9.3.4. IP Transport for User Data (GTP-U)

Το **GTP-U** είναι ένα πρωτόκολλο μεταφοράς που υποστηρίζει τα δεδομένα του user plane στο UMTS δίκτυο. Το GTP-U ανήκει στο domain μεταγωγής πακέτων στο UMTS δίκτυο και τοποθετείται στο RNC στην πλευρά του UTRAN, όπως στο SGSN και στο GGSN στην CN side.

Το GTP-U λειτουργεί σε 3 διαφορετικά επίπεδα, τα Gn, Gp και Iu-PS. Το Gn interface είναι μεταξύ των GSNs (π.χ SGSNs και GGSNs) ανήκει στο ίδιο δίκτυο UMTS. Το Gp interface χρησιμοποιείται στο εσωτερικό δίκτυο μεταξύ των δυο SGSNs ή μεταξύ των SGSN και GGSN που ανήκουν σε διαφορετικά δίκτυα πακέτων UMTS. Το Iu-PS βρίσκεται στο interface μεταξύ του RNC και SGSN.

Σε όλα τα interfaces το GTP-U λειτουργεί στην κορυφή του UDP/IP οικογένειας πρωτοκόλλων. Το user Datagram Protocol (UDP) παρέχει μεταφορά μηνυμάτων χωρίς σύνδεση μεταξύ 2 IP δικτυακών κόμβων. Η διευθυνσιοδότηση του UDP χρησιμοποιείται για να αναγνωρίσει τα GTP-U τελικά σημεία μέσα στην πηγή και στα στοιχεία τη κατεύθυνσης δικτύου. Το UDP επίσης παρέχει έναν μηχανισμό αθροίσματος ελέγχου για να ανιχνεύσει λάθη μεταφοράς μέσα στα πακέτα δεδομένων. Όπως είναι γενικά γνωστό η κύρια υπηρεσία του IP είναι το routing των μηνυμάτων μεταξύ της πηγής και των στοιχείων κατεύθυνσης δικτύου. Το routing βασίζεται στις IP διευθύνσεις (και το IPv4 και το IPv6 μπορούν να χρησιμοποιηθούν μέσα στο δίκτυο UMTS).

Το GTP-U παρέχει υπηρεσίες δεδομένων χωρίς σύνδεση για ανώτερα επίπεδα. Το GTP-U επιτρέπει πολλαπλά πρωτόκολλα για τα

πακέτα των user data για να μπουν σε ένα τούνελ κατά μήκος του Iu-PS, Gu, Gp interfaces.

Αφού ο βασικός σκοπός του GTP-U είναι να μεταφέρει δεδομένα χρηστών, έχει επικεντρωθεί σε αυτήν την δουλειά. Το GTP-U πολυπλέκει τα πακέτα που λαμβάνονται από κάποιο interface και τα στέλνει σε διάφορους προορισμούς (διαφορετικά UE). Το GTP-U λαμβάνει τα πακέτα με τα δεδομένα χρηστών χρησιμοποιώντας διάφορα είδη πρωτοκόλλων στο σκέλος του δικτύου IP. Τα στοιχεία του IP δικτύου και τα πρωτόκολλα μεταφέρουν πακέτα δεδομένων μεταξύ του UTRAN και του GGSN. Έτσι, δεν χρειάζεται να ανησυχεί για μηχανισμούς διευθυσιοδότησης στο επίπεδο IP με σκοπό να είναι ικανό να συνεργαστεί με τα πακέτα δεδομένων σε ειδικά περιεχόμενα PDP.

Το πρωτόκολλο GTP-U πρέπει να λειτουργεί εσωτερικά με άλλο πρωτόκολλο κατά την διάρκεια μεταφοράς των πακέτων δεδομένων. Στο **GGSN**, το πρωτόκολλο GTP-U επικοινωνεί με την λειτουργία καθυστέρησης πακέτων που βρίσκεται στην άκρη του UMTS δικτύου, π.χ. το Gi interfaces. Στην πλευρά του Iu-PS ενός SGSN το πρωτόκολλο GTP-U, λειτουργεί εσωτερικά με ένα άλλο πρωτόκολλο GTP-U στην πλευρά Gn. Με το πρωτόκολλο RNC το πρωτόκολλο GTP-U τερματίζει το τούνελ και προωθεί τα πακέτα στο πεδίο πρωτοκόλλου στο επίπεδο δικτύου. Οι κύριες λειτουργίες του GTP-U είναι:

- Data packet μεταφορά
- Encapsulation and tunneling
- Data packet sequencing
- Path alive check

Το μεγαλύτερο μέγεθος των πακέτων δεδομένων είναι 1500 octets. Αυτά τα πακέτα περιέχουν 1500 octets ή λιγότερα πρέπει να μεταφερθούν σαν ένα πακέτο. Σε περίπτωση που το πακέτο δεδομένων λαμβάνεται αυτό το εξωτερικό δίκτυο από το GGSN μεγαλώνει το όριο των 1500 octets, το GGSN πρέπει να δεχτεί ή να απορριψει το πακέτο δεδομένων που είναι εξαρτώμενο από τον τύπο PDP. Όλες αυτές οι συνδέσεις μεταξύ των στοιχείων δικτύου που περιέχουν το GTP-U πρέπει να έχουν τη Μεγαλύτερη Μονάδα Μεταφοράς (MTU) που εκτείνεται στα 1500 octets συν το μέγεθος των επικεφαλίδων των GTP-U, UDP και IP.

Κάθε πακέτο δεδομένων κρυπτογραφείται πριν μεταφερθεί στο UMTS δίκτυο. Η κρυπτογράφηση προσθέτει μια επικεφαλίδα GTP πρωτοκόλλου που περιέχει πληροφορίες του τούνελ σε κάθε πακέτο δεδομένων. Οι πληροφορίες αυτές περιλαμβάνουν έναν 32bit Tunnel Endpoint Identifier (TEID), ο οποίος έχει 2 βασικούς σκοπούς. **Πρώτον**, ο TEID χρησιμοποιείται για να στείλει τα περιεχόμενα ενός PDP μέσα στον τελικό σημείο του τούνελ. Έτσι, αυτό αναφέρεται αντίστροφα, σε διαφορετικά UEs τα οποία έχουν 1 ή περισσότερα περιεχόμενα PDP στο UMTS δίκτυο. **Δεύτερον**, το tunneling δίνει την δυνατότητα πολυπλεξίας των πακέτων δεδομένων που κατευθύνονται σε διαφορετικές διευθύνσεις μέσα σε ένα μόνο μονοπάτι το οποίο έχει αναγνωριστεί από δυο IP διευθύνσεις. Αυτό απομακρύνει την ανάγκη να καταλάβουμε πολλά διαφορετικά πρωτόκολλα που χρησιμοποιεί ο χρήστης στο UMTS κι έτσι κάνει το UMTS πιο απλό.

Σαν ένα βασικό χαρακτηριστικό του GTP-U μπορεί να παρουσιαστεί η σειρά των πακέτων δεδομένων μεταξύ του RNC και του GGSN. Κατά την διάρκεια της εγκατάστασης του περιεχομένου του PDP στο control plane η επαναδιαμόρφωση μπορεί να είναι διαπραγματεύσιμη. Σε περίπτωση που το πακέτο δεδομένων στην επαναδιαμόρφωση του τεθεί, η επικεφαλίδα GTP πρέπει να περιέχει μια σειρά ακολουθίας

αριθμών 16bit, τον οποίο το GTP-U χρησιμοποιεί για να τερματιστεί αν τα πακέτα δεδομένων των χρηστών λαμβάνονται με την σωστή σειρά ή αν αυτό χρειάζεται να περιμένει για τα πακέτα που έχουν χαθεί. Οστόσο, σε περίπτωση που τα χαμένα πακέτα έχουν τελείως χαθεί, ο μηχανισμός ακολουθίας του αριθμού των πακέτων δεδομένων δεν παρέχει ένα μηχανισμό για να επαναφέρει το χαμένο πακέτο. Εξαρτάται από τα άλλα επίπεδα να επαναφερθεί το χαμένο πακέτο δεδομένων.

Το GTP μπορεί να στέλνει μηνύματα "echo" για να δει αν το peer GTP λειτουργεί, σε τακτά χρονικά διαστήματα. Το peer GTP πρέπει να απαντήσει στο μήνυμα "echo" με ένα echo response μήνυμα.

Οι βασικές procedures που χρησιμοποιεί το GTP-U, στο UMTS δίκτυο, είναι κυρίως η μεταφορά πακέτων δεδομένων χρηστών μεταξύ του UTRAN και του SGSN όπως και ανάμεσα στα SGSN και GGSN. Όταν η περιοχή που χρησιμοποιεί η procedure αναβάθμισης απαιτεί να αλλάξουμε ένα GTP-U τούνελ από ένα SGSN σε άλλο, το GTP-U χρησιμοποιείται για να βασίζονται τα πακέτα δεδομένων που δεν έχουν σταλεί στα UE από το παλιό SGSN στο καινούριο.

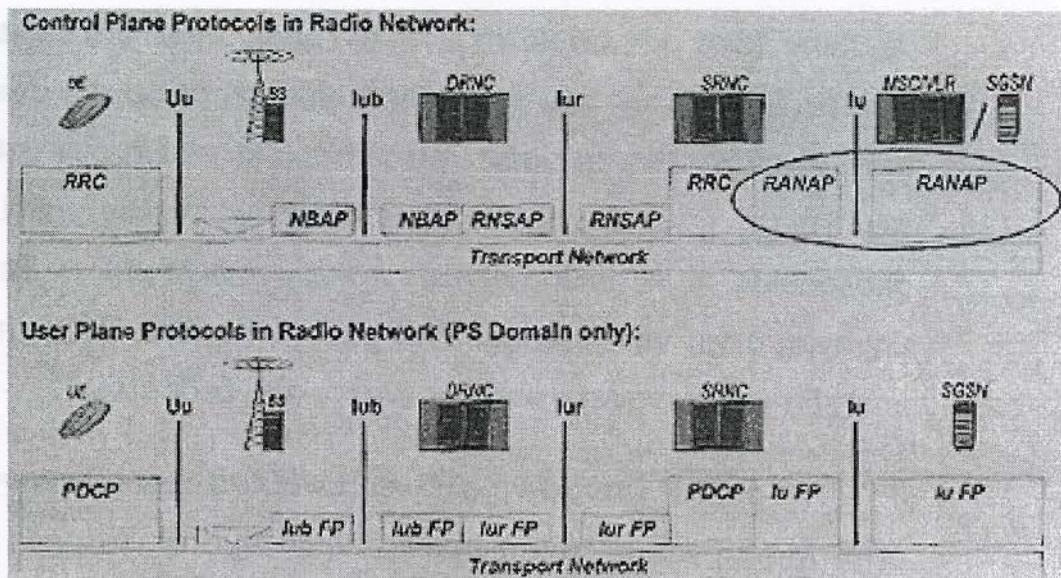
Το GTP-U καθορίζεται στις προδιαγραφές 3GPP TS 29060.

Πρωτόκολλα ΡαδιοΔικτύου

9.4.1. Radio Network Control Plane

9.4.1.1 RANAP – Radio Access Network Application – Εφαρμογές Ραδιοπρόσβασης δικτύου

Το Iu interface συνδέει το UMTS δίκτυο και το CN μεταξύ τους. Το ίδιο Iu interface χρησιμοποιείται για να συνδέσει και την CS υπηρεσία και την PS υπηρεσία στο UTRAN (εικόνα 111).



Εικόνα 111 Ραδιο Δίκτυο RANAP

Από την πλευρά του UMTS είναι λογικό πως οι συνδέσεις στην CS και PS υπηρεσία είναι ίδιες περίπου. Γι' αυτό ένα πρωτόκολλο σηματοδότησης μεταξύ του UTRAN και του CN έχει καθοριστεί. Ονομάζεται RANAP και καθορίζεται στις προδιαγραφές 3GPP TS 25413 και το CS και το PS domain χρησιμοποιούν το RANAP πρωτόκολλο για ένα έχουν πρόσβαση σε υπηρεσίες που παρέχονται από το UTRAN.

Το RANAP είναι το πρωτόκολλο που ελέγχει τις πηγές στο Iu interface. Ένα RANAP βρίσκεται στο RNC και η άλλη peer οντότητα του βρίσκεται στο MSC ή στο SGSN.

Το RANAP βρίσκεται στην κορυφή του Iu επιπέδου σηματοδότησης. Το RANAP χρησιμοποιεί την υπηρεσία μεταφοράς σηματοδότησης για να μεταφέρει RANAP μηνύματα μέσω του Iu interface. Στο 3GPP R99 τα επίπεδα μεταφοράς στο Iu interface χρησιμοποιούνται μέσω ενός SS7 πρωτοκόλλου stack over ATM ή IP μέσω ATM.

Το SS7 αποτελείται από πολλά επίπεδα πρωτοκόλλων αλλά το πιο σημαντικό είναι πάντα το SCCP. Είναι πάντα ένα SCCP πρωτοκόλλο που

προσφέρει στο RANAP το interface σε υπηρεσίες του πρωτοκόλλου μεταφοράς.

Το RANAP έχει συγκεκριμένες απαιτήσεις από τα επίπεδα μεταφοράς. Έχουμε υποθέσει ότι για κάθε μήνυμα (PDU), το οποίο το RANAP στέλνει στην peer οντότητα θα φτάσει στον προορισμό χωρίς κανένα λάθος.

Κάθε PDU των αφιερωμένων υπηρεσιών ελέγχου πρέπει να στέλνεται σε μια μοναδική σύνδεση σηματοδότησης. Αν η Iu signalling bearer σύνδεση κοπεί για κάποιο λόγο, το SCCP ενημερώνει το RANAP γι' αυτό.

Το RANAP προσφέρει υπηρεσίες στα ανώτερα επίπεδα πρωτοκόλλων: στο MSC/VLR και SGSN τα non-access stratum πρωτόκολλα που κάνουν χρήση τις RANAP υπηρεσίες. Λειτουργώντας εσωτερικά με RRC πρωτόκολλο στο RNC, το RANAP συνεισφέρει στην μεταφορά των μηνυμάτων σηματοδότησης αυτών των πρωτοκόλλων των πάνω δικτύων μεταξύ του UE και του CN.

Οι υπηρεσίες RANAP χωρίζονται σε 2 groups, τις **γενικές υπηρεσίες ελέγχου** και τις **αφιερωμένες υπηρεσίες ελέγχου**. Οι γενικές υπηρεσίες ελέγχου σχετίζονται με ολόκληρο το Iu interface μεταξύ του RNC και του CN.

Οι αφιερωμένες υπηρεσίες υποστηρίζουν τον διαχωρισμό κάθε UE στο Iu interface: είναι πάντα σχετικές με ένα UE. Η κυριαρχία των RANAP υπηρεσιών είναι αφοσιωμένες υπηρεσίες. Όλα τα μηνύματα RANAP των αφοσιωμένων υπηρεσιών ελέγχου στέλνονται σε μια αφιερωμένη – μισθωμένη σύνδεση. Αυτή η σύνδεση καλείται σύνδεση σηματοδότησης.

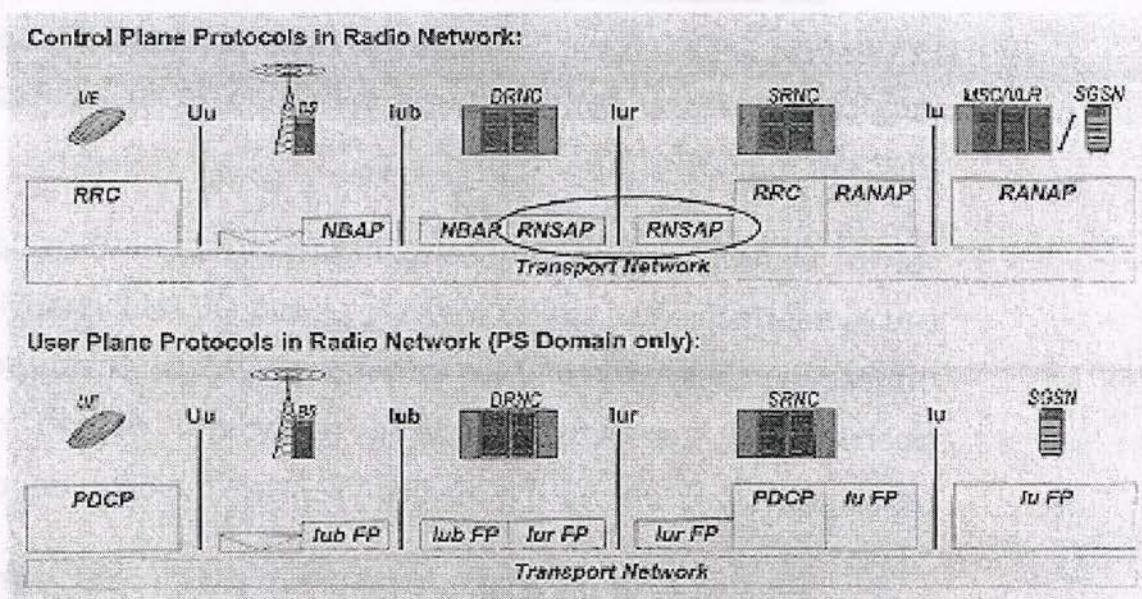
Η ολική RAB διαχείριση είναι μια από τις κύριες υπηρεσίες που το RANAP προσφέρει. Το RANAP παρέχει την έννοια για το CN να ελέγχει

την εγκατάσταση, την μετατροπή και την απελευθέρωση των RABs μεταξύ του UE και του CN. Σύμφωνα με αυτό, το RANAP υποστηρίζει την κινητικότητα του UE μεταφέροντας το RAB σε ένα νέο RNS όταν το UE μετακινείται από την μια περιοχή του RNS σε άλλη. Αυτή η υπηρεσία ονομάζεται SRNS επανατοποθετείται. Ελέγχοντας τον κόμβο ασφαλείας στο UTRAN είναι μια από τις υπηρεσίες που είναι αφιερωμένες υπηρεσίες ελέγχου. Οι γενικές υπηρεσίες ελέγχου χρειάζονται σε ιδιαίτερες περιπτώσεις.

Οι λεπτομερείς προδιαγραφές του RANAP βρίσκονται στις προδιαγραφές της 3GPP TS 25413.

9.4.1.2. RNSAP – Radio Network Subsystem Application Protocol

Το RNSAP είναι ένα πρωτόκολλο του control plane στο επίπεδο δικτύου (Εικόνα 112). Παρέχει αλλαγή ελέγχου σηματοδosis κατά μήκος του Iur interface. Το RNSAP τρέχει από δυο RNCs, το ένα από τα οποία αναλαμβάνει το ρόλο του Serving RNC (SRNC) και το άλλο λειτουργεί σαν Drifting RNC (DRNC). Το SRNC είναι αυτό που έχει την RANAP σύνδεση σηματοδosis στο CN.



Εικόνα 112 Ραδιοδίκτυο - RNSAP

Το RNSAP λειτουργεί πάντα στην κορυφή του SCCP πρωτοκόλλου. Όπως και στο RANAP, υπάρχουν 2 περιπτώσεις μεταφοράς πέρα από το SCCP: ή το ATM με ένα AAL5 επίπεδο εφαρμογής ή μια μεταφορά βασισμένη σε IP όπου τα SCTP και M3UA πρωτόκολλα χρησιμοποιούνται στο επίπεδο εφαρμογής. Το SCCP σαν πρωτόκολλο μεταφοράς σηματοδοσίας παρέχει 2 διαφορετικούς κόμβους για το RNSAP: περιορισμένη σύνδεση και υπηρεσία connectionless μεταφοράς δεδομένων.

Το RNSAP είναι υπεύθυνο για την διαχείριση της σηματοδοσίας του bearer κατά μήκος του Iur interface. Το RNSAP χρησιμοποιείται για την εγκατάσταση των ραδιοσυνδέσεων και επιτρέπει στο SRNC να ελέγχει εκείνες τις ραδιοσυνδέσεις που χρησιμοποιούν μισθωμένες πηγές μέσα στο DRNS.

Το πρωτόκολλο RNSAP χρησιμοποιεί μια σύνδεση σηματοδοσίας άνα ένα DRNC και ένα UE όπου το ένα UE μπορεί να έχει μια ή περισσότερες ενεργές ραδιοσυνδέσεις για την μεταφορά των 3 μηνυμάτων του δικτύου.

Οι πληροφορίες που μεταφέρονται στο Iur interface κατηγοριοποιούνται ως εξής:

- **Σηματοδοσία ελέγχου κινητικότητας:** το Iur interface παρέχει την δυνατότητα να υποστηρίζει την κινητικότητα στο ραδιο interface μεταξύ των RNSs για τα UEs που έχουν σύνδεση με το UTRAN. Αυτή η ικανότητα περιλαμβάνει την υποστήριξη handover, τον έλεγχο των ραδιοποηγών και τον συγχρονισμό μεταξύ των RNSs.
- **Ροές Δεδομένων στα Iub / Iur DCH:** το Iur interface παρέχει την έννοια της μεταφοράς των uplink και downlink κατευθύνσεων των Iub /

Iur πεδίων DCH που μεταφέρει δεδομένα χρηστών και πληροφορίες ελέγχου μεταξύ του SRNC και του κινητού BS, μέσω του DRNS.

- **Ροές Δεδομένων στο Iur DSCH:** μια ροή δεδομένων DSCH σε περιβάλλον Iur ανταποκρίνεται στα δεδομένα που μεταφέρονται σε ένα κανάλι μεταφοράς DSCH για ένα UE. Ένα UE μπορεί να έχει πολλαπλές ροές δεδομένων Iur DSCH. Επιπρόσθετα, το interface παρέχει μια έννοια στο SRNC για αναφορά ουράς και για το DRNC που βρίσκει την ισχύ στο SRNC.

- **Ροές Δεδομένων στο Iur RACH / CRCH:** σε μεταβλητές WCDMA FDD μόνο.

- **Ροές Δεδομένων στο Iur FACH**

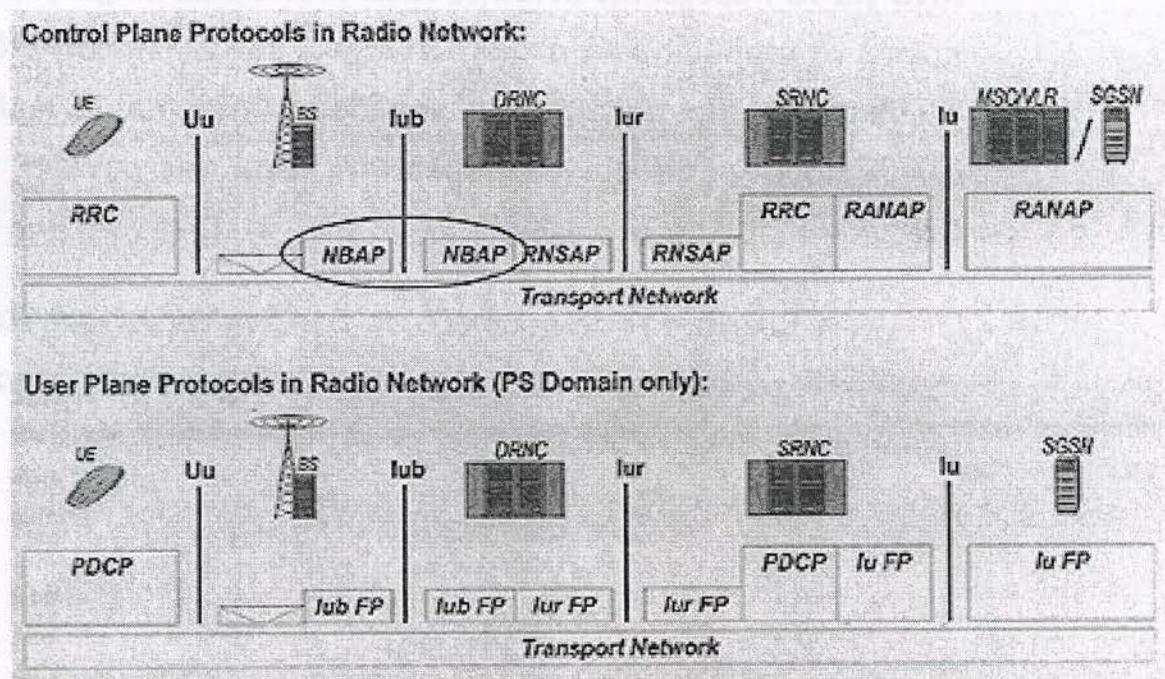
Οι κύριες λειτουργίες ελέγχου του UTRAN που υποστηρίζονται από το πρωτόκολλο RNSAP είναι:

- Διαχείριση Δικτύου Μεταφοράς
- Διαχείριση Κίνησης των κοινών καναλιών μεταφοράς, π.χ. paging
- Διαχείριση κίνησης μισθωμένων καναλιών, τα οποία περιλαμβάνουν π.χ. εγκατάσταση ραδιοσυνδεσης, πρόσθεση και διαγραφή της αναφοράς μέτρησης
- Διαχείριση κίνησης των καναλιών μεταφοράς που μοιράζονται στην downlink σύνδεση, η οποία περιλαμβάνει, π.χ. εγκατάσταση ραδιοσύνδεσης, πρόσθεση και αφαίρεση της τοποθέτησης ισχύς.
- Αναφορά μέτρησης για κοινά και μισθωμένα αντικείμενα μέτρησης

- Επανατοποθέτηση του SRNS: αυτή η λειτουργία επαναπροσδιορίζει τις ενέργειες όταν ο ρόλος του RNS που χρησιμοποιείται είναι να αναλαμβάνεται αυτό από κάποιο άλλο RNS.

9.4.1.3. NBAP – Node B Πρωτόκολλο Εφαρμογής

Το NBAP είναι ένα πρωτόκολλο επιπέδου δικτύου, το οποίο περιέχει την σηματοδοσία του control plane κατά μήκος του Iu interface και τις πηγές ελέγχου στο Iub interface και παρέχει κατά μια έννοια για τον BS και τον RNS να επικοινωνούν (Εικόνα 113).



Εικόνα 113 Ραδιοδίκτυο NBAP

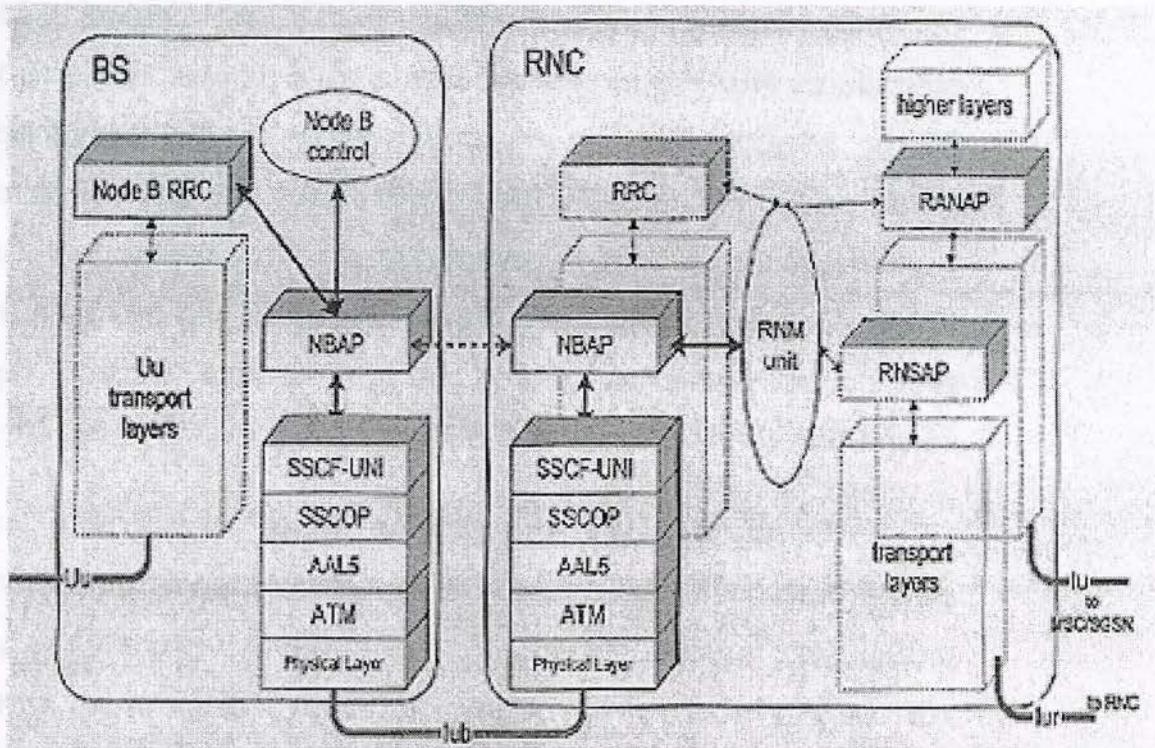
Το NBAP βρίσκεται στην κορυφή των επιπέδων μεταφοράς του Iub και χρησιμοποιούν τις δικές του υπηρεσίες για να μεταφέρει τα μηνύματα NBAP μέσω του Iub interface. Η επιλογή 99 της τεχνολογίας μεταφορών χρησιμοποιείται για να μεταφέρει την σηματοδοσία NBAP μέσω του Iub interface είναι το ATM.

Η ATM σύνδεση μαζί με τα κατάλληλα επίπεδα εφαρμογής ATM παρέχουν έναν bearer σηματοδοσίας για το NBAP όπως καθορίζεται στις προδιαγραφές της 3GPP TS 25432.

Νέα επίπεδα μεταφοράς μπορούν να χρησιμοποιηθούν με το NBAP χωρίς να υπάρχει ανάγκη να επανακαθορισθεί η λειτουργικότητα αυτού του πρωτοκόλλου.

Το NBAP προσφέρει τις υπηρεσίες του στις μονάδες ελέγχου του RNS και τον BS. Το NBAP έχει επίσης ένα interface με το πρωτόκολλο RRC για να παρέχει την οντότητα RRC στον BS με πληροφορίες, οι οποίες πρέπει να τοποθετηθούν στο BCCH λογικό κανάλι. Το NBAP δεν έχει άλλα interfaces στα πρωτόκολλα του επιπέδου δικτύου του UTRAN και όλες οι αλληλεπιδράσεις με αυτές μεταφέρονται μέσω της μονάδας ελέγχου του RNC.

Η Εικόνα 114 παρουσιάζει το περιβάλλον λειτουργίας του NBAP πρωτοκόλλου και όλα τα interfaces του NBAP παρουσιάζονται σαν έντονα μαύρα όπως στην εικόνα.



Εικόνα 114 Λειτουργικό περιβάλλον του NBAP

Μια σημαντική υπευθυνότητα του NBAP είναι να εγκαθιστά και να διατηρεί μια σύνδεση control plane κατά μήκος του Iub interface να ικανοποιεί την εγκατάσταση και την απελευθέρωση των μισθωμένων συνδέσεων user plane κατά μήκος του Uu interface και να διατάζει το BS να ενεργοποιεί πηγές για νέες ραδιοσυνδέσεις κατά μήκος του Uu interface. Όλες οι λειτουργίες σηματοδότησης NBAP χωρίζονται σε **κοινές procedures** και **μισθωμένες procedures**.

Οι **κοινές procedures NBAP** δεν σχετίζονται με οποιοδήποτε συγκεκριμένο UE αλλά με κοινές πηγές κατά μήκος του Iub interface. Η σηματοδότηση που σχετίζεται με το Λογικό O&M του BS (Πληροφορίες που αναφέρονται σαν Λογική Λειτουργία και Διατήρηση (Logical O&M) του BS) αποτελούν το κυριότερο κομμάτι των κύριων procedures για την διαχείριση του configuration των λογικών πηγών και procedures, το οποίο δίνει την δυνατότητα στον BS να ενημερώνει το RNC σχετικά με την κατάσταση των λογικών πηγών στον BS. Οι κοινές procedures NBAP επιτρέπουν επίσης το RNC να καθορίζει ειδικές μετρήσεις στον BS και αργότερα να αναφέρει

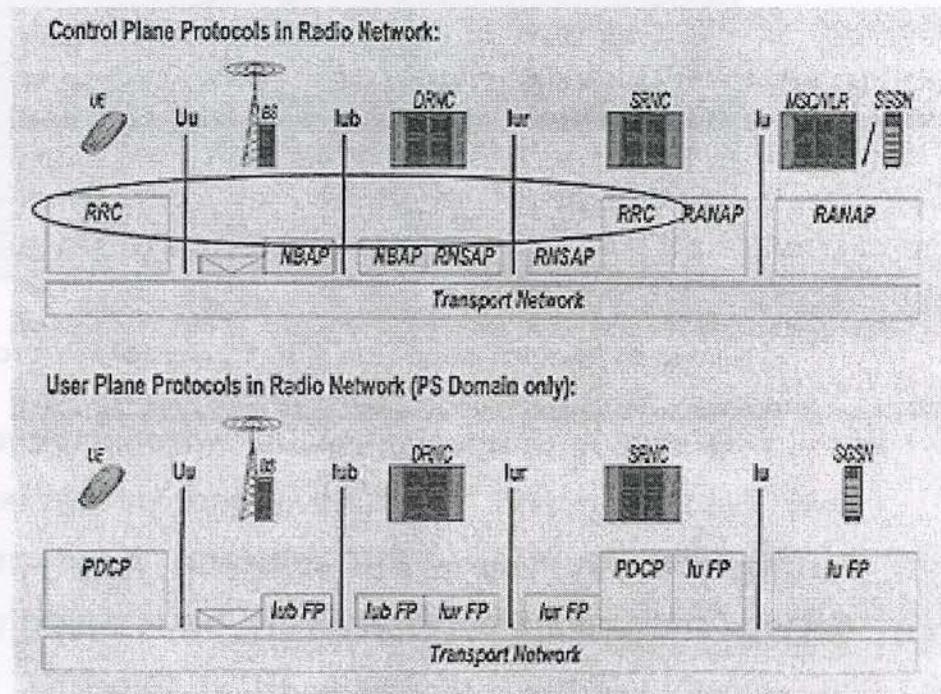
τα αποτελέσματα των μετρήσεων. Δίπλα στο Logical O&M, οι κοινές procedures NBAP χρησιμοποιούνται για να μεταφέρουν από το RNC στον BS τις πληροφορίες για να μεταφερθούν σε ένα broadcast κανάλι. Οι κοινές procedures NBAP επίσης καθορίζουν την δημιουργία ενός νέου UE για κάθε ειδικό UE στον BS εγκαθιστώντας την πρώτη ραδιοένωση γι' αυτό το UE. Οι κοινές procedures NBAP διατηρούν μια σύνδεση σηματοδοσίας ενός control plane κατά μήκος του lub interface, η οποία τερματίζει στην κοινή θύρα (port) ελέγχου του BS.

Οι μισθωμένες procedures NBAP σχετίζονται πάντα με ένα συγκεκριμένο UE, του οποίου UE το περιεχόμενο υπάρχει ήδη στον BS. Οι μισθωμένες procedures NBAP περιλαμβάνουν procedures για διαχείριση και έλεγχο των υπάρχοντων ραδιοσυνδέσεων των οποίων τα UE συνδεόνται με το BS. Αυτές οι procedures επιτρέπουν στο RNC να διατάζει τον BS να εγκαθιστά ή να απελευθερώνει μερικές ραδιοσυνδέσεις για το περιεχόμενο του UE. Οι αφοσιωμένες procedures NBAP παρέχουν επίσης τον BS ή αναλαμβάνουν την αποθήκευση των μεταφορών στις ραδιοσυνδέσεις. Οι μισθωμένες procedures NBAP περιλαμβάνουν επίσης την διαχείριση της reconfiguration των ραδιοσυνδέσεων και υποστηρίζει τις μετρήσεις σε μισθωμένες πηγές και η ανταποκρινόμενη δύναμη ελέγχου των ενεργειών, το οποίο επιτρέπει στο RNC να εφαρμόζει στο downlink power level στις ραδιοσυνδέσεις. Οι μισθωμένες procedures σηματοδοσίας του NBAP μεταφέρονται μέσω ενός από τα port επικοινωνίας του λογικού μοντέλου του BS. Μπορεί να υπάρχουν πολλές διαφορετικές ενώσεις για τις μισθωμένες procedures NBAP κατά μήκος του lub interface. Οι πληρείς προδιαγραφές του NBAP πρωτοκόλλου βρίσκονται στις προδιαγραφές της 3GPP TS 25433.

9.4.1.4. Πρωτόκολλο RRC (Radio Resource Control)

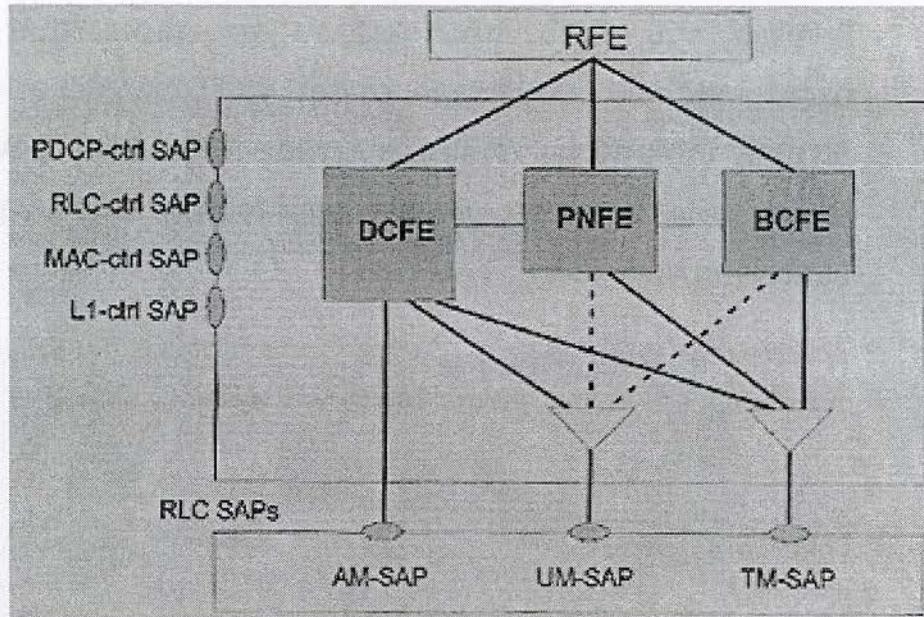
Το RRC πρωτόκολλο είναι το κλειδι-πηγή ελέγχου μέσα στο UTRAN (Εικόνα 115). Υποστηρίζει την λειτουργικότητα RRM. Με την

βοήθεια του RRC πρωτοκόλλου το αποτέλεσμα των αποφάσεων διαχείρισης των ραδιοπηγών μπορεί να εξαπλωθεί σε όλα τα στοιχεία του δικτύου UTRAN με τέτοιες αποφάσεις. Τα RRC μηνύματα μεταφέρουν επίσης στην τιμή τους όλη την σηματοδοσία που ανήκει στα non-access stratum πρωτόκολλα.



Εικόνα 115 Ραδιοδίκτυο – (RRC) πρωτοκόλλου

Το RRC λειτουργεί ανάμεσα στο UE και το RNC. Οι οντότητες του πρωτοκόλλου RRC χρησιμοποιούν τους bearers σηματοδοσίας οι οποίοι παρέχονται από το ημιεπίπεδο RLC για να μεταφέρουν τα μηνύματα σηματοδοσίας. Όλοι οι 3 κόμβοι του RLC είναι διαθέσιμοι σε διαφορετικά είδη των SAPs που φαίνονται στην εικόνα 116.



Εικόνα 116 Λογική Δομή ενός RRC πρωτοκόλλου στο WCDMA-FDD

Ο κόμβος μεταφοράς TM-SAP χρησιμοποιείται, για παράδειγμα, όταν ένα UE πρέπει να επικοινωνήσει με ένα κύριο RNC για να εγκατασταθεί μια πλήρης RRC σύνδεση. Χρησιμοποιείται επίσης για σύντομα επαναλαμβανόμενα μηνύματα, όπως paging για να αποφευχθούν τα μη απαραίτητα overheads. Ο άγνωστος κόμβος AM-SAP χρησιμοποιείται για την σηματοδότηση ελέγχου ειδικά για ένα UE όταν η αξιοπιστία του μηνύματος απαιτείται. Ο unacknowledged κόμβος UM-SAP από την άλλη μεριά χρησιμοποιείται για να αποφευχθεί μια πιθανή καθυστέρηση που θα παρουσιαστεί σε ένα κόμβο (acknowledged) σηματοδότησης. Για παράδειγμα, όταν απελευθερώνουμε μια σύνδεση RRC το μήνυμα απελευθέρωσης επαναλαμβάνεται πολλές φορές (γρήγορη λειτουργία επανάληψης) μέσω του UM-SAP για να αυξήσει την πιθανότητα να το λάβει το UE.

Η Εικόνα 116 δείχνει επίσης την λογική του RRC πρωτοκόλλου. Η Μισθωμένη Λειτουργία Ελέγχου (DCFE) χρησιμοποιείται για να χειριστούμε όλες τις σηματοδοσίες ειδικές για ένα UE. Στο SRNC υπάρχει μια μόνο DCFE για κάθε UE που έχει μια σύνδεση RRC με αυτό το RNC. Η Paging

and Notification Control Entity (**PNFE**) χειρίζεται μηνύματα paging στον idle κόμβο των UEs. Σε ένα CRNS υπάρχει τουλάχιστον μια οντότητα PNFE οντότητα για κάθε κυψέλη για να ελεγχθεί. Η Broadcast Control Function Entity (**BCFE**) χειρίζεται πληροφορίες συστήματος που μεταδίδονται στα BCCH και στα FACH λογικά κανάλια. Υπάρχει τουλάχιστον μια BCFE για κάθε κυψέλη στο CRNC. Πέρα από τις λειτουργίες αυτές μια ειδική λειτουργία routing (**RFE**) έχει μοντελοποιηθεί στην κορυφή της Εικόνας 116. Η εργασία του είναι να διαμοιράζει τα non-access stratum μηνύματα σε διαφορετικές MM/CM οντότητες στην πλευρά UE και σε διαφορετικά CN domains στην RN πλευρά.

Η κύρια λειτουργία του RRC είναι να ελέγχει τους radio bearers, τα κανάλια μεταφοράς και τα φυσικά κανάλια. Αυτό γίνεται με την εγκατάσταση, reconfiguration απελευθέρωση των διαφορετικών ειδών των radio bearers. Πριν τέτοιες ενεργειες γίνουν, η επικοινωνία του πρωτοκόλλου RRC η ίδια πρέπει να είναι καθορισμένη χρησιμοποιώντας έναν αριθμό τουλάχιστον 4άρων radio bearers σηματοδosis. Η σύνδεση σηματοδosis που προκύπτει ονομάζεται RRC σύνδεση. Κατά την διάρκεια της RRC σύνδεσης, εγκατάστασης, reconfiguration και απελευθέρωσης από τους άλλους radio bearers κίνησης του user plane μπορεί να εκτελεστούν με τις ανταλασσόμενες διαταγές και τις πληροφορίες κατάστασης μεταξύ των peer οντοτήτων RRC σύνδεσης κατά μήκος των bearers σηματοδosis. Η σύνδεση RRS θα συνεχίσει να υπάρχει μέχρι όλοι οι bearers του user plane να έχουν απελευθερωθεί και η σύνδεση RRC μεταξύ του UE και του RNC να έχει απελευθερωθεί.

Οι μηχανισμοί ασφάλειας που χρησιμοποιούν τους bearers ενεργοποιούνται και απενεργοποιούνται κάτω από τον έλεγχο του RRC πρωτοκόλλου. Πέρα από την ενεργοποίηση της εμπιστευτικής προστασίας μέσω του ciphering, το RRS μπορεί επίσης να εγγυηθεί την integrity όλων

των υψηλών επιπέδων σηματοδοσίας μηνυμάτων τόσο καλά όσο στα περισσότερα από τα δικά του μηνύματα σηματοδοσίας.

Η διαχείριση της κινητικότητας του UE στο επίπεδο UTRAN ελέγχεται από την σηματοδότηση RRS. Τέτοιες λειτουργίες διαχείρισης κινητικότητας που εκτελούνται από το RRC πρωτόκολλο είναι η αναβάθμιση της κυψέλης.

Ο έλεγχος και η αναφορά των ραδιομετρήσεων αναλαμβάνεται από το RRC πρωτοκόλλου. Ένα σύνολο από 7 κατηγορίες μετρήσεων μπορούν να ενεργοποιηθούν στο UE και πέρα από αυτά μπορούν να ενεργοποιηθούν και οι μετρήσεις θέσης για το UE. Κάθε μέτρηση μπορεί να μετρηθεί και να αναφερθεί ανεξάρτητα από τις άλλες μετρήσεις.

Το RRC ελέγχει τη ματάδοση των πληροφοριών και την σελιδοποίηση των UEs και των ανταλλασσόμενων παραμέτρων για τις περιπτώσεις ελέγχου ισχύος.

Το RRC είναι πολύ περίπλοκο. Έχει 40 διαφορετικές procedures και περισσότερα από 60 διαφορετικά είδη PDUs.

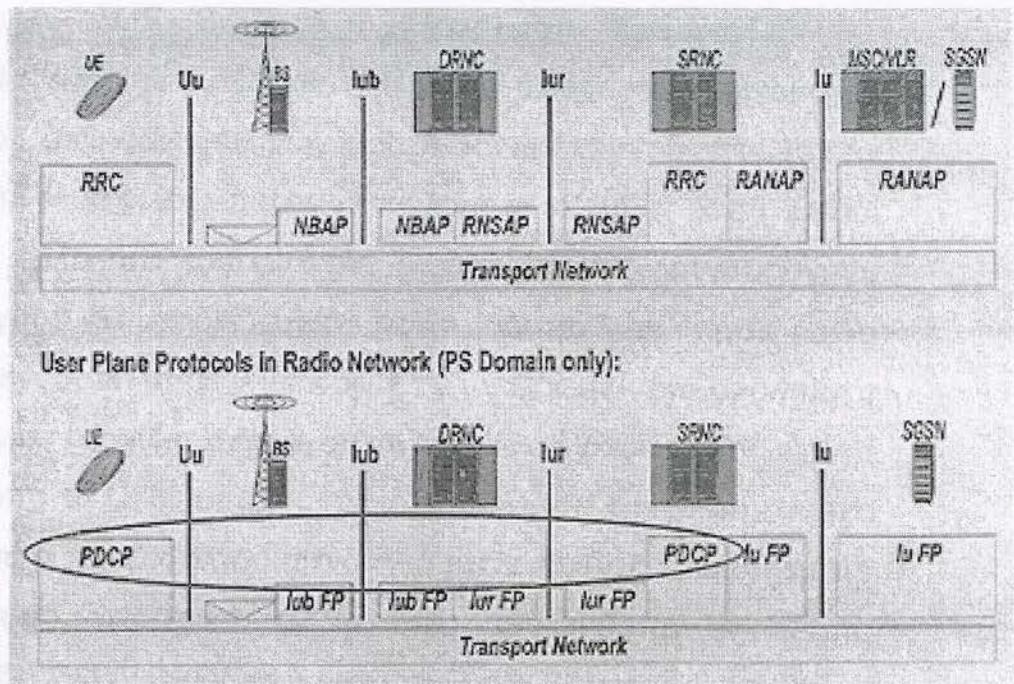
Οι προδιαγραφές του RRC φαίνονται στο 3GPP TS 25331.

9.4.2. ΡαδιοΔίκτυο

9.4.2.1 PDCP-Packet Data Convergence Protocol

Το PDCP σχεδιάστηκε για να κάνει τα πρωτόκολλα WCDMA κατάλληλα για μεταφορά των περισσοτέρων κοινών πρωτοκόλλων από χρήστη σε χρήστη, TCP-IP. Έτσι, τα πρωτόκολλα PDCP μπορεί να βρεθούν και στις δυο πλευρές του WCDMA interface: στο RNC και στο UE. Η κύρια λειτουργία του PDCP πρωτοκόλλου είναι να συμπιέσει τις επικεφαλίδες του πρωτοκόλλου payloads, το οποίο αν σταλεί, χωρίς συμπίεση, θα χαλάσουν την invaluable capacity της ραδιοένωσης. Η μόνη

συμπύεση της IP επικεφαλίδας δείχνεται αποκλειστικά για την 3GPP R99 είναι το RFC2507 καθορισμένα από το IETF.



Εικόνα 117 Ραδιοδίκτυο σε user plane- PDCP

Το PDCP πρωτόκολλο χρησιμοποιεί τις υπηρεσίες του επιπέδου RLC σε 3 διαφορετικούς κόμβους. Έτσι, αυτές οι υπηρεσίες είναι διαθέσιμες σε 3 διαφορετικά σημεία πρόσβασης (SAPs):

- Μεταφορά δεδομένων η οποία είναι acknowledged (AM-SAP)
- Μεταφορά δεδομένων η οποία είναι unacknowledged (UM-SAP)

- Μεταφορά δεδομένων σε κόμβο transparent (TM-SAP)

Οι πληροφορίες που παρέχει το PDCP στα επίπεδα είναι οι εξής:

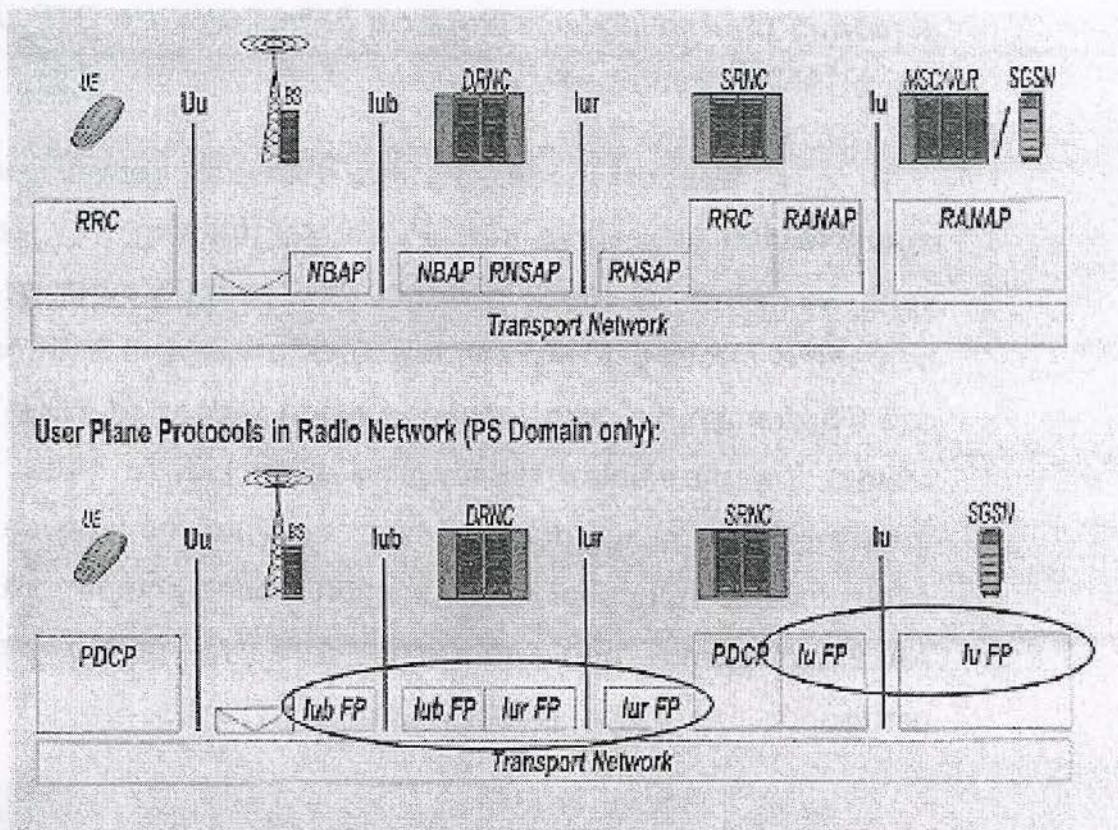
- Μεταφορά πακέτων (SDUs) είτε σε acknowledged, unacknowledged, transparent κόμβο

- Έλεγχο των ραδιο bearer με εγκατάσταση, reconfiguration και απελευθέρωση ενός ραδιο bearer στο PC domain.

Το PDCP πρωτόκολλο τρέχει στο RNC το οποίο πρέπει να λειτουργήσει εσωτερικά με τα πρωτόκολλα του πεδίου UTRAN με σκοπό να καθυστερήσει τα πακέτα δεδομένων στην downlink κατεύθυνση από το Iub/Iur προς το Iu. Σε φυσιολογικές περιπτώσεις αυτό επιτυγχάνεται απλά αντιγράφοντας πακέτα από το ένα interface στο άλλο και παρέχουν την ειδική συμπίεση / αποσυμπίεση επικεφαλίδας. Τα πράγματα γίνονται πιο περίπλοκα όταν χρειάζεται να γίνει intersystem handover. Γι' αυτό το λόγο το PDCP πρωτόκολλο είναι εξοπλισμένο με ειδικούς εσωτερικούς κανόνες, σχετικά με τα πρωτόκολλα πεδίων Iu και το RRC τα οποία διαβεβαιώνουν ότι τα πακέτα δεν χάνονται ή γίνονται διπλά και ότι η ακολουθία πακέτων μπορεί να αποθηκευθεί μετά το handover στο σύστημα. Οι πλήρεις προδιαγραφές του PDCP είναι μέσα στο 3GPP TS25.323.

9.4.2.2 Utran Frame Protocols

Χρησιμοποιούνται στο επίπεδο δικτύου αυτά τα πρωτόκολλα, τα οποία μεταφέρουν τα δεδομένα χρηστών UMTS μέσα του κοινού δικτύου UTRAN (Εικόνα 118). Είναι ενεργά κατά μήκος του interface Iu, Iur, Iub στο UTRAN. Χρησιμοποιούν την υπηρεσία μεταφοράς δικτύου.



Εικόνα 118 Ραδιοδίκτυο του user plane - UTRAN πρωτόκολλα

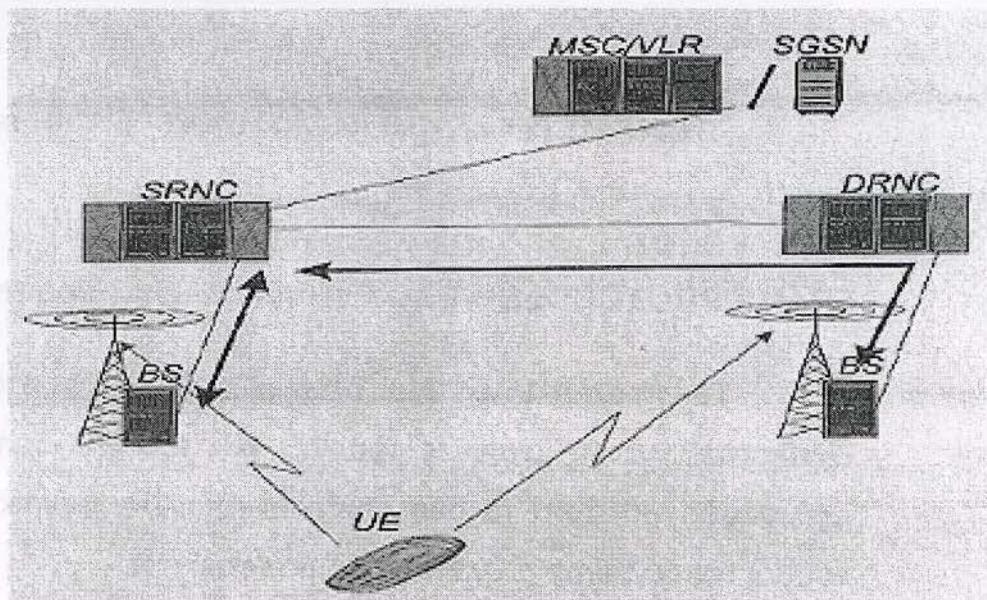
FRAME PROTOCOLS AT Iu –Πρωτόκολλα πεδίου στο Iu

Το πρωτόκολλο που διαχειρίζεται πεδία στο Iu interface έχει σχεδιαστεί για τις ανάγκες του CS και του PS domain. Οι υπηρεσίες μεταφοράς για αυτά τα δύο domains είναι διαφορετικές και γι' αυτό δυο κόμβοι του Iu frame protocol χρησιμοποιούνται:

- **Transparent mode**, ο οποίος χρησιμοποιείται σε τέτοιους bearers, οι οποίοι δεν απαιτούν οποιαδήποτε ειδική ενέργεια πρωτοκόλλου, όπως framing. Γι' αυτό τα δεδομένα χρηστών σε αυτό τον κόμβο περνούν κατά μήκος του δικτύου μεταφοράς χωρίς να προσθέτει οποιαδήποτε πληροφορία επικεφαλίδων πρωτοκόλλου. Ο transparent mode έτσι γίνεται ένα μηδενικό πρωτόκολλο και χρησιμοποιείται π.χ. για

μεταφορά μη πραγματικών πακέτων δεδομένων στο GTP-U από το RNC στο SGSN και αντίστροφα.

- **Support mode**, το οποίο παίρνει τη μορφή ενός πραγματικού πρωτοκόλλου με έλεγχο των PDUs και framing των δεδομένων των χρηστών. Αυτοί οι τύποι πρωτοκόλλου εφαρμόζονται σε radio access bearers, οι οποίοι μεταφέρουν, π.χ. κωδικοποιημένα AMR δεδομένα λόγου στο CS domain. Γι' αυτό ο support mode ελέγχει τα PDUs και μπορεί να ελέγχει τον rate control και τον time alignment, τα οποία χρειάζονται να υποστηρίξουν την μεταφορά λόγου πραγματικού χρόνου. Σε αυτή την περίπτωση το πρωτόκολλο του support mode χρησιμοποιεί απευθείας την AAL2 υπηρεσία που παρέχεται από το δίκτυο υπογεγραμμένης μεταφοράς.

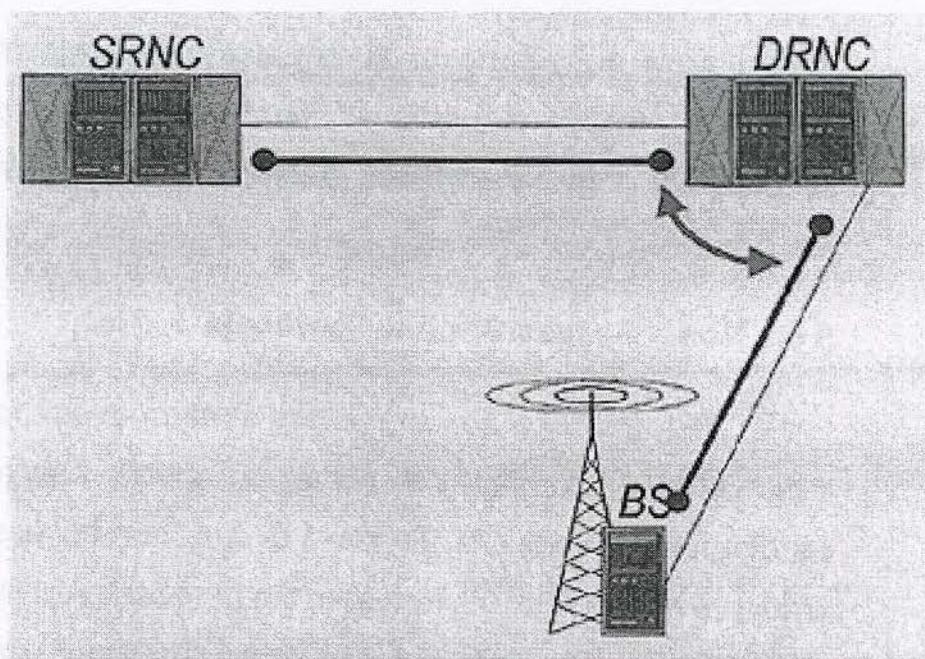


Εικόνα 119 Frame πρωτόκολλα για τα αφιερωμένα κανάλια του Iub/Iur

FRAME PROTOCOL FOR DEDICATED CHANNELS AT Iur & Iub

Υπάρχει ένα κοινό πρωτόκολλο για τα αφιερωμένα κανάλια στα Iub και Iur όπως παρουσιάζονται στην εικόνα 83 9.35. Με αυτό το πρωτόκολλο

το SRNC μπορεί να αλλάξει τα πεδία δεδομένων χρηστών με τα Ues που εξυπηρετούνται από τους δικούς τους μετακινούμενους BSs.



ΕΙΚΟΝΑ 120 Frame πρωτόκολλα για κοινά κανάλια μεταφοράς του Iub/Iur

Πέρα από την φυσιολογική μεταφορά δεδομένων των κατευθύνσεων uplink και downlink, αυτό το πρωτόκολλο πεδίων είναι ικανό να εκτελεί πολλές λειτουργίες ελέγχου. Τέτοιες λειτουργίες πρωτοκόλλου έχουν να κάνουν με την εφαρμογή χρόνου και τον συγχρονισμό.

FRAME PROTOCOL FOR COMMON TRANSPORT CHANNELS AT Iur ΚΑΙ Iub

Για να στέλνεις και να λαμβάνεις πεδία δεδομένων μέσω κοινών καναλιών μεταφοράς υπάρχουν 2 διαφορετικά πρωτόκολλα: Ένα για το Iub και ένα για το Iur. Γι' αυτό, οι εσωτερικές συνεργασίες μεταξύ αυτών των πρωτοκόλλων γίνεται στο DRNC. Τα πρωτόκολλα πεδίων εκτελούν και τις εργασίες ελέγχου.

9.5 System Network Protocol-Πρωτόκολλο συστήματος

Αυτά τα πρωτόκολλα δημιουργούν υπηρεσίες επικοινωνίας σε χρήστες τέτοιων τερματικών. Τα πρωτόκολλα συστήματος δικτύου λειτουργούν στην κορυφή του ραδιοδικτύου και μέσα στο UMTS CN το ίδιο.

9.5.1 Non – Access Stratum Protocols

Τα πρωτόκολλα non-access stratum αναφέρονται στην ομάδα των πρωτοκόλλων του control plane, τα οποία ελέγχουν την επικοινωνία μεταξύ των UEs και CN. Το κοινό όνομα “non-access stratum” αναφέρεται στο γεγονός ότι αυτά τα πρωτόκολλα μεταφέρονται transparently μέσω του ραδιοδικτύου. Τα πρωτόκολλα αυτά ανήκουν σε 2 ημιεπίπεδα του συστήματος δικτύου. Το MM ημιεπίπεδο λειτουργεί στην κορυφή της σύνδεσης σηματοδότησης που παρέχεται από το δίκτυο. Πέρα από την δική του λειτουργικότητα, το MM λειτουργεί σαν μεταφορέας των πρωτοκόλλων του ημιεπιπέδου MM.

9.5.1.1. MM Πρωτόκολλο για το CS Domain

Το MM πρωτόκολλο λειτουργεί μεταξύ του UE και του MSC / VLR. Αυτό το πρωτόκολλο παρέχει βασικούς μηχανισμούς σηματοδότησης για να ελέγχει την διαχείριση κινητικότητας και τις λειτουργίες αυθεντικότητας μεταξύ των UEs και του CN CS domain. Το MM υποστηρίζεται από τα UEs που λειτουργούν μαζί στο PS/CS λειτουργικό κόμβο ή στον CS- μόνο λειτουργικό κόμβο.

Το MM χρησιμοποιεί την σύνδεση σηματοδότησης που παρέχεται από τα επίπεδα δικτύου. Αυτή η σύνδεση σηματοδότησης μερικές φορές αναφέρεται σαν σύνδεση ραδιοπηγής (RR),το οποίο αποτελείται από το

RRC σύνδεση πρωτοκόλλου μέσω του bearer σηματοδοσίας και την RANAP σύνδεση κατά μήκος του Iur bearer. Πριν από οποιαδήποτε ενέργεια MM πρωτοκόλλου για να γίνει η σύνδεση σηματοδοσίας πρέπει πρώτα να εγκατασταθεί. Μέσα στο CN το MM πρωτόκολλο στην πλευρά MSC/VLR πρέπει να λειτουργήσει εσωτερικά με το MAP πρωτόκολλο με σκοπό να διατηρήσουν την θέση εγκατάστασης στο HLR.

Το MM ελέγχει την κατάσταση MM του UE και την ανταποκρινόμενη peer οντότητα στην πλευρά του δικτύου. Οι κύριες καταστάσεις αυτών των πρωτοκόλλων υποδεικνύουν την αναβάθμιση της κατάστασης θέσης του UE, το οποίο έχει μια κύρια επιρροή στις ενέργειες του για να χρησιμοποιήσει τις υπηρεσίες του ημιεπιπέδου CM. **Έτσι, γι' αυτό το MM πρωτόκολλο χρησιμοποιείται για μεταφορά μηνυμάτων των πρωτοκόλλων των ημιεπιπέδων CM μεταξύ του UE και των MSC/VLR.**

Το MM έχει τρεις βασικές κατηγορίες procedures:

- MM connection procedures
- MM common procedures
- MM specific procedures

Οι **MM connection procedures** χρησιμοποιούνται για την εγκατάσταση και την απελευθέρωση συνδέσεων MM αλλά και για την μεταφορά μηνυμάτων του ημιεπιπέδου CM. Μια σύνδεση MM γίνεται όταν υπάρχει απελευθέρωση μετά από αίτηση του CM.

Όταν η MM σύνδεση εγκατασταθεί και γίνει γνωστό στο UE, το MM πρωτόκολλο στέλνει ένα CM SERVICE REQUEST με τις ακόλουθες παραμέτρους:

- Ταυτότητα του UE, π.χ. TMSI

- Classmark2 του κινητού σταθμού
- Ακολουθία αριθμών του chiphering key
- Τύπος της υπηρεσίας CM που αναγνωρίζει τον τύπο της αλλαγής που έχει ζητηθεί, που μπορεί να είναι, π.χ. αρχική εγκατάσταση κινητής τηλεφωνίας, εγκατάσταση επείγουσας κλήσης, υπηρεσία σύντομων μηνυμάτων ή υπηρεσία υποστήριξης.

Το MM πρωτόκολλο θα παραλάβει το αίτημα στη CN πλευρά θα αναλύσει αυτές τις 3 παραμέτρους και αποφασίζει για την αποδοχή και την συνέχιση της υπηρεσίας που ζητήθηκε.

Από την άλλη μεριά μπορεί να ζητηθεί η MM σύνδεση από το CM στην πλευρά του δικτύου. Αυτό επιτυγχάνεται κάνοντας το UE να εγκαταστήσει σύνδεση MM μέσω της paging procedure.

Αφού εγκατασταθεί μπορεί να χρησιμοποιηθεί από το ημιεπίπεδο CM για μεταφορά πληροφοριών. Κάθε CM έχει την δική του MM σύνδεση. Αυτές οι διαφορετικές MM συνδέσεις βρίσκονται και αναγνωρίζονται στο Protocol Discriminator (PD) και στο Transaction Identifier (TI).

Οι κοινές procedures MM μπορεί να χρησιμοποιηθούν οποιαδήποτε στιγμή καθώς οι MM συνδέσεις είναι ενεργές. Αυτές οι procedures χρησιμοποιούνται κυρίως για λειτουργίες ασφάλειας όταν η ταυτότητα και η θέση του UE είναι γνωστή από το CN και η MM σύνδεση υπάρχει από το CN στο UE.

Οι κυριότερες MM common procedures είναι:

- **TMSI reallocation procedure:** χρησιμοποιείται για να παρέχει εμπιστευτικά την ταυτότητα του χρήστη π.χ. για να προστατεύσει τον χρήστη από το να αναγνωρίζεται και να τοποθετείται από ένα εισβολέα. Σε αυτή τη procedure η TMSI τοποθετείται από το MSC/VLR για χρήστη μέσα

στις procedures του radio interface και είναι προσωρινή αντί για μόνιμη. Αναγνωρίζεται από το CN και παράγει συνήθως στο ciphered mode.

- **Authentication procedure:** επιτρέπει στο CN να ελέγχει αν η ταυτότητα που παρέχεται από το UE είναι αποδεκτή ή όχι, και παρέχει παραμέτρους που κάνουν ικανό το USIM να υπολογίζει νέα ciphering και integrity κλειδιά. Σε μια πρόκληση UMTS, η procedure αυτή επιτρέπει στο UE να ελέγξει την αυθεντικότητα του CN. Αυτό δείχνει, π.χ. την ανίχνευση ενός λάθους σταθμού βάσης. Η authentication procedure πάντα αναγνωρίζεται από το CN.

- **Identification procedure:** Χρησιμοποιούνται από το CN για να ζητήσει από το UE να παρέχει ειδικές παραμέτρους αναγνώρισης στα δίκτυα όπως το IMSI και IMEI.

- **IMSI detach procedure:** αναγνωρίζεται από το UE όταν το UE είναι ανενεργό ή αν το USIM είναι detached απο το ME. Κάθε UMTS δίκτυο μπορεί να κάνει broadcast μια σημαία με τις πληροφορίες συστήματος για να δείξει αν η detach procedure απαιτείται από τα UEs. Όταν λαμβάνεται ένα μήνυμα MM IMSI DETACH INFORMATION, το δίκτυο μπορεί να θέσει μια μη ενεργή indication για το IMSI. Καμιά απάντηση δεν επιστρέφεται από το UE. Μετά από το δίκτυο πρέπει να απελευθερώσει τοπικά μια οποιαδήποτε ongoing σύνδεση MM και να ξεκινήσει τη φυσιολογική σύνδεση σηματοδοσίας απελευθερώνει τις procedures.

- **Abort procedure:** Χρησιμοποιείται από το CN για να σταματήσει οποιαδήποτε εγκατάσταση ongoing σύνδεσης MM ή των ήδη εγκατεστημένων συνδέσεων MM εξαιτίας της αποτυχίας του δικτύου ή να έχει βρει ένα παράνομο ME.

Οι MM specific procedures διαχειρίζονται μηνύματα που χρησιμοποιείται στις procedures αναβάθμισης της θέσης. Υπάρχουν 3 μεταβλητές της βασικής procedures που αναβαθμίζει τη θέση:

- **Normal Location updating procedure:** για την περίπτωση που το UE έχει ανιχνεύσει ότι η περιοχή τοποθέτησης αλλάζει και είναι απαραίτητο να ενημερώσει το CN σχετικά με τη νέα κατεύθυνση. Η ανίχνευση γίνεται ελέγχοντας τη Location Area Identifier (LAI) που μεταδίδονται από το δίκτυο ενάντια στη πρόσφατη LAI τιμή που είναι αποθηκευμένη στο USIM. Η procedure αυτή πρέπει να ξεκινά αν το δίκτυο δείχνει ότι το UE είναι άγνωστο στο VLR στην απάντηση στο αίτημα υπηρεσίας. Το UE πρέπει να διατηρεί μια λίστα των “απαγορευμένων τοποθεσιών roaming” στο USIM βασιζόμενοι στα αποτυχημένα αιτήματα αναβάθμισης θέσης.

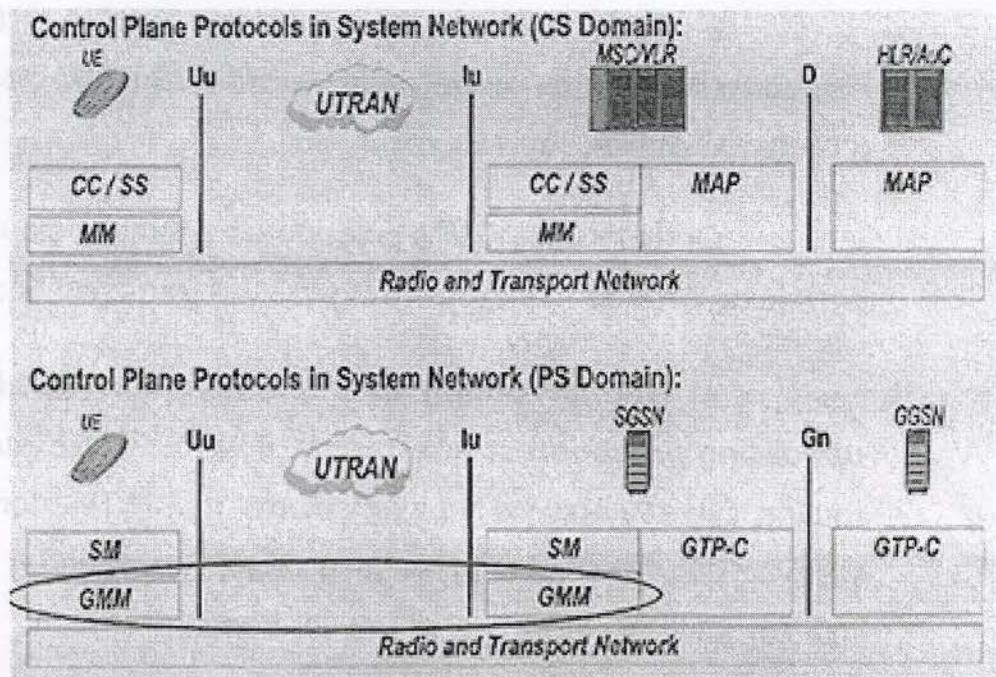
- **Periodic Location Upadating procedure:** χρησιμοποιείται για να τονίσει περιοδικά την ικανότητα και την τοποθεσία του UE στο CN σύμφωνα με τον μετρητή στο UE. Η τιμή λήξης του χρόνου γι’ αυτόν τον μετρητή λαμβάνεται από το block των broadcasted πληροφοριών του συστήματος.

- **IMSI attach procedure:** γίνεται όταν το UE εισάγεται (ή ανάβει) στο δίκτυο στην ίδια περιοχή τοποθεσίας, όπου είχε νωρίτερα detached, π.χ. όταν η τιμή LAI broadcasted στο πρόσφατο κελί ανιχνεύεται για να είναι ίδιο στην τιμή LAI στο USIM.

9.5.1.2 GPRS Mobility Management for Ps Domain (GMM)

Το GMM λειτουργεί μεταξύ του UE και του SGSN (Εικόνα 121). Όπως το MM πρωτόκολλο, το GMM χρησιμοποιεί μια σύνδεση σηματοδότησης μεταξύ του UE και του SGSN. Το GMM στην πλευρά SGSN

πρέπει να συνεργάζεται εσωτερικά με το GTP-U για ανταλλαγή πληροφοριών θέσης.



Εικόνα 121 MM non-access stratum πρωτόκολλα για το PS domain

Για τις υπηρεσίες πακέτων δεδομένων είναι σημαντικό να γίνεται μια διάκριση μεταξύ της κατάστασης, όταν το UE μαζί με την ταυτότητα του και την θέση του είναι γνωστό από το CN PS domain και την κατάσταση όταν δεν είναι γνωστή. Η σημαντικότητα έρχεται από το γεγονός ότι τα πακέτα δεδομένων προστατεύονται με κωδικοποίηση που κάνει χρήση τα ειδικά κλειδια-χρήστες. Ο διαχωρισμός γίνεται από το GMM. Όταν ο χρήστης είναι γνωστός στο CN PS domain δίκτυο το GMM υπάρχει, διαφορετικά δεν υπάρχει.

Οι procedures GMM για ειδική εγκατάσταση και απελευθέρωση του GMM context είναι:

- **GPRS attach and combined GPRS attach procedures:** χρησιμοποιούνται για να δείξουν την ταυτότητα του χρήστη (P-TMSI) και την πρόσφατη περιοχή routing στο δίκτυο και να εγκαταστήσει ένα GMM

για τον χρήστη. Μια τυπική κατάσταση για να εκτελεστεί αυτή η procedure είναι όταν ο κόμβος πακέτων του UE ανάβει ή το USIM εισάγεται σε αυτό.

- **GPRS detach or combined GPRS detach procedures:** ενεργοποιούνται όταν το UE είναι κλειστό ή το USIM αφαιρείται από το UE ή το δίκτυο αποτυγχάνει να εμφανιστεί.

Οι ακόλουθες GMM procedures χρησιμοποιούνται για την τοπική διαχείριση όταν το περιεχόμενο ενός GMM υπάρχει ήδη:

- **Normal routing area updating and combined routing area updating procedures:** εκτελούνται όταν το UE αναγνωρίζει ότι η περιοχή routing έχει αλλάξει για να ενημερώσει το CN PS domain σχετικά με το γεγονός. Στην combined routing area updating η τοποθεσία θέσης περιλαμβάνεται επίσης για το CN CS domain.

- **Periodic routing area updating procedures:** μπορεί να χρησιμοποιείται για να τονίσει περιοδικά την διαθεσιμότητα του UE στο CN σύμφωνα με τον χρονομετρητή στο UE.

Οι ακόλουθες GMM common procedures για λόγους ασφαλείας μπορεί να χρησιμοποιούνται όταν το GMM context για τον χρήστη έχει εγκατασταθεί.

- **P-TMSI re-allocation:** παρέχει μια προσωρινή random αναγνώριση, packet – TMSI για χρήση μέσα στις ραδιο interface procedures αντί για μόνιμη αναγνώριση IMSI.

- **APRS authentication and chiphering procedure:** εφαρμόζεται πάντα από το CN, επιτρέπει στο CN να ελέγχει αν η ταυτότητα που παρέχεται από το UE είναι αποδεκτή. Επίσης, παρέχει παραμέτρους που κάνουν ικανό το USIM να υπολογίζει το UMTS

chiphering και τα κλειδιά integrity πιτρέπει στο UE να κάνει το CN ανθεκτικό.

- **GPRS identification procedure:** χρησιμοποιείται από το CN PS domain να ζητά από το UE να παρέχει ειδικές παραμέτρους αναγνώρισης στα δίκτυα όπως το IMSI και IMEI.

Μια ακόμα GMM procedure χρειάζεται για να παρέχει υπηρεσίες στο CM ημιεπίπεδο στην κορυφή του GMM πρωτοκόλλου.

- **A service request procedure:** εφαρμόζεται από το UE, και χρησιμοποιείται για να εγκαταστήσει μη ασφαλή σύνδεση στο δίκτυο και / ή να ζητήσει την εγκατάσταση bearer για αποστολή δεδομένων. Η procedure αυτή χρησιμοποιείται τυπικά όταν το UE έχει ένα τέτοιο μήνυμα σηματοδότησης (π.χ. SM ή μήνυμα απάντησης paging) ή πακέτα δεδομένων, που απαιτούν προστασία ασφάλειας να σταλούν.

Περισσότερες πληροφορίες σχετικά με το GMM μπορούν να βρεθούν στο 3GPP TS 24.008.

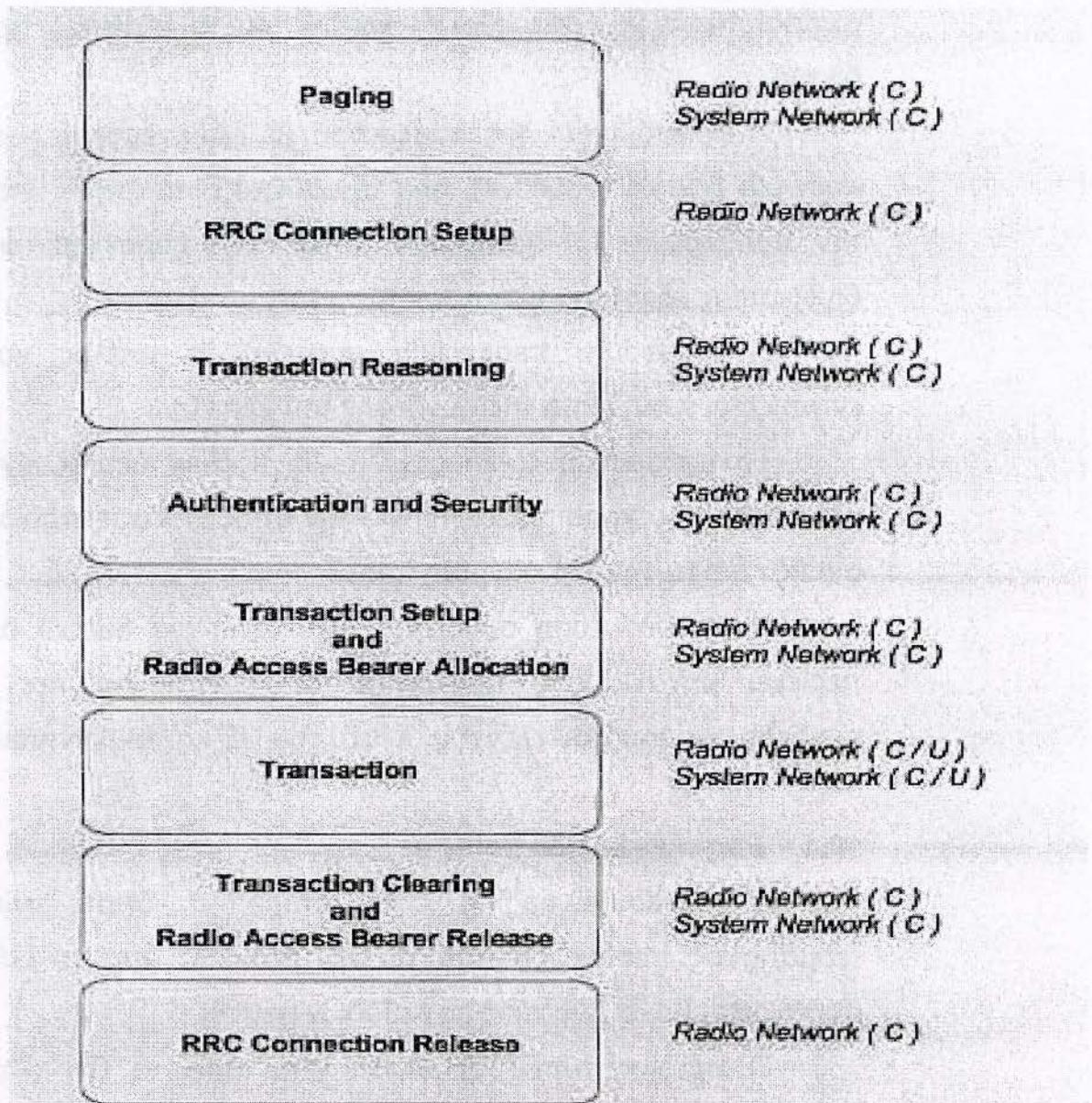
ΚΕΦΑΛΑΙΟ 10 Παραδείγματα εφαρμογών

10.1 Εισαγωγή

Το signaling της μετάδοσης είναι πάντοτε απαραίτητο και η μεταφορά των δεδομένων των χρηστών χρειάζεται σε πολλές εσωτερικές λειτουργίες (transactions). Οι λειτουργίες του radio network καλούνται όποτε είναι απαραίτητες οι υπηρεσίες πρόσβασης σε δίκτυο εντός μιας βασικής procedure. Ο συνολικός έλεγχος των transactions συστήματος πραγματοποιείται από τα πρωτόκολλα συστήματος δικτύου, που κατανέμουν ιεραρχικά τις θεμελιώδεις procedures και καθορίζουν την πρόοδο της transaction.

Το paging είναι μια διαδικασία mobility management που χρησιμοποιείται κατά την αναζήτηση συγκεκριμένου συνδρομητή (subscriber) από την ευρύτερη περιοχή δικτύου. Αυτή η διαδικασία εκτελείται μόνο όταν η transaction προέρχεται από την πλευρά του δικτύου. Τα υπόλοιπα 7 βήματα παραμένουν ίδια είτε η transaction προέρχεται είτε τερματίζεται από το UE. Η εγκατάσταση του Radio Resource Control-RRC, είναι μία βασική procedure που περιέχει δραστηριότητες και ροή μηνυμάτων που αποβλέπουν στην πραγματοποίηση σύνδεσης ασύρματου ελέγχου (radio control connection) μεταξύ του τερματικού και του δικτύου ασύρματης πρόσβασης. Οι λεπτομέρειες αυτής της διαδικασίας ποικίλλουν ανάλογα με την περίπτωση.

Βασικά κάθε transaction δικτύου μπορεί να διαιρεθεί σε 8 βήματα όπως παρουσιάζεται στην παρακάτω εικόνα 122.



Εικόνα 122 Βασικό μοντέλο της transactions του UMTS δικτύου

Το transaction reasoning είναι μια βασική procedure, κατά την οποία το τερματικό υποδεικνύει στο κεντρικό δίκτυο (Core Network-CN) ποιο είδος transaction απαιτείται. Βασισμένο στις πληροφορίες αυτές, το CN καθορίζει αν θα συνεχίσει με την transaction ή αν θα τερματίσει την εκτέλεσή της. Συνήθως, μετά από αυτά τα στάδια, ακολουθεί η διαδικασία αυθεντικοποίησης ταυτότητας και ασφάλειας (authentication and security procedure). Αυτή η βασική procedure εξακριβώνει την μεταξύ των UMTS subscribers και του δικτύου επικοινωνία κι έπειτα ενεργοποιεί τους

απαραίτητους μηχανισμούς ασφάλειας για τη σύνδεση πρόσβασης στο δίκτυο.

Η εγκατάσταση της transaction με radio access bearer allocation είναι μία βασική procedure που προσδιορίζει τις πηγές επικοινωνίας για την transaction. Γι' αυτόν τον λόγο, τα χαρακτηριστικά αυτής της διαδικασίας εξαρτώνται από τον τύπο της.

Η procedure transaction αποτελεί το σκέλος κατά το οποίο εντοπίζεται η οντότητα της σύνδεσης του χρήστη.

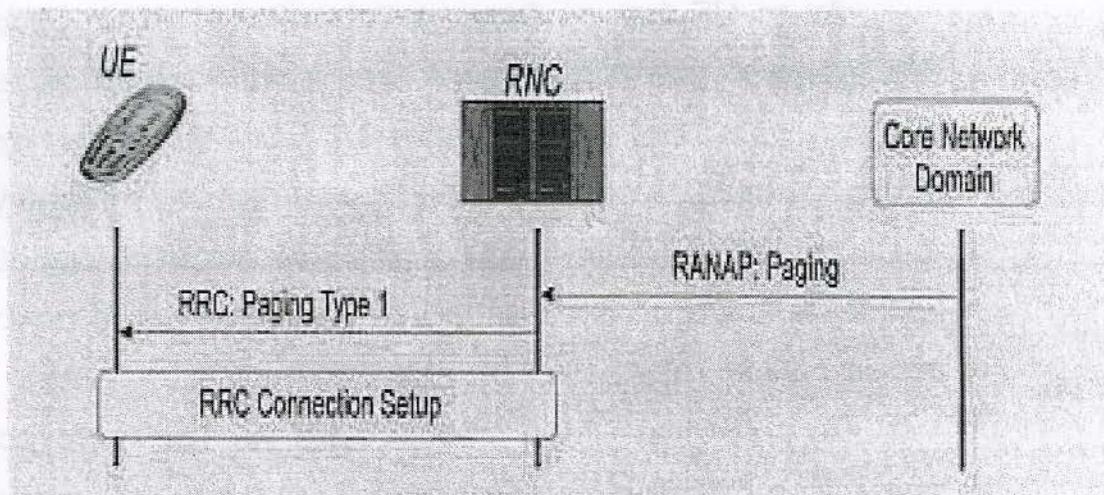
Το transaction clearing με radio access bearer είναι μία βασική procedure που χρησιμοποιείται για την αποδέσμευση πόρων δικτύου που σχετίζονται με τη συγκεκριμένη transaction.

Η αποδέσμευση σύνδεσης RRC είναι μία βασική διαδικασία που περιέχει μηχανισμούς που χρησιμοποιούνται για την αποδέσμευση σύνδεσης ασύρματου ελέγχου μεταξύ του UE και του δικτύου πρόσβασης.

10.1.1 Paging - Σελιδοποίηση

Η procedure paging, είναι απαραίτητη όποτε πραγματοποιείται τερματισμός transaction από το UE. Αντίθετα από το GSM, το UMTS συμπεριλαμβάνει δύο τύπους μεθόδων paging.

Ο πρώτος τύπος χρησιμοποιείται από τα CN (Core Networks) domains και αποτελεί τον «συμβατικό» (conventional) τρόπο χρήσης του paging. Το paging είναι μέρος της οντότητας/στοιχείου του ελέγχου ασύρματου δικτύου και επιτυγχάνεται μέσω του lu interface με τη χρήση μηνύματος RANAP (Paging message). Το CN domain κατά τη διαδικασία του paging, το αποστέλλει στα Las/RAs στα οποία υπήρξε η τελευταία αναφορά του UE.



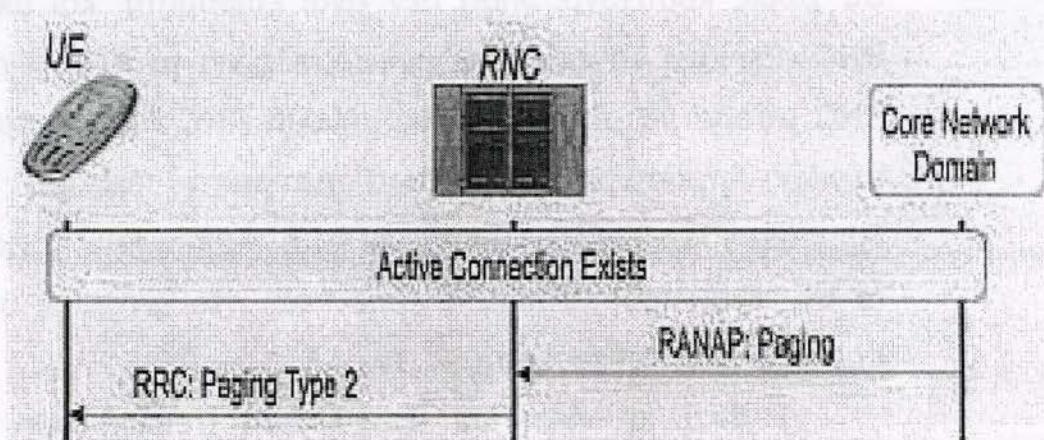
Εικόνα 123 Paging Type 1

Ένα μήνυμα RANAP περιλαμβάνει δύο βασικές παραμέτρους, το απαιτούμενο CN domain και το IMSI. Από πλευράς ασφάλειας συστήματος, η μη απαραίτητη μεταφορά IMSI εντός του σημείου αναφοράς Uu χωρίς κρυπτογράφηση δεν είναι επιθυμητή, και ως αποτέλεσμα το RNC αδυνατεί να εκτελέσει μετατροπές για το IMSI. Για παράδειγμα, το RNC μπορεί να αποστείλει ένα μήνυμα RRC Paging πρώτου τύπου που περιέχει προσωρινή ταυτότητα ασύρματο δικτύου (Radio Network Temporary Identity-RNTI) αντί του IMSI. Αυτή η λειτουργία, ανατίθεται όταν το UE είναι προσκολλημένο (attached) στο δίκτυο ή όταν εκτέλεσε την προηγούμενη transaction.

Τυπικά, η λήψη και αναγνώριση (receipt and recognition) του πρώτου τύπου μηνύματος (RRC Paging Type 1) από το UE, οδηγεί στην πραγματοποίηση σύνδεσης RRC που είναι απαραίτητη για τη συνέχιση της transaction που ξεκίνησε από το paging. Επιπρόσθετα στην προαναφερόμενη χρήση, το RRC Paging Type 1, έχει ορισμένες συγκεκριμένες χρήσεις RAN. Όταν το UE δεν είναι σε κατάσταση idle (idle mode) και αλλάζει τις παραμέτρους πληροφοριών συστήματος που είναι απαραίτητο να γνωστοποιηθούν, το RNC μπορεί να χρησιμοποιήσει RRC Paging Type 1 για να «αφυπνίσει» το UE έτσι ώστε να διαβάσει τις παραλλαγμένες νέες πληροφορίες συστήματος ή συγκεκριμένα μέρη τους.

Αν το UE έχει σύνδεση packet switched χωρίς δραστηριότητα, το RNC χρησιμοποιεί RRC Paging Type 1 για να ενημερώσει το UE ότι η σύνδεση χρειάζεται να ενεργοποιηθεί ξανά. Σε αυτήν την περίπτωση, υπάρχουν ορισμένα πακέτα δεδομένων τα οποία πρόκειται να παραδώσει το CN στο UE. Αυτό, υποχρεώνει το UE να εκτελέσει αναβάθμιση cell (cell update) κι έπειτα το RNC μπορεί να δρομολογήσει τα πακέτα δεδομένων στο κατάλληλο UE.

Τα τερματικά UMTS προορίζονται για την ταυτόχρονη διαχείριση ποικίλων συνδέσεων, καθώς μπορεί να έχουν περισσότερες από μία συνδέσεις με CN domains. Όταν το UE έχει ήδη σύνδεση με ένα CN domain και πραγματοποιείται άλλη μια σύνδεση με το ίδιο domain, το CN στέλνει μήνυμα RANAP Paging όπως και στις άλλες περιπτώσεις. Το paging που δέχτηκε το UE από το SRNC είναι τώρα δευτέρου τύπου (RRC Paging Type 2).



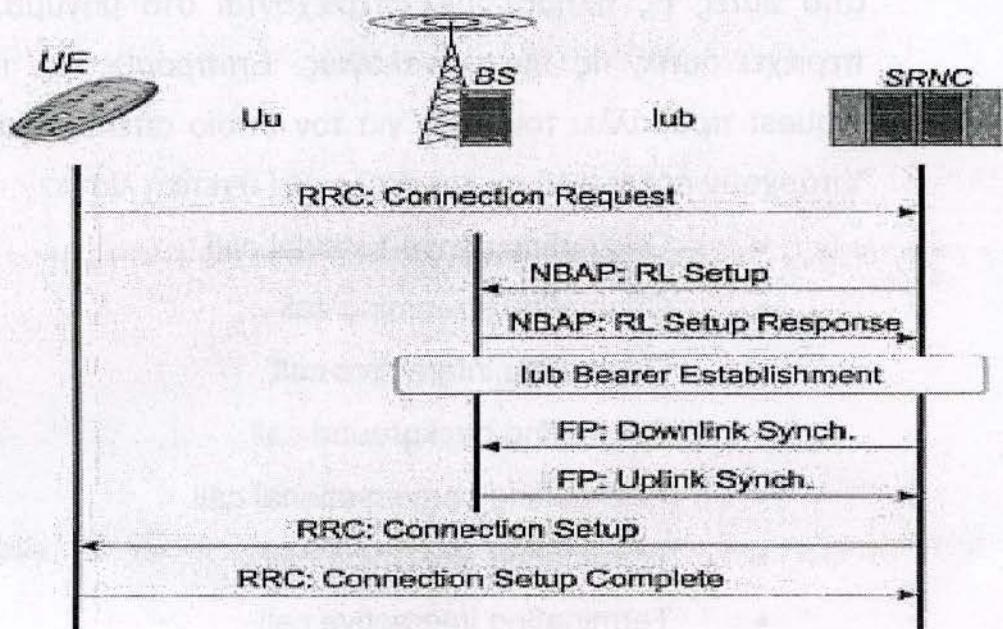
Εικόνα 124 Paging Type 2

Ο διαχωρισμός μεταξύ πρώτου και δευτέρου τύπου paging γίνεται εντός του RNC, με το μήνυμα RANAP να εμφανίζεται όμοιο. Η διαφορά όμως εντοπίζεται στο ότι το Type 1 χρησιμοποιείται για paging στα UEs που βρίσκονται σε idle mode, cell-PCH ή URA-PCH κατάσταση, που σημαίνει ότι μπορεί να χρησιμοποιηθεί είτε για συγκεκριμένα UEs είτε για όλα τα UEs εντός cell. Από την άλλη πλευρά, το Type 2 χρησιμοποιείται

για UEs που βρίσκονται σε κατάσταση cell-DCH ή cell-FACH, οπότε αφιερώνεται και αποστέλλεται σε ένα μόνο UE.

10.1.2. Εγκατάσταση της σύνδεσης της RRC Connection

Στην εικόνα 125 βλέπουμε την ιεραρχία της ασύρματης σύνδεσης μεταξύ του UE και του RNC όπως πραγματοποιείται μέσω του Uu interface και του εσωτερικού interface πρόσβασης σε domain Iub (access domain internal interface Iub).



Εικόνα 125 Εγκατάσταση σύνδεσης RRC

Η εγκατάσταση της σύνδεσης RRC ξεκινάει πάντα από το UE με το μήνυμα αίτησης σύνδεσης (RRC Connection Request) που αποστέλλεται μέσω κοινού καναλιού ελέγχου (Common Control Channel-CCCH). Το CCCH κατά το uplink, ακολουθεί τυχαία πρόσβαση (random access) και στην πραγματικότητα το απαιτούμενο περιεχόμενο της σύνδεσης RRC προέρχεται από το UE μέσω φυσικού RACH ως αποτέλεσμα της αρχικής διαδικασίας πρόσβασης. Αυτό το μήνυμα καταφτάνει στο RNC μέσω της θύρας (data port) Iub RACH. Κατά τη λήψη του συγκεκριμένου μηνύματος, το RRC απ' την πλευρά του RNC αλλάζει την κατάστασή του από idle

mode σε Connected Cell-FACH ή Cell-DCH. Έπειτα, το RNC επικοινωνεί με το UE μέσω κοινών καναλιών ελέγχου (common control channels) από τα οποία τα χρησιμοποιημένα είναι FACH και RACH. Το μήνυμα αίτησης σύνδεσης RRC (RRC connection request message) περιέχει πολυάριθμες πληροφορίες σχετικά με την απαιτούμενη ασύρματη σύνδεση, όπως είναι η ταυτότητα του τερματικού ή του συνδρομητή, όπου το UE στέλνει στο δίκτυο IMSI ή TMSI, IMEI, location area identity και routing area identity.

Το μήνυμα αίτησης σύνδεσης RRC πρέπει να προσδιορίζει ποιες από αυτές τις πληροφορίες περιέχονται στο μήνυμα, όπως επίσης να περιέχει αυτές τις τιμές αναλόγως. Επιπροσθέτως, η RRC connection request προβάλλει τον λόγο για τον οποίο αιτείται η ασύρματη σύνδεση. Υπάρχουν αρκετοί λόγοι και ακολουθεί σχετική λίστα:

- Originating conversational call
- Originating streaming call
- Originating interactive call
- Originating background call
- Terminating conversational call
- Terminating streaming call
- Terminating interactive call
- Terminating background call
- Emergency call
- High priority signaling
- Low priority signaling
- Call re-establishment

Όπως φαίνεται στη λίστα, η RRC connection request προβάλλει τα ερωτήματα που θα προκύψουν καθώς θα προχωράει η transaction. Η κλήση ανάγκης (emergency call) διαχωρίζεται καθώς θα αντιμετωπιστεί διαφορετικά από το δίκτυο σε σχέση με τις συνηθισμένες transactions.

Ανάλογα με την αιτία της αίτησης, το RNC καθορίζει αν θα διαθέσει αποκλειστικούς ή κοινούς πόρους σε αυτήν την transaction. Στα πλαίσια αυτού του διαχωρισμού, το SRNC διανέμει RNTI και άλλους πόρους σε αυτήν την transaction.

Το interface Iub καλείται όταν το RNC στέλνει μήνυμα εγκατάστασης ασύρματης σύνδεσης NBAP (NBAP radio link set-up message) στο BS. Το μήνυμα αυτό περιέχει περιγραφή του τύπου (format) μετάδοσης, πληροφορίες κώδικα (code) και ενεργού ελέγχου (power control) που είναι κρυπτογραφικός κώδικας για το WCDMA-FDD κατά το uplink. Το BS επιβεβαιώνει τη λήψη αυτού του μηνύματος στέλνοντας μήνυμα ανταπόκρισης (NBAP radio link set-up response message). Αυτό το μήνυμα ενημερώνει το RNC δίνοντας πληροφορίες σχετικά με τα επίπεδα μετάδοσης (transport layer addressing information-AAL2 address) και την τοποθέτηση/ανάθεση φορέα Iub (establishment of an Iub bearer) στο δίκτυο μετάδοσης.

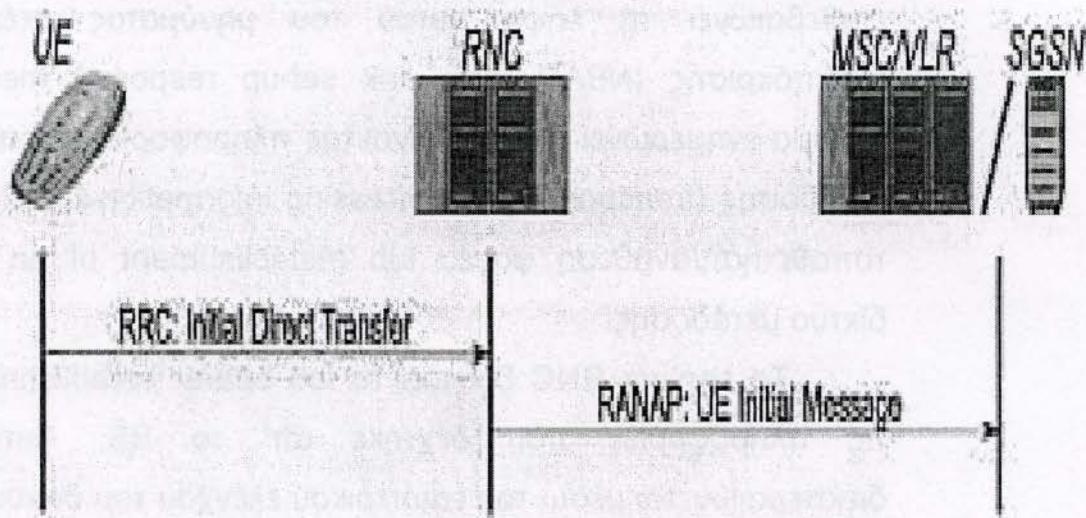
Το serving RNC ξεκινάει το Iub bearer establishment σύμφωνα με τις πληροφορίες που δέχτηκε απ' το BS. Αυτή η διαδικασία διεκπεραιώνεται μέσω του εσωτερικού ελέγχου του δικτύου μετάδοσης του Iub interface. Ο Iub bearer (φορέας) που προκύπτει, είναι συνδεδεμένος με το DCH (Dedicated Channel-αποκλειστικό κανάλι) που έχει ανατεθεί στην transaction. Έπειτα, το πρωτόκολλο σύνδεσης στο Iub συγχρονίζεται με την ανταλλαγή μηνυμάτων. Αν υποθέσουμε ότι έχουμε στήσει μία αποκλειστικής χρήσης ασύρματη σύνδεση (dedicated radio connection) που χρησιμοποιεί DCH, τότε στο Iub αντιστοιχεί το (frame) πρωτόκολλο αποκλειστικού καναλιού.

Όταν είναι έτοιμη η επικοινωνία Iub, το RNC στέλνει στο UE μήνυμα εγκατάστασης σύνδεσης RRC (RRC connection setup message) χρησιμοποιώντας κοινό κανάλι ελέγχου (common control channel) – στη συγκεκριμένη περίπτωση FACH. Με αυτό το μήνυμα, το SRNC ενημερώνει το UE σχετικά με το τύπο μετάδοσης, power control και κώδικες (codes)

που στην περίπτωση του WCDMA-FDD αποτελεί κρυπτογραφικό κώδικα downlink. Το UE επιβεβαιώνει την πραγματοποίηση της σύνδεσης RRC στέλνοντας μήνυμα ολοκλήρωσής της (RRC connection setup complete).

10.1.3. Transaction Reasoning

Μετά την ολοκλήρωση της σύνδεσης RRC, το UE στέλνει μήνυμα άμεσης αρχικής μετάδοσης (RRC initial direct transfer). Αυτή η λειτουργία μεταφέρει (φορτίο) το πρώτο μήνυμα του συστήματος δικτύου της transaction από το UE προς το δίκτυο.



Εικόνα 126 Transaction Reasoning

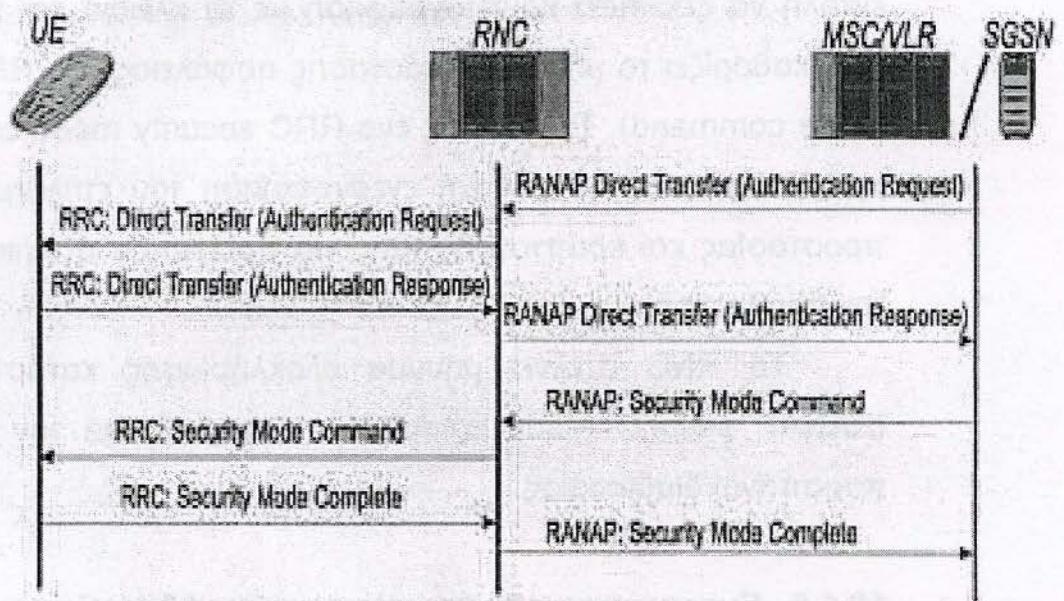
Κατά τη λήψη των παραπάνω πληροφοριών, το RNC προσθέτει μερικές ακόμα παραμέτρους και τις αποστέλλει στο κατάλληλο CN domain με τη μορφή RANAP UE initial message. Το μήνυμα αυτό φέρει τα περιεχόμενα του αρχικού μηνύματος RRC direct transfer μαζί με το πρώτο μήνυμα συστήματος δικτύου (system network message) από το UE.

Τα περιεχόμενα του αρχικού μηνύματος από το UE (UE initial message) παρέχουν στο CN πολυάριθμες πληροφορίες σχετικά με την transaction που εκκίνησε το UE. Μεταξύ αυτών των πληροφοριών είναι η υποτιθέμενη ταυτότητα του συνδρομητή UMTS (IMSI ή TMSI), η δικτυακή περιοχή του και το είδος της transaction που απαιτείται. Όλες αυτές οι

πληροφορίες χρησιμοποιούνται από το CN για τον προσδιορισμό της πορείας έπειτα από το αίτημα (request) transaction.

10.1.4. Έλεγχος εξακρίβωσης και ασφάλειας

Κατά τη διάρκεια της σύνδεσης RRC το UE ενημερώνει το RNC σχετικά με τη UE classmark parameter και για τις δυνατότητές της σε πολλούς τομείς, ένας απ' τους οποίους είναι οι αλγόριθμοι ασφάλειας που υποστηρίζονται από το UE.



Εικόνα 127 Έλεγχος εξακρίβωσης και ασφάλειας

Το UE και το δίκτυο αναγνωρίζονται μεταξύ τους στέλνοντας μήνυμα αίτησης επιβεβαίωσης (authentication request message) που περιέχεται στο φορτίο (πακέτο δεδομένων) των μηνυμάτων άμεσης μετάδοσης του RANAP και RRC προς το UE (direct transfer messages). Μετά την εκτέλεση των αλγόριθμων επιβεβαίωσης στο USIM, το UE ανταποκρίνεται με authentication response message (ανταπόκριση) που περιέχεται πάλι στα RNC και RANAP direct transfer messages. Σε αυτήν την περίπτωση το RNC συμπεριφέρεται ως κόμβος (relay) που αναλαμβάνει την

αποστολή των περιεχομένων του RANAP direct transfer στο RNC direct transfer και το αντίστροφο.

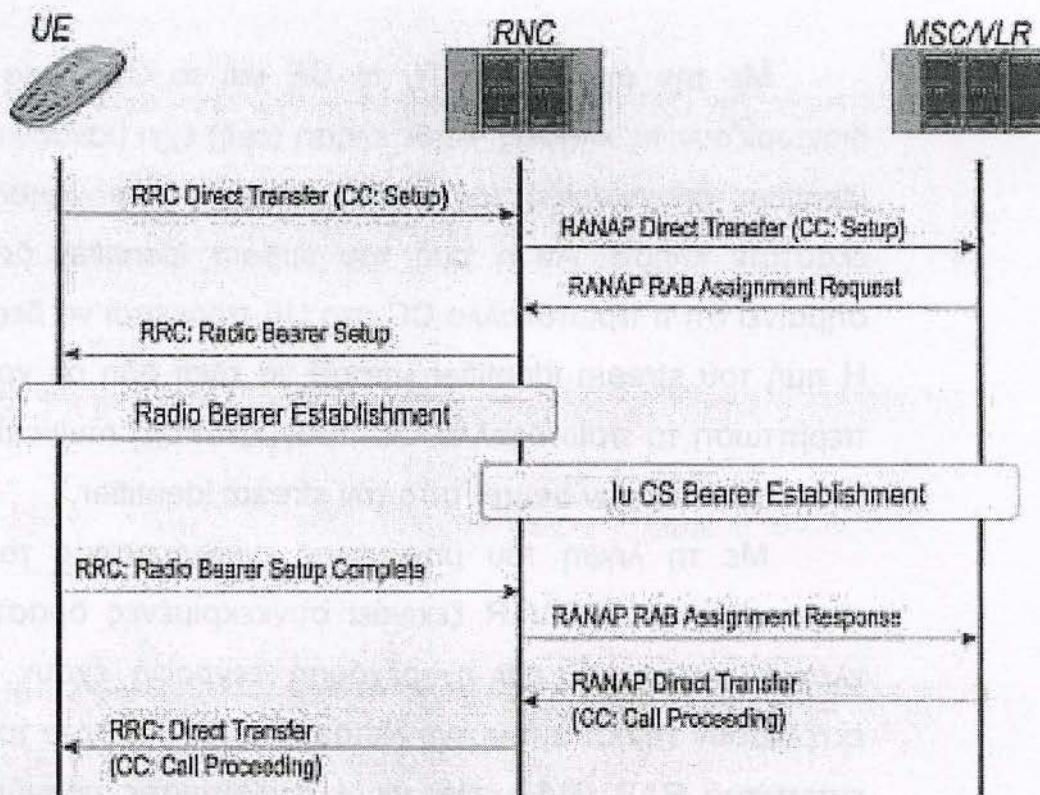
Με ένα μήνυμα κατάστασης ασφάλειας (RANAP security mode command message) το σχετιζόμενο CN domain αναφέρει στο UTRAN ότι η transaction θα χρειαστεί κρυπτογράφηση. Το μήνυμα αυτό περιέχει τους επιλεγμένους αλγόριθμους και παραδίδει τα κλειδιά ακεραιότητας και κρυπτογράφησης (integrity and encryption keys) στο UTRAN.

Βασιζόμενο σε αυτές τις πληροφορίες, το RNC στέλνει στο UE εντολή να ξεκινήσει κρυπτογράφηση με τα κλειδιά και τους αλγόριθμους που καθορίζει το μήνυμα κατάστασης ασφάλειας του RRC (RRC security mode command). Στέλνοντας ένα RRC security mode complete message το UE δηλώνει την επιτυχή ενεργοποίηση του επιλεγμένου αλγόριθμου προστασίας και κρυπτογράφησης για προστασία ή επικοινωνία σε αυτήν την transaction.

Το RNC στέλνει μήνυμα ολοκλήρωσης κατάστασης ασφάλειας (RANAP security mode complete message) μετά την ολοκλήρωση της παραπάνω διαδικασίας.

10.1.5. Εγκατάσταση transaction με την Allocation του Radio Access Bearer (RAB)

Έως τώρα, τα περιεχόμενα των βασικών procedures υπήρξαν παρόμοια και εξαρτώμενα από τα CN domains. Η εγκατάσταση μίας transaction με radio access bearer allocation είναι το πρώτο τμήμα όπου πρέπει να ληφθεί υπόψη η διαφορετική φύση των CN domains.



Εικόνα 128 Εγκατάσταση transaction με την Allocation του Radio Access Bearer (RAB) (Circuit Switched)

Στην περίπτωση των circuit switched transactions οι πληροφορίες εγκατάστασης μεταδίδονται μέσω μηνυμάτων άμεσης μεταφοράς (RRC/RANAP direct transfer messages). Αυτά, μπορεί να περιέχουν το μήνυμα εγκατάστασης ελέγχου κλήσης (Call Control –CC- setup message), το οποίο αναγνωρίζει την transaction και υποδεικνύει τις προδιαγραφές QoS, π.χ. το είδος του φορέα που απαιτείται για την εκάστοτε υπηρεσία με τις ακόλουθες παραμέτρους:

- Transaction identifier (TI)
- Stream identifier
- Traffic class
- Asymmetry indicator
- Maximum bitrate
- Guaranteed bitrate

Με την παράμετρο TI, το UE και το CN node είναι σε θέση να διαχωρίζουν τις κλήσεις. Κάθε κλήση (call) έχει μοναδική τιμή TI. Ο stream identifier αναγνωρίζει τον φορέα (bearer) που χρησιμοποιείται για την εκάστοτε κλήση. Αν η τιμή του stream identifier δεν υπάρχει ακόμα, σημαίνει ότι το πρωτόκολλο CC στο UE πρόκειται να δεσμεύσει νέο bearer. Η τιμή του stream identifier μπορεί να είναι ήδη σε χρήση. Σε αυτήν την περίπτωση το πρωτόκολλο CC πραγματοποιεί multicall χρησιμοποιώντας έναν προϋπάρχον bearer από τον stream identifier.

Με τη λήψη του μηνύματος εγκατάστασης του CC (CC set-up message) το MSC/VLR ξεκινάει συγκεκριμένες δραστηριότητες. Αρχικά, ελέγχει αν το UE και η τρέχουσα εγγραφή έχουν τη δυνατότητα να εκτελέσουν την απαιτούμενη λειτουργία. Αν ναι, τότε το MSC/VLR ξεκινάει εντοπισμό RAB (RAB allocation) αναθέτοντας μοναδική ταυτότητα RAB (unique RAB ID) και καλώντας ένα RAB με δεδομένες παραμέτρους QoS προς εγκατάσταση στέλνοντας μέσω του lu interface το μήνυμα RANAP RAB assignment request.

Με τη λήψη του προαναφερθέντος μηνύματος, το RNC ξεκινάει δραστηριότητες για προσδιορισμό ασύρματου φορέα (radio bearer allocation) ελέγχοντας πρώτα αν υπάρχουν αρκετοί διαθέσιμοι πόροι για την πλήρωση της απαιτούμενης QoS. Αν υπάρχουν, πραγματοποιείται ο προσδιορισμός (allocation) του radio bearer σύμφωνα με το μήνυμα αίτησης. Στην αντίθετη περίπτωση, το RNC είτε προχωρεί στο allocation με χαμηλότερες τιμές QoS (lowered QoS values) – για παράδειγμα είναι δυνατή η μείωση του μέγιστου ρυθμού μετάδοσης (bitrate) -, είτε επιλέγει να θέσει την αίτηση (request) σε κατάσταση αναμονής μέχρι να βρεθούν διαθέσιμοι πόροι. Αυτές οι ειδικές περιπτώσεις απαιτούν επιπρόσθετους προσδιορισμούς παραμετροποίησης.

Το RNC ενημερώνει το UE σχετικά με το bearer allocation στέλνοντας μήνυμα RRC radio bearer set-up στο UE. Το UE, με τη λήψη

αυτού του μηνύματος, συνδιάζει τις πληροφορίες που αρχικά στάλθηκαν στο δίκτυο με τον ληφθέντα radio bearer identifier. Έπειτα, το UE μπορεί να οδηγήσει τα δεδομένα χρήστη (User data traffic) στον σωστό radio bearer. Τη στιγμή που το UE μπορεί να λάβει δεδομένα από τον νέο radio bearer, στέλνει στο RNC μήνυμα επιβεβαίωσης ολοκλήρωσης εγκατάστασης radio bearer (RRC radio bearer set-up complete). Το RNC πρέπει επίσης να δεσμεύσει lu bearer για τη νέα transaction.

Έπειτα, το RNC ενημερώνει ότι έγινε προσδιορισμός του RAB στέλνοντας στο MSC/VLR μήνυμα ανταπόκρισης RAB (RANAP RAB assignment response). Οι αλλαγές που μπορεί να έκανε το RNC στις τιμές QoS φαίνονται στο παράπανω μήνυμα.

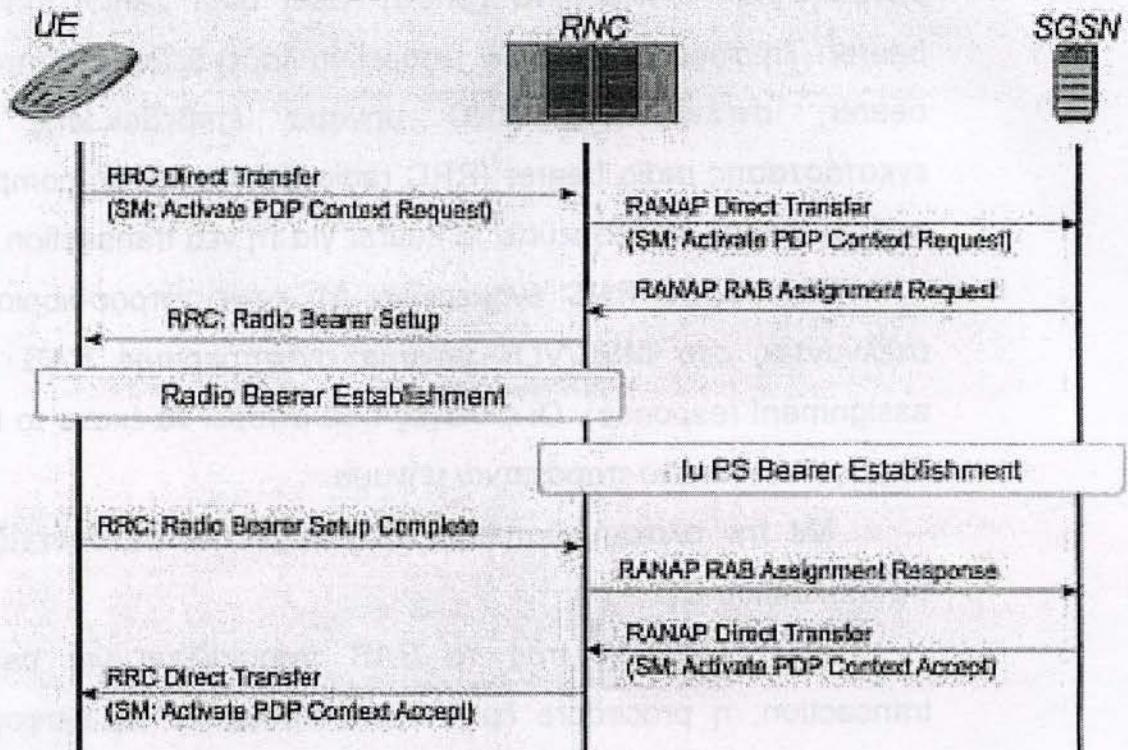
Με την ολοκλήρωση του RAB, η procedure συνεχίζει σε επίπεδο πρωτοκόλλου CC.

Σε περίπτωση που το RAB προορίζεται για packet switched transaction, η procedure εμφανίζεται όμοια, με τις διαφοροποιήσεις να εντοπίζονται εντός των μηνυμάτων. Το UE χρησιμοποιεί τώρα πρωτόκολλο SM αντί του CC. Το UE στέλνει μήνυμα αίτησης ενεργοποίησης περιεχομένου PDP (SM activate PDP context request message) στο δίκτυο ως μήνυμα άμεσης μεταφοράς (RANAP direct transfer) στο SGSN εντός του CN.

Το radio bearer allocation παραπαιτεί σε circuit switched traffic με τη διαφορά να εντοπίζεται στην περιγραφή των του QoS. Για παράδειγμα, το προκαθορισμένο bitrate είναι βασική παράμετρος στην περίπτωση του packet switched RAB αλλά όχι χαρακτηριστική παράμετρος στα circuit switched RABs.

Μετά την υλοποίηση του RAB το CN domain επιβεβαιώνει την packet session establishment με την αποστολή μηνύματος αποδοχής ενεργοποίησης περιεχομένου PDP (SM activate PDP context accept message). Στον τομέα της διαχείρισης management (Session Management – SM) αυτό σημαίνει ότι το SM είναι τώρα ενεργό και τα UE

και CN domain μπορούν να ανταλλάσσουν δεδομένα packet switched (data).



Εικόνα 129 Εγκατάσταση transaction με την Allocation του Radio Access Bearer (RAB) (Packet Switched)

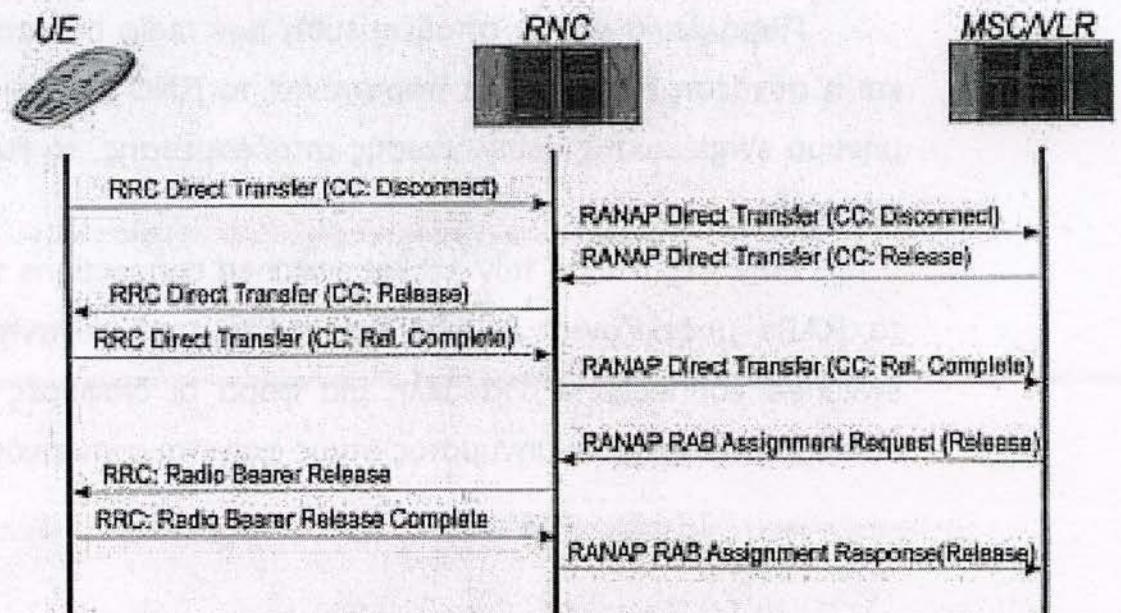
10.1.6 Transaction

ΣΤΙΣ ΠΙΟ ΤΥΠΙΚΕΣ ΠΕΡΙΠΤΩΣΕΙΣ αυτό το στάδιο transaction περιλαμβάνει ενεργή user plane connection. Παραδείγματα αυτού του είδους transactions συναντώνται παρακάτω. Παρ' όλ' αυτά, αν ο σκοπός της request για σύνδεση RRC είναι καθαρά για signalling (προσδιοριστικός) όπως είναι η δραστηριότητα MM (MM activity), δεν είναι απαραίτητοι οι user plane bearers. Αντιθέτως, εδώ χρησιμοποιείται μία signalling connection για τη διεκπαιρέωση της MM activity.

10.1.7 Transaction Clearing και απελευθέρωση του RAB

Αν η transaction είχε ένα user plane ενεργό, το user plane αποσυνδέεται πρώτο. Η διαδικασία αποσύνδεσης εξαρτάται από τον τύπο

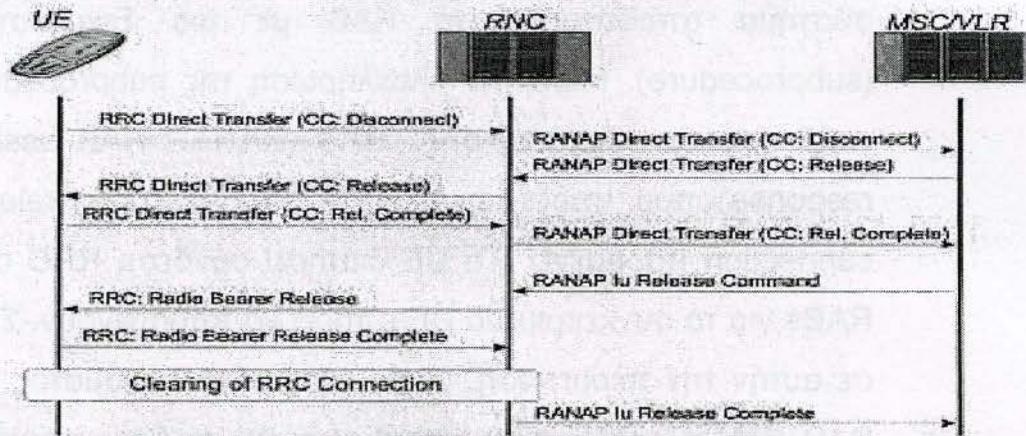
της transaction. Σε αυτήν την περίπτωση το clearing ξεκινάει από το UE αλλά μπορεί και το CN να εκκινήσει την αποσύνδεση του user plane. Γενικότερα, και οι δύο πλευρές μπορούν να καθαρίσουν μια κλήση (normal switched call clearing) και αυτό δεν εξαρτάται από την πλευρά (party) που θα ξεκινήσει την κλήση (call). Μετά την αποσύνδεση του user plane το σύστημα αποδεσμεύει το RAB με μια ξεχωριστή υποδιαδικασία (subprocedure). Μετά την ολοκλήρωση της subprocedure μέσω αίτησης ανάθεσης και ανταπόκρισης RAB (RANAP RAB assignment request - response) που υποδηλώνουν την αποδέσμευση (release), η signalling connection παραμένει. Το UE διατηρεί σύνδεση RRC στο UTRAN και τα RABs για το συγκεκριμένο UE μπορεί να παραμένουν. Σε γενικές γραμμές, σε αυτήν την περίπτωση, μέσω ενός μόνο μηνύματος αίτησης ανάθεσης RAB (RANAP RAB assignment request) το CN μπορεί να δημιουργήσει, σβήσει ή τροποποιήσει RABs.



Εικόνα 130 Transaction Clearing και απελευθέρωση του RAB

Αν όλα τα RABs μεταξύ του UE και του CN domain απελευθερωθούν ταυτόχρονα και οι συσχετισμένοι πόροι (radio resources) αποσυσχετιστούν (deallocation), σημαίνει ότι έχει

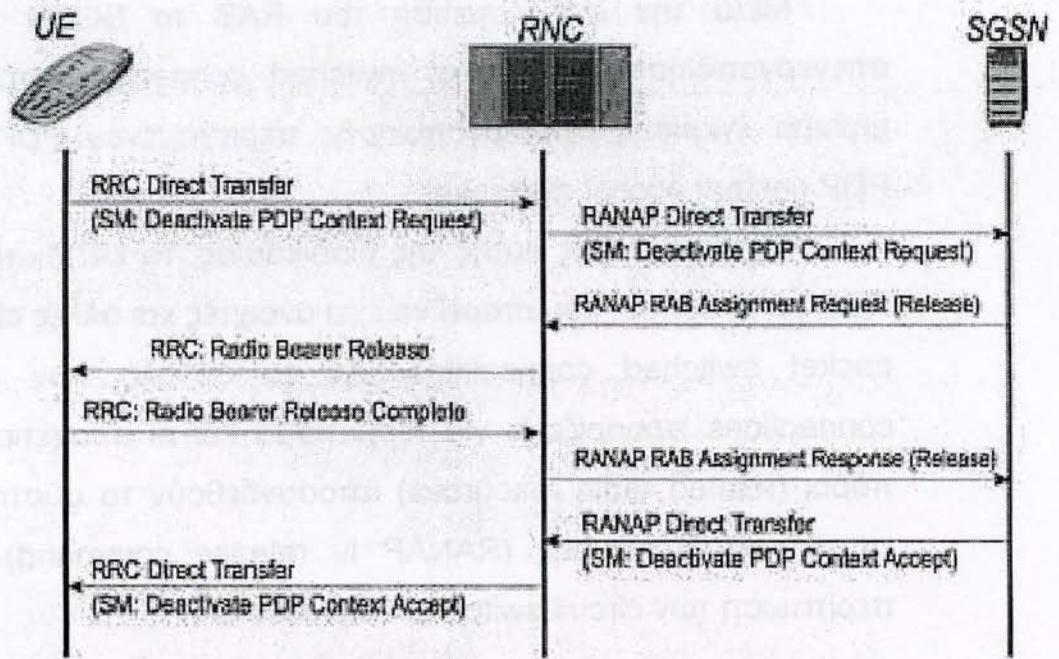
χρησιμοποιηθεί εντολή αποδέσμευσης RANAP lu (RANAP lu release command) όπως φαίνεται στην εικόνα 131. Το RNC με τη λήψη αυτού του μηνύματος ξεκινάει αποδέσμευση του ασύρματου φορέα RRC (RRC radio bearer release) μέσω/πάνω στο interface Iub. Επίσης αποδεσμεύονται όλοι οι πιθανοί radio bearers που δημιουργήθηκαν μέσω DRNCs.



Εικόνα 131 Transaction Clearing με απελευθέρωση του lu (Circuit Switched)

Παράλληλα με την αποδέσμευση των radio bearers αποδεσμεύεται και η σύνδεση RRC. Για τα παραπάνω, το RNC στέλνει στο CN domain μήνυμα ενημέρωσης ολοκλήρωσης αποδέσμευσης, το RANAP lu release complete.

Στην περίπτωση των packet switched connections το user plane και τα RABs μηδενίζονται με τον ίδιο τρόπο που συναντούμε στις circuit switched connections. Για άλλη μια φορά οι διαφορές εντοπίζονται σε επίπεδο παραμέτρων μηνύματος όπως φαίνεται στην εικόνα 132.



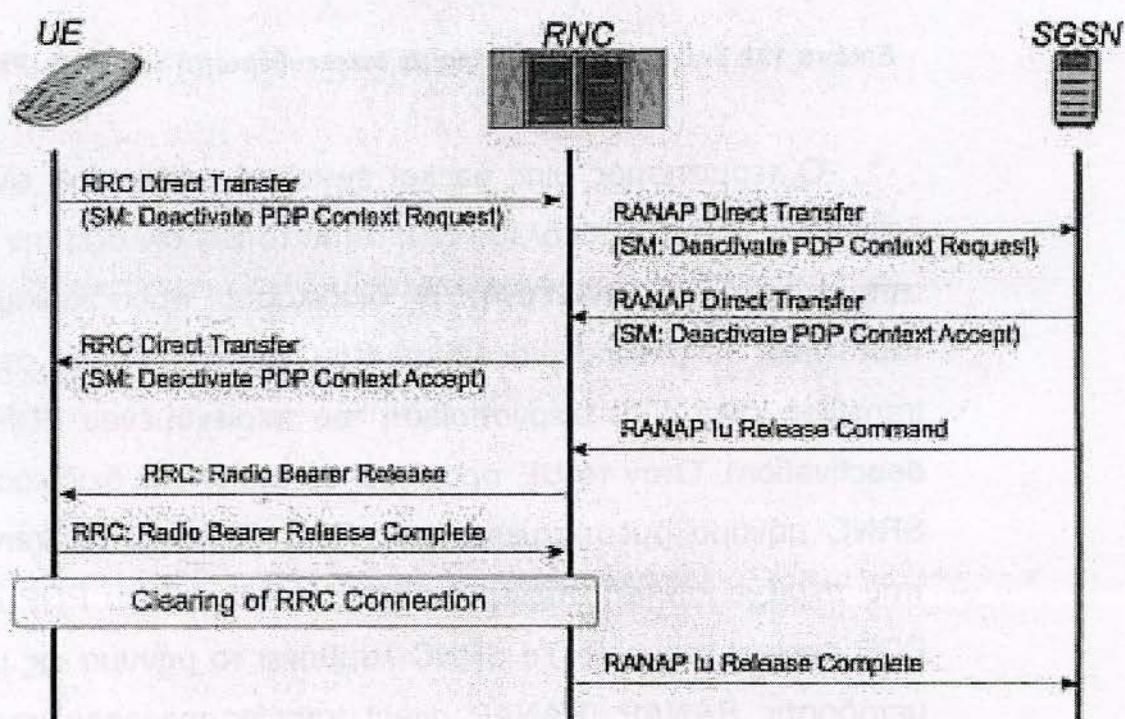
Εικόνα 132 Transaction Clearing με απελευθέρωση του RAB (Packet Switched)

Ο τερματισμός μίας packet switched connection είναι μία από τις διεργασίες του πρωτοκόλλου SM, όπου το SM αλλάζει την κατάσταση του από ενεργή σε ανενεργή. Η διαδικασία προσδιορισμού στίγματος-ταυτότητας (signalling procedure) που χρησιμοποιείται σε αυτό το είδος transition είναι η απενεργοποίηση του περιεχομένου PDP (PDP context deactivation). Όταν το UE προχωρεί σε αυτήν την διαδικασία, στέλνει στο SRNC μήνυμα άμεσης μεταφοράς RRC (RRC direct transfer message) που περιέχει αίτηση απενεργοποίησης περιεχομένου PDP (SM deactivate PDP context request). Το SRNC λαμβάνει το μήνυμα ως μήνυμα άμεσης μετάδοσης RANAP (RANAP direct transfer message) προς το CN PS domain.

Η αίτηση απενεργοποίησης περιεχομένου PDP (PDP context deactivation request) δηλώνει στο SGSN ότι το RAB που προορίζεται γι' αυτήν την packet switched connection δεν είναι πλέον απαραίτητο οπότε αποδεσμεύεται. Αυτή η αποδέσμευση πραγματοποιείται όπως και στην περίπτωση των circuit switched connections.

Μετά την αποδέσμευση του RAB το SGSN γνωστοποιεί την απενεργοποίηση της packet switched connection στέλνοντας στο UE μήνυμα έγκρισης απενεργοποίησης περιεχομένου PDP (SM deactivate PDP context accept message).

Μετά το πέρας αυτής της διαδικασίας, το UE διατηρεί μία σύνδεση RRC με το δίκτυο, και μπορεί να έχει ανοιχτές και άλλες circuit switched και packet switched connections. Αν το σύνολο των packet switched connections προορίζεται για τερματισμό και οι συσχετισμένοι ασύρματοι πόροι (related radio resources) αποσυνδεθούν το σύστημα χρησιμοποιεί εντολή αποδέσμευσης (RANAP lu release command) όπως και στην περίπτωση των circuit switched connections.



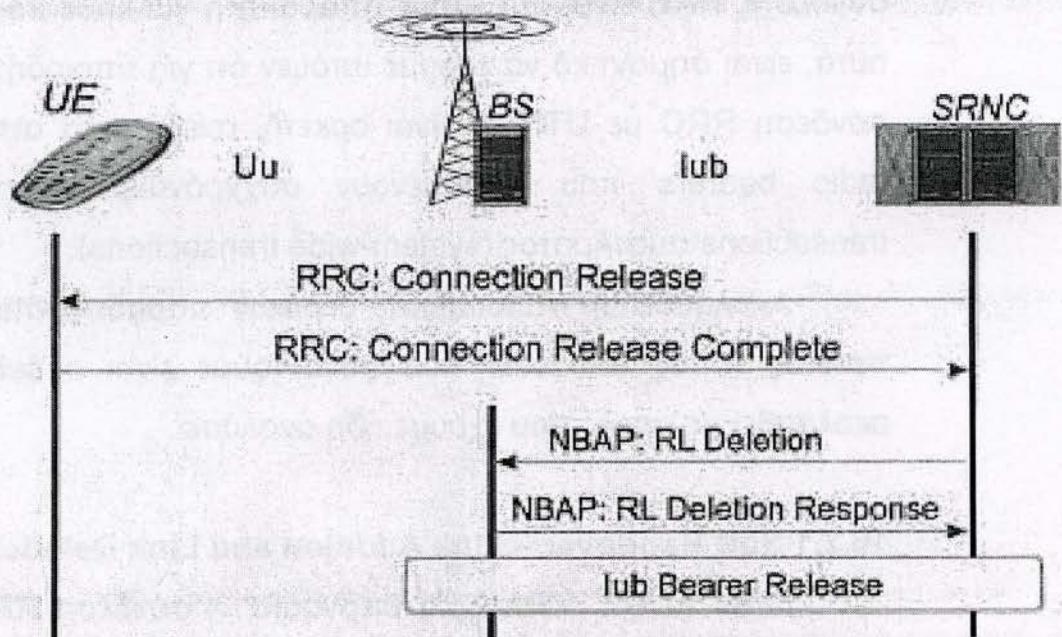
Εικόνα 133 Transaction Clearing με απελευθέρωση του RANAP (Packet Switched)

10.1.8 RRC Connection Release

Η παραπάνω διαδικασία ξεκινάει πάντα από το RNC. Το RNC αναγνωρίζει ποια σύνδεση RRC προορίζεται για αποδέσμευση κι έπειτα στέλνει αυτές τις πληροφορίες στο UE μέσω μηνύματος αποδέσμευσης σύνδεσης RRC (RRC connection release). Το UE επιβεβαιώνει την

αποδέσμευση της σύνδεσης RRC στέλνοντας μήνυμα ολοκλήρωσής της (RRC connection release complete).

Έπειτα, το RNC ξεκινάει την αποδέσμευση των πόρων του Iub interface. Αυτό επιτυγχάνεται με ανταλλαγή μηνυμάτων τερματισμού ασύρματης σύνδεσης και ανταπόκρισης NBAP (NBAP radio link deletion – NBAP radio link deletion response messages). Όταν η radio link deletion εγκρίνεται σε επίπεδο NBAP, ο φορέας μετάδοσης δεδομένων (transport data bearer) στο Iub interface αποδεσμεύεται. Όποιες radio links εντοπίζονται στο DRNC πρέπει να αποδεσμευτούν με τη χρήση υποδιαδικασιών (subprocedures) Iur.



Εικόνα 134 RRC Connection Release

10.2 RRM Procedure Examples

Όπως περιγράφηκε σε περασμένη ενότητα, το RRM είναι ένα σύνολο αλγορίθμων οι οποίοι είναι απαραίτητοι για την πραγματοποίηση και διατήρηση καλής ποιότητας ασύρματης επικοινωνίας (radio path) μεταξύ RNC και UE. Γι' αυτόν τον λόγο, κάθε εμπριεχόμενος στο RRM αλγόριθμος εντοπίζεται σε οποιαδήποτε transaction με την οποία σχετίζεται το UTRAN. Οι αλγόριθμοι RRM διακρίνονται σε handover, power

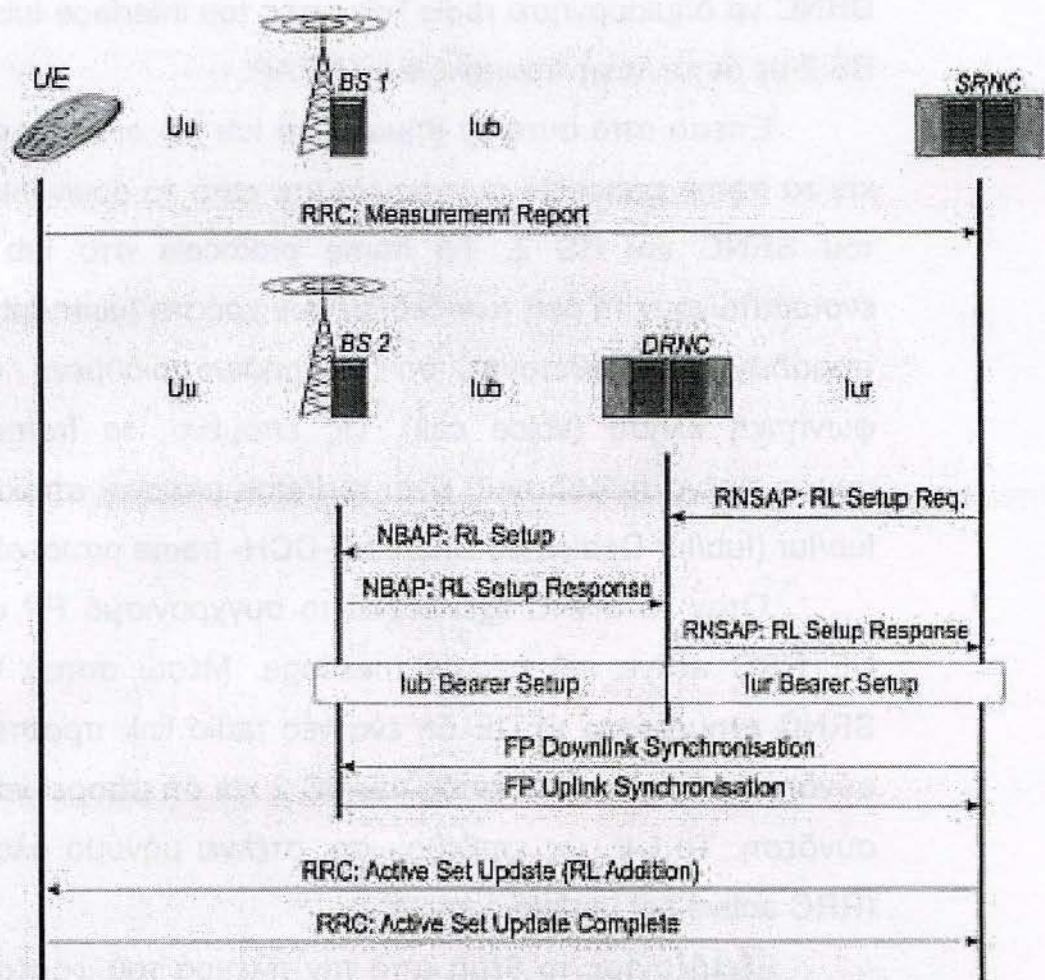
control, admission control, packet scheduling και code management αλγόριθμους, από τους οποίους οι power control, admission control και packet scheduling χρησιμοποιούνται συνεχώς από την εκκίνηση της transaction και καθ' όλη τη διάρκειά της σε όλα τα στάδια. Το packet scheduling χρησιμοποιείται στο περιεχόμενο (context) των packet switched transactions και οι handovers όποτε είναι απαραίτητοι είτε για circuit είτε για packet switched transactions.

Τα στοιχεία RRM (RRM entities) που εντοπίζονται σε UE και RNC επικοινωνούν μεταξύ τους σε επίπεδο διαχείρισης πόρων (radio resource management) μέσω πρωτοκόλλου RRC. Ως επόμενο, η δημιουργία σύνδεσης RRC είναι απολύτως απαραίτητη για κάθε transaction. Παρ' όλ' αυτά, είναι σημαντικό να έχουμε υπόψιν ότι για οποιοδήποτε UE μία μόνο σύνδεση RRC με UTRAN είναι αρκετή, ανεξάρτητα απ' τον αριθμό των radio bearers που παραμένουν συγχρόνως ανοιχτοί για ποικίλες transactions συστήματος (system-wide transactions).

Ακολουθεί η παρουσίαση μερικών παραδειγμάτων handovers. Ο πρώτος τύπος handover που συναντούμε είναι ο soft handover, που ακολουθεί τις αρχές που έχουμε ήδη αναλύσει.

10.2.1 Soft Handover – Link Addition and Link Deletion

Όταν το UE εκτελεί μία διεργασία, η σύνδεση RRC με το UTRAN είναι ενεργή. Σε αυτήν την περίπτωση, το UE ελέγχει συνεχώς την ασύρματη σύνδεση και στέλνει αναφορές στο SRNC.



Εικόνα 135 Soft Handover – Link Addition

Ο αλγόριθμος handover που εντοπίζεται στο SRNC ελέγχει και κατηγοριοποιεί τα περιεχόμενα των ληφθέντων αναφορών. Το SRNC βασισμένο στα αποτελέσματα αυτά, αντιλαμβάνεται ότι το UE δέσμευσε ένα cell τοποθετημένο στο BS 2 έτσι ώστε να διατηρεί συνθήκες (radio conditions) που να πληρούν τα κριτήρια handover όπως αυτά προσδιορίζονται στο SRNC. Το SRNC, στηριζόμενο στη βάση δεδομένων πληροφοριών του ασύρματου δικτύου, εντοπίζει ότι το συγκεκριμένο cell σε BS 2 δεν ανήκει στο ίδιο RNS.

Το SRNC ξεκινάει διαδικασίες (arrangements) από πλευράς UTRAN, ζητώντας από το DRNC, μέσω interface Iur να δημιουργήσει νέα ασύρματη σύνδεση (radio link). Αυτό συμβαίνει με την αποστολή μηνύματος RNSAP RL set-up request message. Το μήνυμα αυτό καλεί το

DRNC να δημιουργήσει radio link εντός του interface Iub μεταξύ DRNC και BS 2 με ανταλλαγή πρωτοκόλλου NBAP.

Έπειτα από αυτά τα βήματα, το Iub και οι Iur bearers εδραιώνονται και τα frame protocols συγχρονίζονται κατά το downlink και uplink μεταξύ του SRNC και BS 2. Τα frame protocols στο Iub και Iur interface ενσωματώνουν τη ροή των δεδομένων χρήστη (user data flow). Σε αυτό το παράδειγμα, υποθέτουμε ότι η χρησιμοποιούμενη υπηρεσία είναι η φωνητική κλήση (voice call). Ως επόμενο, το frame protocol για το συγκεκριμένο παράδειγμα είναι το frame protocol αποκλειστικού καναλιού Iub/Iur (Iub/Iur Dedicated Channel –DCH- frame protocol).

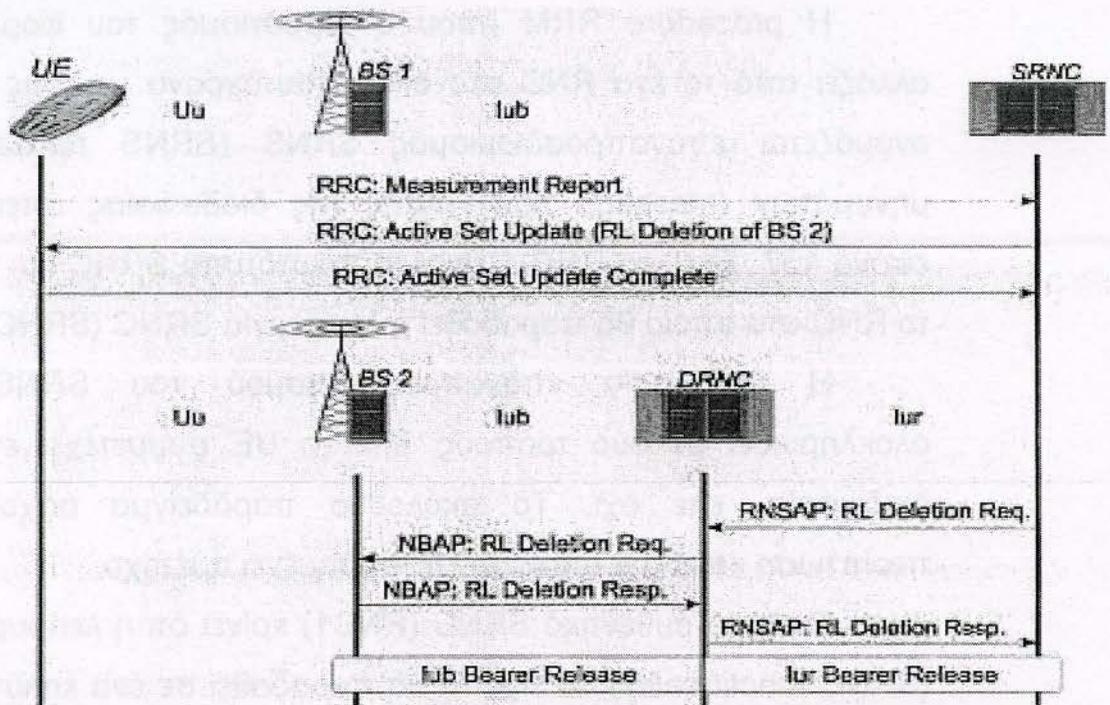
Όταν το SRNC έχει δεχτεί το συγχρονισμό FP uplink, στέλνει στο UE RRC active set update message. Μέσω αυτού του μηνύματος το SRNC ενημερώνει το UE ότι ένα νέο radio link προστέθηκε στην ενεργή σύνδεση μέσω του cell εντός του BS 2 και ότι μπορεί να χρησιμοποιηθεί η σύνδεση. Το UE, ως επιβεβαίωση, στέλνει μήνυμα ολοκλήρωσης update (RRC active set update complete).

Εξετάζοντας το θέμα από την πλευρά του φορέα (bearer), αυτό το παράδειγμα παρουσιάζει μία κατάσταση όπου το UE έχει ενεργό circuit switched RAB. Το RAB αυτό εντοπίζεται εντός UTRAN από τον Iu bearer που βρίσκεται μεταξύ SRNC και CN καθώς και από έναν radio bearer του SRNC που προορίζεται για το UE μέσω ενός cell σε BS 1. Η διαδικασία που περιγράφεται (εικόνα 135) αποτελεί μία περίπτωση κατά την οποία το SRNC προσθέτει έναν επιπλέον radio bearer στην υπάρχουσα σύνδεση. Το RAB και ο φορέας Iu (bearer) παραμένουν ανέπαφοι. Όταν τα frame protocols συγχρονιστούν, το SRNC εκτελεί RAB mapping στους radio bearers.

Όταν το UE κινείται στο δίκτυο κατά τη διάρκεια της transaction, φτάνει στο σημείο όπου το SRNC συμπεραίνει από τις ληφθείσες αναφορές μετρήσεων (measurement reports) ότι μία radio connection που μεταφέρει τον radio bearer εντός ενός cell στο BS 2, δεν πληρεί πλέον τα

κριτήρια που διέπουν τη σύνδεση. Σε αυτήν την περίπτωση, το SRNC ενημερώνει το UE ότι η συγκεκριμένη radio connection μπορεί να απομακρυνθεί από το ενεργό σύνολο (active set). Αυτό επιτυγχάνεται στέλνοντας ξανά στο UE μήνυμα ανανέωσης του ενεργού συνόλου (RRC active set update) προτείνοντας την λήξη της σύνδεσης. Το UE επιβεβαιώνει τον τερματισμό της σύνδεσης (radio connection) στέλνοντας στο SRNC μήνυμα ολοκλήρωσης update (RRC active set update complete).

Το SRNC, με τη λήψη της επιβεβαίωσης του UE, μπορεί να προχωρήσει στη διαγραφή του radio link μεταξύ εκείνου (SRNC) και του BS 2. Αυτό επιτυγχάνεται μέσω αίτησης διαγραφής RNSAP RL (RNSAP Radio Link deletion request) εντός του interface Iur, το οποίο με τη σειρά του ενεργοποιεί το DRNC να διαγράψει το radio link στο interface Iub με την ανταλλαγή πρωτοκόλλου NBAP. Μετά το τερματισμό του radio link στα Iub και Iur, αποδεσμεύονται οι φορείς Iub και Iur (bearers). Η ροή μηνυμάτων (message flow) που αφορά έναν soft handover κατά τη διαγραφή radio link απεικονίζεται στο παρακάτω σχήμα.



Εικόνα 136 Soft Handover – Link Deletion

Από την λειτουργική πλευρά (αρχιτεκτονική) του φορέα, αυτό το παράδειγμα διαγραφής radio link ασχολείται με την περίπτωση κατά την οποία το SRNC απομακρύνει έναν radio bearer αλλά το RAB μεταξύ CN και UE παραμένει.

10.2.2. SRNS Relocation – Circuit Switched

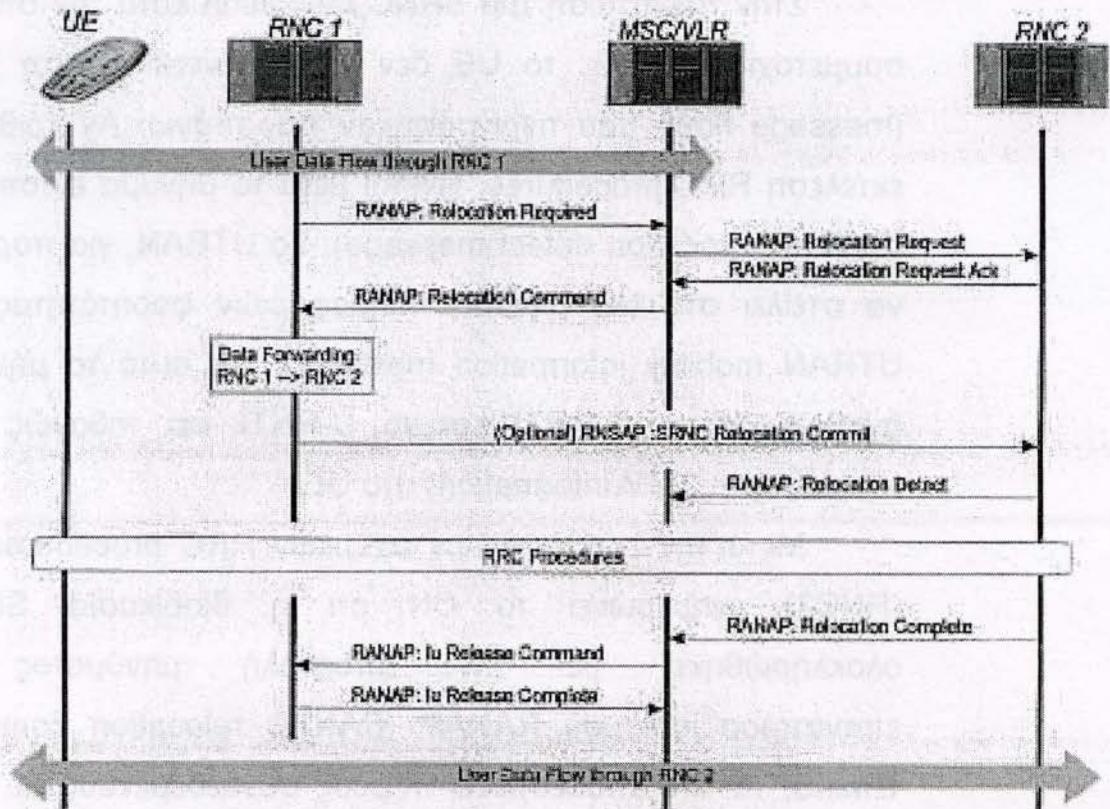
Ο ρόλος του Serving RNC (SRNC) εντοπίζεται στο ότι το RNC διατηρεί τον φορέα Iu και εκτελεί RAB mapping στους radio bearers που αφορούν ένα μόνο ενεργό UE. Τα χαρακτηριστικά του radio link των radio bearers μπορεί να αλλάζουν συνεχώς λόγω των soft handovers, και ως επόμενο το SRNC μπορεί να οδηγηθεί σε μία κατάσταση κατά την οποία δε θα διαχειρίζεται πλέον άμεσα radio links με το δικό του BS εντός του Iub. Όταν συμβαίνει αυτό, η διεργασία RAB mapping θα πρέπει να ανατεθεί σε ένα άλλο RNC που είναι πιο κατάλληλο για την εκτέλεσή της. Από τη στιγμή που το RAB mapping απαιτεί/προϋποθέτει την ύπαρξη του Iu bearer στο ίδιο RNC, θα αλλάξει και η σύνδεση CN.

Η procedure RRM όπου ο τερματισμός του φορέα Iu (bearer) αλλάζει από το ένα RNC στο άλλο (ταυτόχρονα με τους radio bearers) ονομάζεται επαναπροσδιορισμός SRNS (SRNS relocation). Η ροή μηνυμάτων (message flow) αυτής της διαδικασίας απεικονίζεται στην εικόνα 137. Εκεί, το RNC 1 είναι το πρωτότυπο SRNC και το RNC 2 είναι το RNC στο οποίο θα παραδοθεί η λειτουργία SRNC (SRNC functionality).

Η διαδικασία επαναπροσδιορισμού του SRNS μπορεί να ολοκληρωθεί με δύο τρόπους: είτε το UE συμμετέχει ενεργά κατά τη διαδικασία, είτε όχι. Το ακόλουθο παράδειγμα ασχολείται με την περίπτωση κατά την οποία το UE παραμένει αμέτοχο.

Όταν το αυθεντικό SRNC (RNC1) κρίνει ότι η λειτουργία του SRNC (SRNC functionality) θα πρέπει να παραδοθεί σε ένα καλύτερο υποψήφιο RNC (RNC2), ξεκινάει αυτήν την διαδικασία επικοινωνώντας με το

ανάλογο CN domain με μήνυμα αίτησης επαναπροσδιορισμού RANAP (RANAP relocation required message). Αυτό το μήνυμα περιέχει την αιτία του relocation, αναγνώριση του επιθυμητού RNS (target RNS identification) και πληροφορίες για το UE (UE classmark information). Βασιζόμενο στο target RNS identification, το CN domain μπορεί να οδηγήσει αυτό το αίτημα στο επιθυμητό (target) RNS. Αυτό το επαναπροσδιορισμένο αίτημα είναι το μήνυμα αίτησης επαναπροσδιορισμένου RANAP (RANAP relocation request message). Εκτός από τις σχετικές με το relocation πληροφορίες, το μήνυμα αυτό περιέχει πληροφορίες για το περιεχόμενο των φορέων (bearer context), με τις οποίες το CN μεταφέρει το end-point του RAB και της σύνδεσης RRC από το αρχικό SRNC (RNC1) προς το επιθυμητό (target) SRNC (RNC2).



Εικόνα 137 SRNS Relocation – Circuit Switched (το USE δεν περιλαμβάνεται)

Αν το target RNC είναι σε θέση να παρέχει πόρους διαχείρισης του επερχόμενου (incoming) SRNC και της λειτουργίας του, επιβεβαιώνει την αίτηση από και προς το CN, το οποίο με τη σειρά του περνά την

επιβεβαίωση στο αρχικό (source) RNS. Για το RNC1 αυτή η επιβεβαίωση (acknowledgement) αποτελεί εντολή έναρξης του relocation, καθώς όλα είναι πλέον έτοιμα στο target RNC.

Με τη λήψη της εντολής επανατοποθέτησης του RANAP (RANAP relocation command), το original SRNC (RNC1) ξεκινάει την προώθηση δεδομένων προς το target SRNC (RNC2). Το τελευταίο (RNC2) δέχεται τα εισερχόμενα δεδομένα και ενημερώνει το CN domain σχετικά με τον εντοπισμό του SRNS relocation στέλνοντας μήνυμα RANAP relocation detect. Υπάρχει παράλληλα η δυνατότητα το αρχικό (source) SRNC (RNC1) να στείλει στο target SRNC (RNC2) μήνυμα δέσμευσης επαναπροσδιορισμού SRNC (RNSAP SRNC relocation commit message) μέσω του Iur interface.

Στην περίπτωση του SRNC relocation κατά την οποία δεν υπάρχει συμμετοχή του UE, το UE δεν ενημερώνεται για τη ροή μηνυμάτων (message flow) που περιγράφηκαν παραπάνω. Αν κριθεί απαραίτητη η εκτέλεση RRC procedures, γίνεται μετά το μήνυμα εντοπισμού relocation (RANAP relocation detect message). Το UTRAN, για παράδειγμα, μπορεί να στείλει στο UE μήνυμα πληροφοριών φορητότητας UTRAN (RRC UTRAN mobility information message). Με αυτό το μήνυμα το UTRAN αναβαθμίζει το C-RNTI και το U-RNTI και πιθανώς άλλες σχετικές πληροφορίες (MM information) στο UE.

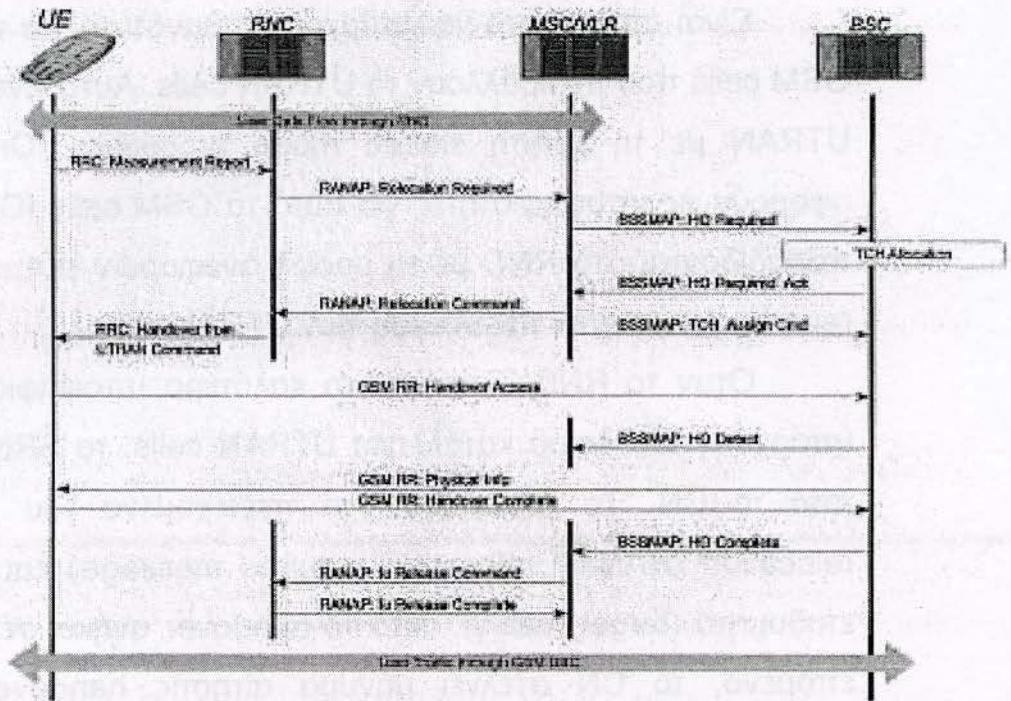
Μετά την εκτέλεση των σχετικών RRC procedures, το νέο SRNC (RNC2) ενημερώνει το CN ότι η διαδικασία SRNC relocation ολοκληρώθηκε, με την αποστολή μηνύματος ολοκλήρωσης επαναπροσδιορισμού RANAP (RANAP relocation complete message). Έπειτα, το CN αποδεσμεύει πόρους συνδεδεμένους με το παλιό SRNC (RNC1), με μήνυμα αποδέσμευσης Iu (RANAP Iu release message) το οποίο δέχεται το παλιό SRNC (RNC1).

Τώρα η ροή των δεδομένων χρήστη (user data flow) μεταφέρεται στο νέο RNC το οποίο δρα ως macrodiversity combination point για το UE

και ελέγχει όλες τις δραστηριότητες RRC (RRC activities) για το συγκεκριμένο UE.

10.2.3 Inter – System Handover from UMTS to GSM – Circuit Switched

Οι προδιαγραφές 3GPP (3GPP specifications) ορίζουν ότι ένας handover μεταξύ δύο ασύρματων δίοδων (radio access) είναι θεμελιώδους σημασίας για το σύστημα. Για το UMTS, αυτό σημαίνει ότι το σύστημα πρέπει να είναι σε θέση να εκτελεί handover μεταξύ UTRAN και ενός GSM BSS. Το handover εντός συστήματος (inter – system handover) μεταξύ UTRAN και GSM BSS είναι μια ειδική περίπτωση διαδικασίας relocation όπως παρουσιάζεται στο ακόλουθο σχήμα.



Εικόνα 138 Inter – System Handover from UMTS to GSM – Circuit Switched

Στην πραγματικότητα, το RANAP μεταφέρει τις ίδιες και ακόμα περισσότερες πληροφορίες με εκείνες του πρωτοκόλλου BSSMAP στο δίκτυο GSM. Αν η εκτέλεση του handover γίνει απ' την πλευρά του UTRAN προς ένα GSM BSS, τα μηνύματα του UTRAN είναι ακριβώς ίδια όπως στην περίπτωση του SRNS relocation αλλά τα περιεχόμενά τους ποικίλουν

π.χ., το μήνυμα αίτησης επαναπροσδιορισμού RANAP (RANAP relocation required) περιέχει την ταυτότητα/διακριτικά του επιθυμητού RNC (target RNC ID) κατά τη διεργασία του RNC relocation. Όταν το target RNC βρίσκεται στην πλευρά του GSM, η ID του αντικαθίσταται από cell global identity που είναι μια παράμετρος πιο οικεία στο GSM BSC.

Αντίθετα από το SRNS relocation, το handover εντός συστήματος (inter – system handover) είναι μια διαδικασία (procedure) στην οποία συμμετέχει πάντα το UE, καθώς το τελευταίο πρέπει να εκτελέσει δραστηριότητες ραδιοφωνικών πόρων (Radio Resource –RR- activities) έτσι ώστε να αποκτήσει πρόσβαση στο GSM BSS – σημείωση: το GSM BSS δεν μπορεί να χειριστεί κανένα είδος πληροφοριών που είναι έγκυρα (valid) στο UTRAN.

Είναι απαραίτητο να υπάρχει η πιθανότητα για το UE να εκτιμάει τα GSM cells που περιβάλλουν τα UTRAN cells. Αυτό γίνεται εφικτό εντός του UTRAN με τη χρήση slotted mode procedure. Οι πληροφορίες που αφορούν τις υποψηφιότητες για αυτά τα GSM cells (GSM cell candidates) παραδίδονται στο RNC με τη μορφή αναφορών εκτίμησης (measurement reports) όπως στην περίπτωση των UTRAN cells.

Όταν το RNC εντοπίσει το καλύτερο υποψήφιο GSM cell και δεν υπάρχουν διαθέσιμα κατάλληλα UTRAN cells, το SRNC ζητάει relocation από το CN. Το CN ελέγχει τα περιεχόμενα του μηνύματος αίτησης relocation (RANAP relocation required message) και συμπεραίνει ότι το επιθυμητό (target) cell γι' αυτό το handover ανήκει σε ένα GSM BSS. Ως επόμενο, το CN στέλνει μήνυμα αίτησης handover (GSM BSSMAP handover required) στο target BSC εντός του δικτύου GSM.

Ακολουθεί η δημιουργία Traffic Channel (TCH) στο οποίο θα παραδοθεί η σύνδεση. Μετά την επιτυχή τοποθέτηση του TCH εντός του GSM BSS, η αίτηση handover (handover request) αποστέλλεται πίσω στο CN. Το CN απαντά στέλνοντας στο SRNC μήνυμα εντολής επαναπροσδιορισμού RANAP (RANAP relocation command message).

Μετά από το παραπάνω μήνυμα ξεκινάει η relocation procedure εντός του SRNC. Από τη στιγμή που εξετάζουμε την περίπτωση στην οποία συμμετέχει το UE, το SRNC δίνει εντολή στο UE να εκτελέσει inter – system handover στέλνοντας μήνυμα εντολής RRC handover from UTRAN command. Το μήνυμα αυτό περιέχει πληροφορίες για το target system και μπορεί να μεταφέρει στο φορτίο του όποιες άλλες επιπρόσθετες πληροφορίες σχετίζονται με το inter – system handover.

Μετά τη λήψη του RRC handover μέσω της εντολής του UTRAN (UTRAN command), το UE ελέγχει αν το μήνυμα περιείχε ένδειξη χρονικού περιορισμού εκτέλεσης του handover (η αρχική –default- ρύθμιση δηλώνει άμεση εκτέλεση) και ξεκινάει διεργασίες handover αναλόγως. Η πρόσβαση (target radio access) είναι GSM, οπότε το UE στέλνει μήνυμα πρόσβασης handover (GSM RR handover access message) στο target cell του GSM BSS. Όταν το τελευταίο λάβει το παραπάνω μήνυμα, δηλώνει στο BSC ότι το UE έχει πρόσβαση στο GSM BSS. Έπειτα, το GSM BSC ενημερώνει το CN σχετικά με το επερχόμενο (incoming) UE στέλνοντας μήνυμα εντοπισμού handover (GSM BSSMAP handover detect).

Ως επιβεβαίωση της πρόσβασης του handover (GSM RR handover access), το UE λαμβάνει πληροφορίες (GSM RR physical info) από το GSM BSS cell. Το μήνυμα αυτό περιέχει πληροφορίες οι οποίες δραστηριοποιούν/δίνουν τη δυνατότητα στο UE έτσι ώστε να ξεκινήσει τη χρήση ασύρματης πρόσβασης (GSM radio access), όπως είναι για παράδειγμα οι περιγραφές των καναλιών (channel descriptions).

Στο τελικό στάδιο, όταν το UE έχει πλέον επιτυχώς πρόσβαση στο GSM BSS cell, στέλνει στο GSM BSC μήνυμα ολοκλήρωσης handover (GSM RR handover complete). Το BSC αποστέλει τις ίδιες πληροφορίες στο CN δηλώνοντας ότι το UE έχει τώρα ενσωματωθεί στο GSM BSS και ότι το inter – system handover έχει ολοκληρωθεί επιτυχώς.

Το UE δε χρησιμοποιεί πλέον πόρους του UTRAN (UTRAN resources) οπότε όλοι οι πόροι που σχετίζονται με το UE μπορούν να αποδεσμευτούν και το CN στέλνει εντολή αποδέσμευσης Iu (RANAP Iu release). Η εντολή αυτή αναθέτει στο RNC τον τερματισμό της σύνδεσης RRC και αποδεσμεύει όλους τους πόρους που σχετίζονται με το UE. Έπειτα, το RNC επιβεβαιώνει στο CN τη συγκεκριμένη αποδέσμευση (release) με μήνυμα ολοκλήρωσης αποδέσμευσης (RANAP Iu release complete).

10.3 MM Procedure Examples

Συγκριτικά με το GSM, το MM συμπεριφέρεται κατά κύριο λόγο με τον ίδιο τρόπο εντός UMTS, όμως παρ' όλ' αυτά υπάρχουν ορισμένες διαφορές. Το MM καλύπτει όλες τις διαδικασίες, μεθόδους και διακριτικά (procedures – methods – identities) που απαιτούνται για τη διατήρηση επίγνωσης σχετικά με την θέση του UE όταν κινείται στο δίκτυο.

Στα δίκτυα GSM, το MM διαχειρίζεται αποκλειστικά από MS και NSS. Στα δίκτυα UMTS οι περισσότερες λειτουργίες του MM (MM functions) διαχειρίζονται ισομερώς από το UE και το CN. Το RNC χειρίζεται εν μέρει την κίνηση του UE μέσα στο δίκτυο (radio access network) με τη χρήση κατάλληλων RRC procedures. Οι δραστηριότητες MM (MM activities) που διαχειρίζονται από το RNC είναι αναβαθμίσεις/ανανεώσεις cell και URA (cell and UTRAN Registration Area Updates).

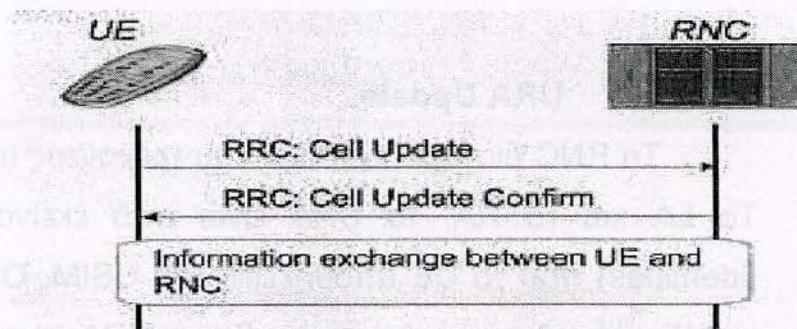
10.3.1 Cell update

Κατά τη διάρκεια μιας circuit switched transaction, το CN γνωρίζει τη θέση (location) του UE με ακρίβεια περιοχής (location area) και το RNC με ακρίβεια cell ή (για να είμαστε πιο ακριβείς) cells αν το UE βρίσκεται σε κατάσταση soft handover (soft handover state). Οι πληροφορίες του cell αλλάζουν συνεχώς κατά τη διάρκεια της transaction. Ο ρυθμός αλλαγών

(pace of change) εξαρτάται από τις συνθήκες που επικρατούν στο δίκτυο (radio network) και απ' το εάν το UE μετακινείται και με τι ταχύτητα.

Στην περίπτωση των packet switched transactions οι πληροφορίες θέσης (location information) διανέμονται με τέτοιον τρόπο έτσι ώστε το CN PS domain να γνωρίζει τη θέση του UE με ακρίβεια περιοχής θέσης (location area) και περιοχής δρομολόγησης (routing area) ενώ το RNC γνωρίζει τη θέση του του UE με ακρίβεια cell. Επειδή η packet switched connection παρουσιάζει από τη φύση της ασυνέχεια (discontinuous in nature), οι πληροφορίες του cell στο RNC θα είναι εκπρόθεσμες (out-of-date) όταν η σύνδεση μεταξύ UE και CN κλείσει προσωρινά. Ως επόμενο, η packet switched connection ενεργοποιείται από το UE και το CN αλλά το RNC αδυνατεί σε αυτήν την κατάσταση να δρομολογήσει πακέτα δεδομένων (route data packets in this state).

Αν το UE πρόκειται επιθυμεί να στείλει δεδομένα και το τρέχον (current) cell είναι διαφορετικό απ' ότι προηγουμένως, το UE εκτελεί διαδικασία ανανέωσης cell (RRC cell update procedure) προς ενημέρωση του RNC σχετικά με το τρέχον cell. Έπειτα είναι δυνατή οποιαδήποτε δραστηριότητα RRC (RRC activity), όπως είναι για παράδειγμα η δημιουργία ενός radio bearer.



Εικόνα 139 Διαδικασία εγκατάστασης κυψέλης

Από την άλλη πλευρά, αν είναι το CN PS domain εκείνο που διαθέτει πακέτα δεδομένων (data packets) που πρόκειται να αποσταλούν στο UE, το CN PS domain αρχικά εκδίδει (issues) RANAP paging έτσι ώστε το RNC να στείλει στο UE RRC paging Type 1. Μετά από αυτό το UE ελέγχει

αν είναι απαραίτητη η διαδικασία ανανέωσης cell (cell update procedure). Αν ναι, το UE την εκτελεί και είναι πλέον έτοιμο να δεχτεί πακέτα δεδομένων.

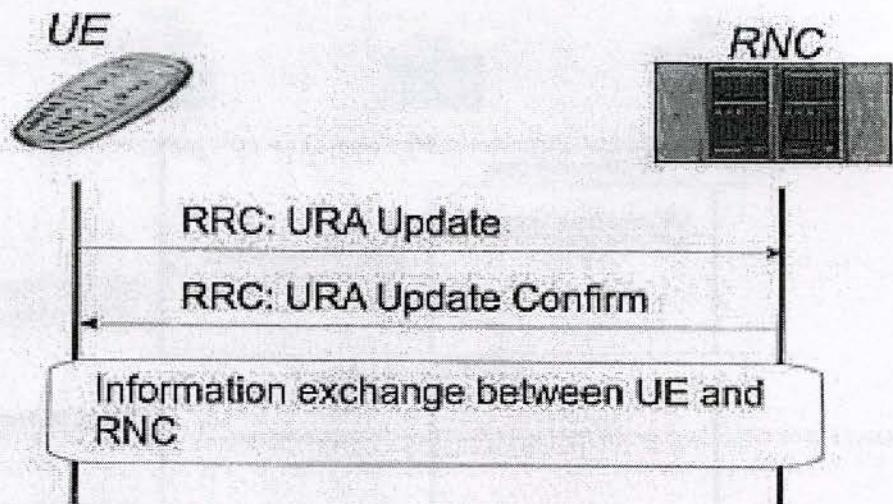
Επιγραμματικά, οι διάφοροι λόγοι για να εκτελέσει το UE ανανέωση cell (cell update) είναι οι ακόλουθοι:

Επαναεπιλογή cell	Cell reselection
Περιοδική ανανέωση cell	Periodic cell update
Μετάδοση/εκπομπή δεδομένων κατά το uplink	Uplink data transmission
Ανταπόκριση paging	Paging response
Ξαναεισαχθείσα περιοχή υπηρεσιών	Re-entered service area
Αποτυχία ραδιοφωνικής/ασύρματης σύνδεσης	Radio link failure
Μη αναστρέψιμο σφάλμα RLC	Unrecoverable RLC error

Σε συνδιασμό με τη διαδικασία ανανέωσης cell (cell update procedure) το RNC είναι πιθανό να τοποθετήσει ένα καινούριο RNTI στη σύνδεση RRC.

10.3.2 URA Update

Το RNC διατηρεί εγγραφή του τρέχοντος (current) URA για κάθε UE. Το LA και το RA, το URA είναι από εκείνα τα στοιχεία ταυτότητας (identities) που το UE αποθηκεύει στο USIM. Όταν είναι ενεργοποιημένη, το UE ελέγχει συνεχώς τη ληφθείσα URA identity. Αν η ληφθείσα URA διαφέρει από εκείνη που είναι αποθηκευμένη στο USIM, το UE εκτελεί διαδικασία ανανέωσης URA (RRC URA update procedure).

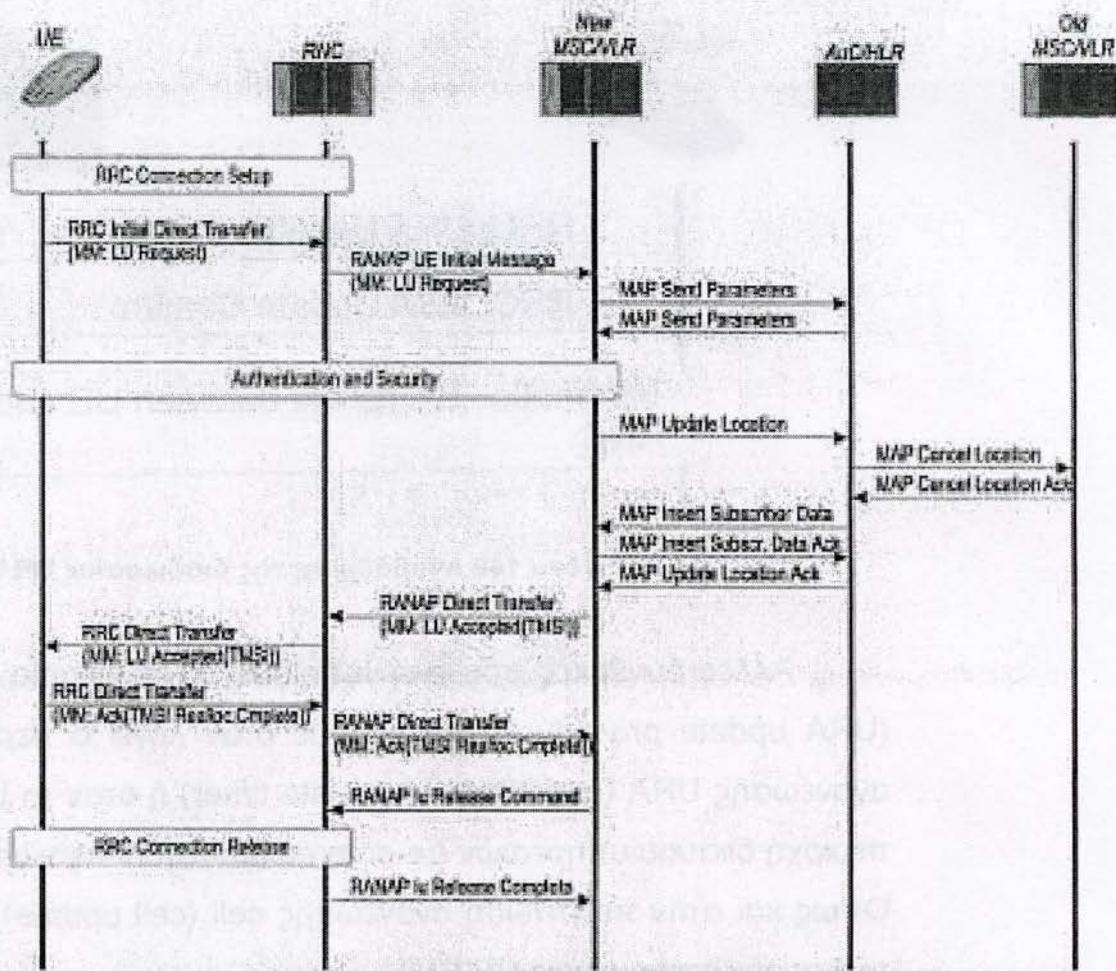


Εικόνα 140 Αναβάθμιση της διαδικασίας URA

Άλλες συνθήκες που ενεργοποιούν τη διαδικασία ανανέωσης URA (URA update procedure) συναντούμε όταν λήγει ο περιοδικός μετρητής ανανέωσης URA (periodic URA update timer) ή όταν το UE ξαναμπήκε σε περιοχή δικτύου υπηρεσιών (re-entered a network service area). Όπως και στην περίπτωση ανανέωσης cell (cell update), το RNC αλλάζει το προοριζόμενο για το UE RNTI.

10.3.3 Location Update to the CN CS domain

Στην εικόνα 141 απεικονίζεται η ροή προσδιοριστικών μηνυμάτων (signaling message flow) για μία ανανέωση θέσης (location update) που εκτελείται μεταξύ του UE και του CN circuit switched domain.



Εικόνα 141 Αναβάθμιση τοποθεσίας στο CN CS

Αν το UE δεν έχει σύνδεση RRC με το UTRAN, πρώτα πραγματοποιείται η σύνδεση RRC. Η ταυτότητα LA (LA identity) ενεργοποιεί την ανανέωση θέσης (Location Update – LU). Το UE έχει αποθηκεύσει την LA στο USIM και αν η LA identity που έλαβε από τις πληροφορίες συστήματος (system information) του εγκατεστημένου (camped) cell είναι διαφορετική από εκείνη που βρίσκεται αποθηκευμένη στο USIM, το UE ξεκινάει διαδικασία ανανέωσης θέσης (location update procedure) έτσι ώστε να ενημερώσει το CN για την τρέχουσα θέση του.

Το μήνυμα αίτησης LU (MM LU request message) μεταφέρεται μέσω του αρχικού φακέλου άμεσης μεταφοράς (RRC initial direct transfer

envelope) προς το RNC όπου συνδέεται με το CN μέσω μηνύματος RANAP UE initial.

Το μήνυμα αίτησης LU (LU request message) περιέχει μια παλιά και μια νέα LA identity όπως επίσης και την επιπρόσθετη αναγνώριση του συνδρομητή (subscriber identification). Στις συνηθισμένες περιπτώσεις, αυτή η ταυτότητα είναι μια τιμή TMSI η οποία τοποθετήθηκε προηγουμένως από το MSC/VLR.

Το VLR ελέγχει αν έχει τμήματα αυθεντικοποίησης (authentication vectors) για αυτόν τον συνδρομητή (subscriber). Αν δεν υπάρχουν, υιοθετούνται οι παράμετροι ασφαλείας (security parameters) από το AuC, το οποίο στέλνει στο VLR μια προϋπάρχουσα ποσότητά τους με μήνυμα αποστολής παραμέτρων (MAP send parameters message). Με τη λήψη αυτών των παραμέτρων, το VLR αποκτά πρόσβαση στις διαδικασίες ασφαλείας (access level security procedures) για επιβεβαίωση/αυθεντικοποίηση (authentication) και ciphering.

Αν η παλιά ταυτότητα LA (LA identity) διαφέρει απ' την καινούρια, το VLR ενημερώνει το HLR του συνδρομητή (subscriber's HLR) για τη νέα θέση (location). Το HLR καταργεί την παλιά θέση του UE με μήνυμα ανανέωσης θέσης (MAP cancel location message) και ξεκινάει τη λειτουργία καταχώρησης δεδομένων συνδρομητή (MAP insert subscriber data operation).

Λειτουργία MAP μεταφέρει το προφίλ του συνδρομητή (subscriber profile) στο νέο VLR. Το subscriber profile περιέχει όλες τις πληροφορίες ταυτότητας και υπηρεσιών και τους πιθανούς περιορισμούς που αφορούν τη χρήση τους.

Όταν το VLR έχει ανανεώσει (update) το ίδιο με πληροφορίες για τη θέση εκείνου και του subscriber, το CN domain ενημερώνει το UE σχετικά με την επιτυχή ολοκλήρωση της διαδικασίας (procedure) στέλνοντας μήνυμα έγκρισης LU (MM LU accepted message). Το μήνυμα αυτό

περιέχει επίσης ένα νέο TMSI για τον subscriber. Το RNC προωθεί αυτές τις πληροφορίες στο UE μέσω άμεσης μεταφοράς (RRC direct transfer).

Το UE επιβεβαιώνει την αποδοχή του LU (LU acceptance) και μια νέα τιμή TMSI (TMSI value) στέλνοντας στο MSC/VLR μήνυμα ολοκλήρωσης επαναπροσδιορισμού TMSI (MM TMSI reallocation complete).

Με τη λήψη της επιβεβαίωσης για το reallocation του TMSI, το VLR ξεκινάει την αποδέσμευση της signaling connection. Το lu interface αποδεσμεύεται με εντολή αποδέσμευσης (RANAP lu release command) με τη λήψη της οποίας το RNC αποδεσμεύει τη σύνδεση RRC (RRC connection). Ακολουθεί η επιβεβαίωση της αποδέσμευσης (release) με μήνυμα ολοκλήρωσης αποδέσμευσης (RANAP lu release complete message) προς το MSC/VLR.

10.3.4. Routing Area Update to the CN PS domain

Το PS domain αναγνωρίζει την LA αλλά η πιο ουσιαστική εγγραφή (registration) αυτού του περιεχομένου (context) είναι η περιοχή δρομολόγησης Routing Area (RA). Το UE έχει αποθηκεύσει το πιο πρόσφατο RA στο σημείο εκτέλεσης ανανέωσης RA (RA update). Το UE λαμβάνει την τρέχουσα (current) ταυτότητα RA (RA identity) από τις πληροφορίες συστήματος (system information) που του έστειλε το εγκατεστημένο/δεσμευμένο (camped) cell μέσω broadcast (εκπομπής). Αν αυτή (RA identity) διαφέρει από την αποθηκευμένη στο USIM, το UE ξεκινάει την λειτουργία ανανέωσης Routing Area (Routing Area Update – RAU- transaction).

Σε πρώτη φάση, το UE στέλνει μήνυμα αίτησης RAU (GMM RAU request message) μέσω άμεσης μεταφοράς (direct transfer). Το μήνυμα αυτό περιέχει την παλιά RA και νέες τιμές διακριτικών/δεικτών RA (RA identifier values). Το μήνυμα αυτό φτάνει στο νέο SGSN μέσω του lu interface. Το νέο SGSN γνωρίζει το “περιβάλλον MM” (“MM environment) –

τα περιβάλλοντα/γειτονικά RAs και τη σχέση τους με άλλα SGSNs στο δίκτυο. Βασισμένο σε αυτές τις πληροφορίες, το νέο SGSN μπορεί να καθορίσει το παλιό SGSN και του ζητάει/προσκομίζει πληροφορίες για τον συνδρομητή/εγγεγραμμένο (subscriber) μέσω μηνύματος αίτησης περιεχομένου SGSN (GTP-C SGSN context request message). Με άλλα λόγια, το νέο SGSN ανακαλύπτει/προσδιορίζει αν το UE που εκτελεί RAU (Routing Area Update) έχει ήδη υπάρχον περιεχόμενο PDP (PDP context).

Έπειτα το νέο SGSN μπορεί να ζητήσει το AuC του subscriber έτσι ώστε να αποκτήσει τμήματα/στοιχεία αυθεντικοποίησης/επιβεβαίωσης (authentication vectors). Το AuC τα υπολογίζει (calculate) και επιστρέφει ένα μέρος τους (set of vectors) στο νέο SGSN μέσω μηνύματος αποστολής παραμέτρων (MAP send parameters message). Τώρα, το νέο SGSN είναι σε θέση να ξεκινήσει αυθεντικοποίηση και έλεγχο ασφάλειας (security control) για το UE εντός/μέσω UTRAN. Μετά την επιτυχή ολοκλήρωση των λειτουργιών αυθεντικοποίησης και ασφάλειας (authentication and security activities) το νέο SGSN ενημερώνει το GGSN στέλνοντάς του μήνυμα ανανέωσης περιεχομένου PDP (GTP-C update PDP context message). Το νέο SGSN ενημερώνει το GGSN για την αλλαγή του SGSN και ότι οι πληροφορίες περιεχομένου PDP (PDP context information) άλλαξαν αναλόγως.

Τώρα, το νέο SGSN ανανεώνει τις πληροφορίες θέσης (updates location info) με το HLR μέσω μηνύματος ανανέωσης θέσης (MAP update location message). Με τη λήψη του μηνύματος αυτού, το HLR καταργεί/ακυρώνει την παλιά/προηγούμενη θέση (old location) του UE από το παλιό SGSN. Έπειτα, το HLR ξεκινάει τη μεταφορά/μετάδοση (transfer) του προφίλ του εγγεγραμμένου/συνδρομητή (subscriber profile) στο νέο SGSN με τη λειτουργία καταγραφής/εκχώρησης/εγγραφής δεδομένων συνδρομητή (MAP insert subscriber data operation).

Όταν ολοκληρωθεί η ανανέωση (update) του προφίλ του συνδρομητή/εγγεγραμμένου (subscriber profile) στο νέο SGSN, το

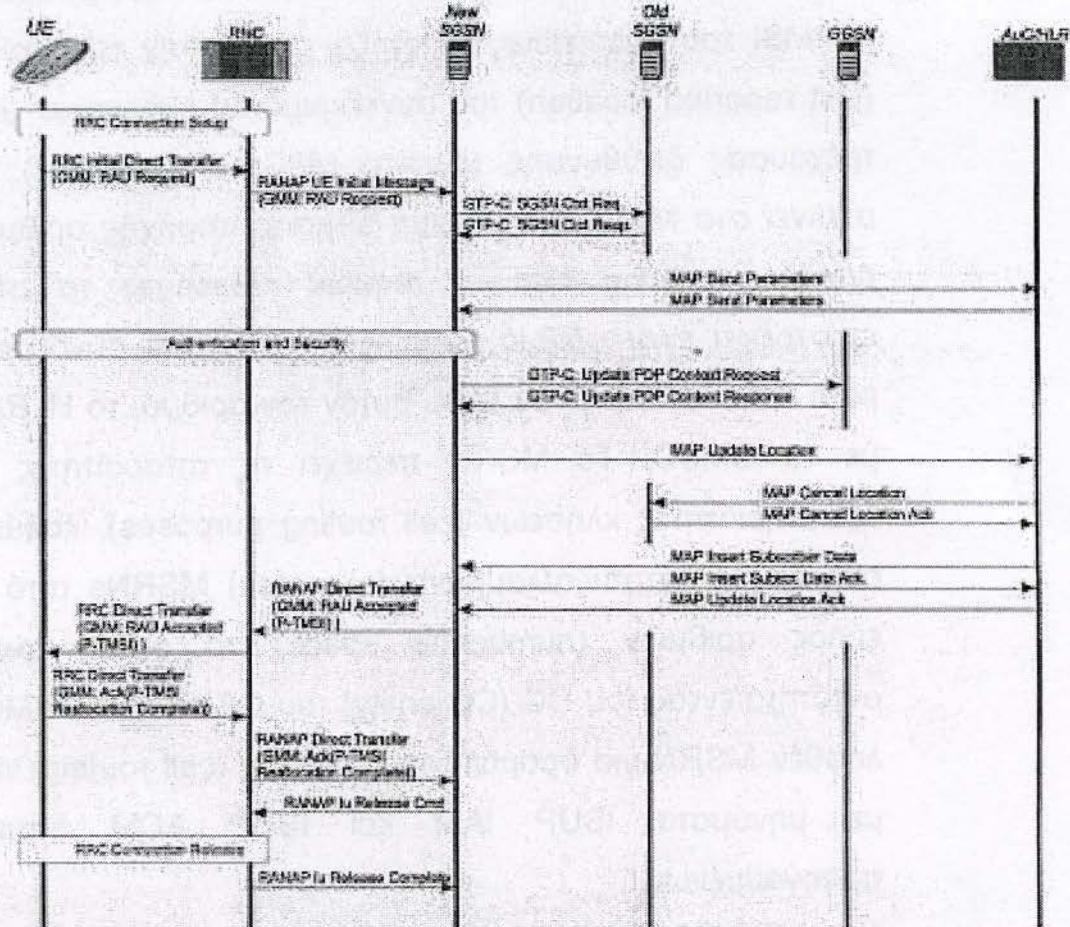
τελευταίο (SGSN) στέλνει στο UE μήνυμα αποδοχής RAU (RAU accepted message). Εντός αυτής της παραμέτρου βρίσκεται η νέα τιμή P-TMSI, την οποία το UE αποθηκεύει στο USIM και γνωστοποιεί/επιβεβαιώνει τη λήψη του (P-TMSI) στέλνοντας στο SGSN μήνυμα γνωστοποίησης/επιβεβαίωσης (GMM acknowledgement).

Με την ολοκλήρωση της ανανέωσης του RA (RA update) το SGSN αποδεσμεύει τη signaling connection που χρησιμοποιείται σε αυτήν την transaction.

Η ροή μηνυμάτων (message flow) όπως παρουσιάζεται στο 10.21 αναπαριστά την ανανέωση RA (Routing Area Update) στην περίπτωση που αλλάζει το SGSN. Το SGSN δεν αλλάζει κάθε φορά που ανανεώνεται το RA. Αν το SGSN παραμένει το ίδιο, η διαδικασία (procedure) είναι πιο απλή καθώς δεν είναι απαραίτητη η διαδραστικότητα/διάλογος (MAP dialogue) μεταξύ SGSN και HLR.

10.4 CC Procedure Example

Στην εικόνα 142 απεικονίζεται η ροή μηνυμάτων (signaling message flow) από μία τερματισμένη κλήση του UE (UE terminated circuit switched call) προερχόμενη από δημόσιο/κοινόχρηστο τηλεφωνικό δίκτυο (Public Switched Telephone Network – PSTN). Το PSTN signaling και το signaling που χρησιμοποιείται μεταξύ των κόμβων MSC (MSC nodes) είναι υποθετικά ISUP (ISDN User Port).



Εικόνα 142 Κλήση μεταγωγής κυκλώματος – USE terminating – UE clears

Η κλήση (call) εισέρχεται αρχικά στο gateway MSC από το PSTN με μήνυμα αρχικής διεύθυνσης (ISUP Initial Address message – IAM). Το μήνυμα αυτό περιέχει το νούμερο/αριθμό MSISDN (MSISDN number) του καλούμενου συνδρομητή/εγγεγραμμένου (UMTS subscriber). Παράλληλα, αυτός ο αριθμός MSISDN αναγνωρίζει/εντοπίζει την υπηρεσία (service) που προορίζεται προς χρήση. Για το σήσιμο/εγκατάσταση του διαύλου (circuit switched path) μεταξύ GMSC και PSTN, το GSMC απαντάει με μήνυμα ολοκλήρωσης διεύθυνσης/προορισμού (ISUP Address Complete Message – ACM).

Το GSMC ζητάει από το HLR την παροχή πληροφοριών πορείας/δρομολόγησης (routing information) για τον subscriber στέλνοντας μήνυμα αίτησης αποστολής πληροφοριών (MAP send routing information message). Με αυτό το μήνυμα, το GSMC στέλνει στο HLR τον ληφθέντα

αριθμό (number) MSISDN με τον οποίο το HLR μπορεί να εντοπίσει/βρει το IMSI του subscriber. Εντοπίζει επίσης την τελευταία αναφορά θέσης (last reported location) του συγκεκριμένου subscriber με την ακρίβεια της τρέχουσας διεύθυνσης (current MSC/VLR address). Έπειτα, το HLR στέλνει στο MSC/VLR μήνυμα αίτησης παροχής αριθμού roaming (MAP provide roaming number request message) το οποίο εντοπίζει κι επιστρέφει έναν αριθμό roaming (MSRN) για σύνδεση (circuit switched path connection). Όταν λάβει αυτόν τον αριθμό, το HLR συνδέει το MSRN με το GMSC. Το MSRN περιέχει τις απαραίτητες πληροφορίες για δραστηριότητες κλήσεων (call routing purposes), καθώς κάθε MSC/VLR στο δίκτυο εντοπίζει/λαμβάνει (allocates) MSRNs από ένα καθορισμένο εύρος αριθμών (numbering space) το οποίο αναγνωρίζεται στην οντότητα/εντός του CC (CC entity) του GSMC. Το GSMC χρησιμοποιεί το ληφθέν MSRN για δρομολόγηση κλήσης (call routing) προς το MSC/VLR με μηνύματα ISUP IAM και ISUP ACM όπως περιγράφηκαν προηγουμένως.

Το MSC/VLR αναγνωρίζει/διακρίνει το MSRN που εντόπισε και καθορίζει ότι αυτή η κλήση (call) θα (αυτό-)τερματιστεί στο UTRAN. Γι' αυτόν τον σκοπό, στέλνει μηνύματα RANAP paging στα RNCs που διατηρούν τα cells, τα οποία ανήκουν στο LA, όπου το UE εκτέλεσε την τελευταία/πιο πρόσφατη ανανέωση θέσης (latest location update). Τα RNCs στέλνουν στο Uu interface μηνύματα RRC paging Type 1 και το UE που έχει υποστεί paging ανταποκρίνεται ξεκινώντας διαδικασία θεμελίωσης/δημιουργίας σύνδεσης RRC (RRC connection establishment procedure).

Η ανταπόκριση/αντίδραση στο paging πραγματοποιείται με το αρχικό μήνυμα του UE (RANAP UE initial message) με τη λήψη του οποίου το CN ξεκινάει δραστηριότητες (activities) αυθεντικοποίησης /εξακρίβωσης και ασφάλειας (authentication and security) για την κλήση (call). Αν οι δραστηριότητες/διεργασίες ασφάλειας είναι επιτυχείς, το CN

ξεκινάει το στήσιμο/εγκατάσταση (set-up) transaction, ενημερώνοντας το UE με μήνυμα CC set-up message σχετικά με μια εισερχόμενη κλήση και τη φύση/είδος/χαρακτηριστικά της (incoming call and its nature).

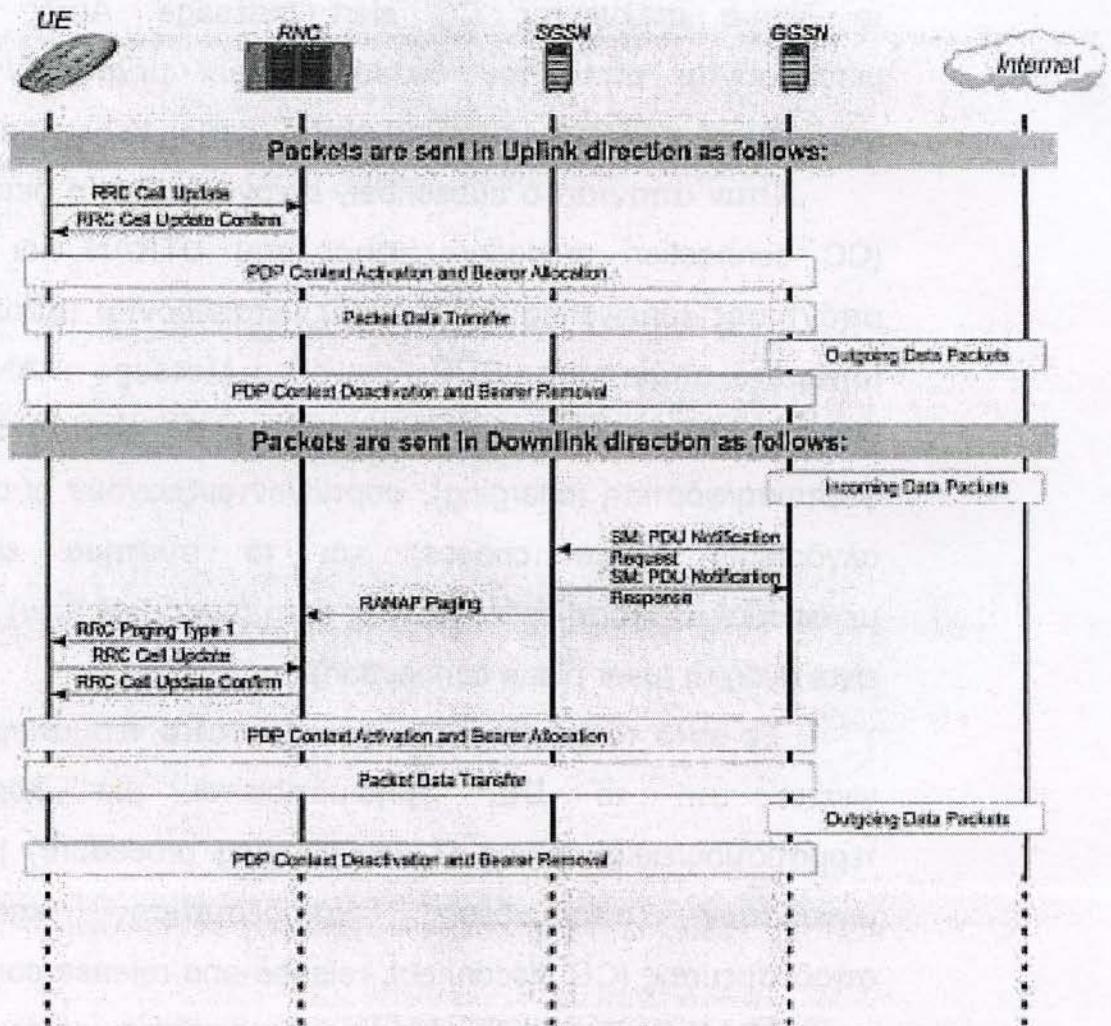
Αν το UE δεχτεί αυτήν την κλήση, το CN ξεκινάει τον εντοπισμό του RAB (RAB allocation). Έπειτα, το UE ενεργοποιεί/δραστηριοποιεί (alerts) τον εγγεγραμμένο/συνδρομητή (subscriber) και ενημερώνει γι' αυτό (alert) το δίκτυο στέλνοντας CC alert message. Αυτές οι πληροφορίες μεταφέρονται μέσω του δικτύου/δικτύων μέχρι την ανταλλαγή του συνδρομητή που πραγματοποιεί κλήση (calling subscriber exchange).

Όταν απαντάει ο subscriber, ενεργοποιείται η διαδικασία σύνδεσης (CC connection procedure) εντός του UTRAN και οι πληροφορίες απάντησης (answering information) μεταφέρονται μέσω των δικτύων με μηνύματα απάντησης (ISUP Answering Message – ANS). Τώρα που ο δίαυλος κλήσης (circuit switched call path) είναι ανοιχτός, ξεκινάει η φόρτωση/φόρτιση (charging), φορτώνονται/ξεκινούν οι σχετικοί φωνητικοί αλγόριθμοι (voice codecs) και το σύστημα είναι έτοιμο για μεταφορά/μετάδοση δεδομένων χρήστη (user data flow) καθώς η σύνδεση είναι ανοιχτή (user plane connection).

Σε αυτό το παράδειγμα, φαινομενικά ο τερματισμός της σύνδεσης γίνεται απ' το UE. Χρησιμοποιείται μια 3δρομη διαδικασία τερματισμού/εκκαθάρισης (3-way clearing procedure) με την ανταλλαγή μηνυμάτων αποσύνδεσης, αποδέσμευσης και ολοκλήρωσης αποδέσμευσης (CC disconnect, release and release complete messages) στο UTRAN. Η ίδια διαδικασία πραγματοποιείται για την πλευρά ISUP με μηνύματα αποδέσμευσης και ολοκλήρωσης αποδέσμευσης (ISUP Release and ISUPRLComplete). Αυτά τα μηνύματα σταματούν τη φόρτωση/φόρτιση (charging) και τερματίζουν τη σύνδεση μεταξύ των κόμβων (nodes). Μετά τον καθαρισμό του διαύλου (circuit switched path) το CN αποδεσμεύει τη σύνδεση RRC και το RAB μέσω διαδικασίας αποδέσμευσης lu (lu release procedure).

10.5 Packet Data Example

Η εικόνα 143 απεικονίζει ένα μικρό δείγμα απ' το τι συμβαίνει κατά τη διάρκεια μιας packet session. Είναι επόμενο να υποθέσουμε ότι το UE μετακινείται συνεχώς στην περιοχή του UTRAN.



Εικόνα 143 Μεταφορά πακέτα δεδομένων – uplink και downlink

Κάτω απ' αυτές τις συνθήκες η εφαρμογή του χρήστη (user application) στο UE συνηθίζει να στέλνει πακέτα δεδομένων (data packets) στο δίκτυο (uplink). Από τη στιγμή που το UE μετακινείται συνεχώς, πρέπει πρώτα να εκτελέσει ανανέωση cell (cell update). Με τον τρόπο αυτό, το UE

βεβαιώνει με ακρίβεια cell (cell accuracy) ότι οι πληροφορίες θέσης/στίγματος του (location information) είναι έγκυρες.

Μετά την ανανέωση cell (cell update) το UE είναι σε θέση να ζητήσει ενεργοποίηση περιεχομένου PDP (PDP context activation) μέσω του τρέχοντος (current) cell, ενώ παράλληλα μπορεί να εντοπισθεί το RAB για τη μεταφορά πακέτων δεδομένων (packet data transfer). Στο 10.8 απεικονίζεται η ολοκληρωμένη ροή μηνυμάτων (complete message flow) για αυτήν την διαδικασία.

Όταν το packet session είναι ανοιχτό, το UE εκπέμπει πακέτα δεδομένων προς το δίκτυο (uplink data packets) τα οποία καταφτάνουν πρώτα στο SRNC μέσω των ραδιοφωνικών/ασύρματων συνδέσμων/συνδέσεων (radio links), τα οποία συνθέτουν έναν ασύρματο/ραδιοφωνικό φορέα (radio bearer) γι' αυτό το session. Η κίνηση των πακέτων (packet traffic) μεταφέρεται/λαμβάνει μέρος έπειτα μεταξύ του RNC και του GGSN με το πρωτόκολλο GTP-U και η δίοδος (tunnel) αυτή αποτελείται από δύο μέρη, τον φορέα Iu (Iu bearer) εντός του Iu interface και του θεμελιώδους φορέα του PS domain (PS domain backbone bearer) μεταξύ SGSN και GGSN. Η δίοδος (tunnel) καταλήγει στο GGSN, από όπου τα πακέτα δεδομένων χρήστη (user data packets) δρομολογούνται/αποστέλονται (routed) σε ένα δίκτυο εξωτερικών πακέτων δεδομένων (external packet data network) με βάση μία μέθοδο που περιγράφηκε στον τύπο σύνδεσης παραμέτρων περιεχομένου PDP (PDP context parameter connection type). Αυτές οι παράμετροι μπορεί να έχουν τιμές (values) PPP (Point-to-Point Protocol) ή X.25. Όταν δεν υπάρχουν πλέον δεδομένα προς μεταφορά, το περιεχόμενο PDP (PDP context) απενεργοποιείται και το RAB αποδεσμεύεται. Στο 10.11 απεικονίζεται η ολοκληρωμένη ροή μηνυμάτων (complete message flow) κατά τη διάρκεια αυτής της απενεργοποίησης.

Κατά το downlink, το GGSN μπορεί να διαπιστώσει ότι καταφτάνουν πακέτα από άλλα δίκτυα. Το γεγονός αυτό ενεργοποιεί/ξεκινά τη

διαδικασία προσδιορισμού/σημείωσης μονάδας πακέτων δεδομένων (SM PDU Data Unit – notification procedure) που οδηγεί στην ενεργοποίηση περιεχομένου PDP απ' την πλευρά του δικτύου (network - initiated PDP context activation). Το SGSN, αφού λάβει το μήνυμα αίτησης (SM PDU notification request message), εκτελεί paging στα RNCs που ελέγχουν την RA όπου το UE πραγματοποίησε την τελευταία ανανέωση RA (RA update). Τα RNCs παραδίδουν/πραγματοποιούν έπειτα paging στο UE με τη μορφή RRC paging Type 1. Από τη στιγμή που κινείται/μεταβάλλεται συνεχώς, το UE εκτελεί ξανά ανανέωση cell (cell update) έτσι ώστε να καταγράψει στο RNC έγκυρες πληροφορίες cell (valid cell information).

Μετά την ανανέωση του cell (cell update) ενεργοποιείται το περιεχόμενο PDP (PDP context), προσδιορίζεται/εντοπίζεται το RAB και ξεκινάει η ροή πακέτων δεδομένων από το GGSN στο UE. Αν το UE διαθέτει data packets προς αποστολή, μπορεί να τα στείλει παράλληλα με εκείνα του GGSN. Τα πακέτα δεδομένων που μεταφέρονται uplink (προς το δίκτυο) δια/χειρίζονται όπως περιγράφηκε νωρίτερα. Όταν δεν υπάρχουν δεδομένα προς αποστολή/μεταφορά, το περιεχόμενο PDP (PDP context) απενεργοποιείται και το RAB αποδεσμεύεται.

Κεφάλαιο 11 Η Εποχή της 3G στην Ελλάδα

Εισαγωγή

Μετά από αρκετή υπομονή, οι υπηρεσίες Τρίτης Γενιάς κάνουν επιτέλους το ντεμπούτο τους στην Ελλάδα. Ας υποδεχθούμε τη hi-tech mobile χρονιά.

Η κινητή τηλεφωνία Τρίτης Γενιάς UMTS (Universal Mobile Telecommunications System), η οποία υποστηρίζει τη μεταφορά οπτικοακουστικών δεδομένων με εξαιρετικά μεγάλες ταχύτητες και υπόσχεται δυνατότητες βιντεοκλήσεων (video call), προηγμένες multimedia εφαρμογές καθώς επίσης video/ audio streaming. Αυτό σημαίνει ότι θα έχουμε την δυνατότητα να σερφάρουμε στο Internet και να κατεβάζουμε δεδομένα multimedia με ταχύτητα που αγγίζει τα 384kbps ανά δευτερόλεπτο σε σχέση με τα 57,6 kbps ανά δευτερόλεπτο των δικτύων Δεύτερης Γενιάς (GSM), ότι θα μπορούμε να μιλάμε με τους φίλους μας και να τους βλέπουμε ταυτόχρονα στην οθόνη του κινητού σας, ότι θα έχουμε την ευκαιρία να βλέπουμε video και να ακούμε την αγαπημένη μας μουσική στη συσκευή μας αλλά και να στέλνουμε MMS στους φίλους μας με πλουσιότερο περιεχόμενο και σε χρόνο ρεκόρ.

Το κρίσιμο ερώτημα που προκύπτει είναι πότε θα συμβούν όλα αυτά στην Ελλάδα; Ευτυχώς τα νέα είναι καλά, καθώς όλες οι μεγάλες εταιρείες κινητής τηλεφωνίας έχουν κάνει σημαντικά βήματα προς την ανάπτυξη και την υποδομή του δικτύου 3G αλλά και την παροχή των αντίστοιχων υπηρεσιών.

Πρώτη η **TIM** (το νέο όνομα της Telestet) ανακοίνωσε την εμπορική διάθεση των υπηρεσιών 3G. Έτσι, οι ενδιαφερόμενοι πελάτες της μπορούν να εγγραφούν στο ειδικά διαμορφωμένο οικονομικό πρόγραμμα Tim3G70 και να γνωρίσουν το θαυμαστό νέο κόσμο των υπηρεσιών Τρίτης Γενιάς. Το πακέτο 3G της εταιρείας αυτής, έχει μηνιαίο πάγιο €23 και προσφέρει 70 λεπτά δωρεάν χρόνο ομιλίας για φωνητικές κλήσεις σε δίκτυο GSM ή UMTS και χρέωση €0,0034 ανά δευτερόλεπτο για χρήση επιπλέον των 70 λεπτών. Τα πρώτα 40 MB δεδομένων που κατεβαίνουν από Internet (και WAP) είναι δωρεάν, ενώ από εκεί και πέρα υπάρχει χρέωση €0,0006/KB και €0,02/KB για πλοήγηση στο Internet και WAP αντίστοιχα. Επίσης δωρεάν είναι 15 MMS το μήνα, ενώ η χρέωση είναι €0,39 για κάθε αποστολή από κινητό σε κινητό και €0,5 ανά MMS για τη λήψη υπηρεσιών με multimedia περιεχόμενο. Η χρέωση για τις βιντεο-κλήσεις είναι €0,005 ανά δευτερόλεπτο για τον 1ο μήνα σύνδεσης και €0,01 ανά δευτερόλεπτο μετά τον 1ο μήνα, με ελάχιστη διάκεια τα 30 δευτερόλεπτα, ενώ η τιμή ενός γραπτού μηνύματος είναι €0,085. Προς το παρόν, οι συσκευές που κυκλοφορούν στην αγορά και είναι συμβατές με τις υπηρεσίες 3G της TIM είναι οι Nokia 6650, Nokia 7600, Motorola A835 και Siemens U15. Αξίζει να σημειωθεί ότι όλες οι παραπάνω συσκευές λειτουργούν σε δίκτυα τόσο GSM όσο και UMTS. Υπολογίζεται ότι η συνολική δαπάνη για την ανάπτυξη του θα ανέλθει στα 300 εκατομμύρια ευρώ.

Αλλά και η **Vodafone** έχει προχωρήσει στην υποδομή του δικτύου UMTS, η οποία αναμένεται να ολοκληρωθεί το 2008. Ωστόσο, η εταιρεία σχεδιάζει να λανσάρει στην αγορά στις αρχές του Μαΐου, υπηρεσίες 3G που θα εμπόμπουν σε δυο κατηγορίες: τις υπηρεσίες που ήδη παρέχει το πρόγραμμα Vodafone Live! Σε συνδιασμό με τις ασύλληπτες ταχύτητες που υποστηρίζει το δίκτυο Τρίτης Γενιάς και τις επαγγελματικές υπηρεσίες Vodafone Mobile Connect Card. Αξίζει να σημειωθεί ότι το συνολικό κόστος του εγχειρήματος θα φτάσει τα 600 εκατομμύρια ευρώ.

Τέλος, η **Cosmote** έχει κάνει τα πρώτα βήματα για την υποδομή του δικτύου UMTS στην Αθήνα και την Θεσσαλονίκη ενώ ο ως μεγάλος χορηγός των Ολυμπιακών Αγώνων, σχεδιάζει να επεκτείνει την ανάπτυξη του δικτύου 3G στις Ολυμπιακές Πόλεις μέσα στο 2004. Μάλιστα, η εταιρεία έχει υπογράψει και συμφωνία με την Ericsson για την παροχή του απαραίτητου εξοπλισμού. Εκτός από τις κοινές υπηρεσίες Τρίτης Γενιάς που θα παρέχει στους συνδρομητές της, η Cosmote πρόκειται να λανσάρει και ειδικές υπηρεσίες 3G για τους Ολυμπιακούς Αγώνες. Προς το παρόν, θα ξεκινήσει ένα πιλοτικό πρόγραμμα παροχής υπηρεσιών Τρίτης Γενιάς για «φιλικούς χρήστες». Υπολογίζεται ότι η συνολική επένδυση μέχρι το τέλος του έτους θα ανέρχεται στο ποσό των 35 εκατομμυρίων ευρώ.

Αλλά καλό είναι να δούμε σε ποια φάση βρίσκεται σήμερα η ανάπτυξη του δικτύου UMTS στην Ελλάδα. Έχουν ήδη προχωρήσει, από πλευράς της TIM, οι εγκαταστάσεις του δικτύου σε Αθήνα, Θεσσαλονίκη, Πάτρα και Ηράκλειο έχοντας καλύψει το 25% του πληθυσμού της Ελλάδας, ενώ σε δεύτερη φάση και ως το 2006 θα επεκταθεί το δίκτυο Τρίτης Γενιάς στις μεγαλύτερες πόλεις της Ελλάδας. Ορόσημο αποτέλεσε η έναρξη της εμπορικής διάθεσης υπηρεσιών 3ης γενιάς στις 27 Ιανουαρίου 2004. Οι πελάτες έχουν την δυνατότητα να κάνουν χρήση τις υπηρεσίες «βιντεοκλήσεων», προκειμένου να βλέπουν το συνομιλητή τους στην οθόνη του κινητού σε πραγματικό χρόνο καθώς και να χρησιμοποιούν υπηρεσίες multimedia, με υψηλότερες ταχύτητες και πλουσιότερο περιεχόμενο και να πραγματοποιούν πλοήγηση στο Internet και στο WAP με ταχύτητες, μέχρι και 384 kbps.

Ένα άλλο σημαντικό ερώτημα είναι αν η τιμή των κινητών τηλεφώνων του δικτύου UMTS είναι προσιτή ή υψηλή; Επειδή είναι μια καινούρια τεχνολογία και απαιτεί αρκετό νέο εξοπλισμό οι τιμές των κινητών θα είναι υψηλές αλλά οι πελάτες μπορούν να επιλέγουν ποιες

υπηρεσίες τους εξυπηρετούν και έτσι να μειώσουν το κόστος απόκτησης τους.

Το βασικό παράπονο των χρηστών είναι η ποιότητα σήματος. Τα κινητά 3G πόσο ποιο ευαίσθητα θα είναι σε αυτό τον τομέα; Στα κινητά 3ης γενιάς δεν τίθεται θέμα «ευαισθησίας». Η ποιότητα του σήματος εξαρτάται από τις δυνατότητες της τεχνολογίας. Θα πρέπει να υπάρχει άριστη διασύνδεση μεταξύ των δικτύων GSM και UMTS για να διασφαλιστεί ότι η επικοινωνία των χρηστών 3G δεν διακόπτεται στις περιπτώσεις που δεν υπάρχει κάλυψη UMTS, αφού αυτόματα εξυπηρετείται από το 2ης γενιάς δίκτυο της.

Υπάρχει ανταπόκριση από την πλευρά των πελατών για την 3ης γενιάς κινητή τηλεφωνία στην Ελλάδα; Αν και έχουν περάσει μόνο μερικοί μήνες από το ξεκίνημα της εμπορικής διάθεσης των υπηρειών 3ης γενιάς (κυρίως από την TIM) η ανταπόκριση των χρηστών είναι σημαντική και έχει εκφραστεί τόσο από τις επισκέψεις για ενημέρωση στα διάφορα καταστήματα εταιρειών κινητής τηλεφωνίας όσο και από κάποιες ενεργοποιήσεις κυριώς από επιχειρήσεις που ζητούν τα υψηλής δυναμικότητας χαρακτηριστικά της 3ης γενιάς.

Χρειάζονται μεγάλα κεφάλαια να επενδυθούν στην υποδομή του δικτύου; Το κεφάλαιο που απαιτείται είναι αρκετά μεγάλο γιατί η τεχνολογία αυτή είναι νέα για την Ελλάδα και δεν υπάρχει η κατάλληλη υποδομή. Για την απόκτηση μόνο της άδειας απαιτούνται 146,7 εκατ. Ευρώ. Από εκεί και πέρα χρειάζονται επενδύσεις ύψους πολλών εκατομμυρίων ευρώ που θα γίνου σταδιακά μέχρι το 2007-2008.

Ποια κινητά τηλέφωνα σήμερα υποστηρίζουν τεχνολογία 3ης γενιάς κινητής τηλεφωνίας; *Siemens U15 - Motorola A835*: Κομψά, εύχρηστα και εξοπλισμένα με hitech χαρακτηριστικά. Οι συσκευές έχουν τα ίδια τεχνικά χαρακτηριστικά αλλά κάθε εταιρεία τις έχει ντύσει με το δικό

της λογισμικό και εξωτερική εμφάνιση. Είναι τα πρώτα κινητά στην Ελλάδα που υποστηρίζουν video call με μπροστινή κάμερα, η οποία μας κινηματογραφεί την ώρα που μιλάμε, αναμεταδίδοντας σε πραγματικό χρόνο την εικόνα μας στον συνομιλητή μας. Υποστηρίζει προχωρημένες εφαρμογές multimedia και μας δίνει την δυνατότητα να κατεβάζουμε, να παίζουμε και να αναπαράγουμε video με ήχο αλλά και να κινηματογραφούμε τα δικά μας clips. Από αυτά τα κινητά δεν λείπουν οι επαγγελματικές εφαρμογές, όπως ο συγχρονισμός με το Outlook, το organizer καθώς επίσης και το Bluetooth.

Κεφάλαιο 3

Κεφάλαιο 4

Περιεχόμενα Εικόνων

Κεφαλαίο 2

1. Τύποι Εξέλιξης.....	14
------------------------	----

Κεφαλαίο 3

2. Βασικά Στοιχεία ενός ραδιο συστήματος επικοινωνίας.....	21
3. Συλλογή από κυψέλες σε ένα κυψελλοειδές δίκτυο.....	23
4. Βασική Δομή ενός κυψελλοειδούς συστήματος.....	23
5. Παρέμβαση INTER-CELL και INTRA-CELL σε ένα κυψελλοειδές σύστημα	24
6. FREQUENCY RE – USE PATTERN, FR=7 AND FR = 1.....	25
7. CDMA (CODE DIVISION MULTIPLE ACCESS).....	29
8. Το 3G System Spectrum.....	31
9. WCDMA AIR INTERFACE AND BIT TREATMENT.....	33
10. Τύποι καναλιών και η θέση τους στο UTRAN.....	34
11. Τοποθέτηση των λογικών, φυσικών καναλιών και των καναλιών μεταφοράς στην DOWNLINK κατεύθυνση.....	37
12. Τοποθέτηση των λογικών, φυσικών καναλιών και των καναλιών μεταφοράς στην UPLINK κατεύθυνση.....	39
13. WCDMA Φυσικά Κανάλια.....	41
14. DPDCH AND DPCCCH στην UPLINK και DOWNLINK κατεύθυνση.....	42
15. Random Accesses.....	44

Κεφαλαίο 4

16. BEARER / QoS αρχιτεκτονική στο UTRAN.....	46
17. UTRAN αρχιτεκτονική.....	47
18. Λογική Δομή του Σταθμού Βάσης BS.....	48
19. Αρχές Διαδικασίας διαχείρισης του QPSK.....	50
20. Χρησιμοποιημένες μέθοδοι μορφοποίησης και οι κατευθύνσεις τους.....	51
21. Λογική Δομή του RNC.....	54

22. Διαδικασία Handover.....	58
23. Γενικές αρχές των αλγορίθμων των handovers.....	60
24. INTRA-FREQUENCY HARD HANDOVER.....	61
25. INTER-FREQUENCY HARD HANDOVER.....	62
26. Intra – frequency soft handover.....	63
27. INTRA – Frequency softer Handover.....	64
28. Η micro diversity στο BS.....	65
29. Macro diversity στο BS.....	66
30. OLPC για την uplink κατεύθυνση.....	68
31. Βασικός μηχανισμός CLPC στην uplink κατεύθυνση.....	69
32. Έλεγχος ισχύς σε συνεργασία με το soft handover.....	70
33. Site Selection Diversity (SSDT).....	71
34. Σχέση μεταξύ των SRB, RB, signalling connection, RACH and the role of RNC.....	73
35. Κατάσταση αυτοματισμού του RNC.....	75

Κεφαλαίο 5

36. Αρχιτεκτονική του Bearer and του QoS architecture στο CN.....	80
37. Παγκόσμιο Δίκτυο για ασύρματη πρόσβαση.....	80
38. Αρχιτεκτονική του CN.....	81
39. Το interface του CN στην 3GPP R99.....	84
40. Παγκόσμιες Ταυτότητες Χρηστών Κινητής Τηλεφωνίας (IMSI).....	86
41. Αριθμός ISDN του χρήστη κινητής τηλεφωνίας (MSISDN).....	87
42. Αριθμός Roaming για τον χρήστη κινητής τηλεφωνίας (MSRN).....	88
43. Θέση της ταυτότητας του προσωρινού χρήστη κινητής τηλεφωνίας (TMSI)	43
44. Παγκόσμια ταυτότητα εξοπλισμού κινητής τηλεφωνίας (IMEI).....	89
45. MM λογικές οντότητες και οι σχέσεις τους.....	91
46. Μοντέλο MM σε μεταγωγή κυκλώματος (MM).....	92
47. Μοντέλο MM σε μεταγωγή πακέτου (PMM).....	92
48. Αρχικό διάγραμμα διαχείρισης σύνδεσης μεταγωγής κυκλώματος.....	94
49. Η δύναμη ανάκλασης και από που προέρχεται αυτή.....	95

Κεφαλαίο 6

50. Θέση των κύριων οντοτήτων σε ένα UE.....	103
51. Παράγοντες που επηρεάζουν το UE.....	103
52. Ταυτότητα των μοντέλων των χρηστών στο GSM και στην 3G.....	110
53. Conceptual UMTS τερματικά.....	112

Κεφαλαίο 7

54. Οι υπηρεσίες στο UMTS και οι θέσεις τους στο δίκτυο.....	113
55. Οι υπηρεσίες 3 ^{ης} γενιάς και η επιχειρηματική αλυσίδα.....	114
56. Ο πίνακας με τα bit rates του UMTS.....	114
57. Χαρακτηριστικά του UMTS bearer service (partial and indicator).....	118
58. Χαρακτηριστικά του UMTS radio access bearer service (partial and indicator).....	118
59. Παράγοντες που επηρεάζουν το QoS (pronocative).....	120
60. Κατάσταση του κόστους δικτύων και του QoS (pronocative).....	121
61. Δυνατότητες υπηρεσιών στην εφαρμογή 3GPP R99.....	124
62. Δυνατότητες υπηρεσιών στην εφαρμογή 3GPP R4/R5.....	126
63. Διάλογος στο WAP – ιδεώδες διάγραμμα.....	127
64. Round Trip Time (RRT) positioning.....	130
65. Time of arrival (TOA) positoning.....	131
66. Time Difference of Arrival (TDOA) positioning.....	133
67. Angle of Arrival (AOA) positioning.....	135
68. GPS positioning.....	136
69. GPS positioning.....	139
70. Cell ID based positioning, general procedure.....	141
71. Assisted GPS.....	144
72. General LCS architecture in UMTS.....	146
73. Μοντέλο αναφοράς LCS.....	147
74. Αρχές του MExE.....	154
75. Profiles των χρηστών.....	155
76. Αρχές του USAT.....	156
77. Περιβάλλον λειτουργίας του CAMEL.....	158
78. Παράδειγμα για τις ικανότητες των υπηρεσιών.....	159
79. Υπηρεσίες που κληρονομούνται από το GSM και η μεταχείρισή τους στο 3GPP R99.....	162
80. VoIP και δίκτυα.....	163
81. Το περιβάλλον του H.323 πρωτοκόλλου.....	165
82. Η συνομιλία σηματοδότησης με παράδειγμα το SIP και ISUP.....	167
83. παράδειγμα για τη χρήση της πηγής MP3.....	168
84. Οι αρχές του VHE.....	171

Κεφαλαίο 8

85. Η ασφάλεια και ο ρόλος της στη 3G.....	174
86. Ενεργή επίθεση.....	177
87. Αίτηση και απάντηση εξακρίβωσης δεδομένων.....	180
88. Αίτηση και απάντηση εξακρίβωσης χρήστη.....	182
89. Γενιά του φορέα εξακρίβωσης.....	183
90. Χειρισμός της εξακρίβωσης στο USIM.....	185
91. Επαναληπτική Διαδικασία συγχρονισμού.....	187
92. Αλλαγή ροής στο UMTS.....	190
93. Κωδικός εξακρίβωσης μηνύματος.....	194
94. Encapsulation Security Payload (ESP).....	202
95. Πρωτόκολλα ασφαλείας σε διαφορετικά OSI επίπεδα.....	204

Κεφαλαίο 9

96. Μοντέλο αναφοράς των πρωτοκόλλων του ραδιο interface.....	206
97. Γενικό μοντέλο UTRAN (Αναφερόμενοι στις προδιαγραφές της 3GPP: $x=1$ Iu protocol; $x=2$ Iur protocols; $x=3$ Iub protocols).....	208
98. Τα πρωτόκολλα μη προσπέλασης του UMTS.....	211
99. Αρχιτεκτονική των UMTS πρωτοκόλλων εσωτερικής λειτουργίας.....	214
100. Τα πρωτόκολλα δικτύου μεταφοράς στο 3GPP R99.....	215
101. Το φυσικό επίπεδο στο Uu interface.....	216
102. Το φυσικό επίπεδο σε άλλα interfaces.....	216
103. Δίκτυο μεταφοράς – Μέση πρόσβασης έλεγχος.....	219
104. Συνδιασμοί μεταφοράς στο MAC πρωτόκολλο.....	220
105. Μεταφορά δικτύου – έλεγχος ραδιοένωσης.....	221
106. Εσωτερική οργάνωση του RLC με τη βοήθεια του MAC στα αφοσιωμένα κανάλια.....	222
107. Δομή του ATM cell.....	225
108. Η δομή των επικεφαλίδων των ATM κυψελών.....	227
109. Γενική Δομή του AAL.....	228
110. Επίπεδα εφαρμογής του ATM τα οποία χρησιμοποιούνται στα UTRAN interfaces.....	228
111. Ραδιο Δίκτυο RANAP.....	233
112. Ραδιοδίκτυο – RNSAP.....	235
113. Ραδιοδίκτυο NBAP.....	238
114. Λειτουργικό περιβάλλον του NBAP.....	240
115. Ραδιοδίκτυο – (RRC) πρωτοκόλλου.....	242
116. Λογική Δομή ενός RRC πρωτοκόλλου στο WCDMA-FDD.....	243
117. Ραδιοδίκτυο σε user plane- PDCP.....	246
118. Ραδιοδίκτυο του user plane - UTRAN πρωτόκολλα.....	248
119. Frame πρωτόκολλα για τα αφιερωμένα κανάλια του Iub/Iur.....	249

120. Frame πρωτόκολλα για κοινά κανάλια μεταφοράς του Iub/Iur.....	250
121. MM non-access stratum πρωτόκολλα για το PS domain.....	256

Κεφαλαίο 10

122. Βασικό μοντέλο της transactions του UMTS δικτύου.....	261
123. Paging Type 1.....	263
124. Paging Type 2.....	264
125. Εγκατάσταση σύνδεσης RRC.....	265
126. Transaction Reasoning.....	268
127. Έλεγχος εξακρίβωσης και ασφάλειας.....	269
128. Εγκατάσταση transaction με την Allocation του Radio Access Bearer (RAB) (Circuit Switched)	271
129. Εγκατάσταση transaction με την Allocation του Radio Access Bearer (RAB) (Packet Switched).....	274
130. Transaction Clearing και απελευθέρωση του RAB.....	275
131. Transaction Clearing με απελευθέρωση του Iu (Circuit Switched).....	276
132. Transaction Clearing με απελευθέρωση του RAB (Packet Switched).....	277
133. Transaction Clearing με απελευθέρωση του RANAP (Packet Switched).....	278
134. RRC Connection Release.....	279
135. Soft Handover – Link Addition.....	281
136. Soft Handover – Link Deletion.....	283
137. SRNS Relocation – Circuit Switched (το USE δεν περιλαμβάνεται).....	285
138. Inter – System Handover from UMTS to GSM – Circuit Switched.....	287
139. Διαδικασία εγκατάστασης κυψέλης.....	291
140. Αναβάθμιση της διαδικασίας URA	292
141. Αναβάθμιση τοποθεσίας στο CN CS.....	293
142. Κλήση μεταγωγής κυκλώματος – USE terminating – UE clears.....	298
143. Μεταφορά πακέτα δεδομένων – uplink και downlink.....	301



Βιβλιογραφία

Η βιβλιογραφία περιλαμβάνει κάποιες πηγές οι οποίες είναι χρήσιμες για πληροφορίες στα ακόλουθα θέματα

- ✓ Radio Communications (CDMA συστήματα)
- ✓ Προδιαγραφές για την 3GPP
- ✓ Δίκτυα ATM και τα πρωτόκολλά τους
- ✓ Δίκτυα IP και τα πρωτόκολλά τους
- ✓ Τοποθέτηση κινητού τερματικού
- ✓ Πρωτόκολλα WAP και οι υπηρεσίες τους
- ✓ Αλγόριθμοι Ασφάλειας και πρωτόκολλα

1. Ηλεκτρονικές Αναζητήσεις

- ✓ Προδιαγραφές για την 3GPP: <http://www.3gpp.org>
- ✓ Προδιαγραφές για την Internet Engineering Task Force (IETF): <http://www.ietf.org>
- ✓ Προδιαγραφές για το Wireless Application Protocol (WAP) από το forum του: <http://www.wapforum.org>
- ✓ Προδιαγραφές για το UMTS Network από το forum του: <http://www.umtsforum.org>

2. Άλλες λογοτεχνικές πηγές

- ✓ Wiley. UMTS NETWORKS (Architecture, Mobility and Services), Heikki Kaaranen, Ari Ahtiainen, Lauri Laitinen, Siamak Naghian, Valtteri Niemi, 2001, 302pp.
- ✓ Black U. ATM, volume II: Signaling in broadband networks. Englewood Cliffs, NJ: Prentice Hall, 1998, 224pp.
- ✓ Black U. ATM, volume I: Foundation for broadband networks. Englewood Cliffs, NJ: Prentice Hall, 1999, 450pp.
- ✓ Corner DE. Internetworking with TCP/IP, volume I: Principles, protocols and architecture, 4th edition. Englewood Cliffs, NJ: Prentice Hall, 2000, 775pp.
- ✓ Περιοδικό Tomorrow, Τεύχος 34, Μάρτιος 2004

Βιβλιογραφία

Η βιβλιογραφία περιλαμβάνει κάποιες πηγές οι οποίες είναι χρήσιμες για τη μελέτη του θέματος.

- ✓ Radio Communications (CDMA συστήματα)
- ✓ Προβλήματα για την 3GPP
- ✓ Δίκτυα ATM και τα πρωτόκολλα τους
- ✓ Δίκτυα IP και τα πρωτόκολλα τους
- ✓ Τεχνολογίες κινητού τηλεφώνου
- ✓ Πρωτόκολλα VoIP και οι υπηρεσίες τους
- ✓ Ασύρτητες Αποστάσεις και Πρωτόκολλα

1. Ηλεκτρονικές Αναφορές

- ✓ Προβλήματα για την 3GPP: <http://www.3gpp.org>
- ✓ Προβλήματα για την Internet Engineering Task Force (IETF): <http://www.ietf.org>
- ✓ Προβλήματα για το Wireless Application Protocol (WAP) και το forum του: <http://www.wapforum.org>
- ✓ Προβλήματα για το UMTS Network and the forum του: <http://www.umtsforum.org>

2. Άλλες Λογισμικές Πηγές

- ✓ Wiley UMTS NETWORKS (Architecture, Mobility and Services), Håkan Karlsson, Anu Ahtainen, Lantti Laitinen, Simeon Nishjan, Valden Niemi, 2001, 302pp.
- ✓ Black U. ATM, volume II: Signaling in broadband networks, Englewood Cliffs, NJ: Prentice Hall, 1998, 224pp.
- ✓ Black U. ATM, volume I: Foundation for broadband networks, Englewood Cliffs, NJ: Prentice Hall, 1999, 450pp.
- ✓ Comer DE, Internetworking with TCP/IP, volume I: Principles, protocols and architecture, 4th edition, Englewood Cliffs, NJ: Prentice Hall, 2000, 725pp.
- ✓ Θεωρητικό Τεχνολογίας, Τεύχος 34, Μάρτιος 2004



Η βιβλιογραφία περιλαμβάνει κάποιες πηγές οι οποίες είναι χρήσιμες για τη μελέτη του θέματος.

