Κινητές επικοινωνίες

Κεφάλαιο 7

Γενιά 3G - UMTS

Εισαγωγή

- Ο Οργανισμός ITU σχεδίασε το σύστημα IMT-2000 (International Mobile Telecommunications System) με σκοπό να συγκεράσει τα πλεονεκτήματα του GSM και του GPRS με υπηρεσίες διαδικτύου, όπως ηλεκτρονικό ταχυδρομείο, τηλεδιάσκεψη, πρόσβαση σε ιστοσελίδες, ηλεκτρονικό εμπόριο και εφαρμογές πολυμέσων.
- Κομμάτι το IMT-2000 είναι το UMTS (Universal Mobile Telecommunications System).

Εισαγωγή (συνέχεια)

- Το IMT-2000 ξεκίνησε με στόχο να υπάρξει ένα και μοναδικό σύστημα τρίτης γενιάς για όλη την υφήλιο.
- Για λόγους τεχνικούς αλλά και πολιτικούς, ο στόχος αυτός δεν επετεύχθη.
- Η πολιτική της ITU ήταν αρκετά ελαστική προκειμένου να θεωρήσει κάποιο σύστημα συμβατό με το πρότυπο IMT-2000. Επομένως, στο πρότυπο εντάχθηκαν σχεδόν όλα τα συστήματα που πληρούσαν κάποιες υποτυπώδεις προδιαγραφές, με αποτέλεσμα το IMT-2000 να αποτελεί μία οικογένεια προτύπων.
- Επικράτησε η τεχνολογία που συνδυάζει το WCDMA με το GSM.
- Ο λόγος για αυτή την επικράτηση είναι το ότι η τεχνολογία GSM ήταν ήδη η πιο διαδεδομένη, άρα η τεχνολογία αυτή ήταν η οικονομικότερη.
- Ο συνδυασμός του WCDMA με τις εξελίξεις του GSM όσον αφορά το κεντρικό δίκτυο, ονομάζεται Universal Mobile Telecommunications System (UMTS).

Υπηρεσίες στο UMTS

- Internet access—Messaging, video/music download, voice/video over IP, mobile commerce, travel and information services
- Intranet/extranet access—Enterprise application (e-mail/messaging, travel assistance, mobile sales, technical services, corporate database access, fleet/warehouse management, conferencing and video telephony)
- Customized information/entertainment—Information (photo/video/music download), travel assistance, distance education, mobile messaging, gaming, voice portal services
- Multimedia messaging—SMS extensions for images, video, and music; unified messaging; document transfer
- Location-based services—Yellow pages, mobile commerce, navigational service, trading

WCDMA

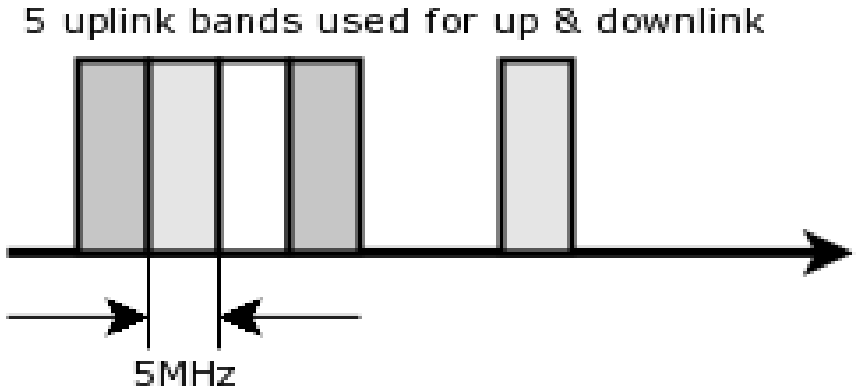
- Εύρος ζώνης : 5 MHz (Wide CDMA γιατί έχει μεγαλύτερο εύρος ζώνης από ό,τι το CDMA που ήδη χρησιμοποιούνταν στην Αμερική – CDMA2000)
- CDMA: Ο αποστολέας της πληροφορίας, πριν αποστείλει τα δεδομένα, τα πολλαπλασιάζει με τον κώδικά του. Ο παραλήπτης γνωρίζει εκ των προτέρων τον κώδικα του αποστολέα. Όταν ο παραλήπτης πολλαπλασιάσει τα δεδομένα που έλαβε με τον κώδικα του αποστολέα, τότε ανακτά τα αρχικά δεδομένα. Μετά από αυτόν τον υπολογισμό, τα υπόλοιπα δεδομένα που εστάλησαν από άλλους χρήστες, δεν επηρεάζουν καθόλου (απορρίπτονται ως θόρυβος). Αυτό οφείλεται χάρη στην κατάλληλη επιλογή των κωδίκων.
- Όλοι οι χρήστες μεταδίδουν ταυτόχρονα, την ίδια χρονική στιγμή και στην ίδια συχνότητα.
- Το CDMA αναπτύσσεται και περιγράφεται στο εργαστήριο του παρόντος μαθήματος.

Πολυπλεξία στο UMTS

- Το WCDMA είναι και η κύρια διαφορά μεταξύ UMTS και GSM/GPRS (όπου εκεί έχουμε TDMA/FDMA πολυπλεξία).
- Το WCDMA έχει δύο τρόπους λειτουργίας: TDD (Time Division Duplex) και FDD (Frequency Division Duplex)

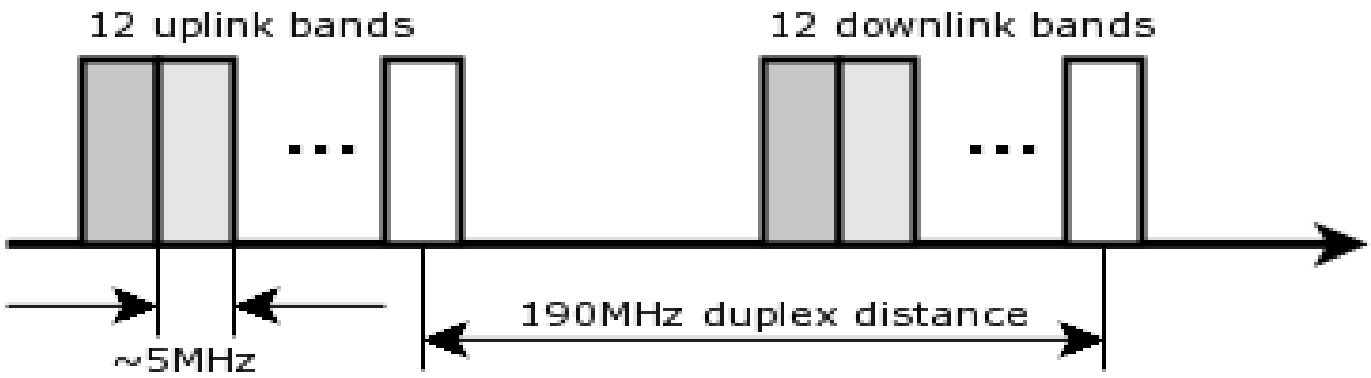
UMTS TDD

- Uplink & Downlink: 1900 - 1920 MHz and 2020 - 2025 MHz
  - 5 «παράθυρα» συχνοτήτων εύρους 5MHz
  - 15 χρονοθυρίδες ανά πλαίσιο.
  - Ένας χρήστης μπορεί να χρησιμοποιεί περισσότερες από μία χρονοθυρίδες.
  - Και οι δύο κατευθύνσεις (uplink και downlink) χρησιμοποιούν την ίδια ζώνη συχνοτήτων. Στην περίπτωση αυτή οι 15 χρονοθυρίδες κάθε πλαισίου κατανέμονται δυναμικά μεταξύ του ανερχόμενου και του κατερχόμενου συνδέσμου.

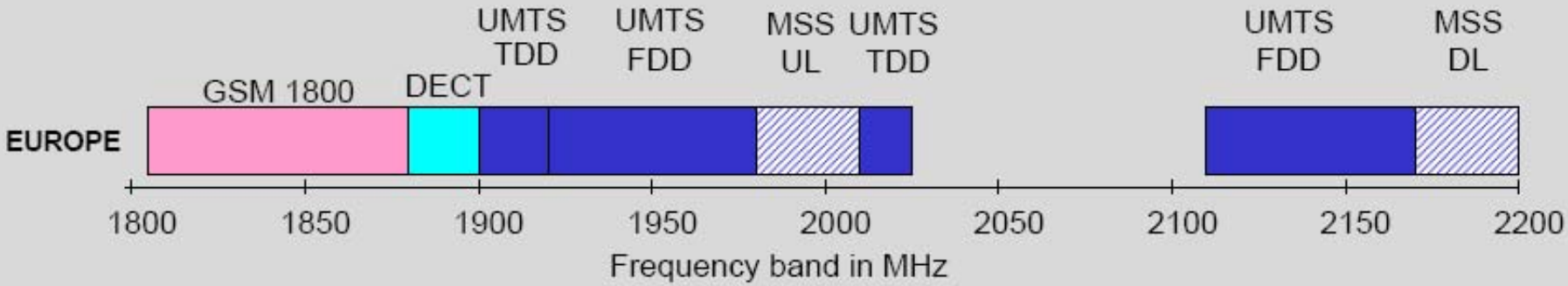


UMTS FDD

- Uplink: 1920 - 1975 MHz
- Downlink: 2110 - 2165 MHz
- 190 MHz απόσταση μεταξύ uplink - downlink
- 12 «παράθυρα» συχνοτήτων (carriers) για το uplink και άλλα τόσα για το downlink, όλα εύρους 5MHz
- Στον FDD ο ανερχόμενος και ο κατερχόμενος σύνδεσμος χρησιμοποιούν διαφορετικές ζώνες συχνοτήτων, κάθε μία από τις οποίες έχει εύρος ζώνης 5 MHz.



Ελληνική πραγματικότητα



*FDD 2*60MHz (1920-1980MHz, 2110-2170MHz)*
TDD 25MHz (1900-1920MHz, 2020-2025MHz)

Κινητά συστήματα 3ης γενιάς στην Ελλάδα:

2*20MHz FDD και 5MHz TDD στην VODAFON, έναντι περίπου 60δις

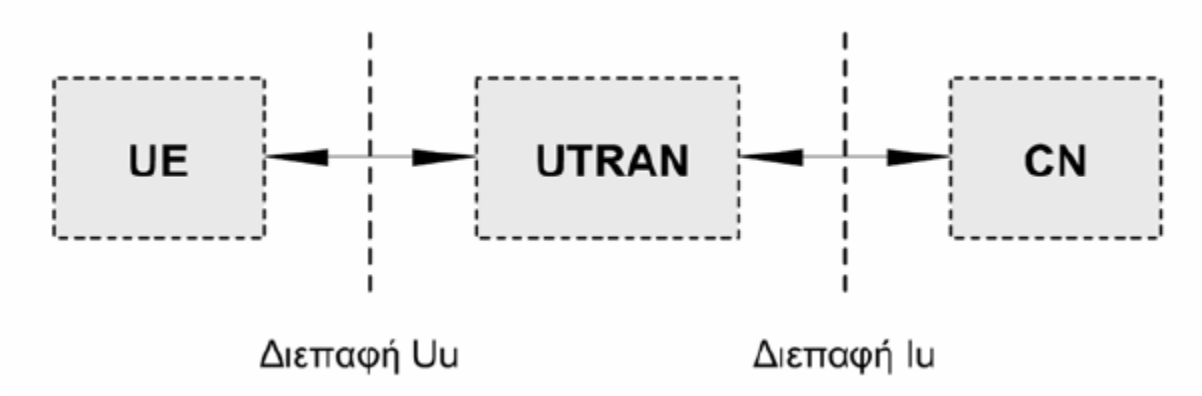
2*15MHz FDD και 5MHz TDD στην COSMOTE, έναντι περίπου 55δις

2*10MHz FDD και 5MHz TDD στην TIM HELLAS, έναντι 50δις.

UMTS – Ταχύτητες

- Το UMTS αυξάνει τις δυνατότητές του δικτύου κινητής τηλεφωνίας και υποστηρίζει μεγάλους ρυθμούς μετάδοσης:
  - GSM (9.6Kbps)
  - GPRS (115Kbps)
  - EDGE (384 Kbps)
  - UMTS (1920 Kbps)

Δομή του UMTS

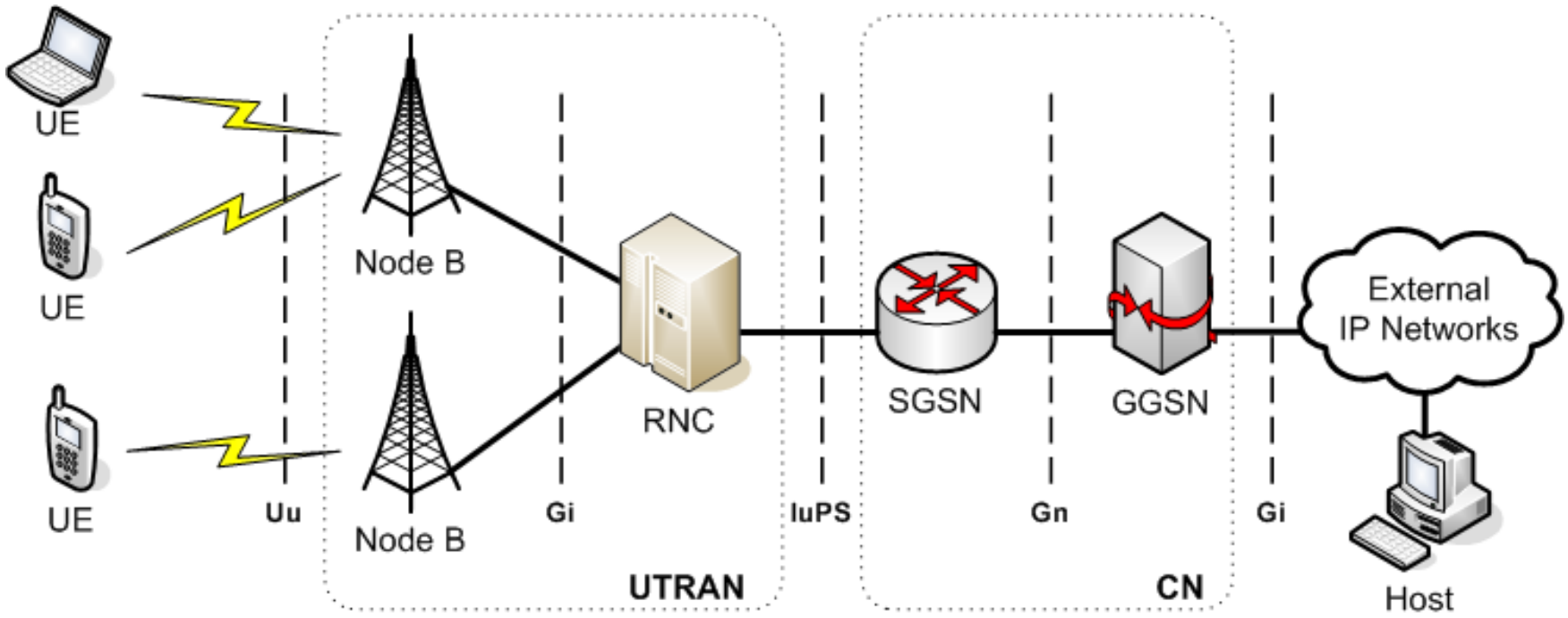


- UE: User Equipment
- UTRAN: UMTS Terrestrial Radio Access Network
- CN : Core Network

UMTS – Αρχιτεκτονική (I)

- Το UMTS αποτελείται:
  - CN (Core Network)
    - SGSN
    - GGSN
    - Κόμβοι GSM
  - UTRAN (UMTS Terrestrial Radio Access Network – RAN)
    - RNC (Radio Network Controller)
    - Node B
  - UE (User Equipment)

UMTS – Αρχιτεκτονική (II)



Φορητή Συσκευή (User Equipment)

- Είναι συνδεδεμένη με το UTRAN, μέσω διεπαφής Uu, που βασίζεται στο WCDMA.
- Μπορεί να συνδεθεί ταυτόχρονα με περισσότερες από μία κυψέλες.
- Αποτελείται από:
  - Mobile Equipment (η ίδια η συσκευή)
  - Κάρτα USIM: Αντίστοιχη της κάρτας SIM του GSM, αλλά με πολύ μεγαλύτερη χωρητικότητα (Mbyte αντί για 32kbyte)

UTRAN

- Νέο δίκτυο, ειδικά σχεδιασμένο για το UMTS.
- Βασικότερη λειτουργία του είναι η εποπτεία και η διαχείριση των ασύρματων πόρων του δικτύου
  - Διαχείριση μεταπομπών, έλεγχος της ισχύος

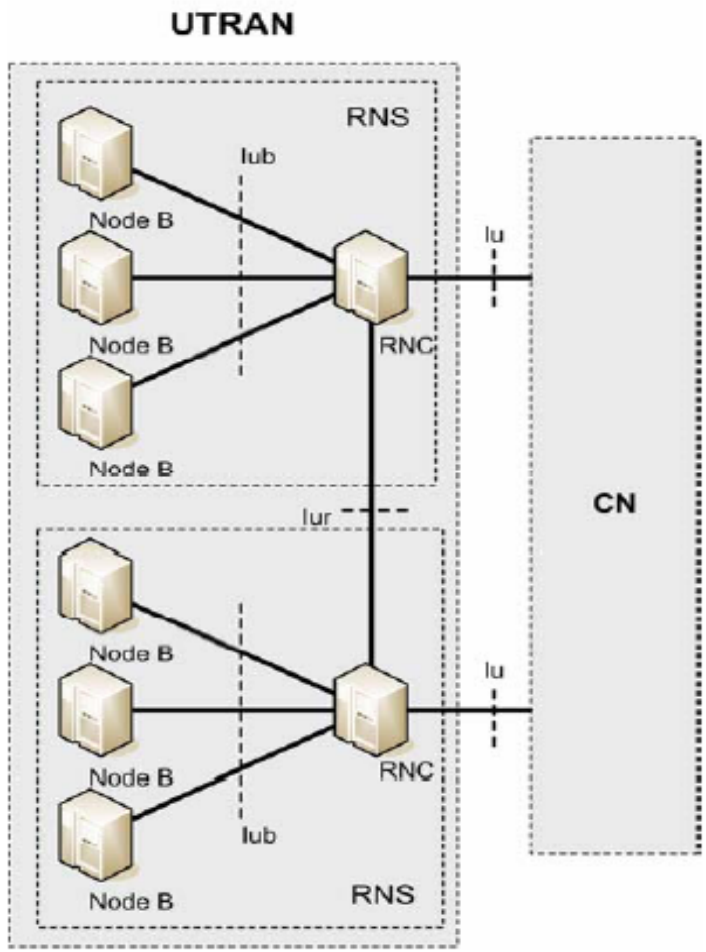
Η δομή του UTRAN

Οι Κόμβοι Β είναι υπεύθυνοι για τον έλεγχο ενός ή περισσοτέρων κυψελών. Μία ομάδα από Κόμβους Β συνδέεται με έναν κόμβο RNC (Radio Network Controller).

Ένας Κόμβος Β μεταφέρει δεδομένα προς τον RNC στον οποίο είναι συνδεδεμένος. Επιπλέον, κάνει μετρήσεις πάνω στην ποιότητα και την ισχύ των ασύρματων συνδέσμων προς τα UEs και δίνει αναφορές στον RNC. Ο Κόμβος Β μπορεί να συνδέεται με ένα ή περισσότερα BTS (συνήθως με τρία).

Ένας κόμβος RNC, που είναι αντίστοιχος του BSC σε λειτουργικότητα, μαζί με τους συνδεδεμένους σε αυτόν Κόμβους Β αποτελούν ένα Radio Network Subsystem (RNS). Ο RNC λαμβάνει τις πληροφορίες που συλλέγουν οι Κόμβοι Bs του δικού του RNS και προσαρμόζει τις παραμέτρους του ασύρματου υποσυστήματος. Μία τέτοια παράμετρος μπορεί να είναι η ισχύς του ασύρματου σήματος στο UE ή στον Κόμβο Β.

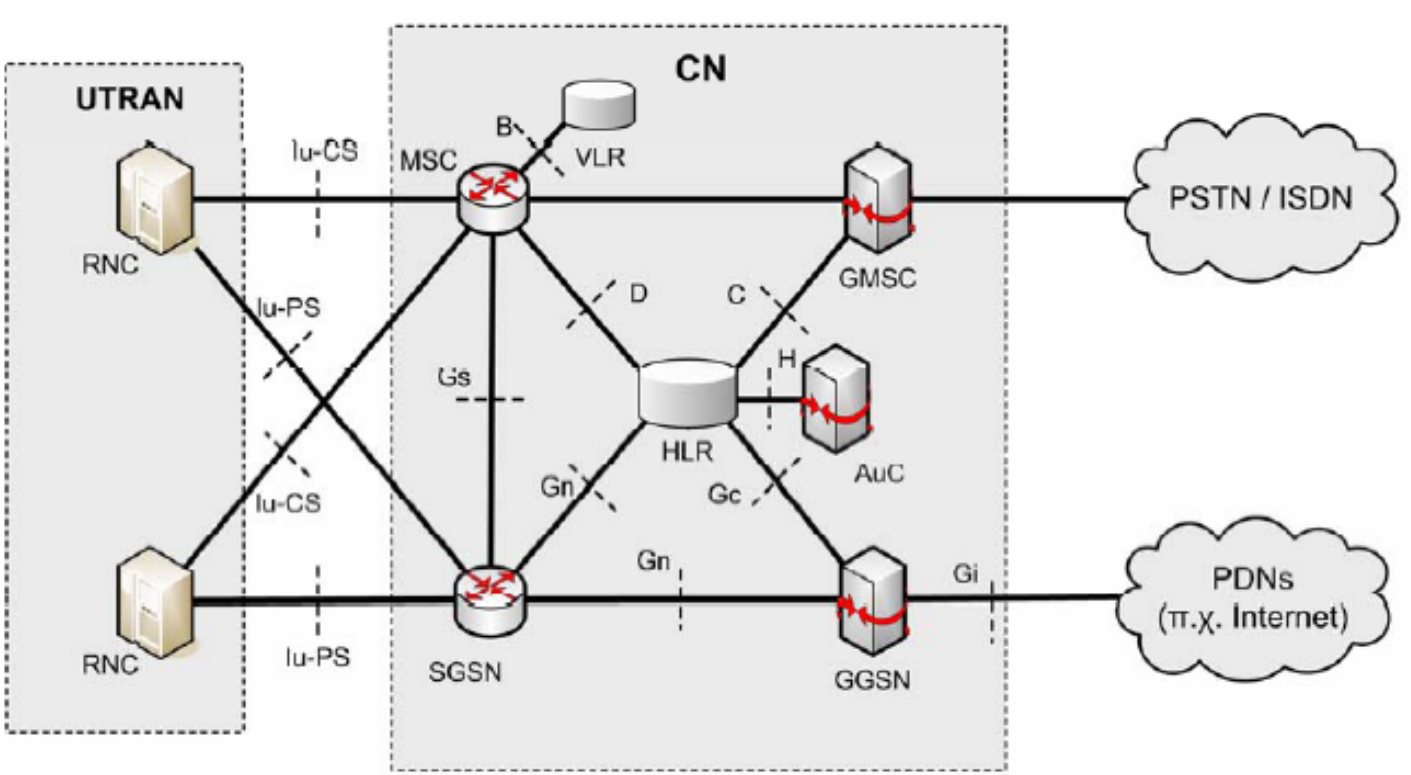
Επίσης, ο RNC είναι υπεύθυνος για την ανάθεση του κώδικα WCDMA που θα χρησιμοποιήσουν ο Κόμβος Β και η κινητή συσκευή στη μεταξύ τους επικοινωνία. Τέλος, οι κόμβοι RNC ελέγχουν τις μεταπομπές μεταξύ διαφορετικών RNSs.



Δίκτυο Κορμού (Core Network)

- Συνδέεται με άλλα δίκτυα (PSTN, Internet κ.α.)
- Είναι υπεύθυνο για τη δρομολόγηση, την ταυτοποίηση, τον εντοπισμό των χρηστών κ.α.

Δομή του CN



- Αποτελείται από μονάδες μεταγωγής κυκλώματος (CS) και μεταγωγής πακέτου (PS)

CN: Μονάδες μεταγωγής κυκλώματος

- **MSC:** Κόμβος μεταγωγής ο οποίος δρομολογεί τα δεδομένα των υπηρεσιών μεταγωγής κυκλώματος εντός του δικτύου UMTS. Κάθε κόμβος MSC διαχειρίζεται πολλά RNCs. Είναι επίσης συνδεδεμένος με τις βάσεις δεδομένων του δικτύου, δηλαδή τον HLR και τον VLR. Τέλος, διαχειρίζεται την κινητικότητα των χρηστών για τις υπηρεσίες μεταγωγής κυκλώματος.

- **GMSC:** Ο κόμβος GMSC είναι συνδεδεμένος με τους κόμβους MSC. Η λειτουργία του είναι να διασυνδέει το δίκτυο UMTS με άλλα δίκτυα μεταγωγής κυκλώματος όπως PSTN και ISDN.

- **VLR:** Βάση δεδομένων (όπως ακριβώς στο GSM), όπου αποθηκεύει προσωρινή πληροφορία σχετικά με την ταυτοποίηση και την ασφάλεια καθώς και άλλες χρήσιμες πληροφορίες που σχετίζονται με όλους τους χρήστες που διαχειρίζεται κάθε δεδομένη στιγμή ο αντίστοιχος MSC. Ο VLR λαμβάνει την αρχική πληροφορία από τον HLR και αναλαμβάνει να τον ενημερώσει για τυχόν μεταβολές στα δεδομένα του. Όλες οι συναλλαγές μεταξύ VLR και HLR γίνονται μέσω ενός MSC.

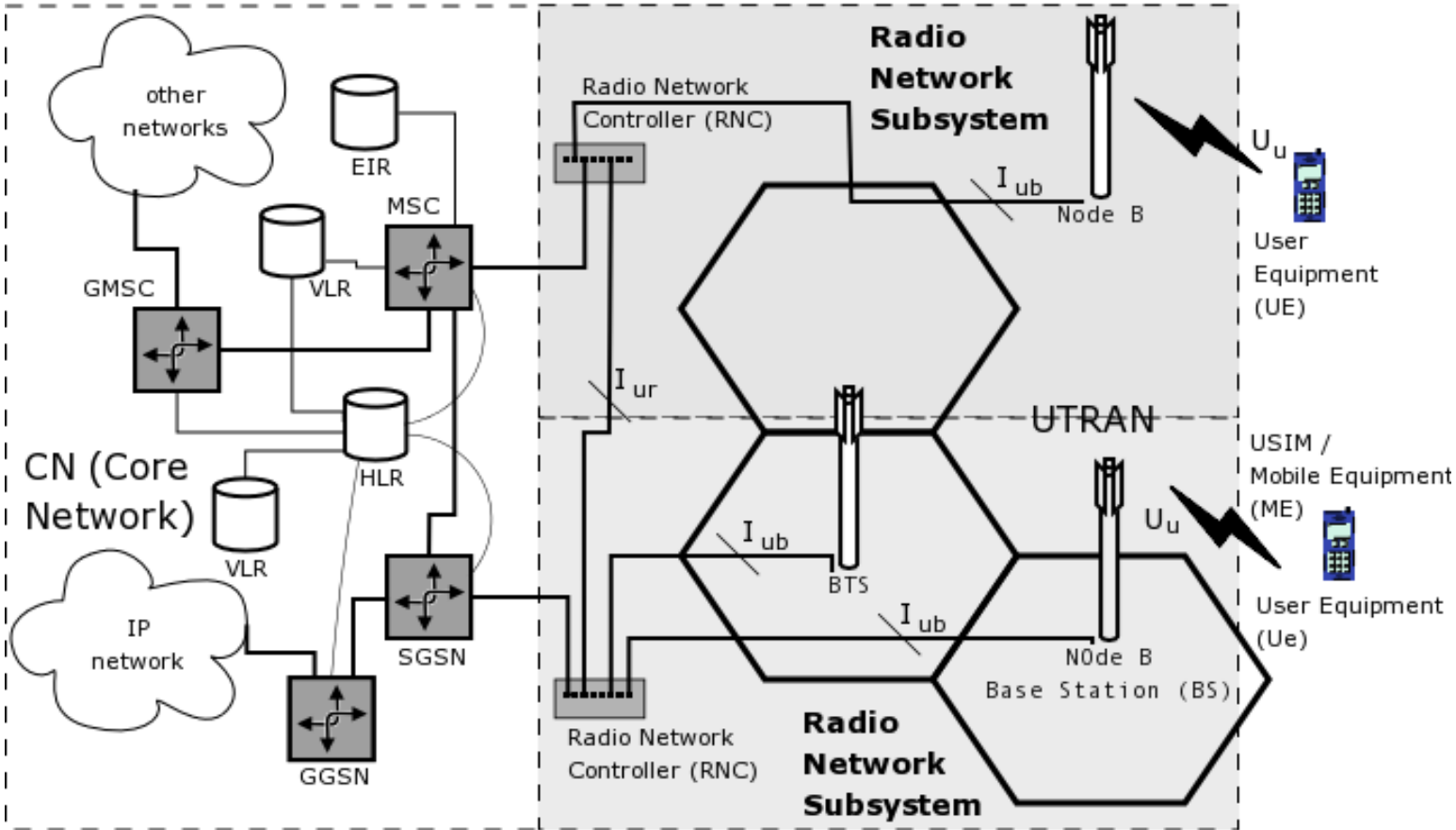
CN: Μονάδες μεταγωγής πακέτου

- ***Serving GPRS Support Node (SGSN)*:** Ο SGSN αποτελεί τον αντίστοιχο κόμβο του MSC για τη μεταγωγή πακέτου. Αυτό σημαίνει ότι αναλαμβάνει τη δρομολόγηση δεδομένων των υπηρεσιών μεταγωγής πακέτων εντός του δικτύου UMTS. Επιπλέον, διαχειρίζεται τους κόμβους RNCs οι οποίοι είναι συνδεδεμένοι σε αυτόν. Αλληλεπιδρά με βάσεις δεδομένων, όπως ο HLR. Τέλος, ο κόμβος SGSN είναι υπεύθυνος για τη διαχείριση της κινητικότητας των χρηστών για τις υπηρεσίες μεταγωγής πακέτων.

- ***Gateway GPRS Support Node (GGSN)*:** Πρόκειται για έναν κόμβο αντίστοιχο του GMSC του πεδίου CS. Διασυνδέει τους κόμβους SGSNs με εξωτερικά δίκτυα μεταγωγής πακέτων όπως το X.25 και το Internet.

Συγκεντρωτικά

- **Η σύγκλιση του GSM και του GPRS στο UMTS γίνεται προφανής από τα παραπάνω – «ίδιοι» κόμβοι, με τις ίδιες λειτουργίες.**
- **Αντίστοιχα, στο UMTS υπάρχουν οι HLR και AuC, με ανάλογες λειτουργίες όπως στο GSM ή GPRS (δεν εντάσσονται ούτε στο PS τμήμα ούτε στο CS)**



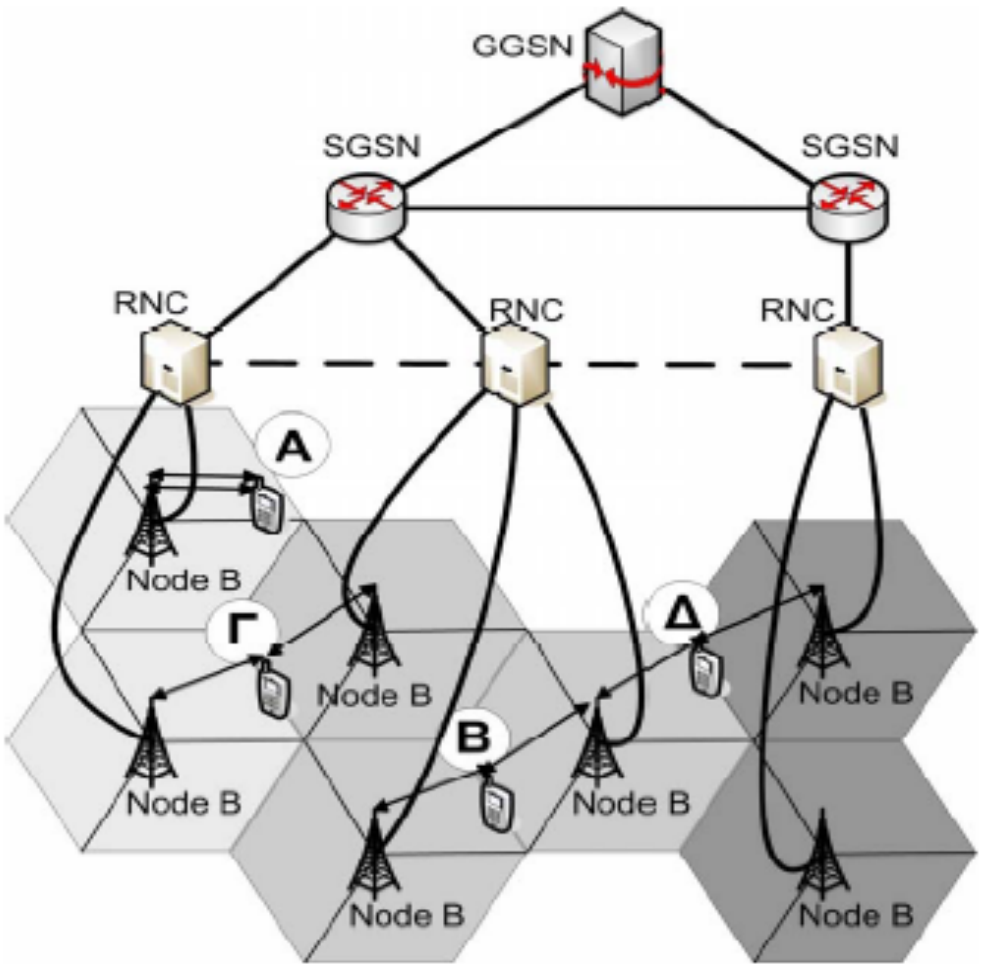
Οι μεταπομπές στο UMTS

- Τα handovers στο CDMA (συστήματα UMTS) διαφέρουν κατά πολύ από τα handovers στο TDMA (συστήματα GSM). Αυτό γιατί στο UMTS, αντίθετα με το GSM όλα οι συσκευές χρησιμοποιούν διαρκώς το ίδιο φάσμα συχνοτήτων.
- Υπάρχουν διάφορα είδη μεταπομπών

Soft και softer handover

- Κατά τη διάρκεια ενός soft handover, το κινητό είναι συνδεδεμένο ταυτόχρονα σε περισσότερους από έναν Κόμβους Β. Επειδή οι μεταδόσεις αυτές γίνονται στην ίδια συχνότητα, η συσκευή τις αντιλαμβάνεται σαν τμήματα της ίδιας πληροφορίας. Το μόνο που διαφέρει σε κάθε τμήμα είναι ο κώδικας διαμόρφωσης που χρησιμοποιείται σε κάθε μετάδοση. Όταν η σύνδεση με έναν από τους Κόμβους Β δεν είναι απαραίτητη, η αντίστοιχη σύνδεση μπορεί να εγκαταλειφτεί. Το soft handover Λαμβάνει χώρα όταν το κινητό κινείται στα όρια δύο κυψελών.
- Το softer handover είναι ένα handover μεταξύ δύο τομέων μίας κυψέλης (Περίπτωση Α στο Σχήμα στην επόμενη διαφάνεια). Από την πλευρά του κινητού, το softer handover είναι μία άλλη περίπτωση soft handover. Από την πλευρά του δικτύου, πρόκειται για μία εσωτερική διαδικασία του εμπλεκόμενου Κόμβου Β (Intra Node B Handover). Ο κόμβος RNC που ελέγχει τον Κόμβο Β δε συμμετέχει στη διαδικασία.

Σχηματική αναπαράσταση



•*Inter-Node B/intra-RNS handover*: Εκτελείται όταν το κινητό μετακινείται από μία κυψέλη ενός Κόμβου Β σε κυψέλη άλλου Κόμβου Β ο οποίος ανήκει στο ίδιο RNS με τον αρχικό (περίπτωση Β).

• *Inter-Node B/inter-RNS/intra-SGSN*: Σε αυτή την περίπτωση το κινητό μετακινείται από την κυψέλη ενός Κόμβου Β στην κυψέλη ενός άλλου Κόμβου Β ο
οποίος ανήκει σε διαφορετικό RNS σε σχέση με τον αρχικό. Συνεπώς, οι Κόμβοι Β ελέγχονται από διαφορετικούς RNC οι οποίοι όμως συνδέονται με τον ίδιο SGSN (περίπτωση Γ).

• *Inter-Node B/inter-RNS/inter-SGSN*: Σε αυτή την περίπτωση το κινητό μετακινείται από την κυψέλη ενός Κόμβου Β στην κυψέλη ενός άλλου Κόμβου Β ο οποίος ανήκει σε διαφορετικό RNS σε σχέση με τον αρχικό, ενώ επιπλέον, οι αντίστοιχοι RNC συνδέονται με διαφορετικούς SGSN (περίπτωση Δ).

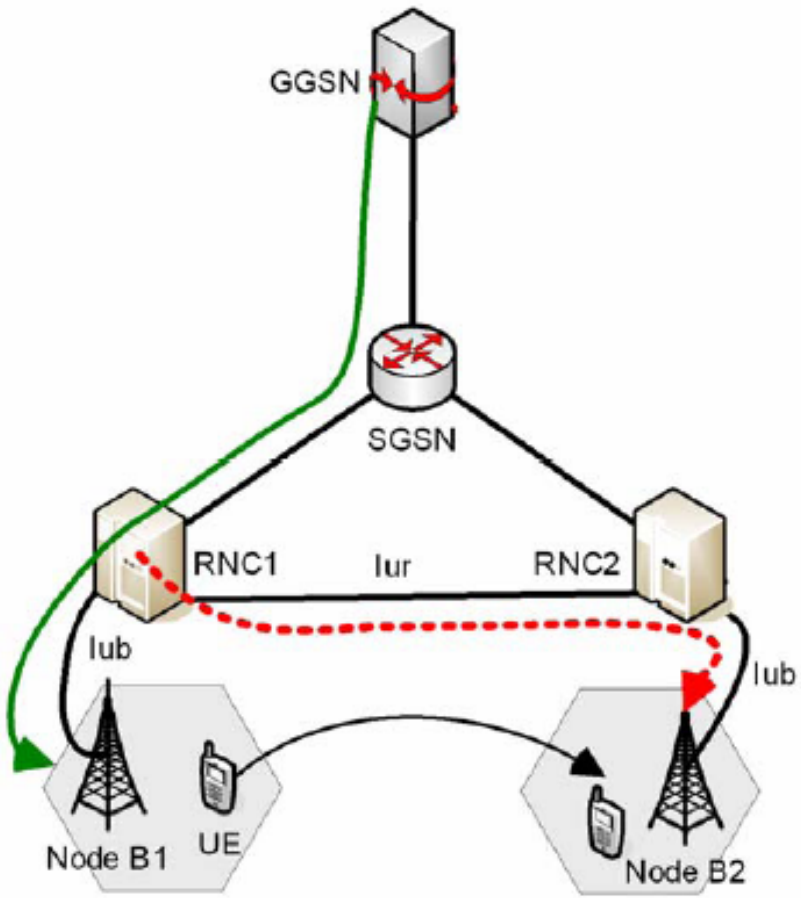
Μηχανισμός διαχείρισης μεταπομπών

- Γίνονται μετρήσεις στο uplink, ενώ για το downlink τα αποτελέσματα συλλέγονται από τις συσκευές. Οι κυψέλες διαχωρίζονται σε τρία σύνολα:
  - το active set: περιέχει τους Κόμβους Β που εμπλέκονται σε ένα soft handover. Όταν η ένταση του σήματος ενός Κόμβου Β ξεπερνά κάποιο κατώφλι, ο συγκεκριμένος Κόμβος προστίθεται στο active set. Αντίστοιχο κατώφλι υπάρχει και για την απόρριψη ενός Κόμβου Β από το active set.
  - το monitored set: περιέχει κυψέλες που συνορεύουν με το κελί στο οποίο βρίσκεται η συσκευή, και ως εκ τούτου είναι υποψήφια για handover. Από το monitored set εξαιρούνται οι Κόμβοι Β που έχουν ήδη προστεθεί στο active set. Η κινητή συσκευή παρακολουθεί την ένταση του σήματος από τους Κόμβους Β του monitored set σύμφωνα με κάποιους κανόνες.
  - το detected set: περιέχει όλους τους Κόμβους Β από τους οποίους το κινητό λαμβάνει μεν σήμα, αλλά οι οποίοι δε συνορεύουν με την κελί στην οποία βρίσκεται το κινητό τη συγκεκριμένη στιγμή

Inter-RNS μεταπομπές

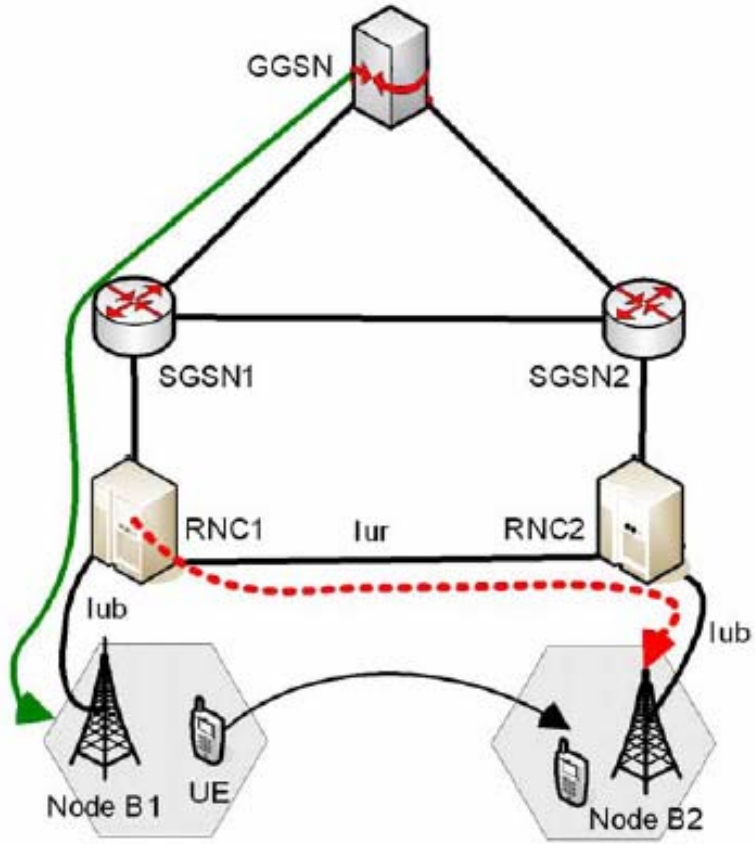
- Στόχος στο UMTS είναι να μην εμπλέκεται το CN στη διαδικασία του handover, κάτι το οποίο ίσχυε στα συστήματα GSM. Για το σκοπό αυτό, στην περίπτωση που εκτελείται μία inter-RNS , ο αρχικός RNC είναι ο μόνος RNC που διατηρεί σύνδεση με το CN. Ο συγκεκριμένος RNC ονομάζεται Serving RNC (SRNC) και είναι ο κόμβος που μεταδίδει τα δεδομένα της κίνησης προς το κινητό, στους υπόλοιπους RNC. Οι υπόλοιποι RNC ονομάζονται Drift RNC (DRNC).

Inter-RNS/intra-SGSN μεταπομπή



- Ο RNC1 είναι ο SRNC, ενώ ο RNC2 είναι ο DRNC.
- Η ενιαία (πράσινη) γραμμή απεικονίζει την αρχική ροή δεδομένων προς τη συσκευή.
- Η διακεκομμένη (κόκκινη) γραμμή απεικονίζει τη ροή δεδομένων που αποκαθίσταται μετά την ολοκλήρωση του soft handover.
- ΤΟ CN (δηλαδή το SGSN) δεν εμπλέκεται καθόλου

Inter-RNS/inter-SGSN μεταπομπή



- Ο RNC1 είναι ο SRNC, ενώ ο RNC2 είναι ο DRNC.
- Η ενιαία (πράσινη) γραμμή απεικονίζει την αρχική ροή δεδομένων προς τη συσκευή.
- Η διακεκομμένη (κόκκινη) γραμμή απεικονίζει τη ροή δεδομένων που αποκαθίσταται μετά την ολοκλήρωση του soft handover.
- ΤΟ CN δεν εμπλέκεται καθόλου.
- Ο κόμβος SGSN2 δεν μεταδίδει δεδομένα στον RNC2, αντίθετα ο RNC2 λαμβάνει από τον RNC1 τα δεδομένα που θα αποστείλει στο κινητό

Πλεονεκτήματα/Μειονεκτήματα

- Πλεονεκτήματα
  - η ποιότητα της επικοινωνίας διατηρείται υψηλή αφού το κινητό λαμβάνει ταυτόχρονα την ίδια πληροφορία από περισσότερες από μία κεραίες.
  - Δεν υπάρχουν διακοπές στην επικοινωνία
  - Πιο απλός ο έλεγχος λάθους, οπότε περιορίζεται η επαναμετάδοση πακέτων
  - Οικονομία ενέργειας: κάθε κεραία διατηρεί ένα σχετικά χαμηλό επίπεδο έντασης του σήματος, αφού πολλές κεραίες μεταδίδουν στο κινητό
  - Ελαττώνεται το φαινόμενο ping pong.
- Μειονέκτημα
  - Μεγάλο κόστος υλοποίησης λόγω των πολύπλοκων διαδικασιών

Διαδικασία “SRNS Relocation”

- Η διαδικασία SRNS relocation λαμβάνει χώρα όταν έχει ήδη προηγηθεί ένα inter-RNS soft handover.
- Μετά την εκτέλεση του soft handover, ο SRNC αναλαμβάνει να προωθεί προς τον DRNC τα δεδομένα που απευθύνονται στη συγκεκριμένη κινητή συσκευή.
- Μετά την εκτέλεση της SRNS relocation, ο SRNC παύει να εξυπηρετεί τη συσκευή και κάποιος από τους DRNC αναλαμβάνει την εξυπηρέτηση του συγκεκριμένου κινητού.
- Ο λόγος για τον οποίο ενεργοποιείται η διαδικασία SRNS relocation είναι η οικονομία στους πόρους του δικτύου. Κατά τη διάρκεια του soft handover η συσκευή UE λαμβάνει την ίδια πληροφορία τόσο από κεραίες που ελέγχονται από τον SRNC, όσο και από κεραίες που ελέγχονται από τον DRNC. Στην περίπτωση που το κινητό έχει απομακρυνθεί αρκετά από τον SRNC, το σήμα που λαμβάνει από τις αντίστοιχες κεραίες είναι αδύναμο. Συνεπώς, προκειμένου να μην υπάρχει σπατάλη στους πόρους του SRNC, κάποιο άλλο RNC αναλαμβάνει το ρόλο του SRNC.

Hard Handover

- Σε ένα hard handover, η ασύρματη συχνότητα που χρησιμοποιεί η συσκευή αλλάζει «απότομα». Πιο συγκεκριμένα, το κινητό παύει να χρησιμοποιεί την αρχική συχνότητα, στη συνέχεια μετακινείται σε διαφορετική συχνότητα και ξεκινά να λειτουργεί στη συχνότητα αυτή (εμφανίζεται κενό επικοινωνίας).
- Είναι η συνηθέστερη περίπτωση μεταπομπών στο GSM.
- Σπάνια χρησιμοποιείται στο UMTS, όπου το κινητό μεταδίδει συνέχεια στο χρόνο (όχι σε χρονοθυρίδες), άρα δεν υπάρχουν ελεύθερες χρονοθυρίδες προκειμένου το κινητό να κάνει μετρήσεις σε άλλη συχνότητα

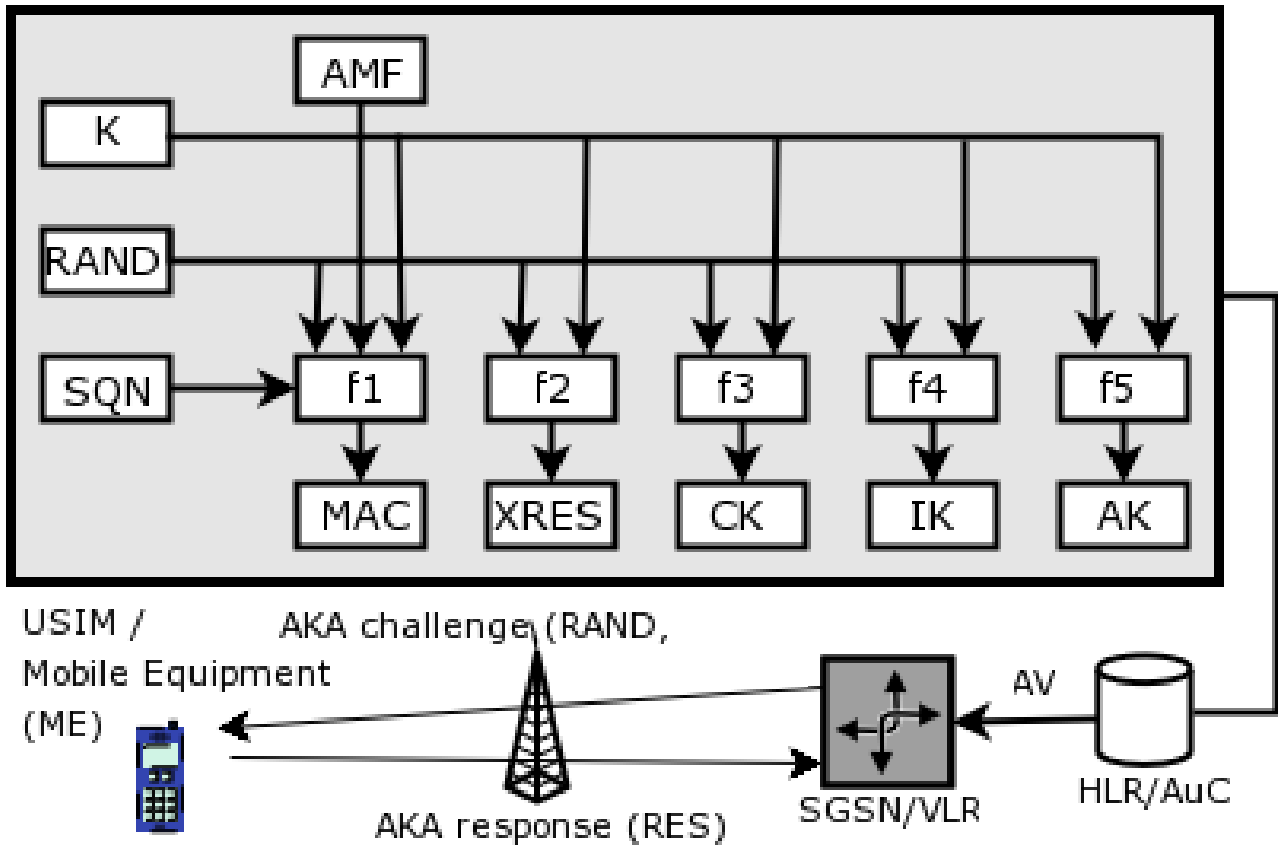
Ασφάλεια στο UMTS

- Καλύτερη από ό,τι στο GSM γιατί:
  - Δεν αυθεντικοποιείται μόνο ο χρήστης στο δίκτυο, αλλά και το δίκτυο στον χρήστη
  - “Προστατεύονται” και τα σήματα σηματοδοσίας εκτός από τα δεδομένα
  - Στο UMTS, τα σήματα είναι κρυπτογραφημένα μέχρι τον Radio Network Controller (RNC) και όχι απλά μέχρι το Σταθμό Βάσης, όπως ίσχυε στο GSM.
  - Χρησιμοποιούνται καλύτεροι αλγόριθμοι κρυπτογράφησης, με κλειδιά μεγαλύτερου μήκους

Αυθεντικοποίηση

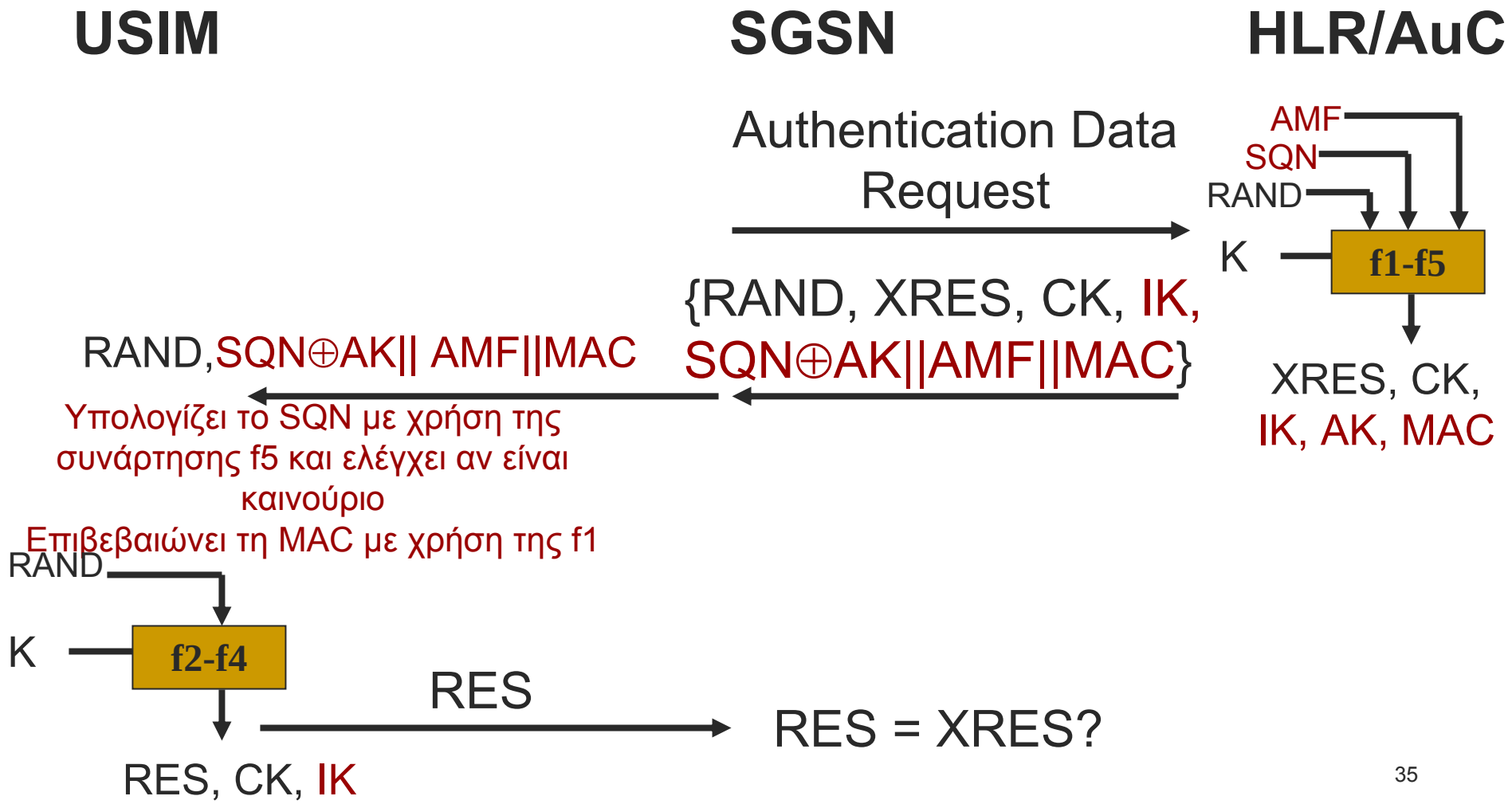
- Όπως και στο GSM, η αυθεντικοποίηση στηρίζεται σε ένα μυστικό κλειδί K, το οποίο το γνωρίζουν μόνο η USIM και ο HLR/AuC του παρόχου
- Ο SGSN που πρέπει να αυθεντικοποιήσει τον χρήστη ζητάει από τον HLR/AuC κάποιο σύνολο από AV (Auth Vectors)
- Κάθε AV είναι μία πεντάδα που αποτελείται
  - RAND (random challenge) και XRES (απάντηση στο RAND) για την αυθεντικοποίηση του χρήστη (όπως ακριβώς και στο GSM)
  - CK (cipher key) που είναι το κλειδί κρυπτογράφησης, IK (integrity key) for protection of integrity, AUTN (auth token) για την αυθεντικοποίηση του δικτύου.

Διάγραμμα



Ο AuC έχει ένα random number generator (RAND) και ένα sequence number generator (SQN)

Αυθεντικοποίηση στο UMTS (πιο αναλυτικά)



Παράμετροι

K = Subscriber authentication key (128 bit)

RAND = User authentication challenge (128 bit)

SQN = Sequence number (48 bit)

AMF = Authentication management field (16 bit)

MAC = $f1_K$ (SQN||RAND||AMF) = Message Authentication Code (64 bit)

(X)RES = $f2_K$ (RAND) = (Expected) user response (32-128 bit)

CK = $f3_K$ (RAND) = Cipher key (128 bit)

IK = $f4_K$ (RAND) = Integrity key (128 bit)

AK = $f5_K$ (RAND) = Anonymity key (48 bit)

AUTN = SQN⊕AK|| AMF||MAC = Authentication Token (128 bit)

Authentication quintet = {RAND, XRES, CK, IK, AUTN} (544-640 bit)

Κρυπτογράφηση των δεδομένων

- Τα δεδομένα που μεταδίδονται στη ραδιοζεύξη (στον αέρα), μεταξύ κινητού και RNC, κρυπτογραφούνται.
- Ως κλειδί κρυπτογράφησης χρησιμοποιείται το CK (μήκους 128 bit), το οποίο το υπολογίζουν τόσο η συσκευή όσο και το δίκτυο κατά τη διάρκεια της αυθεντικοποίησης
  - Παράγεται από τη συνάρτηση f3, με χρήση του μυστικού κλειδιού K που γνωρίζουν μόνο το δίκτυο και η κάρτα USIM

Κρυπτογράφηση των δεδομένων (2)

- Αλγόριθμος κρυπτογράφησης: UMTS Encryption Algorithm (UEA), ο οποίος είναι stream cipher (όπως ήταν και ο αντίστοιχος αλγόριθμος κρυπτογράφησης στον GSM)
- Ο αλγόριθμος αυτός έχει προτυποποιηθεί (UEA1) και είναι υλοποιημένος στις συσκευές, όχι στη USIM
- Από το 2006 έχει αρχίσει ήδη και εφαρμόζεται και ο UEA2

Ασφάλεια και στα σήματα σηματοδοσίας

- Ένα από τα επιπρόσθετα χαρακτηριστικά ασφαλείας του UMTS (σε αντίθεση με το GSM) είναι το ότι προστατεύονται και τα σήματα σηματοδοσίας (από τροποποιήσεις τους, ενώ επίσης αποτρέπεται η δυνατότητα επανεκπομπής τους από κάποιον υποκλοπέα).
- Το κλειδί που χρησιμοποιείται για την προστασία των σημάτων σηματοδοσίας είναι το IK μήκους 128 bit (το οποίο υπολογίζεται και από τα δύο μέλη επίσης κατά τη διάρκεια της αυθεντικοποίησης)
- Υπάρχει και για αυτήν την κρυπτογράφηση προτυποποιημένος αλγόριθμος: ο UIA1. Είναι επίσης υλοποιημένος στη συσκευή και όχι στη USIM
  - Από το 2006 έχει αρχίσει ήδη και εφαρμόζεται και ο UIA2

Η Γενιά 3,5

- Με τον όρο «γενιά 3,5» αναφερόμαστε στη νέα γενιά κινητών δικτύων τα οποία εκτός από την τεχνολογία WCDMA έχουν ενσωματώσει την τεχνολογία High Speed Downlink Packet Access (HSDPA).
- Η HSDPA αποτελεί μία νέα τεχνολογία η οποία σχεδιάστηκε προκειμένου να αυξήσει τη χωρητικότητα της κατερχόμενης ζεύξης για τα κινητά δίκτυα τρίτης γενιάς. Το γεγονός αυτό θεωρήθηκε απαραίτητο καθώς, στην πράξη, οι μέγιστοι ρυθμοί μετάδοσης για τα κινητά δίκτυα τρίτης γενιάς αποδείχθηκαν χαμηλοί για multimedia εφαρμογές. Ιδιαίτερα στην περίπτωση που θα υπήρχαν πολλοί χρήστες στην ίδια κυψέλη που θα εκκινούσαν τέτοιες εφαρμογές, η απόδοση του δικτύου σε αυτήν την κυψέλη μειωνόταν δραστικά.
- Η βασική ιδέα του HSDPA είναι η προσθήκη ενός νέου τύπου ευρυζωνικού καναλιού, του High-Speed Downlink Shared Channel (HS-DSCH), στο οποίο έχουν ενσωματωθεί διάφορες τεχνικές που αποσκοπούν στη βελτιστοποίησή των δυνατοτήτων του όσον αφορά ρυθμό μετάδοσης. Δεν είναι ωστόσο κατάλληλο για όλες τις εφαρμογές (π.χ. πραγματικού χρόνου).