ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Εθνικόν και Καποδιστριακόν
Πανεπιστήμιον Αθηνών

Συστήματα Κινητών και Προσωπικών Επικοινωνιών

Ενότητα 6: Διαχείριση κινητικότητας

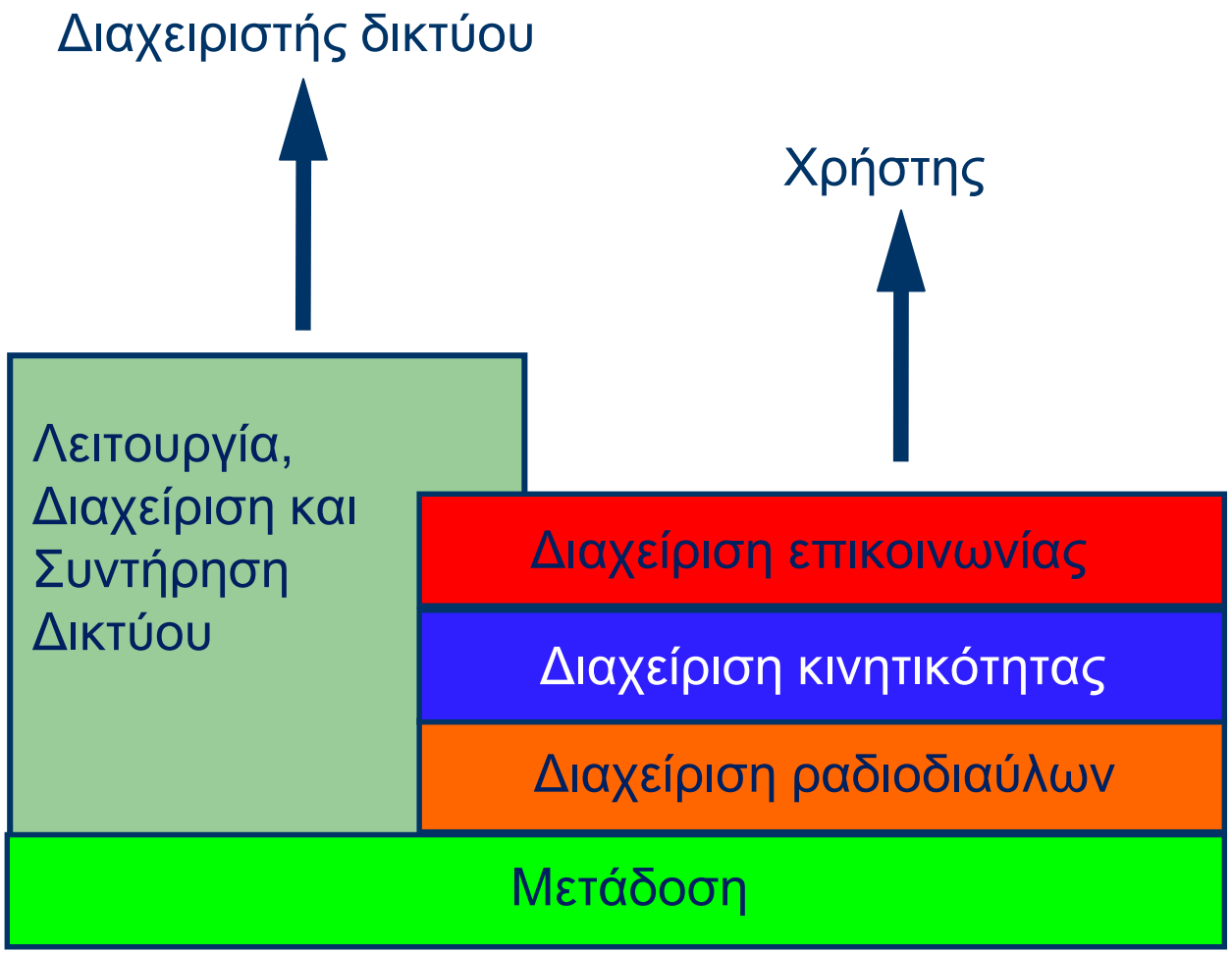
Νικόλαος Πασσάς
Σχολή Θετικών Επιστημών
Τμήμα Πληροφορικής και Τηλεπικοινωνιών

Περιγραφή ενότητας

- Διαχείριση εντοπισμού
  - Ενημέρωση θέσης
  - Παράδοση κλήσης
- Διαχείριση εντοπισμού στα επίγεια Συστήματα Κινητών επικοινωνιών
- Ενημέρωση θέσης και εντοπισμός δεδομένων
  - Κεντρικές βάσεις δεδομένων
  - Κατανεμημένες βάσεις δεδομένων
- Ενημέρωση θέσης και Αναζήτηση
  - Δυναμικές μέθοδοι ενημέρωσης θέσης
  - Μέθοδοι αναζήτησης
- Διαχείριση εντοπισμού στο UMTS
- Διαχείριση ασφάλειας στο GSM και στο UMTS

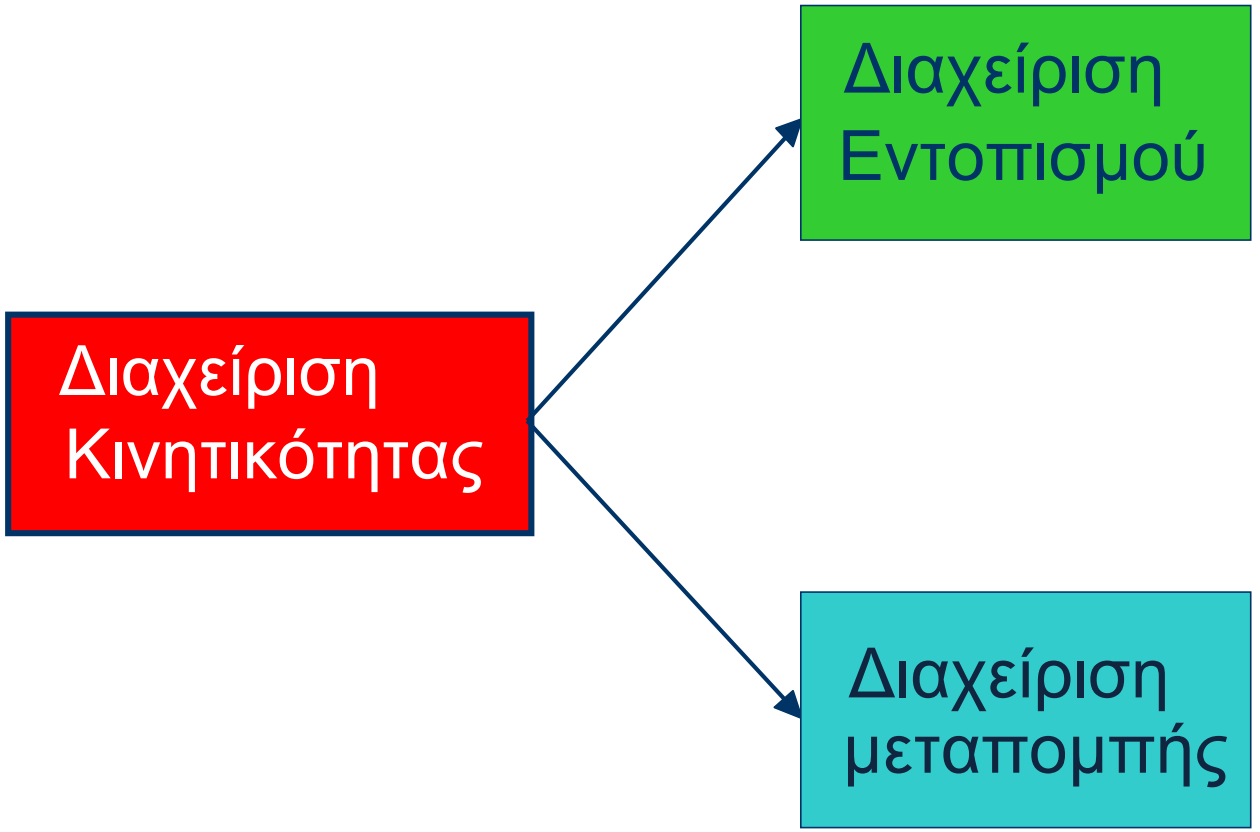
Διαχείριση κινητικότητας

Διαχείριση κινητικότητας (1/3)



Διαχείριση κινητικότητας (2/3)

- Λειτουργίες και διαδικασίες που έχουν σχέση με την κίνηση των χρηστών και των τερματικών



Διαχείριση κινητικότητας (3/3)

Περιλαμβάνει το σύνολο των διαδικασιών που αφορούν:

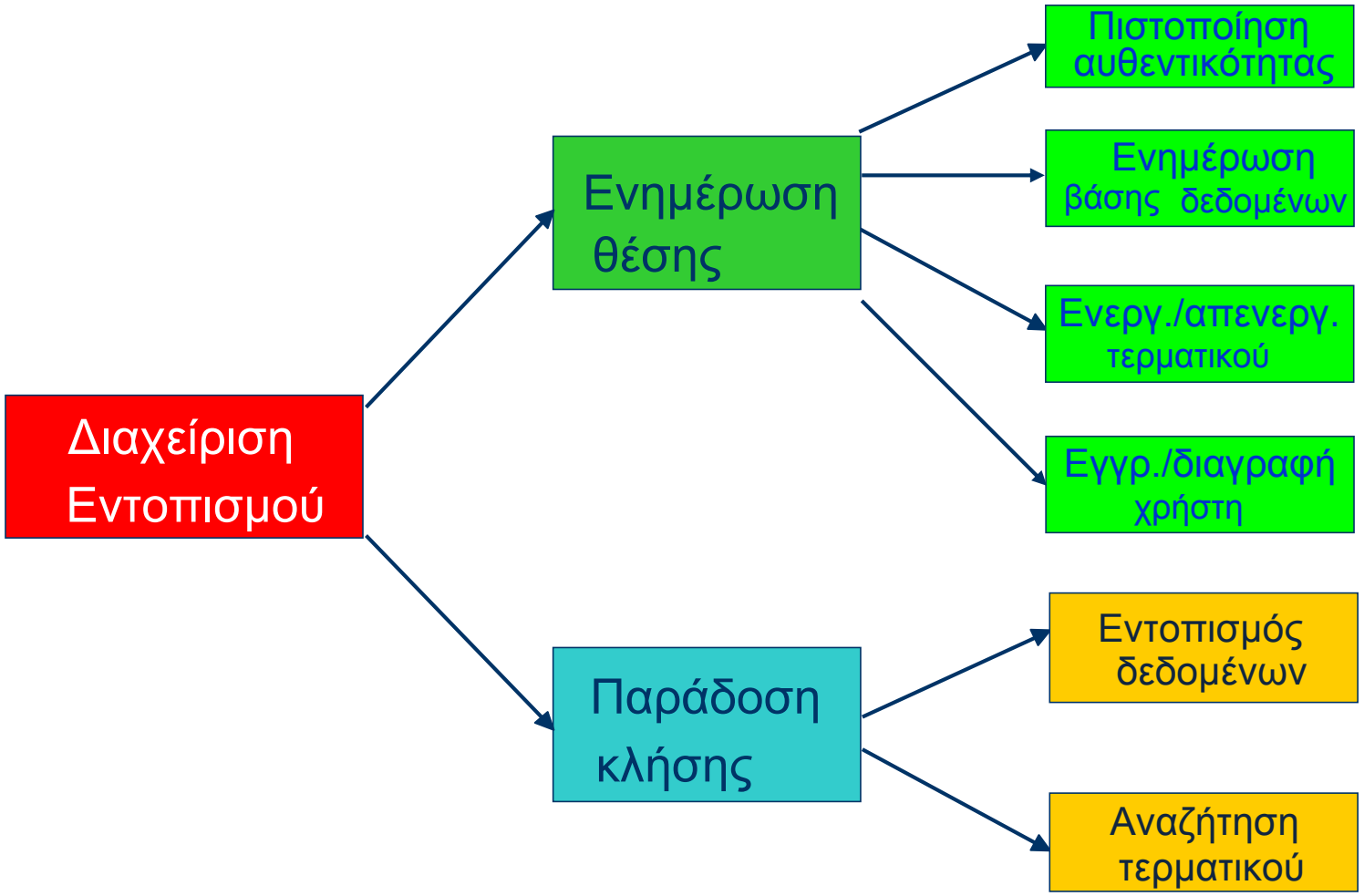
- Τη διαχείριση εντοπισμού
  - Ενημέρωση του δικτύου για τη θέση και την κατάσταση των κινητών τερματικών (χρηστών).
  - Προσδιορισμός της θέσης του καλούμενου για προώθηση της εισερχόμενης κλήσης.
- Τη διαδικασία της μεταπομπής

Διαχείριση εντοπισμού (1/2)

Η διαχείριση εντοπισμού έχει δύο όψεις:

1) Πώς ο κινούμενος χρήστης ή το κινούμενο τερματικό αντιμετωπίζει την αλλαγή περιβάλλοντος (της θέσης του).
2) Πώς η υποδομή του συστήματος διαχειρίζεται τα δεδομένα που αφορούν τη θέση των τερματικών (χρηστών), ώστε να καθιστά δυνατή την εγκατάσταση κλήσεων προς κινούμενα τερματικά (χρήστες).

Διαχείριση εντοπισμού (2/2)



Διαδικασία ενημέρωσης θέσης

- Οι λειτουργίες που απαρτίζουν τη διαδικασία ενημέρωσης θέσης **δεν σχετίζονται με τις κλήσεις.**
- Έχουν ως σκοπό να ενημερώνουν το δίκτυο για:
  - Τη θέση των τερματικών που βρίσκονται σε λειτουργία
  - Την παρούσα κατάσταση των τερματικών
  - Την κατάσταση εγγραφής των χρηστών

Διαδικασία παράδοσης της κλήσης

- Οι λειτουργίες που απαρτίζουν τη διαδικασία παράδοσης της κλήσης **ενεργοποιούνται μόνο όταν υπάρχει εισερχόμενη κλήση** για κινητό τερματικό.
  - Εντοπισμός δεδομένων
  - Αναζήτηση τερματικού

Διαχείριση εντοπισμού στα επίγεια συστήματα κινητών επικοινωνιών

- Οι τρέχουσες τεχνικές βασίζονται σε ιεραρχική βάση δεδομένων δύο επιπέδων.
- Οι πληροφορίες που αφορούν χρήστες (τερματικά) αποθηκεύονται σε δύο τύπους καταχωρητών.
  - **Καταχωρητής θέσης οικείων** (Home Location Register, HLR)
  - **Καταχωρητής θέσης επισκεπτών** (Visitors Location Register, VLR)

HLR (1/2)

- Η *στατική* (μόνιμη) πληροφορία του HLR είναι:
  - Ο αριθμός κλήσης του κινητού συνδρομητή (*Mobile Subscriber Number, MSN).*
  - Η διεθνής ταυτότητα του συνδρομητή (*International Mobile Subscriber Identity, IMSI*).
  - Το κλειδί ελέγχου αυθεντικότητας.
  - Οι πληροφορίες για τις βασικές και συμπληρωματικές υπηρεσίες (profile).

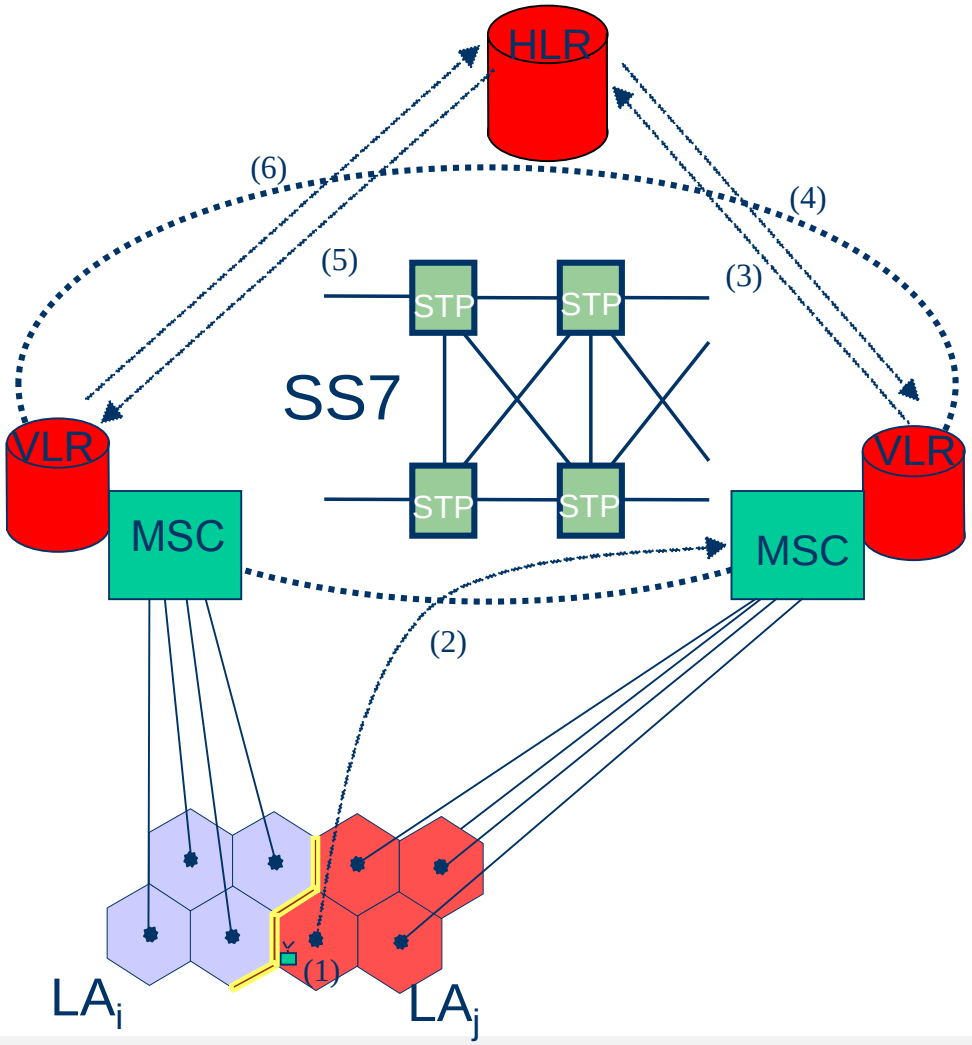
HLR (2/2)

- Η *δυναμική* πληροφορία του HLR περιλαμβάνει:
  - Τις παραμέτρους ελέγχου αυθεντικότητας και κρυπτογράφησης.
  - Τον αριθμό περιαγωγής κινητού σταθμού (*Mobile Station Roaming Number, MSRN*), ή
  - Τη διεύθυνση του MSC/VLR ή αντίστοιχα την ταυτότητα της LA.
  - Την κατάσταση του κινητού τερματικού (attached / detached).
  - Προσωρινές πληροφορίες σχετικές με τις υπηρεσίες που χρησιμοποιεί.

VLR

- Ο VLR περιέχει στατική και δυναμική πληροφορία ανάλογη με εκείνη του HLR.
- Περιέχει επιπλέον και την προσωρινή ταυτότητα κινητού συνδρομητή (*Temporary Mobile Subscriber Identity, TMSI*).

Διαδικασία ενημέρωσης θέσης

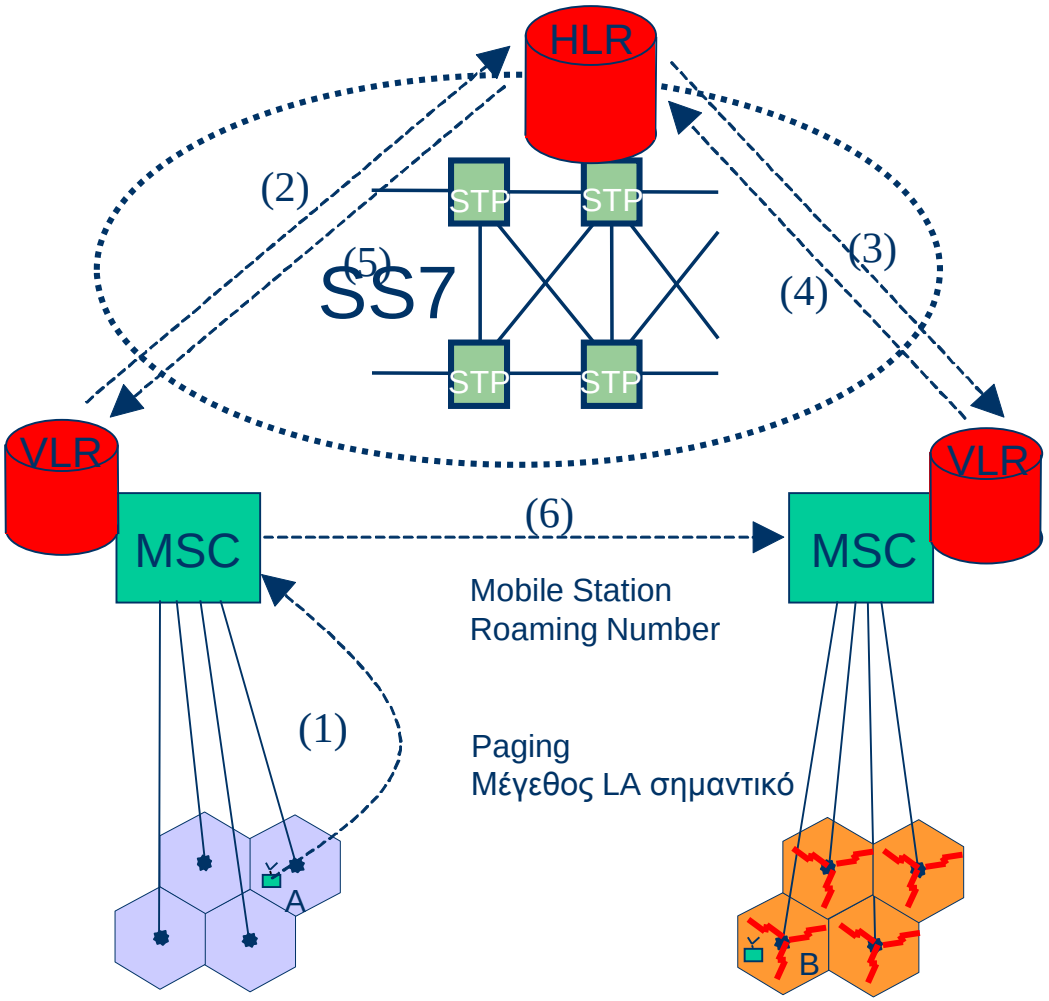


Διαδικασία παράδοσης της κλήσης

- Διακρίνουμε δύο κυρίως βήματα:

1) Προσδιορισμός του MSC/VLR που εξυπηρετεί το καλούμενο κινητό τερματικό (interrogation).
2) Εντοπισμός της τρέχουσας κυψέλης στην οποία περιφέρεται το καλούμενο κινητό τερματικό (paging).

Διαδικασία παράδοσης της κλήσης GSM

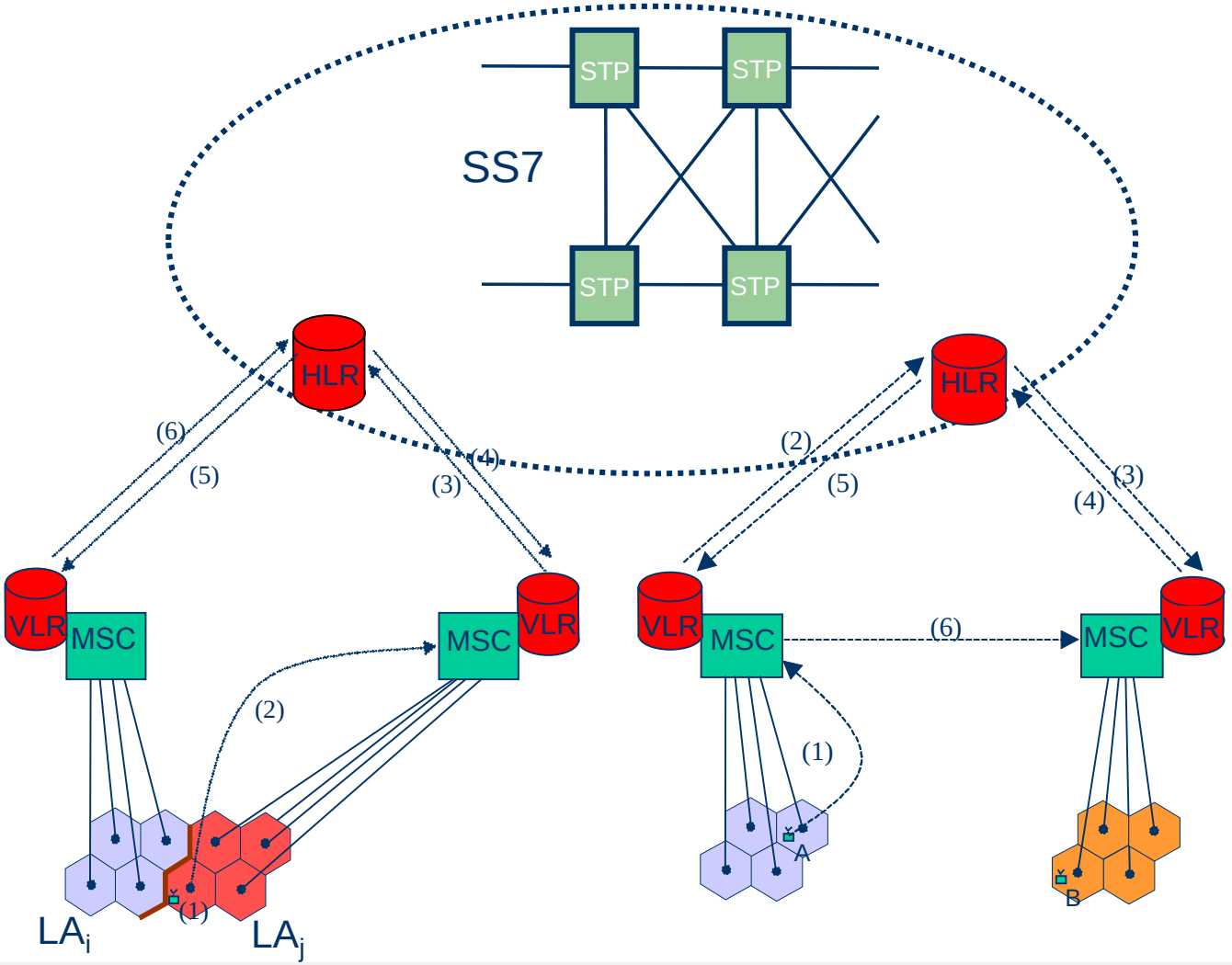


Προβληματική τεχνική για δίκτυα >3G (πολλαπλά επίπεδα κυψελών)

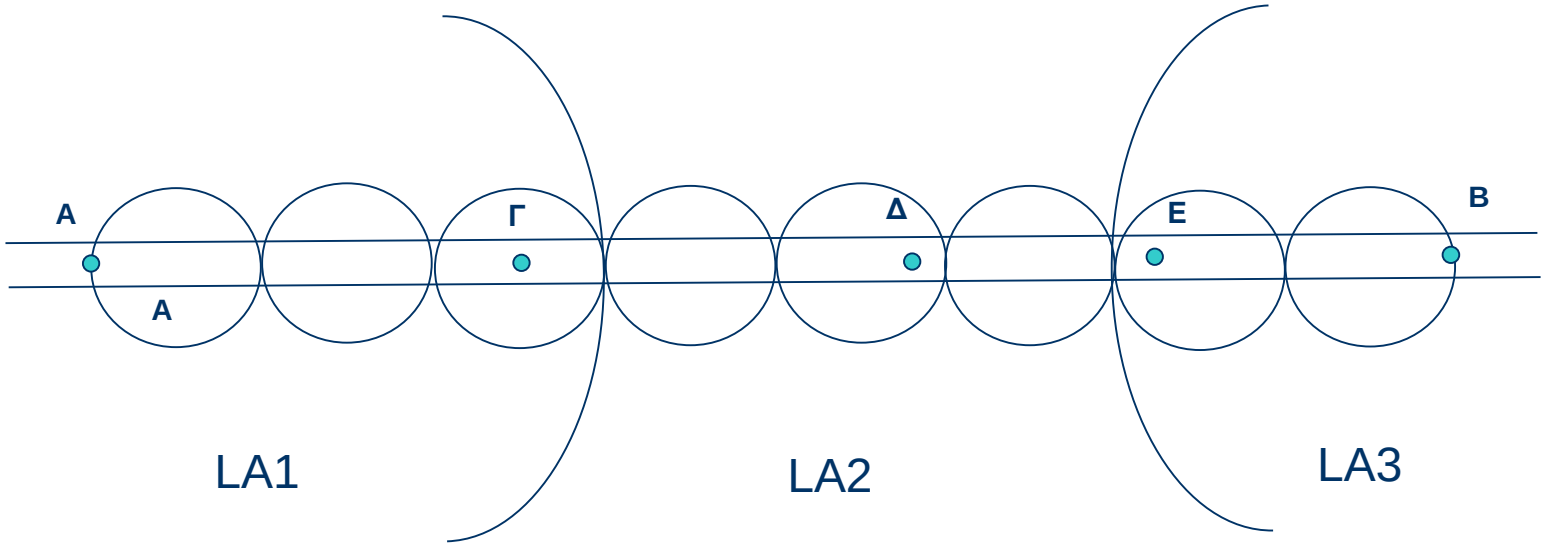
Διαδικασία παράδοσης της κλήσης

- Ο σχεδιασμός των LA (σχήμα, θέση, διάταξη) και η στρατηγική αναζήτησης στην LA είναι μεγάλης σημασίας, διότι:
  - Καθορίζουν τις απαιτήσεις σε σηματοδοσία (διαδικασία ενημέρωσης θέσης, αναζήτηση),
  - Επηρεάζουν σημαντικά τον ρυθμό προσβάσεων στη βάση δεδομένων (διαδικασία ενημέρωσης θέσης).
- Ο εντοπισμός δεδομένων και η αναζήτηση είναι **συμπληρωματικές** διαδικασίες.

Ενημέρωση θέσης και εντοπισμός δεδομένων (1/3)



Παράδειγμα 10.1



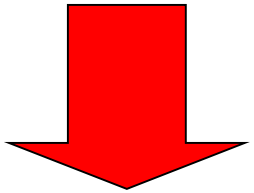
U=120km/h
R=3km

Συνδιάλεξη α) 7min b) 11 min

Περιγράψτε τις διαδικασίες σε κάθε περίπτωση

Ενημέρωση θέσης και εντοπισμός δεδομένων (2/3)

- Οι διαδικασίες αυτές μπορεί να έχουν μεγάλο κόστος όταν το MT βρίσκεται μακριά από τον HLR.
- Όσο αυξάνει ο αριθμός των χρηστών, το φορτίο σηματοδοσίας που οφείλεται στη διαδικασία εντοπισμού δεδομένων είναι υπερβολικά μεγάλο.



Αναζήτηση μεθόδων για τον περιορισμό του φορτίου σηματοδοσίας για τον εντοπισμό των δεδομένων.

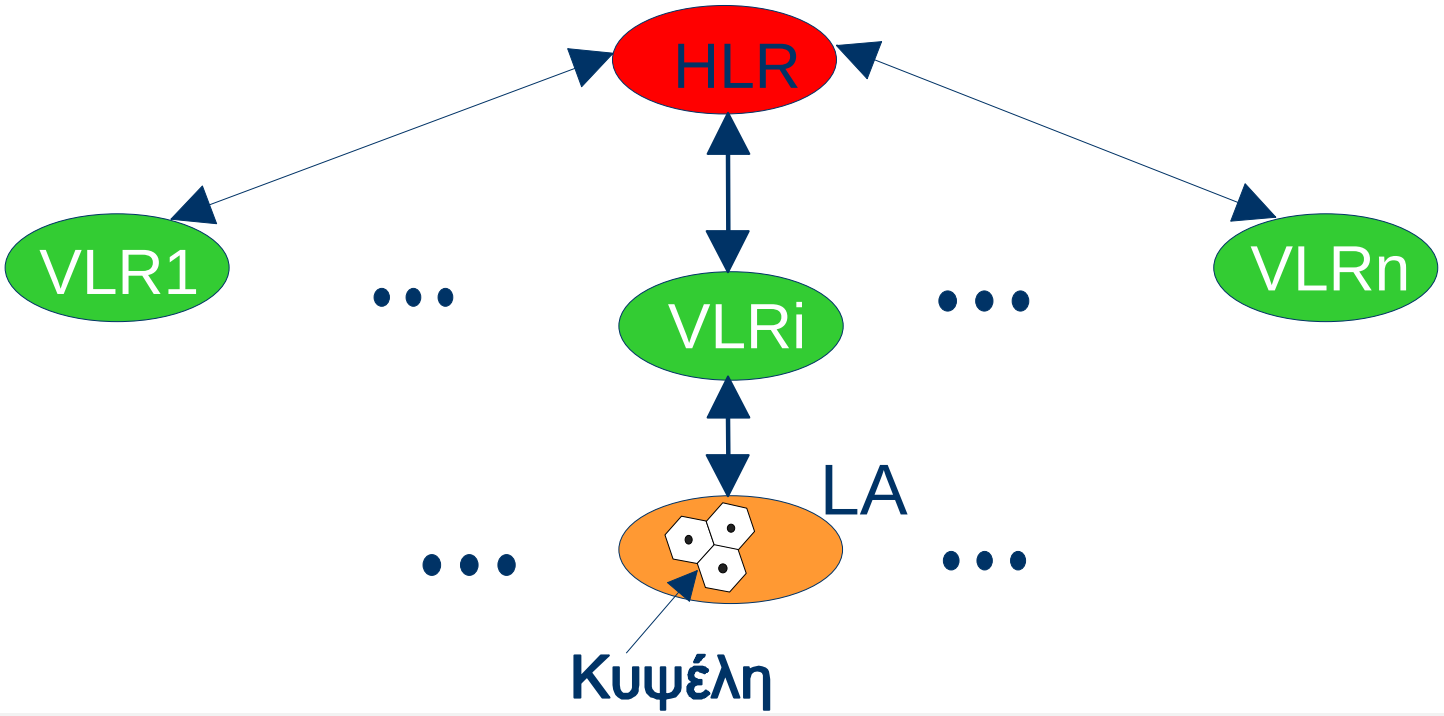
Ενημέρωση θέσης και εντοπισμός δεδομένων (3/3)

Η έρευνα στην περιοχή αυτή μπορεί γενικά να χωριστεί σε δύο κατηγορίες:

1) **Επεκτάσεις** της στρατηγικής εντοπισμού δεδομένων που εφαρμόζεται στα υπάρχοντα συστήματα
2) Εντελώς **νέες αρχιτεκτονικές**, οι οποίες απαιτούν νέα σχήματα για τις διαδικασίες ενημέρωσης θέσης και παράδοσης κλήσης.

Αρχιτεκτονικές κεντρικών βάσεων δεδομένων (1/6)

- Αναφέρονται στη δομή δυο επιπέδων που εφαρμόζεται στα δίκτυα 2ης γενιάς και στις βελτιώσεις της δομής αυτής, με στόχο τη μείωση του κόστους διαχείρισης εντοπισμού

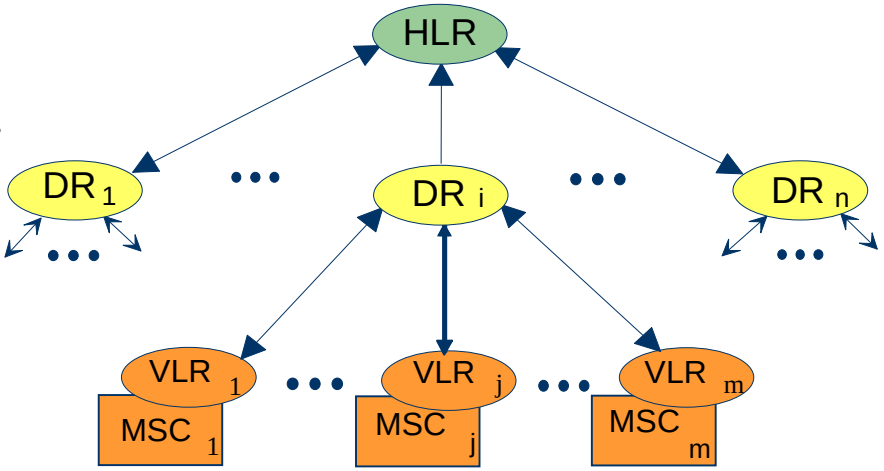


Αρχιτεκτονικές κεντρικών βάσεων δεδομένων (2/6)

Προσθήκη νέου ιεραρχικού επιπέδου: Καταχωρητές καταλόγου (DR)

Ο Directory Register (DR) υπολογίζει και αποθηκεύει μια μορφή δείκτη θέσης για κάθε τερματικό που εξυπηρετεί.

- Τοπικός δείκτης DR→MSC)
- Άμεσος απόμακρος δείκτης (DR → MSC)
- Έμμεσος απόμακρος δείκτης (DR → DR)



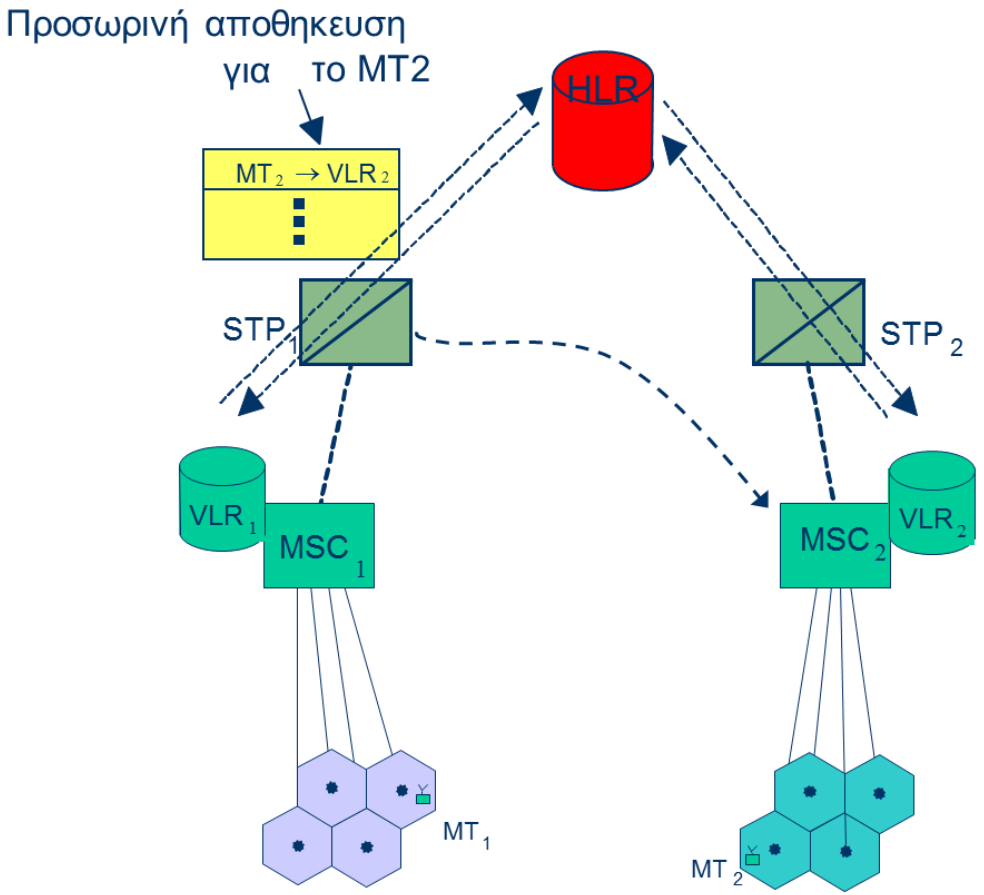
Ο HLR μπορεί να τροποποιηθεί, ώστε να φυλάσσει έναν δείκτη είτε προς τον τρέχοντα DR είτε προς το τρέχον MSC.

Παράδειγμα: Κλήση τερματικού εγγεγραμμένου στην Ελλάδα που είναι προσωρινά στη Γερμανία από γερμανικό κινητό

Αρχιτεκτονικές κεντρικών βάσεων δεδομένων (3/6)

Προσωρινή αποθήκευση της θέσης του MT

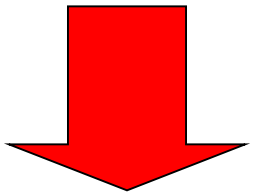
- Διατήρηση προσωρινής πληροφορίας θέσης του MT στο πλησιέστερο STP.
- Προσπαθούμε να αποφύγουμε την ερώτηση προς τον HLR, όποτε είναι δυνατό.



Αρχιτεκτονικές κεντρικών βάσεων δεδομένων (4/6)

Επανάληψη του προφίλ του χρήστη σε επιλεγμένες τοπικές βάσεις δεδομένων.

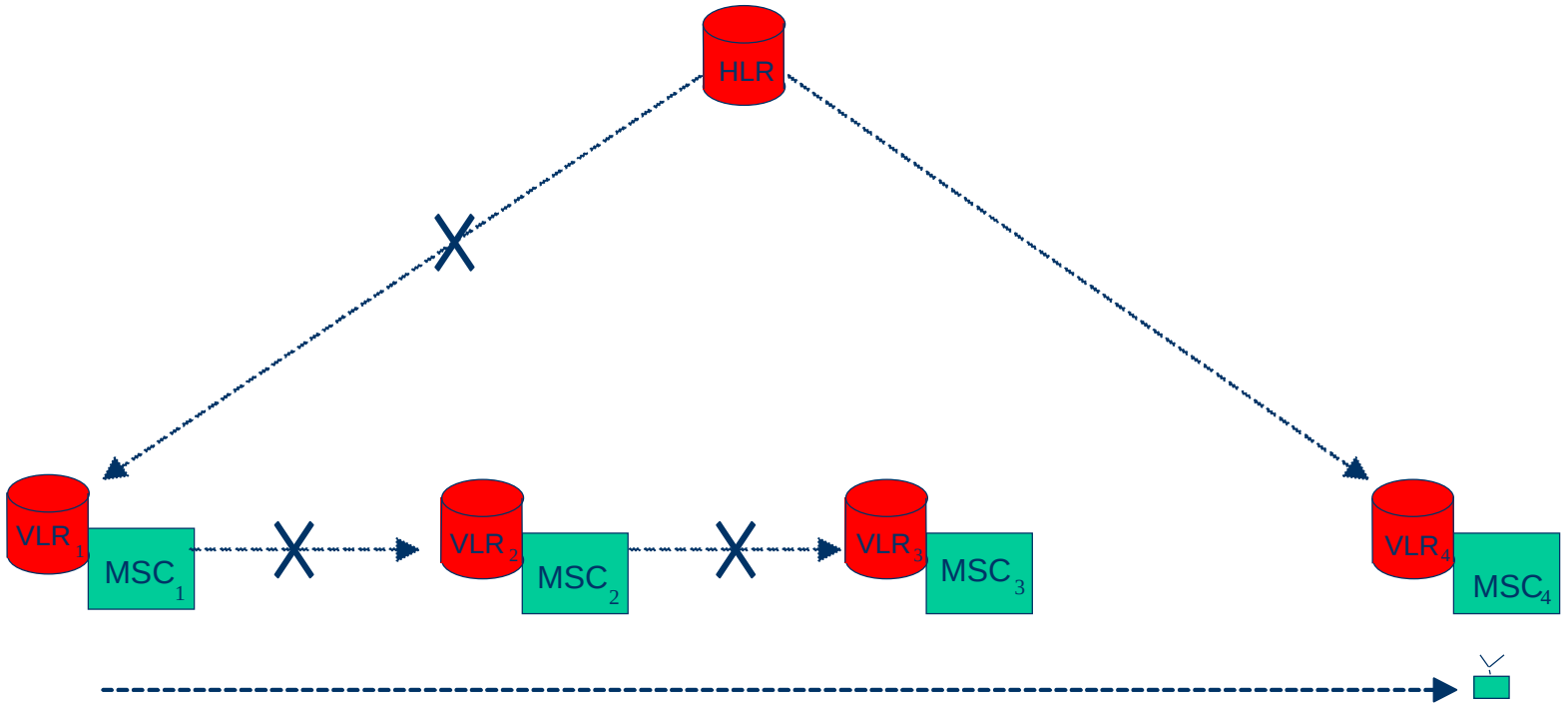
- Ελέγχεται πρώτα αν υπάρχει διαθέσιμο τοπικό αντίγραφο, αν όχι ερωτάται ο HLR.
- Σε μετακίνηση του MT ενημερώνονται όλα τα αντίγραφα.



- Μεγαλύτερη σηματοδοσία ενημέρωσης θέσης.
- Μέθοδος καθορισμού επανάληψης προφίλ.

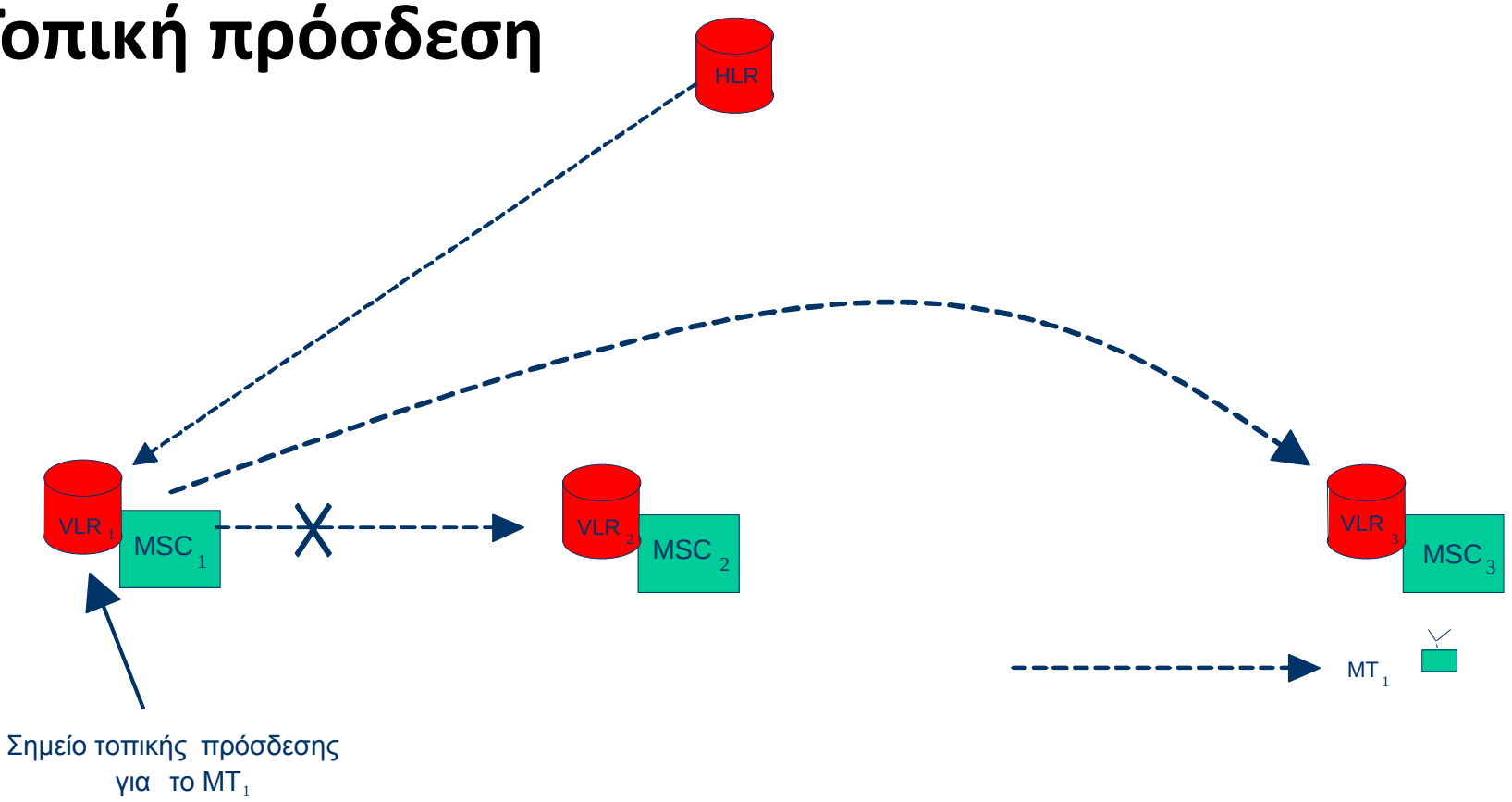
Αρχιτεκτονικές κεντρικών βάσεων δεδομένων (5/6)

Προώθηση του δείκτη για αναζήτηση δεδομένων



Αρχιτεκτονικές κεντρικών βάσεων δεδομένων (6/6)

Τοπική πρόσδεση



Στατικό και δυναμικό σημείο πρόσδεσης

Αρχιτεκτονικές κατανεμημένων βάσεων δεδομένων (1/2)

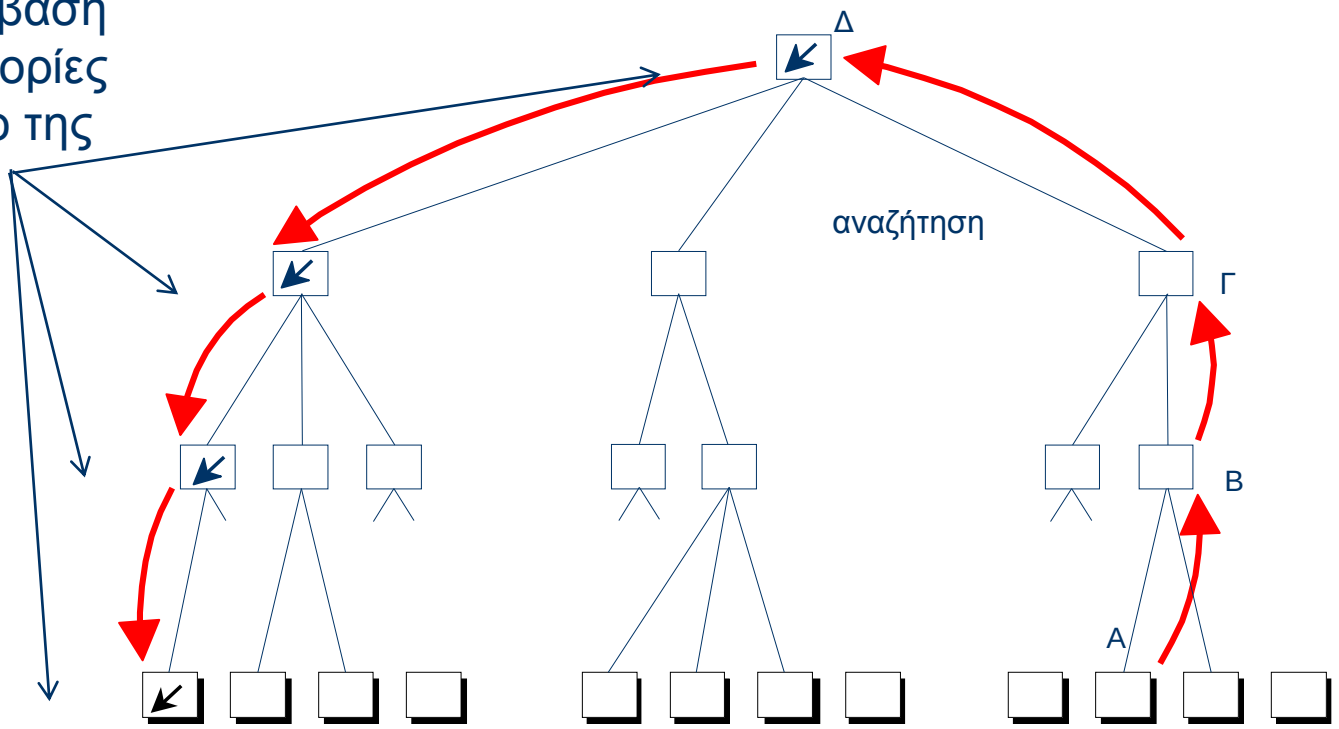
- Η κατανεμημένη βάση δεδομένων (Distributed Data Base, DDB) προσφέρει λύσεις:
  - Στην συγχρονη πολυεπίπεδη αρχιτεκτονική κινητών επικοινωνιών.
  - Στην ταχεία πρόσβαση στα δεδομένα.
  - Στον υψηλό αριθμό επικοινωνιών, με εκμετάλλευση της τοπικότητας της ζητούμενης πληροφορίας.
  - Στη σταδιακή απορρόφηση νέων συνδρομητών.
  - Στην αξιοπιστία του συστήματος και στη διαθεσιμότητα της πληροφορίας (αντίγραφα σε περισσότερους από έναν κόμβους).

Αρχιτεκτονικές κατανεμημένων βάσεων δεδομένων (2/2)

- Τα μειονεκτήματα προέρχονται από την πολυπλοκότητα διαχείρισης των δεδομένων.
  - Η αναγνώριση της πληροφορίας που ακολουθεί τον χρήστη / συνδρομητή, ώστε να εξασφαλίζεται η τοπικότητα της πληροφορίας.
  - Η συνέπεια (consistency) της πληροφορίας.
  - Η διαχείριση κατανεμημένων λειτουργιών (συγχρονισμός).
  - Η ασφάλεια της πληροφορίας και η προστασία του ιδιωτικού απόρρητου.

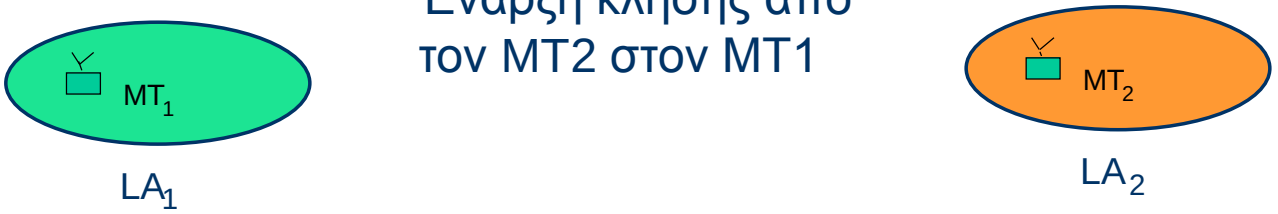
Πλήρως κατανεμημένη βάση

Κάθε ενδιάμεση βάση περιέχει πληροφορίες για το υποδέντρο της



Εγγραφή σε κάθε βάση κατά μήκος της διαδρομής μέχρι τη ρίζα του δέντρου

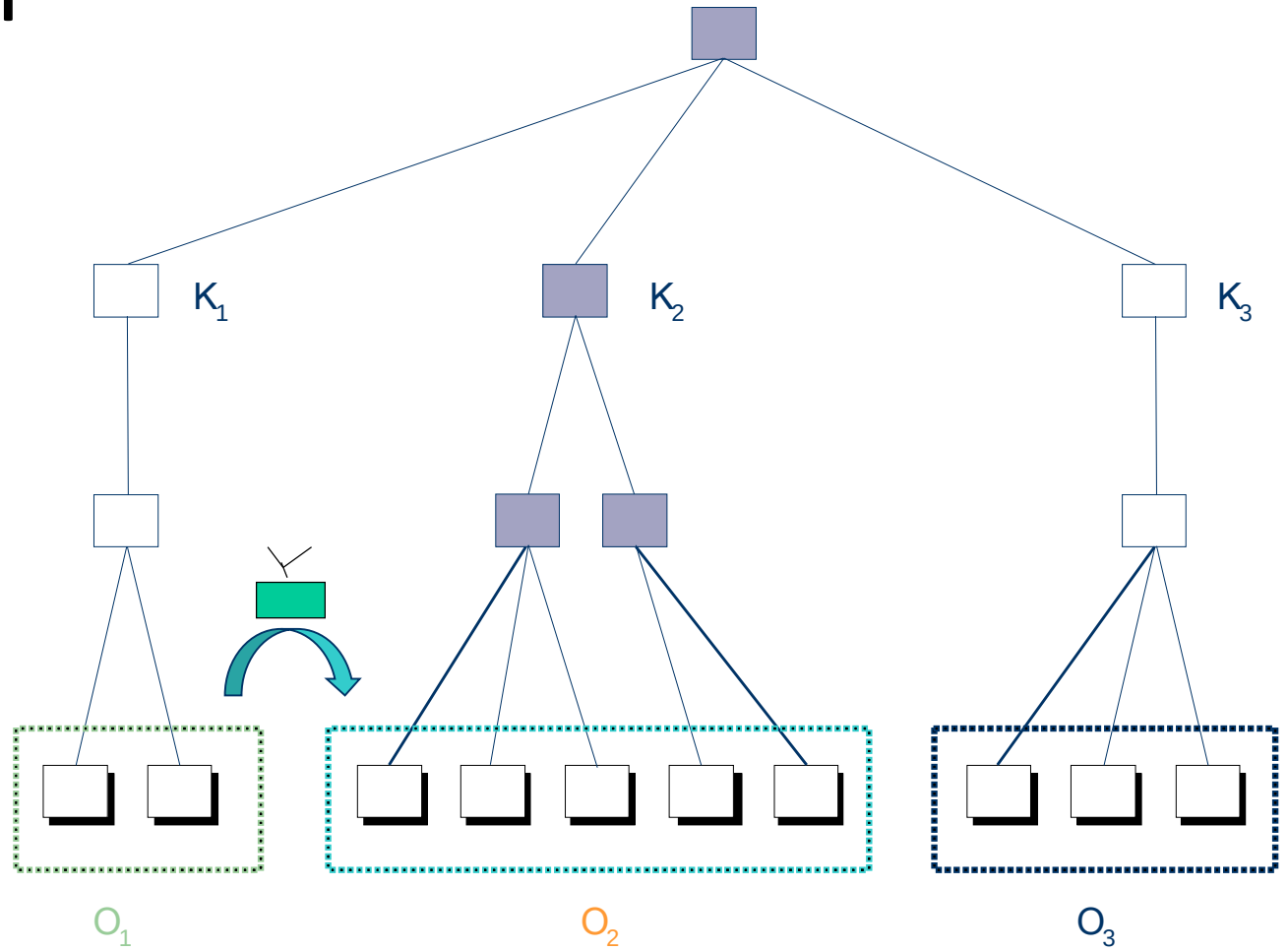
Έναρξη κλήσης από τον MT2 στον MT1



Αρχιτεκτονικές κατανεμημένων βάσεων δεδομένων (1/3)

Ομαδοποίηση

Ενημέρωση μόνο κατά την είσοδο ΜΤ σε ομάδα

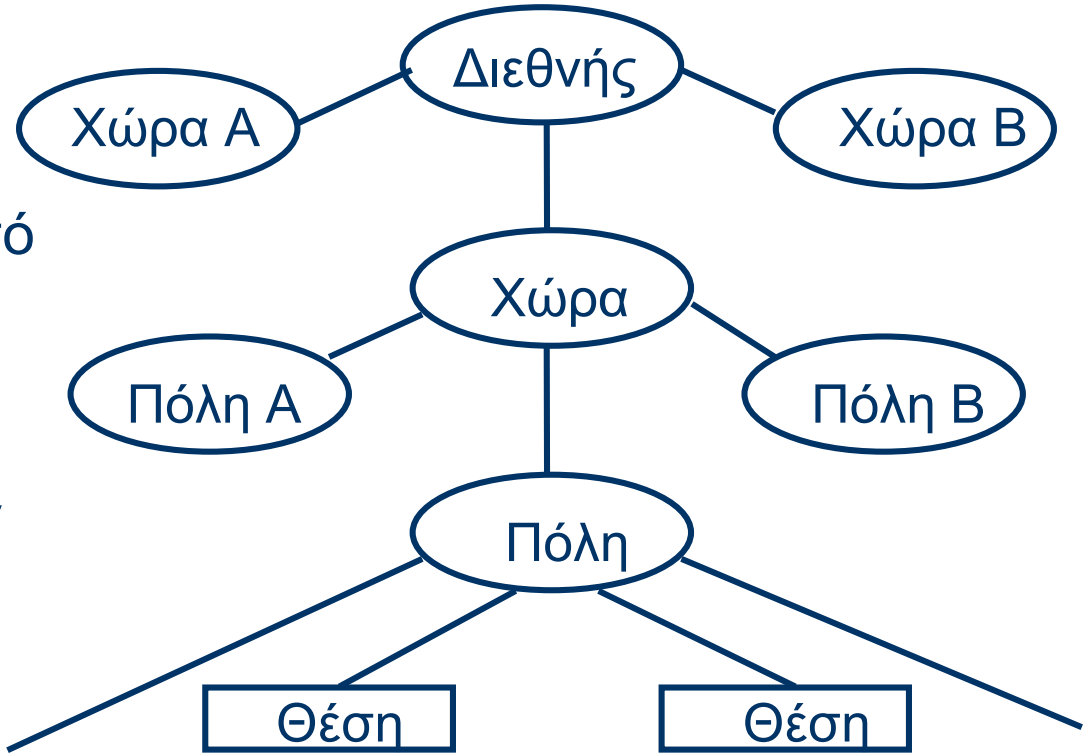


Αρχιτεκτονικές κατανεμημένων βάσεων δεδομένων (2/3)

Ιεραρχικά κατανεμημένη DB

Η θέση υποδεικνύεται από τον αριθμό

Ενημέρωση μόνο όταν ο χρήστης δεν κινείται στην περιοχή του

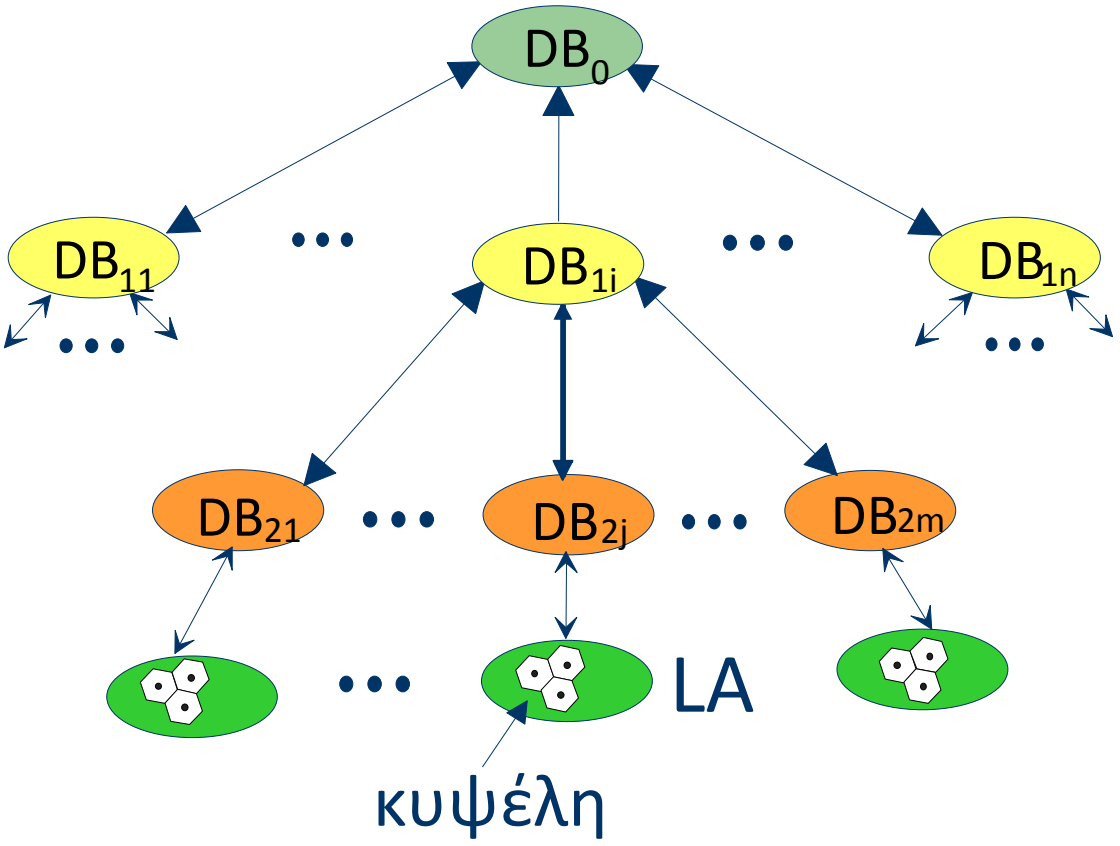


Χώρα	Πόλη	Θέση

Μορφή αριθμού

Αρχιτεκτονικές κατανεμημένων βάσεων δεδομένων (3/3)

Ιεραρχική DB με τρία επίπεδα



Στρατηγικές εντοπισμού δεδομένων στην DDB (1/8)

- Η υιοθέτηση μιας συγκεκριμένης στρατηγικής επηρεάζεται σημαντικά από τον τρόπο κατανομής της πληροφορίας της DDB στους κόμβους της.
- Η βασική παραδοχή είναι, ότι πληροφορία που αφορά χρήστες και τερματικά χρειάζεται σε δύο περιοχές της βάσης δεδομένων:
  - Στην οικεία περιοχή (Resident Data Storage Node).
  - Στην περιοχή που επισκέπτεται ο χρήστης (Visitors Data Storage Node).

Στρατηγικές εντοπισμού δεδομένων στην DDB (2/8)

Όσον αφορά τη συνολική επίδοση του συστήματος, η στρατηγική εντοπισμού δεδομένων επηρεάζει:

- Την καθυστέρηση εντοπισμού δεδομένων (interrogation delay).
- Την επίδοση της DDB
  - Επηρεάζει τον αριθμό των κατανεμημένων κόμβων της DDB, που θα ερωτηθούν.
  - Καθορίζει τον μηχανισμό ενημέρωσης της πληροφορίας στους κατάλληλους κόμβους.
  - Επηρεάζει τον χώρο αποθήκευσης που χρειάζεται για τη σωστή λειτουργία της.

Στρατηγικές εντοπισμού δεδομένων στην DDB (3/8)

Από την πλευρά του παρόχου δικτύου, μια αποτελεσματική στρατηγική εντοπισμού δεδομένων πρέπει να έχει τα εξής χαρακτηριστικά:

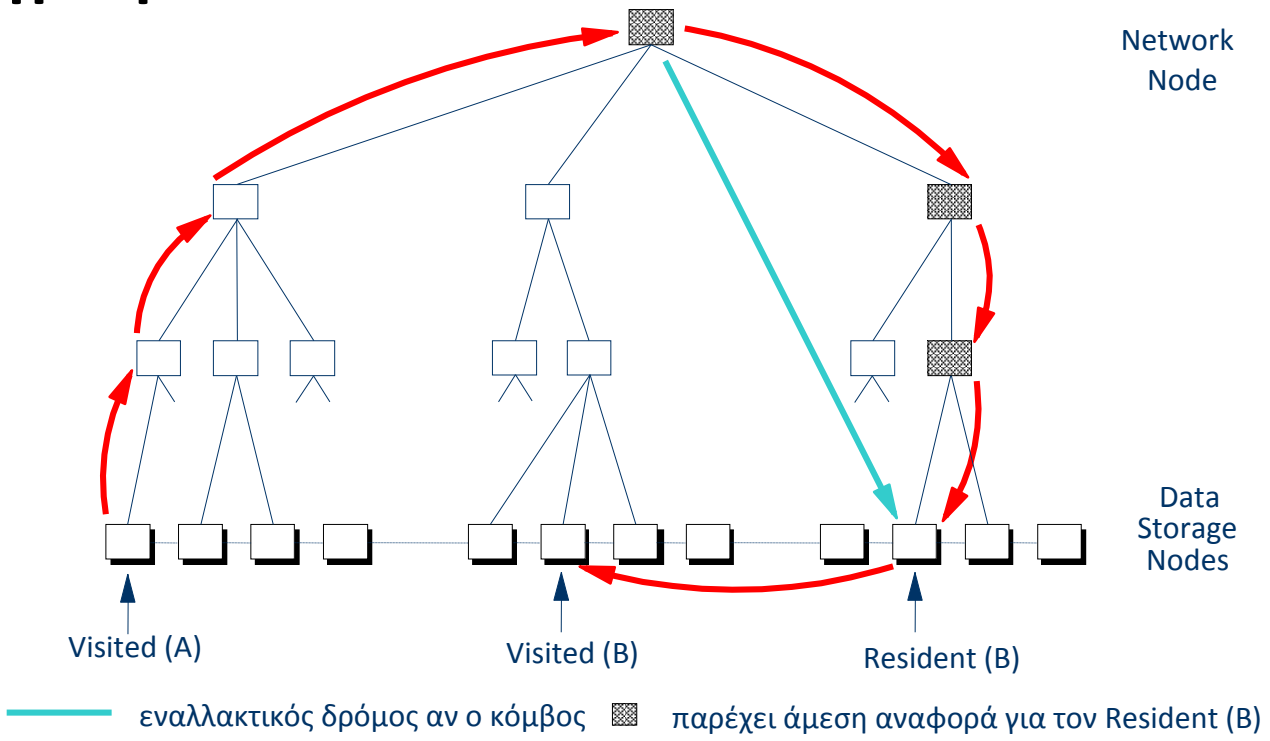
- Να ελαχιστοποιεί, όσο είναι δυνατό, τον απαιτούμενο **χώρο αποθήκευσης**.

– Να ελαχιστοποιεί τον **ρυθμό άφιξης ερωτήσεων**, κατά τη διάρκεια του εντοπισμού της ζητούμενης πληροφορίας.

– Να ελαχιστοποιεί τον ρυθμό άφιξης αιτήσεων που αφορούν την **ενημέρωση της πληροφορίας** παραπομπών.

Στρατηγικές εντοπισμού δεδομένων στην DDB (4/8)

Στρατηγική R

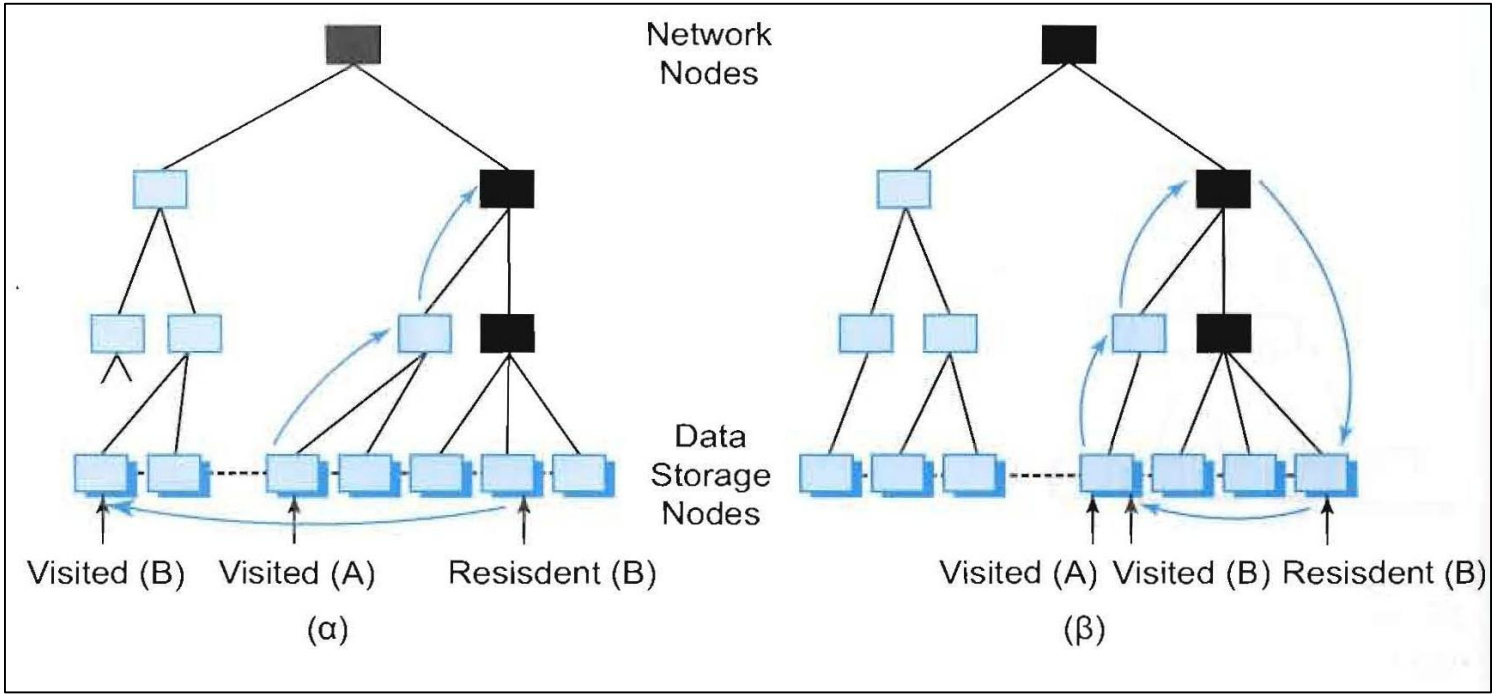


Εικόνα 1.

\+ απλοί κανόνες
\- μεγάλοι βρόχοι
\- οικείος κόμβος εκτός ⇒ οικείοι χρήστες εκτός

Στρατηγικές εντοπισμού δεδομένων στην DDB (5/8)

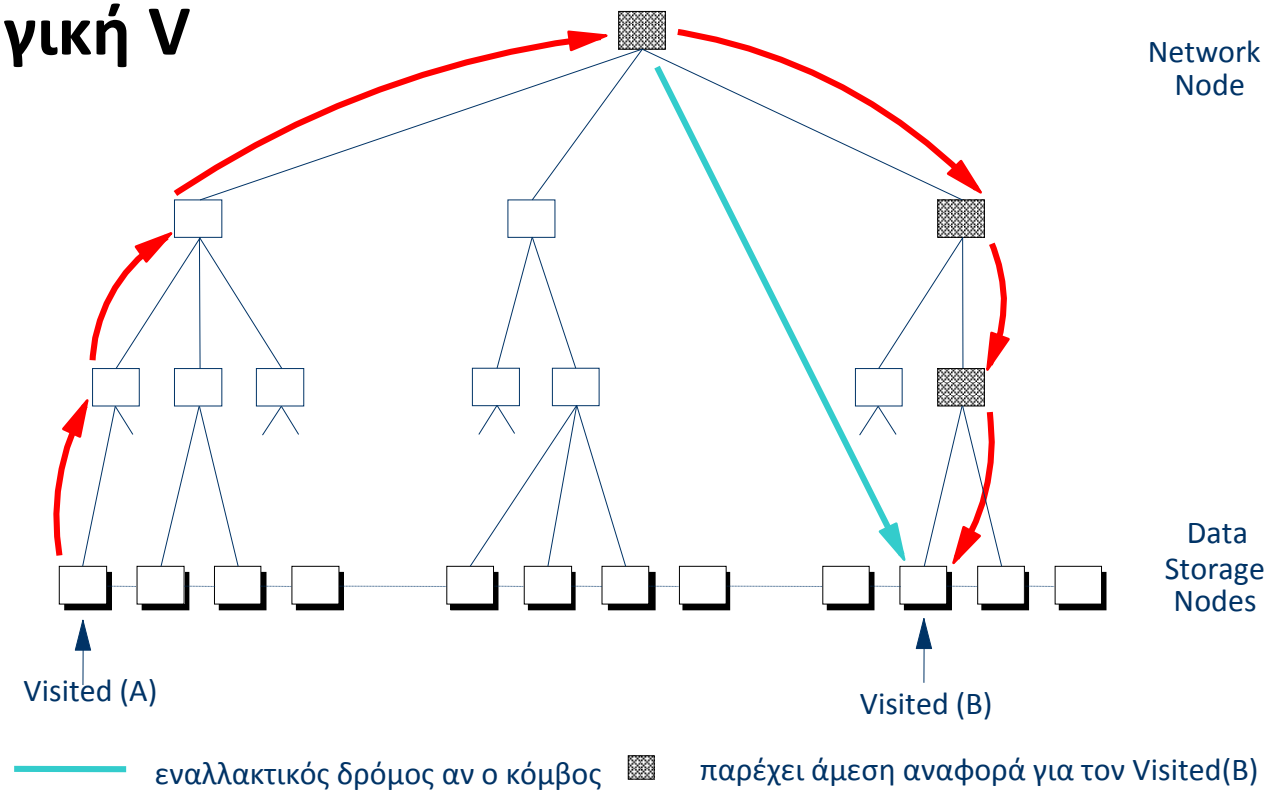
Στρατηγική R - Παραδείγματα



- Ακολουθείται η λογική του GSM (αναζήτηση του χρήστη στο οικείο δίκτυο πρώτα)
- Δεν ευνοούνται οι τοπικές κλήσεις

Στρατηγικές εντοπισμού δεδομένων στην DDB (6/8)

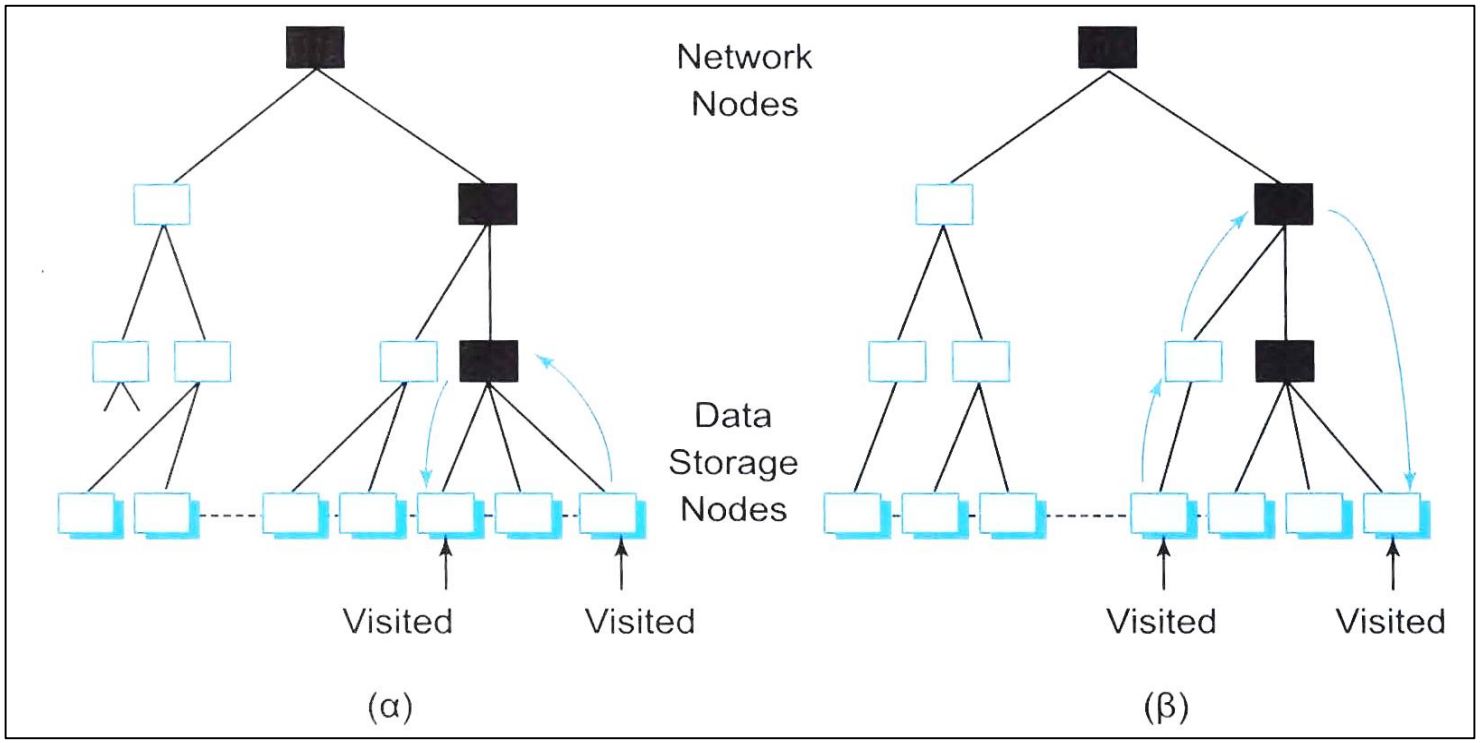
Στρατηγική V



+ υποστηρίζει τοπικότητα, όχι μεγάλοι βρόχοι
- καθυστέρηση για κλήσεις μεγάλων αποστάσεων
- Περισσότερες ενημερώσεις

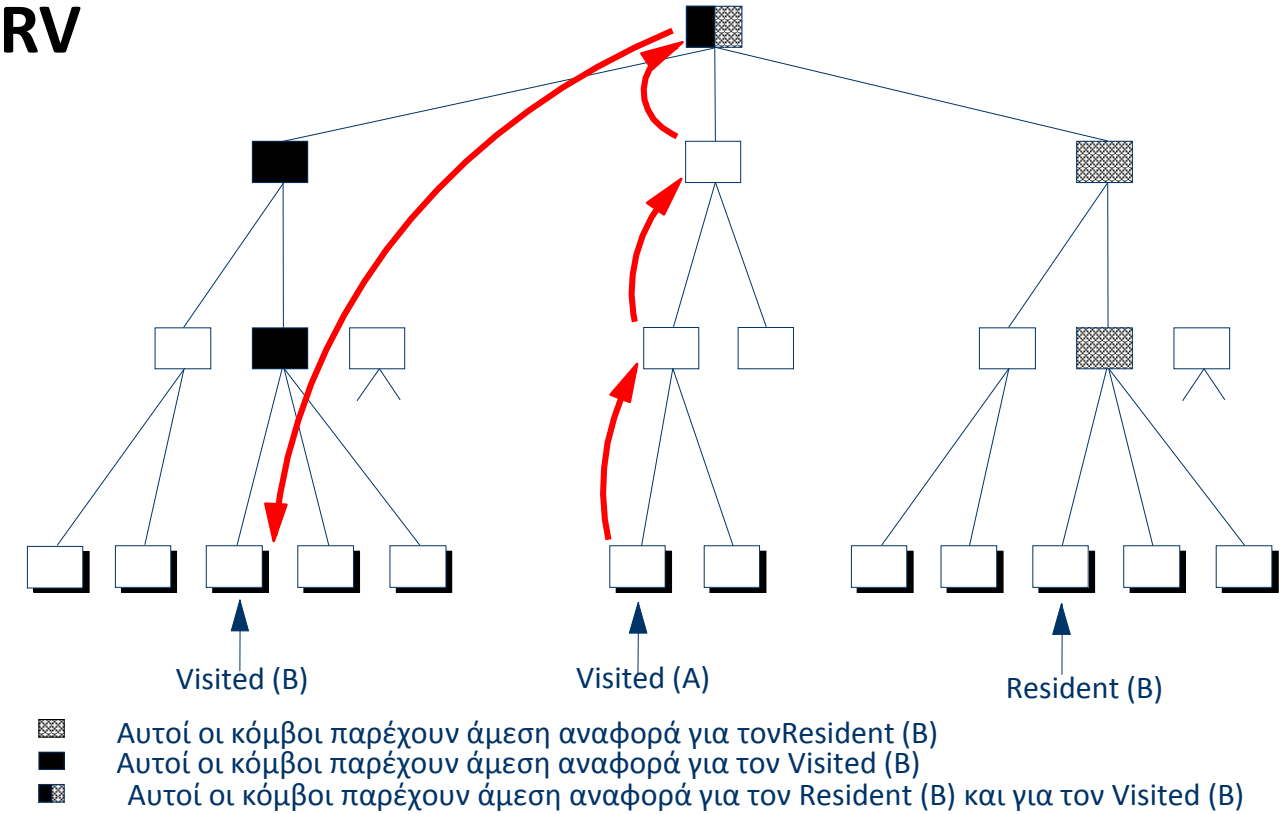
Στρατηγικές εντοπισμού δεδομένων στην DDB (7/8)

Στρατηγική V - Παραδείγματα



Στρατηγικές εντοπισμού δεδομένων στην DDB (8/8)

Στρατηγική RV



\+ υποστηρίζει τοπικότητα

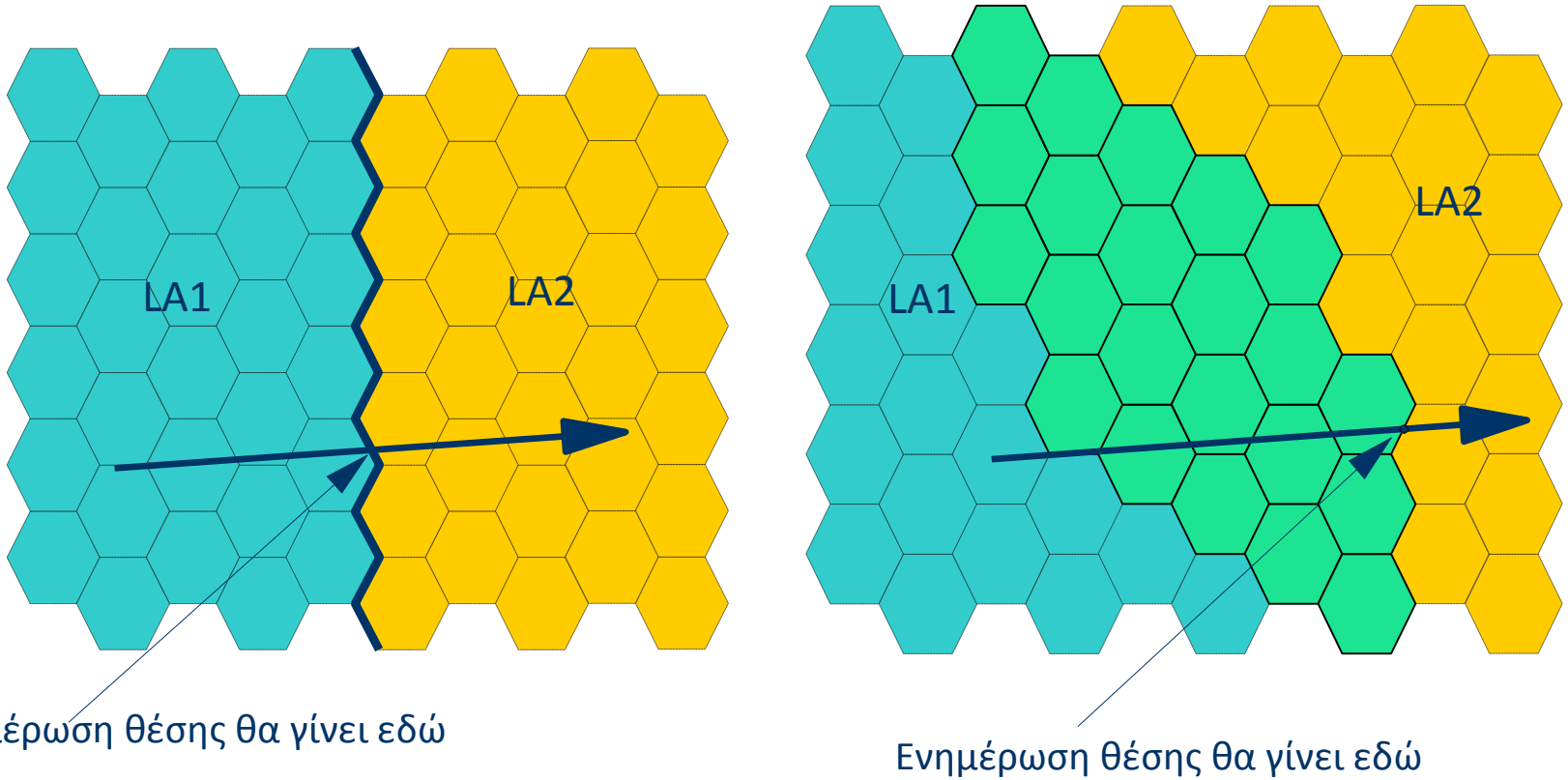
\+ λιγότερες ανεπιτυχείς αναζητήσεις στους ενδιάμεσους

\- μεγαλύτερος χώρος αποθήκευσης

Ενημέρωση θέσης και αναζήτηση (1/3)

- Υπάρχουν μερικά **μειονεκτήματα**, όσον αφορά την επίδοση των διαδικασιών ενημέρωσης θέσης και αναζήτησης που βασίζονται στις LA.
  - **Υπερβολικές ενημερώσεις** θέσης από MT που μετακινούνται κατά μήκος των **συνόρων** δύο LA.
  - Η **αναζήτηση** ενός MT σε όλη την LA, μπορεί να έχει ως αποτέλεσμα υπερβολικό **όγκο κίνησης**.
  - Η κινητικότητα και ο ρυθμός άφιξης των κλήσεων των MT μεταβάλλονται και **δεν υπάρχει ένα μέγεθος LA, το οποίο να είναι βέλτιστο** για όλους τους χρήστες ή **ακόμα και για τον ίδιο χρήστη**.

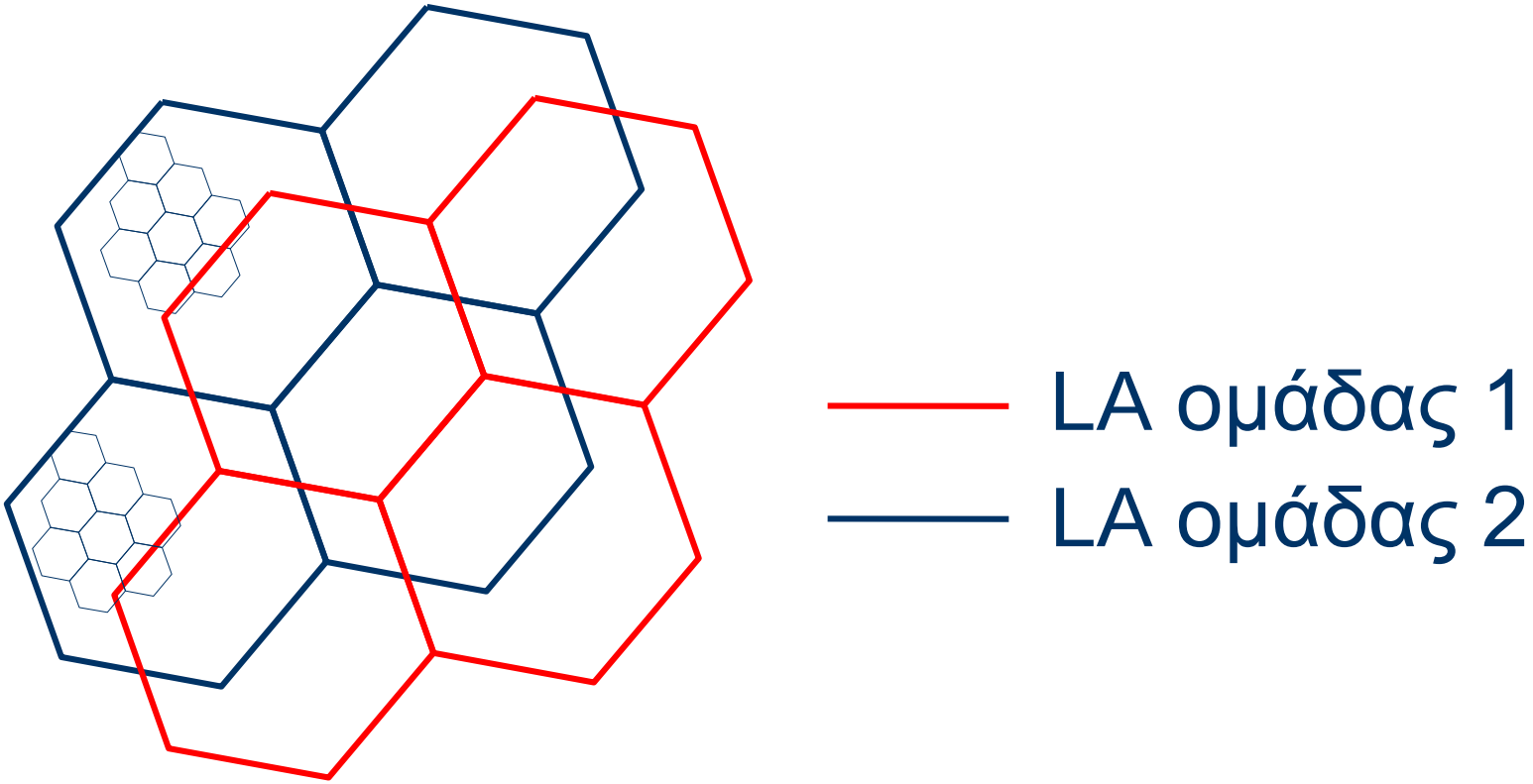
Αντιμετώπιση προβλήματα ζιγκ-ζαγκ: Επικαλυπτόμενες LAs



Τι πληρώνουμε: Απαιτούνται μεγαλύτερες ή περισσότερες LAs

Επιβάρυνση κυψελών στα σύνορα με μεγάλη σηματοδοσία

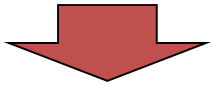
- Διαφορετικές Las για διαφορετικές ομάδες χρηστών: Οι χρήστες μοιράζονται



Ενημέρωση θέσης και αναζήτηση (2/3)

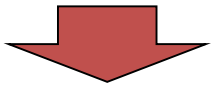
- Το κόστος λειτουργίας του συστήματος για την ενημέρωση θέσης και για την αναζήτηση εξαρτάται από δύο παράγοντες:

  1. Το **φορτίο σηματοδοσίας**, που προκαλείται από τις ανταλλαγές μηνυμάτων κατά τη διάρκεια των διαδικασιών **ενημέρωσης θέσης και αναζήτησης**.

     Κατάλληλος σχεδιασμός των περιοχών εντοπισμού και αναζήτησης, περίτεχνες τεχνικές ενημέρωσης θέσης και αναζήτησης.

  2. Το πλήθος **διεργασιών με τη βάση δεδομένων**, που πραγματοποιείται κατά την ενημέρωση θέσης και την αναζήτηση.

     Κατανεμημένες βάσεις δεδομένων.

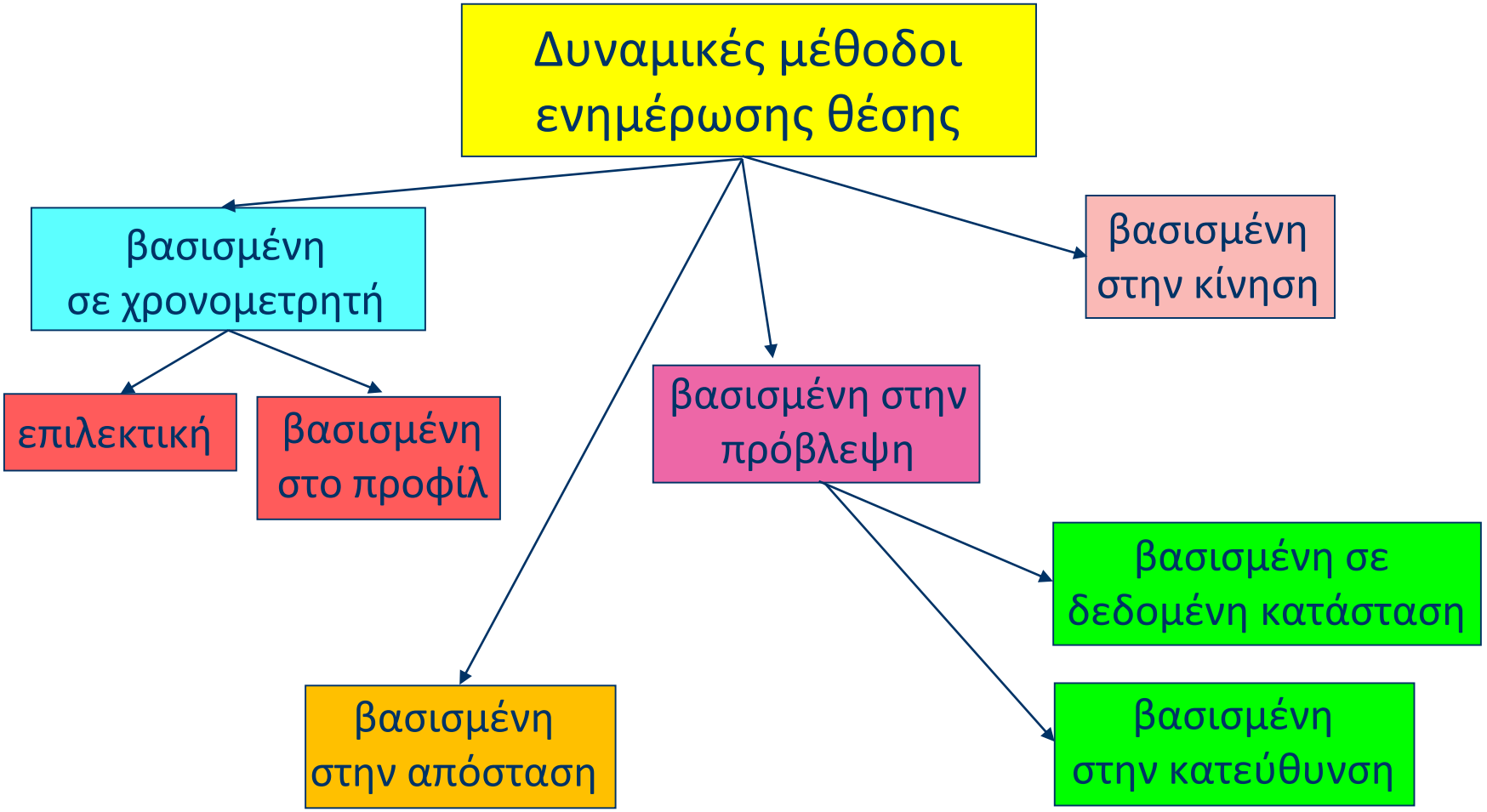
Ενημέρωση θέσης και αναζήτηση (3/3)

- Ο σχεδιασμός των LAs πολυ σημαντικός για τον όγκο σηματοδοσίας και την καθυστέρηση ενημέρωσης και αναζήτησης
- 2 ακραίες λύσεις:
  1. **Κάθε κυψέλη είναι και διαφορετική LA**: Πολλές ενημερώσεις, ταχύτατη αναζήτηση
  2. **Μία μόνο LA ίση με όλο το δίκτυο**: Καμιά ενημέρωση, μεγάλη καθυστέρηση αναζήτησης
- Γενικά
  1. Μικρή κινητικότητα = μικρές LAs
  2. Μεγάλη κινητικότητα = μεγάλες LAs
- Ομαδοποίηση χρηστών ανά προφίλ κινητικότητας και διαφορετικές LAs ανά ομάδα

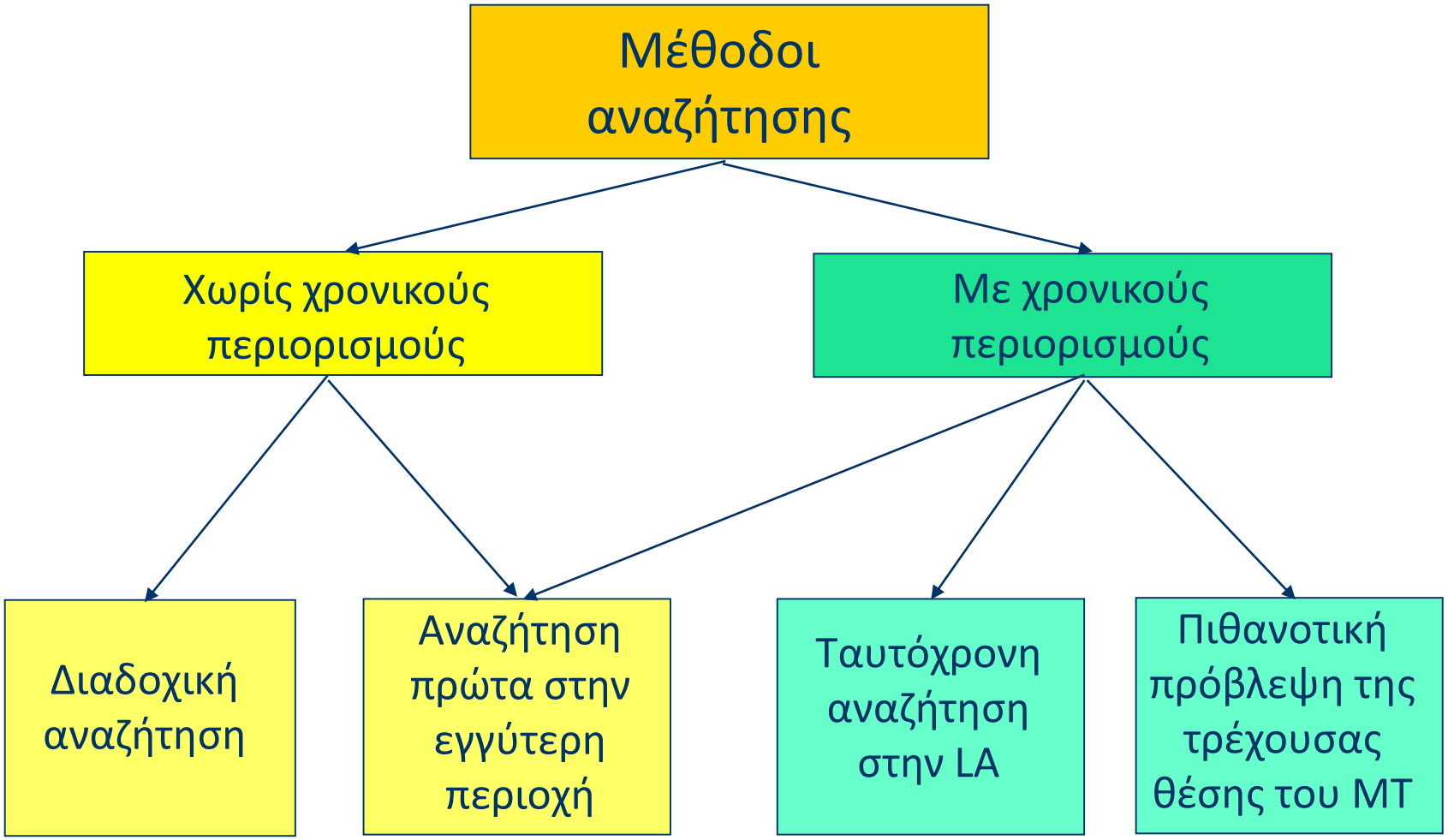
Δυναμικές μέθοδοι ενημέρωσης θέσης (1/2)

- Δυναμική ρύθμιση των παραμέτρων διαχείρισης εντοπισμού των επιμέρους χρηστών, ώστε να βελτιστοποιηθεί η επίδοση του συστήματος.
  - Μέθοδοι που βασίζονται στον ***χρόνο***
  - Μέθοδοι που βασίζονται στην ***κίνηση***
  - Μέθοδοι που βασίζονται στην ***απόσταση***
  - Μέθοδοι ***πρόβλεψης***

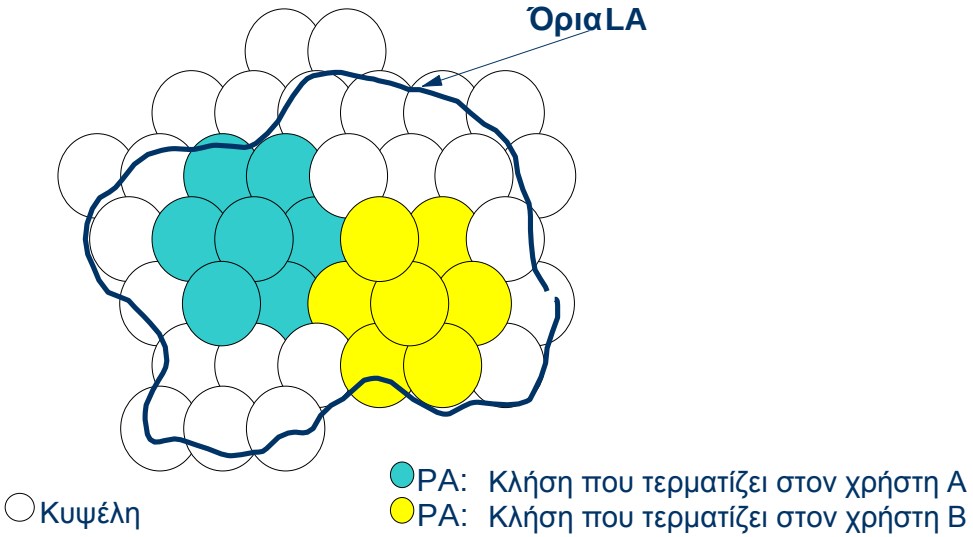
Δυναμικές μέθοδοι ενημέρωσης θέσης (2/2)



Μέθοδοι αναζήτησης

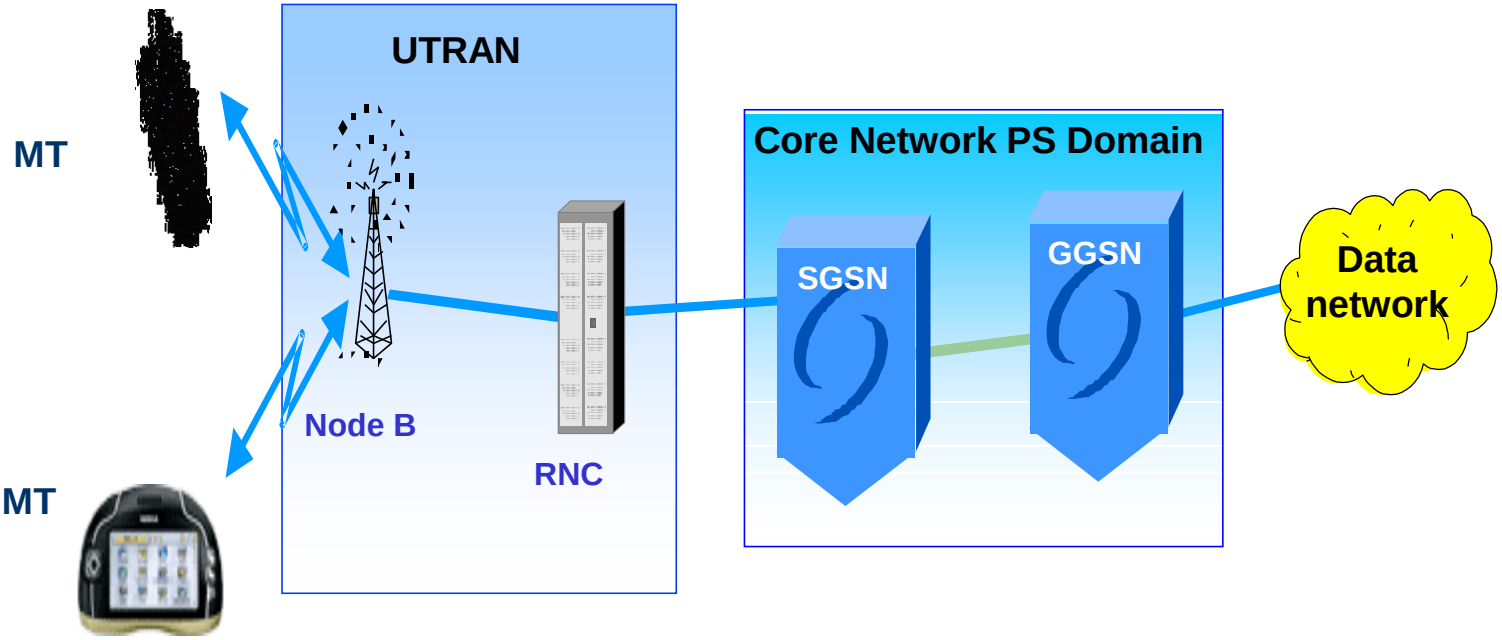


Ευφυής αναζήτηση



Διαφορετικά LAs ανά χρήστη, ανάλογα με: κινητικότητα, πρόσφατη επικοινωνία, ώρα ημερας, δημοφιλή σημεία, κτλ.

Διαχείριση εντοπισμού στο UMTS (1/2)



Node B: Base station

RNC: Radio Network Controller

MT: Mobile Terminal

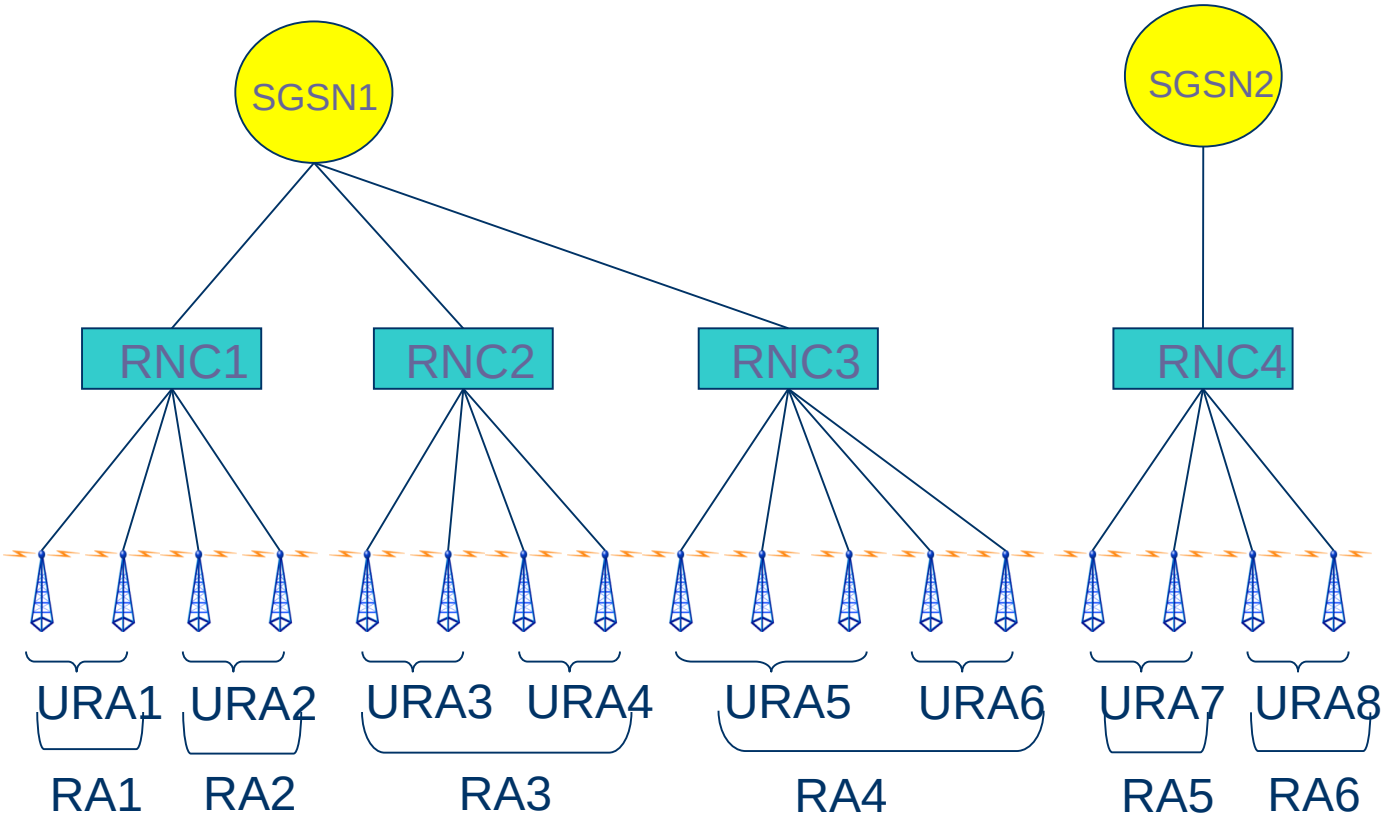
GGSN: Gateway GPRS Support Node

SGSN: Serving GPRS Support Node

UTRAN: UMTS Terrestrial Radio Access Network

Εικόνα 2.

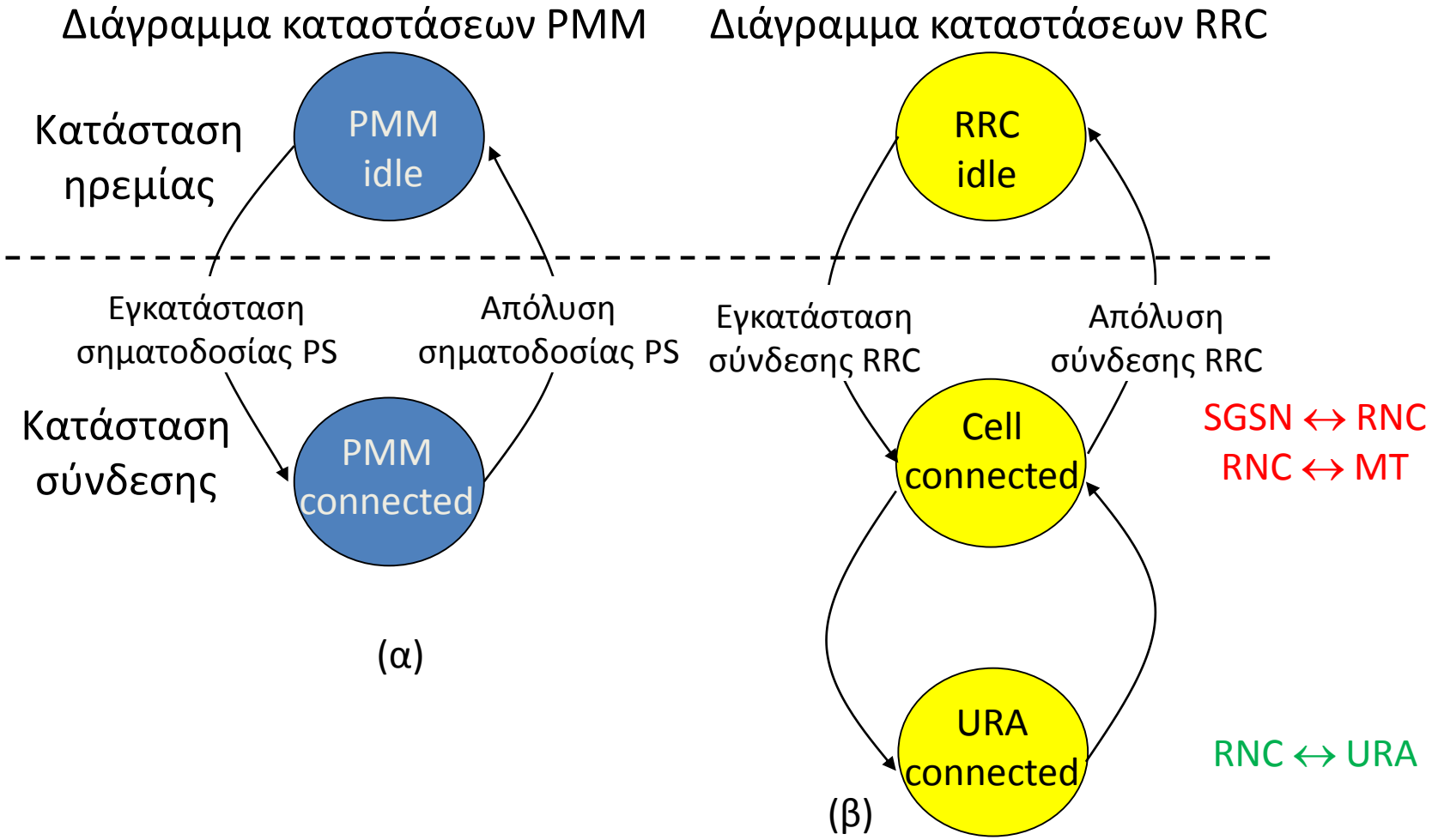
Διαχείριση εντοπισμού στο UMTS (2/2)



RA: Routing Area
URA: UTRAN Registration Area

Εικόνα 3.

Διαχείριση εντοπισμού στο UMTS για μετάδοση δεδομένων



Διαχείριση ασφάλειας

Ασφάλεια στα ψηφιακά δίκτυα: ορολογία

Αυθεντικότητα:

- Αυθεντικότητα SIM
- Αυθεντικότητα χρήστη
- Αυθεντικότητα δικτύου

Ακεραιότητα:

- Ακεραιότητα δεδομένων σηματοδοσίας και χρήστη

Εμπιστευτικότητα (≈ privacy):

- Κρυπτογράφηση των σημάτων στην ασύρματη διεπαφή.
- Απόκρυψη των αναγνωριστικών χρήστη στην ασύρματη διεπαφή.
- Απόκρυψη απ’ άκρη σ’ άκρη (από τον πάροχο υπηρεσίας).

Πιστοποίηση Αυθεντικότητας

Διαδικασία διακρίβωσης της αυθεντικότητας μιας οντότητας (χρήστης, τερματικό, δίκτυο, στοιχείο δικτύου). Είναι η οντότητα εκείνη που ισχυρίζεται ότι είναι;

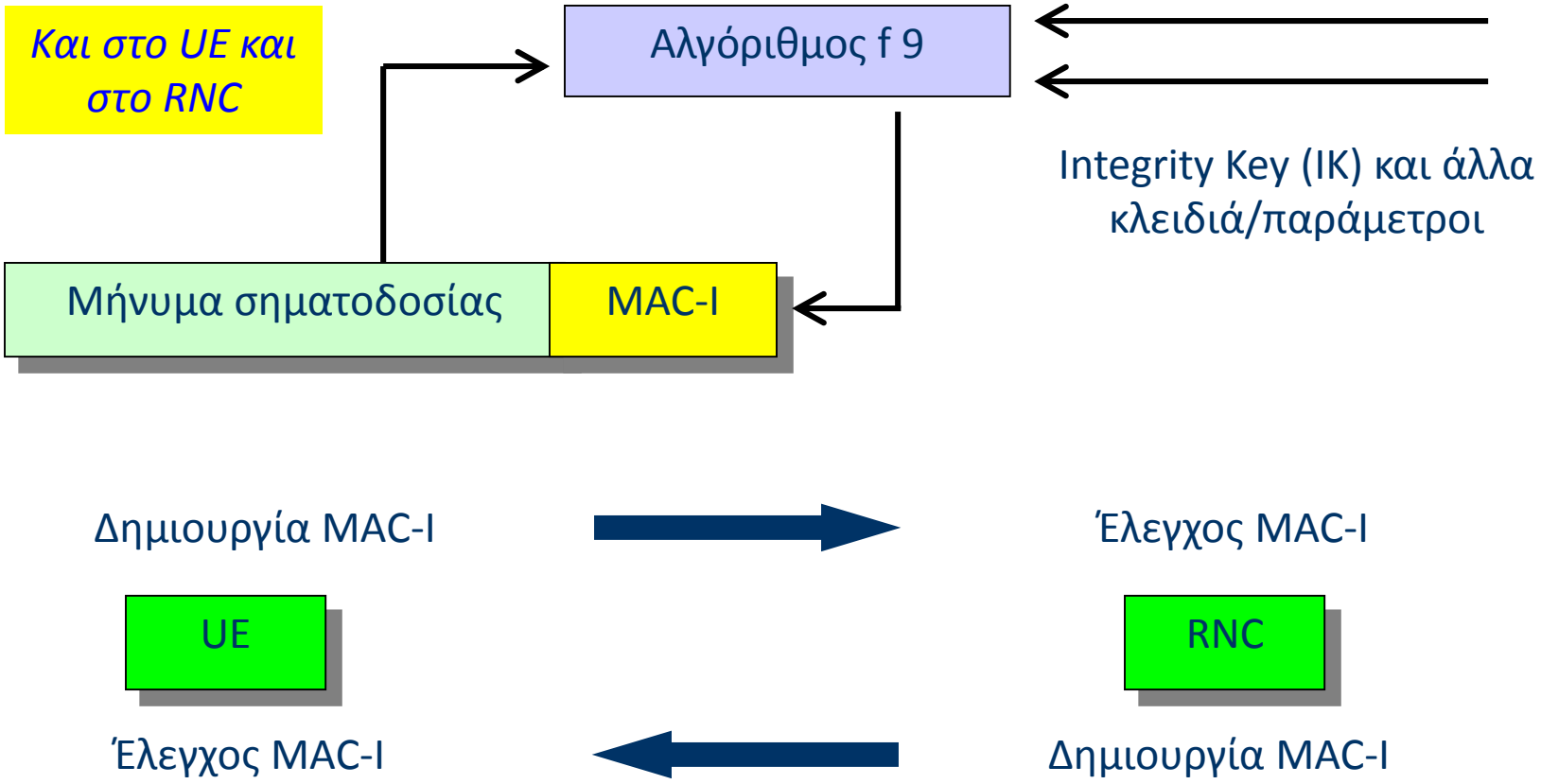
- Η πιστοποίηση αυθεντικότητας SIM είναι τοπική (το δίκτυο δεν παρεμβαίνει).
- Στο GSM, πιστοποιείται μόνο η αυθεντικότητα του χρήστη (τερματικού).
- Στο UMTS, πιστοποιείται η αυθεντικότητα και του χρήστη (τερματικού) και του δικτύου.
- Η πιστοποίηση της αυθεντικότητας χρήστη/δικτύου γίνεται στην αρχή κάθε διεργασίας μεταξύ χρήστη-δικτύου (π.χ. ενημέρωση θέσης ή εγκατάσταση σύνδεσης) και πάντα πριν αρχίσει η κρυπτογράφηση.

Ακεραιότητα δεδομένων

Η ιδιότητα ότι τα δεδομένα δεν έχουν αλλαχθεί κατά μη εγκεκριμένο τρόπο.

- Επίθεση ασφάλειας, π.χ. παραπλανητικός BS.
- Έλεγχος ακεραιότητας σηματοδοσίας δεν γίνεται στο GSM.
- Στο UMTS, επισυνάπτεται στα μηνύματα σηματοδοσίας ένα πεδίο ασφαλείας 32 bit (MAC-I) στο τερματικό ή στο RNC, πριν τη μετάδοσή τους και ελέγχονται στη πλευρά της λήψης.
- Στο UMTS, προστατεύεται ο όγκος των δεδομένων χρήστη (όχι τα δεδομένα αυτά καθαυτά).

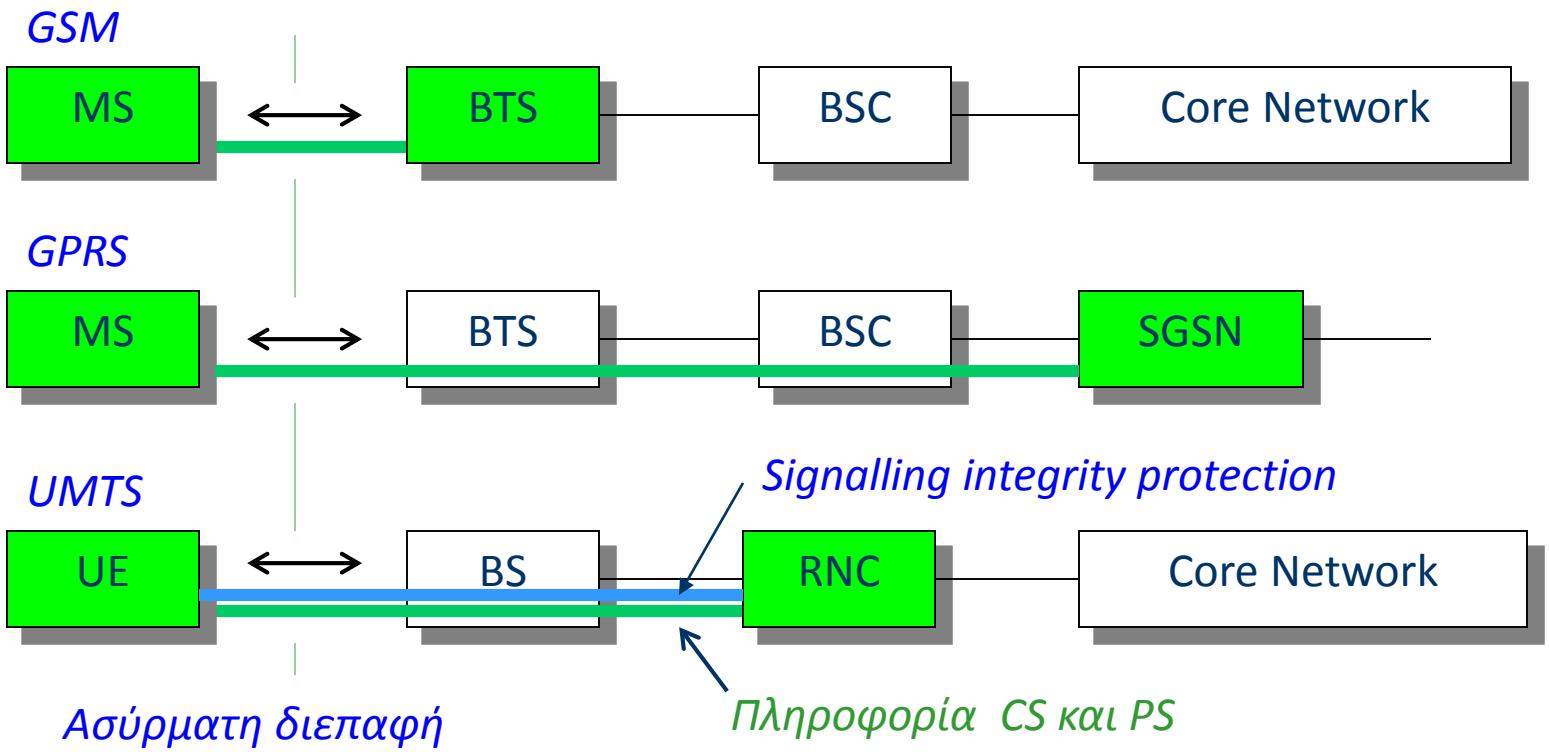
Ακεραιότητα δεδομένων σηματοδοσίας στο UMTS



Εμπιστευτικότητα

- Η ιδιότητα ότι η πληροφορία δεν γίνεται προσιτή σε μη εξουσιοδοτημένα άτομα, οντότητες ή διαδικασίες.
- **Παράδειγμα 1**: Κρυπτογράφηση στην ασύρματη διεπαφή.
- **Παράδειγμα 2**: Παρεμπόδιση μη κρυπτογραφημένης μετάδοσης πληροφορίας που αφορά την ταυτότητα του χρήστη, όπως π.χ. μετάδοση του IMSI στην ασύρματη διεπαφή.
- Παράγεται η Temporary Mobile Subscriber Identity (TMSI) στο τέλος κάθε διεργασίας MM και χρησιμοποιείται στην έναρξη της επόμενης διεργασίας αντί του IMSI.

Κρυπτογράφηση: Παραδείγματα



Διαχείριση ασφάλειας στο GSM (1/2)

- Στοχεύει στην προστασία της ασύρματης διεπαφής.
- Δεν υπάρχει προστασία στο ενσύρματο μέρος του δικτύου (ούτε για εμπιστευτικότητα ούτε για προστασία απορρήτου).
- Το φιλοξενούν δίκτυο έχει πρόσβαση σε όλα τα δεδομένα (εκτός από το μυστικό κλειδί του χρήστη).
- Έχουν αναφερθεί επιτυχείς επιθέσεις:
  - παραπλανητικοί σταθμοί βάσης
  - κλωνοποιήσεις της κάρτας SIM

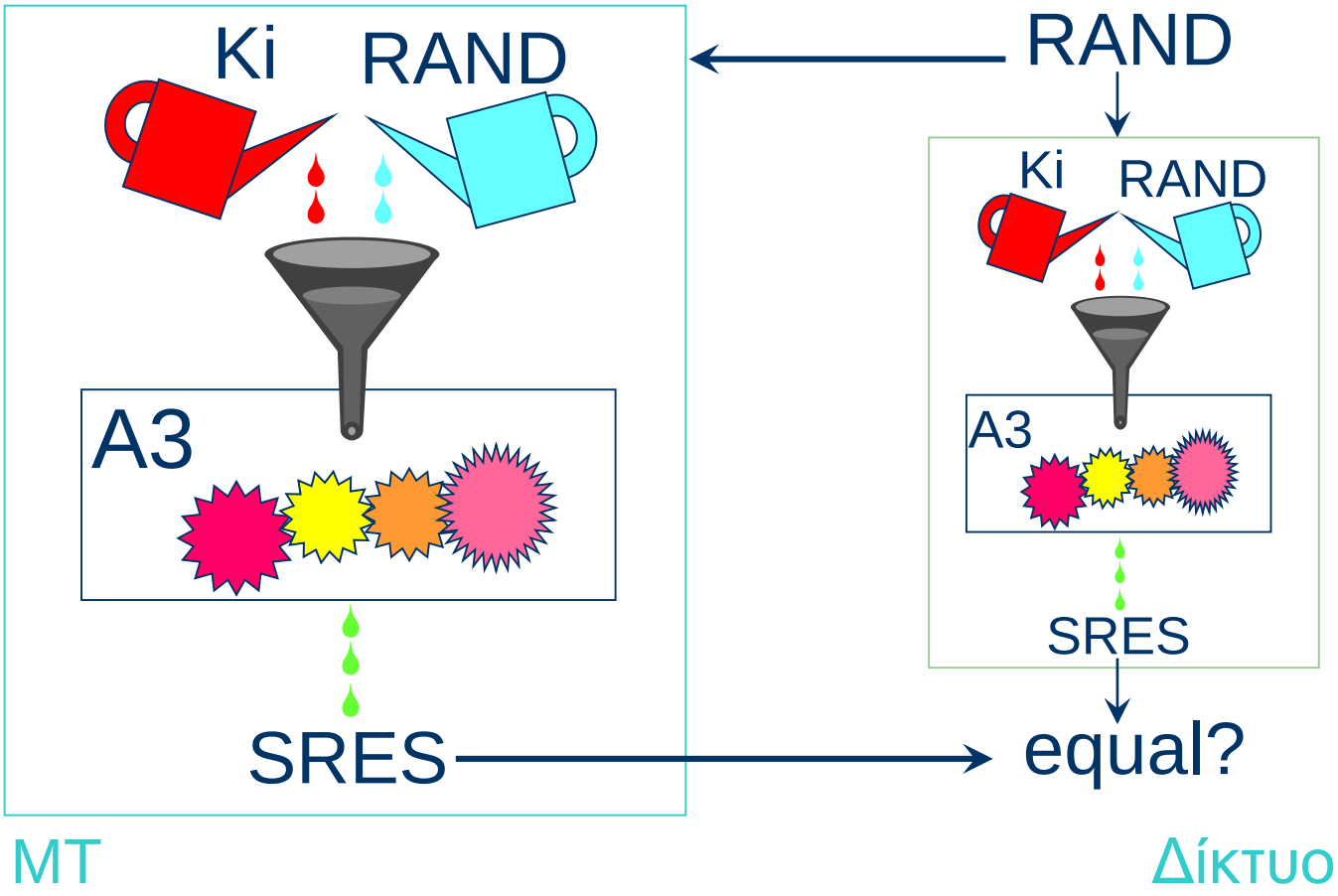
Διαχείριση ασφάλειας στο GSM (2/2)

- Δύο στόχοι:
- Προστασία δικτύου από μη εξουσιοδοτημένη πρόσβαση.
  - Πιστοποίηση αυθεντικότητας
- Προστασία του απορρήτου της επικοινωνίας.
  - Κρυπτογραφημένη μετάδοση στο ασύρματο τμήμα.
  - Προστασία σηματοδοσίας με τον ίδιο τρόπο.
  - Αντικατάσταση του IMSI με TMSI.

Λειτουργίες ασφάλειας (1/3)

- Απλή πιστοποίηση αυθεντικότητας (χρήση PIN).
  - Μικρή προστασία.
  - Στο GSM το PIN ελέγχεται από το SIM χωρίς να μεταδίδεται στο ασύρματο τμήμα.
- Μία πιο περίτεχνη τεχνική συνίσταται στο να γίνει κάποια ερώτηση, που μόνο ο σωστός χρήστης (MT με το SIM) μπορεί να απαντήσει.
- Υπάρχει ένας τεράστιος αριθμός ερωτήσεων και είναι απίθανο να χρησιμοποιηθεί δύο φορές η ίδια ερώτηση.

Λειτουργίες ασφάλειας (2/3)



SRES: SignedRESult

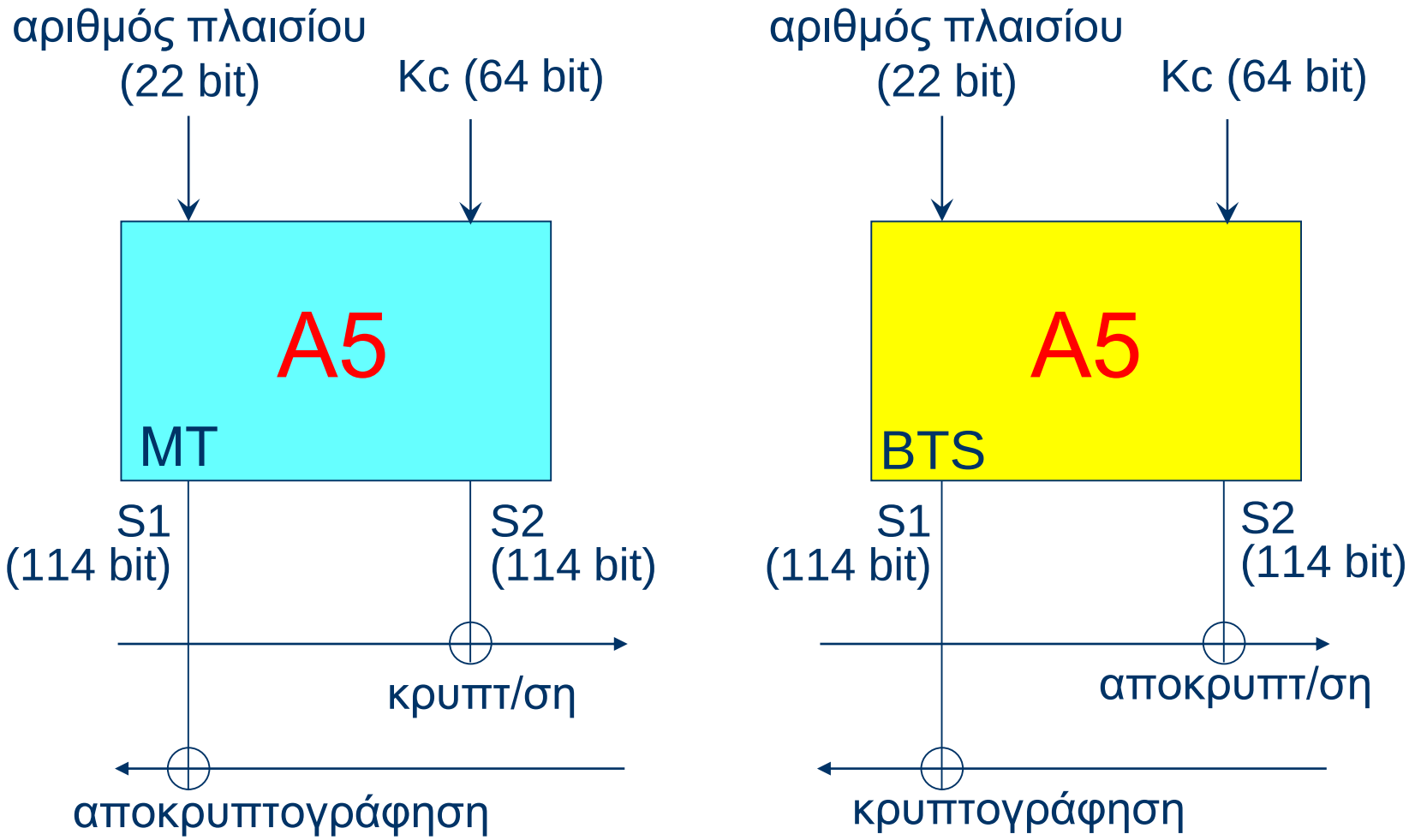
Λειτουργίες ασφάλειας (3/3)

- SRES = f (Ki, RAND) : εύκολο
- Ki = g (SRES, RAND) : όσο το δυνατό πιο πολύπλοκο
- Ακόμη και αν είναι γνωστά αρκετά ζεύγη (RAND,SRES) για τον ίδιο χρήστη (δηλ. το ίδιο Ki), ο υπολογισμός πρέπει να παραμένει πολύ πολύπλοκος.
- Ο μόνος περιορισμός είναι τα 128 bit του RAND και τα 32 bit του SRES. Το Ki μπορεί να έχει οποιοδήποτε μήκος (αν μεταφέρεται, περιορίζεται στα 128 bit).

Κρυπτογράφηση (1/2)

- Λειτουργία exclusive OR μεταξύ:
  - 114 κωδικοποιημένων bit μιας ριπής
  - 114 bit της ακολουθίας κρυπτογράφησης που παράγεται από ειδικό αλγόριθμο, τον A5
- Η ακολουθία κρυπτογράφησης για κάθε ριπή παράγεται από τον A5 με υπολογισμό δύο εισόδων:
  - Αριθμός πλαισίου
  - Kc (συμφωνείται μεταξύ MT και δικτύου)

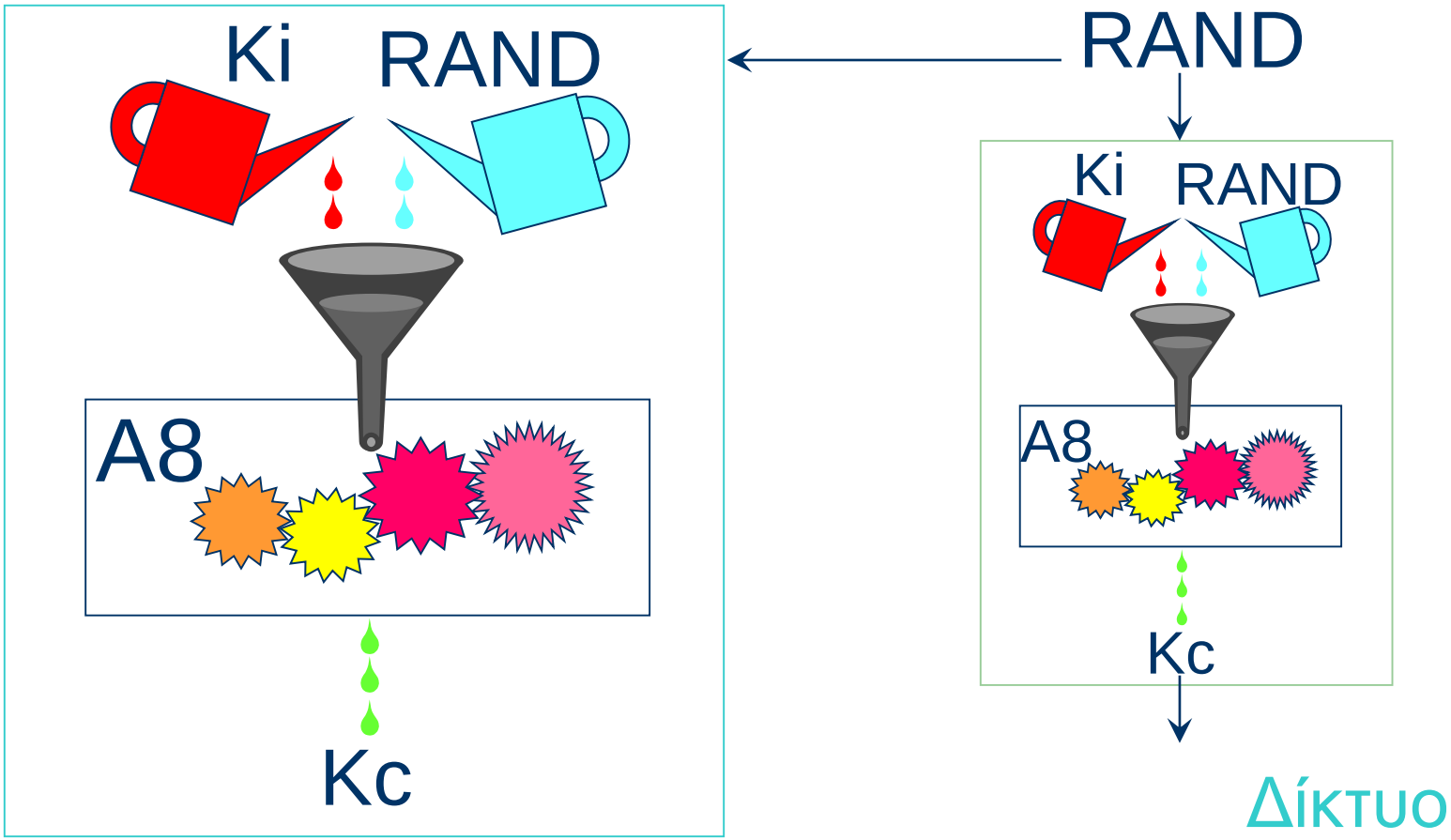
Κρυπτογράφηση (2/2)



Διαχείριση κλειδιών (1/3)

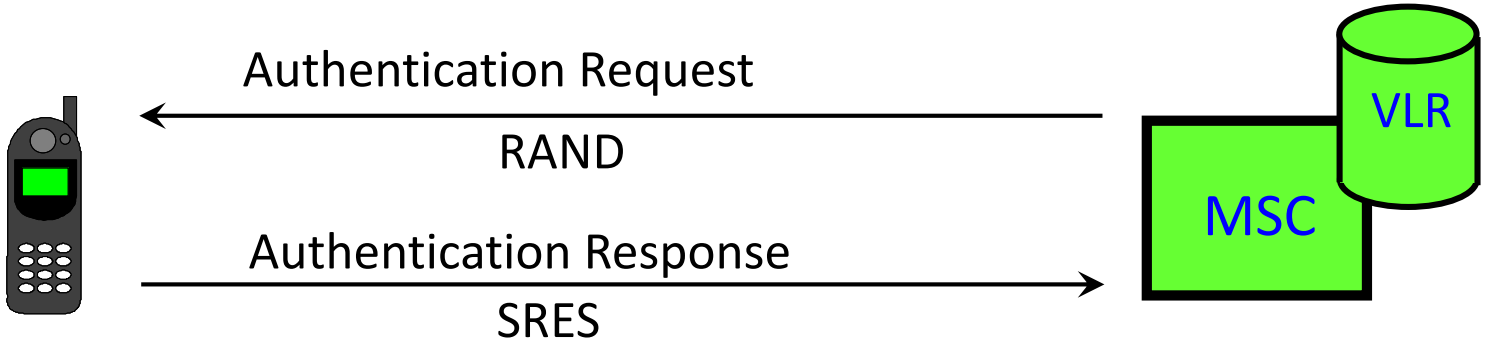
- Το Kc συμφωνείται μεταξύ ΜΤ και δικτύου πριν αρχίσει η κρυπτογράφηση.
- Υπολογίζεται κατά τη διάρκεια της διαδικασίας πιστοποίησης αυθεντικότητας.
- Το Kc φυλάσσεται στο SIM για να υπάρχει και μετά το switch-off. Φυλάσσεται επίσης και στο MSC/VLR.
- Αλγόριθμος A8 για τον υπολογισμό του Kc από τον RAND.

Διαχείριση κλειδιών (2/3)

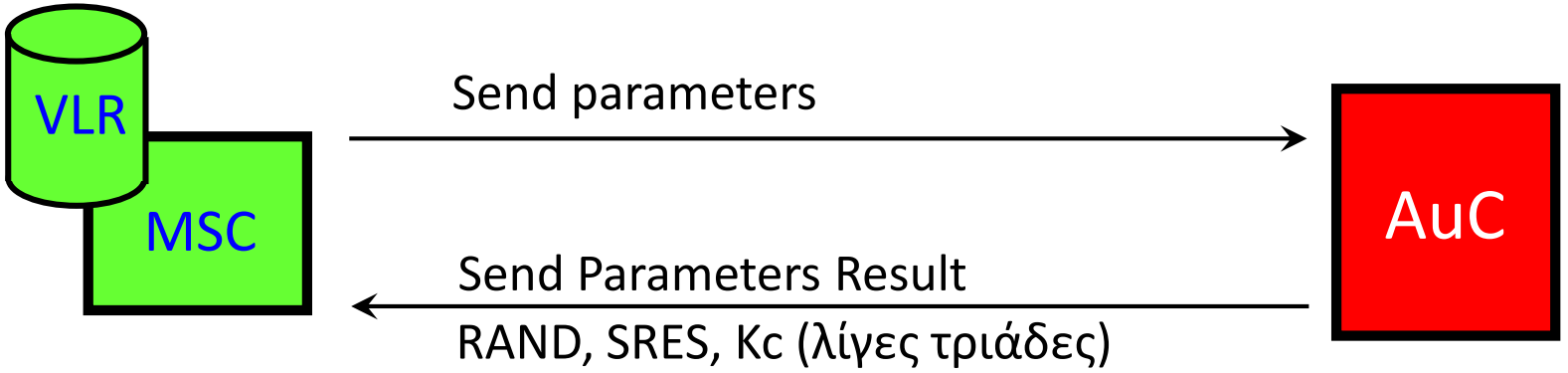


Διαχείριση κλειδιών (3/3)

Πιστοποίηση αυθεντικότητας και παραγωγή κλειδιών



Μεταφορά δεδομένων ασφαλείας



Διαχείριση ασφάλειας στο UMTS

GSM

SIM authentication (PIN code)

User authentication

Ciphering (air interface)

UMTS

USIM authentication (PIN code)

User authentication

Network authentication

Ciphering (air interface)

Signalling data integrity

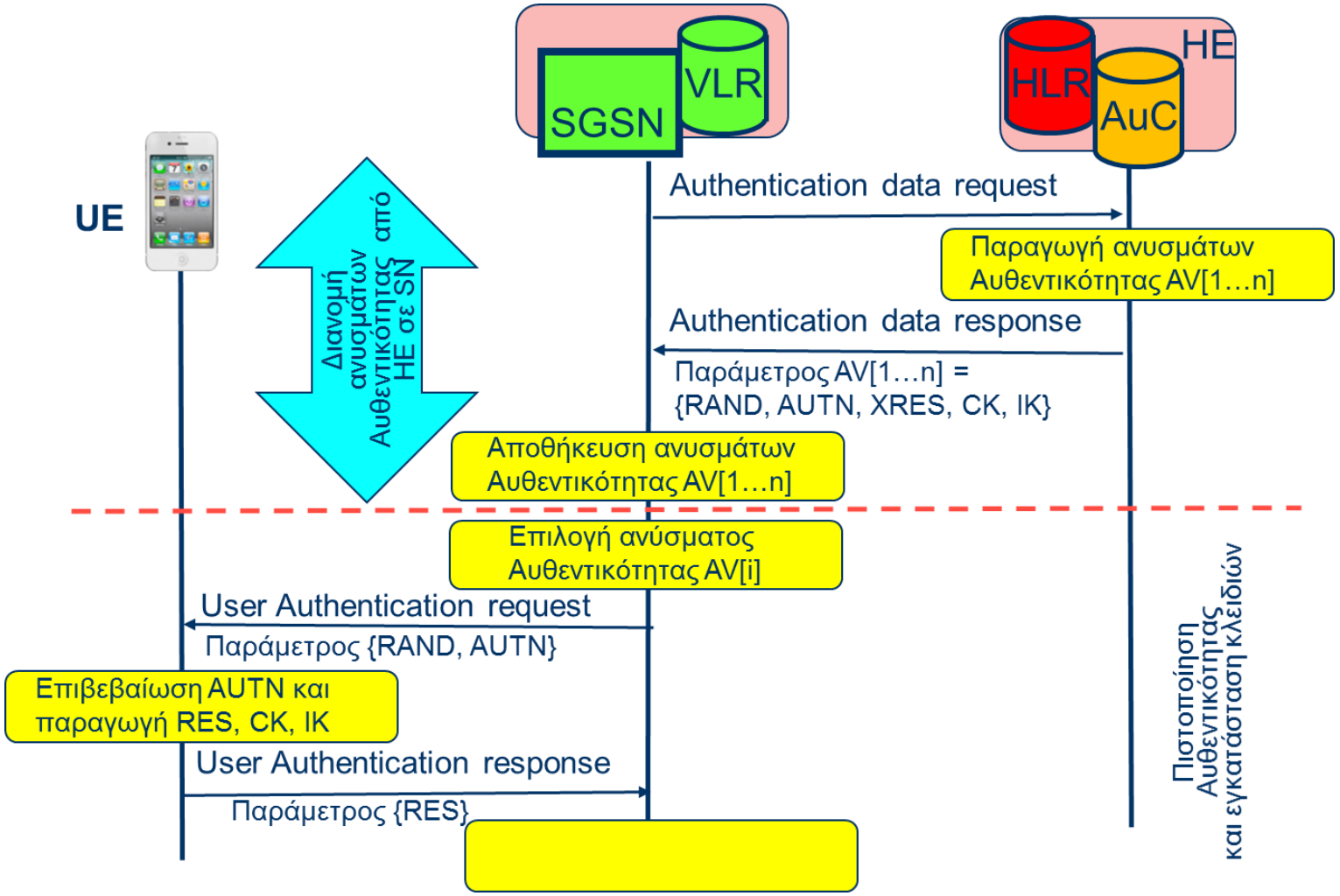
IP security (e.g. IPSEC)

UMTS: μεγαλύτερα μήκη κλειδιών απ' ό,τι στο GSM

Βελτιώσεις ως προς το GSM

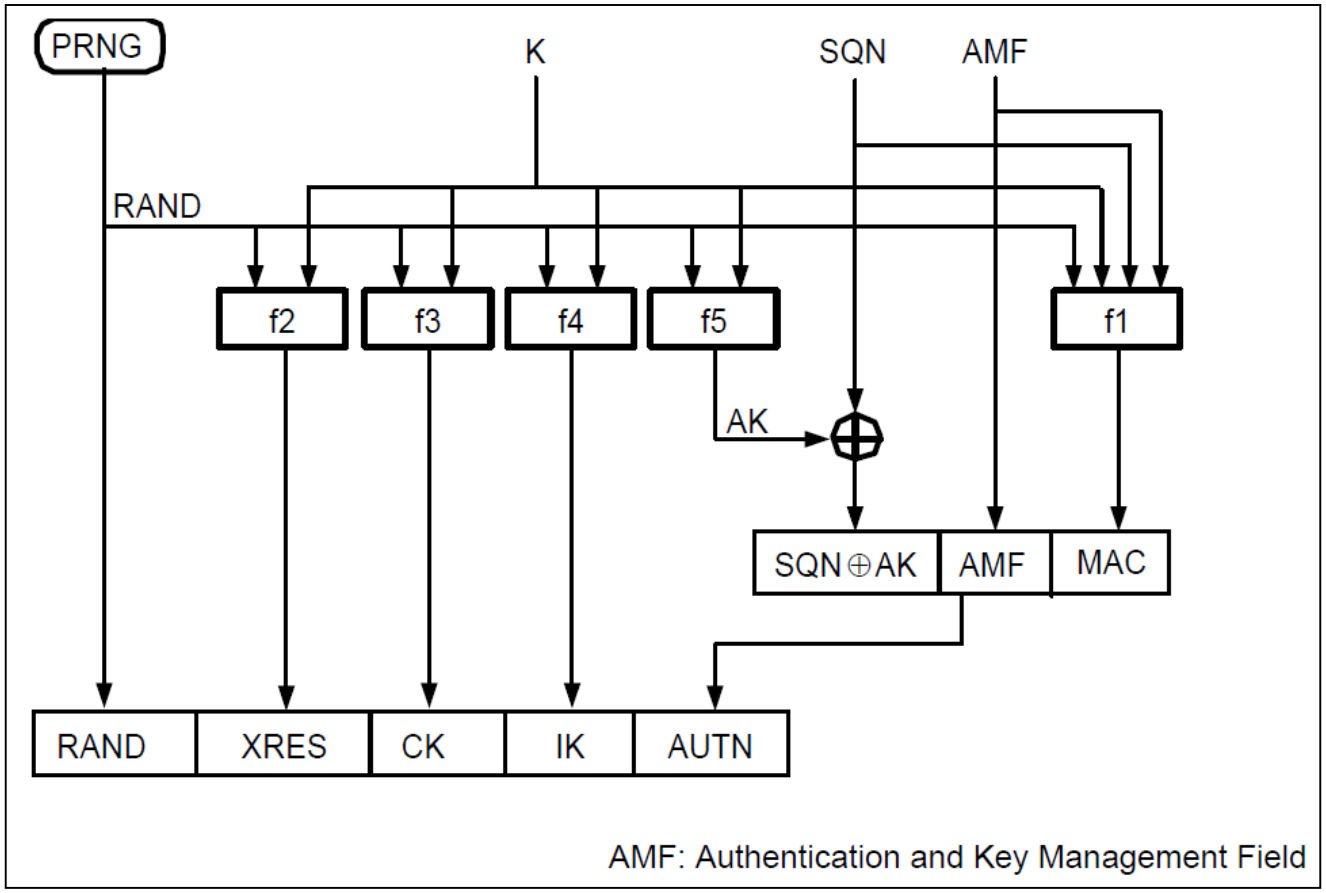
- Αμοιβαία πιστοποίηση αυθεντικότητας με επαναλαμβανόμενη προστασία.
- Προστασία δεδομένων σηματοδοσίας.
  - Ασφαλής διαπραγμάτευση των αλγορίθμων ασφαλείας.
  - Προστασία ακεραιότητας και authentication πηγής.
  - Εμπιστευτικότητα.
- Προστασία του payload των δεδομένων χρήστη.
  - Εμπιστευτικότητα.
- Κλειδιά κρυπτογράφησης και δεδομένα αυθεντικότητας μεταφέρονται διαφανώς μεταξύ των δικτύων.
- Επίπεδο ασφάλειας (μέγεθος κλειδιών): 128 bits
- Προστασία μέσα στο δίκτυο.

UMTS AKA



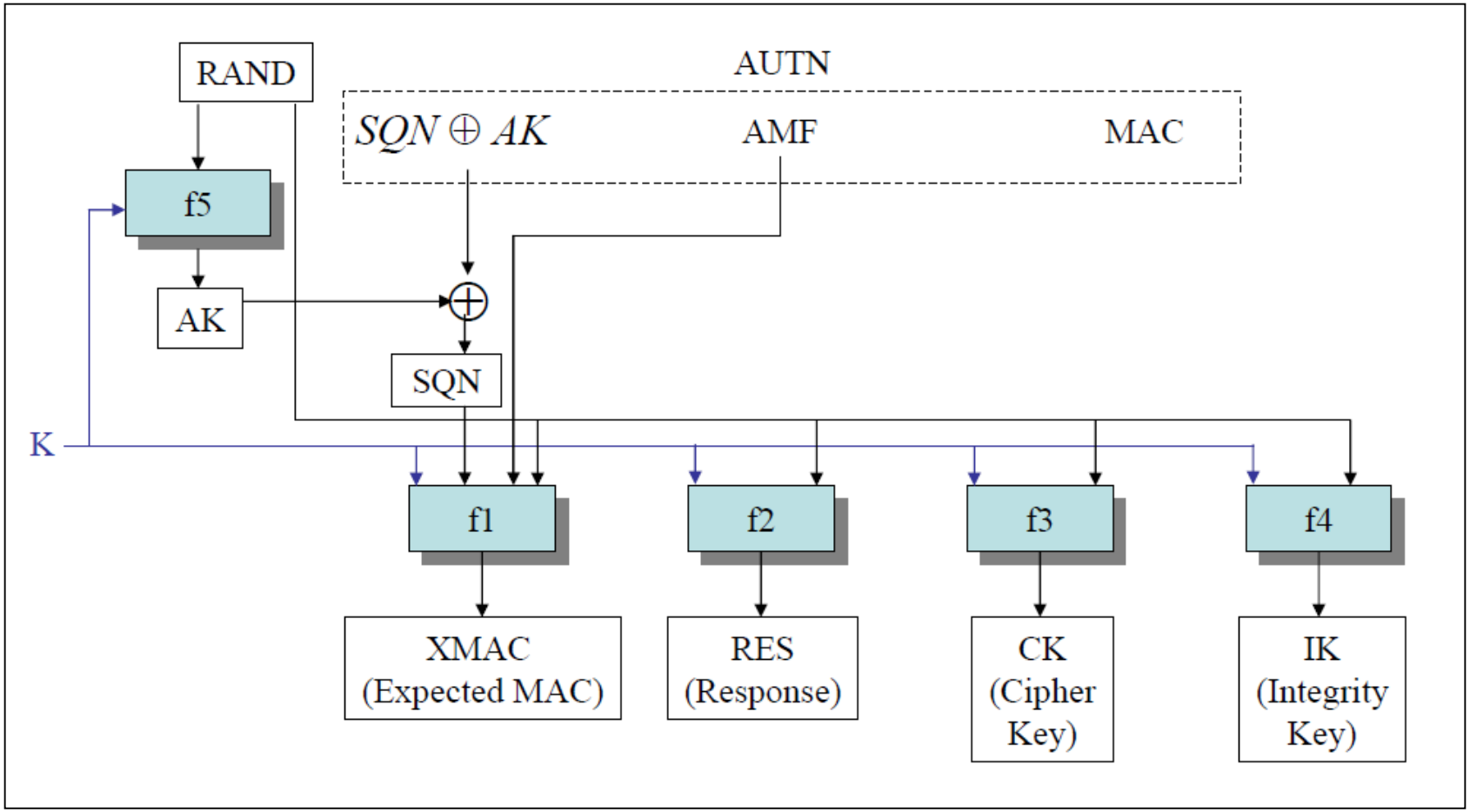
Εικόνα 4.

Παραγωγή ανυσμάτων αυθεντικότητας



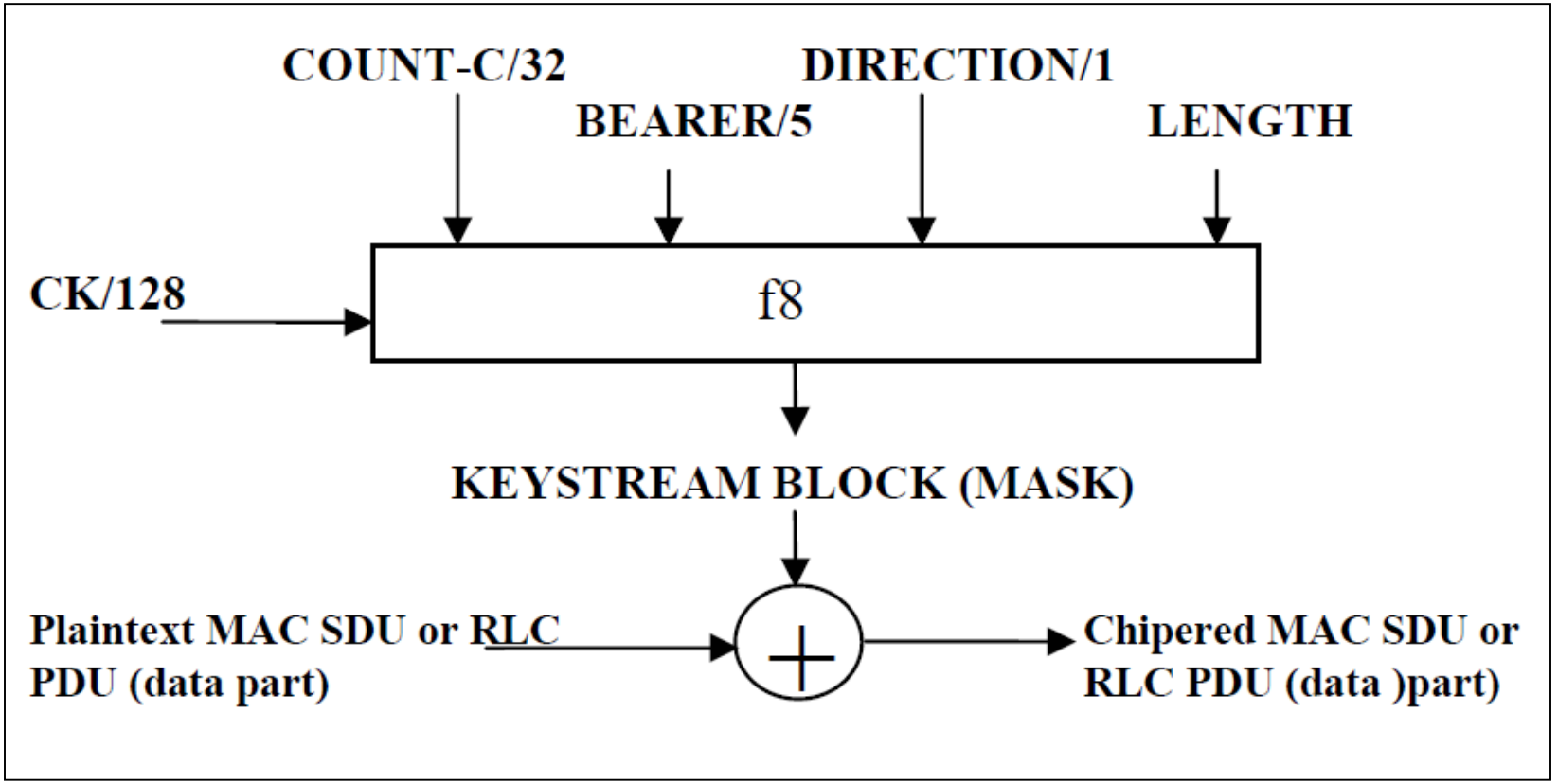
Εικόνα 5.

Επιβεβαίωση AUTN και παραγωγή RES, CK, IK



Εικόνα 6.

Κρυπτογράφηση δεδομένων



Εικόνα 7.

Τέλος Ενότητας

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στο πλαίσιο του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Αθηνών**» έχει χρηματοδοτήσει μόνο την αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Σημειώματα

Σημείωμα Ιστορικού Εκδόσεων Έργου

Το παρόν έργο αποτελεί την έκδοση 1.0.

Έχουν προηγηθεί οι κάτωθι εκδόσεις:

- Έκδοση διαθέσιμη εδώ.

Σημείωμα Αναφοράς

Σημείωμα Αδειοδότησης

Διατήρηση Σημειωμάτων

Οποιαδήποτε αναπαραγωγή ή διασκευή του υλικού θα πρέπει να συμπεριλαμβάνει:

- το Σημείωμα Αναφοράς
- το Σημείωμα Αδειοδότησης
- τη δήλωση Διατήρησης Σημειωμάτων
- το Σημείωμα Χρήσης Έργων Τρίτων (εφόσον υπάρχει)

μαζί με τους συνοδευόμενους υπερσυνδέσμους.

Σημείωμα Χρήσης Έργων Τρίτων

Το Έργο αυτό κάνει χρήση των ακόλουθων έργων:

Εικόνες/Σχήματα/Διαγράμματα/Φωτογραφίες

Εικόνες 1 έως 7: Copyrighted