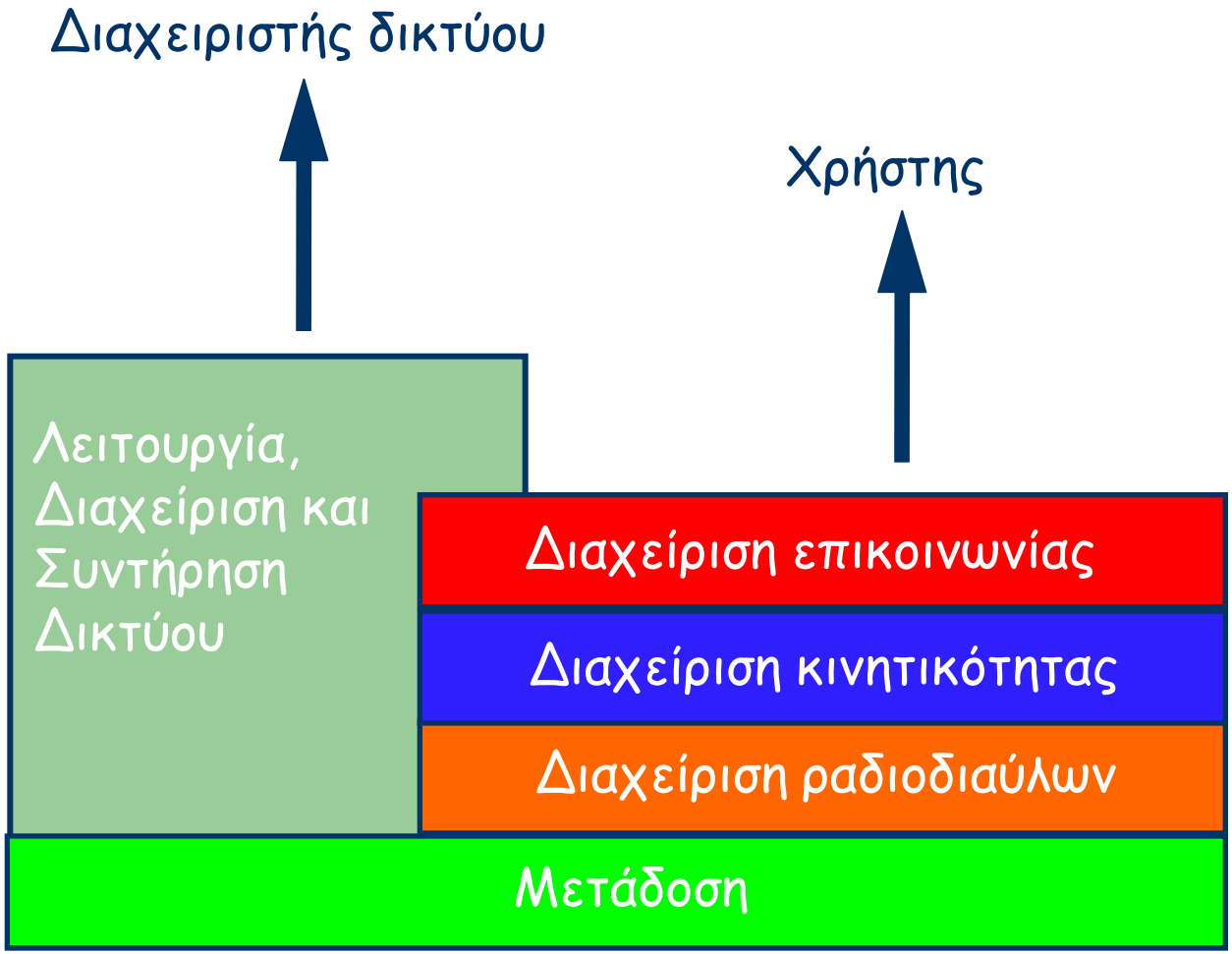
Δίκτυα Κινητών και Προσωπικών Επικοινωνιών

Διαχείριση κινητικότητας

Περίληψη

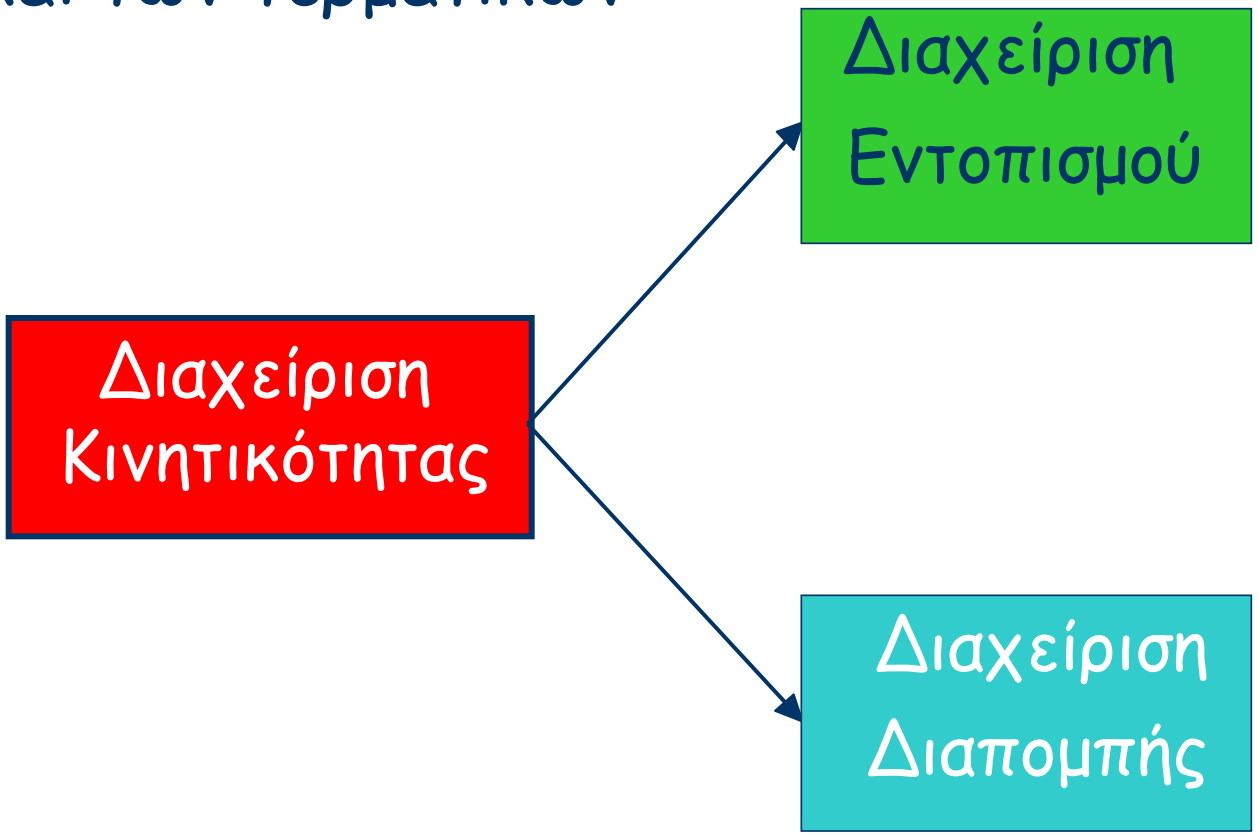
- Διαχείριση εντοπισμού
  - Ενημέρωση θέσης
  - Παράδοση κλήσης
- Διαχείριση εντοπισμού στα επίγεια δίκτυα κινητών επικοινωνιών
- Ενημέρωση θέσης και εντοπισμός δεδομένων
  - Κεντρικές βάσεις δεδομένων
  - Κατανεμημένες βάσεις δεδομένων
- Ενημέρωση θέσης και Αναζήτηση
  - Δυναμικές μέθοδοι ενημέρωσης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

Διαχείριση κινητικότητας



Διαχείριση κινητικότητας

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



Διαχείριση κινητικότητας

Περιλαμβάνει το σύνολο των διαδικασιών που αφορούν:

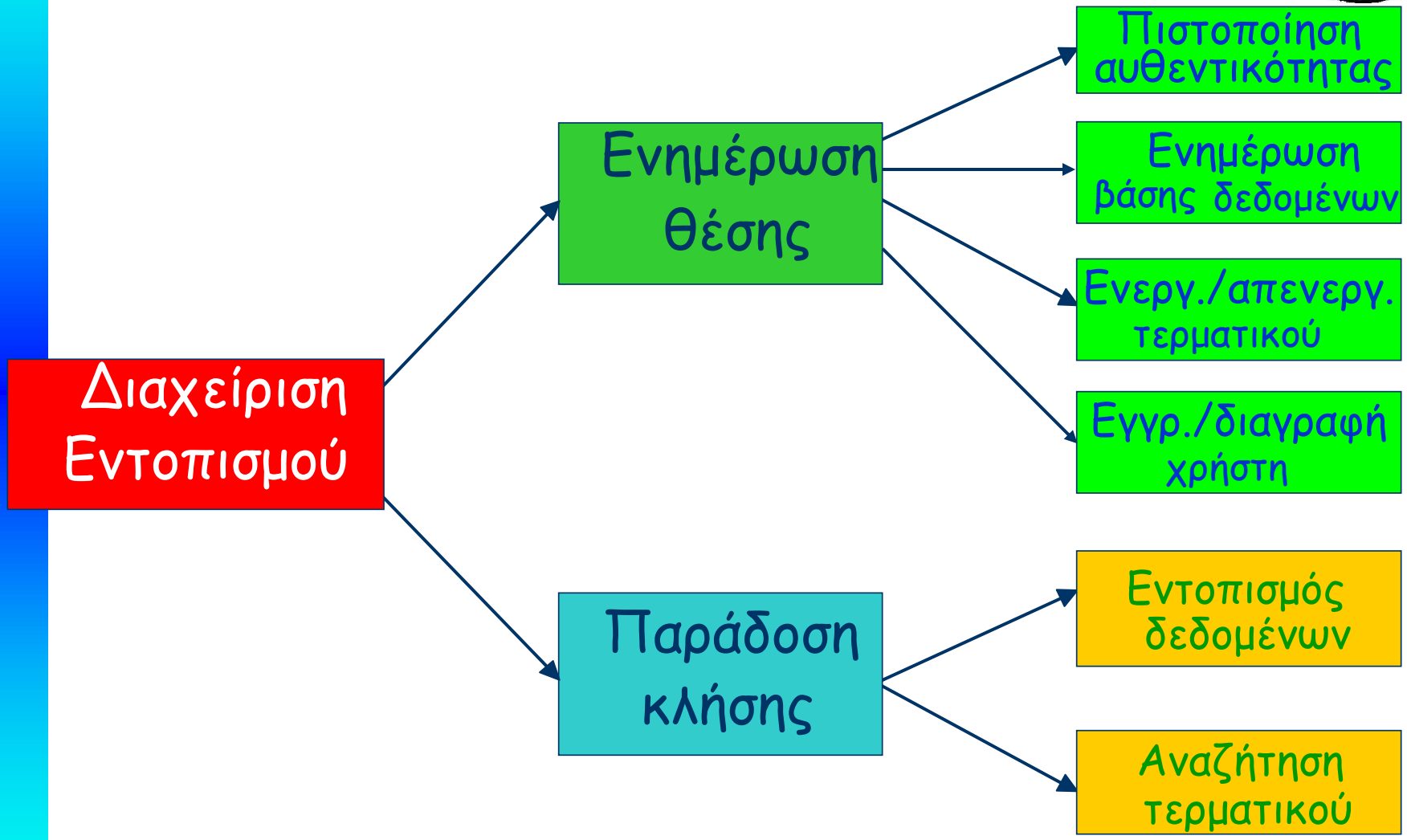
- τη διαχείριση εντοπισμού
  - ενημέρωση του δικτύου για τη θέση και την κατάσταση των κινητών τερματικών (χρηστών)
  - προσδιορισμός της θέσης του καλούμενου για προώθηση της εισερχόμενης κλήσης
- τη διαδικασία της διαπομπής

Διαχείριση εντοπισμού

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



Διαχείριση εντοπισμού

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 δίκτυα 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)

Διαχείριση εντοπισμού στα επίγεια δίκτυα κινητών επικοινωνιών

HLR

- 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)

Διαχείριση εντοπισμού στα επίγεια δίκτυα κινητών επικοινωνιών

HLR

- 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
  - προσωρινές πληροφορίες σχετικές με τις υπηρεσίες που χρησιμοποιεί

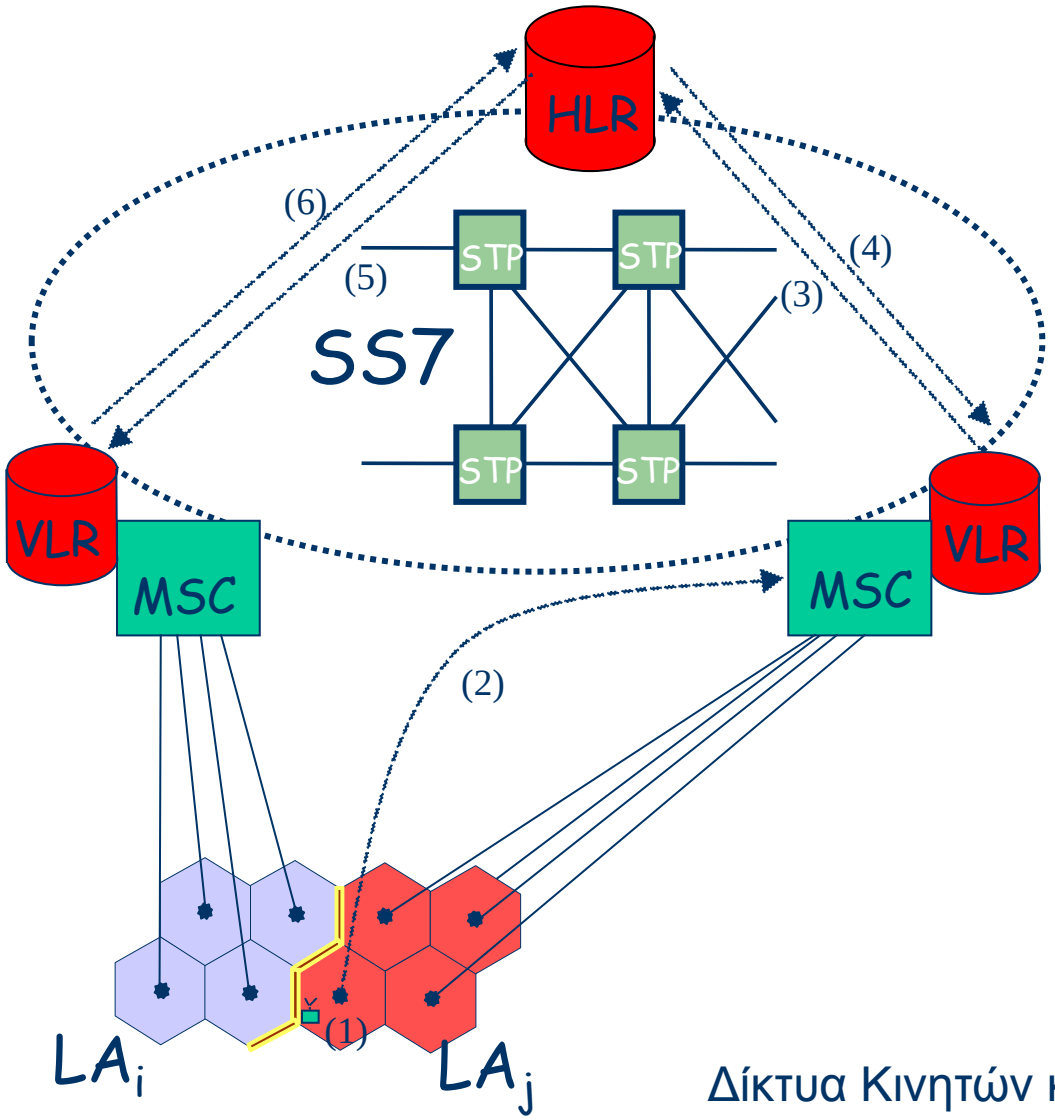
Διαχείριση εντοπισμού στα επίγεια δίκτυα κινητών επικοινωνιών

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*).

Διαχείριση εντοπισμού στα επίγεια δίκτυα κινητών επικοινωνιών

Διαδικασία ενημέρωσης θέσης



Διαχείριση εντοπισμού στα επίγεια δίκτυα κινητών επικοινωνιών

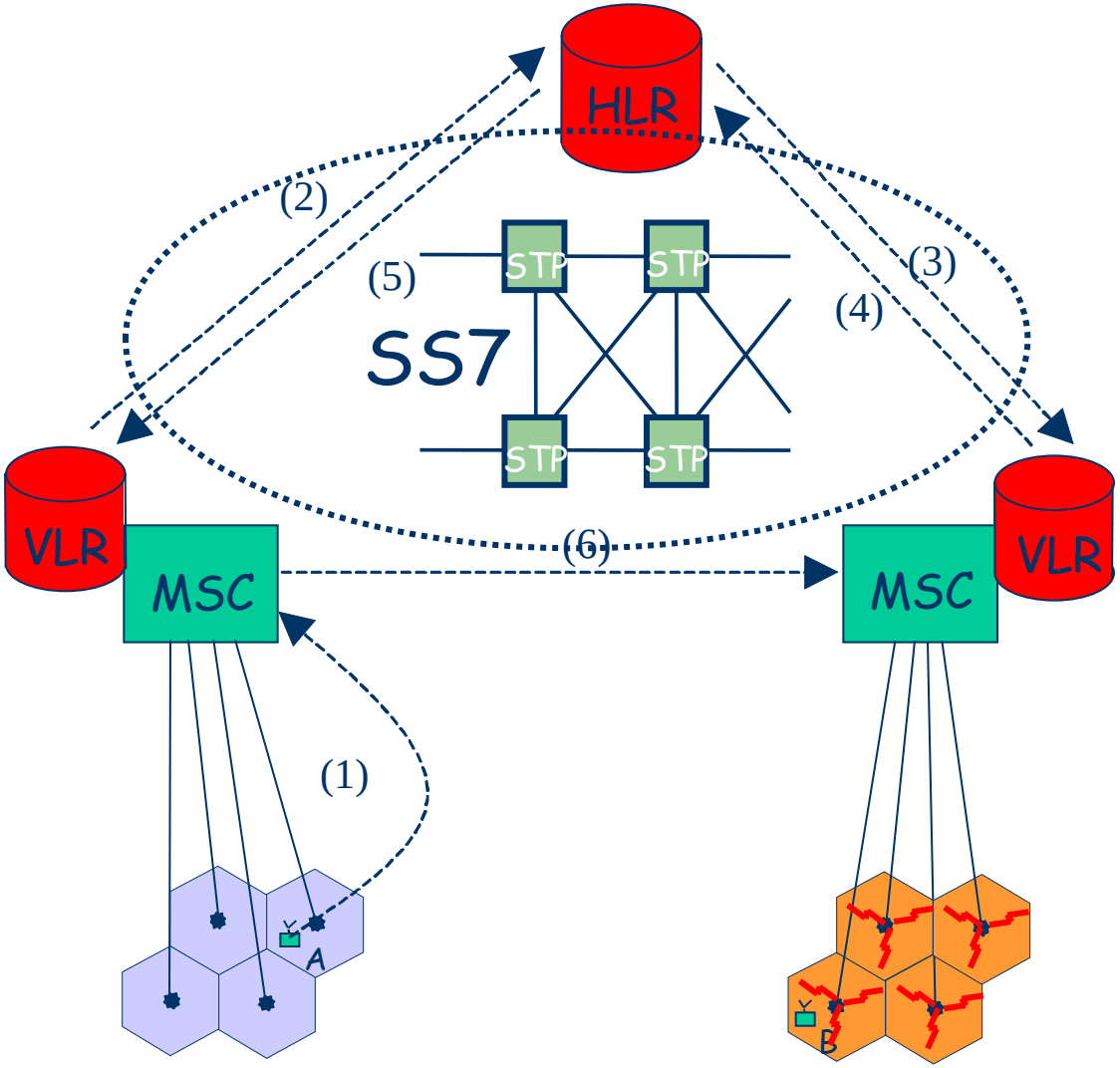
Διαδικασία παράδοσης της κλήσης

- 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).

Διαχείριση εντοπισμού στα επίγεια δίκτυα κινητών επικοινωνιών

Διαδικασία παράδοσης της κλήσης

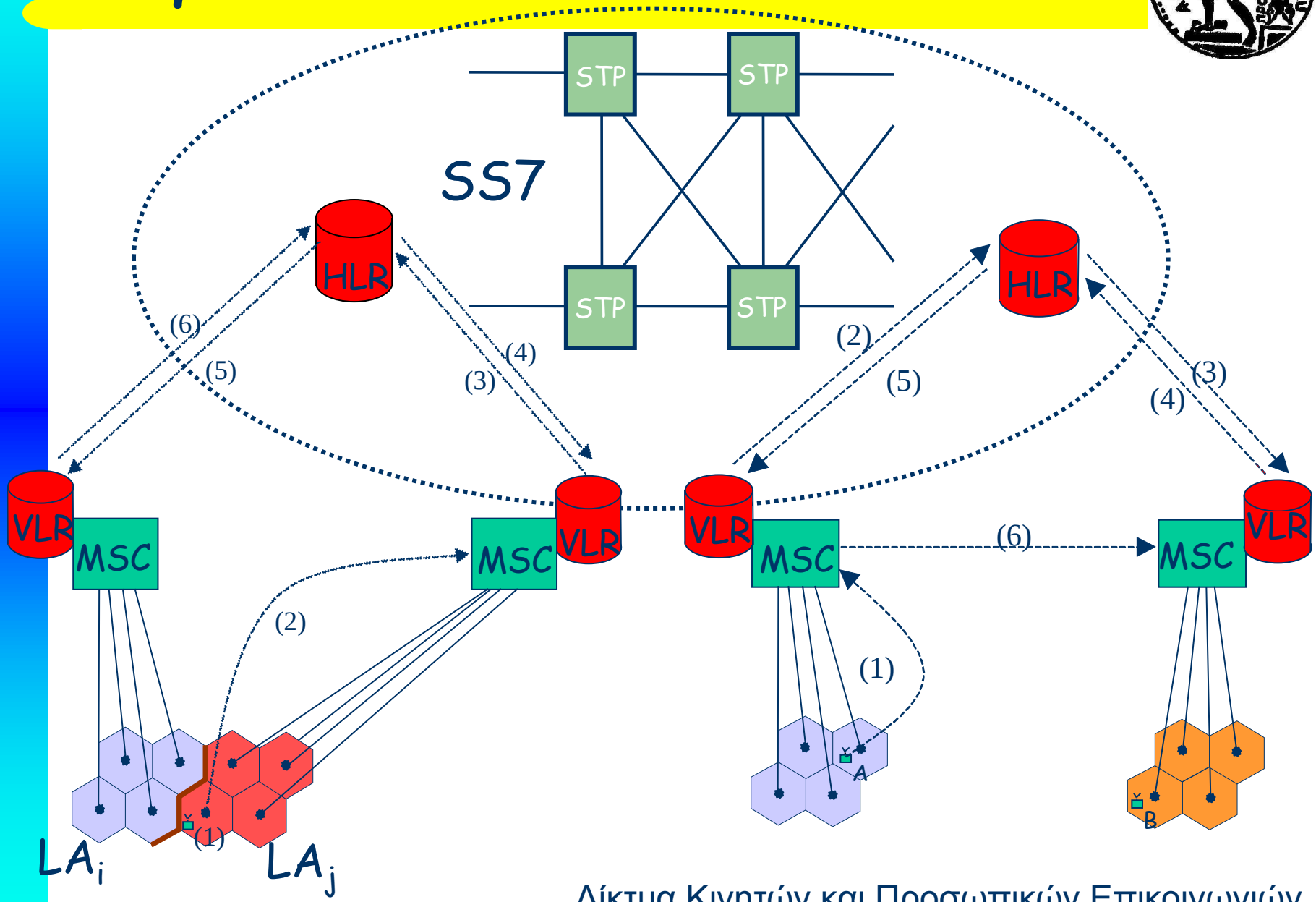


Διαχείριση εντοπισμού στα επίγεια δίκτυα κινητών επικοινωνιών

Διαδικασία παράδοσης της κλήσης

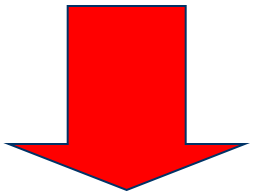
- Ο σχεδιασμός των LA (σχήμα, θέση, διάταξη) και η στρατηγική αναζήτησης στην LA είναι μεγάλης σημασίας, διότι:
  - καθορίζουν τις απαιτήσεις σε σηματοδοσία (διαδικασία ενημέρωσης θέσης, αναζήτηση),
  - επηρεάζουν σημαντικά τον ρυθμό προσβάσεων στη βάση δεδομένων (διαδικασία ενημέρωσης θέσης).
- Ο εντοπισμός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

Ενημέρωση Θέσης και εντοπισμός δεδομένων



Ενημέρωση θέσης και εντοπισμός δεδομένων

- 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

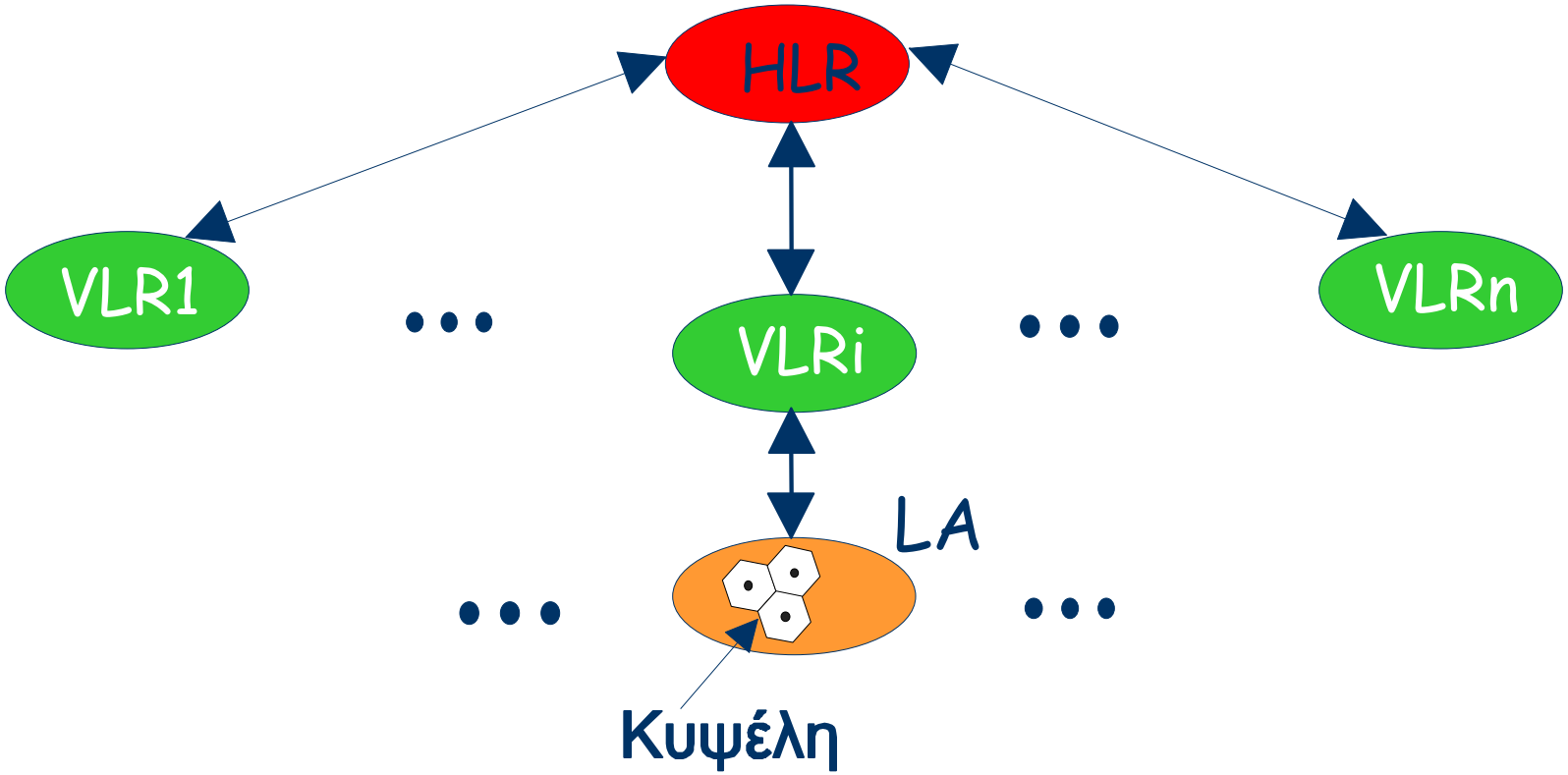
Η έρευνα στην περιοχή αυτή μπορεί γενικά να χωριστεί σε δύο κατηγορίες:

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

Ενημέρωση Θέσης και εντοπισμός δεδομένων

Αρχιτεκτονικές κεντρικών βάσεων δεδομένων

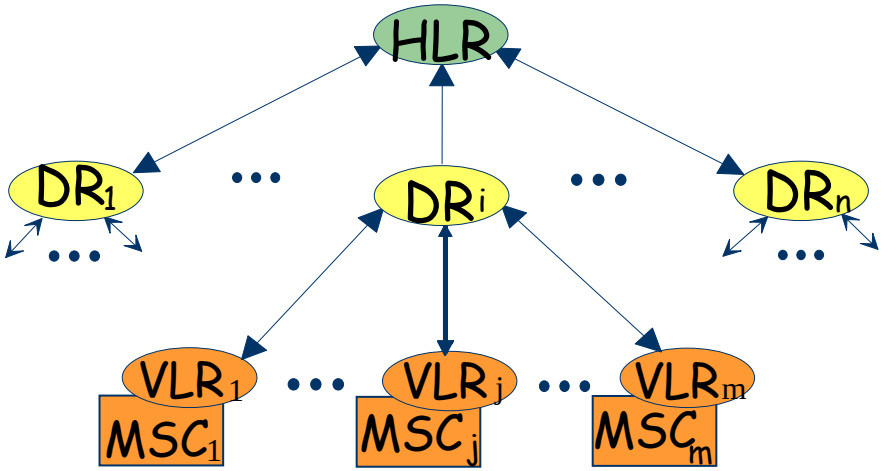
Αναφέρονται στη δομή δυο επιπέδων που εφαρμόζεται στα δίκτυα 2ης γενιάς και στις βελτιώσεις της δομής αυτής, με στόχο τη μείωση του κόστους διαχείρισης εντοπισμού.



Ενημέρωση θέσης και εντοπισμός δεδομένων

Αρχιτεκτονικές κεντρικών βάσεων δεδομένων

Προσθήκη νέου ιεραρχικού επιπέδου: Καταχωρητές καταλόγου (DR)



Ο 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)

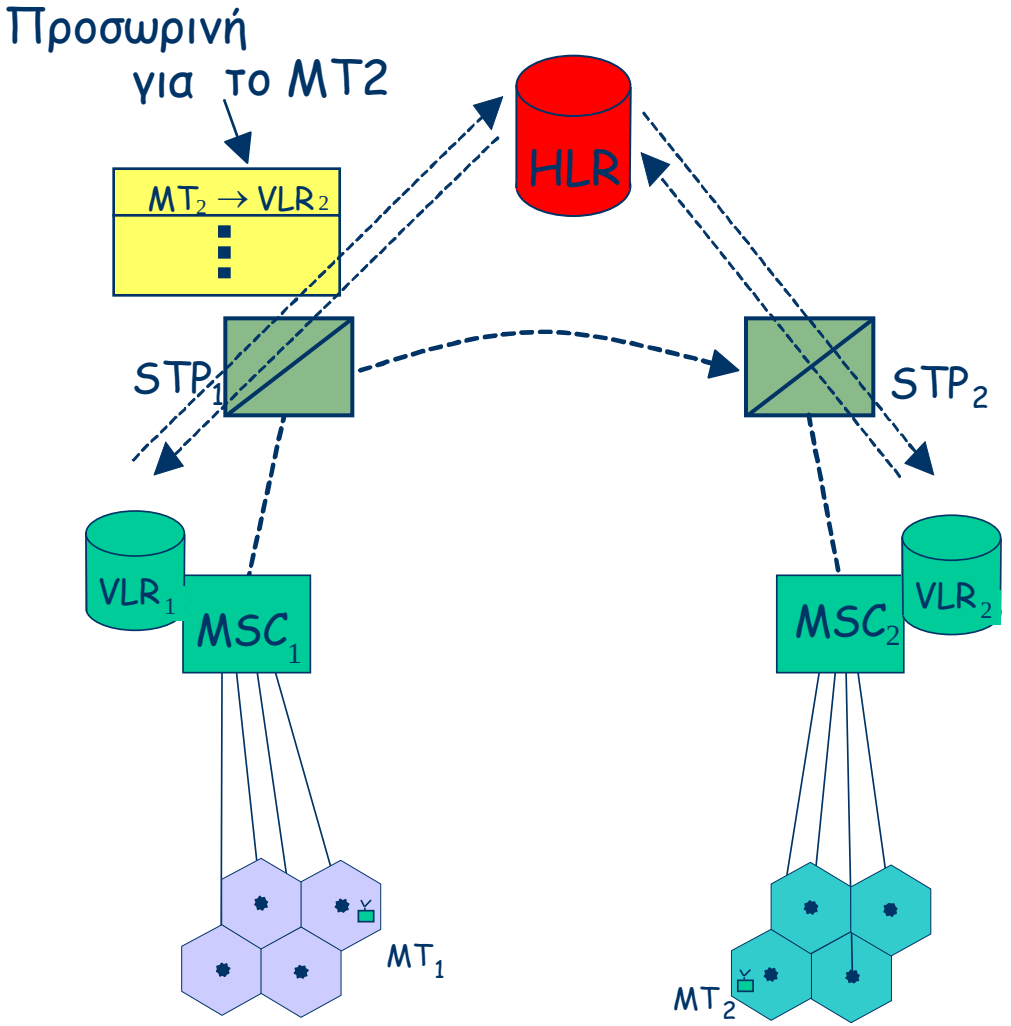
Ο HLR μπορεί να τροποποιηθεί, ώστε να φυλάσσει έναν δείκτη είτε προς τον τρέχοντα DR είτε προς το τρέχον MSC.

Ενημέρωση θέσης και εντοπισμός δεδομένων

Αρχιτεκτονικές κεντρικών βάσεων δεδομένων

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.

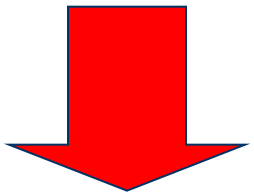


Ενημέρωση θέσης και εντοπισμός δεδομένων

Αρχιτεκτονικές κεντρικών βάσεων δεδομένων

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.

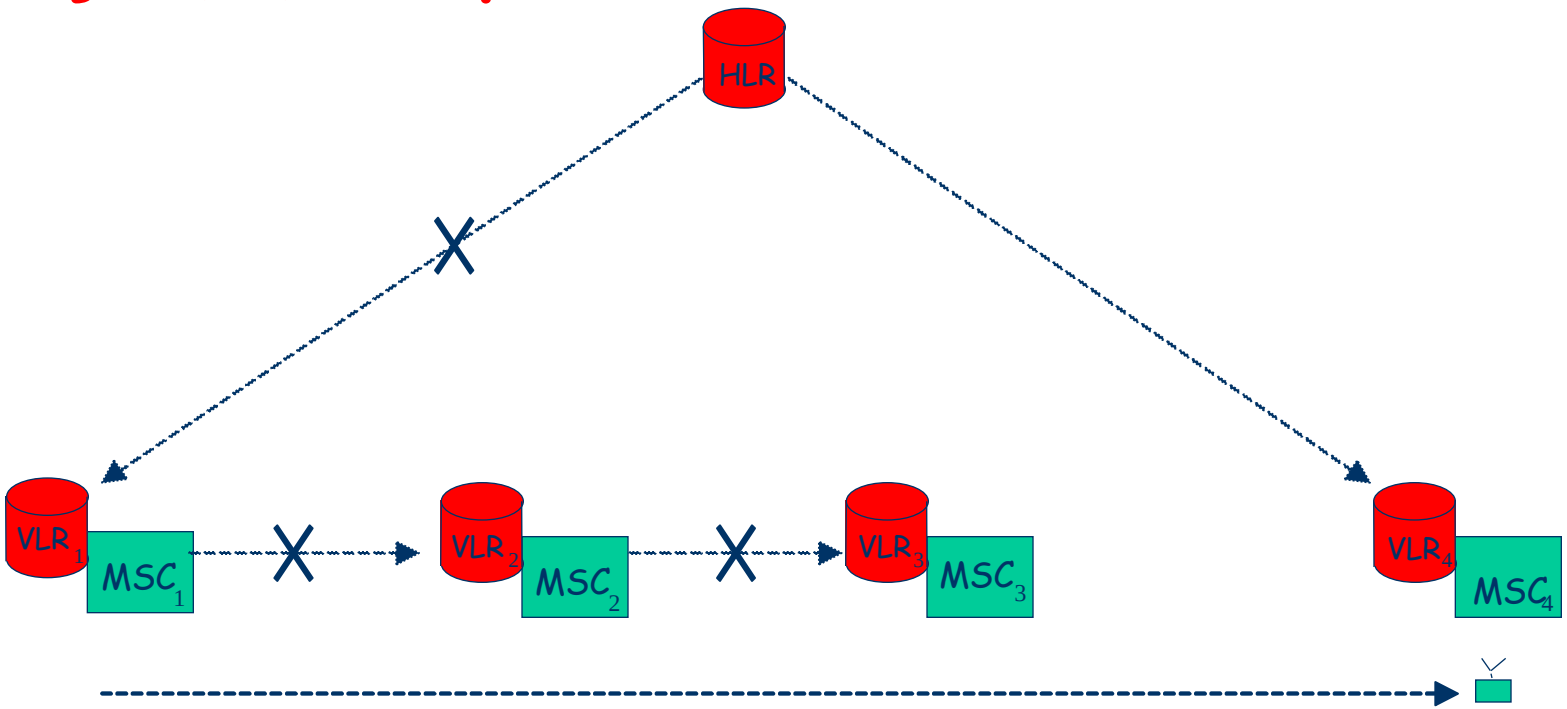


- Μεγαλύτερη σηματοδοσία ενημέρωσης θέσης.
- Μέθοδος καθορισμού επανάληψης προφίλ.

Ενημέρωση θέσης και εντοπισμός δεδομένων

Αρχιτεκτονικές κεντρικών βάσεων δεδομένων

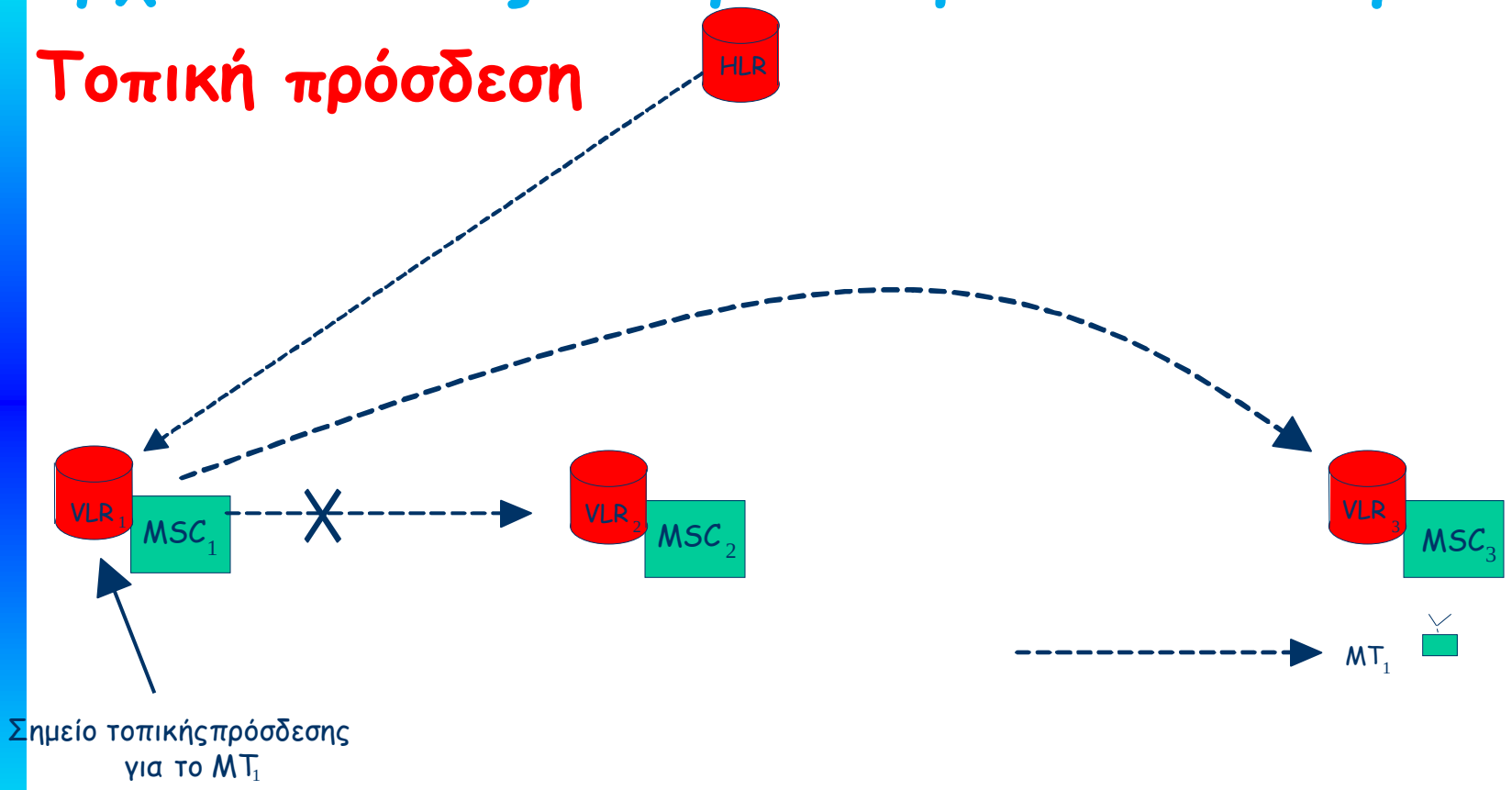
Προώθηση του δείκτη για αναζήτηση δεδομένων



Ενημέρωση θέσης και εντοπισμός δεδομένων

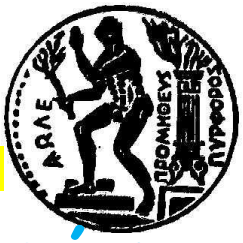
Αρχιτεκτονικές κεντρικών βάσεων δεδομένων

Τοπική πρόσδεση



Στατικό και δυναμικό σημείο πρόσδεσης

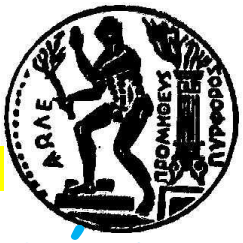
Ενημέρωση θέσης και εντοπισμός δεδομένων



Αρχιτεκτονικές κατανεμημένων βάσεων δεδομένων

- Η κατανεμημένη βάση δεδομένων (Distributed Data Base, DDB) προσφέρει λύσεις:
  - 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)

Ενημέρωση θέσης και εντοπισμός δεδομένων



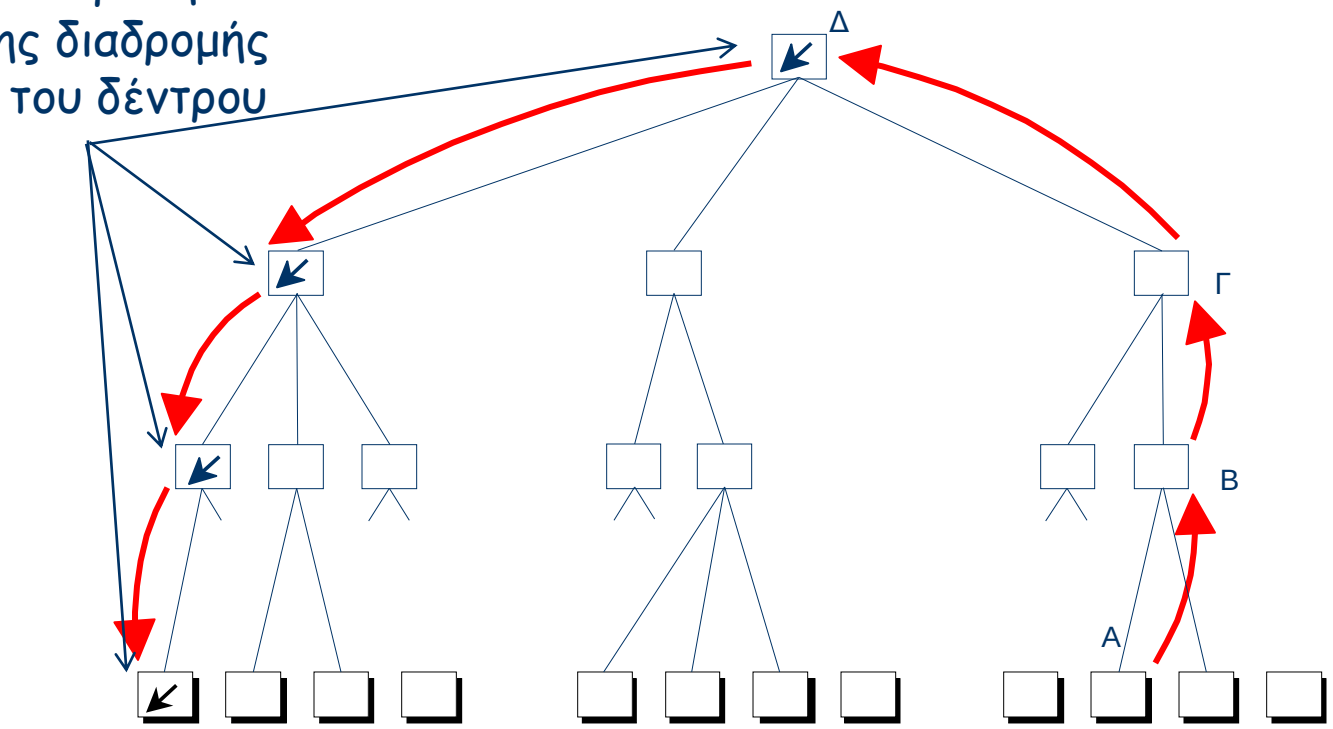
Αρχιτεκτονικές κατανεμημένων βάσεων δεδομένων

- 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

Ενημέρωση θέσης και εντοπισμός δεδομένων

Αρχιτεκτονικές κατανεμημένων βάσεων δεδομένων

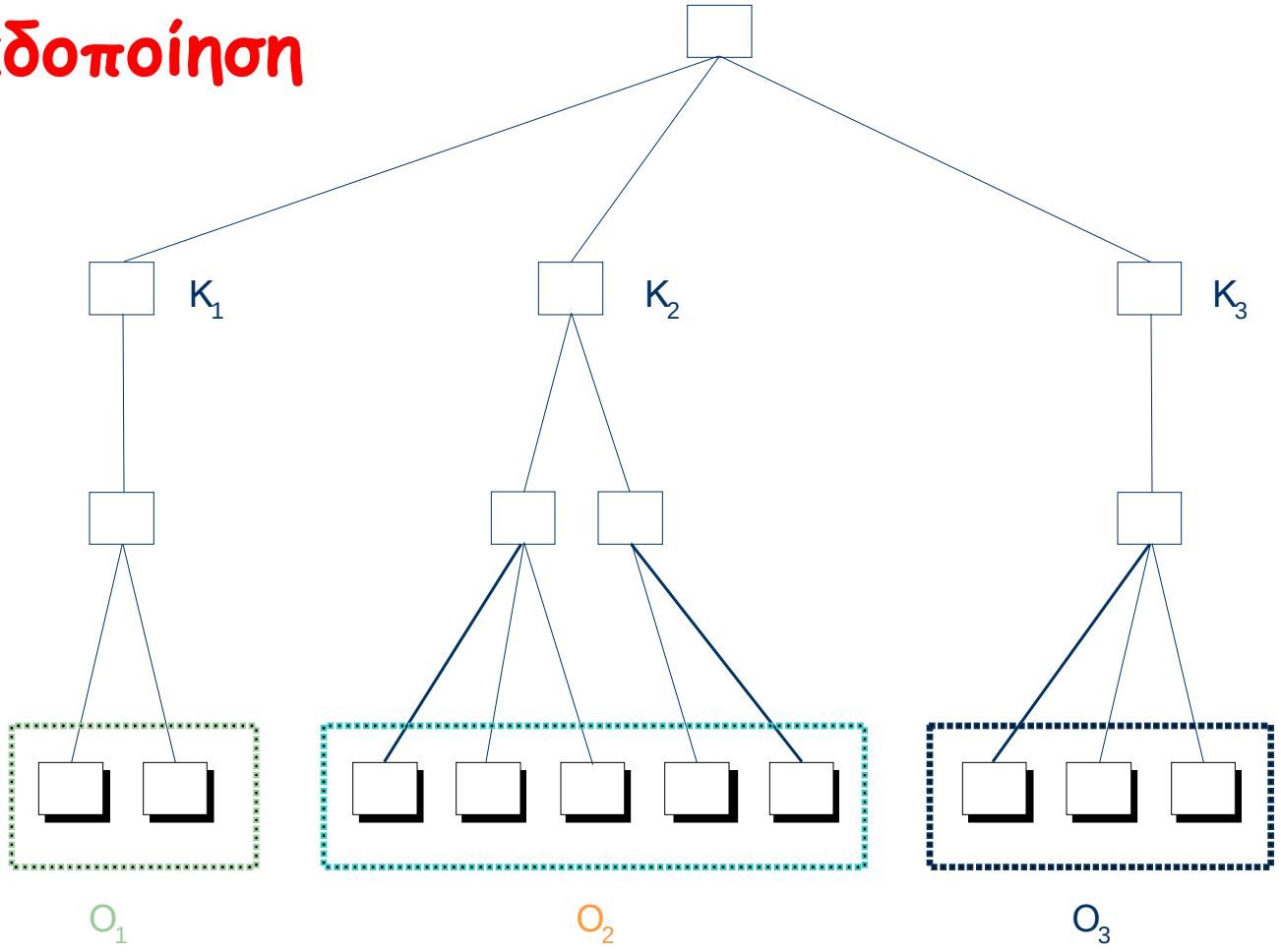
Εγγραφή σε κάθε βάση
κατά μήκος της διαδρομής
μέχρι τη ρίζα του δέντρου



Ενημέρωση θέσης και εντοπισμός δεδομένων

Αρχιτεκτονικές κατανεμημένων βάσεων δεδομένων

Ομαδοποίηση

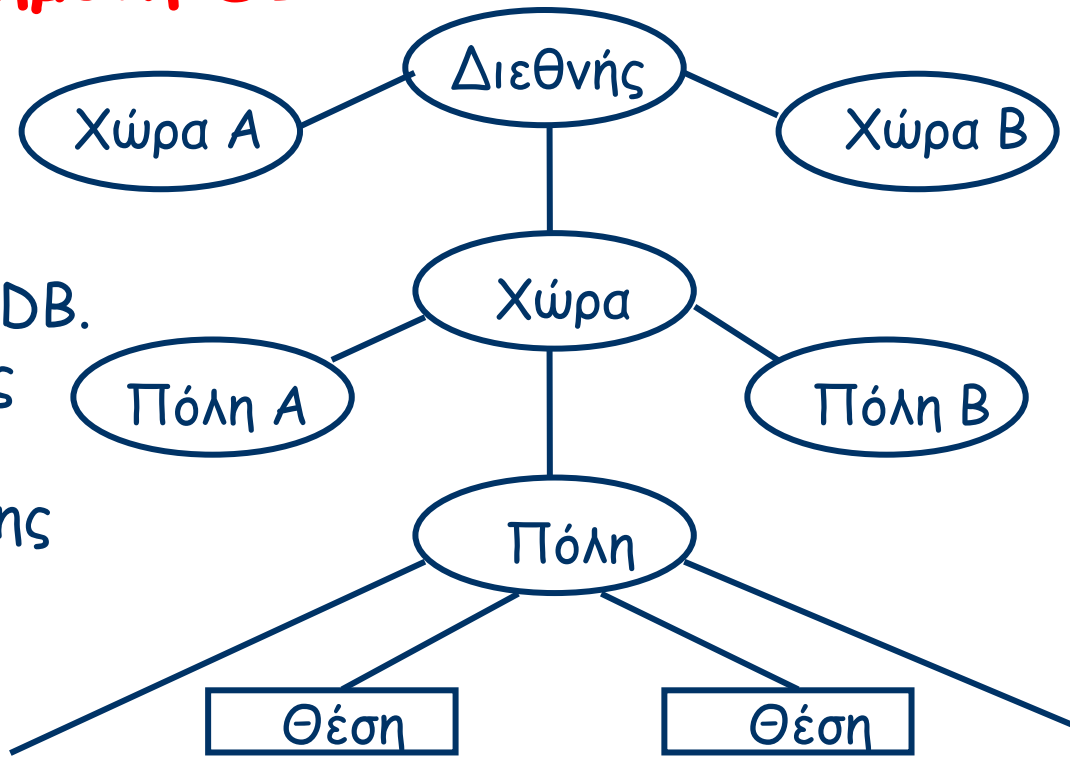


Ενημέρωση θέσης και εντοπισμός δεδομένων

Αρχιτεκτονικές κατανεμημένων βάσεων δεδομένων

Ιεραρχικά κατανεμημένη DB

Στα PCS προτιμάται η ιεραρχικά κατανεμημένη DB. Το σχέδιο αριθμοδότησης του PCS έχει μεγάλη επίδραση στη σχεδίαση της κατανεμημένης DB.



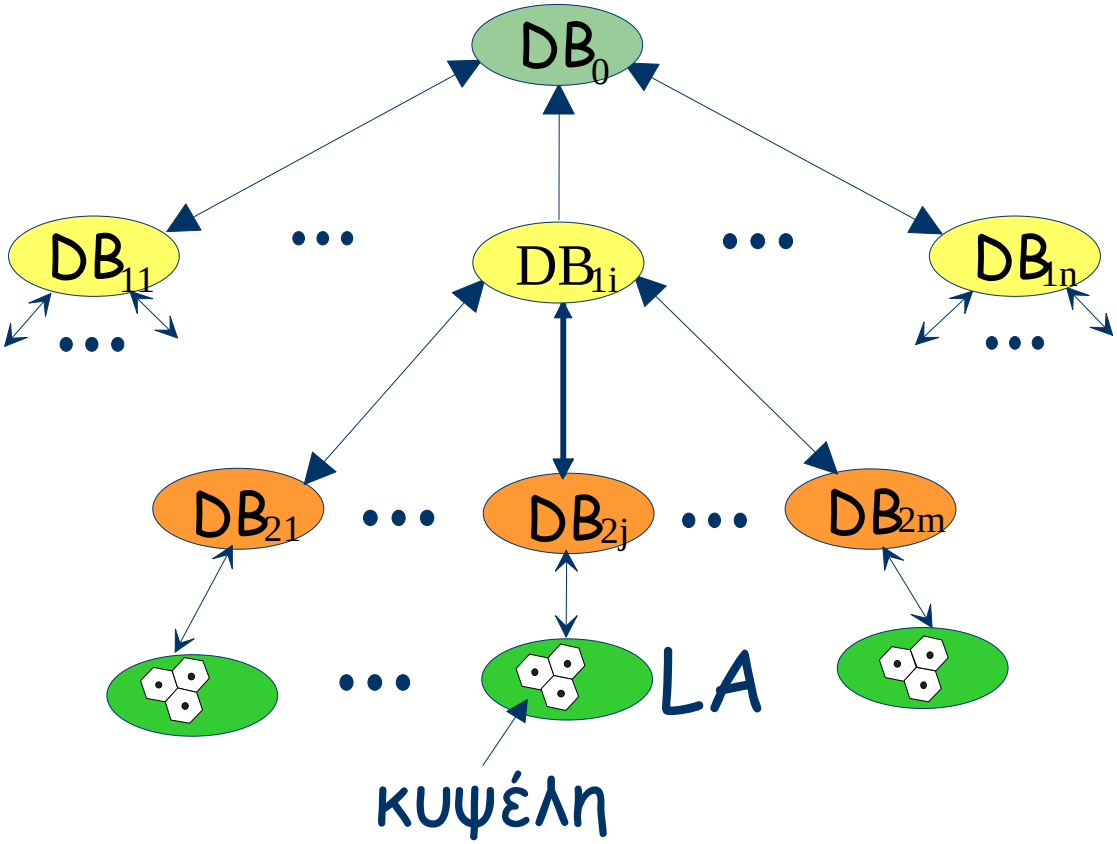
Χώρα	Πόλη	Θέση

Μορφή αριθμού

Ενημέρωση Θέσης και εντοπισμός δεδομένων

Αρχιτεκτονικές κατανεμημένων βάσεων δεδομένων

Ιεραρχική DB με τρία επίπεδα



Ενημέρωση θέσης και εντοπισμός δεδομένων

Στρατηγικές εντοπισμού δεδομένων στην DDB

- 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).

Ενημέρωση θέσης και εντοπισμός δεδομένων

Στρατηγικές εντοπισμού δεδομένων στην DDB

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

Ενημέρωση θέσης και εντοπισμός δεδομένων

Στρατηγικές εντοπισμού δεδομένων στην DDB

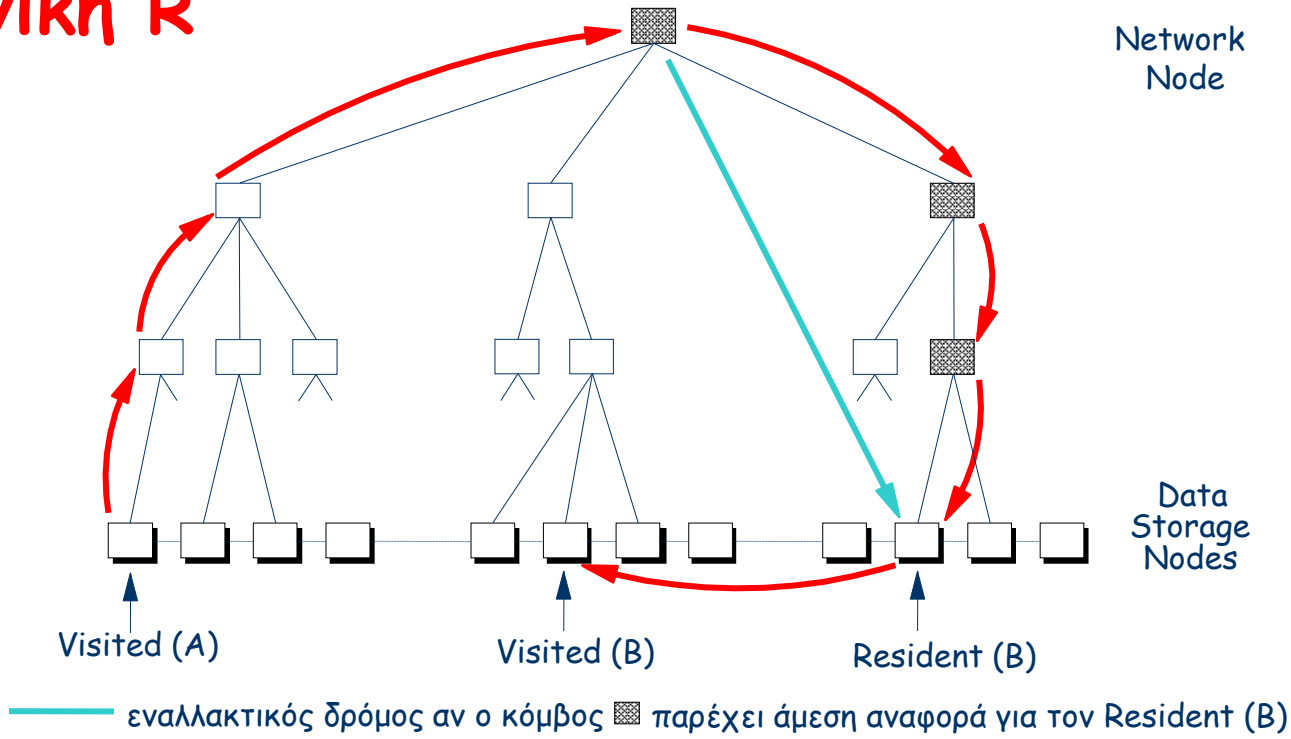
Από την πλευρά του παρόχου δικτύου, μια αποτελεσματική στρατηγική εντοπισμού δεδομένων πρέπει να έχει τα εξής χαρακτηριστικά:

- 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

Ενημέρωση θέσης και εντοπισμός δεδομένων

Στρατηγικές εντοπισμού δεδομένων στην DDB

Στρατηγική R

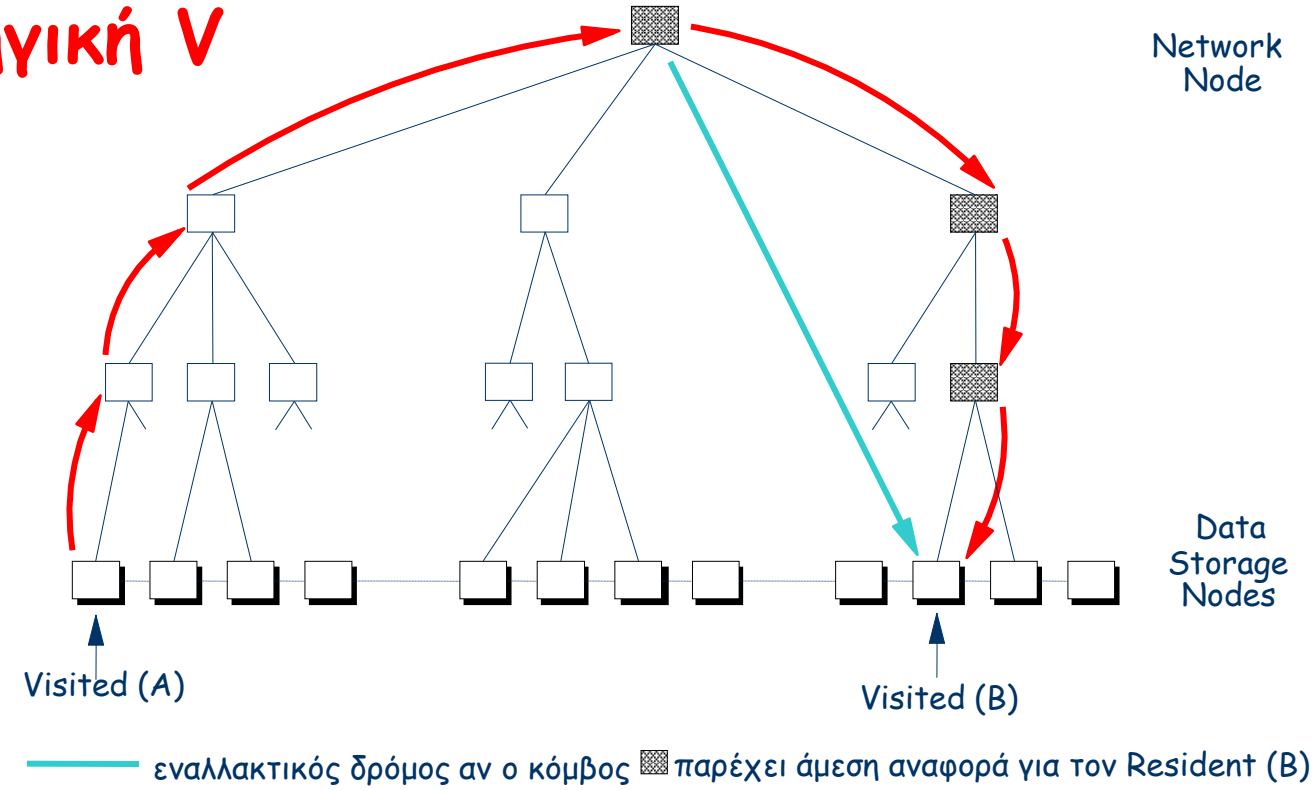


+ απλοί κανόνες
- μεγάλοι βρόχοι
- οικείος κόμβος εκτός ⇒ οικείοι χρήστες εκτός

Ενημέρωση θέσης και εντοπισμός δεδομένων

Στρατηγικές εντοπισμού δεδομένων στην DDB

Στρατηγική V

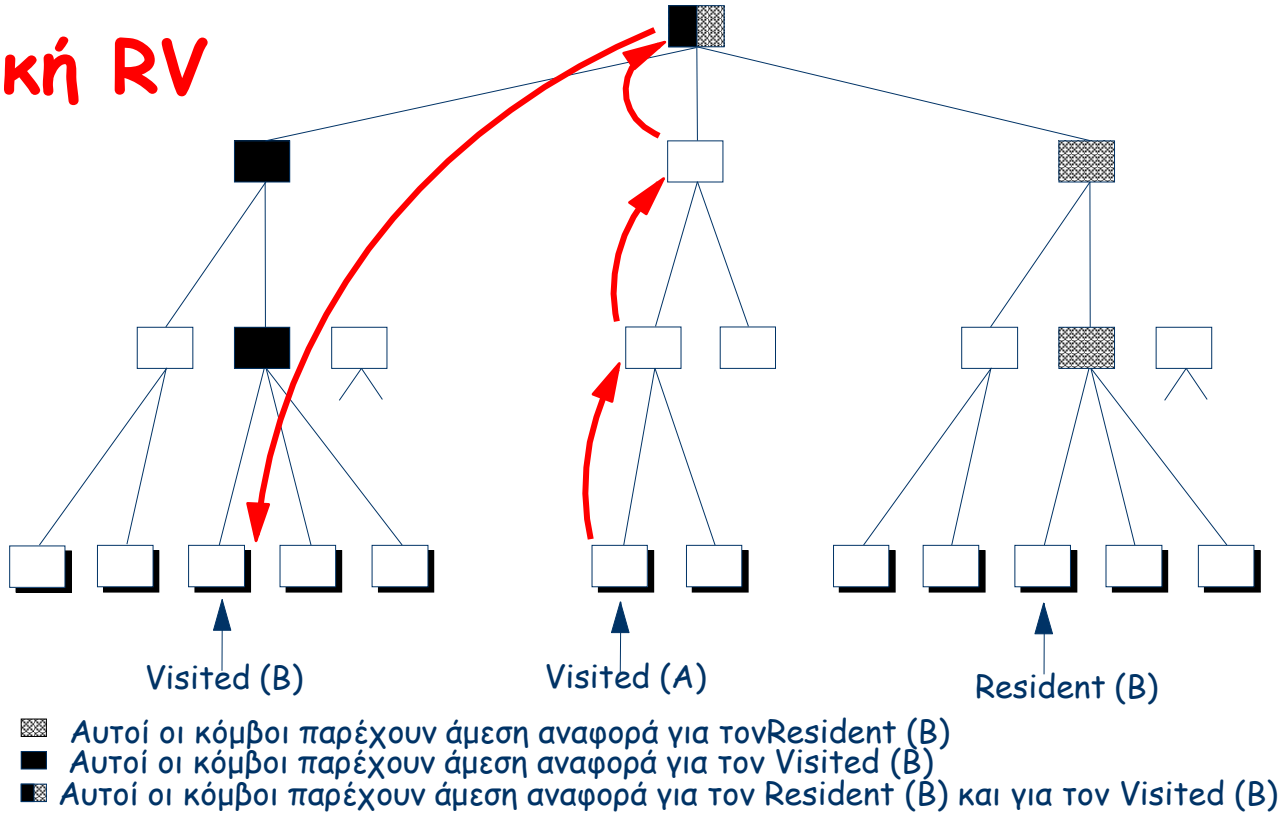


+ υποστηρίζει τοπικότητα, όχι μεγάλοι βρόχοι
- καθυστέρηση
- αναποτελεσματική χρήση των ISN

Ενημέρωση Θέσης και εντοπισμός δεδομένων

Στρατηγικές εντοπισμού δεδομένων στην DDB

Στρατηγική RV

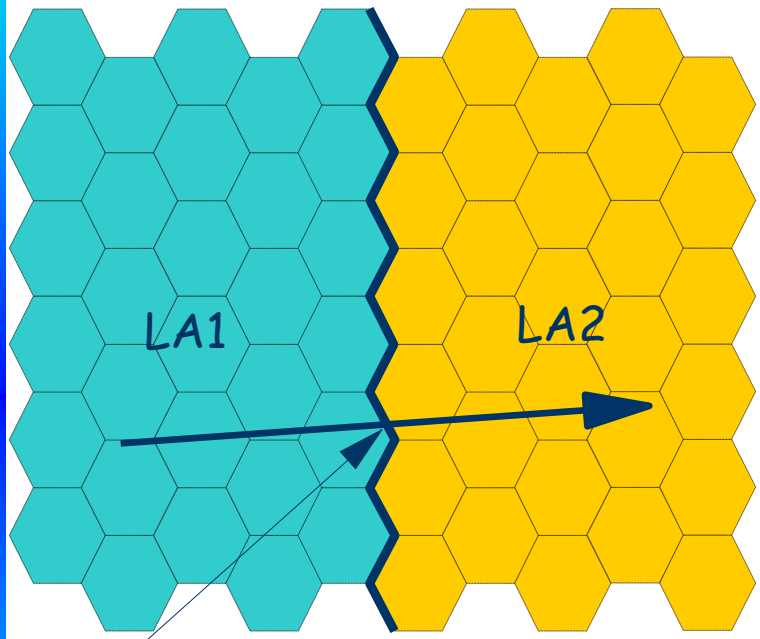


+ υποστηρίζει τοπικότητα
+ λιγότερες ανεπιτυχείς αναζητήσεις στους ISN
- μεγαλύτερος χώρος αποθήκευσης

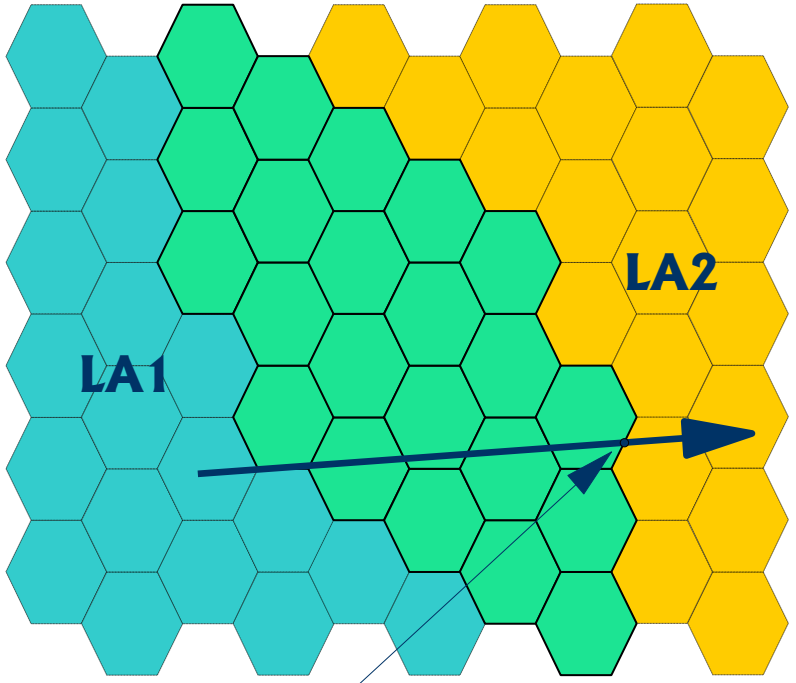
Ενημέρωση θέσης και αναζήτηση

- 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.

Ενημέρωση θέσης και αναζήτηση

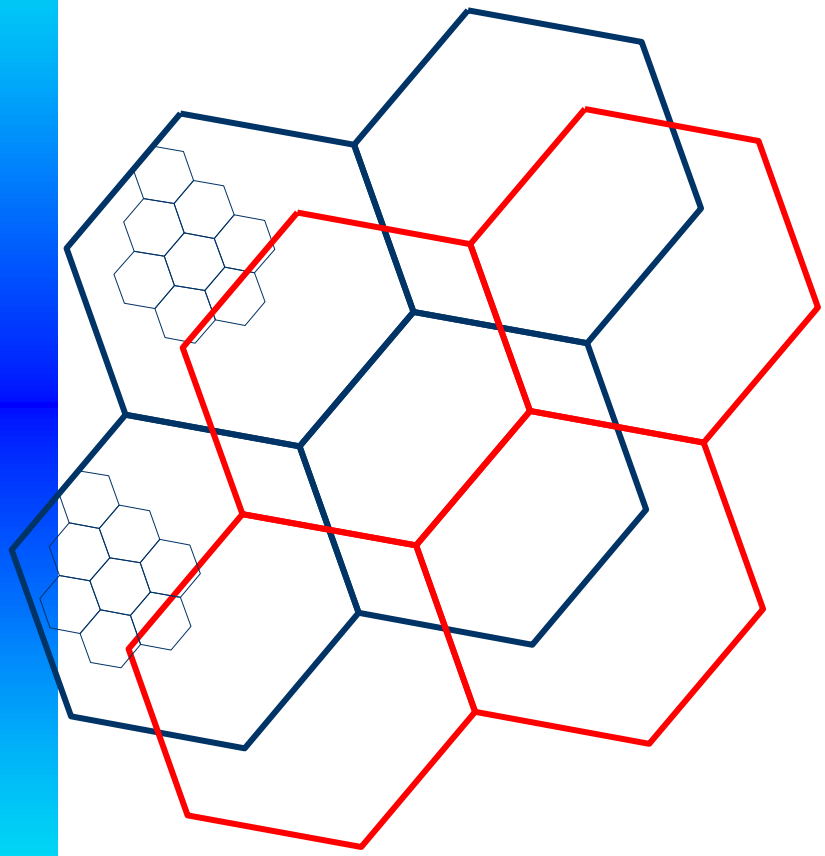


Ενημέρωση θέσης θα γίνει εδώ



Ενημέρωση θέσης θα γίνει εδώ

Ενημέρωση θέσης και αναζήτηση



LA ομάδας 1

LA ομάδας 2

Ενημέρωση θέσης και αναζήτηση

- 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.

     ⇓

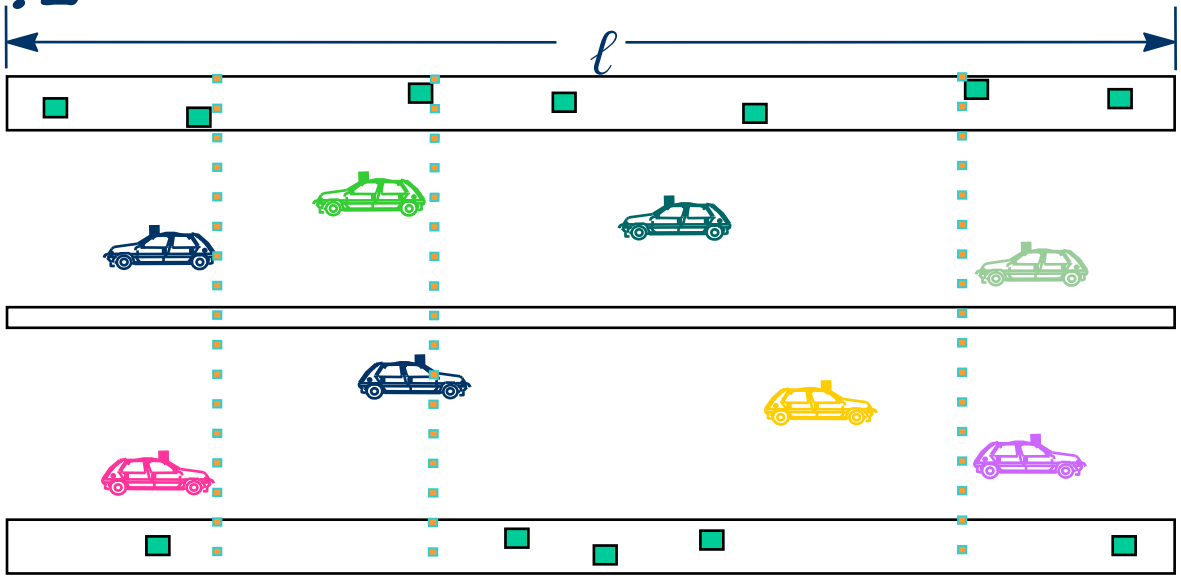
     Κατάλληλος σχεδιασμός των περιοχών εντοπισμού και αναζήτησης, περίτεχνες τεχνικές ενημέρωσης θέσης και αναζήτησης.
  2. Το πλήθος διεργασιών με τη βάση δεδομένων, που πραγματοποιείται κατά την ενημέρωση θέσης και την αναζήτηση.

     ⇓

     Κατανεμημένες βάσεις δεδομένων.

Ενημέρωση θέσης και αναζήτηση

Παράδειγμα 10.2



L: αριθμός LA

ρ(x): γραμμική πυκνότητα χρηστών

q(x): ρυθμός διελεύσεων από το όριο x

Να βρεθούν τα όρια των περιοχών αναζήτησης, ώστε να ελαχιστοποιείται το κόστος του φορτίου αναζήτησης και ενημέρωσης θέσης.

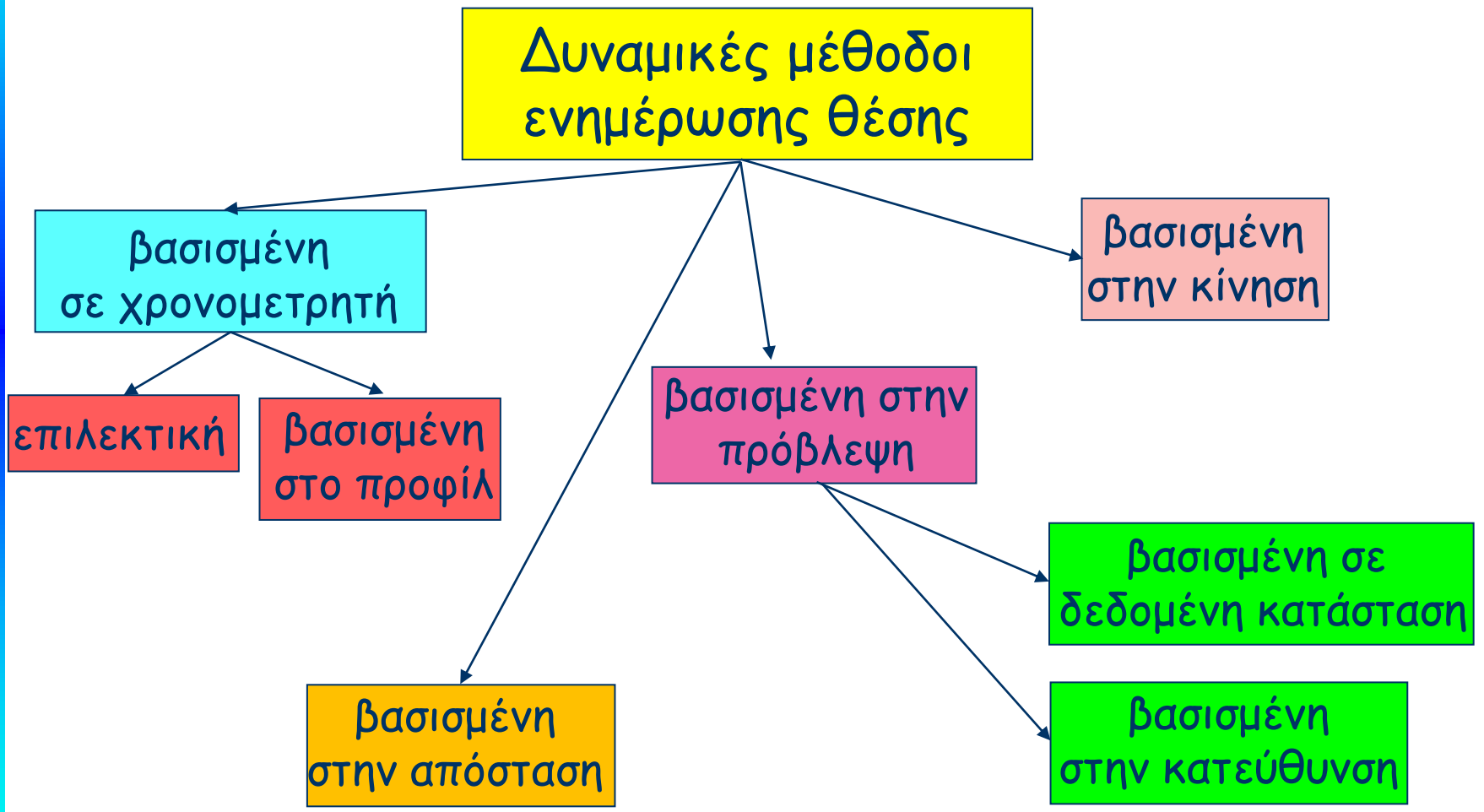
Ενημέρωση θέσης και αναζήτηση

Δυναμικές μέθοδοι ενημέρωσης θέσης

- 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*

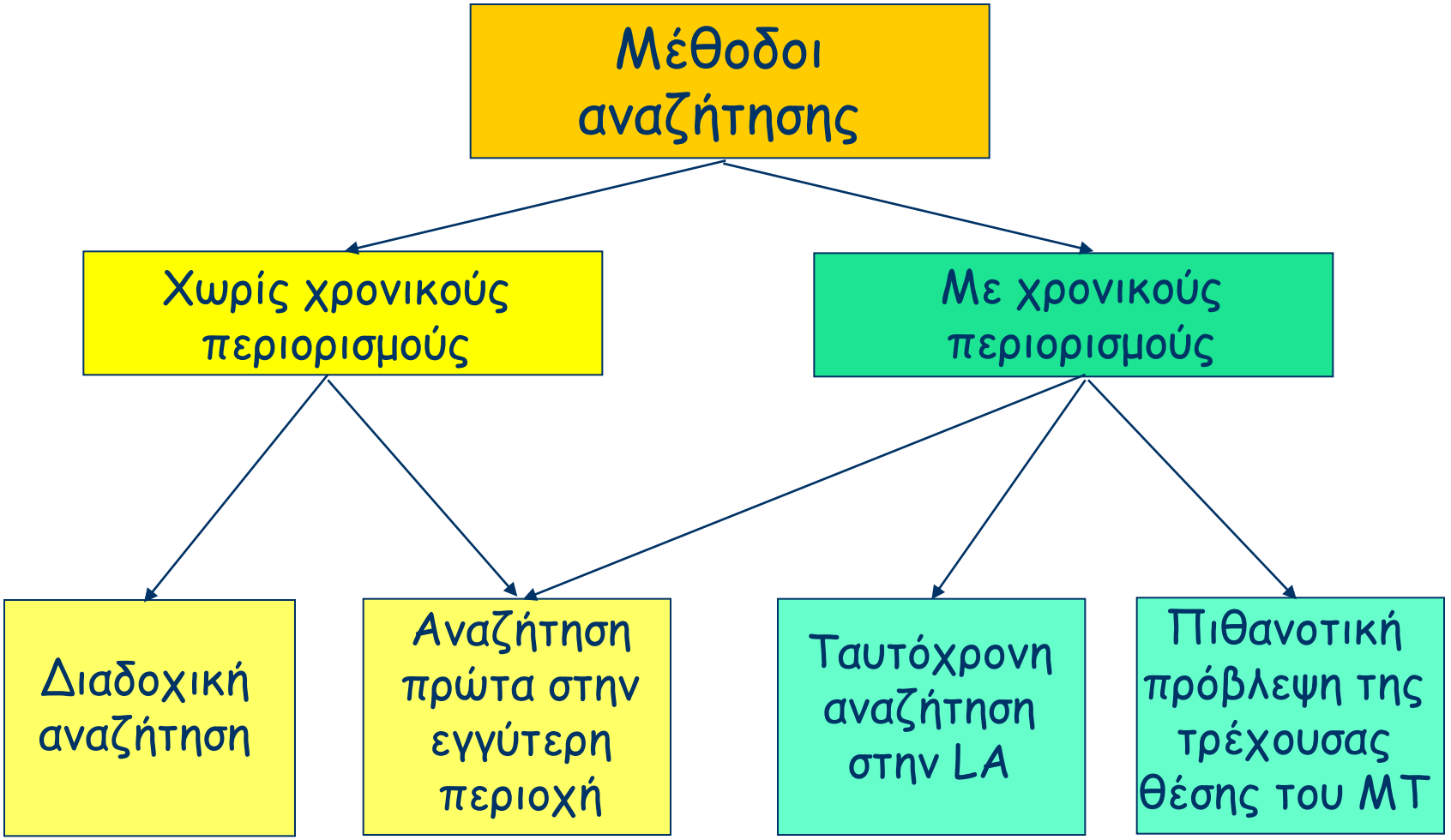
Ενημέρωση θέσης και αναζήτηση

Δυναμικές μέθοδοι ενημέρωσης θέσης



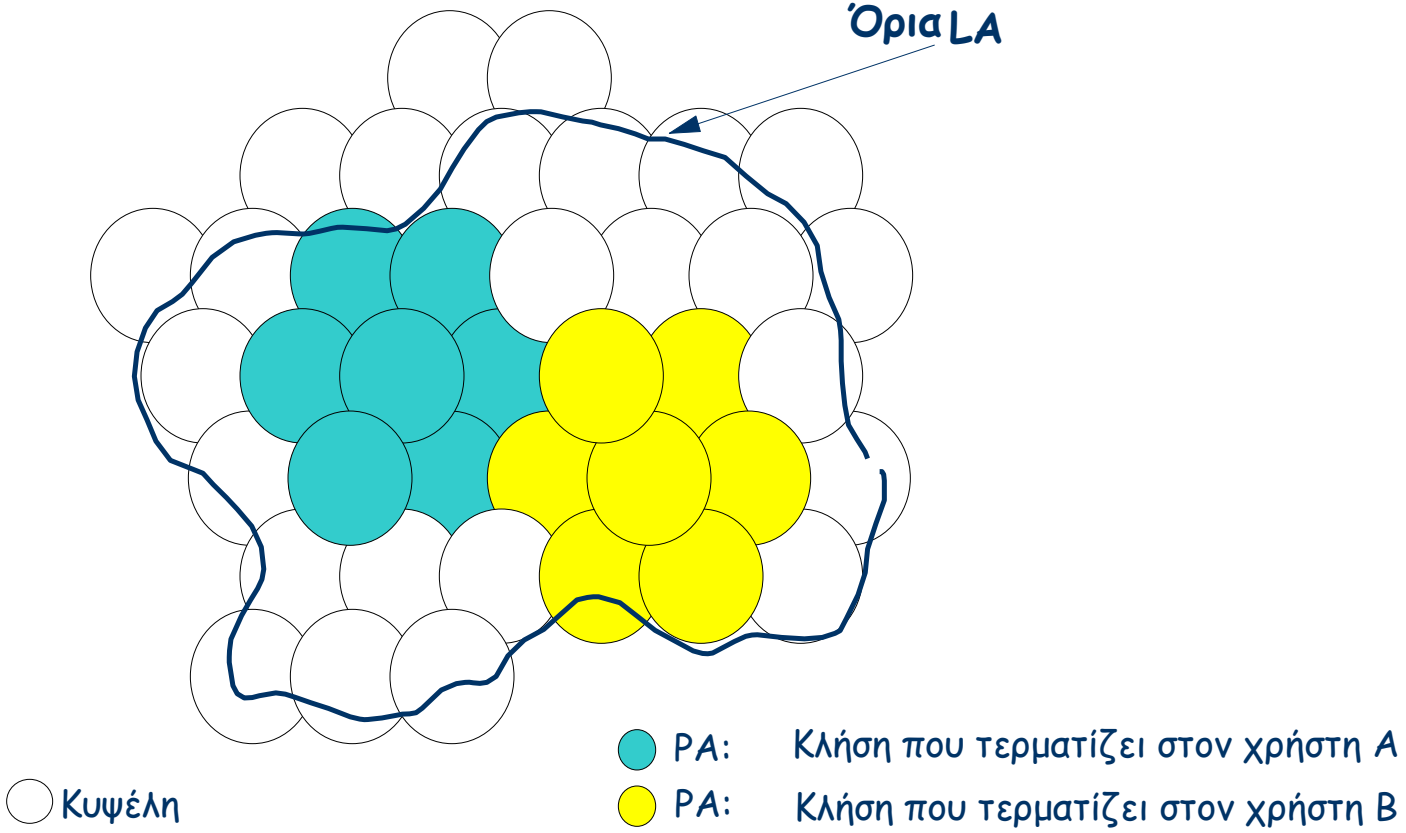
Ενημέρωση θέσης και αναζήτηση

Μέθοδοι αναζήτησης

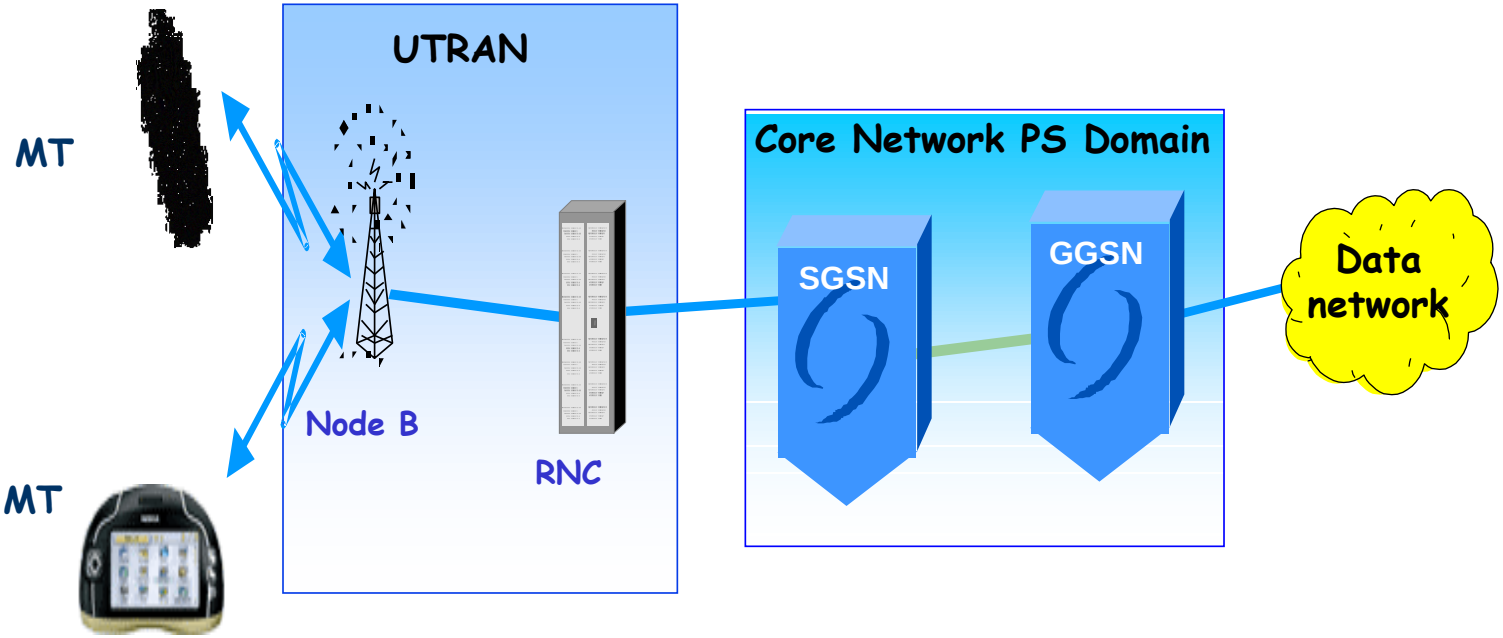


Ενημέρωση θέσης και αναζήτηση

Ευφυής αναζήτηση



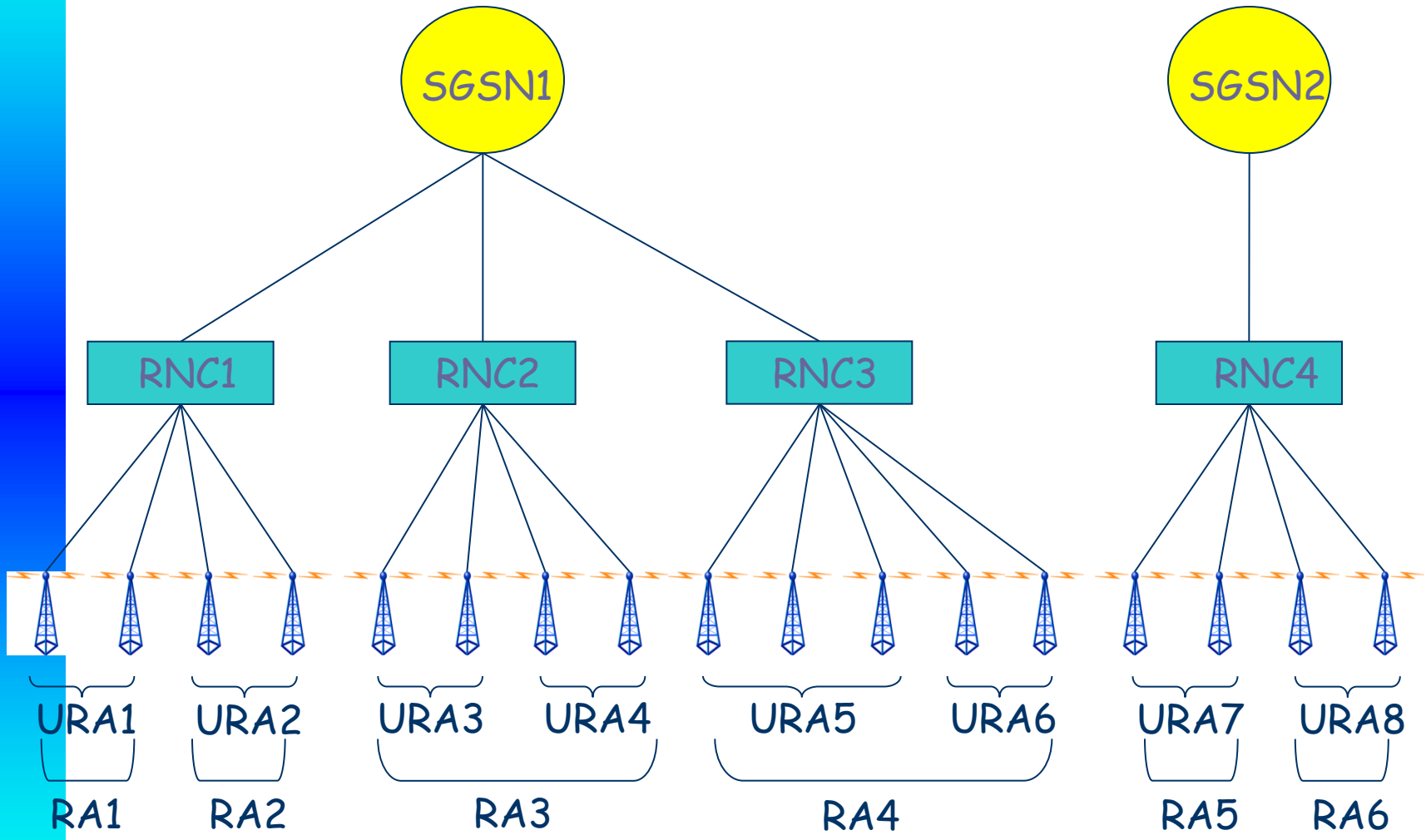
Διαχείριση εντοπισμού στο UMTS



Node B: Base station
RNC: Radio Network Controller
MT: Mobile Terminal

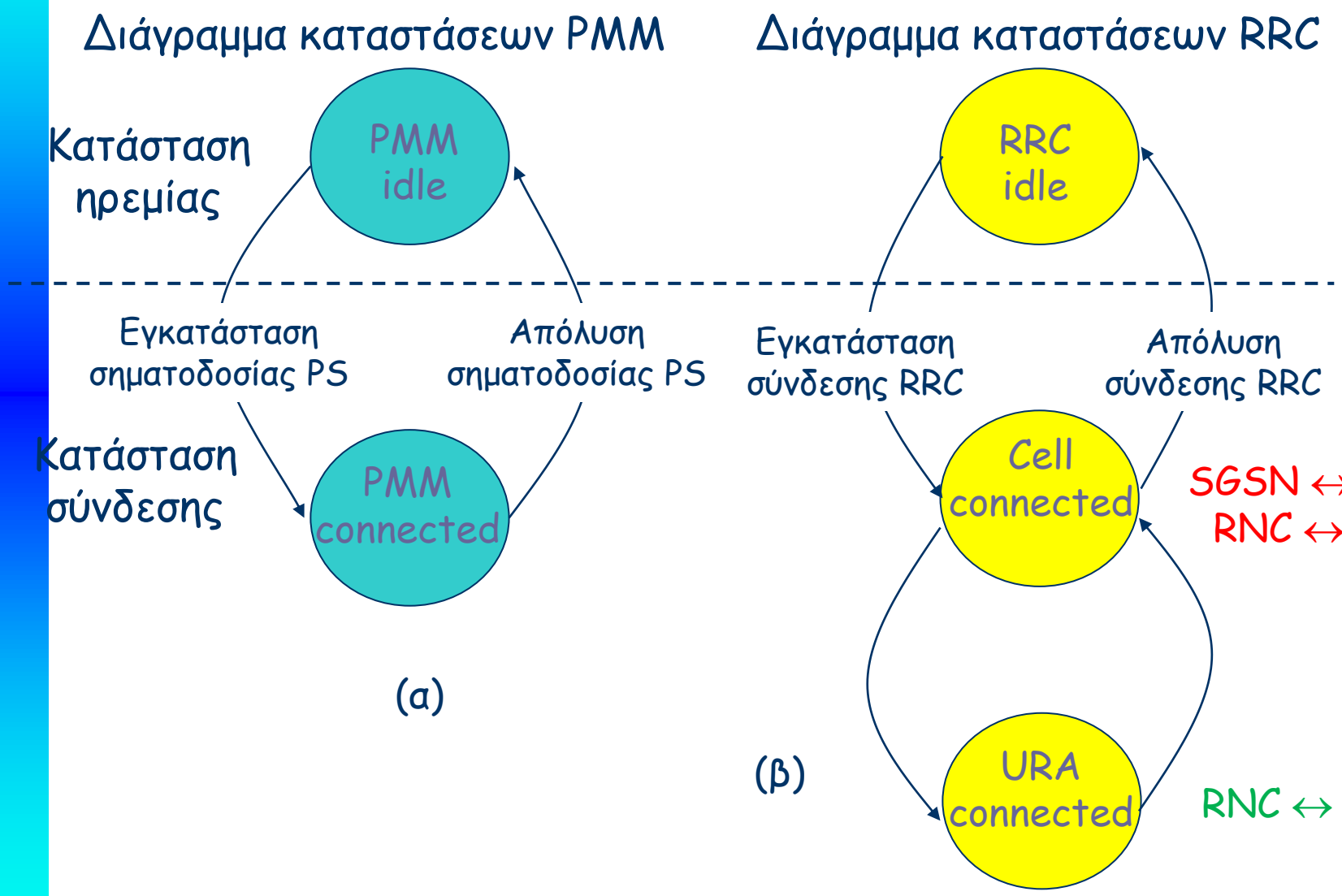
GGSN: Gateway GPRS Support Node
SGSN: Serving GPRS Support Node
UTRAN: UMTS Terrestrial Radio Access Network

Διαχείριση εντοπισμού στο UMTS



RA: Routing Area
URA: UTRAN Registration Area

Διαχείριση εντοπισμού στο UMTS



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)

Διαχείριση ασφάλειας

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.
- Στο UMTS, πιστοποιείται η αυθεντικότητα και του χρήστη 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.

Διαχείριση ασφάλειας

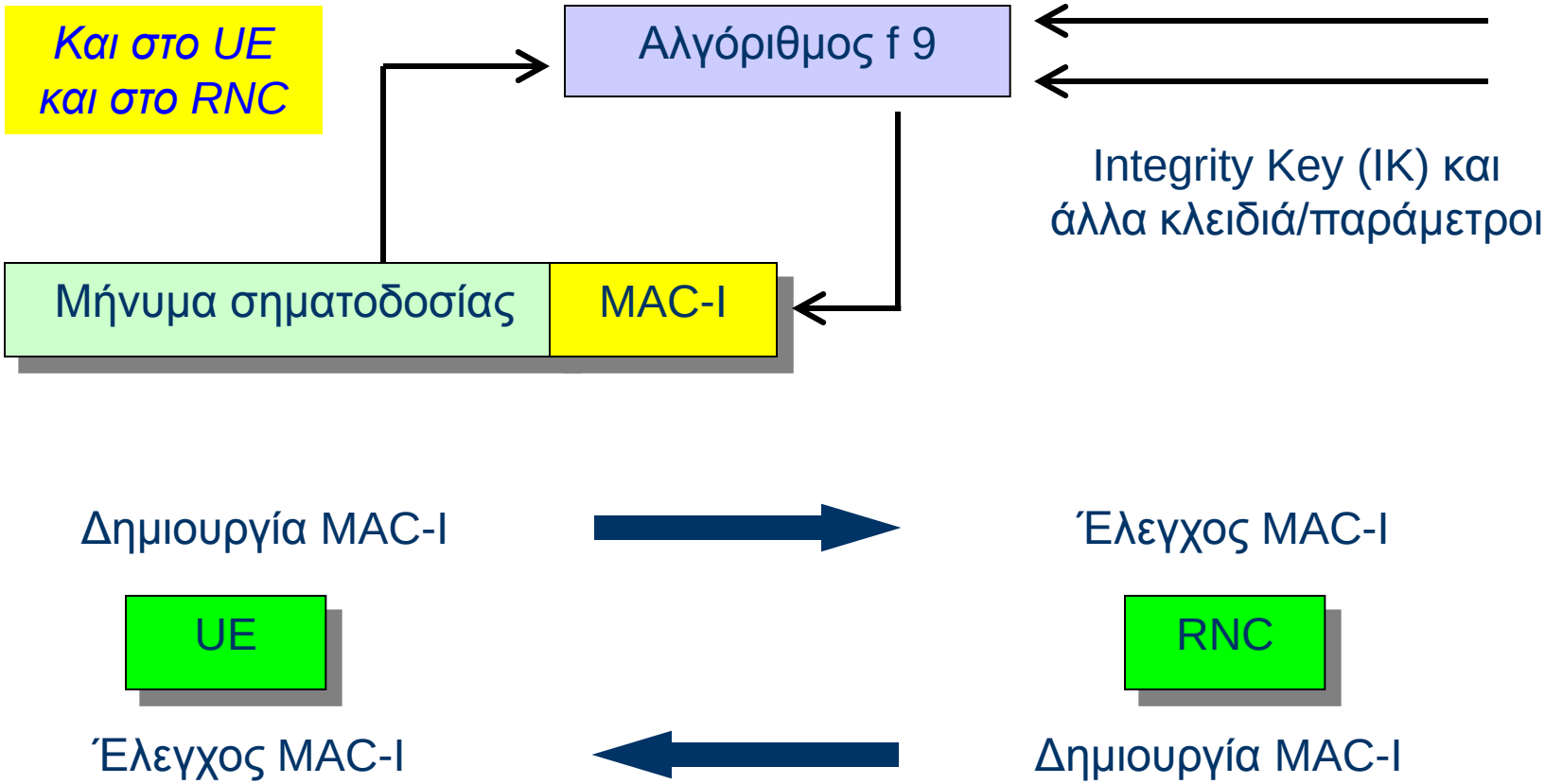
Ακεραιότητα δεδομένων

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).

Διαχείριση ασφάλειας

Ακεραιότητα δεδομένων σηματοδοσίας στο UMTS



Διαχείριση ασφάλειας

Εμπιστευτικότητα

Η ιδιότητα ότι η πληροφορία δεν γίνεται προσιτή σε μη εξουσιοδοτημένα άτομα, οντότητες ή διαδικασίες.

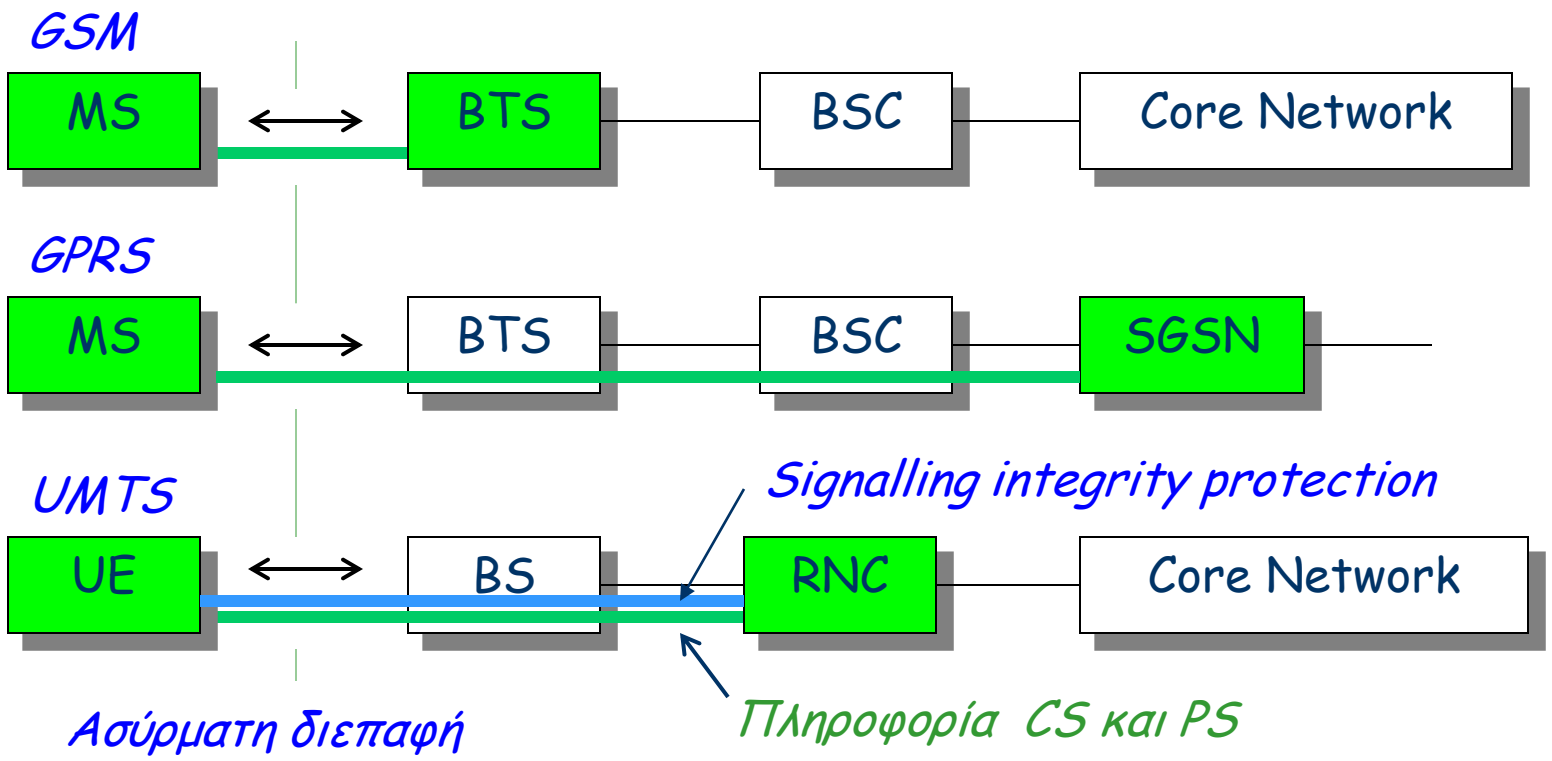
Παράδειγμα 1: Κρυπτογράφηση στην ασύρματη διεπαφή

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.

Διαχείριση ασφάλειας

Κρυπτογράφηση: Παραδείγματα



Διαχείριση ασφάλειας στο GSM

- 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

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

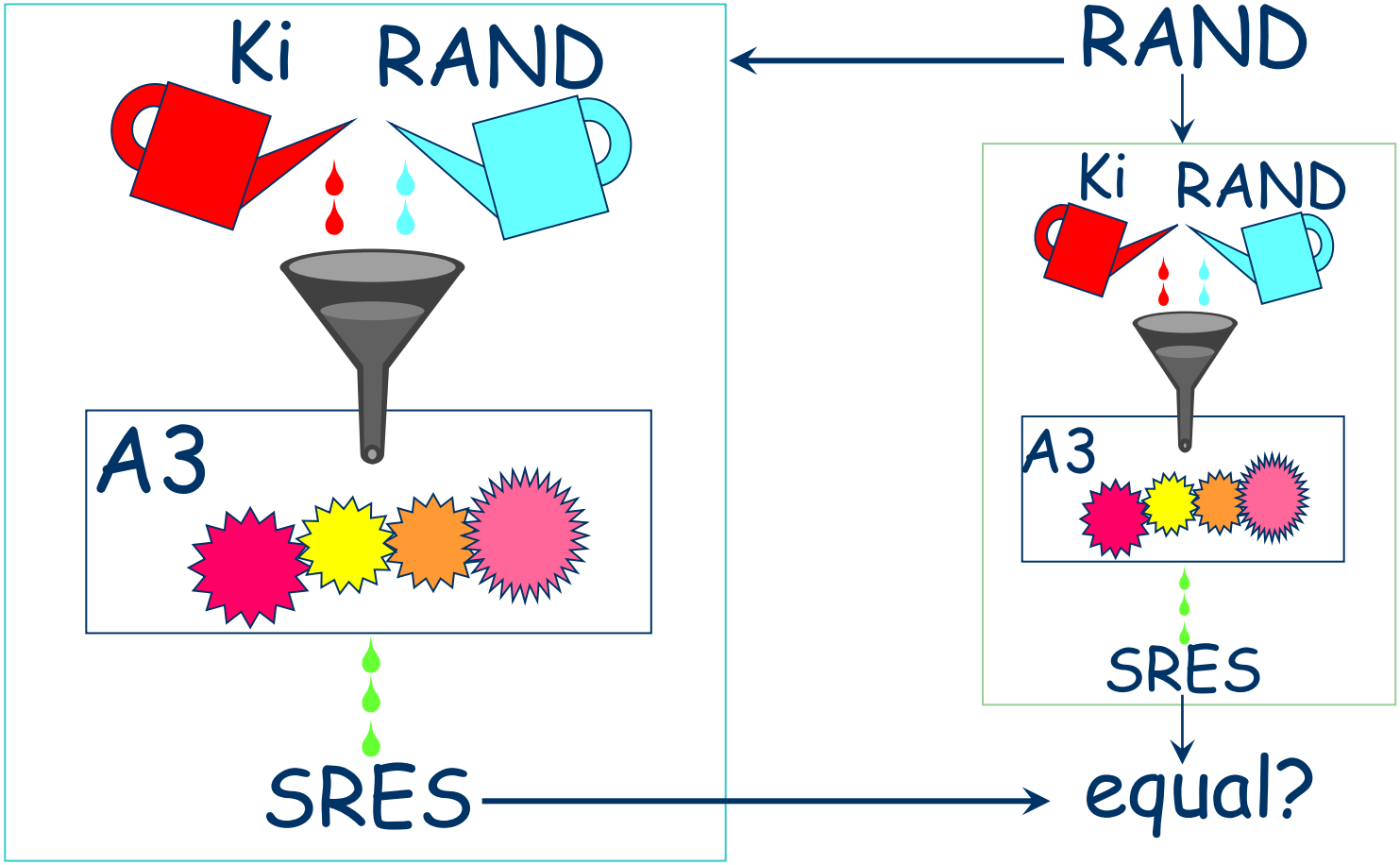
Διαχείριση ασφάλειας στο GSM

Λειτουργίες ασφάλειας

- 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.

Διαχείριση ασφάλειας στο GSM

Λειτουργίες ασφάλειας



SRES: SignedRESult

Διαχείριση ασφάλειας στο GSM

Λειτουργίες ασφάλειας

- 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).

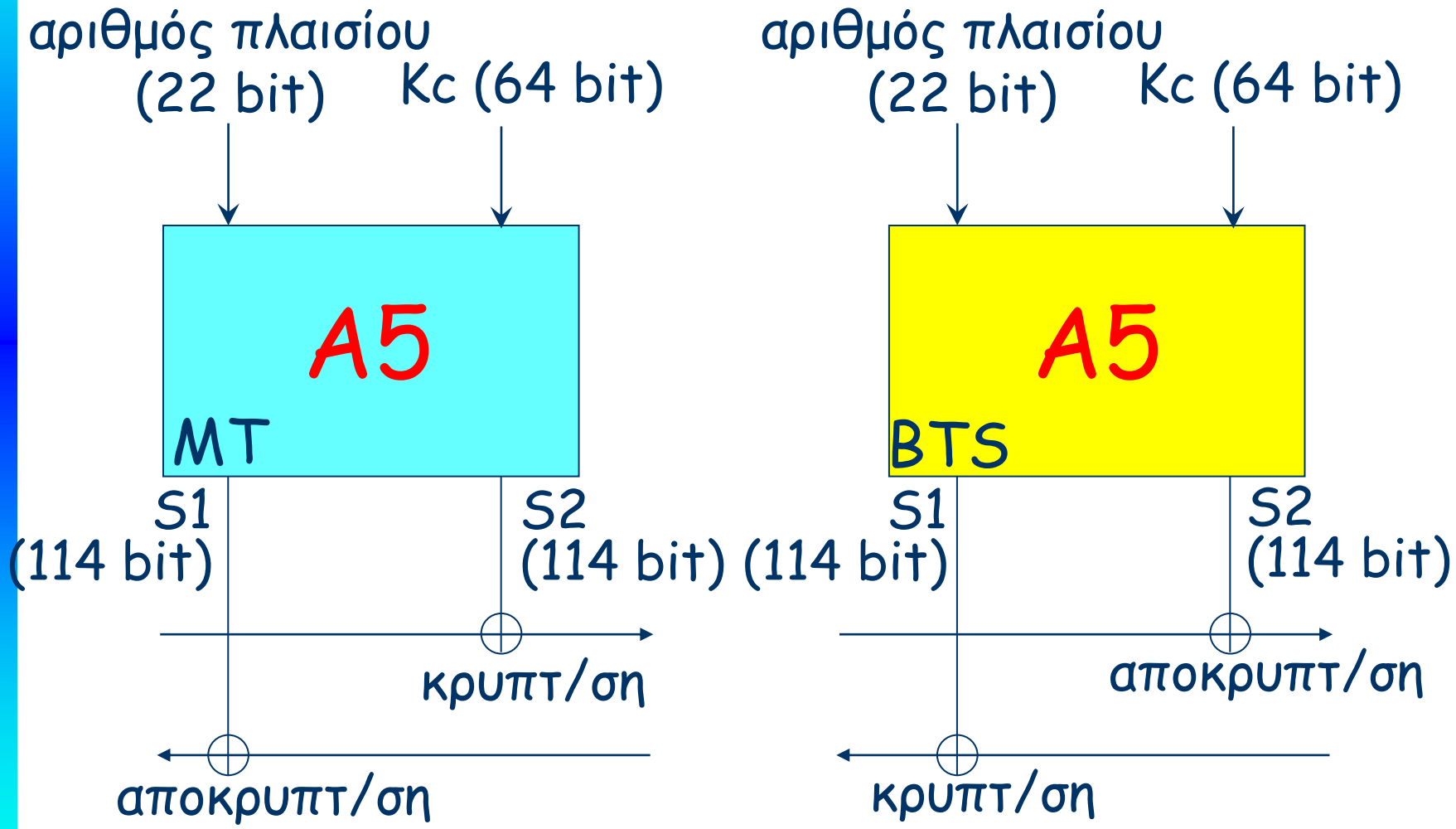
Διαχείριση ασφάλειας στο GSM

Κρυπτογράφηση

- 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)

Διαχείριση ασφάλειας στο GSM

Κρυπτογράφηση



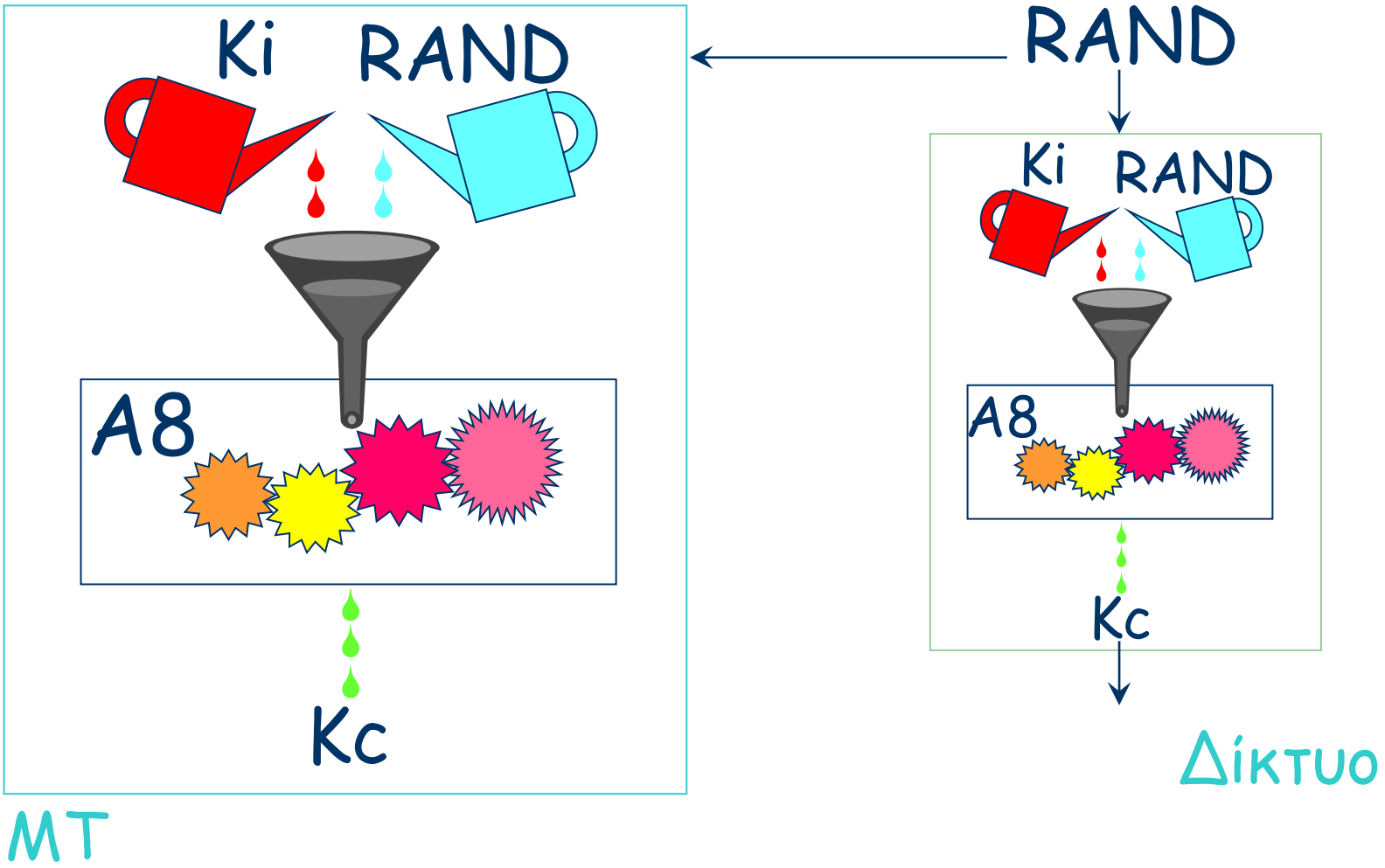
Διαχείριση ασφάλειας στο GSM

Διαχείριση κλειδιών

- Το Kc συμφωνείται μεταξύ MT 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 ασφάλειας στο GSM

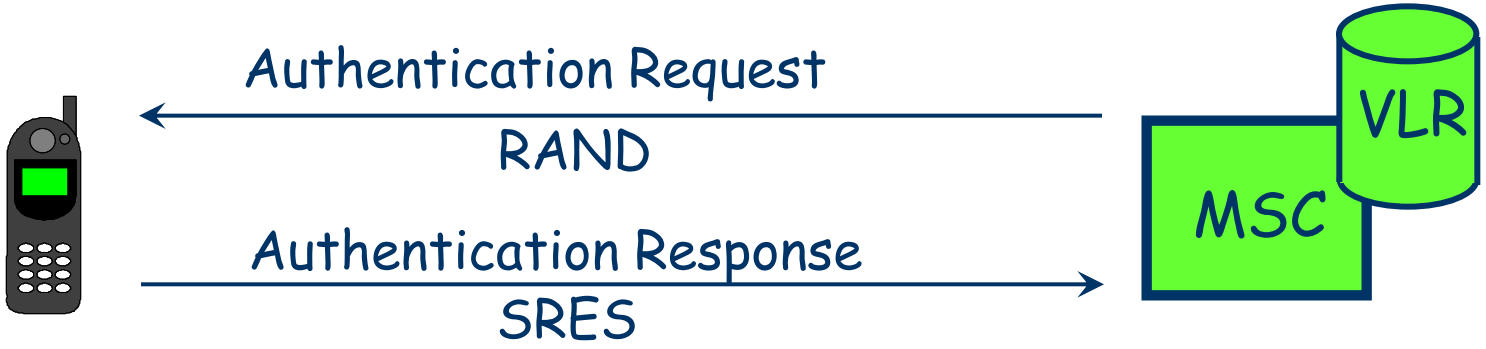
Διαχείριση κλειδιών



Διαχείριση ασφάλειας στο GSM

Διαχείριση κλειδιών

Πιστοποίηση αυθεντικότητας και παραγωγή κλειδιών



Μεταφορά δεδομένων ασφαλείας

Διαχείριση ασφάλειας στο UMTS

GSM	UMTS
SIM authentication (PIN code)	USIM authentication (PIN code)
User authentication	User authentication
	Network authentication
Ciphering (air interface)	Ciphering (air interface)
	Signalling data integrity
	IP security (e.g. IPSEC)

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

Διαχείριση ασφάλειας στο UMTS

Βελτιώσεις στο GSM

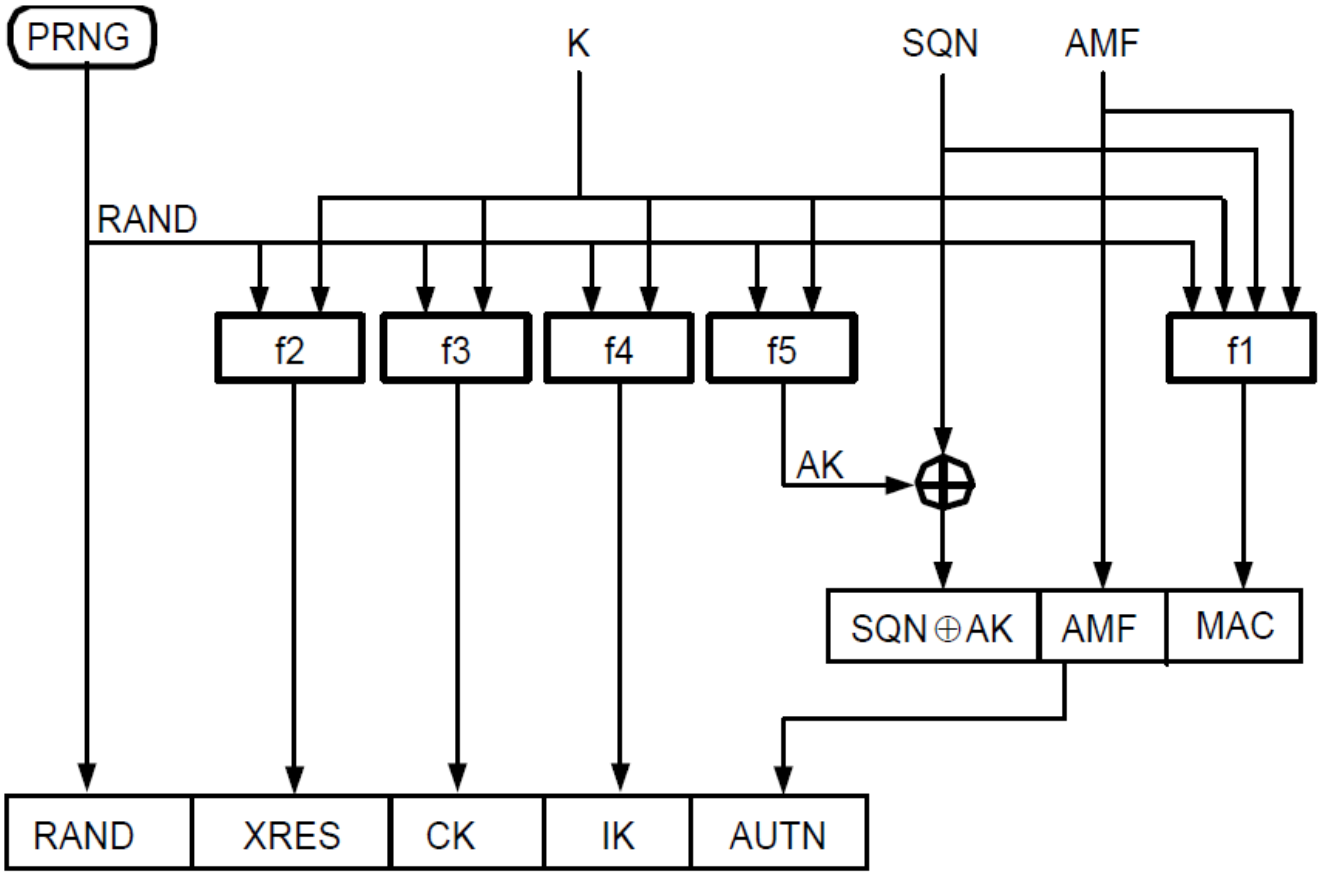
- Αμοιβαία πιστοποίηση αυθεντικότητας με επαναλαμβανόμενη προστασία
- Προστασία δεδομένων σηματοδοσίας
  - Ασφαλής διαπραγμάτευση των αλγορίθμων ασφαλείας
  - Προστασία ακεραιότητας και authentication πηγής
  - Εμπιστευτικότητα
- Προστασία του payload των δεδομένων χρήστη
  - Εμπιστευτικότητα
- Κλειδιά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

Διαχείριση ασφάλειας στο UMTS

UMTS AKA

Διαχείριση ασφάλειας στο UMTS

Παραγωγή ανυσμάτων αυθεντικότητας



AMF: Authentication and Key Management Field

Διαχείριση ασφάλειας στο UMTS

Επιβεβαίωση AUTN και παραγωγή RES, CK, IK