Ίδρυμα Τεχνολογία και Έρευνας (ΙΤΕ)
Ινστιτούτο Πληροφορικής

Ασφάλεια σε ασύρματα δίκτυα πλέγματος: απαιτήσεις και επιλογές σχεδίασης

Ιωάννης Γ. Ασκοξυλάκης

Εργαστήριο Τηλεπικοινωνιών και Δικτύων

asko@ics.forth.gr

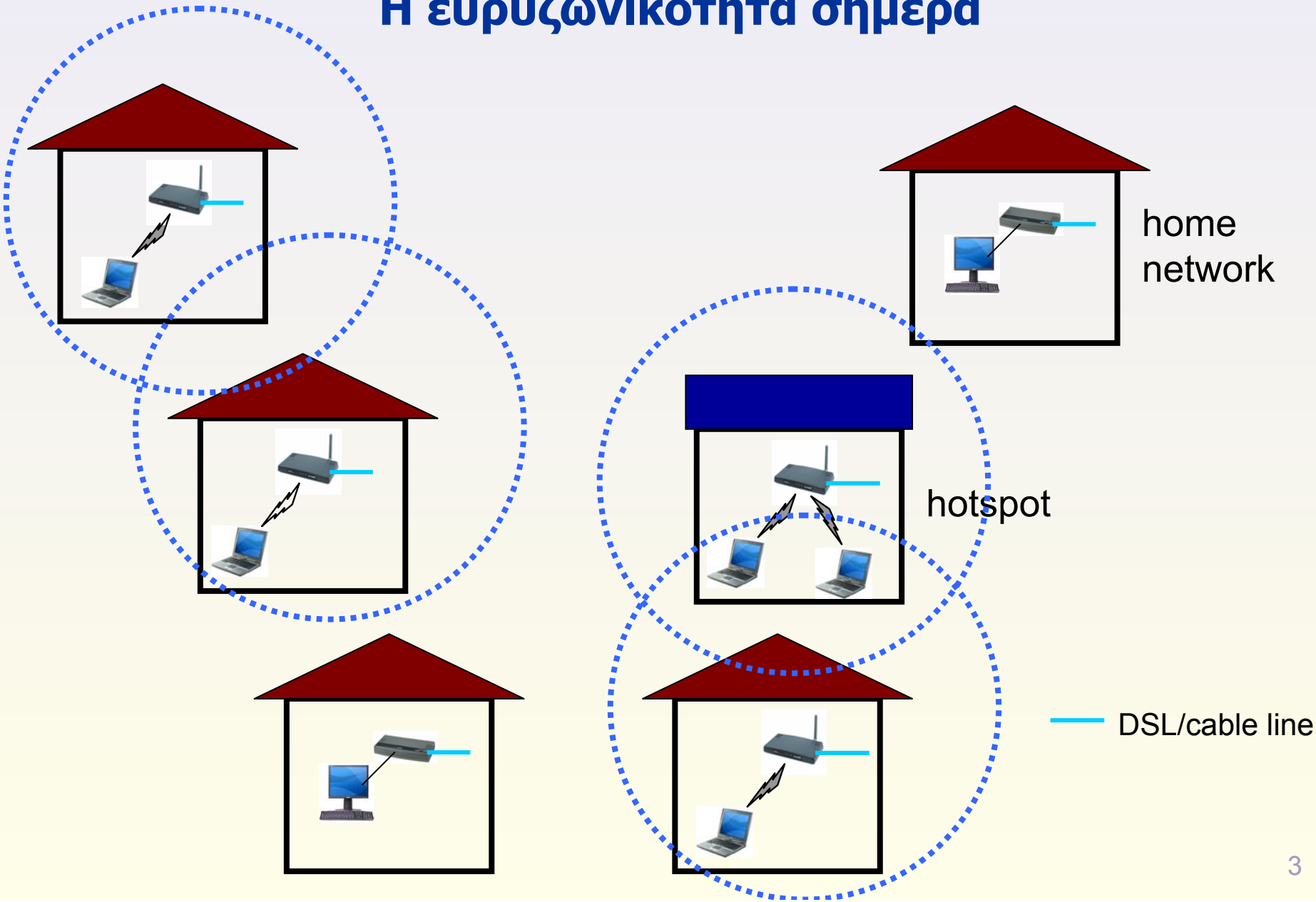
http://www.ics.forth.gr/tnl

http://www.ics.forth.gr/~asko

Οργάνωση παρουσίασης

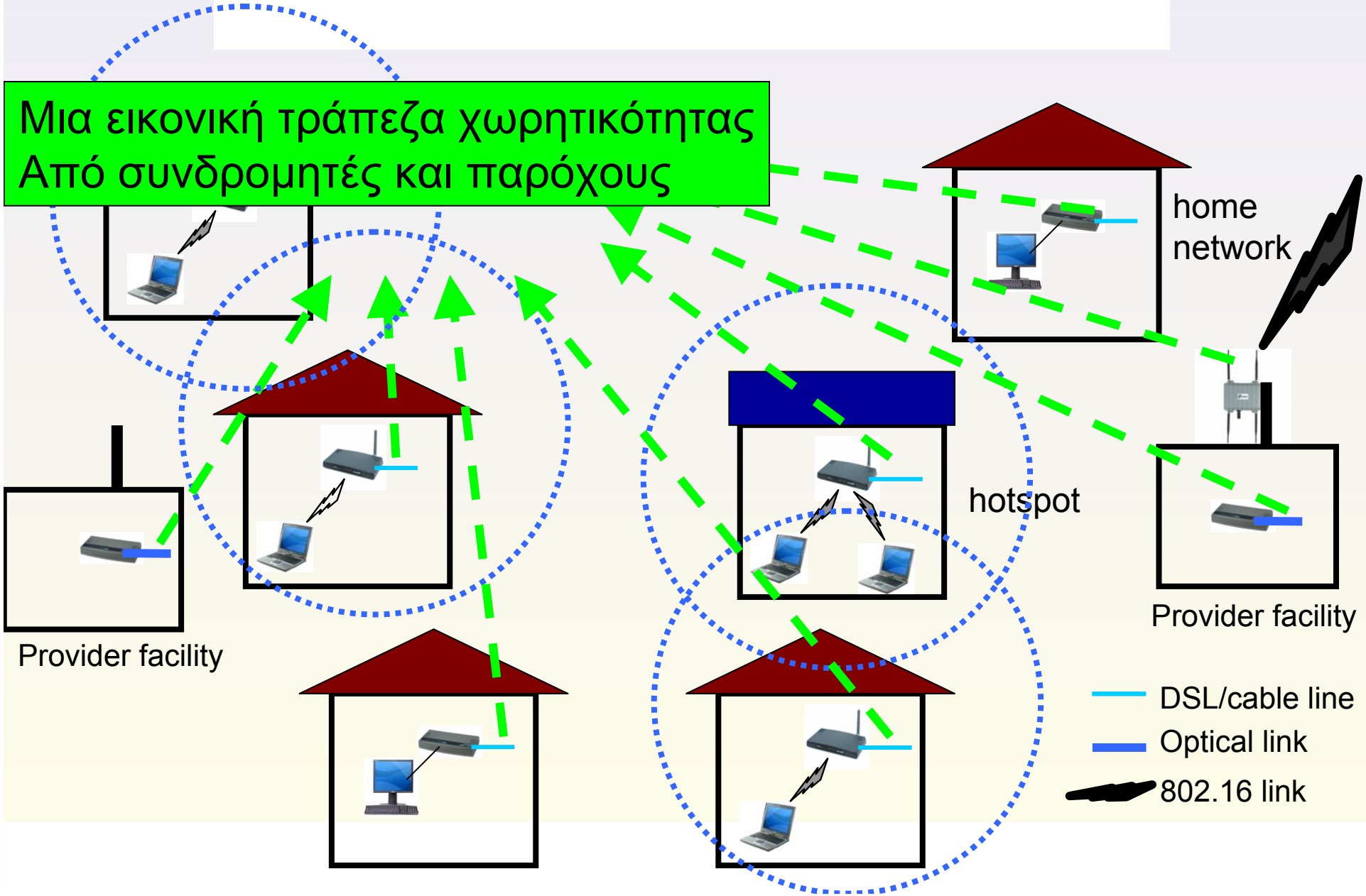
- Ασύρματα δίκτυα πλέγματος-περιγραφή
- Μοντελοποίηση των επιθέσεων (adversary model)
- Απαιτήσεις ασφάλειας
- Πιστοποίηση ταυτότητας τελικών χρηστών και επιβολή ελέγχου πρόσβασης
- Προστασία του ασύρματου μέσου
- Επίλογος

Η ευρυζωνικότητα σήμερα

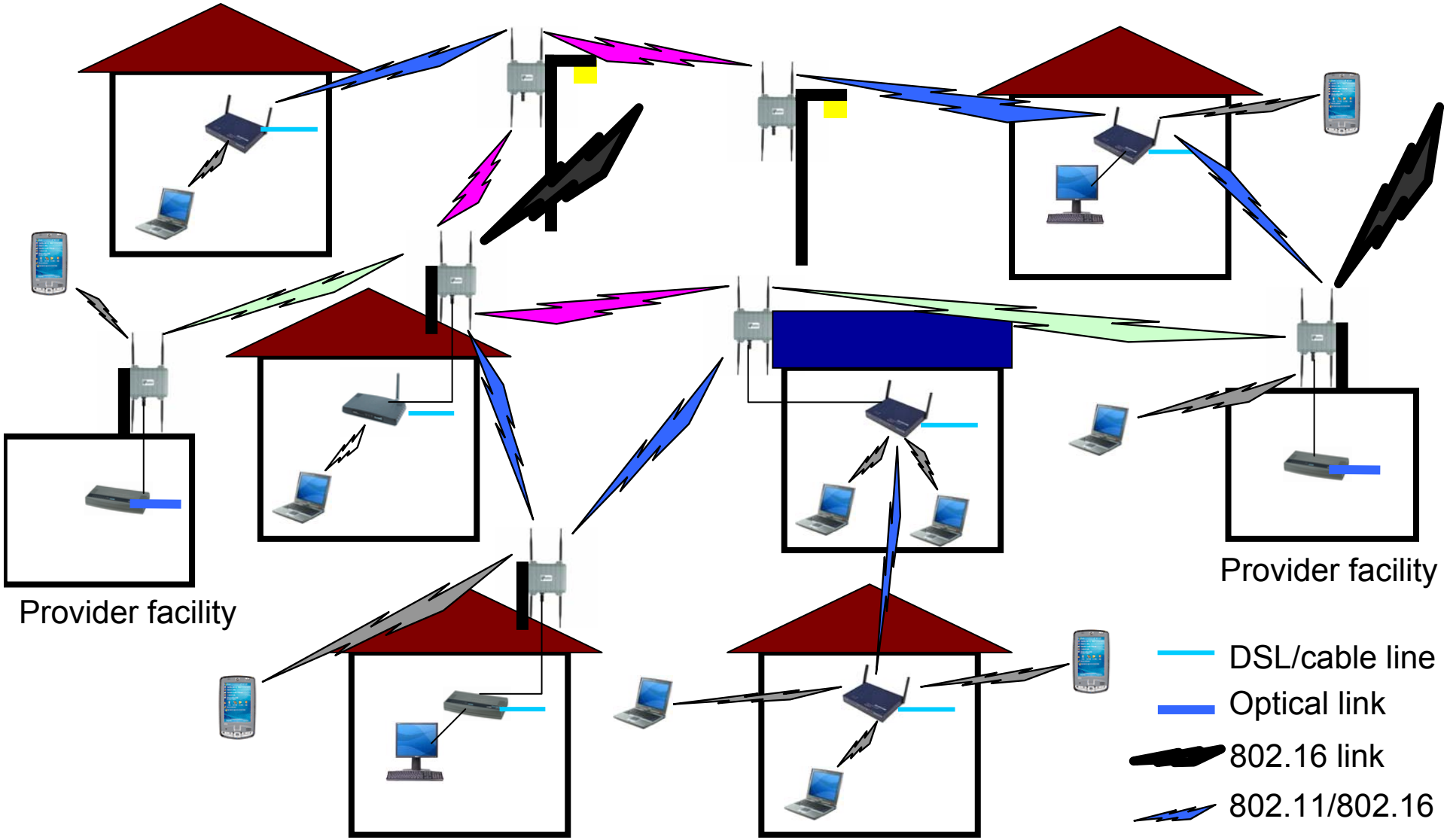


Το μέλλον με τα ασύρματα δίκτυα πλέγματος

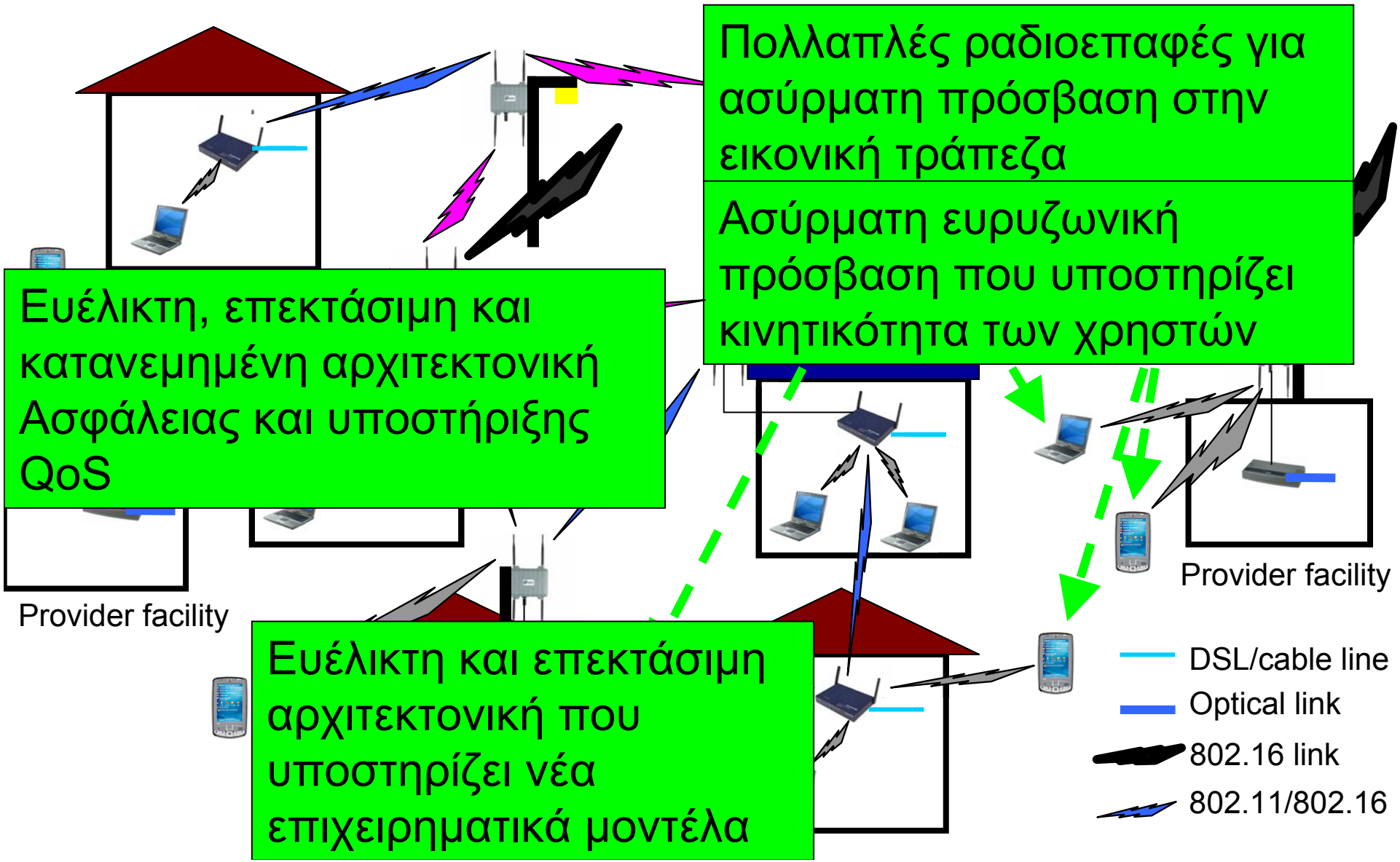
Μια εικονική τράπεζα χωρητικότητας
Από συνδρομητές και παρόχους



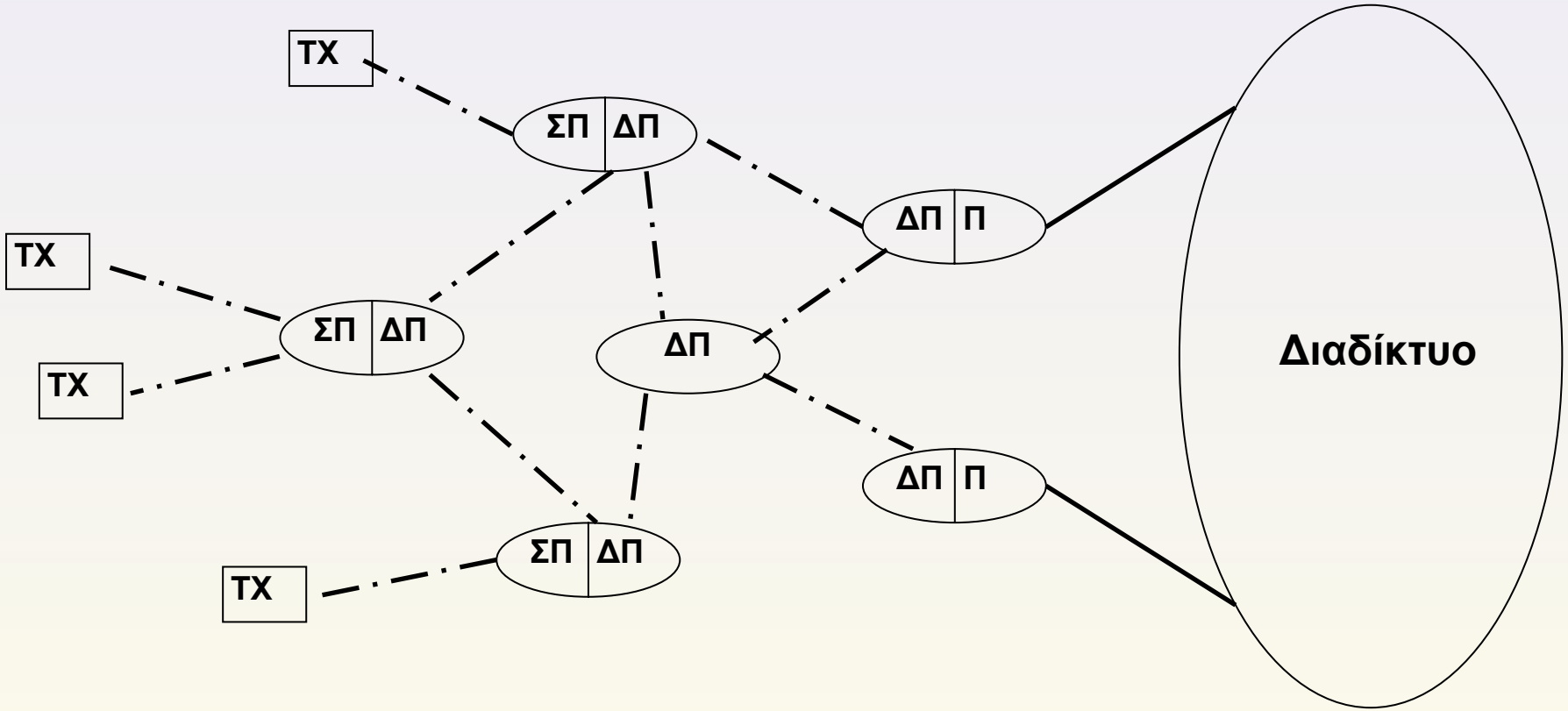
Το μέλλον με τα ασύρματα δίκτυα πλέγματος



Το μέλλον με τα ασύρματα δίκτυα πλέγματος



Ασύρματα δίκτυα πλέγματος



ΣΠ – Σημείο Πρόσβασης (Access Point)
Π – Πύλη (Gateway)
ΔΠ – Δρομολογητής Πλέγματος (Mesh Router)
ΤΧ – Τελικός Χρήστης (Mesh Client)

Ασύρματη ζεύξη
Ενσύρματη σύνδεση

Μοντελοποίηση των επιθέσεων (adversary model)

- Κατηγορίες επιτιθέμενων
  - Εξωτερικοί επιτιθέμενοι
  - Ανέντιμοι χρήστες
  - Ανέντιμοι πάροχοι
- Στόχοι επιθέσεων
  - Μη εξουσιοδοτημένη πρόσβαση στις παρεχόμενες υπηρεσίες
  - Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα πελατών και σε μέτα-δεδομένα
  - Άρνηση εξυπηρέτησης
  - Απόκτηση πλεονεκτήματος έναντι ανταγωνιστών

Μοντελοποίηση των επιθέσεων (adversary model)

- Μηχανισμοί επιθέσεων
  - Επιθέσεις στην ασύρματη επικοινωνία (στο ασύρματο μέσο)
    - Ωτακουστές
    - Παρεμβολές
    - επανάληψη και έγχυση μηνυμάτων
  - Εγκατάσταση παραπλανητικών δρομολογητών πλέγματος
  - παράνομη απόκτηση ελέγχου υπάρχοντων δρομολογητών

Απαιτήσεις ασφάλειας

- Πιστοποίηση ταυτότητας χρήστη δικτύου πλέγματος και επιβολή ελέγχου πρόσβασης
- Προστασία του ασύρματου μέσου
  - Εμπιστευτικότητα, ακεραιότητα των δεδομένων, προστασία δεδομένωναπό μη εξουσιοδοτημένη πρόσβαση.
  - ακεραιότητα και πιστοποίηση προέλευσης των δεδομένων σε κάθε ασύρματη διασύνδεση (άμεσος εντοπισμόςπλαστών, τροποποιημένων ή επαναλαμβανόμενων μηνυμάτων)
  - Αποφυγή κακόβουλης ανάλυσης της κίνησης του δικτύου

Απαιτήσεις ασφάλειας

- Αύξηση της ανθεκτικότητας των δικτυακών μηχανισμών.
  - διασφάλιση των πρωτοκόλλων δρομολόγησης καθώς αυτά επηρεάζουν την λειτουργία ολόκληρου του δικτύου ενώ επιθέσεις σε χαμηλότερα επίπεδα επηρεάζουν μόνο τοπικά την λειτουργία.
- Ανίχνευση εισβολέων και ανάκαμψη.
  - Η αντιμετώπιση «εσωτερικών» επιθέσεων είναι αδύνατη με την χρήση κρυπτογραφικών μηχανισμών.
  - εκτός από προστατευτικούς μηχανισμούς ασφάλειας, απαραίτητη ύπαρξη μηχανισμών ασφάλειας σε δεύτερο χρόνο μετά από επίθεση ή απλή δυσλειτουργία του δικτύου με
  - Ικανότητα ανίχνευσης των επιθέσεων, τις επιπτώσεις τους στο δίκτυο και να οδηγούν το δίκτυο σε μια διαδικασία ανάκαμψης ώστε να φτάσει στο επίπεδο ασφάλειας που βρισκόταν πριν την επίθεση ή την δυσλειτουργία.

Πιστοποίηση ταυτότητας

- Απαιτήσεις
  - Γρήγορη πιστοποίηση ταυτότητας για υποστήριξη κινητικότητας χρηστών
  - Τα προσωρινά κλειδιά διασύνδεσης δεν πρέπει να οδηγούν στα μακροπρόθεσμα κλειδιά λειτουργίας του δικτύου
  - Ανεξαρτησία των κλειδιών διασύνδεσης
  - Ανανέωση των κλειδιών
  - Ανθεκτικότητα στην Άρνηση Εξυπηρέτησης
  - Συμβατότητα με τα πρότυπα (Standards)
  - Επεκτασιμότητα
  - Ανεξαρτησία οντοτήτων

Πιστοποίηση ταυτότητας

- Μέθοδοι πιστοποίησης ταυτότητας

  Ταξινόμηση ανάλογα με το σημείο επιβολής του ελέγχου πρόσβασης και το είδος της πιστοποίησης
  - Κεντρικός έλεγχος πρόσβασης
  - Έλεγχος πρόσβασης στα όρια του ασύρματου δικτύου πλέγματος
  - Κατανεμημένος έλεγχος πρόσβασης
    - Απομακρυσμένος εξυπηρετητής πιστοποίησης
    - Τοπικός εξυπηρετητής πιστοποίησης
    - Τα σημεία πρόσβασης λειτουργούν σαν κατανεμημένοι εξυπηρετητές πιστοποίησης

Πιστοποίηση ταυτότητας

- Πιστοποίησης ταυτότητας κινούμενων χρηστών
  - *Μεταδραστική (reactive) πιστοποίηση:* Η πιστοποίηση του τελικού χρήστη στο επόμενο σημείο πρόσβασης και η εγκατάσταση του κλειδιού διασύνδεσης πραγματοποιούνται αφού ο χρήστης συνδεθεί με το επόμενο σημείο πρόσβασης
  - *Προδραστική (proactive) πιστοποίηση:* Τα κλειδιά διασύδεσης αποστέλλονται στα πιθανά επόμενα σημεία πρόσβασης πριν πραγματοποιηθεί η πιστοποίηση.

Πιστοποίηση ταυτότητας

- Προδραστική (proactive) πιστοποίηση: Κατηγοριοποίηση ανάλογα με την οντότητα που διαχειρίζεται την διανομή των κρυπτογραφικών κλειδιών
  - *Κατανομή κλειδιών από τους τελικούς χρήστες:* Ο τελικός χρήστης δημιουργεί ασφαλή/είς συνδέσεις με το επόμενο/α σημείο/α πρόσβασης, πριν την μεταπομπή του.
  - *Κατανομή κλειδιών από τον εξυπηρετητή πιστοποίησης:* Ένας εξυπηρετητής πιστοποίησης διανέμει στους τελικούς χρήστες κρυπτογραφικά κλειδιά για την διασύνδεση τους με τα πιθανά σημεία πρόσβασης με τέτοιο τρόπο ώστε να κλειδιά αυτά να είναι διαθέσιμα στους τελικούς χρήστες πριν την μετακίνησή τους από το σημείο πρόσβασης που βρίσκονται στο επόμενο.

Πιστοποίηση ταυτότητας

- **Κεντρική επιβολή ελέγχου πρόσβασης.**
  - απαιτείται πιστοποίηση στα σημεία πρόσβασης κατά την διάρκεια της μεταπομπής.
  - Ο τελικός χρήστης συνδέεται σε ένα σημείο πρόσβασης και ο έλεγχος πρόσβασης οδηγεί την κίνηση στην κεντρική μονάδα επιβολής ελέγχου πρόσβασης.
  - Η κεντρική μονάδα παίρνει αποφάσεις προώθησης βασιζόμενη σε στοιχεία της πηγή προέλευσης της κίνησης, όπως οι διευθύνσεις MAC και/ή IP του τελικού χρήστη.
  - Η λύση αυτή συναντάται σε κλασσικά WiFi hotspots, όπου συνήθως χρησιμοποιείται η υλοποίηση Chilispot.
  - Το κύριο μειονέκτημα της λύσης αυτής είναι η έλλειψη κρυπτογραφικών κλειδιών διασύνδεσης και έτσι ενας επιτιθέμενος μπορεί εύκολα να αποκτήσει πρόσβαση χρησιμοποιώντας MAC ή IP διευθύνσεις από συσκευές που έχουν ήδη πιστοποιηθεί.

Πιστοποίηση ταυτότητας

- **Επιβολή ελέγχου πρόσβασης στις πύλες**
  - Όταν ο έλεγχος πρόσβασης επιβάλλεται στα όρια του ασύρματου δικτύου πρόσβασης ο τελικός χρήστης μπορεί να πιστοποιηθεί είτε στην πύλη είτε στον κεντρικό εξυπηρετητή πιστοποίησης.
  - Μέχρι σήμερα δεν υπάρχει κάποια λύση όπου ο τελικός χρήστης πιστοποιείται στην πύλη.
  - Το πρωτόκολλο PANA μπορεί να χρησιμοποιηθεί όταν ο τελικός χρήστης πιστοποιείται σε έναν κεντρικό εξυπηρετητή πιστοποίησης ενώ ο έλεγχος πρόσβασης επιβάλλεται στις πύλες. Αυτό είναι εφικτό γιατί το PANA επιτρέπει την ύπαρξη πολλαπλών οντοτήτων επιβολής ελέγχου πρόσβασης.
  - Έτσι κάθε πύλη μπορεί να είναι μία οντότητα επιβολής ελέγχου πρόσβασης η οποία λαμβάνει τα αντίστοιχα κλειδιά από τον εξυπηρετητή πιστοποίησης.

Πιστοποίηση ταυτότητας

Κατανεμημένη επιβολή ελέγχου πρόσβασης με:

- μεταδραστική πιστοποίηση από απομακρυσμένο εξυπηρετητή πιστοποίησης
- μεταδραστική πιστοποίηση από τοπικό εξυπηρετητή πιστοποίησης
- προδραστική πιστοποίηση από εξυπηρετητή πιστοποίησης
- προδραστική πιστοποίηση από τους τελικούς χρήστες

Πιστοποίηση ταυτότητας

- **Κατανεμημένη επιβολή ελέγχου πρόσβασης με μεταδραστική πιστοποίηση από απομακρυσμένο εξυπηρετητή πιστοποίησης.**
  - Ένα χαρακτηριστικό παράδειγμα πιστοποίησης και ελέγχου πρόσβασης είναι το IEEE 802.1X όπως περιγράφεται στο πρότυπο IEEE 802.11i
  - ο έλεγχος πρόσβασης επιβάλλεται στα σημεία πρόσβασης με κατανεμημένο τρόπο
  - Ο τελικός χρήστης πιστοποιείται σε ένα απομακρυσμένο εξυπηρετητή πιστοποίησης ο οποίος ενημερώνει το σημείο πρόσβασης για το αποτέλεσμα της πιστοποίησης και στέλνει το αντίστοιχο κλειδί διασύνδεσης.
  - Το κλειδί διασύνδεσης, (ή ένα δεύτερο κλειδί που προκύπτει από αυτό) χρησιμοποιείται για να διασφαλίσει την διασύνδεση στο επίπεδο σύνδεσης.
  - Το κύριο μειονέκτημα- ο χρόνος αποστολής και λήψης μηνυμάτων αυξάνει αρκετά όσο αυξάνει η απόσταση (τα βήματα μεταξύ ασύρματων σημείων πρόσβασης).
    - Ο χρόνος μπορεί να ειναι μεγαλύτερος από τον χρόνο που θέτουν ως προϋπόθεση ορισμένες εφαρμογές με συγκεκριμένη ποιότητα υπηρεσίας.
    - Ο κεντρικός εξυπηρετητής πιστοποίησης είναι μοναδικό σημείο όπου σφάλματα και επιθέσεις τον καθιστούν ευάλωτο σε επιθέσεις άρνησης εξυπηρέτησης.

Πιστοποίηση ταυτότητας

- **Κατανεμημένη επιβολή ελέγχου πρόσβασης με μεταδραστική πιστοποίηση από τοπικό εξυπηρετητή πιστοποίησης.**
  - Χρήση τοπικών εξυπηρετητών πιστοποίησης κοντά στα σημεία πρόσβασης.
  - Επεκτάσεις του EAP πρότυπου προτείνουν μείωση του χρόνου αποστολής και λήψης μηνυμάτων κάνοντας χρήση τοπικών εξυπηρετητών πιστοποίησης ανάμεσα στα σημεία πρόσβασης και του κεντρικού εξυπηρετητή πιστοποίησης.
  - ο κεντρικός εξυπηρετητής πιστοποίησης μπορεί να μοιράζεται ένα κλειδί ή ένα άλλο κλειδί που προκύπτει από το κλειδί πιστοποίησης, με τους τοπικούς εξυπηρετητές πιστοποίησης.
  - Όταν ένα σημείο πρόσβασης στραφεί προς έναν τοπικό εξυπηρετητή πιστοποίησης, ο δεύτερος στέλνει ένα κλειδί διασύνδεσης στο σημείο πρόσβασης.
  - Το μόνο μειονέκτημα των τοπικών εξυπηρετητών είναι βρίσκονται εντός του ασύρματου δικτύου πρόσβασης και κατά συνέπεια μπορεί να είναι απροστάτευτοι → είναι επικίνδυνο να κατέχουν μακροπρόθεσμα κλειδιά πιστοποίησης, καθώς μπορεί να υποκλαπούν.

Πιστοποίηση ταυτότητας

- **Κατανεμημένη επιβολή ελέγχου πρόσβασης με προδραστική πιστοποίηση από εξυπηρετητή πιστοποίησης.**
  - ο εξυπηρετητής πιστοποίησης είναι υπεύθυνος να κατανείμει τα κρυπτογραφικά κλειδιά διασύνδεσης πριν πραγματοποιηθεί μεταπομπή.
  - κατά την διάρκεια της μεταπομπής τα σημεία πρόσβασης που συμμετέχουν σε αυτήν αποκτούν την δυνατότητα να λαμβάνουν αποφάσεις ελέγχου πρόσβασης τοπικά, χωρίς να ζητούν επιπλέον πληροφορίες από τον εξυπηρετητή.

Πιστοποίηση ταυτότητας

- **Κατανεμημένη επιβολή ελέγχου πρόσβασης με προδραστική πιστοποίηση από τους τελικούς χρήστες.**
  - Σε αντίθεση με τους προδραστικούς μηχανισμούς πιστοποίησης που βασίζονται σε εξυπηρετητή πιστοποίησης, στους μηχανισμούς αυτούς οι τελικοί χρήστες είναι αρμόδιοι να παράσχουν τα κλειδιά διασύνδεσης στα σημεία πρόσβασης.
  - Ένας μηχανισμός προ-πιστοποίηση, έχει προταθεί στο πρότυπο IEEE 802.11i
    - επιτρέπει στους τελικούς χρήστες να εγκαταστήσουν κλειδί διασύνδεσης με το εν δυνάμει επόμενο σημείο πρόσβασης, πριν την πραγματοποίηση της μεταπομπής, πραγματοποιώντας πλήρη πιστοποίηση με το σημείο πρόσβασης που είναι ήδη συνδεδεμένοι.
    - Το πλεονέκτημα-ήδη προτυποποιημένος και υποστηρίζει υπηρεσίες εγγυημένης ποιότητας.
    - Το μειονέκτημα-επιτρέπει μετάβαση μόνο σε άμεσους γείτονες του συγκεκριμένου σημείου πρόσβασης.

Πιστοποίηση ταυτότητας

- **Κατανεμημένη επιβολή ελέγχου πρόσβασης με προδραστική πιστοποίηση στα σημεία πρόσβασης**
  - Αντί της πιστοποίησης σε ένα τοπικό ή απομακρυσμένο εξυπηρετητή πιστοποίησης, στην κατηγορία αυτή, ο τελικός χρήστης πιστοποιείται στο σημείο πρόσβασης εκ των προτέρων (προδραστικά).
  - Δυο προτεινόμενες λύσεις:
    - 1η το ήδη χρησιμοποιούμενο κλειδί διασύνδεσης μεταξύ τελικού χρήστη και σημείου πρόσβασης, αποστέλλεται από το σημείο πρόσβασης στα γειτονικά, ώστε να χρησιμοποιηθεί από το σημείο πρόσβασης στο οποίο ο τελικός χρήστης θα συνδεθεί κατά την κίνησή του
    - 2η ο τελικός χρήστης μεταφέρει το νέο κλειδί διασύνδεσης με μία ηλεκτρονική εξουσιοδότηση που του έχει σταλεί από το σημείο πρόσβασης όπου είναι συνδεδεμένος, πριν πραγματοποιήσει την μεταπομπή. Η εξουσιοδότηση είναι κρυπτογραφημένο με ένα κλειδί το οποίο μοιράζονται όλα τα σημεία πρόσβασης. Μετά την σύνδεση με το επόμενο σημείο πρόσβασης, ο τελικός χρήστης δείχνει το πιστοποιητικό του και το νέο σημείο πρόσβασης το αποκρυπτογραφεί και αποκτά το κλειδί διασύνδεσης

Πιστοποίηση ταυτότητας

- **Δημιουργία κρυπτογραφικών κλειδιών διασύνδεσης.**
  - τα κλειδιά διασύνδεσης, σε όλες τις παραπάνω περιπτώσεις, υπολογίζονται από τα παρακάτω δεδομένα (ή τμήματα αυτών)
    - το κλειδί πιστοποίησης
    - το προηγούμενο κλειδί διασύνδεσης
    - δημόσια πληροφορία του σημείου πρόσβασης
    - τυχαίους αριθμούς
  - είναι απαραίτητο να μην υπάρχει η δυνατότητα από τα σημεία πρόσβασης να εξάγουν το κλειδί πιστοποίησης από τα υπολογισμένα κλειδιά διασύνδεσης.
  - Επιπρόσθετα, η απαίτηση για ανεξαρτησία των κλειδιών διασύνδεσης μπορεί να ικανοποιηθεί αν πραγματοποιείται πλήρης πιστοποίηση του τελικού χρήστη μετά από κάθε γρήγορη μεταπομπή

Πιστοποίηση ταυτότητας

- ***Απαιτήσεις και προτεινόμενες λύσεις για δημιουργία κλειδιών διασύνδεσης***

	Αμφίδρομη πιστοποίηση	Προστασία ακεραιότητας κλειδιού	Ανταλλαγή κλειδιών διαφορετικής ασφάλειας	Ανανέωση
Κλειδί πιστοποίησης	√	χ	χ	χ
Προηγούμενο κλειδί διασύνδεσης	X	√		√
Δημόσια πληροφορία του σημείου πρόσβασης	X	√	√	χ
Τυχαίοι αριθμοί από τον εξυπηρετητή πιστοποίησης	X	√	√	χ
Τυχαίοι αριθμοί από τον τελικό χρήστη	X	√	√	√

Πιστοποίηση ταυτότητας

- ***Απαιτήσεις και μέθοδοι πιστοποίησης*-Σύνοψη**

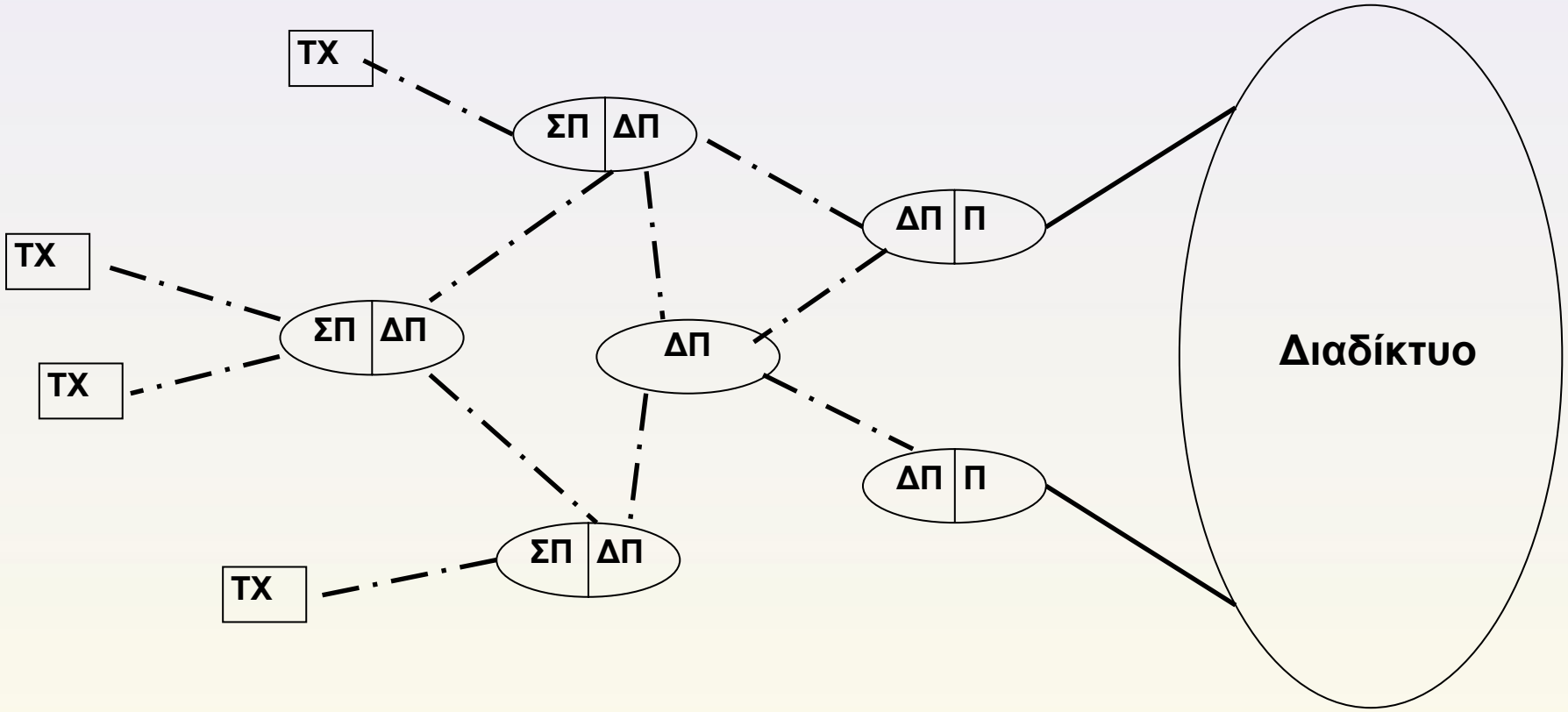
				Γρήγορη επαναπιστοποίηση	Ανθεκτικότητα σε DoS	Συμβατότητα με πρότυπα	Επεκτασιμότητα	Ανεξαρτησία στοιχείων
	Κεντρική επιβολή ελέγχου πρόσβασης			√	X	√	X	√
	Συνοριακή επιβολή ελέγχου πρόσβασης			√	X	√	√	√
Κατανεμημένη επιβολή ελέγχου πρόσβασης		**Μεταδραστική**	**Απομακ. Εξυπ. Πιστοποίησης**	X	X	√	X	√
		Μεταδραστική	**Τοπικός Εξυπ. Πιστοποίησης**	√	√	X	√	X
	Κεντρικά	**Προδραστική**	**Εξυπηρετητής Πιστοποίησης**	√	√	X	√	√
	Τελ. χρήστης	**Προδραστική**	**Εξυπηρετητής Πιστοποίησης**	√	√	√	√	√
		Μεταδραστική	**Σημείο πρόσβασης**	√	√	-	√	X
	Κεντρικά	**Προδραστική**	**Σημείο πρόσβασης**	√	√	X	√	X
	Τελ. Χρήστης	**Προδραστική**	**Σημείο πρόσβασης**	√	√	X	√	X

Προστασία του ασύρματου μέσου

- Προστασία από σημείο σε σημείο (end-to-end)
  - Η πληροφορία προστατεύεται από τον χρήστη μέχρι το τελικό άκρο της επικοινωνίας τους
- Προστασία από διασύνδεση σε διασύνδεση (link-by-link)
  - Η πληροφορία προστατεύεται μόνο στις ασύρματες διασυνδέσεις (μεταξύ δρομολογητών πλέγματος και δρομολογητών-τελικών χρηστών).
  - Επιτρέπει χρήση διαφορετικών μηχανισμών σε διαφορετικές διασυνδέσεις
- Προστασία τμημάτων διαδρομής
  - Η πληροφορία προστατεύεται για ένα τμήμα της συνολικής διαδρομής μεταξύ χρήστη και τελικού άκρου

Προστασία του ασύρματου μέσου

Προστασία από σημείο σε σημείο (end-to-end)

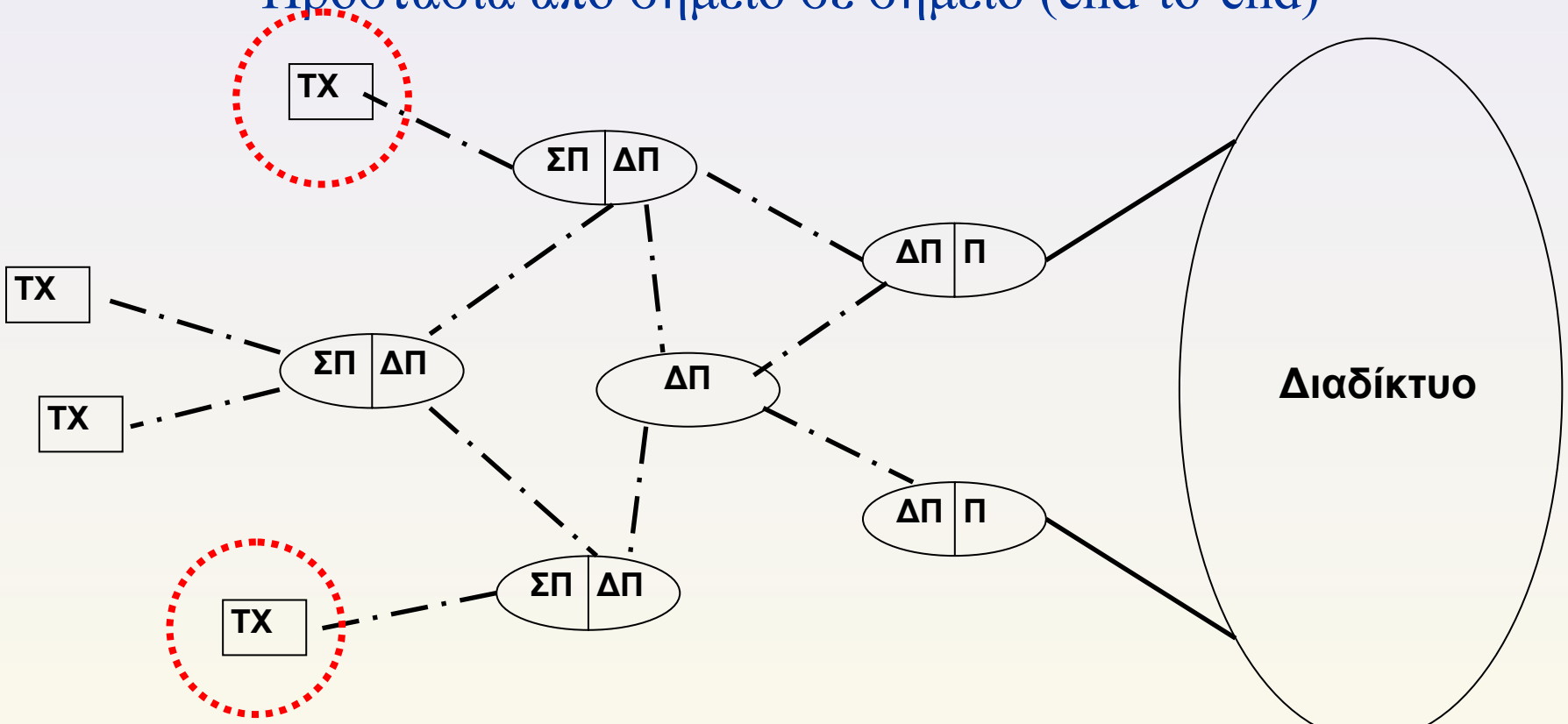


ΣΠ – Σημείο Πρόσβασης (Access Point)
Π – Πύλη (Gateway)
ΔΠ – Δρομολογητής Πλέγματος (Mesh Router)
ΤΧ – Τελικός Χρήστης (Mesh Client)

Ασύρματη ζεύξη
Ενσύρματη σύνδεση

Προστασία του ασύρματου μέσου

Προστασία από σημείο σε σημείο (end-to-end)

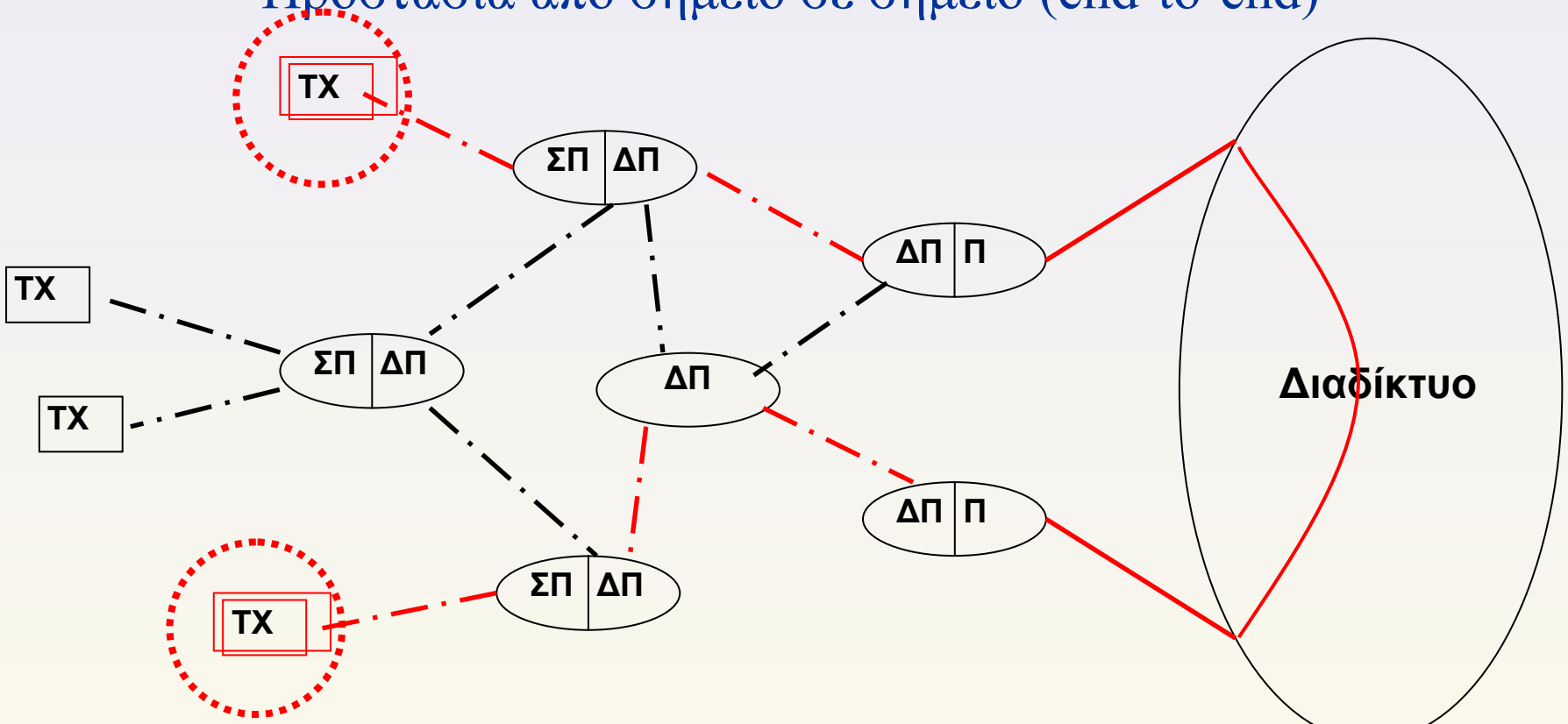


ΣΠ – Σημείο Πρόσβασης (Access Point)
Π – Πύλη (Gateway)
ΔΠ – Δρομολογητής Πλέγματος (Mesh Router)
ΤΧ – Τελικός Χρήστης (Mesh Client)

Ασύρματη ζεύξη
Ενσύρματη σύνδεση

Προστασία του ασύρματου μέσου

Προστασία από σημείο σε σημείο (end-to-end)



ΣΠ – Σημείο Πρόσβασης (Access Point)
Π – Πύλη (Gateway)
ΔΠ – Δρομολογητής Πλέγματος (Mesh Router)
ΤΧ – Τελικός Χρήστης (Mesh Client)

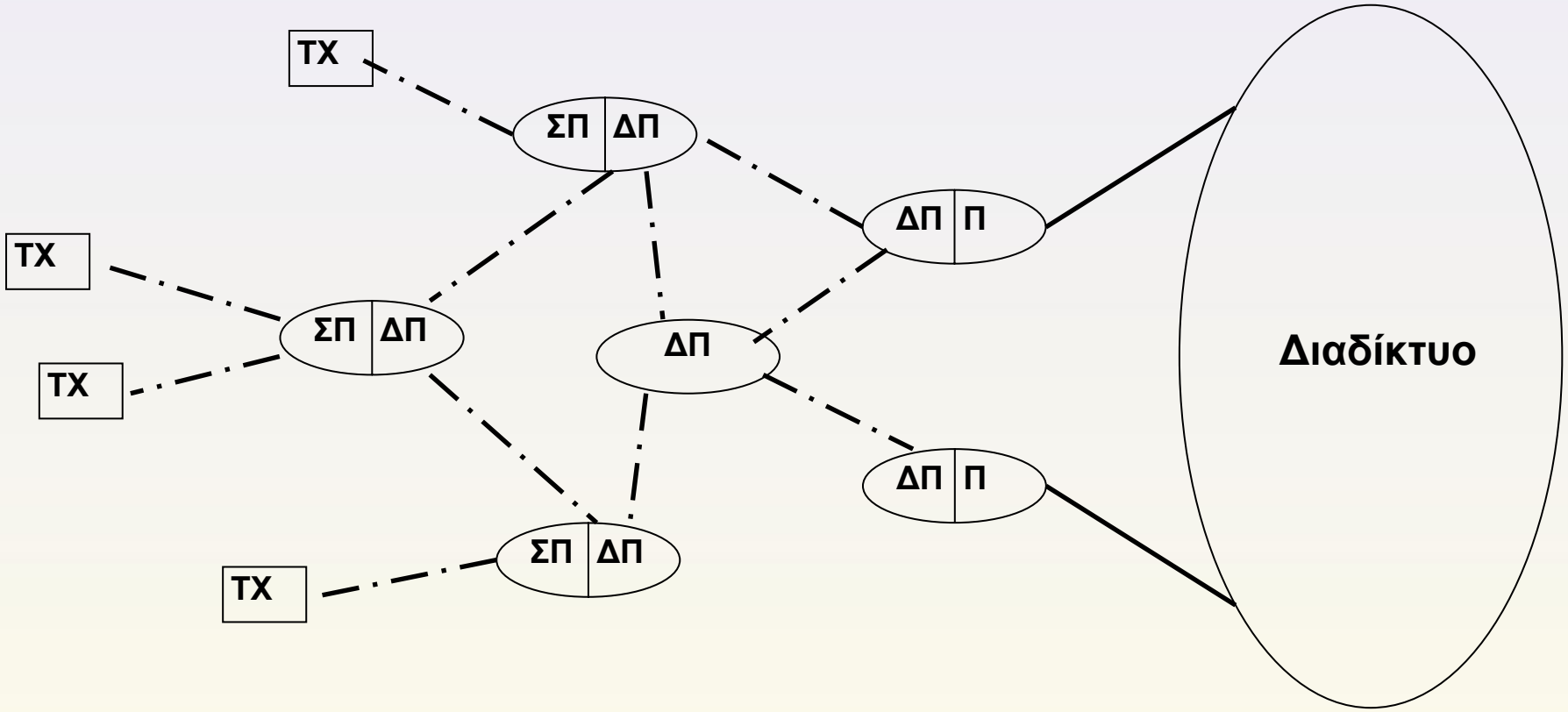
Ασύρματη ζεύξη
Ενσύρματη σύνδεση

Προστασία του ασύρματου μέσου

- Προστασία από σημείο σε σημείο (end-to-end)
  - Η πληροφορία προστατεύεται από τον χρήστη μέχρι το τελικό άκρο της επικοινωνίας τους
  - Είναι ανεξάρτητη από τους ενδιάμεσους δρομολογητές πλέγματος
  - Οι ενδιάμεσοι δρομολογητές πλέγματος δεν μπορούν να ελέγξουν την ακεραιότητα των δεδομένων που προωθούν
  - Προστατεύει τα δεδομένα και εκτός δικτύου πλέγματος (όταν περνάνε και από το Internet)
  - Ο μηχανισμός προστασίας πρέπει να υποστηρίζεται και από τους δύο τελικούς χρήστες

Προστασία του ασύρματου μέσου

Προστασία από διασύνδεση σε διασύνδεση (link-by-link)

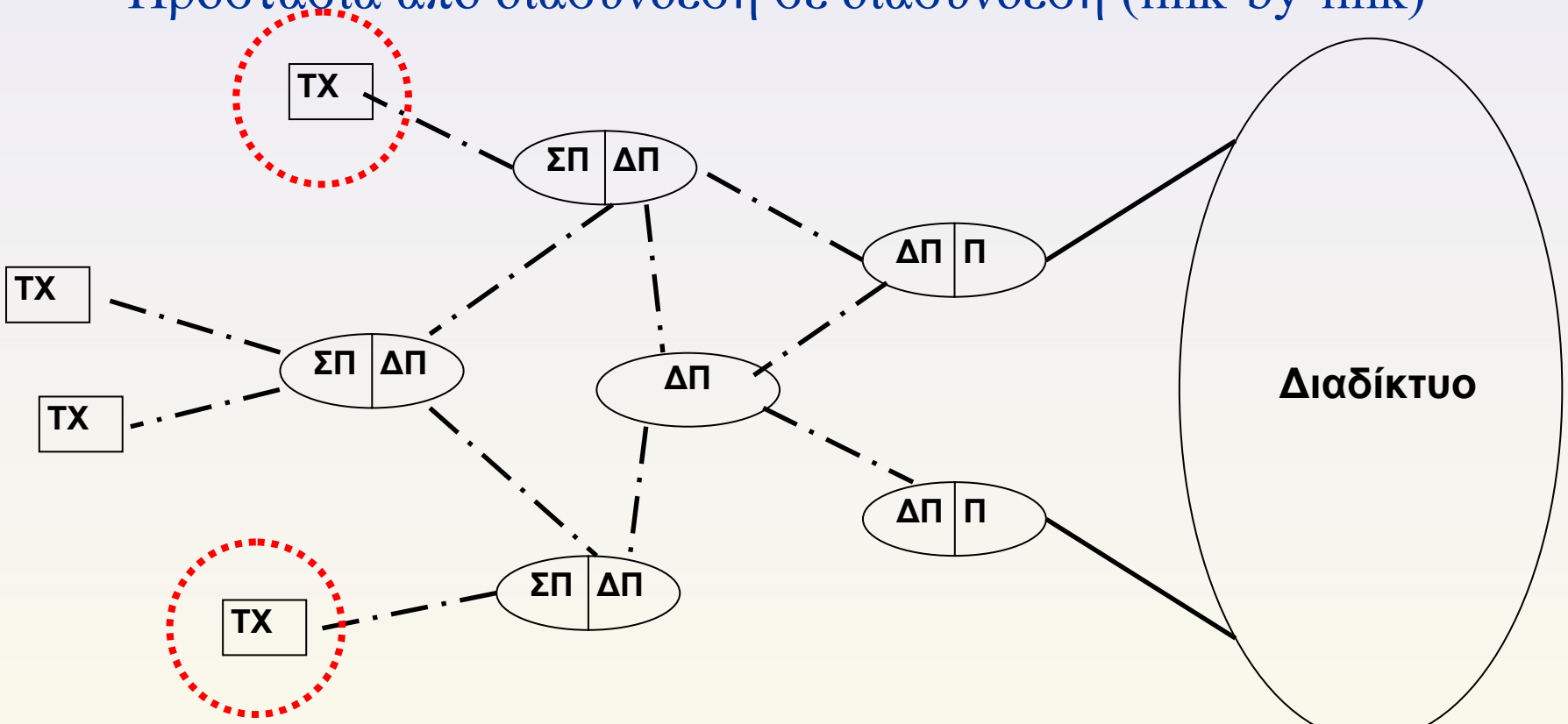


ΣΠ – Σημείο Πρόσβασης (Access Point)
Π – Πύλη (Gateway)
ΔΠ – Δρομολογητής Πλέγματος (Mesh Router)
ΤΧ – Τελικός Χρήστης (Mesh Client)

Ασύρματη ζεύξη
Ενσύρματη σύνδεση

Προστασία του ασύρματου μέσου

Προστασία από διασύνδεση σε διασύνδεση (link-by-link)

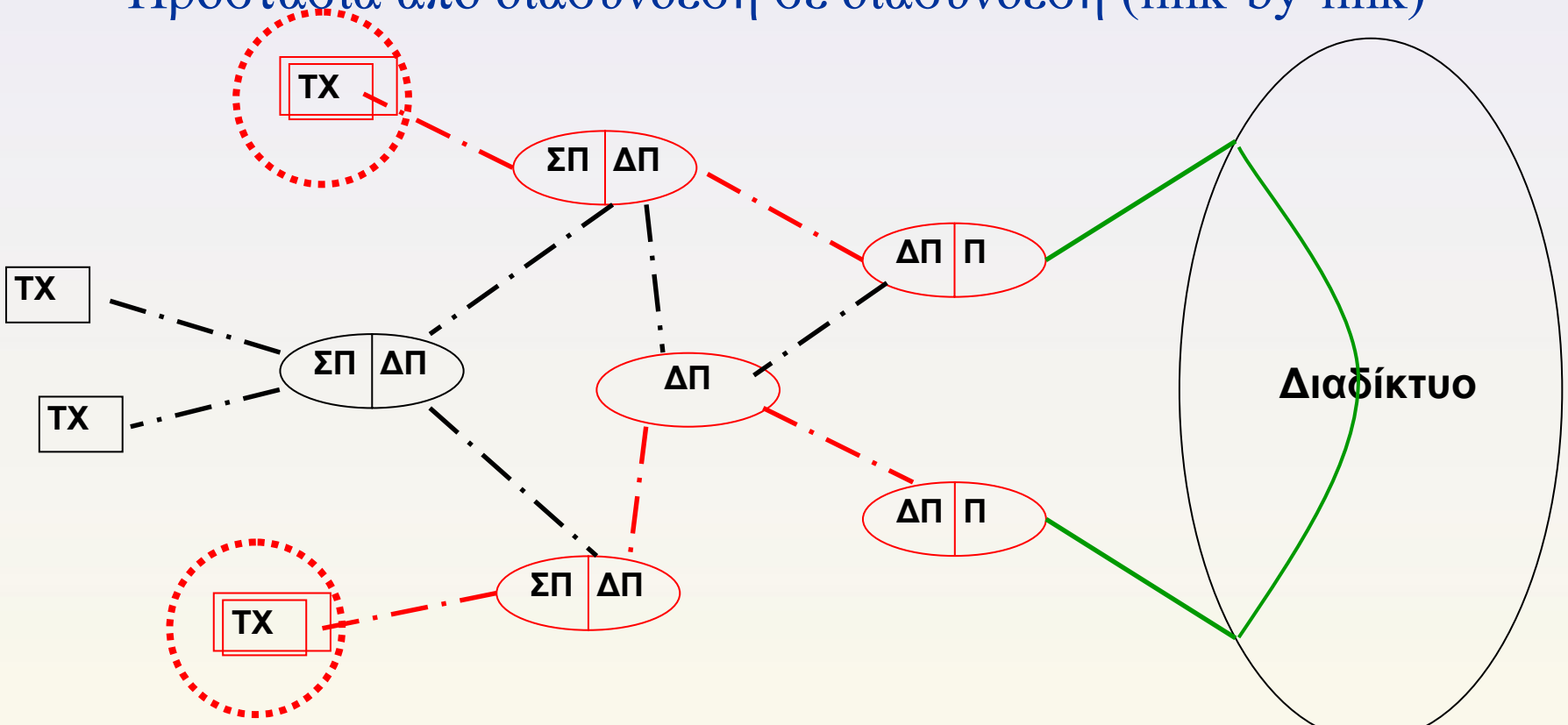


ΣΠ – Σημείο Πρόσβασης (Access Point)
Π – Πύλη (Gateway)
ΔΠ – Δρομολογητής Πλέγματος (Mesh Router)
ΤΧ – Τελικός Χρήστης (Mesh Client)

Ασύρματη ζεύξη
Ενσύρματη σύνδεση

Προστασία του ασύρματου μέσου

Προστασία από διασύνδεση σε διασύνδεση (link-by-link)



ΣΠ – Σημείο Πρόσβασης (Access Point)
Π – Πύλη (Gateway)
ΔΠ – Δρομολογητής Πλέγματος (Mesh Router)
ΤΧ – Τελικός Χρήστης (Mesh Client)

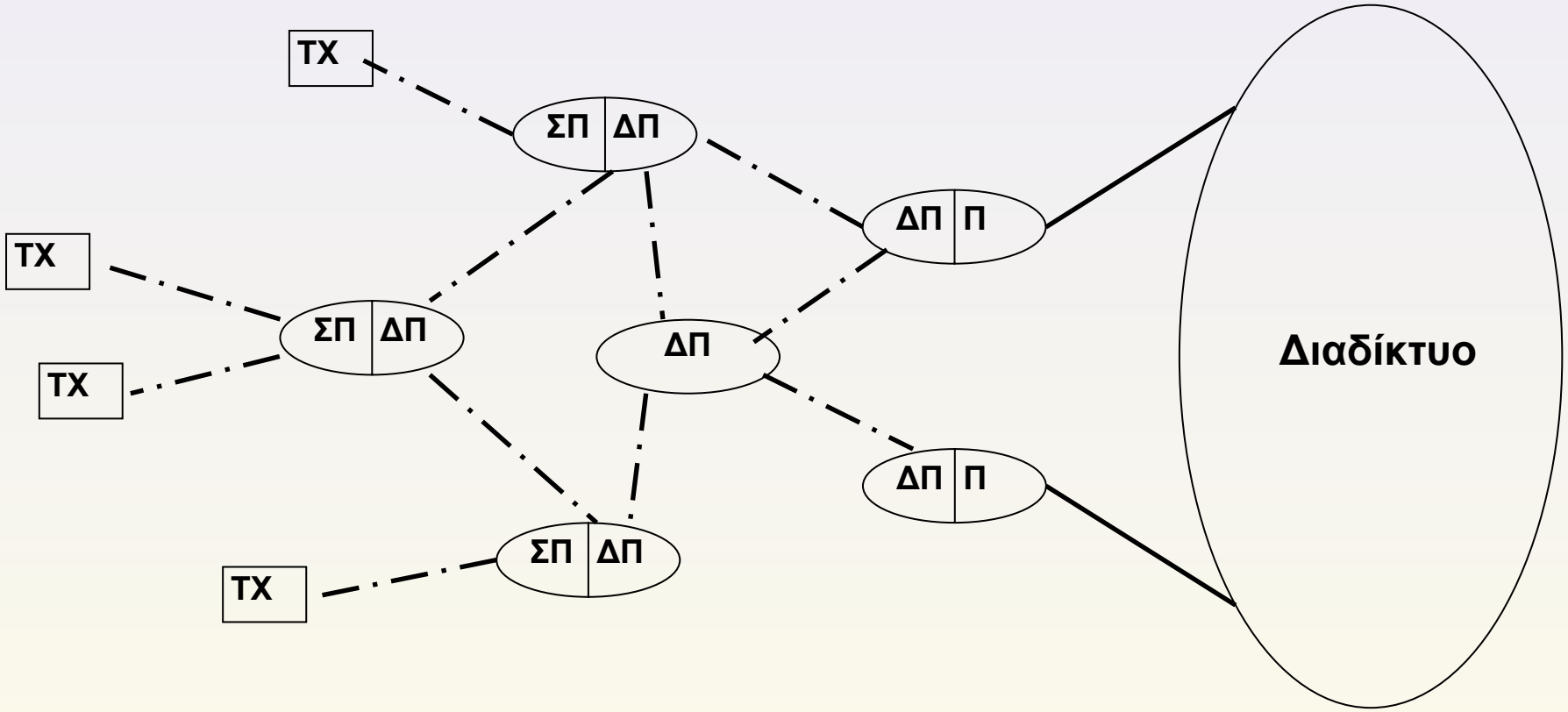
Ασύρματη ζεύξη
Ενσύρματη σύνδεση

Προστασία του ασύρματου μέσου

- Προστασία από διασύνδεση σε διασύνδεση (link-by-link)
  - Η πληροφορία προστατεύεται βήμα προς βήμα (στις ασύρματες ζεύξεις)
  - Η προστασία εξαρτάται από τους ενδιάμεσους δρομολογητές πλέγματος
  - Τα επίπεδα προστασίας και οι μηχανισμοί μπορεί να διαφέρουν μεταξύ διαφορετικών ζεύξεων
  - Οι ενδιάμεσοι δρομολογητές πλέγματος μπορούν να
    - ελέγξουν την ακεραιότητα των δεδομένων που προωθούν
    - Επέμβουν στα δεδομένα αυτά
  - Δεν προστατεύει τα δεδομένα εκτός δικτύου πλέγματος (όταν περνάνε και από το Internet)
  - Προστατεύονται τα μέτα-δεδομένα (διευθύνσεις, ονόματα κτλ)
  - Ενδείκνυται η χρήση σε συνδυασμό με προστασία από σημείο σε σημείο

Προστασία του ασύρματου μέσου

Προστασία τμημάτων διαδρομής

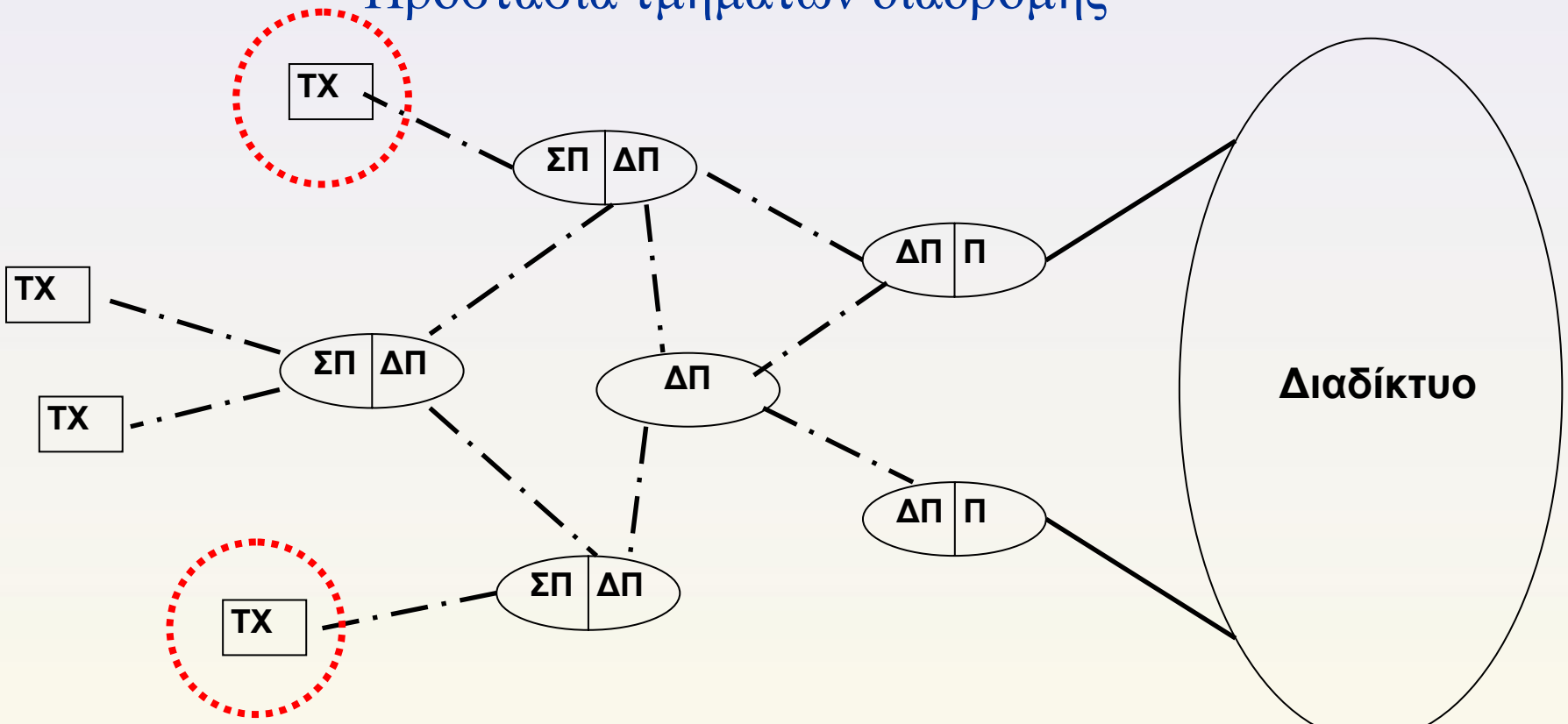


ΣΠ – Σημείο Πρόσβασης (Access Point)
Π – Πύλη (Gateway)
ΔΠ – Δρομολογητής Πλέγματος (Mesh Router)
ΤΧ – Τελικός Χρήστης (Mesh Client)

Ασύρματη ζεύξη
Ενσύρματη σύνδεση

Προστασία του ασύρματου μέσου

Προστασία τμημάτων διαδρομής

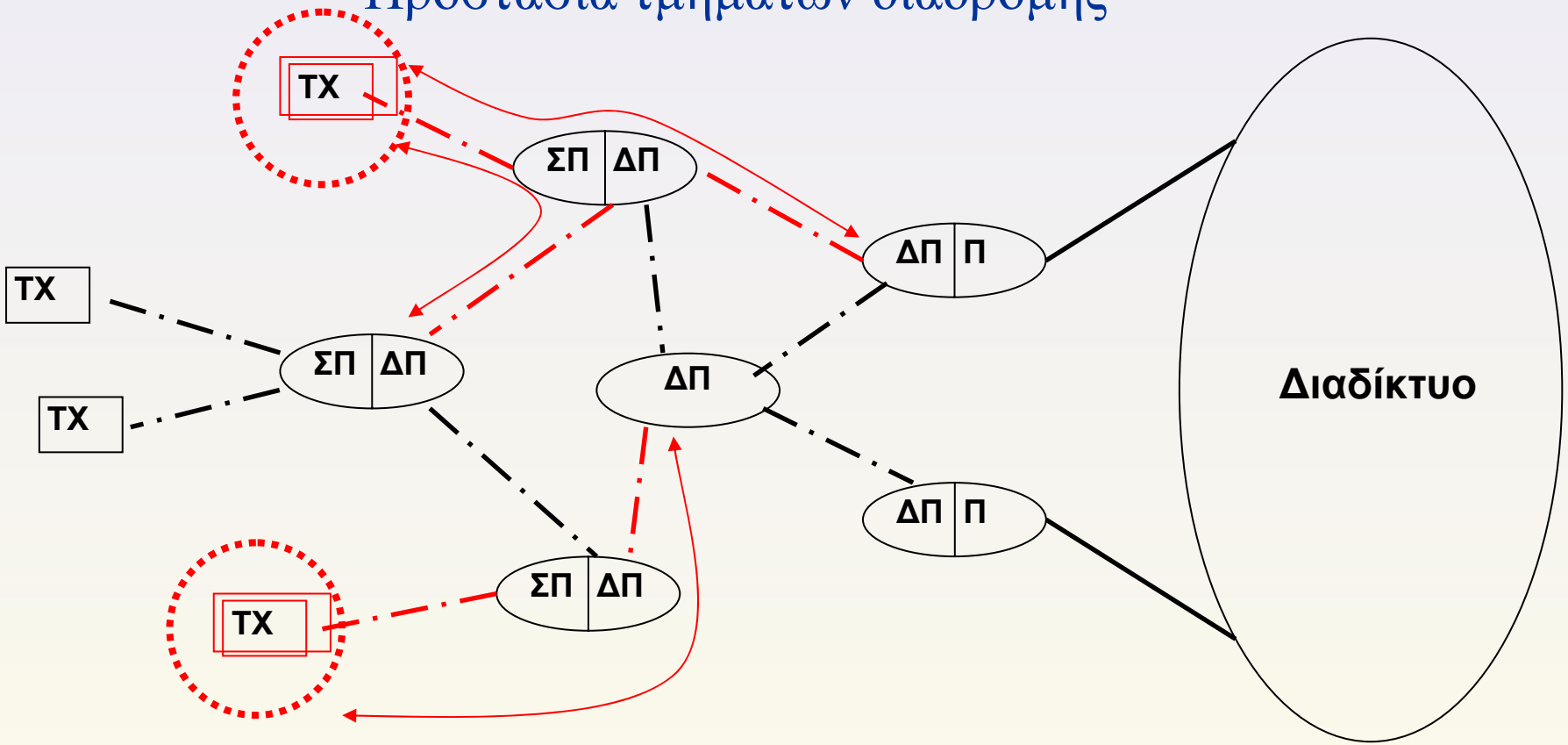


ΣΠ – Σημείο Πρόσβασης (Access Point)
Π – Πύλη (Gateway)
ΔΠ – Δρομολογητής Πλέγματος (Mesh Router)
ΤΧ – Τελικός Χρήστης (Mesh Client)

Ασύρματη ζεύξη
Ενσύρματη σύνδεση

Προστασία του ασύρματου μέσου

Προστασία τμημάτων διαδρομής



ΣΠ – Σημείο Πρόσβασης (Access Point)
Π – Πύλη (Gateway)
ΔΠ – Δρομολογητής Πλέγματος (Mesh Router)
ΤΧ – Τελικός Χρήστης (Mesh Client)

Ασύρματη ζεύξη
Ενσύρματη σύνδεση

Προστασία του ασύρματου μέσου

- Προστασία τμημάτων διαδρομής
  - Χρήσιμη μέθοδος σε περιβάλλοντα πολλαπλών παρόχων
  - Προστασία μεταξύ τελικού χρήστη και σημείου πρόσβασης
  - Προστασία σε τμήματα του δικτύου πλέγματος που ανήκουν σε άλλο πάροχο
  - Προστασία μεταξύ τελικού χρήστη και πύλης
  - Προστασία μεταξύ τελικού χρήστη και σημείου συλλογής

Προστασία του ασύρματου μέσου

- Προστασία από ανάλυση κίνησης
  - Χρήση προστασίας διασύνδεσης
  - Εσκεμμένη εισαγωγή περιττών δεδομένων (χωρίς πληροφορία)
    - Ο επιτιθέμενος δεν μπορεί να διαχωρίσει τα περιττά δεδομένα από την πραγματική πληροφορία
    - Μειονέκτημα: δημιουργία περισσότερης κίνησης (φόρτου) στο δίκτυο
    - Αντίμετρο: δυναμική τροποποίηση του όγκου των περιττών δεδομένων ανάλογα με τον φόρτου πραγματικής πληροφορίας του δικτύου

Επίλογος

- Ασφαλής δρομολόγηση δεδομένων
- Διαχείριση κρυπτογραφικών κλειδιών
- Ανίχνευση εισβολέων και ανάκαμψη

Περισσότερες πληροφορίες: www.eu-mesh.eu

EU-MESH: **Enhanced, Ubiquitous and Dependable Broadband Access using MESH Networks**

FP7 ICT-1-1.1: The Network of the Future

Project No. 215320

Σχετική βιβλιογραφία

I. Askoxylakis, B. Bencsath, L. Buttyan, L. Dora, V. Siris, D. Szili, I. Vajda

Securing Multi-operator Based QoS-aware Mesh Networks: Requirements and Design Options

International Journal on Wireless Communications and Mobile Computing,

Wiley InterScience, DOI: 10.1002/wcm.0000

Ιωάννης Ασκοξυλάκης, Βασίλειος Σύρης και Απόστολος Τραγανίτης

Απαιτήσεις ασφάλειας και επιλογές σχεδίασης για την πιστοποίηση ταυτότητας και τον έλεγχο πρόσβασης τελικών κινούμενων χρηστών σε ασύρματα δίκτυα πλέγματος πολλαπλών συνεργαζόμενων παρόχων`

Τεχνική αναφορά
Οκτώβριος 2008
Ίδρυμα Τεχνολογίας και Έρευνας
Ινστιτούτο Πληροφορικής

Ασύρματα δίκτυα πλέγματος