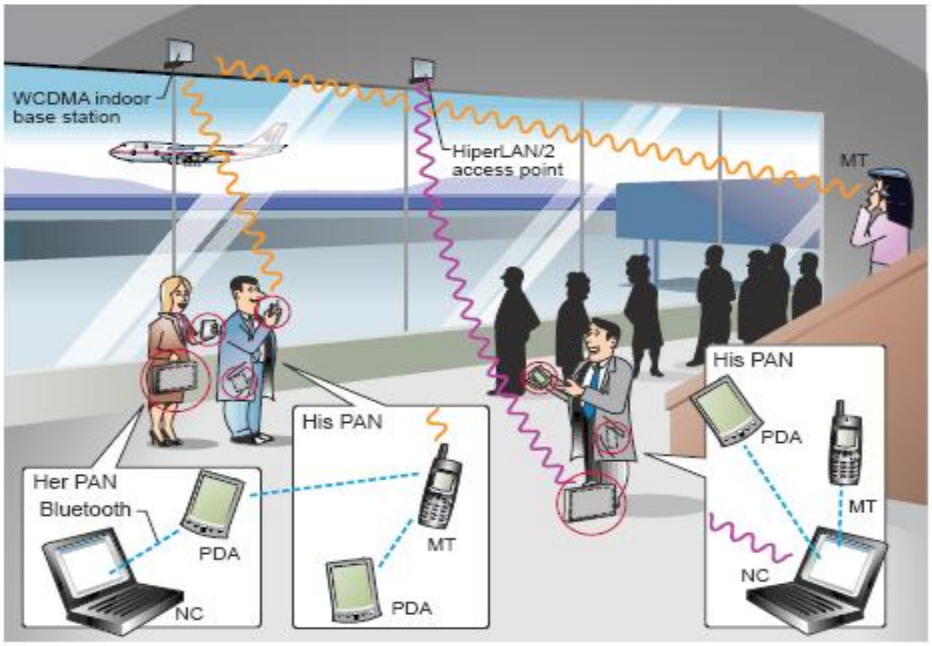
Πανεπιστήμιο Πειραιώς
ΤΜΗΜΑ ΔΙΔΑΚΤΙΚΗΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ
ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΠΜΣ – ΨΗΦΙΑΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ & ΔΙΚΤΥΑ

Ασφαλής δρομολόγηση Ad-hoc δικτύων



Όνομα φοιτητή: Τεμένος Παύλος
Όνομα διδάσκοντος: κ. Ξενάκης Χρήστος

Πειραιάς 2008

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

1. Εισαγωγή στις Ασύρματες Τεχνολογίες

Οι ασύρματες τεχνολογίες επιτρέπουν σε μία η περισσότερες συσκευές να επικοινωνήσουν μεταξύ τους χωρίς φυσικές συνδέσεις, χωρίς δηλαδή την ανάγκη για καλωδίωση. Για την μετάδοση των δεδομένων χρησιμοποιούν την 'ραδιο-συχνότητα' (radio-frequency), όπου παλία η μετάδοση γινόταν μέσω των καλωδίων.

Οι ασύρματες τεχνολογίες κυμαίνονται από πολύπλοκα συστήματα, όπως τα Wireless Local Area Network (WLAN), μέχρι τις απλές συσκευές όπως μικρόφωνα, ακουστικά και άλλες απλές συσκευές που δεν επεξεργάζονται η αποθηκεύουν πληροφορία. Περιλαμβάνουν επίσης τις συσκευές με υπέρυθρες ακτίνες (IR), όπως τα remote controls, ασύρματα πληκτρολόγια, ασύμρατα ποντίκια και γενικά συσκευές που απαιτούν απευθείας οπτική επαφή μεταξύ της συσκευής που μεταδίδει τα κύματα και της συσκευής που τα λαμβάνει.

1.1 Ασύρματα δίκτυα

Τα ασύρματα δίκτυα χρησιμεύουν ως ο μηχανισμός για την μεταφορά δεδομένων μεταξύ των συσκευών και των παραδοσιακών ασύρματων δικτύων (π.χ διαδίκτυο) μαζί με άλλες συσκευές.
Υπάρχουν πολλά και διαφορετικά ασύρματα δίκτυα, αλλά συχνά ταξινομούνται σε τρεις ομάδες ανάλογα με την ακτίνα κάλυψης τους: Wireless Wide Area Networks (WWANs), Wireless Local Area Networks (WLANs) και Wireless Personal Area Networks (WPANs). Τα WWANs περιλαμβάνουν τεχνολογίες ευρύας περιοχής κάλυψης όπως το GSM (Global System for Mobile Communications), Mobitex και CDPD (Cellural Digital Packet Data). Τα WLAN αντιπροσωπεύουν τα ασύρματα δίκτυα τοπικής περιοχής όπου περιλαμβάνουν το 802.11 και το HiperLan. Τέλος το WPAN αντιπροσωπεύει το ασύρματο δίκτυο προσωπικής περιοχής όπως για παράδειγμα το Bluetooth και τις υπέρυθρες ακτίνες (IR).

Όλες αυτές οι τεχνολογίες λαμβάνουν και διαβιβάζουν τα διάφορα δεδομένα χρησιμοποιώντας ηλεκτρομαγνητικά κύματα.

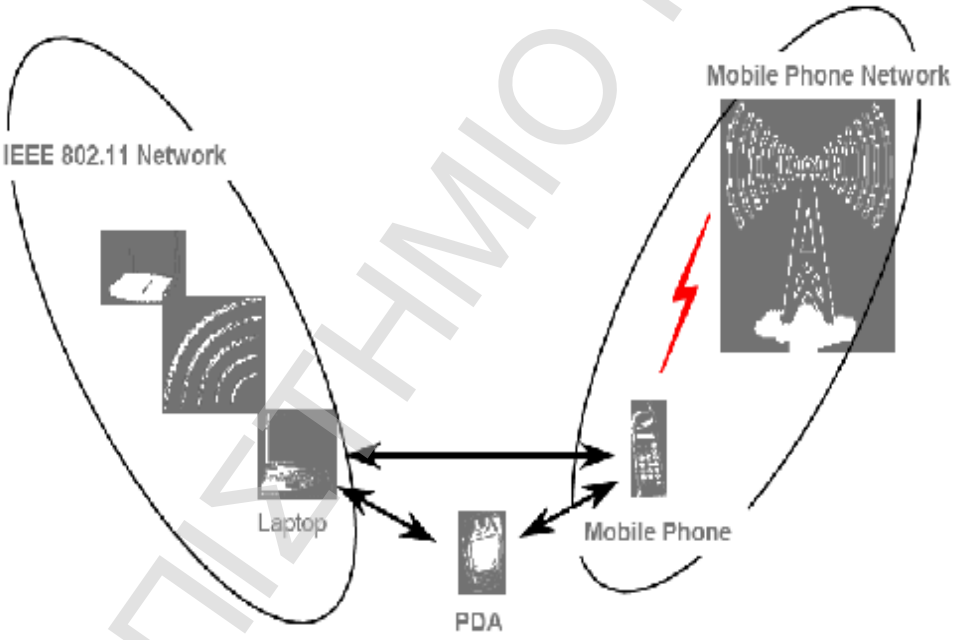
1.1.2 Wireless LANS

Τα WLANs επιτρέπουν μεγαλύτερη ευελιξία και φορητότητα από τα παραδοσιακά ενσύρματα δίκτυα τοπικής περιοχής. Αντίθετα από τα παραδοσιακά LANs τα οποία απαιτούν καλώδιο για την σύνδεση του υπολογιστή ενός χρήστη στο δίκτυο, ένα WLAN συνδέει υπολογιστές και άλλες συσκευές στο δίκτυο χρησιμοποιώντας μια συσκευή σημείου

πρόσβασης, το γνωστό ως access point (AP). Ένα AP επικοινωνεί με συσκευές εξοπλισμένες με προσαρμοστές (adaptors) ασύρματων δικτύων (συνδέεται με Ethernet LAN μέσω μίας θύρας RJ-45). Οι access point συσκευές έχουν ακτίνα κάλυψης γύρω στα 100 μέτρα περίπου.

1.1.3 Ad hoc δίκτυα

Τα ad hoc δίκτυα όπως θα δούμε λεπτομερώς πιο κάτω είναι δίκτυα τυχαία διαμορφωμένα, χωρίς σταθερή υποδομή δικτύου. Βασίζονται στο σύστημα master-slave και συνδέονται με ασύρματες συνδέσεις ώστε να μπόρουν να επικοινωνούν μεταξύ τους οι συσκευές. Είναι δηλαδή δίκτυα σχεδιασμένα να ενώνουν απομακρυσμένες συσκευές όπως φορητούς υπολογιστές και PDAs. Ένα παράδειγμα ad hoc δικτύου φαίνεται στην πιο κάτω εικόνα.



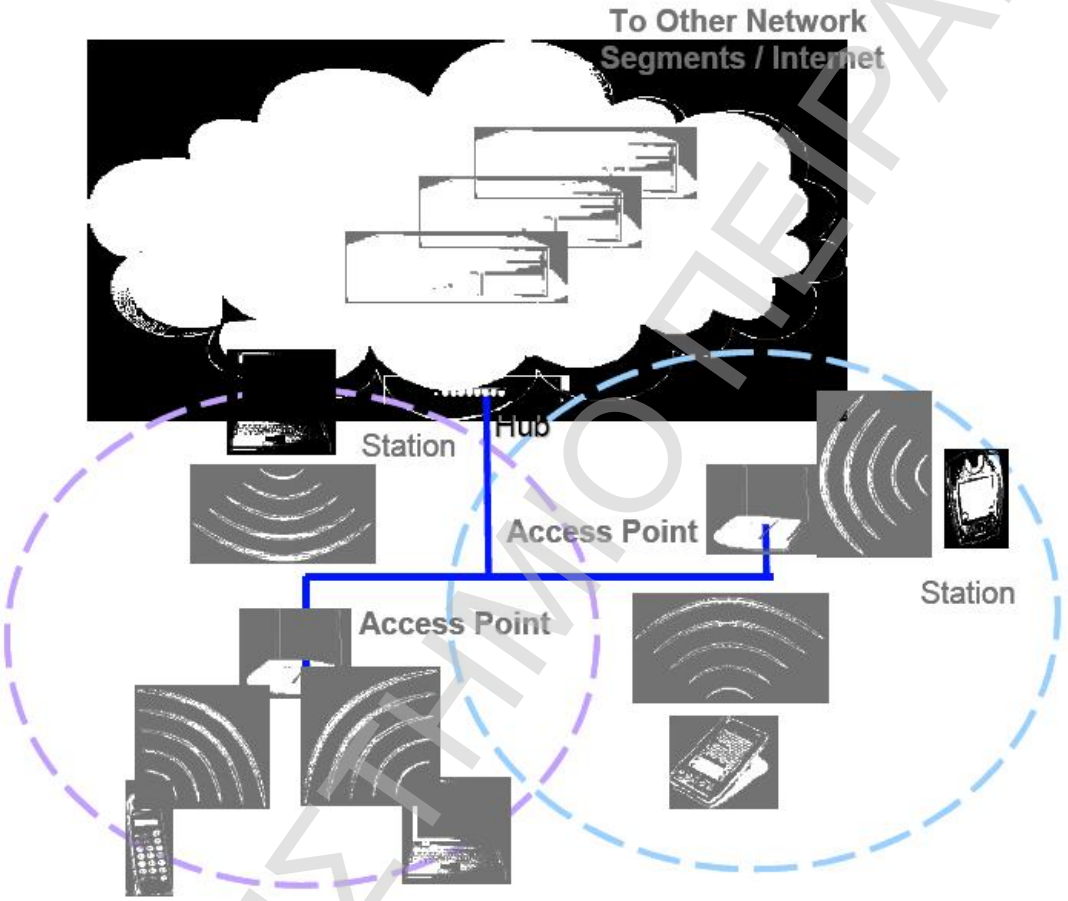
1.2 Ασύρματα πρότυπα

Τα WLANs βασίζονται στα IEEE 802.11 πρότυπα, τα οποία πρωτοεμφανίστηκαν το 1997. Η IEEE σχεδίασε την σειρά 802.11 προτύπων κυρίως για να υποστηρίζονται υψηλοί ρυθμοί μετάδοσης δεδομένων, όπως τα δίκτυα Ethernet.

Τα 802.11 πρότυπα επιτρέπουν σε συσκευές να ενώνονται σε peer-to-peer (P2P) δίκτυα ή δίκτυα βασισμένα σε ένα σταθερό access point όπου όλοι οι σταθμοί μπορούν να έχουν επικοινωνία.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Η βασική τοπολογία ενός WLAN φαίνεται στην πιο κάτω εικόνα.



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

2. AD-HOC ΔΙΚΤΥΑ

2.1 Τι είναι ένα ad-hoc δίκτυο

Ad-hoc δίκτυο είναι ένα δίκτυο διαμορφομένο χωρίς κανένα κεντρικό administration και αποτελείται από κινητούς σταθμούς που χρησιμοποιούν μια ασύρματη διεπαφή για να στέλλουν πακέτα δεδομένων. Δεδομένου ότι οι κόμβοι σε ένα δίκτυο αυτού του είδους μπορούν να χρησιμεύσουν ως routers και hosts, μπορούν να διαβιβάζουν πακέτα για λογαριασμό άλλων σταθμών και να τρέχουν τις εφαρμογές χρηστών.

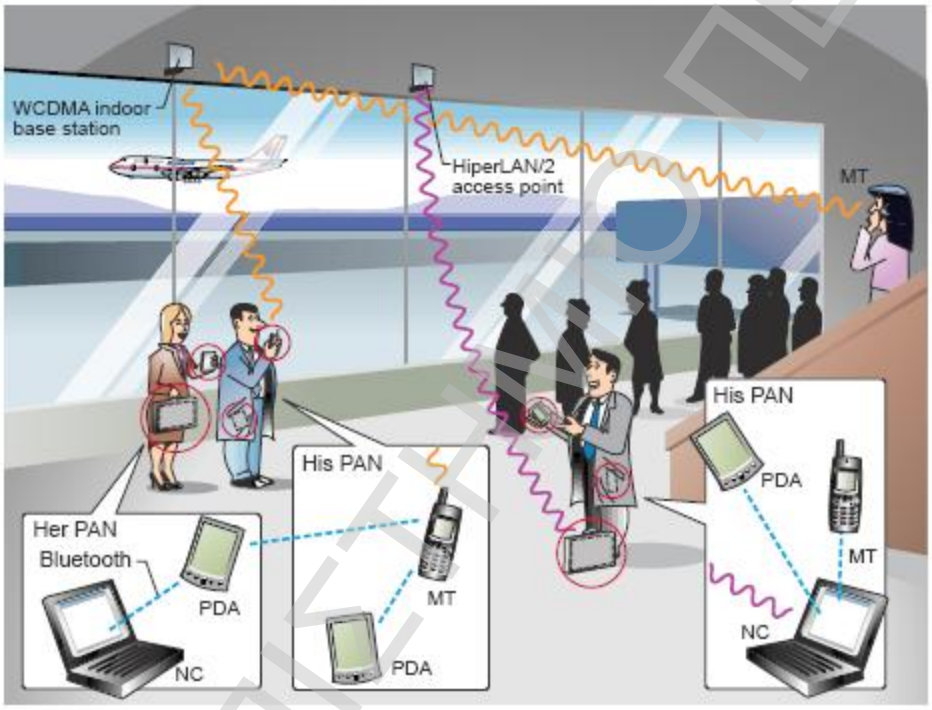
Οι ρίζες της ad-hoc δικτύωσης μπορούν να επισημανθούν γύρω στο 1968, όταν άρχισε η εργασία για το δίκτυο ALOHA όπου στόχος αυτού του δικτύου ήταν να συνδεθούν διάφορες εκπαιδευτικές εγκαταστάσεις στην Χαβάη. Αν και οι σταθεροί σταθμοί υιοθετήθηκαν, το πρωτόκολλο ALOHA παραχωρήθηκε στη distributed channel-access διαχείρηση και ως εκ τούτου παρείχε μια βάση για την επόμενη ανάπτυξη των distributed channel-access μοντέλων που ήταν κατάλληλα για την ad-hoc δικτύωση. Το πρωτόκολλο ALOHA από μόνο του ήταν ένα single-hop πρωτόκολλο που δεν υποστήριζε εγγενώς τη δρομολόγηση. Αντί αυτού κάθε κόμβος έπρεπε να είναι προσιτός από όλους τους άλλους συμμετεχόντες κόμβους.

Εμπνευσμένο από το δίκτυο ALOHA και την πρόωρη ανάπτυξη της σταθερού δικτύου μεταγωγής πακέτου (packet switching), το DARPA άρχισε να λειτουργεί το 1973 για το PRnet (packet radio network) σε ένα multihop δίκτυο. Το PRnet παρείχε τους μηχανισμούς για τη λειτουργία διαχείρισης κεντρικά καθώς επίσης και σε distributed βάση. Σαν πρόσθετο όφελος, συνειδητοποιήθηκε ότι οι multihopping τεχνικές αύξησαν την χωρητικότητα των δικτύων, δεδομένου ότι μια περιοχή μπορούσε να επαναχρησιμοποιηθεί για τις ταυτόχρονες αλλά φυσικά χωριστές συνόδους multihop.

Αν και πολλά πειραματικά δίκτυα packet-radio αναπτύχθηκαν αργότερα, αυτά τα ασύρματα συστήματα ποτέ δεν είχαν σημαντική καταναλωτική χρήση. Όταν αναπτύχθηκε το 802.11 προτύπο για τα ασύρματα δίκτυα τοπικής περιοχής (WLAN) η IEEE αντικατέστησε τα packet-radio δίκτυα με τα ad-hoc δίκτυα. Τα packet-radio δίκτυα είχαν συνδεθεί με τα multihop δίκτυα σε διάφορες στρατιωτικές υπηρεσίες, και αλλάζοντας τους όνομα η IEEE έλπιζε ότι με αυτό τον τρόπο να επεκταθούν περισσότερο.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Σήμερα, ένας από τους στόχους των ad-hoc δικτύων περιλαμβάνει το πιο κάτω σενάριο όπως απεικονίζεται στο σχήμα 1, όπου οι άνθρωποι έχουν συσκευές με τις οποίες μπορούν να ενωθούν στο δίκτυο. Μια συσκευή ενός χρήστη π.χ μπορεί να συνδεθεί με μια άλλη και να συνδεθούν με ένα σημείο πληροφοριών για να παρακολουθούν ανανεώσεις όπως για παράδειγμα στις αναχωρήσεις, από αυτά που βλέπουμε τώρα συχνά στα αεροδρόμια, και να ανακτήσουν διάφορες πληροφορίες για την ακριβή ώρα αναχώρησης ή αλλαγή πόρτας εξόδου κ.λ.π. Αυτό το απλό σενάριο στο αεροδρόμιο περιέχει ένα μίγμα απλών και πολλαπλών radio hops.



Για να αρχίσει κάποιος να εκτιμά σωστά τα ad-hoc δίκτυα, θα δούμε πιο κάτω μερικές παρατηρήσεις για την ασύρματη επικοινωνία, αρχίζοντας με τα παρόντα κυψελοειδή συστήματα, τα οποία στηρίζονται σε μεγάλο βαθμό στην υποδομή: η κάλυψη παρέχεται από τους σταθμούς βάσης, οι πηγές σημάτων ρυθμίζονται από μια κεντρική θέση, και οι υπηρεσίες είναι ενσωματωμένες στο σύστημα. Όλα τα πιο πάνω οδηγούν στην σωστή και προβλεπόμενη υπηρεσία των παρόντων κυψελωτών συστημάτων.

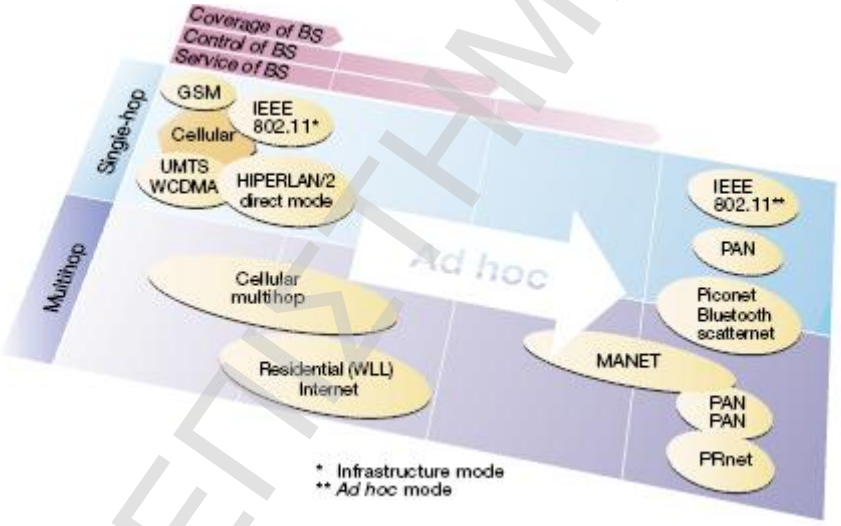
Δεδομένης της απομάκρυνσης μας από την κεντρική διαχείριση, βρισκόμαστε προς την κατεύθυνση της ad-hoc

λειτουργίας, η οποία επίσης μπορεί να ταξινομηθεί από την χρησιμοποίηση των απλών και πολλάπλών hops.

Χωρίς να έχει εγκαταλειφθεί εντελώς ο έλεγχος, αλλά με άμεσο τρόπο επικοινωνίας σε HiperLAN/2, τα παρακείμενα τερματικά μπορούν να επικοινωνήσουν απευθείας το ένα με το άλλο. Κατά συνέπεια, η μεταφορά της κίνησης δεν εξαρτάται εξ ολοκλήρου από την κάλυψη που παρέχεται από τα σημεία πρόσβασης.

Η εξάρτηση στην κεντρική administreted κάλυψη μειώνεται περαιτέρω όταν τα end-user τερματικά αναμεταδίδουν την κυκλοφορία σε μια multihop μορφή μεταξύ άλλων τερματικών και του σταθμού βάσης. Κάτι παρόμοιο ισχύει και για τα εμπορικά και κατοικημένα ασύρματα local loop (WLL) multihop συστήματα πρόσβασης.

Πλήρως αποκεντρωμένα σήματα, πρόσβαση, και τεχνολογίες δρομολόγησης (Bluetooth, IEEE 802.11 , ad-hoc δίκτυα, PRnet, το κινητό ad-hoc δίκτυο (MANET), καθώς και άλλες έννοιες όπως το PAN (personal area network) ή PAN-to-PAN επικοινωνία, ταιριάζουν λίγο η πολύ με την έννοια του ad-hoc δικτύου.



2.2 Εφαρμογές ad-hoc δικτύων

Τα κινητά ad-hoc δίκτυα αποτελούν την εστίαση πολλών πρόσφατων προσπαθειών έρευνας και ανάπτυξης. Μέχρι τώρα, τα ad-hoc packet-radio δίκτυα έχουν εξεταστεί και χρησιμοποιηθεί κυρίως σε στρατιωτικές εφαρμογές, όπου μια αποκεντρωμένη διαμόρφωση δικτύων αποτελεί ένα πλεονέκτημα ή ακόμα και μια ανάγκη.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Στον εμπορικό τομέα, ο ασύρματος εξοπλισμός, οι φορητοί υπολογιστές και άλλες συσκευές είχαν μια ιδιαίτερα τσουχτερή τιμή. Εντούτοις, καθώς η ικανότητα των κινητών υπολογιστών αυξάνεται σταθερά, η ανάγκη για απεριόριστη δικτύωση αναμένεται επίσης να αυξηθεί ραγδία.

Τα εμπορικά ad-hoc δίκτυα θα μπορούσαν να χρησιμοποιηθούν σε καταστάσεις όπου καμία υποδομή (σταθερή ή κυψελοειδής) δεν είναι διαθέσιμη. Σε τέτοια παραδείγματα περιλαμβάνονται διαδικασίες διάσωσης σε απομακρυσμένες περιοχές, ή όταν πρέπει η τοπική κάλυψη να επεκταθεί γρήγορα σε ένα μακρινό τόπο κατασκευής. Η ad-hoc δικτύωση θα μπορούσε επίσης να χρησιμοποιηθεί ως ασύρματη δημόσια πρόσβαση σε αστικές περιοχές, παρέχοντας έτσι γρήγορη επέκταση και εκτεταμένη κάλυψη. Τα σημεία πρόσβασης στα δίκτυα αυτού του είδους θα μπορούσαν να χρησιμεύσουν ως stationary radio relay σταθμοί που εκτελούν ad-hoc δρομολόγηση μεταξύ τους και μεταξύ των σταθμών χρηστών. Μερικά από τα σημεία πρόσβασης θα μπορούσαν να περιέχουν επίσης τις πύλες μέσω των οποίων οι χρήστες θα μπορούσαν να συνδεθούν με ένα σταθερό δίκτυο.

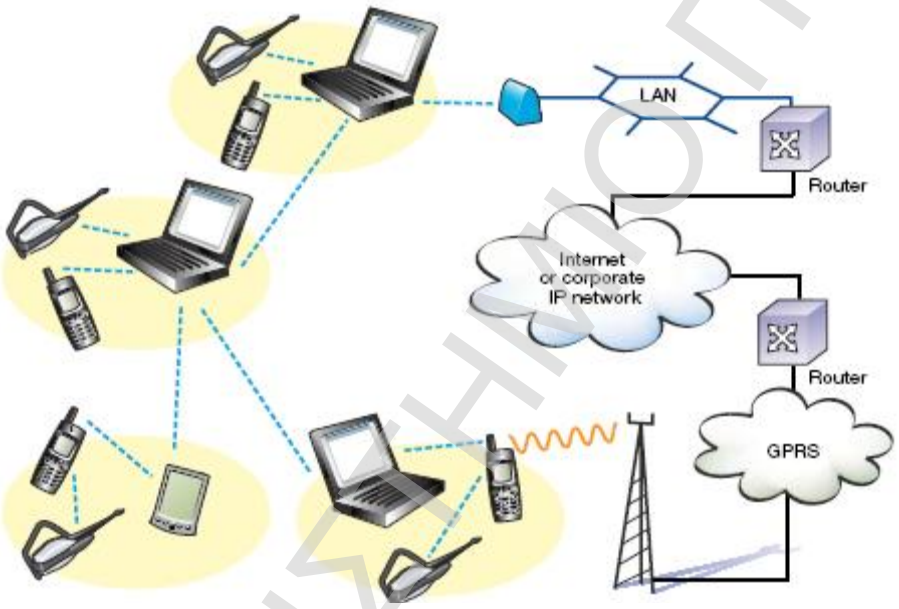
Σε τοπικό επίπεδο, τα ad-hoc δίκτυα που συνδέουν φορητούς υπολογιστές ή palmtop υπολογιστές θα μπορούσαν να χρησιμοποιηθούν για να διαδώσουν και να μοιραστούν τις πληροφορίες μεταξύ των συμμετεχόντων σε μια διάσκεψη. Επίσης μπορεί να είναι κατάλληλοι για την εφαρμογή στα δίκτυα που έχει ο καθένας στο σπίτι όπου οι συσκευές μπορούν να επικοινωνήσουν άμεσα για να αλλάξουν πληροφορίες, όπως audio/video, συναγερμούς, και ενημερώσεις διαμόρφωσης. Ίσως οι πιό εκτεταμένες εφαρμογές σε αυτό το πλαίσιο είναι λίγο-πολύ τα αυτόνομα δίκτυα των διασυνδεμένων εγχώριων ρομπότ που καθαρίζουν, πλένουν τα πιάτα, κόβουν το χορτοτάπητα, επιτηρούν με ασφάλεια το σπίτι και τα λοιπά.

Τα περιορισμένου φάσματος ad-hoc δίκτυα μπορούν να απλοποιήσουν την ενδοεπικοινωνία μεταξύ των διάφορων κινητών συσκευών (όπως ένα κινητό τηλέφωνο ή ένα PDA) με τη διαμόρφωση ενός PAN (Personal Area Network), και με αυτόν τον τρόπο να εξαλείψουν την ανάγκη για καλωδίωση. Αυτό θα μπορούσε επίσης να επεκτείνει την κινητικότητα που παρέχεται από το σταθερό δίκτυο (δηλαδή mobile IP) στους σταθμούς. Το σύστημα Bluetooth είναι ίσως η πιό ελπιδοφόρα τεχνολογία στα πλαίσια της προσωπικής δικτύωσης.

2.3 Personal Area Network

Από την άποψη του παραδοσιακού κινητού δικτύου, ένα βασισμένο σε PAN Bluetooth ανοίγει νέους ορίζοντες στην

επέκταση των κινητών δικτύων. Κάποιος σε ένα ταξίδι π.χ, που έχει πρόσβαση σε ένα Bluetooth PAN θα μπορούσε να χρησιμοποιήσει το GPRS/UMTS κινητο του τηλέφωνο για να μπει στο διαδίκτυο. Από την άποψη του φορτίου κυκλοφορίας στο δίκτυο, η συνολική κυκλοφορία του PAN θα υπέρβαινε αυτή του κινητού τηλεφώνου. Επιπλέον, εάν τα Bluetooth PANs θα μπορούσαν να διασυνδεθούν με τα scatternets, αυτή η ικανότητα θα αυξανόταν. Το σχήμα 3 παρουσιάζει ένα σενάριο στο οποίο χρησιμοποιούνται 4 Bluetooth PANs. Τα PANs διασυνδέονται μέσω των φορητών υπολογιστών με συνδέσεις Bluetooth. Επιπλέον, δύο από τα PANs συνδέονται με ένα IP backbone δίκτυο, ένα μέσω ενός σημείου πρόσβασης του τοπικού LAN και το άλλο μέσω ενός GPRS/UMTS τηλεφώνου.



Εικόνα 3

Ένα PAN μπορεί επίσης να καλύψει τεχνολογίες διαφορετικής πρόσβασης. Παραδείγματος χάριν, ένας φορητός υπολογιστής θα μπορούσε να έχει μια ασύρματη LAN (WLAN) διεπαφή (όπως ieee 802.11 ή HiperLAN/2) που θα παρέχει την πρόσβαση στο δίκτυο όταν χρησιμοποιείται ο υπολογιστής. Κατά συνέπεια, το PAN θα ωφελούταν πολύ από το άθροισμα όλων των τεχνολογιών πρόσβασης που χρησιμοποιούν οι PAN συσκευές. Δεδομένου ότι η PAN έννοια ωριμάζει, θα επιτρέψει σε νέες συσκευές και νέες τεχνολογίες πρόσβασης να ενσωματωθούν στο PAN πλαίσιο. Πρέπει επίσης να εξαλειφθεί η ανάγκη δημιουργίας υβριδικών συσκευών, όπως ένας συνδυασμός PDA- κινητού τηλεφώνου επειδή το PAN δίκτυο θα επιτρέψει αντ' αυτού την ασύρματη ολοκλήρωση. Με άλλα λόγια, δεν θα

είναι απαραίτητο να ανταλλαχτεί η μορφή για τη λειτουργία.

2.4 Χαρακτηριστικά και απαιτήσεις

Σε αντίθεση με την παραδοσιακή καλωδίωση ή τα ασύρματα δίκτυα, ένα ad-hoc δίκτυο θα μπορούσε να λειτουργήσει σε ένα περιβάλλον δικτύων στο οποίο μερικοί ή όλοι οι σταθμοί είναι κινητοί. Σε αυτό το δυναμικό περιβάλλον, οι λειτουργίες δικτύων πρέπει να λειτουργούν σε μια distributed μορφή, δεδομένου ότι οι σταθμοί μπορεί ξαφνικά να μπαίνουν και να βγαίνουν από το δίκτυο. Γενικά, εντούτοις, οι ίδιες βασικές απαιτήσεις χρηστών για τη συνδετικότητα και την διάδωση που ισχύουν για τα παραδοσιακά δίκτυα θα ισχύσουν για τα ad-hoc δίκτυα. Πιο κάτω, θα δούμε μερικά λειτουργικά χαρακτηριστικά και τις επιπτώσεις που έχουν αυτά στις απαιτήσεις για τις σχετικές λειτουργίες δικτύωσης. Θα επικεντρωθούμε στην περίπτωση ενός PAN-oriented ad-hoc δικτύου που αποτελείτε από ένα μίγμα φορητών υπολογιστών, των κινητών τηλεφώνων, και PDAs.

- Distributed Operation:

Ένας σταθμός σε ένα ad-hoc δίκτυο δεν μπορεί να στηριχθεί σε ένα δίκτυο για να υποστηρίξει τις λειτουργίες ασφάλειας και δρομολόγησης. Αντί αυτού αυτές οι λειτουργίες πρέπει να σχεδιαστούν έτσι ώστε να μπορούν να λειτουργούν αποτελεσματικά κάτω από distributed κατάστασεις.

- Dynamic Network Topology:

Η συνδετικότητα μέσα στο δίκτυο πρέπει να διατηρείτε για να επιτρέπει στις εφαρμογές και τις υπηρεσίες να λειτουργουν. Ειδικότερα, αυτό θα επηρεάσει το σχέδιο της δρομολόγησης των πρωτοκόλλων. Επιπλέον, ένας χρήστης στο ad-hoc δίκτυο θα απαιτήσει επίσης την πρόσβαση σε ένα σταθερό δίκτυο (όπως το διαδίκτυο) ακόμα κι αν οι σταθμοί κινούνται γύρω. Αυτό γίνεται για τις λειτουργίες διαχείρησης κινητικότητας που επιτρέπουν την πρόσβαση στο δίκτυο για συσκευές που βρίσκονται πολύ μακριά από ένα σημείο πρόσβασης στο δίκτυο.

- Fluctuating Link Capacity:

Τα αποτελέσματα των high bit error rates μπορεί να είναι μεγαλύτερα σε ένα multihop ad-hoc δίκτυο, δεδομένου ότι το σύνολο όλων των λαθών στις συνδέσεις έχει επιπτώσεις σε μια multihop διαδρομή. Επιπλέον, περισσότερες από μια end-to-end διαδρομές μπορούν να χρησιμοποιήσουν μια δεδομένη σύνδεση, η οποία αν σπάσει, θα μπορούσε να αναστατώσει διάφορες συνόδους κατά τη διάρκεια των high bit error rates. Επίσης, εδώ επηρεάζεται η λειτουργία

δρομολόγησης, αλλά οι αποδοτικές λειτουργίες για την προστασία στρώματος συνδέσεων όπως το FEC (forward error correction) και το ARQ (automatic repeat request) μπορούν ουσιαστικά να βελτιώσουν την ποιότητα της σύνδεσης.

- Low-Power Devices:

Σε πολλές περιπτώσεις, οι σταθμοί ενός δικτύου λειτουργούν με μπαταρίες και αυτός ο λόγος θα μπορούσε να έχει επιπτώσεις στην CPU επεξεργασία , το μέγεθος και τη χρήση της μνήμης καθώς και την επεξεργασία του σήματος.

Λαμβάνοντας υπόψη τους πιο πάνω όρους που αναφέραμε, τι μπορεί ο χρήστης πλέον να αναμένει από ένα ad-hoc PAN δίκτυο; Η υποστήριξη των υπηρεσιών πολυμέσων θα απαιτηθεί πιθανότατα μέσα σε όλο το ad-hoc PAN. Για παράδειγμα, οι ακόλουθες τέσσερις κατηγορίες ποιότητας (QoS) θα διευκόλυναν τη χρήση των εφαρμογών πολυμέσων.

- Conversational(voice)
- Streaming(video/audio)
- Interactive(web)
- Background (FTP).

Αυτές οι κατηγορίες υπηρεσιών έχουν προσδιοριστεί για την υποστήριξη QoS στα δίκτυα UMTS και μπορούν επίσης να υποστηριχθούν σε PAN περιβάλλον. Σε αυτές τις περιπτώσεις υπάρχουν δυσκολίες όσο αφορά τις εγγυήσεις των υπηρεσιών που προσφέρονται σε μια συσκευή. Στα δίκτυα αυτού του είδους, οι σταθερές εγγυήσεις θα οδηγούσαν στις απαιτήσεις για το πώς οι σταθμοι κινούνται, καθώς επίσης και τις απαιτήσεις για την πυκνότητα σταθμών, η οποία θα εμπόδιζε την λειτουργία των ad-hoc δικτύων. Εντούτοις, όταν η επικοινωνία είναι σταθερή, η PAN υποδομή πρέπει να παρέχει το ίδιο QoS όπως έχει καθοριστεί για το δίκτυο πρόσβασης.

Η υποστήριξη QoS σε ένα ad-hoc δίκτυο έχει επιπτώσεις στις περισσότερες από τις λειτουργίες δικτύωσης που συζητήθηκαν πιο πάνω, ειδικά στην δρομολόγηση και την κινητικότητα. Επιπλέον, η τοπική διαχείριση buffer και μηχανισμών προτεραιότητας πρέπει να επεκταθούν στις συσκευές προκειμένου να αντιμετωπιστούν διάφορες αλλαγές στα ρεύματα κίνησης.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

2.5 Χαρακτηριστικές Λειτουργίες Ad-hoc Δικτύων

- **Ασφάλεια**

Προφανώς, η ασφάλεια αποτελεί μια από τις μεγαλύτερες ανησυχίες σε ένα ad-hoc δίκτυο, ειδικότερα αν υιοθετούνται πολλαπλά hops. Πώς μπορεί ένας χρήστης να είναι σίγουρος ότι κανένας δεν παρακολουθεί τα δεδομένα ή την ομιλία του μέσω ενός άλλου σταθμού; Είναι ο χρήστης στην άλλη άκρη πραγματικά το πρόσωπο που υποστηρίζει ότι είναι; Από κρυπτογραφικής άποψης, οι ad-hoc υπηρεσίες δεν παρουσιάζουν πολλά νέα προβλήματα. Οι απαιτήσεις σχετικά με την αυθεντικοποίηση, την εμπιστευτικότητα, και την ακεραιότητα ή το nonrepudiation είναι οι ίδιες όπως για πολλά άλλα δημόσια δίκτυα επικοινωνίας. Εντούτοις, σε ένα ασύρματο ad-hoc δίκτυο, η εμπιστευτικότητα είναι ένα μείζον πρόβλημα. Δεδομένου ότι δεν μπορούμε να εμπιστευθούμε το μέσο, η μόνη επιλογή μας είναι να χρησιμοποιήσουμε την κρυπτογράφηση, η οποία μας αναγκάζει να στηριχθούμε στα κρυπτογραφικά κλειδιά τα οποία χρησιμοποιούνται. Κατά συνέπεια, η βασική πρόκληση είναι η δημιουργία σχέσεων ‘εμπιστοσύνης’ μεταξύ των κλειδιών χωρίς την ενίσχυση μιας εμπιστευτικής τρίτου βαθμού πιστοποίησης.

Δεδομένου ότι τα ad-hoc δίκτυα δημιουργούνται αυθόρμητα μεταξύ των οντοτήτων που συμβαίνει να είναι στην ίδια φυσική θέση, δεν υπάρχει καμία εγγύηση ότι κάθε σταθμός κρατά τα δημόσια κλειδιά άλλων σταθμών ή ότι μπορεί να παρουσιάσει τα πιστοποιητικά που θα εμπιστευθούν άλλα συμβαλλόμενα μέρη. Εντούτοις, αν υπάρχει εμπιστοσύνη για εξουσιοδότηση μεταξύ των σταθμών, οι σταθμοί που ήδη έχουν καθιερώσει τις εμπιστευτικές σχέσεις μπορούν να επεκτείνουν αυτό το προνόμιο σε άλλα μέλη της ομάδας.

2.6 Δρομολόγηση στα ad-hoc δίκτυα

Στα κινητά ad-hoc δίκτυα, το ζήτημα της δρομολόγησης των πακέτων μεταξύ οποιωνδήποτε σταθμών αποτελεί ένα ‘στόχο’ επειδή οι σταθμοί μπορούν να κινηθούν τυχαία μέσα στο δίκτυο. Ένα μονοπάτι που θεωρείτο βέλτιστο σε ένα δεδομένο χρονικό σημείο μπορεί να μην λειτουργήσει λίγη ώρα αργότερα. Επιπλέον, οι στοχαστικές ιδιότητες των ασύρματων καναλιών προσθέτονται στην αβεβαιότητα της ποιότητας των μονοπατιών.

Τα παραδοσιακά πρωτόκολλα δρομολόγησης είναι δυναμικά δεδομένου ότι διατηρούν τις διαδρομές σε όλους τους σταθμούς, συμπεριλαμβανομένων των σταθμών στους οποίους κανένα πακέτο δεν στέλνεται. Αντιδρούν σε οποιαδήποτε αλλαγή στην τοπολογία ακόμα κι αν καμία κίνηση δεν επηρεάζεται από την αλλαγή, και απαιτούν περιοδικά

μηνύματα ελέγχου για να διατηρήσουν τις διαδρομές σε κάθε σταθμό στο δίκτυο. Το ποσοστό στο οποίο αυτά τα μηνύματα ελέγχου στέλνονται πρέπει να απεικονίσει τη δυναμική του δικτύου προκειμένου να διατηρηθούν τα έγκυρα μονοπάτια. Κατά συνέπεια, οι λιγοστές πηγές όπως η δύναμη και το εύρος ζώνης των συνδέσεων θα χρησιμοποιούνται συχνότερα για τον έλεγχο της κίνησης καθώς η κινητικότητα των σταθμών αυξάνεται.

Μια εναλλακτική προσέγγιση περιλαμβάνει την καθιέρωση των ενεργών διαδρομών, η οποία υπαγορεύει ότι οι διαδρομές μεταξύ των σταθμών καθορίζονται απλώς όταν απαιτείτε να καθοδηγούν τα πακέτα. Αυτό αποτρέπει τους σταθμούς από την ενημέρωση κάθε πιθανής διαδρομής στο δίκτυο, και τους επιτρέπει αντ' αυτού να εστιαστούν είτε στις διαδρομές που χρησιμοποιούνται, είτε στις διαδρομές που είναι στο στάδιο της σύστασης.

Σε μια μελέτη προσομοίωσης,την SwitchLab (έρευνα της Ericsson) έγινε σύγκριση μεταξύ δύο αλγόριθμων δρομολόγησης, (τους οποίους θα μελετήσουμε πιο κάτω), του AODV και του DSR,καθώς και ενός δυναμικού αλγόριθμου δρομολόγησης του DSDV. Σε κάθε δοκιμασία, οι δύο πρώτοι αλγόριθμοι ξεπέρασαν τον DSDV αλγόριθμο από την άποψη της ρυθμοαπόδοσης και της καθυστέρησης. Επιπλέον, τα reactive πρωτόκολλα συμπεριφέρθηκαν ομοίως στις περισσότερες περιπτώσεις. Το κύριο συμπέρασμα που προέρχεται από αυτήν την μελέτη είναι ότι μια reactive προσπέλαση είναι απαραίτητη σε ένα κινητό περιβάλλον με περιορισμένη ικανότητα εύρους ζώνης. Η δυναμική προσπέλαση μειώνει πάρα πολλές πηγές που ενημερώνουν τις διαδρομές. Εάν το διάστημα ενημερώσεων είναι πάρα πολύ μεγάλο, το δίκτυο περιέχει απλά ένα μεγάλο ποσό διαδρομών στους σταθμούς, το οποίο οδηγεί σε μια σημαντική απώλεια πακέτων.

2.7 Στόχοι ασφάλειας

Η ασφάλεια ως γνωστό είναι ένα πολύ σημαντικό ζήτημα για τα ad-hoc δίκτυα, ειδικά για τις ευαίσθητες σε ασφάλεια εφαρμογές. Για την ασφάλεια ενός ad-hoc δικτύου, θα συζητήσουμε τις ακόλουθες ιδιότητες: availability (διαθεσιμότητα), confidentiality(εμπιστευτικότητα), integrity (ακεραιότητα), authentication (αυθεντικοποίηση), και nonrepudiation.

- availability

Εξασφαλίζει την ικανότητα επιβίωσης των υπηρεσιών δικτύων απέναντι σε επιθέσεις DoS (Denial-of-Service) . Μια επίθεση DoS θα μπορούσε να προωθηθεί σε οποιοδήποτε

στρώμα ενός ad-hoc δικτύου. Στο φυσικό στρώμα ελέγχου και στο MAC (Media Access Control), ένας αντίπαλος θα μπορούσε να μπλοκάρει την επικοινωνία στα φυσικά κανάλια. Στο στρώμα δικτύου, ένας αντίπαλος θα μπορούσε να ενοχλήσει το πρωτόκολλο δρομολόγησης και να αποσυνδέσει το δίκτυο. Στα υψηλότερα στρώματα, ένας αντίπαλος θα μπορούσε να κτυπήσει τις υψηλού επιπέδου υπηρεσίες. Ένας τέτοιος στόχος είναι το key Management Service, οποίο θα δούμε πιο κάτω, μια ουσιαστική υπηρεσία για οποιοδήποτε πλαίσιο ασφάλειας.

- confidentiality

Η εμπιστευτικότητα εξασφαλίζει μεταξύ άλλων ότι ορισμένες κύριες πληροφορίες δεν αποκαλύπτονται ποτέ σε αναρμόδιες οντότητες. Η μετάδοση στο δίκτυο σημαντικότατων πληροφοριών, όπως στρατηγικής μορφής πληροφορίες, απαιτούν μεγάλη εμπιστευτικότητα. Η διαρροή τέτοιων πληροφοριών στους εχθρούς θα μπορούσε να έχει καταστρεπτικές συνέπειες. Οι πληροφορίες δρομολόγησης πρέπει επίσης να παραμείνουν εμπιστευτικές σε ορισμένες περιπτώσεις επειδή οι πληροφορίες μπορεί να είναι χρήσιμες για τους εχθρούς ώστε να προσδιορίσουν και να εντοπίσουν τους στόχους τους σε ένα πεδίο μάχης.

- integrity

Η ακεραιότητα εγγυάται ότι ένα μήνυμα που μεταφέρεται δεν αλλοιώνεται ποτέ. Ένα μήνυμα θα μπορούσε να αλλοιωθεί λόγω των καλοκάγαθων αποτυχιών, όπως η εξασθένιση του σήματος κατά την διάδοση, ή λόγω των κακόβουλων επιθέσεων στο δίκτυο.

- authentication

Η αυθεντικοποίηση επιτρέπει σε έναν κόμβο να εξασφαλίζει την ταυτότητα του κόμβου με τον οποίο επικοινωνεί. Χωρίς την αυθεντικοποίηση, ένας αντίπαλος θα μπορούσε να παριστάνει ένα κόμβο, κερδίζοντας κατά συνέπεια την αναρμόδια πρόσβαση στην πηγή και τις ευαίσθητες πληροφορίες παρεμποδίζοντας έτσι τη λειτουργία άλλων κόμβων.

- nonrepudiation

Τέλος, το nonrepudiation εξασφαλίζει ότι η προέλευση ενός μηνύματος δεν μπορεί να αρνηθεί στο μήνυμα την αποστολή Το nonrepudiation είναι χρήσιμο για την ανίχνευση και την απομόνωση των συμβιβασμένων κόμβων.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

2.8 Προκλήσεις

Τα χαρακτηριστικά γνωρίσματα των ad-hoc δικτύων θέτουν διάφορες προκλήσεις για την επίτευξη των πιο πάνω στόχων ασφάλειας.

Κατ' αρχάς, η χρήση των ασύρματων συνδέσεων καθιστά ένα ad-hoc δίκτυο ευαίσθητο στις επιθέσεις συνδέσεων (που κυμαίνονται από την παρακολούθηση ομιλίας μέχρι την προσποίηση κάποιου άλλου), την επανάληψη μηνυμάτων, καθώς και τη διαστρέβλωση τους. Κρυφακούοντας κάποιος μπορεί να κερδίσει πρόσβαση σε μυστικές πληροφορίες, παραβιάζοντας έτσι την εμπιστευτικότητα. Οι ενεργές επιθέσεις επιτρέπουν στον αντίπαλο να διαγράψει μηνύματα, να εγχύσει λανθασμένα μηνύματα, να τα τροποποιεί, και να παριστάνει ένα άλλο κόμβο, παραβιάζοντας έτσι κατά συνέπεια τη διαθεσιμότητα, την ακεραιότητα, την αυθεντικοποίηση, και το nonrepudiation.

Για να μπορέσουν να επιβιώσουν τα ad-hoc δίκτυα πρέπει να έχουν μια distributed αρχιτεκτονική χωρίς κεντρικές οντότητες. Η εισαγωγή οποιασδήποτε κεντρικής οντότητας στη λύση ασφάλειάς μας θα μπορούσε να οδηγήσει στη σημαντική ευπάθεια δηλαδή εάν αυτή η συγκεντρωμένη οντότητα συμβιβάζεται, ολόκληρο το δίκτυο υπονομεύεται.

Επίσης, ένα ad-hoc δίκτυο χαρακτηρίζεται δυναμικό λόγω των συχνών αλλαγών στην τοπολογία του και στην ικανότητα των κόμβων του να μπαίνουν και να βγαίνουν στο δίκτυο. Οι σχέσεις εμπιστοσύνης μεταξύ των κόμβων αλλάζουν επίσης. Αντίθετα από άλλα ασύρματα κινητά δίκτυα, όπως η κινητή IP, οι κόμβοι σε ένα ad-hoc δίκτυο μπορούν να συνδεθούν δυναμικά με τις διοικητικές περιοχές (administrative domains). Οποιαδήποτε λύση ασφάλειας με μια στατική διαμόρφωση δεν θα αρκούσε. Είναι επιθυμητό για τους μηχανισμούς ασφάλειάς να προσαρμόζονται σε αυτές τις αλλαγές.

Τέλος, ένα ad-hoc δίκτυο μπορεί να αποτελείται από εκατοντάδες ή ακόμα και χιλιάδες κόμβους. Οι μηχανισμοί ασφάλειας πρέπει να είναι εξελίσσονται συνεχώς με τον χρόνο ώστε να μπορούν να χειριστούν ένα τέτοιο μεγάλο δίκτυο.

2.9 Scope and Roadmap

Οι παραδοσιακοί μηχανισμοί ασφάλειας όπως τα πρωτόκολλα αυθεντικοποίησης, η ψηφιακή υπογραφή, και κρυπτογράφηση, διαδραματίζουν ακόμα σημαντικό ρόλο στην επίτευξη της εμπιστευτικότητας, της ακεραιότητας, της αυθεντικοποίησης, και του nonrepudiation της επικοινωνίας

στα ad-hoc δίκτυα. Εντούτοις, αυτοί οι μηχανισμοί δεν είναι αποδοτικοί από μόνοι τους.

Θα βασιστούμε περαιτέρω στις ακόλουθες δύο αρχές. Κατ' αρχάς,θα εκμεταλλευτούμε την ύπαρξη πολλαπλών διαδρομών μεταξύ των σταθμών (redundancies) σε ένα δίκτυο για να πετύχουμε τη διαθεσιμότητα. Η δεύτερη αρχή είναι διανομή της εμπιστοσύνης. Αν και κανένας κόμβος δεν είναι αξιόπιστος σε ένα ad-hoc δίκτυο λόγω της μειωμένης ασφάλειας και της διαθεσιμότητας, μπορούμε να διανείμουμε την εμπιστοσύνη στο σύνολο των σταθμών.

Όλα τα βασισμένα σε κλειδί κρυπτογραφικά σχέδια (π.χ., ψηφιακή υπογραφή) απαιτούν μια key management υπηρεσία, η οποία είναι αρμόδια για την παρακολούθηση των συνδέσεων μεταξύ των κλειδιών και των κόμβων, και την ενίσχυση της καθιέρωσης της αμοιβαίας εμπιστοσύνης και της ασφαλούς επικοινωνίας μεταξύ των κόμβων.

2.10 Ασφαλής δρομολόγηση

Για την εξασφάλιση της διαθεσιμότητας, τα πρωτόκολλα δρομολόγησης πρέπει να είναι ‘γερά’ ενάντια στη δυναμικά μεταβαλλόμενη τοπολογία και τις κακόβουλες επιθέσεις. Τα πρωτόκολλα δρομολόγησης που προτείνονται για τα ad-hoc δίκτυα αντιμετωπίζουν καλά τη δυναμικά μεταβαλλόμενη τοπολογία. Εντούτοις, κανένα από τα γνωστά πρωτόκολλα δεν έχει προσαρμόσει μηχανισμούς που να υπερασπίζουν τα δίκτυα από τις κακόβουλες επιθέσεις. Για τα πρωτόκολλα δρομολόγησης των ad-hoc δικτύων γίνονται ακόμα έρευνες. Δεν υπάρχει ακόμα ούτε ένα κατάλληλο πρωτόκολλο δρομολόγησης χωρίς ατέλειες. Επομένως, στόχος είναι η σύλληψη των κοινών απειλών ασφάλειας και η παροχή ασφάλειας στα πρωτόκολλα δρομολόγησης.

Στα περισσότερα πρωτόκολλα δρομολόγησης, οι δρομολογητές ανταλλάσσουν πληροφορίες για την τοπολογία του δικτύου προκειμένου να καθιερωθούν οι διαδρομές μεταξύ των σταθμών. Τέτοιες πληροφορίες θα μπορούσαν να γίνουν στόχος για τους κακόβουλους αντιπάλους που σκοπεύουν να κτυπήσουν το δίκτυο.

Υπάρχουν δύο πηγές απειλών στα πρωτόκολλα δρομολόγησης. Ο πρώτος προέρχεται από τους εξωτερικούς επιτιθεμένους. Με την διοχέτευση λανθασμένων πληροφοριών δρομολόγησης, επαναλαμβάνοντας παλιές πληροφορίες δρομολόγησης, ή διαστρεβλώνοντας τις πληροφορίες δρομολόγησης, ένας επιτιθέμενος θα μπορούσε επιτυχώς να χωρίσει ένα δίκτυο ή να εισαγάγει υπερβολικό φορτίο κυκλοφορίας στο δίκτυο προκαλώντας αναμεταδόσεις και άρα ανεπαρκή δρομολόγηση. Το δεύτερο είδος απειλής προέρχεται από τους συμβιβασμένους κόμβους, οι οποίοι διαδίδουν ανακριβείς

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

πληροφορίες δρομολόγησης σε άλλους κόμβους. Η ανίχνευση τέτοιων ανακριβών πληροφοριών είναι πολύ δύσκολη υπόθεση.

Για την προστασία από το πρώτο είδος απειλής, οι κόμβοι μπορούν να προστατεύσουν τις πληροφορίες δρομολόγησης με τον ίδιο τρόπο όπως προστατεύουν την μεταφορά δεδομένων, δηλαδή μέσω της χρήσης των κρυπτογραφικών σχεδίων όπως η ψηφιακή υπογραφή. Αυτό όμων δεν είναι αποτελεσματικό ενάντια στις επιθέσεις από τους συμβιβασμένους servers. Χειρότερα ακόμα, όπως έχουμε υποστηρίξει, δεν μπορούμε να παραμελήσουμε την δυνατότητα των κόμβων να συμβιβάζονται σε ένα ad-hoc δίκτυο. Η ανίχνευση των συμβιβασμένων κόμβων μέσω της δρομολόγησης των πληροφοριών είναι επίσης δύσκολη σε ένα ad-hoc δίκτυο λόγω της δυναμικά μεταβαλλόμενης τοπολογίας της. Όταν ένα μέρος της πληροφορίας βρεθεί άκυρο, οι πληροφορίες θα μπορούσαν να παραχθούν από έναν συμβιβασμένο κόμβο, ή θα μπορούσε να θεωρηθεί άκυρο το αποτέλεσμα των αλλαγών τοπολογίας.

Αφ' ετέρου, μπορούμε να εκμεταλλευτούμε ορισμένες ιδιότητες των ad-hoc δικτύων για να επιτύχουμε ασφαλή δρομολόγηση. Τα πρωτόκολλα δρομολόγησης στα ad-hoc δίκτυα πρέπει να χειριστούν την ξεπερασμένη πληροφορία δρομολόγησης για να προσαρμόσουν τη δυναμικά μεταβαλλόμενη τοπολογία. Οι λανθασμένες πληροφορίες δρομολόγησης που παρήχθησαν από τους συμβιβασμένους κόμβους θα μπορούσαν, ως ένα ορισμένο βαθμό, να θεωρηθούν ξεπερασμένες πληροφορίες. Εφ' όσον υπάρχουν αρκετοί σωστοί κόμβοι, το πρωτόκολλο δρομολόγησης πρέπει να είναι σε θέση να βρεί τις διαδρομές που πηγαίνουν γύρω από αυτούς τους συμβιβασμένους κόμβους. Αυτή η ικανότητα των πρωτοκόλλων δρομολόγησης στηρίζεται συνήθως στις πλεονάζουσες πολλαπλές διαδρομές μεταξύ των κόμβων στα ad-hoc δίκτυα. Εάν τα πρωτόκολλα δρομολόγησης ανακαλύψουν πολλαπλές διαδρομές (π.χ.,τα πρωτόκολλα ZRP, DSR, TORA, και AODV μπορούν να το επιτύχουν αυτό), οι σταθμοί μπορούν να μεταπηδήσουν σε μια εναλλακτική διαδρομή όταν εμφανίζεται πρόβλημα στην αρχική διαδρομή.

Η diversity κωδικοποίηση εκμεταλλεύεται τις πολλαπλές διαδρομές με έναν αποδοτικό τρόπο χωρίς αναμετάδοση μηνυμάτων. Η βασική ιδέα είναι να διαβιβαστούν οι περιττές πληροφορίες μέσω των πρόσθετων διαδρομών για την ανίχνευση και τη διόρθωση λάθους. Παραδείγματος χάριν, εάν υπάρχουν χ διαδρομές μεταξύ δύο σταθμών, μπορούμε να χρησιμοποιήσουμε το χ - ρ κανάλια για να διαβιβάσουμε τα δεδομένα και να χρησιμοποιήσουμε τα άλλα ρ κανάλια για να διαβιβάσουμε τις πλεονάζουσες πληροφορίες. Ακόμα κι αν ορισμένες διαδρομές εκτεθούν, ο δέκτης μπορεί ακόμα να είναι σε θέση να επικυρώσει τα μηνύματα και να τα ανακτήσει από τα λάθη χρησιμοποιώντας τις πλεονάζουσες πληροφορίες από τα πρόσθετα ρ κανάλια.

2.11 Key Management Service

Με την υιοθέτηση κρυπτογραφικών σχεδίων, όπως οι ψηφιακές υπογραφές, προστατεύουμε τις πληροφορίες δρομολόγησης και την κίνηση των δεδομένων. Η χρήση τέτοιων σχεδίων απαιτεί συνήθως μια key management (KM) υπηρεσία. Υιοθετούμε μια υποδομή δημοσίου κλειδιού λόγω της ανωτερότητάς της στη διανομή των κλειδιών, στην επίτευξη ακεραιότητας και στο nonrepudiation. Τα αποδοτικά σχέδια μυστικού κλειδιού χρησιμοποιούνται για να εξασφαλίσουν περαιτέρω επικοινωνία αφότου γίνει αυθεντικοποίηση μεταξύ των σταθμών και καθιερώωθεί ένα κοινό μυστικό κλειδί συνόδου.

Σε μια υποδομή δημοσίου κλειδιού, κάθε σταθμός έχει ένα ζευγάρι δημόσιου και ιδιωτικού κλειδιού. Τα δημόσια κλειδιά μπορούν να διανεμηθούν σε άλλους σταθμούς, ενώ τα ιδιωτικά κλειδιά πρέπει να κρατηθούν εμπιστευτικά στους μεμονωμένους σταθμούς. Υπάρχει μια οντότητα για την ‘εμπιστοσύνη’ αποκαλούμενη αρχή πιστοποίησης (CA) για τη διαχείριση των κλειδιών. Το CA έχει ένα ζευγάρι δημόσιου/ιδιωτικού κλειδιού, όπου το δημόσιο κλειδί είναι γνωστό σε κάθε σταθμό, και υπογράφει τα πιστοποιητικά που δεσμεύουν τα δημόσια κλειδιά στους σταθμούς.

Το CA πρέπει να είναι συνδεδεμένο για να απεικονίσει τα τρέχοντα bindings, επειδή τα bindings μπορούν να αλλάζουν με τον χρόνο. Ένα δημόσιο κλειδί πρέπει να ανακληθεί από ένα σταθμό εάν ο σταθμός δεν είναι πλέον εμπιστεύσιμος ή αν βρίσκεται εκτός δικτύου.

Η καθιέρωσης μιας υπηρεσίας διαχείρισης κλειδιού με την βοήθεια μιας CA αποτελεί ένα από τα μεγάλα προβλήματα των ad-hoc δικτύων. Το CA , που είναι αρμόδιο για την ασφάλεια ολόκληρου του δικτύου, φυσικά και αποτελεί ένα τρωτό σημείο για το δίκτυο. Αν το CA δεν είναι διαθέσιμο, οι σταθμοί δεν μπορούν να πάρουν τα τρέχοντα δημόσια κλειδιά άλλων σταθμών ή να καθιερώσουν ασφαλή επικοινωνία με άλλους. Εάν το CA εκτεθεί και διαρρεύσει το ιδιωτικό κλειδί σε έναν αντίπαλο, ο αντίπαλος μπορεί έπειτα να υπογράψει οποιοδήποτε λανθασμένο πιστοποιητικό χρησιμοποιώντας αυτό το ιδιωτικό κλειδί υποδύοντας ένα άλλο σταθμό ή να ανακαλέσει οποιοδήποτε πιστοποιητικό.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

2.12 The System Model (SM)

Η key management (KM) υπηρεσία εφαρμόζεται σε ένα ασύγχρονο ad-hoc δίκτυο δηλαδή ένα δίκτυο χωρίς δέσμευση στους χρόνους παράδοσης και επεξεργασίας μηνυμάτων. Επίσης υποθέτουμε ότι το στρώμα δικτύου παρέχει αξιόπιστες συνδέσεις.Όλη η υπηρεσία, συνολικά, έχει ένα ζευγάρι δημόσιου/ιδιωτικού κλειδιού. Όλοι οι κόμβοι στο σύστημα ξέρουν το δημόσιο κλειδί της υπηρεσίας και εμπιστεύονται οποιαδήποτε πιστοποιητικά υπογεγραμμένα χρησιμοποιώντας το αντίστοιχο ιδιωτικό κλειδί. Οι κόμβοι, ως πελάτες, μπορούν να υποβάλουν τα αιτήματα τους για να αποκτήσουν τα δημόσια κλειδιά άλλων πελατών ή να υποβάλλουν αιτήματα για την αναπροσαρμογή ή την αλλαγή των δημοσίων κλειδιών τους.

Η key management (KM) υπηρεσία, με (χ, ψ + 1) διαμόρφωση (χ>3ψ+1), αποτελείται από τους ειδικούς κόμβους χ, οι οποίοι καλούνται servers σε ένα ad-hoc δίκτυο. Κάθε server έχει επίσης το δικό του ζευγάρι κλειδιών και αποθηκεύει τα δημόσια κλειδιά όλων των κόμβων στο δίκτυο. Επίσης κάθε server ξέρει τα δημόσια κλειδιά των άλλων servers. Κατά συνέπεια, οι servers μπορούν να εγκαταστήσουν ασφαλείς συνδέσεις μεταξύ τους.

Η όλη υπηρεσία λειτουργά σωστά αν τηρούνται οι ακόλουθες 2 καταστάσεις:

- Robustness:

Η υπηρεσία είναι πάντα ικανή να επεξεργάζεται query και αιτήματα ενημέρωσης από τους πελάτες. Κάθε query επιστρέφει πάντα το τελευταίο ενημερωμένο δημόσιο κλειδί που συνδέεται με το ζητούμενο πελάτη.

- Confidentiality:

Το ιδιωτικό κλειδί της υπηρεσίας δεν αποκαλύπτεται ποτέ σε κανένα αντίπαλο. Κατά συνέπεια, ένας αντίπαλος δεν είναι ποτέ ικανός να εκδώσει τα πιστοποιητικά, που υπογράφονται από το ιδιωτικό κλειδί, για τις λανθασμένες συνδέσεις.

2.13 Λειτουργίες Κινητικότητας (Mobility functions)

Στα παρόντα κυψελοειδή δίκτυα, η κινητικότητα σταθμών και χρηστών αντιμετωπίζεται κυρίως με τη βοήθεια του forwarding. Κατά συνέπεια, όταν κυκλοφορεί ένας χρήστης έξω από το εγχώριο δίκτυό του οποιεσδήποτε κλήσεις που κατευθύνονται σε αυτόν θα διαβιβαστούν στο δίκτυο ‘επίσκεψης’ μέσω του εγχώριου δικτύου του. Αυτή η ίδια αρχή διαβίβασης ισχύει για την κινητή IP. Ένας χρήστης ή καλύτερα ένας σταθμός με μια διεπαφή IP, μπορεί επίσης να συνεχίσει να χρησιμοποιεί μια διεύθυνση IP έξω από το

υποδίκτυο στο οποίο ανήκει. Ένας σταθμός περιαγωγής σε ένα ξένο δίκτυο συνδέεται με μια διεύθυνση c/o που παρέχεται από έναν Foreign Agent (FA). Στο εγχώριο δίκτυο, ένας Home Agent(HA) εγκαθιδρύει μια IP σήραγγα στον FA χρησιμοποιώντας τη διεύθυνση c/o. Οποιοδήποτε πακέτο που στέλνεται στη διεύθυνση περιαγωγής του σταθμού στέλνεται αρχικά στον HA, ο οποίος την διαβιβάζει στον FA μέσω της διεύθυνσης c/o. Το FA decapsulates έπειτα το πακέτο και το στέλνει στον σταθμό περιαγωγής χρησιμοποιώντας την αρχική διεύθυνση IP. Η πραγματική δρομολόγηση στο σταθερό δίκτυο δεν επηρεάζεται με αυτήν μέθοδο και μπορεί να χρησιμοποιήσει τα παραδοσιακά πρωτόκολλα δρομολόγησης όπως το Open shortest Path First (OSPF), το Routing Information Protocol και το Border Gateway Protocol(BGP). Αυτή η προσέγγιση αποστολής είναι κατάλληλη σε περιπτώσεις όπου μόνο οι σταθμοί (τερματικά) κινούνται στα ίδια τα άκρα των δικτύων.

Εντούτοις, σε ένα ad-hoc δίκτυο δεδομένου ότι οι κόμβοι στο κέντρο του δικτύου μπορούν επίσης να μετακινούντε, ολόκληρο το δίκτυο είναι βασισμένο στην ιδέα των συσκευών που χρησιμεύουν και ως δρομολογητές και ως hosts συγχρόνως. Ως εκ τούτου, σε ένα ειδικό δίκτυο, η κινητικότητα αντιμετωπίζεται άμεσα από τον αλγόριθμο δρομολόγησης. Εάν ένας κόμβος κινείται, προκαλώντας κίνηση, το πρωτόκολλο δρομολόγησης φροντίζει τις αλλαγές στον πίνακα δρομολόγησης των σταθμών. Σε πολλές περιπτώσεις, η αλληλεπίδραση μπορεί να αναμένεται μεταξύ των ad-hoc και σταθερών δικτύων. Η αλληλεπίδραση θα καθιστούσε πιθανό για έναν χρήστη σε ένα ταξίδι που συμμετέχει σε μια διάσκεψη με τον φορητό του υπολογιστή αλλά θέλει να είναι εφικτή η κινητικότητα μέσω του σταθερού δικτύου IP. Επιπλέον, δεδομένου ότι ο χρήστης θέλει να είναι προσιτός από το σταθερό δίκτυο, η κινητή IP θα ήταν ένας κατάλληλος τρόπος να τον κάνει προσιτό μέσω του σταθερού δικτύου IP. Εάν ο χρήστης βρίσκεται μερικά βήματα μακρία από το σημείο πρόσβασης, η κινητή IP και το πρωτόκολλο δρομολόγησης του ad-hoc δικτύου πρέπει να αλληλεπιδρήσουν για να παρέχουν τη συνδετικότητα μεταξύ του κινούμενου χρήστη και των σταθμών.

2.14 Πρωτόκολλα δρομολόγησης για κινητά ad-hoc δίκτυα

- Destination-sequenced distance vector

Το DSDV είναι ένα δυναμικό hop-by-hop distance vector πρωτόκολλο δρομολόγησης. Κάθε κόμβος δικτύων διατηρεί έναν πίνακα δρομολόγησης που περιέχει τον επόμενο hop σε οποιοδήποτε ‘εφικτό’ προορισμό καθώς επίσης και τον αριθμό των hop που θα απαιτηθούν. Για να εγγυηθεί ομαλή

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

κυκλοφορία(π.χ loops-freedom),το DSDV χρησιμοποιεί μια έννοια που είναι βασισμένη σε αριθμούς ακολουθίας (sequence number)για να δείξει πόσο νέα μια δεδομένη διαδρομή είναι. Η διαδρομή R, παραδείγματος χάριν, θα θεωρηθεί καλύτερη από την R' αν η R έχει ψηλότερο αριθμό ακολουθίας (seq no). Αν όμως οι διαδρομές έχουν τον ίδιο αριθμό ακολουθίας, η R θα έχει το χαμηλότερο, ή πιο πρόσφατο hop-count.
Σε έναν distance vector (ή Bellman Ford) αλγόριθμο, οι κόμβοι του δικτύου ανταλλάσσουν πληροφορίες δρομολόγησης με τους γείτονές τους. Ο πίνακας δρομολόγησης σε έναν κόμβο περιέχει τον επόμενο hop για κάθε προορισμό στο δίκτυο, και συνδέεται με ένα distance-metric, για παράδειγμα, τον αριθμό των hops. Με βάση αυτές τις πληροφορίες που βρίσκονται στους πίνακες δρομολόγησης των γειτονικών κόμβων, είναι δυνατό να υπολογιστούν οι συντομότερες διαδρομές (ή καλύτερα μονοπάτια) σε κάθε προορισμό σε έναν πεπερασμένο χρόνο για ένα δίκτυο χωρίς αλλαγές τοπολογίας.

- *Ad hoc* on-demand distance vector

Όπως και το DSDV,το AODV είναι ένα distance vector πρωτόκολλο δρομολόγησης, αλλά είναι reactive σε σχέση με το προηγούμενο. Αυτό σημαίνει ότι το AODV ζητά απλώς μια διαδρομή όταν χρειάζεται μία, και δεν απαιτεί οι κόμβοι να πρέπει να διατηρήσουν διαδρομές σε προορισμούς που δεν επικοινωνούν μεταξύ τους. Το AODV χρησιμοποιεί τους αριθμούς ακολουθίας με έναν τρόπο παρόμοιο με DSDV για να αποφύγει routing loops και για να δείξει πόσο νέα είναι μια διαδρομή. Όποτε ένας κόμβος πρέπει να βρεί μια διαδρομή για έναν άλλο κόμβο, εκπέμπει ένα μήνυμα αιτήματος διαδρομής (Route request-RREQ) σε όλους τους γείτονές του. Το μήνυμα RREQ μεταδίδεται μέσω του δικτύου έως ότου φθάνει στον προορισμό ή έναν κόμβο που έχει μια νέα διαδρομή στον προορισμό. Στο δρόμο του μέσω του δικτύου, το μήνυμα RREQ αρχίζει τη δημιουργία των προσωρινών καταχωρήσεων στον πίνακα δρομολόγησης για την αντίστροφη διαδρομή στους κόμβους που περνά. Εάν βρεθεί ο προορισμός ή μια διαδρομή, η διαθεσιμότητά της θα υποδειχθεί από ένα route reply (RREP) μήνυμα που είναι unicast πίσω στην πηγή κατά μήκος της προσωρινής αντίστροφης πορείας του λαμβανόμενου μηνύματος RREQ.

- Dynamic source routing

Το Dynamic source routing είναι ένα reactive πρωτόκολλο δρομολόγησης που χρησιμοποιεί τη δρομολόγηση πηγής για να παραδώσει τα πακέτα με τα δεδομένα. Οι επικεφαλίδες των πακέτων με τα δεδομένα μεταφέρουν τις διευθύνσεις των κόμβων μέσω των οποίων το πακέτο πρέπει να περάσει. Αυτό σημαίνει ότι οι ενδιάμεσοι κόμβοι πρέπει να παρακολουθούν μόνο τους άμεσους γείτονες τους

προκειμένου να διαβιβάσουν τα πακέτα με τα δεδομένα. Η πηγή, αφ' ετέρου, πρέπει να ξέρει την πλήρη ακολουθία των hop στον προορισμό. Όπως στο AODV, η διαδικασία αποκτήσεων διαδρομών σε DSR ζητά μια διαδρομή με την πλημμύρα του συστήματος με ένα πακέτο RREQ. Ένας κόμβος που λαμβάνει ένα πακέτο RREQ ψάχνει την κρύπτη διαδρομών του, όπου όλες οι γνωστές διαδρομές της αποθηκεύονται, για μια διαδρομή στο ζητούμενο προορισμό. Εάν καμία διαδρομή δεν βρίσκεται, διαβιβάζει το πακέτο RREQ μετά από πρώτα να έχε προσθέσει τη διεύθυνσή της στην ακολουθία λυκίσκου που αποθηκεύεται στο πακέτο. Το πακέτο διαδίδεται μέσω του δικτύου έως ότου φθάνει είτε στον προορισμό, είτε έναν κόμβο με μια διαδρομή στον προορισμό. Εάν βρεθεί μια διαδρομή, ένα πακέτο RREP που περιέχει την κατάλληλη ακολουθία hop για την επίτευξη του προορισμού είναι unicast στον κόμβο. Ένα άλλο χαρακτηριστικό γνώρισμα του πρωτοκόλλου DSR είναι ότι μπορεί να μάθει τις διαδρομές από την πηγή μέσω των πακέτων που λαμβάνει.

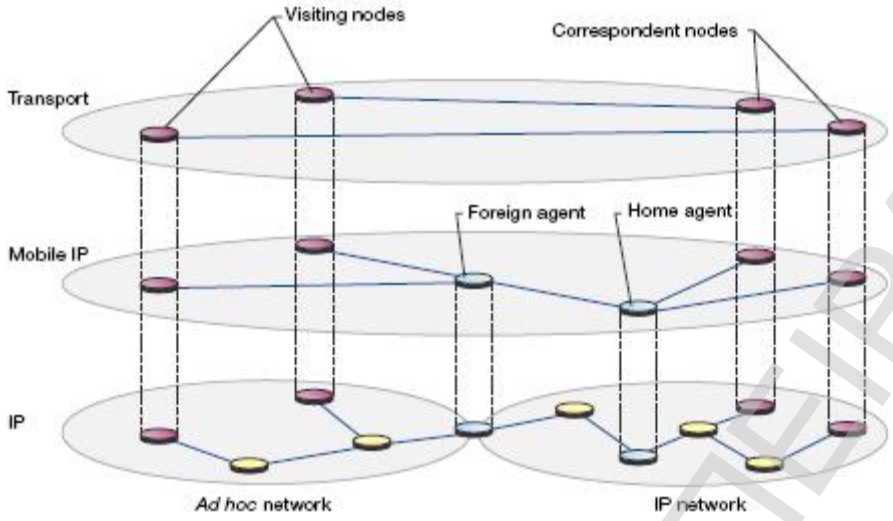
2.15 MIPMANET

Η κινητή IP για τα κινητά ad-hoc δίκτυα (MIPMANET) σχεδιάστηκε για να δώσει στους σταθμούς ενός ad-hoc δικτύου:

- πρόσβαση στο δίκτυο στο Διαδίκτυο
- υπηρεσίες για κινητή IP.

Έτσι χρησιμοποιούνται οι κινητοί IP FA ως σημεία πρόσβασης στο Διαδίκτυο για να ‘παρακολουθήσουν’ το ad-hoc δίκτυο στο οποίο βρίσκεται οποιοσδήποτε δεδομένος κόμβος, και να κατευθύνουν τα πακέτα στην άκρη εκείνου του ad-hoc δικτύου. Το ad-hoc πρωτόκολλο δρομολόγησης χρησιμοποιείται για να μεταφέρει τα πακέτα μεταξύ του FA και του κόμβου επίσκεψης. Μια στρωματοποιημένη προσέγγιση (όπως φαίνετε στο πιο κάτω σχήμα) εφαρμόζεται στην εξωτερική ροή δεδομένων (data flow), χωρίζει την κινητή λειτουργία IP από το ad-hoc πρωτόκολλο δρομολόγησης και επεξηγεί πώς η κινητή IP και η ad-hoc λειτουργία δρομολόγησης είναι βρίσκονται στο σχήμα. Αυτό καθιστά ικανό το MIPMANET να παρέχει πρόσβαση στο διαδίκτυο διευκολύνοντας τους σταθμούς να επιλέξουν τα πολλαπλά σημεία πρόσβασης.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



Με λίγα λόγια το MIPMANET λειτουργεί ως εξής:

- Οι σταθμοί σε ένα ad-hoc δίκτυο που θέλουν πρόσβαση στο διαδικτύου χρησιμοποιούν τις τοποικές IP διευθύνσεις για την επικοινωνία.
- Για να σταλεί ένα πακέτο σε έναν host στο διαδίκτυο, ο σταθμός στο ad-hoc δίκτυο στέλλει το πακέτο στον FA.
- Για να ληφθούν τα πακέτα από τους host στο διαδίκτυο, τα πακέτα δρομολογούνται στον FA από τους συνηθισμένους κινητούς μηχανισμούς IP. Ο ξένος πράκτορας παραδίδει έπειτα τα πακέτα στον σταθμό στο ad-hoc δίκτυο
- Σταθμοί που δεν απαιτούν πρόσβαση στο διαδίκτυο αλληλεπιδρούν με το ad-hoc δίκτυο σαν να είναι ένα αυτόνομο δίκτυο.
- Αν ένας σταθμός δεν μπορεί να καθορίσει από τη διεύθυνση IP αν ο προορισμός βρίσκεται μέσα ή έξω από το ad-hoc δίκτυο, θα ψάξει αρχικά για τον ‘επισκεπτόμενο’ κόμβο μέσα στο ειδικό δίκτυο πρίν στείλει το πακέτο.

Το MIPMANET μπορεί να χρησιμοποιεί την default διαδρομή στα ad-hoc πρωτόκολλα δρομολόγησης όπως AODV και DSR, χωρίς την απαίτηση οποιονδήποτε σημαντικών τροποποιήσεων. Τα πακέτα που απευθύνονται σε προορισμούς που δεν βρίσκονται μέσα στο ad-hoc δίκτυο στέλλονται στους FA. Στο MIPMANET, μόνο στους καταχωρημένους σταθμούς δίνεται πρόσβαση στο διαδίκτυο, κατά συνέπεια η μόνη κίνηση που παρατηρείτε στο ad-hoc δίκτυο από το διαδίκτυο είναι η κίνηση ανάμεσα σε ένα FA και ένα εγγραμμένο HA του σταθμού.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

3. BLUETOOTH

3.1 Τι είναι το Bluetooth

Το Bluetooth είναι μια προδιαγραφή ασύρματων ραδιοκυμάτων με σκοπό να αντικαταστήσει την τεχνολογία της καλωδίωσης. Η προδιαγραφή καθορίζεται από την Bluetooth Special Interest Group (SIG), η οποία αποτελείται από πάνω από 1000 βιομηχανίες. Το Bluetooth στην αρχή ήταν προορισμένο για κινητές συσκευές και σχεδιάστηκε με κύρια του προτεραιότητα το μικρό μλεγεθος, την μικρή κατανάλωση ισχύος καθώς και το μικρό κόστος. Η προδιαγραφή Bluetooth επιδιώκει να απλοποιήσει την επικοινωνία μεταξύ των ηλεκτρονικών συσκευών αυτοματοποιώντας την επεξεργασία σύνδεσης.

Ο Gartner εκτιμά ότι το 2004, 365 εκατομμύρια συσκευές Bluetooth χρησιμοποιήθηκαν στην αγορά, το 2005 περισσότερες από 800 εκατομμύρια ενώ από το 2006 και μετά ο αριθμός αυτος ξεπέρασε κατά πολύ το 1 δις. Το Bluetooth χρησιμοποιείτε σε συσκευές όπως φορητούς υπολογιστές, PDAs, εκτυπωτές, ψηφιακές κάμερες και άλλες ηλεκτρονικές συσκευές. Τον τελευταίο καιρό ακόμα και όλα τα αυτοκίνητα έχουν ενσωματωμένο σύστημα Bluetooth.

3.1.1 Ιστορική αναδρομή

Η πρώτη ονομασία του Bluetooth ήταν Ericson Mobile Communication. Η ονομασία όμως Bluetooth έχει ιστορία μερικούς αιώνες πριν, και ειδικά από τον δέκατο αιώνα από τον Δανό βασιλιά Harald Bluetooth. Το 1998 η IBM, η Intel, και η Toshiba διαμόρφωσαν το Bluetooth SIG το οποίο χρησιμοποιήθηκε ως η 'ραχοκοκκαλια' της προδιαγραφής.

Το SIG άρχισε σιγά σιγά να παρακολουθεί την ανάπτυξη της τεχνολογία όσο αφορά τα ασύρματα, και δημιούργησε έτσι ένα παγκόσμιο και ανοικτό για όλους πρότυπο. Σήμερα, πολλές χιλιάδες οργανισμοί αποτελούν μέρος του Bluetooth SIG, που περιλαμβάνει από κολοσσούς στις τηλεπικοινωνίες μέχρι βιομηχανίες που βοηθούν στην ανάπτυξη και προώθηση της τεχνολογίας Bluetooth.

Το Bluetooth σχεδιάστηκε αρχικά ως πρωτόκολλο για την αντικατάσταση της τεχνολογίας όπου υπήρχε χρήση καλωδίων. Εντούτοις, στόχος της SIG είναι στο εγγύς μέλλον όλη η επικοινωνία να γίνεται ασύρματα με καθόλου ενσύρματες συσκευές.

Το Bluetooth από το 1999 είναι πρωτυποποιημένο από την IEEE ως 802.15 Personal Area Network (PAN).

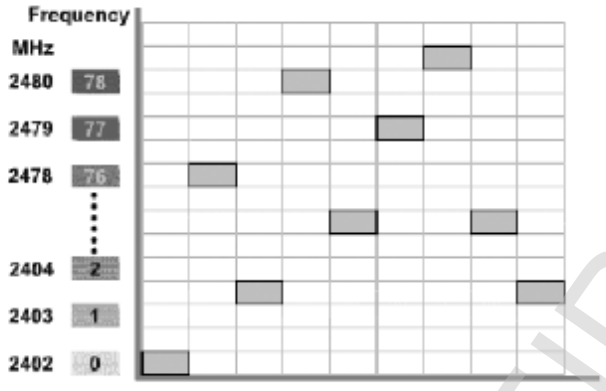
ΠΑΝΕΠΙΣΤΗΜΙΑΚΑ

ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ BLUETOOTH	ΠΕΡΙΓΡΑΦΗ
Physical Layer	Frequency Hopping Spread Spectrum (FHSS)
Frequency Band	2,4 - 2,4835 GHz (ISM Band)
Hop Frequency	1600 hop/sec
Data Rate	3 Mbps
Data and Network Service	3 είδη ασφάλειας (none, link-level, service-level), 2 στάδια εμπιστευτικότητας συσκευής, 3 στάδια service security, κρυπτογράφηση, challenge-response για αυθεντικοποίηση, PIN και διάφορα κλειδία για διαχείρηση
Operating Range	Γύρω στα 10 μέτρα αλλά μπορεί να φτάσει και μέχρι τα 100
Throughput	Περίπου στα 2,2 Mbps
Πλεονεκτήματα	'Οχι χρήση καλωδίων, δυνατότητα διαπέρασης τοίχων και άλλων εμποδίων, χαμηλό κόστος και δύναμη, ελάχιστο hardware
Μειονεκτήματα	Πιθανότητα για επέμβαση άλλων ISM Band τεχνολογιών, ακόμα χαμηλός ρυθμός δεδομένων αναλόγως

3.2 Πως δουλεύει το Bluetooth

Το Bluetooth σχεδιάστηκε να λειτουργεί στην χωρίς-άδεια ISM (Industrial Scientific and Medical) ζώνη συχνοτήτων στα 2,4GHz. Αυτή η συχνότητα χρησιμοποιείται από συσκευές όπως οι φούρνοι μικροκυμάτων, τα ασύρματα τηλέφωνα και τις ασύρματες συσκευές δικτύωσης 802.11b/g. Για την αποφυγή παρεμβάσεων από αυτές τις συσκευές, το Bluetooth χρησιμοποιεί μια τεχνολογία που λέγεται FHSS (Frequency Hopping Spread Spectrum), η οποία αλλάζει την συχνότητα μετάδοσης μέχρι 1600 φορές ανά δευτερόλεπτο, σε 79 διαφορετικές συχνότητες σε διαστημα καναλιών 1 MHz.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



A sample FHSS distribution

Ένα κανάλι χρησιμοποιείται σε 625ms ακολουθούμενο από ένα hop σε μια ψευδοτυχαία διαταγή σε ένα άλλο κανάλι για 625ms και αυτή η διαδικασία επαναλαμβάνεται συνεχώς. Η τεχνολογία Bluetooth επιτρέπει ταχύτητες μετάδοσης μέχρι 3Mbps στις μέρες μας επιτυχάνοντας ρυθμοαπόδοση περίπου γύρω στα 2,4Mbps.

Υπάρχουν 3 κλάσεις των συσκευών Bluetooth, που χωρίζονται με βάση την δύναμη που χρησιμοποιούν και την ακτίνα που έχουν.

Type	Power	Power Level	Operating Range
Class 1 Devices	High	100 mW (20 dBm)	Up to 100 meters
Class 2 Devices	Medium	2.5 mW (4 dBm)	Up to 10 meters
Class 3 Devices	Low	1 mW (0 dBm)	0.1–10 meters

Οι Bluetooth συσκευές στα ad-hoc δίκτυα λέγονται piconets. Στα piconets, μια Bluetooth συσκευή συμπεριφέρεται σαν master και οι άλλες σαν slaves. Οι master ρυθμίζουν την frequency hopping συμπεριφορά στο piconet. Είναι επίσης δυνατό να συνδεθούν μέχρι 10 piconets το ένα με το άλλο, σε μια μορφή η οποία ονομάζεται scatternets.

Οι Bluetooth συσκευές αυτόματα προσπαθούν να επικοινωνήσουν όταν μια συσκευή έρχεται στην ακτίνα της άλλης. Ανακαλύπτουν η μία την άλλη και έτσι αρχίζουν να επικοινωνούν έχοντας έτσι την δυνατότητα να διαμορφώνουν τα ad-hoc δίκτυα. Η τοπολογία αυτών των δικτύων είναι προσωρινή και τυχαία. Στα ad-hoc δίκτυα 2 ή περισσότερες συσκευές ονομάζονται piconet.

Όταν 2 Bluetooth συσκευές δημιουργήσουν μια σύνδεση, καθορίζουν αυτόματα αν μια συσκευή χρειάζεται να ελέξει την άλλη. Γενικά η συσκευή που αρχίζει την επικοινωνία

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

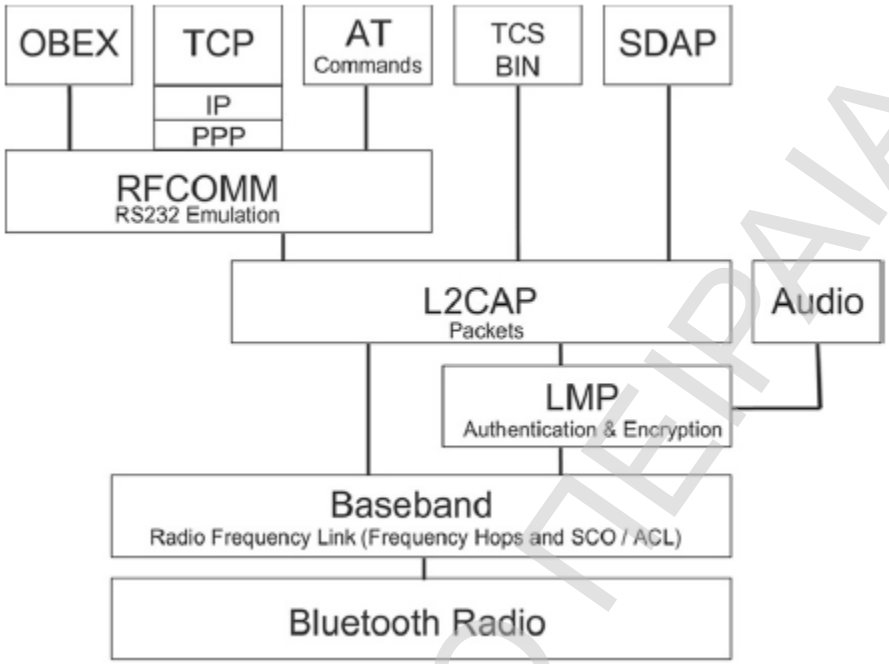
υποτίθεται έχει τον ρόλο του master και ασκεί ορισμένους ελέγχους στα μέρη του piconet, τα γνωστά ως slaves. Οι slaves συσκευές συγχρονίζουν την frequency hopping ακολουθία τους και το system clock με αυτό του master ώστε να διατηρήσουν την σύνδεση τους. Μια συσκευή master μπορεί να έχει μέχρι 7 slaves. Ένας slave μέσα σε ένα piconet μπορεί να αποτελεί τον master κάποιου άλλου, επιτρέποντας έτσι στα piconets να αλληλεπιδρούν διαμορφώνοντας αυτό που είναι γνωστό ως scatternets.

Η συχνότητα με την οποία όλες οι Bluetooth συσκευές, όπως είδαμε και πιο πάνω, διαβιβάζουν τα σήματα τους έχει έυρος από 2,402 μέχρι 2,480GHz. Αυτή η συχνότητα υποδιαιρείται σε 79 ζώνες. Η master συσκευή ελέγχει την πρόσβαση σε αυτές τις ζώνες και τα hop μεταξύ των καναλιών έχουν ποσοστό περίπου 1600 φορές το δευτερόλεπτο.

Το Bluetooth περιέχει μια σειρά προφίλ που επιτρέπει την ανακάλυψη και την ανταλλαγή δεδομένων. Το SDAP (Service Discovery Application Profile) ανακαλύπτει άλλες συσκευές και τις υπηρεσίες που προσφέρουν. Μόλις ανακαλυφθεί μία, ο χρήστης μπορεί να χρησιμοποιήσει οποιαδήποτε από τα υποστηριζόμενα προφίλ όπως τα προφίλ τηλεφωνικού ελέγχου (όπου επιτρέπουν φωνή και walkie-talkie συνομιλία), serial-port προφίλ (για πρόσβαση δικτύου και dial-up συνδέσεις) ή OBEX (Object Exchange προφίλ για συγχρονισμό, ή μεταφορά αρχείων). Νέα και ενημερωμένα προφίλ συνεχώς προστίθενται στις προδιαγραφές Bluetooth για περαιτέρω βελτιώσεις και επέκταση της λειτουργίας.

Τα πρωτόκολλα Bluetooth δεν δουλεύουν ξεχωριστά αλλά συνδυάζονται μεταξύ τους για την παράδοση των υπηρεσιών όπως φαίνεται και στην πιο κάτω εικόνα.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



Πρωτόκολλα Bluetooth

3.3 Bluetooth Protocols

- Bluetooth Radio

Το bluetooth Radio είναι το χαμηλότερο στρώμα όπως καθορίζεται από την bluetooth προδιαγραφή. Καθορίζει τις απαιτήσεις των συσκευών πομποδεκτών bluetooth που λειτουργούν στην ζώνη των 2,4 GHz.

- Bluetooth Baseband

Το Baseband χαρακτηρίζεται ως το φυσικό στρώμα του bluetooth. Διαχειρίζεται τα φυσικά κανάλια και συνδέσεις καθώς και άλλες υπηρεσίες όπως την διόρθωση λάθους και την ασφάλεια του bluetooth. Το baseband στρώμα βρίσκεται πάνω από το bluetooth radio στρώμα στην στοίβα πρωτοκόλλων. Το πρωτόκολλο baseband μεταφέρει link layer routines όπως link connections και power control.
Το baseband διαχειρίζεται επίσης τις ασύγχρονες και σύγχρονες συνδέσεις, χειρίζεται τα πακέτα και ελέγχει όλες τις συσκευές που βρίσκονται στην περιοχή.

- Link Manager Protocol (LMP)

Ο link manager πραγματοποιεί την οργάνωση των συνδέσεων, την επικύρωση, την διαμόρφωση των συνδέσεων καθώς και άλλων πρωτοκόλλων. Ανακαλύπτει άλλους απομακρυσμένους link managers και επικοινωνεί μαζί τους μέσω του link manager protocol. Για να εκτελέσει τον ρόλο του ως

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

πάροχος υπηρεσιών χρησιμοποιεί τις υπηρεσίες του link controller (LC).

- Host Controller Interface (HCI)

Ο host controller interface παρέχει μια command interface στον baseband controller και τον link manager, καθώς και πρόσβαση στο hardware. Ουσιαστικά αυτή η διεπαφή παρέχει μια ομοιόμορφη μέθοδο για πρόσβαση σε δυνατότητες του bluetooth baseband. Το HCI υπάρχει σε 3 τμήματα, host, το transport layer και το host controller. Καθένα από αυτά τα 3 τμήματα διαδραματίζει διαφορετικό ρόλο στο HCI σύστημα.

- Logical Link Control and Adaptation Protocol (L2CAP)

Το L2CAP στην στοίβα πρωτοκόλλων του bluetooth τοποθετείται πάνω από το baseband και το LMP. Παρέχει connection-oriented και connectionless υπηρεσίες δεδομένων στα ανώτερα στρώματα πρωτοκόλλων κυρίως με την διαδικασία του κατακερματισμού και της επανασυναρμολόγησης. Το L2CAP επιτρέπει στα πρωτόκολλα των υψηλότερων στρωμάτων και τις εφαρμογές τους να διαβιβάσουν και να λάβουν πακέτα δεδομένων μέχρι 64 KB μήκος. Εξετάζει επίσης και την ποιότητα υπηρεσίας (QoS). Δύο τρόποι συνδέσεων υποστηρίζονται για το baseband στρώμα: οι Synchronous connection-oriented συνδέσεις (SCO) και οι Asynchronous connection-less συνδέσεις (ACL). Οι SCO συνδέσεις υποστηρίζουν κυκλοφορία φωνής σε πραγματικό χρονο χρησιμοποιώντας διατηρημένο BW. Οι ACL υποστηρίζουν καλύτερη προσπάθεια κυκλοφορίας.
Η προδιαγραφή L2CAP καθορίζεται μόνο για συνδέσεις ACL ενώ οι SCO δεν υποστηρίζονται.

- RFComm

Το RFComm παρέχει emulation των σειριακών πορτών πέρα από το L2CAP, δηλ μαζί με τα προφίλ υπηρεσιών επιδυκνύουν και επιτρέπουν υπηρεσίες.

- Service Discovery Application (SDAP)

Το SDAP παρέχει διάφορα μέσα για τις εφαρμογές ώστε να ανακύφθούν ποιες υπηρεσίες έιναι διαθέσιμες και να καθορίσει τα χαρακτηριστικά αυτών των διαθέσιμων υπηρεσιών.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

3.4 Bluetooth profiles

Τα προφίλς έχουν αναπτυχθεί προκειμένου να περιγράψουν πως οι εφαρμογές των μοντέλων-προτύπων χρηστών πρόκειται να ολοκληρωθούν. Τα μοντέλα χρηστών περιγράφουν διάφορα σενάρια χρηστών όπου το bluetooth εκτελεί την ‘ραδιομετάδοση’.
Τα σημαντικότερα προφίλ παρουσιάζονται πιο κάτω:

- GAP Profile (Generic Access Profile)
- DNP ή DUN (dial up network)
- SPP (serial port) (rfcomm)
- LAP Lan access profile
- Pan (BNEP) Personal area network
- Sdap (Service Discovery Application Profile)
- CTP (Cordless Telephony Profile)
- IP (Intercom profile)
- HS (Headset profile)
- FP (Fax profile)
- GOEP (Generic Object Exchange Profile) (obex)
- OPP (Object push profile)
- FTP (File transfer profile)
- SP (Synchronisation profile) (PIM-data)

- **GAP Profile**

Το GAP προφίλ καθορίζει τις γενικές διαδικασίες που είναι σχετικές με την ανακάλυψη bluetooth συσκευών και διάφορες άλλες πτυχές όσον αφορά το management στις συνδέσεις με τις bluetooth συσκευές. Αποτελέι τον πυρήνα στον οποίο όλα τα άλλα προφίλ είναι βασισμένα.

- **DNP ή DUN profile**

Το DUN προφίλ καθορίζει τις απαιτήσεις που θα χρησιμοποιηθούν από τις συσκευές (π.χ μόντεμς και κινητά τηλέφωνα) εφαρμόζοντας το μοντέλο χρήσης αποκαλούμενο ως internet brigde. Ο ρόλος των πυλών (gateways) χρησιμοποιείται χαρακτηριστικα σε έαν κινητό τηλέφωνο το οποίο έχει την ικανότητα εισόδου στο διαδίκτυο.

- **STP Profile**

Το STP προφίλ καθορίζει τις απαιτήσεις για τις συσκευές bluetooth που είναι απαραίτητες για τις ρυθμίσεις των σειριακών συνδέεων με την χρήση του RFComm μεταξύ δύο όμοιων συσκευών.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

- LAP Profile

Το LAP προφίλ καθορίζει πως το bluetooth επιτρέπει σε συσκευές να έχουν πρόσβαση σε ένα LAN χρησιμοποιώντας PPP. Επίσης αυτο το προφίλ μας δείχνει πως οι ίδιο PPP μηχανισμοί χρησιμοποιούνται για να διαμορφώσουν ένα δίκτυο που αποτελείται από 2 bluetooth συσκευές.

- PAN Profile

Η PAN Bluetooth προδιαγραφή ενθυλάκωσης δικτύων περιγράφει το πρωτόκολλο που χρησιμοποιείται από τα bluetooth PANs προφίλ (BNET – Bluetooth Network Encapsulation Protocol). Καθορίζεται ένα σχήμα πακέτων για την ενθυλάκωση δικτύων με bluetooth που χρησιμοποιείται για να μεταφέρει τα κοινά πρωτόκολλα δικτύωσης πέρα από τα μέσα bluetooth. Η ενθυλάκωση δικτύων bluetooth υποστηρίζει τα ίδια πρωτόκολλα δικτύωσης που υποστηρίζονται από την IEEE 802.3/Ethernet για την ενθυλάκωση.

- SDAP Profile

Το SDAP προφίλ καθορίζει τα χαρακτηριστικά γνωρίσματα και τις διαδικασίες για μια εφαρμογή σε μια συσκευή Bluetooth ώστε να ανακαλυφθούν οι υπηρεσίες που εγγράφονται σε άλλες συσκευές Bluetooth και να ανακτηθούν οποιεσδήποτε επιθυμητές διαθέσιμες πληροφορίες σχετικά με αυτές τις υπηρεσίες.

- CTP Profile

Το CTP καθορίζει τα χαρακτηριστικά γνωρίσματα και τις διαδικασίες που απαιτούνται για τη διαλειτουργικότητα μεταξύ των διαφορετικών ενεργιών που παρουσιάζονται στην περίπτωση της τηλεφωνικής χρήσης. Αυτό το σχεδιάγραμμα επιδεικνύει επίσης πώς η περίπτωση χρήσης μπορεί να εφαρμοστεί γενικά για την ασύρματη τηλεφωνία, σε ένα κατοικημένο ή ένα μικρό περιβάλλον γραφείων.

- IP Profile

Το IP προφίλ καθορίζει τις απαιτήσεις για τις συσκευές Bluetooth που είναι απαραίτητες για την υποστήριξη της λειτουργίας ενδοσυνεννοήσεων σε μία περίπτωση τηλεφωνικής χρήσης. Αυτό μπόρει επίσηση να αναφερθέι ως ένα έιδος ' walkie-talkie' με την χρήση Bluetooth.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

- HS Profile

Το HS καθορίζει τις απαιτήσεις που θα χρησιμοποιηθούν από τις συσκευές με την εφαρμογή του μοντέλου χρήσης αποκαλούμενο ως 'Ultimate Headset'.

- FP Profile

Το FP προφίλ καθορίζει τις απαιτήσεις για τις συσκευές Bluetooth οι οποίες είναι απαραίτητες για να υποστηρίξουν την χρήση fax. Αυτό επιτρέπει σε ένα κινητό τηλέφωνο Bluetooth (ή το μόντεμ) να χρησιμοποιηθεί από έναν υπολογιστή ως ένα ασύρματο fax που στέλνει και λαμβάνει ένα μήνυμα fax.

- GOEP Profile

Το GOEP προφίλ καθορίζει τα πρωτόκολλα και τις διαδικασίες για τις συσκευές Bluetooth που είναι απαραίτητες για την υποστήριξη των object exchange usage models, όπως τον συγχρονισμό ή την μεταφορά αρχείων.

- OPP Profile

Τα χαρακτηριστικά σενάρια που καλύπτονται από αυτό το προφίλ περιλαμβάνουν pushing/pulling των αντικειμένων στοιχείων μεταξύ των συσκευών Bluetooth.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

3.5 Security Modes - **Τρόποι Ασφάλειας**

Το Bluetooth χαρακτηρίζεται από 3 διαφορετικούς τρόπους ασφάλειας. Κάθε Bluetooth συσκευή μπορεί να λειτουργήσει με μόνο ένα τρόπο σε μία ορισμένη στιγμή. Οι τρεις τρόποι είναι:

- Security Mode 1 – Nonsecure mode
- Security Mode 2 – Service level mode
- Security Mode 3 – Link Service mode

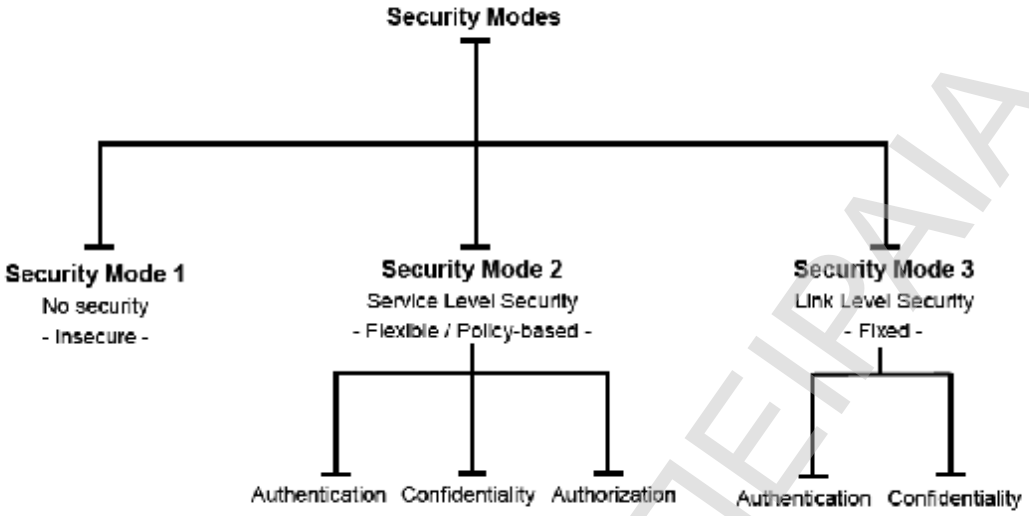
Στον nonsecure mode μία συσκευή δεν αρχίζει από μόνη της οποιεσδήποτε διαδικασίες ασφάλειας. Εδώ, οι διάφορες λειτουργίες ασφάλειας όπως η αυθεντικοποίηση και η κρυπτογράφηση παρακάμπτονται εντελώς. Αυτός ο τρόπος είναι κατάλληλος για συσκευές στις οποίες δεν απαιτείται μεγάλη ασφάλεια.

Στον service level security mode οι διαδικασίες για την ασφάλεια ξεκινούν μετά την καθιέρωση του καναλιού στο Logical Link Control and Adaptation Protocol (L2CAP). Το L2CAP είναι μέρος του στρώματος σύνδεσης δεδομένων και παρέχει connection-oriented και connectionless υπηρεσίες δεδομένων στα ανώτερα στρώματα, όπως είδαμε και πιο πάνω. Σε αυτόν τον τρόπο, ένας διαχειριστής ασφάλειας ελέγχει την πρόσβαση στις υπηρεσίες και τις συσκευές. Περισσότερη ασφάλεια και διάφορα επίπεδα εμπιστοσύνης μπορεί να είναι καθορισμένα για εφαρμογές με διαφορετικές απαιτήσεις ασφάλειας. Έτσι είναι πιθανό να χορηγηθεί πρόσβαση σε μερικές υπηρεσίες χωρίς να δοθεί όμως σε άλλες.

Στο link level security mode μία Bluetooth συσκευή αρχίζει τις διαδικασίες ασφάλειας χωρίς να έχει καθιερωθεί το κανάλι. Είναι ένας ενσωματωμένος μηχανισμός ασφάλειας και δεν γνωρίζει οποιαδήποτε ασφάλεια στα στρώματα εφαρμογών. Αυτός ο τρόπος υποστηρίζει την αυθεντικοποίηση και την κρυπτογράφηση. Αυτά τα χαρακτηριστικά είναι βασισμένα σε ένα μυστικό κλειδί σύνδεσης που μοιράζεται από ένα ζευγάρι συσκευών. Για την δημιουργία αυτού του κλειδιού μία διαδικασία ένωσης χρησιμοποιείται όταν δύο συσκευές επικοινωνούν για πρώτη φορά.

Οι πιο πάνω τρόποι φαίνονται σχεδιαγραμματικά στην πιο κάτω εικόνα.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



3.6 Security Objectives

Access Control
Authentication (link layer)
Authorization (application layer)
Confidentially
Integrity

3.7 Επισκόπηση ασφάλειας

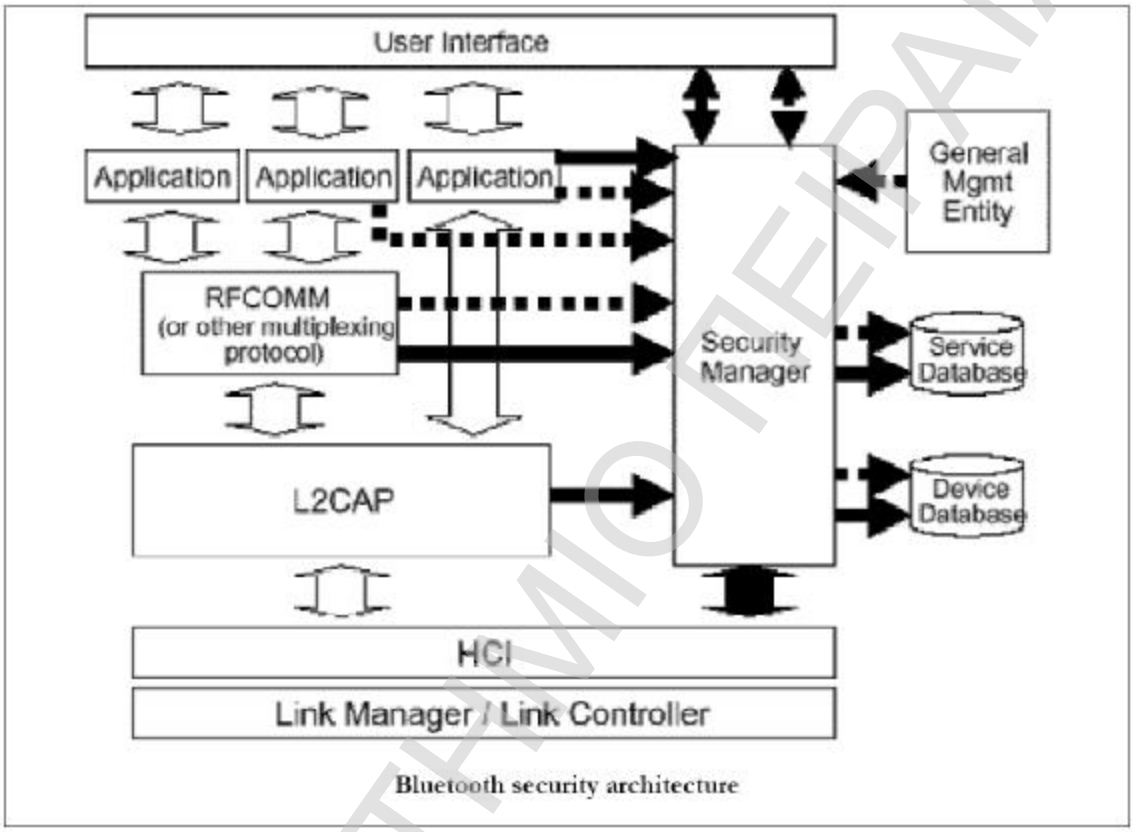
Το Bluetooth χρησιμοποιεί ένα συμμετρικό μοντέλο κρυπτογράφησης. Επομένως όπως είναι λογικό με τον ίδιο τρόπο εκτελείται και η αποκρυπτογράφηση, χρησιμοποιώντας το ίδιο κλειδί και στην κρυπτογράφηση, ενώ τα μυστικά κλειδιά πρέπει να αλλάζονται.

Για την διατήρηση της ασφάλειας στο στρώμα σύνδεσης χρησιμοποιούνται 4 διαφορετικές οντότητες:

- Μια Bluetooth device address, BD_ADDR ίση με 48 bits
- Ένα μυστικό authentication key, το link key που είναι ίσο με 128 bits
- Ένα μυστικό encryption key από 8-128 bits, το οποίο προέρχεται από το authentication key. Κάθε φορά που ενεργοποιείται η κρυπτογράφηση, ένα νέο encryption key δημιουργείται.
- Ένας ψευδοτυχαίος αριθμός RAND ίσος με 128 bits, ο οποίος αναπαράγεται για κάθε νέα συναλλαγή. Κάθε συσκευή έχει μια ειδική γεννήτρια η οποία είναι υπεύθυνη για την αναπαραγωγή αυτών των ψευδοτυχαίων αριθμών.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Το στρώμα σύνδεσης είναι διαφανής στους ελέγχους ασφαλείας που επιβάλλονται από το στρώμα εφαρμογής. Έτσι αυτό είναι πιθανό να επιβάλει used-based αυθεντικοποίηση και fine-grained έλεγχο πρόσβασης στο πλαίσιο ασφαλείας του Bluetooth.



Bluetooth security architecture

3.8 Integrity check

Τα πακέτα ελέγχονται για λάθη ή για λανθασμένη μεταφορά κωδικό πρόσβασης καναλιού, το HEC για την επικεφαλίδα ή το CRC για το φορτίο.

Ένα πακέτο μπορεί να αποτελείται από:

- Τον μικρότερο κωδικό πρόσβασης μόνο
- Τον κωδικό πρόσβασης και την επικεφαλίδα του πακέτου
- Τον κωδικό πρόσβασης, την επικεφαλίδα του πακέτου καθώς και το φορτίο.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Κωδικός πρόσβασης
Κάθε πακέτο αρχίζει με ένα κωδικό πρόσβασης, ο οποίος χρησιμοποιείται για συγχρονισμό και έλεγχο ταυτότητας. Ο κωδικός πρόσβασης αναγνωρίζει όλα τα πακέτα που ανταλλάζονται σε ένα φυσικό κανάλι.

Header Check Error (HEC)
Κάθε επικεφαλίδα έχει ένα HEC για να ελέγχει την ακεραιότητα της επικεφαλίδας. Το HEC είναι ένας κώδικας μήκους 8 bit.

CRC κώδικας
Σε κάθε φορτίο υπάρχει ένας CRC κώδικας ίσος με 16 bit.

3.9 Key Management Service
Ένα κλειδί σύνδεσης (link key) χρησιμοποιείται κατά την διάρκεια της διαδικασίας της αυθεντικοποίησης και μία από τις παραμέτρους του είναι ο υπολογισμός του κλειδιού κρυπτογράφησης (encryption key).

Τα κλειδιά σύνδεσης είναι είτε προσωρινά είτε ημι-μόνιμα. Ένα ημι-μόνιμο κλειδί σύνδεσης μπορεί να αποθηκεύεται σε μια αμετάβλητη μνήμη και μπορεί να χρησιμοποιηθεί αφότου τερματιστεί η τρέχουσα σύνδεση. Η διάρκεια ζωής ενός προσωρινού κλειδιού σύνδεσης εξαρτάται από την διάρκεια ζωής της τρέχουσας συνόδου.

Υπάρχουν 4 τύποι κλειδιών συνδέσεων:

- **Το** unit key K_a: Αν μία συσκευή Α έχει μικρή μνήμη, τότε μπορεί να χρησιμοποιήσει το unit key για όλες τις συνδέσεις. Αυτό το κλειδί αλλάζει πολύ σπάνια.
- **Το** initialization key K_{init}: Το initialization key χρησιμοποιείται ως κλειδί σύνδεσης κατά την διάρκεια της επεξεργασίας του initialization. Οι παραμέτροι initialization είναι κρυπτογραφημένοι χρησιμοποιώντας το initialization key και μεταφέρονται. Το κλειδί προέρχεται από ένα τυχαίο αριθμό, ένα L-byte PIN κώδικα και ένα BD_ADDR.
- **Το** combination key K_{AB}: Το combination key είναι συγκεκριμένο για κάθε ζευγάρι από συσκευές.
- **Το** temporary key K_{master}: Αν μια master συσκευή θέλει να στείλει ένα μήνυμα σε περισσότερες από μια συσκευές ταυτόχρονα, αντικαθιστά το αυθεντικό link

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

key προσωρινά με ένα master key και έτσι χρησιμοποιείται το master key ως link key.

Το combination key και το unit key λειτουργικά δεν έχουν μεγάλες διαφορές μεταξύ τους. Η διαφορά τους είναι στον τρόπο με τον οποίο δημιουργούνται.

3.10 PIN

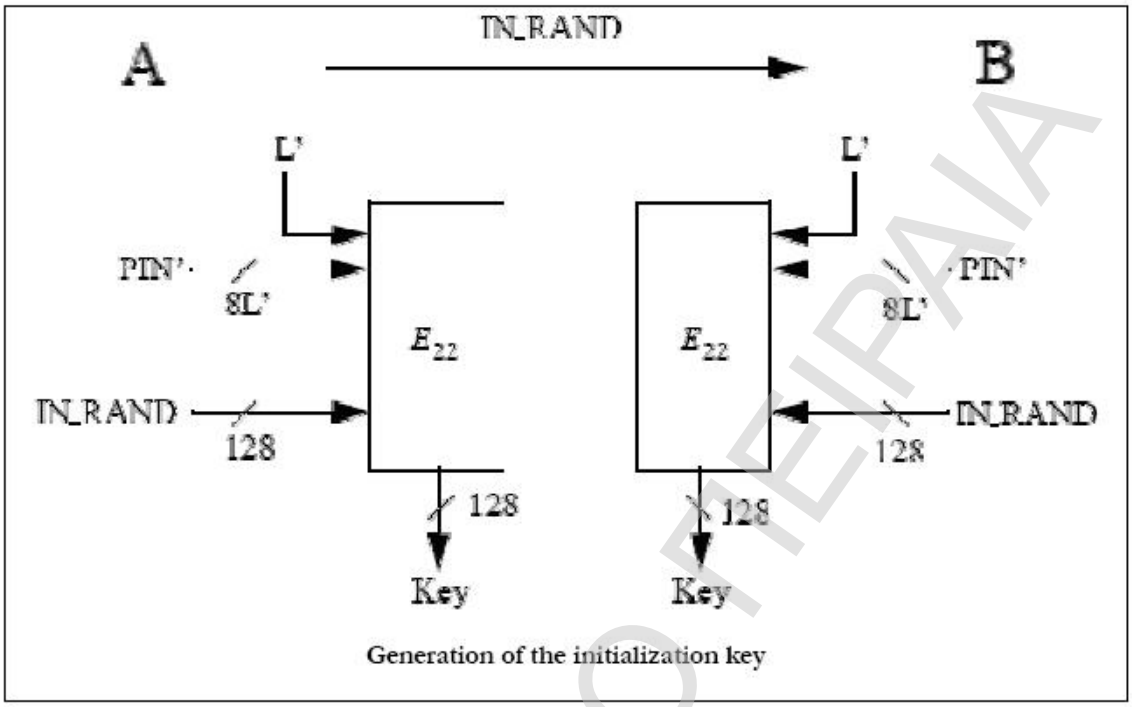
Το PIN είναι ένας σταθερός αριθμός που παρέχεται με την συσκευή ή μπορεί να διαλεχθεί από τον χρήστη. Εάν δεν είναι διαθέσιμο, χρησιμοποιείτε μια αρχική τιμή με μηδενικά (0X00). Ο κωδικός PIN μπορεί να έχει οποιοδήποτε μέγεθος από 1 μέχρι 16 bytes.

3.11 Encryption key K_c

Το encryption key ανακτάται από το τρέχον link key. Κάθε φορά που ενεργοποιείται η κρυπτογράφηση, το encryption key αλλάζει αυτόματα. Για να είναι εφικτή η χρησιμοποίηση ενός encryption key χωρίς αδυναμίες στην αυθεντικοποίηση, το μήκος του μπορεί να διαμορφώνεται ξεχωριστά.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

3.12.1 **Δημιουργία του** initialization key K_{init}



Generation of the initialization key

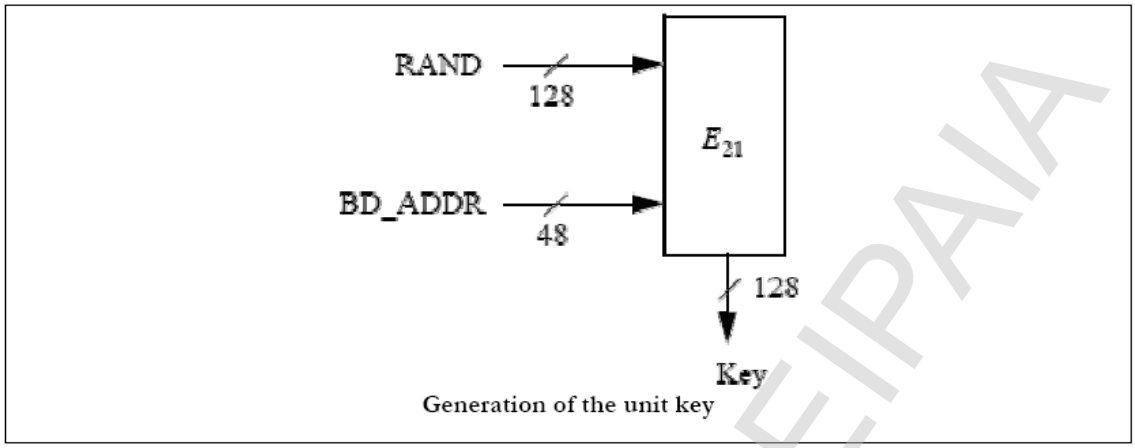
Ένα link key το οποίο χρησιμοποιείται προσωρινά κατά την διάρκεια του initialization, ονομάζεται initialization key.
Ο αλγόριθμος E 22 (τον οποίο θα μελετήσουμε πιο κάτω) παράγει το initialization key από ένα BD_ADDR, ένα PIN κώδικα, το μήκος του PIN (σε bytes L) και ένα τυχαίο αριθμό IN_RAND.

Το PIN μπαίνει από ένα χρήστη και στις 2 συσκευές και χρησιμοποιείται ως το αυθεντικό μυστικό που χρησιμοποιείται για την δημιουργία του κλειδιού. Το PIN αυξάνεται με το BD_ADDR. Αν μια συσκευή έχει ένα σταθερό PIN, θα χρησιμοποιηθεί από την άλλη συσκευή το BD_ADDR. Αν και οι 2 συσκευές έχουν μεταβλητό PIN θα χρησιμοποιήσουν το BD_ADDR από την συσκευή που έχει λάβει το IN_RAND. Αν 2 συσκευές έχουν σταθερό PIN δεν μπορούν να γίνουν ζευγάρι. Από την στιγμή που το μέγιστο μήκος του PIN που χρησιμοποιείται στον αλγόριθμο δεν ξεπερνάει τα 16 bytes, είναι πιθανό να μην χρησιμοποιηθούν όλα τα bytes από το BD_ADDR.

3.12.2 Δημιουργία του unit key K_A

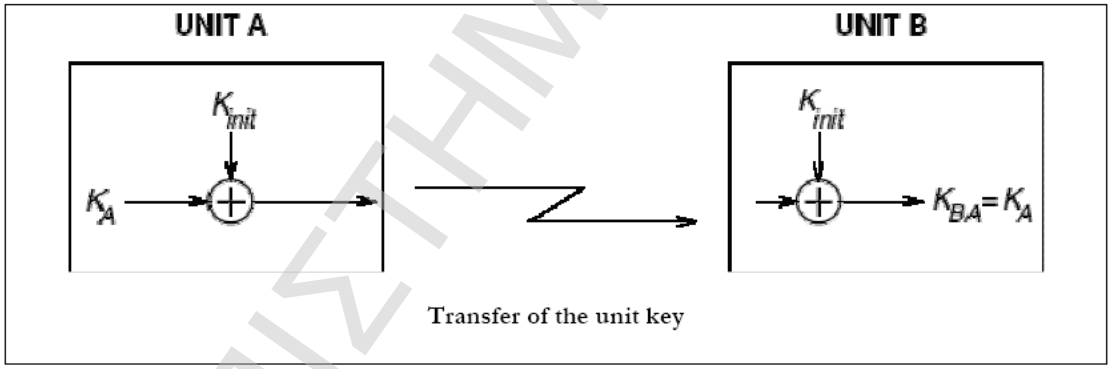
Το unit key δημιουργείται από τον αλγόριθμο E21 (τον οποίο θα δούμε και αυτόν αργότερα).

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



Generation of the unit key

Το unit key της συσκευής A, K_A, χρησιμοποιείται ως το link key για την σύνδεση A-B. Η συσκευή A στέλλει το unit key K_A στην συσκευή B, όπου η συσκευή B θα αποθηκεύσει το K_A ως link key K_{BA}. Για άλλο initialization, για παράδειγμα με την συσκευή C, η συσκευή A θα ξαναχρησιμοποιήσει το unit key K_A όπου η συσκευή C θα το αποθηκεύσει ως το K_{CA}.



Transfer of the unit key

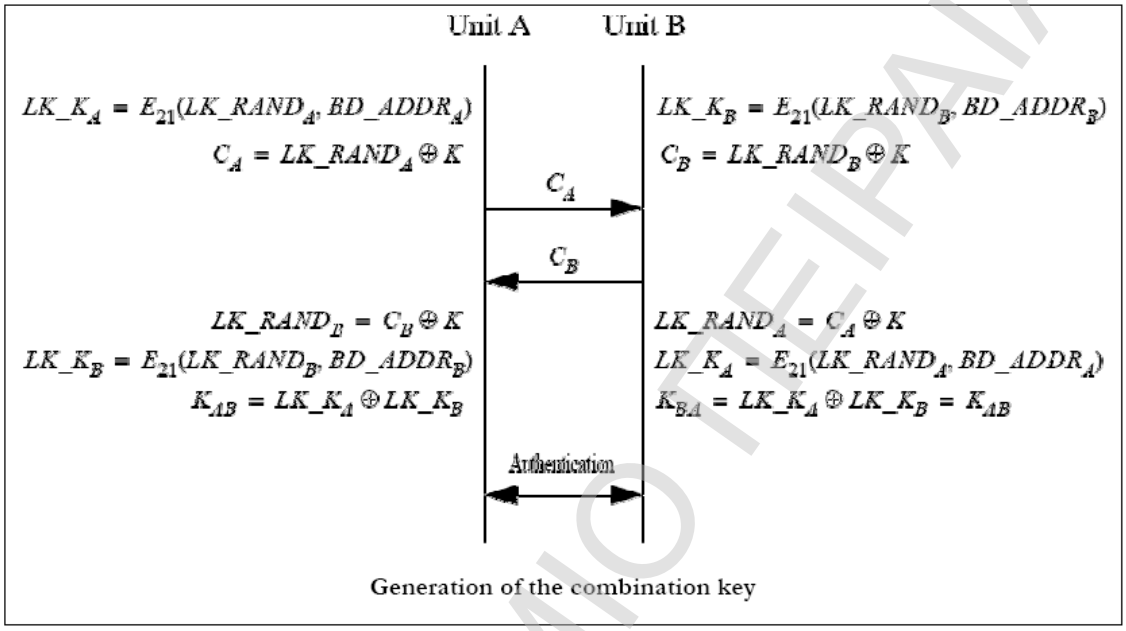
3.12.3 Δημιουργία του combination key K_{AB}

Το combination key είναι ο συνδυασμός 2 αριθμών που δημιουργήθηκαν σε μια συσκευή A και μία άλλη B αντιστοίχως.
Κάθε συσκευή δημιουργά ένα τυχαίο αριθμό LK_RAND_A και LK_RAND_B. Μετά, με την έναρξη του E21 δημιουργούνται τα LK_K_A και LK_K_B.

LK_K = E21 (LK_RAND, BD_ADDR)

Στο LK_K_A και LK_K_B γίνεται η μέθοδος XOR με το τρέχον link key το οποίο ήδη μοιράστηκε και ανταλλάκτηκε. Η

συσκευή A υπολογίζει το LK_RAND_A και η συσκευή B το LK_RAND_B.
Το K_{AB} υπολογίζεται απλά με την μέθοδο XOR μεταξύ του LK_K_A και LK_K_B.



Generation of the combination key

Όταν και οι 2 συσκευές παράγουν το νέο combination key, μια αμοιβαία διαδικασία αυθεντικοποίησης αρχίζει ώστε να έχουμε επιβεβαίωση για την επιτυχή ανταλλαγή. Το παλιό link key απορρίπτεται μετά την επιτυχημένη ανταλλαγή ενός καινούργιου combination key.

3.12.4 Δημιουργία του master key K_{master}

Ο master δημιουργεί ένα νέο link key από 2 28-bit τυχαίους αριθμούς, το RAND1 και RAND2

K_{master} = E22 (RAND1, RAND2, 16)

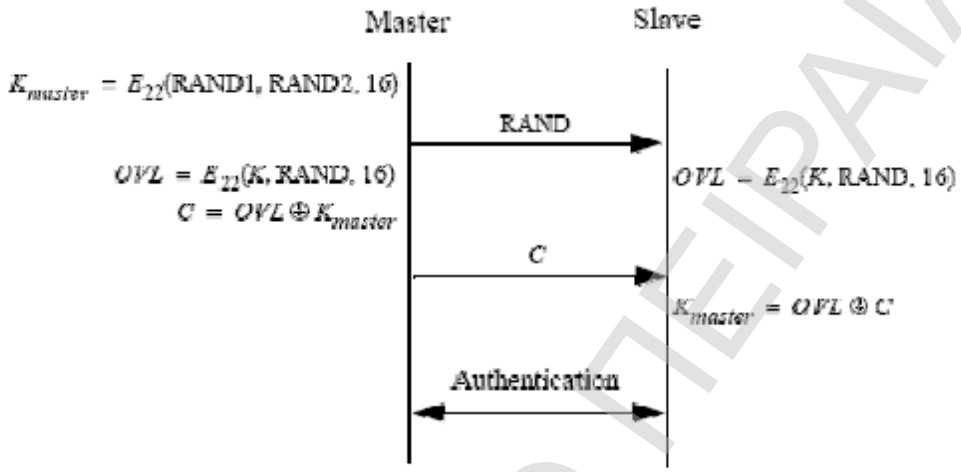
Ένα ακόμα RAND στέλλεται στον slave. Και στις 2 μεριές υπολογίζεται ένα overlay (OVL) χρησιμοποιώντας τον αλγόριθμο E22 μαζί με το τρέχον link key και το RAND.

OVL = E22 (K, RAND, 16)

Ο slave στέλλει τα ήδη γνωστά bit (από την μέθοδο XOR) από το OVL και το νέο link key στον slave. Ο slave ξαναυπολογίζει το K_{master}. Για να επαληθεύσουν την επιτυχία αυτής της ανταλλαγής, οι συσκευές εκτελούν μια διαδικασία

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

αυθεντικοποίησης χρησιμοποιώντας το νέο link key. Η διαδικασία επαναλαμβάνεται για κάθε slave που λαμβάνει ένα νέο Link key.



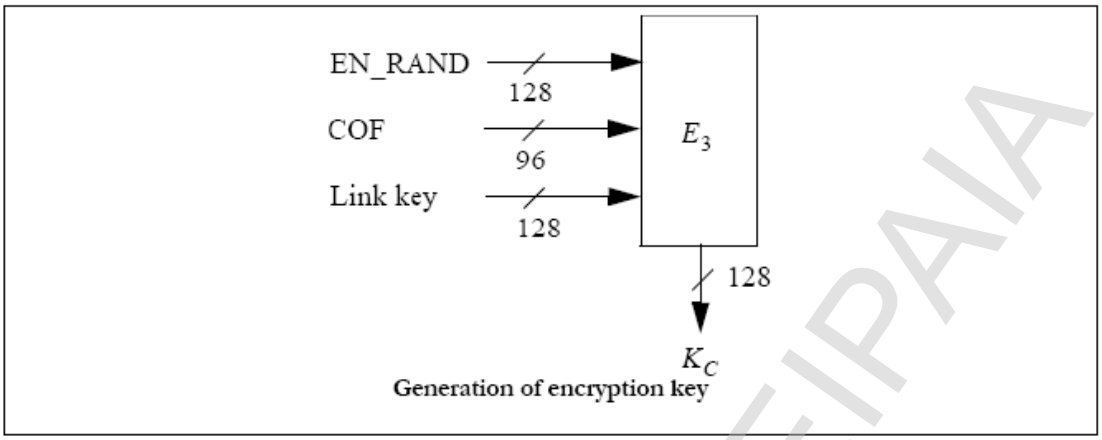
Distribution of the master key

3.12.5 Δημιουργία του encryption key K_c

Το encryption key παράγεται από τον αλγόριθμο E3 από το τρέχον link key, ένα 96-bit Ciphering Offset number (COF) και ένα 128-bit τυχαίο αριθμό. Το COF καθορίζεται με ένα από τους εξής 2 τρόπους: αν το τρέχον link key είναι ένα master key τότε το COF παράγει ένα BD_ADDR από μόνο του, αλλιώς είναι ένα ACO (ορισμός που θα δούμε αργότερα) όπως υπολογίζεται κατά την διάρκεια της διαδικασίας αυθεντικοποίησης.

$$COF = \begin{cases} BD\_ADDR \cup BD\_ADDR, & \text{if link key is a master key} \\ ACO, & \text{otherwise.} \end{cases}$$

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



Generation of encryption key

3.13 Authorization

Authorization,(έγκριση) είναι η διαδικασία από την οποία μια συσκευή Bluetooth καθορίζει αν μια άλλη συσκευή μπορεί να έχει ή όχι πρόσβαση σε μια συγκεκριμένη υπηρεσία. Το authorization ενσωματώνει 2 σημαντικές έννοιες ασφάλειας για το Bluetooth: Σχέσεις εμπιστοσύνης και υπηρεσίες επιπέδων ασφαλείας. Το authorization εξαρτάται από αυθεντικοποίηση, όπου η διαδικασία αυθεντικοποίησης καθιερώνει την ταυτότητα συσκευών η οποία χρησιμοποιείται για τον καθορισμό πρόσβασης.

Η προδιαγραφή Bluetooth επιτρέπει 3 διαφορετικά επίπεδα εμπιστοσύνης μεταξύ των συσκευών:

- Trusted: η συσκευή έχει περάσει από αυθεντικοποίηση και η πρόσβαση σε υπηρεσίες στην συσκευή επιτρέπονται.
- Untrusted: έχει περάσει από αυθεντικοποίηση αλλά όμως η πρόσβαση σε υπηρεσίες στην συσκευή δεν επιτρέπονται.
- Unknown: η συσκευή δεν έχει περάσει από αυθεντικοποήση και θεωρείται ως μη εμπιστεύσιμη.

Υπάρχουν 3 επίπεδα υπηρεσίας ασφαλείας:

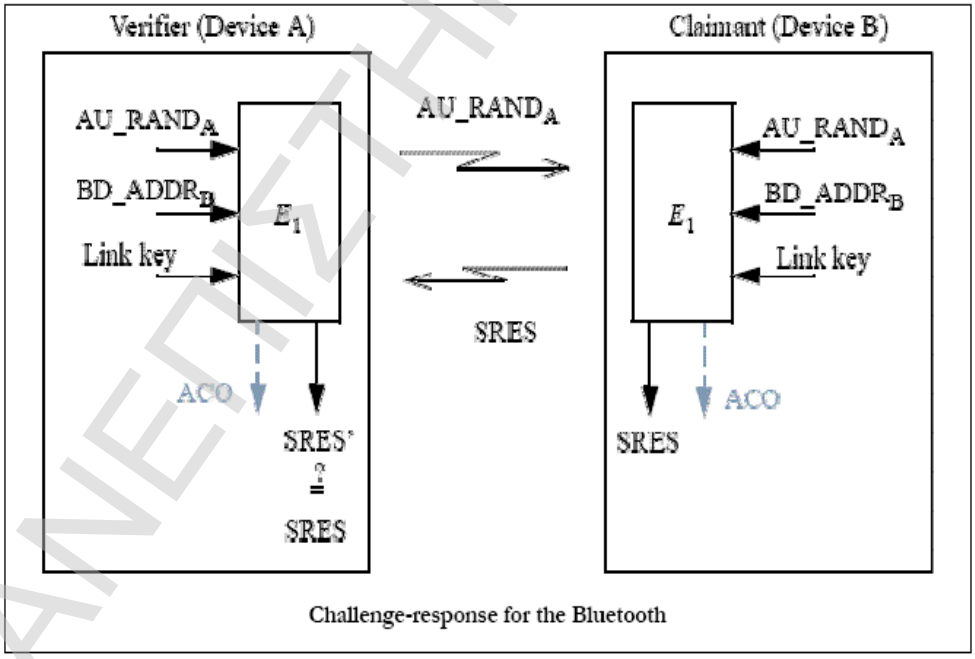
- Το επίπεδο 1: εδώ απαιτούνται και η έγκριση και η αυθεντικοποίηση. Η ταυτότητα της αιτούσας συσκευής πρέπει να επιβεβαιωθεί και η αιτούσα συσκευή πρέπει να λάβει συγκεκριμένη άδεια για πρόσβαση στις υπηρεσίες.
- Το επίπεδο 2: εδώ μόνο η αυθεντικοποίηση απετείται. Η ταυτότητα της αιτούσας συσκευής πρέπει μόνο να επαληθευτεί ότι είναι γνήσια ώστε να επιτύχει πρόσβαση στις υπηρεσίες.
- Το επίπεδο 3: έιναι ανοικτό για όλες τις συσκευές. Η πρόσβαση σε υπηρεσίες θα δοθεί σε όποιαδήποτε συσκευή η οποία είναι κρυπτογραφημένη.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

3.14 Authentication

Για κάθε νέα σύνδεση μεταξύ των συσκευών A και B, χρησιμοποιείται το κοινό link key για αυθεντικοποίηση. Δεν είναι αναγκαία η δημιουργία ενός νέου initialization key. Κατά την διάρκεια της αυθεντικοποίησης ένα νέο AU_RAND_A δημιουργείται.

Η αυθεντικοποίηση χρησιμοποιεί ένα challenge-response μοντέλο στο οποίο η (claimant) πληροφορία ενός μυστικού κλειδιού ελέγχεται διαμέσου ενός πρωτοκόλλου το οποίο αποτελείται από 2 βήματα και χρησιμοποιεί συμμετρικά μυστικά κλειδιά. Αυτό προυποθέτει ότι ένα σωστό ζευγάρι claimant/verifier μοιράζεται το ίδιο μυστικό κλειδί, για παράδειγμα το K. Στο challenge-response μοντέλο ο verifier προκαλεί τον claimant να αυθεντικοποιήσει μια τυχαία είσοδο (πρόκληση) με το AU_RAND_A, με ένα αυθεντικοποιημένο κώδικα, με την χρήση του E1 και επιστρέφει τα αποτελέσματα SRES στον verifier.
Η πιο κάτω εικόνα δείχνει επίσης ότι η είσοδος στο E1 αποτελείται από το AU_RAND_A και την BD_ADDR του claimant. Η χρήση αυτής της διεύθυνσης αποτρέπει οποιαδήποτε απλή σκέψη για επίθεση.



Challenge-response for the Bluetooth

Όταν μια προσπάθεια για αυθεντικοποίηση αποτύχει, για κάθε μεταγενέστερη αποτυχία αυθεντικοποίησης με την ίδια

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

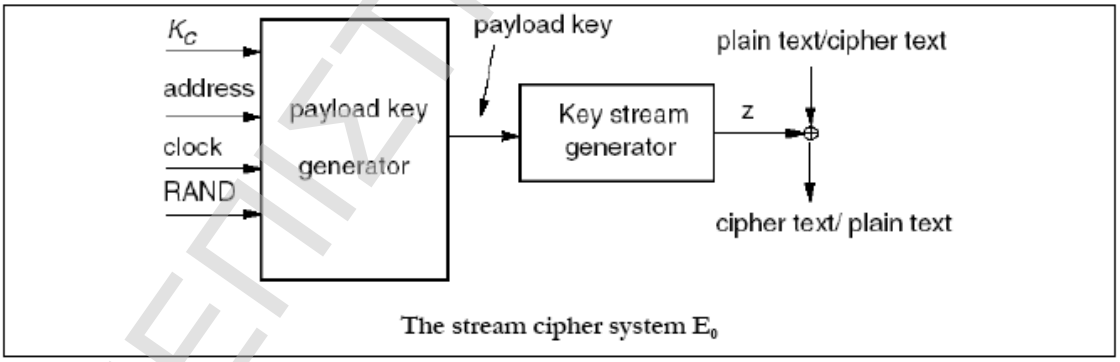
διεύθυνση συσκευής Bluetooth, ο χρόνος αναμονής αυξάνεται εκθετικά.

Όταν δεν παρουσιάζονται νέες αποτυχημένες προσπάθειες κατά την διάρκεια μιας συνηθισμένης χρονικής περιόδου, ο χρόνος αναμονής μειώνεται εκθετικά. Αυτή η διαδικασία αποτρέπει τις denial-of-service (DoS) επιθέσεις, διάφορους παρείσακτους για την επαναλαμβανόμενη διαδικασία αυθεντικοποίησης με ένα μεγάλο αριθμό διαφορετικών κλειδιών.

Για να γίνει το σύστημα λιγότερο τρωτό σε DoS επιθέσεις, η συσκευή πρέπει να κρατά μια λίστα από τους χρόνους αναμονής για κάθε συσκευή με την οποία είχε επαφή. Για την αμοιβαία αυθεντικοποίηση, το πρωτόκολλο που αναφέραμε πιο πριν επαναλαμβάνεται με διαφορετικούς ρόλους.

3.15 Κρυπτογράφηση

Κρυπτογραφημένο είναι μόνο το πακέτο με το χρήσιμο φορτίο (payload). Ο κωδικός πρόσβασης με την επικεφαλίδα του πακέτου ποτέ δεν είναι κρυπτογραφημένα. Η κρυπτογράφηση πραγματοποιείται με ένα 'stream cipher' E_0. Το E_0 συγχρονίζεται κάθε φορά για κάθε φορτίο.



The stream cipher system E_0

Το πιο πάνω σύστημα αποτελείται από 3 μέρη.

- Το πρώτο μέρος εκτελεί το initialization (δημιουργία του payload key). Ο δημιουργός του payload key συνδυάζει τα εισερχόμενα bits με μια κατάλληλη διαταγή και τα αλλάζει σε 4 LFSRs που χρησιμοποιούνται στην δημιουργία του κλειδιού.
- Το δεύτερο μέρος δημιουργά τα key stream bits χρησιμοποιώντας μια μέθοδο, την Massey και Rueppel μέθοδο. Το δεύτερο μέρος είναι και το κύριο μέρος

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

του stream cipher, το οποίο χρησιμοποιείται και στο initialization.

- Το τρίτο μέρος εκτελεί την κρυπτογράφηση και την αποκρυπτογράφηση.

3.15.1 Κρυπτογράφηση για μεταδιδόμενα μηνύματα

Υπάρχουν 3 διαφορετικοί τρόποι κρυπτογράφησης.

- 1ος τρόπος: όχι κρυπτογράφηση
- 2ος τρόπος: point-to-point κρυπτογράφηση. Τα μηνύματα δεν είναι κρυπτογραφημένα.
- 3ος τρόπος: όλα τα μηνύματα είναι κρυπτογραφημένα.

3.15.2 Διαδικασία κρυπτογράφησης

Κάθε συσκευή πρέπει να έχει μέγιστο και ελάχιστο επιτρεπόμενο μήκος κλειδιού. Πριν την δημιουργία του encryption key, οι συσκευές διαπραγματεύονται και αποφασίζουν το μέγεθος που θα χρησιμοποιήσουν.

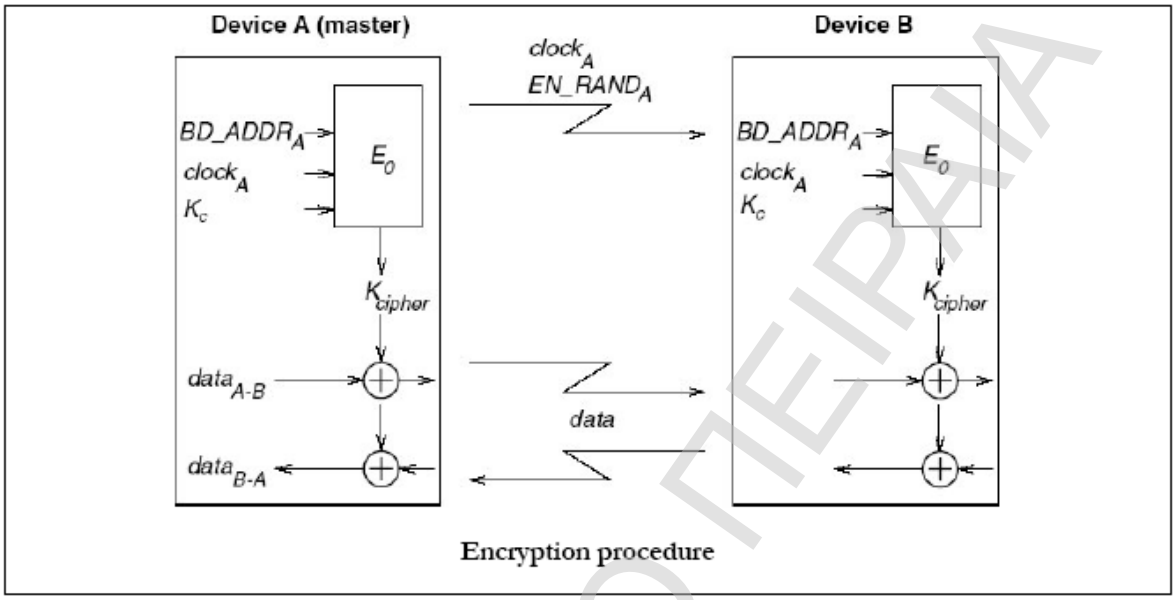
Κάθε πακέτο με φορτίο είναι κρυπτογραφημένο ξεχωριστά. Ο αλγόριθμος E_0 χρησιμοποιεί την master BD_ADDR, 26 bit από το master real-time clock και το encryption key ως είσοδο.

Ο αλγόριθμος κρυπτογράφησης E_0 δημιουργά ένα binary keystream, K_{cipher}, όπου κάνοντας XOR με τα δεδομένα γίνεται κρυπτογραφημένο. Το encryption key παράγεται από το τρέχον link key, το COF, και ένα τυχαίο αριθμό EN_RAND_A, όπως θα δούμε πιο κάτω.

$$E_0 (BD\_ADDR, CLK_{26-1}, K_C)$$

Το real-time clock προσαυξάνεται για κάθε σχισμή. Ο αλγόριθμος E_0 ξαναρχικοποιείται στην αρχή κάθε νέου πακέτου. Χρησιμοποιώντας το CLK_{26-1}, τουλάχιστον ένα bit αλλάζει μεταξύ 2 μεταδόσεων. Έτσι, ένα νέο keystream δημιουργείται μετά από κάθε επαναρχικοποίηση. Για πακέτα που καλύπτουν περισσότερες από μια σχισμή, το Bluetooth clock χρησιμοποιείται όπως βρέθηκε στην πρώτη σχισμή για ολόκληρο το πακέτο.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



Ο αλγόριθμος κρυπτογράφησης E_0 δημιουργά ένα binary keystream όπως αναφέραμε και πιο πριν, όπου κάνοντας XOR με τα δεδομένα γίνεται κρυπτογραφημένο. Η κρυπτογραφία είναι συμμετρική, και ως εκτούτου και η αποκρυπτογράφηση πραγματοποιείται ακριβώς με τον ίσιο τρόπο χρησιμοποιώντας το ίδιο ακριβώς κλειδί όπως και για την κρυπτογράφηση.

Επιπλέον για την μείωση επεμβάσεων από παρείσακτους, η μειωμένη ακτίνα του Bluetooth καθώς και το spread spectrum frequency hopping βοηθούν στην εμπιστευτικότητα μειώνοντας έτσι την πιθανότητα να έρθουμε σε επαφή με παρείσακτους. Η χρήση του γρήγορου hopping (1600 hop ανά δευτερόλεπτο), αποτελεί ένα σημαντικό εμπόδιο για υποκλοπή. Από τότε που ο μεταδότης επιμένει σε μια συγκεκριμένη συχνότητα για 625 ms, είναι δύσκολο να ανιχνεύσει την παρουσία μιας Bluetooth συσκευής.

Οι περισσότερες Bluetooth συσκευές εφοδιάζονται με radios τα οποία έχουν ακτίνα ίση περίπου με 10 μέτρα. Πιθανοί παρείσακτοι πρέπει να είναι μέσα σε αυτήν την ακτίνα για να καταφέρουν να υποκλέψουν διάφορες πληροφορίες κατά την μετάδοσης μιας Bluetooth συσκευής.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

3.16 Βασικά προβλήματα ασφάλειας του Bluetooth

PIN
Το PIN είναι το μόνο 'μυστικό' που χρησιμοποιείται για την δημιουργία κάποιου κλειδιού το οποίο δεν μεταφέρεται με ασύρματη επικοινωνία. Για πολλές εφαρμογές, το PIN έχει σχετικά μικρό μήκος από αριθμούς. Βασικά μπορεί να αποτελείται από μόνο 4 ψηφία. Εάν το PIN είναι μικρό, ή ακόμα χειρότερα έχει την τιμή 0, τότε μετά μια καλή έρευνα θα μπορούσε να παράγει τα κλειδιά.

Character set used	Min. recommended length	Minimum PIN length
0-9 (10 characters)	19 characters (= 63 bits)	12 characters (= 40 bits)
0-9 A-Z (36 characters)	12 characters (= 62 bits)	8 characters (= 41 bits)
0-9 A-Z, a-z (62 characters)	11 characters (= 65 bits)	7 characters (= 42 bits)
(Printable) ASCII (95 characters)	10 characters (= 66 bits)	6 characters (= 39 bits)

Το μήκος του encryption key **πρέπει να είναι πιο πλύπλοκο**:
Μια πιο δυναμική διαδικασία δημιουργίας initialization key πρέπει να αναπτυχθεί. Ειδικά πρέπει να επιβάλει το μήκος του κλειδιού να μην είναι τόσο μικρό.

Ο E_0 stream cipher **αλγόριθμος είναι πολύ αδύναμος**:
Η Bluetooth SIG πρέπει να αναπτύξει μια πιο δυναμική διαδικασία κρυπτογράφησης.

Το unit key **μπορεί να πέσει σε παρείσακτους**:
Μια κακόβουλη συσκευή όπου μια φορά πήρε πληροφορία για ένα unit key μιας άλλης συσκευής μπόρει να υποκλέψει επιπλέον επικοινωνία που πραγματοποιείται χρησιμοποιώντας αυτό το εκτεθιμένο unit key.

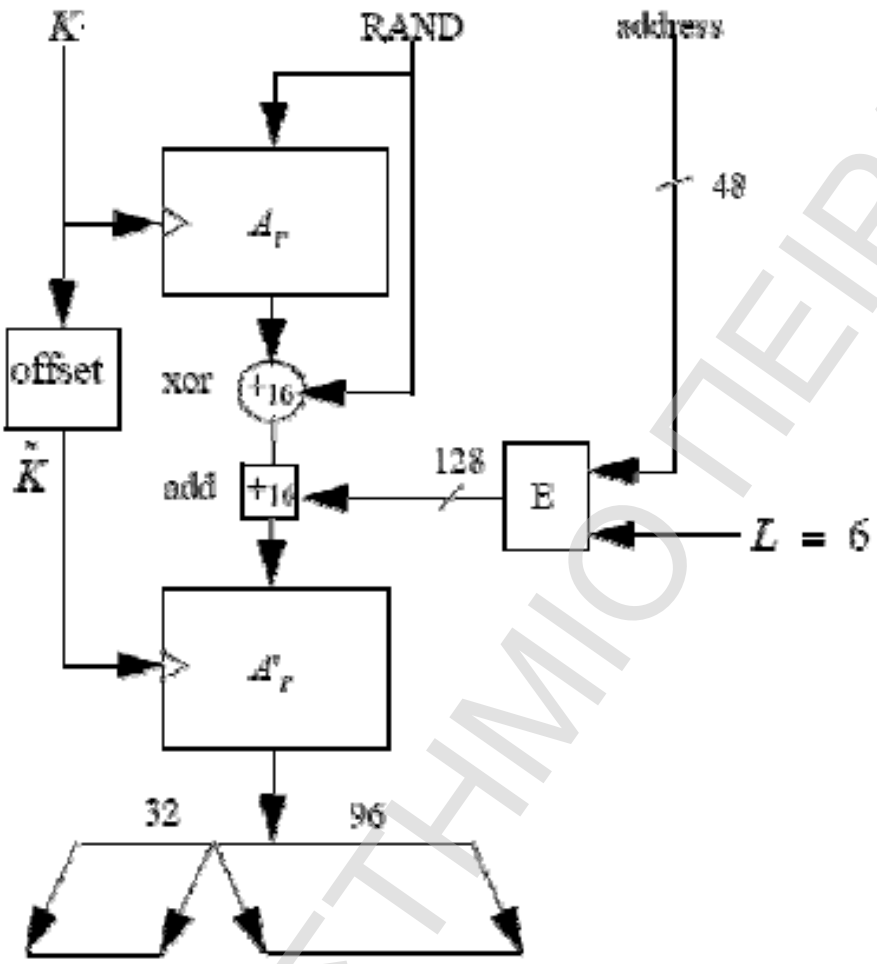
Η end-to-end **ασφάλεια δεν εκτελείτε**:
Μόνο σε χωριστές συνδέσεις γίνεται κρυπτογράφηση και αυθεντικοποίηση. Μπορούν να αναπτυχθούν εφαρμογές software με πρόσθετες υπηρεσίες ασφάλειας στο Bluetooth software.

Η διεύθυνση συσκευής δεν είναιαμα έγκυρη:
Οι διευθύνσεις δεν είναι έγκυρες και ως εκτούτου μπορεί να γίνει εξαπάτηση-προσποίηση ταυτότητας (spoofing), κάτι που μοιάζει πολύ στο IP spoofing.
Μια συσκευή κάποιου επιτιθέμενου είναι σε θέση να ενωθεί με την αυθεντική συσκευή και δημιουργήσει ένα piconet.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

THE AUTHENTICATION AND KEY-GENERATING FUNCTIONS

The Authentication Function E_i



$\tilde{K}[0] = (K[0] + 233) \mod 256$ $\quad \tilde{K}[1] = K[1] \oplus 229$

$\tilde{K}[2] = (K[2] + 223) \mod 256$ $\quad \tilde{K}[3] = K[3] \oplus 193$

$\tilde{K}[4] = (K[4] + 179) \mod 256$ $\quad \tilde{K}[5] = K[5] \oplus 167$

$\tilde{K}[6] = (K[6] + 149) \mod 256$ $\quad \tilde{K}[7] = K[7] \oplus 131$

$\tilde{K}[8] = K[8] \oplus 233$ $\quad \tilde{K}[9] = (K[9] + 229) \mod 256$

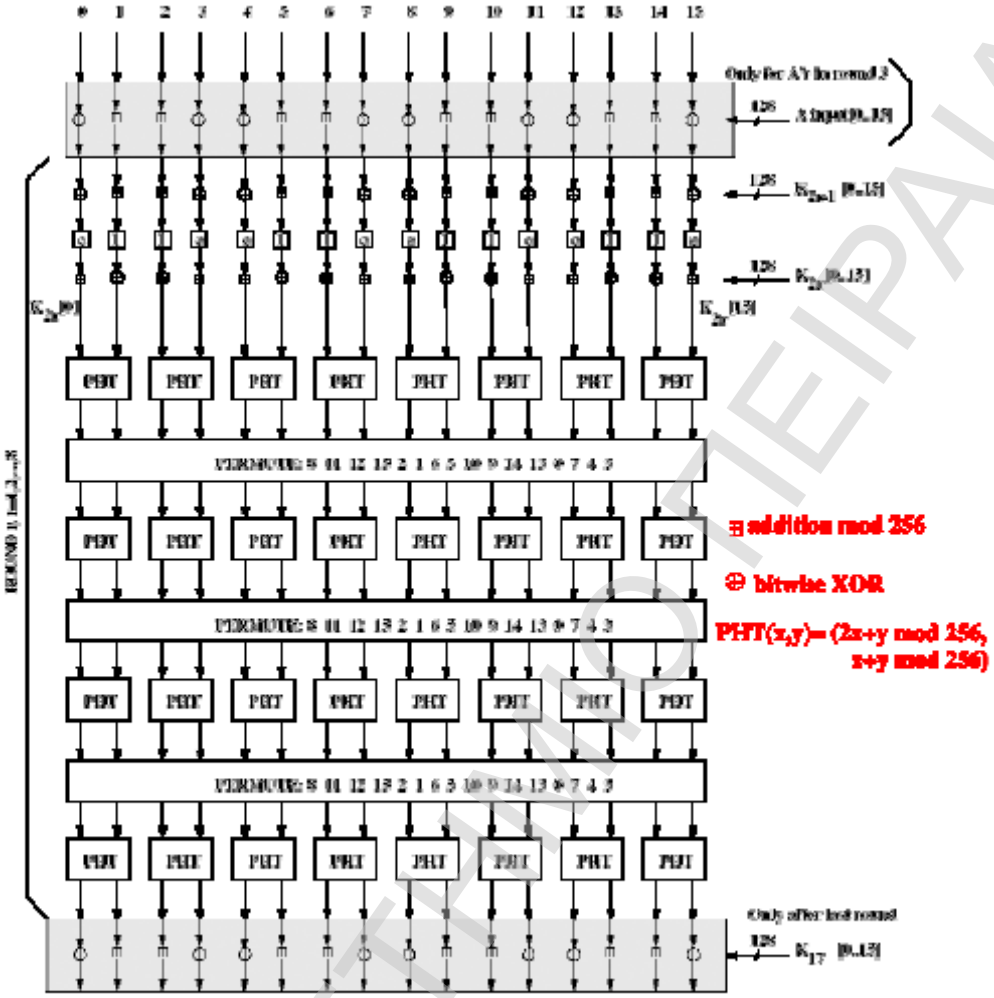
$\tilde{K}[10] = K[10] \oplus 223$ $\quad \tilde{K}[11] = (K[11] + 193) \mod 256$

$\tilde{K}[12] = K[12] \oplus 179$ $\quad \tilde{K}[13] = (K[13] + 167) \mod 256$

$\tilde{K}[14] = K[14] \oplus 149$ $\quad \tilde{K}[15] = (K[15] + 131) \mod 256$

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

A, and A', (SAFER+)

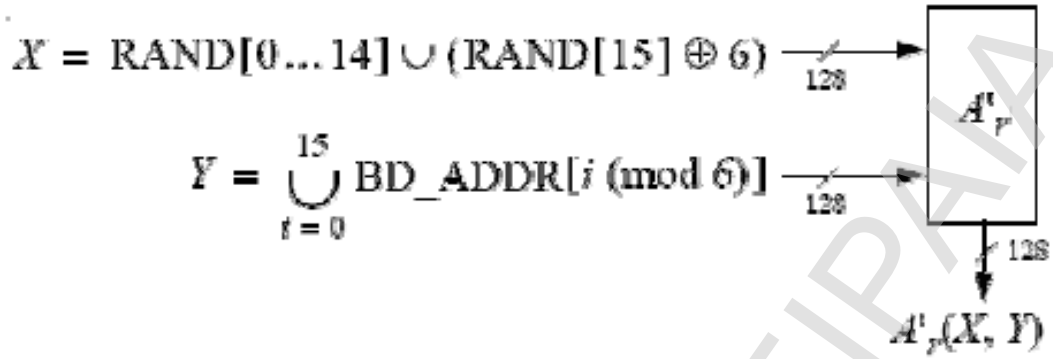


ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

E_{21} Key Generation Function for Authentication

$$X = \mathrm{RAND}[0 \ldots 14] \cup (\mathrm{RAND}[15] \oplus 6)$$

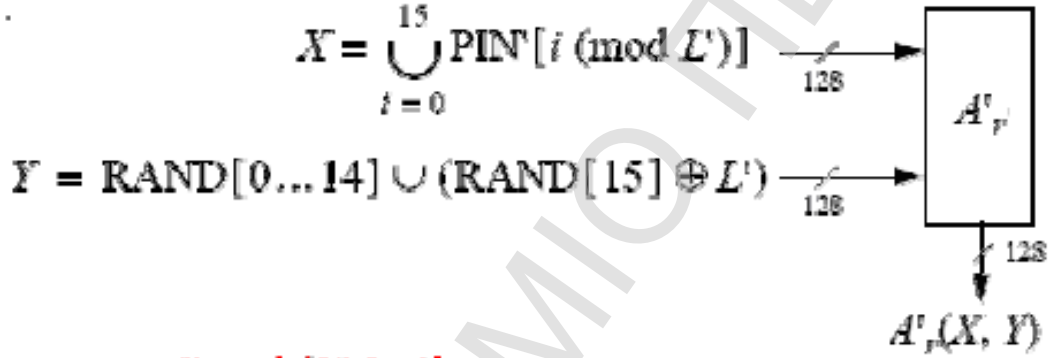
$$Y = \bigcup_{i=0}^{15} \mathrm{BD\_ADDR}[i \pmod 6]$$



E_{22} Key Generation Function for Authentication

$$X = \bigcup_{i=0}^{15} \mathrm{PIN}'[i \pmod{L'}]$$

$$Y = \mathrm{RAND}[0 \ldots 14] \cup (\mathrm{RAND}[15] \oplus L')$$

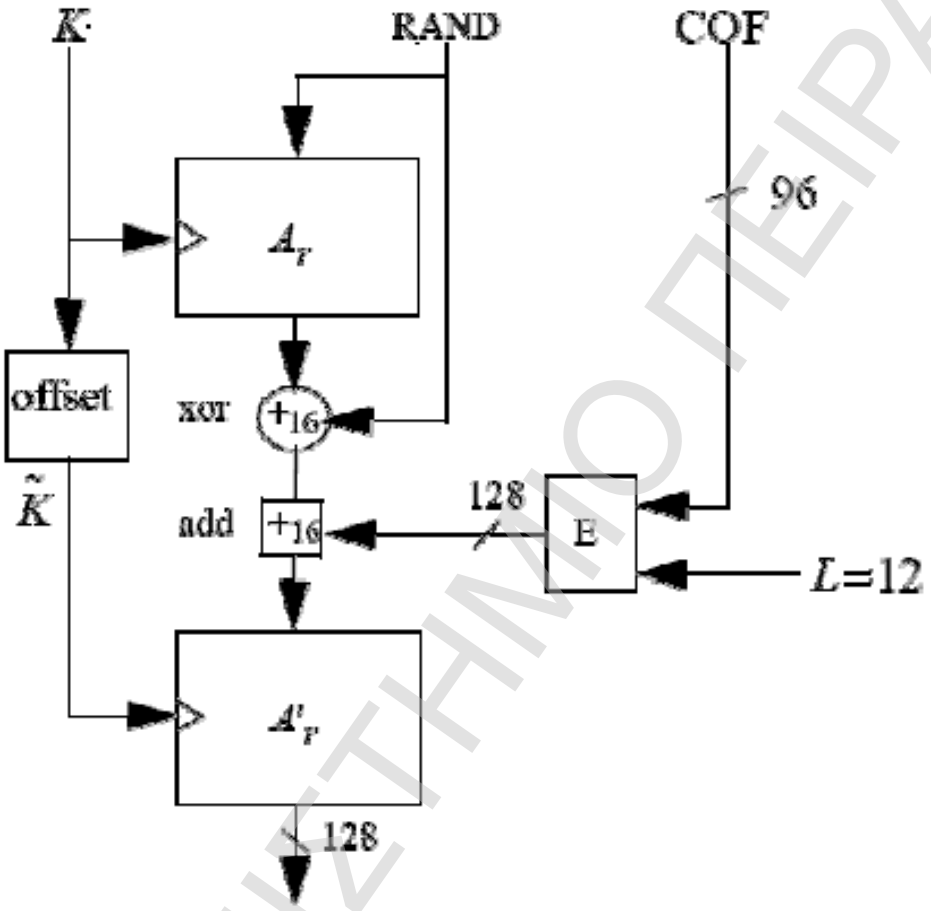


$$L' = \min\{16, L + 6\}$$

$$\mathrm{PIN}' = \begin{cases} \mathrm{PIN}[0 \ldots L-1] \cup \mathrm{BD\_ADDR}[0 \ldots \min\{5, 15-L\}], & L < 16, \\ \mathrm{PIN}[0 \ldots L-1], & L = 16, \end{cases}$$

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

E_3 Key Generation Function for Encryption



$$COF = \begin{cases} BD\_ADDR \circ BD\_ADDR, & \text{if link key is a unit key} \\ ACO, & \text{otherwise.} \end{cases}$$

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

3.17 Ευπάθειες του Bluetooth

Οι ευπάθειες (vulnerabilities) είναι συχνά αποτέλεσμα φτωχών εφαρμογών Bluetooth, όπως για παράδειγμα να επιτρέπουν στα δεδομένα να λαμβάνονται ανώνυμα. Επιπλέον, μνήμη μπορεί να είναι προσβάσιμη από μία εμπιστεύσιμη στο παρελθόν συσκευή κερδίζοντας έτσι πρόσβαση στο λειτουργικό σύστημα του Bluetooth στο επίπεδο εντολών.

Ένας μεγάλος αριθμός εργαλείων Bluetooth για χάκερ βρίσκονται διαθέσιμα δωρεάν στο διαδίκτυο.

Το BlueStrumbler είναι ένα sniffing λογισμικό το οποίο έχει την ικανότητα να ελέγχει και να καταγράφει όλες τις Bluetooth συσκευές.

Το BlueBrowse είναι ένα άλλο εργαλείο το οποίο είναι παρόμοιο με ένα ανιχνευτή πορτών και επιδικνύει όλες τις διαθέσιμες υπηρεσίες σε μια συσκευή. Δουλεύει σε κινητά τηλέφωνα τα οποία υποστηρίζουν την JSR-82, την Java Bluetooth προδιαγραφή.

Τα πιο πάνω εργαλεία επιτρέπουν την χρήση του BlueJacking, την αποστολή δηλαδή ανώνυμων μηνυμάτων σε άλλες συσκευές Bluetooth. Ένα κινητό Bluetooth δημιουργεί ένα μήνυμα ως είσοδο στις επαφές και ακολούθως καθοδηγεί το τηλέφωνο για να το στείλει μέσω του Bluetooth. Το τηλέφωνο αναζητά όποιοδήποτε άλλο Bluetooth τηλέφωνο μέσα στην ακτίνα του και τα μηνύματα αυτά εμφανίζονται πάνω στην οθόνη του άλλου κινητού. Αυτο μπορεί να γίνει και υπό μορφή αναφορών, SPAM ή άλλα ενοχλητικά μηνύματα. Επιπλέον, η χρήση αυτών των εργαλείων μπορεί να παραβιάσει το δικαίωμα ιδιοτηκότητας του χρήστη όταν όλες του οι μετακινήσεις μπορούν να καταγράφονται.

Μια ακόμα πιο σοβαρή μορφή παραβίασης ασφάλειας είναι οι BlueSnarfing επιθέσεις. Οι συσκευές είναι ιδιαίτερα τρωτές σε αυτής της μορφής επίθεσης. Εργαλεία που χρησιοποιούνται για downloading επιτρέπουν πρόσβαση σε δεδομένα όπως επαφές, ημερολόγιο, εικόνες, επαγγελματικές κάρτες και όλα αυτά μπορούν να γίνους χωρίς να προειδοποιηθεί ο ιδιοκτήτης. Επιθέσεις BlueSnarfing που συνδυάζονται με διάφορα εργαλεία όπως το BlueBag και το Gnokii επιτρέπουν πρόσβαση σε AT εντολές. Οι επιτιθέμενοι μπορούν έτσι να στέλλουν SMS μηνύματα, να έχουν πρόσβαση στο διαδίκτυο, να κάνουν διάφορα τηλεφωνήματα χωρίς να χρεώνονται οι ίδιοι και όλα αυτά χωρις πάντα την γνώση του ιδιοκτήτη.

Πρόσθετες επιθέσεις προέρχονται από την εκμετάλλευση της εμπιστοσύνης που υπάρχει μεταξύ των Bluetooth συσκευών ή κατά της διάρκεια της ανταλλαγής του key_{init}. Δεδομενου ότι αυτο πραγματοποιείται με μη κρυπτογραφημένη σύνδεση το καθιστά ευπαθή. Ένας χάκερ μπορεί να καταγράψει

οποιαδήποτε αρχική μετάδοση και ακολούθως με την βοήθεια της να δημιουργήσει ένα νέο PIN. Αυτό το σπασμένο PIN μπορεί να επιτευχθεί και μέσω ακόμα της τροποποίησης των πακέτων. Ο επιτιθέμενος δημιουργεί ένα μήνυμα το οποίο παρεμβάλλεται σε ένα συγκεκριμένο σημείο μέσα στο πρωτόκολλο αναγκάζοντας τις master και slave συσκευές να επαναλάβουν την διαδικασία της ένωσης. Έκτοτε ο επιτιθέμενος με εξειδικευμένο hardware μπορεί να εξαπατήσει την διεύθυνση Bluetooth και να σπάσει το PIN.

Δεδομένου ότι δεν υπάρχει έλεγχος ακεραιότητας στα πακέτα Bluetooth, Man-in-the-middle επιθέσεις και τροποποίησης πακέτων επιθέσεις είναι δύσκολο να αποφευχθούν. Ένα τέτοιο παράδειγμα είναι η Relay επίθεση, όπου ένας χάκερ τοποθετείτε σε δύο piconets και διαλέγει δύο θύματα (ένα σε κάθε piconet). Ακολούθως ο επιτιθέμενος υποδύεται τα θύματα στέλλοντας authentication sms στα piconets.

Προς το τέλος του 2003, ο Adam Laurie ανακοίνωσε αρκετές ευπάθειες και η σημαντικότερη όπως προαναφέραμε είναι το BlueSnarfing, όπου τα δεδομένα μπορούν να διαβαστούν από κάποιον άλλο χωρίς την έγκριση του χρήστη. Ο Laurie εξέτασε αρκετά κινητά τηλέφωνα κυρίως από την Nokia και την Ericson. Στα περισσότερα μοντέλα μπορούσε να ανκτήσει σημαντικά δεδομένα όπως τον κατάλογο με τις επαφές. Είδικα στις Nokia συσκευές μπορούσε να γίνει ακόμα επίθεση έστω και αν η υπηρεσία Bluetooth δεν ήταν φανερή για κάποιον άγνωστο. Κανονικά πρόσβαση σε αυτού του τύπου προσωπικά δεδομένα απαιτούσε μια απομακρυσμένη συσκευή να εκτελεί κάποια μέθοδο αυθεντικοποίησης. Στην περίπτωση των πιο πάνω τηλεφώνων ένας επιτιθέμενος μπορεί να μπορεί να ενωθεί με το τηλέφωνο και να ανακτήσει δεδομένα χωρίς αυθεντικοποίηση. Λαμβάνοντας υπόψη την σημαντικότητα μερικών πληροφοριών σε ένα κατάλογο ή ημερολόγιο κάποιου χρήστη, αυτή η περίπτωση αποτελεί ένα πολύ σημαντικό πρόβλημα για την ασφάλεια των δεδομένων μας.

Η Nokia μετά από όλα αυτα συμβουλεύει τους πελάτες της ότι ο καλύτερος τρόπος ώστε να μην πέσουν θύματα αυτού του είδους επίθεσης είναι να μην έχουν τις συσκευές τους ορατές για τον έξω κόσμο. Με αυτό τον τρόπο οι συσκευές δεν θα είναι ορατές εμποδίζοντας έτσι τους επιτιθέμενους να κτυπήσουν το τηλέφωνο, αποφεύγοντας έτσι τον κίνδυνο να τους κλαπούν προσωπικά δεδομένα.

Ένα άλλο συχνο φαινόμενο που παρατηρείται στην ασφάλεια του Bluetooth είναι η έννοια του Backdoor. Η ένωση (pairing) είναι ένα σημαντικό τμήμα του μοντέλου ασφαλείας του Bluetooth. Είναι σχεδιασμένο να επιτρέπει σε μια συσκευή να δημιουργήσει μια σχέση εμπιστοσύνης με μία άλλη συσκευή διευκολύνοντας με αυτόν τον τρόπο την δημιοιυργία ασφαλούς σύνδεσης μεταξύ τους. Συνήθως χρησιμοποιείται μεταξύ δύο συσκευών του ίδιου χρήστη, οι οποίες επικοινωνούν επανηλημμένα μεταξύ τους. Όταν

προσπαθήσεις να διαγράψεις μια ένωση σε μία συσκευή, το τηλέφωνο θα εξακολουθήσει να έχει τις πληροφορίες της ένωσης. Αυτό επιτρέπει σε μια προηγούμενα ενωμένη συσκευή να συνδέεται με το άλλο τηλέφωνο ακόμα και αν οι πληροφορίες ένωσης έχουν διαγραφεί. Έτσι μπορούν πολύ εύκολα να διαρρεύσουν διάφορες σημαντικές πληροφορίες και δεδομένα σε αναρμόδια άτομα.

Διάφορα πλαστά μηνύματα, ακόμα ένα πολύ γνωστο φαινόμενο στις μέρες μας, εμποδίζουν τους χρήστες από το να πάρουν διάφορες πληροφορίες και αυτό μπορεί να οδηγήσει μερικές φορές σε μεγάλα προβλήματα. Μία μορφη DoS (Denial-of-Service) επίθεσης περιλαμβάνει τις BlackList DoS επιθέσεις, όπου συσκευές αποτυχάνουν να αυθεντικοποιηθούν και έτσι μπαίνουν σε μία μαύρη λίστα. Αν ένας επιτιθέμενος αλλάζει συνεχώς τις Bluetooth διευθύνσεις, μπαίνουν σε μάυρη λίστα όλες οι άλλες συσκευές με τις οποίες θα ήθελε η συσκευή να επικοινωνήσει. Μία άλλη μορφή DoS επίθεσης είναι όταν γεμίζει η λίστα της μαύρης λίστας (η οποία κρατάει μόνο ένα ορισμένο αριθμό διευθύνσεων) προκαλώντας έτσι υπερχείλιση στον buffer και η συσκευή θα κλήσει.

Όταν ένας χάκερ κτυπά μια συσκευή με διάφορες εντολές χωρίς να ενημερώνεται ο χρήστης, τότε αυτό το είδος επίθεση ονομάζεται BlueBagging. Έτσι ο χάκερ μπόρει να κρυφακούσει διάφορες συνομιλίες, να στείλει και να λάβει μηνύματα, ακόμα και να συνδεθεί στο διαδίκτυο. Αυτό το είδος επίθεσης είναι περίπου το ίδιο με το BlueSnarfing.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

3.18 Αδυναμίες Bluetooth

Η αρχιτεκτονική για την ασφάλεια του Bluetooth όπως είναι λογικό θα έχει και μερικές αδυναμίες. Πιο κάτω θα μελετήσουμε τις αδυναμίες του Bluetooth που βρέθηκαν ως αποτέλεσμα με την εφαρμογή του Verdict, οι οποίες εμφανίζονται στον πιο κάτω πίνακα. Με την χρήση δηλαδή του Verdict έγιναν διάφορα πειράματα ώστε να ανακαλυφθούν οι πιο κάτω αδυναμίες. Εκτός από το Verdict (Validation, Exposure Randomness Improrer Conditions Taxonomy) το οποίο χρησιμοποιείται για να ανακαλύψουμε πιθανες αδυναμίες σε θέματα ασφαλείας στο Bluetooth, θα χρησιμοποιήσουμε και Bluetooth development kit και hardware από 3 διαφορετικούς vendors τον A, τον B και τον C. Το development kit του C έχει λιγότερα χαρακτηριστικά και δυνατότητες από τα άλλα 2. Τα Bluetooth kit υποστηρίζουν θύρα USB και σειριακή πόρτα και το software του είναι γραμμένο να αλληλεπιδρά με το HCI (Host Controller Interface) στρώμα της στοίβας πρωτοκόλλων.

Improper Validation	Improper Exposure	Improper Randomness	Improper Deallocation
Device Address Validation Invalid State (Link Control) Invalid States (Encryption Modes) Encryption Keys Link Keys	Non-Secret Link Key Master-Slave Switching	PIN and Key Generation	Deallocation Following a Master-Slave Switch Authentication After Encryption

1. Device Address Validation

Επισκόπηση: η 48-bit BD_ADDR χρειάζεται να επικυρωθεί επαρκώς. Έχει την ίδια μορφή με μία IEEE 802.3 διεύθυνση και είναι παρόμοια με μία Ethernet διεύθυνση. Η Bluetooth διεύθυνση μπορεί να δείξει αν η ανάθεση διευθύνσεων είναι σφαιρική η μεμονομένη. Δεν γίνεται 2 διευθύνσεις να είναι οι ίδιες. Εφόσων η διεύθυνση Bluetooth είναι παρόμοια με μία Ethernet διεύθυνση, έχουν περίπου τα ίδια χαρακτηριστικά και στην ασφάλεια. Από την στιγμή που δεν υπάρχει καμιά επικύρωση των διευθύνσεων, αυτές οι διευθύνσεις μπορούν να εξαπατηθούν, όπως περίπου γίνεται και με το IP spoofing.

Μεθοδολογία: δύο συσκευές από τον Vendor A τέθηκαν να έχουν την ίδια BD_ADDR. Η συσκευή A_2 έκανε μια προσπάθεια να εξαπατήσει την BD_ADDR της συσκευής A_1. Αυτό έγινε χρησιμοποιώντας μία από τις υπηρεσίες στο software development key του vendor A. Η συσκευή A_1 επιλέχθηκε ως ο ιδιοκτήτης της αυθεντικής BD_ADDR και η A_2 ως αυτή που εξαπάτησε την BD_ADDR. Μεταξύ των συσκευών δοκιμάστηκαν μερικά διαφορετικά master και slave switches.

Αποτέλεσμα: Καθορίστηκε ότι η εξαπατημένη συσκευή ήταν ικανή να δημιουργήσει ένα piconet με την αυθεντική συσκευή. Τα μηνύματα κειμένου μεταφέρθηκαν μεταξύ των δύο συσκευών. Επιπλέον τα master και slaves switches έγιναν μεταξύ των δύο ίδιων διευθύνσεων.

2. Invalid States (Link Control)

Επισκόπηση: Υπάρχουν δύο σημαντικά ‘μέρη’ που χρησιμοποιούνται στο Bluetooth Link Controller, το Standby και το Connection. Κατακρίβιαν υπάρχουν εφτά μέρη (page, page scan, inquiry, inquiry scan, master response, slave response και inquiry response). Είναι προσωρινά και χρησιμοποιούνται για να προσθέτουν νέους slaves σε ένα piconet. Για την μετακίνηση από το ένα μέρος στο άλλο, χρησιμοποιούνται είτε εντολές από το Bluetooth link manager ή διάφορα εσωτερικά μηνύματα του link controller. Ένα bit μπορεί να αντιπροσωπεύει τα δύο σημαντικά μέρη, ενώ 3 bit μπορούν να αντιπροσωπεύουν τα εφτά υπομέρη. Οι σχεδιαστές πρέπει να είναι σίγουροι ότι το άκυρο όγδοο μέρος από τον αχρησιμοποίητο συνδυασμό των 3 bit ποτέ δεν θα επιτευχθεί. Εάν αυτό επιτευχθεί από κάποια απρόβλεπτη περίσταση, πρέπει να υπάρχει ένας τρόπος ώστε να μεταβιβαστεί σε ένα έγκυρο μέρος. Χωρίς αυτήν την μετάβαση η συσκευή δεν θα λειτουργεί σωστά.

Μεθοδολογία: συσκευές και από τους 3 vendors (προμηθευτές) που είδαμε πριν, εξετάστηκαν για τον βαθμό υποστήριξης και λειτουργίας στην προδιαγραφή Bluetooth. Μία σειρά από διαφορετικές εντολές διανεμήθηκαν στις Bluetooth συσκευές μεταξύ των διαφορετικών μερών.

Αποτελέσματα: Βρέθηκαν περιστασιακές δυσλειτουργίες κατά την προσπάθεια μεταγωγής από το υπομέρος page στο page scan, σε μία πραγματική σύνδεση. Μερικές φορές δηλαδή οι Bluetooth συσκευές δεν μπορούν να ενωθούν η μία με την άλλη. Αυτό δεν μπορεί να καθοριστεί αν είναι αποτέλεσμα ενός ελαττωματικού hardware στην μετάβαση σε άλλα υπομέρη

ΔΙΔΑΚΤΟΡΙΚΟ ΠΕΙΡΑΜΑ

ή αν η συσκευή δεν είναι πλήρως συμβατή με την προδιαγραφή.

3. Invalid States (Encryption Mode)

Επισκόπηση: Αν μία slave συσκευή έχει λάβει ένα master key, τότε υπαρχουν 3 πιθανοί συνδυασμοί για κρυπτογράφηση, όπως φαίνονται στον πιο κάτω πίνακα.

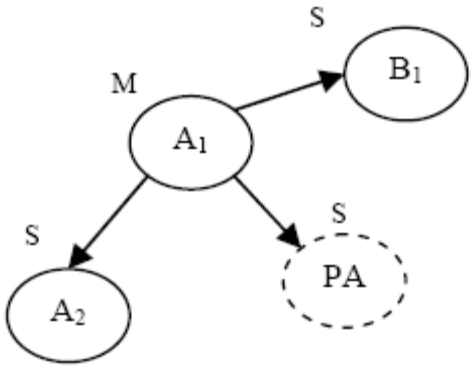
State Number	Broadcast Traffic	Unicast Traffic
1	No encryption	No encryption
2	No encryption	Encryption (master key)
3	Encryption (master key)	Encryption (master key)
4 (invalid state)	Encryption (master key)	No encryption

Σε αυτήν την περίπτωση όλες οι μονάδες στο piconet χρησιμοποιούν ένα κοινό link key, συγκεκριμένα το master key. Για να ενεργοποιηθεί η κρυπτογράφηση απαιτείται μια συγκεκριμένη link manager εντολή.

Ένα σχέδιο μπορεί να χρησιμοποιήσει 2 bit για να αντιπροσωπεύσει τα 4 μέρη (που εμφανίζονται στον πίνακα) ή συνδυασμοί κρυπτογράφησης κυκλοφορίας που επιτρέπουν 4 μέρη το πολύ. Το τέταρτο μέρος δεν πρέπει να επιτευθχεί,γιατί η broadcast κυκλοφορία θα κρυπτογραφόταν πιο μετά, αλλά η σημείο-σε-σημείο κυκλοφορία δεν θα κρυπτογραφόταν. Αυτό θα επέτρεπε σε ένα ψευδή master να αιτηθεί δεδομένα από τον slave τα οποία θα είναι κρυπτπγραφημένα.

Μεθοδολογία: Για αυτά τα πειράματα μόνο τα kits από τον vendor A και B χρησιμοποιήθηκαν γιατί οι συσκευές από τον C δεν υποστηρίζουν μετάδοση broadcast μηνύματος. Στο piconet, το A_1 ενώθηκε πρώτα με το A_2 και μετά το A_1 με το B_1. Ο αναλυτής του πρωτοκόλλου μετά έγινε slave στο A_1 για να ελέξει όλα τα πακέτα που στάληκαν και παραλήφθησαν από το A_1. Αυτή η διαμόρφωση παρουσιάζεται στην πιο κάτω εικόνα όπου τα βέλη δείχνουν την κατεύθυνση του αιτήματος σύνδεσης και το σημείο σύνδεσης με την slave συσκευή μιας σύνδεσης.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



Οι Bluetooth συσκευές εξετάστηκαν για να δούν αν υποστηρίζονται οι δύο τρόποι κρυπτογράφησης. Ακολούθως εξετάστηκαν αν υποστηρίζουν την κρυπτογράφηση broadcast μετάδοσης. Μία συσκευή πρέπει να master ώστε να μεταδίδει broadcast μηνύματα. Αν δεν λαμβάνουμε ACK όταν στέλλονται, υπάρχει μια επιλογή να στέλλονται πολλαπλά μηνύματα κάθε φορά. Αν ένας slave δεν είναι κρυπτογραφημένος, τότε τα μηνύματα δεν είναι ούτε αυτά κρυπτογραφημένα.

Αποτέλεσματα: Ανακαλύφθηκε ότι η κρυπτογράφηση broadcast μετάδοσης είναι βιώσιμη σε περιορισμένο βαθμό. Εάν η αυθεντικοποίηση και η κρυπτογράφηση (με όλους τους τρόπους) είναι εφικτή πριν οι συνδέσεις γίνουν μεταξύ τους,2 από τις 3 συσκευές σε αυτό το πεδίο δοκιμής τότε τα μηνύματα στέλλονται κρυπτογραφημένα. Αν μία άλλη συσκευή εισέλθει στο piconet, τότε ένα κρυπτογραφημένο μήνυμα θα παραληφθεί μόνο από την πρόσφατη σύνδεση στην master συσκευή.

Το invalid state δεν επιτεύχθηκε ποτέ γιατί τα Kits χρησιμοποιούν master keys μετά την κρυπτογράφηση multicast μηνύματος μέσω της HCI εντολής του. Αντιθέτως τα unicast μηνύματα πάντα στέλλονται αποκρυπτογραφημένα.

4. Encryption Keys

Επισκόπηση: Η προδιαγραφή Bluetooth δηλώνει ότι ο master δεν μπορεί να χρησιμοποιεί διαφορετικά κλειδία κρυπτογράφησης για την μετάδοση broadcast μηνυμάτων και χωριστά διευθυνσιοδοτημένης κυκλοφορίας. Ο master πρέπει να πει στις διάφορες slave συσκευές να χρησιμοποιούν ένα κοινό Link key, και ως εκτούτου να χρησιμοποιούν και ένα κοινό encryption key. Αυτό αποκαλύπτει μία δευτερεύουσα αδυναμία στο πρωτόκολλο, επιτρέποντας σε ένα εισβολέα να αποκρυπτογραφήσει και να χρησιμοποιήσει μόνο ένα link key και επομένως ένα encryption key παρεμποδίζοντας έτσι πληροφορίες για όλες τις συσκευές σε ένα piconet.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Μεθοδολογία: Συσκευές και από τους 3 vendors υποστηρίζουν encryption keys μήκους μίας μέχρι 8 οκτάδων (δηλαδή 8-128bit). Μία συσκευή με ένα encryption key μήκους 8 bit θα προσπαθήσει να επικοινωνίσει με μία άλλη συσκευή η οποία δεν διευκρυνίζει ελάχιστο μήκος για το encryption key.

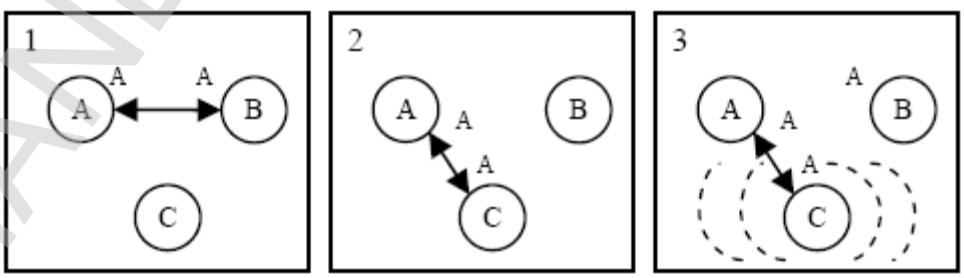
Αποτελέσματα: Αν μια συσκευή δεν έχει ελάχιστο μήκος encryption key πάνω από 8bit, τότε μετά όποια άλλη συσκευή μπορεί να αιτηθεί κρυπτογράφηση με κλειδί μήκους 8 bit. Η λύση σε αυτό το πρόβλημα είναι να τεθεί ελάχιστο μήκος encryption key ίσο με 128 bits.

Πρέπει να αναφερθεί ότι μερικές Bluetooth συσκευές είναι κατασκευασμένες με σταθερό μήκος κλειδιού, και έτσι διάφορες διαπραγματεύσεις για την κρυπτογράφηση πάντα θα αποτυχάνουν, εκτός και αν χρησιμοποιηθεί αυτό το σταθερό μήκος κλειδιού.

5. Link keys

Επισκόπηση: Στο μοντέλο του unit key υπάρχει ακόμα ένα σημαντικό πρόβλημα. Η αυθεντικοποίηση και η κρυπτογράφηση είναι βασισμένες στην υπόθεση ότι το link key αποτελεί το κοινό μυστικό όλων όσων συμμετέχουν. Όλες οι άλλες πληροφορίες που συμμετέχουν στην υπόλοιπη διαδικασία είναι δημόσιες.

Ας υποθέσουμε ότι οι συσκευές A και B χρησιμοποιούν ως link key τους το unit key του A. Την ίδια στιγμή η συσκευή C μπορεί να επικοινωνίσει με την A και να χρησιμοποιήσει πάλι ως link key το unit key του A. Αυτό σημαίνει ότι η συσκευή B, που νωρίτερα έχει λάβει το unit key του A, μπορεί να χρησιμοποιήσει το unit key μαζί με μία ψεύτικη διεύθυνση συσκευής για να υπολογίσει το encryption key και επομένως να 'ακούσει' την κυκλοφορία μεταξύ των συσκευών A και B. Μπορεί επίσης να αυθεντικοποιηθεί από μόνη της στην συσκευή A ως συσκευή C και να κάνει το ίδιο με την συσκευή C ως συσκευή A. Η διαδικασία εξαπάτησης μιας συσκευής με ένα link key φαίνεται στην πιο κάτω εικόνα.



Μεθοδολογία: Το Link key (που ανταλλάσσεται όπως φαίνεται στο σχήμα 1 της πιο πάνω εικόνας) έπρεπε να βρίσκεται στην μνήμη της συσκευής Β. Ακολούθως η συσκευή Β πρέπει να μιμηθεί την ακριβή hopping ακολουθία ώστε να λάβει οποιαδήποτε κρυπτογραφημένα μηνύματα που στέλλονται από την συσκευή Α στην συσκευή Β. Επιπλέον το link key πρέπει να χρησιμοποιηθεί για να δημιουργήσει ένα ίδιο ακριβώς encryption key, που σημαίνει ότι οι άλλοι 3 παραμέτροι για την δημιουργία του encryption key πρέπει να είναι οι ίδιοι. Μόλις δημιουργηθεί το encryption key, τα πακέτα με το φορτίο θα μπορούν να αποκρυπτογραφηθούν.

Αποτελέσματα: Αυτή η αδυναμία δεν έχει εξεταστεί πλήρως γιατί οι Bluetooth συσκευές δεν καταφέρνουν παθητικά να ακούσουν άλλες Bluetooth συσκευές. Εντούτοις, ο Jakobsson και ο Wetzel ανάφεραν ότι έχουν εφαρμόσει την αδυναμία του link key και στο Bluetooth πρωτόκολλο.

Μία λύση σε αυτή την αδυναμία είναι να χρησιμοποιηθούν master keys σε κρυπτογραφημένη επικοινωνία και να υπάρχει αλληλεπίδραση με Bluetooth συσκευή μόνο μία φορά. Έτσι όμως η λειτουργία των Bluetooth συσκευών θα περιοριζόταν αισθητά.

6. Non secret link key

Επισκόπηση: Το link key μπορεί να χρησιμοποιηθεί για να αποκρυπτογραφήσει την κυκλοφορία μεταξύ μιας συσκευής που είχε αλληλεπιδράσει προηγούμενα με μία ψευδή συσκευή και ακόμα μία Bluetooth συσκευή. Όσο η ψευδής συσκευή βρίσκεται στην ακτίνα των άλλων Bluetooth συσκευών, μπορεί πολύ εύκολα να ακούει την κυκλοφορία. Έτσι εκτίθεται κατά πολύ το Bluetooth πρωτόκολλο.

Μεθοδολογία: Η ακτίνα μίας Bluetooth συσκευής καθορίζει την μέγιστη απόσταση όπου ένας εισβολέας μπορεί να χρησιμοποιήσει ένα παλιό link key ώστε να αποκρυπτογραφήσει μηνύματα.

Αποτελέσματα: Το μήκος της ακτίνας που χρησιμοποιείται εδώ είναι 10 μέτρα. Και εδώ μόνο με την χρήση master keys επικοινωνώντας με μόνο μία συσκευή την φορά μπορούμε να ξεπεράσουμε το πρόβλημα.

7. PIN and key Generation

Επισκόπηση: το PIN χρησιμοποιείται, άμεσα και έμμεσα, στην δημιουργία των κλειδιών ασφάλειας για το Bluetooth. Μπορεί να είναι ένας σταθερός αριθμός ενσωματωμένος στην συσκευή ή μπορεί να επιλεχθεί αυθαίρετα από τον χρήστη και να ενταχθεί έπειτα και στις δύο συσκευές που θα επικοινωνίσουν. Βάζοντας ένα PIN και στις δύο μονάδες

είναι ασφαλέστερο από το να χρησιμοποιείς ένα σταθερό PIN και επομένως να χρησιμοποιείται όταν είναι δυνατόν. Αν δεν υπάρχει διαθέσιμο PIN, τότε θα χρησιμοποιηθεί η τιμή με τα μηδενικά. Για πολλές εφαρμογές το PIN είναι σχετικά μία μικρή ακολουθία αριθμών. Μπορεί μάλιστα να αποτελείται και από μόνο 4 ψηφία. Αν το PIN είναι μικρό, η χειρότερα έχει την τιμή 0 τότε με μία σχετικά μικρή προσπάθεια μπόρεις να δημιουργήσεις τα κλειδιά ασφαλείας.

Μεθοδολογία: Αν ο χρήστης έχει ένα σύντομο σε ψηφία PIN τότε θα μπορούσαν να δοκιμαστούν διάφορες τιμές PIN για τα κλειδιά ασφαλείας και έτσι θα μπορούσε να εξαπατησεί η διαδικασία της αυθεντικοποίησης ή να αποκρυπτογραφηθούν τα μηνύματα.

Αποτελέσματα: Δυστυχώς οι συσκευές που χρησιμοποιήθηκαν σε αυτά τα πειράματα έχουν σταθερό PIN και έτσι ο έλεγχος για διαφορετικά κλειδία δεν ήταν εφικτός.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

3.19 Σουίτες Bluetooth

Μια σουίτα μπορεί να χαρακτηριστεί ως μια αποθήκη εργαλείων, μια ομάδα εργαλείων δηλαδή που βρίσκονται όλα μαζι και μπορούν να χρησιμοποιηθούν το καθένα ξεχωριστά. Οι σημαντικότερες σουίτες οι οποίες υπάρχουν για το Bluetooth είναι το Bluediving, το BlueZ, το BTAudit και το Bloover II.

Πιο κάτω θα δούμε αναλυτικά μερικα χαρακτηριστικά γνωρίσματα και τα σημαντικότερα εργαλεία που χρησιμοποιά η κάθε σουίτα ξεχωριστά.

- Bluediving: Το bluediving εφαρμόζει επιθέσεις όπως bluebug, bluesnarf και bluesmack και έχει χαρακτηριστικά γνωρίσματα όπως το spoofing (υποκρισία) διευθύνσεων Bluetooth, ένα AT και ένα RFComm socket και διάφορα εργαλεία όπως το carwhisperer, το L2CAP packetgenerator, την σύνδεση L2CAP resetter και τον ανιχνευτή RFComm.

  Τα σημαντικότερα εργαλεία που χρησιμοποιεί είναι:
  - Btftp
  - Carwhisperer
  - Greenplague
  - Bccmd
  - Bdaddr
  - Hstest
  - Redfang
  - Bss

- BlueZ: Το BlueZ είναι μια στοίβα πρωτοκόλλων Bluetooth για LINUX. Υποστηρίζεται από όλα τα στρώματα και πρωτόκολλα Bluetooth και έχει εύκαμπτη, αποδοτική και έξυπνη αρχιτεκτονική. Έχει πολλά ενδιαφέροντα χαρακτηριστικά γνωρίσματα όπως την υποστήριξη σε πολλαπλές Bluetooth συσκευές, πολύπλοκη επεξεργασία δεδομένων, την αφαίρεση υλικού και την διεπαφή socket σε όλα τα στρώματα. Το BlueZ αποτελεί μέρος του επίσημου πυρήνα LINUX (Linux Kernel). Με το BlueZ οι χρήστες LINUX μπορούν να συνδεθούν και να χρησιμοποιήσουν Bluetooth συσκευές. Μπορούν εύκολα να χρησιμοποιήσουν usb-dongles, κινητα τηλέφωνα που να υποστηρίζουν Bluetooth, ακόμα και access points. Κατά συνέπεια, μπόρουν να συνδέσουν ασύρματα δύο ή περισσότερους υπολογιστές.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Τα σημαντικότερα εργαλεία τα οποία υποστηρίζει το BlueZ είναι τα πιο κάτω:

- RFComm
- L2Ping
- Hid2hci
- Hcid
- Hcitool
- Hciconfing
- Ciptool
- Dund

- BT Audit: Η Bluetooth αρχιτεκτονική ως γνωστό αποτελείτε από 2 κύρια πρωτόκολλα, το RFComm και το L2CAP,τα οποία και έχουμε προαναφέρει.Το BT Audit παρέχει εφαρμογές για την ανίχνευση του L2CAP PSMs (Protocol Service Multiplexers) και των RFComm καναλιών. Χωρίζεται σε 2 διαφορετικά εργαλεία, ένα για κάθε πρωτόκολλο, τα οποία είναι τα PSM_SCAN και RFCOMM_SCAN για PSM και RFOMM Channel scanning. Με λίγα λόγια ανιχνεύει τις πόρτες κάποιου κινητού τηλεφώνου, με σκοπό να μπόρει να τις χρησιμοποιήσει αργότερα για τις επιθέσεις με άλλα εργαλεία.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

3.20 Εργαλεία Bluetooth

- Bloover: Το Bloover είναι ένα proof-of-concept εργαλείο, παρόμοιο με το BlueSnarf, το οποίο είναι σχεδιασμένο να λειτουργεί σε τηλέφωνα με J2ME. Είναι ένα εργαλείο με το οποίο οι άνθρωποι μπόρουν να ελέγχουν αν το κινητό τους ή το κινητό φιλικών τους ατόμων έχει δεχτεί επίθεση.

  Link – Source:
  http://trifinite.org/trifinite_stuff_blooover.html

  Screenshot – Logo

- BlueAlert: Αυτό το εργαλείο είναι ένα εργαλείο ‘προειδοποίησης’ το οποίο δημιουργά ένα pop-up εικονίδιο το οποίο σε ενημερώνει πότε η Bluetooth συσκευή σου είναι ενεργή.

  Link – Source:

http://www.tdksystems.com/software/apps/content.asp?id

http://www.tdksystems.com/

- BlueBug: Αυτό το εργαλείο επιτρέπει σε αναρμόδια άτομα να κατέβάζουν λίστες τηλεφώνων, να στέλλουν και να διαβάζουν SMS μηνύματα από το επιτιθέμενο τηλέφωνο καθώς και πολλά άλλα πράγματα.

  Link – Source:

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

http://trifinite.org/trifinite_stuff_bluebug.html

Το εργαλείο και ο κώδικας δεν είναι διαθέσιμα.
Screenshot – Logo

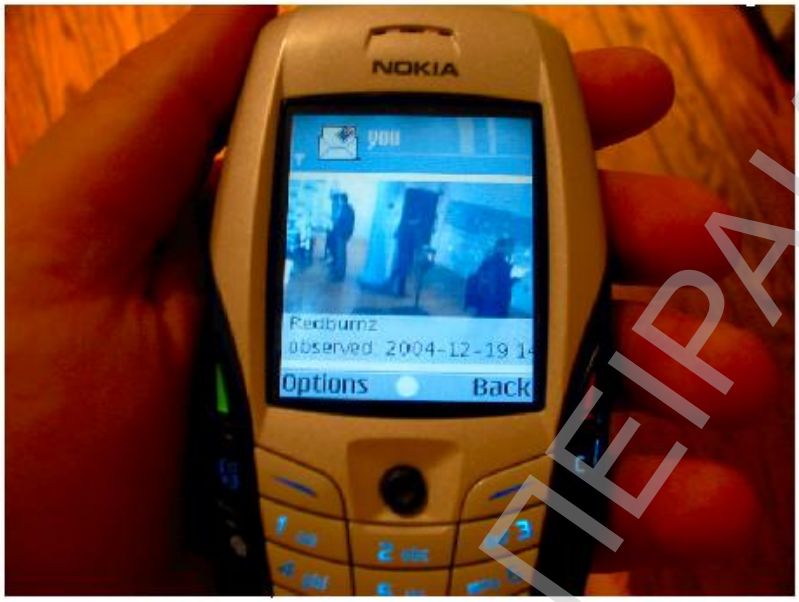
- BlueFish: Είναι ένα σύστημα το οποίο ανιχνεύει την παρουσία Bluetooth συσκευών και τους χρήστες τους. Ανιχνεύει δηλαδή συσκευές όπως τηλέφωνα, PDAs, και φορητούς υπολογιστές. Όταν βρεθεί μια νέα συσκευή, τότε το Bluetooth φωτογραφίζει την περιοχή στην οποία βρέθηκε η συσκευή και ακολούθως ψάχνει πληροφορίες για την συσκευή. Αν η συσκευή βρεθεί και σε άλλη περιοχή, τότε φωτογραφίζεται και η άλλη περιοχή. Όλες οι εικόνες φυλάγονται μαζί με το όνομα της συσκευής καθώς και την ώρα την οποία τελευταία φωτογραφήθηκε.

  Link – Source:

  http://www.nobodaddy.org/portfolio/bluefish.html

  Screenshot – Logo

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



- BluePrinting: Είναι μια μέθοδος ώστε να μπόρεις να βρεις απομακρυσμένα διάφορες λεπτομέρειες για τις συσκευές που έχουν Bluetooth. Χρησιμοποιείται για την δημιουργία στατιστικών για τον κατασκευαστή και τα μοντέλα και για να βρεις ποιες συσκευές στην ακτίνα σου είναι ασφαλείς. Κάθε Bluetooth συσκευή έχει μερικά χαρακτηριστικά όπως την BD_ADDR που είδαμε πιο πριν, προδιαγραφές κατασκευαστή ή διάφορα χαρακτηριστικά του μοντέλου.

Link – Source:

http://trifinite.org/trifinite_stuff_blueprinting.html

http://trifinite.org/Downloads/Blueprinting.pdf

http://trifinite.org/Downloads/bp_v100.zip

Screenshot – Logo

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

- BleuSmack: Είναι μια επίθεση Bluetooth η οποία αχρηστεύει άμεσα μερικές Bluetooth συσκευές. Αυτή η Denial-of-Service επίθεση χρησιμοποιεί διάφορα εργαλεία τα οποία περιέχονται στο Linux BlueZ utils πακέτο.

  Link – Source:
  http://trifinite.org/trifinite_stuff_bluesmack.html

  http://www.insecure.org/sploits/ping-o-death.html

Screenshot – Logo

- BlueSpam: Είναι μία εφαρμογή η οποία ψάχνει για όλες τις Bluetooth συσκευές που έχουν ανακαλυθφεί και τους στέλλει χωρίς την θέληση τους, αν υποστηρίζουν OBEX.

  Link – Source:
  http://www.mulliner.org/palm/bluespam.php

  Screenshot – Logo

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

- Bluetooth Location Tracker Project: Είναι ένα LINUX λογισμικό που ανακαλύπτει Bluetooth συσκευές συνδυάζοντας GPS συσκευές και αρχιτεκτονική client and server.

  Link – Source:
  http://www.betaversion.net/blt

  http://www.betaversion.net/blt/blt.pdf

  http://www.betaversion.net/blt/blt_server-0.15.tgz

  http://www.betaversion.net/blt/blt-bluez-client.tgz

  http://www.betaversion.net/blt/bltwebd-0.1.tgz

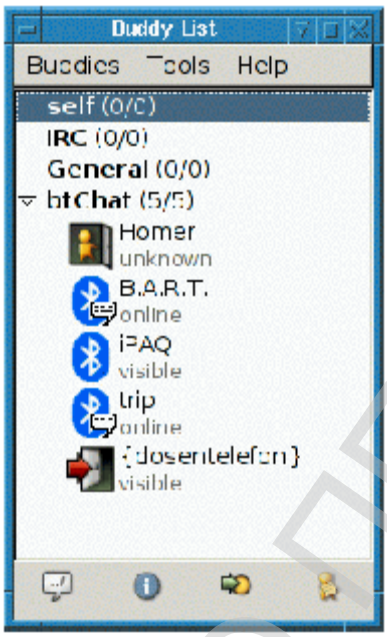
  Screenshot – Logo

- BTChat: Είναι ένα Bluetooth σύστημα βασισμένο σε chatting/IM (instand messaging)

  Link – Source:
  http://www.mulliner.org/bluetooth/btchat/

  Screenshot – Logo

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



- BTFS Bluetooth FileSystemMapping: Το BTFS παρέχει βασική υποστήριξη Bluetooth στα συστήματα αρχείων με το να χαρτογραφεί λειτουργίες όπως διάφορες έρευνες και μεταφορά αρχείων (μέσω του OBEX), για διάφορες λειτουργίες. Το BTFS είναι μία FUSE εφαρμογή (Filesystem in Userspace).

  Link – Source:
  www.mulliner.org/bluetooth/btfs.php

- BthDisc: Χρήση απλής γραμμής εντολών όπου εμφανίζονται σε λίστα όλες οι Bluetooth συσκευές που έχουν ανακαλυφθεί. Απαιτεί Microsoft Bluetooth Stack.

  Link – Source
  http://archiv.egocrew.de/tools/windows-utilities/bthdisc-00.00.01.zip

  http://www.meer-net.com/Info/WindowsXP.html

  http://securityprotocols.com/modules.php?name=News&file=article&sid=1880

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

- BtScanner: Το BtScanner είναι ένα εργαλείο ειδικό ώστε να αποσπά όσο περισσότερη πληροφορία γίνεται από μία Bluetooth συσκευή. Μία οθόνη όπου φαίνονται πάνω της πληροφορίες αποσπά HCI και SDP πληροφορία και διατηρεί μία ανοικτή σύνδεση ώστε να ελέγχει το RSSI και την ποιότητα της σύνδεσης. Είναι βασισμένο στο BlueZ Bluetooth Stack.

  Link – Source
  http://www.pentest.co.uk/cgibin/viewcat.cgi?cat=downloads&section=01_bluetooth

  Screenshot – Logo

- Fine Tooth Comb: Είναι ένα Bluetooth scanner για freeBSP. Αυτό το εργαλείο προσπαθεί να βρει Bluetooth συσκευές με 3 διαφορετικούς τρόπους:
  1. περιοδικό σκανάρισμα πληροφοριών.
  2. αναφορά συσκευών που προσπαθούν να συνδεθούν με τον σκαναρισμένο host.
  3. προσπάθεια όλων των πιθανών ID όλων των συσκευών.

  Link – Source
  http://bluetooth.shmoo.com

  http://www.oook.cz/bsd/bluetooth.html

  Screenshot – Logo

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

- FreeJack: Είναι μία εφαρμογή java βασισμένη στο BlueJacking για κινητές συσκευές. Ο σκοπός αυτού του λογισμικού είναι να επιτρέπει σε ανώνυμους να στέλλουν μηνύματα σε συσκευές με Bluetooth μέσα στην ίδια ακτίνα.

  Link – Source
  http://www.software13.co.uk/freejack/

  Screenshot – Logo

- HCIDump: Είναι ένας αναλυτής πακέτων HCI. Διαβάζει τα HCI δεδομένα που έρχονται και πάνε σε μια Bluetooth συσκευή και εμφανίζει στην οθόνη εντολές, γεγονότα και δεδομένα.

  Link – Source
  http://linuxcommand.org/man_pages/hcidump8.html

- Impronto: Το Impronto development key είναι ένα java εργαλείο που σχεδιάστηκε για να δημιουργεί εφαρμογές Bluetooth εύκολα. Το πλαίσιο του Impronto περιλαμβάνει περίπλοκα Bluetooth πρωτόκολλα πίσω από πρότυπα APIS (ISR 82) αφήνοντας τους δημιουργούς να εστιαστούν στο γράψιμο ασύρματων εφαρμογών παρά στα

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

περί δικτύωσης του Bluetooth. Έτσι το αποτέλεσμα είναι γρηγορότερο, καθώς και ευκολότερη η κατασκευή των Bluetooth εφαρμογών.

Link – Source
http://rococosoft.com

http://www.rococosoft.com/blue_university.html

http://www.rococosoft.com/blue_dk.html

Screenshot – Logo

- OpenOBEX: Είναι μια δωρεάν εφαρμογή από το Object Exchange πρωτόκολλο. Το OBEX είναι ένα πρωτόκολλο συνόδου, καλύτερα όμως μπορεί να χαρακτηριστεί ως ένα HTTP πρωτόκολλο. Μπορεί να χρησιμοποιηθεί για την ανταλλαγή όλων των τύπων αντικείμενα όπως αρχεία, εικόνες και επαγγελματικές κάρτες. Το Open Object Project σχετίζεται με την IrCp (infrared copy) εφαρμογή και μία ObexFTP εφαρμογή.

Link – Source
http://openobex.sourceforge.net/

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

http://prdownloads.sourceforge.net/openobex/openobex-1.0.1.tar.gz

http://prdownloads.sourceforge.net/openobex/openobex-apps-1.0.0.tar.gz

- ObexFTP: Είναι και αυτό μια δωρεάν εφαρμογή από το Object Exchange πρωτόκολλο όπως και το OpenOBEX. Έχει τις ίδιες λειτουργίες με πριν αλλά η κύρια χρήση του είναι να δίνει πρόσβαση στην μνήμη του κινητού τηλεφώνου για να αποθηκεύει και να επανακτύει διάφορα αντικείμενα όπως μουσική και εικόνες.

  Link – Source
  http://triq.net/obex/

  http://openobex.sourceforge.net/

  http://triq.net/obex/examples.html

- PsmScan: Αυτό το εργαλείο δημιουργήθηκε για την ασφάλεια της βάσης δεδομέων μίας Bluetooth συσκευής. Μερικοί κατασκευαστές hardware μπορούσαν να κρύψουν διάφορες ειδικές λειτουργίες στο PSM (Protocol/Service/Multiplexing) χωρίς να τις βάλουν στην STP βάση δεδομένων. Με την χρήση αυτού του εργαλείου θα μπορούσαμε να τους ανακαλύπσουμε.

  Link – Source
  http://www.betaversion.net/btdsd/

- RedSnarf: Το RedSnarf είναι μία εφαρμογή της @Shake για την BLueStumbler και την BLueSnarf εφαρμογή. Σε μερικές συσκευές είναι πιθανό να συνδεθείς με την συσκευή, χωρις να προειδοποιηθεί ο ιδιοκτήτης, κερδίζοντας έτσι πρόσβαση σε περιορισμένα μέρη όπου αποθηκέυονται δεδομένα όπως τον τηλεφωνικό κατάλογο, το ημερολόγιο και εταιρικές κάρτες. Αυτό το εργαλείο και ο κώδικας δεν είναι διαθέσιμα.

  Link – Source
  http://www.atstake.com

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

http://cansecwest.com/csw04/csw04-Whitehouse.pdf

http://www.thebunker.net/security/bluetooth.html

Screenshot – Logo

- BTCrawler: Είναι ένα scanner για κινητά Windows. Ανιχνεύει όλες τις συσκευές που βρίσκονται στην ακτίνα και εκτελεί διάφορες υπηρεσίες. Εφαρμόζεται στις επιθέσεις BLueJacking και BlueSnarfing που αναφέραμε πιο πριν.

  Link – Source
  www.silentservices.de/btcrawler.html

  Screenshot – Logo

- CIHWB: Το CIHWB (Can I Hack With Bluetooth) είναι ένα πλαίσιο για την ασφάλεια του Bluetooth για τα Windows κινητά 2005. Υποστηρίζει εργαλεία όπως το BlueSnarf, BlueJack και άλλες DoS επιθέσεις. Εργάζεται σε οποιοδήποτε PocketPC το οποίο έχει Microsoft Bluetooth Stack.

  Link – Source
  http://sourceforge.net/project/showfiles.php?group_id=173145

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

- Transient Bluetooth Environment Auditor: Η T-BEAR είναι μία πλατφόρμα για την ασφάλεια των Bluetooth συσκευών. Αποτελείτε από Bluetooth discovery, sniffing και cracking εργαλεία.

  Link – Source
  www.freshment.net.redir/tbear/67412/url_tgz/tbear.tar.gz

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Βιβλιογραφία:

https://www.bluetooth.org/apps/search/?q=security

http://www.cisco.com/web/learning/netacad/index.html

B. Dahill, B. Neil, E. Royer, C. Sheilds, A secure protocol for ad hoc networks, in: Proceedings of IEEE ICNP, 2002.

V. Gupta, S. Krishnamurthy, M. Faloutsos, Denial of Service attacks at the mac layer in wireless ad hoc networks, in: Proceedings of IEEE MILCOM, 2002.

Y. Hu, D. Johnson, A. Perrig, Sead: Secure Efficient Distance vector routing for mobile wireless ad hoc networks, in: Proceedings of IEEE WMCSA, 2002.

B. Awerbuch, D. Holmer, C. Nita-Rotaru, H. Rubens, An ondemand secure routing protocol resilient to byzantine failures, in: Proceedings of ACM Workshop on Wireless Security (WiSe), 2002.

H. Yang, X. Meng, S. Lu, Self-organized network layer security in mobile ad hoc networks, in: Proceedings of ACM Workshop on Wireless Security (WiSe), 2002.

Y. Hu, A. Perrig, D. Johnson, Packet leashes: a defense against wormhole attacks in wireless networks, Proceedings of IEEE INFOCOM, 2002.

E.M. Royer, C.K. Toh, A review of current routing protocols for ad hoc mobile wireless networks, IEEE Personal Communications 6 (1999) 46–55. April.

Bluetooth Special Interest Group, “The Bluetooth Specification, v.1.1,” February 22, 2001. At http://www.bluetooth.com/developer/specification/ specification.asp.html

J. Rice, “Collaborative Production Strategies for Technological Innovation and Leadership in Network Industries: The Case of Bluetooth,” technical report, Queensland University of Technology, Brisbane Queensland, Australia, 2000.

D.L.Lough, “A Taxonomy of Computer Attacks with Applications to Wireless Networks,” Ph.D. dissertation, Virginia Polytechnic Institute and State University, Blacksburg, Virginia, USA, April 2001.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

C. Hager and S. Midkiff, “An Analysis of Bluetooth Security Vulnerabilities,” Proc. of Wireless Communications and Networking Conference (WCNC), New Orleans, LA, 2003.

B. O’Hara and A. Petrick, The IEEE 802.11 Handbook: A Designer’s Companion. New York, NY: IEEE Press, 1999.

J. T. Vainio, “Bluetooth security,” Proc. Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory, Seminar on Internetworking: Ad Hoc Networking, Spring 2000. At http://www.niksula.cs.hut.fi/~jiitv/bluesec.html.

M. Jakobsson and S. Wetzel, “Security weaknesses in Bluetooth,” Proc. Cryptographer's Track at RSA Conf. (CT-RSA 2001), Laboratory Notes in Computer Science 2020. Berlin, Germany: Springer, 2001.

Z. J. Haas and B. Liang, “Ad Hoc Mobility Management using Quorum Systems,” IEEE/ACM Trans. Net., 1999.

S. Jacobs and M. S. Corson, “MANET Authentication Architecture,” Internet draft (draft-jacobs-imep-auth-arch-01.txt), Feb. 1999.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ