Τ.Ε.Ι. ΗΠΕΙΡΟΥ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ

ΑΣΦΑΛΕΙΑ BLUETOOTH

ΣΠΟΥΔΑΣΤΡΙΑ:
ΠΑΠΑΔΟΠΟΥΛΟΥ ΧΑΡΙΚΛΕΙΑ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:
ΣΤΕΡΓΙΟΥ ΕΛΕΥΘΕΡΙΟΣ

ΑΡΤΑ, ΦΕΒΡΟΥΑΡΙΟΣ 2005

ΑΦΙΕΡΩΣΕΙΣ

Η παρούσα εργασία αφιερώνεται στους γονείς μου Γιώργο και Κυριακή και τον αδερφό μου Γιάννη ως ελάχιστο δείγμα ευγνωμοσύνης για τα όσα μου προσφέρουν.

ABSTRACT

Το Bluetooth είναι μια νέα τεχνολογία για ασύρματη επικοινωνία. Χρησιμοποιείται σε ραδιοζεύξεις μικρής εμβέλειας αντικαθιστώντας τις καλωδιακές συνδέσεις μεταξύ κινητών και σταθερών ηλεκτρονικών συσκευών, εξασφαλίζοντας τοπικές ασύρματες συνδέσεις μεταξύ των συσκευών αυτών.

Εν ολίγοις είναι ένα πρωτόκολλο μικρής πολυπλοκότητας, χαμηλής ισχύος, χαμηλού κόστους και παρέχει διασφάλιση έναντι των παρεμβολών με χρήση κρυπτογράφησης και αυθεντικοποίησης.

Το πρωτόκολλο αναμένεται να έχει γρήγορη ανάπτυξη και ήδη υποστηρίζεται από αρκετούς κατασκευαστές.

ΚΕΦΑΛΑΙΑ

Στην παρούσα εργασία επιχειρείται η μελέτη της Ασφάλειας Bluetooth που η δομή της είναι η εξής :
Στο **κεφάλαιο 1** γίνετε μια εισαγωγή στο Bluetooth, στη συνέχεια, μια ιστορική αναδρομή στην πορεία του και τέλος μια αναφορά για ποιο λόγο χρησιμοποιούμε το Bluetooth.
Στο **κεφάλαιο 2** ρίχνουμε μια ματιά στην τεχνολογία Bluetooth, ποιες πιθανές χρήσεις έχει και πως εφαρμόζεται.
Στο **κεφάλαιο 3** παρουσιάζεται η αρχιτεκτονική Bluetooth, εξηγούμε την στοίβα του πρωτοκόλλου. Ακόμη αναφέρουμε τις υπηρεσίες ανεύρεσης του πρωτοκόλλου.
Στο **κεφάλαιο 4** εξετάζουμε γενικά την ασφάλεια Bluetooth και το σχέδιο ασφάλειας Bluetooth. Ακόμη κάνουμε μια αναλυτική περιγραφή στα κλειδιά διαχείρισης και στην διαχείριση ασφάλειας. Αναφέρουμε την κρυπτογράφηση και την αυθεντικοποίηση. Και εξετάζουμε την ασφάλεια των διανεμημένων συστημάτων Bluetooth.
Στο **κεφάλαιο 5** έχουμε μια σύντομη παρουσίαση στην ασφάλεια των δικτύων ad hoc και τι απαιτείται από τις προδιαγραφές ασφάλειας Bluetooth.
Στο **κεφάλαιο 6** κάνουμε μια επισκόπηση της ιδανικής και πραγματικής λειτουργίας Bluetooth, αυτό το τμήμα περιλαμβάνει επίσης μια συνοπτική επισκόπηση των επιθέσεων του συστήματος. Παρακάτω απαριθμούμε τις επιθέσεις στο πρότυπο Bluetooth και τέλος αναφέρουμε μερικά μέτρα.
Στο **κεφάλαιο 7** αρχίζουμε με λίγα λόγια για το πρότυπο 802.11, δηλαδή πώς λειτουργεί και ποιος ο σκοπός του. Ακόμη γίνεται σύγκριση του πρωτοκόλλου Bluetooth με την ασύρματη τεχνολογία 802.11 και με τις δύο εκδόσεις αυτού του προτύπου.
Και τέλος, στο **κεφάλαιο 8** κλείνουμε με τα συμπεράσματα και τις προβλέψεις για τη μελλοντική χρήση του Bluetooth να ολοκληρώνουν αυτή την εργασία πάνω σε αυτήν την τεχνολογία.

ΠΕΡΙΕΧΟΜΕΝΑ

Σελίδα

ΑΚΡΩΝΥΜΙΑ

ACL: Asynchronous Connectionless Links

ACO: Authenticated Ciphering Offset

AFH: Adaptive Frequency Hopping

AM_ADDR: Active Member Address

AR_ADDR: Access Request Address

BD_ADDR: Bluetooth Device Address

CA: Certification Authority

CDC: Certification Distribution Center

CID: Logical Channel Identifier

COF: Ciphering Offset Number

DOS: Denial of Service

ESN: Electronic Serial Numbers

FEC: Forward Error Connection

FHSS: Frequency-Hopping Spread Spectrum

FSM: Frequency Selection Module

GFSK: Gaussian Frequency Shift Keying

HCI: Host Controller Interface

HMI: Human-Machine Interface

IEEE: Institute of Electrical and Electronics Engineers

irOBEX: Object Exchange Protocol

ISM: Industrial Scientific and Medical

KDC: Key Distribution Center

LAN: Local Area Networks

LAP: Lower Address Part

LEL: Low Energy Lasers

LFSR: Linear Feedback Shift Registers

LM: Link Manager

LMP: Link Manager Protocol

MAC: Medium Access Control

MIN: Mobile Identification Numbers

MTU: Maximum Transmission Unit

NAP: Non-significant Address Part

OSA: Open System Authentication

PAN: Personal Area Networks

PDA: Personal Digital Assistant

PDU: Protocol Data Unit

PIN: Personal Identification Number

PKI: Public Key Infrastructure

PM_ADDR: Parked Member Address

PSM: Minimum Protocol / Service Multiplexer

QoS: Quality of Service

RF: Radio Frequency

SCO: Synchronous Connection-Orriented

SDP: Service Discovery Protocol

SIG: Special Interest Group

TCS: Telephony Control Protocol Specification

TTP: Trusted Third Party

UAP: Upper Address Part

UUID: Universally Unique Identifier

WAP: Wireless Application Protocol

WEP: Wireless Equivalent Privacy

ΔΗΛΩΣΗ ΠΕΡΙ ΜΗ ΑΝΤΙΓΡΑΦΗΣ

ΔΗΛΩΣΗ ΠΕΡΙ ΛΟΓΟΚΛΟΠΗΣ

Όλες οι προτάσεις οι οποίες παρουσιάζονται σε αυτό το κείμενο και οι οποίες ανήκουν σε άλλον αναγνωρίζονται από τα εισαγωγικά και υπάρχει η σαφής δήλωση του συγγραφέα .Τα υπόλοιπα αναγραφόμενα είναι επινόηση του γράφοντος ο οποίος φέρει και την καθολική ευθύνη για αυτό το κείμενο και δηλώνω υπεύθυνα ότι δεν υπάρχει λογοκλοπή σε αυτό το κείμενο.

Ονοματεπώνυμο : ……..

Υπογραφή : …… Ημερομηνία .....

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΙΚΑ

1.1 ΕΙΣΑΓΩΓΙΚΑ

Το Bluetooth είναι μια νέα τεχνολογία για την ασύρματη επικοινωνία. Ο στόχος του προτύπου αυτού είναι να συνδεθούν ασύρματα διαφορετικές συσκευές μαζί σε μια μικρή περιοχή όπως ένα γραφείο ή ένα σπίτι. Το πρότυπο Bluetooth περιορίζει την περιοχή, η οποία είναι προς το παρόν περίπου 10 μέτρα. Πριν την αποδοχή της τεχνολογίας πρέπει να ρίξουμε μια ματιά στη λειτουργία ασφάλειας. Ιδιαίτερα στην αρχή οι πληροφορίες που μεταδίδονταν ραδιοφωνικά (broadcasted) πέρα από το Bluetooth piconet ήτανε ευαίσθητες και απαιτούσανε καλή ασφάλεια.

Το Bluetooth χρησιμοποιεί διάφορα επίπεδα ασφάλειας, όπως κρυπτογράφηση και αυθεντικοποίηση χρηστών. Οι συσκευές Bluetooth χρησιμοποιούν έναν συνδυασμό του personal identification number (PIN) και μιας διεύθυνσης Bluetooth για να επικοινωνήσουνε με άλλες συσκευές Bluetooth. Τα στοιχεία κρυπτογράφησης χρησιμοποιούνται για να ενισχύσουν περαιτέρω το βαθμό ασφάλειας Bluetooth. [5]

Το Bluetooth χρησιμοποιεί το σχέδιο μετάδοσης που παρέχει από μόνο του ένα επίπεδο ασφάλειας. Αντί της μετάδοσης πάνω από μια συχνότητα μέσα στη ζώνη 2,4 GHz, το radio Bluetooth χρησιμοποιεί μια γρήγορη frequency-hopping spread spectrum (FHSS), που επιτρέπει μόνο στους συγχρονισμένους δέκτες να έχουν πρόσβαση στα δεδομένα. [5]

1.2 ΙΣΤΟΡΙΑ ΤΟΥ BLUETOOTH

Το Bluetooth είναι η νέα αναδυόμενη τεχνολογία για την ασύρματη επικοινωνία. Αναπτύχθηκε από μια ομάδα αποκαλούμενη Special Interest Group Bluetooth (SIG), που διαμορφώθηκε τον Μάιο του 1998. Η ομάδα αυτή σχηματίστηκε από εταιρίες κινητής τηλεφωνίας και επωνύμων εταιριών του κλάδου της πληροφορικής όπως την Ericsson, Nokia, Intel, IBM και Toshiba. Από τότε, σχεδόν όλες οι μεγαλύτερες εταιρίες στην επιχείρηση τηλεπικοινωνιών (π.χ. 3Com, Microsoft, Motorola) έχουν

διαμορφώσει το Bluetooth SIG και ο αριθμός των επιχειρήσεων που συμμετέχουνε είναι τώρα πάνω από 1.500 [5] .

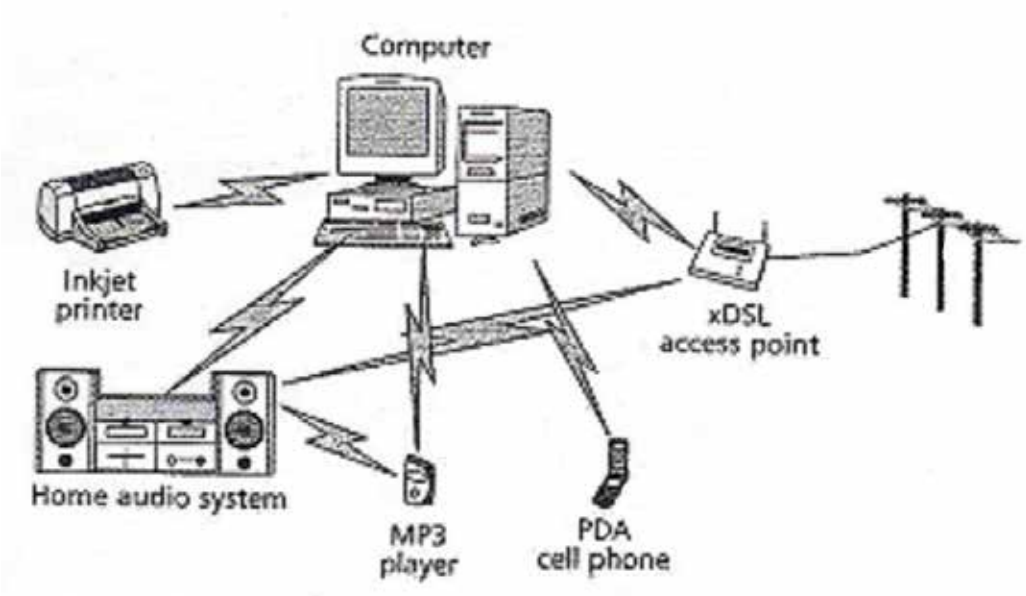
Το Bluetooth εφευρέθηκε το 1994 από το γιο L. M.Ericsson στη Σουηδία. Τα πρότυπα ονομάστηκαν Harald Blaatand "Bluetooth" II, από τον βασιλιά της Δανίας ο οποίος είπε το εξής:

«Τα σημειωματάρια και κυψελοειδή τηλέφωνα πρέπει να επικοινωνήσουν χωρίς καλώδιο».

Το Bluetooth μπορεί να χρησιμοποιηθεί για να συνδέσει σχεδόν οποιαδήποτε συσκευή με μια άλλη. Το παραδοσιακό παράδειγμα είναι να συνδεθεί ένας Personal Digital Assistant (PDA) ή ένα lap-top με ένα κινητό τηλέφωνο, χωρίς ο χρήστης να βγάλει το κινητό τηλέφωνο από την τσέπη του και χωρίς την ακαταστασία που προκαλούν τα καλώδια. Το Bluetooth μπορεί επίσης να χρησιμοποιηθεί για να διαμορφώσει τα ad hoc δίκτυα διαφορετικών συσκευών (μέχρι οκτώ), αποκαλούμενα ως Piconets. Αυτό μπορεί να είναι χρήσιμο για παράδειγμα σε μια συνεδρίαση, όπου όλοι οι συμμετέχοντες έχουν το δικό τους σύστημά για laptops που είναι συμβατό με το Bluetooth, και θέλουν να μοιραστούν αρχεία ο ένας με τον άλλον.[4]

1.3 ΓΙΑΤΙ ΧΡΗΣΙΜΟΠΟΙΟΥΜΕ BLUETOOTH;

Το Bluetooth προσπαθεί να παρέχει σημαντικά πλεονεκτήματα πέρα από άλλες τεχνολογίες μεταφοράς δεδομένων, όπως οι IrDA και HomeRF. Παρά τα σχόλια από την ομάδα Bluetooth SIG δείχνει ότι η τεχνολογία Bluetooth συμπληρωματικά με την IrDA, είναι σαφώς ανταγωνιστής για τα PC σε περιφερειακές συνδέσεις. Το IrDA είναι ήδη δημοφιλές στις περιφερειακές μονάδες των PC, αλλά περιορίζεται σοβαρά από την απαίτηση για μικρή απόσταση σύνδεσης -1 μέτρο- Line-of-sight για επικοινωνία. Αυτός ο περιορισμός αποβάλλει τη δυνατότητα της IrDA για αναγνώριση συσκευών, όπου οι συσκευές επικοινωνίας είναι κοντινές αλλά μη ορατές η μια με την άλλη.



Σχήμα 1.1

Λόγω της φύσης των ραδιοσυχνοτήτων (RF), το Bluetooth δεν υπόκειται σε τέτοιους περιορισμούς. Εκτός από τις ασύρματες συνδέσεις συσκευών μέχρι και 10 μέτρα (ή μέχρι και 100 μέτρα εάν η δύναμη του πομπού αυξάνεται), οι συσκευές δεν χρειάζονται να είναι σε οπτική επαφή (line-of-sight) και μπορούν ακόμη και να επικοινωνήσουν μέσω τοίχων ή άλλων αμέταλλων αντικειμένων. Αυτό επιτρέπει σε εφαρμογές όπως ένα κυψελοειδές (cell) τηλέφωνο σε μια τσέπη ή ένας Hi-tec χαρτοφύλακας ως modem για ένα lap-top ή ένα PDA.

Το Bluetooth σχεδιάστηκε με σκοπό να έχει χαμηλότερο κόστος ανά μονάδα. Σ' αυτή τη περίπτωση, είναι περιορισμένη η απόσταση σύνδεσης και πολύ μικρές οι ταχύτητες μετάδοσης. Το Bluetooth υποστηρίζει μόνο 780 kb/s, τα οποία μπορούν να χρησιμοποιηθούν για μεταφορά 721Kb/s μονοκατευθυντικών (unidirectional) στοιχείων (επιστροφή κατεύθυνσης 57,6 kb/s) ή μέχρι μεταφορά 432,6 kb/s μεταφορά συμμετρικών δεδομένων. Αυτά τα ποσοστά είναι συγκρίσιμα με 1-2 Mb/s που υποστηρίζεται από HomeRF, αν και το live ψηφιακό βίντεο είναι ακόμα πέρα από την ικανότητα οποιασδήποτε τεχνολογίας RF, που είναι επαρκές για τις εφαρμογές μεταφοράς και εκτύπωσης αρχείων.

Τέλος, η κύρια δύναμη Bluetooth είναι η δυνατότητά του ταυτόχρονου χειρισμού δεδομένων και μετάδοσης φωνής. Είναι σε θέση να υποστηρίζει ένα ασύγχρονο κανάλι δεδομένων και μέχρι τρία σύγχρονα κανάλια φωνής, ή ένα κανάλι που υποστηρίζει και φωνή και δεδομένα. Αυτή η ικανότητα συνδυάστηκε με ad hoc σύνδεση συσκευών και αποτελεί λύση για τις κινητές συσκευές και τις εφαρμογές του Internet. Αυτός ο συνδυασμός επιτρέπει τέτοιες καινοτόμες λύσεις όπως για παράδειγμα ένα hands free κινητού τηλεφώνου που το χρησιμοποιούμαι για μετάδοση φωνής, και είναι ικανό να τυπώσει Fax, και ο αυτόματος συγχρονισμός PDA, ή lap-top, και οι εφαρμογές τηλεφωνικού καταλόγου κυψελοειδών τηλεφώνων (σχήμα 1.1).

ΚΕΦΑΛΑΙΟ 2

ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ BLUETOOTH

2.1 ΓΕΝΙΚΑ

Οι συσκευές Bluetooth ταξινομούνται σε τρεις διαφορετικές κατηγορίες ανάλογα με την ισχύ που χρησιμοποιούν. Η πρώτη κατηγορία με 1 συσκευή έχει ισχύ η μετάδοσης μέχρι 100 mW σε απόσταση μέχρι 100 μέτρα. [6] Η δεύτερη κατηγορία με 2 συσκευές έχει ισχύ μετάδοσης 1-2,5 mW σε απόσταση 10 μέτρων. Η τρίτη κατηγορία με 3 συσκευές έχει ισχύ μετάδοσης 1mW σε απόσταση 0.1-10 μέτρα.

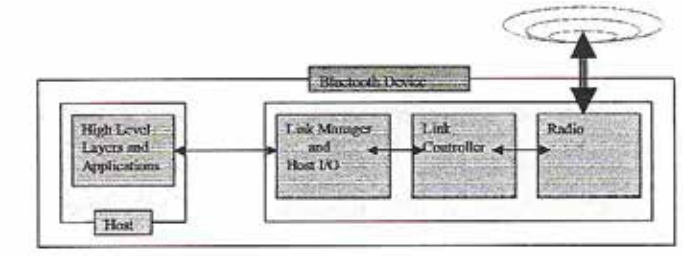
Η αρχιτεκτονική Bluetooth διαμορφώνεται από την ραδιοσυχνότητα των σταθμών βάσης και τον διαχειριστή σύνδεσης. Το Bluetooth χρησιμοποιεί την ραδιοσυχνότητα των 2,45 GHz. Το θεωρητικό μέγιστο εύρος ζώνης είναι 1 Mb/s, το οποίο μειώνεται λίγο από την πρόσθια διόρθωση σφαλμάτων (Forward Error Correction (FEC)). Η προδιαγραφή Bluetooth ορίζεται από την μεταπήδηση κατά συχνότητα (hopping frequency) που εφαρμόζεται με την Gaussian Frequency Shift Keying(GFSK).

Ο διαχειριστής σύνδεσης (link manager) είναι ένα σημαντικό τμήμα της αρχιτεκτονικής Bluetooth. Χρησιμοποιεί το πρωτόκολλο διαχείρισης σύνδεσης (LMP) για να διαμορφώσει την αυθεντικοποίηση και να χειριστεί τις συνδέσεις μεταξύ των συσκευών Bluetooth. Λειτουργεί επίσης η διαχείριση ισχύος (power management scheme), το οποίο διαιρείται σε τρία μοντέλα: **sniff**, **hold** και **park.** [7]

Όπως συζητήθηκε νωρίτερα, διάφορες συσκευές Bluetooth μπορούν να διαμορφώσουν ένα ad hoc δίκτυο. Σε αυτά τα piconets, μια από τις συσκευές Bluetooth θα ενεργήσει ως master και οι άλλες ως slave. Η master θέτει την μεταπήδηση κατά συχνότητα (frequency-hopping) που συμπεριφέρεται ως piconet. Είναι επίσης δυνατό να συνδεθούν μέχρι 10 piconets που όλα μαζί αποκαλούνται scatternets .

2.2 ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ BLUETOOTH

Το Bluetooth είναι ανοικτό πρότυπο ραδιοσυχνότητας που χρησιμοποιείται από την τεχνολογία frequency hopping spread spectrum και πολλαπλά επίπεδα ισχύος(power level).



Σχήμα 2.1

2.2.1. Επίπεδα ισχύος

Οι συσκευές Bluetooth ταξινομούνται σε τρεις διαφορετικές κατηγορίες σύμφωνα με την ισχύ που χρησιμοποιούν (πίνακας 1).

Power Classes

Power Class	MilliWatt (mW)	Range (meters)
1	~100 mW	100
2	1-2.5 mW	10
3	1 mW	0.1-10

Table 1: Power Class Specifications

Πίνακας 2.1

Ο διαχειριστής σύνδεσης λειτουργεί με δυναμική διαχείριση ισχύος, η οποία διαιρείται σε τρεις τύπους: **sniff, hold** και **park**. [11]

2.2.2. Ραδιοσυχνότητα (radio frequency)

Η ραδιοσυχνότητα (RF) είναι μέρος της συχνότητας βασικής ζώνης και ο διαχειριστής σύνδεσης χρησιμοποιεί ραδιοσυχνότητα στα 2,45 GHz. Το φάσμα RF που κατανέμεται σε Bluetooth ονομάζεται ISM, International Scientific,και Medical Band. Το ISM επιτρέπει σε διάφορους τύπους συσκευών να μεταφέρει την ίδια συχνότητα και να αποφεύγει την παρεμβολή χρησιμοποιώντας την τεχνολογία μεταπήδησης συχνότητας (frequency-hopping).

Τα πρότυπα εύρους ζώνης του ISM δεν είναι ίδια σε κάθε χώρα, έτσι η καινοτομία Bluetooth επιτρέπει την προσαρμογή σε διάφορες περιοχές του

κόσμου. Το πρωτόκολλο επικοινωνίας RF του Bluetooth υποθέτει ότι οποιαδήποτε στιγμή μόνο ένας μικρός αριθμός σταθμών συμμετέχει στις επικοινωνίες. Αυτές οι ομάδες οργανώνονται σε piconets. Σε ένα piconet, ο master μπορεί να επικοινωνήσει με επτά ενεργούς slave και μέχρι 255 ανενεργούς (parked) slaves. Αν περισσότεροι από οκτώ σταθμοί απαιτήσουν επικοινωνία, τα piconets προκύπτουν ως scatternets. Δηλαδή πολλά piconets δημιουργούν πιο σύνθετο και διαπλεκόμενο δίκτυο το οποίο ονομάζεται scatternets. Αυτό μπορεί να είναι χρήσιμο για παράδειγμα σε μια συνεδρίαση (meeting), όπου όλοι οι συμμετέχοντες έχουν το δικό τους lap-top Bluetooth, και θέλουν να μοιραστούν αρχεία ο ένας με τον άλλον [14]. Αυτή η εξέλιξη επιτρέπει το πρωτόκολλο επικοινωνίας Bluetooth να είναι πολύ ευέλικτο. Επίσης η δομή του scatternet επεκτείνει την εμβέλεια της διασύνδεσης των κόμβων εφ ‘όσον μερικοί σταθμοί μπορεί να λειτουργήσουν σαν γέφυρες μιας διασύνδεσης.

Μια απλή μονάδα μπορεί να μεταφέρει το μέγιστο μέχρι 721 Kbits/sec ή το μέγιστο μέχρι 3 κανάλια. Επίσης είναι εφικτή η ανάμιξη φωνής και δεδομένων με σκοπό την μεταφορά πολυμέσων. Κάθε κανάλι φωνής μπορεί να θεωρηθεί περίπου 64 Kbits/sec. Για την μεταφορά με ασφάλεια της φωνής, ιδιαίτερα σε πολύ θορυβώδες περιβάλλον, χρησιμοποιεί την τεχνική frequency hopping.

2.2.3. Frequency Hopping Spread Spectrum

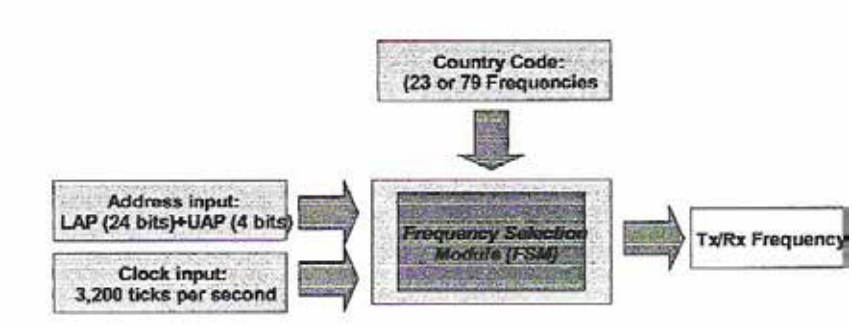
Η επικοινωνία μεταξύ των σταθμών έχει πραγματοποιηθεί μέσου του frequency hopping. Οι συγκρούσεις αποφεύγονται με τη χρησιμοποίηση ενός συνδυασμού διάφορων συχνοτήτων από μια ευρεία σειρά αναπήδησης ακολουθίας (hopping sequences) η οποία είναι χρήσιμη στο piconets . Η προδιαγραφή Bluetooth υλοποιεί την frequency hopping που εφαρμόζεται με την Gaussian Frequency Shift Keying (GFSK). Το σχέδιο Hopping είναι το ακόλουθο :

- ***χρονικός συγχρονισμός*** (time synchronization): Οι μεταδόσεις να είναι συχνότητες που γνωρίζουνε και την μετάδοση και την παραλαβή, και το χρονικό διάστημα που είναι επίσης συγχρονισμένο.
- ***Διανομή πληροφορίας*** (information delivery): Στο Bluetooth οι πληροφορίες στέλνονται σε μορφή πακέτων, με ένα πακέτο που περιλαμβάνεται μεταξύ ένα και πέντε frequency hops.
- ***Επιλογή συχνότητας*** (frequency selection): Ο διαμοιραζόμενος αλγόριθμος απαιτείται για την επιλογή συχνότητας. Στη περίπτωση του Bluetooth, ο master σταθμός διευθυνσιοδότησης μιας συσκευής και το ρολόι καθορίζει τις συχνότητες. Για εφαρμογές στις ΗΠΑ και την Ευρώπη, υπάρχουν εβδομήντα εννέα κανάλια από τα οποία επιλέγουμε. Στον υπόλοιπο κόσμο το φάσμα περιορίζεται σε είκοσι τρία κανάλια.
- ***Συχνότητα Hop***: Το ποσοστό hop είναι 1,600 συχνότητες ανά δευτερόλεπτο (το μήκος χρόνου hop είναι 625ms).

Ένα σύστημα FHSS είναι σαν το ραδιόφωνο σε ένα αυτοκίνητο όπου τα ενεργά κουμπιά πατώντας το ένα μετά το άλλο είναι προφανώς μια τυχαία ακολουθία. Ο χρόνος του κάθε καναλιού είναι πολύ σύντομος, αλλά σε ένα ποσοστό στοιχείων 1Mbps ή υψηλότερο, ακόμη και σε ένα κλάσμα δευτερολέπτου παρέχει τη σημαντική ρυθμοαπόδοση για το σύστημα επικοινωνιών [9]. Το FHSS είναι βασισμένο σε μια δεδομένη συχνότητα που είναι σταθερή για ένα μικρό χρονικό διάστημα και κινείται έπειτα προς μια νέα συχνότητα. Η ακολουθία διαφορετικών

καναλιών καθορίζεται από το σχέδιο μεταπήδησης συχνότητας. Το FHSS χρησιμοποιεί ψευδοτυχαίες ακολουθίες, οι οποίες είναι πολύ μακροχρόνιες ακολουθίες κώδικα (μερικές φορές πάνω από 65.000 hops) και κάνουν τις ακολουθίες να εμφανίζονται τυχαίες. Οι 65.000 hops είναι υψηλές όταν συγκρίνονται με άλλα κινητά δίκτυα. Το ποσοστό υψηλού hop μαζί με το πρωτόκολλο επικοινωνίας δίνει στο Bluetooth αυξανόμενες ταχύτητες μετάδοσης (1 Megabit/second). Ο πομποδέκτης (συσκευή που αποστέλλει και δέχεται σήματα, μέσου ενός διαύλου επικοινωνίας) έχει σε αυτήν την περίπτωση ένα κοινό μυστικό κωδικό, ο οποίος είναι ένας αλγόριθμος. Αυτό καθιστά το σύστημα FHSS πολύ ασφαλές ενάντια στην παρεμβολή και την παρεμπόδιση. Εάν ένας επιτιθέμενος (attacker) ήξερε τον αλγόριθμο FH, οι παράμετροί της θα ήτανε δυνατές να μπούνε στην ασύρματη επικοινωνία πρωτοκόλλου Bluetooth από τον έλεγχο ολόκληρου του φάσματος συχνότητας.

Είναι στατιστικά δύσκολες οι εμπλοκές συχνοτήτων, δεδομένου ότι οι συχνότητες που χρησιμοποιούνται από το σύστημα είναι ισχυρές. Η εμπλοκή όλων των συχνοτήτων απαιτεί πολλή ισχύ, το εύρος ζώνης δεν είναι συνήθως «λαθραίο (stealthy)». Για τα τοπικά δίκτυα (LANs) και τα μικρά ασύρματα δίκτυα (π.χ. Bluetooth) το FHSS δίνει καλύτερη ασφάλεια, προσαρμοστικότητα και χαρακτηριστικά γνωρίσματα εύρους ζώνης.



Σχήμα 2.2

Το frequency selection module (FSM) περιέχει έναν αλγόριθμο για την επιλογή της επόμενης συχνότητας μέσω του Bluetooth. Οι συσκευές που επικοινωνούν, πρέπει να διαβιβάζουν και να λαμβάνουν την ίδια συχνότητα συγχρόνως. Το FSM δέχεται τρεις εισόδους, κατόπιν παράγεται η μετάδοση και λαμβάνονται οι συχνότητες. Η είσοδος διευθύνσεων (**address input**) καθορίζει την πραγματική ακολουθία FH και αποτελείται από ένα τμήμα διεύθυνσης 24-bit (LAP) και ένα τμήμα ανώτερης διεύθυνσης 4-bit (UAP).

Τα διάφορα μέρη του BD_ADDR, που περιλαμβάνουν LAP, UAP, και ένα ασήμαντο μέρος διευθύνσεων (NAP) περιλαμβάνοντας όλες τις πλευρές του Bluetooth. Το FSM, εξαρτώμενο από τον **country code**, λειτουργεί με εμβέλεια συχνοτήτων 23 ή 79 καναλιών. Η είσοδος χρονιστή (**clock input)** καθορίζει τη φάση της ακολουθίας FH.

Το master στο piconet καθορίζει την συμπεριφορά frequency-hopping των piconets. Είναι δυνατό να συνδέσει πάνω από 10 piconets το ένα με το άλλο για να διαμορφώσει ένα "scatternet."

2.3 ΛΕΠΤΟΜΕΡΕΙΕΣ ΤΗΣ ΠΡΟΔΙΑΓΡΑΦΗΣ BLUETOOTH

Παρακάτω, παρουσιάζονται οι λεπτομέρειες των προδιαγραφών Bluetooth που σχετίζονται με τις επιθέσεις.

Καταστάσεις συσκευών. Οι συσκευές μπορούν να είναι δύο καταστάσεων, οι αποκαλούμενες ανακαλύψιμες (discoverable) και οι *μη-ανακαλύψιμες (non* discoverable) καταστάσεις λειτουργίας [10]. Επιπλέον, μια συσκευή μπορεί να είναι είτε σε κατάσταση με *σύνδεση (connectable)* είτε σε κατάσταση χωρίς σύνδεση [10]. Όταν είναι με *σύνδεση* θα αποκριθεί στα μηνύματα που λαμβάνει από τις ήδη ανακαλύψιμες συσκευές [8]

Addressing. Κάθε συσκευή συνδέεται με ένα μοναδικό τρόπο που ονομάζεται διευθυνσιοδότηση συσκευής Bluetooth και χρησιμοποιείται για να εγκαταστήσει όλη την επικοινωνία. Εάν στην κατάσταση με σύνδεση, που αναφέρεται ως κωδικός πρόσβασης συσκευής (device access code) (DAC) χρησιμοποιείται για να εξετάσει τη συσκευή. Επιπλέον, για κάθε point-to-point ή point-to-multipoint επικοινωνία χρησιμοποιείται ένα ξεχωριστό κανάλι. Το προσδιοριστικό κανάλι, καλείται κωδικός πρόσβασης καναλιών (channel access code) (CAC) καθώς επίσης και το DAC καθορίζεται ως λειτουργία της μοναδικής διεύθυνσης συσκευών Bluetooth και απλά διαβιβάζεται [8] .

Προσδιορισμός του κλειδιού αρχικοποίησης. Το ακόλουθο πρωτόκολλο εκτελείται πριν από την έναρξη του πρωτοκόλλου παραγωγής κλειδιού σύνδεσης και ανταλλάσσει ένα προσωρινό κλειδί αρχικοποίησης που θα χρησιμοποιηθεί για την κρυπτογράφηση και την αποκρυπτογράφηση των πληροφοριών στο πρωτόκολλο παραγωγής κλειδιών σύνδεσης. Το πρωτόκολλο είναι το ακόλουθο:

1. μια συσκευή επιλέγει έναν τυχαίο αριθμό και τον μεταφέρει σε άλλη συσκευή. Τότε, και οι δύο συσκευές Bluetooth υπολογίζουν το κλειδί αρχικοποίησης ως μία λειτουργία διαμεριζόμενου PIN, που είναι η διεύθυνση συσκευών Bluetooth της συσκευής που έλαβε τον τυχαίο αριθμό, και ο ίδιος ο τυχαίος αριθμός [8].
2. προκειμένου να επιβεβαιωθεί η επιτυχία της συναλλαγής (δηλ., για να επιβεβαιώσει ότι και οι δύο οι συσκευές έχουν το ίδιο κλειδί), εκτελείται μια αμοιβαία αυθεντικοποίηση . Αυτό είναι βασισμένο σε ένα σχέδιο *πρόκλησης-απάντησης* στο οποίο η πρώτη μονάδα επιλέγει ένα τυχαίο αριθμό και υπολογίζει μια λειτουργία άλλων συσκευών της διεύθυνσης Bluetooth, ο τυχαίος αριθμός και το νέο πραγματικό κλειδί [8]. Επιλέγουμε τον τυχαίο αριθμό και τον μεταφέρουμε σε άλλη συσκευή, που υπολογίζει τη λειτουργία διευθυνσιοδότησης Bluetooth. Λαμβάνουμε τον τυχαίο αριθμό και τα κλειδιά, τα οποία απαντούν στην πρώτη συσκευή με αποτέλεσμα τον υπολογισμό. Η πρώτη συσκευή ελέγχει ότι η τιμή που έλαβε είναι η ίδια τιμή που υπολόγισε. Κατόπιν, οι ρόλοι αντιστρέφονται.

Παραγωγή Ι κλειδιού σύνδεσης. Όταν μια από τις συσκευές που είναι σχετικές με το πρωτόκολλο παραγωγής κλειδιού σύνδεσης έχει έλλειψη μνήμης, ζητά να χρησιμοποιηθεί αυτό το πρώτο πρωτόκολλο παραγωγής του κλειδιού σύνδεσης [8]. Το πρωτόκολλο είναι το ακόλουθο:

1. οι συσκευές εγκαθιστούν ένα κλειδί αρχικοποίησης χρησιμοποιώντας το παραπάνω πρωτόκολλο.
2. η συσκευή Bluetooth με τις περιορισμένες ικανότητες μνήμης κρυπτογραφεί το κλειδί μονάδας χρησιμοποιώντας το κλειδί αρχικοποίησης. Το προκύπτον κρυπτογράφημα μεταφέρεται στην άλλη συσκευή.
3. η μονάδα αποκρυπτογραφεί το μήνυμα που έλαβε χρησιμοποιώντας το κλειδί αρχικοποίησης, και το προκύπτον κλειδί χρησιμοποιείται ως κλειδί σύνδεσης. Ο αποστολέας χρησιμοποιεί το μήνυμα του κλειδιού μονάδας σαν κλειδί σύνδεσης (οι δύο συσκευές συνεπώς χρησιμοποιούν το ίδιο κλειδί σύνδεσης) .Ο δέκτης λαμβάνει το απλό κείμενο (plaintext) αφού ο παραλήπτης αποκρυπτογραφήσει το κρυπτογραφημένο κείμενο (ciphertext) που είναι το κλειδί μονάδας του αποστολέα.

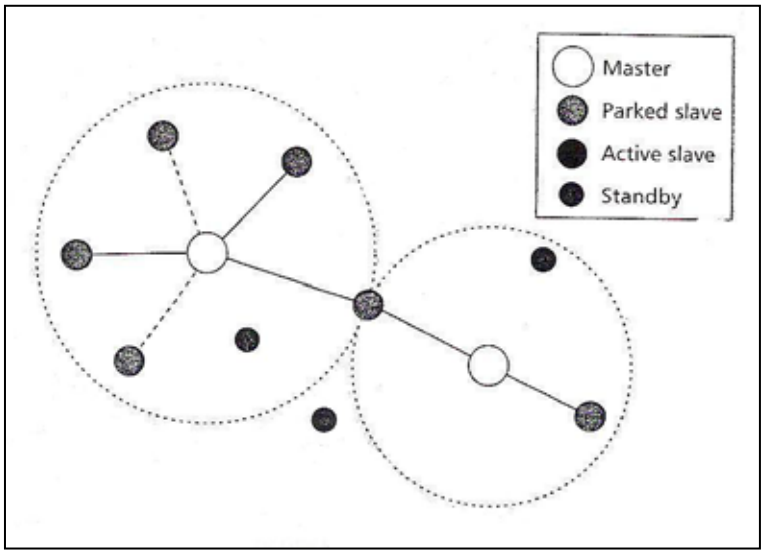
Παραγωγή ΙΙ κλειδιού σύνδεσης. Αυτό το δεύτερο πρωτόκολλο παραγωγής κλειδιού σύνδεσης οργανώνεται όταν έχουν και οι δύο συσκευές ικανοποιητικούς πόρους μνήμης [8]. Το πρωτόκολλο είναι το ακόλουθο:

1. οι συσκευές εγκαθιστούν το κλειδί αρχικοποίησης χρησιμοποιώντας προηγουμένως λεπτομερή πρωτόκολλο.
2. και οι δύο συσκευές, που καλούνται *A* και B, επιλέγουν τους τυχαίους αριθμούς, *το* $rand_A$ και το $rand_B$ αντίστοιχα. Η συσκευή *A* (B) έπειτα υπολογίζει τον αριθμό *LK-*K_A *(LK-*K_B*)* σαν μια λειτουργία $rand_A$ ($rand_B$) και της μοναδικής διεύθυνσης των συσκευών.
3. *το A* και *το B* κρυπτογραφούν τους τυχαίους αριθμούς $rand_A$ και $rand_B$ χρησιμοποιώντας το κλειδί αρχικοποίησης. Ανταλλάσσονται τα προκύπτοντα κρυπτογραφημένα κείμενα.
4. και οι δύο μονάδες αποκρυπτογραφούν τα λαμβανόμενα κρυπτογραφημένα κείμενα χρησιμοποιώντας το συμμετρικό κλειδί αρχικοποίησης. Δεδομένου ότι και οι δύο μονάδες γνωρίζουν τις άλλες μοναδικές συσκευές, αυτές μπορούνε να υπολογίσουνε τα άλλα συμβαλλόμενα μέρη LK_K_B *(LK_*K_A*).*
5. και οι δύο μονάδες υπολογίζουν το κλειδί σύνδεσης *LK-*K_AÅ *LK-*K_B*.*
6. εκτελείται μια αμοιβαία επαλήθευση για να επιβεβαιώσει την επιτυχία παραγωγής του κλειδιού σύνδεσης όπως στο βήμα 2 του κλειδιού αρχικοποίησης πρωτοκόλλου εγκατάστασης σύνδεσης.

ΚΕΦΑΛΑΙΟ 3

ΑΡΧΙΤΕΚΤΟΝΙΚΗ BLUETOOTH

Το υλικό (hardware) ελέγχου σύνδεσης Bluetooth, που ενσωματώνεται είτε ως ένα τσιπ είτε ως ράδιο μονάδα, εφαρμόζει το RF, τη βασική ζώνη, και τα τμήματα διαχείρισης σύνδεσης των προδιαγραφών Bluetooth. Αυτό το υλικό χειρίζεται την ράδιο μετάδοση και την λήψη, καθώς επίσης απαιτεί την επεξεργασία ψηφιακού σήματος για το πρωτόκολλο βασικής ζώνης. Οι λειτουργίες της περιλαμβάνουν: εγκατάσταση της σύνδεσης, υποστήριξη για ασύγχρονες (δεδομένα) και σύγχρονες συνδέσεις (φωνή), διορθώσεις λάθους, και αυθεντικοποίηση (authentication). Το υλικολογισμικό διαχείρισης σύνδεσης που παρέχεται με τη βασική ζώνη της CPU εκτελεί τον εντοπισμό της συσκευής χαμηλού επιπέδου, την αποκατάσταση (setup) σύνδεσης και την αυθεντικοποίηση. Ο διαχειριστής σύνδεσης στις χωριστές συσκευές επικοινωνεί χρησιμοποιώντας το πρωτόκολλο διαχείρισης σύνδεσης (LMP), το οποίο χρησιμοποιεί τις υπηρεσίες του βαθύτερου ελέγχου σύνδεσης (βασικής ζώνης). Το υλικό ελέγχου σύνδεσης μπορεί επίσης να παρέχει επαφή ελεγκτών οικοδεσποτών (HCI) ως τυποποιημένη (standard) επικοινωνία στο λογισμικό.

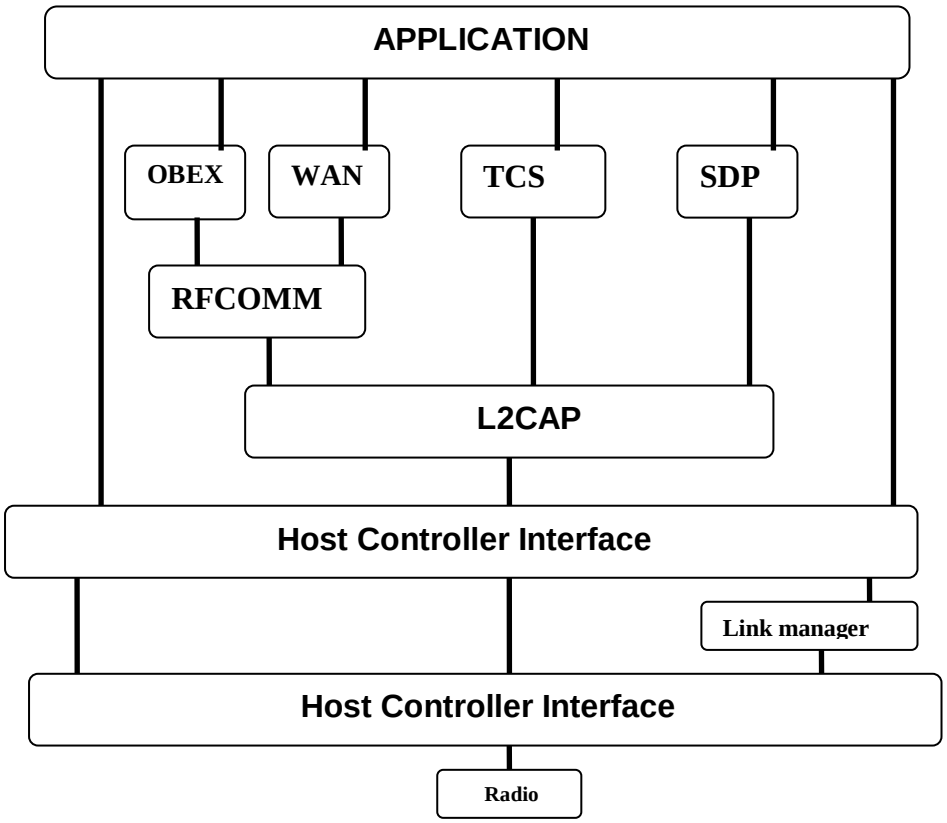


Σχήμα 3.1: Bluetooth scatter-net diagram

3.1 ΤΟΠΟΛΟΓΙΑ ΔΙΚΤΥΩΝ

Οι συσκευές Bluetooth οργανώνονται γενικά σε ομάδες από δύο έως οκτώ συσκευές και ονομάζονται ***piconets,*** *αποτελούμενες* από μια κοινή master συσκευή και μια ή περισσότερες συσκευές slave. Μια συσκευή μπορεί επιπλέον να ανήκει σε περισσότερα από ένα piconet, είτε ως slave και είτε ως master από ένα piconet και ένα Slave από άλλο. Αυτές οι συσκευές συνδέουν αποτελεσματικά τα piconets με ένα **scatternet.** Ένα διάγραμμα ενός Bluetooth scatternet παρουσιάζεται στο σχήμα 3.1.

Το Bluetooth λειτουργεί στην μη εξουσιοδοτημένη ISM ζώνη συχνότητας, που γενικά αναμιγνύεται με σήματα από άλλες συσκευές όπως: πόρτες γκαράζ, baby monitors, και φούρνοι μικροκυμάτων. Για να βοηθήσει τις συσκευές Bluetooth να συνυπάρξουν και να λειτουργήσουν αξιόπιστα δίπλα σε άλλες ISM συσκευές, κάθε Bluetooth piconet είναι συγχρονισμένο σε ένα συγκεκριμένο σχέδιο μεταπήδησης συχνότητας. Αυτό το σχέδιο, που κινείται μέσω 1600 διαφορετικών συχνοτήτων ανά δευτερόλεπτο, είναι μοναδικό σε ένα συγκεκριμένο piconet. Κάθε μεταπήδηση συχνότητας είναι μια χρονοθυρίδα κατά τη διάρκεια της οποίας μεταφέρονται τα δεδομένα πακέτων. Ένα πακέτο μπορεί στην πραγματικότητα να καλύπτει μέχρι και πέντε χρονοθυρίδες, οπότε σ'αυτή την περίπτωση η συχνότητα παραμένει συνεχής κατά τη διάρκεια αυτής της μεταφοράς.



Σχήμα 3.2: Η Στοίβα του Πρωτοκόλλου Bluetooth

3.2 ΜΗΧΑΝΗ ΚΑΤΑΣΤΑΣΗΣ ΒΑΣΙΚΗΣ ΖΩΝΗΣ (BASEBAND STATE MACHINE).

Τα Piconets μπορεί να είναι στατικά ή να διαμορφώνονται δυναμικά καθώς οι συσκευές κινούνται μέσα και έξω από την εμβέλεια μιας άλλης. Μια συσκευή που είναι σε κατάσταση αναμονής (κατάσταση χαμηλής ισχύος) με την εκκίνηση ή μιας αναζήτησης ή μιας εντολής σελιδοποίησης. Μια αναζήτηση μπορεί να χρησιμοποιηθεί εάν η διεύθυνση μιας **καταληκτικής** (target) συσκευής (είναι αυτή η συσκευή που εκτελεί ένα καταληκτικό πρόγραμμα, το οποίο έχει μεταφραστεί σ' έναν άλλο υπολογιστή) είναι άγνωστη, τότε πρέπει να ακολουθηθεί από μια εντολή σελιδοποίησης. Μια εντολή σελιδοποίησης που περιέχει έναν συγκεκριμένο κωδικό πρόσβασης συσκευής (Device Access code) χρησιμοποιείται για να συνδέσει μια απομακρυσμένη συσκευή. Μόλις αποκριθεί (respond) η απομακρυσμένη συσκευή, και οι δύο συσκευές μπαίνουν στην κατάσταση σύνδεσης, με τη συσκευή εκκίνησης να γίνεται master και την αποκρινόμενη συσκευή να ενεργεί ως slave.

Πάντα στην κατάσταση σύνδεσης, η slave συσκευή θα συγχρονίσει τον χρονιστή της master στο σωστό μοντέλο μεταπήδησης συχνότητας. Σε αυτό το σημείο, οι διαχειριστές σύνδεσης ανταλλάσσουν εντολές για να αποκατασταθεί η σύνδεση και να αποκτήσει η συσκευή τις πληροφορίες που χρειάζεται. Ο master θα αρχίσει έπειτα κανονικά την μετάδοση (transmissions) προκειμένου να κρατήσει συγχρονισμένο το piconet. Οι slave ανιχνεύει κάθε χρονοθυρίδα (time slot) που διαβιβάζει η master (slot: περιοχή της κύριας μνήμης, με μέγεθος κατάλληλο για την αποθήκευση μιας μονάδας δεδομένων) προκειμένου να συγχρονιστούν με τον master και να καθορίσουν εάν έχει διευθυνσιοδοτηθεί.

Σε κάθε ενεργό slave εκχωρείται μια διεύθυνση ενεργού μέλους (AM_ADDR) και συμμετέχει ενεργά στο piconet, ανιχνεύοντας όλες τις master χρονοθυρίδες για να καθορίσει εάν διευθυνσιοδοτείται από τον master. Επιπλέον, υπάρχουν τρεις καταστάσεις χαμηλότερης ισχύος για την συσκευή που ενεργεί ως slave**:** οι **sniff, hold**, και **park**. Ένας master μπορεί μόνο να διαβιβάσει σε συσκευές κατάστασης **sniff** κατά τη διάρκεια των χρονοθυρίδων που προσδιορίζονται από το sniff. Επομένως, αυτές οι συσκευές αφουγκράζονται μόνο κατά τη διάρκεια αυτών των ειδικών χρονοθυρίδων και είναι ανενεργές τον υπόλοιπο χρόνο. Ένας slave στην κατάσταση **hold**, στην συνέχεια, δεν λαμβάνει καθόλου ασύγχρονα πακέτα και αφουγκράζεται για το πότε θα γίνει πάλι ενεργή. Τέλος, μια συσκευή στην κατάσταση **park** όχι μόνο σταματά να αφουγκράζεται αλλά και εγκαταλείπει τη διεύθυνση ενεργού μέλους. Είναι μόνο μέλος του piconet δεδομένου ότι παραμένει συγχρονισμένο με το μοντέλο μεταπήδησης συχνότητας.

3.3 ΣΥΝΔΕΣΕΙΣ ΒΑΣΙΚΗΣ ΖΩΝΗΣ (BASEBAND LINKS)

Η βασική ζώνη Bluetooth παρέχει κανάλια μετάδοσης και για δεδομένα και για φωνή, και είναι σε θέση να υποστηρίξει μια ασύγχρονη σύνδεση δεδομένων μέχρι και τρεις σύγχρονες συνδέσεις φωνής (ή μια σύνδεση που υποστηρίζει και τις δύο).

Η σύγχρονη σύνδεση (Synchronous connection-oriented - SCO) χρησιμοποιείται συνήθως για μετάδοση φωνής. Αυτές είναι συμμετρικές συνδέσεις από σημείο σε σημείο (point-to-point) που διατηρούν τις χρονοθυρίδες (time slots: είναι ο χρόνος που χρειάζεται να αποθηκευτεί μια μονάδα δεδομένων στην κύρια μνήμη) προκειμένου να εγγυηθεί η έγκαιρη μετάδοση. Η slave συσκευή μπορεί να ανταποκριθεί κατά τη διάρκεια *της χρονοθυρίδας* αμέσως μετά από μια μετάδοση SCO από τον master. Ένας master μπορεί να υποστηρίξει μέχρι τρεις συνδέσεις SCO με έναν ή πολλαπλούς slave, αλλά ένας slave μπορεί να υποστηρίξει μόνο δύο συνδέσεις SCO με διαφορετικούς master. Τα πακέτα SCO δεν αναμεταδίδονται ποτέ.

Οι ασύγχρονες ασυνδεσμικές συνδέσεις (ACL) χρησιμοποιούνται συνήθως για μετάδοση δεδομένων. Η μετάδοση σε αυτές τις συνδέσεις εγκαθίσταται σε μια βάση ανά-υποδοχή (per-slot) (στις υποδοχές που δεν κρατούνται για τις συνδέσεις SCO). Οι συνδέσεις ACL υποστηρίζουν point-to-multipoint μεταφορές είτε ασύγχρονων είτε ισόχρονων δεδομένων. Μετά από μια μετάδοση ACL από τον master, μόνο η διευθυνσιοδοτημένη slave συσκευή μπορεί να αποκριθεί (respond) κατά τη διάρκεια της επόμενης χρονοθυρίδας, ή εάν καμία συσκευή δεν διευθυνσιοδοτείται, το πακέτο θεωρείται ένα μήνυμα εκπομπής (broadcast). Οι περισσότερες συνδέσεις ACL περιλαμβάνουν πακέτα αναμετάδοσης.

3.4 ΔΙΑΧΕΙΡΙΣΤΗΣ ΣΥΝΔΕΣΗΣ (LINK MANAGER)

Ο μηχανισμός κατάστασης βασικής ζώνης (baseband state machine) ελέγχεται κατά ένα μεγάλο μέρος από το διαχειριστή σύνδεσης. Αυτό το υλικολογισμικό (firmware), γενικά παρέχεται με το υλικό ελέγχου σύνδεσης, χειρίζεται αποκατάσταση σύνδεσης, ασφάλεια, και έλεγχο. Οι ικανότητές του περιλαμβάνουν την αυθεντικοποίηση (authentication) και υπηρεσίες ασφάλειας, ποιότητα παρακολούθησης υπηρεσιών, και την κατάσταση βασικής ζώνης. Ο διαχειριστής σύνδεσης ελέγχει τη σελιδοποίηση, τους μεταβαλλόμενους τύπους slave, και τις διαχειριζόμενες απαραίτητες αλλαγές στους ρόλους master/slave. Εποπτεύει επίσης τη σύνδεση και ελέγχει το χειρισμό των πακέτων multislot.

Οι διαχειριστές σύνδεσης επικοινωνούν ο ένας με τον άλλον χρησιμοποιώντας το *πρωτόκολλο διαχείρισης σύνδεσης (Link Management Protocol* - LMP),το οποίο χρησιμοποιεί βαθύτερες υπηρεσίες βασικής ζώνης. Τα πακέτα LMP, που στέλνουν ωφέλιμο φορτίο στο ACL, διαφοροποιούνται από τα πρωτόκολλα προσαρμογής ελέγχου σύνδεσης (L2CAP) με ένα κομμάτι επικεφαλίδας (header) ACL. Αυτά στέλνονται πάντα ως πακέτα single-slot και έχουνε πιο υψηλή προτεραιότητα από τα πακέτα L2CAP. Αυτό βοηθά στο να εξασφαλιστεί η ακεραιότητα της σύνδεσης κάτω από υψηλή απαίτηση κυκλοφορίας.

3.5 ΔΙΕΠΑΦΗ ΕΛΕΓΚΤΩΝ ΟΙΚΟΔΕΣΠΟΤΩΝ (HOST CONTROLLER INTERFACE)

Κάποιοι ελεγκτές σύνδεσης hardware μπορούν να περιλάβουν ένα στρώμα HCI επάνω από το διαχειριστή σύνδεσης. Αυτό το υλικολογισμικό (firmware) στρώμα χρησιμοποιείται για να απομονώσει την βασική ζώνη Bluetooth και τον διαχειριστή σύνδεσης από ένα πρωτόκολλο μεταφοράς όπως USB ή RS- 232. Αυτό επιτρέπει μια τυποποιημένη διεπαφή επεξεργασίας χρηστών στο hardware Bluetooth. Ένας driver HCI στον χρήστη (host) χρησιμοποιείται στη διεπαφή μια εφαρμογή Bluetooth με την μεταφορά του πρωτοκόλλου. Συγχρόνως υποστηρίζονται τρεις μηχανισμοί μεταφοράς: USB, RS- 232, και UART. Το στρώμα HCI παρουσιάζεται στο σχέδιο 3.3, χρησιμοποιώντας HCI, μια εφαρμογή Bluetooth μπορεί να έχει πρόσβαση στο hardware Bluetooth χωρίς γνώση του στρώματος μεταφοράς ή άλλων λεπτομερειών της υλοποίησης του hardware.

3.6 ΠΡΩΤΟΚΟΛΛΑ ΛΟΓΙΣΜΙΚΟΥ

Τα υπόλοιπα πρωτόκολλα Bluetooth υλοποιούνται στο λογισμικό. Το L2CAP, το χαμηλότερο στρώμα, παρέχει την διεπαφή στον διαχειριστή σύνδεσης και επιτρέπει τη διαλειτουργικότητα μεταξύ των συσκευών Bluetooth. Παρέχει πολυπλεξία πρωτοκόλλου, η οποία επιτρέπει υποστήριξη για πολλά τρίτα μέρη (third-party) ανώτερου επιπέδου πρωτόκολλα όπως το TCP/ IP και vCard/vCalendar. Επιπλέον, το L2CAP παρέχει τη διαχείριση ομάδας χαρτογραφώντας τις ανώτερες(upper) ομάδες πρωτοκόλλου σε Bluetooth piconets, την κατάτμηση και την επανασυναρμολόγηση των πακέτων μεταξύ των στρωμάτων, και την ποιότητα διαπραγμάτευσης και ελέγχου της υπηρεσίας μεταξύ των συσκευών.

Διάφορα πρωτόκολλα Bluetooth επικοινωνούνε στο στρώμα σύνδεσης L2CAP. Το SDP παρέχει συγκεκριμένες υπηρεσίες ανεύρεσης για το περιβάλλον Bluetooth χωρίς παρεμπόδιση χρήσης άλλων υπηρεσιών ανεύρεσης πρωτοκόλλων. Η RFCOMM είναι ένα απλό πρωτόκολλο μεταφοράς παρέχοντας σειριακή(serial) μεταφορά δεδομένων. Μια port emulation entity χρησιμοποιείται για να χαρτογραφήσει την επικοινωνία API στις υπηρεσίες RFCOMM, επιτρέποντας αποτελεσματικά στο λογισμικό να λειτουργήσει η συσκευή Bluetooth. Η προδιαγραφή πρωτοκόλλου ελέγχου τηλεφωνίας (Telephony Control Protocol Specification) (TCS) παρέχεται για έλεγχο κλήση φωνής και δεδομένων, παρέχοντας δυνατότητες ομάδας διαχείρισης και ασυνδεσμικές TCS, οι οποίες επιτρέπουν σηματοδότηση ανεξάρτητη από μια τρέχουσα κλήση. Και η point-to-point και point-to-multipoint σηματοδότηση υποστηρίζεται χρησιμοποιώντας τα κανάλια L2CAP, αν και η πραγματική φωνή ή τα δεδομένα μεταφέρονται απευθείας και από τη βασική ζώνη - που παρακάμπτει το L2CAP - πέρα από τις συνδέσεις SCO.

Το Bluetooth υποστηρίζει επίσης το πρωτόκολλο ανταλλαγής αντικειμένου (Object Exchange Protocol - IrOBEX), ένα πρωτόκολλο συνόδου που καθορίζεται από το IrDA. Αυτό το πρωτόκολλο μπορεί να επαναληφθεί πέρα από άλλα στρώματα μεταφοράς, συμπεριλαμβανομένου το RFCOMM και TCP,IP. Για τις συσκευές Bluetooth, υποστηρίζονται μόνο συνδέσεις OBEX. Τρία σχεδιαγράμματα εφαρμογής έχουν αναπτυχθεί χρησιμοποιώντας OBEX. Αυτά

περιλαμβάνουν τη λειτουργία συγχρονισμού για τους τηλεφωνικούς καταλόγους, ημερολόγια, μηνύματα, λειτουργίες μεταφοράς αρχείων κ.ο.κ.

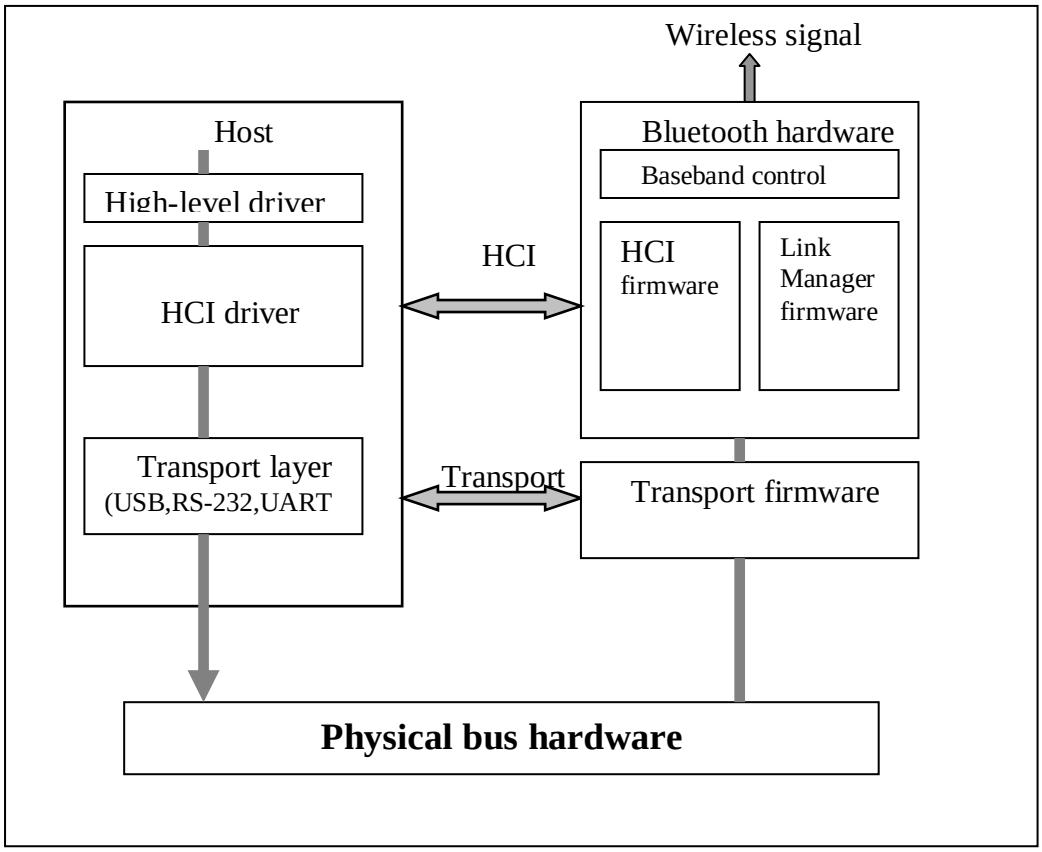
Για να καταλάβουμε τι είναι το OBEX το εξηγούμε παρακάτω :

Είναι ένα πρωτόκολλο ανταλλαγής αντικειμένου ή αυτό που καλούμε δεδομένα- ανταλλάσσεται μεταξύ δύο συσκευών που χρησιμοποιούν ένα μοντέλο πελάτη/ εξυπηρετητή υπολογιστών. Το Bluetooth έχει υιοθετήσει το πρωτόκολλο ανταλλαγής αντικειμένου (OBEX) που έχει καθοριστεί αρχικά από την υπέρυθρη ένωση στοιχείων (IrDA) για να διευκολύνει την ανταλλαγή των στοιχείων μεταξύ των διαφορετικών συσκευών.

Το πρωτόκολλο OBEX όχι μόνο επιτρέπει την ανταλλαγή στοιχείων μεταξύ δύο συσκευών, αλλά και καθορίζει ένα φάκελο-ενταγμένο σε λίστα αντικειμένου, το οποίο μπορεί να χρησιμοποιηθεί για να κοιτάξει το περιεχόμενο των φακέλων που βρίσκεται σε ένα βασισμένο International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) Q.931 πρότυπο για τον έλεγχο κλήσης τηλεφωνίας.

Περιλαμβάνει ένα εύρος εντολών σήματος από την ομάδα διαχείρισης στην εισερχόμενη κλήση, καθώς επίσης και την μεταφορά των ακουστικών δεδομένων και τη λήξη της σύνδεσης. Χρησιμοποιείται και στα ασύρματα σχεδιαγράμματα τηλεφωνίας και στην ενδοεπικοινωνία.

Τέλος, το Bluetooth μπορεί να χρησιμοποιηθεί ως ασύρματο πρωτόκολλο εφαρμογής (Wireless Application Protocol - WAP) για να εφαρμόσει υπηρεσίες Διαδικτύου στα ψηφιακά κυψελοειδή τηλέφωνα και άλλες μικρές ασύρματες συσκευές. Για παράδειγμα ένα κινητό που επιτρέπει την σύνδεση με internet (συνήθως αποκαλούμενο web phone), πίσω από το web τηλέφωνο είναι το WAP πρωτόκολλο που φυλλομετρά τον Ιστό και χειρίζεται το ηλεκτρονικό ταχυδρομείο και άλλες πληροφορίες βασισμένες στο Internet.



Σχήμα 3.3: Το Επιπεδο HCI

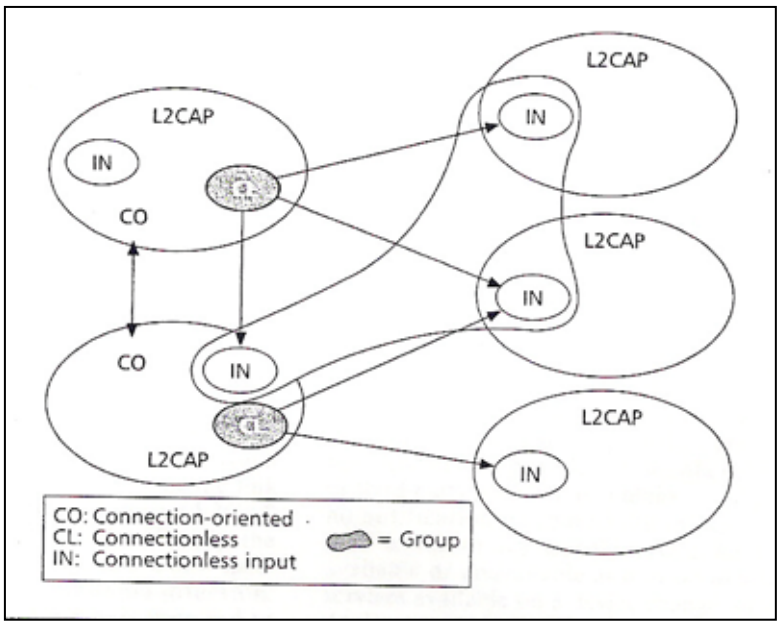
3.7 ΠΡΩΤΟΚΟΛΛΟ ΠΡΟΣΑΡΜΟΓΗΣ ΕΛΕΓΧΟΥ ΣΥΝΔΕΣΗΣ (L2CAP)

Το στρώμα σύνδεσης L2CAP λειτουργεί πέρα από μια σύνδεση ACL που παρέχεται από τη βασική ζώνη. Μια απλή σύνδεση ACL, που εγκαθίσταται από το διαχειριστή σύνδεσης χρησιμοποιώντας LMP, είναι πάντα διαθέσιμη μεταξύ του master και οποιουδήποτε ενεργού slave. Αυτό παρέχει μια σύνδεση point-to-multipoint υποστηρίζοντας και ασύγχρονη και ισόχρονη μεταφορά δεδομένων. Το L2CAP παρέχει υπηρεσίες σε ανώτερου επιπέδου πρωτόκολλα διαβιβάζοντας πακέτα δεδομένων πέρα από τα κανάλια L2CAP. Υπάρχουν τρεις τύποι καναλιών L2CAP:

i. *αμφίδρομα κανάλια σήματος,* που μεταφέρουν τις εντολές,

ii. *connection-oriented κανάλια* για αμφίδρομες point-to-point συνδέσεις και

iii. *μονόδρομα (unidirectional) χωρίς σύνδεση κανάλια* που υποστηρίζουν point-to-multipoint συνδέσεις, επιτρέποντας σε μια τοπική οντότητα L2CAP να συνδεθεί με μια ομάδα απομακρυσμένων συσκευών.



Σχήμα 3.4: Ένα Διάγραμμα καναλιών L2CAP

3.7.1 Κανάλια

Το σχήμα 3.4 παρουσιάζει οντότητες L2CAP με διάφορους τύπους καναλιών. Κάθε κανάλι L2CAP περιλαμβάνει δύο σημεία προορισμού (endpoint) που αναφέρονται από ένα λογικό προσδιοριστικό κανάλι (logical channel identifier - CID). Κάθε CID μπορεί να αντιπροσωπεύσει ένα σημείο προορισμού (endpoint) καναλιών

για ένα κανάλι χωρίς σύνδεση, ή ένα κανάλι με σήμα. Δεδομένου ότι απαιτείται ένα αμφίδρομο σήμα μεταξύ δύο οντοτήτων L2CAP προτού μια επικοινωνία να μπορέσει να πραγματοποιηθεί, κάθε οντότητα L2CAP θα έχει ένα κανάλι σήματος σημείου προορισμού (endpoint) με ένα δεσμευμένο CID 0x0001. Όλα τα κανάλια σημάτων μεταξύ της τοπικής οντότητας L2CAP και κάθε απομακρυσμένη οντότητα χρησιμοποιούν αυτό το σημείο προορισμού (endpoint).

Κάθε κανάλι connection-oriented στην οντότητα των L2CAP θα έχει ένα τοπικό CID που κατανέμεται δυναμικά. Όλες οι προσανατολισμένες προς τη σύνδεση CIDs πρέπει να συνδεθούν με ένα μονό κανάλι, και εκείνο το κανάλι πρέπει να διαμορφωθεί προτού πραγματοποιηθεί η μεταφορά δεδομένων. Το κανάλι σε εκείνο το σημείο θα δεσμευθεί σε ένα συγκεκριμένο πρωτόκολλο υψηλού επιπέδου. Επιπλέον, μια συμφωνία ποιότητας υπηρεσίας (OoS) θα εγκατασταθεί για το κανάλι μεταξύ των δύο συσκευών. Το QoS διαπραγματεύεται για κάθε κανάλι κατά τη διάρκεια της διαμόρφωσης και περιλαμβάνει δεδομένα ροής παραμέτρου όπως το μέγιστο εύρος ζώνης, καθώς επίσης και τον τύπο μετάδοσης.

Τα ασυνδεσμικά (connectionless) κανάλια είναι μονοκατευθυντικά και χρησιμοποιούνται για να διαμορφώσουν τις ομάδες. Ένα μονό εξερχόμενο ασυνδεσμικό CID σε μια τοπική συσκευή μπορεί να είναι λογικά συνδεδεμένο με πολλαπλές απομακρυσμένες συσκευές. Οι συσκευές που συνδέονται σ' αυτό το εξερχόμενο σημείο προορισμού σχηματίζουν μια λογική ομάδα. Αυτά τα εξερχόμενα CIDs κατανέμονται δυναμικά. Το εισερχόμενο ασυνδεσμικό CID, εντούτοις, καθορίζεται σε 0x0002. Αν και το πολλαπλό εξερχόμενο CIDs μπορεί να δημιουργηθεί για να σχηματίσει τις πολλαπλές λογικές ομάδες, μόνο ένα εισερχόμενο ασυνδεσμικό CID παρέχεται σε κάθε οντότητα L2CAP. Όλα τα εισερχόμενα ασυνδεσμικά δεδομένα φθάνουν μέσω αυτού του σημείου προορισμού. Αυτά τα κανάλια δεν απαιτούν σύνδεση ή διαμόρφωση. Επομένως, οποιεσδήποτε απαραίτητες πληροφορίες διαμόρφωσης, όπως υψηλού επιπέδου πρωτόκολλα, περνούν ως τμήμα του πακέτου δεδομένων.

3.7.2 Channel State Machine

Ένα σημείο προορισμού σε κανάλι connection-oriented L2CAP μπορεί να είναι σε μια από τις διάφορες πιθανές καταστάσεις με πιθανή μεταφορά στοιχείων μόνο σε OPEN κατάσταση. Αρχικά, ένα σημείο προορισμού (endpoint) είναι CLOSED, δηλώνοντας ότι κανένα κανάλι δεν συνδέεται με το CID. Αυτή είναι η μόνη κατάσταση στην οποίο μια βασική ζώνη δεν απαιτείται, και είναι σε κατάσταση endpoint που θα προκαθορίσει εάν η σύνδεση είναι αποσυνδεμένη.

3.7.3 Σύνδεση

Προκειμένου να ανοιχτεί ένα κανάλι, το σημείο προορισμού ((endpoint) είναι ο σταθμός ή ο κόμβος προορισμού ενός μηνύματος, που μεταδίδεται μέσω ενός δικτύου) του καναλιού πρέπει να συνδεθεί και να διαμορφωθεί. Μια σύνδεση συμβαίνει είτε όταν μια τοπική L2CAP οντότητα ζητάει σύνδεση σε μια απομακρυσμένη συσκευή είτε υπάρχει ένδειξη ότι μια απομακρυσμένη οντότητα

L2CAP ζητά σύνδεση σε ένα τοπικό CID. Στην πρώτη περίπτωση, η αίτηση προέρχεται από το πρωτόκολλο υψηλού επιπέδου, έχει περάσει προς την απομακρυσμένη συσκευή, και η τοπική οντότητα μπαίνει στην κατάσταση W4_L2CAP_Connect_RSP για να περιμένει μια απάντηση. Στην τελευταία περίπτωση, το ενδεικτικό σήμα αναγνωρίζεται σαν ένα αίτημα σύνδεσης. Το αίτημα έχει μεταφερθεί προς το ανώτερο στρώμα, και η τοπική οντότητα μπαίνει στην κατάσταση W4_L2CA_Connect_RSP για να περιμένει απάντηση. Σε άλλη περίπτωση, όταν παραλαμβάνεται η αναμενόμενη απάντηση, η τοπική συσκευή μπαίνει σε κατάσταση CONFIG.

3.7.4 Διαθεσιμότητα (Configuration)

Ένα κανάλι connection-oriented πρέπει να είναι διαθέσιμο προτού μπορέσουν να διαβιβαστούν τα δεδομένα. Η διαμόρφωση περιλαμβάνει μια διαπραγμάτευση μεταξύ και των δύο πλευρών της σύνδεσης έως ότου συμφωνούνται όλες οι επιλογές. Αυτό γίνεται χρησιμοποιώντας το αίτημα διαθεσιμότητας (Configuration Request) και τις εντολές απάντησης διαθεσιμότητας (Configuration Response commands). Οι υποστηριζόμενοι τύποι επιλογής διαθεσιμότητας περιλαμβάνουν μια μέγιστη μονάδα μετάδοσης **(MTU** - maximum transmission unit), ένα **flush timeout**, και μια συμφωνία **QoS**.

Η επιλογή MTU απεικονίζει το μεγαλύτερο πακέτο L2CAP που είναι ωφέλιμο φορτίο και μπορεί να χειριστεί μια τοπική συσκευή. Το flush timeout καθορίζει το χρονικό διάστημα που ο ελεγκτής σύνδεσης (link controller) θα προσπαθήσει να διαβιβάσει ένα τμήμα L2CAP πριν γίνει flushing το πακέτο. Τέλος, η συμφωνία QoS χρησιμοποιείται για να διαπραγματευτεί μια ροή προδιαγραφών για μια ενιαία κατεύθυνση μετάδοσης. Οι εφαρμογές L2CAP απαιτούνται μόνο για να υποστηρίξουν την καλύτερη υπηρεσία, αλλά καμία κυκλοφορία ή εγγυημένη υπηρεσία δεν μπορεί επίσης να διαπραγματευτεί.

Άλλες παράμετροι στην προδιαγραφή ροής περιλαμβάνουν: τον ρυθμό token, το μέγεθος token, το εύρος ζώνης, το χρόνο αναμονής και την καθυστέρηση. Η συσκευή αίτησης δείχνει όλες τις όχι εξ ορισμού (nondefault) επιλογές που θα δεχτεί, στο οποίο η αποκρυνόμενη (responding) συσκευή είτε συμφωνεί ή παρέχει εναλλακτική τοποθέτηση. Αυτή η διαδικασία συνεχίζεται έως ότου συμφωνήσουν όλες οι επιλογές. Αυτή η διαμόρφωση είναι για μονοκατευθυντική μεταφορά, εντούτοις, και η διαδικασία πρέπει έπειτα να επαναληφθεί για την αντίθετη κατεύθυνση μεταφοράς. Αφότου έχουν καθοριστεί όλες οι παράμετροι διαθεσιμότητας, και οι δύο οντότητες L2CAP μπαίνουν στην OPEN κατάσταση, στην οποία τα δεδομένα σημείου μπορούν να αρχίσουν την μεταφορά.

3.7.5 Αποσύνδεση

Για να κλείσει ένα κανάλι, μια οντότητα L2CAP πρέπει να στείλει ένα αίτημα αποσύνδεσης στην άλλη. Εάν μια οντότητα λάβει το αίτημα της αποσύνδεσης από το πρωτόκολλο υψηλού επιπέδου, περνά το αίτημα στην απομακρυσμένη συσκευή, και η τοπική οντότητα μπαίνει στην κατάσταση W4_L2CAP_ DISCONNECT_RSP για να

περιμένει απάντηση. Εάν η τοπική οντότητα λάβει μια ένδειξη ότι η απομακρυσμένη συσκευή ζητά αποσύνδεση, στέλνει ένα αίτημα αποσύνδεσης στο ανώτερο στρώμα και μπαίνει έπειτα στην κατάσταση W4_L2CA_DISCONNECT_RSP για να περιμένει απάντηση. Σε διαφορετική περίπτωση, όταν παραλαμβάνεται η αναμενόμενη απάντηση, η τοπική συσκευή εισέρχεται στην CLOSED κατάσταση.

3.7.6 Πακέτα

Τα δεδομένα μεταφέρονται στα κανάλια χρησιμοποιώντας πακέτα. Ένα κανάλι σύνδεσης χρησιμοποιεί πακέτα με header 32bit που ακολουθείται από ένα ωφέλιμο φορτίο (payload) μέχρι 65.535 bytes. Το payload είναι το τρίτο μέρος ενός πακέτου βασικής ζώνης Bluetooth στο οποίο βρίσκονται οι πληροφορίες χρηστών. Η δομή payload διαφέρει, ανάλογα με εάν το πακέτο είναι ένα FHS, ένα ACL, ή ένας τύπος SCO.

Το πακέτο FHS ακολουθείται από τα πακέτα ACL και SCO στο επόμενο τμήμα. Η επικεφαλίδα (header) περιλαμβάνει ένα μήκος 16bit ωφέλιμου φορτίου που χρησιμοποιεί για τον έλεγχο και το 16bit προορισμού CID. Το ωφέλιμο φορτίο περιέχει πληροφορίες που παραλαμβάνονται από ή που στέλνεται στο πρωτόκολλο υψηλού επιπέδου. Τα ασυνδεσμικά πακέτα καναλιών περιλαμβάνουν επίσης μια επικεφαλίδα αλλά πάντα χρησιμοποιούν 0x0002 για απομακρυσμένο CID. Επιπλέον, η επικεφαλίδα ακολουθείται από ένα 16bit (ελάχιστο) πολυπλέκτης υπηρεσίας/ πρωτοκόλλου (protocol/service multiplexer - PSM), ο οποίος χρησιμοποιείται για να δείξει από ποιο πρωτόκολλο υψηλού επιπέδου προέρχεται. Αυτό επιτρέπει την επανασυναρμολόγηση των πακέτων στην απομακρυσμένη συσκευή. Το πεδίο PSM δεν απαιτείται για τα connection-oriented κανάλια δεδομένου ότι είναι συνδεδεμένα σε ένα συγκεκριμένο πρωτόκολλο κατά τη διάρκεια της σύνδεσης.

3.8. SERVICE DISCOVERY PROTOCOL (ΥΠΗΡΕΣΙΑ ΑΝΕΥΡΕΣΗΣ ΠΡΩΤΟΚΟΛΛΟΥ)

Η υπηρεσία ανεύρεσης πρωτοκόλλου (SDP) παρέχει μια εξήγηση για να καθορίσει ποιες υπηρεσίες Bluetooth είναι διαθέσιμες σε μια ειδική συσκευή. Μια συσκευή Bluetooth μπορεί να ενεργήσει ως client SDP που ζητά τις υπηρεσίες, ένας server SPD παρέχει υπηρεσίες, ή και τα δύο. Μια μοναδική συσκευή Bluetooth θα έχει όχι περισσότερους από έναν server SDP, αλλά μπορεί να ενεργήσει ως client σε περισσότερες από μια απομακρυσμένες συσκευές. Το SDP παρέχει πρόσβαση μόνο στις πληροφορίες για υπηρεσίες και η χρησιμοποίηση εκείνων των υπηρεσιών πρέπει να παρέχεται μέσω ενός άλλου Bluetooth ή πρωτόκολλο τριών τμημάτων (third-party). Επιπλέον, το SDP δεν παρέχει κανέναν μηχανισμό γνωστοποίησης για να δηλώσει ένα server SDP, ή οποιαδήποτε συγκεκριμένη υπηρεσία, έχει γίνει διαθέσιμη ή μη διαθέσιμη καθώς μπορεί να εμφανιστεί όταν είναι διαθέσιμη η υπηρεσία στην αλλαγή συσκευής, ή όταν μια συσκευή εισέρχεται ή βγαίνει από την εμβέλεια RF. Αυτό θα ήταν ένα κοινό περιστατικό σε ένα δίκτυο που υποστηρίζει τις κινητές (mobile) συσκευές. Ο client μπορεί να καταγράψει έναν

server για να ανιχνεύσει την μη διαθεσιμότητα, όμως άλλα μέσα απαιτούνται για να ανιχνεύσουν έναν server ή μια υπηρεσία που έχει διατεθεί πρόσφατα.

3.8.1 Service Records (Υπηρεσία εγγραφών)

Η SDP, είναι μια υπηρεσία που μπορεί να παρέχει πληροφορίες, πραγματοποίηση μιας ενέργειας, ή να ελέγξει μια πηγή. Οι server SDP διατηρούν τα αρχεία υπηρεσιών για να καταχωρήσουν όλες τις διαθέσιμες υπηρεσίες που παρέχονται από τη συσκευή. Κάθε υπηρεσία αντιπροσωπεύεται από ένα μοναδικό αρχείο υπηρεσιών με έναν δυναμικά διατιθέμενο χειρισμό υπηρεσιών αρχείων που είναι μοναδική μέσα στον server. Ένα ειδικό αρχείο υπηρεσιών, με ένα χειρισμό αρχείων υπηρεσιών 0x00000000, παρέχεται για να περιγράψει τον ίδιο το server SDP και το πρωτόκολλο που υποστηρίζεται από αυτόν.

Οι ιδιότητες υπηρεσιών μέσα σε ένα αρχείο περιγράφουν και καθορίζουν την υποστηριγμένη υπηρεσία συμπεριλαμβάνοντας τον τύπο υπηρεσιών, μια ID υπηρεσία, τα υποστηριγμένα πρωτόκολλα, το όνομα υπηρεσίας, μια περιγραφή υπηρεσίας, και άλλα. Αυτά τα χαρακτηριστικά αποτελούνται από 16bit ID και μια τιμή μεταβλητού μήκους. Οι ιδιότητες τιμών περιλαμβάνουν στη συνέχεια ένα πεδίο επικεφαλίδας, έναν τύπο δεδομένων, ένα μέγεθος δεδομένων, και ένα πεδίο δεδομένων. Μια σειρά τύπων δεδομένων υποστηρίζεται από: κενό(null), ακέραιο χωρίς πρόσημο (unsigned integer), signed twos-complement integer, παγκοσμίως μοναδικό αναγνωριστικό(Universally Unique Identifier) (UUID)), αλφαριθμητικό (text string), Boolean, ακολουθία στοιχείου δεδομένων (data element sequence - set)), επιλογή στοιχείου δεδομένων (data element alternative), και URL. Η ερμηνεία αυτών των δεδομένων εξαρτάται από τα χαρακτηριστικά ID και την κατηγορία υπηρεσιών στις οποίες ανήκουν οι υπηρεσίες.

3.8.2 Discovering Services (Υπηρεσίες Ανεύρεσης)

Ο σκοπός του SDP είναι η ανακάλυψη και όχι πρόσβαση στις υπηρεσίες του. Υποστηρίζονται δύο διαδικασίες: η αναζήτηση (searching) και η φυλλομέτρηση (δηλαδή η αναζήτηση κάποιας πληροφορίας μέσα σ' ένα αρχείο, χωρίς να είναι κατ΄ανάγκη γνωστή η ύπαρξη ή η μορφή της). Η έρευνα είναι βασισμένη σε UUIDs. Ένα αρχείο υπηρεσιών επιστρέφεται από μια αναζήτηση μόνο εάν όλα τα UUIDs στο σχέδιο αναζήτησης υπηρεσιών βρίσκονται μέσα στις χαρακτηριστικές τιμές αρχείων υπηρεσιών. Δεν υπάρχει λόγος για το τι χαρακτηριστικό UUID βρέθηκε, ή εάν το UUID είναι μόνο ένα στοιχείο σε έναν κατάλογο, εφ' όσον όλη η αναζήτηση UUIDs περιλαμβάνεται κάπου μεταξύ των χαρακτηριστικών τιμών και της υπηρεσίας.

3.8.3. Πρωτόκολλο

Το SDP είναι ένα βασισμένο σε πακέτα πρωτόκολλο που χρησιμοποιεί μια αρχιτεκτονική αίτησης-απάντησης (request-response). Το SDP πακέτο αναφέρεται ως μονάδα πρωτοκόλλου δεδομένων (protocol data unit - PDU), η οποία περιλαμβάνει μια επικεφαλίδα που ακολουθείται από έναν μεταβλητό αριθμό παραμέτρων. Το μήκος της παραμέτρου αναφέρεται στην επικεφαλίδα (header), όπως είναι ο τύπος (PDU ID), ο οποίος μπορεί να δείξει μια αίτηση-απάντηση για τις αναζητήσεις ή χαρακτηριστικές ερωτήσεις. Η επικεφαλίδα περιλαμβάνει

επίσης μια συναλλαγή ID που χρησιμοποιείται για να ταιριάξει ένα αίτημα με την αντίστοιχη απάντηση. Εάν για κάποιο λόγο ο server δεν μπορεί να χειριστεί το αίτημα, τότε μπορεί να στείλει μια απάντηση του τύπου Error Response (PDU ID 0x01).

η απάντηση είναι δυνατόν να είναι πάρα πολύ μεγάλη για να ταιριάξει σε ένα μοναδικό PDU. Για να προσαρμοστεί αυτό, μια συνεχής κατάσταση παραμέτρου υποστηρίζεται από το PDUs. Σε μια απάντηση, αυτή η παράμετρος δείχνει τον αριθμό bytes που εκκρεμούν. Ο client μπορεί έπειτα να στείλει εκ νέου το αρχικό αίτημα, με ένα νέο ID (ταυτότητα) συναλλαγής αλλά με την συνέχεια της κατάστασης παραμέτρου. Αυτό προειδοποιεί τον server να στείλει στη συνέχεια την απάντηση. Το σημείο που είναι χωρισμένη μια απάντηση καθορίζεται από τον server.

Τρεις κατηγορίες συναλλαγών (PDU IDs) υποστηρίζονται:

i. service search transactions (συναλλαγές αναζήτησης υπηρεσιών),

ii. service attribute transactions (συναλλαγές ιδιοτήτων υπηρεσιών) και

iii. service search attribute transactions (συναλλαγές ιδιοτήτων αναζήτησης υπηρεσιών).

Οι service search transactions χρησιμοποιούνται για να ζητήσουν έναν κατάλογο που χειρίζεται αρχεία υπηρεσιών που έχουν τις ιδιότητες να περιέχουν όλο το UUIDs σε ένα σχέδιο αναζήτησης υπηρεσιών. Δεν υπάρχει κανένας μηχανισμός για να ζητήσει όλα τα αρχεία υπηρεσιών, αν και η φυλλομέτρηση υποστηρίζεται ήδη. Οι service attribute transactions χρησιμοποιούνται για να ζητήσουν συγκεκριμένες τιμές χαρακτηριστικών από ένα αρχείο υπηρεσιών. Οι service search attribute συνδυάζουν τις υπηρεσίες αναζήτησης και τις συναλλαγές χαρακτηριστικών υπηρεσιών, οι οποίες επιτρέπουν συγκεκριμένες τιμές χαρακτηριστικών για όλα τα αρχεία υπηρεσιών που ταιριάζουν με την αναζήτηση υπηρεσιών.

3.8.4 Frame Formats

Τα πρωτόκολλα της κύριας μνήμης (core) Bluetooth αποτελούνται από την βασική ζώνη, το LMP, το L2CAP, και το SDP. Η βασική ζώνη και ο έλεγχος σύνδεσης επιτρέπει τη φυσική σύνδεση RF μεταξύ των μονάδων Bluetooth που διαμορφώνουν ένα piconet. Δεδομένου ότι το σύστημα Bluetooth RF είναι frequency hopping spread-spectrum στο οποίο τα πακέτα διαβιβάζονται στις καθορισμένες χρονικές υποδοχές (times slots) στις καθορισμένες συχνότητες, το στρώμα αυτό χρησιμοποιεί αναζητήσεις σελιδοποίησης στις διαδικασίες για να συγχρονίσει τη μετάδοση αναπήδησης κατά συχνότητα και το ρολόι των διαφορετικών συσκευών Bluetooth. (δες το κουτάκι παρακάτω).

Connection-oriented σχεδίασμος πακέτου
Length (16 bits) dest CID (16 bits) payload (0-65,535 bytes)
Ασυνδεσμικός σχεδιασμός πακέτου
Length (16 bits) dest CID 0*0002 PSM payload (0-65,535 bytes)
Σχεδιασμός πακέτου βασικής ζώνης
Access code header payload header payload CRC

Το πρωτόκολλο διαχείρισης της σύνδεσης (LMP) είναι αρμόδιο για την οργάνωση σύνδεσης μεταξύ των συσκευών Bluetooth. Αυτό περιλαμβάνει τα χαρακτηριστικά ασφάλειας, όπως την αυθεντικοποίηση και την κρυπτογράφηση, ανταλλαγή, έλεγχο σύνδεσης, κρυπτογράφηση κλειδιών, έλεγχο και τη διαπραγμάτευση στο μέγεθος του πακέτου της βασικής ζώνης.

Το L2CAP παρέχει την connection-oriented και ασυνδεσμικές υπηρεσίες δεδομένων στο υψηλό-επίπεδο πρωτοκόλλου παρέχει ικανότητα πολυπλεξίας, κατάτμηση και την επανασυναρμολόγηση. Οι υπηρεσίες που ανακαλύφθηκαν είναι κρίσιμες για το πλαίσιο Bluetooth. Αυτές οι υπηρεσίες παρέχουν τη βάση για όλα τα πρότυπα χρήσης.

ΚΕΦΑΛΑΙΟ 4

ΑΣΦΑΛΕΙΑ BLUETOOTH

4.1 ΕΠΙΠΕΔΑ ΑΣΦΑΛΕΙΑΣ

Το Bluetooth έχει διαφορετικά επίπεδα ασφάλειας που μπορούν να καθοριστούν για τις συσκευές και τις υπηρεσίες. Όλες οι συσκευές παίρνουν ένα ρόλο όταν συνδεθούν για πρώτη φορά με μια άλλη συσκευή.

4 .1.1 Επίπεδο έμπιστης συσκευής

Οι συσκευές μπορούν να έχουν δύο επίπεδα αξιοπιστίας: τα *έμπιστα* (trusted) και *μη έμπιστα* (untrusted). Το έμπιστο επίπεδο απαιτεί μια σταθερή και έμπιστη σύνδεση και έχει απεριόριστη πρόσβαση σε όλες τις υπηρεσίες. Η συσκευή πρέπει προηγουμένως να αυθεντικοποιηθεί. Η μη έμπιστη συσκευή δεν έχει καθορίσει τη σχέση και η πρόσβασή της στις υπηρεσίες είναι περιορισμένη. Μια μη έμπιστη συσκευή μπορεί επίσης να έχει μια σταθερή σύνδεση, αλλά δεν θεωρείται ως έμπιστη. Μια νέα συσκευή χαρακτηρίζεται ως άγνωστη (unknown) συσκευή και είναι πάντα μη αξιόπιστη.

4.1.2 Τρόποι Ασφάλειας

Το Bluetooth έχει τρεις διαφορετικούς τρόπους ασφάλειας και είναι οι ακόλουθοι:

Mode 1: Μια συσκευή δεν θα αρχίσει κανένα μέτρο ασφάλειας. Είναι ένας μη-ασφαλής τρόπος και έτσι η επικοινωνία πραγματοποιείται χωρίς πιστοποίηση ή κρυπτογράφηση. [19]

Mode 2: Μια συσκευή δεν αρχίζει διαδικασίες ασφάλειας πριν από την εγκατάσταση καναλιών στο επίπεδο L2CAP. Αυτός ο τρόπος επιτρέπει διαφορετικές και εύκαμπτες πολιτικές πρόσβασης για τις εφαρμογές, ειδικά τρέχοντας εφαρμογές παράλληλα με διαφορετικές

απαιτήσεις ασφάλειας. Επιβάλλετε ένας τρόπος ασφάλειας στο επίπεδο υπηρεσιών.

Mode 3: Μια συσκευή αρχίζει τις διαδικασίες ασφάλειας προτού να ολοκληρωθεί η οργάνωση σύνδεσης στο επίπεδο LPM. Επιβάλλετε ένας τρόπος ασφάλειας στα επίπεδα σύνδεσης.

Η παραπάνω διαδικασία χρησιμοποιεί πιο πολύ τον τρόπο ασφάλειας 2.

Μια συσκευή που χρησιμοποιεί τον τρόπο ασφάλειας 2, θα κινήσει τις διαδικασίες ασφάλειας όταν παραλαμβάνεται ένα L2CAP_ConnectReq που συνδέεται με ένα κανάλι που απαιτεί ασφάλεια. Τα μέτρα ασφάλειας ολοκληρώνονται προτού να επιστραφεί L2CAP_ConnectRsp. Οι απαιτήσεις ασφάλειας αυτού του καναλιού θα μπορούσαν να περιλάβουν την πιστοποίηση, έγκριση, και ίσως την κρυπτογράφηση, και διαφορετικά κανάλια μπορούν να έχουν διαφορετικές απαιτήσεις ασφάλειας. Για τον τρόπο ασφάλειας 3, οι διαδικασίες ασφάλειας ξεκινούν όταν λαμβάνεται το LMP_hostconnection_req και ολοκληρώνονται προτού να σταλεί το LMP_setup_complete.

Παραδείγματος χάριν, ένας πελάτης θα μπορούσε να συνδεθεί με έναν server με μια σύνδεση ACL, που υλοποιείται με ένα κανάλι L2CAP, για να φυλλομετρήσει τις υπηρεσίες χωρίς την ανάγκη για ασφάλεια. Όταν γίνεται προσπάθεια για να έχουμε πρόσβαση σε μια υπηρεσία, η πιστοποίηση, που ακολουθήθηκε από έναν έλεγχο έγκρισης, θα μπορούσε να απαιτηθεί προτού να χορηγηθεί η πρόσβαση.

4.1.3 Επίπεδο ασφάλειας υπηρεσιών

Η ανάγκη για εξουσιοδότηση (authorization), αυθεντικοποίηση και κρυπτογράφηση αλλάζει. Όταν αρχίζει μια σύνδεση υπάρχουν διαφορετικά επίπεδα ασφάλειας όπου ο χρήστης μπορεί να επιλέξει. Το επίπεδο ασφάλειας μιας υπηρεσίας καθορίζεται από τρεις ιδιότητες:

Εξουσιοδότηση (authorization): Η πρόσβαση χορηγείται αυτόματα μόνο στις έμπιστες συσκευές ή τις μη έμπιστες (untrusted) μετά από μια διαδικασία εξουσιοδότησης.
Αυθεντικοποίηση (authentication): Η απομακρυσμένη συσκευή πρέπει να αυθεντικοποιηθεί. πριν συνδεθεί με την εφαρμογή,
Κρυπτογράφηση (encryption): Η σύνδεση πρέπει να αλλάξει τρόπο κρυπτογράφησης, προτού να έχουμε πρόσβαση στην υπηρεσία.

Στο χαμηλότερο επίπεδο οι υπηρεσίες μπορούν να γίνουν προσβάσιμες για όλες τις συσκευές. Συνήθως υπάρχει ανάγκη περιορισμών, έτσι όταν ο χρήστης ζητήσει μια υπηρεσία είναι αναγκαία η αυθεντικοποίηση. Όταν απαιτηθεί υπηρεσία στο πιο υψηλό επίπεδο ασφάλειας τότε μπορεί να ζητήσει εξουσιοδότηση και αυθεντικοποίηση. Σ' αυτό το επίπεδο η έμπιστη συσκευή έχει πρόσβαση στις υπηρεσίες, αλλά η μη έμπιστη (untrusted) συσκευή χρειάζεται εξουσιοδότηση από τον χρήστη.

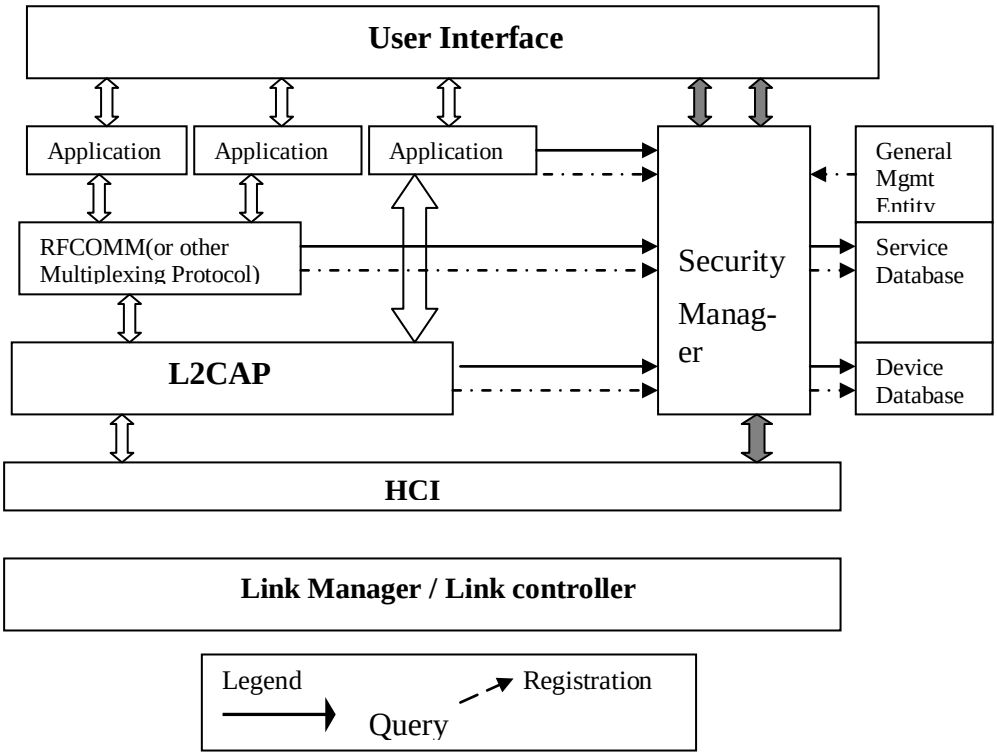
4.2 ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ

Εάν οποιοδήποτε μέρος της ασφάλειας Bluetooth μπορεί να πραγματοποιηθεί αυτόματα, τότε ένας διαχειριστής ασφάλειας πρέπει να είναι μέρος του πακέτου λογισμικού host. Επιπλέον, για μεγαλύτερη ευελιξία, η πιστοποίηση και η εξουσιοδότηση θα έπρεπε να εμφανιστούν μετά από τον καθορισμό του επιπέδου ασφάλειας της απαιτούμενης υπηρεσία. Έτσι τα μέτρα ασφάλειας πρέπει να εφαρμοστούν αφότου εγκατασταθεί η σύνδεση ACL. Αυτό υπονοεί ότι πραγματοποιείται ο τρόπος ασφάλειας 2 (σύνδεση με επιβεβλημένη ασφάλεια). Φυσικά, μια άλλη αυθεντικοποίηση θα μπορούσε να εμφανιστεί με την αρχική εγκατάσταση σύνδεσης ACL, αλλά σε πολλές περιπτώσεις θα ήταν περιττή αυτή η αυθεντικοποίηση.

Το σχήμα 4.1 παρουσιάζει τον διαχειριστή ασφάλειας που υπάρχει σε έναν host Bluetooth επικοινωνώντας με L2CAP και με το LM μέσω του HCI. Ένα τυπικό σενάριο ασφάλειας μοιάζει με αυτό:

1. Στο επίπεδο L2CAP φτάνει ένα αίτημα σύνδεσης από μια άλλη συσκευή.
2. Ο L2CAP ζητά αποτίμηση από το διαχειριστή ασφάλειας.
3. Ο διαχειριστής ασφάλειας ανατρέχει στην απαιτούμενη υπηρεσία στη βάση δεδομένων για τις πληροφορίες ασφάλειας.
4. Ο διαχειριστής ασφάλειας ανατρέχει στο BD_ADDR της συσκευής αίτησης μέσα στη βάση δεδομένων για τις εγκρίσεις πρόσβασης.
5. Ο διαχειριστής ασφάλειας αρχίζει την απαραίτητη πιστοποίηση και (εάν χρειάζεται) διαδικασίες κρυπτογράφησης με το LM μέσω HCI.
6. Εάν όλα είναι καλά, ο LM δίνει μια ευνοϊκή απάντηση μέσω HCI.
7. Ο L2CAP τελειώνει τη διαδικασία οργάνωσης σύνδεσης.

Η αρχιτεκτονική διαχειριστή ασφάλειας στο σχήμα 4.1 θα μπορούσε να χρησιμοποιηθεί για να εφαρμόσει τον τρόπο 3 ασφάλειας. Μια πιθανή σύγκρουση θα εμφανιστεί όταν αποθηκευθούν τα κλειδιά σύνδεσης σε δύο διαφορετικές θέσεις: στην μονάδα Bluetooth για ενισχυμένο επίπεδο ασφάλειας σύνδεσης και στον host για ενισχυμένη ασφάλεια. Προκειμένου να αποτραπεί η αδικαιολόγητη αξιοπιστία χορήγησης κλειδιών σύνδεσης της συσκευής τα οποία αποθηκεύονται στην μονάδα, ο διαχειριστής ασφάλειας μπορεί να αφαιρέσει αυτά τα κλειδιά, καταργώντας κατά συνέπεια τη σύνδεση μεταξύ των συσκευών, με τη χρησιμοποίηση των εντολών HCI.

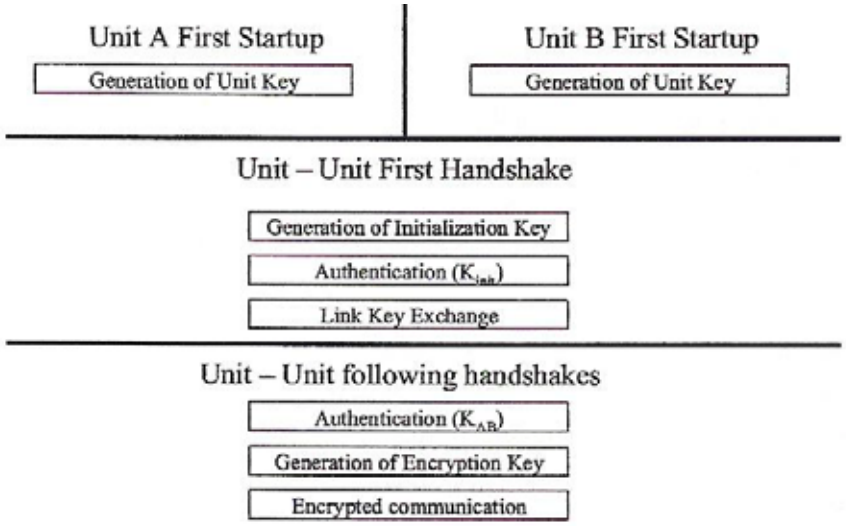


Σχήμα 4.1: Η στοίβα του Πρωτοκόλλου Bluetooth

4.3 ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ BLUETOOTH

Το σχήμα 4-2 αντιπροσωπεύει το γενικό σχέδιο ασφάλειας Bluetooth, υποθέτοντας ότι υπάρχουν μόνο δύο συσκευές που προσπαθούν να επικοινωνήσουν η μια με την άλλη. Τα σημαντικότερα βήματα σε κάθε φάση είναι:

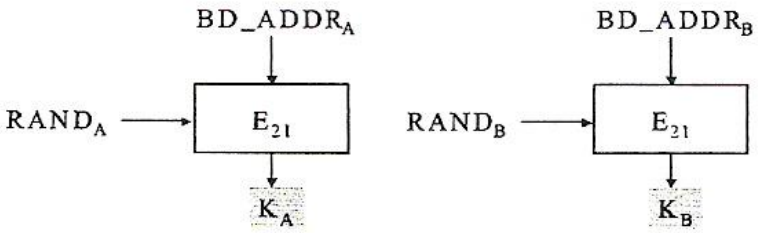
1. οι μονάδες ανοίγονται για πρώτη φορά (unit first startup),
2. έχουν επαφή για πρώτη φορά (first handshake) προκειμένου να δημιουργηθεί ένα μυστικό κλειδί για να ακολουθήσει η επικοινωνία τους και
3. όταν χρησιμοποιούν αυτή την αποθήκευση, ανταλλάσσουν το αμετάβλητο μυστικό κλειδί για την έναρξη ανταλλαγής των δεδομένων (following handshakes).



Σχήμα 4.2

4.3.1 Παραγωγή κλειδιού μονάδας (Generation of the unit key)

Αυτήν η φάση (που παρουσιάζεται στο σχήμα 4-3) συμβαίνει ουσιαστικά μόνο μια φορά σε κάθε διάρκεια ζωής της συσκευής, την πρώτη φορά που ανοίγεται (turned on).



Σχήμα 4.3

Η συσκευή παράγει το δικό της κλειδί μονάδας (unit key) (στο σχήμα ονομάζεται K_A και K_B στο σχήμα), το οποίο βασίζεται πάνω στο δικό του BD_ADDR (που είναι μια κατασκευαστική παράμετρος μοναδική σε κάθε συσκευή, όπως είναι ο medium access control (MAC) για τις κάρτες Ethernet), και έναν τυχαία παραγόμενο αριθμό. Αυτό το κλειδί μονάδας αποθηκεύεται έπειτα σε δικιά του αμετάβλητη μνήμη. Με το Bluetooth, οι απαιτήσεις που χρησιμοποιήθηκαν τοποθετούνται σε έναν τυχαίο αριθμό που είναι μη-επαναλαμβανόμενος (non-repeating)ι και παράγεται τυχαία. Μη- επαναλαμβανόμενος (non-repeating) σημαίνει ότι θα είναι ιδιαίτερα απίθανη η τιμή να επαναληφθεί η ίδια μέσα στη διάρκεια ζωής της αυθεντικοποίησης του κλειδιού. Τυχαία παραγόμενος (randomly generated) σημαίνει ότι δεν θα είναι δυνατό να προβλεφθεί η τιμή του, με μια πιθανότητα που είναι σημαντικά μεγαλύτερη από το μηδέν .[1]

Αυτό το κλειδί θα μπορούσε επίσης να απορριφθεί ρητώς και να αναπαραχθεί λόγω της επέμβασης χρηστών· Επομένως, κάθε σύνδεση με κάθε άλλη μονάδα

ακυρώνεται αυτόματα, έτσι ώστε η ακόλουθη φάση θα πρέπει να εμφανιστεί πάλι σε κάθε άλλη συσκευή για να επικοινωνήσει.

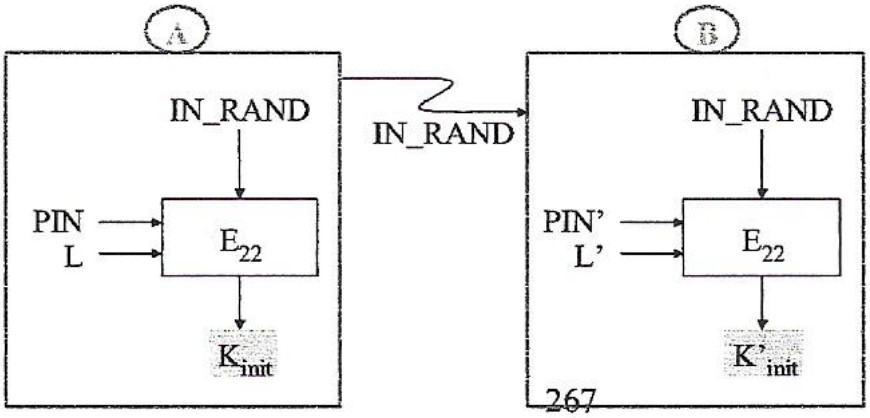
4.3.2 First Handshake

Τι θα συμβεί όταν δύο μονάδες Bluetooth δεν έχουνε ποτέ πριν επαφή; Μια από τις δύο μονάδες (ο αποστολέας, μονάδα B) που προσπαθεί να προσεγγίσει την άλλη (ο παραλήπτης, μονάδα A), εμφανίζεται η πρώτη επαφή (handshake). Ο αποστολέας θα πρέπει να αποδείξει ότι είναι μια εξουσιοδοτημένη μονάδα πριν λάβει οποιαδήποτε ανταλλαγή δεδομένων με τον παραλήπτη.

Ορισμός, κάθε αποστολέας εξουσιοδοτείται εάν χρησιμοποιήσει το ίδιο PIN με τον παραλήπτη. Το PIN είναι ένας κωδικός μεταβλητού μήκους. Θα μπορούσε να είναι τετραψήφιος, όπως η χρήση εισαγωγής PIN στα κινητά τηλέφωνα, ή ένα πιο μεγάλο κλειδί (μέχρι 16 octets, το οποίο είναι 128 bit) που είναι συμβατό με άλλες μεθόδους όπως το κλειδί συμφωνίας Diffie-Hellman. Στη χειρότερη περίπτωση, όταν μια από τις δύο μονάδες είναι μια συσκευή πολύ περιορισμένης μνήμης (memory-limited), το PIN θα ήταν ενσωματωμένο από το εργοστάσιο και όχι με την αλληλεπίδραση των χρηστών.

4.3.2.α Παραγωγή του κλειδιού αρχικοποίησης (Generation of the init key)

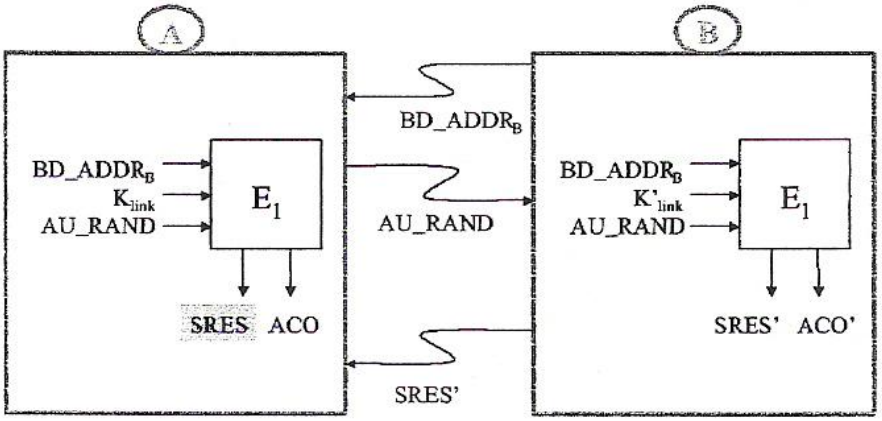
Αυτό το βήμα χρησιμοποιείται μόνο για να παράγει ένα κλειδί αρχικοποίησης (initialization key) για αποτελεσματική αυθεντικοποίηση που απαιτείται στο ακόλουθο σχήμα. Το κλειδί αρχικοποίησης παράγεται ως εξής: Η μονάδα A στέλνει έναν τυχαίο αριθμό IN_RAND στη μονάδα B. Τώρα και οι δύο μονάδες μπορούν να παραγάγουν το *κλειδί αρχικοποίησης* (initialization key) $K_{init}=E_{22}(PIN,PIN\_LENGTH,IN\_RAND)$, το οποίο χρησιμοποιεί το ακόλουθο βήμα ως *προσωρινό κλειδί σύνδεσης* (temporary link key).



Σχήμα 4.4

4.3.2.β Αυθεντικοποίηση (Authentication)

Αυτό το σχήμα αυθεντικοποίησης είναι το ίδιο ανεξάρτητα από το γεγονός αν είμαστε στη φάση 1 ή φάση 2. Η διαφορική παράμετρος είναι το κλειδί σύνδεσης K_{link}. Είναι το προσωρινό κλειδί σύνδεσης για την πρώτη επαφή, ενώ είναι ένα ημιμόνιμο κλειδί σύνδεσης κοινό στις δύο μονάδες Α και Β για τις τυποποιημένες επαφές. Αυτό το βήμα, είναι βασισμένο στο σχέδιο αυθεντικοποίησης *πρόκλησης / απάντησης* όπου για να αποδείξει ο αποστολέας τη σωστή γνώση σύνδεσης του κλειδιού, που είναι το K_{AB}, και η K_{init} για την πρώτη αυθεντικοποίηση. Η μονάδα Α παράγει έναν τυχαίο αριθμό AU_RAND και τον στέλνει στη μονάδα Β. Και οι δύο μονάδες, Α και Β. παράγουν έπειτα τα SRES και SRES' αντίστοιχα. Με τον υπολογισμό του SAFER+ βασισμένου στην MAC λειτουργία E1(AU_RAND, BD_ADDR_B, K_{link}), το SRES' έπειτα στέλνεται πίσω στη μονάδα Α. Εάν ισχύει SRES=SRES', η διαδικασία αυθεντικοποίησης είναι επιτυχής και οι μονάδες μπορούν να αρχίσουν την επικοινωνία.

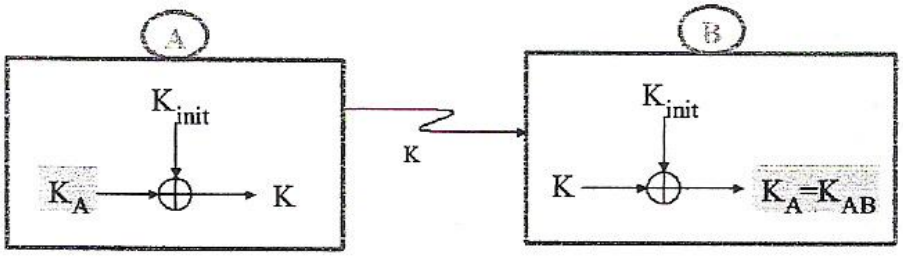


Σχήμα 4.5

4.3.2.γ Ανταλλαγή κλειδιού σύνδεσης (Link key exchange)

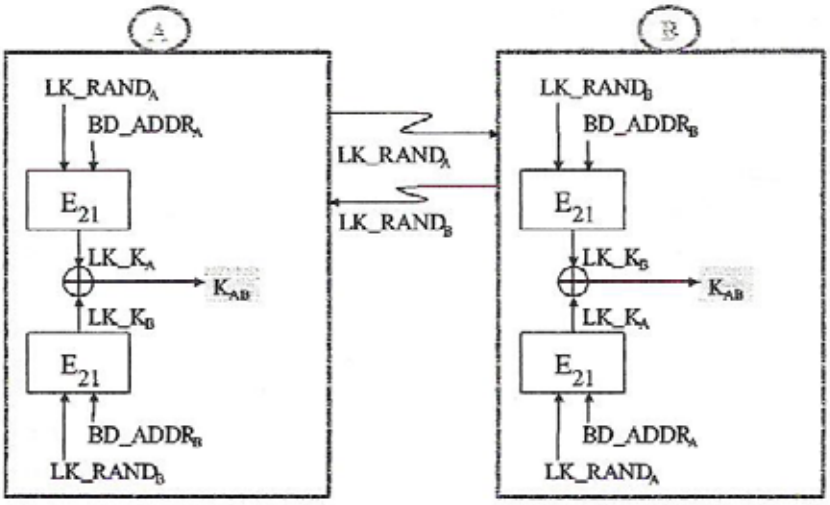
Είναι σημαντικό το ημιμόνιμο κλειδί σύνδεσης (K_{AB}) μεταξύ των δύο μονάδων (που θα αποθηκευθεί σε κάθε μια για οποιαδήποτε μελλοντική αυθεντικοποίηση ώστε να εγκατασταθεί μια σύνδεση) να συμφωνηθεί και να ανταλλαχθεί. Η σύνδεση κλειδιού είναι είτε εξαρτώμενη από την απαίτηση του επιπέδου ασφάλειας είτε απο τους περιορισμούς μνήμης της συσκευής:

- Το κλειδί μονάδας(unit key) σε μια από τις δύο συσκευές (σχήμα 4-6), ή
- Το κλειδί συνδυασμού (combination key) προέρχεται από το κλειδί μονάδαςκαι των δύο μονάδων (εικόνα 4-7).



Σχήμα 4.6

Εάν το κλειδί σύνδεσης είναι ένα κλειδί μονάδας (π.χ. η μονάδα του A), μεταφέρεται από τη μονάδα A στη μονάδα B απλά XOR'd με το κλειδί αρχικοποίησης.



Σχήμα 4.7

Εάν το κλειδί σύνδεσης είναι ένα κλειδί συνδυασμού, συμβαίνουν τα εξής:

- Η μονάδα A παράγει έναν τυχαίο αριθμό LK_RAND_A, και υπολογίζει το (με τον ίδιο αλγόριθμο που χρησιμοποιείται για να παράγει το νέο unit key) $LK\_KA = E_{21}(LK\_RAND_A, BD\_ADDR_A)$.
- η μονάδα B παράγει έναν τυχαίο αριθμό LK_RAND_B, και υπολογίζει το $LK\_K_B = E_{21}(LK\_RAND_B, BD\_ADDR_B)$.
- Το LK_RAND_A στέλνεται στη μονάδα B, και αντίστροφα.
- Κάθε μονάδα υπολογίζει το δικό της κλειδί, και το πραγματικό κλειδί συνδιασμού K_{AB} είναι απλά η XOR των δύο κλειδιών.

Μετά από αυτά που έχουνε συμβεί στα προηγούμενα βήματα (π.χ., μετά από την ανταλλαγή του κλειδιού σύνδεσης), το παλαιό, προσωρινό κλειδί αρχικοποίησης απορρίπτεται οριστικά. Κατόπιν αυτού ξεκινάμε μια νέα φάση αυθεντικοποίησης (αυτή τη φορά με την ανταλλαγή του κλειδιού σύνδεσης).

4.3.3 Αλληλεπίδραση (interaction) συσκευών

Αφού οι δύο μονάδες έχουν ανταλλάξει ένα κοινό κλειδί σύνδεσης όπως στο προηγούμενο βήμα, το χρησιμοποιούν κάθε φορά για να πιστοποιήσουν η μία την άλλη. Επίσης, αν είναι απαραίτητο, μπορεί να γίνει κρυπτογράφηση.

4.3.3.α Αυθεντικοποίηση

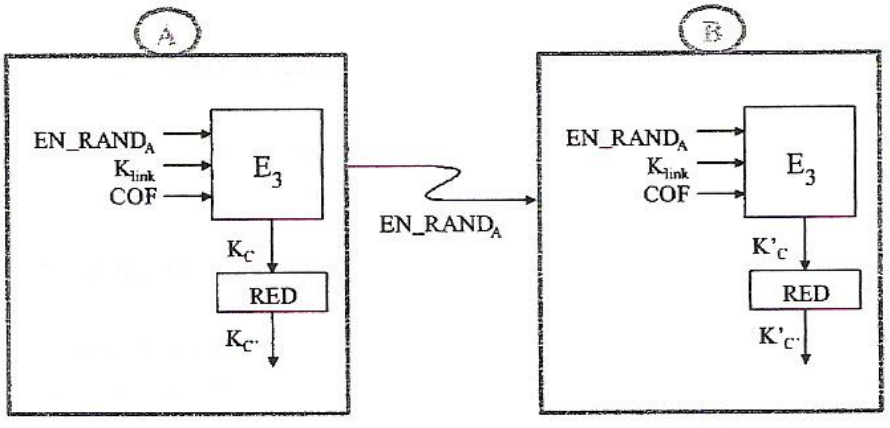
Σ΄ αυτή τη φάση που είναι ακριβώς ίδια με την παράγραφο 3.2.2, με τη μόνη διαφορά ότι χρησιμοποιείται το κοινό, ημιμόνιμο (semi-permanent) κλειδί σύνδεσης αντί το κλειδί αρχικοποίησης (initialization key).

4.3.3.β Παραγωγή κλειδιού κρυπτογράφησης (Encryption key generation)

Μετά από μια επιτυχή αυθεντικοποίηση, η κρυπτογράφηση μπορεί να επιτραπεί και ένα κλειδί κρυπτογράφησης πρέπει να παραχθεί.

Η παράμετρος ciphering offset number (COF) εξαρτάται από τον πραγματικό τύπο επικοινωνίας. Θα μπορούσε να είναι είτε:

- Η authenticated ciphering offset (ACO) που παράγεται κατά τη διάρκεια της αυθεντικοποιημένης φάσης πρόκλησης – απάντησης (challenge-response) ή
- Την αλληλουχία της διεύθυνσης συσκευής Bluetooth του αποστολέα για μια κρυπτογραφημένη αναμετάδοση (broadcast) επικοινωνίας (BD_ADDR + BD_ADDR).

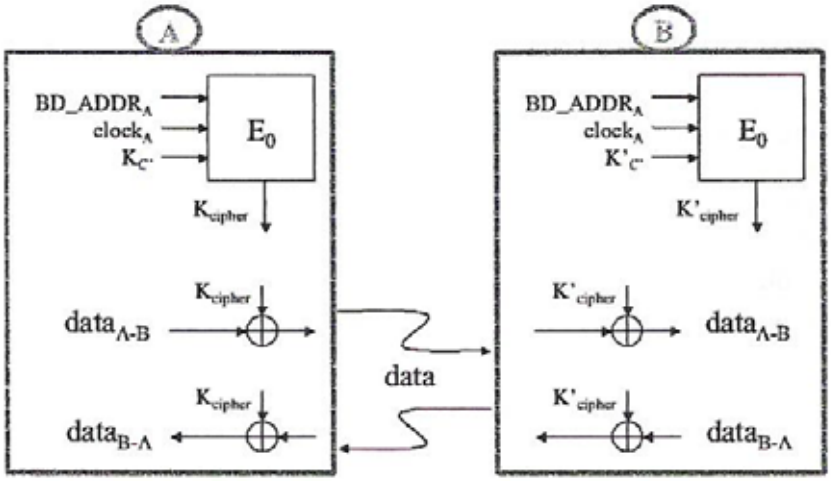


Σχήμα 4.8

Εάν είναι απαραίτητο, το κλειδί κρυπτογράφησης θα μπορούσε να τροποποιηθεί σε ένα πιο σύντομο κλειδί χρησιμοποιώντας μια κατάλληλη μειωμένη λειτουργία, RED.

4.3.3.γ Κρυπτογράφηση επικοινωνίας (Encrypted communication)

Το σχέδιο κρυπτογράφησης είναι απλό. Λαμβάνοντας υπόψη την προηγούμενη παραγωγή κρυπτογράφησης κλειδιού $K_{C'}$, και οι δύο μονάδες χρησιμοποιούν τις ενδεικνυόμενες παραμέτρους (BD_ADDR_A, $clock_A$, $K_{c'}$) για να λάβει μια ροή δεδομένων η οποία θα είναι XOR'd στα εξερχόμενα και εισερχόμενα δεδομένα για να το κρυπτογραφήσει και να το αποκρυπτογραφήσει, αντίστοιχα. Ο κύριος χρονιστής χρησιμοποιείται για να παρέχει μια harder-to-guess ροή κρυπτογράφησης.



Σχήμα 4.9

4.4 ΚΛΕΙΔΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

Υπάρχουν διάφορα είδη κλειδιών στο σύστημα Bluetooth για να εξασφαλίσουν ασφαλή μετάδοση. Το σημαντικότερο κλειδί είναι το κλειδί σύνδεσης, το οποίο χρησιμοποιείται μεταξύ δύο συσκευών Bluetooth με σκοπό την αυθεντικοποίηση. Χρησιμοποιώντας το κλειδί σύνδεσης παράγεται το κλειδί κρυπτογράφησης. Αυτό εξασφαλίζει τα στοιχεία του πακέτου και αναπαράγεται για όλες τις νέες μεταδόσεις.

4.4.1 Κλειδιά Σύνδεσης

Υπάρχουν τέσσερα κλειδιά σύνδεσης για να καλύψουν τις διαφορετικές εφαρμογές που χρησιμοποιούνται. Όλα τα κλειδιά είναι 128-bit τυχαίων αριθμών και είναι είτε *προσωρινά (temporary)* είτε *ημιμόνιμα (semi-permanent)*.

Το ***κλειδί μονάδας (unit key)***, K_A παράγεται κατά την εγκατάσταση της συσκευής Bluetooth από μια μονάδα Α. Η αποθήκευση του K_A απαιτεί μικρό χώρο

μνήμης και χρησιμοποιείται συχνά όταν έχει η συσκευή μικρή μνήμη ή όταν πρέπει η συσκευή να είναι προσιτή σε μια μεγάλη ομάδα χρηστών.

Το ***κλειδί συνδυασμού (combination key)***, K_{AB} προέρχεται από δύο μονάδες A και B. Αυτό το κλειδί παράγεται για κάθε ζευγάρι (pair) συσκευών και χρησιμοποιείται όταν απαιτείται περισσότερη ασφάλεια. Απαιτεί περισσότερη μνήμη, δεδομένου ότι η συσκευή πρέπει να αποθηκεύσει το κλειδί συνδυασμού για κάθε σύνδεση που έχει.

Το ***κύριο κλειδί (master key),*** K_{master}, χρησιμοποιείται όταν θέλει η κύρια συσκευή να διαβιβάσει δεδομένα σε διάφορες συσκευές.

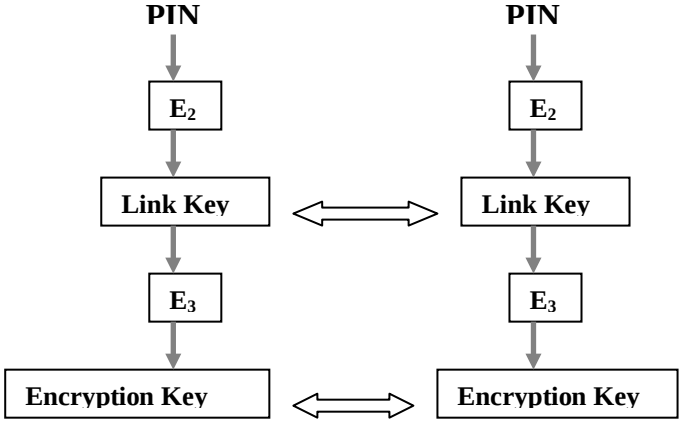
Το ***κλειδί αρχικοποίησης (initialization key),*** K_{init}, χρησιμοποιείται στη διαδικασία αρχικοποίησης. Αυτό το κλειδί προστατεύει τις παραμέτρους αρχικοποίησης όταν αυτές μεταδίδονται. Αυτό το κλειδί διαμορφώνεται από έναν τυχαίο αριθμό, ένας L-octet κώδικας PIN, και το BD_ADDR του παραλήπτη (claimant).

4.4.2 Κλειδί κρυπτογράφησης

Το κλειδί κρυπτογράφησης προέρχεται από το τρέχον κλειδί σύνδεσης. Κάθε φορά που απαιτείται κρυπτογράφηση το κλειδί κρυπτογράφησης αλλάζει αυτόματα. Ο σκοπός του ξεχωριστού κλειδιού αυθεντικοποίησης και του κλειδιού κρυπτογράφησης είναι να διευκολύνει τη χρήση ενός πιο σύντομου κλειδιού κρυπτογράφησης χωρίς την αποδυνάμωση της ισχύος της διαδικασίας αυθεντικοποίησης [1]

4.4.3 Κωδικός PIN

Αυτός είναι ένας αριθμός, ο οποίος μπορεί να καθοριστεί ή να επιλεχτεί από το χρήστη. Το μήκος του είναι συνήθως 4 ψηφία, αλλά μπορεί να είναι μεταξύ 1 έως 16 octets. Ο χρήστης μπορεί να το αλλάξει όταν θελήσει γεγονός που προσθέτει ασφάλεια στο σύστημα. Το PIN μπορεί να χρησιμοποιηθεί εισάγοντας το σε μια συσκευή (σταθερό PIN), αλλά είναι ασφαλέστερο να εισαχθεί και στις δύο μονάδες. Για παράδειγμα το τελευταίο μπορεί να χρησιμοποιηθεί όταν υπάρχει σύνδεση σε ένα lap-top και ένα τηλέφωνο .



Σχήμα 4-10: Κρυπτογράφηση και έλεγχος κλειδιού

4.4.4 Παραγωγή κλειδιού και αρχικοποίηση (Generation key and initialization)

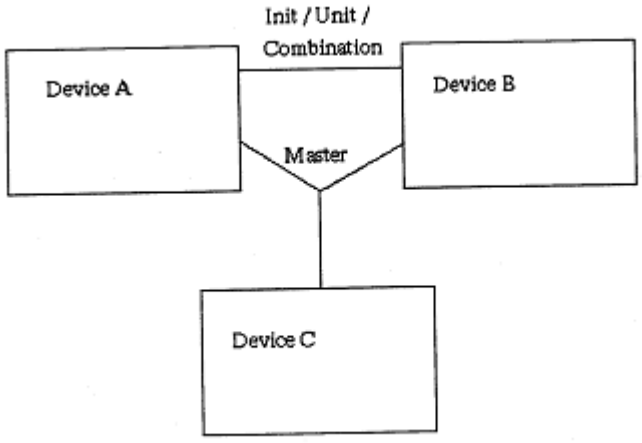
Η ανταλλαγή των κλειδιών πραγματοποιείται κατά τη διάρκεια μιας αρχικής φάσης, η οποία πρέπει να πραγματοποιηθεί χωριστά για κάθε δύο μονάδες που θέλουν να εφαρμόσουν την αυθεντικοποίηση και την κρυπτογράφηση. Όλες οι διαδικασίες αρχικοποίησης αποτελούνται από τα ακόλουθα πέντε μέρη:

- Δημιουργία ενός αρχικού κλειδιού
- Αυθεντικοποίηση
- Παραγωγή του κλειδιού σύνδεσης
- Ανταλλαγή κλειδιού σύνδεσης
- Παραγωγή του κλειδιού κρυπτογράφησης σε κάθε μονάδα [1]

Μετά από αυτήν την διαδικασία η σύνδεση μπορεί να υλοποιηθεί ή να απορριφθεί.

4.5 ΤΑ ΚΛΕΙΔΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΛΕΠΤΟΜΕΡΕΣΤΕΡΑ[5]

Όλες οι συναλλαγές ασφάλειας μεταξύ δύο ή περισσότερων συμβαλλόμενων μερών πραγματοποιούνται από το κλειδί σύνδεσης (link key). Το κλειδί σύνδεσης είναι ένας τυχαίος αριθμός 128bit. Χρησιμοποιείται στη διαδικασία αυθεντικοποίησης και ως παράμετρος κατά την παραγωγή του κλειδιού κρυπτογράφησης. Η διάρκεια ζωής ενός κλειδιού σύνδεσης εξαρτάται από εάν ένα κλειδί είναι ημιμόνιμο ή προσωρινό. Ένα ημιμόνιμο κλειδί μπορεί να χρησιμοποιηθεί αφότου η τρέχουσα σύνοδος έχει αυθεντικοποιήσει τις μονάδες Bluetooth που το μοιράζονται. Ένα προσωρινό κλειδί διαρκεί μόνο έως ότου ολοκληρώνεται η τρέχουσα σύνοδος και δεν μπορεί να επαναχρησιμοποιηθεί. Τα προσωρινά κλειδιά χρησιμοποιούνται συνήθως στις point-to-multipoint συνδέσεις, όπου οι ίδιες πληροφορίες διαβιβάζονται σε διάφορους παραλήπτες.

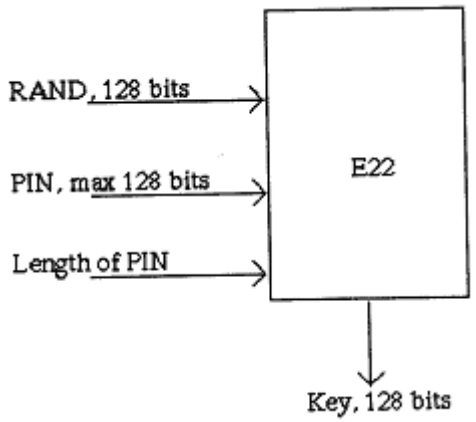


Σχήμα 4.11: Διάφορα κλειδιά σύνδεσης μεταξύ συσκευών

Υπάρχουνε διάφοροι τύποι κλειδιών στο Bluetooth .Τα κλειδιά σύνδεσης μπορεί να είναι κλειδιά συνδυασμού (combination key), κλειδιά μονάδας (unit key), κύρια κλειδιά (master key), ή κλειδιά αρχικοποίησης (initialization keys), ανάλογα με τον τύπο εφαρμογής. Εκτός από τα κλειδιά σύνδεσης (link keys), υπάρχει και το κλειδί κρυπτογράφησης (encryption key).

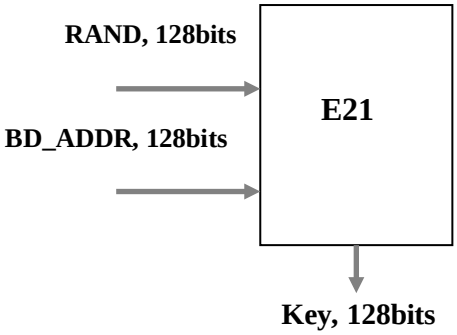
Το κλειδί μονάδας (unit key) παράγεται σε μια απλή συσκευή όταν εγκαθίσταται. Το κλειδί συνδυασμού (combination key) προέρχεται από τις πληροφορίες από δύο συσκευές και παράγεται για κάθε νέο ζευγάρι των συσκευών Bluetooth. Το κύριο κλειδί (master key) είναι ένα προσωρινό κλειδί, το οποίο αντικαθιστά το τρέχον κλειδί σύνδεσης (current link key). Μπορεί να χρησιμοποιηθεί όταν θέλει η κύρια μονάδα (master unit) να διαβιβάσει τις πληροφορίες σε περισσότερους από έναν παραλήπτες. Το κλειδί αρχικοποίησης (initialization key) χρησιμοποιείται ως κλειδί σύνδεσης (link key) κατά τη διάρκεια της διαδικασίας αρχικοποίησης όταν δεν υπάρχουν ακόμα κλειδιά μονάδας (unit key) ή κλειδιά συνδυασμού (combination key). Αυτό χρησιμοποιείται μόνο κατά τη διάρκεια της εγκατάστασης.

Το μήκος του προσωπικού αριθμού πιστοποίησης (personal identification number - PIN) που χρησιμοποιείται στις συσκευές Bluetooth μπορεί να ποικίλει μεταξύ 1 και 16 octets. Ο κανονικός τετραψήφιος κώδικας είναι ικανοποιητικός για μερικές εφαρμογές, αλλά για να έχουμε υψηλότερη ασφάλεια ίσως να χρειαστούμε πιο μεγάλους κωδικούς. Ο κώδικας PIN της συσκευής μπορεί να καθοριστεί, έτσι ώστε να πρέπει να εισαχθεί μόνο στη συσκευή που επιθυμεί τη σύνδεση. Μια άλλη δυνατότητα είναι ότι ο κωδικός PIN πρέπει να πληκτρολογηθεί και στις δύο συσκευές κατά τη διάρκεια της έναρξης σύνδεσης.



Σχήμα 4.12: Παραγωγή κλειδιού αλγόριθμου E22 για master και κλειδιά αρχικοποίησης

Το κλειδί αρχικοποίησης (initialization key) χρειάζεται όταν πρέπει να επικοινωνήσουν δύο συσκευές χωρίς τις προηγούμενες δεσμεύσεις. Κατά τη διάρκεια της διαδικασίας αρχικοποίησης, ο κωδικός PIN πληκτρολογείται και στις δύο συσκευές. Το ίδιο το κλειδί αρχικοποίησης παράγεται από τον αλγόριθμο E22, ο οποίος χρησιμοποιεί τον κωδικό PIN, την διεύθυνση συσκευών Bluetooth του παραλήπτη (claimant) συσκευής και έναν τυχαίο αριθμό 128bit που παράγεται από τον αποστολέα (verifier) συσκευής. Το προκύπτον κλειδί αρχικοποίησης των 128bit χρησιμοποιείται για το κλειδί ανταλλαγής (key exchange) κατά τη διάρκεια της παραγωγής ενός κλειδιού σύνδεσης (link key). Μετά το κλειδί ανταλλαγής το κλειδί αρχικοποίησης απορρίπτεται.

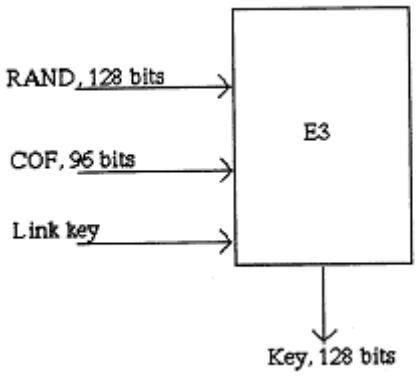


Σχήμα 4.13 : Αλγόριθμος παραγωγής κλειδιών E21 για κλειδιά μονάδας και συνδυασμού.

Το *κλειδί μονάδας* παράγεται με τον αλγόριθμο E21 παραγωγής κλειδιού όταν η συσκευή Bluetooth τίθεται σε λειτουργία για πρώτη φορά. Αφότου έχει δημιουργηθεί, αποθηκεύεται στην αμετάβλητη μνήμη της συσκευής και αλλάζει σπάνια. Μια άλλη συσκευή μπορεί να χρησιμοποιήσει το κλειδί μονάδας άλλων συσκευών ως κλειδί σύνδεσης μεταξύ αυτών των συσκευών. Κατά τη διάρκεια της διαδικασίας αρχικοποίησης, η εφαρμογή αποφασίζει ποιο κομμάτι θα μπορεί να παρέχει το κλειδί μονάδας της ως κλειδί σύνδεσης. Εάν μια από τις συσκευές έχει μνήμη περιορισμένων ικανοτήτων (δηλ. δεν μπορεί να απομνημονεύσει οποιαδήποτε πρόσθετα κλειδιά), τότε χρησιμοποιείται το κλειδί σύνδεσης.

Το *κλειδί συνδυασμού* (combination key) παράγεται κατά τη διάρκεια της διαδικασίας αρχικοποίησης εάν οι συσκευές έχουν αποφασίσει να επικοινωνήσουνε. Παράγεται και από τις δύο συσκευές συγχρόνως. Κατ' αρχάς, και οι δύο μονάδες παράγουν έναν τυχαίο αριθμό. Με τον αλγόριθμο E21 παραγωγής κλειδιού, και οι δύο συσκευές παράγουν ένα κλειδί, συνδυάζοντας τον τυχαίο αριθμό και τις διευθύνσεις συσκευών Bluetooth. Μετά από αυτό, οι συσκευές ανταλλάσσουν τους τυχαίους αριθμούς και υπολογίζουν το κλειδί συνδυασμού για να το χρησιμοποιήσουν μεταξύ τους.

Το *κύριο κλειδί* (master key) είναι το μόνο προσωρινό κλειδί από τα κλειδιά σύνδεσης που περιγράφονται παραπάνω. Παράγεται από την κύρια συσκευή χρησιμοποιώντας τον αλγόριθμο E22 παραγωγής κλειδιού με δύο τυχαίους αριθμούς των 128bit. Καθώς όλα τα κλειδιά σύνδεσης έχουνε μήκος 128 bit, η παραγωγή του E22 αλγορίθμου είναι επίσης 128bit. Ο λόγος για τη χρησιμοποίηση του αλγορίθμου παραγωγής κλειδιού στην πρώτη φάση είναι απλά να βεβαιωθεί ότι ο προκύπτων τυχαίος αριθμός είναι τυχαίος. Ένας τρίτος τυχαίος αριθμός διαβιβάζεται έπειτα στον slave και με τον αλγόριθμο παραγωγής κλειδιού και το τρέχον κλειδί σύνδεσης, ένα τμήμα επικάλυψης (overlay) υπολογίζεται και από τον master και από το slave. Το νέο κλειδί σύνδεσης (το master key) στέλνεται έπειτα στον slave, δυαδικό ψηφίο (bitwise) XORed με τμήμα επικάλυψης (overlay). Με αυτό, ο slave μπορεί να υπολογίσει το master κλειδί. Αυτή η διαδικασία πρέπει να εκτελεσθεί με κάθε slave που ο master θέλει να χρησιμοποιήσει το κύριο κλειδί.



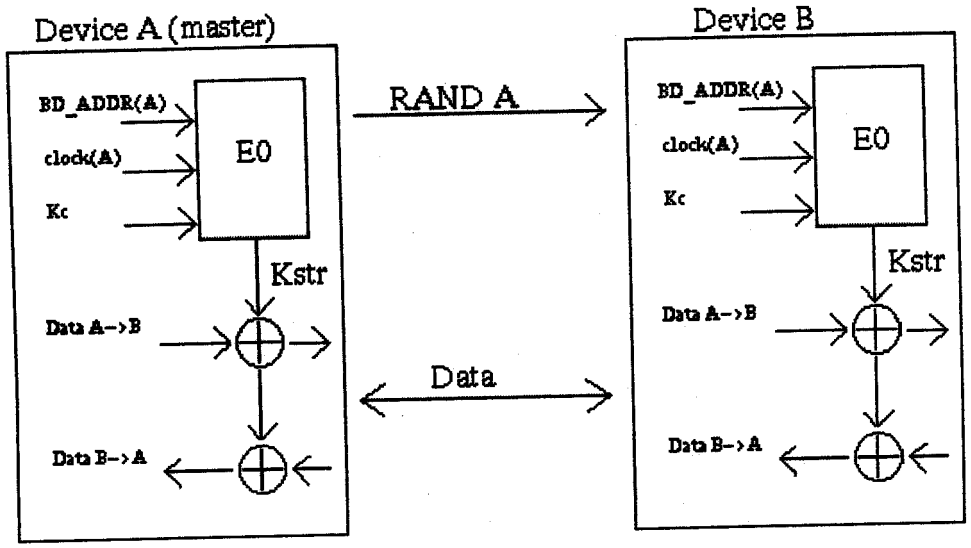
Σχήμα 4.14: Ο αλγόριθμος E3 παραγωγής κλειδιού για το κλειδί κρυπτογράφησης

Το κλειδί κρυπτογράφησης παράγεται από το τρέχον κλειδί σύνδεσης, ένας αριθμός μετατόπισης κρυπτογράφησης των 96bit (Ciphering Offset Number)(COF) και ένας τυχαίος αριθμός των 128 bit. Το COF είναι βασισμένο στον επικυρωμένο λογαριασμό μετατόπισης (Authenticated Ciphering Offset) (ACO), ο οποίος παράγεται κατά τη διάρκεια της διαδικασίας αυθεντικοποίησης. Όταν ο διαχειριστής σύνδεσης (Link Manager - LM) ενεργοποιεί την κρυπτογράφηση, παράγεται το κλειδί κρυπτογράφησης. Αλλάζει αυτόματα κάθε φορά που εισάγει η συσκευή Bluetooth τον τρόπο κρυπτογράφησης.

4.6 ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Το σύστημα κρυπτογράφησης Bluetooth κρυπτογραφεί τα ωφέλιμα φορτία των πακέτων. Αυτό γίνεται με ροή κρυπτογράφησης (stream cipher) E0, το οποίο είναι επανα-συγχρονισμένο για κάθε ωφέλιμο φορτίο (payload). Η ροή κρυπτογράφησης ΕΟ αποτελείται από τον μηχανισμό παραγωγής κλειδιού (generator) ωφέλιμων φορτίων, τον μηχανισμό παραγωγής ροής κλειδιού (stream generator key) και το τμήμα κρυπτογράφησης / αποκρυπτογράφησης. [10].

Ο μηχανισμός παραγωγής κλειδιού ωφέλιμου φορτίου συνδυάζει τα bit εισαγωγής σε μια κατάλληλη σειρά και τα μετατοπίζει στους τέσσερις γραμμικούς καταχωρητές μετατόπισης ανατροφοδότησης (Linear Feedback Shift Registers - LSFR) από το μηχανισμό παραγωγής ροής κλειδιού. Η ροή κλειδιού bits παράγεται με μια μέθοδο που προέρχεται από τον μηχανισμό παραγωγής κρυπτογράφησης ροής αθροίσματος (summation stream cipher generator) [15].



Σχήμα 4.15: Η επεξεργασίας κρυπτογράφησης

Υπάρχουν διαθέσιμοι διάφοροι τρόποι κρυπτογράφησης, αυτό εξαρτάται απ' το εάν μια συσκευή χρησιμοποιεί ένα ημιμόνιμο κλειδί σύνδεσης ή ένα κύριο κλειδί (master key). Εάν χρησιμοποιείται ένα κλειδί μονάδας (unit key) ή ένα κλειδί συνδυασμού, η κυκλοφορία αναμετάδοσης δεν κρυπτογραφείται. Η ατομική διευθυνσιοδοτούμενη μεταφορά μπορεί είτε να κρυπτογραφηθεί είτε όχι. Εάν χρησιμοποιείται ένα κύριο κλειδί, υπάρχουν τρεις πιθανοί τρόποι. Στην κρυπτογράφηση *mode 1*, τίποτα δεν κρυπτογραφείται. Στην κρυπτογράφηση *mode 2,* η κυκλοφορία αναμετάδοσης δεν κρυπτογραφείται, αλλά η ατομική διευθυνσιοδοτούμενη κυκλοφορία κρυπτογραφείται με το κύριο κλειδί. Και στην κρυπτογράφηση *mode 3*, όλη η κυκλοφορία κρυπτογραφείται με το κύριο κλειδί.

Δεδομένου ότι το μέγεθος του κλειδιού κρυπτογράφησης ποικίλλει από 8bit μέχρι 128bit, παρακάτω συζητείται το μέγεθος του κλειδιού κρυπτογράφησης που χρησιμοποιείται μεταξύ δύο συσκευών. Σε κάθε συσκευή, υπάρχει μια παράμετρος που καθορίζει το μέγιστο μήκος κλειδιού. Στο μέγεθος κλειδιού (key size) διαπραγμάτευσης, ο master στέλνει την πρότασή του για το μέγεθος κλειδιού κρυπτογράφησης στο slave. Ο slave μπορεί είτε να την δεχτεί και να την αναγνωρίσει, είτε να στείλει μια άλλη πρόταση. Αυτό συνεχίζεται, έως ότου επιτυγχάνεται μια συναίνεση ή μια από τις συσκευές σταματήσει τη διαπραγμάτευση. Το τέλος της διαπραγμάτευσης γίνεται από τη χρησιμοποιούμενη εφαρμογή. Σε κάθε εφαρμογή, καθορίζεται ένα ελάχιστο αποδεκτό μέγεθος κλειδιού, και εάν η απαίτηση δεν καλύπτεται από τον καθέναν που συμμετέχει, η εφαρμογή σταματά τη διαπραγμάτευση και η κρυπτογράφηση δεν μπορεί να χρησιμοποιηθεί. Αυτό είναι απαραίτητο για να αποφύγει την κατάσταση όπου μια κακόβουλη συσκευή κάνει την κρυπτογράφηση να είναι χαμηλής ποιότητας προκειμένου να γίνει κάποια διαρροή δεδομένων.

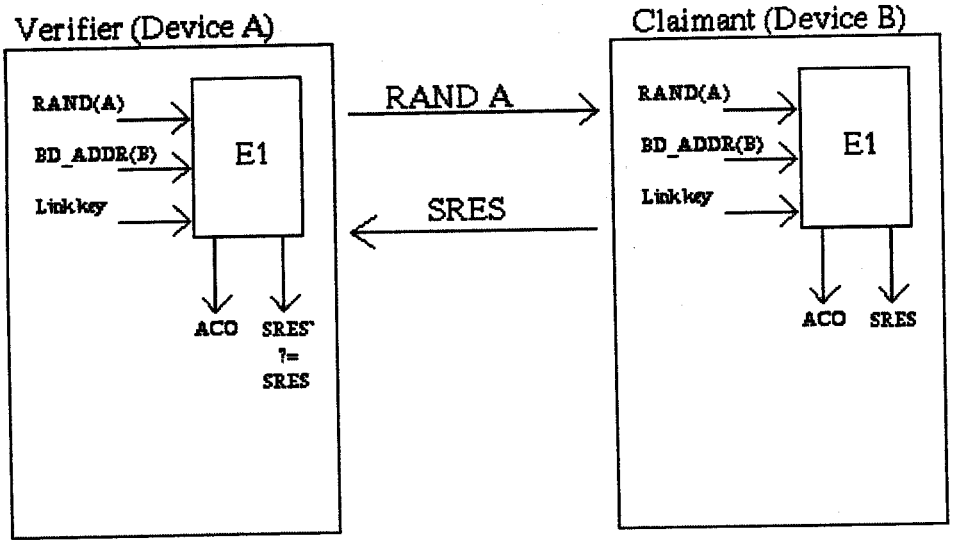
Ο αλγόριθμος κρυπτογράφησης χρησιμοποιεί τέσσερα LFSR με μήκος 25, 31, 33 και 39, με συνολικό μήκος 128. Η αρχική τιμή 128bit των τεσσάρων LFSRs προσδιορίζεται από την ροή του μηχανισμού παραγωγής κλειδιού χρησιμοποιώντας το κλειδί κρυπτογράφησης, ένας τυχαίος αριθμός των 128bit, η

διεύθυνση συσκευών Bluetooth της συσκευής και η τιμή 26bit του κύριου χρονιστή (master clock).

4.7 ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ [5]

Το σχέδιο αυθεντικοποίησης Bluetooth χρησιμοποιεί μια στρατηγική πρόκλησης-απάντησης, όπου ένα πρωτόκολλο 2-move χρησιμοποιείται για να ελέγξει εάν το άλλο συμβαλλόμενο μέρος γνωρίζει το μυστικό κλειδί. Το πρωτόκολλο χρησιμοποιεί συμμετρικά κλειδιά (symmetric keys), έτσι μια επιτυχής αυθεντικοποίηση είναι βασισμένη στο γεγονός ότι και οι δύο συμμετέχοντες μοιράζονται το ίδιο κλειδί. Ακολούθως, η (Authentication Cipher Offset) (ACO) υπολογίζεται και αποθηκεύεται και στις δύο συσκευές και χρησιμοποιείται για παραγωγή κλειδιού κρυπτογράφησης.

Κατ' αρχάς, ο αποστολέας (verifier) στέλνει στον παραλήπτη (claimant) έναν τυχαίο αριθμό που επικυρώνεται. Κατόπιν, και οι δύο συμμετέχοντες χρησιμοποιούν τη λειτουργία αυθεντικοποίησης (authentication) E1 με τον τυχαίο αριθμό, η διεύθυνση συσκευών παραλήπτη Bluetooth και το τρέχον κλειδί σύνδεσης παίρνει μια απάντηση. Ο παραλήπτης στέλνει την απάντηση στον αποστολέα, ο οποίος σιγουρεύεται έπειτα για την αντιστοιχία των απαντήσεων.



Σχήμα 4.16: Η επεξεργασία αυθεντικοποίησης

Η χρησιμοποιημένη εφαρμογή προσδιορίζει ποιος πρόκειται να αυθεντικοποιηθεί. Έτσι ο αποστολέας δεν μπορεί να είναι απαραιτήτως ο master. Μερικές από τις εφαρμογές απαιτούν μόνο έναν τρόπο αυθεντικοποίησης, έτσι ώστε μόνο ένα τμήμα να επικυρωθεί. Αυτό δεν είναι πάντα έτσι, θα μπορούσε να υπάρξει μια αμοιβαία αυθεντικοποίηση, όπου και τα δυο μέρη επικυρώνονται με τη σειρά.

Εάν η αυθεντικοποίηση αποτύχει, υπάρχει μια χρονική περίοδος που πρέπει να περάσει έως ότου μπορεί να γίνει μια νέα προσπάθεια αυθεντικοποίησης. Η χρονική περίοδος διπλασιάζεται για κάθε επόμενη αποτυχημένη προσπάθεια από την ίδια διεύθυνση, έως ότου επιτευχθεί ο μέγιστος χρόνος αναμονής. Ο χρόνος αναμονής μειώνεται εκθετικά σε ένα ελάχιστο όταν δεν γίνεται καμία αποτυχημένη προσπάθεια αυθεντικοποίησης κατά τη διάρκεια μιας χρονικής περιόδου.

4.8 ΚΑΤΑΝΕΜΗΜΕΝΑ ΣΥΣΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ

Σε αυτή την ενότητα εξετάζονται οι απειλές στα συστήματα ηλεκτρονικών υπολογιστών και έπειτα εξετάζεται η ασφάλεια των κατανεμημένων συστημάτων. Κυρίως επικεντρωνόμαστε στις πτυχές που διαφέρουν από τα παραδοσιακά συστήματα ασφάλειας υπολογιστών.

Οι απειλές στα συστήματα ηλεκτρονικών υπολογιστών, διαιρούνται σε τρεις τύπους:

- Ø απειλές κοινοποίησης (disclosure threats),
- Ø απειλές ακεραιότητας (integrity threats)
- Ø και οι απειλές άρνησης υπηρεσιών.

Αυτός ο διαχωρισμός δεν καλύπτει όλες τις πιθανές απειλές, αλλά αρκεί για την παρούσα εργασία. Η *απειλή κοινοποίησης* (disclosure threat) περιλαμβάνει τη διαρροή των πληροφοριών από το σύστημα σε ένα συμβαλλόμενο μέρος που δεν θα έπρεπε να έχει δει τις πληροφορίες και είναι μια απειλή ενάντια στην εμπιστευτικότητα των πληροφοριών. Η *απειλή ακεραιότητας* περιλαμβάνει μια ανεξουσιοδοτημένη (unauthorized) αλλαγή πληροφοριών. Η *απειλή άρνησης των υπηρεσιών* περιλαμβάνει την παρεμπόδιση της πρόσβασης στους πόρους συστημάτων από έναν κακόβουλο επιτιθέμενο (attacker). Είναι μια απειλή ενάντια στη διαθεσιμότητα του συστήματος.[1] Η αυθεντικοποίηση σημαίνει την εξασφάλιση της ταυτότητας ενός άλλου χρήστη, έτσι ώστε να ξέρει με ποιόν επικοινωνεί

Στα κατανεμημένα συστήματα, τα αντικείμενα βρίσκονται σε διαφορετικές θέσεις. Αυτό καθιστά δυσκολότερα τα ζητήματα ασφάλειας. Για παράδειγμα, σε ένα κατανεμημένο σύστημα, η αυθεντικοποίηση χρηστών είναι δυσκολότερη. Εάν η αυθεντικοποίηση γίνεται με κωδικούς πρόσβασης (passwords), η σύνδεση πραγματοποιείται με το μηχανισμό αυθεντικοποίησης .

Εάν η σύνδεση δεν είναι ασφαλής, γεγονός που είναι σπάνιο, πρέπει να εξασφαλιστεί ότι κανένας και με κανέναν τρόπο δεν μπορεί να πάρει τον κωδικό πρόσβασης. Αυτό είναι το σημαντικότερο σημείο. Σε ένα κατανεμημένο σύστημα, υπάρχουν συνήθως διάφορα ενδιαφερόμενα μέρη. Μπορεί να μην υπάρξει μια σαφής συναίνεση στη χρήση πολιτικής ασφάλειας. Εάν οι διαφορετικοί συμμετέχοντες επιβάλλουν διαφορετικά είδη πολιτικών ασφάλειας, η συνεργασία είναι αδύνατη.

Ένα άλλο θέμα είναι μια διαδικασία που ονομάζεται εξουσιοδότηση (delegation). Όταν ένας χρήστης χρησιμοποιεί μια τοπική πρόσβαση στη σύνδεση σε ένα δίκτυο και θέλει να εκτελέσει ένα πρόγραμμα για μια απομακρυσμένη συσκευή, προκύπτουν μερικά προβλήματα. Το πρόγραμμα θα χρειαστεί ορισμένα δικαιώματα για να χρησιμοποιηθούν οι πόροι της απομακρυσμένης συσκευής. Κατόπιν οι εκπρόσωποι των χρηστών έχουνε σωστή πρόσβαση στα δικαιώματα του προγράμματος, έτσι ώστε μπορεί να συνεχιστεί η επικοινωνία με την

απομακρυσμένη συσκευή. Το πρόβλημα σε αυτή τη περίπτωση είναι ότι οι χρήστες έχουν πολύ λίγο έλεγχο της απομακρυσμένης συσκευής, όμως πρέπει να εξουσιοδοτήσουν τα δικαιώματά τους σε ένα πρόγραμμα που τρέχει στις συσκευές αυτές. Στα κατανεμημένα συστήματα, υπάρχει πάντα η απειλή ότι η απομακρυσμένη συσκευή δεν είναι καλά προστατευμένη και ένας κακόβουλος χρήστης μπορεί να εκμεταλλευτεί τα δικαιώματα του χρήστη.

Ένας άλλος τομέας που έχει πρόβλημα στην ασφάλεια των κατανεμημένων συστημάτων είναι η αυθεντικοποίηση. Η απόφαση που πρέπει να ληφθεί είναι εάν η ασφάλεια πρέπει να επιβληθεί κεντρικά ή τοπικά. Στη συγκεντρωμένη απειλή ασφάλειας, θα μπορούσε να υπάρξει κάποιο Κέντρο Διανομής Κλειδιών (Key Distribution Center - KDC), όπου θα αποθηκεύονται τα κλειδιά όλων των συσκευών. Το KDC ενεργεί ως Έμπιστη Τρίτη Οντότητα (TTP) όπου οι χρήστες μπορούν να χρησιμοποιήσουν την αυθεντικοποίηση με άλλους χρήστες, ώστε να έχει ασφάλεια σύνδεσης όλο το δίκτυο. Υπάρχουν διάφοροι τρόποι που μπορεί να συμβεί αυτό, για παράδειγμα, η αυθεντικοποίηση του Kerberos και το πρωτόκολλο ανταλλαγής κλειδιού [15]. Το μεγαλύτερο πρόβλημα σε αυτό είναι η μη αξιοπιστία της Έμπιστης Τρίτης Οντότητας.

Από την άλλη πλευρά, εάν αποφασιστεί ότι το σχέδιο επιβολής ασφάλειας πρόκειται να είναι τοπικό, απαιτούνται άλλα είδη μέτρων ασφάλειας. Κάθε χρήστης επιβάλλει την δική του πολιτική ασφάλειάς και εμπιστεύεται τις συσκευές που συνδέεται. Θα μπορούσε να υπάρξει μια Αρχή Πιστοποίησης (Certification Authority - CA), η οποία εκδίδει τα δημόσια κλειδιά και ένα Κέντρο Διανομής Πιστοποίησης (Certification Distribution Center - CDC), το οποίο αποθηκεύει όλα τα πιστοποιητικά που εκδίδονται από την Αρχή Πιστοποίησης. Οι χρήστες έχουν ζεύγη κλειδιών και μπορούν να πιστοποιήσουν τα δημόσια κλειδιά τους με την Αρχή Πιστοποίησης. Κατόπιν, εάν ένας χρήστης χρησιμοποιεί το κλειδί του για να υπογράψει κάτι, η υπογραφή μπορεί να ελεγχθεί για να αντιστοιχηθεί με ένα δημόσιο κλειδί. Το δημόσιο κλειδί μπορεί στη συνέχεια να ελεγχθεί με το Κέντρο Διανομής Πιστοποίησης ώστε να πιστοποιηθεί ότι το δημόσιο κλειδί ανήκει πραγματικά στο χρήστη που έκανε αρχικά την υπογραφή. Κατ' αυτό τον τρόπο, μπορούμε να επιβάλουμε την τοπική ασφάλεια και να έχουμε ακόμα την αυθεντικοποίηση του συστήματος με το Public Key Infrastructure (PKI).

ΚΕΦΑΛΑΙΟ 5

ΑΣΦΑΛΕΙΑ ΣΕ ΔΙΚΤΥΑ AD HOC

Σε αυτό το κεφάλαιο, παρουσιάζονται οι διαφοροποιήσεις ασφάλειας στα ad hoc δίκτυα σχετικά με την ασφάλεια στα παλαιά κατανεμημένα συστήματα. Κατ' αρχάς, εξετάζονται τα χαρακτηριστικά των ad hoc δικτύων και στη συνέχεια τα προβλήματα ασφάλειας.

Η ad hoc λειτουργία, η οποία επίσης λέγεται και λειτουργία peer – to peer είναι απλά ένα σύνολο από σταθμούς που επικοινωνούν μεταξύ τους κατευθείαν χωρίς την χρήση σημείων πρόσβασης ή οποιαδήποτε σύνδεση με το καλωδιωμένο δίκτυο. Αυτός ο τρόπος λειτουργίας είναι χρήσιμος για την γρήγορη και εύκολη εγκατάσταση ενός ασύρματου δικτύου οπουδήποτε δεν υπάρχει καλωδιακή υποδομή ή δεν απαιτείται η χρήση των παραπάνω υπηρεσιών για παράδειγμα σε ένα συνεδριακό κέντρο, σε δωμάτια ξενοδοχείου, αεροδρόμια, ή όπου η πρόσβαση στο δίκτυο δεν επιτρέπεται.

Ενώ όταν δεν υπάρχει ad hoc σύνδεση, το ασύρματο δίκτυο αποτελείται από τουλάχιστον 1 σημείο πρόσβασης το οποίο συνδέεται με το καλωδιωμένο δίκτυο και ένα σύνολο από ασύρματους σταθμούς.

Στα ad hoc δίκτυα, δεν υπάρχει καμία σταθερή υποδομή. Τα δίκτυα είναι διαμορφωμένα on-the-fly, δηλαδή αυτόματα. Όλες οι συσκευές σε ένα ad hoc δίκτυο συνδέονται η μια με την άλλη μέσω ασύρματων συνδέσεων. Οι μεμονωμένες συσκευές ενεργούν ως δρομολογητές κατά την αναμετάδοση μηνυμάτων σε άλλες συσκευές, οι οποίες είναι πάρα πολύ μακριά εκτός από το να στέλνουν και λαμβάνουν το μήνυμα άμεσα. Η τοπολογία ενός ad hoc δικτύου δεν καθορίζεται. Αλλάζει όλη την ώρα όταν κινούνται αυτές οι κινητές συσκευές μέσα και έξω από την εμβέλεια μετάδοσης άλλων συσκευών. Όλο αυτό καθιστά τα ad hoc δίκτυα πολύ τρωτά στις επιθέσεις και τα θέματα ασφάλειας πολύ περίπλοκα.

5.1 ΔΙΑΘΕΣΙΜΟΤΗΤΑ

Στα ad hoc δίκτυα, η εξασφάλιση της διαθεσιμότητας είναι ίσως σημαντικότερη από την παραδοσιακή ασφάλεια. Όπως όλες οι συσκευές στο δίκτυο εξαρτώνται η μια από την άλλη για να αναμεταδώσουνε τα μηνύματα, οι επιθέσεις άρνησης των υπηρεσιών είναι εύκολο να εκτελεσθούν. Και πάλι, καθώς όλες οι πληροφορίες μεταφέρονται μέσω του αέρα, η επίθεση της άρνησης των υπηρεσιών γίνεται ακόμη μεγαλύτερη. Για παράδειγμα, ένας κακόβουλος χρήστης θα μπορούσε να

προσπαθήσει να παρεμβάλει παράσιτα (jam) ή να προσπαθήσει να παρέμβει στην ροή των πληροφοριών μέσω αέρος. Έτσι το πρωτόκολλο δρομολόγησης που χρησιμοποιήθηκε στο δίκτυο θα μπορούσε να διαταραχθεί με τις ανακριβείς πληροφορίες. [17]

Τα πιο τρωτά σημεία στα ad hoc δίκτυα είναι τα πρωτόκολλα δρομολόγησης. Η δρομολόγηση των πρωτοκόλλων πρέπει να είναι σε θέση να χειριστεί και τη μεταβαλλόμενη τοπολογία του δικτύου και τις επιθέσεις από τους κακόβουλους χρήστες. Υπάρχουν πρωτόκολλα δρομολόγησης που μπορούν να προσαρμοστούν στη μεταβαλλόμενη τοπολογία [17].

Ένα άλλο τρωτό σημείο, που δεν υπάρχει στα παραδοσιακά δίκτυα, είναι η μπαταρία της συσκευής στο ad hoc δίκτυο. Κανονικά, αυτές οι συσκευές προσπαθούν να αποθηκεύσουν ενέργεια με χρήση μπαταρίας, έτσι ώστε όταν η συσκευή δεν είναι σε ενεργή χρήση, να μην καταναλώνεται ενέργεια. Με τις επιθέσεις εξάντλησης μπαταριών, ένας κακόβουλος χρήστης μπορεί να καταναλώσει περισσότερη ενέργεια από την μπαταρία μιας συσκευής, έτσι ώστε τελικά η ισχύς της μπαταρίας να εξαντληθεί νωρίτερα [16]

5.2 ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΚΑΙ ΚΛΕΙΔΙ ΔΙΑΧΕΙΡΙΣΗΣ

Η εξουσιοδότηση είναι ένα άλλο δύσκολο θέμα στα ad hoc δίκτυα. Δεδομένου ότι υπάρχει πολύ ελάχιστη ή καθόλου υποδομή, ο προσδιορισμός των χρηστών (π.χ. οι συμμετέχοντες σε ένα ad hoc δίκτυο σε μια αίθουσα συνεδριάσεων) δεν είναι εύκολος. Υπάρχουν προβλήματα με την Έμπιστη Τρίτη Οντότητα και μηχανισμοί βασισμένοι στην ταυτότητα του κλειδιού συμφωνίας. [4]

Ωστόσο, είναι δυνατό να κατασκευαστούν πολύ καλοί μηχανισμοί αυθεντικοποίησης για τα ad hoc δίκτυα. Πάλι, ένα γενικό πρωτόκολλο για αυθεντικοποίηση του κωδικού πρόσβασης (password) περιγράφεται με το κλειδί ανταλλαγής .Έχει διάφορα μειονεκτήματα και όχι καλή ακολουθία για τις ad hoc συσκευές δικτύωσης (με ίσως μικρότερες CPUs από τους κανονικούς υπολογιστές γραφείου). Έτσι παρουσιάζεται η αυθεντικοποίηση του password με το παρακάτω κρυπτογραφικό πρωτόκολλο: το σύστημα ανταλλαγής μυστικού κλειδιού Diffie-Hellman, το οποίο φαίνεται να αποφεύγει τα προβλήματα του γενικού πρωτοκόλλου που προαναφέραμε παραπάνω. [4]

5.3 ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ ΚΑΙ ΑΚΕΡΑΙΟΤΗΤΑ

Η εμπιστευτικότητα, επίσης, είναι ένα πολύ τρωτό σημείο στα ad hoc δίκτυα. Με την ασύρματη επικοινωνία, καθένας μπορεί να εισβάλει στα μηνύματα που στέλνονται μέσω αέρα και χωρίς την κατάλληλη κρυπτογράφηση, όλες οι πληροφορίες μπορούν να είναι διαθέσιμες στον καθένα. Αφ' ετέρου, χωρίς κατάλληλη εξουσιοδότηση, δεν υπάρχει κανένας λόγος να αναφερθούμε στην εμπιστευτικότητα.

Τα ίδια πράγματα ισχύουν και για την ακεραιότητα,. Εκτός από τις κακόβουλες επιθέσεις, η ακεραιότητα μπορεί να συμβιβαστεί λόγω της ράδιο παρεμβολής, έτσι καθορίζονται σίγουρα μερικά είδη προστασίας της ακεραιότητας.

ΚΕΦΑΛΑΙΟ 6

ΑΔΥΝΑΜΙΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ BLUETOOTH

6.1 ΓΕΝΙΚΑ

Σε αυτό το κεφάλαιο περιγράφονται τρεις τύποι ενδεχόμενων επιθέσεων που αντιμετωπίζουν τα πρότυπα Bluetooth.

Η *πρώτη* προσβολή του συστήματος από μια επίθεση, συμβαίνει όταν ένας αντίπαλος (adversary) υπό ορισμένες συνθήκες είναι σε θέση να βρει το κλειδί που ανταλλάσσεται από δύο *συσκευές «θύματα»* (victim devices:δηλαδή η συσκευή η οποία δέχεται την επίθεση). Όταν ο επιτιθέμενος καταφέρει να προσδιορίσει το κλειδί μπορεί να υποκλέψει (eavesdropping) δεδομένα και πιθανόν να παριστάνει ότι είναι κάποια άλλη συσκευή. Αυτό μπορεί να γίνει είτε με συνεχή αναζήτηση του PIN (αλλά χωρίς αλληλεπίδραση με τις συσκευές οι οποίες δέχονται την επίθεση), είτε με την εφαρμογή που ονομάζεται επίθεση μέσου - χρήστη (middle-person).

Η δεύτερη προσβολή του συστήματος από μια επίθεση ονομάζεται *επίθεση τοποθεσίας (location).* Στην επίθεση αυτού του τύπου ένας επιτιθέμενος είναι σε θέση να προσδιορίσει και να καθορίσει τη γεωγραφική θέση των συσκευών οι οποίες δέχονται την επίθεση. Αυτό, στη συνέχεια, μπορεί να χρησιμοποιηθεί για βιομηχανική κατασκοπεία (industrial espionage), να εκβιάσει (blackmail), και να εκτελέσει άλλες ανεπιθύμητες δραστηριότητες.

Η τρίτη προσβολή αφορά την κρυπτογράφηση (cipher). Υπάρχουν δύο επιθέσεις πάνω στην κρυπτογράφηση.

6.2 ΑΝΑΛΥΣΗ ΑΔΥΝΑΜΙΑΣ BLUETOOTH

Κατά συνέπεια, η προσεκτική ανάλυση των αδυναμιών του προτύπου Bluetooth και ο καλός σχεδιασμός είναι ζωτικής σημασίας στην επιτυχία των προϊόντων. Επίσης προτείνονται κάποια περιορισμένα μέτρα για την επιτυχία των ήδη γνωστών τύπων επιθέσεων. Αυτά τα μέτρα είναι εύκολα να εκτελεστούν άλλα στο λογισμικό επίπεδο της εφαρμογής και άλλα στο υλικό μέρος (hardware).

Στον πρώτο τύπο επίθεσης, ένας αντίπαλος (adversary) μπορεί να κλέψει τα κλειδιά μονάδας (unit key), τα κλειδιά σύνδεσης και τα κλειδιά κρυπτογράφησης από

τις συσκευές οι οποίες δέχονται την επίθεσή του. Αυτό, στη συνέχεια, επιτρέπει στον αντίπαλο να προσωποποιήσει τα συμβαλλόμενα μέρη και να υποκλέψει (eavesdrop) την κρυπτογραφημένη επικοινωνία. Αυτό μπορεί να γίνει είτε με συνεχή αναζήτηση του PIN, είτε με το να τοποθετήσει έναν ενδιάμεσο χρήστη (middle person). Οι επιθέσεις αυτές μπορούν να αποτραπούν είτε με τη βοήθεια ενός αρκετά μεγάλου PIN (μεγαλύτερος απο 64 bit) είτε με τη βοήθεια του μηχανισμού δημόσιων κλειδιών στο στρώμα εφαρμογής.

Στο δεύτερο τύπο επίθεσης, ο επιτιθέμενος μπορεί να χαρτογραφήσει περίπου τα φυσικά χαρακτηριστικά των χρηστών που χρησιμοποιούν οι συσκευές Bluetooth με ανίχνευση των συσκευών αυτών στις τοποθεσίες που τον ενδιαφέρουνε.

Προκειμένου να παραχθούν χρήσιμες πληροφορίες από έναν επιτιθέμενο μπορεί να τοποθετήσει συσκευές υποκλοπής σε επιλεγμένες θέσεις, όπως στα αεροδρόμια επιτρέποντάς του να καθορίσει αυτόματα ποιοι άνθρωποι ταξιδεύουν. Οι λαμβανόμενες πληροφορίες θα μπορούσαν να συσχετιστούν με την ταυτότητα των χρηστών από πληροφορίες που μπορεί να έχουν ληφθεί κατά τη διάρκεια μιας συναλλαγής πιστωτικών καρτών μέσω συσκευών Bluetooth.

Τέλος, *ο τρίτος τύπος επίθεσής* αφορά ένα κρυπτογραφημένο κείμενο [1]. Ένας επιτιθέμενος μπορεί να σπάσει την ασφάλεια του κρυπτογραφημένου κειμένου που απαιτεί 2^{100} bit λειτουργίες [12].

6.3 ΕΠΙΘΕΣΕΙΣ

6.3.1 Υποκλοπή (eavesdropping) και bit αλλαγής

Άλλη κοινή επίθεση επικοινωνίας είναι η *υποκλοπή* και το *bit αλλαγής*. Η υποκλοπή συμβαίνει όταν ένας επιτιθέμενος χρησιμοποιεί έναν ανιχνευτή για να λάβει την συχνότητα αυτού που τον έχει καλέσει. Με τον ανιχνευτή, εάν η κλήση δεν είναι κρυπτογραφημένη, ο επιτιθέμενος έχει τη γνώση της συνομιλίας.

Με το bit αλλαγής, ο επιτιθέμενος χρησιμοποιεί έναν περιπλέκτη (scrambler) για να μπερδέψει το σήμα που έρχεται μεταξύ του χρήστη και του δικτύου. Αυτή η μέθοδος δεν παρέχει οποιεσδήποτε νέες πληροφορίες στον επιτιθέμενο αλλά ο χρήστης δεν θα είναι σε θέση να επικοινωνήσει. Το bit αλλαγής είναι απίθανο να χρησιμοποιηθεί στην μεταπήδηση συχνότητας.

Το κλειδί αρχικοποίησης υπολογίζεται ως λειτουργία του PIN, ενός τυχαίου αριθμού και της διεύθυνσης συσκευής Bluetooth[8]. Εάν δεν είναι διαθέσιμο κανένα PIN (σ' αυτή την περίπτωση θεωρείται ότι έχει τιμή μηδέν), τότε το PIN μπορεί να γίνει γνωστό στον επιτιθέμενο. Εάν το PIN επικοινωνεί εκτός ζώνης (π.χ., που εισάγεται σε κάθε συσκευή από το χρήστη) τότε ο επιτιθέμενος μπορεί να μάθει με εξαντλητική αναζήτηση όλων των πιθανών PINs, εάν χρησιμοποιούνται εύκολα ή όχι αρκετά μεγάλα PINs . Αυτό μπορεί να γίνει ως εξής:

Offline PIN crunching. Αρχικά εξετάζεται η εκδοχή όπου ο επιτιθέμενος κάνει υποκλοπή σε δύο συσκευές και προσπαθεί να καθορίσει ποιο κλειδί χρησιμοποιούν. Κατόπιν ο επιτιθέμενος αρχίζει τη διαδικασία ανταλλαγής με μια συσκευή η οποία δέχεται την επίθεση, έπειτα καθορίζονται ποια PIN χρησιμοποίησε αυτή η συσκευή, και έτσι προσδιορίζεται ένα κλειδί για τη συσκευή η οποία δέχεται την επίθεση βασισμένη σε αυτό το κλεμμένο PIN.

1. **περίπτωση I***:* **Υποκλοπή (eavesdropping).** Ο επιτιθέμενος υποθέτει εξαντλητικά όλα τα PINs μέχρι ένα ορισμένο μήκος. Ο αντίπαλος ελέγχει

την ορθότητα του PIN με εκτέλεση επαλήθευσης του κλειδιού αρχικοποίησης πρωτοκόλλου[8]. Εάν το αποτέλεσμα είναι σωστό τότε το κλειδί έχει προσδιοριστεί σωστά. Σημειώνουμε ότι ο αντίπαλος είναι παθητικός και ότι λαμβάνει μόνο και δεν μεταφέρει.

2. **περίπτωση II*:* Κλοπή συμμετοχής (stealing by participation)**. Ο επιτιθέμενος εισάγει το PIN που έχει μαντέψει, και εκτελεί το πρώτο βήμα του πρωτοκόλλου για την καθιέρωση του κλειδιού αρχικοποίησης. Εκτελεί έπειτα το δεύτερο βήμα με τη συσκευή η οποία δέχεται την επίθεση. Ο επιτιθέμενος είναι το συμβαλλόμενο μέρος που αρχίζει την πρώτη αποστολή απόκρισης πρωτοκόλλου. Η απόκριση επαλήθευσης στην έξοδο θα είναι σωστή (correct) εάν και μόνο εάν δεν εξαπατήσει την συσκευή η οποία δέχεται την επίθεση, και ο επιτιθέμενος έχει υποθέσει το σωστό PIN. (ένα πρωτόκολλο πρόκλησης-απάντησης είναι στην έξοδο "correct" εάν και μόνο εάν ένα δεδομένο κλειδί αρχικοποίησης συμφωνεί με το PIN και τις σταλμένες τυχαίες στοιχειοσειρές (strings). Αφού λάβει το αντίγραφο πρόκλησης-απάντησης από αυτόν που δέχτηκε την επίθεση (victim), ο επιτιθέμενος (attacker) υπολογίζει το αντίστοιχο κλειδί αρχικοποίησης για κάθε PIN που επιθυμεί να ελέγχει και έπειτα τρέχει τον αλγόριθμο επαλήθευσης στο υπολογισμένο κλειδί αρχικοποίησης και λαμβάνει αντίγραφο πρόκλησης-απάντησης. Εάν ο αλγόριθμος επαλήθευσης βγάλει στην έξοδο "incorrect", τότε ο επιτιθέμενος εκτελεί τον υπολογισμό επαλήθευσης στα κλειδιά που αντιστοιχούν στο επόμενο PIN που επιθυμεί να ελέγξει. Αυτό επαναλαμβάνεται έως ότου τα αποτελέσματα αλγορίθμου επαλήθευσης στην έξοδο να βγάλουνε 'correct', όταν ο επιτιθέμενος έχει βρει το PIN χρησιμοποιώντας το στη συσκευή η οποία δέχεται την επίθεση. Συνεχίζει έπειτα τον καθορισμό του κλειδιού του πρωτοκόλλου πριν χρησιμοποιήσει το κλειδί που βρέθηκε.

Εκτελείται offline επίθεση μόλις ο επιτιθέμενος λάβει ένα ζευγάρι πρόκλησης-απάντησης. Επομένως, η back-off μέθοδο που υιοθετείται για να αποφύγει τον προσδιορισμό του PIN δεν προσθέτει οποιαδήποτε ασφάλεια. Στην πραγματικότητα, ο εκθέτης back-off δίνει στον επιτιθέμενο επιπλέον χρόνο να ψάξει εξαντλητικά για PINs.

Κατά συνέπεια, ο επιτιθέμενος μπορεί να μάθει το συμμετρικό κλειδί αρχικοποίησης. Δεδομένου ότι η ασφάλεια των επόμενων βημάτων του κλειδιού εγκατάστασης στηρίζεται στη μυστικότητα (secrecy) του κλειδιού αρχικοποίησης [8], ο επιτιθέμενος μπορεί να αποκρυπτογραφήσει την επικοινωνία σε αυτήν την φάση εάν ξέρει το κλειδί αρχικοποίησης. Εάν ο επιτιθέμενος λάβει το κλειδί αρχικοποίησης, αυτός θα λάβει επίσης το κλειδί σύνδεσης. Επιπλέον, δεδομένου ότι τα κλειδιά κρυπτογράφησης υπολογίζονται από τα κλειδιά σύνδεσης [8], θα είναι σε θέση να τα λάβει.

Ενώ η παραπάνω επίθεση εξάγει τα κλειδιά σύνδεσης και κρυπτογράφησης, είναι επίσης δυνατό για έναν επιτιθέμενο να λάβει το κλειδί μονάδας μιας συσκευής (και μετά μπορεί να προσωποποιηθεί η συσκευή, και να λάβει τα προκύπτοντα κλειδιά σύνδεσης.) Δηλαδή, εάν μια συσκευή έχει περιορίσει τους πόρους μνήμης, θα ζητήσει τη χρήση του πρώτου κλειδιού πρωτοκόλλου εγκαθίδρυσης, στο οποίο το κλειδί μονάδας χρησιμοποιείται ως κλειδί σύνδεσης. Συνεπώς, ένας επιτιθέμενος θα είναι σε θέση να λάβει τα κλειδιά μονάδας απλά με την έναρξη της επικοινωνίας με μια τέτοια συσκευή και με ποιο κλειδί προτείνει αυτή η συσκευή.

Είναι επίσης δυνατό ένας επιτιθέμενος να λάβει αυτό το κλειδί μόνο με υποκλοπή. Αφού πρώτα, λάβει το κλειδί αρχικοποίησης όπως παραπάνω, μόνο με υποκλοπή, μπορεί έπειτα να λάβει το κλειδί μονάδας.

Εξετάζεται μια άλλη επίθεση, στην οποία ένας επιτιθέμενος να έχει λάβει ήδη το κλειδί σύνδεσης που χρησιμοποιήθηκε από δύο συσκευές, και όπου αυτές οι συσκευές έχουν πραγματοποιήσει επικοινωνία. Ο επιτιθέμενός έρχεται σε επαφή με καθεμία από αυτές και οργανώνει δύο νέα κλειδιά σύνδεσης. Αυτό είναι επομένως μια επίθεση ενδιάμεσου χρήστη [7]. Οι δύο συσκευές θεωρούν ότι επικοινωνούν η μια με την άλλη, και ότι η άλλη συσκευή άρχισε την επικοινωνία. Ο επιτιθέμενος μπορεί για παράδειγμα να κάνει και τις δυο συσκευές slave, ή και τις δύο master.

Οι συσκευές οι οποίες δέχονται την επίθεση θα ακολουθήσουν διαφορετικές ακολουθίες μεταπήδησης (hop), δεδομένου ότι μια συσκευή θα ακολουθήσει την σειρά μεταπήδησης (hop sequence) βασισμένη στην ταυτότητα της συσκευής η οποία θεωρεί ότι είναι ο master piconet. Επομένως, δεν θα δουν τα μηνύματα που μεταφέρουν ο ένας στον άλλο (δεδομένου ότι ακούνε και μεταφέρουνε κατά τρόπο μη συγχρονισμένο) αλλά ο επιτιθέμενος επιλέγει μόνο τα μηνύματα που θα στείλει. Συνεπώς, ο επιτιθέμενος είναι σε θέση να προσωποποιήσει τις δύο συσκευές.

6.3.2 Επιθέσεις τοποθεσίας

Εάν μια συσκευή βρίσκεται σε κατάσταση αναζήτησης τότε αυτή θα αποκριθεί στην έρευνα εκτός αν κάποια άλλη δραστηριότητα βασικής ζωνης (baseband) το απαγορεύει [8].(για να εντοπιστούν μεταξύ τους, δύο ή περισσότερες συσκευές ανιχνεύουνε τις συχνότητες σε μερικές ψευδοτυχαίες εντολές, και με διαφορετικές σχετικές ταχύτητες, προκαλούνε τις slave να ανιχνεύσουνε τελικά το σήμα του master και αποκρίνονται με τις αντίστοιχες ταυτότητές τους). Καθιερώνουν έπειτα μια ακολουθία μεταπήδησης συχνότητας (frequency hopping), η οποία είναι μια ψευδοτυχαία ακολουθία.

Σε μια αναζήτηση, ο slave διαβιβάζει την ταυτότητά του στη βασική ζώνη. Επομένως, ένας επιτιθέμενος μπορεί να καθορίσει τη θέση και τις μετακινήσεις των συσκευών οι οποίες δέχονται την επίθεση με τη διατήρηση των γεωγραφικά διανεμημένων συσκευών που ερευνούν συνεχώς όλες τις συσκευές που εισάγονται μέσα στην εμβέλεια τους, και καταγράφουν τις ταυτότητες δίνοντας απαντήσεις. Δεδομένου ότι οι συσκευές θα χρησιμοποιήσουν τις ίδιες ταυτότητες όλη την ώρα [8] αυτό επιτρέπει στον επιτιθέμενο να καθορίσει τις μετακινήσεις τους. Λαμβάνοντας υπόψη τις πληροφορίες συγχρονισμού, ο επιτιθέμενος μπορεί αρκετά απλά να πιστοποιήσει ποιες συσκευές ταξιδεύουν μαζί για μακρύτερες χρονικές περιόδους, ή συναντιούνται επανειλημμένα.

Ομοίως, ο επιτιθέμενος (με τη βοήθεια των ιστοσελίδων) είναι σε θέση να προτρέψει τη συσκευή η οποία δέχεται την επίθεση να ανιχνεύσει τις συσκευές συνδέοντας τες, αναγκάζοντας έτσι τη συσκευή η οποία δέχεται την επίθεση να αποκαλύψει την ταυτότητά της σε αυτές τις συσκευές. Εάν υποθέσουμε ότι ο αντίπαλος έχει τον έλεγχο της συσκευής η οποία δέχεται την επίθεση, δεν έχει σημασία ποιον τύπο (mode) θα ακολουθήσει, δεδομένου ότι αυτό είναι ικανό για μεταγωγή από το στρώμα εφαρμογής.

Επίσης ανεξάρτητα εάν μια συσκευή είναι σε κατάσταση αναζήτησης ή όχι, ένας επιτιθέμενος που κάνει υποκλοπή στη βασική ζώνη μπορεί να καθορίσει το CAC που συνδέεται με κάθε μήνυμα που παρεμποδίζει. Δεδομένου ότι το CAC

υπολογίζεται από τη μοναδική διεύθυνση συσκευών Bluetooth της κύριας μονάδας μπορεί έπειτα να συντάξει ευρετήριο σ'αυτούς που δέχονται την επίθεση από CACs τους. Εναλλακτικά, μπορεί να καθορίσει τη σχέση μεταξύ των προσδιοριστικών συσκευών και των CACs χρησιμοποιώντας μια βάση δεδομένων των προϋπολογισμένων σχέσεων.

Σημειώνουμε ότι διάφορες συσκευές θα χαρτογραφηθούν στο ίδιο CAC, δεδομένου ότι το CAC υπολογίζεται από 24 έως 32bit διεύθυνσης συσκευών Bluetooth του master. Ωστόσο, αυτό δεν είναι μεγάλος πρακτικός περιορισμός στον επιτιθέμενο, δεδομένου ότι οι συγκρούσεις μεταξύ δύο τυχαίων επιλεγμένων συσκευών εμφανίζονται μόνο με την πιθανότητα μια στα δέκα έξι εκατομμύρια, που είναι πολύ απίθανο.

6.3.3 Μεταπήδηση κατά μήκος (hopping along)

Ο αντίπαλος για να είναι σε θέση να παρακολουθήσει μια συνομιλία μέσα σε ένα piconet, πρέπει είτε να ανιχνεύσει όλες τις ζώνες (bands) είτε να ακολουθήσει τις συχνότητες στις οποίες επικοινωνούν η master και η slave.

Στις ΗΠΑ και τις περισσότερες άλλες χώρες έχουν οριστεί 79 ζώνες προς χρήση από τις συσκευές Bluetooth, ενώ στην Ισπανία και στην Γαλλία μόνο 23 ζώνες. Προκειμένου να ακολουθηθεί η επικοινωνία που χρησιμοποιεί μια απλή συσκευή Bluetooth, ο επιτιθέμενος πρέπει να πιστοποιήσει ποιος seed χρησιμοποιείται για την ακολουθία ψευδοτυχαίας μεταπήδησης (hopping). Για τις συσκευές αναζήτησης στο substate, ο seed προέρχεται από έρευνα της συσκευής χρονιστή και την έρευνα του γενικού κώδικα πρόσβασης [8] ,ενώ με τη σύνδεση του substate, ο seed καθορίζεται από το χρονιστή και τη διεύθυνση Bluetooth της master συσκευής. Για την αναζήτηση, μόνο χρησιμοποιούνται 32 μεταπηδήσεις συχνότητας. Σε μια έρευνα, μια συσκευή αποκαλύπτει το χρονιστή της καθώς επίσης και τη διεύθυνση συσκευών Bluetooth της. Κατά συνέπεια, ο επιτιθέμενος μπορεί να καθορίσει το seed για τη σελιδοποίηση μεταπήδησης ακολουθίας με ανίχνευση μέσω των συχνοτήτων αναζήτησης και να γίνει υποκλοπή στα μηνύματα απόκρισης. Στη συνέχεια, μπορεί να παραγάγει το seed για την μεταπήδηση ακολουθίας του piconet δεδομένου ότι ο master θα αποκαλύψει την ταυτότητα και το χρονιστή κατά τη διάρκεια της σελιδοποίησης.

6.3.4 Μια συνδυασμένη επίθεση (combined attack)

Εάν ένας επιτιθέμενος λαμβάνει αρχικά τα κλειδιά μονάδας ή σύνδεσης μιας συσκευής, και μπορεί αργότερα να επισημάνει τη θέση του, μπορεί επίσης να γίνει υποκλοπή κατά την επικοινωνία με τρόπο πολύ αποτελεσματικό. (Σε δραστηριότητες όπου επιτρέπεται μόνο αδύναμη ή καθόλου κρυπτογράφηση, η επίθεση μπορεί να εκτελεσθεί χωρίς γνώση των κλειδιών.)

Πιο συγκεκριμένα, ο επιτιθέμενος θα καθορίσει την προσδιοριστική συσκευή και το χρονιστή αυτού που δέχεται την επίθεση, που υποθέτουμε ότι είναι μια master συσκευή. Από αυτό, μπορεί να λάβει την μεταπήδηση ακολουθίας. Με την παρεμπόδιση της κυκλοφορίας στις αντίστοιχες ζώνες, ο επιτιθέμενος μπορεί να λάβει μεγάλα τμήματα επικοινωνίας, εάν όχι ολόκληρη. Εάν η συσκευή η οποία

δέχεται την επίθεση κινείται σε απόσταση που δεν μπορεί να φτάσει η συσκευή που κάνει την επίθεση, οι επιτιθέμενες συσκευές θα την αναζητούσαν.

6.3.5 Επιθέσεις στην αυθεντικοποίηση

Η αυθεντικοποίηση βασίζεται στο διαμοιρασμό του ίδιου κλειδιού σύνδεσης μεταξύ δύο μονάδων. Αυτό το κλειδί σύνδεσης (link key) θα μπορούσε να είναι το αρχικό κλειδί, ή ένα προηγούμενο κλειδί σύνδεσης.

Εάν αυτό το κλειδί σύνδεσης ήταν το αρχικό κλειδί, τα πάντα βασίζονται στο PIN που διαμοιράζεται στις δύο μονάδες, δεδομένου ότι είναι το μόνο μυστικό κομμάτι των πληροφοριών που χρησιμοποιείται για να δημιουργήσει το αρχικό κλειδί, και επομένως, το μόνο μυστικό κομμάτι της πληροφορίας χρησιμοποιείται για επικύρωση. Αυτό το PIN είναι συνήθως ένας τετραψήφιος αριθμός (4-digit), ο οποίος περιορίζει το βασικό διάστημα σε 10.000 διαφορετικές τιμές. Αν δεν εισαχθεί από κάποιον χρήστη το PIN, τότε τίθεται το ερώτημα ποια επικύρωση να αναπτυχθεί.

Σε περίπτωση που το κλειδί σύνδεσης δεν είναι το αρχικό κλειδί, εμφανίζεται πρόβλημα όταν το κλειδί σύνδεσης παράγεται από το κλειδί μονάδας το οποίο έχει μεγάλο περιορισμό στη μνήμη της συσκευής. Σε αυτήν την περίπτωση, εάν η συσκευή A επικοινωνεί με μια άλλη συσκευή B, και επικοινωνεί αργότερα με μια συσκευή C, δεδομένου ότι η A και η C μπορούν να χρησιμοποιήσουν την μονάδα κλειδιού του A σαν κλειδί σύνδεσης, και να υποθέσει ότι η A και B χρησιμοποίησαν το ίδιο κλειδί, κατόπιν αυτές οι τρεις συσκευές χρησιμοποίησαν το ίδιο κλειδί σύνδεσης, και μπορεί επομένως να προσωποποιηθεί η καθεμία.

Οι επιθέσεις στην αυθεντικοποίηση βασίζονται στην αδυναμία παραγωγής αλγορίθμου απόκρισης (SAFER+), δεδομένου ότι η μόνη διαθέσιμη παραγωγή είναι η απόκριση string (στοιχειοσειρά) που παράχθηκε κατά την διάρκεια της αυθεντικοποίησης. Εντούτοις, στην περίπτωση της λήψης τιμών που έχουν εισαχθεί, ο επιτιθέμενος θα μπορούσε να λάβει το κλειδί σύνδεσης, και από αυτό, θα ήταν σε θέση να προσωποποιήσει τη συσκευή στις μελλοντικές αυθεντικοποιήσεις, καθώς επίσης και να πάρει το κλειδί κρυπτογράφησης.

6.3.6 Επιθέσεις στην κρυπτογράφηση

Προκειμένου να αποκρυπτογραφηθεί επιτυχώς μια τρέχουσα επικοινωνία μεταξύ δύο συσκευών, ένας που κάνει υποκλοπή (eavesdropper) πρέπει να έχει υπό κατοχή το κλειδί κρυπτογράφησης που παράγεται από τις δυο προηγούμενες συσκευές. Αυτό το κλειδί κρυπτογράφησης θα μπορούσε να είναι μεταβλητού μεγέθους (κυμαινόμενο μεταξύ 8 και 128 bit), το οποίο θα εξαρτάται κάθε φορά από τις απαιτήσεις του επιπέδου ασφάλειας. Επιπρόσθετα, αυτός που κάνει την επίθεση πρέπει επίσης να είναι σε θέση να συγχρονιστεί με την μονάδα του κύριου χρονιστή, η οποία συνεισφέρει στην παραγωγή μιας κατάλληλης κρυπτογραφημένης ροής.

Δεδομένου ότι οι μόνες απόρρητες πληροφορίες επάνω στην οποία το κλειδί κρυπτογράφησης υπολογίζεται σαν το link key, η γνώση του κλειδιού σύνδεσης και η υποκλοπή κατά την διάρκεια της επικύρωσης είναι αρκετά για να αποκρυπτογραφήσει ολόκληρη την μετάδοση.

Το τελευταίο είδος επίθεσης βασίζεται στην αδυναμία του κωδικού PIN, όταν χρησιμοποιείται ένας τετραψήφιος αριθμός. Ένας εισβολέας (intruder) που παρεμποδίζει την επικοινωνία από την πρώτη χειραψία (headshake), θα μπορούσε να υποστεί μια δύσκολη επίθεση του PIN για να συναχθούν για παράδειγμα οι παράμετροι της αλυσίδας συμπεριλαμβανομένου το κλειδί σύνδεσης. Τα PINs απαιτούνται για την παραγωγή του K_{init}. Όταν δύο συσκευές θέλουν να επικοινωνήσουν από την πρώτη στιγμή, εισάγουν την αρχική διαδικασία, και παράγουν το K_{init}. Δεν πρέπει να παράγουν ένα νέο K_{init} κατά την διάρκεια της post επικοινωνίας αλλά οι χρήστες μπορούν να απαιτήσουν ένα νέο K_{init} για περισσότερη ασφάλεια.

6.3.7.Προσωποποίηση

Μια άλλη επίθεση στην επικοινωνία είναι η προσωποποίηση (impersonation). Η προσωποποίηση είναι μια επίθεση που χρησιμοποιεί έναν ανιχνευτή για να καταγράψει τους Mobile Identification Numbers (MIN) και Electronic Serial Numbers (ESN) ενεργών χρηστών. Ο επιτιθέμενος (attacker) χρησιμοποιεί το MIN και το ESN για να κάνει κλίση, ο οποίος είναι γνωστός μόνο στον ανυποψίαστο χρήστη. Στην προδιαγραφή Bluetooth ,το πλαίσιο του πακέτου μπορεί να τροποποιηθεί σε τρία μέρη:

1) τα 3 bit member address,

2) το bit acknowledgement, και

3) τα 8bit ελέγχου σφάλματος header

6.3.8 Επιθέσεις μεταπήδησης συχνότητας (frequency hopping)

Αν και είναι υπερβολικά δύσκολη η οποιαδήποτε επίθεση στην μεταπήδηση συχνότητας, μερικές φορές αντιμετωπίζει κάποιες επιθέσεις. Το σχέδιο μεταπήδηση συχνότητας στηρίζεται στον χρονιστή Bluetooth, στην διάδοση ράδιο κυμάτων και στην ισχύ που παρέχουν τα ραδιοκύματα. Αυτές οι τρεις παράμετροι μπορούν να εκμεταλλευτούν τα ακόλουθα:

Κάθε συσκευή Bluetooth τρέχει ένα 28bit χρονιστή που δεν είναι ποτέ ρυθμισμένος ή κλειστός. Ο χρονιστής χτυπά 3.200 φορές ανά δεύτερο ή μία φορά κάθε 312 msec, το οποίο ανταποκρίνεται σε ένα χρονιστή με ποσοστό 3,2 KHZ. Ο χρονιστής έχει μια ακρίβεια ±20 parts per million (ppm) αλλά στους τύπους χαμηλής ισχύος (π.χ. standby or park) η ακρίβεια μειώνεται στα ±250ppm χρησιμοποιώντας έναν ταλαντωτή χαμηλής ισχύος. Ο επιτιθέμενος που χρησιμοποιεί λέιζερ χαμηλής ενέργειας (low energy lasers - LEL) ή ηλεκτρονικούς μαγνητικούς παλμούς (EMP) μπορεί να διακόψει τον χρονιστή Bluetooth και να θέσει εκτός λειτουργίας την επικοινωνία μεταξύ όλων των συσκευών. Αυτός ο τύπος επίθεσης θέτει σε μη-λειτουργικότητα οποιοδήποτε δίκτυο επικοινωνίας. Και οι επιθέσεις LEL και EMP είναι υπερβολικά σπάνιο να συμβούν και υπάρχει ένα πολύ μικρό ρίσκο από αυτόν τον τύπο επίθεσης.

Πλέον η ραδιοεπικοινωνία δικτύων βασίζεται στην (μονοκατευθυντική) omnidirectional διάδοση επικοινωνίας από μια συσκευή σε άλλη. Η

μονοκατευθυντική διάδοση είναι επίσης σημαντική αδυναμία. Η μονοκατευθυντική διάδοση εξασφαλίζει ότι ο δέκτης (συσκευή ή χρήστης) μπορεί να επικοινωνήσει μέσα από line-of-sight μεταδόσεις. Οι συσκευές Bluetooth ενεργούν ως μεταγωγοί δικτύων στις συσκευές για να επεκτείνουν line-of-sight επικοινωνία αλλά αυτό επεκτείνει επίσης και τις επιθέσεις που μπορεί να δεχτεί η επικοινωνία. Τα ράδιο κύματα διαδίδονται πέρα από τα όρια ενός κτηρίου και ένας επιτιθέμενος μπορεί να υποκλέψει στην επικοινωνία για μια μεγάλη χρονική περίοδο.

Τα μέτρα ενάντια σε αυτές τις επιθέσεις περιλαμβάνουνε χρήση μόνο της απαραίτητης ισχύος που απαιτείται για την επικοινωνία μεταξύ των συσκευών και την εξασφαλίζουν από αυτούς που κάνουνε υποκλοπές και από τους χάκερ. Μετά από μια συγκεκριμένη χρονική περίοδο, ο επιτιθέμενος μπορεί να αποκτήσει χρήσιμες πληροφορίες για τον αλγόριθμο μεταπήδησης συχνότητας και για τις παραμέτρους από τις μονοκατευθυντικές μεταδόσεις μεταξύ των συσκευών.

Η ανάμειξη με τη διαχείριση ισχύος μπορεί να έχει επιπτώσεις στο FSM καθώς επίσης και σε όλες τις λειτουργίες μέσα στο Bluetooth. Οι συσκευές σε μια κατάσταση σύνδεσης μπορούν να ρυθμίσουν την σύνδεση με τα piconets. Οι συσκευές έχουν επίσης τη δυνατότητα να τροποποιούν την ισχύ και μπορούν να ζητήσουν επικοινωνία με την άλλη συσκευή ρυθμίζοντας την ισχύ μετάδοσης που εξαρτάτε από την ποιότητα σύνδεσης. Εάν ένας επιτιθέμενος μπορεί να καταστρέψει ή να διακόψει την παροχή ισχύος σε μια ή όλες τις συσκευές μέσα σε ένα piconet ή scatternet, το δίκτυο Bluetooth θα ήταν σε χαοτική κατάσταση. Χωρίς την κατάλληλη ισχύ, το FSM δεν λειτουργεί κατάλληλα και η μεταπήδηση συχνότητας εμποδίζεται ή υποβιβάζεται.

6.3.9 Επίθεση επανάληψης

Μια άλλη επίθεση είναι η χρήση μιας συσκευής επίθεσης επανάληψης Bluetooth. Η επίθεση επανάληψης συμβαίνει όταν καταγράφει ο επιτιθέμενος την συνομιλία των δύο συσκευών για να δει ποιες συσκευές επικοινωνούν. Με την καταγραμμένη συνομιλία για ένα συγκεκριμένο χρονικό διάστημα ο επιτιθέμενος μπορεί να προκαλέσει ζημία.

Για παράδειγμα, εάν η συσκευή Α είναι ένα PDA που πραγματοποιεί μια τραπεζική συναλλαγή και η συσκευή Β είναι ένας ασύρματος δρομολογητής μιας τράπεζας. Ο επιτιθέμενος λαμβάνει μια προειδοποίηση για την συναλλαγή που στέλνεται από τον Α στον Β στέλνοντας την πολλές φορές αναγκάζοντας την τράπεζα να ελέγχει κάθε φορά την ακεραιότητα κάθε συναλλαγής. Στο Bluetooth, ένας επιτιθέμενος πρέπει να καταγράψει 79 κανάλια συγχρόνως κατά τη διάρκεια της συναλλαγής λόγω της μεταπήδησης συχνότητας. Αυτή είναι μια ασυνήθιστη τεχνολογία που λίγοι την κατέχουν. Υποτίθεται ότι ο επιτιθέμενος έχει την τεχνολογία να καταγράψει 79 κανάλια συγχρόνως κάθε δευτερόλεπτο. Ο επιτιθέμενος μπορεί ακόμα να αποκρυπτογραφήσει πώς η συναλλαγή μεταπηδά (jump) μέσω των ποικίλων καναλιών ώστε να συνθέσει ένα αξιόπιστο μήνυμα επανάληψης.

6.4 ΜΕΤΡΑ ΕΝΑΝΤΙΑ ΣΤΙΣ ΕΠΙΘΕΣΕΙΣ

Παρακάτω αναφέρουμε κάποιες μεθόδους αντιμετώπισης των επιθέσεων στο πρότυπο Bluetooth που θεωρούνται πιο κατάλληλες.

Μήκος (length) PIN. Προκειμένου να αποφύγουμε μια κατάσταση στην οποία ένας επιτιθέμενος είναι σε θέση να ανακαλύψει τα μυστικά κλειδιά των συσκευών που έχουνε δεχτεί την επίθεση, είναι σημαντικό να χρησιμοποιηθεί ένα αρκετά μεγάλο PIN. Εάν οι χρήστες επιλέξουν όλοι να χρησιμοποιήσουν ένα τυχαίο PIN των 64bit η πρακτική αυτή θεωρείται ως ασφαλής. Έτσι ένας επιτιθέμενος δεν θα καταβάλει μεγάλη προσπάθεια στο να ανακαλύψει τα κλειδιά αλλά θα στραφεί σε κάποιο άλλο σημείο του συστήματος, όπως για παράδειγμα στην κρυπτογράφηση των δεδομένων.

Προστασία κλειδιού μονάδας. Προκειμένου να αποφευχθεί ο επιτιθέμενος να μάθει το κλειδί μονάδας των συσκευών, η συσκευή με χαμηλή ικανότητα μνήμης μπορεί να χρησιμοποιήσει ένα αρκετά μεγάλο σύνολο κλειδιών, ένα για κάθε συσκευή που επικοινωνεί με αυτή, ή μπορεί να παραγάγει κλειδιά χρησιμοποιώντας τα κλειδιά μονάδας.

Ασφάλεια επιπέδου εφαρμογής (application layer security). Κάποιος μπορεί να χρησιμοποιήσει τις μεθόδους ανταλλαγής κλειδιών και κρυπτογράφησης στο επίπεδο εφαρμογής για να εξασφαλίσει την επικοινωνία, και τα μέτρα ασφάλειας Bluetooth. Σημειώνεται ότι εάν υιοθετούνται στη μέθοδο οι τυποποιημένες βάσεις πιστοποίησης, αυτό είναι δυνατό να αποτρέψει τις επιθέσεις ενδιάμεσου χρήστη.

Πολιτικές που προστατεύουν τις επιθέσεις ενδιάμεσων χρηστών. Υπενθυμίζεται ότι η επίθεση του ενδιάμεσου χρήστη στηρίζεται στο να πείσει και τις δύο συσκευές να γίνουνε master, ή και οι δύο να γίνουνε slave, προκειμένου να αποφευχθεί η συμφόρηση του καναλιού επικοινωνίας από τον επιτιθέμενο. Επομένως, ορισμένες επιθέσεις ενδιάμεσων χρηστών μπορούν να αποφευχθούν με τη βοήθεια πολιτικών που καθορίζουνε ποια συσκευή μπορεί να πάρει το ρόλο του master ή του slave και κάτω από ποιες περιστάσεις.

Φυσική προστασία (physical protection). Οι επιθέσεις στο κλειδί ανταλλαγής στηρίζονται στον επιτιθέμενο που είναι σε θέση να ανιχνεύσει τα σήματα που μεταφέρονται από τις συσκευές οι οποίες έχουνε δεχτεί την επίθεση. Η χρήση του κλωβού Faraday (με τη μορφή ενός μεταλλικού καλύμματος) μπορεί να είναι χρήσιμη για την ασφάλεια ενάντια σε αυτή την επίθεση.

Κρυπτογραφημένο κείμενο(cipher). Οι επιθέσεις ενάντια στο κρυπτογραφημένο κείμενο μπορούν να αποφευχθούν με την αντικατάσταση του κρυπτογραφημένου κειμένου, π.χ. με AES [5].

ΚΕΦΑΛΑΙΟ 7

ΣΥΓΚΡΙΣΗ ΑΣΦΑΛΕΙΑΣ BLUETOOTH ΜΕ ΤΟ ΠΡΟΤΥΠΟ 802.11

7.1 ΛΙΓΑ ΛΟΓΙΑ ΓΙΑ ΤΟ ΠΡΟΤΥΠΟ 802.11

7.1.1 Γενικά

Το 802.11 είναι το όνομα του project της ομάδας εργασίας του IEEE για τα ασύρματα δίκτυα .Το IEEE 802.11 έχει ταχύτητα 2Mbps και είναι το πρότυπο με βάση το οποίο υλοποιούνταν μέχρι τώρα τα ασύρματα δίκτυα Ethernet.Υπόρχουν δυο εκδόσεις φυσικού επιπέδου:

- το 802.11a, και
- το 802.11b.

Η έκδοση IEEE 802.11b (γνωστή και ως IEEE 802.11 High Rate ή Wi-Fi) έχει ταχύτητα 11Mbps ενώ η έκδοση IEEE 802.11a,που βρίσκεται ακόμη στο στάδιο της ανάπτυξης, προβλέπει ταχύτητες μέχρι 54Mbps. Το IEEE802.11b είναι, ουσιαστικά, το στάνταρ στα ασύρματα δίκτυα Ethernet και υποστηρίζει τόσο επικοινωνία point-to-point (η οποία ονομάζεται ad hoc) όσο και επικοινωνία point-to-multipoint. Οι υπολογιστές που βρίσκονται στον ίδιο χώρο. π.χ, μπορούν να οριστούν σε κατάσταση ad hoc και να επικοινωνήσουν άμεσα μεταξύ τους. Μέρος επίσης του 802.11b αποτελεί και το WEP (Wired Equivalent Privacy, μυστικότητα αντίστοιχα με τα καλωδιωμένα δίκτυα) το οποίο χρησιμοποιεί τον αλγόριθμο RC4 και προσφέρει δυνατότητα εξουσιοδότησης κάθε κόμβου και κρυπτογράφησης δεδομένων. Η τεχνολογία Bluetooth και το πρότυπο 802.11b είναι πραγματικά αρκετά παρόμοια. Και τα δύο είναι μέθοδοι που επιτρέπουν στους υπολογιστές να επικοινωνήσουν με άλλες συσκευές, χρησιμοποιούν ασύρματη τεχνολογία και λειτουργούν σε ζώνη φάσμα τος 2,4GHz.

Παρακάτω παρουσιάζονται οι δύο κύριες επιθέσεις στο 802.11b καθώς και γιατί αυτές οι επιθέσεις δεν είναι αποτελεσματικές στις ασύρματες επικοινωνίες Bluetooth.

7.1.2 Πως λειτουργεί

Το Bluetooth και το 802.11 χρησιμοποιούν τη ραδιοφωνική μετάδοση σημάτων RF στη ζώνη 2.4 GHz. Το Bluetooth χρησιμοποιεί την τεχνολογία FHSS ενώ το 802.11 χρησιμοποιεί την DSSS (direct sequence spread spectrum).

Η διαφορά μεταξύ FHSS και DSSS είναι ότι τα σήματα FHSS μεταπηδούν εντός 79 διαφορετικών συχνοτήτων που χωρίζονται σε διαστήματα των 1MHz. Τα σήματα DSSS καθορίζονται μέσα σε ένα κανάλι 17 MHz (τρία εκ των οποίων είναι διαθέσιμα στη ζώνη 2.4 GHz), αλλά καλύπτονται με τεχνητό θόρυβο για να μειώσουν την παρέμβαση και να βελτιώσουν την ασφάλεια. Η πρόσθετη ασφάλεια παρέχεται από το πρότυπο κρυπτογράφησης Wireless Equivalent Privacy (WEP), το οποίο χρησιμοποιεί τεχνολογία κρυπτογράφησης των 128-bit.

Ένα αποτέλεσμα της χρησιμοποίησης DSSS αντί FHSS είναι ότι το 802.11 υποστηρίζει πιο γρήγορη μετάδοση δεδομένων που φτάνει μέχρι τα 11Mbps. Από αυτή την άποψη, το 802.11 είναι αποδεκτό υποκατάστατο του Ethernet, το οποίο έχει παρόμοιες ταχύτητες μετάδοσης. Το μειονέκτημα της χρησιμοποίησης DSSS είναι ότι το 802.11 είναι πιο ευαίσθητο στην παρεμβολή από άλλες συσκευές που χρησιμοποιούν ζώνη των 2.4 GHz, ειδικά συσκευές που βρίσκονται σε περιβάλλον σπιτιού, π.χ. ασύρματα τηλέφωνα σπιτιών, πόρτες γκαράζ, φούρνοι μικροκυμάτων.

Ένα 802.11 δίκτυο απαιτεί χρήση υλικού σημείου πρόσβασης (σταθμός βάσης), το οποίο μπορεί να αυξήσει το κόστος του δικτύου. Ένα σημείο πρόσβασης είναι η μονάδα δεκτών/ πομπών αποστολής σημάτων στο οποίο οι απομακρυσμένες συσκευές έχουν πρόσβαση ώστε να συνδεθούν με το δίκτυο.

7.1.3 Σκοπός του 802.11

Ο σκοπός του προτύπου 802.11 είναι η παροχή ασύρματης σύνδεσης σε αυτόματα μηχανήματα, σε εξοπλισμό ή σε σταθμούς που η λειτουργία τους απαιτείται να είναι πολύ γρήγορη και οι οποίοι μπορεί να είναι φορητοί ή να βρίσκονται πάνω σε οχήματα που κινούνται σε μια μικρή περιοχή. Έχει σαν στόχο να περιγράψει ένα WLAN που παρέχει υπηρεσίες, οι οποίες μέχρι τώρα υπήρχαν μόνο στα ενσύρματα δίκτυα, όπως υψηλή απόδοση, αξιόπιστη μετάδοση δεδομένων και συνεχή σύνδεση με το δίκτυο.

Ειδικότερα, το πρότυπο 802.11:

- Περιγράφει τις λειτουργίες και τις υπηρεσίες που απαιτούνται, ώστε να μπορεί μία συμβατή με το IEEE 802.11 συσκευή να λειτουργεί μέσα σε ασύρματα τοπικά δίκτυα.
- Ορίζει τις MAC διαδικασίες για την υποστήριξη των υπηρεσιών παράδοσης της μονάδας υπηρεσιών ασύγχρονων δεδομένων MAC.
- Ορίζει μερικές τεχνικές και διαδικασίες διεπαφής για τα σήματα του φυσικού επιπέδου, τα οποία ελέγχονται από το 1EEE 802.11 MAC.
- Επιτρέπει τη λειτουργία μιας συμβατής με το IEEE 802.11 συσκευής μέσα σε ένα ασύρματο τοπικό δίκτυο το οποίο μπορεί να συνυπάρξει με άλλα επικαλυπτόμενα IEEE 802.11 LAN.

	Bluetooth	**IEEE802.11**	**IEEE802.11b**	**IEEE802.11a**
Ταχύτητα	1Mbps	2Mbps	11Mbps	54 Mbps
Εμβέλεια	10μ	100μ	100μ	100μ
Συχνότητα	2,4 Hz	2,4 Hz	2,4 Hz	5 GHz
Διασύνδεση	Καμία	Ethernet	Ethernet	Ethernet
Κατάσταση	Διαθέσιμο	Διαθέσιμο	Διαθέσιμο	Σε ανάπτυξη
Υποστηρικτές	Ericsson IBM, Toshiba, Intel, Nokia, Motorola		Cisco, Lucent, 2Com, Apple, Compaq, Zoom, Dell, Nokia	

Πίνακας 7.1: Σύγκριση των ασύρματων δικτύων

7.2 ΥΠΟΚΛΟΠΗ ΤΟΥ 802.11b (EAVESDROPPING)

Όταν ένας χρήστης στέλνει τα στοιχεία μέσω ενός ασύρματου δίκτυου, έχει μια λογική προσδοκία ότι τα μη εξουσιοδοτημένα (unauthorized) πρόσωπα δεν μπορούν να διαβάσουν τα δεδομένα του. Αντίθετα από ένα ενσύρματο δίκτυο που απαιτεί μια φυσική παρείσφρηση, τα ασύρματα πακέτα δεδομένων μπορούν να παραληφθούν με έναν κατάλληλο δέκτη, ενδεχομένως έξω από τα φυσικά εμπόδια ασφάλειας μιας οργάνωσης. Αυτό ονομάζεται Parking lot attacks, στις οποίες ένας που επιτίθεται (attacker) κάθεται σε ένα αυτοκίνητο στο χώρο στάθμευσης του προοριζόμενου θύματος (victim) (δηλαδή του ατόμου που δέχεται την επίθεση). Συνεπώς, και οι δύο τεχνολογίες Bluetooth και 802.11 χρησιμοποιούν την κρυπτογράφηση δεδομένων στα χαμηλότερα στρώματα δικτύων.

Η 802.11b προδιαγραφή χρησιμοποιεί ένα πλαίσιο ασφάλειας αποκαλούμενο πρωτόκολλο μυστικότητας ασύρματου δικτύου (wireless equivalent privacy protocol) (WEP). Ένα κλειδί εξαρτημάτων του WEP είναι η χρήση της ροής κρυπτογράφησης (stream cipher) RC4. Το RC4 (είναι αλγόριθμος που τον χρησιμοποιεί το 802.11b) είναι γνωστό και συνήθως χρησιμοποιείται ως ροή κρυπτογράφησης, αλλά η χρήση της στο 802.11b είναι αμφισβητήσιμη εξ αιτίας της φύσης των πακέτων ασύρματου δικτύου.

Το RC4 ενεργοποιείται από XORing ένα απλό κείμενο (plaintext) δεδομένων με ένα κλειδί ρευματικής κρυπτογράφησης. Το αποτέλεσμα καλείται συνήθως κρυπτογράφημα (ciphertext). Το RC4 αρχικοποιείται με ένα μυστικό κλειδί WEP και ένα δημόσιο κλειδί μήκους 24 bit IV (διάνυσμα αρχικοποίησης). Εάν ένας επιτιθέμενος (attacker) γνωρίζει ένα απλό κείμενο (plaintext) και ένα κρυπτογραφημένο, μπορεί να υπολογίσει το κλειδί κρυπτογράφησης χρησιμοποιώντας τη λειτουργία XOR.

Λόγω της χαμηλής εντροπίας των περισσότερων απλών κειμένων, εάν ένας επιτιθέμενος μπορεί να καταγράψει έναν μεγάλο αριθμό κρυπτογραφημένων μηνυμάτων μπορεί επίσης, να υπολογίσει το κλειδί κρυπτογράφησης. Για αυτόν τον λόγο οι χρήστες RC4 ενθαρρύνονται να αλλάζουν το κλειδί κρυπτογράφησης σε κάθε μήνυμα. Το βασικό πρόβλημα με το RC4 πάνω στο πρότυπο 802.11b είναι ότι τα ασύρματα κανάλια, από τη φύση τους, χάνουν περιστασιακά πακέτα δεδομένων. Κατά συνέπεια, ο συγχρονισμός μεταξύ κρυπτογράφησης και αποκρυπτογράφησης είναι δύσκολο να διατηρηθεί για οποιοδήποτε χρονικό διάστημα. Για να ξεπεράσει αυτόν τον περιορισμό, το WEP

διατηρεί το συγχρονισμό αλλάζοντας το διάνυσμα αρχικοποίησης 24-bit (IV) σε κάθε πακέτο. Ωστόσο, τα πακέτα του 802.11b είναι σχετικά κοντά το ένα με το άλλο. Επομένως, κάποιος μπορεί να περιμένει ένα κλειδί/IV συνδυασμού να επαναλαμβάνεται κάθε λίγα δευτερόλεπτα. Κατά συνέπεια, η κρυπτογράφηση WEP είναι σχετικά εύκολο να σπάσει. [4] [5] .

7.3 ΛΑΝΘΑΣΜΕΝΗ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ 802.11b

Για να επιτευχθεί πρόσβαση σε ένα δίκτυο, ένας χρήστης πρέπει να αυθεντικοποιηθεί. Ενώ η αυθεντικοποίηση γίνεται σε πιο υψηλό επίπεδο δικτύων, οι τεχνολογίες 802.11b και Bluetooth υποστηρίζουν, επίσης, την αυθεντικοποίηση των συσκευών.

Στο 802.11b η αυθεντικοποίηση εκτελείται από μια διαδικασία πρόκλησης-απάντησης (challenge response) χρησιμοποιώντας ένα κοινό μυστικό (shared secret). Αφού ζητηθεί η αυθεντικοποίηση, αυτός που εκτελεί τη διαδικασία αυθεντικοποίησης (authenticator) στέλνει σε αυτόν που ξεκινά την πρόκληση έναν τυχαίο αριθμό 128-octet. Ο δεύτερος κάνει την κρυπτογράφηση χρησιμοποιώντας το κοινό μυστικό και την διαβιβάζει πίσω στον αυθεντικοποιητή (authenticator). Η κρυπτογράφηση εκτελείται από XORing πρόκληση με μια ψευδοτυχαία σειρά που διαμορφώνεται από το κοινό μυστικό και το δημόσιο IV. Το μόνο πράγμα που αλλάζει από αυθεντικοποίηση σε αυθεντικοποίηση με έναν συγκεκριμένο χρήστη είναι το plaintext (απλό κείμενο) .

Μια επίθεση σε αυτόν τον μηχανισμό αυθεντικοποίησης παρουσιάζεται παρακάτω:[6] Πρώτα ο εισβολέας (intruder) προσδιορίζει την ψευδοτυχαία σειρά (pseudorandom) με την καταγραφή της πρόκλησης (απλό κείμενο) και της απάντησης (κρυπτογραφημένο κείμενο) και XORing. Έπειτα προσωποποιείται το άτομο το οποίο δέχεται την επίθεση με τη χρησιμοποίηση της ψευδοτυχαίας σειράς για να υπολογίσει την απάντηση στις επόμενες προκλήσεις. Σημειώνεται ότι ο επιτιθέμενος (attacker) δεν χρειάζεται να προσδιορίσει το κοινό μυστικό, η γνώση της ψευδοτυχαίας σειράς είναι ικανοποιητική.

7.4 ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ ΣΥΣΚΕΥΩΝ ΣΕ ΤΕΧΝΟΛΟΓΙΑ BLUETOOTH

Όπως και το πρότυπο 802.11b, η τεχνολογία Bluetooth παρέχει μια μέθοδο αυθεντικοποίησης συσκευών. Η αυθεντικοποίηση συσκευών παρέχεται χρησιμοποιώντας ένα κοινό μυστικό μεταξύ των δύο συσκευών. Το κοινό μυστικό καλείται *κλειδί σύνδεσης (link key).* Αυτό το κλειδί σύνδεσης καθορίζεται σε μια ειδική συνεδρίαση επικοινωνίας αποκαλούμενη σύνδεση (pairing). Όλες οι συσκευές ταξινομούνται (συσκευές σύνδεσης που είχαν μια προηγούμενη σύνδεση για να καθορίσουν τις διαδικασίες ασφάλειας) και μοιράζονται ένα κοινό κλειδί σύνδεσης. Υπάρχουν δύο τύποι κλειδιών σύνδεσης: τα **κλειδιά μονάδας** (unit key) και τα **κλειδιά συνδυασμού** *(combination key)* [8]*.*

Μια συσκευή που χρησιμοποιεί το *κλειδί μονάδας* χρησιμοποιεί το ίδιο μυστικό κλειδί για όλες τις συνδέσεις. Τα κλειδιά μονάδας είναι κατάλληλα για συσκευές με περιορισμένη μνήμη ή περιορισμό διεπαφής (interface) με τον χρήστη. Κατά τη διάρκεια της διαδικασίας σύνδεσης το κλειδί μονάδας μεταφέρεται (κρυπτογραφημένο) στην άλλη μονάδα. Σημειώνεται ότι μόνο μια από τις δύο ταξινομημένες μονάδες σύνδεσης επιτρέπεται να χρησιμοποιήσει ένα κλειδί μονάδας.

Τα κλειδιά *συνδυασμού* είναι κλειδιά σύνδεσης που είναι μοναδικά σε ένα συγκεκριμένο ζευγάρι (pair) συσκευών. Το κλειδί συνδυασμού χρησιμοποιείται μόνο για να προστατεύσει την επικοινωνία μεταξύ των δύο αυτών συσκευών.

Σαφώς, μια συσκευή που χρησιμοποιεί ένα κλειδί μονάδας δεν είναι τόσο ασφαλής όσο μια συσκευή που χρησιμοποιεί ένα κλειδί συνδυασμού. Δεδομένου ότι το κλειδί μονάδας είναι κοινό για όλες τις συσκευές με τις οποίες η συσκευή έχει συνδεθεί (paired), όλες αυτές οι συσκευές έχουν γνώση του κλειδιού μονάδας. Συνεπώς, είναι σε θέση να υποκλέψουν οποιαδήποτε κυκλοφορία βασισμένη σε αυτό το κλειδί. Επιπλέον, θα μπορούσαν, θεωρητικά, να τροποποιηθούν παριστάνοντας άλλες συσκευές χρησιμοποιώντας το κλειδί. Κατά συνέπεια, όταν χρησιμοποιείται ένα κλειδί μονάδας δεν υπάρχει καμία προστασία ενάντια σε επιθέσεις από άλλες συσκευές με τις οποίες η συσκευή έχει συνδεθεί. Κατά συνέπεια, το Bluetooth SIG (special interest group) αποθαρρύνει τη χρήση του κλειδιού μονάδας σε ασφαλείς εφαρμογές.

Η αυθεντικοποίηση εκτελείται με ένα σχέδιο πρόκλησης-απάντησης (challenge-response) που χρησιμοποιεί τον E1 αλγόριθμο. Ο E1 είναι μια τροποποίηση του μπλοκ cipher SAFER+. Το σχέδιο λειτουργεί ως εξής: Ο αποστολέας (verifier) εκδίδει μια μεγάλη πρόκληση των128bit. Ο παραλήπτης (claimant) εφαρμόζει έπειτα τον αλγόριθμο E1 χρησιμοποιώντας την πρόκληση, τη διεύθυνση Bluetooth 48bit , και το τρέχον κλειδί σύνδεσης. Επιστρέφει έπειτα τα 32 σημαντικότερα bit από τα 128 bit. [Τα υπόλοιπα bits ονομάζονται Authentication Ciphering Offset (ACO) και χρησιμοποιούνται για να παραγάγουν το κλειδί κρυπτογραφημένου κειμένου (ciphering) για τα δεδομένα κρυπτογράφησης]. Ο αποστολέας (verifier) επιβεβαιώνει την απάντηση, οπότε σ' αυτή την περίπτωση η αυθεντικοποίηση έχει πετύχει και οι ρόλοι αντιστρέφονται και η ίδια διαδικασία εφαρμόζεται πάλι, έτσι ολοκληρώνετε η αμοιβαία αυθεντικοποίηση.

Ο αλγόριθμος πρόκλησης-απάντησης Bluetooth διαφέρει από τον 802.11b σε πολύ σημαντικά σημεία. Στον 802.11b η μορφή πρόκλησης-απάντησης είναι μια σύνδεση plaintext/ciphertext. Αυτό το γεγονός, που συνδυάζεται με την απλότητα της μεθόδου κρυπτογράφησης (XOR), επιτρέπει σε έναν εισβολέα (intruder) να υπολογίσει εύκολα τη βασική σειρά αυθεντικοποίησης με την παρακολούθηση μιας διαδικασίας αυθεντικοποίησης. Αντίθετα, η μέθοδος αυθεντικοποίησης Bluetooth δεν μεταφέρει ποτέ την πλήρη σύνδεση πρόκλησης-απάντησης.

Επιπλέον, ο E1 αλγόριθμος δεν είναι εύκολα αντιστρέψιμος. Κατά συνέπεια ακόμα κι αν ένας επιτιθέμενος (attacker) έχει καταγράψει μια συνεδρίαση (session) αυθεντικοποίησης πρόκλησης-απάντησης, δεν μπορεί (άμεσα) να χρησιμοποιήσει αυτό το στοιχείο για να υπολογίσει το κλειδί αυθεντικοποίησης.

7.5 ΣΤΟΙΧΕΙΑ ΥΠΟΚΛΟΠΗΣ ΤΟΥ 802.11

Τα πρότυπα Bluetooth δεν χρησιμοποιούν το RC4 αλλά μάλλον την ροή κρυπτογράφησης EO, η οποία έχει ως σκοπό να τρέξει πέρα από ένα ασύρματο δίκτυο πακέτων Bluetooth. Ένα μοναδικό κλειδί κρυπτογράφησης παράγεται για κάθε συνεδρίαση (session) από την οποία προέρχονται τα κλειδιά ανά-πακέτο, με έναν τρόπο ώστε να αποφεύγεται το πρόβλημα 802.11b που προκαλείται από τη συχνή επαναχρησιμοποίηση των κλειδιών ανά-πακέτο.

Οι άμεσες επιθέσεις κρυπτογράφησης EO είναι γνωστές αλλά είναι μεγάλης πολυπλοκότητας. Παρουσιάζονται στην προδιαγραφή δύο τέτοιες επιθέσεις η πρώτη είναι 2¹°° πολυπλοκότητα, η δεύτερη είναι μια " επίθεση birthday type " 2^{66} γενικής πολυπλοκότητας.

Όπως το RC4, έτσι και το ΕΟ απαιτεί ένα κρυπτογραφημένο κλειδί. Το κρυπτογραφημένο κλειδί υπολογίζεται ως παρεμβολή ραδιοσυχνοτήτων ενός τυχαίου αριθμού, του κλειδιού σύνδεσης και ενός υποπροϊόντος (byproduct) διαδικασίας αυθεντικοποίησης του επικυρωμένου λογαριασμού μετατόπισης (Authentication Ciphering Offset - ACO).

Ενώ το κλειδί σύνδεσης χρησιμοποιείται επίσης για να παραγάγει ένα κρυπτογραφημένο κλειδί που χρησιμοποιείται για την κρυπτογράφηση δεδομένων, δεν χρησιμοποιείται για την κρυπτογράφηση των δικών του στοιχείων. Αυτό είναι ένα σημαντικό πλεονέκτημα του 802.11b στο οποίο το ίδιο κλειδί χρησιμοποιείται για αυθεντικοποίηση και κρυπτογράφηση.

Συμπερασματικά, οι γνωστές επιθέσεις κρυπτογράφησης ΕΟ που χρησιμοποιούνται σε Bluetooth είναι πολύ πιο σύνθετες υπολογιστικά από αντίστοιχες επιθέσεις RC4 που χρησιμοποιούνται σε 802.11b. Μέχρι τώρα, καμία πρακτική άμεση επίθεση δεν έχει αναφερθεί. Αντίθετα στο 802.11b, χρησιμοποιούνται διαφορετικά κλειδιά για αυθεντικοποίηση και κρυπτογράφηση. Αναλόγως οι πρακτικές μελέτες για την ασφάλεια Bluetooth έχουν στραφεί στις μεθόδους για να υποθέσουν ή να υποκλέψουν το κλειδί. Ο λογικότερος χρόνος για να δοκιμαστεί αυτό είναι κατά τη διάρκεια της διαδικασίας σύνδεσης.

7.6 ΣΥΝΔΕΣΗ (PAIRING) BLUETOOTH

Η σύνδεση είναι η διαδικασία όπου εγκαθίσταται μια σχέση (κλειδί σύνδεσης) μεταξύ δύο προηγούμενων άγνωστων συσκευών. Το κλειδί σύνδεσης παράγεται όταν οι συσκευές είναι αρχικά ενωμένες (δηλαδή το κλειδί σύνδεσης δεν υπάρχει πριν από τη διαδικασία ένωσης). Η σύνδεση διευκολύνεται με ακόμα ένα κλειδί, το κλειδί αρχικοποίησης (initialization key). Αυτό το κλειδί υπολογίζεται από ένα ζευγάρι (pair) συσκευών χρησιμοποιώντας τις διευθύνσεις Bluetooth κάθε συσκευής, ένα τυχαίο αριθμό, και ένα κοινό μυστικό (shared secret) (PIN). Δεδομένου ότι χρησιμοποιείται μόνο η αρχική σύνδεση (initial pairing), το κλειδί αρχικοποίησης χρησιμοποιείται μόνο μια φορά.

Η αρχική σύνδεση είναι η πιο πρόσφορη περιοχή επίθεσης σε μια συσκευή Bluetooth. Εάν ο επιτιθέμενος (attacker) μπορεί να υποθέσει ή να κλέψει το PIN κατά τη διάρκεια της αρχικής σύνδεσης, κατόπιν μπορεί να εκτελέσει μια αποδοτικότερη αναζήτηση για να παραγάγει το κλειδί σύνδεσης. Αυτή η αναζήτηση απλοποιείται περαιτέρω εάν οι επικοινωνίες που εμφανίζονται μέσω των συσκευών ενώνονται και καταγράφονται. Για αυτόν τον λόγο το Bluetooth SIG ενθαρρύνει έντονα τη μεγάλη χρήση των τυχαίων PINs και προτείνει να εκτελεσθεί η σύνδεση μόνο σε μια ιδιωτική θέση. Υποθέτοντας ότι και οι δύο συσκευές έχουν επικοινωνία ανθρώπου-μηχανής (όπως ένα αριθμητικό πληκτρολόγιο) προτείνεται το PIN να εισάγεται από τον χρήστη και στις δύο συσκευές. Κατά συνέπεια, το μεγάλο PIN παρέχει βελτιωμένη ασφάλεια δεδομένου ότι το PIN δεν μπορεί να ληφθεί μέσω αέρος (over-the-air). Για να κλέψει το PIN ένας επιτιθέμενος πρέπει να υποθέσει ή να το καταγράψει με μερικά άλλα μέσα όπως την άμεση παρατήρηση του χρήστη, μια δυσκολότερη διαδικασία εάν το PIN είναι μεγάλο και η σύνδεση εκτελείται μυστικά.

ΚΕΦΑΛΑΙΟ 8

ΣΥΜΠΕΡΑΣΜΑΤΑ

8.1 ΜΕΛΛΟΝΤΙΚΕΣ ΕΞΕΛΙΞΕΙΣ

Ποιες όμως θα είναι στο μέλλον οι εξελίξεις στη βασική λειτουργία του Bluetooth;

Δεδομένου ότι το Bluetooth ωριμάζει και οι ικανότητες και οι περιορισμοί του είναι δοκιμασμένες σε πραγματικές εφαρμογές, η προσοχή θα στραφεί στο πώς μπορεί να βελτιωθεί η απόδοσή του. Παρακάτω παρουσιάζονται μερικές από τις δυνατότητες για μελλοντικές εξελίξεις στη λειτουργία του Bluetooth, με έμφαση στα χαμηλότερα επίπεδα πρωτοκόλλου:

1. Γίνεται έρευνα από την ομάδα εργασίας για υψηλότερες ροές δεδομένων.
2. Η AFH (Προσαρμοστική μεταπήδηση συχνότητας - Adaptive frequency hopping - AFH). μπορεί να μειώσει την απώλεια πακέτων εάν εφαρμοστεί κατάλληλα. Πολλοί θεωρούν ότι η AFH θα γίνει τελικά μέρος της προδιαγραφής Bluetooth.
3. Στις έξυπνες κεραίες υπάρχει η δυνατότητα να αυξηθεί η επεξεργασία σήματος ακόμη περισσότερο.

8.2 ΓΕΝΙΚΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ

Το Bluetooth είναι ένα σύστημα που χρησιμοποιείται σε ραδιοζεύξεις μικρής εμβέλειας και πρόκειται να αντικαταστήσει τις καλωδιακές συνδέσεις μεταξύ κινητών και σταθερών ηλεκτρονικών συσκευών, εξασφαλίζοντας έτσι τοπικές ασύρματες συνδέσεις μεταξύ των φορητών συσκευών. Είναι ιδιαίτερα κατάλληλο για ad-hoc δίκτυα και οι εναέριες διασυνδέσεις έχουν βελτιστοποιηθεί έτσι ώστε να εξασφαλίζουν τη μέγιστη διασφάλιση έναντι των παρεμβολών σε εύρος 2,4 GHz ISM. Ακόμη, το σύστημα αυτό, καθορίζει μια ομοιόμορφη δομή για ένα μεγάλο εύρος συσκευών, ώστε να επικοινωνούν μεταξύ τους με ελάχιστη προσπάθεια από το χρήστη. Οι κυριότερες ιδιότητες του είναι η μικρή πολυπλοκότητα, η χαμηλή ισχύς και το χαμηλό κόστος.

Επίσης, το σύστημα υποστηρίζεται από αρκετούς κατασκευαστές προσωπικών υπολογιστών και τηλεπικοινωνιακών εξοπλισμών. Το πρώτο καταναλωτικό προϊόν που υποστηρίζει το Bluetooth εμφανίστηκε από την Ericsson στα τέλη του 1999.

Εξετάζοντας το σύστημα και τους ημιαγωγούς που σχεδιάστηκαν νωρίτερα στη διαδικασία σχεδιασμού, παρατηρούμε ότι σε αυτό το σημείο μπορούμε να αυξήσουμε σημαντικά την πιθανότητα εντοπισμού και διόρθωσης των σχεδιαστικών ελαττωμάτων που η διόρθωση τους είναι δαπανηρή. Αυτό μειώνει την πιθανότητα να βγουν αργότερα στην επιφάνεια τα ελαττώματα του σχεδιασμού, όταν είναι ακριβή η διόρθωση τους και μπορεί να καθυστερήσει σημαντικά την παράδοση των προϊόντων. Έχοντας ένα ξεκάθαρο αρχιτεκτονικό πρότυπο, εξασφαλίζεται η καλύτερη επικοινωνία και ελαχιστοποίηση των διαφωνιών μεταξύ των μελών της ομάδας.

Τέλος ο σκοπός του συστήματος αυτού είναι να παρέχει εύκολο service για κινητά και επιχειρηματίες διαμέσου ενός μικρού ασύρματου βραχυπρόθεσμου δικτύου. Σύμφωνα με τις προδιαγραφές το μέλλον μας θα εξαρτάται όπως φαίνεται από ασύρματες συνδέσεις που θα μας διευκολύνουν, σε κάθε μας εργασία.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] ”Bluetooth SIG Specification of the Bluetooth system ,Profiles”,
[2] “Bluetooth SIG Specification of the Bluetooth system , Core”,
[3] Information on Bluetooth (Official Homepage)
http://www.bluetooth.com/

[4]. Bluetooth information,
http://www.bluetoothcentral.com/

[5] Bluetooth, The Bluetooth Specification, V.1.0B
http://www.bluetooth.com/developer/_specification/specification.asp

[6] Miller T., Bluetooth Security Architecture,
http://www.bluetooth.com/developer/download/download.asp?doc=174 >

[7]. Bluetooth Baseband
http://www.infotooth.com/tutorial/BASEBAND.htm

[8]. Bluetooth - an inferior LAN concept?
http://www.infotooth.com/knowbase/ othernetworks/71.htm

[9]. Bluetooth Glossary
http://www.infotooth.com/glossary.htm#authentication

[10]. Authentication process in Bluetooth
http://www.infotooth.com/knowbase/security/66.htm

[11]. Authentication in Bluetooth
http://www.infotooth.com/knowbase/security/80.htm

[12]. Knowledge Base for Bluetooth information
http://www.infotooth.com/

[13] W. A. Arbaugh, "Wireless Research",
http://www.cs.umd.edu/~waa/wireless.html

[14] J. Walker, "Unsafe at any key size; An analysis of the WEP encapsulation",
http://grouper.IEEE.org/groups/802/11/Documents/DocumentsHolder/0-362.zip

[15] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11."
http://www.issac.sc.berkley.edu/issac/wep-faq.html.

[16] W. Arbaugh, N. Shankar, Y.CJ. Wan, "Your 802.11 Wireless Network has No Clothes"
http://www.cs.umd.edu/~waa/wireless.pdf

[17] M. Jakobsson and S. Wetzel, "Security Weaknesses in Bluetooth"
http://www.rsasecurity.com/rsalabs/staff/bios/mjakobsson/bluetooth/bluetooth.pdf

[18] S.Fluhrer and S.Lucks,"Analysis of the E0 Encryption System"
http://th.informatik.uni-mannheim.de/People/Lucks/papers/e0.ps.gz.

[19] "B.Miller,"IEEE 802.11 and Bluetooth wireless technology",
http://www -106.ibm.com/developerworks/wireless/library/wi-phone

[20]. General information on bluetooth
http://www.mobi1einfo.com/bluetooth/

[21]. Annikka Aalto , Bluetooth
http://www.tml.hut.f1/Studies/Tikl1 O.300/1999/Essays/bluetooth.html

[22]. Oraskari, Jyrki, Bluetooth 2000
http://www.hut.f1/~joraskur/bluetooth.html

[23]. How Stuff Works, information on BT
http://www.howstuffworks.com/bluetooth3.htm

[24] Stajano F. & Anderson R, The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks,
http://www.cl.cam.ac.uk/~fims27/duckling/ >

[25] Zhou L. & Haas Z. , Securing Ad Hoc Networks
http://www.ee.cornell.edu/~haas/Publications/network99.ps >

[26] Dasgupta, Korak. "Bluetooth Protocol and Security Architecture Review.
http://www.cs.utk.edu/~desgupta/bluetooth.

[27] "Bluetooth - An Overview"
http://www.abc.se/~m10183/bluet00.htm.

[28] "Bluetooth - An Overview, Security"
http://www.abc.se/~m10183/bluet08.htm.

[29] Wireless LAN Systems-Technology and Specification." NDC Communications
http://www.ndclan.com/wireless/wlanwl.htm.

[30] "Frequency Hopping Spread Spectrum PHY of the 802.11 Wireless LAN Standard." Proxim Corporation
http://www.proxim.com/wireless/whiteppr/r12security.shtml.

[31]. Thomas Muller, Bluetooth WHITE PAPER: Bluetooth
Security Architecture, Version 1.0.

[32]. D. Bleichenbacher, personal communication.

[33] Amoroso E., Fundamentals of Computer Security Technology , Prentice Hall(σελ 403)

[34] Asokan N. & Ginzboorg P., Key Agreement in Ad-Hoc Networks

[35] Bradbury D., Disable the Cable, Personal Computer World

[36] Gollmann D., Computer Security, John Wiley & Sons Inc.(σελ 336)

[37] Hermelin M. & Nyberg κ., Correlation Properties of the Bluetooth Combiner

[38] Joronen J., Bluetooth Tunkee Piireihin, Prosessori

[39] Schneier B.,Applied Cryptography, 2nd Ed, John *Wiley* & Sons Inc,(σελ 758)

[40] J.C. Haartsen ET, "The Bluetooth Radio system" , Σ. 28-36.

[41] M. Albrecht et Al, "IP Services Over Bluetooth"

[42] 0, Miklos et al, "performance aspects of Bluetooth scatternet formation"

[43] P. Bhagwat, L. Tassiulas, και R. LaMaire, "Distributed topology construction of Bluetooth personal area networks".

[44]. Specification of the Bluetooth System, volume IB

[45]. "Specification of the Bluetooth System", Specification Volume 1, v.I.0B

[46]. "Specification of the Bluetooth System", Specification Volume 2, v.I.0B