ΑΝΑΛΥΣΗ ΑΣΦΑΛΕΙΑΣ ΕΠΙΠΕΔΟΥ ΣΥΝΔΕΣΗΣ ΔΕΔΟΜΕΝΩΝ ΓΙΑ ΔΙΚΤΥΑ ΤΕΧΝΟΛΟΓΙΑΣ BLUETOOTH

ΑΡΤΕΜΙΟΣ Γ. ΒΟΓΙΑΤΖΗΣ
Ερευνητής Πληροφορικής
ΔΗΜΗΤΡΙΟΣ Ν. ΣΕΡΠΑΝΟΣ
Αναπληρωτής Καθηγητής Πανεπιστημίου Πατρών

ΠΕΡΙΛΗΨΗ

Το Bluetooth είναι μία αναδυόμενη τεχνολογία για την υλοποίηση ασύρματων τοπικών δικτύων (WLAN). Ένα συγκριτικό πλεονέκτημα του έναντι άλλων αρχιτεκτονικών WLAN είναι η συμπερίληψη αρχιτεκτονικής ασφάλειας στην προτυποποίηση του. Επιπλέον, οι προδιαγραφές, η αρχιτεκτονική ασφάλειας αλλά και οι αλγόριθμοι κρυπτογράφησης είναι δημοσίως γνωστά, επιτρέποντας την αποδοτική ανάλυση και αξιολόγηση των προδιαγραφών από τους ειδικούς. Στην παρούσα εργασία αναλύουμε την αρχιτεκτονική ασφάλειας, η οποία θεωρείται καλοσχεδιασμένη και εύρωστη. Συγκεκριμένα, εντοπίζουμε και ταξινομούμε τα προβλήματα ασφάλειας, που υπάρχουν στο επίπεδο σύνδεσης, ένα ζωτικό σημείο στην αρχιτεκτονική ασφάλειας του Bluetooth, και παρουσιάζουμε σημεία απειλής για την ιδιωτικότητα του χρήστη, την ακεραιότητα και μυστικότητα των δεδομένων, τον έλεγχο πρόσβασης, τη διαθεσιμότητα του δικτύου και την αυθεντικότητα της πηγής. Επίσης, παρουσιάζουμε ρεαλιστικά σενάρια χρήσης, τα οποία οδηγούν σε επιθέσεις άρνησης υπηρεσίας για όλο το δίκτυο. Για λόγους πληρότητας, καλύπτουμε και τους κρυπτογραφικούς αλγόριθμους, που χρησιμοποιούνται, παρουσιάζοντας τα νεότερα ευρήματα σχετικά με τη κρυπτανάλυσή τους (μαθηματική και υλικού). Οι αδυναμίες ασφάλειας του Bluetooth, που περιγράφονται σε αυτή την εργασία, υποδεικνύουν ότι παρά την καλοσχεδιασμένη αρχιτεκτονική ασφάλειας, πρέπει να δίνεται ιδιαίτερη προσοχή στη σχεδίαση ασύρματων δικτύων Bluetooth για εφαρμογές με υψηλές απαιτήσεις ασφάλειας.

Index Terms — Bluetooth, security, WLAN.

1. ΕΙΣΑΓΩΓΗ

Τα τελευταία χρόνια έχουν αρχίσει να υλοποιούνται οικονομικά και χαμηλής ενέργειας δίκτυα επικοινωνιών τοπικής εμβέλειας, βασισμένα σε ραδιοσυχνότητες. Τα ασύρματα δίκτυα δίνουν μεγάλη ευελιξία υλοποίησης, καθώς δεν απαιτούν καλωδίωση. Αντίθετα, μπορούν να εκμεταλλευτούν με κατάλληλες πύλες (gateways) την υπάρχουσα καλωδίωση για να επεκτείνουν την εμβέλεια δράσης τους. Ουσιώδες ζήτημα στα ασύρματα δίκτυα είναι η διασφάλιση του απορρήτου των επικοινωνιών, καθώς το μέσο μετάδοσης (ο αέρας) είναι άμεσα προσβάσιμο από όλους.

Οι τεχνολογίες των ασύρματων δικτύων χωρίζονται σε τρεις κατηγορίες, με βασικό κριτήριο την απόσταση της ασύρματης συσκευής από το σταθμό βάσης, το οποίο αναφέρεται και ως σημείο πρόσβασης (access point). Πρόκειται για τα προσωπικά ασύρματα δίκτυα μικρής εμβέλειας (Wireless Personal Area Network ή WPAN), όπου κύριος εκπρόσωπος είναι η τεχνολογία Bluetooth, τα τοπικά ασύρματα δίκτυα (Wireless LAN ή WLAN), με κυριότερους εκπροσώπους τις τεχνολογίες IEEE 802.11, IEEE 802.11b (γνωστή και ως Wi-Fi), IEEE 802.11a, HyperLAN/2 (Wi-Fi5) και HomeRF και, τέλος, τα ασύρματα δίκτυα ευρείας κλίμακας (Wireless WAN ή WWAN), με κυριότερους εκπροσώπους τις τεχνολογίες GSM, GPRS και 3G.

Το Bluetooth αναπτύσσεται από μία ομάδα, γνωστή με το όνομα «Bluetooth Special Interest Group» (Bluetooth SIG, Inc) [1], η οποία δημιουργήθηκε το Μάιο του 1998. Τα ιδρυτικά μέλη ήταν οι εταιρείες Ericsson, Nokia, Intel, IBM και Toshiba. Έκτοτε, σχεδόν όλες οι μεγάλες εταιρείες της βιομηχανίας των τηλεπικοινωνιών, όπως για παράδειγμα οι 3Com, Lucent, Microsoft και Motorola, προσχώρησαν στο Bluetooth SIG, το οποίο σήμερα αριθμεί συνολικά 2.500 μέλη. Η πρώτη έκδοση της προδιαγραφής Bluetooth εγκρίθηκε το καλοκαίρι του 1999, ενώ η τελευταία έκδοση 1.1 εγκρίθηκε το Φεβρουάριο του 2001 [2] [3].

Τα όρια μεταξύ προσωπικών και τοπικών ασύρματων δικτύων (WPAN και WLAN) δεν είναι διακριτά. Ο διαχωρισμός είναι μάλλον τεχνητός, καθώς οι τεχνολογίες WLAN καλύπτουν πολύ ικανοποιητικά τις απαιτήσεις των WPAN. Το κόστος ανάπτυξης ενός δικτύου με τεχνολογία Bluetooth είναι άμεσα συγκρίσιμο με αυτό ενός WLAN, ενώ τα WLAN προσφέρουν πολύ μεγαλύτερους ρυθμούς μετάδοσης (π.χ., 11 Mbps το IEEE 802.11b). Για

το λόγο αυτό, η τεχνολογία Bluetooth καλείται να ανταγωνιστεί και τεχνολογίες WLAN. Παραπέμπουμε τον αναγνώστη στα [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19] για τις απόψεις σχετικά με τη θέση της τεχνολογίας Bluetooth στην αγορά των ασύρματων δικτύων.

Οι χρήστες έχουν αυξημένο βαθμό ανησυχίας για θέματα ασφάλειας που εγείρονται σε ασύρματες μεταδόσεις. Συνήθως, αυτές οι ανησυχίες επιβραδύνουν σημαντικά τη μαζική αποδοχή μίας νέας τεχνολογίας, κυρίως ασύρματης όπου ο φόβος της παραβίασης της ιδιωτικότητας (privacy) είναι ιδιαίτερα υψηλός. Έχοντας υπόψη τις ανησυχίες των χρηστών, το Bluetooth SIG όρισε δημοσίως την προδιαγραφή της τεχνολογίας και της ασφάλειάς της [2],[3]. Το Bluetooth SIG αλλά και ανεξάρτητοι ερευνητές έχουν περιγράψει την αρχιτεκτονική ασφάλειας που ενσωματώνεται στην προδιαγραφή του Bluetooth, σε διάφορα επίπεδα λεπτομέρειας για ευκολότερη κατανόηση [21],[22],[23],[24].

Σκοπός της εργασίας αυτής είναι η εξέταση της ασφάλειας, που προσφέρει η τεχνολογία Bluetooth. Παρουσιάζουμε τα κύρια χαρακτηριστικά της αρχιτεκτονικής και την συγκρίνουμε με παρόμοιες τεχνολογίες. Η τεχνολογία Bluetooth προδιαγράφει εγγενώς μηχανισμούς για τη διασφάλιση της μυστικότητας των επικοινωνιών. Εξετάζουμε τους μηχανισμούς και αξιολογούμε το επίπεδο ασφάλειας που προσφέρουν, εστιάζοντας στην κάλυψη των απαιτήσεων για τη χρήση της σε βιομηχανικά συστήματα.

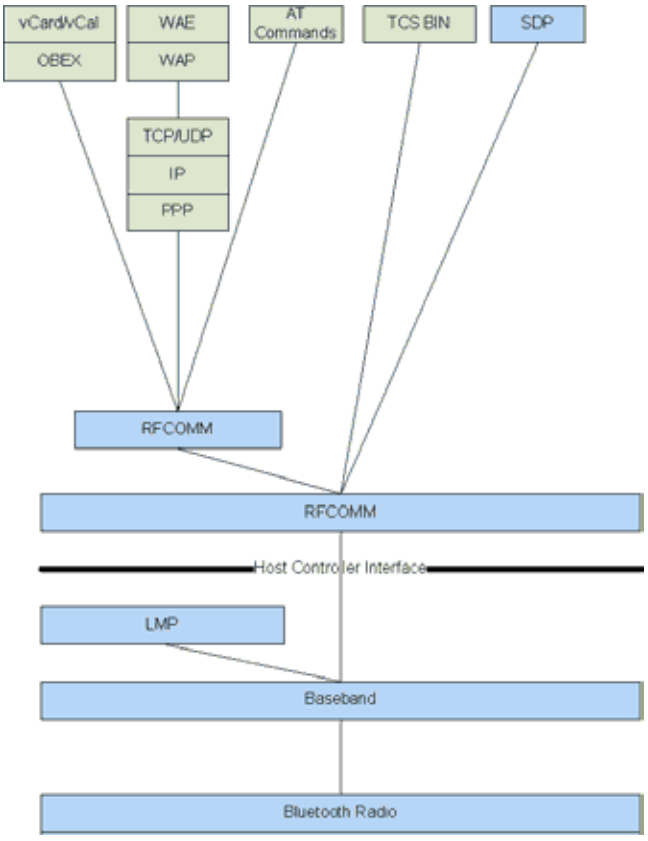
2. Η ΤΕΧΝΟΛΟΓΙΑ BLUETOOTH

Στο Σχήμα 1 παρουσιάζεται η στοίβα πρωτοκόλλων, που προδιαγράφει η αρχιτεκτονική της τεχνολογίας Bluetooth. Τα πρωτόκολλα που αφορούν στην τεχνολογία Bluetooth σημειώνονται με μπλε (θαλασσί) χρώμα. Συνοπτικά η λειτουργικότητα των πρωτοκόλλων είναι η εξής:

- Baseband: επιτρέπει τη φυσική σύνδεση μεταξύ δύο συσκευών Bluetooth.
- L2CAP (Logical Link Control and Adaptation Protocol): ενθυλακώνει τα πρωτόκολλα υψηλότερου επιπέδου για τη μετάδοσή τους μέσω του Baseband.
- LMP (Link Manager Protocol): δημιουργεί μία σύνδεση μεταξύ δύο συσκευών και καθορίζει το μέγεθος πακέτου μετάδοσης, τις υπηρεσίες ασφάλειας και τη διαχείριση

των κλειδιών κρυπτογράφησης που θα χρησιμοποιηθούν.

- SDP (Service Discovery Protocol): χρησιμοποιείται από τις συσκευές τεχνολογίας Bluetooth για τη συλλογή πληροφοριών σχετικά με τους τύπους συσκευών, υπηρεσίες και προδιαγραφές υπηρεσιών που βρίσκονται στην εμβέλεια τους, ώστε να είναι εφικτή η δημιουργία συνδέσεων μεταξύ αυτών.



Σχήμα 1: *Στοίβα πρωτοκόλλων Bluetooth.*

Επίσης, το πρότυπο του Bluetooth ορίζει και τη διεπαφή HCI (Host Controller Interface), μεταξύ του Baseband και του L2CAP, η οποία είναι απαραίτητη για την επικοινωνία των διεργασιών λογισμικού του L2CAP με τις διεργασίες του LMP και των άλλων ελεγκτών του υλικού (hardware).

Η αρχιτεκτονική πρωτοκόλλων της τεχνολογίας Bluetooth έχει ορισθεί λαμβάνοντας υπόψη και άλλα πρωτόκολλα που ήδη χρησιμοποιούνται, όπως για παράδειγμα τα WAP, WAE, TCP/UDP/IP, PPP, vCard, vCal και IrMC. Επίσης, υποστηρίζονται πρωτόκολλα όπως το RFCOMM (για ασύρματη επικοινωνία) και οι εντολές AT (για πρωτόκολλα προσαρμογέων τηλεφωνίας). Όλα αυτά τα πρωτόκολλα έχουν ενσωματωθεί στην προδιαγραφή του Bluetooth, ώστε να μπορεί το Bluetooth να ενσωματωθεί σε ήδη υπάρχουσες εφαρ-

μογές και πρωτόκολλα μεταφοράς δεδομένων, επιτυγχάνοντας ευρεία εξάπλωση της τεχνολογίας. Επίσης, η δομή αυτή των πρωτοκόλλων επιτρέπει την υλοποίηση ανεξάρτητων μηχανισμών ασφάλειας στο επίπεδο εφαρμογής, αν απαιτείται, και στα χαμηλότερα επίπεδα, όπου εκτελούνται τα πρωτόκολλα του Bluetooth.

2.1. Τεχνολογικά Χαρακτηριστικά

Το Bluetooth σχεδιάστηκε με γνώμονα την ευρωστία (robustness) και τη χαμηλή κατανάλωση. Η υλοποίηση βασίζεται σε ένα ενσωματωμένο ραδιοπομποδέκτη χαμηλής κατανάλωσης και υψηλής απόδοσης. Οι συσκευές Bluetooth κατηγοριοποιούνται σε τρεις διαφορετικές κλάσεις, ανάλογα με την ισχύ του ραδιοπομποδέκτη: συσκευή κλάσης 3 έχει ισχύ εκπομπής 1 mW και εμβέλεια 0.10-10 μέτρα, συσκευή κλάσης 2 έχει ισχύ εκπομπής 1-2.5 mW και εμβέλεια 10 μέτρα, ενώ συσκευή κλάσης 1 έχει ισχύ εκπομπής έως 100 mW και εμβέλεια έως 100 μέτρα.

Το Bluetooth χρησιμοποιεί τη συχνότητα των 2.4 GHz, στη ζώνη συχνοτήτων ISM (Industrial, Scientific, Medical), όπου δουλεύουν οι περισσότεροι φούρνοι μικροκυμάτων, ώστε να είναι ελεύθερη (unlicensed) η χρήση της. Τη συγκεκριμένη ζώνη συχνοτήτων χρησιμοποιούν, επίσης, οι τεχνολογίες Wi-Fi, HomeRF και IEEE 802.15. Καθώς η συγκεκριμένη ζώνη συχνοτήτων εμφανίζεται αρκετά «συνωστισμένη», το Bluetooth χρησιμοποιεί την τεχνική μεταπήδησης συχνότητας (frequency hopping) με ρυθμό 1.600 φορές το δευτερόλεπτο για να αποφύγει το συνωστισμό. Η μεταπήδηση συχνότητας υλοποιείται με GFSK (Gaussian Frequency Shift Keying).

Ο θεωρητικά μέγιστος ρυθμός μετάδοσης δεδομένων είναι 1 Mbps, ο οποίος όμως περιορίζεται σε 721 Kbps, εξαιτίας της χρήσης κώδικα διόρθωσης λαθών τύπου FEC (Forward Error Correction). Ο ρυθμός αυτός αφορά ασύμμετρη επικοινωνία, όπου η αποστολή γίνεται με ρυθμό 721 Kbps και η λήψη με ρυθμό 57 Kbps. Αν υλοποιείται συμμετρική επικοινωνία, ο ρυθμός μειώνεται σε 423,6 Kbps. Πειραματικές μετρήσεις έχουν δείξει ότι ο ρυθμός μετάδοσης που επιτυγχάνεται κυμαίνεται μεταξύ 30 και 400 Kbps. Αυτό οφείλεται στο γεγονός ότι το μέγιστο εύρος ζώνης διαμοιράζεται μεταξύ των κόμβων ενός δικτύου Bluetooth.

Οι συσκευές Bluetooth επικοινωνούν δημιουργώντας δίκτυα ad hoc τοπικής εμβέλειας,

τα οποία αναφέρονται ως piconet στην ορολογία του Bluetooth. Σε ένα piconet υποστηρίζονται έως οκτώ συσκευές, και έως δέκα δίκτυα piconet μπορούν να ενωθούν μεταξύ τους για να σχηματήσουν ένα μεγαλύτερο δίκτυο, το οποίο ονομάζεται scatternet.

Σχετικά με τη μεθοδολογία μετάδοσης, το Bluetooth χρησιμοποιεί ένα συνδυασμό τεχνολογίας μεταγωγής κυκλώματος και μεταγωγής πακέτου (circuit and packet switching). Το Bluetooth μπορεί να υποστηρίξει είτε ένα ασύγχρονο κανάλι δεδομένων και τρία ταυτόχρονα σύγχρονα κανάλια φωνής, είτε ένα κανάλι, το οποίο μεταφέρει ταυτόχρονα δεδομένα με ασύγχρονο τρόπο και φωνή με σύγχρονο τρόπο. Σε ένα scatternet, ο μέγιστος συνολικός ρυθμός μετάδοσης δεδομένων είναι 10 Mbps ή 20 κανάλια φωνής. Για τη μετάδοση φωνής, χρησιμοποιείται ένα εύρωστο σχήμα κωδικοποίησης φωνής ρυθμού 64 Kbps. Για να υποστηρίξει αυτούς τους ρυθμούς μεταγωγής, το Bluetooth χρησιμοποιεί ένα συνδυασμό από πρωτόκολλο μεταγωγής πακέτων, τεχνική μεταπήδησης συχνότητας και προηγμένο σχήμα κωδικοποίησης φωνής. Επίσης, υποστηρίζει τη βαθμιαία επιβράδυνση των ρυθμών μετάδοσης δεδομένων και φωνής, όταν υπάρχει μεγάλος συνωστισμός στις ραδιοσυχνότητες που χρησιμοποιούνται.

2.2. Σενάρια χρήσης

Η τεχνολογία Bluetooth μπορεί να χρησιμοποιηθεί για τη διασύνδεση σχεδόν οποιωνδήποτε συσκευών. Ένα τυπικό παράδειγμα είναι η διασύνδεση ενός PDA ή ενός φορητού υπολογιστή με ένα κινητό τηλέφωνο. Με τον τρόπο αυτό μπορούμε να δημιουργούμε απομακρυσμένες συνδέσεις με προσωπικές συσκευές, χωρίς να χρειάζεται να βγάζουμε για παράδειγμα το τηλέφωνό μας από την τσέπη μας και χωρίς συνδέσεις με καλώδια. Ένα σημαντικό πλεονέκτημα του Bluetooth σε τέτοιου είδους εφαρμογές, είναι ότι δεν απαιτείται οπτική επαφή μεταξύ των συσκευών, όπως συμβαίνει για παράδειγμα με την τεχνολογία υπέρυθρων ακτινών (Infrared).

Η δημιουργία δικτύων piconet είναι χρήσιμη για παράδειγμα σε μία εταιρική συνάντηση, όπου όλοι οι συμμετέχοντες έχουν φορητούς υπολογιστές με υποστήριξη Bluetooth και διαμοιράζονται αρχεία μεταξύ τους [4]. Σε ένα άλλο σενάριο, ένα τηλέφωνο με υποστήριξη Bluetooth μπορεί να εξυπηρετεί τρεις διαφορετικές λειτουργίες: στο γραφείο χρησιμοποιείται για τις εσωτερικές κλήσεις (χωρίς χρέωση από τον πάροχο τηλεφωνίας),

στο σπίτι ως ασύρματο τηλέφωνο (όπως τα γνωστά τηλέφωνα DECT, με χρέωση κατά τον πάροχο σταθερής τηλεφωνίας) και σε εξωτερικούς χώρους ως κινητό τηλέφωνο (με χρέωση κατά τον πάροχο κινητής τηλεφωνίας).

Σε ένα άλλο σενάριο δημιουργίας piconet, ο φορητός υπολογιστής μπορεί να λαμβάνει ηλεκτρονικά μηνύματα, ενώ βρίσκεται στην τσάντα του κατόχου και να ειδοποιεί τον παραλήπτη των μηνυμάτων με ένα μήνυμα SMS στο κινητό του (το οποίο επίσης υποστηρίζει τεχνολογία Bluetooth).

Ένα τελευταίο σενάριο χρήσης, αφορά στον αυτόματο συγχρονισμό των δεδομένων μεταξύ διάφορων συσκευών (π.χ. σταθμού εργασίας, φορητού υπολογιστή, υπολογιστή παλάμης, PDA και κινητού τηλεφώνου), χωρίς να απαιτείται κάποια ενέργεια από το χρήστη και η οποιαδήποτε διασύνδεση μεταξύ όλων αυτών των συσκευών με καλώδια [20].

Η τεχνολογία Bluetooth παρουσιάστηκε στην αγορά με σκοπό να προσφέρει την ευκολία που προσφέρουν οι ασύρματες επικοινωνίες στη δημιουργία δικτύων επικοινωνίας τοπικής εμβέλειας. Η ευκολία διασύνδεσης σε συνδυασμό με το χαμηλό κόστος είναι τα κύρια πλεονεκτήματα της τεχνολογίας Bluetooth, συγκρινόμενη με τις ενσύρματες τεχνολογίες. Οι συσκευές, στις οποίες απευθύνεται η τεχνολογία, είναι τα περιφερειακά προσωπικών υπολογιστών και οι ενσωματωμένες συσκευές (embedded).

Στην παρούσα χρονική περίοδο, οι προβλέψεις του Bluetooth SIG δεν έχουν επιβεβαιωθεί. Ένας σημαντικός λόγος για αυτό είναι το γεγονός ότι τα ολοκληρωμένα κυκλώματα, που υλοποιούν την τεχνολογία Bluetooth, παραμένουν πολύ ακριβά. Ενώ οι αρχικές εκτιμήσεις, κατά το σχεδιασμό της τεχνολογίας, αναφέρονταν σε ολοκληρωμένα με κόστος 5 δολλάρια Η.Π.Α., τα πρώτα προϊόντα που παρουσιάστηκαν είχαν κόστος 150-200 δολλάρια, ενώ αυτή τη στιγμή κυμαίνονται στα 20-50 δολλάρια και είναι επομένως αρκετά ακριβά για ευρεία χρήση.

Για την ασύρματη διασύνδεση περιφερειακών συσκευών, η τεχνολογία υπέρυθρων IrDA διατηρεί την ηγετική της θέση, έχοντας μία εγκατεστημένη βάση 150.000.000 μονάδων και ρυθμό αύξησης 40% ετησίως. Το κόστος ολοκλήρωσης σε μία συσκευή είναι 2 δολλάρια, ενώ μία μονάδα μπορεί να έχει κόστος ακόμη και 1 δολλάριο. Η τεχνολογία IrDA, επίσης, προσφέρει σημαντικά υψηλότερους ρυθμούς διαμεταγωγής, 4-16 Mbps,

ενώ η τεχνολογία Bluetooth 1 Mbps της τεχνολογίας. Ωστόσο, η IrDA δεν υποστηρίζει μετάδοση φωνής (voice channels) και έχει κατευθυνόμενη λήψη σε ακτίνα 30 μοιρών [7].

3. Η ΑΣΦΑΛΕΙΑ ΤΟΥ BLUETOOTH

Περιγράφουμε την αρχιτεκτονική ασφάλειας του Bluetooth σε επίπεδα, αντίστοιχα με το μοντέλο αναφοράς OSI. Στην πρώτη ενότητα περιγράφουμε την αρχιτεκτονική ασφάλειας του Bluetooth, τα συστατικά της και τον τρόπο που αυτά αλληλεπιδρούν μεταξύ τους για την παροχή υπηρεσιών ασφάλειας, ενώ στη δεύτερη επικεντρώνουμε την περιγραφή στο πρωτόκολλο ασφάλειας στο επίπεδο σύνδεσης δεδομένων, αφού αυτό το επίπεδο είναι υπεύθυνο για την υποστήριξη ασφαλούς επικοινωνίας μεταξύ συσκευών Bluetooth.

3.1. Αρχιτεκτονική Ασφάλειας

Τα θέματα ασφάλειας στην τεχνολογία Bluetooth αντιμετωπίζονται σε πολλαπλά επίπεδα. Στο επίπεδο φυσικής σύνδεσης, προδιαγράφεται η χρήση της τεχνικής μεταπήδησης συχνότητας (frequency hopping) με ρυθμό 1.600 φορές το δευτερόλεπτο, σύμφωνα με μία μοναδική για κάθε συσκευή ψευδοτυχαία ακολουθία αριθμών. Έτσι δεν είναι δυνατή η παρακολούθηση της επικοινωνίας μεταξύ δύο συσκευών τεχνολογίας Bluetooth, χωρίς τη γνώση της γεννήτριας των τυχαίων αριθμών και τον απόλυτο συγχρονισμό με αυτή.

Στο επίπεδο συνδέσμου (link layer), το πρωτόκολλο LMP είναι η «καρδιά» της ασφάλειας του Bluetooth. Υποστηρίζει μονόδρομη και αμοιβαία ταυτοποίηση συσκευής (device authentication) και εγκαθίδρυση κρυπτογραφημένης επικοινωνίας (η διαδικασία ταυτοποίησης και κρυπτογράφησης θα εξετασθεί αναλυτικά σε επόμενη ενότητα).

Η προδιαγραφή του Bluetooth ορίζει τρεις τρόπους ασφάλειας (security mode) για τις συσκευές:

- Security Mode 1: μία συσκευή Bluetooth δεν ορίζει οποιαδήποτε λειτουργία ασφάλειας. Η συσκευή θεωρείται ότι είναι σε «αναζήτηση» (discovery mode), επιτρέποντας σε άλλες συσκευές να εγκαθιδρύσουν επικοινωνία μαζί της. Είναι ο πλέον ανασφαλής τρόπος λειτουργίας.
- Security Mode 2: το επίπεδο ασφάλειας οριοθετείται αφού εγκαθιδρυθεί μία σύνδε-

ση στο επίπεδο L2CAP. Με τον τρόπο αυτό μπορούν να οριστούν ευέλικτες πολιτικές ασφάλειας για την επικοινωνία, οι οποίες μπορούν να οριστούν από το επίπεδο εφαρμογής.

- Security Mode 3: επιβάλλει διαδικασίες ταυτοποίησης και κρυπτογράφησης στο χαμηλότερο επίπεδο, το Baseband, πριν ακόμη δημιουργηθεί μία σύνδεση μεταξύ των συσκευών. Η διαδικασία κρυπτογράφησης στο επίπεδο Baseband διατηρείται και μετά τη δημιουργία της σύνδεσης. Ο τρόπος αυτός ελέγχεται συνήθως από το επίπεδο LMP και παρέχει το υψηλότερο επίπεδο ασφάλειας.

Η προδιαγραφή του Bluetooth επιτρέπει τον ορισμό επιπρόσθετων επιπέδων ασφάλειας, τόσο για τις ίδιες τις συσκευές, όσο και για τις υπηρεσίες που παρέχουν. Σε αυτό το πλαίσιο και σε επίπεδο συσκευής, μία απομακρυσμένη συσκευή που προσπαθεί να δημιουργήσει μία σύνδεση μπορεί να θεωρείται:

- Έμπιστη: να έχει πρόσβαση σε όλες τις τοπικές υπηρεσίες, για τις οποίες έχει οριστεί ανάλογη σχέση εμπιστοσύνης (trust relationship).
- Αναξιόπιστη: να έχει περιορισμένη πρόσβαση στις τοπικές υπηρεσίες. Συνήθως τέτοιες συσκευές δε διαθέτουν μία μόνιμη σχέση εμπιστοσύνης με τις υπόλοιπες συσκευές.

Στο επίπεδο υπηρεσιών, ορίζονται τρία επίπεδα ασφάλειας:

- Υπηρεσίες που απαιτούν εξουσιοδότηση (authorization) και ταυτοποίηση (authentication).
- Υπηρεσίες που απαιτούν μόνο ταυτοποίηση. Η εξουσιοδότηση δεν είναι αναγκαία.
- Υπηρεσίες ελεύθερες προς όλους. Δεν απαιτείται εξουσιοδότηση ή ταυτοποίηση για την παροχή της υπηρεσίας.

Πρέπει να τονισθεί ότι οι προδιαγραφές της τεχνολογίας Bluetooth ορίζουν τα επίπεδα ασφάλειας και εμπιστοσύνης σε σχέση με τις συσκευές και τις υπηρεσίες που προσφέρουν και όχι σε σχέση με το χρήστη. Έτσι, μία απομακρυσμένη συσκευή, η οποία έχει την απαραίτητη εξουσιοδότηση και ταυτοποίηση, θα έχει πρόσβαση σε μία τοπική υπηρεσία, ανεξάρτητα από το ποιος τη χειρίζεται. Αυτό συμβαίνει, διότι οι υπηρεσίες ασφάλειας που προδιαγράφονται αφορούν το επίπεδο συνδέσμου, στο οποίο δε συμπεριλαμβάνονται οι εφαρμογές και οι χρήστες, και είναι επομένως αδύνατο να

έχουμε εξουσιοδότηση και ταυτοποίηση ανά εφαρμογή ή και χρήστη. Ωστόσο, οι προδιαγραφές είναι αρκετά ευέλικτες, ώστε να μπορούν οι εφαρμογές, που χρησιμοποιούν το Bluetooth ως υποδομή, να υλοποιούν αντίστοιχα σχήματα ταυτοποίησης και εξουσιοδότησης στο επίπεδο τους.

Η γεννήτρια τυχαίων αριθμών είναι αναπόσπαστο τμήμα της αρχιτεκτονικής ασφάλειας, καθώς πολλά χαρακτηριστικά ασφάλειας στηρίζονται στην παραγωγή τυχαίων αριθμών. Η προδιαγραφή της τεχνολογίας Bluetooth δεν ορίζει κάποια συγκεκριμένη γεννήτρια αριθμών αλλά επιβάλλει την ύπαρξή της σε κάθε συσκευή. Αυτό είναι λογικό, καθώς αναμένεται ότι το Bluetooth θα ενσωματωθεί σε πληθώρα συσκευών με πολύ διαφορετικά χαρακτηριστικά ως προς την επεξεργαστική και αποθηκευτική ισχύ τους. Στα προϊόντα που έχουν παρουσιαστεί μέχρι σήμερα χρησιμοποιούνται γεννήτριες ψευδοτυχαίων αριθμών και υλοποιούνται με λογισμικό. Η προδιαγραφή ορίζει τις ακόλουθες γενικές απαιτήσεις για τη γεννήτρια τυχαίων αριθμών:

1. Οι αριθμοί που παράγονται να είναι μη επαναλαμβανόμενοι (non-repeating).
2. Οι αριθμοί να παράγονται με τυχαίο τρόπο (randomly generated).

Η έκφραση «μη επαναλαμβανόμενοι» οριοθετείται κατά τη διάρκεια ζωής του κλειδιού ταυτοποίησης, στο οποίο θα αναφερθούμε στη συνέχεια. Η έκφραση «να παράγονται με τυχαίο τρόπο» οριοθετείται, ώστε να είναι αδύνατο να προβλέψει κανείς την επόμενη έξοδο της γεννήτριας με πιθανότητα μεγαλύτερη του $\left(1/2\right)$, δηλαδή για μία ακολουθία L δυαδικών ψηφίων, η πιθανότητα σωστής πρόβλεψης της ακολουθίας να είναι $\left(1/2\right)^L$.

Αν το πρωτόκολλο LMP είναι η «καρδιά» της ασφάλειας του Bluetooth, ο Διαχειριστής Ασφάλειας (Security Manager) είναι ο «εγκέφαλος» του συστήματος. Ο Διαχειριστής Ασφάλειας αποφασίζει ποιες πολιτικές ασφάλειας πρέπει να εφαρμοσθούν, όταν υπάρχει μία αίτηση σύνδεσης, τόσο για εξερχόμενες όσο και για εισερχόμενες. Οι αποφάσεις αυτές βασίζονται στον τύπο της υπηρεσίας, στον τύπο της συσκευής και στο αν μία συσκευή θεωρείται έμπιστη ή όχι. Οι αποφάσεις αφορούν στην ταυτοποίηση σε επίπεδο εφαρμογής, την κρυπτογράφηση της επικοινωνίας και άλλες πολιτικές πρόσβασης. Ο Διαχειριστής Ασφάλειας για να μπορεί να λαμβάνει αποφάσεις, χρησιμοποιεί δύο βάσεις, τη Βάση Συσκευών (Device Database) και τη Βάση Υπηρεσιών (Service Database). Η

Βάση Συσκευών διατηρεί πληροφορίες για τις συσκευές: τον τύπο τους, αν θεωρούνται έμπιστες ή όχι και το μήκος του κλειδιού που χρησιμοποιείται για την κρυπτογράφηση σε επίπεδο σύνδεσης. Η Βάση Υπηρεσιών διατηρεί πληροφορίες σχετικά με τις απαιτήσεις των υπηρεσιών για ταυτοποίηση, εξουσιοδότηση και κρυπτογράφηση.

Όταν μία απομακρυσμένη υπηρεσία αιτείται πρόσβαση σε μία τοπική υπηρεσία, ακολουθείται το εξής σενάριο από το Διαχειριστή Ασφάλειας:

1. Η απομακρυσμένη συσκευή αιτείται την πρόσβαση.
2. Η αίτηση σύνδεσης λαμβάνεται από το πρωτόκολλο L2CAP.
3. Το L2CAP ζητά από το Διαχειριστή Ασφάλειας να εγκρίνει το δικαίωμα πρόσβασης.
4. Ο Διαχειριστής Ασφάλειας αναζητά τις σχετικές πληροφορίες στη Βάση Συσκευών και στη Βάση Υπηρεσιών.
   α. Αν η συσκευή είναι έμπιστη, ο Διαχειριστής Ασφάλειας μπορεί να ζητήσει την ταυτοποίηση ή/και εξουσιοδότηση σε επίπεδο συνδέσμου.
   β. Αν η συσκευή δεν είναι έμπιστη, τότε ο Διαχειριστής Ασφάλειας μπορεί είτε να τερματίσει άμεσα τη σύνδεση ή να επιβάλει την ταυτοποίησή της. Η ταυτοποίηση θα συμβεί καταρχήν στο επίπεδο συνδέσμου. Αν το προβλέπει η πολιτική ασφάλειας της υπηρεσίας, μετά την ταυτοποίηση σε επίπεδο συνδέσμου, μπορεί να γίνει ταυτοποίηση σε επίπεδο εφαρμογής. Στην προδιαγραφή προβλέπονται και άλλα σχήματα ταυτοποίησης, πέραν του επιπέδου εφαρμογής, για μεγαλύτερη ευελιξία.
5. Ο Διαχειριστής Ασφάλειας στη συνέχεια αποφασίζει αν η πρόσβαση στην υπηρεσία απαιτεί κρυπτογράφηση σε επίπεδο συνδέσμου. Εάν ναι, τότε συμφωνούνται και ανταλλάσσονται τα κατάλληλα κρυπτογραφικά κλειδιά, στο επίπεδο του πρωτοκόλλου L2CAP, το οποίο είναι αρμόδιο. Σε κάθε περίπτωση, συνεχίζουμε με τη διαδικασία της εγκαθίδρυσης σύνδεσης.

Η μόνη εξαίρεση για το παραπάνω σενάριο αφορά στην περίπτωση, όπου η συσκευή που δέχεται την αίτηση είναι σε Security Mode 3. Τότε ο Διαχειριστής Ασφάλειας στο βήμα 4 ζητά από το πρωτόκολλο LMP να ταυτοποιήσει τη συσκευή που αιτείται την υπηρεσία και να κρυπτογραφηθεί η επικοινωνία τους από αυτό το βήμα, αντί να γίνει προαιρετικά στο βήμα 5.

3.2. Ασφάλεια επιπέδου σύνδεσης δεδομένων

Στην ενότητα αυτή αναλύουμε τους μηχανισμούς ασφάλειας, που υλοποιούνται στο επίπεδο συνδέσμου, δηλαδή στο πρωτόκολλο LMP. Το πρωτόκολλο αυτό παρέχει την υπηρεσία ταυτοποίησης μίας απομακρυσμένης συσκευής και την υπηρεσία κρυπτογραφημένης επικοινωνίας μεταξύ των συσκευών.

Η αρχιτεκτονική ασφάλειας της τεχνολογίας Bluetooth παρέχει ασφάλεια σε επίπεδο συσκευής και όχι σε επίπεδο εφαρμογής ή χρήστη, όπως αναφέρθηκε προηγουμένως. Η ταυτοποίηση των απομακρυσμένων συσκευών και η χρήση των καθορισμένων πολιτικών ασφάλειας για τις συσκευές είναι μείζονος σημασίας, καθώς οι αποφάσεις του Διαχειριστή Ασφάλειας σχετίζονται άμεσα με την ταυτότητα της απομακρυσμένης συσκευής και το επίπεδο εμπιστοσύνης που έχει οριστεί για αυτή. Για τους λόγους αυτούς, η αξιόπιστη παροχή υπηρεσιών ασφάλειας από το πρωτόκολλο LMP είναι η «καρδιά» της ασφάλειας της τεχνολογίας Bluetooth.

Για την υλοποίηση της ασφάλειας στο επίπεδο συνδέσμου, χρησιμοποιούνται τέσσερις οντότητες: μία δημόσια διεύθυνση, η οποία είναι μοναδική για κάθε συσκευή, δύο μυστικά κλειδιά και ένας τυχαίος αριθμός που παράγεται από τη γεννήτρια τυχαίων αριθμών και είναι μοναδικός για κάθε συνεδρία. Στον Πίνακα 1 συνοψίζονται οι οντότητες αυτές.

Το μυστικό κλειδί για την κρυπτογράφηση είναι ότι έχει μεταβλητό μέγεθος και μπορεί να οριστεί κατά περίπτωση σε πολλαπλάσια των 8 bit. Δύο λόγοι οδήγησαν σε αυτήν την επιλογή. Ο πρώτος αφορά στους περιορισμούς στη χρήση κρυπτογραφίας σε διάφορες χώρες και στους νόμους περί εξαγωγής τέτοιων συσκευών (π,χ. στις Η.Π.Α. υπάρχουν νόμοι που θέτουν περιορισμούς στις εξαγωγές προϊόντων που υποστηρίζουν ισχυρή κρυπτογράφηση). Ο δεύτερος αφορά στην πρόβλεψη για μελλοντική χρήση: κατά τη σύνταξη της προδιαγραφής το 1999, θεωρούνταν ότι ένα κλειδί μεγέθους 64 bit προσφέρει μεγάλο βαθμό ασφάλειας, ενώ με την πρόβλεψη έως και του διπλασιασμού αυτού του μεγέθους, η προδιαγραφή μεριμνά, ώστε να μην απαιτείται επανασχεδιασμός των κρυπτογραφικών αλγορίθμων για αρκετό διάστημα. Κάτι τέτοιο θα είχε τεράστιες οικονομικές συνέπειες και πολλά προϊόντα θα ήταν ασύμβατα μεταξύ τους.

Το μυστικό κλειδί για την ταυτοποίηση είναι εντελώς διαφορετικό από αυτό για την κρυπτογράφηση. Όπως αναφέρουμε παρακάτω, ένα νέο κλειδί κρυπτογράφησης παρά-

γεται από το κλειδί ταυτοποίησης κάθε φορά που απαιτείται η δημιουργία μίας κρυπτογραφημένης σύνδεσης. Το μυστικό κλειδί ταυτοποίησης θεωρείται στατικό, αφού δημιουργείται κατά την αρχικοποίηση της συσκευής και χρησιμοποιείται συνεχώς.

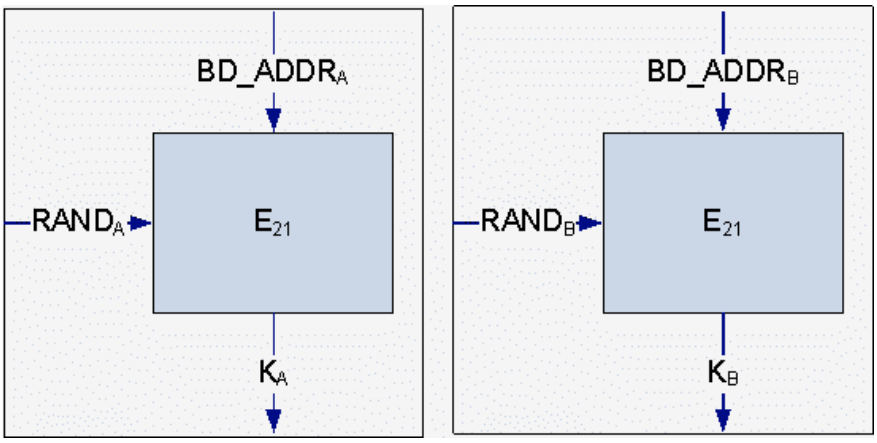
Πίνακας 1: *Οντότητες ασφάλειας επιπέδου συνδέσμου.*

Οντότητα	**Μέγεθος**
BD_ADDR	48 bit
Private user key for authentication	128 bit
Private user key for encryption	8-128 bit
RAND	128 bit

Το περιβάλλον χρήσης συσκευών τεχνολογίας Bluetooth είναι αρκετά δυναμικό, καθώς τα δίκτυα Bluetooth είναι ad hoc και δεν υπάρχει κάποια προκαθορισμένη υποδομή (infrastructure). Γι' αυτό το λόγο προδιαγράφονται διάφοροι τύποι κλειδιών, για διαφορετικές λειτουργίες. Για να γίνει κατανοητή η χρήση και η διαχείριση των κλειδιών, θα χρησιμοποιήσουμε ένα σενάριο λειτουργίας μίας συσκευής Bluetooth, ακολουθώντας τη συσκευή από τη γραμμή παραγωγής έως την εισαγωγή της σε ένα piconet.

Κάθε συσκευή τεχνολογίας Bluetooth έρχεται από τον κατασκευαστή με ένα Προσωπικό Αριθμό Αναγνώρισης (PIN), τη μοναδική διεύθυνσή της, BD_ADDR και ένα προκαθορισμένο μέγεθος μυστικού κλειδιού κρυπτογράφησης. Το μέγεθος του μυστικού κλειδιού κρυπτογράφησης τίθεται από τον κατασκευαστή της συσκευής και δεν μπορεί να αλλαχθεί από το επίπεδο εφαρμογής ή το χρήστη. Αυτό είναι αναγκαίο, ώστε να επιτυγχάνεται το απαραίτητο επίπεδο ασφάλειας στο επίπεδο του Bluetooth ανεξάρτητα από την εφαρμογή και για να αντιμετωπίζονται τα προβλήματα με την εξαγωγή των προϊόντων.

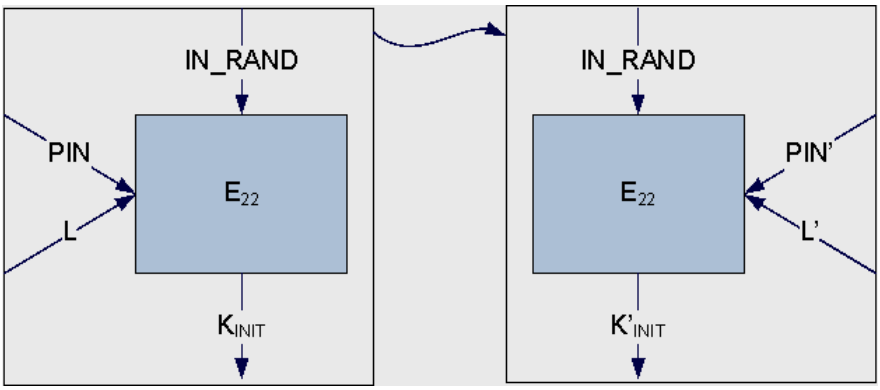
Την πρώτη φορά που η συσκευή τίθεται σε λειτουργία, παράγει το κλειδί μονάδας (unit key), χρησιμοποιώντας τη μοναδική διεύθυνση **BD_ADDR** και ένα τυχαίο αριθμό, **RAND**. Τα κλειδιά των συσκευών αυτών συμβολίζονται με $\mathbf{K_A}$ και $\mathbf{K_B}$ για τις δύο συσκευές που θα χρησιμοποιήσουμε στο παράδειγμά μας. Η διαδικασία παρουσιάζεται στο Σχήμα 2. Στα παρακάτω σχήματα, χρησιμοποιούμε το γράμμα **E**, πολλές φορές με κάποιο δείκτη. Αυτό συμβολίζει μία διαδικασία κρυπτογράφησης με έναν από τους αλγορίθμους κρυπτογράφησης που θα παρουσιαστούν στην επόμενη ενότητα. Εδώ, οι αλγόριθμοι μπορούν να θεωρηθούν ως απλές συναρτήσεις μετασχηματισμού των εισόδων τους.



Σχήμα 2: *Παραγωγή κλειδιού μονάδας.*

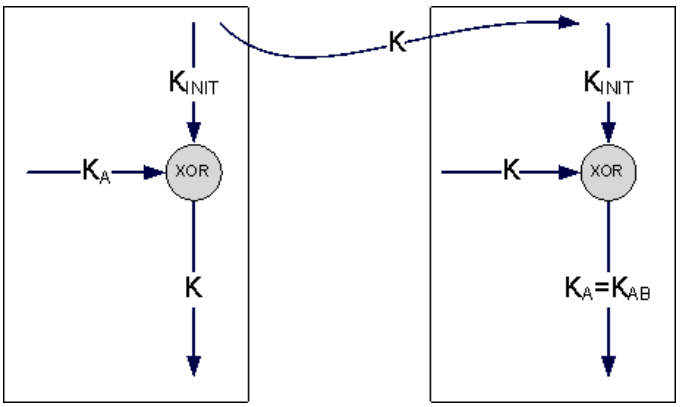
3.2.1. Δημιουργία Κλειδιού Σύνδεσης

Για να εισέλθει μία συσκευή σε ένα piconet, θα πρέπει ο χρήστης της να της ορίσει το ίδιο PIN που έχει οριστεί και στις άλλες συσκευές του δικτύου. Την πρώτη φορά που η συσκευή εισέρχεται στο piconet, λαμβάνει από την συσκευή ταυτοποίησης ένα τυχαίο αριθμό. Ο τυχαίος αριθμός, το PIN και το μήκος του PIN χρησιμοποιούνται για την παραγωγή ενός προσωρινού κλειδιού $\mathbf{K_{INIT}}$, το οποίο αναφέρεται ως προσωρινό κλειδί συνδέσμου (temporary link key), όπως φαίνεται στο Σχήμα 3.



Σχήμα 3: *Παραγωγή προσωρινού κλειδιού συνδέσμου.*

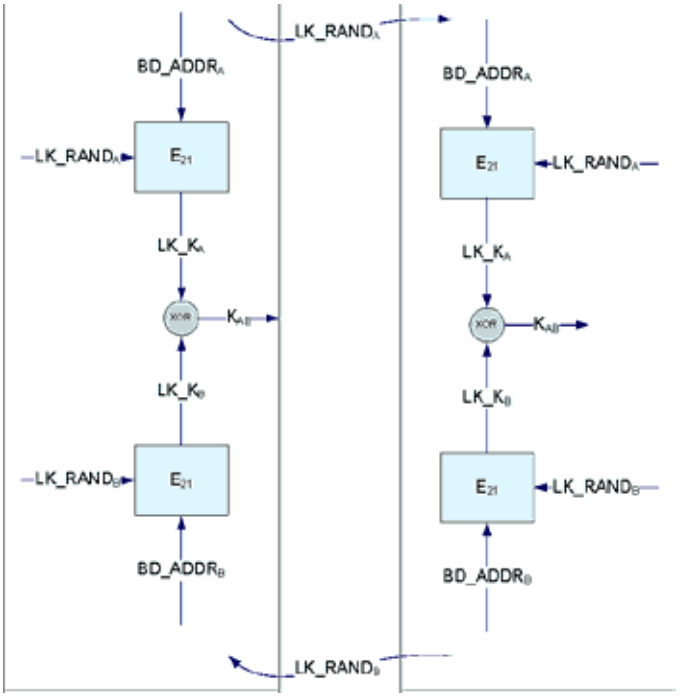
Το επόμενο βήμα είναι η δημιουργία ενός ημι-μόνιμου κλειδιού συνδέσμου. Γι' αυτή την περίπτωση θα πρέπει να ληφθούν υπόψη οι δυνατότητες της συσκευής **A**. Αν δεν έχει αρκετή μνήμη, τότε τίθεται ως κλειδί συνδέσμου το $\mathbf{K_{AB}}$, όπως περιγράφεται στο Σχήμα 4. Σε αυτήν την περίπτωση, το ημι-μόνιμο κλειδί συνδέσμου είναι το κλειδί μονάδας της «αδύναμης» συσκευής.



Σχήμα 4: *Κλειδί συνδέσμου για συσκευή μικρής μνήμης.*

Αν και οι δύο συσκευές έχουν αρκετή μνήμη, τότε ακολουθείται το πρωτόκολλο που παρουσιάζεται στο Σχήμα 5, για να παραχθεί ένα συνδυασμένο κλειδί:

1. η μονάδα Α παράγει ένα τυχαίο αριθμό **LK_RAND$_A$** και το στέλνει στη Β,
2. η μονάδα Β παράγει ένα τυχαίο αριθμό **LK_RAND$_B$** και το στέλνει στην Α,
3. οι δύο μονάδες υπολογίζουν ανεξάρτητα τα **LK_K$_A$** και **LK_K$_B$** με βάση τις πληροφορίες που έλαβαν,
4. το κλειδί συνδέσμου τίθεται ως το αποτέλεσμα της λογικής πράξης exclusive-OR των δύο αριθμών που υπολογίστηκαν.



Σχήμα 5: *Παραγωγή συνδυασμένου κλειδιού συνδέσμου.*

Ανεξάρτητα από το ποια από τις δύο μεθόδους χρησιμοποιείται τελικά (κλειδί μονάδας ή συνδυασμένο κλειδί), το αποτέλεσμα είναι ένα νέο κλειδί συνδέσμου για την επικοινω-

νία των δύο συσκευών. Το παλαιό προσωρινό κλειδί συνδέσμου, $\mathbf{K_{INIT}}$, δεν πρόκειται να χρησιμοποιηθεί ξανά και μπορεί να διαγραφεί.

3.2.2. Ταυτοποίηση

Για την ταυτοποίηση μίας συσκευής (authentication) χρησιμοποιείται ένα πρωτόκολλο τύπου πρόκλησης-απάντησης (challenge-response protocol). Το πρωτόκολλο αυτό είναι ανεξάρτητο από το είδος του κλειδιού συνδέσμου που χρησιμοποιείται, το οποίο θεωρεί ότι έχει ήδη οριστεί από τα προηγούμενα πρωτόκολλα. Στόχος του πρωτοκόλλου είναι να αποδείξει η συσκευή Β ότι γνωρίζει το μυστικό κλειδί συνδέσμου που χρησιμοποιείται. Αυτό είναι αναγκαίο, καθώς στα προηγούμενα βήματα δεν έχει αποδειχθεί ότι οι δύο συσκευές συμφώνησαν στο κλειδί συνδέσμου και άρα γνώριζαν το σωστό PIN.

Σχήμα 6: *Πρωτόκολλο ταυτοποίησης τύπου πρόκλησης-απάντησης.*

Για την εκτέλεση του πρωτοκόλλου, η μονάδα Α στέλνει ως πρόκληση ένα τυχαίο αριθμό **AU_RAND**. Το αποτέλεσμα του πρωτοκόλλου είναι δύο ποσότητες, η **SRES** και η **ACO**. Ο αριθμός **SRES** επιστρέφεται στη μονάδα Α ως απάντηση του πρωτοκόλλου, ενώ η ποσότητα **ACO** χρησιμοποιείται για την προαιρετική κρυπτογράφηση του καναλιού.

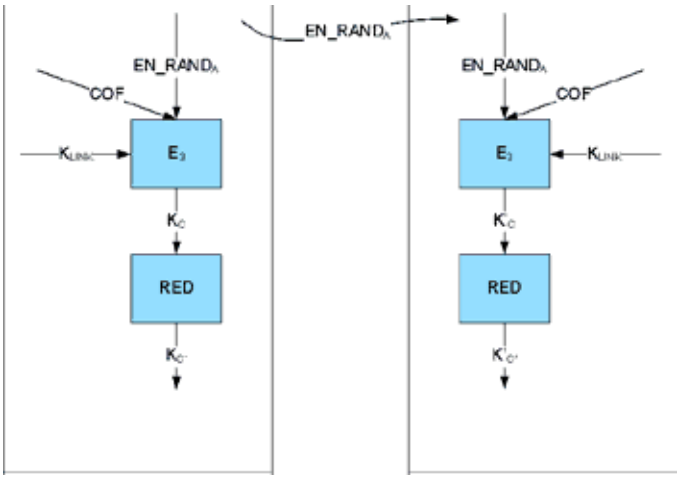
3.2.3. Πρώτο Κλειδί Κρυπτογράφησης

Αφού ολοκληρωθεί η διαδικασίας ταυτοποίησης, μπορεί να απαιτείται η κρυπτογραφημένη επικοινωνία μεταξύ των κόμβων του piconet. Για να οριστεί το πρώτο κλειδί κρυπτογράφησης, χρησιμοποιείται ο αριθμός **COF**, που είναι:

- η ποσότητα **ACO**, που υπολογίστηκε στο βήμα της ταυτοποίησης, αν πρόκειται για εκπομπή μεταξύ δύο κόμβων,
- η ποσότητα που προκύπτει από τη συνένωση της διεύθυνσης του σταθμού εκπομπής δύο φορές, αν πρόκειται για ευρεία εκπομπή (broadcast).

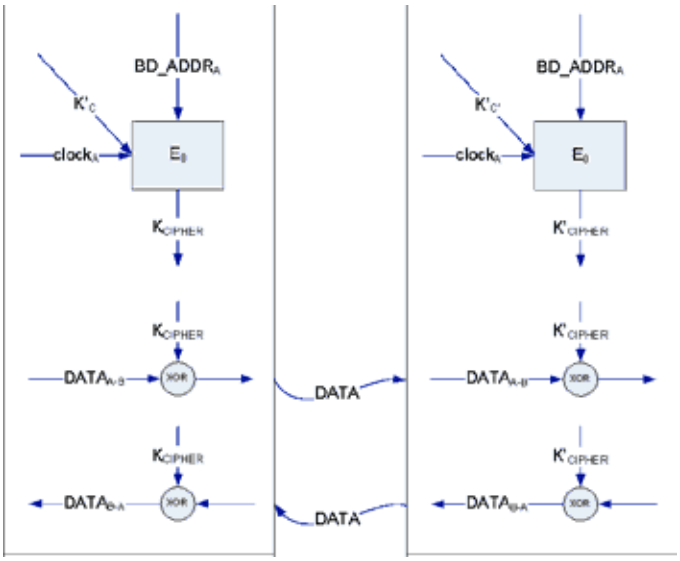
Το πρώτο κλειδί κρυπτογράφησης υπολογίζεται με βάση τον αλγόριθμο, που περιγρά-

φεται στο Σχήμα 7. Σημειώνεται ότι σε περίπτωση που απαιτείται η χρήση μικρότερου κλειδιού κρυπτογράφησης, χρησιμοποιείται η συνάρτηση μείωσης του μεγέθους RED. Σε κάθε περίπτωση, μετά το πέρας της διαδικασίας αυτής, οι δύο σταθμοί έχουν υπολογίσει ένα πρώτο κλειδί κρυπτογράφησης, $\mathbf{K_c}$.



Σχήμα 7: *Παραγωγή πρώτου κλειδιού κρυπτογράφησης.*

3.2.4. Κρυπτογραφημένη Επικοινωνία



Σχήμα 8: *Κρυπτογράφηση ροής δεδομένων με ανατροφοδοτούμενο κλειδί.*

Για την κρυπτογράφηση της επικοινωνίας σε επίπεδο συνδέσμου, χρησιμοποιείται το κλειδί κρυπτογράφησης που παράχθηκε στο προηγούμενο βήμα για την παραγωγή κλειδιών ενός συμμετρικού αλγόριθμου κρυπτογράφησης ροής δεδομένων με ανατροφοδοτούμενο κλειδί, όπως φαίνεται στο Σχήμα 8. Η ποσότητα clock_A παρέχεται από τον κύριο (master) σταθμό ενός piconet για να δημιουργεί ανατροφοδοτούμενα κλειδιά με βάση το

πρώτο κλειδί κρυπτογράφησης.

3.2.5. Διαχείριση Κλειδιών

Στις προηγούμενες ενότητες παρουσιάσαμε τους μηχανισμούς ασφάλειας, που υλοποιούνται στο επίπεδο συνδέσμου. Θεωρώντας ότι όλα τα παραπάνω σχήματα ικανοποιούν τις απαιτήσεις ασφάλειας, που θέτουν οι προδιαγραφές, είναι απαραίτητο να εξετάσουμε τη διαχείριση των κλειδιών σε περιπτώσεις αλλαγών στη σύνθεση του piconet. Δεδομένου ότι τα δίκτυα piconet είναι εγγενώς ad hoc, περιμένουμε διαρκείς αλλαγές στη σύνθεσή τους στο πέρασμα του χρόνου. Σε πολλές περιπτώσεις οι αλλαγές αυτές επιβάλλονται για διαχειριστικούς λόγους.

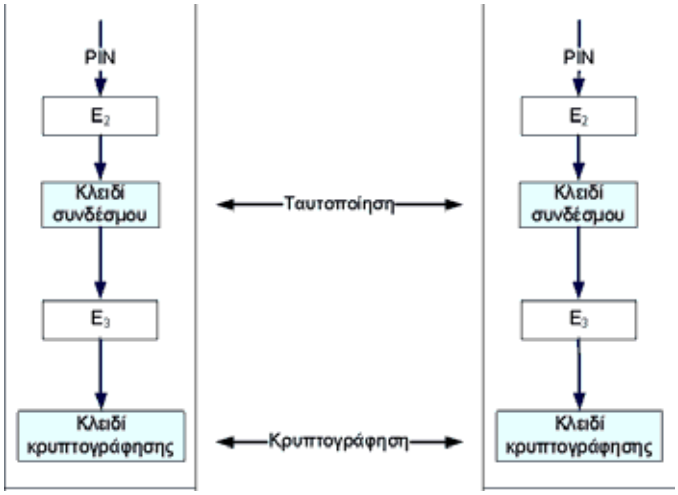
Είναι σύνηθες για πολλές εφαρμογές να απαιτείται επικοινωνία τύπου broadcast. Η προδιαγραφή Bluetooth ορίζει σαφώς ότι ένας σταθμός δεν είναι σε θέση να λαμβάνει ταυτόχρονα πακέτα broadcast και πακέτα απευθυνόμενα σε συγκεκριμένο σταθμό, αν είναι κρυπτογραφημένα. Αυτό πρακτικά σημαίνει ότι αν υπάρχει έστω και μία εφαρμογή στο piconet, η οποία απαιτεί κρυπτογραφημένη επικοινωνία τύπου broadcast, τότε όλες οι επικοινωνίες πρέπει να είναι κρυπτογραφημένες broadcast. Σε αυτήν την περίπτωση όλοι οι σταθμοί του piconet μοιράζονται ένα κοινό κλειδί κρυπτογράφησης, το οποίο ορίζεται από τον κύριο σταθμό του δικτύου και αναφέρεται ως $\mathbf{K_{MASTER}}$. Το κλειδί αυτό παράγεται με τις ίδιες διαδικασίες που περιγράψαμε προηγουμένως, με τη διαφορά ότι η τυχαία πρόκληση $\mathbf{EN\_RAND_A}$ στο Σχήμα 7 αποστέλλεται σε όλους τους σταθμούς του piconet. Θα πρέπει να σημειώσουμε ότι η διαδικασία αυτή θα πρέπει να λάβει υπόψη της σταθμούς, οι οποίοι δεν έχουν τη δυνατότητα να συμφωνήσουν σε συνδυασμένο κλειδί συνδέσμου. Αυτοί οι σταθμοί θα πρέπει να αποκλείονται από το σύνολο ευρείας εκπομπής (broadcast), ώστε να μη δημιουργείται σύγκρουση στη συμφωνία του κλειδιού συνδέσμου, αφού καθένας από αυτούς θα προσπαθεί να θέσει το δικό του κλειδί μονάδας ως κλειδί συνδέσμου.

Οι περιοδικές αλλαγές των κλειδιών συνδέσμου για κατευθυνόμενη επικοινωνία είναι, επίσης, χρήσιμες σε αρκετές περιπτώσεις. Για παράδειγμα, ένας χρήστης δεν πρέπει να έχει πρόσβαση πλέον σε έναν εκτυπωτή δικτύου. Σε αυτήν την περίπτωση, θα πρέπει ο κύριος σταθμός (master) του piconet να διαγράψει το υπάρχον μόνιμο κλειδί συνδέσμου,

που διαθέτει για τις συσκευές του συγκεκριμένου χρήστη και να εγκαθιδρύσει ένα νέο μόνιμο κλειδί συνδέσμου (σε συνεργασία με το Διαχειριστή Ασφάλειας), όταν επιτραπεί και πάλι η πρόσβαση στον εκτυπωτή για το συγκεκριμένο χρήστη.

3.2.6. Σύνοψη

Η αρχιτεκτονική ασφάλειας της τεχνολογίας Bluetooth προβλέπει μία σειρά από κλειδιά, τα οποία παράγονται για να ικανοποιήσουν διαφορετικές απαιτήσεις ασφάλειας. Με βάση τον Πίνακα 1 και την περιγραφή που δώσαμε, είναι κατανοητό ότι τα μυστικά κλειδιά παράγονται υπό τη μορφή μίας αλυσίδας, όπου κάθε νέο κλειδί, στηρίζεται στο προηγούμενο. Το Σχήμα 9 συνοψίζει αυτήν την κατάσταση, όπου το πρώτο μυστικό κλειδί είναι ο Προσωπικός Αριθμός Αναγνώρισης (PIN), ο οποίος ορίζεται από το χρήστη. Όλες οι ενδιάμεσες πληροφορίες, που χρησιμοποιούνται, είτε είναι δημόσιες, π.χ. η διεύθυνση **BD_ADDR** μίας συσκευής Bluetooth, είτε διαμοιράζονται μέσω του δικτύου, π.χ. οι διάφοροι τυχαίοι αριθμοί που είναι προσβάσιμοι σε όλους τους σταθμούς.



Σχήμα 9: *Αλυσίδα μυστικών κλειδιών.*

3.3. Κρυπτογραφικοί αλγόριθμοι

Η αρχιτεκτονική ασφάλειας της τεχνολογίας Bluetooth προδιαγράφει τη χρήση κρυπτογραφικών αλγορίθμων για μία πληθώρα λειτουργιών. Οι αλγόριθμοι αυτοί είναι οι $\mathbf{E_0}$,$\mathbf{E_1}$,$\mathbf{E_2}$,$\mathbf{E_3}$,$\mathbf{E_{21}}$ και $\mathbf{E_{22}}$, όπως σημειώθηκαν παραπάνω. Οι αλγόριθμοι είναι παραλλαγές του αλγόριθμου κρυπτογράφησης SAFER+, που σχεδιάστηκε από την εταιρεία Cylink Corporation, η οποία έδωσε άδεια χρήσης στον οργανισμό Bluetooth SIG. Η προδια-

γραφή του αλγόριθμου SAFER+ είναι ελεύθερα διαθέσιμη. Ο αλγόριθμος είναι μία βελτιωμένη έκδοση του αλγόριθμου SAFER-SK128 της ίδιας εταιρείας και είχε υποβληθεί στο διαγωνισμό του οργανισμού NIST των Η.Π.Α. ως υποψήφιος για το πρότυπο Advanced Encryption Standard (AES) [27], το οποίο είναι ο διάδοχος του γνωστού αλγόριθμου συμμετρικής κρυπτογράφησης DES. Ο NIST τελικά επέλεξε τον αλγόριθμο Rijndael [28] για το πρότυπο AES. Οι αλγόριθμοι προδιαγράφονται λεπτομερώς στα [2] και [3].

4. ΑΝΑΛΥΣΗ ΑΣΦΑΛΕΙΑΣ

Η τεχνολογία Bluetooth έχει προκαλέσει το ενδιαφέρον σημαντικής μερίδας ερευνητών, ως προς τα χαρακτηριστικά ασφάλειας που μπορεί να προσφέρει. Ο ορισμός μίας εγγενούς αρχιτεκτονικής ασφάλειας, το γεγονός ότι η προδιαγραφή είναι δημόσια διαθέσιμη και η χρήση αλγορίθμων κρυπτογράφησης, των οποίων οι προδιαγραφές είναι δημόσια διαθέσιμες, θεωρούνται κινήσεις προς τη σωστή κατεύθυνση, ως προς το σχεδιασμό νέων τεχνολογιών.

Η αρχιτεκτονική ασφάλειας θεωρείται από την κοινότητα των ερευνητών σε θέματα ασφάλειας πολύ καλά σχεδιασμένη και αρκετά εύρωστη (robust). Ωστόσο, έχουν εντοπιστεί αρκετά *κενά ασφάλειας*, τα οποία παρουσιάζουμε στη συνέχεια. Για την ταξινόμηση των κενών, θα χρησιμοποιήσουμε την κοινή πρακτική, που ακολουθείται στην αξιολόγηση ασφάλειας συστημάτων επικοινωνίας. Ένα ασφαλές σύστημα επικοινωνίας χαρακτηρίζεται από έξι ιδιότητες:

- Ιδιωτικότητα (privacy)
- Εμπιστευτικότητα δεδομένων (Data confidentiality)
- Ακεραιότητα δεδομένων (Data integrity)
- Έλεγχος πρόσβασης (Access control)
- Διαθεσιμότητα (Availability)
- Ταυτοποίηση πηγής (Source authentication)

Παρουσιάζουμε στη συνέχεια τα κενά ασφάλειας, που έχουν εντοπιστεί μέχρι σήμερα για τις έξι αυτές ιδιότητες.

4.1. Ιδιωτικότητα (Privacy)

Κάθε συσκευή τεχνολογίας Bluetooth, όπως έχουμε παρουσιάσει, έχει μία μοναδική διεύθυνση μεγέθους 48 bit. Η διεύθυνση αυτή τίθεται από τον κατασκευαστή και δεν μπορεί να αλλάξει από το χρήστη. Η διεύθυνση αυτή μεταδίδεται συνεχώς από κάθε συσκευή, στην προσπάθεια της να ανακαλύπτει και να συνδέεται σε υποψήφια piconet, ακριβώς λόγω της μορφής ad hoc που έχουν τα δίκτυα Bluetooth. Επίσης, η διεύθυνση αυτή χρησιμοποιείται σε κάθε επικοινωνία της συσκευής, ώστε να μπορούν να αναγνωρίζουν οι υπόλοιπες συσκευές τα πακέτα δεδομένων που αποστέλλει.

Είναι εμφανές ότι κακόβουλοι χρήστες ή εταιρείες μπορούν να εκμεταλλευτούν αυτή τη μοναδική διεύθυνση, ώστε να παρακολουθούν ένα χρήστη-κάτοχο συσκευής τεχνολογίας Bluetooth. Σε ένα ακραίο παράδειγμα χρήσης, μία εταιρεία η οποία παρέχει υπηρεσίες βασισμένες στη θέση του χρήστη (location-based services), π.χ. σε μία πόλη, μπορεί να χρησιμοποιήσει την υπάρχουσα υποδομή του δικτύου Bluetooth για να παρακολουθεί τις κινήσεις οποιουδήποτε χρήστη με αξιοσημείωτη ακρίβεια και ανεξάρτητα του αν είναι συνδρομητής στις υπηρεσίες της. Υπενθυμίζουμε ότι μία συσκευή τεχνολογίας Bluetooth κλάσης 3 έχει μέγιστη ακτίνα δράσης δέκα μέτρα. Άρα μπορεί κάποιος να εντοπίζει ένα συγκεκριμένο χρήστη με ακρίβεια δέκα μέτρων, η οποία είναι αρκετά μικρότερη από την ακτίνα εντοπισμού του πολιτικού[1] συστήματος προσδιορισμού θέσης GPS (Geographic Position System). Η δυνατότητα αυτή σε πολλές περιπτώσεις είναι ανεπιθύμητη και εγείρει σημαντικό θέμα στην προστασία της ιδιωτικότητας ενός χρήστη.

Είναι αρκετοί αυτοί που υποστηρίζουν ότι η τεχνική της μεταπήδησης συχνότητας (frequency hopping) είναι ικανοποιητική για την αντιμετώπιση τεχνικών παρακολούθησης. Η ίδια η προδιαγραφή της τεχνολογίας Bluetooth εντάσσει τη διαδικασία αυτή στα χαρακτηριστικά ασφάλειας (όπως και στην ανοχή σε παρεμβολές, για την οποία αρχικώς σχεδιάστηκε). Η τεχνική της μεταπήδησης συχνότητας είναι τόσο ασφαλής, όσο τυχαία είναι η ακολουθία μεταπήδησης. Ιδανικά, η ακολουθία παράγεται από μία κρυπτογραφικά ασφαλή γεννήτρια τυχαίων αριθμών.

Στο [29] παρουσιάζεται η λειτουργία της ψευδοτυχαίας γεννήτριας της ακολουθίας μεταπήδησης, την οποία μεταφέρουμε σε ελεύθερη απόδοση στα ελληνικά:. «*... Στις*

[1] Σε αντιδιαστολή με τα αντίστοιχα στρατιωτικά συστήματα GPS, τα οποία έχουν σημαντικά μικρότερη απόκλιση εντοπισμού

Η.Π.Α., όπως και στις περισσότερες χώρες, έχουν οριστεί 79 διαφορετικές ζώνες μεταπήδησης, ενώ στην Ισπανία και Γαλλία μόνο 23. Είναι εύκολο να κατασκευάσει κανείς μία συσκευή με 79 ή 23 παράλληλους δέκτες. Η συσκευή αυτή μπορεί να παρακολουθεί ταυτόχρονα όλες τις ζώνες. Για να παρακολουθήσει κανείς μία συγκεκριμένη συσκευή, αρκεί να εντοπίσει το σπόρο (seed) της ψευδοτυχαίας γεννήτριας, η οποία παράγει την ακολουθία μεταπηδήσεων. Ο σπόρος όμως υπολογίζεται ντετερμινιστικά. Όταν η συσκευή είναι σε κατάσταση αναζήτησης δικτύου, υπολογίζεται από το ρολόι της συσκευής και έναν κωδικό, το «General Inquiry Access Code» (GIAC), ο οποίος είναι κοινός για όλες τις συσκευές. Στην κατάσταση σύνδεσης, ο σπόρος υπολογίζεται από το ρολόι του κύριου (master) σταθμού του δικτύου και τη διεύθυνσή του. Στην κατάσταση αναζήτησης χρησιμοποιούνται μόνο 32 ζώνες μεταπήδησης. Ανταποκρινόμενη λοιπόν μία συσκευή σε ένα μήνυμα αναζήτησης, φανερώνει το ρολόι της καθώς και τη διεύθυνσή της. Έτσι, ένας επιτιθέμενος μπορεί να βρει το σπόρο της γεννήτριας σαρώνοντας στις συχνότητες αναζήτησης και υποκλέπτοντας τα μηνύματα απάντησης. Στη συνέχεια, μπορεί να υπολογίσει το σπόρο της ακολουθίας μετάβασης του piconet, αφού ο κύριος σταθμός θα αποκαλύψει την ταυτότητα και το ρολόι του ...». Παρόμοια αποτελέσματα παρουσιάζονται και στην εργασία [30].

Είναι φανερό από τα παραπάνω, ότι η κατασκευή μίας συσκευής παρακολούθησης είναι εύκολη. Επίσης, είναι εξίσου εύκολος ο υπολογισμός του σπόρου, δεδομένου ότι ο αλγόριθμος που τον υπολογίζει είναι δημοσιευμένος στην προδιαγραφή του Bluetooth και οι είσοδοί του μπορούν εύκολα να υποκλαπούν από το δίκτυο, στο οποίο συμμετέχει η συσκευή-στόχος. Είναι λοιπόν σφάλμα να θεωρεί κανείς ότι η τεχνική μεταπήδησης συχνότητας προσθέτει στην ασφάλεια της τεχνολογίας Bluetooth. Συνεπώς, ο χρήστης παραμένει άμεσα εκτεθειμένος σε έναν κακόβουλο, σε ό,τι αφορά στο θέμα της ιδιωτικότητας.

4.2. Ασφάλεια δεδομένων

Στον όρο *ασφάλεια δεδομένων* θα επισυνάψουμε τις ιδιότητες *εμπιστευτικότητα δεδομένων, ακεραιότητα δεδομένων, έλεγχος πρόσβασης και ταυτοποίηση πηγής*. Στην περίπτωση της τεχνολογίας Bluetooth αυτό είναι αναγκαίο, καθώς τα κρυπτογραφικά κλειδιά

που χρησιμοποιούνται για την υλοποίηση κάθε μίας ιδιότητας είναι οργανωμένα σε μία σειρά, όπως φαίνεται στο Σχήμα 9. Συνεπώς η παραβίαση ενός κλειδιού για μία λειτουργία, οδηγεί άμεσα στην παραβίαση και των επόμενων κλειδιών. Ορισμένες από τις επιθέσεις, που περιγράφονται στη συνέχεια, έχουν παρουσιαστεί ανεξάρτητα στα [29] και [30].

Παρατηρούμε στο Σχήμα 9 ότι η ασφάλεια των κρυπτογραφικών κλειδιών για την ταυτοποίηση, τον έλεγχο πρόσβασης και την κρυπτογράφηση των δεδομένων στηρίζεται αποκλειστικά στο μυστικό αριθμό PIN που ορίζει ο χρήστης για τις συσκευές. Αρχικά εστιάζουμε στο PIN.

4.2.1. Επιθέσεις Βασισμένες στη Γνώση του Μυστικού PIN

Η προδιαγραφή ορίζει ότι το PIN μπορεί να είναι οτιδήποτε μεταξύ τεσσάρων και δεκαέξι byte. Είναι σύνηθες για τους ανθρώπους να χρησιμοποιούν PIN τεσσάρων αριθμών. Στην πραγματικότητα, τα περισσότερα συστήματα όπου χρησιμοποιείται, το PIN έχει μέγεθος τέσσερις δεκαδικούς αριθμούς. Είναι φανερό ότι αυτό δημιουργεί ένα μεγάλο κενό ασφάλειας. Ένας επιτιθέμενος, χρησιμοποιώντας εξαντλητική αναζήτηση ή κοινωνική μηχανική (social engineering), μπορεί με το πολύ 10.000 δοκιμές να ανακαλύψει το PIN ενός piconet. Ο αριθμός των δοκιμών είναι πολύ μικρός, με βάση τη σημερινή υπολογιστική δύναμη που έχει ο μέσος χρήστης.

Η ανεπιθύμητη γνώση του PIN ενός piconet δημιουργεί σημαντικά προβλήματα ασφάλειας. Ο επιτιθέμενος μπορεί να συμμετάσχει στο δίκτυο, λαμβάνοντας και στέλνοντας πληροφορίες. Μπορεί επίσης να ταυτοποιηθεί επιτυχώς και να ορίσει κατάλληλα κλειδιά συνδέσμου και κρυπτογραφημένης επικοινωνίας. Σε συνδυασμό με την πλαστοπροσωπία της διεύθυνσης Bluetooth μίας υπάρχουσας συσκευής, μπορεί να ταυτοποιηθεί επιτυχώς αντ' αυτής και να έχει πρόσβαση στις υπηρεσίες του piconet, που αναφέρονται σε εκείνη. Μπορεί, επίσης, να αναγκάσει το piconet να λειτουργήσει σε χαμηλότερο επίπεδο ασφάλειας, υποχρεώνοντας τον κύριο σταθμό να λειτουργήσει σε κατάσταση ευρείας εκπομπής (broadcast), με κλειδί συνδέσμου, το οποίο θα παράσχει η ίδια.

Ο κατάλογος των επιθέσεων, που μπορεί να υλοποιήσει κάποιος, που γνωρίζει το PIN ενός piconet περιορίζεται μόνο από τη φαντασία του επιτιθέμενου. Το PIN είναι η ραχοκοκαλιά της ασφάλειας του Bluetooth και για αυτό θα πρέπει να είναι ο καθένας πολύ

προσεκτικός στην επιλογή του PIN και να χρησιμοποιεί όσο το δυνατό πιο μεγάλη και πλούσια συμβολοσειρά (όχι μόνο δεκαδικά ψηφία).

4.2.2.. Επιθέσεις στο Πρωτόκολλο Ταυτοποίησης

Θεωρώντας ότι έχουμε εξασφαλίσει την ασφάλεια του PIN, εξετάζουμε το πρωτόκολλο ταυτοποίησης. Στις επιθέσεις που θα εξετάσουμε στη συνέχεια, είναι αναγκαία η πρότερη γνώση του PIN από τον επιτιθέμενο. Αυτό μπορεί να επιτευχθεί, αν ο κακόβουλος χρήστης (για την ακρίβεια η συσκευή που υλοποιεί την επίθεση) υπήρξε κατά το παρελθόν μέλος του piconet, στο οποίο επιτίθεται.

Το πρώτο πρόβλημα εντοπίζεται στην ταυτοποίηση συσκευών με περιορισμένους πόρους. Τέτοιες συσκευές ορίζουν ως κλειδί συνδέσμου το (μοναδικό) κλειδί μονάδας, όπως είδαμε στο Σχήμα 4. Μία κακόβουλη συσκευή, έστω Β, μπορεί να ζητήσει επικοινωνία με μία τέτοια μονάδα, έστω Α, και να δημιουργήσει κλειδί συνδέσμου μαζί της. Με τον τρόπο αυτό αποκτά το κλειδί συνδέσμου που χρησιμοποιεί η συσκευή Α. Έχοντας την πληροφορία αυτή, μπορεί να δημιουργήσει στη συνέχεια συνδέσεις με άλλες συσκευές, παρουσιαζόμενη ως η συσκευή Α. Παρατηρούμε ότι στα πρωτόκολλα που έπονται της ταυτοποίησης απαιτείται η γνώση του κλειδιού συνδέσμου και η διεύθυνση της συσκευής. Άρα, με τις παραπάνω πληροφορίες, η συσκευή Β μπορεί να εκτελέσει επιτυχώς όλα τα επόμενα πρωτόκολλα. Το πρόβλημα οφείλεται στη μοναδικότητα του κλειδιού συνδέσμου, που χρησιμοποιεί μία συσκευή περιορισμένων πόρων και στην άμεση σύνδεσή του με τη διεύθυνσή της.

Μία δεύτερη επίθεση που μπορεί να υλοποιήσει ένας κακόβουλος χρήστης στο πρωτόκολλο ταυτοποίησης στηρίζεται στην επίθεση του ενδιάμεσου ανθρώπου (man-in-the-middle attack). Σε αυτήν την περίπτωση, ο επιτιθέμενος έχει στην κατοχή του το κλειδί συνδέσμου, το οποίο έχει χρησιμοποιηθεί κατά το παρελθόν από δύο συσκευές, οι οποίες ολοκλήρωσαν την επικοινωνία τους. Ο επιτιθέμενος λοιπόν συνδέεται με τις δύο συσκευές ανεξάρτητα, παρουσιαζόμενος στην καθεμία ως η άλλη συσκευή. Ο επιτιθέμενος δημιουργεί με τις συσκευές δύο νέα κλειδιά συνδέσμου, ένα για κάθε επικοινωνία. Οι δύο συσκευές πιστεύουν ότι επικοινωνούν μεταξύ τους και ότι η άλλη εγκαθίδρυσε την επικοινωνία. Αυτό είναι δυνατόν, γιατί κατά την εγκαθίδρυση της επικοινωνίας και

πριν τον ορισμό του κλειδιού συνδέσμου, ορίζεται ο ρόλος της κάθε συσκευής (κύρια ή δευτερεύουσα) με κατάλληλα μηνύματα. Το αποτέλεσμα είναι ότι οι συσκευές ακολουθούν διαφορετικές ακολουθίες μεταπήδησης συχνότητας, βασισμένες στην ταυτότητα του ενδιάμεσου, ο οποίος πλαστοπροσωπεί τις ταυτότητές τους. Ο ενδιάμεσος είναι σε θέση να παρακολουθεί και τις δύο ακολουθίες μεταπήδησης και συνεπώς να προωθεί όσα μηνύματα κρίνει σκόπιμο. Οι δύο συσκευές δε μπορούν να παρακολουθούν τα μηνύματα που στέλνει η μία στην άλλη και συνεπώς να ανιχνεύσουν την πλαστοπροσωπία, ακριβώς γιατί ακολουθούν διαφορετικές ακολουθίες μεταπήδησης.

Η *επίθεση του ενδιάμεσου ανθρώπου* εφαρμόζεται σε όλα τα πρωτόκολλα ταυτοποίησης, όπου δεν υπάρχει πρότερη γνώση της ταυτότητας της οντότητας, που ταυτοποιείται. Για να επιτευχθεί η πρότερη γνώση, συνήθως χρησιμοποιούνται ψηφιακά πιστοποιητικά (digital certificates), αλλά σε πολλές περιπτώσεις (όπως και στην τεχνολογία Bluetooth) δεν χρησιμοποιούνται, λόγω σημαντικού διαχειριστικού κόστους.

4.2.3.. Επιθέσεις στους Αλγορίθμους Κρυπτογράφησης

Το τελευταίο θέμα, που θα εξετάσουμε στην ασφάλεια των δεδομένων στο Bluetooth, αφορά στην ασφάλεια των αλγορίθμων κρυπτογράφησης. Η επιλογή ενός ασφαλούς PIN δεν είναι αρκετή, αν οι αλγόριθμοι κρυπτογράφησης είναι αδύναμοι και μπορούν να οδηγήσουν στην αποκάλυψή του. Το επίπεδο ασφάλειας της κρυπτογραφημένης επικοινωνίας είναι, επίσης, σημαντικό θέμα, καθώς ο νόμος του Moore επιβεβαιώνεται συνεχώς: καθώς η υπολογιστική ισχύς αυξάνεται συνεχώς, τα όρια ασφάλειας που θέτουν οι αλγόριθμοι μειώνονται με σταθερό ρυθμό, αφού είναι ολοένα και πιο πρακτικές οι εξαντλητικές αναζητήσεις των κρυπτογραφικών κλειδιών.

Το πρώτο πρόβλημα, που εντοπίζεται, αφορά στη χρήση κοινού κλειδιού κρυπτογράφησης για τις δύο κατευθύνσεις επικοινωνίας (βλ. Σχήμα 8). Αν ένας κακόβουλος χρήστης μπορεί να γνωρίζει τα δεδομένα της μίας κατεύθυνσης, $data_{A\to B}$, τότε, υποκλέπτοντας την κρυπτογραφημένη επικοινωνία $data_{A\to B} \oplus K_{CIPHER}, data_{B\to A} \oplus K_{CIPHER}$ των συσκευών, μπορεί να υπολογίσει την απάντηση της άλλης συσκευής, ως:

$$\left[data_{A\to B} \oplus K_{CIPHER}\right] \oplus \left[data_{B\to A} \oplus K_{CIPHER}\right]$$
$$\oplus\, data_{A\to B} = data_{B\to A}$$

Ένα σενάριο για την παραπάνω επίθεση είναι το εξής: μία κακόβουλη συσκευή υποχρεώνει μία συσκευή, έστω Α, να εκκινήσει ένα γνωστό πρωτόκολλο επικοινωνίας με μία συσκευή Β, ώστε τελικά να λάβει η κακόβουλη συσκευή μία απάντηση, ανεξάρτητη από το πρωτόκολλο επικοινωνίας. Γνωρίζοντας το πρωτόκολλο επικοινωνίας μεταξύ της Α και της Β, η κακόβουλη συσκευή μπορεί να γνωρίζει το περιεχόμενο του μηνύματος που έστειλε η Α και συνεπώς να γνωρίζει την απάντηση της Β, χρησιμοποιώντας την παραπάνω επίθεση.

Η κρυπτογραφική κοινότητα έχει εστιάσει ιδιαίτερα τα τελευταία χρόνια στους αλγορίθμους κρυπτογράφησης, που χρησιμοποιεί η τεχνολογία Bluetooth και ιδιαίτερα στον αλγόριθμο κρυπτογράφησης δεδομένων Ε0. Ο αλγόριθμος αυτός υλοποιείται με τέσσερις καταχωρητές ολίσθησης (LFSR1, LFSR2, LSFR3, LSFR4) με γραμμική ανάδραση (Linear Feedback Shift Register, LFSR) και μία Μηχανή Πεπερασμένης Κατάστασης (Finite State Machine, FSM). Κάθε βήμα εκτέλεσης παράγει ένα bit ροής κλειδιού (key stream). Ο αλγόριθμος αρχικοποιείται με το πρώτο κλειδί κρυπτογράφησης K_C, τη δημόσια διεύθυνση της συσκευής και την τιμή από το κεντρικό ρολόι του piconet (βλ. Σχήμα 7 και Σχήμα 8).

Η προδιαγραφή της τεχνολογίας Bluetooth θεωρεί ότι συμμετρικά κλειδιά μεγέθους 64 bit είναι ασφαλή σήμερα και προβλέπει τη χρήση των αλγορίθμων με κλειδιά μεγέθους έως 128 bit για μεγαλύτερη ασφάλεια. Στην πραγματικότητα τα κλειδιά μεγέθους 64 bit δε θεωρούνται πλέον ασφαλή. Τα τελευταία τρία χρόνια έχουν παρουσιαστεί πολλές υλοποιήσεις μηχανών με λογικό κόστος, οι οποίες μπορούν να ανακαλύπτουν τέτοια κλειδιά σε λιγότερο από 24 ώρες [36], [37]. Σήμερα, είναι απαραίτητο να χρησιμοποιούνται, όταν επιτρέπεται, κλειδιά μεγέθους 128 bit για ένα ικανοποιητικό βαθμό ασφάλειας. Οι κρυπταναλυτές ωστόσο έχουν εστιάσει σε αυτήν την έκδοση του αλγορίθμου και υπάρχουν ήδη σημαντικά αποτελέσματα για το επίπεδο ασφάλειας που προσφέρει.

Στο [31] παρουσιάστηκε η πρώτη επίθεση στον αλγόριθμο κρυπτογράφησης Ε0. Χρησιμοποιώντας 125 bit ροής κλειδιού και μαντεύοντας την κατάσταση των τριών καταχωρητών LFSR1, LFSR2, LSFR3 και της FSM (συνολικά 93 bit), ο επιτιθέμενος μπορεί να ανακατασκευάσει πλήρως την κατάσταση του αλγορίθμου και συνεπώς να εντοπίσει το

πρώτο κλειδί κρυπτογράφησης. Αυτό μπορεί να χρησιμοποιηθεί για την εύρεση οποιουδήποτε σημείου της ροής κλειδιών, αφού είναι η μόνη μυστική πληροφορία εισόδου στον αλγόριθμο. Η συγκεκριμένη επίθεση λοιπόν μειώνει την ασφάλεια του αλγορίθμου από 128 σε 100 bit. Ο αριθμός των δοκιμών, 2^{100} , που πρέπει να γίνουν για την επιτυχή υλοποίηση της επίθεσης είναι πολύ μεγαλύτερος από την υπολογιστική ισχύ των σημερινών υπολογιστών. Για το λόγο αυτό η επίθεση χαρακτηρίζεται ως θεωρητική.

Στο [29], η επίθεση βελτιώνεται, ώστε αρχικά να απαιτεί 2^{93} δοκιμές και τελικά $O(2^{66})$ χρόνο και $O(2^{66})$ γνωστά bit της ροής κλειδιού. Στο [33], η αρχική κατάσταση υπολογίζεται σε $O(2^{64})$ χρόνο, δεδομένων $O(2^{64})$ γνωστών bit της ροής κλειδιών, ενώ στο [32] η αρχική κατάσταση εντοπίζεται σε $O(2^{61})$ χρόνο και $O(2^{50})$ γνωστά bit της ροής κλειδιού. Στο [34], η επίθεση απαιτεί $O(2^{84})$ και 135 γνωστά bit της ροής κλειδιού. Η πολυπλοκότητα μειώνεται σε $O(2^{77})$ με $O(2^{30})$ γνωστά bit της ροής κλειδιού ή $O(2^{73})$ με $O(2^{34})$ γνωστά bit της ροής κλειδιού, ενώ αναμένεται με ενδιαφέρον η δημοσίευση [35].

Οι παραπάνω επιθέσεις δεν είναι πρακτικές σήμερα και χαρακτηρίζονται θεωρητικές. Ωστόσο, η υποθετική ασφάλεια που προσφέρει ο αλγόριθμος έχει μειωθεί σημαντικά από τα 128 bit που θεωρεί η κατασκευάστρια εταιρεία Cylink. Επιπρόσθετα, έχει αποδειχθεί ότι ο φόρτος εργασίας θα παραμείνει στις ίδιες τάξεις μεγέθους ακόμη και αν αυξηθεί το μέγεθος του κλειδιού πάνω από 128 bit [34]. Το αποτέλεσμα αυτό είναι πολύ σημαντικό, διότι θα καταρρεύσει η ασφάλεια της κρυπτογράφησης, εάν υπάρξει μεγαλύτερη πρόοδος στην κρυπτανάλυση, και το Bluetooth SIG θα πρέπει να αλλάξει την προδιαγραφή του αλγορίθμου και να χρησιμοποιήσει κάποιον πιο ασφαλή.

4.3. Διαθεσιμότητα

Η διαθεσιμότητα των κόμβων και της υποδομής ενός δικτύου επικοινωνίας είναι απαραίτητη για την απρόσκοπτη ανταλλαγή δεδομένων και πληροφοριών μεταξύ των μελών του, δηλαδή για το σκοπό που κατασκευάζει κανείς ένα δίκτυο επικοινωνίας. Τα ασύρματα δίκτυα καθώς και τα δίκτυα ad hoc παρουσιάζουν αρκετές προκλήσεις στους σχεδιαστές σε ό,τι αφορά ζητήματα διαθεσιμότητας. Η τεχνολογία Bluetooth συνδυάζει τις δύο ιδιότητες και είναι ενδιαφέρον να δει κανείς πώς αντιμετωπίζει ζητήματα διαθεσιμότητας. Προβλήματα διαθεσιμότητας μπορούν να προκύψουν από κακόβουλο χειρισμό

των πρωτοκόλλων επικοινωνίας. Τέτοια προβλήματα αναφέρθηκαν προηγουμένως, π.χ. στην πλαστοπροσωπία μίας συσκευής. Εδώ θα εστιάσουμε στην προσπέλαση του μέσου, τη δρομολόγηση σε ένα piconet και την εξάντληση της μπαταρίας.

4.3.1. Αδυναμία Προσπέλασης Μέσου

Ένα κοινό πρόβλημα σε όλα τα κατανεμημένα συστήματα είναι η έννοια του χρόνου. Ιδανικά, σε ένα τέτοιο σύστημα, όλες οι συσκευές έχουν κοινή αναφορά στο χρόνο. Πρακτικά όμως, και ιδιαίτερα στα ασύρματα δίκτυα ad hoc, είναι πολύ δύσκολο έως αδύνατο να εξασφαλίσει κανείς κοινό ρολόι. Η τεχνολογία Bluetooth χρησιμοποιεί ένα σχετικό ρολόι, το οποίο είναι απαραίτητο για τη σωστή μετάδοση στις αντίστοιχες χρονοσχισμές και στο συγχρονισμό της εκπομπής και λήψης μεταξύ των σταθμών. Κάθε συσκευή τεχνολογίας Bluetooth χρησιμοποιεί ένα ρολόι 28 bit, το οποίο ποτέ δε ρυθμίζεται ή σταματά να μετρά. Το ρολόι έχει συχνότητα 3.2 KHz με ακρίβεια ± 20 ppm (parts per million), η οποία μειώνεται σε ± 250 ppm, όταν η συσκευή λειτουργεί σε κατάσταση χαμηλής κατανάλωσης ισχύος. Ένας επιτιθέμενος μπορεί να διαταράξει τα ρολόγια, χρησιμοποιώντας laser χαμηλής ενέργειας (Low Energy Laser, LEL) ή ηλεκτρομαγνητικούς παλμούς (Electromagnetic Pulses, EMP), με αποτέλεσμα την ολική κατάρρευση του δικτύου [25]. Η κατάσταση δεν είναι αναστρέψιμη, καθώς δεν προβλέπεται κάποιος τρόπος για την επαναφορά του ρολογιού σε μία σωστή θέση. Τέτοιες επιθέσεις όμως είναι αρκετά σπάνιες, καθώς απαιτείται πολύ προηγμένος εξοπλισμός. Για το λόγο αυτό, η επίθεση θεωρείται πολύ απίθανη και συνεπώς αυτός ο κίνδυνος είναι αμελητέος.

Παρόμοια αποτελέσματα θα μπορούσε να επιτύχει κάποιος, εκμεταλλευόμενος το σχήμα διαχείρισης ισχύος των συσκευών. Προκειμένου να εξοικονομήσουν ενέργεια, οι συσκευές μπορούν να λειτουργήσουν σε ένα τρόπο χαμηλής κατανάλωσης, όταν δεν ανταλλάσσουν πληροφορίες. Κατά τη διάρκεια της επικοινωνίας, ο παραλήπτης ελέγχει την ποιότητα λήψης στο σύνδεσμο και μπορεί να ζητήσει την ενίσχυση ή μείωση της ισχύος εκπομπής του δέκτη. Στο [25] περιγράφεται το παρακάτω σενάριο επίθεσης στο σχήμα διαχείρισης ισχύος. Αν ένας επιτιθέμενος μπορέσει να επηρεάσει το σχήμα διαχείρισης ισχύος μίας ή όλων των συσκευών ενός piconet (για παράδειγμα εισάγοντας πλαστά μηνύματα στο δίκτυο), τότε μπορεί να οδηγήσει το δίκτυο σε μία χαοτική κατά-

σταση. Συσκευές θα απομονωθούν, λειτουργώντας σε τρόπο χαμηλής κατανάλωσης και χάνοντας μηνύματα που απευθύνονται προς αυτές. Χωρίς την κατάλληλη ισχύ λειτουργίας, η συσκευή θα υπολειτουργεί και ο ρυθμός μεταπήδησης συχνότητας θα μειωθεί, αποσυγχρονίζοντας τις εκπομπές της.

4.3.2. Δρομολόγηση

Η δρομολόγηση σε δίκτυα ad hoc έχει πολύ διαφορετικά χαρακτηριστικά και τρωτά σημεία σε σχέση με τα σταθερά (fixed) δίκτυα. Τα τρωτά σημεία είναι περισσότερα, όταν το μέσο μετάδοσης είναι ο αέρας, καθώς είναι άμεσα προσβάσιμος, χωρίς να απαιτείται η φυσική παραβίαση του μέσου (για παράδειγμα εγκατάσταση εξοπλισμού).

Η τεχνολογία Bluetooth έχει τη δυνατότητα να αποφεύγει τις παραμορφώσεις και συγκρούσεις με εκπομπές από τρίτες συσκευές. Αυτό είναι απαραίτητο, καθώς στη συγκεκριμένη ζώνη συχνοτήτων παρατηρείται μεγάλος συνωστισμός εκπομπών. Η τεχνική της μεταπήδησης συχνότητας (frequency hopping) επιτυγχάνει το σκοπό αυτό. Μάλιστα, η τεχνολογία Bluetooth υπερτερεί σημαντικά της τεχνολογίας IEEE 802.11 στην αντιμετώπιση των παρεμβολών [38], [39], [40]. Ωστόσο, μπορεί κανείς να εισάγει θόρυβο μεγάλης ισχύος (παρεμβολή παρασίτων) σε όλες τις συχνότητες εκπομπής, που χρησιμοποιεί η τεχνολογία Bluetooth. Αυτό οδηγεί πρακτικά στην κατάρρευση του piconet, καθώς καμία συσκευή δεν μπορεί να επικοινωνήσει με οποιαδήποτε συσκευή [25].

Τα πρωτόκολλα δρομολόγησης είναι ένα από τα πιο τρωτά σημεία των δικτύων ad hoc. Λόγω του δυναμικού χαρακτήρα αυτών των δικτύων, είναι εφικτός ο κακόβουλος χειρισμός των πληροφοριών δρομολόγησης. Τέτοιοι χειρισμοί είναι για παράδειγμα η εισαγωγή πλαστών πληροφοριών, η διαγραφή κόμβων και η εισαγωγή κόμβων, που εμφανίζονται να λειτουργούν ως δρομολογητές [25]. Σύμφωνα με τον ορισμό της προδιαγραφής της τεχνολογίας Bluetooth, κάθε συσκευή που προσπελαύνει ένα piconet, πρακτικά επεκτείνει την ακτίνα δράσης του, καθώς μπορεί να λειτουργήσει ως κόμβος πρόσβασης για πιο απομακρυσμένες συσκευές. Αυτό σημαίνει ότι οι πληροφορίες δρομολόγησης, όπως για παράδειγμα η τοπολογία του δικτύου και ο ρόλος των σταθμών, μεταδίδονται σε ολοένα και μεγαλύτερες αποστάσεις, οπότε διευκολύνεται σημαντικά το έργο ενός επιτιθέμενου, που υποκλέπτει. Ο επιτιθέμενος διευκολύνεται, επίσης, στην εισαγωγή πλαστών πληρο-

φοριών στο δίκτυο, καθώς δεν χρειάζεται να προσεγγίσει σημαντικά τον κύριο (master) σταθμό του δικτύου.

4.3.3. Εξάντληση Μπαταρίας

Οι συσκευές τεχνολογίας Bluetooth χρησιμοποιούν μπαταρίες ως πηγή ενέργειας, προκειμένου να λειτουργούν. Αυτό είναι εν μέρει απαραίτητο, ώστε να εκμεταλλεύεται κανείς τις δυνατότητες ασύρματης επικοινωνίας, χωρίς να απαιτείται ενσύρματη πηγή ενέργειας (το οποίο θα ήταν οξύμωρο). Λόγω του χαρακτήρα ad hoc των δικτύων Bluetooth, μία συσκευή είναι υποχρεωμένη να επεξεργάζεται πακέτα που λαμβάνει από το δίκτυο, ακόμη και αν τελικά δεν προσφέρει κάποια υπηρεσία. Αυτό οδηγεί σε μία πρακτική επίθεση εξάντλησης της μπαταρίας.

Ένας επιτιθέμενος μπορεί να απευθύνει συνεχώς πακέτα προς μία συσκευή, χωρίς να έχει σημασία το περιεχόμενο τους. Εξαναγκάζει, έτσι, τη συσκευή να λειτουργεί σε κανονικό τρόπο λειτουργίας και να επεξεργάζεται συνεχώς τα δεδομένα, που λαμβάνει από το δίκτυο. Έτσι, εξαντλείται η μπαταρία της συσκευής χωρίς λόγο και δε θα μπορεί από ένα σημείο και μετά να συμμετέχει κανονικά στο piconet [25]. Ο χρόνος εξάντλησης της μπαταρίας μπορεί να μειωθεί σημαντικά, εάν ο επιτιθέμενος μπορεί να υποχρεώσει τη συσκευή να μεταδίδει με τη μέγιστη ισχύ εκπομπής, χρησιμοποιώντας κατάλληλα πακέτα από το σχήμα διαχείρισης ισχύος εκπομπής.

5. ΕΠΙΛΟΓΟΣ - ΣΥΜΠΕΡΑΣΜΑΤΑ

Στην παρούσα εργασία εστιάσαμε στην ασφάλεια, που προσφέρει η τεχνολογία ασύρματης δικτύωσης Bluetooth. Η τεχνολογία Bluetooth προδιαγράφει εγγενώς μία αρχιτεκτονική ασφάλειας, σε αντίθεση με τις περισσότερες αντίστοιχες τεχνολογίες. Περιγράψαμε την αρχιτεκτονική αυτή, με έμφαση στην ασφάλεια στο επίπεδο συνδέσμου και παρουσιάσαμε τις διάφορες επιθέσεις, που έχουν προταθεί, τόσο για την αρχιτεκτονική όσο και για τους αλγόριθμους κρυπτογράφησης, που χρησιμοποιούνται.

Θεωρούμε πολύ θετικό ότι το Bluetooth SIG όρισε μία εγγενή αρχιτεκτονική ασφάλειας στην προδιαγραφή της τεχνολογίας. Θεωρούμε εξίσου σημαντικό ότι η προδιαγραφή και οι αλγόριθμοι κρυπτογράφησης παρέχονται ελεύθερα, γιατί δίνεται έτσι η δυνατό-

τητα να αναλυθούν καλύτερα και από όλους τους εμπλεκομένους, ώστε να διορθωθούν τυχόν σφάλματα όσο το δυνατό συντομότερα.

Διαπιστώνουμε ότι η αρχιτεκτονική ασφάλειας του Bluetooth έχει αδυναμίες. Τα διάφορα αδύναμα σημεία, που εντοπίζονται, οφείλονται περισσότερο στα χαρακτηριστικά ασφάλειας και στα τρωτά σημεία που παρουσιάζουν τα ασύρματα δίκτυα γενικά, παρά σε προβλήματα της συγκεκριμένης τεχνολογίας. Αντίθετα, θεωρούμε ότι η σημαντική προσπάθεια του Bluetooth SIG είναι αρκετά επιτυχής, ώστε η αρχιτεκτονική ασφάλειας να είναι εύρωστη.

6. ΠΑΡΑΠΟΜΠΕΣ ΚΑΙ ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Bluetooth Special Interest Group, Inc. URL: http://www.bluetooth.com/

[2] Bluetooth SIG, Inc. "Specification of the Bluetooth System – Core", February 2001. URL: http://www.bluetooth.com/files/Bluetooth_11_Specifications_Book.pdf

[3] Bluetooth SIG, Inc. "Specification of the Bluetooth System – Profiles". February 2001. URL: http://www.bluetooth.com/files/Bluetooth_11_Profiles_Book.pdf

[4] Danny Bradbury, "Bluetooth is here to disable the cable", Personal Computer World, March 2000. pp. 130-135. URL: http://myhome.asia1.com/home/n/ntu_ac233/wa8.htm

[5] Jim Kardach, "The naming of a Technology". Click I.T. Ltd "Incisor" electronic newsletter, volume 34, August 2001. URL: http://www.click.co.uk/inc_34_aug2001.pdf

[6] Jim Kardach, "The naming of a Technology". Click I.T. Ltd "Incisor" electronic newsletter, volume 35, September 2001. URL: http://www.click.co.uk/inc_35_sep2001.pdf

[7] Dave Suvak, "IrDA and Bluetooth: A complementary comparison". Extended Systems, Inc. white paper, 2000. URL: http://www.extendedsystems.com/

[8] Jennifer Bray, "802.11b is dead. Long live Bluetooth". Click I.T. Ltd "Incisor" electronic newsletter, volume 35, September 2001. URL: HYPERLINK "http://www.click.co.uk/inc_35_sep2001.pdf" http://www.click.co.uk/inc_35_sep2001.pdf

[9] Paul Rasmussen, "Bluetooth PANs (Paranoia, Anxiety and Neurosis)". Click I.T. Ltd "Incisor" electronic newsletter, volume 35, September 2001. URL: http://www.click.co.uk/inc_35_sep2001.pdf

[10] Paul Rasmussen, "Confused Connections". Click I.T. Ltd "Incisor" electronic newsletter, volume 35, September 2001. URL: http://www.click.co.uk/inc_35_sep2001.pdf

[11] Ασημακόπουλος Ζώης, «Wi-Fi4. Αερογέφυρες επικοινωνίας στην μπάντα των 5 GHz». Περιοδικό RAM, τεύχος 154 σελίδες 250-252. Ιανουάριος 2002.

[12] Mark Lambert, "Positioning Bluetooth amongst other wireless technologies for effortless connectivity". Morgan Stanley Dean Witter Bluetooth Conference: The Wireless Future. June 200. URL: http://www.cambridge-consultants.com/PDFs/MSDWBlutooth.pdf

[13] Mark Lambert, "DECT and Bluetooth: What is their impact upon each other?". IIR Bluetooth Conference. April 2000.

[14] Jyrki Oraskari, "Bluetooth versus WLAN IEEE 802.11x". URL: http://www.hut.fi/~joraskur/BT2.pdf

[15] Joanie Wexler, "802.11 vs. Bluetooth". Network World Wireless Newsletter, July 5, 2000. URL: http://www.nwfusion.com/newsletters/wireless/2000/0703wire2.html

[16] ZDNet.com, "Wireless Standard Compared". Online publication from PC Magazine, March 28, 2000. URL: http://www.zdnet.com/products/stories/reviews/0,4161,2475113,00.html

[17] Cassimir Medford, "Teething Problems". Mobile Computing Online. August 2, 2001. Online publication. URL: http://www.mobilecomputing.com/printarchives.cgi?151

[18] Paul Rasmussen, "WLAN provokes ostrich behaviour". Click I.T. Ltd "Incisor" electronic newsletter, volume 33, July 2001. URL: http://www.click.co.uk/inc_33_jul2001.pdf

[19] Cathal McDaid, "Bluetooth and 802.11b". On-line publication. January 2002. URL: http://www.infotooth.com/bluearticles/cc4_bluetooth802.11b_part1.asp

[20] Jaap Haarsten, Mahmoud Naghshineh, Jon Inouye, Olaf J. Joeressen and Warren

Allen, Bluetooth: Vision, Goals, and Architecture. In ACM Mobile Computing and Communications Review 2(4):38-45, October 1998. URL: http://www.cse.ogi.edu/~jinouye/papers/btmc2r.ps

[21] Thomas Mȯller, "Bluetooth Security Architecture version 1.0". Bluetooth SIG white paper. July 15, 1999.

[22] Nikhil Anand, "An Overview of Bluetooth Security". SANS Institute on-line publication. URL: http://rr.sans.org/wireless/bluetooth.php

[23] Marjaana Trδskbδck, "Security of Bluetooth: An Overview of Bluetooth Security". On-line publication. URL: http://www.cs.hut.fi/Opinnot/Tik-86.174/Bluetooth_Security.pdf

[24] Cathal McDaid, "Bluetooth Security". On-line publication. February 2001. URL: http://www.infotooth.com/bluearticles/cc1_security1.asp

[25] Gregory Lamn, Gerlando Falauto, Jorge Estrada, Jag Gadiyaram and Daniel Cockerham, Bluetooth Wireless Networks Security Features. In Proceedings of the 2001 IEEE Workshop on Information Assurance and Security. United Sates Military Academy, West Point, NY, 5-6 June, 2001.

[26] Cylink Corporation. URL: http://www.cylink.com/

[27] National Institute of Standards and Technology, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)". Federal Information Processing Standards Publication 197 (FIPS 197). November 26, 2001. URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[28] National Institute of Standards and Technology, "AES Algorithm (Rijndael) Information". On-line publication. URL: http://csrc.nist.gov/encryption/aes/rijndael/

[29] Markus Jakobsson and Susanne Wetzel, Security Weaknesses in Bluetooth. In David Naccache, editor, Progress in Cryptology – CT-RSA 2001: The Cryptographer's Track at RSA Conference 2001, volume 2020 of Lecture Notes in Computer Science, pages 176-191. Springer-Verlag 2001. URL: http://link.springer.de/link/service/series/0558/papers/2020/20200176.pdf

[30] Juha T. Vainio. Bluetooth Security. In Proceedings of Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory, Seminar on Internetworking: Ad hoc networking. May 25, 2000. URL: http://www.niksula.cs.hut.fi/~jiitv/bluesec.html

[31] Markku-Juhani O. Saarinen. "Re: Bluetooth und E0", Posting to sci.crypt.research, February 9, 2000. URL: http://groups.google.com/groups?q=Re:+Bluetooth+und+E0

[32] Patrik Ekdahl and Thomas Johansson. Some Results on Correlations in the Bluetooth Stream Cipher. In Proceedings of the 10th Joint Conference on Communications and Coding. Oberauern, Austria, March 11-18, 2000.

[33] Mija. Hermelin and Kaisa. Nyberg, Correlation Properties of the Bluetooth Combiner. In Proceedings of the 3rd International Conference on Information Security and Cryptology – ICISC '99, volume 1787 of Lecture Notes in Computer Science.. Springer-Verlag 1999.

[34] Scott R. Fluhfer and Stefan Lucks, Analysis of the E_0 Encryption System. In Serge Vaudenay and Amr M. Youssef, editors, Selected Areas in Cryptography 8th Annual Workshop – SAC 2001, volume 2259 of Lecture Notes in Computer Science, pages 38-48. Springer-Verlag 2001. URL: http://link.springer.de/link/service/series/0558/papers/2259/22590025.pdf

[35] Jovan Golic and Vittorio Bagini and Guglielmo Morgari, Linear Cryptanalysis of Bluetooth Stream Cipher. In Eurocrypt 2002, to appear, April 28-May 2, 2002.

[36] Electronic Frontier Foundation, "EFF DES Cracker Project". On-line publication. URL: http://www.eff.org/descracker/

[37] Electronic Frontier Foundation, Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design, O' Reilly, 1998.

[38] Jim Geier, Interference Potential Between Bluetooth and IEEE 802.11, Wireless-Net Ltd. White Paper. January 2000. URL http://www.wireless-nets.com/whitepaper_interference.htm

[39] IEEE 802.15 WPAN Task Group 2 (TG2). IEEE Task Group Website available at URL:

http://grouper.ieee.org/groups/802/15/pub/TG2.html

[40] Jim Zyren, Reliability of IEEE 802.11 Hi Rate DSSS WLANs in a High Density Bluetooth Environment. WLANA White Paper. June 8, 1999. URL: http://www.wlana.org/learn/reliabwlan.pdf

[41] BlueGiga Technologies. URL: http://www.bluegiga.com/

[42] connectBlue AB. URL: http://www.connectblue.se/

[43] Bitstream. URL: http://www.bitstream.se/wireless/e_productstxt.htm

[44] Crossbow Technologies, Inc. URL: http://www.xbow.com/crossnet/Products/Node.htm

[45] Impulsesoft Pvt. Ltd. URL: http://www.impulsesoft.com/

[46] Possio AB. URL: http://www.possio.com/

[47] Mathew C. Valenti, Max Robert and Jeffrey H. Reed, On the Throughput of Bluetooth Data Transmissions. In Proceedings of IEEE Wireless Communications and Networking Conference (WCNC), March 2002, to appear.