ΜΕΛΕΤΗ ΚΑΙ ΑΞΙΟΛΟΓΗΣΗ ΤΩΝ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ ΤΟΥ ΠΡΩΤΟΚΟΛΛΟΥ BLUETOOTH

Η Διπλωματική Εργασία

παρουσιάστηκε ενώπιον

του Διδακτικού Προσωπικού του

Πανεπιστημίου Αιγαίου

Σε Μερική Εκπλήρωση

των Απαιτήσεων για το Δίπλωμα του

Μηχανικού Πληροφοριακών και Επικοινωνιακών Συστημάτων

του

ΑΝΔΡΕΑΔΗ ΑΛΕΞΗ

και

ΠΑΓΑΝΟΥ ΧΑΡΑΛΑΜΠΟΥ

ΕΑΡΙΝΟ ΕΞΑΜΗΝΟ 2005

Η ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ ΔΙΔΑΣΚΟΝΤΩΝ ΕΓΚΡΙΝΕΙ
ΤΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
ΤΟΥ ΑΝΔΡΕΑΔΗ ΑΛΕΞΗ ΚΑΙ ΠΑΓΑΝΟΥ ΧΑΡΑΛΑΜΠΟΥ

ΓΚΡΙΤΖΑΛΗΣ ΣΤΕΦΑΝΟΣ, Επιβλέπων
Τμήμα Μηχανικών Πληροφοριακών και
Επικοινωνιακών Συστημάτων

ΚΑΜΠΟΥΡΑΚΗΣ ΓΕΩΡΓΙΟΣ, Μέλος
Τμήμα Μηχανικών Πληροφοριακών και
Επικοινωνιακών Συστημάτων

ΛΑΜΠΡΙΝΟΥΔΑΚΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ, Μέλος
Τμήμα Μηχανικών Πληροφοριακών και
Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΕΑΡΙΝΟ ΕΞΑΜΗΝΟ 2005

ΠΕΡΙΛΗΨΗ

Αντικείμενο της παρούσας διπλωματικής εργασίας είναι η μελέτη και αξιολόγηση των χαρακτηριστικών ασφαλείας του πρωτοκόλλου Bluetooth. Η ασύρματη τεχνολογία του πρωτοκόλλου Bluetooth παρέχει μικρής εμβέλειας ασύρματη επικοινωνία μεταξύ διαφόρων συσκευών, όπως είναι ηλεκτρονικοί υπολογιστές, κινητά τηλέφωνα και PDAs. Όμως, εξαιτίας της ασύρματης φύσης του τα δεδομένα που ανταλλάσει αποστέλλονται διαμέσου του αέρα και κατά συνέπεια μπορούν να γίνουν στόχος οποιουδήποτε κακόβουλου χρήστη. Εξετάζουμε, λοιπόν, τα γηγενή χαρακτηριστικά ασφαλείας (καταστάσεις ασφαλείας), τα σημεία ευπάθειας που έχουν ανακαλυφθεί μέχρι σήμερα και προτείνουμε λύσεις με στόχο την όσο το δυνατόν μεγαλύτερη διασφάλιση της μετάδοσης. Γίνεται ιδιαίτερη αναφορά για την περίπτωση των ad hoc δικτύων που χρησιμοποιούν το πρωτόκολλο Bluetooth και περιγράφονται τα προβλήματα ασφαλείας που εμφανίζονται. Επίσης, χρησιμοποιήθηκαν τα εργαλεία redfang και hcitool σε περιβάλλον Linux.

Στη δεύτερη ενότητα, στόχος μας είναι η αξιολόγηση της απόδοσης ενός δικτύου PAN (Personal Area Network) το οποίο χρησιμοποιεί το πρωτόκολλο Bluetooth ανάλογα με το αν εφαρμόζει τα γηγενή χαρακτηριστικά ασφαλείας, το πρωτόκολλο SSH ή το πρωτόκολλο IPsec. Στόχος μας είναι να συμπεράνουμε ποια προτεινόμενη λύση είναι πιο αποδοτική αλλά και πιο ασφαλής. Για αυτό το σκοπό, βασιστήκαμε σε μετρήσεις για κάθε περίπτωση μεταφέροντας δυο αρχεία διαφορετικού μεγέθους και στη συνέχεια συγκρίναμε πέντε δείκτες απόδοσης του δικτύου: χρόνος μεταφοράς, καθυστέρηση, εύρος ζώνης, throughput και χρησιμοποίηση του δικτύου.

ΑΝΔΡΕΑΔΗΣ ΑΛΕΞΗΣ, ΠΑΓΑΝΟΣ ΧΑΡΑΛΑΜΠΟΣ
Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ABSTRACT

The objective of our diploma thesis is the study and evaluation of the security characteristics of Bluetooth protocol. The wireless technology of Bluetooth protocol provides wireless communication of short range between various devices, such as personal computers, mobile phones and PDAs. However, due to its wireless nature, the exchanged data are sent through the air and consequently malicious users could capture them. So, we examine the native security characteristics (security modes), some vulnerability issues which have been mentioned till today and we suggest solutions aiming to raise the security standards of the communication. Also, we have used the hcitool and redfang tool under the Linux operating system.

In the second section, our aim is the evaluation of the performance of a Bluetooth PAN (Personal Area Network) which uses various security mechanisms such as the native security mechanism of Bluetooth protocol, the SSH protocol and the IPsec protocol. We aim to figure out which of the suggested solutions is more secure and efficient. For this purpose, we based on measurements for each case. We used two files of different size, transferred them through the PAN and at the end we compared five network parameters: transfer time, latency, bandwidth, throughput and network utilization.

ANDREADIS ALEXIS, PAGANOS CHARALAMPOS
Department of Information and Communication Systems Engineering
UNIVERSITY OF THE AEGEAN

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΓΡΑΦΗΜΑΤΩΝ

ΚΕΦΑΛΑΙΟ 1
ΕΙΣΑΓΩΓΗ

Είναι πλέον γεγονός πως βρισκόμαστε στην κοινωνία της πληροφορίας. Οι τεχνολογίες της πληροφορικής και των επικοινωνιών καλύπτουν όλο το φάσμα της οικονομικής και κοινωνικής ζωής. Για τη μετάδοση των δεδομένων ολοένα και περισσότερο χρησιμοποιούνται οι ασύρματες και κινητές τεχνολογίες. Μία απ' αυτές είναι και το Bluetooth τα οφέλη του οποίου είναι αρκετά ελκυστικά. Οπότε, οι συσκευές εξοπλισμένες με Bluetooth έχουν βρει το δικό τους δρόμο σε διάφορα περιβάλλοντα και χρησιμοποιούνται για ένα ευρύ φάσμα εφαρμογών. Ωστόσο, επειδή αυτή η τεχνολογία είναι σχετικά νέα, πρέπει να αναλυθούν προσεκτικά τα σημεία ασφάλειας.

Οι επιλογές ασφαλείας που καθορίζονται από τις προδιαγραφές θα περιγραφούν διεξοδικά. Όμως, δε θα περιοριστούμε σ' αυτά που ήδη έχουν γραφτεί αλλά θέλουμε να δώσουμε μια εκ των έσω άλλη διάσταση στο πώς οι ενδεχόμενοι κίνδυνοι και οι απειλές στην ασφάλεια έχουν επίδραση στην ανάπτυξη της τεχνολογίας του Bluetooth προτείνοντας παράλληλα και αντίμετρα σε αντίστοιχες επιθέσεις.

1.1 Ιστορική αναδρομή

Η τεχνολογία Bluetooth αποτελεί μια από τις νεότερες τεχνολογίας ασύρματης επικοινωνίας. Το όνομα προέρχεται από το Δανό βασιλιά του δέκατου αιώνα Harald Bluetooth, ο οποίος ένωσε την Δανία και εγκαθίδρυσε τον Χριστιανισμό ως επίσημη θρησκεία. Οι ερμηνείες για αυτή την επιλογή είναι πολλές και δεν υπάρχει κάποιος ιδιαίτερος λόγος να αναζητήσουμε ποια είναι η αληθινή [1].

Ο αρχικός στόχος των σχεδιαστών της τεχνολογίας Bluetooth ήταν η δημιουργία ενός πρωτόκολλου αντικατάστασης των καλωδίων για ασύρματη σύνδεση. Στην συνέχεια επεκτάθηκε για να συμπεριλάβει και περιπτώσεις σύνδεσης με σημεία πρόσβασης (φωνής και δεδομένων) και προσωπικά περιστασιακά δίκτυα (ad hoc personal area networks, PAN).

Υπεύθυνη για τον σχεδιασμό, την διάδοση και την εξέλιξη της τεχνολογίας Bluetooth είναι η Ομάδα Ειδικού Ενδιαφέροντος Bluetooth (Bluetooth Special Interest Group, SIG). Η ομάδα αυτή ιδρύθηκε το Μάιο του 1998, ενώ τα ιδρυτικά της μέλη ήταν οι εταιρείες Ericsson, Nokia, Intel, IMB και Toshiba [2]. Από την ίδρυσή της μέχρι σήμερα έχουν ενσωματωθεί στην Ομάδα Ειδικού Ενδιαφέροντος οι μεγαλύτερες εταιρείες τηλεπικοινωνιών, όπως οι 3Com, Microsoft, Motorola, Lucent κ.α. Ο αριθμός των μελών της έχει ξεπεράσει πλέον τις 1800, καθιστώντας έτσι την τεχνολογία Bluetooth μια από τις πιο γρήγορα αναπτυσσόμενες τεχνολογίες παγκοσμίως [3] [4].

Η ασύρματη τεχνολογία Bluetooth παρέχει μικρής εμβέλειας ασύρματη επικοινωνία μεταξύ διαφόρων συσκευών, π.χ. ηλεκτρονικοί υπολογιστές , κινητά τηλέφωνα, PDAs [5]. Μια πολύ κοινή πλέον χρήση του είναι η αποστολή αρχείων (εικόνες , ήχοι κλπ) μεταξύ συσκευών κινητών τηλεφώνων. Έτσι, αποφεύγεται η χρήση καλωδίων αλλά και πλέον οι συσκευές που επικοινωνούν δεν χρειάζεται να

έχουν απόλυτη οπτική επαφή μεταξύ τους όπως χαρακτηριστικά συνέβαινε με την χρήση των υπέρυθρων ακτίνων. Η χρησιμότητα αυτής της δυνατότητας είναι προφανής αρκεί να σκεφθούμε πόσο συχνά χρειαστήκαμε να δημιουργήσουμε ένα τοπικό δίκτυο μεταξύ υπολογιστών (φορητών και σταθερών) χωρίς όμως να θέλουμε να μπλέξουμε με καλώδια. Έτσι απλά, ο κάθε προσωπικός υπολογιστής με την χρήση ενός Bluetooth adaptor μπορεί να συνδεθεί στο δίκτυο. Στα ασύρματα περιβάλλοντα όπου οι συνδέσεις εγκαθίστανται μετά από αίτηση και όχι εξ ορισμού (χωρίς την ανάγκη κεντρικοποιημένης υποδομής) και όπου ένας κόμβος μπορεί να επικοινωνήσει με έναν άλλον, τα δίκτυα αυτά ονομάζονται ad hoc.Αυτού του τύπου δίκτυα μπορεί να είναι και συνδέσεις Bluetooth. Έτσι, το Bluetooth μπορεί να χρησιμοποιηθεί για τον σχηματισμό ad hoc δικτύων μέχρι 8 συσκευών (piconets). Όπως θα δούμε παρακάτω, τα ad hoc δίκτυα επιβάλλουν ειδικές απαιτήσεις για την ασφαλή λειτουργία του συστήματος [6].

1.2 Δομή του Bluetooth

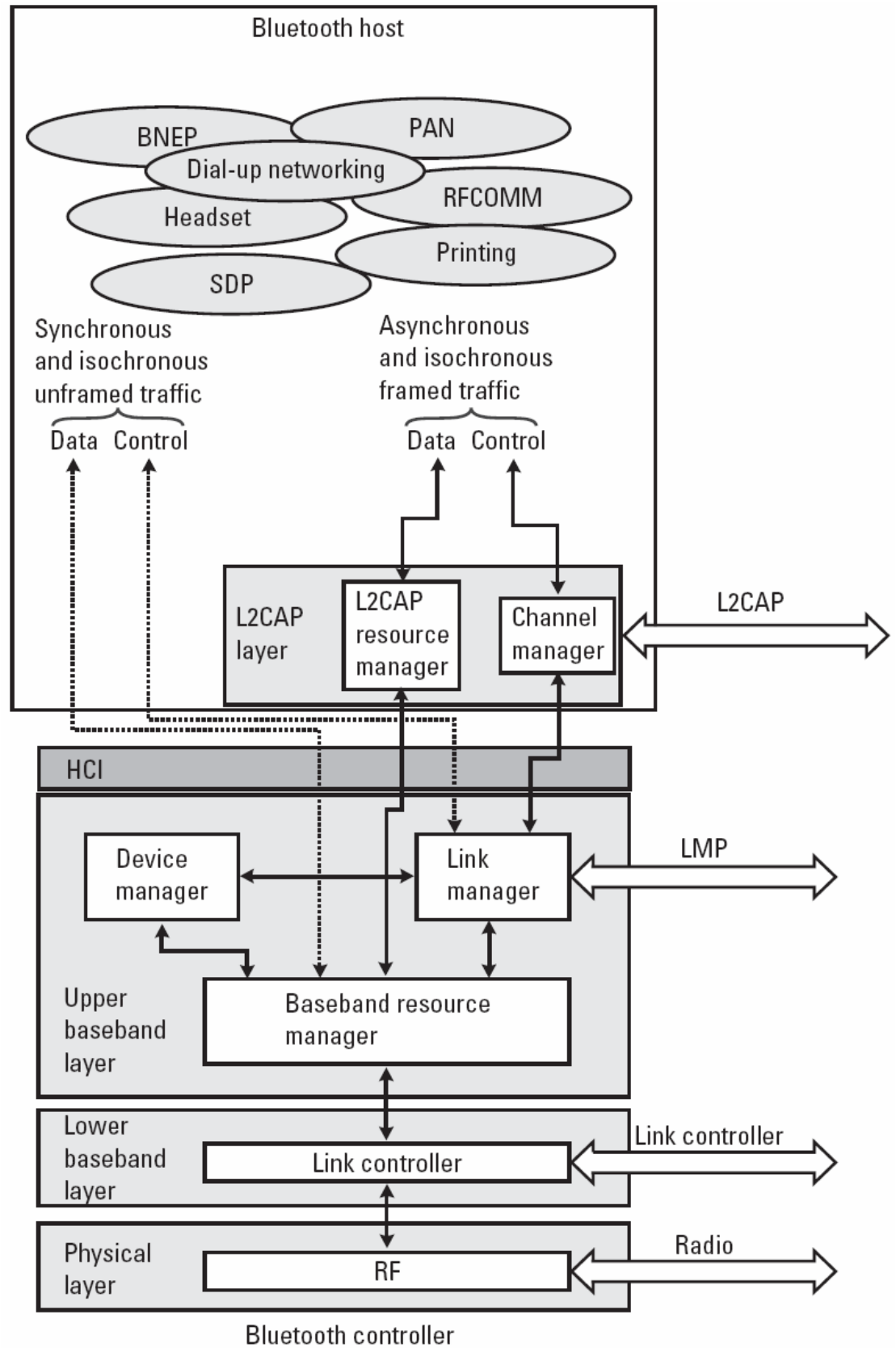
Η στοίβα του Bluetooth χωρίζεται σε επίπεδα σύμφωνα με το παρακάτω σχήμα (εικόνα 1-1). Χαμηλά βρίσκεται το *φυσικό επίπεδο* στο οποίο γίνεται η μετάδοση των κυμάτων. Τα όρια στην ευαισθησία (ακτίνα δράσης) και την παρεμβολή καθορίζονται από το σήμα και τα φίλτρα που έχουν υλοποιηθεί σ' αυτό το επίπεδο [7].

Πάνω από το φυσικό επίπεδο έχουμε το *baseband επίπεδο* το οποίο χωρίζεται σε άνω και κάτω μέρη. Σ' αυτό το στρώμα μορφοποιούνται τα πακέτα: δημιουργία επικεφαλίδων, υπολογισμοί του checksum, διαδικασία αναμετάδοσης και, προαιρετικά, κρυπτογράφηση και αποκρυπτογράφηση. Ο ελεγκτής της σύνδεσης (*link controller* – LC) είναι μια οντότητα που υλοποιεί το πρωτόκολλο και τις διαδικασίες στο baseband.

Οι Bluetooth συνδέσεις διαχειρίζονται από το διαχειριστή της σύνδεσης (*link manager* – LM). Οι συσκευές εγκαθιστούν τις συνδέσεις, διαπραγματεύονται τις επιλογές και διαχειρίζονται τις συνδέσεις που τρέχουν χρησιμοποιώντας το πρωτόκολλο διαχείρισης της σύνδεσης (*link manager protocol* – LMP) [8].

Τα μεγάλα πακέτα δεδομένων χρειάζεται να μορφοποιηθούν σε μικρότερες μονάδες πριν μεταδοθούν πάνω από τη σύνδεση Bluetooth. Ευθύνη γι' αυτό έχει το πρωτόκολλο επικοινωνίας και προσαρμογής της λογικής σύνδεσης (*logical link communication and adaption protocol* – L2CAP).

Σε πολλές περιπτώσεις, η λειτουργικότητα του Bluetooth ολοκληρώνεται σε μια φιλοξενούμενη οντότητα που έχει υπολογιστική δύναμη αλλά στερείται δυνατοτήτων στο μέρος της ραδιοζεύξης. Γι' αυτό το σκοπό, τα *Bluetooth modules* χειρίζονται τα υπάρχοντα κατώτερα επίπεδα. Η οντότητα αυτή που χειρίζεται τη λειτουργικότητα σε αυτά τα επίπεδα ονομάζεται ελεγκτής Bluetooth (*Bluetooth controller*). Για παράδειγμα, ένας φορητός υπολογιστής που είναι ικανός στο να χειρίζεται πρωτόκολλα υψηλού επιπέδου μπορεί να επεκταθεί σε module που διευθύνει τη σηματοδοσία, το baseband και το L2CAP. Σε μια τέτοια εγκατάσταση, τα υψηλότερα επίπεδα που υλοποιούνται στην φιλοξενούμενη οντότητα θα επικοινωνούν με τα χαμηλότερα επίπεδα μέσω της αλληλεπίδρασης του φιλοξενούμενου ελεγκτή (*host controller interface* – HCI).



Εικόνα 1-1 Bluetooth protocol stack architecture

1.2.1 Φυσικό επίπεδο

Η σηματοδοσία του Bluetooth λειτουργεί στην ελεύθερη και παγκοσμίως διαθέσιμη για βιομηχανικούς, επιστημονικούς και ιατρικούς σκοπούς (ISM) μπάντα των 2,4 GHz [9]. Επειδή η μπάντα αυτή είναι ελεύθερη, το Bluetooth μοιράζεται αυτές τις συχνότητες και με άλλα συστήματα. Αρκετά συστήματα ασύρματης επικοινωνίας καθώς και οι φούρνοι μικροκυμάτων λειτουργούν σ' αυτή την περιοχή συχνοτήτων με αποτέλεσμα να είναι πιθανό να παρουσιαστεί παρεμβολή. Στην πραγματικότητα η διαρροή μπορεί να είναι έως και 1000 φορές πιο δυνατή από το σήμα που μια συσκευή προσπαθεί να λάβει, έτσι η παρεμβολή δεν μπορεί να αγνοηθεί. Για να αντιμετωπιστεί αυτό το πρόβλημα, το Bluetooth έχει αναπτύξει μια τεχνολογία αναπήδησης συχνοτήτων (*frequency hopping* – FH). Υπάρχουν 79 κανάλια κάθε ένα από τα οποία χρησιμοποιεί εύρος ζώνης 1 MHz. Κατά τη διάρκεια της επικοινωνίας, το σύστημα κάνει 1600 αναπηδήσεις το δευτερόλεπτο δοκιμάζοντας μετάδοση πάνω απ' αυτά τα κανάλια σύμφωνα με μια ψευδοτυχαία σειρά. Η ιδέα είναι ότι εάν υπάρχει μετάδοση δεδομένων σε ένα «κακό» κανάλι, με την επόμενη αναπήδηση συχνότητας, που είναι μόλις 625 μs αργότερα, ελπίζουμε να βρεθούμε σε ένα «καλό» κανάλι. Γενικότερα, η γρηγορότερη αναπήδηση μεταξύ των συχνοτήτων μας δίνει καλύτερη μετάδοση και βελτιώνει την προστασία από πιθανή παρεμβολή. Ωστόσο, η επίδοση εξαρτάται και από την πολυπλοκότητα της αναπήδησης. Έτσι, ο ρυθμός της αναπήδησης πρέπει να βρίσκεται στη χρυσή τομή μεταξύ της επίδοσης και της πολυπλοκότητας.

Το σήμα μεταδίδεται χρησιμοποιώντας οκταδικό κλειδί με μετακίνηση συχνότητας. Ο ρυθμός μετάδοσης είναι 1 Mbps αλλά εξαιτίας των διαφόρων πρωτοκόλλων που τρέχουν, ο ρυθμός μετάδοσης των δεδομένων του χρήστη δεν μπορεί να ξεπεράσει τα 723 Kbps.

Οι συσκευές αυτές χωρίζονται σε τρεις κατηγορίες ανάλογα με την ισχύ που χρησιμοποιούν. Η *κατηγορία 3* (class 3) έχει ισχύ μετάδοσης 1 mWatt και εμβέλεια 0,1 με 10 μέτρα. Η *κατηγορία 2* (class 2) έχει ισχύ μετάδοσης 1 με 2,5 mWatt και εμβέλεια 10 μέτρων. Τέλος, στην *κατηγορία 1* (class 1) η ισχύς μετάδοσης φθάνει μέχρι τα 100 mWatt ενώ η εμβέλεια αγγίζει τα 100 μέτρα. Οι περισσότερες συσκευές Bluetooth ανήκουν κυρίως στην δεύτερη και τρίτη κατηγορία. Επίσης στις συσκευές ενσωματώνεται ένας μηχανισμός περιορισμού της ισχύς μετάδοσης στην απολύτως αναγκαία, ανάλογα με την απόσταση μεταξύ των συσκευών.

1.2.2 Baseband

Διευθυνσιοδότηση και εγκατάσταση συνδέσεων

Κάθε Bluetooth συσκευή έρχεται με μία μοναδική, ορισμένη από τον κατασκευαστή 48-bit διεύθυνση. Αυτή η διεύθυνση λέγεται *Bluetooth device address* (BD_ADDR) και χρησιμοποιείται για τη βασική αυθεντικοποίηση των συσκευών όταν οι συνδέσεις εγκαθίστανται. Πριν από την εγκατάσταση οποιασδήποτε σύνδεσης, η BD_ADDR πρέπει να γνωστοποιείται στην πλευρά που αρχικοποιεί τη σύνδεση. Για συνδέσεις, οι οποίες πρώτη φορά εγκαθίστανται, η γνωστοποίηση της διεύθυνσης της συσκευής γίνεται με τον εξής τρόπο: Η πλευρά που αρχικοποιεί τη σύνδεση συλλέγει όλες τις διευθύνσεις των συσκευών από τις κοντινές μονάδες και έπειτα επιλέγει τη διεύθυνση του ενδιαφέροντός του. Αυτό το βήμα είναι γνωστό ως *διαδικασία αναζήτησης* (inquiry procedure). Υπό φυσιολογικές συνθήκες, αυτό

γίνεται μόνο μια φορά, η πληροφορία αποθηκεύεται και μπορεί να ξαναχρησιμοποιηθεί χωρίς την ανάγκη αναζήτησης της διεύθυνσης για τις ήδη γνωστές συσκευές.

Αναλυτικά, ο τρόπος με τον οποίο γίνεται η αρχικοποίηση μιας συσκευής: Το πρώτο βήμα στην αναζήτηση άλλων συσκευών είναι να στείλει μήνυμα αναζήτησης. Αυτό το μήνυμα μπορεί να επαναλαμβάνεται ανά τακτά χρονικά διαστήματα. Κάθε συσκευή που θέλει να είναι ορατή σε άλλους σαρώνει με κάποια συγκεκριμένη συχνότητα για μηνύματα αναζήτησης. Αυτή η διαδικασία είναι γνωστή ως *σάρωση αναζήτησης* (inquiry scan). Στη συνέχεια, η συσκευή αυτή θα απαντήσει με την BD_ADDR της και την τρέχουσα τιμή του τοπικού της ρολογιού. Εδώ πρέπει να σημειώσουμε ότι το αρχικό μήνυμα αναζήτησης είναι ανώνυμο, έτσι η αναζητούμενη συσκευή δε γνωρίζει ποιος έκανε την αναζήτηση ούτε αν ο αναζητών έλαβε σωστά την απάντηση.

Ο αναζητών συλλέγει απαντήσεις για ένα χρονικό διάστημα και αναλόγως τι επιθυμεί αγγίζει μια συγκεκριμένη συσκευή μέσω ενός μηνύματος αναφώνησης (*page* message). Το μήνυμα αυτό στέλνεται με μια ακολουθία 32 αναπηδήσεων καθορισμένο από τα 24 τελευταία σημαντικά bits της BD_ADDR (αυτά δηλώνονται από το *κατώτερο μέρος της διεύθυνσης* (lower address part – LAP) της συσκευής-στόχου. Μία συσκευή ακούει για page μηνύματα όταν βρίσκεται στην κατάσταση σάρωσης page μηνυμάτων (*page scan state*). Η ρύθμιση της ακολουθίας αναπήδησης συχνοτήτων καθορίζεται από το υπάρχον ρολόι της συσκευής. Η συσκευή που καλεί την άλλη έχει γνώση της συγκεκριμένης ακολουθίας από τη μήνυμα απάντησης που έχει ήδη λάβει. Όταν ληφθεί η απάντηση, συγχρονισμός συχνότητας συμβαίνει μεταξύ των δύο συσκευών. Εξ ορισμού, η καλούσα ονομάζεται κύρια (*master*) και η κληθείσα δευτερεύουσα (*slave*) συσκευή.

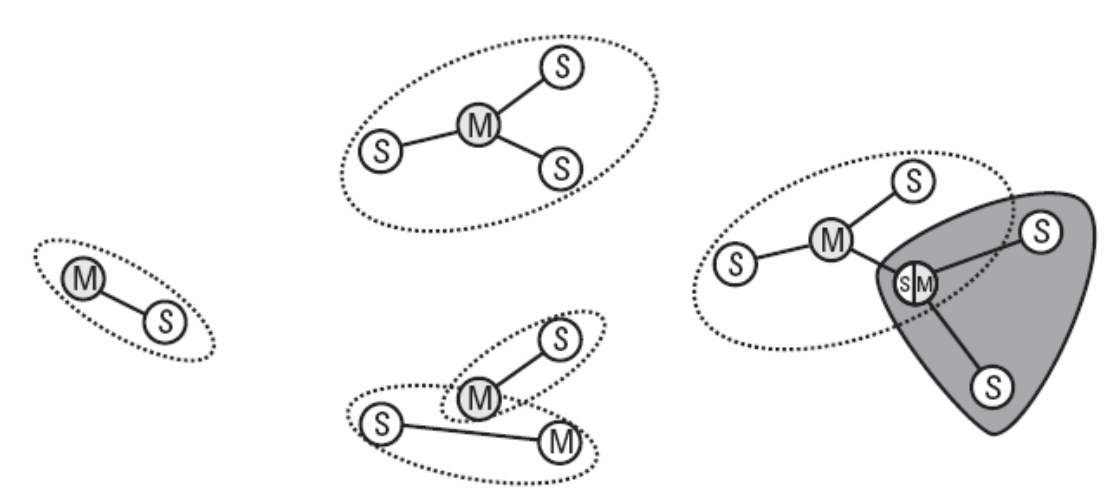
Πριν γίνει η εγκατάσταση του καναλιού κάποιες επιπλέον πληροφορίες πρέπει να ανταλλαχθούν μεταξύ των συσκευών. Η σειρά αναπήδησης της συχνότητας, ο χρονισμός και ο κωδικός πρόσβασης του καναλιού (*channel access code* – CAC) διατίθενται από την κύρια συσκευή. Με σκοπό να ρυθμιστεί σωστά ο συγχρονισμός των συχνοτήτων, η δευτερεύουσα συσκευή χρειάζεται την BD_ADDR και το ρολόι της κύριας. Η πληροφορία αυτή μεταδίδεται σε ένα ειδικό πακέτο που στέλνεται από τη master στη slave συσκευή. Με όλα αυτά τα δεδομένα και στις δυο πλευρές, οι συσκευές μπορούν πλέον να μεταφερθούν από τη συχνότητα ακρόασης (που καθορίζεται από τη δευτερεύουσα συσκευή) στη συχνότητα του βασικού καναλιού (που καθορίζεται από την κύρια συσκευή).

Τοπολογία και έλεγχος πρόσβασης

Τα δίκτυα στο Bluetooth έχουν την τοπολογία αστέρα. Όχι περισσότερες από οκτώ συσκευές μπορούν να συμμετέχουν σε ένα τέτοιο *piconet*. Ο κεντρικός κόμβος του δικτύου ονομάζεται κύριος (master) και οι υπόλοιποι δευτερεύοντες (slaves). Έτσι, ένα δίκτυο Bluetooth πρέπει να έχει ακριβώς ένα κύριο κόμβο και τουλάχιστον ένα αλλά όχι περισσότερους από οχτώ δευτερεύοντες κόμβους. Μερικές από τις πιθανές μορφές τοπολογίας ενός δικτύου Bluetooth φαίνονται παρακάτω (εικόνα 1-2).

Η ανταλλαγή πληροφοριών σε ένα τέτοιο δίκτυο γίνεται στέλνοντας πακέτα από και προς τις συσκευές. Η διπλοκατευθυντική επικοινωνία μεταξύ των συσκευών επιτυγχάνεται με τη μέθοδο του διπλού διαχωρισμού του χρόνου. Μ' αυτόν τον τρόπο το κανάλι χωρίζεται σε χρονοθυρίδες ανάλογα με τον αριθμό των επικοινωνούντων

μερών. Για το ποιος έχει πρόσβαση στο κανάλι υπεύθυνη είναι η κύρια συσκευή του piconet. Μόνο η master-to-slave και slave-to-master επικοινωνία είναι δυνατή. Συνεπώς, η διακίνηση δεδομένων μεταξύ δύο δευτερευόντων συσκευών γίνεται διαμέσου της κύριας. Βέβαια, το γεγονός ότι μία και μόνο συσκευή εμπλέκεται στη μεταφορά των δεδομένων, αυτό κρύβει τον κίνδυνο να υπάρξει συμφόρηση. Ωστόσο, μία σημαντική αρχή στο Bluetooth είναι ότι οποιαδήποτε συσκευή έχει την ικανότητα να λάβει ρόλο είτε ως δευτερεύουσα είτε ως κύρια και έτσι κάποιες δευτερεύουσες συσκευές μπορούν να δημιουργήσουν ένα άλλο piconet. Επίσης μια συσκευή Bluetooth επιτρέπεται να συμμετέχει σε περισσότερα του ενός δικτύων. Για να συμβεί όμως αυτό η συσκευή αυτή θα πρέπει να διαμοιράζει τον διαθέσιμο χρόνο και στα δύο δίκτυα. Για να προσαρμοστεί όμως παράλληλα και στο άλλο δίκτυο χρειάζεται να μπει σε κατάσταση χαμηλής ισχύος (lower-power mode) ώστε να μπορεί να αφήνει εικονικά το ένα δίκτυο και να πηγαίνει προσωρινά στο άλλο. Πάντως υπάρχουν και κάποια πρακτικά προβλήματα σ' αυτή τη δυνατότητα, όπως ο καταμερισμός του χρόνου, η ποιότητα των παρερχομένων υπηρεσιών και περιορισμός ότι μια συσκευή μπορεί να είναι κύρια το πολύ σε ένα piconet.



Εικόνα 1-2 Τρόποι σύνδεσης Bluetooth συσκευών

Τρόποι μετάδοσης δεδομένων

Η τεχνολογία ασύρματης επικοινωνίας Bluetooth έχει σχεδιαστεί έτσι ώστε να μπορεί να χειριστεί διαφορετικούς τρόπους μετάδοσης δεδομένων. Η μετάδοση μπορεί να είναι *ασύγχρονη* όταν δεν έχουμε μεγάλες απαιτήσεις για ποιότητα υπηρεσίας, όπως η μεταφορά δεδομένων. Από την άλλη μπορεί να είναι και *σύγχρονη* π.χ. όταν πρόκειται για πραγματικού χρόνου εφαρμογές ή διμερείς συνδέσεις.

Μια σύγχρονη σύνδεση είναι η σύγχρονη προσανατολισμένα επικοινωνία (synchronous connection oriented – SCO) και η εμπλουτισμένη σύγχρονη προσανατολισμένη επικοινωνία (enhanced synchronous connection oriented – eSCO). Και οι δυο αυτές συνδέσεις παρέχουν σταθερό ρυθμό μετάδοσης δεδομένων μεταφέροντας προκαθορισμένου μεγέθους πακέτα σε ήδη κατειλλημένες θύρες πάνω από το φυσικό κανάλι. Το eSCO είναι πιο ευέλικτο από το SCO επειδή προσφέρει μεγαλύτερη ελευθερία στην επιλογή του ρυθμού μετάδοσης και πιο αξιόπιστο διότι ένας περιορισμένος αριθμός επανεκπομπών μπορεί να συμβεί στις εφεδρικές θύρες.

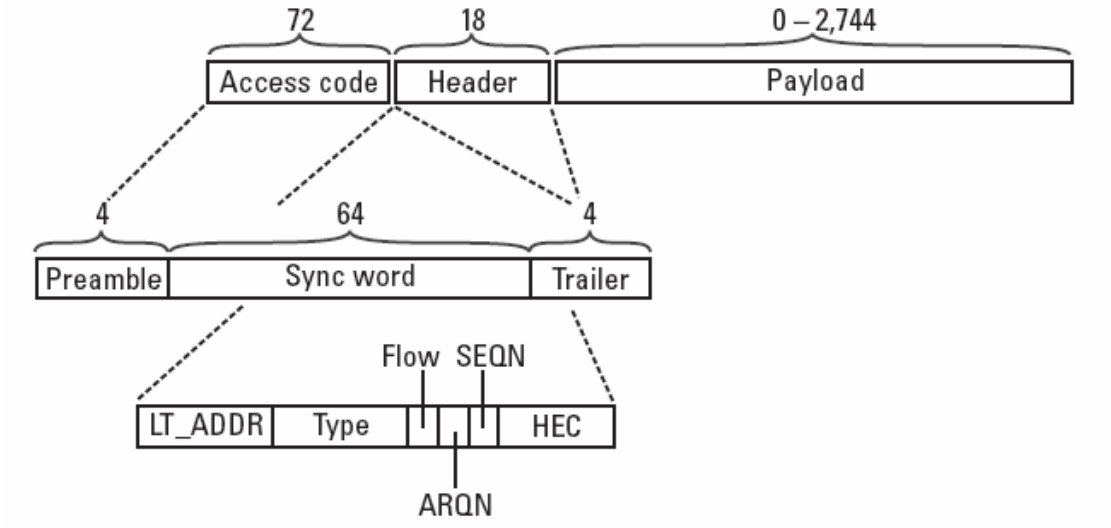
Μια ασύγχρονη σύνδεση είναι η ασύγχρονη προσανατολισμένη επικοινωνία (asynchronous connection oriented – ACL). Αυτή είναι point-to-multipoint σύνδεση μεταξύ της κύριας συσκευής και όλων των άλλων των δευτερευόντων. Εδώ δε χρησιμοποιούνται κατειλλημένες θυρίδες.

Δομή πακέτων

Ένα πακέτο αποτελείται από τον κωδικό πρόσβασης, την επικεφαλίδα και το ωφέλιμο φορτίο (payload). Ο κωδικός πρόσβασης που είναι πρώτος σε κάθε πακέτο χρησιμοποιείται για να «ξυπνήσει» και να συγχρονίσει τον παραλήπτη. Κάθε δίκτυο χρησιμοποιεί έναν μοναδικό κωδικό πρόσβασης που προέρχεται από την BD_ADDR της κύριας συσκευής. Έτσι, εξετάζοντας τον κωδικό πρόσβασης, ο παραλήπτης μπορεί να προσδιορίσει αν ένα πακέτο προέρχεται από κάποιο άλλο δίκτυο και να το απορρίψει. Επιπλέον, αφού ο κωδικός αυτός καθορίζει τα όρια των θυρίδων, χρησιμοποιείται για να συγχρονίσει τα ρολόγια της δευτερεύουσας συσκευής με την κύρια.

Η επικεφαλίδα του πακέτου χρησιμοποιείται για να διευθύνει τις δευτερεύουσες συσκευές του δικτύου. Για το σκοπό αυτό υπάρχει ένα πεδίο 3 bits που λέγεται logical transport address (LT_ADDR). Η κύρια συσκευή αναθέτει μη μηδενικές διευθύνσεις (η μηδενική διεύθυνση χρησιμοποιείται για broadcast μηνύματα) κατά την εγκατάσταση της σύνδεσης. Εκτός απ' αυτό, η επικεφαλίδα ενός πακέτου περιέχει πληροφορίες για το είδος της μετάδοσης των δεδομένων, τον έλεγχο ροής και το σχέδιο για επανεκπομπή. Για να αυξηθεί η αξιοπιστία της επικεφαλίδας κάθε bit επαναλαμβάνεται τρεις φορές. Η δομή ενός πακέτου στο επίπεδο baseband αναπαρίσταται παρακάτω.

Τα δεδομένα του χρήστη ονομάζονται ωφέλιμο φορτίο. Το μήκος αυτού του πεδίου διαφέρει ανάλογα με το είδος της μετάδοσης. Μπορεί να είναι από 0 bytes αν πρόκειται για μήνυμα επιβεβαίωσης ή αν δεν χρειάζεται να σταλούν δεδομένα έως και 339 bytes (επιπλέον των 4 bytes για την επικεφαλίδα του payload και του CRC).



Εικόνα 1-3 Η δομή των πακέτων Bluetooth

Ένα πακέτο μπορεί να καταλαμβάνει 1, 3, ή 5 θυρίδες αναλόγως τον τύπο του. Αυτό επιτρέπει την ασύμμετρη μετάδοση δεδομένων χωρίς να υπάρχει το μειονέκτημα περίσσειας επικεφαλίδων για ένα πακέτο. Ανίχνευση λαθών μπορεί να συμβεί μέσω ενός 16-bit CRC κωδικού. Επιπλέον είναι δυνατόν να γίνει και διόρθωση των λαθών στο ωφέλιμο φορτίο (forward error correction – FEC) με ρυθμό επανάληψης R=1/3 ή 2/3. Ακολουθούν δυο συνόψεις με τους τύπους των πακέτων και τους ρυθμούς μετάδοσης δεδομένων.

					Asymmetric Max. Rate	
Type	**Payload (Information Bytes)**	**FEC**	**CRC**	**Symmetric Max. Rate**	**Forward**	**Reverse**
DM1	0–17	2/3	Yes	108.8	108.8	108.8
DH1	0–27	No	Yes	172.8	172.8	172.8
DM3	0–121	2/3	Yes	258.1	387.2	54.4
DH3	0–183	No	Yes	390.4	585.6	86.4
DM5	0–224	2/3	Yes	286.7	477.8	36.3
DH5	0–339	No	Yes	433.9	723.2	57.6
AUX1	0–29	No	No	185.6	185.6	185.6

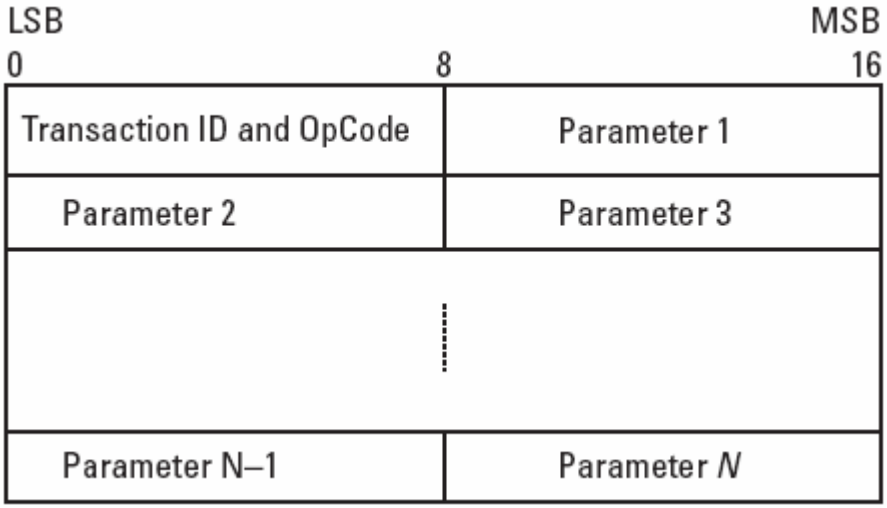
Type	**Payload (Information Bytes)**	**FEC**	**CRC**	**Symmetric Max. Rate**
HV1	10	1/3	No	64
HV2	20	2/3	No	64
HV3	30	No	No	64
DV	10 + (0–9)*	2/3*	Yes*	64 + 57.6*
EV3	1–30	No	Yes	96
EV4	1–120	2/3	Yes	192
EV5	1–180	No	Yes	288

Πίνακας 1-1 Σύνοψη πακέτων (τύποι και ρυθμοί μετάδοσης)

1.2.3 Link manager protocol

Ο διαχειριστής της σύνδεσης (*link manager* - LM) είναι υπεύθυνος για τον έλεγχο της σύνδεσης Bluetooth. Αυτό περιλαμβάνει όλα τα καθήκοντα που έχουν σχέση με την εγκατάσταση, την αμεροληψία και τη διαμόρφωση μιας σύνδεσης. Ο διαχειριστής της σύνδεσης είναι επίσης υπεύθυνος για την ανταλλαγή μηνυμάτων σχετιζόμενα με την ασφάλεια. Οι διαχειριστές ελέγχου σε διαφορετικές μονάδες ανταλλάσσουν μηνύματα ελέγχου χρησιμοποιώντας το πρωτόκολλο διαχείρισης της σύνδεσης (*link manager protocol* – LMP). Ένα σύνολο από μηνύματα ελέγχου ή μονάδες δεδομένων πρωτοκόλλου (*protocol data units* – PDU) LMP έχουν καθοριστεί. Πολλά απ' αυτά σχετίζονται με την ασφάλεια και χρησιμοποιούνται για να μεταφέρουν πληροφορίες που χρειάζεται στην αυθεντικοποίηση και την κρυπτογράφηση.

Τα LMP PDU μεταφέρονται στο ωφέλιμο φορτίο αντί των συνηθισμένων δεδομένων. Αυτά στέλνονται πάντα ως πακέτα μονής θυρίδας και μπορούν να μεταφερθούν σε δύο διαφορετικούς τύπους δεδομένων. Για να ξεχωρίσουμε τα LMP πακέτα από τα υπόλοιπα, ένας ειδικός κωδικός χρησιμοποιείται στις επικεφαλίδες των πακέτων και για να αποφύγουμε υπερχείλιση στο buffer των λαμβανόμενων πακέτων συνήθως εφαρμόζουμε την ασύγχρονη μετάδοση. Η μορφή του ωφέλιμου φορτίου των LMP PDU φαίνεται στο παρακάτω σχήμα. Αποτελείται, λοιπόν, από την επικεφαλίδα που είναι 1 byte και ακολουθούν τα δεδομένα του διαχειριστή της σύνδεσης (LM). Η επικεφαλίδα με τη σειρά της έχει δύο πεδία. Το πρώτο είναι μόνο 1 bit και περιέχει την ταυτότητα της συναλλαγής (*identifier* – ID). Το δεύτερο πεδίο είναι 7 bits και περιέχει τον κωδικό της λειτουργίας (*operation code* – OpCode). Ο κωδικός της λειτουργίας αναφέρει τον τύπο των LMP PDU που στέλνονται. Κάθε LMP μήνυμα έχει μοναδικό OpCode.



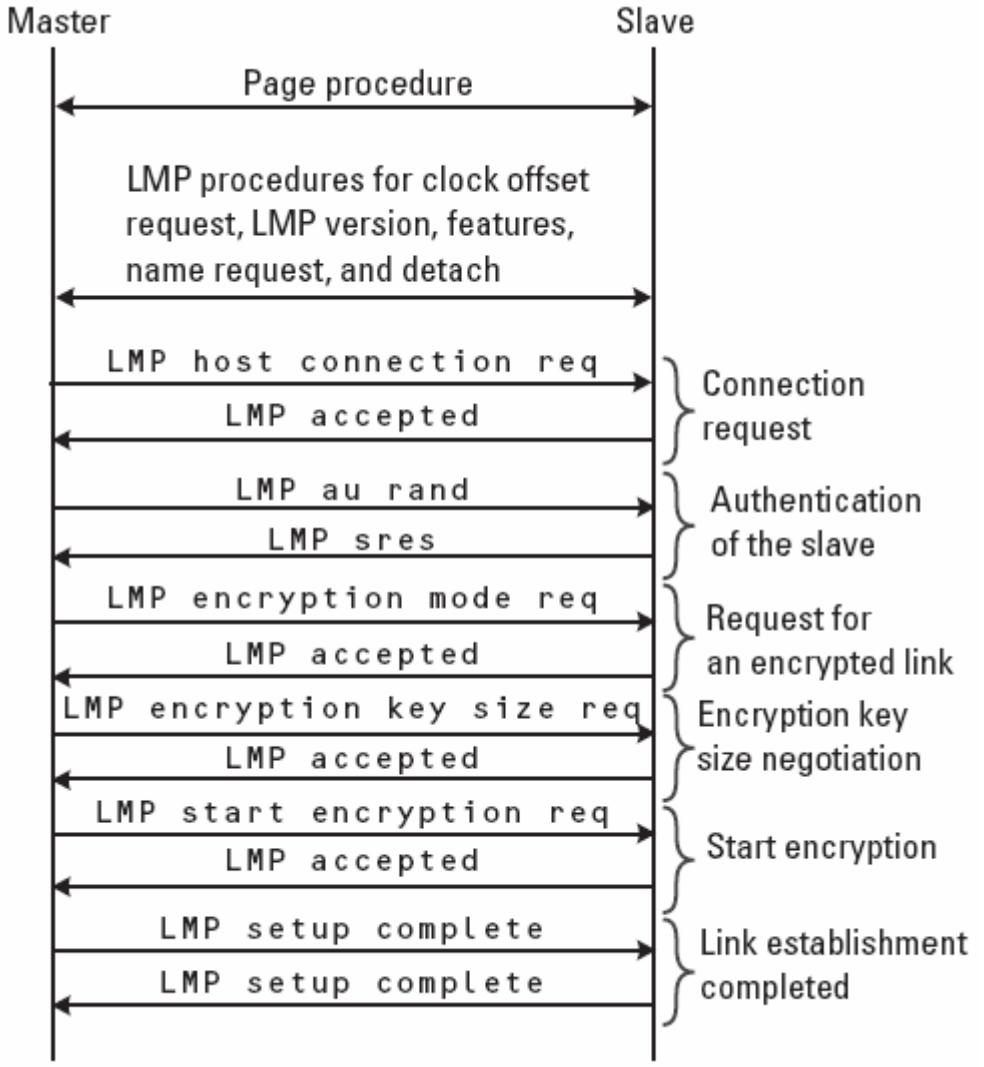
Εικόνα 1-4 Μορφή ωφέλιμου φορτίου

Όπως περιγράψαμε, το LMP χρησιμοποιείται για ελέγχει και να εγκταταστεί τη σύνδεση. Μια τυπική σειρά PDU για τη δημιουργία μιας σύνδεσης φαίνεται στο παρακάτω σχήμα. Η ίδρυση της σύνδεσης ξεκινά με την αναφώνηση (page) της δευτερεύουσας μονάδας από την κύρια. Μετά την αναφώνηση και την ανταλλαγή απαντητικών μηνυμάτων, η εγκατάσταση μπορεί να ξεκινήσει. Προτού όμως η κύρια συσκευή στείλει αίτηση για σύνδεση, πρέπει να συλλέξει κάποιες πληροφορίες από την άλλη συσκευή, όπως το ρολόι, την έκδοση του πρωτοκόλλου διαχείρισης της

σύνδεσης, άλλες παραμέτρους και το όνομα της. Ένα σύνολο από LMP PDU έχουν καθοριστεί γι' αυτό το σκοπό. Η διαδικασία εγκατάστασης της σύνδεσης τότε πραγματικά ξεκινάει με την αποστολή από την κύρια συσκευή ενός μηνύματος "LMP connection request". Έπειτα λαμβάνει χώρα η ανταλλαγή μηνυμάτων σχετικά με την ασφάλεια και τελικά η εγκατάσταση της σύνδεσης ολοκληρώνεται με την ανταλλαγή μηνυμάτων "LMP setup complete".

Ειδικά PDU σχετιζόμενα με την ασφάλεια έχουν καθοριστεί με σκοπό να επιτευχθεί:

- Αυθεντικοποίηση
- Κρυπτογράφηση
- Αλλαγή του κλειδιού της σύνδεσης



Εικόνα 1-5 Διαδικασία εγκατάστασης σύνδεσης

1.2.4 Logical link control και adaptation control

Το πρωτόκολλο επικοινωνίας και προσαρμογής της λογικής σύνδεσης (*logical link communication and adaptation protocol* – L2CAP) φροντίζει για τη κατάτμηση και επανένωση των δεδομένων, την πολύπλεξη και θέματα ποιότητας υπηρεσιών. Το L2CAP αποτελεί ένα φίλτρο ανάμεσα στα ανεξάρτητα υψηλότερα επίπεδα που τρέχουν σε μια συσκευή και στα κατώτερα επίπεδα που ανήκουν μοντέλο του Bluetooth. Για παράδειγμα, τα TCP πακέτα είναι τόσο μεγάλα για να ταιριάξουν σε ένα baseband πακέτο. Γι' αυτό, τέτοια πακέτα πρέπει να κόβονται σε μικρότερα τεμάχια δεδομένων πριν σταλούν στο baseband για περαιτέρω επεξεργασία. Στην απέναντι πλευρά, η διαδικασία αυτή αντιστρέφεται: Τα κατακερματισμένα πακέτα επανενώνονται σε μεγαλύτερες οντότητες πριν προωθηθούν στα ανώτερα στρώματα.

1.2.5 Host control interface

Η διεπαφή ελέγχου του εξυπηρετούμενου (*host control interface* – HCI) είναι μια κοινά καθορισμένη διεπαφή μεταξύ των άνω και κάτω επιπέδων στη στοίβα του Bluetooth. Όπως περιγράψαμε νωρίτερα, το HCI παρέχει τη δυνατότητα να χωρίζει τις συναρτήσεις του υλικού από τα πρωτόκολλα των υψηλότερων επιπέδων. Έτσι χρησιμοποιώντας το HCI, είναι δυνατό να χρησιμοποιούμε ένα Bluetooth module για διαφορετικές συσκευές και εφαρμογές. Ομοίως, οι υψηλού επιπέδου εφαρμογές που υλοποιούνται σε μία συσκευή μπορούν να χρησιμοποιούν οποιοδήποτε Bluetooth module που υποστηρίζεται από το HCI.

Στο παρακάτω σχήμα φαίνεται μια απεικόνιση των κατώτερων στρωμάτων του Bluetooth και του HCI. Οι HCI εντολές για ένα Bluetooth module χειρίζονται από το firmware του HCI που έχει πρόσβαση στο baseband και τον link manager. Οι εντολές αυτές μεταφέρονται ανάμεσα στο module και τον host μέσω φυσικών διαύλων, όπως μια θύρα USB ή μια κάρτα υπολογιστή.

Τα πακέτα των εντολών μπορούν να χωριστούν σε έξι υποκατηγορίες:

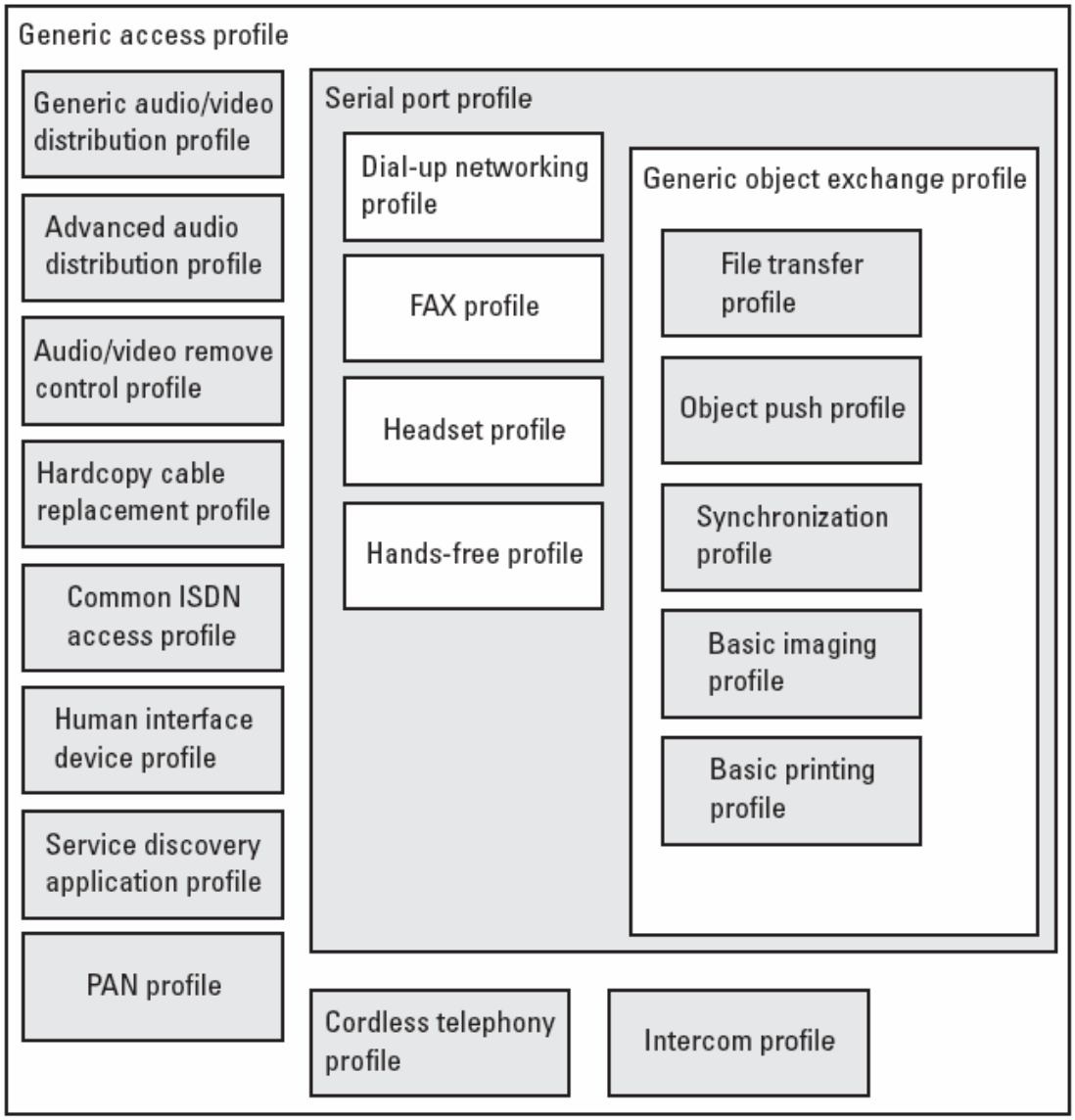
1. Εντολές ελέγχου της σύνδεσης
2. Εντολές πολιτικής της σύνδεσης
3. Εντολές του ελεγκτή του εξυπηρετούμενου και του baseband
4. Εντολές ανάγνωσης πληροφοριών
5. Εντολές ανάγνωσης καταστάσεων
6. Εντολές δοκιμών

1.2.6 Profiles

Η τεχνολογία Bluetooth δεν περιορίζεται στην περιορισμένη χρήση κάποιων εφαρμογών. Έτσι, η SIG ανέπτυξε ένα σύνολο προφίλ. Ένα προφίλ δίνει μια σαφή περιγραφή της επικοινωνίας δύο μονάδων για μία υπηρεσία. Τέτοια προφίλ έχουν καθοριστεί και για θεμελιώδεις διαδικασίες του Bluetooth αλλά και για ειδικές υπηρεσίες [10] [11].

Ένα προφίλ μπορεί να χτιστεί πάνω σε ένα ήδη υπάρχον επιτρέποντας έτσι την επαναχρησιμοποίηση των υπαρχόντων πρωτοκόλλων και διαδικασιών. Μ' αυτόν τον τρόπο δίνεται σημασία στην ιεραρχική δομή, όπως φαίνεται και στο παρακάτω σχήμα. Οι πιο βασικοί ορισμοί και απαιτήσεις που σχετίζονται με τη λειτουργία, τις

συνδέσεις και την εγκατάσταση των καναλιών δίνονται στο προφίλ γενικής πρόσβασης (*generic access profile* – GAP). Όλα τα άλλα υπάρχοντα προφίλ κάνουν χρήση του GAP. Ο πρωταρχικός σκοπός του Bluetooth ήταν η αντικατάσταση των καλωδίων στην επικοινωνία δύο συσκευών. Έτσι, εξομοίωση της σειριακής θύρας γίνεται με το *serial port profile*. Άλλα τώρα προφίλ, όπως το *dial-up networking profile* και το *hands-free profile* κάνουν χρήση του τελευταίου.



Εικόνα 1-6 Κατηγοριοποίηση των Bluetooth profiles

ΚΕΦΑΛΑΙΟ 2
ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΑΣΦΑΛΕΙΑΣ ΣΤΟ BLUETOOTH

2.1 Βασικά θέματα ασφαλείας

Τα θέματα ασφαλείας αναφέρθηκαν από την αρχή του σχεδιασμού της τεχνολογίας Bluetooth. Αποφασίστηκε ότι ακόμα και για τα απλούστερα σενάρια χρήσης, το Bluetooth πρέπει να παρέχει επιλογές ασφαλείας [12].

Βέβαια, ο ίδιος ο τρόπος μετάδοσης και λειτουργίας που χρησιμοποιεί η τεχνολογία Bluetooth παρέχει ως ένα βαθμό προστασία ενάντια στο νούμερο ένα κίνδυνο των ασυρμάτων επικοινωνιών, την υποκλοπή των δεδομένων στον ραδιοδίαυλο λόγω της αναπήδησης συχνοτήτων. Ο μηχανισμός αυτός καθιστά δύσκολο, αλλά όχι αδύνατο, σε κάποιον να βρει και να παρακολουθήσει την συχνότητας της σύνδεσης μίας συσκευής, ώστε να υποκλέψει τα δεδομένα που μεταδίδονται [13]. Επίσης υπάρχει ένας μηχανισμός για να μειώνεται στο αναγκαίο η ενέργεια που μεταδίδεται στο χώρο. Η βασική λειτουργία του μηχανισμού αυτού είναι η μείωση της κατανάλωσης ενέργειας από ελαφριές συσκευές, μειώνοντας παράλληλα και τις απαιτήσεις που αυτές έχουν από τις μπαταρίες (σχέση βάρους και απόδοσης). Παράλληλα όμως με το παραπάνω πλεονέκτημα ο μηχανισμός περιορίζει και την ακτίνα διάδοσης των δεδομένων που αποστέλλονται. Έτσι αν κάποιος θέλει να υποκλέψει τα δεδομένα θα πρέπει να βρίσκεται κοντά στην συσκευή που τα μεταδίδει κάτι που δεν είναι πάντα πολύ εύκολο.

Υπάρχουν 4 θεμελιώδεις απαιτήσεις για ασφάλεια στο Bluetooth. Αυτές είναι:

1. Εύχρηστη διαμόρφωση της ασφάλειας
2. Εμπιστευτικότητα
3. Αυθεντικοποίηση των συνδεδεμένων συσκευών
4. Ανωνυμία

2.2 Κλειδιά

2.2.1 Τύποι κλειδιών

Η διαχείριση των κλειδιών περιλαμβάνει την δημιουργία, αποθήκευση και διανομή κλειδιών για τους σκοπούς της κρυπτογράφησης των δεδομένων, της παροχής εξουσιοδότησης καθώς και της πιστοποίησης της ταυτότητας της συσκευής. Γίνεται φανερό λοιπόν ότι η διαχείριση των διαφόρων κλειδιών είναι μία από τις σπουδαιότερες παραμέτρους των διαδικασιών ασφαλείας που έχουν ενσωματωθεί στην τεχνολογία Bluetooth.

Παρόλο που η κρυπτογράφηση με την χρήση δημοσίου κλειδιού θα διευκόλυνε σε μεγάλο βαθμό την διαχείριση των κλειδιών, δεν χρησιμοποιήθηκε από την Ομάδα Ειδικού Ενδιαφέροντος κατά τον σχεδιασμό της τεχνολογίας Bluetooth . Ένας λόγος για αυτό είναι ίσως ότι η χρήση δημοσιών κλειδιών απαιτεί μεγαλύτερη υπολογιστική ισχύ από την χρήση συμμετρικών αλγορίθμων κρυπτογράφησης.

Η ασφάλεια που παρέχεται από το Bluetooth είναι χτισμένη πάνω από τη χρήση συμμετρικών μηχανισμών κρυπτογράφησης. Αρκετοί τύποι κλειδιών χρησιμοποιούνται στις συνδέσεις απ' αυτούς τους μηχανισμούς. Στο Bluetooth η σύνδεση είναι ένα κανάλι επικοινωνίας που εγκαθίσταται μεταξύ δύο συσκευών. Για να ελεγχθεί ότι η σύνδεση εγκαθίσταται μεταξύ των σωστών συσκευών, μία διαδικασία αυθεντικοποίησης πρέπει πρώτα να ξεκινήσει. Ο μηχανισμός της αυθεντικοποίησης χρησιμοποιεί το κλειδί σύνδεσης (*link key*). Όπως θα δούμε και παρακάτω, υπάρχουν αρκετών ειδών κλειδιά σύνδεσης ενώ κάποια απ' αυτά δε χρησιμοποιούνται μόνο για αυθεντικοποίηση. Χρησιμοποιείται επίσης για την παραγωγή του κλειδιού που ελέγχει την κρυπτογράφηση των δεδομένων που στέλνονται μέσω μίας σύνδεσης. Μέσω αυτής της κρυπτογράφησης η εμπιστευτικότητα των μεταδιδόμενων δεδομένων γίνεται πραγματικότητα. Έτσι, ο μηχανισμός κρυπτογράφησης χρησιμοποιεί το κλειδί κρυπτογράφησης της σύνδεσης (*link encryption key*).

Όπως είπαμε, το *κλειδί σύνδεσης* χρησιμοποιείται για την αυθεντικοποίηση μεταξύ δύο συσκευών και για να παραχθεί το κλειδί κρυπτογράφησης. Το κλειδί σύνδεσης είναι ένας τυχαίος αριθμός μήκους 128 bits. Ο χρόνος ζωής ενός κλειδιού σύνδεσης εξαρτάται από το αν είναι *ημιμόνιμο* ή *προσωρινό* κλειδί. Ημιμόνιμο ονομάζεται το κλειδί που μπορεί να χρησιμοποιηθεί και μετά το τέλος της εκάστοτε συνόδου με σκοπό την αυθεντικοποίηση των τμημάτων που το χρησιμοποίησαν. Ενώ, προσωρινό ονομάζεται το κλειδί που μετά το τέλος της συνόδου , δεν μπορεί να επαναχρησιμοποιηθεί. Τα προσωρινά κλειδιά χρησιμοποιούνται συνήθως σε συνδέσεις point–to–multipoint, δηλαδή όταν θέλουμε ένα αρχείο να έχει πολλαπλούς παραλήπτες.

Υπάρχουν τέσσερα είδη κλειδιών σύνδεσης [14] [15]: το κλειδί μονάδος (unit key), το κλειδί συνδυασμού (combination key), το κύριο κλειδί (master key) και το κλειδί αρχικοποίησης (initialization key). Εκτός από τα κλειδιά σύνδεσης υπάρχουν και τρία είδη κλειδιών για την κρυπτογράφηση: το κλειδί κρυπτογράφησης (encryption key), το περιορισμένο κλειδί κρυπτογράφησης (constrained encryption key) και το κλειδί ωφέλιμου φορτίου (payload key).

- *Κλειδί μονάδος (unit key):* Το κλειδί μονάδος K_{unit} είναι ημιμόνιμο κλειδί σύνδεσης που δημιουργείται από την ίδια την συσκευή όταν αυτή τίθεται σε λειτουργία για πρώτη φορά και σπάνια αλλάζει η τιμή του. Όμως το κλειδί αυτό που μια συσκευή έχει μπορεί να γνωστοποιηθεί σε πολλές άλλες. Μπορεί οπότε να χρησιμοποιηθεί με ασφάλεια μόνο όταν πρόκειται για συσκευές οι οποίες είναι πλήρως έμπιστες. Κι αυτό διότι οποιαδήποτε συσκευή να υποδύεται μία άλλη κρατώντας το κλειδί μονάδος. Μάλιστα, από την έκδοση 1.2 του Bluetooth δεν προτείνεται η χρήση του, αν και για λόγους συμβατότητας εξακολουθεί να υπάρχει. Σε κάποιες περιπτώσεις προτείνεται για συσκευές που έχουν πολύ περιορισμένη χωρητικότητα μνήμης ή που χρησιμοποιούνται από ένα μεγάλο αριθμό χρηστών να χρησιμοποιείται το κλειδί μονάδος ως κλειδί σύνδεσης.
- *Κλειδί Συνδυασμού (combination key):* Το κλειδί συνδυασμού K_{AB} είναι ημιμόνιμο και παράγεται από τη συσκευή σε συνεργασία με άλλη. Αφορά αποκλειστικά τις δύο αυτές συσκευές και δεν γνωστοποιείται αλλού.
- *Κλειδί αρχικοποίησης (initialization key):* Το κλειδί αρχικοποίησης K_{init} είναι προσωρινό και χρησιμοποιείται κατά την διαδικασία αρχικοποίησης μεταξύ δύο συσκευών που δεν είχαν στο παρελθόν κάποια επικοινωνία μεταξύ τους. Ο σκοπός του είναι να προστατεύσει την μεταφορά των δεδομένων

αρχικοποίησης και δεν θα πρέπει να χρησιμοποιείται αφού η διαδικασία αρχικοποίησης λήξει.

- *Κύριο κλειδί (master key):* Το κύριο κλειδί K_{master} είναι ένα προσωρινό κλειδί. Αντικαθιστά το κλειδί σύνδεσης όταν η συσκευή θέλει ταυτόχρονα να επικοινωνήσει με παραπάνω από μία συσκευές. Το κλειδί αυτό είναι ιδιαίτερα ευαίσθητο από την πλευρά της ασφάλειας του δικτύου ακριβώς επειδή είναι κοινό σε ένα μεγάλο αριθμό συσκευών. Θα πρέπει όλες οι συσκευές να είναι έμπιστες και να παραμένουν έμπιστες για όσο χρόνο χρησιμοποιείται το κλειδί αυτό ώστε να περιοριστούν οι κίνδυνοι που προκύπτουν από την χρήση του.
- *Κλειδί κρυπτογράφησης (encryption key):* Το κλειδί κρυπτογράφησης K_C αποτελεί το κύριο κλειδί το οποίο ελέγχει την κρυπτογράφηση. Επειδή το μήκος του μπορεί να υπερβαίνει το μέγιστο επιτρεπόμενο όριο, δε χρησιμοποιείται άμεσα αλλά αντικαθίσταται από το constrained encryption key.
- *Περιορισμένο κλειδί κρυπτογράφησης (constrained encryption key):* Το περιορισμένο κλειδί κρυπτογράφησης K'_C έχει μήκος μεταξύ 8 και 128 bits και εξάγεται από το K_C. Η επιθυμία για παγκόσμια διάδοση της τεχνολογίας Bluetooth, οδήγησε την Ομάδα Ειδικού Ενδιαφέροντος να ορίσει μεταβλητό μήκος για το κλειδί κρυπτογράφησης ώστε να συμβαδίσει με τους διαφορετικούς περιορισμούς που θέτει η κάθε χώρα. Επίσης με τον τρόπο αυτό θεωρήθηκε ότι θα είναι ευκολότερη η αναβάθμιση του επιπέδου ασφαλείας που προσφέρεται χωρίς να είναι απαραίτητος ο επανασχεδιασμός των αλγορίθμων και του εξοπλισμού που χρησιμοποιείται.
- *Κλειδί ωφέλιμου φορτίου (payload key):* Το κλειδί ωφέλιμου φορτίου K_P προέρχεται από το K'_C. Το κλειδί αυτό είναι η αρχική κατάσταση της μηχανής κρυπτογράφησης πριν γεννηθεί η ακολουθία του κρυπτογραφήματος.

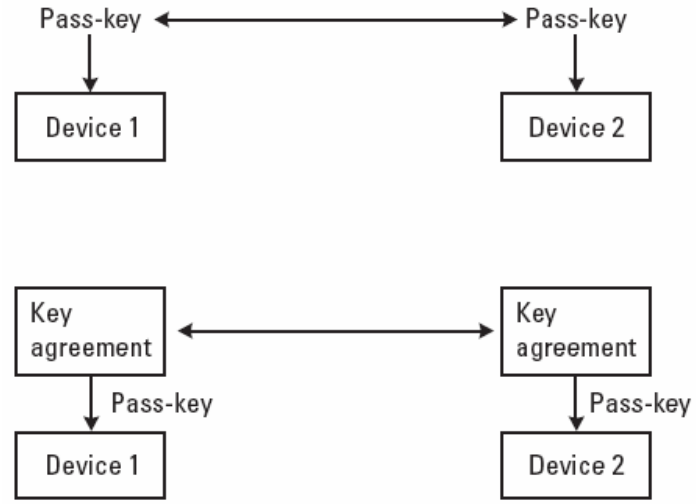
Purpose	Semipermanent		Temporary	
Authentication key generation	Unit key	Combination key	Initialization key	Master key
Ciphering			Encryption key Constrained encryption key	Payload key

Πίνακας 2-1 Κατηγορίες κλειδιών

2.2.2 Ζευγάρωμα και αλληλεπίδραση χρήστη

Όπως είπαμε προηγουμένως, το «ζευγάρωμα» δύο συσκευών είναι η διαδικασία με την οποία δύο συσκευές εγκαθιστούν μία σύνδεση με ένα κοινό «μυστικό» και το οποίο μπορούν να χρησιμοποιήσουν όταν συναντηθούν ξανά. Το «ζευγάρωμα» απαιτεί και την αλληλεπίδραση του χρήστη ˙ για παράδειγμα την εισαγωγή ενός pass-key. Στις προδιαγραφές του Bluetooth, αυτό μπορεί να είναι κάποιες φορές και ο

προσωπικός αριθμός αναγνώρισης (*personal identification number* – PIN). Το Bluetooth επιτρέπει το pass-key να έχει μήκος και 128 bits. Βέβαια, ένα τόσο μεγάλο κλειδί θα ήταν μη φιλικό προς το χρήστη όταν το εισάγει χειροκίνητα. Ωστόσο, η επιλογή αυτή επιτρέπει τη χρησιμοποίηση ενός υψηλότερου επιπέδου «συμφωνίας» κλειδιών που να μπορεί να τροφοδοτεί το συμφωνηθέν pass-key κατά τη διαδικασία του «ζευγαρώματος», όπως φαίνεται στο παρακάτω σχήμα. Η υψηλού επιπέδου «συμφωνία» κλειδιού μπορεί να είναι ένα πρωτόκολλο ασφάλειας στο επίπεδο του δικτύου ή της μεταφοράς.



Εικόνα 2-1 (α) Ζευγάρωμα μέσω διάδρασης των δυο χρηστών, (β) ζευγάρωμα με το πρωτόκολλο ξεχωριστών συμφωνιών κλειδιών

Σύμφωνα, λοιπόν, με την ορολογία στο Bluetooth υπάρχουν δύο τύποι pass-keys: το *μεταβλητό* και το *σταθερό* pass-key.Ο πρώτος τύπος αποτελεί ένα pass-key το οποίο αυθαίρετα μπορεί να επιλεχθεί. Αυτό απαιτεί την αλληλεπίδραση του χρήστη έτσι ώστε να δώσει στη συσκευή την τιμή του pass-key. Ένα παράδειγμα μιας Bluetooth συσκευής που χρησιμοποιεί μεταβλητό pass-key είναι τα κινητά τηλέφωνα. Αντίθετα, το σταθερό pass-key δεν μπορεί να επιλεχθεί αυθαίρετα όταν χρειαστεί. Αυτός ο τύπος χρησιμοποιείται όταν δεν μπορεί να υπάρξει αλληλεπίδραση με το χρήστη έτσι ώστε να εισαχθεί η τιμή του pass-key. Βέβαια, για να μπορέσει να γίνει το «ζευγάρωμα» μόνο μία συσκευή μπορεί να έχει σταθερό pass-key. Τέτοιες συσκευές Bluetooth είναι τα ποντίκια και τα ακουστικά.

2.3 Αυθεντικοποίηση και εμπιστευτικότητα

Μία συσκευή Bluetooth που βρίσκεται σε κατάσταση αναμονής δέχεται αιτήσεις από άλλες. Αυτό σημαίνει ότι υπάρχει κίνδυνος η συσκευή αυτή να συνδεθεί και να προσβληθεί από μία που μπορεί να της κάνει ζημιά. Αυτό θα μπορούσε να αντιμετωπιστεί με το να αποφεύγαμε να βάζαμε τη συσκευή σε κατάσταση αναμονής. Από την άλλη δε θα ήταν δυνατό να εγκατασταθούν και άλλες συνδέσεις που θέλουμε. Συμπεραίνουμε, λοιπόν, ότι υπάρχει ανάγκη για ασφαλή αναγνώριση της άλλης πλευράς. Η αναγνώριση της συσκευής παρέχεται μέσω του μηχανισμού αυθεντικοποίησης του Bluetooth. Κατά τη διαδικασία της αυθεντικοποίησης η συσκευή «επαληθευτής» *(verifier)* στέλνει μια τυχαία αίτηση στη συσκευή

«διεκδικητής» *(claimant)* και περιμένει να επιστραφεί μια έγκυρη τιμή απάντησης. Η διαδικασία αυτή είναι μονόδρομη και αν χρειάζεται αμοιβαία αυθεντικοποίηση επαναλαμβάνονται τα ίδια βήματα με τη μόνη διαφορά ότι αντιστρέφονται πλέον οι ρόλοι του επαληθευτή και του διεκδικητή. Αναλυτικά η διαδικασία της αυθεντικοποίησης περιγράφεται στο επόμενο κεφάλαιο.

Ένα άλλο μείζον θέμα ασφάλειας στο Bluetooth είναι η ιδιωτικότητα και η εμπιστευτικότητα. Η υποκλοπή των ραδιοκυμάτων μπορεί να γίνει σχετικά εύκολα. Αν και το Bluetooth βασίζεται στην αναπήδηση συχνοτήτων, αυτό δεν αποτελεί πραγματική προστασία απέναντι στην υποκλοπή δεδομένων. Κι αυτό διότι όπως έχουμε ήδη αναφέρει η συχνότητα των επισκεπτόμενων καναλιών καθορίζεται από το κατώτερο μέρος της διεύθυνσης της κύριας συσκευής και το τοπικό ρολόι, τα οποία είναι κοινώς γνωστά.

2.3.1 Προστασία της σύνδεσης

Είναι σημαντικό να τονίσουμε ότι το Bluetooth καθορίζει την ασφάλεια για τη σύνδεση μεταξύ δύο μονάδων και όχι για ολόκληρο το μονοπάτι από την πηγή στον προορισμό στο επίπεδο εφαρμογής. Όλα τα πρωτόκολλα και τα προφίλ που χρειάζονται end-to-end προστασία πρέπει να την παρέχουν από μόνα τους. Οι επιπτώσεις αυτού του γεγονότος είναι ολοφάνερες όταν η απομακρυσμένη εφαρμογή τρέχει σε μία μονάδα που βρίσκεται πολύ μακριά και η δρομολόγηση της κίνησης θα περιλαμβάνει αρκετές άγνωστες συνδέσεις εκτός από τη μικρή ραδιοζεύξη μεταξύ της τοπικής μονάδας και του σημείου πρόσβασης (access point). Από τη στιγμή, λοιπόν, που ο χρήστης δεν έχει τον έλεγχο ολόκληρου του μονοπατιού της σύνδεσης, η υψηλότερου επιπέδου ασφάλεια είναι αναγκαία προϋπόθεση για να διασφαλίσουμε την εμπιστευτικότητα.

2.3.2 Αλγόριθμοι κρυπτογράφησης

Υπάρχουν δυο τύποι αλγόριθμων κρυπτογράφησης: block και stream cipher. Τα block και stream ciphers είναι αναστρέψιμοι μετασχηματισμοί οι οποίοι χρησιμοποιούνται για την κρυπτογράφηση μιας πληροφορίας. Τα block ciphers χρησιμοποιούνται πάρα πολύ στους μηχανισμούς γέννησης κλειδιών. Αυτό συμβαίνει επειδή ο τρόπος λειτουργίας αυτών των μηχανισμών-αλγορίθμων (E_1, E_{21}, E_{22} και E_3), μοιάζει ιδιαίτερα με αυτόν ενός block cipher.

Για την επιλογή του τελικού αλγορίθμου που θα χρησιμοποιούνταν στο σύστημα ασφαλείας του Bluetooth, τέθηκαν ορισμένες απαιτήσεις. Έτσι, μια απαίτηση ήταν ο αλγόριθμος να είναι αρκετά δυνατός αλλά και κατανοητός. Επειδή, τα κλειδιά που χρησιμοποιούνται από το σύστημα του Bluetooth είναι μήκους 128 bits, απαιτείται ένας αλγόριθμος που θα μπορεί να μετατρέψει δεδομένα μήκους 128 bits με ένα κλειδί 128 bits. Ο πιο σημαντικός λόγος, όμως, ήταν το να μπορεί ο αλγόριθμος να χρησιμοποιηθεί ελεύθερα και να μην προστατεύεται από κάποια πατέντα. Με βάση τα προαναφερθέντα στοιχεία, οι σχεδιαστές του Bluetooth οδηγήθηκαν στην απόφαση να χρησιμοποιήσουν τον αλγόριθμο SAFER+. Μέχρι και σήμερα δεν έχει αναφερθεί κάποια αδυναμία που μπορεί να αποτελέσει πιθανό σημείο ευπάθειας για το Bluetooth.

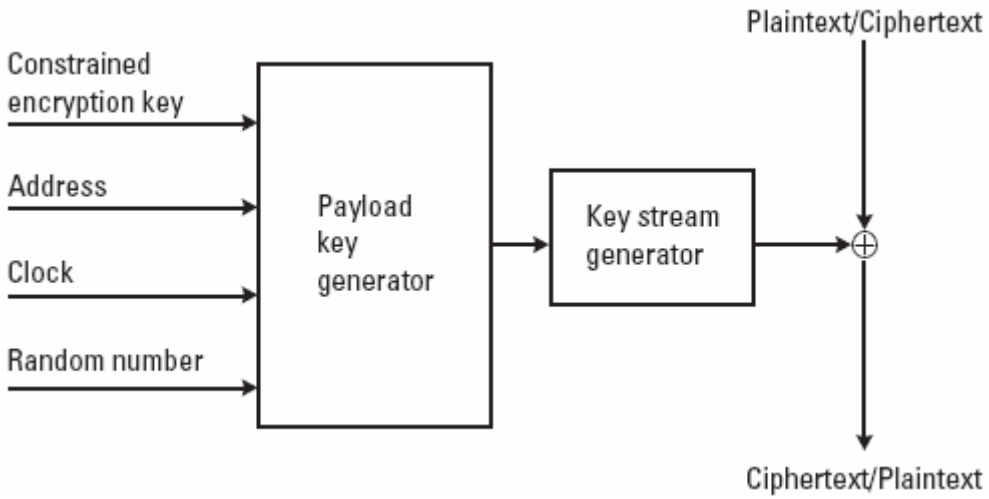
Τα stream ciphers ενδείκνυνται για χρήση σε επικοινωνιακά συστήματα καθώς μπορούν με μεγάλη ευκολία να χειριστούν δεδομένα με διάφορα μήκη. Ένα ακόμα

πλεονέκτημα είναι το γεγονός ότι έχουν σχεδιαστεί με πολύ μικρή πολυπλοκότητα. Γενικά, υπάρχουν δυο σχεδιαστικές προσεγγίσεις ενός stream cipher: άμεση και έμμεση με χρήση ενός block cipher.

Ο αλγόριθμος E_0 βασίζεται σε μια άμεση υλοποίηση και χρησιμοποιεί έναν αλγόριθμο, τον λεγόμενο συνδυαστή αθροισμάτων, ο οποίος έχει τις ρίζες του σε έναν αλγόριθμο υλοποιημένο από τους Massey και Rueppel στα μέσα της δεκαετίας του 1980. Η πιο αποτελεσματική και ισχυρή επίθεση που μπορεί να πραγματοποιηθεί σε αυτό τον αλγόριθμο είναι η επίθεση συσχετίσεων και εξαντλητικής αναζήτησης σε ένα δοθέν σύνολο κλειδιών.

Η εμπιστευτικότητα στο Bluetooth υλοποιείται με τη χρήση μεθόδων συμμετρικής κρυπτογράφησης. Η κρυπτογράφηση/αποκρυπτογράφηση είναι συνεχής (stream cipher) και υλοποιείται σε τρία μέρη:

1. Αρχικοποίηση του κλειδιού ωφέλιμου φορτίου (payload key - K_P)
2. Γέννηση μιας ακολουθίας ψηφίων (key stream)
3. Κρυπτογράφηση/αποκρυπτογράφηση των δεδομένων



Εικόνα 2-2 Χρησιμοποίηση stream cipher στο Bluetooth

Για να δημιουργηθεί το payload key K_P, ο payload key generator δέχεται ως είσοδο κάποιες παραμέτρους:

- Περιορισμένο κλειδί κρυπτογράφησης K'_C. Αυτό γεννιέται και από τις δύο συσκευές τη στιγμή που αποφασίζουν να αρχίσει η κρυπτογράφηση. Παραμένει σταθερό καθ' όλη τη διάρκεια της συνόδου εκτός κι αν αποφασίσουν να κάνουν χρήση ενός προσωρινού κλειδιού. Μπορεί να είναι από 8 ως και 129 bits.
- Διεύθυνση: Ως διεύθυνση καλούμε τη 48-bit διεύθυνση της κύριας συσκευής.
- Ρολόι: Είναι 28 bits και προέρχεται από το τοπικό ρολόι της κύριας συσκευής.
- Τυχαίος αριθμός: Αλλάζει κάθε φορά που και το κλειδί κρυπτογράφησης τροποποιείται. Ο αριθμός αυτός διανέμεται από την κύρια συσκευή πριν μπει σε κατάσταση κρυπτογράφησης.

Έτσι λοιπόν, η γεννήτρια του κλειδιού του ωφέλιμου φορτίου συνδυάζει τα δεδομένα εισόδου με κατάλληλο τρόπο και τα εισάγει στους τέσσερις καταχωρητές γραμμικής ολίσθησης με ανατροφοδότηση (Linear Shift Feedback Registers, LSFR) με σκοπό να παραχθεί το K_P. Στη συνέχεια, τα ψηφία του key stream δημιουργούνται

από μια μέθοδο που απορρέει από την αθροιστική γεννήτρια συνεχούς κρυπτογράφησης (summation stream cipher generator). Τέλος, το key stream χρησιμοποιείται για να γίνει η κρυπτογράφηση/αποκρυπτογράφηση των δεδομένων.

2.3.3 Unicast και broadcast

Η κρυπτογράφηση σε μια *εκπομπή (broadcast)* αποτελεί ένα πρόβλημα επειδή για κάθε σύνδεση μεταξύ της κύριας και της δευτερεύουσας συσκευής χρησιμοποιείται διαφορετικό κλειδί κρυπτογράφησης, Έτσι, αν η κύρια συσκευή ήθελε να στείλει ένα κρυπτογραφημένο μήνυμα σε όλες τις άλλες συσκευές θα μπορούσε να στείλει ξεχωριστά μηνύματα στη καθεμία *(unicast)*. Ένας καλύτερος εναλλακτικός τρόπος είναι να αλλάξει η κύρια συσκευή όλα τα κλειδιά σύνδεσης σε ένα προσωρινό κλειδί, το *κύριο κλειδί Kmaster (master key)*. Χρησιμοποιώντας αυτό, όλες οι συσκευές μπορούν να δημιουργήσουν ένα κοινό κλειδί κρυπτογράφησης το οποίο μπορεί να χρησιμοποιηθεί για μεταδόσεις εκπομπής.

Ένα μειονέκτημα αυτής της προσέγγισης είναι ότι η μίξη unicast και broadcast κίνησης δεν είναι δυνατή αφού ο χρήστης μόνο μια απ' αυτές μπορεί να διευθετήσει κάθε φορά. Ο δέκτης δεν μπορεί να προσδιορίσει αν θα χρησιμοποιήσει το κλειδί για την master-slave σύνδεση ή το κλειδί για την broadcast μέχρι να του γίνει γνωστή η LT_ADDR. Αν αυτή η διεύθυνση είναι όλο μηδενικά, τότε το μήνυμα είναι εκπομπης˙ διαφορετικά προορίζεται μια συγκεκριμένη μόνο συσκευή. Μιας και η LT_ADDR λαμβάνεται μαζί με το payload, υπάρχει ένα μικρό χρονικό διάστημα για το μηχανισμό αποκρυπτογράφησης ώστε να αρχικοποιηθεί σωστά. Για την αποφυγή αβεβαιότητας για το ποιο κλειδί να χρησιμοποιήσουμε, μόνο ένα κλειδί μπορεί να είναι έγκυρο κάθε χρονική στιγμή.

Υπάρχουν τρεις υποστηριζόμενοι τύποι για την κίνηση στο Bluetooth:

1. Χωρίς κρυπτογράφηση.
2. Κρυπτογράφηση μόνο σε point-to-point συνδέσεις χρησιμοποιώντας ημιμόνιμο κλειδί σύνδεσης.
3. Κρυπτογράφηση σε point-to-point και point-to-multipoint συνδέσεις χρησιμοποιώντας το ίδιο κλειδί και για τους δύο τύπους κίνησης.

Στα σενάρια εκπομπής, αφού όλοι οι κόμβοι χρησιμοποιούν το ίδιο κλειδί κρυπτογράφησης, πρέπει να υποστηρίζουν το μήκος κλειδιού που η κύρια συσκευή επιλέγει. Το μέγιστο μήκος κλειδιού που υποστηρίζεται καθορίζεται από τον κατασκευαστή της συσκευής και δεν μπορεί να αλλαχθεί. Για να επιλέξει η κύρια συσκευή το μήκος του κλειδιού, χρειάζεται να μάθει τα υποστηριζόμενα μήκη απ' όλες τις συσκευές. Η διαλειτουργικότητα επιτυγχάνεται με τη χρησιμοποίηση των δύο παρακάτω LMP εντολών (αυτές δεν υποστηρίζονται σε παλιές εκδόσεις):

- LMP encryption key size mask req
- LMP encryption key size mask res

Η πρώτη εντολή χρησιμοποιείται για να ζητήσει η κύρια συσκευή μία bit mask που περιγράφει το υποστηριζόμενο μήκος κλειδιού από τη δευτερεύουσα συσκευή. Στη συνέχεια, απαντάει χρησιμοποιώντας τη δεύτερη εντολή και επιστρέφοντας το μήκος κλειδιού.

Για να είναι δυνατή η κρυπτογράφηση της εκπομπής, η κύρια συσκευή πρέπει να αλλάξει το τρέχων κλειδί σύνδεσης. Για τη μεταγωγή από ημιμόνιμο σε προσωρινό κλειδί, κάποια βήματα πρέπει να εκτελεστούν. Αρχικά, γεννιέται το προσωρινό κλειδί σύνδεσης Kmaster. Όπως γίνεται αντιληπτό, αυτό δεν μπορεί να σταλεί χωρίς κρυπτογράφηση στις άλλες συσκευές. Η διαδικασία κατά την οποία γεννιέται και

γνωστοποιείται το κύριο κλειδί έχει περιγραφεί στο προηγούμενο κεφάλαιο. Στη συνέχεια, μέσω των δύο προηγούμενων LMP εντολών, η κύρια συσκευή ενημερώνεται για τα υποστηριζόμενα μήκη κλειδιών και καθορίζει το τελικό κλειδί.

Υπάρχει επίσης η εντολή LMP encryption mode req μέσω της οποίας καθορίζεται αν θέλουμε να υποστηρίξουμε κρυπτογράφηση ή όχι. Αν ο τύπος της κρυπτογράφησης θέτεται σε 0x1 ή 0x2, εφαρμόζεται κρυπτογράφηση σε point-to-point κίνηση. Στην περίπτωση αυτή αν χρησιμοποιηθεί προσωρινό κλειδί, τα μηνύματα εκπομπής κρυπτογραφούνται˙ ενώ αν χρησιμοποιείται ημιμόνιμο, αυτό δεν ισχύει. Από την έκδοση 1.2 του Bluetooth δεν προτείνεται η χρήση του 0x2. Συμερασματικά, για να εφαρμοστεί κρυπτογράφηση πρέπει η παράμετρος της εντολής HCI Write Encryption Mode να πάρει την τιμή 0x0 και 0x1. Τέλος, για να ενεργοποιηθεί το κύριο κλειδί σύνδεσης πρέπει να δοθεί η εντολή HCI Master Link Key.

2.4 Πολιτική ασφαλείας

Η εφαρμογή των μεθόδων ασφαλείας πολλές φορές οδηγούν στη χαμηλότερη απόδοση και στην αύξηση της πολυπλοκότητας των συστημάτων. Γι' αυτό το λόγο οι μηχανισμοί ασφαλείας πρέπει να χρησιμοποιούνται μόνο όταν πραγματικά χρειάζεται. Οι προδιαγραφές του Bluetooth παρέχουν ορισμένες βασικές αρχές για την ενίσχυση της ασφάλειας και την εφαρμογή πιο ανεπτυγμένων πολιτικών μέσω τριών καθορισμένων καταστάσεων ασφαλείας.

2.4.1 Καταστάσεις ασφαλείας

Οι προδιαγραφές του Bluetooth καθορίζουν διαφορετικές βασικές διαδικασίες ασφαλείας. Κάθε συσκευή μπορεί να λειτουργήσει σε τρεις διαφορετικές καταστάσεις [16] [17]:

- *Κατάσταση ασφαλείας 1 (Security mode 1):* Μία Bluetooth μονάδα σε αυτή την κατάσταση δεν ξεκινάει καμία διαδικασία ασφάλειας. Αυτό σημαίνει ότι ποτέ δεν απαιτεί αυθεντικοποίηση ή κρυπτογράφηση για τη σύνδεση. Βέβαια, αν αυτό της ζητηθεί από μία άλλη συσκευή, είναι υποχρεωμένη να το υποστηρίξει. Ποτέ, λοιπόν, δε στέλνει από μόνη της αιτήσεις για αυθεντικοποίηση ή ασφάλεια παρά μόνο μπορεί να απαντήσει σε τέτοιες.
- *Κατάσταση ασφαλείας 2 (Security mode 2):* Η κατάσταση αυτή παρέχει την καλύτερη απόδοση παρέχοντας και ασφάλεια. Η συσκευή δε θα πρέπει να ξεκινάει κάποια διαδικασία ασφαλείας ζητώντας αυθεντικοποίηση ή κρυπτογράφηση στην εγκατάσταση της σύνδεσης. Ζητάει, όμως, ασφάλεια στο κανάλι (L2CAP) ή όταν έχει γίνει η σύνδεση. Έτσι, όταν μία εφαρμογή ή υπηρεσία το ζητήσει θα ενεργοποιηθούν οι απαιτούμενοι μηχανισμοί. Για να μπορέσουμε να χειριστούμε τους μηχανισμούς αυτούς για την κάθε υπηρεσία ή εφαρμογή, υπάρχει ο διαχειριστής ασφαλείας *(security manager)*.
- *Κατάσταση ασφαλείας 3 (Security mode 3):* Μία συσκευή σε αυτή την κατάσταση πάντα ξεκινάει διαδικασίες ασφαλείας με το που αρχίζει η εγκατάσταση της σύνδεσης. Υπάρχουν δύο πιθανές πολιτικές: να ζητάει πάντα αυθεντικοποίηση ή να ζητάει και αυθεντικοποίηση και κρυπτογράφηση. Αν έστω και μια από τις δύο συσκευές που είναι σ' αυτή την κατάσταση ζητήσει κρυπτογράφηση, και οι δύο συσκευές θα την υποστηρίξουν ˙ αλλιώς η σύνδεση θα τερματιστεί.

2.4.2 Διαχείριση πολιτικής ασφαλείας

Εάν η κατάσταση ασφαλείας 2 πρέπει να συνδυαστεί με ένα υψηλό επίπεδο ασφαλείας, πρέπει να υλοποιηθεί μια εξειδικευμένη πολιτική ασφαλείας. Μία δυνατότητα είναι να χρησιμοποιήσουμε έναν διαχειριστή ασφαλείας που να χειρίζεται την πολιτική ασφαλείας και να ενδυναμώνει τους μηχανισμούς. Ο διαχειριστής ασφαλείας είναι η υπεύθυνη οντότητα για την ενδυνάμωση της ασφάλειας και αλληλεπιδρά με διάφορα επίπεδα στη στοίβα. Στην αρχιτεκτονική αυτή, ένα σύνολο εφαρμογών (ή υπηρεσιών) καταχωρεί τις απαιτήσεις ασφαλείας στον διαχειριστή ασφαλείας. Οι απαιτήσεις ασφαλείας όλων των υποστηριζόμενων εφαρμογών αποτελούν την πολιτική ασφαλείας και ο security manager χειρίζεται την πολιτική αυτή. Από τη στιγμή που η ασφάλεια στο Bluetooth σχετίζεται με τις διευθύνσεις των

συσκευών και τα κλειδιά, ο διαχειριστής ασφαλείας πρέπει να έχει πρόσβαση σε μία βάση δεδομένων που να περιέχει πληροφορίες για τις διάφορες συσκευές και τα κλειδιά σύνδεσης και σε μία άλλη βάση που να περιέχει τις ειδικές απαιτήσεις ασφαλείας για κάθε ξεχωριστή υπηρεσία.

ΚΕΦΑΛΑΙΟ 3
ΖΕΥΓΑΡΩΜΑ ΣΥΣΚΕΥΩΝ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΚΛΕΙΔΙΩΝ

Όταν αναφερόμαστε στον όρο «ζευγάρωμα» στο πρωτόκολλο Bluetooth, εννοούμε την διαδικασία που ακολουθείται για να συνδεθούν δυο συσκευές μεταξύ τους. Η διαδικασία του «ζευγαρώματος» είναι πολύ σημαντική για την διασφάλιση της σύνδεσης των δυο συσκευών. Για να εγκαταστήσουμε μια σύνδεση Bluetooth, ξεκινάμε από την εγκατάσταση μιας Asynchronous Connectionless σύνδεσης. Μόλις ολοκληρωθεί αυτή η διαδικασία, οι συσκευές μπορούν να ανταλλάξουν μηνύματα μέσω του ασύρματου καναλιού επικοινωνίας.

Για να μπορέσουν οι συσκευές να χρησιμοποιήσουν μηχανισμούς αυθεντικοποίησης και κρυπτογράφησης θα πρέπει αρχικά να μοιραστούν ένα κοινό μυστικό. Αυτός ο διαμοιρασμός πραγματοποιείται κατά το «ζευγάρωμα» των δυο συσκευών.

Οι συσκευές Bluetooth πρέπει να έχουν την δυνατότητα να αποθηκεύουν έναν αριθμό ζευγαριών του τύπου (κλειδί σύνδεσης, διεύθυνση συσκευής) σε μια βάση δεδομένων τα οποία πρόκειται να τα χρησιμοποιήσουν σε μελλοντικά «ζευγαρώματα». Σε περίπτωση που δυο συσκευές Bluetooth θέλουν να επικοινωνήσουν, γίνεται έλεγχος αν στο παρελθόν έχουν ξαναεπικοινωνήσει και σε αυτή την περίπτωση ανακαλούνται οι σχετικές πληροφορίες από την βάση.

Στη συνέχεια, θα αναλυθεί η διαδικασία του «ζευγαρώματος» και της δημιουργία των κλειδιών ανάλογα με το επίπεδο του πρωτοκόλλου. Έτσι, θα αναλυθούν τα επίπεδα HCI, LMP και baseband.

3.1 Πρωτόκολλο HCI

Για να πραγματοποιηθεί η διαδικασία του pairing, απαιτείται η ανταλλαγή ενός pass key. Ο Host Controller (HC) γεννάει το γεγονός *HCI PIN Code Request*. Αποτέλεσμα αυτού μπορεί να είναι είτε το pass key, συνοδευόμενο από διάφορες άλλες πληροφορίες, είτε μια αρνητική απάντηση του host που καταδεικνύει την αδυναμία δημιουργίας του κλειδιού. Στην τελευταία περίπτωση, βέβαια, η προσπάθεια για «ζευγάρωμα» αποτυγχάνει. Αν όλα πάνε καλά, αποστέλλεται το pass key από το HCI στο Baseband για περαιτέρω επεξεργασία. Στη συνέχεια, ο Διαχειριστής Σύνδεσης (Link Manager - LM) αποστέλλει έναν 128 bit τυχαίο αριθμό (IN_RAND) στην απομακρυσμένη συσκευή στην οποία ενεργοποιείται ένα αντίστοιχο *HCI PIN Code Request* γεγονός.

Παρακάτω, αναλαμβάνει ο Διαχειριστής Σύνδεσης να διεκπεραιώσει τις απαιτούμενες ενέργειες για να ολοκληρωθεί η διαδικασία του «ζευγαρώματος». Το Link Manager Protocol (LMP) διασφαλίζει ότι το κοινό μυστικό, δηλαδή το κλειδί σύνδεσης, δημιουργείται και στις δυο πλευρές. Όταν οι Διαχειριστές Σύνδεσης έχουν τερματίσει τις διαπραγματεύσεις για το κλειδί σύνδεσης και οι δυο hosts ενημερώνονται μέσω του γεγονότος *HCI Link Key Notification* .

3.2 Πρωτόκολλο Διαχείρισης Σύνδεσης

Ο Διαχειριστής Σύνδεσης βοηθάει στην διαδικασία με το να μεταδίδει τις παραμέτρους και τα διάφορα αποτελέσματα μεταξύ των δυο συσκευών. Όλοι οι

υπολογισμοί πραγματοποιούνται στο επίπεδο του baseband. Η συμμετοχή του LMP στο «ζευγάρωμα» ξεκινάει με την μετάδοση του PDU *LMP in rand* στην απομακρυσμένη συσκευή. Έτσι, ενεργοποιείται η διαδικασία γέννησης του κλειδιού αρχικοποίησης (initialization key) το οποίο απαιτείται για την δημιουργία του κλειδιού σύνδεσης.

Στην περίπτωση που πρόκειται να χρησιμοποιηθεί κλειδί συσκευής (unit key), εκτελείται η εντολή *LMP unit key* η οποία αποστέλλεται προς μια και μόνο κατεύθυνση. Αυτή η εντολή περιέχει το μυστικό κλειδί συσκευής το οποίο έχει γίνει για λόγους ασφαλείας XOR με το κλειδί αρχικοποίησης. Έτσι, καθώς ο παραλήπτης γνωρίζει αυτό το κλειδί είναι εύκολο στη συνέχεια να υπολογίσει το κλειδί συσκευής.

Αντίστοιχα για την περίπτωση του κλειδιού συνδυασμού (combination key), εκτελείται η εντολή *LMP comb key*. Όπως είναι γνωστό για την δημιουργία αυτού του κλειδιού απαιτούνται παράμετροι και από τις δυο πλευρές του «ζευγαρώματος» και για αυτό το λόγο είναι πιο πολύπλοκος ο υπολογισμός του επιθυμητού κλειδιού.

Μόλις καθοριστεί ο τύπος του κλειδιού και γίνουν οι απαραίτητες ενέργειες για την δημιουργία του, ακολουθεί μια αμοιβαία αυθεντικοποίηση των συσκευών. Για αυτό τον σκοπό αποστέλλεται μια πρόκληση των 128-bit μέσω της εντολής *LMP au rand* ενώ η απάντηση χρησιμοποιεί το *LMP sres*.

3.3 Baseband

Σε αυτό το επίπεδο, οι εντολές διαχείρισης κλειδιών του LMP μετατρέπονται σε σειρές από baseband events. Τα πιο σημαντικά γεγονότα είναι αυτά που υποστηρίζουν:

- Το «ζευγάρωμα» των συσκευών
- Την εγκατάσταση ενός κλειδιού σύνδεσης
- Την εγκατάσταση του ciphering offset και των κλειδιών κρυπτογράφησης (ciphering keys)

3.3.1 Γέννηση του κλειδιού αρχικοποίησης

Είναι προσωρινά κλειδιά με μικρή διάρκεια ζωής που χρησιμοποιούνται κατά το «ζευγάρωμα» δυο συσκευών. Το K_{INIT} είναι το κλειδί σύνδεσης κατά την φάση αρχικοποίησης καθώς τότε δεν υπάρχουν κλειδιά συνδυασμού και συσκευής (combination και unit keys) [18] [19].

Υπολογίζεται με την χρήση του αλγόριθμου E22 και με τις παραμέτρους: BD_ADDR, το pass-key PKEY, το μήκος αυτού L_{PKEY} (σε οκτάδες) και ένας 128-bit τυχαίος αριθμός.

$$PKEY' = \begin{cases} PKEY \cup BD\_ADDR, L_{PKEY} \le 10 \\ PKEY \cup BD\_ADDR[0...(15-L)], 10 < L_{PKEY} \le 15 \\ PKEY, L_{PKEY} = 16 \end{cases}$$

$$L'_{PKEY} = \min(L_{PKEY} + 6, 16)$$

Έτσι, το K_{INIT} είναι : K_{INIT} = E22 (PKEY',IN_RAND,L'$_{PKEY}$) .

3.3.2 Γέννηση του κλειδιού συσκευής

Έστω ότι η συσκευή A εκκινεί την διαδικασία του «ζευγαρώματος» και η B είναι ο πελάτης. Το κλειδί συσκευής K_A υπολογίζεται με την χρήση του αλγόριθμου E_{21} με παραμέτρους: ένα τοπικά γεννημένο τυχαίο αριθμό (128-bit) LK_RAND_A και το BD_ADDR της συσκευής.

$$K_A = E21(LK\_RAND_A, BD\_ADDR_A)$$

Μόλις, δημιουργηθεί το K_A «περνάει» μέσα από μια XOR μαζί με το K_{INIT} και έχουμε το K'_A το οποίο και αποστέλλεται τελικά στην άλλη συσκευή.

$$K'_A = K_A \oplus K_{INIT}$$

Στη συνέχεια, είναι πολύ εύκολο για τη συσκευή B να εξάγει το K_A καθώς η ίδια γνωρίζει το ποιο είναι το K_{INIT}.

$$K'_A \oplus K_{INIT} = K_A \oplus K_{INIT} \oplus K_{INIT} = K_A$$

3.3.3 Γέννηση του κλειδιού συνδυασμού

Το κλειδί συνδυασμού δημιουργείται με την συνεισφορά και των δυο εμπλεκόμενων συσκευών. Ουσιαστικά, πρόκειται για το αποτέλεσμα της πράξης XOR μεταξύ των μυστικών κλειδιών K_A και K_B.

$$K_A = E21(LK\_RAND_A, BD\_ADDR_A)$$
$$K_B = E21(LK\_RAND_B, BD\_ADDR_B)$$

,όπου LK_RAND_X ένας τυχαίος 128-bit αριθμός δημιουργημένος τοπικά στην συσκευή x.

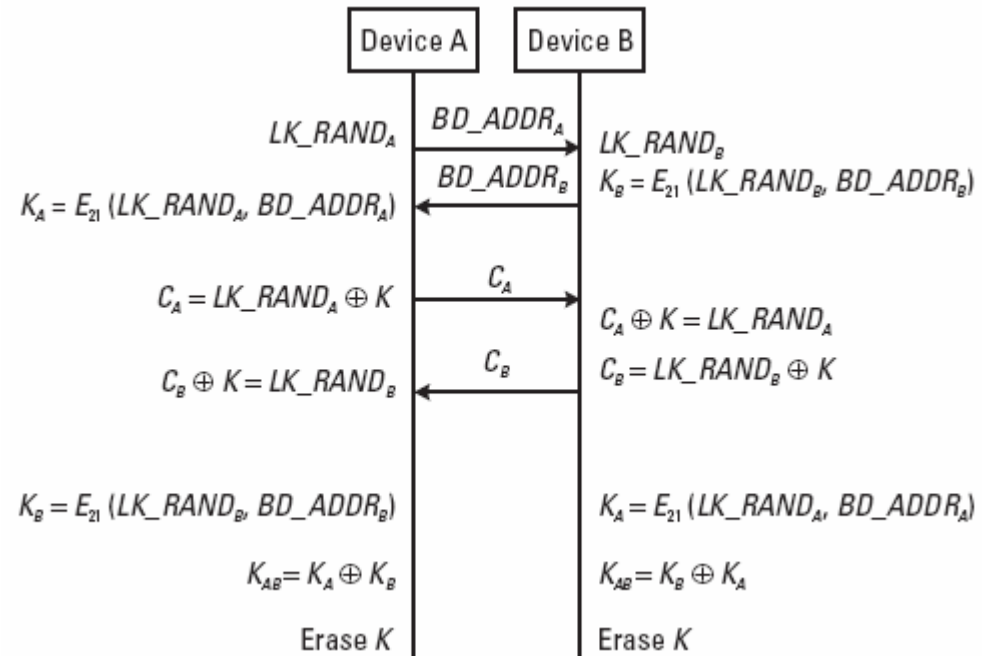
Μέχρι τώρα, κάθε συσκευή έχει δημιουργήσει το K_X της. Για να μπορέσει, όμως να γεννήσει το K_{AB} θα πρέπει να γνωρίζει και το παραχθέν κλειδί της άλλης. Από τις παραμέτρους δημιουργίας των κλειδιών, δεν είναι γνωστό το LK_RAND της μιας συσκευής στην άλλη, ενώ οι συσκευές γνωρίζουν η καθεμία το BD_ADDR της άλλης. Αποστέλλεται, λοιπόν, το LK_RAND της μιας συσκευής στην άλλη κωδικοποιημένο με το τρέχων κλειδί σύνδεσης K.

$C_A = LK\_RAND_A \oplus K$, αποστέλλεται από τη συσκευή A στην B

$C_B = LK\_RAND_B \oplus K$, αποστέλλεται από τη συσκευή B στην A

Το K όμως είναι γνωστό και στις δυο συσκευές. Έτσι, μπορούν εύκολα να απομονώσουν το LK_RAND.

$$C_B \oplus K = (LK\_RAND_B \oplus K) \oplus K = LK\_RAND_B$$
$$C_A \oplus K = (LK\_RAND_A \oplus K) \oplus K = LK\_RAND_A$$



Εικόνα 3-1 Δημιουργία του κλειδιού συνδυασμού

Έτσι, μόλις απομονωθεί το LK_RAND μπορεί η μια συσκευή να υπολογίσει το K της άλλης και κατά συνέπεια να παράξουν το κλειδί συνδυασμού K_{AB}. Στη συνεχεία, ακολουθεί η αυθεντικοποίηση της μιας συσκευής στην άλλη. Αυτό πρακτικά σημαίνει ότι κάθε συσκευή πρέπει να αποδείξει στην άλλη ότι κατέχει το σωστό κλειδί σύνδεσης.

3.3.4 Αυθεντικοποίηση

Κατά την φάση της αυθεντικοποίησης, υπάρχουν δυο ρόλοι για την εκάστοτε συσκευή. Έτσι, λοιπόν, μια συσκευή μπορεί να έχει τον ρόλο του διεκδικητή (claimant) ή του επαληθευτή (verifier).

Έστω, ότι η συσκευή Α είναι ο επαληθευτής και η Β ο διεκδικητής. Η Α προκαλεί την Β στέλνοντας την τυχαία 128-bit τιμή AU_RAND και περιμένει απάντηση από την Β του τύπου:

$$SRES = E1(K, AU\_RAND, BD\_ADDR_B)$$

, όπου K το κλειδί σύνδεσης και E_1 η συνάρτηση αυθεντικοποίησης.

Η συσκευή Α μόλις λάβει την απάντηση SRES της Β, την συγκρίνει με την αναμενόμενη SRES και αποφαίνεται ανάλογα. Αν οι τιμές συμπίπτουν η διαδικασία ολοκληρώνεται επιτυχώς αλλιώς επιστρέφει ένα σφάλμα.

Στην περίπτωση που ζητηθεί από τον Διαχειριστή Σύνδεσης να γίνει αμοιβαία αυθεντικοποίηση τότε οι ρόλοι αλλάζουν και πραγματοποιείται η ίδια διαδικασία. Πρέπει να τονιστεί ότι η master συσκευή δεν παίρνει πάντα τον ρόλο του επαληθευτή. Εξαρτάται από την εφαρμογή να ορίσει τους ρόλους και τον τύπο της αυθεντικοποίησης (μονόδρομη , αμφίδρομη).

Κατά την διαδικασία αυτή, παράγεται επίσης και το Authenticated Ciphering Offset (ACO), το οποίο είναι απαραίτητο για τον υπολογισμό του κλειδιού

κρυπτογράφησης. Στην περίπτωση της αμοιβαίας αυθεντικοποίησης, χρησιμοποιείται το ACO που παράχθηκε τελευταίο.

3.3.5 Γέννηση του κύριου κλειδιού

Το κύριο κλειδί είναι ένα προσωρινό κλειδί το οποίο χρησιμοποιείται για να προστατεύει τα δεδομένα που στέλνονται σε broadcast μηνύματα, δηλαδή από την κύρια συσκευή σε όλους τους «σκλάβους». Το κλειδί αυτό αντικαθιστά το κλειδί σύνδεσης όσο διαρκεί η εκπομπή της αναμετάδοσης.

$$K_{master} = E22(LK\_RAND1, LK\_RAND2,16)$$

,όπου LK_RAND_X τυχαίος αριθμός 128-bit τοπικά γεννημένος.

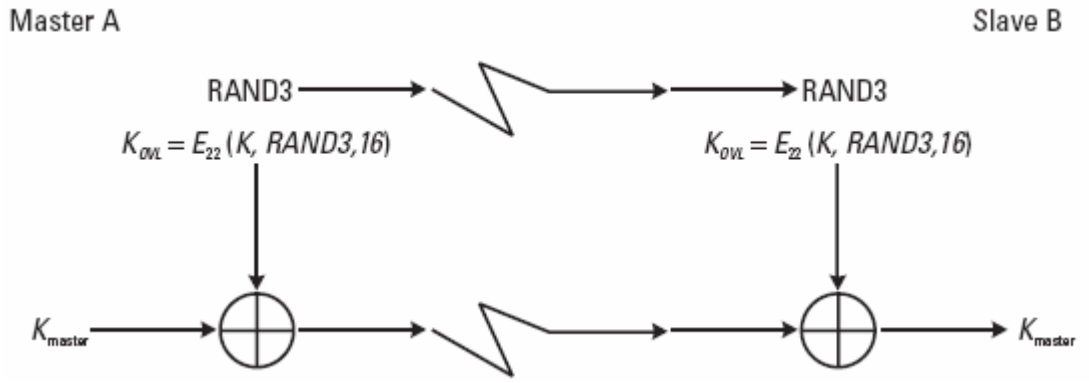
Το K_{master} αποστέλλεται στους σκλάβους κρυπτογραφημένο με το K_{ovl}.

$$K_{ovl} = E22(K, RAND3,16)$$

Ο RAND3 είναι τυχαίος 128-bit αριθμός ο οποίος είναι γνωστός σε όλες τις συσκευές. Έτσι, είναι πολύ εύκολο για μια συσκευή σκλάβο να ανακαλύψει το K_{master}.

$$K_{AB} \oplus K_{ovl} = (K_{master} \oplus K_{ovl}) \oplus K_{ovl} = K_{master}$$

Αυτή η διαδικασία πραγματοποιείται με όλους τους σκλάβους. Οι τιμές των ACOs δεν πρέπει να αντικαθιστούν τις υπάρχουσες.



Εικόνα 3-2 Μεταφορά του κύριου κλειδιού στον slave κόμβο

3.4 Αλληλεπίδραση με τον χρήστη

Η δημιουργία του κλειδιού σύνδεσης πολλές φορές απαιτεί την συμμετοχή του χρήστη με το να εισάγει αυτός δηλαδή το pass-key. Το ζήτημα που ανακύπτει είναι ότι υπάρχει η πιθανότητα μια από τις συσκευές να μην έχει μονάδα εισόδου (πχ headset, ασύρματο ποντίκι). Σε αυτή την περίπτωση, η συσκευή μπορεί να έχει αποθηκευμένο ένα fixed pass-key ή να δημιουργεί εκείνη τη στιγμή ένα τυχαίο το οποίο θα εμφανίζεται στην οθόνη της συσκευής.

Κατά την εισαγωγή του pass-key από τον χρήστη, κάθε χαρακτήρας μετατρέπεται σύμφωνα με την κωδικοποίηση UTF-8 και όλα τα δεκαδικά ψηφία βρίσκονται μεταξύ των ορίων του Unicode 0x00 – 0x7F. Είναι υποχρεωτικό για όλες τις συσκευές που δέχονται ως είσοδο το pass-key , να υποστηρίζουν την χρήση δεκαδικών ψηφιών (η υποστήριξη άλλων χαρακτήρων είναι προαιρετική).

Εισαγόμενη συμβολοσειρά	Pass-key (Δεκαεξαδική μορφή)
'0123'	0x30313233
'Arlig'	0xC384726C67

Πίνακας 3-1 Αντιστοιχία συμβολοσειράς με το pass-key

Ένα ακόμα πρόβλημα παρατηρείται στην χρήση για ζευγάρωμα ενός υπολογιστή με ένα Bluetooth – enabled πληκτρολόγιο. Τα πληκτρολόγια χρησιμοποιούν διαφορετικά σύνολα χαρακτήρων για τα διάφορα αλφάβητα. Επίσης, σε πολλές χώρες διαφέρει η διάταξη των χαρακτήρων στο πληκτρολόγιο, πχ Αμερική – QWERTY, Γαλλία – AZERTY. Για αυτό η λύση που προτείνεται είναι η χρήση μόνο αριθμητικών χαρακτήρων οι οποίοι καταλαμβάνουν την ίδια θέση στα σύνολα χαρακτήρων ανά τις χώρες.

3.5 Γέννηση του κλειδιού κρυπτογράφησης

Στο Bluetooth, το κλειδί σύνδεσης δεν χρησιμοποιείται για την κρυπτογράφηση των πακέτων που μεταδίδονται. Αντιθέτως, μια πιο πολύπλοκη διαδικασία ακολουθείται για την δημιουργία του κλειδιού κρυπτογράφησης. Έχει, όμως, άμεση σχέση με το κλειδί σύνδεσης και το ACO το οποίο προέρχεται από την τελευταία αυθεντικοποίηση των συσκευών.

3.5.1 Κλειδί κρυπτογράφησης K_C

Το πρώτο βήμα της κρυπτογράφησης είναι ο υπολογισμός του K_C από το οποίο στη συνέχεια υπολογίζονται όλα τα υπόλοιπα κλειδιά της διαδικασίας. Έτσι, λοιπόν, το K_C έχει ως παραμέτρους το τρέχων link key K, ένα 96-bit ciphering offset (COF) και ένα 128-bit τυχαίο αριθμό (EN_RAND).

$$COF = \begin{cases} BD\_ADDR & ,masterkey \\ ACO & ,\alpha\lambda\lambda\iota\acute{\omega}\varsigma \end{cases}$$

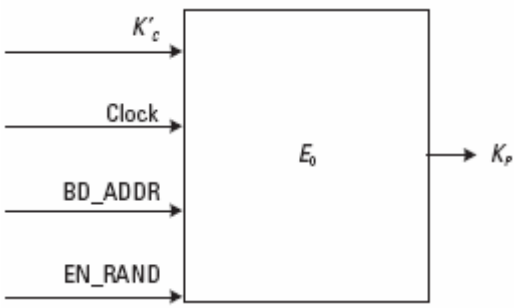
$$K_C = E3(K, EN\_RAND, COF)$$

3.5.2 Κλειδί Περιορισμού K'_C

Όπως έχει ήδη αναφερθεί στο εισαγωγικό κεφάλαιο, δίνεται η δυνατότητα από το Bluetooth να μην χρησιμοποιηθεί το κλειδί κρυπτογράφησης (encryption key) το οποίο έχει μέγεθος 128 bits αλλά ένα άλλο κλειδί του οποίου το μήκος μπορεί να προσαρμοστεί σε μικρότερα μεγέθη. Αυτός ο περιοριστικός μηχανισμός υιοθετήθηκε από το Bluetooth λόγω κάποιων περιορισμών εξαγωγής των κλειδιών που τέθηκαν στην κρυπτογράφηση που υλοποιείται από το υλικό μέρος .

3.5.3 Κλειδί Ωφέλιμου Φορτίου K_P

Το κλειδί ωφέλιμου φορτίου (payload key) χρησιμοποιείται για να πραγματοποιηθεί η (από) κρυπτογράφηση των εισερχόμενων/ εξερχόμενων πακέτων. Η τιμή του κλειδιού υπολογίζεται ξεχωριστά για κάθε πακέτο και πιο συγκεκριμένα εκτελείται ο αλγόριθμος E_0 με εισόδους το K'_C, 26 bits της τρέχουσας τιμής του ρολογιού, τη διεύθυνση της συσκευής καθώς και ένα τυχαίο αριθμό των 128 bits.



Εικόνα 3-3 Διαδικασία δημιουργίας του κλειδιού ωφέλιμου φορτίου

3.6 Βάσεις Δεδομένων Κλειδιών

Όλα τα ημιμόνιμα κλειδιά, combination & unit keys, μπορούν να χρησιμοποιηθούν για επαναλαμβανόμενες συνόδους μεταξύ δυο συσκευών. Για αυτό κρίνεται απαραίτητη η αποθήκευσή τους σε μια βάση δεδομένων.

3.6.1 Απαιτήσεις γέννησης των κλειδιών συσκευής

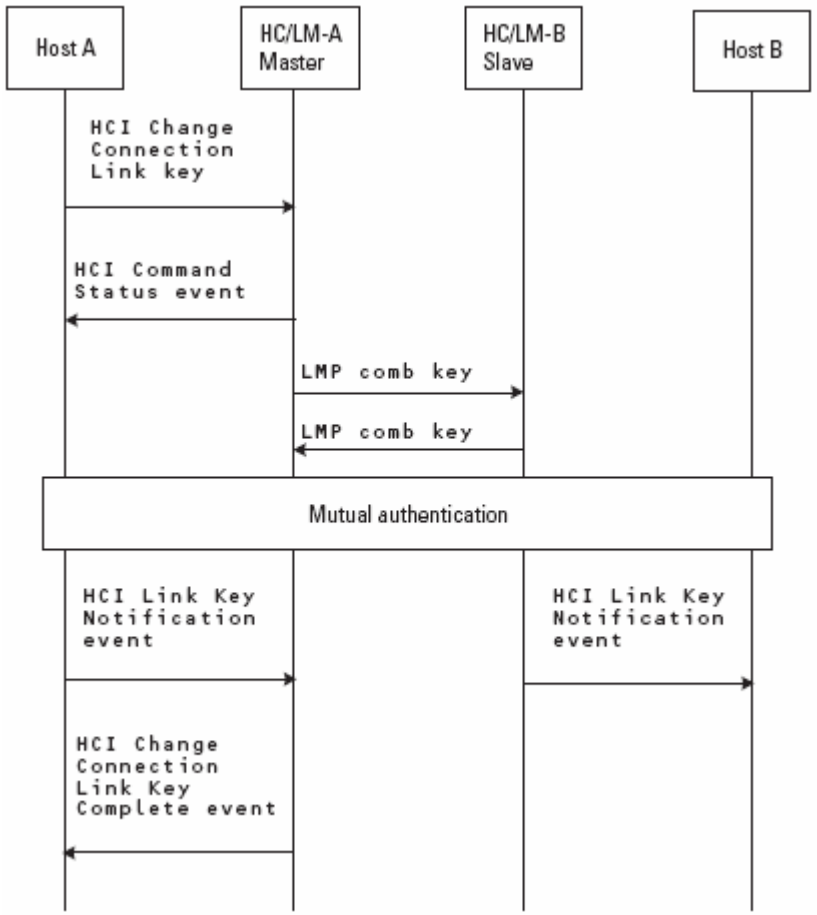
Μια σημαντική παράμετρος που πρέπει να προσεχθεί κατά την γέννηση του κλειδιού συσκευής είναι η σωστή λειτουργία του μηχανισμού που είναι υπεύθυνος για την δημιουργία του τυχαίου αριθμού που χρησιμοποιείται. Επιπλέον, κάθε τιμή που χρησιμοποιείται για ένα κλειδί συσκευής θα πρέπει αμέσως μετά να απορρίπτεται έτσι ώστε να αποφευχθεί πιθανή επαναχρησιμοποίησή της. Το κλειδί συσκευής μετά την δημιουργία του αποθηκεύεται σε μια μη πτητική μνήμη και δεν πρέπει να τροποποιηθεί έκτοτε.

3.6.2 Απαιτήσεις γέννησης των κλειδιών συνδυασμού

Ομοίως και το κλειδί συνδυασμού πρέπει να αποθηκεύεται σε μια μη πτητική μνήμη και μπορεί να παραμείνει σταθερή η τιμή του. Όμως, είναι μια καλή πολιτική ασφαλείας να τροποποιείται η τιμή του κατά συχνά χρονικά διαστήματα.

Η διαδικασία που ακολουθείται για να τροποποιηθεί η τιμή του κλειδιού συνδυασμού είναι παρόμοια με αυτή της αρχικής δημιουργίας του. Υπάρχει μια συγκεκριμένη εντολή HCI που μπορεί να χρησιμοποιήσει μια συσκευή για να πραγματοποιήσει την αλλαγή : *HCI Change Connection Link Key*. Πιο συγκεκριμένα, όταν ο Διαχειριστής Σύνδεσης της συσκευής Α λάβει ένα τέτοιο αίτημα από το HCI τότε αποστέλλει ένα μήνυμα *LMP comb key* στην συσκευή Β. Οπότε η συσκευή Β αν αποδεχτεί την αλλαγή θα απαντήσει με ένα *LMP comb key* ή αν αρνηθεί με ένα *LMP*

not accepted. Μετά την επιτυχή τροποποίηση του κλειδιού, πρέπει απαραιτήτως να πραγματοποιηθεί μια εκ νέου αμοιβαία αυθεντικοποίηση.



Εικόνα 3-4 Διάγραμμα ανανέωσης του κλειδιού συνδυασμού

Μετά και από την αυθεντικοποίηση, οι host controller και των δυο συσκευών θα ενεργοποιήσουν το γεγονός *HCI Link Key Notification*. Ενώ, ο host controller του A θα ενεργοποιήσει το γεγονός *HCI Change Connection Link Key Complete* το οποίο ουσιαστικά αποδεικνύει αν η τροποποίηση ολοκληρώθηκε με επιτυχία ή όχι.

Είναι πολύ σημαντικό η πολιτική ασφαλείας του κλειδιού συνδυασμού να είναι μέρος και της πολιτικής ασφαλείας της ίδιας της συσκευής. Έτσι, αν το κλειδί χρησιμοποιείται πολύ συχνά , θα πρέπει και να τροποποιείται πολύ συχνά.

3.6.3 Βάσεις δεδομένων των κλειδιών

Όπως αναφέρθηκε και προηγουμένως, για την καλύτερη χρήση και λειτουργία των κλειδιών, προτείνεται ως βέλτιστη λύση η χρήση βάσης δεδομένων. Αυτό συμβαίνει επειδή αν εισάγουμε όλα τα κλειδιά σε μια βάση δεδομένων θα μπορούμε πολύ πιο εύκολα να τα διαχειριστούμε και να τα επεξεργαστούμε.

Πιο συγκεκριμένα, μια μορφή της ΒΔ για τα κλειδιά είναι ένας απλός πίνακας ο οποίος θα αποτελείται από δυο στήλες: την διεύθυνση της συσκευής (48 bits) και το αντίστοιχο κλειδί (128 bits).

Device Address	Key
10FA48C7DE52	1B4D5698AE374FDE8390912463DFE3AB
047F6BB427EA	FE729425BC9A95D39132BDE275917823
A5EE29667190	091827AD41D4E48D29CBE82615D18490
⋮	⋮
068935F6B3E2	126304467592CD71FF19B4428133AD8E

Πίνακας 3-2 Βάση δεδομένων κλειδιών σύνδεσης

Το ζήτημα που δημιουργείται είναι ότι τα κλειδιά δεν είναι πάντα ενός τύπου. Έτσι, μπορεί να έχουμε κλειδιά τύπου συσκευής ή συνδυασμού. Για αυτό τον λόγο, οι πίνακες που χρησιμοποιούνται αποτελούνται από ένα ακόμα πεδίο το οποίο προσδιορίζει τον τύπο του κλειδιού που χρησιμοποιείται .

Device Address	Key	Key Type
10FA48C7DE52	1B4D5698AE374FDE8390912463DFE3AB	C
047F6BB427EA	FE729425BC9A95D39132BDE275917823	C
A5EE29667190	091827AD41D4E48D29CBE82615D18490	C
⋮	⋮	⋮
068935F6B3E2	126304467592CD71FF19B4428133AD8E	U

Πίνακας 3-3 Βάση δεδομένων κλειδιών σύνδεσης με πεδίο για τον τύπο κλειδιού

Επίσης, ένας πίνακας θα ήταν ακόμα πιο πλήρης αν περιελάμβανε ένα πεδίο ελέγχου πλεονασμού το οποίο θα μας ενημέρωνε για τυχόν σφάλματα στο συγκεκριμένο κλειδί.

Κατεστραμμένες ΒΔ

Είναι πολύ πιθανό η βάση δεδομένων που αποθηκεύει τα κλειδιά σύνδεσης για κάποιο λόγο να καταστραφεί μερικώς ή ολικώς. Αυτό μπορεί να οφείλεται είτε στο μέσο στο οποίο αποθηκεύεται είτε στον μηχανισμό ο οποίος είναι υπεύθυνος για την προστασία αποθήκευσης. Σε περίπτωση λάθους, η συσκευή συνήθως ζητάει να πραγματοποιηθεί εξαρχής η διαδικασία του «ζευγαρώματος». Αυτή η αίτηση στέλνεται με την εντολή *LMP in rand*. Στην περίπτωση, όμως, που η συσκευή έχει ήδη λάβει μια αίτηση αυθεντικοποίησης από την άλλη συσκευή και εκ των υστέρων αντιληφθεί ότι η εγγραφή είναι κατεστραμμένη τότε απαντάει με ένα *LMP not accepted* με το δικαιολογητικό "key missing". Η συνέχεια εξαρτάται από την συσκευή καθώς μπορεί είτε να ζητήσει επανάληψη της διαδικασίας «ζευγαρώματος» είτε να απορρίψει την αίτηση και να αποσυνδεθεί.

Αποθήκευση

Δυο είναι τα σημαντικά θέματα που αφορούν την αποθήκευση των κλειδιών: ο έλεγχος πρόσβασης και η ασφαλής αποθήκευση. Λέγοντας έλεγχο πρόσβασης αναφερόμαστε στο γεγονός ότι δεν πρέπει να επιτρέπεται σε μη εξουσιοδοτημένους χρήστες η πρόσβαση (ανάγνωση ή /και επεξεργασία) στη βάση δεδομένων που περιέχει τα κλειδιά. Ομοίως, δεν θα πρέπει να έχει την δυνατότητα ένας χρήστης να διαβάσει τα δεδομένα απευθείας από το μέσω στο οποίο έχουν αποθηκευτεί. Βέβαια,

όλα αυτά εξαρτώνται από την πολιτική ασφαλείας που εφαρμόζουμε στην συσκευή μας. Ο πιο συνηθισμένος τρόπος ελέγχου πρόσβασης είναι αυτός της αυθεντικοποίησης του χρήστη με κάποιο συνθηματικό ή PIN.

Υπάρχουν τρεις διαφορετικές προσεγγίσεις στη αποθήκευση της βάσης δεδομένων. Μια από αυτές είναι η **Integrated Circuit Card** (ICC). Για να αποκτήσει ένας χρήστης πρόσβαση σε αυτό θα πρέπει να εισάγει ένα PIN . Αυτή η προσέγγιση προσφέρει ασφαλή αποθήκευση των δεδομένων και μηχανισμό αυθεντικοποίησης των χρηστών και προτιμάται όταν μπορεί να χρησιμοποιηθεί.

Η επόμενη λύση είναι να αποθηκευτούν τα δεδομένα σε ένα μέσο γενικής αποθήκευσης, όπως είναι ο σκληρός δίσκος και η flash memory, το οποίο βρίσκεται στον υπολογιστή. Υπάρχει η δυνατότητα να κρυπτογραφείτε η βάση δεδομένων αλλά θα πρέπει να παρέχεται στο σύστημα ένα κλειδί κρυπτογράφησης. Οπότε, χρησιμοποιείται μια συνάρτηση η οποία θα ζητάει από τον χρήστη ένα συνθηματικό και σε συνδυασμό με διάφορες άλλες παραμέτρους, παράγει το κλειδί κρυπτογράφησης. Σε αυτή την περίπτωση , χρησιμοποιείται ευρέως το RSA PKCS#5.

Τέλος, η τρίτη προσέγγιση είναι να μην υπάρχει κάποια ιδιαίτερη ασφάλεια στη βάση δεδομένων και να στηρίζεται το σύστημα μόνο στο σύστημα σύνδεσης (login) του χρήστη.

ΚΕΦΑΛΑΙΟ 4
ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ

4.1 Στόχοι

Μία σύνδεση Bluetooth μοιράζεται από πολλές διαφορετικές εφαρμογές ή υπηρεσίες που τρέχουν σε μια συσκευή. Κάθε μία απ' αυτές έχει ιδιαίτερες απαιτήσεις για εξουσιοδότηση, αυθεντικοποίηση και εμπιστευτικότητα. Γι' αυτό είναι απαραίτητη η ύπαρξη ενός μηχανισμού ασφαλείας. Ο σκοπός αυτού του μηχανισμού είναι να παρέχει τη δυνατότητα στις εφαρμογές να ζητούν τον τύπο της σύνδεσης που αυτές κάθε φορά επιθυμούν. Έτσι, μιλάμε για *service level-enforced* ασφάλεια.

4.1.1 Έμπιστες σχέσεις

Με τον όρο *έμπιστη* συσκευή αναφερόμαστε σε μια συσκευή στην οποία έχει εγκατασταθεί μία σχέση ασφαλείας και αυτή διαρκεί για περισσότερο χρονικό διάστημα από την τρέχουσα σύνοδο. Σε μία έμπιστη συσκευή δίνεται απεριόριστη πρόσβαση σε όλες τις υπηρεσίες αφού βέβαια πρώτα επιβεβαιωθεί η ταυτότητά της μέσω του πρωτοκόλλου αυθεντικοποίησης.

Σε άλλες περιπτώσεις, η σύνδεση είναι προσωρινή. Χρειάζεται να κρυπτογραφηθεί η σύνδεση αλλά δεν είναι απαραίτητη η μόνιμη σύνδεση μεταξύ των συμβαλλόμενων μερών. Έτσι, οι παράμετροι της σύνδεσης αυτής δεν χρειάζεται να αποθηκευτούν για μελλοντική χρήση. Εδώ μιλάμε για *μη έμπιστες* συσκευές.

4.1.2 Επίπεδα ασφαλείας

Μία υπηρεσία μπορεί ελεύθερα να θέτει τις απαιτήσεις της σε εξουσιοδότηση, αυθεντικοποίηση και κρυπτογράφηση. Έτσι η κάθε υπηρεσία εμπίπτει σε τρία επίπεδα ασφαλείας:

1. Εξουσιοδότηση και αυθεντικοποίηση
2. Αυθεντικοποίηση μόνο
3. Υπηρεσίες ανοιχτές σε όλες τις συσκευές

Στην περίπτωση που είναι επιθυμητή η εξουσιοδότηση, ο χρήστης πρέπει ενεργά να εγκρίνει την πρόσβαση σε μία υπηρεσία ακόμα κι αν ο συνδεδεμένος πελάτης τρέχει πάνω σε μία έμπιστη συσκευή. Από την άλλη, οι ανοιχτές υπηρεσίες δε χρειάζονται ούτε εξουσιοδότηση, ούτε αυθεντικοποίηση. Έτσι προφανώς το επίπεδο της σύνδεσης δεν μπορεί να κρυπτογραφηθεί αφού το πρωτόκολλο απαιτεί προηγουμένως αυθεντικοποίηση.

4.1.3 Ευελιξία

Για να είναι χρήσιμη, η αρχιτεκτονική ασφαλείας πρέπει να παρέχει ξεχωριστές ρυθμίσεις για τις πολιτικές πρόσβασης των διαφόρων υπηρεσιών. Για παράδειγμα ένα κινητό τηλέφωνο μπορεί να έχει μία «ανοιχτή» πολιτική στην πρόσβαση των

εγγραφών του ευρετηρίου αλλά περιοριστική πολιτική στην πρόσβαση για τα ακουστικά ή την dial-up δικτύωση. Για να αυξήσουμε την ευχρηστία, η μεσολάβηση του χρήστη για να έχει πρόσβαση σε μία υπηρεσία πρέπει να κρατιέται στο ελάχιστο. Βασικά, αυτή χρειάζεται όταν δημιουργούμε μια έμπιστη σχέση με μία συσκευή ή στην περίπτωση μιας περιορισμένης πρόσβαση για κάποια υπηρεσία.

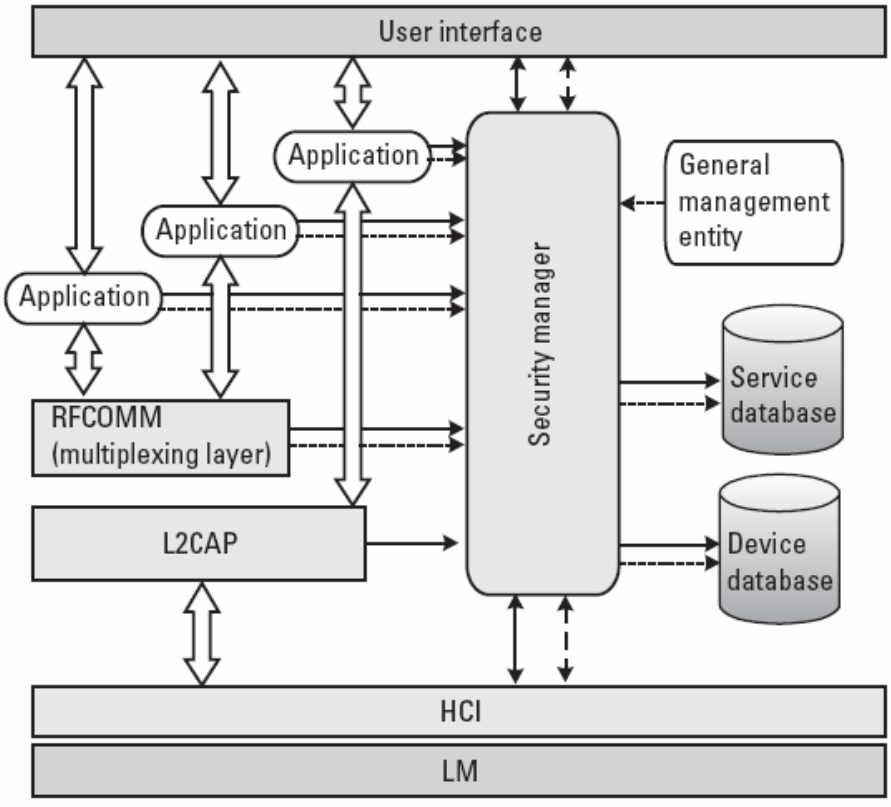
Στο Bluetooth κάποια πρωτόκολλα έχουν τις δικές τους επιλογές ασφαλείας. Η αρχιτεκτονική ασφαλείας πρέπει να το υπολογίζει αυτό έτσι ώστε τα διάφορα υψηλού επιπέδου πρωτόκολλα να επιβάλλουν πολιτικές ασφαλείας για διαφορετικές υπηρεσίες. Για παράδειγμα, το L2CAP ενισχύει την ασφάλεια στην κινητή τηλεφωνία, το RFCOMM στην dial-up δικτύωση και τέλος το OBEX ενδυναμώνει την πολιτική ασφαλείας για τη μεταφορά αρχείων. Τα χαμηλότερα στρώματα δε χρειάζεται να γνωρίζουν τις ρυθμίσεις και τις πολιτικές ασφαλείας των υψηλότερων επιπέδων. Επιπλέον, οι πολιτικές ασφαλείας μπορεί να διαφέρουν από το πελάτη και τον διακομιστή. Αυτό πρέπει να χειρίζεται από τον διαχειριστή ασφαλείας.

4.2 Αρχιτεκτονική διαχειριστή ασφαλείας

4.2.1 Περίληψη

Οι κύριες εργασίες που ένας διαχειριστής ασφαλείας πρέπει να πραγματοποιεί είναι:

- Αποθήκευση πληροφοριών σχετικές με την ασφάλεια των υπηρεσιών
- Αποθήκευση πληροφοριών σχετικές με την ασφάλεια των συσκευών
- Αποδοχή ή απόρριψη των αιτήσεων για πρόσβαση από πρωτόκολλα ή εφαρμογές
- Αυθεντικοποίηση / κρυπτογράφηση πριν τη σύνδεση με μία εφαρμογή
- Αρχικοποίηση της εγκατάστασης των έμπιστων σχέσεων σε επίπεδο συσκευών
- Ερώτηση στον χρήστη ή την εφαρμογή για pass-key όταν αυτό χρειάζεται



Εικόνα 4-1 Η αρχιτεκτονική του διαχειριστή ασφαλείας

Ο διαχειριστής ασφαλείας ελαφρύνει τις συσκευές από το φορτίο να υλοποιούν όλες αυτές τις εργασίες. Το πρωτόκολλο που αλληλεπιδρά με τον διαχειριστή ασφαλείας αποτελείται από απλές διαδικασίες ερωτήσεων / απαντήσεων και καταχωρήσεων. Αφού η πολιτική ασφαλείας ενθυλακώνεται μέσα στον διαχειριστή ασφαλείας, μπορούν να γίνουν τροποποιήσεις σ' αυτή χωρίς την ανάγκη ενημέρωσης των οντοτήτων που αλληλεπιδρούν μ' αυτή. Επίσης, οι πολιτικές ασφαλείας εφαρμόζονται τόσο στην εισερχόμενη όσο και στην εξερχόμενη κίνηση.

4.2.2 Επίπεδα εμπιστοσύνης συσκευών

Σύμφωνα με το διαχειριστή ασφαλείας, κάθε απομακρυσμένη συσκευή που συνδέεται αυτόν εμπίπτει σε από τα καθορισμένα επίπεδα εμπιστοσύνης των συσκευών:

1. *Έμπιστη συσκευή:* Μία συσκευή που έχει αυθεντικοποιηθεί προηγουμένως, το κλειδί σύνδεσης της οποίας έχει αποθηκευτεί και έχει επονομαστεί ως έμπιστη στη βάση δεδομένων της συσκευής.
2. *Μη έμπιστη συσκευή:* Μία συσκευή που έχει αυθεντικοποιηθεί προηγουμένως, το κλειδί σύνδεσης της οποίας έχει αποθηκευτεί αλλά έχει επονομαστεί ως μη έμπιστη στη βάση δεδομένων της συσκευής.
3. *Άγνωστη συσκευή:* Δεν είναι διαθέσιμη κάποια πληροφορία γι' αυτή τη συσκευή. Εξ' ορισμού θεωρείται ως μη έμπιστη.

Ο διαχειριστής ασφαλείας διατηρεί βάση δεδομένων απ' όλες τις γνωστές συσκευές και δρα σύμφωνα με την πολιτική για το αντίστοιχο επίπεδο εμπιστοσύνης

της απομακρυσμένης συσκευής. Μία έμπιστη σχέση συνήθως εγκαθίσταται κατά τη διαδικασία του ζευγαρώματος. Ο χρήστης μπορεί να ειδοποιηθεί και να του δοθεί η επιλογή να προσθέσει την απομακρυσμένη συσκευή στη λίστα των έμπιστων συσκευών. Είναι επίσης δυνατό να προσθέσει αργότερα μη έμπιστες συσκευές στη λίστα αυτή. Όποτε η απομακρυσμένη συσκευή έχει κλειδί σύνδεσης, η αυθεντικοποίηση πραγματοποιείται σύμφωνα με τη διαδικασία που περιγράφεται στις προδιαγραφές του LMP και του baseband. Για να πιστοποιηθεί ως έμπιστη, πρέπει η αυθεντικοποίηση να επιτύχει και η σημαία εμπιστοσύνης να τοποθετηθεί στην εσωτερική βάση δεδομένων. Για τις άγνωστες συσκευές, τέλος, το ζευγάρωμα είναι απαραίτητο προτού γίνει η αυθεντικοποίηση.

4.2.3 Επίπεδο ασφαλείας για υπηρεσίες

Ανάλογα με την περίπτωση της βάσης δεδομένων των συσκευών, ο διαχειριστής ασφαλείας τηρεί και μια βάση δεδομένων των υπηρεσιών για ρυθμίσεις σχετικές με υπηρεσίες παρά με συσκευές. Το επίπεδο ασφαλείας μιας υπηρεσίες καθορίζεται από τρία χαρακτηριστικά:

1. *Απαίτηση εξουσιοδότησης:* Οι έμπιστες συσκευές αυτόματα έχουν πρόσβαση, ενώ οι μη έμπιστες χρειάζονται την έγκριση του χρήστη προκειμένου να αποκτήσουν το δικαίωμα αυτό.
2. *Απαίτηση αυθεντικοποίησης:* Η απομακρυσμένη συσκευή πρέπει να αυθεντικοποιηθεί προτού δοθεί πρόσβαση στην εφαρμογή.
3. *Απαίτηση κρυπτογράφησης:* Η σύνδεση πρέπει κρυπτογραφηθεί προτού δοθεί πρόσβαση στην εφαρμογή ή υπηρεσία.

Αυτά τα τρία χαρακτηριστικά μπορούν να τεθούν ανεξάρτητα για τις εισερχόμενες και τις εξερχόμενες συνδέσεις. Εξ ορισμού, κάθε υπηρεσία πρέπει να χειρίζεται από κάποια εφαρμογή. Έτσι, κάθε εφαρμογή είναι υπεύθυνη να καταγράφει με τον διαχειριστή ασφάλειας και να καθορίζει το επίπεδο ασφαλείας της.

Αν δεν υπάρχει εγγραφή στη βάση των υπηρεσιών για μια συγκεκριμένη αίτηση εισερχόμενης ή εξερχόμενης σύνδεσης, εφαρμόζονται οι παρακάτω προκαθορισμένες ρυθμίσεις:

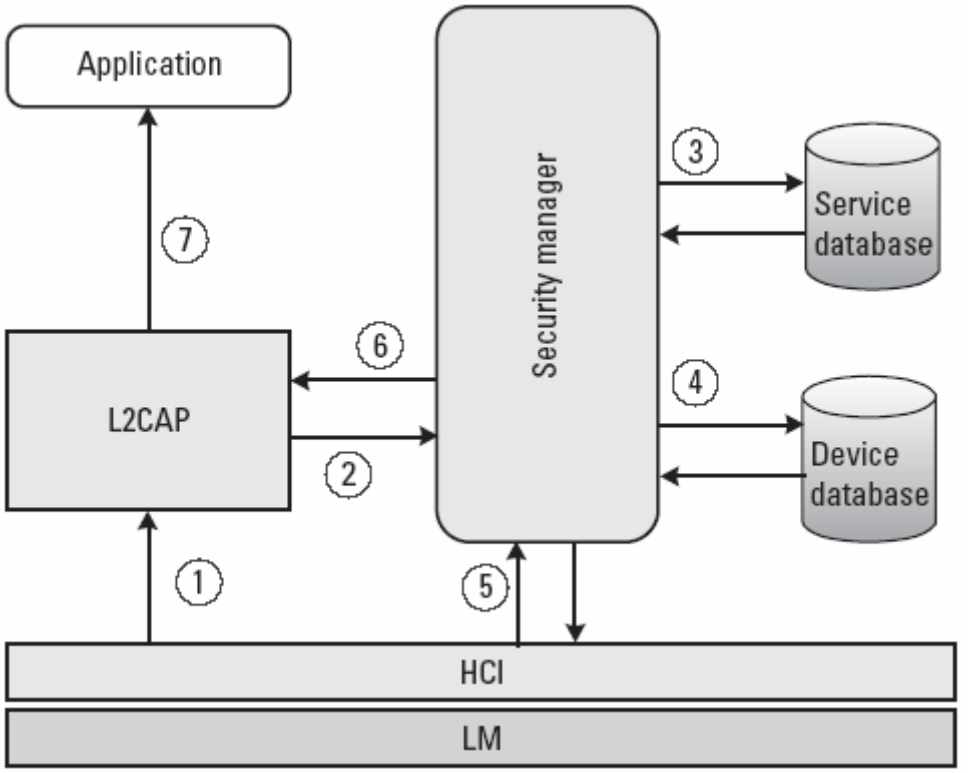
- *Εισερχόμενη σύνδεση:* Απαίτηση εξουσιοδότησης (ενδεχομένως και αυθεντικοποίησης).
- *Εξερχόμενη σύνδεση:* Απαίτηση αυθεντικοποίησης.

4.2.4 Εγκατάσταση σύνδεσης

Η σειρά για την εγκατάσταση ενός καναλιού L2CAP είναι η ακόλουθη:

1. Η σύνδεση κάνει αίτηση στο L2CAP
2. Το L2CAP ζητά πρόσβαση από τον διαχειριστή ασφαλείας
3. Ο διαχειριστής ασφαλείας ελέγχει την πολιτική ασφαλείας για την αιτούμενη υπηρεσία στη βάση δεδομένων των υπηρεσιών
4. Ο διαχειριστής ασφαλείας ελέγχει την πολιτική ασφαλείας για τη συνδεόμενη συσκευή στη βάση δεδομένων των συσκευών
5. Αν είναι απαραίτητο, ο διαχειριστής ασφαλείας επιβάλλει αυθεντικοποίηση και κρυπτογράφηση

6. Ο διαχειριστής ασφαλείας παραχωρεί πρόσβαση στην υπηρεσία
7. Το L2CAP συνεχίζει την εγκατάσταση της σύνδεσης



Εικόνα 4-2 Διαδικασία ελέγχου πρόσβασης για την εγκατάσταση του καναλιού L2CAP

4.2.5 Περιεχόμενα βάσεων δεδομένων και διαδικασία εγγραφής

Υπάρχουν δύο βάσεις δεδομένων που βρίσκονται υπό την εποπτεία του διαχειριστή ασφαλείας: η βάση δεδομένων των συσκευών και η βάση δεδομένων των υπηρεσιών. Κάθε εγγραφή της βάσης των συσκευών περιέχει πληροφορίες που επικεντρώνονται στην ταυτότητα, το επίπεδο ασφαλείας και το κλειδί σύνδεσης. Επίσης, μπορούν να αποθηκευτούν κι άλλες χρήσιμες πληροφορίες, όπως το όνομα της συσκευής (το οποίο δίνεται χειροκίνητα από τον χρήστη). Για να είναι χρήσιμη αυτή και σε πολλές συνόδους, η βάση πρέπει να αποθηκεύεται σε μη ασταθή μνήμη.

Η βάση δεδομένων των υπηρεσιών περιέχει πληροφορίες που επικεντρώνονται στις απαιτήσεις εξουσιοδότησης, αυθεντικοποίησης και κρυπτογράφησης για εισερχόμενες και εξερχόμενες αιτήσεις. Επιπλέον αποθηκεύεται και μια τιμή PSM (protocol/service multiplexor). Η τιμή αυτή χρησιμοποιείται από το επίπεδο L2CAP κατά τη διάρκεια της εγκατάστασης του καναλιού για να δρομολογήσει την αίτηση σύνδεσης στο σωστό ανώτερο επίπεδο. Όποτε το L2CAP υποβάλει μία αίτηση, ο διαχειριστής ασφαλείας θα χρησιμοποιήσει την τιμή PSM για να αναγνωρίσει σε ποιο πρωτόκολλο υψηλότερου επιπέδου ανήκει η αίτηση σύνδεσης. Με την πληροφορία αυτή διαθέσιμη, είναι δυνατό να εφαρμοστούν οι σωστές ρυθμίσεις της πολιτικής ασφαλείας για την αντίστοιχη αίτηση σύνδεσης.

Ο διαχειριστής ασφαλείας είναι υπεύθυνος στο να διατηρεί τη βάση δεδομένων των συσκευών. Αυτή πρέπει να ανανεώνεται κάθε φορά που γίνεται σύνδεση με τη

συσκευή. Για καινούριες συσκευές μια νέα εγγραφή δημιουργείται. Αν τα υπάρχον κλειδί σύνδεσης ή το επίπεδο εμπιστοσύνης μιας συσκευής αλλάξει, ανανεώνεται αντίστοιχα και η βάση.

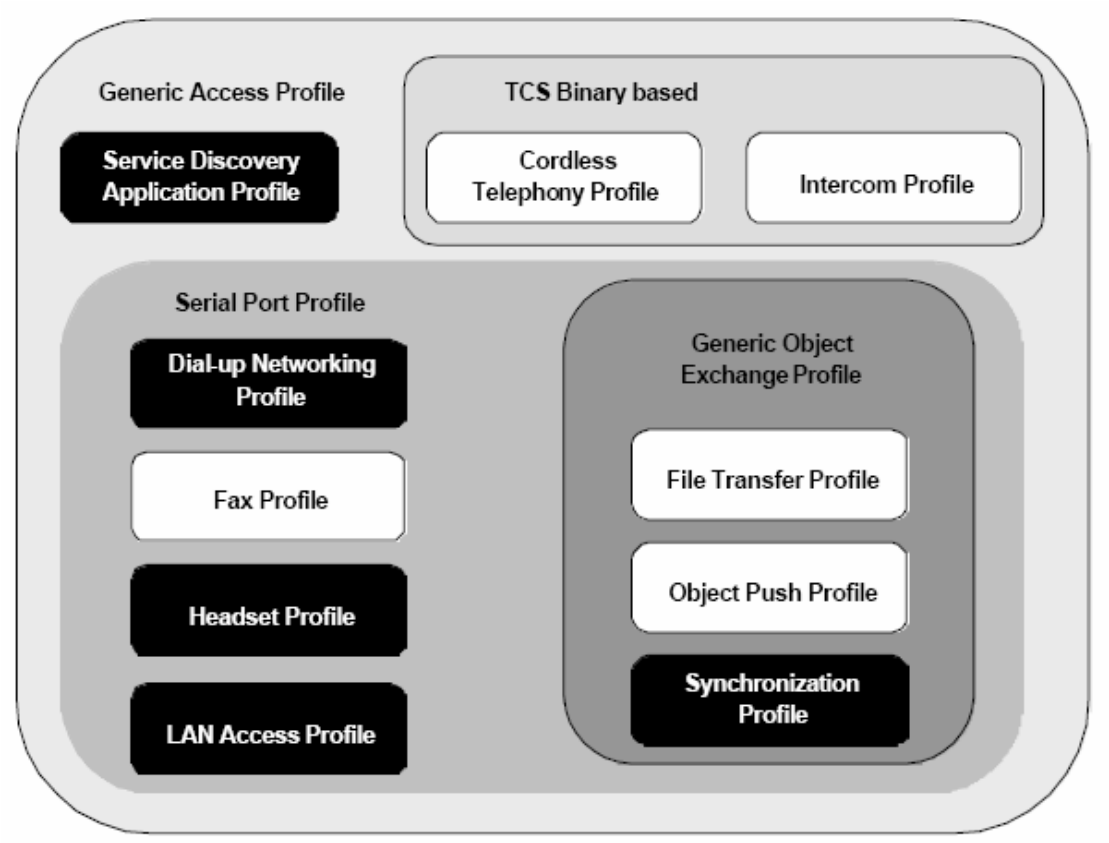
Οι πληροφορίες ασφαλείας που αναφέρονται σε υπηρεσίες ή εφαρμογές χρειάζεται να εγγράφονται στην βάση δεδομένων των υπηρεσιών από το διαχειριστή ασφαλείας προτού μία υπηρεσία προσπελασθεί. Η εγγραφή περιλαμβάνει επίπεδα ασφαλείας για εισερχόμενες και εξερχόμενες αιτήσεις, αναγνώριση πρωτοκόλλων και το PSM που χρησιμοποιείται από το L2CAP.

ΚΕΦΑΛΑΙΟ 5
PROFILES

Στα προηγούμενα κεφάλαια περιγράψαμε αναλυτικά τους μηχανισμούς ασφαλείας. Το πώς όμως χρησιμοποιείται η ασφάλεια στο Bluetooth εξαρτάται σε κάθε περίπτωση από την εφαρμογή. Εδώ θα περιγράψουμε πώς χρησιμοποιούμε διαφορετικούς μηχανισμούς ασφαλείας για τα εξής προφίλ [20]:

1. Headset profile
2. Network access profile

Τα παραπάνω δεν καλύπτουν όλα τα προφίλ όπως φαίνεται και από το παρακάτω σχήμα. Ωστόσο, είναι αντιπροσωπευτικά των προβλημάτων ασφαλείας που παρουσιάζονται.



Εικόνα 5-1 Bluetooth profiles

5.1 Headset profile

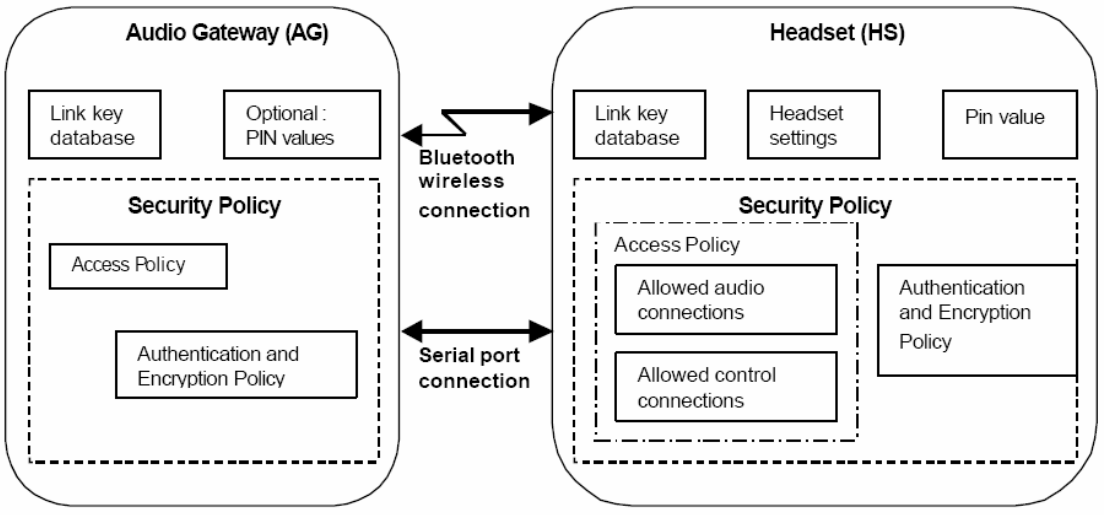
Οι προδιαγραφές του Bluetooth περιέχουν το προφίλ ακουστικών. Το προφίλ αυτό χρησιμοποιείται για συνδέσεις μεταξύ ακουστικών και κινητών τηλεφώνων ή φορητών υπολογιστών. Ένα σημαντικό κομμάτι του ασφαλούς ζευγαρώματος είναι η χρησιμοποίηση passkey όταν δημιουργούνται οι σχέσεις ασφαλείας. Οι σχέσεις

ασφαλείας χρησιμοποιούνται για να αυθεντικοποιήσουμε και να κρυπτογραφήσουμε την επικοινωνία μεταξύ δύο Bluetooth συσκευών.

5.1.1 Μοντέλο ασφαλείας ακουστικών

Όπως φαίνεται και από το παραπάνω σχήμα το προφίλ ακουστικών εξαρτάται από το προφίλ σειριακής θύρας (serial port profile) και από το προφίλ γενικής πρόσβασης (general access profile – GAP). Το GAP καθορίζει το ζευγάρωμα και τη συμπεριφορά ασφαλείας στα περισσότερα προφίλ. Μια τυπική σύνθεση ακουστικών αποτελείται από δύο συσκευές, ένα ακουστικό (headset –HS) και μία πύλη ήχου (audio gateway – AG). Η πύλη ήχου μπορεί να είναι ένα κινητό τηλέφωνο, ένας υπολογιστής ή οποιαδήποτε συσκευή αναπαραγωγής ήχου. Για να προστατεύσουμε το ασύρματο κανάλι, πρέπει η σύνδεση μεταξύ του AG και του HS να αυθεντικοποιηθεί και να κρυπτογραφηθεί.

Για να εγκαταστήσουμε ασφαλή επικοινωνία, το HS και το AG χρειάζεται να αποθηκεύσουν τα απαραίτητα passkeys και κλειδιά σύνδεσης. Από τη στιγμή που το HS δεν αλληλεπιδρά με το χρήστη, μία εξωτερική συσκευή πρέπει να ελέγχει τις βασικές ρυθμίσεις του HS. Τέτοιες μπορούν να είναι η ένταση της φωνής, η διαχείριση των συσκευών που θα συνδεθούν και η ανταλλαγή των passkeys. Η πολιτική ασφαλείας για τα ακουστικά ζητά αυθεντικοποίηση και κρυπτογράφηση αλλά και κανόνες πρόσβασης. Οι τελευταίοι αποτελούν την πολιτική πρόσβασης που καθορίζει ποιες συνδέσεις ήχου επιτρέπονται και ποιες συσκευές μπορούν να έχουν απομακρυσμένο έλεγχο.



Εικόνα 5-2 Αρχιτεκτονική ασφαλείας ακουστικών

Το AG μπορεί να χρησιμοποιεί διαφορετικές καταστάσεις ασφαλείας από το HS. Το HS επίσης μπορεί να λειτουργεί σε όλες τις καταστάσεις. Αν και η κατάσταση ασφαλείας 1 δεν παρέχει ασφάλεια, δεν έχει αποκλειστεί. Ωστόσο, προτείνεται να χρησιμοποιείται η 3. Αν η συγκεκριμένη κατάσταση ασφαλείας είναι προκαθορισμένη, αυτή δεν μπορεί να αλλαχθεί από τον χρήστη. Έτσι, απαιτείται αυθεντικοποίηση κάθε φορά που εγκαθίσταται μια σύνδεση.

5.1.2 Διαχείριση κλειδιών

Γενικώς, τα ακουστικά δεν έχουν κάποια ανεπτυγμένη αλληλεπίδραση με τον χρήστη. Έτσι, είναι δύσκολο, αν όχι ακατόρθωτο, για έναν χρήστη να εισάγει μία καινούρια τιμή pass-key στο HS σε κάθε ζευγάρωμα. Ένα αμετάβλητο pass-key έχει μειονεκτήματα αφού η πιθανότητα να το βρει κάποιος την τιμή του pass-key είναι μεγαλύτερη όταν δεν αυτό δεν αλλάζει ποτέ από όταν ανανεώνεται περιοδικά. Οπότε όσο πιο συχνά αλλάζει η τιμή αυτή, τόσο το καλύτερο. Θα ήταν δυνατό οι ρυθμίσεις των ακουστικών να ελέγχονται από τη πύλη του ήχου. Κι αυτό διότι μια εξωτερική συσκευή έχει καλύτερη αλληλεπίδραση με τον χρήστη και έτσι επιτρέπεται η άμεση αλλαγή του pass-key. Βέβαια, πρέπει να είμαστε σίγουροι ότι η αλλαγή αυτή μπορεί να γίνει μόνο πάνω από αυθεντικοποιημένη και κρυπτογραφημένη σύνδεση.

5.1.3 Παράδειγμα

Έστω ότι έχουμε ακουστικό που θέλουμε να το συνδέσουμε και να το χρησιμοποιήσουμε σε ένα κινητό τηλέφωνο. Τα παρακάτω βήματα περιγράφουν τις ενέργειες του χρήστη, τις αλληλεπιδράσεις του κινητού τηλεφώνου με τα Bluetooth ακουστικά και τους υπολογισμούς ασφαλείας που λαμβάνουν χώρα προτού ο χρήστης να είναι έτοιμος να χρησιμοποιήσει τα ακουστικά με το κινητό τηλέφωνο:

- Ο χρήστης θέτει το ακουστικό σε ανιχνεύσιμη κατάσταση.
- Το ακουστικό υποδηλώνει στον χρήστη ότι είναι έτοιμο για ζευγάρωμα.
- Ο χρήστης ετοιμάζει το κινητό του τηλέφωνο για αναζήτηση νέων συσκευών Bluetooth.
- Το τηλέφωνο εκτελεί αναζήτηση και παίρνει μία απάντηση από το ακουστικό.
- Ως μέρος της εγκατάστασης του καναλιού LMP, το ακουστικό ζητάει αυθεντικοποίηση από το τηλέφωνο.
- Το τηλέφωνο ανιχνεύει ότι δεν έχει κάποιο προηγούμενο κλειδί σύνδεσης με το ακουστικό. Το ζευγάρωμα απαιτείται.
- Το τηλέφωνο προτρέπει τον χρήστη να εισάγει ένα pass-key για το ακουστικό.
- Ο χρήστης εισάγει τον κωδικό. Η ανταλλαγή του κλειδιού γίνεται μεταξύ του ακουστικού και του τηλεφώνου. Ένα κλειδί σύνδεσης παράγεται το οποίο μοιράζεται και στις δύο συσκευές.
- Το νέο κλειδί σύνδεσης αποθηκεύεται σε μια μη ευμετάβλητη μνήμη και στις δύο συσκευές.
- Το ακουστικό αυθεντικοποιεί το τηλέφωνο.
- Το τηλέφωνο αυθεντικοποιεί το ακουστικό.
- Το ακουστικό και το τηλέφωνο εκτελούν ανταλλαγή κλειδιού κρυπτογράφησης.
- Η εγκατάσταση του LMP έχει πλέον ολοκληρωθεί. Οι δύο συσκευές κρυπτογραφούν όλα τα δεδομένα που ανταλλάζουν από εδώ και στο εξής.
- Ο χρήστης βγάζει το ακουστικό από την ανιχνεύσιμη κατάσταση ώστε να μη δέχεται άλλες αιτήσεις για ζευγάρωμα.

5.2 Πρόσβαση σε δίκτυο

Η πρόσβαση μέσω Bluetooth σε ένα IP δίκτυο παρέχεται μέσω του PAN προφίλ. Το PAN επιτρέπει την ενθυλάκωση των Ethernet πακέτων επιτρέποντας την απευθείας πρόσβαση σε ένα τοπικό δίκτυο μέσω ενός σημείου πρόσβασης. Στην ενότητα αυτή θα αναφέρουμε πώς οι μηχανισμοί ασφαλείας μπορούν να εφαρμοστούν για να ασφαλίσουμε την πρόσβαση σε ένα LAN χρησιμοποιώντας το συγκεκριμένο προφίλ.

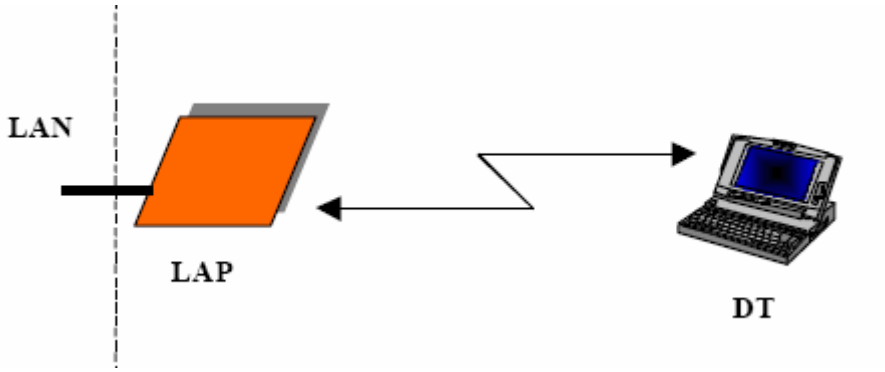
5.2.1 Σκοπός και σενάρια

Υπάρχουν δύο έννοιες που καθορίζονται στο προφίλ αυτό: το σημείο πρόσβασης δικτύου *(LAN access point - LAP)* και το τερματικό δεδομένων *(data terminal - DT)*. Το LAP είναι μία ασύρματη συσκευή Bluetooth που παρέχει πρόσβαση σε ένα LAN, όπως ethernet, token ring κ.τ.λ. Το DT χρησιμοποιεί τις υπηρεσίες του LAP. Τυπικές συσκευές που χρησιμοποιούνται τερματικά δεδομένων είναι οι φορητοί υπολογιστές, τα PDAs κ.τ.λ.

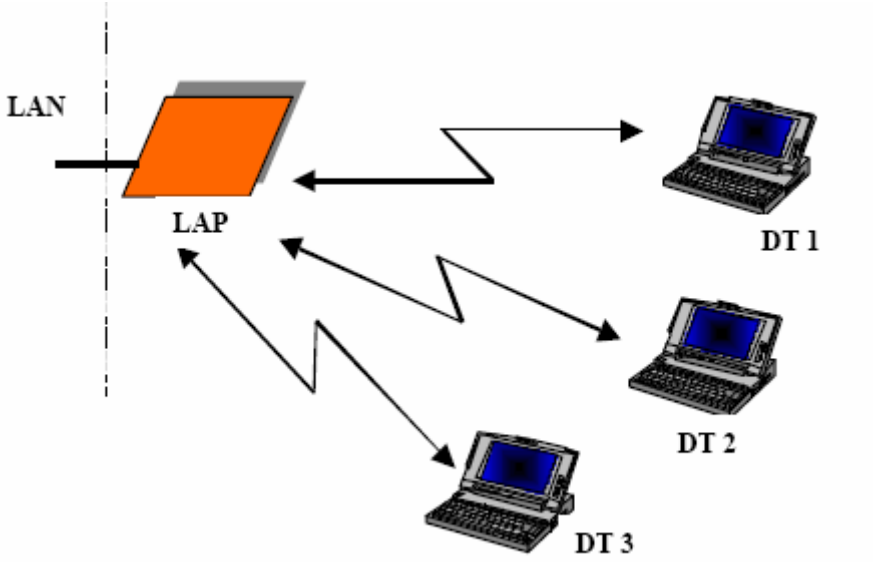
Τα ακόλουθα σενάρια περιγράφονται στο προφίλ πρόσβασης δικτύου:

1. Ένα τερματικό δεδομένων (DT) χρησιμοποιεί ένα σημείο πρόσβασης (LAP) ως ένα ασύρματο μέσο για να συνδεθεί σε ένα τοπικό δίκτυο (LAN).
2. Πολλαπλά τερματικά δεδομένων χρησιμοποιούν ένα σημείο πρόσβασης ως ασύρματο μέσο για να συνδεθεί σε ένα τοπικό δίκτυο.
3. PC-to-PC σύνδεση όπου δύο ασύρματες συσκευές Bluetooth μπορούν να εγκαταστήσουν μία σύνδεση η μία με την άλλη.

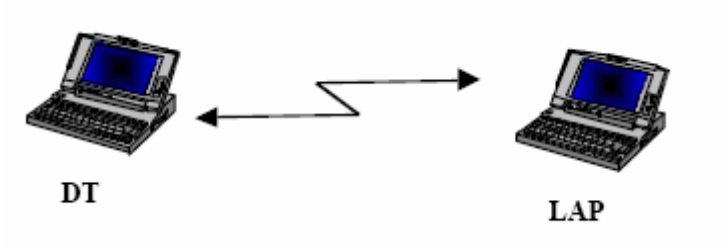
Τα τρία διαφορετικά σενάρια απεικονίζονται παρακάτω:



Εικόνα 5-3 Μία DT χρησιμοποιεί ένα LAP



Εικόνα 5-4 Πολλαπλά DTs χρησιμοποιούν ένα LAP

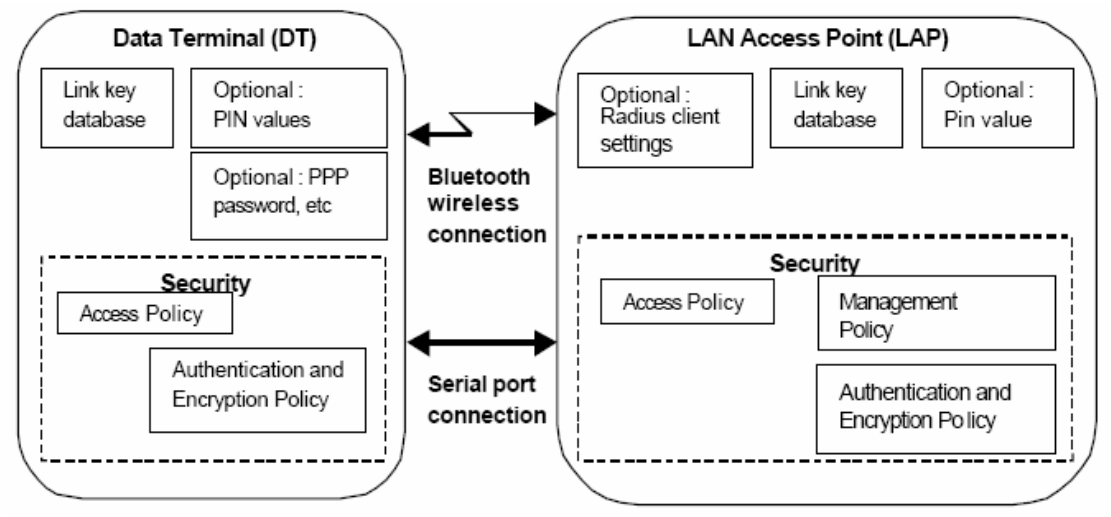


Εικόνα 5-5 PC to PC σύνδεση

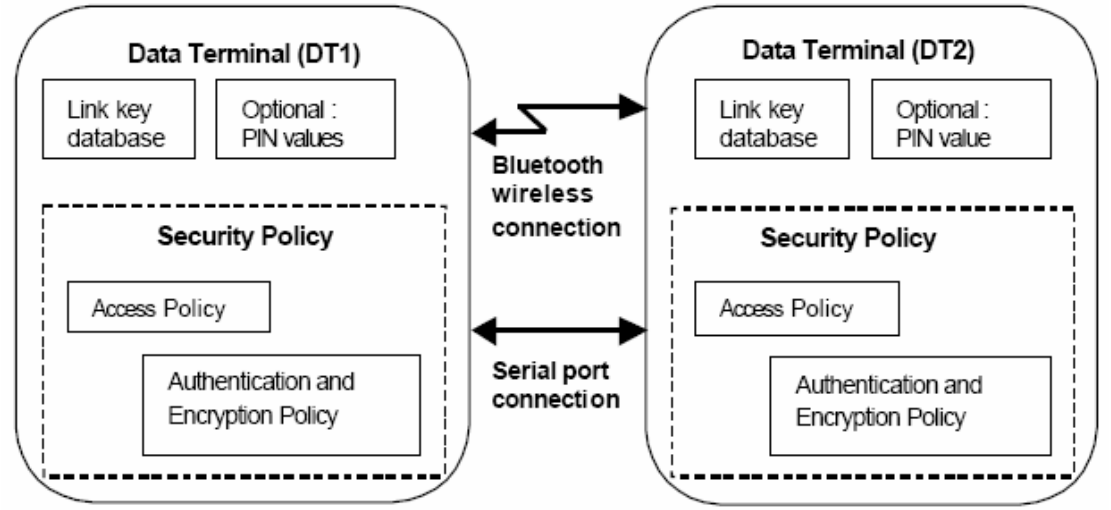
5.2.2 Αρχιτεκτονική ασφαλείας

Η αρχιτεκτονική που θα παρουσιαστεί μπορεί να χρησιμοποιηθεί και για τα τρία σενάρια. Η αυθεντικοποίηση και η κρυπτογράφηση παρέχονται στο επίπεδο IP ή εφαρμογής. Για παράδειγμα ένα πρωτόκολλο όπως το IPsec είναι κατάλληλο για ασφαλείς end-to-end IP υπηρεσίες όπως τα εικονικά προσωπικά δίκτυα (virtual private network). Το IPsec μπορεί να χρησιμοποιηθεί για οποιαδήποτε IP σύνδεση ανεξάρτητα από τον τρόπο σύνδεσης. Εδώ θα ήταν χρήσιμο να τονίσουμε ότι η ασφάλεια στο επίπεδο σύνδεσης δεν αποκλείει αυτή σε επίπεδο IP αλλά συμπληρώνει η μία την άλλη.

Παρακάτω απεικονίζεται η αρχιτεκτονική ασφαλείας στην περίπτωση ενός τερματικού δεδομένων και ενός σημείου πρόσβασης (σενάρια 1 & 2) και δύο τερματικών δεδομένων (σενάριο 3).



Εικόνα 5-6 Αρχιτεκτονική ασφαλείας DT – LAP



Εικόνα 5-7 Αρχιτεκτονική ασφαλείας DT - DT

Η αρχιτεκτονική αυτή βασίζεται στην ιδέα της εισαγωγής ενός νέου κλειδιού. Αυτό λέγεται κλειδί ομάδας *(group key)*. Είναι κλειδί σύνδεσης το οποίο δεν περιορίζεται σε μια συγκεκριμένη σύνδεση αλλά χρησιμοποιείται για όλες τις συνδέσεις που εγκαθίστανται πάνω από ένα συγκεκριμένο δίκτυο. Έτσι, ο χρήστης θα έχει ένα group key για όλα τα σημεία πρόσβασης του συγκεκριμένου δικτύου. Επιπλέον, διαφορετικοί χρήστες θα έχουν διαφορετικά κλειδιά ομάδας στο ίδιο δίκτυο και ένας χρήστης θα χρειάζεται διαφορετικό κλειδί ομάδας για διαφορετικό δίκτυο.

Μπορούμε να διακρίνουμε δύο διαφορετικές καταστάσεις:

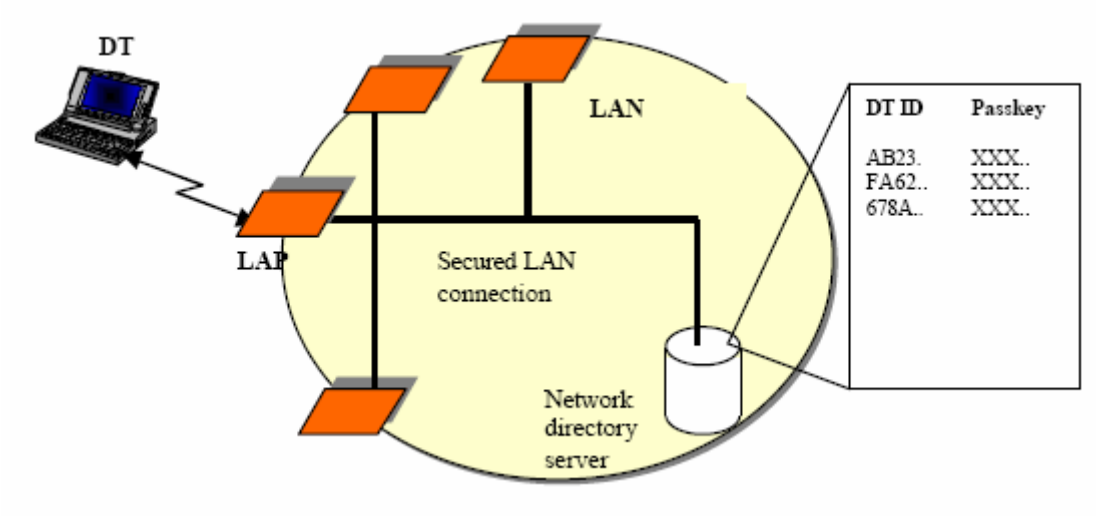
1. *Εγκατάσταση αρχικής σχέσης εμπιστοσύνης:* Αρχικά, ένα τερματικό δεδομένων προσπαθεί να συνδεθεί στο δίκτυο στο οποίο δεν έχει προϋπάρξει σύνδεση άλλη φορά. Οπότε, ένα κλειδί σύνδεσης πρέπει να ανταλλαχθεί.
2. *Μετέπειτα πρόσβαση στο σημείο πρόσβασης:* Εδώ χρησιμοποιούμε την ιδέα της μονάδας σε μία ομάδα και του group key. Αυτό σημαίνει ότι χωρίς την ανάγκη αλληλεπίδρασης με μηχανισμούς ασφαλείας υψηλότερων επιπέδων.

Εγκατάσταση αρχικής σχέσης εμπιστοσύνης

Ας υποθέσουμε ότι ένας χρήστης θέλει να καταχωρήσει το DT για να έχει πρόσβαση στο LAN διαμέσου του LAP. Η διαδικασία που λαμβάνει χώρα είναι η εξής: Όταν ένας χρήστης εγγράφεται σε μια υπηρεσία πρόσβασης LAN, λαμβάνει ένα μοναδικό ID που αναγνωρίζει τον πάροχο της υπηρεσίας. Μαζί με το ID λαμβάνει επίσης και ένα μυστικό Bluetooth passkey. Ο κωδικός αυτός παράγεται από τον πάροχο υπηρεσιών πρόσβασης στο δίκτυο χρησιμοποιώντας έναν ασφαλή γεννήτορα τυχαίων passkeys και είναι μοναδικός για κάθε DT. Ο χρήστης του DT χρειάζεται να εισάγει χειροκίνητα τις δύο αυτές τιμές:

- ID υπηρεσίας πρόσβασης στο δίκτυο
- Bluetooth κωδικός για μια συγκεκριμένη υπηρεσία πρόσβασης στο δίκτυο

Κατά την εγγραφή δίνεται επίσης στον χρήστη ένα μοναδικό DT ID. Αυτό το ID μπορεί να είναι μοναδικό για την πρόσβαση στο δίκτυο ή η Bluetooth διεύθυνση της ασύρματης συσκευής. Στη συνέχεια, ο Bluetooth κωδικός και το DT ID αποθηκεύονται σε μία ασφαλή βάση δεδομένων. Όλα τα LAPs πρέπει να έχουν ασφαλή πρόσβαση σ' αυτή τη βάση δεδομένων.



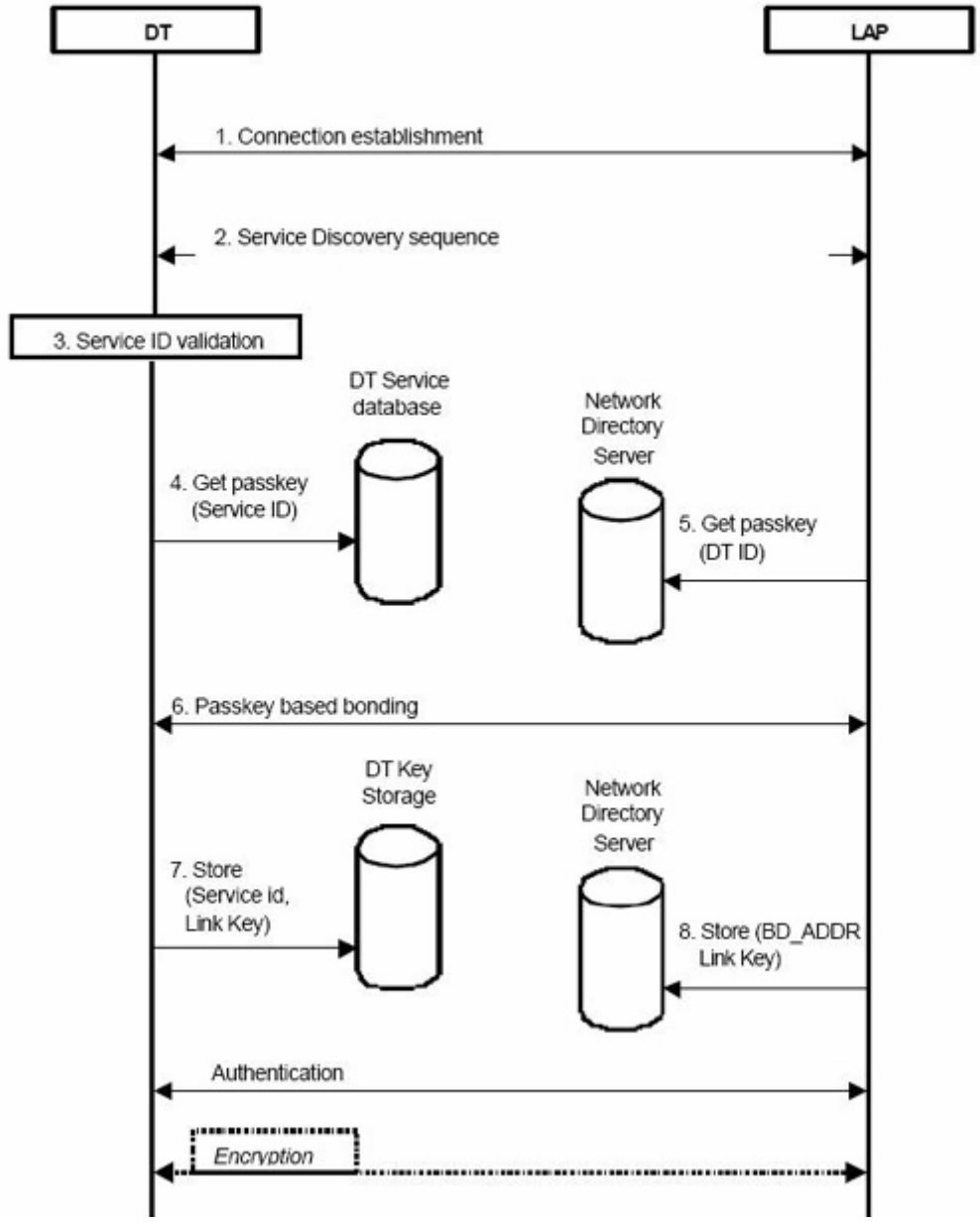
Εικόνα 5-8 Τοπικό δίκτυο με σημεία πρόσβασης και εξυπηρετητή

Από τη στιγμή που το DT λάβει το ID υπηρεσίας και το passkey, είναι δυνατό να συνδεθεί στο δίκτυο. Τα βήματα με τα οποία γίνεται αυτή η διαδικασία είναι τα εξής:

- Το DT συνδέεται στο LAP χρησιμοποιώντας τη διαδικασία αναζήτησης / ζευγαρώματος του Bluetooth.
- Το DT ενεργεί ως πελάτης SDP (service discovery protocol) και αναζητά υπηρεσία πρόσβασης στο δίκτυο πάνω στο LAP. Το DT λαμβάνει το ID υπηρεσίας του LAP. Το LAP μπορεί να εκτελέσει μία παρόμοια αναζήτηση στο DT για να λάβει το DT ID.
- Το DT ID ελέγχει αν γνωρίζει το ID υπηρεσίας που ελήφθη από το πρωτόκολλο SDP. Διαφορετικά διακόπτει τη διαδικασία σύνδεσης.
- Το DT ρωτά την εσωτερική βάση δεδομένων για τον Bluetooth κωδικό που αντιστοιχεί σε μια υπηρεσία.
- Ο κωδικός αυτός επιστρέφεται στο DT.
- Το LAP δημιουργεί μια ασφαλή σύνδεση προς τον server για να αποκτήσει τον Bluetooth κωδικό που αντιστοιχεί στο λαμβανόμενο DT ID.

- Το DT και το LAP «δένονται» μεταξύ τους χρησιμοποιώντας τον Bluetooth κωδικό που αποκτήθηκε από τη βάση δεδομένων. Αυτό έχει ως αποτέλεσμα το διαμοιρασμό ανάμεσα στο DT και το LAP ενός κοινού κλειδιού σύνδεσης.
- Το DT χρησιμοποιεί την HCI εντολή Write_Stored_Link_Key για να αποθηκεύσει το παραγόμενο κλειδί στη μονάδα Bluetooth. Το κλειδί αυτό αποθηκεύεται επίσης ως group key για την υπηρεσία του LAP στη βάση δεδομένων κλειδιών του εξυπηρετούμενου.
- Το LAP χρησιμοποιεί την HCI εντολή Write_Stored_Link_Key για να αποθηκεύσει το παραγόμενο κλειδί στη μονάδα Bluetooth. Το κλειδί αυτό αποθηκεύεται επίσης ως group key για το DT στον server.
- Το DT και το LAP κάνουν αυθεντικοποίηση χρησιμοποιώντας το νέο αυτό κλειδί.
- Προαιρετικά η σύνδεση Bluetooth μπορεί να κρυπτογραφηθεί.

Παρακάτω φαίνεται διαγραμματικά η διαδικασία αυτή:

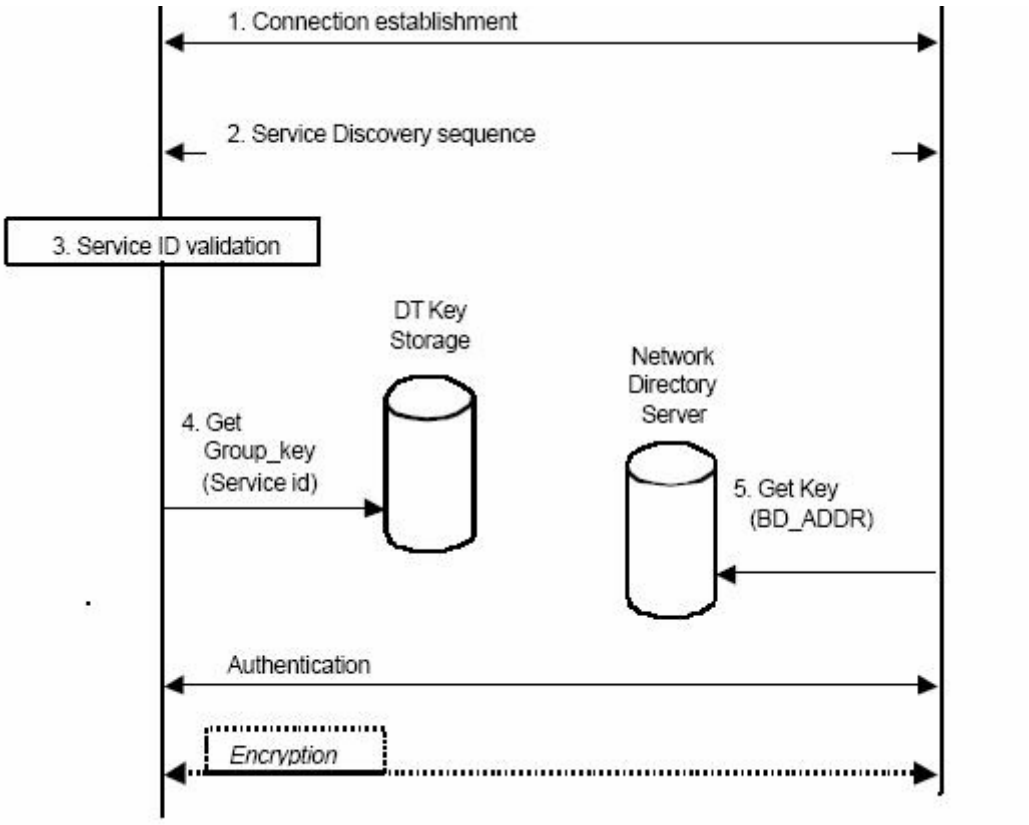


Εικόνα 5-9 Διαδικασία σύνδεσης στο δίκτυο

Μετέπειτα πρόσβαση στο σημείο πρόσβασης

Ας υποθέσουμε ότι βρισκόμαστε στην κατάσταση ασφαλείας 2. Αυτό σημαίνει ότι δεν υπήρξαν διαδικασίες ασφαλείας πριν αρχικοποιηθεί η εγκατάσταση του καναλιού. Η ιδέα του group key μπορεί να χρησιμοποιηθεί μόνο στην κατάσταση ασφαλείας 2. Αν το DT συνδεθεί στο LAN για πρώτη φορά, η αυθεντικοποίηση και κρυπτογράφηση λαμβάνει χώρα σύμφωνα με την περιγραφή στην προηγούμενη ενότητα. Για όλες τις άλλες περιπτώσεις, ακολουθείται η διαδικασία που περιγράφεται παρακάτω:

- Το DT συνδέεται στο LAP χρησιμοποιώντας τη διαδικασία ζευγαρώματος του Bluetooth.
- Το DT ενεργεί ως SDP πελάτης και αναζητά για υπηρεσία πρόσβασης στο δίκτυο. Το DT λαμβάνει το ID υπηρεσίας του LAP.
- Το DT ελέγχει αν γνωρίζει το ID υπηρεσίας που ελήφθη από το SDP πρωτόκολλο. Αν όχι, διακόπτει τη διαδικασία σύνδεσης.
- Αυτή δεν είναι η πρώτη φορά που το DT συνδέεται στο συγκεκριμένο LAN. Το DT διαβάζει το group key που αντιστοιχεί στο λαμβανόμενο ID υπηρεσίας από τη βάση δεδομένων κλειδιών του DT.
- Το LAP δημιουργεί ασφαλή σύνδεση προς τον server του δικτύου για να αποκτήσει το κλειδί σύνδεσης που αντιστοιχεί στην BD_ADDR του συνδεδεμένου DT.
- Το DT και το LAP χρησιμοποιούν την εντολή Write_Strored_Link_Key για να κάνει το κλειδί σύνδεσης διαθέσιμο στην μονάδα Bluetooth. Αμοιβαία αυθεντικοποίηση λαμβάνει χώρα.



Εικόνα 5-10 Εφαρμογή του κλειδιού ομάδας (group key)

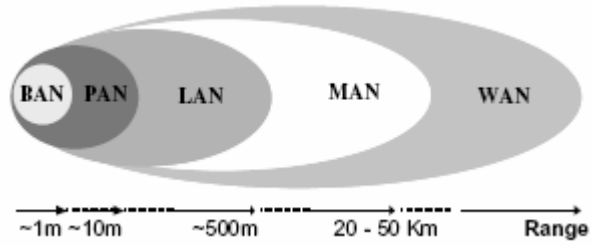
ΚΕΦΑΛΑΙΟ 6
BLUETOOTH ΚΑΙ AD HOC ΔΙΚΤΥΑ

6.1 Εισαγωγή

Ένα δίκτυο ad hoc έχει το βασικό πλεονέκτημα του ότι δεν χρειάζεται κάποιο access point για να συνδεθούν οι υποψήφιοι κόμβοι. Όταν μια συσκευή βρεθεί στην περιοχή κάλυψης του δικτύου και διαθέτει το απαιτούμενο υλικό, στην περίπτωσή μας ένα Bluetooth dongle, μπορεί να συνδεθεί σε αυτό και να γίνει μέλος του. Συνήθως, χρησιμοποιούνται για την επέκταση των υπαρχόντων ενσύρματων ή ασύρματων δικτύων. Μπορούμε να ταξινομήσουμε τα δίκτυα ad hoc με βάση την περιοχή κάλυψης: Body (BAN), Personal (PAN), Local (LAN), Metropolitan (MAN), Wide (WAN).

Τα MAN και WAN ad hoc δίκτυα είναι ασύρματα δίκτυα που χρησιμοποιούν πολλές αναπηδήσεις(multi-hop) αλλά ακόμα αντιμετωπίζουν πολλά προβλήματα που αναζητούν λύση. Μερικά από αυτά είναι η διευθυνσιοδότηση, η δρομολόγηση και η ασφάλεια. Αντιθέτως, τα BAN, LAN και PAN adhoc δίκτυα τα οποία καλύπτουν μικρή περιοχή είναι σε θέση να χρησιμοποιηθούν. Ήδη πολλά κτιριακά συγκροτήματα τα χρησιμοποιούν για να δικτυωθούν. Παρακάτω, θα αναφερθούμε σε αυτά τα δίκτυα πιο αναλυτικά δίνοντας μια μικρή περιγραφή για το καθένα.

Τα BAN δίκτυα συσχετίζονται άμεσα με τους υπολογιστές που μπορούμε να φορέσουμε (wearable computers). Ένας τέτοιος υπολογιστής διανέμει τα κομμάτια του σε ολόκληρο το σώμα του ανθρώπου που τον φέρει. Έτσι, υπάρχουν οθόνες που προσαρμόζονται στα μάτια του φορέα, ακουστικά, μικρόφωνα κλπ. Το δίκτυο αναλαμβάνει να ενώσει όλα αυτά τα κομμάτια έτσι ώστε να δουλεύουν αρμονικά και χωρίς συγκρούσεις. Το εύρος επικοινωνία ενός BAN είναι όσο περίπου είναι ένα ανθρώπινο σώμα, δηλαδή 1,5-2 μέτρα.



Εικόνα 6-1 Τύποι δικτύων ανάλογα με την απόσταση

Τα PAN δίκτυα ενώνουν φορητές συσκευές που κουβαλούν οι χρήστες πάνω τους με άλλες φορητές ή σταθερές συσκευές. Ενώ, τα δίκτυα BAN δικτυώνουν συσκευές σε μια περιοχή 1-2 μέτρων, τα PAN την επεκτείνουν στα 10 μέτρα. Η πιο πολλά υποσχόμενη ραδιοσυχνότητα για αυτή τη χρήση δεν είναι άλλη από αυτή των 2,4 GHz.

Αν θέλουμε να δικτυώσουμε μια ευρύτερη περιοχή η οποία θα φτάνει το ένα οικοδομικό τετράγωνο, δηλαδή 100-500 μέτρα, τότε είναι προτιμότερο να περάσουμε στη λύση του ασύρματου τοπικού δικτύου (WLAN). Ένα τέτοιο δίκτυο θα πρέπει να ικανοποιεί τις απαιτήσεις ενός απλού τοπικού δικτύου, δηλαδή υψηλή χωρητικότητα, πλήρη συνδεσιμότητα μεταξύ των κόμβων κλπ. Όμως, για να ικανοποιηθούν τα παραπάνω θα πρέπει να επιλυθούν κάποια θέματα ασύρματης φύσεως, όπως είναι η

ασφάλεια των δεδομένων που μεταδίδονται στον αέρα, η κατανάλωση ρεύματος και η φορητότητα των κόμβων.

Υπάρχουν δυο προσεγγίσεις για την υλοποίηση ενός τέτοιου δικτύου. Η πρώτη απαιτεί την ύπαρξη μιας σταθερής εγκατάστασης η οποία θα συνδέει το ενσύρματο με το ασύρματο δίκτυο και θα παρέχει σε αυτό πρόσβαση στο Internet. Αυτή η συσκευή ονομάζεται Access Point (AP). Η δεύτερη προσέγγιση χρησιμοποιεί ad hoc δίκτυα, τα οποία είναι peer-to-peer δίκτυα αποτελούμενα από διάφορες συσκευές οι οποίες βρίσκονται η μία εντός της ευρύτερης περιοχής της άλλης. Ένα τέτοιο δίκτυο δεν έχει σταθερή δομή καθώς μπορεί κάποια νέα συσκευή να εισέλθει και να την τροποποιήσει [21].

6.2 Bluestars: ένα μοντέλο σχηματισμού ενός ad hoc Bluetooth δικτύου

Μια διαφορετική λύση στο πρόβλημα σχηματισμού ενός ad hoc δικτύου μεταξύ Bluetooth – ενεργοποιημένων συσκευών προσπαθεί να δοθεί στην [22]. Το μοντέλο που προτείνεται ονομάζεται Bluestars και ακολουθεί τρεις φάσεις για την εγκαθίδρυση ενός τέτοιου δικτύου: ανακάλυψη γειτονικών συσκευών, ομαδοποίηση και διανομή ρόλων σε αυτές.

6.2.1 Ανακάλυψη γειτονικών συσκευών

Το πρώτο βήμα για τη δημιουργία ενός δικτύου μεταξύ Bluetooth – ενεργοποιημένων συσκευών είναι η ανακάλυψη των γειτονικών συσκευών. Η διαδικασία που ακολουθείται πρακτικά είναι η επαναλαμβανόμενη αποστολή ενός μηνύματος σε διαφορετικές συχνότητες (λόγω της αναπήδησης συχνότητας). Οι γειτονικές συσκευές «ακούν» σε μια από τις συχνότητες περιοδικά και όταν λάβουν το μήνυμα αποκρίνονται. Με αυτό τον τρόπο γίνεται η ανακάλυψη των συσκευών.

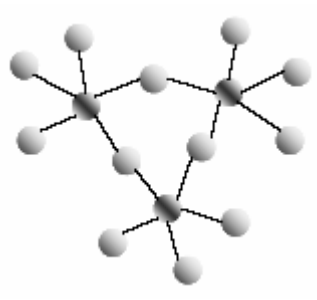
Αυτή η διαδικασία, όμως, δεν είναι απόλυτα επιθυμητή στην περίπτωση της ad hoc δικτύωσης. Ένας λόγος είναι ότι η διαδικασία έρευνας απαιτεί μεγάλο χρονικό διάστημα, κοντά στα 10 δευτερόλεπτα, για να πραγματοποιηθεί. Αυτό σημαίνει ότι για αυτό το χρονικό διάστημα δεν μπορούν να πραγματοποιηθούν άλλες εργασίες στο δίκτυο. Ένα άλλο πρόβλημα που δημιουργείται είναι ότι η διαδικασία ανακάλυψης συσκευών είναι ασύμμετρη. Αυτό σημαίνει ότι ενώ μια συσκευή εκτελεί μια εργασία (πχ inquiry) μια άλλη πρέπει να κάνει κάποια άλλη εργασία. Αυτή η ιδιότητα είναι ανεπιθύμητη για ad hoc δικτύωση.

6.2.2 Ομαδοποίηση γειτονικών συσκευών

Αφού έχει ολοκληρωθεί η διαδικασία εύρεσης των γειτονικών συσκευών και έχουν αναγνωριστεί, το επόμενο βήμα είναι η εγκαθίδρυση μιας λογικής σύνδεσης μεταξύ αυτών. Είναι άκρως σημαντικός ο τρόπος με τον οποίο θα συνδεθούν οι κόμβοι μεταξύ τους, αφού ένας λανθασμένος τρόπος μπορεί να οδηγήσει στην απομόνωση ενός κόμβου ή ακόμα και στην κατάρρευση του δικτύου. Μια πρώτη προφανής προσέγγιση είναι η σύνδεση των κόμβων έτσι ώστε να απέχουν όλοι ένα βήμα. Κάτι τέτοιο όμως θα οδηγούσε σε διαμοιρασμό του εύρους ζώνης σε πολλούς κόμβους άρα και στην μείωση της απόδοσης του δικτύου. Αν, όμως, οδηγούμασταν στην υιοθέτηση μιας προσέγγισης κατά την οποία εγκαθιδρύαμε λογικές συνδέσεις μόνο σε κάποιους από τους κόμβους τότε θα υπήρχε μεγάλη πιθανότητα να

δημιουργούνταν μεγάλα μονοπάτια ή ακόμα και ένας κόμβος να γινόταν απροσπέλαστος. Λόγω των προαναφερθέντων, πρέπει να γίνει προσεκτική επιλογή του τρόπου σύνδεσης των κόμβων λαμβάνοντας υπόψη την επίδοση του δικτύου.

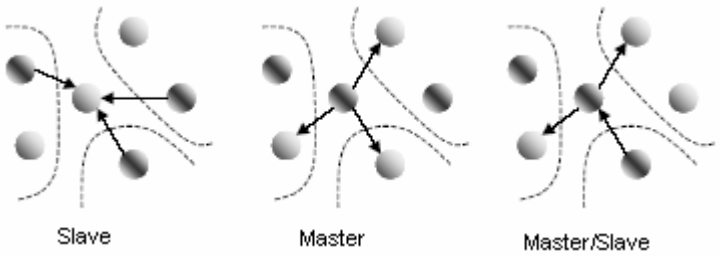
Η λύση που προτείνεται στην εργασία βρίσκεται ενδιάμεση των δυο προτάσεων που αναφέρθηκαν παραπάνω. Έτσι, όλοι οι γειτονικοί κόμβοι ομαδοποιούνται σε σύνολα και δημιουργείται ένας σύνδεσμος σε έναν από τους κόμβους σε κάθε σύνολο. Πιο συγκεκριμένα, ομαδοποιούνται οι κόμβοι ανάλογα με το piconet στο οποίο ανήκουν. Εύκολα μπορεί να πραγματοποιηθεί ο έλεγχος για το αν δυο κόμβοι ανήκουν στην ίδια ομάδα καθώς αρκεί να ανατρέξουν στις λίστες τους και να δουν αν έχουν κοινή εγγραφή για την κύρια (master) συσκευή. Στη συνέχεια, δημιουργείται μια σύνδεση σε έναν κόμβο σε κάθε σύνολο. Η τοπολογία που δημιουργήθηκε, περιλαμβάνει μια άμεση σύνδεση σε κάθε γειτονικό piconet και επιπλέον έχει την ιδιότητα το μονοπάτι μεταξύ δυο κόμβων να αποτελείται το μέγιστο από τρία βήματα. Αυτή η τοπολογία ονομάζεται Bluestars καθώς σχηματικά μοιάζει με ενωμένα αστέρια, όπου κάθε αστέρι αντιστοιχεί σε ένα piconet.



Εικόνα 6-2
Παράδειγμα ενός Bluestar

6.2.3 Διανομή ρόλων στους κόμβους

Το επόμενο βήμα είναι ο ορισμός των ρόλων σε κάθε κόμβο του δικτύου. Έτσι, ένας κόμβος μπορεί να είναι είτε master είτε slave είτε να έχει και τους δυο ρόλους ανάλογα με την ανάγκη που δημιουργείται. Για να καταλήξουμε, στον ρόλο που πρέπει να διανείμουμε σε κάποιον κόμβο πρέπει πρώτα να αναλογιστούμε κάποια πράγματα.



Εικόνα 6-3 Οι διάφοροι ρόλοι ενός κόμβου

Αρχικά, πρέπει να καθοριστεί ο αριθμός των κυρίων συσκευών (masters) ο οποίος είναι ισοδύναμος με τον αριθμό των piconets. Στη συνέχεια, πρέπει να αναγνωρίσουμε τους διαφορετικούς ρόλος που χρειάζεται να παίζει μια συσκευή, καθώς υπερβολικοί ρόλοι μπορούν να προκαλέσουν μεγάλο φόρτο σε μια μικρή συσκευή.

Όταν αναγνωριστεί μια νέα γειτονική συσκευή, ελέγχει πρώτα να δει αν υπάρχουν κοντά κάποιες ομάδες που έχουν κύρια συσκευή και τότε παίρνει τον ρόλο του slave. Σε αυτή την περίπτωση, ο αριθμός των piconets δεν τροποποιείται καθώς δεν άλλαξε ο αριθμός των κυρίων συσκευών. Όταν, όμως, κάποια γειτονική ομάδα δεν έχει κύρια συσκευή ή η κύρια συσκευή δεν μπορεί να εξυπηρετήσει παραπάνω slaves τότε αναλαμβάνει τον ρόλο της κύριας συσκευής. Έτσι, αυξάνεται ο αριθμός των piconets κατά ένα. Η τελευταία περίπτωση επιδιώκεται μόνο στην περίπτωση που οι δυο προηγούμενες δεν ήταν δυνατό να πραγματοποιηθούν.

6.3 Δια-οχηματική επικοινωνία με ad hoc Bluetooth δικτύωση

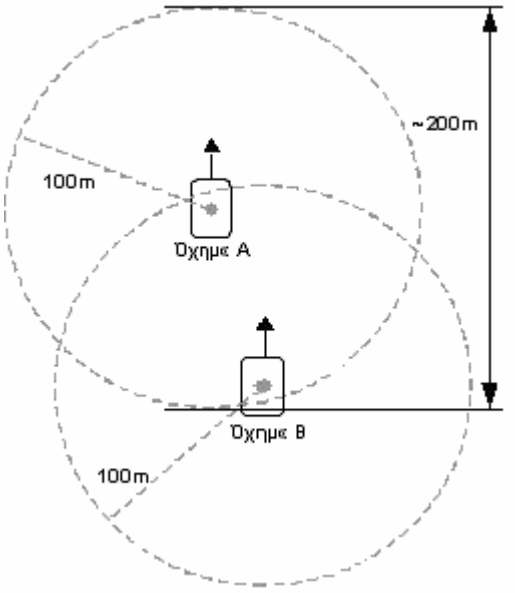
Ένα παράδειγμα δικτύωσης ad hoc είναι η προσπάθεια και έρευνα που πραγματοποιείται τα τελευταία χρόνια πάνω στη δικτύωση των οχημάτων που κινούνται σε ένα δρόμο. Για την αύξηση της φορητότητας των κόμβων του δικτύου χρησιμοποιείται το πρωτόκολλο Bluetooth. Ένα βασικό πεδίο της έρευνας που πραγματοποιείται είναι η εύρεση τρόπου ενσωμάτωσης όλων των συσκευών στα οχήματα [23], [24].

Το βασικό δίκτυο που σχηματίζεται μεταξύ συσκευών Bluetooth ονομάζεται piconet. Κάθε piconet μπορεί να επικοινωνήσει με αντίστοιχα δίκτυα και με αυτό τον τρόπο σχηματίζεται ένα δίκτυο υψηλότερου επιπέδου το οποίο ονομάζεται scatternet. Η δρομολόγηση των πακέτων σε αυτά τα δίκτυα εξαρτάται άμεσα από την τοπολογία τους. Ο τρόπος με τον οποίο δημιουργείται η τοπολογία των scatternets πρόκειται για ένα ξεχωριστό τομέα έρευνας.

Μέχρι αυτή τη στιγμή, η έρευνα στον τομέα των ad hoc Bluetooth δικτύων έχει εστιαστεί σε δίκτυα οι κόμβοι των οποίων δεν μετακινούνται με μεγάλη ταχύτητα άρα και η τοπολογία του δικτύου μπορεί να χαρακτηριστεί σχεδόν σταθερή. Αυτά τα δεδομένα δεν αρκούν όμως για την περίπτωση της δια-οχηματικής επικοινωνίας καθώς η ταχύτητα και η γρήγορη εναλλαγή της τοπολογίας του δικτύου επηρεάζει άμεσα τα πρωτόκολλα που χρησιμοποιούνται.

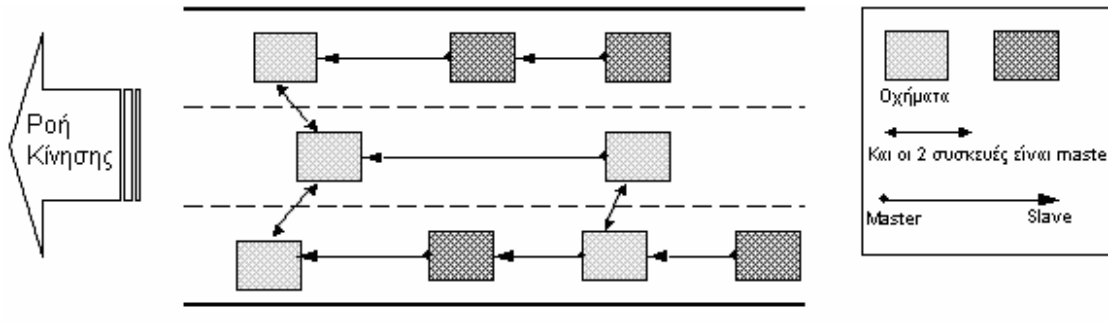
Πιο συγκεκριμένα, γνωρίζοντας τον χρόνο που απαιτείται για να εγκατασταθεί μια σύνδεση μεταξύ δυο συσκευών αλλά και την ταχύτητα των οχημάτων, μπορούμε να υπολογίσουμε τον χρόνο επικοινωνίας μεταξύ αυτών (βλέπε εικόνα 6-4).

Το όχημα Α ταξιδεύει με 97 km/h και το όχημα Β με 113 km/h. Υπάρχει δηλαδή μια διαφορά ταχύτητας 16 km/h η οποία αντιστοιχεί με 4,5 m/s περίπου. Όταν το όχημα Β βρεθεί εντός της περιοχής του Α θα χρειαστεί να καλύψει 200 μέτρα περισσότερα από το Α για να ξεφύγει από την ακτίνα του Bluetooth. Έχοντας ως δεδομένο τις ταχύτητες των οχημάτων τότε μπορούμε να βγάλουμε το συμπέρασμα ότι θα είναι σε απόσταση επικοινωνίας για ένα χρονικό διάστημα των 44 δευτερολέπτων.



Εικόνα 6-4 Απόσταση μεταξύ των οχημάτων και εύρος κάλυψης

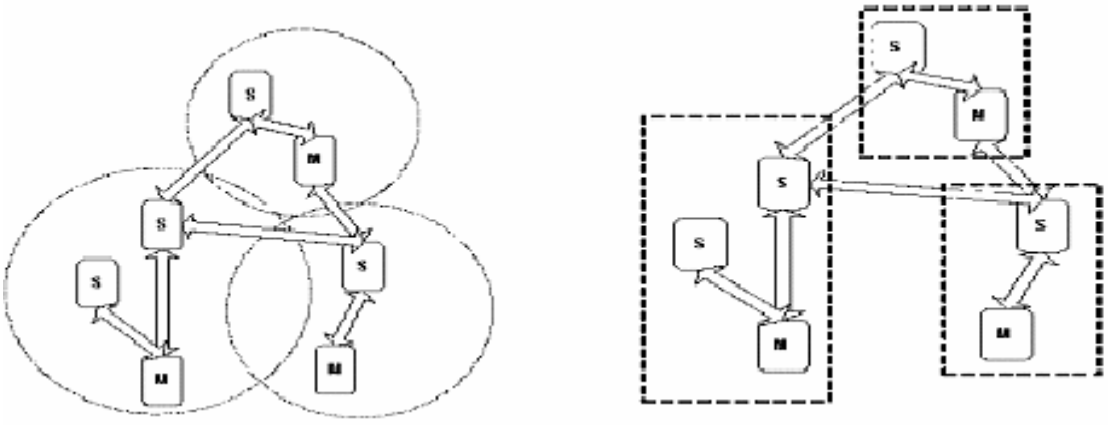
Γίνεται εύκολα κατανοητό ότι οι πληροφορίες θέσης ενός οχήματος μέσα στο δίκτυο είναι άκρως σημαντικές για την λειτουργία του δικτύου. Αυτό συμβαίνει επειδή ένα όχημα μπορεί καθώς κινείται να μετακινείται από το ένα δίκτυο στο άλλο. Αλλά αν χρησιμοποιήσει πληροφορίες θέσης και την ταχύτητα των οχημάτων μπορεί εύκολα να κατανοήσει την σχετική θέση και ταχύτητα των τριγύρω οχημάτων και επομένως να επικοινωνήσει με κάποιο από αυτά.



Εικόνα 6-5 Μεταπήδηση του κόμβου από το ένα δίκτυο στο άλλο

Ένας άλλος τρόπος χειρισμού των δικτύων αυτών είναι η χρήση των ομάδων (clusters). Στο πρωτόκολλο Bluetooth, μια ομάδα δημιουργείται κάθε φορά που δημιουργείται και ένα piconet. Έτσι, κάθε όχημα – κόμβος ανήκει σε μια συγκεκριμένη ομάδα η οποία έχει ένα μοναδικό ID, το οποίο δεν είναι άλλο από τη διεύθυνση Bluetooth της κύριας συσκευής.

Για κάθε piconet μπορούμε να φανταστούμε μια ιδεατή περίμετρο που το ορίζει. Παρακάτω, στο σχήμα εμφανίζονται δυο διαφορετικές περίμετροι για το ίδιο scatternet. Η κύρια (master) συσκευή του κάθε piconet είναι υπεύθυνη για την



Εικόνα 6-6 Δυο διαφορετικές περίμετροι για το ίδιο scatternet

μετάδοση των δεδομένων στους slaves. Κάθε κόμβος – slave που βρίσκεται στα όρια της περιμέτρου μπορεί να παίξει τον ρόλο της σύνδεσης με κάποιο γειτονικό piconet. Με αυτό τον τρόπο, υλοποιείται η διαδικτύωση των piconets άρα και η δημιουργία ενός scatternet. Επίσης, οι κόμβοι θα πρέπει να γνωρίζουν την ταυτότητα των γειτονικών piconets για να ξέρουν ανά πάσα στιγμή αν τους συμφέρει να μεταφερθούν σε κάποιο από αυτά.

6.4 Ασφάλεια στα ad hoc Bluetooth δίκτυα

Η φύση των ad hoc δικτύων είναι αυτή που δημιουργεί κατά ένα πολύ μεγάλο ποσοστό τα όποια προβλήματα ασφαλείας παρουσιάζονται σε αυτά τα δίκτυα. Όταν λέμε φύση αναφερόμαστε στο γεγονός ότι ένα ad hoc δίκτυο δεν έχει σταθερή τοπολογία και οι συνδέσεις μεταξύ των κόμβων του είναι κατά ένα πολύ μεγάλο ποσοστό ασύρματες. Όλο αυτά τα χαρακτηριστικά των ad hoc δικτύων τα καθιστούν περίπλοκα σε ζητήματα ασφάλειας και πολύ ευπαθή σε επιθέσεις [25].

6.4.1 Διαθεσιμότητα

Στα ad hoc δίκτυα η διαθεσιμότητα είναι πιο σημαντική απ' ό,τι στα παραδοσιακά δίκτυα. Και αυτό διότι όλες οι συσκευές εξαρτώνται η μία από την άλλη και επιπλέον όλη η πληροφορία μεταφέρεται μέσω του αέρα με αποτέλεσμα το να "πέσει" το δίκτυο να είναι πολύ εύκολο. Παραδείγματος χάριν, ένας κακόβουλος χρήστης θα μπορούσε να προσπαθήσει να φράξει ή να παρέμβει στη ροή των πληροφοριών μέσω του αέρα. Επίσης, θα μπορούσε να αναστατωθεί το πρωτόκολλο δρομολόγησης που χρησιμοποιήθηκε στο δίκτυο δίνοντας στο δίκτυο ανακριβείς πληροφορίες.

Τα πρωτόκολλα δρομολόγησης είναι στην πραγματικότητα ένα από τα πιο τρωτά σημεία στα ad hoc δίκτυα. Αυτά πρέπει να είναι σε θέση να χειριστούν τη μεταβαλλόμενη τοπολογία του δικτύου και τις επιθέσεις από τους κακόβουλους χρήστες. Υπάρχουν πάντως τέτοια πρωτόκολλα δρομολόγησης που μπορούν να προσαρμοστούν καλά στη μεταβαλλόμενη τοπολογία.

6.4.2 Αυθεντικοποίηση και Διαχείριση Κλειδιών

Η αυθεντικοποίηση είναι ένα άλλο δύσκολο θέμα στα ad hoc δίκτυα. Δεδομένου ότι υπάρχει ελάχιστη ή καμία υποδομή, η αναγνώριση των χρηστών (π.χ. συμμετέχοντες σε μια αίθουσα συνεδριάσεων) δεν είναι εύκολη. Από την άλλη θα μπορούσε να χρησιμοποιηθεί ένα γενικό πρωτόκολλο για τη διαχείριση των κλειδιών. Αυτό όμως παρουσιάζει αρκετά μειονεκτήματα αφού δεν ταιριάζει στα χαρακτηριστικά ενός ειδικού δικτύου (με μικρότερους επεξεργαστές απ' ό,τι οι κανονικοί υπολογιστές, μη συγκεκριμένη τοπολογία).

6.4.3 Εμπιστευτικότητα και ακεραιότητα

Η εμπιστευτικότητα είναι επίσης ένα τρωτό σημείο. Λόγω της ασύρματης επικοινωνίας, οποιοσδήποτε μπορεί να υποκλέψει μηνύματα και μάλιστα χωρίς την απαραίτητη κρυπτογράφηση μπορούν τα δεδομένα αυτά να είναι διαθέσιμα προς ανάγνωση. Ένας τρόπος να διασφαλιστεί η ροή των δεδομένων είναι η χρήση του κλειδιού συνδυασμού για την κρυπτογράφηση τους. Η χρήση αυτού του τύπου κλειδιού συνεπάγεται την δημιουργία τέτοιων κλειδιών από την κύρια συσκευή με κάθε άλλη slave συσκευή ανά ζεύγος . Έτσι, τα δεδομένα από έναν αποστολέα σκλάβο πρώτα μεταφέρονται στον master και μετά από αυτόν καταλήγουν στον παραλήπτη-σκλάβο .

Ένας εναλλακτικός τρόπος διασφάλισης της κίνησης των δεδομένων είναι η χρησιμοποίηση της θεώρησης του κύριου κλειδιού. Πλέον κατά την κρυπτογράφηση των δεδομένων χρησιμοποιείται το ίδιο κλειδί από όλους τους κόμβους του δικτύου . Εδώ φτάνουμε στο όριο της ασφάλειας σε επίπεδο σύνδεσης στα δίκτυα ad hoc. Αν θέλουμε να χρησιμοποιήσουμε πιο πολύπλοκη δικτύωση ad hoc τότε θα πρέπει να μεταφέρουμε την ασφάλεια στο επίπεδο εφαρμογής .

Από την άλλη, χωρίς την απαραίτητη αυθεντικοποίηση, δεν έχει νόημα να μιλάμε για εμπιστευτικότητα αφού δε θα μπορούμε να καθορίσουμε σε ποιον συγκεκριμένο χρήστη θέλουμε να στείλουμε την πληροφορία. Παρόμοια κατάσταση ισχύει και στην ακεραιότητα. Όπως είπαμε, επειδή η σύνδεση είναι ασύρματη, τα δεδομένα είναι δυνατό να τροποποιηθούν με παρέμβαση στη συχνότητα των κυμάτων.

6.4.4 Απειλές Ασφαλείας

Όπως έχει αναφερθεί ήδη παραπάνω, κύριος στόχος των επιθέσεων σε ένα Bluetooth ad hoc δίκτυο είναι το πρωτόκολλο δρομολόγησης [26] [27] [28]. Έτσι, με την είσοδο ενός κακόβουλου κόμβου μπορεί να διαταραχθεί η λειτουργία του μηχανισμού δρομολόγησης. Στόχος, λοιπόν, ενός πρωτοκόλλου ασφαλούς δρομολόγησης είναι το να προστατεύει το δίκτυο από τις επεμβάσεις κακόβουλων κόμβων.

Γενικά, οι επιθέσεις μπορούν να κατηγοριοποιηθούν ως εξής:

- Επιθέσεις διάσπασης της δρομολόγησης

  Σε αυτόν τον τύπο επίθεσης, ο κακόβουλος κόμβος ηθελημένα και επανειλημμένα απορρίπτει πακέτα ελέγχου, δρομολογεί λανθασμένα τα πακέτα και διαδίδει λανθασμένα πληροφορίες που αφορούν τους γειτονικούς του κόμβους. Ο επιτιθέμενος θα προσπαθήσει να:

  1. τροποποιήσει τις διευθύνσεις αποστολέα και παραλήπτη στα δρομολογούμενα μηνύματα.
  2. «ηχήσει» ψεύτικους συναγερμούς λανθασμένης δρομολόγησης ή να τροποποιήσει τα μηνύματα λάθους.
  3. πλαστογραφήσει μηνύματα με το να τροποποιεί τις διευθύνσεις του αποστολέα ή του παραλήπτη.

- Επιθέσεις κατανάλωσης των πόρων

  Σε αυτή την επίθεση, ο επιτιθέμενος προσπαθεί να εξαντλήσει τους πόρους του συστήματος με τους εξής τρόπους:

  1. εκκινεί πολυάριθμες αιτήσεις δρομολόγησης
  2. κάνει επιλεκτική απόρριψη πακέτων κάτι που έχει ως αποτέλεσμα τον αυξημένο αριθμό αιτήσεων δρομολόγησης από τους γειτονικούς κόμβους που έχουν περιορισμένες ικανότητες δρομολόγησης.

- Επιθέσεις στα διακινούμενα δεδομένα

  Σε αυτή την περίπτωση, ο επιτιθέμενος κόμβος τροποποιεί τα διακινούμενα δεδομένα έτσι ώστε να μην είναι πλέον αναγνώσιμα από το σύστημα. Αυτό συνεπάγεται την καταστροφή τους και άρα την επιφόρτιση του δικτύου με την επαναποστολή τους.

6.4.5 Συνεργαζόμενοι κακόβουλοι κόμβοι

Οι επιθέσεις που θα αναφερθούν παρακάτω πραγματοποιούνται από μια ομάδα κακόβουλων κόμβων οι οποίοι συνεργάζονται για να επιφέρουν μεγαλύτερη ζημιά στο δίκτυο.

Wormhole attack

Ένας κακόβουλος κόμβος «ακούει» ένα μήνυμα που διατρέχει μια περιοχή του δικτύου και το αναπαράγει σε μια άλλη περιοχή αυτού με τη βοήθεια ενός άλλου κόμβου.

Επίθεση αόρατου κόμβου

Αυτή η επίθεση μπορεί να πραγματοποιηθεί από οποιονδήποτε κόμβο που βρίσκεται στο μονοπάτι δρομολόγησης. Μπορεί να θεωρηθεί ως μια επίθεση του τύπου *man-in-the-middle attack.* Η ζημιά που προκαλείται από αυτή την επίθεση περιορίζεται στους κόμβους του συγκεκριμένου μονοπατιού.

Rushing attack

Αυτή η επίθεση μπορεί να εφαρμοστεί εναντίον οποιουδήποτε πρωτοκόλλου το οποίο χρησιμοποιεί συναρτήσεις εντοπισμού και διόρθωσης διπλών πακέτων. Ο επιτιθέμενος αποστέλλει ένα πακέτο στον προορισμό (συνήθως πρόκειται για τον ενδιάμεσο κόμβο στο μονοπάτι) το οποίο το έχει διαμορφώσει έτσι ώστε να φαίνεται σαν διπλό πακέτο. Κατά συνέπεια, αυτό το πακέτο απορρίπτεται και άρα η πληροφορία που μετέφερε χάνεται.

ΚΕΦΑΛΑΙΟ 7
ΕΥΠΑΘΕΙΕΣ ΚΑΙ ΙΣΧΥΡΑ ΣΗΜΕΙΑ

7.1 Eavesdropping

[29] [30] [31] Μια σύνδεση Bluetooth χωρίς την εφαρμογή κρυπτογράφησης είναι πολύ εύκολο για κάποιον κακόβουλο χρήστη να υποκλέψει/ αντικαταστήσει το ωφέλιμο φορτίο. Βέβαια, ακόμα και όταν χρησιμοποιήσουμε κρυπτογράφηση της σύνδεσης δεν μπορούμε να είμαστε βέβαιοι για την ασφαλή μεταφορά των δεδομένων μας, καθώς με έναν έξυπνο χειρισμό των δεδομένων και του αντίστοιχου CRC μπορούν να στείλουν τα δικά τους δεδομένα στη θέση των αυθεντικών.

Θεωρούμε ότι ο επιτιθέμενος μπορεί εύκολα ή δύσκολα να απομονώσει το bit stream που παράγεται από την μηχανή κρυπτογράφησης. Το ερώτημα, όμως, που ζητάει απάντηση είναι το αν μπορεί να ανακτήσει το κλειδί κρυπτογράφησης. Για να γίνει αυτό, θα πρέπει ο επιτιθέμενος να ανακτήσει αρκετά κλειδιά ωφέλιμου φορτίου και εν συνεχεία με βάση αυτά να προσπαθήσει να ανακτήσει το K'_C . Με τον καθορισμό του K'_C , ο ωτακουστής μπορεί να «ακούσει» το κανάλι μετάδοσης που έχει δημιουργηθεί μεταξύ των δυο συσκευών, μέχρι το K'_C να ενημερωθεί ή μέχρι να πραγματοποιηθεί εξαρχής αμοιβαία αυθεντικοποίηση των συσκευών. Μια πολύ σημαντική παράμετρος είναι η χρονική διάρκεια της ανάκτησης του κλειδιού ωφέλιμου φορτίου. Αυτός ο χρόνος επηρεάζει άμεσα τον χρόνο καθορισμού του K'_C.

Από όταν οι προδιαγραφές του Bluetooth ανακοινώθηκαν, επιστήμονες ξεκίνησαν έρευνες με σκοπό την ανάλυση του αλγόριθμου E_0 και των επιθέσεων που γίνονται σε αυτόν. Κατέληξαν στο ότι οι επιθέσεις που γίνονται στον αλγόριθμο E_0 έχουν χρονική πολυπλοκότητα μικρότερη του $O(2^{128})$. Αυτό σημαίνει ότι έχουν μικρότερη πολυπλοκότητα από την εξαντλητική έρευνα στο σύνολο των κλειδιών. (Μια γενική ιδέα που χρησιμοποιούν μερικές από τις επιθέσεις αυτές είναι ο συσχετισμός και η αλγεβρική δομή που υπάρχει μεταξύ των εισερχόμενων και εξερχόμενων bits.)

Αυτή τη στιγμή δεν υπάρχει κάποια γνωστή επίθεση που να «σπάει» όλη τη διαδικασία κρυπτογράφησης χρησιμοποιώντας λογικά μέσα, δηλαδή την υπάρχουσα υπολογιστική ισχύ για ανεκτό χρόνο. Βέβαια, η κατάσταση θα τροποποιείται με το πέρας του χρόνου και την αύξηση της υπολογιστικής ισχύος που θα έχουν στα χέρια τους οι κακόβουλοι χρήστες. Έτσι, ενώ τώρα με την χρήση ενός προσωπικού υπολογιστή των 4 GHz για τον υπολογισμό 2^{49} πράξεων απαιτούνται 35 ώρες, μελλοντικά, ο χρόνος πρόκειται να μειωθεί αρκετά. Συνεπώς, δημιουργείται η ανάγκη για την χρησιμοποίηση ενός εναλλακτικού συστήματος κρυπτογράφησης.

7.2 Μεταμφίεση

Το κύριο πρόβλημα που δημιούργησε ο προηγούμενος τύπος επίθεσης είναι η κατάρριψη της εμπιστευτικότητας των αποστελλόμενων δεδομένων. Οι παραλήπτες εκτός της εμπιστευτικότητας, επιθυμούν να είναι σίγουροι ότι όντως λαμβάνουν δεδομένα από τον πραγματικό αποστολέα και όχι από κάποιον που τον παριστάνει. Ο κακόβουλος χρήστης έχει δυο επιλογές: είτε να μιμηθεί τον πραγματικό αποστολέα είτε να εισάγει / αντικαταστήσει το ωφέλιμο φορτίο που αποστέλλεται.

Φυσικά, τα πράγματα δεν είναι τόσο εύκολα. Η πρώτη επιλογή είναι ουσιαστικά αδύνατη, καθώς μέχρι στιγμής δεν υπάρχει κάποια επίθεση που να παρακάμπτει την πρόκληση αυθεντικοποίησης του Bluetooth. Άρα, ο μόνος τρόπος είναι η

τροποποίηση του ωφέλιμου φορτίου. Στην περίπτωση, που δεν έχει εφαρμοστεί κρυπτογράφηση, τότε η κατάσταση διευκολύνεται ακόμα περισσότερο για τον επιτιθέμενο. Αρκεί η προσεκτική τροποποίηση του CRC των πακέτων δεδομένων. Ακόμα και στην περίπτωση που έχουμε κρυπτογράφηση, χρησιμοποιείται η ίδια τεχνική καθώς πλέον έχουμε το άθροισμα του ωφέλιμου φορτίου με το κλειδί. Πρόκειται για μια γραμμική λειτουργία όπως είναι άλλωστε και ο υπολογισμός του CRC, άρα ο επιτιθέμενος μπορεί εύκολα να υπολογίσει πώς να τροποποιήσει το CRC για να ταιριάζει με τις τροποποιήσεις που έγιναν στα κρυπτογραφημένα δεδομένα. Πρέπει να σημειωθεί ότι ο μηχανισμός CRC σε συνδυασμό με την ενεργοποιημένη κρυπτογράφηση μπορεί να εντοπίσει μια τροποποίηση στα δεδομένα υπό την προϋπόθεση, όμως, ότι ο επιτιθέμενος δεν αναπροσαρμόζει τα CRC bits ή τα αλλάζει με τυχαίο τρόπο.

Ακόμα και όταν ο επιτιθέμενος τροποποιεί τυχαία το CRC, έχει μια πιθανότητα να το πράξει σωστά. Η πιθανότητα επιτυχίας ισούται με 2^{-16}, η οποία δεν μπορεί να θεωρηθεί και μικρή. Βέβαια, αυτή η διαδικασία επαναλαμβάνεται για κάθε πακέτο δεδομένων ξεχωριστά. Οπότε, το σύστημα αν ανιχνεύσει μεγάλο αριθμό λανθασμένων CRCs, μπορεί να εξάγει το συμπέρασμα ότι κάποιος κακόβουλος χρήστης προσπάθησε να τροποποιήσει τα μεταδιδόμενα πακέτα.

Συμπερασματικά, βλέπουμε ότι το ωφέλιμο φορτίο στο Bluetooth 1.1 μπορεί εύκολα να τροποποιηθεί. Βέβαια, έχοντας ενεργοποιημένη την κρυπτογράφηση, δεν μπορεί εύκολα ο επιτιθέμενος να πετύχει την τροποποίηση των δεδομένων και το μόνο που μπορεί να καταφέρει είναι να «αναστατώσει» την επικοινωνία (αν αυτός όμως είναι ο στόχος του τότε υπάρχουν και ευκολότεροι τρόποι να τον πετύχει). Ένα άλλο σοβαρό πρόβλημα για τους επιτιθέμενους είναι ότι δεν μπορούν να γνωρίζουν το είδος των δεδομένων που αποστέλλονται. Έτσι, μπορεί να αποστέλλονται δεδομένα σχετικά με υπηρεσίες χαμηλού / υψηλού επιπέδου κ.ά. Κατά συνέπεια, τα δεδομένα του τελικού χρήστη δύσκολα εντοπίζονται και αλλοιώνονται.

7.3 Ζευγάρωμα

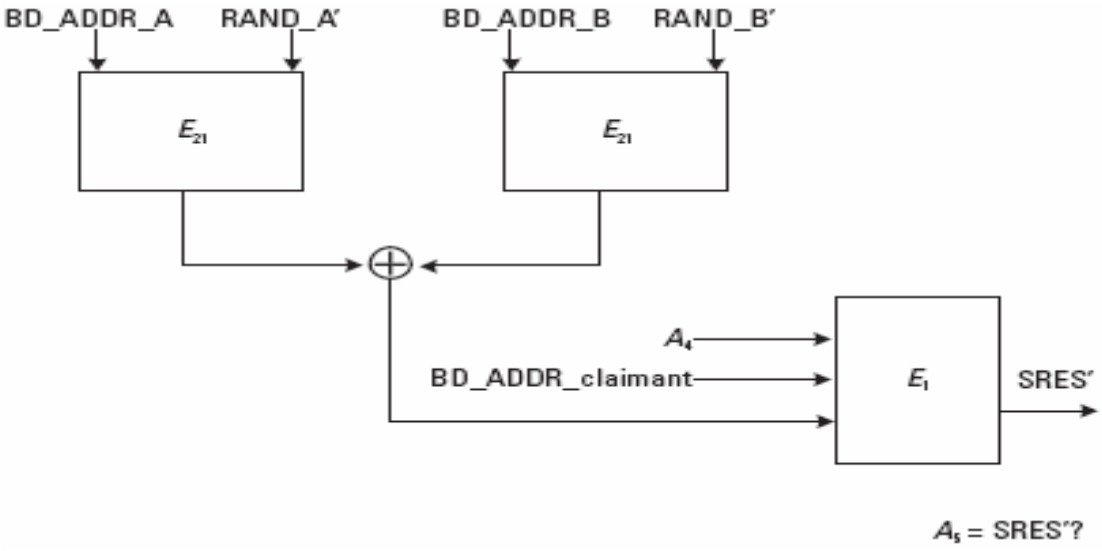
Στις προδιαγραφές του Bluetooth 1.1, έχει δοθεί ιδιαίτερη έμφαση στις επιθέσεις που έχουν ως στόχο τη διαδικασία ζευγαρώματος. Μια τέτοιου τύπου επίθεση μπορεί να πραγματοποιηθεί μόνο κατά τη διάρκεια της διαδικασίας ζευγαρώματος σε δημόσιο χώρο, η οποία συνήθως γίνεται μόνο μια φορά για κάθε ζεύγος. Σαφώς, όταν αναφερόμαστε στη διαδικασία ζευγαρώματος, αναφερόμαστε στη γέννηση του κλειδιού συνδυασμού ή του κλειδιού συσκευής. Επειδή, όμως τα κλειδιά συσκευής έχουν συγκεκριμένα προβλήματα ασφάλειας, θα αναφερθούμε σε αυτά παρακάτω σε ξεχωριστή ενότητα.

Ο υπολογισμός του κλειδιού συνδυασμού αναφέρθηκε αναλυτικά στην ενότητα 3.3. Κατά τη διαδικασία αυτή ανταλλάσσονται δεδομένα τα οποία μπορούν σχετικά εύκολα να ανακτηθούν από κάποιον κακόβουλο χρήστη. Έτσι, ο επιτιθέμενος μαθαίνει τις διευθύνσεις των δυο συσκευών, το IN_RAND καθώς και τις κρυπτογραφημένες τυχαίες τιμές $K_{INIT} \oplus LK\_RAND_A$, $K_{INIT} \oplus LK\_RAND_B$. Στη συνέχεια, πρέπει να μαντέψει το pass key το οποίο είναι η μόνη άγνωστη παράμετρος. Κάθε τιμή για το pass key, αντιστοιχεί σε διαφορετικό κλειδί σύνδεσης. Το επόμενο βήμα είναι ο έλεγχος ορθότητας του pass key ο οποίος για να πραγματοποιηθεί απαιτούνται πρόσθετα στοιχεία. Αυτά λαμβάνονται με την παρακολούθηση της ανταλλαγής του μηνύματος αυθεντικοποίησης, το οποίο έπεται

πάντα του link key calculation exchanges. Συνολικά, αποστέλλονται οι παρακάτω πέντε παράμετροι:

$$A_1 = IN\_RAND$$
$$A_2 = K_{INIT} \oplus LK\_RAND_A$$
$$A_3 = K_{INIT} \oplus LK\_RAND_B$$
$$A_4 = AU\_RAND$$
$$A_5 = SRES$$

Στη συνέχεια και με βάση τις προαναφερθέντες παρατηρήσεις, ο επιτιθέμενος μπορεί να μαντέψει την τιμή του PKEY'. Για να ελέγξει την ορθότητα, ακολουθεί τη διαδικασία του σχήματος που έχει ως αποτέλεσμα το SRES'. Ελέγχει το SRES με το SRES' και αποφαίνεται. Αν οι τιμές είναι ίσες τότε η μαντεψιά ήταν σωστή. Εάν,



Εικόνα 7-1 Επίθεση στο pass-key κατά τη διαδικασία ζευγαρώματος

όμως, το SRES' < SRES, ο επιτιθέμενος γνωρίζει ότι με κάποιες κινήσεις ακόμα μπορεί να επιτύχει. Αν το μήκος του pass key είναι μικρό τότε ο επιτιθέμενος μπορεί να δοκιμάσει διαδοχικά όλες τις πιθανές τιμές μέχρι να πετύχει την ταύτιση του SRES' με το SRES. Το συμπέρασμα είναι ότι τα μικρού μήκους pass key δεν προστατεύουν τους χρήστες από έναν ενδιάμεσο κατά το «ζευγάρωμα».

Το πρόβλημα του μικρού μήκους pass key είναι το σημαντικότερο σημείο ευπάθειας του Bluetooth (μαζί με τα προβλήματα του κλειδιού συσκευής και των επιθέσεων ιδιωτικότητας). Η προτεινόμενη λύση σε αυτή την ευπάθεια είναι φυσικά η χρήση όσο το δυνατόν μεγαλύτερου μήκους pass key.

7.4 Ακατάλληλη αποθήκευση κλειδιού

Αναφερθήκαμε στο τέλος του τρίτου κεφαλαίου στον τρόπο με τον οποίο αποθηκεύονται τα κλειδιά σε μια βάση δεδομένων. Σε αυτή την ενότητα, θα παρουσιαστούν μερικά προβλήματα που δημιουργούνται λόγω της λανθασμένης αποθήκευσης σε αυτή τη βάση.

7.4.1 Αποκάλυψη των κλειδιών

Εάν ένα μυστικό κλειδί αποκαλυφθεί σε κάποιον κακόβουλο χρήστη, υπάρχει ένας εμφανής κίνδυνος να γίνει μια επίθεση μεταμφίεσης. Για αυτό το λόγο, η βάση δεδομένων πρέπει να είναι αναγνώσιμη μόνο από το νόμιμο ιδιοκτήτη.

Στην περίπτωση των μικρών προσωπικών συσκευών όπως είναι τα hands-free και τα κινητά τηλέφωνα, ο κίνδυνος της απώλειας ενός κλειδιού είναι αρκετά μικρός. Αυτό οφείλεται στη δυσκολία τόσο της πρόσβασης στην μνήμη της συσκευής καθώς απαιτείται χρήση ειδικού εξοπλισμού, όσο και της ανάγνωσης της μνήμης λόγω της απουσίας κάποιου καλά δομημένου συστήματος αρχείων. Για πιο πολύπλοκες συσκευές, ο κίνδυνος αυξάνεται. Χαρακτηριστικό παράδειγμα είναι ένας προσωπικός υπολογιστής συνδεδεμένος σε δίκτυο το οποίο χρησιμοποιεί ένα USB dongle για συγχρονισμό ενός κινητού τηλεφώνου (δηλαδή για ανανέωση των στοιχείων του κινητού σύμφωνα με αυτά που υπάρχουν στον υπολογιστή). Γίνεται κατανοητό ότι αν η βάση δεδομένων των κλειδιών είναι αποθηκευμένη σε μορφή απλού κειμένου τότε ο καθένας μπορεί να αποκτήσει πρόσβαση σε αυτή άμεσα (μέσω του ίδιου του υπολογιστή) ή έμμεσα (μέσω απομακρυσμένης σύνδεσης).

Μια παραλλαγή αυτής της επίθεσης είναι η χρήση ενός ειδικού USB dongle που θα αντικαθιστά το υπάρχον και θα έχει ως σκοπό την εξαγωγή των κλειδιών σύνδεσης από τη βάση δεδομένων που βρίσκεται αποθηκευμένη στον ηλεκτρονικό υπολογιστή. Μόλις συνδεθεί η «ψεύτική» συσκευή τότε αποστέλλει ένα *Link Key Request.*Με αυτό τον τρόπο προσπαθεί να ανακτήσει το κλειδί σύνδεσης με μια συγκεκριμένη συσκευή (στην αίτηση υπάρχει ως όρισμα η διεύθυνση της συσκευής). Αν υπάρχει, λοιπόν, σχετική εγγραφή επιστρέφεται το γεγονός *HCI Link Key Request Negative Reply*. Αυτή η διαδικασία, προφανώς, μπορεί να επαναληφθεί όσες φορές επιθυμεί ο επιτιθέμενος με στόχο να ανακτήσει όσο το δυνατόν περισσότερα κλειδιά σύνδεσης.

Αν η βάση δεδομένων αποθηκεύεται στο dongle και όχι στον ηλεκτρονικό υπολογιστή τότε η επίθεση πραγματοποιείται με παρόμοιο τρόπο. Αρκεί ο επιτιθέμενος να αποσυνδέσει το dongle από τον host και να το συνδέσει στον υπολογιστή του. Τότε, αποστέλλει με την χρήση μιας εφαρμογής, το αίτημα *HCI Read Stored Link Key* και αναμένει να του επιστραφεί η λίστα με τα αποθηκευμένα κλειδιά μέσω του γεγονότος *Return Link Keys.* Μόλις ολοκληρωθεί η διαδικασία, το dongle επιστρέφεται στη θέση του.

Ένας άλλος τύπος επίθεσης πραγματοποιείται με την χρήση κακόβουλου (malicious) λογισμικού. Έτσι, με την χρήση ενός Trojan horse μπορούμε να αποκτήσουμε πρόσβαση στη βάση δεδομένων και να την αποστείλουμε σε μια απομακρυσμένη τοποθεσία από την οποία αργότερα θα την ανακτήσουμε. Με παρόμοιο τρόπο, μπορούν να χρησιμοποιηθούν προγράμματα-ιοί και worms. Ουσιαστικά, αυτά τα προγράμματα μόλις εκτελεστούν ψάχνουν για ηλεκτρονικούς υπολογιστές που έχουν τη δυνατότητα σύνδεσης με άλλες συσκευές μέσω της αρχιτεκτονικής Bluetooth.

7.4.2 Παραποιώντας τα κλειδιά

Ένας πιθανός τρόπος για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση ένας χρήστης είναι η προσθήκη στη βάση δεδομένων των κλειδιών μιας εγγραφής ενός νέου κλειδιού σύνδεσης. Όταν μια συσκευή δεχτεί αίτηση σύνδεσης από την συσκευή του επιτιθέμενου τότε ο διαχειριστής σύνδεσης θα ελέγξει τη βάση δεδομένων του

και θα διαπιστώσει (λανθασμένα βέβαια) ότι έχει επικοινωνήσει ξανά με αυτή τη διεύθυνση. Στην περίπτωση που η συσκευή έχει οριστεί ως έμπιστη τότε ο επιτιθέμενος μπορεί να αποκτήσει απεριόριστη πρόσβαση στις προσφερόμενες υπηρεσίες , πχ θα μπορεί να πάρει κάποιο τηλέφωνο μέσω του κινητού τηλεφώνου.

Οι μικρές συσκευές (πχ κινητά τηλέφωνα) δεν είναι τόσο ευαίσθητες σε αυτές τις επιθέσεις καθώς οι βάσεις δεδομένων τους είναι αρκετά πολύπλοκες. Από την άλλη μεριά, οι ηλεκτρονικοί υπολογιστές είναι ο πιο συνηθισμένος στόχος. Θα πρέπει να αποφεύγεται, βέβαια, η πρόσβαση για εγγραφή σε μη εξουσιοδοτημένους χρήστες. Μια πρακτική που θα βελτίωνε αρκετά την κατάσταση θα ήταν η κρυπτογράφηση της βάσης δεδομένων και γενικότερα η περαιτέρω προστασία της.

7.4.3 Άρνηση παροχής υπηρεσίας

Ο επιτιθέμενος έχει διάφορες επιλογές για να πραγματοποιήσει μια επίθεση. Όμως, αν σβήσει κάποια εγγραφή, αφαιρέσει ένα ή περισσότερα κλειδιά ή καταστρέψει κάποια δεδομένα τότε αυτή του η παρέμβαση θα εντοπιστεί. Οι προδιαγραφές του Bluetooth δεν αναφέρουν τον τρόπο με τον οποίο πρέπει να αντιδράσουν οι συσκευές σε περίπτωση καταστροφής της βάσης δεδομένων τους. Μια προσιτή λύση θα ήταν η ενημέρωση του χρήστη με ένα επεξηγηματικό μήνυμα και εν συνεχεία η επανεκκίνηση της διαδικασίας του «ζευγαρώματος».

Βέβαια, ένας επιτιθέμενος που γνωρίζει τη δομή της βάσης μπορεί να αποφύγει την ανίχνευση των αλλαγών, τροποποιώντας κατάλληλα το κλειδί και το σχετικό CRC αν υπάρχει. Έτσι, το σφάλμα δεν θα ανιχνευθεί μέχρι να αποτύχει η αυθεντικοποίηση οπότε και η συσκευή ματαιώνει τη σύνδεση και αποστέλλει την εντολή *LMP detach PDM* συνοδευόμενη από τον κωδικό του σφάλματος. Για να αποφευχθεί το φαινόμενο των επανειλημμένων προσπαθειών σύνδεσης, ο διαχειριστής σύνδεσης της συσκευής δεν επιτρέπει νέες προσπάθειες αυθεντικοποίησης για ένα ορισμένο χρονικό διάστημα, το οποίο σε κάθε αποτυχία αυξάνεται εκθετικά.

Μια λύση σε αυτό το πρόβλημα είναι η εφαρμογή μεγαλύτερης προστασίας της βάσης δεδομένων. Ουσιαστικά, χρησιμοποιούνται περισσότερα bits ισοτιμίας τα οποία σχηματίζουν τον κώδικα επαλήθευσης μηνυμάτων (message authentication code) της αποθηκευμένης πληροφορίας στη βάση. Ο επιτιθέμενος, πλέον, έχει μια πολύ μικρή πιθανότητα να τροποποιήσει την πληροφορία χωρίς να ανιχνευθεί.

7.5 Κλειδί Συσκευής

Η περίπτωση της χρήσης ενός κλειδιού συσκευής δεν διαφέρει αρκετά από αυτή του κλειδιού συνδυασμού καθώς και σε αυτό χρησιμοποιούνται παρόμοιοι μηχανισμοί αυθεντικοποίησης και κρυπτογράφησης. Όμως, η κύρια διαφορά, η οποία είναι και αυτή που δημιουργεί την ευπάθεια στο σύστημα, είναι ότι η συσκευή που χρησιμοποιεί αυτόν τον τύπο κλειδιού, μπορεί να χρησιμοποιεί μόνο ένα κλειδί για όλες τις ασφαλείς συνδέσεις της. Αυτό σημαίνει ότι θα πρέπει να διαμοιράζεται το κλειδί με τις έμπιστες συσκευές. Άρα, αν ένας ωτακουστής μπει ενδιάμεσα μιας έμπιστης επικοινωνίας τότε μπορεί να ανακτήσει το κλειδί και να το χρησιμοποιήσει στη συνέχεια για τους κακόβουλους σκοπούς του. Δηλαδή, συμπεραίνουμε ότι σε περιπτώσεις χρήσης κλειδιού συσκευής, δεν μπορούμε να προστατευτούμε από επιθέσεις που προέρχονται από έμπιστες συσκευές. Οι ευπάθειες αυτές έχουν

αναγνωριστεί επίσημα από το Bluetooth SIG και αποτέλεσμα αυτού ήταν η μη-χρησιμοποίηση του από την έκδοση των τελευταίων προδιαγραφών.

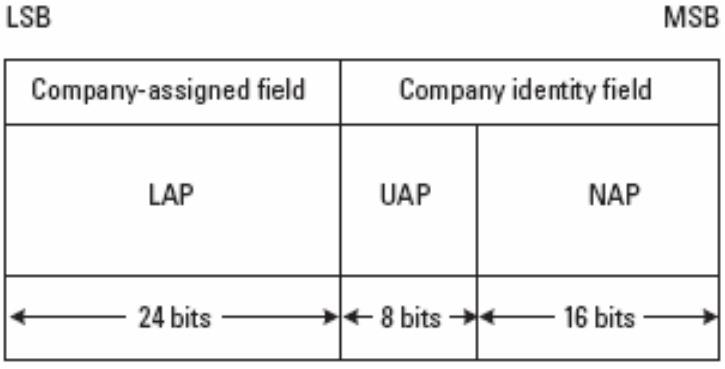
7.6 Εντοπισμός θέσης

Οι χρήστες που χρησιμοποιούν ασύρματα δίκτυα αλλάζουν πολύ συχνά τοποθεσία. Φυσικά, αυτό το στοιχείο επιθυμούν να μην γίνεται γνωστό σε μη έμπιστους χρήστες. Έτσι, είναι πολύ σημαντικό να εξασφαλιστεί η μυστικότητα της τοποθεσίας που βρίσκονται. Το πρόβλημα αυξάνεται αν σκεφτούμε ότι η τοποθεσία μπορεί να εντοπιστεί πολύ εύκολα καθώς το Bluetooth υπάρχει ενσωματωμένο σε πολλές συσκευές, όπως είναι PDAs, κινητά και φορητοί υπολογιστές, και κατά συνέπεια ο οποιοσδήποτε μπορεί να κινείται και να προσπαθεί να εντοπίσει συσκευές με πιθανά αδύνατα σημεία. Το στοιχείο που αρχικά εντοπίζεται και καταγράφεται σε μια συσκευή είναι η διεύθυνση της ή ένα ψευδώνυμο που χρησιμοποιείται σε ορισμένες περιπτώσεις για λόγους φιλικότητας.

Για να αποφύγουμε τον εντοπισμό της τοποθεσίας μιας συσκευής, απαιτείται η ύπαρξη μιας κατάστασης ανωνυμίας. Ουσιαστικά, αυτό που συμβαίνει σε αυτή την περίπτωση είναι ότι οι συσκευές αλλάζουν σε τακτά χρονικά διαστήματα την διεύθυνσή τους.

7.6.1 Διεύθυνση συσκευής και εντοπισμός θέσης

Όπως αναφέρθηκε και προηγουμένως, το στοιχείο που δέχεται ουσιαστικά την επίθεση σε μια τέτοια κατάσταση είναι η διεύθυνση της συσκευής. Άρα, αρχικά θα πρέπει να εξετάσουμε από τι αποτελείται αυτή. Έχει μήκος 48 bits και διαχωρίζεται σε τρία διακριτά μέρη : το lower address part, upper address part (UAP) και το nonsignificant address part (NAP).



Εικόνα 7-2 Μορφή της διεύθυνση μιας Bluetooth συσκευής

Ολόκληρη η διεύθυνση αποστέλλεται κατά την διάρκεια του συγχρονισμού της αναπήδησης συχνότητας (frequency hop synchronization). Αυτό το γεγονός μπορεί να χρησιμοποιηθεί σε διάφορους τύπους επιθέσεων. Φυσικά, αυτή η ευπάθεια δεν περιορίζεται στην περίπτωση που έχουμε ολόκληρη τη διεύθυνση καθώς οποιοδήποτε κομμάτι μιας σταθερής διεύθυνσης συσκευής μπορεί να χρησιμοποιηθεί για τον ίδιο σκοπό. Σε αυτή την περίπτωση, συγκαταλέγονται οι κώδικες πρόσβασης του Bluetooth (Bluetooth Access Codes). Αυτοί οι κώδικες σχηματίζουν το πρώτο μέρος κάθε μεταδιδόμενου πακέτου. Υπάρχουν τρεις διακριτοί κωδικοί πρόσβασης:

1. CAC, προέρχεται από το LAP της κύριας συσκευής
2. DAC (Device Access Code), προέρχεται από το LAP της συσκευής – πελάτη.
3. IAC (Inquiry Access Code)

7.6.2 Πέντε διαφορετικοί τύπου επιθέσεων

Επίθεση αναζήτησης πληροφοριών

[32] [33] Σε αυτό τον τύπο επίθεσης, ο επιτιθέμενος έχει οργανώσει ένα δίκτυο με συσκευές Bluetooth σε μια ορισμένη περιοχή. Αυτό είναι αρκετά εύκολο να πραγματοποιηθεί λόγω του μικρού κόστους των συσκευών Bluetooth. Υποθέτοντας ότι το θύμα έχει αφήσει την συσκευή του σε ορατή κατάσταση τότε μπορεί ο επιτιθέμενος πολύ εύκολα να εντοπίσει την ταυτότητά του και γενικότερα να καταγράψει σε μια λίστα όλες τις συσκευές που υπάρχουν στον χώρο.

Επίθεση παρακολούθησης κίνησης

Σε αυτή την περίπτωση ο επιτιθέμενος απλά παρακολουθεί την επικοινωνία μεταξύ δυο συνδεδεμένων έμπιστων συσκευών. Αυτές οι συσκευές επικοινωνούν χρησιμοποιώντας τον κωδικό πρόσβασης CAC ο οποίος προέρχεται από την κύρια συσκευή του piconet. Με αυτό τον τρόπο, ο επιτιθέμενος μπορεί να εντοπίσει την κύρια συσκευή του δικτύου απλά παρακολουθώντας την επικοινωνία. Με παρόμοιο τρόπο και χρησιμοποιώντας το DAC αυτή τη φορά μπορούμε να εντοπίσουμε οποιαδήποτε άλλη συσκευή-πελάτη που υπάρχει στο δίκτυο.

Επιπλέον, υπάρχει η δυνατότητα να προσδιοριστεί η ταυτότητα μιας συσκευής παρακολουθώντας τα FHS πακέτα / DAC. Βέβαια, δεν είναι τόσο ισχυρή αυτή η επίθεση επειδή η αποστολή αυτών των πακέτων πραγματοποιείται μόνο κατά την αρχικοποίηση της σύνδεσης των δυο συσκευών. Πρέπει να σημειωθεί ότι αυτή η επίθεση μπορεί να πραγματοποιηθεί με επιτυχία ακόμα και αν η συσκευή δεν είναι σε ορατή κατάσταση.

Επίθεση αναζήτησης συσκευής

Αυτός ο τύπος επίθεσης χρησιμοποιείται από τον επιτιθέμενο για να μάθει αν μια συσκευή με συγκεκριμένη διεύθυνση ή DAC βρίσκεται εντός της περιοχής του. Η επίθεση προϋποθέτει ότι η συσκευή θα είναι ορατή. Αυτό που κάνει στην πράξη αυτή η επίθεση είναι ένα είδος ping. Δηλαδή, «στοχεύει» την συσκευή και αναμένει απάντηση. Μόλις την λάβει δεν απαντάει, οπότε η συσκευή κάνει time out την επικοινωνία με αποτέλεσμα το συμβάν να μην καταγράφεται και να μην μεταφέρεται στο στρώμα λογισμικού.

Επίθεση φιλικού προς τον χρήστη ονόματος

Πολλές φορές οι συσκευές για λόγους ευκολίας και ευχρηστίας παρέχουν τη δυνατότητα χρήσης ενός ψευδωνύμου αντί μιας διεύθυνσης (χωρίς αυτό να σημαίνει ότι καταργείται αυτή). Έτσι, αυτό το ψευδώνυμο μπορεί να ανακτηθεί πολύ εύκολα από κάποιον κακόβουλο χρήστη, χρησιμοποιώντας απλά την εντολή *LMP name req*,

ο οποίος στη συνέχεια να το χρησιμοποιήσει για να διευκολύνει την επίθεση εντοπισμού τοποθεσίας της συσκευής.

7.7 Σφάλματα στην υλοποίηση

Ένας πολύ σημαντικός παράγοντας που μπορεί να επηρεάσει την ασφάλεια ενός συστήματος είναι η υλοποίηση. Έτσι, έχουν παρατηρηθεί φαινόμενα κατά τα οποία είχαμε ένα σύστημα ασφαλείας άρτια οργανωμένο και υλοποιημένο όμως η υλοποίηση του υπόλοιπου συστήματος, άφηνε κενά δημιουργώντας τις προϋποθέσεις για να δράσει ένας κακόβουλος χρήστης. Το Bluetooth δεν θα μπορούσε να ξεφύγει από αυτόν τον κανόνα.

Κύριος στόχος των κατασκευαστών είναι η ευχρηστία και η λειτουργικότητα ενός συστήματος. Αυτό σημαίνει όμως ότι παραμελούν πολλές φορές τους ελέγχους για ζητήματα ασφάλειας, οι οποίοι τελικά περιλαμβάνουν μόνο τα βασικά σημεία όπως είναι πιο συγκεκριμένα για την περίπτωσή μας οι λειτουργίες του ζευγαρώματος, της αυθεντικοποίησης κλπ. Πολλά άλλα ζητήματα που δεν περνάνε από έλεγχο, ξεχνιούνται και κατά συνέπεια γίνονται σημεία ευπάθειες προς εκμετάλλευση από κακόβουλους χρήστες.

Πρόσφατα, έγιναν αναφορές για ορισμένες ευπάθειες οι οποίες οφείλονται καθαρά σε σφάλματα υλοποίησης και επιβεβαιώθηκαν από εταιρείες κινητής τηλεφωνίας. Παρακάτω, θα αναφερθούν μερικές από αυτές τις επιθέσεις :

- Snarf attack [34]: ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση στα δεδομένα και τις υπηρεσίες μιας Bluetooth – enabled συσκευής χωρίς την συγκατάθεση του ιδιοκτήτη της.

- Backdoor attack: μοιάζει πολύ με την προηγούμενη επίθεση μόνο που σε αυτή την περίπτωση αρχικά υλοποιείται μια σύνδεση εμπιστοσύνης με την συσκευή. Τότε, ο επιτιθέμενος διαγράφει την εγγραφή από την λίστα της με τις συνδεδεμένες συσκευές αφήνοντας όμως ανέπαφη την βάση δεδομένων των κλειδιών σύνδεσης. Έτσι, μπορεί μελλοντικά να συνδεθεί με την επιθυμητή συσκευή και να αποκτήσει πρόσβαση σε δεδομένα και υπηρεσίες χωρίς την συγκατάθεση του χρήστη.

- Bluejacking: αυτός ο όρος χρησιμοποιείται όταν αποστέλλονται αυτόκλητα μηνύματα σε μια συσκευή Bluetooth. Αυτό που γίνεται στην πραγματικότητα είναι η αντικατάσταση του πεδίου ονόματος μιας εγγραφής του τηλεφωνικού καταλόγου ή της business card που αποστέλλεται στη συσκευή, με ένα μήνυμα. Έτσι, με την λήψη του αντικειμένου συνήθως εμφανίζεται το πεδίο του ονόματος με μια ερώτηση για το αν θέλει ο χρήστης να αποθηκευτεί. Παρόλο που είναι ενοχλητικό, δεν αποτελεί όμως πρόβλημα ασφαλείας για τις συσκευές καθώς δεν τροποποιεί δεδομένα ούτε μπορεί να αποκτήσει πρόσβαση ο κακόβουλος χρήστης σε κάποιες υπηρεσίες.

- Sibyl Attacks [35] [36] [37] [38]: Τα μεγάλα peer-to-peer συστήματα αντιμετωπίζουν απειλές ασφαλείας από ψευδή ή εχθρικά απομακρυσμένα στοιχεία υπολογιστών. Για να αντιμετωπιστούν αυτές οι απειλές, πολλά συστήματα έχουν περίσσεια πόρων. Ωστόσο, αν μία μοναδική οντότητα

μπορεί να παρουσιάζεται με πολλαπλές ταυτότητες, τότε μπορεί να ελέγξει ένα μεγάλο μέρος του συστήματος και ως εκ τούτου να μειώσει τους πόρους του συστήματος. Μια προσέγγιση για να αντιμετωπίσουμε αυτές τις "Sybil attacks" είναι να έχουμε μια έμπιστη υπηρεσία που να πιστοποιεί τις ταυτότητες. Χωρίς αυτή την κεντρικοποιημένη αρχή, οι sibyl επιθέσεις είναι πάντα πιθανές.

Είναι γεγονός πως είναι πρακτικά αδύνατο σε ένα κατανεμημένο υπολογιστικό περιβάλλον για ένα αρχικά άγνωστο υπολογιστικό στοιχείο να εμφανίσει ξεχωριστές ταυτότητες. Χωρίς μια κεντρική, έμπιστη αρχή να επιβεβαιώνει την ένα προς ένα αντιστοίχηση οντότητας και ταυτότητας, είναι πιθανό για μια άγνωστη οντότητα να εμφανίσει παραπάνω από μια ταυτότητες.

Αν η τοπική οντότητα δεν έχει απ' ευθείας φυσική γνώση των απομακρυσμένων οντοτήτων, τις αντιλαμβάνεται μόνο ως πληροφοριακές μονάδες που τις ονομάζουμε ταυτότητες. Το σύστημα πρέπει να εξασφαλίσει ότι η κάθε ταυτότητα αναφέρεται σε διαφορετική οντότητα. Διαφορετικά, όταν η τοπική οντότητα επιλέξει ένα υποσύνολο από ταυτότητες για να εκτελέσουν μια λειτουργία, αυτή μπορεί να ξεγελαστεί επιλέγοντας μια απομακρυσμένη οντότητα αλλά πολλαπλές φορές και έτσι να μειωθεί η περίσσεια πόρων του συστήματος.

Η πλαστογράφηση, λοιπόν, πολλαπλών ταυτοτήτων σε ένα σύστημα έχοντας ένα σύνολο οντοτήτων που αντιπροσωπεύεται από ένα μεγαλύτερο σύνολο ταυτοτήτων ονομάζεται *Sybil attack*. Ο σκοπός μιας τέτοιας επίθεσης είναι να εκβιάσει μια δυσανάλογη κατανομή των πόρων του συστήματος.

Η αντιμετώπιση των επιθέσεων τέτοιου τύπου βρίσκεται στην ύπαρξη κεντρικού μηχανισμού που να πιστοποιεί τη μοναδική ταυτότητα της κάθε οντότητας. Συγκεκριμένα στο Bluetooth, μία προτεινόμενη λύση θα ήταν η ύπαρξη της υπηρεσίας πιστοποίησης ταυτοτήτων στον διαχειριστή ασφαλείας της κύριας συσκευής. Αυτός θα ελέγχει αν η BD_ADDR αντιστοιχεί σε μία και μοναδική ταυτότητα.

ΚΕΦΑΛΑΙΟ 8
ΟΔΗΓΟΙ ΧΡΗΣΕΩΣ ΤΩΝ ΠΡΟΓΡΑΜΜΑΤΩΝ hcitool ΚΑΙ redfang

8.1 HciTool

Πρόκειται για ένα πρόγραμμα με το οποίο δίδεται η δυνατότητα σύνδεσης δυο Bluetooth – enabled συσκευών. Παρέχει πληθώρα παραμέτρων οι οποίοι θα αναλυθούν με παραδείγματα παρακάτω. Γενικά, η δομή της εντολής αυτής είναι η παρακάτω [39]:

hcitool [-h]
hcitool [-i <hciX>] [εντολή [παράμετροι εντολής]]

Παράμετροι

- dev : εμφανίζει τις τοπικές συσκευές που ανακαλύφθηκαν

```
[xaris@localhost ~]$ hcitool dev
Devices:        hci0    00:0B:0D:32:3A:9C
```

- inq : πραγματοποιεί έρευνα για απομακρυσμένες συσκευές. Για κάθε συσκευή που ανακαλύφθηκε, εμφανίζονται η διεύθυνση της συσκευής, το clock offset και η κλάση της, η οποία ορίζει τον τύπο της συσκευής και της υπηρεσίας σε δεκαεξαδική μορφή.

```
[xaris@localhost ~]$ hcitool inq
Inquiring ...
00:11:9F:74:EF:19       clock offset: 0x6dbf    class: 0x50020c
```

- Scan : πραγματοποιεί έρευνα για απομακρυσμένες συσκευές. Η διαφορά της με την inq είναι ότι εμφανίζει απλά την διεύθυνση της συσκευής.

```
[xaris@localhost ~]$ hcitool scan
Scanning ...        00:11:9F:74:EF:19       Hapagan
```

- Name <bdaddr> : εμφανίζει το ψευδώνυμο της συσκευής της οποίας η διεύθυνση δηλώνεται ως όρισμα.

```
[xaris@localhost ~]$ hcitool name 00:11:9F:74:EF:19
Hapagan
```

- Info <bdaddr> : τυπώνει το ψευδώνυμο της συσκευής, την έκδοση και τις υποστηριζόμενες υπηρεσίες της απομακρυσμένης συσκευής με διεύθυνση bdaddr.
- Cmd <ogf> <ocf> [παράμετροι] : υποβάλλει μια HCI εντολή στην τοπική Bluetooth συσκευή. Οι παράμετροι της εντολής παίρνουν δεκαεξαδικές τιμές.
- Con : εμφανίζει τις ενεργές συνδέσεις.
- Cc [--role=m|s] [--pkt-type=<ptype>] <bdaddr> : δημιουργεί μια σύνδεση με μια απομακρυσμένη συσκευή με διεύθυνση bdaddr. Η παράμετρος –pkt-type ορίζει μια λίστα με τους επιτρεπόμενους τύπους πακέτων που μπορούν να αποσταλούν. <ptype> είναι η λίστα η οποία περιέχει τις επιτρεπόμενες τιμές χωρισμένες με κόμματα. Οι αποδεκτοί τύποι πακέτων είναι οι εξής: DM1, DM3, DM5, DH1, DH3, DH5, HV1, HV2 και HV3. Η αρχική επιλογή είναι να επιτρέπονται όλοι οι τύποι πακέτων. Η παράμετρος –role μπορεί να πάρει δυο τιμές : m ή s. Η πρώτη ορίζει ότι η συσκευή δεν μπορεί να αλλάξει ρόλο κατά την διάρκεια της επικοινωνίας και παραμένει στον ρόλο του master. Ενώ, η δεύτερη δίνει τη δυνατότητα στην συσκευή να γίνει slave αν η έταιρη συσκευή απαιτεί να γίνει master.
- Dc <bdaddr> : με αυτή την εντολή τερματίζεται η σύνδεση που έχει δημιουργηθεί με την συσκευή με διεύθυνση bdaddr.
- Sr <bdaddr> <role> : τροποποιούμε τον ρόλο της απομακρυσμένης συσκευής με διεύθυνση bdaddr σε role, δηλαδή ή master ή slave.
- Cpt <bdaddr> <packet types> : αλλάζει την λίστα με τους επιτρεπόμενους τύπους πακέτων. Η νέα λίστα ορίζεται μέσω της παραμέτρου packet types που δεν είναι κάτι άλλο από μια λίστα με τύπους χωρισμένους με κόμματα.
- Rssi <bdaddr> : εμφανίζει πληροφορίες για το σήμα της σύνδεσης με την συσκευή με διεύθυνση bdaddr.
- Lq <bdaddr> : εμφανίζει την ποιότητα της σύνδεσης με την συσκευή με διεύθυνση bdaddr.
- Tpl <bdaddr> [type] : εμφανίζει το επίπεδο της ισχύος μετάδοσης για την σύνδεση με την συσκευή με διεύθυνση bdaddr.Η παράμετρος type μπορεί τιμές 0 ή 1. Με την τιμή 0 αναφερόμαστε στην τρέχουσα τιμής της ισχύος μετάδοσης ενώ με την τιμή 1 για την μέγιστη τιμή.
- Afh <bdaddr> : εμφανίζει τον χάρτη των AFH καναλιών για τη σύνδεση με την συσκευή με διεύθυνση bdaddr.
- Lst <bdaddr> [value] : όταν η παράμετρος value δεν παίρνει κάποια τιμή τότε εμφανίζεται το link supervision timeout για τη σύνδεση με την συσκευή με διεύθυνση bdaddr. Αλλιώς, η τιμή της παραμέτρου δίνεται σε αυτή του timeout.
- auth <bdaddr> : απαιτεί την ύπαρξη αυθεντικοποίησης για την συσκευή με διεύθυνση bdaddr.
- Enc <bdaddr> [encrypt enable] : ενεργοποιεί ή απενεργοποιεί την κρυπτογράφηση για την συσκευή με διεύθυνση bdaddr.
- Key <bdaddr> : αλλάζει το κλειδί σύνδεσης για την συσκευή με διεύθυνση bdaddr.

Δημιουργία δικτύου δυο συσκευών

Έστω ότι έχουμε δυο υπολογιστές, Η1 και Η2, που θέλουμε να δικτυώσουμε. Έχουν διευθύνσεις Bluetooth bdaddr1 και bdaddr2. Θεωρούμε ότι στο δίκτυό μας αυτοί οι υπολογιστές θα έχουν τις εξής IP: Η1 → 192.168.1.3 και Η2 → 192.168.1.4.

Για τη δημιουργία του δικτύου χρησιμοποιούμε το πρόγραμμα pand (personal area networking). Παρακάτω, αναλύονται οι εντολές που θα πρέπει να εισαχθούν από τον χρήστη root του συστήματος. Σημειώνεται ότι αναφερόμαστε πάντα προς το σύστημα Bluetooth και δεν ασχολούμαστε στο παρών παράδειγμα με την εντολή ip.

Εκτελούμε την εντολή *pand –s* στον H1 έτσι ώστε να εκκινηθεί σε αυτόν το πρόγραμμα pand. Έτσι, μπορούμε να δημιουργήσουμε μια σύνδεση από τον H2 στον H1 με την εντολή *pand –c bdaddr1*. Πλέον, αν εκτελέσουμε την εντολή *ip link show* σε έναν από τους κόμβους τότε θα πάρουμε ως αποτέλεσμα κάτι σαν το παρακάτω:

```
bnep0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
 link/ether 00:12:34:56:89:90 brd ff:ff:ff:ff:ff:ff
```

Φυσικά, αντί για 00:12:34:56:89:90 θα δούμε τη διεύθυνση bdaddr1 ή bdaddr2 ανάλογα σε ποιον υπολογιστή εκτελέσαμε την εντολή. Το μόνο που μένει πλέον είναι να αντιστοιχήσουμε αυτό το interface σε μια IP. Αυτό μπορεί να γίνει στον H1 εκτελώντας τις παρακάτω εντολές:

```
ip addr add 192.168.1.3/24 dev bnep0
ip link set bnep0 up
```

Ή στον H2:

```
ip addr add 192.168.1.4/24 dev bnep0
ip link set bnep0 up
```

Έτσι, μπορεί ο H2 να αποκτήσει πρόσβαση στον H1 μέσω της IP 192.168.1.3. Θεωρώντας ότι ο H2 τρέχει έναν sshd τότε μπορεί ο H1 να έχει πρόσβαση στον H2 μέσω της εντολής *ssh 192.168.1.4.*

8.2 Redfang

Αυτό το πρόγραμμα χρησιμοποιείται με σκοπό να ανακαλύψει όλες τις συσκευές Bluetooth που υπάρχουν στην περιοχή μας ακόμα και αυτές που έχουν οριστεί ως μη ανιχνεύσιμες [40] [41] [42]. Η τεχνική που χρησιμοποιείται, είναι η εξής: το πρόγραμμα κάνει αιτήσεις σε όλες τις πιθανές διευθύνσεις (BD_ADDR) και μόλις λάβει απάντηση εκτυπώνει τα στοιχεία της συσκευής. Με αυτό τον τρόπο, μπορεί να εντοπίσει και συσκευές που μπορεί να είναι μη ανιχνεύσιμες. Μπορείτε να δείτε τον πηγαίο κώδικα του προγράμματος στο Παράρτημα Α. Γενικά, συντάσσεται ως εξής: *fang [επιλογές]*.

Επιλογές

- -r <range> : ο χρήστης ορίζει ένα συγκεκριμένο πεδίο τιμών διευθύνσεων στο οποίο θα κάνει έρευνα το πρόγραμμα.

```
[root@localhost redfang]# ./fang –s –r 00:0B:0D:32:3A:7C -
00:0B:0D:32:3A:9C

Scanning 3 address(es)

Address range 00:0B:0D:32:3A:7C -> 00:0B:0D:32:3A:9C

Performing Bluetooth Discovery... Completed.
```

```
Discovered: MyPC [00:0B:0D:32:3A:9C]
```

- -o <filename> : αποθηκεύει το αποτέλεσμα της έρευνας σε ένα αρχείο κειμένου.

```
[root@localhost redfang]# ./fang –s –o test.txt
```

- -t <timeout> : ο χρήστης ορίζει το connection timeout το οποίο εξ'αρχής παίρνει την τιμή 10000.

```
[root@localhost redfang]# ./fang –s –t 15000
```

- -n <num> : ο χρήστης ορίζει τον αριθμό των USB dongles που χρησιμοποιεί.
- -d : εμφανίζει πληροφορίες αποσφαλμάτωσης.
- -s : εκκινεί την αναζήτηση bluetooth συσκευών στην περιοχή του χρήστη.

```
[root@localhost redfang]# ./fang -s
Scanning 281474976710656 address(es)
Address range 00:00:00:00:00:00 -> ff:ff:ff:ff:ff:ff
Performing Bluetooth Discovery... Completed.
Discovered: Hapagan [00:11:9F:74:EF:19]
Getting Device Information.. Connected.
        LMP Version: 1.1 (0x1) LMP Subversion: 0x382
        Manufacturer: Cambridge Silicon Radio (10)
        Features: 0xbf 0xfe 0x0f 0x00
                <3-slot packets>
                <5-slot packets>
                <encryption>
                <slot offset>
                <timing accuracy>
                <role switch>
                <sniff mode>
                <RSSI>
                <channel quality>
                <SCO link>
                <HV2 packets>
                <HV3 packets>
```

```
        <u-law log>
        <A-law log>
        <CVSD>
        <paging scheme>
        <power control>
        <transparent SCO>
Done 1 – 00:00:00:00:00:01 κλπ
```

- -l : εμφανίζει τους κωδικούς για κάθε κατασκευαστή.

```
[xaris@localhost redfang]$ ./fang -l
Valid manf codes are:
    3com          000BAC  3Com Europe Ltd.
    Ericsson      0001EC  Ericsson Group (pre Sony-Ericsson)
    SE            008037  Ericsson Group (Sony-Ericsson)
    SE2           000AD9  Sony Ericsson Mobile Communications Ab
    murata        006057  Murata Manufacturing Co., Ltd. (Nokia)
    Nokia         0002EE  Nokia Danmark A/s
    tdk           008098  TDK Corporation
    dlink         0080C8  D-link Systems, Inc. (CSR Chipset)
    digianswer    0050CD  Digianswer A/s
    Tecom         0003C9  Tecom Co., Ltd.
    apple         000393  Apple Computer, Inc.
    siwave        00033A  Silicon Wave, Inc.
    csr           00025B  Cambridge Silicon Radio
    widcomm       000361  Widcomm, Inc.
    redm          000A1E  Red-M (Communications) Limited
    billion       001060  Billionton Systems, Inc.
    Nokia2        00E003  Nokia Wireless Business Communications
    alpsipaq      0002C7  Alps Electric Co., Ltd. (Ipaq 38xx)
    intelbt       00D0B7  Intel Corporation (Bluetooth)
    3com2         000476  3 Com Corporation (Bluetooth)
    cmt           00308E  Cross Match Technologies, Inc. (Axis)
    windigo       00081B  Windigo Systems
    taiyo         00037A  Taiyo Yuden Co., Ltd.
    abocom        00E098  AboCom Systems, Inc. (Palladio USB CSR
```

```
Chipset)
        anicom          004005  Ani Communications Inc.
        palm            0007E0  Palm Inc.
```

- -h : εμφανίζει ένα αρχείο βοηθείας με αναλυτική αναφορά στις παραμέτρους του προγράμματος.

ΚΕΦΑΛΑΙΟ 9
ΠΡΟΕΤΟΙΜΑΣΙΑ ΤΟΥ ΔΙΚΤΥΟΥ PAN

Η δεύτερη ενότητα της παρούσας διπλωματικής ασχολείται με την πραγματοποίηση μετρήσεων σε ένα δίκτυο τύπου Personal Area Network (PAN) με χρήση του πρωτοκόλλου Bluetooth. Οι μετρήσεις αυτές έχουν σαν σκοπό να εκτιμήσουν την απόδοση του δικτύου σε συνάρτηση με τα χαρακτηριστικά ασφαλείας που εφαρμόζονται κάθε φορά σε αυτό. Για τις ανάγκες των μετρήσεων, πρόκειται να χρησιμοποιηθούν τα πρωτόκολλα ασφαλείας SSH, IPsec αλλά και το γηγενές σύστημα ασφαλείας του πρωτοκόλλου Bluetooth. Με το πέρας των μετρήσεων, θα αναλυθούν τα αποτελέσματα και θα παρουσιαστούν με μορφή συγκριτικών πινάκων και γραφημάτων. Για κάθε περίπτωση προς εξέταση, θα χρησιμοποιηθούν διαφορετικές παράμετροι όπως είναι διάφοροι αλγόριθμοι κρυπτογράφησης και αυθεντικοποίησης. Επιπλέον, όσο αφορά, το γηγενές σύστημα ασφαλείας του Bluetooth, θα χρησιμοποιηθούν και οι τρεις διαφορετικές καταστάσεις ασφαλείας που παρέχονται.

Αρχικά, θα αναλύσουμε εν συντομία τα γηγενή χαρακτηριστικά του πρωτοκόλλου Bluetooth και πώς τα χρησιμοποιήσαμε και τα ρυθμίσαμε για να πάρουμε τις αντίστοιχες μετρήσεις. Επίσης, θα αναφερθούμε στα προγράμματα και τους οδηγούς που χρησιμοποιήσαμε έτσι ώστε να δοθεί μια σαφής εικόνα του πειραματικού περιβάλλοντος μετρήσεων (test-bed). Η επόμενη ενότητα (9.2) αναπτύσσει ζητήματα σχετικά με το πρωτόκολλο ασφαλείας IPsec. Στην εισαγωγή θα γίνει μια γρήγορη αναφορά στα βασικά στοιχεία του πρωτοκόλλου ενώ στη συνέχεια θα παρατεθούν τα προγράμματα και οι διάφορες ρυθμίσεις που έγιναν σε αυτά σε αυτά προκειμένου να ολοκληρωθούν με επιτυχία οι διάφορες μετρήσεις. Τέλος, στη τρίτη ενότητα του κεφαλαίου 9.3 αναλύεται το πρωτόκολλο ασφαλείας SSH καθώς και το λογισμικό που εγκαταστάθηκε και χρησιμοποιήθηκε για την πραγματοποίηση των μετρήσεων.

Για τις ανάγκες των μετρήσεων και της ανάλυσης των αποτελεσμάτων, χρησιμοποιήθηκαν δυο προσωπικοί υπολογιστές με τα χαρακτηριστικά που παρατίθενται στον παρακάτω πίνακα:

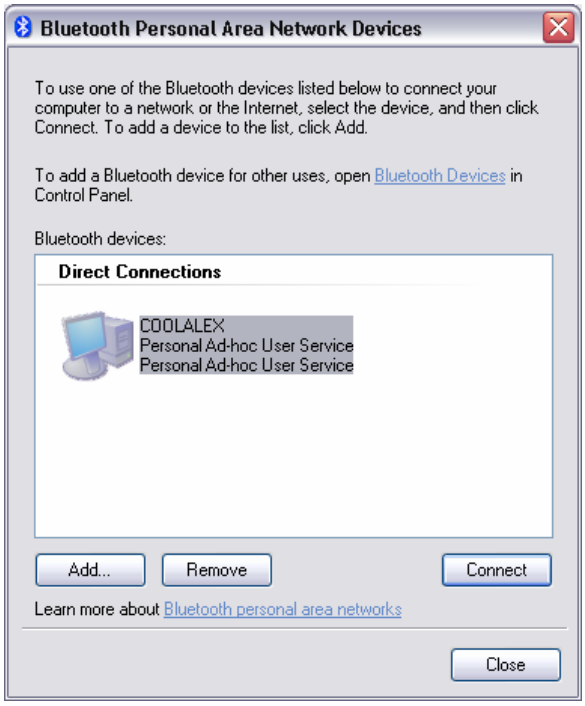
Χαρακτηριστικά στοιχεία των προσωπικών υπολογιστών που χρησιμοποιήθηκαν	**Προσωπικός Υπολογιστής 1**	**Προσωπικός Υπολογιστής 2**
Επεξεργαστής	Intel Pentium 4 2,8GHz	Intel Pentium 4 2,8 GHz
Μνήμη RAM	512 MB DDR	512 MB DDR
Σκληρός Δίσκος	80 GB – 250 GB	60 GB
Λειτουργικά Συστήματα	Windows XP Professional SP2 Mandrake 10.2	Windows XP Professional SP2 SUSE 9.2
Bluetooth Adapter	Trust Bluetooth Adapter Class 1	Trust Bluetooth Adapter Class 1

Πίνακας 9-1 Χαρακτηριστικά στοιχεία των προσωπικών υπολογιστών που χρησιμοποιήθηκαν

Το λογισμικό που χρησιμοποιήθηκε για την καταγραφή των πακέτων που ανταλλάσσονται μεταξύ των κόμβων του δικτύου, είναι το Ethereal Network Protocol Analyzer και πιο συγκεκριμένα η έκδοση 0.10.12. Το Ethereal πρόκειται για ένα

πρόγραμμα ελεύθερου κώδικα (open source) το οποίο διανέμεται με την άδεια χρήσης GNU General Public License.

Η διαδικασία που ακολουθείται για την δικτύωση δυο υπολογιστών σε περιβάλλον Windows είναι σχετικά απλή. Η μοναδική προϋπόθεση είναι η ύπαρξη μιας μικρής συσκευής που θα δίνει τη δυνατότητα στην συσκευή να επικοινωνεί με το πρωτόκολλο Bluetooth. Στη συνέχεια και με τη βοήθεια του σχετικού προγράμματος που παρέχουν τα Windows XP SP2 ή που έχει δοθεί με την συσκευή, ο χρήστης μπορεί να δημιουργήσει ένα PAN με τις κοντινές σε αυτόν συσκευές.



Εικόνα 9-1 "Παράθυρο" επεξεργασίας κόμβων PAN

Αρχικά, πραγματοποιεί μια έρευνα για τον εντοπισμό των κοντινών Bluetooth-ενεργοποιημένων συσκευών που έχουν τη δυνατότητα δικτύωσης και άρα συμμετοχής στο συγκεκριμένο σε ένα PAN. Στη συνέχεια, επιλέγουμε μια από αυτές και πατάμε, όπως φαίνεται και στη διπλανή εικόνα, την σύνδεση. Μόλις, οι συσκευές συνδεθούν τότε αποκτούν από μια διεύθυνση IP και το δίκτυο πλέον λειτουργεί σαν ένα κοινό τοπικό δίκτυο.

9.1 Bluetooth

Όπως αναφέραμε και σε προηγούμενα κεφάλαια, το Bluetooth παρέχει τρεις καταστάσεις ασφαλείας ανάλογα με το αν έχουν ή όχι ενεργοποιηθεί οι υπηρεσίες αυθεντικοποίησης και κρυπτογράφησης. Έτσι, στην κατάσταση ασφαλείας 1 δεν έχει ενεργοποιηθεί καμία από τις προσφερόμενες υπηρεσίες ενώ στη κατάσταση ασφαλείας 2 απαιτείται η ύπαρξη αυθεντικοποίησης του χρήστη και κρυπτογράφησης των δεδομένων αφού έχει γίνει η σύνδεση και μόνο αν αυτό ζητηθεί από μια εφαρμογή ή υπηρεσία. Τέλος, η κατάσταση ασφαλείας 3 απαιτεί την χρήση τόσο αυθεντικοποίησης όσο και κρυπτογράφησης από την (αρχική) εγκαθίδρυση της σύνδεσης.

Οι οδηγοί και τα προγράμματα που παρέχονται στο χρήστη από το Service Pack 2 των Windows XP δίνουν τη δυνατότητα χρήσης αποκλειστικά και μόνο της κατάστασης ασφαλείας 3. Για αυτό το λόγο αναγκαστήκαμε να πραγματοποιήσουμε τις μετρήσεις για το Bluetooth σε περιβάλλον Linux, το οποίο με τη βοήθεια του προγράμματος BlueZ υποστηρίζει τις καταστάσεις ασφαλείας 1 και 3.

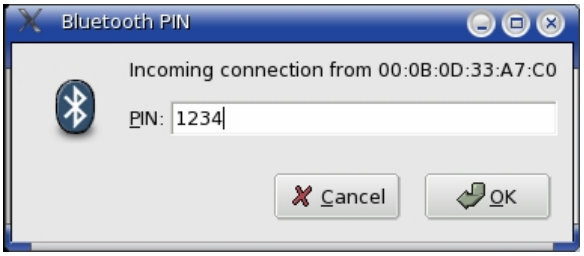
Θεωρούμε ότι έχουμε δυο υπολογιστές που θέλουμε να συνδέσουμε σε δίκτυο PAN σε περιβάλλον Linux χρησιμοποιώντας τα εργαλεία του προγράμματος BlueZ. Αρχικά, θα πρέπει να ξεκαθαρίσουμε το τρόπο με τον οποίο μπορούμε να επιλέξουμε μεταξύ της κατάστασης ασφαλείας 1 και της κατάστασης ασφαλείας 3. Το αρχείο που αποθηκεύει αυτές τις ρυθμίσεις ονομάζεται hcid.conf και βρίσκεται στο μονοπάτι /etc/bluetooth/. Πριν το ανοίξουμε πρέπει να έχουμε δικαιώματα super user (su) έτσι

ώστε να μπορέσουμε να αποθηκεύσουμε τις αλλαγές που θα κάνουμε. Κατόπιν, τροποποιούμε κατάλληλα τις αντίστοιχες γραμμές στις οποίες επιλέγουμε αν θα χρησιμοποιήσουμε αυθεντικοποίηση και κρυπτογράφηση ή όχι. Η τιμή που υπάρχει, πρέπει να είναι απενεργοποιημένη και για τις δυο ιδιότητες τοποθετώντας μια δίεση (#) μπροστά. Θα πρέπει να βγάλουμε την δίεση και από τα δυο για να ενεργοποιηθεί η κατάσταση ασφαλείας 1 ή να βγάλουμε τη δίεση και να κάνουμε τις τιμές από απενεργοποιημένη σε ενεργοποιημένη για την κατάσταση ασφαλείας 1.

```
# Authentication and Encryption (Security Mode 3)
      auth enable;
      encrypt enable;
```

```
# Authentication and Encryption (Security Mode 1)
      auth disable;
      encrypt disable;
```

Αν επιλέξουμε την κατάσταση ασφαλείας 3, τότε μόλις ληφθεί η αίτηση σύνδεσης από τον υπολογιστή-εξυπηρέτη θα του εμφανιστεί το παρακάτω παράθυρο το οποίο θα του ζητάει να εισάγει το σωστό PIN έτσι ώστε να πραγματοποιηθεί η σύνδεση. Το PIN και στους δυο υπολογιστές βρίσκεται αποθηκευμένο στο μονοπάτι /etc/bluetooth/pin.



Εικόνα 9-2 Εισαγωγή PIN κατά την αποδοχή σύνδεσης

Αμέσως μετά, πρέπει να καθορίσουμε τους ρόλους των δυο συσκευών. Αυτό γίνεται με τις παρακάτω εντολές:

```
[root@localhost ~]$  pand –listen –role GN
[root@localhost ~]$  pand –listen –role PANU
```

Με την παράμετρο GN ορίζεται ο υπολογιστής-εξυπηρέτης ενώ με την PANU ο υπολογιστής-πελάτης. Έτσι, το επόμενο βήμα είναι ο πελάτης να συνδεθεί με τον εξυπηρέτη. Φυσικά για να γίνει αυτό θα πρέπει πρώτα να γνωρίζει την Bluetooth Address του. Όπως έχουμε αναφέρει και σε προηγούμενο κεφάλαιο, τη διεύθυνση μπορούμε να την βρούμε κάνοντας χρήση της εντολής hcitool scan.

```
[root@localhost ~]$ hcitool scan
Scanning ...        00:11:9F:74:EF:19       Hapagan

[xaris@localhost ~]$ pand –connect 00:11:9F:74:EF:19
```

Πλέον, έχει πραγματοποιηθεί η σύνδεση σε δίκτυο PAN των δυο υπολογιστών και το μόνο που απομένει είναι να ρυθμίσουμε τις διευθύνσεις IP. Είναι μια απλή

διαδικασία που πραγματοποιείται με την χρήση μιας και μόνο εντολής σε κάθε κόμβο.

```
[root@localhost ~]$ ifconfig bnep0 10.0.0.20
```

Έτσι, οι δυο υπολογιστές μπορούν να κάνουν ping ο ένας στον άλλο και να ανταλλάξουν αρχεία. Για την απομακρυσμένη αντιγραφή αρχείων, χρησιμοποιήσαμε τον FTP Server tftp και για FTP Client τον ενσωματωμένο πελάτη που παρέχει το Linux, ο οποίος εκτελείται με την εντολή ftp.

9.2 IPsec

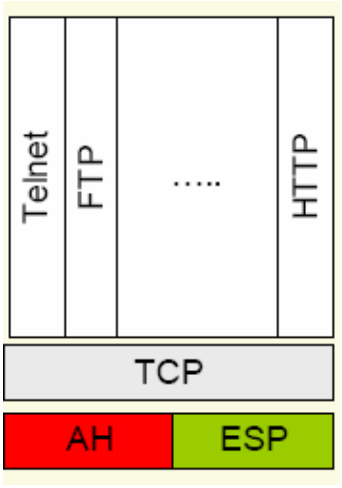
9.2.1 Εισαγωγικά στοιχεία

Μηχανισμοί ασφαλείας

Η IETF έχει επινοήσει μια σειρά πρωτοκόλλων που παρέχουν ασφαλείς επικοινωνίες στο διαδίκτυο. Η σουίτα των πρωτοκόλλων αυτών είναι γνωστή ως *IPsec* (IP security – ασφάλεια IP) και προσφέρει υπηρεσίες αυθεντικοποίησης και εμπιστευτικότητας σε επίπεδο IP ενώ μπορεί να χρησιμοποιηθεί τόσο με IPv4 όσο και με IPv6. Συγκεκριμένα, χρησιμοποιούνται οι παρακάτω δύο μηχανισμοί ασφαλείας [43]:

- *Επικεφαλίδα Αυθεντικοποίησης (Authentication Header – AH):* Παρέχει αυθεντικοποίηση προέλευσης δεδομένων και υπηρεσίες ακεραιότητας δεδομένων χωρίς σύνδεση. Η επικεφαλίδα αυθεντικοποίησης επιτρέπει στον παραλήπτη ενός IP πακέτου να επιβεβαιώνει την ταυτότητα του δημιουργού του και να εξετάζει αν έχει τροποποιηθεί το πακέτο κατά τη διάρκεια της μετάδοσης.
- *Ενθυλακωμένο ωφέλιμο φορτίο ασφαλείας (Encapsulating Security Payload – ESP):* Παρέχει υπηρεσίες εμπιστευτικότητας δεδομένων χωρίς σύνδεση. Εξασφαλίζει έτσι ότι μόνο οι νόμιμοι αποδέκτες ενός IP πακέτου έχουν τη δυνατότητα να το αναγνώσουν.

Το IPsec υλοποιεί κρυπτογράφηση και πιστοποίηση επιπέδου δικτύου παρέχοντας μια λύση ασφαλείας μέσα στην ίδια την αρχιτεκτονική του δικτύου [44] [45] [46] [47] [48]. Έτσι τα συστήματα και οι εφαρμογές που βρίσκονται στις άκρες δεν χρειάζονται αλλαγές ή ρυθμίσεις για να έχουν το πλεονέκτημα της ισχυρής ασφάλειας. Επειδή τα κρυπτογραφημένα πακέτα μοιάζουν με κανονικά IP πακέτα μπορούν εύκολα να δρομολογηθούν μέσα από οποιοδήποτε IP δίκτυο, όπως το Διαδίκτυο, χωρίς καμία αλλαγή στον ενδιάμεσο δικτυακό εξοπλισμό. Οι μόνες συσκευές οι οποίες γνωρίζουν για την κρυπτογράφηση είναι αυτές στα ακραία σημεία. Αυτό το χαρακτηριστικό μειώνει δραστικά τόσο το κόστος της υλοποίησης όσο και το



κόστος της διαχείρισης.

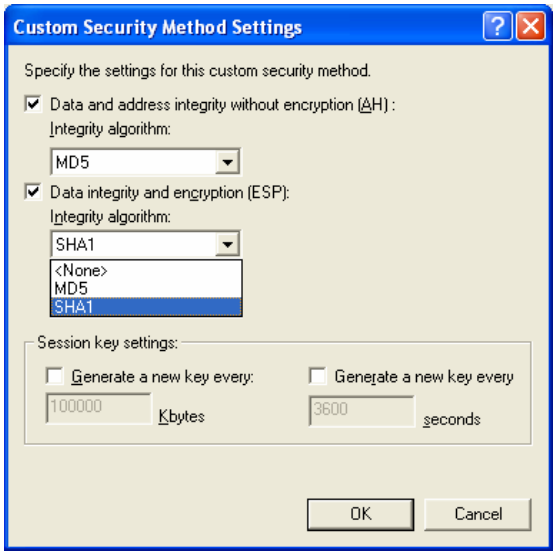
Το IPsec συνδυάζει τις παραπάνω τεχνολογίες ασφάλειας σε ένα ολοκληρωμένο σύστημα το οποίο παρέχει εμπιστευτικότητα, ακεραιότητα και πιστοποίηση της ταυτότητας των IP πακέτων. Το IPsec αναφέρεται και σε μια σειρά άλλων πρωτοκόλλων όπως ορίζεται στα RFC 1825-1829 και σε άλλες δημοσιεύσεις στο Internet. Αυτές οι προδιαγραφές περιλαμβάνουν:

- Κατάλληλο IP πρωτόκολλο ασφαλείας, το οποίο καθορίζει την πληροφορία που πρέπει να προστεθεί σε ένα IP πακέτο για να ενεργοποιηθούν οι έλεγχοι πιστότητας, ακεραιότητας και πιστοποίησης ταυτότητας, όπως επίσης καθορίζει και το πώς πρέπει να γίνει η κρυπτογράφηση των δεδομένων του πακέτου.
- Ανταλλαγή κλειδιών Διαδικτύου, το οποίο διαπραγματεύεται το συσχετισμό ασφάλειας μεταξύ δυο οντοτήτων και ανταλλάσσει το υλικό των κλειδιών. Δεν είναι απαραίτητο να χρησιμοποιηθεί το IKE, αλλά το να ρυθμιστούν χειροκίνητα οι συσχετισμοί ασφάλειας είναι μια δύσκολη και επίπονη διαδικασία. Το IKE πρέπει να χρησιμοποιείται στις περισσότερες εφαρμογές για να ενεργοποιεί ασφαλείς επικοινωνίες μεγάλης κλίμακας.

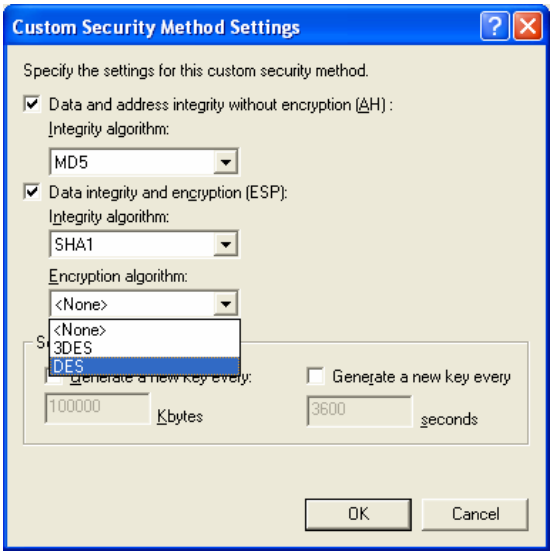
Πακέτα IPsec

Το IPsec ορίζει ένα νέο σετ επικεφαλίδων το οποίο προστίθεται στα IP διαγράμματα. Αυτές οι νέες επικεφαλίδες τοποθετούνται μετά την επικεφαλίδα IP και πριν το πρωτόκολλο επιπέδου 4 (τυπικά το TCP ή το UDP).

Οι μηχανισμοί ασφαλείας AH και ESP μπορούν να χρησιμοποιηθούν ανεξάρτητα ή μαζί. Και για τους δυο αυτούς μηχανισμούς το IPSec δεν καθορίζει συγκεκριμένους αλγόριθμους που πρέπει να χρησιμοποιηθούν, αλλά παρέχει ένα ανοικτό πλαίσιο για βιομηχανική υλοποίηση με παραγωγή ανεξάρτητων αλγορίθμων. Αρχικά οι περισσότερες υλοποιήσεις του IPsec περιλαμβάνουν υποστήριξη για τον MD5 από την RSA Data Security ή για τον SHA (Secure Hash Algorithm) όπως ορίζεται από την κυβέρνηση των Η.Π.Α. για την ακεραιότητα και την πιστοποίηση της ταυτότητας. Το DES (Data Encryption Standard) και εν συνεχεία 3DES είναι προς το παρόν ο πιο κοινά προσφερόμενος αλγόριθμος κρυπτογράφησης αν και υπάρχουν και



Εικόνα 9-3
Επιλογή αλγόριθμου ακεραιότητας



Εικόνα 9-4
Επιλογή αλγόριθμου κρυπτογράφησης

άλλοι όπως οι IDEA, Blowfish και RC4. Οι πρώτοι τέσσερις παραπάνω αλγόριθμοι υποστηρίζονται και από το λειτουργικό σύστημα Windows XP Pro και χρησιμοποιηθήκαν για τις μετρήσεις μας.

Το IPsec παρέχει δυο καταστάσεις λειτουργίας:

- *Κατάσταση μεταγωγής (transport mode):* Στην κατάσταση transport μόνο το IP φορτίο κρυπτογραφείται ενώ οι αρχικές επικεφαλίδες μένουν ανέπαφες. Αυτή η κατάσταση λειτουργίας έχει το πλεονέκτημα της πρόσθεσης μόνο μερικών bytes σε κάθε πακέτο. Επιπλέον, επιτρέπουν σε συσκευές στο δημόσιο δίκτυο να βλέπουν τη πηγή και το προορισμό του πακέτου. Αυτή η δυνατότητα επιτρέπει ειδική επεξεργασία (π.χ. QoS) στο ενδιάμεσο δίκτυο βασισμένη στην πληροφορία που βρίσκεται στην IP επικεφαλίδα. Ωστόσο, η επικεφαλίδα του επιπέδου 4 θα κρυπτογραφηθεί περιορίζοντας τη δυνατότητα έρευνας των πακέτων. Βεβαίως αφήνοντας την IP επικεφαλίδα χωρίς κρυπτογράφηση η κατάσταση λειτουργίας transport επιτρέπει στον επιτιθέμενο να κάνει ανάλυση κίνησης (traffic analysis). Για παράδειγμα ο επιτιθέμενος θα μπορούσε να δει πότε ένας υψηλό στέλεχος της Cisco έστειλε πολλά πακέτα σε ένα άλλο CEO. Ωστόσο, ο επιτιθέμενος θα γνώριζε μόνο την αποστολή των IP πακέτων και δεν θα ήταν σε θέση να καθορίσει αν αυτά ήταν πακέτα e-mail ή κάποιας άλλης εφαρμογής.
- *Κατάσταση διόδου (tunnel mode):* Στην κατάσταση λειτουργίας tunnel όλο το IP διάγραμμα κρυπτογραφείται και γίνεται το φορτίο ενός καινούριου IP πακέτου. Αυτή η κατάσταση λειτουργίας επιτρέπει σε μια δικτυακή συσκευή, όπως ένας δρομολογητής, να ενεργήσει σαν ένας IPSec proxy. Αυτό σημαίνει ότι ο δρομολογητής πραγματοποιεί κρυπτογράφηση για λογαριασμό των υπολογιστών του δικτύου. Η πηγή του δρομολογητή κρυπτογραφεί τα πακέτα και τα προωθεί στο IPsec tunnel. Ο προορισμός του δρομολογητή αποκρυπτογραφεί το αρχικό IP διάγραμμα και το προωθεί στο σύστημα προορισμού του. Το βασικό πλεονέκτημα αυτής της κατάστασης λειτουργίας είναι ότι τα ακραία συστήματα δεν χρειάζεται να ρυθμιστούν για να επικαρπωθούν τα πλεονεκτήματα της IPsec. Η κατάσταση λειτουργίας tunnel προστατεύει επιπλέον το σύστημα από την διαδικασία της ανάλυσης κίνησης. Σε αυτή την κατάσταση λειτουργίας ο επιτιθέμενος μπορεί να καθορίσει μόνο τα ακραία σημεία του tunnel και όχι την πραγματική πηγή και τον προορισμό των πακέτων που κυκλοφορούν μέσα σε αυτό ακόμη και αν είναι τα ίδια με τα ακραία σημεία του tunnel.

Συσχετισμοί ασφαλείας (Security Association - SA)

Η IPsec παρέχει πολλές επιλογές για την υλοποίηση κρυπτογράφησης και πιστοποίησης ταυτότητας στο δίκτυο. Κάθε IPSec σύνδεση μπορεί να παρέχει είτε κρυπτογράφηση είτε ακεραιότητα και πιστοποίηση ταυτότητας δεδομένων ή και τα δυο. Όταν η υπηρεσία ασφάλειας καθοριστεί οι δυο επικοινωνούντες κόμβοι πρέπει να καθορίσουν ακριβώς ποιους αλγόριθμους θα χρησιμοποιήσουν (για παράδειγμα DES ή 3DES για κρυπτογράφηση και MD5 ή SHA για ακεραιότητα δεδομένων). Αφού αποφασίσουν για τους αλγόριθμους οι δυο συσκευές πρέπει να μοιραστούν κλειδιά σύνδεσης. Όπως μπορούμε να δούμε υπάρχει αρκετή πληροφορία προς παρακολούθηση. Η συσχέτιση ασφάλειας είναι μια μέθοδος που χρησιμοποιείται από

την IPsec για την παρακολούθηση όλων των λεπτομερειών που αφορούν μια δεδομένη IPsec επικοινωνία. Μια συσχέτιση ασφάλειας είναι η σχέση μεταξύ δυο ή περισσοτέρων οντοτήτων που περιγράφει πως οι οντότητες θα χρησιμοποιήσουν τις υπηρεσίες ασφάλειας για να επικοινωνήσουν με ασφάλεια. Η νονμεκλατούρα μπερδεύει μερικές φορές διότι οι συσχετισμοί ασφάλειας χρησιμοποιούνται για πολλά περισσότερα από ότι μόνο για την IPsec. Για παράδειγμα, οι συσχετισμοί ασφάλειας ΙΚΕ περιγράφουν τις παραμέτρους ασφάλειας μεταξύ δυο ΙΚΕ συσκευών.

Οι συσχετισμοί ασφάλειας είναι μη κατευθυντικοί που σημαίνει ότι για κάθε ζεύγος επικοινωνούντων συστημάτων υπάρχουν τουλάχιστον δυο συνδέσεις ασφάλειας—μια από το Α στο Β και μια από το Β στο Α. Ο συσχετισμός ασφάλειας αναγνωρίζεται μοναδικά από έναν τυχαία επιλεγμένο μοναδικό αριθμό ο οποίος λέγεται SPI (Security Parameter Index) και από την IP διεύθυνση του προορισμού. Όταν ένα σύστημα στέλνει ένα πακέτο το οποίο απαιτεί IPSec προστασία κοιτάει τον συσχετισμό ασφάλειας στη βάση δεδομένων του, εφαρμόζει τη συγκεκριμένη επεξεργασία και μετά εισάγει τον SPI από το συσχετισμό ασφάλειας στην IPsec επικεφαλίδα. Όταν το αντίστοιχο μηχάνημα IPsec λαμβάνει το πακέτο κοιτάει με τη σειρά του το συσχετισμό ασφάλειας βάσει της διεύθυνσης προορισμού και του SPI και μετά επεξεργάζεται το πακέτο όπως ορίζεται. Με λίγα λόγια ο συσχετισμός ασφάλειας είναι απλώς μια δήλωση της διαπραγματεύσιμης πολιτικής ασφάλειας μεταξύ δυο συσκευών.

Πρωτόκολλο διαχείρισης κλειδιών διαδικτύου (Internet key exchange protocol – IKE)

Το IPsec μπορεί να θεωρήσει ότι ένας συσχετισμός ασφάλειας υπάρχει αλλά δεν έχει το μηχανισμό να τον δημιουργήσει. Η IETF επέλεξε να σπάσει τη διαδικασία αυτή σε δύο μέρη: η IPsec παρέχει την επεξεργασία των πακέτων επιπέδου IP και το πρωτόκολλο διαχείρισης κλειδιών Internet *(IKMP—Internet Key Management Protocol)*, ασχολείται με ότι έχει να κάνει με τους συσχετισμούς ασφάλειας.

Το ΙΚΕ δημιουργεί ένα πιστοποιημένο και ασφαλές κανάλι – τούνελ μεταξύ δύο οντοτήτων και κατόπιν διαπραγματεύεται τους συσχετισμούς ασφάλειας για την IPsec. Αυτή η διαδικασία απαιτεί από τις δύο οντότητες να πιστοποιήσουν η μία την άλλη και να μοιράσουν κλειδιά.

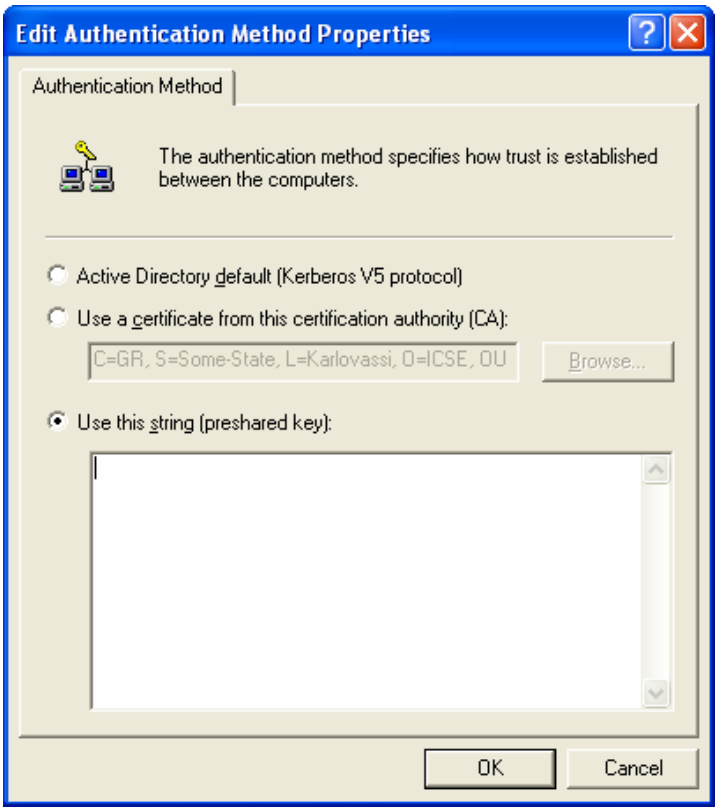
Το ΙΚΕ είναι πολύ ευέλικτο και υποστηρίζει πολλές διαφορετικές μεθόδους πιστοποίησης της ταυτότητας. Οι δύο οντότητες πρέπει να συμφωνήσουν σε ένα κοινό πρωτόκολλο πιστοποίησης μέσω μιας κατάλληλης διαδικασίας. Σε αυτή τη φάση υλοποιούνται συνήθως οι παρακάτω μηχανισμοί:

- *Προμοιρασμένα Συμμετρικά Κλειδιά (preshared key):* Το ίδιο κλειδί προ-εγκαθίσταται και στις δύο μηχανές. Κατά την πιστοποίηση αποστέλλεται από τη μία μηχανή στην άλλη μία επεξεργασμένη μορφή (με τη βοήθεια μιας hash συνάρτησης) του ίδιου κλειδιού. Εάν αυτή η μορφή συμπίπτει με αυτήν που υπολογίζεται τοπικά σε κάθε μηχανή, τότε η διαδικασία πιστοποίησης έχει θετικό αποτέλεσμα.
- *Κρυπτογράφηση Δημοσίων Κλειδιών:* Κάθε μηχανή "γεννάει" έναν ψευδο-τυχαίο αριθμό τον οποίο και κρυπτογραφεί με το public key (δημόσιο κλειδί) της άλλης μηχανής. Η πιστοποίηση επιτυγχάνεται μέσω της ικανότητας των μηχανών να υπολογίσουν μια hash συνάρτηση του τυχαίου αριθμού αποκρυπτογραφώντας με τα private keys (ιδιωτικά κλειδιά) ότι λαμβάνουν από το συνομιλητή τους. Το σύστημα παρέχει ακόμα και δυνατότητα άρνησης

συμμετοχής σε οποιαδήποτε διαδικασία πιστοποίησης. Προς το παρόν μόνο ο αλγόριθμος δημοσίων κλειδιών της RSA υποστηρίζεται.

- *Ψηφιακές Υπογραφές (digital signatures):* Κάθε συσκευή υπογράφει ψηφιακά ένα σύνολο δεδομένων και τα στέλνει στην άλλη. Αυτή η μέθοδος είναι παρόμοια με την προηγούμενη μόνο που δεν παρέχει μηχανισμό άρνησης της εμπλοκής της σε κάποια προσπάθεια πιστοποίησης. Προς το παρόν υποστηρίζονται τόσο ο αλγόριθμος δημοσίων κλειδιών της RSA όσο και οι προδιαγραφές ψηφιακών υπογραφών (DSS).

Τόσο η διαδικασία κρυπτογράφησης όσο και αυτή των ψηφιακών υπογραφών απαιτεί τη χρήση *ψηφιακών πιστοποιητικών* για την επικύρωση της δημόσιας σε ιδιωτική αντιστοίχησης. Το IKE επιτρέπει την ανεξάρτητη ανταλλαγή των ψηφιακών πιστοποιητικών με τη χρήση για παράδειγμα του DNSSEC ή την ανταλλαγή τους σαν μέρος του IKE.



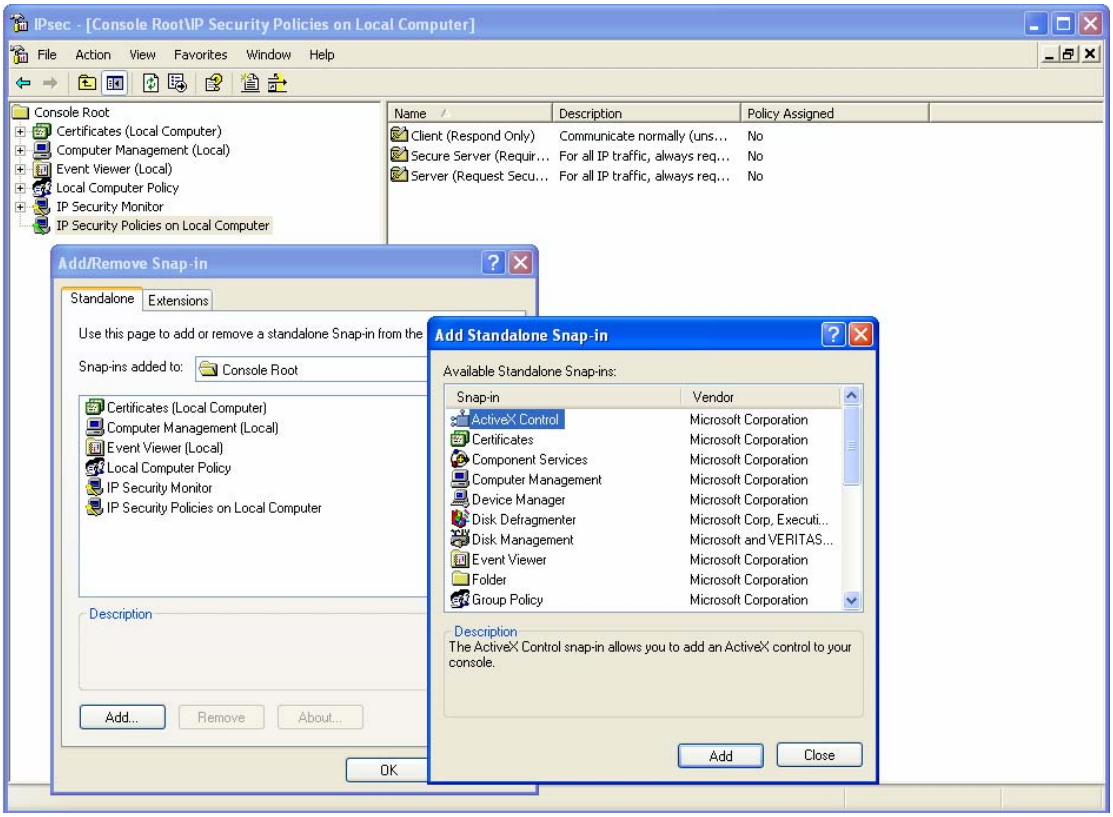
Εικόνα 9-5 Επιλογή προμοιρασμένου κλειδιού ως μέθοδο αυθεντικοποίησης

9.2.2 Εφαρμογή IPsec σε περιβάλλον Windows

Στη περίπτωση που έχουμε δημιουργήσει ένα Bluetooth PAN, όπως περιγράψαμε στην πρώτη υποενότητα, η κάθε συσκευή έχει τη δική της IP διεύθυνση. Έτσι μπορούμε να εφαρμόσουμε το πρωτόκολλο IPsec για να προστατεύσουμε τα δεδομένα μας κατά την επικοινωνία με Bluetooth [49] [50]. Τα Windows XP Professional υποστηρίζουν IPsec αλλά για να το εφαρμόσουμε χρειάζονται μια σειρά από βήματα και στους δύο υπολογιστές που θα περιγράψουμε αμέσως παρακάτω.

Δημιουργία κονσόλας

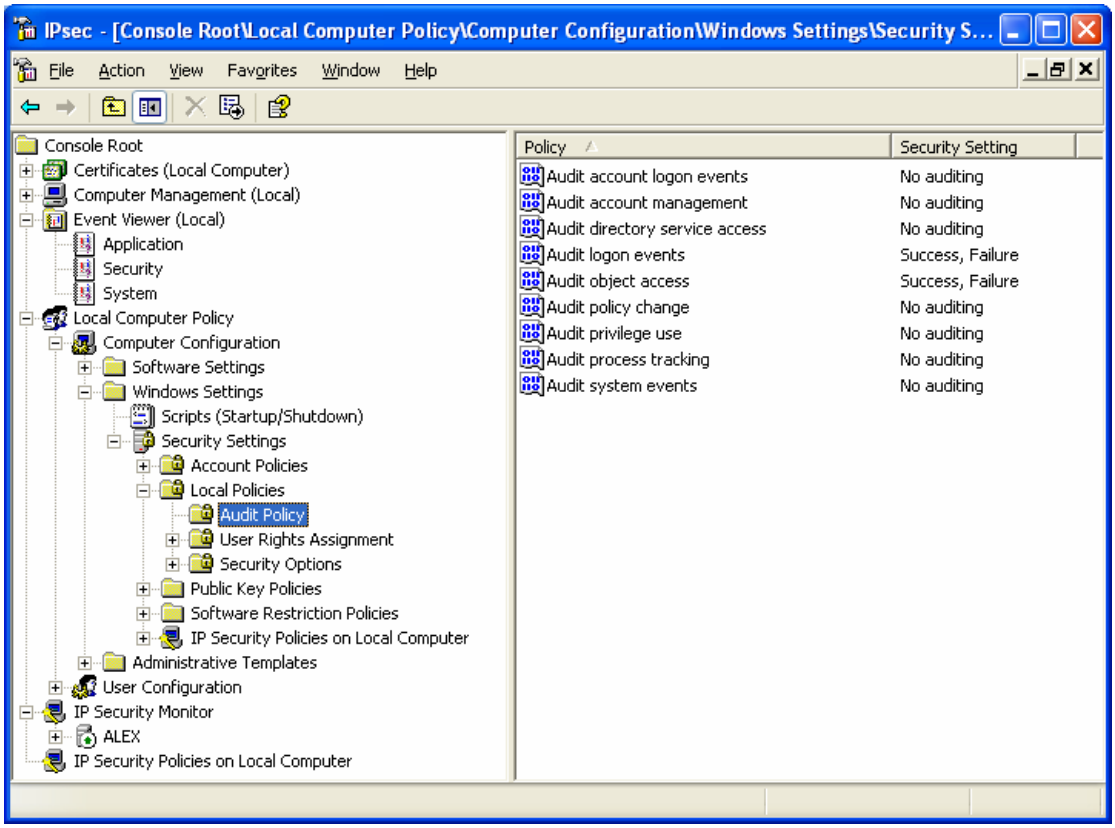
Καταρχήν, από το Start > Run > mmc δημιουργούμε μία κονσόλα πάνω στην οποία θα εισάγουμε τα στοιχεία που είναι απαραίτητα για την εφαρμογή του IPsec. Από το μενού της κονσόλας εισάγουμε τα εξής snap-in: IP Security Policy Management, IP Security Monitor, Group Policy, Event Viewer, Certificates και Computer Management, όπως φαίνεται στο παρακάτω screenshot.



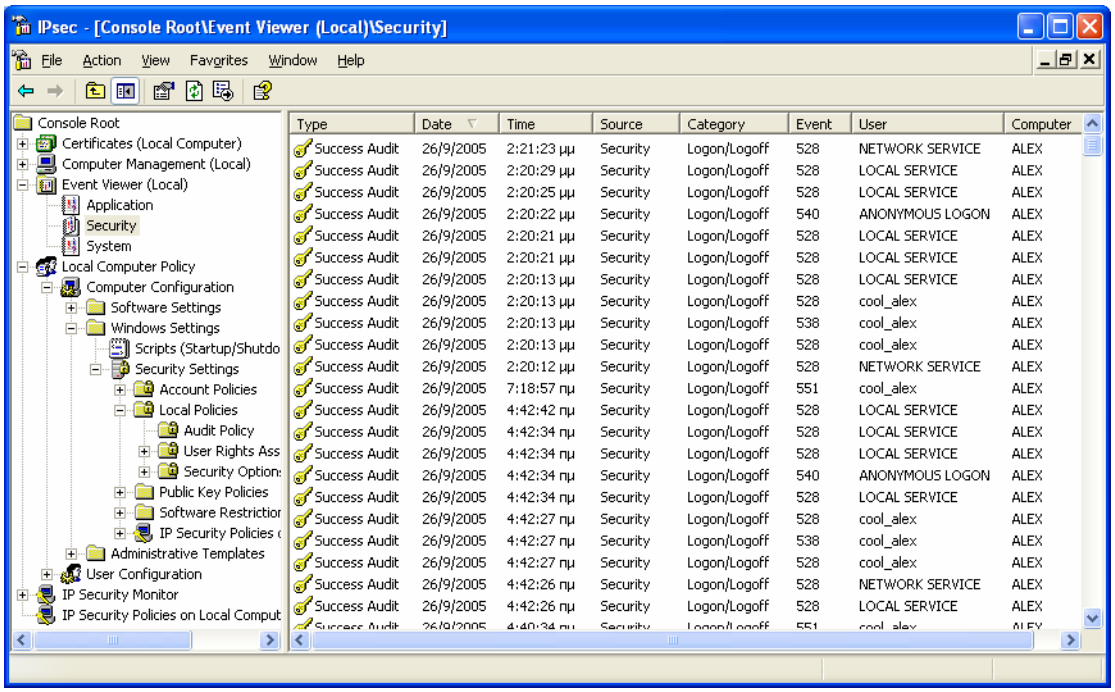
Εικόνα 9-6 Εισαγωγή snap-in στην κονσόλα

Το κύριο snap-in είναι το IP Security Policy. Αυτό χρησιμοποιούμε για να εφαρμόσουμε κάθε φορά την πολιτική ασφαλείας που εμείς θέλουμε. Τα υπόλοιπα λειτουργούν ως προαπαιτούμενα ή βοηθητικά. Έτσι, τα Certificates τα εισάγουμε για να τα χρησιμοποιήσουμε αργότερα ως μία από τις μεθόδους αυθεντικοποίησης στο IPsec, το Event Viewer για να παρακολουθούμε αν πράγματι έχει εφαρμοστεί το IPsec αφού καταγράφεται η δραστηριότητα σε log αρχείο, το Local Computer Policy για να ενεργοποιήσουμε τον Event Viewer όσον αφορά το IPsec και τέλος το IP Security Monitor για την καταγραφή στατιστικών.

Η ενεργοποίηση του Event Viewer γίνεται από το Local Computer Policy → Computer Configuration → Windows Settings → Security Settings → Local Policies → Audit Policy και από εκεί ενεργοποιούμε το Success και Failure στα χαρακτηριστικά “Audit logon events” και “Audit object access”. Με την ολοκλήρωση των παραπάνω βημάτων ο Event Viewer μπορεί πλέον να καταγράφει τα γεγονότα IPsec τα οποία μπορούμε να δούμε επιλέγοντας Event Viewer → Security.



Εικόνα 9-7 Ενεργοποίηση Event Viewer για IPsec



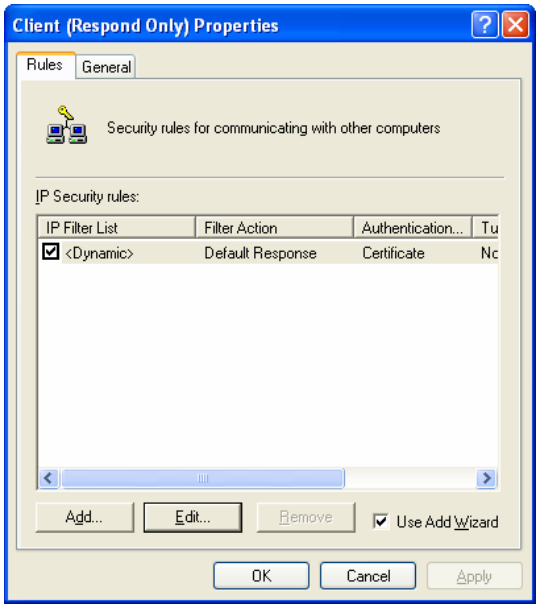
Εικόνα 9-8 Event Viewer για Security

Εφαρμογή πολιτικής ασφαλείας IPsec

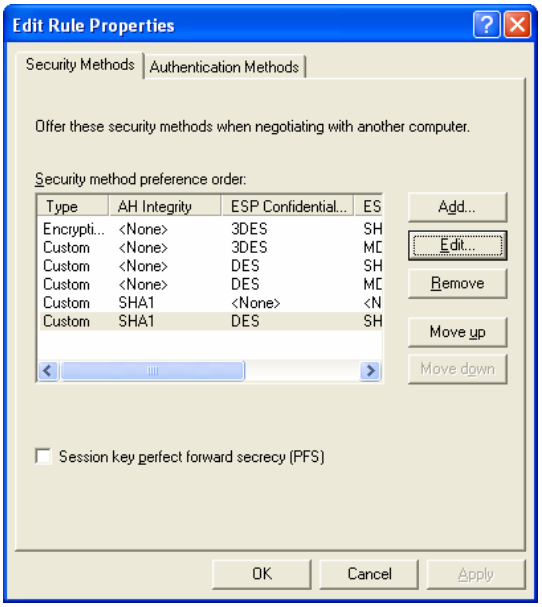
Το σημαντικότερο βήμα είναι η εφαρμογή της πολιτικής ασφαλείας IPsec. Σε ένα Bluetooth PAN ένας υπολογιστής θα παίζει το ρόλο του διακομιστή και ο άλλος του πελάτη. Ο εξυπηρέτης (Secure Server) θα πρέπει να απαιτεί ασφάλεια (Require Security) και ο εξυπηρετούμενος (Client) να απαντάει στην απαίτηση αυτή (Respond

Only). Σε διαφορετική περίπτωση δε θα είναι εφικτή η σύνδεση των δύο υπολογιστών. Οι δύο υπολογιστές πρέπει να έχουν τις ίδιες ρυθμίσεις εφαρμόζοντας τις ίδιες μεθόδους ασφαλείας για ακεραιότητα και κρυπτογράφηση και αυθεντικοποίησης.

Οι μέθοδοι αυτοί μπορούν να παραμετροποιηθούν από το IP Security Policies πηγαίνοντας στις ιδιότητες του διακομιστή και του πελάτη αντίστοιχα. Μας εμφανίζεται έτσι ένα νέο παράθυρο στο οποίο με τη χρήση της μπάρας Rules (αν επιλέξουμε Edit) μπορούμε να αλλάξουμε τους αλγορίθμους για την ακεραιότητα και την κρυπτογράφηση και τις μεθόδους αυθεντικοποίησης.

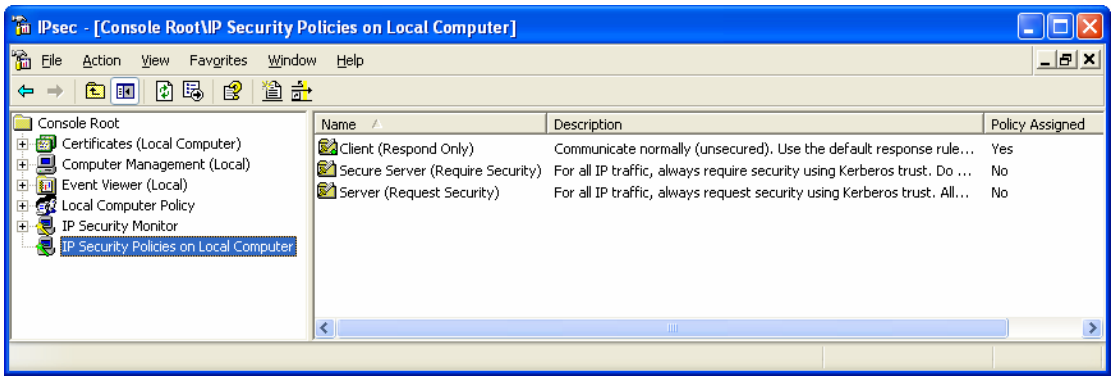


Εικόνα 9-10 Ιδιότητες πελάτη



Εικόνα 9-9 Παραμετροποίηση αλγορίθμων

Όπως αναφέραμε και προηγουμένως στις προδιαγραφές του IPsec ως αλγόριθμοι ακεραιότητας υποστηρίζονται οι MD5 και SHA1, ενώ ως αλγόριθμοι κρυπτογράφησης οι DES και 3DES. Από την άλλη, ως μέθοδοι αυθεντικοποίησης χρησιμοποιούνται τα πιστοποιητικά (certificates) και τα προμοιρασμένα κλειδιά που ουσιαστικά είναι η χρήση ενός κωδικού. Υπάρχει και η δυνατότητα να αυθεντικοποιηθεί ένας χρήστης μέσω του πρωτοκόλλου Κέρβερος αλλά αυτό μπορεί να συμβεί μόνο στην περίπτωση που οι υπολογιστές ανήκουν σε συγκεκριμένο domain, κάτι το οποίο δεν ισχύει στην περίπτωση του Bluetooth. Τέλος, αφού λάβουν χώρα όλες αυτές οι ρυθμίσεις και στους δύο υπολογιστές, πρέπει να κάνουμε Assign με δεξί click πάνω στον διακομιστή και τον πελάτη αντίστοιχα ώστε να εφαρμοστεί η

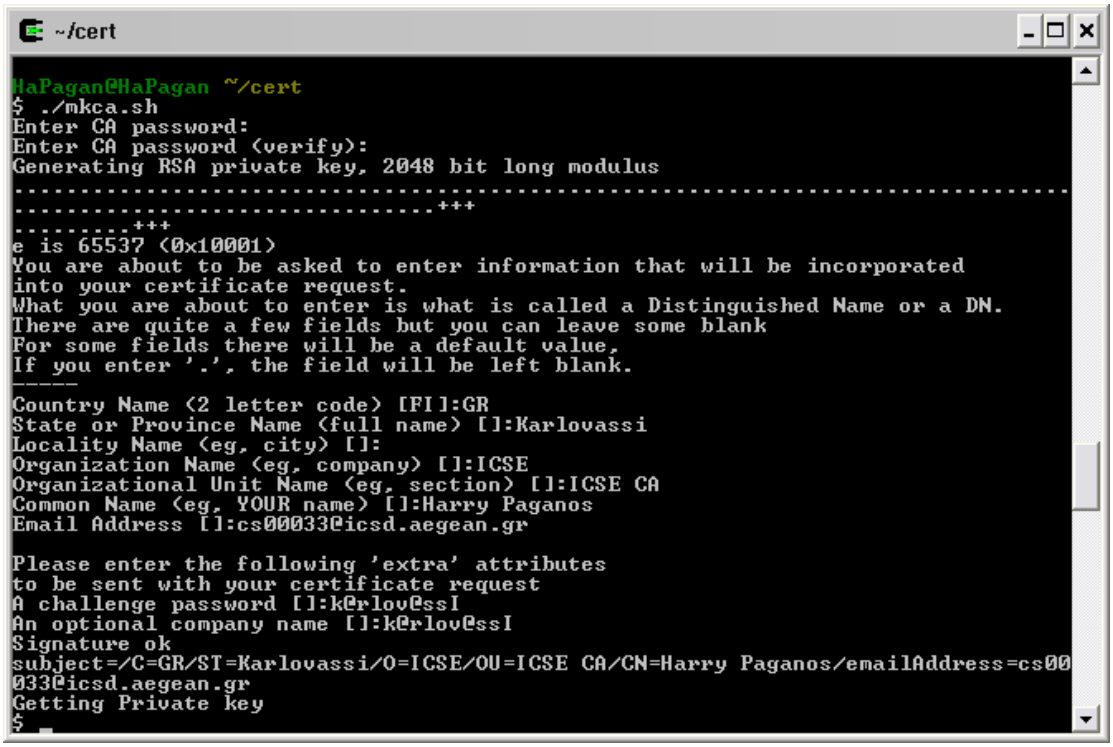


Εικόνα 9-11 Εφαρμογή πολιτικής ασφαλείας

συγκεκριμένη πολιτική ασφαλείας. Κάνουμε save την κονσόλα και πλέον είμαστε έτοιμοι να επικοινωνήσουμε μέσω IPsec.

Δημιουργία Αρχής Πιστοποίησης και Πιστοποιητικών Πελάτη

Για τις μετρήσεις που θα πραγματοποιήσουμε απαιτείται η χρήση αυθεντικοποίησης με χρήση πιστοποιητικών. Έτσι, πρέπει να δημιουργήσουμε τα δικά μας πιστοποιητικά (client certificates) αλλά και την δική μας αρχή πιστοποίησης (certification authority – CA) η οποία αναλαμβάνει να δημιουργήσει και να υπογράψει τα πιστοποιητικά των πελατών. Για τη δημιουργία των προαναφερθέντων θα χρησιμοποιήσουμε το πρόγραμμα OpenSSL [51] [52] [53] [54] [55] κάτω από το περιβάλλον του εξομοιωτή Cygwin [56] και πιο συγκεκριμένα κάποια scripts που δημιουργήθηκαν από τον Jarkko Turkulainen.

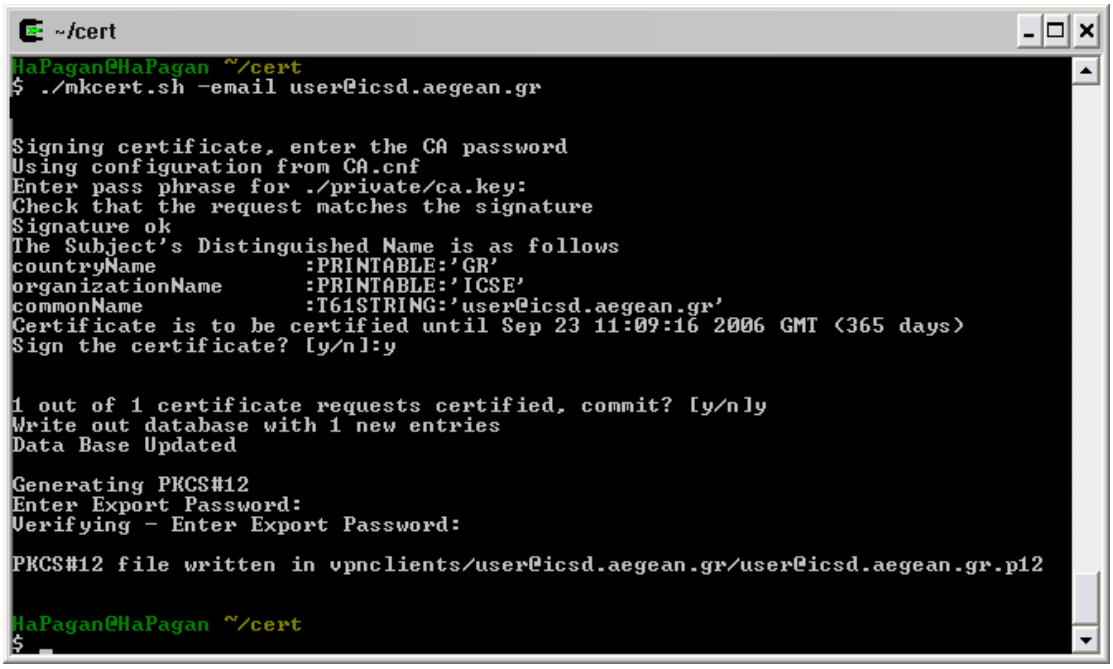


Εικόνα 9-12 Προετοιμασία της αρχής πιστοποίησης

Η πρώτη μας ενέργεια είναι η προετοιμασία της αρχής πιστοποίησης (CA). Έτσι, για αυτό τον σκοπό εκτελούμε το script με όνομα mkca.sh. Αρχικά, μας ζητείται να εισάγουμε ένα συνθηματικό το οποίο θα χρησιμοποιείται για την αυθεντικοποίησή μας όταν θα θέλουμε να υπογράψουμε κάποια πιστοποιητικά πελατών. Μετά την δημιουργία του RSA ιδιωτικού κλειδιού μας με μήκος 2048 bits, πρέπει να συμπληρώσουμε τα στοιχεία του CA. Η CA που μόλις παραμετροποιήσαμε έχει κάποια χαρακτηριστικά στοιχεία τα οποία είναι επιλεγμένα από το script που χρησιμοποιούμε αλλά μπορούμε να τα αλλάξουμε τροποποιώντας το αρχείο mkca.sh. Αυτά τα στοιχεία είναι το μήκος κλειδιού του CA, οι ημέρες μετά τις οποίες λήγει το πιστοποιητικό του CA αλλά και μερικά άλλα στοιχεία.

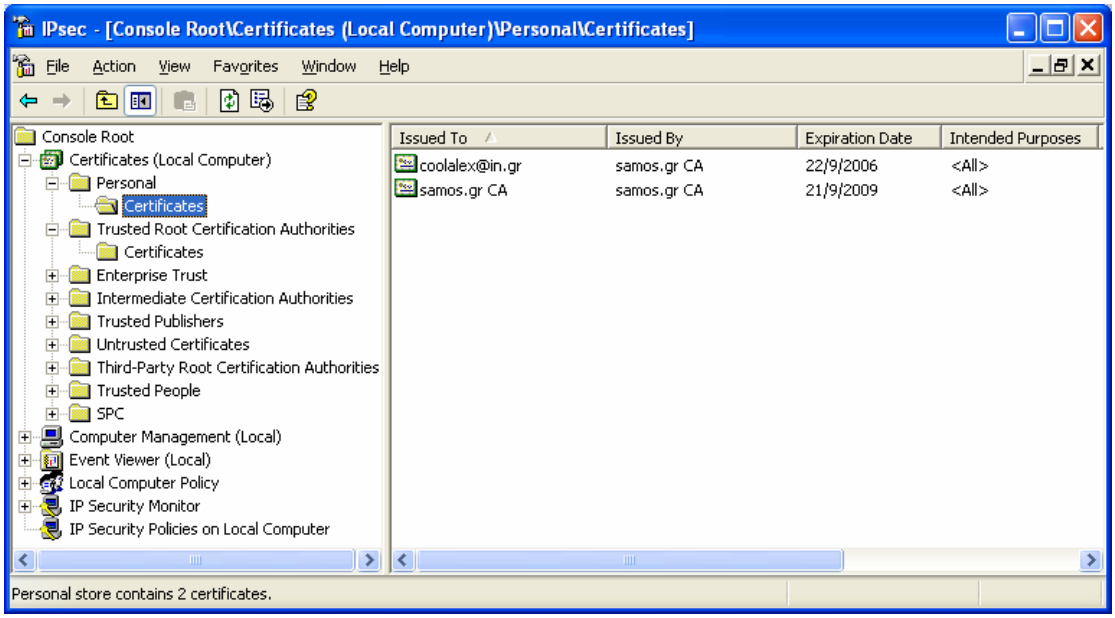
Η δημιουργία των πιστοποιητικών των πελατών είναι μια εύκολη διαδικασία. Εκτελούμε το script με όνομα mkcert.sh χρησιμοποιώντας την παράμετρο –email <client's_email>. Υπάρχει η δυνατότητα χρήσης των παραμέτρων –ip ή –dns αν

θέλουμε να δημιουργήσουμε πιστοποιητικό για κάποια πύλη (gateway). Πριν ακόμα, εκτελέσουμε το script θα ήταν καλό να τροποποιήσουμε το αρχείο mkcert.sh και πιο συγκεκριμένα τις ορισμένες μεταβλητές COUNTRY και ORGANISATION, καθώς έχουν τιμές άλλες από αυτές που θέλουμε να χρησιμοποιήσουμε. Απλά, βάζουμε ως τιμές τις αντίστοιχες τιμές που βάλαμε κατά τη δημιουργία της CA μας. Αυτό έχει σαν αποτέλεσμα, το πιστοποιητικό του χρήστη του παραδείγματος καθώς και το ιδιωτικό του κλειδί βρίσκονται αποθηκεμένα στον φάκελο /vpnclients/user@icsd.aegean.gr/.

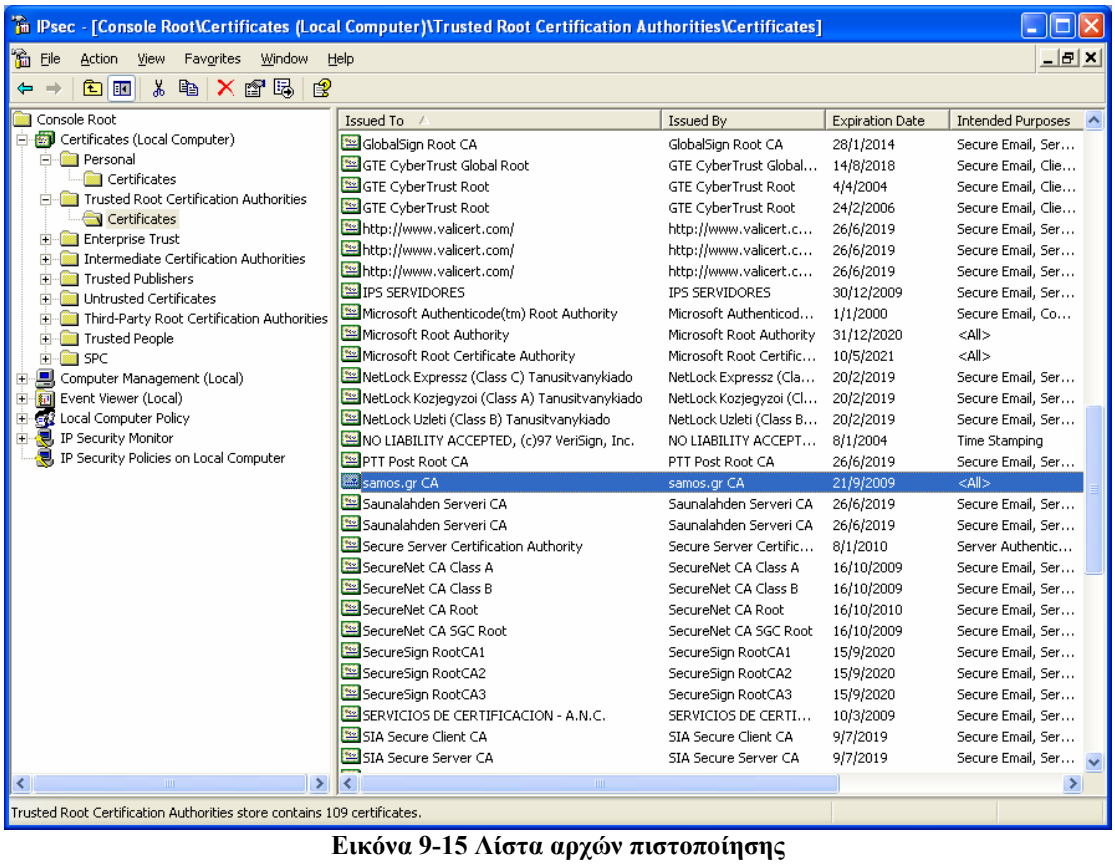


Εικόνα 9-13 Δημιουργία πιστοποιητικού πελάτη

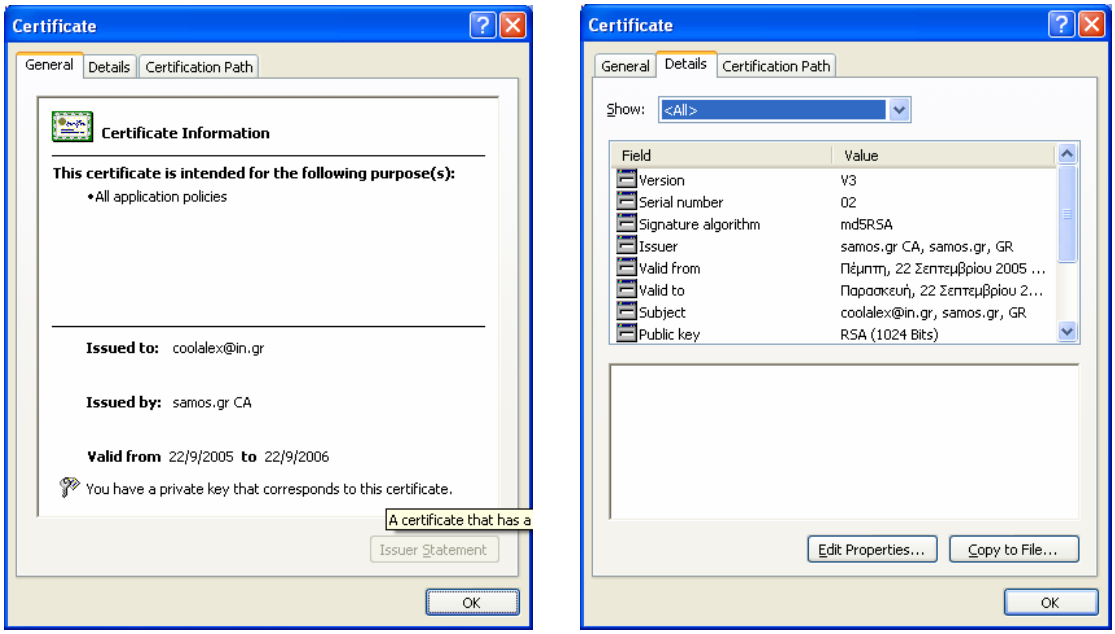
Κατόπιν η αρχή πιστοποίησης και τα αντίστοιχα πιστοποιητικά πρέπει να γίνουν import ώστε να είναι διαθέσιμα κατά την επιλογή τους ως μέθοδος αυθεντικοποίησης. Στο Certificates > Trusted Root Certification Authorities > Certificates κάνουμε import τη certification authority και στο Certificates > Personal > Certificates το προσωπικό πιστοποιητικό που δημιουργήσαμε μέσω της CA. Παρακάτω φαίνεται τόσο η αρχή πιστοποίησης όσο και το αντίστοιχο πιστοποιητικό.



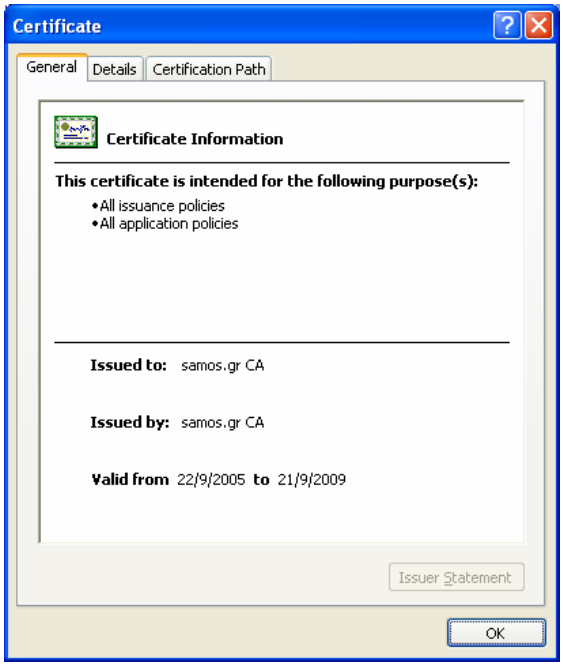
Εικόνα 9-14 Λίστα προσωπικών πιστοποιητικών



Εικόνα 9-15 Λίστα αρχών πιστοποίησης



Το πιστοποιητικό με τις λεπτομέρειές του

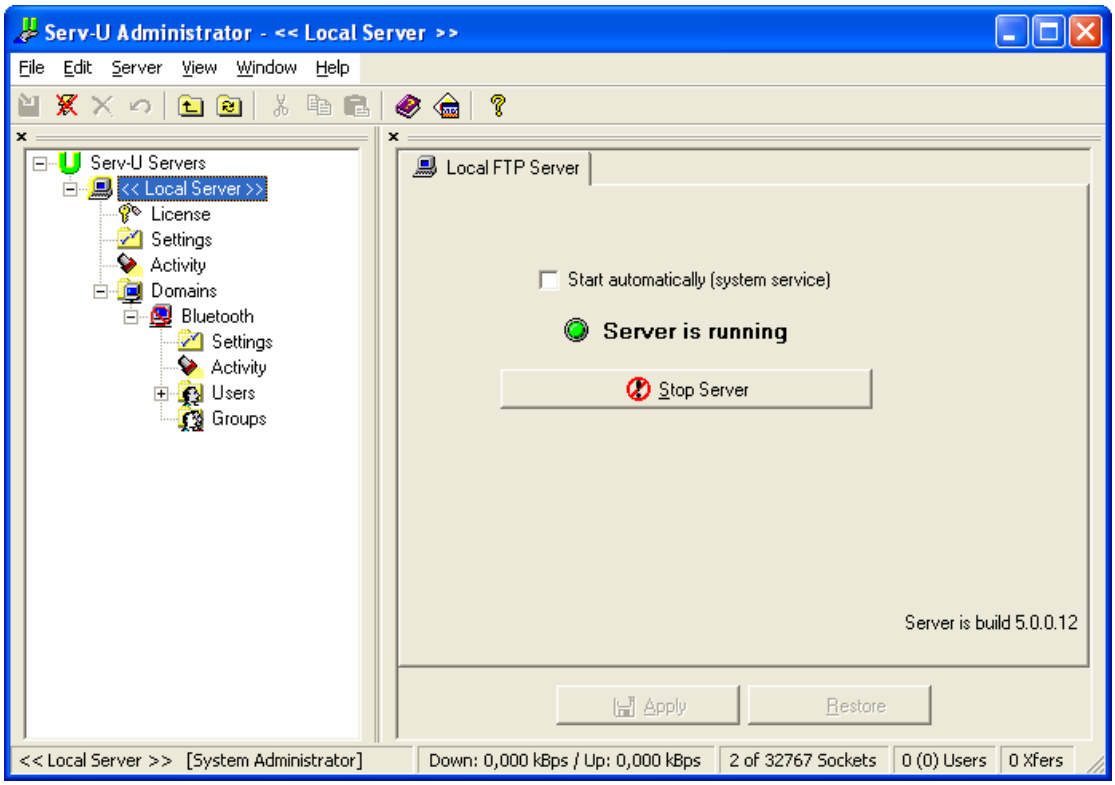


Εικόνα 9-16 Η αρχή πιστοποίησης

Κατόπιν, αφού κάναμε import όλα τα απαιτούμενα πιστοποιητικά, για να τα χρησιμοποιήσουμε ως μέθοδο αυθεντικοποίησης στο IP Security Policies και συγκεκριμένα στις ιδιότητες των μεθόδων αυθεντικοποίησης, επιλέγουμε "Use a certificate from this certification authority" και «φορτώνουμε» τη CA που δημιουργήσαμε από μια λίστα που μας εμφανίζεται. Είμαστε πλέον έτοιμοι να κάνουμε χρήση των δικών μας πιστοποιητικών.

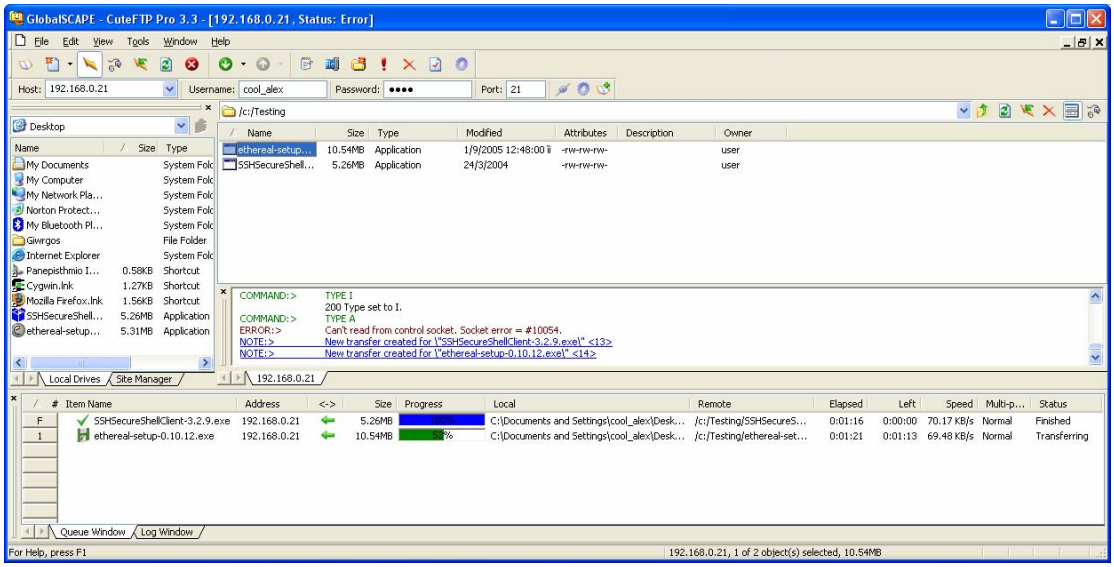
9.2.4 Προετοιμασία μετρήσεων

Έχουμε πλέον ολοκληρώσει με την εφαρμογή του IPsec στα συστήματά μας. Αυτό που υπολείπεται είναι ο τρόπος με τον οποίο θα πάρουμε τις μετρήσεις. Θα χρησιμοποιήσουμε το πρωτόκολλο ftp για τη μεταφορά των αρχείων από τον ένα υπολογιστή στον άλλον βασιζόμενοι στο μοντέλο εξυπηρέτη – πελάτη. Η μία συσκευή λοιπόν θα εκτελεί έναν ftp server και η άλλη έναν ftp client. Συγκεκριμένα, στον εξυπηρέτη θα εγκαταστήσουμε τον Serv-U FTP Server και στον πελάτη το CuteFTP Pro.



Εικόνα 9-17 Serv-U FTP Server

Ο πελάτης πρέπει να δηλώσει την IP διεύθυνση, το username και τον κωδικό του εξυπηρέτη στον ftp client ώστε να του επιτραπεί η σύνδεση. Πλέον έχει πρόσβαση στα αρχεία του server και μπορεί να κάνει μεταφορά με το πρωτόκολλο ftp.



Εικόνα 9-18 CuteFTP Pro

9.3 Secure Shell (SSH)

Το Secure Shell, ή πιο σύντομα SSH [57] [58], πρόκειται για ένα πρόγραμμα το οποίο αναλαμβάνει να διασφαλίσει την μετάδοση των δεδομένων μας στο επίπεδο μεταφοράς. Μπορεί να χρησιμοποιηθεί στη θέση προγραμμάτων, όπως είναι τα rlogin, rsh, rdist, καθώς παρέχει ισχυρή αυθεντικοποίηση και ασφαλή επικοινωνία μέσω μη ασφαλών διαύλων.

Υλοποιήθηκε από τον T. Ylonen από το Helsinki University of Technology της Φινλανδίας. Αυτή τη στιγμή υπάρχουν δυο εκδόσεις στην αγορά. Η πρώτη είναι ελεύθερη προς χρήση χωρίς κάποιο αντίτιμο και ο πηγαίος κώδικάς της είναι διαθέσιμος. Υπάρχει, όμως, και μια εμπορική έκδοση η οποία ενσωματώνει έναν αριθμό από επιπλέον χαρακτηριστικά, όπως είναι η δυνατότητα για ασφαλή χρήση του πρωτοκόλλου ftp το οποίο λέγεται sftp, αλλά και τεχνική υποστήριξη από την εταιρεία.

9.3.1 Διαδικασία εγκαθίδρυσης σύνδεσης με SSH

Θεωρούμε ένα παράδειγμα στο οποίο ένας υπολογιστής προσπαθεί να συνδεθεί με έναν εξυπηρέτη με χρήση του πρωτοκόλλου SSH. Ο εξυπηρέτης «ακούει» διαρκώς για συνδέσεις TCP/IP στην πόρτα 22. Ο πελάτης αποστέλλει μια αίτηση αυθεντικοποίησης στον εξυπηρετεί. Τότε, αυτός επιστρέφει στον πελάτη το δικό του κλειδί (host key) μήκους 1024 bits καθώς και ένα δημόσιο server key μήκους 768 bits το οποίο τροποποιείται κάθε εξήντα λεπτά. Το host key χρησιμοποιείται για τον καθορισμό της σύνδεσης με τον εκάστοτε εξυπηρέτη ενώ το server key για την αποφυγή αποκρυπτογράφησης των δεδομένων στην περίπτωση που το host key εκτεθεί. Μόλις ο πελάτης λάβει το host key, ελέγχει την εσωτερική του βάση δεδομένων των δημοσίων host κλειδιών. Αν δεν υπάρχει κάποια εγγραφή τότε

προστίθεται μια νέα με τα στοιχεία του εξυπηρέτη και εν συνεχεία αποστέλλει στον εξυπηρέτη ένα κρυπτογραφημένο τυχαίο κλειδί συνόδου μήκους 256 bits. Ο αλγόριθμος κρυπτογράφησης που χρησιμοποιείται είναι ένας από αυτούς που υποστηρίζονται από τον εξυπηρέτη: Blowfish, DES, 3DES. Μόλις λάβει ο εξυπηρέτης το κλειδί συνόδου, μπορούν και οι δυο πλευρές να επικοινωνήσουν με ασφάλεια (SSH). Προκειμένου να επιβεβαιωθεί το γεγονός ότι ο εξυπηρέτης κατάφερε να αποκρυπτογραφήσει το κλειδί συνόδου, αποστέλλει ένα κρυπτογραφημένο μήνυμα επιβεβαίωσης με το κλειδί συνόδου στον πελάτη.

Σε ορισμένες περιπτώσεις, απαιτείται η πιστοποίηση της ταυτότητας του πελάτη στον εξυπηρέτη. Η διαδικασία πιστοποίησης εκκινείται με την αποστολή από τον πελάτη στον εξυπηρέτη μιας αίτησης πιστοποίησης στην οποία αναφέρεται το όνομα του χρήστη που θέλει να συνδεθεί. Οι υποστηριζόμενες μέθοδοι στην έκδοση 1.0 του SSH είναι δυο:

- Αυθεντικοποίηση με συνθηματικό (password authentications): το συνθηματικό του πελάτη μεταδίδεται κρυπτογραφημένο από το SSH.
- Αυθεντικοποίηση με RSA: ο εξυπηρέτης αποστέλλει στον πελάτη έναν τυχαίο αριθμό κωδικοποιημένο με το δημόσιο κλειδί του πελάτη. Για να γίνει αυτό θα πρέπει ο εξυπηρέτης να έχει πρόσβαση σε μια βάση δεδομένων με τα δημόσια κλειδιά των χρηστών. Προκειμένου ο πελάτης για να είναι ικανός να αποκρυπτογραφήσει το εισερχόμενο μήνυμα θα πρέπει να γνωρίζει το αντίστοιχο ιδιωτικό κλειδί. Στη συνέχεια, ο πελάτης πρέπει να απαντήσει με μια σωστή MD5 σύνοψη του αποκρυπτογραφημένου μηνύματος συν κάποιων άλλων παραμέτρων. Τέλος, ο εξυπηρέτης απαντάει με ένα μήνυμα ανάλογα με το αν η αυθεντικοποίηση πραγματοποιήθηκε επιτυχώς ή όχι.

9.3.2 Secure Shell 2.0

Η τελευταία έκδοση του SSH αλλάζει σε μεγάλο βαθμό τον τρόπο με τον οποίο οργανώνεται το πρωτόκολλο. Ενώ στην έκδοση 1.0, όπως εξηγήσαμε παραπάνω, αναλύουμε το SSH ως ολότητα, πλέον στην δεύτερη έκδοση έχουμε την δημιουργία δυο ξεχωριστών τμημάτων: το πρωτόκολλο επιπέδου μεταφοράς SSH και το πρωτόκολλο αυθεντικοποίησης SSH.

Το πρωτόκολλο επιπέδου μεταφοράς SSH

Το πρωτόκολλο επιπέδου μεταφοράς SSH αναλαμβάνει την παροχή αυθεντικοποίησης του host, εμπιστευτικότητας και προστασίας των μεταδιδόμενων δεδομένων. Όπως αναφέρθηκε και προηγουμένως, δεν παρέχει αυθεντικοποίηση χρήστη καθώς αυτή την έχει αναλάβει εξολοκλήρου το πρωτόκολλο αυθεντικοποίησης SSH, το οποίο «κάθεται» πάνω από το πρωτόκολλο επιπέδου μεταφοράς SSH.

Πριν την εγκαθίδρυση μιας σύνδεσης με το πρωτόκολλο SSH, οι 2 πλευρές ανταλλάσουν πληροφορίες σχετικές με το λογισμικό που χρησιμοποιεί η κάθε μια αλλά και πληροφορίες αναγνώρισης ταυτότητας. Αρχικά, λοιπόν, δεν έχει οριστεί ούτε συμπίεση δεδομένων ούτε αλγόριθμος κρυπτογράφησης και αυθεντικοποίησης.

Κατά τη διάρκεια ανταλλαγής των κλειδιών, συμφωνούν και οι δυο πλευρές στο λογισμικό που θα χρησιμοποιήσουν στη σύνοδό τους. Στους παρακάτω πίνακες αναφέρονται οι αλγόριθμοι συμπίεσης, κρυπτογράφησης και αυθεντικοποίησης που μπορούν να εφαρμοστούν στο πρωτόκολλο SSH 2.0.

Αλγόριθμοι Συμπίεσης Δεδομένων	
Τιμή	**Περιγραφή**
Κανένας	Χωρίς συμπίεση
Zlib	GNU Zlib συμπίεση στο επίπεδο

Πίνακας 9-2 Αλγόριθμοι συμπίεσης δεδομένων

Αλγόριθμοι Κρυπτογράφησης	
Τιμή	**Περιγραφή**
Κανένας	Χωρίς κρυπτογράφηση
3DES	Three key Triple-DES
IDEA	IDEA
ARCFOUR	Arcfour stream cipher
Blowfish	Blowfish

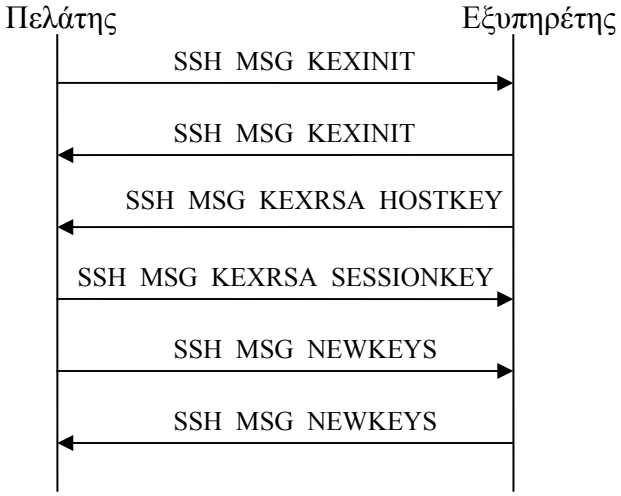
Πίνακας 9-3 Αλγόριθμοι κρυπτογράφησης

Αλγόριθμοι Αυθεντικοποίησης	
Τιμή	**Περιγραφή**
Κανένας	Χωρίς χρήση MAC
Hmac-md5	HMAC-MD5
Hmac-sha	HMAC-SHA
Md5-8	8 πρώτα bits του κλειδιού MD5 + data + key
Sha-8	8 πρώτα bits του κλειδιού SHA + data + key
SHA	Κλειδί SHA + data + key

Πίνακας 9-4 Αλγόριθμοι αυθεντικοποίησης

Με τον όρο MAC αναφερόμαστε στον κώδικα αυθεντικοποίησης μηνύματος. Ο MAC ενσωματώνεται σε κάθε μήνυμα SSH. Υπολογίζεται λαμβάνοντας υπόψιν ένα κοινό μυστικό κλειδί, ένα αριθμό 32 bits καθώς και το περιεχόμενο του μηνύματος.

Στο παρακάτω διάγραμμα απεικονίζεται η αλληλουχία των μηνυμάτων κατά την εκτέλεση του πρωτοκόλλου επιπέδου μεταφοράς SSH. Τα πρώτα δυο μηνύματα που ανταλλάσσονται περιέχουν την λίστα με τους επιθυμητούς αλγόριθμους συμπίεσης, κρυπτογράφησης και αυθεντικοποίησης. Ο εκάστοτε πρώτος αλγόριθμος στη λίστα του πελάτη είναι αυτός που τελικά χρησιμοποιείται, αν φυσικά υποστηρίζεται από τον εξυπηρέτη. Με το επόμενο μήνυμα, ο εξυπηρέτης εκκινεί τη διαδικασία ανταλλαγής κλειδιών. Τότε, ο πελάτης αποστέλλει ένα μήνυμα του τύπου *SSH_MSG_KEXRSA_SESSIONKEY* με το οποίο εξακριβώνει ότι το παρόν host κλειδί ανήκει στον εξυπηρέτη. Στη συνέχεια, ο πελάτης αποστέλλει στον εξυπηρέτη το μήνυμα του τύπου *SSH_MSG_KEXRSA_SESSIONKEY* το οποίο περιέχει το κλειδί συνόδου. Τα δυο τελευταία μηνύματα που ανταλλάσσονται χρησιμοποιούν τους παλαιούς αλγόριθμους και κλειδιά και δηλώνουν ότι από αυτό το σημείο και μετά θα χρησιμοποιούνται μόνο τα καινούργια.



Εικόνα 9-19 Αλληλουχία μηνυμάτων στο πρωτόκολλο μεταφοράς SSH

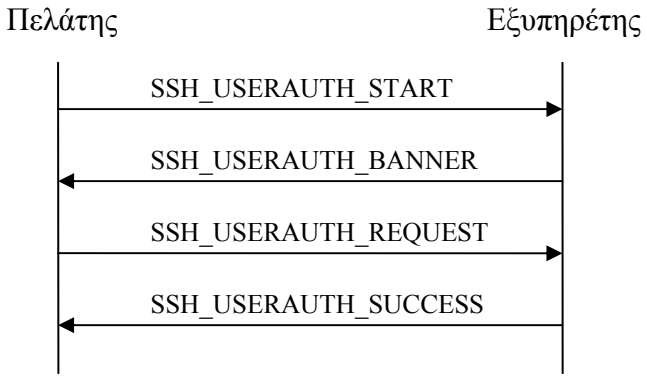
Το πρωτόκολλο αυθεντικοποίησης SSH

Το πρωτόκολλο αυθεντικοποίησης SSH βρίσκεται πάνω από το πρωτόκολλο επιπέδου μεταφοράς SSH. Η διαδικασία εκκινείται με την αποστολή από τον πελάτη στον εξυπηρέτη του ονόματος της υπηρεσίας που θέλει να χρησιμοποιήσει και του ονόματος του χρήστη. Στη συνέχεια, ο εξυπηρέτης απαντάει με μια λίστα με τις διαθέσιμες μεθόδους αυθεντικοποίησης και ο πελάτης επιστρέφει μια παρόμοια λίστα. Η συζήτηση συνεχίζεται έως ότου η πρόσβαση επιτραπεί ή απορριφθεί. Στον παρακάτω πίνακα παρουσιάζονται οι μέθοδοι αυθεντικοποίησης που υποστηρίζονται από το SSH.

Τιμή	**Μέθοδος Αυθεντικοποίησης**
Password	Αυθεντικοποίηση με χρήση συνθηματικού
Secured	SecurID αυθεντικοποίηση
Sey	S/Key one-time password αυθεντικοποίηση
Oie	OPIE one-time password αυθεντικοποίηση
Publickey	Κατοχή του ιδιωτικού κλειδιού
Hostbased	Ταυτότητα του host πελάτη και του χρήστη
Kerberos4	Kerberos V4 αυθεντικοποίηση
Kerberos5	Kerberos V5 αυθεντικοποίηση
Kerberos-afs	AFS Kerberos αυθεντικοποίηση

Πίνακας 9-5 Μέθοδοι αυθεντικοποίησης του χρήστη

Παρακάτω, παρουσιάζεται σχηματικά η διαδικασία αυθεντικοποίησης ενός χρήστης στο επίπεδο αυθεντικοποίησης SSH. Αρχικά, ο πελάτης αποστέλλει ένα μήνυμα *SSH_USERAUTH_START* με το οποίο εκκινεί τη διαδικασία. Ο εξυπηρέτης απαντάει με ένα μήνυμα



Εικόνα 9-20 Διαδικασία αυθεντικοποίησης του χρήστη στο επίπεδο αυθεντικοποίησης SSH

του τύπου *SSH_USERAUTH_BANNER* το οποίο περιέχει ένα μήνυμα που θα εμφανιστεί στον χρήστη που θέλει να αυθεντικοποιηθεί. Στη συνέχεια, ο πελάτης αποστέλλει ένα μήνυμα του τύπου *SSH_USERAUTH_REQUEST* με το οποίο δημοσιοποιεί στον εξυπηρέτη κάποια χαρακτηριστικά του χρήστη (αναγνωριστικό ταυτότητας) καθώς και ποια μέθοδο αυθεντικοποίησης επιθυμεί να εφαρμόσουν. Τέλος και ανάλογα με την εξέλιξη των διαπραγματεύσεων μεταξύ των δυο πλευρών ο εξυπηρέτης αποστέλλει ένα μήνυμα του τύπου *SSH_USERAUTH_SUCCESS* αν όλα έχουν πάει καλά αλλιώς ένα μήνυμα του τύπου *SSH_USERAUTH_FAILURE*.

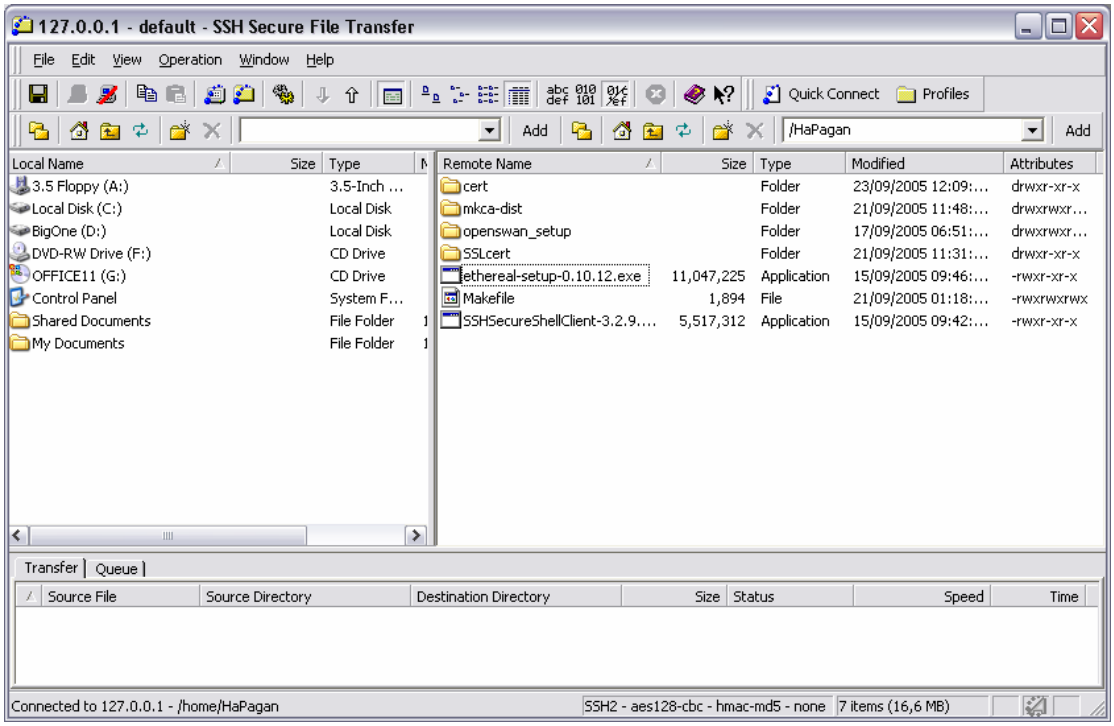
9.3.3 Προγράμματα που χρησιμοποιήθηκαν

Οι μετρήσεις πραγματοποιήθηκαν με την λογική της επικοινωνίας πελάτη–εξυπηρέτη [59]. Έτσι, ο ένας προσωπικός υπολογιστής έπαιζε τον ρόλο του πελάτη εκτελώντας το αντίστοιχο πρόγραμμα SSH Client ενώ ο άλλος εκτελούσε το πρόγραμμα του SSH Server.

Πιο συγκεκριμένα, χρησιμοποιήσαμε το πρόγραμμα cygwin το οποίο εξομοιώνει το περιβάλλον του λειτουργικού συστήματος Unix στα Windows, και σε συνεργασία με το λογισμικό OpenSSH μπορέσαμε να εγκαταστήσουμε και να χρησιμοποιήσουμε έναν SSH Server. Το OpenSSH παρέχει υποστήριξη για αυθεντικοποίηση του χρήστη με ζεύγος δημοσίου-ιδιωτικού κλειδιού, συνθηματικού και πιστοποιητικών. Μάλιστα, με τη χρήση κάποιων βοηθητικών προγραμμάτων παρέχεται η δυνατότητα για δημιουργία κλειδιών RSA [60]. Έτσι, η διαδικασία επιλογής μεθόδου αυθεντικοποίησης και παραγωγής των κλειδιών είναι αρκετά απλή. Στη συνέχεια, αρκεί η εγκατάσταση ενός προγράμματος πελάτη το οποίο θα αναλάβει τη διαδικασία σύνδεσης και μεταφοράς των αρχείων από τον απομακρυσμένο εξυπηρέτη.

Στο πρόγραμμα πελάτη, μπορούμε να ορίσουμε τον αλγόριθμο κρυπτογράφησης που επιθυμούμε να χρησιμοποιήσουμε καθώς και τον αλγόριθμο αυθεντικοποίησης. Μόλις γίνει η συνεννόηση μεταξύ των δυο υπολογιστών και αν ο εξυπηρέτης υποστηρίζει τους επιλεγμένους αλγόριθμους τότε ο πελάτης συνδέεται και είναι έτοιμος να μεταφέρει τα αρχεία που επιθυμεί. Στην παρούσα εργασία χρησιμοποιήθηκε το πρόγραμμα SSH Secure File Transfer για την πραγματοποίηση της αντιγραφής των αρχείων από τον απομακρυσμένο κόμβο. Μπορούμε να παρατηρήσουμε ότι στο κάτω μέρος του παραθύρου του προγράμματος και μετά την σύνδεση, εμφανίζεται ο αλγόριθμος κρυπτογράφησης (aes128-cbc), η χρήση

συμπίεσης των δεδομένων (none) αλλά και ο αλγόριθμος αυθεντικοποίησης (hmac-md5).



Εικόνα 9-21 SSH Secure File Transfer

Εγκατάσταση και χρήση του cygwin

Ένα πολύ σημαντικό στοιχείο που πρέπει να προσεχθεί κατά τη διάρκεια της εγκατάστασης του cygwin είναι ότι θα πρέπει να επιλεγεί το πακέτο OpenSSH με το οποίο μπορούμε να ενεργοποιήσουμε τη δυνατότητα χρήσης του SSH στις συνδέσεις μας. Στη συνέχεια και πριν τρέξουμε για πρώτη φορά το πρόγραμμα, πρέπει να ορίσουμε ορίσουμε μια νέα μεταβλητή συστήματος με όνομα CYGWIN και την τιμή ntsec tty. Επίσης, πρέπει να προσθέσουμε στο path του λειτουργικού συστήματος την πλήρη διαδρομή στην οποία βρίσκεται ο φάκελος bin του cygwin. Πλέον, είμαστε έτοιμοι να εκτελέσουμε το πρόγραμμα.

Η πρώτη κίνησή μας είναι να ρυθμίσουμε κατάλληλα τον εξυπηρέτη ssh. Για αυτό το σκοπό εκτελούμε την εντολή *ssh-host-config*, η οποία μας θέτει κάποια ερωτήματα. Το βασικό είναι να αποδεχτούμε ότι ο δαίμονας του SSH θα εκτελείται

Εικόνα 9-22 Εκκίνηση και τερματισμός του ssh δαίμονα

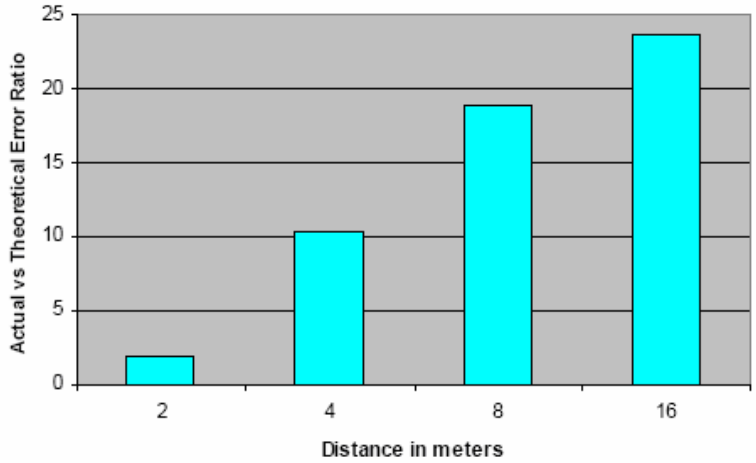
ως υπηρεσία των Windows. Στη συνέχεια για να εκτελέσουμε τον δαίμονα, απλά πληκτρολογούμε την εντολή *net start sshd* ή *cygrunsrv –start sshd.* Το πρόγραμμα τερματίζεται βάζοντας stop αντί για start στις προηγούμενες εντολές.

Αφού έχουμε ρυθμίσει και εκτελέσει τον εξυπηρέτη SSH μπορούμε να συνδεθούμε σε αυτόν με την χρήση κάποιων προγραμμάτων-πελατών. Το cygwin παρέχει αυτή τη δυνατότητα. Έτσι, εκτελώντας την εντολή *ssh $USERNAME@127.0.0.1* πραγματοποιείται μια απομακρυσμένη σύνδεση με τον εξυπηρέτη. Μπορούμε επίσης να χρησιμοποιήσουμε την εντολή *sftp $USERNAME@127.0.0.1* και να συνδεθούμε με ένα ασφαλές πρωτόκολλο μεταφοράς αρχείων.

9.4 Σχετικές εργασίες στη συγκεκριμένη ερευνητική περιοχή

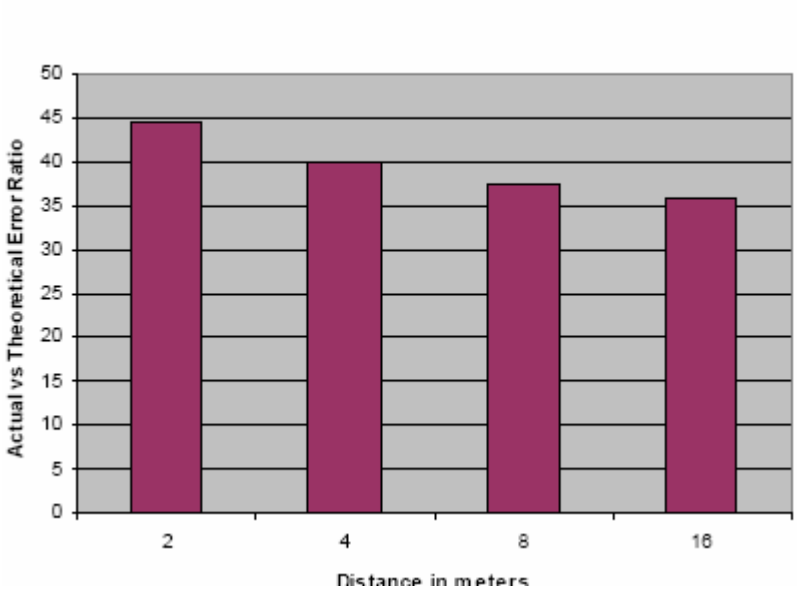
Πριν προχωρήσουμε στην παρουσίαση των γραφικών παραστάσεων και των πινάκων που εξάγαμε από τις μετρήσεις που πραγματοποιήσαμε, θα αναφερθούμε σε κάποιες σχετικές εργασίες πάνω στο πεδίο της αξιολόγησης της απόδοσης του πρωτοκόλλου Bluetooth. Οι περισσότερες από αυτές ασχολούνται με την αξιολόγηση της απόδοσης του πρωτοκόλλου Bluetooth σε συνδυασμό με την ύπαρξη στην περιοχή ενός ασυρμάτου δικτύου WLAN. Επίσης, ένας αριθμός άλλων εργασιών εξετάζουν την επίδοση σε επίπεδο προσομοίωσης και όχι πραγματικών συνθηκών.

Η πρώτη εργασία στην οποία θα αναφερθούμε, ασχολείται όπως φαίνεται και από τον τίτλο της με την αξιολόγηση της απόδοσης των Bluetooth-enabled δικτύων αλλά και με την απόδοση αυτών όταν συνυπάρχουν στο ίδιο περιβάλλον με ασύρματα δίκτυα 802.11 [61]. Οι δείκτες αξιολόγησης που εξετάζονται, είναι το throughput σε bit/sec και ο ρυθμός σφαλμάτων ανάλογα με την απόσταση των δυο κόμβων. Το αποτέλεσμα που εξάγεται είναι ότι με την αύξηση της απόστασης, αυξάνεται και ο ρυθμός των σφαλμάτων, όπως φαίνεται χαρακτηριστικά και στο παρακάτω γράφημα.



Γράφημα 9-1 Ρυθμός σφαλμάτων ανάλογα με την απόσταση (Bluetooth)

Εξετάζοντας τον ίδιο δείκτη στην περίπτωση της παρεμβολής με ένα δίκτυο 802.11 παρατηρούμε ότι ο ρυθμός σφαλμάτων μειώνεται με την αύξηση της απόστασης μεταξύ των κόμβων.



Γράφημα 9-2 Ρυθμός σφαλμάτων ανάλογα με την απόσταση (Bluetooth vs 802.11)

Άλλη μια εργασία που ασχολείται με το θέμα της απόδοσης σε περιβάλλον συνύπαρξης του Bluetooth με το WLAN [62]. Πιο συγκεκριμένα εξετάζει την απόδοση σχετικά με το TCP. Τα αποτελέσματα εξάγονται σε περιβάλλον προσομοίωσης και κυρίως λαμβάνονται υπόψη τρεις δείκτες: χάσιμο πακέτων, TCP throughput και η καθυστέρηση.

Στο ίδιο πεδίο αλλά με άλλο στοιχείο υπό παρακολούθηση ασχολείται η [63]. Χρησιμοποιεί το πρόγραμμα προσομοίωσης του Πανεπιστημίου του Berkeley Network Simulator (ns). Το πιο σημαντικό συμπέρασμα της εργασίας είναι ότι το μέγεθος των πακέτων UDP μπορεί να επηρεάσει την απόδοση ενός Bluetooth δικτύου. Επίσης, όσο μεγαλύτερη είναι η συχνότητα της αναζήτησης πληροφοριών (πχ αναζήτηση νέων συσκευών) τόσο χειρότερο είναι το throughput.

Η εργασία [64] προτείνει μια λύση στο πρόβλημα απόδοσης που παρατηρείται σε περιβάλλοντα συνύπαρξης του πρωτοκόλλου Bluetooth με το 802.11. Τα αριθμητικά αποτελέσματα δείχνουν ότι η προτεινόμενη λύση προσφέρει 100% βελτίωση της απόδοσης κατά την μετάδοση raw δεδομένων και 51-85% κατά την μεταφορά αρχείων με χρήση του πρωτοκόλλου ftp.

Η επόμενη εργασία εξετάζει την απόδοση ενός Bluetooth piconet στην περίπτωση που χρησιμοποιούνται όχι μία αλλά πολλές σχισμές (slots) για την αποστολή των πακέτων. Τέλος, συγκρίνει τα αποτελέσματα των μετρήσεων τόσο για μία όσο και για πολλές σχισμές με βάση διάφορες παραμέτρους (πχ χρησιμοποίηση καναλιού) [65].

Η τελευταία εργασία [66] εξετάζει την απόδοση σε συσχετισμό με το πρωτόκολλο MAC του Bluetooth, το L2CAP. Αρχικά, η απόδοση αυτού αναλύθηκε χρησιμοποιώντας ένα αναλυτικό μοντέλο του οποίου τα αποτελέσματα μετά συγκρίθηκαν με τα αποτελέσματα μιας προσομοίωσης.

ΚΕΦΑΛΑΙΟ 10

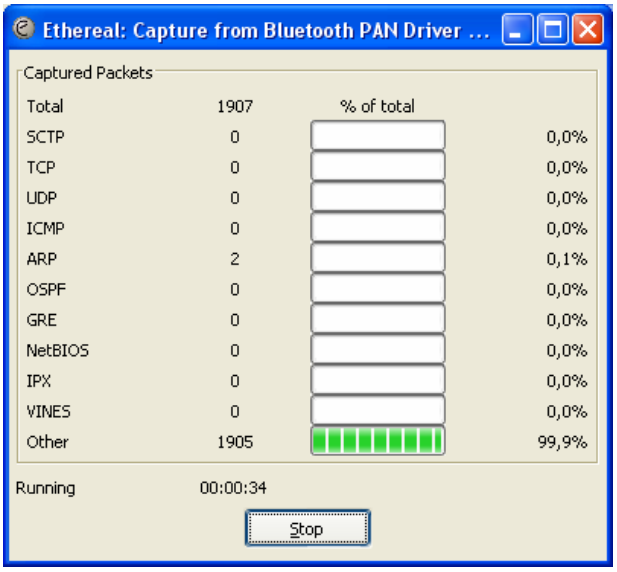
ΜΕΤΡΗΣΕΙΣ, ΣΥΓΚΡΙΤΙΚΟΙ ΠΙΝΑΚΕΣ ΚΑΙ ΓΡΑΦΗΜΑΤΑ

10.1 Εισαγωγή

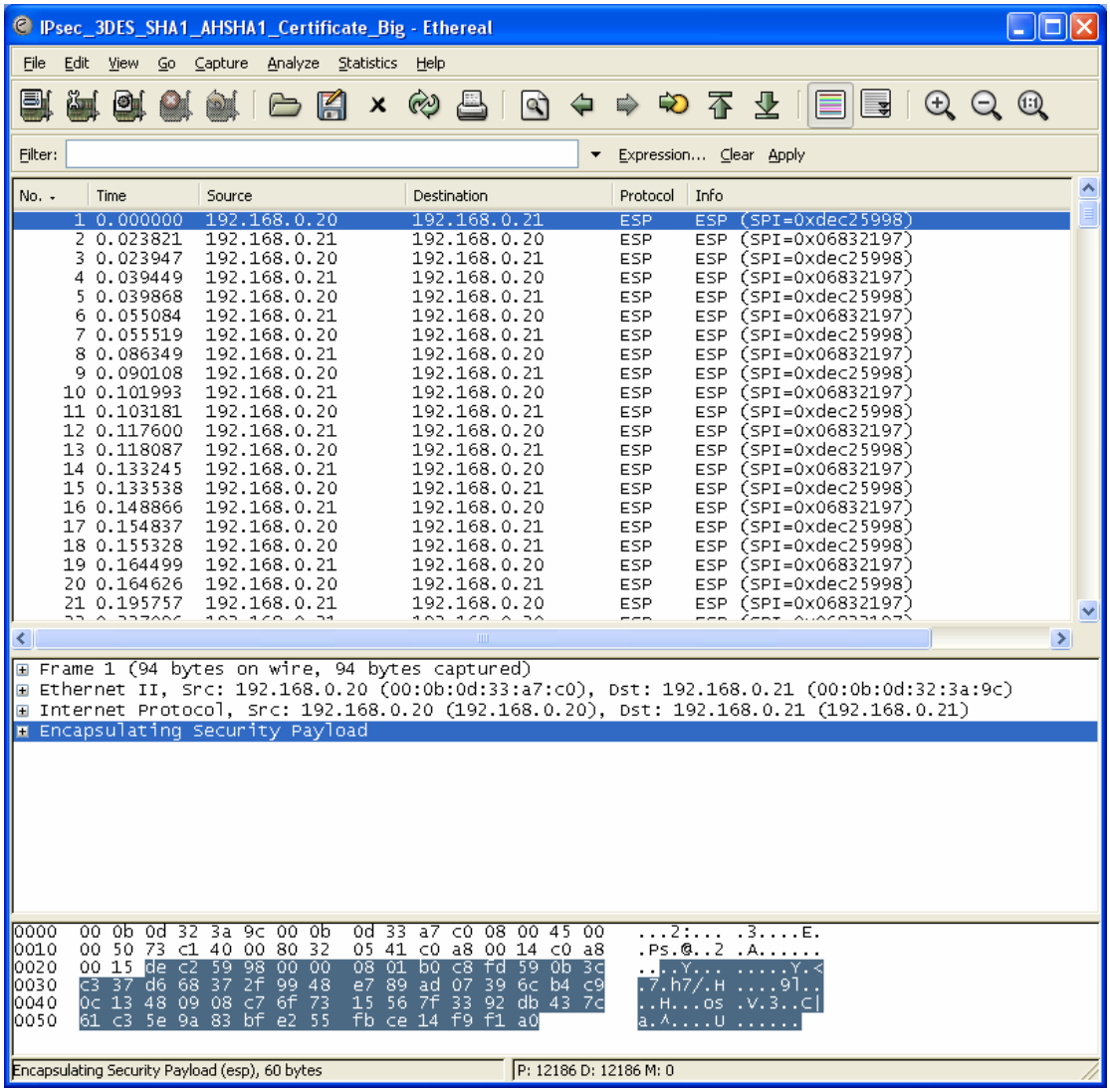
Οι συνδέσεις με Bluetooth security modes, IPsec ή SSH έχουν δημιουργηθεί, όπως περιγράψαμε στο προηγούμενο κεφάλαιο, και πλέον είμαστε έτοιμοι να πάρουμε τις μετρήσεις. Για κάθε μία από τις τρεις αυτές τεχνολογίες ασφαλείας, θα εφαρμόσουμε όλους τους δυνατούς συνδυασμούς κρυπτογράφησης και αυθεντικοποίησης. Μάλιστα, κάθε μέτρηση με τις αντίστοιχες παραμέτρους ασφαλείας θα πραγματοποιηθεί με τη χρησιμοποίηση δύο αρχείων διαφορετικού μεγέθους ώστε να βγάλουμε πιο αξιόπιστα αποτελέσματα. Συγκεκριμένα, θα χρησιμοποιήσουμε τα αρχεία SSHSecureShellClient-3.2.9.exe (μικρό) και ethereal-setup-0.10.12.exe (μεγάλο) που έχουν μέγεθος 5,26 και 10,5 MB αντίστοιχα. Για την περίπτωση των καταστάσεων ασφαλείας θα χρησιμοποιηθούν δυο επιπλέον αρχεία μεγέθος 7 και 15 MB αντίστοιχα.

Θα μεταφέρουμε, λοιπόν, το αρχείο από τον έναν υπολογιστή στον άλλον και κατά τη διάρκεια της μεταφοράς θα χρησιμοποιούμε ένα network analyzer πρόγραμμα έτσι ώστε να βλέπουμε τα πακέτα που μεταφέρονται και να παρακολουθούμε την κίνηση του δικτύου. Για το σκοπό αυτό θα χρησιμοποιήσουμε το Ethereal v 0.10.12 για το οποίο υπάρχει η δυνατότητα εγκατάστασής του τόσο σε λειτουργικό σύστημα Windows όσο και σε Linux και που είναι open source λογισμικό [67].

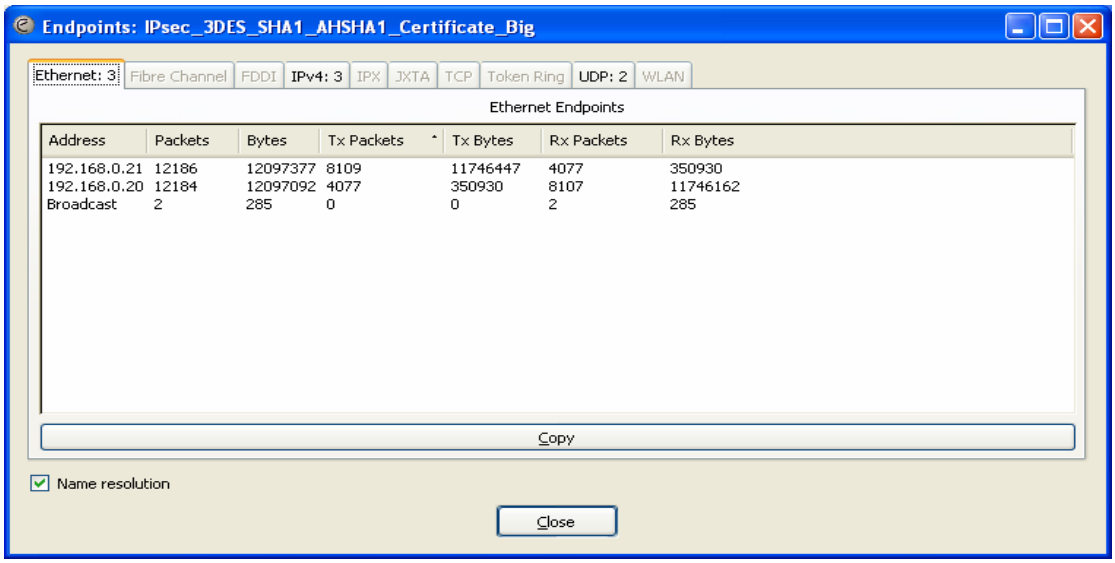
Στην συνέχεια βλέπουμε άποψη του Ethereal. Στην πρώτη εικόνα γίνεται σύλληψη των πακέτων κατά τη μεταφορά του αρχείου στο Bluetooth PAN και στη δεύτερη φαίνονται τα πακέτα που συλλάβαμε. Στη συγκεκριμένη περίπτωση μεταφέραμε το μεγάλο αρχείο εφαρμόζοντας IPsec με αυθεντικοποίηση μέσω ψηφιακών πιστοποιητικών, Authentication Header (AH) με τον αλγόριθμο SHA1 και Encapsulating Security Payload (ESP) με 3DES για κρυπτογράφηση και SHA1 για ακεραιότητα. Φαίνεται μάλιστα το ενθυλακωμένο ωφέλιμο φορτίο του πακέτου. Στην τρίτη και τέταρτη εικόνα παρουσιάζονται κάποια στατιστικά στοιχεία για τη συγκεκριμένη μεταφορά αρχείου.



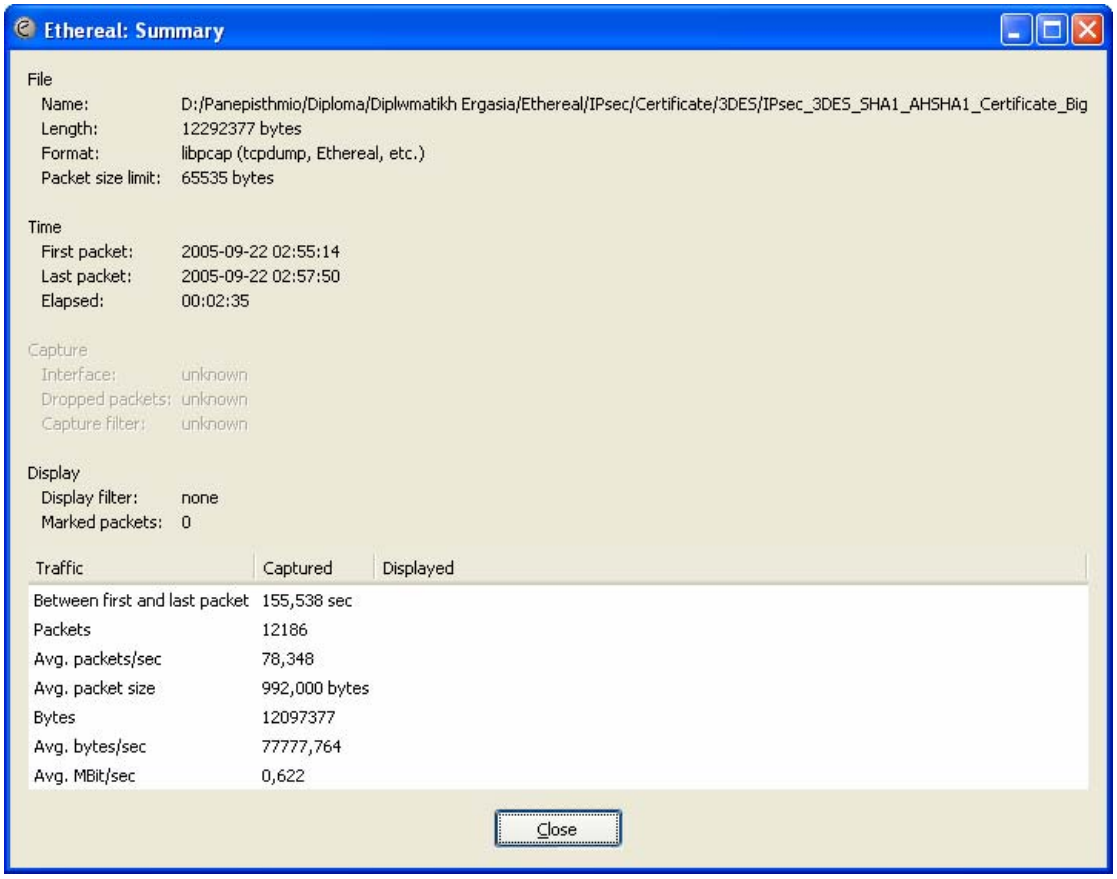
Εικόνα 10-1 Σύλληψη πακέτων μέσω του Ethereal



Εικόνα 10-2 Τα πακέτα της μεταφοράς και η δομή τους



Εικόνα 10-3 Ο αριθμός των Bytes και πακέτων που μεταφέρθηκαν



Εικόνα 10-4 Σύντομα στατιστικά στοιχεία

Με βάση τα στατιστικά στοιχεία που παρέχονται από το Ethereal, θα εκτιμήσουμε την απόδοση του δικτύου Bluetooth σε συνάρτηση με τις τεχνολογίες ασφαλείας που εφαρμόζουμε κάθε φορά. Η εκτίμηση της επίδοσης του PAN θα γίνει υπολογίζοντας 5 βασικές παραμέτρους ενός δικτύου:

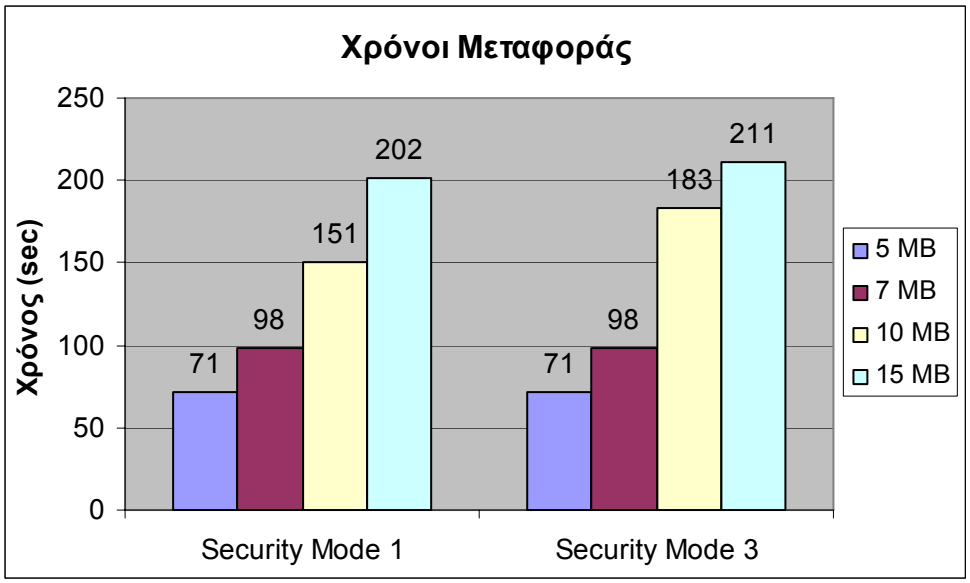
- Χρόνος μεταφοράς
- Εύρος ζώνης (Bandwidth)
- Καθυστέρηση (Latency)
- Χρησιμοποίηση δικτύου (Utilization)
- Throughput

10.2 Καταστάσεις ασφαλείας Bluetooth

Σε αυτή την ενότητα, θα ασχοληθούμε με την ανάλυση των πέντε βασικών δεικτών αξιολόγησης ενός δικτύου σε συνδυασμό με την εκάστοτε κατάσταση ασφαλείας Bluetooth που εφαρμόζεται. Έτσι, θα εξετάσουμε τον χρόνο μεταφοράς των τεσσάρων αρχείων, το εύρος ζώνης, την καθυστέρηση, την χρησιμοποίηση του δικτύου και το throughput. Στο τέλος, θα εξάγουμε ένα συμπέρασμα για το ποια κατάσταση ασφαλείας είναι πιο αποδοτική.

10.2.1 Χρόνος μεταφοράς

Σε αυτή την υποενότητα, θα ασχοληθούμε με ένα πολύ σημαντικό χαρακτηριστικό του δικτύου μας που δεν είναι άλλο από τον χρόνο μεταφοράς τεσσάρων αρχείων διαφορετικού μεγέθους (βλ ενότητα 10.1). Ο χρόνος αποτελεί έναν από τους δείκτες που θα εξετάσουμε κατά την αξιολόγηση της απόδοσης του δικτύου μας. Παρακάτω, παρουσιάζεται μια γραφική παράσταση που μας δείχνει τον χρόνο μεταφοράς των τεσσάρων αρχείων ανάλογα με την κατάσταση ασφαλείας που έχει επιλεγεί.



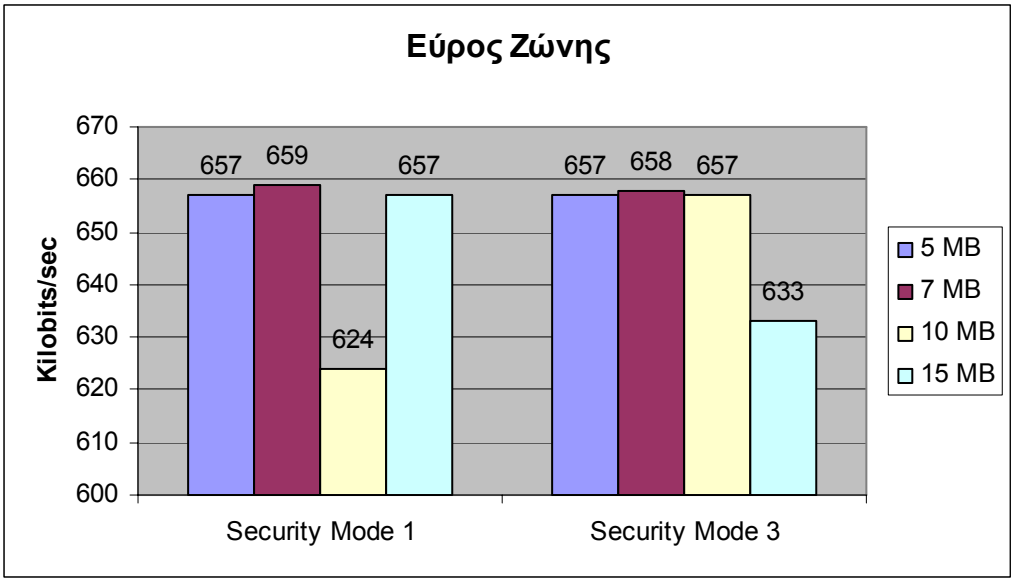
Γράφημα 10-1 Χρόνοι μεταφοράς αρχείων ανάλογα την κατάσταση ασφαλείας

Παρατηρούμε λοιπόν, ότι έχοντας επιλέξει την κατάσταση ασφαλείας 3 η μεταφορά του μεγάλου αρχείου (μεγέθους 15MB) γίνεται πιο αργά από ότι με την κατάσταση ασφαλείας 1. Αυτό θεωρείται λογικό αφού η κατάστασης ασφαλείας 3 απαιτεί την εφαρμογή κρυπτογράφησης και αυθεντικοποίησης. Μια σημαντική παρατήρηση είναι ότι για τα δυο αρχείο με μέγεθος 5 και 7 MB οι χρόνοι μεταφοράς παραμένουν ίδιοι είτε χρησιμοποιείται κατάσταση ασφαλείας 1 είτε κατάσταση ασφαλείας 3.

10.2.2 Εύρος ζώνης

Εύρος ζώνης σε ένα δίκτυο ονομάζουμε την ταχύτητα, σε bits/sec συνήθως, με την οποία μεταδίδονται τα δεδομένα. Το χρησιμοποιούμενο εύρος ζώνης μεταξύ δυο κόμβων του δικτύου μπορεί να επηρεάσει σημαντικά την απόδοση του. Σε ένα ιδανικό δίκτυο το εύρος ζώνης θα παρέμενε σταθερό αλλά φυσικά δεν υπάρχει κάτι τέτοιο και το εύρος ζώνης επηρεάζεται από πολλούς παράγοντες με αποτέλεσμα να μη διατηρεί μια σταθερή τιμή.

Παρακάτω, θα δούμε μια γραφική παράσταση που παρουσιάζει το εύρος ζώνης κατά την μεταφορά τεσσάρων αρχείων διαφορετικού μεγέθους ανάλογα με την κατάσταση ασφαλείας που έχει επιλεχτεί (βλ ενότητα 10.1).



Γράφημα 10-2 Εύρος ζώνης ανάλογα με την κατάσταση ασφαλείας

Στην αριστερή μεριά του γραφήματος βλέπουμε τις τιμές του εύρους ζώνης για την κατάσταση ασφαλείας 1 και δεξιά για την κατάσταση ασφαλείας 3. Παρατηρούμε γενικά ότι υπάρχει μια σταθερότητα του εύρους ζώνης η τιμή του οποίου ισούται περίπου με 657 kbps. Εξαιρέσεις αποτελούν οι περιπτώσεις της μεταφοράς του αρχείου μεγέθους 10MB με κατάσταση ασφαλείας 1 και του αρχείου μεγέθους 15MB με κατάσταση ασφαλείας 3 για τις οποίες το εύρος ζώνης είναι 624 και 633 kbps αντίστοιχα. Ειδικότερα, για τα δυο μικρά αρχεία μεγέθους 5 και 7 MB βλέπουμε ότι το εύρος ζώνης παραμένει σταθερό είτε εφαρμόζεται η κατάσταση ασφαλείας 1 είτε η κατάσταση ασφαλείας 3.

10.2.3 Καθυστέρηση

Για να αποκτήσουμε μια περισσότερο ξεκάθαρη εικόνα της απόδοσης του δικτύου μας, πρέπει να ελέγξουμε και την καθυστέρηση μετάδοσης, δηλαδή τον πόσο χρόνο χρειάζεται ένα πακέτο να διασχίσει το δίκτυο. Η καθυστέρηση επηρεάζει το πόσο γρήγορα θα λειτουργούν οι εφαρμογές που θα χρησιμοποιηθούν.

Για τον καθορισμό της καθυστέρησης, χρησιμοποιήσαμε την εντολή ping η οποία αποστέλλει αιτήσεις με πακέτα ICMP και περιμένει απαντήσεις από τον αντίστοιχο κόμβο. Έτσι, λοιπόν, μπορούμε να καθορίσουμε με την εντολή ping τον αριθμό των πακέτων που θα σταλούν αλλά και το μέγεθος τους. Εμείς χρησιμοποιήσαμε 100 πακέτα ICMP με μέγεθος 56 bytes (*ping 192.168.0.20 –n 100 –l 56*) . Στο τέλος, η εντολή επιστρέφει κάποια συνολικά χρονικά στοιχεία, όπως είναι ο μέγιστος/ελάχιστος χρόνος και ο μέσος χρόνος που χρειάστηκε να αποσταλεί η αίτηση και να απαντήσει ο απομακρυσμένος κόμβος.

Εκτελέσαμε συνολικά τρεις φορές την εντολή καθώς πήραμε μετρήσεις για τις καταστάσεις ασφαλείας 1 και 3 σε περιβάλλον Linux και για την κατάσταση ασφαλείας 1 σε περιβάλλον Windows.

Καθυστέρηση		
	Windows	Linux
Κατάσταση Ασφαλείας 1	-	21,7 ms
Κατάσταση Ασφαλείας 3	15 ms	19,7 ms

Πίνακας 10-1 Χρόνοι καθυστέρησης για τις 2 καταστάσεις ασφαλείας

Παρατηρούμε ότι η κατάσταση ασφαλείας 1 παρουσιάζει μεγαλύτερη καθυστέρηση από την κατάσταση ασφαλείας 3 τόσο σε περιβάλλον Linux αλλά και σε Windows. Αυτό σημαίνει ότι για εφαρμογές που απαιτούν τα πακέτα να μεταδίδονται γρήγορα είναι προτιμητέα η λύση της κατάστασης ασφαλείας 3.

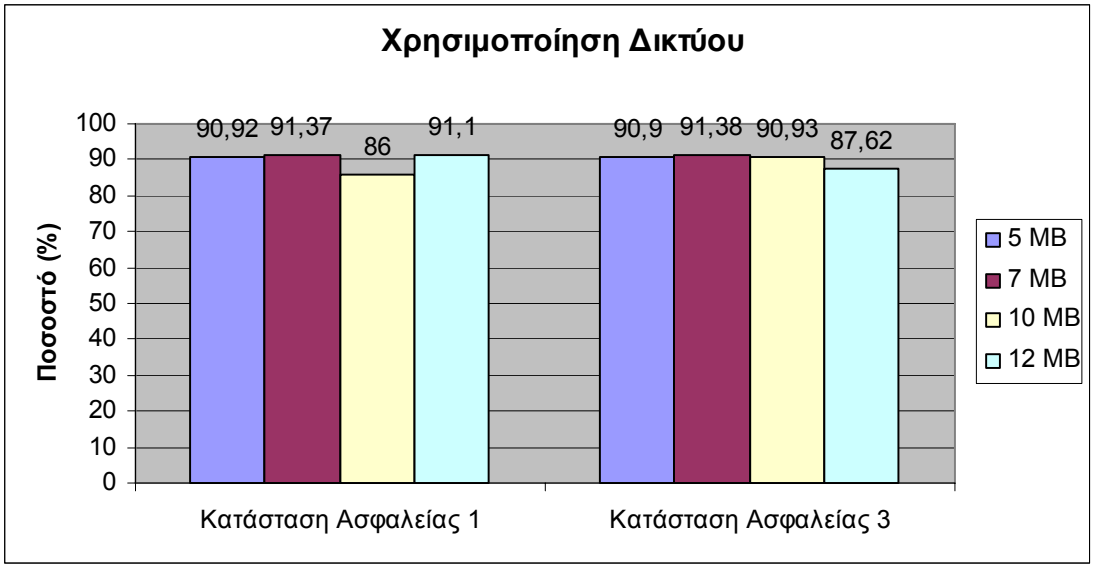
Η διαφορά στους χρόνους μεταξύ της εφαρμογής της κατάστασης ασφαλείας 3 σε περιβάλλον Windows και περιβάλλον Linux έγκειται στη διαφορετική υλοποίηση των οδηγών της συσκευής αλλά και του συνοδευτικού λογισμικού.

10.2.4 Χρησιμοποίηση δικτύου

Η χρησιμοποίηση του δικτύου αναφέρεται στο ποσοστό του χρόνου κατά τον οποίο το δίκτυο είναι σε χρήση. Για τον υπολογισμό αυτού του δείκτη, ουσιαστικά πρέπει να μετρήσουμε τον αριθμό των bytes που μεταδίδονται σε ένα καθορισμένο χρονικό διάστημα. Για τον υπολογισμό, λοιπόν, της χρησιμοποίησης του δικτύου θα χρησιμοποιήσουμε τον παρακάτω τύπο:

$$\%utilization = ((datasent + datarecv) * 8) / (intspeed * sampletime) * 100)$$

όπου datasent τα δεδομένα που αποστέλλονται, datarecv τα δεδομένα που λαμβάνονται, intspeed το συνολικό εύρος ζώνης του δικτύου και sampletime το αντίστοιχο χρονικό διάστημα. Ο αριθμητής πολλαπλασιάζεται επί οκτώ έτσι ώστε να βρεθεί ο συνολικός αριθμός των bits που μεταδόθηκαν. Ενώ, το κλάσμα πολλαπλασιάζεται επί εκατό έτσι ώστε να έχουμε ως αποτέλεσμα ποσοστό επί τοις εκατό.



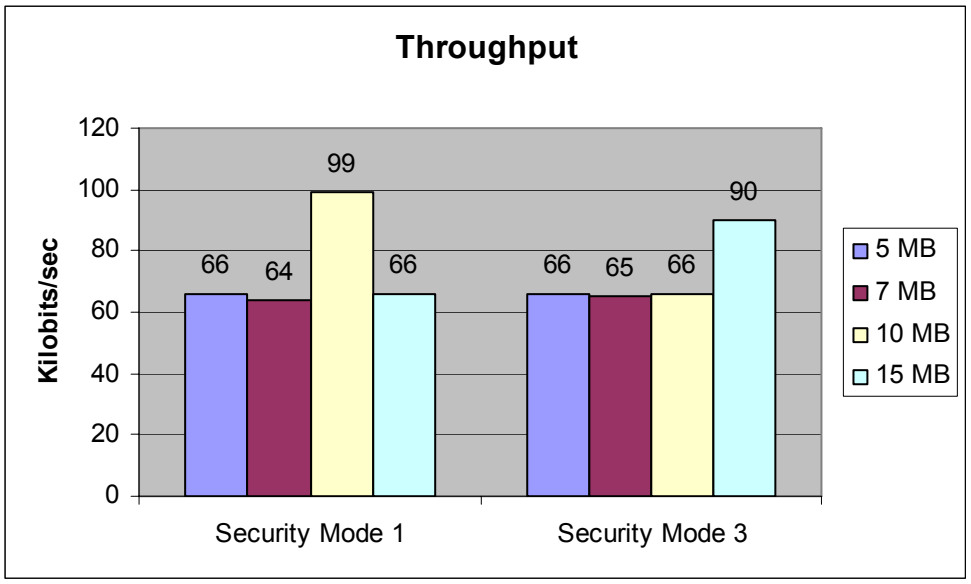
Γράφημα 10-3 Χρησιμοποίηση δικτύου ανάλογα με την κατάσταση ασφαλείας

Με εξαίρεση των περιπτώσεων της μετάδοσης του αρχείου μεγέθους 10MB με επιλεγμένη την κατάσταση ασφαλείας 1 και του αρχείου μεγέθους 15MB με εφαρμογή της κατάστασης ασφαλείας 3, οι υπόλοιπες κυμαίνονται με απειροελάχιστες διαφορές στην ίδια χρησιμοποίηση του δικτύου. Άρα, σε αυτό τον δείκτη αξιολόγησης δεν μπορούμε να πούμε ότι κάποια από τις δυο υπερέχει.

10.2.5 Throughput

Το throughput παριστάνει το διαθέσιμο εύρος ζώνης του δικτύου σε κάποια χρονική στιγμή. Δηλαδή, το throughput είναι το υπόλοιπο από το συνολικά διαθέσιμο εύρος ζώνης. Είναι κρίσιμος δείκτης για κάθε δίκτυο. Καθορίζοντας το thoughput ενός δικτύου, μπορούμε να αποφύγουμε τα λεγόμενα bottlenecks, δηλαδή κάποια σημεία του δικτύου στα οποία συσσωρεύονται δεδομένα λόγω σύνδεσης μικρής ταχύτητας μεταξύ κόμβων υψηλής ταχύτητας. Βέβαια, η εύρεση των bottlenecks δεν είναι πάντα μια εύκολη υπόθεση καθώς μπορεί ανάμεσα δυο κόμβων να υπάρχουν πολλές δικτυακές συσκευές (π.χ. hubs, switches, routers ακόμα και άλλοι κόμβοι).

Όπως είναι φυσιολογικό, αφού έχουμε ήδη δει το γράφημα για το εύρος ζώνης, το μεγαλύτερο throughput παρουσιάζεται στην περίπτωση της μεταφοράς του αρχείου μεγέθους 10 MB εφαρμόζοντας την κατάσταση ασφαλείας 1 και αμέσως μετά του αρχείου μεγέθους 15MB με χρήση της κατάστασης ασφαλείας 3.



Γράφημα 10-4 Throughput ανάλογα με την κατάσταση ασφαλείας

10.2.6 Συμπεράσματα καταστάσεων ασφαλείας 1 και 3 του πρωτοκόλλου Bluetooth

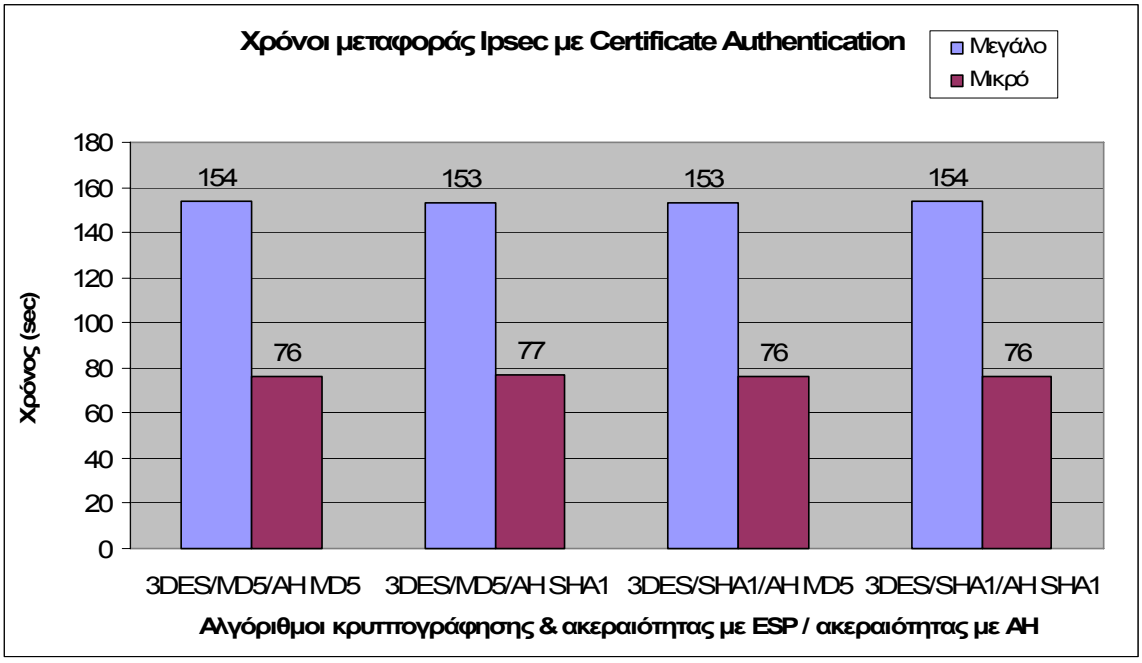
Το συμπέρασμα που βγαίνει μετά την ανάλυση των πέντε προαναφερθέντων δεικτών αξιολόγησης της απόδοσης των 2 καταστάσεων ασφαλείας που μελετήσαμε είναι ότι είναι προτιμητέα η χρήση και εφαρμογή της κατάστασης ασφαλείας 3 η οποία παρουσιάζει την μικρότερη καθυστέρηση, το μεγαλύτερο εύρος ζώνης και την μεγαλύτερη χρησιμοποίηση του δικτύου. Ενώ, η κατάσταση ασφαλείας παρουσιάζει τον μικρότερο χρόνο μεταφοράς των δυο αρχείων.

10.3 IPsec

Όπως αναφέραμε και στο προηγούμενο κεφάλαιο στο IP χρησιμοποιούνται κάποιες μέθοδοι για την αυθεντικοποίηση, την ακεραιότητα και την κρυπτογράφηση των δεδομένων. Έτσι, η αυθεντικοποίηση έγινε με δύο τρόπους: τη χρήση ψηφιακών πιστοποιητικών και κωδικού. Από την άλλη, για το μηχανισμό AH χρησιμοποιήσαμε τους αλγόριθμους MD5 και SHA1, ενώ για το μηχανισμό ESP τους MD5 και SHA1 για ακεραιότητα και τους DES και 3DES για κρυπτογράφηση. Τα γραφήματα που θα παρουσιαστούν στη συνέχεια βασίστηκαν στις μετρήσεις με όλους τους παραπάνω δυνατούς συνδυασμούς. Να σημειώσουμε επίσης ότι για τον κάθε συνδυασμό πήραμε μετρήσεις για δύο αρχεία διαφορετικού μεγέθους.

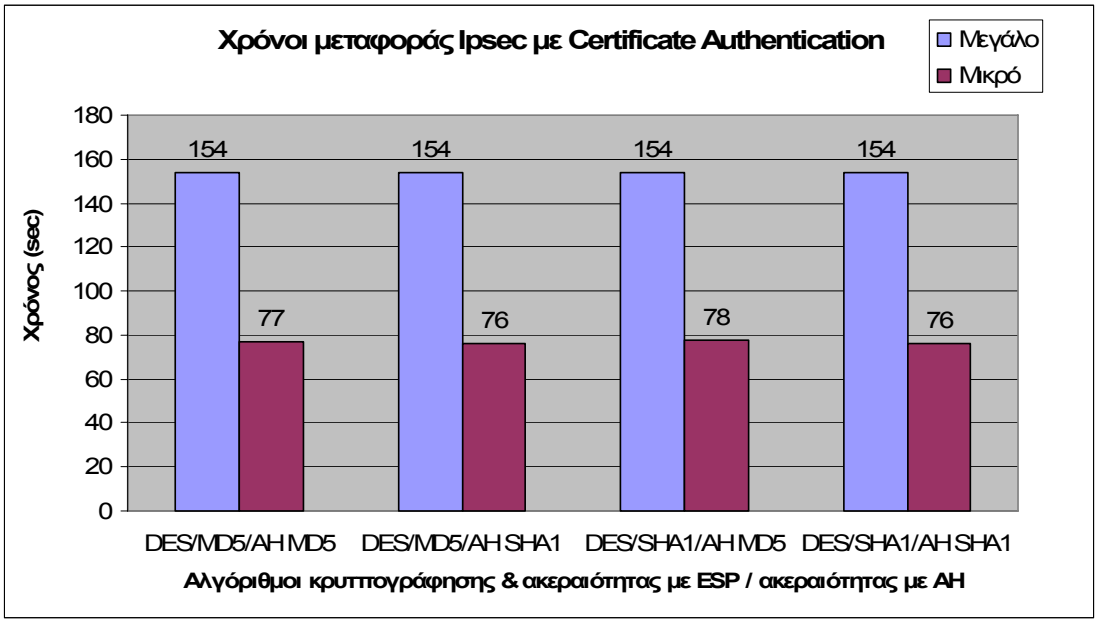
10.3.1 Χρόνος μεταφοράς

Παρακάτω παρατίθενται τα γραφήματα με τους χρόνους μεταφοράς των αρχείων χρησιμοποιώντας ψηφιακά πιστοποιητικά για αυθεντικοποίηση. Απ' ότι μπορούμε να διακρίνουμε δεν υπάρχουν ιδιαίτερες διαφορές μεταξύ των αλγορίθμων.



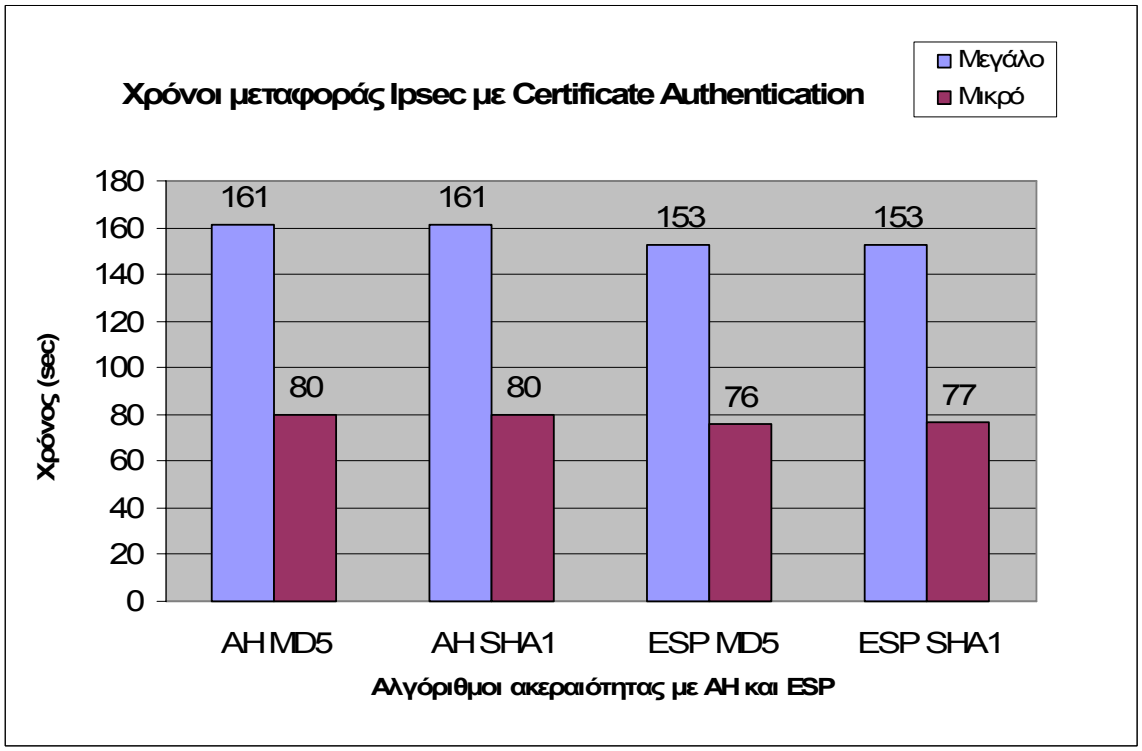
Γράφημα 10-5 Χρόνοι μεταφοράς IPsec με Certificate Authentication και 3DES

Για την καλύτερη κατανόηση των γραφημάτων κάτω από κάθε μπάρα έχουμε ένα τίτλο της μορφής X/Y/Z,
όπου X: ο αλγόριθμος κρυπτογράφησης στο ESP
Y: ο αλγόριθμος ακεραιότητας στο ESP
Z: ο αλγόριθμος ακεραιότητας στο AH



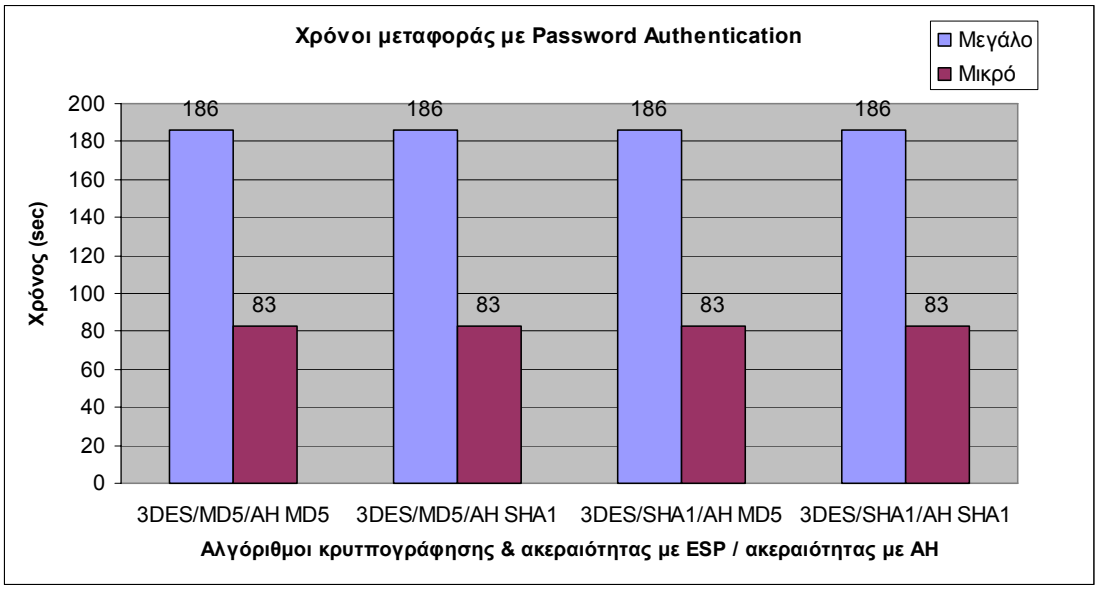
Γράφημα 10-6 Χρόνοι μεταφοράς IPsec με Certificate Authentication και DES

Στο IPsec κάναμε επίσης μετρήσεις έχοντας μόνο αυθεντικοποίηση και ακεραιότητα και όχι κρυπτογράφηση για να συγκρίνουμε τις επιμέρους περιπτώσεις. Έτσι, μη εφαρμόζοντας κρυπτογράφηση έχουμε το παρακάτω γράφημα. Αντίστοιχα γραφήματα θα έχουμε και παρακάτω με αυθεντικοποίηση με χρήση κωδικού και για κάθε παράμετρο του δικτύου.

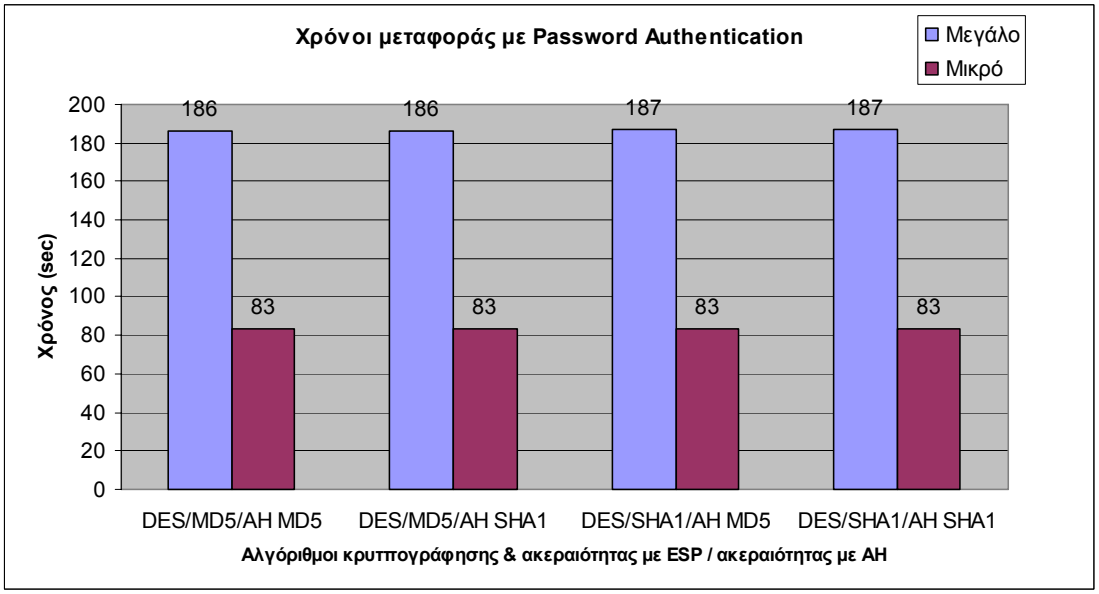


Γράφημα 10-7 Χρόνοι μεταφοράς IPsec με Certificate Authentication χωρίς κρυπτογράφηση

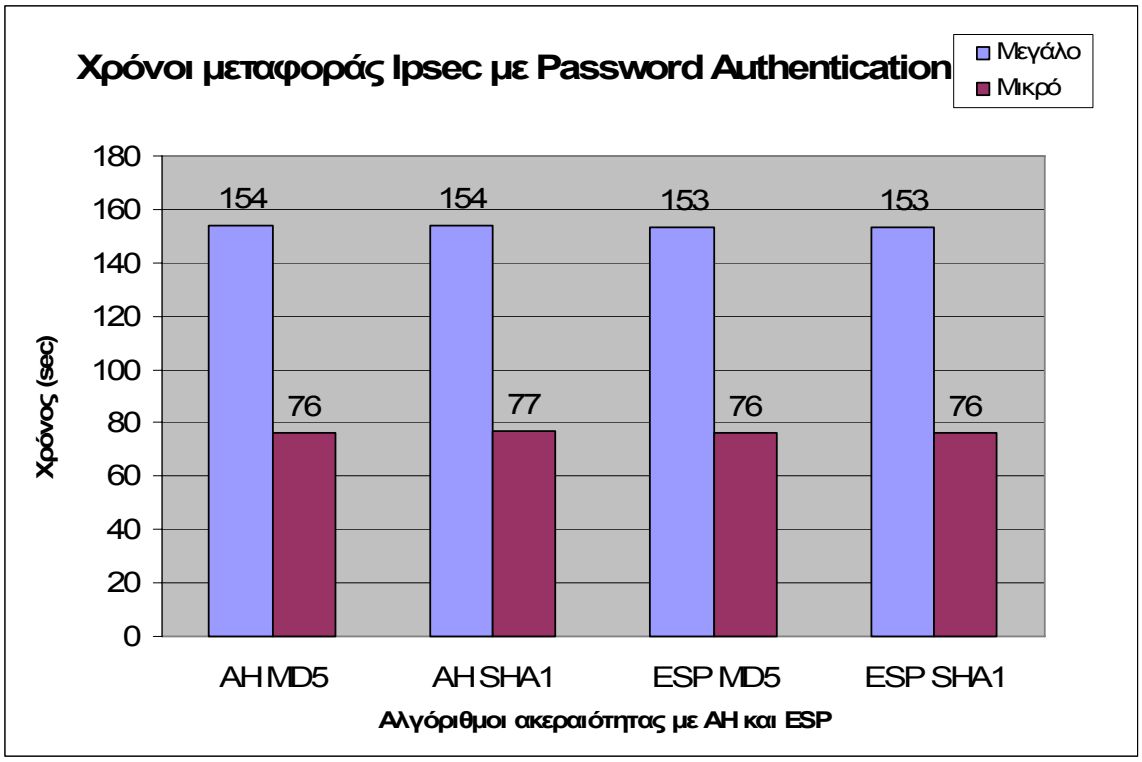
Στη συνέχεια έχουμε τα διαγράμματα με επιλογή ενός συνθηματικού για αυθεντικοποίηση.



Γράφημα 10-8 Χρόνοι μεταφοράς IPsec με Password Authentication και 3DES



Γράφημα 10-9 Χρόνοι μεταφοράς IPsec με Certificate Authentication και DES

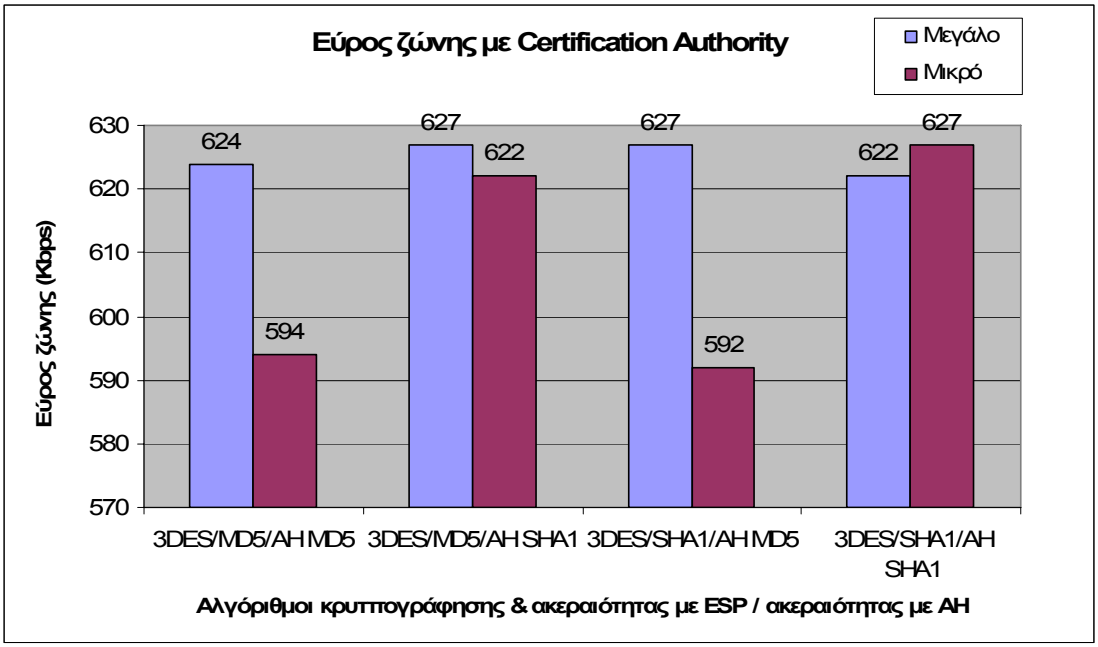


Γράφημα 10-10 Χρόνοι μεταφοράς IPsec με Password Authentication χωρίς κρυπτογράφηση

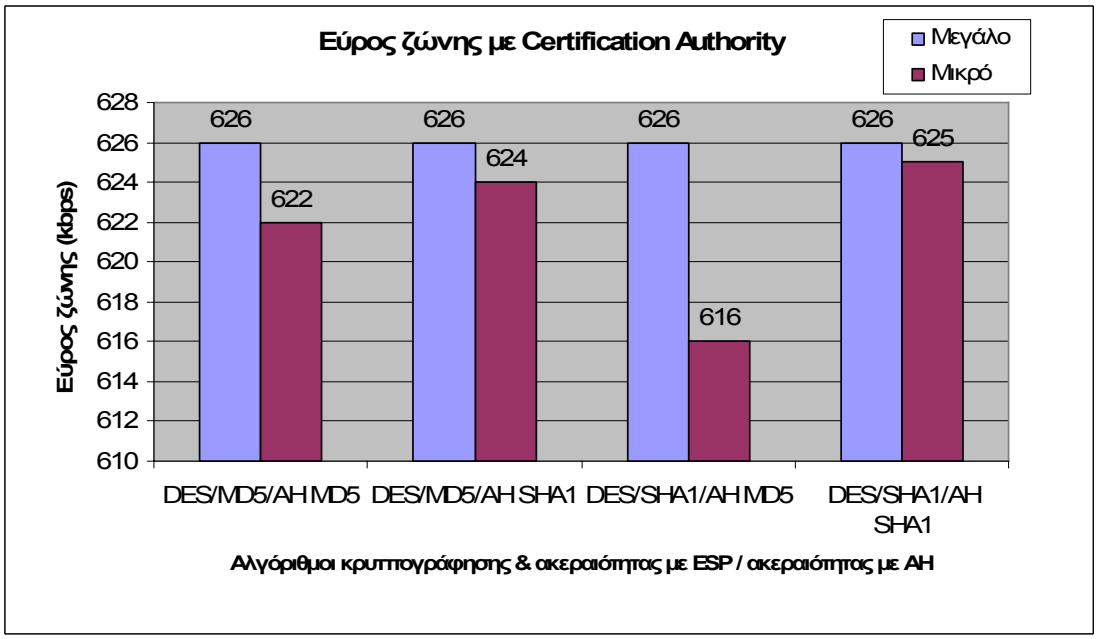
Αυτό που μας κάνει ιδιαίτερη εντύπωση είναι το γεγονός ότι αν και μεταξύ των αλγορίθμων κρυπτογράφησης και ακεραιότητας με τη μέθοδο ESP και ακεραιότητας με τη μέθοδο AH τα αποτελέσματα είναι ίδια, η αλλαγή της μεθόδου αυθεντικοποίησης επιφέρει μεγάλες αλλαγές στον χρόνο μεταφοράς ενός αρχείου. Για παράδειγμα εφαρμόζοντας MD5 και 3DES για ESP και SHA1 για AH, παρατηρούμε ότι με χρήση πιστοποιητικού ο χρόνος μεταφοράς για το μεγάλο αρχείο είναι 153 δευτερόλεπτα ενώ με χρήση κωδικού 13 δευτερόλεπτα μεγαλύτερος. Επίσης, εφαρμόζοντας αυθεντικοποίηση με κωδικό αλλά χωρίς κρυπτογράφηση οι χρόνοι μεταφοράς των αρχείων έχουν μειωθεί αισθητά!

10.3.2 Εύρος ζώνης

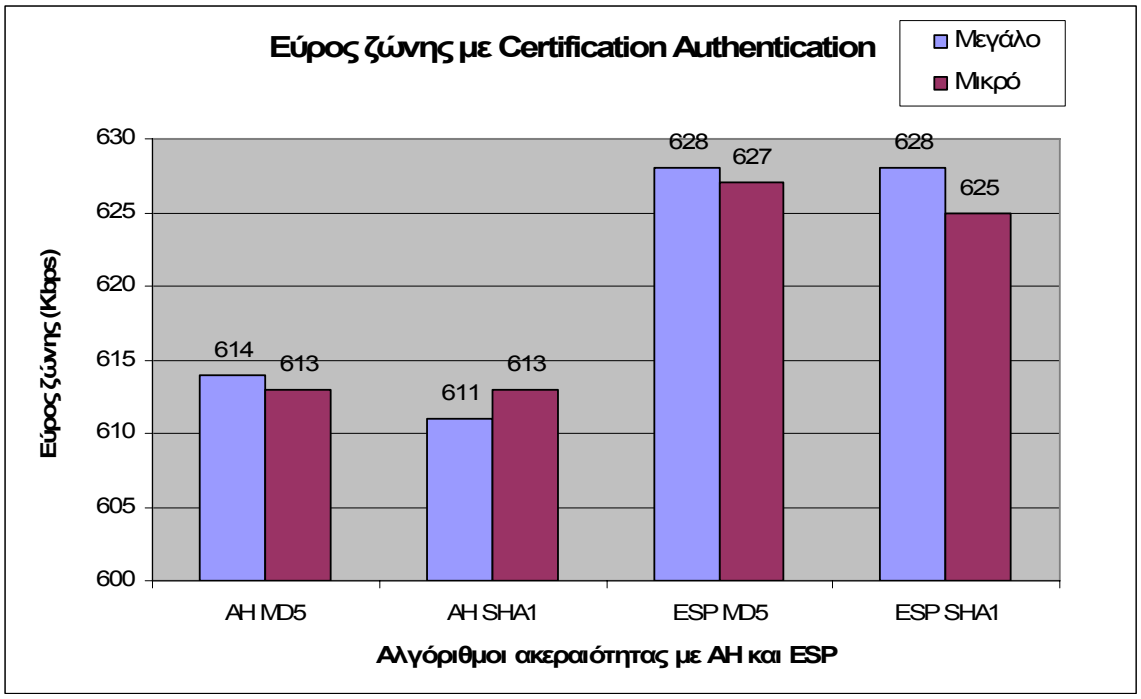
Επόμενη παράμετρος του Bluetooth δικτύου μας αποτελεί το εύρος ζώνης. Είναι, ίσως η πιο σημαντική όσον αφορά την επίδοση ενός δικτύου.



Γράφημα 10-11 Εύρος ζώνης IPsec με Certificate Authentication και 3DES



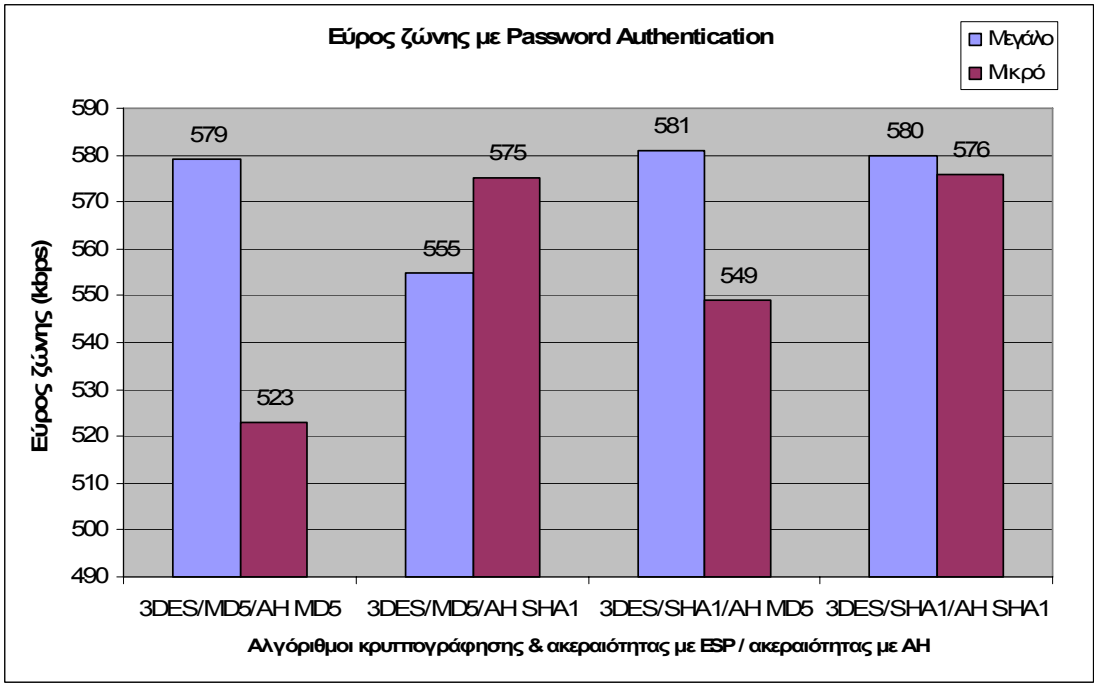
Γράφημα 10-12 Εύρος ζώνης IPsec με Certificate Authentication και DES



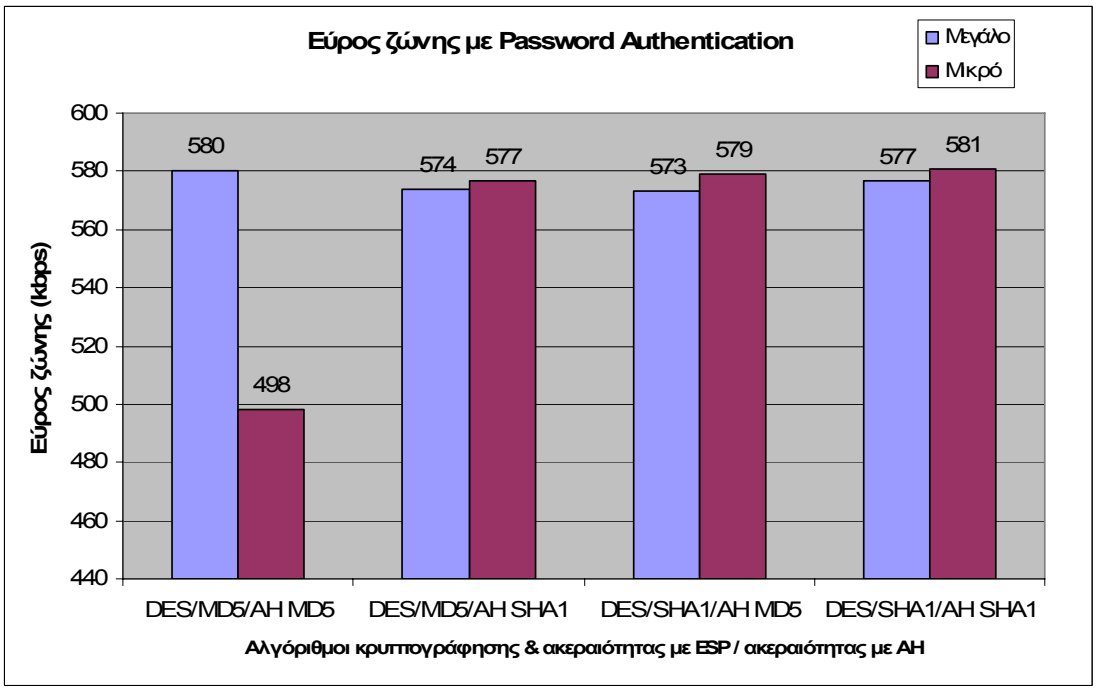
Γράφημα 10-13 Εύρος ζώνης IPsec με Certificate Authentication χωρίς κρυπτογράφηση

Είναι αξιοσημείωτο ότι όταν χρησιμοποιούμε τον αλγόριθμο MD5 στην AH, το bandwidth είναι αρκετά μικρότερο σε κάθε περίπτωση και μάλιστα σε αρκετά μεγάλο βαθμό (30 kbps).

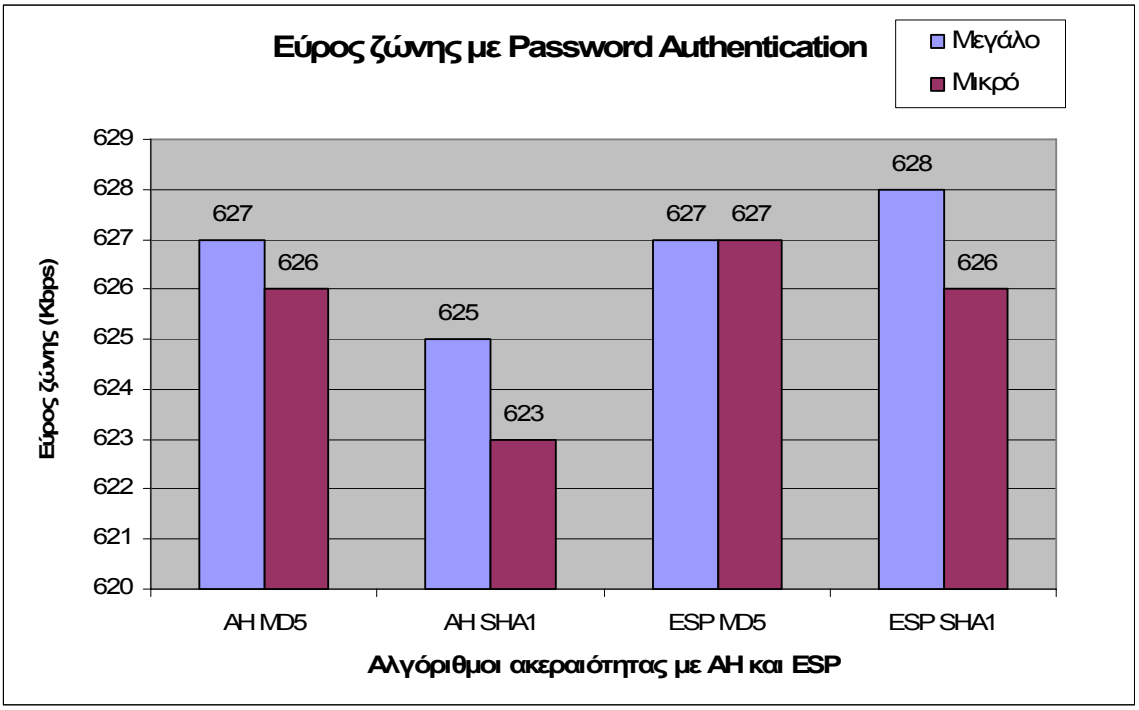
Η παραπάνω διαπίστωση ισχύει και με password authentication, όπως μπορούμε να παρατηρήσουμε στα δύο επόμενα διαγράμματα.



Γράφημα 10-14 Εύρος ζώνης IPsec με Password Authentication και 3DES



Γράφημα 10-15 Εύρος ζώνης IPsec με Password Authentication και DES

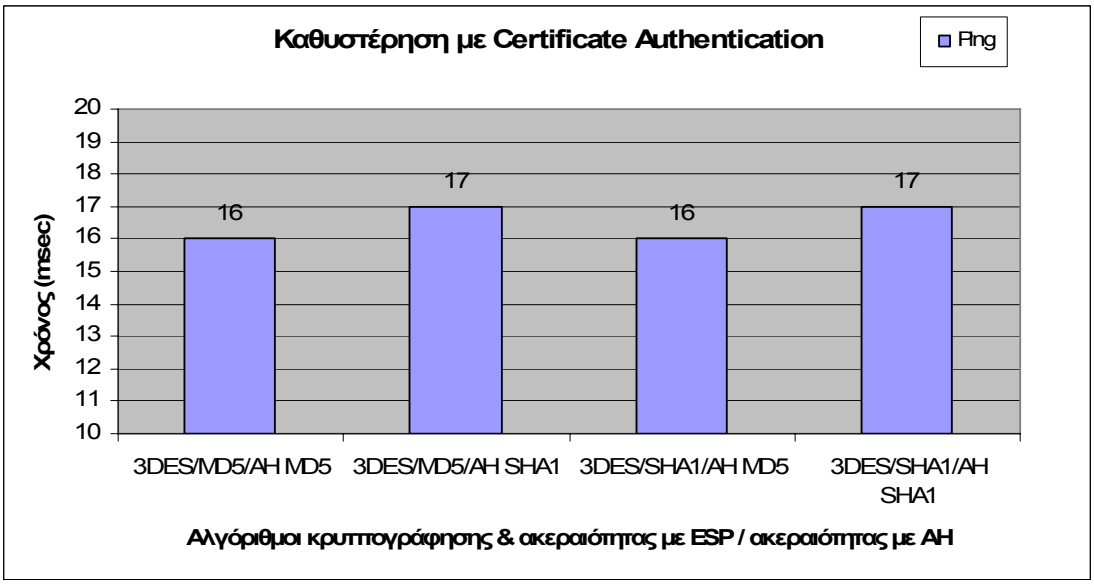


Γράφημα 10-16 Εύρος ζώνης IPsec με Password Authentication χωρίς κρυπτογράφηση

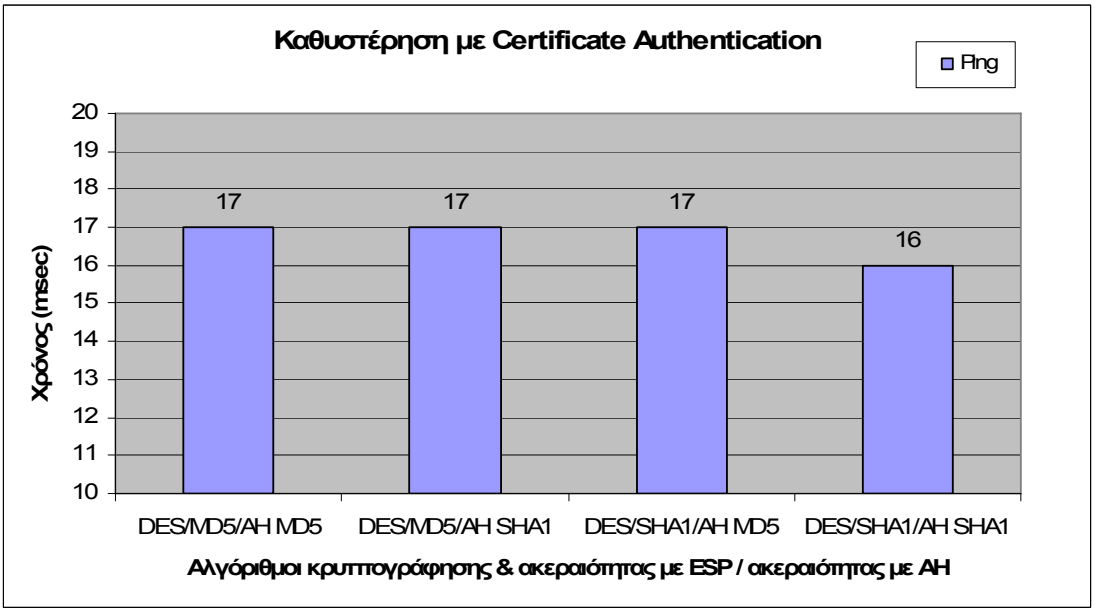
Παρατηρούμε ότι με αυθεντικοποίηση χρησιμοποιώντας συνθηματικό χωρίς όμως κρυπτογράφηση το εύρος ζώνης αυξάνεται. Τέλος, συγκρίνοντας τις δύο μεθόδους αυθεντικοποίησης, καταλήγουμε στο συμπέρασμα ότι σε όλες τις περιπτώσεις το εύρος ζώνης με χρήση πιστοποιητικών είναι μεγαλύτερο. Μάλιστα η μέγιστη τιμή του εύρους ζώνης με αυθεντικοποίηση μέσω συνθηματικού δεν ξεπερνάει την ελάχιστη τιμή μέσω ψηφιακού πιστοποιητικού!

10.3.3 Καθυστέρηση

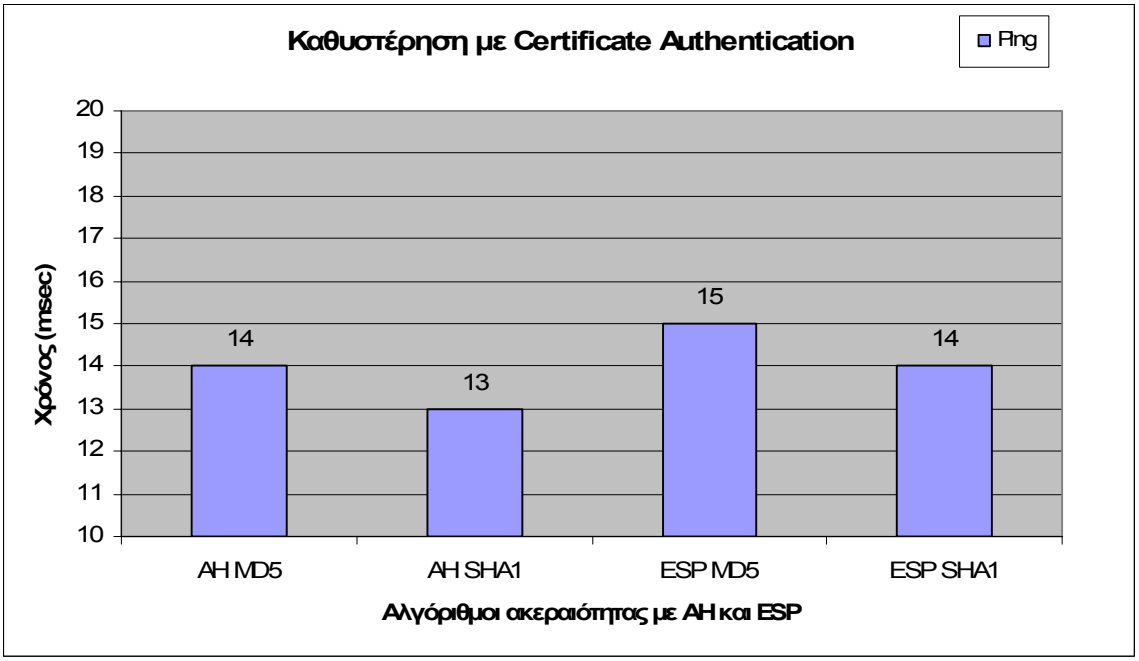
Η καθυστέρηση (latency) παραμένει ουσιαστικά ίδια σε όλους τους δυνατούς συνδυασμούς μεθόδων αυθεντικοποίησης, εμπιστευτικότητας και ακεραιότητας. Συγκεκριμένα, το ping μάς επέστρεψε διαφορές χρόνων 1 msec.



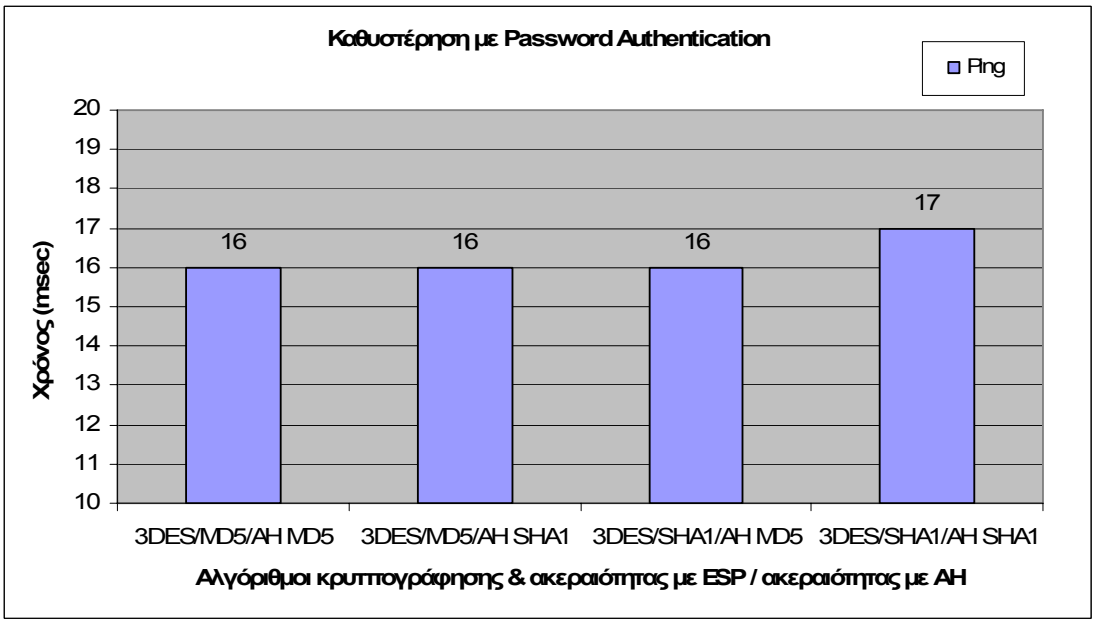
Γράφημα 10-17 Καθυστέρηση IPsec με Certificate Authentication και 3DES



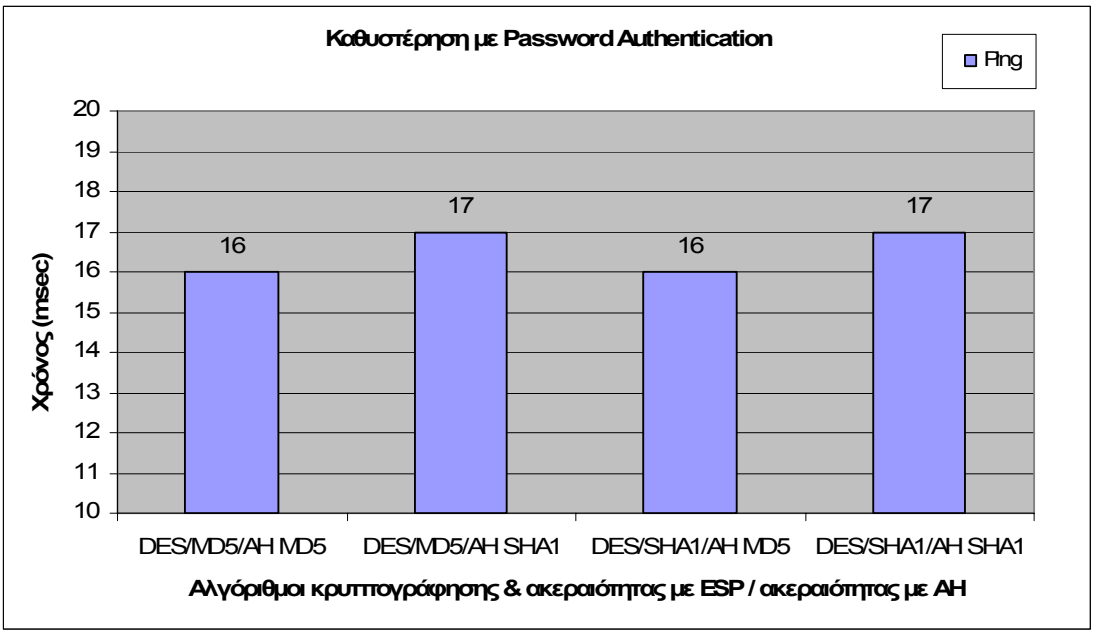
Γράφημα 10-18 Καθυστέρηση IPsec με Certificate Authentication και DES



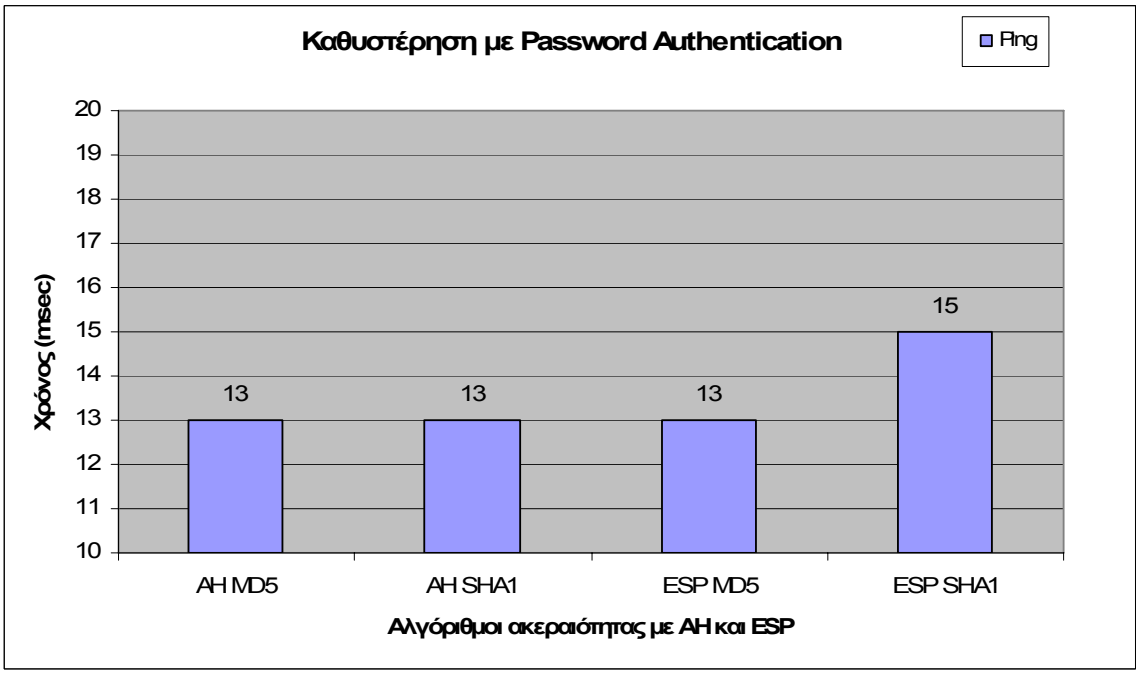
Γράφημα 10-19 Καθυστέρηση IPsec με Certificate Authentication χωρίς κρυπτογράφηση



Γράφημα 10-20 Καθυστέρηση IPsec με Password Authentication και 3DES



Γράφημα 10-21 Καθυστέρηση IPsec με Password Authentication και DES

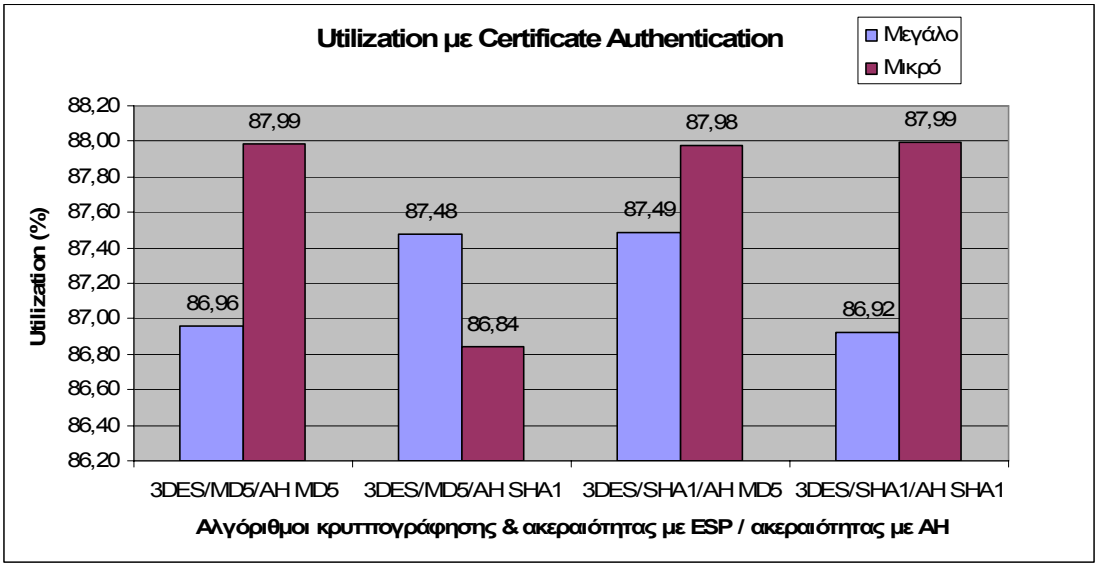


Γράφημα 10-22 Καθυστέρηση IPsec με Password Authentication χωρίς κρυπτογράφηση

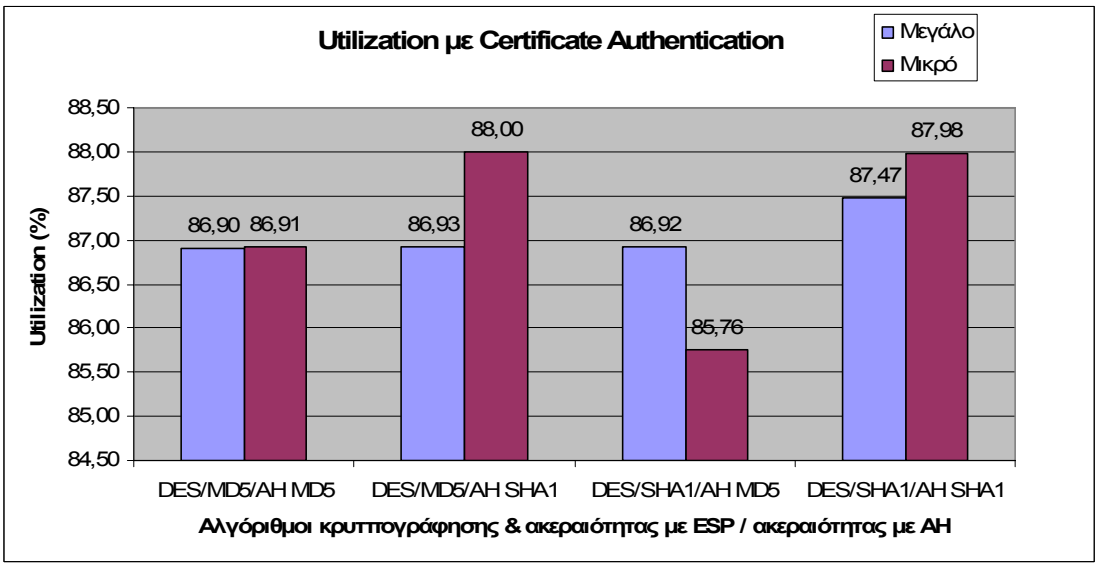
Συμπεραίνουμε ότι χωρίς την εφαρμογή κρυπτογράφησης τόσο με αυθεντικοποίηση με χρήση πιστοποιητικών όσο και κωδικού, η καθυστέρηση μειώνεται αισθητά.

10.3.4 Χρησιμοποίηση δικτύου

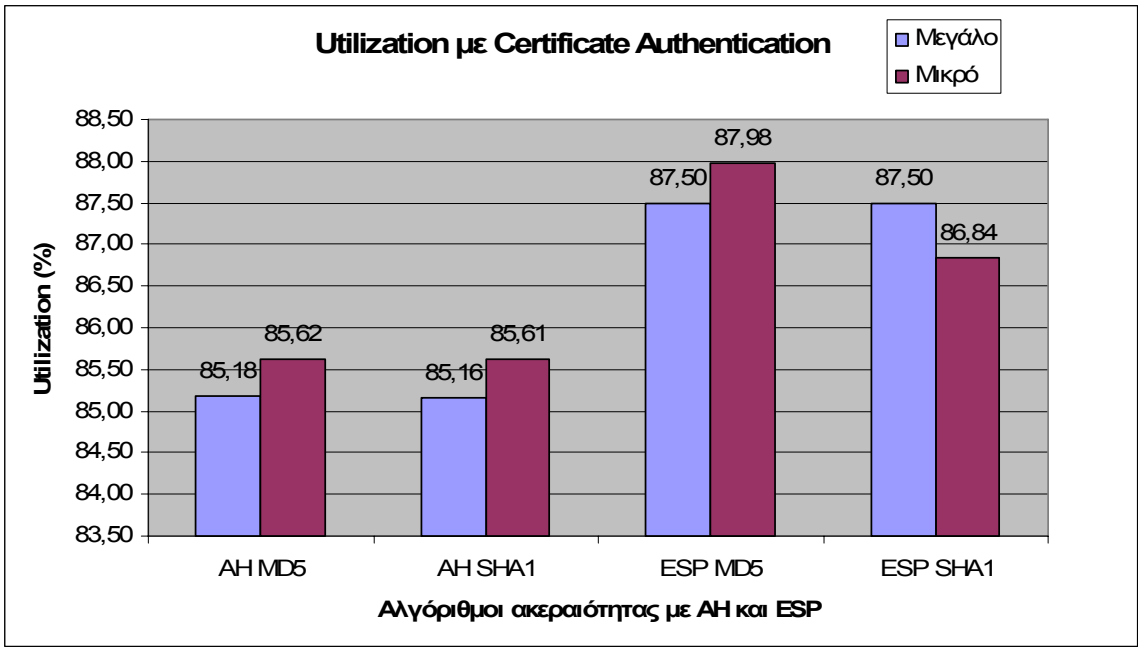
Εξετάζοντας τη χρησιμοποίηση του δικτύου με χρήση ψηφιακών πιστοποιητικών για αυθεντικοποίηση βλέπουμε κάποιες τυχαίες διακυμάνσεις, ενώ τη μικρότερη χρησιμοποίηση των πόρων κάνει το DES/SHA1/AH MD5 με 85,76%.



Γράφημα 10-23 Χρησιμοποίηση δικτύου με Certificate Authentication και 3DES



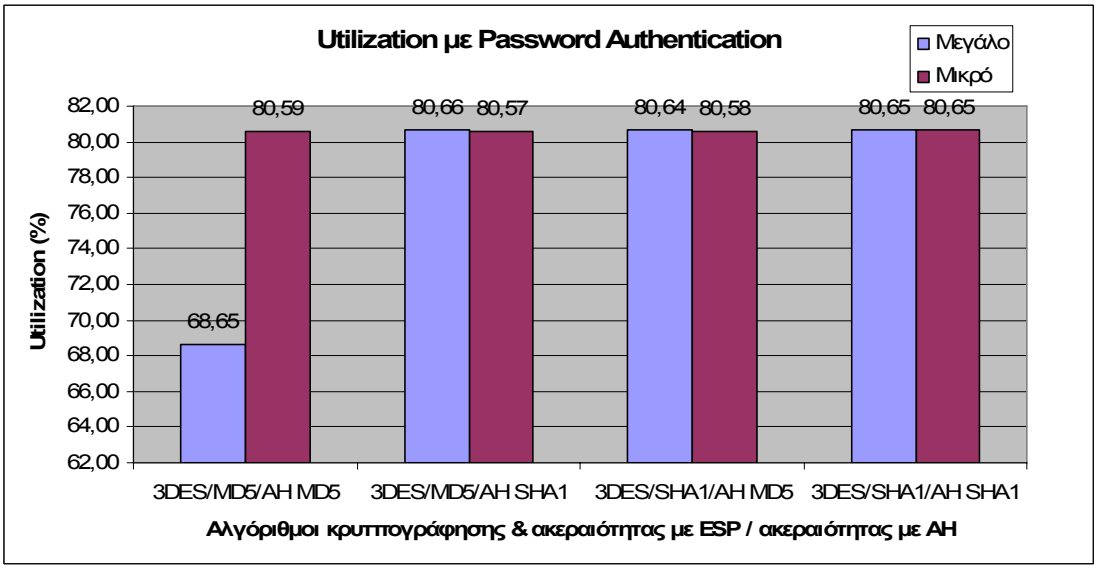
Γράφημα 10-24 Χρησιμοποίηση δικτύου με Certificate Authentication και DES



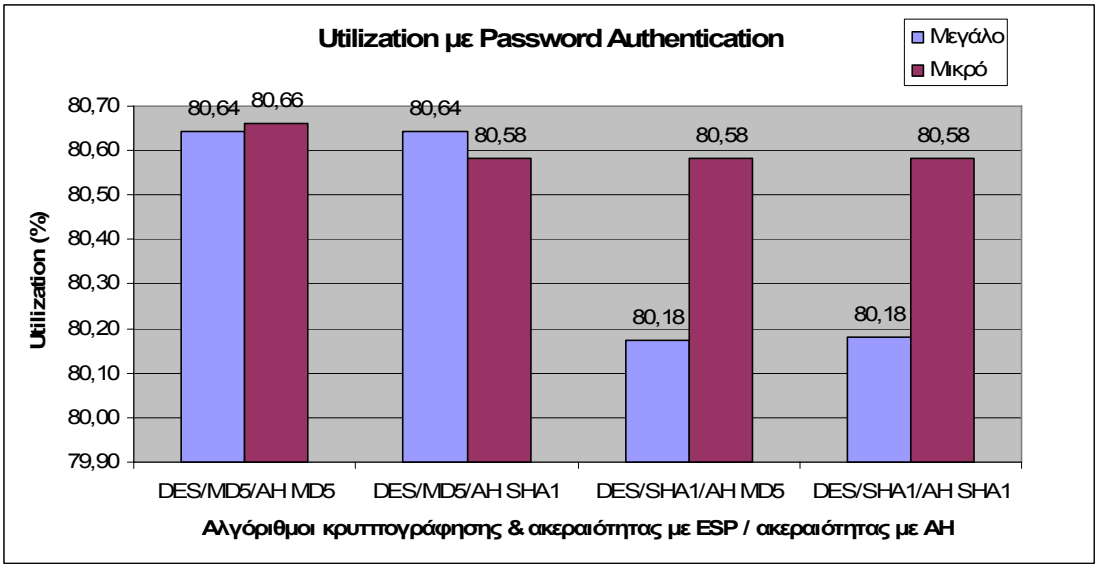
Γράφημα 10-25 Χρησιμοποίηση δικτύου με Certificate Authentication χωρίς κρυπτογράφηση

Συγκρίνοντας, όμως, τα αποτελέσματα των μετρήσεων με αυθεντικοποίηση πιστοποιητικών και συνθηματικού, παρατηρούμε ότι στη δεύτερη περίπτωση η χρησιμοποίηση του δικτύου είναι αρκετά χαμηλότερη. Αυτό μάλιστα δεν είναι ένα μεμονωμένο αποτέλεσμα αλλά γενικό χαρακτηριστικό του δικτύου. Έτσι, βλέπουμε και διαφορές που αγγίζουν το 7% κατά την μεταφορά και των δυο αρχείων.

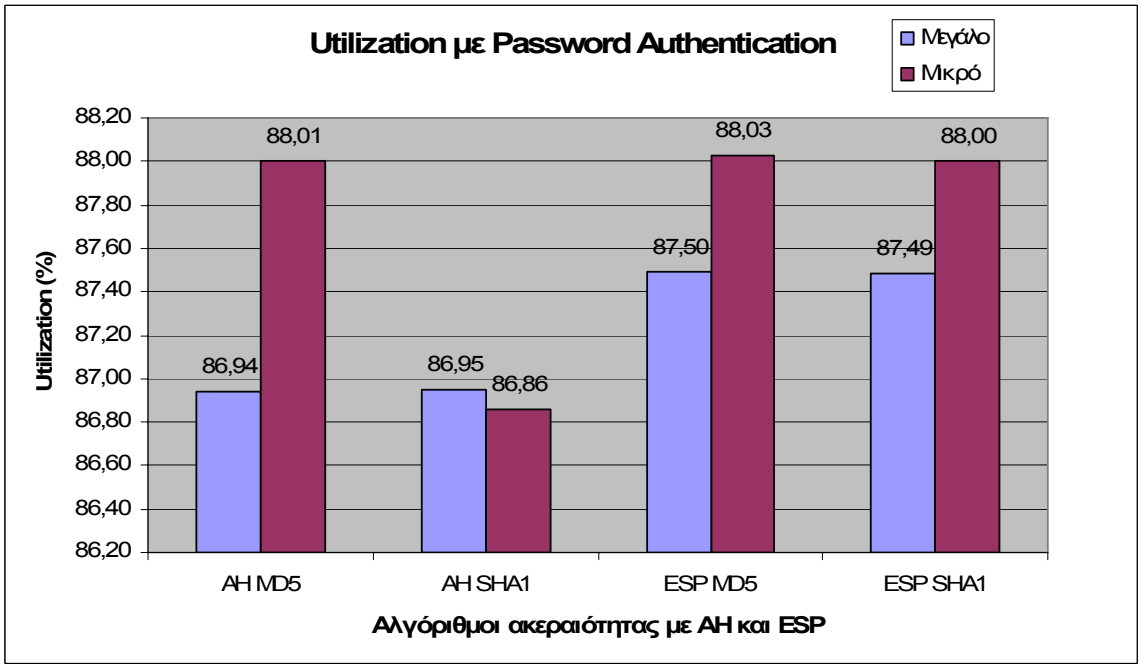
Μία άλλη σημαντική παρατήρηση είναι το γεγονός ότι η κατώτερη τιμή της χρησιμοποίησης του δικτύου (85,76%) κατά την μεταφορά του μικρού αρχείου με χρήση πιστοποιητικών είναι μεγαλύτερη από τη μέγιστη τιμή με χρήση συνθηματικού (80,66%) !!!



Γράφημα 10-26 Χρησιμοποίηση δικτύου με Password Authentication και 3DES



Γράφημα 10-27 Χρησιμοποίηση δικτύου με Password Authentication και DES



Γράφημα 10-28 Χρησιμοποίηση δικτύου με Password Authentication χωρίς κρυπτογράφηση

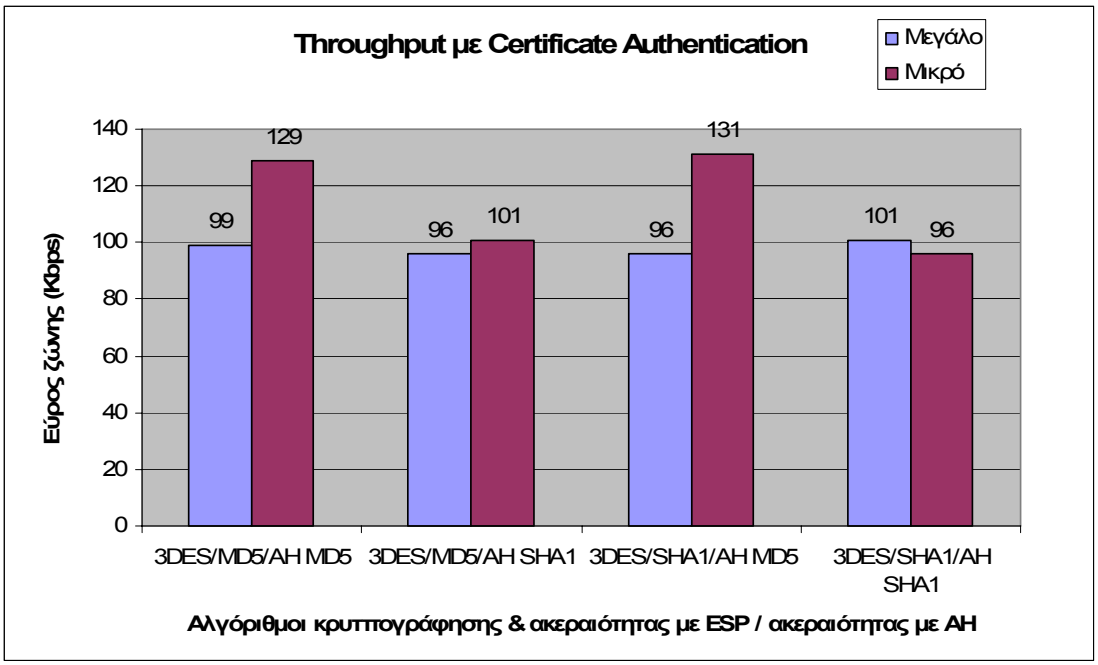
Συγκρίνοντας τα γραφήματα που έχουμε εφαρμόσει κρυπτογράφηση ή όχι, στην περίπτωση της χρήσης πιστοποιητικών δε βλέπουμε αξιοσημείωτες διαφορές. Ωστόσο με χρήση συνθηματικού, συμπεραίνουμε ότι χωρίς κρυπτογράφηση έχουμε καλύτερη χρησιμοποίηση των πόρων του δικτύου.

Καταλήγουμε, λοιπόν, στο συμπέρασμα ότι η αυθεντικοποίηση με συνθηματικό αφήνει ανεκμετάλλευτο μεγάλο ποσοστό των πόρων του δικτύου εκτός κι αν δεν εφαρμόσουμε κρυπτογράφηση κάτι το οποίο μειώνει τη ασφάλεια του συστήματος.

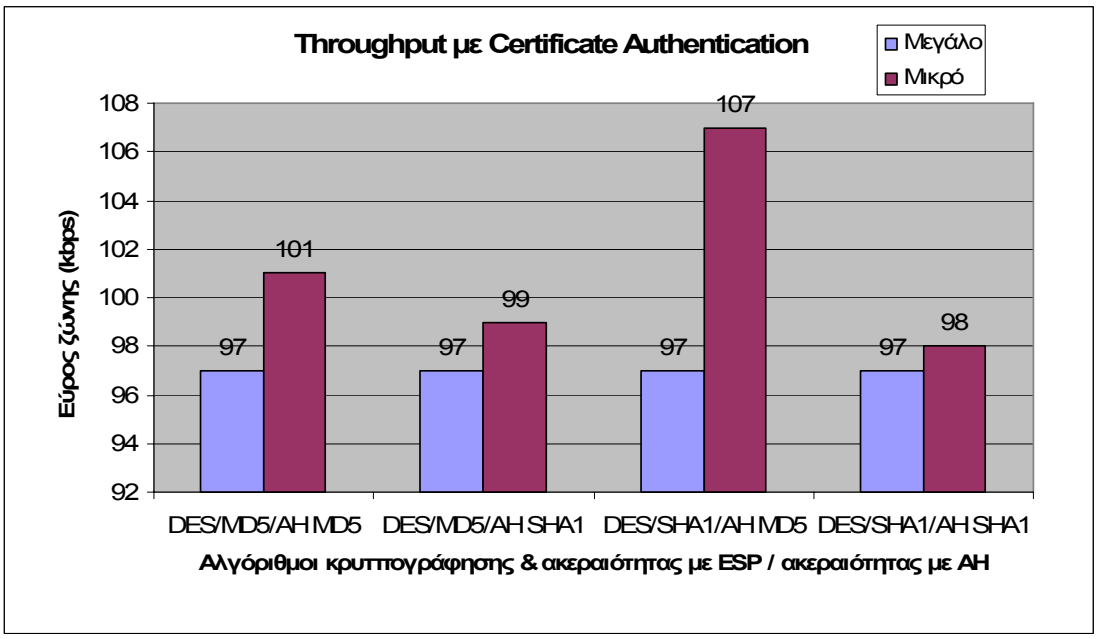
10.3.5 Throughput

Βλέποντας με μια πρώτη ματιά τα δύο διαγράμματα καταλαβαίνουμε ότι δεν υπάρχουν ουσιαστικές διαφορές. Αν προσέξουμε όμως καλύτερα, ξεχωρίζουμε στο

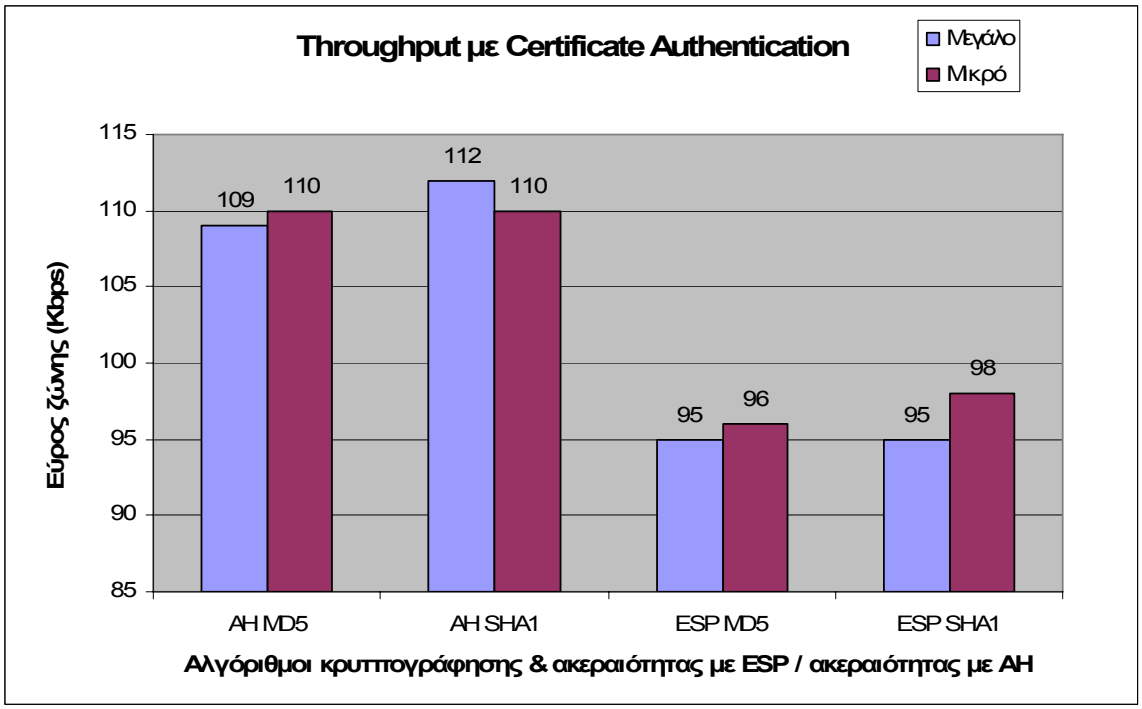
πρώτο σχήμα δύο μπάρες να εξέχουν. Αυτό συμβαίνει στην περίπτωση που χρησιμοποιούμε τους αλγορίθμους 3DES για κρυπτογράφηση στο ESP και MD5 για ακεραιότητα στην AH.



Γράφημα 10-29 Throughput με Certificate Authentication και 3DES

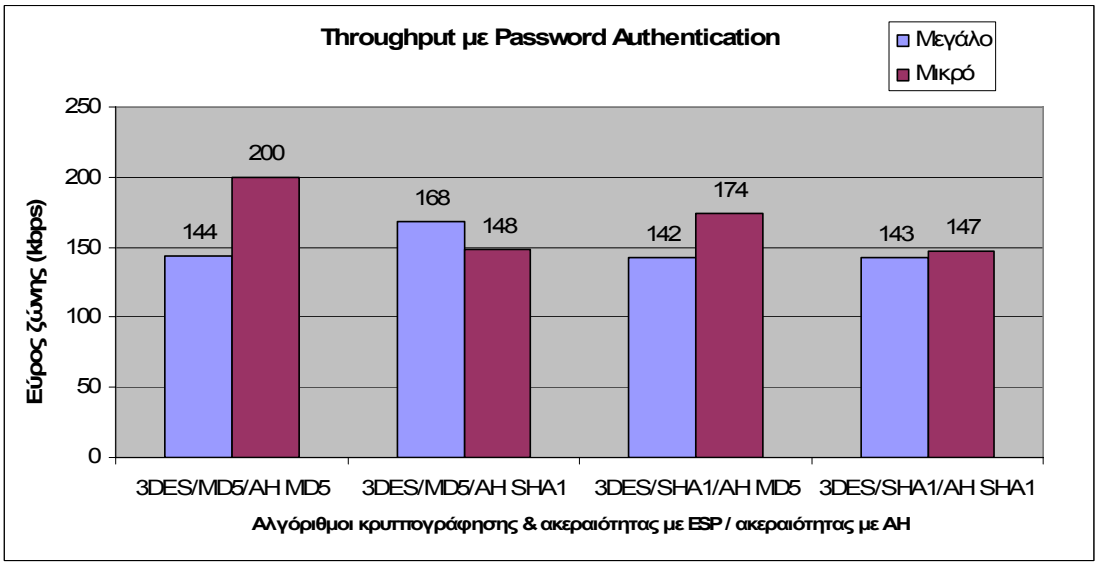


Γράφημα 10-30 Throughput με Certificate Authentication και DES

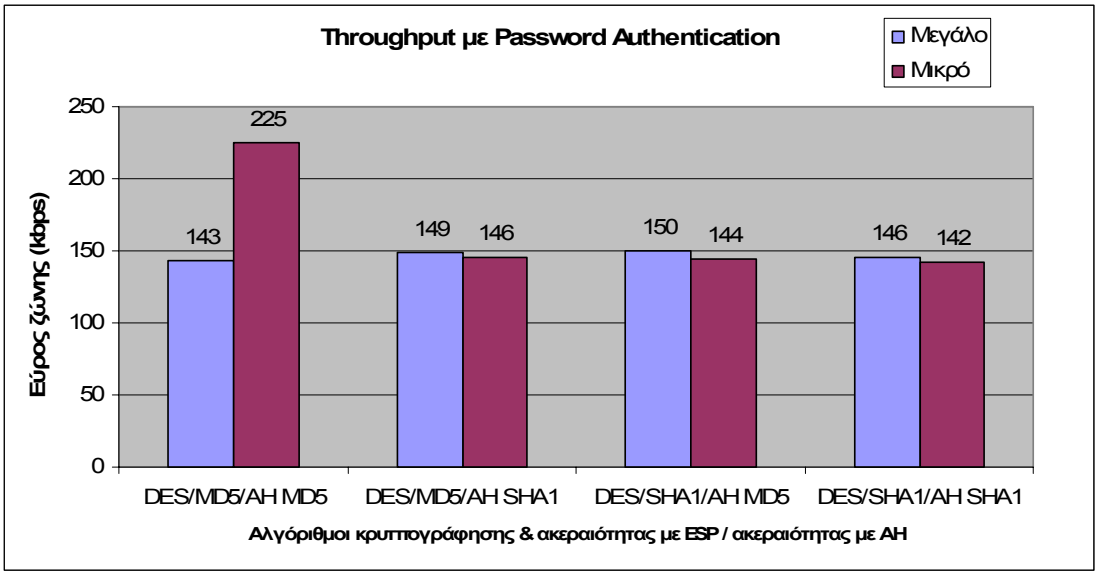


Γράφημα 10-31 Throughput με Certificate Authentication χωρίς κρυπτογράφηση

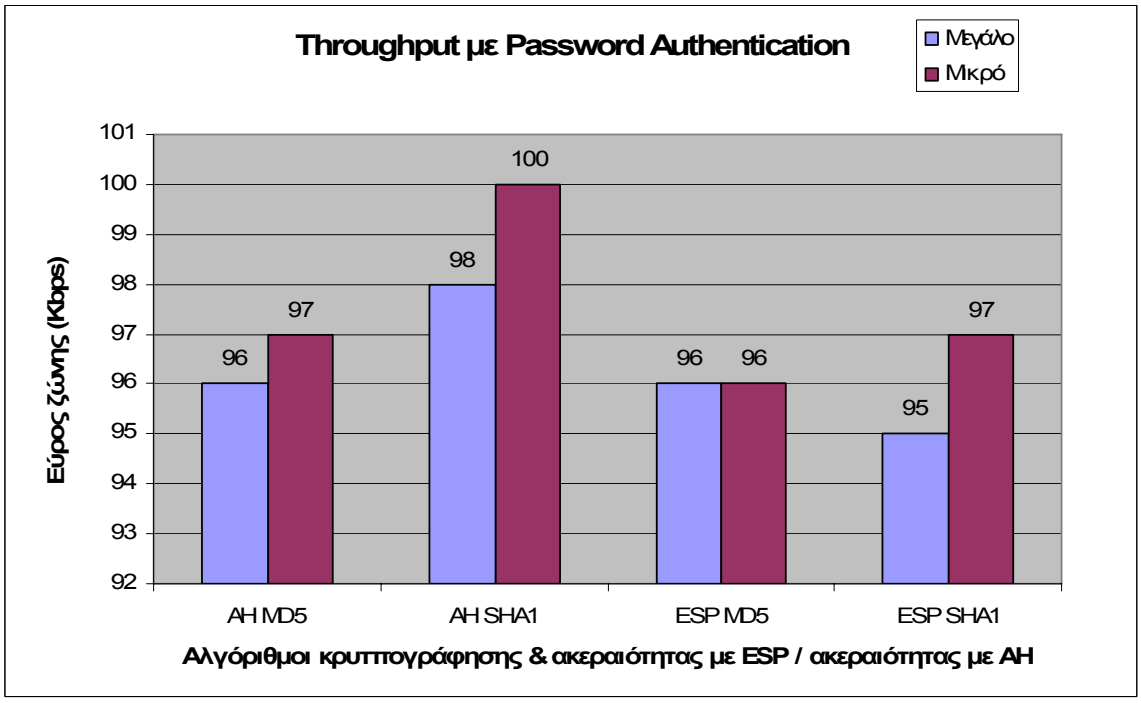
Στην περίπτωση της αυθεντικοποίησης με συνθηματικό, το throughput γενικότερα είναι μεγαλύτερο από τις προηγούμενες περιπτώσεις.



Γράφημα 10-32 Throughput με Password Authentication και 3DES



Γράφημα 10-33 Throughput με Password Authentication και DES



Γράφημα 10-34 Throughput με Password Authentication χωρίς κρυπτογράφηση

10.3.6 Συμπεράσματα

Αφού αναλύσαμε τα επιμέρους αποτελέσματα των μετρήσεων καταλήγουμε στο συμπέρασμα ότι *η χρησιμοποίηση ψηφιακών πιστοποιητικών για αυθεντικοποίηση αποτελεί αποδοτικότερη λύση όσον αφορά την επίδοση των Bluetooth δικτύων* . Από την άλλη, η επιλογή αλγορίθμου για κρυπτογράφηση και ακεραιότητα στο ESP και για ακεραιότητα στο AH δεν επηρεάζει σε ουσιαστικό βαθμό τη λειτουργία του δικτύου εκτός ελάχιστων περιπτώσεων που σημειώθηκαν στις επιμέρους αναλύσεις. Όταν όμως δεν εφαρμόζουμε καθόλου κρυπτογράφηση, έχουμε βελτιωμένα αποτελέσματα στην περίπτωση της αυθεντικοποίησης με χρήση κωδικού.

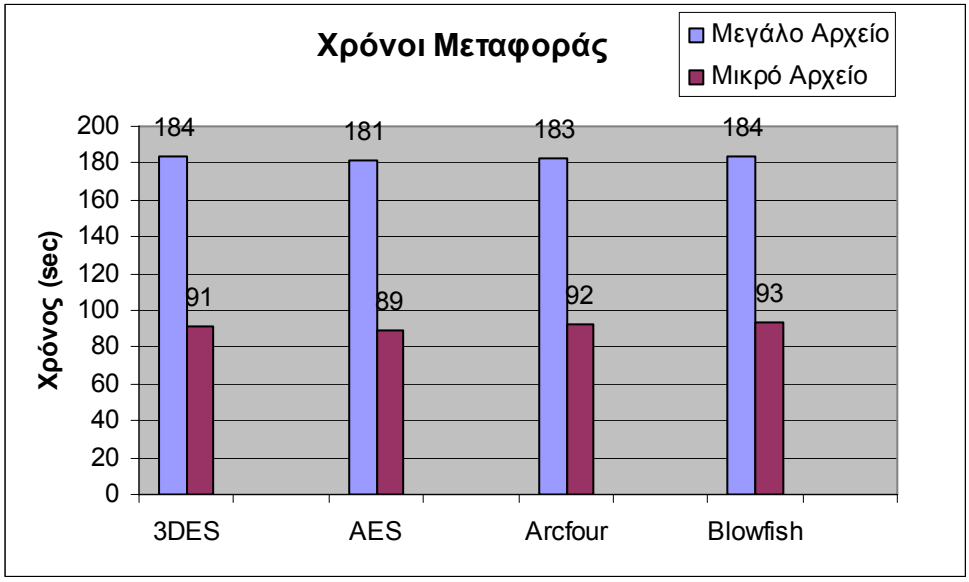
10.4 Secure Shell (SSH)

Πριν την αξιολόγηση των δεικτών για την απόδοση του δικτύου, πρέπει να σημειώσουμε ότι χρησιμοποιήσαμε διάφορους αλγόριθμους κρυπτογράφησης των μεταδιδόμενων δεδομένων. Αυτοί οι αλγόριθμοι είναι οι εξής: 3DES, AES, Blowfish και Arcfour. Επίσης, δεν χρησιμοποιήθηκε η επιλογή συμπίεσης δεδομένων και για την αυθεντικοποίηση του εξυπηρέτη επιλέχθηκε ο αλγόριθμος αυθεντικοποίησης hmac-md5. Ενώ, για την αυθεντικοποίηση του χρήστη χρησιμοποιήθηκαν δυο περιπτώσεις: χρήση συνθηματικού και χρήση ζεύγους δημοσίου/ιδιωτικού κλειδιού.

10.4.1 Χρόνος Μεταφοράς

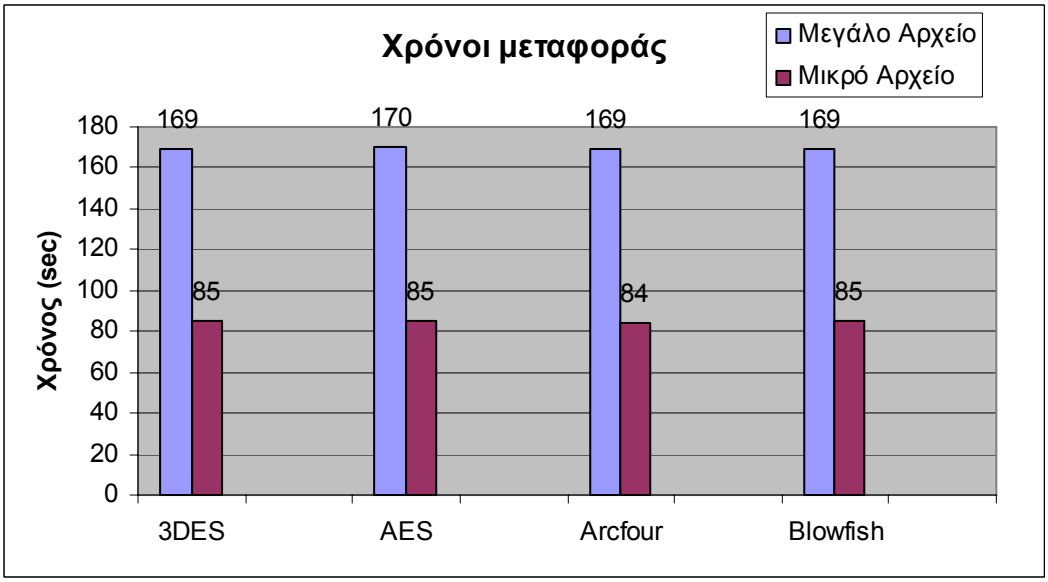
Πρώτος δείκτης είναι ο χρόνος μεταφοράς δυο αρχείων διαφορετικού μεγέθους όπως αναφέραμε και προηγουμένως. Σε αυτή την περίπτωση, έχουμε τέσσερα ζεύγη μετρήσεων όσοι είναι και οι αλγόριθμοι κρυπτογράφησης που χρησιμοποιήθηκαν για τις δυο περιπτώσεις αυθεντικοποίησης του χρήστη.

Αρχικά, παρατίθεται το γράφημα της αυθεντικοποίησης του χρήστη με χρήση συνθηματικού. Παρατηρούμε ότι ο γρηγορότερος αλγόριθμος κρυπτογράφησης τόσο για την περίπτωση του μεγάλου αλλά και του μικρού αρχείου είναι ο AES. Ενώ αμέσως μετά έρχονται ο 3DES και ο Arcfour.



Γράφημα 10-35 Χρόνοι μεταφοράς για SSH με χρήση συνθηματικού

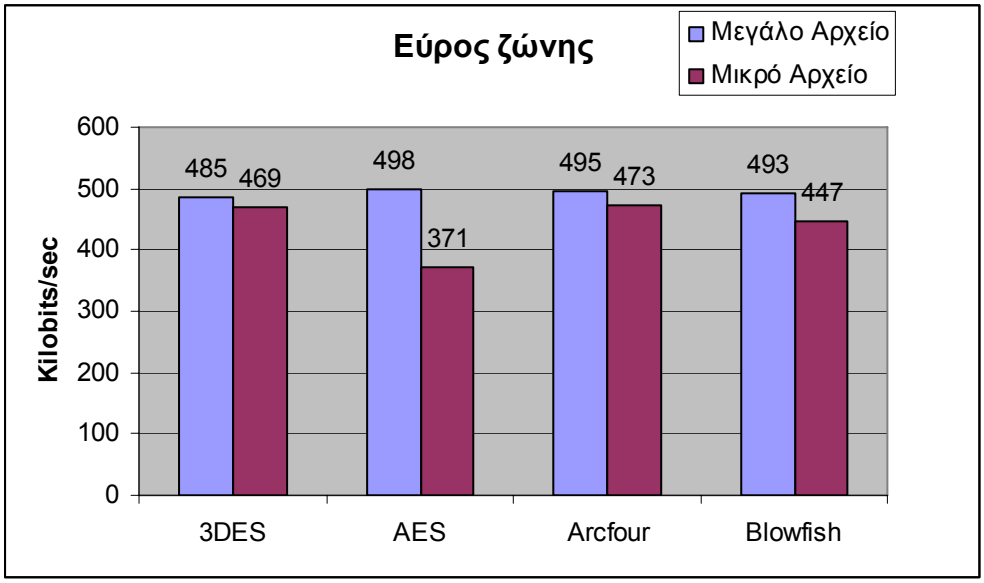
Στη συνέχεια, παρουσιάζεται το γράφημα των χρόνων μεταφοράς με την εφαρμογή αυθεντικοποίησης με χρήση ζεύγους δημόσιου/ιδιωτικού κλειδιού. Παρατηρούμε ότι δεν υπάρχει ιδιαίτερη διαφορά μεταξύ των αλγορίθμων κρυπτογράφησης. Για πολύ λίγο πιο γρήγορος φαίνεται να είναι ο Arcfour.



Γράφημα 10-36 Χρόνοι μεταφοράς με χρήση ζεύγους δημόσιου/ιδιωτικού κλειδιού

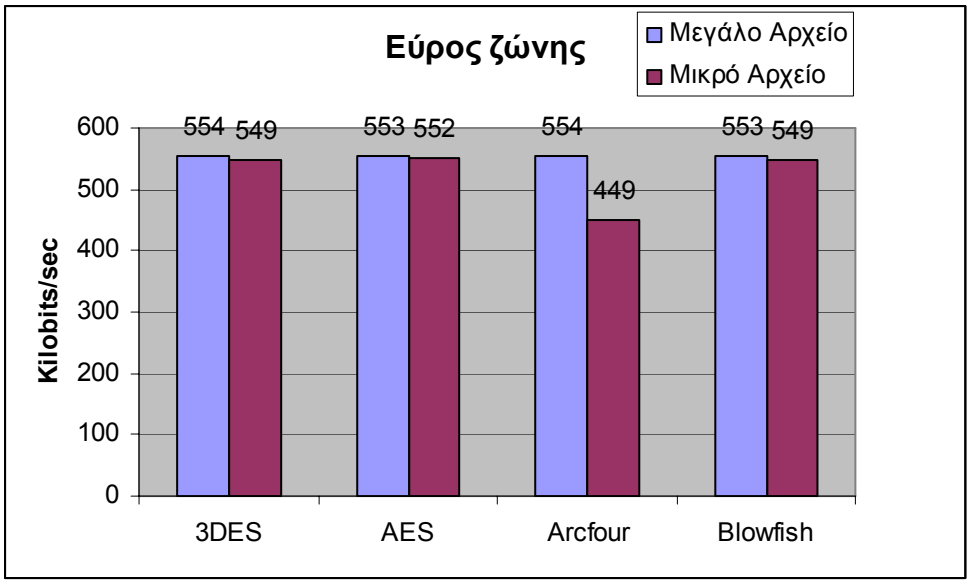
10.4.2 Εύρος ζώνης

Συνεχίζουμε με την παρουσίαση των γραφημάτων για τις δυο περιπτώσεις αυθεντικοποίησης του χρήστη ανάλογα με τον χρησιμοποιούμενο αλγόριθμο κρυπτογράφησης. Αρχικά, θα αναλύσουμε το γράφημα για την αυθεντικοποίηση με χρήση συνθηματικού.



Γράφημα 10-37 Εύρος ζώνης για αυθεντικοποίηση με χρήση συνθηματικού σε SSH

Το συμπέρασμα που μπορεί να εξαχθεί από το παραπάνω γράφημα είναι ότι το μεγάλο αρχείο μεταφέρεται γρηγορότερο με χρήση του αλγόριθμου κρυπτογράφησης AES ενώ για το μικρό αρχείο με τον αλγόριθμο Arcfour.



Γράφημα 10-38 Εύρος ζώνης με χρήση ζεύγους δημόσιου/ιδιωτικού κλειδιού σε SSH

Σχετικά με τη δεύτερη περίπτωση, τα πράγματα είναι κάπως ξεκάθαρα καθώς και οι τέσσερις αλγόριθμοι κατά την μεταφορά του μεγάλου αρχείου παρουσιάζονται ισοδύναμοι. Ενώ, στην μεταφορά του μικρού αρχείου υπερέχει λίγο ο AES.

10.4.3 Καθυστέρηση

Μετά την εκτέλεση της εντολής ping για κάθε μια από τις γνωστές περιπτώσεις, πήραμε τα αποτελέσματα που φαίνονται στον παρακάτω πίνακα.

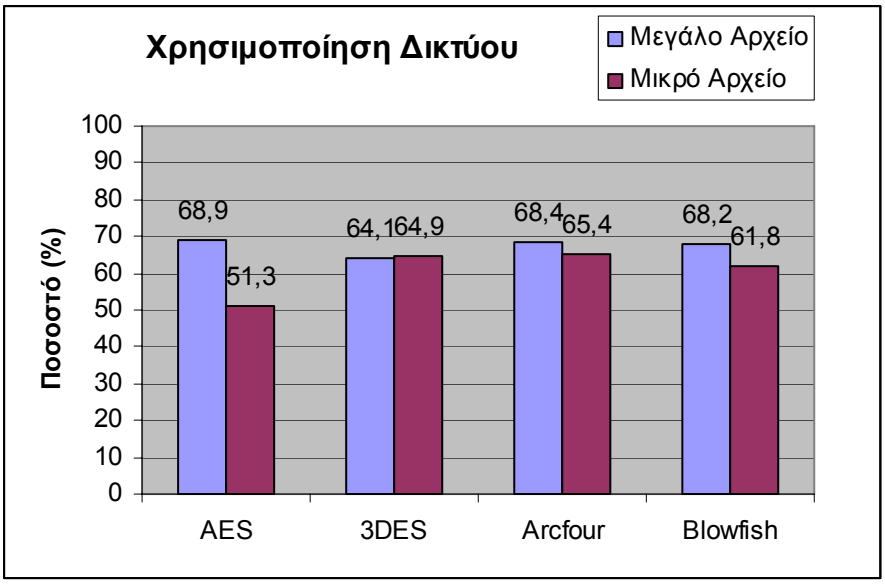
	AES	**3DES**	**Arcfour**	**Blowfish**
Συνθηματικό	24ms	23ms	23ms	23ms
Δημόσιο Κλειδί	23ms	23ms	23ms	24ms

Πίνακας 10-2 Χρόνοι καθυστέρησης στο SSH ανάλογα με τον αλγόριθμο κρυπτογράφησης που εφαρμόζεται

Η καθυστέρηση μεταξύ των αλγορίθμων στην περίπτωση της αυθεντικοποίησης με χρήση συνθηματικού δε διαφέρει και παίρνει τιμή 23ms. Ομοίως, για την περίπτωση της αυθεντικοποίησης με ζεύγος δημόσιου/ιδιωτικού κλειδιού.

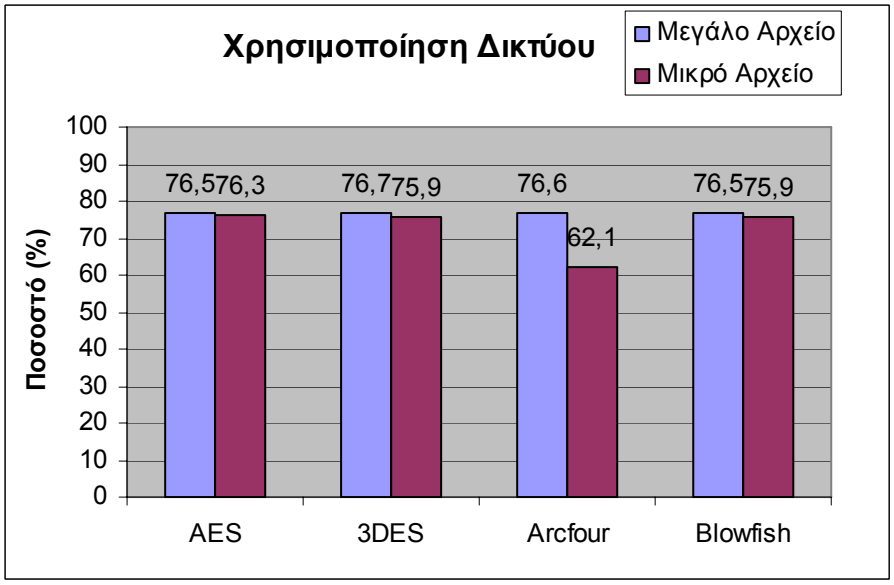
10.4.4 Χρησιμοποίηση Δικτύου

Αρχικά, εξετάζουμε την χρησιμοποίηση του δικτύου για την περίπτωση της χρήσης συνθηματικού. Παρατηρώντας τα αποτελέσματα μπορούμε να πούμε ότι η μέγιστη χρησιμοποίηση του δικτύου γίνεται από τους αλγόριθμους κρυπτογράφησης AES, Arcfour και Blowfish για το μεγάλο αρχείο ενώ για το μικρό στα ίδια επίπεδα κυμαίνονται οι αλγόριθμοι 3DES και Arcfour.



Γράφημα 10-39 Χρησιμοποίηση δικτύου με χρήση συνθηματικού για SSH

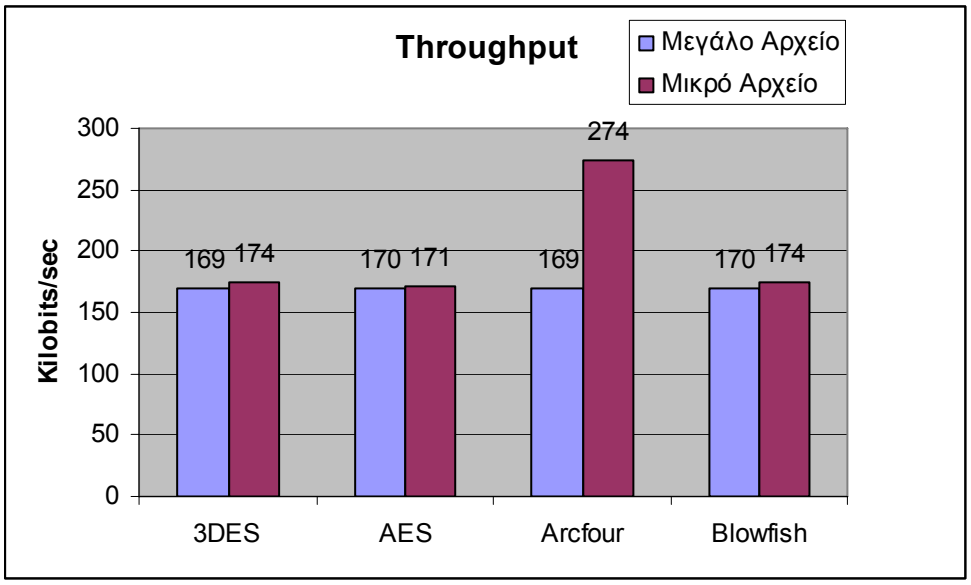
Στη συνέχεια, παρουσιάζεται το αντίστοιχο γράφημα για την περίπτωση της αυθεντικοποίησης με χρήση ζεύγους δημόσιου/ιδιωτικού κλειδιού. Κατά την μεταφορά του μεγάλου αρχείου, παρατηρείται μια ισόποση χρησιμοποίηση του δικτύου και στους τέσσερις χρησιμοποιούμενους αλγόριθμους. Ενώ, αντιθέτως φαίνεται ότι στην μεταφορά του μικρού αρχείου την μικρότερη χρησιμοποίηση του δικτύου εμφανίζει ο αλγόριθμος Arcfour.



Γράφημα 10-40 Χρησιμοποίηση δικτύου με χρήση ζεύγους δημόσιου/ιδιωτικού κλειδιού

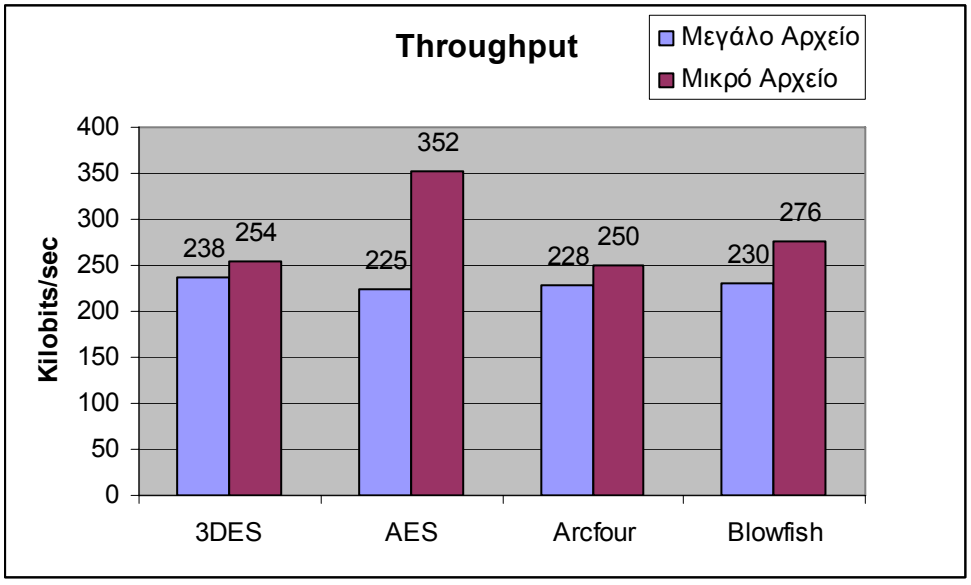
10.4.5 Throughput

Το throughput παρουσιάζει μια σταθερότητα στην περίπτωση της αυθεντικοποίησης με χρήση ζεύγους δημόσιου/ιδιωτικού κλειδιού. Εξαίρεση του κανόνα στην συγκεκριμένη περίπτωση είναι ο αλγόριθμος Arcfour όταν κρυπτογραφεί το μικρό αρχείο.



Γράφημα 10-41 Throughput με χρήση δημόσιου/ιδιωτικού κλειδιού για SSH

Το διαθέσιμο εύρος ζώνης κατά την μετάδοση του μεγάλου αρχείου όταν χρησιμοποιείται συνθηματικό για την αυθεντικοποίηση του χρήστη είναι σχετικά σταθερό και κυμαίνεται από 225 έως 238 kbps. Ενώ κατά την μετάδοση του μικρού αρχείου, παρατηρείται μια διαφοροποίηση στην περίπτωση του αλγόριθμου 3DES ο οποίος παρουσιάζει ένα throughput με τιμή 352 kbps αρκετά μεγαλύτερη των άλλων.



Γράφημα 10-42 Throughput με χρήση συνθηματικού για SSH

10.4.6 Συμπεράσματα

Το συμπέρασμα που εξάγεται από την μελέτη των πέντε προαναφερθέντων δεικτών αξιολόγησης του δικτύου στην περίπτωση της εφαρμογής SSH είναι ανάλογο με τον τρόπο που πραγματοποιείται η αυθεντικοποίηση. Έτσι, με την χρήση συνθηματικού υπερέχουν οι αλγόριθμοι κρυπτογράφησης AES και Arcfour, ενώ με την χρήση ζεύγους κλειδιών οι αλγόριθμοι 3DES και AES δείχνουν να είναι αποδοτικότεροι.

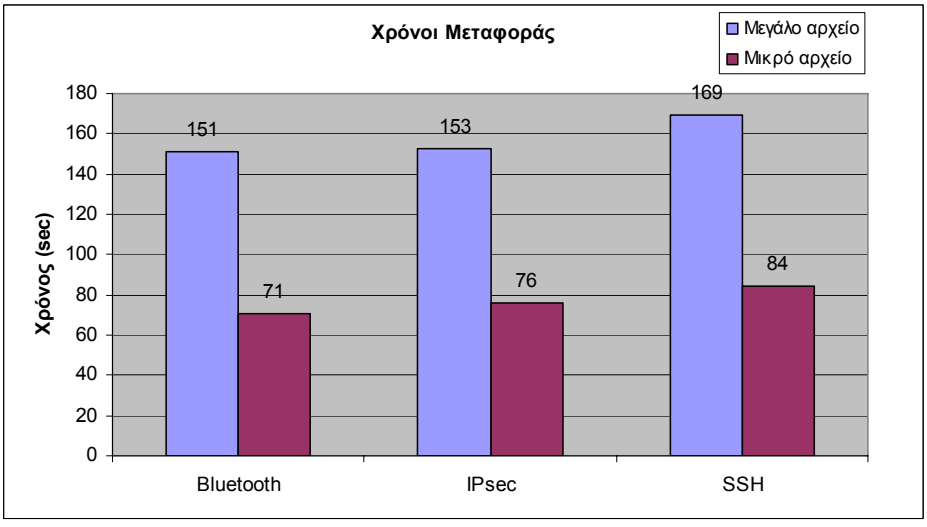
10.5 Σύγκριση περιπτώσεων

10.5.1 Βέλτιστες περιπτώσεις ανά παράμετρο δικτύου

Για κάθε μία από τις παραμέτρους του δικτύου, θα βρούμε τη βέλτιστη επιλογή μέσα απ' όλες τις μετρήσεις που κάναμε.

Για το χρόνο μεταφοράς:

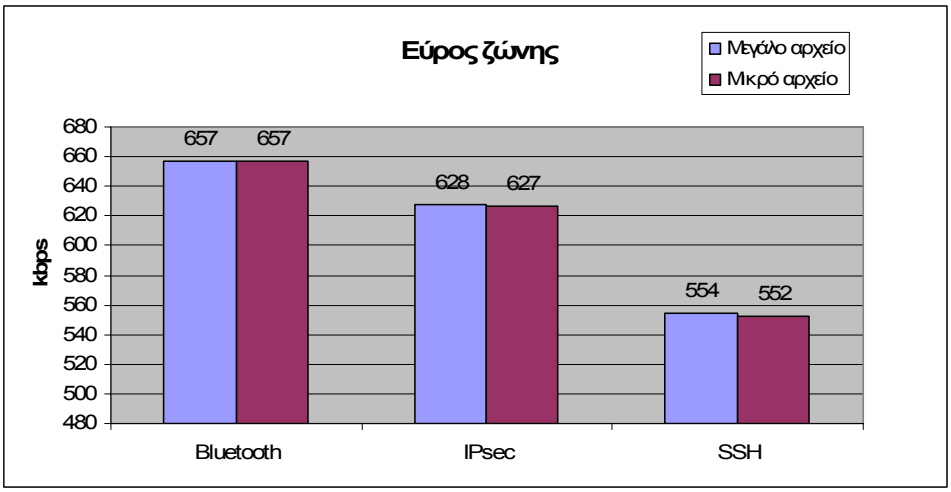
Bluetooth
Μεγάλο αρχείο: Κατάσταση ασφαλείας 3
Μικρό αρχείο: Κατάσταση ασφαλείας 1 & 3 (οι χρόνοι ισούνται)
IPsec
Μεγάλο αρχείο: Αρκετοί συνδυασμοί αλγορίθμων δίνουν το ίδιο αποτέλεσμα στις μετρήσεις μας με προβάδισμα στην αυθεντικοποίηση με χρήση πιστοποιητικών
Μικρό αρχείο: Ομοίως
SSH
Μεγάλο αρχείο: Αυθεντικοποίηση με χρήση δημοσίου κλειδιού, κρυπτογράφηση με AES
Μικρό αρχείο: Αυθεντικοποίηση με χρήση δημοσίου κλειδιού, κρυπτογράφηση με Arcfour



Γράφημα 10-43 Βέλτιστος χρόνος μεταφοράς για Bluetooth security modes, IPsec και SSH

Για το εύρος ζώνης:

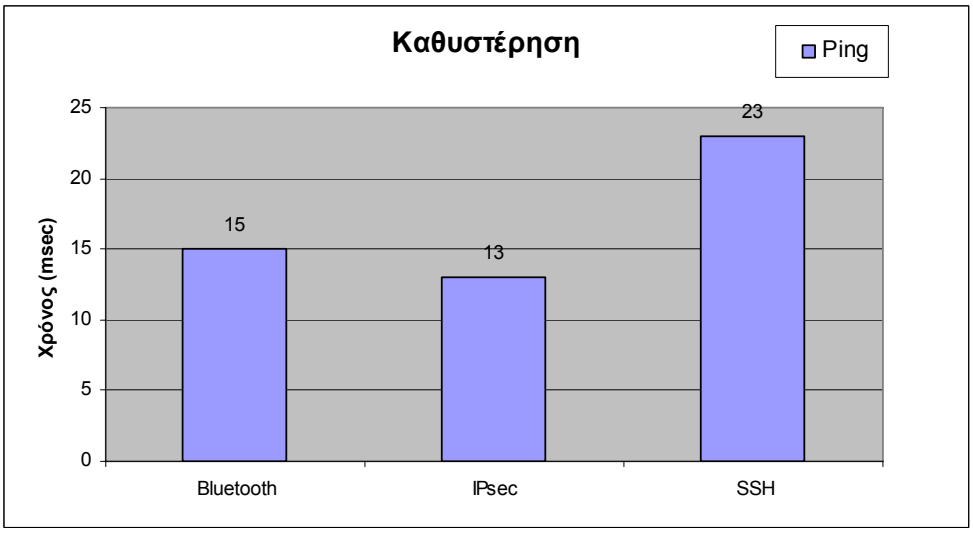
Bluetooth
Μεγάλο αρχείο: Κατάσταση ασφαλείας 3
Μικρό αρχείο: Κατάσταση ασφαλείας 1 & 3
IPsec
Μεγάλο αρχείο: Αυθεντικοποίηση με χρήση κωδικού και ακεραιότητα στο ESP με SHA1
Μικρό αρχείο: Αυθεντικοποίηση με χρήση πιστοποιητικού, κρυπτογράφηση με 3DES, ακεραιότητα με SHA1 στο ESP και SHA1 στο AH ή
Αυθεντικοποίηση με χρήση πιστοποιητικού και ακεραιότητα με MD5 στο ESP ή
Αυθεντικοποίηση με χρήση κωδικού και ακεραιότητα στο ESP με MD5
SSH
Μεγάλο αρχείο: Αυθεντικοποίηση με χρήση δημοσίου κλειδιού και κρυπτογράφηση με 3DES ή
Αυθεντικοποίηση με χρήση δημοσίου κλειδιού και κρυπτογράφηση με Arcfour
Μικρό αρχείο: Αυθεντικοποίηση με χρήση δημοσίου κλειδιού και κρυπτογράφηση με AES



Γράφημα 10-44 Βέλτιστο εύρος ζώνης για Bluetooth security modes, IPsec και SSH

Για την καθυστέρηση:

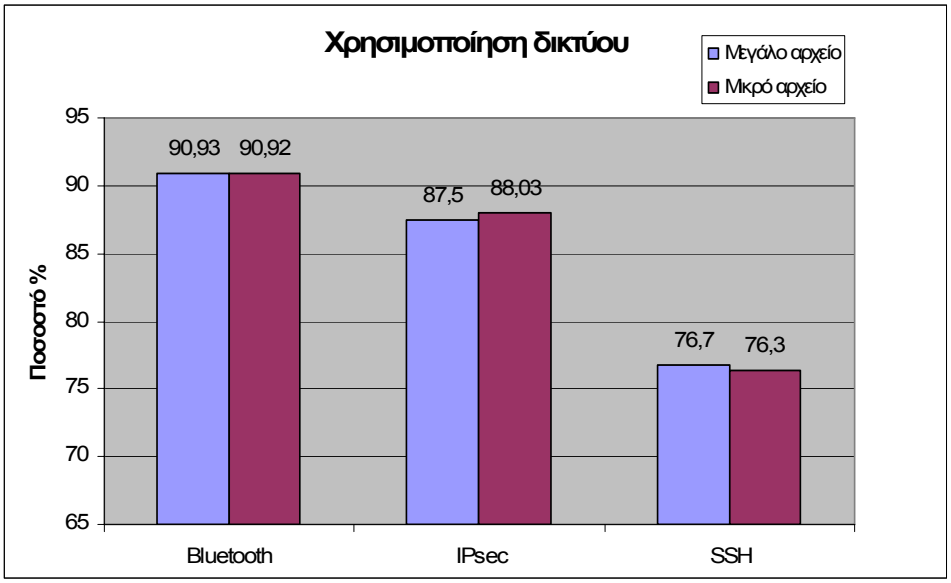
Bluetooth
Κατάσταση ασφαλείας 3 (Windows)
IPsec
Αυθεντικοποίηση με χρήση πιστοποιητικού και ακεραιότητα με SHA1 στο AH ή
Αυθεντικοποίηση με χρήση κωδικού και ακεραιότητα με MD5 στο AH ή
Αυθεντικοποίηση με χρήση κωδικού και ακεραιότητα με SHA1 στο AH ή
Αυθεντικοποίηση με χρήση κωδικού και ακεραιότητα με MD5 στο ESP
SSH
Όλοι σχεδόν οι μέθοδοι αυθεντικοποίησης και κρυπτογράφησης έχουν την ίδια καθυστέρηση.



Γράφημα 10-45 Βέλτιστη καθυστέρηση για Bluetooth security modes, IPsec και SSH

Για τη χρησιμοποίηση του δικτύου:

Bluetooth
Μεγάλο αρχείο: Κατάσταση ασφαλείας 3
Μικρό αρχείο: Κατάσταση ασφαλείας 1
IPsec
Μεγάλο αρχείο: Αυθεντικοποίηση με χρήση πιστοποιητικού και ακεραιότητα με MD5 στο ESP ή
Αυθεντικοποίηση με χρήση πιστοποιητικού και ακεραιότητα με SHA1 στο ESP ή
Αυθεντικοποίηση με χρήση κωδικού και ακεραιότητα με MD5 στο ESP
Μικρό αρχείο: Αυθεντικοποίηση με χρήση κωδικού και ακεραιότητα με MD5 στο ESP

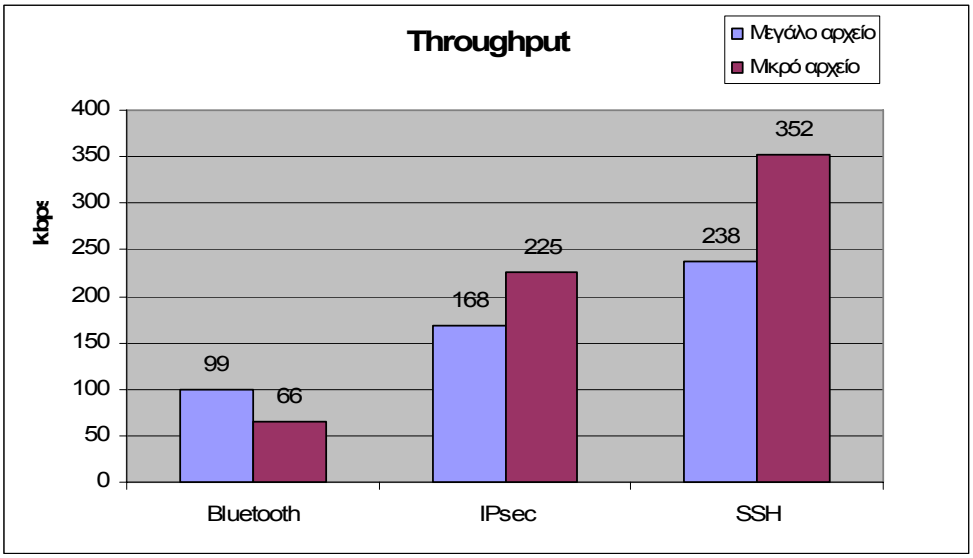


Γράφημα 10-46 Βέλτιστη χρησιμοποίηση δικτύου για Bluetooth security modes, IPsec και SSH

SSH
Μεγάλο αρχείο: Αυθεντικοποίηση με χρήση δημοσίου κλειδιού και κρυπτογράφηση με 3DES
Μικρό αρχείο: Αυθεντικοποίηση με χρήση δημοσίου κλειδιού και κρυπτογράφηση με AES

Για το throughput:

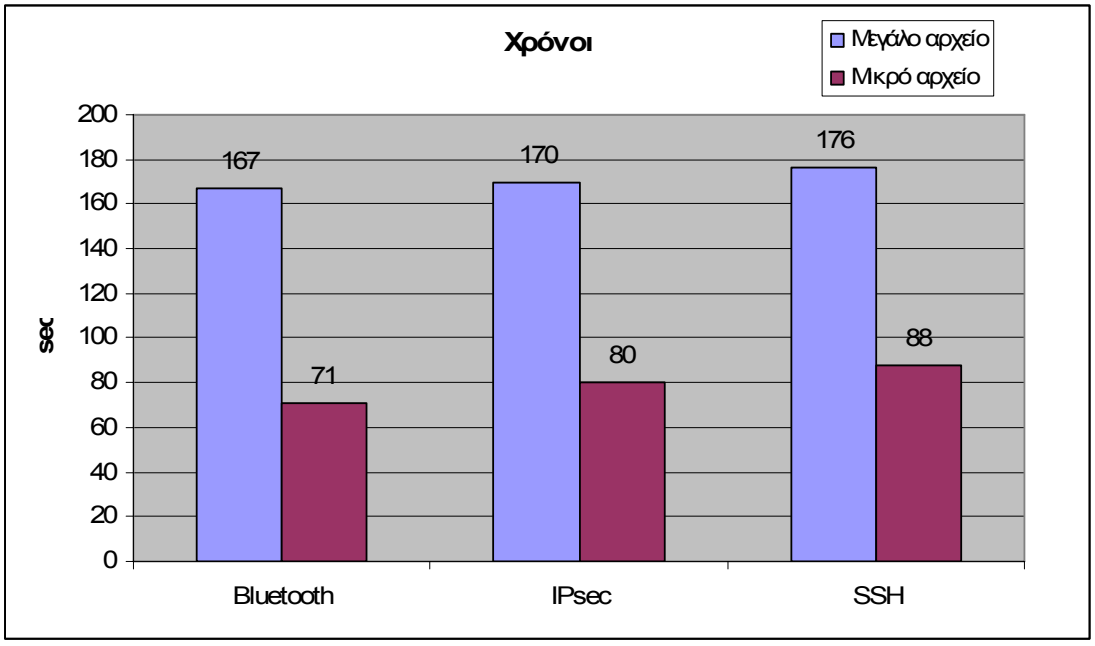
Bluetooth
Μεγάλο αρχείο: Κατάσταση ασφαλείας 1
Μικρό αρχείο: Κατάσταση ασφαλείας 1 & 3
IPsec
Μεγάλο αρχείο: Αυθεντικοποίηση με χρήση κωδικού, κρυπτογράφηση με 3DES και ακεραιότητα με MD5 στο ESP και SHA1 στο AH
Μικρό αρχείο: Αυθεντικοποίηση με χρήση κωδικού, κρυπτογράφηση με DES και ακεραιότητα με MD5 στο ESP και MD5 στο AH
SSH
Μεγάλο αρχείο: Αυθεντικοποίηση με χρήση κωδικού, κρυπτογράφηση με 3DES
Μικρό αρχείο: Αυθεντικοποίηση με χρήση κωδικού, κρυπτογράφηση με AES



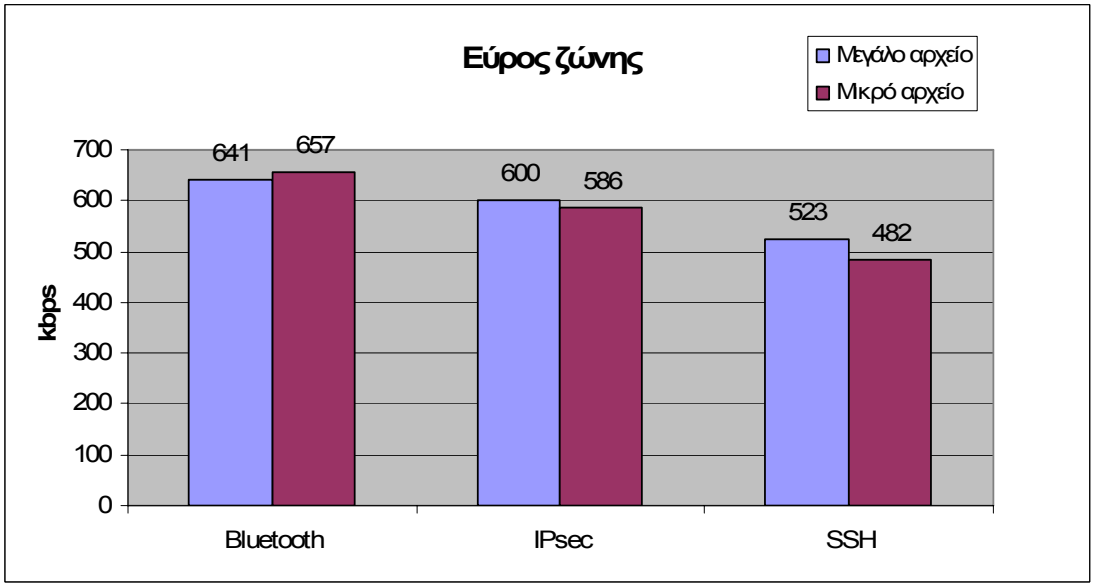
Γράφημα 10-47 Βέλτιστο throughput για Bluetooth security modes, IPsec και SSH

10.5.2 Μέσοι όροι τιμών παραμέτρων δικτύου σε Bluetooth security modes, IPsec και SSH

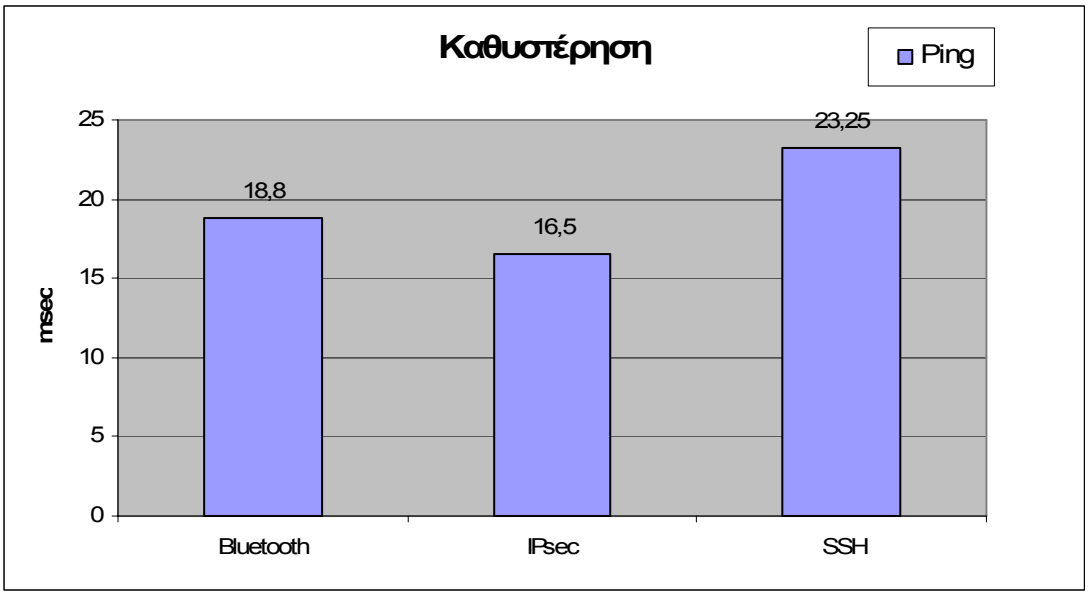
Στην υποενότητα αυτή θα βγάλουμε συγκεντρωτικά αποτελέσματα για τις καταστάσεις ασφαλείας του Bluetooth, το IPsec και το SSH. Συγκεκριμένα για κάθε μία από τις παραμέτρους του δικτύου, θα υπολογίσουμε το μέσο όρο τους για το μεγάλο και το μικρό αρχείο αντίστοιχα. Ο μέσος όρος προέρχεται από τον ισοδύναμο συμψηφισμό των δυνατών συνδυασμών μεθόδων αυθεντικοποίησης και κρυπτογράφησης για κάθε μηχανισμό ασφαλείας.



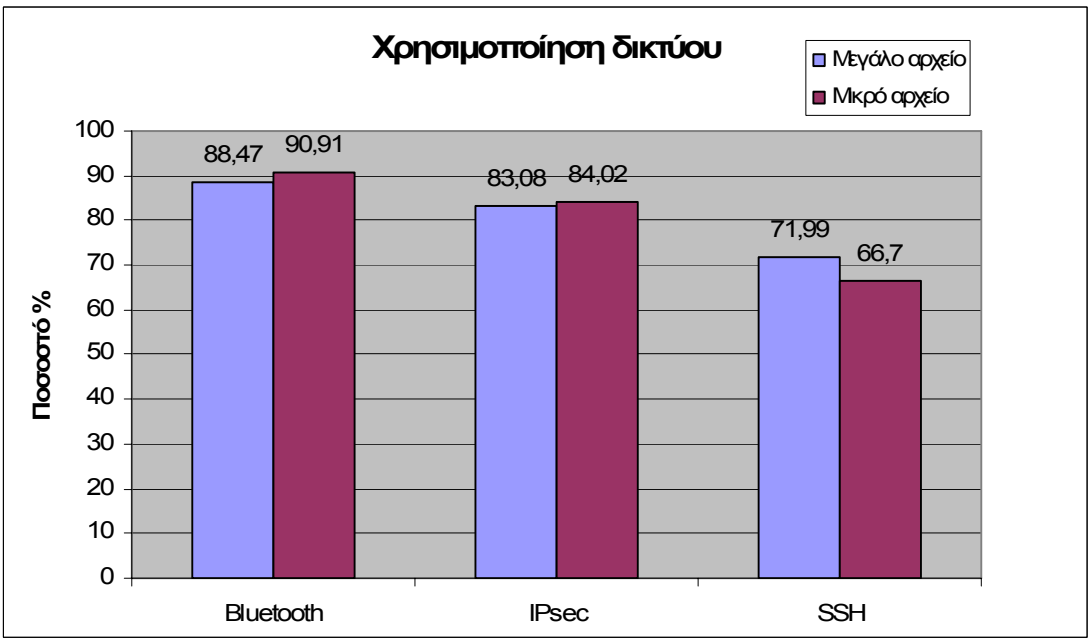
Γράφημα 10-48 Μέσος χρόνος μεταφοράς για Bluetooth security modes, IPsec και SSH



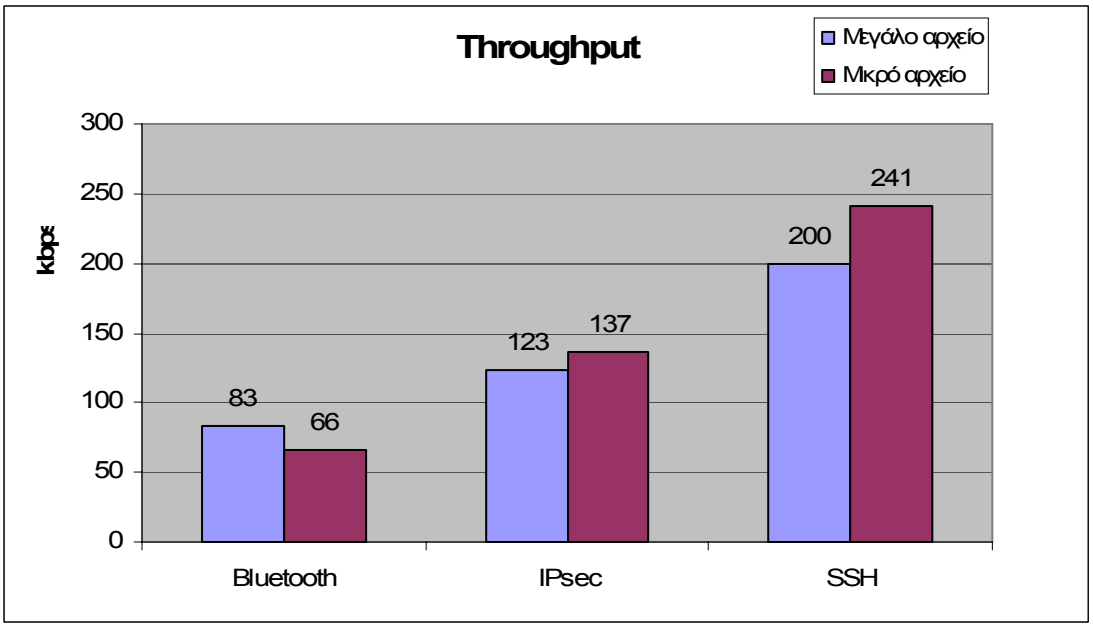
Γράφημα 10-49 Μέσο εύρος ζώνης για Bluetooth security modes, IPsec και SSH



Γράφημα 10-50 Μέση καθυστέρηση για Bluetooth security modes, IPsec και SSH



Γράφημα 10-51 Μέση χρησιμοποίηση δικτύου για Bluetooth security modes, IPsec και SSH



Γράφημα 10-52 Μέσο throughput για Bluetooth security modes, IPsec και SSH

10.5.3 Σύγκριση Bluetooth security modes, IPsec και SSH

Σύμφωνα με τα παραπάνω γραφήματα, θα συγκρίνουμε τους τρεις μηχανισμούς ασφαλείας και στη συνέχεια θα εξάγουμε τα τελικά συμπεράσματα.

Για το χρόνο μεταφοράς:

Παρατηρούμε ένα εμφανές προβάδισμα των προκαθορισμένων καταστάσεων ασφαλείας του Bluetooth. Ακολουθεί το IPsec και τρίτο σε επίδοση, με διαφορά από το δεύτερο, το SSH.

Για το εύρος ζώνης:

Παρόμοια αποτελέσματα έχουμε και στην παράμετρο αυτή. Τα γηγενή χαρακτηριστικά ασφαλείας έχουν το καλύτερο εύρος ζώνης, ακολουθεί το IPsec και τέλος το SSH. Τόσο στο χρόνο μεταφοράς όσο και στο εύρος ζώνης, βλέπουμε μια σταθερή διαφορά των καταστάσεων ασφαλείας με το IPsec και του IPsec με το SSH αντίστοιχα.

Για την καθυστέρηση:

Κάνοντας ping 100 πακέτα των 56 bytes, τη μικρότερη καθυστέρηση έχει το IPsec. Αυτό που μας κάνει εντύπωση είναι ότι αν και η κατάσταση ασφαλείας 3 έχει μεμονωμένα το μικρότερο ping, όπως διαπιστώσαμε από την προηγούμενη υποενότητα, συνολικά το IPsec έχει καλύτερη επίδοση. Έτσι, δεύτερα κατά μέσο όρο έρχονται τα security modes και τέλος το SSH.

Για τη χρησιμοποίηση του δικτύου:

Το ποσοστό χρησιμοποίησης του δικτύου μεγιστοποιείται στην περίπτωση των καταστάσεων ασφαλείας του Bluetooth. Έπεται το IPsec και τρίτο το SSH. Τα αποτελέσματα αυτά θα λέγαμε ότι είναι αναμενόμενα λαμβάνοντας υπόψη τον χρόνο μεταφοράς και το εύρος ζώνης από τα προηγούμενα γραφήματα .

Για το throughput:

Στο throughput την καλύτερη επίδοση έχει το SSH, στη συνέχεια έρχεται το IPsec και τρίτα τα security modes.

Από τα παραπάνω, παρατηρούμε ότι τα γηγενή χαρακτηριστικά ασφαλείας του πρωτοκόλλου Bluetooth έχουν την καλύτερη επίδοση στο χρόνο μεταφοράς, το εύρος ζώνης και τη χρησιμοποίηση του δικτύου. Το IPsec είναι καλύτερο όσον αφορά την καθυστέρηση και το SSH στο throughput. Άρα πρώτες στην απόδοση ενός Bluetooth προσωπικού δικτύου είναι οι καταστάσεις ασφαλείας. Ανάμεσα στο IPsec και το SSH, το IPsec βρίσκεται σε σαφώς καλύτερη θέση αφού σε όλες τις περιπτώσεις εκτός από το throughput δίνει καλύτερα αποτελέσματα.

Εν κατακλείδι, ο μηχανισμός ασφαλείας που προτείνουμε, με στόχο τη βέλτιστη απόδοση, είναι οι καταστάσεις ασφαλείας. Ακολουθεί η εφαρμογή IPsec και τέλος το SSH. Όμως, όταν θέλουμε να χρησιμοποιήσουμε κάποιο λογισμικό ή υπηρεσίες που απαιτούν υψηλότερα επίπεδα ασφάλειας, είναι προτιμότερο να χρησιμοποιήσουμε το πρωτόκολλο IPsec και ειδικότερα συνδυασμό αυτού με χρήση ψηφιακών πιστοποιητικών ως μέθοδο αυθεντικοποίησης και 3DES ως αλγόριθμο κρυπτογράφησης.

ΚΕΦΑΛΑΙΟ 11
ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΠΡΟΟΠΤΙΚΕΣ

11.1 Σύνοψη

Στην πρώτη ενότητα της εργασίας μας, αρχικά κάναμε μια εκτενή αναφορά στον τρόπο λειτουργίας του πρωτοκόλλου Bluetooth και στη συνέχεια το εξετάσαμε υπό το πρίσμα της αρχιτεκτονικής ασφαλείας που ενσωματώνει, τα σημεία ευπάθειας που έχουν ανακαλυφθεί και αντίστοιχους τρόπους επίλυσης των σημείων ευπάθειας. Κάναμε σχετική αναφορά σε δίκτυα ad hoc που υλοποιούνται με χρήση του πρωτοκόλλου Bluetooth, αναλύσαμε τα προβλήματα ασφαλείας σε αυτά και προτείναμε αντίστοιχες λύσεις.

Στη δεύτερη ενότητα, ασχοληθήκαμε με την αξιολόγηση της απόδοσης του πρωτοκόλλου Bluetooth ανάλογα με το αν χρησιμοποιεί τα γηγενή χαρακτηριστικά ασφαλείας, το πρωτόκολλο SSH ή το πρωτόκολλο IPsec. Στα δυο αυτά πρωτόκολλα εφαρμόσαμε πολλούς αλγόριθμους κρυπτογράφησης (π.χ. 3DES, DES, Arcfour) και μεθόδους αυθεντικοποίησης (π.χ. συνθηματικό, πιστοποιητικά, ζεύγος δημόσιου/ιδιωτικού κλειδιού) προκειμένου να εξετάσουμε ποιος συνδυασμός είναι αποδοτικότερος. Για την πραγματοποίηση των μετρήσεων χρησιμοποιήσαμε δυο αρχείο διαφορετικού μεγέθους (πέντε και δέκα MB αντίστοιχα). Έχοντας πραγματοποιήσει πλήθος μετρήσεων, επεξεργαστήκαμε όλες τις πληροφορίες και τελικά εξαγάγαμε ένα συμπέρασμα για την απόδοση του PAN.

11.2 Συμπεράσματα

Το πρωτόκολλο Bluetooth, όπως και άλλα ασύρματα δίκτυα, αντιμετωπίζει αρκετά προβλήματα ασφαλείας καθώς τα δεδομένα «ταξιδεύουν» στον αέρα και μπορούν να γίνουν ανά πάσα στιγμή στόχος κακόβουλων χρηστών. Βέβαια, το πρωτόκολλο Bluetooth ενσωματώνει αρκετούς μηχανισμούς ασφαλείας όπως είναι η αναπήδηση συχνοτήτων, η υπηρεσία κρυπτογράφησης και αυθεντικοποίησης. Αλλά, αυτοί οι μηχανισμοί δεν αρκούν όταν το λογισμικό που θέλει να χρησιμοποιήσει ο χρήστης απαιτεί υψηλότερο βαθμό ασφάλειας. Έτσι, η προτεινόμενη λύση είναι η παροχή αυτής της ασφάλειας στο επίπεδο του λογισμικού και ο συνδυασμός αυτού με τα γηγενή χαρακτηριστικά ασφαλείας του πρωτοκόλλου Bluetooth.

Έχοντας εφαρμόσει τα προαναφερθέντα κάνοντας χρήση των πρωτοκόλλων SSH και IPsec, σε ένα δίκτυο PAN προσπαθήσαμε να αξιολογήσουμε την απόδοση του δικτύου στις διάφορες περιπτώσεις. Για την αξιολόγηση του δικτύου χρησιμοποιήσαμε πέντε βασικές παραμέτρους: χρόνος μεταφοράς των αρχείων, καθυστέρηση, εύρος ζώνης, throughput και χρησιμοποίηση του δικτύου. Το συμπέρασμα είναι ότι χρησιμοποιώντας τις προκαθορισμένες καταστάσεις ασφαλείας στο Bluetooth έχουμε την καλύτερη απόδοση στο δίκτυο. Αλλά, αυτό δεν μας αρκεί για ένα περιβάλλον αυξημένων κινδύνων. Έτσι, από τα δυο άλλα πρωτόκολλα το IPsec σημειώνει καλύτερη απόδοση από το πρωτόκολλο SSH. Η βέλτιστη λύση είναι η χρήση του πρωτοκόλλου IPsec σε συνδυασμό με ψηφιακά πιστοποιητικά ως μέθοδο αυθεντικοποίησης και 3DES ως αλγόριθμο κρυπτογράφησης.

11.3 Προοπτικές

Μελλοντικά, θα μπορούσε να εμπλουτιστεί η παρούσα εργασία με περαιτέρω μετρήσεις για υποφορητούς υπολογιστές όπως είναι τα handhelds και τα pocket PCs. Θα μπορούσαμε έτσι να εξετάσουμε αν η απόδοση των δικτύων PAN επηρεάζεται από την επεξεργαστική ισχύ της συσκευής, που στην περίπτωση των υποφορητών υπολογιστών είναι πολύ μικρότερη των φορητών και επιτραπέζιων υπολογιστών. Επίσης, ενδιαφέρουσα προσθήκη θα ήταν η πραγματοποίηση μετρήσεων με περισσότερα των δυο αρχείων. Με αυτό τον τρόπο, θα ελέγχαμε την συμπεριφορά του δικτύου κατά την μεταφορά ενός αρχείου μεγέθους 20 MB.

Προσθέτοντας αυτά τα δυο στοιχεία στις μετρήσεις και τα συμπεράσματα που παρουσιάστηκαν στην εργασία μας, θα αποκτούσαμε μια πιο πλήρη εικόνα της συμπεριφοράς των δικτύων PAN που χρησιμοποιούν το πρωτόκολλο Bluetooth.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Τσουμελέας Ηλίας, *Ασφάλεια Τηλεπικοινωνιών,* 2004

[2] Ericsson, *Bluetooth beginner's guide*

[3] Hewlett Packard Smart Handheld Group, *Bluetooth technology overview*

[4] The official Bluetooth membership site, https://www.bluetooth.org

[5] Unwired revolution, http://www.myphone.gr

[6] The official Bluetooth wireless info site, http://www.bluetooth.com

[7] Christian Gehramann, Joakim Persson and Ben Smeets, *Bluetooth Security*

[8] Nikhil Anand - *An overview of Bluetooth Security,* 2001

[9]Bluetooth resource center, www.palowireless.com/infotooth

[10] Bluetooth Tutorial – Profiles, www.palowireless.com/infotooth/tutorial/profiles.asp

[11] Bluetooth profiles, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wcecomm5/html/wce50conBluetoothProfiles.asp

[12] Bruce Potter - *Security optional*

[13] Richard Barber - *Security in a mobile world: is Bluetooth the answer?,* 2001

[14] Juha Vainio, *Bluetooth security*, 2000, http://www.niksula.cs.hut.fi/~jiitv/bluesec.html

[15] Catharina Candolin, *Security issues for wearable computing and Bluetooth technology*

[16] Wireless Security, http://www.bluetooth.com/help/security.asp

[17] Sill Janssens, *Preliminary study: Bluetooth Security,* 2005

[18] Word Ford Long, *Overview of Bluetooth security*, 2003

[19] Joakim Persson and Ben Smeets, *Bluetooth Security – An overview,* 2000

[20] Bluetooth SIG Security expert group, *Bluetooth Security White Paper,* 2002

[21] Imrich Chlamtac, Marco Conti and Jennifer J.-N. Liu, *Mobile Ad hoc networking: imperatives and challenges*

[22] JiHyuck, Jesung Kim, Yong-suk Kim, Joong Soo Ma, A three-phase ad hoc network formation protocol for Bluetooth systems

[23] Patrick Murphy, Erik Welsh and J. Patrick Frantz, *Using Bluetooth for Short-Term Ad Hoc Connections Between Moving Vehicles: A Feasibility Study*

[24] Goonewardene Rohan and Baburam Arun, *Bluetooth Ad-hoc Networking for Inter-Vehicle Communication*

[25] Refik Molva and Pietro Michiardi, *Security in Ad hoc networks*

[26] Bruce Potter, *Bluetooth "vulnerabilities"*

[27] Mark Rowe and Tim Hurman, *Bluetooth security: Issues, threats and consequences, 2004,* http://www.pentest.co.uk/documents/wbf_slides.pdf

[28] Rob Flickenger, *Wireless hacks,* 2003

[29] Trifinite group and Bluetooth projects, http://trifinite.org

[30] Sil Janssens, *Attacking Bluetooth devices,* 2004, http://student.vub.ac.be/~sijansse/2e%20lic/BT/Voorstudie/PreliminaryStudy.pdf

[31] Sil Janssens, *Bluettoh security tools,* 2005, http://student.vub.ac.be/~sijansse/2e lic/BT/Tools/Tools.pdf

[32] Adam Laurie, Marcel Holtmann and Martin Herftur, *Hacking Bluetooth enabled mobile phones and beyond*

[33] Bluetooth security threat starting to spread, http://www.technewsworld.com/story/40124.html

[34] Hannover Fairground - *Bluesnarfing*

[35] Daniel Cvroek and Vaclav Matyas, *Pseudonimity in the light of edvidence-based trust*

[36] John Douceur, *The Sybil attack*

[37] Jean-Marc Seigneur, Alan Gray and Christian Damsgaard Jensen, *Trust transfer: encouraging self-recommendations without Sybil attack*

[38] Glenn Mahoney, *Trust, distributed systems and the Sybil attack,* 2002

[39] Suse Linux – Administration guide

[40] BlueZ – Official Linux Bluetooth protocol stack, http://www.bluez.org

[41] RedFang - Bluetooth discovery tool, http://www.securiteam.com/tools/5JP0I1FAAE.html

[42] @stake, http://www.atstake.com

[43] Γκρίτζαλης Στέφανος, Κάτσικας Σωκράτης και Γκρίτζαλης Δημήτρης, *Ασφάλεια δικτύων υπολογιστών*, 2003

[44] Αποστολόπουλος Παναγιώτης, Γεωργιάδης Παύλος και Τζαβέλλας Σπυρίδων, Εισαγωγή στο IPsec

[45] Douglas E. Comer, *Internetworking with TCP/IP*

[46] Μάγκος Κώστας και Νιξαρλίδης Άρης, *Ασφάλεια στο διαδίκτυο*

[47] IPsec RFC, http://rfc.net/rfc2411.html

[48] IPsec: secure IP over the internet, http://lartc.org/howto/lartc.ipsec.html

[49] An illustrated guide to IPsec, http://www.unixwiz.net/techtips/iguide-ipsec.html

[50] Step-by-Step Guide to Internet Protocol Security, http://www.microsoft.com/windows2000/techinfo/planning/walkthroughs/default.asp

[51] Certificate management and inastallation with OpenSSL, http://www.gagravarr.org/writing/openssl-certs/index.shtml

[52] OpenSSL, http://www.openssl.org

[53] OpenSSL Documentation, http://sial.org/howto/openssl

[54] OpenSSL certificate cookbook, http://www.pseudonym.org/ssl/ssl_cook.html

[55] Simple CA for OpenBSD based VPN, http://klake.org/~jt/mkca

[56] Cygwin, http://www.cygwin.com

[57] OpenSSH, http://www.openssh.org

[58] The Secure Shell FAQ, http://www.ayahuasca.net/ssh/ssh-faq.html#toc1

[59] How to install OpenSSH sshd server and sftp server on Windows, http://pigtail.net/LRP/printsrv/cygwin-sshd.html

[60] SSH authentication via public/private keypairs, http://www.modwest.com/help/kb20-90.html

[61] Guillermo A. Francia III, Aditya Kilaru, Le Phuong and Mehul Vashi, *An empirical study of Bluetooth performance*

[62] N. Golmie, O. Rebala, *Techniques to improve the performance of TCP in a mixed Bluetooth and WLAN Environement*

[63] Martin Connoly and Cormac J. Sreenan, *Analysis of UDP performance over Bluetooth*

[64] S. Zeadally, A. Banda, A.Kumar, *Improving Bluetooth performance in 802.11 interfere environments*

[65] Daniele Miorandi, Carlo Caimi, Andrea Zanella, *Performance Characterization of a Bluetooth Piconet with Multi-Slot Packets*

[66] Carlos de Morais Cordeiro, Djamel Sadok, Dharma P. Agrawal, *Modeling and evaluation of Bluetooth MAC protocol*

[67] Ethereal, http://www.ethereal.com