Ανώτατο Τεχνολογικό Ίδρυμα Θεσσαλονίκης
Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Ηλεκτρονικής

Επίδραση των Μηχανισμών Ασφαλείας στην Απόδοση των Ασυρμάτων LAN/MAN IEEE802.11

Κωδικός: 06222ΥΣ

Καθηγητής: Πούρος Σωτήριος

Χρίστος Ζάχος
ΚΑΣ: 598022

Θεσσαλονίκη 2007

Στους γονείς μου,
Κωνσταντίνο και Ελένη,
και στη Νάνσυ

Περίληψη

Στην παρούσα πτυχιακή εργασία εξετάζεται πειραματικά η επίδραση των διαφόρων μηχανισμών ασφαλείας στην απόδοση των ασυρμάτων τοπικών και μητροπολιτικών δικτύων IEEE 802.11. Για την πλήρη κατανόηση του θέματος της απόδοσης και της ανάγκης ύπαρξης των παραπάνω μηχανισμών, εξετάζονται οι παράγοντες του φυσικού στρώματος και του στρώματος ζεύξης δεδομένων που την επηρεάζουν και παρουσιάζονται οι τύποι των επιθέσεων. Επίσης, στα πλαίσια του θέματος, αναλύονται όλοι οι τρόποι κρυπτογράφησης και πιστοποίησης που έχουν δημοσιευτεί από το IEEE, καθώς και οι αδυναμίες τους και οι τρόποι εφαρμογής τους.

Abstract

In this paper, I survey experimentally the effect of the various security mechanisms over the throughput of the IEEE 802.11 wireless local and metropolitan networks. For the full understanding of the concept of performance and the need of the above mechanisms, I review the factors of physical and data link layer in regard and I represent the types of attack. Moreover, in the scope of security, I survey all the means of encryption and authentication published by the IEEE, included their weaknesses and ways of implementation.

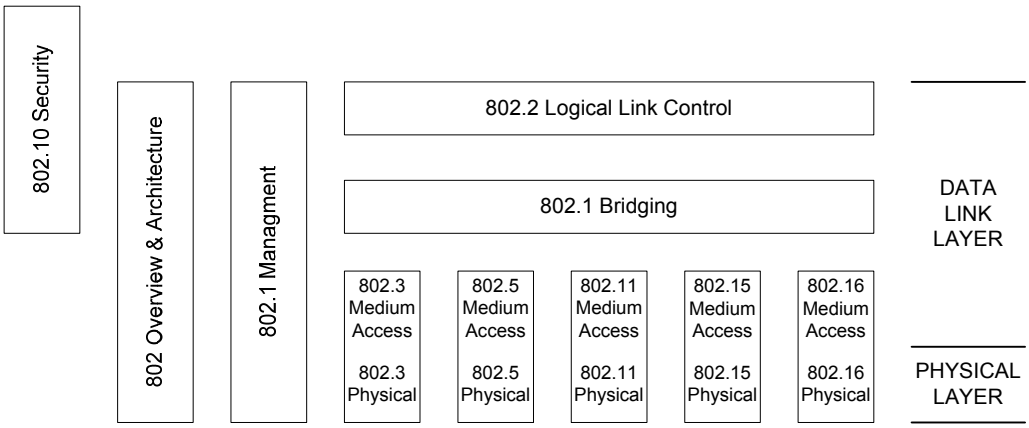
Περιεχόμενα

Κεφάλαιο 1.
Εισαγωγή στα Ασύρματα Δίκτυα IEEE 802.11

Τα ασύρματα δίκτυα της οικογενείας 802.11 βρίσκονται πλέον παντού. Ο όρος WiFi hotspot έχει γίνει της μόδας όχι μόνο σε χώρους εργασίας και σταθμούς μέσων μαζικής μεταφοράς αλλά και σε χώρους διασκέδασης. Ασύρματες κάρτες δικτύου ολοκληρώνονται σε κινητά τηλέφωνα, φωτογραφικές μηχανές, παιχνιδομηχανές, ακόμα και σε οικιακές συσκευές. Τα ασύρματα δίκτυα έγιναν ευρέως διαδεδομένα κυρίως γιατί είναι εύκολα στην υλοποίηση και στην χρήση τους. Παρ' όλα αυτά, η τεχνολογία που κρύβεται πίσω από την υλοποίηση, αν και διαφανής για τον τελικό χρήστη, είναι κάθε άλλο παρά απλή.

1.1 Τοπικά και Μητροπολιτικά Δίκτυα 802

Το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE) είναι υπεύθυνο για την προτυποποίηση σχεδόν του συνόλου των τεχνολογιών που αφορούν τα τοπικά και μητροπολιτικά δίκτυα. Στο παρακάτω σχήμα φαίνεται η διαστρωμάτωσή τους σύμφωνα με το πρότυπο αναφοράς OSI.



Σχήμα 1. 1

Το IEEE χωρίζει το στρώμα ζεύξης δεδομένων σε δύο υποστρώματα. Το πάνω υπόστρωμα Logical Link Control είναι κοινό και ανεξάρτητο του φυσικού στρώματος (PHY), πράγμα που κάνει εξαιρετικά εύκολη την επικοινωνία μεταξύ των διαφορετικών τεχνολογιών. Το κάτω υπόστρωμα, Media Access Control (MAC), ορίζει την πρόσβαση των συμμετεχόντων στο δίκτυο στο φυσικό μέσο. Λόγω της στενής σχέσης με το φυσικό στρώμα, τα πρότυπα για MAC και PHY δημοσιεύονται ως ένα. Τα κυριότερα είναι τα παρακάτω:

- 802.3 CSMA/CD Access Method and PHY (Ethernet)
- 802.5 Token Ring Access Method and PHY
- 802.11 Wireless LAN MAC and PHY (WiFi)
- 802.15 Wireless MAC and PHY for Personal Area Networks

- 802.16 Air Interface for Fixed Broadband Wireless (WiMax)

1.2 Πρότυπα Ασυρμάτων Δικτύων 802.11

Ο όρος δίκτυα 802.11 περιλαμβάνει μια συλλογή προτύπων που αφορούν το PHY και το MAC, καθώς και επιμέρους στοιχεία για την αύξηση της απόδοσης και της ασφάλειας των ασυρμάτων δικτύων. Τα πρότυπα που έχουν δημοσιευτεί, προς το παρόν, είναι:

- 802.11 – αρχικό MAC και PHY στα 1 και 2 Mbps
- 802.11a – επέκταση PHY στα 54 Mbps και 5GHz
- 802.11b – επέκταση PHY στα 11 Mbps και 2,4GHz
- 802.11d – πολλαπλοί ρυθμιστικοί φορείς
- 802.11e – ποιότητα υπηρεσίας (QoS)
- 802.11f – πρωτόκολλο επικοινωνίας μεταξύ Access Points
- 802.11g – επέκταση PHY στα 54 Mbps και 2,4GHz
- 802.11h – έλεγχος ισχύος εκπομπής
- 802.11i – ασφάλεια
- 802.11j – ορισμός καναλιών για την Ιαπωνία στα 5GHz
- 802.11k – μέτρηση
- 802.11m – συντήρηση
- 802.11n[1] – επιπλέον αύξηση της ταχύτητας στα 2,4GHz

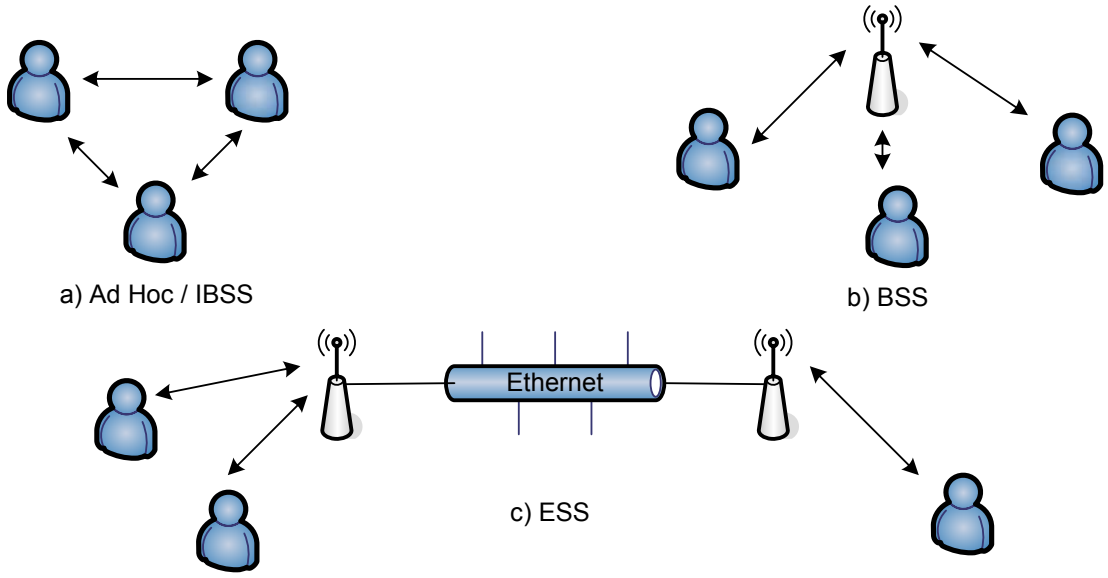
1.3 Τοπολογίες Ασυρμάτων Δικτύων

Τα ασύρματα δίκτυα αποτελούνται από τις ασύρματες κάρτες δικτύου (Network Interface Cards, NIC) και σταθμούς βάσεις ή σημεία πρόσβασης τα *Access Points* (AP). Η λογική ομαδοποίηση διαφόρων συσκευών για την δημιουργία δικτύου ονομάζεται *Service Set*.
Σε ένα ασύρματο τοπικό δίκτυο η πρόσβαση επιτυγχάνεται με την εκπομπή (broadcast) σήματος σε συγκεκριμένες ραδιοσυχνότητες. Με μέσο διάδοσης τον αέρα δεν υπάρχει τρόπος χωρικού διαχωρισμού ενός service set από ένα άλλο εντός εμβέλειας και κοινής μπάντας συχνοτήτων. Ο διαχωρισμός των πλαισίων του κάθε service set γίνεται μετά την λήψη τους με την βοήθεια του *Service Set Identifier* (SSID). Όσες συσκευές είναι ρυθμισμένες με το ίδιο SSID συμμετέχουν στο ίδιο δίκτυο.
Όταν υπάρχει Access Point στο δίκτυο, αποτελεί το κοινό σημείο επικοινωνίας των συσκευών. Οι κύριες λειτουργίες ενός AP είναι η σύνδεση των ασυρμάτων τερματικών με την ενσύρματη υποδομή του τοπικού δικτύου και η υλοποίηση των μηχανισμών ασφάλειας.

Τα ασύρματα δίκτυα είναι ευέλικτα από τον σχεδιασμό τους και υπάρχουν τρεις διαθέσιμες φυσικές τοπολογίες:

[1] Πρότυπο προς έκδοση (Απρίλιος 2007).

- Independent Basic Service Set (IBSS)
- Basic Service Set (BSS)
- Extended Service Set (ESS)



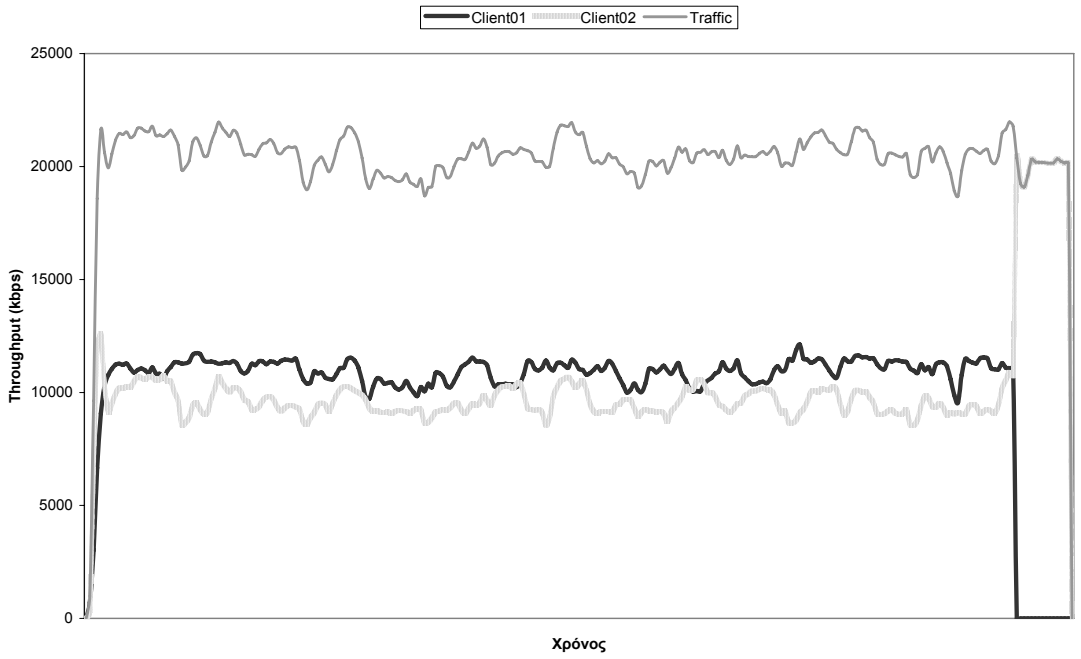
Σχήμα 1. 2

Η τοπολογία IBSS ή Ad Hoc δημιουργείται χωρίς την παρουσία AP και είναι στην ουσία ένα απλό peer-to-peer τοπικό δίκτυο. Όλοι οι σταθμοί επικοινωνούν άμεσα ο ένας με τον άλλο. Τα Ad Hoc δίκτυα είναι μικρά και έχουν ελάχιστη διάρκεια ζωής. Επίσης, λόγω έλλειψης AP δεν υπάρχει τρόπος σύνδεσης σε ενσύρματο δίκτυο.
Ένα BSS αποτελείτε από σταθμούς που επικοινωνούν μέσω ενός AP. Σε αντίθεση με τα Ad Hoc, ο χρόνος εκπομπής του κάθε σταθμού δεν γίνεται με κατανεμημένο τρόπο αλλά ελέγχεται από το AP. Συνήθως, το BSS συνδέεται με την ενσύρματη υποδομή.
Η σύνδεση πολλαπλών BSS μεταξύ τους σχηματίζει ένα ESS. Η σύνδεση δεν είναι υποχρεωτικά ενσύρματη αλλά η συνηθέστερη διάταξη είναι πολλά AP να συνδέονται στο σύστημα διανομής του Ethernet για αύξηση της κάλυψης ή/και του διαθέσιμου εύρους ζώνης του ασυρμάτου δικτύου.

1.3.1 Επίδραση Λογικής Τοπολογίας

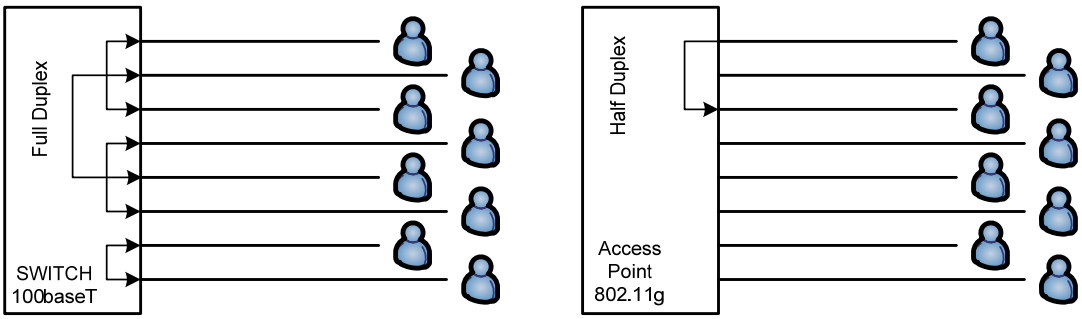
Άσχετα με την φυσική τοπολογία που συνήθως είναι αστέρας με το AP στο κέντρο του, όλα τα ασύρματα τερματικά ανήκουν στον ίδιο τομέα σύγκρουσης (collision domain) οπότε η λογική τοπολογία είναι *δίαυλος*. Το μέσο είναι κοινό και συνεχές: ο αέρας. Το αντίστοιχο στα γνωστά δίκτυα Ethernet είναι τοπολογία αστέρα με κέντρο ένα hub.
Η λογική τοπολογία διαύλου έχει μεγάλο αντίκτυπο στην απόδοση των δικτύων 802.11. Το βασικό αρνητικό είναι ότι το εύρος ζώνης διαμοιράζεται στους συμμετέχοντες: Σε ένα δίκτυο 802.11g με ονομαστική ταχύτητα

56Mbps, και δέκα τερματικά, μακροπρόθεσμα, η ωφέλιμη ταχύτητα του καθ' ενός θα είναι 5,6Mbps. Επίσης, το γεγονός ότι χρησιμοποιείται το ίδιο μέσο για αποστολή και λήψη δεδομένων αποκλείει επικοινωνία full duplex. Στο σχήμα φαίνεται το διάγραμμα απόδοσης δύο τερματικών που προσπαθούν να στείλουν ταυτόχρονα τον ίδιο όγκο δεδομένων, σε πραγματικές συνθήκες.



Σχήμα 1. 3

Τα παραπάνω θα πρέπει να λαμβάνονται υπ' όψη όταν γίνεται σύγκριση μεταξύ ενσύρματων και ασύρματων δικτύων. Ο πιο διαδεδομένος τρόπος δικτύωσης, αυτή τη στιγμή, είναι το Fast Ethernet (IEEE 802.3u) 100baseT στα 100Mbps με χρήση switch. Το switch επιτρέπει λειτουργία full duplex και κάθε τομέας σε κάθε θύρα του αποτελεί διαφορετικό collision domain. Αυτό εξασφαλίζει σε κάθε χρήστη 200Mbps (100 για αποστολή και 100 για λήψη). Επιπλέον, κάθε δυνατό ζεύγος χρηστών μπορεί να επικοινωνεί ανεξάρτητα από κάποιο άλλο. Στο σενάριο του σχεδίου 1.3, το switch μπορεί να έχει, θεωρητική, απόδοση 800Mbps (200 για κάθε ζεύγος). Στην ίδια περίπτωση, αλλά ασύρματα, το AP έχει απόδοση 56Mbps.



Σχήμα 1. 4

1.4 Μηχανισμοί Πρόσβασης στο Μέσο

Στα ενσύρματα δίκτυα Ethernet ο μηχανισμός που χρησιμοποιείται για πρόσβαση στο μέσο είναι, ως γνωστών, ο CSMA/CD. Εν ολίγοις, αν κάποιος σταθμός θέλει να στείλει δεδομένα, αρχικά ελέγχει το καλώδιο και περιμένει μέχρι να μην στέλνει κάποιος άλλος (Carrier Sense) και στην συνέχεια ξεκινάει η αποστολή. Εάν δύο ή περισσότεροι σταθμοί αρχίσουν να στέλνουν ταυτόχρονα υπάρχει σύγκρουση, την οποία και ανιχνεύουν (Collision Detection). Όλοι οι σταθμοί σταματούν την αποστολή, περιμένουν για ένα τυχαίο χρονικό διάστημα (backoff time) και η διαδικασία επαναλαμβάνεται.
Μια ταυτόχρονη εκπομπή στα ενσύρματα δίκτυα, δηλαδή μια σύγκρουση, είναι πολύ εύκολα ανιχνεύσιμη αφού αυξάνεται η τάση στο καλώδιο. Επίσης, το μέσο διάδοσης είναι αρκετά σταθερό και ελεύθερο από παρεμβολές και ο αποστολέας μπορεί να υποθέσει, με αρκετά μεγάλη βεβαιότητα, ότι η πληροφορία έχει φτάσει στον παραλήπτη, από την στιγμή που δεν συνέβη κάποια σύγκρουση.

1.4.1 CSMA/CA

Τα παραπάνω δεν μπορούν να εφαρμοστούν ως έχουν σε ένα ασύρματο περιβάλλον. Δεν υπάρχει καμία βεβαιότητα κατά την αποστολή και το κυριότερο, δεν υπάρχει τρόπος ανίχνευσης μιας σύγκρουσης. Αυτό οδήγησε σε ένα πιο πειθαρχημένο σχήμα γνωστό ως Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) που έχει σαν στόχο την εξ αρχής αποφυγή των συγκρούσεων. Οι κυριότερες προσθήκες και αλλαγές είναι οι παρακάτω:

- Πριν την εκκίνηση της εκπομπής, ο αποστολέας ενημερώνει για την διάρκειά της.
- Κανένας άλλος σταθμός δεν μπορεί να εκπέμψει πριν το πέρας του παραπάνω χρονικού διαστήματος.
- Ο αποστολέας δεν έχει την δυνατότητα να ξέρει αν οι πληροφορίες του έχουν φτάσει. Ο παραλήπτης θα πρέπει να στέλνει επιβεβαίωση.
- Αν δύο σταθμοί αρχίσουν να εκπέμπουν ταυτόχρονα, δεν μπορούν να ξέρουν ότι υπάρχει σύγκρουση. Μετά το τέλος της αποστολής καταλαβαίνουν ότι υπήρχε πρόβλημα γιατί δεν λαμβάνουν επιβεβαίωση.
- Σε περίπτωση που δεν ληφθεί επιβεβαίωση, οι συμμετέχοντες στο δίκτυο περιμένουν για ένα τυχαίο χρονικό διάστημα πριν επιχειρήσουν να ξαναστείλουν.

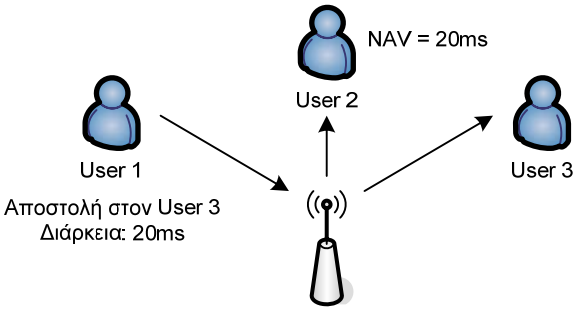
Σύμφωνα με το πρότυπο του IEEE υπάρχουν τέσσερις συνιστώσες που ολοκληρώνουν το CSMA/CA:

- Ανίχνευση του φέροντος (Carrier Sense)
- Distributed Coordination Function (DCF)
- Πλαίσια επιβεβαίωσης (ACK)

- Κράτηση του μέσου RTS/CTS (Request to Send/Clear to Send)

1.4.2 NAV

Όπως έχει περιγραφεί και παραπάνω, ένας σταθμός που θέλει να εκπέμψει πρέπει πρώτα να βεβαιωθεί ότι το μέσο δεν χρησιμοποιείται. Στα ασύρματα δίκτυα, υπάρχει περίπτωση το μέσο να είναι σε χρήση από κάποιον σταθμό ακόμα και αν δεν υπάρχει εκπομπή.
Ο τρόπος που χρησιμοποιείται από τους σταθμούς για να ελέγξουν την κατάσταση του φυσικού στρώματος λέγεται Διάνυσμα Κατανομής Δικτύου (Network Allocation Vector, NAV). Το NAV είναι ένας μετρητής που συγχρονίζεται από τα πλαίσια που εκπέμπονται στο μέσο και στην ουσία είναι ο χρόνος που χρειάζεται ο αποστολέας για την εκπομπή των δεδομένων του συν τον χρόνο για την επιβεβαίωση.

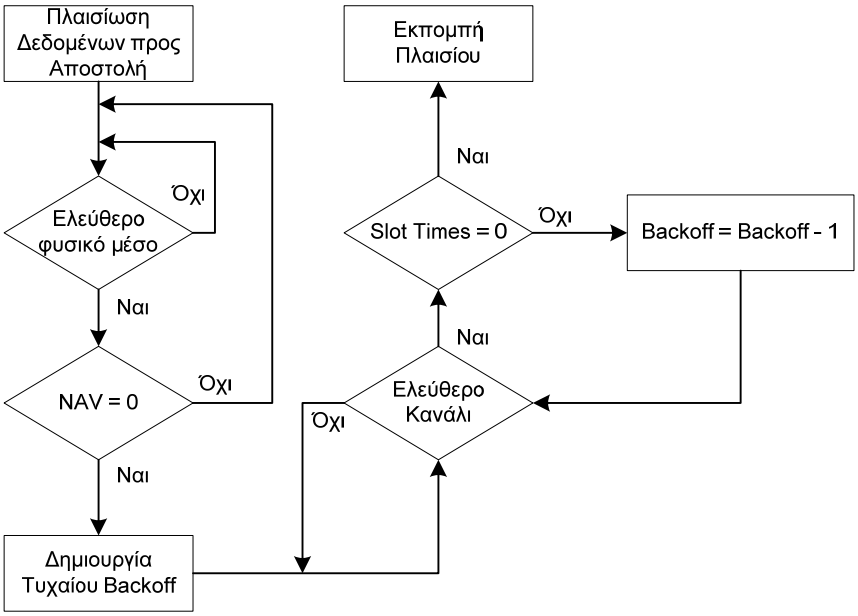


Σχήμα 1. 5

Στο παραπάνω σχήμα, όταν ο User 1 στέλνει δεδομένα στον User 3, τα πλαίσια τα λαμβάνει και ο User 2. Στα πλαίσια του 802.11 υπάρχει πεδίο με την διάρκεια της διαδικασίας αποστολής. Αυτό το πεδίο ο User 2 το χρησιμοποιεί για τον συγχρονισμό του NAV.

1.4.3 Distributed Coordination Function

Το IEEE ονομάζει την κύρια διαδικασία πρόσβασης στο μέσο για τα δίκτυα 802.11 Distributed Coordination Function, DCF.
Σύμφωνα με την λειτουργία του DCF, κάθε σταθμός που έχει δεδομένα προς εκπομπή, μετά τον μηδενισμό του NAV, θα πρέπει να περιμένει κάποιο τυχαίο χρονικό διάστημα πριν αρχίσει την εκπομπή. Χωρίς αυτή τη διαδικασία, όλοι οι σταθμοί που περιμένουν τον μετρητή NAV θα άρχιζαν να εκπέμπουν ταυτόχρονα μετά τον μηδενισμό του, με αποτέλεσμα υπερβολικό αριθμό συγκρούσεων.

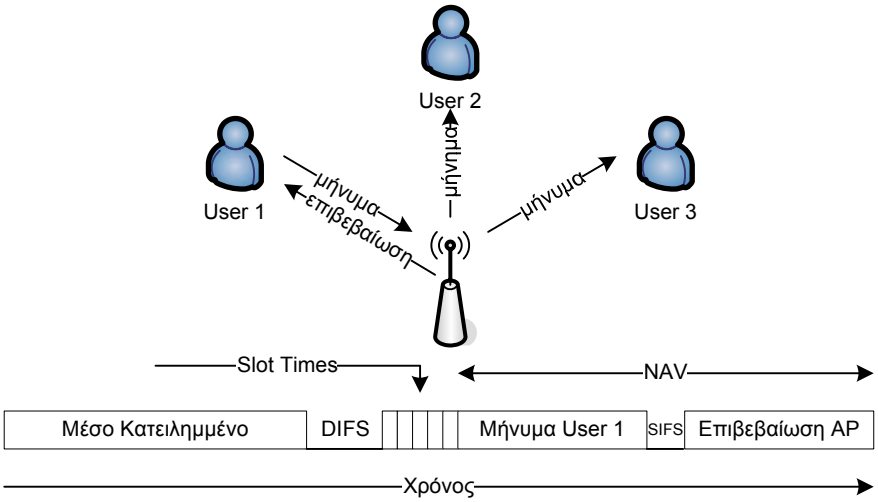


Σχήμα 1. 6

Το χρονικό διάστημα που περιμένει ο κάθε σταθμός ορίζεται από το DCF interval (DIFS) και από την τιμή ενός μετρητή που ονομάζεται backoff timer. Η τιμή του backoff δημιουργείτε από την NIC τοπικά σε κάθε σταθμό και είναι τυχαία με εύρος τιμών από 0 έως την τιμή contention window, CW. Η CW είναι μια σταθερά που εξαρτάτε από τους κατασκευαστές.
Η τιμή εκκίνησης του μετρητή backoff δεν είναι ο χρόνος μετά το DIFS αλλά ο αριθμός των χρονοθυρίδων (time slots) που πρέπει να περιμένει επιπλέον ο κάθε σταθμός. Η διάρκεια της κάθε χρονοθυρίδας ορίζεται από το πρότυπο του φυσικού στρώματος. Στο διάγραμμα του σχήματος 1.6 φαίνεται συγκεντρωτικά η διαδικασία. Ο χρόνος αναμονής του κάθε σταθμού υπολογίζεται όπως παρακάτω:

$$\text{Total} = \text{DIFS} + (\text{Backoff}) \cdot (\text{TimeSlots})$$

Τα παραπάνω σχετικά με τον χρόνο που μεσολαβεί μεταξύ δύο πλαισίων ισχύουν για κάθε τύπο εκτός από τα πλαίσια επιβεβαίωσης. Όπως αναφέρθηκε, αν ο σταθμός αποστολής δεν λάβει, εγκαίρως, επιβεβαίωση για τα απεσταλμένα δεδομένα, θεωρεί ότι έχουν απορριφτεί.

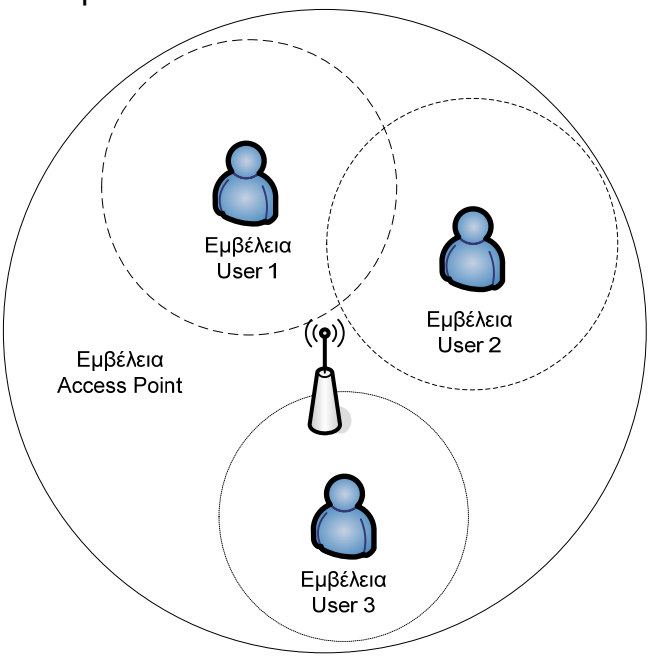


Σχήμα 1. 7

Η προτεραιότητα των πλαισίων επιβεβαίωσης εξασφαλίζεται από το MAC με δύο τρόπους: Αρχικά, κατά την κράτηση του μέσου μέσω του μετρητή NAV, συμπεριλαμβάνεται και ο χρόνος για την επιβεβαίωση. Όμως, σε ένα ασύρματο περιβάλλον, ο χρόνος του NAV είναι μια πρόβλεψη. Σε περίπτωση αστοχίας του NAV, το πρότυπο προβλέπει ένα ειδικό χρονικό διάστημα, το short interframe space (SIFS), που σε κάθε περίπτωση δίνει προτεραιότητα στα πλαίσια επιβεβαίωσης αφού η διάρκειά του είναι κατά δύο χρονοθυρίδες μικρότερη από αυτή του DIFS (σχ. 1.7).

1.4.4 Κρυμμένος Κόμβος

Κατά την περιγραφή του CSMA/CA αναφέρεται ότι κάθε σταθμός θα πρέπει να ελέγχει το φυσικό μέσο για την διαθεσιμότητα του. Αυτό, πρακτικά, σημάνει ότι κάθε σταθμός μπορεί να ακούει όλους τους άλλους. Στο σχήμα 1.8 δεν είναι αυτή η περίπτωση.



Σχήμα 1. 8

Όλοι οι χρήστες είναι εντός εμβέλειας του AP και συμμετέχουν στο ίδιο BSS άρα στο ίδιο δίκτυο. Παρ' όλα αυτά, ο User 3 είναι εκτός εμβέλειας των User 1 και User 2 οπότε δεν μπορεί να ξέρει πότε αυτοί εκπέμπουν ή όχι. Αυτό είναι γνωστό ως το πρόβλημα του κρυμμένου κόμβου (hidden node problem). Το ίδιο πρόβλημα αντιμετωπίζουν και δίκτυα στα οποία χρησιμοποιούνται δύο τεχνολογίες ταυτόχρονα, πχ. όταν συνυπάρχουν τερματικά 802.11b και 802.11g.
Η λύση στο πρόβλημα είναι η διαιτησία του AP και τα πλαίσια RTS/CTS. Ο σταθμός που θέλει να εκπέμψει στέλνει ένα πλαίσιο RTS ως αίτηση εκπομπής στο AP μαζί με τον χρόνο NAV. Το AP αποστέλλει σε όλους τους συμμετέχοντες πλαίσια CTS που τους ενημερώνει ποιος σταθμός έχει προτεραιότητα και για ποιο χρονικό διάστημα. Τα CTS είναι μια ακόμη περίπτωση πλαισίων προτεραιότητας και εκπέμπονται από το AP μετά από χρόνο SIFS.

RTS	Frame Control 2 Octets	Duration 2 Octets	Receiver MAC Address 6 Octets	Transmitter MAC Address 6 Octets	FCS 4 Octets
CTS	Frame Control 2 Octets	Duration 2 Octets	Receiver MAC Address 6 Octets	FCS 4 Octets	

Σχήμα 1. 9

Πρακτικά, η διαδικασία RTS/CTS εισάγει μεγάλη καθυστέρηση και μειώνει την απόδοση του δικτύου. Πολλά AP επιτρέπουν από τις ρυθμίσεις τους την απενεργοποίηση της όλης διαδικασίας αν ο διαχειριστής του δικτύου κρίνει ότι δεν υπάρχει πρόβλημα κρυμμένου κόμβου.

1.5 Σύνδεση Σταθμών

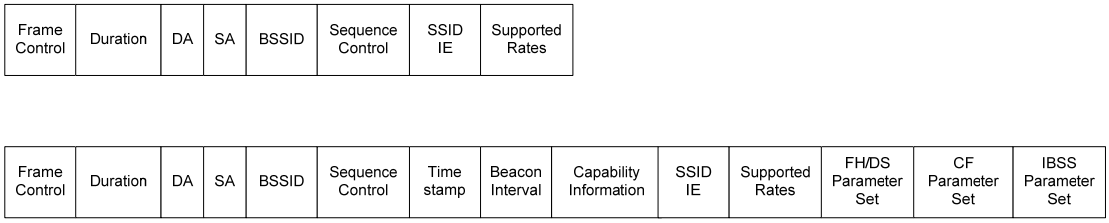
Η σύνδεση ενός σταθμού σε ένα ενσύρματο δίκτυο μπορεί να είναι τόσο απλή όσο η σύνδεση ενός καλωδίου στην κατάλληλη υποδοχή. Η συσχέτιση ενός ασύρματου τερματικού με το κατάλληλο AP μπορεί να είναι ακόμη απλούστερη, δηλαδή απλώς να βρεθεί εντός εμβέλειας και αυτό είναι ένας από τους λόγους που υπάρχουν τόσα προβλήματα ασφάλειας. Παρ' όλη την ευκολία της σύνδεσης, στο παρασκήνιο εκτελούνται τρεις διακριτές διαδικασίες:

- Διαδικασία βολιδοσκόπησης (probe).
- Διαδικασία πιστοποίησης (authentication).
- Διαδικασία συσχέτισης (association).

Κατά την εκκίνηση μιας ασύρματης κάρτας δικτύου, είναι αδύνατο να γνωρίζει οτιδήποτε για τα διαθέσιμα ασύρματα δίκτυα που βρίσκονται εντός εμβέλειας. Η διαδικασία βολιδοσκόπησης εξυπηρετεί στην ανεύρεση των διαθέσιμων δικτύων και ξεκινάει με τον σταθμό να στέλνει πλαίσια probe request σε όλα

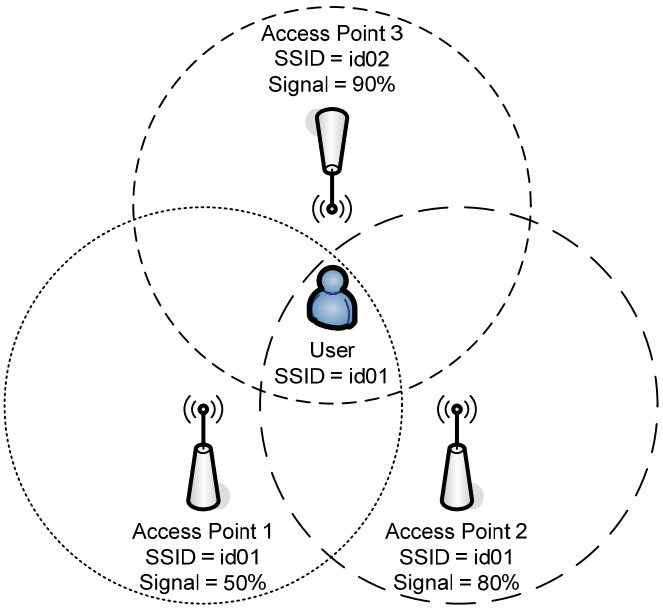
τα κανάλια και στην μικρότερη δυνατή ταχύτητα του 1 Mbps. Οι κυριότερες πληροφορίες που αποστέλλονται με αυτό τον τρόπο είναι τα SSID με τα οποία είναι ρυθμισμένος ο σταθμός και οι ταχύτητες που υποστηρίζονται από την κάρτα δικτύου.
Όταν ένα AP λάβει ένα probe request frame χωρίς σφάλματα απαντάει με ένα probe response frame που περιέχει τις απαραίτητες πληροφορίες για την συνέχεια της διαδικασίας. Τα κυριότερα τμήματα του πλαισίου probe response είναι:

- Timestamp: Χρησιμοποιείται για τον συγχρονισμό των clock του σταθμού και του AP.
- Capability Information: Οι δυνατότητες του AP στα PHY και MAC.
- SSID Element: Το SSID με το οποίο είναι ρυθμισμένο το AP.
- Support Rates Element: Όλες οι υποστηριζόμενες ταχύτητες.
- PHY Parameter Set: Αν το AP χρησιμοποιεί αναπήδηση συχνοτήτων ή κάποια από τις άλλες τεχνολογίες φυσικού μέσου.



Σχήμα 1. 10

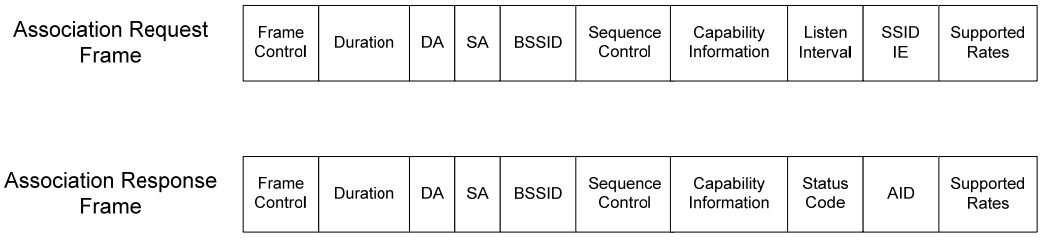
Όταν ένας σταθμός λάβει το probe response frame, εκτός των άλλων πληροφοριών, μπορεί να μετρήσει την ισχύ του σήματος του κάθε AP.
Ό μηχανισμός που χρησιμοποιείται από της ασύρματες κάρτες δικτύου για την επιλογή του καταλληλότερου AP δεν περιγράφεται σε κανένα πρότυπου του IEEE αλλά αφήνεται στους κατασκευαστές. Τα συνηθέστερα κριτήρια είναι το SSID, η ισχύς του σήματος και οι υποστηριζόμενες ταχύτητες. Για παράδειγμα, ο χρήστης στο σχήμα 1.11 θα διαλέξει να συσχετιστεί με το Access Point 2 και όχι με το AP 1 λόγω ισχυρότερου σήματος.



Σχήμα 1. 11

Με την επιλογή του AP από τον σταθμό τελειώνει η διαδικασία βολιδοσκόπησης και ξεκινάει η διαδικασία πιστοποίησης. Με διαδικασία πιστοποίησης το AP ελέγχει αν ο σταθμός ή/και ο χρήστης έχει δικαίωμα να χρησιμοποιήσει το δίκτυο. Η διαδικασία πιστοποίησης είναι άρρηκτα δεμένη με την έννοια της ασφάλειας και περιγράφεται λεπτομερώς στο αντίστοιχο κεφάλαιο.

Εάν ο σταθμός πιστοποιηθεί με επιτυχία, ξεκινάει η διαδικασία συσχέτισης του σταθμού με το AP. Η διαδικασία συσχέτισης επιτρέπει στα AP να καθορίσουν μια πύλη εισόδου, μια λογική θύρα στο δίκτυο, για τους σταθμούς. Αρχικά, ο σταθμός στέλνει ένα πλαίσιο association request με τις δυνατότητές του. Στην συνέχεια, το AP απαντάει με ένα πλαίσιο association response που ενημερώνει τον σταθμό για την αποδοχή του ή όχι στο δίκτυο. Σε περίπτωση αποτυχίας αποστέλλεται και ο κωδικός σφάλματος. Σε περίπτωση επιτυχίας το AP χαρτογραφεί τον σταθμό, δίνοντάς του ένα αναγνωριστικό κωδικό συσχέτισης (Association Identifier, AID).



Σχήμα 1. 12

Τα σημαντικότερα πεδία του πλαισίου association request είναι αυτά που αφορούν το SSID και τις υποστηριζόμενες ταχύτητες. Τα αντίστοιχα στα πλαίσια association response είναι:

- Status Code: Υποδεικνύει την επιτυχία (0x00) ή την αποτυχία και τον λόγο αυτής (πχ. 0x01 χωρίς λόγο, 0x0A αδυναμία υποστήριξης όλων των δυνατοτήτων του σταθμού κτλ.)
- Association ID: Όπως έχει περιγραφεί το AID είναι το αντίστοιχο μιας θύρας ενός hub ή ενός switch στα ασύρματα.

1.6 Πλαισίωση Δεδομένων

Η πλαισίωση δεδομένων είναι η διαδικασία προσθήκης πληροφοριών πριν (header) και μετά (trailer) τα δεδομένα του χρήστη ώστε να εξασφαλιστεί η σωστή δρομολόγησή τους στο δίκτυο.
Όπως φαίνεται στο σχήμα 1.13, σε ένα δίκτυο Ethernet οι απαραίτητες πληροφορίες για την σωστή αποστολή και λήψη του πακέτου του στρώματος δικτύου είναι:

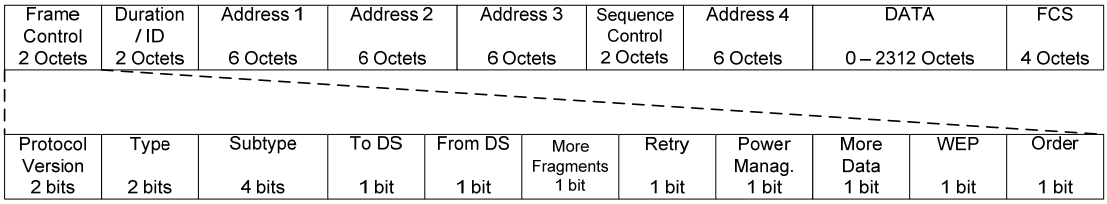
- Preamble και Start of Frame Delimiter: Ακολουθία από εναλλασσόμενα 0 και 1 που σηματοδοτούν την έναρξη του πλαισίου.
- Destination Address: Η διεύθυνση MAC του παραλήπτη.
- Source Address: Η διεύθυνση MAC του αποστολέα ώστε ο παραλήπτης να μπορεί να απαντήσει.
- Type: Ο τύπος του πρωτοκόλλου που χρησιμοποιείται στο στρώμα δικτύου (πχ. IPv4, IPv6, IPX, AppleTalk κτλ.)
- Frame Check Sequence: Μια τιμή για τον έλεγχο της ακεραιότητας των δεδομένων.

Preamble 56 bits	SFD 8 bits	Destination 48 bits	Source 48 bits	Type 16 bits	DATA μέχρι 1500 bytes	FCS 32 bits

Σχήμα 1. 13

Για ακόμα μια φορά οι απαιτήσεις και οι δυσκολίες της ασύρματης μετάδοσης των δεδομένων στο 802.11 οδήγησαν σε ένα αρκετά πολυπλοκότερο σχήμα. Παρακάτω φαίνεται η γενική μορφή ενός 802.11 MAC πλαισίου και το ανάπτυγμα του πεδίου Frame Control:

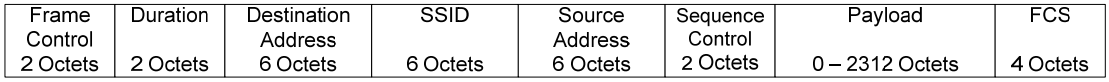
- Frame Control: Το κυριότερο πεδίο με 11 υπο-πεδία με πληροφορίες που δείχνουν τον τύπο του πλαισίου, την διαχείριση ενέργειας, την κρυπτογράφηση κτλ.
- Duration / ID: Ανάλογα με τον τρόπο λειτουργίας. Γενικά είναι ο χρόνος που θα χρειαστεί για την αποστολή και την επιβεβαίωση (βλ. NAV).
- Address 1, 2, 3, 4: Η χρήση τους εξαρτάτε από τα υπο-πεδία type και sub-type του frame control.
- Sequence Control: Υποδεικνύει αν οι πληροφορία στο πλαίσιο είναι συνέχεια από προηγούμενο πλαίσιο ή όχι και την σειρά του.
- Frame Check Sequence: Όμοια με το Ethernet.



Σχήμα 1. 14

Το 802.11, εκτός από περισσότερα πεδία στο header, προβλέπει τρεις κύριους τύπους πλαισίων στο υπόστρωμα MAC:

- Τα πλαίσια δεδομένων μεταφέρουν τα δεδομένα των χρηστών του δικτύου. Το μέγιστο "ωφέλιμο φορτίο" τους είναι 2312 bytes. Στο σχήμα χ.χ φαίνεται η μορφή ενός data frame.
- Τα πλαίσια ελέγχου διευκολύνουν την ανταλλαγή δεδομένων κατά την κανονική λειτουργία του δικτύου (βλ. RTS, CTS, ACK κτλ.).
- Τα διαχειριστικά πλαίσια χρησιμοποιούνται κατά την σύνδεση των σταθμών (βλ. probe, authentication, association κτλ.).



Σχήμα 1. 15

1.7 Απόδοση του στρώματος ζεύξης δεδομένων.

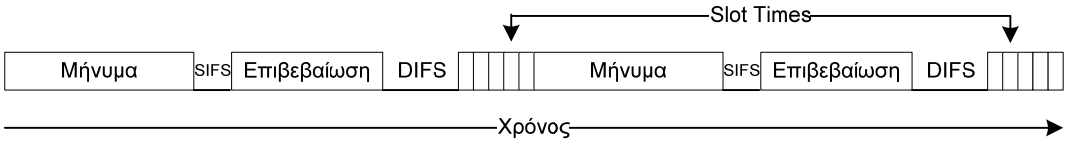
Στον παρακάτω πίνακα[2] φαίνονται οι θεωρητικές μέγιστες αποδόσεις των διαφόρων τεχνολογιών του προτύπου 802.11. Οι θεωρητικές τιμές επιβεβαιώθηκαν σε πολύ μεγάλο βαθμό στο πειραματικό μέρος της εργασίας.

Τρόπος Σύνδεσης	Διαμόρφωση	Μέγιστη Ταχύτητα Σύνδεσης	Θεωρητική Μέγιστη (TCP)	Θεωρητική Μέγιστη (UDP)
802.11b	CCK	11 Mbps	5,9 Mbps	7,1 Mbps
802.11g (με 802.11b)	OFDM / CCK	54 Mbps	11,4 Mbps	19,5 Mbps
802.11g	OFDM / CCK	54 Mbps	24,4 Mbps	30,5 Mbps
802.11a	OFDM	54 Mbps	24,4 Mbps	30,5 Mbps

Μια πρώτη παρατήρηση που μπορεί να γίνει είναι ότι η υποβάθμιση της μέγιστης ταχύτητας του link στην θεωρητική μέγιστη είναι ανεξάρτητη της τεχνολογίας φυσικού στρώματος. Η υποβάθμιση της ταχύτητας είναι η ίδια (43,52% στο UDP) στο 802.11g και στο 802.11a παρόλο που έχουν διαφορετικά PHY με το πρώτο να λειτουργεί στα 2,4GHz και το δεύτερο στα 5GHz. Οπότε το overhead οφείλεται αποκλειστικά σε διεργασίες του στρώματος ζεύξης δεδομένων που είναι κοινές σε όλους τους τρόπους σύνδεσης.

[2] Στοιχεία της Atheros Communications, Inc. Οι υπολογισμοί έγιναν με payload 1500 bytes.

Η πλαισίωση των δεδομένων εισάγει επιπλέον πληροφορία (περίπου 2% καθυστέρηση με payload 1500 bytes) και η λειτουργία του 802.11 προβλέπει και κάποια διαχειριστικά πλαίσια κατά την κανονική χρήση του δικτύου αλλά αυτά δεν είναι ικανά να εξηγήσουν μια πτώση σχεδόν 45%.
Την πραγματικά μεγάλη διαφορά από την ονομαστική ταχύτητα την κάνει η διαδικασία πρόσβασης στο μέσο και η καθυστέρηση που εισάγεται από την επιβεβλημένη επιβεβαίωση των αποσταλμένων δεδομένων (σχ. 1.16)



Σχήμα 1. 16

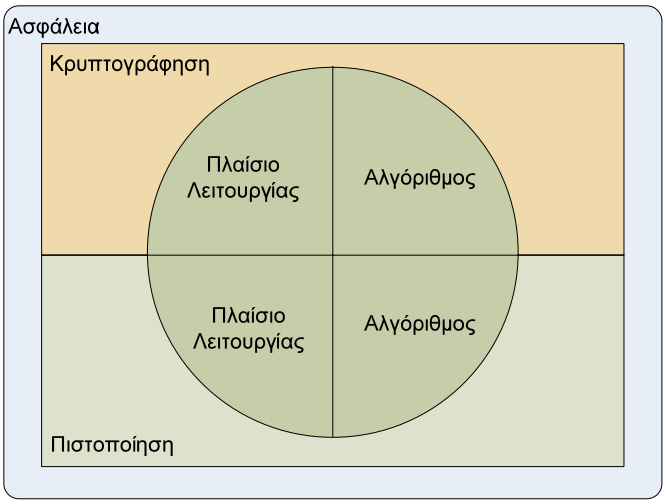
Τέλος, μια άλλη παρατήρηση που μπορεί να γίνει είναι ότι η μεγαλύτερη υποβάθμιση (63,89%) παρατηρείται σε περιπτώσεις που στο δίκτυο υπάρχουν τερματικά διαφορετικών αλλά συμβατών τεχνολογιών όπως στην περίπτωση του 802.11b και του 802.11g. Η επιπλέον καθυστέρηση μπορεί να χρεωθεί στο πρόβλημα κρυμμένου κόμβου που δημιουργείται και στην διαδικασία Request to Send / Clear to Send που καλείται να το λύσει.

Κεφάλαιο 2
Ασφάλεια

2.1 Ασφάλεια Δικτύων

Με την ευρεία χρήση των δικτύων και του Διαδικτύου για την διακίνηση κρίσιμων και προσωπικών δεδομένων και την ανάπτυξη του ηλεκτρονικού εγκλήματος, η ασφάλεια των δικτύων έχει αναχθεί σε μείζων θέμα. Παρ' όλη την κρισιμότητα του θέματος, τα συστήματα ασφάλειας προσπαθούν να απαντήσουν δύο απλά ερωτήματα:

- Ποιος έχει δικαίωμα χρήσης των πόρων ενός δικτύου και
- Αν κάποιος παράνομα αποκτήσει πρόσβαση ή υποκλέψει δεδομένα, πως αυτά θα του είναι άχρηστα.



Σχήμα 2. 1

Η απάντηση στο πρώτο ερώτημα δίνεται μέσω των μεθόδων πιστοποίησης (authentication) και στο δεύτερο μέσω της κρυπτογράφησης των δεδομένων.
Η ασφάλεια των δεδομένων δεν είναι ένα ζήτημα που απασχολεί τα δύο πρώτα στρώματα του μοντέλου αναφοράς OSI. Επίσης, όλες οι απειλές ως προς το τοπικό δίκτυο, θεωρούνται εξωτερικές και αντιμετωπίζονται, συνήθως, στο σημείο εξόδου προς τον ISP με πολιτικές ασφάλειας στους δρομολογητές, με firewall κτλ. Λόγω της φύσης του μέσου μετάδοσης στα ασύρματα δίκτυα τίποτα από τα παραπάνω δεν ισχύει. Ένα ασύρματο δίκτυο είναι δύσκολο, αν όχι αδύνατο, να περιοριστεί χωρικά και να γίνει "τοπικό".

2.2 Ασφάλεια Ασυρμάτων Δικτύων

Η ασφάλεια στα ασύρματα δίκτυα έγινε μείζων θέμα κυρίως λόγω της αποτυχίας της πρώτης υλοποίησής της. Η πρώτη προσπάθεια της IEEE δημοσιεύτηκε ταυτόχρονα με τις πρώτες προδιαγραφές για το στρώμα φυσικού μέσου (PHY) και το στρώμα ελέγχου πρόσβασης στο μέσο (MAC) στο 802.11 standard του 1999. Το πρωτόκολλο Wired Equivalent Privacy (WEP) χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης RC4 και μπορεί να χρησιμοποιηθεί για να παράσχει μυστικότητα αντίστοιχη με αυτή των ενσύρματων δικτύων που *δεν* χρησιμοποιούν καμία τεχνική κρυπτογράφησης των δεδομένων. Το WEP πολύ γρήγορα αποδείχτηκε εξαιρετικά επισφαλής και το θέμα πήρε τεράστιες διαστάσεις. Αυτό οδήγησε την IEEE στη δημιουργία του Task Group I (TGi) με αντικείμενο εργασίας την λύση του θέματος της ασφάλειας.

Το 802.11i standard δημοσιεύτηκε στις 23 Ιουλίου 2004 και προτείνει δύο λύσης: Μια μερική, αλλά προς τα πίσω συμβατή με το WEP και μια συνολικά νέα. Το Temporal Key Integrity Protocol (TKIP) μπορούσε να χρησιμοποιηθεί από την ήδη εγκατεστημένη βάση υλικού μέσω μιας απλής αναβάθμισης του firmware των Access Points (AP) και των οδηγών των καρτών δικτύου. Το TKIP χρησιμοποιεί το WEP στο σύνολό του αλλά παρέχοντας τα μέσα για την αντιμετώπιση των κενών ασφαλείας του. Το Counter Mode with Cipher-Block Chaining with Massage Authentication Code Protocol (CCMP) είναι μια λύση από το μηδέν που για την κρυπτογράφηση βασίζεται στο Advanced Encryption Standard (AES) του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας (NIST) των ΗΠΑ. Για την πιστοποίηση των χρηστών, και οι δύο λύσεις, χρησιμοποιούν το Extensive Authentication Protocol (EAP) του Internet Engineering Task Force (IETF) όπως αυτό υλοποιείτε και περιγράφετε στο 802.1x standard.

2.3 Οργανισμοί, Πρότυπα και Ακρωνύμια

IEEE: Institute of Electrical and Electronics Engineers, ο οργανισμός προτυποποίησης των ασυρμάτων δικτύων 802.11.

WiFi: Wireless Fidelity Alliance, συμμαχία κατασκευαστών με σκοπό την πιστοποίηση της διαλειτουργικότητας μεταξύ συσκευών διαφορετικών κατασκευαστών. Προήλθε από την παλαιότερη Wireless Ethernet Compatibility Alliance (WECA). Έχει τον τελευταίο λόγο στα πρότυπα και τις εμπορικές ονομασίες.

WEP: Wired Equivalent Privacy, το αρχικό πλαίσιο λειτουργίας της πιστοποίησης και της κρυπτογράφησης στο πρότυπο 802.11. Για την κρυπτογράφηση χρησιμοποιεί τον αλγόριθμο RC4.

RC4: Rivest Cipher 4, αλγόριθμος κρυπτογράφησης. Ιδιοκτησία της RSA Data Security, inc. Εφευρέθηκε από τον Ron Rivest το 1987. Χρησιμοποιείται από τα πλαίσια λειτουργίας WEP και TKIP.

TKIP: Temporal Key Integrity Protocol, πλαίσιο λειτουργίας κρυπτογράφησης. Προσπάθεια βελτίωσης των αδυναμιών του WEP. Περιλαμβάνεται στο RSN του προτύπου 802.11i.

802.11i: Το πρότυπο της IEEE που ασχολείται αποκλειστικά με την ασφάλεια των ασυρμάτων δικτύων. Περιλαμβάνει περιγραφή του RSN και του παλαιότερου WEP.

RSN: Robust Security Network, η ονομασία του IEEE για το πλαίσιο ασφάλειας μετά το αναποτελεσματικό WEP. Περιλαμβάνει τα πλαίσια λειτουργίας κρυπτογράφησης TKIP και CCMP καθώς και τα πλαίσια λειτουργίας πιστοποίησης Pre-shared Key και 802.1x προσαρμοσμένο στα 802.11.

CCMP: Counter Mode with Cipher-Block Chaining with Message Authentication Code Protocol, πλαίσιο λειτουργίας κρυπτογράφησης. Χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης Rijndael.

Rijndael: Αλγόριθμος κρυπτογράφησης. Η ονομασία προέρχεται από τους εφευρέτες του Joan Daeman και Vincent Rijmen.

AES: Advanced Encryption Standard, το επίσημο όνομα του Rijndael. Το 2002 ο Rijndael επιλέχθηκε από το NIST ως ο επίσημος αλγόριθμος κρυπτογράφησης της κυβέρνησης των ΗΠΑ (FIPS 197).

NIST: National Institute of Standards and Technology, το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ.

FIPS: Federal Information Processing Standard, ονομασία των προτύπων του NIST.

802.1x: Πρότυπο πλαισίου λειτουργίας πιστοποίησης του IEEE. Προσαρμόζει τις αρχές του EAP στα ενσύρματα δίκτυα. Προβλέπει ότι η πιστοποίηση θα γίνεται από ένα εξυπηρετητή πιστοποίησης, του οποίου την λειτουργία δεν ορίζει αλλά συνήθως είναι ένας RADIUS server.

EAP: Extensible Authentication Protocol (RFC 2284), πλαίσιο λειτουργίας πιστοποίησης. Πρότυπο του IETF για την πιστοποίηση των Dial – Up συνδέσεων.

IETF: Internet Engineering Task Force, οργανισμός που ασχολείται με την προτυποποίηση των δικτύων. Τα πρότυπα που εκδίδει είναι ελεύθερα για χρήση και τροποποίηση, χωρίς πνευματικά δικαιώματα ή πατέντες.

RFC: Request for Comments, τα πρότυπα του IETF εκδίδονται σε μορφή αρχείων για σχολιασμό.

RADIUS: Remote Access Dial – In User Service, πρότυπο που περιγράφει τις λειτουργίες ενός εξυπηρετητή πιστοποίησης καθώς και τον τρόπο που άλλες συσκευές έχουν πρόσβαση σ' αυτές τις λειτουργίες. Στην περίπτωση των ασυρμάτων δικτύων χρησιμοποιείται το πρότυπο EAP over RADIUS (RFC 2869).

EAPOL: EAP over LAN, προσαρμογή της πλαισίωσης των μηνυμάτων πιστοποίησης του EAP για ενσύρματα τοπικά δίκτυα. Περιγράφεται στο 802.1x.

PEAP, LEAP κτλ: Αλγόριθμοι πιστοποίησης που λειτουργούν με πλαίσιο πιστοποίησης το EAP. Κάποιοι είναι ανοιχτοί και κάποιοι ιδιοκτησία εταιριών. Η WiFi ορίζει πέντε απ' αυτούς ως εναλλακτικές για χρήση στα ασύρματα δίκτυα.

WPA: WiFi Protected Access, εμπορική ονομασία της WiFi Alliance για την αποφυγή των παραπάνω ακρωνύμων από τους καταναλωτές. Έχει δύο τρόπους λειτουργίας Personal και Enterprise. Το WPA Personal περιλαμβάνει κρυπτογράφηση TKIP και πιστοποίηση Pre-shared Key, ενώ το WPA Enterprise κρυπτογράφηση TKIP και πιστοποίηση EAP/802.1x.

WPA2: Βελτίωση του παραπάνω και 100% συμβατό με το RSN του 802.11i. Οι τρόποι λειτουργίας παραμένουν. Το WPA2 Personal περιλαμβάνει κρυπτογράφηση CCMP και πιστοποίηση Pre-shared Key, ενώ το WPA2 Enterprise κρυπτογράφηση CCMP και πιστοποίηση EAP/802.1x.

2.4 Τύποι Επιθέσεων

Η πρόσβαση σε ξένα δεδομένα, είτε γίνεται με κίνητρο το συμφέρον, είτε την περιέργεια, είναι πάντα γοητευτική. Δυστυχώς, σε πολλές περιπτώσεις στα ασύρματα δίκτυα είναι εκτός από γοητευτική και εύκολη. Ο στόχος των επιθέσεων δεν είναι πάντα τα δεδομένα των χρηστών αλλά και οι πόροι του δικτύου ή ακόμα και η προσωρινή αχρήστευσή του. Ανάλογα με το τι θέλει να πετύχει ο επιτιθέμενος, μπορεί να χρησιμοποιήσει διάφορες προσεγγίσεις. Γενικά, οι επιθέσεις εναντίων ασυρμάτων δικτύων μπορούν να χωριστούν σε παθητικές και ενεργητικές.

2.4.1 Παθητικές Επιθέσεις

Όλες οι επιθέσεις ξεκινούν παθητικά. Παθητικές μπορούν να χαρακτηριστούν όλες οι ενέργειες που δεν συμπεριλαμβάνουν συμμετοχή στο δίκτυο. Η πιο απλή επίθεση αυτού του τύπου είναι η συλλογή πληροφοριών. Ο στόχος αυτής της ενέργειας είναι ο εντοπισμός του δικτύου και η αποκάλυψη ορισμένων χαρακτηριστικών του. Τέτοια χαρακτηρίστηκα είναι το SSID του

ασυρμάτου δικτύου, το κανάλι εκπομπής, η μέθοδος κρυπτογράφησης, το σχήμα διευθυνσιοδότησης του στρώματος δικτύου και η συλλογή των διευθύνσεων MAC των συμμετεχόντων. Για την πραγματοποίηση αυτής της επίθεσης δεν χρειάζεται τίποτα παραπάνω από ένα Η/Υ με ασύρματη κάρτα δικτύου και ένα πρόγραμμα όπως το Network Stumbler. Εδώ να σημειωθεί ότι στις νομοθεσίες κάποιων χωρών ακόμα και η γνώση των IP διευθύνσεων θεωρείται παράνομη. Η Ελλάδα δεν συμπεριλαμβάνεται σ' αυτές.
Ένας άλλος τύπος παθητικής επίθεσης είναι η συλλογή πακέτων (packet sniffing). Στην πιο απλή περίπτωση, ο επιτιθέμενος συλλέγει τα πακέτα που ανταλλάσσονται μέσω του αέρα και προσπαθεί να ανασυνθέσει τα μηνύματα για την αποκάλυψη κάποιων χρήσιμων πληροφοριών όπως usernames, passwords κτλ. Σε περίπτωση που τα δεδομένα στέλνονται κρυπτογραφημένα, ο σκοπός είναι να αλιευτούν αρκετά πακέτα ώστε με μεθόδους κρυπτανάλυσης να αποκαλυφθούν τα κλειδιά που είναι απαραίτητα για την αποκρυπτογράφηση των δεδομένων ή την περεταίρω διείσδυση στο δίκτυο. Και σε αυτή την περίπτωση, οι γνώσεις του επιτιθέμενου μπορούν να είναι περιορισμένες. Τα απαραίτητα εργαλεία είναι ένας Η/Υ με ασύρματη κάρτα δικτύου που να υποστηρίζει promiscuous mode[3], ένα λογισμικό ανάλυσης πακέτων όπως το Ethereal και πιθανώς ένα λογισμικό όπως το AirSnort που χρησιμοποιείται για την αποκάλυψη του κλειδιού του WEP.

2.4.2 Ενεργητικές Επιθέσεις

Όπως αναφέρθηκε, οι ενεργητικές επιθέσεις απαιτούν την συμμετοχή του επιτιθέμενου στο δίκτυο. Αυτό δεν σημαίνει αυτόματα και την χρήση των πόρων ως μέλος του δικτύου, όπως και κάθε μη πιστοποιημένη σύνδεση σε ένα δίκτυο, αν και παράνομη, δεν αποτελεί επίθεση. Εάν ένα δίκτυο είναι εντελώς αφύλακτο κάποιος μπορεί να συνδεθεί μέχρι και κατά λάθος αν βρεθεί εντός εμβέλειας. Οι ενεργητικές επιθέσεις χωρίζονται σε τρεις επιμέρους κατηγορίες:

- Επιθέσεις πλαστογραφίας (forgery attacks)
- Επιθέσεις μετατροπής μηνυμάτων
- Επιθέσεις άρνησης υπηρεσίας (Denial of Service, DoS)

Ακόμα και σε ένα αφύλακτο δίκτυο, ο επιτιθέμενος που συνδέεται στο δίκτυο θα έχει πρόβλημα αν αφήσει ίχνη και εντοπιστεί. Ο καλύτερος τρόπος και να έχει πρόσβαση στο δίκτυο και να μην υπάρχει περίπτωση να εντοπιστεί είναι να παρουσιαστεί σαν κάποιος άλλος πιστοποιημένος χρήστης του δικτύου. Αυτό αποτελεί μια επίθεση πλαστογραφίας. Για την επίτευξη μιας επίθεσης πλαστογραφίας χρειάζονται στοιχεία που αποκαλύπτονται με επίθεση συλλογής πληροφοριών όπως η διεύθυνση MAC ενός πιστοποιημένου χρήστη και πιθανώς άλλα στοιχεία όπως κλειδιά κρυπτογράφησης και πιστοποίησης κτλ. Η επίθεση ολοκληρώνεται με αποστολή στον χρήστη-στόχο μηνύματος

[3] Promiscuous mode είναι η κατάσταση λειτουργίας μιας κάρτας δικτύου που λαμβάνει παθητικά όλα τα πακέτα από όλα τα δίκτυα που βρίσκονται εντός εμβέλειας χωρίς αυτή να εκπέμπει ή να συμμετέχει σε κάποιο. Είναι αδύνατο να εντοπιστεί.

απο-πιστοποίησης (deauthentication) με σκοπό να βγει από το δίκτυο και στην συνέχεια πιστοποίηση του επιτιθέμενου.
Οι επιθέσεις μετατροπής μηνυμάτων είναι γνωστές ως επιθέσεις Man-in-the-Middle. Όπως φαίνεται και από το όνομα, ο επιτιθέμενος βρίσκεται στην μέση της συνομιλίας δύο συμμετεχόντων στο δίκτυο. Στα ασύρματα δίκτυα ένας από τους συμμετέχοντες είναι πάντα το AP και ο άλλος ένας από τους χρήστες. Θεωρητικά, ο επιτιθέμενος μπορεί να αναχαιτίσει σε πραγματικό χρόνο το μήνυμα του χρήστη, να αλλοιώσει το περιεχόμενό του και να στείλει το αλλοιωμένο μήνυμα στο AP αλλά κανονική επιβεβαίωση στον χρήστη. Το αποτέλεσμα είναι ο χρήστης να νομίζει ότι το μήνυμα έχει αποσταλεί αλλά το AP να το έχει απορρίψει. Πρακτικά, κάτι τέτοιο είναι αδύνατο να γίνει σε πραγματικό χρόνο και οι επιθέσεις περιορίζονται σε επιθέσεις επανάληψης που σκοπό έχουν ή να δυσχεράνουν την χρήση του δικτύου ή σε σπάνιες περιπτώσεις την αποκάλυψη κάποιων στοιχείων για το Ethernet μέρος του δικτύου όπως οι διευθύνσεις IP κάποιων εξυπηρετητών. Γενικά, αυτού του είδους οι επιθέσεις έχουν μεγάλη δυσκολία, μεγάλη πιθανότητα να αποκαλυφθούν και μικρό αποτέλεσμα. Παρ' όλα αυτά, στα πρωτόκολλα TKIP και CCMP υπάρχει μηχανισμός αποτροπής τους.
Πολύ πιο αποτελεσματικές είναι οι επιθέσεις DoS. Ο σκοπός τους είναι η ολική αχρήστευση του ασυρμάτου δικτύου για κάποιο χρονικό διάστημα και κύριος στόχος τους είναι εταιρικά δίκτυα στα οποία ο χρόνος αδράνειας (downtime) ισοδυναμεί με μεγάλη οικονομική ζημιά. Μια επίθεση DoS μπορεί να πραγματοποιηθεί με δύο τρόπους στα ασύρματα δίκτυα. Ο πρώτος τρόπος είναι να καταληφθεί το φυσικό μέσο με τόσο δυνατά σήματα στην μπάντα λειτουργίας του δικτύου ώστε να μην είναι δυνατή η επικοινωνία μεταξύ των σταθμών. Αν και ένας φούρνος μικροκυμάτων θα μπορούσε να κάνει την δουλεία, αυτή η μέθοδος είναι αρκετά επικίνδυνη για τον επιτιθέμενο αφού είναι εύκολη στον εντοπισμό. Η δεύτερη μέθοδος για την πραγματοποίηση της επίθεσης είναι μέσω κορεσμού των πόρων του δικτύου. Πρακτικά, αυτό σημαίνει την παραγωγή τόσο μεγάλου αριθμού πακέτων (packet flooding) που όλη η επεξεργαστική ισχύς του AP να καταναλώνεται στην επεξεργασία τους. Και αυτός ο τύπος της επίθεσης μπορεί να γίνει με λογισμικό που διατίθεται ελεύθερα στο Internet. Επίσης, έχουν καταγραφεί και άλλοι τρόποι πραγματοποίησης της επίθεσης όπως η μαζική αποστολή πακέτων από-πιστοποίησης όλων των σταθμών (management frame DoS).
Οι επιθέσεις άρνησης υπηρεσίας είναι οι λιγότερο πιθανές να αποτραπούν. Το IEEE στο πρότυπο 802.11i που ασχολείται με την ασφάλεια των ασυρμάτων δικτύων δεν έχει λάβει καμία μέριμνα ενάντια στις επιθέσεις DoS αφού σε κάθε περίπτωση μένει ανοιχτή η πιθανότητα επίθεσης στο φυσικό στρώμα.

2.4.3 WarDriving και WarChalking

Οι όροι WarDriving και WarChalking αναπτύχθηκαν μαζί με τα ασύρματα δίκτυα και, αν και είναι συνδεδεμένοι με τις παθητικές επιθέσεις, δεν αποτελούν σε καμία περίπτωση επιθέσεις.
Με τον όρο WarDriving περιγράφεται η ενασχόληση κάποιου προσώπου με την αποκάλυψη και πιθανώς την χαρτογράφηση των ασυρμάτων δικτύων μιας

περιοχής. Ο σκοπός για τον οποίο κάποιος ασχολείται με το WarDriving δεν συμπεριλαμβάνεται στον όρο.
Το WarChalking προϋποθέτει το WarDriving και περιγράφει την σημείωση των δικτύων που έχουν αποκαλυφθεί, και κυρίως τα αφύλακτα, πάνω ένα ψηφιοποιημένο χάρτη ή στα αρχικά στάδια με κιμωλία (chalk) πάνω σε τοίχους ή πεζοδρόμια. Τέτοιοι χάρτες κυκλοφορούν ελεύθερα στο Internet σχεδόν για κάθε κύρια πόλη του κόσμου. Το WarChalking δεν είναι, ούτε αυτό, παράνομο.
Τα εργαλεία που χρειάζονται για WarDriving είναι τα ίδια με αυτά της επίθεσης συλλογής πληροφοριών, με την διαφορά ότι χρησιμοποιούνται μόνο τα αναγκαία για την αποκάλυψη του SSID και τον τύπο της ασφάλειας που χρησιμοποιείται. Το WarChalking μπορεί να απλοποιηθεί αν το λογισμικό που χρησιμοποιείται συνεργάζεται με δέκτη GPS.

2.4.4 Rogue[4] Access Points

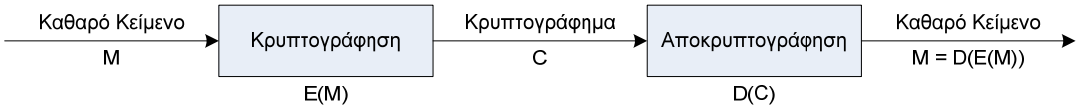
Ο όρος rogue AP (RAP) είναι, επίσης, ένας όρος που δεν παραπέμπει υποχρεωτικά σε παράνομη δραστηριότητα. Rogue χαρακτηρίζεται ένα AP που εγκαταστάθηκε χωρίς την συγκατάθεση του ιδιοκτήτη του δικτύου. Τα RAP αποτελούν πύλες εισόδου στο δίκτυο που αχρηστεύουν οποιαδήποτε προσπάθεια ασφάλειας και είναι ακόμα πιο επικίνδυνα σε δίκτυα που δεν συμπεριλαμβάνουν και ασύρματο μέρος.
Κάποιος εχθρικά διακείμενος σε μία εταιρία μπορεί να μπει στα γραφεία της και να εγκαταστήσει ένα AP σε μια ελεύθερη πρίζα που συνδέεται με το switch, χωρίς να γίνει αντιληπτός. Αυτό είναι ένα σενάριο. Κάποιος υπάλληλος της εταιρίας που έχει βαρεθεί τα καλώδια, αλλά έχει πλήρη άγνοια από ασφάλεια δικτύων (αυτός μπορεί να είναι και ο διευθυντής…), αγοράζει ένα AP και σύμφωνα με τις οδηγίες τοποθετεί την τροφοδοσία στην πρίζα και το καλώδιο δικτύου στην κατάλληλη υποδοχή της συσκευής. Με το κόστος των AP κάτω από τα 100€ και με όλα τα σύγχρονα laptop να ολοκληρώνουν ασύρματες κάρτες δικτύου, αυτό είναι ένα ακόμα πιο πιθανό σενάριο.
Σύμφωνα με έρευνες, τουλάχιστον το 20% των επιχειρήσεων στις ΗΠΑ έχουν εγκατεστημένο ένα ή περισσότερα RAP στο εταιρικό τους δίκτυο[5]. Με όποιο τρόπο και να έχουν τοποθετηθεί, τα RAP αποτελούν μεγάλο κίνδυνο για την ασφάλεια ενός δικτύου. Το αρνητικό είναι ότι για την οριστική λύση του προβλήματος απαιτούνται μέθοδοι πιστοποίησης που η υλοποίησή τους είναι κάθε άλλο παρά απλή και οικονομική.

2.5 Αρχές Κρυπτογράφησης

Κρυπτογραφία είναι η επιστήμη που ασχολείται με την ασφάλεια των μηνυμάτων. Η επιστήμη που ασχολείται με την ανακάλυψη των αδυναμιών της κρυπτογραφίας λέγεται *κρυπτανάλυση*. Ο κλάδος των μαθηματικών που ασχολείται με την κρυπτογραφία και την κρυπτανάλυση λέγεται *κρυπτολογία*.

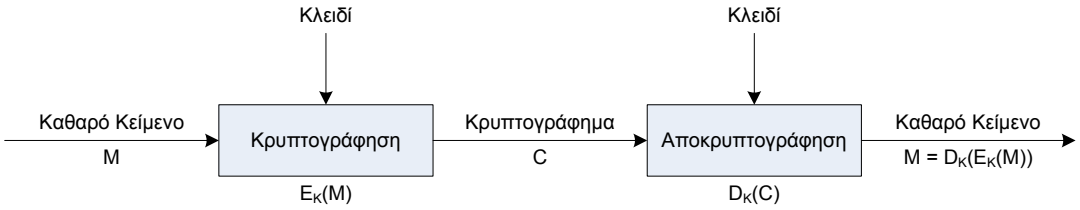
[4] Rogue: Μονήρες (ή αδέσποτο σε ελεύθερη μετάφραση).
[5] Gartner Group, Αύγουστος 2001.

Με όρους κρυπτογραφίας, το αρχικό προς αποστολή μήνυμα λέγεται *καθαρό κείμενο M* (plaintext) και η διαδικασία της μετατροπής του σε κάτι μη αναγνωρίσιμο *κρυπτογράφηση E(M)* (encryption). Το αποτέλεσμα της κρυπτογράφησης λέγεται *κρυπτογράφημα C* (ciphertext). Η διαδικασία της ανάκτησης του καθαρού κειμένου από το κρυπτογράφημα λέγεται *αποκρυπτογράφηση D(C)* (decryption).

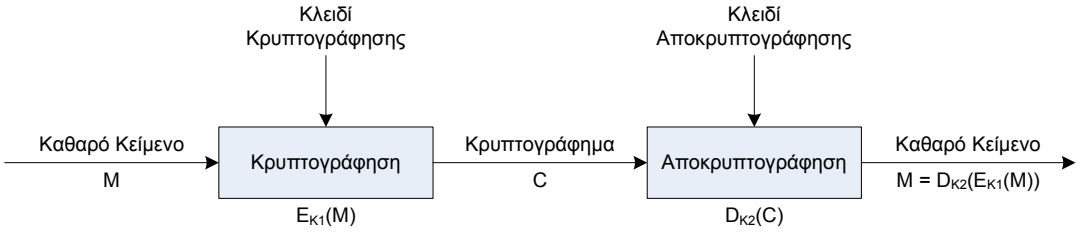


Σχήμα 2. 2

Ο αλγόριθμος (cipher) της κρυπτογράφησης είναι η μαθηματική συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση.
Εάν η ασφάλεια που προσφέρει ένας αλγόριθμος βασίζεται στο γεγονός ότι ο τρόπος λειτουργίας του είναι μυστικός, τότε ο αλγόριθμος λέγεται *περιορισμένος* (restricted). Οι περιορισμένοι αλγόριθμοι έχουν αποδειχθεί επισφαλείς και η λειτουργία τους είναι αδύνατο να κρατηθεί μυστική για πολύ καιρό (περίπτωση του RC4).
Το γεγονός ότι η συνάρτηση κρυπτογράφησης είναι γνωστή στην επιστημονική κοινότητα παρέχει αρκετά πλεονεκτήματα. Το βασικό πλεονέκτημα είναι ο ενδελεχής έλεγχος που μπορεί να γίνει ώστε να βρεθούν πιθανά κενά στην λειτουργία των αλγόριθμων ή του πλαισίου λειτουργίας τους. Επίσης, οι υλοποιήσεις που προκύπτουν είναι βασισμένες σε κάποιο πρότυπο και είναι συμβατές μεταξύ τους. Τέλος, η προσέγγιση που προκύπτει από ένα ανοιχτό αλγόριθμο είναι ότι ο αλγόριθμος μπορεί να σπάσει αλλά το χρονικό διάστημα που απαιτείται είναι απαγορευτικό, πράγμα που είναι ασφαλέστερο από οποιοδήποτε βιομηχανικό μυστικό.
Οι περισσότεροι αλγόριθμοι είναι πλέον ανοιχτοί και η προστασία που προσφέρουν βασίζεται στην πολυπλοκότητά τους και στην μυστικότητα του *κλειδιού K* (key).
Ανάλογα με το αν το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση προκύπτει από, ή είναι το ίδιο με, το κλειδί της κρυπτογράφησης ή όχι, οι αλγόριθμοι κρυπτογράφησης χωρίζονται σε *συμμετρικούς* και *ασύμμετρους*. Στην περίπτωση της ασφάλειας των ασυρμάτων δικτύων χρησιμοποιούνται μόνο συμμετρικοί αλγόριθμοι κρυπτογράφησης.



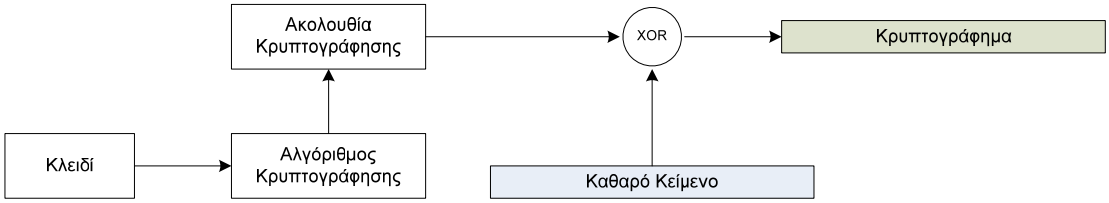
Α. Συμμετρικός Αλγόριθμος



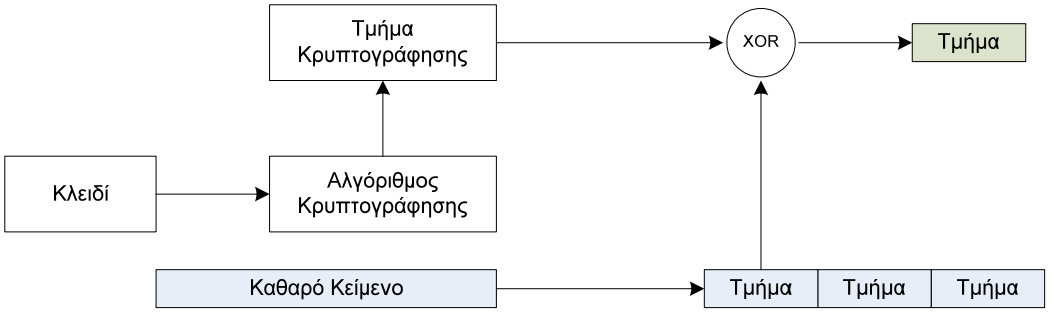
Β. Ασύμμετρος Αλγόριθμος

Σχήμα 2. 3

Οι συμμετρικοί αλγόριθμοι κρυπτογράφησης χωρίζονται σε δύο κύριες κατηγορίες. Οι αλγόριθμοι που ενεργούν σε ένα bit του μηνύματος κάθε φορά ανεξάρτητα από το μήκος της ακολουθίας λέγονται *αλγόριθμοι ροής* (stream ciphers). Από την άλλη μεριά, οι *τμηματικοί αλγόριθμοι* (block ciphers) ενεργούν στα δεδομένα αφού αυτά έχουν κατακερματιστεί σε τμήματα σταθερού μήκους.



Α. Αλγόριθμος Ροής



Β. Τμηματικός Αλγόριθμος

Σχήμα 2. 4

Όπως φαίνεται και από τα παραπάνω σχήματα, ο κάθε αλγόριθμος κρυπτογράφησης παράγει, ανάλογα με το κλειδί, μια ακολουθία κρυπτογράφησης (key stream). Ανάλογα με τον τύπο του συμμετρικού αλγόριθμου το key stream είναι σταθερού μήκους ή παράγεται μαζί με την

ροή των δεδομένων. Το κρυπτογράφημα προκύπτει από την μίξη (με XOR) του key stream και του καθαρού κειμένου.

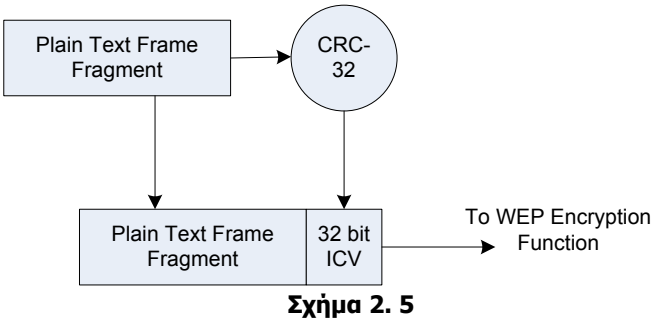
2.6 Wired Equivalent Privacy

Για τα πρώτα πέντε χρόνια της ύπαρξης των ασυρμάτων δικτύων 802.11 από το πρότυπο είχε οριστεί μόνο ένας τρόπος ασφάλειας και αυτός δεν ήταν υποχρεωτικός στις υλοποιήσεις. Αν κάποιος αναλογιστεί ότι αρχικά το πρότυπο στόχευε σε υλοποιήσεις πολύ χαμηλών δυνατοτήτων, προσανατολισμένες σε εφαρμογές όπως ασύρματα barcode scanners, η μη ύπαρξη απόλυτης προστασίας ήταν κάτι ανεκτό. Μόνο μετά την ευρεία αποδοχή του 802.11b άρχισε η ασφάλεια να απασχολεί.
Σύμφωνα με το IEEE, το WEP υιοθετήθηκε από την επιτροπή 802.11 για τους παρακάτω λόγους:

- Είναι *αρκετά* ασφαλές. Βασίζεται στον αλγόριθμο κρυπτογράφησης RC4 που χρησιμοποιείται ευρέως σε software εφαρμογές με επιτυχία και κατά κόρων σε εφαρμογές ηλεκτρονικού εμπορίου.
- Είναι αυτό-συγχρονιζόμενος. Αυτή η ιδιότητα είναι πολύ χρήσιμη σε ασύρματες εφαρμογές όπου ο ρυθμός απώλειας δεδομένων μπορεί να είναι μεγάλος.
- Είναι αποδοτικός και μπορεί να υλοποιηθεί πολύ εύκολα σε υλικό ή λογισμικό. Επίσης, εισάγει σχετικά μικρή καθυστέρηση.
- Χρησιμοποιεί κλειδί μήκους 40bit. Η κυβέρνηση των ΗΠΑ απαγόρευε το 1999 την εξαγωγή προϊόντων που χρησιμοποιούσαν κρυπτογράφηση με μήκους κλειδιού μεγαλύτερο των 40bit.

2.6.1 Ακεραιότητα Δεδομένων

Όπως φαίνεται και στο σχήμα χ.χ, η εμπιστευτικότητα και η ακεραιότητα των δεδομένων προστατεύονται με τον ίδιο μηχανισμό στο WEP. Πριν την κρυπτογράφηση το frame τεμαχίζεται σε μικρότερα τμήματα. Στη συνέχεια, με την χρήση του αλγόριθμου ελέγχου ακεραιότητας δεδομένων Cyclic Redundancy Check (CRC-32) υπολογίζεται ένα hash των 32bit που ονομάζεται Integrity Check Value (ICV) και προσκολλάτε στην συνέχεια του τμήματος του αρχικού frame (σχ. 2.5).



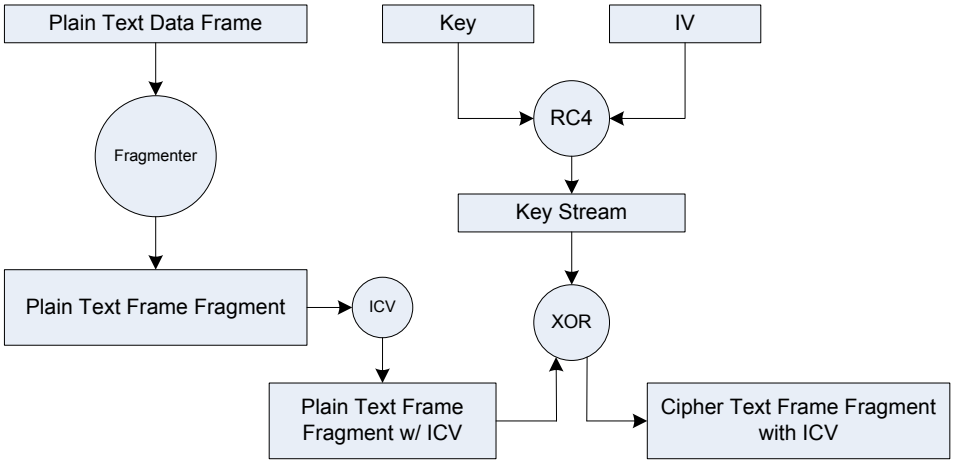
Σχήμα 2. 5

Για την υλοποίηση του CRC-32 χρησιμοποιείται καταχωρητής ολίσθησης γραμμικής ανατροφοδότησης (LFSR) με χαρακτηριστικό πολυώνυμο:

$$G(X) = X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$$

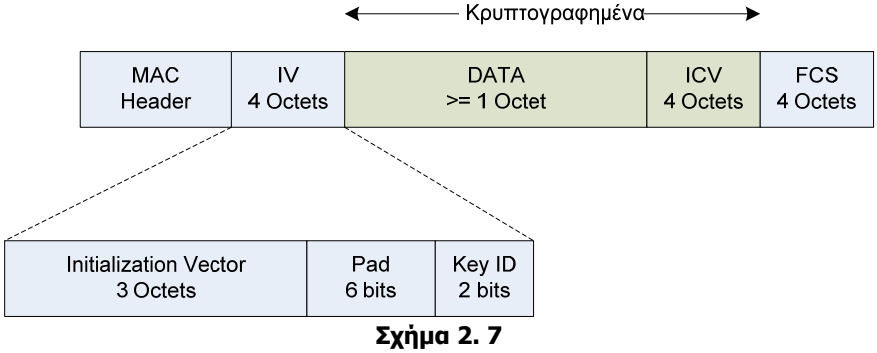
2.6.2 Πλαισίωση και Κρυπτογράφηση

Για την αλλαγή της ακολουθίας που αναμιγνύεται με τα αρχικά δεδομένα (key stream) για να μας δώσει το κρυπτογράφημα ανά frame, όπως περιγράφθηκε παραπάνω, επιλέγεται τυχαία ένα Initialization Vector (IV) που στο WEP είναι 24bit. Το IV και το κοινό κλειδί εισάγονται στον RC4 για την παραγωγή του key stream.



Σχήμα 2. 6

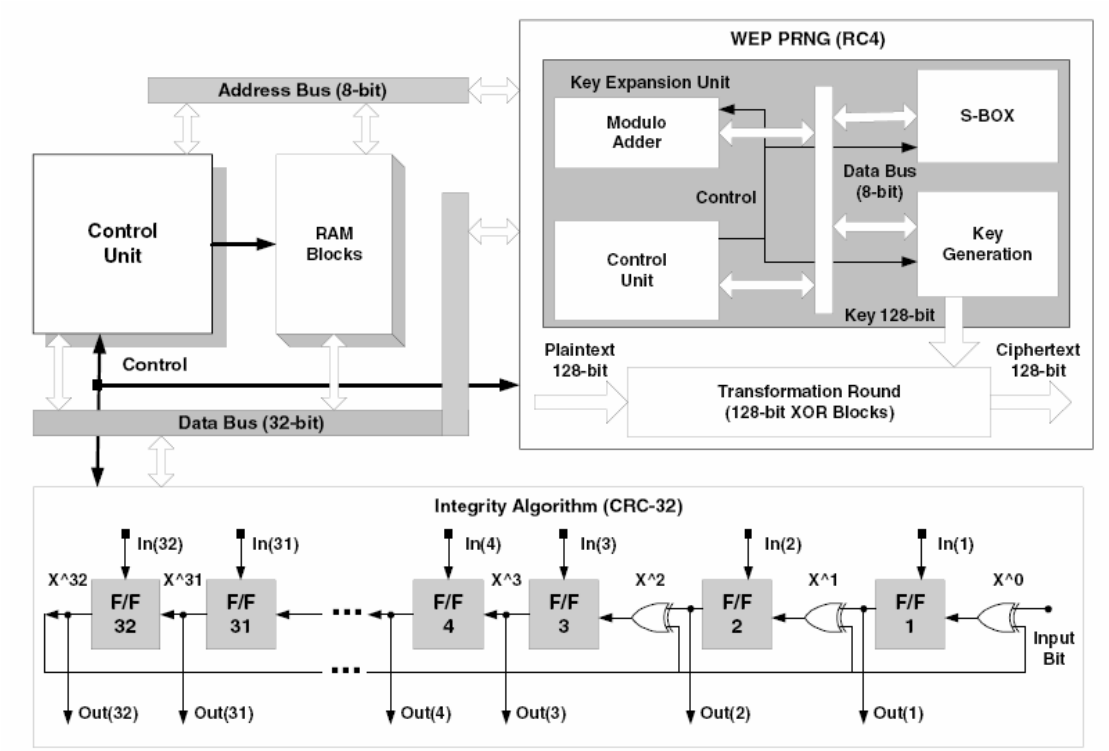
Στην συνέχεια, για την παραγωγή της τελικής κρυπτογραφημένης ακολουθίας γίνεται XOR μεταξύ του τμήματος του frame συν το ICV trailer με το key stream. Το τελικό frame που φεύγει, τελικά, από τον πομπό αποτελείται από το αποτέλεσμα της XOR με την προσθήκη της επικεφαλίδας IV (σχήμα 2.6).



Σχήμα 2. 7

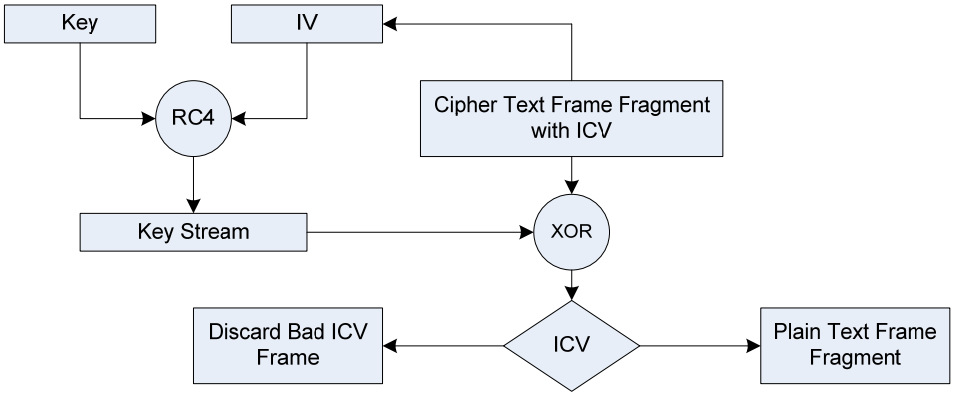
Η επικεφαλίδα IV περιέχει τις απαραίτητες πληροφορίες για τον δέκτη (και όχι μόνο) για την αποκρυπτογράφηση. Τα πρώτα 3 byte είναι το ίδιο το τυχαία επιλεγμένο Initialization Vector. Τα επόμενα 6 bits είναι pad, δηλαδή μηδενικά απλά και μόνο για να μεγαλώσει το μήκος μιας ακολουθίας στο επιθυμητό. Τα

τελευταία δύο bit είναι το αναγνωριστικό του κοινό κλειδιού (key ID). Το key ID είναι απαραίτητο γιατί σε κάθε συσκευή που συμμετέχει στο BSS, προβλέπεται να έχουν καθοριστεί μέχρι τέσσερα διαφορετικά κλειδιά.



Σχήμα 2. 8

Για την αποκρυπτογράφηση στο δέκτη ακολουθείται η αντίστροφη διαδικασία. Από την κεφαλίδα του frame, εξάγονται το IV και το key ID. Από το κοινό κλειδί και το IV υπολογίζεται το key stream που έχει κρυπτογραφήσει τα δεδομένα και γίνεται XOR με κρυπτογράφημα. Το αποτέλεσμα είναι το αρχικό τμήμα των δεδομένων με το ICV που υπολογίστηκε στον αποστολέα. Το ICV trailer αφαιρείται και υπολογίζεται το ξανά το ICV, έστω ICV', αυτή την φορά στον δέκτη. Αν ICV = ICV' τότε τα αρχικά δεδομένα δεν έχουν υποστεί αλλοίωση και η επεξεργασία τους μπορεί να συνεχιστεί. Σε άλλη περίπτωση, το frame απορρίπτεται.



Σχήμα 2. 9

Τέλος να επισημανθεί ότι το πρότυπο προβλέπει κοινό κλειδί μήκους 40bit και μόνο. WEP με κλειδί 104bit (ή WEP2 όπως αναφέρεται πολλές φορές) υπάρχει μόνο ως υλοποίηση εταιριών και η λειτουργικότητα μεταξύ συσκευών διαφορετικών κατασκευαστών δεν είναι εγγυημένη. Επίσης, αναφορές σε κλειδιά μήκους 64bit και 128bit υπονοούν τα παραπάνω συν τα 24bit του IV.

2.6.3 Αδυναμίες του WEP

Όπως αναφέρθηκε κατά την περιγραφή των αλγόριθμων κρυπτογράφησης, όλοι οι stream ciphers έχουν μία ιδιότητα που καθιστά την χρήση του ίδιου κλειδιού περισσότερο από μια φορά επικίνδυνη. Έστω, ένας συμμετρικός ακολουθιακός αλγόριθμος κρυπτογράφησης παράγει το key stream: $K_1,K_2,K_3\ldots K_n$. Ο αποστολέας θα χρησιμοποιήσει την ακολουθία K_j για να κρυπτογραφήσει την ακολουθία των δεδομένων $P_1,P_2,P_3\ldots P_n$, με αποτέλεσμα την ακολουθία $C_1,C_2,C_3\ldots C_n$, μέσω XOR.

$$C_j = P_j \oplus K_j, \quad j = 1,2,3...n \qquad (1)$$

Ο λήπτης του κρυπτογραφήματος ανακτά τα αρχικά δεδομένα με την αντίστροφη διαδικασία. Δηλαδή, με XOR μεταξύ της κρυπτογραφημένης ακολουθίας και του key stream.

$$P_j = C_j \oplus K_j, \qquad j = 1,2,3...n \qquad (2)$$

De facto, κάποιος εχθρικά διακείμενος μπορεί να μάθει τον αλγόριθμο κρυπτογράφησης, όπως επίσης και να υποκλέψει το κρυπτογράφημα C_j. Αν μπορέσει να μάθει ή να μαντέψει κάποια από τις αρχικές τιμές P_j, τότε μπορεί να μάθει και όλες τις αντίστοιχες αρχικές τιμές P_j' που έχουν κρυπτογραφηθεί με το ίδιο κλειδί. Πρώτα, υπολογίζει την τιμή του αντίστοιχου bit του key stream:

$$K_j = C_j \oplus P_j$$

Στην συνέχεια με χρήση της σχέσης (2) υπολογίζει την νέα τιμή P_j':

$$P'_j = C'_J \oplus K_j$$

Εάν, ο αριθμός των γνωστών αρχικών δεδομένων είναι σημαντικός, κάποιος θα μπορούσε να εξάγει το κοινό κλειδί, οπότε κάθε προσπάθεια κρυπτογράφησης θα ήταν άχρηστη.

Πρέπει να επισημανθεί ότι η γνώση των αρχικών μη κρυπτογραφημένων δεδομένων ή έστω μέρος αυτών δεν απαιτεί υποχρεωτικά και την υποκλοπή τους που θα ήταν αρκετά δύσκολη. Η δομή και τα περιεχόμενα κάποιων διαχειριστικών, κυρίως, πακέτων είναι γνωστά. Για παράδειγμα, υπάρχει πιθανότητα να αποκαλυφθεί το κλειδί μόνο από πακέτα DHCP.

Επίσης, για δύο ακολουθίες που έχουν κρυπτογραφηθεί με το ίδιο κλειδί ισχύει

$$C_1 \oplus C_2 = P_1 \oplus P_2$$

Οπότε υπάρχει τρόπος σύγκρισης τον δεδομένων για την ανεύρεση μοτίβων, πχ. το γράμμα e εμφανίζεται συχνότερα σε αγγλικά κείμενα, δεύτερο είναι το t κτλ.

Ο σχεδιασμός του WEP αντιμετωπίζει αυτό το πρόβλημα με την χρήση του IV. Όπως έχει αναφερθεί, το IV του WEP έχει μήκος 24bit και συνδυάζεται με το κοινό κλειδί για την παραγωγή 2^{24} διαφορετικών κλειδιών (περίπου 16,5 εκατομμύρια πιθανά κλειδιά).
Το όλο σχήμα πάσχει από ένα βασικό πρόβλημα: Για να τηρείται η μη επαναχρησιμοποίηση των κλειδιών, όλοι οι χρήστες ενός ασύρματου δικτύου θα έπρεπε να αλλάζουν το κοινό κλειδί τους το πολύ μετά από μια ώρα χρήσης του σε ένα τυπικό περιβάλλον γραφείου. Σε περιβάλλον ESS με περισσότερα AP τα κλειδιά εξαντλούνται με ρυθμό αντιστρόφως ανάλογο του αριθμού των AP.
Το πρόβλημα γίνεται ακόμα χειρότερο γιατί δεν υπάρχει μηχανισμός που να αποτρέπει ένα χρήστη από το να χρησιμοποιεί ένα κλειδί που χρησιμοποιείται ήδη από κάποιον άλλο χρήστη.
Αυτό που γίνεται είναι η τυχαία επιλογή IV, αλλά και αυτό δεν αποτελεί λύση: Έστω ένα σύνολο αποτελείται τα n στοιχεία και τα στοιχεία επιλέγονται τυχαία, ένα κάθε φορά, με επανατοποθέτηση και k ο αριθμός των επαναλήψεων του πειράματος τύχης. Η πιθανότητα να έχει επιλεχθεί το ίδιο στοιχείο είναι:

$$p_2 = \frac{1}{n}, \quad k = 2$$
$$p_k = p_{k-1} + \frac{(k-1)\cdot(1-p_{k-1})}{n}, \quad k \geq 3$$

Στην περίπτωσή μας, $n = 2^{24} = 16.777.216$ στοιχεία. Οι πιθανότητες επαναχρησιμοποίησης ενός κλειδιού, σε συνάρτηση με τα απεσταλμένα frames, φαίνονται στον παρακάτω πίνακα:

frames	p (%)
19	0,001
59	0,01
184	0,1
582	1
1.881	10
4.823	50
12.430	99

Αν υπολογίσουμε, χονδρικά, ότι για την αποστολή 1MB δεδομένων χρειάζονται περίπου 500 frames, τότε σε ένα BSS 802.11g με κανονική κίνηση

θα χρειαστεί λιγότερο από ένα δευτερόλεπτο για σχεδόν βέβαιη επανάληψη του κλειδιού. Δυστυχώς, η επιμήκυνση του κοινού στατικού κλειδιού στα 104bit ή και παραπάνω δεν έχει καμία επίδραση στο πλήθος των διαθέσιμων κλειδιών.

Τον Αύγουστο του 2001 οι Fluhrer, Mantin και Shamir δημοσίευσαν μια έρευνα με τίτλο "Weaknesses in the Key Scheduling Algorithm of RC4". Στην δημοσίευση περιγράφεται, μεταξύ άλλων, μια θεωρητική επίθεση στο WEP. Η επίθεση βασίζεται στον τρόπο που ο RC4 παράγει το key stream. Το μόνο που προϋποθέτει για την πραγματοποίηση της επίθεσης είναι η γνώση του πρώτου byte του κρυπτογραφήματος. Δυστυχώς, αυτό είναι γνωστό σε όλους: το 802.11 χρησιμοποιεί το 802.2 ως Logical Link Layer οπότε το πρώτο byte είναι πάντα 0xAA (SNAP header). Όπως περιγράφθηκε παραπάνω, είναι εύκολο να βρεθεί το πρώτο byte του key stream ως το αποτέλεσμα του XOR μεταξύ του 0xAA και του πρώτου κρυπτογραφημένου byte.
Η επίθεση επικεντρώνεται σε μια κλάση αδύναμων IV της μορφής (B+3):FF:N. Κάθε διαφορετικό IV χρησιμοποιείται για την αποκάλυψη διαφορετικού τμήματος του κοινού κλειδιού. Το στάνταρ WEP κλειδί έχει μήκος 40bit ή 5 byte αριθμημένα από 0 έως 4 (τιμές του B). Η γνώση του N είναι απαραίτητη αλλά μπορεί να έχει οποιαδήποτε τιμή από 0 έως 0xFF. Για την αποκάλυψη του πρώτου byte του κοινού κλειδιού (B=0), τα αδύναμα IV έχουν τη μορφή 3:FF:N, για το δεύτερο 4:FF:N και ούτω καθεξής. Όπως μπορεί πολύ εύκολα να υπολογιστεί, το πλήθος των αδύναμων IV στο 40bit WEP είναι 5x1x256=1.280.
Οι Fluhrer, Mantin και Shamir υπολόγισαν ότι αρκούν 60 αδύναμα IV για την αποκάλυψη ενός byte του κοινού κλειδιού με αρκετά μεγάλη πιθανότητα επιτυχίας. Αυτό σημάνει ότι πρέπει να υποκλαπούν 1.000.000 έως 4.000.000 frames για μια επιτυχημένη επίθεση.
Το ενδιαφέρον με αυτή την επίθεση είναι ότι το μέγεθος της αδυναμίας είναι ανάλογη του μήκους του αρχικού κοινού κλειδιού. Συνήθως, δυσκολία αποκρυπτογράφησης αυξάνεται εκθετικά με το μήκος του κλειδιού. Σ' αυτή την περίπτωση λειτουργεί γραμμικά, οπότε διπλασιασμός του κλειδιού σημαίνει διπλασιασμό των frames που πρέπει κάποιος να συλλέξει, δηλαδή διπλασιασμός του χρόνου μέχρι την αποκρυπτογράφηση.

Μήκος Κλειδιού (bits)	Τιμές του B (B+3):FF:N	Πλήθος Αδύναμων IV	Ποσοστό Διαθέσιμων IV
40	0≤B≤5	1.280	0,008%
104	0≤B≤13	3.328	0,02%
128	0≤B≤16	4.096	0,024%
256	0≤B≤32	8.192	0,048%

Η επίθεση των Fluhrer, Mantin και Shamir εκτός από το θεωρητικό ενδιαφέρον υπήρξε και η αρχή του τέλους του WEP. Τον ίδιο μήνα με την δημοσίευση, οι Stubblefield/Ioannidis/Rubin υλοποίησαν την επίθεση εργαστηριακά αλλά σε πραγματικό δίκτυο και σε όλες τις περιπτώσεις το κοινό κλειδί αποκαλύφθηκε. Αργότερα τον ίδιο Αύγουστο, κυκλοφόρησε το AirSnort

των Bruestle και Hegerle, ένα λογισμικό ανοιχτού κώδικα ανάκτησης του κοινού κλειδιού του WEP.

2.7 Temporal Key Integrity Protocol

Μετά την έκδοση του AirSnort το WEP δεν είχε λόγο ύπαρξης αφού σχεδόν όποιος μπορούσε να χρησιμοποιήσει ηλεκτρονικό υπολογιστή μπορούσε να το σπάσει. Το IEEE σύστησε το TGi, αλλά η δημιουργία και η έκδοση ενός προτύπου είναι χρονοβόρα διαδικασία. Όπως συμβαίνει σε τέτοιες περιπτώσεις, οι κατασκευαστές άρχισαν να παρουσιάζουν κάποιες λύσεις που στερούνταν δια-λειτουργικότητα και κόστιζαν αρκετά. Οι περισσότερες από αυτές στηρίχτηκαν σε κάποιο τύπο EAP ή σε άλλες υπάρχουσες τεχνολογίες όπως τα virtual private networks (VPN), demilitarized zones κτλ.
Το WEP εκτός από τα κενά στην ασφάλεια, άφησε μια μεγάλη εγκατεστημένη βάση μηχανημάτων βασισμένα σε φτηνούς επεξεργαστές χαμηλής ισχύος. Οι επεξεργαστές που χρησιμοποιήθηκαν ήταν, συνήθως, οι i486, ARM7 και PowerPC χρονισμένοι στα 25 ή 40MHz. Η διαχείριση της κίνησης ενός δικτύου καταναλώνει έως και το 90% της επεξεργαστικής ισχύος των παραπάνω CPU. Το υπόλοιπο 10% αφήνει διαθέσιμες περίπου 2 εκατομμύρια εντολές ανά δευτερόλεπτο. Μια υλοποίηση του 3DES (το πρότυπο στη θέση του AES πριν το 2004) σε C++ έχει ένα μέσο κόστος 180 εντολές / byte δεδομένων. Ένας χρήστης 802.11g μπορεί να έχει ένα throughput των 30,5Mbps, δηλαδή περίπου 3,8 εκατομμύρια bytes το δευτερόλεπτο. Η επεξεργαστική ισχύς που απαιτείται για την κρυπτογράφησή τους με χρήση του 3DES είναι 180x3.800.000 = 684.000.000 εντολές το δευτερόλεπτο. Η διαφορά είναι τεράστια με τις μόλις 2.000.000 διαθέσιμες.
Ένα ακόμα πρόβλημα, με την αλλαγή του WEP, είναι ότι στα περισσότερα AP την κρυπτο/αποκρυπτογράφηση την αναλαμβάνουν custom ολοκληρωμένα, κυρίως FPGA (σχ. 2.8) για να μην απασχολείται η CPU. Η αντικατάσταση όλου του εξοπλισμού είναι οικονομικά ασύμφορη, οπότε το WEP παραμένει. Την λύση, αρχικά, την έδωσε η WiFi Alliance με την έκδοση του WiFi Protected Access (WPA, 2003), ένα συνδυασμό του TKIP με το 802.1x. Αργότερα, ο ίδιος συνδυασμός υιοθετήθηκε και από το TGi ως μέρος του Robust Security Network (RSN).

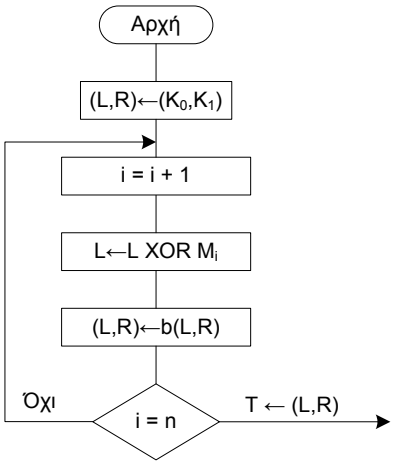
Το TKIP είναι μια συλλογή αλγόριθμων *γύρω* από το WEP που σκοπό έχουν να μεγιστοποιήσουν την ασφάλεια δεδομένων των προβλημάτων του. Ο σχεδιασμός έγινε με γνώμονα τους περιορισμούς του εξοπλισμού και την μικρότερη δυνατή υποβάθμιση της απόδοσης των δικτύων. Το TKIP προσθέτει τέσσερα νέα στοιχεία στο WEP:

- Ένα κρυπτογραφικό Message Integrity Code (MIC) με την ονομασία Michael.
- Ένα κανόνα διαδοχής των IV.
- Μια συνάρτηση ανάμειξης για την παραγωγή μοναδικών κλειδιών ανά frame.

- Ένα μηχανισμό αλλαγής του κοινού κλειδιού που γίνεται πλέον προσωρινό.

2.7.1 Michael

Κάθε MIC έχει τρία στοιχεία: ένα κρυφό κλειδί πιστοποίησης K κοινό μόνο μεταξύ αποστολέα και παραλήπτη, ένα αλγόριθμο παραγωγής του MIC και κάποια διαδικασία επαλήθευσης. Ο αλγόριθμος έχει ως εισόδους το κλειδί K και το μήνυμα M και στην έξοδό του παράγει την ακολουθία (tag) T. Ο αποστολέας στέλνει τα M και T. Για τον έλεγχο της ακεραιότητας των δεδομένων, ο παραλήπτης ξανα-υπολογίζει το T και αν T=T' τότε τα δεδομένα θεωρούνται αυθεντικά.
Το κλειδί του Michael έχει μήκος 64bit χωρισμένα σε δύο λέξεις των 32bit (K_0,K_1). Στην αρχή τα δεδομένα συμπληρώνονται με την τιμή 0x5A και αρκετά μηδενικά ώστε το μήκος τους να είναι πολλαπλάσιο του 32 και στην συνέχεια χωρίζονται σε λέξεις των 32bit M_1 M_2 … M_n. Τέλος, υπολογίζεται το T:



Σχήμα 2. 10

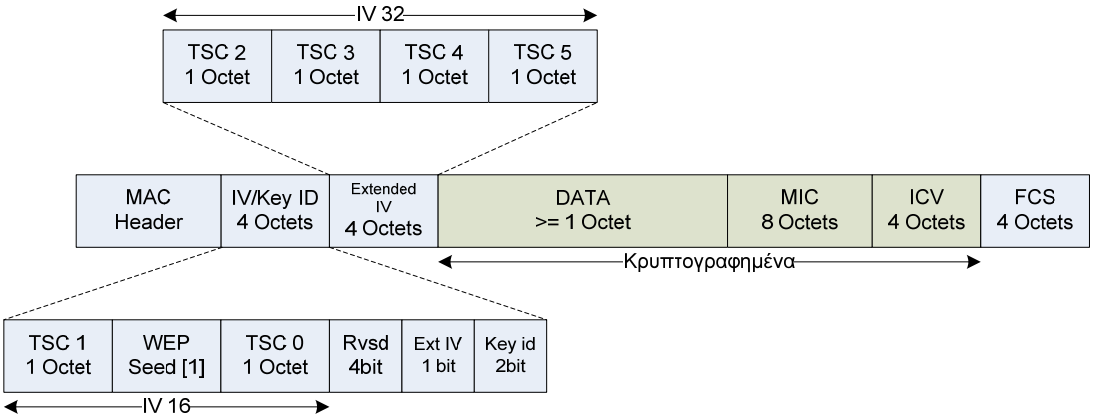
Όπου τα L και R είναι 32bit μεταβλητές και το b είναι μια απλή διαδικασία από διαδοχικές αντιμεταθέσεις, προσθέσεις και περιστροφές μεταξύ των bits των μεταβλητών.
Παρόλο που ο Michael αποτελείται από απλές πράξεις έχει ένα κόστος 3,5 εντολών ανά byte σε ARM7 και 5,5 σε i486. Αυτό σημαίνει μια επιβάρυνση από 3,1 έως 4,8 εκατομμύρια εντολές το δευτερόλεπτο σε δίκτυα 802.11b και σχεδόν το πενταπλάσιο σε 802.11g. Λαμβάνοντας υπ' όψιν τα σχεδόν 2 εκατομμύρια διαθέσιμες, θα πρέπει να περιμένουμε επιβάρυνση στην απόδοση.

2.7.2 Επιλογή και χρήση IV

Τα περισσότερα προβλήματα και οι αδυναμίες του WEP συγκεντρώνονται γύρω από την επιλογή και την χρήση του IV. Στο TKIP εισάγονται οι παρακάτω διορθώσεις:

- Το μήκος του IV αυξάνεται από 24 στα 48bit.

- Το IV παίζει πλέον και τον ρόλο του αναγνωριστικού του πακέτου (Packet Number, PN) για την αποφυγή επιθέσεων επανάληψης.
- Αποκλείονται τα αδύναμα IV της επίθεσης των Flurer-Martin-Shamir.



Σχήμα 2. 11

Όπως φαίνεται και στο σχήμα χ.χ, για την αύξηση του μήκους του IV προστέθηκαν 32 επιπλέον bit μεταξύ της αρχικής κεφαλίδας του πλαισίου και των κρυπτογραφημένων δεδομένων. Μαζί τα 24 αρχικά bit, το συνολικό μήκος του IV είναι 56bit. Για να αποκλειστούν τα αδύναμα IV της κλάσης B+3:FF:N, το ένα byte απορρίπτεται και έτσι προκύπτει το τελικό μήκος των 48bit.
Μ' αυτό τον τρόπο, το μεγάλο πρόβλημα της επαναχρησιμοποίησης των IV λύνεται. Με τα 24bit του IV, τα διαθέσιμα κλειδιά περιορίζονταν στα 16.777.216 και ο χρόνος μέχρι την εξάντλησή τους ήταν μερικά λεπτά. Με το IV των 48bit και ένα μέσο ρυθμό μετάδοσης των 3000 πλαισίων το δευτερόλεπτο, ο χρόνος μέχρι την εξάντληση όλων των πιθανών κλειδιών υπολογίζεται σε πάνω από 250 χρόνια.
Ο τρόπος αποφυγής των επιθέσεων επανάληψης είναι απλός: Σε κάθε πλαίσιο που μεταδίδεται προστίθεται ένας σειριακός αριθμός αναγνώρισης. Για κάθε επόμενο πλαίσιο ο αριθμός αυξάνεται κατά ένα. Ο παραλήπτης μπορεί να αναγνωρίσει μια επίθεση επανάληψης αν ο σειριακός αριθμός είναι μικρότερος από αυτόν του τελευταίου πακέτου. Το TKIP διορθώνει την παράληψη ενός τέτοιου αριθμού στο WEP με το TKIP Sequence Counter (TSC), το οποίο ταυτίζεται με το IV.

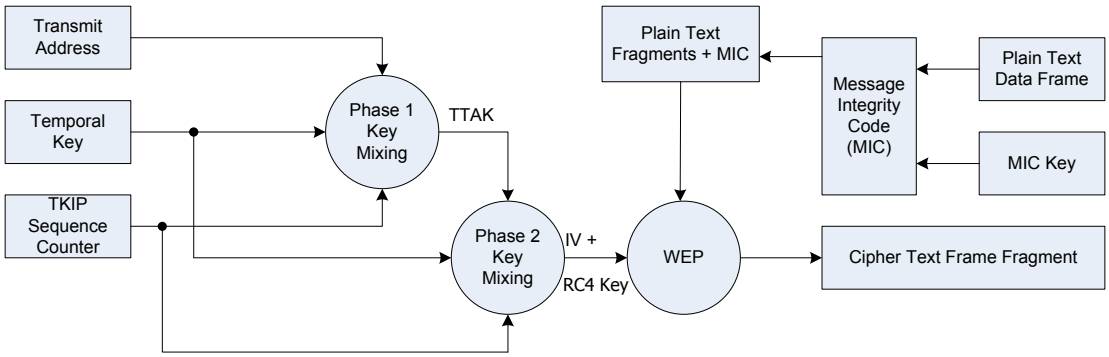
2.7.3 Αλγόριθμος Ανάμειξης Κλειδιών

Η πλειοψηφία των επιθέσεων κατά του WEP προϋποθέτουν την συλλογή αρκετών πακέτων (packet sniffing) κρυπτογραφημένων με το ίδιο κλειδί. Ο στόχος του μηχανισμού ανάμειξης κλειδιών είναι το κάθε πακέτο πληροφορίας να κρυπτογραφείται με διαφορετικό, μοναδικό κλειδί.
Στην παραγωγή του μοναδικού κλειδιού συμμετέχουν η διεύθυνση MAC του αποστολέα (transmit address,TA), το TSC και το προσωρινό κλειδί που είναι κοινό μεταξύ αποστολέα και παραλήπτη. Η ανάμειξη γίνεται σε δύο φάσεις.
Στην πρώτη φάση γίνεται ανάμειξη της TA, των 32 πιο σημαντικών bit του TSC και των 80 πιο σημαντικών bit του προσωρινού κλειδιού. Για να

αποφευχθεί επιβάρυνση του επεξεργαστή, η ανάμειξη περιλαμβάνει μόνο απλές πράξεις όπως πρόσθεση, AND και XOR. Το αποτέλεσμα της πρώτης φάσης είναι μια ακολουθία 80bit που στο πρότυπο ονομάζεται TKIP mixed Transmit Address and Key, TTAK.
Στην δεύτερη φάση του αλγόριθμου ανάμειξης κλειδιών συμμετέχουν το TTAK, το πλήρες προσωρινό κλειδί και το TSC. Και στη δεύτερη φάση, η ανάμειξη γίνεται με πράξεις μικρού επεξεργαστικού κόστους. Το αποτέλεσμα είναι το κλειδί που χρησιμοποιείται από το WEP, το λεγόμενο WEP seed, με μήκος 128bit.

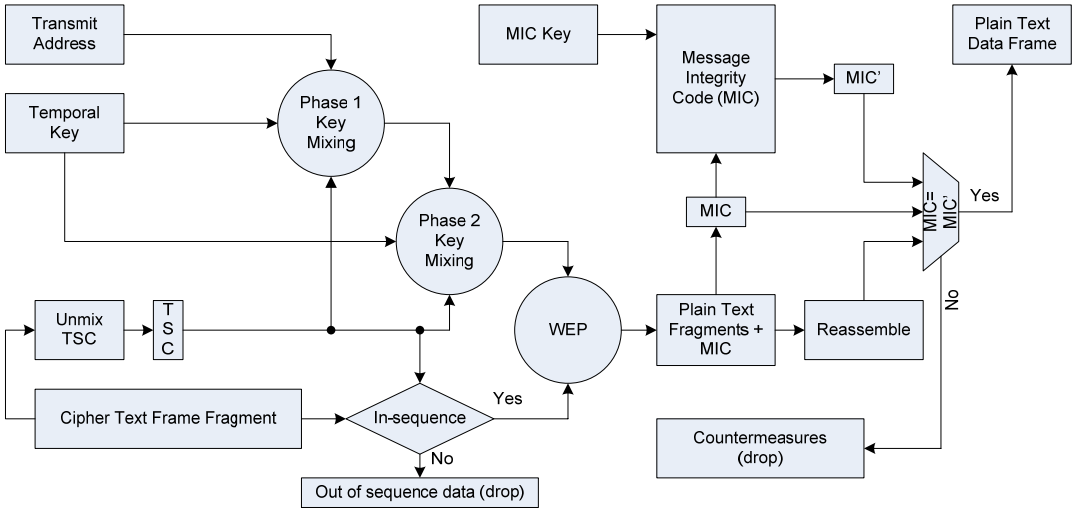
2.7.4 Δημιουργία Πλαισίων TKIP

Το πρώτο βήμα στην δημιουργία του κρυπτογραφημένου πλαισίου αποστολής είναι ο υπολογισμός του κώδικα ακεραιότητας δεδομένων MIC. Τα δεδομένα που προστατεύονται από το MIC είναι το μήνυμα και οι διευθύνσεις του αποστολέα και του παραλήπτη. Τα παραπάνω και το κλειδί του MIC είναι οι είσοδοι του Michael. Τα 8 byte του MIC που προκύπτουν, προσκολλούνται στο αρχικό μήνυμα και η ακολουθία που προκύπτει είναι τα τελικά δεδομένα που θα κρυπτογραφηθούν από το WEP.



Σχήμα 2. 12

Στην συνέχεια, αν υπάρχει ανάγκη, τα δεδομένα τεμαχίζονται. Ο αποστολέας για κάθε τμήμα αυξάνει το TKIP Sequence Counter και γίνεται η ανάμιξη των κλειδιών για την παραγωγή του WEP seed.
Τέλος, κατά τα γνωστά από το WEP, υπολογίζεται το ICV και γίνεται η κρυπτογράφηση από τον RC4.



Σχήμα 2. 13

Για την ανάκτηση των αρχικών δεδομένων ακολουθείται η διαδικασία του σχήματος 2.13. Αρχικά, ο παραλήπτης υπολογίζει το WEP seed όπως και ο αποστολέας και εάν το πακέτο έχει το TSC που πρέπει. Εάν όχι, το πακέτο απορρίπτεται πριν αποκρυπτογραφηθεί. Στην συνέχεια τα τμήματα αποκρυπτογραφούνται και επανενώνονται στο αρχικό μήνυμα. Τέλος, ο παραλήπτης υπολογίζει το MIC και το συγκρίνει με αυτό του αποστολέα. Εάν το αποτέλεσμα είναι διαφορετικό, υποτίθεται ότι το δίκτυο δέχεται επίθεση. Στην περίπτωση αυτή, έχουν λαμβάνονται κάποια αντίμετρα για την αποτροπή της επίθεσης. Τα αντίμετρα αυτά είναι η απόρριψη του πακέτου και η αποβολή του αποστολέα από το δίκτυο για ένα λεπτό.

2.7.5 Αδυναμίες του TKIP

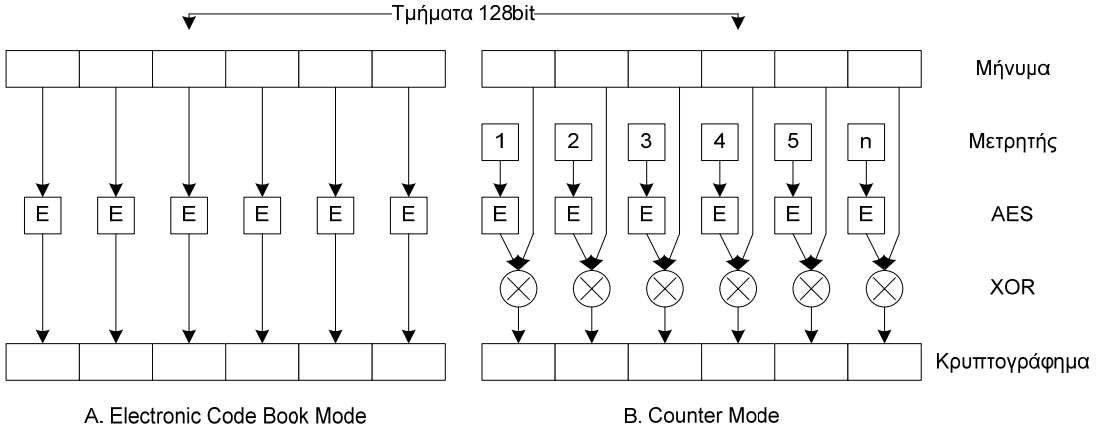
Το μόνο πρόβλημα που έχει αναφερθεί στο TKIP είναι η χρησιμοποίηση των αντίμετρων του Michael για την πραγματοποίηση επίθεσης άρνησης υπηρεσίας. Η επίθεση είναι τόσο δύσκολη που παραμένει θεωρητική.
Γενικά, η μέθοδος που θα πρέπει να χρησιμοποιηθεί είναι όμοια με τις επιθέσεις man-in-the-middle. Αρχικά, ο επιτιθέμενος πρέπει να αναχαιτίσει ένα πακέτο πριν να φτάσει στο AP. Στην συνέχεια, θα πρέπει να μετατρέψει το πακέτο με τέτοιο τρόπο που να έχει ίδιο ICV με το αρχικό και να περάσει τον έλεγχο του WEP, αλλά διαφορετικό MIC. Τέλος, όταν αποσταλεί στο AP η τιμή του TSC του τροποποιημένου πλαισίου θα πρέπει να ίση ή μεγαλύτερη από την τρέχουσα ώστε να μην απορριφτεί στον έλεγχο για επίθεση επανάληψης.
Εάν πραγματοποιηθούν τα παραπάνω, ο χρήστης που έστειλε το αρχικό πλαίσιο θα απορριφτεί από το δίκτυο για ένα λεπτό. Και θα συνεχίζει να μην μπορεί να χρησιμοποιήσει το δίκτυο για όσο διαρκεί η επίθεση. Αυτή η επίθεση μπορεί να είναι απίθανη αλλά όχι αδύνατη.

2.8 Counter Mode with Cipher-Block Chaining Massage Authentication Code Protocol (CCMP)

Όπως έχει περιγραφεί παραπάνω, το TKIP παρέχει επαρκή ασφάλεια στα ασύρματα δίκτυα και έχει ελάχιστες πιθανότητες να παραβιαστεί στο μέλλον. Παρ' όλα αυτά, το TKIP δεν αποτελεί την βασική μέθοδο ασφάλειας του 802.11i αλλά μία εναλλακτική λύση για μηχανήματα που κατασκευάστηκαν πριν την δημοσίευσή του. Το πρωτόκολλο που προτείνεται από το IEEE και υιοθετήθηκε από την WiFi Alliance ως το Wireless Protected Access 2 (WPA2) είναι το CCMP.
Το CCMP μπορεί να θεωρηθεί, γενικά, ασφαλέστερο του TKIP. Το βασικό του πλεονέκτημα είναι ότι σχεδιάστηκε από την αρχή, χωρίς να κληρονομεί την αποτυχία του WEP. Επιπλέον, βασίζεται σε ένα πολύ ισχυρότερο του RC4 αλγόριθμο κρυπτογράφησης, τον Rijndael. Ο Rijndael είναι το νέο πρότυπο κρυπτογράφησης της κυβέρνησης των ΗΠΑ, στην θέση του DES, και είναι ευρύτερα γνωστός ως το Advanced Encryption Standard (AES). Το γεγονός ότι μηχανήματα που ολοκληρώνουν το AES μπορούν να χρησιμοποιηθούν, χωρίς μετατροπές, από κυβερνητικές υπηρεσίες αποτελεί από μόνο του μεγάλο πλεονέκτημα από τους κατασκευαστές.
Το AES είναι ένας συμμετρικός τμηματικός αλγόριθμος κρυπτογράφησης (block cipher). Τα κρυπτογραφημένα τμήματα έχουν το ίδιο μήκος με τα αρχικά και στην περίπτωση του 802.11i, αυτό έχει οριστεί στα 128 bit. Τα δεδομένα σε ένα δίκτυο δεν αποτελούνται από τμήματα σταθερού μήκους, οπότε δημιουργείται η ανάγκη τεμαχισμού τους ανά 128 bit. Επίσης, θα πρέπει να υπάρχει κάποιος τρόπος αναγνώρισης αυτών των τμημάτων κατά την αποκρυπτογράφηση για την επαναφορά του αρχικού μηνύματος. Η μέθοδος της μετατροπής και επαναφοράς των μηνυμάτων σε τμήματα αναφέρεται ως τρόπος λειτουργίας (mode of operation) του block cipher.

2.8.1 Counter Mode

Ο απλούστερος τρόπος λειτουργίας ενός τμηματικού αλγόριθμου κρυπτογράφησης είναι ο Electronic Code Book (σχ. 2.14.Α). Το μεγάλο πρόβλημα με αυτό τον τρόπο είναι ότι η ίδια είσοδος οδηγεί πάντα στο ίδιο κρυπτογράφημα. Όσο ισχυρός και να είναι ο αλγόριθμος κρυπτογράφησης, μια τέτοια υλοποίηση θα οδηγούσε σε παρόμοια προβλήματα με αυτά του WEP.

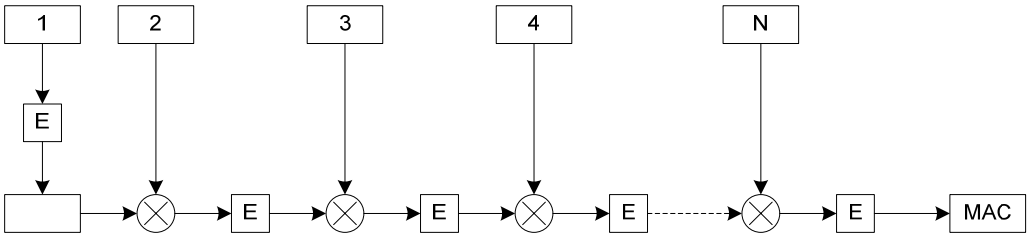


Σχήμα 2. 14

Ο τρόπος που έχει επιλεγεί από IEEE λέγεται Counter Mode (σχ. 2.14.Β). Με αυτό τον τρόπο, το AES δεν χρησιμοποιείται για απ' ευθείας κρυπτογράφηση των τμημάτων των δεδομένων αλλά κρυπτογραφείται η έξοδος ενός μετρητή. Η τελική κρυπτογράφηση των δεδομένων επιτυγχάνεται με XOR μεταξύ των αρχικών τμημάτων και της κρυπτογραφημένης τιμής του μετρητή.
Ο Counter Mode έχει αρκετά πλεονεκτήματα στην ολοκλήρωσή του με τα ασύρματα δίκτυα. Πρώτον, εξαλείφεται το πρόβλημα του ECB. Ακόμα και με ίδια δεδομένα εισόδου, η έξοδος θα είναι διαφορετική αφού η τιμή του μετρητή αλλάζει για κάθε block. Επιπλέον, λύνεται ένα από τα προβλήματα κατά τον τεμαχισμό των δεδομένων. Τα δεδομένα πλέον δεν χρειάζεται να μετατραπούν σε μήκος πολλαπλάσιο των 128 bit, γιατί XOR μεταξύ ακολουθιών διαφορετικού μήκους έχει ως αποτέλεσμα ακολουθία με μήκος το μήκος της μεγαλύτερης. Τέλος, η υλοποίηση του είναι σχετικά απλή γιατί με την ίδια διάταξη επιτυγχάνεται κρυπτογράφηση και αποκρυπτογράφηση. Αν στο παράδειγμα του σχήματος χ.χ.Β, ως είσοδος μπει το κρυπτογράφημα, το αποτέλεσμα της XOR θα είναι το αρχικό μήνυμα.

2.8.2 Cipher-Block Chaining Massage Authentication Code (CBC MAC)

Για την σωστή λειτουργία της κρυπτογράφησης και την ασφάλεια των δεδομένων θα πρέπει να υπάρχει κάποιος τρόπος εξακρίβωσης ότι τα δεδομένα δεν έχουν αλλοιωθεί κατά την εκπομπή. Όπως έχει περιγραφεί παραπάνω, οι μέθοδοι εξακρίβωσης της ακεραιότητας των δεδομένων στο WEP και TKIP ήταν οι CRC-32 και Michael αντίστοιχα. Στην περίπτωση του CCMP η μέθοδος που χρησιμοποιείται είναι ο CBC – MAC.
Η λειτουργία του CBC MAC είναι απλή: Όπως και κατά την κρυπτογράφηση, ο μήνυμα τεμαχίζεται σε τμήματα σταθερού μήκους και στην περίπτωσή μας σε τμήματα των 128 bit. Στην συνέχεια, το πρώτο τμήμα κρυπτογραφείται με το AES. Το αποτέλεσμα της κρυπτογράφησης αναμιγνύεται, με XOR, με το επόμενο τμήμα του καθαρού κειμένου και το αποτέλεσμα κρυπτογραφείται. Το αποτέλεσμα της κρυπτογράφησης αναμιγνύεται με το τρίτο τμήμα του καθαρού κειμένου και ούτω καθεξής (σχ. 2.15).



Σχήμα 2. 15

Το αποτέλεσμα των διαδοχικών μίξεων και κρυπτογραφήσεων είναι μια ακολουθία 128bit που περιέχει πληροφορίες απ' όλα τα τμήματα του καθαρού κειμένου. Η πιθανότητα να έχει αλλοιωθεί το αρχικό μήνυμα και να έχει το ίδιο MAC (ή MIC κατά το IEEE[6]) είναι μια στα $3,4*10^{38}$.

2.8.3 Counter Mode + CBC MAC = CCM

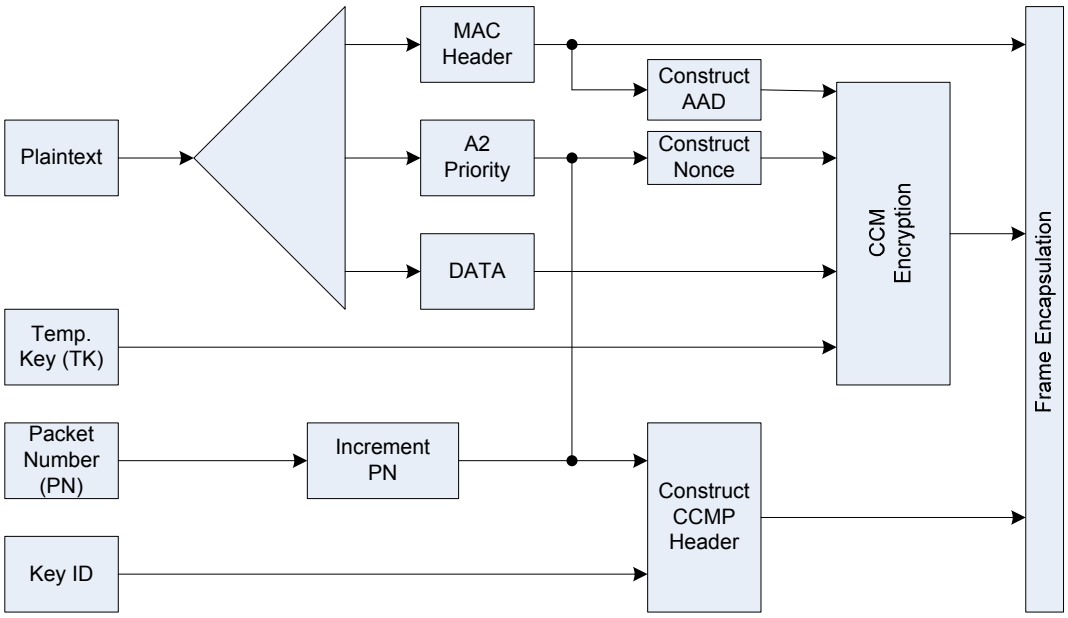
Το CCM είναι ένας ξεχωριστός τρόπος λειτουργίας του AES που αναπτύχθηκε από μέλη του TGi ειδικά για την ασφάλεια των ασυρμάτων δικτύων και συνδυάζει τα πλεονεκτήματα του Counter Mode και του CBC MAC. Ο λόγος που ανάγκασε την ανάπτυξη του CCM είναι ότι τα Counter Mode και CBC είναι ασύμβατα μεταξύ τους και η συνύπαρξή τους προϋποθέτει κάποιες μετατροπές και προσθήκες.
Η βασική προσθήκη έπρεπε να γίνει με σκοπό η κρυπτογράφηση και η ακεραιότητα του μηνύματος θα πρέπει να λειτουργούν με το ίδιο μοναδικό κλειδί κρυπτογράφησης. Όμως, δύο λειτουργίες με το ίδιο κλειδί αποτελεί κενό στην ασφάλεια. Το πρόβλημα έχει λυθεί με την χρήση διαφορετικών IV για την κρυπτογράφηση και διαφορετικό για το MIC με αποτέλεσμα να δημιουργούνται δύο διαφορετικά key stream.
Για την σωστή λειτουργία του δικτύου δεν είναι δυνατό να κρυπτογραφούνται όλα τα δεδομένα που αποστέλλονται. Αναγκαστικά, η κεφαλίδα του πλαισίου πρέπει να είναι καθαρό κείμενο. Η αλλοίωση της κεφαλίδας του πλαισίου, όμως, αποτελεί είδος επίθεσης από μόνη της και έτσι θα πρέπει να προστατεύεται από το MIC. Το γεγονός ότι έτσι η είσοδος του Counter Mode είναι μόνο τμήμα αυτής του CBC MAC αποτελεί άλλο ένα πρόβλημα που για την αντιμετώπισή του απαιτείται αλλαγή στον τρόπο λειτουργίας του αλγόριθμου κρυπτογράφησης.
Ένα ακόμα από τα επιπρόσθετα στοιχεία του CCM στην λειτουργία του Counter Mode είναι ο ορισμός της παραγωγής μιας μοναδικής τιμής εκκίνησης του μετρητή διαφορετικής για κάθε μήνυμα. Αυτή η τιμή αναφέρεται ως *nonce* και δεν επιτρέπει διαδοχικά μηνύματα να έχουν κρυπτογραφική συνοχή.

2.8.4 Λειτουργία του CCM Protocol

Το πρώτο βήμα για την κρυπτογράφηση στο CCMP είναι ο υπολογισμός του MIC. Ο MIC υπολογίζεται με βάση το σώμα του πλαισίου αλλά και την

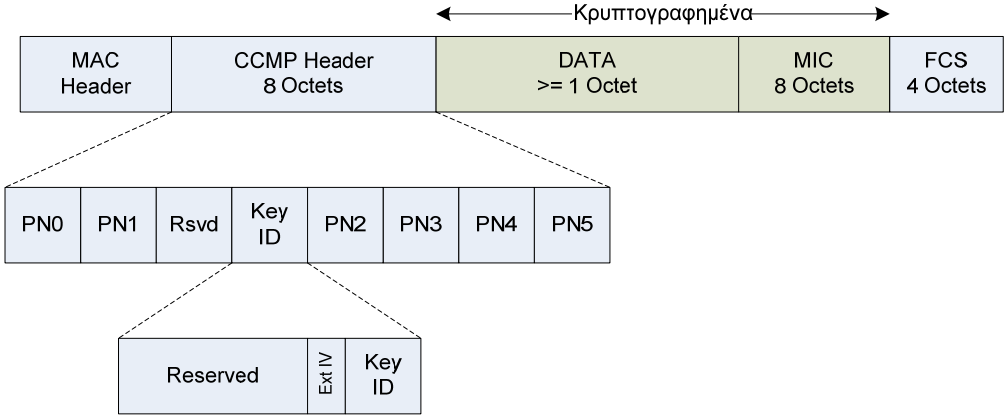
[6] Το ακρώνυμο MAC χρησιμοποιείται ήδη από το IEEE ως Medium Access Control και το Message Authentication Code (MAC) αντικαταστάθηκε από το Message Integrity Code (MIC).

κεφαλίδα MAC που στο πρότυπο 802.11i αναφέρεται ως Additional Authenticated Data (AAD).



Σχήμα 2. 16

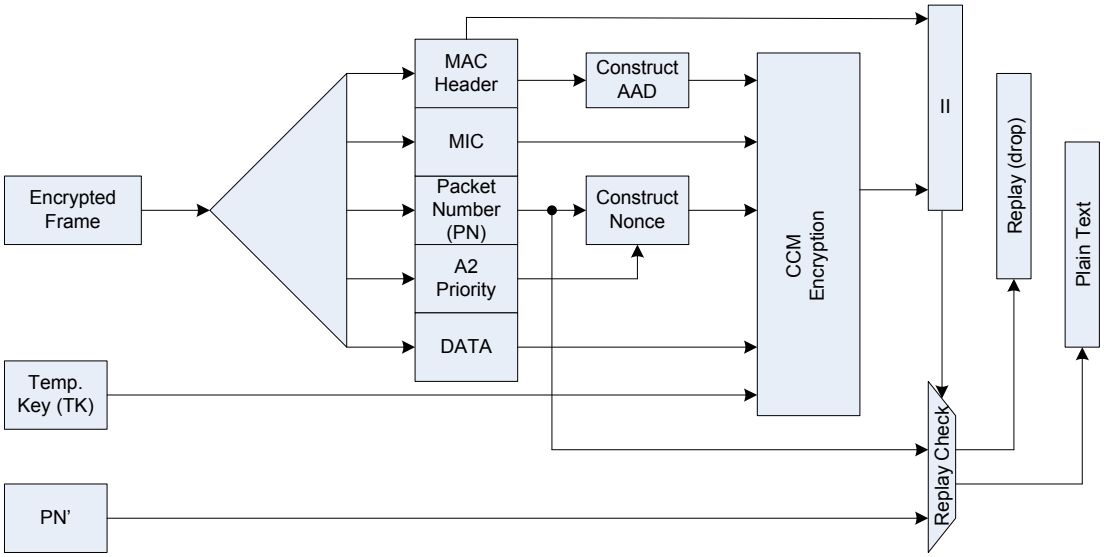
Ο MIC υπολογίζεται σύμφωνα με το CBC MAC με κάποιες διαφοροποιήσεις. Το αρχικό τμήμα των 128bit που κρυπτογραφείται δεν είναι το πρώτο τμήμα του καθαρού κειμένου (σχ. 2.14.Β) αλλά το nonce για να διασφαλίζεται η μοναδικότητά του. Το nonce αποτελείται από τρία τμήματα: Την διεύθυνση MAC του αποστολέα, τον αναγνωριστικό αριθμό του πακέτου Packet Number (PN) και την τιμή Priority που είναι σταθερή, προς το παρόν, και προορίζεται για μελλοντική χρήση. Κατά τ' άλλα, ο υπολογισμός του κώδικα ακεραιότητας υπολογίζεται κατά τα γνωστά με αποτέλεσμα μια ακολουθία των 128bit. Ο τελικός MIC που χρησιμοποιείται στο πλαίσιο (σχ. 2.17) είναι τα 64 πιο σημαντικά bits της παραπάνω ακολουθίας.



Σχήμα 2. 17

Μετά τον υπολογισμό του MIC, τα πεδία της κεφαλίδας του CCMP έχουν συμπληρωθεί και η διαδικασία μπορεί να προχωρήσει με την κρυπτογράφηση των πεδίων του μηνύματος και του MIC. Η διαδικασία κρυπτογράφησης είναι

αυτή του Counter Mode (σχ. 2.14.Β) με κάποιες τροποποιήσεις, όπως και στην περίπτωση του CBC MAC. Όπως έχει ήδη αναφερθεί, η αρχική τιμή του μετρητή είναι η nonce, η ίδια με αυτή που χρησιμοποιήθηκε για τον MIC.
Όπως και στην περίπτωση του TKIP, το κλειδί της κρυπτογράφησης δημιουργείται κατά την διαδικασία πιστοποίησης του χρήστη ή του τερματικού (βλέπε ανάλογο κεφάλαιο) και μπορεί να αλλάζει ανά τακτά χρονικά διαστήματα (temporal keys) αλλά πάντα καταστρέφεται κατά την αποσύνδεση.



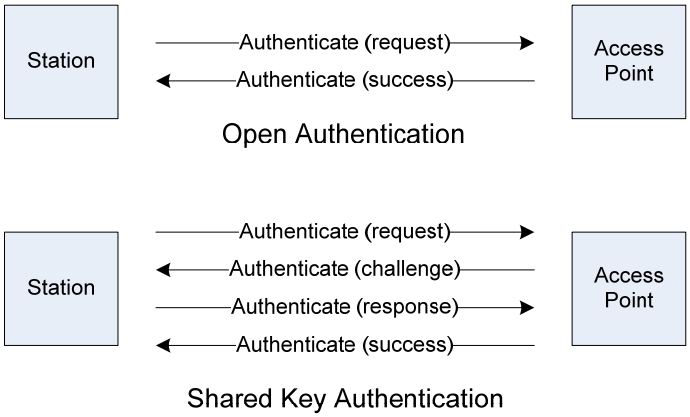
Σχήμα 2. 18

Η ανάκτηση του καθαρού κειμένου είναι ακριβώς η αντίστροφη διαδικασία της κρυπτογράφησης συν δύο επιπλέων ελέγχους. Ο πρώτος, ελέγχει το packet number και αν αυτό έχει μικρότερη τιμή από το προηγούμενο πλαίσιο υποτίθεται ότι έχει γίνει επίθεση επανάληψης και το πακέτο απορρίπτεται. Κατά τον δεύτερο έλεγχο, επαναϋπολογίζεται ο MIC για την επαλήθευση της ακεραιότητας των δεδομένων.

2.9 Πιστοποίηση πριν το 802.11i

Το πρώτο 802.11 standard ορίζει δύο τρόπους πιστοποίησης. Έναν "ανοιχτό" (open) και ένα με την χρήση του κοινού κλειδιού του WEP (shared key).
Με την Open Authentication, πρακτικά, οποιοσδήποτε ζητάει να πιστοποιηθεί λαμβάνει έγκριση από το Access Point και δεν μπορεί να θεωρηθεί πιστοποίηση αλλά ένας τρόπος εκκίνησης της σύνδεσης. Παρ' όλα αυτά, οι κατασκευαστές χρησιμοποιούν την Open πιστοποίηση ως μέσο για έλεγχο πρόσβασης με φιλτράρισμα της MAC Address. Ο διαχειριστής του δικτύου συμπληρώνει μια λίστα με τις διευθύνσεις MAC των καρτών δικτύου που επιθυμεί να συνδέονται στο AP. Κατά την διαδικασία της πιστοποίησης το AP δεν εγκρίνει αιτήσεις από μηχανήματα που δεν συμπεριλαμβάνονται στην

λίστα. Πρακτικά, με αυτό τον τρόπο, το δίκτυο προστατεύεται μόνο από πολύ απλές επιθέσεις και κατά λάθος συνδέσεις.



Σχήμα 2. 19

Στον δεύτερο τρόπο πιστοποίησης του 802.11 γίνεται έλεγχος του κοινού κλειδιού του WEP. Αρχικά, ο σταθμός στέλνει μια αίτηση για συμμέτοχη στο δίκτυο. Στην συνέχεια, το AP του στέλνει ένα τυχαίο αριθμό, το challenge text. Ο σταθμός λαμβάνει το challenge text, το κρυπτογραφεί με το WEP και το στέλνει πίσω στο AP. Το AP αποκρυπτογραφεί την απάντηση με το κοινό κλειδί και την συγκρίνει με το αρχικό challenge text. Αν οι δύο αριθμοί ταυτίζονται, δηλαδή ο σταθμός έχει το σωστό κλειδί, η αίτηση εγκρίνεται. Σε διαφορετική περίπτωση η αίτηση απορρίπτεται.
Η παραπάνω μέθοδος έχει τρία βασικά αρνητικά σημεία. Πρώτον, η πιστοποίηση αυτού του τύπου είναι μονόδρομη. Το δίκτυο πιστοποιεί τον χρήστη αλλά ο χρήστης δεν έχει δυνατότητα πιστοποίησης του δικτύου. Δεύτερον, αν κάποιος υποκλέψει μια επιτυχημένη διαδικασία πιστοποίησης, μπορεί πολύ εύκολα, με XOR μεταξύ του μη κρυπτογραφημένου challenge text και της κρυπτογραφημένης απάντησης, να αποκαλύψει όλο το key stream. Τελευταίο και σημαντικότερο, με αυτή τη μέθοδο δεν πιστοποιείται η ταυτότητα του χρήστη αλλά το γεγονός ότι ένα μηχάνημα έχει ρυθμιστεί με το σωστό κοινό κλειδί. Κανένας δεν εμποδίζει ένα μη πιστοποιημένο χρήστη να χρησιμοποιήσει ένα πιστοποιημένο σταθμό. Επιπλέον, όπως έχει αναφερθεί, η αποκάλυψη του κοινού κλειδιού είναι αρκετά εύκολη οπότε και η πιστοποίηση του σταθμού δεν μπορεί να είναι στεγανή.
Η χρήση shared key authentication ταυτόχρονα με την χρήση του WEP δεν είναι υποχρεωτική από το πρότυπο αλλά δίνεται σαν επιλογή. Τα παραπάνω προβλήματα, και ιδιαίτερα το δεύτερο, καθιστούν την χρήση της ανοιχτής πιστοποίησης ασφαλέστερη. Ωστόσο, η συνύπαρξη open authentication και WEP δημιουργεί κάποια διαχειριστικά προβλήματα. Για παράδειγμα, ένας σταθμός με λάθος κλειδί θα φαίνεται κανονικά συνδεδεμένος στο δίκτυο αλλά όλα τα πακέτα θα απορρίπτονται κάνοντας την επικοινωνία αδύνατη.

2.10 Πιστοποίηση μετά το 802.11i

Όπως είδαμε, οι μηχανισμοί πιστοποίησης του αρχικού προτύπου 802.11 παρέχουν μηδενικό επίπεδο ασφάλειας. Η λύση αναζητήθηκε, αρχικά από την WiFi Alliance και στην συνέχεια από το TGi, σε ήδη υπάρχουσες τεχνολογίες. Παρατηρήθηκε ότι υπάρχει αναλογία στα θέματα πιστοποίησης μεταξύ των ασυρμάτων δικτύων και των dial-up συνδέσεων. Φυσικά, οι λύσεις που δόθηκαν στα peer-to-peer δίκτυα, αρκετά χρόνια πριν την ύπαρξη των ασυρμάτων, δεν θα μπορούσαν να εφαρμοστούν ως έχουν. Μετά τις απαραίτητες προσαρμογές προέκυψε μία μεγάλη συλλογή από πρότυπα διαφόρων οργανισμών και πάρα πολλά ακρωνύμια που προκαλούν σύγχυση.
Από τις dial-up συνδέσεις διατηρήθηκε το Extensible Authentication Protocol (EAP) που περιγράφει, αλλά δεν ορίζει, τον τρόπο πιστοποίησης και τα μηνύματα μεταξύ της οντότητας που αιτείται (Supplicant) και της οντότητας που πιστοποιεί (Authenticator). Ο τρόπος πιστοποίησης αφήνεται να οριστεί από άλλα πρότυπα όπως τα EAP-TLS και PEAP, όπως θα δούμε αργότερα. Η διαδικασία αποστολής της πληροφορίας στα peer-to-peer δίκτυα και στα τοπικά δίκτυα είναι πολύ διαφορετική, οπότε έπρεπε να βρεθεί τρόπος ανταλλαγής των μηνυμάτων του EAP. Ο τρόπος αυτός και η πλαισίωση των μηνυμάτων του EAP ονομάζεται EAP over LAN (EAPOL) και περιγράφεται στο πρότυπο IEEE 802.1x. Το ίδιο πρότυπο εισάγει και την έννοια του εξυπηρετητή πιστοποίησης (authentication server, AS) αλλά και πάλι χωρίς να την ορίζει. Για τον ορισμό του AS και τον τρόπο επικοινωνίας του με την οντότητα που πιστοποιεί, το 802.1x προτείνει, και η WiFi επιβάλλει, μια ακόμα τεχνολογία δανεισμένη από τις dial-up συνδέσεις, την Remote Access Dial-in User Service (RADIUS). Τέλος, από τις διάφορες μεθόδους πιστοποίησης που βασίζονται στο EAP, η WiFi Alliance ορίζει τις:

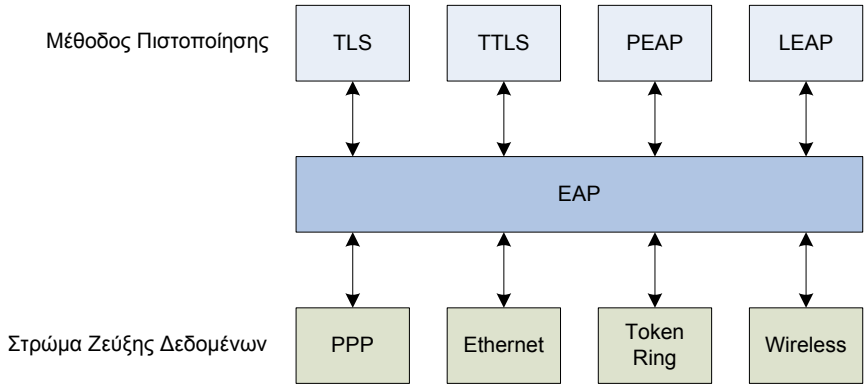
- EAP-TLS
- EAP-TTLS/EAP-MS-CHAPv2
- PEAPv0/EAP-MS-CHAPv2
- PEAPv1/EAP-GTC
- EAP-SIM

ως μέρος των προτύπων WPA-Enterprise και WPA2-Enterprise.

2.11 Extensible Authentication Protocol

Το EAP είναι ένα ευέλικτο πρωτόκολλο μεταφοράς πληροφοριών πιστοποίησης. Επίσημα, παρουσιάστηκε στο RFC 2284 της IETF, ένα έγγραφο δεκαέξι μόλις σελίδων και αρχικά αναπτύχθηκε για χρήση με το Point to Point Protocol (PPP) στις dial-up συνδέσεις.
Το EAP έχει δύο βασικά και πολύ χρήσιμα χαρακτηρίστηκα. Πρώτον, διαχωρίζει την ανταλλαγή των μηνυμάτων πιστοποίησης, παρέχοντας ένα ανεξάρτητο στρώμα, από την διαδικασία της πιστοποίησης. Αυτό μας οδηγεί στο δεύτερο χαρακτηριστικό, την επεκτασιμότητα. Η μέθοδος πιστοποίησης

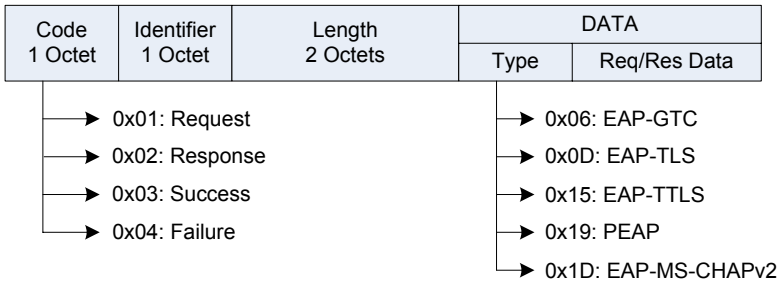
μπορεί να αλλάζει με κάποια άλλη, πιθανώς νεότερη, για μεγαλύτερη ασφάλεια χωρίς αντίκτυπο στον τρόπο μεταφοράς των μηνυμάτων, δηλαδή στο στρώμα EAP.



Σχήμα 2. 20

Το RFC 2284 ορίζει τέσσερις τύπους μηνυμάτων:

- *Request*: Μηνύματα από τον authenticator στον supplicant.
- *Response*: Μηνύματα από τον supplicant στον authenticator.
- *Success*: Στέλνεται από τον authenticator για τον τερματισμό επιτυχημένης διαδικασίας πιστοποίησης.
- *Failure*: Στέλνεται από τον authenticator για τον τερματισμό αποτυχημένης διαδικασίας πιστοποίησης.



Σχήμα 2. 21

Όπως φαίνεται και στο σχήμα χ.χ, ο τύπος του κάθε μηνύματος φαίνεται στο πρώτο byte του EAP header (πεδίο Code). Τα μηνύματα Request/Response χωρίζονται περεταίρω στο πεδίο Type ανάλογα με την μέθοδο πιστοποίησης που χρησιμοποιείται κάθε φορά. Εκτός από την μέθοδο πιστοποίησης, οι κώδικες 1 ως 3 ορίζουν και κάποια διαχειριστικά μηνύματα. Στο σχήμα φαίνονται οι κωδικοί των τύπων που αφορούν στα ασύρματα δίκτυα.
Οι πρώτοι έξι κώδικες του πεδίου Type δεσμεύονται από το RFC 2284 και είναι οι:

1. Identity
2. Notification
3. NAK (μόνο response)
4. MD5-Challenge
5. One-Time Password (OTP)

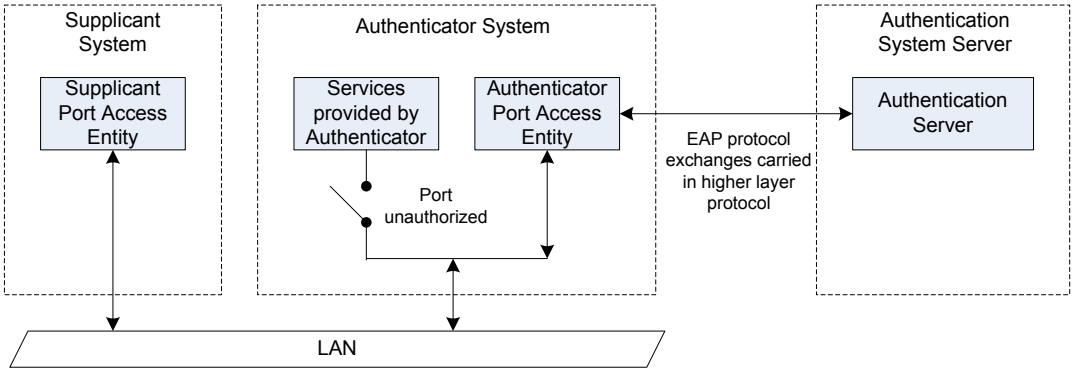
6. Generic Token Card (GTC)

Οι υπόλοιποι καθορίζονται αποκλειστικά από την Internet Assigned Numbers Authority (IANA) και αποδίδονται σε κάθε νέα μέθοδο.

Γενικά, η διαδικασία της πιστοποίησης εκκινεί με τον authenticator να ζητάει την ταυτότητα του supplicant, στέλνοντάς του ένα Request Identity μήνυμα. Στην συνέχεια ο supplicant στέλνει ένα Response Identity μήνυμα με τα απαραίτητα στοιχεία. Κατά την απλούστερη δυνατή διαδικασία πιστοποίησης ο authenticator θα μπορούσε να στείλει ένα μήνυμα Success ή Failure και να ολοκληρωθεί εκεί αλλά συνήθως αυτή είναι μόνο η αρχή και η διαδικασία συνεχίζεται ανάλογα με την μέθοδο.
Το μήνυμα με κωδικό Type 2 μπορεί να χρησιμοποιηθεί από τον authenticator για να εμφανίσει κάποιο κείμενο στο τερματικό του supplicant αλλά γενικά δεν χρησιμοποιείται σε εφαρμογές ασυρμάτων δικτύων.
Το τελευταίο διαχειριστικό μήνυμα του EAP είναι το NAK. Εάν ο supplicant χρησιμοποιεί μια μέθοδο πιστοποίησης διαφορετική από αυτή που περιέχεται στο Request του authenticator, ο supplicant στέλνει ένα μήνυμα NAK ώστε να γίνει αλλαγή της μεθόδου. Αν αυτό είναι δυνατό, ο authenticator αλλάζει μέθοδο. Αν και πάλι οι δύο μέθοδοι δεν συμπίπτουν, ο supplicant ξαναστέλνει ένα NAK και ούτω καθ' εξής.

2.12 802.1x: Port-Based Network Access Control

Όπως φαίνεται και από τον τίτλο, το 802.1x έχει στόχο τον έλεγχο πρόσβασης στο σημείο εισόδου στο δίκτυο. Όταν εκδόθηκε για πρώτη φορά αφορούσε τα δύο ενσύρματα πρότυπα τοπικών δικτύων του IEEE, δηλαδή τα Ethernet και Token Ring. Στα ενσύρματα δίκτυα, όπως το Ethernet, σημείο εισόδου στο δίκτυο είναι η κάθε θύρα ενός switch. Στα ασύρματα δίκτυα, δεν υπάρχει τέτοιο υλικό σημείο οπότε εισάγεται η έννοια της λογικής θύρας, δηλαδή ένα λογικό σημείο εισόδου, διαφορετικό για κάθε σύνδεση μεταξύ ασύρματου σταθμού και Access Point.



Κατά το 802.1x όλο το δίκτυο χωρίζεται σε τρείς οντότητες:

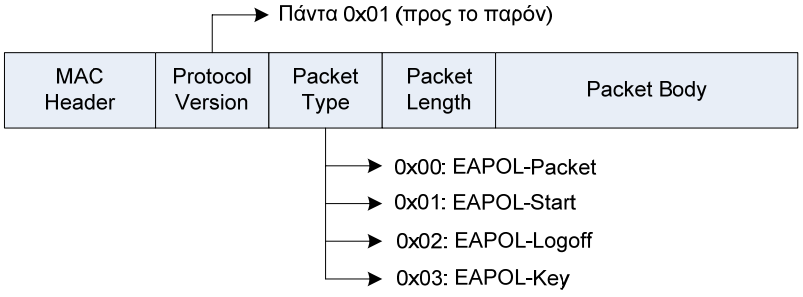
- Τους αιτούντες (supplicants) που ζητούν πρόσβαση στο δίκτυο.

- Τους πιστοποιητές (authenticators) που ελέγχουν την πρόσβαση στο δίκτυο.
- Τους εξυπηρετητές πιστοποίησης (authentication servers) που λαμβάνουν τις αποφάσεις για την πρόσβαση.

Στην περίπτωση των ασυρμάτων δικτύων, αιτούντες είναι όλοι οι σταθμοί που συμμετέχουν στο BSS και πιστοποιητής είναι το Access Point. Όπως φαίνεται και στο σχήμα, αρχικά ο κάθε supplicant μπορεί να έχει πρόσβαση μόνο στον AS. Πρακτικά, έχει πρόσβαση και σε όλες τις άλλες υπηρεσίες, όπως σε DHCP servers, που είναι αναγκαίες για την επικοινωνία με τον AS, αλλά η πρόσβαση στις άλλες υπηρεσίες του authenticator, δηλαδή τους πόρους του δικτύου, είναι απαγορευμένη. Εάν η διαδικασία πιστοποίησης είναι επιτυχής, τότε ο authenticator παρέχει στον supplicant πλήρη πρόσβαση στους πόρους του δικτύου.
Όπως και στην περίπτωση του EAP, το 802.1x δίνει μόνο το πλαίσιο λειτουργίας και όχι τις επιμέρους λεπτομέρειες της πιστοποίησης που τις αφήνει, αόριστα, σε πρωτόκολλα ανωτέρου στρώματος.

2.12.1 EAP over LAN

Το RFC του EAP δεν καθορίζει πως θα πρέπει να μεταφέρονται τα μηνύματά του σε ένα δίκτυο. Στα τοπικά δίκτυα κάθε πληροφορία θα πρέπει να πλαισιωθεί με το κατάλληλο header και πιθανώς και με ένα trailer στο στρώμα ζεύξης δεδομένων για την μετάδοσή του στο φυσικό στρώμα. Για τις πληροφορίες του EAP ο τρόπος αυτός περιγράφεται στο πρότυπο 802.1x και ονομάζεται EAP over LAN (EAPOL).



Σχήμα 2. 22

Το IEEE εκτός από το να προσθέσει ένα MAC header στα μηνύματα του EAP για την αποστολή τους στο δίκτυο, εισάγει και κάποιους άλλους τύπους μηνυμάτων χρήσιμους για την διεκπεραίωση διαχειριστικών εργασιών. Συνολικά, ορίζονται πέντε τύποι μηνυμάτων EAPOL:

- EAPOL – Start
- EAPOL – Key
- EAPOL – Packet
- EAPOL – Logoff
- EAPOL – Encapsulated-ASF-Alert

Ο τελευταίος τύπος δεν έχει υιοθετηθεί από την WiFi και δεν χρησιμοποιείται στα ασύρματα δίκτυα.
Όταν ένας χρήστης επιχειρεί να συνδεθεί στο δίκτυο δεν μπορεί να ξέρει αν υπάρχει authenticator και ακόμη περισσότερο λεπτομέρειες όπως η MAC διεύθυνσή του. Για να ξεκινήσει η διαδικασία πιστοποίησης, ο client στέλνει ένα πλαίσιο EAPOL – Start ως multicast. Στην συνέχεια, ο authenticator στέλνει ένα μήνυμα EAP-Request Identity σε ένα πλαίσιο EAPOL – Packet.
Από όλα τα πλαίσια του EAPOL, τα EAPOL – Packet είναι αυτά που χρησιμοποιούνται για την αποστολή των μηνυμάτων του EAP.

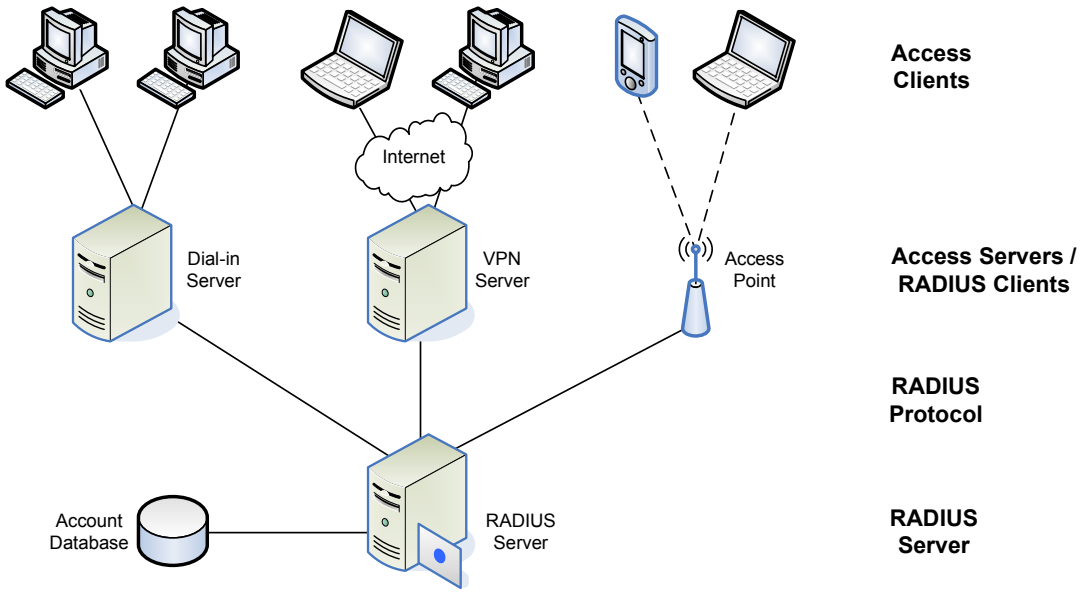
2.13 Remote Access Dial-in User Service (RADIUS)

Στην παράγραφο του 802.1x έγινε αναφορά για την ανάγκη ύπαρξης ενός εξυπηρετητή πιστοποίησης. Ούτε το πρότυπο 802.1x αλλά ούτε και το 802.11i αναφέρεται στον τύπο αυτού του server και στον τρόπο επικοινωνίας με τους πιστοποιητές και τους αιτούντες. Στο 802.11i γίνεται αναφορά σε δύο τύπους, στον RADIUS και στον Diameter, που θα μπορούσαν να χρησιμοποιηθούν αλλά όχι υποχρεωτικά. Οι λόγοι που αναφέρομαι συγκεκριμένα στο RADIUS και όχι στον Diameter ή στον TACACS ή σε οποιονδήποτε άλλο είναι ότι ο RADIUS χρησιμοποιήθηκε στο πειραματικό μέρος της εργασίας, είναι ανοιχτό πρότυπο και ολοκληρώνεται στο γνωστότερο λειτουργικό σύστημα για servers[7].
Το RADIUS είναι ο τρόπος του IETF για το λεγόμενο AAA (Authentication, Authorization, Accounting). Ένα ολοκληρωμένο σύστημα AAA περιγράφει τον τρόπο που γίνεται η πιστοποίηση των χρηστών, η εξουσιοδότησή τους στους πόρους του δικτύου και την καταγραφή των δραστηριοτήτων τους, αλλά και είναι ένα πρωτόκολλο επικοινωνίας μεταξύ των πιστοποιητών και του εξυπηρετητή πιστοποίησης. Το IETF έχει εκδώσει διάφορα πρότυπα ανάλογα με την τεχνολογία που χρησιμοποιείται στο στρώμα ζεύξης δεδομένων αλλά και της τεχνολογίας του πλαισίου λειτουργίας της πιστοποίησης. Τα πρότυπα που εμπλέκονται στα ασύρματα δίκτυα είναι τα:

- RFC2865: Remote Access Dial-in User Service (RADIUS)
- RFC2869: RADIUS Extensions (EAP over RADIUS)
- RFC2548: Microsoft Vendor-specific RADIUS attributes
- RFC3580: IEEE 802.1x RADIUS Usage Guidelines

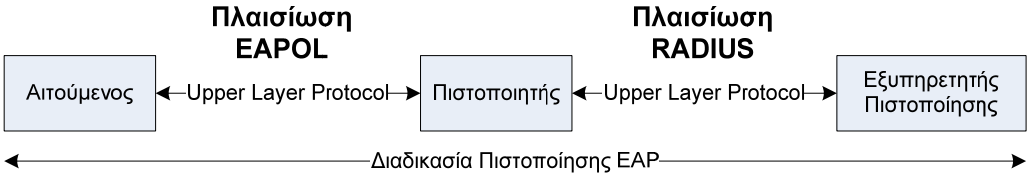
Σύμφωνα με το πρότυπο, στο δίκτυο υπάρχουν τρείς οντότητες (σχ. χ.χ). Ο RADIUS server έχει τον ρόλο του εξυπηρετητή πιστοποίησης. Οι RADIUS clients ή Access servers δέχονται τις αιτήσεις και σύμφωνα με το 802.1x είναι οι πιστοποιητές. Στην περίπτωση των ασυρμάτων, access server είναι το access point. Τέλος, οι αιτούντες αναφέρονται ως Access clients.

[7] Το πρωτόκολλο RADIUS ολοκληρώνεται στις enterprise εκδόσεις των MS Windows Server 2000 / 2003 με την ονομασία Internet Authentication Service (IAS).



Σχήμα 2. 23

Οι access clients στέλνουν τις αιτήσεις πιστοποίησης στους RADIUS clients χρησιμοποιώντας μηνύματα κάποιου τρίτου πρωτοκόλλου όπως το EAP. Ο RADIUS client μεταφέρει αυτές τις αιτήσεις στον RADIUS server για έγκριση με την μορφή μηνυμάτων του πρωτοκόλλου RADIUS. Εδώ πρέπει να σημειωθεί ότι η αλλαγή των μηνυμάτων δεν αλλάζει τον τρόπο πιστοποίησης που συνεχίζει να ελέγχεται από το EAP. Ειδικά στο EAP over RADIUS που χρησιμοποιείται στα ασύρματα, ο πιστοποιητής παίζει απλά τον ρόλο διεπαφής μεταφράζοντας και περνώντας τα μηνύματα μεταξύ των δύο πρωτοκόλλων.



Σχήμα 2. 24

2.13.1 Μηνύματα πρωτοκόλλου RADIUS

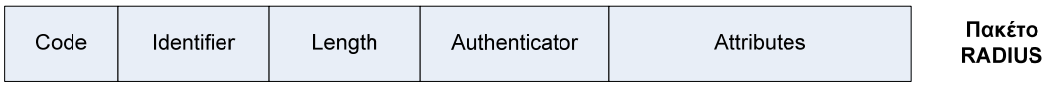
Κατά την επικοινωνία μεταξύ ενός RADIUS server και των RADIUS clients χρησιμοποιούνται έξι τύποι μηνυμάτων, τέσσερις για την διαδικασία πιστοποίησης και δυο για την καταγραφή της δραστηριότητας των χρηστών.

- **Access-Request** Στέλνεται από τους RADIUS clients για κάθε νέα προσπάθεια εισόδου στο δίκτυο.
- **Access-Accept** Στέλνεται από τον RADIUS server ως απάντηση στο Access-Request. Πληροφορεί τον RADIUS client ότι η προσπάθεια εισόδου στο δίκτυο έχει πιστοποιηθεί και εξουσιοδοτηθεί.
- **Access-Reject** Στέλνεται από τον RADIUS server ως απάντηση στο Access-Request. Πληροφορεί τον RADIUS client ότι η αίτηση εισόδου στο δίκτυο έχει απορριφθεί. Στέλνεται σε περίπτωση που τα διαπιστευτήρια του χρήστη δεν ισχύουν.

- **Access-Challenge** Στέλνεται από τον RADIUS server ως απάντηση στο Access-Request. Σκοπός του είναι να εξακριβώσει την ταυτότητα του RADIUS client.
- **Accounting-Request** Στέλνεται από τους RADIUS clients και περιέχει πληροφορίες σχετικά με την χρήση του δικτύου.
- **Accounting-Response** Στέλνεται από τον RADIUS server ως απάντηση στο Accounting-Request. Πληροφορεί τον RADIUS client ότι το μήνυμα έχει ληφθεί με επιτυχία.

2.13.2 Πλαισίωση Μηνυμάτων RADIUS

Ένα πακέτο του πρωτοκόλλου RADIUS αποτελείται από πέντε πεδία και έχει την μορφή του σχ. 2.25.



Σχήμα 2. 25

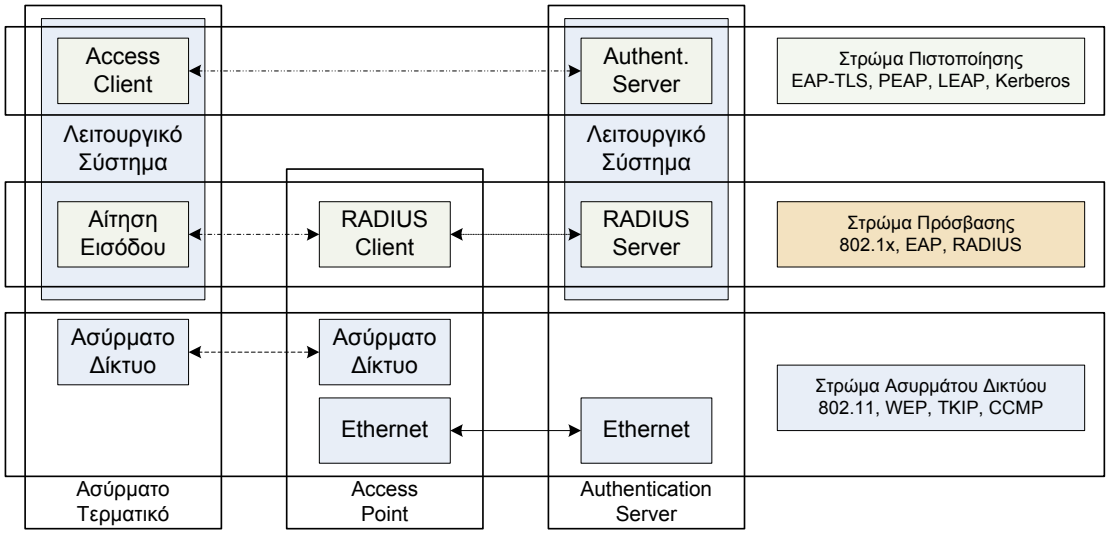
Πρώτο είναι το πεδίο του κωδικού του μηνύματος και η τιμή του εξαρτάτε από τον τύπο του μηνύματος. Για τα τέσσερα μηνύματα πιστοποίησης οι τιμές είναι:

- Access-Request – Code 01
- Access-Accept – Code 02
- Access-Reject – Code 03
- Access-Challenge – Code 11

Το πιο σημαντικό πεδίο του πακέτου, από την άποψη της ασφάλειας, είναι το Authenticator. Το πεδίο έχει μήκος 128 bit και η χρήση του εξαρτάτε από τον τύπο του μηνύματος. Στο Access-Request το πεδίο περιέχει ένα τυχαίο αριθμό που αλλάζει κάθε φορά (nonce). Στα attributes του πακέτου περιέχονται ευαίσθητα δεδομένα, όπως το password του αιτούμενου, που χρειάζονται κρυπτογράφηση. Η κρυπτογράφηση γίνεται με χρήση MD5 (Message Digest 5) hash. Το κλειδί της κρυπτογράφησης προκύπτει από το κοινό σταθερό κλειδί που είναι ρυθμισμένο στους RADIUS clients και στον server και το nonce. Τα υπόλοιπα τρία μηνύματα είναι απαντήσεις στο Access-Request και είναι σημαντικό να προέρχονται από τον server και να μην έχουν τροποποιηθεί στην πορεία. Σ' αυτά τα μηνύματα, το πεδίο authenticator περιέχει μια ακολουθία ακεραιότητας αντίστοιχη του ICV.
Το πεδίο Identifier περιέχει μια τυχαία τιμή που σκοπό έχει την αντιστοίχιση των αιτήσεων και των απαντήσεων και το πεδίο Length υποδεικνύει το συνολικό μήκος του πακέτου.

2.14 Μέθοδοι Πιστοποίησης Ανωτέρου Στρώματος

Η ασφάλεια στα ασύρματα δίκτυα μπορεί να μοντελοποιηθεί και να διαχωριστεί σε τρία στρώματα. Το στρώμα ασυρμάτου δικτύου, το στρώμα πρόσβασης και το στρώμα πιστοποίησης.



Σχήμα 2. 26

Στο χαμηλότερο στρώμα, το στρώμα ασυρμάτου δικτύου λαμβάνει χώρα η πραγματική επικοινωνία καθώς και η κρύπτο/αποκρυπτογράφηση των δεδομένων. Όλες οι λειτουργίες γίνονται σε επίπεδο hardware και η αντιστοίχιση στο πρότυπο αναφοράς OSI είναι στο φυσικό στρώμα και στο στρώμα ζεύξης δεδομένων.
Το δεύτερο στρώμα, το στρώμα πρόσβασης, είναι επί της ουσίας η διεπαφή μεταξύ των δύο άλλων στρωμάτων. Το στρώμα πρόσβασης μπορεί να αντιστοιχιστεί στο στρώμα δικτύου του OSI. Πρακτικά, προσφέρει τις υπηρεσίες του στο στρώμα πιστοποίησης και καθορίζει την μορφή και τον τρόπο πλαισίωσης των μηνυμάτων πιστοποίησης.
Το περιεχόμενο αυτών των μηνυμάτων πιστοποίησης και άλλες υπηρεσίες όπως η δημιουργία των κλειδιών κρυπτογράφησης του στρώματος ασύρματου δικτύου, αφήνεται σε πρωτόκολλα ανώτερου στρώματος. Το ανώτερο στρώμα είναι το στρώμα πιστοποίησης. Ανάλογα με το πρωτόκολλο που χρησιμοποιείται, το στρώμα πιστοποίησης μπορεί να τοποθετηθεί οπουδήποτε μεταξύ των στρωμάτων μεταφοράς και εφαρμογής. Όλες οι λειτουργίες του στρώματος συμβαίνουν σε επίπεδο λογισμικού. Όπως υπονοείται και από τον τίτλο "πρωτόκολλα ανώτερου στρώματος", τα πρωτόκολλα πιστοποίησης είναι ανεξάρτητα της τεχνολογίας των δικτύων και οπότε εκτός του πεδίου δράσης του IEEE.
Η επιλογή επαφίεται στους σχεδιαστές των δικτύων και τους κατασκευαστές. Η WiFi Alliance προωθεί το EAP-TLS, η Microsoft το PEAP σε συνδυασμό με το δικό της MS-CHAP-v2 και η Cisco το LEAP. Τα δύο πρώτα είναι ανοιχτά πρότυπα του IETF, ενώ το τελευταίο πατενταρισμένο. Επίσης, αν και το PEAP υποστηρίζεται από τη WiFi, κάποιος κατασκευαστής αρκεί να ολοκληρώνει το

EAP-TLS για να πιστοποιηθεί. Από την άλλη μεριά, το PEAP είναι νεότερο και ασφαλέστερο πρότυπο.

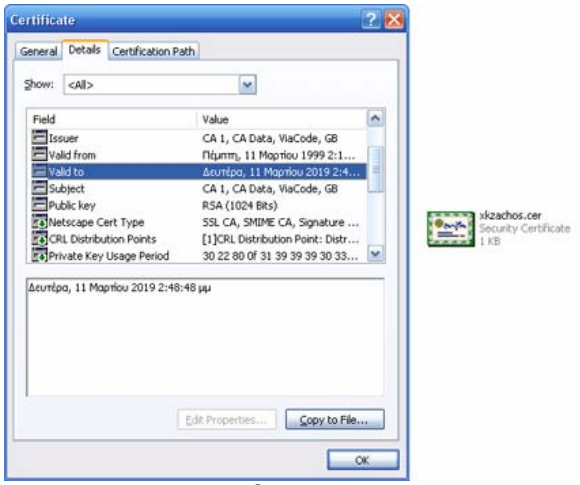
2.14.1 Transport Layer Security (TLS)

Το TLS εκδόθηκε από το IETF στο πρότυπο RFC2246 του 1999 και αποτελεί την προτυποποιημένη και ανοιχτή εκδοχή του SSL 3.0 της Netscape. Το SSL είναι η στάνταρ μέθοδος προστασίας των συναλλαγών στο Internet. Όπως εξάγεται και από την ονομασία, το TLS κατατάσσεται στις διεργασίες του στρώματος μεταφοράς.
Το TLS είναι ένας ολοκληρωμένος μηχανισμός ασφάλειας και διαχείρισης δεδομένων με υπηρεσίες πιστοποίησης, κρυπτογράφησης και συμπίεσης δεδομένων. Οι περισσότερες απ' αυτές είναι άχρηστες στα ασύρματα δίκτυα αφού η κρυπτογράφηση συμβαίνει σε χαμηλότερο επίπεδο και συμπίεση δεδομένων δεν προβλέπεται σε καμία περίπτωση. Στο RSN χρησιμοποιείται το υποσύνολο του TLS που αφορά την πιστοποίηση. Για την πιστοποίηση των χρηστών, το πρωτόκολλο χρησιμοποιεί ψηφιακά πιστοποιητικά.

2.14.2 Ψηφιακές Υπογραφές, Ψηφιακά Πιστοποιητικά και Αρχές Έκδοσης

Όπως έχει περιγραφεί στην παράγραφο Αρχές Κρυπτογράφησης, υπάρχουν δύο είδη κρυπτογράφησης, η συμμετρική και η ασύμμετρη. Η ασύμμετρη κρυπτογράφηση αναφέρεται και ως κρυπτογράφηση δημόσιου κλειδιού (public key).
Στην κρυπτογράφηση δημόσιου κλειδιού χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση. Από τα δύο κλειδιά, το κλειδί της κρυπτογράφησης είναι δημόσιο και γνωστό σε όλους. Το κλειδί της αποκρυπτογράφησης είναι ιδιωτικό και γνωστό μόνο σε ένα μέλος. Το δημόσιο κλειδί προκύπτει μαθηματικά από το ιδιωτικό. Κατά την κρυπτογράφηση, ο αποστολέας χρησιμοποιεί το δημόσιο κλειδί του παραλήπτη και ο παραλήπτης χρησιμοποιεί το αντίστοιχο ιδιωτικό για την αντίστροφη διαδικασία.
Εκτός από την κρυπτογράφηση δεδομένων, η κρυπτογράφηση δημόσιου κλειδιού χρησιμοποιείται στην δημιουργία ψηφιακών υπογραφών. Η ψηφιακή υπογραφή είναι ένας τρόπος ελέγχου της ταυτότητας του αποστολέα και της ακεραιότητας του μηνύματος.
Για την δημιουργία ψηφιακής υπογραφής, αρχικά, υπολογίζεται ένα hash του μηνύματος. Το hash είναι μια μαθηματική περίληψη των δεδομένων του μηνύματος. Στην συνέχεια, ο αποστολέας κρυπτογραφεί το hash χρησιμοποιώντας το ιδιωτικό του κλειδί. Η ψηφιακή υπογραφή είναι το κρυπτογραφημένο hash. Όταν ο παραλήπτης λάβει το μήνυμα αποκρυπτογραφεί την ψηφιακή υπογραφή με το δημόσιο κλειδί του αποστολέα και υπολογίζει το hash. Αν οι δύο τιμές είναι ίσες τότε ο παραλήπτης μπορεί είναι βέβαιος για την ταυτότητα του αποστολέα και την ακεραιότητα του μηνύματος.

Η μαθηματική εξάρτηση μεταξύ του ιδιωτικού και του δημόσιου κλειδιού εξασφαλίζει στον παραλήπτη ότι ο αποστολέας έχει το ιδιωτικό κλειδί. Το πρόβλημα με την ψηφιακή υπογραφή είναι ότι από μόνη της δεν μπορεί να βεβαιώσει την ταυτότητα αυτού που την εκδίδει. Όπως και στην πραγματικότητα, χρειάζεται μια αρχή που ο χρήστης να μπορεί να εμπιστευτεί και να βεβαιώσει την γνησιότητά της. Στην περίπτωσή μας, αυτή η τρίτη οντότητα είναι η Αρχή Έκδοσης Ψηφιακών Πιστοποιητικών (Certification Authority, CA). Μια CA μπορεί να είναι ένας εξυπηρετητής σε εταιρικά δίκτυα ή κάποια εταιρία που παρέχει τέτοιου είδους υπηρεσίες στο Internet.
Η πιστοποίηση της γνησιότητας και ακεραιότητας μιας ψηφιακής υπογραφής γίνεται μέσω αντιστοίχισης του δημόσιου κλειδιού με το πρόσωπο ή τη συσκευή ή την υπηρεσία που κρατάει το ιδιωτικό κλειδί. Αυτή η αντιστοίχιση επιτυγχάνεται με τα ψηφιακά πιστοποιητικά.



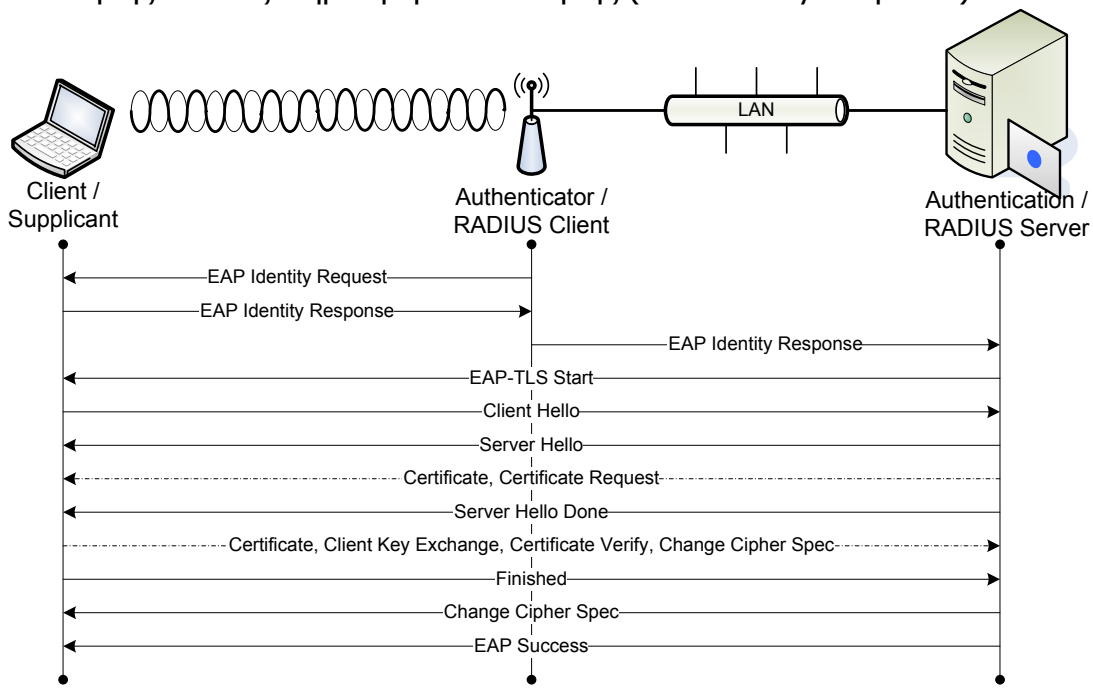
Σχήμα 2. 27

Το ψηφιακό πιστοποιητικό είναι μια δομή δεδομένων που εκδίδεται από μια CA και μεταξύ άλλων περιέχει το δημόσιο κλειδί. Η δομή του ακολουθεί κάποιο πρότυπο όπως το X.509 και είναι ψηφιακά υπογεγραμμένο από την CA που το εκδίδει. Οι πληροφορίες που περιέχει φαίνονται παρακάτω:

- **Subject** Πληροφορίες για την οντότητα που κατέχει το ιδιωτικό κλειδί. Μπορεί να είναι χρήστης, υπολογιστής ή κάποια υπηρεσία ενός Η/Υ.
- **Subject Public Key** Το δημόσιο κλειδί.
- **Subject ID Information** Επιπλέον πληροφορίες για την ταυτότητα της οντότητας που έχει το ιδιωτικό κλειδί.
- **Validity Period** Η περίοδος ισχύος του πιστοποιητικού. Μετά την λήξη, ο χρήστης του πιστοποιητικού θα πρέπει να ζητήσει ένα νέο από τη CA.
- **Issuer ID Information** Πληροφορίες σχετικά με την ταυτότητα της CA.
- **Certificate Signature** Η ψηφιακή υπογραφή της CA.

2.14.3 Πιστοποίηση με EAP-TLS

Στην διαδικασία πιστοποίησης TLS συμμετέχουν το σταθμός που αιτείται πρόσβαση στο δίκτυο και ο εξυπηρετητής πιστοποίησης. Ο ρόλος του πιστοποιητή περιορίζεται στην μεταβίβαση των μηνυμάτων των δύο πλευρών που όπως έχει αναφερθεί είναι EAP over LAN (client-AP) και EAP over RADIUS (AP-Authentication Server). Η διαδικασία ανταλλαγής μηνυμάτων με σκοπό την εξακρίβωση και την πιστοποίηση των δύο πλευρών είναι γνωστή ως χειραψία (handshake).
Η έναρξη της επικοινωνίας γίνεται όπως και σε κάθε πρωτόκολλο που χρησιμοποιεί πλαισίωση EAP με την απαίτηση της ταυτότητας του αιτούμενου από τον πιστοποιητή (EAP Identity Request) και την μεταβίβαση της απάντησης στον εξυπηρετητή πιστοποίησης (EAP Identity Response).



Σχήμα 2. 28

Η διαδικασία συνεχίζεται με τα μηνύματα του TLS. Το πρώτο μήνυμα είναι το client hello από τον αιτούμενο στον εξυπηρετητή. Το client hello περιέχει πληροφορίες για τον τύπο των πιστοποιητικών που υποστηρίζει ο client, τις μεθόδους κρυπτογράφησης και της μεθόδους ακεραιότητας των δεδομένων. Επίσης, περιέχει και έναν τυχαίο αριθμό που σκοπό έχει να εξασφαλίσει το handshake από επιθέσεις επανάληψης.
Η συνεδρία συνεχίζεται με την αποστολή του μηνύματος server hello. Το server hello υποδεικνύει ότι ο server υποστηρίζει τουλάχιστον ένα από τους τύπους πιστοποιητικών και κρυπτογράφησης που περιείχε το client hello και η διαδικασία μπορεί να συνεχιστεί. Επιπλέον, περιέχει δύο σημαντικές τιμές, το αναγνωριστικό της συνεδρίας (session ID) και μία τυχαία τιμή, διαφορετική από εκείνη του client. Το session ID χρησιμεύει σε περιπτώσεις που η συνεδρία διακοπεί και χρειαστεί ανακεφαλαίωση.

Στην συνέχεια ο server στέλνει το ψηφιακό πιστοποιητικό του και ζητάει, σε δεύτερο μήνυμα το ψηφιακό πιστοποιητικό του client. Ο client απαντάει με ένα μήνυμα που περιέχει το πιστοποιητικό.
Ακολουθεί το μήνυμα client key exchange. Σε αυτό το σημείο, ο client γνωρίζει όλα τα απαραίτητα για την παραγωγή του μοναδικού κλειδιού (Master Key) που θα χρησιμοποιηθεί στην κρυπτογράφηση με TKIP ή CCMP. Το master key προκύπτει από την ανάμειξη τριών στοιχείων: των δύο τυχαίων τιμών που δημιουργήθηκαν στα μηνύματα hello και μιας τρίτης τυχαίας τιμής που δημιουργεί ο client γνωστή ως Pre-Master Key. Το pre-master key είναι απαραίτητο γιατί τα αρχικά μηνύματα του EAP-TLS αποστέλλονται χωρίς κρυπτογράφηση και είναι γνωστά σε όποιον παρακολουθεί την συνεδρία.
Επίσης, ο client γνωρίζει το δημόσιο κλειδί του server μέσω του πιστοποιητικού του. Το περιεχόμενο του client key exchange είναι το pre-master key κρυπτογραφημένο με το δημόσιο κλειδί του server. Ο server από την μεριά του αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί και έτσι το pre-master key είναι πλέον γνωστό και στις δύο πλευρές με κάθε ασφάλεια.
Με το επόμενο μήνυμα, το certificate verify, ο client καλείται να αποδείξει ότι είναι ο νόμιμος κάτοχος του πιστοποιητικού που έστειλε στο μήνυμα certificate. Με άλλα λόγια, ο client πρέπει να αποδείξει ότι όχι μόνο έχει στην κατοχή του το πιστοποιητικό αλλά έχει και το αντίστοιχο ιδιωτικό κλειδί. Για να γίνει αυτό ο client δημιουργεί μια ψηφιακή περίληψη όλων των μέχρι τώρα μηνυμάτων που έχουν ανταλλαγεί, δηλαδή ένα hash. Στην συνέχεια, υπογράφει ψηφιακά το hash, με τον τρόπο που έχει περιγραφεί παραπάνω και το στέλνει στον server. Ο server, που έχει πάρει ήδη το πιστοποιητικό με το δημόσιο κλειδί, ελέγχει την εγκυρότητα της υπογραφής αλλά και το hash. Αν ένας από τους δύο ελέγχους αποτύχει, η συνεδρία διακόπτεται με EAP failure.
Εάν η πιστοποίηση είναι επιτυχής, αυτό που μένει είναι η δημιουργία του master key και η εκκίνηση της διαδικασίας κρυπτογράφησης (μήνυμα change cipher spec). Η διαδικασία του handshake ολοκληρώνεται με το μήνυμα EAP success που πληροφορεί τον client για την επιτυχή είσοδό του στο δίκτυο.

2.14.4 Πιστοποίηση με Protected EAP

Όλα τα μηνύματα του EAP όπως τα identity request, success, failure κτλ. στέλνονται ως καθαρό κείμενο και κάποιος που παρακολουθεί την συνεδρία μπορεί να τα συλλέξει χρήσιμες πληροφορίες όπως η ταυτότητα του client, το πρωτόκολλο που θα χρησιμοποιηθεί για την πιστοποίηση και τον τύπο των πιστοποιητικών.
Στόχος του Protected EAP (PEAP) είναι όλη η διαδικασία πιστοποίησης να γίνεται με ένα τρόπο στεγανό. Η λύση είναι η δημιουργία ενός ασφαλούς "τούνελ" που μέσω αυτού θα πραγματοποιείται η επικοινωνία μεταξύ client – server. Αυτό μπορεί να επιτευχθεί μέσω της κρυπτογράφησης των μηνυμάτων του EAP, αλλά αυτά τα ίδια μηνύματα έχουν σαν στόχο, εκτός των άλλων, την παραγωγή των κλειδιών της κρυπτογράφησης.
Το PEAP δεν είναι ένα ανεξάρτητο πρωτόκολλο πιστοποίησης ανωτέρου στρώματος αλλά ένα πλαίσιο μέσα στο οποίο φιλοξενούνται τα διάφορα πρωτόκολλα. Η πιστοποίηση μέσω PEAP είναι μια διαδικασία δύο φάσεων.

Στην πρώτη φάση, γίνεται η πιστοποίηση μόνο της πλευράς του server και παράγονται τα κλειδιά της κρυπτογράφησης. Μετά την έναρξη της λειτουργίας της κρυπτογράφησης, έχει δημιουργηθεί το ασφαλές τούνελ στην επικοινωνία client – server και μπορεί να περάσει στην δεύτερη φάση, την φάση της πιστοποίησης του χρήστη.
Κατά την πρώτη φάση λειτουργίας του PEAP, χρησιμοποιείται πάντα το πρωτόκολλο EAP-TLS. Οι αλλαγές σε σχέση με την κανονική λειτουργία που έχει περιγραφεί παραπάνω έχουν γίνει για την απόκρυψη των στοιχείων του χρήστη:

- Ο χρήστης δεν υποχρεούται να αποκαλύψει την ταυτότητά του και στα μηνύματα EAP identity request μπορεί να απαντήσει με ένα όνομα του τύπου peap@anonymous.com.
- Δεν γίνεται πιστοποίηση του χρήστη, οπότε η απάντηση στο μήνυμα certificate request του server είναι κενά μηνύματα του τύπου EAP response.
- Με το τέλος της TLS συνεδρίας δεν υπάρχει EAP success / failure αλλά εκκινεί μια νέα συνεδρία EAP.

Το πρωτόκολλο πιστοποίησης που θα χρησιμοποιηθεί κατά την φάση της πιστοποίησης του χρήστη μπορεί να είναι και πάλι το TLS ή και οποιοδήποτε άλλο. Τα πρότυπα WPA/WPA2 προβλέπουν την χρήση του PEAP με MS-CHAPv2 και EAP-GTC. Στο πειραματικό μέρος της εργασίας έχει χρησιμοποιηθεί το πρώτο.

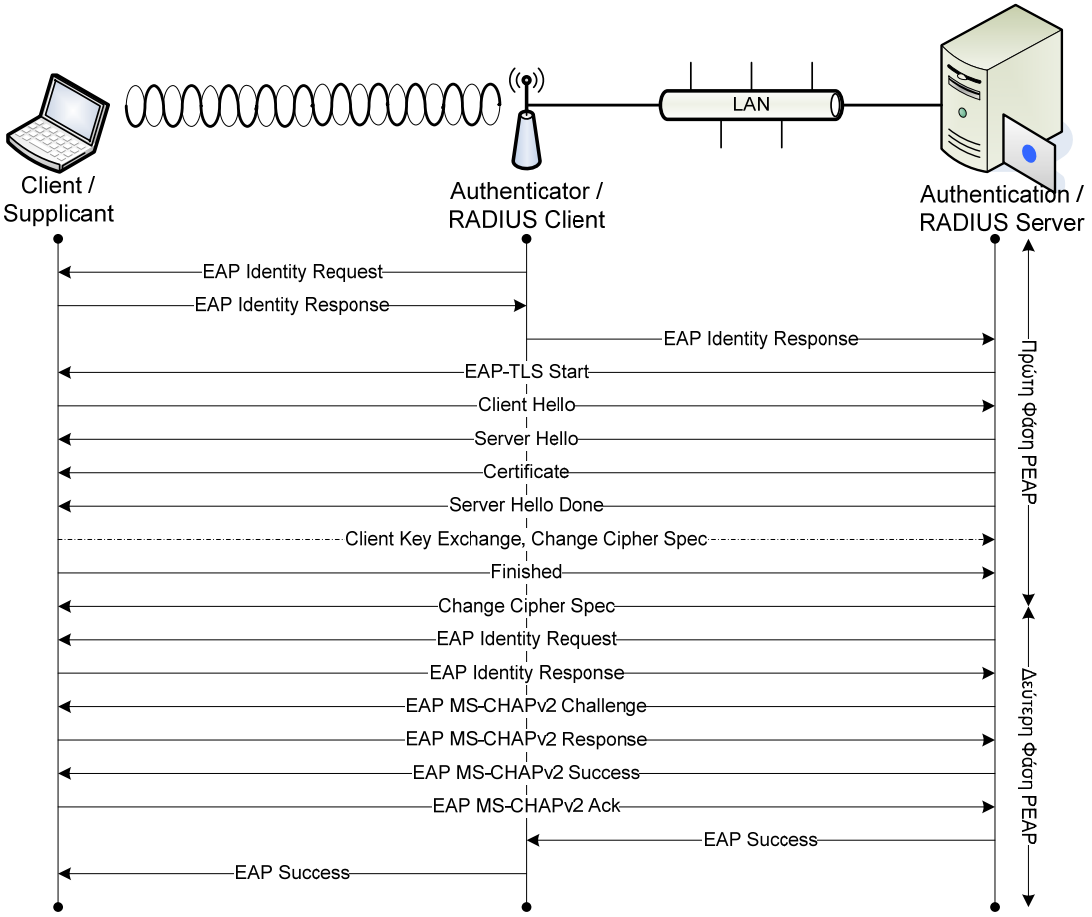
2.14.5 PEAP MS-CHAPv2

Το Microsoft Challenge Authentication Protocol στην δεύτερή του έκδοση είναι ένα πρωτόκολλο αμοιβαίας πιστοποίησης client – server μέσω μιας διαδικασίας κρυπτογράφησης μηνυμάτων και χρησιμοποιεί τους αλγόριθμους Message Digest 4 και DES. Η πιστοποίηση του χρήστη δεν γίνεται μέσω ψηφιακών πιστοποιητικών αλλά μέσω του password του κάθε χρήστη. Το password του MS-CHAPv2 μπορεί να είναι ίδιο με αυτό για την είσοδο του χρήστη στο εταιρικό domain και έτσι διευκολύνεται πολύ η διαδικασία. Όπως και οι περισσότερες τεχνολογίες που χρησιμοποιούνται στα ασύρματα δίκτυα, το MS-CHAPv2 αρχικά αναπτύχθηκε για χρήση με συνδέσεις PPP.
Αναλυτικά, το handshake της πιστοποίησης με την χρήση PEAP MS-CHAPv2 έχει ως εξής:

Φάση 1η: Δημιουργία TLS τούνελ

- Μετά την σύνδεση του client, το AP του στέλνει ένα μήνυμα Identity Request.
- Ο client ανταποκρίνεται με ένα μήνυμα Identity Response με ανώνυμο περιεχόμενο. Το μήνυμα προωθείται στον Authentication Server. Από το σημείο αυτό τα μηνύματα δεν αφορούν το AP.

- Εκκινεί η συνεδρία του EAP-TLS με το client να στέλνει τις απαραίτητες πληροφορίες για τα υποστηριζόμενα πιστοποιητικά.
- Απάντηση του server και αποστολή του πιστοποιητικού του.
- Δημιουργία των pre-master και master key της σύνδεσης.
- Εκκίνηση της λειτουργίας των αλγόριθμων κρυπτογράφησης και τέλος της πρώτης φάσης.



Σχήμα 2. 29

Φάση 2η (κρυπτογραφημένη): Πιστοποίηση με MS-CHAPv2

- Ο server απαιτεί την ταυτότητα του χρήστη (EAP Identity Request).
- Ο client απαντάει αυτή την φορά με το username ή το όνομα του Η/Υ ανάλογα με το ποιος πιστοποιείται.
- Ο server στέλνει ένα μήνυμα EAP MS-CHAPv2 Challenge που περιέχει μία τυχαία σειρά.
- Ο client απαντάει με ένα EAP MS-CHAPv2 Response που περιέχει την κρυπτογραφημένη σειρά του server αλλά και ένα challenge string για την πιστοποίηση του server.
- Ο server αποκρυπτογραφεί την απάντηση του client και αν το αποτέλεσμα είναι η αρχική σειρά στέλνει ένα μήνυμα EAP MS-CHAPv2 Success. Εκτός της ανακοίνωσης της πιστοποίησης του client περιέχει και το κρυπτογραφημένο challenge string του client.
- Ο client ελέγχει την απάντηση του server και αν είναι σωστή του απαντάει με ένα μήνυμα EAP MS-CHAPv2 Acknowledgement.

- Η επιτυχής πιστοποίηση και η είσοδος του χρήστη στο δίκτυο σφραγίζεται με την αποστολή ενός EAP Success από τον server στο AP και από το AP στον client.

Στο τέλος της διαδικασίας και τα δύο μέρη έχουν αποδείξει ότι γνωρίζουν το password του χρήστη οπότε και υπάρχει αμοιβαία πιστοποίηση.
Γενικά, η πιστοποίηση μέσω password θεωρείται λιγότερο ασφαλείς από αυτή που χρησιμοποιεί ψηφιακά πιστοποιητικά. Ειδικότερα, όπως και όλες οι διαδικασίες που περιλαμβάνουν εισαγωγή password από τους χρήστες, μπορεί να γίνει επίθεση είτε με λεξικό passwords[8], είτε επίθεση brute force[9].
Στην περίπτωση του PEAP MS-CHAPv2 δεν μπορεί να ισχύει κάτι τέτοιο για δύο λόγους. Στην πρώτη φάση, η ταυτότητα του server πιστοποιείται με ψηφιακό πιστοποιητικό. Στην δεύτερη φάση, αυτό του απασχολεί τον επιτιθέμενο δεν είναι τα passwords αλλά η κρυπτογράφηση.

2.15 Preshared Key

Οι μέθοδοι και τα πρωτόκολλα πιστοποίησης που αναλύθηκαν παραπάνω μπορούν να θεωρηθούν αξιόπιστα και πολύ ασφαλή. Το μόνο που χρειάζεται είναι ένα έτοιμο domain, μια Certification Authority, ένας RADIUS server, ένα ή και περισσότερα Access Point που να έχουν δυνατότητες RADIUS client και, φυσικά, ένα τμήμα IT για να ρυθμίζει και να διαχειρίζεται τα προηγούμενα.
Όλα τα παραπάνω πρέπει να θεωρηθούν, και είναι, αδιανόητα για τον οικιακό χρήστη αλλά και μικρές εταιρίες με περιορισμένες οικονομικές δυνατότητες.
Για την κρυπτογράφηση με TKIP ή CCMP το πρότυπο 802.11i προϋποθέτει την χορήγηση ενός κλειδιού από μια τρίτη οντότητα. Η τρίτη αυτή οντότητα δεν ορίζεται στο πρότυπο και αφήνεται, όπως έχει αναφερθεί, σε πρωτόκολλα ανωτέρου στρώματος. Σε καμία περίπτωση δεν αποκλείεται το αρχικό κλειδί να εισάγεται από τον χρήστη στο στρώμα εφαρμογής.
Η απ' ευθείας εισαγωγή του κλειδιού από τον χρήστη αποτελεί και την πλέον ανέξοδη λύση διαχείρισης των κλειδιών. Και εδώ τελειώνουν τα θετικά.
Η λύση των προεγκατεστημένων κλειδιών (Preshared Keys, PSK) κληρονομεί όλα τα διαχειριστικά προβλήματα του WEP. Τα PSK είναι γενικώς στατικά και είναι αδύνατο να αλλάξουν κεντρικά. Ο κάθε χρήστης θα πρέπει να ρυθμίσει το τερματικό του με το PSK, γι' αυτό και είναι γνωστό σε όλους τους συμμετέχοντες στο δίκτυο. Με το TKIP και το CCMP η αποκάλυψη του κλειδιού είναι αδύνατη με απλή συλλογή πακέτων. Αυτό που δεν είναι αδύνατο με την χρήση του PSK είναι η αποκάλυψη του κλειδιού σε περίπτωση κλοπής υλικού ή σε περίπτωση του κάποιος απολυμένος θελήσει να κάνει ζημιά στην εταιρία του.
Εάν το κλειδί παραμείνει μυστικό, ένα δίκτυο που χρησιμοποιεί WPA/WPA2 personal είναι ασφαλές και έχει όλα τα πλεονεκτήματα του RSN.

[8] Dictionary Attack: Έχουν δημιουργηθεί διάφορα λεξικά με πιθανά passwords και ο επιτιθέμενος τα δοκιμάζει με την σειρά. Σκοπός είναι να ελαχιστοποιηθεί ο χρόνος σε σχέση με την επίθεση brute force.
[9] Brute Force Attack: Χρησιμοποιείται όχι μόνο στα passwords αλλά και εναντίων κλειδιών κρυπτογράφησης. Κατά την επίθεση δοκιμάζονται όλοι οι πιθανοί συνδυασμοί. Σίγουρη μέθοδος αλλά μπορεί να διαρκέσει αιώνες.

2.16 Ασφάλεια και Απόδοση

Παρ' όλη την διείσδυσή τους στην αγορά των δικτύων και την ανάπτυξη νέων προτύπων, τα ασύρματα δίκτυα ακόμα χαρακτηρίζονται ανασφαλή από τον "ειδικό" τύπο. Ο λόγος, σε καμία περίπτωση, δεν είναι η ανεπάρκεια των νέων μηχανισμών ασφάλειας. Τα προβλήματα παρουσιάζονται σε περιπτώσεις που δεν είναι δυνατή η αλλαγή της εγκατεστημένης βάσης μηχανημάτων με νεότερα ή τουλάχιστον η αναβάθμισή τους.
Επίσης, όπως έχει ήδη περιγραφεί, τα προβλήματα στην απόδοση λόγω των μηχανισμών ασφαλείας θα πρέπει να αναμένονται σε μηχανήματα που έχουν αναβαθμιστεί για να υλοποιούν το TKIP. Σε νεότερα μηχανήματα που υλοποιούν το WPA2 δεν πρέπει αναμένεται υποβάθμιση της απόδοσης λόγω έλλειψης επεξεργαστικής ισχύος.

Κεφάλαιο 3
Πειραματικό Μέρος

Σκοπός του πειραματικού μέρους της εργασίας είναι η διερεύνηση της επίδρασης των μηχανισμών ασφαλείας που περιγράφτηκαν στα προηγούμενα κεφάλαια σε δίκτυα του τρέχοντος στάνταρ 801.11g των 54Mbps. Επίσης, εξετάστηκε η επίδρασή τους σε συνδυασμό με άλλους παράγοντες όπως το πρωτόκολλο του στρώματος μεταφοράς, το μήκος των δεδομένων ανά πακέτο (payload), το πλήθος των ασύρματων τερματικών, η επεξεργαστική ισχύς των Access Point καθώς και συνδυασμός των παραπάνω.

Οι μηχανισμοί ασφάλειας που εξετάστηκαν καλύπτουν το σύνολο των δημοσιευμένων ως τώρα προτύπων του IEEE και της WiFi Alliance.

1. Καμία ασφάλεια, κρυπτογράφηση ή πιστοποίηση. Χρησιμοποιείται ως μέτρηση αναφοράς.
2. Έλεγχος Πρόσβασης (Access Control). Χωρίς κρυπτογράφηση ή πιστοποίηση. Χρησιμοποιεί έλεγχο της MAC Address του χρήστη.
3. WEP με μήκος κοινού κλειδιού 40bit και Open πιστοποίηση.
4. WEP με μήκος κοινού κλειδιού 40bit και Shared πιστοποίηση.
5. WEP με μήκος κοινού κλειδιού 104bit και Open πιστοποίηση.
6. WEP με μήκος κοινού κλειδιού 104bit και Shared Key πιστοποίηση.
7. WPA-Personal με κρυπτογράφηση TKIP και πιστοποίηση Preshared Key (PSK).
8. WPA2-Personal με κρυπτογράφηση AES-CCMP και πιστοποίηση Preshared Key (PSK).
9. WPA-Enterprise κρυπτογράφηση TKIP και πιστοποίηση Protected EAP με χρήση RADIUS Server.
10. WPA2-Enterprise κρυπτογράφηση AES-CCMP και πιστοποίηση Protected EAP με χρήση RADIUS Server.

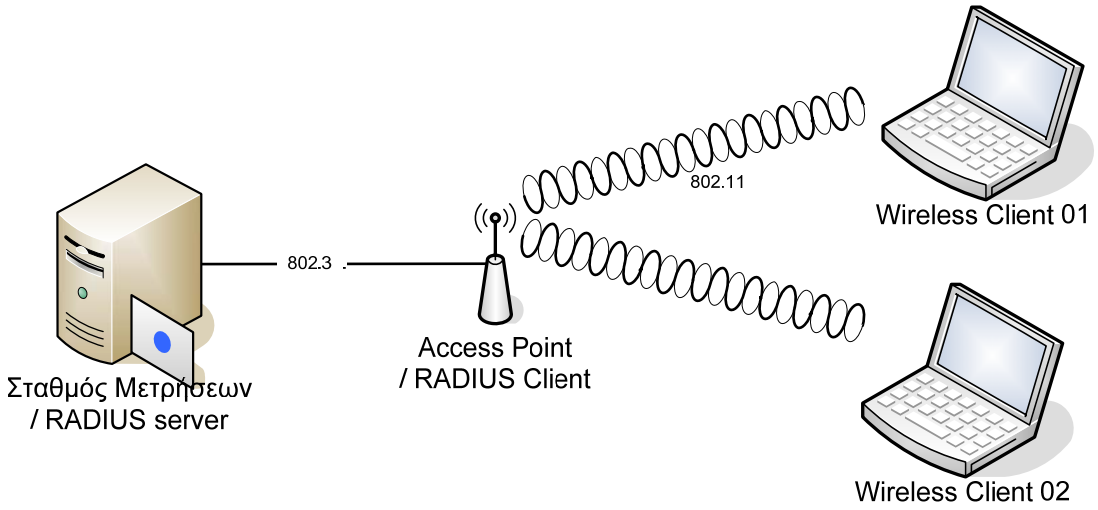
3.1 Το Υλικό

Για τις ανάγκες των μετρήσεων χρησιμοποιήθηκαν τρία Access Point διαφορετικών κατηγοριών και δυνατοτήτων.

1. Το WG602v3 της Netgear με επεξεργαστή τον IDT 32334 Communications Processor χρονισμένο στα 150MHz. Ανήκει στην κατηγορία Small Office/Home Office (SOHO) με κόστος μικρότερο των €100. Υποστηρίζει WPA-Personal και WPA2-Personal.

2. Το ProSafe FWG114Pv2 της Netgear με επεξεργαστή τον Brecis MSP2007 χρονισμένο 166MHz. Είναι ένα entry-level enterprise μοντέλο με κόστος γύρο στα €350. Υποστηρίζει όλα τα πρότυπα ασφάλειας.

3. Το WAG345G της Linksys. Είναι ένα από τα δημοφιλέστερα AP στην Ελλάδα αφού συμπεριλαμβάνεται στον εξοπλισμό ευζωνικής σύνδεσης μεγάλου ISP.

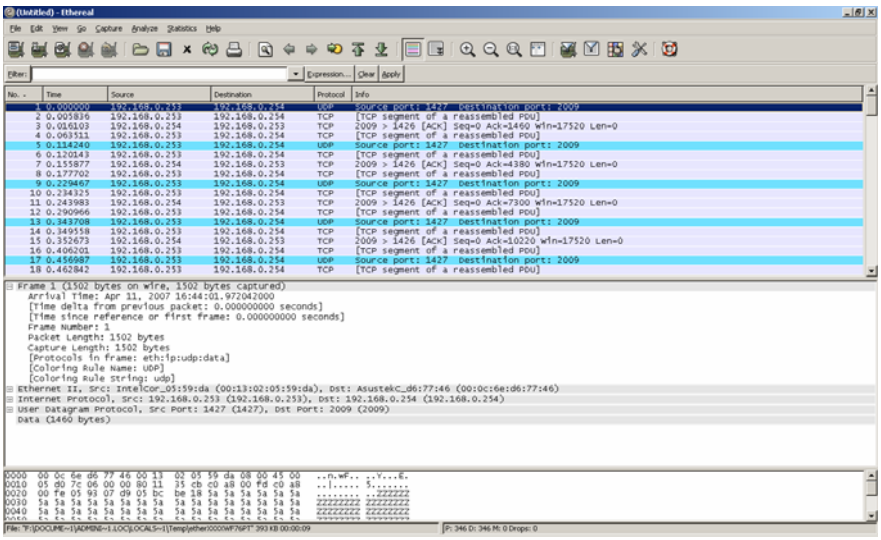


Σχήμα 3. 1

Η διάταξη των μετρήσεων συμπληρώνεται από τρεις ηλεκτρονικούς υπολογιστές. Ένα desktop (CPU Intel Pentium 4 χρονισμένο στα 3,4GHz, RAM 2GB και Gigabit Ethernet NIC της 3COM) με λειτουργικό Microsoft Windows 2003 Server Enterprise Edition ανέλαβε χρέη domain controller, DNS server, RADIUS server, Certification Authority και σταθμού μετρήσεων. Ο κυρίως ασύρματος client ήταν ένα VAIO VGN-FE11S της Sony (CPUs Intel Centrino Duo T2400 χρονισμένους στα 1,84GHz, RAM 1GB και NIC Intel PRO/Wireless 3945ABG). Για τις μετρήσεις με πολλαπλά ασύρματα τερματικά, χρησιμοποιήθηκε ένα laptop της ACER με παρόμοια χαρακτηρίστηκα.

3.2 Το Λογισμικό

Για την πραγματοποίηση του πειράματος χρειάστηκε ένα traffic generator για την παραγωγή των πακέτων και για τις μετρήσεις και ένα network protocol analyzer για την επαλήθευση των μετρήσεων και την παρακολούθηση της κίνησης του δικτύου. Χρησιμοποιήθηκαν τα προγράμματα LanTraffic V2 2.4 της ZTI και Ethereal Network Analyzer 0.99.0 ανοιχτού κώδικα.



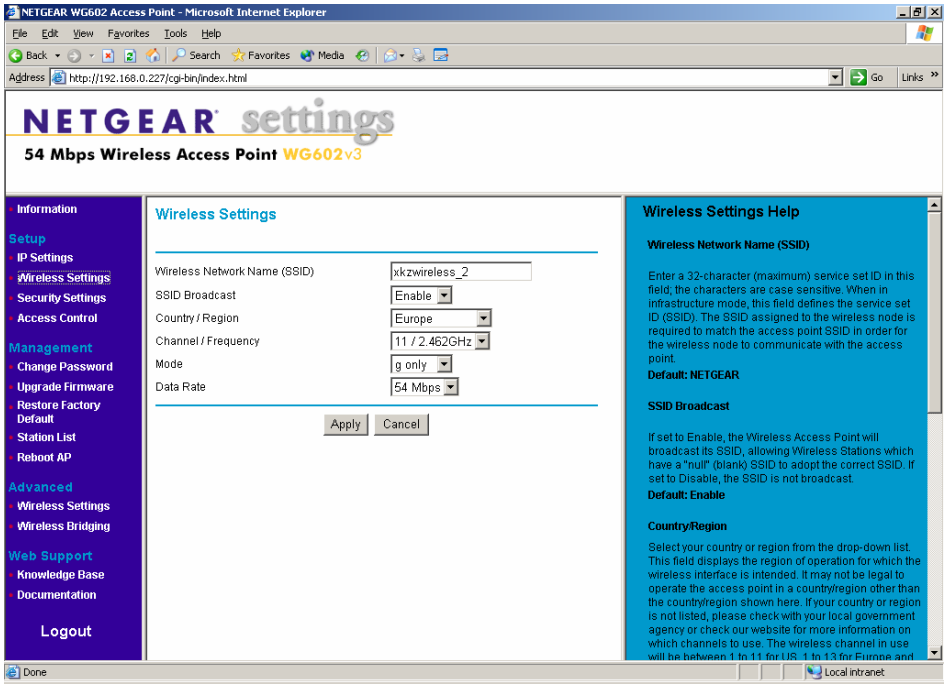
Σχήμα 3. 2

3.3 Ρυθμίσεις

3.3.1 Access Points και Wireless NICs

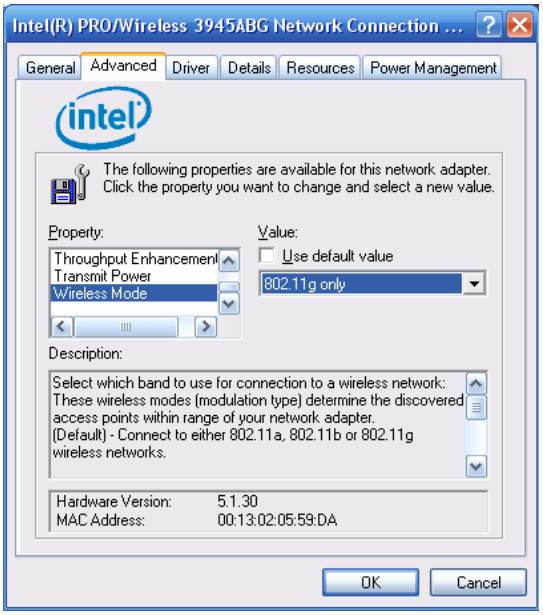
Οι ρυθμίσεις των AP που δεν αφορούν την ασφάλεια έγιναν με γνώμονα την μέγιστη απόδοση και ήταν κοινές σε όλα:

SSID Broadcast	Enable
Channel / Frequency	11 / 2.462MHz
Mode	802.11g only
Data Rate	54 Mbps
WMM Support	Disable
RTS Threshold	2347 bytes
Fragmentation Length	2346 bytes
Beacon Interval	100ms
DTIM Interval	1
Preamble Type	Short



Σχήμα 3. 3

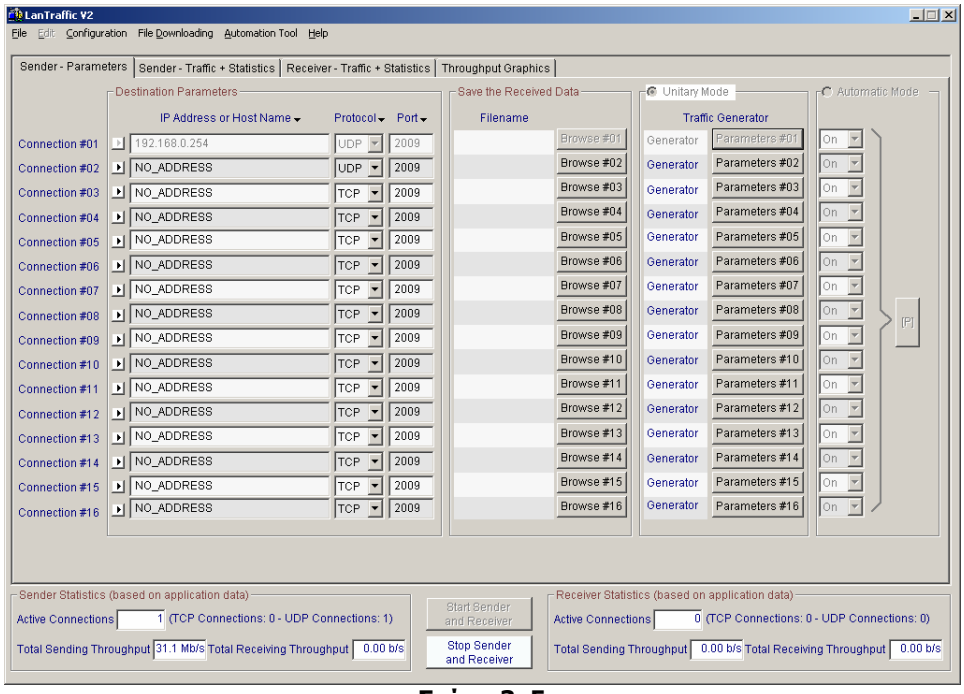
Αντίστοιχες ρυθμίσεις έγιναν και στους οδηγούς των καρτών δικτύου των τερματικών, όπου αυτό ήταν απαραίτητο.



Σχήμα 3. 4

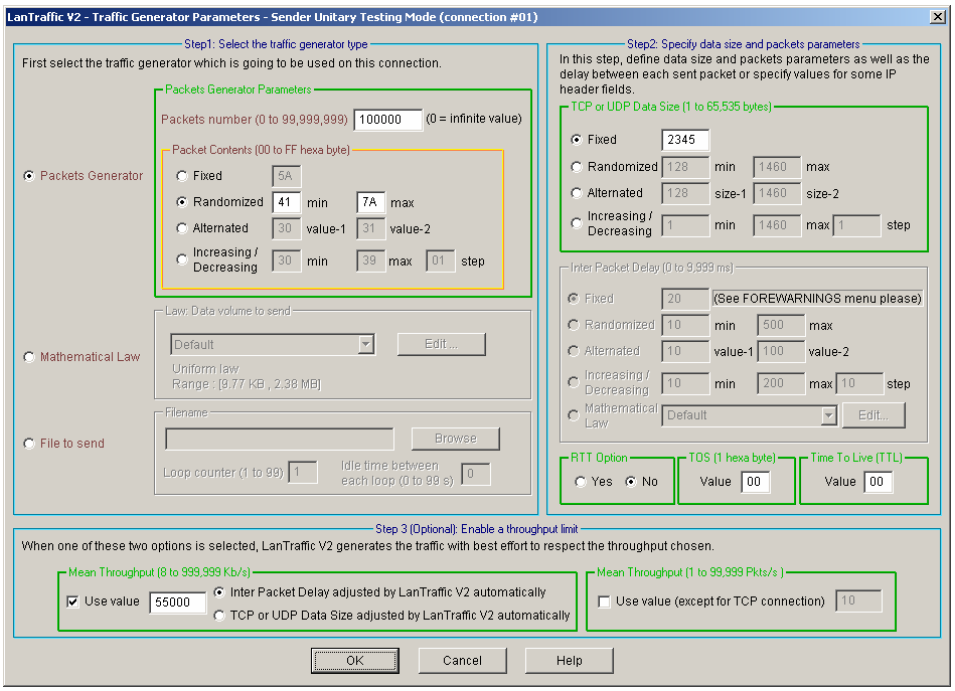
3.3.2 LanTraffic V2

Το κύριο εργαλείο των μετρήσεων ήταν η software γεννήτρια πακέτων IP LanTraffic στην δεύτερή της έκδοση. Το λογισμικό ήταν πλήρως λειτουργικό στην δοκιμαστική έκδοση 30 ημερών που υπήρχε διαθέσιμη.



Σχήμα 3. 5

Αρχικά, έπρεπε να ρυθμιστούν οι συνδέσεις μεταξύ του server και των ασύρματων τερματικών καθώς και ο τύπος του πρωτοκόλλου του στρώματος μεταφοράς (σχ. 3.5). Ανάλογα με τον τύπο των μετρήσεων επιλεγόταν UDP ή TCP.



Σχήμα 3. 6

Στην συνέχεια, γινόταν ρύθμιση των παραμέτρων της γεννήτριας. Ο αριθμός των προς αποστολή πακέτων εξαρτάτε από το μήκος του πακέτου και κυμάνθηκε μεταξύ 100.000 για πακέτα μεγαλύτερα από 1500bytes ως 600.000 για πακέτα μικρότερα από 500bytes.

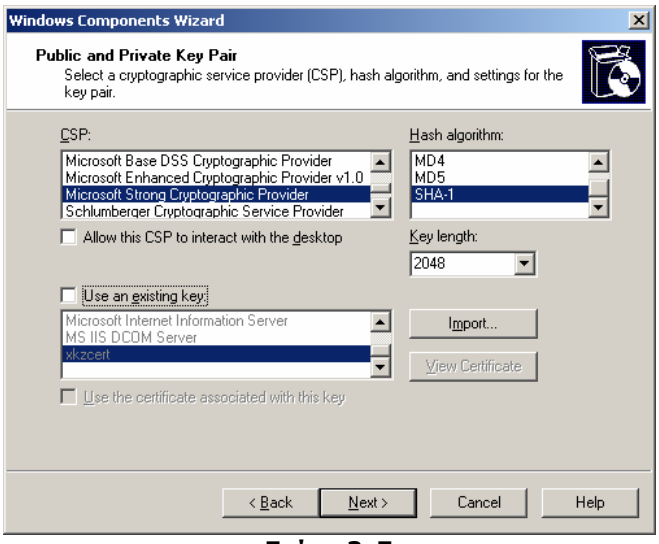
Τέλος, γινόταν ρύθμιση του ρυθμού αποστολής. Ο σκοπός της εργασίας είναι η συμπεριφορά των ασυρμάτων δικτύων στο όριο των δυνατοτήτων τους, οπότε ο ρυθμός ορίστηκε στα 55Mbps, δηλαδή αρκετά παραπάνω από το μέγιστο θεωρητικό όριο των 31Mbps.

3.4 Εγκατάσταση RADIUS server και Certification Authority

Για τις ανάγκες της μέτρησης απόδοσης του δικτύου με ασφάλεια WPA/WPA2 Enterprise χρειάστηκε η εγκατάσταση των αναγκαίων υπηρεσιών για την εξυπηρέτηση ενός εταιρικού δικτύου. Το λειτουργικό σύστημα που χρησιμοποιήθηκε είναι το Microsoft Windows 2003 Server στην Enterprise εκδοχή του.
Οι ρυθμίσεις και η εγκατάσταση του DNS server και του Active Directory Controller για την δημιουργία domain βρίσκονται εκτός του θέματος της εργασίας και θεωρούνται δεδομένα. Το Active Directory ήταν το local. xkzachos.net και υπήρχε ένα μέλος στους Computers (xkzlap.local. xkzachos.net) και ένας νέος λογαριασμός χρήστη. Στον Η/Υ που έγιναν οι μετρήσεις (localserver.local.xkzachos.net) χρησιμοποιήθηκε μόνο ο λογαριασμός του Administrator.
Στην περιγραφή των πρωτοκόλλων πιστοποίησης ανωτέρου στρώματος αναφέρθηκε η ανάγκη ύπαρξης μιας αρχής έκδοσης των ψηφιακών πιστοποιητικών (CA). Για την εγκατάσταση της CA ακολουθούνται τα παρακάτω βήματα:

Add or Remove Programs
↳Add/Remove Windows Components
↳Certificate Services
↳Enterprise root CA

Οι ρυθμίσεις για πάροχο υπηρεσιών κρυπτογράφησης, αλγόριθμο hash, μήκος κλειδιού και χρόνο ισχύος των πιστοποιητικών παρέμειναν οι αρχικές (σχ. 3.7).



Σχήμα 3. 7

Με το τέλος της εγκατάστασης δημιουργείται και το ψηφιακό πιστοποιητικό της CA. Στην περίπτωσή μας το xkzcert.crt.

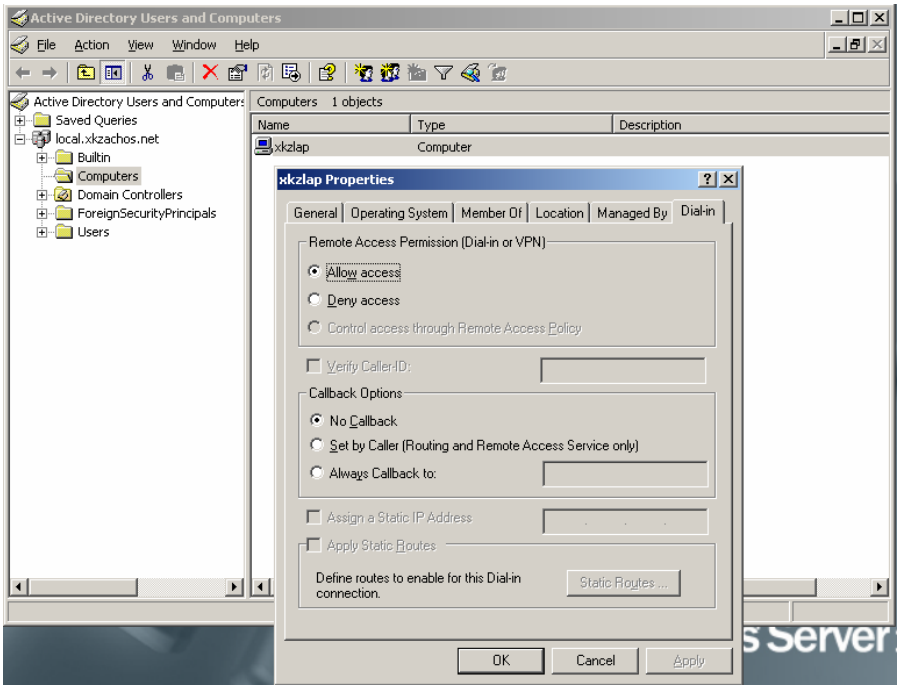
Για την λειτουργία του πρωτοκόλλου RADIUS σε περιβάλλον Windows Server πρέπει να εγκατασταθούν οι υπηρεσίες Internet Information Services και Internet Authentication Service. Όπως και προηγουμένως, η εγκατάσταση γίνεται από το Add/Remove Windows Components με τις παρακάτω επιλογές:

Application Server → Details
↳ Internet Information Services

Networking Services → Details
↳ Internet Authentication Service

Οι χρήστες και οι υπολογιστές που συμμετέχουν στο ασύρματο δίκτυο αντιμετωπίζονται από τον server ως απομακρυσμένοι και ως εκ τούτου θα πρέπει να τους δοθούν τα αντίστοιχα δικαιώματα:

Active Directory Users and Computers
↳ Computers → Client (xkzlap) → Properties
↳ Remote Access Permission
↳ Dial-in → Allow Access



Σχήμα 3. 8

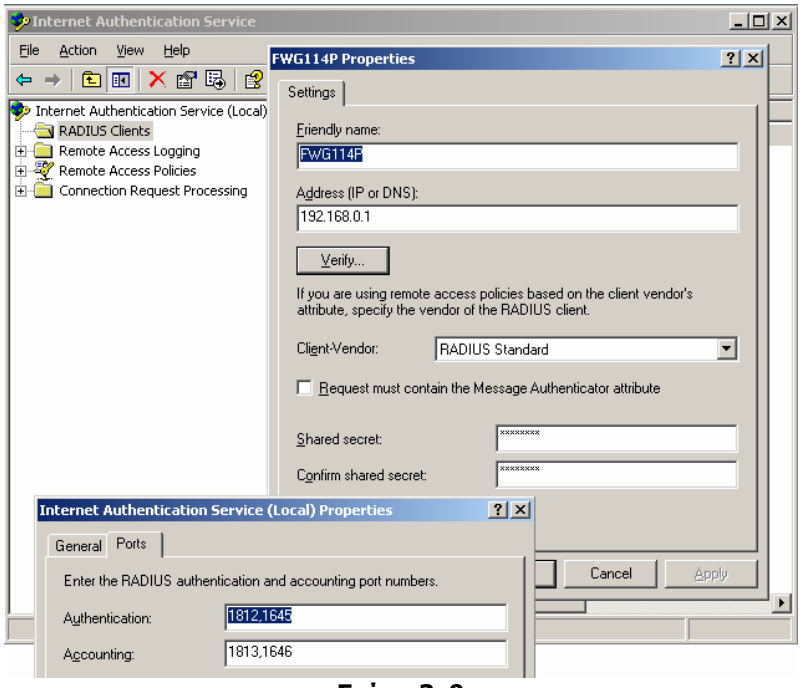
Η ίδια διαδικασία πρέπει να επαναληφθεί και για κάθε χρήστη του ασυρμάτου δικτύου.

Σ' αυτό το σημείο, καλό θα ήταν να δημιουργηθεί και ένα group με τους ασύρματους χρήστες για να γίνεται ομαδικά η εφαρμογή των πολιτικών ασφάλειας. Αρχικά δημιουργείται το group και στην συνέχεια προστίθενται οι χρήστες ως μέλη:

Built-in New → Group
↳ Group Name: (πχ.) WirelessUsers
↳ Group Scope: Global
↳ Group Type: Security

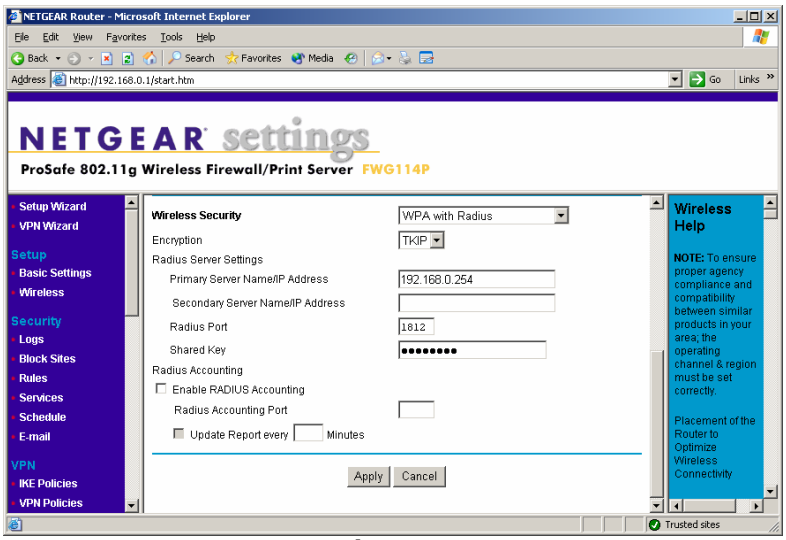
Στην υπηρεσία του RADIUS server IAS που εγκαταστάθηκε πρέπει να ρυθμιστούν οι RADIUS clients και η πολιτική απομακρυσμένης πρόσβασης. Όπως έχει ήδη αναφερθεί, RADIUS client είναι το Access Point. Στην πολιτική απομακρυσμένης πρόσβασης ρυθμίζεται ποιος έχει δικαίωμα χρήσης της υπηρεσίας, με ποιο τρόπο και ποια θα είναι η μέθοδος πιστοποίησης:

Internet Authentication Service
↳ RADIUS Client → New RADIUS Client
↳ Friendly Name: το όνομα του AP (FWG114P)
↳ Client IP: η διεύθυνση IP του AP (192.168.0.1)
↳ Client Vendor: RADIUS Standard
↳ Shared Secret: το κοινό κλειδί που χρησιμοποιείται στο Access-Challenge
↳ Authentication Port Number: 1812, 1645 (θύρες στρώματος μεταφοράς)
↳ Accounting Port Number: 1813, 1646
↳ Remote Access Policies
↳ Access Method: Wireless
↳ User or Group Access: WirelessUsers
↳ Authentication Methods: Protected EAP



Σχήμα 3. 9

Οι αντίστοιχες ρυθμίσεις με τον RADIUS server πρέπει να γίνουν και στο Access Point (σχ. 3.10), ώστε να είναι δυνατός ο έλεγχος της σύνδεσης.

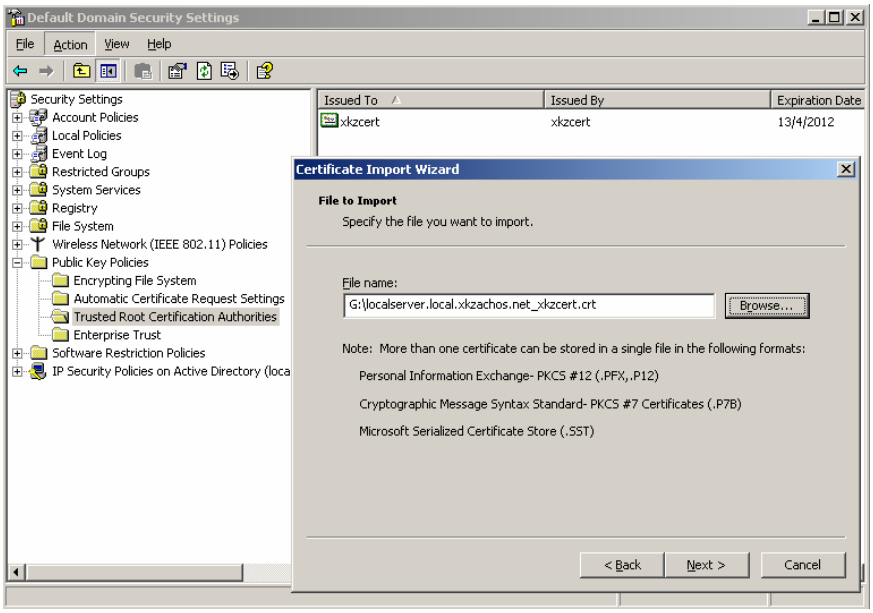


Σχήμα 3. 10

Με την επιβεβαίωση της σύνδεσης μεταξύ RADIUS server και AP, η εγκατάσταση και οι ρυθμίσεις της IAS έχουν ολοκληρωθεί. Βεβαίως, από την πλευρά του server εκκρεμούν οι ρυθμίσεις της έκδοσης και της απόδοσης των πιστοποιητικών.

Αρχικά, η CA που εγκαταστάθηκε στην αρχή θα πρέπει να γίνει μέλος αυτών που το δίκτυο μπορεί να εμπιστευτεί:

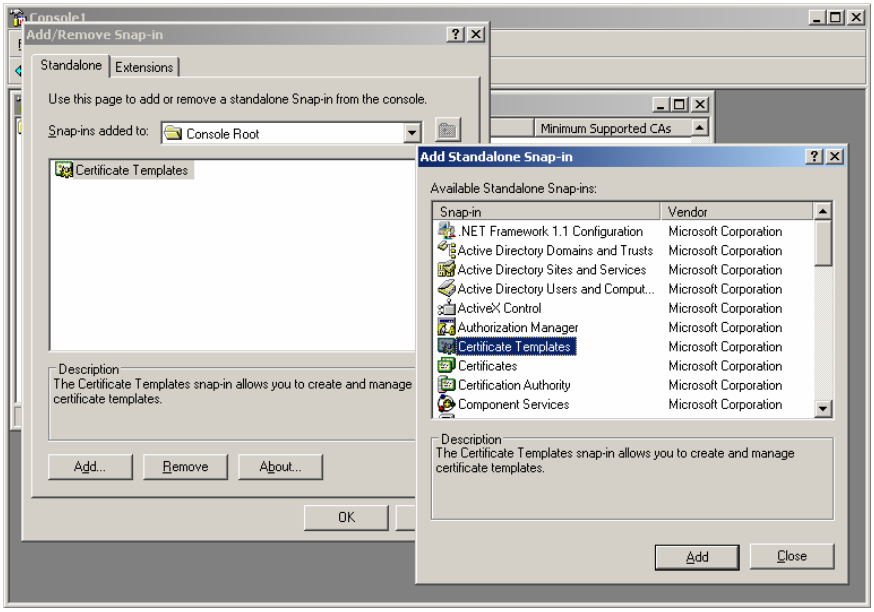
Default Domain Security Settings
↳ Public Key Policies
↳ Automatic Certificate Request
↳ Certificate Templates: localserver.local.xkzachos.net
↳ Trusted Root Certification Authorities
↳ Action → Import
↳ File name: localserver.local.xkzachos.net_xkzcert.crt



Σχήμα 3. 11

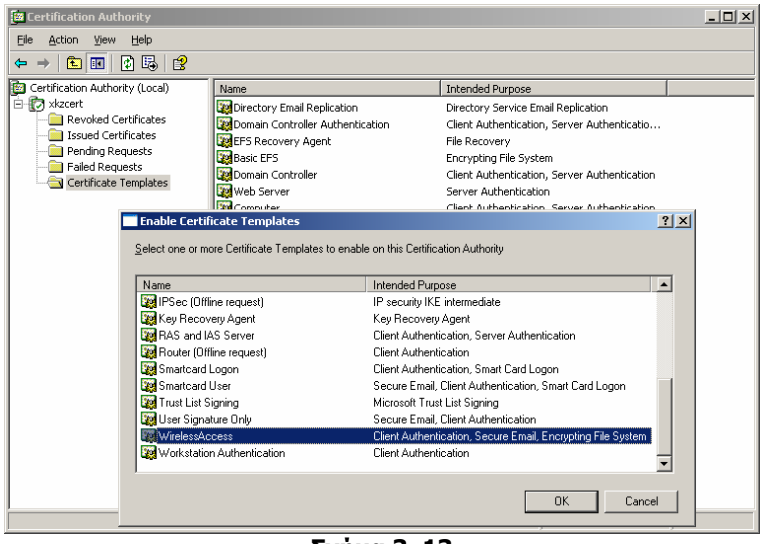
Στην συνέχεια πρέπει να δημιουργηθεί η φόρμα των πιστοποιητικών (template) και αυτή να αποδοθεί στη CA, ώστε η τελευταία να εκδίδει πιστοποιητικά:

Start → Run → mmc
↳ File → Add/Remove Snap-in
↳ Standalone → Certificate Templates → Add
↳ User → Duplicate Template
↳ Template Name: WirelessAccess (οποιοδήποτε όνομα)



Σχήμα 3. 12

Certification Authority
↳ Certificate Templates
↳ New → Certificate Template to Issue
↳ Enable Certificate Template → WirelessAccess



Σχήμα 3. 13

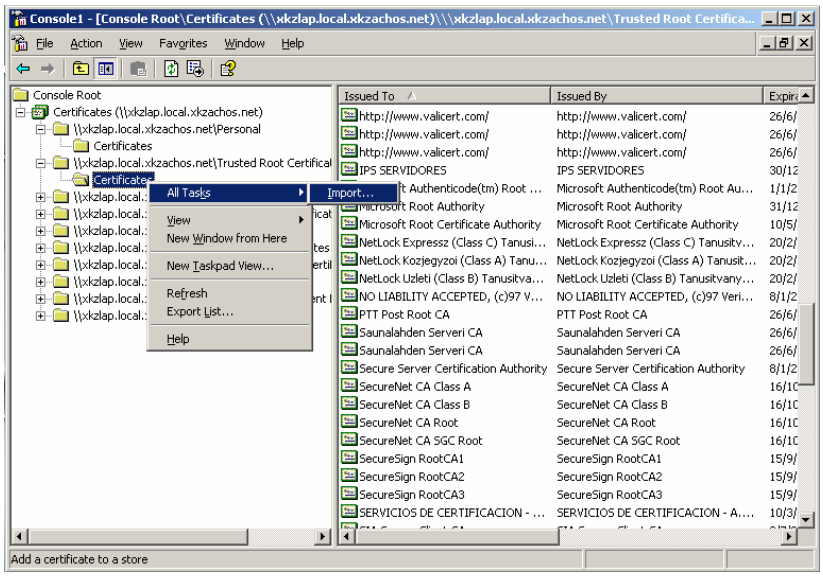
Από πλευράς server, έχουν τελειώσει όλες οι απαραίτητες ρυθμίσεις και μένουν μόνο οι ρυθμίσεις στα ασύρματα τερματικά. Και πάλι, οι ρυθμίσεις που

αφορούν την είσοδο του χρήστη στο domain είναι εκτός του θέματος της εργασίας και θεωρείται ότι έχουν γίνει και λειτουργούν. Οι ρυθμίσεις που απομένουν έχουν να κάνουν με την εγκατάσταση του πιστοποιητικού και την ασύρματη κάρτα δικτύου.

Θεωρητικά, για την εγκατάσταση του πιστοποιητικού αρκεί να υπάρχει το αρχείο του πιστοποιητικού στο τερματικό και η εγκατάσταση να γίνει αυτόματα μέσω οδηγού. Πρακτικά, η αυτόματη προσέγγιση δεν λειτούργησε (το πιστοποιητικό δεν εμφανιζόταν στην λίστα του σχ. χ.χ) και ακολουθήθηκε η παρακάτω διαδικασία:

Start → Run → mmc
↳ File → Add/Remove Snap-in
↳ Standalone → Certificates → Add
↳ Computer Account: Local Computer

Certificates
↳ Personal → All Tasks → Import → File name: xkzachos.crt
↳ Trusted Root Certificate Authority → All Tasks → Import → File name: xkzcert.crt

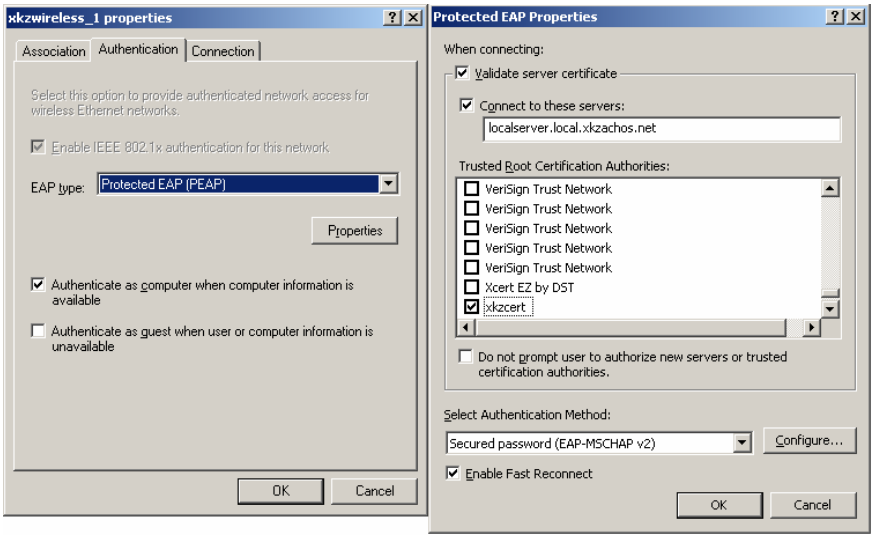


Σχήμα 3. 14

Τέλος, μένουν οι ρυθμίσεις της ασύρματης κάρτας δικτύου. Με το αρχικό πρόγραμμα διαχείρισης της ασύρματης σύνδεσης που χρησιμοποιήθηκε (Intel PROset Wireless), η σύνδεση δεν έγινε δυνατή και έτσι χρησιμοποιήθηκε το πρόγραμμα των Windows XP. Οι ρυθμίσεις που πρέπει να γίνουν στον οδηγό της κάρτας δικτύου είναι:

- SSID: το όνομα του SSID πχ. xkzwireless
- Network Authentication: WPA / WPA2
- Data Encryption: TKIP / AES
- ✓ The key is provided for me automatically (λειτουργία Enterprise)
- ✓ Enable IEEE 802.1x authentication for this network
- EAP Type: Protected EAP (PEAP)
- ✓ Validate server certificate

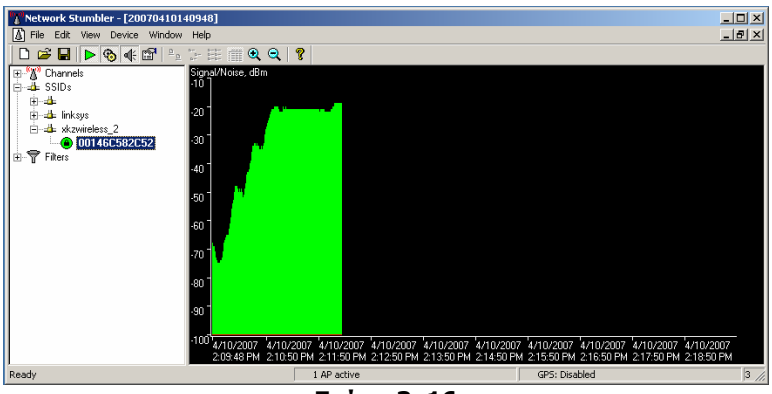
- ✓ Connect to these servers: localserver.local.xkzachos.net
- Trusted Root Certification Authorities: xkzcert
- Authentication Method: EAP-MSCHAP v2
- ✓ Automatically use my Windows logon name and password



Σχήμα 3. 15

3.5 Λήψη Μετρήσεων

Κύριος στόχος κατά την διάρκεια των μετρήσεων ήταν να αποκλειστεί κάθε υποβάθμιση της απόδοσης που οφείλεται στο φυσικό στρώμα. Ο χώρος που έγιναν οι μετρήσεις ήταν καθαρός από παρεμβολές άλλων συσκευών που λειτουργούν στα 2,4GHz όπως άλλα ασύρματα δίκτυα και φορητά τηλέφωνα. Για την αποκάλυψη άλλων ασυρμάτων δικτύων αλλά και την εύρεση της θέσης με την μέγιστη ισχύ του σήματος χρησιμοποιήθηκε το πρόγραμμα NetStumbler στην έκδοση 0.4.0 (σχ. 3.16).

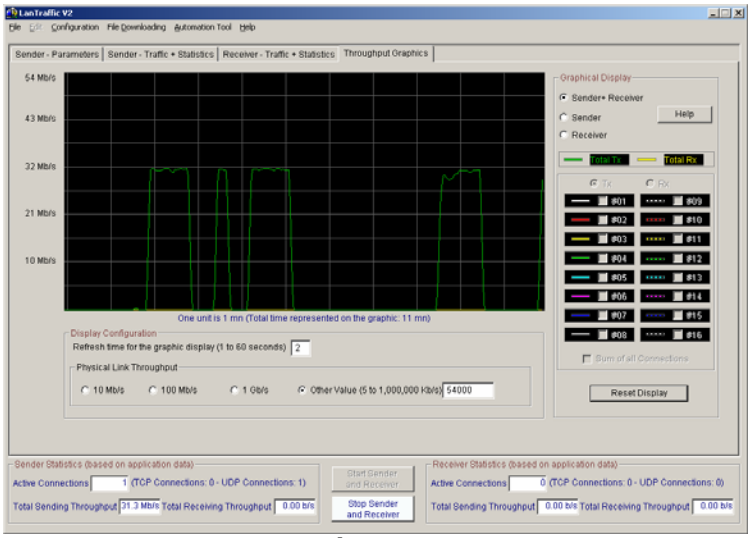


Σχήμα 3. 16

Για την αποφυγή αλλοίωσης των αποτελεσμάτων από άλλες εργασίες των Η/Υ έγινε σε όλους καθαρή εγκατάσταση λειτουργικού συστήματος και εγκατάσταση μόνο των απαραίτητων για την λήψη των μετρήσεων οδηγών

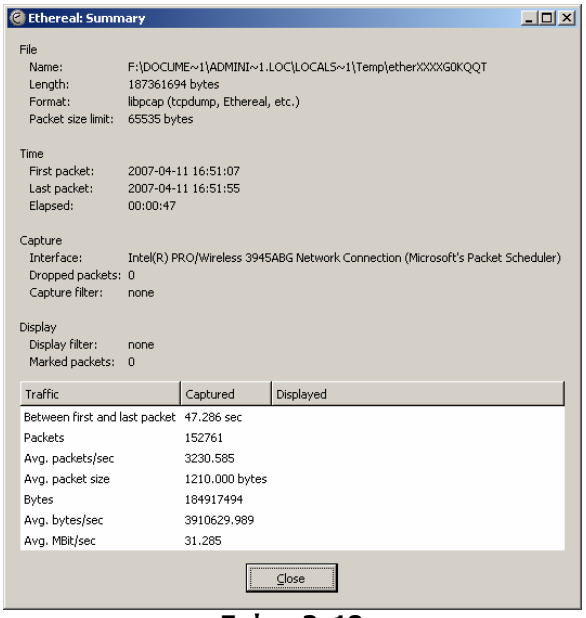
στις τελευταίες τους εκδόσεις. Επίσης, όπου αυτό ήταν δυνατό, έγινε και αναβάθμιση του firmware των συσκευών.
Πριν την λήψη κάθε ομάδας μετρήσεων γινόταν οι παρακάτω εργασίες και έλεγχοι:

- Ρύθμιση του Access Point
- Ρύθμιση των ασύρματων καρτών δικτύου των τερματικών
- Ρύθμιση του server (όπου χρειάστηκε)
- Έλεγχος συνδεσιμότητας μεταξύ των συσκευών του δικτύου
- Μέτρηση του σήματος λήψης των τερματικών
- Ρύθμιση και έλεγχος λειτουργίας του traffic generator



Σχήμα 3. 17

Κάθε μέτρηση επαναλαμβανόταν πέντε φορές και το πλήθος των πακέτων ρυθμιζόταν έτσι ώστε να μην διαρκεί κάτω από μισό λεπτό. Το τελευταίο κρίθηκε αναγκαίο γιατί το δίκτυο δεν απέδιδε τα μέγιστα ακαριαία. Κάθε μέτρηση ελεγχόταν και μετά (με το traffic analyzer, σχ. 3.17) και κατά την διάρκεια (οπτικά, σχ. 3.18) για μη αναμενόμενες πτώσης της απόδοσης, όπως πχ. από μεγάλο αριθμό σφαλμάτων. Σε τέτοιες περιπτώσεις, η μέτρηση επαναλαμβανόταν.

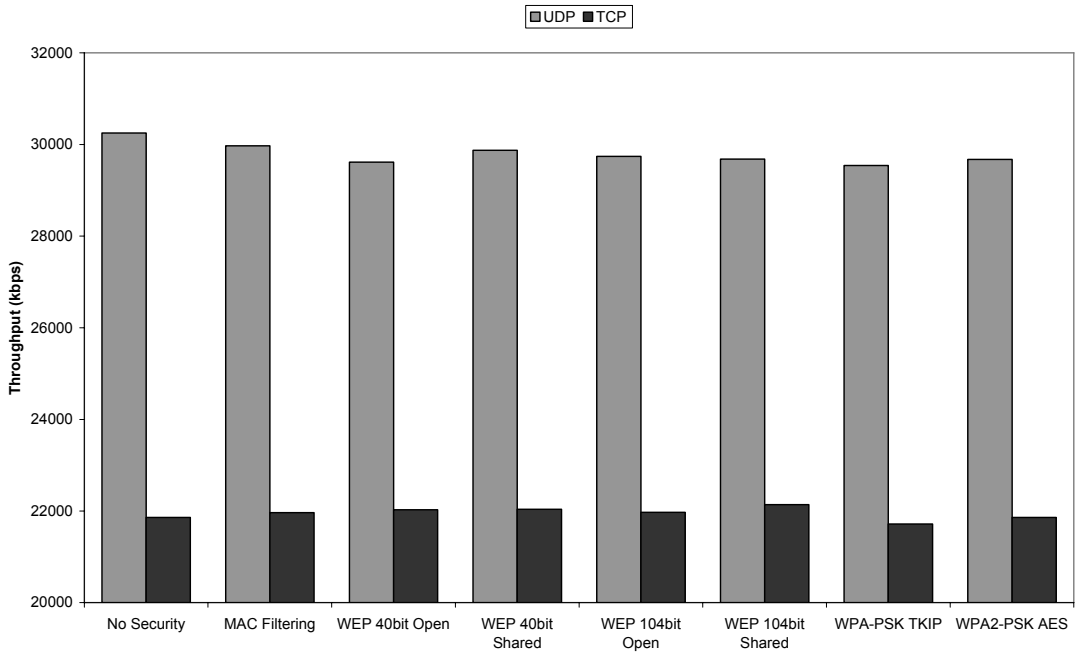


Σχήμα 3. 18

Στο τέλος κάθε ομάδας μετρήσεων, το αρχείο κειμένου καταγραφής των στιγμιαίων τιμών που δημιουργούσε το traffic generator εισάγονταν σε πρόγραμμα λογιστικών φύλλων για περεταίρω επεξεργασία. Από τα δεδομένα κάθε μέτρησης, η αρχικές και τελικές τιμές που δεν ανήκουν στην σταθερή κατάσταση της μετάδοσης απορρίπτονταν. Από τις υπόλοιπες τιμές, εξάγονταν ο μέσος όρος που είναι και η μέση τιμή του μέγιστου ρυθμού μεταφοράς κάθε τύπου μέτρησης.

3.6 Μετρήσεις με το Netgear WG602v3

Οι περισσότερες μετρήσεις έγιναν πάνω στο Access Point WG602v3. Το WG602v3 είναι ένα αντιπροσωπευτικό δείγμα σύγχρονου, χαμηλού κόστους AP για οικιακή χρήση ή χρήση σε μικρές επιχειρήσεις. Εκτός από τις διάφορες παραλλαγές του WEP, υποστηρίζει τα WPA και WPA2 στις εκδόσεις personal. Παρακάτω φαίνονται τα αποτελέσματα των μετρήσεων με ένα χρήστη και μήκος πακέτου 2.346 bytes.



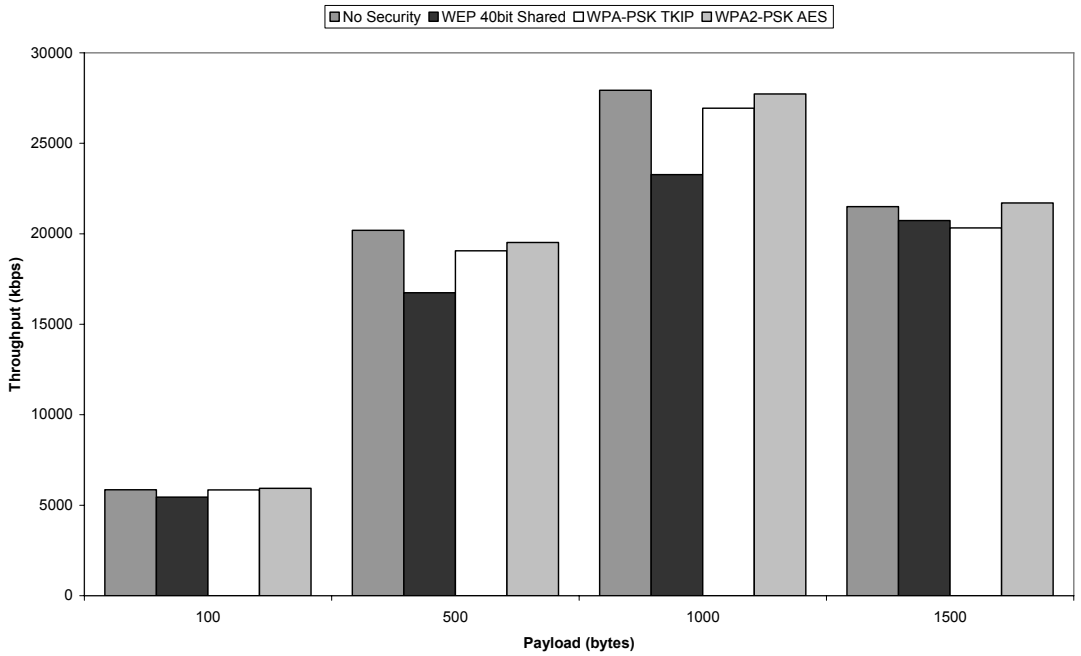
Γράφημα 1

Κρυπτογράφηση	Πιστοποίηση	Απόδοση (Kbps)		Διαφορά (%)	
		UDP	TCP	UDP	TCP
Καμία	Καμία	30.252,14	21.859,11	-	-
Καμία	MAC address	29.970,76	21.965,91	-0,93	0,4886
WEP 40bit	Open	29.613,99	22.027,22	-2,11	0,7691
WEP 40bit	Shared Key	29.873,99	22.037,68	-1,25	0,8169
WEP 104bit	Open	29.739,74	21.972,01	-1,69	0,5165
WEP 104bit	Shared Key	29.681,60	22.139,28	-1,89	1,2817
TKIP	Shared Key	29.543,33	21.714,84	-2,34	-0,6600
AES	Shared Key	29.675,17	21.858,86	-1,91	-0,0011

Η πρώτη παρατήρηση που μπορεί να γίνει πάνω στις μετρήσεις είναι ότι επαληθεύονται τα θεωρητικά μέγιστα των 30,5 και 24,4Mbps για τα πρωτόκολλα UDP και TCP αντίστοιχα. Η διαφορά στις μετρήσεις χωρίς την εφαρμογή κανενός είδους ασφάλειας είναι μόλις 0,81% από το θεωρητικό για πακέτα UDP. Για πακέτα TCP η διαφορά αυξάνεται στα 9,84%.
Μια άλλη σημαντική παρατήρηση είναι ότι η διαφορές στις μετρήσεις με την εφαρμογή των διαφόρων μεθόδων κρυπτογράφησης και πιστοποίησης είναι αμελητέες. Ένα συμπέρασμα που προκύπτει είναι μια μικρή επιβάρυνση στην απόδοση λόγω της εφαρμογής του TKIP που παρατηρήθηκε στην σύγκριση με τις στιγμιαίες τιμές της αρχικής μέτρησης. Σε όλες τις άλλες περιπτώσεις οι ελάχιστες διαφορές που παρατηρούνται μπορεί να είναι αποτέλεσμα αλλαγών στο φυσικό μέσο, θορύβου κτλ.

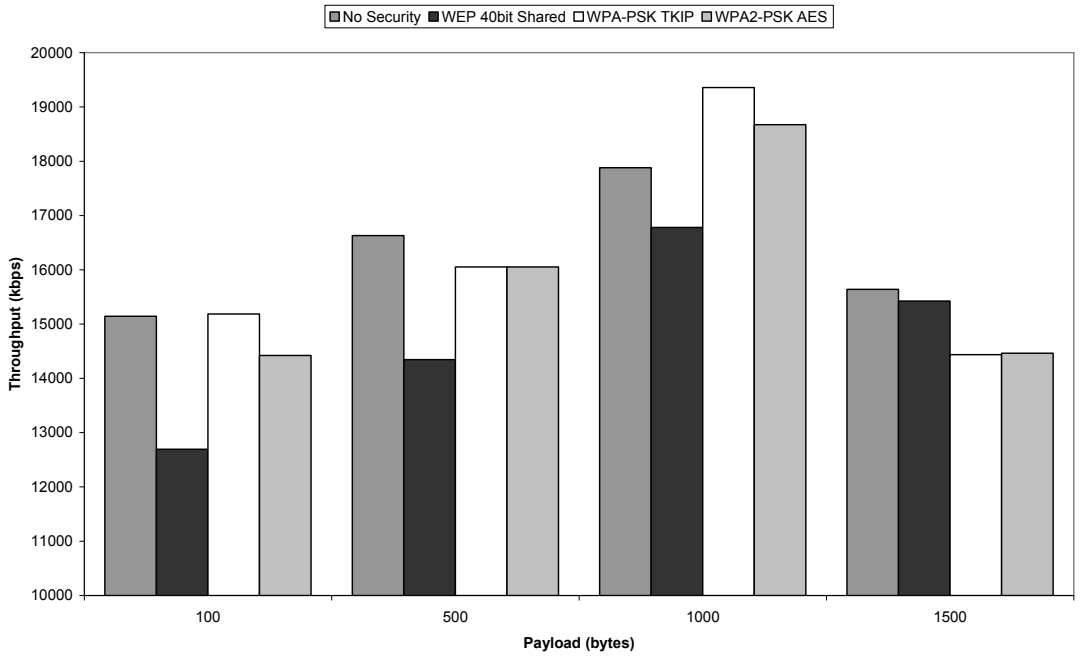
3.6.1 Μετρήσεις Μήκους Πακέτου

Με την επόμενη ομάδα μετρήσεων εξετάζεται η συμπεριφορά των κυριότερων μηχανισμών ασφάλειας σε σχέση με το μήκος των δεδομένων αποστολής.



Γράφημα 2

Ασφάλεια	Απόδοση (Kbps)							
	UDP				TCP			
	100	500	1000	1500	100	500	1000	1500
Καμία	5847,62	20193,1	27939,1	21507,8	15143,8	16629,8	17881,7	15638,8
WEP	5444,03	16742,1	23271,8	20734,3	12693,5	14345,1	16781,9	15425
WPA	5843,02	19057,6	26947	20330,1	15187,1	16052,5	19358,8	14438,2
WPA2	5934,67	19519,2	27724,8	21705,9	14421,7	16051,3	18672,2	14462,1



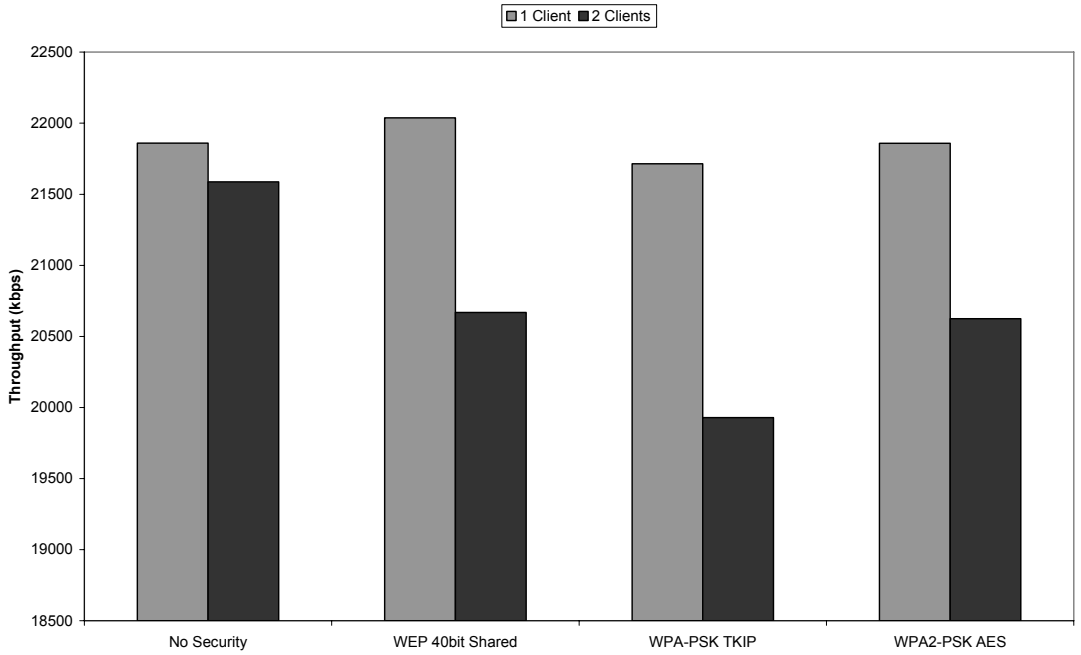
Γράφημα 3

Θεωρητικά, όσο μεγαλύτερο είναι το μήκος των δεδομένων τόσο καλύτερη η απόδοση του δικτύου. Αυτό συμβαίνει γιατί ο λόγος των χρήσιμων

πληροφοριών, δηλαδή τα δεδομένα του χρήστη, προς τις πληροφορίες της πλαισίωσης αυξάνεται σημαντικά. Βεβαίως, και σ' αυτό τον κανόνα υπάρχει ένα άνω όριο.
Η αύξηση των δεδομένων ενός πλαισίου (payload) δεν είναι πανάκεια. Σε ένα περιβάλλον που προκαλεί μεγάλο αριθμό σφαλμάτων είναι προτιμότερα πακέτα μικρού μήκους για μικρότερες απώλειες (βλ. δίκτυα ATM). Τα άνω όρια που ορίζονται από τα πρότυπα και είναι 1500bytes και 2346bytes για Ethernet και 802.11 αντίστοιχα. Δεδομένα μεγαλύτερα από αυτούς τους αριθμούς τεμαχίζονται πριν την αποστολή τους.

3.6.2 Μετρήσεις με Πολλαπλούς Χρήστες

Στο επόμενο πείραμα, προστέθηκε ένας ακόμα χρήστης στο δίκτυο και έγιναν μετρήσεις στους τρεις κυριότερους τρόπους ασφάλειας. Αυτή τη φορά, το traffic generator που είχε εγκατασταθεί στον σταθμό μετρήσεων προσπαθούσε να στείλει δεδομένα με ρυθμό 54Mbps και στους δύο χρήστες. Οι υπόλοιπες ρυθμίσεις παρέμειναν ως είχαν.



Γράφημα 4

Κρυπτογράφηση	Πιστοποίηση	Απόδοση (Kbps)		Διαφορά (%)	
		UDP	TCP	UDP	TCP
Καμία	Καμία	21.859,11	21.587,51	-	-
WEP 40bit	Shared Key	22.037,68	20.668,48	0,8169	-4,2572
TKIP	Shared Key	21.714,84	19.928,28	-0,6600	-7,6860
AES	Shared Key	21.858,86	20.624,31	-0,0011	-4,4618

Και σ' αυτή την περίπτωση, η μέγιστη υποβάθμιση της αρχικής απόδοσης του δικτύου παρατηρήθηκε στην εφαρμογή του TKIP.
Επίσης, εδώ φαίνεται και η μεγάλη επίδραση του πρωτοκόλλου του στρώματος μεταφοράς: Σε πακέτα UDP οι διαφορές παρέμειναν αμελητέες σε σύγκριση με την αποστολή χωρίς ασφάλεια. Αντίθετα, με πακέτα του

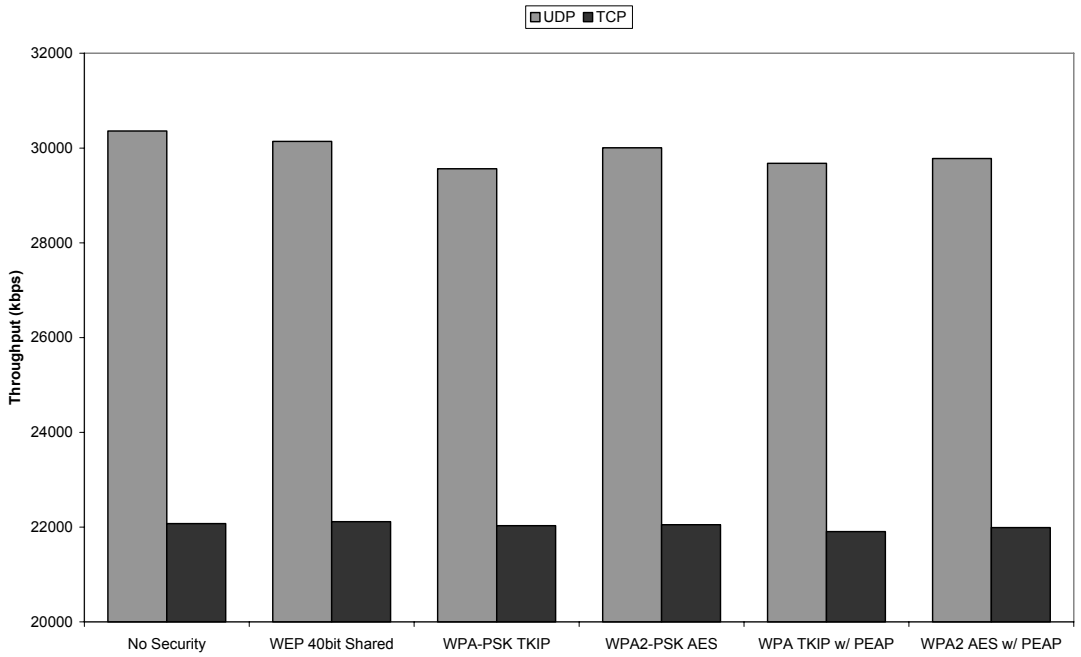
απαιτητικότερου TCP, το ποσοστό της πτώσης της ταχύτητας 7πλασιάστηκε σε σχέση με τις μετρήσεις με ένα χρήστη.

3.7 Μετρήσεις με το Netgear FWG114Pv2

Με τον διαχωρισμό των προτύπων ασφάλειας της WiFi Alliance σε personal και enterprise, ο ίδιος διαχωρισμός έγινε και από τους κατασκευαστές στα Access Points.
Ένα AP για να πιστοποιηθεί από την WiFi ως WPA2 enterprise ready χρειάζεται να υποστηρίζει τουλάχιστον τρεις παραμέτρους:

- Να υποστηρίζει κρυπτογράφηση AES.
- Να μπορεί να λειτουργεί Access Server.
- Να υποστηρίζει τουλάχιστον το EAP-TLS για πιστοποίηση.

Τα AP αυτής της κατηγορίας έχουν, συνήθως, πολύ περισσότερες λειτουργίες από τις παραπάνω, ισχυρούς επεξεργαστές και hardware, αλλά και αρκετά μεγάλο κόστος που κυμαίνεται μεταξύ 300 και 2000 ευρώ.
Το FWG114Pv2 ανήκει στο κάτω άκρο από άποψη κόστους και χρησιμοποιήθηκε στην εργασία με σκοπό την μέτρηση της επίδρασης των πρωτοκόλλων πιστοποίησης ανωτέρου στρώματος στην απόδοση αλλά και την πιθανή αύξηση, γενικά, της απόδοσης λόγω καλύτερου υλικού.



Γράφημα 5

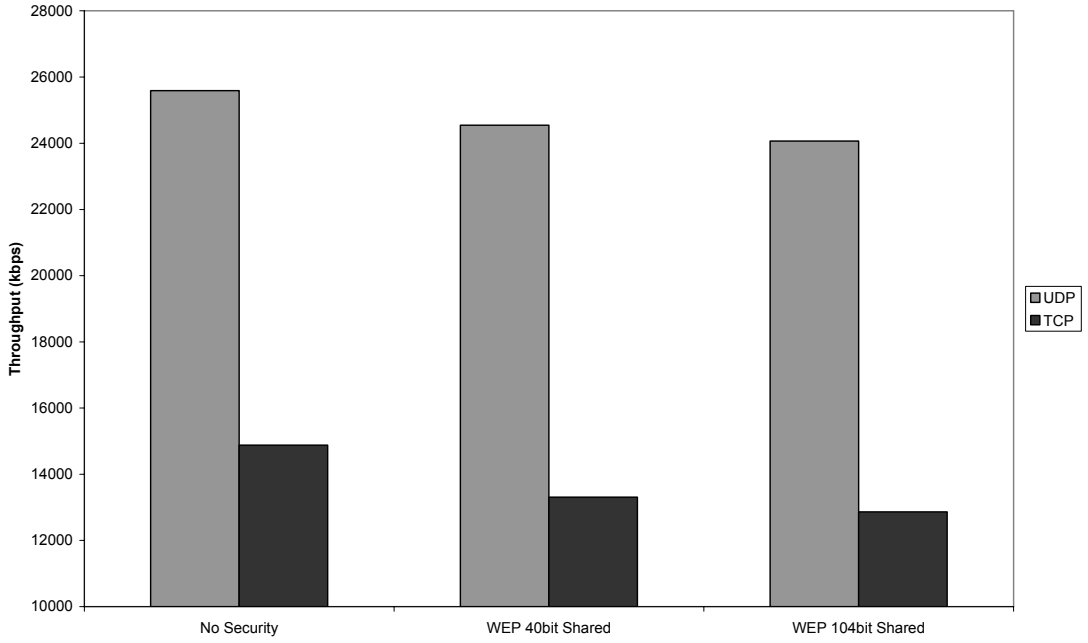
Κρυπτογράφηση	Πιστοποίηση	Απόδοση (Kbps)		Διαφορά (%)	
		UDP	TCP	UDP	TCP
Καμία	Καμία	30.360,69	22.074,20	-	-
WEP 40bit	Shared Key	30.139,54	22.114,79	-0,7284	0,1839
TKIP	Shared Key	29.563,75	22.031,85	-2,6249	-0,1918
AES	Shared Key	30.004,96	22.049,45	-1,1717	-0,1121

TKIP	802.1x/PEAP	29.676,59	21.907,04	-2,2532	-0,7572
AES	802.1x/PEAP	29.780,22	21.990,96	-1,9119	-0,3771

Όπως ήταν αναμενόμενο δεν υπάρχει κάποια επίπτωση στην απόδοση του δικτύου λόγω της πιστοποίησης Protected EAP. Η πιστοποίηση είναι μια λειτουργία που γίνεται κατά την είσοδο του χρήστη στο δίκτυο και δεν εμπλέκεται στην μετάδοση. Το μόνο που μπορεί να διακόψει την ομαλή ροή δεδομένων είναι η ανανέωση των temporal keys αλλά και αυτό συμβαίνει σε τακτά αλλά σπάνια διαστήματα.
Όπως και στις μετρήσεις με το WG602v3, η μεγαλύτερη πτώση της απόδοσης εμφανίστηκε με την χρήση του TKIP και μάλιστα μεγαλύτερη με πιστοποίηση PSK (-2,62%) και όχι PEAP (-2,25%).
Τέλος, αν και οι επιδόσεις του FWG114Pv2 ήταν παντού καλύτερες, μια αύξηση της τάξης του 0,36% σε UDP και 1% σε TCP δεν μπορεί από μόνη της να δικαιολογήσει το 4πλάσιο κόστος.

3.8 Μετρήσεις με το Linksys WAG345G

Το WAG345G είναι ένα από τα AP που υποστηρίζει την ταχύτητα του 802.11g αλλά όχι το WPA. Εάν ήταν δυνατή η αναβάθμιση του firmware ώστε να είναι δυνατή η εφαρμογή κρυπτογράφησης TKIP, θα έδινε την δυνατότητα πειραματικής επιβεβαίωσης της μεγάλης υποβάθμισης που αναμένεται θεωρητικά. Δυστυχώς, η εταιρία κατασκευής δεν είχε εκδώσει μια τέτοια αναβάθμιση το χρονικό διάστημα διεξαγωγής των πειραμάτων.



Γράφημα 6

Κρυπτογράφηση	Πιστοποίηση	Απόδοση (Kbps)		Διαφορά (%)	
		UDP	TCP	UDP	TCP
Καμία	Καμία	25.588,43	14.879,25	-	-
WEP 40bit	Shared Key	24.544,90	13.310,80	-4,0781	-10,5412
WEP 104bit	Shared Key	24.065,04	12.862,79	-5,9534	-13,5522

Κατά την λήψη των μετρήσεων παρατηρήθηκε πολύ μεγάλος αριθμός σφαλμάτων και αυτό φαίνεται και στις μέσες τιμές του πίνακα. Πρέπει να σημειωθεί ότι ο ρυθμός των σφαλμάτων ήταν σταθερός και έχει αποκλειστεί οποιοσδήποτε άλλος λόγος δημιουργίας τους εκτός του ίδιου του AP[10].
Παρ' όλα αυτά, στις μετρήσεις μπορεί να παρατηρηθεί καθαρά η πτώση στην απόδοση λόγω της επιβάρυνσης της κεντρικής μονάδας επεξεργασίας του AP από την κρυπτογράφηση.

3.9 Συμπεράσματα

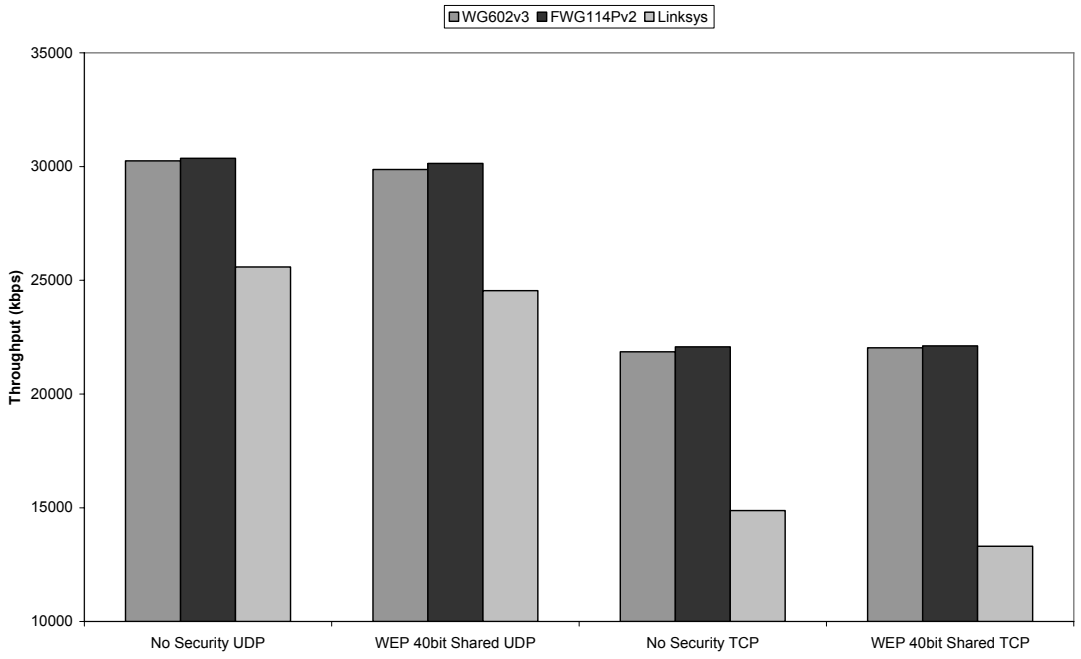
3.9.1 Επίδραση Μηχανισμών Ασφάλειας

Όπως αναφέρθηκε και κατά την παρουσίαση των αποτελεσμάτων των μετρήσεων, η πτώση της απόδοσης με την εφαρμογή κρυπτογράφησης και πιστοποίησης είναι αμελητέα. Με μέγιστη πτώση 2,63% και σε κάποιες μετρήσεις ακόμα και αύξηση μισής ποσοστιαίας μονάδας, το μόνο ασφαλές συμπέρασμα που μπορεί να εξαχθεί είναι ότι τα τελευταίας γενιάς AP δεν παρουσιάζουν κανένα πρόβλημα ακόμα και κατά την κρυπτο / αποκρυπτογράφηση με χρήση πολύ απαιτητικών από άποψη επεξεργαστικής ισχύος διεργασίες όπως το AES.
Το αντίθετο, τα δύο AP που υποστηρίζουν εγγενώς το 802.11i, δεν παρουσίασαν μέγιστη πτώση της απόδοσης κατά την εφαρμογή του WPA2 με κρυπτογράφηση AES αλλά στην εφαρμογή του θεωρητικά απλούστερου TKIP. Το παραπάνω μπορεί να αποδοθεί στην χρήση συνεπεξεργαστών αφιερωμένων στην κρυπτογράφηση του AES, ενώ στην περίπτωση του TKIP χρησιμοποιείται το WEP και τα υπόλοιπα στοιχεία του υλοποιούνται μέσω λογισμικού που επιβαρύνει τον κεντρικό επεξεργαστή.
Ευτυχώς ή δυστυχώς[11], στην παρούσα εργασία δεν παρατηρήθηκε θεαματική πτώση της απόδοσης της τάξης του 85,5% μόνο με την χρήση του WEP, όπως αναφέρεται σε παλαιότερες έρευνες. Με την έκδοση του 802.11i, την υιοθέτησή του από την WiFi Alliance και την ολοκλήρωσή του σε νέα μηχανήματα από τους κατασκευαστές, φαίνεται ότι η ασφάλεια των ασυρμάτων δικτύων δεν θα ξαναασχολήσει, τουλάχιστον όχι όσον αφορά την απόδοσή τους.

3.9.2 Επίδραση Υλικού

Στο παρακάτω γράφημα φαίνονται οι επιδόσεις των τριών Access Point που χρησιμοποιήθηκαν και στον πίνακα καταγράφονται οι διαφορές από τις μέγιστες θεωρητικές τιμές των 30,5Mbps και 24,4Mbps για UDP και TCP.

[10] Το AP είχε μόλις έρθει από το service της Linksys με την διαβεβαίωση ότι λειτουργεί άψογα. Οπότε, μπορεί να γίνει η υπόθεση ότι τα σφάλματα δεν οφείλονται σε βλάβη αλλά σε κακή υλοποίηση.
[11] Good news, no news. Πραγματικά μεγάλη πτώση της απόδοσης θα είχαμε αν στο Linksys, που δεν υποστηρίζει εξ αρχής το 802.11i, ήταν δυνατή η μεταπήδηση σε TKIP με αναβάθμιση του firmware. Τουλάχιστον μέχρι την διεξαγωγή των μετρήσεων αυτό δεν κατέστη δυνατό.



Γράφημα 7

Ασφάλεια / Πρωτόκολλο	WG602v3		FWG114v2		Linksys	
	Απόδοση	Διαφορά	Απόδοση	Διαφορά	Απόδοση	Διαφορά
Καμία / UDP	30.252,14	-0,81%	30.360,69	-0,46%	25.588,43	-16,11%
WEP / UDP	29.873,99	-2,05%	30.139,54	-1,18%	24.544,90	-19,52%
Καμία / TCP	21.859,11	-10,41%	22.074,20	-9,53%	14.879,25	-39,02%
WEP / TCP	22.037,68	-9,68%	22.114,79	-9,36%	13.310,80	-45,45%

Όπως φαίνεται από τις μετρήσεις, μια κακή υλοποίηση μπορεί να υποβαθμίσει την απόδοση του δικτύου ως και κατά 45% καθιστώντας αδύνατη την χρήση ισχυρών μηχανισμών ασφάλειας.
Ένας ρυθμός σφαλμάτων, όπως αυτός που παρατηρήθηκε στην λειτουργία του AP της Linksys, μπορεί να καταστήσει ένα ασύρματο δίκτυο πρακτικά άχρηστο. Ειδικά εάν το σενάριο μεταφερθεί σε πραγματικές συνθήκες χρήσης του δικτύου με αναπόφευκτη την υποβάθμιση του σήματος λόγω απόστασης, διάθλασης και θορύβου, και διαμοιρασμό του εύρους ζώνης στους χρήστες.

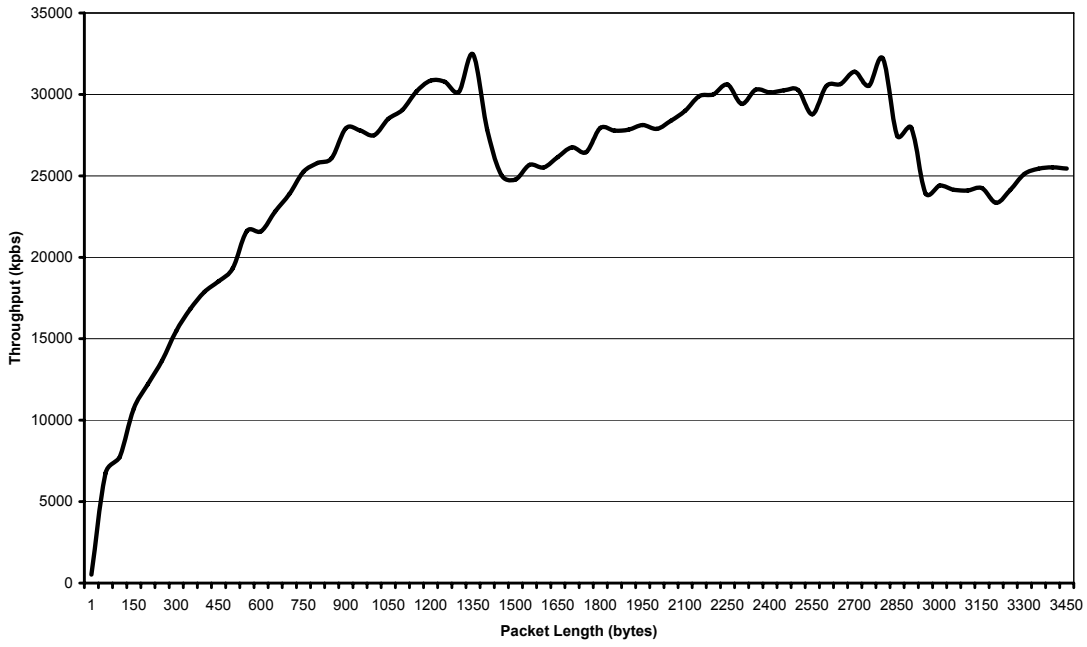
3.9.3 Επίδραση Αριθμού Χρηστών

Όπως ήταν αναμενόμενο, όσο αυξάνεται ο αριθμός των χρηστών τόσο μειώνεται η απόδοση του δικτύου.
Με βάση τα αποτελέσματα των μετρήσεων μπορούν να γίνουν δύο παρατηρήσεις. Η πρώτη είναι ότι το πρωτόκολλο UDP του στρώματος μεταφοράς φαίνεται περισσότερο ευάλωτο στην αύξηση του αριθμού των χρηστών από το TCP. Η δεύτερη παρατήρηση επιβεβαιώνει την ικανότητα των AP στην εφαρμογή των πρωτοκόλλων ασφαλείας ακόμα και με την επιβάρυνση περισσοτέρων τερματικών.

Ασφάλεια	Απόδοση (Kbps)				Διαφορά (%)	
	Ένας χρήστης		Δύο χρήστες			
	UDP	TCP	UDP	TCP	UDP	TCP
Καμία	30.252,14	21.859,11	21.859,11	21.587,51	-27,74	-1,243
WEP	29.873,99	22.037,68	22.037,68	20.668,48	-26,23	-6,213
WPA	29.543,33	21.714,84	21.714,84	19.928,28	-26,5	-8,227
WPA2	29.675,17	21.858,86	21.858,86	20.624,31	-26,34	-5,648

3.9.4 Επίδραση Μήκους Πακέτου

Στο σχήμα χ.χ φαίνεται το αποτέλεσμα των μετρήσεων χωρίς καμία ασφάλεια και με το μήκος του πακέτου να εκκινεί από 1 byte και να αυξάνεται κατά 50bytes σε κάθε ομάδα μετρήσεων.
Θεωρητικά, με την αύξηση του μήκους του πακέτου θα έπρεπε να υπάρχει αντίστοιχη αύξηση στην απόδοση του δικτύου. Ο λόγος είναι ότι με κάθε αύξηση της ωφέλιμης πληροφορίας στο πλαίσιο μειώνεται ο λόγος της πληροφορίας της πλαισίωσης προς την ωφέλιμη πληροφορία. Πρακτικά και όπως προέκυψε από τις μετρήσεις, η θεωρία ακολουθείται μέχρι τα 1500bytes περίπου που είναι το μέγιστο ωφέλιμο φορτίο του πρωτοκόλλου IP. Μετά από αυτό το όριο, υπάρχει πτώση της απόδοσης, προφανώς λόγω της διαδικασίας τεμαχισμού των δεδομένων που εισάγει αφ' ενός κάποια καθυστέρηση και αφ' εταίρου λόγω της ύπαρξης δύο πακέτων διαφορετικού μήκους. Πχ. αν ένα τεμάχιο πληροφορίας έχει μήκος 2000bytes στο στρώμα μεταφοράς, όταν περνάει στο στρώμα δικτύου τεμαχίζεται σε δύο πακέτα: ένα των 1500bytes και ένα των 500bytes.



Γράφημα 8

Το παραπάνω μπορεί να εξηγεί και την ανακολουθία που εμφανίστηκε στις μετρήσεις με την απόδοση να αυξάνεται σε κάποιες περιπτώσεις μετά την

εφαρμογή των μηχανισμών ασφαλείας και την αύξηση της κεφαλίδας του πλαισίου.

Βιβλιογραφία

[1] ANSI/IEEE Std 802.11, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 1999 Edition

[2] IEEE Std 802.11a-1999 *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications High-speed Physical Layer in the 5 GHz Band*

[3] IEEE Std 802.11b-1999 *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band*

[4] IEEE Std 802.11g™-2003 *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band*

[5] IEEE Std 802.11i™-2004 *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements*

[6] IEEE Std 802.1x™-2004 *IEEE Standard for Local and metropolitan area networks Port – Based Network Access Control*

[7] Nathan J. Muller, 2003. *Wireless A to Z*. Mc Graw Hill.

[8] United States Government Accountability Office, *Information Security Federal Agencies Need to Improve Controls over Wireless Networks*. (d05383)

[9] Tom Karygiannis Les Owens, 2005. *Wireless Network Security 802.11, Bluetooth™ and Handheld Devices*. National Institute of Standards and Technology. (draft-sp800-48)

[10] The United States House of Representatives, *Wireless Network Security Policy*. March 27, 2003. (HISPOL006-0Wireless)

[11] Scott Fluhrer, Itsik Mantin, and Adi Shamir, 2001. *Weaknesses in the Key Scheduling Algorithm of RC4*. (rc4_ksaproc)

[12] Wi-Fi Alliance April 29, 2003. *Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks*. (Whitepaper_Wi-Fi_Security4-29-03)

[13] Wireless Networking in the Developing World. First edition, January 2006. (wndw-print)

[14] Wi-Fi Alliance, February 6, 2003. *Enterprise Solutions for Wireless LAN Security*. (wp_3_Securing Wi-Fi In The Enterprise_2-6-03)

[15] Wi-Fi Alliance, February 6, 2003. *Securing Wi-Fi Wireless Networks with Today's Technologies*. (wp_4_Securing Wireless Networks_2-6-03)

[16] Wi-Fi Alliance, February 6, 2003. *Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks*. (wp_8_WPA Security_4-29-03)

[17] Nikita Borisov, Ian Goldberg and David Wagner. *Intercepting Mobile Communications: The Insecurity of 802.11*. (wep-draft)

[18] William A. Arbaugh,Narendar Shankar and Y.C. Justin Wan. March 30, 2001. *Your 802.11 Wireless Network has No Clothes*. (wireless)

[19] Jesse R. Walker, 2003. *Unsafe at any key size; An analysis of the WEP encapsulation*. Intel Corporation.

[20] Atheros Communications Inc. 2003. *802.11 Wireless LAN Performance*. (atheros_range_whitepaper)

[21] Y.C. Tay and K.C. Chua. *A capacity analysis for the IEEE 802.11 MAC protocol*. National University of Singapore. (a-capacity-analysis-for)

[22] Martin Heusse, Franck Rousseau, Gilles Berger-Sabbatel, Andrzej Duda. *Performance Anomaly of 802.11b*. IEEE Infocom 2003. (21_01)

[23] Daniel Aguayo, John Bicket, Sanjit Biswas, Glenn Judd, Robert Morris. *Link-level Measurements from an 802.11b Mesh Network*. M.I.T. Computer Science and Artificial Intelligence Laboratory. (p442-aguayo)

[24] Tim Moors. *Characterising Errors In Wireless LAN*. University of New South Wales. (thesis)

[25] WiFi Alliance. *WPA and WPA2 Questions and Answers*. (kc_11_WPA2%20QandA_3-23-05)

[26] Moen, Raddum and Hole. *Weaknesses in the Temporal Key Hash of WPA*. University of Bergen. (WPA_attack)

[27] Mishra and Arbaugh. *An Initial Security Analysis of the IEEE 802.1X Standard*. University of Meryland. (1x)

[28] Changhua He, John C Mitchell. *Analysis of the 802.11i 4-Way Handshake*. Stanford University. (p43-he)

[29] Wireless Security Corporation. *WPA-PSK: A Limited Solution for Securing a Wireless Network*. (WSC_Compared_to_WPA_PSK)

[30] Matthew J. Gast. 802.11 *Wireless Networks The Definitive Guide,* 2nd Edition. O' Reilly.

[31] Jim Geier, 2005. *Wireless Networks*. Cisco Press.

[32] Tom Thomas, 2004. *Network Security*. Cisco Press.

[33] D. Castaneda, O. Mc Alasdair, C. Vinckier, 2006. *The Business Case for Enterprise – Class Wireless LANs*. Cisco Press.

[34] P. Roshan, J. Leary, 2004. *802.11 Wireless LAN Fundamentals*. Cisco Press.

[35] Harry R. Anderson, 2003. *Fixed Broadband Wireless System Design*. Wiley.

[36] Cisco Systems, 2005. *Cisco Networking Academy Program CCNA 1 and 2 Companion Guide*, 3rd Edition. Cisco Press.

[37] Cisco Systems, 2003. *Cisco Networking Academy Program CCNA 3 and 4 Companion Guide*, 3rd Edition. Cisco Press.

[38] Andrew S. Tanenbaum, 2000. *Δίκτυα Υπολογιστών*, Τρίτη Έκδοση. Εκδόσεις Παπασωτηρίου.

[39] H. Taub, D. Schilling, 1998. *Τηλεπικοινωνιακά Συστήματα*, Δεύτερη Έκδοση. Εκδόσεις Τζιόλα.

[40] Φ. Κωνσταντίνου, Χ. Καψάλης, Π. Κώττης. *Εισαγωγή στις Τηλεπικοινωνίες*. Εκδόσεις Παπασωτηρίου.

[41] Dr. Eric Cole, Dr. Ronald Krutz, and James W. Conley, 2005. *Network Security Bible*. Wiley Publishing, Inc.

[42] Patil, Saifullah etc. 2003. *IP in Wireless Networks*. Prentice Hall.

[43] Interlink Networks. *Link Layer and Network Layer Security for Wireless Networks.* (Layer2_Layer3_whitepaper_03_2006)

[44] Bob Fleck, Bruce Potter, 2002. *802.11 Security*. O' Reilly.

[45] Hossam Afifi, Djamal Zeghlache, 2001. *Applications and Services in Wireless Networks.* Hermes Science Publications.

[46] Joseph Davies, 2004. *Deploying Secure 802.11 Wireless Networks with Microsoft Windows.* Microsoft Press.

[47] Chris Hurley, Michael Puchol, Russ Rogers and Frank Thornton, 2004. *WarDriving: Drive, Detect, Defend: A Guide to Wireless Security.* Syngress Publishing.

[48] Jack McCullough, 2004. *Wireless Networking: Preventing a Data Disaster.* John Wiley & Sons.

[49] John Edney, William A. Arbaugh, 2003. *Real 802.11 Security: Wi-Fi Protected Access and 802.11i.* Addison Wesley.

[50] C. Peikari, S. Fogie, 2006. *Maximum Wireless Security.* Sams Publishing.

[51] Morinaga, Kohno and Sampei, 2002. *Wireless Communication Technologies: New Multimedia Systems.* Kluwer Academic Publishers.

[52] H. Vincent Poor, Gregory W. Wornell, 1998. *Wireless Communications: Signal Processing Perspectives.* Prentice Hall.

[53] Rob Flickenger, 2002. *Building Wireless Community Networks.* O' Reilly.

[54] Praphul Chandra, 2005. *Bulletproof Wireless Security: GSM, UMTS, 802.11 and Ad Hoc Security.* Elsevier.

[55] Bruce Schneier, 1996. *Applied Cryptography, 2nd Edition.* Wiley.

[56] Menezes, van Oorschot and Vanstone, 1996. *Handbook of Applied Cryptography.* MIT Press.

[57] Fred Piper and Sean Murphy, 2002. *Cryptography: A Very Short Introduction.* Oxford University Press.

[58] Chey Cobb, 2004. *Cryptography for Dummies.* Wiley.

[59] Cisco Systems, 2003. *Aironet Wireless LAN Fundamentals.* Cisco Press.

[60] Kaveh Pahlavan and Allen H. Levesque, 2005. *Wireless Information Networks, Second Edition.* Wiley.

[61] Jesse Walker, 2002. *The Temporal Key Integrity Protocol.* Intel Corporation. (17769_80211_part2)

[62] Jesse Walker, 2002. *AES – based Encapsulations of 802.11 Data.* Intel Corporation. (17770_80211_part3)

[63] Jesse Walker, 2005. *IEEE 802.11i Standard Improves Wireless LAN Security.* Technology@Intel Magazine. (80211i-0505)

[64] Han, Zheng and Chen, 2004. *Some Remarks on the TKIP Key Mixing Function of 802.11i.* China National Laboratory of Modern Communications. (129)

[65] Internet Engineering Task Force, April 1992. *RFC 1321: The MD5 Message-Digest Algorithm*.

[66] Internet Engineering Task Force, December 1994. *RFC 1750: Randomness Recommendations for Security.*

[67] Internet Engineering Task Force, February 1997. *RFC 2104: HMAC: Keyed-Hashing for Message Authentication.*

[68] Internet Engineering Task Force, September 1997. *RFC 2202: Test Cases for HMAC-MD5 and HMAC-SHA-1.*

[69] Internet Engineering Task Force, September 2002. *RFC 3394: Advanced Encryption Standard (AES) Key Wrap Algorithm.*

[70] Internet Engineering Task Force, September 2003. *RFC 3610: Counter with CBC-MAC (CCM).*

[71] Internet Engineering Task Force, June 2004. *RFC 3748: Extensible Authentication Protocol (EAP).*

[72] Joan Daemen and Vincent Rijmen, March 1999. *AES Proposal: Rijndael.*

[73] Federal Information Processing Standards, November 2001. *Publication 197: Advanced Encryption Standard (AES).*

[74] Federal Information Processing Standards, April 1995. *Publication 180-1: Secure Hash Standard.*

[75] Vocal Technologies, Ltd, 2003. *Counter CBC-MAC Protocol (CCMP) Encryption Algorithm.* (CCMP)

[76] Mitch Tulloch, 2003. *Microsoft Encyclopedia of Security.* Microsoft Press.

[77] Sankar, Sandalingam, Ballisky and Miller, 2004. *Cisco Wireless LAN Security.* Cisco Press.

[78] Rittinghouse and Randsome, 2004. *Wireless Operational Security.* Digital Press.

[79] Vladimirov, Gavrilenco and Mikhailovsky, 2004. *Wi – Foo.* Addison Wesley.