ΑΝΩΤΑΤΟ ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

Συγκριτική μελέτη αλγορίθμων κρυπτογράφησης πρωτοκόλλων ασύρματης επικοινωνίας

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΜΠΑΤΙΣΤΑΤΟΥ ΜΑΡΙΑ ΑΜ: 781

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:
ΤΣΑΚΑΝΙΚΑΣ ΒΑΣΙΛΕΙΟΣ

ΝΑΥΠΑΚΤΟΣ 2014

ΠΕΡΙΛΗΨΗ

Τα ασύρματα τοπικά δίκτυα έχουν κερδίσει την δημοτικότητα λόγω του ότι είναι οικονομικά, ευέλικτα, γρήγορα και εύκολα στην χρήση. Ωστόσο, αντιμετωπίζουν κάποιες σοβαρές προκλήσεις όσον αφορά την ασφάλεια και η επιλογή του πρωτόκολλου ασφάλειας είναι ένα κρίσιμο θέμα για τους IT administrators.
Η επιλογή του καταλληλότερου πρωτόκολλου ασφάλειας εξαρτάται από διάφορους παράγοντες όπως ο βαθμός ασφάλειας που προσφέρεται από το κάθε πρωτόκολλο, το πόσο συνεισφέρουν αυτά τα πρωτόκολλα στην μείωση της λειτουργίας του δικτύου, οι απαιτούμενες αναβαθμίσεις υλικού και λογισμικού για την εφαρμογή των διαφορετικών ασύρματων πρωτοκόλλων, η πιθανότητα υλοποίησης αυτών των πρωτόκολλων σε παλαιό ασύρματο υλικό και το τί πρωτόκολλο ασφάλειας είναι κατάλληλο για συγκεκριμένο μέγεθος δικτύου (μικρό, μεσαίο, μεγάλο).
Η επιρροή των πολλών σχεδίων ασφάλειας στην λειτουργία του δικτύου μελετήθηκε από διάφορους ερευνητές αναφορικά με το throughput των δικτύων IEEE 802.11, κάτω από διαφορετικό φόρτο (load), φυσιολογικό και συμφορισμένο, και για ποικίλα μεγέθη πακέτων κίνησης (από 100 bytes έως 1500 bytes).
Μέσω των διάφορων μελετών που έχουν διεξαχθεί, η παρούσα εργασία έχει ως σκοπό να μελετήσει και να συγκρίνει τους αλγόριθμους κρυπτογράφησης που χρησιμοποιούνται στα ασύρματα πρωτόκολλα ασφάλειας των ασύρματων τοπικών δικτύων αναφορικά με την αποτελεσματικότητά τους, την απόδοση, την ταχύτητα και το overhead. Έτσι σε κάθε περίπτωση παρουσιάζεται και το πόρισμα για την βέλτιστη επιλογή του πρωτόκολλου που πρέπει να χρησιμοποιηθεί.

Πίνακας Περιεχόμενων

Πίνακας Εικόνων

1. Ιστορική αναδρομή στην ασφάλεια ασύρματων δικτύων

1.1. Ασύρματα δίκτυα

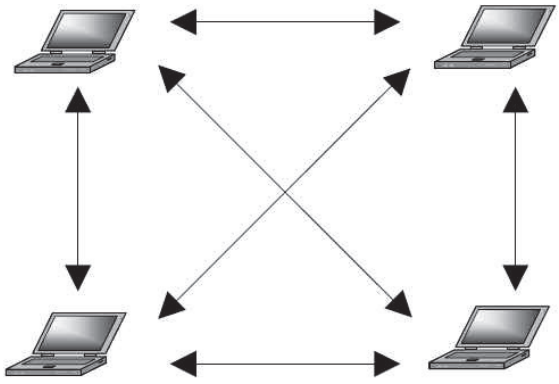
Ασύρματο δίκτυο αποτελεί κάθε δομημένο τηλεπικοινωνιακό δίκτυο που αποτελείται από δίκτυα και συσκευές υπολογιστών ή τηλεφωνίας και χρησιμοποιεί ως μέσο τον αέρα για την μετάδοση της πληροφορίας. Τα δεδομένα μεταφέρονται με ηλεκτρομαγνητικά κύματα (ραδιοκύματα ή υπέρυθρη ακτινοβολία), μέσω της διαδικασίας της διαμόρφωσης, με συχνότητα φέροντος η οποία εξαρτάται κάθε φορά από τον ρυθμό μετάδοσης δεδομένων που απαιτείται να υποστηρίζει το δίκτυο. Δεν αποτελούν ασύρματα δίκτυα το ραδιόφωνο και η τηλεόραση, όπως την ξέρουμε μέχρι στιγμής, αν και εντάσσονται στα ασύρματα τηλεπικοινωνιακά μέσα, αλλά η μετάδοση γίνεται προς κάθε κατεύθυνση χωρίς να υπάρχει κάποιο δομημένο δίκτυο τηλεπικοινωνιακών κόμβων.

Παραδείγματα ασύρματων δικτύων θεωρούνται τα εξής:

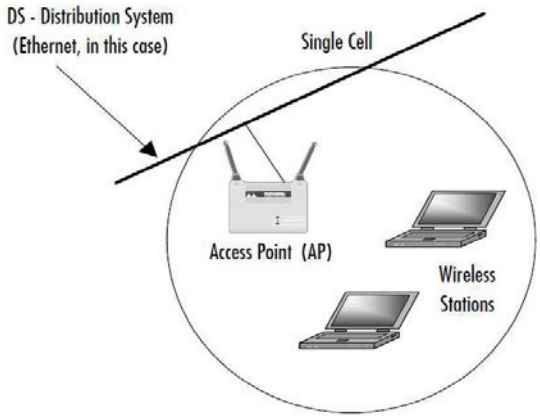
- Δίκτυα κινητής τηλεφωνίας
- Ασύρματα τηλέφωνα
- Δορυφορικές επικοινωνίες
- Ασύρματα δίκτυα ευρείας περιοχής (WWAN)
- Ασύρματα μητροπολιτικά δίκτυα (WMAN)
- Ασύρματα τοπικά δίκτυα (WLAN)
- Ασύρματα προσωπικά δίκτυα (WPAN)
- Ασύρματα τοπικά δίκτυα (WLAN) ή Wi-Fi

1.2. Ιστορία των WLAN

Η Motorola ανέπτυξε ένα από τα πρώτα εμπορικά συστήματα WLAN με το προϊόν της Altair. Ωστόσο, οι πρώιμες τεχνολογίες WLAN είχαν αρκετά προβλήματα που απαγόρευαν την γενικευμένη χρήση τους. Αυτά τα τοπικά δίκτυα (LAN) ήταν ακριβά και παρείχαν χαμηλούς ρυθμούς μετάδοσης δεδομένων όντας επιρρεπή σε παρεμβολές ραδιοσυχνοτήτων και σχεδιασμένα κυρίως για χρήση σε ιδιόκτητα δίκτυα τεχνολογίας RF. Το 1997, το IEEE ενέκρινε για πρώτη φορά το διεθνές πρότυπο διαλειτουργικότητας 802.11. Το πρότυπο IEEE 802.11 επιτρέπει στις συσκευές να δημιουργήσουν είτε δίκτυα peer-to-peer (P2P) ή δίκτυα που βασίζονται σε σταθερά σημεία πρόσβασης (AP) με τα οποία κινητοί κόμβοι μπορούν να επικοινωνήσουν.
Συνεπώς, το πρότυπο ορίζει δύο βασικές τοπολογίες δικτύων: το δίκτυο υποδομής και το δίκτυο ad hoc.



Εικόνα 1 Ένα δίκτυο ad-hoc/IBSS.



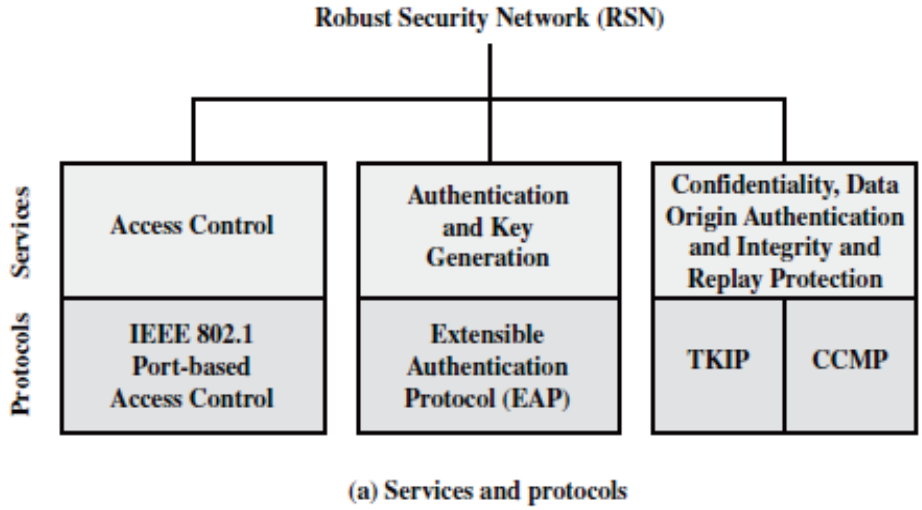
Εικόνα 2 BSS τοπολογία ασύρματου δικτύου.

Τα ενσύρματα δίκτυα έχουν δύο χαρακτηριστικά που δεν υπάρχουν στα ασύρματα δίκτυα:
1. Προκειμένου να εκπέμψει ένας σταθμός μέσω ενός ενσύρματου LAN, πρέπει να είναι συνδεδεμένος στο δίκτυο LAN. Από την άλλη, σε ένα ασύρματο δίκτυο LAN, κάθε σταθμός μπορεί να εκπέμψει εντός του εύρους κάλυψης των άλλων συσκευών. Κατά αυτή την έννοια, υπάρχει μια μορφή πιστοποίησης σε ένα ενσύρματο δίκτυο LAN.
2. Ομοίως, προκειμένου να λάβει μια εκπομπή από ένα σταθμό που είναι μέρος ενός ενσύρματου LAN, ο σταθμός λήψης θα πρέπει επίσης να είναι συνδεμένος στο ενσύρματο δίκτυο LAN. Από την άλλη, σε ένα ασύρματο δίκτυο LAN, κάθε σταθμός εντός της ακτίνας εκπομπής μπορεί να γίνει δέκτης της .Έτσι, τα ενσύρματα δίκτυα LAN παρέχουν ένα βαθμό ιδιωτικότητας, περιορίζοντας την λήψη των δεδομένων σε σταθμούς συνδεδεμένους στο δίκτυο LAN.
Αυτές οι διαφορές ασύρματων και ενσύρματων δικτύων υπερτονίζουν την ανάγκη ύπαρξης ανθεκτικών μηχανισμών ασφαλείας στα ασύρματα δίκτυα.

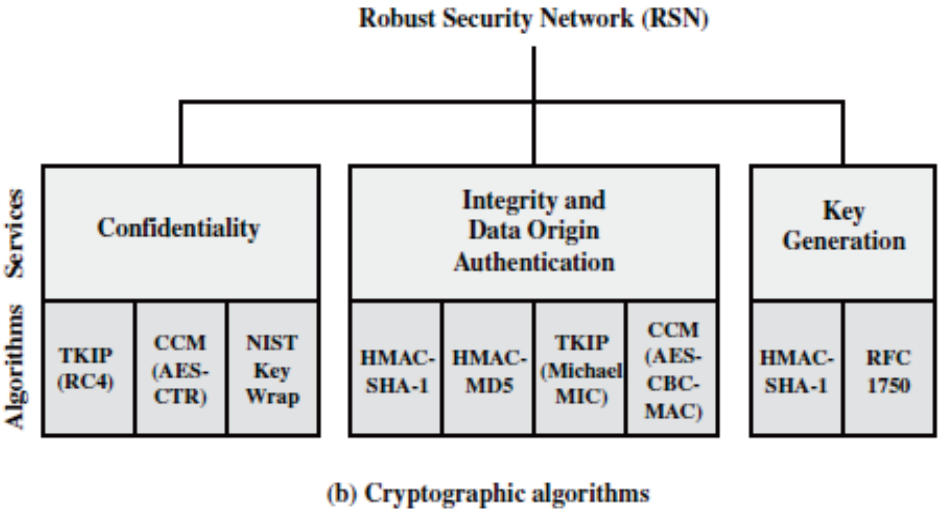
Το αρχικό πρότυπο 802.11 περιλάμβανε μια σειρά από μηχανισμούς προστασίας της ιδιωτικότητας και ταυτοποίησης που ήταν όμως ασθενείς. Σε ότι αφορά την ιδιωτικότητα, το πρότυπο 802.11 όρισε τον αλγόριθμο Wired Equivalent Privacy (WEP). Το τμήμα του προτύπου που σχετιζόταν με την ιδιωτικότητα εμφάνιζε μεγάλες αδυναμίες. Μετά την ανάπτυξη του WEP , η ομάδα για το πρότυπο 802.11i ανέπτυξε μια σειρά από μέτρα ώστε να αντιμετωπιστούν τα προβλήματα των δικτύων WLAN. Προκειμένου να επιταχύνει την εφαρμογή ισχυρών μηχανισμών ασφαλείας στα ασύρματα δίκτυα η Wi-Fi Alliance υποστήριξε την εφαρμογή του προτύπου Wi-Fi Protected Access (WPA), ως πρότυπο συνδεσιμότητας Wi-fi. Το πρότυπο WPA είναι ένα σύνολο μηχανισμών που επιλύει τα προηγούμενα ζητήματα ασφαλείας και βασίστηκε στην υπάρχουσα δομή του προτύπου 802.11i. Η τελική μορφή του προτύπου 802.11i αναφέρεται ως Robust Security Network (RSN).
Το πρότυπο 802.11i RSN παρέχει υπηρεσίες:

- ταυτοποίησης,
- ελέγχου πρόσβασης
- προστασίας της ιδιωτικότητας μαζί με ακεραιότητα μηνυμάτων.

Το παρακάτω γράφημα δείχνει τους αλγορίθμους και τα πρωτόκολλα ασφαλείας που χρησιμοποιούνται για την παροχή αυτών των υπηρεσιών:



(a) Services and protocols



(b) Cryptographic algorithms

CBC-MAC = Cipher Block Block Chaining Message Authentication Code (MAC)
CCM = Counter Mode with Cipher Block Chaining Message Authentication Code
CCMP = Counter Mode with Cipher Block Chaining MAC Protocol
TKIP = Temporal Key Integrity Protocol

Εικόνα 3 Αλγόριθμοι και πρωτόκολλα ασφάλειας που παρέχουν RSN υπηρεσίες .

1.3. Εξέλιξη της ασφάλειας των ασύρματων δικτύων

Ήδη από την δεκαετία του 40 η πρόοδος στην ανάπτυξη των ασύρματων τεχνολογιών συμβαδίζει με την ανάπτυξη εργαλείων και μεθόδων που έχουν ως στόχο την υποκλοπή των πληροφοριών που μεταδίδονται. Κατά την διάρκεια του δεύτερου παγκοσμίου πολέμου, όπου και οι δύο αντιμαχόμενες πλευρές χρησιμοποιούσαν ευρέως ραδιοεπικοινωνίες, τα εργαλεία υποκλοπής αποτέλεσαν μια αναγκαιότητα αφού όπως ήταν φυσικό μπορούσαν να προσφέρουν στρατηγικό πλεονέκτημα έναντι του αντιπάλου. Χαρακτηριστικό παράδειγμα τέτοιου πλεονεκτήματος αποτελεί η μάχη του Midway, όπου το Αμερικάνικο ναυτικό κατάφερε να κατανοήσει και ακολούθως να διασπάσει τον κώδικα επικοινωνίας γνωστό ως JN-25 που χρησιμοποιούσαν οι Ιάπωνες. Κατά τη διάρκεια επίσης του ψυχρού πολέμου (1950-1980) η ανάγκη για προστασία των ραδιοεπικοινωνιών βοήθησε ώστε να αναπτυχθούν και ακολούθως να βελτιστοποιηθούν νέες μέθοδοι εξασφάλισης των εκπεμπόμενων δεδομένων. Την δεκαετία του 80 η υποκλοπή ασύρματων μεταδόσεων ήταν εφικτή ακόμα και με ένα απλό ραδιοδέκτη / ανιχνευτή (radio scanner) που μπορούσε κάποιος να αγοράσει από ένα κατάστημα

ηλεκτρονικών. Η κατάσταση αυτή οδήγησε κάποιες κυβερνήσεις να απαγορεύσουν τη χρήση ανάλογων ραδιο-ανιχνευτών και έτσι οι εταιρίες κατασκευής συσκευών ασύρματων επικοινωνιών άρχισαν να σκέφτονται να υιοθετήσουν κρυπτογραφικές μεθόδους για την προστασία των εκπεμπόμενων δεδομένων. Χαρακτηριστικό παράδειγμα στις ΗΠΑ ο σχετικός νόμος που ψηφίστηκε από το Κογκρέσο του 1986 και είναι γνωστός ως Electronic Communications Privacy Act. Παράλληλα με την δυνατότητα υποκλοπής ή παρακολούθησης (intercepting / eavesdropping) των ασύρματων επικοινωνιών, μεγάλη απήχηση, ειδικά για στρατιωτικούς σκοπούς, είχε και η παρεμπόδιση τους μέσω παρεμβολών (jamming). Αν και τέτοιου είδους εξοπλισμός παρεμβολών απαγορεύτηκε από πολλά κράτη, διάφοροι ανεξάρτητοι κατασκευαστές κατασκευάζουν και πωλούν παρόμοια προϊόντα παρανόμως. Οι συσκευές αυτές μπορούν να παρεμποδίσουν την επικοινωνία όχι μόνο ενός ατόμου, αλλά και μιας ολόκληρης περιοχής αν ο επιτιθέμενος έχει ως στόχο για παράδειγμα μια κεραία κινητής τηλεφωνίας (radio tower) ή ένα ασύρματο σημείο πρόσβασης (access point, AP). Με την έλευση του ασύρματου διαδικτύου και σε συνδυασμό με τα ενσύρματα δίκτυα, τα ζητήματα και περιστατικά παραβίασης της ασφάλειας και ιδιωτικότητας (privacy) των χρηστών άρχισαν να πληθαίνουν και να γίνονται περισσότερο πιεστικά ως προς την αντιμετώπισή τους.
Παρακάτω παρουσιάζονται με χρονολογική σειρά οι τρόποι ασφάλειας των ασύρματων τοπικών δικτύων.

1.1.1 Στατική διαμόρφωση δικτύου

Οι διαχειριστές διαμόρφωναν στατικά τους πελάτες με απενεργοποιημένο το DHCP, και με στατικά τα: IP, μάσκα υποδικτύου (subnet mask), gateway, διευθύνσεις DNS server. Έτσι ο εισβολέας θα έπρεπε πρώτα να αποκτήσει πληροφορίες σχετικές με το δίκτυο έτσι ώστε να μπορέσει να το διαμορφώσει όπως εκείνος θέλει. Αυτός ο τρόπος απαιτεί υψηλό διαχειριστικό overhead[1]. Κοινότυπο πρόβλημα σε αυτά τα συστήματα είναι η απόκτηση πληροφοριών, η αναδιαμόρφωση του συστήματος και η παρεμπόδιση των νόμιμων χρηστών του δικτύου. Δεν παρέχεται εμπιστευτικότητα ή πιστοποίηση και η ασφάλεια στηρίζεται στην μυστικότητα.

1.2.1 Απενεργοποίηση εκπομπής SSID

Τα σημεία Πρόσβασης (Access Points, AP) σε κανονική λειτουργία εκπέμπουν το SSID ώστε οι πελάτες να μπορούν να ανιχνεύσουν το δίκτυο. Με την απενεργοποίηση της εκπομπής του SSID απαιτείται ο διαχειριστής να διαμορφώνει τους πελάτες χειροκίνητα. Έτσι είναι πιο δύσκολο να ανιχνευτεί η παρουσία του ασύρματου δικτύου αφού ο πελάτης πρέπει να διαμορφωθεί χειροκίνητα. Ωστόσο, είναι εύκολο αν θέλει κάποιος να ανιχνεύσει το ασύρματο δίκτυο, μαθαίνοντας απλώς το SSID, και στη συνέχεια να το διαμορφώσει διακόπτοντας τους νόμιμους χρήστες από την σύνδεσή τους στο ασύρματο δίκτυο. Είναι λοιπόν είναι πολύ μικρό το όφελος της ασφάλειας που παρέχει αυτή η διαδικασία.

1.3.1 Φιλτράρισμα MAC

Με αυτόν τον τρόπο τα APs επιτρέπουν την πρόσβαση σε γνωστές MAC Διευθύνσεις ενώ αρνούνται την πρόσβαση στις υπόλοιπες. Η πρόσβαση στο ασύρματο δίκτυο περιορίζεται μόνο σε γνωστούς πελάτες αλλά μπορεί να παραχωρηθεί εύκολα με MAC spoofing επιθέσεις όπου σε αυτή την περίπτωση

[1] Στην επιστήμη των υπολογιστών, το overhead είναι κάθε συνδυασμός υπερβολικού ή έμμεσου χρόνου υπολογισμού, μνήμης, εύρους ζώνης, ή άλλων πόρων που απαιτούνται για την επίτευξη ενός συγκεκριμένου στόχου.

περιορίζεται η πρόσβαση σε δικαιούχους πελάτες (Denial Of Service, DoS) ή περιμένουν οι νόμιμοι χρήστης μέχρι να αποσυνδεθεί ο επιτιθέμενος.
Το φιλτράρισμα MAC είναι μια λύση ασφάλειας για μικρή και σταθερή λίστα πελατών αλλά δεν συστήνεται για μεγάλες και δυναμικές λίστες.

1.4.1 Ιστορία του WEP

Το WEP (Wired Equivalent Protocol) είναι ένα ασύρματο πρωτόκολλο ασφάλειας το οποίο επικυρώθηκε το Σεπτέμβριο του *1999* από την IEEE (Institute of Electrical and Electronics Engineers). Έκτοτε, το WEP χρησιμοποιείται ευρέως στον τομέα των τηλεπικοινωνιών.
Ο αλγόριθμος κρυπτογράφησης WEP μπορεί εύκολα να σπάσει λόγω των ευρέως καταγεγραμμένων αδυναμιών του. Το 2005, μια ομάδα του προσωπικού του FBI έδωσε μια επίδειξη για το πώς μπορούν να χρησιμοποιήσουν εύκολα εργαλεία πρόσβασης για να σπάσουν το WEP κρυπτογραφημένο σύστημα σε λιγότερο από 3 λεπτά. Αυτή η επίδειξη είναι μία από τις πιο δημοφιλείς αναφορές που επιβεβαιώνουν την αδυναμία του WEP.
Στη συνέχεια, το IEEE διακήρυξε ότι το WEP ήταν απαρχαιωμένο και είχε αντικατασταθεί από το WPA/WPA2 (Wi-Fi Protected Access). Σχεδόν όλες οι ασύρματες συσκευές επικοινωνίας στην αγορά μετά το 2003, οι οποίες πωλήθηκαν με λειτουργία WEP, απενεργοποιήθηκαν. Ωστόσο, για ορισμένες συσκευές υπάρχουν επιλογές που επιτρέπουν την λειτουργία WEP, κυρίως για ακαδημαϊκούς και ερευνητικούς σκοπούς. Οπουδήποτε το WEP είναι ενεργοποιημένο, ένα προειδοποιητικό μήνυμα θα εμφανιζόταν προτρέποντας τον χρήστη σχετικά με την ευπάθεια του WEP.
Ορισμένες επιχειρήσεις εξακολουθούν να χρησιμοποιούν το WEP εξαιτίας της έλλειψης επίγνωσης σε θέματα ασφάλειας, οικονομικής δυσχέρειας ή επειδή είναι δύσκολη η αντικατάσταση των παρωχημένων συσκευών επικοινωνίας στις οποίες το WEP είναι ήδη εγκατεστημένο.
Από την ίδρυσή του, το WEP έχει χρησιμοποιηθεί από οργανισμούς ή ιδιώτες ως ασύρματο πρωτόκολλο ασφάλειας. Το *2001*, ο *Scott Fluhrer, ο Itsik Mantin και ο Adi Shamir* (*FMS εν συντομία*) δημοσίευσαν το διάσημό τους χαρτί πάνω στο WEP *«Weakness in the Key Scheduling Algorithm of RC4»*, παρουσιάζοντας δύο ευπάθειες στον αλγόριθμο κρυπτογράφησης RC4: αδυναμία σταθερότητας και γνωστές επιθέσεις IV. Και οι δύο επιθέσεις βασίζονται στο γεγονός ότι για ορισμένες τιμές κλειδιού είναι δυνατόν για bits του αρχικού byte της keystream να εξαρτώνται από μόνο λίγα bits του κλειδιού κρυπτογράφησης (αν και συνήθως κάθε keystream έχει 50% πιθανότητες να είναι διαφορετική από την προηγούμενη). Δεδομένου ότι το κλειδί κρυπτογράφησης αποτελείται από αλληλουχία του μυστικού κλειδιού με το IV, ορισμένες IV τιμές παράγουν αδύναμα κλειδιά.
Οι ευπάθειες έγιναν αντικείμενο εκμετάλλευσης από εργαλεία ασφάλειας όπως το *AirSnort*, επιτρέποντας την ανάκτηση των κλειδιών WEP, αναλύοντας ένα επαρκές ποσό της κίνησης. Ενώ αυτού του είδους η επίθεση θα μπορούσε να διεξαχθεί με επιτυχία σε ένα πολυάσχολο δίκτυο εντός εύλογου χρονικού διαστήματος, ο χρόνος που απαιτείται για την επεξεργασία των δεδομένων ήταν αρκετά μεγάλος. Ο *David Hulton (h1kari*) επινόησε μια βελτιστοποιημένη έκδοση για την επίθεση, λαμβάνοντας υπόψη όχι μόνο το πρώτο byte της εξόδου RC4 (όπως η FMS μέθοδος), αλλά και τα επόμενα. Αυτό οδήγησε σε μικρή μείωση του ποσού των απαιτούμενων δεδομένων για την ανάλυση. Το στάδιο ελέγχου ακεραιότητας δεδομένων υποφέρει επίσης από μια σοβαρή αδυναμία λόγω του CRC32 αλγόριθμου που χρησιμοποιείται για την αποστολή αυτή. Ο CRC32 χρησιμοποιείται συνήθως για ανίχνευση σφαλμάτων, αλλά δεν θεωρήθηκε ποτέ κρυπτογραφικά ασφαλής λόγω της γραμμικότητάς του, όπως ο *Nikita Borisov, Ian Goldberg και David Wagner* δήλωσαν ήδη το *2001*. Από τότε είχε γίνει δεκτό ότι το WEP παρέχει ένα αποδεκτό επίπεδο ασφαλείας μόνο για οικιακούς χρήστες και μη κρίσιμες εφαρμογές.

Ωστόσο, ακόμα και αυτή η προσεκτική επιφύλαξη παρεκτράπηκε με την εμφάνιση των *KoreK επιθέσεων το 2004*, ενός ανώνυμου συμμετέχοντος των security forums του NetStumbler.org. Αυτές οι επιθέσεις αποτελούνταν από γενικευμένες FMS επιθέσεις που επέτρεπαν στον επιτιθέμενο να ανακτήσει το κλειδί γρηγορότερα, συμπεριλαμβανομένων βελτιστοποιήσεις από h1kari.
Ο KoreK δημοσίευσε μία επίθεση, την *A-neg*, η οποία επιτρέπει στον επιτιθέμενο να μειώσει την έκταση του κλειδιού και επακολούθως να βρει το κλειδί γρηγορότερα. Ο ίδιος πάλι δημιούργησε την *Chopchop επίθεση* εκμεταλλευόμενος αυτή την φορά, όχι την αδυναμία του RC4 αλγόριθμου, αλλά τα ελαττώματα του σχεδιασμού του ίδιου του WEP (CRC32 checksum και την έλλειψη προστασίας από replay attack[2]).
Η *Chopchop* επίθεση στοχεύει στο να δώσει στον επιτιθέμενο την δυνατότητα να αποκρυπτογραφήσει ένα πακέτο χωρίς να γνωρίζει το κλειδί. Παρ' όλα αυτά , εξαιτίας της ελλιπής ταχύτητας, η πρακτική της χρήση είναι περιορισμένη στο να κρυφακούσει ένα πακέτο, να το αποκρυπτογραφήσει, να το τροποποιήσει και να το εμβάλει πάλι στο δίκτυο για να δημιουργήσει περισσότερη κίνηση και έτσι να δώσει περισσότερη ωφέλιμη πληροφορία για να εκτελέσει μια επίθεση ανάκτησης πλήρους κλειδιού.
Η *Fragmentation Attack ανακοινώθηκε το 2005* από τον *Bittau et al* σε ένα parer ονομαζόμενο *"The final nail in WEP coffin"*. Η επίθεση λειτουργεί ως εξής: αρχικά ο επιτιθέμενος χρειάζεται να κρυφακούσει το πακέτο. Αφού όλα τα πακέτα που στέλνονται σε ένα δίκτυο 802.11 έχουν όμοιες κεφαλίδες, ο επιτιθέμενος μπορεί να γνωρίζει / μαντέψει τα πρώτα 8 bytes του καθαρού κειμένου. Εφαρμόζοντας XOR σε αυτά τα 8 bytes με 8 αντίστοιχα bytes κρυπτογραφημένου κειμένου αποκτούμε 8 bytes του Keystream για ένα συγκεκριμένο IV. Αυτά τα 8 bytes του keystream δεν μπορούν να χρησιμοποιηθούν για να σταλεί ένα ολόκληρο πακέτο στο δίκτυο επειδή θα ήταν τραγικά μικρό. Αλλά το πρωτόκολλο WEP επιτρέπει να σταλεί ένα μοναδικό πακέτο μέχρι 16 fragments. Έτσι μπορούμε να χρησιμοποιήσουμε τα 8 bytes του keystream που γνωρίζουμε προκειμένου να εκπέμψουμε ένα πακέτο που περιέχει 64 bytes γνωστού κειμένου σε 16 fragments. Μπορούμε να έχουμε μόνο 64 bytes γνωστού κειμένου επειδή κάθε fragment χρειάζεται το δικό του 4 bytes μήκους CRC32 checksum. Όταν το AP λαμβάνει αυτά τα 16 fragments, θα τα αποκρυπτογραφήσει, θα τα συνδυάσει σε ένα μοναδικό πακέτο, θα τα κρυπτογραφήσει και θα τα στείλει πάλι πίσω στο δίκτυο. Αυτό το πακέτο είναι μήκους 68 bytes (64 bytes του γνωστού κειμένου και 4 bytes ICV). Με μια XOR ο επιτιθέμενος έχει τώρα 68 bytes keystream για δοσμένο IV. Με την επανάληψη αυτής της διαδικασίας, ο επιτιθέμενος μπορεί να φτάσει τα 1500 bytes keystream για ένα IV. Όταν γνωρίζει τα 1500 bytes keystream για ένα δοσμένο IV, είναι εύκολο να πάρει 1500 bytes keystream για άλλα IV στέλνοντας απλώς ένα εκπεμπόμενο πακέτο των 1500 bytes στο AP. Το AP στη συνέχεια θα αναμεταδώσει αυτό το πακέτο, αλλά κρυπτογραφημένο με ένα νέο IV. Αφού C XOR M = K ο επιτιθέμενος μπορεί να λάβει το keystream για άλλα IV και να χτίσει ένα λεξικό, επιτρέποντας του να αποκρυπτογραφήσει κάθε μοναδικό πακέτο του δικτύου και να δημιουργήσει κίνηση.
Αναφορικά, άλλες επιθέσεις στο WEP είναι η *Pyshkin Tews Weinmann (PTW) attack* που εμφανίστηκε το *2007*, η *Google Replay Attack*, το 2010, (στηρίζεται στο γεγονός ότι κάθε λάμδα χρήστης με μια πρόσβαση στο Internet θα κάνει τουλάχιστον μια εύρεση στο Google έχοντας τη διεύθυνση www.google.com ως homepage) και η *Coolface Attack* το 2010 επίσης.

[2] Μια replay attack (επίσης γνωστή ως playback attack) είναι ενός είδους δικτυακή επίθεση στην οποία μια έγκυρη μετάδοση δεδομένων επαναλαμβάνεται ή καθυστερείται λόγω κακόβουλης ή απατηλής επίθεσης. Αυτές οι επιθέσεις πραγματοποιούνται είτε από τον δημιουργό είτε από έναν αντίπαλο που παρεμβάλλεται στα δεδομένα και τα αναμεταδίδει, πιθανώς ως μέρος της μεταμφιεσμένης επίθεσης μέσω IP packet αντικατάστασης (όπως η επίθεση stream cipher).

Name	Type	Year	Packets	Ratio
FMS	statistical	2001	6,000,000 (64 bit WEP)	86
KoreK	statistical	2004	200,000 (64 bit WEP)	3
PTW	statistical	2007	70,000 (64 bit WEP)	1

Εικόνα 4 Επιθέσεις ανάκτησης κλειδιού.

Name	Type	Year	Packets
Chopchop	fake ARP	2004	1 at begin (later: injection-capture)
Fragmentation	fragmentation	2005	1 at begin (later: injection-capture)
Google replay	replay	2010	1 at begin (later: injection-capture)
Coolface	man-in-the-middle	2010	0 at begin (later: injection-capture)

Εικόνα 5 Επιθέσεις με κατασκευή πακέτων.

Η *ανεστραμμένη Arbaugh επαγωγική επίθεση* επιτρέπει αυθαίρετα πακέτα να αποκρυπτογραφούνται χωρίς γνώση κλειδιού χρησιμοποιώντας packet injection[3]. Εργαλεία cracking όπως το *CrackAircrack* από τον *Christophe Devine* ή το *WepLab* από τον *José Ignacio Sanchez* εφαρμόζουν αυτές τις επιθέσεις και μπορούν να ανακτήσουν ένα 128-bit WEP κλειδί σε λιγότερο από 10 λεπτά (ή λίγο περισσότερο, ανάλογα με το συγκεκριμένο access point ή wireless card).
Η προσθήκη packet injection βελτίωσε αισθητά τις φορές WEP cracking, απαιτώντας όχι εκατομμύρια, αλλά μόνο χιλιάδες πακέτων με αρκετά μοναδικά IV- περίπου 150.000 για ένα 64-bit WEP κλειδί και 500.000 για ένα 128-bit. Με το packet injection για να συγκεντρωθούν τα απαραίτητα δεδομένα ήταν θέμα λεπτών.

[3] Packet injection (επίσης γνωστό ως πλαστογραφία πακέτων ή spoofing packets) είναι όρος στα δίκτυα υπολογιστών και αναφέρεται στην διαδικασία της παρεμβολής σε μία εγκατεστημένη δικτυακή σύνδεση, μέσω της κατασκευής πακέτων να εμφανίζονται σαν να είναι μέρος της φυσιολογικής ακολουθίας της επικοινωνίας. Η διαδικασία packet injection επιτρέπει σε έναν τρίτο άγνωστο να διασπά και να παρεμποδίζει πακέτα από τα συνεννοημένα πρόσωπα που επικοινωνούν, το οποίο μπορεί να οδηγήσει σε υποβιβασμό ή μπλοκάρισμα της ικανότητας των χρηστών να χρησιμοποιούν βασικές υπηρεσίες δικτύου ή πρωτόκολλα. Το Packet injection χρησιμοποιείται κυρίως σε επιθέσεις man in the middle και denial of service.

Date	Description
September 1995	Potential RC4 vulnerability (Wagner)
October 2000	First publication on WEP weaknesses: *Unsafe at any key size; An analysis of the WEP encapsulation* (Walker)
May 2001	An inductive chosen plaintext attack against WEP/WEP2 (Arbaugh)
July 2001	CRC *bit flipping* attack – *Intercepting Mobile Communications: The Insecurity of 802.11* (Borisov, Goldberg, Wagner)
August 2001	FMS attacks – *Weaknesses in the Key Scheduling Algorithm of RC4* (Fluhrer, Mantin, Shamir)
August 2001	Release of AirSnort
February 2002	Optimized FMS attacks by h1kari
August 2004	KoreK attacks (unique IVs) – release of chopchop and chopper
July/August 2004	Release of Aircrack (Devine) and WepLab (Sanchez) implementing KoreK attacks

Εικόνα 6 Χρονοδιάγραμμα θανάτου του WEP.

1.5.1 Ιστορία του WPA

Οι επιθέσεις στα ασύρματα LAN έχουν γίνει πιο ευρέως διαδεδομένες και η ασφάλεια έχει εξελιχθεί από αυτή που προσέφερε το αρχικό πρωτόκολλο IEEE 802.11, στο IEEE 802.11i πρωτόκολλο το οποίο χρησιμοποιείται σήμερα. Η εξέλιξη συνέβη σε τρία βασικά στάδια: το αρχικό πρωτόκολλο IEEE 802.11 b, ένα ενδιάμεσο στάδιο με το Wi-Fi Protected Access (WPA), και η τρίτη φάση με τον καθορισμό του IEEE 802.1i πρωτόκολλου. Μετά τις επιτυχημένες επιθέσεις που εμφανίστηκαν στο πρότυπο ασφαλείας του IEEE 802.11 - Wireless Equivalent Privacy (WEP) - το IEEE και η Wi-Fi Alliance άρχισαν τον σχεδιασμό του IEEE 802.11i προτύπου (ως απάντηση στις ποικίλες σοβαρές αδυναμίες που εντόπισαν οι ερευνητές του προηγούμενου συστήματος) το οποίο επικυρώθηκε το 2004 και άρχισε να χρησιμοποιείται το έτος 2006.
Για να προσφερθεί προσωρινή προστασία, η Wi-Fi Alliance δημιούργησε το δικό της υποσύνολο του πρωτοκόλλου 802.11i το οποίο ονομάζεται Wi-Fi Protected Access (WPA) και εφαρμόζει την πλειοψηφία του προτύπου. Η IEEE 802.11 Task Group I (TGi) εισήγαγε την WPA δομή ασφάλειας που περιλαμβάνει το Temporal Key Integrity Protocol (TKIP). Η WPA λειτουργεί με δύο τρόπους: Preshared Key (PSK) και Enterprise . Το WPA-PSK προσφέρει λιγότερη ασφάλεια από ότι η έκδοση Enterprise, καθώς απαιτεί ένα κοινό μυστικό-ωστόσο είναι ευκολότερη στην εγκατάσταση. Το TKIP είναι ένα WEP patch, το οποίο είναι σχεδιασμένο για να λειτουργεί με υπάρχων υλικό (hardware), τυλίγοντας το πρωτόκολλο WEP με τρία νέα στοιχεία: ένα message integrity code (MIC) με όνομα Μάικλ, μια

διαδικασία αλληλουχίας πακέτου, και λειτουργία μίξης κλειδιών ανά πακέτο. Η κρυπτογράφηση ακόμα πραγματοποιείται χρησιμοποιώντας το RC4 Stream Cipher. Το WPA είναι σχεδιασμένο για να λειτουργεί με όλες τις κάρτες διεπαφής ασύρματου δικτύου αλλά όχι απαραιτήτως με τα πρώτης γενιάς ασύρματα σημεία πρόσβασης. Το WPA2, εφαρμόζει το πλήρες πρότυπο, αλλά δεν λειτουργεί με ορισμένες παλαιότερες κάρτες δικτύου.
Και τα δύο παρέχουν καλή ασφάλεια, με μερικά σημαντικά ζητήματα:

- Είτε το WPA ή το WPA2 πρέπει να είναι ενεργοποιημένο και να έχει επιλεγεί κατά προτίμηση αντί του WEP. Το WEP συνήθως παρουσιάζεται ως η πρώτη επιλογή ασφαλείας στις περισσότερες οδηγίες εγκατάστασης.
- Στην "Προσωπική" λειτουργία, η πιθανότερη επιλογή για το σπίτι και μικρά γραφεία, απαιτείται passphrase, για πλήρη ασφάλεια, η οποία πρέπει να είναι μεγαλύτερη από το τυπικό 6 έως 8 χαρακτήρων password που οι χρήστες έχουν μάθει να χρησιμοποιούν.
- Το WPA, δημιουργήθηκε από το Wi-Fi Alliance, μια βιομηχανική εμπορική ομάδα, η οποία είναι ιδιοκτήτρια του εμπορικού σήματος για το όνομα Wi-Fi και πιστοποιεί συσκευές που φέρουν αυτό το όνομα.
- Το WPA είναι σχεδιασμένο για χρήση με ένα IEEE 802.1X εξυπηρετητή πιστοποίησης, ο οποίος διανέμει διαφορετικά κλειδιά σε κάθε χρήστη, ωστόσο, μπορεί επίσης να χρησιμοποιηθεί σε μια λιγότερο ασφαλή λειτουργία **"pre-shared key"** mode, όπου σε κάθε χρήστη δίνεται ο ίδιος κωδικός πρόσβασης. Η σχεδίαση του WPA βασίζεται στο *σχέδιο 3* του προτύπου IEEE 802.11i.
- Η Wi-Fi Alliance δημιούργησε το WPA για να επιτραπεί η εισαγωγή ασφαλών ασύρματων προϊόντων δικτύου βασισμένων σε πρότυπα προτού η ομάδα IEEE 802.11i τελειώσει το έργο της. Η Wi-Fi Alliance εκείνη την χρονική περίοδο ήδη πρόσμενε την πιστοποίηση WPA2 με βάση το τελικό σχέδιο του IEEE 802.11i προτύπου, έτσι τα tags στο πεδίο πλαισίου (Information Elements ή IEs) είναι επίτηδες διαφορετικά από το 802,11i για να αποφευχθεί η σύγχυση της ενοποιημένης υλοποίησης WPA/WPA2.
- Τα δεδομένα είναι κρυπτογραφημένα με το RC4 stream cipher μαζί με ένα 128-bit κλειδί και ένα 48-bit initialization vector (IV). Μια σημαντική βελτίωση στο WPA συγκριτικά με το WEP είναι το Temporal Key Integrity Protocol (TKIP), που αλλάζει δυναμικά τα κλειδιά καθώς χρησιμοποιείται το σύστημα. Όταν χρησιμοποιείται σε συνδυασμό με το πολύ μεγαλύτερο IV, αυτό εμποδίζει τις πολύ γνωστές επιθέσεις ανάκτησης κλειδιού (key recovery attacks) στο WEP.
- Επιπρόσθετα, στον έλεγχο ταυτότητας και στην κρυπτογράφηση, το WPA παρέχει τεράστια βελτιωμένη *ακεραιότητα ωφέλιμου φορτίου (payload)*. Ο cyclic redundancy check (CRC) που χρησιμοποιείται στο WEP είναι εγγενώς μη ασφαλής- είναι δυνατόν να μεταβάλει το ωφέλιμο φορτίο και να ανανεώσει (update) το μήνυμα χωρίς να γνωρίζει το κλειδί WEP. Ένας πιο ασφαλής message authentication code (συνήθως γνωστός ως MAC, αλλά εδώ ονομάζεται "Message Integrity Code"(MIC) χρησιμοποιείται στο WPA, ένας αλγόριθμος που ονομάζονται "Michael". Ο MIC που χρησιμοποιείται στο WPA περιλαμβάνει έναν μετρητή πλαισίου, πράγμα που εμποδίζει την εκτέλεση επαναλαμβανόμενων επιθέσεων (replay attacks).
- Με την αύξηση του μεγέθους των κλειδιών και του IV, μειώνεται ο αριθμός των πακέτων που στέλνονται με τα σχετικά κλειδιά, και προστίθεται ένα σύστημα επαλήθευσης ασφαλούς μηνύματος, το WPA κάνει την διείσδυση στο ασύρματο LAN πολύ πιο δύσκολη. Ο αλγόριθμος Michael ήταν ο ισχυρότερος που θα μπορούσαν να προσφέρουν οι σχεδιαστές WPA ο οποίος θα μπορούσε να εξακολουθεί να λειτουργεί με τις περισσότερες παλαιότερες κάρτες δικτύου. Λόγω των αναπόφευκτων αδυναμιών του Michael, το WPA περιλαμβάνει ειδικό αντίμετρο μηχανισμό που ανιχνεύει

την απόπειρα που σκοπεύει να σπάσει το TKIP και εμποδίζει προσωρινά τις επικοινωνίες με τον επιτιθέμενο.

Επιθέσεις στο WPA

Το *2008 ο Beck και ο Tews* δημοσίευσαν μια επίθεση στο WPA. Αυτή, δεν είναι επίθεση ανάκτησης κλειδιού αλλά εκμεταλλεύεται τις αδυναμίες στο TKIP έτσι ώστε να επιτρέψει στον επιτιθέμενο να αποκρυπτογραφήσει πακέτα ARP και να εισάγει κίνηση μέσα σε ένα δίκτυο, ακόμα και να του επιτρέψει να εκτελέσει DoS (Denial of Service) ή ARP poisoning.

Ohigashi-Morii Attack (Beck-Tews + Man-in-the-middle)

Η επίθεση *Ohigashi-Morii Attack (2009)* είναι μια βελτιωμένη έκδοση της επίθεσης Beck-Tews στο WPA-TKIP. Στην πραγματικότητα, αυτή η νέα επίθεση είναι εφικτή σε όλες τις καταστάσεις του WPA και όχι μόνο σε εκείνες με χαρακτηριστικά QoS . Ο χρόνος εισβολής ενός ψεύτικου πακέτου μειώνεται σε περίπου 15 λεπτά έως 1 λεπτό στην καλύτερη περίπτωση. Για αυτή την επίθεση, μια επίθεση man-in-the-middle τοποθετείται πάνω από την επίθεση Beck-Tews, με πληροφορίες για να μειώσουν τον χρόνο εκτέλεσης της επίθεσης.

Επιθέσεις Michael (Michael Attacks)

Ο αλγόριθμος Michael αναμενόταν να παράγει ένα hash κάποιου καθαρού κειμένου (plaintext). Παρ' όλα αυτά, το 2008, ο Beck και Tews βρήκαν έναν τρόπο να αναιρέσουν τον αλγόριθμο Michael.
Και το *2010, ο Beck* βρήκε έναν τρόπο να εκτελέσει μία επίθεση με βάση τα ελαττώματα στον Michael. Βασικά, βρήκε ότι εάν η εσωτερική κατάσταση στον Michael φτάσει σε ένα συγκεκριμένο σημείο, τότε ο αλγόριθμος Michael επαναφέρεται στην αρχική του κατάσταση (reset). Έτσι , μπορούμε να εισάγουμε κάποιο κείμενο της επιλογής μας σε ένα πακέτο, να προσθέσουμε μια σειρά string χαρακτήρων που θα κάνει reset στον αλγόριθμο Michael, και το πακέτο αλλάζει αλλά το αποτέλεσμα του Michael παραμένει σωστό. Ένα ολοκληρωμένο πρωτόκολλο που επιτρέπει την εκτέλεση μιας *επίθεσης Michael Reset Attack* περιγράφεται στο paper του Beck, αλλά κάποιος πρέπει να παρατηρήσει ότι οι απαιτήσεις αυτής της επίθεσης είναι ακόμα πιο "σφικτές " από τις απαιτήσεις μιας κλασσικής επίθεσης Beck και Tews. Επιπλέον, το απλό γεγονός απενεργοποίησης του QoS καθιστά αυτή την επίθεση απίθανη.

Η ευπάθεια της τρύπας 196 (The Hole196 Vulnerability)

Η ευπάθεια της τρύπας 196, βρέθηκε από τον *Sohail Ahmad (Airtight Networks) το 2010*, προέρχεται από την σελίδα 196 του πρότυπου paper σχετικά με τα πρωτόκολλα 802.11, όπου υπάρχει μια τρύπα.
Αυτού του είδους η επίθεση δεν είναι επίθεση ανάκτησης κλειδιού, ο επιτιθέμενος πρέπει να είναι εγκεκριμένος (authorized) χρήστης του δικτύου. Πρώτα, στέλνει μία αίτηση ARP με την MAC-address και την IP-address του AP. Έτσι οι άλλοι πελάτες του AP θα ανανεώσουν (update) τους πίνακες ARP, και θα στείλουν τα πακέτα τους στην MAC-address του επιτιθέμενου. Έτσι ο επιτιθέμενος θα λάβει τα πακέτα αποκρυπτογραφημένα από το AP και θα τα επανακρυπτογραφήσει με το κλειδί του- είναι επίσης ικανός να τα διαβάσει. Αυτή είναι μια επίθεση man-in-the-middle, και λειτουργεί επειδή οποιοσδήποτε μπορεί να δημιουργήσει και να εκπέμψει ψεύτικα πακέτα με το GTK (shared group key).

Επίθεση λεξικού ενάντια στην χειραψία (Dictionary attack against the handshake)

Υπάρχει μια επίθεση ανάκτησης κλειδιού στο WPA (Pre-Shared Key έκδοση), όπου το κλειδί είναι μια λέξη του λεξικού.
Κρυφακούγοντας το δίκτυο, στόχος του επιτιθέμενου είναι να λάβει μια χειραψία: το hash του ανταλλασσόμενου κλειδιού μεταξύ πελάτη και AP όταν ο πελάτης ξεκινάει τη σύνδεση. Ο επιτιθέμενος μπορεί να περιμένει, ή να εξαπολύσει μια επίθεση αναίρεσης πιστοποίησης (deauthenticate-attack) εναντίον του πελάτη. Όταν λάβει το hash, μπορεί να δοκιμάσει να βρει το κλειδί με επίθεση λεξικού, μια επίθεση ουράνιου τόξου (rainbow-attack) ή μια από τις πολλαπλές επιθέσεις που υπάρχουν σε κλειδιά με hash γενικά.

Επίθεση Chop-Chop

Η βασική επίθεση εναντίον του TKIP ονομάζεται Chopchop και δεν είναι επίθεση ανάκτησης κλειδιού. Η επίθεση chopchop εφαρμόστηκε αρχικά εναντίον του WEP και επιτρέπει στον επιτιθέμενο να αποκρυπτογραφήσει διαδραστικά τα τελευταία m bytes του καθαρού κειμένου ενός κρυπτογραφημένου πακέτου στέλνοντας m*128 πακέτα κατά μέσο όρο στο δίκτυο . Βασίζεται στην αδυναμία CRC32 checksum που ονομάζεται ICV που επισυνάπτεται στα δεδομένα του πακέτου. Ο επιτιθέμενος περικόβει το τελευταίο byte του κρυπτογραφημένου πακέτου και μαντεύει την τιμή και επιστρέφει το πακέτο στο AP. Εάν δεν είναι σωστό τότε το πακέτο θα απορριφθεί με ένα λάθος checksum και ο επιτιθέμενος τότε θα ξέρει ότι ήταν λάθος. Όταν μαντέψει τη σωστή τιμή για το τελευταίο byte συνεχίζει αντίστροφα στα υπόλοιπα bytes μέχρι να μαντέψει ολόκληρο το πακέτο. Κατά μέσο όρο χρειάζεται 128 υποθέσεις ανά byte για να μαντέψει την σωστή τιμή. Ωστόσο, αφού ο MIC και οι μετρητές ακολουθίας περιλαμβάνονται στο WPA μπορεί να εμποδιστεί αυτή η επίθεση από το να δουλέψει με τον αυθεντικό τρόπο. Ο επιτιθέμενος τώρα αιχμαλωτίζει ένα πακέτο και βρίσκει ένα κανάλι χαμηλής κίνησης όπου ο μετρητής ακολουθίας θα είναι ακόμα χαμηλός και δοκιμάζει την επίθεση. Εάν ο επιτιθέμενος μαντέψει το τελευταίο byte λάθος τότε το AP θα πετάξει το πακέτο σιωπηλά, αλλά εάν η υπόθεση είναι σωστή τότε ένα πλαίσιο αναφοράς αποτυχίας του MIC στέλνεται στον πελάτη. Αφού ληφθεί αυτό το πλαίσιο από τον επιτιθέμενο τότε καταλαβαίνει ότι η υπόθεση του ήταν σωστή και θα πρέπει να περιμένει το λιγότερο 60 δευτερόλεπτα προτού να μαντέψει με σκοπό να εμποδίσει τον πελάτη από το να αποσυνδεθεί. Αφού ο επιτιθέμενος έχει αποκρυπτογραφήσει τα τελευταία 12 bytes θα έχει το MIC και ICV σε καθαρό κείμενο. Χρησιμοποιώντας το ICV, ο επιτιθέμενος μπορεί να μαντέψει το υπόλοιπο του πακέτου και να εκτελέσει το CRC32 μέχρι να ταιριάζουν οι τιμές και να ξέρει ότι έχει αποκρυπτογραφήσει το πακέτο. Με το ανακτημένο MIC ο επιτιθέμενος μπορεί να αντιστρέψει τον αλγόριθμο για να ανακτήσει το κλειδί του MIC. Με το κλειδί MIC ανακτημένο ο επιτιθέμενος μπορεί να στείλει πακέτα στους πελάτες οποιουδήποτε καναλιού όπου ο μετρητής ακολουθίας είναι χαμηλός και να εκτελέσει έναν αριθμό επιθέσεων όπως επαναδρομολόγηση κίνησης .

Name	Year	Utility	Ratio
Beck and Tews	2008	inject traffic (QoS features)	24
Ohigashi-Morii	2009	inject traffic (in all modes)	2
Michael	2010	inject traffic (in all modes)	1
Hole196	2010	man-in-the-middle, inject traffic, DoS attack	-
Dictionary attack		key-recovery	-

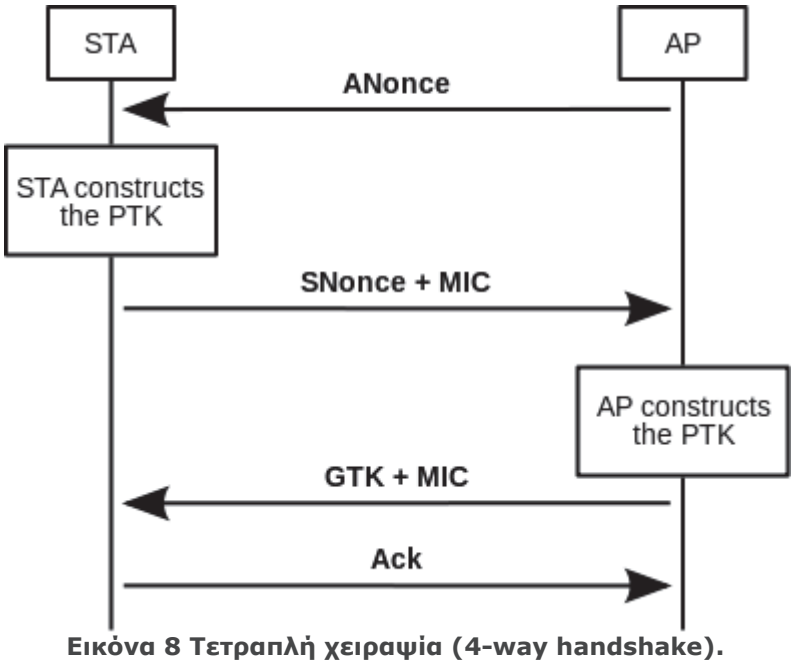
Εικόνα 7 Οι επιθέσεις στο WPA.

1.6.1 Ιστορία του 802.11i/WPA2

Τον Ιανουάριο του 2001, δημιουργήθηκε το i task group από την IEEE για να βελτιώσει την 802.11 πιστοποίηση δεδομένων και την ασφάλεια κρυπτογράφησης.

Τον Απρίλιο του 2003, η Wi-Fi Alliance (μια συνεργασία για την προώθηση και πιστοποίηση των Wi-Fi) εξέδωσε μια πρόταση ως απάντηση στις ανησυχίες σχετικά με την ασύρματη ασφάλεια. Ωστόσο, είχαν επίγνωση ότι οι πελάτες δεν θα επιθυμούσαν να αντικαταστήσουν τον υπάρχων εξοπλισμό τους. Έτσι ξεχώρισαν την πιστοποίηση χρήστη από την επιβολή μηνύματος ακεραιότητας και την εμπιστευτικότητα, παρέχοντας με αυτόν τον τρόπο μια ισχυρή και επεκτάσιμη αρχιτεκτονική ασφαλείας εξίσου κατάλληλη για τα οικιακά δίκτυα και μεγάλα εταιρικά συστήματα. Η νέα αρχιτεκτονική για τα ασύρματα δίκτυα ονομάζεται Ισχυρή ασφάλεια δικτύου (Robust Security Network, RSN) και χρησιμοποιεί 802.1X πιστοποίηση, διανομή ισχυρού κλειδιού και νέα ακεραιότητα και μηχανισμό μυστικότητας (Privacy).
Ενώ η RSN αρχιτεκτονική είναι πιο πολύπλοκη, παρέχει ασφαλείς και κλιμακούμενες λύσεις για ασύρματες επικοινωνίες. Μία RSN χαρακτηριστικά αποδέχεται μόνο RSN-ικανές συσκευές, αλλά η 802.11i ορίζει μια αρχιτεκτονική Μεταβατικής ασφάλειας δικτύου (Transitional Security Network, TSN) στην οποία μπορούν να συμμετέχουν και RSN και WEP συστήματα, επιτρέποντας στους χρήστες να ανανεώνουν (update) τον εξοπλισμό τους εγκαίρως. Εάν η διαδικασία πιστοποίησης ή συσχέτισης που χρησιμοποιείται μεταξύ των σταθμών χρησιμοποιεί της τετραπλή χειραψία (4-way handshake), η συσχέτιση ονομάζεται RSNA (Robust Security Network Association).

4-way handshake:
Η four-way handshake χρησιμοποιείται για να εγκαταστήσει ένα άλλο κλειδί που ονομάζεται PTK (Pairwise Transient Key). Το PTK δημιουργείται από τη συνένωση των παρακάτω χαρακτηριστικών: PMK, AP nonce (ANonce), STA nonce (SNonce), διεύθυνση MAC AP και τη MAC διεύθυνση STA. Το προϊόν που παράγεται στη συνέχεια τοποθετείται μέσα σε PBKDF2-SHA1 ως συνάρτηση κρυπτογράφησης hash.
Η χειραψία δίνει επίσης το GTK (Group Temporal Key), που χρησιμοποιείται για την αποκρυπτογράφηση multicast και broadcast κίνησης. Τα πραγματικά μηνύματα που ανταλλάσσονται κατά τη διάρκεια της χειραψίας απεικονίζονται στο σχήμα και εξηγούνται παρακάτω:



Εικόνα 8 Τετραπλή χειραψία (4-way handshake).

1. Το AP στέλνει μια τιμή nonce στον STA (ANonce). Ο πελάτης έχει πλέον όλα τα χαρακτηριστικά για την κατασκευή του PTK.
2. Ο STA στέλνει την δικιά του τιμή nonce (SNonce) στο AP μαζί με ένα MIC, συμπεριλαμβανομένης της πιστοποίησης ταυτότητας, η οποία είναι στην

πραγματικότητα ένα μήνυμα ταυτότητας και κώδικας ακεραιότητας (Message Authentication and Integrity Code, MAIC).
3. Το AP στέλνει το GTK και έναν αριθμό ακολουθίας μαζί με ένα άλλο MIC. Αυτός ο αριθμός ακολουθίας θα χρησιμοποιηθεί στο επόμενο πλαίσιο multicast ή broadcast, έτσι ώστε ο STA λήψης να μπορεί να εκτελέσει βασική επανάληψη ανίχνευσης.
4. Ο STA στέλνει μήνυμα επιβεβαίωσης στο AP.

Η Χειραψία Group Key

Το GTK που χρησιμοποιείται στο δίκτυο μπορεί να χρειαστεί να ανανεωθεί ύστερα από την λήξη του προρυθμισμένου χρονοδιακόπτη. Όταν μια συσκευή αποσυνδέεται από το δίκτυο, το GTK πρέπει επίσης να ανανεωθεί. Αυτό συμβαίνει για να αποτρέψει τη συσκευή να λαμβάνει πλέον multicast ή broadcast μηνύματα από το AP.
Για να χειριστεί την ανανέωση, το 802.11i ορίζει μια **Χειραψία Group Key** που αποτελείται από διπλή handshake:
1. Το AP αποστέλλει το νέο GTK σε κάθε STA στο δίκτυο. Το GTK κρυπτογραφείται με το KEK που διατίθενται για το STA, και προστατεύει τα δεδομένα από παραβιάσεις, με τη χρήση ενός MIC.
2. Το STA αναγνωρίζει το νέο GTK και απαντά στο AP.

Το 2004, το IEEE 802.11 πρότυπο επικυρώθηκε και αναφέρεται από την Wi-Fi Alliance με το όνομα WPA2 και υλοποιεί τα υποχρεωτικά στοιχεία του 802,11i. Ειδικότερα, εκτός από το TKIP και τον αλγόριθμο Michael, εισάγει έναν νέο αλγόριθμο βασισμένο στον 128-bit AES για κρυπτογράφηση και έλεγχο ταυτότητας , το CCMP, που θεωρείται απόλυτα ασφαλής. Θύρες (ports) χωρίς κάποιον έλεγχο χρησιμοποιούνται για αιτήσεις πριν από την εξουσιοδότηση (authorization).
Στη συνέχεια παρέχεται πρόσβαση στους πόρους του δικτύου μόνο στους πιστοποιημένους πελάτες (authentication) σε ελεγχόμενες θύρες.
Επιπλέον το 802.11i μπορεί να χρησιμοποιήσει πιστοποίηση επιπέδου εφαρμογής.
Στα Windows, η υποστήριξη WPA2 δεν είναι built-in. Μπορεί να απαιτούνται οδηγοί αναβαθμίσεων (Driver upgrades) για κάρτες δικτύου.
Ένα update για τα Windows XP SP2 (KB893357) δημοσιεύθηκε στις 29 Απριλίου 2005, προσθέτοντας το WPA2 και βελτιώνοντας την ανίχνευση δικτύου. Άλλα λειτουργικά συστήματα Microsoft πρέπει να χρησιμοποιήσουν έναν εξωτερικό ικέτη (supplicant) (εμπορικό ή ανοικτού κώδικα όπως το *wpa_supplicant* – η έκδοση Windows είναι πειραματική).
Οι υπολογιστές Apple υποστηρίζουν WPA2, σχετικά σε όλα τα Macintosh με ενεργοποιημένο το AirPort Extreme, το AirPort Extreme Base Station, και το AirPort Express. Οι απαιτούμενες αναβαθμίσεις υλικολογισμικού (firmware), περιλαμβάνονται στο AirPort 4.2, που δημοσιεύθηκε στις 14 Ιουλίου 2005.
Σημειώνεται ότι από 13 Μαρτίου 2006 η πιστοποίηση WPA2 είναι υποχρεωτική για όλες τις νέες συσκευές που επιθυμούν να είναι Wi-Fi certified.
Στα Linux και *BSD, το *wpa_supplicant* ήταν έτοιμο για το WPA2 όταν το πρότυπο 802.11i εκδόθηκε. Ο εξωτερικός supplicant υποστηρίζει έναν μεγάλο αριθμό μεθόδων EAP και χαρακτηριστικά διαχείρισης κλειδιού για το WPA, WPA2 και WEP. Πολλαπλά δίκτυα μπορούν να δηλωθούν με ποικίλες κρυπτογραφήσεις, διαχείριση κλειδιού και μεθόδους EAP.

Επιθέσεις στο WPA2

Ο κόσμος άλλαξε από τότε που το αυθεντικό WPA/WPA2 Cracking tutorial του Brandon Teska γράφτηκε το 2008. Ενώ υπάρχουν μερικά ασύρματα δίκτυα που χρησιμοποιούν ακόμα το WEP, υπήρξε μαζική μετανάστευση στην ασύρματη ασφάλεια WPA2-AES. Η αιτία-κλειδί για αυτή την μετανάστευση ήταν το 802.11n, το οποίο απαιτεί ενεργοποιημένη την ασφάλεια WPA2/AES προκειμένου να πετύχει ταχύτητες συνδέσμου πάνω από 54 Mbps. Οι τεχνικές Cracking έχουν επίσης αλλάξει. Ενώ οι περισσότερες τεχνικές χρησιμοποιούν ακόμα κάποιου είδους εκμεταλλεύσεις (exploits) βασισμένες σε λεξικό, η ισχύς του cloud (Internet, μεγάλα τοπικά δίκτυα κτλ.) έχει φτάσει να έχει συνάφεια με password cracking. Οι πληροφορίες που χρειαζόμαστε να συλλάβουμε περιέχονται στην μετάδοση μεταξύ του AP και STA (station, πελάτη) γνωστή ως τετραπλή χειραψία (four-way handshake). Οι τεχνικές που χρησιμοποιούνται για να ανακτηθεί η passphrase είναι πρωταρχικά είδη επιθέσεων λεξικού.
Το WPA2-PSK (Pre-Shared Key) είναι το πιο ασφαλές είδος κρυπτογράφησης που χρησιμοποιείται στα προσωπικά ασύρματα δίκτυα (personal wireless networks). Χρησιμοποιεί τον αλγόριθμό Advanced Encryption Standard (AES) για να κρυπτογραφήσει τα δεδομένα αντί του RC4 stream cipher. Παρ' όλο που υπάρχουν κάποιες δημοσιευμένες θεωρητικές επιθέσεις στον AES, θεωρείται ακόμα πολύ ασφαλές και οι επιθέσεις στην κρυπτογράφηση αυτή κάθε αυτή θα ήταν πολύ σύνθετες.
Ωστόσο, αυτό δεν σημαίνει ότι το WPA2 είναι ασφαλές ενάντια σε επιθέσεις ανάκτησης κλειδιού. Όταν ένας πελάτης συνδέεται σε ένα WPA2-PSK εκτελείται μια τετραπλή χειραψία για να πιστοποιήσει τον πελάτη με το AP. Κατά τη διάρκεια αυτής της χειραψίας, ο πελάτης εκτελεί τον αλγόριθμο Secure Hash Algorithm 1 (SHA-1) στο κοινό κλειδί "μαγειρεμένο" με το Service Set Identifier (SSID) του AP και το στέλνει στο AP για επαλήθευση. Με παθητικό άκουσμα στην κίνηση του δικτύου, ένας επιτιθέμενος μπορεί να αιχμαλωτίσει αυτό το πακέτο. Εάν δεν συνδέεται κανένας πελάτης εκείνη τη στιγμή, ο επιτιθέμενος περιμένει, μπορεί να εκτελέσει μια επίθεση αναίρεσης πιστοποίησης με σκοπό να εξαναγκάσει την χειραψία να συμβεί.
Μια επίθεση deauthentication συμβαίνει όταν ο επιτιθέμενος στέλνει ένα πακέτο deauthentication στον πελάτη αφού μεταμφιέσει τον εαυτό του σαν το AP. Εάν ο πελάτης δεχτεί αυτό το πακέτο θα αναιρέσει την πιστοποίησή του με το AP και ο επιτιθέμενος μπορεί να συλλάβει την χειραψία. Αφού ο επιτιθέμενος λάβει την χειραψία είναι πολύ εύκολο να εκτελέσει μια επίθεση ωμής βίας όσο και λεξικού για να ανακτήσει το καθαρό κείμενο του κοινού κλειδιού. Η ταχύτητα αυτής της επίθεσης κυρίως εξαρτάται καθαρά από την ταχύτητα του επεξεργαστή αφού όταν η χειραψία ληφθεί ο επιτιθέμενος μπορεί να σπάσει το κοινό κλειδί με την άνεσή του. Με την διαθεσιμότητα των αρχείων λεξικού που περιέχουν τα πιο κοινά passwords όπως επίσης τα προγράμματα (όπως το John the Ripper το οποίο μπορεί να δημιουργήσει διαφορετικούς συνδυασμούς βασισμένους σε αυτά τα passwords) μπορεί να κατασκευαστεί ένα αρκετά περιεκτικό λεξικό. Επιπλέον, η διαδικασία μπορεί να επιταχυνθεί με τη χρήση των Rainbow Tables οι οποίοι είναι προ-κρυπτογραφημένες συλλογές από τους πιο κοινούς κωδικούς πρόσβασης και τα πιο κοινά SSID σταθμού βάσης. Επίσης το 2005 ανακαλύφθηκε ότι συγκρούσεις μπορούν να υπάρχουν στην λειτουργία SHA-1 hashing.

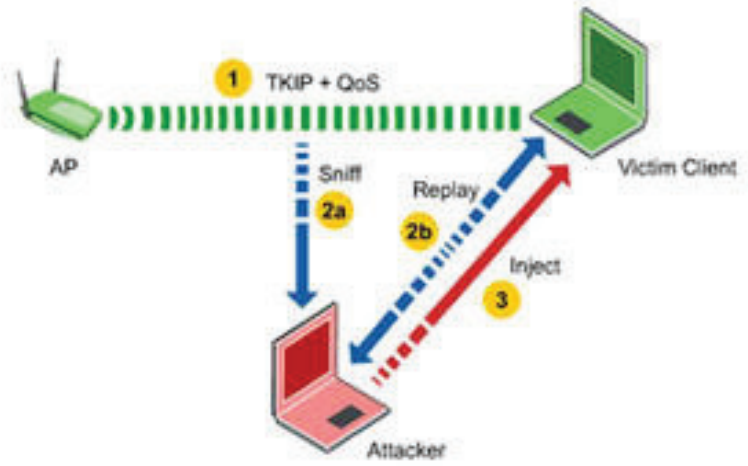
Η ευπάθεια "Τρύπα196" στο WPA2

Η "Τρύπα196" είναι μια ευπάθεια στο πρωτόκολλο ασφαλείας WPA2, που εκθέτει τα δίκτυα Wi-Fi με WPA2 ασφάλεια στις εσωτερικές επιθέσεις. Τα δίκτυα AirTight αποκάλυψαν μια αδυναμία στο πρωτόκολλο WPA2, η οποία ήταν τεκμηριωμένη (documented) αλλά θάφτηκε στην τελευταία γραμμή στη σελίδα 196 των 1232-σελίδων πρότυπου IEEE 802.11 (Αναθεώρηση 2007). Έτσι, έμεινε το όνομα "τρύπα196 ". Στο επίκεντρο αυτής της ευπάθειας είναι η ομάδα temporal key

(group temporal key , GTK) που μοιράζεται σε όλους τους εξουσιοδοτημένους πελάτες σε ένα WPA2 δίκτυο. Στην τυπική συμπεριφορά, μόνο ένα AP υποτίθεται ότι πρέπει να μεταδώσει κίνηση δεδομένων διευθυνσιοδοτημένων στην ομάδα τα οποία να είναι κρυπτογραφημένα με το GTK και οι πελάτες της υποτίθεται ότι αποκρυπτογραφούν την κίνηση χρησιμοποιώντας το GTK. Ωστόσο, τίποτα στο πρότυπο δεν εμποδίζει έναν κακόβουλο εγκεκριμένο πελάτη από το να εισχωρήσει πλαστογραφημένα GTK-κρυπτογραφημένα πακέτα! Εκμεταλλευόμενος την ευπάθεια, ο εισβολέας (ο εξουσιοδοτημένος χρήστης) μπορεί να "μυρίσει" και να αποκρυπτογραφήσει δεδομένα από άλλους εξουσιοδοτημένους χρήστες καθώς και να σαρώσει τις Wi-Fi συσκευές τους, να εγκαταστήσει λογισμικό κακόβουλης λειτουργίας και ενδεχομένως να συμβιβάσει αυτές τις συσκευές. Εν ολίγοις, αυτή η ευπάθεια σημαίνει ότι η προστασία των δεδομένων των ενδοχρηστών μεταξύ εξουσιοδοτημένων χρηστών είναι εγγενώς απούσα στον αέρα σε ένα WPA2 δίκτυο. Για να εκμεταλλευτεί την τρύπα 196, ένας κακόβουλος χρήστης χρειάζεται να ξέρει το GTK που διαμοιράζεται από τους εξουσιοδοτημένους χρήστες αυτού του Wi-Fi δικτύου. Έτσι μόνο το μέλος (εξουσιοδοτημένος χρήστης) ενός δικτύου WPA2, έχοντας πρόσβαση στο GTK μπορεί να εκμεταλλευτεί αυτήν την ευπάθεια.

WPA/WPA2 επίθεση TKIP

Μετά την εισαγωγή του WPA το έτος 2003, το WPA έχει υπηρετήσει πολύ καλά το σκοπό που σχεδιάστηκε και δεν ανακαλύφθηκαν ευπάθειες / exploits να στοχεύουν τα WPA enterprise τα τελευταία 5 χρόνια. Πολλοί οργανισμοί σήμερα έχουν μεταναστεύσει σε WPA τα ασύρματα πλαίσια ασφάλειάς τους. Ωστόσο, το Νοέμβριο του 2008 για πρώτη φορά, το TKIP, ένα ουσιώδες στοιχείο κρυπτογράφησης του WPA, το οποίο ανακηρύχθηκε για χρόνια ως η αντικατάσταση για τη σπασμένη κρυπτογράφηση WEP, φάνηκε να είναι ευάλωτο σε packet injection exploit (Αναβάθμιση τον Σεπτέμβριο 2009).
Ορισμένες βελτιώσεις στην ανωτέρω επίθεση έχουν αναφερθεί πρόσφατα. Η νέα ανακάλυψη έχει δραματοποιηθεί ως "σπασμένο σε 1 λεπτό". Τώρα, μια νέα μελέτη που δημοσιεύθηκε στο *International Journal of Information and Computer Security*, αποκαλύπτει ότι ένα από τα παλαιότερα ισχυρότερο ασύρματα συστήματα ασφαλείας, Wi-Fi protected access 2 (WPA2) μπορεί επίσης εύκολα να σπάσει στα ασύρματα τοπικά δίκτυα (WLANs). Ο Αχιλλέας Τσιρούλης του Πανεπιστημίου Brunel, UK, ο Δημήτρης Λαμπούδης του Πανεπιστήμιου Μακεδονίας, και ο Εμμανουήλ Τσεκλεβές του Πανεπιστήμιου Lancaster έχουν διερευνήσει τις ευπάθειες στο WPA2, παρουσιάζουν την αδυναμία του. Λένε ότι αυτό το σύστημα ασύρματης ασφαλείας θα μπορούσε τώρα να παραβιαστεί με σχετική ευκολία από κακόβουλη επίθεση στο δίκτυο. Προτείνουν ότι είναι πλέον επείγον να εργαστούν μαζί οι ειδικοί ασφαλείας και προγραμματιστές για να αφαιρέσουν τα τρωτά σημεία στο WPA2, προκειμένου να ενισχύσουν την ασφάλεια ή να αναπτύξουν εναλλακτικά.



Εικόνα 9 WPA/WPA2 επίθεση TKIP.

Η ευκολία της συνδεσιμότητας ασύρματου δικτύου των κινητών συσκευών επικοινωνίας, όπως έξυπνα τηλέφωνα, υπολογιστές tablet και φορητοί υπολογιστές, τηλεοράσεις, προσωπικοί υπολογιστές και άλλος εξοπλισμός, αντισταθμίζεται από την εγγενή ευπάθεια ασφαλείας. Η πιθανότητα για ένα τρίτο μέρος να κρυφακούσει τη μετάδοση σημάτων μεταξύ των συσκευών είναι συνεχώς παρούσα. Αντίθετα ένα ενσύρματο δίκτυο είναι εγγενώς πιο ασφαλές επειδή απαιτεί μια φυσική σύνδεση με το σύστημα προκειμένου να συλλάβει πακέτα δεδομένων. Για λόγους ευκολίας, ωστόσο, πολλοί άνθρωποι είναι έτοιμοι για συμβιβασμούς στην ασφάλεια. Μέχρι τώρα, η υπόθεση ήταν ότι ο κίνδυνος ενός εισβολέα να παραβιάσει το ασύρματο δίκτυο με ασφάλεια WPA2 ήταν επαρκώς προστατευμένη. Ο Τσιρούλης και οι συνάδελφοί του υποστηρίζουν ότι δεν είναι αυτό το θέμα. Εάν έχει ρυθμιστεί σωστά, το WPA2 το οποίο χρησιμοποιεί κλειδιά κρυπτογράφηση pre-shared key (PSK) μπορεί να είναι ασφαλές. Ανάλογα με την τρέχουσα έκδοση που είναι παρούσα στην ασύρματη συσκευή έχει επίσης το πλεονέκτημα της χρήσης ισχυρής κρυπτογράφησης με βάση είτε το temporal key integrity protocol (TKIP) ή το πιο ασφαλές counter mode με cipher block chaining message authentication code protocol (CCMP). Κρυπτογράφηση 256-Bit είναι διαθέσιμη και ένας κωδικός πρόσβασης μπορεί να είναι μια αλφαριθμητική συμβολοσειρά με ειδικούς χαρακτήρες έως 63 χαρακτήρες.
Οι ερευνητές έχουν δείξει ότι η επίθεση ωμή βίας, στον κωδικό πρόσβασης WPA2 είναι πιθανή και μπορεί να γίνει exploit, αν και ο χρόνος που απαιτείται για να εισχωρήσει στο σύστημα αυξάνει όσο μεγαλώνουν οι κωδικοί πρόσβασης. Ωστόσο, είναι το de-authentication βήμα στην ασύρματη ρύθμιση που αντιπροσωπεύει ένα πολύ πιο προσβάσιμο σημείο εισόδου για έναν εισβολέα με τα κατάλληλα εργαλεία hacking. Ως μέρος των φερόμενων πρωτόκολλα ασφαλείας τα router που χρησιμοποιούν WPA2 πρέπει να επανασυνδέονται και να επανελέγχουν την ταυτότητα των συσκευών περιοδικά και να μοιράζονται ένα νέο κλειδί κάθε φορά. Η ομάδα επισημαίνει ότι το de-authentication βήμα ουσιαστικά αφήνει μια πίσω πόρτα ξεκλείδωτη έστω και προσωρινά. Προσωρινά είναι αρκετό για ένα γρήγορο ασύρματο scanner και έναν αποφασισμένο εισβολέα. Επισημαίνουν επίσης ότι ενώ περιορίζοντας την πρόσβαση στο δίκτυο σε συγκεκριμένες συσκευές με ένα συγκεκριμένο αναγνωριστικό, τα media access control (MAC διευθύνσεις), αυτές μπορούν να πλαστογραφηθούν. Έτσι υπάρχουν διάφορα σημεία εισόδου για το WPA2 πρωτόκολλο, τα οποία η ομάδα αναφέρει με λεπτομέρειες στο βιβλίο τους. Εν τω μεταξύ, οι χρήστες θα πρέπει να συνεχίσουν να χρησιμοποιούν το πιο ισχυρό πρωτόκολλο κρυπτογράφησης που διατίθεται με το πιο περίπλοκο κωδικό πρόσβασης και να περιορίσουν την πρόσβαση σε γνωστές συσκευές μέσω MAC address, μέχρι ένα νέο σύστημα ασφαλείας να είναι διαθέσιμο.

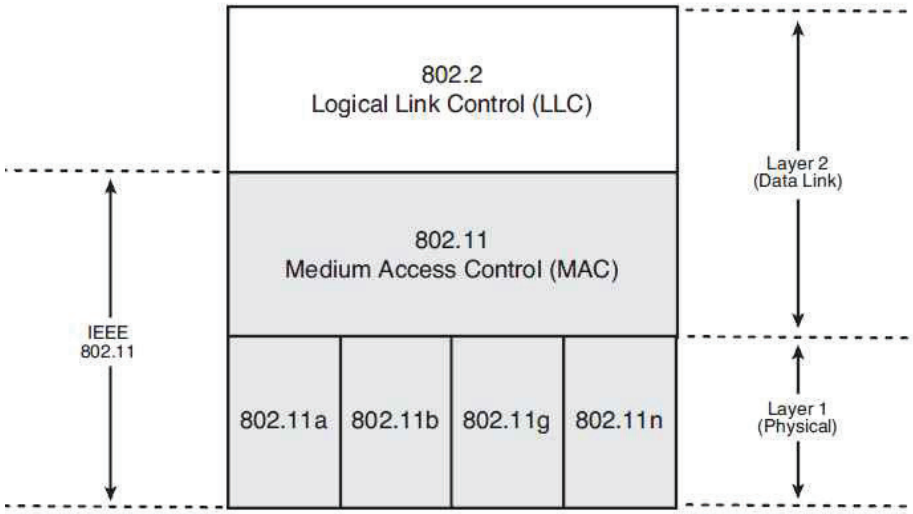
2. Ασφάλεια στα ασύρματα τοπικά δίκτυα

2.1. Ασύρματο τοπικό δίκτυο WLAN

Ασύρματο τοπικό δίκτυο είναι ένα μοιραζόμενο μέσο επικοινωνίας που διαβιβάζει πληροφορίες μέσα από ασύρματες διασυνδέσεις μεταξύ τερματικών που βρίσκονται εντός της εμβέλειάς του. Τα WLAN λειτουργούν με ένα από τα τρία ακόλουθα φυσικά μέσα: υπέρυθρες ακτίνες, μικροκύματα με διασπορά φάσματος, μικροκύματα με στενή ζώνη.
Η βασική μονάδα ενός ασύρματου τοπικού δικτύου είναι η ***κυψέλη***. Η κυψέλη είναι η περιοχή όπου λαμβάνει χώρα η ασύρματη επικοινωνία. Η περιοχή κάλυψης μιας κυψέλης εξαρτάται από την ισχύ του μεταδιδόμενου σήματος και του τύπου και της κατασκευής των τοίχων, των χωρισμάτων και άλλων φυσικών χαρακτηριστικών του εσωτερικού χώρου. Οι χρήστες έχουν τη δυνατότητα να κινούνται μέσα στην περιοχή κάλυψης μένοντας συνδεδεμένοι στο δίκτυο. Η ακτίνα δράσης μπορεί να είναι αρκετά μέτρα επιτρέποντας την διασύνδεση ενός κτιρίου, γραφείου, ή πανεπιστημιούπολης.
Υπάρχουν αρκετά πρότυπα για τα ασύρματα τοπικά δίκτυα αλλά μόνο δύο χρησιμοποιούνται: το ευρωπαϊκό πρότυπο ασύρματων τοπικών δικτύων υψηλής ταχύτητας HIPERLAN και η οικογένεια προτύπων IEEE 802.11x (γνωστό και ως *Wireless Ethernet* ή *Wi-Fi*).

2.2. Οικογένεια Προτύπων IEEE 802.11

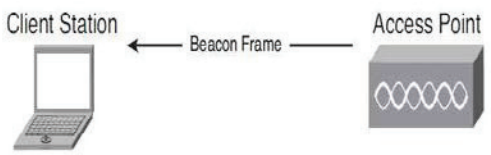
Από την δεκαετία του ’90 έχει κυριαρχήσει το πρότυπο IEEE 802.11 για ασύρματα δίκτυα ή Wi-Fi hotspots. Από λογικής απόψεως, το πρότυπο 802.11 περιγράφει τις λειτουργίες που αφορούν τα δύο πρώτα επίπεδα του OSI μοντέλου. Το Layer 1, δηλαδή το φυσικό επίπεδο (*Physical layer,* PHY) και το Layer 2, δηλαδή το επίπεδο ζεύξης δεδομένων (*data link layer*). Συγκεκριμένα καθορίζει ένα κομμάτι του δεύτερου επιπέδου, το MAC (*medium access control*) υποεπίπεδο, το οποίο αλληλεπιδρά με το 802.2 επίπεδο ελέγχου λογικού συνδέσμου (*logical link control*, LLC). Η φιλοσοφία που ακολουθεί το πρότυπο 802.11 είναι η ύπαρξη ενός μόνο MAC που όμως υποστηρίζει περισσότερα του ενός φυσικά στρώματα. Υπάρχουν αρκετά 802.11 φυσικά επίπεδα όπως τα **802.11a**, **802.11b, 802.11g** και **802.11n**.
Η τεχνολογία 802.11 προσφέρει ευρυζωνική πρόσβαση σε χρήστες που διαθέτουν ασύρματο τερματικό εξοπλισμό (κατάλληλες κάρτες δικτύου - NICs). Πρόκειται λοιπόν κυρίως για τεχνολογία εσωτερικών χώρων (indoor) και πολλαπλής πρόσβασης (*point-to-multipoint*). Ένας σταθμός βάσης εκπέμπει στις συχνότητες 2,4 (*ISM band*) και 5 GHz (*UNII band*). *Η δυνατότητα μετάδοσης εξαρτάται από το πρότυπο.*
Η κύρια υπηρεσία του προτύπου αυτού είναι η μεταφορά των M-SDU (*MAC Service Data Unit*) μεταξύ ομότιμων στρωμάτων ζεύξης δεδομένων. Παράλληλα περιλαμβάνει βασικές υπηρεσίες όπως διασύνδεση με τα εξωτερικά δίκτυα, συσχέτιση ενός σταθμού με ένα σημείο πρόσβασης, επανασυσχέτιση ενός σταθμού σε περίπτωση μετακίνησης, τερματισμό της συσχέτισης, πιστοποίηση (*authentication*), ασφάλεια και διαχείριση ισχύος ενός τερματικού.



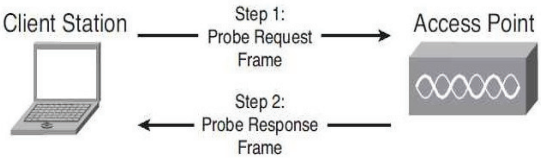
Εικόνα 10 Λειτουργίες φυσικού και MAC επιπέδου του 802.11.

2.3. Διασύνδεση συσκευών με τα ασύρματα δίκτυα

Στο 802.11 κάθε ασύρματος σταθμός πρέπει να συσχετιστεί με ένα σημείο πρόσβασης (*access point*, AP) προτού αρχίσει να μπορεί να στέλνει ή να δέχεται δεδομένα επιπέδου δικτύου. Ο διαχειριστής του δικτύου εγκαθιστά ένα AP και καταχωρεί σε αυτό ένα αναγνωριστικό συνόλου υπηρεσιών (*service set identifier*, SSID) μίας ή δύο λέξεων. Επιπλέον καταχωρεί και έναν αριθμό καναλιού.
Για να μπορέσει ένας φορητός υπολογιστής να αποκτήσει πρόσβαση στο Internet πρέπει να έχει μια κάρτα δικτύου η οποία στέλνει το δικό της ραδιοσήμα σε ένα ασύρματο δρομολογητή ο οποίος με την σειρά του συνδέεται στη πηγή παροχής Internet μέσω θύρας Ethernet, καλωδίου ή DSL modem και αναγνωρίζεται από τον φορητό υπολογιστή μόνο αν αυτός είναι εντός της εμβέλειάς του. Ο δρομολογητής μετατρέπει τα ψηφιακά σήματα σε υψηλής συχνότητας ραδιοσήματα.
Υπάρχει πολλές φορές το ενδεχόμενο της κατάστασης *Wi-Fi jungle*. Είναι μια φυσική τοποθεσία όπου ένας ασύρματος σταθμός δέχεται ένα αρκετά ισχυρό σήμα από δύο ή περισσότερα σημεία πρόσβασης που ανήκουν σε διαφορετικό υποδίκτυο και τους έχει εκχωρηθεί ανεξάρτητα ένα κανάλι. Για να συσχετιστεί (*associate*) ο ασύρματος σταθμός με ένα μόνο από αυτά, δημιουργεί ένα εικονικό κύκλωμα μεταξύ αυτού και του σημείου πρόσβασης. Έτσι το AP στέλνει πλαίσια δεδομένων στον ασύρματο σταθμό και ο σταθμός στέλνει πλαίσια προς το Διαδίκτυο μέσω του συσχετισμένου AP.
Το 802.11 πρότυπο απαιτεί ένα AP να στέλνει περιοδικά πλαίσια συγχρονισμού (*beacon frames*) το καθένα από τα οποία περιέχει το SSID και τη MAC διεύθυνση του AP. Ο ασύρματος σταθμός γνωρίζοντας ότι κάθε AP στέλνει πλαίσια σινιάλα, σαρώνει τα κανάλια ψάχνοντας για τέτοια πλαίσια από οποιοδήποτε AP βρίσκεται εκεί κοντά. Αφού μάθει ο σταθμός ποια είναι τα διαθέσιμα AP επιλέγει με ποιο από αυτά θα συσχετιστεί (ο χρήστης). Για την επιλογή αυτή δεν καθορίζεται αλγόριθμος αλλά αφήνεται στους σχεδιαστές του υλικού και λογισμικού της φορητής συσκευής και του 802.11 λογισμικού μέσα σε αυτή. Συνήθως συσχετίζεται με το AP του οποίου το beacon frame λαμβάνεται με την μεγαλύτερη ισχύ σήματος.
Η διεργασία σάρωσης των καναλιών και ακρόασης για beacon frames ονομάζεται παθητική σάρωση (*passive scanning*). Κατά το passive scanning ο σταθμός δεν εκπέμπει τίποτα, εξοικονομώντας έτσι ενέργεια. Ένας ασύρματος υπολογιστής μπορεί να κάνει επίσης ενεργή σάρωση (*active scanning*) εκπέμποντας περιοδικά σε όλα τα διαθέσιμα κανάλια *Probe Request* πλαίσια που περιέχουν και το SSID (ή network name) του δικτύου που ψάχνει. Επίσης έχει προβλεφθεί κάποια διαδικασία ώστε να καταλαβαίνει ο σταθμός πότε ένα κανάλι είναι ανενεργό.



Εικόνα 11 Παθητική Σάρωση.



Εικόνα 12 Ενεργητική Σάρωση.

Αφού επιλέξει με ποιο AP θα συνδεθεί, ο ασύρματος σταθμός στέλνει ένα πλαίσιο αίτησης συσχέτισης στο AP και το AP αποκρίνεται με ένα πλαίσιο απόκρισης συσχέτισης. Αφού συσχετιστεί με ένα AP ο ασύρματος σταθμός θα θέλει να συνδεθεί στο υποδίκτυο στο οποίο ανήκει το AP υπό την έννοια της διευθυνσιοδότησης IP. Στέλνει έτσι ένα μήνυμα ανακάλυψης DHCP στο υποδίκτυο, μέσω του AP ώστε να πάρει μια διεύθυνση στο υποδίκτυο. Στις περισσότερες περιπτώσεις για να δημιουργηθεί μια συσχέτιση με ένα συγκεκριμένο AP, η φορητή συσκευή απαιτείται να αυθεντικοποιηθεί στο AP. Το πρότυπο 802.11 παρέχει αρκετές εναλλακτικές μεθόδους για αυθεντικοποίηση και για πρόσβαση. Κάποιοι τρόποι αποδοχής της πρόσβασης μπορεί να είναι με βάση τη διεύθυνση MAC ενός σταθμού, ή με βάση το όνομα χρήστη και τον κωδικό πρόσβασης όπου το AP επικοινωνεί με έναν εξυπηρετητή αυθεντικοποίησης (*authentication server*) μεταφέροντας πληροφορίες ανάμεσα στον ασύρματο τερματικό σταθμό και στον εξυπηρετητή αυθεντικοποίησης χρησιμοποιώντας πρωτόκολλο. Ένας τέτοιος εξυπηρετητής μπορεί να εξυπηρετεί πολλά AP κρατώντας χαμηλό το κόστος και την πολυπλοκότητα των AP.

2.4. Το φυσικό στρώμα του 802.11

Το φυσικό επίπεδο ή στρώμα εξασφαλίζει την μετάδοση των bits μέσα από τα κανάλια επικοινωνίας. Αυτό περιλαμβάνει όλες τις απαραίτητες ενέργειες που απαιτούνται για να οριστεί ο φυσικός συνδυασμός των σημάτων που στέλνονται διαμέσου του ασύρματου δικτύου. Το φυσικό επίπεδο του 802.11 ορίζει τύπους διαμορφώσεων, συχνότητες και διαδικασίες συγχρονισμού των σημάτων και περιλαμβάνει διαφορετικές προδιαγραφές φυσικού επιπέδου. Όλα τα φυσικά επίπεδα μοιράζονται κοινές λειτουργίες του υποεπιπέδου MAC.
Όταν ένας υπολογιστής συνδέεται μέσω ενός δικτυακού καλωδίου σε ένα hub, switch ή router, προκειμένου να συνδεθεί με ένα δίκτυο ή στο Internet, η κάρτα διεπαφής δικτύου (*network interface card*, NIC) στέλνει μηδέν και ένα στο καλώδιο αλλάζοντας την τάση από 5 volts σε -5 volts, με προσχεδιασμένο ρυθμό. ***Το 802.11 δεν αλλάζει την τάση των καλωδίων αφού τα αντικαθιστά με μικρά, χαμηλής ενέργειας, ραδιοκύματα. Κωδικοποιεί τα δυαδικά μηδέν και ένα τοποθετώντας ένα εναλλασσόμενο ραδιοσήμα, πάνω από ένα σταθερό υπάρχον σήμα, με προκαθορισμένο ρυθμό.***

2.5. Λειτουργίες 802.11 φυσικού επιπέδου

Το πρότυπο 802.11 υποστηρίζει τις παρακάτω επιτρεπόμενες τεχνικές μετάδοσης για το φυσικό επίπεδο. Η κάθε μία κάνει δυνατή τη μετάδοση ενός πλαισίου MAC από τον ένα σταθμό στον άλλο. Οι τεχνικές διαφέρουν στη χρησιμοποιούμενη τεχνολογία και στις ταχύτητες που επιτυγχάνουν. Οι τεχνικές που χρησιμοποιούνται πλέον είναι:

- Ορθογώνια Πολύπλεξη με Διαίρεση Συχνότητας (*Orthogonal Frequency-Division Multiplexing*, OFDM)(802.11a)
- Εξάπλωση Φάσματος Άμεσης Ακολουθίας Υψηλού Ρυθμού Μετάδοσης (*High-Rate Direct-Sequence Spread-Spectrum*, HR-DSSS)(802.11b)
- *Extended-Rate PHY* (802.11g)
- *High-Throughput PHY* (802.11n)

Υπέρυθρες (Infrared)

Η υπέρυθρη επιλογή χρησιμοποιεί διάχυτη μετάδοση στα **850 ή 950nm** και επιτρέπονται δύο ταχύτητες: **1 Mbps και 2 Mbps**. Για την λειτουργία των προϊόντων υπέρυθρης μετάδοσης χρησιμοποιούνται **τρείς τεχνικές**:
Διάχυτη εκπομπή που πραγματοποιείται από έναν πανκατευθυντικό πομπό και το σήμα που παράγεται ακτινοβολείται σε όλες τις κατευθύνσεις παρέχοντας κάλυψη στους κόμβους του δικτύου.
Ανάκλαση του μεταδιδόμενου σήματος σε οροφή όπου το σήμα στοχεύεται σε ένα σημείο μιας διάχυτα ανακλαστικής οροφής και λαμβάνεται με πανκατευθυντικό τρόπο από τους δέκτες.
Εστιασμένη μετάδοση στην οποία η εμβέλεια μετάδοσης εξαρτάται από την ισχύ εκπομπής της ακτίνας και τον βαθμό εστίασής της.
Η ακτίνα λειτουργίας μπορεί να φτάσει περίπου τα 20 μέτρα, σε ελεύθερο φυσικά οπτικό πεδίο. Το υπέρυθρο φώς απορροφάται από τα σκοτεινά αντικείμενα και ανακλάται από τα φωτεινά. Έτσι, τα υπέρυθρα σήματα δεν μπορούν να διαπεράσουν τους τοίχους και οι κυψέλες που βρίσκονται σε διαφορετικά δωμάτια είναι καλά απομονωμένες η μία από την άλλη. Ωστόσο, λόγω του χαμηλού εύρους ζώνης και του γεγονότος ότι το φως του ήλιου εξαφανίζει τα υπέρυθρα σήματα, η επιλογή αυτή δεν είναι δημοφιλής.

Εξάπλωσης φάσματος ραδιοεπικοινωνίας (Spread Spectrum)

Μια από τις βασικές τεχνολογίες που κρύβονται κάτω από την οικογένεια IEEE 802.11 προτύπων είναι η ραδιοεπικοινωνία εξάπλωσης φάσματος. Αυτή η θεμελιώδης έννοια είναι η *χρήση ενός ευρύτερου εύρους ζώνης συχνότητας από αυτό που απαιτείται για τις πληροφορίες που μεταδίδονται*. Η χρησιμοποίηση του πρόσθετου εύρους ζώνης φαίνεται να είναι σπάταλη, αλλά οδηγεί πραγματικά σε διάφορα οφέλη, συμπεριλαμβανομένης της μειωμένης ευπάθειας στο μπλοκάρισμα (*jammin*g), της λιγότερης ευαισθησίας στις παρεμβολές, και τη συνύπαρξη με τις περιορισμένης ζώνης μεταδόσεις. Διάφορες τεχνικές εξάπλωσης φάσματος είναι διαθέσιμες όπως η χρονική μεταπήδηση (*time hopping*), η διαμόρφωση συχνότητας (*frequency modulation*), η *FHSS*, η *DSSS*, και τα υβρίδια αυτών. *Οι FHSS και DSSS δεν είναι τεχνικές διαμόρφωσης, αλλά μέθοδοι για να διανέμουν το ραδιοσήμα δια μέσω του εύρους ζώνης*. Εκτός από τη διάδοση του σήματος δια μέσω μιας ζώνης συχνότητας, τα συστήματα εξάπλωσης φάσματος διαμορφώνουν το σήμα. Η διαμόρφωση είναι η παραλλαγή ενός ραδιοσήματος για να μεταβιβάσει τις πληροφορίες. Το βασικό σήμα καλείται φέρον. Η παραλλαγή μπορεί να βασιστεί στην ισχύ (διαμόρφωση εύρους, *amplitude modulation* [AM]), τη συχνότητα, ή τη φάση (συχνότητα που αντισταθμίζεται) του σήματος. Η τεχνική διαμόρφωσης έχει επιπτώσεις άμεσα στον ρυθμό δεδομένων. Οι υψηλότερου ρυθμού δεδομένων διαμορφώσεις είναι γενικά πιο σύνθετες και ακριβές να εφαρμόσουν αλλά συσκευάζουν περισσότερες πληροφορίες στο ίδιο εύρος ζώνης. Οι μικρές διασπάσεις στο σήμα προκαλούν την υποβάθμιση περισσότερων δεδομένων. Αυτό σημαίνει ότι το σήμα πρέπει να έχει μια υψηλότερη αναλογία σήματος προς θόρυβο (SNR) στο δέκτη ώστε να έχει αποτελεσματική επεξεργασία. Επειδή ένα ραδιοσήμα όσο πιο κοντά είναι στην πηγή τόσο πιο ισχυρό είναι, ο λόγος SNR μειώνεται με την απόσταση. Γι' αυτό τα συστήματα υψηλής ταχύτητας έχουν μικρότερο εύρος. Παραδείγματα των τεχνικών διαμόρφωσης που χρησιμοποιούνται στα πρότυπα IEEE 802.11 περιλαμβάνουν τη δυαδική διαμόρφωση μετατόπισης φάσης (*binary phase-shift keying,* BPSK), τη διαμόρφωση τετραγωνισμού μετατόπισης φάσης (*quadrature phase-shift keying,* QPSK), την διαμόρφωση γκαουσσιανής μετατόπισης συχνότητας (*Gaussian frequency-shift keying,* GFSK), και τη CCK (*Complementary Code Keying*).

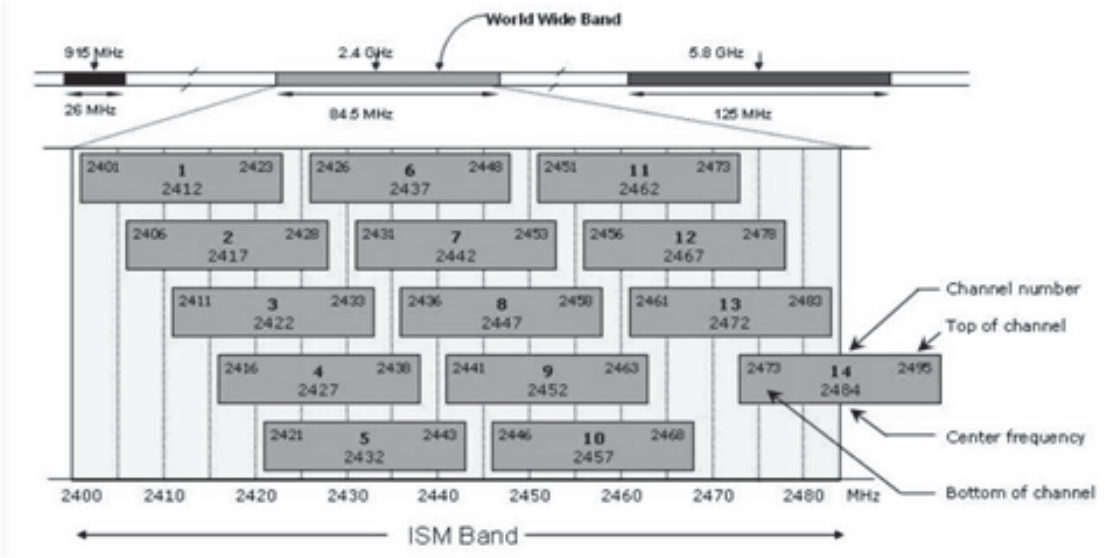
Εξάπλωση Φάσματος με Συνεχή Αλλαγή Συχνότητας (Frequency-Hopping Spread Spectrum, FHSS)

Με τη χρήση αυτής της τεχνικής, το σήμα εκπέμπεται μέσω ενός φαινομενικά τυχαίου συνόλου καναλιών συχνότητας, μεταπηδώντας (*hopping*) από συχνότητα σε συχνότητα ανά τακτά χρονικά διαστήματα στις οποίες μεταβαίνουν διαδοχικά οι σταθμοί. Η χρονική διάρκεια (*dwell time*) στην οποία μένουν οι σταθμοί στη ίδια συχνότητα ονομάζεται *chip* και είναι μία ρυθμιζόμενη παράμετρος η οποία θα πρέπει να είναι μικρότερη από 400 msec. Ο δέκτης εκτελεί την ίδια ακολουθία μεταπήδησης ενώ διατηρείται σε συγχρονισμό με τον πομπό και έτσι λαμβάνει τα δεδομένα που μεταφέρονται. Όταν βρισκόμαστε σε ένα κανάλι, το πραγματικό μεταδιδόμενο σήμα είναι το αποτέλεσμα της διαμόρφωσης της κεντρικής συχνότητας του καναλιού με το αρχικό σήμα.
Το φυσικό στρώμα αυτό, διαιρεί την ISM μπάντα των 902 MHz σε κανάλια εύρους 0,5 MHz και την μπάντα των 2,4 GHz και 5,8 GHz σε κανάλια εύρους 1 MHz. Οι προδιαγραφές της ομάδας IEEE 802.11 για το φυσικό επίπεδο FHSS υπαγορεύουν τη χρήση γκαουσιανής διαμόρφωσης μετατόπισης συχνότητας (*Gaussian Frequency Shift Keying*, GFSK) η οποία αλλάζει τη συχνότητα φέροντος για να αναπαριστά διαφορετικά δυαδικά σύμβολα για την μετάδοση δεδομένων με ταχύτητα 1 ή 2 Mbps στην ζώνη 2,4 GHz. Επιπλέον ορίζεται ότι περίπου το 99% της ενέργειας του εκπεμπόμενου σήματος πρέπει να βρίσκεται μέσα στο κανάλι. Διαφορετικά κανάλια είναι διαθέσιμα για χρήση σε διάφορες χώρες
Στις ΗΠΑ και στην Ευρώπη οι αρμόδιοι οργανισμοί έχουν θεσπίσει διαφορετικούς περιορισμούς για τα συστήματα Frequency Hopping. Για παράδειγμα, στις ΗΠΑ η FCC απαιτεί τουλάχιστον 75 διαφορετικά κανάλια (hopping channels) ενώ η Ευρωπαϊκή ETSI μόλις 20, περιορίζοντας όμως περισσότερο την ακτινοβολούμενη ισχύ. Τελικά, για να ικανοποιεί ένα προϊόν τις προδιαγραφές και της FCC και της ETSI πρέπει να ικανοποιεί τις αυστηρότερες από αυτές σε κάθε τομέα (στο παραπάνω παράδειγμα δηλαδή ένα σύστημα πρέπει να έχει τουλάχιστον 75 hopping channels και να ικανοποιεί και τους αυστηρούς περιορισμούς ισχύος της ETSI).
Όσο αναφορά την επίδοση του Frequency Hopping φυσικού στρώματος παρουσία θορύβου και παρεμβολών στενής ζώνης, αυτή είναι αρκετά καλή και μειώνεται γραμμικά όσο αυξάνονται οι παρεμβολές. Η παραγωγή της τυχαίας ακολουθίας παρέχει ένα δίκαιο τρόπο εκχώρησης του φάσματος καθώς επίσης και κάποια περιορισμένη ασφάλεια, αφού ένας εισβολέας που δεν γνωρίζει την ακολουθία συχνοτήτων ή το χρόνο παραμονής δεν μπορεί να υποκλέψει τις μεταδόσεις. Είναι επίσης ανθεκτική στις ραδιοκυματικές μεταβολές. Μεγάλες παρεμβολές σε ένα από τα χρησιμοποιούμενα κανάλια δεν προκαλεί σπουδαία ελάττωση της επίδοσης. Όσο όμως ο αριθμός των καναλιών που επηρεάζονται από τις παρεμβολές αυξάνει, η ελάττωση της επίδοσης αρχίζει να γίνεται πιο έντονη. Κύρια μειονεκτήματα αυτής της τεχνικής είναι το χαμηλό εύρος ζώνης και ότι σε μεγάλες αποστάσεις μπορεί να δημιουργήσει πρόβλημα η εξασθένηση των πολλαπλών διαδρομών.

Εξάπλωση Φάσματος Άμεσης Ακολουθίας (*Direct-Sequence Spread-Spectrum*, DSSS)

Τα συστήματα DSSS χρησιμοποιούν παρόμοια τεχνολογία με τα δορυφορικά συστήματα παγκόσμιας πλοήγησης (*Global Positioning System*, GPS) καθώς και με μερικούς τύπους κινητών τηλέφωνων.
Η βασική ιδέα της άμεσης ακολουθίας (*direct sequence*) είναι να εξαπλώσει ψηφιακά τα πλαίσια δεδομένων της βασικής μπάντας και στη συνέχεια να διαμορφώσει τα απλωμένα δεδομένα σε μια ειδική συχνότητα. Κάθε κομμάτι πληροφορίας (bit) συνδυάζεται στον πομπό με ένα μακρύτερο ψευδοτυχαίο αριθμητικό (*pseudorandom numerical*, PN) στη διαδικασία μετάδοσης. Αυτό έχει ως αποτέλεσμα ένα υψηλής ταχύτητας ψηφιακό ρεύμα (*stream*) το οποίο στη συνέχεια διαμορφώνεται σε μια συχνότητα φέροντος χρησιμοποιώντας διαφορική διαμόρφωση μετατόπισης φάσης (*differential phase-shift keying,* DPSK).

Για το φυσικό στρώμα αυτό ορίστηκαν 14 κανάλια (στην μπάντα των 2,4 GHz με εύρος 5 MHz το κάθε ένα) των οποίων 11 παρακείμενα κανάλια επικαλύπτουν μερικώς και τα υπόλοιπα 3 δεν επικαλύπτονται. Το κανάλι 1 έχει κεντρική συχνότητα τα 2,412 GHz τα υπόλοιπα ακολουθούν κάθε 5 MHz. Στην πράξη κάθε κανάλι καταλαμβάνει περίπου 22 MHz εύρος, γύρω από την κεντρική του συχνότητα. Αυτό σημαίνει ότι υποστηρίζει τρία μη επικαλυπτόμενα κανάλια για τη λειτουργία. Γίνεται χρήση RF φίλτρων για να καταπιέζονται οι πλευρικοί λοβοί έξω από τα 22 MHz. Ακόμα και έτσι, κανάλια που χρησιμοποιούνται σε διπλανές «κυψέλες» πρέπει να απέχουν μεταξύ τους 25 MHz (πέντε κανάλια των 5 MHz) για να αποφεύγονται οι παρεμβολές. Αυτό περιορίζει τον μέγιστο αριθμό καναλιών που μπορούν να χρησιμοποιηθούν. Σε κάθε χώρα επιτρέπεται η χρήση συγκεκριμένων καναλιών.



Εικόνα 13 Το 2,4 GHz κανάλι.

Τα δεδομένα στέλνονται διαμέσου ενός από αυτά τα κανάλια 22 MHz χωρίς μεταπήδηση σε άλλα κανάλια, προκαλώντας το θόρυβο στο δεδομένο κανάλι. Για να μειώσει τον αριθμό αναμεταδόσεων και θορύβου, χρησιμοποιείται διάσπαση για να μετατρέψει κάθε κομμάτι των δεδομένων χρηστών σε μια σειρά πλεοναζόντων bit, *chip*. Ο πλεονασμός κάθε *chip*, συνδυάζεται με τη διάδοση του σήματος πάνω στο κανάλι 22 MHz, παρέχοντας έλεγχο και διόρθωση λαθών για να ανακτήσει τα δεδομένα. Τα *chip* εκτείνονται από 11 bits σε εξαιρετικά επιμήκεις ακολουθίες. Η ταχύτητα με την οποία διαβιβάζονται καλείται *chipping rate*. Σε έναν παρατηρητή, αυτές οι ακολουθίες εμφανίζονται ως θόρυβος και καλούνται επίσης ψευδοτυχαίοι κώδικες θορύβου (*pseudorandom noise codes* , Pncodes). Οι Pncodes εισάγονται με διάφορες τεχνικές συμπεριλαμβανομένων των Barker κωδίκων, των Gold κωδίκων, των μ-ακολουθιών, και των κωδίκων Kasami. Ένα από τα πλεονεκτήματα τους είναι ότι ακόμα κι αν ένα ή περισσότερα από τα bit χαθούν κατά τη διάρκεια της μετάδοσης, οι ενσωματωμένες στατιστικές τεχνικές στην ραδιοσυχνότητα μπορούν να ανακτήσουν τα αρχικά δεδομένα χωρίς την ανάγκη για την αναμετάδοση. Στο δέκτη, ένα αντίστοιχο φίλτρο συσχέτισης χρησιμοποιείται για να αφαιρέσει την ακολουθία PN και να ανακτήσει το αρχικό ρεύμα δεδομένων.

802.11b: Εξάπλωση Φάσματος Άμεσης Ακολουθίας Υψηλού Ρυθμού Μετάδοσης (*High-Rate Direct-Sequence Spread-Spectrum*, HR-DSSS)

Το 802.11b είναι το πρώτο πρότυπο που χρησιμοποιήθηκε ευρέως στα τοπικά ασύρματα δίκτυα. Μπορεί να θεωρηθεί σαν επέκταση του αρχικού DSSS φυσικού στρώματος που ορίστηκε στο 802.11 και μάλιστα χρησιμοποιεί τα ίδια κανάλια με

αυτό, πετυχαίνοντας αρκετά μεγαλύτερους ρυθμούς μετάδοσης. Μόνο τρία IEEE 802.11b συστήματα DSSS μπορούν να συνδυαστούν.
Το IEEE 802.11 διευκρινίζει **δύο τύπους διαμορφώσεων DPSK** (*Differential Phase Shift Keying*) για τα συστήματα DSSS. Ο πρώτος είναι ο **BPSK** και ο δεύτερος είναι ο **QPSK**. Η διαμόρφωση μετατόπισης φάσης (*Phase-shift keying*, PSK), όπως το όνομα υπονοεί, ανιχνεύει τη φάση του ραδιοσήματος. Ο BPSK ανιχνεύει μια 180 μοιρών αντιστροφή του σήματος, που αντιπροσωπεύει ένα δυαδικό 0 ή 1. Αυτή η μέθοδος έχει ως αποτελεσματικό ρυθμό δεδομένων 1 Mbps. Ο QPSK ανιχνεύει τις 90 μοίρες μετατοπίσεις φάσης. Αυτό διπλασιάζει τον ρυθμό δεδομένων σε 2 Mbps. Το IEEE 802.11b προσθέτει τη CCK (*Co Complementary Code Keying*) και τη δυαδική συνελικτική κωδικοποίηση πακέτων (*packet binary convolutional coding*, PBCC). Υποστηρίζει ρυθμούς δεδομένων **1, 2, 5.5, ή 11 Mbps**. Σε ενδοκτιριακές εφαρμογές πετυχαίνει κάλυψη ως **150 μέτρα**.

802.11a: Ορθογώνια Πολυπλεξία με Διαίρεση Συχνότητας (*Orthogonal Frequency-Division Multiplexing*, OFDM)

Το IEEE 802.11 φυσικό επίπεδο ορθογώνιας πολυπλεξίας με διαίρεση συχνότητας (OFDM) μεταφέρει **6 Mbps έως 54 Mbps ρυθμούς δεδομένων σε ζώνη UNII 5 GHz** και αναφέρεται ως 802.11a. Η 802.11a τροποποίηση στο πρότυπο επικυρώθηκε το 1999, αλλά τα προϊόντα έγιναν διαθέσιμα το 2001 που ήταν αρκετό καιρό μετά τα δίκτυα 802.11b. Χρησιμοποιεί BPSK, QPSK, και QAM για να επιτύχει τους διάφορους ρυθμούς δεδομένων. Βασισμένο σε μια μαθηματική διαδικασία αποκαλούμενη γρήγορο μετασχηματισμό κατά Φουριέ (*Inverse FFT*), επιτρέπει σε 52 κανάλια να επικαλύπτονται παραμένοντας ξεχωριστά και ορθογώνια μεταξύ τους. Η επικάλυψη των καναλιών είναι μια αποδοτικότερη χρήση του φάσματος και επιτρέπει την αποτελεσματικότερη επεξεργασία του στον δέκτη. Οι συχνότητες λειτουργίας ποικίλλουν ανάλογα με την χώρα εφαρμογής του ασύρματου δικτύου. Το IEEE 802.11a OFDM δεν είναι είδος τεχνικής εξάπλωσης φάσματος. Αντιθέτως, διαιρεί τη συχνότητα φέροντος σε 52 χαμηλής ταχύτητας υποφέροντα που περιέχονται σε 20 MHz κανάλι. Σαράντα οκτώ (48) από αυτά χρησιμοποιούνται για τα δεδομένα και τέσσερα (4) χρησιμοποιούνται συγχρονισμό στο δέκτη.
Ένα από τα μεγαλύτερα πλεονεκτήματα της OFDM είναι η αντίστασή του στην παρέμβαση της πολυόδευσης και στην καθυστέρηση διάδοσης. Η πολυόδευση προκαλείται όταν τα ραδιοκύματα ανακλώνται και περνούν μέσω των αντικειμένων στο περιβάλλον. Τα ραδιοκύματα εξασθενούν ή αποδυναμώνονται σε ένα ευρύ φάσμα ανάλογα με το υλικό του αντικειμένου. Μερικά υλικά (όπως το μέταλλο) είναι αδιαφανή στις ραδιομεταδόσεις. Ένα περιβάλλον με πολλά εμπόδια είναι πολύ διαφορετικό από ένα ανοικτό περιβάλλον για τη μετάδοση και λήψη ραδιοκυμάτων. Αυτή η περιβαλλοντική μεταβλητότητα είναι ο λόγος που είναι τόσο δύσκολο να εκτιμηθεί ο ρυθμός δεδομένων και το εύρος ενός IEEE 802.11 συστήματος. Λόγω των αντανακλάσεων και της εξασθένησης, μια μοναδική μετάδοση μπορεί να έχει διαφορετική ισχύ σήματος από διαφορετικές κατευθύνσεις ανάλογα με τους τύπους υλικών που αντιμετωπίζει.
Η καθυστέρηση στην διάδοση συνδέεται με το φαινόμενο πολυόδευσης. Επειδή το σήμα ταξιδεύει μέσα από τις διαφορετικές πορείες μέχρι να καταλήξει στον δέκτη, το σήμα φθάνει σε διαφορετικούς χρόνους. Όσο ο ρυθμός μετάδοσης αυξάνεται τόσο αυξάνεται και η πιθανότητα της παρέμβασης από προηγούμενα μεταδοθέντα σήματα.
Η OFDM δεν είναι μια νέα τεχνική διαφέρει όμως από άλλες αναδυόμενες τεχνικές κωδικοποίησης όπως η πολλαπλή πρόσβαση με διαίρεση κώδικα (*Code Division Multiple Access* ,CDMA). Η CDMA χρησιμοποιεί τις σύνθετες μαθηματικές μετατροπές για να τοποθετήσει πολλές μεταδόσεις πάνω σε ένα μοναδικό φέρον. Η OFDM κωδικοποιεί μια ενιαία μετάδοση σε πολλαπλά υποφέροντα κρύβοντας λιγότερα μαθηματικά από την CDMA. Οι συσκευές OFDM χρησιμοποιούν ένα ευρύ κανάλι συχνότητας και το σπάνε σε πολλαπλά υποκανάλια. Κάθε υποκανάλι

χρησιμοποιείται για να διαβιβάσει τα δεδομένα. Όλα τα υποκανάλια πολυπλέκονται έπειτα και συνδιάζονται σε ένα κανάλι.[8]
Παρόλα αυτά οι υψηλότερες ραδιοσυχνότητες μειώνουν κατά πολύ την απόσταση κάλυψης καθώς και την διεισδυτική δύναμη του 802.11a , ειδικά σε εσωτερικούς χώρους. Εκεί που μια μετάδοση 802.11b θα περνούσε έναν τοίχο, μια μετάδοση 802.11a μπορεί να εμποδιστεί. Το γεγονός αυτό μπορεί να εμποδίσει την εγκατάσταση σε μεγάλη κλίμακα ενός δικτύου 802.11a καθώς απαιτούνται πιο πολλά Access Points για την κάλυψη του χώρου.

Channel Identifier	Frequency (in MHz)	Regulatory Domains			
		Americas	EMEA	Japan	Rest of World
34	5170	-	-	x	-
36	5180	x	x	-	x
38	5190	-	-	x	-
40	5200	x	x	-	x
42	5210	-	-	x	-
44	5220	x	x	-	x
46	5230	-	-	x	-
48	5240	x	x	-	x
52	5260	x	x	-	x
56	5280	x	x	-	x
60	5300	x	x	-	x
64	5320	x	x	-	x
100	5500	-	x	-	x
104	5520	-	x	-	x
108	5540	-	x	-	x
112	5560	-	x	-	x
116	5580	-	x	-	x
120	5600	-	x	-	x
124	5620	-	x	-	x
128	5640	-	x	-	x
132	5660	-	x	-	x
136	5680	-	x	-	x
140	5700	-	x	-	x
149	5745	x	-	-	x
153	5765	x	-	-	x
157	5785	x	-	-	x
161	5805	x	-	-	x

Εικόνα 14 Τα 802.11a κανάλια.

802.11g: Extended-Rate PHY

Τον Ιούνιο του 2003 η ομάδα εργασίας IEEE ολοκλήρωσε τις εργασίες της και εξέδωσε το πρότυπο 802.11g. Το 802.11g είναι ένας συνδυασμός των παραλλαγών 802.11a και 802.11b, δηλαδή επιτυγχάνονται **υψηλοί ρυθμοί μετάδοσης της τάξης των 54 Mbps**, διατηρώντας παράλληλα τη προς πίσω συμβατότητα με το διαδεδομένο 802.11b. Χρησιμοποιεί διαμόρφωση OFDM (όπως το 802.11a), καθώς και τη διαμόρφωση CCK ενώ λειτουργεί στη ζώνη συχνοτήτων **ISM 2,4 Ghz** (όπως το 802.11b).
Το 802.11g αντιμετωπίζει τους περιορισμούς σε bandwidth του 802.11b και παράλληλα προσφέρει την διεισδυτική δύναμη της μπάντας των μικροκυμάτων καθώς και την ικανότητα μετάδοσης σε μεγάλες αποστάσεις. Παρόλα αυτά δεν περιορίζει το πρόβλημα της συμφόρησης στην συγκεκριμένη μπάντα στην οποία λειτουργούνε πολλές συσκευές. Το 802.11g είναι επίσης περιορισμένο σε τρία μη αλληλοεπικαλυπτόμενα κανάλια όπως και ο προκάτοχος του, το 802.11b. Το 802.11g μπορεί να έχει τα ίδια προβλήματα απόδοσης όπως και το 802.11b λόγω της συμβατότητας προς τα πίσω που έχει. Εάν ένας σταθμός 802.11b είναι παρόν σε ένα δίκτυο 802.11g, όλοι οι σταθμοί θα πρέπει να χρησιμοποιήσουν την διαμόρφωση σήματος του 802.11b για συμβατότητα. Παρόλα αυτά σε ένα καθαρά 802.11g δίκτυο μπορεί κάποιος να εκμεταλλευτεί πλήρως τις ικανότητες της

τεχνολογίας. Επίσης μια εξωτερική κεραία που λειτουργεί σε 802.11b δίκτυο μπορεί να λειτουργήσει και σε 802.11g μειώνοντας έτσι το κόστος αναβάθμισης.

Channel Identifier	Frequency (in MHz)	Regulatory Domains			
		Americas	EMEA	Japan	Rest of World
1	2412	x	x	x	x
2	2417	x	x	x	x
3	2422	x	x	x	x
4	2427	x	x	x	x
5	2432	x	x	x	x
6	2437	x	x	x	x
7	2442	x	x	x	x
8	2447	x	x	x	x
9	2452	x	x	x	x
10	2457	x	x	x	x
11	2462	x	x	x	x
12	2467	-	x	x	x
13	2472	-	x	x	x
14	2484	-	-	x	-

Εικόνα 15 Τα κανάλια 802.11b/g.

802.11n: High-Throughput PHY

Στις αρχές του 2004, το IEEE ανακοίνωσε ότι σχημάτισε μια νέα ομάδα εργασίας, η οποία ονομάζεται Task Group n ή TGn. Η ομάδα αυτή ανέλαβε την δημιουργία μιας τροποποίησης του αρχικού προτύπου 802.11, με σκοπό την επίτευξη πραγματικού ρυθμού μεταφοράς τουλάχιστον 100 Mbps. Αυτό σημαίνει ότι ο θεωρητικός ρυθμός μεταφοράς θα πρέπει να είναι τουλάχιστον **600 Mbps**. Ο μέγιστος ρυθμός δεδομένων εξαρτάται από τα ποιά χαρακτηριστικά 802.11n υποστηρίζονται μεταξύ των 802.11n συσκευών και από το τί υποστηρίζει το περιβάλλον. Για να επιτευχθούν τέτοιες ταχύτητες επιβάλλεται η μετάβαση σε νέες τεχνολογίες ασύρματης μετάδοσης και στη συγκεκριμένη περίπτωση, θα χρησιμοποιηθεί η **τεχνολογία MIMO** (*Multiple Input – Multiple Output*). Η ονομασία προήλθε από το γεγονός ότι η τεχνολογία αυτή χρησιμοποιεί πολλαπλές κεραίες για την αποστολή και λήψη δεδομένων και οι οποίες λειτουργούν ταυτόχρονα και ανεξάρτητα η κάθε μία. Αυτό το πρότυπο επικυρώθηκε το 2009 και λειτουργεί στις μπάντες συχνοτήτων **2,4 GHz και 5GHz** και είναι προς τα πίσω συμβατό με το 802.11a και 802.11b/g. Το 802.11n δεσμεύει 2 κανάλια των 20 MHz σε ένα των 40 MHz.

Channel Identifier	Frequency (in MHz)	Regulatory Domains			
		Americas	EMEA	Japan	Rest of World
(36, 1) (40,-1)	5190	x	-	x	-
(44, 1) (48,-1)	5230	x	-	x	-
(52, 1) (56,-1)	5270	x	-	x	-
(60, 1) (64, -1)	5310	x	-	-	x
(100, 1) (104, -1)	5510	-	x	-	x
(108, 1) (112, -1)	5550	-	x	-	x
(116, 1) (120, -1)	5590	-	x	-	x
(124, 1) (128,-1)	5630	-	x	-	x
(132, 1) (136,-1)	5670	-	x	-	x
(149, 1) (153,-1)	5755	x	-	-	x
(157, 1) (161,-1)	5795	x	-	-	x

Εικόνα 16 Τα κανάλια 802.11n.

2.6. Το υπόστρωμα MAC του 802.11

Το 802.11 MAC είναι κοινό για όλα τα IEEE 802.11 PHY στρώματα και είναι αρμόδιο για τη διαχείριση της μεταφοράς δεδομένων από τις υψηλότερου επιπέδου λειτουργίες στα φυσικά μέσα. Εδρεύει εντός του επιπέδου κατάστασης συνδέσμων και επιτρέπει σε πολλαπλές συσκευές πελατών (αναφέρονται συνήθως ως σταθμοί) να μοιράζονται το κοινό μέσο μετάδοσης του αέρα μέσω ενός *carrier sense* πρωτόκολλου. Αυτό το πρωτόκολλο συντονίζει την πρόσβαση στο κοινό μέσο έτσι ώστε οι σταθμοί να μπορούν να μοιράζονται την ίδια συχνότητα και τον ίδιο χώρο στο ραδιοφάσμα. Οι λειτουργίες του MAC παρέχουν επίσης αξιόπιστη μετάδοση των δεδομένων πάνω από το αρκετά επιρρεπές, και σε μεγάλο βαθμό, σε σφάλματα ασύρματο μέσο. Για να γίνει πιο κατανοητό, θεωρούμε μια αίθουσα με ανθρώπους που λαμβάνουν μέρος στην ίδια συζήτηση. Κάθε άτομο μπορεί να ακούσει αν κάποιος μιλάει. Αυτό αντιπροσωπεύει μια ολοκληρωμένη τοπολογία bus όπου ο καθένας επικοινωνεί χρησιμοποιώντας την ίδια συχνότητα (φωνή) και τον ίδιο χώρο (την αίθουσα). Για να αποφύγουμε να μιλάνε ταυτόχρονα δύο άνθρωποι, όταν κάποιος θελήσει να πει κάτι, θα πρέπει να περιμένει μέχρι ένα άλλο άτομο σταματήσει να μιλάει. Αυτό το απλό πρωτόκολλο βεβαιώνει ότι μόνο ένα άτομο μιλάει σε δεδομένη χρονική στιγμή, προσφέροντας με αυτόν τον τρόπο μία διαμοιραζόμενη χρήση του κοινού μέσου επικοινωνίας.

Το 802.11 λειτουργεί με παρόμοιο τρόπο. Όταν ένας σταθμός θέλει να μεταδώσει δεδομένα, "ακούει" πρώτα το μέσο και αν είναι αδρανές (*idle*), δηλαδή δεν χρησιμοποιείται από κάποιον άλλον σταθμό, αρχίζει την μετάδοση των δεδομένων εξαρτώμενο από επιπρόσθετους κανόνες που ορίζει το πρότυπο. Αν το μέσο είναι απασχολημένο ο σταθμός αναβάλλει την μετάδοση. Αυτό το πρωτόκολλο αναφέρεται ως πολλαπλή πρόσβαση με ανίχνευση φέροντος (*carrier sense multiple access*, CSMA).

Το 802.11 ανταπεξέρχεται στον έλεγχο λαθών έχοντας σε κάθε σταθμό έλεγχο στα εισερχόμενα δεδομένα για αλλαγμένα bits. Αν ο σταθμός προορισμού δεν αντιληφθεί σφάλματα, στέλνει μια επιβεβαίωση πίσω στον σταθμό-πηγή. Σε αντίθετη περίπτωση, αν αντιληφθεί σφάλματα, το πρωτόκολλο data-link βεβαιώνει ότι ο σταθμός-πηγή θα ξαναστείλει το πακέτο. Λόγω καθυστερήσεων στην διάδοση, είναι πιθανό δύο ασύρματοι σταθμοί να ανιχνεύσουν ότι το μέσο δεν είναι απασχολημένο και να αρχίσουν και οι δύο να μεταδίδουν. Για να αποφύγει το

802.11 την πρόσκρουση αυτή, οι δύο σταθμοί σταματούν τη μετάδοση, περιμένουν για κάποιο χρονικό διάστημα και προσπαθούν ξανά.

Υπηρεσίες MAC στρώματος

Το MAC παρέχει τις παρακάτω εννέα λογικές υπηρεσίες. Ένα AP χρησιμοποιεί και τις εννέα υπηρεσίες. Ένα τελικό σημείο χρησιμοποιεί την επικύρωση, το deauthentication, τη μυστικότητα, και την παράδοση στοιχείων. Κάθε υπηρεσία χρησιμοποιεί ένα σύνολο μηνυμάτων με τα στοιχεία πληροφοριών που αρμόζουν στις υπηρεσίες.

1 **Distribution:** Η υπηρεσία αυτή είναι απαραίτητη για την παράδοση ενός πλαισίου από το AP στον τελικό προορισμό του. Συνίσταται στον εντοπισμό του παραλήπτη, ώστε να γίνει εφικτή η τελική παράδοση του πλαισίου. Έτσι λαμβάνεται απόφαση αν ένα πλαίσιο πρέπει να σταλεί στο ίδιο BSS ή πρέπει να σταλεί στο DS προς παράδοση σε σταθμό συσχετιζόμενο με άλλο AP.
2 **Integration:** Η υπηρεσία αυτή παρέχεται από το σύστημα διανομής. Είναι υπεύθυνη για τη διασύνδεση του συστήματος διανομής DS σε ένα δίκτυο διαφορετικό του 802.11. Στην ουσία είναι υπεύθυνη για την μετάφραση των πλαισίων από τον ένα τύπο στον άλλο.
3 **MSDU Delivery:** Η παράδοση των πλαισίων MAC (*MAC Service Data Unit*) στον τελικό προορισμό τους.
4 **Association:** Απαραίτητη διαδικασία συσχετισμού ενός σταθμού με το AP, προκειμένου να είναι σε θέση να στείλει και να δεχτεί πλαίσια μέσω του ασυρμάτου δικτύου. Όταν ένας σταθμός είναι συσχετισμένος με ένα AP, δημιουργείται τότε μια λογική σχέση μεταξύ τους, ώστε το DS να γνωρίζει που και πώς να παραδώσει δεδομένα σε έναν ασύρματο σταθμό.
5 **Reassociation:** Χρησιμοποιείται από τους κινητούς σταθμούς σε περίπτωση μετακίνησης από μία BSS σε μία άλλη. Είναι μέρος του μηχανισμού της διαπομπής.
6 **Disassociation:** Η διαδικασία αυτή αφαιρεί έναν σταθμό από το δίκτυο. Το MAC του 802.11 μπορεί να χειριστεί και σταθμούς που εγκαταλείπουν το δίκτυο χωρίς να κάνουν πρώτα disassociation.
7 **Authentication:** Αν απαιτείται από το διαχειριστή του δικτύου, πρέπει κάθε χρήστης να πιστοποιεί την ταυτότητά του πριν να προχωρήσει στη διαδικασία του association.
8 **Deauthentication:** Τερματισμός μιας ισχύουσας κατάστασης authentication. Τερματίζει επίσης και το association, εφόσον το authentication είναι προαπαιτούμενο αυτού.
9 **Privacy:** Λόγω του ασύρματου περιβάλλοντος μετάδοσης έχει οριστεί από το 802.11 μία προαιρετική υπηρεσία κρυπτογράφησης των δεδομένων που ονομάζεται WEP (*Wired Equivalent Privacy*) το οποίο είναι πολύ αδύναμη κρυπτογράφηση που εύκολα μπορεί να σπάσει κάποιος.

2.7. Ασφάλεια στα ασύρματα δίκτυα

Τα Wi-Fi μπορεί να είναι λιγότερο ασφαλή συγκριτικά με τις ενσύρματες συνδέσεις, όπως το Ethernet, αφού ο εισβολέας δεν χρειάζεται μια φυσική σύνδεση. Οι σελίδες Web οι οποίες χρησιμοποιούν SSL είναι ασφαλείς αλλά η μη κρυπτογραφημένη πρόσβαση μπορεί πολύ εύκολα να ανιχνευτεί από τους εισβολείς στο διαδίκτυο. Λόγω αυτού του γεγονότος, τα Wi-Fi υιοθέτησαν ποικίλες τεχνολογίες κρυπτογράφησης. Η αρχική κρυπτογράφηση, το WEP, αποδείχτηκε εύκολο να σπάσει. Υψηλότερης ποιότητας πρωτόκολλα όπως (WPA, WPA2) προστέθηκαν αργότερα. Ένα προαιρετικό χαρακτηριστικό προστέθηκε το 2007, με την ονομασία Wi-Fi Protected Setup (WPS) το οποίο είχε ένα σημαντικό ελάττωμα που επέτρεπε στον εισβολέα να ανακτήσει τον κωδικό πρόσβασης του router. Η

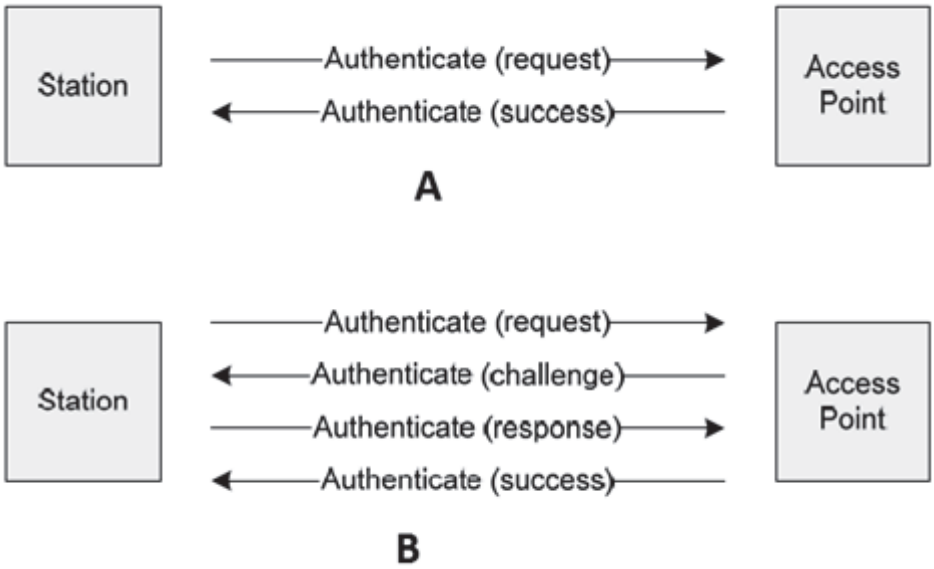
Wi-Fi Alliance έχει ενημερώσει από τότε τα σχέδια δοκιμασιών της και τα προγράμματα πιστοποίησης για να διασφαλίσει ότι όλες οι νέες πιστοποιημένες συσκευές αντιστέκονται στις επιθέσεις. Παρακάτω παρουσιάζονται αναλυτικά οι τεχνικές ασφάλειας που εφαρμόστηκαν στα ασύρματα δίκτυα κατά χρονολογική σειρά.

2.8. Pre-RSN Πιστοποίηση

Εάν ένας σταθμός λαμβάνει ένα αίτημα συσχέτισης (*association request*) από έναν σταθμό που δεν είναι πιστοποιημένος με αυτόν, στέλνει μια ειδοποίηση *deauthentication* στον αιτούντα. Η πιστοποίηση επιτυγχάνεται από μια ανταλλαγή των πακέτων διαχείρισης (*management packets*) τα οποία χρησιμοποιούνται για να υποστηρίξουν την πιστοποίηση, την συσχέτιση, και το συγχρονισμό. Το πρότυπο 802.11 υποστηρίζει διάφορους τύπους πιστοποίησης.

Τα αρχικά πρότυπα παρείχαν μόνο δύο μορφές πιστοποίησης: ανοικτού συστήματος και κοινού κλειδιού.

Πιστοποίηση ανοικτού συστήματος (Open system authentication): Αυτή είναι η προκαθορισμένη μέθοδος πιστοποίησης του 802.11. Οποιοσδήποτε κόμβος, συμβατός με το πρότυπο, πιστοποιείται αυτόματα. Συγκεκριμένα, ο σταθμός που θέλει να χρησιμοποιήσει την υπηρεσία στέλνει ένα πλαίσιο ελέγχου με την ταυτότητα του αποστολέα και ο σταθμός που το λαμβάνει στέλνει ως απάντηση ένα πλαίσιο, με το οποίο αναγνωρίζει ή όχι την ταυτότητα του αποστολέα.
Πιστοποίηση κοινού κλειδιού (Shared key authentication): Αυτός ο τύπος πιστοποίησης προϋποθέτει ότι όλοι οι σταθμοί έχουν λάβει μέσω ενός καναλιού (ανεξάρτητου από το 802.11 δίκτυο) ένα μυστικό κλειδί, με τη χρήση του οποίου λαμβάνει χώρα η πιστοποίηση. Για τη χρήση αυτής της μεθόδου εφαρμόζεται ο αλγόριθμος WEP (Wired Equivalent Privacy) και ο κόμβος πρέπει να αποδείξει ότι ξέρει ένα από τα κλειδιά WEP που λειτουργούν στο δίκτυο.



Εικόνα 17 A) Open System Authentication B) Shared Key Authentication.

Αυτές οι αρχικές μέθοδοι πιστοποίησης, που σχετίζονται με συστήματα pre-RSN (*pre-Robust Security Network)*, υποστηρίζονται ακόμα, αλλά η αναθεώρηση 802.11i πρόσθεσε επιπλέον βήματα για τα δίκτυα που χρησιμοποιούν νεώτερες μεθόδους κρυπτογράφησης. Για να αποφευχθούν οι σύνθετες αλλαγές στο αρχικό πρωτόκολλο, αυτές οι νεώτερες μέθοδοι πρώτα χρησιμοποιούν την παλαιότερη ανοικτού συστήματος πιστοποίηση, έπειτα δημιουργούν μια νέα συσχέτιση ασφάλειας μεταξύ των δύο κόμβων κατά τη διάρκεια της φάσης συσχέτισης που

ακολουθεί αμέσως. *Η συσχέτιση ασφάλειας περικλείει και την πιστοποίηση και την κρυπτογράφηση* και μπορεί να αντιμετωπιστεί από έναν ξεχωριστό 802.1x εξυπηρετητή πιστοποίησης (*authentication server*), ή να βασίζεται στην επίδειξη της κατοχής του σωστού προ-κοινού κλειδιού (*Pre-Shared key, PSK*). Το πρότυπο υποστηρίζει επίσης ένα προαιρετικό μέτρο της προ-πιστοποίησης (*pre-authentication*) για roaming σε ένα ESS από τους σταθμούς που πιστοποιήθηκαν ήδη με το δίκτυο.

2.9. Κρυπτογράφηση WEP (Wired Equivalent Privacy)

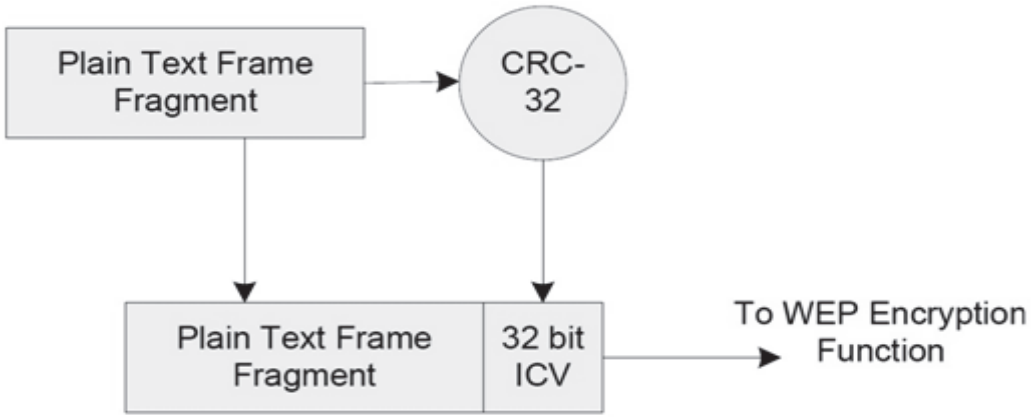
Η πιο γνωστή επιλογή παροχής ασφάλειας, που ορίστηκε για τα ασύρματα δίκτυα από το αρχικό πρότυπο 802.11, είναι το WEP. Με την επιλογή του WEP ένα κοινό κλειδί μοιράζεται ανάμεσα στο σημείο πρόσβασης και στους ασύρματους πελάτες του. Εάν επιθυμούμε εμπιστευτικότητα, μπορούμε να χρησιμοποιήσουμε την επιλογή του WEP και να κρυπτογραφήσουμε τα δεδομένα πριν αυτά σταλούν. Το WEP χειρίζεται ταυτόχρονα τόσο την προστασία όσο και την ακεραιότητα των δεδομένων.

Κατακερματισμός

Το πακέτο δεδομένων, που μεταδίδεται, περιέχει τις κατάλληλες πληροφορίες για την αποστολή του και καλείται MSDU (*Mac Service Data Unit*). Το πακέτο αυτό χωρίζεται σε μικρότερα κομμάτια, με τη διαδικασία του κατακερματισμού (*fragmentation*). Κάθε κομμάτι ακολουθεί τη δική του πορεία στην κρυπτογράφηση WEP. Επομένως το αρχικό πακέτο δεδομένων χωρίζεται σε μικρότερα μηνύματα, MPDU (Mac Protocol Data Unit) στα οποία προστίθενται και άλλα bytes. Έπειτα, τα δεδομένα καταφθάνουν στο επίπεδο MAC του προορισμού και σκοπός είναι να περάσουν στο λειτουργικό σύστημα και να μετατεθούν στην κατάλληλη εφαρμογή.

Εξασφάλιση Ακεραιότητας Δεδομένων

Η εξασφάλιση της ακεραιότητας του μηνύματος στο WEP βασίζεται στον αλγόριθμο *CRC-32*. Ο αλγόριθμος CRC-32 εφαρμόζεται στο απλό κείμενο και παράγει την τιμή ελέγχου ακεραιότητας (ICV - *Integrity Check Value*) μήκους 4 bytes (32bits) και συνεισφέρει στην αποφυγή της τροποποίησης του μηνύματος κατά τη μετάδοση. Η τιμή αυτή προστίθεται στο τέλος του πλαισίου πριν από την επεξεργασία για μετάδοση. Αυτή η πληροφορία αργότερα κρυπτογραφείται μαζί με το απλό κείμενο, με τον RC4 αλγόριθμο. Η κρυπτογράφηση του ICV μαζί με το απλό κείμενο κάνει δύσκολη την τροποποίηση των κρυπτογραφημένων δεδομένων και του ICV, με τέτοιο τρόπο ώστε το νέο ICV να ανταποκρίνεται στα τροποποιημένα δεδομένα. Αν αλλάξει έστω και ένα bit από το μήνυμα, ο παραλήπτης θα υπολογίσει διαφορετική τιμή του CRC από αυτή που μεταφέρει ο πομπός και επομένως θα απορρίψει το μήνυμα. Παρόλο που ο έλεγχος εντοπίζει τυχαία λάθη, δεν είναι δυνατόν να αναγνωρίσει σκόπιμα λάθη, καθώς ο εισβολέας είναι σε θέση να υπολογίσει τη νέα τιμή CRC και να αντικαταστήσει την αρχική. Ο αλγόριθμος CRC-32 περιγράφεται στο RFC 3309.



Εικόνα 18 Εξασφάλιση ακεραιότητας δεδομένων με τον αλγόριθμο CRC-32.

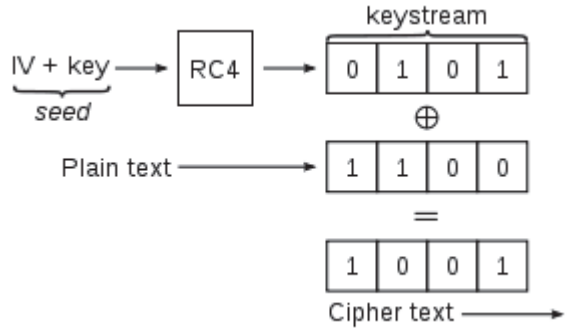
Αλγόριθμος Κρυπτογράφησης

Το WEP κάνει χρήση του αλγόριθμου κρυπτογράφησης RC4. Ο συγκεκριμένος αλγόριθμος είναι απλός στην υλοποίηση του και αρκετά ισχυρός. Οι αδυναμίες του WEP δεν οφείλονται στον ίδιο τον RC4 αλλά στον τρόπο χρήσης του μέσα στον WEP.
Ο RC4 είναι ένας συμμετρικός αλγόριθμος (χρησιμοποιεί το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση) και είναι αλγόριθμος συρμού *(stream cipher)*. Αυτό σημαίνει ότι το κλειδί θεωρείται ως ένας συρμός (*stream*) από bits και εφαρμόζεται στο απλό κείμενο (*Plain Text*) bit προς bit για να παραχθεί το κρυπτογραφημένο κείμενο (*Cipher Text*). Αυτό έχει το πλεονέκτημα ότι μπορεί να εφαρμοστεί σε κείμενο μεταβλητού μεγέθους, σε αντίθεση με τους *Block Ciphers* που εφαρμόζονται σε κομμάτια *(blocks)* κειμένου σταθερού μεγέθους (συνήθως 64 bits).
Ο RC4 περιλαμβάνει δύο φάσεις: Την παραγωγή του συρμού κλειδιού *(Key Stream)* και την κρυπτογράφηση του καθαρού κειμένου.
Για την παραγωγή του *keystream* ο RC4 δέχεται σαν είσοδο ένα *seed* και χρησιμοποιεί μια διαδικασία παραγωγής ψευδοτυχαίων αριθμών. Με βάση την ιδιότητα της XOR:

A (XOR) B= C, τότε C (XOR) B = A
Ο αλγόριθμος RC4 εκμεταλλεύεται την παραπάνω ιδιότητα ως εξής:

Κρυπτογράφηση: **plaintext (XOR) keystream = cipher text**
Αποκρυπτογράφηση: **cipher text (XOR) keystream = plaintext**

Η τυχαία ακολουθία κλειδιού ορίζεται από το IV και ονομάζεται ψευδοτυχαία διότι θα πρέπει να δείχνει τυχαία σε εισβολέα αλλά τα δυο άκρα της ζεύξης που επικοινωνούν θα πρέπει να παράγουν την ίδια τυχαία τιμή για κάθε byte που επεξεργάζονται.
Η πράξη XOR υλοποιείται πολύ εύκολα οπότε, το πιο δύσκολο κομμάτι αποτελεί ο υπολογισμός μιας καλής ψευδοτυχαίας ροής bytes. Ουσιαστικά χρειαζόμαστε ένα ψευδοτυχαίο byte για κάθε byte του μηνύματος προς κρυπτογράφηση.



Εικόνα 19 Παραγωγή του κρυπτογραφημένου κειμένου με τον αλγόριθμο RC4.

Seed και Μήκος Κλειδιού

Το WEP seed παράγεται βάση του IV (Initialization Vector) μήκους 24 bits και ενός κλειδιού 40 bits που παρέχεται από τον χρήστη. Ο συνδυασμός των δύο αυτών δίνει τον σπόρο μήκους 64 bits. Διάφορες υλοποιήσεις έχουν αυξήσει το μήκος του κλειδιού σε 104-bit, δίνοντας ένα μήκος σπόρου 128-bit.
Σημείωση: Ο RC4 μπορεί να χρησιμοποιήσει μήκη κλειδιών έως 256 bytes. Τα 24 bits είναι για το IV, αφήνοντας 232 πραγματικά bits για την προστασία. Όμως για το πρότυπο 802.11 επιλέχτηκε μήκος κλειδιού 40 bits εξαιτίας απαγορεύσεων εξαγωγής αλγορίθμων κρυπτογράφησης.

Τα κλειδιά που χρησιμοποιούνται στο WEP

Τα κλειδιά κρυπτογράφησης που χρησιμοποιούνται στο WEP έχουν τα ακόλουθα χαρακτηριστικά:

Σταθερό μήκος: Συνήθως 40 ή 104 bits.
Στατικά: Δεν μεταβάλλεται η τιμή του κλειδιού εφόσον δεν αλλάξουν οι ρυθμίσεις.
Διαμοιραζόμενα (shared): Τόσο το σημείο πρόσβασης όσο και η κινητή συσκευή διαθέτουν αντίγραφο των ίδιων κλειδιών.
Συμμετρικά: Χρήση του ίδιου κλειδιού για κρυπτογράφηση και αποκρυπτογράφηση των πληροφοριών.

Κάθε σταθμός μπορεί να έχει τέσσερα κλειδιά ταυτόχρονα και να χρησιμοποιεί ένα από αυτά σε κάθε αποστολή ή λήψη πλαισίου, για κρυπτογράφηση και αποκρυπτογράφηση. Το πιο κάθε φορά χρησιμοποιείται ορίζεται σε ένα πεδίο του κρυπτογραφημένου πλαισίου που λέγεται αριθμός κλειδιού (*KeyID*). Η αντιστοιχία και η αρίθμηση θα πρέπει να είναι η ίδια μεταξύ των σταθμών. Η δυνατότητα παράλληλης χρήσης περισσοτέρων κλειδιών αυξάνει την συνολική ασφάλεια της επικοινωνίας. Η καλύτερη δημόσια επίθεση ενάντια στο WEP μπορεί να ανακτήσει το κλειδί σε μερικά δευτερόλεπτα. Εφόσον γίνεται ήδη χρήση και των τεσσάρων κλειδιών, ο χρόνος που απαιτείται για την εύρεση αυτών με τη μέθοδο της εξαντλητικής αναζήτησης (*brute force*) τετραπλασιάζεται.

Παραγωγή του IV (Initialization Vector – Διάνυσμα Αρχικοποίησης)

Η ύπαρξη του IV είναι αναγκαία προκειμένου το ίδιο κλειδί με τα ίδια δεδομένα να μην παράγουν το ίδιο κρυπτογραφημένο κείμενο. Κάτι τέτοιο θα επέτρεπε την εφαρμογή ορισμένων στατιστικών μεθόδων προκειμένου να ανακαλυφθεί το απλό κείμενο (*residual effect*).
Το IV αλλάζει για κάθε πακέτο που αποστέλλεται και συνδυάζεται με το μυστικό κλειδί. Έτσι ακόμα και εάν τα αρχικά δεδομένα είναι ίδια, η κρυπτογραφημένη μορφή τους είναι πάντα διαφορετική. Το IV δεν είναι μυστικό, ενώ στέλνεται σε μη

κρυπτογραφημένη μορφή σε κάθε μετάδοση ώστε ο παραλήπτης να είναι σε θέση να αποκρυπτογραφήσει την πληροφορία χρησιμοποιώντας την αντίστοιχη τιμή IV.

Διανομή κλειδιού

Το βασικότερο μειονέκτημα του WEP είναι πρόβλημα της διανομής του κλειδιού. Τα μυστικά κομμάτια του κλειδιού WEP πρέπει να μοιραστούν σε όλους τους σταθμούς που συμμετέχουν στο δίκτυο. Το 802.11 πρότυπο, δεν μας παρέχει ένα μηχανισμό παραγωγής κλειδιού έτσι ο καθένας πρέπει να δακτυλογραφεί το κλειδί στον οδηγό της συσκευής.
Οι δυσκολίες ενός τέτοιου πρωτοκόλλου είναι:

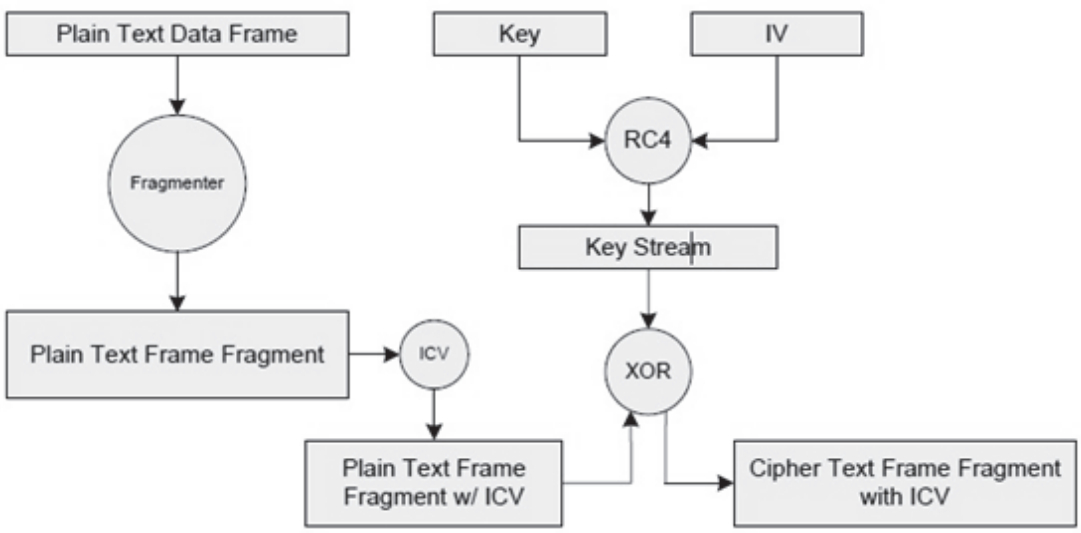
Τα κλειδιά δεν είναι ουσιαστικά μυστικά, αφού εισάγονται στους οδηγούς software ή firmware στην ασύρματη κάρτα. Έτσι ένας τοπικός χρήστης μπορεί να έχει πρόσβαση στο μυστικό κλειδί.
Εάν τα κλειδιά είναι προσιτά στους χρήστες, αυτά θα πρέπει να αλλάζουν συχνά. Η γνώση κλειδιών WEP επιτρέπει σε έναν χρήστη να φτιάξει έναν 802.11 σταθμό να ελέγχει παθητικά και να αποκρυπτογραφεί την κυκλοφορία χρησιμοποιώντας το μυστικό κλειδί.
Οι επιχειρήσεις με μεγάλο αριθμό εξουσιοδοτημένων χρηστών πρέπει να δημοσιεύσουν το κλειδί στους χρήστες και έτσι δεν υφίσταται πλέον η μυστικότητα του κλειδιού.

Σύνθεση Πλαισίου

Ο αλγόριθμος RC4 παράγει βάση του σπόρου και του αρχικών δεδομένων, τα κρυπτογραφημένα δεδομένα, τα οποία μαζί με το IV και το Key ID τοποθετούνται στο πλαίσιο προς αποστολή. Πρέπει να τονιστεί ότι κρυπτογραφημένα είναι μόνο τα δεδομένα και το ICV, ενώ όλα τα υπόλοιπα στέλνονται χωρίς κρυπτογράφηση.

Η κρυπτογράφηση

Το μυστικό κλειδί συνδέεται με το *διάνυσμα έναρξης* (IV) και το αποτέλεσμα τους εισάγεται στον αλγόριθμο RC4. Ο αλγόριθμος RC4 παράγει μια ακολουθία κλειδιού *keystream.*
Για προστασία από αναρμόδια τροποποίηση δεδομένων, εφαρμόζεται ο αλγόριθμος ακεραιότητας επάνω στα δεδομένα και παράγεται το ICV.
Η κρυπτογράφηση ολοκληρώνεται με τη λογική πράξη του αποκλειστικού Η (XOR) μεταξύ της ακολουθίας κλειδιού και των δεδομένων που μετατράπηκαν σε ICV.

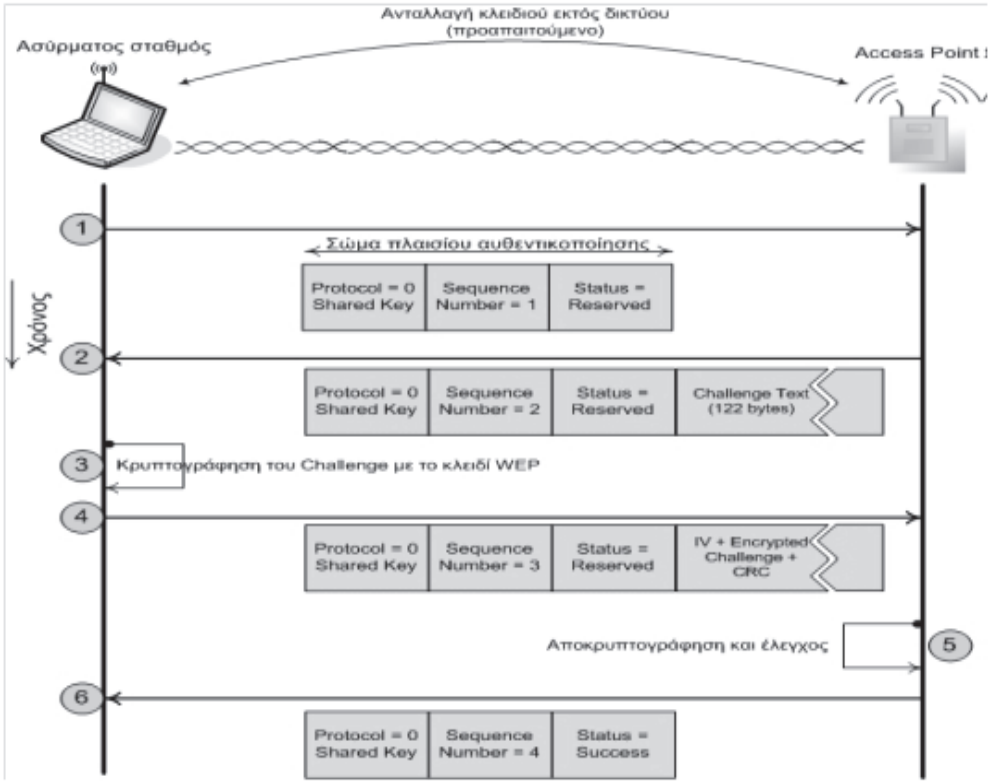


Εικόνα 20 Διαδικασία κρυπτογράφησης WEP.

Αποκρυπτογράφηση

Κατά την λήψη του πλαισίου ακολουθείται η αντίστροφη διαδικασία. Εντοπίζεται το κλειδί που χρησιμοποιήθηκε βάσει του πεδίου key ID, παράγεται το keystream και αποκρυπτογραφείται το περιεχόμενο του πλαισίου. Όταν ο παραλήπτης αποκρυπτογραφήσει το πακέτο υπολογίζει ξανά την τιμή ελέγχου ακεραιότητας ICV και τη συγκρίνει με αυτή που περιείχε το πακέτο που παρέλαβε. Αν οι δύο τιμές ταυτίζονται, τότε θεωρείται ότι το πακέτο είναι έγκυρο.

Επαλήθευση ταυτότητας



Εικόνα 21 Επαλήθευση ταυτότητας στο WEP.

Βήμα 1ο: Ο σταθμός που επιχειρεί να πιστοποιηθεί, στέλνει αίτημα πιστοποίησης στο AP (ή άλλο σταθμό εάν πρόκειται για ad-hoc δίκτυο).
Βήμα 2ο: Το AP απαντάει με μία τυχαία συμβολοσειρά (*Challenge Text*). Η τυχαία συμβολοσειρά αποσκοπεί στην αποφυγή της επίθεσης *Off-line Brute Force*.
Βήμα 3ο: Ο σταθμός κρυπτογραφεί την τυχαία συμβολοσειρά με το WEP κλειδί που διαθέτει.
Βήμα 4ο: Ο σταθμός αποστέλλει το κρυπτογραφημένο αποτέλεσμα στο AP.
Βήμα 5ο: Το AP αποκρυπτογραφεί την κρυπτογραφημένη τυχαία συμβολοσειρά με το δικό του WEP κλειδί. Αν η αποκρυπτογραφημένη τυχαία συμβολοσειρά είναι ίδια με την αρχική που είχε αποστείλει, συμπεραίνει ότι τα δύο κλειδιά είναι ίδια.
Βήμα 6ο: Αν στο βήμα 5 αποδείχτηκε ότι τα κλειδιά είναι ίδια, τότε το AP πιστοποιεί τον σταθμό.

Ωστόσο η μέθοδος αυτή αποτελεί πολύ μεγάλο πρόβλημα για την ασφάλεια της κρυπτογράφησης καθώς δίδει πληροφορίες σε κακόβουλους χρήστες, που παρακολουθούν την επικοινωνία τόσο της κρυπτογραφημένης αλλά και της μη κρυπτογραφημένης πληροφορίας.

Αδυναμίες του WEP

Παρακάτω αναφέρονται αναφορικά τα σημεία στα οποία εντοπίστηκαν αδυναμίες:
- Η επιλογή του IV καθώς και η έλλειψη μυστικότητάς του δίνει την ευκαιρία σε έναν εισβολέα να επιτεθεί σε ένα σχετικά αδύναμο κλειδί.
- Η μετάδοση του IV
- Η ύπαρξη αδύναμων IV
- Η ύπαρξη αδύναμων κλειδιών RC4
- Ο μηχανισμός CRC-32
- Η απουσία μηχανισμού αυτόματης διαμοίρασης των κλειδιών
- Η απουσία μηχανισμού αμοιβαίας πιστοποίησης μεταξύ των κόμβων. Το κλειδί που χρησιμοποιείται στη διαδικασία πιστοποίησης είναι το ίδιο με αυτό της κρυπτογράφησης, δίνοντας έτσι την ευκαιρία σε έναν επιτιθέμενο να αποκτήσει στοιχεία.

2.10. Wi-Fi Protected Access (WPA)

Για να διεκπεραιωθούν οι ευπάθειες του WEP, η IEEE εγκαθίδρυσε την ομάδα εργασίας 802.11 Working Group το 2001. Βασισμένη στα αρχικά σχέδια του Working Group, η *Wi-Fi Alliance Trade Group* εγκαθίδρυσε το WPA ως προσωρινή λύση που θα μπορούσε να επιτευχθεί με τον υπάρχοντα εξοπλισμό χρησιμοποιώντας μόνο ενημερώσεις λογισμικού και firmware. Το WPA εξασφαλίζεται σε όλες τις εκδόσεις 802.11. Ως υποσύνολο του 802.11i (γνωστού επίσης ως WPA2), το WPA είναι και προς τα εμπρός και προς τα πίσω συμβατό. Το WPA αυξάνει το επίπεδο προστασίας των δεδομένων που μεταδίδονται στον αέρα και τον έλεγχο πρόσβασης στα Wi-Fi δίκτυα. Παρέχει ισχυρή κρυπτογράφηση δεδομένων και προσθέτει την πιστοποίηση χρήστη που έλειπε κατά ένα μεγάλο μέρος από το WEP. Έτσι διαβεβαιώνει ότι τα δεδομένα στα δίκτυα Wi-Fi θα παραμείνουν προστατευμένα και ότι μόνο εξουσιοδοτημένοι χρήστες θα έχουν πρόσβαση στο δίκτυο.
Επιπλέον, προσφέρει καλύτερης κατηγορίας ασφάλεια στις επιχειρήσεις καθώς και στα δίκτυα μικρών γραφείων και σπιτιών (*small office / home office*, SOHO). Τα σημεία πρόσβασης (APs) απαιτούν βελτίωση λογισμικού. Οι τερματικοί σταθμοί πελατών απαιτούν βελτίωση λογισμικού στην NIC και μια πιθανή βελτίωση λογισμικού στο λειτουργικό σύστημα. Για τα δίκτυα επιχειρήσεων, η εφαρμογή του WPA περιλαμβάνει την ανάπτυξη μιας υποδομής 802.1x, δηλαδή:

Επιλογή των τύπων EAP που θα υποστηριχθούν στη NIC του πελάτη και στους εξυπηρετητές πιστοποίησης.

Επιλογή και ανάπτυξη εξυπηρετητή πιστοποίησης.
Βελτίωση των APs με WPA ή της αγοράς νέων APs με WPA εγκατεστημένο.
Βελτίωση της NIC του WLAN-πελάτη με WPA ή αγοράς νέας ασύρματης NIC με WPA εγκατεστημένο.

Το WPA εφοδιάζει τους χρήστες σπιτιού ή SOHO, που δεν έχουν διαθέσιμους τέτοιους εξυπηρετητές, με έναν ειδικό τρόπο που χρησιμοποιεί έναν κοινό κωδικό πρόσβασης που ενεργοποιεί την προστασία WPA.
Τα ενισχυμένα σχέδια κρυπτογράφησης και πιστοποίησης WPA είναι ιδανικά για δημόσια hotspots δεδομένου ότι παρέχουν ένα υψηλό επίπεδο ασφάλειας για τους φορείς παροχής υπηρεσιών και τους κινητούς χρήστες που δεν χρησιμοποιούν συνδέσεις VPN.

Μηχανισμός ασφάλειας στο WPA

Μια από τις κύριες αδυναμίες WEP είναι ότι χρησιμοποιεί ένα μικρό στατικό κλειδί για να αρχίσει την κρυπτογράφηση. Αυτό το 40bit κλειδί εισάγεται χειροκίνητα στο AP και σε όλους τους πελάτες που επικοινωνούν με το AP. Δεν αλλάζει εκτός αν ξαναεισαχθεί χειροκίνητα σε όλες τις συσκευές, μια τρομακτικά εντατική εργασία σε έναν μεγάλο οργανισμό.
Οι κρυπτογραφικές μελέτες έχουν δείξει ότι ένας εισβολέας που συλλέγει αρκετά δεδομένα μπορεί να απειλήσει ένα δίκτυο WEP με τρεις τρόπους: με την παρεμπόδιση και την αποκρυπτογράφηση των δεδομένων που μεταδίδονται στον αέρα, με την αλλαγή των δεδομένων που επικοινωνούν, και με πρόβλεψη του κλειδιού WEP αποκτώντας μη εξουσιοδοτημένη πρόσβαση σε υπηρεσίες του δικτύου και Διαδικτύου. Αυτό θα μπορούσε να ολοκληρωθεί σε ζήτημα ωρών σε ένα πολυάσχολο, εταιρικό WLAN.
Επίσης, το WEP στερείται την πιστοποίηση για να εξασφαλίσει ότι μόνο εκείνοι που πρέπει να είναι στο δίκτυο έχουν την άδεια να έχουν πρόσβαση σε αυτό.
Το WPA εξετάζει αυτά τα ελαττώματα και φέρνει πρόσθετα μέτρα προστασίας στην ασφάλεια WI-Fi. Χρησιμοποιεί ένα πολύ ενισχυμένο σχέδιο κρυπτογράφησης, το πρωτόκολλο TKIP (*Temporal Key Integrity Protocol*). Μαζί με την πιστοποίηση 802.1x/EAP, το TKIP υιοθετεί μια ιεραρχία κλειδιού που ενισχύει πολύ την προστασία. Προσθέτει επίσης έναν έλεγχο ακεραιότητας μηνυμάτων (Message Integrity Check, MIC, μερικές φορές ο αποκαλούμενος «Michael») για προστασία από τις παραποιήσεις πακέτων.

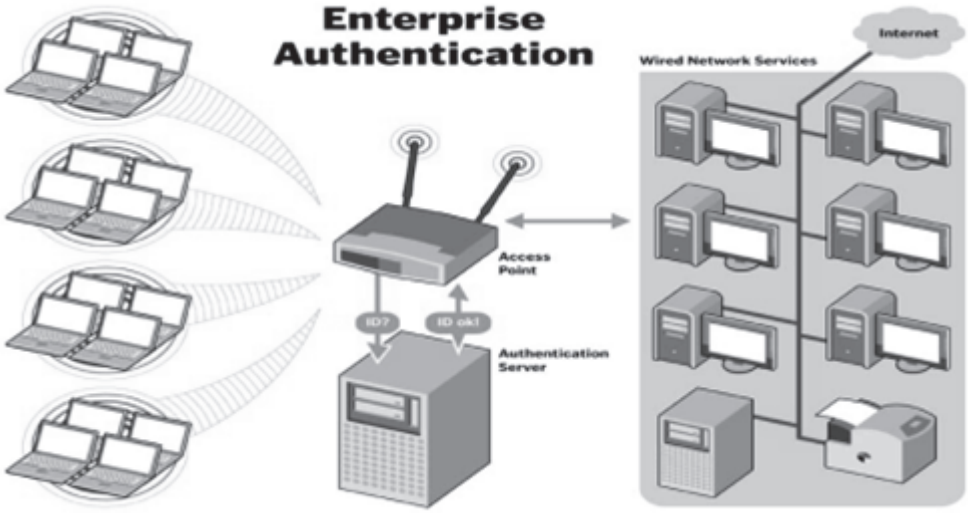
Κρυπτογράφηση και ακεραιότητα μηνυμάτων

Το TKIP αυξάνει το μέγεθος του κλειδιού από τα 40 στα 128 bit και αντικαθιστά το μοναδικό στατικό κλειδί του WEP με κλειδιά που παράγονται δυναμικά και διανέμονται από τον εξυπηρετητή πιστοποίησης (*authentication server*). Το TKIP χρησιμοποιεί μια ιεραρχία κλειδιού και μια μεθοδολογία διαχείρισης κλειδιού που αφαιρεί την προβλεψιμότητα επάνω στην οποία στηρίζονται οι εισβολείς για να εκμεταλλευτούν το κλειδί WEP.
Για να το κάνει αυτό, το TKIP ισχυροποιεί τη δομή 802.1x/EAP. Ο εξυπηρετητής πιστοποίησης, αφού αποδεχτεί τα πιστοποιητικά ενός χρήστη, χρησιμοποιεί τη δομή 802.1x για να παράγει έναν μοναδικό κύριο (*master*), ή «*pair-wise*» κλειδί για αυτή την σύνοδο υπολογισμού. Το TKIP διανέμει αυτό το κλειδί στον πελάτη και στο AP και εγκαθιστά μια ιεραρχία κλειδιού και ένα σύστημα διαχείρισης, χρησιμοποιώντας το pair-wise κλειδί για να παράγει δυναμικά τα μοναδικά κλειδιά κρυπτογράφησης δεδομένων για να κρυπτογραφήσει το κάθε πακέτο δεδομένων που επικοινωνεί ασύρματα κατά τη διάρκεια της συνόδου εκείνου του χρήστη. Η ιεραρχία του κλειδιού του TKIP ανταλλάσει το μοναδικό στατικό κλειδί του WEP για 500 τρισεκατομμύρια περίπου πιθανά κλειδιά που μπορούν να χρησιμοποιηθούν σε ένα πακέτο δεδομένων.

Ο έλεγχος ακεραιότητας μηνυμάτων (*Message Integrity Check*, MIC) έχει ως σκοπό να αποτρέψει έναν επιτιθέμενο από την σύλληψη των πακέτων δεδομένων, την αλλαγή τους και την εκ νέου αποστολή τους. Ο MIC παρέχει μια ισχυρή μαθηματική συνάρτηση με την οποία ο αποστολέας και λήπτης υπολογίζει ξεχωριστά και στη συνέχεια συγκρίνουν το MIC. Εάν δεν ταιριάζουν, τα δεδομένα υποτίθεται ότι έχουν πειραχτεί και το πακέτο απορρίπτεται.
Με την μεγάλη επέκταση του μεγέθους των κλειδιών, τον αριθμό των κλειδιών σε χρήση και τη δημιουργία μηχανισμού ελέγχου, το TKIP ενισχύει την πολυπλοκότητα και τη δυσκολία στην αποκωδικοποίηση δεδομένων όσον αφορά ένα δίκτυο WI-Fi. Το TKIP αυξάνει πολύ τη δύναμη και πολυπλοκότητα της ασύρματης κρυπτογράφησης, που κάνει δύσκολο σε έναν εν δυνάμει εισβολέα να σπάσει ένα δίκτυο WI-Fi.
Σχεδιασμένο για να επεκταθεί με τις υπάρχουσες επικυρωμένες συσκευές WI-Fi, το TKIP περιλαμβάνεται και στα WPA2 πρότυπα.

Πιστοποίηση

Το WPA χρησιμοποιεί πιστοποίηση 802.1x με ένα από τα πρωτόκολλα EAP που είναι διαθέσιμα σήμερα. Το 802.1x είναι μια μέθοδος ελέγχου πρόσβασης στο δίκτυο, βασισμένη σε θύρες (*port-based*), τόσο για ενσύρματα όσο και για ασύρματα δίκτυα. Υιοθετήθηκε ως πρότυπο από την IEEE τον Αύγουστο του 2001.
Το EAP χειρίζεται την παρουσίαση των πιστοποιητικών των χρηστών υπό μορφή ψηφιακών πιστοποιητικών, μοναδικών ονομάτων χρηστών (*usernames*) και κωδικών πρόσβασης (*passwords*), έξυπνων καρτών, ασφαλών IDs, ή οποιοδήποτε άλλο πιστοποιητικό ταυτότητας αναπτύξει ο διαχειριστής δικτύου.
Το WPA είναι ευέλικτο και στον τύπο πιστοποιητικών που χρησιμοποιούνται και στην επιλογή του τύπου EAP. Ένας ευρύς αριθμός, βασισμένων στο πρότυπο, εφαρμογών EAP είναι διαθέσιμος για χρήση. Με το EAP, το 802.1x δημιουργεί μια δομή στην οποία οι τερματικοί σταθμοί πελατών πιστοποιούνται αμοιβαία με τον εξυπηρετητή πιστοποίησης. Αυτή η αμοιβαία πιστοποίηση αποτρέπει τους χρήστες από τυχαία σύνδεση με ένα *rogue* ή μη εξουσιοδοτημένο AP στο δίκτυο Wi-Fi και επίσης εξασφαλίζει ότι οι χρήστες που έχουν πρόσβαση στο δίκτυο είναι αυτοί που θα έπρεπε να είναι εκεί. Όταν ένας χρήστης ζητά πρόσβαση στο δίκτυο, ο πελάτης στέλνει τα πιστοποιητικά του χρήστη στον εξυπηρετητή πιστοποίησης μέσω του AP. Εάν ο server δέχεται τα πιστοποιητικά του χρήστη, το κύριο κλειδί (*master key*) TKIP στέλνεται και στον πελάτη και στο AP. Η χειραψία τεσσάρων καταστάσεων (*four-way handshake*), αποτελεί μια διαδικασία στην οποία ο πελάτης και το AP αναγνωρίζουν ο ένας τον άλλον και εγκαθιστούν τα κλειδιά, ολοκληρώνοντας έτσι τη διαδικασία.

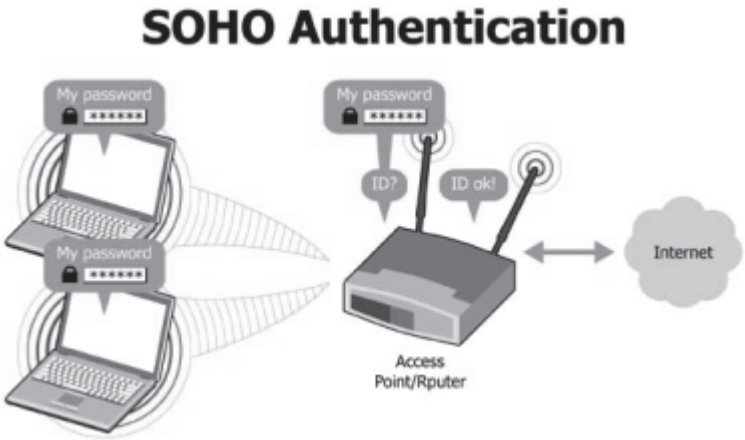


Εικόνα 22 Μηχανισμός WPA πιστοποίησης σε επιχειρησιακό περιβάλλον.

Ασφάλεια σπιτιών και μικρών γραφείων (Small Office, Home Office **- SOHO)**

Οι χρήστες σε περιβάλλοντα μικρών γραφείων και γραφείων σπιτιών στερούνται προϋπολογισμό και προσωπικό για να εγκαταστήσουν και να διατηρήσουν RADIUS servers. Το WPA προσφέρει σε αυτούς τους χρήστες τα οφέλη της ασφάλειάς του μέσω της χρήσης προ-μοιραζόμενου κλειδιού (*pre-shared key*, PSK) ή κωδικού πρόσβασης.
Το PSK παρέχει σε SOHO περιβάλλοντα την ίδια ισχυρή κρυπτογράφηση TKIP, κατασκευή κλειδιού για κάθε πακέτο (*per-packet*), και διαχείριση κλειδιού που παρέχει το WPA στην επιχείρηση.
Η διαφορά είναι ότι εδώ, ένας προσωπικός κωδικός πληκτρολογείται με το χέρι στις συσκευές πελατών και στο AP ή την ασύρματη πύλη (*gateway*) και χρησιμοποιείται για πιστοποίηση. Το PSK παρέχει μια χρήσιμη εναλλακτική λύση για τα μικρότερα δίκτυα αν και δεν αποτελεί ισχυρή διαδικασία πιστοποίησης όπως τα RADIUS, EAP και 802.1x.
Η αναβάθμιση του WPA στο σπίτι και τα μικρά περιβάλλοντα γραφείων είναι απλή. Τα βήματα είναι:

1 Αναβάθμιση APs με το λογισμικό WPA.
2 Αναβάθμιση των NICs των WLAN με WPA λογισμικό.
3 Διαμόρφωση του PSK, ή του κύριου κωδικού πρόσβασης, στο AP.
4 Διαμόρφωση του PSK στους τερματικούς σταθμούς πελατών.



Εικόνα 23 Μηχανισμός WPA πιστοποίησης σε σπίτι ή γραφείο.

2.11. Wi-Fi Protected Access Version 2 (WPA2)

Η *Wi-Fi Alliance* αναφέρεται στην εφαρμογή πιο γερών χαρακτηριστικών ασφαλείας που καθορίζονται στο έγγραφο 802.11i-2004, το οποίο εισήγαγε την έννοια *Robust Security Network Association* (RSNA), ως WPA2. Η πιο ισχυρή κρυπτογράφηση απαιτεί ανάπτυξη του υλικού καθώς δεν υποστηρίζεται από παλαιότερο εξοπλισμό.
Το WPA2 είναι η σημερινή παραγωγή ασφάλειας στα δίκτυα Wi-Fi. Θεμελιώνεται με δύο βασικούς μηχανισμούς:
AES (*Advanced Encryption Standard*): το πρωτόκολλο κρυπτογράφησης που χρησιμοποιείται από τις Ηνωμένες Πολιτείες και άλλες κυβερνήσεις, για να προστατεύουν εμπιστευτικές και απόρρητες πληροφορίες, και από τις επιχειρήσεις για να παρέχουν ασφάλεια στα WLANs.
IEEE 802.1x: ένα ευρέως χρησιμοποιημένο πρότυπο στα εταιρικά δίκτυα για να παρέχει γερή επικύρωση και περίπλοκα χαρακτηριστικά γνωρίσματα ελέγχου προσπέλασης δικτύων.

Το WPA2 παρέχει 128-bit AES block cipher[4] κρυπτογράφηση με βάση το πρωτόκολλο CCMP (*Message Authentication Code Protocol*). Παρέχει επίσης αμοιβαία πιστοποίηση με προ-μοιραζόμενο κλειδί (PSK στον Personal τρόπο) και με IEEE 802.1x/EAP (στον Enterprise τρόπο).

Τεχνολογική επισκόπηση του WPA2

Αμοιβαία πιστοποίηση (*Mutual Authentication*): Το WPA2 χρησιμοποιεί IEEE 802.1x (*WPA2-Enterprise*) και PSK (*WPA2-Personal*) για να παρέχει αμοιβαία πιστοποίηση. Με τη μονόδρομη πιστοποίηση, η συσκευή πελάτη στέλνει τα πιστοποιητικά της και, εάν η πρόσβαση εξουσιοδοτείται, η συσκευή πελάτη συνδέεται με το δίκτυο. Η αμοιβαία πιστοποίηση απαιτεί η συσκευή πελάτη να επαληθεύσει το πιστοποιητικό δικτύου προτού εγκαταστήσει τη σύνδεση, για να αποτρέψει το χρήστη από τη σύνδεση με μη εξουσιοδοτημένα σημεία πρόσβασης.
Ισχυρή κρυπτογράφηση (*Strong Encryption*): Ο **AES** ορίζεται ως ένα ομοσπονδιακό πρότυπο επεξεργασίας πληροφοριών (*Federal Information Processing Standard*, FIPS Publication 197) και είναι ο πρώτος δημόσια διαθέσιμος μηχανισμός κρυπτογράφησης που καλύπτει τις απαιτήσεις της Αμερικανικής κυβέρνησης για την προστασία ευαίσθητων και ταξινομημένων πληροφοριών. Μέχρι σήμερα, ο AES έχει αποδειχθεί εξαιρετικά ανθεκτικός παρά το μεγάλο αριθμό των δημοσιευμένων επιθέσεων που προκαλούνται από την ευρεία υιοθέτηση του. Τα δεδομένα που ταξιδεύουν μέσω ενός WPA2 δικτύου *κρυπτογραφούνται χρησιμοποιώντας τον αλγόριθμο CCMP με AES*, τα οποία παρέχουν μαζί προηγμένη μέθοδο κρυπτογράφησης δεδομένων που είναι διαθέσιμη. Η υποστήριξη AES απαιτείται από πολλά πρωτόκολλα και εφαρμογές που χρησιμοποιούνται παγκοσμίως στα δίκτυα επιχειρήσεων.
Διαλειτουργικότητα (*Interportability*): Το WPA2 είναι μια λύση, βασισμένη στο πρότυπο, που υποστηρίζεται από όλο τον Wi-Fi επικυρωμένο εξοπλισμό που έχει υποβληθεί σε εξέταση από το 2006. Το WPA2 μπορεί να ενεργοποιηθεί μέσα σε οποιαδήποτε σύνοδο στην οποία το σημείο πρόσβασης και η συσκευή πελάτη το υποστηρίζουν, ανεξάρτητα από τα εμπορικά ονόματα (*brands*) του εξοπλισμού που εμπλέκονται. Αυτό επεκτείνει πολύ τη διαθεσιμότητα του WPA2 και δίνει την σιγουριά στους διαχειριστές δικτύου και στους χρήστες ότι τα δίκτυα τους, οι συσκευές, και οι ροές δεδομένων τους μπορούν να προστατευθούν παντού.
Ευκολία στη χρήση (*Ease of use*): Το WPA2 είναι όχι μόνο ένα ισχυρό εργαλείο για να προστατεύσει τους χρήστες Wi-Fi, αλλά και εύκολο να ενεργοποιηθεί. Το 2007 η Wi-Fi Alliance εισήγαγε ένα χωριστό πρόγραμμα πιστοποίησης, το *Wi-Fi Protected Setup*, για να απλοποιήσει τη διαμόρφωση του WPA2 και για να επιταχύνει την υιοθέτησή του στα οικιακά δίκτυα.

Το Πρότυπο AES

Το πρότυπο AES περιγράφει μια συμμετρική μπλοκ διαδικασία κρυπτογράφησης μυστικού κλειδιού. Το πρότυπο υποστηρίζει την χρήση κλειδιών μήκους 128, 192 και 256 bits. Ανάλογα με το ποιο μήκος κλειδιού χρησιμοποιείται, συνήθως χρησιμοποιείται η συντόμευση AES-128, AES-192 και AES-256 αντίστοιχα. Ανεξάρτητα από το μήκος κλειδιού, ο αλγόριθμος επενεργεί πάνω σε μπλοκ δεδομένων μήκους 128 bits. Η διαδικασία κρυπτογράφησης είναι επαναληπτική. Αυτό σημαίνει ότι σε κάθε μπλοκ δεδομένων γίνεται μια επεξεργασία η οποία

[4]**Block cipher** είναι ένας ντετερμινιστικός αλγόριθμος που λειτουργεί στις καθορισμένου μήκους ομάδες bits, αποκαλούμενες blocks, με έναν αμετάβλητο μετασχηματισμό που διευκρινίζεται από ένα συμμετρικό κλειδί και αποτελούν σημαντικά στοιχειώδη συστατικά στον σχεδιασμό πολλών κρυπτογραφικών πρωτοκόλλων, και χρησιμοποιούνται ευρέως για να εφαρμόσουν την κρυπτογράφηση μαζικών δεδομένων.

επαναλαμβάνεται έναν αριθμό από φορές ανάλογα με το μήκος κλειδιού. Κάθε επανάληψη ονομάζεται γύρος (round). Στον πρώτο γύρο επεξεργασίας ως είσοδος είναι ένα plaintext μπλοκ και το αρχικό κλειδί, ενώ στους γύρους που ακολουθούν ως είσοδος είναι το μπλοκ που έχει προκύψει από τον προηγούμενο γύρο καθώς και ένα κλειδί που έχει παραχθεί από το αρχικό με βάση κάποια διαδικασία που ορίζει ο αλγόριθμος. Το τελικό προϊόν της επεξεργασίας είναι το κρυπτογραφημένο μπλοκ (ciphertext). Το μπλοκ αυτό πρέπει να σημειωθεί ότι έχει ακριβώς το ίδιο μέγεθος (128 bits) με το plaintext μπλοκ.

Είσοδοι, Έξοδοι και Εσωτερική Κατάσταση

Όπως ήδη αναφέρθηκε, ο AES τροφοδοτείται με ακολουθίες από bits των 128 bits (μπλοκ) καθώς και από κλειδιά, που μπορεί να έχουν μέγεθος 128, 192 ή 256 bits. Τα κλειδιά αυτά ονομάζονται κλειδιά κρυπτογράφησης (cipher keys) για να διαχωριστούν από τα κλειδιά που παράγονται κατά την λειτουργία του αλγορίθμου. Η βασική μονάδα επεξεργασίας στον AES είναι το byte. Έτσι τα bits ενός μπλοκ ή ενός κλειδιού χωρίζονται σε ομάδες των 8 για να σχηματιστούν τα bytes. Κάθε byte στον AES αντιστοιχεί σε ένα πολυώνυμο (αριθμητική πεπερασμένων πεδίων - finite field arithmetic). Αν υποθέσουμε ότι τα bits που αποτελούν ένα byte είναι τα {b7, b6, b5, b4, b3, b2, b1, b0}, τότε το byte αυτό αναπαριστά το πολυώνυμο :

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x^1 + b_0 = \sum_{i=0}^{7} b_i x^i$$

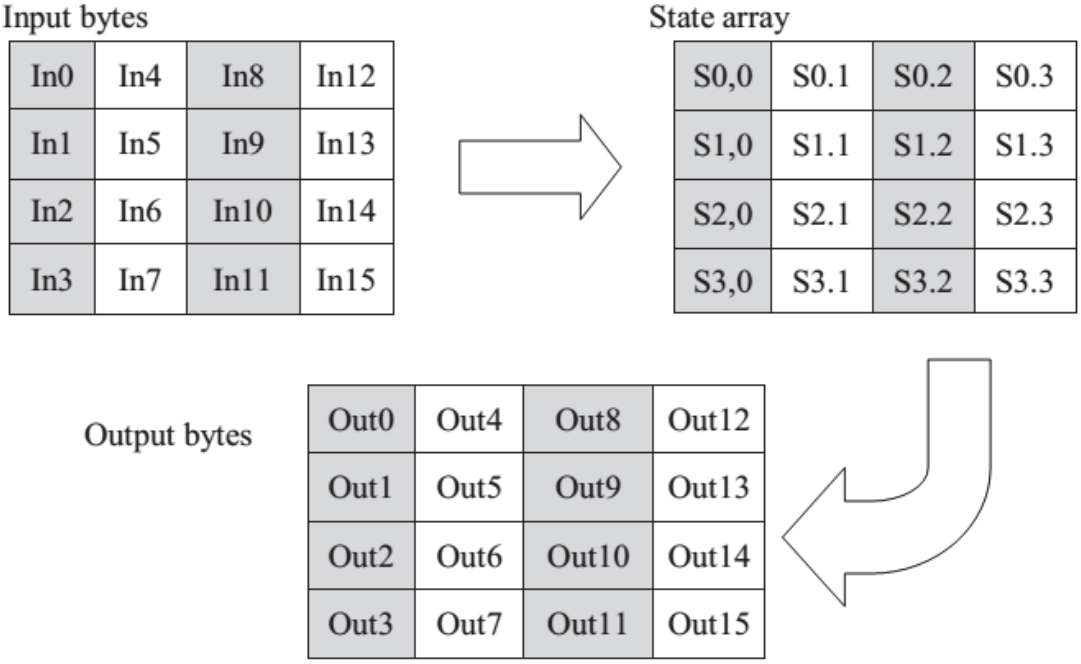
Έτσι για παράδειγμα το byte {11001101} αντιστοιχεί στο πολυώνυμο
$x^7 + x^6 + x^3 + x^2 + 1$

Κλείνοντας την αναφορά στις μονάδες των δεδομένων που διαχειρίζεται ο AES, πρέπει να αναφερθεί το πώς γίνεται η δεικτοδότηση των bits και των bytes στα μπλοκ και στα κλειδιά. Το παρακάτω σχήμα δείχνει την αντιστοιχία.

Input bit sequence	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	.....
Byte number	0								1								.....
Bit numbers in byte	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	.....

Εικόνα 24 Δεικτοδότηση των bits και bytes.

Όλες οι λειτουργίες που επιτελεί ο αλγόριθμος γίνονται πάνω σε ένα δισδιάστατο πίνακα που αποκαλείται Κατάσταση (State). Ο πίνακας αυτός περιλαμβάνει τέσσερις γραμμές από bytes, με κάθε μία γραμμή να αποτελείται από Nb bytes. Ο αριθμός που αντιστοιχεί στην ποσότητα Nb υπολογίζεται αν διαιρεθεί το μήκος του μπλοκ με το 32. Εφόσον στον AES υποστηρίζονται μπλοκ μεγέθους μόνο 128 bits, το Nb θα έχει τιμή 4.
Το μπλοκ εισόδου περιλαμβάνει 16 bytes, τα οποία δεικτοδοτούνται in0 έως in15. Το κρυπτογραφημένο μπλοκ εξόδου περιλαμβάνει επίσης 16 bytes που δεικτοδοτούνται ως out0 έως out15. Η State χρησιμοποιεί την μεταβλητή s με δύο δείκτες που δηλώνουν την θέση κάθε byte στον πίνακα. Η πρώτη λοιπόν και τελευταία λειτουργία που μπορεί να υποτεθεί ότι γίνεται στον AES είναι να αντιστοιχηθούν τα bytes εισόδου σε κάποια θέση του πίνακα της State και το αντίστροφο στην έξοδο. Το παρακάτω σχήμα δείχνει πώς γίνεται αυτό.



Εικόνα 25 Αντιστοίχηση των bytes εισόδου σε κάποια θέση του πίνακα της State και το αντίστροφο στην έξοδο.

Η αντιστοίχηση που περιγράφηκε παραπάνω μπορεί να περιγραφεί μαθηματικά. Η αντιστοίχηση εισόδου στην State περιγράφεται από την σχέση :
$s[r,c] = in[r+4c]$ για $0 \leq r < 4$ και $0 \leq c < Nb$
ενώ η αντιγραφή της State στην έξοδο από την σχέση :
$out[r+4c] = s[r,c]$ για $0 \leq r < 4$ και $0 \leq c < Nb$
Ένας άλλος τρόπος να δει κάποιος τα περιεχόμενα της State είναι σαν 32-bit λέξεις (words) αντί για byte. Μια 32-bit word περιλαμβάνει τα 4 bytes μιας στήλης, οπότε τα 4 words που αποτελούν την State είναι τα ακόλουθα :

w(0) = s(0,0) s(1,0) s(2,0) s(3,0)
w(1) = s(0,1) s(1,1) s(2,1) s(3,1)
w(2) = s(0,2) s(1,2) s(2,2) s(3,2)
w(3) = s(0,3) s(1,3) s(2,3) s(3,3)

Περιγραφή Αλγορίθμου:
Όπως αναφέρθηκε, το πρότυπο AES ορίζει ότι τα μπλοκ που επεξεργάζεται ο αλγόριθμος έχουν μέγεθος 128 bits και αυτό ορίζεται από την ποσότητα Nb = 4, που συμβολίζει τον αριθμό των 32-bit λέξεων στο μπλοκ. Από την άλλη, τα κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση, μπορούν να έχουν μήκος 128, 192 ή 256 bits. Η μεταβλητή Nk συμβολίζει τον αριθμό των 32-bit λέξεων που μπορεί να περιλαμβάνει ένα κλειδί και κατά συνέπεια μπορεί να πάρει τις τιμές 4, 6 και 8. Ανάλογα με το μήκος κλειδιού που θα επιλεχθεί για την κρυπτογράφηση, ο αλγόριθμος ορίζει έναν αριθμό από γύρους επεξεργασίας που απαιτούνται για την ολοκλήρωση της. Η μεταβλητή Nr χρησιμοποιείται για να δηλώσει το πλήθος των γύρων. Αν χρησιμοποιηθεί μήκος κλειδιού 128 bits τότε απαιτούνται 10 γύροι επεξεργασίας. Για μήκη κλειδιού ίσα με 192 και 256 bits απαιτούνται αντίστοιχα 12 και 14 γύροι.

	Key Length (Nk words)	Block Size (Nb words)	Number Of Rounds (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Εικόνα 26 Μέγεθος των μεταβλητών του αλγορίθμου.

Nr = Αριθμός των γύρων
Nb = Αριθμός των byte
Nk = Μέγεθος κλειδιού

Να σημειωθεί ότι οι παραπάνω συνδυασμοί μήκους μπλοκ, μήκους κλειδιού και γύρων επεξεργασίας είναι αυτοί που ορίζονται αυστηρά στο πρότυπο AES. Ο αλγόριθμος κρυπτογράφησης Rijndael στον οποίο βασίζεται ο AES δίνει την δυνατότητα πραγματοποίησης περισσότερων συνδυασμών. Έτσι, καταλαβαίνει κανείς ότι ο AES ουσιαστικά ορίζει ένα υποσύνολο του αλγορίθμου Rijndael.
Τόσο κατά την διάρκεια της διαδικασίας κρυπτογράφησης όσο και αποκρυπτογράφησης, κάθε γύρος επεξεργασίας αποτελείται από μια σειρά μετασχηματισμών σε επίπεδο byte. Για την ακρίβεια, χρησιμοποιούνται 4 τύποι μετασχηματισμών :

- ένας μετασχηματισμός αντικατάστασης bytes χρησιμοποιώντας κάποιον σχετικό πίνακα αντικατάστασης
- ένας μηχανισμός ολίσθησης των bytes της State κατά διαφορετικά offsets
- μια διαδικασία ανάμειξης των bytes της State
- μια πρόσθεση ενός κλειδιού στην State

Ο Αλγόριθμος Κρυπτογράφησης

Στην αρχή της διαδικασίας κρυπτογράφησης ένα μπλοκ εισόδου (plaintext) αντιγράφεται στην State. Μετά από έναν αρχικό γύρο πρόσθεσης κλειδιού, ακολουθούν 10, 12 ή 14 γύροι επεξεργασίας, με τον τελευταίο γύρο να διαφέρει από τους υπόλοιπους. Η τελική State αντιγράφεται στην έξοδο και η επεξεργασία για το συγκεκριμένο block ολοκληρώνεται (παραγωγή του ciphertext μπλοκ).
Το μυστικό κλειδί κρυπτογράφησης που χρησιμοποιείται σαν είσοδος στον αλγόριθμο είναι το κλειδί που προστίθεται στο μπλοκ εισόδου πριν αρχίσει η επεξεργασία. Σε καθέναν από τους γύρους επεξεργασίας, όπως αναφέρθηκε παραπάνω, υπάρχει μια φάση κατά την οποία προστίθεται στο μπλοκ και ένα κλειδί. Το κλειδί που προστίθεται στις περιπτώσεις αυτές, δεν είναι το αρχικό μυστικό κλειδί αλλά κάποιο που έχει προκύψει με μια συγκεκριμένη διαδικασία από το μυστικό κλειδί και είναι διαφορετικό για κάθε γύρο. Για τον λόγο αυτό, τα κλειδιά αυτά ονομάζονται round keys. Η διαδικασία με την οποία προκύπτουν τα round κλειδιά ονομάζεται Επέκταση Κλειδιού.
Αυτό που πρέπει να διευκρινιστεί είναι η έννοια της πρόσθεσης στον AES αλγόριθμο. Τα bytes της πληροφορίας κατά την επεξεργασία τους λαμβάνονται ως πολυώνυμα. Έτσι, η πράξη της πρόσθεσης είναι ουσιαστικά μια διαδικασία πρόσθεσης πολυωνύμων. Η πρόσθεση μεταξύ πολυωνύμων πραγματοποιείται με την πρόσθεση των συντελεστών των αντίστοιχων όρων (δυνάμεων) των πολυωνύμων. Η πρόσθεση γίνεται modulo-2, δηλαδή μέσω μιας XOR πράξης. Να ενθυμηθεί ότι η XOR πράξη μεταξύ δύο bits (συμβολίζεται με)
έχει τον εξής πίνακα αληθείας:

$0 \oplus 0 = 0$
$0 \oplus 1 = 1$
$1 \oplus 0 = 1$
$1 \oplus 1 = 0$

Αν κάθε βασικός μετασχηματισμός του AES αναπαρασταθεί από μια συνάρτηση που επενεργεί στην State, τότε ο αλγόριθμος κρυπτογράφησης μπορεί να περιγραφεί από τον ψευδοκώδικα που παρουσιάζεται στο ακόλουθο σχήμα.

```
Cipher (byte in [4*Nb], byte out [4*Nb], byte key [4*Nb]
        word w [Nb*(Nr+1)])
Begin
     Byte state [4, Nb]
     State=in
     KeyExpansion(key,w);
     AddRoundKey (state, w [0, Nb-1])

     For round=1 step 1 to Nr-1
       SubBytes (state)
       ShiftRows (state)
       MixColumns (state)
       AddRoundKey (state, w [round*Nb, (round+1)*Nb-1])
     End for

     SubBytes (state)
     ShiftRows (state)
     AddRoundKey (state, w [Nr*Nb, (Nr+1)*Nb-1]
     Out=state
 End
```

Εικόνα 27 Ψευδοκώδικας Κρυπτογράφησης.

Οι συναρτήσεις αυτές αναφέρονται ως SubBytes(), ShiftRows(), MixColumns() και AddRoundKey() και αντιστοιχούν (με αυτήν την σειρά) στους μετασχηματισμούς 1 έως 4 όπως αναφέρθηκαν παραπάνω. Να σημειωθεί ότι το array w χρησιμοποιείται για να δηλώσει την συλλογή των round keys που παράγονται από την διαδικασία επέκτασης κλειδιού. Εξήγηση του ψευδοκώδικα για την διαδικασία κρυπτογράφησης. Όπως βλέπουμε παίρνει σαν είσοδο (In) το plaintext βγάζει σαν έξοδο (out) το cipher text και παίρνουμε και τον πινάκα W ο οποίος έχει δημιουργηθεί κατά την λειτουργία της συνάρτησης key expansion όπου εκεί έχει ανακατευτεί το κλειδί που έχουμε δώσει. Λοιπόν στον γύρο 0 στο state όρισμα αντιγράφουμε το plaintext και στη συνέχεια καλούμε τη συνάρτηση AddRoundKey. Μετά από το γύρο 1 έως τον Nr-1 (ανάλογα το bits αλγορίθμου που έχουμε επιλέξει για να δουλέψουμε 128,196,256) καλούμε με τη σειρά τις συναρτήσεις SubBytes, Shiftrows, MixColumns και AddRoundKey όπου εκεί θα ανακατευτεί διαδοχικά το state.
Στον τελευταίο γύρο το state θα ανακατευτεί με τις συναρτήσεις SubBytes, Shiftrows και AddRoundKey όπου το τελικό αποτέλεσμα θα είναι το cipher text.

Συναρτήσεις του Αλγορίθμου Κρυπτογράφησης

- **Μετασχηματισμός SubBytes**

X/Y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	fb	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	fd	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	fd	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Εικόνα 28 Ο πίνακας αντικατάστασης S-Box.

Ο μετασχηματισμός SubBytes αποτελεί μια μη γραμμική αντικατάσταση των bytes της State με την χρήση ενός πίνακα αντικατάστασης (S-Box). Οι τιμές του πίνακα αυτού (που είναι αντιστρέψιμος) υπολογίζονται με την σύνθεση των δύο ακόλουθων μετασχηματισμών παίρνοντας τον πολλαπλασιαστικό αντίστροφο στο πεπερασμένο πεδίο GF(28) - με το στοιχείο {00} να αντιστοιχίζεται στον εαυτό του εφαρμόζοντας τον ακόλουθο μετασχηματισμό (στο GF(2)):

$$b_i' = b_i \oplus b_{(i+4) \bmod 8} \oplus b_{(i+5) \bmod 8} \oplus b_{(i+6) \bmod 8} \oplus b_{(i+7) \bmod 8} \oplus c_i$$

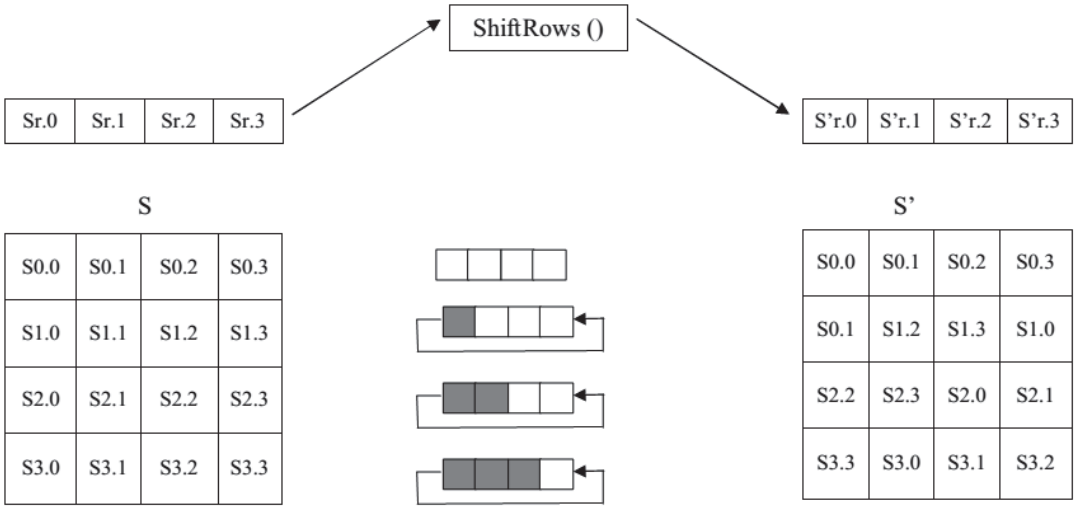
για 0 ≤ i < 8 , όπου bi είναι το i-οστό bit του byte, και ci είναι το i-οστό bit του byte c με την τιμή {63} or {01100011}.
Ο πίνακας S-Box τυπικά δεν υπολογίζεται κατά την διαδικασία της κρυπτογράφησης, αλλά οι τιμές του έχουν προϋπολογιστεί. Στο σχήμα που ακολουθεί παρατίθενται οι τιμές του πίνακα S-Box όπως τις παρουσιάζει το NIST στο επίσημο έγγραφο για τον AES. Για όσους από τους αναγνώστες δεν είναι εξοικειωμένοι με την γραφή αριθμών στο δεκαεξαδικό σύστημα, να σημειωθεί ότι ένας αριθμός στο δεκαεξαδικό σύστημα χρειάζεται 4 bits για να αναπαρασταθεί. Κατά συνέπεια, ένα byte αναπαρίσταται από 2 δεκαεξαδικά ψηφία χωρίζοντας το σε 2 ομάδες των 4 bits. Έτσι η γραμμή x του πίνακα αναφέρεται στα πρώτα 4 bits του byte και η στήλη y στα επόμενα 4.
Εφόσον αναφέρθηκε ο θεωρητικός τρόπος με τον οποίο προκύπτει ο πίνακας S-Box, καλό θα ήταν να διευκρινιστεί τι σημαίνει πολλαπλασιασμός στο GF(28). Είναι ο πολλαπλασιασμός μεταξύ πολυωνύμων modulo ένα irreducible πολυώνυμο βαθμού 8. Irreducible ονομάζεται ένα πολυώνυμο αν διαιρείται μονάχα από τον εαυτό του και την μονάδα. Το πολυώνυμο που έχει επιλεχθεί για το AES είναι το :

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

Η modulo πράξη εξασφαλίζει ότι το πολυώνυμο που θα προκύψει θα είναι ένα δυαδικό πολυώνυμο βαθμού μικρότερου του 8, άρα θα μπορεί να αναπαρασταθεί από ένα byte. Να σημειωθεί ότι το ουδέτερο στοιχείο της πράξης είναι το {01} και ότι το σύμβολο που χρησιμοποιείται για να διακρίνει την πράξη αυτή από έναν κοινό αριθμητικό πολλαπλασιασμό είναι το • .

- **Μετασχηματισμός ShiftRows**

Ο μετασχηματισμός αυτός επιβάλει την κυκλική ολίσθηση των bytes των γραμμών της State. Η πρώτη γραμμή παραμένει ανέπαφη, ενώ στις υπόλοιπες τα bytes ολισθαίνουν με διαφορετικό offset.
Το ακόλουθο σχήμα παρουσιάζει ενδεικτικά πώς γίνεται ο μετασχηματισμός αυτός. Όπως μπορεί να παρατηρηθεί από το σχήμα, η δεύτερη γραμμή ολισθαίνει αριστερά κατά μία θέση με αποτέλεσμα το πρώτο byte της γραμμής να βρεθεί τελευταίο (κυκλική ολίσθηση). Με αντίστοιχο τρόπο ολισθαίνουν και οι γραμμές 3 και 4 αλλά κατά 2 και 3 θέσεις αντίστοιχα.



Εικόνα 29 Ο μετασχηματισμός ShiftRows ολισθαίνει κυκλικά προς τα αριστερά τις τρεις τελευταίες.

- **Ο Μετασχηματισμός MixColumns**

Ο μετασχηματισμός αυτός εφαρμόζεται στις στήλες της State. Η κάθε στήλη θεωρείται σαν πολυώνυμο τρίτης τάξης με συντελεστές τις τιμές των bytes της στήλης.

$$s(x)_i = s_{3,i} \cdot x^3 + s_{2,i} \cdot x^2 + s_{1,i} \cdot x + s_{0,i}$$

Τα πολυώνυμα πολλαπλασιάζονται modulo (x4 + 1) με ένα καθορισμένο πολυώνυμο που δίνεται από την σχέση :

$$a(x) = \{03\} \cdot x^3 + \{01\} \cdot x^2 + (01) \cdot x + (02)$$

Η διαδικασία αυτή του υπολογισμού της αρχικής πράξης, $s'(x) = a(x) \otimes s(x)$ όπου με $\otimes$ συμβολίζεται ο modulo πολλαπλασιασμός μετασχηματίζεται τελικά στις εξής σχέσεις :

$$s'_{0,c} = (\{02\} \bullet s_{0,c}) \oplus (\{03\} \bullet s_{1,c}) \oplus s_{2,c} \oplus s_{3,c}$$

$$s'_{1,c} = s_{0,c} \oplus (\{02\} \bullet s_{1,c}) \oplus (\{03\} \bullet s_{2,c}) \oplus s_{3,c}$$

$$s'_{2,c} = s_{0,c} \oplus s_{1,c} \oplus (\{02\} \bullet s_{2,c}) \oplus (\{03\} \bullet s_{3,c})$$

$$s'_{2,c} = \{03\} \bullet s_{0,c} \oplus s_{1,c} \oplus s_{2,c} \oplus (\{02\} \bullet s_{3,c})$$

$$\text{για } 0 \leq c < Nb$$

- **Μετασχηματισμός AddRoundKey**

Ο μετασχηματισμός αυτός επιβάλει την πρόσθεση της τιμής της ποσότητας round key στα bytes των στηλών του πίνακα State. Επειδή κάθε τιμή του round

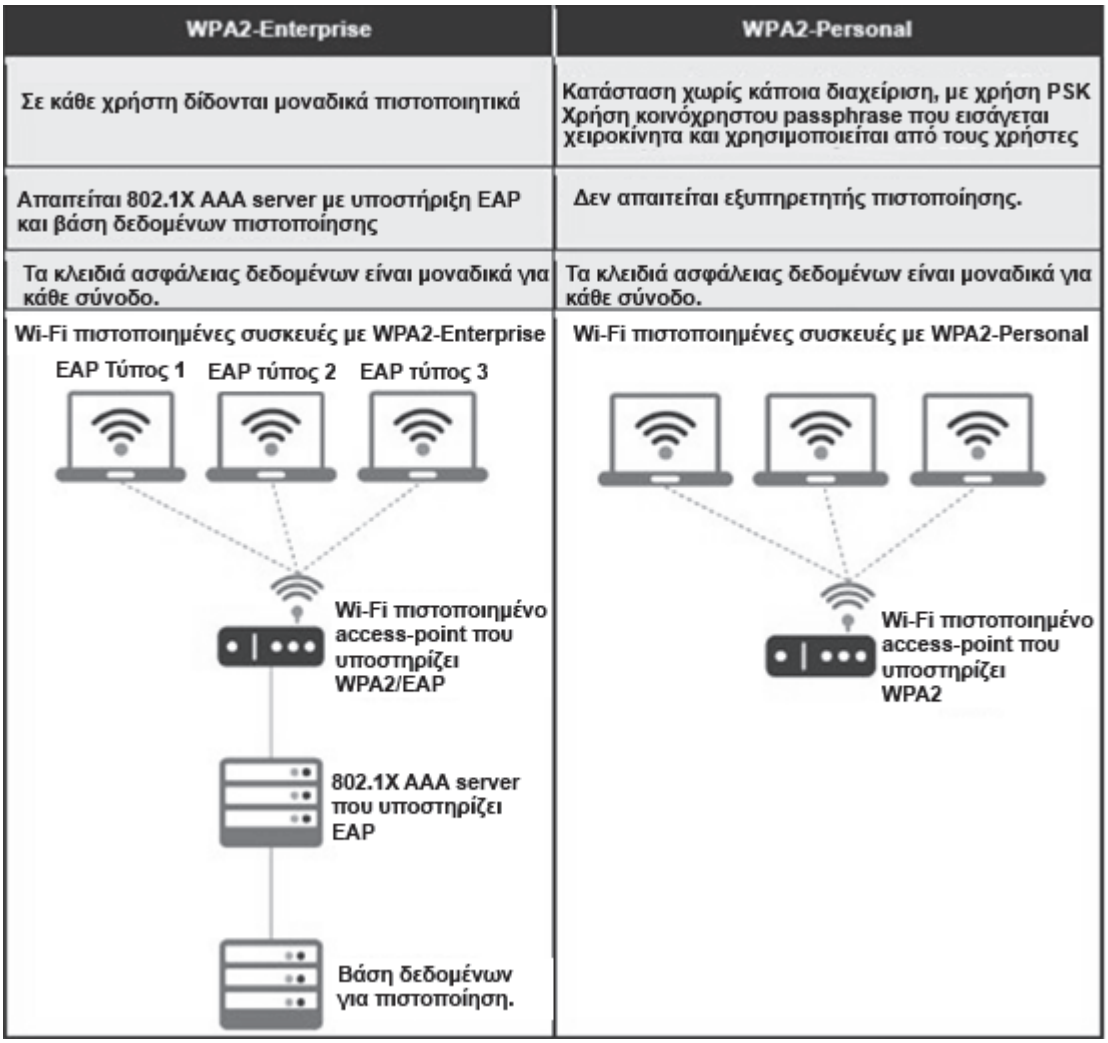
key αποτελείται από Nb λέξεις, επιλέγεται κάθε φορά η επιθυμητή λέξη. Η πράξη αυτή υλοποιείται σαν απλή XOR πράξη ανάμεσα στα bits των ποσοτήτων (bitwise XOR). Η πράξη αυτή μεταφράζεται μαθηματικά στην εξής σχέση:

$$[S'_{0,c}, S'_{1,c}, S'_{2,c}, S'_{3,c}] = [S_{0,c}, S_{1,c}, S_{2,c}, S_{3,c}] \oplus [W_{round*Nb+c}]$$

για $0 \leq c < Nb$

WPA2-Enterprise και WPA2-Personal

Το WPA2 λειτουργεί σε δύο τρόπους, *Enterprise* και *Personal*, ανάλογα με τις απαιτήσεις του δικτύου. Η υποστήριξη για WPA2-Personal είναι υποχρεωτική σε όλες τις επικυρωμένες συσκευές Wi-Fi και τα σημεία πρόσβασης των πελατών. Η υποστήριξη για WPA2-Enterprise είναι προαιρετική, αλλά συστήνεται για συσκευές που λειτουργούν σε μεγάλης κλίμακας δίκτυα. Οι συγκεκριμένες απαιτήσεις ασφάλειας υπαγορεύουν ποιος τρόπος χρησιμοποιείται μέσα σε ένα δίκτυο.
Τα οικιακά και μικρά δίκτυα γραφείων χρησιμοποιούν τυπικά *WPA2-Personal*, επειδή δεν απαιτείται οποιοσδήποτε εξοπλισμός πέρα από ένα *Wi-Fi Certified* σημείο πρόσβασης και μια συσκευή. Στο WPA2-Personal, το κλειδί παράγεται από το καθορισμένο SSID (Service Set Identifier) και μία φράση εισόδου (*passphrase*) που εισάγονται από το χρήστη. Απαιτείται η επιλογή ενός ισχυρού passphrase προκειμένου να εκμεταλλευθεί πλήρως την προστασία WPA2. Τα μακριά, σύνθετα, και τυχαία pass phrases , όπως και οι συχνές αλλαγές passphrase, είναι κρίσιμα για την καλή ασφάλεια.
Τα δίκτυα επιχειρήσεων με IEEE 802.1x AAA (*Authentication, Authorization, Accounting*) εξυπηρετητές μπορούν να ωφεληθούν από την περιπλοκότερη λειτουργία που διατίθεται από το *WPA2-Enterprise*, το οποίο περιλαμβάνει τη δυνατότητα να ελέγξει και να διαχειριστεί την κυκλοφορία, να καθορίσει τα ειδικού χρήστη επίπεδα πιστοποίησης, και να προσφέρει πρόσβαση στους φιλοξενούμενους. Το WPA2-Enterprise επιτρέπει επίσης στην ασύρματη πρόσβαση να ενσωματώνεται με γενικό έλεγχο προσπέλασης δικτύου που επιτυγχάνεται με καταμερισμό των υπαρχόντων βάσεων δεδομένων χρηστών.



Εικόνα 30 Μηχανισμός πιστοποίησης σε WPA2-Enterprise και WPA2-Personal.

- **Προηγμένη ασφάλεια με 802.1x και EAP**

Το 802.1x παρέχει μια δομή πιστοποίησης (network port authentication) στα WLANs, επιτρέποντας σε έναν χρήστη να επικυρώνεται από μια κεντρική αρχή. Η δομή αυτή αποτελείται από τρία συστατικά μέρη:

Supplicant (συνήθως το λογισμικό πελατών)
Authenticator (συνήθως το AP) συνδέεται με το δίκτυο του τοπικού LAN
Εξυπηρετητής Πιστοποίησης/AS, *Authentication Server* – AS

Το 802.1x χρησιμοποιεί το EAP , ένα υπάρχον πρωτόκολλο (RFC 2284) που λειτουργεί σε Ethernet, token ring, ή WLANs για την ανταλλαγή μηνυμάτων κατά τη διάρκεια της διαδικασίας πιστοποίησης.

3. Συγκριτική μελέτη αλγορίθμων κρυπτογράφησης πρωτόκολλων WLAN

3.1 Μέτρα Αξιολόγησης Ενός Δικτύου

Η αξιολόγηση μιας αρχιτεκτονικής δικτύου είναι πολύπλοκη υπόθεση και απαιτεί την εξέταση πολλών παραμέτρων. Όσον αφορά την ικανότητα ενός δικτύου να υποστηρίξει εφαρμογές πολυμέσων, μπορούμε να διακρίνουμε έξι παράγοντες καθοριστικής σημασίας:

1. Ρυθμός Εξυπηρέτησης (Throughput)
2. Καθυστέρηση Μεταφοράς (Transit Delay)
3. Μεταβλητότητα της Καθυστέρησης (Delay Variation)
4. Ισοχρονισμός (Isochronism)
5. Mutlticasting
6. Ρυθμοί Λαθών (Error Rates)

Παρακάτω εξηγούνται ορισμοί που θα μας απασχολήσουν σε αυτό το κεφάλαιο.

Καθυστέρηση

Η χρονική καθυστέρηση που περικλείεται στην κίνηση της μεταφοράς των δεδομένων μέσω του δικτύου. Οι τρείς πηγές της καθυστέρησης είναι η καθυστέρηση στην εξάπλωση (propagation delay), που προκαλείται από τον απαραίτητο χρόνο που χρειάζονται τα δεδομένα για να ταξιδέψουν κατά μήκος του συνδέσμου, η καθυστέρηση μετάδοσης, που είναι ο ακριβής χρόνος απαραίτητος για τα δεδομένα να μετακινηθούν κατά μήκος του δικτύου και η καθυστέρηση επεξεργασίας που είναι ο απαραίτητος χρόνος για την ενθυλάκωση των πακέτων και την εγκαθίδρυση διαδρομής.

Επιβάρυνση (Overhead)

Ο χρόνος παράλληλης εκτέλεσης που δαπανάται για το συντονισμό των παραλλήλων εργασιών σε αντίθεση με τον χρόνο ωφέλιμου υπολογισμού (δηλαδή αυτόν που εκτελεί το πρόγραμμα και στην ακολουθιακή του μορφή). Η επιβάρυνση εξαρτάται από παράγοντες όπως: Δημιουργία και διανομή εργασιών, συγχρονισμός, επικοινωνία, τερματισμός εργασιών, κλήσεις συστήματος, χρήση βιβλιοθηκών, οδηγίες μεταγλωττιστών κλπ

Ρυθμός Εξυπηρέτησης (Throughput)

Το δείκτη αυτό τον έχουμε ήδη χρησιμοποιήσει με τα ονόματα bit rate, ρυθμό μεταφοράς δεδομένων (transfer rate) ή εύρος ζώνης (bandwidth). Ο τελευταίος όρος τυπικά αναφέρεται στο εύρος συχνοτήτων ενός μέσου μετάδοσης, αλλά γενικεύεται κατά αναλογία και στην περίπτωση του δικτύου. Ο ρυθμός εξυπηρέτησης μπορεί να οριστεί ως εξής:
Ο ρυθμός μεταφοράς των δεδομένων μεταξύ δύο συστημάτων ορίζεται ως το πλήθος των δυαδικών ψηφίων (ή πακέτων) που μπορεί να δεχτεί και μεταδώσει το δίκτυο στη μονάδα του χρόνου και επηρεάζεται από τον επεξεργαστή την λειτουργία του δίσκου, τις δυνατότητες του λειτουργικού συστήματος τους περιορισμούς του δικτυακού υλικού και την ποσότητα των δεδομένων που μεταδίδονται.
Ο ορισμός αυτό έχει ένα κρυφό σημείο. Δεν καθορίζει ακριβώς τον τρόπο μέτρησης του ρυθμού εξυπηρέτησης. Έτσι μια τιμή μπορεί να αναφέρεται στο μέγιστο ρυθμό εξυπηρέτησης είτε στο ρυθμό εξυπηρέτησης που μπορεί να διατηρηθεί σταθερός από το δίκτυο.

Οι συνήθεις μονάδες μέτρησης είναι τα πολλαπλάσια του bps (bits per second): Kbps, Mbps, Gbps. Σε δίκτυα όπου η πληροφορία μεταδίδεται σε πακέτα, μπορούμε να μιλήσουμε για packets/sec.
Στο ορισμό παρατηρούμε μια διαφοροποίηση μεταξύ του μέγιστου δυνατού ρυθμού αποδοχής των δεδομένων, που θα ονομάσουμε ρυθμό ή ταχύτητα πρόσβασης (access speed), και του ρυθμού μετάδοσης τους από το δίκτυο. Πράγματι, υπάρχουν δίκτυα, όπως τα περισσότερα από αυτά που χρησιμοποιούν διαμεταγωγή με πακέτα, που δέχονται δεδομένα τα οποία όμως, για διάφορους λόγους, δεν μπορούν να μεταδοθούν αμέσως και τοποθετούνται σε ουρές αναμονής. Αντίθετα, τα δίκτυα μεταγωγής κυκλώματος μπορούν να εξασφαλίσουν σταθερό bit rate παρόμοιο με αυτό του ρυθμού εισόδου πελατών.
Τα περισσότερα προϊόντα **802.11n ρίχνουν το throughput μέχρι 80% εάν χρησιμοποιείται ασφάλεια WEP ή WPA/TKIP**. Η αιτία είναι ότι οι προδιαγραφές 802.11n υποστηρίζουν ότι οι υψηλότεροι ρυθμοί throughput (ρυθμός συνδέσμου πάνω από 54 Mbps) δεν μπορούν να ενεργοποιηθούν εάν χρησιμοποιείται μία από αυτές τις απαρχαιωμένες μεθόδους ασφάλειας.
Οι μόνες εξαιρέσεις είναι κάποια προϊόντα τα οποία δεν είναι Wi-Fi πιστοποιημένα για 802.11n. Η σουίτα ελέγχου πιστοποίησης Wi-Fi ελέγχει για σωστή λειτουργία με χρήση WEP, WPA και WPA2. Αλλά εάν οι κατασκευαστές δεν υποβάλουν τα προϊόντα τους για πιστοποίηση, ίσως δεν "ξεκλειδώσουν" τους υψηλότερους ρυθμούς. Επιπρόσθετα, μπορεί να χρησιμοποιηθεί μόνο ασύρματη ασφάλεια WPA2/AES (ή καθόλου ασφάλεια) εάν δεν θέλουμε να χάσουμε πολλή ταχύτητα.
Όμοια, το WMM (Wi-Fi Multimedia) πρέπει να είναι ενεργοποιημένο με σκοπό την επίτευξη ταχυτήτων συνδέσμου υψηλότερων των 54 Mbps. Βασικά, οι προδιαγραφές 802.11n απαιτούν οι συσκευές να υποστηρίζουν το **802.11e** (εμπλουτισμός Quality of Service, QoS, για ασύρματα LAN) για χρήση **HT** (High Throughput) ρυθμών συνδέσμου υψηλότερων των 54 Mbps.
Το WMM είναι υποσύνολο του 802.11e που δημιουργήθηκε από την Wi-Fi Alliance σαν μέτρο παύσης ενώ το 802.11e εισερχόταν αργά μέσω την IEEE διαδικασίας αναθεώρησης. Το πεδίο του WMM, το **Traffic Identifier (TID),** είναι το κλειδί του μηχανισμού συσσώρευσης, το οποίο περιλαμβάνει **block acknowledgement (block ACK)**, και επιτρέπει στο 802.11n υψηλούς ρυθμούς throughput.

3.2 WLAN χαρακτηριστικά αρμόδια για τον σχεδιασμό των πρωτόκολλων ασφάλειας

Roaming

Είναι η ικανότητα να διανέμονται οι υπηρεσίας στους ασύρματους σταθμούς έξω από την βασική περιοχή υπηρεσίας (Basic Service Area). Όταν ένας ασύρματος σταθμός περιηγείται, πρέπει να εκτελείται νέα πιστοποίηση μέσω του ασύρματου μέσου για να διαβεβαιώσει την νέα αυθεντικότητα της επικοινωνίας και το καινούριο κλειδί συνόδου από την μη πιστοποιημένη πρόσβαση και χρήση. Σε αυτή τη περίπτωση είναι επιθυμητό ο καινούριος μηχανισμός ασφάλειας που εκτελείται στην καινούρια περιοχή της υπηρεσίας να διαφυλάσσεται minimal για να βεβαιώνει παρόμοια μεταφορά μεταξύ των περιοχών.

Μείωση της κατανάλωσης ενέργειας

Αφού τα WLAN προορίζονται για ασύρματους σταθμούς με φορητή μπαταρία, η χαμηλή κατανάλωση ενέργειας είναι ένας πολύ σημαντικός παράγοντας. Έτσι, ο προηγμένος μηχανισμός ασφάλειας θα πρέπει να χρησιμοποιεί χαμηλής πολυπλοκότητας κρυπτογραφικούς αλγόριθμους.

Περιορισμένο Bandwidth

Το περιορισμένο φάσμα συχνοτήτων ISM που προσδιορίζεται από το FCC και οι απαιτήσεις για την χρήση επικοινωνίας εξάπλωσης φάσματος (spread spectrum) περιορίζει τον ρυθμό δεδομένων (data rate). Για παράδειγμα το IEEE 802.11 πρότυπο ορίζει ρυθμό δεδομένων μέχρι 2Mbps. Αυτό το χαρακτηριστικό απαιτεί σχεδιασμό πρωτόκολλου ασφάλειας που ελαχιστοποιεί τον αριθμό των μηνυμάτων που ανταλλάσσονται στο ασύρματο μέσο.

Κανάλι με θόρυβο

Στα WLAN ο ρυθμός σφάλματος bit (bit error rate) σχετίζεται πολύ με το ενσύρματο μέσο μετάδοσης. Αυτό το χαρακτηριστικό υπαγορεύει στα ασύρματα πρωτόκολλα, τα οποία ενσωματώνουν κατάλληλες διατάξεις, για λανθασμένα μηνύματα και διαδικασίες αναμετάδοσης.

3.3 Σύγκριση ασύρματων πρωτόκολλων ασφάλειας

Όπως είδαμε και στα προηγούμενα κεφάλαια, τα ασύρματα τοπικά δίκτυα έχουν κερδίσει την δημοτικότητα λόγω του ότι είναι οικονομικά, ευέλικτα, γρήγορα και εύκολα στην χρήση. Ωστόσο, αντιμετωπίζουν κάποιες σοβαρές προκλήσεις όσων αφορά την ασφάλεια και η επιλογή του πρωτόκολλου ασφάλειας είναι ένα κρίσιμο θέμα για τους IT administrators.
Η επιρροή των πολλών σχεδίων ασφάλειας στην λειτουργία του δικτύου μελετήθηκε από διάφορους ερευνητές με αναφορικά με το throughput των δικτύων IEEE 802.11, κάτω από διαφορετικό φόρτο (load), φυσιολογικό και συμφορισμένο, και για ποικίλα μεγέθη πακέτων κίνησης (από 100 bytes έως 1500 bytes). ***Τα αποτελέσματα που προέκυψαν έδειξαν ότι για όλα τα φορτία δικτύου και τα μεγέθη πακέτων το WEP προσφέρει την καλύτερη λειτουργία δικτύου***. Η χρήση του WPA οδηγεί στην μετρίαση της λειτουργίας του δικτύου (με τη χρήση της κρυπτογράφησης TKIP) και σχεδόν την ίδια λειτουργία δικτύου με το WEP χρησιμοποιώντας AES κρυπτογράφηση αντί για TKIP.
Τελικά, ***το IEEE 802.11i προσφέρει την πιο αδύναμη λειτουργία δικτύου εξαιτίας της επιπλέον απαιτούμενης επεξεργασίας της πιστοποίησης, της κρυπτογράφησης, και τη δημιουργία των συσχετίσεων ασφάλειας. Το IEEE802.11i είναι πολύ καλή επιλογή για την ασφάλεια των WLAN σε μεγάλης κλίμακας περιβάλλοντα δικτύων.***
Τα ασύρματα AP και οι κάρτες δικτύου από τους προμηθευτές hardware (όπως CISCO, 3Com και Siemens) υποστηρίζουν όλα τα πρωτόκολλα ασφάλειας WLAN. Αυτά τα προϊόντα είναι κατάλληλα για μεγάλα δίκτυα. Καθώς το WPS μπορεί να χρησιμοποιηθεί για να απλοποιήσει την εγκατάσταση ασφάλειας και την διαχείριση μικρών και μεσαίων ασύρματων δικτύων, προτείνεται η χρήση ασύρματων προϊόντων που υποστηρίζουν WPS όπως: 3Com, Belkin, Broadcom, Brother, Buffalo, Linksys, D-link, Fujitsu, Intel και HP.
Καταλήγουμε ότι ***η επιλογή του καταλληλότερου πρωτόκολλου ασφάλειας εξαρτάται από τους παρακάτω παράγοντες***:

- Ο βαθμός ασφάλειας που προσφέρεται από το κάθε πρωτόκολλο.
- Πόσο συνεισφέρουν αυτά τα πρωτόκολλα στην μείωση της λειτουργίας του δικτύου.
- Οι απαιτούμενες αναβαθμίσεις υλικού και λογισμικού για την εφαρμογή των διαφορετικών ασύρματων πρωτοκόλλων.
- Την πιθανότητα υλοποίησης αυτών των πρωτόκολλων σε παλαιό ασύρματο υλικό.
- Τί πρωτόκολλο ασφάλειας είναι κατάλληλο για συγκεκριμένο μέγεθος δικτύου (μικρό, μεσαίο, μεγάλο).

Επειδή υπάρχει μια συναλλαγή μεταξύ ασφάλειας και λειτουργίας, και η απόφαση εξαρτάται από τους παραπάνω τρείς παράγοντες, γι’ αυτό αν ο επιθυμητός βαθμός

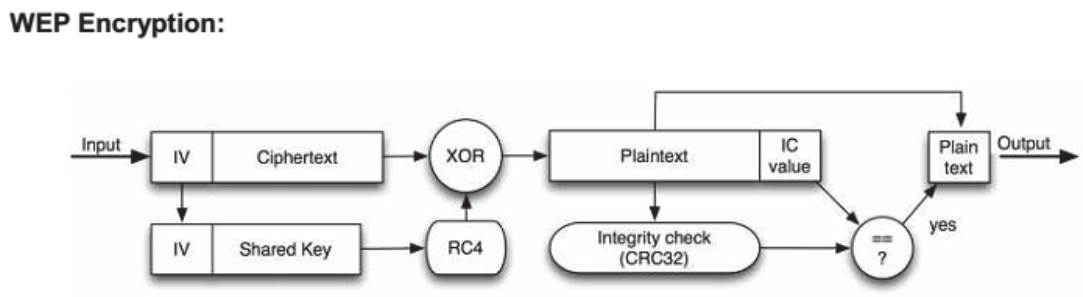
ασφάλειας είναι υψηλός, τότε το IEEE802.11i είναι η καλύτερη επιλογή σε βάρος της χαμηλότερης λειτουργίας δικτύου. Εάν ο επιθυμητός βαθμός ασφάλειας είναι μέτριος τότε το WPA είναι καλή επιλογή, ειδικά εάν αναμειγνύεται με την κρυπτογράφηση AES για να προσφέρει ισχυρότερη ασφάλεια και υψηλότερη λειτουργία δικτύου. Τελικά, ***λόγω των αδύναμων χαρακτηριστικών ασφάλειας του WEP προτείνεται η χρήση μεθόδων ασφάλειας WEP μόνο στις συσκευές κληρονομιάς και για οικιακές συσκευές.***

Παρακάτω εξετάζονται τα ασύρματα πρωτόκολλα ασφάλειας και συγκρίνονται ως προς την ταχύτητα, το overhead, την απόδοση και την αποτελεσματικότητα των αλγορίθμων κρυπτογράφησης ασύρματης επικοινωνίας.

3.4 Αδυναμία του WEP

Ένα υψηλό ποσοστό των ασύρματων δικτύων έχουν απενεργοποιημένο το WEP λόγω του ***administrative overhead της διαχείρισης ενός κοινού κλειδιού WEP***.
Το WEP έχει το ίδιο πρόβλημα με όλα τα συστήματα που βασίζονται σε κοινά κλειδιά:

1. οποιοδήποτε μυστικό κρατιέται από περισσότερους του ενός ατόμου σύντομα γίνεται κοινώς γνωστό. Ένα παράδειγμα είναι κάποιος εργαζόμενος που αφήνει μια εταιρία και γνωρίζει ακόμα το κοινό WEP κλειδί, και θα μπορούσε να κάτσει έξω από την εταιρία και να κάνει sniffing στην κίνηση του δικτύου ή ακόμα και να επιτεθεί σε ένα εσωτερικό δίκτυο.
2. Το IV (διάνυσμα αρχικοποίησης, initialization vector) το οποίο εφοδιάζει τον αλγόριθμο WEP στέλνεται καθαρό.
3. Το WEP checksum (άθροισμα ελέγχου) είναι γραμμικό και προβλέψιμο.



Εικόνα 31 Κρυπτογράφηση WEP.

3.5 Αδυναμία του WPA/WPA2

Η μόνη διαφορά μεταξύ WPA και WPA2 είναι η προϋπόθεση χρήσης της κρυπτογράφησης CCMP με WPA2. Όπως το WPA, έτσι και το WPA2 είναι διαθέσιμο σε personal και enterprise καταστάσεις. Το WPA2 επιτρέπει μια εύκολη μετάβαση από την κατάσταση WPA χρησιμοποιώντας ανάμεικτη κατάσταση WPA/WPA2, έτσι οι δικτυωμένοι υπολογιστές μπορούν να χρησιμοποιήσουν είτε WPA ή WPA2. Δεν λειτουργεί τον RC4 όπως στο WEP και WPA αλλά χρησιμοποιεί πρωτόκολλο Counter Mode με CBC-MAC (CCMP) για να κρυπτογραφήσει την κίνηση του δικτύου. Το CCMP εφαρμόζει AES (Advanced Standard Encryption) αλγόριθμο κρυπτογράφησης. Το 802.11 είναι προς τα πίσω συμβατό με το WPA αλλά όχι με το WEP.
Έτσι το WPA2 είναι περισσότερο ασφαλές μεταξύ των υπαρχόντων πρωτόκολλων ασφάλειας αλλά έχει μερικές ***πολυπλοκότητες που σχετίζονται με το overhead της κρυπτογράφησης***. ***Η υψηλή κατανάλωση ενέργειας ακόμα θέτει προβλήματα στο WPA2***. *Το overhead που σχετίζεται με το WPA2 μεγαλώνει δραστικά εξαιτίας του ισχυρού μηχανισμού AES σε αυτό το*

πρωτόκολλο. Όπως το WEP, έτσι και το WPA2 χρησιμοποιεί μόνο έναν αλγόριθμο και ένα κλειδί για να κρυπτογραφήσει και να αποκρυπτογραφήσει όλα τα πακέτα. Έτσι λοιπόν, εάν ο μηχανισμός δεσμευτεί μια φορά δεν μπορεί να συντηρηθεί. ***Επίσης, όταν το δίκτυο είναι μεγάλο με πολλούς κόμβους, το overhead στην λειτουργία του δικτύου που σχετίζεται με το WPA2 είναι πολύ υψηλό***. Παρόλο που το σχέδιο ασφάλειας WPA/WPA2 είναι ισχυρό, *έχουν ήδη υλοποιηθεί επιθέσεις εναντίον τους*. Αυτές οι επιθέσεις βασίζονται στην τάση των χρηστών να χρησιμοποιούν αδύναμους κωδικούς πρόσβασης που είναι εύκολοι να μαντευθούν. Το Cowpatty είναι ένα εργαλείο που βρίσκει όλους τους πιθανούς συνδυασμούς κλειδιού (brute force) ξεκινώντας από τις πιο εύκολες επιλογές. Με αυτή την στρατηγική μπορεί να σπάσει ένας εύκολος κωδικός πρόσβασης. Η πηγή αυτού του προβλήματος έγκειται στην έλλειψη ευχρηστίας, με άλλα λόγια, όταν εγκαθίσταται ένα ασύρματο δίκτυο, οι χρήστες ακόμα πρέπει να εισάγουν τα κλειδιά χειροκίνητα, το οποίο καταναλώνει χρόνο και μπορεί να αποτελεί πρόκληση για τους αρχάριους. Έτσι, το σχήμα ασφάλειας WPA/WPA2 χρειάζεται ακόμα ανάπτυξη.

3.6 Σύγκριση WEP-WPA

Το WEP και το WPA χρησιμοποιούν και τα δύο για κρυπτογράφηση τον RC4 stream cipher. Ωστόσο, αντί του κανονικού συνδυασμού 24-bit IV και 40/104-bit κλειδιού του WEP, το WPA λειτουργεί ένα 48-bit μαζί με ένα 128-bit κλειδί. Η μη επαρκής ασφάλεια του WEP ήταν αποτέλεσμα των συγκρούσεων IV και των τροποποιημένων πακέτων. Στο WPA, αυτά τα προβλήματα έχουν εξαλειφτεί με έναν συνδυασμό TKIP (Temporal Key Integrity Protocol), με MIC (Message Integrity Check) και επεκταμένο διάστημα IV. Η ιεραρχία του κλειδιού του TKIP ανταλλάσει το μοναδικό στατικό κλειδί του WEP για περίπου 500 τρισεκατομμύρια πιθανά κλειδιά που μπορούν να χρησιμοποιηθούν για την κρυπτογράφηση ενός πακέτου. Συνδυασμένο με ένα 48-bit IV, το TKIP κάνει αποτελεσματικά ακατόρθωτες τις επιθέσεις που βασίζονται σε ανάκτηση κλειδιού. Το MIC και ο αλγόριθμος κρυπτογράφησης Michael, βάζουν ένα φράγμα στην πλαστογραφία πακέτου που ήταν πιθανή στο WEP λόγω της γραμμικότητας του CRC.
Το πλαίσιο framework 802.1X/EAP και PSK-mode παρέχει στο WPA ένα συγκεκριμένο μηχανισμό για πιστοποίηση χρήστη, που λείπει σε μεγάλο βαθμό στο WEP. Όπως ειπώθηκε νωρίτερα, στο WEP, ο χρήστης μπορούσε να πιστοποιηθεί μέσω μηχανισμού πιστοποίησης Shared-Key, ένα προαιρετικό χαρακτηριστικό που εμπεριέχει την χρήση προκλήσεων. Αυτό το σχήμα βασίζεται στη χρήση του ίδιου pre-shared WEP κλειδιού που χρησιμοποιείται στην κρυπτογράφηση, με αποτέλεσμα να αποδειχθεί κίνδυνος για την ασφάλεια. *Στο WPA η κρυπτογράφηση και η πιστοποίηση είναι ξεχωριστά.* Αφού κάποιος πιστοποιηθεί στον 802.1X server/AP με πιστοποιητικά/passphrase τα κλειδιά διανέμονται στον χρήστη αυτόματα.
Συνοπτικά, το IEEE 802.11i ξεπερνά τα προβλήματα των προκάτοχων του, εξαιτίας των *πλεονεκτημάτων του CCMP* πρωτοκόλλου και των λειτουργιών που το απαρτίζουν, τα οποία συνοψίζονται παρακάτω:

- Προστατεύει την εμπιστευτικότητα των δεδομένων χρησιμοποιώντας την λειτουργία Counter σε συνδυασμό με τον αλγόριθμο AES, η οποία αποτελεί μία ισχυρή μέθοδο κρυπτογράφησης.
- Προστατεύει την ακεραιότητα του μηνύματος και πιστοποιεί τον χρήστη μέσω της χρήσης του MIC. Επιπλέον, η χρήση του MIC προστατεύει τις διευθύνσεις πηγής και προορισμού από τροποποιήσεις.
- Προστατεύει τους χρήστες από τις επιθέσεις επανάληψης πακέτων, καθώς χρησιμοποιεί ακολουθιακούς αριθμούς πακέτων.
- Απαγορεύει την επαναχρησιμοποίηση κλειδιού. Ο

CCMP χρησιμοποιεί το TK, το οποίο έχει προκύψει κατά την διάρκεια της πιστοποίησης και συγκεκριμένα κατά την διάρκεια του 4-way handshake. Το IEEE 802.11i καθορίζει ότι οι παράγοντες αρχικοποίησης των λειτουργιών CBC-MAC και COUNTER, ποτέ δεν επαναχρησιμοποιούνται με το ίδιο κλειδί.

Παρακάτω φαίνεται η σχέση μεταξύ WPA2, WPA και WEP.

WEP	WPA	WPA2
Προδιαμοιραζόμενο κλειδί το οποίο εγκαθίσταται χειροκίνητα στα τερματικά και στο BSS/ESS	802.1X για πιστοποίηση και διανομή κλειδιών. Υποστηρίζει και προδιαμοιρασμένα κλειδιά όπως το WEP	το ίδιο με το WPA
Χρησιμοποιεί σύγχρονο κρυπταλγόριθμο ροής (RC4) που είναι ακατάλληλος για ασύρματες ζεύξεις	Το ίδιο με το WEP	Αντικαθιστά τον RC4 με κρυπταλγόριθμο block, τον AES
Παράγει ένα κλειδί ανά πακέτο με το να προσθέτει απευθείας το IV στο master κλειδί, το οποίο πλέον είναι εκτεθειμένο σε επιθέσεις τύπου FMS	Εισάγει την έννοια του PTK στην ιεραρχία κλειδιών. Χρησιμοποιεί μια συνάρτηση αναδιανομής κλειδιών.	Το ίδιο με το WPA
Πολύ περιορισμένο εύρος κλειδιών λόγω στατικού master κλειδιού, μικρού IV και παραγωγής κλειδιού ανά πακέτο.	Αυξάνει το IV σε 56bits φυλάσσοντας τα 8bits για να απορρίπτει αδύναμα κλειδιά. Μεγαλύτερο σύνολο κλειδιών λογω καινούριου PTK για κάθε σύνοδο	Το ίδιο με το WPA
Πολύ πιθανή η επαναχρησιμοποίηση κλειδιών λόγω προαιρετικής αλλαγής του IV	Καθορίζει αυστηρά ότι πομπός και δέκτης αρχικοποιούν το IV σε 0 για κάθε καινούριο PTK και το αλλάζουν μετά από κάθε αποστολή πακέτου	Το ίδιο με το WPA
Ελλείπεις προστασία ακεραιότητας με το CRC-32	Michael αντί για CRC. Επίσης καθορίζει εναλλακτικές στην περίπτωση που ο Michael παραβιαστεί	Πιο ισχυρή προστασία ακεραιότητας με χρήση AES CCMP
Ευάλωτο σε επιθέσεις ανακατεύθυνσης γιατί το ICV δε προστατεύει την ακεραιότητα της επικεφαλίδας του 802.11	Διευρύνει τον υπολογισμό του ICV περιλαμβάνοντας τις MAC διευθύνσεις πομπού και δέκτη	Το ίδιο με το WPA
Καμιά προστασία απέναντι σε επιθέσεις επανάληψης	Η χρήση του IV ως αύξοντα αριθμού σειράς παρέχει ασφάλεια σε τέτοιες επιθέσεις	Το ίδιο με το WPA
Καμιά υποστήριξη ώστε τα τερματικά να πιστοποιήσουν το δίκτυο	Το 802.1X θα μπορούσε να χρησιμοποιηθεί από τις συσκευές για την πιστοποίηση του δικτύου	Το ίδιο με το WPA

Εικόνα 32 Σύγκριση αρχιτεκτονικών ασφάλειας WEP, WPA, WPA2.

3.7 AES έναντι TKIP: Μία δικτυακή επισκόπηση

Κάθε πρωτόκολλο έχει τις μοναδικές δυνάμεις και αδυναμίες του που το κάνουν περισσότερο ή λιγότερο κατάλληλο για συγκεκριμένες εφαρμογές. Παρά το γεγονός ότι τα AES και TKIP είναι σχεδιασμένα για να διαχειρίζονται διαφορετικές καταστάσεις, ανακαλύψεις πάνω σε αυτά τα πρωτόκολλα έδειξαν πως είναι αρκετά λιγότερο κατάλληλα για χρήση όταν η ασφάλεια είναι σημαντική.
Ο κύριος λόγος για τον οποίο ο RC4 είναι δημοφιλής είναι το γεγονός ότι είναι απλός και μπορεί να γίνει πολύ γρήγορος. Αυτός έχει ήδη κατευναστεί από τότε

που οι *AES* υλοποιήσεις στο hardware γίνονται πολύ δημοφιλείς καθώς αυτός *παρέχει πλεονεκτήματα στην ταχύτητα έναντι των υλοποιήσεων λογισμικού.* Τελευταία, ο RC4 είναι σήμα κατατεθέν (εμπορικό σήμα) αφού αρχικά ήταν ένα εμπορικό μυστικό, το οποίο οδήγησε κάποιους ανθρώπους να προβούν σε εφευρετικούς τρόπους για να ανακαλέσουν την διαρρέουσα περιγραφή το 1994: όπως το ARCFOUR και ARC4 (αποκαλούμενο RC4). Από την άλλη, ο AES είναι δημόσια διαθέσιμος και μπορεί να χρησιμοποιηθεί δωρεάν χωρίς να δημιουργήσει κάποιο νομικό πρόβλημα.
Όπως είδαμε, ο AES (Advanced Encryption Standard) είναι ένα σύνολο κρυπτογραφιών σχεδιασμένος για να εμποδίζει τις επιθέσεις στα ασύρματα δίκτυα. Ο AES διατίθεται ως block ciphers των 128, 192 ή 256 bits εξαρτάται από το hardware που πρόκειται να χρησιμοποιηθεί με αυτόν. Στο κομμάτι της δικτύωσης, ο AES θεωρείται ότι είναι ανάμεσα στους πιο ασφαλής από όλα τα κοινά εγκατεστημένα πακέτα κρυπτογράφησης.
Ο TKIP δεν είναι ακριβώς κρυπτογράφηση αλλά ένα σύνολο αλγορίθμων ασφάλειας που σκοπεύει να βελτιώσει την ολική ασφάλεια των δικτύων WEP. *Ο TKIP είναι software driven και ο AES είναι hardware driven.* Το TKIP προσθέτει αρκετά επιπλέον επίπεδα προστασίας στο WEP, αλλά το πρωτόκολλο έχει μια σημαντική αδυναμία από μόνο του.
Το TKIP είναι ευπαθές σε επίθεση ανάκτησης keystream, μια μέθοδος που χρησιμοποιείται από hackers όπου το ασύρματο δίκτυο βασικά αποκαλύπτει το κλειδί δικτύου σε εκείνους που ξέρουν πως να εμποδίζουν και να αναλύουν κατάλληλα τα δημόσια δεδομένα τα οποία δημιουργεί το δίκτυο . Η ευπάθεια του TKIP σε αυτό το είδος επίθεσης είναι μια σοβαρή παράβλεψη καθώς η επίθεση, γνωστή κοινώς ως chop-chop επίθεση είναι παλαιότερη από το ίδιο το TKIP. *Ως αποτέλεσμα των εγκαθιδρυμένων ευπαθειών και του WEP και του TKIP η απέραντη πλειοψηφία των κατασκευαστών δεν παράγει πια hardware που χρησιμοποιεί αυτά τα πρωτόκολλα.*
Ο AES είναι μακράν η ανώτερη μέθοδος κρυπτογράφησης. *Ο AES δεν είναι μόνο πολύ περισσότερο ασφαλής από το TKIP, είναι κυρίως γρηγορότερος και λιγότερο διεξοδικός στους πόρους από τα παλαιότερα πρωτόκολλα.* Επιπρόσθετα, οι περισσότεροι από τους καινούριους εξοπλισμούς δικτύου είναι εξοπλισμένοι εργοστασιακά με AES. *Οι μόνες εφαρμογές όπου το TKIP είναι καλύτερη επιλογή είναι εκείνες όπου είναι η μόνη επιλογή, δηλαδή παλαιό hardware που δεν έχει την δυνατότητα να τρέξει τον AES*. Ακόμα και σε αυτές τις περιπτώσεις, απαιτείται επαγρύπνηση από την πλευρά του διαχειριστή καθώς ένα δίκτυο που χρησιμοποιεί TKIP είναι αρκετά ευαίσθητο σε επιθέσεις.
Εξαιτίας της σημαντικής ευπάθειας απέναντι στις επιθέσεις chop-chop, ο TKIP είναι κατάλληλος μόνο όταν χρησιμοποιείται με παλαιό hardware ή σε καταστάσεις όπου η ασφάλεια δεν είναι κυρίαρχη. Ο AES, από την άλλη, παραμένει ένα αξιόπιστο και υψηλής ασφάλειας πρωτόκολλο που παρέχει σημαντική προστασία στα ασύρματα δίκτυα.
Ο AES χρειάζεται περισσότερη υπολογιστική ισχύ για να τρέξει έτσι οι μικρές συσκευές όπως το Nintendo DS δεν τον έχουν. Οπουδήποτε ενεργοποιείται η ασφάλεια σε ένα ασύρματο δίκτυο προκαλείται κάποιου είδους σύγκρουση στην εκτέλεση, (performance hit), αφού *η ασφάλεια απαιτεί επιπλέον bandwidth και χρόνο επεξεργασίας. Παραδόξως, το hit για τον AES είναι πολύ πιο μικρό από την πτώση στο WEP ή TKIP!*

3.8 Σύγκριση αποτελεσματικότητας ασύρματης κρυπτογράφησης

Το παρακάτω πείραμα προβάλει μια επισκόπηση των ασύρματων πρωτόκολλων ασφάλειας που χρησιμοποιούνται σήμερα εκθέτοντας την ευπάθεια των ασύρματων τοπικών δικτύων και προβάλλοντας την αποτελεσματικότητά τους. Για το πείραμα αυτό χρησιμοποιήθηκαν τα **BACKTRACK** και **aircrack-ng**. Το Aircrack-ng διαβάζει μέσα σε κάθε μοναδικό IV από όλα τα αρχεία που αιχμαλωτίζονται και μετά εκτελεί μια στατιστική επίθεση σε αυτά τα IV.

Περιλαμβάνει το υλοποιήσεις του φυσικού επιπέδου του και 802.11g με διαθέσιμη MAC layer διαμόρφωση και πιθανούς θεωρητικούς ρυθμούς δεδομένων που καθορίζονται από την IEEE. Τα πρωτόκολλα ασφάλειας που εφαρμόστηκαν σε αυτό το πείραμα περιλαμβάνουν τα WEP, WPA και WPA2.

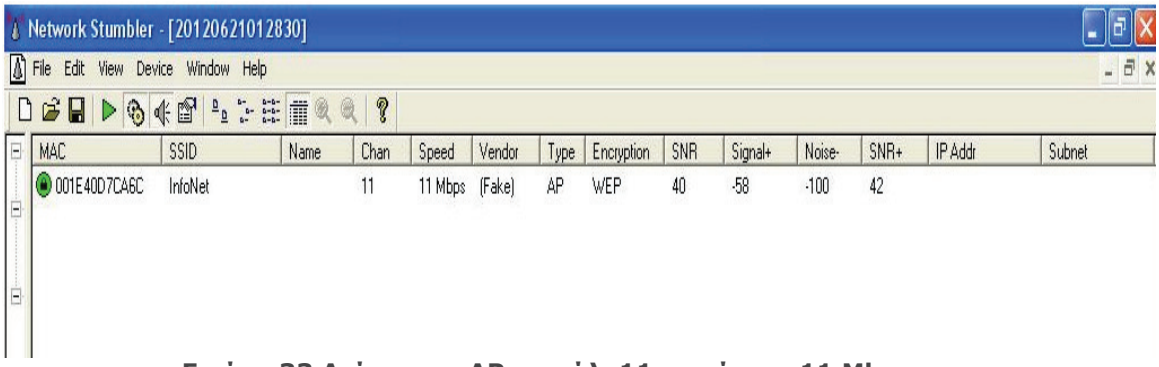
Παράμετροι

Οι μετρήσεις της εκτέλεσης της προσομοίωσης είναι ο συνολικός χρόνος προσομοίωσης, το throughput, το τμήμα διανομής πακέτου και ο μέσος όρος τμήματος end-end διανομής πακέτου.
Μετρήθηκε επίσης η διανομή του συνολικού χρόνου προσομοίωσης και το throughput για 20 και 50 nodes σε διαφορετικούς ρυθμούς δεδομένων.

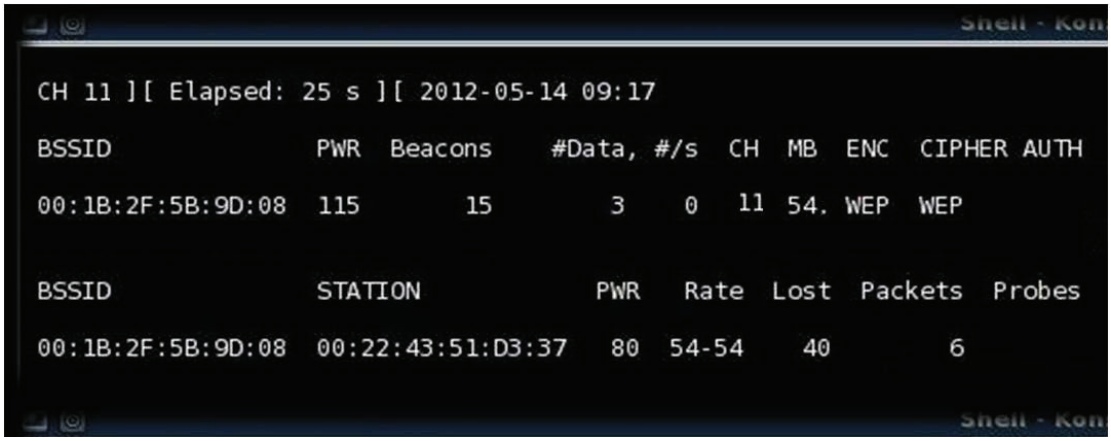
Αποτελέσματα

Στο πείραμα, αποτιμήθηκαν αρκετές διαμορφώσεις για 802.11b και 802.11g δίκτυα και λήφθηκαν αρκετές τιμές λειτουργίας. Παρακάτω τονίζεται η σύγκριση μεταξύ WEP, WPA και του πιο ασφαλούς μηχανισμού WPA2 στα WLAN με βάση ποικίλλων μετρικών λειτουργίας δικτύου. Τα ακόλουθα γραφήματα δείχνουν μερικά από τα ενδιαφέροντα αποτελέσματα της αποτίμησης με χρήση του aircrack-ng και Backtrack.

WEP Αποτελέσματα



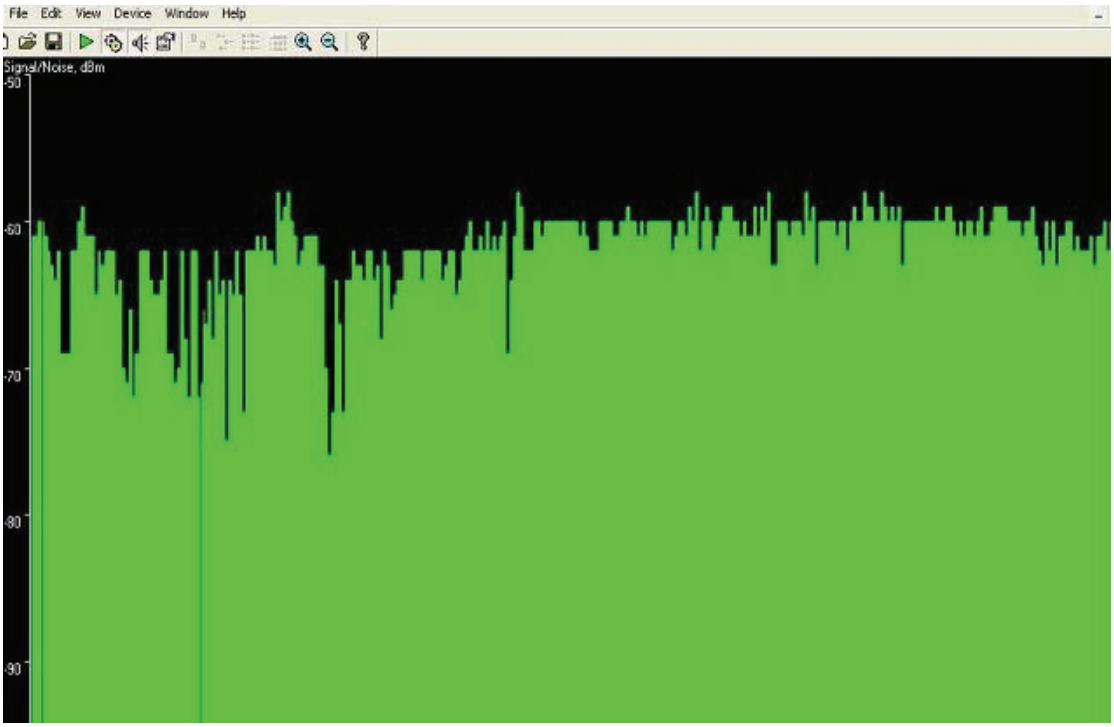
Εικόνα 33 Ανίχνευση AP, κανάλι 11, ταχύτητα 11 Mbps.



Εικόνα 34 Κανάλι 11, χρόνος που χρειάστηκε για σάρωση δικτύου 25sec όταν ακούμε το WLAN Interface για να δούμε ποιοί πελάτες συνδέονται στο συγκεκριμένο AP.

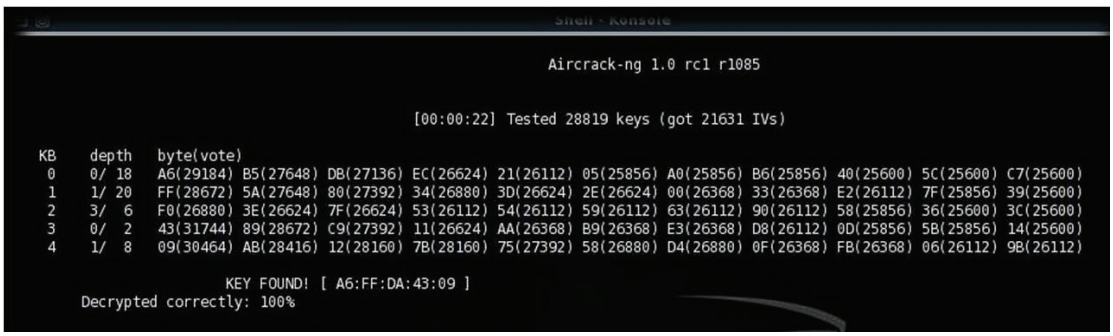
Εδώ φαίνονται οι λεπτομέρειες της περιγραφής του WEP χρησιμοποιώντας BACKTRACK. Διαβάζονται όλα τα ασύρματα δίκτυα που μπορεί να δει ο ασύρματος adapter του συστήματός μας. Σε αυτή το κανάλι που φαίνεται είναι το 11. Αλλά

δεν είναι απαραίτητο να είναι πάντα το κανάλι 11 για αυτό. Εάν αποσυνδέσουμε το modem και το ξανασυνδέσουμε μπορούμε τότε να πάρουμε άλλα κανάλια όπως 12, 44, 53, κτλ.



Εικόνα 35 Σταθερό γράφημα, όχι και η καλύτερη ασφάλεια.

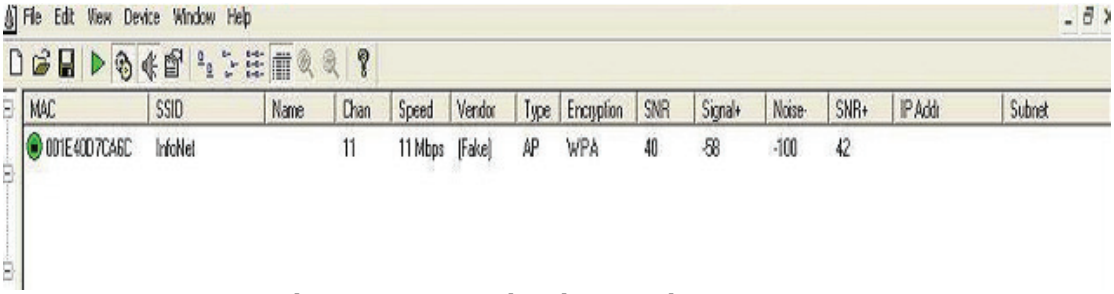
Στο παραπάνω γράφημα, βλέπουμε ότι μετά τις δύο επιθέσεις το γράφημα είναι εντελώς σταθερό το οποίο σημαίνει ότι δεν είναι η καλύτερη ασφάλεια.



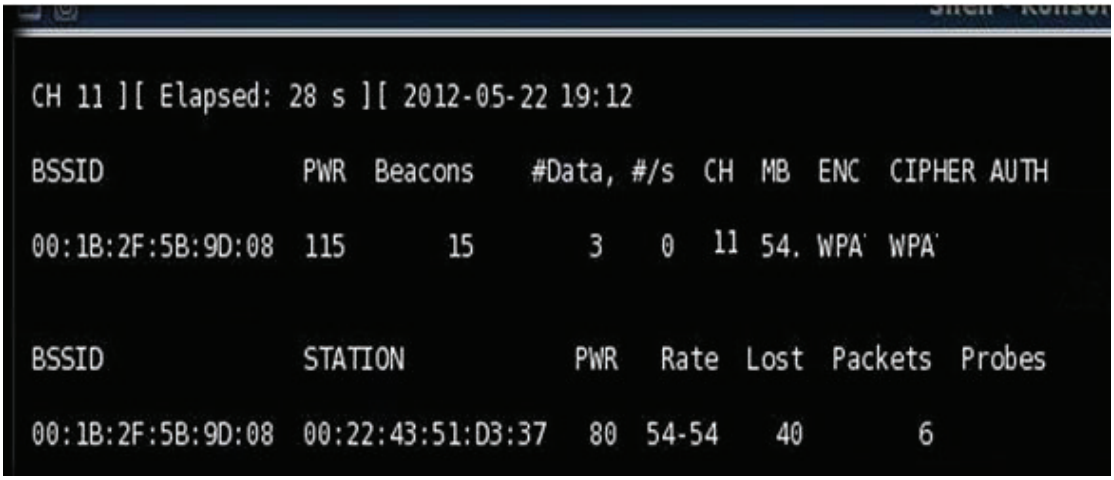
Εικόνα 36 Αποκρυπτογράφηση 100%.

Όπως διαφαίνεται παραπάνω , το WEP cracking έχει γίνει υπερβολικά εύκολο μέσα στα χρόνια, και ενώ στο παρελθόν μπορεί να χρειάζονταν εκατοντάδες, χιλιάδες πακέτα ή μέρες για να αιχμαλωτιστούν τα δεδομένα και να σπάσει το WEP, σήμερα μπορεί να επιτευχθεί μέσα σε λίγα λεπτά περίπου 20kπακέτα δεδομένων. Η επίθεση στο WEP Μπορεί να ελαχιστοποιηθεί ή να γίνει πιο δύσκολη χρησιμοποιώντας μεγαλύτερο μέγεθος IV όπως 48bit IV αντί για 24bit IV και αυτή η ασφάλεια σπάει σε 22 seconds.

WPA Αποτελέσματα

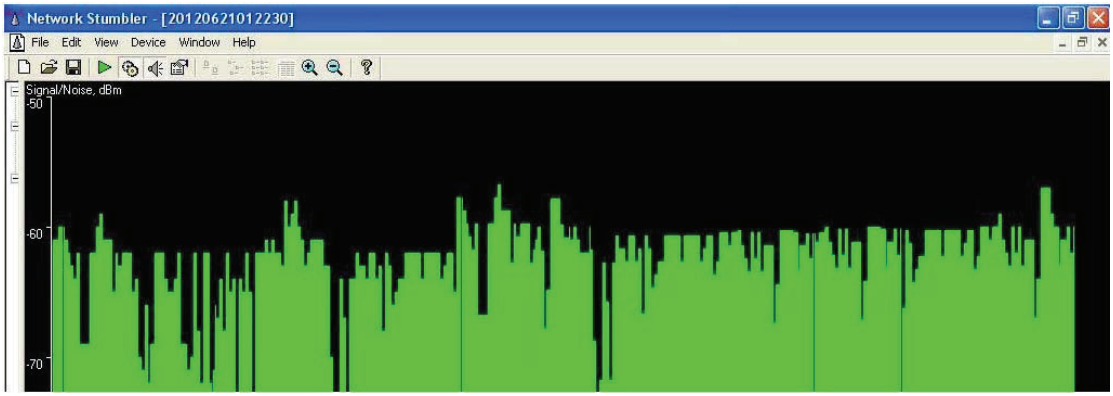


Εικόνα 37 Ίδιο κανάλι, ίδια ταχύτητα με WEP.



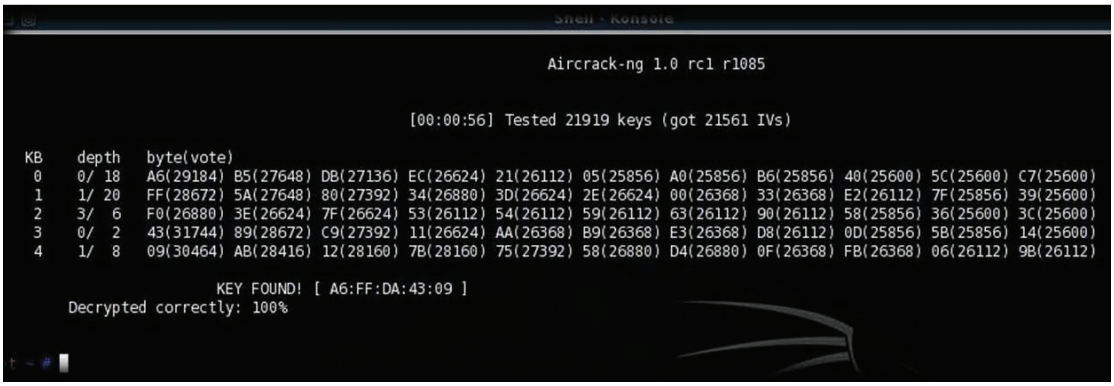
Εικόνα 38 Ανίχνευση κάρτας και σάρωση δικτύου σε 28 sec.

Εδώ το κανάλι της ασφάλειας WPA που φαίνεται είναι το 11. Το γράφημα του WPA φαίνεται παρακάτω:



Εικόνα 39 Μετά από δύο επιθέσεις το γράφημα γίνεται σταθερό.

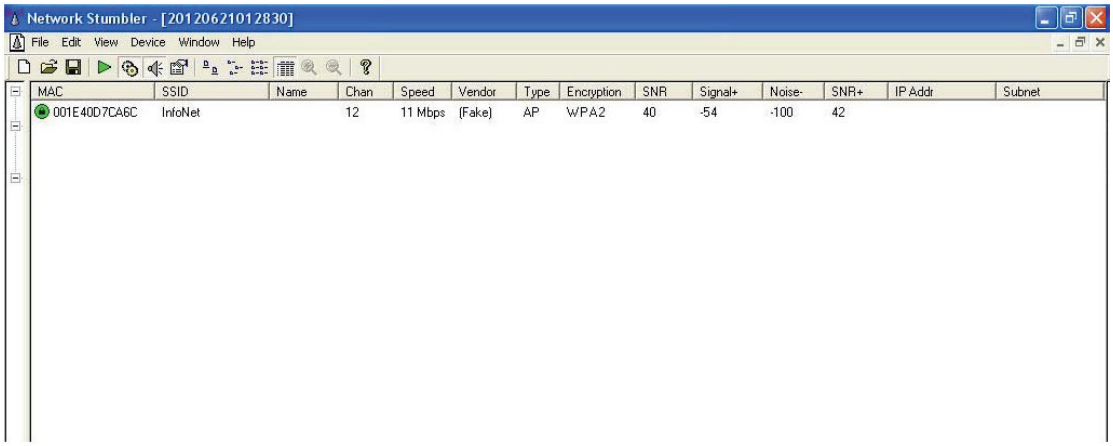
Σε αυτό το γράφημα, καταλήγουμε ότι μετά την εφαρμογή περισσότερων των δύο επιθέσεων, γίνεται επίσης σταθερό για κάποια ώρα.



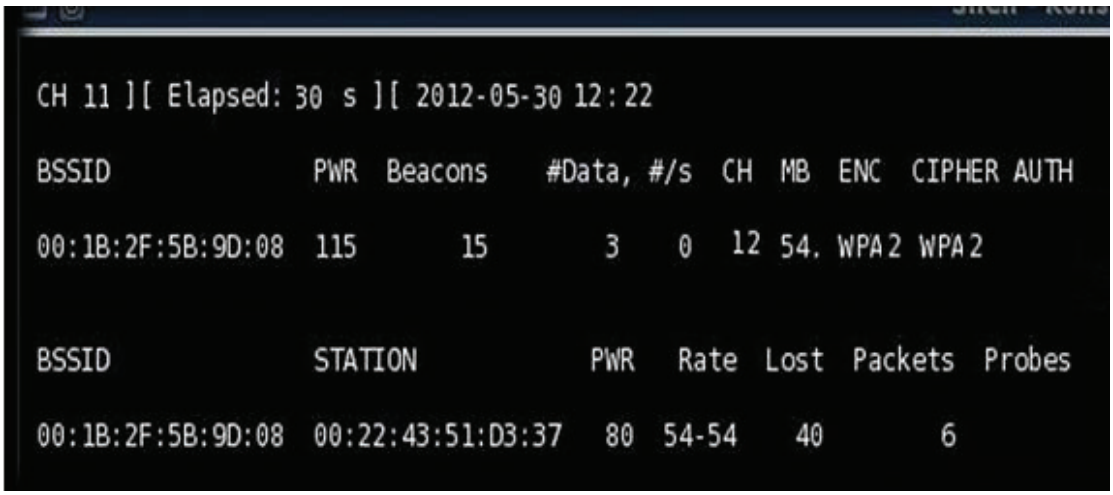
Εικόνα 40 Το κλειδί βρέθηκε. Επιτυχής αποκρυπτογράφηση.

Αυτό δείχνει πως όταν χρησιμοποιείται WPA pre-shared κλειδί δεν είναι εντελώς ασφαλές. Παρόλο που αυτή η επίθεση δεν λειτουργεί πάντα 100% αλλά αν ο τελικός χρήστης χρησιμοποιεί κοινή λέξη φράσης μπορεί εύκολα να σπάσει. Χρησιμοποιώντας το Back Track3 αυτή η ασφάλεια σπάει σε 56 seconds. Έτσι η κρυπτογράφηση του WPA2-PSK είναι περισσότερο ασφαλής και δυνατή από το WPA-PSK επειδή τπ WPA έσπασε μετά από λίγη ώρα ενώ το WPA2-PSK χρησιμοποιεί μεγαλύτερες φράσεις από το WPA.

WPA2 Αποτέλεσμα

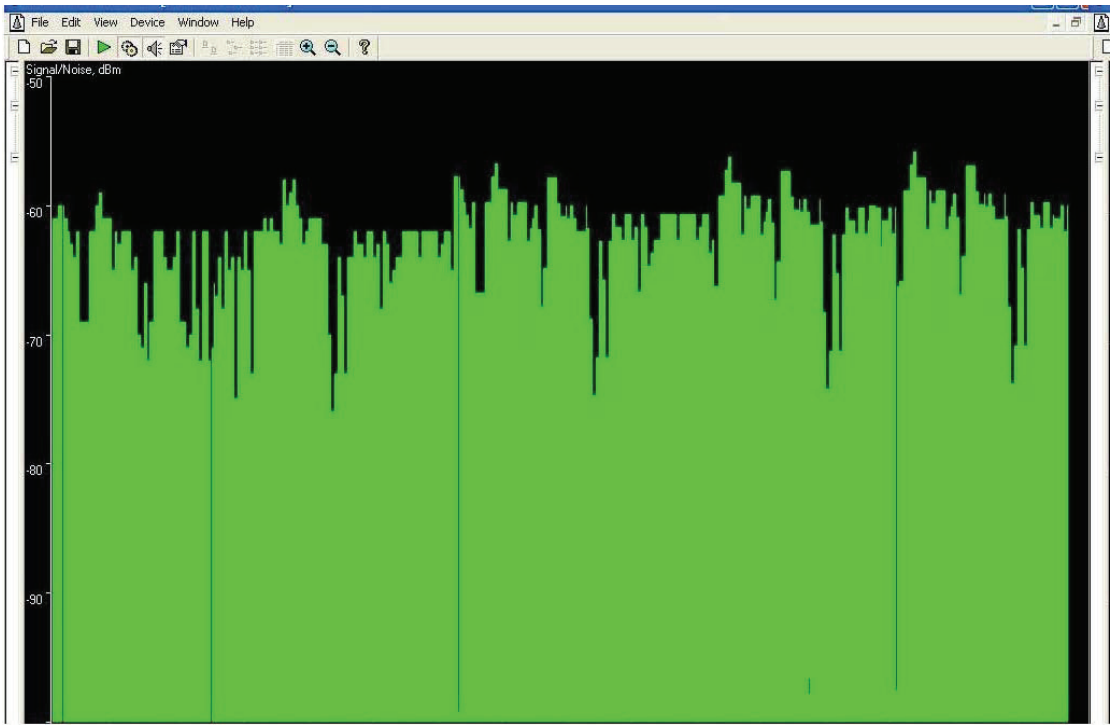


Εικόνα 41 Κανάλι 12, ταχύτητα 11Mbps.



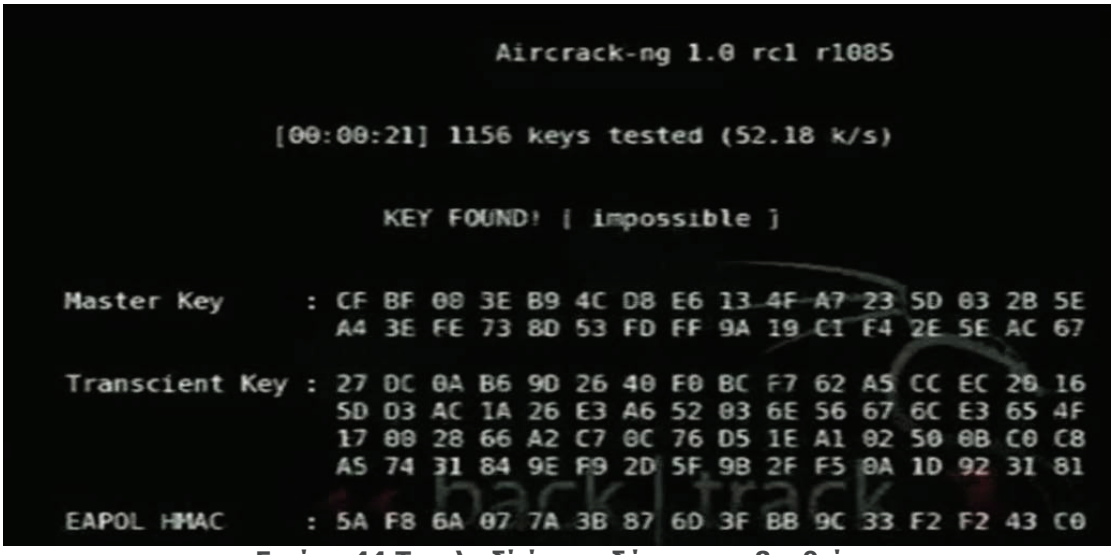
Εικόνα 42 Ανίχνευση κάρτας και σάρωση δικτύου σε 30 sec.

Εδώ το κανάλι που φαίνεται είναι το 12 και ο τύπος κρυπτογράφησης είναι το WPA2. Το γράφημα του WPA2 φαίνεται παρακάτω:



Εικόνα 43 Όχι σταθερό γράφημα, πιο ασφαλές.

Το γράφημα δείχνει πως όταν εφαρμόζουμε τόσες πολλές επιθέσεις αυτή η ασφάλεια δεν μπορεί να σταθεροποιηθεί το οποίο σημαίνει ότι είναι η πιο ασφαλής συγκριτικά με τις άλλες ασφάλειες.



Εικόνα 44 Το κλειδί ήταν αδύνατο να βρεθεί.

Αυτό το τμήμα δείχνει πως όταν χρησιμοποιείται WPA2 pre-shared κλειδί είναι εντελώς ασφαλές. Ενώ αυτή η επίθεση λειτουργεί 100% με χρήση Back Track3 αυτή η ασφάλεια δεν σπάει. Έτσι η κρυπτογράφηση WPA2-PSK είναι πιο δυνατή και ασφαλής καθώς χρησιμοποιεί μεγάλες φράσεις. Το WPA2 όμως μπορεί να σπάσει εύκολα στις μέρες μας στην περίπτωση που το passphrase δεν είναι δυνατό

καθώς τα εργαλεία που χρησιμοποιούνται είναι βελτιωμένα και αρκετά ικανά για να το σπάσουν.

Συμπέρασμα

Μεταξύ των υπαρχόντων πρωτόκολλων ασφάλειας στα WLANs, το WPA2 είναι το πιο ασφαλές πρωτόκολλο ασφάλειας αλλά το *trade-off* [5]*μεταξύ ασφάλειας και overhead που σχετίζονται με αυτό δεν είναι καλό*. Βασικό θέμα είναι η επιλογή μιας πολύ ισχυρής passphrase έτσι ώστε να είναι δύσκολο να ανιχνευτεί και να σπάσει από τον επιτιθέμενο.

3.9 Σύγκριση ταχύτητας στο WEP και WPA

Θεωρητική επίδραση στην ταχύτητα

Όλη η κρυπτογράφηση υλοποιείται μέσω του συνδυασμού του αυθεντικού μηνύματος με μια μαθηματική λειτουργία που το μετατρέπει σε μια μορφή που είναι απίθανη να διαβαστεί. Ένα μαθηματικό κλειδί χρησιμοποιείται στην αρχή της μετάδοσης για να μετατρέψει το μήνυμα σε μια κρυπτογραφημένη μορφή που στέλνεται, μετά χρησιμοποιείται πάλι στο άκρο που την λαμβάνει έτσι ώστε να αποκρυπτογραφηθεί στην αρχική του μορφή. Αυτές οι λειτουργίες απαιτούν χρόνο υπολογιστικής επεξεργασίας για να ολοκληρωθούν και από τις δύο πλευρές, έτσι όλη η κρυπτογραφική κίνηση θα είναι θεωρητικά πιο αργή από ότι να στελνόταν το αρχικό μήνυμα σε καθαρή μορφή χωρίς την χρήση αυτής της ασφαλούς μεθόδου.

Πρακτική επίδραση

Το WEP και WPA χρησιμοποιούν χρόνο υπολογιστικής επεξεργασίας, αλλά οι περισσότερες διαδικτυακές μεταδόσεις δεν μειώνονται αξιοσημείωτα σε αυτό το στάδιο. Το φρακάρισμα στην ταχύτητα προέρχεται δε από την σύνδεση του διαδικτύου, η οποία θέτει το ανώτατο όριο στην μέγιστη ταχύτητα μετάδοσης που μπορεί να ταξιδέψει. Τα δεδομένα που φεύγουν από το router μπορούν να μετακινηθούν σε κλάσματα της μέγιστης ταχύτητάς του, αλλά αν αυτό το κλάσμα είναι από μόνο του μεγαλύτερο σε megabits per second από την γρηγορότερη ταχύτητας της σύνδεσης του Internet που μπορεί να διατηρήσει, δεν θα έχει κανένα αποτέλεσμα στην συνολική δικτυακή ταχύτητα.

WEP, WPA και ταχύτητα

Ενώ το WPA είναι νεότερη και πιο ισχυρή τεχνική κρυπτογράφησης από το WEP, τυπικά η πιο ισχυρή κρυπτογράφηση είναι και πιο αργή, αλλά υπάρχει μια εξήγηση για οποιαδήποτε παρερμηνεία σε αυτόν τον υπολογισμό. Μερικά routers δεν χρησιμοποιούν την μεγαλύτερη δυνατή ταχύτητά τους εάν δεν είναι ρυθμισμένα να χρησιμοποιούν κρυπτογράφηση WPA2. Η ταχύτητα επηρεάζεται επίσης από την κατασκευή του εξοπλισμού του router καθώς το υλικό που είναι βελτιωμένο για WPA μπορεί να ολοκληρώνει αυτές τις λειτουργίες γρηγορότερα ακόμα κι αν είναι πιο πολύπλοκες.

Αξιολόγηση της ταχύτητας και της ασφάλειας

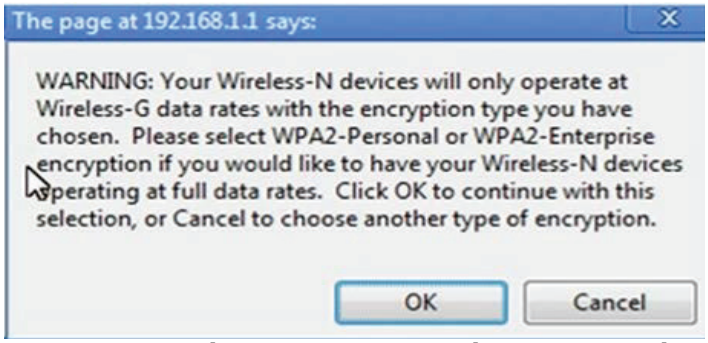
Σχεδόν σε όλες τις περιπτώσεις όπου είναι διαθέσιμο το WEP και WPA, προτείνεται η χρήση WPA. Η κρυπτογράφηση WEP δεν είναι τόσο ασφαλής και σπάει εύκολα αλλά το WPA2 με ισχυρό password δεν μπορεί να σπάσει με εμπορικές μεθόδους.

[5] Το tradeoff είναι όρος που αναφέρεται σε μια κατάσταση στην οποία όταν χάνεις την ποιότητα σε κάτι αναπληρώνοντας το κέρδος στην ποιότητα σε κάτι άλλο.

Ακόμα και αν κάποια test υποδεικνύουν πως το WPA είναι πιο αργό στο δίκτυο από το WEP, είναι σπάνια καλή ιδέα να χρησιμοποιείται φτωχή κρυπτογράφηση. Εάν είναι σημαντικό θέμα η ταχύτητα, μπορούμε να αυξήσουμε την ταχύτητα και την ασφάλεια χρησιμοποιώντας ενσύρματο δίκτυο αν χρειαστεί. Η καλωδίωση Ethernet είναι πολύ πιο γρήγορη για τοπική δικτύωση, και απαιτεί φυσική πρόσβαση στα καλώδια για να επιχειρηθεί εισβολή στο δίκτυο.

3.10 Σύγκριση λειτουργιών WEP και WPA σε περιβάλλον 802.11n.

Έχουν ακουστεί ποικιλες απόψεις πώς το WPA υπερτερεί το WEP στα 802.11n και το αντίθετο, ανάλογα από τον πωλητή. Το 802.11n πρότυπο προσδιορίζει ότι μπορούν να επιτευχθούν μεγαλύτερες ταχύτητες όταν είναι σε λειτουργία το WPA2 + AES αλλιώς όλες οι συσκευές οδηγηθούν πίσω στις ταχύτητες 802.1g των 54 Mbps.



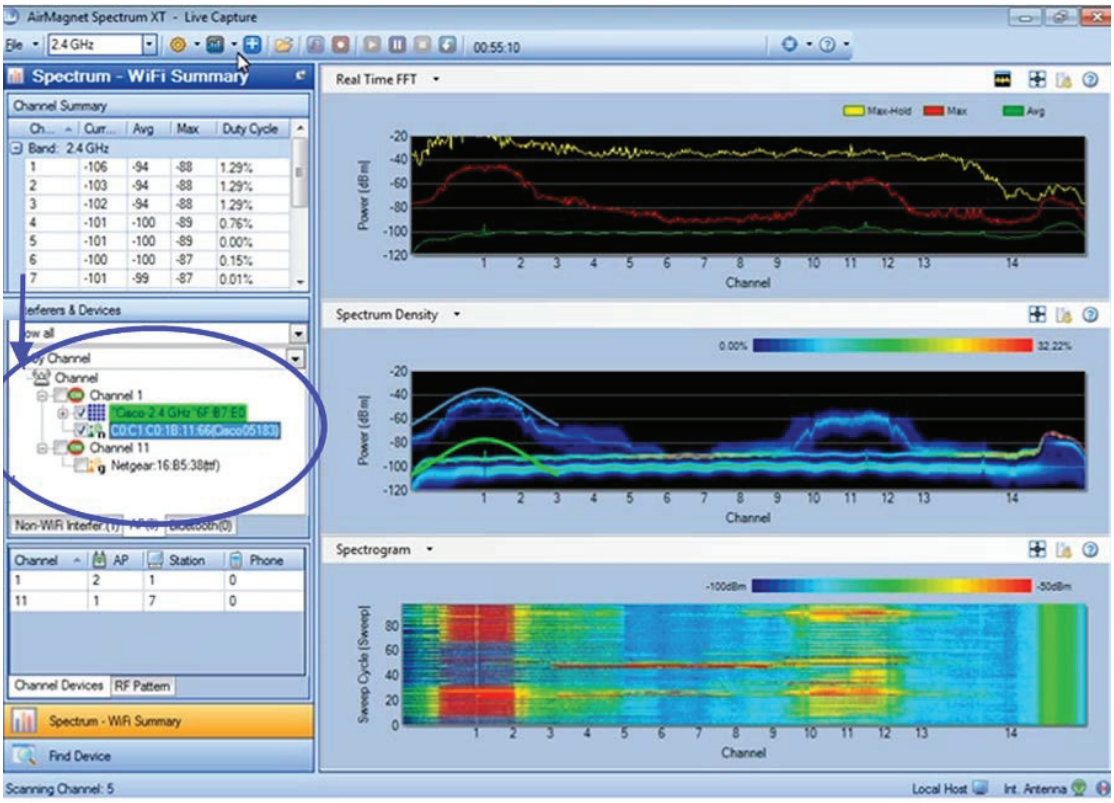
Εικόνα 45 Προειδοποίηση για την επιλογή της λειτουργίας WEP.

Εδώ φαίνεται μια screenshot από ένα Cisco Linksys wireless AP το οποίο όταν επιλεχθεί η λειτουργία WEP προειδοποιεί για την χρήση του. Συγκεκριμένα προειδοποιεί πως οι ασύρματες N συσκευές θα λειτουργούν μόνο σε ασύρματες G data rates με το είδος κρυπτογράφησης που επιλέξαμε (δηλαδή το WEP). Προτείνει, λοιπόν, τη χρήση κρυπτογράφησης WPA2-Personal ή WPA2-Enterprise εάν θέλουμε να λειτουργούν οι ασύρματες N συσκευές στο μέγιστο data rate.
Ας ελέγξουμε κατά πόσο αυτό αληθεύει.
Για το Test χρησιμοποιούμε ένα Gateway Netbook LT2802h ως πελάτη, συνδεδεμένο με καλώδιο Ethernet σε ένα router Cisco Linksys E3000 το οποίο τρέχει την default διαμόρφωσή του. Στη συνέχεια το router επικοινωνεί ασύρματα (Wi-Fi) με έναν server ο οποίος είναι ένα laptop Dell Studio 1737 με ασύρματη κάρτα δικτύου Intel 5100AGN.
Εφαρμόζεται pathtest στον client και στον server. Το PathTest είναι ένα δωρεάν εργαλείο ελέγχου ισχύος το οποίο δίνει τα πιο ακριβή αποτελέσματα που δύναται. PathTest βοηθάει στο να κατανοήσει κάποιος την πραγματική μέγιστη ισχύ του δικτύου του και λειτουργεί σε layer3, layer 4. Επίσης χρησιμοποιείται το Fluke Airmagnet Spectrum XT, ένα εργαλείο για πειραματική αναγνώριση και εντοπισμό οποιοσδήποτε διεπαφής RF (radio frequency) που έχει επίδραση στην λειτουργία Wi-Fi.

Εικόνα 46 Τοπολογία και υλικό για το πείραμα.

Έλεγχος στα 2.4 GHz

Στην συγκεκριμένη περίπτωση χρησιμοποιήθηκε το AIrmagnet Spectrum XT για να δούμε ποιά κανάλια επιλέγει το AP E3000 και να παρατηρήσουμε που βρίσκεται ο θόρυβος RF. Παρόλο που υπάρχει και άλλο AP στο κανάλι ένα μπορεί ελάχιστα να ακουστεί. Είναι σημαντικό να γνωρίζουμε πως γενικά γίνεται αυτόματη επιλογή του καναλιού από το AP (εδώ είναι το κανάλι 1 για το E3000) γι' αυτό βλέπουμε να υπάρχει και άλλο AP που έχει επιλέξει το κανάλι 11. Αν δεν θέλουμε αυτόματη επιλογή καναλιού, θα πρέπει να το εισάγουμε χειροκίνητα στο AP για να επιλέξει το συγκεκριμένο κανάλι που επιθυμούμε.



Εικόνα 47 AP E3000 επιλογή καναλιού 1.

Test 1 -2.4 GHz Εγκατάσταση λειτουργίας WEP

Στο Gateway Netbook το οποίο είναι απευθείας συνδεδεμένο ενσύρματα με το E3000 και έχει απενεργοποιημένο το ασύρματο, εφαρμόζεται pathtest client test χρησιμοποιώντας τις ακόλουθες επιλογές:

- le pathtest –c 192.168.1.143 –bidi – tcp
  - όπου –c client routine, -bidi bidirectional, -tcp πρωτόκολλο που επιλέγεται , η ip διεύθυνση είναι του server

Στο AP E3000 η passphrase είναι 1234567890 και έχει διαμορφωθεί για WEP 64 σε 5 GHz radio me SSID:5ghz καθώς και για 2.4 GHZ radio με SSID:24ghz. Επιλέγει αυτόματα το κανάλι και το πλάτος καναλιού.

Το Dell Studio είναι συνδεδεμένο ασύρματα χρησιμοποιώντας 2.4 WEP radio.

Εικόνα 48 Διαθέσιμα ασύρματα δίκτυα.

Test Number	Upstream	Downstream
1	11.119	10.892
2	10.878	10.654
3	11.156	10.860
4	11.411	10.875
5	11.253	10.188
Average	**11.1634**	**10.6938**

Εικόνα 49 Test 1, 2.4 GHz, αποτελέσματα WEP.

Test 2 -2.4 GHz Εγκατάσταση λειτουργίας WPA

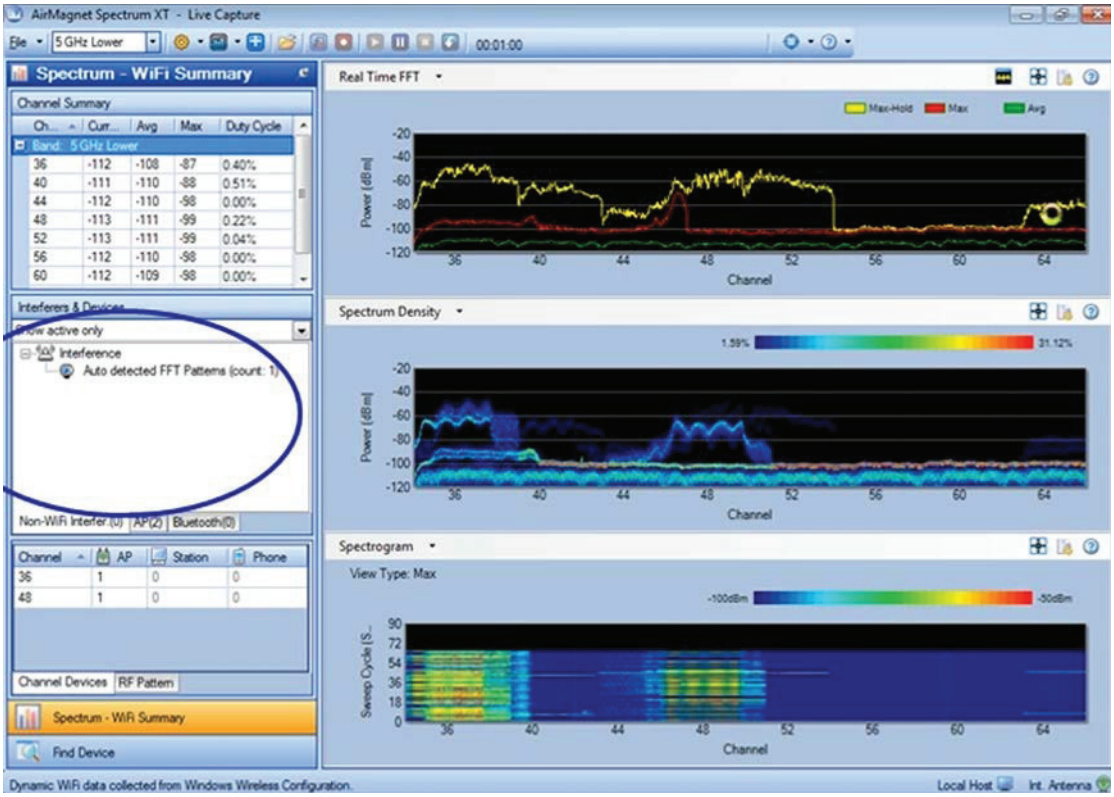
Οι ίδιες ρυθμίσεις με το WEP με μόνη διαφορά το passphrase που είναι 24ghzwpa2.

Test Number	Upstream	Downstream
1	53.570	22.587
2	52.337	23.806
3	38.459	24.221
4	44.419	28.759
5	55.680	23.577
Average	**48.893**	**24.59**

Εικόνα 50 Test 2, 2.4 GHz, αποτελέσματα WPA.

Έλεγχος στα 5 GHz

Παρακάτω φαίνεται η αυτόματη επιλογή του AP στο κανάλι 36 στο οποίο τυχαίνει να βρίσκεται και το router του γραφείου. Έτσι γίνεται χειροκίνητη αλλαγή στο κανάλι 48 για να μην συγκρούονται.



Εικόνα 51 AP E3000 χειροκίνητη επιλογή καναλιού 48.

Test 3 -5.8 GHz Εγκατάσταση λειτουργίας WEP

Οι ρυθμίσεις είναι ίδιες με το Test 1.
Το Dell Studio είναι συνδεδεμένο ασύρματα χρησιμοποιώντας 5 WEP radio.

Test Number	Upstream	Downstream
1	12.304	10.730
2	11.404	11.439
3	11.151	11.135
4	14.956	9.111
5	11.165	11.110
Average	**12.196**	**10.705**

Εικόνα 52 Test 3, 5.8 GHz, αποτελέσματα WEP.

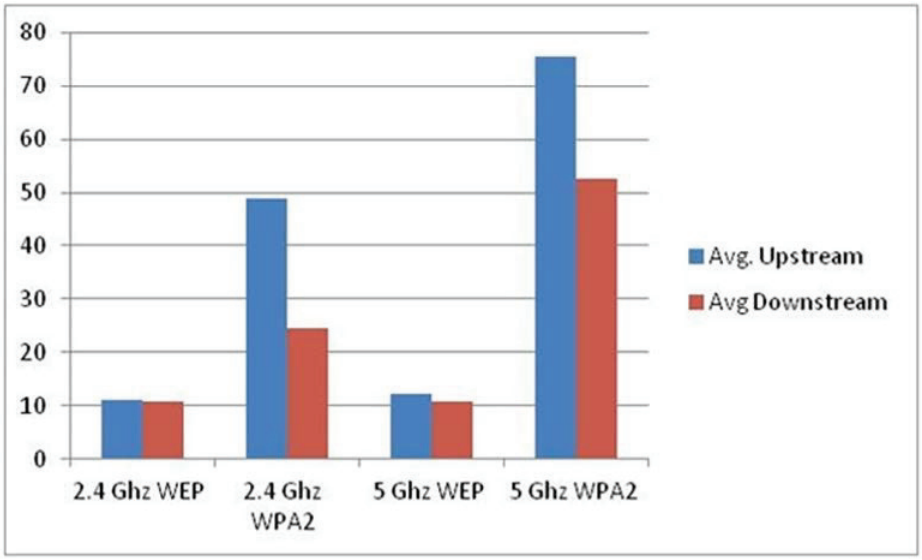
Test 4 -5.8 GHz Εγκατάσταση λειτουργίας WPA

Test Number	Upstream	Downstream
1	51.755	55.840
2	77.738	55.277
3	80.583	53.543
4	88.375	42.036
5	78.686	55.771
Average	**75.4274**	**52.4934**

Εικόνα 53 Test 4, 5.8 GHz, αποτελέσματα WPA.

Test Number	Avg. Upstream	Avg Downstream
2.4 Ghz WEP	**11.1634**	**10.6938**
2.4 Ghz WPA2	**48.893**	**24.59**
5 Ghz WEP	**12.196**	**10.705**
5 Ghz WPA2	**75.4274**	**52.4934**

Εικόνα 54 Συγκριτικά αποτελέσματα.



Εικόνα 55 Γράφημα συγκριτικών αποτελεσμάτων.

Παρατηρείται λοιπόν σημαντική αύξηση στην λειτουργία upstream-downstream με την χρήση WPA/WPA2 και στα 2.4 GHz και στα 5 GHz.

3.11 Αναλύοντας το Overhead στην ασφάλεια των WLAN

Αντικείμενο

Στόχος αυτής της έρευνας είναι να καθορίσει το overhead που σχετίζεται με τα IEEE 802.11 πρωτόκολλα ασφάλειας σε σχέση με την κρυπτογράφηση. Αυτά τα δεδομένα είναι σημαντικά καθώς απαιτείται επιπλέον ασφάλεια στα ασύρματα δίκτυα για την διασφάλιση της αξιοπιστίας και της ακεραιότητας των δεδομένων. Οι εφαρμογές που σχετίζονται με την χρήση των ασύρματων δικτύων εξαπλώνονται συνεχώς, και μπορούν να επηρεαστούν από αργό χρόνο απόκρισης και μειωμένο throughput (απόδοση).
Μερικά παραδείγματα τέτοιων εφαρμογών είναι το roaming (περιαγωγή) των χρηστών VoIP μεταξύ πολλαπλών Access Points, η απομακρυσμένη ασύρματη

γεφύρωση (bridging) και η μετάδοση με χαμηλής ενέργειας συσκευές χειρός. Οι χρήστες που σκοπεύουν να περιαγωγηθούν με τηλέφωνα VoIP μεταξύ σημείων πρόσβασης θα αντιμετωπίσουν παρόμοια προβλήματα με την περιαγωγή των πελατών της κινητής τηλεφωνίας, τα οποία θα μπορούσαν να επηρεαστούν σημαντικά από αρκετές φορές πιστοποιήσεων και επιπλέον υποθέσεις hand-off. Οι ασύρματες γέφυρες που συνδέουν πανεπιστημιακά κτήρια είναι προς το παρόν καλυμμένα στις ταχύτητες του IEEE 802.11g σε ταχύτητα 54Mbps που είναι ήδη πολύ πιο αργή από τις τυπικές gigabit ενσύρματες λύσεις. Η προσθήκη κρυπτογράφησης μπορεί να δυσχεραίνει περαιτέρω την απόδοση αυτών των συνδέσμων, ανεξάρτητα από το γεγονός ότι πολλοί χρήστες θα μπορούσαν να πιστοποιούνται εξίσου σε αυτούς τους συνδέσμους.
Προσφέρεται λοιπόν μια βαθύτερη κατανόηση των συνεπειών της ασφάλειας που μπορεί να προκαλέσει σε διάφορους τύπους της λειτουργίας του δικτύου. Παρέχονται γενικές επισκοπήσεις στα πρωτόκολλα ασφάλειας που χρησιμοποιούνται σήμερα και συγκρίνονται μεταξύ τους αναφορικά με τον χρόνο απόκρισης, την καθυστέρηση και την απόδοση (throughput).

Overhead Κρυπτογράφησης

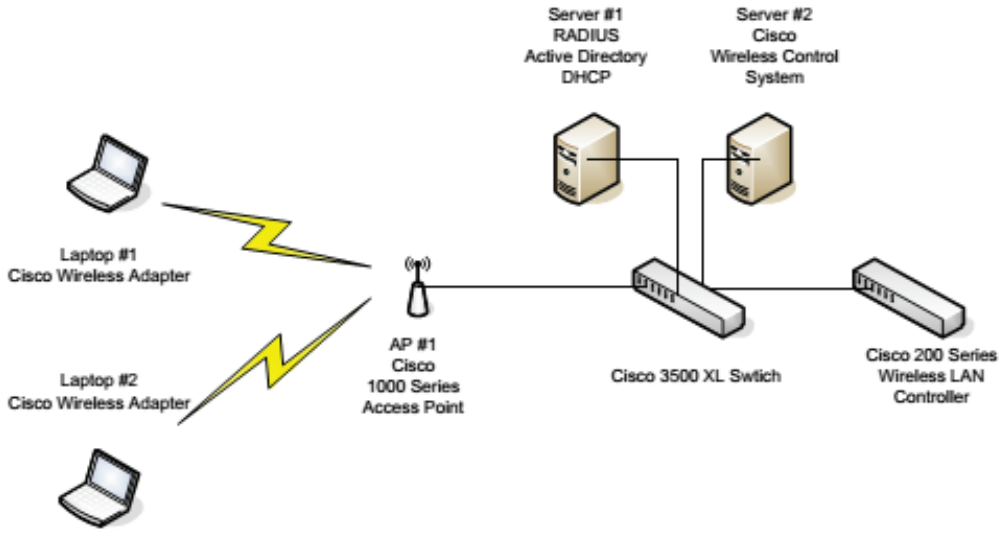
Η κρυπτογράφηση που προστατεύει έναν ασύρματο σύνδεσμο είναι το πιο επίμονο overhead που σχετίζεται με μια διαμόρφωση ασφαλούς δικτύου. Όταν ένας ασύρματος πελάτης πιστοποιείται με έναν RARDIUS server και ανταλλάσσονται τα κλειδιά η κρυπτογράφηση παραμένει παρούσα για ολόκληρη τη σύνοδο επηρεάζοντας όλα τα δεδομένα που μεταδίδονται πάνω στον σύνδεσμο. Η κρυπτογράφηση έχει μικρή επίδραση στην καθυστέρηση που σχετίζεται με τον σύνδεσμο αλλά έχει αντίκτυπο στο throughput σε κατάσταση κορεσμένου δικτύου όπου το bandwidth κατανέμεται για μεγαλύτερα κρυπτογραφημένα πακέτα.

Το throughput μετριέται με το Qcheck (εργαλείο μέτρησης throughput)κατά τη διάρκεια του πειράματος, με το ελάχιστο δέκα δοκιμές ανά πείραμα, στα οποία 1000 Kbytes δεδομένων περνούν από τον πελάτη στον server. Οι τιμές του throughput που λήφθηκαν με κρυπτογράφηση συγκρίθηκαν με το throughput χωρίς παρουσία κρυπτογράφησης για να καθορίσουν το ποσοστό του overhead που σχετίζεται με κάθε σχήμα κρυπτογράφησης. Για να παρέχεται η πιο ακριβής αναπαράσταση των δεδομένων του πραγματικού κόσμου τα μέσα ποσοστά overhead και της TCP και της UDP κίνησης υπολογίζονται κατά μέσο όρο για κάθε φυσική διαμόρφωση.

Υλικό δικτυακών συσκευών πειράματος

1. Cisco 2000 Series Wireless Controller
2. Cisco 1000 Series Access Point
3. Cisco 1200 Series Access Point
4. Cisco 1300 Series Outdoor Bridge
5. Cisco Wireless LAN Client Adapters
6. Cisco 3500 XL Series Switch

Μόνο τρείς από αυτές τις συσκευές χρησιμοποιούνται στην πλειοψηφία των πειραμάτων ασφάλειας και χρησιμοποιούν την διαμόρφωση δικτύου που φαίνεται παρακάτω.



Εικόνα 56 Διαμόρφωση δικτύου.

Το πείραμα περιλαμβάνει ένα κεντρικό Cisco 3500CL switch που διακανονίζει το Ethernet backbone. Οι δύο servers, ο WLAN controller και το access point συνδέονται απευθείας στο switch. Τα δύο laptops φυσικά σταθερές τοποθεσίες κατά τη διάρκεια του πειράματος για να ελαχιστοποιήσουν την εμπλεκόμενη διασπορά RF.

Τα laptops και οι servers που χρησιμοποιούνται έχουν τα παρακάτω χαρακτηριστικά υλικού.

Machine	Laptop #1	Laptop #2	Server #1	Server #2
Brand/Model	HP Pavilion 7000	Dell Inspiron 5150	Dell Client Pro	Dell Power Edge Server
Processor	Pent M 1.6 GHz	P4 3.2 GHz	P4 2.4 GHz	Dual P3 1.26 GHz
Memory	1 GB	1 GB	512K	1 GB
Network	Cisco A/B/G Client Adapter	Cisco A/B/G Client Adapter	Integrated	Integrated

Εικόνα 57 Χαρακτηριστικά υλικού των laptops & servers.

Επιλογή Λογισμικού

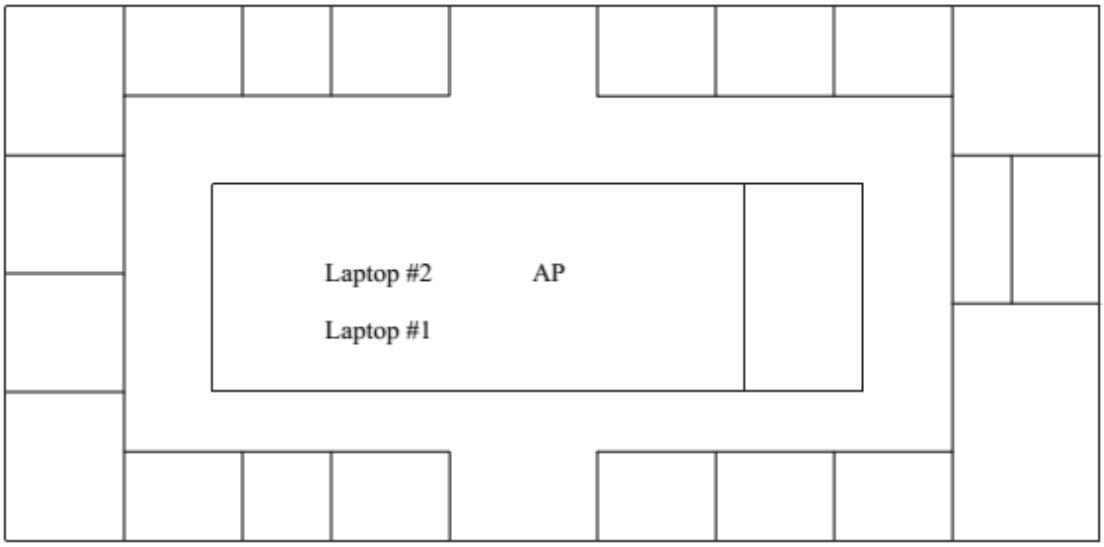
Όλα τα πειράματα διεξάγονται σε λειτουργικό σύστημα Microsoft Windows για ποικίλους λόγους. Ο πιο σημαντικός είναι ότι οι Cisco a/b/g κάρτες PCMCIA που χρησιμοποιούνται με τα laptops δεν έχουν linux-compatible drivers που να μπορούν να βγάλουν εις πέρας την κρυπτογράφηση CCMP. Κάθε server έχει Windows 2003 Server Edition με Service Pack 1 και τα δύο laptops έχουν Windows XP Professional με Service Pack 2.
Το πρόγραμμα μέτρησης του throughput που επιλέχτηκε είναι το Qcheck το οποίο μετράει και τον χρόνο απόκρισης γρήγορα και αποτελεσματικά.

Φυσικές Διαμορφώσεις

Η βασική διαμόρφωση δικτύου που παρουσιάστηκε παραπάνω ήταν η κύρια διάταξη για τον έλεγχο του throughput και την απόκριση. Ωστόσο, για να ελεγχθεί πώς επηρεάζεται το overhead από τα διάφορα φυσικά εμπόδια ή τις διαφορετικές διαμορφώσεις δικτύου, η διάταξη διαρρυθμίστηκε.

Διαμόρφωση 1

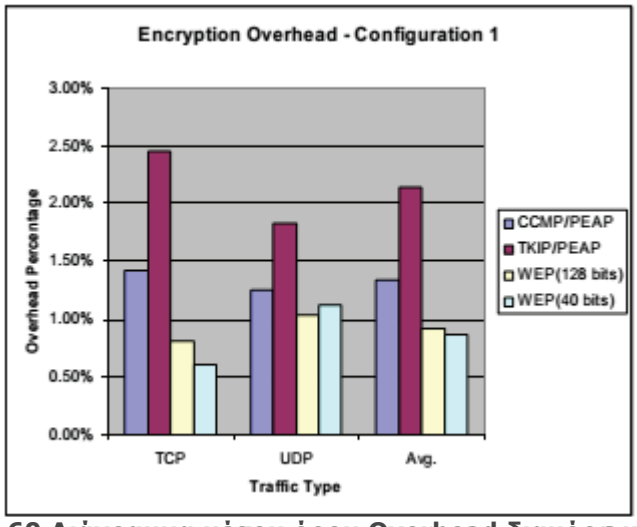
Εδώ χρησιμοποιείται μόνο ένα laptop για testing. Ο server#2 λειτούργησε ως server και το laptop#2 λειτούργησε ως πελάτης. Αυτό ήταν το περιβάλλον που χρησιμοποιήθηκε για να ελεγχθεί το μέγιστο throughput για αυτόν τον σύνδεσμο επειδή με την προσθήκη επιπλέον σταθμών πληρώνεται το τίμημα στο throughput.



Εικόνα 58 Φυσική διαμόρφωση 1.

	CCMP/PEAP	TKIP/PEAP	WEP(128 bits)	WEP
TCP	1.42%	2.45%	0.81%	0.61%
UDP	1.26%	1.83%	1.04%	1.13%
Avg.	1.34%	2.14%	0.92%	0.87%

Εικόνα 59 Μέσος όρος Overhead διαμόρφωσης 1.



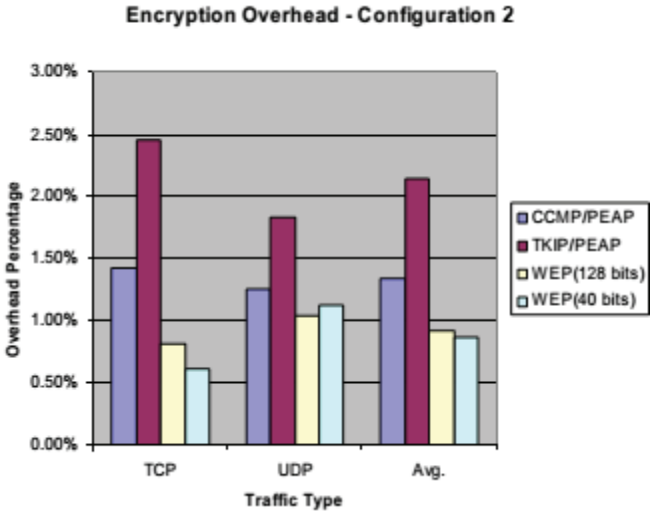
Εικόνα 60 Διάγραμμα μέσου όρου Overhead διαμόρφωσης 1.

Διαμόρφωση 2

Χρησιμοποιείται η ίδια τοπολογία δικτύου με την διαμόρφωση 1 αλλά προστίθεται ένας επιπλέον πελάτης. Το laptop#1 λειτουργεί ως server και το laptop#2 ως πελάτης. Με την προσθήκη αυτή μειώνεται το ολικό throughput του δικτύου, ειδικά όταν το πείραμα διεξάγεται μεταξύ των δύο πελατών. Το overhead κρυπτογράφησης θα διπλασιαστεί σε σύγκριση με την διαμόρφωση 1 λόγω της διαδικασίας ενθυλάκωσης και/από-ενθυλάκωσης που σχετίζεται με διάφορους αλγόριθμους που διεξάγονται διπλά στην διαμόρφωση 2;

	CCMP/PEAP	TKIP/PEAP	WEP(128 bits)	WEP(40 bits)
TCP	1.25%	2.17%	1.83%	0.47%
UDP	1.33%	2.88%	2.59%	1.97%
Avg.	1.29%	2.52%	2.21%	1.22%

Εικόνα 61 Μέσος όρος Overhead διαμόρφωσης 2.

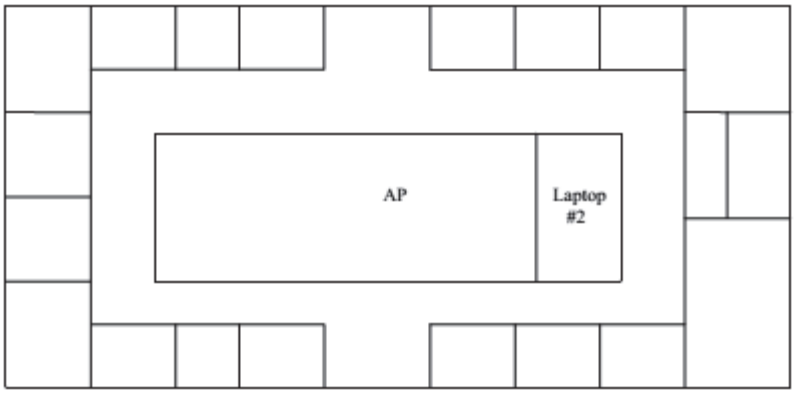


Εικόνα 62 Διάγραμμα μέσου όρου Overhead διαμόρφωσης 2.

Όπως περιμέναμε, το overhead κρυπτογράφησης στο WEP είναι περίπου το διπλάσιο από αυτό της διαμόρφωσης 1. Ωστόσο το overhead στο CCMP και TKIP είναι σχεδόν ακριβώς το ίδιο όπως στην διαμόρφωση 1.

Διαμόρφωση 3

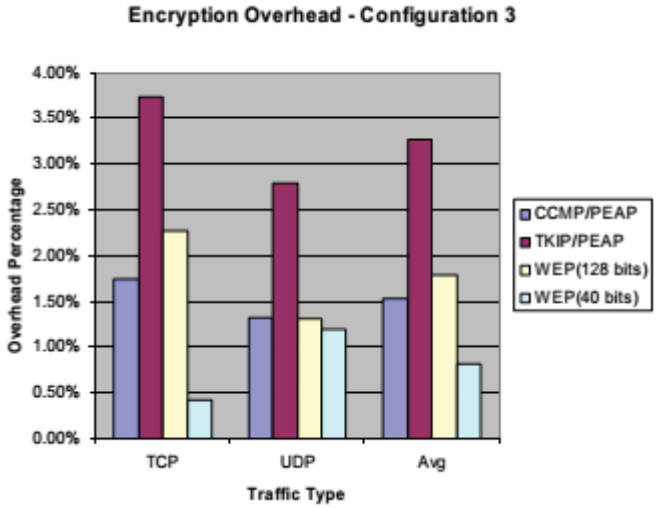
Η μόνη διαφορά σε αυτό το πείραμα, είναι η μετακίνηση του δεύτερου σταθμού πίσω από έναν τεσσάρων ιντσών τοίχο (ελέγχεται παρόμοια με την διαμόρφωση 1) με αποτέλεσμα την μείωση της δύναμης του σήματος σε περίπου 6 dBm. Μόνο ένα laptop χησιμοποιείται για testing. Ο server#2 λειτουργεί ως server και το laptop#2 ως πελάτης. Θέλουμε να ελέγξουμε εάν η μικρή μείωση σε μια λαμβάνουσα ισχύ σήματος θα ανεβάσει το ποσό του overhead που δημιουργείται από την κρυπτογράφηση.



Εικόνα 63 Φυσική διαμόρφωση 3.

	CCMP/PEAP	TKIP/PEAP	WEP(128 bits)	WEP(40 bits)
TCP	1.74%	3.75%	2.28%	0.42%
UDP	1.33%	2.80%	1.30%	1.20%
Avg	1.53%	3.27%	1.79%	0.81%

Εικόνα 64 Μέσος όρος overhead διαμόρφωσης 3.

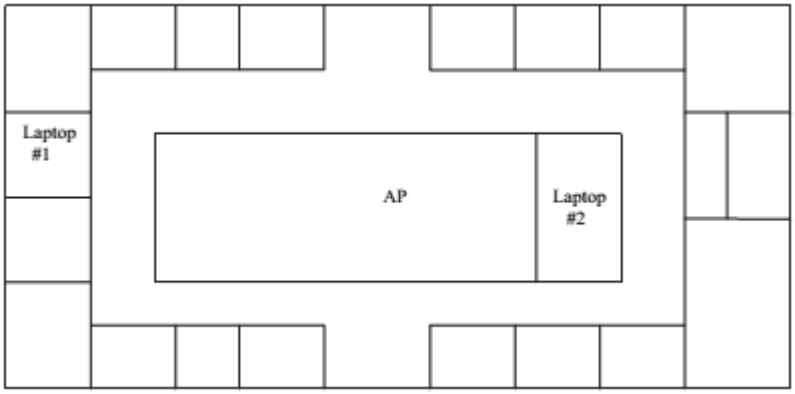


Εικόνα 65 Διάγραμμα μέσου όρου Overhead διαμόρφωσης 3.

Τα αποτελέσματα υποδηλώνουν πως η εξασθένηση 6dBm δεν έχει ουσιαστικά καθόλου αποτέλεσμα στο throughput του συνδέσμου για κανένα από τα σχήματα κρυπτογράφησης που χρησιμοποιούνται. Οι τιμές είναι παρόμοιες με αυτές που προέκυψαν στην διαμόρφωση 1.

Διαμόρφωση 4

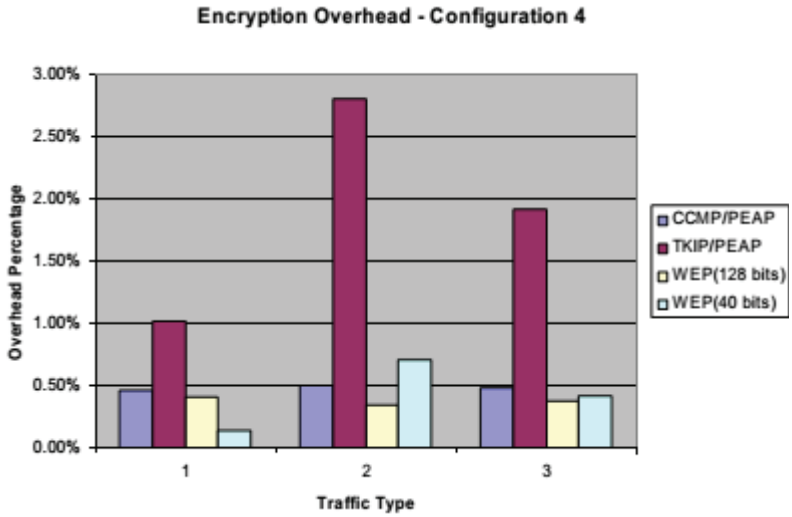
Το κάθε laptop μετακινήθηκαν το καθένα μέσα σε στο κτίριο με 8 έως 15 dBm επιπέδων εξασθένηση εξαιτίας φυσικών εμποδίων. Το laptop#2 έμεινα σε όμοια θέση με την διαμόρφωση 3. Το laptop#1 μετακινήθηκε στην αντίθετη πλευρά του κτιρίου μέσα στην ακτίνα του access point αλλά εκτός ακτίνας του laptop#2 και πίσω από τοίχο τεσσάρων ιντσών.



Εικόνα 66 Φυσική διαμόρφωση 4.

	CCMP/PEAP	TKIP/PEAP	WEP(128 bits)	WEP(40 bits)
TCP	0.46%	1.02%	0.41%	0.14%
UDP	0.51%	2.81%	0.35%	0.71%
Avg	0.48%	1.91%	0.38%	0.42%

Εικόνα 67 Μέσος όρος overhead διαμόρφωσης 4.



Εικόνα 68 Διάγραμμα μέσου όρου Overhead διαμόρφωσης 4.

Οι τιμές αυτού του πειράματος ήταν κάπως αναπάντεχες αφού δεν υπάρχει ξεχωριστή διαφορά μεταξύ 64 και 128bit WEP κλειδιών. Αυτό μπορεί να οφείλεται εξαιτίας ελαφρών ασυνεπειών του δικτύου όταν ολοκληρώθηκαν οι μετρήσεις.

Συμπέρασμα

Υπάρχει ένας σαφές υπόδειγμα στο οποίο το TKIP δημιούργησε το περισσότερο overhead, άρα και την χειρότερη εκτέλεση, ακολουθούμενο από το CCMP και έπειτα από το WEP. Αυτό μπορεί να οφείλεται σε πολλές αιτίες. Οι μικρές αλλαγές σε ένα δυνατό σήμα 802.11 είναι πιθανό να έχουν μικρή επίδραση στην λειτουργία. Φυσικά αν όλα αυτά τα πειράματα εφαρμοστούν σε κατώτερης ποιότητας υλικό , όπως τα SOHO routers και AP, θα οδηγηθούν σε μεγαλύτερο overhead και μεγαλύτερη μείωση στο throughput του δικτύου.

Επιπλέον, το WEP, TKIP, CCMP επισυνάπτουν 8, 20 και 16 octets δεδομένων αντίστοιχα σε κάθε data frame έτσι είναι εφικτό η προσθήκη αυτών των επιπλέον 32 bits να είναι μέρος του προβλήματος. Επίσης όπως προαναφέρθηκε, η κρυπτογράφηση CCMP υλοποιείται τυπικά μέσα στο hardware του AP ή του πελάτη (client) ενώ το TKIP εκτελείται μέσα στο λογισμικό το οποίο είναι σοβαρή αιτία για την μείωση του throughput. Και αυτό γιατί το TKIP αναπτύχθηκε για software update σε WEP συμβατές συσκευές hardware, εμποδίζοντας την ανάγκη για αντικατάσταση παλαιού υλικού. Αυτό συνδυάζεται επιπλέον με το γεγονός ότι το TKIP έχει αρκετές διαδικασίες μίξης που λειτουργούν την ίδια στιγμή για να δημιουργήσουν το data stream. Η δημιουργία των WEP seeds από μόνη της είναι πιο σύνθετη στο TKIP από το βασικό WEP, και η επιπλέον πολυπλοκότητα του αλγόριθμου Michael προσθέτει ένα ακόμα επίπεδο στο overhead.

3.12 Σύγκριση της απόδοσης ασφάλειας στα ασύρματα δίκτυα 802.11a/b/g.

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.

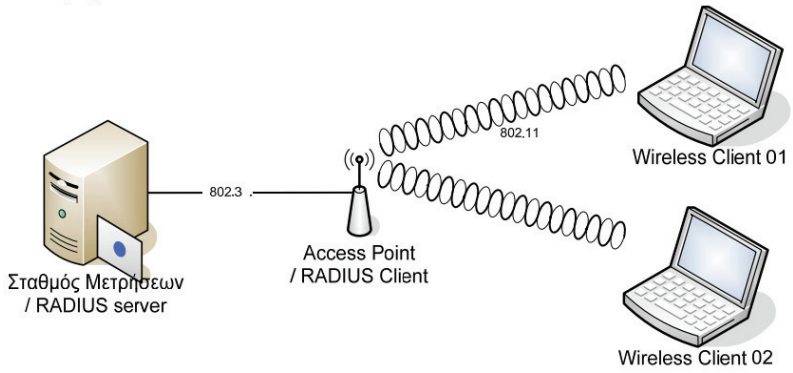
Πειραματικό Μέρος

Σκοπός αυτού του πειραματικού μέρους είναι η διερεύνηση της επίδρασης των μηχανισμών ασφαλείας που περιγράφτηκαν στα προηγούμενα κεφάλαια σε δίκτυα του 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.

Το Υλικό

Για τις ανάγκες των μετρήσεων χρησιμοποιήθηκαν τρία Access Point

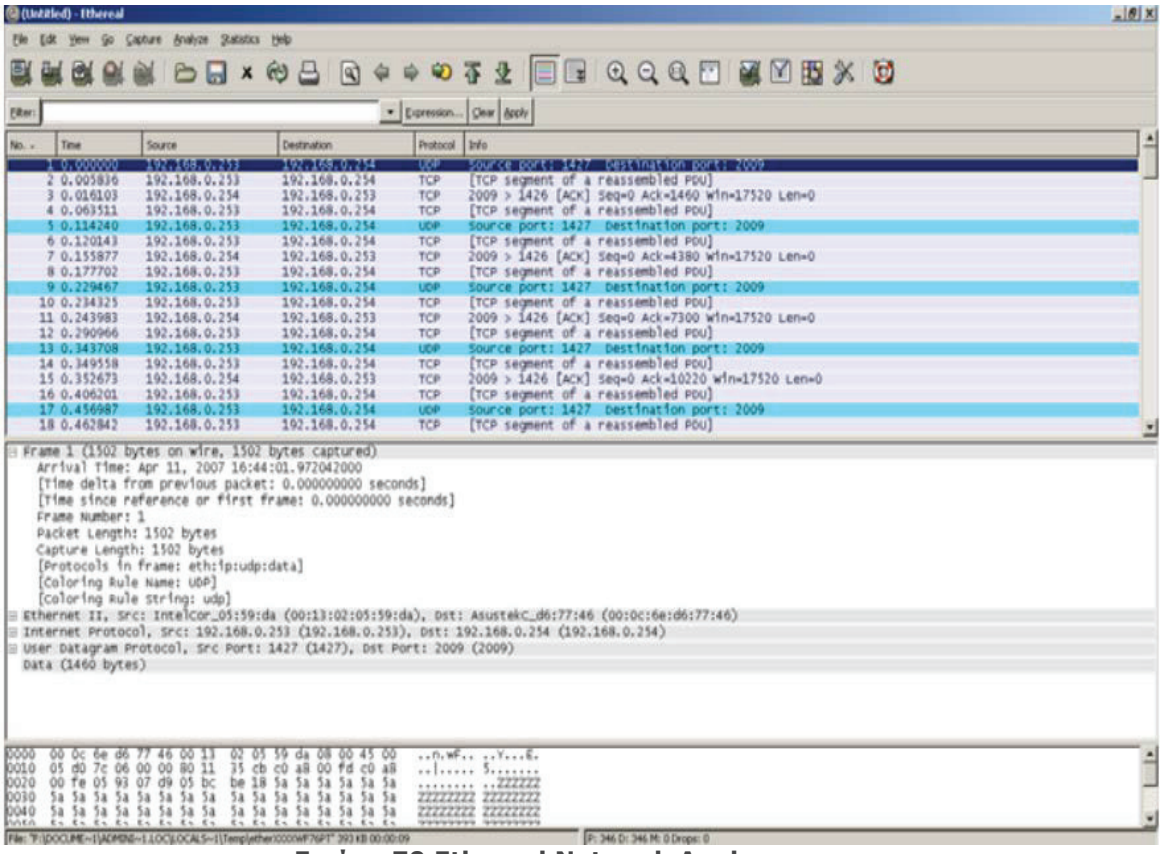
διαφορετικών κατηγοριών και δυνατοτήτων.
1. Το WG602v3 της Netgear με επεξεργαστή τον IDT 32334 Communications Processor χρονισμένο στα 150MHz. Ανήκει στην κατηγορία Small Office/Home Office (SOHO) με κόστος μικρότερο των €100. Υποστηρίζει WPA-Personal και WPA2-Personal.
2. Το ProSafe FWG114Pv2 της Netgear 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.
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.



Εικόνα 69 Η αρχιτεκτονική του δικτύου του πειράματος.

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.



Εικόνα 70 Ethereal Network Analyzer.

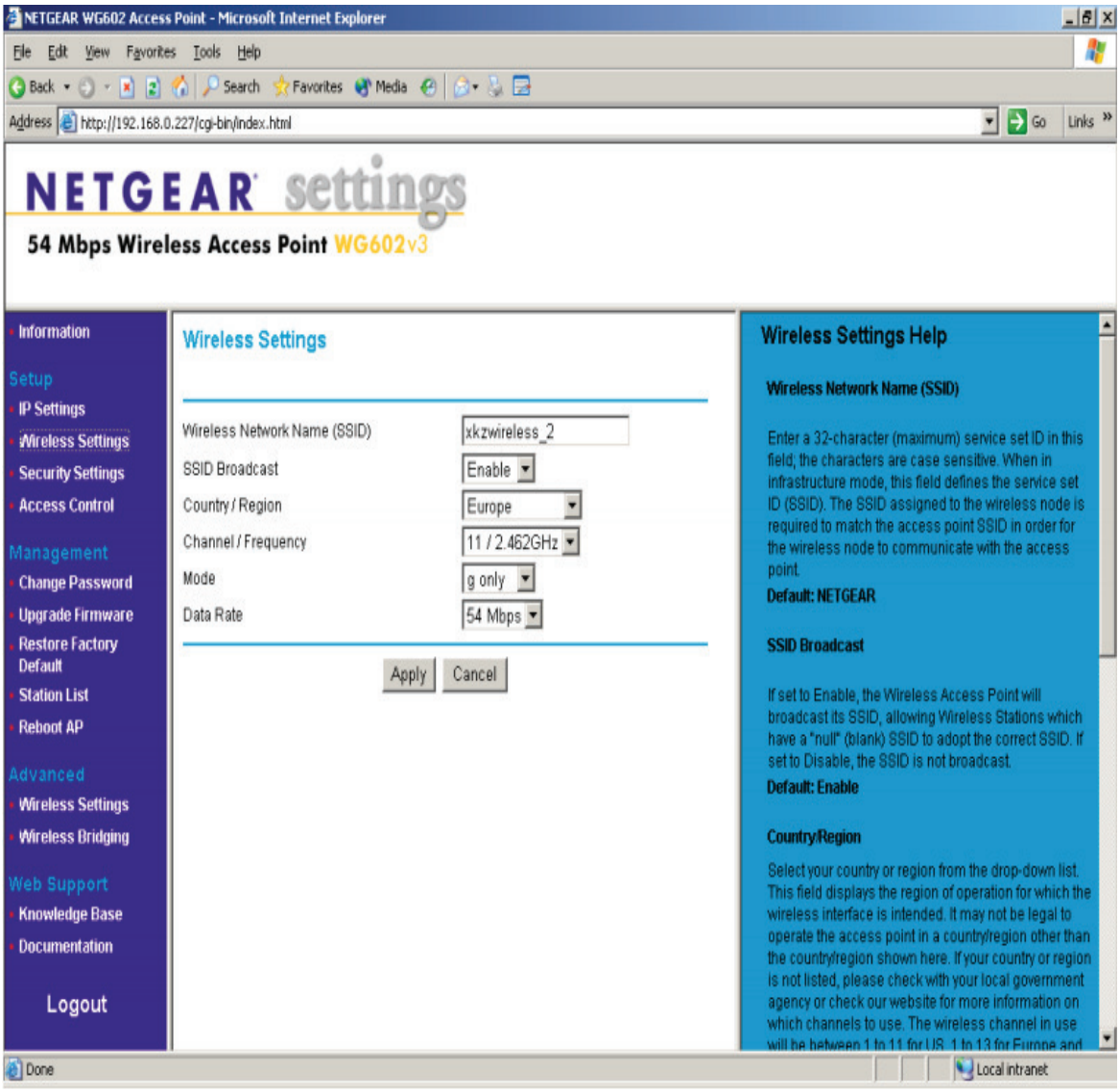
Ρυθμίσεις

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:

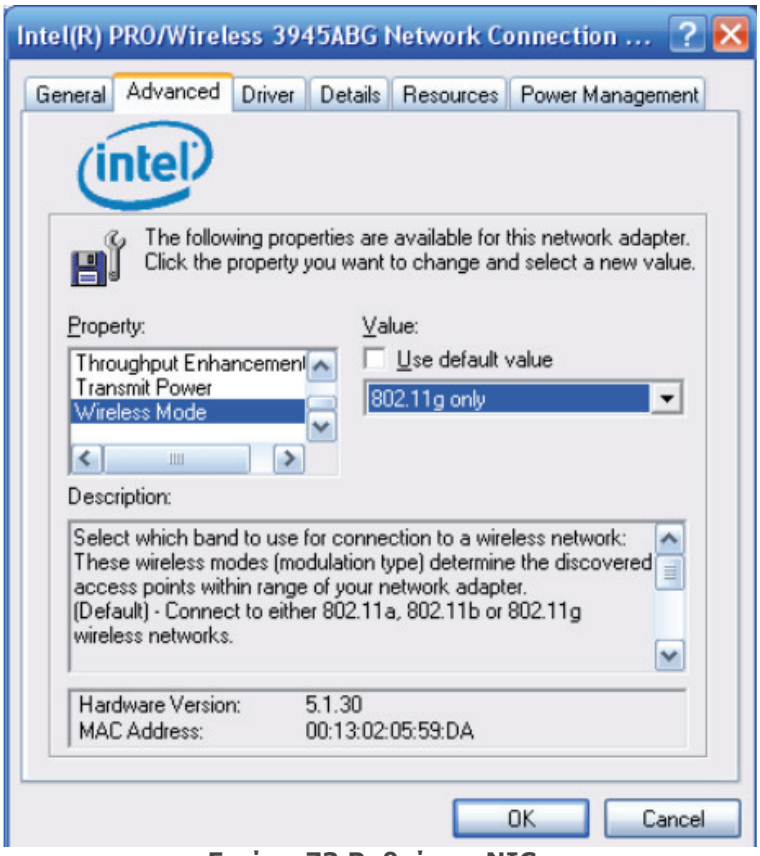
SSID Broadcast	Enable
Channel / Frequency	11 / 2.462MHz
Mode	802.11g only
Data Rate	54 Mbps
WMM Support	Disable
RTS Threshold	2347 bytes
Fragmentation Length	2346 bytes
Beacon Interval	100ms
DTIM Interval	1
Preamble Type	Short

Εικόνα 71 Ρυθμίσεις AP για μέγιστη απόδοση.



Εικόνα 72 Netgear Ρυθμίσεις.

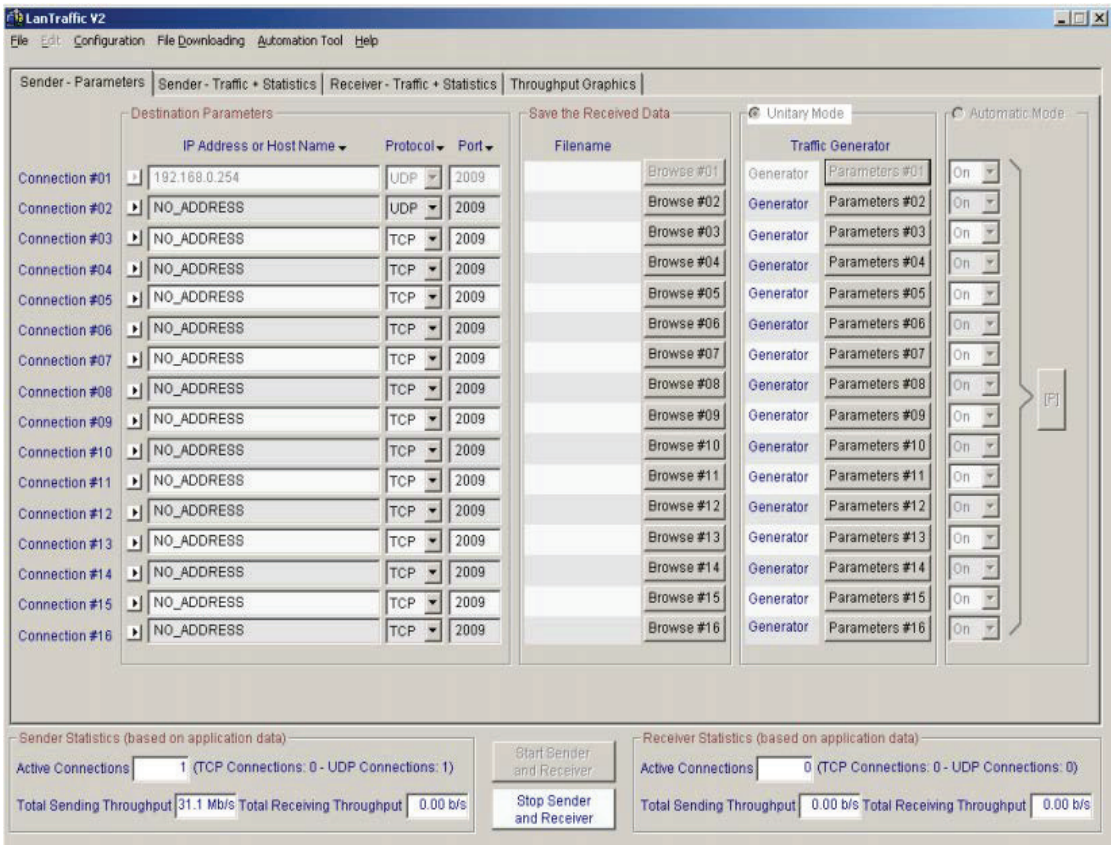
Αντίστοιχες ρυθμίσεις έγιναν και στους οδηγούς των καρτών δικτύου των τερματικών, όπου αυτό ήταν απαραίτητο.



Εικόνα 73 Ρυθμίσεις NIC.

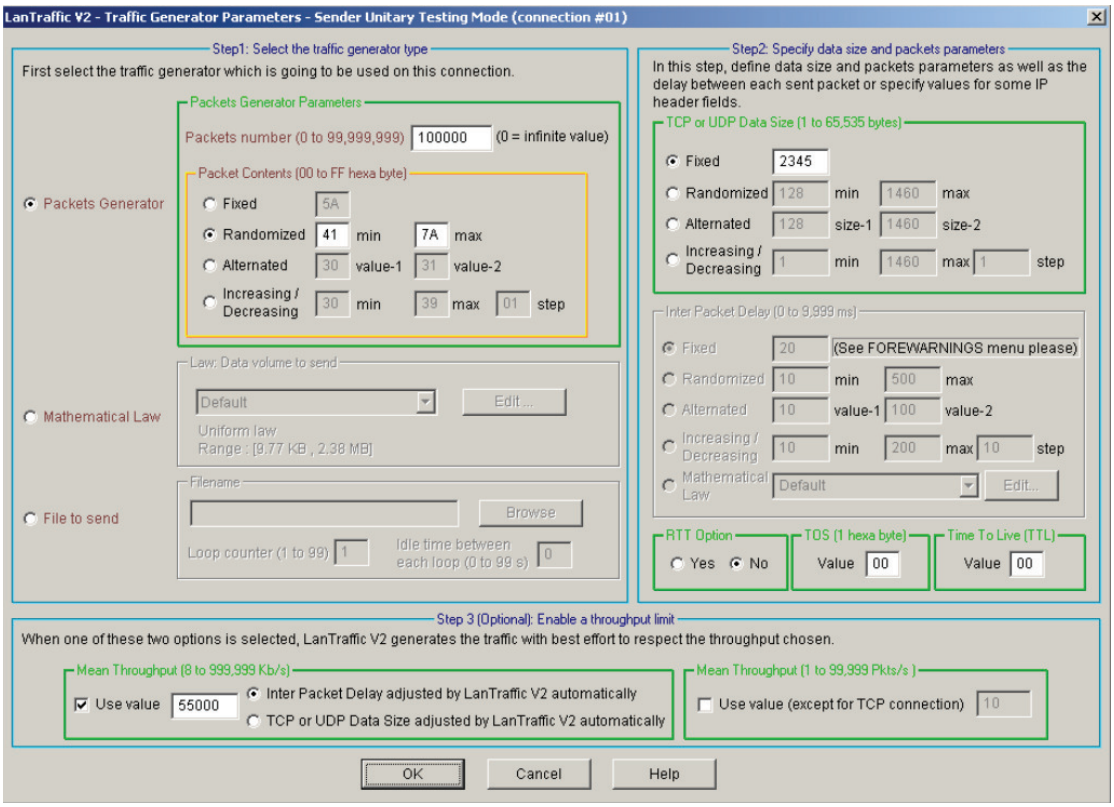
LanTraffic V2

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.



Εικόνα 74 Lan Traffic v2.

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



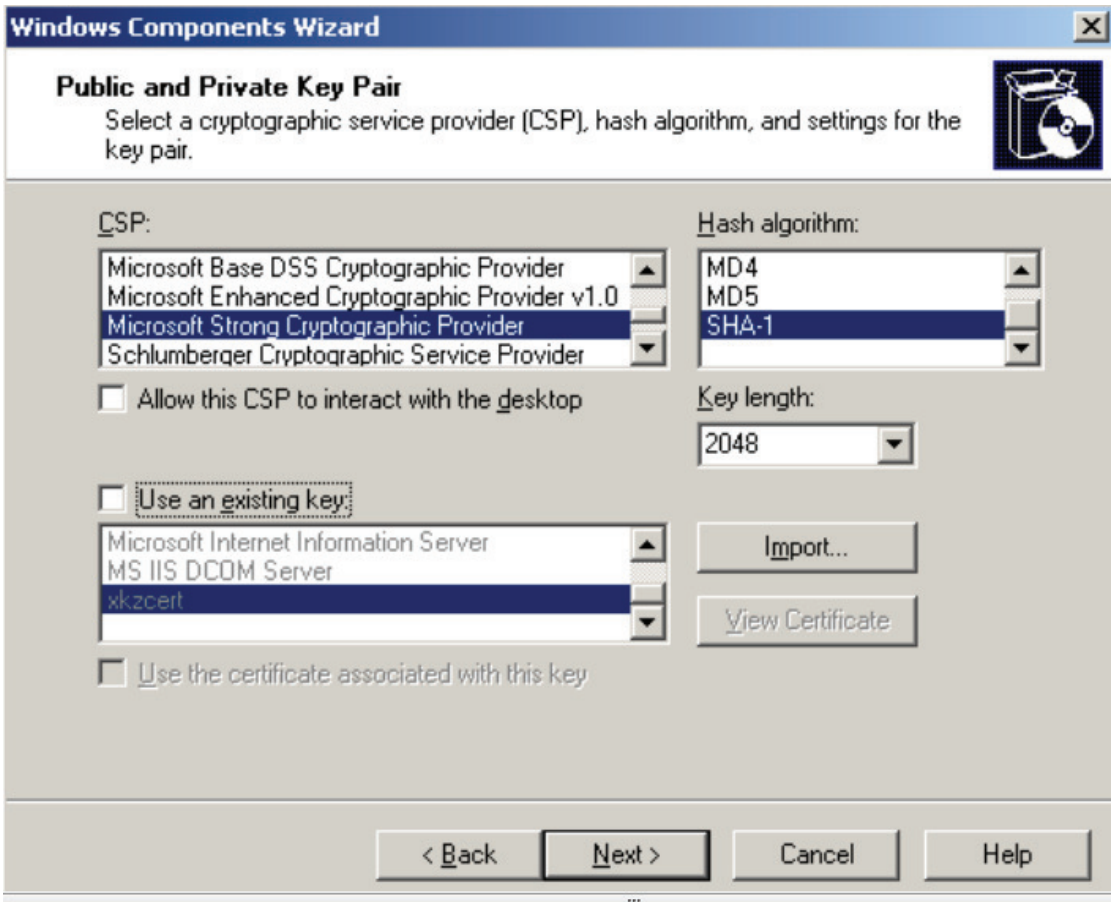
Εικόνα 75 Ρυθμίσεις πακέτων.

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.
67Τέλος, 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.

Εγκατάσταση RADIUS server και Certification Authority

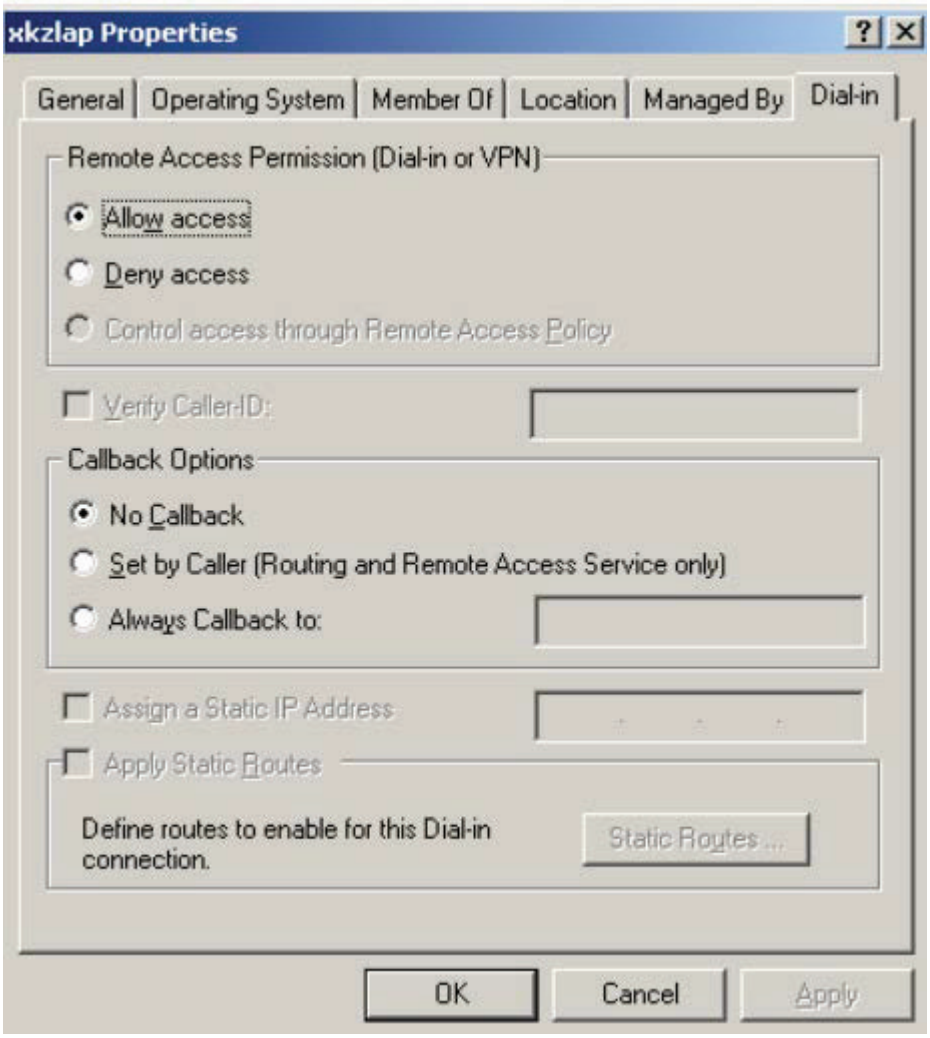
Για τις ανάγκες της μέτρησης απόδοσης του δικτύου με ασφάλεια WPA/WPA2 Enterprise χρειάστηκε η εγκατάσταση των αναγκαίων υπηρεσιών για την εξυπηρέτηση ενός εταιρικού δικτύου. Το λειτουργικό σύστημα που χρησιμοποιήθηκε είναι το Microsoft Windows 2003 Server στην Enterprise εκδοχή του.
Οι ρυθμίσεις και 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 .



Εικόνα 76 Ρυθμίσεις παραμέτρων.

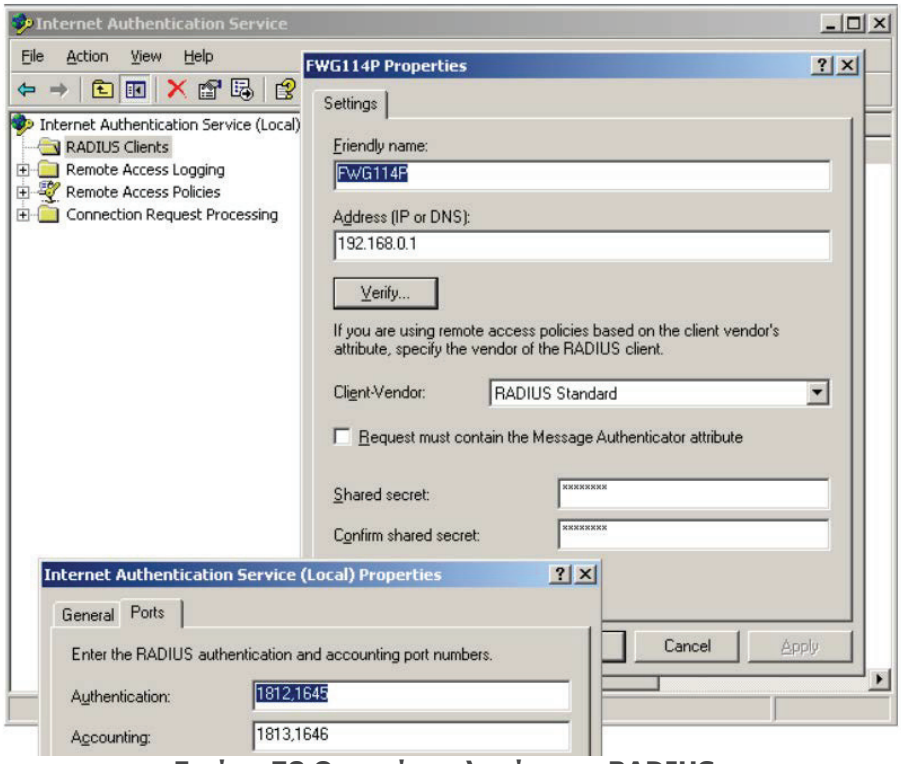
Με το τέλος της εγκατάστασης δημιουργείται και το ψηφιακό πιστοποιητικό της CA. Στην περίπτωσή μας το xkzcert.crt.
Για την λειτουργία του πρωτοκόλλου RADIUS σε περιβάλλον Windows Server πρέπει να εγκατασταθούν οι υπηρεσίες Internet Information Services και Internet Authentication Service. Όπως και προηγουμένως, 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



Εικόνα 77 Να επιτρέπεται η απομακρυσμένη πρόσβαση.

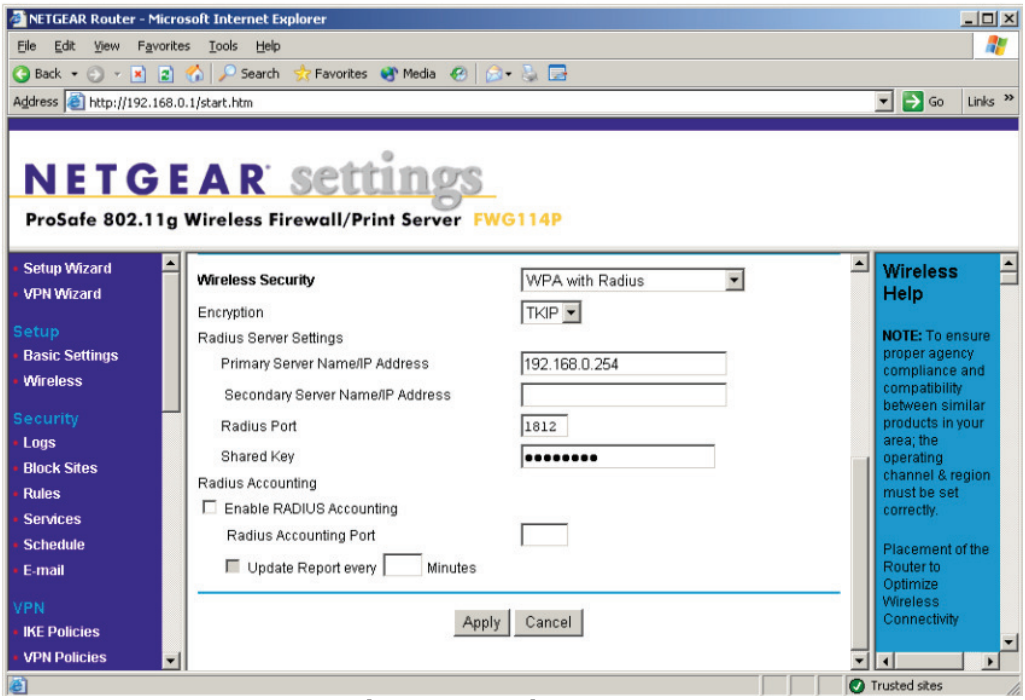
Η ίδια διαδικασία πρέπει να επαναληφθεί και για κάθε χρήστη του ασυρμάτου δικτύου.
Σ' αυτό το σημείο, καλό θα ήταν να δημιουργηθεί και ένα group με τους ασύρματους χρήστες για να γίνεται ομαδικά η εφαρμογή των πολιτικών ασφάλειας. Αρχικά δημιουργείται το group και στην συνέχεια προστίθενται οι χρήστες 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



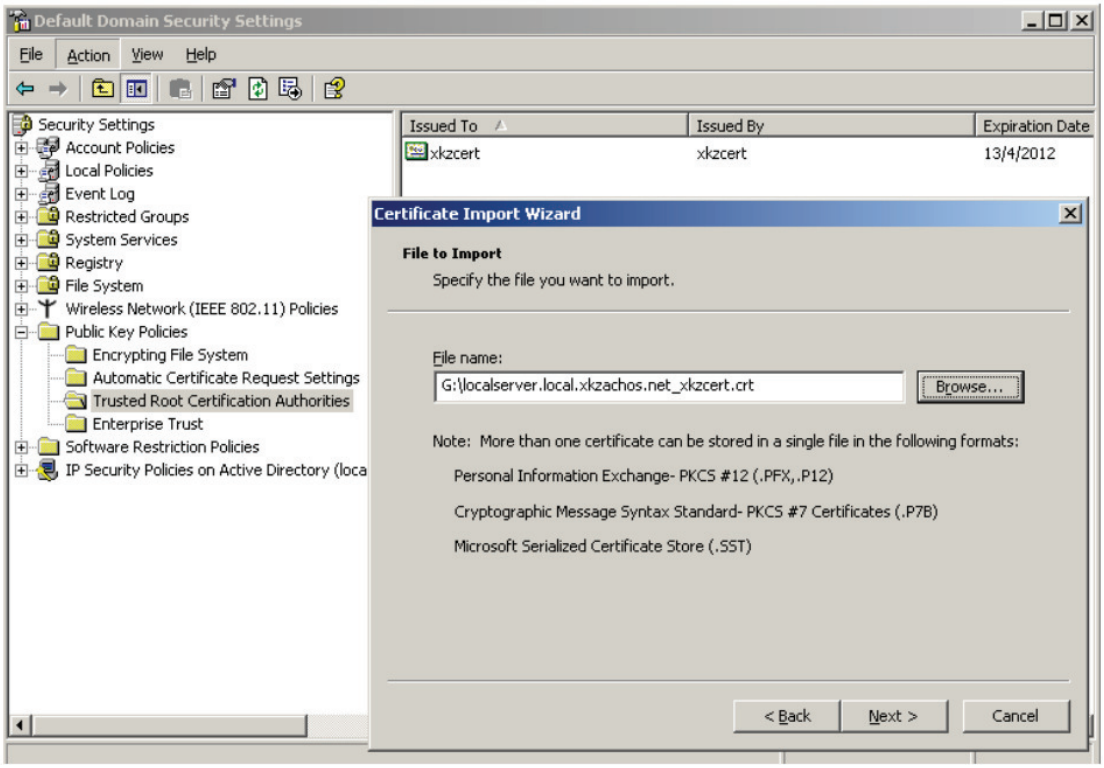
Εικόνα 78 Ορισμός πελατών του RADIUS.

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



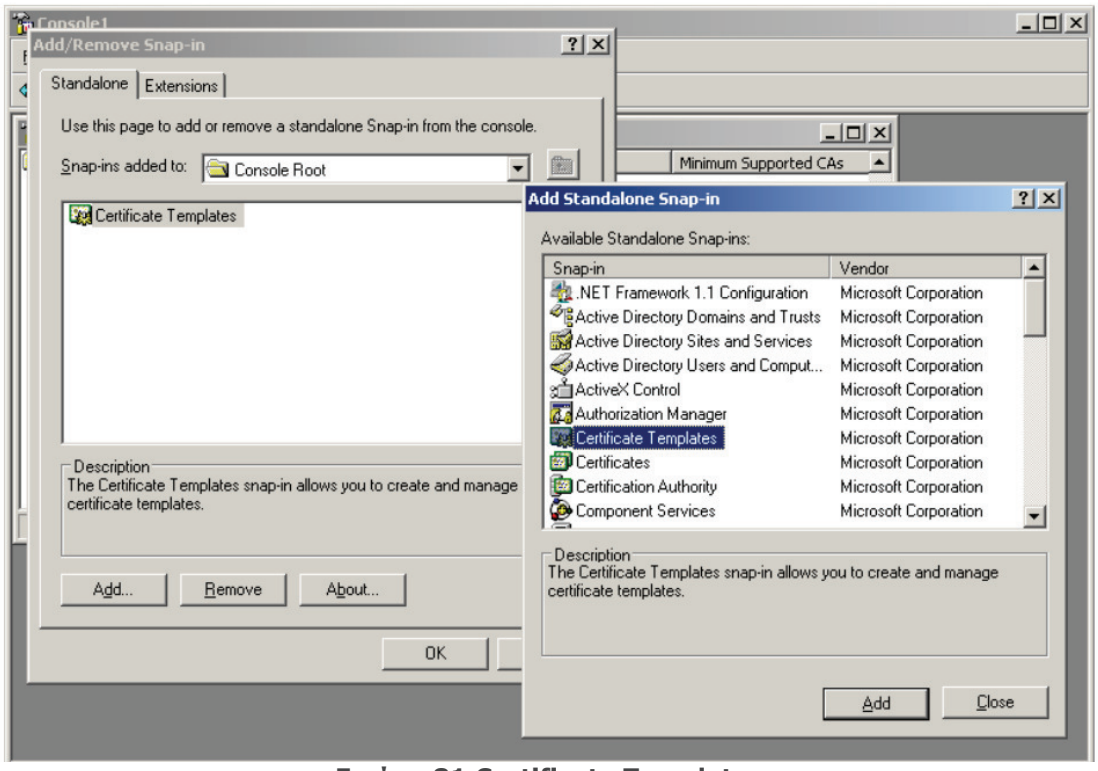
Εικόνα 79 Ρυθμίσεις στο AP.

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



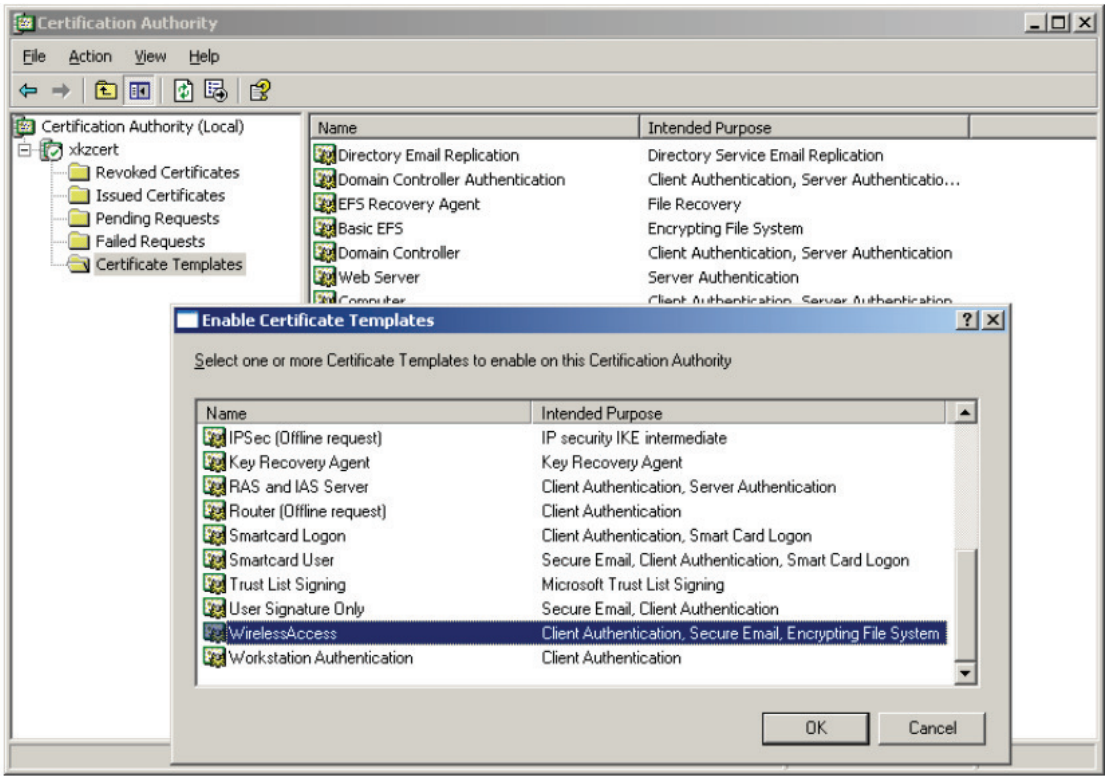
Εικόνα 80 Δημιουργία πιστοποιητικών.

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)



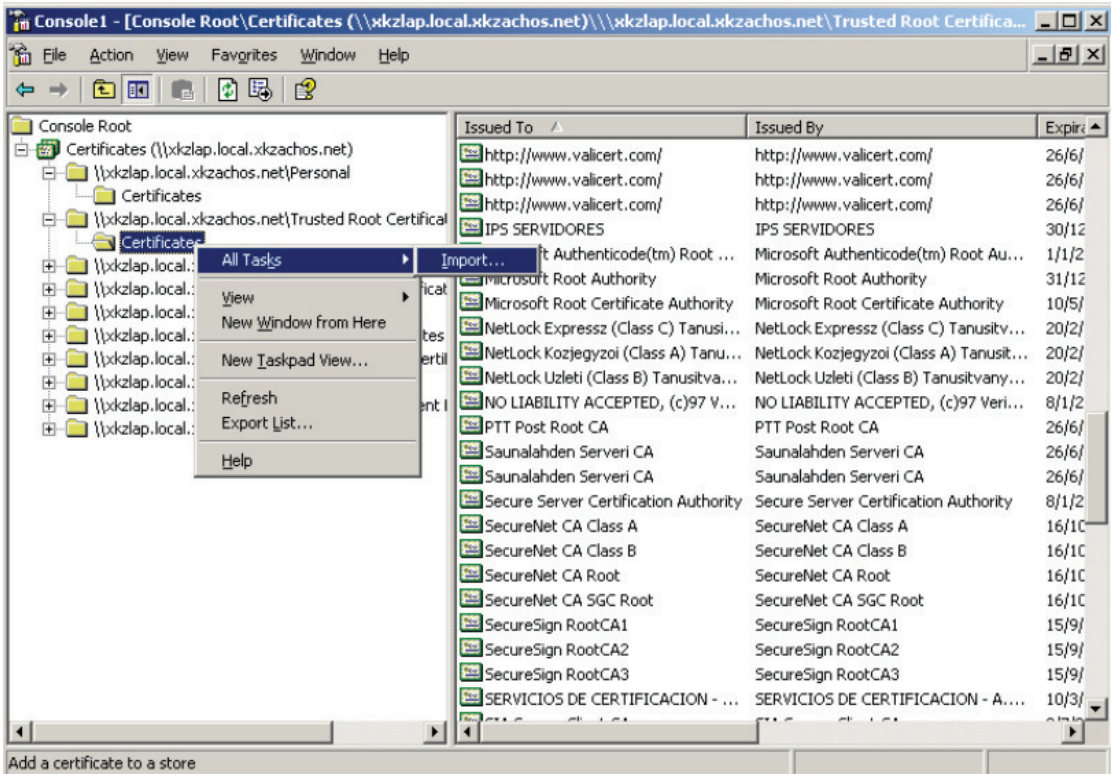
Εικόνα 81 Certificate Template.

Certification Authority
Certificate Templates
New -> Certificate Template to Issue
Enable Certificate Template ->WirelessAccess



Εικόνα 82 Επιλογή Certificate Template.

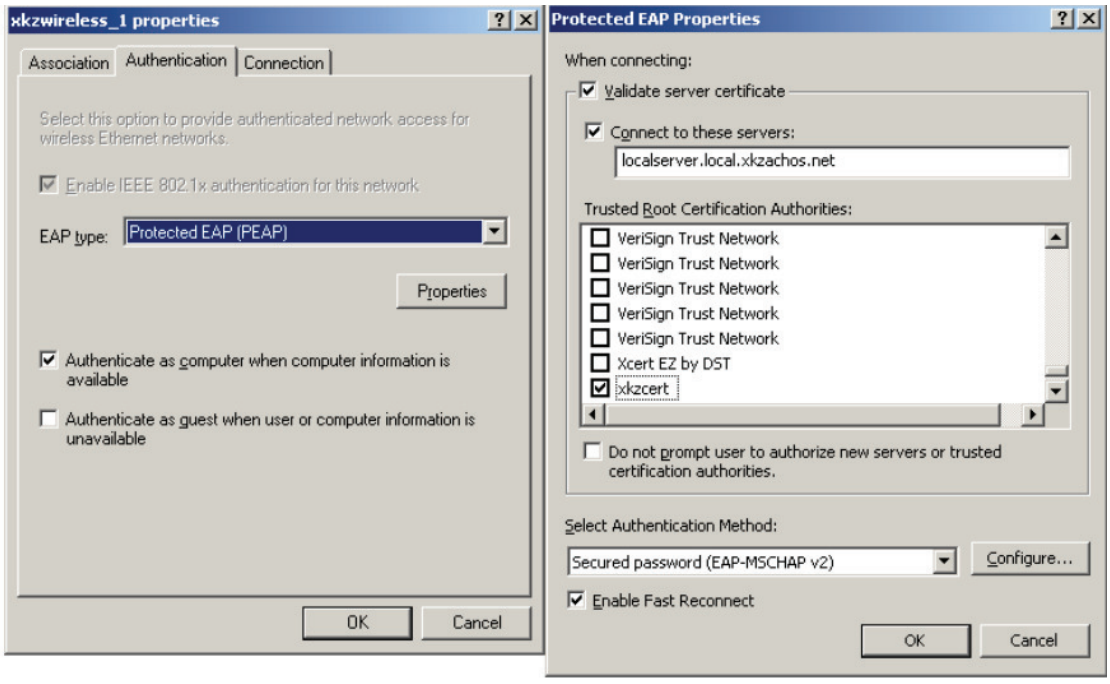
Από πλευράς server, έχουν τελειώσει όλες οι απαραίτητες ρυθμίσεις και μένουν μόνο οι ρυθμίσεις στα ασύρματα τερματικά. Και πάλι, οι ρυθμίσεις που αφορούν την είσοδο του χρήστη στο domain είναι εκτός του θέματος της εργασίας και θεωρείται ότι έχουν γίνει και λειτουργούν. Οι ρυθμίσεις που απομένουν έχουν 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. 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



Εικόνα 83 Εισαγωγή του αρχείου πιστοποιητικού.

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)

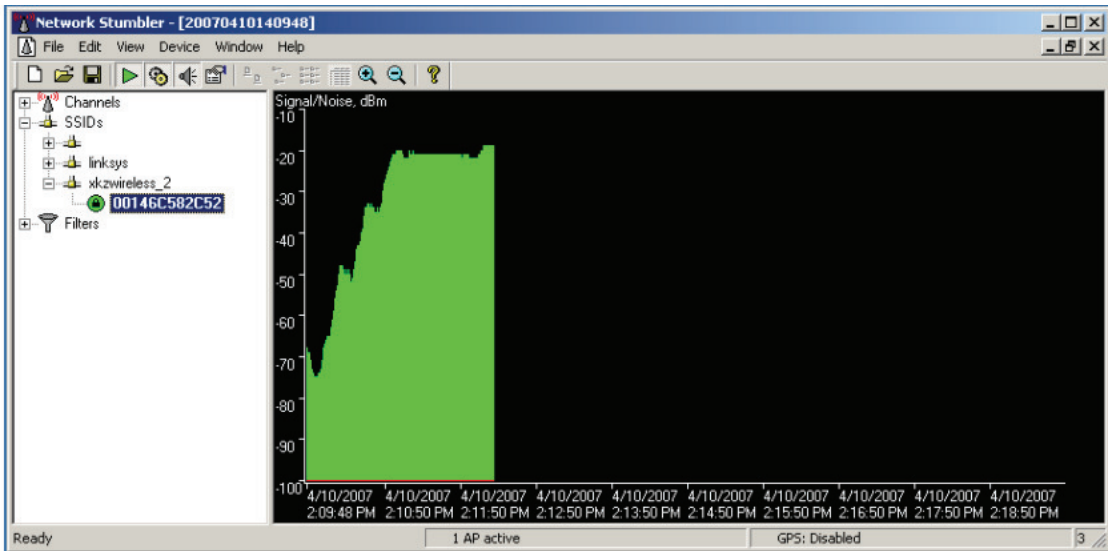
Enable IEEE 802.1x authentication for this network
EAP Type: Protected EAP (PEAP)
3Validate server certificate
Connect to these servers: localserver.local.xkzachos.net
Trusted Root Certification Authorities: xkzcert
Authentication Method: EAP-MSCHAP v2
Automatically use my Windows logon name and password



Εικόνα 84 Επιλογή του τύπου EAP.

Λήψη Μετρήσεων

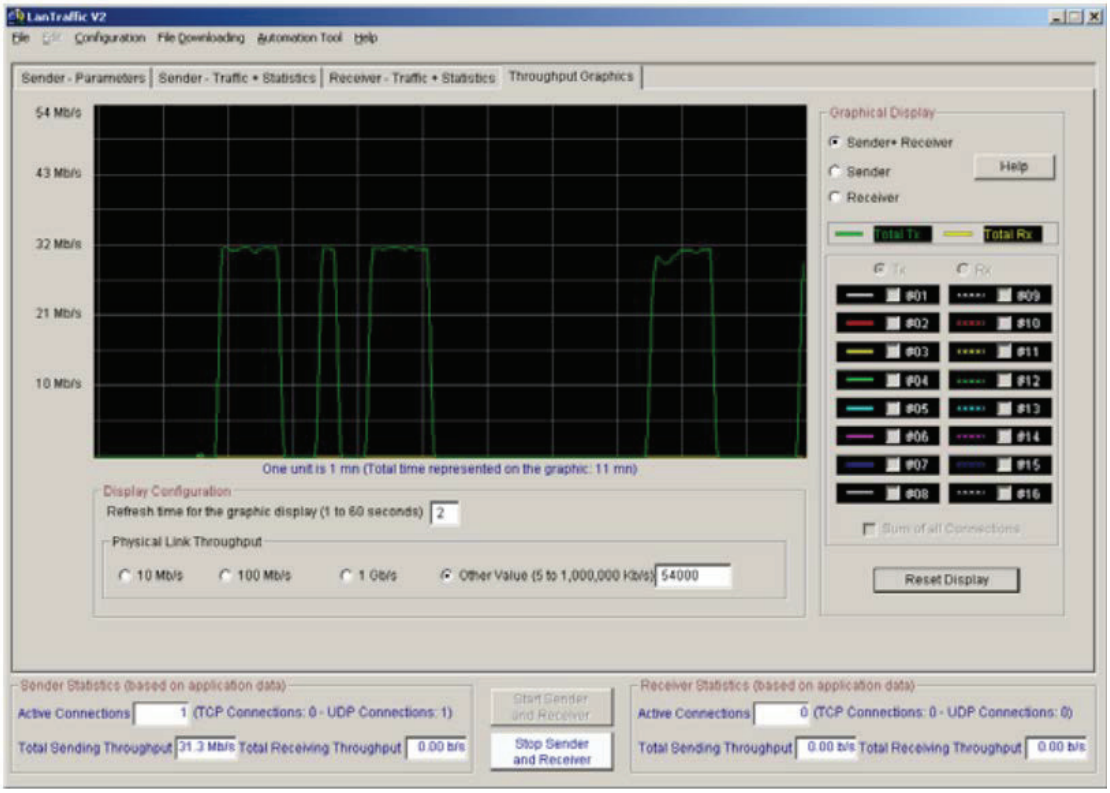
Κύριος στόχος κατά την διάρκεια των μετρήσεων ήταν να αποκλειστεί κάθε υποβάθμιση της απόδοσης που οφείλεται στο φυσικό στρώμα. Ο χώρος που έγιναν οι μετρήσεις ήταν καθαρός από παρεμβολές άλλων συσκευών που λειτουργούν στα 2,4GHz όπως άλλα ασύρματα δίκτυα και φορητά τηλέφωνα. Για την αποκάλυψη άλλων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



Εικόνα 85 Netstumbler.

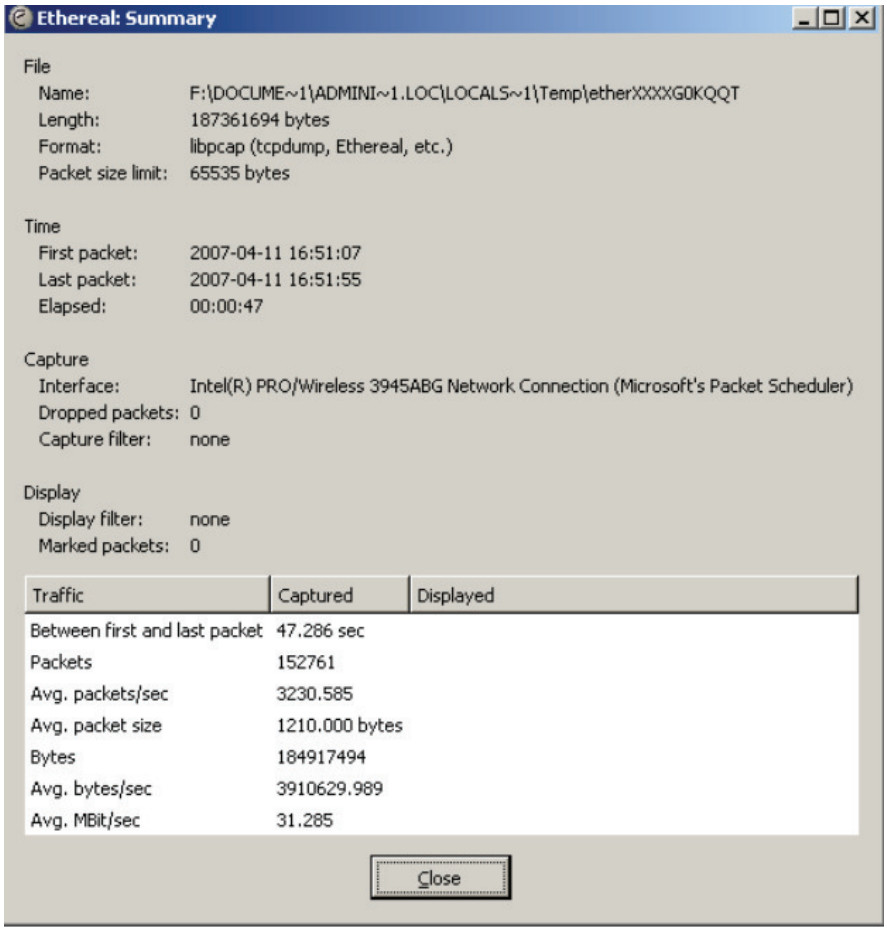
Για την αποφυγή αλλοίωσης των αποτελεσμάτων από άλλες εργασίες των Η/Υ έγινε σε όλους καθαρή εγκατάσταση λειτουργικού συστήματος και εγκατάσταση μόνο των απαραίτητων για την λήψη των μετρήσεων οδηγών στις τελευταίες τους εκδόσεις. Επίσης, όπου αυτό ήταν δυνατό, έγινε και αναβάθμιση του firmware των συσκευών.
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



Εικόνα 86 Lan Traffic V2 throughput graphics.

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, παραπάνω σχήμα) και κατά την διάρκεια (οπτικά, παρακάτω σχήμα) για μη αναμενόμενες πτώσης της απόδοσης, όπως πχ. από μεγάλο αριθμό σφαλμάτων. Σε τέτοιες περιπτώσεις, η μέτρηση επαναλαμβανόταν.

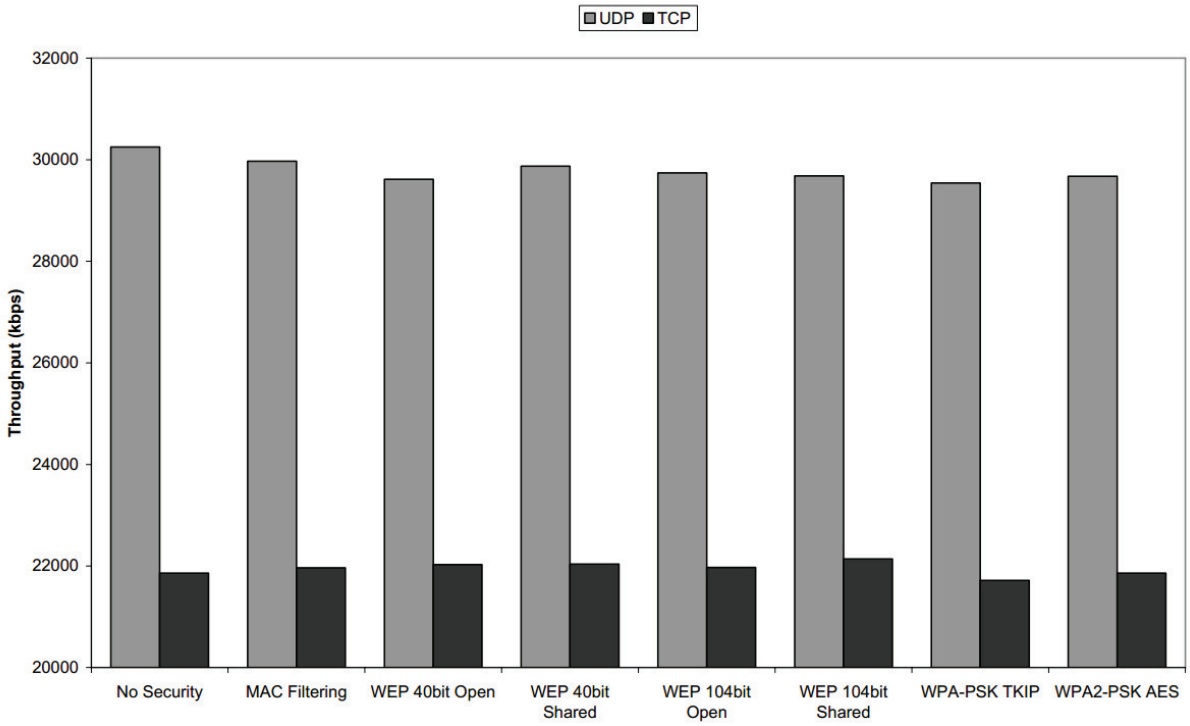


Εικόνα 87 Ethereal.

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.

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.



Εικόνα 88 Γράφημα σύγκριση πρωτόκολλων ασφάλειας WLAN στο Netgear WG602v3.

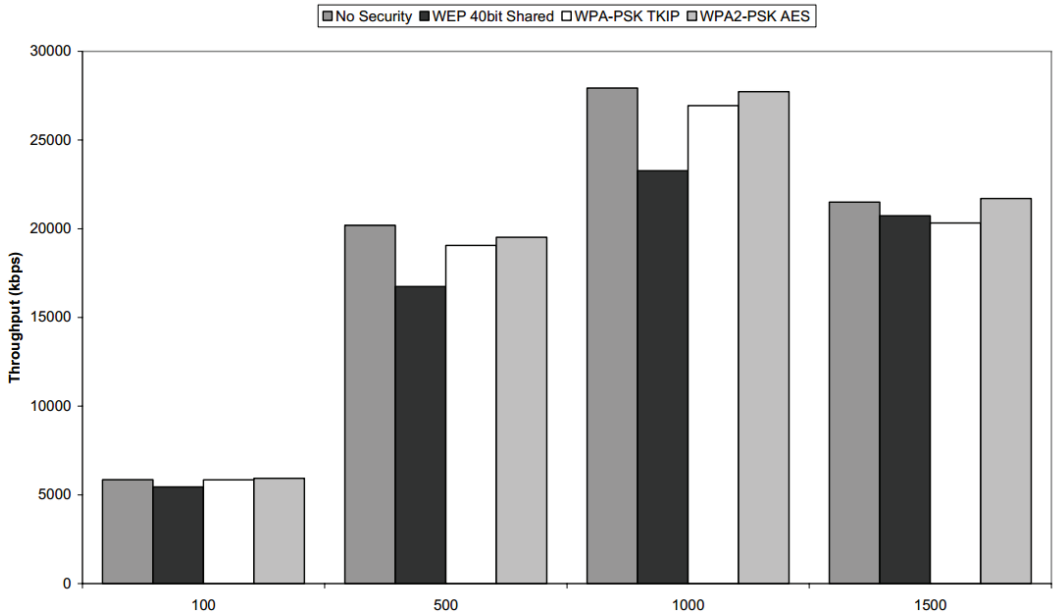
Κρυπτογράφηση	Πιστοποίηση	Απόδοση (Kbps)		Διαφορά (%)	
		UDP	TCP	UDP	TCP
Καμία	Καμία	30.252,14	21.859,11	-	-
Καμία	MAC address	29.970,76	21.965,91	-0,93	0,4886
WEP 40bit	Open	29.613,99	22.027,22	-2,11	0,7691
WEP 40bit	Shared Key	29.873,99	22.037,68	-1,25	0,8169
WEP 104bit	Open	29.739,74	21.972,01	-1,69	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

Εικόνα 89 Σύγκριση αποτελεσμάτων στο Netgear WG602v3.

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.

Μετρήσεις Μήκους Πακέτου

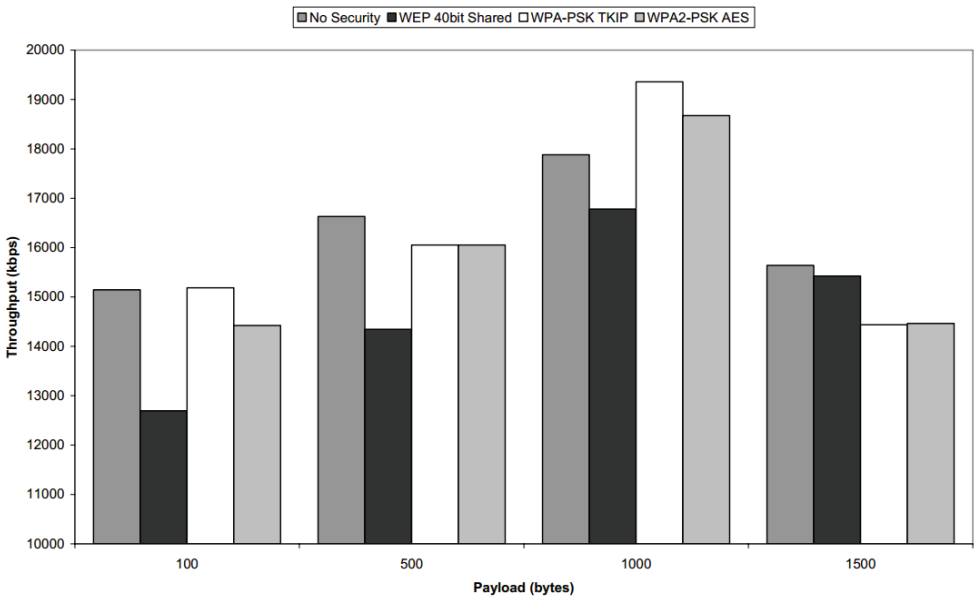
Με την επόμενη ομάδα μετρήσεων εξετάζεται η συμπεριφορά των κυριότερων μηχανισμών ασφάλειας σε σχέση με το μήκος των δεδομένων αποστολής.



Εικόνα 90 Γράφημα σύγκρισης πρωτόκολλων ασφάλειας WLAN για διαφορετικά πακέτα UDP.

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

Εικόνα 91 Αποτελέσματα σύγκρισης πρωτόκολλων ασφάλειας WLAN για διαφορετικά πακέτα.

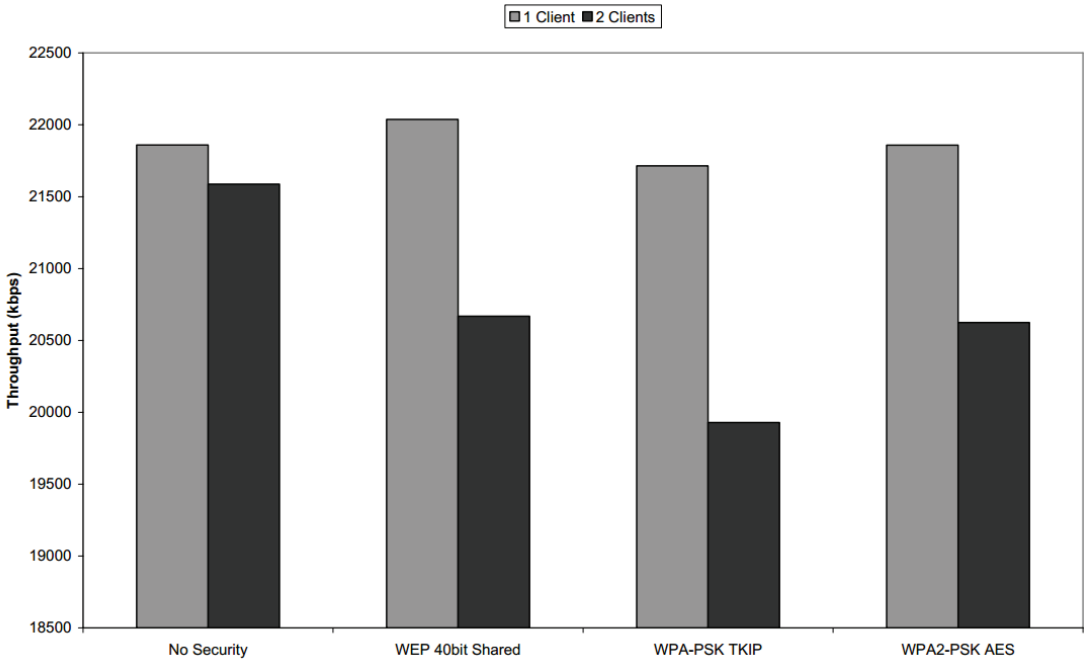


Εικόνα 92 Γράφημα σύγκρισης πρωτόκολλων ασφάλειας WLAN για διαφορετικά πακέτα TCP.

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.

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.



Εικόνα 93 Γράφημα σύγκρισης πρωτόκολλων ασφάλειας WLAN με πολλαπλούς χρήστες.

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

Εικόνα 94 Αποτελέσματα σύγκρισης πρωτόκολλων ασφάλειας WLAN με πολλαπλούς χρήστες.

Και σ' αυτή την περίπτωση, η μέγιστη υποβάθμιση της αρχικής απόδοσης του

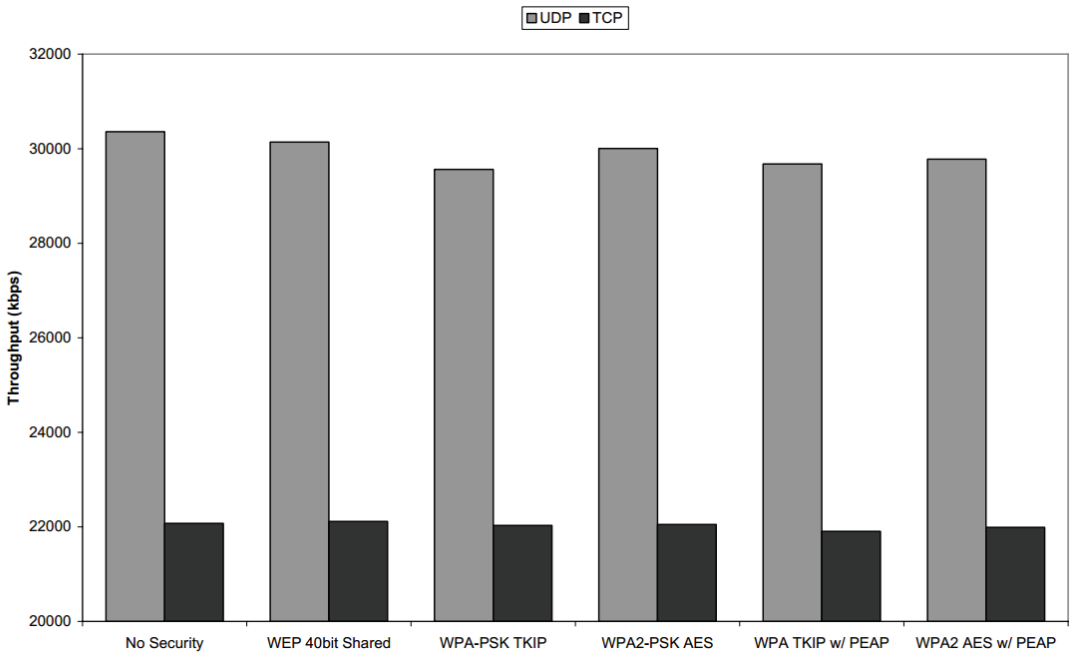
δικτύου παρατηρήθηκε στην εφαρμογή του TKIP.
Επίσης, εδώ φαίνεται και η μεγάλη επίδραση του πρωτοκόλλου του στρώματος μεταφοράς: Σε πακέτα UDP οι διαφορές παρέμειναν αμελητέες σε σύγκριση με την αποστολή χωρίς ασφάλεια. Αντίθετα, με πακέτα του απαιτητικότερου TCP, το ποσοστό της πτώσης της ταχύτητας 7πλασιάστηκε σε σχέση με τις μετρήσεις με ένα χρήστη.

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.



Εικόνα 95 Γράφημα σύγκριση πρωτόκολλων ασφάλειας WLAN στο Netgear FWG114Pv2.

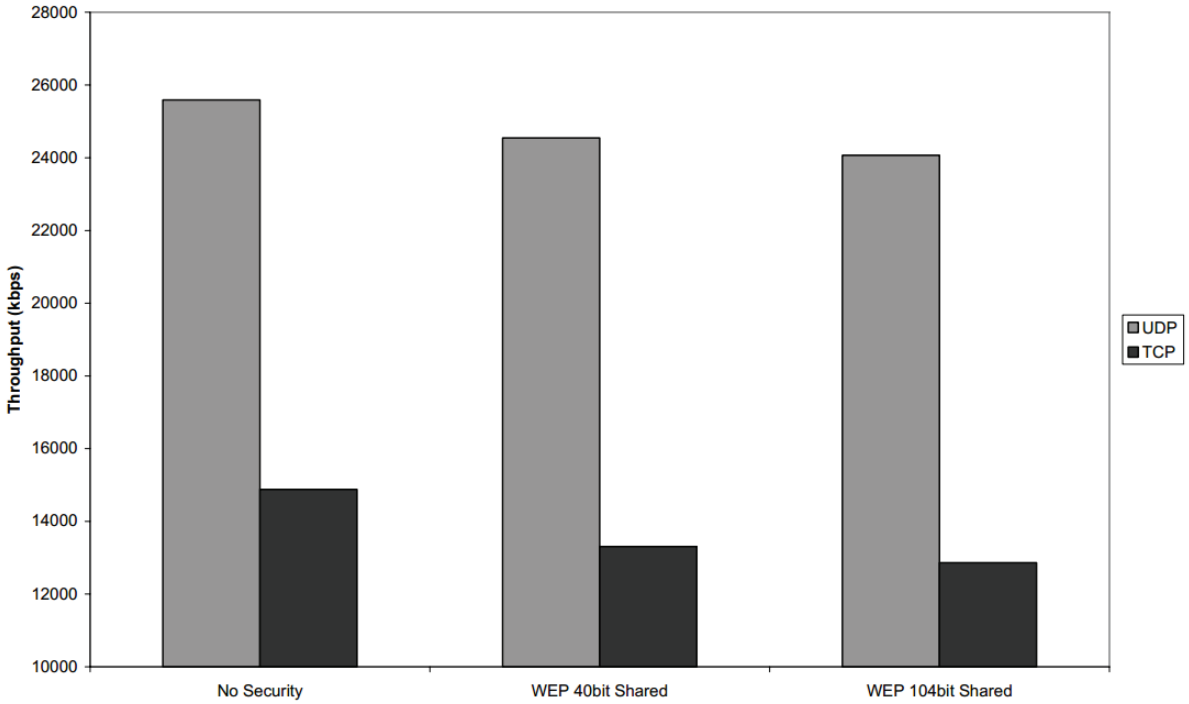
Κρυπτογράφηση	Πιστοποίηση	Απόδοση (Kbps)		Διαφορά (%)	
		UDP	TCP	UDP	TCP
Καμία	Καμία	30.360,69	22.074,20	-	-
WEP 40bit	Shared Key	30.139,54	22.114,79	-0,7284	0,1839
TKIP	Shared Key	29.563,75	22.031,85	-2,6249	-0,1918
AES	Shared Key	30.004,96	22.049,45	-1,1717	-0,1121
TKIP	802.1x/PEAP	29.676,59	21.907,04	-2,2532	-0,7572
AES	802.1x/PEAP	29.780,22	21.990,96	-1,9119	-0,3771

Εικόνα 96 Σύγκριση αποτελεσμάτων στο Netgear FWG114Pv2.

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.

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.



Εικόνα 97 Γράφημα σύγκριση πρωτόκολλων ασφάλειας WLAN στο Netgear WAG345G.

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

Εικόνα 98 Σύγκριση αποτελεσμάτων στο Netgear WAG345G.

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[6] . 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.

Συμπεράσματα

- **Επίδραση Μηχανισμών Ασφάλειας**

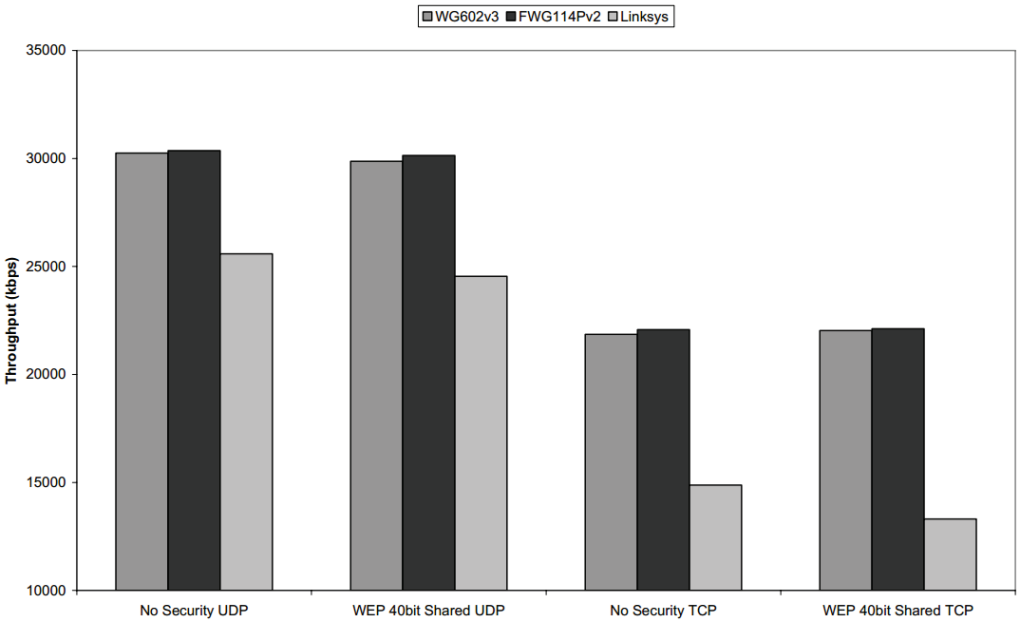
Όπως αναφέρθηκε και κατά την παρουσίαση των αποτελεσμάτων των μετρήσεων, η πτώση της απόδοσης με την εφαρμογή κρυπτογράφησης και πιστοποίησης είναι αμελητέα. Με μέγιστη πτώση 2,63% και σε κάποιες μετρήσεις ακόμα και αύξηση μισής ποσοστιαίας μονάδας, το μόνο ασφαλές συμπέρασμα που μπορεί να εξαχθεί είναι 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[7] , 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 ξαναπασχολήσει, τουλάχιστον όχι όσον αφορά την απόδοσή τους.

1. **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.

[6] 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.

[7] Good news, no news. Πραγματικά μεγάλη πτώση της απόδοσης θα είχαμε αν στο Linksys, που δεν υποστηρίζει εξαρχής το 802.11i, ήταν δυνατή η μεταπήδηση σε TKIP με αναβάθμιση του firmware. Τουλάχιστον μέχρι την διεξαγωγή των μετρήσεων αυτό δεν κατέστη δυνατό.



Εικόνα 99 Γράφημα αναπαράστασης επίδρασης υλικού.

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%

Εικόνα 100 Αποτελέσματα επίδρασης υλικού.

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.

- **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

Εικόνα 101 Αποτελέσματα επίδρασης αριθμού χρηστών.

Επίδραση Μήκους Πακέτου

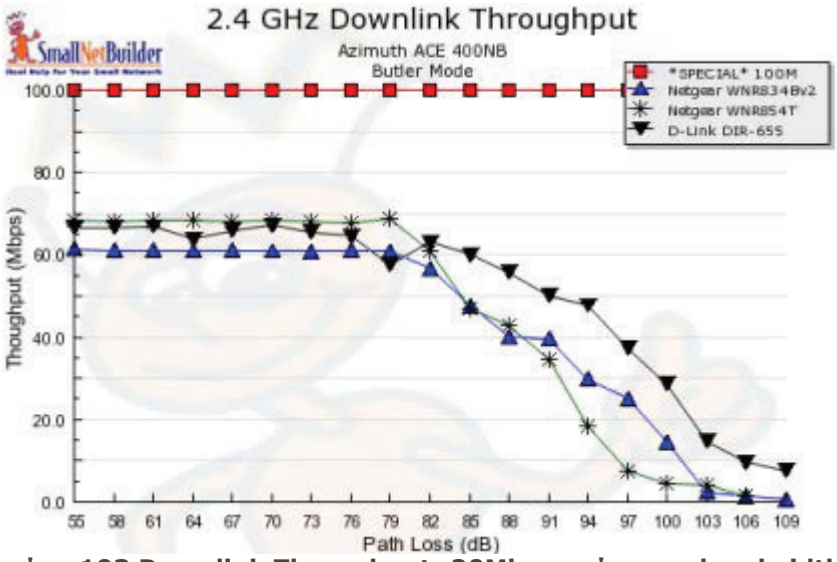
Στο σχήμα παρακάτω φαίνεται το αποτέλεσμα των μετρήσεων χωρίς καμία ασφάλεια και με το μήκος του πακέτου να εκκινεί από 1 byte και να αυξάνεται κατά 50bytes σε κάθε ομάδα μετρήσεων.
Θεωρητικά, με την αύξηση του μήκους του πακέτου θα έπρεπε να υπάρχει αντίστοιχη αύξηση στην απόδοση του δικτύου. Ο λόγος 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.

Εικόνα 102 Γράφημα αναπαράστασης επίδρασης μήκους πακέτου.

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.

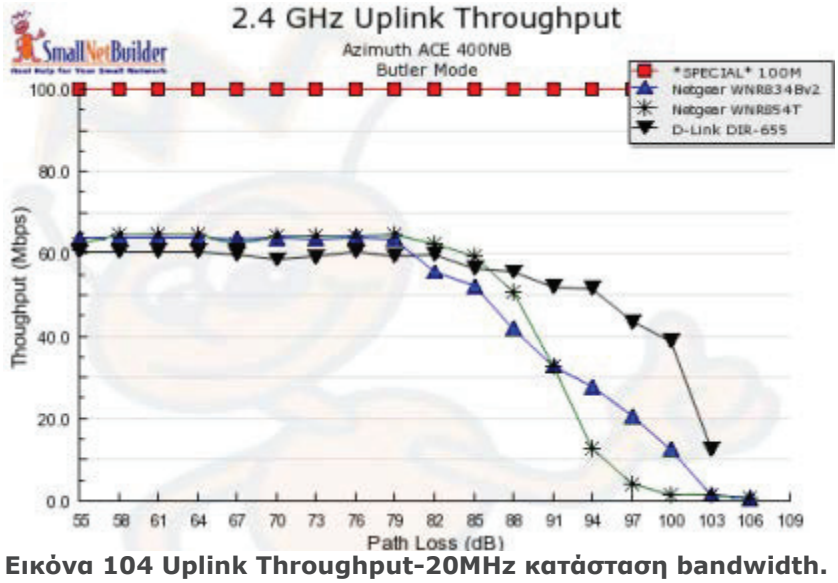
3.13 Σύγκριση της απόδοσης ασφάλειας στα ασύρματα δίκτυα 802.11n.

Παρακάτω φαίνονται διαγράμματα ασύρματης λειτουργίας που παρουσιάζουν το downlink και uplink throughput έναντι της καμπύλης του path loss για τρία 11n προϊόντα, που αντιπροσωπεύουν τρία πολύ σπουδαία 11n chipsets.
Το Netgear WNE854T χρησιμοποιεί Marvell Top Dog, το D-Link DIR-655 αντιπροσωπεύει το XSPAN του Atheros ενώ το Netgear WNR835Vv2 έχει Broadcom Intensi-fi εσωτερικά. Σημειώνεται ότι το Netgear WNR835Vv2 έχει μόνο 100Mbps WAN και LAN Ethernet Ports ενώ τα άλλα προϊόντα έχουν gigabit Ethernet.



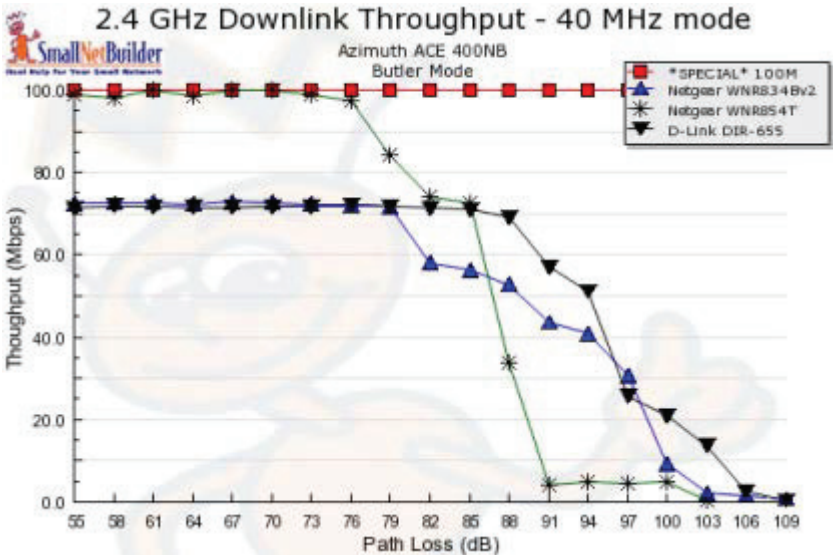
Εικόνα 103 Downlink Throughput- 20Mhz κατάσταση bandwidth.

Είναι ξεκάθαρο ότι κανένα από τα προϊόντα δεν πλησιάζει τα 100Mbps του TCP/IP throughput σε καμία από τις κατευθύνσεις up ή down. Αυτά τα γραφήματα τα έχουν οι συσκευές οι οποίες είναι διαμορφωμένες σε κατάσταση "out of the box", το οποίο σημαίνει χωρίς κρυπτογράφηση και χρησιμοποιώντας κατάσταση bandwidth 20MHz το οποίο βεβαιώνει ήρεμη συνύπαρξη με τα υπάρχοντα δίκτυα 802.11b και g.



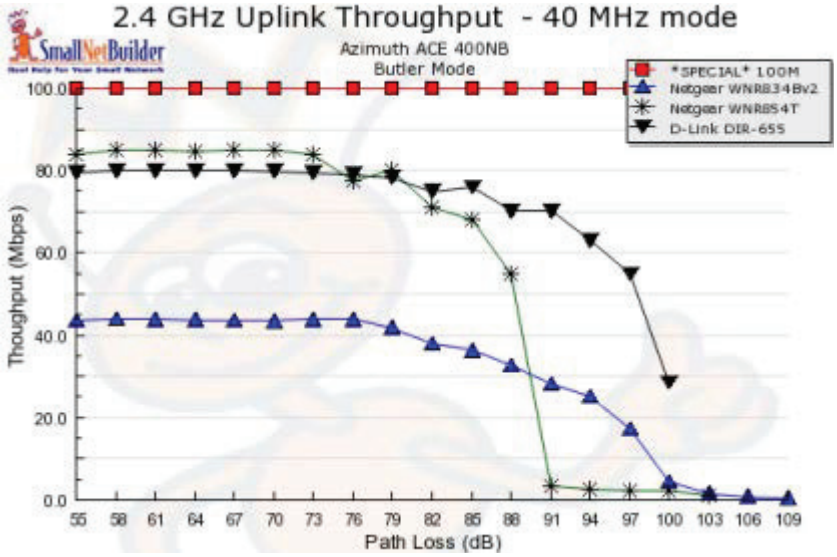
Εικόνα 104 Uplink Throughput-20MHz κατάσταση bandwidth.

Σε περίπτωση που δεν μας ενδιαφέρει να πειράξουμε τα υπάρχοντα WLAN και αλλάξουμε τις συσκευές να χρησιμοποιούν κατάσταση bandwidth 40MHz βλέπουμε παρακάτω τι γίνεται. Το Netgear WNR854T παρέχει throughput ισοδύναμο του 100Mbps Ethernet.



Εικόνα 105 Downlink Througput-40Mhz κατάσταση bandwidth.

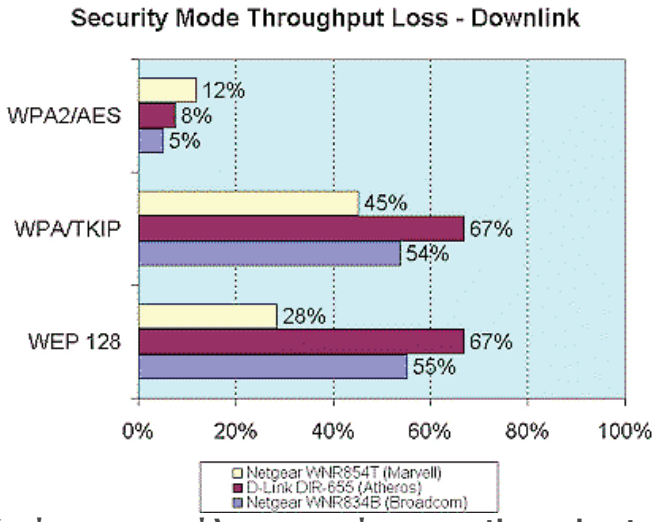
Δυστυχώς αυτό το throughput δεν κρατάει πολύ. Σύμφωνα με μελέτες τα ~80 dB path loss όπου ξεκινάει η λειτουργία να πέφτει αισθητά, αντιστοιχεί σε περίπου 50 feet μέσω μερικών τοίχων γυψοσανίδας ή περίπου 25 feet μέσω ενός οικιακού ξύλινου πατώματος.



Εικόνα 106 Uplink Throughput-40MHz κατάσταση bandwidth.

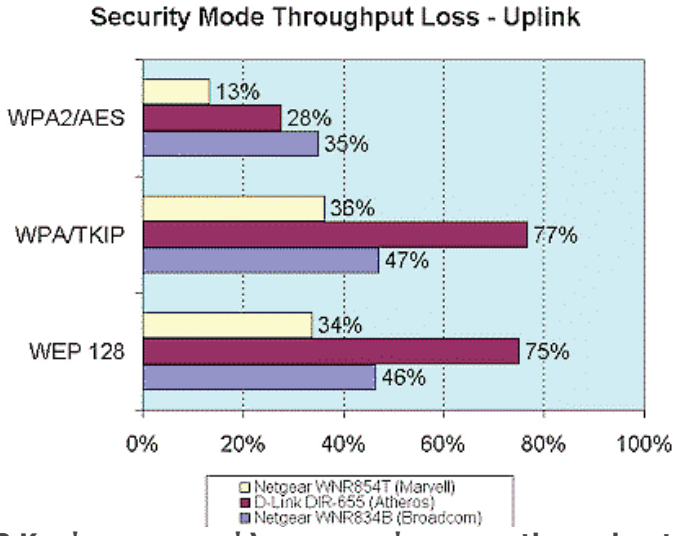
Η παραπάνω εικόνα δείχνει ότι τα δύο προϊόντα με Marvell και Atheros chipsets παρέχουν περίπου 80 Mbps του TCP/IP throughput στην uplink κατεύθυνση. Αλλά το Netgear WNR834Bv2 που χρησιμοποιεί Broadcom chipset χάνει ουσιαστικά γύρω στα 20Mbps του throughput όταν τρέχει uplink.
Πρώτον, πρέπει να ξεχάσουμε το throughput εάν χρειάζεται να χρησιμοποιήσουμε το WEP για να διευκολύνει οποιονδήποτε χρήστη. Βασικά, μπορεί να ξεχαστεί το throughput με ή χωρίς ασφάλεια εάν χρειάζεται να τρέξει ένα ανάμεικτο δίκτυο, αλλά αυτό είναι μια άλλη ιστορία. Από τη στιγμή που το WEP δεν θα είναι μέρος του τελικού 802.11n spec, οι κατασκευαστές δεν έχουν ξοδέψει πολύ χρόνο στο να ρυθμίσουν την λειτουργία του.

Το παρακάτω test έδειξε 28 σε 75% μείωση στο throughput με ενεργοποιημένο το WEP, με το Atheros chipset να εμφανίζει την υψηλότερη μείωση και το Marvell την λιγότερη.



Εικόνα 107 Κατάσταση ασφάλειας με μείωση στο throughput – downlink.

Αλλά αφού σήμερα κανείς δεν θα σκεφτόταν να τρέξει το WEP, τί συμβαίνει όταν χρησιμοποιείται το WPA/TKIP? Δυστυχώς, οι κατασκευαστές του draft 11n εξοπλισμού φαίνεται πως έχουν αποφασίσει επίσης να το αναδείξουν ως μη ελκυστική επιλογή, με ενδείξεις throughput των 35 σε 77%. Τα Atheros και Marvell chipsets πάλι εμφάνισαν την υψηλότερη και την ελάχιστη μείωση στο throughput αντίστοιχα.



Εικόνα 108 Κατάσταση ασφάλειας με μείωση στο throughput – uplink.

Συμπέρασμα

Έτσι, φαίνεται πως το WPA2/AES είναι ο μόνος τρόπος για ασύρματη ασφάλεια στο draft 11n. Αλλά ακόμα και τότε, πρέπει να πληρώσεις για να παίξεις. Το WPA2/AES επίσης δίνει μια επιπλέον καμπύλη με μια σημαντική διαφορετική λειτουργία για το down και uplink στα δύο από τα τρία chipsets.
Ο πιο συνεπής εκτελεστής και στις δύο κατευθύνσεις είναι το Marvell chipset το οποίο ανέρχεται περίπου στα 12% loss. Η μεγαλύτερη διαφορά, 5% loss down,

35% loss up, βρέθηκε με τον καλύτερο εκτελεστή —το Broadcom chipset. Το Atheros ήταν περισσότερο σαν το Broadcom, με 8% loss down και 28% up.
Το αρνητικό με αυτό είναι ότι οι κατασκευαστές καιρό πριν δημιούργησαν μηχανές κρυπτογράφησης hardware στις δικές τους baseband/MAC chipsets με την προσδοκία του πιο ανθεκτικού υλικού που απαιτείται από το WPA/WPA2. Αλλά κάτι φαίνεται να έχει χαθεί στην βιασύνη για το 11n, και άλλη μια φορά, ο τελικός χρήστης πληρώνει μια υπερτίμηση της τιμής για, κάποιες φορές, ένα άλμα οπισθοδρομικό στην λειτουργία.

Βιβλιογραφία

1. http://www.ehow.com/info_12198599_wep-vs-wpa-speed.html
2. http://www.diffen.com/difference/WPA_vs_WPA2
3. http://www.differencebetween.net/technology/internet/difference-between-aes-and-rc4/
4. http://askville.amazon.com/difference-AES-TKIP/AnswerViewer.do?requestId=7123665
5. http://networking.answers.com/wifi/aes-vs-tkip-a-networking-overview
6. http://www.tomshardware.com/reviews/wireless-security-hack,2981-6.html
7. https://supportforums.cisco.com/discussion/11537196/wpa-and-wpa2-both-using-tkip-and-aes
8. https://learningnetwork.cisco.com/thread/11207
9. http://www.cox.com/myconnection/learn/safe-and-sound/wpa-vs-wep.cox
10. http://www.wikihow.com/Secure-Your-Wireless-Home-Network
11. http://www.speedguide.net/faq_in_q.php?qid=331
12. http://www.smallnetbuilder.com/wireless/wireless-features/30184-draft-11n-does-not-equal-100-mbps-ethernet
13. http://hardforum.com/showthread.php?t=1189390
14. http://www.darknet.org.uk/2008/12/confused-by-wep-wpa-tkip-aes-other-wireless-security-acronyms/
15. http://www.differencebetween.net/technology/internet/difference-between-aes-and-rc4/
16. http://compnetworking.about.com/b/2008/08/21/aes-vs-tkip-for-wireless-encryption.htm
17. http://networking.answers.com/wifi/aes-vs-tkip-a-networking-overview
18. http://www.smallnetbuilder.com/wireless/wireless-basics/30664-5-ways-to-fix-slow-80211n-speed
19. http://www.youtube.com/watch?v=aYS56CzVIQM
20. http://www.youtube.com/watch?v=WLS6F0Nb7cU
21. http://www.youtube.com/watch?v=hLQ5rYNUwNg
22. http://www.medialab.ntua.gr/education/MultimediaTechnology/MultimediaTechnologyNotes/chap2d_1.htm
23. Ανάπτυξη εφαρμογών σε προγραμματιστικό περιβάλλον
24. Comparison of various WLAN securities, Shikha Bansal, Manish Mahajan, International Journal Of Enterprise Computing and Business Systems, 2013
25. Comparison of wireless security protocols (wep and wpa2), Baba Banda, Fatehgarh Sahib, International Journal Of Enterprise Computing and Corporate Research, 2012
26. LOTKIP: Low Overhead TKIP Optimization for Ad Hoc Wireless Network, M. Razvi Doomun, K.M. Sunjiv Soyjaudah, paper
27. AES CCMP Algorithm with N-Way Interleaved Cipher Block Chaining, Zadia Codabux-Rossan, M. Razvi Doomun, paper
28. A comparison between wireless lan security protocols, Nidal Turab, Florica Moldoveanu, paper
29. Energy Efficient Novel Cipher Security Mechanism for Wireless, B.T Geetha, M.V Srinath, International Journal of Emerging Trends & Technology in Computer Science
30. A comparison of Security in Wireless Network Standards with a Focus on Bluetooth, WiFi and WiMax, Gunther Lackner, International Journal of Network Security
31. Analyzing Wireless Lan Security Overhead, Harold Lars McCarter, Thesis, Virginia Polytechnic Institute & State University
32. «Ανάπτυξη του πρωτόκολλου CCMP για ασφαλή ασύρματα δίκτυα 802.11 σε FPGA», Λαουδιάς Χρήστος, διπλωματική εργασία, Πανεπιστήμιο Πατρών

33. «Αξιολόγηση της απόδοσης ενός Wi-Fi δικτύου μέσω λήψης μετρήσεων», Σιανκο Ιντριτ, Πτυχιακή εργασία, ΤΕΙ Κρήτης
34. Wireless Network Security Still has no Clothes, Diaa Salama, Hatem Abdual Kader, Mohiry Hadhoud, International Arab Journal of e-Technology
35. Wireless security, Anish Kumar, seminar report
36. «Επίδραση μηχανισμών ασφάλειας στην απόδοση των ασύρματων LAN/MAN 802.11», Χρήστος Ζάχος, διπλωματική εργασία, ΤΕΙ Θεσσαλονίκης
37. «Υλοποίηση κρυπτογραφικού συστήματος σε υλικό για ασύρματες επικοινωνίες», Πρασσά Διονυσία, διπλωματική εργασία, Πανεπιστήμιο Πατρών
38. 802.11 Wireless Networks: The Definitive Guide, Matthew Gast, O'Reilly
39. Building A Cisco Wireless LAN, Eric Ouellet-Robert Padjen-Arthur Pfund, Syngress Publishing, Inc.
40. Cisco Wireless LAN Security, Krishna Sankar-Sri Sundaralingam-Andrew Balinsky-Darrin Miller, Cisco Press
41. CCNA Wireless Official Exam Certification Guide, Brandon James Carroll, Cisco Press
42. The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards, Stanley Wong, paper from SANS Institute
43. Computer Networks (2003), Fourth Edition, Tanenbaum Andrew S.
44. Computer Networking: A Top-Down Approach (2008), Fourth Edition, James F. Kurose-Keith W.Ross
45. Ασύρματα Δίκτυα (2006), P. Nicopolitidis – M. S. Obaidat – G. I. Papadimitriou – A. S. Pomportsis
46. «Υλοποίηση κρυπτογραφικού συστήματος σε υλικό για ασύρματες επικοινωνίες» (2008), ΠΡΑΣΣΑ ΔΙΟΝΥΣΙΑ, διπλωματική εργασία, ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
47. *«Ανάπτυξη εκπαιδευτικού λογισμικού αυτό-διδασκαλίας Πρωτοκόλλων Ασυρμάτων Δικτύων» (2005), ΡΟΥΠΑΣ ΧΡΥΣΟΣΤΟΜΟΣ – ΘΕΙΑΚΟΥΛΗ ΑΓΓΕΛΙΚΗ, ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ*
48. Το Αλφαβητάρι της Ασύρματης Δικτύωσης, Γιαννακός Νικήτας-Κοσσιφίδης Νικόλαος-Πανουσίου Σωκράτης-Πεϊκίδης Ιωάννης
49. Τεχνολογίες σύγχρονων ασύρματων δικτύων δεδομένων (2007), ΚωνσταντίνοςΓεωργακόπουλος, Σχολή Τεχνολογικών Εφαρμογών, Τμήμα Βιομηχανικής Πληροφορικής, ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΑΒΑΛΑΣ
50. 802.11 Wireless Networks Security and Analysis (2010), Alan Holt - Chi-Yu Huang, Springer-Verlag London
51. «Ασφάλεια σε Ασύρματα Δίκτυα 802.11»(2010), Μαρκομανωλάκη Αικατερίνη, πτυχιακή εργασία, ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΡΗΤΗΣ
52. Wireless Communications (2005), Andrea Goldsmith, Cambridge University Press
53. The State of Wi-Fi Security Wi-Fi CERTIFIED WPA2TM Delivers Advanced Security to Homes, Enterprises and Mobile Devices, Wi-Fi Alliance, January 2012
54. Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks, Wi-Fi Alliance, April 29 2003
55. Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise, Wi-Fi Alliance, March 2005
56. http://phys.org/news/2014-03-wpa2-wireless.html

57. www.wikipedia.com
58. http://wiki.freeradius.org/glossary/Wi-Fi-Protected-Access
59. https://www.yumpu.com/en/document/view/16323513/history-of-pre-rsn-ieee-80211-security
60. http://www.airtightnetworks.com/home/resources/knowledge-center/wpa2-hole196-vulnerability.html
61. http://www.smallnetbuilder.com/wireless/wireless-howto/31914-how-to-crack-wpa-wpa2-2012
62. The evolution of wireless security in 802.11networks: WEP, WPA and 802.11 standards, paper, SANS Institute InfoSec Reading Room
63. 802.11 Denial of Service Attacks and Mitigation, paper, SANS Institute
64. InfoSec Reading Room
65. Κρυπτογραφία και ασφάλεια δικτύων, εργασία, Πανεπιστήμιο Πατρών ΜΤΠ Διοίκησης Επιχειρήσεων
66. Security Analysis and Improvements for IEEE 802.11i, paper**,** Changhua He John C Mitchell, Electrical Engineering and Computer Science Departments Stanford University, Stanford CA
67. Identifying and Responding to Wireless Attacks, Chris Hurley, Black Hat Japan 2005
68. Practical attacks against WEP and WPA, paper, Martin Beck, TU-Dresden, Germany, Erik Tews, TU-Darmstadt, Germany, November 8, 2008
69. Beyond cracking your neighbor's wep key, Thomas “Mister X” d'Otreppe de Bouvette, Rick “Zero Chaos” Farina
70. Evolution of Wireless Security, Stephen J. Esposito, II Computing Specialist Y-12 National Security Complex August 9, 2007the Focus of WiFi Security
71. Wi-Fi security – WEP, WPA and WPA2, paper, Guillaume Lehembre
72. A History of 802.11 Security, presentation, Jesse Walker, Communications Technology Lab Intel Corporation
73. Ασφάλεια στα ασύρματα τοπικά δίκτυα (WPA/WPA2), διπλωματική εργασία, Κεφαλάς Γρηγόριος, Πανεπιστήμιο Πειραιώς
74. Evolution of Wireless LAN security architecture to IEEE 802.11i (WPA2),paper, Moffat Mathews, Ray Hunt, Department of Computer Science and Software Engineering, University of Canterbury, New Zealand
75. Ανάπτυξη του πρωτοκόλλου CCMP για ασφαλή ασύρματα δίκτυα 802.11 σε FPGA, διπλωματική εργασία, Λαούδιας Χρήστος, Πανεπιστήμιο Πατρών, Τμήμα Μηχανικών Η/Υ & Πληροφορικής
76. 20 years of Security, magazine, www.scmagazineus.com
77. A review on WEP wireless security protocol, paper, Muhammad Juwaini, Raed Alsaqour, Maha Abdelhaq, Ola Alsukour
78. Attacks against the WiFi protocols WEP and WPA, paper, Matthieu Caneill Jean-Loup Gilis
79. 802.11 Attacks Version 1.0, whitepaper, Brad Antoniewicz
80. «Μελέτη αλγορίθμου κρυπτογράφησης Advanced Encryption Strandard (AES) και υλοποίησή του μέσω λογισμικού. », πτυχιακή εργασία, Νικόλαος Δανδουλάκης, ΤΕΙ Κρήτης