Τ.Ε.Ι. Δυτικής Ελλάδας
Τμήμα Μηχανικών Πληροφορικής Τ.Ε

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επισκόπηση θεμάτων ασφάλειας και ακεραιότητας Δεδομένων σε Δίκτυα Αισθητήρων

ΣΟΦΙΑ ΚΟΝΔΥΛΟΠΟΥΛΟΥ
ΑΜ:1210

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ
ΒΑΣΙΛΕΙΟΣ ΤΣΑΚΑΝΙΚΑΣ

ΠΑΤΡΑ
2015

Πρόλογος

Στα πλαίσια αυτής της πτυχιακής γίνεται μια μελέτη στα Ασύρματα Δίκτυα Αισθητήρων (Wireless Sensor Networks, WSN) που αποτελούν, τα τελευταία χρόνια, μία περιοχή με μεγάλη ερευνητική δραστηριότητα. Οι ιδιαιτερότητες αυτών των δικτύων καθιστούν τη μελέτη τους ξεχωριστή από τις ήδη υπάρχουσες τεχνολογίες ασύρματων δικτύων (όπως Ad-Hoc ή IEEE 802.11). Οι ιδιαιτερότητες των δικτύων αυτών δημιουργούν νέα πεδία εφαρμογής (ιατρικά, επιστημονικά, επιχειρηματικά κ.α.). Η εργασία επεκτείνεται και αναλύει τα διάφορα πρωτόκολλα ασφάλειας και ακαιρεότητας δεδομένων κατά την δρομολόγηση ενώ κυκλώματος, καθώς και τις τεχνολογίες ενδιάμεσου λογισμικού που χρησιμοποιούνται, ή μπορούν να χρησιμοποιηθούν, προκειμένου τα δίκτυα αυτά να λειτουργούν απρόσκοπτα με τη μικρότερη κατανάλωση ενέργειας. Για την πληρότητα του θέματος η μελέτη αυτή ολοκληρώνεται με μια επισκόπηση και σύγκριση κυκλωμάτων χρησιμοποιώντας το εργαλείο προσομείωσεις Matlab.

Θα ήθελα να ευχαριστήσω τον επιβλέποντα της εργασίας, καθηγητή Βασίλειο Τσακανίκα, του Τμήματος Μηχανικών Πληροφορικής για τη δυνατότητα που μου έδωσε προκειμένου να ασχοληθώ με το συγκεκριμένο θέμα όπως επίσης για την ανοχή και υπομονή που έδειξε, καθ' όλη τη διάρκεια της.

Περίληψη

Με την εμφάνιση του Διαδικτύου, κανείς δεν θα μπορούσε να φανταστεί πως αυτό θα μπορούσε να αποτελέσει μέσο για την εκτέλεση διαφόρων τύπων επιθέσεων, που βασικό σκοπό θα είχαν την εκμετάλλευση δεδομένων προκειμένου να προκαλέσουν σημαντικά προβλήματα, ίσως σε ένα ολόκληρο δίκτυο.

Όπως και τα παραδοσιακά δίκτυα, επιθέσεις είναι δυνατόν να δεχτούν και τα ασύρματα δίκτυα αισθητήρων, τα οποία αποτελούν τα τελευταία χρόνια ένα σημαντικό τομέα στον οποίο βασίζονται μεγάλες ερευνητικές δραστηριότητες.
Συγκεκριμένα θα μπορούσαμε να πούμε πως είναι ακόμα πιο ευάλωτα από τα συνηθισμένα δίκτυα λόγω της φύσεως τους.

Αυτού του είδους τα δίκτυα, αποτελούν μια εντελώς διαφορετική κατηγορία δικτύων από τα παραδοσιακά, παρουσιάζοντας κάποιες ιδιαιτερότητες και οι οποίες καθιστούν την μελέτη τους ξεχωριστή, σε σχέση με τα υπόλοιπα.

Ουσιαστικά αυτό που τα καθιστά ιδιαίτερα ως προς τα άλλα, είναι το ότι αποτελούνται από πολλούς κόμβους, μικρού μεγέθους, οι οποίοι λειτουργούν μερικώς αυτόνομα και έχουν περιορισμένες υπολογιστικές δυνατότητες.

Στην παρούσα λοιπόν διπλωματική εργασία, αρχικά γίνεται μια περιγραφή των ασύρματων δικτύων αισθητήρων όπως επίσης και πού μπορούν να βρουν εφαρμογή. Επιπλέον αναφέρονται μερικοί τρόποι αντιμετώπισης επιθέσεων και απειλών, που ενδεχομένως τα δίκτυα αυτά να δεχτούν. Τέλος γίνεται λήψη κάποιων μετρήσεων και γίνεται μια περιγραφή του τρόπου με τον οποίο αντιδρά το σύστημα, όταν σε αυτό βάλουμε κάποιο προτόκολλο ασφάλειας.

Περιεχόμενα

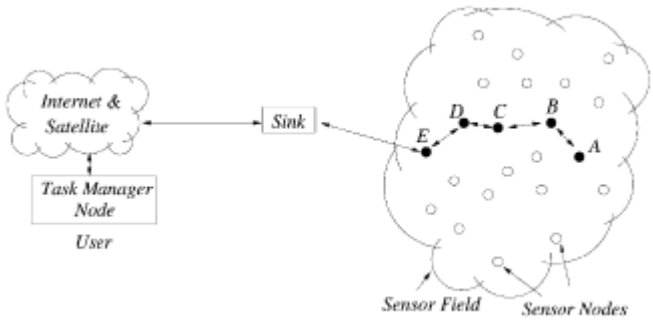
ΚΕΦΑΛΑΙΟ 1

Ασύρματα Δίκτυα Αισθητήρων – WSN

1.1 Εισαγωγή

Η πρόσφατη πρόοδος της τεχνολογίας στις ασύρματες επικοινωνίες και στην ηλεκτρονική έχουν καταστήσει εφικτή την ανάπτυξη αισθητήρων χαμηλού κόστους και ισχύος, που είναι πολύ πολύ μικροί σε μέγεθος, ενεργειακά αυτόνομοι και μπορούν να επικοινωνήσουν σε μικρές αποστάσεις μεταξύ τους. Ένα ασύρματο δίκτυο αισθητήρων (WSN) (Εικόνα 1.1) αποτελείται από ένα μεγάλο αριθμό κόμβων αισθητήρων κατάλληλα τοποθετημένων κοντά στο φαινόμενο παρατήρησης ή μέσα σ' αυτό. Η θέση των αισθητήρων μπορεί να μην είναι σχεδιασμένη ή προκαθορισμένη. Αυτό επιτρέπει την τυχαία ανάπτυξη τους σε περιβάλλοντα μη προσπελάσιμα από τον άνθρωπο ή σε επιχειρήσεις αντιμετώπισης καταστροφών. Από την άλλη πλευρά, αυτό προϋποθέτει ότι τα πρωτόκολλα και οι αλγόριθμοι των δικτύων αυτών έχουν την ικανότητα να οργανώνονται από μόνα τους.

Ένα ακόμα σημαντικό χαρακτηριστικό των δικτύων αισθητήρων είναι και ο τρόπος επικοινωνίας μεταξύ των κόμβων αισθητήρων. Κάθε κόμβος ενσωματώνει και έναν επεξεργαστή που του δίνει την δυνατότητα, αντί να στείλει τα δεδομένα κατευθείαν σε έναν καθορισμένο κόμβο που έχει αναλάβει τη μίξη τους, να χρησιμοποιεί ο ίδιος πρώτα των επεξεργαστή του για την εκτέλεση καθορισμένων απλών υπολογισμών και στη συνέχεια να αποστέλλει μόνο τα απαραίτητα και μερικώς επεξεργασμένα δεδομένα. Η ενσωμάτωση της δυνατότητας τοπικής επεξεργασίας και αποθήκευσης δεδομένων επιτρέπει στις μονάδες να εκτελέσουν πολύπλοκες λειτουργίες σύμφωνα με την εκάστοτε εφαρμογή που υλοποιούν. Επίσης, η δυνατότητα επικοινωνίας μεταξύ τους επιτρέπει όχι μόνο τη μεταφορά και τον έλεγχο των δεδομένων κατά μήκος του δικτύου, αλλά και τη συνεργασία μεταξύ των μονάδων κόμβων προς επίτευξη πολύπλοκων αλγορίθμων και εργασιών, όπως είναι η συνάθροιση δεδομένων (data aggregation), η στατική δειγματοληψία και η παρακολούθηση της κατάστασης και της υγείας ενός συστήματος.



Εικόνα 1.1: Διάσπαρτοι ασύρματοι αισθητήρες σε περιοχή παρακολούθησης

Οι βασικές ιδιότητες των ασύρματων δικτύων αισθητήρων συνοψίζονται στα παρακάτω σημεία:

- Δυνατότητα αυτό-οργάνωσης
- Επικοινωνία περιορισμένου βεληνεκούς και δρομολόγηση πολλαπλών αλμάτων (multi-hop)
- Πυκνή τοποθέτηση των κόμβων και συνεργατική προσπάθεια
- Συχνά μεταβαλλόμενη τοπολογία λόγω εξασθένησης του σήματος και αποτυχίας των κόμβων
- Περιορισμοί στην ενέργεια, την ισχύ εκπομπής, την μνήμη και την υπολογιστική δυνατότητα
- Πιθανότατα έλλειψη γενικής αναγνώρισης (identification) των κόμβων λόγω υψηλού overhead και μεγάλου αριθμού κόμβων

1.2 Διαφορές των ασύρματων δικτύων αισθητήρων

Τα ασύρματα δίκτυα αισθητήρων μπορούν να θεωρηθούν δίκτυα υπολογιστικών συσκευών, όμως έχουν βασικές διαφορές από τα παραδοσιακά δίκτυα δεδομένων(Πίνακας 1.1):

i. Σε σχέση με τα κλασικά δίκτυα υπολογιστών έχουν χαμηλότερη υπολγιστική ισχύ και περιορισμούς στην ενέργεια, την αποθήκευση και το εύρος ζώνης. Οι δρομολόγηση και η διαχείριση κινητικότητας, στα παραδοσιακά ασύρματα δίκτυα, εκτελούνται με σκοπό τη βελτιστοποίηση του QoS. Η κατανάλωση ενέργειας συνιστά δευτερεύουσα απαίτηση, καθώς η πηγή ενέργειας μπορεί να αντικατασταθεί ή να επαναφορτιστεί οποιαδήποτε στιγμή. Τα ασύρματα δίκτυα αισθητήρων έχουν σχεδιαστεί για εφαρμογές σε περιβάλλον λειτουργίας χωρίς την ανάγκη ανθρώπινης παρέμβασης. Συνεπώς, η υπηρεσία της δρομολόγισης πρέπει να αποσκοπεί στη βελτιστοποίηση της χρήσης της ενέργειας, με σκοπό τη μεγιστοποίηση της διάρκειας ζωής του δικτύου.

ii. Η συνήθης κίνηση δεδομένων στα παραδοσιακά δίκτυα υπολογιστών προκύπτει από χρήστες που συνδέονται με έναν κόμβο και απαιτούν κάποια υπηρεσία. Η σύνδεση μεταξύ των δύο αυτών κόμβων πιθανότατα θα πραγματοποιείται με τη βοήθεια και άλλων ενδιάμεσων κόμβων. Ο χρήστης αλληλεπιδρά άμεσα με το χρήστη ή την υπηρεσία στο άλλο άκρο επικοινωνίας από την άποψη ότι το μοντέλο αλληλεπίδρασης είναι ευθύ. Από την άλλη, τα ασύρματα δίκτυα αισθητήρων μοιάζουν περισσότερο σε κατανεμημένα συστήματα και όχι σε τυπικά δίκτυα. Οι κόμβοι

συνεργάζονται για τη παραγωγή των αποτελεσμάτων, ενώ ο χρήστης συνήθως δεν ενδιαφέρεται για τα αποτελέσματα μεμονωμένων κόμβων. Τα ασύρματα δίκτυα αισθητήρων, δεν παρέχουν υπηρεσίες διασύνδεσης απομακρυσμένων κόμβων, αλλά πληροφορίες μεταβολών καταστάσεων από περιοχές του δικτύου, στους χρήστες.

iii. Οι κόμβοι ενός ασύρματου δικτύου αισθητήρων στις περισσότερες εφαρμογες είναι στατικοί αφού τοποθετηθούν, με λίγες εξαιρέσεις σε εφαρμογές οπου η κινητικότητα των κόμβων αποτελεί απαίτηση.

iv. Στους κόμβους των ασύρματων δικτύων αισθητήρων διακινούνται δεδομένα με χαμηλό ρυθμό μετάδοσης, με εμφανές το φαινόμενο του πλεονασμού.

	WSN	Ασύρματα Ad hoc δίκτυα
Αριθμός κόμβων	Μεγάλος εκατοντάδες έως χιλιάδες κόμβοι ή και περισσότεροι	Μικρός μέχρι μέσος
Πυκνότητα κόμβων	Υψηλή	Σχετικά χαμηλή
Πλεονασμός δεδομένων	Υψηλός	Περιορισμένος
Τροφοδότηση ισχύος	Μη επαναφορτιζόμενη λειτουργία αναντικατάστατες μπαταρίες	Επαναφορτιζόμενη λειτουργία και/ή αντικατάσταση μπαταριών
Ρυθμός δεδομένων	Χαμηλός 1-100kbps	Υψηλός
Κινητικότητα των κόμβων	Χαμηλή	Πιθανότατα υψηλή κινητικότητα
Κατεύθυνση της ροής δεδομένων	Κυρίως μονοκατευθυντήρια ροή ασύρματοι κόμβοι → sink	Δικατευθυντήρια από άκρο σε άκρο
Προώθηση πακέτων	Πολλοί κόμβοι σε έναν κατεύθυνση προσανατολισμένη στα δεδομένα (data centric)	Από άκρο σε άκρο κατεύθυνση προσανατολισμένη στη διεύθυνση (address centric)
Φύση αίτησης	Βασισμένη στην κατάσταση(attribute based)	Βασισμένη στον κόμβο
Μετάδοση αιτήσεων	Πολύ-εκπομπή (broadcast)	Πολύ-εκπομπή ή hop by hop
Διευθυνσιοδότηση	Έλλειψη γενικού identification	Χρήση γενικού identification (global id)
Ενεργό Duty cycle	Χαμηλό, έως και 1%	Υψηλό

Πίνακας 1.1: Διαφοροποίηση των WSN από τα ad hoc δίκτυα

1.3 Κατηγορίες ασύρματων δικτύων αισθητήρων

Τα ασύρματα δίκτυα ασθητήρων μπορούν να ταξινομηθούν σύμφωνα με τις απαιτήσεις του χώρου της εφαρμογής σε υπέργεια, υπόγεια, υποθαλάσσια, πολυμεσικά (multi media) και κινούμενα, όπου τα χαρακτηριστικά των οποίων συνοψίζονται στον Πίνακα 1.2.

	Ορισμός	Προκλήσεις	Εφαρμογές
Υπέργεια WSN	Το δίκτυο αποτελείται από εκατοντάδες ή χιλιάδες ασύρματους κόμβους τοποθετημένους στο έδαφος	In network συγκέντρωση δεομένων για βελτίωση της απόστασης στην επικοινωνία, στο ενεργειακό κόστος και την καθυστέρηση. Ελαχιστοποίηση ενεργειακού κόστους. Μείωση της ποσότητας των δεδομένων επικοινωνίας. Εύρεση βέλτιστης διαδρομής. Κατανομή ενεργειακής κατανάλωσεις. Περιορισμός πλεονασμού. Ακριβή εφαρμογή, συντήρηση υψηλό κόστος εξοπλισμού.	Αίσθηση και επίβλεψη περιβάλλοντος. Βιομηχανική επίβλεψη. Εξερευνήσεις επιφάνειας.
Υπόγεια WSN	Το δίκτυο από ασύρματους κόμβους τοποθετημένους υπόγεια, ή σε σπηλιές, ορυχεία.	Απειλές για τις συσκευές (περιβάλλον ζώα). Οι μπαταρίες δεν μπορούν εύκολα να αντικατασταθούν. Προκλήσεις τοπολγίας σε περίπτωση προσχεδιασμένης εφαρμογής. Υψηλά επίπεδα εξασθένησης και απώλειας σήματος.	Επίβλεψη στη γεωργία. Υπόγεια δομική επίβλεψη. Υπόγεια επίβλεψη εδάφους, ορυκτών ή υδάτων. Επίβλεψη στρατιωτικών συνόρων.
Υποθαλάσσια WSN	Το δίκτυο από ασύρματους κόμβους τοποθετημένους στο περιβάλλον του ωκεανού	Ακριβοί υποθαλάσσιοι αισθητήρες. Αστοχία του υλικού λόγω περιβαλλοντικών παραγόντων (π.χ. διάβρωση). Οι μπαταρίες δε μπορούν εύκολα να αντικατασταθούν. Αραιή κατανομή κόμβων. Περιορισμένο εύρος ζώνης. Μεγάλη καθυστέρηση διάδοσης, φαινόμενα εξασθένησης του σήματος.	Παρατήρηση περιβαλλοντικής μόλυνσης. Υποθαλάσσια εξερεύνηση και επιτήρηση. Παρατήρηση σεισμικής δραστηριότητας. Επιτήρηση εξοπλισμού. Υποθαλάσσια ρομποτική.
Multimedia WSN	Το δίκτυο από ασύρματους κόμβους ικανούς να επεξεργάζονται, να αποθηκεύουν και να εξάγουν δεδομένα (βίντεο, εικόνα, ήχο)	In network επεξεργασία φιλτράρισμα και συμπίεση multi-media περιεχομένου. Υψηλή κατανάλωση ενέργειας και υψηλές απαιτήσεις εύρους ζώνης. Ευέλικτη αρχιτεκτονική για την υποστήριξη ποικίλων εφαρμογών. Απαιτήτε ενσωμάτωση ποικίλων ασύρματων τεχνολογιών. Δύσκολη διασφάλιση QoS λόγω της χωρητικότητας της	Ενίσχυση στις υπάρχουσες εφαρμογές όπως επίβλεψη και εντοπισμός.

		ζεύξης και των καθυστερήσεων. Αποτελεσματικός cross-layer σχεδιασμός. Καθοδήγηση και έλεγχος κινούμενων κόμβων. Απαίτηση αυτό-οργάνωσης. Συνδιασμός localization και κινητικότητας.	
Κινούμενα WSN	Το δίκτυο από κινούμενους ασύρματους κόμβους	Ελαχιστοποίηση ενεργειακής κατανάλωσης. Διατήρηση συνδεσιμότητας δικτύου. In network επεξεργασία δεδομένων. Διαχείρηση κινητικότητας. Διατήρηση επαρκούς sensing κάλυψης.	Επίβλεψη περιβαλλοντικών συνθηκών. Παρακολούθηση σε στρατιωτικές εφαρμογές. Ανίχνευση στόχων. Αναζήτηση και διάσωση.

Πίνακας 1.2: Ταξινόμηση των WSN βάση των εφαρμογών που υποστηρίζουν

Τα ασύρματα δίκτυα μπορούν να ταξινομηθούν βάση γενικότερων κριτηρίων (Πίνακας 1.3):

- Σε σχέση με την απόσταση των κόμβων από το σταθμό βάσης, τα ασύρματα δίκτυα αισθητήρων διακρίνονται σε συστήματα επικοινωνίας μονού άλματος (single-hop) ή πολλαπλών αλμάτων (multi-hop). Η πρώτη περίπτωση είναι κατάλληλη για μικρές περιοχές και όλοι οι κόμβοι αποστέλλουν τα δεδομένα απευθείας στο σταθμό βάσης. Το δίκτυο έχει απλούστερη δομή ενώ μπορούν να επιτευχθούν μεγαλύτρα επίπεδα ασφάλειας. Σε εφαρμογές όπου η περιοχή κάλυψης είναι μεγάλη η επικοινωνία πολλαπλών αλμάτων είναι μονόδρομος. Οι κόμβοι μεταδίδουν τα δεδομένα τους στο σταθμό βάσης μέσω ενδιάμεσων κόμβων οι οποίοι εκτελούν τη λειτουργία της δρομολόγησης αλλά και της συγκέντρωσης δεδομένων.
- Σε σχέση με το πόσο πυκνά τοποθετημένοι είναι οι κόμβοι και την επεξεργασία που υπόκεινται τα δεδομένα στους κόμβους, μπορούμε να κατηγοριοποιήσουμε τα ασύρματα δίκτυα αισθητήρων σε aggregating και nonaggregating. Στα δίκτυα της δεύτεης κατηγορίας οι κόμβοι αποστέλλουν τα δεδομένα τους στον προορισμό χωρίς να τα επεξεργαστούν. Η τακτική αυτή οδηγεί σε χαμηλό υπολογιστικό φόρτο στους ενδιάμεσους κόμβους και υψηλή ακρίβεια στο δίκτυο. Ωστόσο, σε μεγαλύτερα δίκτυα η αυξημένη κίνηση ενδέχεται να επιφέρει συγκρούσεις δεδομένων και καθυστέρηση στο δίκτυο. Τα συγκεκριμένα συστήματα είναι κατάλληλα για δίκτυα με χαμηλή πυκνότητα κόμβων στα οποία απαιτείται υψηλή ακρίβεια από τους χρήστες. Από την άλλη πλευρά, σε δίκτυα με πυκνή κατανομή, κάθε κόμβος βρίσκεται συνήθως πλησιέστερα στους γειτονικούς του, με αποτέλεσμα τη δημιουργία πλεονασμού δεδομένων. Απαιτήτε υλοποίηση συνεργατικών λειτουργιών συγκέντρωσης και αποστολής δεδομένων για τον περιορισμό του φαινομένου αυτού. Με τον τρόπο αυτό μειώνεται η συμφόρηση του δικτύου και εξοικονομείται ενέργεια, ενώ παράλληλα αυξάνονται οι εκτελούμενοι υπολογισμοί, αυξάνοντας τις απαιτήσεις μνήμης. Ενδείκνυται

κατά συνέπεια αυτή η κατηγορία για ασύρματα δίκτυα αισθητήρων μεγάλης κλίμακας, με πυκνή τοποθέτηση κόμβων.

- Σε σχέση με τον συνδιασμό του δικτύου μπορούν να διακριθούν σε ντετερμινιστικά ή δυναμικά. Στα ντετερμινιστικά συστήματα η θέση των κόμβων είναι σταθερή ή προσχεδιασμένη, με αποτέλεσμα απλούστερο έλεγχο και εφαρμογή του συστήματος. Ωστόσο, σε πολλές περιπτώσεις η θέση των κόμβων είναι άγνωστη. Συνεπώς, οι κόμβοι οφείλουν να λειτουργούν με δυναμικό και κατανεμημένο τρόπο, που παρέχει μεγαλύτερη ευελιξία και επεκτασιμότητα, αλλά απαιτεί πολυπλοκότερους αλγορίθμους ελέγχου.
- Σε σχέση με την προσέγγιση του ελέγχου, τα ασύρματα δίκτυα αισθητήρων ταξινομούνται σε αυτοπροσδιορίσιμα και μη.

Παράγοντες ταξινόμησης	Κατηγορίες WSN
Απόσταση από το σταθμό βάσης/κέντρο επεξεργασίας	Single hop or Multi hop
Εξάρτηση δεδομένων	Aggregating or non aggregating
Κατανομή κόμβων	Ντετερμινιστικά ή δυναμικά
Προσέγγιση ελέγχου	Non self-configurable or self configurable
Εφαρμογή	Πολυάριθμες κατηγορίες

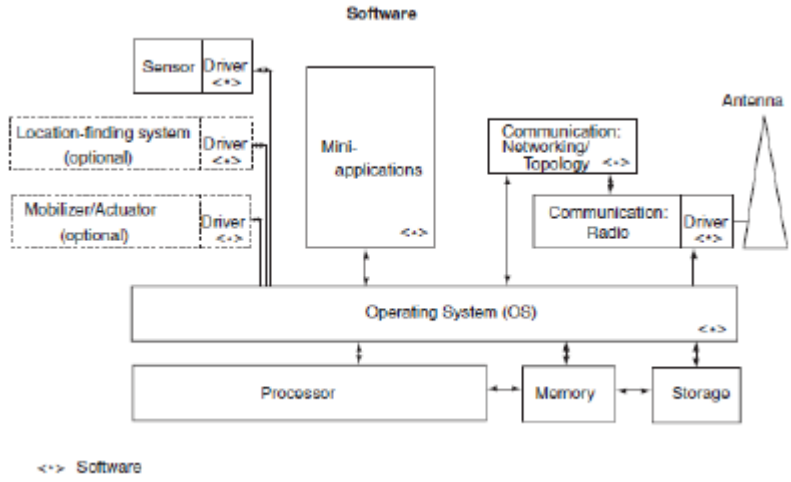
Πίνακας 1.3: Γενικότερα κριτήρια ταξινόμησης WSN

1.4 Βασικά χαρακτηριστικά ασύρματων δικτύων αισθητήρων

1.4.1 Αρχιτεκτονική ασύρματου κόμβου

Η συνήθης αρχιτεκτονική λογισμικού ενός κόμβου ασύρματου δικτύου αισθητήρων περιλαμβάνει τα εξής υποσυστήματα(Εικόνα 1.2):

i. Κώδικας λειτουργικού συστήματος (middleware). Το λειτουργικό σύστημα αποτελεί ένα περιβάλλον επικοινωνίας λογισμικού και επιπέδου μηχανής του μικροεπεξεργαστή σχεδιασμένο με προτεραιότητα την εξοικονόμηση πόρων. Η χρήση ανοιχτού κώδικα λογισμικών, σχεδιασμένων για ασύρματα δίκτυα αισθητήρων, τα οποία συνήθως χρησιμοποιούν αρχιτεκτονική που επιτρέπει ταχεία εφαρμογή και ελαχιστοποίηση του μεγέθους του κώδικα είναι μια προτεινόμενη λύση.
ii. Οδηγοί (drivers) αισθητήρων: είναι τμήματα λογισμικού τα οποία διαχειρίζονται τις βασικές λειτουργίες των πομποδεκτών των κόμβων.
iii. Επεξεργαστές επικοινωνίας: είναι υπεύθυνοι για τις λειτουργίες επικοινωνίας, όπως δρομολόγηση, ενταμίευση και προώθηση πακέτων, διατήρηση της τοπολγίας και έλεγχος πρόσβασης στο μέσο, κρυπτογράφηση (encryption) και Forward Error Correction (FEC).
iv. Οδηγοί (drivers) επικοινωνίας: είναι τμήματα λογισμικού τα οποία βοηθούν στην κωδικοποίηση στο φυσικό επίπεδο, διαχειρίζονται τις οδηγίες που αφορούν το μέσο μετάδοσης, συμπεριλαμβανομένου του χρονισμού και συγχρονισμού, την κωδικοποίηση σήματος και τη διαμόρφωση
v. Εφαρμογές επεξεργασίας δεδομένων: είναι βασικές εφαρμογές, συνήθως μικρού μεγέθους, για την επεξεργασία δεδομένων εντός δικτύου (in-network) στον κόμβο.



Εικόνα 1.2: Βασική αρχιτεκτονική λογισμικού ασύρματου κόμβου

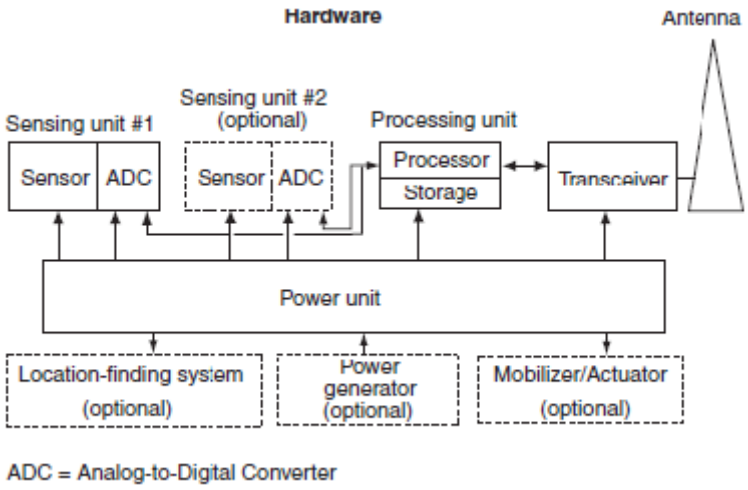
Η βασική αρχιτεκτονική υλικού ενός κόμβου ασύρματου δικτύου αισθητήρων περιλαμβάνει τα παρακάτω υποσυστήματα (Εικόνα 1.3):

i. Υποσύστημα αισθήτηρων: παρέχει τη διεπαφή (interface) για τη μετατροπή των σημάτων από το φυσικό περιβάλλον σε ηλεκτρικά σήματα κατάλληλα για επεξεργασία από ηλεκτρονικές συσκευές. Έτσι οι αισθητήρες μετατρέπουν φυσικά μεγέθη σε ηλεκτρικά σήματα.

ii. Υποσύστημα επεξεργασίας: είναι η μονάδα επεξεργασίας των δεδομένων. Οι σύγχρονοι μικροελεγκτές που απαρτίζουν τη μονάδα αυτή αποτελούνται από μνήμες τύπου flash και RAM, μετατροπείς αναλογικού σήματος σε ψηφιακό (A/D converters) και ψηφιακά I/O σε ένα ολοκληρωμένο κύκλωμα χαμηλού κόστους. Η επιλογή του ελεγκτή βασίζεται σε παράγοντες όπως η κατανάλωση ενέργειας, οι απαιτήσεις σε τάση λειτουργίας, το κόστος, η υποστήριξη περιφερειακών, ο χρόνος αφύπνισης και η ταχύτητά του.

iii. Υποσύστημα επικοινωνιών: αποτελείται από τον πομπό και τον δέκτη. Στη μονάδα αυτή γίνεται η μεγαλύτερη κατανάλωση ενέργειας του συστήματος, επηρεάζοντας την απόδοση του κόμβου αλλά και τη συνολική απόδοση του δικτύου.

iv. Υποσύστημα τροφοδοσίας: αποτελείται συνήθως από κάποιοα μπαταρία ή από κάποια μονάδα μετατροπής ηλιακής, αιολικής ενέργειας. Παρέχει την απαιτούμενη ενέργεια στον κόμβο ενώ η αντικατάσταση ή η φόρτιση της μονάδας αυτή ςσυνήθως δεν είναι εύκολη. Για τον λόγο αυτό η φιλσοφία των ασύρματων δικτύων αισθητήρων στρέφεται στην μέγιστη εξοικονόμηση ενέργειας.



Εικόνα 1.3: Βασική hardware αρχιτεκτονική ασύρματου κόμβου

1.4.2 Δυνατότητα αίσθησης

Η εφαρμογή που καλύμαστε να υλοποιήσουμε θέτει τις απαιτήσεις στον τρόπο με τον οποίο ο αισθητήρας του κόμβου θα πάρει μετρήσεις από την περιοχή επίβλεψης. Ωστόσο ο σχεδιαστής της εφαρμογής πρέπει να έχει υπόψη του τις παρακάτω γενικές λειτουργίες που μπορεί να εκτελέσει ένας κόμβος:

- Μέτρηση ενός φυσικού μεγέθους όπως θερμοκρασία, ατμοσφαιρική πίεση, ποσότητα φωτός, σχετική υγρασία κ.α σε μία δεδομένη τοποθεσία.
- Αντίληψη γεγονότων και εκτίμηση παραμέτρων τους όπως ανίχνευση διέλευσης ενός οχήματος και εκτίμηση της ταχύτητας και κατεύθυνσής του.
- Ανίχνευση αντικειμένου και ταυτοποίηση του όπως ανίχνευση εισβολής στην παρατηρούμενη από το δίκτυο περιοχή και παθανότατα κατηγοριοποίηση αντικειμένου.

Τα ασύρματα δίκτυα αισθητήρων μπορούν να καταταχθούν ανάλογα με τον τρόπο που συλέγουν και αποστέλουν δεδομένα σε:

- Συνεχή: όταν οι κόμβοι συλλέγουν συνεχώς δεδομένα από το περιβάλλον.
- Αντιδραστικά (reactive): όταν οι κόμβοι συλλέγουν και αποστέλλουν δεδομένα έπειτα από ανάλογο σήμα που θα πάρουν από τον συντονιστή του δικτύου ή έπειτα από κάποια μεταβολή στον περιβάλλοντα χώρο για την οποία υπάρχει οδηγία αντίδρασης στο λογισμικό του κόμβου.
- Περιοδικά: όταν οι κόμβοι συλλέγουν δεδομένα κατά περιοδικά χρονικά διαστήματα τα οποία ορίζονται στο λογισμικό της εφαρμογής.

Τα συστήματα τα οποία ενσωματώνουν έναν αριθμό από τις παραπάνω λειτουργίες ονομάζονται υβριδικά. Ανάλογα με τη δυνατότητα αίσθησης των αισθητήρων μπορούν να ταξινομηθούν σε παθητικές συσκευές (μέτρηση σεισμικών δονήσεων, υγρασία, θερμοκρασίας, ακουστικών κυμάτων), συνήθως χαμηλής ενέργειας, ή ενεργητικές (ρανταρ, σόναρ), που τείνουν να είναι υψηλής ενέργειας συστήματα.

Ο ορισμός της αίσθησης μπορεί να αναλυθεί σε όρους όπως η έκθεση (exposure) (ο χρόνος έκθεσης σε συνδιασμό με την απόσταση του κόμβου από την παρατήρηση φαινόμενο), η προσαρμογή (calibration) και η κάλυψη (sensing coverage). Οι έρευνες που γίνονται στο χώρο των ασύρματων δικτύων αισθητήρων επικεντρώνονται στην εξοικονόμηση ενέργειας σε συνάρτηση με τον χώρο κάλυψης, είτε με εύρεση του

ελάχιστου αριθμού ενεργών κόμβων για την κάλυψη μιας περιοχής, είτε με προτάσεις τοποθέτησης των κόμβων για κατανενημένη ανίχνευση σε μεγάλης κλίμακας ασύρματα δίκτυα αισθητήρων. Η συνεχής ενεργή κατάσταση των κόμβων είναι συνήθως μη αποδωτική, ανάλογα πάντα με τις απαιτήσεις που θέτει η κάθε εφαρμογή.είναι αποδεκτό και συνηθίζεται να υπάρχουν πλεονασματικοί κόμβοι (redundancy), δηλαδή επικαλύψεις στην περιοχή εποπτείας ώστε να επιτυχαίνεται μεγαλύτερη ακρίβεια.

1.4.3 Δυνατότητα επεξεργασίας δεδομένων

Η μονάδα επεξεργασίας δεδομένων ενός ασύρματου κόμβου αποτελείται από την μνήμη και τον επεξεργαστή, ο οποίος είναι προγραμματιζόμενος και εκτελεί βασικούς υπολογισμούς επεξεργασίας σήματος και πιθανότατα διεργασίες συσχέτισης δεδομένων. Ο σχεδιασμός αυτής της μονάδας είναι προσανατολισμένος σε λύσεις όπου το κόστος και η κατανάλωση ενέργειας θα κρατηθούν χαμηλά. Επεξεργασίες δεδομένων που πιθανόν να απαιτηθούν από την εφαρμογή είναι η συγχώνευση δεδομένων (data fusion): ένα ή περισσότερα πακέτα που έχουν ληφθεί συνδιάζονται για την δημιουργία ενός μεγαλύτερου πακέτου με σκοπό την εξοικονόμηση ενέργειας, η συμπίεση δεδομένων και η επεξεργασία κώδικα ασφάλειας.

Η επεξεργασία δεδομένων μπορεί να υλοποιηθή από κάθε κόμβο χωριστά ή μ εσυνεργασία των κόμβων προσεγγίζοντας κατανεμημέν συστήματα. Στην πρώτη περίπτωση οι κόμβοι διεξάγουν υπολογισμούς τοπικά και αποστέλλουν ένα υποσύνολο των διατιθέμμενων δεδομένων ή/και των επεξεργασμένων πληροφοριών, ενώ στη δεύτερη η επεξεργασία υλοποιείται σε διαδοχικά επίπεδα, έως ότου η πληροφορία που αφορά τα γεγονότα εωδιαφέροντος καταφθάσει στο σημείο διαχείρισης.

1.4.4 Δυνατότητα επικοινωνίας

Η επικοινωνία σε ένα ασύρματο δίκτυο αισθητήρων μπορεί να χωριστεί σε επικοινωνία υποδομής και επικοινωνία εφαρμογών. Η επικοινωνία υποδομής είναι η επικοινωνία που πραγματοποιείται για τον καθορισμό, την διατήρηση και την βελτιστοποίηση της λειτουργίας του δικτύου, του οποίου η τοπολογία πιθανόν να μεταβάλλεται συχνά. Σε ένα στατικό δίκτυο αισθήτηρων απαιτείται μια αρχική προεργασία για τη δημιουργία του δικτύου ενώ αργότερα η επικοινωνία υποδομής είναι απαραίτητη μόνο για τον επαναπροσδιορισμού του. Στα δίκτυα που περιλαμβάνουν κινούμενους κόμβους, είναι απαραίτητη η επικοινωνία υποδομής για την εύρεση των διαδρομών επικοινωνίας και τον επαναπροσδιορισμό του δικτύου.

Σε ένα δίκτυο ασύρματων αισθητήρων διακρίνονται οι εξής μορφές επικοινωνίας (Εικόνα 1.4):

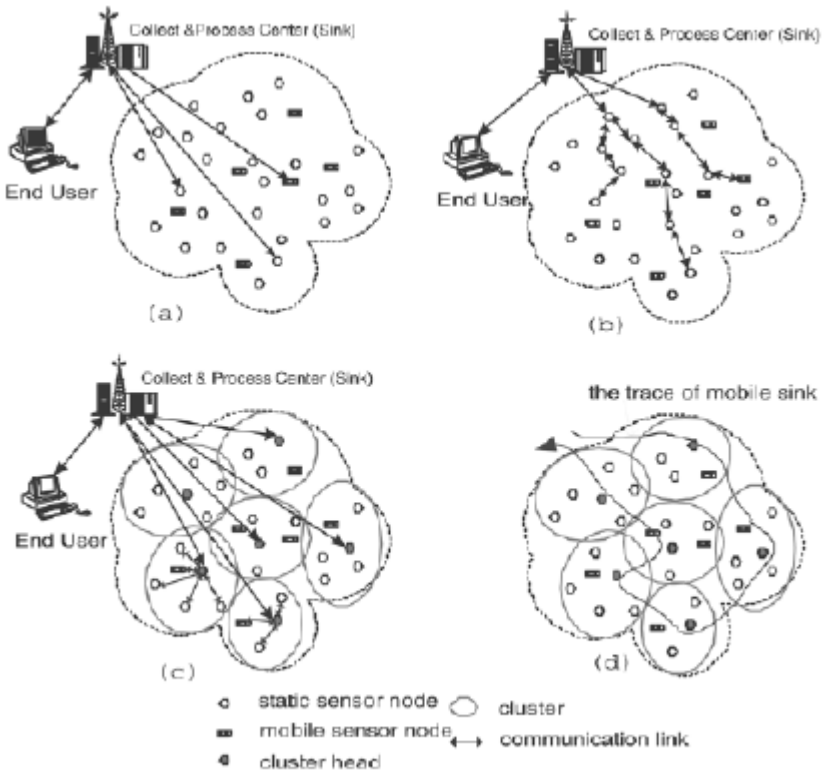
- Άμεση σύνδεση (direct connected WSN): είναι η άμεση επικοινωνία του κάθε κόμβου με το δέκτη δεδομένων (data link). Λόγω του μεγάλου αριθμού κόμβων και του πιθανότατα περιορισμένου εύρους μετάδοσης κάθε κόμβου εξαιτίας ενεργειακών περιορισμών, είναι γενικά ασύμφορη, εώς και αδύνατη. Συνεπώς αυτή η μορφή επικοινωνίας δεν εδεικνύεται για ασύρματα δίκτυα αισθητήρων ευρείας κλίμακας.
- Peer to peer πολλαπλών αλμάτων (multi-hop) επικοινωνία: η επικοινωνία πολλαπλών αλμάτων σε μικρές αποστάσεις οδηγεί σε μικρότερη

κατανάλωση ενέργειας, σε σχέση με μια αντίστοιχη μεγάλων αλμάτων (large-hop) μετάδοση μεταξύ ενός ζεύγους αποστολέα παραλήπτη.

- Επίπεδη ad hoc multi-hop επικοινωνία: στην επικοινωνία αυτού του τύπου κάποιοι κόμβοι έχουν την αρμοδιότητα δρομολόγησης πακέτων, εκτός από την αίσθηση και αποστολής των δικών του δεδομένων. Η μορφή αυτή παρέχει εξοικονόμηση ενέργειας στην επικοινωνία, όμως οι κόμβοι που βρίσκονται πιο κοντά στο δέκτη δεδομένων (data sink) είναι υπεύθυνοι για τη δρομολόγηση προς αυτόν, των πακέτων των υπόλοιπων κόμβων, με αποτέλεσμα, την ανομοιόμορφη κατανάλωση της ενέργειάς τους σε σχέση με τους υπόλοιπους κόμβους.
- Συστάδες πολλαπλών αλμάτων (cluster based multi-hop) επικοινωνία: η μορφή της επικοινωνίας αυτού του τύπου βασίζεται σε συστάδες που συνθέτουν οι κόμβοι και ορίζονται σύμφωνα με κανόνες ένας επικεφαλής για κάθε συστάδα. Εκτός από τις συστάδες ενός επιπέδου, υπάρχουν και σχήματα επικοινωνίας τα οποία βασίζονται σε συστάδες οργανωμένες κατά ιεραρχία. Όπου οι επικεφαλείς συστάδων (cluster heads) χαμηλότερου επιπέδου επικοινωνούν με τους επικεφαλείς συστάδων υψηλότερου επιπέδου. Η συγχώνευση δεδομένων (data fusion) τοπικά στους επικεφαλείς συστάδων μειώνει τον όγκο της αποστελλόμενης πληροφορίας στο δέκτη δεδομένων (data sink) με επακόλουθη μείωση της καταναλισκόμενης ενέργειας. Μειονέκτημα του σχήματος είναι ότι όγκος των δεδομένων επιβαρύνει τους επικεφαλείς συστάδων, με αποτέλεσμα την ασύμμετρη μείωση των ενεργειακών τους αποθεμάτων σε σχέση με τους υπόλοιπους κόμβους και τον αυξημένο φόρτο στους επικεφαλείς συστάδων ανώτερων επιπέδων.

Τα ασύρματα δίκτυα αισθητήρων ταξινομούνται βάση του τρόπου αποστολής δεδομένων ως εξής:

- Συνεχή: στα δίκτυα αυτά οι κόμβοι συλλέγουν και αποστέλλουν αδιαλείπτως δεδομένα προς τον δέκτη δεδομένων (data sink).
- Κατ' αίτηση (on demand): οι κόμβοι αποστέλλουν δεδομένα έπειτα από ανάλογο σήμα που θα λάβουν από τον συντονιστή στου δικτύου.
- Καθοδηγούμενα από γεγονότα: οι κόμβοι αποστέλλουν δεδομένα αφού συμβεί κάποια μεταβολή στον περιβάλλοντα χώρο.
- Προγραμματισμένα: οι κόμβοι αποστέλουν δεδομένα βάση συνθηκών προκαθορισμένων στο λογισμικό της εφαρμογής.



Ε**ικόνα 1.4:** Μορφές επικοινωνίας WSN

1.4.5 Συντήρηση

Ο όρος αυτός αναφέρεται στα ασύρματα δίκτυα αισθητήρων τα οποία μπορούν να εκτελέσουν λειτουργίες όπως ο αυτοπρποσδιορισμού, η αυτοπροστασίας και η επαναφοράς χωρίς να απαιτείται ουσιαστηκή συμετοχή του ανθρώπινου παράγοντα. Η διαδικασία συντήρησης αφορά την ανίχνευση αποτυχιών ή την μείωση της απόδοσης του δικτύου, καθώς και τις διαδικασίες διάγνωσης και απανόρθωσης. Η ανίχνευση αλλαγών στην κατάσταση του δικτύου παρέχει ευελιξία, σθεναρότητα, ανεξαρτησία και δυνατότητα βελτιστοποίησης της συμπεριφοράς του δικτύου.
Διακρύνουμε τους εξής τύπους συντήρησης:

- Corrective: το δίκτυο επανορθώνει τις αποτυχίες
- Adaptive: το δίκτυο προσαρμόζεται στις μεταβολές
- Preventive: το δίκτυο μαθαίνει να αναμένει την επίδραση των αλλαγών
- Proactive: το δίκτυο μαθαίνει να επεμβαίνει ώστε να προλαμβάνει τις αποτυχίες

Ένα παράδειγμα συντήρησης στα ασύρματα δίκτυα αισθητήρων αφορά την πυκνότητα των κόμβων του δικτύου. Σε περίπτωση που δεν απαιτείται υψηλή πυκνότητα των κόμβων μπορεί να πραγματοποιηθεί παροδική απενεργοποίηση ορισμένων κόμβων.

1.4.6 Localization

Τα ασύρματα δίκτυα αισθητήρων μπορούν να ταξινομηθούν σε δομημένα ή μη με κριτήριο αν υπήρξε προσχεδιασμένη ή όχι τοποθέτηση των κόμβων. Συνήθως ένα μη

δομημένο ασύρματο δίκτυο αισθητήρων αποτελείται από ένα πυκνό σύνολο κόμβων, οι οποίοι είναι τυχαία τοποθετημένοι στον χώρο επίβλεψης. Αφού εγκατασταθεί το δίκτυο εκτελεί τις λειτουργίες της επιτήρησης και της αναφοράς δεδομένων χωρίς καμία παρέμβαση. Σε ένα δομημένο ασύρματο δίκτυο αισθητήρων, το σύνολο των κόμβων ή μόνο κάποιοι από αυτούς τοποθετούνται με προσχεδιασμένο τρόπο. Τα δομημένα δίκτυα έχουν πλεονέκτημα στην ευκολία συντήρησης στο κόστος διαχείρισης, καθώς επίσης χρειάζονται λιγότεροι κόμβοι σε συγκεκριμένες θέσεις για την κάλυψη μιας περιοχής. Αντίθετα με την τυχαία τοποθέτηση των κόμβων μπορεί να μείνουν ακάλυπτες περιοχές ή να υπάρξουν πλεονασματικοί κόμβοι. Το πρόβλημα καθορισμού του σημείου τοποθέτησης των κόμβων ονομάζεται localization. Μέθοδοι για την επίλυση του προβλήματος είναι το σύστημα GPS, οι beacon κόμβοι, localization βάσει εγγύτητας αλλά και κάποιοι αλγόριθμοι.

1.4.7 Συγχρονισμός

Για να υπάρξη υποστήριξη σε χρονικά συσχετισμένα δεδομένα στο δίκτυο από τους διαφορετικούς κόμβους του, απαιτείται η ύπαρξη μιας μεθόδου συντονισμού που θα παρέχει μεγάλη ακρίβεια. Υπάρχουν αρκετές μέθοδοι άμεσου ή έμμεσου συγχρονισμού. Πιθανά σφάλματα στον χρονισμό των κόμβων κάνουν αναξιόπιστο το συσχετισμό των δεδομένων, προσβάλλοντας έτσι και τη συνολική αξιοπιστία του δικτύου.

1.4.8 Ασφάλεια

Η ύπαρξη ασφάλειας στα ασύρματα δίκτυα αισθητήρων επιβαρύνει τους κόμβους με την εκτέλεση πολύπλοκων αλγορίθμων αυθεντικοποίησης και κρυπτογράφησης. Λόγω της ευκολίας υποκλοπής και παρεμβολών του ασύρματου καναλιού ματάδοσης, για να παραμείνουν τα δεδομένα αναλλίωτα πρέπει να κρυπτογραφείτε κάθε εκπομπή, αλλά και να γίνει πρόβλεψη κατά την κατασκευή και τοποθέτηση των κόμβων ώστε να εξασφαλίζουν αντοχή στη φυσική παραβίαση (tamper resilience).

Η χρήση τεχνικών αυθεντικοποίησης και κρυπτογράφησης επιδρούν αρνητικά τόσο στην κατανάλωση ισχύος όσο και στο διαθέσιμο εύρος ζώνης του δικτύου ενώ, η ενσωμάτωση επιπλέων bit στα μεταφερόμενα πακέτα, τα οποία περιέχουν τις πληροφορίες αυθεντικότητας, μειώνουν τον αριθμό των πραγματικών δειγμάτων που μπορούν να μεταφερθούν από ένα κόμβο.

1.4.9 Σχεδιαστικοί περιορισμοί

Κατά την σχεδίαση των ασύρματων κόμβων πρέπει να ληφθούν υπόψη ορισμένοι περιορισμοί που απορρέουν από τις ιδιαιτερότητες των ασύρματων δικτύων αισθητήρων. Τα σχεδιαστηκά αυτά ζητήματα περιγράφονται παρακάτω:

- Περιορισμένοι πόροι (υπολογιστική ισχύς, μνήμη, ενέργεια,εύρος ζώνης): συνήθως οι κόμβοι τοποθετούνται σε περιοχές όπου είναι δύσκολη η πρόσβαση τους, με αποτέλεσμα να είναι δύσκολη και η αντικατάσταση της πηγής ενέργειας. Οπότε ο χρόνος ζωής του κάθε κόμβου συνήθως καθορίζεται από τη ζωή της μπαταρίας του. Η ενέργεια του κόμβου καταναλώνεται κυρίως κατά την αποστολή και λήψη δεδομένων με αποτέλεσμα να απαιτήται χρήση πρωτοκόλλων εξοικονόμησης ενέργειας για την επέκταση της ζωής του συστήματος. Επιπλέον, αλγόριθμοι χαμηλής

πολυπλοκότητας οδηγούν στη μείωση του υπολογιστικού χρόνου και της κατανάλισκόμενης ισχύος. Επίσης αποδοτικές τεχνικές στον καθορισμό του εύρους ζώνης επιταχύνουν την παράδοση των δεδομένων.

- Δυναμική τοπολογία και περιβάλλον λειτουργίας: σε ένα ασύρματο δίκτυο αισθητήρων η τοπολογία του ενδέχεται να μεταβάλλεται, λόγω της αναξιοπιστίας κάποιων κόμβων του, ένας κόμβος μπορεί να παρουσιάσει σφάλματα ή και να σταματήσει να λειτουργεί, χωρίς να ενημερώσει τους υπόλοιπους κόμβους, λόγω εξάντλησης της ενέργειάς του. Επιπλέον, καινούργει κόμβοι είναι πιθανό να τοποθετηθούν στην περιοχή επίβλεψης. Επίσης το περιβάλλονόπου είναι τοποθετημένοι οι κόμβοι είναι ευμετάβλητο, γεγονός που μπορεί να προκαλέσει δυσλειτουργία των κόμβων ή αχρίστευση των ήδη συγκεντρωμένων πληροφοριών τους. Για την αντιμετώπιση αυτών των συνθηκών ενδείκνυται η υποστήριξη ευεληξίας και επεκτασιμότητας (flexibility scalability) μέσω της ομαδοποίησης (clustering) και της επικοινωνίας πολλαπλών αλμάτων (multi-hop).
- Πυκνή και τυχαία τοποθέτηση των κόμβων: τα ασύρματα δίκτυα αισθητήρων αποτελούνται από μεγάλο αριθμό κόμβων συνήθως τυχαία τοποθετημένων σε δυσπρόσιτες περιοχές. Για την εξοικονόμηση ενέργειας ο κάθε κόμβος δεν είναι σε μια συνεχήενεργή κατάσταση αλλά αναλλάσσει την λειτουργία του ανάλογα των απαιτήσεων μεταξύ ταν καταστάσεων off, sleep, idle, εκπομπής, λήψης και αστοχίας. Το δίκτυο πρέπει λοιπόν να δημιουργεί συνδέσεις αυτόνομα, ανεξαρτήτως της κατάστασης των κόμβων του. Επιπλέον ενδείκνυται η ανακατεύθυνση των πακέτων μέσω διαδρομών, στις οποίες οι κόμβοι διαφέτουν μεγαλύτερα αποθέματα ενέργειας, ώστε να επιτυγχάνεται η συμμετρική εξασθένηση ενέργειας του δικτύου. Όλα τα παραπάνω συνιστούν το λεγόμενο αυτοπροσδιορισμό του δικτύο (self configuration).
- Ad hoc αρχιτεκτονική και λειτουργία χωρίς ανθρώπινη παρέμβαση: η μη ύπαρξη δομής και η λειτουργία χωρίς την αωθρώπινη παρέμβαση απαιτεί από το δίκτυο να πραγματοποιεί συνδέσεις και να τις συντηρεί αυτόνομα.
- Πλεονασμός δεδομένων: η πυκνή τοποθέτηση των κόμβων οδηγεί σε φαινόμενα πλεονασμού δεδομένων. Για την αποφυγή διακίνησης επιπλέον όγκου δεδομένων από τους κόμβους απαιτείται η συνεργατική επεξεργασία των πληροφοριών, συγχώνευση δεδομένων (data fusion) και υπολογισμοί εντός του δικτύου αισθητήρων. Αντί για την άμεση αποστολή των δεδομένων προς τον δέκτη δεδομένων, ο κάθε κόμβος επεξεργάζεται μερικώς, με απλούς υπολγισμούς, τα δεδομένα και αποστέλλει μόνο τα αποτελέσματα.
- Ασύρματο μέσο επιρρεπές σε σφάλματα: πολλές φορές το περιβάλλον όπου τοποθετούνται οι κόμβοι έχει υψηλό θόρυβο, με αποτέλεσμα να παρουσιάζονται φαινόμενα εξασθένησης του σύματος, χαμηλή αξιοπιστία και QoS, αλλά και περιορισμένης ασφάλειας. Σε αυτούς του χώρους εφαρμογής απαιτείται η εξακρίβωση των δεδομένων σε κάθε επίπεδο του δικτύου και οι λειτουργίες συντήρησης.
- Ανάγκη ειδικών μηχανισμών δρομολόγησης και μετάδοσης δεδομένων: η ύπαρξη διαφορετικών αναγκών δρομολόγησης από τα παραδοσιακά δίκτυα απαιτεί διαφορετικά πρωτόκολλα και σχεδιασμό δικτύου. Μπορούμε να χωρίσουμε τις εξής κατηγορίες σχεδιασμού δικτύων: εστιασμένα στα δεδομένα (data centric), εστιασμένα στην ταυτότητα αλμάτων (cluster based), δομημένης τοποθέτησεις κόμβων (location based) και προσανατολισμένα στην παροχή εξασφαλισμένης ποιότητας επικοινωνίας (QoS oriented).

1.4.10 Κόστος Παραγωγής

Τα ασύρματα δίκτυα αισθητήρων αποτελούνται απί πολλούς κόμβους, με αποτέλεσμα το κόστος του κόμβου να επηράζει σημαντικά την διαμόρφωση του συνολικού κόστους του δικτύου. Πρέπει το κόστος του κάθε κόμβου να κρατηθεί χαμηλά ώστε το συνολικό κόστος του δικτύου, να είναι μικρότερο από το κόστος ενός συμβατικού δικτύου αντίστοιων δυνατοτήτων.

Ένας επιπλέον παράγοντας που επηρεάζει το τελικό κόστος είναι η ευκολία ανάπτυξης του δικτύου. Η ανάπτυξη του δικτύου, στο χώρο λειτουργίας του, πρέπει να είναι εφικτή και από μη εξειδικευμένο προσωπικό. Μια τέτοια δυνατότητα προϋποθέτει να έχει το δίκτυο την ικανότητα να αυτορυθμίζεται. Στην ιδεατή περίπτωση, το σύστημα θα πρέπει να είναι ικανό να ρυθμίζεται αυτόματα, ανεξάρτητα από την κατάσταση που επικρατεί στο περιβάλλον όπου τοποθετείται.

ΚΕΦΑΛΑΙΟ 2

Τα Πρότυπα της Οικογένειας του IEEE 802.15

2.1 Γενικά

Το πρότυπο IEEE 802.15 αποτελεί την 15 η ομάδα εργασίας του IEEE 802, η οποία επικεντρώνεται στα ασύρματα προσωπικά δίκτυα (WPANs) με περιοχή κάλυψης λιγότερη των 10 μέτρων και γι' αυτό αποτελούν την ιδανικότερη λύση για τη σχεδίαση WSNs . Το προσωπικό δίκτυο (PAN), το οποίο χρησιμοποιείται για τη διασύνδεση συσκευών που βρίσκονται σε μικρή απόσταση, μπορεί να είναι είτε ενσύρματο με υπολογιστικούς διαύλους είτε ασύρματο (WPAN).

Το πρότυπο επικοινωνίας για τα προσωπικά δίκτυα ή για τα ασύρματα δίκτυα μικρών αποστάσεων είναι το 802.15. Το IEEE 802.15 περιλαμβάνει πολλές διαφορετικές ομάδες διεργασιών, όπως το 802.15.1 για το Bluetooth, το 802.15.2 για τη συνύπαρξη του WPAN με άλλες ασύρματες συσκευές που λειτουργούν χωρίς άδεια, το 802.15.3 για υψηλού ρυθμού WPAN και το 802.15.4 για χαμηλού ρυθμού WPAN πάνω στο οποίο βασίζεται το ZigBee. Το ZigBee δεν είναι το IEEE 802.15.4 ούτε το IEEE 802.15.4 είναι το ZigBee, αλλά ένα πρωτόκολλο δικτύωσης που υποστηρίζεται αποκλειστικά από την ZigBee Alliance, και χρησιμοποιεί τις υπηρεσίες μεταφοράς δεδομένων που προδιαγράφονται στο IEEE 802.15.4.

Όλα τα επίπεδα δικτύου και εφαρμογών έρχονται να «πατήσουν» πάνω στο 802.15.4 πρωτόκολλο ή και άλλα πρωτόκολλα που ελέγχουν το φυσικό (PHY) επίπεδο και το υπο-επίπεδο Ελέγχου Προσπέλασης στο Μέσο Μετάδοσης (MAC-Medium Access Control) στην περιοχή των 2.4 GHz.
Μερικά από αυτά τα πρότυπα είναι:

▪ WirelessHart
Το πρότυπο WirelessHart παρέχει ένα πρωτόκολλο ασύρματης επικοινωνίας για μετρήσεις διεργασιών και εφαρμογές ελέγχου, στηρίζεται στο πρότυπο IEEE 802.15.4 για λειτουργία χαμηλής ισχύος στα 2.4 GHz και είναι συμβατό με όλες τις υπάρχουσες συσκευές, εργαλεία και συστήματα. Το πρότυπο αυτό διαθέτει αξιοπιστία, ασφάλεια και ενεργειακή αποδοτικότητα.

▪ ISA100
Το ISA100 είναι σχεδιασμένο για ασύρματη επίβλεψη χαμηλού ρυθμού και εφαρμογές διεργασιών αυτοματισμού. Επίσης, καθορίζει τα χαρακτηριστικά του OSI μοντέλου και της διαχείρισης της ασφάλειας και του συστήματος. Το πρότυπο αυτό επικεντρώνεται στη χαμηλή κατανάλωση ενέργειας, στη σθεναρότητα και τη συμβατότητα με άλλες συσκευές.

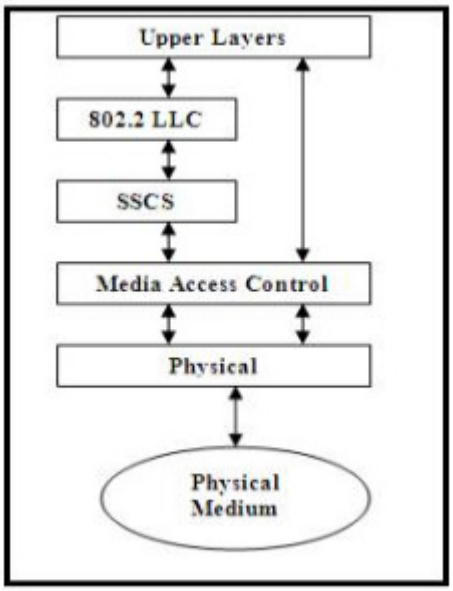
▪ **6LoWPAN**
Το 6LoWPAN επιτρέπει την IPv6 επικοινωνία πακέτων σε ένα IEEE 802.15.4. Ακόμη, το πρότυπο αυτό παρέχει όλα τα πλεονεκτήματα της IP επικοινωνίας και διαχείρισης. Χρησιμοποιείται ένα επίπεδο προσαρμογής δεδομένου ότι το μέγεθος των IP πακέτων είναι μεγαλύτερο από αυτό ενός IEEE 802.15.4 πλαισίου.

▪ **IEEE 802.150.3**
Το IEEE 802.150.3 αποτελεί ένα πρότυπο τόσο PHY επιπέδου όσο και MAC υπο-επιπέδου για δεδομένα υψηλού ρυθμού σε ένα WPAN. Υποστηρίζει την πραγματικού χρόνου ροή δεδομένων μουσικής και video. Επίσης, το πρότυπο αυτό λειτουργεί στα 2.4 GHz με ταχύτητες δεδομένων που κυμαίνονται από 11 έως 55 Mbps.

▪ **Wibree**
Το Wibree συνιστά ένα πρωτόκολλο ασύρματης τεχνολογίας επικοινωνίας με συσκευές χαμηλής κατανάλωσης ισχύος, μετάδοσης περιορισμένου βεληνεκούς και χαμηλού κόστους. Επιτρέπει την επικοινωνία μεταξύ μικρών συσκευών τροφοδοτούμενων με μπαταρία και συσκευών Bluetooth. Ακόμη, το πρότυπο αυτό λειτουργεί στα 2.4 GHz παρέχοντας ρυθμό δεδομένων 1 Mbps για αποστάσεις μεταξύ 5 και 10 m.

2.2 Πρότυπο IEEE 802.15.4

Το IEEE 802.15.4 είναι ένα πρότυπο που ορίζει το φυσικό επίπεδο και τον έλεγχο πρόσβασης μέσου (MAC) για ασύρματα προσωπικά δίκτυα μικρής εμβέλειας και χαμηλής ταχύτητας (LR-WPANs) που σχηματίζονται από σταθερές ή κινούμενες συσκευές, τροφοδοτούμενες από μπαταρίες ή κάποια άλλη πηγή περιορισμένης ενέργειας και ολοκληρώθηκε στις αρχές του 2003. Τα Low-Rate WPANs χαρακτηρίζονται από μικρό αριθμό καθηκόντων, χαμηλό κόστος, μεγάλη διάρκεια ζωής της μπαταρίας και υποστήριξη για μεγάλο αριθμό κόμβων. Η αρχιτεκτονική κάθε LR-WPAN (Low Rate – Wireless Personal Network), στην κατηγορία των οποίων ανήκουν και τα WSNs, κατηγοριοποιείται σε μία σειρά από επίπεδα (layers), τα οποία διευκολύνουν τη μελέτη και το σχεδιασμό του δικτύου και προτυποποιούνται από μία σειρά πρωτοκόλλων. Αποτελείται από το φυσικό επίπεδο, το οποίο περιλαμβάνει έναν πομποδέκτη για τις ράδιο-συχνότητες μαζί με κάποιους μηχανισμούς ελέγχου χαμηλού επιπέδου, και το επίπεδο MAC, το οποίο παρέχει μηχανισμούς πρόσβασης στο φυσικό κανάλι, όπως το CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) για πρόσβαση στο κανάλι μέσω του φυσικού μέσου. Η πρόσβαση στο υπο-επίπεδο MAC γίνεται μέσω του Logical Link Control (LLC) και του υπο-στρώματος σύγκλισης ειδίου ως προς την υπηρεσία (Specific Convergence Sublayer-SSCS). Κάθε επίπεδο επιτελεί συγκεκριμένες λειτουργίες και παρέχει υπηρεσίες μόνο στο υπερκείμενο επίπεδό του.

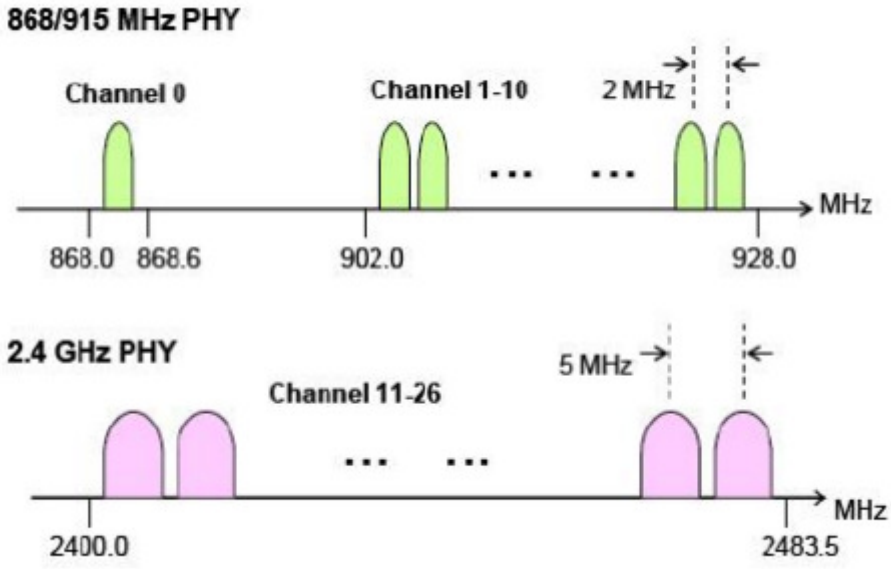


Εικόνα 2.1: Αρχιτεκτονική συσκευής ενός LR-WPAN

Αρχικά τα LR-WPANs σχηματίζονταν από κοντινές ζεύξεις έως και 75 m αλλά πλέον υπάρχει η δυνατότητα αύξησης της εμβέλειας της επικοινωνίας εις βάρος όμως του ρυθμού μετάδοσης των δεδομένων. Οι ασύρματες ζεύξεις υπό την επίβλεψη του προτύπου 802.15.4 μπορούν να λειτουργήσουν σε τρεις ISM (Industrial Scientific Medical) ζώνες συχνοτήτων με ρυθμούς δεδομένων:

· 250 Kbps στη ζώνη των 2.4 GHz με κωδικοποίηση O-QPSK
· 40 Kbps στη ζώνη των 915 MHz με κωδικοποίηση BPSK
· 20 Kbps στη ζώνη των 868 MHz με κωδικοποίηση BPSK

Στο πρωτόκολλο 802.15.4 εκχωρούνται συνολικά 27 κανάλια εκ των οποίων 16 κανάλια ανήκουν στη ζώνη των 2.4 GHz, 10 κανάλια στη ζώνη των 915 MHz και 1 κανάλι στη ζώνη των 868 MHz. Η ζώνη των 2.4 GHz αποτελεί την πιο διαδεδομένη ζώνη συχνοτήτων, που είναι και η κοινή ζώνη συχνοτήτων λειτουργίας με τα υπόλοιπα ασύρματα δίκτυα άρα και επικάλυψης. Σε αυτή τη ζώνη συχνοτήτων εκτελέστηκαν και οι πειραματικές μετρήσεις αυτής της εργασίας με Crossbow iris motes που χρησιμοποιούν αυτή την περιοχή συχνοτήτων.



Εικόνα 2.2: Τα κανάλια συχνοτήτων για το πρωτόκολλο 802.15.4

Η περιοχή κάλυψης δεν είναι αυστηρά καθορισμένη, καθώς τα χαρακτηριστικά διάδοσης είναι δυναμικά και μεταβαλλόμενα. Μικρές μεταβολές της θέσης και της κατεύθυνσης πιθανόν να έχουν άμεση επίπτωση στην ισχύ ή την ποιότητα του λαμβανόμενου σήματος. Οι αλλαγές αυτές προκύπτουν, είτε μια συσκευή είναι στατική είτε κινείται, εξαιτίας των κινούμενων αντικειμένων που παρεμβάλλονται και επιδρούν άμεσα στη ζεύξη μεταξύ πομπού και δέκτη. Το βασικότερο συστατικό των δικτύων που χρησιμοποιούν το πρότυπο 802.15.4 είναι η συσκευή ή κόμβος.

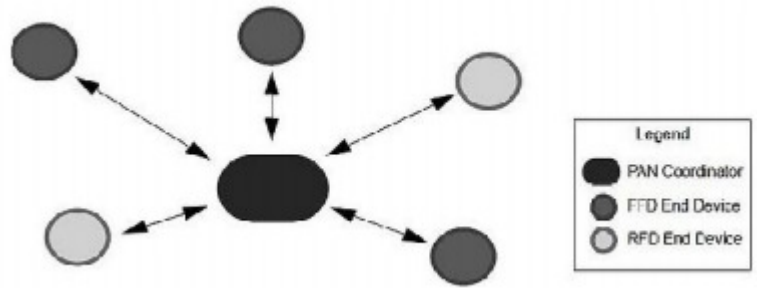
Υπάρχουν δύο είδη κόμβων:

- Συσκευή πλήρους λειτουργίας (Full-Function Device – FFD)
- Συσκευή μειωμένης λειτουργίας (Reduced-Function Device – RFD)

Το πρωτόκολλο IEEE 802.15.4 υποστηρίζει τρεις βασικές τοπολογίες:

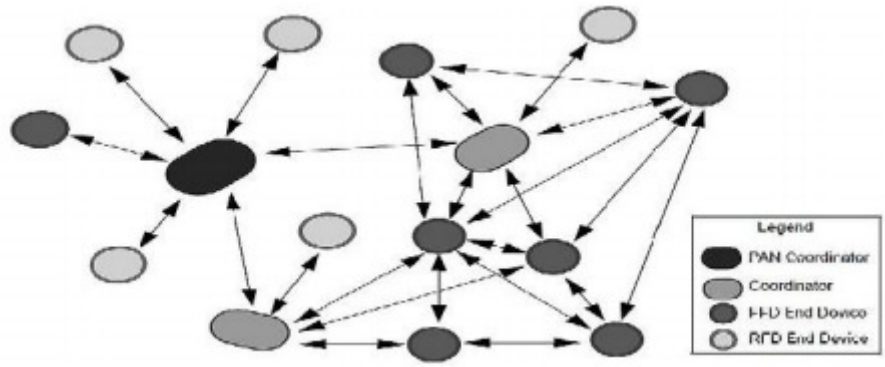
- Τοπολογία αστέρα

Στην τοπολογία αστέρα η συσκευή FFD, μετά την πρώτη ενεργοποίησή της, μπορεί να εγκαθιδρύσει το δίκτυό της και να λειτουργεί ως PAN coordinator. Με την επιλογή ενός PAN Identifier, που είναι μοναδικό για κάθε δίκτυο εντός της περιοχής εκπομπής, όλα τα δίκτυα αστέρα λειτουργούν ανεξάρτητα από τα υπόλοιπα δίκτυα αστέρα σε τρέχουσα λειτουργία.



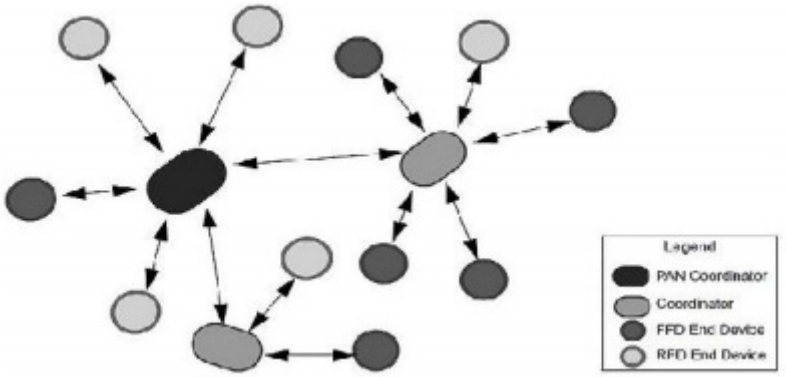
- Τοπολογία peer-to-peer (mesh)

Στην peer-to-peer τοπολογία κάθε συσκευή μπορεί να επικοινωνήσει με κάθε άλλη που βρίσκεται στην περιοχή εκπομπής της, καθώς και να εξαχθούν επιπρόσθετες τοπολογίες όπως η cluster tree μορφή. Μια συσκευή ορίζεται ως PAN coordinator, η οποία μπορεί να αποτελεί την πρώτη συσκευή που επικοινωνεί στο δίκτυο.



- Τοπολογία Cluster – tree

Η τοπολογία αυτή αποτελεί μία ειδική περίπτωση της τοπολογίας peer-to-peer. Οι περισσότερες συσκευές αυτής της τοπολογίας είναι συσκευές FFD, ενώ μία συσκευή RFD μπορεί να συνδεθεί μόνο όταν είναι στο τέλος της διακλάδωσης του cluster, αφού έχει τη δυνατότητα να επικοινωνήσει μόνο με μια συσκευή FFD κάθε φορά. Η κάθε συσκευή FFD έχει τη δυνατότητα να λειτουργήσει σαν συντονιστής και να παρέχει συγχρονισμό σε άλλες συσκευές καθώς και σε άλλους συντονιστές. Ως καθολικός PAN coordinator του δικτύου, ο οποίος καταναλώνει τους περισσότερους υπολογιστικούς πόρους από κάθε άλλη συσκευή, μπορεί να λειτουργήσει μόνο ένας συντονιστής. Ο PAN coordinator σχηματίζει την πρώτη ομάδα – cluster, της οποίας αποτελεί το cluster head –CLH της ομάδας με το cluster identifier – CID να λαμβάνει την τιμή 0, επιλέγει ένα αχρησιμοποίητο PAN identifier και μεταδίδει ευρέως ακολουθίες δεδομένων σε γειτονικές συσκευές. Μια συσκευή, που είναι υποψήφια για σύνδεση, όταν λάβει μια ακολουθία δεδομένων μπορεί να απαιτήσει να συνδεθεί στο δίκτυο μέσω του CLH και αν ο PAN coordinator της επιτρέψει, τότε θα προστεθεί η συσκευή ως child στη λίστα των γειτόνων του. Εν συνεχεία, η συσκευή αυτή θα προσθέσει το CLH ως parent στη λίστα γειτόνων της και θα ξεκινήσει η μετάδοση περιοδικών ακολουθιών (periodic beacons). Αν η σύνδεση αυτή δεν είναι εφικτή, τότε η συσκευή θα αναζητήσει άλλο CLH –parent που ανήκει σε άλλο cluster του δικτύου. Βασικό πλεονέκτημα αυτής της τοπολογίας είναι η ευρεία κάλυψη μιας περιοχής, ενώ μειονέκτημά της είναι η χαμηλή ταχύτητα μετάδοσης των μηνυμάτων.



2.2.1 Το Φυσικό Επίπεδο (Physical Layer) του 802.15.4

Το φυσικό επίπεδο παρέχει την υπηρεσία PHY data service και την PHY management service, που αλληλεπιδρά με την οντότητα διαχείρισης του φυσικού επιπέδου (Physical Layer Management Entity – PLME).

Το πρότυπο 802.15.4 καθορίζει ως επιτρεπόμενη τεχνική μετάδοσης του φυσικού επιπέδου την τεχνική εξάπλωσης φάσματος συνεχούς ακολουθίας DSSS (Direct Sequence Spread Spectrum) με διαμόρφωση BPSK (Binary Phase Shift Keying) ή OQPSK (Offset Quadrature Phase Shift Keying).

Οι βασικές λειτουργίες και υπηρεσίες που υλοποιούνται από το PHY επίπεδο του 802.15.4 είναι:

- Ενεργοποίηση και Απενεργοποίηση του Πομποδέκτη (transceiver), όπου αυτός τίθεται σε μία από τις τρεις καταστάσεις: εκπομπή, λήψη και sleeping.
- Ανίχνευση Ενέργειας (Energy Detection – ED) στο τρέχον κανάλι, η οποία είναι μια εκτίμηση της ισχύος του λαμβανόμενου σήματος.
- Κατανομή Εγγυημένων Χρονοθυρίδων (Guaranteed Time Slots - GTSs)
- Έλεγχος Αδράνειας Καναλιού (Clear Channel Assessment - CCA) για πολλαπλή πρόσβαση χρησιμοποιώντας ED ή ανίχνευση φέροντος σήματος (Carrier Sense mode) ή και συνδυασμό και των δύο. Σε κατάσταση ED το μέσο θεωρείται κατειλημμένο αν ανιχνευθεί επίπεδο ενέργειας πάνω από ένα προκαθορισμένο κατώφλι (threshold), ενώ σε κατάσταση ανίχνευσης φέροντος το μέσο θεωρείται κατειλημμένο αν ανιχνευθεί σήμα με τη διαμόρφωση και τα spreading χαρακτηριστικά του προτύπου 802.15.4. Στη συνδυασμένη κατάσταση, απαιτούνται αμφότερες οι προαναφερθείσες συνθήκες να λαμβάνονται υπόψιν για το αν το μέσο είναι κατειλημμένο ή όχι.
- Ένδειξη Ποιότητας Ζεύξης (Link Quality Indication – LQI) για τα ληφθέντα πακέτα, όπου πραγματοποιείται αυτή η μέτρηση για κάθε πακέτο που λαμβάνεται. Η μέτρηση της ισχύος ή/και της ποιότητας μιας ζεύξης, μέσω της οποίας μεταφέρεται ένα πακέτο, γίνεται με τη χρήση του ED του λήπτη, ένα ποσοστό σήματος προς θόρυβο, ή ένα συνδυασμό αυτών. Βέβαια, ο τρόπος υπολογισμού του LQI από το 802.15.4 δεν καθορίζεται πλήρως, αφήνοντας το σχεδιαστή να εισάγει το δικό του ανάλογα με τους πόρους που διαθέτει, τις απαιτήσεις της εφαρμογής και τις περιβαλλοντικές συνθήκες.
- Επιλογή συχνότητας καναλιού, αφού οι ασύρματες ζεύξεις μπορούν να λειτουργήσουν σε 27 διαφορετικά κανάλια υπό το πρότυπο 802.15.4 και έτσι το φυσικό επίπεδο είναι υπεύθυνο για τη μετάθεση του πομποδέκτη σε ένα συγκεκριμένο κανάλι.
- Αποστολή και λήψη δεδομένων, η οποία και είναι η πιο βασική λειτουργία του φυσικού επιπέδου, εφαρμόζοντας τεχνικές διαμόρφωσης και spreading.
- Δομή των πακέτων του φυσικού επιπέδου, όπου η επικεφαλίδα συγχρονισμού SHR (Synchronization Header) αποτελείται από το preamble σήμα που χρησιμεύει για το συγχρονισμό και από το πεδίο που υποδηλώνει το τέλος του πεδίου συγχρονισμού SFD (Start Offrame Delimiter), που καθορίζει το τέλος του πεδίου SHR και την αρχή του υπόλοιπου πακέτου. Η επικεφαλίδα φυσικού επιπέδου PHR (PHY Header) αποτελείται από 8 bits και περιέχει πληροφορίες για το μήκος του πλαισίου. Το τμήμα δεδομένων του φυσικού επιπέδου (PHY Payload) είναι αυτό που ακολουθεί στο τέλος και περιλαμβάνει και το πλαίσιο MAC, το οποίο είναι μεταβλητού μήκους.

2.2.2 Το Υπο-επίπεδο Ελέγχου Προσπέλασης στο Μέσο Μετάδοσης (MAC-Media Access Control) του 802.15.4

Το MAC υπο-επίπεδο εξασφαλίζει τη διασύνδεση των ανώτερων επιπέδων με το φυσικό, δηλαδή είναι το επίπεδο που δρα ως διεπαφή μεταξύ του υπο-επιπέδου ελέγχου λογικής σύνδεσης (LLC) και του PHY Layer. Το πρωτόκολλο ελέγχου προσπέλασης στο μέσο παρέχει διευθυνσιοδότηση και μηχανισμούς ελέγχου

προσπέλασης του καναλιού, το οποίο καθιστά δυνατή την επικοινωνία μεταξύ των τερματικών ή των κόμβων του δικτύου. Το υπο-επίπεδο MAC εξομοιώνει ένα δικατευθυντήριο κανάλι επικοινωνίας σε δίκτυο πολλών σημείων, όπου το κανάλι μπορεί να παρέχει υπηρεσίες μονοεκπομπής (unicast), πολυεκπομπής (multicast) ή ευρυεκπομπής (broadcast)
Το MAC υπο-επίπεδο παρέχει την υπηρεσία MAC data service και την MAC management service, που διασυνδέονται με την οντότητα διαχείρισης του MAC (MAC Layer Management Entity – MLME) και την υπηρεσία πρόσβασης σημείου (Service Access Point - SAP).

Οι βασικές αρμοδιότητες που υλοποιούνται από το MAC υπο-επίπεδο του 802.15.4 είναι:
* Η διαχείριση του beacon
* Η πρόσβαση στο διαθέσιμο κανάλι
* Η διαχείριση των εγγυημένων χρονοθυρίδων (Guaranteed Time Slots – GTS)
* Η επιβεβαίωση των μεταδιδόμενων frames
* Η αναγνώριση της μεταφοράς των frames

Το πρότυπο 802.15.4 μπορεί να λειτουργήσει είτε σε non-beacon-enabled mode είτε σε beacon-enabled mode. Στην πρώτη περίπτωση, η οποία είναι ιδανική για δίκτυα τοπολογίας αστέρα, υποστηρίζονται δίκτυα πολλαπλών βημάτων (multi-hop), όπου μια ομάδα κόμβων είναι μονίμως ενεργή και αναμεταδίδει μηνύματα που δημιουργήθηκαν από άλλους κόμβους χαμηλής κατανάλωσης. Στην non-beacon λειτουργία, χρησιμοποιείται ο αλγόριθμος CSMA χωρίς χρονοθυρίδες (un-slotted) και δεν χρησιμοποιείται ο μηχανισμός RTS (Ready To Send) / CTS (Clear To Send), αφού το μέγεθος των πλαισίων του 802.15.4 είναι μικρό. Υπάρχει όριο στον αριθμό των αποσύρσεων που γίνονται, για την αποφυγή αέναης απόσυρσης (backoff), στην οποία ο χρόνος απόσυρσης του CSMA αυξάνεται εκθετικά χωρίς όρια, και μόλις φτάσει στο μέγιστο αυτό όριο δημιουργείται μια αναφορά αποτυχίας πρόσβασης στο κανάλι (channel access failure) από το MAC και αποστέλλεται στο ανώτερο επίπεδο της στοίβας. Στην άλλη περίπτωση λειτουργίας, την beacon-enabled mode, ο χρόνος του καναλιού διαιρείται σε υπερ-πλαίσια (super-flames), όπου οριοθετούνται από τους συντονιστές της ομάδας κατά την εκπομπή beacons. Στα πλαίσια μιας ομάδας, όλες οι επικοινωνίες, γίνονται κατά τη διάρκεια ενός τέτοιου υπερ-πλαισίου, η διάρκεια του οποίου ονομάζεται διάρκεια υπερ-πλαισίου (Super-frame Duration – SD). Βέβαια, ο συντονιστής μπορεί να απενεργοποιήσει την εκπομπή των beacons και έτσι να μην χρησιμοποιήσει τη δομή του υπερ-πλαισίου. Εφόσον είναι επιθυμητό, οι αισθητήρες να έχουν χαμηλή ενεργειακή κατανάλωση, στα super-flames υπάρχει ένα συνιστώμενο διάστημα εντός του οποίου ο coordinator δεν δέχεται πακέτα. Έτσι, όλες οι πληροφορίες πρέπει να μεταδοθούν στο ενεργό διάστημα ενώ ο coordinator «πέφτει για ύπνο» (sleep) όλο το υπόλοιπο διάστημα. Συνεπώς, το super-flame αποτελείται από ένα ενεργό και ανενεργό τμήμα, όπου το πρώτο υποδιαιρείται σε σχισμές σταθερού μήκους και αποτελείται από ανενεργό τμήμα, από μία περίοδο ανταγωνισμού πρόσβασης (Contention Access Period – CAP), στην οποία οι κόμβοι μεταδίδουν τα δεδομένα τους χωρίς διαμάχη και σε εγγυημένες χρονικές «σχισμές» (Guaranteed Time Slots–GTS), τις οποίες διαθέτει και διαχειρίζεται ο PAN coordinator.
Το MAC υπο-επίπεδο χρησιμοποιεί τον αλγόριθμο Πολλαπλής Πρόσβασης με Ανίχνευση Φέροντος και Αποφυγή Συγκρούσεων (Carrier Sense Multiple Access with Collision Avoidance – CSMA/CA) για την επιλογή της χρονικής στιγμής που θα

εκπέμψει μια συσκευή ή θα τεθεί σε αναμονή για τη λήψη ενός πακέτου.
Χρησιμοποιούνται δύο τύποι προσπέλασης, οι οποίοι αναφέρθηκαν ονομαστικά πιο πάνω, ανάλογα με τη διαμόρφωση του καναλιού :
► Un-slotted μορφή του αλγορίθμου, που είναι διαδεδομένη σε δίκτυα με απενεργοποιημένη την εκπομπή beacons και με πρόβλεψη της ανίχνευσης του καναλιού πριν την μετάδοση. Έτσι, μια συσκευή σε κάθε εκπομπή δεδομένων, πρέπει να περιμένει ένα τυχαίο χρονικό διάστημα περιόδων backoff. Σε περίπτωση αδράνειας του καναλιού αρχίζει η μετάδοση, ενώ στην περίπτωση που είναι απασχολημένο ακολουθείται ένας τυχαίος αλγόριθμος backoff και έπειτα εκπέμπει. Κατά τη διάρκεια της μετάδοσης, δεν ανιχνεύει το κανάλι και στέλνει την ακολουθία δεδομένων ολόκληρη, η οποία μπορεί να χαθεί λόγω παρεμβολών.

► Slotted μορφή του αλγορίθμου, που χρησιμοποιείται από δίκτυα με ενεργοποιημένη την εκπομπή beacons. Οι χρονοσχισμές απόσυρσης ευθυγραμμίζονται με την αρχή εκπομπής του πλαισίου beacon και όταν ένας κόμβος επιθυμεί να εκπέμψει στη διάρκεια της περιόδου ανταγωνισμού του καναλιού, εντοπίζει το όριο της επόμενης θυρίδας και περιμένει τυχαίο χρόνο. Αν το κανάλι είναι κατειλημμένο, θα πρέπει να περιμένει για ένα τυχαίο αριθμό από θυρίδες και να ξαναδοκιμάσει για την πρόσβασή του στο κανάλι, ενώ αν είναι ελεύθερο περιμένει για το επόμενο όριο της θυρίδας και έπειτα εκπέμπει.

2.2.3 Η Δομή του Πλαισίου του 802.15.4

Τα πλαίσια του 802.15.4, στη γενική τους μορφή, αποτελούνται από:
* Τα bytes του φυσικού επιπέδου, που περιλαμβάνουν το 40bit προοίμιο (preamble), δηλαδή τα bits συγχρονισμού που βοηθούν το δέκτη να ξεχωρίσει το 802.15.4 πακέτο από το θορυβώδες περιβάλλον, και το μήκος πλαισίου.
* Την κεφαλίδα του MAC υπο-επιπέδου (MHR) που περιλαμβάνει το πεδίο για τον έλεγχο πλαισίου, για πληροφορίες διεύθυνσης, για παραμέτρους δικτύου και τέλος, το πεδίο για τον αριθμό ακολουθίας του πακέτου (sequence number).
* Το περιεχόμενο του πακέτου, δηλαδή ένα μεταβλητό data payload.
* Το πλαίσιο τέλους του MAC υπο-επιπέδου (MFR), δηλαδή την ακολουθία ελέγχου που επιτρέπει στο δέκτη να αντιληφθεί τη μεταβίβαση του πακέτου χωρίς σφάλματα (Frame CheckSequence – FCS).

Υπάρχουν τέσσερις δομές πλαισίων του δικτύου 802.15.4 ανάλογα με το σκοπό για τον οποίο προορίζονται:

■ Η δομή για πλαίσιο beacon (Beacon Frame), το οποίο προέρχεται από το εσωτερικό υπόστρωμα του MAC. Ένας συντονιστής μπορεί να μεταδώσει πλαίσια beacons δικτύου σε ένα δίκτυο που επιτρέπεται η αποστολή τους. Το ωφέλιμο φορτίο του MAC περιέχει την προδιαγραφή του super-flame, τα πεδία GTS, την εν αναμονή διεύθυνση (pending address) και το ωφέλιμο φορτίο του beacon, το οποίο είναι προκαθορισμένο με μία επικεφαλίδα MAC (MHR) και επισυνάπτεται με το MFR (MAC footer). Το MHR περιλαμβάνει το πεδίο πλαισίου ελέγχου του MAC (MAC control frame field), τον αριθμό σειράς του beacon (Beacon Sequence Number - BSN), τα πεδία διευθύνσεων (addressing fields) και προαιρετικά τη βοηθητική κεφαλίδα ασφαλείας (security header). Το MFR περιλαμβάνει ένα πλαίσιο ελέγχου σειράς 16 bits (Frame Check Sequence - FCS). Το MHR μαζί με το ωφέλιμο φορτίο του MAC και το MFR σχηματίζουν ένα MAC πλαίσιο beacon (MAC Protocol Data

Unit - MPDU). Το πλαίσιο αυτό
περνά στο φυσικό επίπεδο, ως η φυσική μονάδα δεδομένων υπηρεσίας (PHY Service Data Unit -PSDU), η οποία καθίσταται το ωφέλιμο φορτίο του φυσικού επιπέδου. Το ωφέλιμο φορτίο του φυσικού επιπέδου είναι προκαθορισμένο μαζί με την κεφαλίδα συγχρονισμού (SHR) και περιέχει την ακολουθία προοιμίου (Preamble Sequence), το πεδίο της αρχής του διαχωριστή του πλαισίου (Start-of-Frame Delimiter), καθώς και τη φυσική κεφαλίδα (PHR), που περιλαμβάνει το μέγεθος του ωφέλιμου φορτίου του φυσικού επιπέδου σε bytes. Το SHR, PHR και το ωφέλιμο φορτίο του φυσικού επιπέδου από κοινού σχηματίζουν το πακέτο του φυσικού επιπέδου (PHY Protocol Data Unit - PPDU).

■ Η δομή για πλαίσιο δεδομένων (Data Frame), το οποίο προέρχεται από τα ανώτερα επίπεδα. Το ωφέλιμο φορτίο δεδομένων περνά στο εσωτερικό υπόστρωμα του MAC και αναφέρεται ως MAC μονάδα δεδομένων υπηρεσίας (MSDU). Το ωφέλιμο φορτίο του MAC προκαθορίζεται μαζί με ένα MHR και επισυνάπτεται με ένα MFR. Το MHR περιλαμβάνει το πεδίο του MAC ελέγχου πλαισίου (MAC control frame field), τον αριθμό σειράς των δεδομένων (DSN), τα πεδία διευθύνσεων (addressing fields) και προαιρετικά την βοηθητική κεφαλίδα ασφαλείας (security header). Το MFR περιλαμβάνει ένα πλαίσιο σειράς ελέγχου αποτελούμενο από 16 bits (Frame Check Sequence - FCS). Το MHR μαζί με το ωφέλιμο φορτίο του MAC και το MFR σχηματίζουν ένα MAC πλαίσιο δεδομένων (MPDU). Το MAC πλαίσιο δεδομένων περνά στο φυσικό επίπεδο, ως η φυσική μονάδα δεδομένων υπηρεσίας (PSDU), η οποία καθίσταται το ωφέλιμο φορτίου του φυσικού επιπέδου. Το ωφέλιμο φορτίο του φυσικού επιπέδου είναι προκαθορισμένο μαζί με την κεφαλίδα συγχρονισμού (SHR), και περιέχει την ακολουθία προοιμίου (Preamble Sequence) και το πεδίο αρχής του διαχωριστή του πλαισίου (Start-of-Frame Delimiter), καθώς και τη φυσική κεφαλίδα (PHR), που περιλαμβάνει το μέγεθος του ωφέλιμου φορτίου του φυσικού επιπέδου σε bytes. Η ακολουθία του προοιμίου και τα δεδομένα SFD ενεργοποιούν τον παραλήπτη ώστε να επιτυγχάνει συγχρονισμό συμβόλων. Το SHR, PHR και το ωφέλιμο φορτίο του φυσικού επιπέδου από κοινού σχηματίζουν το πακέτο τουφυσικού επιπέδου (PPDU).

■ Η δομή για πλαίσιο επιβεβαίωσης (Acknowledge Frame), το οποίο προέρχεται από το εσωτερικό υπόστρωμα του MAC. Το πλαίσιο επιβεβαίωσης δημιουργείται από ένα MHR και ένα MFR, ενώ δεν περιέχει ωφέλιμο φορτίο MAC. Το MHR περιλαμβάνει το πεδίο ελέγχου πλαισίου (MAC control frame field) και τον αριθμό σειράς των δεδομένων (DSN). Το MFR περιλαμβάνει ένα πλαίσιο σειράς ελέγχου αποτελούμενο από 16 bits (Frame Check Sequence - FCS). Το MHR μαζί με το MFR σχηματίζουν ένα MAC πλαίσιο επιβεβαίωσης (MPDU). Το MAC πλαίσιο επιβεβαίωσης περνά στο φυσικό επίπεδο, ως η φυσική υπηρεσιακή μονάδα δεδομένων (PSDU), η οποία καθίσταται το ωφέλιμο φορτίου του φυσικού επιπέδου. Το ωφέλιμο φορτίο του φυσικού επιπέδου είναι προκαθορισμένο μαζί με την κεφαλίδα συγχρονισμού (SHR), και περιέχει την ακολουθία προοιμίου (Preamble Sequence) και το πεδίο αρχής του διαχωριστή του πλαισίου (Start-of-Frame Delimiter), καθώς και τη φυσική κεφαλίδα (PHR), που περιλαμβάνει το μέγεθος του ωφέλιμου φορτίου του φυσικού επιπέδου σε bytes. Το SHR, PHR και το ωφέλιμο φορτίο του φυσικού επιπέδου από κοινού σχηματίζουν το πακέτο του φυσικού επιπέδου (PPDU).

■ Η δομή για πλαίσιο εντολής (Command Frame), το οποίο προέρχεται από το εσωτερικό υπόστρωμα του MAC. Το ωφέλιμο φορτίο MAC περιέχει το πεδίο τύπος εντολής (Command Type) και το ωφέλιμο φορτίο εντολής. Το ωφέλιμο φορτίο του MAC προκαθορίζεται μαζί με ένα MHR και επισυνάπτεται με ένα MFR. Το MHR περιλαμβάνει το πεδίο του MAC ελέγχου πλαισίου (MAC control frame field), τον αριθμό σειράς των δεδομένων (DSN), τα πεδία διευθύνσεων (addressing fields) και προαιρετικά τη βοηθητική κεφαλίδα ασφαλείας (security header). Το MFR περιλαμβάνει ένα πλαίσιο σειράς ελέγχου αποτελούμενο από 16 bits (Frame Check Sequence - FCS). Το MHR μαζί με το ωφέλιμο φορτίο του MAC και το MFR σχηματίζουν ένα MAC πλαίσιο εντολής (MPDU). Το MPDU περνά στο φυσικό επίπεδο, ως η φυσική υπηρεσιακή μονάδα δεδομένων (PSDU), η οποία καθίσταται το ωφέλιμο φορτίου του φυσικού επιπέδου. Το ωφέλιμο φορτίο του φυσικού επιπέδου είναι προκαθορισμένο μαζί με την κεφαλίδα συγχρονισμού (SHR), και περιέχει την ακολουθία προοιμίου (Preamble Sequence) και το πεδίο αρχής του διαχωριστή του πλαισίου (Start-of-Frame Delimiter), καθώς και τη φυσική κεφαλίδα (PHR), που περιλαμβάνει το μέγεθος του ωφέλιμου φορτίου του φυσικού επιπέδου σε bytes. Η ακολουθία του προοιμίου και τα δεδομένα SFD ενεργοποιούν τον παραλήπτη ώστε να επιτυγχάνει συγχρονισμό συμβόλων. Το SHR, PHR και το ωφέλιμο φορτίο του φυσικού επιπέδου από κοινού σχηματίζουν το πακέτο του φυσικού επιπέδου (PPDU).

2.3 ZigBee

Πολλές φορές κυριαρχεί λανθασμένα η αντίληψη ότι το πρότυπο 802.15.4 και το ZigBee είναι ταυτόσημα. Το ZigBee αποτελεί επέκταση της στοίβας πρωτοκόλλων του 802.15.4, καθώς υλοποιεί τα επίπεδα δικτύου και εφαρμογών, βασιζόμενο στις υπηρεσίες που παρέχουν το φυσικό επίπεδο και το MAC υπο-επίπεδο του 802.15.4.
Η ZigBee Alliance είναι μια κοινή ομάδα πολλών μεγάλων εταιρειών, η οποία ανέπτυξε το πρωτόκολλο ZigBee ως ένα πρότυπο χαμηλού κόστους, πολύ χαμηλής κατανάλωσης, αμφίδρομης και ασύρματης επικοινωνίας. Οι πρώτες προδιαγραφές του ZigBee επικυρώθηκαν στα τέλη του 2004. Το ZigBee είναι το όνομα της προδιαγραφής για μια συλλογή υψηλού επιπέδου επικοινωνιακών πρωτοκόλλων που στοχεύει στις εφαρμογές ράδιο-συχνοτήτων και σε πιο απλή και οικονομική τεχνολογία σε σχέση με άλλα WPANs, όπως το Bluetooth.
Το IEEE 802.15.4 επικεντρώνεται στα δύο χαμηλότερα επίπεδα της στοίβας του πρωτοκόλλου, ενώ το ZigBee συγκεντρώνεται στην παροχή των πιο υψηλών επιπέδων για τη λειτουργικότητα των δεδομένων δικτύωσης και για υπηρεσίες ασφαλείας. Το πρωτόκολλο ZigBee υποστηρίζει τις τρεις βασικές τοπολογίες του IEEE 802.15.4. Τα βασικά χαρακτηριστικά του είναι ο χαμηλός ρυθμός μετάδοσης δεδομένων, η δυνατότητα να υποστηρίξει μέχρι 254 συσκευές σε τοπολογία αστέρα και η γρήγορη επαναφορά των συσκευών από κατάσταση sleep. Το δίκτυο ZigBee είναι πολλαπλής πρόσβασης, αφού όλες οι συσκευές έχουν ισότιμη πρόσβαση στο μέσο επικοινωνίας και υπάρχουν δύο τύποι μηχανισμών πολλαπλής πρόσβασης. Αυτοί οι τύποι αναφέρθηκαν και στην περίπτωση του προτύπου 802.15.4 και είναι ο μηχανισμός με λειτουργία beacon, όπου οι συσκευές επιτρέπεται να εκπέμπουν μόνο σε προκαθορισμένες χρονοθυρίδες, και η λειτουργία non-beacon, στην οποία όλες οι συσκευές μπορούν να εκπέμψουν οποιαδήποτε χρονική στιγμή, εφόσον το κανάλι είναι ελεύθερο.

2.3.1 Τα Επίπεδα του Πρωτοκόλλου ZigBee

Το πρωτόκολλο Zigbee καθορίζει τα υψηλότερα επίπεδα της στοίβας πρωτοκόλλων, από το επίπεδο δικτύου και πάνω. Η στοίβα πρωτοκόλλων του ZigBee βρίσκεται στο πάνω μέρος του φυσικού επιπέδου και του MAC υπο-επιπέδου, που έχουν καθοριστεί από το πρότυπο IEEE 802.15.4.

Η στοίβα πρωτοκόλλων ορίζει τα ακόλουθα επίπεδα:

1. Επίπεδο Δικτύου - ZigBee Network Layer (NWK)

Το NWK επίπεδο αποτελεί τη γέφυρα μεταξύ των δύο προτύπων, του 802.15.4 και του ZigBee, καθώς εξασφαλίζει τη σωστή λειτουργία του MAC υπο-επιπέδου και παρέχει τις κατάλληλες υπηρεσίες στο επίπεδο εφαρμογών, μέσω των μονάδων NLDE – SAP (Netwotk Layer Data Entity - Service Access Point) και NLME – SAP (Netwotk Layer Management Entity- Service Access Point). Το επίπεδο αυτό περιέχει όλες τις τοπολογίες δικτύωσης, που παρέχονται από τη συγκεκριμένη τεχνολογία και είναι υπεύθυνο για την οργάνωση και παροχή δρομολόγησης σε ένα multi-hop δίκτυο, που βασίζεται στη λειτουργία του IEEE 802.15.4.
Επιπλέον, αρμοδιότητα του NWK επιπέδου είναι η σωστή διατήρηση της επικοινωνίας μεταξύ των συνδεδεμένων συσκευών του δικτύου και η ανίχνευση της λειτουργίας γειτονικών δικτύων, ώστε να αποφευχθεί μια ενδεχόμενη επικάλυψη συχνότητας.

2. Επίπεδο Εφαρμογής - ZigBee Application Layer (APL)

Το επίπεδο αυτό είναι το υψηλότερο και πολυπλοκότερο που ορίζει το πρότυπο και προσφέρει μια δομή για την ανάπτυξη και επικοινωνία κατανεμημένων εφαρμογών. Αποτελείται από τα Αντικείμενα Εφαρμογών (Application Objects), το Αντικείμενο Συσκευής ZigBee (ZigBee Application Object) και το υπο-επίπεδο Υποστήριξης Εφαρμογής (Application Support SubLayer - APS). Τα Αντικείμενα Εφαρμογών είναι οι εφαρμογές που τρέχουν σε μια συσκευή ZigBee και το Αντικείμενο Συσκευής ZigBee παρέχει τη διασύνδεση στα Αντικείμενα Εφαρμογών, που χρησιμοποιείται για την αναγνώριση άλλων συσκευών και υπηρεσιών που αυτές παρέχουν. Το υπο-επίπεδο APS είναι υπεύθυνο για τη διατήρηση των λογικών συνδέσεων μεταξύ των συσκευών επικοινωνίας με την προώθηση παράλληλα των πακέτων δεδομένων μεταξύ των συνδεδεμένων συσκευών. Ακόμη, το υπο-επίπεδο αυτό επικοινωνεί άμεσα με την υπηρεσία παροχής ασφάλειας των δεδομένων μεταφοράς και λήψης δεδομένων (Security Service Provider).

3. Πλαίσιο Εργασίας Εφαρμογών - ZigBee Application Framework (AF)

Το επίπεδο AF είναι το τελευταίο επίπεδο του πρωτοκόλλου ZigBee και είναι υπεύθυνο για την ύπαρξη και διαμονή όλων των αντικειμένων της εφαρμογής στο δίκτυο, που θεωρείται η λογική περιγραφή κάθε συσκευής ZigBee συνδεδεμένης στο δίκτυο και η οποία μπορεί να εκπέμπει και να λαμβάνει πακέτα δεδομένων. Αυτό το επίπεδο διαθέτει μέχρι 240 αντικείμενα εφαρμογών, οντότητες εφαρμογών καθορισμένες από το χρήστη και οι οποίες αποτελούν μέρος της εφαρμογής ZigBee.

2.3.2 Η Δομή του Πλαισίου του ZigBee στο Επίπεδο Δικτύου

Τα πλαίσια του ZigBee στο επίπεδο NWK, στη γενική τους μορφή, αποτελούνται από:
* Την επικεφαλίδα NWK
* Το πλαίσιο ελέγχου
* Το πεδίο διεύθυνσης
* Το πεδίο για πληροφορία αρίθμησης
* Το ωφέλιμο φορτίο NWK

Το πεδίο της διεύθυνσης προορισμού είναι 2 octets, εξαρτάται από το multicast flag sub – field του πεδίου του πλαισίου ελέγχου και διατηρεί 16 bits της διεύθυνσης δικτύου της συσκευής προορισμού, μια broadcast διεύθυνση ή την 16 bits ταυτότητα της ομάδας της προοριζόμενης multicast ομάδας. Το πεδίο της διεύθυνσης πηγής διατηρεί πάντα την 16 bits διεύθυνση του δικτύου της συσκευής πηγής. Το πεδίο αυτό μαζί με τον αριθμό ακολουθίας χαρακτηρίζουν μοναδικά το πλαίσιο. Το πεδίο payload πλαισίου έχει μεταβλητό μήκος και περιέχει πληροφορία με τα μεμονωμένα είδη των πλαισίων. Το πεδίο του πλαισίου ελέγχου είναι 16 bits και περιέχει πληροφορία για τον καθορισμό του είδος του πλαισίου, τη διεύθυνση, τα πεδία αρίθμησης και άλλες σημαίες ελέγχου.

2.4 Πλεονεκτήματα Χρήσης του IEEE 802.15.4 και ZigBee

Η τεχνολογία ZigBee και IEEE 802.15.4 εμφανίζεται να αποτελεί την τεχνολογία με τα περισσότερα πλεονεκτήματα για την εφαρμογή της σε ασύρματα προσωπικά δίκτυα (WPANs). Η ευρεία επέκταση των εφαρμογών τους οφείλεται στα ιδιαίτερα πλεονεκτήματα που παρουσιάζουν αυτά τα πρότυπα, όπως η χαμηλή κατανάλωση ισχύος, δυνατότητα μεταφοράς μικρού μήκους πακέτων δεδομένων σε διάφορες τοπολογίες δικτύων με αξιοπιστία και μεγάλη ταχύτητα. Ακόμη, η τεχνική εξάπλωσης του φάσματος DSSS, που χρησιμοποιείται από το IEEE 802.15.4, δίνει τη δυνατότητα μετάδοσης των δεδομένων ταχύτερα και αποδοτικότερα, αφού πραγματοποιείται μέσω πολλαπλών συχνοτήτων. Η διαδεδομένη χρήση τους οφείλεται επίσης στο χαμηλό κόστος υλικού και λογισμικού, το οποίο οδηγεί σε απλές λύσεις. Έτσι, η χρήση του προτύπου 802.15.4 ή του ZigBee σε ένα δίκτυο, τις περισσότερες φορές διατηρεί σε χαμηλό επίπεδο το κόστος του και περιορίζει το χρόνο ανάπτυξής του. Επίσης, σημαντικό χαρακτηριστικό αυτών των πρωτοκόλλων είναι ότι το εκάστοτε δίκτυο μπορεί να υποστηρίξει πολλές συσκευές καθώς και πολλαπλές τοπολογίες. Το κύριο στοιχείο του 802.15.4 είναι η δυνατότητα επίτευξης χαμηλού κόστους κατασκευής και λειτουργίας με παράλληλα την τεχνολογική απλότητα των δικτύων και των συσκευών. Συνεπώς, το πρότυπο αυτό αποτελεί την κατάλληλη λύση για εφαρμογές με χαμηλή ενέργεια και χαμηλό κόστος, όπως και το ZigBee, που είναι μια τεχνολογία χαμηλού εύρους δεδομένων, χαμηλού κόστους και χαμηλής κατανάλωσης ενέργειας ασύρματων πρωτοκόλλων δικτύωσης.

2.5 Παραλλαγές του Πρωτοκόλλου 802.11

Οι παραλλαγές του 802.11 εμφανίζονται με ένα λατινικό γράμμα το οποίο προέρχεται

απότην ομάδα εργασίας (task group) που έκανε την αναθεώρηση του πρωτοκόλλου.

2.5.1 Το Πρωτόκολλο 802.11a

Το πρωτόκολλο 802.11a αποτελεί ένα πρωτόκολλο για το φυσικό επίπεδο ενός ασύρματου δικτύου και καθορίζει τη λειτουργία του δικτύου στη ζώνη UNII των 5 GHz. Υποστηρίζει ρυθμούς μετάδοσης από 6 έως και 54 Mbps και χρησιμοποιείται πολυπλεξία ορθογώνιας διαίρεσης συχνότητας (Orthogonal Frequency Division Multiplexing). Εξαιτίας της λειτουργίας του στη ζώνη UNII παρουσιάζει λιγότερες παρεμβολές από τη ζώνη ISM και εξαιτίας του υψηλού ρυθμού μετάδοσης προσφέρει πολύ καλύτερες επιδόσεις τόσο από το κλασσικό πρωτόκολλο 802.11 όσο και από το 802.11b, που είναι νεότερο και ευρύτερα εξαπλωμένο.

2.5.2 Το Πρωτόκολλο 802.11b

Το πρωτόκολλο 802.11b κατασκευάστηκε με στόχο να υποστηρίζει ρυθμούς μετάδοσης της τάξης των 5.5Mbps και 10Mbps και αυτό επιτεύχθηκε με την τροποποίηση του τρόπου διαμόρφωσης του σήματος. Έτσι, χρησιμοποιήθηκε η διαμόρφωση CCK (Complementary Code Keying) για να την επίτευξη των νέων ρυθμών, ενώ για να διατηρηθεί η συμβατότητα με το 802.11 με τους ρυθμούς 1Mbps και 2Mbps, χρησιμοποιήθηκε η διαμόρφωση DBPSK (Differential Binary Phase Shift Keying) και DQPSK ((Differential Quadrature phase-shift keying) αντίστοιχα.

2.5.3 Το Πρωτόκολλο 802.11c

Το πρωτόκολλο αυτό παρέχει πληροφορίες για τη διασφάλιση της σωστής λειτουργίας των γεφυρών-bridges και χρησιμοποιούνται κυρίως από τους κατασκευαστές των σημείων πρόσβασης για να εξασφαλίσουν τη διαλειτουργικότητά τους με συσκευές άλλων κατασκευαστών.

2.5.4 Το Πρωτόκολλο 802.11e

Το πρωτόκολλο 802.11e είναι ένα συμπληρωματικό πρωτόκολλο για το επίπεδο πολλαπλής πρόσβασης του 802.11, το οποίο παρέχει βελτιωμένη ποιότητα υπηρεσίας (Quality of Service – QoS). Στοχεύει σε μια από τις βασικές αδυναμίες του κλασσικού 802.11 πρωτοκόλλου, δηλαδή στην έλλειψη δυνατότητας παροχής διαφοροποιημένης μεταχείρισης σε διαφορετικές κατηγορίες κίνησης.

2.5.5 Το Πρωτόκολλο 802.11f

Το πρωτόκολλο 802.11f παρέχει τις απαραίτητες πληροφορίες στα σημεία πρόσβασης για να γίνει περιαγωγή με επιτυχία και να εξασφαλιστεί η ομαλή λειτουργία του συστήματος

2.5.6 Το Πρωτόκολλο 802.11g

Το πρωτόκολλο αυτό έχει στόχο να προσφέρει ρυθμούς μετάδοσης της τάξης των 54 Mbps, όπως και το 802.11a, αλλά να διατηρήσει και τη συμβατότητά του με το διαδεδομένο 802.11b. Το 802.11g λειτουργεί στη ζώνη συχνοτήτων ISM, όπως και το 802.11b, αλλά χρησιμοποιεί διαμόρφωση OFDM, όπως το 802.11a για να πετύχει

υψηλούς ρυθμούς μετάδοσης και λόγω συμβατότητας με το 802.11b υποστηρίζεται και η διαμόρφωση CCK.

2.5.7 Το Πρωτόκολλο 802.11h

Το πρωτόκολλο αυτό είναι συμπληρωματικό του υπο-επιπέδου MAC και συμμορφώνεται με τους ευρωπαϊκούς κανονισμούς για τη χρήση της ζώνης συχνοτήτων στα 5GHz. Συγκεκριμένα οι ευρωπαϊκοί κανονισμοί απαιτούν για τις συσκευές που λειτουργούν σε αυτή τη ζώνη συχνοτήτων να έχουν δυνατότητες ελέγχου εκπεμπόμενης ισχύος (Transmission Power Control) και δυναμικής επιλογής συχνότητας (Dynamic Frequency Selection) για τον καλύτερο έλεγχο των συγκρούσεων.

2.5.8 Το Πρωτόκολλο 802.11i

Το πρωτόκολλο 802.11i είναι ένα συμπληρωματικό πρότυπο για τη βελτίωση της ασφάλειας του συστήματος. Παρέχει έναν εναλλακτικό μηχανισμό του κλασσικού Wired Equivalent Privacy - WEP με καινούριες μεθόδους κρυπτογράφησης και πιστοποίησης.

2.5.9 Το Πρωτόκολλο 802.11n

Το πρωτόκολλο 802.11n είναι το νεότερο πρότυπο της IEEE, το οποίο επικυρώθηκε τον Αύγουστο του 2009, και αναπτύχθηκε για τη λειτουργία πιο γρήγορου LAN. Το πρωτόκολλο αυτό είναι ικανό να μεταδίδει δεδομένα με ταχύτητες της τάξης των 300Mbps. Έτσι, το πρότυπο 802.11n προσφέρει πολύ υψηλότερες ταχύτητες από το προηγουμένως επικυρωμένο 802.11g, το οποίο φτάνει τα 54Mbps και χρησιμοποιεί εύρος ζώνης των 40 MHz. Ακόμη, το πρωτόκολλο αυτό μπορεί να λειτουργήσει τόσο στην περιοχή των 5 GHz όσο και των 2.4 GHz.

2.5.10 Το Πρωτόκολλο 802.11y

Το πρωτόκολλο IEEE 802.11y προσθέτει τρεις νέες έννοιες στο πρωτόκολλο 802.11:
▪ Υποστηρίζει το Πρωτόκολλο Βασισμένο στο Συναγωνισμό (Contention-Based Protocol-CBP), μέσω του οποίου επιτυγχάνονται αυξήσεις στους μηχανισμούς αντίληψης μεταφορέων και ενεργειακής ανίχνευσης του προτύπου 802.11 προκειμένου να καλυφθούν οι απαιτήσεις της FCC (Federal Communications Commission) για το CBP.

▪ Έχει Εκτεταμένη Ανακοίνωση Εναλλαγής Καναλιών (Extended Channel Switch Announcement - ECSA) και παρέχει έναν μηχανισμό για ένα σημείο πρόσβασης, έτσι ώστε αυτό να δηλώνει τους σταθμούς που συνδέονται με βάση την πρόθεσή του να αλλάζει τα κανάλια ή να αλλάζει το εύρος ζώνης των καναλιών. Αυτός ο μηχανισμός θα επιτρέψει στα ασύρματα τοπικά δίκτυα να επιλέγουν συνεχώς το κανάλι που είναι το ελάχιστα θορυβώδες και το λιγότερο πιθανότερο να προκαλέσει την παρεμβολή. Αυτός ο μηχανισμός θα χρησιμοποιηθεί επίσης στο 802.11n, το οποίο θα επιτρέπει στις συσκευές να εναλλάσσονται μεταξύ της λειτουργίας 11y και 11n στις ζώνες των 2.4 και 5 GHz.

▪ Παρέχει Εξαρτώμενη Ενδυνάμωση Σταθμών (Dependent Station Enablement -

DSE) και είναι ο μηχανισμός από τον οποίο ένας χειριστής επεκτείνει και αποσύρει την άδεια από συσκευές, γνωστό ως εξαρτώμενο STAs, να χρησιμοποιήσουν το εξουσιοδοτημένο ραδιοφάσμα. Αυτή η διαδικασία ικανοποιεί πλήρως μια ρυθμιστική απαίτηση που υπαγορεύει ότι μια εξαρτώμενη λειτουργία STAs εξαρτάται από τη δυνατότητά της να λάβει τα περιοδικά μηνύματα από έναν σταθμό βάσεων κατόχων άδειας, αλλά το DSE είναι ιδανικό σε άλλους σκοπούς όσον αφορά τη διαχείριση και το συντονισμό.

2.6 Ασφάλεια στα WSN

2.6.1 Απαιτήσεις Ασφάλειας – Ιδιαιτερότητες των WSN

Η ασφάλεια δικτύου, είναι μία από τις σημαντικότερες ανησυχίες σε όλα τα ασύρματα δίκτυα, συμπεριλαμβανομένου και των ασύρματων δικτύων αισθητήρων. Στο κεφάλαιο αυτό θα παρουσιάσουμε το πρόβλημα ασφάλειας και θα εξηγήσουμε κάποια από τα ειδικά χαρακτηριστικά των ασυρμάτων δικτύων αισθητήρων. Οι σχειδιαστές τωνδικτύων πρέπει να προσέχουν και να επιλέγουν, μηχανοσμούς που να επιτυγχάνουν, έναν ή περισσότερους από τους ακόλουθους στόχους ασφαλείας.

2.6.2 Διαθεσιμότητα

Η σημασία της είναι ότι τα προσόντα δικτύου είναι διαθέσιμα, για να εξουσιοδοτούν τμήματα, όταν χρειάζεται.Επίσης τα ασύρματα δίκτυα αισθητήρων πρέπει να διασφαλίζουν, τη βιωσιμότητα των υπηρεσιών του δικτύου, παρά την άρνηση των επιθέσεων στις υπηρεσίες (denial of service DOS) οι οποίες μπορούν να φορτωθούν σε οποιοδήποτε στρώμα των WSN. Για την διασφάλιση της διαθεσιμότητας της προστασίας μηνυμάτων, το ασύρματο δίκτυο αισθητήρων πρέπει να προστατεύει τις πηγές του (όπως αισθητήριοι κόμβοι), από τα μη απαραίτητα επαξεργασμένα μηνύματα από το κλειδί διοίκησης, προκειμένου να ελαχιστοποιήσει την κατανάλωση ενέργειας και να επεκτείνει τη ζωή του δικτύου.

2.6.3 Αυθεντικότητα

Στα ασύρματα δίκτυα αισθητήρων, η αυθεντικότητα είναι απαραίτητη για πολλούς εκτελεστικούς σκοπούς (π.χ. επαναπρογραμματισμός δικτύου ή έλεγχος κύκλου ασφαλείας σε αισθητήριο κόμβο). Κατά την ίδια στιγμή, ένας εχθρός, μπορεί εύκολα να εισχωρήσει μηνύματα, όπότε ο δέκτης χρειάζεται να βεβαιωθεί ότι η πληροφορία χρησιμοποιήθηκε σε οποιαδήποτε μέθοδο λήψης απόφασης, και προέρχεται από την αξιόπιστη πηγή. Η αυθεντικότητα πληροφορίας, επιτρέπει στον δέκτη, να επιβεβαιώσει ότι η πληροφορία, στάλθηκε τοπικά από τον ισχυρίζοντα αποστολέα. Σκληρότερα επίπεδα αυθεντικότητας (όπως αποκαλυπτικό κλειδί αυθεντικότητας), παρέχονται από κάποια βεβαιωμένα πρωτόκολλα. Παρ'όλα αυτά, τα περισσότερα WSN σενάρια, δεν απαιτούν την επιπλέον «ασφάλεια» και μπορούν να επιβεβαιώσουν κλειδιά παράδοσης, χρησιμοποιώντας, ένα σύστημα εφαρμογής πρωτοκόλλων. Η υπηρεσία αυτή πρέπει να είναι σωστή και έξυπνη αρκετά, έτσι ώστε μόνο τα εξουσιοδοτημένα μερη να μπορούν να χρησιμοποιούν το σύστημα. Επίσης, δεν πρέπει να αρνείται εξουσιοδοτημένα τμήματα από τη χρήση του συστήματος δικτύου.

2.6.4 Εμπιστευτικότητα

Ένα εμπιστευτικό μήνυμα αντιστέκεται στην αποκάλυψη της σημασίας του σε έναν εισβολέα. Ακόμη και οι απ'ευθείας πληροφορίες στα WSN, χρειάζονται να παραμένουν εμπιστευτικές, αφού μπορεί να έχουν χρησιμοποιηθεί, σε μία DOS απειλή. Η κύρια λύση να διατηρήσει τη αυαίσθητη πληροφορία μυστική, είναι να κωδικοποιήσει την πληροφορία, με ένα μυστικό κλειδί το οποίο θα έχουν στην κατοχή τους, μόνο οι προτιθέμενοι δέκτες, γι'αυτό και επιτυγχάνεται η εμπιστευτικότητα. Η εμπιστευτικότητα πρέπει να παρέχεται με κλειδιά με ένα μικρό αντικείμενο(κλειδί κοκκοποιημένο) για να αποθαρύνει ένα απλό σπάσιμο από ένα συμβιβασμό μίας μεγάλης μερίδας του δικτύου αισθητήρων. Με άλλα λόγια, προτιμούνται, βεβαιωμένα μοναδικά κλειδιά μεταξύ κάθε ζεύγους κόμβου αισθητήρων επικοινωνίας σε μία ασφάλεια, στην χρησιμοποίηση ενός κλειδιού απλού δικτύου. Η υπηρεσία αυτή σημαίνει την προστασία της πληροφορίας που έχει μεταφερθεί από το δίκτυο από παθητικές επιθέσεις. Η υπηρεσία εκπομπής μέσων πρέπει να προστατευθεί από τις σταλμένες πληροφορίες από τους χρήστες. Άλλοι τύποι αυτής της υπηρεσίας εμπεριέχουν την ασφάλεια ενός απλού μηνύματος ή ενός συγκεκριμένου πεδίου του μηνύματος. Άλλη μια άποψη της εμπιστευτικότητας είναι η προστασία της κυκλοφορίας από έναν hacker που προσπαθεί να το αναλύσει. Με άλλα λόγια, πρέπει να υπάρχουν κάποια μέτρα τα οποία αρνούνται οι hackers από την παρατήρηση της συχνότητας και το μήκος της ενέργειας, τόσο καλά όσο άλλα χαρακτηριστικά κυκλοφορίας στο δίκτυο.

2.6.5 Μη αποποίηση.

Η υπηρεσία αυτή εμποδίζει την αποστολή ή λήψη τμήματος από την άρνηση των σταλμένων ή παραληφθέντων μηνυμάτων. Αυτό σημαίνει ότι όταν ένα μήνυμα παραλαμβάνεται, ο αποστολέας μπορεί να επιβεβαιώσει ότι το μήνυμα παρελήφθη πράγματι από τον υποτιθέμενο δέκτη.

2.6.6 Ανανέωση-Φρεσκάδα

Αυτό θα μπορούσε να σημαίνει ανανέωση πληροφορίας και ανανέωση κλειδιού. Αφού όλα τα δίκτυα αισθητήρων παρέχουν κάποιες δομές χρόνου ποικίλων καταμετρήσεων, πρέπει να διασφαλίσουμε ότι κάθε μήνυμα είναι φρέσκο. Η ανανέωση πληροφορίας, συνεπάγεται ότι η πληροφορία είναι πρόσφατή και αυτό διασφαλίζει ότι κανένας εχθρός δεν έχει ξαναγράψει παλαιά μηνύματα. Ένα κλειδί βεβαιωμένης μεθόδου, μεταξύ των εμπλεκομένων μπορεί να εγγυηθεί ότι κάθε κλειδί μοιρασμένο είναι καινούργιο(δεν έχει ξαναχρησιμοποιηθεί από κανέναν από τους εμπλεκόμενους). Αυτό επίσης σημαίνει ότι ένα κλειδί, χρησιμοποιείται σε έναν κρυπτογραφικό συνδυασμό, δεν έχει χρησιμοποιηθεί σε άλλο συνδυασμό. Γι'αυτό τα μοιραζόμενα κλειδιά είναι αναγκαίο να αλλάζουν διαρκώς, αφού ένα κλειδί μπορεί να συβιβαστεί, κατά την διάρκεια της προανάτπυξης ή της λειτουργίας των φάσεων ενός WSN.

2.6.7 Ακεραιότητα πληροφορίας

Οι μετρήσεις ακεραιότητας, διασφαλίζουν ότι οι ληφθείσες πληροφορίες, δεν διαφοροποιήθηκαν κατά την μεταφορά από έναν εισβολέα. Η υπηρεσία της ακεραιότητας μπορεί να δημιουργηθεί, χρησιμοποιώντας κρυπτογραφικές λειτουργίες,κομμένες σε κομμάτια, με κάποια μέθοδο κωδικοποίησης.Η υπηρεσία της ακεραιότητας παρέχεται συχνά και απεριόριστα, από την υπηρεσία της αυθεντικότητας, προκειμένου να εξασφαλιστεί η ασφάλεια του δικτύου. Διαφοροποιούμαστε μεταξύ των προσανατολισμένων συνδέσεων και των συνδέσεων που βασίζονται στις υπηρεσίες ακεραιότητας. Η υπηρεσία ακεραιότητας της προσανατολισμένης σύνδεσης, έρχεται αντιμέτωπη με πολλά μηνύματα και διαβεβαιώνει ότι τα μηνύματα στάλθηκαν χωρίς αναπαραγωγή εις διπλούν, τροποποίηση ή απάντηση. Εκτός απ' αυτό, η άρνηση της άποψης της επαναπαραγγελίας της υπηρεσίας κρύβεται κάτω απ' την υπηρεσία της προσανατολισμένης σύνδεσης. Η υπηρεσία ακεραιότητας της έλλειψης σύνδεσης έχει να κάνει μόνο με την προστασία ενάντια της τροποποίησης μηνυμάτων. Ένας υβριδικός τύπος της υπηρεσίας της ακεραιότητας είχε προταθεί να κάνει με τις εφαρμογές που απαιτούν προστασία εναντίον της επαναπαραγγελίας , αλλά χρειάζεται αυστηρή ακολουθία. Ένα καλό ασφαλές σύστημα θα ήταν ικανό να ανιχνεύσει οποιοδήποτε πρόβλημα ακεραιότητας και αν μια παράβαση της διαπιστωθεί, τότε η υπηρεσία πρέπει να αναφέρει αυτό το πρόβλημα. Ένας μηχανισμός software ή παρέμβαση ανθρώπινη θα μπορούσε να λυθεί το πρόβλημα. Η προσέγγιση λογισμικού υποτίθεται να λύσει το πρόβλημα αυτόματα χωρίς παρέμβαση ανθρώπινη.

2.6.8 Διαθεσιμότητα

Κάποιες επιθέσεις μπορούν να έχουν ως αποτέλεσμα την απώλεια ή ελάττωση της διαθεσιμότητας του συστήματος. Κάποια από αυτά τα προβλήματα μπορούν να επιλυθούν, ενώ κάποια άλλα απαιτούν κάποιους τύπους φυσικών διαδικασιών.

2.6.9 Επεκτασιμότητα και αυτό-οργάνωση

Σε αντίθεση με τα γενικά ad-hoc δίκτυα, τα οποία δεν είναι επεκτάσιμα, κατά κύρια προτεραιότητα, τα WSN, δεν μπορούν να χρησιμοποιήσουν βασικό διάγραμμα ο οποίο έχει φτωχές επεκτάσιμες ιδιότητες (είτε σε σχέση με το κόστος ενέργειας είτε με την αφάνεια). Γενικά, ο αριθμός των γειτόνων και οι αποστάσεις ή η απαιτούμενη ισχύς για την αποστολή μηνυμάτων με συγκεκριμένη εκτίμηση λάθους από έναν κόμβο στον άλλον, δεν θα είναι γνωστά στο μέλλον. Σαν συνέπεια οι κόμβοι των WSN πρέπει να είναι ικανοί να αυτοοργανώνονται και να επιλέγουν τους βασικούς μηχανισμούς που ταιριάζουν για την κάθε κατάσταση.

ΚΕΦΑΛΑΙΟ 3

Ασφάλεια σε ασύρματα δίκτυα

3.1 Γενικά

Τα πλεονεκτίατα της χρήσης των ασύρματων δικτύων είναι αναμφίβολα πολλά, με σημαντικότερο την ευελιξία που παρέχουν. Όμως λόγω του ότι τα δεδομένα που διακιούνται στο δίκτυο μεταδίδονται χρησιμοποιώντας ραδιοσυχνότητες, επιτρέπεται στον οποιοδήποτε να συνδεθεί στο δίκτυο. Για αυτό το λόγο δημιουργήθηκε η ανάγκη της ασφάλειας του δικτύου, την οποία ήρθαν να καλύψουν οι τεχνικές κρυπτογράφησης. Η εμπιστοσύνη, η ακεραιότητ, η πιστοποίησηκαι η διαθεσιμότητα της ανταλλασσόμενης πληροφορίας, πλέον οριοθετούνται από τα πρωτόκολλα κρυπτογράφησης, τα οποία βασίζονται σε ήδη γνωστές κρυπτογραφικές μεθόδους, κληρονομώντας έτσι τα όποια μειονεκτίματα και πλεονεκτήματα από άλλες υλοποιήσεις της σύγχρονης επιστήμης της κρυπτογραφίας.

3.2 Κρυπτογράφηση

Κρυπτογράφηση (encryption) είναι ο μετασχηματισμός των δεδομένων σε μορφή που δεν μπορεί να διαβαστεί από κανέναν παρά μόνο από αυτόν που διαθέτει το κατάλληλο κλειδί.

Υπάρχουν δύο οικογένειες αλγορίθμων κρυπτογράφησης:

- Οι συμμετρικοί αλγόριθμοι (ή αλγόριθμοι μυστικού κλειδιού)
- Οι ασύμετροι αλγόριθμοι (ή αλγόριθμοι δημοσίου κλειδιού)

Ο κύριος στόχος της κρυπτογράφησης είναι να παρέχει ασφάλεια στην επικοινωνία δύο ή περισσοτέρων μελλών χωρίς κάποιος άλλος να έχει τη δυνατότητα να διαβάσει την πληροφορία.

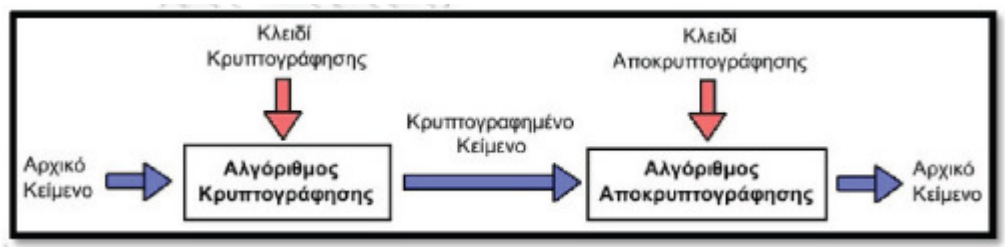
Η κρυπτογραφία παρέχει 4 βασικές λειτουργίες:

- Εμπιστευτικότητα: Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη. Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο.
- Ακεραιότητα: Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη.
- Μη απάρνηση: Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.

- Πιστοποίηση; Οι αποστολείς και οι παραλήπτες μπορούν να εξακριβώνουν τις ταυτότητές τους, καθώς και την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητές τους δεν είναι πλαστές.

Βασική ορολογία κρυπτογράφησης:

- Αρχικό κείμενο (plaintext): είναι το μήνυμα το οποίο αποτελεί την είσοδο σε μία διεργασία κρυπτογράφησης.
- Κλειδί (key): είναι ένας αριθμός αρκετών bit που χρησιμοποιείται ως είσοδος στη συνάρτηση κρυπτογράφησης.
- Κρυπτογραφημένο κείμενο (ciphertext): είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγορίθμου πάνω στο αρχικό κείμενο.



Εικόνα 3.1: Ένα τυπικό σύστημα κρυπτογράφησης – αποκρυπτογράφησης

Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγορίθμου και ενός κλειδιού κρυπτογράφησης . Συνήθως ο αλγόριθμος κρυπτογράφησης είναι γνωστός, οπότε η εμπιστευτικότητα του κρυπτογραφημένου μηνύματος που μεταδίδεται βασίζεται ως επί το πλείστον στη μυστικότητα του κλειδιού κρυπτογράφησης.

3.2.1 Κρυπτογράφηση συμμετρικού κλειδιού

Η κρυπτογράφηση συμετρικού κλειδιού (Symmetric Cryptography) προϋποθέτει την ύπαρξη ενός και μόνο κλειδιού, το οποίο χρησιμοποιείται για την κρυπτογράφηση και για την αποκρυπτογράφηση του μηνύματος. Το πρόβλημα που εντοπίζεται στην κρυπτογράφηση συμμετρικού κλειδιού είναι η αδυναμία ανταλλαγής του κλειδιού με ασφαλή τρόπο. Αυτοί οι αλγόριθμοι χρειάζονται την συμφωνία μεταξύ του αποστολέα και του παραλήπτη για το κλειδί που θα χρησιμοποιηθεί , για να μπορέσουν να επικοινωνίσουν με ασφάλεια. Το βασικό πλεονέκτημα των αλγορίθμων συμμετρικού κλειδιού είναι ότι η διαδικασία της κρυπτογράφησης και αποκρυπτογράφησης είναι πολύ γρήγορη και δεν καταναλώνει σημαντική υπολογιστική ισχύ.

Οι συμμετρικοί αλγόριθμοι μπορούν να διαιρεθούν σε δύο υποκατηγορίες:

- Αλγόριθμοι ροής: (steam ciphers), οι οποίοι λειτουργούν bit προς bit.
- Μπλοκ αλγόριθμοι: (block ciphers), οι οποίοι λειτουργούν πάνω σε κομμάτια δεδομένων (συνήθως των 64bit).

Οι πιο γνωστοί αλγόριθμοι αυτού του είδους είναι οι DES, Triple DES, IDEA, RC2, RC4, AES.

3.2.2 Κρυπτογράφηση δημόσιου κλειδιού ή ασύμετρου κλειδιού

Η κρυπτογράφηση δημοσίου κλειδιού (Public Key Cryptography) ή ασύμμετρου κλειδιού (Asymmetric Cryptography) επινοήθηκε στο τέλος της δεκαετίας του 1970. Η κρυπτογράφηση των κλειδιών γίνεται με τελείως διαφορετικό τρόπο. Είναι σχεδιασμένοι έτσι ώστε το κλειδί που χρησιμοποιείται για την κρυπτογράφηση να είναι διαφορετικό από το κλειδί για την αποκρυπτογράφηση.ο αποστολέας και ο παραλήπτης διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες, το ιδιωτικό (private) και το δημόσιο κλειδί (public key). Το ιδιωτικό κλει΄δι θα πρέπει ο κάθε χρήστης να το κρατάει κρυφό, ενό αντιθέτως το δημόσιο κλειδί μπορεί να ανακοινώνεται στους παραλήπτες. Εάν το ένα χρησιμοποιηθεί για την κρυπτογράφηση κάποιου μηνύματος, τότε το άλλο χρησιμοποιείται για την αποκρυπτογράφηση αυτού. Η επιτυχία αυτού του είδους κρυπτογραφικών αλγορίθμων βασίζεται στο γεγονός ότι η γνώση του δημόσιου κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού.

3.3 Πρωτόκολλα κρυπτογράφησης ασύρματων δικτύων

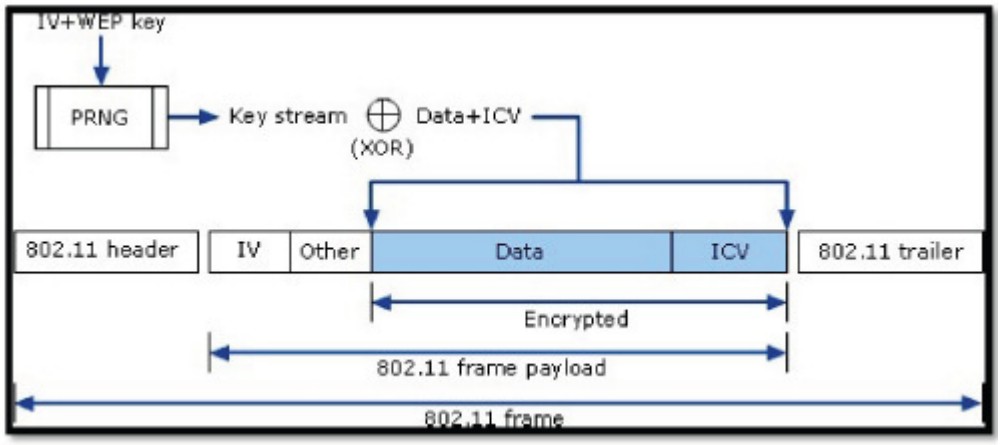
Από την έρευνα που πραγματοποιήθηκε σε κεντρικές περιοχές της πόλης των Αθηνών, ακόμη και σήμερα, παρατηρήθηκε ότι είναι αρκετά τα δίκτυα που δεν χρησιμοποιούν κανενός είδους κρυπτογράφηση. Σε αυτά τα ανασφάλιστα δίκτυα είναι προφανές ότι δεν μπορεί να υπάρξει καμία προστασία στους χρήστες που είναι συνδεδεμένοι, στην πληροφορία που ανταλάσουν, καθώς και στα αποθηκευμένα δεδομένα στο εσωτερικό του δικτύου. Η κρυπτογράφηση των ασύρματων δικτύων μπορεί να χωριστεί σε δύο βασικές κατηγορίες:

- WEP: Χρησμοποιεί τον αλγόριθμο κρυπτογράφησης RC4, για τον οποίο πλέον υπάρχουν διαδεδομένες τεχνικές εύρεσης του μυστικού κλειδιού.
- Στην οικογένεια WPA/WPA2: Θεωρείται το πιο ασφαλές πρωτόκολλο κρυπτογράφησης. Αντικατέστησε το ανασφαλές WEP και χρησιμοποιεί τον αλγόριθμο CCMP, ο οποίος βασίζεται στον AES.

3.4 Κρυπτογράφηση WEP

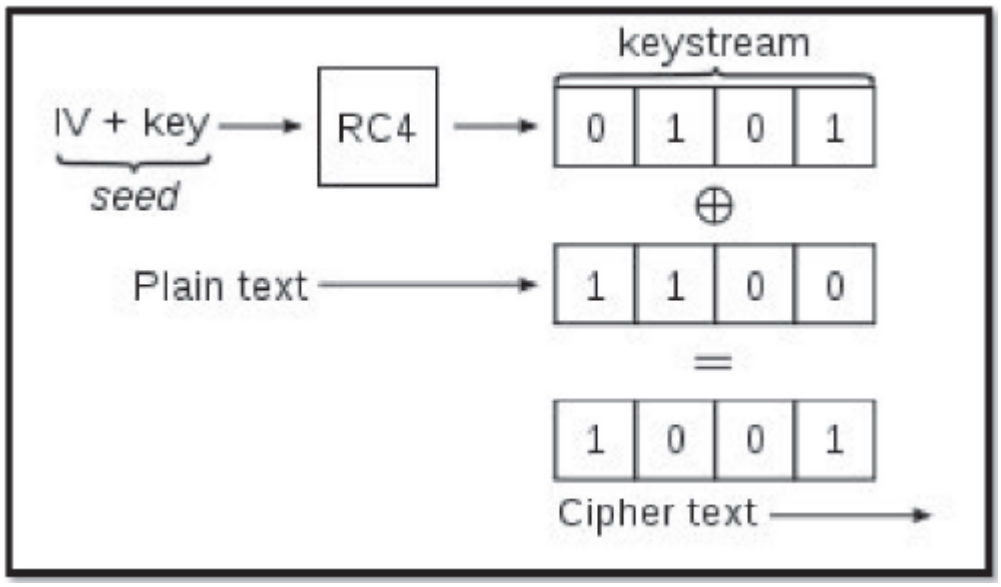
Ο τομέας της ασφάλειας των επικοινωνιών θέτει τους ακόλουθους τρεις σημαντικούς στόχους:

- Εμπιστευτικότητα: με τον όρο αυτό περιγράφεται η προστασία των δεδομένων από την πρόσβαση μη εξουσιοδοτημένων χρηστών.
- Ακεραιότητα: η διασφάλιση ότι το στοιχείο δεν έχει τροποποιηθεί.
- Επικύρωση: η υποστήριξη οποιουδήποτε μηχανισμού ασφάλειας της αξιοπιστίας των δεδομένων.



Εικόνα 3.2: Υλοποίηση WEP

Το πρωτόκολλο κρυπτογράφησης WEP παρέχει τις διαδικασίες που βοηθούν στην επιτυχία αυτών των στόχων. Η εμπιστευτικότητα και η ακεραιότητα των δεδομένων στο πρωτόκολλο αυτό εξασφαλίζεται συγχρόνως, χρησιμοποώντας τον αλγόριθμο κρυπτογράφησης RC4 (River Cipher 4), μήκους 64 ή 128 bit. Είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης ακολουθίας, ο οποίος δημιουργεί μία ψευδοτυχαία ακολουθία από bit, που συνδυάζεται με το υπό κρυπτογράφηση κείμενο (cipher text) με τη γνωστή συνάρτηση XOR για να παράξει το κρυπτογραφημένο κείμενο. Το κρυπτογραφημένο παράγεται χρησιμοποιώντας στα 24 bit του πίνακα αρχικοποίησης (Initialization Vector) και το κλειδί κρυπτογράφησης (pre-shared key) που εισήγαγε ο χρήστης, μήκους 40 ή 104 bit. Το αποτέλεσμα εισάγεται σε μία πύλη XOR μαζί με το αρχικό κείμενο (plain text) ώστε να δημιουργηθεί το τελικό κρυπτογραφημένο κείμενο.



Εικόνα 3.3: Basic WEP encryption: RC4 keystream XORed with plaintext

Το πρωτόκολλο WEP χρησιμοποιεί ένα κλειδί μήκους μόνο 40 bit, λόγω περιορισμών που έθεσε η Αμερικάνικη κυβέρνηση, το οποίο ευνοεί τις brute force επιθέσεις. Οι συγκεκριμένες επιθέσεις χρησιμοποιούν όλους τους πιθανούς συνδιασμούς κλειδιών μέχρι να βρεθεί το σωστό, με αποτέλεσμα υπολογιστές με μεγάλη υπολογιστική ισχύ να το σπάσουν πολύ γρήγορα. Όταν οι περιορισμοί κάφθηκαν, όλοι οι κατασκευαστές προσπάθησαν να το διορθώσουν. Επέκτειναν το μήκος του κλειδιού στα 128 bit χρησιμοποιώντας κλειδί κρυπτογράφησης μήκους 104 bit. Αυτό δεν άλλαξε τον τρόπο επίθεσης, αλλά λόγω της μεγάλης υπολογιστικης ισχύς που χρειάζονταν, καθιστά τις brute force επιθέσεις δυσκολότερες.

Η επικύρωση εξασφαλίζεται μέσω του ελέγχου των πακέτων. Ο αλγόριθμος CRC32 αναπτύχθηκε για να εντοπίζει, να επισημαίνει και πολλές φορές να διορθώνει τα λάθη κατά τη μετάδωση των πακέτων.

3.4.1 Ασφάλεια στο WEP

Η κρυπτογράφηση του πρωτοκόλλου WEP έχει μειωμένα επίπεδα ασφάλειας γεγονός που το κάνει ιδιαίτερα ευάλωτο σε επιθέσεις. Το μήκος του IV είναι μόλις 24 bit, τα οποία θεωρούνται λίγα για να εξασφαλιστεί η εμπιστευτικότητα των δεδομένων. Η τιμή ελέγχου ακεραιότητας (ICV) δεν παρέχει την απαιτούμενη ασφάλεια και δεν αποτρέπει την τροποποίηση των μηνυματων από κάποιον εισβολέα. Επιπλέον, το WEP συνδιάζει το κλειδί της κρυπτογράφησης με το IV, με τέτοιο τρόπο ώστε ο οποιοσδήποτε μπορεί να αποκτήσει το κλειδί της κρυπτογράφησης χρησιμοποιώντας μερικά εκατομμύρια κρυπτογραφημένα πακέτα. Επιπλέον δεν παρέχεται προστασία της ακεραιότητας των διεθύνσεων του αποστολέα και του παραλήπτη.

Οι επιθέσεις στοχεύουν στον πίνακα αρχικοποίησης (IV), ο οποίος εκπέμπεται συνεχώς μαζί με τα πακέτα. Τη στιγμή που θα επανεκπεμφθεί ο ίδιος πίνακας σε δύο διαφορετικά πακέτα, μπορούμε μέσω της XOR να βρούμε κομμάτια του αρχικού κειμένου. Τμηματικά θα αποκαλυφθεί όλο το μη-κωδικοποιημένο κομμάτι του μηνύματος. Επειδή ο χρόνος εκπομπής του πίνακα του πίνακα αρχικοποίησης δεν είναι ίδιος, έχουν αναπτυχθεί διάφορες τεχνικές για την επιτάχυνσή της. Η πιο συνηθησμένη τεχνική είναι ο εξαναγκασμός του σταθμού να εκπέμψει πάλι το πακέτο είτε λόγω απώλειας, είτε απόρριψης, είτε στέλνοντας πακέτα NACK. Με αυτή τη τεχνική, ο σταθμός αναγκάζεται να εκπέμπει συνεχώς, μειώνοντας έτσι ταχύτητα το διαθέσιμο εύρος τιμών του, με αποτέλεσμα σε σύντομο χρονικό διάστημα να επανεκπεμφθεί ο ίδιος πίνακας.
Η ακεραιότητα των δεδομένω δεν είναι καλά προστατευμένη στο WEP, διότι ο αλγόριθμος CRC προστατεύει μόνο από τυχαία λάθη που συμβαίνουν κατά τη μετάδοση. Γι' αυτό το λόγο τα κρυπτογραφημένα πακέτα μπορούν να αλλοιωθούν ή να υποκλαπούν. Οι εταιρίες αναγκάστηκαν να προβούν σε διορθώσεις του πρωτοκόλλου. Νέες εκδόσεις αναπτύχθηκαν για να εξαλειφθούν τα ελαττώματα του. Η πρώτη αναβάθιση έγινε με την έκδοση WEP2 η οποία αύξησε το μέγεθος του πίνακα αρχικοποίησης στα 128 bit. Ως αποτέλεσμα, να αυξηθεί ο χρόνος επανεκπομπής του ίδιου πίνακα αρχικοποίησης. Στη συνέχεια ακολούθησαν ακόμα δύο αναβαθμίσεις, το WEPplus (WEP+) και το Dynamic WEP.

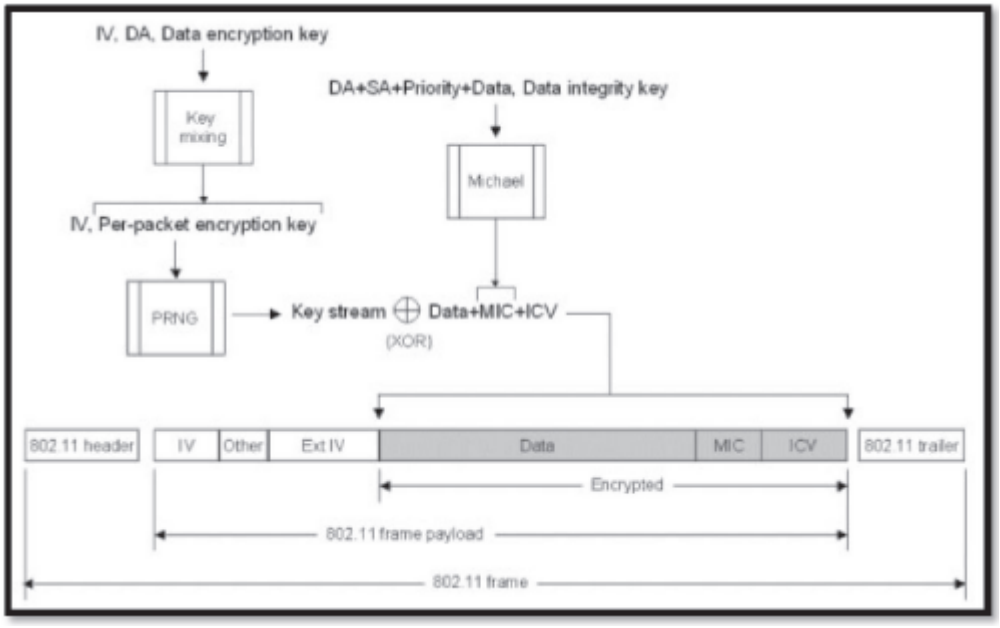
3.5 WPA (Wi-Fi Protested Access)

Το 2004 το πρότυπο IEEE με την έκδοση 802.11i ανέπτυξε ένα καινούριο πρωτόκολλο ασφαλείας για ασύρματη προστατευμένη πρόσβαση, το WPA (Wi-Fi Protected Access). Ουσιαστικά είναι το αντικαταστάσης του WEP, διότι υπήρχε η ανάγκη στις ασύρματες μετάδοσεις για περισσότερη ασφάλεια. Αποτέλεσε μία ενδιάμεση λύση έως την πλήρη ανάπτυξη της έκδοσης 802.11i με το πρωτόκολλο WPA2. Η WPA κρυπτογράφηση βελτιώνει την WEP και προσθέτει έναν ισχυρό μηχανισμό αυθεντικοποίησης. Η αυθεντικοποίηση των χρηστών γίνεται με δύο τρόπους λειτουργίας:

- Μέσω της WPA-Personal ή WPA-PSK ο χρήστης συνδέεται σε ένα Access Point και η αυθεντικοποίηση γίνεται μέσω προ-μοιρασμένων κλειδιών (Pre-Shared keys). Επακόλουθο είναι ότι για την καλύτερη ασφάλεια των συνδέσεων παίζει ρόλο το μήκος και η πολυπλοκότητα του κλειδιού.
- Η ασφαλέστερη λειτουργία εκτελείται με την υλοποίηση WPA-Enterprise, η οποία προϋποθλετει την ύπαρξη ενός 802.1x server, μέσω του οποίου ανά τακτά χρονικά διαστήματα, γίνεται ο διαμοιρασμός διαφορετικών κλειδιών για κάθε υπολογιστή, με αποτέλεσμα το σύστημα να είναι πιο ασφαλές, πιο πολύπλοκο και με μεγαλύτερο κόστος.

3.5.1 Ασφάλεια στο WPA

Το WPA χρησιμοποιεί τον RC4 αλγόριθμο, ο οποίος αποτελείται από τον πίνακα αρχικοποίησης μήκους 48 bit και ένα κλειδί χρονικής κρυπτογράφησης μήκους 128 bit. Η ύπαρξη του RC4 και στην καινούρια έκδοση εξασφαλίζει συμβατότητα με τις προηγούμενες εκδόσεις προϊόντων ασύρματης δικτύωσης. Επιπλέων, το WPA εισάγει ένα νέο πρωτόκολλο χρονικής ακεραιότητας κλειδιού, το TKIP (Temporal Key Integrity Protocol), το οποίο αναλαμβάνει δυναμικά την ανανέωση των κλειδιών κατά τη διάρκεια της σύνδεσης. Για να μειωθεί το ποσοστό επανάληψης του ίδιου κλειδιού, χρησιμοποιείται ανά εκπεμπόμενο πακέτο μία ακολουθία αριθμών, το pre-shared key και η εκπεμπόμενη MAC address.



Εικόνα 3.4: Υλοποίηση WPA

Στο νέο κλειδί που δημιουργείται προστίθεται ο πίνακας αρχικοποίησης και παράγεται μία νέα ακολουθεία κλειδιού (keystream). Για την ενίσχυση της ακεραιότητας των πακέτων έχει προστεθεί ένα πεδίο ελέγχου της ακεραιότητας των δεδομένων, το MIC (Message Integration Check). Η τιμή του MIC υπολογίζεται από τον κρυπτογραφικό αλγόριθμο Michael και προστατεύονται το μήνυμα και οι διευθύνσεις του αποστολέα και παραλήπτη. Ένα επιπλέον χαρακτηριστικό είναι ότιυποστηρίζει έναν ειδικό μηχανισμό, ο οποίος ανιχνεύει οποιαδήποτε προσπάθεια παραβίασης του TKIP, με αποτέλεσμα το μπλοκάρισμα της επικοινωνίας.

3.5.2 Αυθεντικότητα στο WPA

Η αυθεντικοποίηση στο πρωτόκολλο κρυπτογράφησης WPA-Personal ή WPA-PSK έχει σχεδιαστεί για επαγγελματική και οικιακή χρήση. Με αυτή τη μέθοδο η αυθεντικοποίηση των χρηστών γίνεται μέω του Access Point χρησιμοποιώντας μία φράση 8 ή 63 ASCII χαρακτήρες. Όταν επιλέγουν οι ASCII χαρακτήρες, μία hash function αναλαμβάνει τη μείωση από τα 504 bit (63characters * 8bit) στα 256 bit. Ακολούθως το σημείο πρόσβασης παρέχει στο σταθμό ένα προσωρινό κλειδί το οποίο ανανεώνεται σε τακτά χρονικά διαστήματα. Το 256 bit κλειδί υπολογίζεται χρησιμοποιώντας τη hash συνάρτηση PBKDF2 χρησιμοποιώντας τον αρχικό κωδικό ως κλειδί.

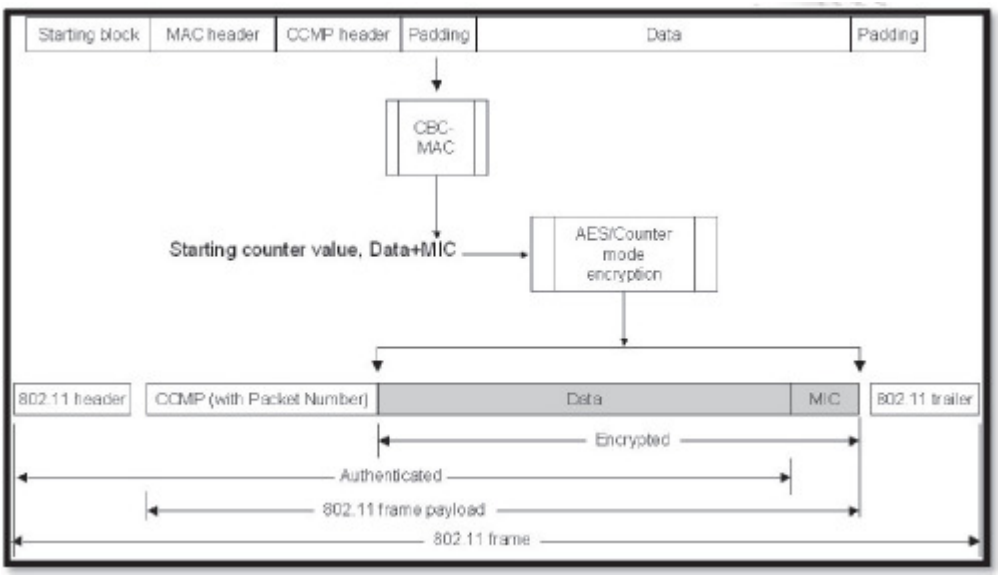
3.6 WPA vs WEP

Τα πρωτόκολλα κρυπτογράφισης WPA και WEP χρησιμοποιούν τον αλγόριθμο RC4 για κρυπτογράφηση. Ωστόσο, το WEP χρησιμοποιεί πίνακα αρχικοποίησης μήκους 24 bit με κλειδί κρυπτογράφησης μήκους 40 ή 104 bit, σε αντίθεση με το WPA που χρησιμοποιεί 48 bit IV με 128 bit κλειδί κρυπτογράφησης. Το WEP είναι ανεπαρκές για ασφάλεια, διότι οι επιθέσεις στοχεύουν στον πίνακα αρχικοποίησης και σις αλλοιώσεις των πακέτων. Στο WPA έχουν ελαχιστοποιηθεί τέτοιου είδους επιθέσεις εξαιτίας του συνδιασμού του πρωτοκόλλου TKIP, του MIC και του μεγαλύτερου μήκους πίνακα αρχικοποίησης. Το κλειδί TKIP χρησιμοποιεί περίπου 300 τρισεκατομμύρια πιθανά κλειδιά για την κρυπτογράφηση του πακέτου. Συνδυάζοντας το με τον 48 bit πίνακα αρχικοποίησης. Το κλειδί TKIP συμβάλλει στην αποτελεσματική ασφάλεια του δικτύου στις επιθέσεις ανάκτησης κλειδιού. Επίσης, το MIC βάζει ένα τέλος στην υποκλοπή πακέτων.

Το WPA-Enterprise και η WPA-PSK κρυπτογράφηση παρέχουν έναν ισχυρό μηχανισμό ασφάλειας, ο οποίος έλειπε από το WEP. Στο WEP η αυθεντικοποίηση του χρήστη γινόταν με τον διαμοιρασμό ενός κοινού κλειδιού. Στο WPA η αυθεντικοποίηση και η κρυπτογράφηση είναι ξεχωριστές λειτουργίες. Η αυθεντικότητα στον 802.1x server γίνεται με credentials, και τα κλειδιά διανέμονται αυτόματα.

3.7 WPA2 (Wi-Fi Protected Access Version 2)

Το πρωτόκολλο κρυπτογράφησης WPA2 είναι ο διάδοχος του WPA. Αποτελέι μέρος του προτύπου 802.11i. Η κρυπτογράφηση γίνεται με τον αλγόριθμο CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), ο οποίος για την ανάπτυξή του βασίστηκε στο CCM (Counter Mode with CMB-MAC) του αλγορίθμου AES (Advanced Encryption Standard), για την προστασία της ιδωτικότητας.



Εικόνα 3.5: Υλοποίηση WPA2

Με την είσοδο του νέου αλγορίθμου αντικαταστάθηκε ο RC4. Όπως το TKIP, έτσι και ο CCMP χρησιμοποιεί πίνακα αρχικοποίησης 48 bit, αλλά αντί για την ακολουθία αριθμών άνα πακέτο χρησιμοποιεί AES κλειδιά για την προστασία της εμπιστευτικότητας και ακεραιότητας του πακέτου. Χρησιμοποιεί πίνακα αρχικοποίησης 48 bit με 128 bit κλειδί κρυπτογράφησης το οποίο ελαχιστοποιεί την ευπάθεια του συστήματος σε επαναλαμβανόμενες επιθέσεις. Η ενισχυμένη προστασία που παρέχει το CCMP σε σύγκριση με το TKIP απαιτεί μεγαλύτερη επεξεργαστική ισχύ, και συχνά χρειάζεται νέο ή αναβαθησμένο hardware.

3.8 Οργανισμοί, Πρότυπα και Ακρωνύμια

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.9 Τύποι επιθέσεων σε ασύρματα δίκτυα

Τα ασύρματα δίκτυα λόγω του μέσου μετάδοσης είναι ευπαθή σε επιθέσεις. Οι επιθέσεις διενεργούνται για διαφορετικούς σκοπούς, για πράδειγμα, ένας εισβολέας μπορεί απλά να θέλει να ελέγξει την κίνηση ή να αποκτήσει πρόσβαση σε ένα δίκτυο. Επίθεση θεωρείται οποιαδήποτε ενέργεια που εκθέτει την ασφάλεια της πληροφορίας. Η πρόσβαση σε ξένα δεδομένα, είτε γίνεται με κίνητρο το συμφέρον, είτε τη περιέργεια, είναι πάντα γοητευτική. Δυστυχώς, σε πολλές περιπτώσεις στα ασύρματα δίκτυα είναι εκτός από γοητευτική και εύκολη. Ο στόχος των επιθέσεων δεν είναι πάντα τα δεδομένα των χρηστών αλλά και οι πόροι του δικτύου ή ακόμα και η προσωρινή αχρήστευσή του. Ανάλογα με το τι θέλει να πετύχει ο επιτιθέμενος, μπορεί να χρησιμοποιήσει διάφορες προσεγγίσεις. Γενικά, οι επιθέσεις εναντίων ασυρμάτων δικτύων μπορούν να χωριστούν σε παθητικές και ενεργητικές.

3.9.1 Παθητικές επιθέσεις

Οι παθητικές επιθέσεις είναι εκείνες στις οποίες ο επιτιθέμενος αποκτά πληροφορίες οι οποίες εκπέμπονται από κάποιο access point. Υπάρχουν δύο τύποι παθητικών επιθέσεων:

- Συλλογή πληροφοριών (traffic analysis)
- Συλλογή πακέτων (packet sniffing)

Οι επιθέσεις traffic analysis είναι εκείνες στιν οποίες ο επιτιθέμενος αποκτά πληροφορίες οι οποίες προέρχονται από τα access points, επομένως γνωρίζει το όνομα του δικτύου, το κανάλι εκπομπής, την μέθοδο κρυπτογράφησης, και τις MAC διευθύνσεις των συμμετοχών.

Οι επιθέσεις συλλογής πακέτων λειτουργούν πανομοιότυπα με τις επιθέσεις traffic analysis, καθώς και εδώ αποκαλύπτονται πληροφορίες του δικτύου. Επιπλέον, ο

επιτιθέμενος έχεις πρόσβαση και διαβάζει το περιεχόμενο των μηνυμάτων. Αν το μήνυμα είναι κρυπτογραφημένο, ο επιτιθέμενος πρέπει να το αποκρυπτογραφήση πρώτα. Εκτός από το διάβασμα της πληροφορίας, γίνονται γνωστά περισσότερα χαρακτηριστικά του πακέτου.

3.9.2 Ενεργητικές επιθέσεις

Οι ενεργητικές επιθέσεις συνεπάγονται τη συμμετοχή του επιτιθέμενου στο δίκτυο και διακρίνονται στις ακόλουθες κατηγορίες:

- Επιθέσεις μη εξουσιοδοτημένης πρόσβασης (Unauthorized Access)
- Επιθέσεις τροποποίησης μηνυμάτων (Man in the Middle Attack)
- Επιθέσεις άρνησης υπηρεσίας (Denial of Service)

Οι επιθέσεις μη εξουσιοδοτημένης πρόσβασης δεν έχουν ως στόχο κάποιον συγκεκριμένο χρήστη, αλλά την μη εξουσιοδοτημένη πρόσβαση στο δίκτυο. Σε κάποιες αρχιτεκτονικές δικτύων όταν ο επιτιθέμενος εισβάλλει σε ένα ασύρματο δίκτυο, αποκτά όλα τα δικαιώματα, ενώ σε άλλες για να έχεις πρόσβαση σε όλες τις συνατότητες του δικτύου πρέπει να είναι εξουσιοδοτημένος χρήστης, συνήθως με την εφαρμογή λιστών πρόσβασης ACL (Access Control Lists). Ωστόσο και ο έλεγχος πρόσβασης μπορεί να παραβιαστεί με την τεχνική της μεταμφίεσης (spoofing). Με την τεχνική αυτή ο επιτιθέμενος αντιγράφη το όνομα δικτύου και δημιουργεί ένα άλλο με δυνατότερο σήμα, με αποτέλεσμα οι υπολογιστές να συνδέονται στο ψεύτικο δίκτυο μεταδίδοντας όλα τα δεδομένα τους μέσα απ' αυτό.

Οι επιθέσεις τροποποίησης μηνυμάτων έχουν έναν έμμεσο τρόπο για να υποκλέπουν δεδομένα. Οι οργανισμοί παρόλο που έχουν αναπτύξει μηχανισμούς ασφαλείας όπως VPN και το IPSec, τα οποία όμως προστατεύουν από άμεσες επιθέσεις. Η επίθεση Man in the Middle, ο επιτιθέμενος βρισκεται στη μέση της συνοιλίας και εμφανίζεται στο access point ως χρήστης και στον χρήστη ως το access point. Ως αποτέλεσμα τα δεδομένα περνάνε πρώτα από τον επιτιθέμενο.

Οι επιθέσεις άρνησης υπηρεσίας είναι η πιο διαδεδομένη επίθεση για να αχρηστευτεί το ασύρματο δίκτυο για κάποιο χρονικό διάστημα. Αυτό μπορεί να επιτευχθεί αποστέλλοντας πολλά πακέτα στο δίκτυο, ώστε όλη η επεξεργαστική ισχύς του access point να καταναλώνεται στην επεξεργασία τους. Μία άλλη μέθοδος για την πραγματοποίηση DoS επιθέσεων είναι να καταληφθεί το φυσικό μέσο με ισχυρά σήματα στο κανάλι λειτουργίας του ώστε να είναι αδύνατη η επικοινωνία μεταξύ των σταθμών. Οι πέντε πιο συμαντικοί τύποι DoS επιθέσεων είναι η επίθεση πλημμύρας (Flood Attack), η επίθεση Ping of Death, η επίθεση SYN, η επίθεση Teardrop και η επίθεση Smurf.

3.9.3 WarDriving και WarChalking

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

Το WarChalking προϋποθέτει το WarDriving και περιγράφει την σημείωση των δικτύων που έχουν αποκαλυφθεί, και κυρίως τα αφύλακτα, πάνω ένα ψηφιοποιημένο χάρτη ή στα αρχικά στάδια με κιμωλία (chalk) πάνω σε τοίχους ή πεζοδρόμια. Τέτοιοι χάρτες κυκλοφορούν ελεύθερα στο Internet σχεδόν για κάθε κύρια πόλη του κόσμου. Το WarChalking δεν είναι, ούτε αυτό, παράνομο.

Τα εργαλεία που χρειάζονται για WarDriving είναι τα ίδια με αυτά της επίθεσης συλλογής πληροφοριών, με την διαφορά ότι χρησιμοποιούνται μόνο τα αναγκαία για την αποκάλυψη του SSID και τον τύπο της ασφάλειας που χρησιμοποιείται. Το WarChalking μπορεί να απλοποιηθεί αν το λογισμικό που χρησιμοποιείται συνεργάζεται με δέκτη GPS.

3.9.4 Rogue[4] Access Points

Ο όρος rogue AP (RAP) είναι, επίσης, ένας όρος που δεν παραπέμπει υποχρεωτικά σε παράνομη δραστηριότητα. Rogue χαρακτηρίζεται ένα AP που εγκαταστάθηκε χωρίς την συγκατάθεση του ιδιοκτήτη του δικτύου. Τα RAP αποτελούν πύλες εισόδου στο δίκτυο που αχρηστεύουν οποιαδήποτε προσπάθεια ασφάλειας και είναι ακόμα πιο επικίνδυνα σε δίκτυα που δεν συμπεριλαμβάνουν και ασύρματο μέρος.

Κάποιος εχθρικά διακείμενος σε μία εταιρία μπορεί να μπει στα γραφεία της και να εγκαταστήσει ένα AP σε μια ελεύθερη πρίζα που συνδέεται με το switch, χωρίς να γίνει αντιληπτός. Αυτό είναι ένα σενάριο. Κάποιος υπάλληλος της εταιρίας που έχει βαρεθεί τα καλώδια, αλλά έχει πλήρη άγνοια από ασφάλεια δικτύων (αυτός μπορεί να είναι και ο διευθυντής…), αγοράζει ένα AP και σύμφωνα με τις οδηγίες τοποθετεί την τροφοδοσία στην πρίζα και το καλώδιο δικτύου στην κατάλληλη υποδοχή της συσκευής. Με το κόστος των AP κάτω από τα 100€ και με όλα τα σύγχρονα laptop να ολοκληρώνουν ασύρματες κάρτες δικτύου, αυτό είναι ένα ακόμα πιο πιθανό σενάριο. Σύμφωνα με έρευνες, τουλάχιστον το 20% των επιχειρήσεων στις ΗΠΑ έχουν εγκατεστημένο ένα ή περισσότερα RAP στο εταιρικό τους δίκτυο5. Με όποιο τρόπο και να έχουν τοποθετηθεί, τα RAP αποτελούν μεγάλο κίνδυνο για την ασφάλεια ενός δικτύου. Το αρνητικό είναι ότι για την οριστική λύση του προβλήματος απαιτούνται μέθοδοι πιστοποίησης που η υλοποίησή τους είναι κάθε άλλο παρά απλή και οικονομική.

ΚΕΦΑΛΑΙΟ 4

Πρωτόκολλα και αλγόριθμοι διασφάλισεις ακεραιότητας δεδομένων

4.1 Γενικά

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

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

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

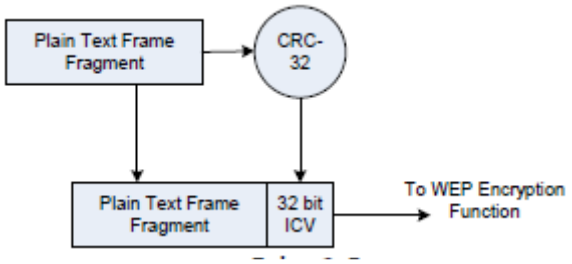
4.2 Wired Equivalent Privacy

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

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

4.3 Ακεραιότητα Δεδομένων σε Ασύρματα Δίκτυα

Όπως φαίνεται και στο σχήμα η εμπιστευτικότητα και η ακεραιότητα των δεδομένων προστατεύονται με τον ίδιο μηχανισμό στο WEP. Πριν την κρυπτογράφηση το frame τεμαχίζεται σε μικρότερα τμήματα. Στη συνέχεια, με την χρήση του αλγόριθμου ελέγχου ακεραιότητας δεδομένων Cyclic Redundancy Check (CRC-32) υπολογίζεται ένα hash των 32bit που ονομάζεται Integrity Check Value (ICV) και προσκολλάτε στην συνέχεια του τμήματος του αρχικού frame (σχ. 4.1).



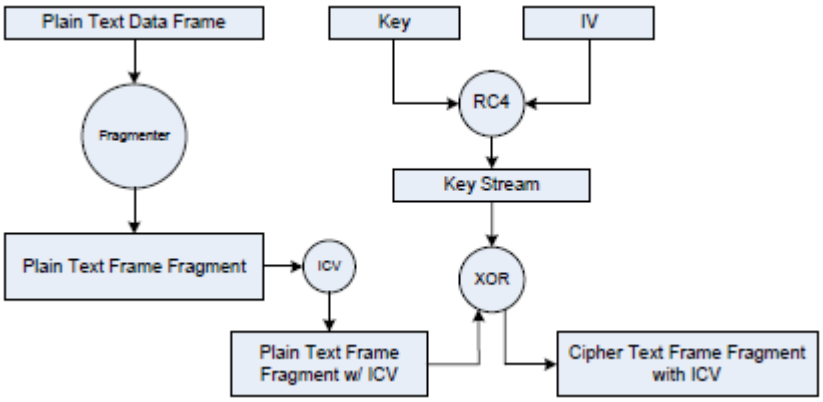
Εικόνα 4.1

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

G(X) = X32+X26+X23+X22+X16+X12+ X11+X10+X8 +X7 +X5 +X4 +X2 +X+1

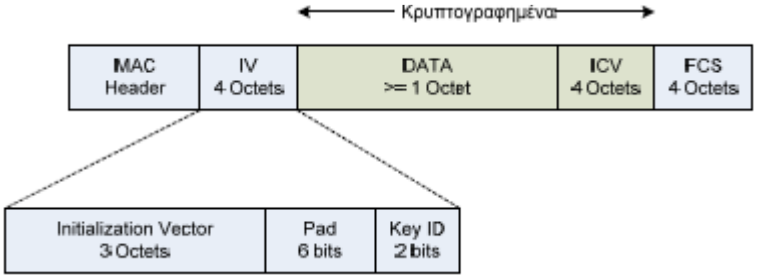
4.3.1 Πλαισίωση και Κρυπτογράφηση

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



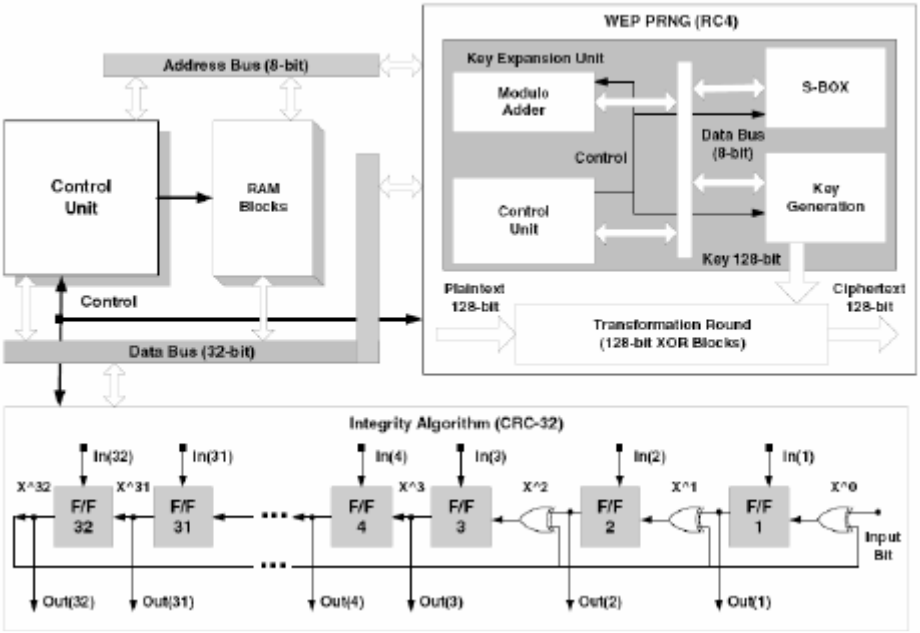
Εικόνα 4.2

Στην συνέχεια, για την παραγωγή της τελικής κρυπτογραφημένης ακολουθίας γίνεται XOR μεταξύ του τμήματος του frame συν το ICV trailer με το key stream. Το τελικό frame που φεύγει, τελικά, από τον πομπό αποτελείται από το αποτέλεσμα της XOR με την προσθήκη της επικεφαλίδας IV (εικόνα 4.2).



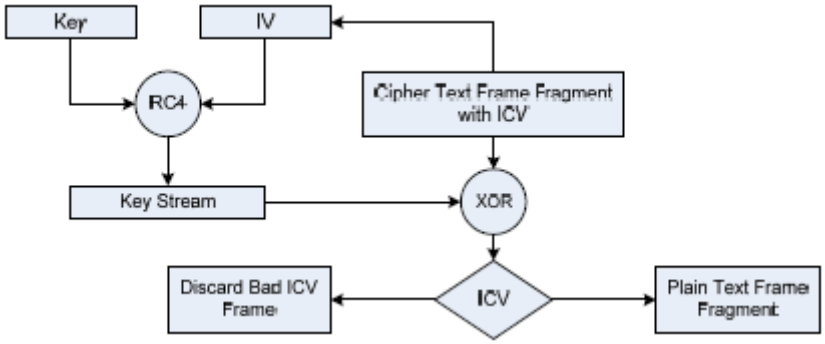
Εικόνα 4.3

Η επικεφαλίδα IV περιέχει τις απαραίτητες πληροφορίες για τον δέκτη (και όχι μόνο) για την αποκρυπτογράφηση. Τα πρώτα 3 byte είναι το ίδιο το τυχαία επιλεγμένο Initialization Vector. Τα επόμενα 6 bits είναι pad, δηλαδή μηδενικά απλά και μόνο για να μεγαλώσει το μήκος μιας ακολουθίας στο επιθυμητό. Τα τελευταία δύο bit είναι το αναγνωριστικό του κοινό κλειδιού (key ID). Το key ID είναι απαραίτητο γιατί σε κάθε συσκευή που συμμετέχει στο BSS, προβλέπεται να έχουν καθοριστεί μέχρι τέσσερα διαφορετικά κλειδιά.



Εικόνα 4.4

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



Εικόνα 4.5

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

4.3.2 Αδυναμίες του WEP

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

$$C_j = P_j \oplus K_{j,} \quad j=1,2,3...n \quad (1)$$

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

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

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

$$K_j = C_j \oplus P_j$$

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

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

Εάν, ο αριθμός των γνωστών αρχικών δεδομένων είναι σημαντικός, κάποιος θα μπορούσε να εξάγει το κοινό κλειδί, οπότε κάθε προσπάθεια κρυπτογράφησης θα ήταν άχρηστη.
Πρέπει να επισημανθεί ότι η γνώση των αρχικών μη κρυπτογραφημένων δεδομένων ή έστω μέρος αυτών δεν απαιτεί υποχρεωτικά και την υποκλοπή τους που θα ήταν αρκετά δύσκολη. Η δομή και τα περιεχόμενα κάποιων διαχειριστικών, κυρίως, πακέτων είναι γνωστά. Για παράδειγμα, υπάρχει πιθανότητα να αποκαλυφθεί το κλειδί μόνο από πακέτα DHCP.

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

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

Οπότε υπάρχει τρόπος σύγκρισης τον δεδομένων για την ανεύρεση μοτίβων, πχ. το γράμμα e εμφανίζεται συχνότερα σε αγγλικά κείμενα, δεύτερο είναι το t κτλ. Ο σχεδιασμός του WEP αντιμετωπίζει αυτό το πρόβλημα με την χρήση του IV. Όπως έχει αναφερθεί, το IV του WEP έχει μήκος 24bit και συνδυάζεται με το κοινό κλειδί για την παραγωγή 224 διαφορετικών κλειδιών (περίπου 16,5 εκατομμύρια πιθανά κλειδιά).
Το όλο σχήμα πάσχει από ένα βασικό πρόβλημα: Για να τηρείται η μη επαναχρησιμοποίηση των κλειδιών, όλοι οι χρήστες ενός ασύρματου δικτύου θα έπρεπε να αλλάζουν το κοινό κλειδί τους το πολύ μετά από μια ώρα χρήσης του σε ένα τυπικό περιβάλλον γραφείου. Σε περιβάλλον ESS με περισσότερα AP τα κλειδιά εξαντλούνται με ρυθμό αντιστρόφως ανάλογο του αριθμού των AP.
Το πρόβλημα γίνεται ακόμα χειρότερο γιατί δεν υπάρχει μηχανισμός που να αποτρέπει ένα χρήστη από το να χρησιμοποιεί ένα κλειδί που χρησιμοποιείται ήδη από κάποιον άλλο χρήστη.
Αυτό που γίνεται είναι η τυχαία επιλογή IV, αλλά και αυτό δεν αποτελεί λύση:
Έστω ένα σύνολο αποτελείται τα n στοιχεία και τα στοιχεία επιλέγονται τυχαία, ένα κάθε φορά, με επανατοποθέτηση και k ο αριθμός των επαναλήψεων του πειράματος τύχης. Η πιθανότητα να έχει επιλεχθεί το ίδιο στοιχείο είναι:

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

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

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

Αν υπολογίσουμε, χονδρικά, ότι για την αποστολή 1MB δεδομένων χρειάζονται περίπου 500 frames, τότε σε ένα BSS 802.11g με κανονική κίνηση θα χρειαστεί λιγότερο από ένα δευτερόλεπτο για σχεδόν βέβαιη επανάληψη του κλειδιού. Δυστυχώς, η επιμήκυνση του κοινού στατικού κλειδιού στα 104bit ή και παραπάνω δεν έχει καμία επίδραση στο πλήθος των διαθέσιμων κλειδιών.
Τον Αύγουστο του 2001 οι Fluhrer, Mantin και Shamir δημοσίευσαν μια έρευνα με τίτλο "Weaknesses in the Key Scheduling Algorithm of RC4". Στην δημοσίευση περιγράφεται, μεταξύ άλλων, μια θεωρητική επίθεση στο WEP. Η επίθεση βασίζεται στον τρόπο που ο RC4 παράγει το key stream. Το μόνο που προϋποθέτει για την πραγματοποίηση της επίθεσης είναι η γνώση του πρώτου byte του κρυπτογραφήματος. Δυστυχώς, αυτό είναι γνωστό σε όλους: το 802.11 χρησιμοποιεί το 802.2 ως Logical Link Layer οπότε το πρώτο byte είναι πάντα 0xAA (SNAP header). Όπως περιγράφθηκε παραπάνω, είναι εύκολο να βρεθεί το πρώτο byte του key stream ως το αποτέλεσμα του XOR μεταξύ του 0xAA και του πρώτου κρυπτογραφημένου byte.
Η επίθεση επικεντρώνεται σε μια κλάση αδύναμων IV της μορφής (B+3):FF:N. Κάθε διαφορετικό IV χρησιμοποιείται για την αποκάλυψη διαφορετικού τμήματος του κοινού κλειδιού. Το στάνταρ WEP κλειδί έχει μήκος 40bit ή 5 byte αριθμημένα από 0 έως 4 (τιμές του B). Η γνώση του N είναι απαραίτητη αλλά μπορεί να έχει οποιαδήποτε τιμή από 0 έως 0xFF. Για την αποκάλυψη του πρώτου byte του κοινού κλειδιού (B=0), τα αδύναμα IV έχουν τη μορφή 3:FF:N, για το δεύτερο 4:FF:N και ούτω καθεξής. Όπως μπορεί πολύ εύκολα να υπολογιστεί, το πλήθος των αδύναμων IV στο 40bit WEP είναι 5x1x256=1.280.
Οι Fluhrer, Mantin και Shamir υπολόγισαν ότι αρκούν 60 αδύναμα IV για την αποκάλυψη ενός byte του κοινού κλειδιού με αρκετά μεγάλη πιθανότητα επιτυχίας. Αυτό σημάνει ότι πρέπει να υποκλαπούν 1.000.000 έως 4.000.000 frames για μια επιτυχημένη επίθεση.
Το ενδιαφέρον με αυτή την επίθεση είναι ότι το μέγεθος της αδυναμίας είναι ανάλογη του μήκους του αρχικού κοινού κλειδιού. Συνήθως, δυσκολία αποκρυπτογράφησης αυξάνεται εκθετικά με το μήκος του κλειδιού. Σ' αυτή την περίπτωση λειτουργεί γραμμικά, οπότε διπλασιασμός του κλειδιού σημαίνει διπλασιασμό των frames που πρέπει κάποιος να συλλέξει, δηλαδή διπλασιασμός του χρόνου μέχρι την αποκρυπτογράφηση.

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

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

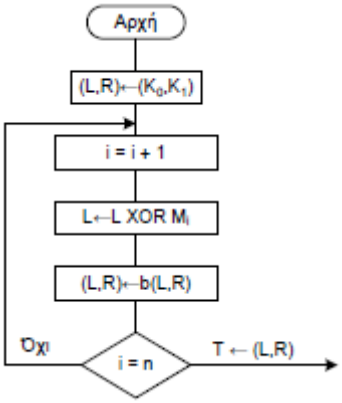
4.4 Temporal Key Integrity Protocol

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

- Ένα κρυπτογραφικό Message Integrity Code (MIC) με την ονομασία Michael.
- Ένα κανόνα διαδοχής των IV.
- Μια συνάρτηση ανάμειξης για την παραγωγή μοναδικών κλειδιών ανά frame.
- Ένα μηχανισμό αλλαγής του κοινού κλειδιού που γίνεται πλέον προσωρινό.

4.4.1 Michael

Κάθε MIC έχει τρία στοιχεία: ένα κρυφό κλειδί πιστοποίησης K κοινό μόνο μεταξύ αποστολέα και παραλήπτη, ένα αλγόριθμο παραγωγής του MIC και κάποια διαδικασία επαλήθευσης. Ο αλγόριθμος έχει ως εισόδους το κλειδί K και το μήνυμα M και στην έξοδό του παράγει την ακολουθία (tag) T. Ο αποστολέας στέλνει τα M και T. Για τον έλεγχο της ακεραιότητας των δεδομένων, ο παραλήπτης ξανα-υπολογίζει το T και αν T=T' τότε τα δεδομένα θεωρούνται αυθεντικά.
Το κλειδί του Michael έχει μήκος 64bit χωρισμένα σε δύο λέξεις των 32bit (K0,K1). Στην αρχή τα δεδομένα συμπληρώνονται με την τιμή 0x5A και αρκετά μηδενικά ώστε το μήκος τους να είναι πολλαπλάσιο του 32 και στην συνέχεια χωρίζονται σε λέξεις των 32bit M1 M2 … Mn. Τέλος, υπολογίζεται το T:



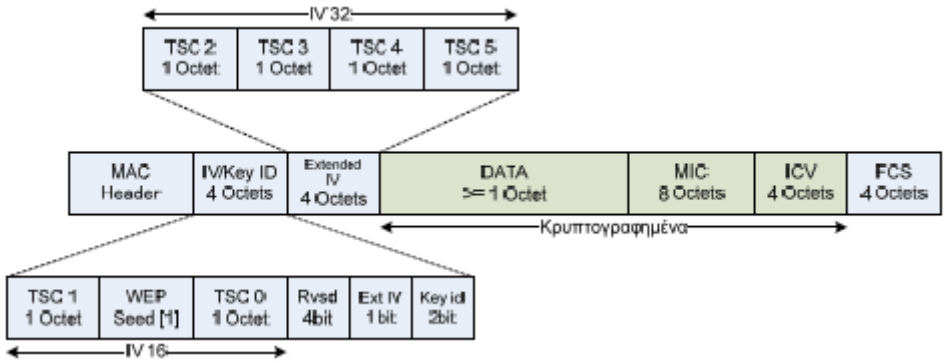
Εικόνα 4.6

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

4.4.2 Επιλογή και χρήση IV

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

- Το μήκος του IV αυξάνεται από 24 στα 48bit.
- Το IV παίζει πλέον και τον ρόλο του αναγνωριστικού του πακέτου (Packet Number, PN) για την αποφυγή επιθέσεων επανάληψης.
- Αποκλείονται τα αδύναμα IV της επίθεσης των Flurer-Martin-Shamir.



Εικόνα 4.7

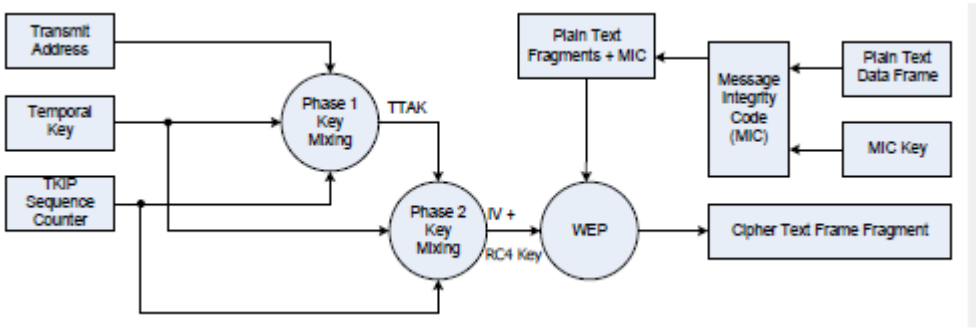
Όπως φαίνεται και στο σχήμα χ.χ, για την αύξηση του μήκους του IV προστέθηκαν 32 επιπλέον bit μεταξύ της αρχικής κεφαλίδας του πλαισίου και των κρυπτογραφημένων δεδομένων. Μαζί τα 24 αρχικά bit, το συνολικό μήκος του IV είναι 56bit. Για να αποκλειστούν τα αδύναμα IV της κλάσης B+3:FF:N, το ένα byte απορρίπτεται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

4.4.3 Αλγόριθμος Ανάμειξης Κλειδιών

Η πλειοψηφία των επιθέσεων κατά του WEP προϋποθέτουν την συλλογή αρκετών πακέτων (packet sniffing) κρυπτογραφημένων με το ίδιο κλειδί. Ο στόχος του μηχανισμού ανάμειξης κλειδιών είναι το κάθε πακέτο πληροφορίας να κρυπτογραφείται με διαφορετικό, μοναδικό κλειδί. Στην παραγωγή του μοναδικού κλειδιού συμμετέχουν η διεύθυνση MAC του αποστολέα (transmit address,TA), το TSC και το προσωρινό κλειδί που είναι κοινό μεταξύ αποστολέα και παραλήπτη. Η ανάμειξη γίνεται σε δύο φάσεις.
Στην πρώτη φάση γίνεται ανάμειξη της TA, των 32 πιο σημαντικών bit του TSC και των 80 πιο σημαντικών bit του προσωρινού κλειδιού. Για να αποφευχθεί επιβάρυνση του επεξεργαστή, η ανάμειξη περιλαμβάνει μόνο απλές πράξεις όπως πρόσθεση, AND και XOR. Το αποτέλεσμα της πρώτης φάσης είναι μια ακολουθία 80bit που στο πρότυπο ονομάζεται TKIP mixed Transmit Address and Key, TTAK.
Στην δεύτερη φάση του αλγόριθμου ανάμειξης κλειδιών συμμετέχουν το TTAK, το πλήρες προσωρινό κλειδί και το TSC. Και στη δεύτερη φάση, η ανάμειξη γίνεται με πράξεις μικρού επεξεργαστικού κόστους. Το αποτέλεσμα είναι το κλειδί που χρησιμοποιείται από το WEP, το λεγόμενο WEP seed, με μήκος 128bit.

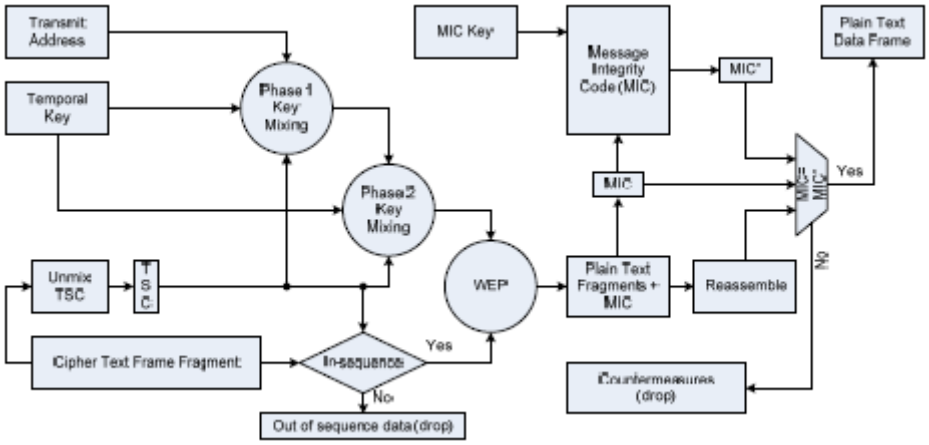
4.4.4 Δημιουργία Πλαισίων TKIP

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



Εικόνα 4.8

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



Εικονα 4.9

Για την ανάκτηση των αρχικών δεδομένων ακολουθείται η διαδικασία του. Σχήματος 4.9. Αρχικά, ο παραλήπτης υπολογίζει το WEP seed όπως και ο αποστολέας και εάν το πακέτο έχει το TSC που πρέπει. Εάν όχι, το πακέτο απορρίπτεται πριν αποκρυπτογραφηθεί. Στην συνέχεια τα τμήματα αποκρυπτογραφούνται και επανενώνονται στο αρχικό μήνυμα. Τέλος, ο παραλήπτης υπολογίζει το MIC και το συγκρίνει με αυτό του αποστολέα. Εάν το αποτέλεσμα είναι διαφορετικό, υποτίθεται ότι το δίκτυο δέχεται επίθεση. Στην περίπτωση αυτή, έχουν λαμβάνονται κάποια αντίμετρα για την αποτροπή της επίθεσης. Τα αντίμετρα αυτά είναι η απόρριψη του πακέτου και η αποβολή του αποστολέα από το δίκτυο για ένα λεπτό.

4.4.5 Αδυναμίες του TKIP

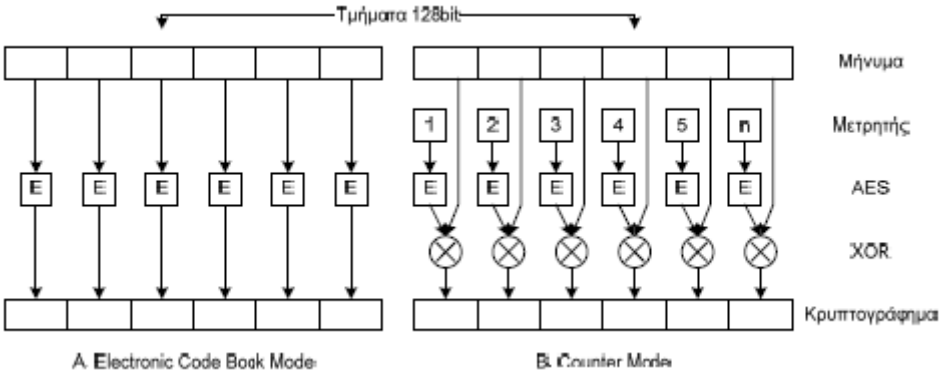
Το μόνο πρόβλημα που έχει αναφερθεί στο TKIP είναι η χρησιμοποίηση των αντίμετρων του Michael για την πραγματοποίηση επίθεσης άρνησης υπηρεσίας. Η επίθεση είναι τόσο δύσκολη που παραμένει θεωρητική. Γενικά, η μέθοδος που θα πρέπει να χρησιμοποιηθεί είναι όμοια με τις επιθέσεις man-in-the-middle. Αρχικά,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

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

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

4.5.1 Counter Mode

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

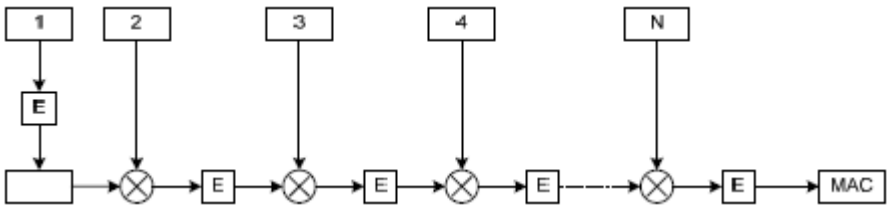


Εικόνα 4.10

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

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

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



Εικόνα 4.11

Το αποτέλεσμα των διαδοχικών μίξεων και κρυπτογραφήσεων είναι μια ακολουθία 128bit που περιέχει πληροφορίες απ' όλα τα τμήματα του καθαρού κειμένου. Η

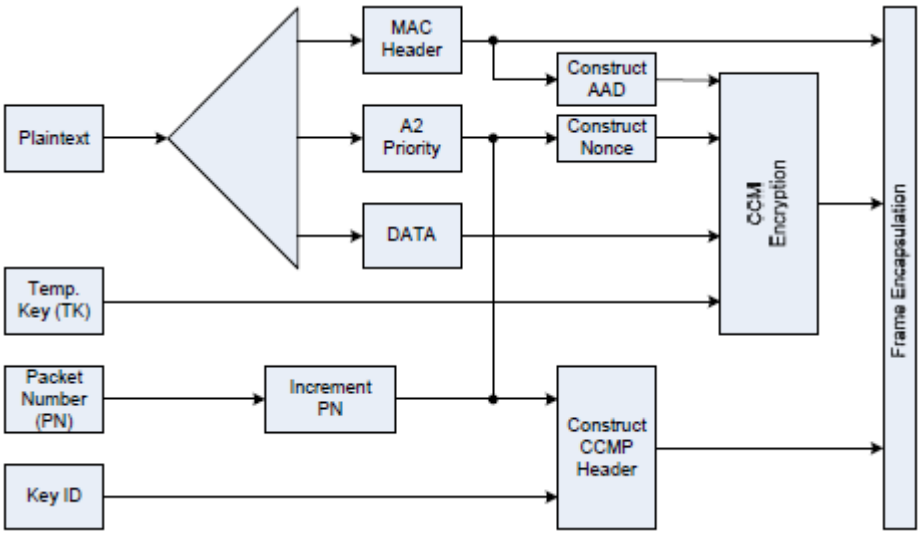
πιθανότητα να έχει αλλοιωθεί το αρχικό μήνυμα και να έχει το ίδιο MAC (ή MIC κατά το IEEE6) είναι μια στα $3,4*10^{38}$.

4.5.3 Counter Mode + CBC MAC = CCM

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

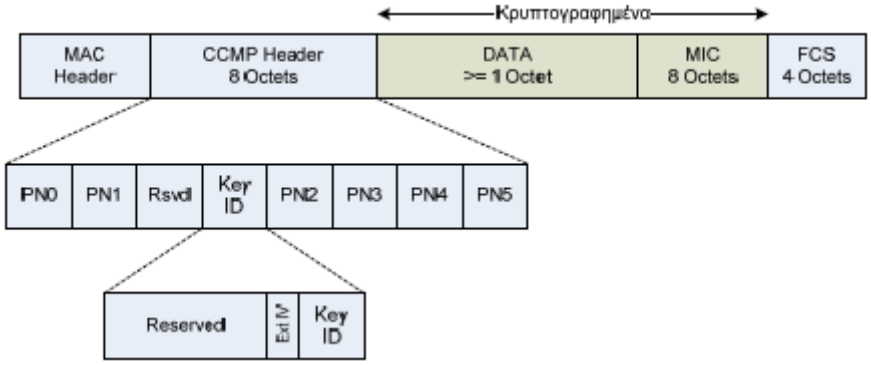
4.5.4 Λειτουργία του CCM Protocol

Το πρώτο βήμα για την κρυπτογράφηση στο CCMP είναι ο υπολογισμός του MIC. Ο MIC υπολογίζεται με βάση το σώμα του πλαισίου αλλά και την κεφαλίδα MAC που στο πρότυπο 802.11i αναφέρεται ως Additional Authenticated Data (AAD).



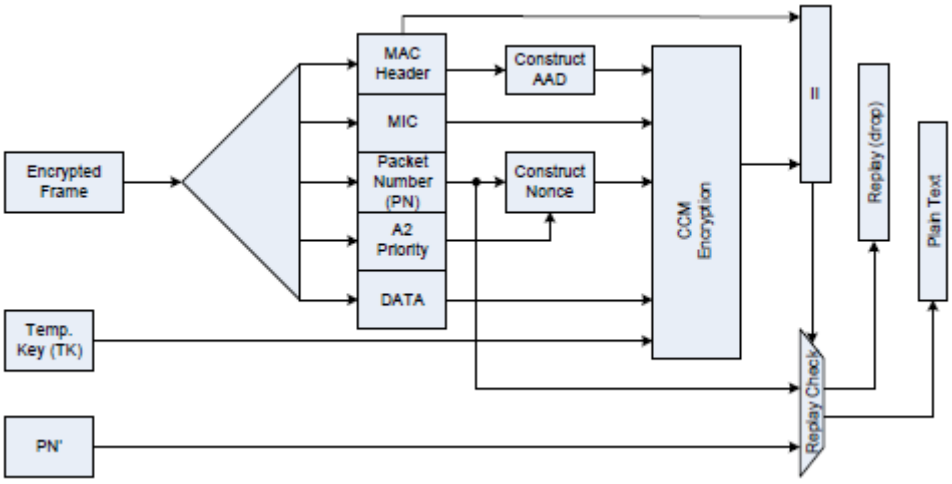
Εικόνα 4.12

Ο MIC υπολογίζεται σύμφωνα με το CBC MAC με κάποιες διαφοροποιήσεις. Το αρχικό τμήμα των 128bit που κρυπτογραφείται δεν είναι το πρώτο τμήμα του καθαρού κειμένου(εικόνα 4.11) αλλά το nonce για να διασφαλίζεται η μοναδικότητά του. Το nonce αποτελείται από τρία τμήματα: Την διεύθυνση MAC του αποστολέα, τον αναγνωριστικό αριθμό του πακέτου Packet Number (PN) και την τιμή Priority που είναι σταθερή, προς το παρόν, και προορίζεται για μελλοντική χρήση. Κατά τ' άλλα, ο υπολογισμός του κώδικα ακεραιότητας υπολογίζεται κατά τα γνωστά με αποτέλεσμα μια ακολουθία των 128bit. Ο τελικός MIC που χρησιμοποιείται στο πλαίσιο(εικόνα 4.13) είναι τα 64 πιο σημαντικά bits της παραπάνω ακολουθίας.



Εικόνα 4.13

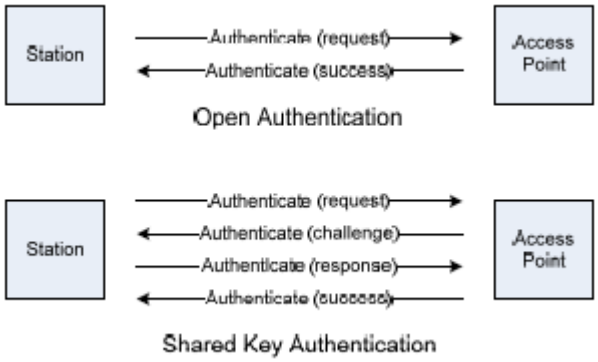
Μετά τον υπολογισμό του MIC, τα πεδία της κεφαλίδας του CCMP έχουν συμπληρωθεί και η διαδικασία μπορεί να προχωρήσει με την κρυπτογράφηση των πεδίων του μηνύματος και του MIC. Η διαδικασία κρυπτογράφησης είναι αυτή του Counter Mode (4.10) με κάποιες τροποποιήσεις, όπως και στην περίπτωση του CBC MAC. Όπως έχει ήδη αναφερθεί, η αρχική τιμή του μετρητή είναι η nonce, η ίδια με αυτή που χρησιμοποιήθηκε για τον MIC. Όπως και στην περίπτωση του TKIP, το κλειδί της κρυπτογράφησης δημιουργείται κατά την διαδικασία πιστοποίησης του χρήστη ή του τερματικού και μπορεί να αλλάζει ανά τακτά χρονικά διαστήματα (temporal keys) αλλά πάντα καταστρέφεται κατά την αποσύνδεση.



Εικόνα 4.14

4.6 Πιστοποίηση πριν το 802.11i

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



Εικόνα 4.15

Στον δεύτερο τρόπο πιστοποίησης του 802.11 γίνεται έλεγχος του κοινού κλειδιού του WEP. Αρχικά, ο σταθμός στέλνει μια αίτηση για συμμέτοχη στο δίκτυο. Στην συνέχεια, το AP του στέλνει ένα τυχαίο αριθμό, το challenge text. Ο σταθμός λαμβάνει το challenge text, το κρυπτογραφεί με το WEP και το στέλνει πίσω στο AP. Το AP αποκρυπτογραφεί την απάντηση με το κοινό κλειδί και την συγκρίνει με το αρχικό challenge text. Αν οι δύο αριθμοί ταυτίζονται, δηλαδή ο σταθμός έχει το σωστό κλειδί, η αίτηση εγκρίνεται. Σε διαφορετική περίπτωση η αίτηση απορρίπτεται. Η παραπάνω μέθοδος έχει τρία βασικά αρνητικά σημεία. Πρώτον, η πιστοποίηση αυτού του τύπου είναι μονόδρομη. Το δίκτυο πιστοποιεί τον χρήστη αλλά ο χρήστης δεν έχει δυνατότητα πιστοποίησης του δικτύου. Δεύτερον, αν κάποιος υποκλέψει μια επιτυχημένη διαδικασία πιστοποίησης, μπορεί πολύ εύκολα, με XOR μεταξύ του μη κρυπτογραφημένου challenge text και της κρυπτογραφημένης απάντησης, να αποκαλύψει όλο το key stream. Τελευταίο και σημαντικότερο, με αυτή τη μέθοδο δεν πιστοποιείται η ταυτότητα του χρήστη αλλά το γεγονός ότι ένα μηχάνημα έχει ρυθμιστεί με το σωστό κοινό κλειδί. Κανένας δεν εμποδίζει ένα μη πιστοποιημένο χρήστη να χρησιμοποιήσει ένα πιστοποιημένο σταθμό. Επιπλέον, όπως έχει αναφερθεί, η αποκάλυψη του κοινού κλειδιού είναι αρκετά εύκολη οπότε και η πιστοποίηση του σταθμού δεν μπορεί να είναι στεγανή.

Η χρήση shared key authentication ταυτόχρονα με την χρήση του WEP δεν είναι υποχρεωτική από το πρότυπο αλλά δίνεται σαν επιλογή. Τα παραπάνω προβλήματα, και ιδιαίτερα το δεύτερο, καθιστούν την χρήση της ανοιχτής πιστοποίησης ασφαλέστερη. Ωστόσο, η συνύπαρξη open authentication και WEP δημιουργεί κάποια διαχειριστικά προβλήματα. Για παράδειγμα, ένας σταθμός με λάθος κλειδί θα φαίνεται κανονικά συνδεδεμένος στο δίκτυο αλλά όλα τα πακέτα θα απορρίπτονται κάνοντας την επικοινωνία αδύνατη.

4.7 Πιστοποίηση μετά το 802.11i

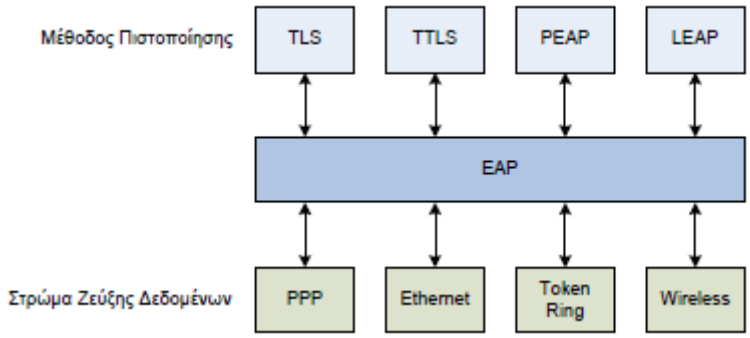
Όπως είδαμε, οι μηχανισμοί πιστοποίησης του αρχικού προτύπου 802.11 παρέχουν μηδενικό επίπεδο ασφάλειας. Η λύση αναζητήθηκε, αρχικά από την WiFi Alliance και στην συνέχεια από το TGi, σε ήδη υπάρχουσες τεχνολογίες. Παρατηρήθηκε ότι υπάρχει αναλογία στα θέματα πιστοποίησης μεταξύ των ασυρμάτων δικτύων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

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

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

4.8 Extensible Authentication Protocol

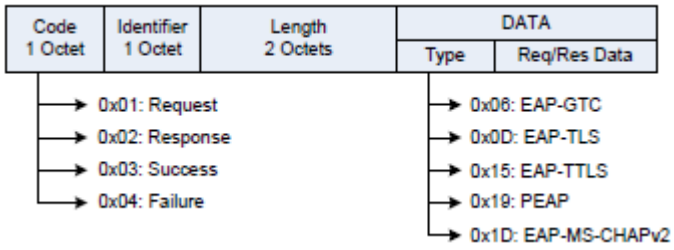
Το EAP είναι ένα ευέλικτο πρωτόκολλο μεταφοράς πληροφοριών πιστοποίησης. Επίσημα, παρουσιάστηκε στο RFC 2284 της IETF, ένα έγγραφο δεκαέξι μόλις σελίδων και αρχικά αναπτύχθηκε για χρήση με το Point to Point Protocol (PPP) στις dial-up συνδέσεις. Το EAP έχει δύο βασικά και πολύ χρήσιμα χαρακτηρίστηκα.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



Εικόνα 4.16

Το RFC 2284 ορίζει τέσσερις τύπους μηνυμάτων:

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



Εικόνα 4.17

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

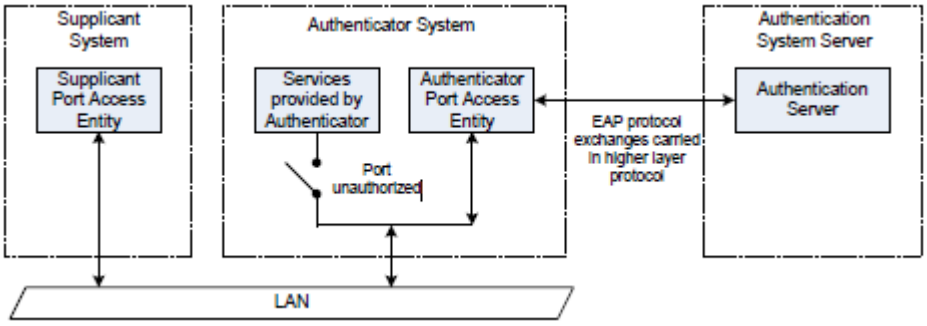
1. Identity
2. Notification
3. NAK (μόνο response)
4. MD5-Challenge
5. One-Time Password (OTP)
6. Generic Token Card (GTC)

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

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

4.9 802.1x: Port-Based Network Access Control

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



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

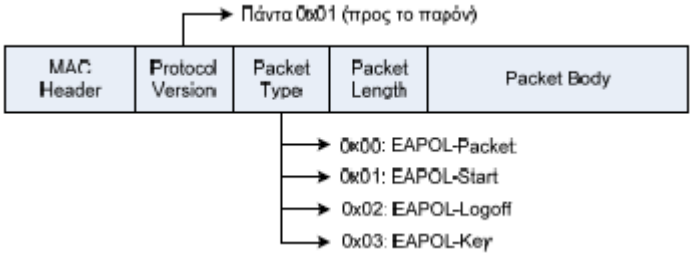
- Τους αιτούντες (supplicants) που ζητούν πρόσβαση στο δίκτυο.
- Τους πιστοποιητές (authenticators) που ελέγχουν την πρόσβαση στο δίκτυο.
- Τους εξυπηρετητές πιστοποίησης (authentication servers) που λαμβάνουν τις αποφάσεις για την πρόσβαση.

Στην περίπτωση των ασυρμάτων δικτύων, αιτούντες είναι όλοι οι σταθμοί που συμμετέχουν στο BSS και πιστοποιητής είναι το Access Point. Όπως φαίνεται και στο σχήμα, αρχικά ο κάθε supplicant μπορεί να έχει πρόσβαση μόνο στον AS. Πρακτικά, έχει πρόσβαση και σε όλες τις άλλες υπηρεσίες, όπως σε DHCP servers, που είναι αναγκαίες για την επικοινωνία με τον AS, αλλά η πρόσβαση στις άλλες υπηρεσίες

του authenticator, δηλαδή τους πόρους του δικτύου, είναι απαγορευμένη. Εάν η διαδικασία πιστοποίησης είναι επιτυχής, τότε ο authenticator παρέχει στον supplicant πλήρη πρόσβαση στους πόρους του δικτύου.
Όπως και στην περίπτωση του EAP, το 802.1x δίνει μόνο το πλαίσιο λειτουργίας και όχι τις επιμέρους λεπτομέρειες της πιστοποίησης που τις αφήνει, αόριστα, σε πρωτόκολλα ανωτέρου στρώματος.

4.9.1 EAP over LAN

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



Εικόνα 4.18

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

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

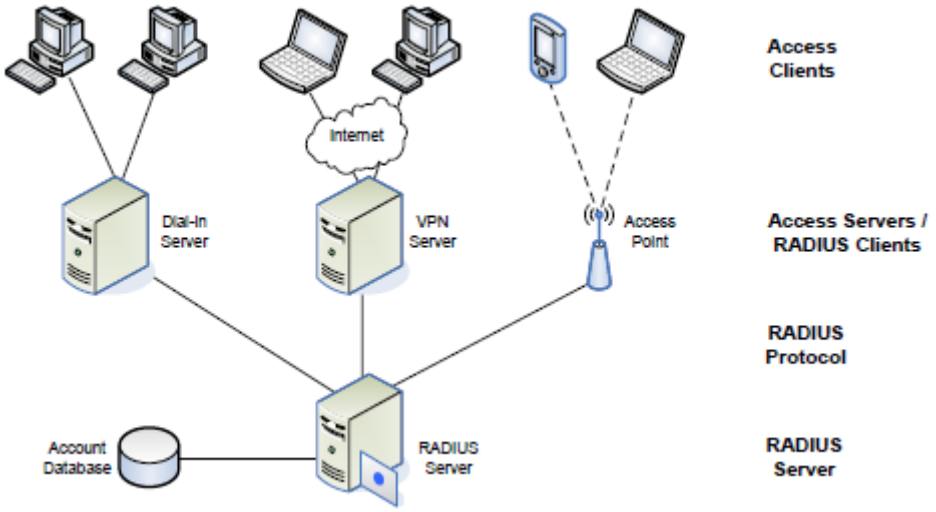
Ο τελευταίος τύπος δεν έχει υιοθετηθεί από την WiFi και δεν χρησιμοποιείται στα ασύρματα δίκτυα.
Όταν ένας χρήστης επιχειρεί να συνδεθεί στο δίκτυο δεν μπορεί να ξέρει αν υπάρχει authenticator και ακόμη περισσότερο λεπτομέρειες όπως η MAC διεύθυνσή του. Για να ξεκινήσει η διαδικασία πιστοποίησης, ο client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

4.10. Remote Access Dial-in User Service (RADIUS)

Στην παράγραφο του 802.1x έγινε αναφορά για την ανάγκη ύπαρξης ενός εξυπηρετητή πιστοποίησης. Ούτε το πρότυπο 802.1x αλλά ούτε και το 802.11i αναφέρεται στον τύπο αυτού του server και στον τρόπο επικοινωνίας με τους πιστοποιητές και τους αιτούντες. Στο 802.11i γίνεται αναφορά σε δύο τύπους, στον RADIUS και στον Diameter, που θα μπορούσαν να χρησιμοποιηθούν αλλά όχι υποχρεωτικά. Οι λόγοι που αναφέρομαι συγκεκριμένα στο RADIUS και όχι στον Diameter ή στον TACACS ή σε οποιονδήποτε άλλο είναι ότι ο RADIUS χρησιμοποιήθηκε στο πειραματικό μέρος της εργασίας, είναι ανοιχτό πρότυπο και ολοκληρώνεται στο γνωστότερο λειτουργικό σύστημα για servers7.
Το RADIUS είναι ο τρόπος του IETF για το λεγόμενο AAA (Authentication, Authorization, Accounting). Ένα ολοκληρωμένο σύστημα AAA περιγράφει τον τρόπο που γίνεται η πιστοποίηση των χρηστών, η εξουσιοδότησή τους στους πόρους του δικτύου και την καταγραφή των δραστηριοτήτων τους, αλλά και είναι ένα πρωτόκολλο επικοινωνίας μεταξύ των πιστοποιητών και του εξυπηρετητή πιστοποίησης. Το IETF έχει εκδώσει διάφορα πρότυπα ανάλογα με την τεχνολογία που χρησιμοποιείται στο στρώμα ζεύξης δεδομένων αλλά και της τεχνολογίας του πλαισίου λειτουργίας της πιστοποίησης. Τα πρότυπα που εμπλέκονται στα ασύρματα δίκτυα είναι τα:

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

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



Εικόνα 4.19

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

Εικόνα 4.20

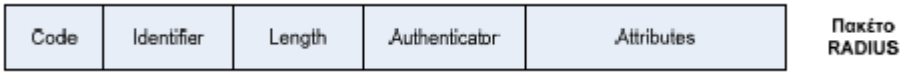
4.10.1. Μηνύματα πρωτοκόλλου RADIUS

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

- **Access-Request** Στέλνεται από τους RADIUS clients για κάθε νέα προσπάθεια εισόδου στο δίκτυο.
- **Access-Accept** Στέλνεται από τον RADIUS server ως απάντηση στο Access-Request. Πληροφορεί τον RADIUS client ότι η προσπάθεια εισόδου στο δίκτυο έχει πιστοποιηθεί και εξουσιοδοτηθεί.
- **Access-Reject** Στέλνεται από τον RADIUS server ως απάντηση στο Access-Request. Πληροφορεί τον RADIUS client ότι η αίτηση εισόδου στο δίκτυο έχει απορριφθεί. Στέλνεται σε περίπτωση που τα διαπιστευτήρια του χρήστη δεν ισχύουν.
- **Access-Challenge** Στέλνεται από τον RADIUS server ως απάντηση στο Access-Request. Σκοπός του είναι να εξακριβώσει την ταυτότητα του RADIUS client.
- **Accounting-Request** Στέλνεται από τους RADIUS clients και περιέχει πληροφορίες σχετικά με την χρήση του δικτύου.
- **Accounting-Response** Στέλνεται από τον RADIUS server ως απάντηση στο Accounting-Request. Πληροφορεί τον RADIUS client ότι το μήνυμα έχει ληφθεί με επιτυχία.

4.10.2 Πλαισίωση Μηνυμάτων RADIUS

Ένα πακέτο του πρωτοκόλλου RADIUS αποτελείται από πέντε πεδία και έχει την μορφή της εικόνας 4.21.



Εικόνα 4.21

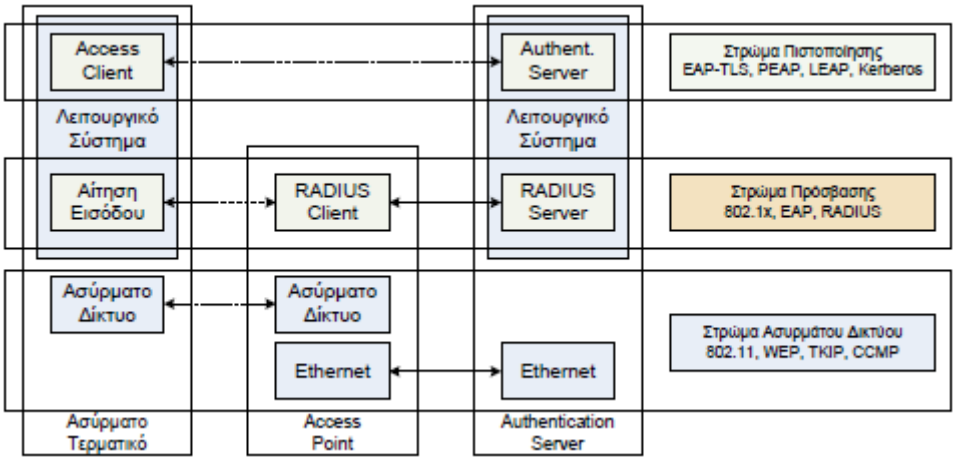
Πρώτο είναι το πεδίο του κωδικού του μηνύματος και η τιμή του εξαρτάτε από τον τύπο του μηνύματος. Για τα τέσσερα μηνύματα πιστοποίησης οι τιμές είναι:

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

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

4.11 Μέθοδοι Πιστοποίησης Ανωτέρου Στρώματος

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



Εικόνα 4.22

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

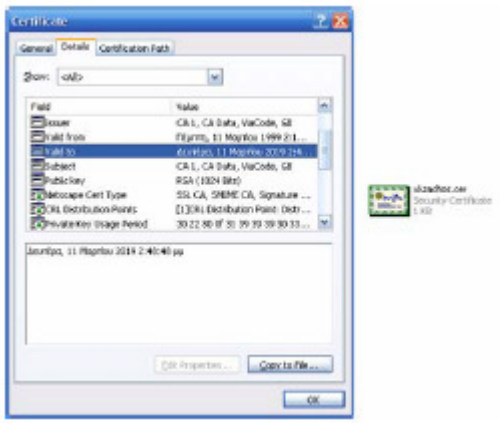
4.11.1. Transport Layer Security (TLS)

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

4.11.2 Ψηφιακές Υπογραφές, Ψηφιακά Πιστοποιητικά και Αρχές Έκδοσης

Όπως έχει περιγραφεί στην παράγραφο Αρχές Κρυπτογράφησης, υπάρχουν δύο είδη κρυπτογράφησης, η συμμετρική και η ασύμμετρη. Η ασύμμετρη κρυπτογράφηση αναφέρεται και ως κρυπτογράφηση δημόσιου κλειδιού (public key). Στην κρυπτογράφηση δημόσιου κλειδιού χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση. Από τα δύο κλειδιά, το κλειδί της κρυπτογράφησης είναι δημόσιο και γνωστό σε όλους. Το κλειδί της

αποκρυπτογράφησης είναι ιδιωτικό και γνωστό μόνο σε ένα μέλος. Το δημόσιο κλειδί προκύπτει μαθηματικά από το ιδιωτικό. Κατά την κρυπτογράφηση, ο αποστολέας χρησιμοποιεί το δημόσιο κλειδί του παραλήπτη και ο παραλήπτης χρησιμοποιεί το αντίστοιχο ιδιωτικό για την αντίστροφη διαδικασία.
Εκτός από την κρυπτογράφηση δεδομένων, η κρυπτογράφηση δημόσιου κλειδιού χρησιμοποιείται στην δημιουργία ψηφιακών υπογραφών. Η ψηφιακή υπογραφή είναι ένας τρόπος ελέγχου της ταυτότητας του αποστολέα και της ακεραιότητας του μηνύματος.
Για την δημιουργία ψηφιακής υπογραφής, αρχικά, υπολογίζεται ένα hash του μηνύματος. Το hash είναι μια μαθηματική περίληψη των δεδομένων του μηνύματος. Στην συνέχεια, ο αποστολέας κρυπτογραφεί το hash χρησιμοποιώντας το ιδιωτικό του κλειδί. Η ψηφιακή υπογραφή είναι το κρυπτογραφημένο hash. Όταν ο παραλήπτης λάβει το μήνυμα αποκρυπτογραφεί την ψηφιακή υπογραφή με το δημόσιο κλειδί του αποστολέα και υπολογίζει το hash. Αν οι δύο τιμές είναι ίσες τότε ο παραλήπτης μπορεί είναι βέβαιος για την ταυτότητα του αποστολέα και την ακεραιότητα του μηνύματος.
Η μαθηματική εξάρτηση μεταξύ του ιδιωτικού και του δημόσιου κλειδιού εξασφαλίζει στον παραλήπτη ότι ο αποστολέας έχει το ιδιωτικό κλειδί. Το πρόβλημα με την ψηφιακή υπογραφή είναι ότι από μόνη της δεν μπορεί να βεβαιώσει την ταυτότητα αυτού που την εκδίδει. Όπως και στην πραγματικότητα, χρειάζεται μια αρχή που ο χρήστης να μπορεί να εμπιστευτεί και να βεβαιώσει την γνησιότητά της. Στην περίπτωσή μας, αυτή η Τρίτη οντότητα είναι η Αρχή Έκδοσης Ψηφιακών Πιστοποιητικών (Certification Authority, CA). Μια CA μπορεί να είναι ένας εξυπηρετητής σε εταιρικά δίκτυα ή κάποια εταιρία που παρέχει τέτοιου είδους υπηρεσίες στο Internet.
Η πιστοποίηση της γνησιότητας και ακεραιότητας μιας ψηφιακής υπογραφής γίνεται μέσω αντιστοίχισης του δημόσιου κλειδιού με το πρόσωπο ή τη συσκευή ή την υπηρεσία που κρατάει το ιδιωτικό κλειδί. Αυτή η αντιστοίχιση επιτυγχάνεται με τα ψηφιακά πιστοποιητικά



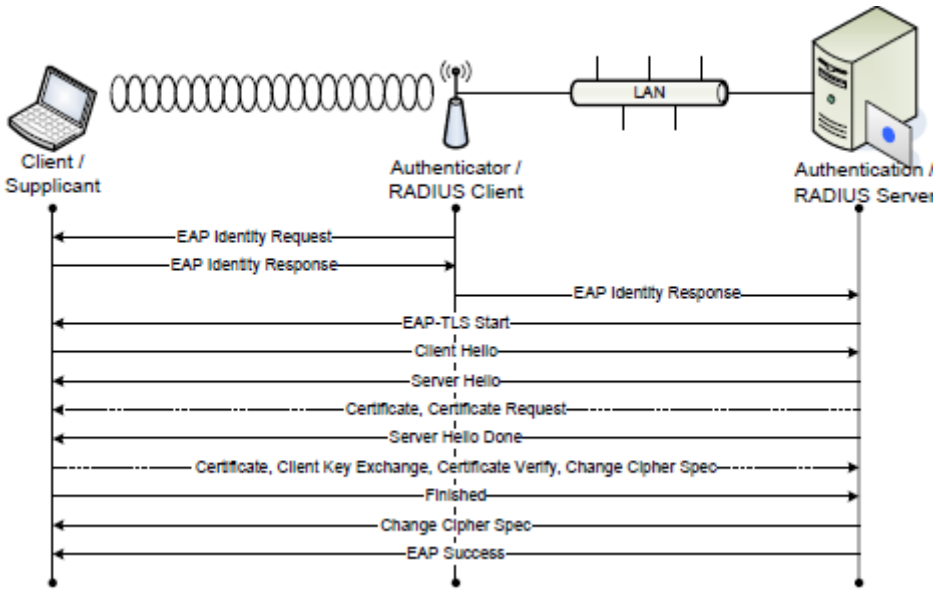
Το ψηφιακό πιστοποιητικό είναι μια δομή δεδομένων που εκδίδεται από μια CA και μεταξύ άλλων περιέχει το δημόσιο κλειδί. Η δομή του ακολουθεί κάποιο πρότυπο όπως το X.509 και είναι ψηφιακά υπογεγραμμένο από την CA που το εκδίδει. Οι πληροφορίες που περιέχει φαίνονται παρακάτω:

- **Subject** Πληροφορίες για την οντότητα που κατέχει το ιδιωτικό κλειδί. Μπορεί να είναι χρήστης, υπολογιστής ή κάποια υπηρεσία ενός Η/Υ.

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

4.11.3 Πιστοποίηση με EAP-TLS

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



Εικόνα 4.23

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

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

4.11.4 Πιστοποίηση με Protected EAP

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

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

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

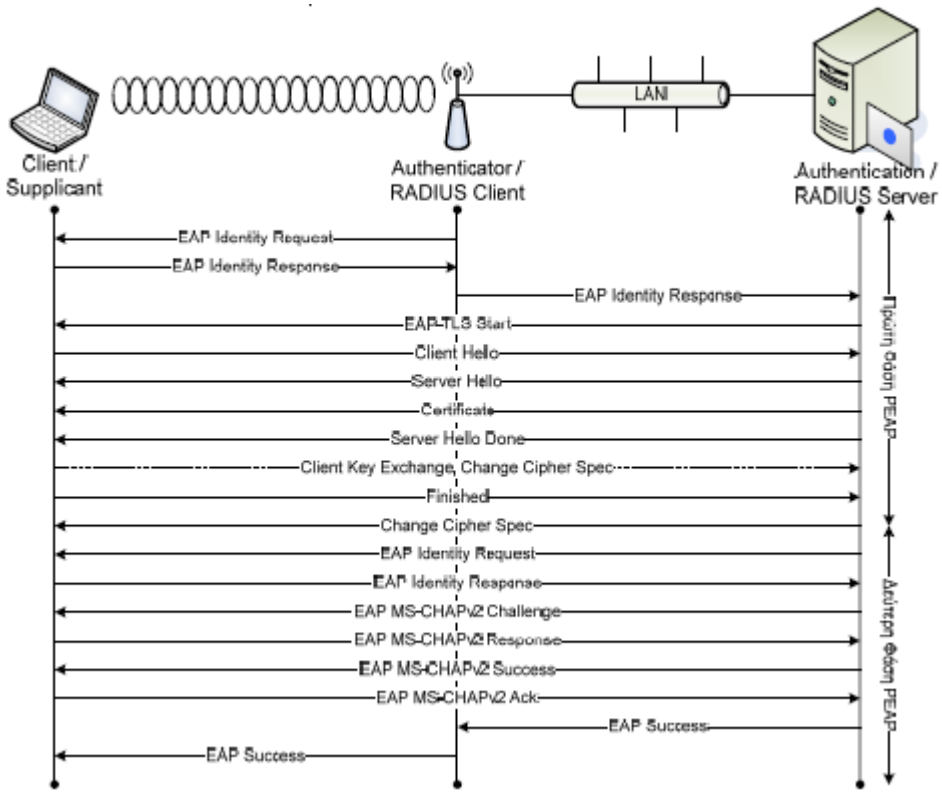
Το πρωτόκολλο πιστοποίησης που θα χρησιμοποιηθεί κατά την φάση της πιστοποίησης του χρήστη μπορεί να είναι και πάλι το TLS ή και οποιοδήποτε άλλο. Τα πρότυπα WPA/WPA2 προβλέπουν την χρήση του PEAP με MSCHAPv2 και EAP-GTC. Στο πειραματικό μέρος της εργασίας έχει χρησιμοποιηθεί το πρώτο.

4.11.5 PEAP MS-CHAPv2

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

Φάση 1η: Δημιουργία TLS τούνελ

- Μετά την σύνδεση του client, το AP του στέλνει ένα μήνυμα Identity Request.
- Ο client ανταποκρίνεται με ένα μήνυμα Identity Response με ανώνυμο περιεχόμενο. Το μήνυμα προωθείται στον Authentication Server. Από το σημείο αυτό τα μηνύματα δεν αφορούν το AP.
- Εκκινεί η συνεδρία του EAP-TLS με το client να στέλνει τις απαραίτητες πληροφορίες για τα υποστηριζόμενα πιστοποιητικά.
- Απάντηση του server και αποστολή του πιστοποιητικού του.
- Δημιουργία των pre-master και master key της σύνδεσης.
- Εκκίνηση της λειτουργίας των αλγόριθμων κρυπτογράφησης και τέλος της πρώτης φάσης.



Εικόνα 4.24

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

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

Στο τέλος της διαδικασίας και τα δύο μέρη έχουν αποδείξει ότι γνωρίζουν το password του χρήστη οπότε και υπάρχει αμοιβαία πιστοποίηση. Γενικά, η πιστοποίηση μέσω password θεωρείται λιγότερο ασφαλείς από αυτή που χρησιμοποιεί ψηφιακά πιστοποιητικά. Ειδικότερα, όπως και όλες οι διαδικασίες που περιλαμβάνουν εισαγωγή password από τους χρήστες, μπορεί να γίνει επίθεση είτε με λεξικό passwords8, είτε επίθεση brute force[9].

Στην περίπτωση του PEAP MS-CHAPv2 δεν μπορεί να ισχύει κάτι τέτοιο για δύο λόγους. Στην πρώτη φάση, η ταυτότητα του server πιστοποιείται με ψηφιακό πιστοποιητικό. Στην δεύτερη φάση, αυτό του απασχολεί τον επιτιθέμενο δεν είναι τα passwords αλλά η κρυπτογράφηση.

4.12 Preshared Key

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

4.13 Ασφάλεια και Απόδοση

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

4.14 Πρωτόκολλο IPSec

Τα πρωτόκολλα TCP/IP δεν παρέχουν μηχανισμούς κρυπτογράφησης. Συνεπώς, για την ασφαλή μετάδοση πάνω σε δίκτυο IP υπήρξε η ανάγκη νέου πρωτοκόλλου με μηχανισμούς κρυπτογράφησης, το οποίο θα είναι εφαρμόσιμο σε IP δίκτυα. Το IPSec (IP Security) αποτελεί ένα σύνολο πρωτοκόλλων ανεπτυγμένων από το Internet Engineering Task Force (IETF) με στόχο την ασφαλή μετάδοση και ανταλλαγή δεδομένων (packets) μέσω του στρώματος IP. Το IPSec σήμερα αποτελεί έναν από τους πιο διαδεδομένους τρόπους υλοποίησης των δικτύων VPN. Ως προς τα επίπεδα του OSI, αντιστοιχίζεται στο επίπεδο 3 (επίπεδο δικτύου).
Τα θέματα ασφάλειας που ανακύπτουν με τη χρησιμοποίηση του Διαδικτύου για τη πραγματοποίηση ιδιωτικών επικοινωνιών είναι τα ακόλουθα:

• Απώλεια της Ιδιωτικότητας των Δεδομένων (Loss of Privacy): Σ' αυτήν την περίπτωση ένας μη εξουσιοδοτημένος χρήστης που έχει καταφέρει να εισχωρήσει σε κάποιο δίκτυο έχει τη δυνατότητα να παρακολουθεί εμπιστευτικά δεδομένα κατά τη διακίνησή τους στο Internet.

• Απώλεια Ακεραιότητας Δεδομένων (Loss of Data Integrity): Σ' αυτήν την περίπτωση ένας μη εξουσιοδοτημένος χρήστης αλλάζει τα δεδομένα που μεταφέρονται στο δίκτυο (π.χ. τους αριθμούς ενός λογαριασμού καταθέσεων)

- *Προσποίηση Ταυτότητας (Identity Spoofing)*: Σ' αυτήν την περίπτωση ένας μη εξουσιοδοτημένος χρήστης παριστάνει ότι είναι ένας νόμιμος χρήστης του δικτύου και ζητά πληροφορίες που σε διαφορετική περίπτωση δε θα μπορούσε να έχει.

• *Άρνηση Υπηρεσιών (Denial-of-Service)*: Σ' αυτήν την περίπτωση γίνεται "επίθεση" σε κάποιον server του δικτύου.

Ο βασικός στόχος στην ανάπτυξη του προτύπου IPSec είναι η αντιμετώπιση των παραπάνω απειλών χωρίς να απαιτείται πρόσθετος εξοπλισμός, ούτε να υπάρχει ανάγκη για ένα σύνολο τροποποιήσεων και αλλαγών σε διάφορες εφαρμογές.
Έτσι οι υπηρεσίες που προσφέρει το πρωτόκολλο IPSec είναι:

• **Ακεραιότητα των δεδομένων (Integrity)**, που διασφαλίζει ότι τα πακέτα των δεδομένων κατά την διάρκεια της μεταφοράς τους δεν έχουν αλλοιωθεί ή παραποιηθεί, είτε από «εισβολείς» είτε από τυχόν σφάλματα επικοινωνίας.

• **Εξακρίβωση γνησιότητας της προέλευσης των δεδομένων (Authentication) ή πιστοποίηση ταυτότητας,** που επαληθεύει ότι τα δεδομένα στάλθηκαν πράγματι από το χρήστη που ισχυρίζεται ότι τα έστειλε.

• **Εμπιστευτικότητα (Confidentiality),** που προσφέρει τη δυνατότητα αναγνώρισης και επεξεργασίας των δεδομένων μόνο από εγκεκριμένους χρήστες.

Το IPSec αναφέρεται σε μια σειρά πρωτοκόλλων όπως ορίζεται στα RFC 2401-2411 και RFC 2451. Αυτά τα πρωτόκολλα χωρίζονται σε δύο κύριες κατηγορίες:

► *Πρωτόκολλα σχετικά με την ασφάλεια*, τα οποία καθορίζουν την πληροφορία που πρέπει να προστεθεί σε ένα IP πακέτο για να ενεργοποιηθούν οι έλεγχοι εμπιστευτικότητας, ακεραιότητας και πιστοποίησης ταυτότητας. Επίσης καθορίζεται και το πως πρέπει να γίνει η κρυπτογράφηση των δεδομένων του πακέτου.
► *Πρωτόκολλα σχετικά με την ανταλλαγή κλειδιών*, τα οποία διαπραγματεύονται το συσχετισμό ασφάλειας μεταξύ των δυο υποψήφιων προς επικοινωνίας οντοτήτων (θα επεξηγηθεί παρακάτω).

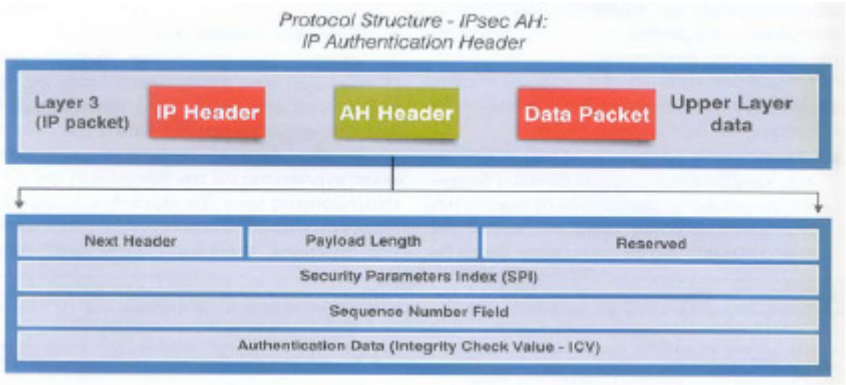
4.14.1 Μηχανισμοί Ασφάλειας

Το IPSec ορίζει ένα νέο σετ κεφαλίδων το οποίο προστίθεται στα IP πακέτα. Προκύπτουν έτσι καινούρια IP πακέτα μεγαλύτερα σε μέγεθος και άλλης δομής, που όμως επιτρέπουν τη διασφάλιση των απαιτήσεων ασφαλείας που περιγράφηκαν παραπάνω. Αυτές οι νέες κεφαλίδες, που διασφαλίζουν την ασφάλεια των IP πακέτων, αναλύονται παρακάτω:

- ✓ **Κεφαλίδα πιστοποίησης ταυτότητας (AH—Authentication Header)**: Αυτή η κεφαλίδα όταν προστίθεται σε ένα IP πακέτο, διασφαλίζει την ακεραιότητα, την πιστοποίηση ταυτότητας των δεδομένων, καθώς και την αποφυγή διπλότυπων πακέτων. Δεν παρέχει ασφάλεια εμπιστευτικότητας. Η ακεραιότητα και η πιστοποίηση πραγματοποιούνται και από τα δύο IPSec μέλη στις άκρες του tunnel εκτελώντας μία συνάρτηση κατακερματισμού στο IP πακέτο χρησιμοποιώντας ένα κοινό κλειδί (Message Authentication Code – MAC). Το αποτέλεσμα του υπολογισμού ο οποίος προκύπτει από τη συνάρτηση κατακερματισμού δεν κρυπτογραφείται και χρησιμοποιείται απλά από το άλλο συμβαλλόμενο μέρος για να ελέγξει ότι τα στοιχεία δεν έχουν τροποποιηθεί. Το γεγονός αυτό καθ' αυτό της χρησιμοποίησης ενός κοινού μυστικού κλειδιού που είναι γνωστό και στα δύο μέρη (αποστολέας-δέκτης) εγγυάται την πιστοποίηση της ταυτότητας των συμβαλλομένων.

Η κεφαλίδα πιστοποίησης ταυτότητας αποτελείται από 5 πεδία (εικόνα 4.25):

- Πεδίο επόμενης κεφαλίδας (Next Header field), όπου προσδιορίζει ποια είναι η επόμενη κεφαλίδα που είναι παρούσα στο IP πακέτο (π.χ. TCP, UDP κ.ο.κ.)
- Μέγεθος του φορτίου (Payload length)
- Δείκτης παραμέτρων ασφαλείας (Security Parameter Index (SPI)) – προσδιορίζει στον παραλήπτη ποια πρωτόκολλα ασφαλείας χρησιμοποιήθηκαν από τον αποστολέα
- Ακολουθιακός αριθμός (Sequence number): αυξάνεται κατά ένα για κάθε νέο πακέτο που καταφτάνει στον δέκτη από τον ίδιο αποστολέα και με το ίδιο SPI.
- Δεδομένα πιστοποίησης ταυτότητας (Authentication data) – το τμήμα εκείνο που εξασφαλίζει την πιστοποίηση ταυτότητας. Όπως ήδη αναφέρθηκε, είναι το αποτέλεσμα μίας συνάρτησης κατακερματισμού (Integration Check Value – ICV).



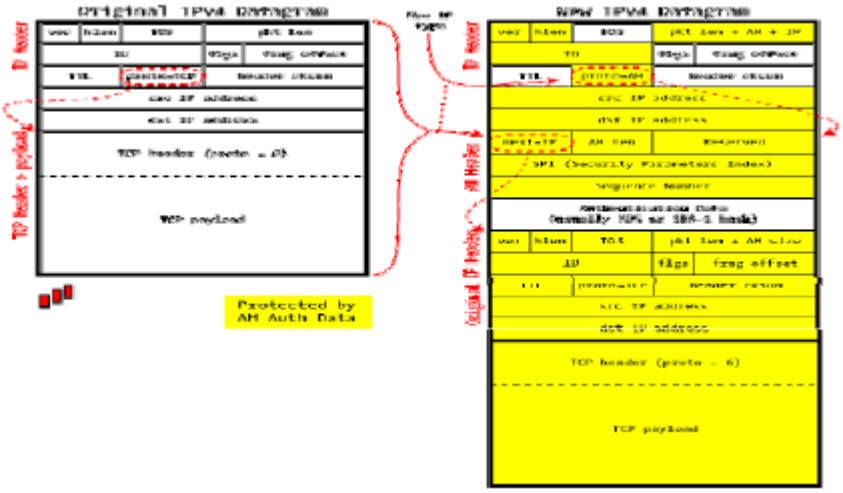
Εικόνα 4.25: Πεδία ενός AH Header.

Οι λειτουργίες ακεραιότητας και πιστοποίησης μέσω της κεφαλίδας πιστοποίησης εφαρμόζονται (εικόνα 4.26):

- Σε ολόκληρο το IP πακέτο, εκτός από εκείνα τα πεδία (IP header fields) που αλλάζουν κατά τη μεταφορά του όπως παραδείγματος χάριν το πεδίο TTL, που αλλάζει από τους δρομολογητές των διάφορων δικτύων (μειώνεται), κατά μήκος της πορείας που ακολουθεί το IP πακέτο.

- Σε όλο το AH header πλην του πεδίου του "Authentication Data" .

- Σε όλα τα δεδομένα των πάνω στρωμάτων της στοίβας πρωτοκόλλου (δεδομένα του IP πακέτου).

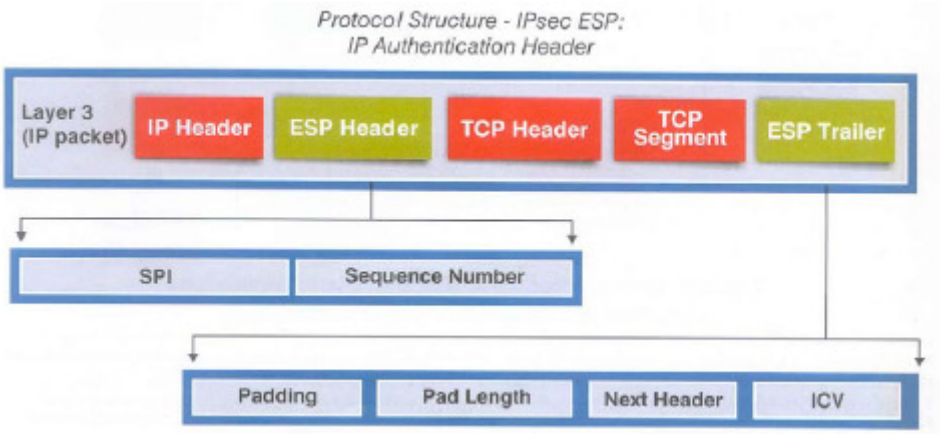


Εικόνα 4.26: Σύγκριση αρχικού IP πακέτου με το νέο, μετά την προσθήκη του AH.

✓ **Ασφαλής Ενθυλάκωση της πληροφορίας (Encapsulating Security Payload – ESP)**: Αυτή η κεφαλίδα παρέχει υπηρεσίες για την πιστοποίηση και ακεραιότητα των πακέτων IP που διαβιβάζονται μεταξύ δύο IPSec συστημάτων. Επιπρόσθετα παρέχει εμπιστευτικότητα μέσω μεθόδων κρυπτογράφησης. Η πιστοποίηση και η ακεραιότητα μπορούν να παρασχεθούν με τον ίδιο τρόπο που τα παρέχει και η κεφαλίδα AH. Το ESP παρέχει εμπιστευτικότητα με την κρυπτογράφησης ενός IP πακέτου. Το ESP υποστηρίζει ένα μεγάλο αριθμό συμμετρικών αλγορίθμων κρυπτογράφησης, αλλά η εξ ορισμού συνηθισμένη προεπιλογή είναι ο αλγόριθμος AES (128-

bit). Αυτό όμως δεν σημαίνει ότι δεν μπορούν να χρησιμοποιηθούν άλλοι αλγόριθμοι – όπως για παράδειγμα ο 3DES ή ο απλός DES.

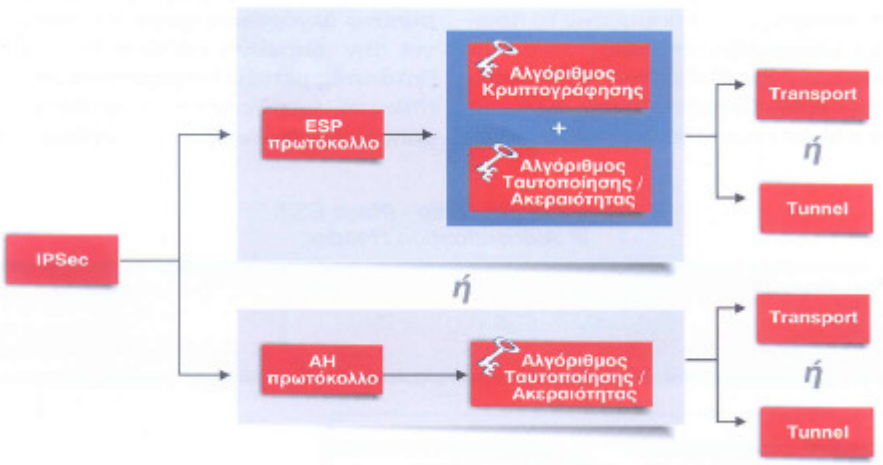
Τα πεδία της κεφαλίδας ESP είναι 6 – δύο από αυτά τοποθετούνται πριν το φορτίο του IP πακέτου (ESP Header) και τα υπόλοιπα τέσσερα μετά από αυτό (ESP Trailer) (εικόνα 4.27). Τα πεδία SPI και Sequence Number του ESP Header έχουν την ίδια λειτουργία όπως στο AH. Το ίδιο ισχύει για τα πεδία Pad Length, Next Header και ICV (το οποίο είναι προαιρετικό) του ESP Trailer. Το πεδίο Συμπλήρωσης (Padding) έχει μέγεθος το πολύ 255 bytes και χρειάζεται για να προσαρμόζεται το μέγεθος του IP πακέτου, ανάλογα με τον αλγόριθμο κρυπτογράφησης που χρησιμοποιείται (αν ανλογιστούμε ότι κάποιοι αλγόριθμοι κρυπτογράφησης απαιτούν τα δεδομένα να είναι μήκους πολλαπλάσιου κάποιου συγκεκριμένου αριθμού bytes).



Εικόνα 4.27: Πεδία ενός ESP Header και Trailer

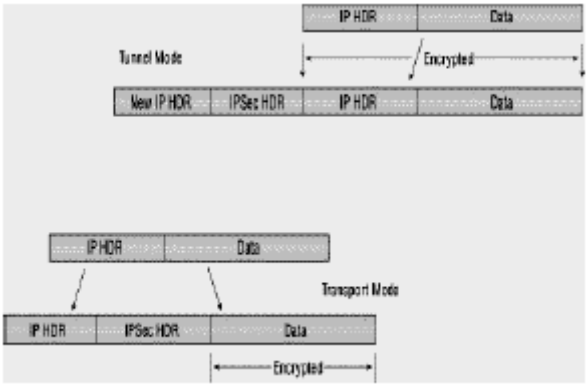
4.14.2 Καταστάσεις ή τρόποι (modes) λειτουργίας

Το IPSec παρέχει δυο καταστάσεις (ή τρόπους) λειτουργίας (που σημαίνει δύο τρόπους με τους οποίους μπορούν τα τοποθετηθούν οι κεφαλίδες AH και ESP): **ο τρόπος μεταφοράς (transport mode)** και **ο τρόπος διόδου (tunnel mode)**, όπως φαίνεται στην εικόνα 4.28.



Εικόνα 4.28: Τρόπος καθορισμού ενός IPSec μετασχηματισμού (πρωτόκολλα-αλγόριθμοι-τρόποι υλοποίησης)

Στην κατάσταση λειτουργίας μεταφοράς (transport mode), οι αρχικές επικεφαλίδες του IP πακέτου μένουν ανέπαφες. Αυτή η κατάσταση λειτουργίας έχει το πλεονέκτημα της προσθήκης μόνο μερικών bytes σε κάθε πακέτο. Επιπλέον οι συσκευές στο δημόσιο δίκτυο (όπως για παράδειγμα οι δρομολογητές) μπορούν να βλέπουν τον τελικό αποδέκτη του πακέτου, αφού οι IP διευθύνσεις μεταδίδονται ανέπαφες (μη κρυπτογραφημένες). Αυτή η δυνατότητα επιτρέπει ειδική επεξεργασία των πακέτων (για παράδειγμα δρομολόγηση με βάση την Ποιότητα Υπηρεσίας - QoS), βασισμένη στην πληροφορία που βρίσκεται στην IP επικεφαλίδα. Μειονέκτημα αυτού του τρόπου λειτουργία είναι το γεγονός ότι αφήνοντας την IP επικεφαλίδα χωρίς κρυπτογράφηση, ένας επιτιθέμενος μπορεί να κάνει ανάλυση κίνησης (traffic analysis). Για παράδειγμα, ο επιτιθέμενος θα μπορούσε να δει πότε ένας εργαζόμενος μίας εταιρίας έστειλε πολλά πακέτα σε έναν άλλο εργαζόμενο. Ωστόσο θα πρέπει να σημειωθεί ότι ο επιτιθέμενος θα γνώριζε μόνο την αποστολή των IP πακέτων και τίποτα άλλο: δεν θα ήταν στη θέση να καθορίσει αν π.χ. αυτά ήταν πακέτα e-mail ή κάποιας άλλης εφαρμογής.
Ο τρόπος λειτουργίας μεταφοράς χρησιμοποιείται κυρίως για διασύνδεση μεταξύ δύο LAN ή για εφαρμογές πελάτη-εξυπηρετητή (client-server). Στην ουσία, είναι ο τρόπος με τον οποίο δύο συσκευές του δικτύου (και όχι οι χρήστες) μπορούν να επικοινωνήσουν.



Εικόνα 4.29: Σύγκριση των πακέτων για τους δύο τρόπους λειτουργίας (tunnel και transport)

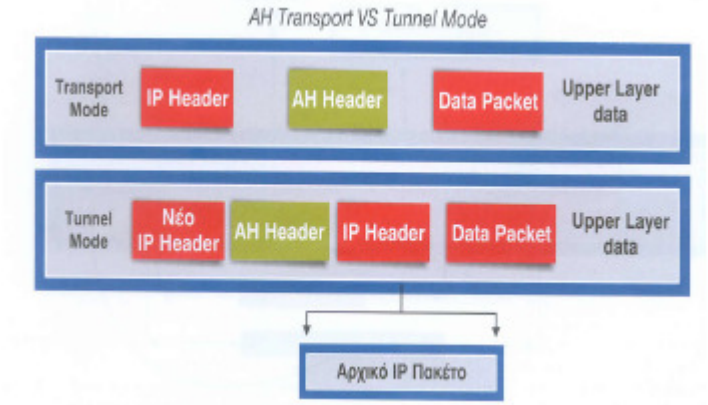
Στην κατάσταση λειτουργίας διόδου (tunnel mode), όλο το αρχικό IP πακέτο κρυπτογραφείται και γίνεται το φορτίο (payload) ενός καινούριου IP πακέτου. Αυτό σημαίνει ότι οι λειτουργίες κρυπτογράφησης, αυθεντικοποίησης κτλ. συντελούνται σε ολόκληρο το πακέτο, συμπεριλαμβανομένης και της αρχικής IP διεύθυνσης (βλέπε εικόνα 4.29). Το καινούριο IP πακέτο που προκύπτει έχει μία νέα IP διεύθυνση (IPSec διεύθυνση). Αυτή η κατάσταση λειτουργίας επιτρέπει σε μια δικτυακή συσκευή, όπως ένας δρομολογητής, να ενεργήσει σαν ένας IPSec proxy. Αυτό σημαίνει ότι ο δρομολογητής είναι αυτός που πραγματοποιεί την κρυπτογράφηση για λογαριασμό των υπολογιστών του δικτύου: συγκεκριμένα, ο δρομολογητής-αποστολέας κρυπτογραφεί τα πακέτα και τα προωθεί στη IPSec δίοδο (tunnel). Ο αποδέκτης-δρομολογητής αποκρυπτογραφεί το αρχικό IP πακέτο και το προωθεί στον τελικό αποδέκτη. Το βασικό πλεονέκτημα λοιπόν είναι ότι τα ακραία συστήματα δεν χρειάζεται να έχουν απαραίτητες ρυθμίσεις έτσι ώστε να απολάβουν τα οφέλη από τη χρήση του IPSec. Με άλλα λόγια, το λειτουργικό σύστημα του χρήστη δεν χρειάζεται τροποποίηση. Άλλο πλεονέκτημα του τρόπου λειτουργίας διόδου είναι ότι προστατεύει το σύστημα από την διαδικασία της ανάλυσης κίνησης. Λόγω του ότι η αρχική IP διεύθυνση είναι «κρυμμένη», ο επιτιθέμενος μπορεί να προσδιορίσει μόνο

τα ακραία σημεία του tunnel και όχι την πραγματική πηγή και τον προορισμό των πακέτων που κυκλοφορούν μέσα σε αυτό. Μειονέκτημα βέβαια είναι η μεγαλύτερη επεξεργασία πακέτων που απαιτείται.

Η κατάσταση διόδου του IPSec αποτελεί τον πιο κοινό τρόπο λειτουργίας όσον αφορά τη σύνδεση μεταξύ δύο gateway συσκευών ή μια σύνδεση μεταξύ μιας gateway συσκευής και ενός τερματικού σταθμού. Ένα παράδειγμα αυτού του τρόπου υλοποίησης είναι ένας κινητός χρήστης που θέλει να συνδεθεί στο δίκτυο ενός οργανισμού για την απόκτηση πρόσβασης στο ηλεκτρονικό ταχυδρομείο ή σε διάφορα αρχεία κ.λ.π.
Ανάλογα με τον τρόπο υλοποίησης του IPSec (μεταφοράς ή διόδου) το τελικό IP πακέτο που δημιουργείται με την εφαρμογή της κεφαλίδας είτε της AH είτε της ESP, είναι διαφορετικό σε κάθε περίπτωση.

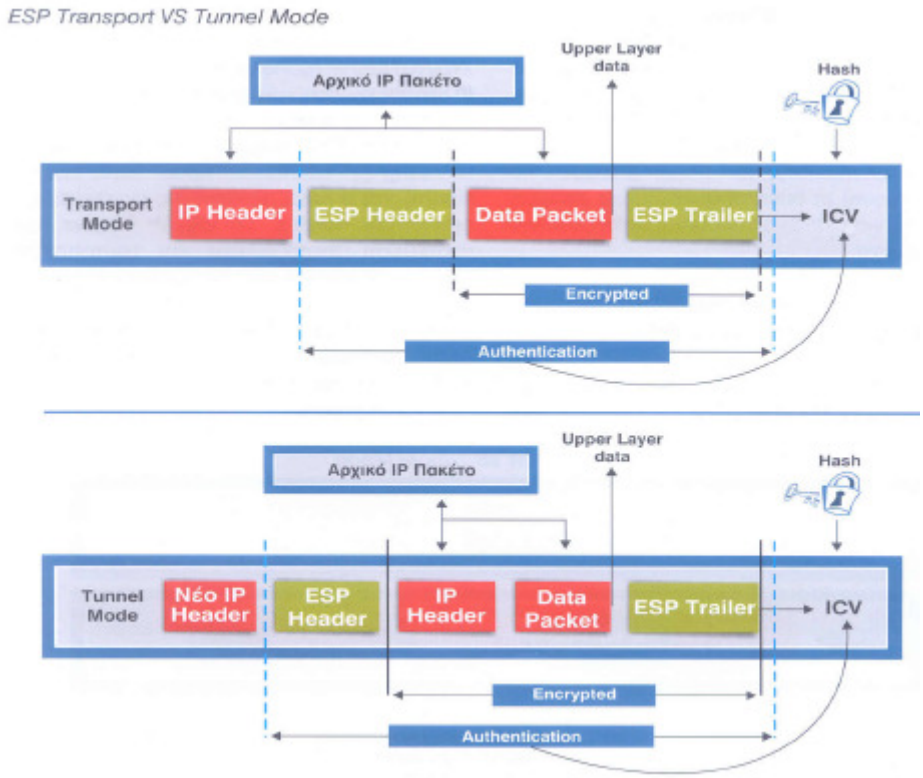
Στον *AH transport τρόπο υλοποίησης* οι υπηρεσίες ακεραιότητας και πιστοποίησης του AH πρωτοκόλλου προστατεύουν το αρχικό IP πακέτο. Η κεφαλίδα AH παρεμβάλλεται μετά από την αρχική IP κεφαλίδα και πριν από τα δεδομένα του IP πακέτου (που είναι τα περιεχόμενα των άνω στρωμάτων της στοίβας πρωτοκόλλου του μοντέλου OSI). Επειδή καμία κρυπτογράφηση δεν περιλαμβάνεται σε αυτό το σημείο, η IP διεύθυνση προορισμού είναι αναγνώσιμη από οποιαδήποτε συσκευή του ανώτερου επιπέδου 3 - όπως π.χ. ένας δρομολογητής.

Στον *AH tunnel τρόπο υλοποίησης*, ολόκληρο το αρχικό IP πακέτο (κεφαλίδα και δεδομένα) γίνονται τα δεδομένα (φορτίο) για το νέο πακέτο. Μία νέα IP κεφαλίδα που περιλαμβάνει πληροφορίες για τα άκρα του tunneling (IP addresses) προστίθεται στο νέο πακέτο. Ολόκληρο το νέο πακέτο (νέο IP Header, AH Header, αρχικό IP Header, και αρχικό IP Payload) προστατεύεται από το πρωτόκολλο AH.



Εικόνα 4.30: Σύγκριση Transport και Tunnel τρόπων υλοποίησης του IPSec, όταν χρησιμοποιείται AH

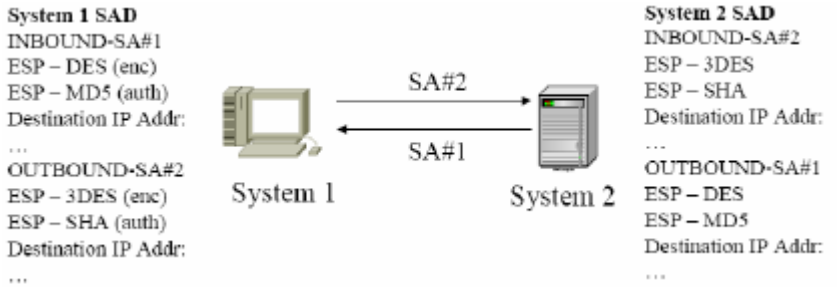
Στον *ESP transport τρόπο υλοποίησης* το νέο ESP header τοποθετείται ανάμεσα στην καφαλίδα και τα δεδομένα του αρχικού πακέτου, ενώ το ESP trailer τοποθετείται μετά από τα δεδομένα του αρχικού IP πακέτου. Από την άλλη μεριά, στον *ESP tunnel τρόπο υλοποίησης* τα ESP header και trailer τοποθετούνται εκατέρωθεν του αρχικού IP πακέτου και επιπλέον προστίθεται ένα νέο IP header που περιλαμβάνει πληροφορίες για τα άκρα του tunneling (IP addresses).



Εικόνα 4.31: Σύγκριση Transport και Tunnel τρόπων υλοποίησης του IPSec, όταν χρησιμοποιείται ESP

4.14.3 Συσχετίσεις Ασφάλειας

Το IPSec παρέχει πολλές επιλογές για την υλοποίηση κρυπτογράφησης και πιστοποίησης ταυτότητας στο δίκτυο. Κάθε IPSec σύνδεση μπορεί να παρέχει είτε κρυπτογράφηση (με ESP) είτε ακεραιότητα και πιστοποίηση ταυτότητας δεδομένων (με AH) ή και τα δύο (με ESP όπου υπάρχει και το αντίστοιχο πεδίο αυθεντικοποίησης των δεδομένων). Όταν η υπηρεσία ασφάλειας καθοριστεί, οι δυο επικοινωνούντες κόμβοι πρέπει να καθορίσουν ακριβώς ποιους αλγόριθμους θα χρησιμοποιήσουν (για παράδειγμα, AES ή 3DES για κρυπτογράφηση και MD5 ή SHA για ακεραιότητα δεδομένων). Αφού αποφασίσουν για τους αλγόριθμους οι δύο συσκευές πρέπει να μοιράσουν κλειδιά σύνδεσης. Η **συσχέτιση ασφάλειας** (**Security Association – SA**) είναι μια μέθοδος που χρησιμοποιείται από το IPSec για την παρακολούθηση όλων των λεπτομερειών που αφορούν μία δεδομένη IPSec επικοινωνία. Μια συσχέτιση ασφάλειας είναι η σχέση μεταξύ δυο ή περισσοτέρων οντοτήτων που περιγράφει πως οι οντότητες θα χρησιμοποιήσουν τις υπηρεσίες ασφάλειας για να επικοινωνήσουν με ασφάλεια. Με άλλα λόγια, είναι η συμφωνία των δύο άκρων για τις παραμέτρους επικοινωνίας, όπως αλγόριθμοι κρυπτογράφησης και αυθεντικοποίησης, τρόπος ανταλλαγής κλειδιών, διάρκεια ισχύος τους κτλ.



Εικόνα 4.32: Συσχετίσεις Ασφάλειας IPSec

Οι συσχετίσεις ασφάλειας είναι μη κατευθυντικές που σημαίνει ότι για κάθε ζεύγος επικοινωνούντων συστημάτων υπάρχουν τουλάχιστον δυο συνδέσεις ασφάλειας—μια από το Α στο Β και μια από το Β στο Α (σχήμα 15). Η συσχέτιση ασφάλειας αναγνωρίζεται από έναν τυχαίως επιλεγμένο μοναδικό αριθμό ο οποίος λέγεται Δείκτης παραμέτρων ασφαλείας (*SPI - Security Parameter Index)* και από την *IP διεύθυνση του προορισμού*. Όταν μία συσκευή στέλνει ένα πακέτο το οποίο απαιτεί IPSec προστασία κοιτάει τη συσχέτιση ασφάλειας στη βάση δεδομένων του, εφαρμόζει τη συγκεκριμένη επεξεργασία και μετά εισάγει τον SPI από τη συσχέτιση ασφάλειας στην IPSec επικεφαλίδα. Όταν το αντίστοιχο μηχάνημα IPSec λαμβάνει το πακέτο κοιτάει με τη σειρά του τη συσχέτιση ασφάλειας στη βάση δεδομένων του (βάσει της διεύθυνσης προορισμού και του SPI) και μετά επεξεργάζεται το πακέτο όπως ορίζεται. Με λίγα λόγια, η συσχέτιση ασφάλειας είναι απλώς μια δήλωση της διαπραγματεύσιμης πολιτικής ασφάλειας μεταξύ δυο συσκευών.

Οι κύριες παράμετροι που προσδιορίζονται σε μία συσχέτιση ασφαλείας είναι:

- IP διεύθυνση πηγής και προορισμού
- Ένα ID χρήστη
- Πρωτόκολλο μεταφοράς (TCP ή UDP)
- Τον αλγόριθμο που χρησιμοποιείται για κρυπτογράφηση, καθώς και τα κλειδιά
- Τον αλγόριθμο που χρησιμοποιείται για κρυπτογράφηση, καθώς και τα κλειδιά
- Τρόπος λειτουργίας του IPSec (transfer ή tunnel mode)
- Διάρκεια ζωής μιας SA

4.14.4 Πρωτόκολλο Διαχείρισης Κλειδιών

Το IPSec περιλαμβάνει, εκτός από την επεξεργασία των πακέτων μέσω των κεφαλίδων AH και ESP, και πρωτόκολλα ανταλλαγής του κλειδιού. Μετά από εξέταση πολλών εναλλακτικών λύσεων για τη διαχείριση του κλειδιού, η IETF επέλεξε το **IKE (Internet Key Exchange)** σαν τον τρόπο ρύθμισης των συσχετίσεων ασφάλειας για το IPSec.

Το IKE (επέκταση του προϋπάρχοντος ISAKMP/Oakley πρωτοκόλλου) δημιουργεί ένα πιστοποιημένο και ασφαλές κανάλι (tunnel) μεταξύ δύο οντοτήτων και κατόπιν διαπραγματεύεται τις συσχετίσεις ασφάλειας για το IPSec. Αυτή η διαδικασία απαιτεί από τις δύο οντότητες να πιστοποιήσουν η μία την άλλη και να μοιράσουν κλειδιά. Οι δύο οντότητες πρέπει να συμφωνήσουν σε ένα κοινό πρωτόκολλο πιστοποίησης μέσω μιας κατάλληλης διαδικασίας. Σε αυτή τη φάση υλοποιούνται συνήθως οι παρακάτω μηχανισμοί :

- **Προ-Μοιρασμένα Κλειδιά**—Το ίδιο κλειδί προ-εγκαθίσταται και στις δύο μηχανές. Κατά την πιστοποίηση αποστέλλεται από τη μία μηχανή στην άλλη μία επεξεργασμένη μορφή (με τη βοήθεια μιας συνάρτησης κατακερματισμο) του ίδιου κλειδιού. Εάν αυτή η μορφή συμπίπτει με αυτήν που υπολογίζεται τοπικά σε κάθε μηχανή, τότε η διαδικασία πιστοποίησης έχει θετικό αποτέλεσμα.

- **Κρυπτογράφηση Δημοσίων Κλειδιών**—Κάθε μηχανή παράγει έναν ψευδο-τυχαίο αριθμό τον οποίο και κρυπτογραφεί με το δημόσιο κλειδί (public key) της άλλης μηχανής. Η πιστοποίηση επιτυγχάνεται μέσω της ικανότητας των μηχανών να υπολογίσουν μια συνάρτηση κατακερματισμού του τυχαίου αριθμού, αποκρυπτογραφώντας με τα ιδιωτικά κλειδιά (private keys) ό,τι λαμβάνουν από το συνομιλητή τους. Υποστηρίζεται μόνο ο αλγόριθμος δημοσίων κλειδιών RSA.

- **Ψηφιακές Υπογραφές**—Κάθε συσκευή υπογράφει ψηφιακά ένα σύνολο δεδομένων και τα στέλνει στην άλλη. Ο αποστολέας χρησιμοποιεί το κρυφό του ιδιωτικό κλειδί για να υπογράψει ηλεκτρονικά τα δεδομένα του. Ο αποδέκτης του κειμένου χρησιμοποιεί το public key του αποστολέα, το οποίο έτσι και αλλιώς γνωρίζει αφού είναι δημόσιο, για να ελέγξει την υπογραφή του αποστολέα. Αν αυτός ο έλεγχος είναι επιτυχής, αυτό σημαίνει ότι το κείμενο δεν έχει αλλαχθεί και έχει πιστοποιηθεί η ταυτότητα του αποστολέα Υποστηρίζονται τόσο ο αλγόριθμος δημοσίων κλειδιών της RSA όσο και οι προδιαγραφές ψηφιακών υπογραφών (DSS).

Μετά την πιστοποίηση της ταυτότητας του κάθε χρήστη, πρέπει να υπάρξει η ανταλλαγή του κλειδιού που θα χρησιμοποιηθεί για την κρυπτογράφηση των δεδομένων που θα σταλούν μετέπειτα, κατά την επικοινωνία των δύο χρηστών. Ως βασικό αλγόριθμο ανταλλαγής κλειδιού το IKE υποστηρίζει τον Diffie-Hellman, αν και μπορεί να υπάρξουν και άλλοι.

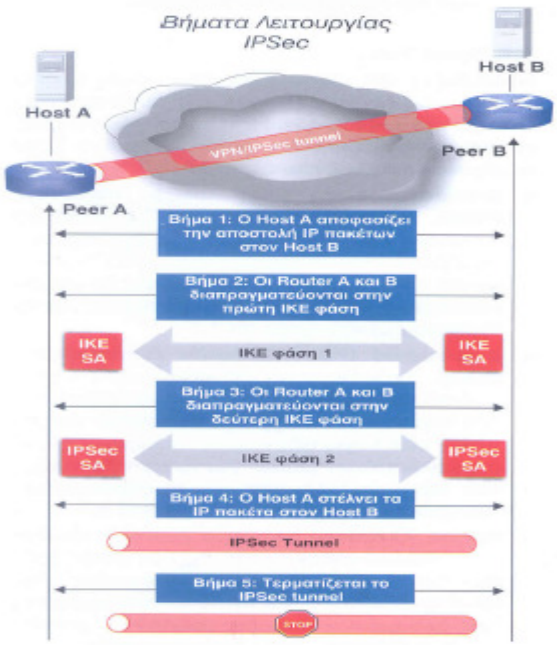
Diffie-Hellman: Μηχανισμός ανταλλαγής κλειδιών που αναπτύχθηκε από τους Diffie και Hellman το 1976. Επιτρέπει σε δύο χρήστες να ανταλλάσσουν ένα μυστικό κλειδί μέσα από ένα μη ασφαλές κανάλι. Είναι ένας κρυπτογραφικός αλγόριθμος δημοσίου κλειδιού. Το πρωτόκολλο έχει δύο παραμέτρους (αριθμούς): p και g. Το p είναι ένας πολύ μεγάλος πρώτος αριθμός και το g είναι ένας αριθμός με την ιδιότητα $g^k \neq 1 \bmod p$ για όλους τους k από 1 μέχρι p-2 (δηλαδή, στοιχείο-γεννήτορας (generator) στο σώμα των ακεραίων Modulo p). Τα p,g τα γνωρίζουν όλοι – είναι δημοσίως γνωστά. Ας υποθέσουμε τώρα ότι δύο χρήστες, ο Α και ο Β, θέλουν να συμφωνήσουν για ένα μυστικό κλειδί. Πρώτα, ο Α παράγει μία τυχαία τιμή x και ο Β μία τυχαία τιμή y (όπου τα x,y είναι μικρότερα του p). Τα x,y κρατούνται μυστικά – μόνο ο Α δηλαδή γνωρίζει το x και μόνο ο Β το y. Στη συνέχεια ο Α υπολογίζει τον αριθμό $x' = g^x \bmod p$ και ο Β τον αριθμό $y' = g^y \bmod p$. Κατόπιν, ο ένας στέλνει στον άλλον τις τιμές αυτές. Τέλος, ο Α κάνει τον υπολογισμό $(y')^x = g^{xy} \bmod p$ και ο Β κάνει με την σειρά του τον υπολογισμό $(x')^y = g^{xy} \bmod p$. Συνεπώς και οι δύο υπολογίζουν τον ίδιο αριθμό – ο οποίος θα είναι το μυστικό κλειδί που θα χρησιμοποιήσουν. Η ασφάλεια του πρωτοκόλλου αυτού βασίζεται στο γεγονός ότι ένας επιτιθέμενος, ο οποίος

παρακολουθεί το τι ανταλλάσσουν οι A και B, δεν μπορεί από τα x', y' να υπολογίσει το μυστικό κλειδί: για να το κάνει αυτό θα πρέπει να ξέρει είτε το x είτε το y. Όμως, όταν τα p και g είναι πολύ μεγάλα, το να ξέρει κανείς το x' ή το y' δεν του αρκεί για να βρει το x ή το y.

Ο ακριβής ρόλος του IKE για τη διεκπαιρέωση μίας IPSec επικοινωνίας μεταξύ δυο ή περισσότερων συσκευών αντικατοπτρίζεται στην ακόλουθη διαδοχή βημάτων που λαμβάνουν χώρα σε μία IPSec ανταλλαγή δεδομένων (εικόνα4.33):

- **Ενεργοποίηση μιας IPSec συνόδου**. Στο βήμα αυτό καθορίζεται το σύνολο των IP πακέτων που πρόκειται να προστατευθούν μέσω του IPSec.
- **IKE - Πρώτη φάση**. Δημιουργία και λειτουργία της IKE Συσχέτισης Ασφαλείας.
- **IKE – Δεύτερη φάση**. Δημιουργία και λειτουργία της AH/ESP Συσχέτισης Ασφαλείας
- **Μεταφορά Δεδομένων**. Τα IP πακέτα που επιλέχθηκαν από το πρώτο βήμα μεταφέρονται.
- **Τερματισμός της IPSec συνόδου**. Εφόσον ολοκληρωθεί η μεταφορά των IP πακέτων και δεν χρησιμοποιείται η παραπάνω σύνοδος, η τελευταία τερματίζεται.

Στην **πρώτη φάση IKE** μέσω των IKE SAs προετοιμάζεται το έδαφος για την επόμενη διαπραγμάτευση των άλλων πρωτοκόλλων ασφάλειας του IPSec (όπως το AH και το ESP πρωτόκολλο). Στην πραγματικότητα υλοποιείται η διαχείριση των κλειδιών μέσω του IKE.



Εικόνα 4.33: Σύνολο βημάτων που πρέπει να πραγματοποιηθούν για την επιτυχή μετάδοση δεδομένων μέσω του IPSec πρωτοκόλλου

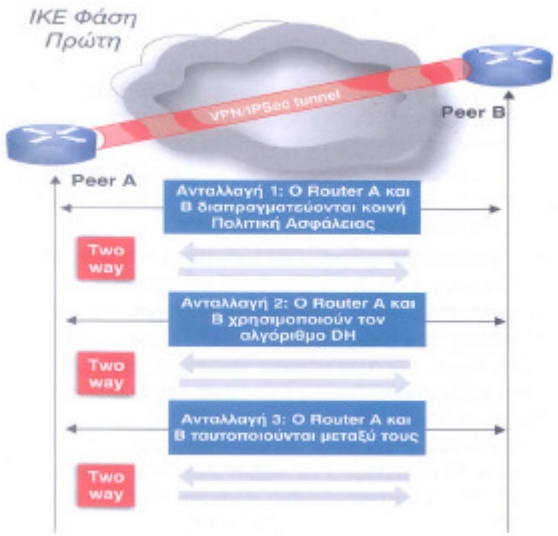
Οι κυριότερες λειτουργίες που συναντάμε στη πρώτη φάση του IKE είναι οι εξής:

- Πιστοποίηση των μελών που συμμετέχουν σε μια IPSec επικοινωνία.

- Ανάπτυξη μιας ή περισσότερων πολιτικών ασφάλειας IKE βασισμένες στη γενική πολιτική ασφάλειας ενός οργανισμού. Κάθε πολιτική απαιτεί την λήψη αποφάσεων για πέντε βασικές επιλογές ασφάλειας: *μέθοδος πιστοποίησης*, *αλγόριθμος κρυπτογράφησης*, *αλγόριθμος κατακερματισμού (για έλεγχο της ακεραιότητας δεδομένων)*, παράμετροι του *Diffie - Hellman αλγορίθμου (που προσδιορίζει το μέγεθος κλειδιού) και διάρκεια ζωής μίας SA*. Οι διαφορετικές πολιτικές μπορεί να απαιτούνται παραδείγματος χάριν στη περίπτωση που ένα IPSec συμβαλλόμενο μέρος δεν υποστηρίζει κάποια από τις παραπάνω μεθόδους ή αλγόριθμους.
- Εκτέλεση αλγόριθμου Diffie-Hellman για την δημιουργία ενός ή περισσοτέρων κοινών μυστικών κλειδιών.

- Δημιουργία ασφαλούς «διόδου» (tunneling) για την ολοκλήρωση της επόμενης (δεύτερης) IKE φάσης.

Η πρώτη φάση του IKE μπορεί να πραγματοποιηθεί με δυο τρόπους: είτε τον κύριο τρόπο (main) είτε τον επιθετικό (aggressive). Με τον πρώτο τρόπο έχουμε συνολικά τρεις ανταλλαγές μηνυμάτων και προς τις δυο κατευθύνσεις μεταξύ των συμβαλλόμενων μερών μιας IPSec επικοινωνίας (εικόνα 4.34), ενώ με τον δεύτερο τρόπο οι παραπάνω ανταλλαγές συμπτύσσονται σε μια μόνο ανταλλαγή με τρία στάδια (αποστολέας - δέκτης, δέκτης - αποστολέας, αποστολέας - δέκτης).



Εικόνα 4.34: Με ένα σύνολο τριών ανταλλαγών η πρώτη IKE φάση δημιουργεί ένα ασφαλές tunnel και ταυτοποιεί τα συμβαλλόμενα μέλη του

Οι ανταλλαγές μηνυμάτων που λαμβάνουν χώρα στην πρώτη φάση του IKE είναι οι εξής:

Πρώτη Ανταλλαγή. Σε αυτή καθορίζονται οι αλγόριθμοι ασφάλειας (κρυπτογράφησης) και πιστοποίησης ταυτότητας οι οποίοι πρόκειται να χρησιμοποιηθούν στα επόμενα βήματα. Για κάθε μια κατεύθυνση μία ξεχωριστή Συσχέτιση Ασφαλείας (SA) δημιουργείται με πληροφορίες που περιλαμβάνουν τους

αλγόριθμους κρυπτογράφησης και πιστοποίησης που υποστηρίζονται από το κάθε άκρο της συνομιλίας, τον αλγόριθμο παραγωγής κοινού μυστικού κλειδιού (συμφωνία αρχικών παραμέτρων του Diffie-Hellman αλγορίθμου), τον χρόνο διάρκειας της πρώτης IKE φάσης, τον τρόπο πιστοποίησης που θα χρησιμοποιηθεί (π.χ. προμοιρασμένα κλειδιά) κ.ο.κ. Στο τέλος της παραπάνω διαδικασίας καθένας από τα IPSec «συνομιλούντες» διαθέτει μία κοινή IKE SA.

Δεύτερη Ανταλλαγή. Εφόσον επέλθει συμφωνία με τις προτεινόμενες παραμέτρους, εκτελείται ο αλγόριθμος παραγωγής κοινού μυστικού κλειδιού (Diffie-Hellman) μέσω του οποίου παράγεται ένα κλειδί που είναι κοινό και στα δύο μέρη. Ο εν λόγω αλγόριθμος είναι κρίσιμος στις διαδικασίες που αφορούν το IPSec πρωτόκολλο επειδή το κοινό μυστικό κλειδί χρησιμοποιείται για να κρυπτογραφήσει τα δεδομένα χρησιμοποιώντας τους βασικούς αλγορίθμους κρυπτογράφησης που διευκρινίζονται στα IPSec SA (π.χ. στον DES).

Τρίτη Ανταλλαγή. Κάθε συμβαλλόμενο μέρος ταυτοποιεί το άλλο με χρήση των κατάλληλων αλγόριθμων (που έχουν οριστεί νωρίτερα).
Η **δεύτερη φάση IKE** πραγματοποιείται αμέσως μετά την ολοκλήρωση της πρώτης φάσης. Στην φάση αυτή εκτελούνται τα εξής:

- **Διαπραγμάτευση μιας κοινής πολιτικής IPSec**. Καθορίζονται οι τρόποι χρήσης των αλγόριθμων κρυπτογράφησης (π.χ. αν θα είναι τρόπος μεταφοράς (transport mode) ή διόδου (tunnel mode), αν θα χρησιμοποιηθεί AH ή ESP κ.ο.κ.)

- **Δημιουργία IPSec Συσχέτισης Ασφαλείας).** Στην δεύτερη IKE φάση κάθε στιγμή μπορεί να δημιουργηθεί ένα νέο IPSec SA στη περίπτωση που το προηγούμενο τερματιστεί, είτε λόγω αδυναμίας συμφωνίας των συμβαλλομένων μερών για τις παραμέτρους επικοινωνίας είτε λόγω παρέλευσης του προκαθορισμένου χρόνου λειτουργίας ενός IPSec SA.

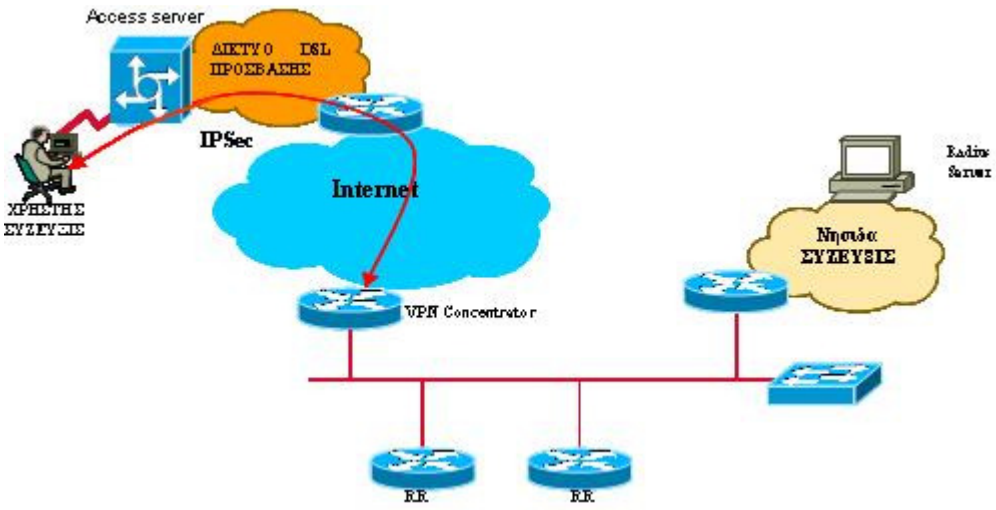
- **Χρήση Κλειδιών**. Τα κοινά μυστικά κλειδιά που δημιουργήθηκαν στη πρώτη φάση χρησιμοποιούνται για τις λειτουργίες της κρυπτογράφησης και αποκρυπτογράφησης των δεδομένων που μεταφέρονται μεταξύ των δύο IPSec συμβαλλομένων μερών.

4.14.5 Εφαρμογές

Το IPSec είναι ένα standard πρωτόκολλο για την υλοποίηση κρυπτογραφικών μηχανισμών σε δρομολογητές, τοίχους ασφαλείας (firewalls), αλλά και σε LANs ή μεμονωμένους κόμβους (hosts) που επικοινωνούν μέσω του Internet. Πιο συγκεκριμένα, υποστηρίζει την ασφαλή επικοινωνία μεταξύ δύο κόμβων, όπως επίσης και μεταξύ δύο LANs, εκτός από την client/server επικοινωνία που υποστηρίζουν τα άλλα πρωτόκολλα.
Επιπλέον, το IPSec είναι χρήσιμο για τη διασφάλιση της απομακρυσμένης πρόσβασης (μέσω dial-up) διασυνδέσεων VPN με απομακρυσμένα σημεία εντός εταιρικών ιδιωτικών δικτύων.
Γενικά, το IPSec χρησιμοποιείται για να προσφέρει τη μέγιστη δυνατή ασφάλεια σε περιπτώσεις χρηματοπιστωτικών ιδρυμάτων, χρηματιστηριακών εταιριών, και γενικά οπουδήποτε η μεταφερόμενη πληροφορία είναι ιδιαίτερα ευαίσθητη. Επιπλέον

προσφέρει εκτός της κρυπτογράφησης, πιστοποίηση της ταυτότητας των μερών που λαμβάνουν μέρος σε ένα VPN (είτε πρόκειται για τοπικά δίκτυα, είτε για μεμονωμένους χρήστες), πιστότητα στη μετάδοση των δεδομένων, και προστασία των τοπικών δικτύων από κακόβουλες επιθέσεις. Με τον τρόπο που διαμορφώνονται σήμερα οι σύγχρονες επιχειρήσεις και με τις συνθήκες που απαιτούνται για την ασφαλή μετάδοση των πληροφοριών, είναι κατανοητό για ποιο λόγο οι τελευταίες καταφεύγουν σε υλοποιήσεις όπως η IPSec τεχνολογία (και τα πρωτόκολλα που τη συνοδεύουν) προκειμένου να πετύχουν το στόχο τους. Αυτός δεν είναι τίποτα άλλο παρά η διασφάλιση της ακεραιότητας, πιστοποίησης και εμπιστευτικότητας των πληροφοριών που μεταδίδονται σήμερα ανά τον κόσμο σε ένα μεγάλο αριθμό δκτυών, είτε αυτά είναι εσωτερικά ενός οργανισμού είτε όχι. Η τεχνολογία IPSec στα VPN δίκτυα, έχει γίνει ευρέως αποδεκτή και αποδεικνύεται ιδιαίτερα επιτυχημένη, αφού αποτελεί μία από τις κυριότερες ασπίδες προστασίας των δεδομένων που μεταδίδονται σήμερα στο διαδίκτυο.

Προβλήματα που καλείται να αντιμετωπίσει το IPSec είναι η αύξηση του μεγέθους των πακετών (που σημαίνει μεγαλύτερος χρόνος επεξεργασίας τους), η μη δυνατότητα καθορισμού συγκεκριμένων καθολικών αλγορίθμων κρυπτογράφησης (λόγω νομοθετικών δυσκολιών που αντιμετωπίζουν πολλοί αλγόριθμοι και σε διάφορες χώρες), καθώς και το γεγονός ότι εφαρμόζεται μόνο σε IP δίκτυα (που σημαίνει ότι σε κάποια υπάρχοντα ιδιωτικά δίκτυα δεν μπορεί να εφαρμοστεί).



Εικόνα 4.35: Η σύνδεση αυτή πραγματοποιείται χρησιμοποιώντας την τεχνολογία ¨IPSec tunnel¨, η οποία εξασφαλίζει την ασφάλεια πρόσβασης ενός χρήστη.

Παρακάτω παρατίθεται ο πίνακας ο οποίος αναφέρει αναλυτικά τα πρωτόκολλα ασφάλειας καθώς και τα χαρακτηριστικά αυτών:

ΠΡΩΤΟΚΟΛΛΑ	ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ
(MAC-Media Access Control) 802.15.4	Παρέχει διευθυνσιοδότηση και μηχανισμούς ελέγχου προσπέλασης του καναλιού
ZigBee	• (υπο-επίπεδο APS) είναι υπεύθυνο για τη διατήρηση των λογικών συνδέσεων μεταξύ των συσκευών επικοινωνίας με την προώθηση παράλληλα των πακέτων δεδομένων μεταξύ των συνδεδεμένων συσκευών. • επικοινωνεί άμεσα με την υπηρεσία παροχής ασφάλειας των δεδομένων μεταφοράς και λήψης δεδομένων (Security Service Provider)
802.11	Παρέχει εναλλακτικό μηχανισμό του κλασσικού Wired Equivalent Privacy - WEP με καινούριες μεθόδους κρυπτογράφησης και πιστοποίησης.
WEP	• Εμπιστευτικότητα • Ακεραιότητα • Επικύρωση
WPA	• εξασφαλίζει συμβατότητα • εισάγει ένα νέο πρωτόκολλο , το TKIP (Temporal Key Integrity Protocol), για την ανανέωση των κλειδιών κατά τη διάρκεια της σύνδεσης
WPA2 (Wi-Fi Protected Access Version 2)	χρησιμοποιεί AES κλειδιά για την προστασία της εμπιστευτικότητας και ακεραιότητας του πακέτου
TKIP (Temporal Key Integrity Protocol)	Κρυπτογράφηση
RSN (Robust Security Network)	• πλαίσια λειτουργίας κρυπτογράφησης TKIP και CCMP • πλαίσια λειτουργίας πιστοποίησης Pre-shared Key και 802.1x
CCMP (Counter Mode with Cipher-	• Κρυπτογράφηση

Block Chaining with Message Authentication Code Protocol)	• Στηρίζεται στον ισχυρό αλγόριμο κρυπτογράφησης Rijndael
EAP(Extensible Authentication Protocol (RFC 2284))	Πιστοποίηση
RADIUS(Remote Access Dial In User)	Χρησιμοποιεί έξι τύπους μηνυμάτων, τέσσερις για την διαδικασία πιστοποίησης και δυο για την καταγραφή της δραστηριότητας των χρηστών
EAP	Ευέλικτο πρωτόκολλο μεταφοράς πληροφοριών πιστοποίησης
EAPOL (EAP over LAN)	Πιστοποίηση EAP για ενσύρματα τοπικά δίκτυα
Transport Layer Security (TLS)	• Πιστοποίηση • Κρυπτογράφηση • Συμπίεση δεδομένων
Protected EAP (PEAP)	• κρυπτογράφηση μηνυμάτων • παραγωγή κλειδιών κρυπτογράφησης
PEAP MS-CHAPv2(Microsoft Challenge Authentication Protocol)	Πιστοποίηση χρήστη μέσω password
Πρωτόκολλο IPSec	• Ακεραιότητα των δεδομένων • Εξακρίβωση γνησιότητας της προέλευσης των δεδομένων ή πιστοποίηση ταυτότητας • Εμπιστευτικότητα
IKE (Internet Key Exchange)	• Πιστοποιημένο και ασφαλές κανάλι (tunnel) • Διαπραγματεύεται τις συσχετίσεις ασφάλειας για το IPSec

ΚΕΦΑΛΑΙΟ 5

Πειραματικό Μέρος

Σκοπός του πειραματικού μέρους της εργασίας είναι να δούμε τη λειτουργία ενώς δικτύου αισθητήρων πως συμπεριφέρεται όταν έχει κάποιο πρωτόκολλο ασφάλειας κατά τη διάρκεια διέλευσης πακέτων. Έτσι δημιουργήσαμε με τη βοήθεια του εργαλίου Matlab κατάλληλο κώδικα που προσομοιώνει ένα ασύρματο δίκτυο με N κόμβους.

Εξετάσαμε τις παρακάτω τοπολογίες:

1. Οι κόμβοι βρίσκονται σε ένα κυκλικό δίκτυο και ανταλλάσουν όλοι μεταξύ τους μηνύματα μιας εφαρμογής που χρησιμοποιούν όλοι μαζί. (περίπτωση peer to peer)

2. Οι κόμβοι βρίσκονται σε ένα κυκλικό δίκτυο και ανταλλάσουν μηνύματα με τον κεντρικό κόμβο (περίπτωση client servers)

3. Οι κόμβοι βρίσκονται σε ένα δίκτυο ενός τετραγωνικού χώρου και ανταλλάσουν μηνύματα μεταξύ τους (peer to peer)

4. Οι κόμβοι βρίσκονται σε ένα δίκτυο ενός τετραγωνικού χώρου και ανταλλάσουν μηνύματα με κεντρικό server στο ένα άκρο του δικτύου. (πάνω αριστερή γωνία , peer to peer).

Το δίκτυο στέλνει Nmsg μηνύματα ανά χρονική στιγμή και το ορίζουμε να λειτουργήσει για Ttotal χρονικές στιγμές.
Παίρνουμε τα παρακάτω γραφήματα.

1. Το γράφημα ανταλλαγής μηνυμάτων
2. Το πλήθος μηνυμάτων που λαμβάνει κάθε κόμβος στο σύνολο του χρόνου
3. Το πλήθος των μηνυμάτων που στέλνει ο κόμβος.

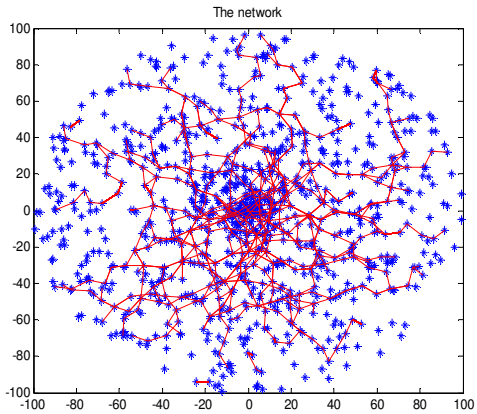
Ορίζουμε την ενεργή ακτίνα κάθε κόμβου δηλαδή την ακτίνα μέσα στην οποία μπορεί να αντιλήφθη έναν άλλο κόμβο και να μπορέσει να λάβει ή να στείλει μήνυμα από αυτόν. Η ενεργή γωνία είναι ένα βασικό μέγεθος και φαίνεται πως επηρεάζει τις παραπάνω μετρήσεις.

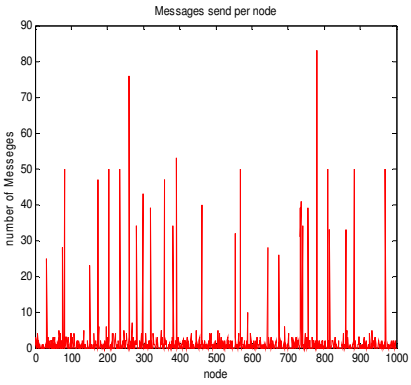
Έτσι το routing γίνεται όπως παρακάτω:

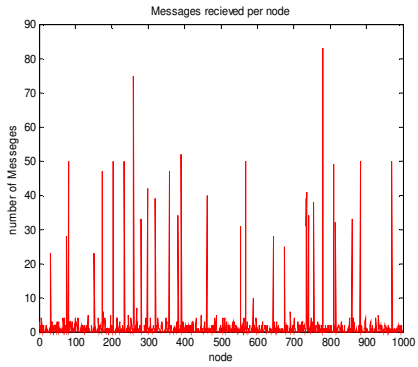
Ένας κόμβος στέλνει ένα μήνυμα σε ένα άλλο κόμβο. Ο κόμβος 1 αφετηρία στέλνει αρχικά στον κοντινότερο σε αυτό κόμβο 2 αλλά και κοντινότερο στον κόμβο προορισμό που βρίσκεται όμως στην ενεργή ακτίνα του κόμβου αφετηρία. Στη συνέχεια ο κόμβος 2 επαναλαμβάνει την διαδικασία κ.ο. μέχρι το μήνυμα να φτάσει στον προορισμό. Αν θεωρήσουμε σαν r την ακτίνα από το κέντρο μέχρι το πάνω μέρος και σαν ενεργή ακτίνα range=r*0.2 παρατηρούμε τα παρακάτω για τις 4

περιπτώσεις:

Δίκτυο κυκλικό Peer to Peeri με range =r*0.2

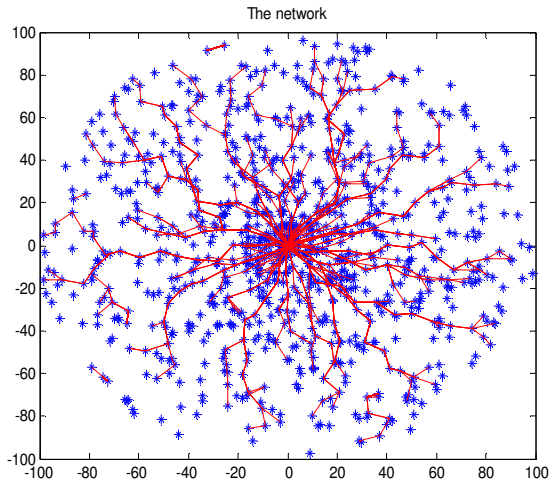


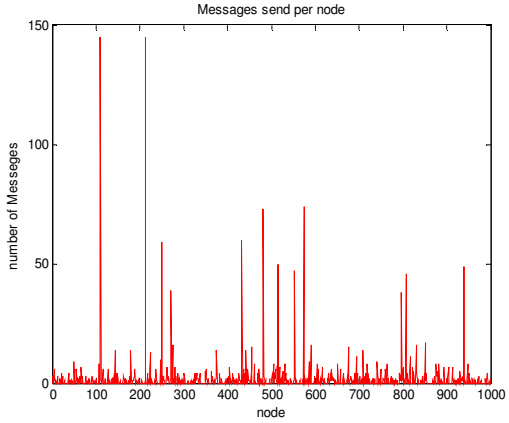


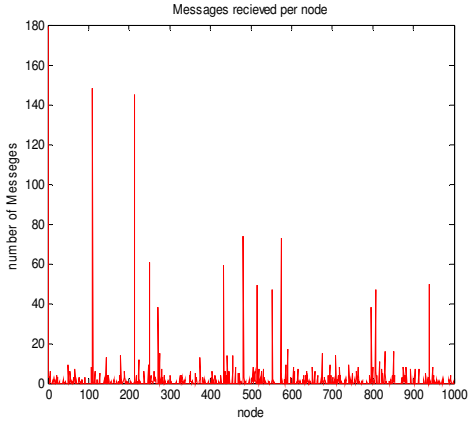


Κυκλικό Δίκτυο Client Server

Εκτελούμε το δίκτυο με αρκετά μικρή ακτίνα range=0.1 r

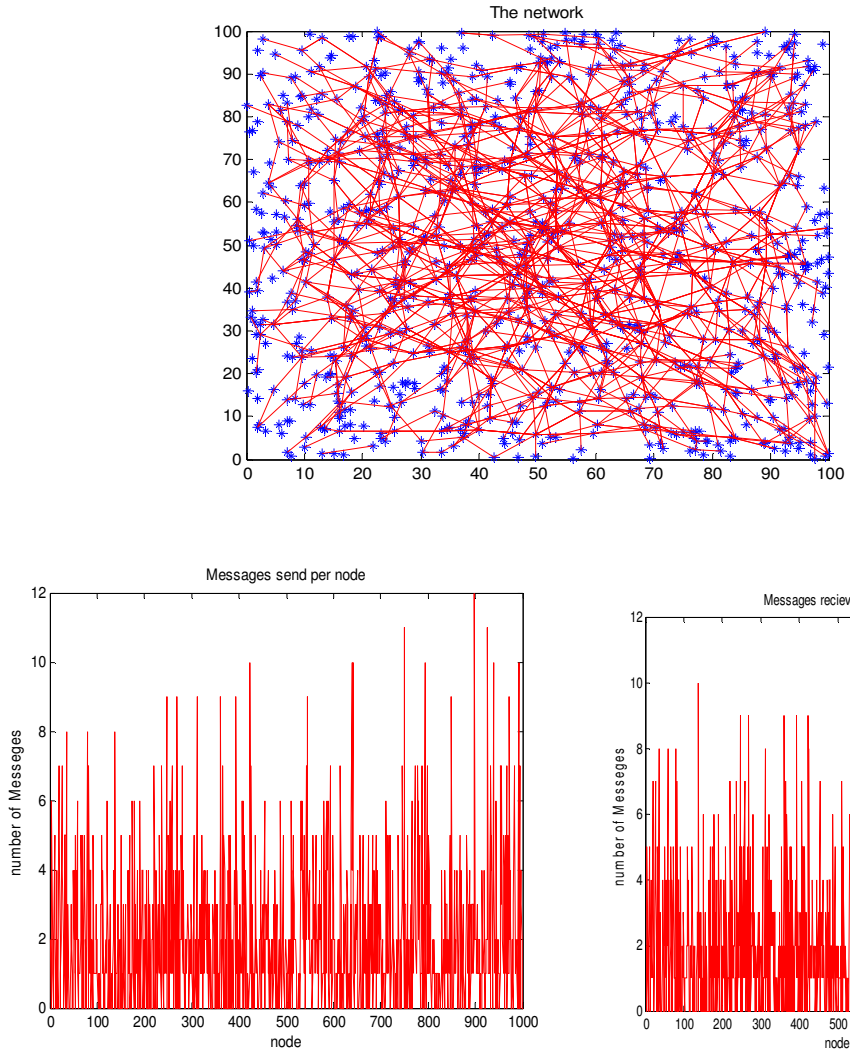






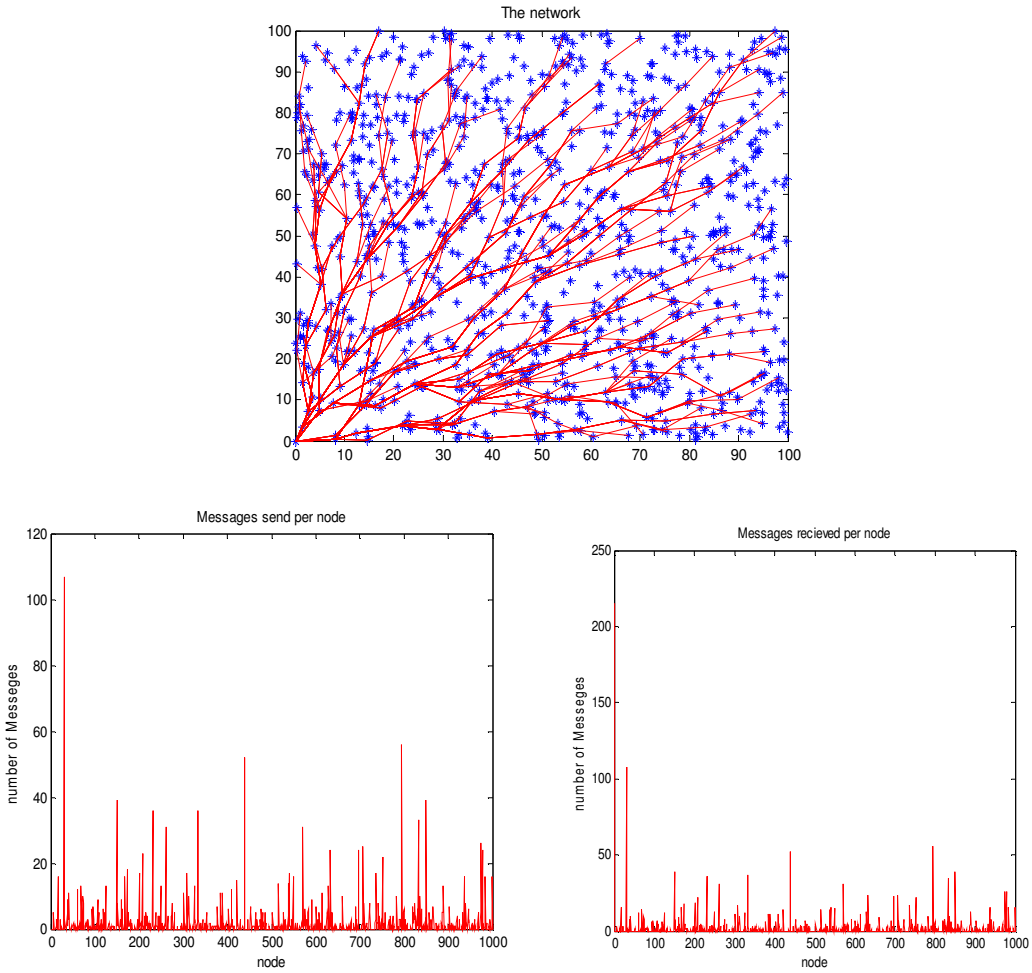
Σε αυτή την περίπτωση παρατηρούμε λόγω της μικρής ακτίνας ότι μηνύματα δεν καταφέρνουν να φτάσουν στον προορισμό όπως και το ότι ο κεντρικός κόμβος που είναι ο 1. Επίσης παρατηρούμε ότι ο κεντρικός κόμβος 1 δεν στέλνει κανένα μήνυμα αφού είναι για όλους προορισμός και επίσης λαμβάνει όλα τα μηνύματα από το δίκτυο. Επίσης παρατηρούμε κάποιοι κόμβοι να στέλνουν πολύ περισσότερα μηνύματα γιατί είναι κοντά στον κόμβο προορισμού.
Ομοίως βλέπουμε και στο τετραγωνικό δίκτυο

Τετραγωνικό δίκτυο peer to peer



Εδώ παρατηρούμε ότι η κατανομή των μηνυμάτων είναι σχετικά ομογενής

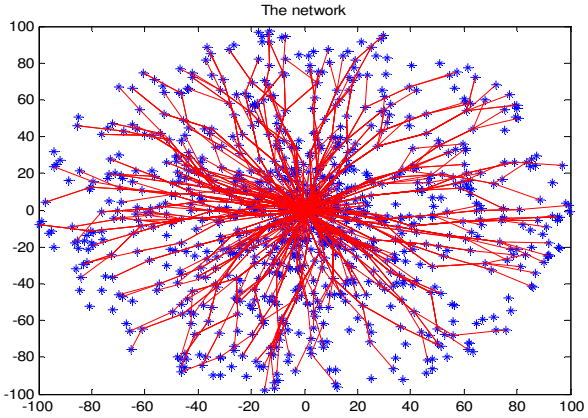
Τετραγωνικό δίκτυο Client Server

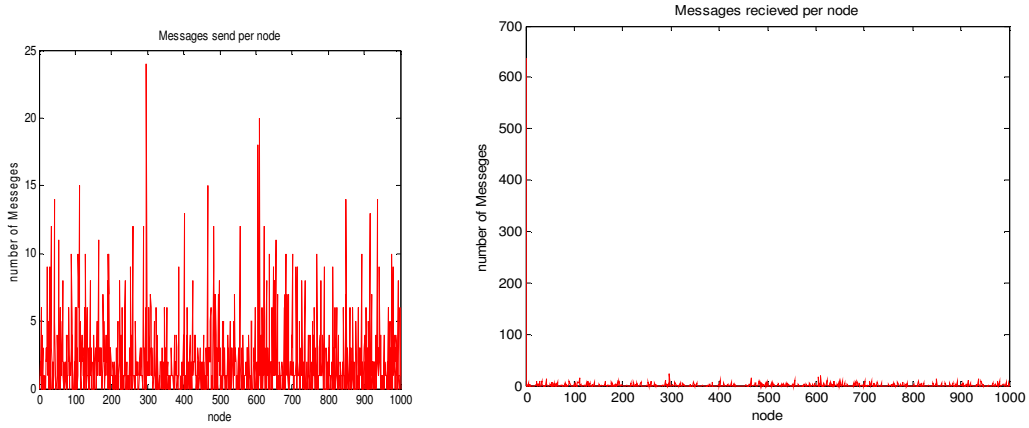


Κι εδώ παρατηρούμε ανάλογη συμπεριφορά με το κυκλικό δίκτυο client server

Κυκλικό δίκτυο Client Server με μεγαλύτερη ακτίνα range=0.4r

Για να δούμε τον ρόλο της ακτίνας εκτελούμε πάλι το κυκλικό δίκτυο client server με αρκετά μεγαλύτερη ενεργή ακτίνα κόμβου.

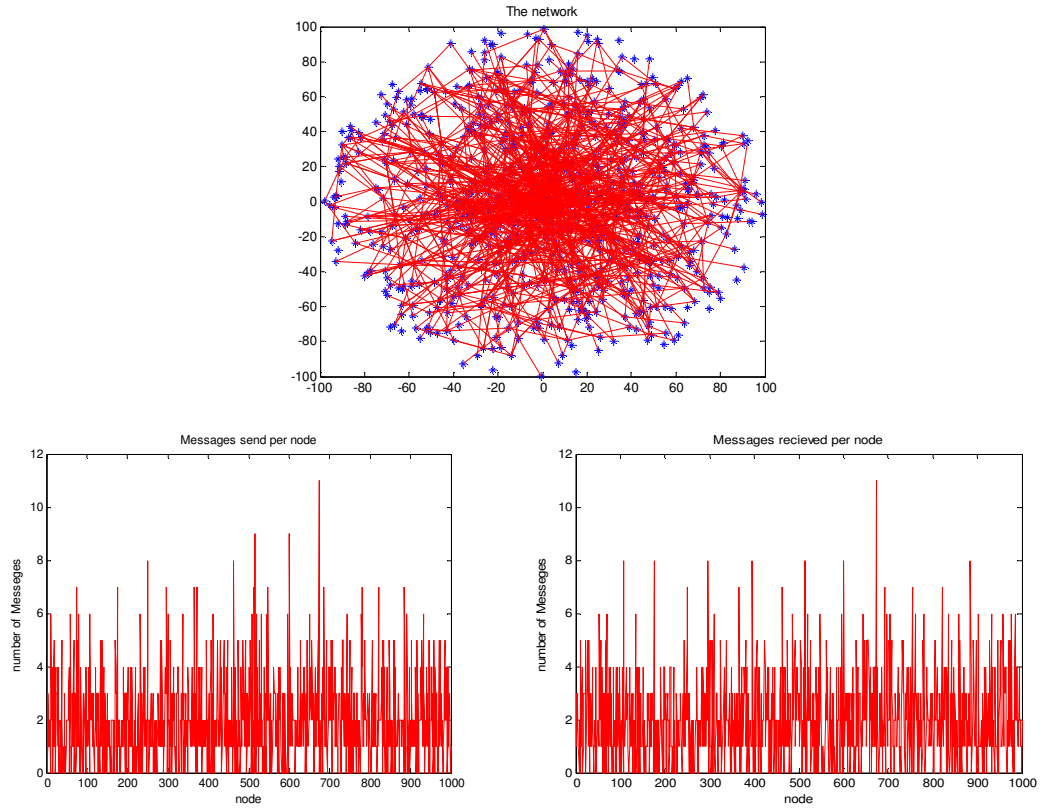




Παρατηρούμε ότι έχουμε πολύ λιγότερα μηνύματα να λαμβάνονται από τους κόμβους αφού γίνονται μεγαλύτερα βήματα και «προσπερνιούνται» κόμβοι αφού τα μηνύματα πάνε στους κοντινότερους κόμβους στον προορισμό μέσα στην ενεργή ακτίνα ενός κόμβου.

Συμπεράσματα

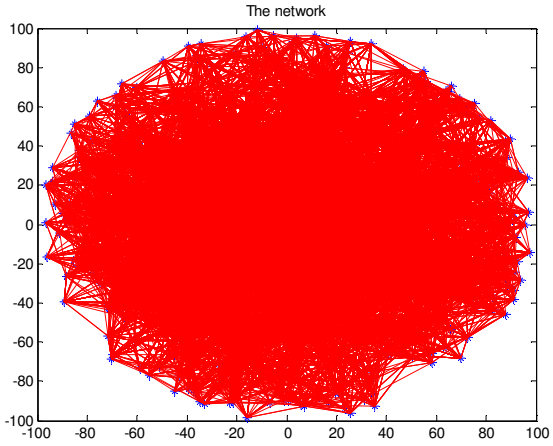
Παρακάτω φαίνεται η χρήση ενός δικτύου peer to peer με λίγα και πολλά πακέτα ανά χρονική στιγμή.

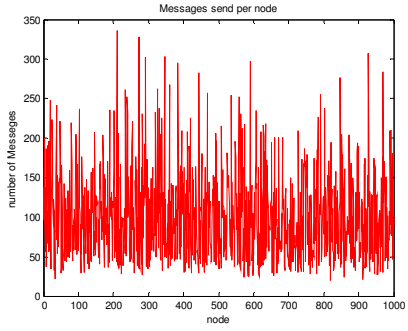


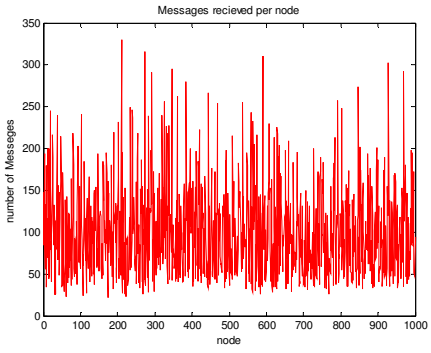
Παρατηρούμε ότι με λίγα πακέτα (20 ανά χρονική στιγμή) η χρήση του πρωτοκόλλου ασφαλείας δεν επηρεάζει το δίκτυο αφού το κάθε πακέτο ναι μεν έχει μια αύξηση του όγκου του σαν μονάδα αλλά διακινείται ελεύθερα στο δίκτυο χωρίς να επηρεάζει τον συνολικό φόρτο. Αυτό γιατί πάντα είναι αρκετά μικρότερος ο όγκος που μεταφέρεται

από το συνολικό bandwidth. Μια άλλη σημαντική παρατήρηση είναι ότι οι διαφορές στις μετρήσεις με την εφαρμογή των διαφόρων μεθόδων κρυπτογράφησης και πιστοποίησης είναι αμελητέες. Σε όλες τις άλλες περιπτώσεις οι ελάχιστες διαφορές που παρατηρούνται μπορεί να είναι αποτέλεσμα αλλαγών στο φυσικό μέσο, θορύβου κτλ.

Αντιθέτος παρατηρούμε ότι όταν ο όγκος των πακέτων αυξηθή τότε έχουμε μια επιβάρυνση αφού ο όγκος πλέον είναι αρκετά μεγάλος σε σχέση με την περίπτωση μη χρήσης πρωτοκόλλου ασφαλείας. Αυτό γιατί η εφαρμογή των διαφόρων μεθόδων κρυπτογράφησης αυξάνουν το μέγεθος του πακέτου που όταν όμως έχουμε χιλιάδες ανά χρονική στιγμή τότε το σύνολο μεταφοράς διογκώνεται με αποτέλεσμα να ξεπερνά το μέγιστο bandwidth.







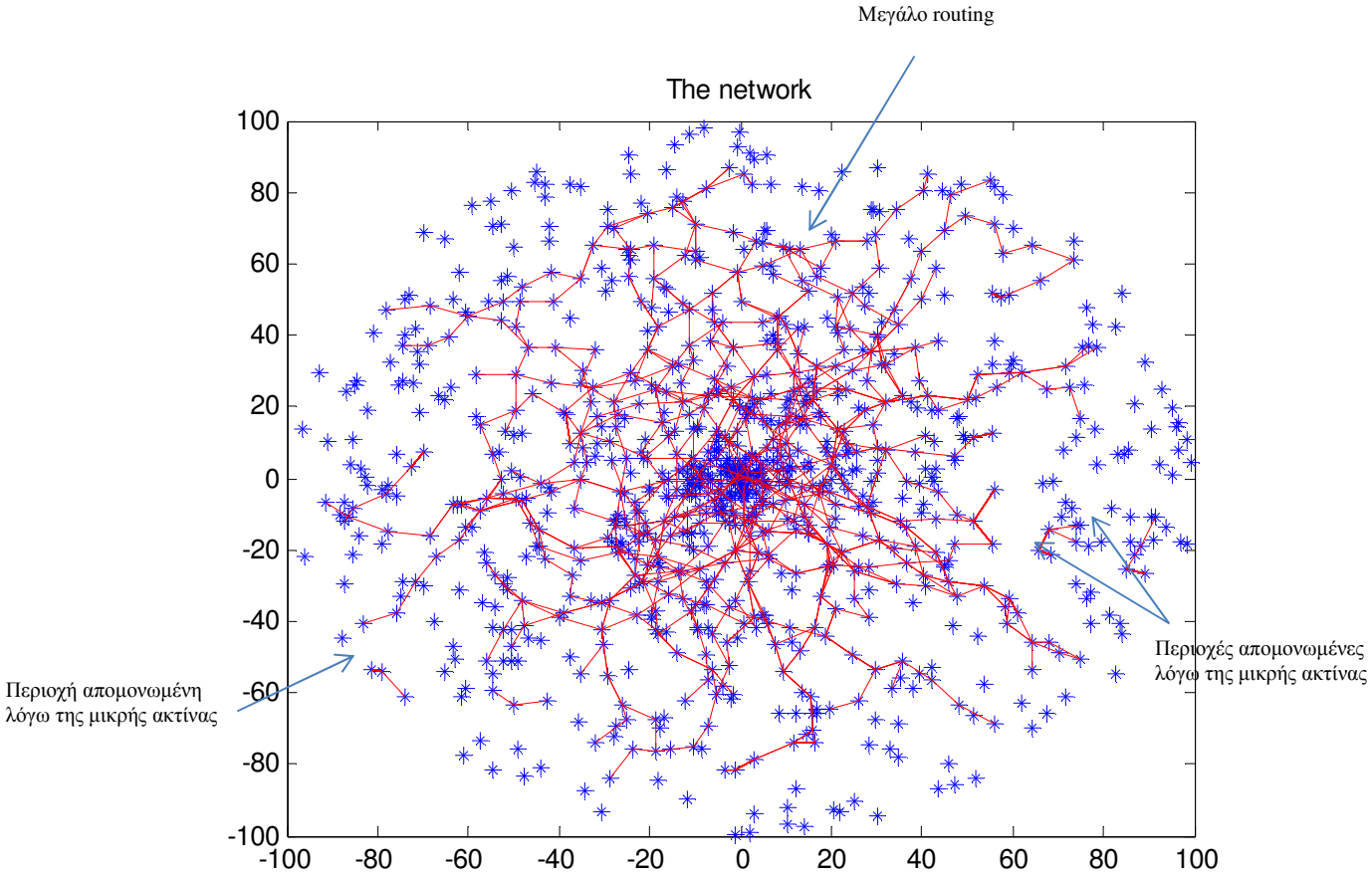
Ενεργειακά η χρήση των πρωτοκόλλων ασφαλείας παρατηρούμε ότι επηρεάζει την κάθε συσκευή του δικτύου αφού απαιτείται μεγαλύτερη υπολογιστική ισχύ λόγω των αλγορίθμων που εκτελούνται για την χρήση των πρωτοκόλλων ασφαλείας. Για παράδειγμα σε πακέτα UDP οι διαφορές είναι αμελητέες σε σύγκριση με την αποστολή χωρίς ασφάλεια. Αντίθετα, με πακέτα του απαιτητικότερου TCP έχει παρατηρηθεί πτώση της ταχύτητας των πακέτων με αποτέλεσμα την γρηγορότερη εξάντληση της μπαταρίας επομένως το δίκτυο αισθητήρων βρίσκεται πιο γρήγορα εκτός λειτουργίας.

Ακτίνα αντίληψης κόμβου δικτύου

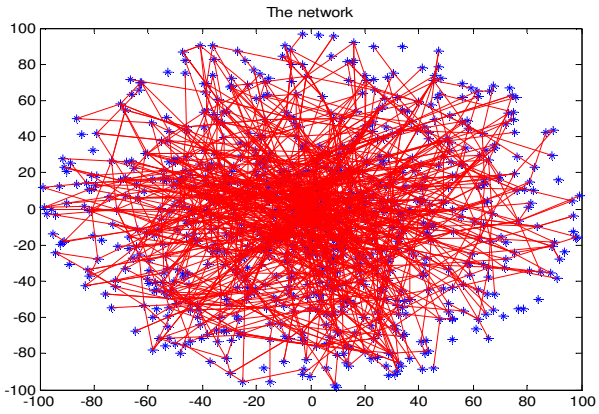
Σημαντικό ρόλο στα ασύρματα δίκτυα παίζει η ακτίνα αντίληψης των κόμβων του δικτύου μας. Η ακτίνα αντίληψης είναι η ακτίνα που ένας κόμβος αντιλαμβάνεται ένα άλλο. Σε αύτη την περίπτωση αν η ακτίνα είναι μικρή τότε υπάρχει περίπτωση να υπάρχουν περιοχές «απομονωμένες» δηλαδή πακέτα που απευθύνονται σε άλλους κόμβους να μην μπορούν να φτάσουν αφού δεν μπορούν να προσεγγιστούν κόμβοι που κάνουν routing.

Παρακάτω φαίνεται η επίδραση της ακτίνας αντίληψης:

Στην παρακάτω περίπτωση έχουμε r=0.1R όπου R η ακτίνα δικτύου.



Στην παρακάτω περίπτωση έχουμε r=0.3R όπου R η ακτίνα δικτύου (δηλαδή η μέγιστη ακτίνα που μπορούν να βρεθούν δύο κόμβοι μακριά).



Ο όγκος μεταφοράς λοιπόν στο δίκτυο επηρεάζεται με την χρήση ή όχι των πρωτοκόλλων αλλά και η ακτίνα αντίληψης των κόμβων επηρεάζει το ασύρματο δίκτυο ανεξάρτητα του πρωτοκόλλου που χρησιμοποιείται.

ΑΝΑΦΟΡΕΣ

[1]. I.F. Akyildiz,W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless Sensor Networks: A Survey”. Computer Networks (Elsevier), March 2002.

[2]. Ian Akyildiz, Weilian Su, Yogesh Sankarasubramanian, Erdal Cayirci, “A Survey on Sensor Network,” IEEE Communications Magazines, August, 2002.

[3]. Malik Tubaishat and Sanjay Madria, “Sensor networks: an overview”, IEEE Potentials, 22(2):20--23, April-May 2003.

[4]. Ning Xu, “A Survey of Sensor Network Applications”, Computer Science Department, University of Southern California. (http://courses.cs.tamu.edu/rabi/cpsc617/resources/sensor%20nw-survey.pdf)

[5]. C. Perkins, “Ad Hoc Networks”, Addison-Wesley, Reading, MA, 2000.

[6]. G. Hoblos, M. Staroswiecki, A. Aitouche, “Optimal design of fault tolerant sensor networks”, IEEE International Conference on Control Applications, Anchorage, AK, September 2000, pp. 467-472.

[7]. D. Nadig, S.S. Iyengar, “A new architecture for distributed sensor integration”, Proceedings of IEEE Southeastcon'93, Charlotte, NC, April 1993.

[8]. C. Shen, C. Srisathapornphat, C. Jaikaeo, “Sensor information networking architecture and applications”, IEEE Personal Communications, August 2001, pp. 52-59.

[9]. S. Cho, A. Chandrakasan, “Energy-efficient protocols for low duty cycle wireless microsensor”, Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Maui, HI Vol. 2 (2000), p. 10.

[10]. N. Bulusu, D. Estrin, L. Girod, J. Heidemann, “Scalable coordination for wireless sensor networks: self-configuring localization systems”, International Symposium on Communication Theory and Applications (ISCTA 2001), Am-bleside, UK, July 2001.

[11]. A. Sinha, A. Chandrakasan, “Dynamic power management in wireless sensor networks”, IEEE Design and Test of Computers, March/April 2001.

[12]. E.M. Petriu, N.D. Georganas, D.C. Petriu, D. Makrakis, V.Z. Groza, “Sensor-based information appliances”, IEEE Instrumentation and Measurement Magazine (December 2000) 31-35.

[13]. A. Cerpa, J. Elson, M. Hamilton, J. Zhao, “Habitat monitoring: application driver for wireless communications technology”, ACM SIGCOMM'2000, Costa Rica, April 2001.

[14]. J.M. Rabaey, M.J. Ammer, J.L. da Silva Jr., D. Patel, S. Roundy, “PicoRadio supports ad hoc ultra-low power wireless networking”, IEEE Computer Magazine (2000) 42-48.

[15]. J. Rabaey, J. Ammer, J.L. da Silva Jr., D. Patel, “Pico-Radio: ad-hoc wireless networking of ubiquitous low-energy sensor/monitor nodes”, Proceedings of the IEEE Computer Society Annual Workshop on VLSI (WVLSI'OO), Orlanda, Florida, April 2000, pp. 9-12.

[16]. C. Intanagonwiwat, R. Govindan, D. Estrin, “Directed diffusion: a scalable and robust communication paradigm for sensor networks”, Proceedings of the ACM Mobi-Com'OO, Boston, MA, 2000, pp. 56-67.

[17]. G.J. Pottie, W.J. Kaiser, “Wireless integrated network sensors”, Communications of the ACM 43 (5) (2000) 551-558.

[18]. J.M. Kahn, R.H. Katz, K.S.J. Pister, “Next century challenges: mobile networking for smart dust”, Proceedings of the ACM MobiCom'99, Washington, USA, 1999, pp. 271-278.

[19]. S. Vardhan, M. Wilczynski, G. Pottie, W.J. Kaiser, “Wireless integrated network sensors (WINS): distributed in situ sensing for mission and flight systems”, IEEE Aerospace Conference, Vol. 7, 2000, pp. 459-463.

[20]. E. Shih, S. Cho, N. Ickes, R. Min, A. Sinha, A. Wang, A. Chandrakasan, “Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks”, Proceedings of ACM MobiCom'Ol, Rome, Italy, July 2001, pp. 272-286.

[21]. A. Perrig, R. Szewczyk, V. Wen, D. Culler, J.D. Tygar, “SPINS: security protocols for sensor networks”, Proceedings of ACM MobiCom'Ol, Rome, Italy, 2001, pp. 189-199.

[22]. L. Li, J.Y. Halpern, “Minimum-energy mobile wireless networks revisited”, IEEE International Conference on Communications ICC'Ol, Helsinki, Finland, June 2001.

[23]. A. Savvides, C. Han, M. Srivastava, “Dynamic fine-grained localization in ad-hoc networks of sensors”, Proceedings of ACM MobiCom'Ol, Rome, Italy, July 2001, pp. 166-179.

[24]. S. Meguerdichian, F. Koushanfar, G. Qu, M. Potkonjak, “Exposure in wireless ad-hoc sensor networks”, Proceedings of ACM MobiCom'Ol, Rome, Italy, 2001, pp. 139-150.

[25]. A. Porret, T. Melly, C.C. Enz, E.A. Vittoz, “A low-power low-voltage transceiver architecture suitable for wireless distributed sensors network”, IEEE International Symposium on Circuits and Systems'OO, Geneva, Vol. 1, 2000, pp. 56-59.

[26]. P. Favre et al., “A 2V, 600 µA, 1 GHz BiCMOS super regenerative receiver for ISM applications”, IEEE Journal of Solid State Circuits 33 (1998) 2186-2196.

[27]. T. Melly, A. Porret, C.C. Enz, E.A. Vittoz, ”A 1.2 V, 430 MHz, 4dBm power amplifier and a 250 µW Frontend, using a standard digital CMOS process”, IEEE International Symposium on Low Power Electronics and Design Conference, San Diego, August 1999, pp. 233-237.

[28]. A. Woo, D. Culler, “A transmission control scheme for media access in sensor networks”, Proceedings of ACM MobiCom'Ol, Rome, Italy, July 2001, pp. 221-235.

[29]. B. Warneke, B. Liebowitz, K.S.J. Pister, “Smart dust: communicating with a cubic-millimeter computer”, IEEE Computer (January 2001) 2-9.

[30]. National Semiconductor Corporation, “LMX3162 Single Chip Radio Transceiver”, Evaluation Notes and Datasheet, March 2000.

[31]. K. Govil, E. Chan, H. Wasserman, “Comparing algorithms for dynamic speed-setting of a low-power CPU”, Proceedings of ACM MobiCom'95, Berkeley, CA, November 1995, pp. 13-25.

[32]. J. Lorch, A. Smith, “Reducing processor power consump-tion by improving processor time management in a single-user operating system”, Proceedings of ACM MobiCom'96, 1996.

[33]. M. Weiser et al., “Scheduling for reduced CPU energy”, Proceedings of 1st USENIX Symposium on Operating System Design and Implementation, November 1994, pp. 13-23.

[34]. D. Estrin, R. Govindan, J. Heidemann, S. Kumar, “Next century challenges: scalable coordination in sensor networks”, ACM MobiCom'99, Washingtion, USA, 1999, pp. 263-270.

[35]. J. Agre, L. Clare, “An integrated architecture for cooperative sensing networks”, IEEE Computer Magazine (May 2000) 106-108.

[36]. M. Bhardwaj, T. Garnett, A.P. Chandrakasan, “Upper bounds on the lifetime of sensor networks”, IEEE International Conference on Communications ICC'Ol, Helsinki, Finland, June 2001.

[37]. P. Bonnet, J. Gehrke, P. Seshadri, “Querying the physical world”, IEEE Personal Communications (October 2000) 10-15.

[38]. A. Cerpa, D. Estrin, “ASCENT: adaptive self-configuring sensor networks topologies”, UCLA Computer Science Department Technical Report UCLA/CSDTR-01-0009, May 2001.

[39]. B. Halweil, “Study finds modern farming is costly”, World Watch 14 (1) (2001) 9-10.

[40]. W.R. Heinzelman, J. Kulik, H. Balakrishnan, “Adaptive protocols for information dissemination in wireless sensor networks”, Proceedings of the ACM MobiCom'99, Seattle, Washington, 1999, pp. 174-185.

[41]. C. Jaikaeo, C. Srisathapornphat, C. Shen, “Diagnosis of sensor networks”, IEEE International Conference on Communications ICC'Ol, Helsinki, Finland, June 2001.

[42]. With Glacier Park in Its Path, Fire Spreads to 40,000 Acres, New York Times, Vol. 150, Issue 51864, p. 24, Op, 1 map, 4c, 9/2/2001.

[43]. S. Slijepcevic, M. Potkonjak, “Power efficient organization of wireless sensor networks”, IEEE International Conference on Communications ICC'Ol, Helsinki, Finland, June 2001.

[44]. http://www.fao.org/sd/Eldirect/Elre0074.htm.

[45]. A. Chandrakasan, R. Amirtharajah, S. Cho, J. Goodman, G. Konduri, J. Kulik, W. Rabiner, A. Wang, “Design considerations for distributed micro-sensor systems”, Proceedings of the IEEE 1999 Custom Integrated Circuits Conference, San Diego, CA, May 1999, pp. 279-286.

[46]. M. Gell-Mann, “What is complexity?” Complexity 1 (1), 1995.

[47]. L. Girod, D. Estrin, “Robust range estimation using acoustic and multimodal sensing”, Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS 2001), Maui, Hawaii, October 2001.

[48]. R. Colwell, Testimony of Dr. Rita Colwell, Director, National Science Foundation, Before the Basic Research Subcommitte, House Science Committe, Hearing on Re-mote Sensing as a Research and Management Tool, September 1998.

[49]. T.H. Keitt, D.L. Urban, B.T. Milne, Detecting critical scales in fragmented landscapes, Conservation Ecology 1 (1) (1997) 4. Available from <http://www.consecolo.org/voll/issl/art4>.

[50]. M.P. Hamilton, M. Flaxman, Scientific data visualization and biological diversity: new tools for spatializing multi-media observations of species and ecosystems, Landscape and Urban Planning 21 (1992) 285-297.

[51]. M.P. Hamilton, Hummercams, robots, and the virtual reserve, Directors Notebook, February 6, 2000, available from http://www.jamesreserve.edu/news.html.

[52]. http://www.alertsystems.org.

[53]. T. Imielinski, S. Goel, DataSpace: querying and monitor-ing deeply networked collections in physical space, ACM International Workshop on Data Engineering for Wireless and Mobile Access MobiDE 1999, Seattle, Washington, 1999, pp. 44-51.

[54]. N. Noury, T. Herve, V. Rialle, G. Virone, E. Mercier, G. Morey, A. Moro, T. Porcheron, Monitoring behavior in home using a smart fall sensor, IEEE-EMBS Special Topic Conference on Microtechnologies in Medicine and Bio-logy, October 2000, pp. 607-610.

[55]. P. Johnson et al., Remote continuous physiological mon-itoring in the home, Journal of Telemed Telecare 2 (2) (1996) 107-113.

[56]. M. Ogawa et al., Fully automated biosignal acquisition in daily routine through 1 month, International Conference on IEEE-EMBS, Hong Kong, 1998, pp. 1947-1950.

[57]. B.G. Celler et al., An instrumentation system for the remote monitoring of changes in functional health status of the elderly, International Conference IEEE-EMBS, New York, 1994, pp. 908-909.

[58]. G. Coyle et al., Home telecare for the elderly, Journal of Telemedicine and Telecare 1 (1995) 183-184.

[59]. Y.H. Nam et al., Development of remote diagnosis system integrating digital telemetry for medicine, International Conference IEEE-EMBS, Hong Kong, 1998, pp. 1170-1173.

[60]. P. Bauer, M. Sichitiu, R. Istepanian, K. Premaratne, The mobile patient: wireless distributed sensor networks for patient monitoring and care, Proceedings 2000 IEEE EMBS International Conference on Information Technol-ogy Applications in Biomedicine, 2000, pp. 17-21.

[61]. B. Sibbald, Use computerized systems to cut adverse drug events: report, CMAJ: Canadian Medical Association Journal 164 (13) (2001) 1878, l/2p, 1c.

[62]. G.D. Abowd, J.P.G. Sterbenz, Final report on the inter-agency workshop on research issues for smart environ-ments, IEEE Personal Communications (October 2000) 36-40.

[63]. C. Herring, S. Kaplan, Component-based software systems for smart environments, IEEE Personal Communications, October 2000, pp. 60-61.

[64]. LA. Essa, Ubiquitous sensing for smart and aware environments, IEEE Personal Communications (October 2000) 47-49.

[65]. D. Estrin, R. Govindan, J. Heidemann, Embedding the Internet, Communication ACM 43 (2000) 38-41.

[66]. N. Priyantha, A. Chakraborty, H. Balakrishnan, The cricket location-support system, Proceedings of ACM MobiCom'OO, August 2000, pp. 32-43.

[67]. E. Shih, B.H. Calhoun, S. Cho, A. Chandrakasan, Energy-efficient link layer for wireless microsensor networks, Proceedings IEEE Computer Society Workshop on VLSI 2001, Orlando, FL, April 2001, pp. 16-21.

[68]. C. Chien, I. Elgorriaga, C. McConaghy, Low-power direct-sequence spread-spectrum modem architecture for distrib-uted wireless sensor networks, ISLPED'Ol, Huntington Beach, California, August 2001.

[69]. J.M. Cramer, R.A. Scholtz, M.Z. Win, On the analysis of UWB communication channels, IEEE MILCOM'99, 1999, pp. 1191-1195.

[70]. F.R. Mireles, R.A. Scholtz, Performance of equicorrelated ultra-wideband pulse-position-modulated signals in the indoor wireless impulse radio channel, IEEE Conference on Communications, Computers and Signal Processing, Vol. 2, 1997, pp. 640-644.