ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
Κατεύθυνση: *Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων*

Μάθημα: Ασφάλεια Δικτύων Υπολογιστών ΙΙ

Υπεύθυνοι Καθηγητές: Σ. Γκρίτζαλης, Γ. Καμπουράκης

Τίτλος Εργασίας:

Ασφάλεια στο πρότυπο IEEE 802.16 (WiMAX)

Φοιτητές

Δουλγέρη Χριστίνα	icsdm05029@icsd.aegean.gr
Κεμαλής Κωνσταντίνος	icsdm05031@icsd.aegean.gr
Μακροβασίλης Αθανάσιος	icsdm05032@icsd.aegean.gr

Καρλόβασι, Μάιος 2006

Περιεχόμενα

1. Εισαγωγή στο WiMax

Το πρότυπο 802.16 είναι γνωστό και ως WiMAX που σημαίνει Worldwide Interoperability for Microwave Access. Το WiMAX δεν είναι ένα πρότυπο αλλά ένα εμπορικό όνομα που αναφέρεται σε κάθε σύστημα και εφαρμογή που χρησιμοποιεί το πρότυπο 802.16.

Η κατασκευή του προτύπου 802.16 άρχισε ως μια πρωτοβουλία της National Wireless Electronics Systems Testbed (N-WEST) η οποία οργάνωσε μια πρώτη συνάντηση κατά την IEEE Radio and Wireless Conference (RAWCON) το 1998. Η ομάδα των 45 εταιρειών μελών της N-WEST δέχτηκε την πρόσκληση και έτσι προέκυψε η συνάντηση με την επιτροπή 802 της IEEE. Έτσι λοιπόν συστήθηκε η πρώτη ερευνητική ομάδα που θα δημιουργούσε το πρότυπο με επικεφαλής τον Roger Marks. Η ομάδα αυτή συναντήθηκε δύο φορές και έγραψε το Task Group1 PAR.Στη συνέχεια έγιναν και άλλες σύνοδοι και αναπτύχθηκαν άλλα Task Group.

Το 2003 η IEEE υιοθέτησε το πρότυπο 802.16, ώστε να ικανοποιήσει τις απαιτήσεις για ασύρματη πρόσβαση ευρείας ζώνης. Όπως συμβαίνει με τα πρότυπα της σειράς 802 για ασύρματα τοπικά δίκτυα LAN, έτσι και το 802.16 καθορίζει μια οικογένεια προτύπων με επιλογές για συγκεκριμένες ρυθμίσεις.

Το πρότυπο αυτό σχεδιάστηκε ώστε να λειτουργεί σε μια ευρεία μπάντα συχνοτήτων η οποία εκτείνεται από 2 ως 66 GHz. Υποστηρίζει ταχύτητες μετάδοσης ως και 72 Mbps στον αέρα ενώ η πραγματική ταχύτητα στο Ethernet υπολογίζεται στα 50Mbps. Οι αποστάσεις που μπορεί να καλυφθούν ξεπερνούν τα 50 χλμ. σε συνθήκες οπτικής επαφής. Μια σημαντική διαφορά του προτύπου IEEE 802.16 σε σχέση με το IEEE 802.11 είναι ότι το πρώτο μπορεί να χρησιμοποιηθεί και σε συνθήκες μη οπτικής επαφής φυσικά με ρυθμούς μετάδοσης πολύ χαμηλότερους των 50Mbps.

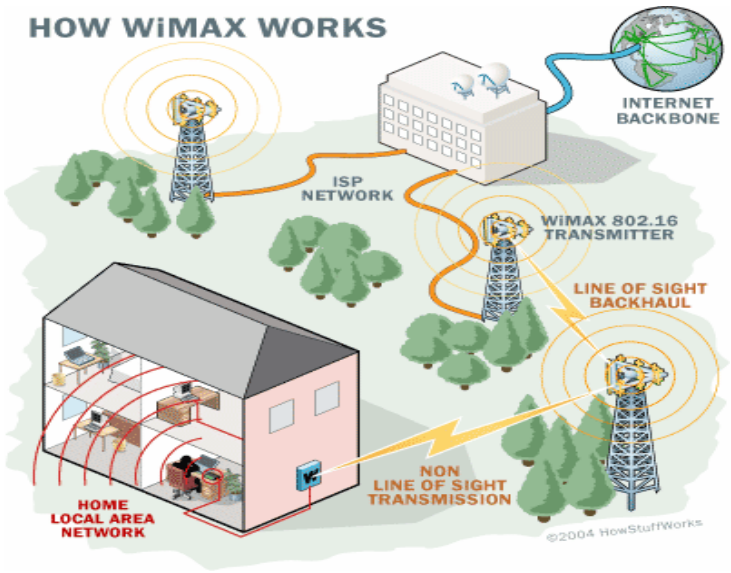
Το WiMAX σχεδιάστηκε κατά βάση ώστε να καλύπτει κυρίως Point-to-Multipoint (PTM) συνδέσεις χωρίς ωστόσο να αποκλείεται και η χρήση του για Point-to-Point (PTP) συνδέσεις. Η διαμόρφωση η οποία χρησιμοποιείται είναι η Orthogonal Frequency Division Multiplexing (OFDM). Πρόκειται για μια πολύ ανθεκτική διαμόρφωση σε ότι αφορά το φαινόμενο της πολυδιόδευσης ειδικότερα στις συχνότητες πάνω των 2 GHz όπου το πρότυπο χρησιμοποιεί. Τυπικά, ένα σύστημα WiMAX αποτελείται από δύο μέρη (Εικόνα 1):

- Ένας Σταθμός Βάσης WiMAX (Base Station - BS): Ο σταθμός βάσης αποτελείται από τις ηλεκτρονικές εγκαταστάσεις και έναν πύργο WiMAX.

Χαρακτηριστικά, ένας σταθμός βάσης μπορεί να καλύψει ακτίνα μέχρι 10 χλμ (θεωρητικά, ένας σταθμός βάσης μπορεί να καλύψει ακτίνα μέχρι 50 χλμ. Οποιοσδήποτε ασύρματος κόμβος μέσα στην περιοχή κάλυψης θα είναι σε θέση να έχει πρόσβαση στο Διαδίκτυο.

- Ένας δέκτης WiMAX (Subscriber Station - SS): Ο δέκτης και η κεραία θα μπορούσαν να είναι ένα αυτόνομο κιβώτιο ή μια κάρτα PCMCIA που βρίσκεται σε ένα laptop ή υπολογιστή . Η πρόσβαση στο σταθμό βάσης WiMAX είναι παρόμοια με στην πρόσβαση ενός ασύρματου σημείου πρόσβασης σε ένα δίκτυο Wi-Fi, αλλά η κάλυψη είναι μεγαλύτερη.

Διάφοροι σταθμοί βάσεων μπορούν να συνδέονται μεταξύ τους μέσω backhaul συνδέσεων μικροκυμάτων μεγάλης ταχύτητας. Αυτό θα επέτρεπε την περιπλάνηση ενός συνδρομητή WiMAX από έναν σταθμό βάσης σε μια άλλη περιοχή σταθμού βάσης, παρόμοια με την περιπλάνηση που επιτρέπεται από τις επιχειρήσεις κινητής τηλεφωνίας.



Εικόνα 1. Σταθμοί βάσης και σταθμοί συνδρομητών WiMAX.

1.1. Ασύρματα Ευρυζωνικά Δίκτυα (BWA)

Πριν γίνει η περιγραφή του WiMax πρέπει να οριστεί τι είναι τα ασύρματα ευρυζωνικά δίκτυα. Τα ασύρματα ευρυζωνικά δίκτυα είναι αυτά που:

- Επιτυγχάνουν ασύρματες συνδέσεις χρησιμοποιώντας μικροκύματα ή χιλιοστομετρικά ραδιοκύματα.
- Χρησιμοποιούν (συνήθως) επιτρεπτές συχνοτικές μπάντες.

- Είναι μητροπολιτικά σε κλίμακα (MAN).
- Παρέχουν δημόσιες δικτυακές υπηρεσίες σε πελάτες με χρηματικό αντάλλαγμα.
- Χρησιμοποιούν PTM αρχιτεκτονική χρησιμοποιώντας κεραίες-πύργους.
- Παρέχουν ικανοποιητική μεταφορά ετερογενών μηνυμάτων, με βασικό στόχο τη ποιότητα παροχής υπηρεσιών (QoS).
- Υποστηρίζουν ικανοποιητικό ρυθμό μεταφοράς δεδομένων, μεγαλύτερο των 2Mbps.

Η τεχνολογία που βασίζεται στο πρότυπο 802.16 σχεδιάστηκε εξ' ολοκλήρου για να προσφέρει ασύρματη επικοινωνία σε μητροπολιτικά δίκτυα και να παρέχει υπηρεσίες ανταγωνιστικές στις ήδη υπάρχουσες ενσύρματες δικτυακές τεχνολογίες (DSL, cable, T1).

1.2. Βασικοί στόχοι και Επιτεύγματα του 802.16

Πριν γίνει ανάλυση της αρχιτεκτονικής του προτύπου IEEE 802.16 πρέπει να αναφέρουμε τους βασικούς στόχους και άξονες που έθεσε η εργασιακή ομάδα του IEEE 802.16 για τη δημιουργία ενός στιβαρού και ευέλικτου προτύπου.

Η εργασιακή ομάδα έδωσε τα εξής χαρακτηριστικά στο πρότυπο. Αρχικά βασικό χαρακτηριστικό του προτύπου είναι η διεκπαιρεωτική ικανότητα (throughput). Επίσης πολύ σημαντικό για τη διάδοση του είναι η επεκτασιμότητα (scalability), η εμβέλεια (coverage) και η παροχή υψηλής ποιότητας υπηρεσιών (QoS). Τέλος μεγάλο βάρος έδωσαν στο θέμα της ασφάλειας. Αυτά τα χαρακτηριστικά αναλύονται παρακάτω.

1.2.1. 802.16 Διεκπαιρεωτική ικανότητα (Throughput)

Το πρότυπο IEEE 802.16 επιτυγχάνει πολύ μεγάλη διεκπαιρεωτική ικανότητα ακόμα και σε μεγάλες αποστάσεις αφού έχει ένα πολύ μεγάλο φάσμα εκπομπής που είναι ιδιαίτερα ανθεκτικό σε αντανακλάσεις του σήματος κατά τη διάρκεια της διαδρομής του. Οι ρυθμοί μετάδοσης του προτύπου εξαρτώνται από την εκάστοτε ψηφιακή διαμόρφωση που χρησιμοποιείται. Στο πρότυπο 802.16 οι σταθμοί βάσης έχουν την δυνατότητα δυναμικά να ρυθμίζουν την απόσταση εκπομπής ή καλύτερα το βελησνεκές εκπομπής με την διεκπαιρεωτική ικανότητα.

1.2.2. 802.16 Επεκτασιμότητα (Scalability)

Το πρότυπο IEEE 802.16 υποστηρίζει ευέλικτα από την άποψη εύρους ζώνης κανάλια επικοινωνίας ώστε να μπορεί να γίνει εύκολος και επεκτάσιμος ο σχεδιασμός κυψελών επικοινωνίας σε επιτρεπόμενες και μη συχνοτικές μπάντες . Για παράδειγμα αν σε κάποιο χειριστή ανατεθεί συχνοτικό φάσμα των 20 MHz, τότε αυτός μπορεί να χωρίσει το φάσμα σε δύο κομμάτια των 10 MHz ή ακόμα σε τέσσερα κομμάτια των 5 MHz. Συγκεντρώντας έτσι όλη την ενέργεια σε ένα πολύ μικρό φάσμα συχνοτήτων ο χειριστής μπορεί να αυξήσει τον αριθμό των χρηστών επιτυγχάνοντας παράλληλα μεγάλο βεληνεκές και διεκπαιρεωτική ικανότητα. Για να επεκτείνει ακόμα περισσότερο την εμβέλεια του σήματος ο χειριστής μπορεί να χωρίσει ακόμα περισσότερο το φάσμα συχνοτήτων δημιουργώντας απομόνωση μεταξύ των κεραιών των σταθμών βάσης.

1.2.3. 802.16 Εμβέλεια (Coverage)

Το πρότυπο IEEE 802.16 κατασκευάζεται έτσι ώστε να υποστηρίζει τεχνολογίες που αυξάνουν την εμβέλεια του σήματος όπως τοπολογίες πλέγματος και έξυπνες κεραίες. Οι τοπολογίες πλέγματος είναι αυτές όπου κάθε κόμβος συνδέεται άμεσα με κάθε άλλο κόμβο του δικτύου. Όσο λοιπόν οι ράδιο-τεχνολογίες βελτιώνονται και το κόστος μειώνεται, μεγαλώνει και η δυνατότητα αύξησης της εμβέλειας και της διεκπαιρεωτικής ικανότητας με τη χρήση πολλαπλών κεραιών καθώς ενθαρρύνεται και η εξάπλωση της εμβέλειας σε περιοχές που παλιότερα ήταν αδύνατο να εξαπλωθεί.

1.2.4. 802.16 Παροχή υψηλής ποιότητας υπηρεσιών (QoS)

Η παροχή υψηλής ποιότητας υπηρεσιών όπως μεταφορά φωνής, είναι εξαιρετικά σημαντική για υιοθέτηση και εξάπλωση του προτύπου. Για αυτό ακριβώς το λόγο το υποπρότυπο 802.16a συμπεριλαμβάνει κάποια ιδιαίτερα χαρακτηριστικά που κάνουν δυνατή τη μεταφορά φωνής και βίντεο αφού για να είναι εφικτή αυτή η μεταφορά χρειάζεται ένα χαμηλού φόρτου δίκτυο. Να σημειώσουμε εδώ ότι τα χαρακτηριστικά του Medium Access Control (MAC) του 802.16a δίνουν τη δυνατότητα σε ένα χειριστή να παρέχει ταυτόχρονα υπηρεσίες σε επιχειρήσεις (υπηρεσίες τύπου τεχνολογίας T1) και σε σπίτια (υπηρεσίες τύπου καλωδιακής επικοινωνίας) χρησιμοποιώντας τον ίδιο σταθμό βάσης.

1.2.5. 802.16 Ασφάλεια (Security)

Η ασφάλεια είναι ένα πολύ σημαντικό κομμάτι στην ανάπτυξη ενός πρότυπου. Η μυστικότητα και η κρυπτογράφηση είναι βασικά χαρακτηριστικά του προτύπου IEEE 802.16 για ασφαλή μεταφορά πληροφορίας. Η ασφάλεια του 802.16 βασίζεται στην κρυπτογράφηση δεδομένων αλλά και στην αυθεντικοποίηση. Το θέμα της ασφάλειας δεν είναι κάτι στατικό αλλά μεταβάλλεται συνεχώς με βάση κάθε φορά τα νέα δεδομένα και προβλήματα.

1.3. Χαρακτηρισμός Καναλιού

Το WiMAX μπορεί να παρέχει δύο είδη ασύρματων υπηρεσιών:

- Υπάρχει η δυνατότητα εξυπηρέτησης της περίπτωσης Line-Of-Sight (LOS), όπου μία σταθεροποιημένη κεραία δείχνει απευθείας στον πύργο WiMAX από κάποια στέγη ή άλλο υπερυψωμένο σημείο. Η LOS σύνδεση είναι πιο δυνατή και σταθερή και για αυτό μπορεί να μεταδίδει σημαντικό μέγεθος δεδομένων χωρίς πολλά λάθη.
- Υπάρχει η περίπτωση Non-Line-Of-Sight (NLOS), ένα είδος υπηρεσίας σαν το Wi-Fi, όπου μία μικρή κεραία στον προσωπικό υπολογιστή συνδέεται σε έναν πύργο. Σε αυτή την περίπτωση, το WiMAX χρησιμοποιεί ένα φάσμα χαμηλότερης συχνότητας της τάξης των 2 GHz με 11 GHz (παρόμοιο με το Wi-Fi). Μεταδόσεις χαμηλότερης κυματομορφής δεν είναι τόσο εύκολο να διακοπούν από φυσικά εμπόδια – μπορούν πολύ πιο εύκολα να διαθλαστούν ή να παρακάμψουν εμπόδια.

Όταν ζητείται η ασύρματη ζεύξη μεταξύ δύο σημείων είναι βασικό να γνωρίζουμε αν τα σημεία αυτά βρίσκονται σε συνθήκες LOS ή NLOS. Σε μια LOS ζεύξη σημείων, το ηλεκτρομαγνητικό κύμα κατευθύνεται απευθείας από την κεραία του πομπού στην κεραία του δέκτη χωρίς να υποστεί κάποια ανάκλαση από γειτονικά εμπόδια. Απαραίτητη προϋπόθεση για να συμβαίνει το παραπάνω είναι να είναι ελεύθερη από εμπόδια μια περιοχή του ασύρματου καναλιού μεταξύ των δύο σημείων προς επικοινωνία που ονομάζεται ζώνη του Fresnel. Η ζώνη Fresnel υπολογίζεται από τον παρακάτω τύπο:

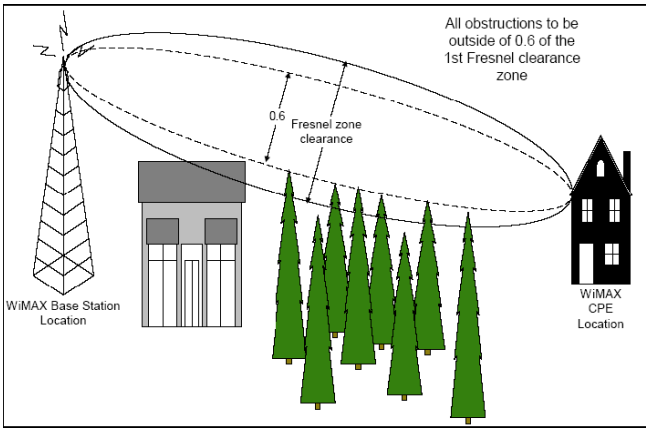
$$F_N = \sqrt{\frac{N_n \lambda \cdot D_1 \cdot D_2}{D_1 + D_2}}$$

όπου: N: ο αριθμός της ζώνης (πχ για N=1 έχουμε την 1η ζώνη Fresnel… κτλ)

λ: το μήκος κύματος και

D1,D2:οι αποστάσεις των δύο κεραιών από το εμπόδιο.

Τα παραπάνω παρουσιάζονται παραστατικά στην Εικόνα 2.



Εικόνα 2. Οι LOS ζώνες του Fresnel.

Όταν ένα εμπόδιο βρίσκεται μέσα στη πρώτη ζώνη του Fresnel τότε το κανάλι χαρακτηρίζεται σαν Optical Line of Site (OLOS). Το πρότυπο IEEE 802.16 μπορεί να παρέχει επικοινωνία και σε σημεία τα οποία βρίσκονται σε συνθήκες OLOS κάτι που ο προκάτοχος του (Wi-Fi) δύσκολα μπορούσε να πετύχει.

Η χρήση της διαμόρφωσης OFDM επιτρέπει στο WiMAX να εξασφαλίζει σταθερές και αξιόπιστες συνδέσεις ακόμα και σε συνθήκες NLOS (Εικόνα 3). Η τεχνική OFDM υποστηρίζει μετάδοση με πολλαπλές φέρουσες προσδίδοντας στο πρότυπο ανθεκτικότητα στη μετάδοση των δεδομένων και πολύ καλές επιδόσεις σε ότι αφορά το φαινόμενο της πολυδιόδευσης. Επιπλέον η χρήση κωδίκων διόρθωσης σφαλμάτων όπως οι Forward Error Correction (FEC) και Cyclic Redundancy Checking (CRC) προσδίδει στο πρότυπο τη δυνατότητα αξιόπιστης μετάδοσης κρατώντας σε χαμηλά επίπεδα την ισχύ εκπομπής και λήψης.

Εικόνα 3. Παράδειγμα NLOS σύνδεσης.

1.4. Τοπολογία

Το WiMAX σχεδιάστηκε τόσο για λειτουργίες ζεύξης PTP όσο και για λειτουργίες PTM. Η PTM ανάπτυξη δικτύου προϋποθέτει μια κυψελοειδούς μορφής αρχιτεκτονική, με κάθε περιοχή κυττάρων να καλύπτει μια ακτίνα μέχρι 5 ή 6 μιλίων και να χειρίζεται μέχρι αρκετές εκατοντάδες συνδρομητές. Ενώ η μέγιστη απόσταση που καλύπτει η τεχνολογία επεκτείνεται λίγο πάνω από 30 μίλια, είναι απίθανο να χρησιμοποιηθεί, με εξαίρεση μερικές back-haul PTP εφαρμογές.

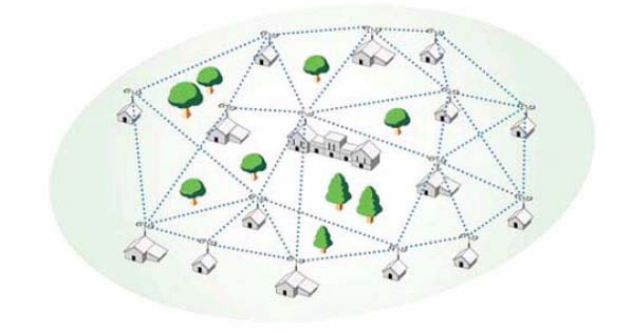
Ο Πίνακας 1 απεικονίζει τις αποστάσεις και τον ρυθμό μετάδοσης δεδομένων σε PTP ανάπτυξη δικτύου και σε PMP ανάπτυξη δικτύου.

Ρυθμός μετάδοσης δεδομένων (Mbps)	Απόσταση (χλμ.) σε PTP	Απόσταση (χλμ.) σε PMP
8	50	28
17	45	24
33	33	15
48	13	4

Πίνακας 1. Αποστάσεις επικοινωνίας PTP και PMP.

Μια συχνή επιλογή για την τοπολογία επικοινωνίας συνδρομητή με συνδρομητή στο WiMAX και στην περίπτωση NLOS είναι η τοπολογία πλέγματος (Εικόνα 4). Συμπεριλαμβάνεται στο πρότυπο για να επιτρέψει υπέρθετα δίκτυα στο φάσμα συχνοτήτων χωρίς άδεια και να επεκτείνει τα άκρα του βελησνεκούς του WMAN με χαμηλό κόστος. Η υποστήριξη της τοπολογίας πλέγματος έχει επεκταθεί πρόσφατα και στις εξουσιοδοτημένες ζώνες.

Αν και έχει ιδιαίτερα σύνθετη τοπολογία και τρόπο αποστολής μηνυμάτων, η τοπολογία πλέγματος είναι μια καλή εναλλακτική λύση στη συνηθισμένη περίπτωση NLOS, δεδομένου ότι κλιμακώνεται καλά και διαχειρίζεται την παρέμβαση που στερείται άδειας. Επιτρέπει σε μία κοινότητα να έχει πυκνές συνδέσεις WiMAX με χαμηλότερο κόστος, με δυνατές επικοινωνίες καθώς υπάρχουν πολλαπλές πορείες για να ακολουθήσει η κίνηση.



Εικόνα 4. Παράδειγμα Τοπολογίας Πλέγματος.

1.5. Πλεονεκτήματα WiMax

Τα βασικά πλεονεκτήματα των συστημάτων που βασίζονται στο WiMAX είναι τα εξής:

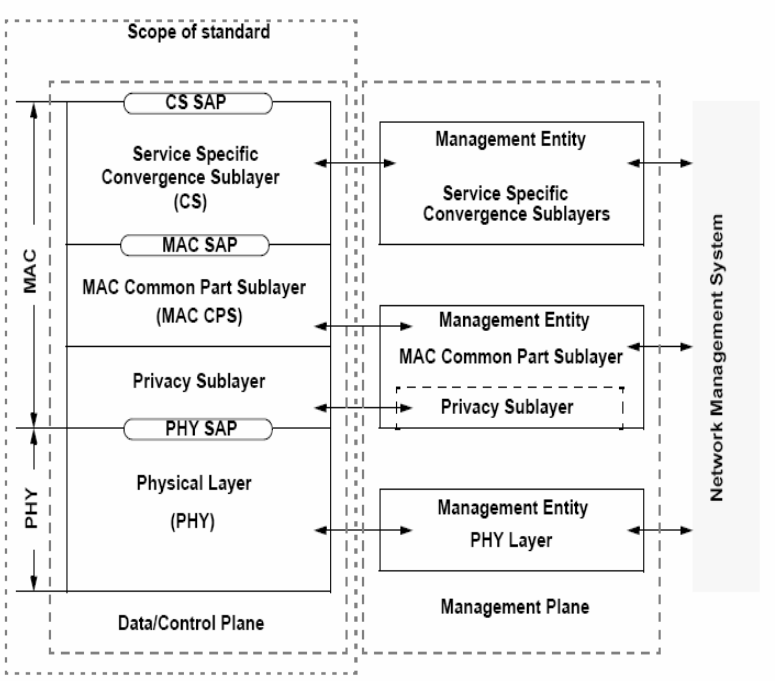
- Η ικανότητα γρήγορης παροχής υπηρεσιών ακόμα και σε περιοχές πολύ απομακρυσμένες όπου η εγκατάσταση ενσύρματων δικτύων θα ήταν εξαιρετικά δύσκολη.
- Αποφυγή μεγάλου κόστους εγκατάστασης.
- Η ικανότητα υπέρβασης των φυσικών περιορισμών που υπάρχουν στην ενσύρματη δικτύωση.

Συνοψίζοντας λοιπόν τα παραπάνω είναι φανερό ότι το WiMAX συνιστά ένα πολύ ευέλικτο και οικονομικό πρότυπο το οποίο μπορεί να καλύψει τις αδυναμίες της ενσύρματης δικτύωσης και επιπλέον να παρέχει νέες υπηρεσίες και προϊόντα.

2. Αρχιτεκτονική

Όπως όλα τα πρότυπα της σειράς 802 της IEEE, έτσι και το 802.16 επικεντρώνεται στα δύο χαμηλότερα στρώματα του μοντέλου διαστρωμάτωσης OSI, δηλαδή στο φυσικό επίπεδο (Physical Layer – PHY) και στο επίπεδο MAC. Οι αλλαγές που επιτελέστηκαν στα δύο παραπάνω στρώματα σε σχέση με το πρότυπο Wi-Fi είναι σημαντικές. Οι αλλαγές αυτές έχουν σαν κύριο στόχο τη δημιουργία ενός προτύπου το οποίο θα μπορούσε να καλύψει τα κενά που αφήνει ο προκάτοχος του (Wi-Fi) και ταυτόχρονα να κάνει γεγονός την Ασύρματη Ευρυζωνική Πρόσβαση.

Η στοίβα πρωτοκόλλων του WiMAX παρουσιάζεται στην Εικόνα 5. Το Service Access Point (SAP) αποτελεί το σημείο επικοινωνίας ενός υποεπιπέδου με το άλλο.



Εικόνα 5. Στοίβα πρωτοκόλλων του 802.16.

Ξεκινώντας από κάτω προς τα πάνω παρατηρούμε ότι το χαμηλότερο επίπεδο είναι το φυσικό επίπεδο το οποίο ασχολείται με τη μετάδοση. Εκεί χρησιμοποιείται η παραδοσιακή μετάδοση ραδιοκυμάτων στενής ζώνης με συμβατικές μεθόδους διαμόρφωσης. Πιο πάνω παρατηρούμε ότι το MAC επίπεδο αποτελείται από τρία υποεπίπεδα. Το πρώτο από αυτά είναι το υποεπίπεδο σύγκλισης εξαρτώμενο από την υπηρεσία (Convergence Sublayer - CS). Γενικά θα μπορούσαμε να πούμε ότι η δουλειά αυτού του υποεπιπέδου είναι η διασύνδεση με το επίπεδο δικτύου. Το επίπεδο που ακολουθεί είναι το MAC υποεπιπέδο κοινού τμήματος (Common Part Sublayer - CPS). Εδώ βρίσκονται τα βασικά πρωτόκολλα όπως η διαχείριση του καναλιού. Το μοντέλο είναι ότι ο BS ελέγχει το σύστημα. Μπορεί δηλαδή να χρονοπρογραμματίσει τα κατερχόμενα κανάλια (τα κανάλια δηλαδή από τον BS προς τον SS), ενώ παίζει ρόλο και στη διαχείριση των ανερχόμενων καναλιών (δηλαδή των καναλιών από τον SS προς τον BS). Το τελευταίο υποεπίπεδο είναι το υποεπίπεδο ιδωτικότητας (Privacy Sublayer - PS). Αυτό το επίπεδο προσφέρει αυθεντικοποίηση, ανταλλαγή κλειδιού ασφαλείας και κρυπτογράφηση.

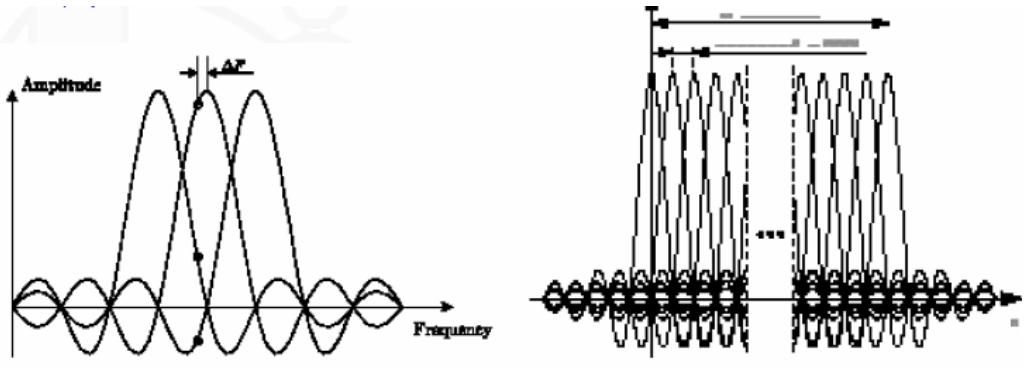
2.1. Φυσικό Επίπεδο

Το φυσικό επίπεδο αναφέρεται στο κομμάτι της μετάδοσης της πληροφορίας για την οποία χρησιμοποιείται η παραδοσιακή μετάδοση ραδιοκυμάτων στενής ζώνης. Όπως φαίνεται από το σχήμα της στοίβας του πρωτοκόλλου, οι υπηρεσίες του φυσικού επιπέδου παρέχονται στο MAC υποεπίπεδο μέσω του PHY SAP.

2.1.1. OFDM

Στο φυσικό επίπεδο η διαμόρφωση η οποία έχει υιοθετηθεί από το WiMAX είναι το OFDM. Ένας από τους κυριότερους λόγους υιοθέτησης του OFDM ως του μοντέλου διαμόρφωσης για ένα ασύρματο τηλεπικοινωνιακό σύστημα είναι η μεγάλη αντοχή που επιδεικνύει σε περιβάλλοντα εξασθένησης σήματος και παρεμβολών. Σε συστήματα μονής φέρουσας ένας επίδοξος παρεμβολέας μπορεί να προκαλέσει ακόμα και την κατάρρευση μιας σύνδεσης, σε αντίθεση με τα συστήματα πολλών φερουσών, όπου ένα μικρό μόνο ποσοστό των φερουσών θα επηρεαστεί. Μία από τις προτεινόμενες λύσεις για βέλτιστη αντιμετώπιση του προβλήματος είναι η χρήση της Κωδικοποίησης Διόρθωσης Σφάλματος (Error Correction Coding - ECC).

Σε ένα κλασικό σύστημα παράλληλης μετάδοσης δεδομένων η συνολικά διαθέσιμη μπάντα συχνοτήτων διαιρείται σε N μη επικαλυπτόμενα υποκανάλια συχνοτήτων. Κάθε υποκανάλι διαμορφώνεται και από διαφορετικό σύμβολο και ακολούθως τα N υποκανάλια πολυπλέκονται στο πεδίο των συχνοτήτων. Η ιδέα που εισήγαγε το OFDM ήταν πρωτοποριακή μιας και οδηγούσε στην εξοικονόμηση φάσματος. Πιο συγκεκριμένα, έκανε λόγο για χρήση επικαλυπτόμενων υποκαναλιών, που χαρακτηρίζονται από την κοινή ιδιότητα της μεταξύ τους ορθογωνιότητας γεγονός που οδηγεί στην αποφυγή ισοστάθμισης, την αντιμετώπιση θορύβου και εξασθένησης σήματος λόγω πολυδιόδευσης καθώς και την πλήρη αξιοποίηση του διαθέσιμου φάσματος.



Εικόνα 6. (a) Συμβατική Τεχνική Πολλών Φερουσών (b) OFDM

Στην Εικόνα 6 είναι φανερή η διαφορά μεταξύ των συμβατικών τεχνικών με μη επικαλυπτόμενα υποκανάλια και του OFDM. Κατά αυτό τον τρόπο επιτυγχάνεται εξοικονόμηση εύρους φάσματος που αγγίζει κατά περίπτωση ακόμα και το 50%. Βέβαια όπως προαναφέρθηκε πρέπει να εξασφαλιστεί η όσο το δυνατόν μικρότερη παρεμβολή μεταξύ των υποφερουσών.

2.1.2. Adaptive Modulation (AM)

Τα συστήματα WiMAX συνδυάζουν τεχνολογίες και αλγόριθμους ώστε να επιτυγχάνουν απόδοση BER των 10 -9 (BER of 10 -9) με διαθεσιμότητα ζεύξης 99,999%. Η αύξηση της φασματικής απόδοσης είναι ένας σημαντικός παράγοντας που επηρεάζει απ' ευθείας το αποτέλεσμα. Για το λόγο αυτό, τα συστήματα WiMAX προσφέρουν διπλής κατευθύνσεως προσαρμοστική διαμόρφωση (Adaptive Modulation - AM) που τα προσαρμόζει ανάμεσα σε έξι τύπους διαμόρφωσης (από QPSK σε 64 QAM) με σκοπό να προσαρμόζει τη ποιότητα διαβάθμισης της ζεύξης ενώ προσφέρουν το μέγιστο ρυθμό μετάδοσης.

Οι ταχύτητες μετάδοσης του προτύπου εξαρτώνται από την εκάστοτε ψηφιακή διαμόρφωση που χρησιμοποιείται. Συνήθεις διαμορφώσεις είναι η 64 QAM, η 16 QAM, η QPSK και η BPSK. Οι διαμορφώσεις QPSK και BPSK είναι για μακρινούς SS, η διαμόρφωση 16 QAM για SS που βρίσκονται σε μεσαία απόσταση και η διαμόρφωση QAM 64 για κοντινούς SS. Όσο πιο μακριά βρίσκεται ο SS από τον BS, τόσο πιο χαμηλός θα είναι ο ρυθμός μετάδοσης. Συνεπώς οι διαμορφώσεις BPSK και QPSK οι οποίες εξασφαλίζουν μεγάλη κάλυψη του συστήματος (χρησιμοποιούνται για SS μακριά από τον BS) έχουν τον χαμηλότερο ρυθμό μετάδοσης δεδομένων, ενώ η διαμόρφωση 64 QAM έχει τον υψηλότερο ρυθμό μετάδοσης.

2.1.3. Διανομή χωρητικότητας Ανερχόμενη-Κατερχόμενη μετάδοση

Το φυσικό επίπεδο του WiMAX υποστηρίζει διαφορετική δομή για τα Point-to-Multipoint κανάλια κατερχόμενης κίνησης και τα Multipoint-to-Point κανάλια ανερχόμενης κίνησης. Αυτές οι δομές αντικατοπτρίζουν τις διαφορετικές απαιτήσεις στις δύο κατευθύνσεις. Γενικά, τα περισσότερα συστήματα απαιτούν μεγαλύτερη χωρητικότητα σε ατομικούς συνδρομητές για να υποστηρίξουν ασύμμετρες συνδέσεις δεδομένων, όπως οι εφαρμογές Ιστού στο διαδίκτυο. Για την ανερχόμενη

κατεύθυνση, καθώς υπάρχουν πολλοί συνδρομητές που ανταγωνίζονται για την διαθέσιμη χωρητικότητα, πρέπει να διευθετηθεί το ζήτημα της πρόσβασης.

- **Ανερχόμενη μετάδοση (uplink)**

Η ανερχόμενη μετάδοση χρησιμοποιεί μια τεχνική DAMA-TDMA (Demand Assignment Multiple Access – Time Division Multiple Access). Η τεχνική DAMA είναι μία τεχνική ανάθεσης χωρητικότητας που προσαρμόζεται όσο χρειάζεται για να ανταποκριθεί βέλτιστα σε αλλαγές απαιτήσεων στους διάφορους σταθμούς. Η τεχνική TDMA είναι απλά μία τεχνική που διαιρεί τον χρόνο σε ένα κανάλι σε μία ακολουθία πλαισίων, κάθε ένα από τα οποία αποτελείται από slots και που διανέμει τα slots σε κάθε πλαίσιο για να σχηματίσει ένα λογικό κανάλι.

Η ανερχόμενη μετάδοση χρησιμοποιεί τον Reed-Solomon κώδικα για διόρθωση σφαλμάτων και ένα σχήμα διαμόρφωσης βασισμένο στο QPSK.

- **Κατερχόμενη μετάδοση (downlink)**

Στην κατερχόμενη μετάδοση, το πρότυπο καθορίζει δύο τρόπους λειτουργίας, που ο ένας υποστηρίζει συνεχόμενη μετάδοση, όπως audio και video, και ο άλλος μετάδοση σε ομάδες, όπως η IP-based κίνηση.

Για την συνεχή κατερχόμενη μετάδοση, χρησιμοποιούμε ένα απλό TDM (Time Division Multiplexing) σχήμα για πρόσβαση στο κανάλι. Η αμφίδρομη τεχνική που χρησιμοποιείται για διανομή χωρητικότητας ανάμεσα στην ανερχόμενη και στην κατερχόμενη κίνηση είναι γνωστή σαν Αμφίδρομη Επικοινωνία με Διαίρεση Συχνότητας ή FDD (Frequency Division Duplexing). Σύμφωνα με αυτήν, χρησιμοποιείται διαφορετική μπάντα συχνοτήτων για μετάδοση σε κάθε κατεύθυνση. Αυτό είναι ισοδύναμο με το FAMA-FDMA (Fixed Assignment Multiple Access – Frequency Division Multiple Access) σχήμα. Το FDD συνεπάγεται ότι κάθε συνδρομητής μπορεί να μεταδίδει και να λαμβάνει στον ίδιο χρόνο, χρησιμοποιώντας διαφορετικές, προδιαγεγραμμένες συχνότητες.

Για την κατερχόμενη μετάδοση σε ομάδες χρησιμοποιείται το DAMA-TDMA σχήμα για πρόσβαση στο κανάλι.

2.1.4. Χαρακτηριστικά του φυσικού επιπέδου

Τα χαρακτηριστικά του φυσικού επιπέδου και τα πλεονεκτήματα που προσφέρουν είναι:

- Χρήση OFDM με 256 φέρουσες.Έτσι μπορούμε να έχουμε επικοινωνίες LOS και NLOS.
- Χρήση προσαρμοστικής διαμόρφωσης και κωδικών διόρθωσης σφαλμάτων. Επομένως έχουμε αποτελεσματικές ζεύξεις με μέγιστο αριθμό bits/sec σε κάθε χρήστη.
- Υποστήριξη TDD και FDD.Με αποτέλεσμα να ικανοποιούνται οι συνθήκες διαχείρισης φάσματος κάθε χώρας.
- Μεταβλητό εύρος ζώνης καναλιού (3.5 MHz, 5MHz, 10MHz).Με δυνατότητα λειτουργίας σε πολλές ζώνες συχνοτήτων ανάλογα με τον κανονισμό της κάθε χώρας.
- Υποστήριξη έξυπνων κεραιών. Με αποτέλεσμα να εξασφαλίζεται το υψηλό κέρδος ισχύος

2.2. MAC Επίπεδο

Το MAC επίπεδο του WiMAX εκτελεί την τυποποιημένη λειτουργία ελέγχου παροχής μιας διεπαφής ανεξάρτητης του μέσου στο φυσικό επίπεδο του WiMAX. Επειδή το φυσικό επίπεδο είναι ένα ασύρματο επίπεδο, η κύρια εστίαση του MAC επιπέδου είναι να ρυθμιστούν οι πόροι της σύνδεσης κατά τρόπο αποδοτικό. Το MAC επίπεδο σχεδιάζεται για να υποστηρίξει PTM. Το MAC επίπεδο είναι συνδεσμο-προσανατολισμένο. Στην είσοδο του δικτύου, κάθε σταθμός συνδρομητών δημιουργεί μια ή περισσότερες συνδέσεις πέρα από στις οποίες τα δεδομένα διαβιβάζονται προς και από το σταθμό βάσης. Το επίπεδο MAC σχεδιάζει τη χρήση των πόρων σύνδεσης και παρέχει διάκριση στην ποιότητα υπηρεσιών. Εκτελεί λειτουργίες προσαρμογής συνδέσεων και αυτόματου αιτήματος επανάληψης (Automatic Repeat Request - ARQ) για να διατηρήσει τα Bit Error Rates (BER) μεγιστοποιώντας την έξοδο δεδομένων. Το MAC επίπεδο χειρίζεται επίσης την είσοδο δικτύων στους σταθμούς συνδρομητών που μπαίνουν και βγαίνουν από το δίκτυο, και αυτό εκτελεί έργα δημιουργίας PDU.

Όταν εγκαθιδρύεται μία σύνδεση, ο χρήστης και το υποδίκτυο, δηλαδή ο πελάτης και ο φορέας, συμφωνούν σε ένα συγκεκριμένο μοτίβο κίνησης για το κύκλωμα αυτό. Μερικές φορές αυτό ονομάζεται Συμφωνία Επιπέδου Υπηρεσιών. Όσο ο πελάτης υπακούει στην συμφωνία, στέλνοντας πακέτα μόνο με βάση το συμφωνημένο συμβόλαιο, ο φορέας υπόσχεται να τα παραδίδει όλα εγκαίρως. Η

μορφοποίηση κίνησης μειώνει την συμφόρηση και βοηθά έτσι τον φορέα να υλοποιήσει την υπόσχεσή του. Οι συμφωνίες αυτές δεν είναι τόσο σημαντικές για τις μεταφορές αρχείων, έχουν όμως μεγάλη σημασία για τα δεδομένα πραγματικού χρόνου, όπως τις συνδέσεις ήχου και βίντεο, όπου υπάρχουν αυστηρές απαιτήσεις ποιότητας υπηρεσιών.

Στο υποεπίπεδο της ασφάλειας, χρησιμοποιείται κρυπτογραφία για να διατηρηθούν μυστικά όλα τα δεδομένα που μεταδίδονται. Κρυπτογραφούνται μόνο τα ωφέλιμα φορτία των πλαισίων και όχι οι κεφαλίδες. Παρακάτω αναλύονται τα τρία υποστρώματα του MAC επιπέδου

2.2.1. Υποεπίπεδο σύγκλισης εξαρτώμενο από την υπηρεσία

Το υποεπίπεδο σύγκλισης ή για λόγους συντομίας CS υποεπίπεδο, αρχικά αντιστοιχίζει ή καλύτερα μετασχηματίζει δεδομένα που λαμβάνει από το σημείο πρόσβασης υπηρεσίας SAP (και που έχουν σταλθεί από το επίπεδο δικτύου) σε MAC SDU (σε τύπου MAC πακέτα δεδομένων υπηρεσίας). Στη συνέχεια αυτά τα «τροποποιημένα» δεδομένα λαμβάνονται με τη σειρά τους από το κοινό τμήμα υποεπιπέδου MAC (MAC CPS) μέσω του MAC SAP.Η διαδικασία αυτή της αντιστοίχησης δεδομένων περιλαμβάνει κατ' αρχήν ταξινόμηση των πακέτων δεδομένων υπηρεσίας που λαμβάνει από το επίπεδο δικτύου με βάση κάποιες παραμέτρους και αντιστοίχηση αυτών των δεδομένων με τη σωστή υπηρεσία του MAC CPS καθώς και με μία ταυτότητα σύνδεσης (CID) ώστε να οριστεί μονοσήμαντα η σύνδεση. Μερικές φορές είναι πιθανόν να εφαρμοστούν ακόμα PHS συναρτήσεις στα δεδομένα, οι οποίες έχουν ως στόχο να απομακρύνουν κάποια δεδομένα που εμφανίζονται δύο φόρες και έτσι η μεταφορά από ένα επίπεδο στο άλλο να γίνει με μεγαλύτερη ευκολία.

Από τα παραπάνω που αναφέραμε φαίνεται ότι το CS υποεπίπεδο αποτελεί ένας είδος διεπαφής με πολλά διαφορετικά πρωτόκολλα. Αναλυτικότερα οι λειτουργίες που εκτελεί φαίνονται παρακάτω:

- Δέχεται από το αμέσως υψηλότερο επίπεδο πακέτα δεδομένων πρωτοκόλλου (PDU).
- Ταξινομεί αυτά τα PDU.
- Επεξεργάζεται τα PDU αν αυτό είναι απαραίτητο ανάλογα με το τρόπο που έχουν ταξινομηθεί.

- Μοιράζει τα CS PDU's στα κατάλληλα σημεία πρόσβασης υπηρεσίας (SAP).

Η μονάδα πληροφορίας SDU μαζί με την επικεφαλίδα (που τοποθετείται κάθε φορά από το αντίστοιχο επίπεδο) συνιστούν τη μονάδα πληροφορίας PDU.

2.2.2. Υποεπίπεδο Κοινό τμήμα

Ένα δίκτυο του οποίου η λειτουργία βασίζεται σε ένα μέσο επικοινωνίας, πρέπει να διαθέτει μηχανισμούς να διαχειρίζεται αυτό το μέσο και να το μοιράζει στους κόμβους του. Στη περίπτωση του πρωτοκόλλου WiMAX το υποεπίπεδο MAC CPS αναλαμβάνειμε το έργο της διαχείρισης του καναλιού.

Το κατέβασμα δεδομένων από το BS στο χρήστη γίνεται με μία PTM λογική. Έτσι το WiMAX λειτουργεί με ένα κεντρικό BS και μία κεραία πολλαπλών τομέων, η οποία έχει τη δυνατότητα να διαχειρίζεται αυτούς τους πολλαπλούς τομείς παράλληλα. Για μία συγκεκριμένη συχνότητα καναλιού και ένα συγκεκριμένο τομέα, όλοι οι χρήστες λαμβάνουν τα ίδια δεδομένα. Για αυτό ακριβώς το λόγο ένας BS εκπέμπει σε ένα συγκεκριμένο τομέα (με συγκεκριμένη συχνότητα καναλιού) και στα μηνύματα απάντησης συγκρατεί τις διευθύνσεις των χρηστών του τομέα για μελλοντική επικοινωνία.

Στην αντίθετη κατεύθυνση οι SS, μοιράζονται το κανάλι επικοινωνίας με το BS, με βάση τις απαιτήσεις που υπάρχουν. Βασικός παράγοντας βέβαια είναι και οι υπηρεσίες που ζητούν.

Σε κάθε τομέα οι χρήστες «υπακούν» ένα πρωτόκολλο μετάβασης, έτσι ώστε ανάλογα με τα χαρακτηριστικά του καναλιού να μπορεί να επιτευχθεί οι εξυπηρέτηση όλων των χρηστών. Υπάρχουν πέντε διαφορετικού τύπου μηχανισμοί χρονοπρογραμματισμού ανεβάσματος δεδομένων στον BS. Οι μηχανισμοί είναι σαφώς ορισμένοι από το πρωτόκολλο έτσι ώστε να μπορούν οι κατασκευάστριες εταιρίες προϊόντων WiMAX να βελτιώνουν όλο και περισσότερο τα προϊόντα τους διαφορετικούς συνδυασμούς τεχνικών που ορίζουν οι παραπάνω μηχανισμοί.

Το MAC CPS δημιουργεί συνδέσεις για να διαχειριστεί το κανάλι. Αυτό ενισχύει την αξιοπιστία και εξασφαλίζει υψηλή ποιότητα υπηρεσιών. Η σύνδεση γίνεται ως εξής. Κάθε φορά που ένα SS εγκαθίσταται στο δίκτυο, τότε αμέσως δημιουργείται μια σύνδεση με αυτόν για να είναι δυνατή η ροή υπηρεσιών. Οι συνδέσεις απαιτούν ενεργή συντήρηση. Αυτή η συντήρηση βέβαια εξαρτάται και από το τύπο της υπηρεσίας που συνδέεται. Για παράδειγμα κάποιο τύποι υπηρεσιών δεν απαιτούν ενεργή συντήρηση της σύνδεσης αφού έχουν σταθερό εύρος ζώνης για κάθε

πακέτο δεδομένων, σε αντίθεση με άλλες υπηρεσίες που αυτό μεταβάλλεται δυναμικά. Τέλος να πούμε ότι η σύνδεση τερματίζεται είτε από το BS είτε από το SS .

Επίτευξη σύνδεσης

Για να επιτευχθεί η σύνδεση κάθε SS έχει μια 48-bit καθολική διεύθυνση όπως ορίζεται από την IEEE για το πρότυπο 802.16. Αυτή η διεύθυνση ορίζει μονοσήμαντα το SS από ένα σύνολο προϊόντων διαφορετικών εταιριών. Επίσης η εγγραφή αυτής της διεύθυνσης γίνεται κατά τη εγκατάσταση μιας σύνδεσης και χρησιμοποιείται στη διαδικασία επικύρωσης μεταξύ BS και SS.

Η σύνδεση μεταξύ ενός BS και ενός SS ταυτοποιείται με τη βοήθεια ενός CID 16 bit, ο οποίος είναι ο κωδικός κάθε σύνδεσης. Κατά την εγκατάσταση του SS τρεις συνδέσεις μεταξύ του SS και του BS αρχικοποιούνται για κάθε κατεύθυνση (SS → BS, BS→ SS). Η βασική σύνδεση χρησιμοποιείται από το BS MAC και το SS MAC για ανταλλαγή μικρών σε μέγεθος, επειγόντων, MAC μηνυμάτων διαχείρισης. Από τις δύο άλλες συνδέσεις η μία χαρακτηρίζεται ως πρωτεύον και η άλλη ως δευτερεύον. Η πρωτεύον χρησιμοποιείται από το BS MAC και το SS MAC για ανταλλαγή μεγάλων, όχι τόσο επειγόντων από άποψη χρόνου μηνυμάτων. Τέλος η δευτερεύον σύνδεση αναφέρεται σε μηνύματα ακόμα πιο ανθεκτικά στο χρόνο.

2.2.3. Υποεπίπεδο ιδιωτικότητας

Το υποεπίπεδο ασφάλειας παρέχει μυστικότητα στους χρήστες του WiMAX ασύρματου ευρυζωνικού δικτύου. Αυτό το επιτυγχάνει αποκρύπτοντας τις συνδέσεις ανάμεσα στα SS και BS. Πιο συγκεκριμένα ο σταθμός βάσης αποτρέπει την αναρμόδια πρόσβαση σε δεδομένα με το να κρυπτογραφεί τις ροές δεδομένων από διάφορες υπηρεσίες κατά μήκος του δικτύου. Το υποεπίπεδο ασφάλειας χρησιμοποιεί ένα πρωτόκολλο διαχείρισης κλειδιού τύπου πελάτη-εξυπηρετητή όπου ο BS που έχει το ρόλο του εξυπηρετητή, ελέγχει τη διανομή του κρυπτογραφημένου υλικού στον πελάτη που είναι ο SS.

2.2.4. Χαρακτηριστικά του MAC

Τα χαρακτηριστικά του φυσικού επιπέδου και τα πλεονεκτήματα που προσφέρουν είναι:

- Χρήση TDM/TDMA. Έτσι έχουμε αποδοτικότητα εύρους ζώνης.

- Υποστήριξη μέχρι και 100 χρηστών ανά BS. Με αποτέλεσμα να είναι εφικτή η αξιόπιστη κάλυψη αστικών περιοχών.
- Υποστήριξη QoS. Με αποτέλεσμα στις υπηρεσίες όπως TDM Voice, VoIP να υπάρχει μικρή καθυστέρηση.
- Υποστήριξη Automatic Repeat Reguest (ARQ). Επομένως βελτιώνεται η από άκρου εις άκρου απόδοση του συστήματος.
- Χρήση προσαρμοστικής διαμόρφωσης και κωδικών διόρθωσης σφαλμάτων. Επομένως έχουμε αποτελεσματικές ζεύξεις με μέγιστο αριθμό bits/sec σε κάθε χρήστη.
- Χρήση Triple DES για ασφάλεια. Έτσι πραγματοποιείται η προστασία δεδομένων.
- Automatic Power Control (APC). Με αποτέλεσμα τη δυνατότητα δημιουργίας κυψελοειδών αρχιτεκτονικών.

3. Υποπρότυπα 802.16

Το IEEE 802.16 αποτελείται από μία σειρά υποπρότυπα. Τα πρότυπα αυτά αναπτύσσονται σταδιακά ανάλογα με τις ανάγκες που προκύπτουν. Οι κύριες διαφορές ανάμεσα σε αυτά είναι σε ποιες συχνοτικές μπάντες δουλεύουν καθώς και ποια ομάδα εργασίας (TG) αναπτύσσει το συγκεκριμένο πρότυπο. Ακόμα μέχρι σήμερα κάποια υποπρότυπα δεν έχουν ολοκληρωθεί.

Στην αρχική του έκδοση το πρότυπο IEEE 802.16 λειτουργούσε στην ζώνη συχνοτήτων 10-66 GHz. Στις παραπάνω συχνότητες η επικοινωνία μεταξύ δύο σταθμών επιτυγχάνεται μόνο όταν οι σταθμοί αυτοί βρίσκονται σε συνθήκες οπτικής επαφής. Η παραπάνω διαδικασία περιγράφεται στο υποπρότυπο IEEE 802.11c. Η ανάγκη για επικοινωνία μεταξύ σταθμών που δεν βρίσκονται σε οπτική επαφή ήταν το κίνητρο για τη δημιουργία του υποπροτύπου IEEE 802.16a. Τον Ιανουάριο του 2003 το πρότυπο επεκτάθηκε ώστε να λειτουργεί και στις συχνότητες από 2-11 GHz όπου στις συχνότητες αυτές ήταν δυνατή η δημιουργία συνδέσεων χωρίς οπτική επαφή πομπού και δέκτη. Το υποπρότυπο το οποίο περιγράφει τη διαδικασία αυτή ονομάστηκε IEEE 802.16a. Τα πρώτα προϊόντα WiMAX τα οποία σήμερα είναι διαθέσιμα στην αγορά ακολουθούν στην μεγαλύτερη τους πλειοψηφία το υποπρότυπο αυτό.

Καθώς η πολυπλοκότητα των εφαρμογών που διαδίδονται πάνω από ένα ασύρματο δίκτυο ολοένα και αυξάνει, η ποιότητα υπηρεσίας πάνω από τέτοια δίκτυα γίνεται ένας πολύ καθοριστικός παράγοντας για την ποιότητα της επικοινωνίας. Για παράδειγμα, η μετάδοση βίντεο σε πραγματικό χρόνο απαιτεί από το δίκτυο συνθήκες πολύ χαμηλής καθυστέρησης μετάδοσης. Για αυτό το λόγο, προκειμένου να ικανοποιηθεί η ανάγκη για ποιότητα υπηρεσίας ορίστηκε το υποπρότυπο IEEE 802.16d.

Η ένωση των υποπροτύπων IEEE 802.11 a, c, d όρισε το πρότυπο IEEE 802.16-2004 το οποίο περιγράφει τη συνολική λειτουργικότητα των επιμέρους υποπροτύπων που προαναφέρθηκαν για συχνότητες λειτουργίας 2-66 GHz.

Το πρότυπο IEEE 802.26-2004 ορίζει την επικοινωνία χρηστών οι οποίοι βρίσκονται μέσα σε ένα κελί το οποίο καλύπτεται από ένα BS. Όταν κάποιος χρήστης κινηθεί σε περιοχή που βρίσκεται εκτός περιοχής κάλυψης του BS η σύνδεση χάνεται. Το υποπρότυπο IEEE 802.16e εισάγει και περιγράφει την έννοια της κινητικότητας των χρηστών από ένα BS σε άλλο. Στο υποπρότυπο αυτό ορίζεται ότι ένας κινητός χρήστης μπορεί να συνεχίσει να εξυπηρετείται από το δίκτυο ακόμα και αν κινείται με ταχύτητες οι οποίες προσεγγίζουν τα 120 χλμ/ώρα.

3.1. Πρότυπο 802.16e

Το 802.16e έγινε αποδεκτό στης 23 Σεπτεμβρίου του 2003. Το πρότυπο αυτό στόχευε στους κινητούς χρήστες οι οποίοι επιθυμούν να διατηρούν τη σύνδεση τους ακόμα και όταν κινούνται από 70 έως 93 μίλια την ώρα και στο ασύρματο διαδίκτυο.

Η νέα αυτή λειτουργικότητα που θα πρόσδιδε το 802.16e γενικά στο πρότυπο 802.16 λέγονταν κινητή ασύρματη ευρυζωνική πρόσβαση ή MBWA. Σκοπός αυτής της νέας λειτουργικότητας ήταν να μπορεί το 802.16e να υποστηρίξει και κινητούς σταθμούς συνδρομητών. Δηλαδή η βασική διαφορά της MBWA από την BWA είναι η κινητικότητα που αυτή προσφέρει και η ταχύτητα κάτω από την οποία τα συστήματα 802.16e μπορούν να λειτουργούν. Ορίστηκαν λοιπόν κάποια επίπεδα κινητικότητας. Αυτά είναι:

- Σταθερή (0 χλμ/ώρα)
- Πεζού (πάνω από 10 χλμ/ώρα)
- Κανονική ταχύτητα οχήματος (πάνω από 100 χλμ/ώρα)
- Πολύ μεγάλη ταχύτητα (πάνω από 500 χλμ/ώρα)

Από τα παραπάνω επίπεδα ταχύτητας το MBWA αναφέρεται στις δύο τελευταίες κατηγορίες (πάνω από 100, 500 χλμ/ώρα).

Τα MBWA συστήματα χρησιμοποιούν το νόμιμο φάσμα συχνοτήτων κάτω των 3.5 GHz. Εξαιτίας της ταχύτητας που πρέπει να υποστηρίζουν, αυτά τα συστήματα χρειάζεται να είναι στιβαρά στις γρήγορες αλλαγές που θα συμβαίνουν στα κανάλια μετάδοσης κατά τη κίνηση. Η κινητικότητα αυτή σίγουρα θα επηρεάζει και θα δυσκολεύει σε επίπεδο IP αφού θα πρέπει να μεταβάλλεται δυναμικά η δρομολόγηση πακέτων κατά τη κίνηση. Αυτό όπως καταλαβαίνουμε κάνει και την αυθεντικοποίηση πιο δύσκολη για τα uplink/downlink πακέτα δεδομένων.

Για να επιτευχθεί η κινητικότητα από το πρότυπο 802.16e ενισχύθηκε το MAC και το PHY επίπεδο, μειώθηκε η κατανάλωση ενέργειας και υποστηρίχτηκε το Hand-off .

- **MAC και PHY επίπεδο**.

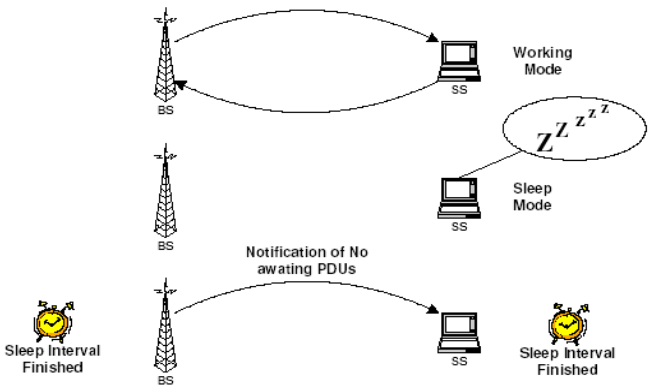
Για να υποστηριχθεί η κινητικότητα το 802.16e πρότεινε βελτιώσεις στο MAC και στο PHY επίπεδο. Οι προτάσεις που έγιναν ήταν στην ανάγκη για διόρθωση της ενέργειας, συχνότητας και χρονισμού κατά τα μεταφορά δεδομένων από το σταθμό βάσης στο χρήστη. Η αρχική πρόταση για το κινητό φυσικό επίπεδο του 802.16e, ήταν η δόμηση ενός στιβαρού PHY που θα μπορεί να ανταπεξέλθει σε δύσκολα κινητά περιβάλλοντα, αλλά θα μπορεί να συνυπάρχει με το OFDM φυσικό επίπεδο του 802.16a. Το προτεινόμενο λοιπόν φυσικό επίπεδο για το 802.16e βασίζεται στα OFDM/OFDMA. Αυτή η πρόταση και προσφέρει συμβατότητα με το 802.16a αλλά και την απαραίτητη στιβαρότητα που απαιτεί η κινητικότητα.

- **Μείωση της κατανάλωσης ενέργειας**.

Η ομάδα του MBWA παρακινήθηκε από την ιδέα να χρησιμοποιείται μπαταρία για το κινητό τερματικό, έτσι ο SS θα μειώσει την ενέργεια που θα καταναλώνει καθώς επίσης δεν καταναλώνεται ενέργεια όταν ο SS μένει ανενεργός. Επίσης η ομάδα του MBWA έκανε εισαγωγή δύο «ταχυτήτων» κατανάλωσης ενέργειας. Η μία ήταν η ταχύτητα αφύπνισης (Awake speed) και η άλλη η ταχύτητα αναμονής (Sleep speed) με σκοπό τη μείωση κατανάλωσης ενέργειας. Η ταχύτητα αφύπνισης είναι όταν ο SS λαμβάνει και στέλνει PDU πακέτα με κανονικό ρυθμό. Αντίθετα στην ταχύτητα αναμονής ούτε στέλνονται ούτε λαμβάνονται PDU και έτσι απαιτείται πολύ λίγη ενέργεια. Να σημειώθεί εδώ ότι η ταχύτητα αναμονής έχει δύο βασικές παραμέτρους που είναι οι εξής:

- **Sleep-interval**: Η παράμετρος αυτή αναφέρεται στο διάστημα που ο SS μπαίνει σε ταχύτητα αναμονής μέχρι να επανέλθει σε ταχύτητα αφύπνισης. Το διάστημα αυτό εξαρτάται από αλγόριθμο ο οποίος όμως είναι ευέλικτος για κάθε SS ανάλογα με τη κίνηση που υπάρχει στο δίκτυο.
- **Listening-interval**: Η παράμετρος αυτή καθορίζει τη χρονική διάρκεια κατά την οποία ο SS πρέπει να αποφασίσει αν θα μείνει στη ταχύτητα αφύπνισης ή θα μεταβεί στην ταχύτητα αναμονής.

Η διαδικασία αλλαγής από ταχύτητα αναμονής σε αφύπνισης (Εικόνα 7) γίνεται ως εξής. Όταν ο SS ζητά από το σταθμό βάσης να μπει σε ταχύτητα αναμονής και μπει τελικά σε αυτή, τότε ο SS θα επιστρέψει σε ταχύτητα αφύπνισης όταν κατά τη διάρκεια του Listening-interval ο SS θα ελέγξει το σταθμό βάσης και διαπιστώσει τα εξής. Αν υπάρχουν PDU's που περιμένουν ο SS θα μεταβεί στη ταχύτητα αφύπνισης. Αν δεν υπάρχουν τότε ο SS θα επιστρέψει στη ταχύτητα αναμονής.

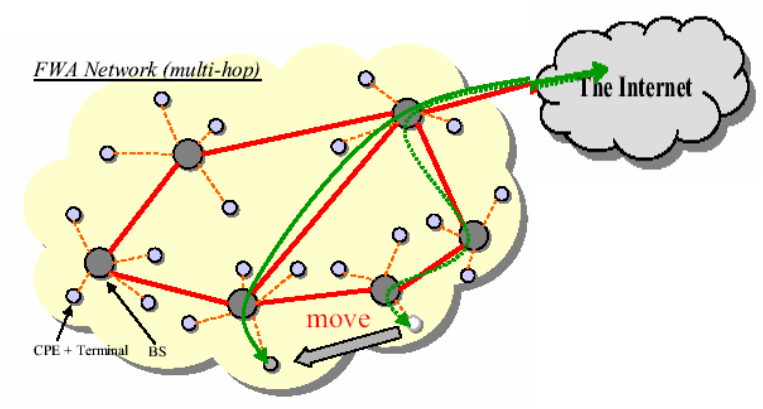


Εικόνα 7. Αλλαγή από κατάσταση αναμονής σε κατάσταση αφύπνισης

- **Hand off**

Η έννοια και ο στόχος του Hand off είναι να επιτρέψει κινητά SS να μετακινούνται με ευκολία και ταχύτητα στους σταθμούς βάσης και να μην χάνονται PDU κατά τη μεταφορά δεδομένων. Αυτό σημαίνει ότι κατά την περιαγωγή κλήσεων (roaming) από ένα BS σε άλλο, η IP στοίβα που βρίσκεται στη κορυφή του MAC CS πρέπει να μένει ανεπηρέαστη από την περιαγωγή κλήσεων.

Στόχος του 802.16e είναι και το ασύρματο διαδίκτυο. Αυτό που θα πρέπει να φροντίσει λοιπόν σε αυτή τη περίπτωση το πρότυπο είναι να διατηρείται η σύνδεση με το διαδίκτυο και να μην αλλάζει η IP διεύθυνση ακόμα και αν το τερματικό αλλάξει τοποθεσία. Αυτό φαίνεται και στην παρακάτω εικόνα.



Εικόνα 8. SS και Διαδίκτυο

Σε ένα multi-hop δίκτυο υπάρχουν βέβαια πολλά διαφορετικά μονοπάτια. Σκοπός του 802.16e είναι να βρει το καλύτερο μονοπάτι μεταξύ του τερματικού και της πύλης. Για να γίνει ανταλλαγή (αποστολή ή λήψη) πακέτων σε μία γνωστή IP όταν υποστηρίζεται η κινητικότητα πρέπει να οριστεί ένα μονοπάτι. Αυτό το μονοπάτι πρέπει να ακολουθεί τη πορεία του τερματικού και αν είναι δυνατόν να είναι το καλύτερο μονοπάτι, δηλαδή αυτό που θα μπορεί να εξασφαλίσει τη μεγαλύτερη ταχύτητα και ασφάλεια.

4. Ασφάλεια στο WiMAX

Έχοντας παρουσιάσει έως τώρα μια αναλυτική περιγραφή της τεχνολογίας του WiMAX, στις ενότητες που ακολουθούν θα γίνει περιγραφή των μηχανισμών ασφάλειας που έχει ενσωματώσει το WiMAX για να αντιμετωπίσει τυπικές απειλές που συναντιούνται σε ασύρματα δίκτυα.

Σήμερα, τυπικές απαιτήσεις ασφάλειας σε ασύρματα δίκτυα περιλαμβάνουν προστασία της ασύρματης σύνδεσης, αμοιβαία αυθεντικοποίηση για πρόσβαση δικτύου, προστασία της ακεραιότητας των μηνυμάτων που στέλνονται.

Η ασφάλεια της ασύρματης σύνδεσης έχει υποβληθεί σε πολυάριθμες βελτιώσεις στην περιοχή του WLAN, το οποίο ορίζει συγκεκριμένα προφίλ ασφάλειας όπως το WPA και το WPA2, καθένα από τα οποία επιτυγχάνει ένα σταθερά εγγυημένο επίπεδο ασφάλειας. Η ασφάλεια στο WiMAX είναι διαφορετική από ότι σε σχέση με το WLAN σε ένα αριθμό θεμάτων, αν και συχνά βασίζονται στις ίδιες αρχές.

4.1. Απειλές ασφάλειας

Κάποιες τυπικές απειλές που έχει να αντιμετωπίσει οποιοδήποτε ασύρματο δίκτυο είναι:

1) Κακόβουλες οντότητες μπορούν να κερδίσουν πρόσβαση στο δίκτυο μέσω των ασύρματων συνδέσεων, οι οποίες δεν είναι αρκετά ασφαλείς. Αυτές οι οντότητες ενδεχομένως μπορούν να παρακάμψουν κάθε προστασία από firewall η οποία ενσωματώνονται στο δίκτυο.
2) Μη κρυπτογραφημένη πληροφορία που περιπλανιέται στον αέρα μπορεί να αναχαιτιστεί από οποιονδήποτε έχει έναν κατάλληλα συντονισμένο δέκτη.
3) DoS επιθέσεις μπορούν να διευθυνθούν πιο εύκολα.
4) Η ταυτότητα ενός νόμιμου χρήστη μπορεί να κλαπεί και οι εγκληματίες μπορούν να μεταμφιεστούν ως νόμιμοι χρήστες.
5) Οι ιοί και άλλοι κακόβουλοι κώδικες μπορούν εύκολα να εισαχθούν στο δίκτυο και επιπλέον να πολλαπλασιαστούν στην ενσύρματη πλευρά του δικτύου.

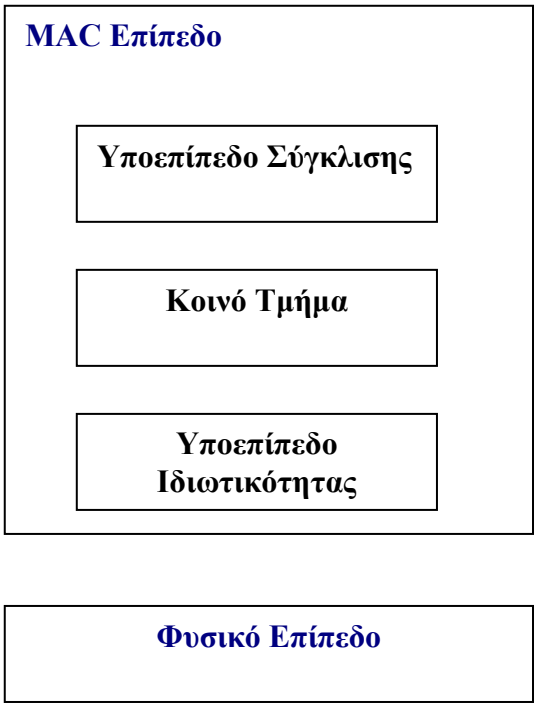
Αυτές είναι μόνο μερικές απειλές, ωστόσο υπάρχουν πολλές άλλες απειλές, οι οποίες μπορεί αν υπάρξουν σε ένα πραγματικό σενάριο. Στη συνέχεια αναλύονται συγκεκριμένες απειλές του WiMAX που εκμεταλλεύονται ευπάθειες του φυσικού και του MAC επιπέδου του προτύπου.

4.1.1. Απειλές φυσικού επιπέδου

Αφού το υποεπίπεδο ιδιωτικότητας είναι επάνω από το φυσικό επίπεδο, το φυσικό επίπεδο μένει ακάλυπτο (όπως απεικονίζεται στην Εικόνα 9). Το WiMAX είναι τρωτό σε επιθέσεις φυσικού επιπέδου όπως jamming (μπλοκάρισμα/ παρεμβολή παρασίτων) και scrambling (παρεμβολές στο σήμα).

Το jamming επιτυγχάνεται με την εισαγωγή μιας πηγής θορύβου αρκετά ισχυρής ώστε να μειώσει σημαντικά την ικανότητα μετάδοσης του καναλιού. Το jamming είναι είτε ακούσιο, είτε κακόβουλο. Οι πληροφορίες και ο εξοπλισμός που απαιτούνται για να εκτελεστεί το jamming δεν είναι δύσκολο να αποκτηθούν. Ο Poisel έχει δημοσιεύσει ένα βιβλίο στο θέμα του jamming αποκλειστικά, δηλαδή πώς να δημιουργηθούν jamming συστήματα και να αντιμετωπιστούν συστήματα που είναι από την κατασκευή τους ανθεκτικά στο jamming [11]. Μια επίθεση jamming είναι πιθανό να εμφανιστεί σε ένα δίκτυο WiMAX. Η ανθεκτικότητα σε μια επίθεση jamming μπορεί να βελτιωθεί αυξάνοντας τη δύναμη των σημάτων ή αυξάνοντας το

εύρος ζώνης των σημάτων, χρησιμοποιώντας διαδεδομένες τεχνικές, όπως αναπήδηση συχνότητας. Επίσης ένας αριθμός από επιλογές είναι διαθέσιμος για να αυξήσει τη δύναμη ενός σήματος, όπως, μια ισχυρότερη συσκευή αποστολής σημάτων, μια υψηλής ενίσχυσης κεραία μετάδοσης και μια υψηλής ενίσχυσης κεραία λήψης. Το jamming είναι εύκολο να ανιχνευτεί με εξοπλισμό ελέγχου ραδιοφάσματος. Οι πηγές είναι σχετικά εύκολο να εντοπιστούν χρησιμοποιώντας εργαλεία ραδιογωνιομετρίας (radio direction finding tools). Η επιβολή νόμου μπορεί να εμπλακεί για να σταματήσει τους jammers. Επειδή το jamming είναι αρκετά εύκολο να ανιχνευτεί και να αντιμετωπιστεί, θεωρείται ότι μπορεί να έχει ένα χαμηλό αντίκτυπο και στο χρήστη και στο σύστημα. Ο κίνδυνος που συνδέεται με το jamming είναι επομένως σημαντικός, κατ' ανώτατο όριο.



Εικόνα 9. Φυσικό και MAC επίπεδο του WiMAX

Το scrambling είναι ένα είδος jamming, αλλά για σύντομα χρονικά διαστήματα και στοχεύει σε συγκεκριμένα πλαίσια ή μέρη των πλαισίων. Οι συσκευές παρεμβολών μπορούν επιλεκτικά να κάνουν παρεμβολές σε πληροφορίες ελέγχου ή διαχείρισης με στόχο να επηρεάσουν την κανονική λειτουργία του δικτύου. Το πρόβλημα αποκτά μεγαλύτερο εύρος για ευαίσθητα χρονικά μηνύματα, που δεν είναι ανεκτικά σε καθυστερήσεις, όπως αιτήσεις ή απαντήσεις αναφορών μέτρησης

καναλιών. Αυλακώσεις κυκλοφορίας δεδομένων που ανήκουν στους στοχευμένους χρήστες μπορεί να υποστούν παρεμβολές επιλεκτικά, αναγκάζοντας τους να αναμεταδώσουν. Με τελικό αποτέλεσμα να παίρνουν λιγότερο από το χορηγημένο εύρος ζώνης τους. Επιλεκτική παρεμβολή των uplink αυλακώσεων άλλων χρηστών μπορεί θεωρητικά να μειώσει το πραγματικό εύρος ζώνης των θυμάτων και να επιτύχει την επεξεργασία των δεδομένων του επιτιθεμένου. Είναι σχετικά δυσκολότερο να επιτευχθεί το scrambling από ότι το jamming λόγω της ανάγκης από τον επιτιθέμενο, να μεταφράσει τις πληροφορίες ελέγχου και να στείλει θόρυβο κατά τη διάρκεια συγκεκριμένων διαστημάτων. Υπάρχουν τεχνικές δυσκολίες να διευθετηθούν από έναν επιτιθέμενο, αλλά είναι επιλύσιμες. Η πιθανότητα εμφάνισης επιθέσεων scrambling είναι δυνατή. Το scrambling είναι δυσκολότερο να ανιχνευθεί λόγω της διακοπτόμενης φύσης της επίθεσης και το γεγονός ότι μπορεί επίσης να οφείλεται σε φυσικές πηγές θορύβου. Το scrambling και οι συσκευές παρεμβολών μπορούν να ανιχνευθούν με παρακολούθηση ανωμαλιών στα κριτήρια απόδοσης. Αυτό το ζήτημα έχει μελετηθεί για συστήματα Wi-Fi από τους Raya, Hubaux και Domino [12]. Η κατάσταση για το WiMAX είναι πολύ διαφορετική και απαιτείται έρευνα για αυτήν την περίπτωση. Ο αντίκτυπος επιθέσεων scrambling είναι χαμηλός, διότι οδηγεί στην ενόχληση ενός περιορισμένου αριθμού χρηστών. Τα αποτελέσματα είναι αντιστρέψιμα, για παράδειγμα με αναμετάδοση. Θεωρείται ότι το scrambling αντιπροσωπεύει έναν δευτερεύοντα κίνδυνο αυτή τη στιγμή.

Μια ακόμα χαρακτηριστική απειλή προκύπτει από την επίθεση water torture, στην οποία ένας επιτιθέμενος στέλνει μια σειρά πλαισίων για να εξαντλήσει τη μπαταρία του δέκτη.

4.1.2. Απειλές MAC επιπέδου

Οι απειλές ασφάλειας ισχύουν και για το PHY και το MAC επίπεδο του IEEE 802.16. Επειδή η WiMAX ασφάλεια λειτουργεί πλήρως στο επίπεδο MAC, δεν κάνει τίποτα για να προστατευτεί ενάντια σε επιθέσεις PHY επιπέδου. Επειδή διαθέσιμες τεχνικές ενάντια σε PHY επιπέδου επιθέσεις είναι ανεπαρκείς για να αξίζουν προτυποποίηση, το μοντέλο ασφάλειας εστιάζει αποκλειστικά στις απειλές MAC επιπέδου.

Προσθέτοντας κινητικότητα στο πρότυπο μέσω του IEEE 802.16e καθίσταται η ζωή του επιτιθεμένου ακόμα ευκολότερη. Η φυσική θέση του επιτιθεμένου δεν περιορίζεται πολύ, κάνοντας τα μηνύματα διαχείρισης πιο τρωτά από ότι στο IEEE

802.11. Η ανάγκη να διατηρηθεί μια ασφαλή κατάσταση ενώ ένα κινητό SS που κινείται μεταξύ των BS εισάγει νέες ευπάθειες.

Διάφορες απειλές είναι γενικές σε οποιοδήποτε ασύρματο μέσο. Επειδή το WiMAX χρησιμοποιεί ασύρματη εκπομπή, καθένας με έναν κατάλληλα τοποθετημένο ασύρματο δέκτη μπορεί να παρεμποδίσει μηνύματα που στέλνονται σε ένα ασύρματο κανάλι. Ως εκ τούτου το σχέδιο ασφάλειας πρέπει να καθορίσει έναν μηχανισμό εμπιστευτικότητας.

Οι σχεδιαστές του WiMAX απέτυχαν να αντιμετωπίσουν άλλη μια απειλή. Καθένας με σωστά τοποθετημένο και διαμορφωμένο ασύρματο πομπό μπορεί να γράψει σε ένα ασύρματο κανάλι. Λόγω αυτής της ευπάθειας, ένας επιτιθέμενος θα μπορούσε να πλαστογραφήσει νέα πλαίσια και να συλλάβει, τροποποιήσει, και αναμεταδώσει πλαίσια από εξουσιοδοτημένα συμβαλλόμενα μέρη. Το σχέδιο ασφάλειας πρέπει επομένως να παρέχει επίσης ένα μηχανισμό αυθεντικότητας δεδομένων.

Ένας επιτιθέμενος μπορεί επίσης να στείλει εκ νέου έναν έγκυρο, ήδη-σταλμένο πλαίσιο χωρίς τροποποιήσεις. Η παρέμβαση και η απόσταση θα μπορούσαν να επιτρέψουν σε έναν επιτιθέμενο να επικοινωνήσει με δύο εξουσιοδοτημένα συμβαλλόμενα μέρη που δεν μπορούν να επικοινωνήσουν άμεσα ο ένας με τον άλλον και να αναδιατάξει και να προωθήσει επιλεκτικά πλαίσια. Κατά συνέπεια, το σχέδιο ασφάλειας πρέπει να ανιχνεύσει επαναληφθέντα πλαίσια.

4.2. Αρχιτεκτονική Ασφάλειας του WiMAX

Η είσοδος στο δίκτυο ενός SS περιλαμβάνει τα ακόλουθα βήματα:

- Κάθε SS ο οποίος προτίθεται να συμμετέχει στο δίκτυο πρέπει να εξετάσει το περιβάλλον του για ένα κατάλληλο κατερχόμενο σήμα, αυτό το κατερχόμενο σήμα θα είναι χρήσιμο για να εγκαταστήσει τις παραμέτρους του καναλιού.
- Χρησιμοποιώντας αυτό το σήμα ο SS εγκαθιστά ένα κύριο κανάλι διαχείρισης με τον BS. Αυτό το κανάλι θα βοηθήσει στη διαπραγμάτευσης δυνατοτήτων, εξουσιοδότησης και διαχείρισης κλειδιού.
- Μόλις οι προεισαγωγικές διαπραγματεύσεις ολοκληρωθούν, το πρωτόκολλο PKM αποκτά τον έλεγχο και εξουσιοδοτεί τον SS στον BS.
- Ο BS σύμφωνα με ένα μήνυμα αίτησης καταχωρεί τον SS.
- Μόλις ο SS καταχωρηθεί, ο BS αποστέλλει μια απάντηση στην οποία εκχωρεί ένα ID σύνδεσης για μια δευτερεύουσα σύνδεση διαχείρισης.

- Τελικά ο SS και ο BS δημιουργούν συνδέσεις μεταφοράς.

Η ασφάλεια WiMAX εφαρμόζεται ως ένα υποεπίπεδο ιδιωτικότητας στο κατώτατο σημείο της εσωτερικής διαστρωμάτωσης του MAC επιπέδου. Ο στόχος του είναι να παρέχει έλεγχο προσπέλασης και εμπιστευτικότητα της σύνδεσης. Η αρχιτεκτονική ασφάλειας WiMAX χρησιμοποιεί πέντε συστατικά, που περιγράφονται στις ακόλουθες υποενότητες.

4.2.1. Σχέσεις ασφάλειας (Security associations).

Οι σχέσεις ασφάλειας (SA) διατηρούν την κατάσταση ασφάλειας που σχετίζεται με μια σύνδεση. Το WiMAX χρησιμοποιεί δύο τύπους SA αλλά ρητά καθορίζει μόνο την SA δεδομένων, η οποία προστατεύει συνδέσεις μεταφορών μεταξύ ενός ή περισσότερων SS και ενός BS. Η SA δεδομένων αποτελείται από

- Ένα 16 bits προσδιοριστικό SA, ή SAID.
- Έναν αλγόριθμο κρυπτογράφησης για να προστατεύσει τα δεδομένα που ανταλλάσσονται μέσω της σύνδεσης. Το πρότυπο χρησιμοποιεί DES σε Cipher Block Chaining (CBC) κατάσταση, [9] αλλά το σχέδιο είναι επεκτάσιμο και σε άλλους αλγόριθμους.
- Δύο κλειδιά κρυπτογράφησης κίνησης (TEK) για την κρυπτογράφηση δεδομένων: το τρέχων λειτουργικό κλειδί και ένα TEK για την περίπτωση που το τρέχων κλειδί λήξει.
- Δύο προσδιοριστικά κλειδιού 2 bits, ένα για κάθε TEK.
- Μια διάρκεια ζωής TEK. Η προκαθορισμένη τιμή για αυτήν την παράμετρο είναι μισή ημέρα και υποθέτει μια ελάχιστη τιμή 30 λεπτών και μια μέγιστη τιμή επτά ημερών.
- Ένα διάνυσμα αρχικοποίησης 64 bits για κάθε TEK.
- Μια ένδειξη του τύπου της SA δεδομένων. Κύρια SAs καθιερώνονται κατά τη διάρκεια της έναρξης συνδέσεων. Στατικά SA διαμορφώνονται στα BS και δυναμικά SA κατασκευάζονται όταν απαιτείται για δυναμικές συνδέσεις μεταφορών.

Για να εξασφαλιστεί μια σύνδεση μεταφορών, ένας SS πρώτα αρχικοποιεί ένα SA δεδομένων χρησιμοποιώντας ένα αίτημα create_connection. Για να υποστηριχθεί πολλαπλή εκπομπή (multicast), το πρότυπο αφήνει πολλά IDs σύνδεσης να

μοιράζονται μια SA. Κατά την εισαγωγή δικτύου, το WiMAX αυτόματα δημιουργεί μια SA για το δευτερεύον κανάλι διαχείρισης. Ένας σταθερός SS επομένως έχει τυπικά δύο ή τρεις SA, ένα για το δευτερεύον κανάλι διαχείρισης και είτε ένα και για την ανερχόμενη και για την κατερχόμενη σύνδεση μεταφορών, είτε ξεχωριστές SA για ανερχόμενες και κατερχόμενες συνδέσεις. Κάθε μια ομάδα πολλαπλής εκπομπής απαιτεί επίσης μια SA να μοιραστεί μεταξύ των μελών της ομάδας.

Η SA εξουσιοδότησης, την οποία το πρότυπο δεν καθορίζει ποτέ ρητά, αποτελείται από:

- Ένα πιστοποιητικό X.509 που προσδιορίζει τον SS.
- Ένα κλειδί εξουσιοδότησης (AK) 160 bits. Σωστή χρήση αυτού του κλειδιού καταδεικνύει η εξουσιοδότηση να χρησιμοποιεί WiMAX συνδέσεις μεταφορών.
- Μια ποσότητα 4 bits για να προσδιορίσει το AK.
- Μια διάρκεια ζωής AK, που κυμαίνεται από μια έως 70 ημέρες. Η προεπιλεγμένη τιμή της διάρκεια ζωής είναι επτά ημέρες.
- Ένα κλειδί κρυπτογράφησης κλειδιού - KEK (112 bits Triple-DES κλειδί) για διανομή των TEK. Το KEK κατασκευάζεται ως εξής:

  $KEK = Truncate\text{-}128(SHA1(((AK \mid 0^{44}) \oplus 53^{64}))$,

  όπου Truncate-128( ) σημαίνει να απορρίψει όλα εκτός από τα πρώτα 128 bits του ορίσματος, το a|b δηλώνει την αλληλουχία των συμβολοσειρών α και β, το ⊕ δηλώνει αποκλειστική διάζευξη (XOR), το a^n δηλώνει την οκτάδα a επαναλαμβανόμενη n φορές, και το SHA1 ορίζεται από το πρότυπο Secure Hash Algorithm [17].
- Ένα κατερχόμενο HMAC κλειδί που παρέχει αυθεντικότητα δεδομένων στα μηνύματα διανομής κλειδιού από το BS στο SS. Αυτό το κλειδί κατασκευάζεται ως εξής: Downlink HMAC key = $SHA1((AK \mid 0^{44}) \oplus 3A^{64})$
- Ένα ανερχόμενο HMAC κλειδί που παρέχει αυθεντικότητα δεδομένων των μηνυμάτων διανομής κλειδιού από τον SS στους BS. Το ανερχόμενο HMAC κλειδί κατασκευάζεται ως: Uplink HMAC key = $SHA1((AK \mid 0^{44}) \oplus 5C^{64})$.
- Έναν κατάλογο εξουσιοδοτημένων SA δεδομένων.

Μια SA εξουσιοδότησης είναι κοινή κατάσταση μεταξύ ενός συγκεκριμένου BS και ενός συγκεκριμένου SS. Το σχέδιο υποθέτει ότι αυτοί οι δύο σταθμοί διατηρούν

το AK μυστικό. Οι BS χρησιμοποιούν τα SA εξουσιοδότησης για να διαμορφώσουν τα SA δεδομένων στον SS.

4.2.2. X.509 Πιστοποιητικά

Αυτά τα πιστοποιητικά χρησιμοποιούνται για την αναγνώριση των επικοινωνούντων μερών. Το προφίλ του πιστοποιητικού όπως ορίζεται στο πρότυπο αποτελείται από τις ακόλουθες πληροφορίες:

- Έκδοση του πιστοποιητικού
- Σειριακός αριθμός του πιστοποιητικού
- Όνομα εκδότη του πιστοποιητικού
- Περίοδος ισχύος του πιστοποιητικού
- Ταυτότητα κατόχου του πιστοποιητικού (MAC διεύθυνση του SS)
- Δημόσιο κλειδί κατόχου του πιστοποιητικού
- Αλγόριθμος υπογραφής του εκδότη και του κατόχου
- Προσδιοριστικό αλγορίθμου υπογραφής
- Υπογραφή της αρχής πιστοποίησης

Το πρότυπο ορίζει ένα πιστοποιητικό κατασκευαστή και ένα SS πιστοποιητικό. Δεν καθορίζει πιστοποιητικά BS. Ο BS χρησιμοποιεί τα πιστοποιητικά δημοσίου κλειδιού του κατασκευαστή για να επικυρώσει την αυθεντικότητα του SS πιστοποιητικού και ως εκ τούτου να προσδιορίσει τη συσκευή όπως γνήσια.. Το μοντέλο υποθέτει ότι ο SS αποθηκεύει το ιδιωτικό κλειδί σε μια «σφραγισμένη» μονάδα αποθήκευσης.

Ένα πιστοποιητικό κατασκευαστή προσδιορίζει τον κατασκευαστή μιας WiMAX συσκευής. Μπορεί να είναι ένα αυτό-υπογεγραμμένο πιστοποιητικό ή εκδιδόμενο από μια τρίτη οντότητα. Ένα πιστοποιητικό SS προσδιορίζει ένα συγκεκριμένο SS και περιλαμβάνει τη MAC διεύθυνση του στο πεδίο κατόχου.

4.2.3. Εξουσιοδότηση PKM

Ο BS έχει πρώτα να εξουσιοδοτήσει έναν SS ο οποίος σκοπεύει να συνδεθεί στο δίκτυο. Η διαδικασία της εξουσιοδότησης αποτελείται από μια ανταλλαγή τριών μηνυμάτων ανάμεσα στον BS και στον SS.

Ο SS χρησιμοποιεί το πρώτο μήνυμα για να ωθήσει στον BS το Cert(Manufacturer(SS)), που είναι το X.509 πιστοποιητικό που προσδιορίζει τον

κατασκευαστή του SS. Το πιστοποιητικό αυτό το χρησιμοποιεί ο BS για να αποφασίσει εάν ο SS είναι μια έμπιστη συσκευή. Το σχέδιο υποθέτει ότι όλες οι συσκευές από έναν αναγνωρισμένο κατασκευαστή μπορούν να είναι έμπιστες. Το WiMAX επιτρέπει στον BS να αγνοήσει αυτό το μήνυμα καθώς η πολιτική ασφάλειάς του μπορεί να επιτρέπει την πρόσβαση μόνο σε συσκευές γνωστές εκ των προτέρων.

Ο SS στέλνει το δεύτερο μήνυμα αμέσως μετά από το πρώτο μήνυμα. Το δεύτερο μήνυμα αποτελείται από το Cert(SS), το οποίο είναι ένα X.509 πιστοποιητικό με το δημόσιο κλειδί του SS, τις δυνατότητες ασφάλειας και την ταυτότητα SAID. Το Cert(SS) αφήνει τον BS να καθορίσει εάν ο SS εξουσιοδοτείται και το δημόσιο κλειδί του Cert(SS) αφήνει το BS να κατασκευάσει το τρίτο μήνυμα.

Εάν ο BS μπορεί να επαληθεύσει το Cert (SS) και ο SS είναι εξουσιοδοτημένος, αποκρίνεται με το τρίτο μήνυμα, το οποίο δημιουργεί μια SA εξουσιοδότησης μεταξύ των δύο σταθμών. Σωστή χρήση αυτού του AK καταδεικνύει την εξουσιοδότηση για προσπέλαση στο κανάλι WiMAX. Το σχέδιο υποθέτει ότι μόνο ο BS και ο SS κατέχουν το AK. Αυτό σημαίνει, ότι το κλειδί δεν αποκαλύπτεται ποτέ σε οποιοδήποτε άλλο συμβαλλόμενο μέρος.

Μήνυμα 1:

SS → BS Cert(Manufacturer(SS))

Μήνυμα 2:

SS → BS Cert(SS) | Capabilities | SAID

Μήνυμα 3:

BS → SS RSA-Encrypt(PubKey(SS), AK) | Lifetime | SeqNo | SAIDList

4.2.4. Ιδιωτικότητα και Διαχείριση Κλειδιού

Το πρωτόκολλο PKM καθιερώνει μια SA δεδομένων μεταξύ BS και SS. Το πρωτόκολλο PKM αποτελείται από ανταλλαγή δύο ή τριών μηνυμάτων μεταξύ του SS και του BS. Ο BS χρησιμοποιεί το πρώτο μήνυμα, το οποίο είναι προαιρετικό, για να αναγκάσει νέα δημιουργία του κλειδιού. Διαφορετικά, ο SS αρχίζει το πρωτόκολλο με αποστολή του δεύτερου μηνύματος και ο BS αποκρίνεται με το τρίτο μήνυμα (Επεξηγήσεις των όρων που χρησιμοποιούνται δίνονται στον Πίνακα 2):

Μήνυμα 1 (Προαιρετικό):

BS → SS: SeqNo | SAID | HMAC(1)

Μήνυμα 2:

SS → BS: SeqNo | SAID | HMAC(2)

Μήνυμα 3:

BS → SS: SeqNo | SAID | OldTEK | NewTEK | HMAC(3)

SecNo	Το AK που χρησιμοποιείται για την ανταλλαγή
OldTEK	Το διάνυσμα αρχικοποίησης, ο εναπομείνας χρόνος ζωής (σε δευτερόλεπτα) και το σειριακός αριθμός για την SA δεδομένων που καθορίζεται από το SAID πριν την δημιουργία του TEK
NewTEK	Το διάνυσμα αρχικοποίησης, ο χρόνος ζωής (σε δευτερόλεπτα) και το σειριακός αριθμός για την SA δεδομένων που καθορίζεται από το SAID για το επόμενο TEK

Πίνακας 2. Επεξηγήσεις όρων

Ο BS δεν χρησιμοποιεί ποτέ το πρώτο μήνυμα εκτός αν θέλει να αναδημιουργήσει το κλειδί μιας SA δεδομένων ή να δημιουργήσει μια νέο SA. Ο υπολογισμός της τιμής HMAC(1), επιτρέπει στον SS να ανιχνεύσει πλαστογραφήσεις.

Ο SS χρησιμοποιεί το δεύτερο μήνυμα για να ζητήσει παραμέτρους της SA. Ο SS πρέπει να πάρει το SAID από τη SAIDList του πρωτόκολλου εξουσιοδότησης ή από ένα μήνυμα 1 με έγκυρο HMAC(1). Ο SS παράγει ένα ξεχωριστό μήνυμα 2 για κάθε SA δεδομένων. Υπολογίζει την τιμή HMAC(2) για να επιτρέψει στον BS να ανιχνεύσει πλαστογραφήσεις.

Εάν το HMAC(2) είναι έγκυρο και το SAID προσδιορίζει μια από τις SA του SS, ο BS διαμορφώνει την SA χρησιμοποιώντας το μήνυμα 3. Η τιμή OldTEK επαναλαμβάνει τις ενεργές παραμέτρους SA, ενώ η τιμή NewTEK ορίζει τιμές παραμέτρων για να χρησιμοποιηθούν στη λήξη του τρέχοντος TEK. Ο BS κρυπτογραφεί με Triple DES τα παλαιά και νέα TEK στο πλαίσιο του KEK της SA εξουσιοδότησης, χρησιμοποιώντας Electronic Code Book (ECB) κατάσταση. Το πρότυπο δεν επιβάλλει καμία απαίτηση παραγωγής TEK. Υπολογισμός της τιμής HMAC(3) επιτρέπει στον SS να ανιχνεύσει πλαστογραφήσεις.

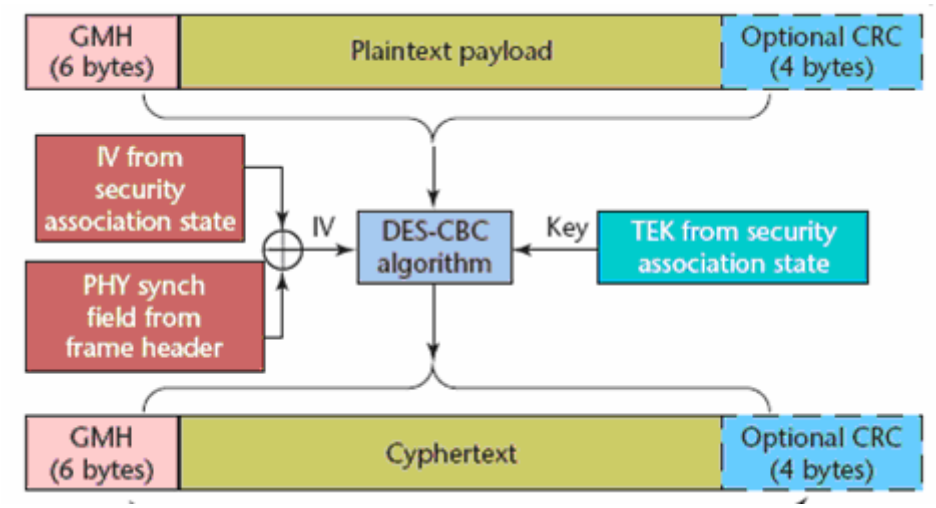
Μια έγκυρη τιμή HMAC(2) αυθεντικοποιεί το SS στο BS. Δύο υποθέσεις υποστηρίζουν αυτήν την αξίωση:

- μόνο ο SS μπορεί να αποκαλύψει το AK που στέλνεται στο μήνυμα 3 του πρωτόκολλου εξουσιοδότησης, και
- το AK είναι απρόβλεπτο.

Το πρωτόκολλο δεν αναγνωρίζει καμία συγκρίσιμη αυθεντικοποίηση του BS στον SS. Στην πραγματικότητα, σωστές τιμές HMAC(1) και HMAC(3) καταδεικνύουν μόνο ότι ένα συμβαλλόμενο μέρος που ξέρει την τιμή AK που λήφθηκε από το SS στο μήνυμα 3 κατασκεύασε μηνύματα διαχείρισης κλειδιού 1 και 3.

4.2.5. Κρυπτογράφηση

Η κρυπτογράφηση DES-CBC (Εικόνα 10), που λειτουργεί πάνω στο πεδίο ωφέλιμου φορτίου, κρυπτογραφεί ένα plaintext MPDU, αλλά όχι το MPDU GMH ή το CRC, όπως απεικονίζει το ακόλουθο σχήμα.

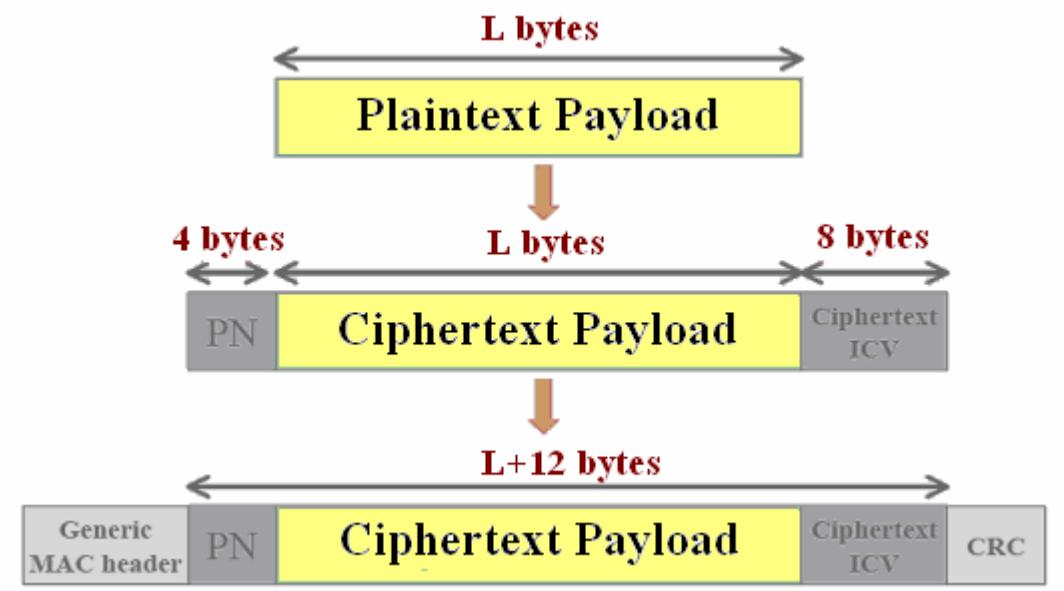


Εικόνα 10. Διαδικασία κρυπτογράφησης DES-CBC

Το MPDU GMH φέρει δύο bits για να υποδείξει το TEK που χρησιμοποιείται. Δεν φέρει το διάνυσμα αρχικοποίησης κατάστασης CBC. Για να υπολογίσει το MPDU διάνυσμα αρχικοποίησης, η υπομονάδα WiMAX κρυπτογράφησης κάνει XOR την SA με το περιεχόμενο του πεδίου συγχρονισμού PHY του πιο πρόσφατου GMH. Επειδή το SA διάνυσμα αρχικοποίησης είναι σταθερό και δημόσιο για το TEK του και επειδή το πεδίο συγχρονισμού PHY είναι ιδιαίτερα επαναλαμβανόμενο και

προβλέψιμο, το MPDU διάνυσμα αρχικοποίησης είναι επίσης προβλέψιμο. Το IEEE 802.16 δεν παρέχει καμία αυθεντικότητα δεδομένων.

Η τροποποίηση IEEE 802.16e υιοθέτησε πρόσφατα το AES-CCM (Εικόνα 11), δηλαδή AES [10] σε CCM κατάσταση, ως νέο αλγόριθμο κρυπτογράφησης σύνδεσης δεδομένων. Η κατάσταση CCM [18] συνδυάζει κρυπτογράφηση σε κατάσταση μετρητή για εμπιστευτικότητα δεδομένων με την CBC-MAC για αυθεντικότητα δεδομένων. Ως εκ τούτου, σωστή χρήση του AES-CCM αντιμετωπίζει την πιο θεμελιώδη ανεπάρκεια στο αρχικό σχήμα προστασίας δεδομένων, την έλλειψη ενός μηχανισμού αυθεντικότητας δεδομένων.



(Όπου PN = Packet Number, ICV = Integrity Check Value)

Εικόνα 11. Διαδικασία κρυπτογράφησης AES-CCM

Οι σχεδιαστές επέλεξαν το AES-CCM για ποικίλους λόγους, συμπεριλαμβανομένης της χρήσης του στο IEEE 802.11i και την επόμενη διερεύνηση. Το αμερικανικό εθνικό ίδρυμα προτύπων και τεχνολογίας (NIST) έχει δείξει ότι το CCM θα γίνει μια εγκεκριμένη κατάσταση λειτουργίας για το AES. Το CCM προστατεύει σχετικά δεδομένα (δηλαδή, επικυρωμένα αλλά μη κρυπτογραφημένα δεδομένα), τα οποία αφήνουν το σχήμα κρυπτογράφησης να προστατεύει την GMH. Δεν υπάρχουν αξιώσεις πνευματικής ιδιοκτησίας ενάντια στο CCM.

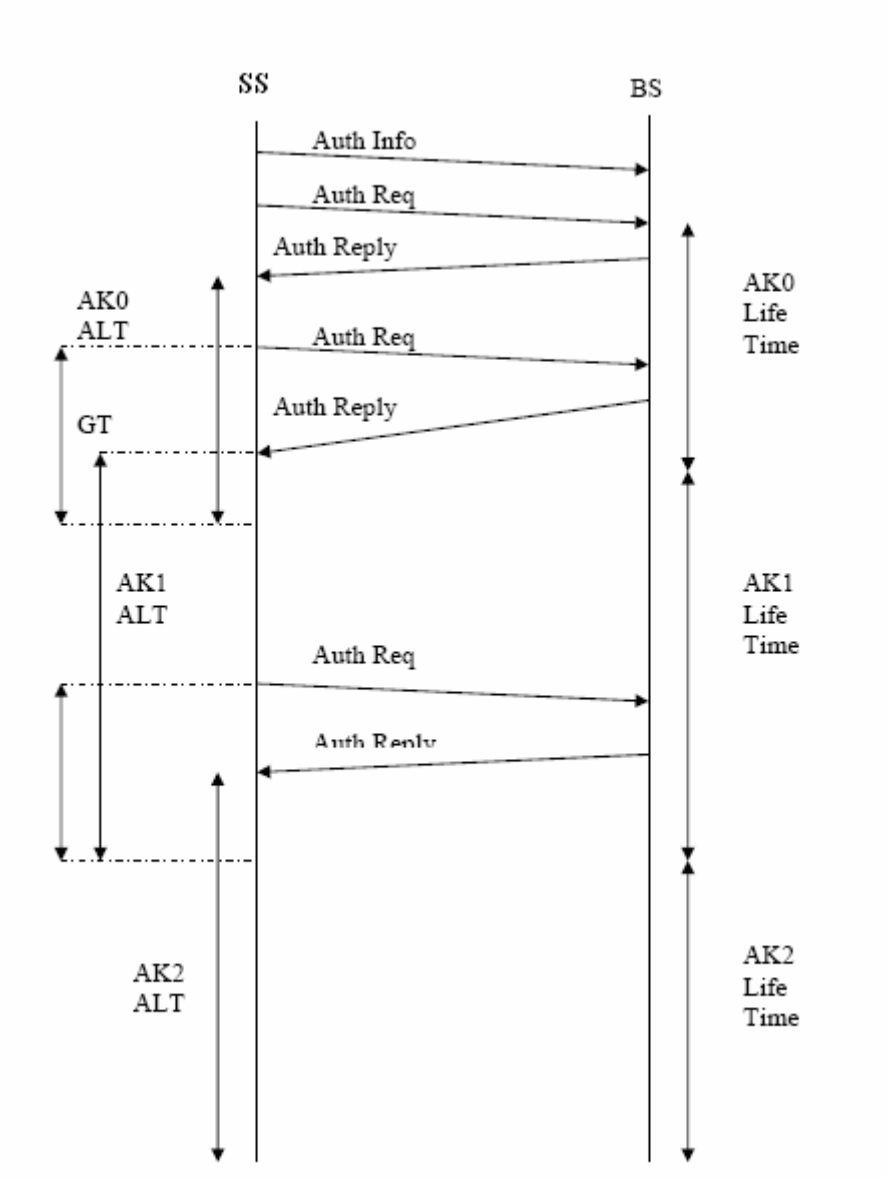
Το AES-CCM απαιτεί ότι ο πομπός κατασκευάζει ένα μοναδικό nonce, το οποίο είναι ένας μηχανισμός τυχαιότητας στην κρυπτογράφηση ανά πακέτο. Σε συνέπεια με

τη λύση του IEEE 802.11i, το IEEE 802.16e παρεμβάλλει έναν αριθμό πακέτου σε κάθε MPDU για να εξασφαλίσει τη μοναδικότητα κάθε nonce. Ένας δέκτης επικυρώνει ότι τα λαμβανόμενα πακέτα αποκρυπτογραφούνται σωστά κάτω από το AES-CCM και έχει έναν μονοτονικά αυξανόμενο αριθμό πακέτου.

5. Χρήση Κλειδιού

AK: Ο BS είναι υπεύθυνος για τη συντήρηση όλων των πληροφοριών των κλειδιών για όλα τα SA. Όταν ο BS λαμβάνει μια αίτηση εξουσιοδότησης εισάγει δύο AK και ενεργοποιεί ένα από τα δύο εισαγόμενα κλειδιά. Αυτό το ενεργοποιημένο κλειδί στέλνεται δια μέσου του SS. Μόλις η διάρκεια ζωής του κοντεύει να λήξει ο SS κάνει μια αίτηση για επανεξουσιοδότηση. Απαντώντας σ' αυτό ο BS ενεργοποιεί το δεύτερο κλειδί και το στέλνει ως απάντηση στο μήνυμα επανεξουσιοδότησης το οποίο έχει παραληφθεί από τον SS. Καθώς ενεργοποιείται το δεύτερο κλειδί εισάγεται ένα τρίτο κλειδί το οποίο κρατείται σε αναμονή για την επόμενη λειτουργία. Γι' αυτό το λόγω ο BS πάντα θα είναι έτοιμος να στείλει ένα AK για να αποφύγει τις επιθέσεις επανάληψης (replay attacks).

TEK: Το διάγραμμα αλληλεπίδρασης της διαχείρισης του TEK είναι παρόμοιο με αυτό του AK. Ο BS παράγει δύο TEK για κάθε SA. Διαδοχικά διατηρεί την παραγωγή καινούργιων κλειδιών καθώς τα παλιά λήγουν. Ο BS χρησιμοποιεί το παλιότερο από τα δύο ενεργά κλειδιά για κρυπτογράφηση το κατερχόμενου καναλιού αν και χρησιμοποιεί το ένα ή το άλλο από τα κλειδιά για να αποκρυπτογραφήσει την ανερχόμενη κίνηση ανάλογα με ποιο κλειδί χρησιμοποιεί ο SS. Ο BS θα αλλάξει το κλειδί του κάθε φορά που το υπάρχον κλειδί λήγει. Η ευθύνη της ενημέρωσης των κλειδιών αφήνετε στον SS. Η μηχανή κατάστασης TEK θα προκαλέσει το γεγονός της αίτησης για ένα καινούργιο κλειδί οποτεδήποτε το υπάρχον κλειδί πρόκειται να λήξει. Ο SS θα χρησιμοποιήσει το πιο πρόσφατο από τα δύο κλειδιά τα οποία έχει διαθέσιμα για να κρυπτογραφήσει την ανερχόμενη κίνηση, αν και μπορεί να χρησιμοποιήσει το ένα ή το άλλο κλειδί για να αποκρυπτογραφήσει την κατερχόμενη κίνηση εξαρτώμενος από το ποιο κλειδί χρησιμοποιείται από τον BS.



Εικόνα 12. Χρήση του AK

6. Ασφάλεια Πρόσβασης Δικτύου

Αυτή η παράγραφος θα δώσει μια σύντομη περίληψη στη διαδικασία της ασφαλής προσάρτησης σε ένα δίκτυο WiMAX, υπερτονίζοντας την ασφάλεια της ασύρματης σύνδεσης και την υποδομή η οποία παρέχεται για την SS αυθεντικοποίηση στο δίκτυο WiMAX.

6.1. Αυθεντικοποίηση χρήστη και συσκευής

Η ασφάλεια του δικτύου WiMAX, ως ένα επαναστατικό βήμα συγκρινόμενο με το WLAN, θα υποστηρίζει αυθεντικοποίηση χρήστη και αυθεντικοποίηση συσκευής

όπως περιγράφεται με περισσότερη λεπτομέρεια σε αυτή την ενότητα. Σύμφωνα με την μέθοδο αυθεντικοποίησης διευθύνομενη από την πολιτική δικτύου, η αυθεντικοποίηση συσκευής και χρήστη μπορούν να εκτελεστούν ανεξάρτητα, ή να συνδυαστούν, κατά τη διάρκεια της αρχικής εισόδου στο δίκτυο.

Εδώ, η αυθεντικοποίηση χρήστη είναι συγκρίσιμη με την βασισμένη σε AAA/EAP αυθεντικοποίηση πρόσβασης δικτύου για Wi-Fi δίκτυα σύμφωνα με το WPA/WPA2, ή στην βασισμένη σε USIM κάρτα αυθεντικοποίηση για πρόσβαση σε 3GPP (UMTS) δίκτυα όπου η USIM κάρτα αντιπροσωπεύει τον κινητό συνδρομητή. Αντίθετα, η αυθεντικοποίηση συσκευής που βασίζεται σε κρυπτογραφικά διαπιστευτήρια, δεν είναι διαθέσιμη στο Wi-Fi. Αναμφίβολα εκτελείται σε δίκτυα 3GPP με την επικύρωση του IMEI αριθμού της τερματικής κινητής συσκευής και προστατεύοντας αυτή την μοναδική ταυτότητα ενάντια σε τροποποίηση από κακόβουλους χρήστες.

6.2. IEEE 802.16e Ασφάλεια Σύνδεσης

Οι διαδικασίες εξουσιοδότησης για πρόσβαση στο δίκτυο WiMAX βασίζονται στο πρωτόκολλο PKM έκδοση 2 και σχετικές πολιτικές εξουσιοδότησης που περιγράφονται από το IEEE 802.16e. Το 802.16e μοντέλο δικτύου αποτελείται από τρεις οντότητες: έναν Mobile Station (MS) και ένα BS, συνδεόμενα μέσω μιας 802.16 φυσικής και MAC σύνδεσης, συν έναν προαιρετικό AAA εξυπηρετητή, ο οποίος γενικά αναφέρεται ως Authentication and Service Authorization (ASA) εξυπηρετητής. Ένα σύνολο από BS κάτω από τον έλεγχο ενός διαχειριστή δικτύου παρέχεται από έναν ASA εξυπηρετητή.

Το 802.16-2004 καθορίζει την εναέρια διασύνδεση του WiMAX για σταθερή ασύρματη πρόσβαση. Η ασφάλεια που προσφέρεται εκεί έχει ενημερωθεί σε έναν αριθμό σημείων από το IEEE 802.16e, και ειδικά για την βασισμένη σε EAP αυθεντικοποίηση. Το 802.16e έχει υιοθετήσει τη μοναδική πολιτική εξουσιοδότησης (PKMv1 RSA) διαθέσιμη στην 802.16-2004 για κληρονομικούς λόγους. Στο Extensive Authentication Protocol (EAP), επιτρέπεται η αμοιβαία αυθεντικοποίηση μεταξύ των BS και των MS και παρέχονται δύο two-round πρωτόκολλα αυθεντικοποίησης και εξουσιοδότησης, αποτελούμενα από, για παράδειγμα, μια πρώτη και μια δεύτερη πλήρη EAP συνομιλία για την προετοιμασία της αυθεντικοποίησης συσκευής και χρήστη κατά τη διάρκεια πρόσβασης στο δίκτυο. Η πλήρης λίστα των PKMv2 πολιτικών εξουσιοδότησης είναι η εξής:

- PKMv2 EAP: Εξουσιοδότηση βασισμένη σε EAP
- PKMv2 EAP-AuthEAP: Αυθεντικοποιημένη εξουσιοδότηση βασισμένη σε EAP μετά από εξουσιοδότηση βασισμένη σε EAP
- PKMv2 RSA: Εξουσιοδότηση βασισμένη σε RSA
- PKMv2 RSA-AuthEAP: Αυθεντικοποιημένη εξουσιοδότηση βασισμένη σε EAP μετά από εξουσιοδότηση βασισμένη σε RSA
- PKMv2 RSA-EAP: Εξουσιοδότηση βασισμένη σε EAP μετά από εξουσιοδότηση βασισμένη σε RSA

Ο όρος "AuthEAP" υποδηλώνει ότι η ακεραιότητα και η αυθεντικότητα αυτής της EAP συνομιλίας προστατεύεται στο 802.16 MAC επίπεδο μέσω των κωδικών αυθεντικοποίησης μηνύματος (message authentication codes). Τα κλειδιά τα οποία χρειάζονται για τον υπολογισμό αυτών των κωδικών παράγονται από ένα EAP Integrity Key (EIK). Το EIK είναι ένα από τα αποτελέσματα του πρώτου γύρου εξουσιοδότησης. (δηλαδή, EAP στο "EAP-Auth EAP" και RSA στο "RSA-AuthEAP").

Ανεξαρτήτως από την εκάστοτε πολιτική εξουσιοδότησης, ο πρωταρχικός σκοπός για κάθε μια από αυτές τις πολιτικές από την ασύρματη πλευρά σύνδεσης είναι να εγκαθιδρύσει ένα μυστικό, δηλαδή, ένα Authorization Key (AK), διαμοιραζόμενο μεταξύ του MS και του BS. Ο τρόπος με τον οποίο αυτό το AK παράγεται δύσκολα, εξαρτάται από την εκάστοτε πολιτική εξουσιοδότησης. Ωστόσο, το 160-bit AK πάντα προωθείται ως παράμετρος εισόδου στην παραγωγή των κλειδιών για τους κώδικες αυθεντικοποίησης μηνυμάτων προστατεύοντας τα μηνύματα διαχείρισης και τα KEK κρυπτογραφώντας τα TEK όταν μεταφέρονται στους MS. Τα TEK, αφού έχουν μεταφερθεί με ασφάλεια στο MS, ενεργούν όπως τα κλειδιά τα οποία χρησιμοποιούνται για να κρυπτογραφήσουν (και ανάλογα με τον αλγόριθμο, προστατεύουν επίσης την ακεραιότητα και την αυθεντικότητα αυτών), δεδομένα κίνηση, δηλαδή τα ωφέλιμα φορτία των 802.16 MAC PDU που ανταλλάσσονται μεταξύ MS και BS.

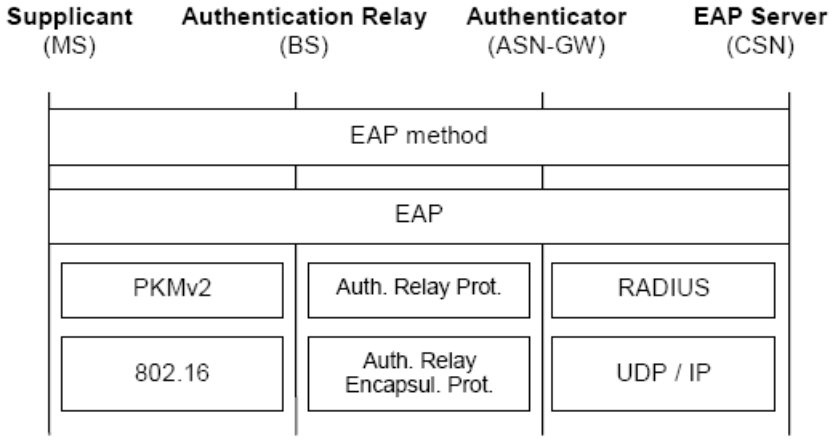
Σημειώνεται εδώ ότι από τη μια πλευρά, αν και το EAP μοντέλο αυθεντικοποίησης συμπεριλαμβανομένου της AAA υποδομής η οποία συζητείται παρακάτω είναι παρόμοιο, υπάρχει ένας αριθμός διαφορών στο πως πραγματοποιείται ασφαλής πρόσβαση δικτύου στο 802.11. Από την άλλη πλευρά η εισαγωγή μιας συσκευής αυθεντικοποίησης σε σχέση με την αυθεντικοποίηση του χρήστη οδηγεί σε

διαφορετικές μεθόδους οι οποίες χρειάζεται να διαπραγματευτούν στο ασύρματο MAC επίπεδο. Η EAP αυθεντικοποίηση υποτίθεται ότι είναι ανεξάρτητη επιπέδου σύνδεσης. Ωστόσο, το πλαίσιο κλειδιού και η παραγωγή είναι διαφορετικές για το 802.16e, όπως η καθιέρωση των κλειδιών για προστασία των 802.16 MAC PDU είναι διαφορετική. Η διαπραγμάτευση της ασφάλειας μεταξύ MS και BS χρησιμοποιεί three-way handshake αντί του four-way handshake.

6.2.1. WiMAX Εξουσιοδοτημένη Πρόσβαση Δικτύου: Single EAP

Είναι σημαντικό, να σημειωθεί ότι το WiMAX περιγράφει τις PKMv2 πολιτικές εξουσιοδότησης κατά τέτοιο τρόπο ώστε να μην κάνει χρήση των PKMv2 πολιτικών εξουσιοδότησης περιλαμβάνοντας την βασισμένη σε RSA αυθεντικοποίηση, αλλά έχει υιοθετήσει την PKMv2 EAP και την PKMv2 EAP–AuthEAP για εξουσιοδοτημένη πρόσβαση στο δίκτυο και τις καλεί "Single EAP" και "Double EAP", αντιστοίχως. Στην πραγματικότητα, αυτό σημαίνει ότι η αυθεντικοποίηση συσκευής στο WiMAX είναι πάντα βασισμένη στο EAP.

Η εικόνα 13 δείχνει πως το WiMAX έχει προσαρμόσει το PKMv2 EAP στο μοντέλο δικτύου, παίρνοντας ως δεδομένο ότι το EAP τερματίζει στο Home CSN και κανένα Visited CSN δεν είναι μεταξύ του ASN και του Home CSN:



Εικόνα 13. WiMAX διαστρωμάτωση πρωτοκόλλου για εξουσιοδότηση πρόσβασης δικτύου.

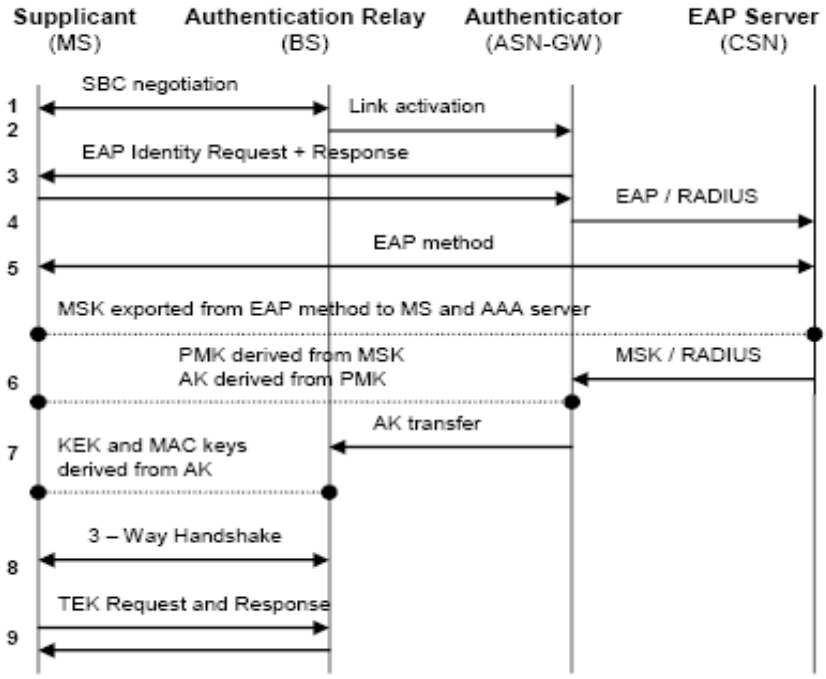
Μια EAP μέθοδος στο WiMAX εκτελείται εντός του EAP πρωτοκόλλου ανάμεσα σε έναν MS ενεργώντας ως τον EAP ικέτη και τον EAP εξυπηρετητή του MS εγχώριου δικτύου. Όπως φαίνεται και στην εικόνα 13, το WiMAX επιτρέπει για την τοποθέτηση της EAP λειτουργίας αυθεντικοποίησης η οποία προωθεί τα EAP

μηνύματα μεταξύ του MS και του EAP εξυπηρετητή στην ASN πύλη (ASN-GW), αντί να τα τοποθετήσει απευθείας στο BS. Ο σκοπός είναι να εξυπηρετεί αρκετούς BS με τον ίδιο EAP αυθεντικοποιητή. Ωστόσο, αυτή η προσέγγιση απαιτεί ένα πρωτόκολλο αυθεντικοποίησης της μετάδοσης (ARP) το οποίο προωθεί EAP μηνύματα από τον BS στην ASN-GW και μετά από πετυχημένη αυθεντικοποίηση, μεταφέρει ασφαλές το AK που παράγεται από τον Αυθεντικοποιητή στον BS. Το WiMAX έχει αποφασίσει να απασχολήσει το RADIUS ως το AAA πρωτόκολλο μεταξύ του Αυθεντικοποιητή και του EAP εξυπηρετητή. Μέσω της εναέριας διασύνδεσης που συνδέει τον MS και τον BS, τα PKMv2 μηνύματα όπως περιγράφονται από το 802.16e ανταλλάσσονται, μεταφέροντας, για παράδειγμα, ενθυλακωμένα EAP μηνύματα ως επίσης και PKMv2 αιτήσεις και απαντήσεις κλειδιών.

Η εικόνα 14 απεικονίζει τη ροή του μηνύματος για single-EAP (τερματίζοντας σε Home CSN και όχι Visited CSN) και επεξηγεί την WiMAX EAP ιεραρχία κλειδιού η οποία ιδρύεται κατά τη διάρκεια αυτής της διαδικασίας. Η εικόνα παρουσιάζει την περίπτωση ενός MS που αρχικά εισέρχεται σε ένα WiMAX δίκτυο και εκτελεί την αυθεντικοποίηση χρήστη χρησιμοποιώντας μια κατάλληλη EAP μέθοδο. Εκτός αυτής της πρότυπης περίπτωσης, ένας αριθμός από παραλλαγές και βελτιστοποιήσεις εφαρμόζονται για επαναυθεντικοποίηση και ελέγχους, ως επίσης και για την συσκευή και συνδυάζοντας αυθεντικοποίηση χρήστη και συσκευής.

Στο βήμα 1, μέσω των 802.16e Station Basic Capabilities (SBC) μηνυμάτων του συνδρομητή, ο MS και BS διαπραγματεύονται ποια PKM έκδοση (σ' αυτό το παράδειγμα: PKMv2), ποια πολιτική αυθεντικοποίησης (σ' αυτό το παράδειγμα: PKMv2 EAP), και ποιους τύπους κωδικών αυθεντικοποίησης μηνύματος πρόκειται να απασχολήσουν. Δύο τύποι αυτών των κωδικών είναι διαπραγματεύσιμοι: hashed – based (HMAC, χρησιμοποιώντας SHA) και cipher-based (CMAC, χρησιμοποιώντας AES). Το μήνυμα ενεργοποίησης της σύνδεσης (Link Activation) στέλνεται στο βήμα 2 στον Αυθεντικοποιητή δραστηριοποιώντας τα μηνύματα αίτησης και απόκρισης ταυτότητας EAP στο βήμα 3. Στο βήμα 4, ο Αυθεντικοποιητής μεταφέρει το EAP μήνυμα απόκρισης ταυτότητας στο Home CSN χρησιμοποιώντας RADIUS. Στο βήμα 5, μια EAP μέθοδος εκτελείται μεταξύ του MS ενεργώντας ως ικέτης και του EAP εξυπηρετητή που είναι τοποθετημένος στο Home CSN. Μετά από μια επιτυχημένη αυθεντικοποίηση, η EAP μέθοδος εξάγει ένα 512-bit Master Session Key (MSK) στον MS και ο AAA Εξυπηρετητής συνδέεται στον EAP εξυπηρετητή. Ο AAA

εξυπηρετητής μεταφέρει το MSK μέσω του RADIUS στον Αυθεντικοποιητή στο βήμα 6. Ο MS παράγει το MSK από μόνος του. Ο Αυθεντικοποιητής και ο MS περικόπτουν το MSK σε μήκος των 160bits. Το κλειδί που προκύπτει αναφέρεται ως Pairwise Master Key (PMK) και χρησιμοποιείται ως είσοδο στην παραγωγή του 160-bit AK. Μια συγκεκριμένη για το 802.16e λειτουργία Παραγωγής Κλειδιού είναι υπεύθυνη για τον υπολογισμό του AK. που δεν εξαρτάται μόνο από το PMK, αλλά επίσης και από τη διεύθυνση MAC του MS και ένα προσδιοριστικό BS . Στο βήμα 7, το ARP μεταφέρει το AK από τον Αυθεντικοποιητή στον BS. Χρησιμοποιώντας την προαναφερθείσα Λειτουργία Παραγωγής Κλειδιού (Key Derivation Function) και το AK ως παράμετρο εισόδου, ο MS και ο BS υπολογίζουν το KEK και δύο κλειδιά για κώδικες αυθεντικοποίησης μηνύματος: ένα για ανερχόμενη (MS→BS) και ένα για την κατερχόμενη (BS→MS) κατεύθυνση.



Εικόνα 14. Single EAP ροή μηνύματος και ιεραρχία κλειδιού.

Στο βήμα 8, ο MS και ο BS εκτελούν μια 3-Way Handshake, κατά τη διάρκεια όπου ο MS και ο BS διαπραγματεύονται ποιος αλγόριθμο κρυπτογράφησης πρόκειται να απασχοληθεί για τη μεταφορά του TEK και την προστασία των δεδομένων κίνησης. Η ακεραιτότητα και η αυθεντικότητα αυτού του handshake προστατεύεται από κλειδιά κωδικών αυθεντικοποίησης μηνύματος που παράγονται ακολουθώντας το

βήμα 7. Τέλος, στο βήμα 9, ο MS αιτείται TEK από τον BS. Ο MS προστατεύει αυτή την αίτηση με το ανερχόμενο κλειδί κωδικών αυθεντικοποίησης μηνύματος. Αν ο BS είναι ικανός να αυθεντικοποιεί επιτυχώς αυτή την αίτηση, ο BS θα στείλει τα TEK στον MS, κρυπτογραφημένα μέσω του KEK όπως δημιουργήθηκε από το βήμα 7. Ένας κατερχόμενος κωδικός αυθεντικοποίησης μηνύματος ασφαλίζει την ακεραιότητα και την αυθεντικότητα αυτής της απόκρισης .

6.2.2. WiMAX Εξουσιοδοτημένη Πρόσβαση Δικτύου: Double-EAP

Η προσαρμογή της PKMv2 EAP – AuthEAP πολιτικής Εξουσιοδότησης στην αρχιτεκτονική δικτύου του WiMAX αναφέρεται ως "Double EAP", αποτελούμενη από δύο πλήρης γύρους EAP. Ο πρώτος γύρος του EAP είναι πάντα υπεύθυνος για την αυθεντικοποίηση της συσκευής και για την παραγωγή ενός πρώτου Master Session Key MSK1. Από την πλευρά του δικτύου, τερματίζει είτε στην ASN είτε στην CSN. Στην περίπτωση της ASN, πρέπει να χρησιμοποιηθεί αυθεντικοποίηση βασισμένη σε πιστοποιητικά για τον MS δεδομένου ότι θα ήταν μια μη ρεαλιστική υπόθεση ένας MS να αναπτύσσει κοινά κλειδιά με κάθε ένα ASN. Αυτό υποστηρίζεται ειδικά για καταστάσεις περιαγωγής κλείσεων. Εδώ, η ASN-GW από μόνη της αναπτύσσει μια λειτουργικότητα EAP εξυπηρετητή για να τερματίσει την αυθεντικοποίηση συσκευής. Ως αποτέλεσμα της αυθεντικοποίησης συσκευής, ένα EIK παράγεται από το MSK1 για να προστατεύσει την ακεραιότητα και την αυθεντικότητα του δεύτερου EAP γύρου στην 802.16 σύνδεση.

Η αυθεντικοποίηση χρήστη λαμβάνει χώρα κατά τη διάρκεια του δεύτερου γύρου του EAP. Αυτή πάντα τερματίζει στο Home CSN. Η μέθοδος EAP όταν εκτελεστεί εξάγει ένα δεύτερο Master Session Key MSK2 στο MS και ο AAA εξυπηρετητής συνδέεται στον EAP εξυπηρετητή στην Home CSN. Σε εξάρτηση με το MSK1 και το MSK2, ο MS και ο Αυθεντικοποιητής υπολογίζουν το AK και η δεύτερη από τους προαναφερόμενους οντότητα δικτύου στέλνει το AK στον BS. Ο MS και ο BS είναι τώρα ικανοί να εκτελέσουν τη 3-Way Handshake και να εγκαθιδρύσουν τα TEK.

6.3. EAP Μέθοδοι Αυθεντικοποίησης

Το EAP [8] το οποίο χρησιμοποιείται για την αυθεντικοποιημένη πρόσβαση στο δίκτυο WiMAX είναι ένα γενικό πρωτόκολλο αυθεντικοποίησης για την υποστήριξη ποικίλων μεθόδων αυθεντικοποίησης ή μεθόδων EAP. Πολλές τέτοιες μέθοδοι είναι

διαθέσιμες ως Internet Drafts. Ωστόσο, μόνο μερικές από αυτές είναι διαθέσιμες ως τελικές προδιαγραφές.

Αν και είναι υποχρεωτικό να χρησιμοποιούνται EAP μέθοδοι για αυθεντικοποίηση χρήστη και για αυθεντικοποίηση συσκευής, το WiMAX δεν περιορίζεται από μόνο του σε ένα σύνολο από EAP μεθόδους οι οποίες πρόκειται να υποστηριχτούν και από τερματικά και δίκτυα. Η επιλογή των EAP μεθόδων παραμένει απόφαση του χειριστή.

Μια ταξινόμηση των EAP μεθόδων βασισμένη στον υποστηριζόμενο τύπο των κρυπτογραφικών διαπιστευτηρίων δίνεται εδώ:

- Μέθοδοι οι οποίες χρησιμοποιούν ασύμμετρα διαπιστευτήρια και X.509 πιστοποιητικά. Ένα παράδειγμα μεθόδου είναι το EAP-TLS [1]. Μέθοδοι αυτής της τάξης απαιτούν τον πελάτη να χρησιμοποιεί ένα ζεύγος δημόσιου / ιδιωτικού κλειδιού και πιστοποιητικό ως είσοδο στην EAP μέθοδο. Λόγω του τυπικά μεγάλου αριθμού των ασύρματων συσκευών, η ανάπτυξη σε συνδυασμό με μια ανάλογη υποδομή δημοσίου κλειδιού δεν είναι κοινή σήμερα. Ωστόσο, το 802.16e υποχρεώνει κάθε WiMAX συσκευή να εφοδιάζεται με ασύμμετρα διαπιστευτήρια για την αυθεντικοποίηση της συσκευής.
- Μέθοδοι οι οποίοι χρησιμοποιούν δυνατά διαμοιρασμένα μυστικά. Παραδείγματα είναι το EAP-PSK, το EAP-SIM και το EAP-AKA. Οι τελευταίες δύο μέθοδοι χρησιμοποιούν 3GPP USIM κάρτες οι οποίες αποθηκεύουν τα διαπιστευτήρια του χρήστη σε ένα ανθεκτικό σε απάτες τεκμήριο.
- Μέθοδοι οι οποίες χρησιμοποιούν συνθηματικά, μια αδύνατη μορφή διαμοιραζόμενων μυστικών προσφέροντας συγκεκριμένες απαιτήσεις στη μέθοδο EAP. Ένα παράδειγμα θα μπορούσε να είναι PEAP –MSCHAP-v2. Έχει αποδειχτεί ότι είναι δύσκολο για τις μεθόδους EAP να υποστηρίξουν μεθόδους βασισμένες σε συνθηματικά και να ταιριάσουν ισχυρές απαιτήσεις ασφάλειας, όπως η προστασία της ταυτότητας ή η αντίσταση ενάντιας σε επιθέσεις λεξικού την ίδια χρονική στιγμή. Ωστόσο, τα συνθηματικά χρησιμοποιούνται αρκετά σε υπάρχουσες υλοποιήσεις .

Δυνατές μέθοδοι βασισμένες σε συνθηματικά τυπικά χρησιμοποιούν μια υβριδική προσέγγιση: πρώτα, ο EAP εξυπηρετητής αυθεντικοποιεί βασισμένος σε

ασύμμετρα διαπιστευτήρια και ένα ασφαλή δίοδος εγκαθίσταται. Διαδοχικά ο πελάτης στέλνει ένα το συνθηματικό (ή ένα αδύνατο διαμοιραζόμενο κλειδί) δια μέσου της προηγούμενης διόδου. Εκτός από αυτή αναφερόμενη μέθοδο, το EAP-IKEv2 υποστηρίζει αυτή τη συμπεριφορά.

7. Ρήγματα Ασφάλειας

Σε αυτή την ενότητα θα παρουσιαστούν διάφορα λάθη και ρήγματα που έχουν αναφερθεί για το μοντέλο ασφάλειας του WiMAX.

7.1. Έλλειψη ρητών ορισμών

Το πιο αξιοσημείωτο πράγμα για το σχεδιασμό του IEEE 802.16 είναι η αποτυχία του να καθορίσει ρητά την SA εξουσιοδότησης, που σημαίνει ότι δεν λαμβάνει ποτέ την ίδια προσοχή με τη λήψη SA δεδομένων. Οι απειλές ενάντια σε SA δεδομένων εφαρμόζονται άμεσα στο SA εξουσιοδότησης, έτσι αυτή η αποτυχία θα οδηγήσει πιθανώς σε προβλήματα.

Παραδείγματος χάριν, δεν διακρίνεται ποτέ μια SA εξουσιοδότησης από μια άλλη, αφήνοντας το πρωτόκολλο ανοικτό σε επιθέσεις επανάληψης. Επιπλέον, η SA εξουσιοδότησης δεν περιλαμβάνει την ταυτότητα του BS, έτσι ο SS δεν μπορεί να διακρίνει εξουσιοδοτημένους από μη εξουσιοδοτημένους BS. Αν και η απόκρυψη της ταυτότητας του BS από το χρήστη μπορεί να είναι επιθυμητή, κρύβοντας την από τον SS αποτρέπει τη διαχείριση κλειδιού και την προστασία του SS από επιθέσεις πλαστογραφίας και επανάληψης.

Αυτό προκαλεί ένα σχετικό πρόβλημα για τις SA δεδομένων. Επειδή ο SS δεν μπορεί να διακρίνει επαναχρησιμοποιημένες SA εξουσιοδότησης, δεν μπορεί επίσης να αναγνωρίσει επαναχρησιμοποιημένες SA δεδομένων. Το σχήμα κρυπτογράφησης είναι επομένως τρωτό σε επίθεση μέσω της επαναχρησιμοποίησης του κλειδιού κρυπτογράφησης.

Ο ασφαλέστερος τρόπος να διορθωθεί η ευπάθεια επανάληψης είναι η πρόσθεση μιας τυχαίας τιμής από τον BS και τον SS στην SA εξουσιοδότησης. Η απαίτηση της εισαγωγής από αμφότερα τα συμβαλλόμενα μέρη μπορεί να προστατεύσει τις συνεισφορές τους. Μια αυθεντικοποιημένη ταυτότητα BS μειώνει επίσης την απειλή ενάντια στους SS λόγω της ασυμμετρίας πιστοποιητικών.

Η απροσεξία στην επανάληψη εμφανίζεται επίσης στον ορισμό SA δεδομένων. Το πρότυπο μεταχειρίζεται το 2-bit προσδιοριστικό κλειδιού ως κυκλικό καταχωρητή, επιτρέποντας σε έναν επιτιθέμενο να παρεμβάλει επαναχρησιμοποιημένα TEK. Οι σχεδιαστές του προτύπου πρέπει να επεκτείνουν το διάστημα προσδιοριστικού κλειδιού για να επιτρέψουν τόσα προσδιοριστικά κλειδιού, όσα μπορούν να μεταφερθούν από τη μεγαλύτερη τιμή διάρκειας ζωής AK. Επειδή ένα AK μπορεί να διαρκέσει μέχρι και 70 ημέρες, ενώ μια διάρκεια ζωής TEK μπορεί να είναι τόσο μικρή όσο 30 λεπτά, μια SA δεδομένων μπορεί να καταναλώσει μέχρι 3.360 TEK κατά τη διάρκεια ζωής του AK, απαιτώντας το διάστημα SAID να αυξηθεί από 2 σε τουλάχιστον 12 bits.

Αυτό εγείρει το σχετικό ερώτημα του πότε ένα TEK πρέπει να λήξει. Στο τρέχον πρότυπο, το TEK λήγει μετά από μια διαμορφώσιμη χρονική περίοδο. Αν και βεβαίως αυτό είναι απαραίτητο, δεν είναι ικανοποιητικό. Στο WiMAX η προεπιλεγμένη διάρκεια ζωής του TEK είναι μισή ημέρα, και το πρότυπο επιτρέπει μια μέγιστη διάρκεια ζωής του TEK επτά ημερών. Αυτοί οι αριθμοί μπορεί να οδηγήσουν σε προβλήματα.

7.2. Ανάγκη για αμοιβαία αυθεντικοποίηση

Η προφανέστερη ρωγμή ολόκληρου του σχεδίου ασφάλειας του WiMAX είναι η έλλειψη ενός πιστοποιητικού BS. Ο μόνος τρόπος να υπερασπίσει ο πελάτης ενάντια σε μια επίθεση πλαστογραφίας ή επανάληψης είναι να αντικαταστήσει το σχήμα αυθεντικοποίησης του προτύπου με ένα σχήμα που παρέχει αμοιβαία αυθεντικοποίηση. Η αμοιβαία αυθεντικοποίηση απαιτείται για οποιοδήποτε ασύρματο μέσο.

7.3. Ευπάθειες εξουσιοδότησης

Η έλλειψη μέσων του σχεδίου IEEE 802.16 για αυθεντικοποίηση του BS στο SS αφήνει το πρωτόκολλο PKM ανοικτό σε επιθέσεις πλαστογράφησης. Σε μια επίθεση πλαστογράφησης, ο SS δεν μπορεί να επικυρώσει ότι οποιαδήποτε μηνύματα πρωτοκόλλου εξουσιοδότησης λαμβάνονται παράχθηκαν από ένα εξουσιοδοτημένο BS. Ο BS κατασκευάζει τις απαντήσεις πρωτοκόλλου εξουσιοδότησης που στέλνει σε έναν SS χρησιμοποιώντας εξ ολοκλήρου δημόσιες πληροφορίες, έτσι οποιοσδήποτε απατεώνας BS μπορεί να δημιουργήσει μια απάντηση. Η απαίτηση του SS για να αυθεντικοποιήσει τον BS μπορεί να περιορίσει αυτήν την ευπάθεια.

Το πρωτόκολλο εξουσιοδότησης υποβάλλει τον SS σε επιθέσεις επανάληψης. Ο απλούστερος τρόπος να αποτραπεί μια τέτοια επίθεση είναι να απαιτήσει ο SS να παραγάγει μια τυχαία πρόκληση στο μήνυμα 2 του πρωτόκολλου αυθεντικοποίησης και ο BS να περιλάβει την πρόκληση στην κατάσταση που επιστρέφει αυθεντικοποιώντας τον ίδιο στο SS.

Το πρωτόκολλο εξουσιοδότησης εκθέτει έναν σοβαρό πρόβλημα σχετικό με το AK. Το πρότυπο δεν επιβάλλει καμία απαίτηση στην παραγωγή AK, ακόμα κι αν η πιο πρόσφατη χρήση της υποθέτει τυχαία παραγωγή (αυτό σημαίνει ότι ένα AK επιλέγεται χρησιμοποιώντας μια ομοιόμορφη κατανομή πιθανότητας στο χώρο των συμβολοσειρών των 160-bit). Το πρότυπο πρέπει να καταστήσει ρητή αυτή την υπόθεση.

Μια άλλη αδυναμία υπάρχει επειδή ο BS συνεισφέρει όλα τα bits σε ένα AK. Αυτό το κοινό σχέδιο σημαίνει ότι ο SS πρέπει να εμπιστευθεί ότι ο BS παράγει πάντα ένα νέο AK που είναι κρυπτογραφικά ξεχωριστό από όλα τα άλλα AK που παράγονται από όλους τους BS. Επίσης σημαίνει ότι η γεννήτρια τυχαίων αριθμών του BS πρέπει να είναι τέλεια, γιατί εάν παρουσιάσει σημαντική στατιστική απόκλιση, αυτό θα μπορούσε να εκθέσει το AK και ως εκ τούτου όλα τα TEK. Ένα ασφαλέστερο σχέδιο θα υπολόγιζε το AK με συνεισφορά από bits και των δυο μερών, παραδείγματος χάριν, AK = HMAC-SHA1(<AK του BS>, <κάποια τυχαία τιμή που παράγεται από το SS>). Συμπεριλαμβάνοντας ακόμη μια δημόσια τυχαία τιμή που παράγεται από έναν SS στον υπολογισμό του AK θα βεβαίωνε το SS ότι τα κλειδιά του είναι φρέσκα.

Τέλος, το πρωτόκολλο υποθέτει ότι τα πιστοποιητικά είναι σωστά εκδιδόμενα. Αυτό σημαίνει ότι κανένα συμβαλλόμενο μέρος με διαφορετικά ζεύγη δημόσιου ή ιδιωτικού κλειδιού δεν πιστοποιείται να χρησιμοποιήσει την ίδια διεύθυνση MAC. Εάν αυτός ο όρος δεν ικανοποιείται, κάθε συμβαλλόμενο μέρος μπορεί να μεταμφιέσει ως άλλο. Η προδιαγραφή πρέπει ρητά να επιβάλλει την υπόθεσή ότι κάθε επικυρωμένη διεύθυνση MAC είναι διακριτή.

Τα προβλήματα με το πρωτόκολλο εξουσιοδότησης αντιπροσωπεύουν μια καταστροφική αποτυχία του IEEE 802.16 σχεδίου ασφάλειας. Τα τμήματα διαχείρισης κλειδιού και κρυπτογράφησης της IEEE 802.16 ασφάλειας δεν προσφέρουν καμία διαβεβαίωση επειδή η ασφάλεια και των δύο στηρίζεται στην ακρίβεια του πρωτοκόλλου εξουσιοδότησης. Αυτή η αποτυχία καταδεικνύει ότι οι

αλγόριθμοι ασφάλειας δεν μπορούν να μεταφέρονται από ένα πλαίσιο σε άλλο χωρίς μεγάλη προσοχή.

7.4. Αποτυχίες διαχείρισης κλειδιού

Λαμβάνοντας υπόψη τις αποτυχίες του πρωτοκόλλου εξουσιοδότησης του WiMAX, δεν έχει σημασία εάν το πρωτόκολλο διαχείρισης κλειδιού είναι σωστό. Εντούτοις, εάν τα λάθη σχεδίου του πρωτοκόλλου εξουσιοδότησης διορθωνόταν, τα προβλήματα στο πρωτόκολλο διαχείρισης κλειδιού θα υπονόμευαν ακόμα την ασφάλεια.

Το πρότυπο αποτυγχάνει να καθορίσει ότι τα TEK είναι τυχαία παραγόμενα χρησιμοποιώντας μια ομοιόμορφη κατανομή πιθανότητας και μια κρυπτογραφικά-ποιοτική γεννήτρια τυχαίων αριθμών. Επειδή το σχήμα κρυπτογράφησης απαιτεί αυτόν τον όρο, το πρότυπο πρέπει να τον επιβάλλει ρητά.

Ομοίως, το σχήμα διανομής κλειδιού δεν προσφέρει καμία διαβεβαίωση φρεσκάδας του TEK. Αυτό είναι βεβαίως αναπόφευκτο για πολλαπλή εκπομπή, αλλά όχι για μονή εκπομπή. Ακόμα, χρησιμοποιώντας ένα σχήμα παραγωγής κλειδιού για να αναμιχθεί η τυχαιότητα του SS στο TEK που παρέχεται από τον BS εύκολα διορθώνει αυτό το πρόβλημα.

Τέλος, για να αποτραπούν οι επαναλήψεις ενάντια στο πρωτόκολλο διαχείρισης κλειδιού, το πρότυπο πρέπει να δέσει τα μηνύματα σε μια συγκεκριμένη περίπτωση πρωτοκόλλου.

7.5. Λάθη προστασίας δεδομένων

Θυμηθείτε ότι το IEEE 802.16 χρησιμοποιεί DES σε CBC κατάσταση για κρυπτογράφηση. Το DES χρησιμοποιεί ένα 64-bit μέγεθος μπλοκ που σημαίνει ότι λειτουργεί σε 64-bit μπλοκ δεδομένων για να επηρεάσει κάθε λειτουργία κρυπτογράφησης ή αποκρυπτογράφησης. Μια CBC κατάσταση χρησιμοποιώντας έναν block cipher με έναν n-bit μπλοκ χάνει την ασφάλειά της μετά από λειτουργία $2^{n/2}$ μπλοκ με το ίδιο κλειδί κρυπτογράφησης. Για το DES ισχύει n=64, έτσι το WiMAX μπορεί ακίνδυνα να προστατεύσει το πολύ 2^{32} 64-bit blocks. Μια μέση παραγωγή 6,36 Mbps παράγει 2^{32} 64-bit blocks σε μισή ημέρα. Ένας μέσος όρος παραγωγής 455 Kbps παράγει 2^{32} 64-bit blocks μέσα στο μέγιστο επιτρεπτό όριο των επτά ημερών. Εάν η μέση ροή δεδομένων υπερβαίνει αυτό το επιτρεπτό από τη

ρύθμιση παραμέτρου διάρκειας ζωής όριο, η χρησιμότητα του σχήματος κρυπτογράφησης είναι πολύ μειωμένη.

Οι άνθρωποι καταλαβαίνουν ότι το DES αποτυγχάνει να παρέχει ισχυρή εμπιστευτικότητα δεδομένων. Εντούτοις, το σχήμα προστασίας δεδομένων πάσχει από σοβαρότερα προβλήματα,.

Το σημαντικότερο αυτών των προβλημάτων είναι η αποτυχία του σχήματος να προστατεύσει από πλαστογραφήσεις ή επαναλήψεις, που είναι οι σοβαρότερες απειλές ενάντια σε οποιοδήποτε ασύρματο σχήμα προστασίας δεδομένων. Ακριβώς όπως το πρωτόκολλο Wired Equivalent Privacy (WEP) του IEEE 802.11, το σχήμα προστασίας δεδομένων δεν προστατεύει ενάντια σε πλαστογράφηση. Η κρυπτογράφηση προστατεύει την ανάγνωση μόνο στο κανάλι WMAN. Δεν προστατεύει το κανάλι από εγγραφές, ακόμη και από κάποιον που δεν κατέχει το κλειδί κρυπτογράφησης.

Το πρωτόκολλο εκθέτει επίσης ένα σοβαρό λάθος σε χρήση κρυπτογράφησης. Το WiMAX χρησιμοποιεί DES σε κατάσταση CBC. Η κατάσταση CBC απαιτεί ένα τυχαίο διάνυσμα αρχικοποίησης για να ασφαλίσει το σχήμα, αλλά το WiMAX χρησιμοποιεί ένα προβλέψιμο διάνυσμα αρχικοποίησης. Η διόρθωση αυτού του προβλήματος απαιτεί τυχαία παραγωγή των διανυσμάτων αρχικοποίησης κάθε πλαισίου και τοποθέτηση τους στο ωφέλιμο φορτίο. Αν και αυτό αυξάνει το overhead της κρυπτογράφησης, δεν υπάρχει καμία άλλη εναλλακτική λύση.

8. Επίλογος

Το WiMAX στοχεύει στο να δώσει τη δυνατότητα σε εκατομμύρια ανθρώπους να έχουν πρόσβαση στο διαδίκτυο ασύρματα, γρήγορα, αλλά και φθηνά.

Η παρούσα εργασία εστιάζεται στην παρουσίαση της τεχνολογίας του IEEE 802.16, αλλά κυρίως στην ανάλυση της αρχιτεκτονικής της ασφάλειας του προτύπου. Επίσης, γίνεται μια μελέτη των πιθανών απειλών που μπορεί να εμφανιστούν σε ασύρματα δίκτυα WiMAX.

Η περιοχή της ασφάλειας αποτελεί ένα επίκαιρο και ανοικτό θέμα προς έρευνα, λόγω των ευπαθειών που συνεχίζουν να παρουσιάζονται στα WiMAX δίκτυα.

9. Αναφορές

[1] Aboba, B., Simon, D., "PPP EAP TLS Authentication Protocol", IETF RFC 2716, 1999

[2] Arbaugh William, Shankar Narendar, Wan Y.C. Justin, "Your 802.11 Wireless network has No clothes", March 2001, http://www.cs.umd.edu/~waa/wireless.pdf.

[3] Barbeau Michel, "WiMax/802.16 Threat Analysis", *Q2SWinet'05*, Montreal, Quebec, Canada, October 2005.

[4] Brayley Jeremy, "Layer 2 Transport Services: An Emerging Application of MPLS", White Paper, Laurel Networks, August 2001.

[5] Falk Rainer, Guenther Christian, Kroeselberg Dirk, Lior Avi, "WiMAX Security Architecture"

[6] Johnston David, Walker Jesse, "Overview of IEEE 802.16 Security", *IEEE Security and Privacy*, Volume 2, Issue 3, pp 40 – 48, May/June 2004.

[7] Kompella Kireeti, "MPLS-based Layer 2 Virtual Private Networks", White Paper, Juniper networks, 2001

[8] Levkowetz, H., "Extensible Authentication Protocol (EAP)", IETF RFC 3748, 2004

[9] NIST FIPS PUB 180-1, "Secure Hash Standard", Apr. 1995, http://csrc.nist. gov/CryptoToolkit/tkhash.html.

[10] NIST FIPS PUB 197, "Advanced Encryption Standard (AES)", November 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[11] Poisel R., *"Modern Communications Jamming Principles and Techniques"*, Artech House Publishers, 2003.

[12] Raya M., Hubaux J.-P., Domino I. Aad., "A system to detect greedy behavior in IEEE 802.11 hotspots", *Proceedings of the 2nd International Conference on Mobile Systems, Applications and Service (MobiSys)*, Boston, 2004.

[13] Simon Dan, "The EAP TLS Authentication Protocol", IETF DRAFT, February 2006

[14] Stallings William, "Wireless Communications and Networks", Prentice Hall, 2002.

[15] Tanenbaum Andrew, *"Δίκτυα Υπολογιστών"*, Εκδόσεις Κλειδάριθμος, Fourth Edition, 2004.

[16] Thikrait Al Mosawi, "Review of existing mobile MBWA technologies (IEEE 802.16 and IEEE 802.20)", November 2004

[17] Walker J., "Unsafe at Any Key Size," Oct. 2000, http://grouper.ieee.org/groups/11/Documents/DocumentHolder/0-362.zip

[18] Whiting D., Housley R., Ferguson N., "Counter with CBC-MAC (CCM)", IETF RFC 3610, September 2003.

[19] Xu Sen, Matthews Manton, Huang Chin-Tser, "Security Issues in Privacy and Key Management Protocols of IEEE 802.16", ACM SE'06, March 2006, Florida, USA

10. Ακρωνύμια

3GPP	Third Generation Partnership Project = Συνεταιρικό Ερευνητικό Έργο Τρίτης Γενιάς
AAA	Authentication Authorization and Accounting protocol = Πρωτόκολλο Αυθεντικοποίησης, Εξουσιοδότησης και Λογαριασμών Πρόσβασης
AES	Advanced Encryption Standard = Προχωρημένο Πρότυπο Κρυπτογράφησης
AI	Authorization Information = Πληροφορία Εξουσιοδότησης
AK	Authorization Key = Κλειδί Εξουσιοδότησης
ALT	Active Life Time of the key = Ενεργή διάρκεια ζωής του κλειδιού
AM	Adaptive Modulation = Προσαρμοστική Διαμόρφωση
APC	Automatic Power Control = Αυτόματος Έλεγχος Ισχύς
Areq	Authentication request = Αίτηση Αυθεντικοποίησης
ARP	Authentication Relay Protocol = Πρωτόκολλο Αυθεντικοποίηση Αναμετάδοσης
ARQ	Automatic Repeat Request = Αυτόματο Αίτημα Επανάληψης
ASA	Authentication and Service Authorization = Αυθεντικοποίηση και Εξουσιοδότηση Υπηρεσίας
ASN	Access Service Network = Υπηρεσία Πρόσβασης Δικτύου
BER	Bit Error Rate = Ρυθμός Λάθους σε Bit
BPSK	Binary PSK = Δυαδική PSK
BS	Base Station = Σταθμός Βάσης
BWA	BroadBand Wireless Access = Ασύρματη Ευρυζωνική Πρόσβαση
CBC	Cipher Block Chaining
CCM	Counter with CBC MAC= Μετρητής με CBC MAC
CID	Connection ID = ID Σύνδεσης
CPS	Common Part Sublayer = Υποεπίπεδο Κοινού Τμήματος
CRC	Cycling Redundancy Checking = Κυκλικός Έλεγχος Πλεονασμού
CS	Convergence Sublayer = Υποεπίπεδο Σύγκλισης
CSN	Connectivity Service Network = Υπηρεσία Συνδεσιμότητας Δικτύου
DAMA	Demand Assignment Multiple Access = Απαίτηση Εκχώρησης Πολλαπλής Πρόσβασης
DES	Data Encryption Standard = Πρότυπο Κρυπτογράφησης Δεδομένων

DoS	Denial of Service = Άρνηση Υπηρεσίας
DSL	Digital Subscriber Line = Ψηφιακή Συνδρομητική Γραμμή
EAP	Extensive Authentication Protocol = Εκτεταμένο Πρωτόκολλο Αυθεντικοποίησης
ECB	Electronic Code Book = Βιβλίο Ηλεκτρονικών Κωδικών
ECC	Error Connection Coding = Κωδικοποίηση Διόρθωσης Σφάλματος
EIK	EAP Integrity Key = EAP Κλειδί Ακεραιότητας
FAMA	Fixed Assignment Multiple Access = Σταθερή Εκχώρηση Πολλαπλής
FDD	Frequency Division Duplexing = Διπλή Διαίρεση Συχνότητας
FDMA	Frequency Division Multiple Access = Πρόσβαση Πολλαπλής Διαίρεσης Συχνότητας
FEC	Forward Error Correction = Προοδευτική Διόρθωση Λαθών
GMH	Generic MAC Header = Γενική MAC Επικεφαλίδα
GSM	Group Special Mobile = Ψηφιακό Δίκτυο Κυψελώδης Επικοινωνίας
HMAC	Hash function-based Message Authentication Code = Κώδικας Αυθεντικοποίησης μηνύματος βασισμένος σε συνάρτηση σύνοψης
IP	Internet Protocol = Πρωτόκολλο Διαδικτύου
IV	Initialization Vector = Διάνυσμα Αρχικοποίησης
KEK	Key Encryption Key = Κλειδί Κρυπτογράφησης Κλειδιού
LAN	Local Area Network = Τοπικό Δίκτυο
LOS	Line – Of – Sight = Γραμμή Οπτικής Επαφής
MAC	Medium Access Control
MAN	Metropolitan Area Network = Μητροπολιτικό Δίκτυο
MBWA	Mobile BWA = Κινητό BWA
MPDU	MAC PDU
MS	Mobile Station = Κινητός Σταθμός
MSK	Master Session Key = Κύριο Κλειδί Συνόδου
N – WEST	National Wireless Electronics Systems Testbed
NLOS	Non Line – Of – Sight = Γραμμή χωρίς Οπτική Επαφή
NWG	Network Operating Group = Ομάδα Δικτύωσης
OFDM	Orthogonal Frequency Division Multiplexing = Ορθογώνια Πολλαπλή Διαίρεση Συχνότητας
OLOS	Optical Line – Of – sight = Γραμμή Οπτικής Επαφής με Εμπόδια
PCMCIA	Personal Computer Memory Card Interface

PDU	Protocol Data Units = Μονάδες Δεδομένων Πρωτοκόλλου
PHY	Physical Layer = Φυσικό Επίπεδο
PK	Public Key = Δημόσιο Κλειδί
PKM	Privacy and Key Management = Ιδιωτικότητα και Διαχείριση Κλειδιού
PMK	Pairwise Master Key
PS	Privacy Sublayer = Υποεπίπεδο Ιδιωτικότητας
PSK	Phase Shift Keying = Ψηφιακή Διαμόρφωση Φάσης
PTM	Point – to – Multipoint = Πολυσημειακή Σύνδεση
PTP	Point – to – Point = Σύνδεση Σημείου προς Σημείου
QAM	Quadrature Amplitude Modulation = Τετραγωνική Διαμόρφωση Πλάτους
QoS	Quality of Services = Ποιότητα Υπηρεσιών
QPSK	Quad PSK = PSK Τεσσάρων Φάσεων
RAWCON	Radio and Wireless Conference = Συνέδριο Ραδιοεπικοινωνιών και Ασύρματων Δικτύων
SA	Security Association = Σχέση Ασφάλειας
SAID	Security Association Identifier = Προσδιοριστικό Σχέσης Ασφάλειας
SAP	Service Access Point = Σημείο Πρόσβασης Υπηρεσίας
SBC	Station Basic Capabilities
SHA	Secure Hash Algorithm = Αλγόριθμος Ασφαλής Σύνοψης
SS	Subscriber Station = Σταθμός Συνδρομητή
TC	Task Group = Ομάδα Εργασίας
TDMA	Time Division Multiple Access
TEK	Traffic Encryption Keys = Κλειδιά Κρυπτογράφησης της Κίνησης
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module
VoIP	Voice over IP
WEP	Wired Equivalent Privacy
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network = Τοπικό Ασύρματο Δίκτυο
WMAN	Wireless Metropolitan Area Network = Μητροπολιτικό Ασύρματο Δίκτυο

11. Απόδοση Αγγλικών-Ελληνικών Όρων

Awake Speed = Ταχύτητα Αφύπνισης

Cells = Κυψέλες

Coverage = Εμβέλεια

Credentials = Διαπιστευτήρια

Downlink = Κατερχόμενη Μετάδοση

End – to – end = Από άκρο σε άκρο

Fresnel Zone = Ζώνη του Fresnel

Global Roaming = Παγκόσμια Περιαγωγή Κλήσεων

Hand over = Αναλαμβάνω τον έλεγχο

Home Operator = Πατρικός, Εγχώριος Χειριστής

Jamming = Μπλοκάρισμα, Παρεμβολή Παρασίτων

Licensed Band = Αδειοδοτημένη Ζώνη

Mesh Mode = Τοπολογία Πλέγματος

Mobility = Κινητικότητα

Mobility Communication = Κινητή Επικοινωνία

Monitoring Anomalies = Παρακολούθηση Ανωμαλιών

Multicast = Πολλαπλή Εκπομπή

Multipath Fading = Πολυδιόδευση

Payload = Ωφέλιμο Φορτίο

Radio Direction Finding tools = Εργαλεία Ραδιογωνιομετρίας

Radio Spectrum = Ραδιοφωνικό Φάσμα, Ραδιοφάσμα

Rekeying = Επαναδημιουργία Κλειδιού

Scalability = Επεκτασιμότητα

Scrambler = Συσκευή Παρεμβολών

Scrambling = Παρεμβολή στο σήμα, Είδος Jamming

Sleep Speed = Ταχύτητα Αναμονής

Spread Spectrum = Εύρος Φάσματος

Standard = Πρότυπο

Tamper-proof = Ανθεκτικό σε απάτες

Throughput = Διεκπεραιωτή Ικανότητα

Uplink = Ανερχόμενη Μετάδοση

Visited Operator = Επισκέψιμος Χειριστής