WiMax Security

Marco Vallini

15 febbraio 2006

Indice

Sommario III

1 Descrizione della tecnologia WiMAX **1**
1.1 Tecnologie d'accesso alle reti geografiche 1
1.2 Definizioni dello standard 2
1.3 Architettura di rete 2
1.4 Copertura del segnale e banda trasmissiva 3
1.5 Servizi a QoS 3
1.6 I livelli MAC e PHY, modello di riferimento 4
1.7 Medium Access Control (Livello MAC) 4
1.8 Physical Layer (Livello fisico) 5
1.8.1 Banda 10 GHz - 66 GHz 5
1.8.2 Banda 2 GHz - 11 GHz 5

2 Analisi delle funzioni di sicurezza **6**
2.1 Proprietà generali della sicurezza 6
2.2 Instaurazione della comunicazione 6
2.3 Architettura di sicurezza 7
2.4 Security Association (SA) 7
2.5 X.509 Certificate profile 9
2.6 PKM (Privacy and Key Management) 10
2.6.1 SS Authorization 10
2.6.2 Stati 10
2.6.3 Scambio e Aggiornamento delle chiavi di traffico (TEK) 11
2.7 Key Usage (considerazioni sull'utilizzo delle chiavi) 12
2.7.1 Authorization Key 12
2.7.2 Traffic Encryption Key 13
2.8 Cryptography 15
2.8.1 Crittografia dei pacchetti dati 16
2.8.2 AK(Authorization Key) 17
2.8.3 TEK (Traffic Encryption Key) 17
2.8.4 KEK (Key Encryption Key) 18
2.8.5 Message Digest 18
2.9 Considerazioni sulle funzionalità di sicurezza offerte 18

3 Vulnerabilità, attacchi e soluzioni **19**
3.1 Introduzione . . . 19
3.2 Tipologie di attacchi e considerazioni generali . . . 19
3.3 Livello fisico . . . 20
3.3.1 Water Torture . . . 20
3.3.2 Jamming . . . 21
3.3.3 Scrambling . . . 21
3.4 Livello MAC . . . 22
3.4.1 Vulnerabilità nelle Security Association . . . 22
3.4.2 Vulnerabilità nell' autenticazione semplice . . . 22
3.4.3 Vulnerabilità generiche associate a messaggi di autenticazione e autorizzazione 23
3.4.4 Vulnerabilità nella generazione della chiave AK . . . 24
3.4.5 Vulnerabilità nella generazione della chiave TEK . . . 24
3.4.6 Vulnerabilità nella crittografia dei dati . . . 25
3.5 Nuovi meccanismi di sicurezza . . . 25
3.5.1 Autenticazione mediante protocollo EAP . . . 25
3.5.2 Miglioramenti nella gestione delle chiavi . . . 25
3.5.3 Ottimizzazione delle procedure di re-autenticazione per la mobilità . . . 26

4 Considerazioni finali **27**

Bibliografia **28**

Sommario

Questo documento, tratta l'analisi della tecnologia, delle funzionalità di sicurezza, delle vulnerabilità e dei possibili rimedi dello standard WiMAX (definito da WiMAX Forum), complementare a quello 802.16 (definito da IEEE). Le informazioni raccolte per le prime due parti, si basano sugli ultimi standard 802.16-2002 e 802.16-2004 (revisione del 2001), disponibili pubblicamente. Attualmente è stato approvato lo standard 802.16e (non disponibile pubblicamente), che introduce e specifica il concetto di mobilità delle stazioni. La trattazione delle vulnerabilità, e dei possibili rimedi, si basa sull'analisi di alcuni articoli liberamente disponibili in rete.

Capitolo 1

Descrizione della tecnologia WiMAX

1.1 Tecnologie d'accesso alle reti geografiche

Le installazioni presenti per le tecnologie di accesso alle reti geografiche, si possono suddividere in tre tipologie:

- Broadband: utilizzata in ambito sia domestico che aziendale, dove è presente una linea DSL o un cable modem, e, normalmente solo in ambito aziendale, con linee HDSL, T1, T3 ed a fibra ottica.
- Wi-Fi: utilizzata sia in ambito casalingo che aziendale, ove è presente un router o access point Wi-Fi, oppure in zone hot spots, come ristoranti, alberghi, stazioni, aeroporti
- Dial-up: utilizzata normalmente in ambito casalingo, spesso perché la tecnologia broadband non è disponibile

La tecnologia d'accesso broadband, è tuttavia, abbastanza costosa, e normalmente viene utilizzata in aree densamente popolate, a scapito di aree rurali. Spesso, il costo della posa o dell'utilizzo di apparecchiature dedicate, non la rendono conveniente dal punto di vista economico. Il Wi-Fi, è una tecnologia flessibile, tuttavia i limiti principali sono tre: scarsa copertura del segnale (da qualche decina a un centinaio di metri), scarsa diffusione sul territorio di hot spots pubblici, e problemi di sicurezza più complessi, rispetto alle tecnologie wired. Il Dial-up, è una tecnologia sempre meno utilizzata, soprattutto per la scarsa banda disponibile nelle trasmissioni. La tecnologia WiMAX (Worldwide Interoperability for Microwave Access), standardizzata da IEEE nel 802.16, prevede:

- Alta velocità per servizi broadband
- Tecnologia senza fili (wireless) per abbattere i costi di posa ed installazione
- Copertura del servizio ad ampio raggio, a livello geografico, per es. in zone rurali

Un'ulteriore caratteristica, che potrà rendere il WiMAX, una tecnologia più flessibile sarà l'impiego di terminali mobili (Mobile WiMAX, 802.16e), che potranno scambiare informazioni anche in movimento. Questa, potrà incrementare le potenzialità dei servizi come VoIP e del Video On Demand, ponendola in diretta competizione con l'UMTS. Tuttavia, le tecnologie wireless, sono soggette a problematiche di sicurezza più complesse rispetto a quelle wired.

1.2 Definizioni dello standard

Lo standard della tecnologia WiMAX, definito da IEEE nell'802.16 e, successivamente aggiornato nel 802.16a, specifica l'interfaccia *aria* (detta air interface) per l'accesso wireless broadband (BWA) per i sistemi fissi. Vengono definiti: il livello MAC (Medium Access Control) ed il livello PHY (Physical), in modo da rispettare diversi ambienti operativi. Lo standard, definisce inoltre un insieme di tipologie di servizi supportati, come VoIP, trasferimento dati e Video On Demand.

1.3 Architettura di rete

La tecnologia WiMAX, opera in modo simile al Wi-Fi, garantendo però maggiore velocità, maggiore diffusione (sotto questo aspetto più simile alle reti cellulari) e, in generale, maggiore sicurezza (vi sono tuttavia alcune problematiche abbastanza critiche). L'architettura si basa su due elementi principali:

- Base Station (BS) detta anche WiMAX tower: è il concentratore, concettualmente simili alle base station della telefonia cellulare
- Subscriber Station (SS) detta anche WiMAX receiver: è il dispositivo, composto da ricevitore ed antenna, che permette la comunicazione tra client e BS. Nello standard 802.16e sono ridefinite MS (Mobile Station)

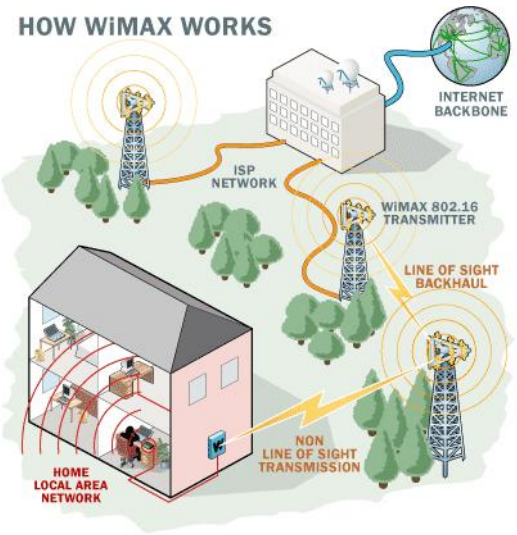

Figura 1.1. Modello d'accesso alla rete, Rif.[1]

La Base Station può essere configurata in due modalità: può essere connessa direttamente al backbone (utilizzando una linea wired broadband, per es. fibre ottiche), oppure, può essere connessa utilizzando un collegamento, in modalità line-of-sight (LOS), ad un'altra base station (configurazione detta backhaul). Attualmente, lo standard della tecnologia WiMAX definisce due modalità di servizio: non-line-of-sight (NLOS), oppure line-of-sight (LOS). La modalità non-line-of-sight dovrebbe essere utilizzata nelle frequenze da 2 GHz a 11 GHz, e impiegare un'antenna di dimensioni ridotte. Queste trasmissioni non sono facilmente interrotte da ostacoli fisici. La

seconda modalità, quella line-of-sight, dovrebbe essere utilizzata dalle frequenze tra 10 GHz e 66 GHz, impiegando un'antenna esterna più complessa e fissa. L'utilizzo di queste frequenze consente una maggiore banda trasmissiva, trascurando gli effetti di multipath (percorsi multipli).

1.4 Copertura del segnale e banda trasmissiva

Il dato generico, fornito sulla copertura del segnale radio, è di circa 50 Km di raggio, tuttavia può essere fuorviante, in quando tecnicamente dipende dalla modalità di trasmissione LOS, oppure NLOS. In particolare, in modalità LOS, la copertura è circa 16 Km di raggio, che consente una buona scalabilità. La modalità NLOS, permette di ottenere un raggio di trasmissione di circa 6-8 Km. Ciò comporta l'utilizzo di più celle per raggiungere sia una maggiore copertura, che una maggiore qualità del segnale, soprattutto in presenza di servizi che richiedano QoS (Quality of Service). Il throughput è abbastanza elevato, il dato teorico è di circa 70-75 Mbps per canale. Tuttavia, nelle applicazioni reali, si può ottenere un valore prossimo a 45 Mbps per canale (Rif.[7]). Questa differenza è dovuta principalmente, alla condivisione del servizio radio. Altri elementi che influiscono sul throughput sono:

- schema di modulazione, per es. QPSK, 16QAM, 64QAM, ecc.
- distanza dalla Base Station
- dimensione dello spettro del canale (per es. da 1 a 20 MHz)

In generale si osserva che, a basse frequenze è possibile aumentare l'estensione del segnale radio, a scapito della banda trasmissiva e, ad alte frequenze, è possibile aumentare la banda trasmissiva, a scapito dell'estensione del segnale. Si può quindi concludere che le scelte, sulla dimensione della banda di trasmissione e sull'estensione del segnale, debbano essere considerate in base al tipo di servizio offerto (per es. trasmissione dati, VoIP, Video On Demand), ed alla morfologia del territorio.

1.5 Servizi a QoS

In generale con QoS, ci si riferisce a tutti quei servizi che possiedono requisiti specifici sul traffico generato. Formalmente indica la probabilità che una rete possa soddisfare particolari specifiche sul traffico. Alcuni esempi sono le applicazioni in cui il ritardo è un requisito indispensabile, come per il VoIP, oppure applicazioni real-time. Le standard 802.16 supporta i servizi QoS attraverso:

- l'introduzione di un insieme di tipologie di traffico definite nel livello MAC
- l'introduzione di una modulazione adattativa
- l'introduzione della capacità di configurazione dinamica dei collegamenti in funzione delle condizioni di traffico
- l'introduzione di tecniche per diminuire l'overhead dei messaggi di segnalazione e, meccanismi efficienti di polling

Tuttavia i dettagli che riguardano gli aspetti della gestione, della schedulazione e della prenotazione, non sono stati standardizzati, per consentire la differenziazione delle soluzioni dei produttori, permettendo approcci diversi, in funzione delle caratteristiche del servizio offerto (per es. applicazioni VoIP piuttosto che applicazioni real-time con requisiti più stringenti in termini di ritardo).

1.6 I livelli MAC e PHY, modello di riferimento

Il modello di riferimento comprende due livelli: il livello MAC (Medium Access Control) ed il livello PHY (Physical). Il livello MAC è stato progettato principalmente per supportare una topologia di rete punto-multipunto (condivisione del mezzo trasmissivo), ma consente, opzionalmente, anche l'utilizzo di quella mesh (maglia). La struttura del MAC consente di supportare diverse specifiche per il livello fisico (PHY), ognuna indicata per un particolare ambiente operativo. La flessibilità offerta da questi livelli, permette operazioni sulla dimensione in termini di banda dei canali, divisione in frequenza (FDD) e divisione in tempo (TDD). Anche se vi sono diversità nelle modalità di utilizzo e di allocazione dei canali, vi sono alcune caratteristiche comuni, tra cui l'inizializzazione, la registrazione, la richiesta di banda e l'utilizzo di canali connection-oriented, per la gestione e la trasmissione dati. La trasmissione, si basa sul concetto di frame. Il downlink frame (dalla BS alla SS) contiene al suo interno, due slot map: uno dedicato al downlink (DL_MAP) e l'altro dedicato all'uplink (UP_MAP). Le informazioni contenute nelle slot map riguardano la posizione, la dimensione e la codifica di tutti gli slot presenti nei frame di uplink e downlink. Il livello MAC è connection-oriented, ed ogni slot appartenente ad una determinata connessione, è identificato tramite un'etichetta (ID). Vi sono due tipologie di connessione: management connection e transport connection. La prima, è una connessione che viene utilizzata per tutte le operazioni di gestione, come richieste di banda, messaggi di gestione ecc. E' presente anche una seconda connessione, di tipo management, che viene utilizzata per trasportare i pacchetti di gestione del protocollo IP. La seconda, quella di tipo transport, è utilizzata per trasportare i dati. Il meccanismo di gestione del collegamento di 802.16, si occupa di allocare dinamicamente le connessioni di trasporto per i pacchetti utente. Un aspetto importante, dal punto di vista della sicurezza, è la protezione da parte di 802.16 solo dei dati utente e del secondo canale di management, quello che trasporta i pacchetti di gestione di IP.

1.7 Medium Access Control (Livello MAC)

Sia le funzionalità espresse in precedenza, che le altre del livello MAC, sono distribuite in tre sottolivelli:

- Service-Specific Convergence Sublayer (CS)
- MAC Common Part Sublayer (CPS)
- Security Sublayer (anche detto Privacy Sublayer)

Il sottolivello CS si occupa principalmente di trasformare i dati provenienti dalla rete, della classificazione, dell'associazione degli stessi ai flussi dei diversi servizi MAC e, dell'identificazione del collegamento. Sono inoltre previste, alcune specifiche per l'interfacciamento verso diversi protocolli. Il sottolivello CPS provvede alle funzionalità chiave dell'accesso al sistema, come l'allocazione di banda, l'instaurazione di connessioni ed il mantenimento delle stesse. Il sottolivello di sicurezza si occupa invece delle funzioni di autenticazione, distribuzione delle chiavi, integrità e crittografia dei dati. Lo standard specifica che: sia l'accesso che l'allocazione di banda, sono stati progettati per supportare centinaia di client per canale, con terminali che possono essere condivisi da più utenti. Inoltre il livello fisico specifica il supporto al traffico, sia a flusso continuo che in modalità burst, per soddisfare le diverse tipologie di servizi utilizzate dagli utenti, come voce e dati. Per quanto riguarda gli aspetti della modulazione e degli schemi di codifica, l'interfaccia tra MAC e PHY è stata progettata per consentire adattamenti per ogni singolo burst, aumentando così l'efficienza del sistema. I pacchetti generati dal livello MAC sono detti MAC PDU, e sono costituiti tra tre sezioni:

header, payload e CRC (opzionale). Infine il livello MAC contiene funzionalità per la gestione di diversi livelli di QoS, per un terminale. E' specificato che, anche in presenza di più connessioni, l'efficienza non diminuisce ed i livelli di QoS sono preservati. Questa affermazione presuppone che il servizio sia garantito solo per un numero massimo di utenti, stabilito a priori.

1.8 Physical Layer (Livello fisico)

Il livello fisico può operare principalmente in due range di frequenze diversi. Il primo, standardizzato nel 2002 (il documento è datato 2002, l'approvazione è avvenuta nel 2001), è stato quello tra 10 GHz e 66 GHz. Successivamente, nel 2004 (802.16a), è stato approvato quello operante nel range da 2 GHz a 11 GHz.

1.8.1 Banda 10 GHz - 66 GHz

L'utilizzo della banda tra 10 GHz e 66 GHz, richiede una licenza. La modalità di trasmissione adottata è quella LOS ed, a causa della lunghezza d'onda, il multipath è trascurabile. I canali utilizzati, hanno una dimensione di 25-28 MHz. Questa banda trasmissiva, è adatta ad ambienti SOHO (Small Office/Home Office). La modulazione è a single-carrier, ovvero, un tipo di trasmissione che prevede l'invio di un singolo canale per portante. L'interfaccia è denominata WirelessMAN-SC.

1.8.2 Banda 2 GHz - 11 GHz

Per quanto riguarda le frequenze sotto gli 11 GHz, a causa della lunghezza d'onda maggiore, rispetto al caso precedente, si può utilizzare la modalità NLOS, tuttavia il problema del multipath può diventare significativo. L'utilizzo di questa modalità di trasmissione, richiede di implementare, a livello fisico, diverse funzionalità rispetto alla modalità LOS, come per esempio, tecniche avanzate di power management, tecniche di correzione dovute ad interferenze e, l'analisi di problematiche derivanti dall'impiego di antenne multiple. Vi sono quattro tipologie di interfacce: WirelessMAN-SCa, WirelessMAN-OFDM, WirelessMAN-OFDMA e WirelessHUMAN.

Capitolo 2

Analisi delle funzioni di sicurezza

2.1 Proprietà generali della sicurezza

In generale, quando si vuole rendere sicura una comunicazione, si considerano diverse proprietà, che correttamente integrate, permettono di definire l'architettura ed i meccanismi da utilizzare a questo scopo. Alcune proprietà sono:

- Riservatezza o confidenzialità: protegge il trasferimento delle informazioni da attacchi passivi. Dovrebbe essere garantita sia sui dati utente che su altre informazioni di gestione
- Integrità: garantisce contro la modifica dei dati durante il trasferimento. In generale, il meccanismo utilizzato è il calcolo del digest
- Autenticazione: garantisce che l'identità della sorgente è quella definita nel mittente nei messaggi trasferiti. Può essere semplice o mutua. L'autenticazione può essere anche dei dati oltre che per i soggetti
- Non ripudio: garantisce che l'autore dei dati non possa smentire di averli creati e/o inviati. E' una prova formale che può essere utilizzata in tribunale
- Controllo dell'accesso/Autorizzazione: capacità di verificare e controllare l'accesso alle risorse di un sistema, ogni entità deve essere identificata e autenticata
- Disponibilità: capacità di evitare la perdita o la riduzione della disponibilità di una risorsa e/o di un servizio di un sistema
- Tracciabilità: capacità di verificare e controllare le operazioni svolte da una entità

2.2 Instaurazione della comunicazione

Prima di affrontare l'analisi dell'architettura, e delle caratteristiche di sicurezza del WiMAX, è necessario comprendere le modalità ed i meccanismi per l'instaurazione di una comunicazione tra SS e BS. La sequenza di operazioni è la seguente:

1. SS effettua una scansione per cercare un segnale di downlink adatto (segnale trasmesso dalla BS), che userà per impostare i parametri del canale

2. con i dati acquisiti dal segnale di downlink, la SS imposta a livello fisico i parametri corretti per aprire un canale primario di management verso la BS. Questo canale è utilizzato per la negoziazione dei parametri di comunicazione, per l'autorizzazione e per la gestione della chiave di cifratura

3. Il protocollo PKM (Privacy and Key Management) è responsabile dell'autorizzazione, quindi se la SS possiede i diritti necessari, la autorizza a registrarsi presso la BS

4. Se l'autorizzazione è stata concessa, la SS deve registrarsi presso la BS trasmettendo un messaggio di request. La BS risponde, assegnando un identificatore (ID) per la seconda connessione di management

5. SS e BS creano una connessione di trasporto, utilizzando la primitiva MAC_create_connection. Inoltre, in una richiesta di creazione di una connessione di questo tipo, viene specificato se sia necessario utilizzare le funzionalità di crittografia a livello MAC

2.3 Architettura di sicurezza

L'architettura di sicurezza è implementata nel sottolivello Security Sublayer del MAC. Lo scopo di questo livello è, come detto in precedenza, quello di gestione dell'autenticazione, distribuzione delle chiavi, verifica dell'autenticità di alcuni messaggi (integrità) e crittografia dei dati, per garantirne la proprietà di riservatezza. L'architettura utilizza due tipologie di protocolli:

- *encapsulation protocol*: crittografa i pacchetti di dato, definisce: (1) un insieme di suite di crittografia (cryptographic suite), per esempio gli algoritmi di autenticazione e, (2) le regole di applicazione degli algoritmi al payload MAC PDU.

- *PKM*: distribuisce le chiavi in modo sicuro tra BS ed SS. Attraverso questo protocollo, BS ed SS sincronizzano le chiavi, inoltre la BS lo utilizza anche per condizionare l'accesso ai servizi

L'architettura del livello di sicurezza, utilizza cinque meccanismi principali: Security Association, X.509 Certificate profile, PKM (Privacy and Key Management), Key usage, cryptography.

2.4 Security Association (SA)

La security association è un insieme di informazioni di sicurezza, che la BS condivide con uno o più SS, per supportare una comunicazione sicura e, sono identificate tramite un'etichetta, detta SAID. Le informazioni condivise in SA includono la suite di crittografia (Cryptographic suite), ed eventualmente, TEK e vettore di inizializzazione. Il contenuto, può variare, in quanto dipende direttamente dalla suite di crittografia utilizzata. Sono definiti tre tipi di SA:

- Primary: viene utilizzata da una SS durante la fase di inizializzazione

- Static: viene configurata dalla BS

- Dynamic: viene instaurata e distrutta in modo dinamico, per l'inizializzazione e la terminazione di flussi specifici

Quando la SS entra in rete, la BS genera automaticamente una SA, per il canale secondario di management. In generale una SS possiede due o tre SA: una per il canale di management e una o due per i canali di traffico in uplink e downlink. Uplink e downlink, quindi, possono condividere una

SA. Per garantire il supporto multicast ogni gruppo necessita di una SA condivisa, da distribuire a tutti i membri. Lo standard consente l'utilizzo della stessa security association per connessioni diverse. Per rendere sicura una connessione di tipo trasporto, la SS inizializza una SA utilizzando la primitiva di richiesta *create_connection*. In genere le informazioni contenute nella SA sono:

- Identificatore SAID, 16 bit
- Algoritmo di cifratura, utilizzato per crittografare i dati durante la trasmissione: lo standard del 2001 proponeva DES in modalità CBC, lo standard del 2004 aggiunge AES CCM
- Due chiavi di crittografia per il traffico (TEK - Traffic Encryption Key): una valida per le operazioni correnti e l'altra utilizzata alla scadenza della prima
- Un identificatore a 2-bit per ogni TEK
- Durata del TEK (TEK lifetime). Il valore di default è 12 ore, il minimo 30 minuti, il massimo 7 giorni
- Un vettore di inizializzazione a 64-bit per ogni TEK
- Un indicatore sulla tipologia di SA: Primary, Static, Dynamic

Nell'802.16, viene inoltre definita, una particolare security association per scopi di autorizzazione, detta Authorization SA e composta da:

- X.509 certificate profile che identifica la SS
- AK (Authorization Key): una chiave di autorizzazione a 160-bit
- 4-bit per identificare AK
- Durata di AK: variabile da 1 a 70 giorni, di default è 1 giorno
- KEK (Key Encryption Key): 112-bit Triple-DES. Utilizzato per distribuire TEK. (Per la costruzione della chiave si rimanda alla sezione *cryptography*)
- Downlink authentication code (HMAC) key: (basato su una funzione di hash), provvede a garantire l'autenticità del messaggio di distribuzione della chiave, dalla BS alla SS. (Per la costruzione della chiave si rimanda alla sezione *cryptography*)
- Uplink HMAC key: (anch'esso basato su una funzione di hash) provvede a garantire l'autenticità del messaggio di distribuzione della chiave, dalla SS alla BS. (Per la costruzione della chiave si rimanda alla sezione *cryptography*)
- Una lista contenente le SA autorizzate

Una Authorization SA è uno stato condiviso tra una specifica BS ed una SS. Lo standard assume che sia la BS che la SS mantengano segreta la chiave AK. Le base station utilizzano le authorization SA, per configurare i dati riguardanti le SA delle subscriber station. Utilizzando il protocollo PKM, la SS richiede alla BS informazioni sulle impostazioni riguardanti la chiave di cifratura (keying material) della SA (per es. l'algoritmo di crittografia utilizzato). Queste informazioni hanno una durata limitata. Quando la BS informa la SS include anche la durata delle stesse. E' compito della SS richiedere nuove informazioni prima che le *keying material* in possesso scadano. Il protocollo PKM specifica come SS e BS mantengono la sincronizzazione della chiave

2.5 X.509 Certificate profile

Lo standard 802.16 utilizza la versione 3 dei certificati X.509, ma non le relative estensioni, definite dalla IETF nell'RFC 2459. Tutti i certificati sono firmati utilizzando l'algoritmo RSA, e come funzione di hash SHA1. Nel WiMAX, esistono due tipologie di certificati: *Manufacturer certificate* e *SS certificate*. Non esistono, invece, certificati per le BS. Il primo riguarda il costruttore del dispositivo, ed il secondo, il dispositivo stesso. Il certificato del costruttore può essere self-signed, oppure firmato da una terza parte. Il certificato della subscriber station è generato e firmato dal costruttore, identifica una particolare SS, e contiene all'interno del campo *subject* l'indirizzo MAC. In generale la BS utilizza la chiave pubblica del costruttore, per verificare il certificato proposto dalla SS, valutando quindi l'autenticità del dispositivo. Lo standard, definisce anche alcune precauzioni e modalità di conservazione degli SS certificate. In particolare devono essere registrati in modo permanente, all'interno della SS, in una memoria scrivibile una sola volta. L'installazione della coppia chiave pubblica e privata, deve essere introdotta durante la fase di produzione. La memoria e le sue informazioni, non devono poter essere alterate, almeno in linea di principio. Queste specifiche di sicurezza sono particolarmente importanti, in quanto, poter manipolare le informazioni registrate all'interno della memoria, costituisce una fonte di possibili attacchi al sistema. Per esempio, consideriamo il caso di possedere due schede, di tipo SS dello stesso produttore. Se si potesse prelevare il certificato di una scheda ed inserirlo nell'altra, modificando il MAC address in accordo con il campo *subject* del certificato, un attaccante, potrebbe riuscire a ingannare la BS, presentandosi con credenziali appartenenti ad un altro dispositivo. Lo standard X.509 definisce diversi campi, quelli più significativi per lo standard WiMAX sono:

- Version: versione 3
- Serial number: un identificativo univoco di tipo intero, che la CA (Certification Authority) assegna al certificato
- Signature: algoritmo utilizzato per la firma
- Issuer: nome della CA che ha rilasciato il certificato
- Validity: periodo di validità, specifica data di inizio e data di scadenza
- Subject: nome appartenente all'entità che è stata certificata
- SubjectPublicKeyInfo: contiene i parametri e la chiave pubblica dell'entità certificata
- SignatureAlgorithm: algoritmo utilizzato
- SignatureValue: contiene la firma della CA

Nello standard alcuni campi dei certificati contengono delle restrizioni rispetto all'X.509. Il campo di validità (*validity*) specifica la durata sia per il Manufacturer certificate che per il SS certificate. In generale, per l'SS certificate, la data di inizio validità coincide con la produzione del dispositivo e, la data di scadenza, dovrebbe essere superiore alla durata di utilizzo (lo standard consiglia almeno 10 anni). Il certificato non è rinnovabile. La data di scadenza del Manufacturer certificate dovrebbe essere, per ovvie ragioni, superiore a quella dei SS certificate che produce. Il campo, che esprime il numero di serie (*serial number*), è assegnato dal costruttore in ordine crescente. I campi *signature* e *signature algorithm* contengono i riferimenti all'algoritmo RSA e alla funzione di hash SHA1.

2.6 PKM (Privacy and Key Management)

2.6.1 SS Authorization

La BS, prima di accettare l'associazione alla rete da parte una SS, deve valutare se sia in possesso delle credenziali opportune. Questa valutazione avviene attraverso il protocollo PKM authorization, che ha il compito di distribuire i token di autorizzazione alle SS. Più precisamente, il processo di autorizzazione è costituito da tre messaggi, scambiati tra BS e SS. Nel primo messaggio, la SS invia un Authentication Information (IA). Subito dopo, l'SS invia il secondo messaggio, contenente un Authorization request (Areq) alla BS. In risposta a questo messaggio, la BS invia un Authorization reply (Arep) alla SS. La sequenza dei messaggi scambiati è la seguente:

```
Messaggio1: (AI) : SS -> BS : Cert(Manufacturer(SS))
Messaggio2: (Areq) : SS -> BS : Cert(SS) | capabilities | CID
Messaggio3: (Arep) : BS -> SS : RSA-Encrypt(PubKey(SS), AK) |
AK lifetime | SeqNo (4-bit) | SAIDs
```

Nel *Messaggio1*, SS invia il certificato X.509 del costruttore. Questo messaggio è solo informativo, tuttavia è importante, in quanto è il meccanismo con cui la BS riceve il certificato del costruttore della SS. Il Messaggio2, è inviato subito dopo, e contiene il certificato della SS (questo è il certificato specifico del dispositivo), è utilizzato per richiedere l'AK (Authorization Key) e per la lista di SAID (Security Association ID). La richiesta di autorizzazione contiene anche:

- La descrizione degli algoritmi di crittografia utilizzati
- CID (Connection ID): è il primo identificatore che la BS assegna alla SS durante l'inizializzazione, ottenuto dal segnale di beacon

In risposta all'Authorization request (*Messaggio2*), la BS valida l'identità della SS, determina la suite di crittografia ed i protocolli supportatati dalla SS, attiva l'AK, la crittografa utilizzando la chiave pubblica della SS, ed invia queste informazioni nel Messaggio3 direttamente alla SS. La risposta all'autorizzazione contiene inoltre:

- Un sequence number (SeqNo) espresso su 4-bit, usato per identificare l'AK, distinguendola da quelle generate precedentemente
- Durata di validità della chiave AK (AK lifetime)
- La lista delle security associations (SAIDs) e le proprietà

Quando la BS provvede a valutare il certificato del costruttore inviatole dalla SS, analizzando lo standard, si assume che tutti i costruttori riconosciuti siano considerati attendibili. Periodicamente la SS, prima che l'AK scada, richiede una nuova chiave, attraverso l'utilizzo del *Messaggio2*, senza più inviare il *Messaggio1*. Per evitare problemi d'interruzione, dovuti alla durata di vita della chiave, nella fase di transizione per il passaggio da una chiave ad un'altra, sia la BS che la SS supportano l'utilizzo di due chiavi attive contemporaneamente.

L'implementazione del processo di autorizzazione, avviene attraverso una macchina a stati finiti, modellata attraverso sei stati e otto eventi.

2.6.2 Stati

Start: stato iniziale, nessuna risorsa è stata assegnata, nessun processo è programmato.
Auth Wait (*Authorize Wait*): la SS ha ricevuto l'evento *Communication Established*, che indica

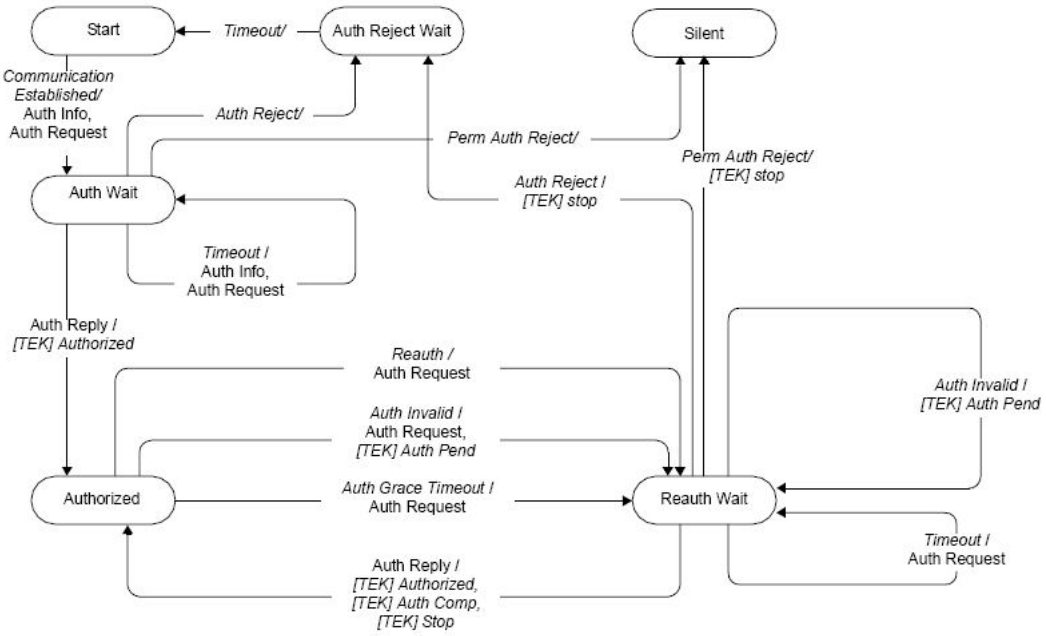

Figura 2.1. Authorization state machine, Rif.[1]

il completamento della negoziazione delle capabilities con la BS. In risposta a questo evento, la SS invia il *Messaggio1* (Authentication Information) ed il *Messaggio2* (Authorization request) alla BS.
Authorized: la SS ha ricevuto dalla BS il *Messaggio3* (Authorization reply), contenente la chiave AK e la lista delle SAID. La transizione in questo stato innesca la creazione di una macchina a stati finiti (di tipo TEK) per ogni SAID abilitato.
Reauth Wait (*Reauthorize Wait*): la SS ha inviato una richiesta di re-autorizzazione, e sta attendendo una risposta. Questo perché l'autorizzazione sta per scadere, oppure ha ricevuto un messaggio di Authorization Invalid dalla BS.
Auth Reject Wait (*Authorize Reject Wait*): la SS ha ricevuto un messaggio di Authorization Reject, in risposta all'ultimo messaggio di richiesta di autorizzazione (Auth request). Il codice ritornato, indica che la situazione di errore non è permanente. In risposta a questo evento, la SS innesca il timer e aspetta il timeout, passando successivamente nello stato di *Start*.
Silent: la SS ha ricevuto un messaggio di Authorization Reject, in risposta all'ultimo messaggio di richiesta di autorizzazione (Auth request). Il codice ritornato in questo caso indica che la situazione di errore è permanente. La SS quindi non può inviare traffico.

2.6.3 Scambio e Aggiornamento delle chiavi di traffico (TEK)

Dopo aver ottenuto la chiave AK dalla BS, e dopo essere entrata nello stato *Authorized*, la SS, crea una *state machine*, per ottenere dalla BS una chiave di crittografia per il traffico. La macchina a stati è responsabile della gestione delle chiavi di traffico per ogni SAID. Attraverso una sequenza di 2/3 messaggi, la SS ottiene la chiave TEK. La sequenza dei messaggi, è la seguente:

```
Messaggio1: BS -> SS : SeqNo | SAID | HMAC(1)
```

```
Messaggio2: SS -> BS : SeqNo | SAID | HMAC(2)
Messaggio3: BS -> SS : SeqNo | SAID | OldTek | NewTek | HMAC(3)
```

Il *Messaggio1* è opzionale, in quanto utilizzato dalla BS solo per forzare la rigenerazione delle chiavi di traffico, in presenza di una precedente o nuova SA di tipo dati. In generale è la SS che, utilizzando il *Messaggio2*, richiede i nuovi parametri per le SA. In questo messaggio sono specificati il SAID e l'HMAC. Il primo è l'identificativo di una particolare SA, prelevato dalla lista delle SAID. Il secondo provvede a garantire l'autenticità del messaggio di distribuzione della chiave dalla SS alla BS, in questo modo la BS riconosce se il messaggio è stato *falsificato*. Nel *Messaggio3* si possono osservare due chiavi di traffico: OldTek che NewTek. Questo perché la prima chiave sarà utilizzata prima della scadenza e, successivamente sarà impiegata l'altra. La chiave TEK è distribuita mediante KEK (Key Encryption Key), crittografata con Triple-DES a 112-bit. Una considerazione rilevante riguarda il *Messaggio2*. Il campo HMAC, spiegato in precedenza, è responsabile in questa procedura di verificare l'autenticità del client, da parte della BS. L'HMAC è costruito con una funzione di hash, e presuppone la conoscenza della chiave AK. Dunque la SS effettua il calcolo del HMAC, e lo invia alla BS. La BS, che conosce AK, esegue anch'essa il calcolo e verifica che l'HMAC, inviatole dalla SS, sia valido, quindi verifica l'integrità del messaggio, e considera il messaggio attendibile. Dunque i fattori critici, in questo meccanismo, riguardano la distribuzione e la conoscenza della chiave AK. Solo le due parti interessate, BS e SS, devono conoscerla.

2.7 Key Usage (considerazioni sull'utilizzo delle chiavi)

L'utilizzo delle chiavi AK (Authorization Key) e TEK (Traffic Encryption Key) impongono la definizione delle modalità di ottenimento, di rinfresco e di impiego. Questa sezione intende integrare e sintetizzare parte delle informazioni precedentemente trattate. In generale la BS è responsabile di mantenere le informazioni inerenti ad ogni SA, tra cui le chiavi utilizzate. Il protocollo PKM specifica le modalità di distribuzione e i meccanismi di sincronizzazione delle chiavi.

2.7.1 Authorization Key

Quando una BS riceve una richiesta di autorizzazione, si occupa di inizializzare due chiavi di autorizzazione, e ne attiva una. Questa, viene inviata alla SS, che la utilizzerà fino alla scadenza. La SS, prima che il tempo di vita della chiave corrente si esaurisca, effettua una nuova richiesta di re-autorizzazione alla BS. In risposta al messaggio, la base station, attiva la seconda chiave (che aveva precedentemente inizializzato) e la invia alla SS. Durante l'attivazione della seconda chiave, contestualmente, si ha la creazione di una terza chiave, che sarà attivata quando la SS ne farà richiesta. Quindi, la BS, conserva sempre due chiavi, di cui una attiva (quella corrente) e una pronta per essere attivata *su ordinazione*. Un aspetto rilevante di sicurezza riguarda la possibilità di attacchi di tipo replay. Per evitare questa situazione, la BS, assegna un numero di sequenza (campo SeqNo) a ogni AK, generato in ordine incrementale. Questo campo è presente nel *Messaggio3*, all'interno della procedura *SS Authorization*. La BS utilizza inoltre la chiave AK, per generare KEK, e verificare il digest HMAC, ottenuto dalla SS, tramite il messaggio di richiesta della chiave. L'utilizzo del KEK è necessario per crittografare il TEK, prima di inviarlo alla SS. Una volta ricevuta la chiave AK, la SS configura un *grace time*, che rappresenta il tempo di validità rimanente della chiave attualmente attiva. La configurazione di questo parametro, è soggetta ad alcune valutazioni, tra cui, i ritardi introdotti dai sistemi. Inoltre, il *grace time*, viene impostato esclusivamente sulla subscriber station. La stessa dovrà dunque effettuare una nuova richiesta, prima che il *grace time* si esaurisca.

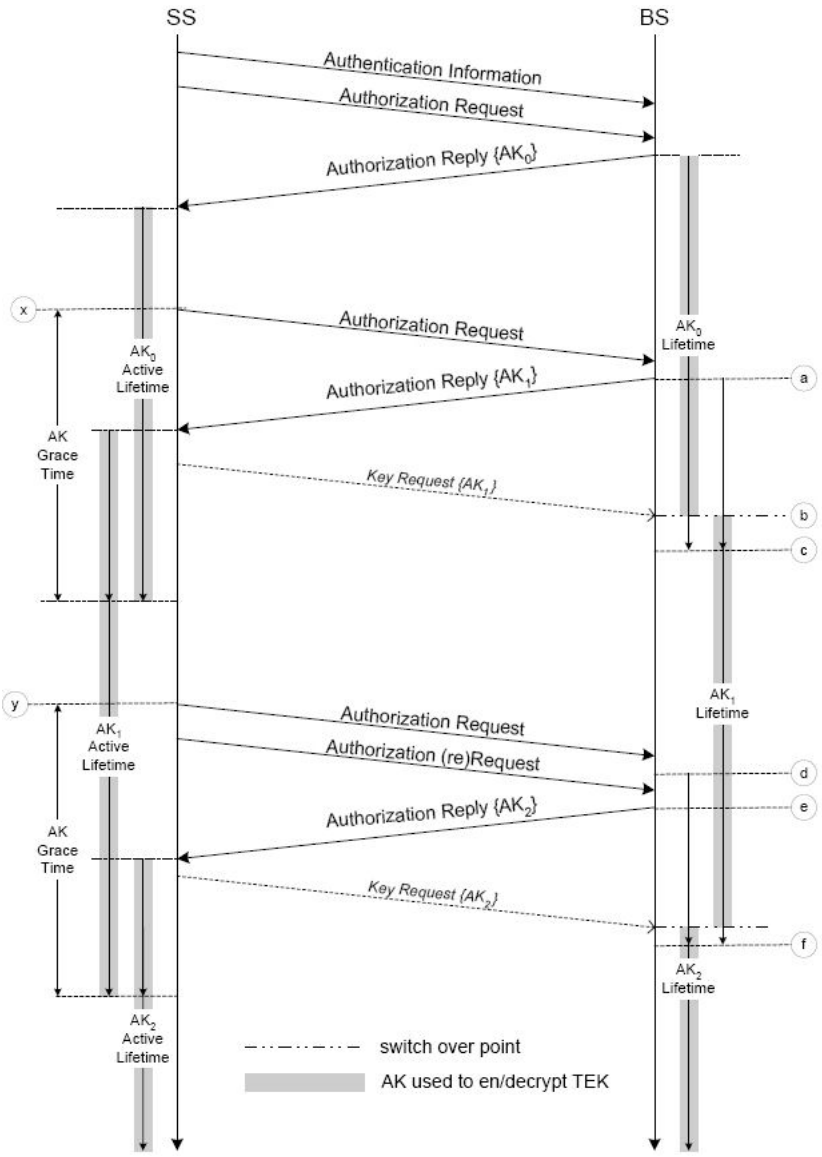

Figura 2.2. AK management, Rif.[1]

2.7.2 Traffic Encryption Key

La BS, genera due chiavi TEK per ogni security association (SA) e, quando la meno recente scade, provvede a generarne altre due. Per crittografare il canale in downlink, la BS utilizza la chiave meno recente, tra le due attive e, spesso, anche per decrittografare il canale in uplink (che contiene i dati provenienti dalla SS). Lo standard specifica che la SS, può utilizzare la chiave TEK più recente, per crittografare il traffico verso la BS (canale in uplink), invece dell'altra. Tuttavia, la BS, cambierà la chiave meno recente quando questa scadrà. Il compito di aggiornare le chiavi, è lasciato alla SS. La macchina a stati finiti, che implementa il TEK, innesca la nuova richiesta non

appena la chiave utilizzata è prossima alla scadenza. Anche in questo caso, in modo simile alla gestione della chiave AK, la SS genera un *grace time*. In generale, in prossimità della scadenza della chiave, la SS utilizza la chiave più recente per crittografare il traffico in uplink (verso la BS) e, la BS, per decrittografare il traffico in downlink, impiegherà quella meno recente.

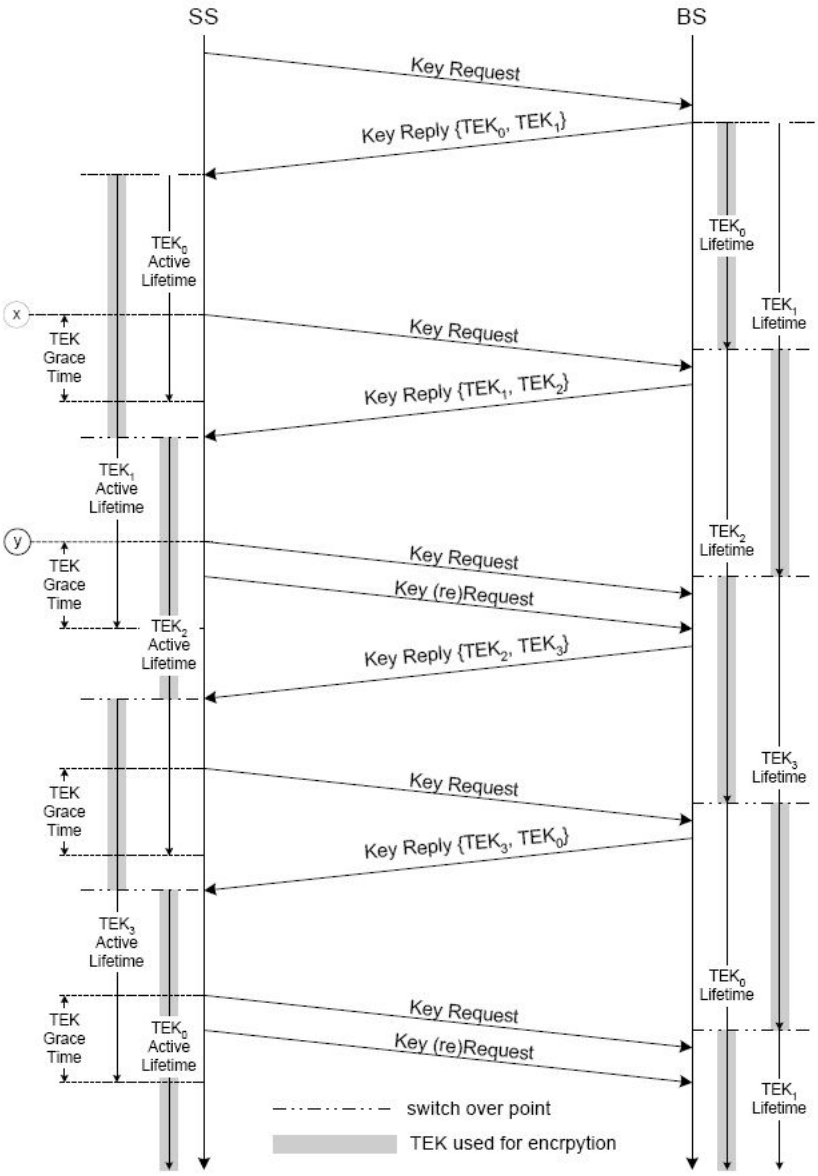

Figura 2.3. TEK management, Rif.[1]

2.8 Cryptography

Questa sezione descrive i metodi crittografici utilizzati dallo standard WiMAX, per quanto riguarda il protocollo PKM. Sia la SS che la BS, implementano i metodi necessari per:

- crittografia dei pacchetti dati
- AK

- TEK
- KEK
- message digest

Le chiavi AK e TEK sono costruire utilizzando un generatore casuale o pseudo casuale di numeri. La stessa modalità di generazione riguarda anche il vettore di inizializzazione (IV).

2.8.1 Crittografia dei pacchetti dati

Viene utilizzata, per crittografare i dati utente delle connessioni, secondo l'algoritmo specificato nel campo *data encryption algorithm*, della security association (SA). La crittografia è applicata solo al MAC PDU payload, mai al MAC Header. Per la crittografia dei pacchetti di dati sono definiti due algoritmi: DES CBC e AES CCM (introdotto nella versione 2004). L'algoritmo DES CBC, ormai considerato obsoleto, e sostituito da AES, deve essere inizializzato con un vettore detto IV (Initialization Vector). In downlink l'IV è inizializzato con:

`(IV del messaggio TEK)` $\oplus$ `(campo Synchronization in PHY dell'ultimo DL_MAP)`

In uplink con:

`(IV del messaggio TEK)` $\oplus$ `(campo Synchronization in PHY dell'ultimo UL_MAP)`

L'algoritmo AES utilizza lo standard NIST, e prevede una modalità diversa nella cifratura del payload. Viene introdotto un formato che prevede di aggiungere due elementi: uno in testa e l'altro in coda al payload. Quello in testa, denominato PN (Packet Number), è in chiaro e contiene su 4 byte il numero del pacchetto generato in ordine crescente. Quello in coda, denominato ICV (Integrity Check Value), permette di introdurre la funzionalità di integrità, espresso su 8 byte. Payload e ICV sono crittografati utilizzando la chiave TEK attiva. Questa modalità introduce una maggiore lunghezza nel pacchetto PDU di 12 byte. Quando l'SS o la BS, ricevono il pacchetto così costituito, valutano se sia integro e se l'ordine è corretto (se il PN del pacchetto è maggiore del valore registrato dalla stazione). Se almeno una delle due condizioni non è rispettata, il pacchetto dovrebbe essere scartato. L'utilizzo del PN è utile ad impedire attacchi di tipo replay, l'integrità permette invece di evitare attacchi di falsificazione dei pacchetti.

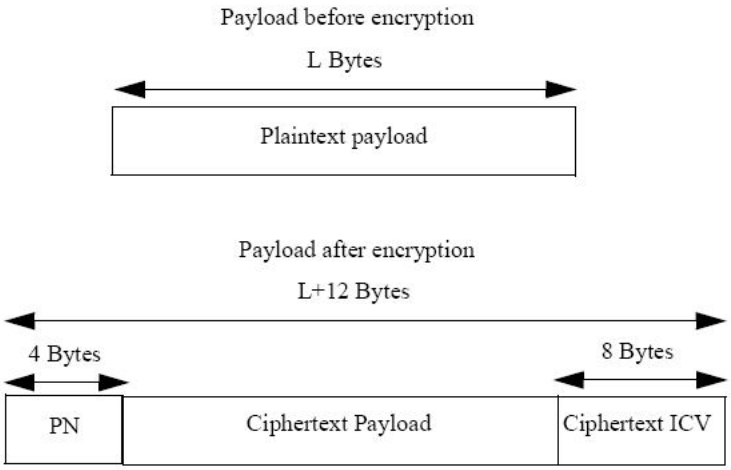

Figura 2.4. Formato del pacchetto PDU, Rif.[1]

2.8.2 AK(Authorization Key)

La chiave di autorizzazione AK, generata dalla BS e, inviata in risposta al messaggio di richiesta della SS, è generata in modo randomico o pseudo randomico. E' inoltre crittografata con l'algoritmo RSA e con la chiave pubblica della subscriber station.

2.8.3 TEK (Traffic Encryption Key)

La chiave TEK (Transport Encryption Key), per la crittografia del traffico, è generata in modo randomico o pseudo randomico e può essere protetta utilizzando tre diversi algoritmi di cifratura: Triple-DES, RSA e AES 128-bit. L'implementazione di default, prevede che il TEK, sia crittografato utilizzando l'algoritmo Triple-DES a 112 bit secondo il seguente schema:

```
C = Ek1[Dk2[Ek1[P]]]
P = Dk1[Ek2[Dk1[C]]]
```

Dove:
`P`: TEK in chiaro a 64 bit
`C`: TEK cifrato a 64 bit
`k1`: i 64 bit più significativi del KEK a 128 bit
`k2`: i 64 bit meno significativi del KEK a 128 bit
`E[]`: cifratura a 56 bit in modalità DES ECB
`D[]`: decifratura a 56 bit in modalità DES ECB
La crittografia, mediante algoritmo RSA, prevede l'utilizzo della versione 2 dello standard (PKCS #1 v2.0). Lo standard del 2004 non specifica ulteriori informazioni a riguardo.
L'utilizzo dell'algoritmo AES a 128-bit, prevede l'utilizzo in modalità ECB secondo il seguente schema:

```
C = Ek1[P]
P = Dk1[C]
```

Dove:
`P`: TEK in chiaro a 128 bit
`C`: TEK cifrato a 128 bit
`k1`: chiave KEK a 128 bit
`E[]`: cifratura a 128 bit in modalità AES ECB
`D[]`: decifratura a 128 bit in modalità AES ECB

2.8.4 KEK (Key Encryption Key)

La chiave Triple-DES KEK, derivata da AK, è utilizzata per cifrare il TEK. Lo schema per la costruzione della chiave KEK è il seguente:

$$\texttt{KEK = Truncate-128(SHA1((AK | } 0^{44}\texttt{)} \oplus 53^{64}\texttt{))}$$

Il KEK è costruito selezionando i primi 128 bit dell'espressione (`Truncate-128()`). Il simbolo `|` denota la concatenazione tra stringhe, il simbolo a^n denota che l'ottetto a è ripetuto n volte, `SHA1` un algoritmo di hash definito nel secure hash standard.

2.8.5 Message Digest

Il calcolo dei message digest, per la verifica dell'autenticità dei messaggi di aggiornamento e scambio delle chiavi TEK, inviati tra SS e BS, utilizza lo standard HMAC (IETF RFC 2104), con l'algoritmo di hash SHA1 (FIPS 180-1). Per verificare l'autenticità dei messaggi in downlink e in uplink sono necessarie due chiavi, dette rispettivamente `HMAC_KEY_D` e `HMAC_KEY_U`. Queste sono derivate da AK, e il numero di sequenza (SeqNo), è uguale a quello della chiave AK. In particolare, la costruzione delle chiavi è la seguente:

$$\texttt{HMAC\_KEY\_D: SHA1((AK | } 0^{44}\texttt{)} \oplus 3A^{64}\texttt{)}$$
$$\texttt{HMAC\_KEY\_U: SHA1((AK | } 0^{44}\texttt{)} \oplus 5C^{64}\texttt{)}$$

L'utilizzo di queste chiavi, è necessario per garantire che i messaggi scambiati tra BS e SS, siano autentici (integri), e che sia possibile verificarlo dalle stazioni, attraverso la conoscenza del segreto condiviso (AK) e il calcolo del digest. Senza questa precauzione si potrebbero sottoporre alle stazioni pacchetti alterati, falsificando la provenienza.

2.9 Considerazioni sulle funzionalità di sicurezza offerte

In sintesi, lo standard è abbastanza articolato ed impone alcune misure di sicurezza efficaci, tuttavia sono state riscontrate alcune vulnerabilità. Questa condizione si verifica per due ragioni: la notevole complessità del sistema che facilita i bug, inoltre alcune scelte effettuate in fase di progettazione si sono rivelate rischiose. (per es. l'uso di DES a 56-bit).

Capitolo 3

Vulnerabilità, attacchi e soluzioni

3.1 Introduzione

La tecnologia senza fili WiMAX, per la sua stessa natura, introduce problematiche di sicurezza maggiori rispetto a quelle wired. Lo standard che attualmente ha più analogie con l'802.16 è il Wi-Fi (802.11). La differenza sostanziale riguarda due aspetti: estensione del segnale e funzionalità di sicurezza. Il Wi-Fi, infatti, non è una tecnologia di accesso alla rete geografica ma locale, questo lo rende senz'altro meno flessibile, ma intrinsecamente più semplice da rendere sicuro, data la limitata estensione del segnale. Lo standard 802.16, già nelle prime versioni, incorpora soluzioni e funzionalità di sicurezza migliori del Wi-Fi, ma tuttavia insufficienti rispetto al bacino d'utenza. Innanzi tutto perché il segnale radio dell'802.16 si estende per diversi chilometri, invece di rimanere relativamente confinato in un edificio. Questo permette attacchi anche da punti fisicamente molto distanti e, in alcuni casi, l'individuazione può essere molto complessa, se non impossibile. Un altro problema, introdotto con l'approvazione dell'ultima versione dello standard, riguarda la mobilità delle stazioni (MS), per esempio durante l'handover tra le *celle* delle base station, dovendo mantenere le connessioni attive (possibili problemi nei messaggi di gestione, in quanto non protetti, oppure nel mantenimento di uno stato sicuro). L'introduzione del concetto di mobilità permette inoltre ad un attaccante di compiere un attacco in movimento, rendendo la sua individuazione fisica molto più complessa.

3.2 Tipologie di attacchi e considerazioni generali

Le tipologie di attacchi, valutati in questo documento sono:

- *DoS* (Denial of Service): interruzione del servizio, il sistema o il servizio non è più utilizzabile
- *Intercettazione* (Eavesdropping): accesso non autorizzato ad una risorsa del sistema o ad una comunicazione
- *Modifica/Cancellazione* (Tampering) (Man in the Middle) (Connection hijacking): intercettazione del contenuto di una comunicazione e modifica/cancellazione
- *Falsificazioni di credenziali* (Masquerade): si emettono o si ricevono messaggi sfruttando le credenziali di un altro utente, falsificando la propria identità

In oltre, gli attacchi si possono classificare in attivi e passivi. Gli attacchi passivi, sono quelli che riguardano l'intercettazione e l'analisi del traffico, con lo scopo di accedere alle informazioni. Gli attacchi attivi comportano la modifica del flusso di traffico e/o la generazione di un altro flusso. I più noti sono: DoS, Modifica/Cancellazione (Tampering) (Man in the Middle) (Connection hijacking), Falsificazioni di credenziali (Masquerade) e Replay. L'attacco di tipo replay, in generale, consiste nell'intercettazione di un pacchetto e nella successiva ritrasmissione verso la destinazione. Questo, è un attacco abbastanza comune, in quanto per evitarlo sono necessarie le seguenti condizioni: (1) autenticare la sorgente in modo sicuro (per. es. con una sfida), (2) aggiungere l'integrità al pacchetto, (3) numerare la sequenza dei pacchetti. La terza condizione è essenziale, in quanto la destinazione potrà verificare se ha già ricevuto il pacchetto. In questo caso, se il pacchetto fosse inviato una seconda volta, la stazione individuerebbe l'attacco, scartando il pacchetto. Si ricorda in oltre che, molto spesso, i bug possono costituire fonte di insicurezza nei sistemi (per es. buffer/stack overflow). Dato che l'assenza di bug nei sistemi è molto rara, se non impossibile, questo aspetto merita molta attenzione, soprattutto nella fase di progetto e d'implementazione, seguendo le diverse metodologie disponibili per limitarli al minimo. A volte anche l'impiego delle tecnologie e delle architetture di sicurezza più evolute, se non accompagnate da una corretta implementazione nel sistema, possono essere compromesse da attacchi relativamente semplici (per es. l'invio di alcuni pacchetti malformati). Un ulteriore aspetto, spesso sottovalutato, riguarda l'analisi e l'integrazione dei componenti di sicurezza. In particolare bisogna valutare per ogni componente l'impatto sugli aspetti della sicurezza che produce. Per esempio, potrebbe essere una buona soluzione sfruttare l'autenticazione di una sorgente mediante un certificato ed una sfida, tuttavia questo meccanismo garantisce che la sorgente sia autentica. Lo stesso, non si potrebbe dire per i dati, se non si introducessero meccanismi a protezione della loro integrità. L'analisi delle vulnerabilità, si concentra sul livello fisico e su quello MAC. In sintesi, nel primo non sono previsti meccanismi di sicurezza, mentre nel secondo, sono implementate all'interno di un sottolivello.

3.3 Livello fisico

A livello fisico, il flusso dei bit è strutturato in sequenze di frame di uguale lunghezza. Vi sono inoltre due sottoframe, uno per il flusso in downlink (dalla BS alla SS) e uno per l'uplink (dalla SS alla BS) e due modalità operative, TDD (Time Division Duplex) e FDD (Frequency Division Duplex). Nella modalità FDD i sottoframe sono simultanei ma non interferiscono, a causa della diversa frequenza utilizzata. Nella modalità TDD, i sottoframe sono consecutivi. Il livello fisico, non implementa nessuna funzionalità di protezione, ciò lo rende particolarmente insicuro. Le vulnerabilità di questo livello sono individuabili attraverso tre tipologie di attacchi possibili:

- *Water torture*
- *Jamming*
- *Scrambling*

3.3.1 Water Torture

Questa tipologia di attacco, prevede l'invio da parte dell'attaccante di una serie di frame, per scaricare le batterie della stazione ricevente. E' un attacco che prevede, in certe condizioni, l'interruzione del servizio alla stazione bersaglio. Essendo interessata solo la stazione bersaglio, l'impatto è abbastanza esiguo. Negli articoli analizzati sono presenti poche informazioni a riguardo.

3.3.2 Jamming

Questa tipologia di attacco, prevede l'introduzione di una sorgente di rumore sul canale, con l'obiettivo di diminuirne la capacità. E' chiaro che il rumore introdotto debba essere elevato, tale da provocare alterazioni. Lo scopo dell'attacco è diminuire o negare la comunicazione tra le parti coinvolte. L'articolo Rif.([5]) sostiene che l'attrezzatura necessaria per condurre un attacco di Jamming, sia abbastanza semplice da ottenere, e rimanda ad un libro, che tratta l'argomento in modo più approfondito. Considerando le informazioni disponibili, si può dedurre che la probabilità che si verifichi questa tipologia di attacco, sia piuttosto elevata. I possibili rimedi, consistono principalmente nell'aumentare la potenza dei segnali, oppure nell'aumentare la dimensione della banda dei segnali, utilizzando la tecnica di diffusione spettrale (Per es. FH - Frequency Hopping oppure DSSS - Direct Sequence Spread Spectrum). Le modalità per aumentare la potenza dei segnali sono molteplici, per esempio agendo sul guadagno, oppure sulle antenne in trasmissione e ricezione. L'attacco di jamming è facilmente individuabile utilizzando strumenti per monitorare lo spettro del segnale radio. Tuttavia, anche se il jamming presenta una elevata probabilità di verificarsi, l'impatto sui sistemi è basso in quanto può essere facilmente evitato o contrastato.

3.3.3 Scrambling

Lo scrambling, è una specie di jamming, ma agisce su periodi temporali minori, e riguarda frame specifici o parti di essi. Gli attaccanti, utilizzando questa tecnica possono selezionare alcuni messaggi di gestione (in quanto non protetti) e compromettere il normale funzionamento della rete. Il problema principale riguarda quei messaggi, che per natura non sono tolleranti ai ritardi, per esempio quelli che si occupano di effettuare misurazioni sul canale. Inoltre, l'attacco agli slot di traffico di specifici utenti porta alla loro ritrasmissione, con la conseguente diminuzione dell'ampiezza di banda. Si consideri, per esempio, il caso dei servizi VoIP, in cui il ritardo è un aspetto cruciale, l'attacco agli slot di traffico e la conseguente ritrasmissione possono compromettere la qualità del servizio, fino a renderlo inadeguato. Questa tecnica è più complessa da sfruttare, in quanto l'attaccante dovrebbe interpretare correttamente i messaggi di gestione ed agire inserendo un segnale di rumore, con tempistiche precise. La probabilità che si verifichi lo scrambling è dunque minore rispetto a quella del jamming, ma è più complesso individuare l'attacco. Questo è dovuto principalmente alla natura intermittente dell'attacco, che può essere scambiata per una naturale sorgente di rumore. Tuttavia, l'analisi delle anomalie, utilizzando criteri di prestazioni sul servizio offerto, possono rilevare questa tecnica. L'impatto, in generale, è abbastanza basso, in quanto la problematica potrebbe portare solo alla diminuzione del numero di utenti per cella. In sintesi, l'attacco di tipo jamming, è quello che presenta un maggior rischio e una maggiore probabilità di verificarsi. Una problematica, alla base di queste due tipologie di attacchi, riguarda la mancata protezione dei messaggi di gestione, sia dal punto di vista della riservatezza, che da quello dell'integrità. Questo permette ad un attaccante, che sia in possesso delle informazioni e dell'attrezzatura opportuna, di catturare frame dal canale, modificare parte di essi e ritrasmetterli. Un vincolo fondamentale da rispettare riguarda la scrittura sul canale, che non può essere impedita. E' dunque necessario prevedere meccanismi che possano proteggere anche i messaggi in chiaro. Le tecniche che si potrebbero utilizzare dovrebbero focalizzarsi sull'autenticazione, sull'integrità, ed evitare attacchi di tipo replay. Queste modifiche porterebbero inevitabilmente ad un aumento dei dati trasmessi, ma considerando le capacità di calcolo disponibili, per esempio come sistemi crittografici realizzati in hardware (microprocessori crittografici), la soluzione, almeno in linea di principio sarebbe auspicabile ed adottabile.

3.4 Livello MAC

Nel sottolivello *security* del MAC è presente l'implementazione delle funzionalità e dei meccanismi di sicurezza, discusse nel capitolo precedente. La valutazione delle minacce e delle vulnerabilità si basa sull'analisi degli aspetti della confidenzialità, dell'autenticazione e dell'integrità. Come trattato in precedenza, il pacchetto MAC, detto PDU, è composto da un header (trasmesso in chiaro), un payload e un CRC opzionale. Il payload contiene il traffico utente, l'header contiene, tra le varie informazioni, un flag che specifica se il payload è crittografato. In ogni caso, l'header è sempre trasmesso in chiaro, così come i messaggi di gestione a livello MAC. Questa scelta è giustificata dal fatto di voler semplificare le operazioni del livello, nella gestione dei pacchetti. In particolare, sono individuabili alcune vulnerabilità, all'interno dei seguenti meccanismi di sicurezza:

- Security Association
- PKM (Privacy and Key Management)
- Key Usage
- Cryptography

3.4.1 Vulnerabilità nelle Security Association

Il compito della SA authorization è quello di autorizzare una comunicazione tra SS e BS, mediante la chiave segreta AK. Il problema principale è la mancanza di un campo che identifichi una istanza di SA authorization da un'altra. Questa vulnerabilità si traduce nella possibilità di incorrere in attacchi di tipo replay. In questo attacco, si potrebbe riutilizzare una SA authorization, intercettata in precedenza. Le vulnerabilità all'interno della SA authorization possono generare ulteriori problemi alle SA di dati, in quanto è possibile riutilizzare anche questa senza che la SS se ne accorga. Inoltre, date queste considerazioni, lo schema di crittografia diventa quindi vulnerabile agli attacchi che sfruttano il riutilizzo della chiave (mediante le tecniche di crittanalisi di dati crittografati). Le criticità degli attacchi di tipo replay e di falsificazione possono essere risolte attraverso alcuni meccanismi. Il modo migliore per correggere le vulnerabilità agli attacchi di tipo replay consiste nell'introdurre un numero, generato in modo casuale, nell'SA authorization tra base station e subscriber station. Inoltre, il campo (a 2-bit) che identifica il TEK, limita notevolmente il numero di chiavi di traffico utilizzabili, tanto da essere soggetto ad attacchi d'intercettazione. Dato che il tempo di vita della chiave AK, può arrivare fino a 70 giorni, è necessario poter variare molto spesso la chiave TEK, identificandola ogni volta con un valore diverso. Si rende quindi necessario, aumentare la dimensione del campo che identifica la chiave TEK da 2-bit ad almeno 12-bit. (Rif.[4]) Il rischio non è molto elevato, in quanto, se le chiavi TEK venissero cambiate spesso non si avrebbero problemi di crittanalisi sui dati. Il rischio per l'attacco di tipo replay è più elevato, perché mancano le informazioni che discriminano una istanza di SA da un'altra. L'impatto delle due tipologie di attacco è piuttosto elevato, in quanto, nel primo caso non sarà rispettata la proprietà di riservatezza. Nel secondo caso, l'attacco di tipo replay non permette al sistema di rilevare un messaggio già ricevuto da un altro.

3.4.2 Vulnerabilità nell' autenticazione semplice

La seconda problematica riscontrata riguarda la mancata identificazione della BS da parte della SS. In questo modo, la SS non può distinguere una base station autorizzata da una non autorizzata, favorendo attacchi sia di falsificazione (dell'identità della BS) che di replay (riutilizzo di messaggi). Consideriamo per esempio il caso in cui, una BS non autorizzata, possa posizionarsi fisicamente

tra una SS e una BS autorizzata. In questo caso, la BS potrebbe catturare il traffico, modificarne parte di esso (falsificandolo) e instradarlo verso la SS. Potrebbe anche effettuare attacchi di replay sempre verso la SS. Il meccanismo di autenticazione semplice della SS verso la BS, è uno dei maggiori difetti per quanto riguarda l'aspetto della sicurezza. Questa problematica è risolvibile introducendo lo schema di mutua autenticazione tra subscriber station e base station. Senza questa rettifica non è possibile difendere il sistema da attacchi di falsificazione e di replay. La vulnerabilità dell'autenticazione si riflettono anche sul protocollo di gestione della riservatezza e delle chiavi (PKM), rendendolo oggetto di possibili attacchi di falsificazione. In questa tipologia di attacco, la SS non può verificare che i messaggi del protocollo PKM provengano da una fonte autorizzata. Infatti la BS costruisce i messaggi da inviare alla SS utilizzando informazioni pubbliche, e quindi qualsiasi base station non autorizzata potrebbe fare altrettanto. Richiedendo alla SS di autorizzare la BS si elimina il problema. La seconda tipologia di attacco riguarda il replay, ovvero la cattura di un messaggio e la sua ritrasmissione verso un destinatario. La soluzione consiste nell'introdurre, da parte della SS, nel *Messaggio2*, dell'authorization protocol, una sfida generata casualmente, a cui la BS risponderà nel *Messaggio3*, inserendo la risposta alla sfida e firmando, con la sua chiave privata, il messaggio. In questo modo la SS, verificando la firma inviata e la risposta alla sfida, stabilisce l'identità della BS. L'attacco che sfrutta l'autenticazione semplice, per introdurre una BS non autorizzata, non è molto semplice da portare a termine. In generale la falsa BS deve essere in grado di trasmettere al momento opportuno, e sovrastare il segnale della BS autentica. In particolare, l'attaccante deve preoccuparsi che il segnale generato arrivi al bersaglio con una potenza maggiore rispetto alla BS autentica. In questo modo, la SS attaccata, sceglierà il segnale a potenza maggiore. Il rischio dunque non è molto elevato, l'impatto tuttavia potrebbe essere maggiore, in quanto potrebbe coinvolgere un certo numero di utenti che si servono di una BS. Tuttavia, dato che la BS non autorizzata, deve sovrastare la potenza del segnale di quella autorizzata, la zona coperta (dalla BS non autorizzata) sarà minore e così il numero degli utenti coinvolti. Correlato al caso precedente, vi è il problema di distinguere, da parte degli utenti, un'istanza del protocollo rispetto ad un'altra, soprattutto in caso di supporto alla mobilità. Per esempio, un utente con un terminale mobile che transita da una zona coperta da una base station ad un'altra, deve poterle distinguere. La soluzione (Rif.[4]) a questo caso si ottiene introducendo una struttura dati opportuna, forma da quattro elementi:

- identità della BS (certificata)
- identità della SS (certificata)
- numero generato casualmente e pubblico della BS per una certa istanza
- numero generato casualmente e pubblico della SS per la medesima istanza

Utilizzando queste informazioni, gli utenti possono legare le istanze del protocollo di gestione delle chiavi alle istanze delle autorizzazioni. Lo standard assume inoltre che, associato ad un indirizzo MAC, esista una sola coppia di chiavi pubblica e privata. Questa situazione deve essere comunque verificata, altrimenti qualche entità del sistema potrebbe sostituirsi ad un'altra.

3.4.3 Vulnerabilità generiche associate a messaggi di autenticazione e autorizzazione

Vi sono alcune vulnerabilità associate alle procedure ed ai messaggi di autenticazione e autorizzazione. La macchina a stati, che implementa l'autenticazione e l'autorizzazione, contiene procedure abbastanza lunghe e complesse. L'inondazione con messaggi di autenticazione, non correttamente gestiti, potrebbe avere come risultato l'interruzione del servizio. (DoS - Denial of Service) (Rif.[5]).

Il rischio di questo attacco non sembra perché presuppone di conoscere a fondo le possibili problematiche legate alla macchina a stati. Se l'attacco fosse diretto ad una BS, l'impatto potrebbe essere abbastanza rilevante, ma il sistema intero non può essere compromesso.

3.4.4 Vulnerabilità nella generazione della chiave AK

Tra le funzionalità di crittografia, vi è quella che provvede alla generazione della chiave di autorizzazione, Authorization Key (AK). Lo standard non provvede a specificare nessuna procedura particolare, e non pone il vincolo di rispettare particolari requisiti. Tuttavia sarebbe necessario almeno imporre la generazione casuale della chiave, e imporre la selezione, considerando una distribuzione di probabilità uniforme per tutti i 160-bit. Un'altra possibile debolezza riguarda le entità coinvolte nella generazione della chiave. In particolare la chiave AK, attualmente viene generata esclusivamente dalla BS. Questa modalità, per ritenersi abbastanza sicura, dovrebbe rispettare due condizioni:

- l'identità della BS dovrebbe essere certificata (dalla SS)
- il generatore casuale presente nella BS dovrebbe essere implementato correttamente, in modo che le diverse AK generate, non siano correlate tra loro

L'implementazione di un generatore casuale non è semplice, tanto che, in alcuni casi, è possibile individuare parte della chiave utilizzando metodi di crittanalisi semplici. Ciò è dovuto al fatto che parte della chiave potrebbe essere fissa o calcolabile con parametri pubblici. Per migliorare la variabilità delle chiavi, e diminuire il rischio connesso alla generazione da parte di una sola entità, sia la BS che la SS dovrebbero partecipare con alcuni bit alla sua costruzione. Per esempio, una possibile formazione della chiave, potrebbe essere il risultato di un digest, costruito con alcuni bit proposti dalla BS e gli altri dalla SS:

3.4.5 Vulnerabilità nella generazione della chiave TEK

La prima problematica della chiave TEK, contenuta nella Security Association (SA) e accennata in precedenza, riguarda il tempo di vita. Per default, è pari a 12 ore e la durata massima è 7 giorni. Quest'ultimo valore, potrebbe essere troppo elevato in quanto, in presenza di traffico sostenuto, crittografato sempre con la medesima chiave, sarebbe possibile effettuare attacchi di crittanalisi, disponendo di diverso testo cifrato. La disponibilità di testo cifrato con una certa chiave è legata al massimo numero di messaggi TEK diversi utilizzabili. Questo numero è espresso dal sequence number; maggiore è la dimensione del campo SeqNo e minore sarà la probabilità di una sua ripetizione all'interno del tempo di vita della chiave. Inoltre, la chiave TEK, utilizzata per crittografare il traffico, soffre di un ulteriori problematiche legate alla sua generazione. Innanzi tutto è costruita da un generatore casuale, e se questo non fosse implementato in modo adeguato potrebbe essere affetta dagli stessi problemi di AK. Anche in questo caso è necessario che la chiave sia generata secondo una distribuzione di probabilità, quanto più uniforme possibile. Le vulnerabilità nella generazione di AK e TEK, si trasformano in possibili attacchi di crittanalisi. Il rischio associato non è molto elevato, perché sarebbe necessario intercettare una notevole quantità di traffico crittografato. L'impatto invece, potrebbe essere elevato, in quanto ottenendo le chiavi sarebbe possibile decrittografare i dati e violare la proprietà di riservatezza. Tuttavia, questo potrebbe riguardare un limitato numero di utenti.

3.4.6 Vulnerabilità nella crittografia dei dati

Lo standard 802.16 del 2001 proponeva, come algoritmo per crittografare i dati, il DES a 56-bit, oggi considerato debole. I principali difetti, sono: la lunghezza della chiave e la prevedibilità nella costruzione del vettore d'inizializzazione dello schema proposto dallo standard. La rettifica, avvenuta nello standard del 2004, introduce l'algoritmo AES CCM, evitando così ulteriori vulnerabilità. Per ulteriori dettagli sull'impiego di AES CCM, si rimanda al capitolo precedente. Anche in questo caso, soprattutto con l'algoritmo DES, è possibile sfruttare attacchi di crittanalisi e violare la proprietà di riservatezza. In oltre il pacchetto MAC PDU, costruito con l'algoritmo AES CCM contiene un campo per verificare l'integrità dei dati, meccanismo non implementato nello standard del 2001. Questa condizione aggiunge una vulnerabilità che, permette la modifica dei dati e quindi i relativi attacchi (Tampering). Il rischio in presenza dell'uso di DES è senz'altro più elevato rispetto all'uso di AES CCM. L'impatto tuttavia, non è molto elevato perché potrebbe riguardare un limitato numero di utenti.

3.5 Nuovi meccanismi di sicurezza

Negli ultimi standard approvati, successivi al 2004, e in quelli in corso di approvazione, sono stati introdotti alcuni miglioramenti nei meccanismi di sicurezza, in particolare:

- Utilizzo di AES CCM (dalla versione 2004, già approfondita in precedenza)
- Introduzione di EAP come ulteriore schema di autenticazione
- Miglioramento nelle specifiche delle security association (SA) (approfondite in precedenza)
- Miglioramenti nella gestione delle chiavi
- Ottimizzazione delle procedure di re-autenticazione in caso di dispositivi mobili

3.5.1 Autenticazione mediante protocollo EAP

Innanzi tutto EAP (Extensible Authentication Protocol) è un protocollo di tipo generale per l'autenticazione, che supporta diversi metodi diversi, ed è un'estensione di PPP. Non è un meccanismo ma una piattaforma di autenticazione (authentication framework) a livello data-link. L'utilizzo del protocollo EAP (Extensible Authentication Protocol) consente di introdurre uno schema più flessibile di autenticazione. L'approccio dominante è quello di inserire i messaggi EAP all'interno dei frame di gestione, permettendo l'autenticazione nella fase di instaurazione del collegamento. A questo proposito lo standard inserisce due primitive nel protocollo PKM:

- PKM-EAP-REQ
- PKM-EAP-RSP

E' importante osservare che lo standard non definisce ancora il metodo di autenticazione utilizzato, in quanto ancora in fase di ricerca.

3.5.2 Miglioramenti nella gestione delle chiavi

Per quanto riguarda l'aspetto della gestione delle chiavi, lo standard del 2004 non specifica cambiamenti rispetto a quello del 2001. Tuttavia, l'articolo (Rif.[4]), propone due migliorie: una per quanto riguarda l'autorizzazione e l'altra riguardo allo scambio delle chiavi TEK. La prima, quella di autorizzazione, introduce la sequenza:

```
Messaggio1: (AI) : SS -> BS : Cert(Manufacturer(SS))
Messaggio2: (Areq) : SS -> BS : SS-Rand | Cert(SS) |
capabilities | CID
Messaggio3: (Arep) : BS -> SS : BS-Rand | SS-Rand |
RSA-Encrypt(PubKey(SS), AK) | AK lifetime |
SeqNo (4-bit) | SAIDs | Cert(BS) | Sign(BS)
```

E calcolando AK utilizzando un digest, nel seguente modo:

```
AK = HMAC-SHA1(pre-AK, SS-Rand | BS-Rand | SS-MAC-Addr | BS-MAC-Addr)
```

La nuova chiave AK, si basa su quella generata dalla BS precedentemente (pre-AK), da due numeri casuali generati da BS e SS, e dai rispettivi MAC address. La lunghezza, rimane pari a 160-bit. La seconda, quella che riguarda lo scambio delle chiavi TEK, modifica la sequenza in:

```
Messaggio1: BS -> SS : SS-Rand | BS-Rand | SeqNo12 |
SAID | HMAC(1)
Messaggio2: SS -> BS : SS-Rand | BS-Rand | SeqNo12 |
SAID | HMAC(2)
Messaggio3: BS -> SS : SS-Rand | BS-Rand | SeqNo12 |
SAID | OldTek | NewTek | HMAC(3)
```

Questa nuova sequenza introduce, oltre che ai numeri generati casualmente dalla BS e dalla SS, un nuovo numero di sequenza, espresso su 12 bit. L'introduzione di queste modifiche permette di associare i messaggi a determinate connessioni e numeri di sequenza, evitando attacchi di tipo replay e crittanalisi. La nuova chiave TEK viene generata in questo modo:

```
TEK = HMAC-SHA1(pre-TEK, SS-Rand | BS-Rand | SS-MAC-Addr | BS-MAC-Addr | SeqNo12)
```

Mantenendo la lunghezza precedente di 160-bit.
Si può osservare che l'algoritmo SHA1 è stato sostituito con HMAC-SHA1 per evitare attacchi alla funzione di hash. Questa operazione si rende necessaria in seguito alla scoperta di alcune vulnerabilità, annunciate da alcuni ricercatori cinesi della *Shandong Univerity* e, successivamente pubblicate nel blog di *Bruce Schneier* (Rif.[9]).

3.5.3 Ottimizzazione delle procedure di re-autenticazione per la mobilità

Come accennato in precedenza, l'operazione di autenticazione coinvolge una macchina a stati ed è particolarmente costosa. Considerando uno scenario che permetta ai terminali la mobilità, il conseguente spostamento fisico da una zona di copertura di una BS ad un'altra è inevitabile. Questa situazione, soprattutto in presenza di servizi vocali (come VoIP), impone dei vincoli temporali sulle procedure di handover (passaggio da una cella ad un'altra, problematica simile alle reti cellulari) che coinvolgono anche l'autenticazione. L'impiego durante il passaggio da una BS ad un'altra, delle stesse chiavi AK e TEK, è molto rischioso dal punto di vista della sicurezza, anche se è la soluzione più semplice. Scegliendo questa modalità, compromettendo una BS si potrebbero compromettere altre BS e quindi, teoricamente il sistema intero. E' dunque necessario considerare algoritmi efficienti ma allo stesso tempo sicuri, ovvero che permettano una sorta di re-autenticazione durante la fase di transizione. Attualmente questi sono ancora in fase di studio.

Capitolo 4

Considerazioni finali

In questo documento, sono stati trattati tre aspetti della tecnologia WiMAX: il funzionamento, i meccanismi di sicurezza e le vulnerabilità note. Per quanto riguarda l'aspetto del funzionamento e, degli scopi della tecnologia, possiamo concludere che il WiMAX potrà essere utile specialmente in due circostanze: (1) raggiungere zone ove i costi del cablaggio fisico sono proibitivi oppure è impossibile per la morfologia del territorio; (2) servizi d'accesso in condizioni di emergenza, in zone non coperte dal servizio, oppure dove i servizi di TLC principali non sono più utilizzabili (per es. in caso di catastrofi naturali). L'aspetto che tratta le funzionalità e i meccanismi di sicurezza, compie un'analisi abbastanza specifica sulle modalità di implementazione, descritte negli standard considerati: del 2001 e del 2004. Una considerazione piuttosto generale, riguarda i meccanismi di sicurezza offerti dal WiMAX rispetto al Wi-Fi. I miglioramenti sono senz'altro notevoli, soprattutto per quanto riguarda gli aspetti di autenticazione, crittografia dei dati e scambio delle chiavi. Tuttavia, mettendo in relazione queste due tecnologie per quanto riguarda gli aspetti di copertura del segnale, si evince che il WiMAX dovrebbe implementare meccanismi di sicurezza più efficaci. Ciò perché si rivolge ad un bacino d'utenza decisamente maggiore, di conseguenza la probabilità di attacchi è maggiore. Le vulnerabilità rilevate non sono poche, alcune di esse, sono già state affrontate negli standard successivi, già approvati o in corso di approvazione. Si conclude che, questa analisi non è aggiornata agli ultimi standard a causa della indisponibilità per il pubblico. Tuttavia, anche gli articoli più recenti analizzati evidenziano ancora vulnerabilità di sicurezza. In sintesi, la tecnologia WiMAX si propone come valida alternativa per risolvere il problema dell'accesso a banda larga, soprattutto nelle zone che, con le tecnologie attuali, difficilmente potranno essere raggiunte. Per facilitare l'introduzione e la diffusione della tecnologia è necessario garantire le classiche proprietà di sicurezza, ricordate in precedenza, effettuando alcune modifiche nei meccanismi.

Bibliografia

[1] IEEE 802.16 Broadband Wireless Access Working Group, *Air Interface for Fixed Broadband Wireless Access Systems*, 2004.

[2] IEEE 802.16 Broadband Wireless Access Working Group, *IEEE Standard 802.16: A Technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access*, 2001.

[3] Edward Grabianowski, Marshall Brain, *How WiMAX Works*, sito web: computer.howstuffworks.com/wimax.htm/printable.

[4] Intel, *Overview of IEEE 802.16 Security*, 2004.

[5] Michel Barbeau, *WiMAX/802.16 Threat Analysis*, 2005.

[6] Jagannath, *Wireless Security - 802.16*, 2005.

[7] www.wimax.com, *WiMAX Faq*.

[8] Marco Listanti, *Aspetti di sicurezza nelle reti TLC*, 2005/2006.

[9] Antonio Lioy, *Introduzione alla sicurezza delle reti e dei sistemi informativi*, 2005.