Introduzione

Questa tesi sarà organizzata in quattro capitoli dedicati interamente al WiMAX (Worldwide Interoperability for Microwave Access). Nel primo capitolo illustrerò i concetti generali della tecnologia, la sua evoluzione, i suoi vantaggi. Nel secondo capitolo parlerò dell'architettura protocollare dell'802.16 e di come il WiMAX implementa la sicurezza. Tratterò le vulnerabilità presenti nel WiMAX e come lo standard evolvendosi ha risolto alcune debolezze. Nel terzo capitolo parlerò di come il protocollo 802.1X può essere utilizzato per migliorare la sicurezza della tecnologia WiMAX e di come ho implementato nel laboratorio di telecomunicazioni del DEIS una piccola rete per testare il funzionamento reale del protocollo 802.1X. Nel quarto capitolo spiegherò come ho realizzato l'infrastruttura di rete che mi ha permesso di analizzare le performance di una rete WiMAX.
Nei paragrafi successivi evidenzierò i punti salienti di ogni capitolo per una piccola anteprima dei concetti che svilupperò ed amplierò nel mio percorso di tesi.

Capitolo 1: Introduzione al WiMAX

Il WiMAX è il nome commerciale dello standard IEEE 802.16, uno standard iniziato nel 1998 dal National Institute of Standards and Technologies e trasferito successivamente all'IEEE. Negli ultimi anni, la grandissima diffusione di Internet, ha fatto si che aumentasse sempre più la richiesta di servizi per l'accesso ad Internet ad alta velocità. In poco tempo, nel mondo, le sottoscrizioni a banda larga sono letteralmente esplose. Sarà possibile combinare la convenienza del wireless con le ottime performance della banda larga? Questo è l'obiettivo del WiMAX, la cui intenzione è quella di fornire l'accesso wireless a banda larga su scala MAN, Metropolitan Area Network, e di soppiantare gli attuali sistemi di accesso a banda larga come la *DSL (Digital subscriber line)*. L'accesso wireless a banda larga offre convenienza e semplicità. Non ha bisogno di cavi e questo gli permette di arrivare anche in quelle zone rurali dove la dorsale in cavo è difficile da impiantare. Lo standard 802.16 è stato progettato per supportare sia il *fixed wireless broadband* che offre servizi simili alle tradizionali DSL, sia il *mobile broadband* che aggiunge la portabilità e la mobilità, dando ai notebook ed ai telefonini l'accesso diretto ad Internet anche in movimento. La

tecnologia supporta velocità di trasmissione di dati condivisi fino a 70 Mbit/s in aree metropolitane. Non richiede necessariamente visibilità ottica diretta LOS (Line of Sight), ma senza di essa, cioè con la presenza sul territorio di ostruzioni, si passa alla modalità di propagazione NLOS (not line of sight) e le prestazioni sono decisamente inferiori. Un sistema WiMAX consiste di due componenti fondamentali:

- una **Stazione Base** (BS - Base Station). La BS è l'entità che implementa le caratteristiche PHY e MAC definite dallo standard.
- **un ricevitore WiMAX.** È un sistema radio che comunica con una Base Station. Può essere stazionario ed in questo caso viene chiamato Subscriber Station o SS, oppure mobile(un notebook, un cellulare) ed in questo caso parliamo di una Mobile Station o MS.

Il WiMAX non si presenta come un'alternativa al WiFi, ma, anzi, si pone in collaborazione con esso, fornendo agli hotspot wifi l'accesso ad Internet.

Capitolo 2: I livelli Fisico, MAC e la sicurezza nella tecnologia WiMAX

Lo standard IEEE 802.16 implementa solo due livelli del modello OSI: il livello fisico ed il livello Medium Access Control (MAC).

Il livello PHY stabilisce la connessione fisica tra le due parti, spesso in tutte e due le direzioni (uplink e downlink). Dato che l'802.16 è evidentemente una tecnologia digitale, lo strato fisico è responsabile della trasmissione delle sequenze di bit. Esso definisce il tipo di segnale utilizzato, il tipo di modulazione e demodulazione, la potenza di trasmissione e tante altre caratteristiche fisiche.

Il MAC del WiMAX supporta in primo luogo un'architettura punto-multipunto(PMP) ed opzionalmente una topologia mesh. È strutturato in modo tale da supportare molti strati fisici (PHY), ma in realtà, solo due di essi sono utilizzati: l'OFDM e l'OFDMA. Il MAC fornisce i servizi di accesso al mezzo, di autenticazione ed associazione alla rete, di frammentazione e riassemblaggio dei pacchetti e di Quality of Service (QoS). Comprende tre sottolivelli: Il Sottolivello di Convergenza di Servizio Specifico (CS), Sottolivello MAC a Parte Comune (MAC CPS), Sottolivello di Privacy (Privacy Sublayer). Il MAC CS si occupa di accettare protocolli dai livelli superiori (Livello 3), per poi processarli, classificarli e garantire un'adeguata trasmissione/ricezione verso i CS di altre unità. Il MAC CPS garantisce l'accesso al sistema, l'allocazione della banda

e l'instaurazione e la manutenzione della connessione. Il WiMAX, a differenza del WiFi, è stato progettato con la sicurezza in mente, sin dall'inizio. L'autenticazione, la crittografia e lo scambio delle chiavi, infatti, sono in carico del Sottolivello di Privacy, un sottolivello per la sicurezza apposito. Il sottostrato di sicurezza utilizza due protocolli: (a) un protocollo di incapsulamento per la crittografia dei pacchetti di dati attraverso la rete 802.16.(b) il protocollo PKM(Privacy and Key Management) per la distribuzione sicura delle chiavi di negoziazione tra la Base Station e la Subscriber Station. L'intero meccanismo di sicurezza della tecnologia WiMAX è definito dalle SA (Security Association) composte da un insieme di parametri di sicurezza per la protezione dei dati e della trasmissione, dai certificati X.509, dall'autorizzazione PKM e dalla crittografia dei dati e delle chiavi di gestione. Le comunicazioni WiMAX, seguono una procedura di sicurezza in tre fasi. Nella **prima fase** la SS si identifica con la BS. Se le credenziali sono accettate la BS autorizza la SS all'uso dei link cifrati di uplink e downlink e le invia una specifica chiave di autorizzazione, l'Authorization Key (AK). Nella **seconda fase** avviene lo scambio delle chiavi TEK(Traffic encryption key), le chiavi necessarie alla crittografia dei dati. Dall'AK la SS ricava altre tre chiavi: la KEK(Key Encryption Key) per la crittografia delle chiavi TEK, una chiave per criptare i messaggi di gestione della BS verso la SS ed un'ultima chiave per l'oscuramento dei messaggi di gestione della SS verso la BS. Nella **terza fase** inizia lo scambio dei dati tra la BS e la SS. Per garantire la confidenzialità dei dati, viene utilizzata la chiave TEK per la crittografia, ed uno specifico algoritmo di cifratura (es. AES) per l'oscuramento dei dati.

Il primo standard, l'IEEE 802.16-2004 e la prima versione del PKM non erano molto sicuri. Presentavano molte vulnerabilità. Tre di esse, però, meritano un'attenzione particolare.

L'autenticazione unilaterale della SS verso la BS. La Subscriber Station non aveva nessuna possibilità di verificare l'identità della BS. Questo poteva portare al furto dei dati, ad attacchi DoS e man-in-the-middle.

Le debolezze dell'algoritmo DES-CBC. Questo è un algoritmo di cifratura debole che non assicura la confidenzialità dei dati.

Riuso delle chiavi TEK. L'identificatore della chiave TEK a 2 bit consente solo quattro valori rendendo il sistema vulnerabile. Un malintenzionato potrebbe riutilizzare chiavi TEK scadute ed effettuare attacchi di tipo replay rubando le informazioni di un ignaro utente.

Il PKM v2 e lo standard 802.16e-2005 hanno risolto molti dei problemi dello standard precedente. Hanno introdotto l'autenticazione mutuale basata su EAP: anche la BS si deve identificare con la SS, una varietà di nuovi algoritmi di crittografia molto più robusti e la numerazione dei pacchetti per evitare gli attacchi di tipo replay. Nonostante questo enorme passo in avanti, nemmeno le versioni più recenti dello standard sono immuni agli attacchi e presentano alcune vulnerabilità. Per esempio:

Messaggi di gestione non crittografati. Per facilitare l'entrata iniziale nella rete, la registrazione dei nodi e l'allocazione della banda, le BS e le SS comunicano usando messaggi di gestione non cifrati. Questi messaggi sono soggetti ad intercettazione, attacchi di tipo replay, attacchi scrambling e manipolazioni subdole volte a declassare il servizio. Se non viene utilizzato l'AES-CCM, una rete WiMAX rimane vulnerabile agli attacchi man-in-the-middle.

Uso del wireless come mezzo di trasmissione. Possono essere eseguiti attacchi DoS con l'introduzione di una potente sorgente radio intesa a sopraffare lo spettro del sistema radio.

Capitolo 3: Rendere più sicura una rete WiMax: il protocollo 802.1X

L'implementazione dell'accesso port-based dell'802.1x e quindi l'autenticazione degli utenti prima di entrare in una rete, costituisce un grande passo in avanti verso la messa in sicurezza delle reti wired e wireless. **L'IEEE 802.1x** è uno standard IEEE basato sul controllo delle porte di accesso alla rete. Questo standard provvede a autenticare e autorizzare i dispositivi collegati alle porte della rete (switch e access point) stabilendo un collegamento punto a punto e prevenendo collegamenti non autorizzati alla rete locale. Si basa sul protocollo EAP, Extensible Authentication Protocol. L'IEEE 802.1X determina i tre ruoli coinvolti nell'autenticazione: un supplicant che è il cliente 802.1x (un PC per esempio), un authenticator che può essere uno switch, un Access Point o come nel mio caso una Base Station e l'authentication server che è il server AAA (Authentication, Authorization, Accounting), tipicamente un server RADIUS(Remote Authentication Dial In User Service). Il RADIUS rappresenta uno degli strumenti più efficaci nell'autenticazione delle reti. Un supplicant è un dispositivo client che deve essere autenticato prima di avere accesso alla rete. È un utente non ancora riconosciuto. La sua identità è in questione fino a quando presenta

valide credenziali al server di autenticazione. Una volta che il sistema verifica il supplicant, l'autenticatore aprirà una porta e il client la userà per accedere alla rete protetta. Lo standard 802.1x crea dunque due distinti punti di accesso. Un punto d'accesso permette lo scambio non controllato (uncontrolled) di PDU tra un client e gli altri dispositivi della rete senza badare allo stato di autenticazione (uncontrolled port); l'altro punto di accesso permette lo scambio di PDU solo se lo stato della porta è Autorizzato (controlled Port). L'autenticazione quindi fornisce due grandissimi benefici. Dà la possibilità al service provider di identificare gli utenti e di permettere l'accesso alla rete solo al personale autorizzato. Offre inoltre agli utenti la certezza che sono connessi alla rete alla quale volevano realmente connettersi, evitando eventuali attacchi man-in-the-middle.

Capitolo 4: Analisi delle performance di una rete WiMAX

Ho realizzato una struttura di rete utilizzando due antenne WiMAX (la Base Station e la Subscriber Station) collegate punto-punto. Le antenne utilizzate sono unità wireless predisposte per l'esterno, operanti nella banda dei 5GHz. Alla BS ho connesso un computer nel laboratorio di telecomunicazioni, alla SS ho collegato tramite Ethernet il mio portatile. I due computer si venivano a trovare nella stessa rete e comunicavano tramite il link tra la BS e la SS. La BS, che riceveva i dati dal PC del laboratorio tramite Ethernet, li trasmetteva mediante il link wireless punto-punto alla Subsciber Station. I dati ricevuti dalla SS venivano ritrasmessi al mio portatile tramite ethernet. Per testare il link, ho utilizzato due software: VLC media player per la trasmissione/ricezione di un video tra i due Computer e Wireshark, sul mio portatile, per catturare i pacchetti che ricevevo. Tutti i test sono stati tenuti sul ponte superiore di Ingegneria. Il punto di inizio, dove era fissata la Base Station, era di fronte al cubo 42C, sede del laboratorio di telecomunicazioni. Con la Subscriber Station mi muovevo verso l'ingresso del ponte. La massima distanza tra la BS è la SS è stata di 72m. In ogni test erano presenti due variabili: la Potenza di trasmissione della Base Station e la distanza della Subscriber Station rispetto alla BS. La BS, infatti, era tenuta fissa, veniva allontanata solo la SS. La metodologia applicata, sommariamente, è stata questa:

1. Impostavo la potenza di trasmissione della BS ad un determinato valore (es. 0dB)
2. Spostavo la SS, con collegato il mio portatile, alla distanza minima: 2m
3. Lanciavo con VLC, dal computer del laboratorio, un video di 10 minuti

4. Dal mio portatile collegato alla SS, con VLC ricevevo il video, e con Wireshark nel frattempo catturavo i pacchetti.
5. Terminato il video, salvavo il file Wireshark nell'hard disk del mio portatile.
6. A questo punto se potevo andare avanti, spostavo la SS alla distanza successiva e ripartivo dal punto 3, altrimenti, se ero a 72m, settavo la BS alla potenza di trasmissione successiva e ripartivo dal punto 2.

Quello che volevo capire era la distanza fino alla quale il link tra le due antenne rimaneva stabile. I risultati ottenuti dall'analisi dei log di wireshark verranno ampiamente commentati nel quarto capitolo e nelle conclusioni.