

RETI WIRELESS

Premessa

La tecnologia Wireless è sempre più di moda e presente. La crescita è derivata dalla sempre più impellente necessità di mobilità ed interoperabilità. E' importante poter collegare due o più reti di uno stesso istituto poste in località distanti ma non tanto da non poter essere collegati via etere; inoltre, gli istituti tradizionali quali licei, scuole medie ecc. situate al centro di una città dove il vincolo architettonico impedisce di avere una rete tradizionale, possono avere l'ormai necessario collegamento in rete ed in internet. Infine, vi è la possibilità di poter compiere il proprio lavoro in rete senza alcun collegamento fisico e lontani dalla propria scrivania.

Basterà avere a portata di mano, entro un certo raggio d'azione che può in ogni modo essere aumentato con l'utilizzo d'antenne altamente direttive, un *access point* cioè un apparecchio che permette di integrarsi con una rete LAN preesistente.

Il mio interesse sull'argomento è derivato dalle parole del Ministro dell'Istruzione che fanno intendere ad una rivoluzione nel campo delle trasmissioni a banda larga e wireless nelle scuole dello Stato.

La tecnologia wireless si sta espandendo oggi in modo estremamente veloce per la facilità e rapidità d'installazione, per il basso costo, per la facile manutenzione, per la flessibilità e la mobilità.

Standard IEEE 802.11

La commissione IEEE ha presentato lo standard wireless, conosciuto come 802.11, nel 1997 e successivamente modificato nel 1999, anche se il progetto era iniziato molto tempo prima e ciò perché le varie compagnie che entravano a far parte della commissione inserivano e/o modificavano le specifiche per avvicinarle ai propri prodotti.

Tale standard definisce le specifiche del livello MAC e di tre livelli fisici: uno operante nell'infrarosso alla velocità di 1 o 2 Mb/s e due operanti nella banda ISM (Industrial Scientific and Medical) di circa 2,45 GHz.

Il livello operante nell'infrarosso ha perso nel tempo d'importanza; pertanto, solo i due livelli fisici operanti nella banda ISM sono rimasti funzionanti e per la precisione FHSS (Frequency Hopping Spread Spectrum) a 1 Mb/s e DSSS (Direct Sequence Spread Spectrum) a 1 o 2 Mb/s.

Poi, lo standard è stato esteso per supportare FHSS a 2 Mb/s e soprattutto DSSS a 5 e 11 Mb/s (conosciuto come 802.11b o Wi-Fi). E' quest'ultima tecnologia che ha fatto decollare il mercato delle LAN wireless.

IL livello MAC è un insieme di protocolli responsabili dell'autenticazione e della cifratura mediante l'algoritmo WEP (Wired Equivalent Privacy), vero handicap dello standard, e del controllo dell'accesso al mezzo di trasmissione. Le modalità di accesso sono due, anche se la seconda è poco diffusa, CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) e Polling Mode o modo coordinato.

Nelle reti wireless non è possibile utilizzare il rilevamento delle collisioni e questo perché sostanzialmente un nodo che sta trasmettendo non è capace di ascoltare contemporaneamente il canale. Per questo motivo non ci devono essere collisioni. E' questa la maggiore differenza con le reti a tecnologia Ethernet.

Il funzionamento di una rete wireless è molto semplice. Un nodo, prima di poter trasmettere il proprio pacchetto dati, deve essere sicuro che nessun altro nodo sta trasmettendo. Per tale scopo il nodo trasmittente manda al nodo ricevente un segnale di RTS (Ready To send) che contiene informazioni sulla lunghezza del pacchetto. Il nodo ricevente, se è in grado di ricevere i dati, risponde con un segnale CTS (Clear To Send).

A questo punto inizia la trasmissione che viene controllata in ricezione da un algoritmo CRC e se tutto va bene il ricevente invia un segnale di ACK al nodo trasmittente.

Il motivo per cui vengono utilizzati questi scambi, che potrebbero essere superflui, è che così si risolve il problema del nodo nascosto.

Per capire il problema, supponiamo di avere 3 nodi A, B e C sistemati in modo che A e C possono comunicare con B ma non possono farlo tra di loro perché troppo distanti. Pertanto, A potrebbe pensare che B sia libero quando questo invece sta comunicando con C. A non si accorge di nulla perché dal suo punto di vista C non esiste. Allora se A manda il segnale di RTS a B e questo non risponde perché occupato da C, A non trasmette i propri pacchetti dati, finché B non ha terminato con C e ha trasmesso ad A il segnale CTS.

La tecnologia *Spread Spectrum*

La tecnologia maggiormente utilizzata dalle LAN è, come già visto, quella Spread Spectrum. E' una tecnica di radio frequenza a banda larga sviluppata dai militari per un utilizzo in sistemi di comunicazione affidabili, sicuri e per missioni critiche. Tale tecnologia prevede l'utilizzo di una banda più grande di quella necessaria per la trasmissione delle informazioni ad una certa velocità. In

questo modo è possibile avere più forte, con maggiore energia, e quindi, più facilmente rilevabile, ridimensionando fortemente quelle che erano le interferenze e quindi il tasso di errore delle trasmissioni. Abbiamo visto l'esistenza di due schemi che utilizzano questa tecnica: FHSS e DSSS.

1. **FHSS.** Si ha un salto da una frequenza portante ad un'altra, conosciute da entrambi le parti. In questo modo, cioè avendo delle frequenze ridondanti, si riesce a mantenere un singolo canale logico con piccole interferenze.
2. **DSSS.** Questo schema, invece, genera una sequenza di bit ridondante per ciascun bit trasmesso. Cioè si genera una stringa di bit che rappresenta lo 0 binario ed un'altra che rappresenta l'1 binario. E' ovvio che ciò comporta una banda molto elevata, ma anche la possibilità di ripristinare un eventuale errore.

Altri standard

Per completare l'argomento è giusto dare un cenno su altri standard che si sono formati nel panorama delle comunicazioni wireless.

Questi standard sono: HiperLan, HiperLan II, HomeRF, Bluetooth.

1. **HiperLan.** E' uno standard completamente progettato da una commissione di ricercatori dell'ETSI (European Telecommunications Standard Institute), semplice ma con i vantaggi di lavorare in una banda europea da 5,1 a 5,3 GHz con 5 canali fissi e soprattutto una velocità di trasmissione di 23 Mb/s. Il protocollo MAC usa una variante del CSMA/CA ed include se si vuole una cifratura dei pacchetti. La caratteristica fondamentale sta nella capacità dei nodi di compiere automaticamente il forwarding dei pacchetti nel caso in cui due nodi non possono comunicare direttamente. Opera esclusivamente in modalità ad-hoc¹.
2. **HiperLan II.** E' un sistema wireless ATM (Asynchronous Transfer Mode) e opera esclusivamente nella modalità infrastructure. Con la stessa banda della precedente riesce a trasmettere alla velocità di 54 Mb/s. Riesce, inoltre, a trasportare anche pacchetti IP, Firewire e voce digitale con cifratura DES a 168 bit. Il vantaggio principale rispetto alla prima è la minore latenza.
3. **HomeRC.** E' stato proposto da un gruppo di grosse compagnie e consente una velocità di 10 Mb/s anche con grosse interferenze. Riesce a supportare voce e dati con cifratura a 128 bit.
4. **Bluetooth.** Si propone, in modo molto ambizioso, come cable replacement per qualunque sistema che prevede l'uso dei cavi per i collegamenti. E' una tecnologia molto complessa, che opera nella banda dei 2,4 GHz.

¹ Insieme alla modalità infrastructure è un modo per configurare la rete.

Modalità di configurazione

Si è già detto nella nota che esistono due sole possibili modalità per la configurazione di una rete LAN wireless: ad-hoc e infrastructure.

La prima configurazione permette di creare una rete dinamica “al volo”, dove in linea di principio ogni nodo può comunicare con tutti gli altri. Si presta per conferenze e non certo per le scuole. Esistono degli algoritmi per gestire tale situazione abbastanza confusa. Uno di questi è il SEA (Spokesman Election Algorithm) che elegge uno dei nodi come nodo master e tutti gli altri come slave.

L'altra modalità di configurazione permette, invece, di estendere la precedente modalità utilizzando un'architettura di rete con infrastruttura. Entra in gioco un'apparecchiatura di rete denominata access point con cui i nodi entrano in connessione. Tale apparecchiatura è da un lato connessa alla rete cablata preesistente e dall'altro comunica via radio con i dispositivi wireless, ad esempio un portatile con scheda wireless.

In questo caso si ha una notevole utilità sia per le aziende sia per quelle scuole che avevano problemi, come visto nella premessa, di cablare una rete fisica.

Ogni apparecchiatura riesce a gestire più nodi client anche se un numero preciso non è possibile definirlo a priori perché dipende da vari fattori, quali il numero ed il tipo di trasmissioni, la posizione, etc. In ogni caso, mediamente si possono gestire fino ad una quarantina di nodi client.

Vulnerabilità e sicurezza dello standard IEEE 802.11b

Il problema delle reti wireless è la sicurezza. I pacchetti viaggiano nell'etere e sono soggetti ad ogni tipo di attacco sia esso proveniente dall'esterno sia dall'interno. Pertanto, se non si ha un sistema di sicurezza all'altezza della situazione si rischia di avere dati alla portata di tutti. Anche se è stato approvato di recente un nuovo standard IEEE 802.11g che viaggia alla velocità di 54 Mb/s e che è totalmente compatibile con il vecchio standard in quanto funziona alla frequenza di 2,45GHz, la maggior parte dei prodotti wireless si basano ancora oggi sul vecchio standard IEEE 802.11b che viaggia alla velocità nominale di 11 Mb/s.

Tanto per peggiorare le cose, l'INTEL ha annunciato di volersi dedicare ad un altro standard: 802.11a perché è meno soggetto ad interferenze e veloce fino a 54 Mb/s, ma centrato intorno alla frequenza di 5,2 GHz e, quindi, non compatibile con gli altri due standard.

In generale lo standard IEEE 802.11 introduce i diversi servizi di sicurezza che sono il controllo degli accessi, l'integrità e la riservatezza, attraverso la definizione di due meccanismi:

- SSID (Service Set Identifier): una parola chiave condivisa ed utilizzata per la prima autenticazione dai dispositivi wireless;
- Il protocollo WEP che crittografa le informazioni scambiate in rete ed introduce un controllo di integrità delle stesse.

Una rete wireless 802.11b generalmente utilizza uno o più access point per le comunicazioni fra i vari client della stessa rete. Secondo lo standard 802.11b un client, per poter instaurare una qualsiasi comunicazione dati con un access point, deve eseguire due processi fondamentali:

- **Processo di Autenticazione:** rappresenta il passo iniziale fondamentale per identificare un dispositivo che vuole accedere alla rete wireless. Si considerano due meccanismi di base che utilizzano un identificatore alfanumerico o una password di rete (SSID) che è condivisa da tutti i dispositivi che appartengono alla stessa rete wireless:
 - Sistema di Autenticazione Aperto (Open System Authentication): il client invia un pacchetto di richiesta di autenticazione che verrà esaminato dall'access point. Se il processo andrà a buon fine, questo ultimo invierà un messaggio di risposta per segnalare l'avvenuta autenticazione.
 - Sistema di Autenticazione a chiave condivisa (Shared Key Authentication): processo simile al precedente, si articola sullo scambio di quattro messaggi. L'access point, dopo aver ricevuto il messaggio di richiesta di autenticazione, invia un messaggio di sfida generato in modo casuale. Il client deve crittografare tale messaggio usando la chiave segreta condivisa del protocollo WEP, per poi spedirlo al dispositivo di accesso. Questo ultimo dopo aver controllato il messaggio ricevuto, invia la risposta di avvenuta autenticazione.
- **Processo di Associazione:** rappresenta tutte le azioni che consentono di stabilire una comunicazione tra l'access point e il client.

Entrambi i sistemi di autenticazione sfruttano il fatto che gli access point, per farsi identificare, trasmettono ad intervalli regolari dei segnali di riconoscimento detti di *beacon*. Questo messaggio è captato dal client per identificare il dispositivo disponibile nella zona in cui esso si trova. Se gli access point non trasmettono nulla, allora il client invia un messaggio con lo scopo di trovare un access point vicino. Questa fase è chiamata di *probe*. In ogni caso l'identificatore di rete viaggia nell'etere senza alcuna protezione.

Durante i due processi di autenticazione e di associazione, le informazioni per il controllo dell'accesso alla rete wireless (SSID) viaggiano in chiaro e quindi sono di dominio pubblico, perché possono essere scoperti con software ottimi free come l'analizzatore di rete Network Stumbler (<http://www.netstumbler.com>).

Inoltre, vi è un altro metodo per il controllo degli accessi alla rete ed è basato sul fatto che ogni scheda ha un proprio indirizzo MAC unico. Quindi, in ogni access point vi è memorizzata una lista di tutti gli indirizzi MAC delle schede che possono entrare in rete. Sarebbe un metodo ottimo, ma in realtà ha alcuni inconvenienti. Prima di tutto l'aggiornamento della lista che raramente è automatica e quindi deve essere effettuata manualmente. Inoltre, così si riesce ad autenticare solo il dispositivo e non chi lo usa. Infine, il problema più grave è che l'indirizzo MAC può essere intercettato in modo semplicissimo utilizzando dei programmi chiamati **sniffer** di pacchetti e poi utilizzato in modo non legale.

Purtroppo, anche il protocollo di sicurezza WEP, definito all'interno dello standard 802.11, ha molti punti deboli. Il protocollo WEP è stato implementato soprattutto per garantire la riservatezza delle informazioni, utilizzando l'algoritmo di cifratura RC4, che consente, attraverso l'espansione della chiave condivisa k (di 40 o 104 bit) con il vettore di inizializzazione IV (di 24 bit) che viene generato dal singolo dispositivo di rete wireless, di generare la Key Stream (di 64 o 128 bit) che verrà, a sua volta, utilizzata per la cifratura.

Questo algoritmo effettua uno XOR tra il messaggio da trasmettere e la key stream generata, ottenendo il messaggio crittografato che sarà trasmesso sulla rete. Si presuppone che tutte le entità coinvolte conoscano la chiave condivisa k anche se il protocollo, ed è questo il punto critico per la sicurezza, non definisce alcuna procedura per la sua distribuzione.

L'uso del protocollo WEP comporta dei problemi connessi: a come si genera la key stream, alla lunghezza limitata del vettore IV che potrebbe portare ad avere la stessa chiave per crittografare messaggi diversi, ed alla modalità statica con la quale vengono gestite le componenti che lo gestiscono. Esistono, infatti, molti software di pubblico dominio come AirSnort (<http://airsnort.shmoo.com>), WEPcrack (<http://sourceforge.net/projects/wepcrack>) che riescono a automatizzare il processo di cracking del protocollo WEP raccogliendo mediamente dati da 100 MB a 1 GB e questo perché vi è una forte correlazione tra la chiave segreta k ed il messaggio crittografato trasmesso.

Soluzioni per la sicurezza

A causa delle vulnerabilità dello standard 802.11, sono sorte alcune soluzioni proprietarie tendenti a migliorare sia il controllo degli accessi sia la gestione delle chiavi di cifratura del protocollo WEP. Pertanto, è nato il progetto WPA (Wi-Fi Protected Access) che introduce due nuovi meccanismi di sicurezza:

- Protocollo di sicurezza TKIP (Temporal Key Integrity). E' un nuovo meccanismo di crittografia che utilizza un vettore di inizializzazione esteso e che consente l'aggiornamento dinamico delle chiavi di cifratura.
- Architettura di sicurezza IEEE 802.1x/EAP (Extensible Authentication Protocol). Permette di aumentare il controllo degli accessi alla rete utilizzando un server esterno che dialoga con i vari access point della rete stessa per autenticare l'identità di ogni client che si vuole collegare.

Entrambi questi meccanismi faranno parte del nuovo standard 802.11i mediante il quale si vuole standardizzare la sicurezza per le reti wireless. Purtroppo, la sua uscita è prevista per la fine del 2003.

Una ulteriore soluzione potrebbe essere quella di utilizzare delle connessioni virtuali (VPN), attraverso le quale far viaggiare i dati crittografati in modo sicuro. E' necessario, in questo caso avere dei firewall e dei software particolari.

Conclusioni

Ricordiamo sempre che non esiste la sicurezza in assoluto, ma un giusto compromesso tra il livello di protezione scelto e la trasparenza dell'accesso alla rete.

Si è visto che quelle che dovevano essere le protezioni per la trasmissione dei dati in reti wireless, sono in realtà i punti deboli.

Il problema è l'assoluta fiducia nei mezzi messi a disposizione da parte degli utenti. In realtà i problemi visti denotano la possibilità che dati importanti possono essere alla portata di tutti, con un grado di sicurezza minimo.

Per cercare di limitare i "danni", conviene seguire alcune regole semplici ma fondamentali, nell'attesa di un nuovo standard finalmente sicuro:

1. Mettere la propria rete dietro un firewall;
2. Crittografare personalmente i dati da trasmettere, a prescindere dal protocollo WEP, con tecnologia PGP, SSH + VNC;
3. Disabilitare i messaggi beacon nel caso di un solo access point;
4. Cambiare le chiavi WEP di default e, se possibile, utilizzare i nuovi meccanismi EAP;
5. Utilizzare una lista MAC dinamica delle sole schede abilitate alla rete wireless;
6. Utilizzare un SSID casuale;

7. Cercare di inserire gli access point in posti lontani dalla periferia della struttura e usare, come detto nella premessa, antenne direzionali per evitare di irradiare nelle strade, dove chiunque con un po' di pratica, software semplici da usare e un portatile potrebbe entrare nella rete;
8. Non fidarsi della teoria e controllare periodicamente il perimetro della struttura con quei software di monitoraggio di cui si parlava prima.