Conosci tutto sul WiFi?

By Redazione | Fare Elettronica 345 - Marzo 2014

Come e' stata pensata e sviluppata la tecnologia Wi-Fi? Quali sono le soluzioni tecnologiche che permettono la trasmissione a distanza di grandi flussi di dati in un etere sempre più sovraccarico di utilizzatori?

Il termine Wi-Fi – l'abbreviazione Wireless Fidelity che fa il verso all'audiofilo Hi-Fi- viene usato per riferirsi a dispositivi che possono collegarsi a reti senza fili basate sulla standardizzazione dell' IEEE conosciuta con il codice 802.11 (nella realtà, come vedremo dopo, il nome Wi-Fi e' associato formalmente alla specifica 802.11 b). La tecnologia Wi-Fi consiste di protocolli e soluzioni hardware che danno all'utente la possibilità di scambiare dati ad una elevata velocità, senza utilizzare alcun cavo di rete (wireless), mantenendo quindi una completa libertà di movimento. Lo standard IEEE 802.11 detta le specifiche della tecnologia solo per i livelli più bassi dello strato ISO/OSI (vedi Glossario). Una delle possibili classificazioni di un sistema wireless e' quella che riguarda il range di distanze coperte. Con il termine Wireless PAN (Personal Area Network) vengono indicate piccole reti wireless costituite da un terminale wireless, da una o più periferiche e con estensione uguale o minore ai 30 piedi (circa 10 metri), esempi di queste sono Bluetooth e Zigbee. Con il termine WLAN (Wireless Local Area Network) vengono indicate reti di più terminali wireless (es. notebook o

palmari) con estensione maggiore dei 10 m., ma inferiore alle migliaia di metri. Il termine WLAN si trova spesso come sinonimo di Wi-Fi, la standardizzazione 802.11, come già detto sopra, descrive soltanto la parte più vicina alla trasmissione fisica del Il termine WLAN si trova spesso come sinonimo di Wi-Fi, ma la standardizzazione 802.11, come già detto sopra, descrive soltanto la parte più vicina alla trasmissione fisica delle informazioni, e quindi si può, a giusta causa, parlare di Wi-Fi anche per applicazioni molto diverse dalle reti di PC alle quali siamo abituati (comprese applicazioni embedded molto interessanti ai nostri scopi).

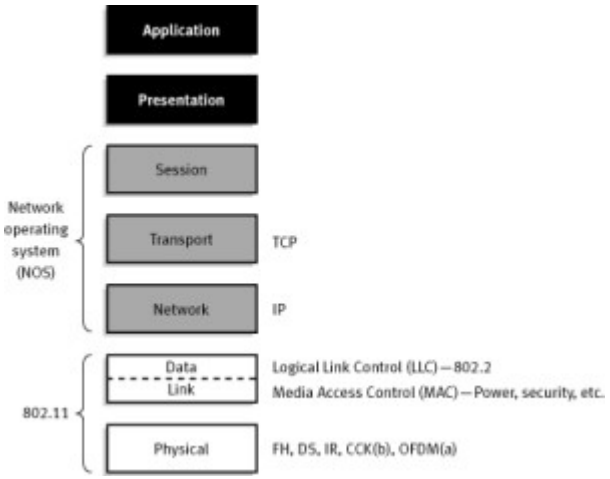

Figura 1: modello ISO

Breve storia del Wi-Fi

La prima sperimentazione di wireless network precede di molto la nascita delle reti Wi-Fi, e addirittura delle stesse reti cablate di tipo Ethernet. Fu nel lontano 1971 che iniziò lo sviluppo da parte dell' Università delle Hawaii della rete Aloha, allo scopo iniziale di collegare gli elaboratori di quattro isole, senza utilizzare costose linee telefoniche sottomarine. Il progetto portò a buoni risultati pratici, ma soprattutto fu una fucina di nuove idee, che negli anni successivi resero possibile lo sviluppo di reti asincrone senza coordinamento centrale, come Ethernet. Nel 1985 la Federal Communication Commission (FCC) statunitense rese disponibili all'uso non licenziato, alcune bande di frequenza molto interessanti (compresa la banda intorno ai 2.4GHz, che fino ad allora era stata dedicata a emissioni non intenzionali in campo industriale) allo scopo di sperimentare su larga scala la comunicazione a spettro esteso (Spread Spectrum). Questo attirò l'attenzione di diverse aziende elettroniche, attive nel campo della grande distribuzione (tra le prime NCR e Symbol Technologies), che provarono a partire da qualcosa di semplice e molto ben maneggiato all'epoca: chip che implementassero la parte bassa dello standard Ethernet (in particolare MAC e PHY), con aggiunta di qualche modifica, per gestire le ovvie differenze tra i mezzi trasmissivi. L'obiettivo immediato per l'epoca, era costruire una tecnologia con adeguata banda, che supportasse la presenza di diversi nodi in un' eventuale rete, che fosse in grado di comunicare attraverso ostacoli anche metallici e potesse essere utilizzata in qualsiasi ambiente di lavoro (anche industriale). Diversi tipi di rete proprietaria incominciarono a prendere piede agli inizi degli anni '90. Con l'andare del tempo, le prime implementazioni si dimostrarono costose e mancanti della minima interoperabilità (non permettevano, cioè, di comunicare con nessun altro sistema prodotto terzo che non fosse dello stesso tipo). Come spesso capita nell' ambito industriale elettronico, il vantaggio commerciale si realizza, dati gli ingenti costi, in presenza di forti economie di scala; queste, però, soprattutto nelle reti di comunicazioni, esistono solo se il numero degli utilizzatori supera una massa critica (con una locuzione tradotta male dall'inglese si parla di 'esternalità' di rete'),, ergo le soluzioni proprietarie si rivelarono, una volta di più, incapaci di fornire il necessario supporto economico allo sviluppo della tecnologia wireless. Di necessità (altrui) fece virtù l'IEEE (Institute of Electrical and Electronics

Engineers) statunitense, ed elaborò uno standard per la comunicazione wireless. Lo standard venne naturalmente associato ad una delle declinazioni descritte nella macro/classe 802, e gli si diede nome 802.11. Ancora oggi lo standard 802.11 porta con sé, come ogni figlio, somiglianze, limiti e vantaggi del padre originale (Ethernet). In effetti il design originario verteva, oltre che nella proposta di uno strato fisico (PHY) adeguato alle frequenze liberalizzate e al flusso di dati voluto, alla modifica dello strato MAC originale di Ethernet per gestire i vari problemi del mondo wireless (tra i quali, il più importante, l'impossibilità di rilevare collisioni, usando le tecniche di una rete cablata). Le dichiarazioni di intento della standardizzazione prevedevano di:

- creare uno standard globale per reti operanti in una banda libera, senza la necessità di utilizzare alcuna licenza;

- raggiungere la completa Interoperabilità delle apparecchiature;

- rendere l'utilizzo di queste apparecchiature possibile in qualunque parte del mondo;

- creare apparecchiature utilizzabili non soltanto in ambienti interni;

Gli scopi furono raggiunti avendo:

- utilizzo della frequenza dei 2,4 GHz, una banda senza licenza nella quasi totalità dei paesi del mondo e riservata per impieghi industriali, scientifici e medici (ISM) con eventuale adeguamento dei livelli di potenza consentiti in base al paese;

- interoperabilità: lo standard IEEE 802.11, comprende la possibilità, da parte delle stazioni, di operare in due configurazioni: modalità peer-to-peer (direttamente le une con le altre), oppure modalità denominata ad infrastruttura. In questo ultimo caso necessita di un punto di accesso, che permette di far comunicare stazioni wireless con stazioni che si trovavano su LAN cablata (cosiddetto Access Point);

- Utilizzo anche in ambienti esterni: l'ambiente in cui doveva essere localizzata una wireless LAN, non doveva essere il solo ufficio. Lo standard avrebbe permesso di utilizzare la tecnologia wireless in grandi realtà come magazzini, negozi, ospedali e grossi edifici, ma anche in ampi spazi aperti come parcheggi, campus universitari e perfino nelle aree di stoccaggio merci;

Specifiche ed evoluzioni dell' IEEE 802.11

La prima versione dello standard 802.11 venne presentata nel 1997 ("802.11 legacy"): essa specificava velocità di trasferimento comprese tra 0.9 e 2 Mb/s e prevedeva due diversi PHY: quello a raggi infrarossi (IR) o quello radio nella frequenza di 2,4 GHz. La trasmissione infrarosso, anche se prevista in teoria, è sempre stata poco implementata: la maggior parte dei costruttori, infatti, non aveva optato per lo standard ***IrDA,*** per ragioni di velocità, e capacità trasmissive nel campo del prossimo-visibile, preferendo quindi la trasmissione radio. Negli anni successivi, allo scopo di superare i limiti della prima definizione, (soprattutto nei riguardi della larghezza di banda) due gruppi di studio indipendenti in seno all'IEEE proposero due nuovi standard, che miglioravano il throughput della rete usando dei PHY modificati. Quello più conservativo (compatibile con il passat o), come spesso accade, ebbe molto successo e questo portò alla definizione dello standard 802.11b, più comunemente conosciuto con il nome di Wi-Fi (Wireless Fidelity), dal nome del marchio registrato. Oltre al vantaggio della retro compatibilità con il vecchio standard, lo 802.11b ebbe il vantaggio di essere supportato da molte industrie leader nel settore, come Nokia, 3Com, Apple, Cisco System, Intersil, Compaq, IBM, le quali nel 1999 avevano fondato il WECA (Wireless Ethernet Compatibility Alliance) con l'obiettivo della certificazione, dell'interoperabilità e compatibilità tra i

prodotti. Allo stato attuale, la famiglia di protocolli 802.11 include tre diverse evoluzioni del protocollo iniziale (a, b, g), che implementano diversi strati fisici e quindi migliorano le prestazioni iniziali; il concetto di sicurezza è stato incluso in uno standard a parte, lo 802.11i. Gli altri standard della famiglia (c, d, e, f, h, etc.) riguardano estensioni dei servizi base e miglioramenti di quelli già disponibili. Il primo protocollo largamente diffuso dopo l'implementazione legacy (che come già detto soffriva di alcune limitazioni) è stato il ***b***; nello stesso periodo fu sviluppato il 802.11 ***a,*** che sfruttava bande di frequenza molto diverse e quindi perdeva la compatibilità con il passato, ed infine il protocollo ***g*** che e' una sintesi dei punti di forza di entrambi.

Caratteristiche dei vari protocolli

IEEE 802.11 classica

E' la prima versione dello standard 802.11. Venne presentata nel 1997; specificava velocità di trasferimento comprese tra 0.9 e 2 Mb/s e prevedeva tre PHY possibili: i raggi infrarossi (IR) o le onde radio nella frequenza di 2,4 GHz, usando in alternativa una tecnica di frequency hopping spread spectrum(FHSS) oppure una di Direct Sequence Spread Spectrum (DSSS); le differenze nella larghezza di banda (1 o 2 Mbps) derivano dall'uso, a basso livello, di due modulazioni differenti: differential Binary Phase Shift Keying (BPSK) oppure Quadrature Phase-Shift Keying (QPSK) con differente contenuto informativo di ogni simbolo trasmesso (1 bit per Baud per BPSK e 2 bit per Baud per QPSK). Lo strato MAC è un evoluzione dello standard CSMA/CD, il Carrier Sense Multiple Access con Collision Avoidance (CSMA/CA) e nella pratica è rimasto immutato in tutte le altre declinazioni di 802.11.

IEEE 802.11 b (Wi-Fi)

802.11b ha la capacità di trasmettere al massimo 11Mbit/s, e per raggiungere questo scopo usa una versione modificata dello strato PHY, con una segnalazione DSSS molto diversa dalla precedente e molto più complessa (a volte citata come High Rate – DSSS), che implementa delle tecniche di pre-codifica dei dati trasmessi, allo scopo di avere allo stesso tempo affidabilità della trasmissione e aumento della larghezza di banda. Il primo produttore commerciale a utilizzare il protocollo 802.11b è stato Apple Computer, con il marchio AirPort, il primo produttore per IBM compatibili è stato Linksys.

IEEE 802.11 a

Questo standard utilizza lo spazio di frequenze nell'intorno dei 5 GHz e opera con una velocità massima di 54 Mb/s, sebbene, nella realtà, la velocità reale disponibile all'utente sia di circa 23 Mb/s. Questo standard non ha riscosso i favori del pubblico, dato che usando una banda di frequenze diverse perdeva la compatibilità con il 802.11 classico, ma anche perché in molti paesi l'uso delle frequenze a 5 GHz è tuttora riservato. In Europa lo standard 802.11a non è stato autorizzato all'utilizzo, dato che quelle frequenze erano riservate alla Wi-Fi europea, HIPERLAN; solo a metà del 2002 tali frequenze vennero liberalizzate e quindi si poté utilizzare l'802.11a.

IEEE 802.11 g

Questo standard venne ratificato nel giugno del 2003. Utilizza le stesse frequenze dello standard 802.11b (cioè la banda di 2,4 GHz) e fornisce una banda teorica di 54 Mb/s, che nella realtà si traduce in una throughput tipico di 19 Mb/s, simile a quella dello standard 802.11a. È totalmente compatibile con lo standard b, ma quando si trova a operare con periferiche b, deve ovviamente

adottare delle precauzioni per poter comunicare con le vecchie stazioni e per non interferire con il loro traffico.

Il primo grande produttore a rilasciare schede con le specifiche ufficiali 802.11g, fu nuovamente Apple, che presentò i suoi prodotti "AirPort Extreme". Cisco decise di entrare nel settore acquistando Linksys, e fornì i suoi prodotti con il nome di "Aironet".

Tecnologia Wi-Fi

Come già accennato, l'implementazione dello standard 802.11 da parte di IEEE, ha usato come punto di partenza Ethernet. In effetti la 802.11 descrive soltanto i due strati più bassi dello stack ISO/OSI, quelli che sono cioè indispensabili per l'implementazione e il mantenimento di una comunicazione wireless. Relativamente al layer datalink (layer 2), quindi, l'unica parte veramente modificata e' il MAC, mentre il LLC e' esattamente quel 802.2 usato in Ethernet (in effetti per come e' naturale che sia, visto che 802.2 e' praticamente un protocollo a sé stante, focalizzato sulle 'necessità dei layer superiori').Ci concentreremo, qui, sulla parte fisica (PHY) e le sue differenti implementazioni nelle evoluzioni dello standard, e sullo strato MAC, che nella pratica e' sempre lo stesso per tutti i vari 802.11x.

Strato Medium Access Control (MAC)

Il compito dello strato MAC è garantire la possibilità di accedere al mezzo trasmissivo (radio nel caso che ci interessa), usando strategie che minimizzino la probabilità di collisioni tra messaggi inviati da sorgenti diverse. Infatti, data la difficoltà tecnica, la bassa affidabilità ed il costo di avere un network di stazioni sincronizzate tra loro, fin dagli albori del networking si è lavorato per costruire reti fatte di stazioni asincrone senza coordinamento centrale; questo, se da un lato migliora gli aspetti citati, porta però con sé la necessità di un qualche algoritmo distribuito che eviti situazioni in cui stazioni provino a trasmettere insieme e si disturbino l'una con l'altra. Nella Ethernet Wired (*not-switched* per la precisione) il criterio implementativo è il ben noto CSMA/CD (*Carrier Sense Multiple Access/Collision Detect*), nel quale i tentativi di trasmissione vengono effettuati, mentre allo stesso tempo un circuito di rilevazione delle collisioni controlla che nessun' altra stazione stia trasmettendo. A collisione avvenuta, le stazioni coinvolte attendono un tempo casuale, scelto con un algoritmo detto di *backoff esponenziale*, tempo che aumenta o diminuisce con le sequenze di collisioni rilevate. Si può chiaramente intuire come tutto questo sia possibile poiché in un mezzo fisico, come un cavo coassiale o un doppino twisted pair, una collisione porta con sé una particolare condizione elettrica (indicativamente possiamo dire che si trova la presenza di un valor medio di tensione diverso da zero e superiore ad una certa soglia, che per il tipo di modulazione del segnale usata (*Manchester*) è impossibile con una trasmissione non corrotta). In un sistema Wireless questo è molto più complesso da realizzare e intrinsecamente poco efficace, quindi la scelta è di usare un **CSMA/CA** (*Carrier Sense Multiple Access/Collision Avoidance*). Ciò significa che si cerca, con diverse strategie, di limitare il numero di collisioni. Quello che si fa è:

- nell'header di ogni frame inviato sulla rete vi è un indicatore della durata del frame stesso; le stazioni riceventi settano attivo il loro "segnale di portante virtuale" (nella terminologia 802.11 è chiamato NAV) sino allo scadere del tempo di occupazione indicato; un NAV attivo (leggi "diverso da zero") ha il significato di "mezzo occupato non trasmettere";

- un pacchetto di livello due molto breve (ACK), viene usato per confermare la ricezione di ogni singolo frame sulla rete; la mancata ricezione di questo è interpretata come "Collisione Avvenuta": viene applicato il protocollo di backoff esponenziale per attendere il momento giusto di ritrasmettere;

- viene usato un meccanismo di prenotazione del mezzo, attraverso due pacchetti brevi (RTS/CTS); questo minimizza le problematiche dei nodi nascosti (nodo che sente la sorgente, ma non il ricevente e il contrario) poiché prevede un'attività trasmissiva preparatoria da parte di entrambe le stazioni che vogliano comunicare;

Il MAC qui descritto è in pratica immutato in tutte le implementazioni dello standard 802.11.

Strato Fisico (PHY)

Già detto che l'interesse intorno all'uso del wireless nacque con la liberalizzazione della banda ISM intorno ai 2,45 GHz da parte di FCC; nella realtà le raccomandazioni da parte di FCC furono sull'utilizzo, in quelle bande di tecniche di trasmissione a Spettro Espanso (Spread Spectrum). di cosa si tratta? Le tecnologie sfruttate nella realizzazione di comunicazioni wireless sono sostanzialmente due: Narrowband e Spread Spectrum.

- La prima è vincolata dal fatto che gli utenti sfruttano frequenze radio ben definite, limitando le emissioni di potenza ad una banda molto ridotta; la tecnologia necessaria alla comunicazione è molto semplice ed economica, ma la robustezza alle interferenze in banda è bassa;

- La seconda, invece, diffusa nella realizzazione di WLAN (e non solo Wi-Fi), utilizza una banda molto maggiore di quella strettamente necessaria al segnale modulante, ma ha il vantaggio di: essere estremamente più robusta alle interferenze, essere intrinsecamente robusta contro intercettazioni della comunicazione, ma soprattutto di avere meno energia trasmessa per frequenza. Di contro le stazioni sono più complesse (e costose) dovendo risultare sempre opportunamente sincronizzate tra loro, altrimenti il segnale viene "visto" come un rumore di fondo e, in più, devono essere capaci di estrarre il segnale RF su bande più ampie.

L'implementazione della tecnologia Spread Spectrum nell'ambito del Wi-Fi è diversa a seconda dello standard usato**,** in generale si può affermare che (guardare la tabella in alto) tutte le implementazioni ricadono in una delle tre tecniche citate sotto:

- **FHSS** (*Frequency Hopping Spread Spectrum*): Il segnale trasmesso con la modalità FHSS è caratterizzato dal fatto che la frequenza di trasmissione si modifica costantemente nel tempo, secondo una ben definita sequenza pseudo casuale e l'intero spettro è suddiviso in canali trasmissivi (79 canali larghi 1 MHz ciascuno, in particolare per 802.11 legacy). Questa sequenza è calcolabile usando lo stesso seed (seme), sia dalla stazione trasmittente che da quella ricevente; quindi, a patto di usare lo stesso periodo di permanenza in un canale, il ricevitore può agganciarsi al segnale trasmesso e seguire i salti, mentre allo stesso tempo decodifica i frame inviati;

- **DSSS** *(Direct Sequence Spread Spectrum*): Ogni singolo bit del dato da trasmettere è moltiplicato per una sequenza di valori (nel caso *802.11 classico*, una sequenza di 11 valori detta di Barker) in cui ogni elemento della sequenza è detto chip. Il risultato della moltiplicazione è usato come segnale trasmesso. Quello che si ottiene è che il tempo di trasmissione di un bit nella sequenza originale sarà usato, dopo la moltiplicazione, per trasmettere una sequenza di N chip; ovviamente la trasmissione dovrà avere una frequenza N volte più alta (allargamento della banda del segnale). Alla ricezione la stazione interessata, conoscendo la sequenza usata dalla sorgente, effettuerà la stessa operazione per estrarre dal segnale RF la sequenza di bit modulante nella banda più stretta. Pertanto l'effetto macroscopico è che moltiplicando il segnale a banda larga ricevuto per la sequenza di chip, l'energia distribuita sullo spettro espanso viene 'pressata' in una banda più stretta (quella della sequenza originale di bit), mentre allo stesso tempo ogni eventuale disturbo a banda stretta, essendo

statisticamente poco correlato alla sequenza di chip, ha la sua energia spalmata casualmente nella banda ristretta e con effetto trascurabile sul segnale. Si ha un cosiddetto *spreading gain,* un miglioramento del rapporto S/N dovuto all'uso furbo di una banda più grande di quella strettamente necessaria al throughput dei dati.

- **HR-DSSS***(High Rate – Direct Sequence Spread Spectrum*): E' un'evoluzione del DSSS, nella quale non vi è una sequenza di Barker che moltiplica il segnale originale, ma in realtà si usano tecniche di pre-codifica dei dati (come CCK e PBCC) per ottenere baud rate più alte.

- **OFDM (Orthogonal Frequency Division Multiplexing) :** Come si può immaginare, con questa tecnica il segnale dati viene modulato, usando una baud rate più bassa, su diverse frequenze molto vicine tra loro (sottoportanti) che trasportano contemporaneamente parti dell'informazione; il problema è che se fatto in una maniera tradizionale questo porta ad uno spreco eccessivo di banda, dovuto al fatto che per avere un'interferenza bassa le frequenze usate non possono essere troppo vicine e ad un aumento del costo dell'apparato ricevente, che deve estrarre il segnale da tante sottoportanti.

Il trucco è quindi quello di usare l'ortogonalità delle trasmissioni su frequenze diverse (detto in parole povere, l'indipendenza e la capacità di coesistere senza interferire), per avere trasmissioni senza eccesive bande di guardia tra le sottoportanti (quindi senza spreco) e usare in maniera massiccia tool matematici "aggressivi" (Fast Fourier Transform) per estrarre i segnali ricevuti sulle diverse frequenze, in maniera sostenibile per la potenza di calcolo dei micro attuali;

Riservatezza in Wi-Fi

La maggior parte delle reti Wi-Fi non prevede alcuna protezione da un uso non autorizzato. Questo è dovuto al fatto che, all'atto dell'acquisto, le impostazioni predefinite non impongono all'utente l'utilizzo di nessun metodo di protezione (di conseguenza l'utente medio non le modifica o per ignoranza o per comodità). Questo ha portato al proliferare, in zone urbane, di un numero considerevole di reti private liberamente accessibili. A volte accade di utilizzare reti altrui senza autorizzazione, se esse hanno un livello di segnale più forte della propria. Questo comporta problemi di sicurezza nel caso vengano trasmessi dati sensibili o personali (numeri di carte di credito, numeri telefonici, coordinate bancarie). Le Wlan possono essere soggetti a numerosi attacchi:

- **"Eavesdropping"**: Attraverso questo attacco un malintenzionato potrebbe intercettare e decodificare i segnali radio, utilizzando apparecchiature semplici quanto quelle usate per accedere alla lan stessa.

- **"Jamming"**: si verifica quando si provocano accidentalmente o intenzionalmente delle interferenze, rendendo praticamente inutilizzabile il canale di comunicazione.

- **"Injection e attacchi Man in the Middle":** In una connessione wireless è possibile immettere dei dati ad una connessione esistente, in questo modo è possibile sia dirottare che inviare dati e comandi senza permesso.

Nello standard 802.11 l'unico mezzo di protezione progettato è il WEP (Wired Equivalent Privacy), un algoritmo di crittografia che, per problemi di gestione e di implementazione, è praticamente inservibile. Il Wep è stato progettato con un'unica chiave statica che deve essere utilizzata da tutti gli utenti, e cambiarla continuamente è praticamente impossibile. Un aggressore, semplicemente intercettando soltanto un segmento di traffico di rete, è in grado di ricostruire completamente la

chiave. I limiti del WEP sono così seri, da aver trasformato in una vera e propria moda l'attività di caccia alle reti wireless insicure (il "Wardriving"), per sfruttarle sia come accesso gratuito ad Internet (a insaputa del proprietario) oppure, nei casi peggiori, come ponte per sferrare attacchi completamente anonimi. Questi continui problemi e le continue lamentele da parte degli utenti del WI-FI, avrebbero di certo, a lungo andare, compromesso l'ulteriore sviluppo del Wi-Fi. Lo standard, infatti, fu aspramente criticato dai mass-media, dal settore dei prodotti commerciali e dalla maggior parte degli addetti ai lavori del settore della sicurezza informatica, proprio per la mancanza di adeguate specifiche per la sicurezza. Nella speranza di riuscire a risolvere i problemi di sicurezza e ridurre i rischi connessi con l'attuale infrastruttura 802.11, lo IEEE (assieme ai partner commerciali e a quelli del mondo accademico) ha preparato il protocollo 802.11x. Oltre agli obbiettivi riguardanti l'infrastruttura, sono stati affrontati principalmente i problemi di sicurezza, inclusa la crittografia e l'autenticazione. Il nuovo protocollo permetterà di avere una crittografia continua dei nodi, effettuata grazie a diverse chiavi segrete, colmando uno dei problemi del WEP. Mentre per quanto riguarda l'autenticazione, questa avverrà in modalità duale, invece di un semplice processo handshake client-to-server; il tutto avverrà tramite uno schema client-to-server, server-to-client. Anche se questa soluzione non offrirà una protezione a tutti i tipi di attacco elencati precedentemente, rappresenta comunque un passo importante verso la costituzione di un sistema più sicuro. Per sopperire ai problemi del WEP sono stati introdotti i protocolli ***WPA*** ed il ***WPA2,*** che offrono livelli di sicurezza maggiori. Per avere un livello di sicurezza maggiore è però necessario implementare sistemi di autenticazione ad un livello della pila ISO/OSI superiore. Essi possono essere: l'autenticazione basata su Radius server, la creazione di tunnel PPPoverEth o di VPN crittografate. Ovviamente il miglior metodo di protezione rimane contenere la propagazione delle onde radio dove non siano necessarie. Ciò si può attuare limitando via software la potenza di trasmissione, oppure utilizzando antenne con un lobo di radiazione indirizzato esclusivamente alle zone in cui si richieda la connettività.

Logo Wi-Fi e certificazione

Un dispositivo, anche se conforme alle specifiche IEEE 802.11, non può utilizzare il logo ufficiale Wi-Fi se non ha superato le procedure di certificazione stabilite dal consorzio Wi-Fi Alliance (Wireless Ethernet Compatibility Alliance), che testa e certifica la compatibilità dei componenti wireless con gli standard 802.11x (della famiglia 802.11). La presenza del marchio Wi-Fi su di un dispositivo dovrebbe quindi garantirne l'interoperabilità con gli altri dispositivi certificati, anche se prodotti da aziende differenti.

Conclusione.

Per i bassissimi costi della tecnologia, il Wi-Fi è la soluzione principale per il digital divide, che esclude numerosi cittadini dall'accesso alla banda larga. Wi-Fi è usato da anni in tutto il mondo per portare connettività veloce nelle zone isolate e nei piccoli centri. Negli USA (laddove l'UMTS si è rivelato un fallimento), si è sperimentata anche un'integrazione con la telefonia mobile; il Wi-Fi dovrebbe sostituire le vecchie antenne ***GSM/GPRS/UMTS***, con una nuova rete, in grado di dare le velocità sperate e i servizi di videotelefonia. Ci sono prospettive di integrare fonia fissa e mobile in un unico apparecchio, che con lo stesso numero sia in grado di funzionare come telefono fisso, se utilizzato nel raggio di 300 metri da casa; oltre i 300mt da casa deve poter funzionare come un normale cellulare. Grazie al Wi-Fi, anche i centri più piccoli hanno spesso possibilità di accesso veloce ad Internet, pur non essendo coperti da ADSL. In molti sostengono che i dispositivi Wi-Fi

sostituiranno i telefoni cellulari e le reti GSM. Nel futuro più prossimo, fattori che costituiscono ostacoli a questo fatto sono di seguito: l'impossibilità del roaming e delle opzioni di autenticazione (802.1x, SIM e RADIUS), la limitatezza dello spettro di frequenze disponibili e del raggio di azione del Wi-Fi. Come sempre questa è solo un'introduzione ad un argomento quanto mai vasto che vuole stimolare la curiosità ad approfondire i vari argomenti, magari usando i riferimenti citati in calce.

Riferimenti

- http://en.wikipedia.org/wiki/ALOHAnet I segreti di Aloha, la mamma di tutte le reti asincrone.

- http://it.wikipedia.org/wiki/IEEE_802.11 pagina di Wikipedia su standard IEEE 802.11

- http://www.wi-fi.org/ Sito Web Ufficiale della Wi-Fi alliance

- http://www.ieee802.org/11/ sito ufficiale IEEE 802

- http://standards.ieee.org/getieee802/802.11.html specifiche nel sito IEEE