LA SICUREZZA DELLE RETI WIRELESS: PROTEZIONE E TECNICHE DI PROGETTAZIONE OTTIMIZZATA

Fabio Garzia
Ingegneria della Sicurezza – Dipartimento ICMMPM
Università degli Studi di Roma "La Sapienza"
Via Eudossiana, 18 - 00184 Roma
tel. 0644585626, fax 06233207150, email fabio.garzia@uniroma1.it
sito web: w3.uniroma1.it/sicurezza

1.INTRODUZIONE

Le reti wireless stanno avendo una grande diffusione perché liberano coloro i quali utilizzano computer portatili e computer fissi dalla schiavitù del cavo di rete.
Il termine corrente che si utilizza sempre più frequentemente per indicare le tecnologie che utilizzano le reti wireless è *Wi-Fi*, abbreviazione di *Wireless Fidelity*. In realtà anche la telefonia cellulare di nuova generazione (la cosiddetta 3 G, rappresentata per esempio dal UMTS), nata per comunicazioni fonia e dati (comunicazione che può peraltro già avvenire, seppur con velocità inferiore e con alcune limitazioni, con le generazioni 2 G e 2,5 G rappresentate, la prima dal GSM e la seconda dal GPRS e dal EDGE) rappresenta un sistema wireless, con la differenza che essa può raggiungere distanze tra terminale e stazione radio base (o punto di accesso alla rete fissa) di qualche chilometro, al contrario dei sistemi wireless che si tratteranno nel seguito, i quali sono in grado di raggiungere al massimo la distanza di qualche centinaio di metri in aria libera. Di contro, i più veloci sistemi wireless attuali possono raggiungere velocità massime dell'ordine dei 100 Mbit/s di fronte ai 2 Mbit/s raggiungibili dal sistema UMTS. I due sistemi, piuttosto che contrastanti, sono effettivamente complementari ed infatti si stanno realizzando tentativi dispositivi di convergenza, che possano utilizzare l'una o l'altra delle reti in funzione della disponibilità del servizio, potendo il sistema UMTS garantire, sempre e comunque, una copertura quasi completa su tutto il territorio utilizzando il roaming con gli altri gestori.
La tecnologia più utilizzata per il *Wi-Fi* si basa sul protocollo IEEE 802.11X, sviluppato dal International Institute of Electrical and Electronical Engineers. La X finale sta ad indicare le varie versioni che si sono susseguite (a, b, g), caratterizzate da una velocità di trasferimento dei dati sempre crescente (variabili da 11 sino a 54 Mbit/s potendo raggiungere i 108 Mbit/s in modalità denominata veloce, uguale, quindi a quella delle normali reti cablate), unitamente al livello di sicurezza (protocollo crittografico).
In realtà esistono anche altri standard Wi-Fi, come il Bluetooth, riservati comunque a realizzare reti per la connessione di dispositivi che si trovano ad una distanza reciproca non superiore a 10 metri, raggiungendo al massimo 1 Mbit/s. Tali reti si definiscono anche Personal Area Network o PAN.
A rigore, rientrano nella categoria wireless anche le connessioni ad infrarossi tra 2 dispositivi, le quali non permettono di superare la distanza, rigorosamente in linea retta ed in assenza di ostacoli, di mezzo metro con velocità massima di 4 Mbit/s. Tale connessione, dato il sempre minore utilizzo da parte degli utenti, non verrà trattata nel seguito.
Le reti wireless, prese in considerazione nel seguito, utilizzando onde elettromagnetiche alla frequenza delle microonde (2,5 o 5 GHz), pongono 2 tipi di problemi:
1) sicurezza e protezione della persona dal punto di vista sanitario (*safety*) all'esposizione ai campi elettromagnetici;
2) sicurezza e protezione della rete wireless e dei computer ad essa connessi da attacchi volontari e premeditati (*security*) al fine di acquisire in maniera fraudolenta i dati che vengono scambiati in essa o semplicemente per provocarne il malfunzionamento.

Nel seguito si illustreranno i principi di funzionamento delle reti wireless, nonché si approfondiranno gli aspetti gli aspetti di sicurezza sia dal punto di vista *safety* che dal punto di vista *security*. Infine si illustrerà una tecnica di ottimizzazione estremamente efficiente per la realizzazione di reti wireless basata sugli algoritmi genetici.

2. PRINCIPIO DI FUNZIONAMENTO DELLE RETI WIRELESS

Le reti wireless utilizzano le onde elettromagnetiche alla frequenza delle microonde (2,5 GHz, detta anche banda ISM, Industrial-Sanitary-Medical, o 5 GHz).
Esse permettono la connessione punto-punto tra due dispositivi (connessione peer to peer) o una connessione multi-punto tra più dispositivi.
In entrambi i casi uno dei dispositivi può essere rappresentato da un punto di accesso (PA o *access point*) che funziona in maniera analoga alle stazioni radio base per telefonia cellulare, permettendo a tutti i dispositivi della rete abilitati di accedere alla rete LAN (Local Area Network) fissa a cui il punto di accesso è connesso. Tale rete fissa può anche essere rappresentata da internet.

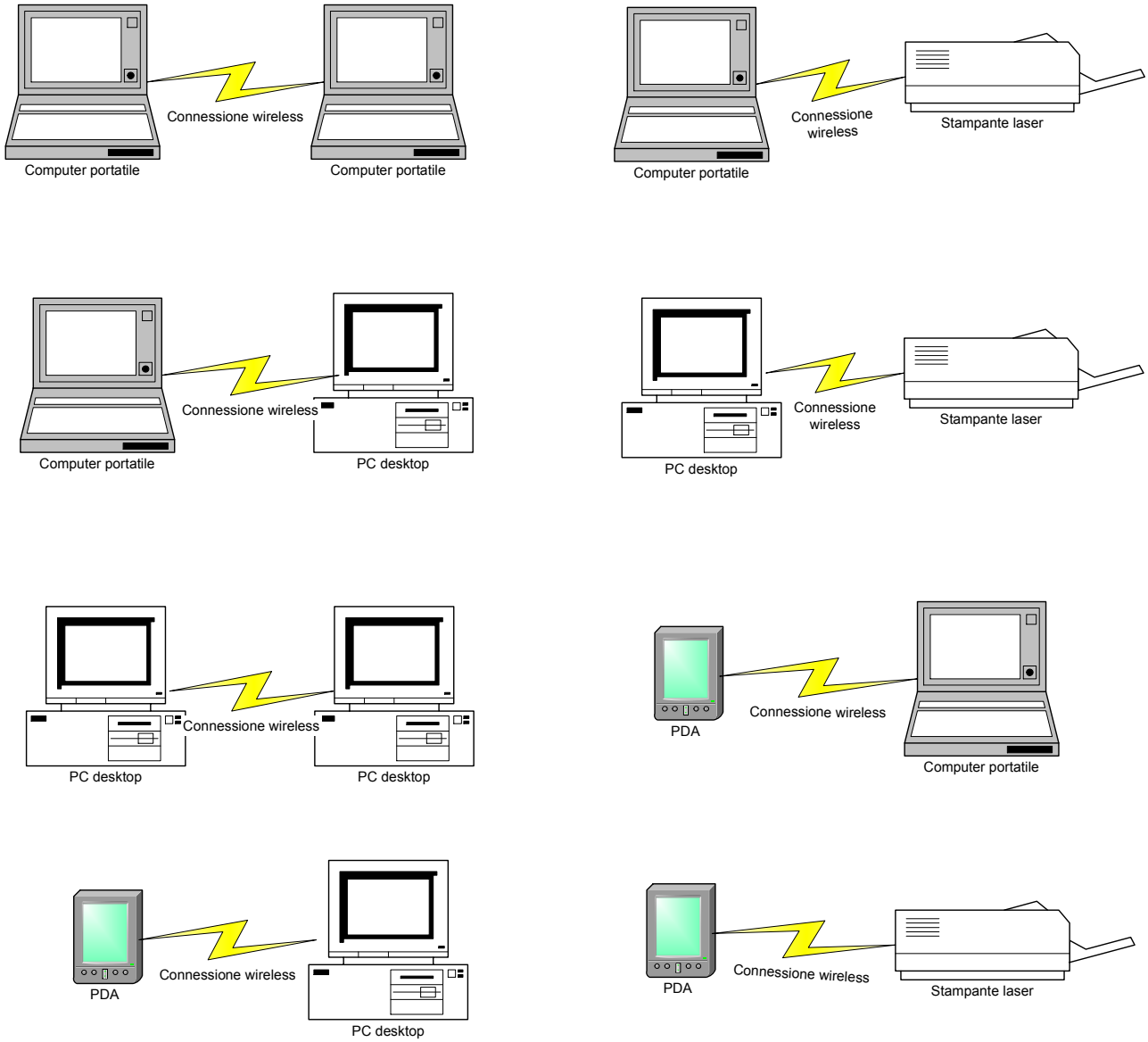

Fig.1 Esempi di rete wireless punto-punto (portatile- portatile, portatile – stampante, portatile – fisso, fisso – stampante, fisso – fisso, palmare – portatile, palmare – fisso, palmare - stampante).

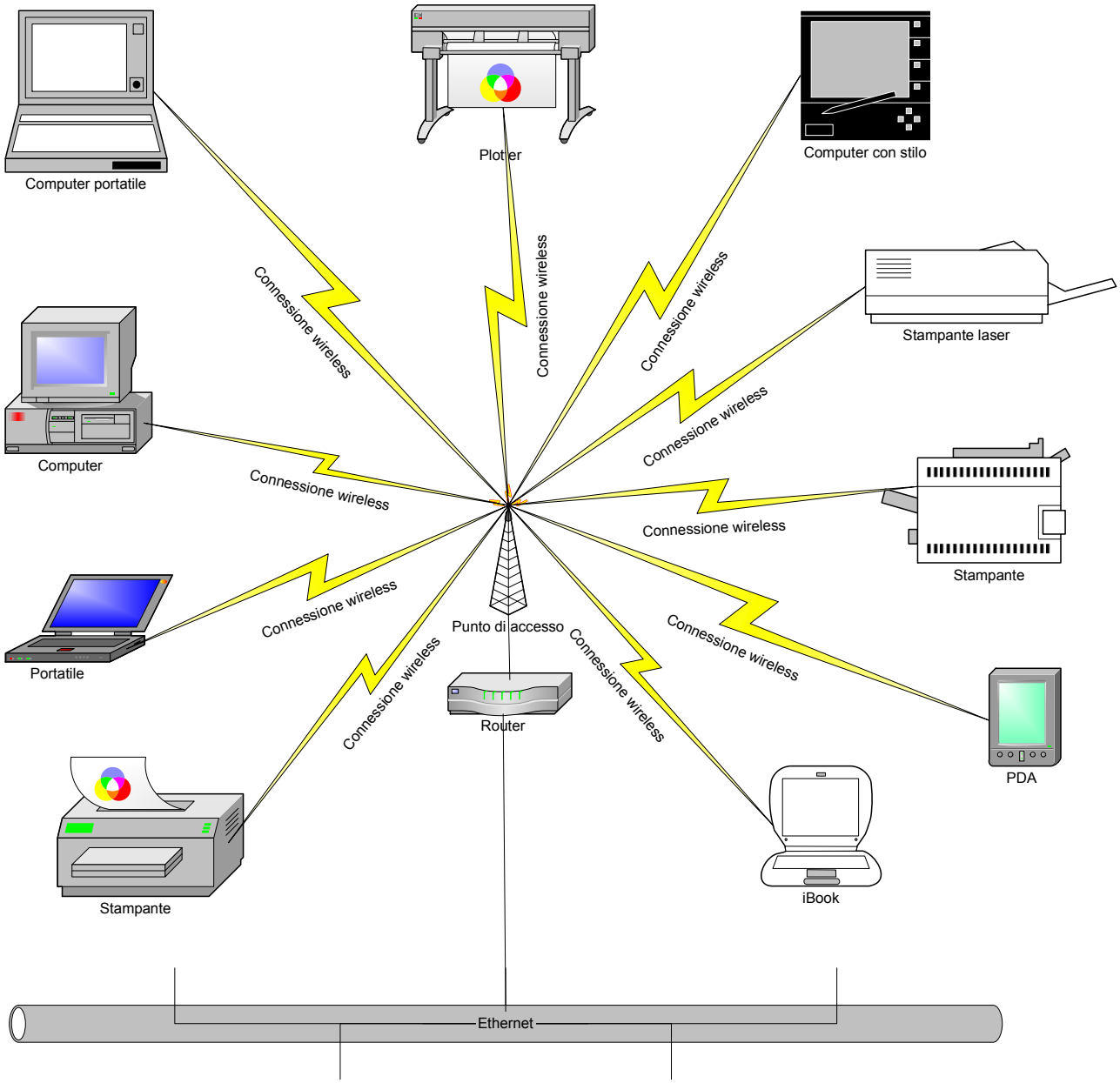

Fig.2 Esempio di rete wireless multi-punto.

La portata massima raggiungibile dipende principalmente da 2 fattori:
1) la potenza di emissione dei dispositivi della rete;
2) il tipo di modulazione utilizzata.
Maggiore è la potenza di emissione e maggiore è la portata raggiungibile. La potenza di emissione non può ovviamente superare determinati livelli al di sopra dei quali si potrebbero creare dei problemi sanitari di esposizione della popolazione. Ai livelli comunemente utilizzati, ben al di sotto della soglia sanitaria e di cui si parlerà nel paragrafo seguente, la portata raggiungibile varia dai 300 metri in aria libera sino a 50-100 metri all'interno di edifici.
Il tipo di modulazione utilizzata influenza sia gli aspetti *safety* (a parità di portata raggiungibile si può utilizzare una potenza ridotta) sia gli aspetti *security* (a parità di potenza di emissione e di distanza raggiungibile i dati scambiati possono essere letti solo dai dispositivi autorizzati).
Il tipo di modulazione più utilizzata nei sistemi wireless è quella ad espansione di spettro in cui lo spettro del segnale trasmesso da ogni dispositivo (che è in genere proporzionale alla velocità di trasmissione in bit/s) viene opportunamente espanso sino ad occupare un'intera banda comune a tutti i dispositivi. L'espansione avviene moltiplicando il segnale emesso dal singolo dispositivo per

un segnale, o codice di espansione, che gode della proprietà di essere ortogonale rispetto ai codici emessi dagli altri dispositivi. Utilizzando la proprietà di ortogonalità dei codici di espansione, si ottiene il risultato che ogni segnale espanso emesso da un dispositivo si comporta come un rumore di fondo nei confronti degli altri dispositivi e viceversa: in tal modo un numero elevato di dispositivi può emettere nella stessa banda aumentando solo il rumore di fondo, senza disturbare in maniera specifica una particolare frequenza di emissione. Tale tecnica di modulazione viene anche denominata CDMA (Code Domain Multiple Access o Accesso Multiplo a Divisione di Codice).
In genere la frequenza F_C del codice di espansione è da 100 a 1000 volte superiore a quella F_S del segnale da espandere e la banda del segnale espanso è pari F_C/F_S.
Se, al contrario, si utilizzassero tecniche di modulazioni tradizionali, si dovrebbero accuratamente assegnare le frequenze disponibili ai vari dispositivi, in quanto un eventuale utilizzo della stessa frequenza da parte di dispositivi differenti porterebbe ad un livello di mutua interferenza tale da non permettere, ad entrambi i dispositivi, di poter operare correttamente.
Il segnale originale può essere decodificato correttamente moltiplicando il segnale espanso per il relativo codice di espansione, rendendo l'operazione di ricezione estremamente semplice ed immediata.
Le tecniche di modulazione CDMA principalmente utilizzate sono:
1) a spettro espanso a sequenza diretta (DSSS – Direct Sequenze Spread Spectrum), utilizzata dal protocollo IEEE 802.11b e anche dal sistema di telefonia cellulare UMTS (il protocollo 802.11g utilizza una tecnica analoga denominata OFDM – Ortogonality Frequency Divisional Multiplexing);
2) a spettro espanso a salto di frequenza (FHSS – Frequency Hopping Spread Spectrum), utilizzata dal protocollo BlueTooth.
Nella tecnica DSSS l'espansione avviene moltiplicando semplicemente il segnale originale per un codice binario che rispetta i parametri di frequenza indicati, espandendo il segnale nell'intera banda considerata: se i codici binari di espansione relativi ai vari dispositivi sono ortogonali, i dispositivi potranno utilizzare l'intera banda senza interferire.
Nella tecnica FHSS il segnale originale viene spostato ciclicamente e con frequenza molto più elevata rispetto a quella del segnale stesso, seguendo una sequenza specifica. Il risultato è che il segnale originale salta con un elevata velocità all'interno della banda di espansione, occupandola parzialmente per una quantità pari alla sua larghezza di banda per ogni salto, avendola comunque occupandola interamente alla fine di ogni ciclo di salto. Se le sequenze di salto sono differenti per ogni dispositivo, i dispositivi potranno utilizzare contemporaneamente l'intera banda senza disturbarsi reciprocamente.
Per poter operare in una rete wireless i vari dispositivi devono essere equipaggiati opportunamente. In particolare, i computer devono essere equipaggiati con specifiche schede wireless in grado di supportare il protocollo di comunicazione della rete o, eventualmente, più protocolli tra cui poter scegliere quello più efficiente per la rete. Nella maggior parte dei casi le antenne per l'emissione e la ricezione della radiofrequenza sono integrate all'interno della scheda, riducendo l'ingombro della stessa, soprattutto per quanto riguarda i computer portatili.

Fig.3 Immagine di tipiche schede wireless: formato PCMCIA per computer portatile con antenna interna (a sinistra) e su bus PCI per computer fisso con antenna esterna (a destra).

Per quanto riguarda questi ultimi, le case produttrici di microprocessori hanno iniziato a produrre CPU (come il *Centrino* della INTEL®) che implementano già al loro interno funzionalità wireless.
Una volta attivate le funzionalità wireless sul dispositivo, esso è in grado di scambiare dati con tutti i dispositivi che utilizzano lo stesso protocollo e sono stati autenticati all'interno della rete.
Se si desidera che la rete wireless sia connessa ad una rete fissa (come una LAN domestica, aziendale o a internet) è necessario aggiungere uno o più punti di accesso (o access point) che permettano ai dispositivi appartenenti alla rete wireless l'accesso alla rete fissa. In genere un access point di medie caratteristiche può consentire un accesso simultaneo variabile da 60 a 250 dispositivi.

Fig.4 Immagine di tipici punti di accesso: con antenne interne (a sinistra) e con antenne esterne (a destra).

La velocità di scambio dei dati decresce sia con la distanza che con il livello di disturbo elettromagnetico presente nella banda di frequenza utilizzata, passando per esempio dagli 11 Mbit/s ad una distanza di 35 m da un access point di medie caratteristiche che utilizza un protocollo 802.11b all'interno di un edificio, sino a 1 Mbit/s ad una distanza di 100 metri. Il protocollo 802.11g permette di raggiungere velocità di 54 Mbit/s in modalità standard e di 108 Mbit/s (comparabile con quella delle reti cablate).

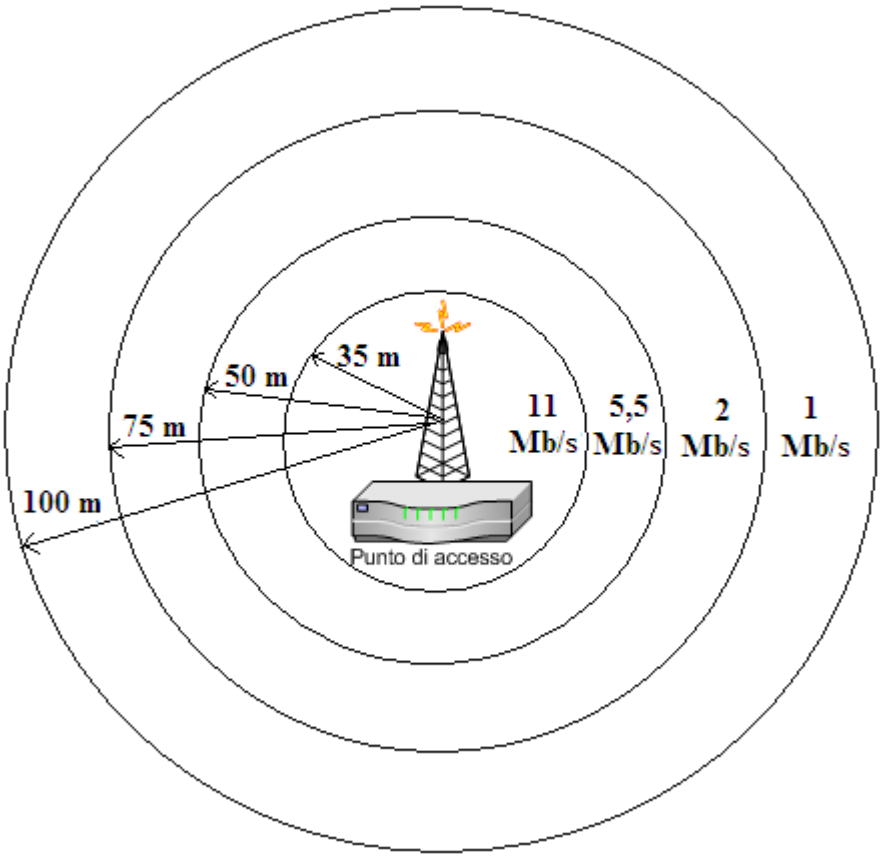

Fig.5 Velocità di scambio dei dati in funzione della distanza per un access point di medie caratteristiche che utilizza il protocollo 802.11b.

3. GLI ASPETTI *SAFETY* DELLE RETI WIRELESS

Si è già detto che i dispositivi wireless utilizzano onde elettromagnetiche alla frequenza delle microonde per poter operare.
Poiché, a parità di frequenza e di caratteristiche tecniche dei dispositivi in gioco, la portata raggiungibile è direttamente proporzionale alla potenza emessa, è evidente che, con i dovuti adattamenti dovuti ai differenti dispositivi utilizzati, le potenze in gioco nei dispositivi wireless oggetto del presente lavoro e che sono in grado di raggiungere il centinaio di metri sono notevolmente più basse rispetto alle potenze utilizzate dai dispositivi per telefonia cellulare (UMTS, GPRS, GSM) i quali sono in grado di raggiungere e superare qualche chilometro di distanza.
Infatti, trascurando i dispositivi che utilizzano lo standard Bluetooth i quali, operando nel raggio di una decina di metri, emettono potenze dell'ordine del milliWatt, i dispositivi che utilizzano lo standard 802.11X emettono potenze di qualche decina di milliWat (in genere non superiori a 100 mW per lo standard 802.11b e non superiori a 30 mW per lo standard 802.11g), al contrario dei telefoni cellulari i quali, in condizione di massima emissione, possono superare anche il Watt. Le potenze di emissione dei dispositivi wireless sono in genere regolabili da zero sino al massimo previsto.

Inoltre, i dispositivi wireless, siano essi access point o schede, non operano mai a contatto diretto con il corpo umano, mentre i telefoni cellulari, se non si utilizzano auricolari o accorgimenti opportuni, operano direttamente a contatto con la testa per cui è evidente che, in prima approssimazione, se il livello di esposizione del corpo umano ai telefoni cellulari rientra negli standard di sicurezza (*safety*) internazionali, il livello di esposizione ai dispositivi wireless, che operano con livelli di potenza dai 10 ai 100 volte inferiori, rientra senz'altro in qualunque standard di sicurezza internazionale, anche i più restrittivi.
I dispositivi wireless rispettano comunque vari standard *safety* internazionali quali: IEC&EN 60950 e UL 2043.
E' comunque possibile eseguire una rapida verifica numerica. La regione di campo radiativo, per una sorgente che opera ad una frequenza di 2,5 GHz, inizia a partire da una distanza di 12 cm dalla sorgente stessa (distanza comparabile alla lunghezza d'onda che può essere calcolata dividendo la velocità della luce nel vuoto per la frequenza di emissione), supponendo che il dispositivo utilizzi un radiatore isotropo (se è presente un'antenna omnidirezionale si è nella condizione suddetta). Nella regione di campo radiativo i campi elettromagnetici iniziano a propagare sotto forma di onde e il rapporto tra campo elettrico E e campo magnetico H è pari all'impedenza del mezzo Z_0 (che in aria è circa uguale a quella del vuoto, cioè 377 ohm) e l'intensità del campo I, che normalmente vale **I**= **E** x **H**, può essere scritta come:

$$I = \frac{E^2}{Z_0} = Z_0 H^2 \qquad [1]$$

Nella regione di campo radiativo, nelle condizioni di radiazione su indicate (emissione mediante radiatore isotropo e quindi sotto forma di onde sferiche nella regione di campo radiativo), l'intensità, ad una distanza R dalla sorgente, è legata alla potenza P emessa dalla sorgente stessa, dalla relazione:

$$I = \frac{P}{4\pi R^2}. \qquad [2]$$

Sostituendo l'eq.[1] nella eq. [2] e risolvendo rispetto ad R si ottiene:

$$R = \frac{1}{E}\sqrt{\frac{PZ_0}{4\pi}} \cong \frac{5{,}48}{E}\sqrt{P} \qquad [3]$$

che permette di conoscere la distanza oltre la quale il campo elettrico E emesso da una sorgente che irradia, nelle condizioni considerate, con una potenza P, si riduce al di sotto di valore dato (purché il valore della distanza R sia superiore alla distanza oltre la quale inizia la regione di campo radiativo).
Tali considerazioni valgono ovviamente se la sorgente si trova nel vuoto. Poiché nella maggior parte dei casi ciò non avviene a causa della presenza di oggetti vari nei dintorni della sorgente, soprattutto di natura metallica, i quali possono alterare il campo emesso, il valore calcolato con l'eq.[3] può discostarsi in maniera non trascurabile, sia per eccesso che per difetto.
Supponendo di avere un dispositivo che emette al massimo della potenza prevista (100 mW) e di utilizzare gli stringenti limiti di 6 V/m per esposizione della popolazione superiore a 4 ore continue, previsti dal previsti dal DPCM 8 luglio 2003 "Fissazione dei limiti di esposizione, dei valori di attenzione e degli obiettivi di qualità per la protezione della popolazione dalle esposizioni a campi elettrici, magnetici ed elettromagnetici generati a frequenze comprese tra 100 kHz e 300 GHz (GU n. 199 del 28-8-2003)", si ottiene una distanza di 29 cm circa (superiore alla distanza di 12 cm oltre la quale inizia la regione di campo radiativo).
Il valore di 6 V/m risulta invece essere notevolmente inferiore ai limiti previsti nelle "Prescrizioni minime di sicurezza e di salute relative all'esposizione dei lavoratori ai rischi derivanti dagli agenti fisici (campi elettromagnetici)", CE direttiva Parlamento Europeo e Consiglio 29 aprile 2004, n. 2004/40/CE. Tenendo conto che raramente ci si troverà ad una distanza inferiore ai 29 cm da punti di accesso wireless, i livelli di campo a cui si è esposti possono essere considerati più che sicure dal punto di vista sanitario.

I dispositivi wireless vengono sovente utilizzati in ambienti in cui sono presenti altri dispositivi elettronici o comunque sensibili ai disturbi elettromagnetici. Il tipo di modulazione utilizzata e le potenze emesse li rendono compatibili anche con gli ambienti più sensibili, rispettando la maggior parte delle normative internazionali di compatibilità elettromagnetica quali la EN 55022/4.

4. GLI ASPETTI *SECURITY* DELLE RETI WIRELESS

Le reti wireless, oltre alle consuete minacce provenienti dalle reti fisse e da internet, devono fronteggiare anche le vulnerabilità provenienti dall'utilizzo di radiofrequenza nello spazio libero: se non si attivano opportune funzionalità di sicurezza di tipo *security*, chiunque si trovi a passare nel raggio di azione dell'access point della rete stessa potrebbe collegarsi alla stessa sottraendo dati e informazioni riservate, installare virus o altri programmi di controllo sui computer della rete e persino compiere reati informatici addossando la colpa al possessore della rete.
E' inoltre necessario ricordare che il furto di dati personali di altre persone o aziende comporta un reato per mancanza di un adeguata custodia dei dati stessi ed in particolare la nuova legge sulla privacy impone di adottare accorgimenti opportuni per assicurare la riservatezza dei dati custoditi sui computer.
Per quanto riguarda l'utilizzo della radiofrequenza quale vettore di comunicazione, le stesse tecniche CDMA assicurano l'impossibilità di lettura, se non con un dispositivo utilizzante lo stesso protocollo wireless, delle informazioni scambiate (supponendo che tutte le misure *security*, di cui si tratterà nel seguito, non siano attive).
Una prima regola di *security* consiste nel non rendere visibile a chiunque la presenza dei router wireless in maniera tale che chi si trovi a passare nel loro raggio di azione non si accorga della presenza di una rete wireless. Solitamente questa impostazione si ottiene disattivando l'opzione *Broadcast SSID*, funzionalità utilizzata per la pubblicazione dell'identificativo della rete.
Una seconda regola da rispettare consiste nel permettere l'accesso alla rete alle sole schede wireless utilizzate, identificabili univocamente attraverso un indirizzo specifico per ciascuna di essa, denominato *Mac Address* (MAC - *Medium Access Control*). In tal caso è necessario fornire al punto di accesso l'elenco dei *Mac Address* che possono avere accesso alla rete. Tale sistema non garantisce una sicurezza assoluta giacché tali indirizzi possono essere contraffatti e un eventuale attaccante può provare sistematicamente una serie di indirizzi sino a raggiungere un indirizzo valido che consenta l'accesso alla rete (purché l'utente legittimo non stia in quel momento utilizzando la rete, poiché in tal caso si genererebbe una collisione di indirizzi che verrebbe immediatamente rivelata).
Una terza regola, forse la più importante, consiste nell'utilizzare un protocollo di cifratura adeguato. Data l'importanza di questo punto è opportuno fornire maggiori informazioni sui sistemi di cifratura o crittografici.
Un sistema di cifratura permette di generare, a partire da un messaggio in chiaro, un messaggio cifrato che può essere trasmesso attraverso un mezzo caratterizzato da un livello di sicurezza non elevato, per poter essere decifrato, una volta giunto a destinazione, restituendo il messaggio in chiaro originale.
I moderni sistemi di cifratura separano l'algoritmo crittografico vero e proprio dalla chiave di cifratura. Utilizzando lo stesso testo in chiaro e lo stesso algoritmo di cifratura, si otterrà un messaggio cifrato che varierà al variare della chiave di cifratura. Nei sistemi a chiave privata o simmetrica, il testo originale potrà essere decifrato solo se si è in possesso della chiave di decifratura (che è uguale alla chiave di cifratura).
La massima sicurezza è raggiungibile se si utilizza una chiave casuale e caratterizzata dalla massima entropia (in cui non ci sia alcuna correlazione tra i singoli elementi che la compongono) che viene miscelata con il messaggio da cifrare. Tale chiave deve inoltre essere utilizzata una sola

volta. Tale soluzione è purtroppo poco pratica nella maggior parte dei casi (si pensi per esempio alle difficoltà che si avrebbero nel cifrare messaggi lunghi svariati Mbit).
Per tale motivo si utilizzano algoritmi di cifratura estremamente robusti che si basano su problemi matematici estremamente complessi, in maniera tale che l'unico modo per decifrare il messaggio consista nel tentare tutte le possibili chiavi di decifratura sino a trovare quella che permette all'algoritmo stesso di restituire il messaggio originale in chiaro: tale modo di procedere viene comunemente definito attacco a forza bruta.

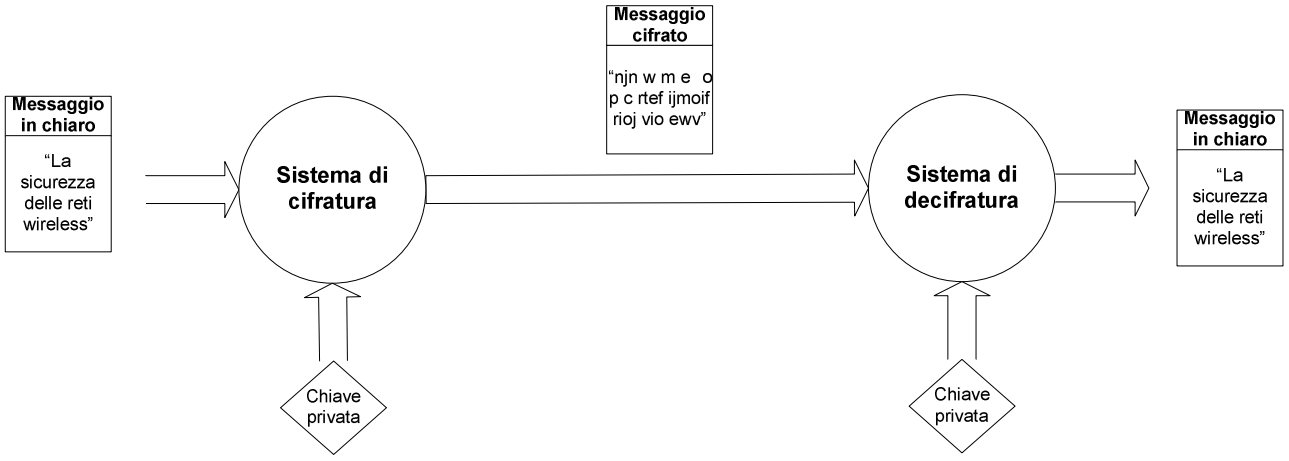

Fig.6 Schema di sistema di cifratura a chiave privata

E' evidente che maggiore è la lunghezza della chiave di cifratura (misurata in bit) e maggiore sono i tentativi che devono essere eseguiti per un attacco a forza bruta. Per tale attacco si ricorre di solito a supercalcolatori in grado di eseguire un elevatissimo numero di tentativi al secondo: per un calcolatore in grado di eseguire R tentativi al secondo, per un attacco a forza bruta nei confronti di un algoritmo la cui chiave è lunga L bit, sono necessari $2^L/R$ secondi per trovare quella valida nella peggiore delle ipotesi (chiave trovata alla fine di tutti i tentativi). Un rapido conto ci permette di dire che un calcolatore in grado di eseguire 10^9 tentativi al secondo impiegherà, per forzare un algoritmo che utilizza una chiave a 128 bit, un tempo di $2^{128}/10^9$ secondi, pari a circa 10^{22} anni, tempo notevolmente superiore all'età dell'universo (attualmente intorno ai 1,5 10^{10} anni).
Poiché le operazioni di cifratura e decifratura richiedono l'esecuzione di operazioni matematiche estremamente complesse, maggiore è la lunghezza della chiave e maggiori saranno il numero di operazioni da eseguire per cifrare o decifrare le informazioni da trasmettere.
Gli algoritmi di cifratura comunemente utilizzati sono vari e in genere i dispositivi wireless di nuova generazione sono in grado di supportare anche gli algoritmi utilizzati dai dispositivi meno recenti.
La prima generazione di dispositivi utilizzava il sistema di cifratura WEP (Wired Equivalent Privacy o privacy equivalente alla rete cablata), previsto dallo standard 802.11b. Successivamente si è scoperto che tale sistema di cifratura presentava delle vulnerabilità non risolvibili con facilità mediante semplice aggiornamento del software e per tale motivo, nell'attesa che gli organismi internazionali definissero quale dovesse essere lo standard successivo da adottare, la Wi-Fi Alliance (che è un consorzio costituito dai principali costruttori di dispositivi di rete) ha adottato una soluzione di compromesso che permettesse di utilizzare buona parte dei dispositivi di rete attualmente disponibili. Tale soluzione è rappresentata dal WAP (*Wireless Protected Access*) che, al momento, rappresenta la soluzione più pratica per utilizzo domestico o in uffici di dimensioni ridotte ma assolutamente non ideale per grandi organizzazioni o laddove è richiesta una elevata sicurezza.
Recentemente IEEE ha ratificato il protocollo 802.11i che specifica i sistemi di sicurezza da adottare nelle reti wireless. Il protocollo di sicurezza, brevemente denominato WPA2, si basa

sull'algoritmo AES (*Advanced Encryption Standard*) a 128 bit il quale impone che sui dati da trasmettere vengano eseguite operazioni matematiche così complesse da richiedere la presenza di un microprocessore dedicato allo scopo e quindi solo i dispositivi che hanno al loro interno un chip per la codifica AES potranno utilizzare lo standard WPA2. Ovviamente è sufficiente che in una rete un solo dispositivo non sia compatibile con il sistema più avanzato per renderlo inutilizzabile anche dagli altri dispositivi, che per comunicare con lui dovranno ridurre il loro livello di protezione.
Inoltre, per aumentare il livello di sicurezza, i moderni dispositivi wireless utilizzano il cosiddetto DSL (*Dynamic Security Link* o connessione dinamica di sicurezza) in cui viene assegnata una chiave di cifratura differente ai dispositivi che si connettono di volta in volta, rendendo praticamente nulla la probabilità di conduzione con successo di un attacco a forza bruta.
Una volta adottate le soluzione di sicurezza proposte non bisogna dimenticare che se la rete wireless è connessa ad una rete fissa mediante un access point o addirittura ad internet, la rete stessa è esposta ai ben noti e sempre più raffinati attacchi informatici che provengono dalla grande rete. In tal caso è assolutamente necessario ricorrere ad un dispositivo di protezione noto come *firewall*, da interporre tra l'access point e la connessione ad internet, il quale, se di elevata qualità e se ben programmato, può evitare che si verifichino i problemi menzionati, o comunque ridurne le probabilità di accadimento. Diversamente, si rischia di adottare sistemi di protezione estremamente sofisticati ed avanzati sul lato della rete wireless ma di rendere la rete stessa banalmente vulnerabile nei confronti delle minacce tradizionali, ormai ben conosciute, provenienti da internet.

Fig.7 La marchiatura che accerta che il prodotto è conforme allo standard Wi-Fi.

5. PROGETTAZIONE OTTIMIZZATA DELLE RETI WIRELESS MEDIANTE ALGORITMI GENETICI

Il numero di punti di accesso, la loro posizione e il numero di dispositivi che utilizzano ciascuno di essi rappresentano un tipico problema di ottimizzazione, nel quale è necessario ridurre il più possibile i costi di installazione, riducendo il numero di punti di accesso e posizionando gli stessi correttamente in maniera tale da raggiungere il maggior numero di dispositivi possibile.
I dati di ingresso del problema sono dunque:
1) posizione dei dispositivi;
2) possibile posizione dei punti di accesso;
3) costo dei punti di accesso;
4) massima velocità di trasmissione dei punti di accesso;
I vincoli sono rappresentati da:
1) massima distanza punto di accesso/dispositivo;
2) minima velocità richiesta alla connessione punto di accesso/dispositivo;
3) massimo numero di dispositivi che possono accedere al singolo punto di accesso;

4) utilizzo del minimo numero di punti di accesso.

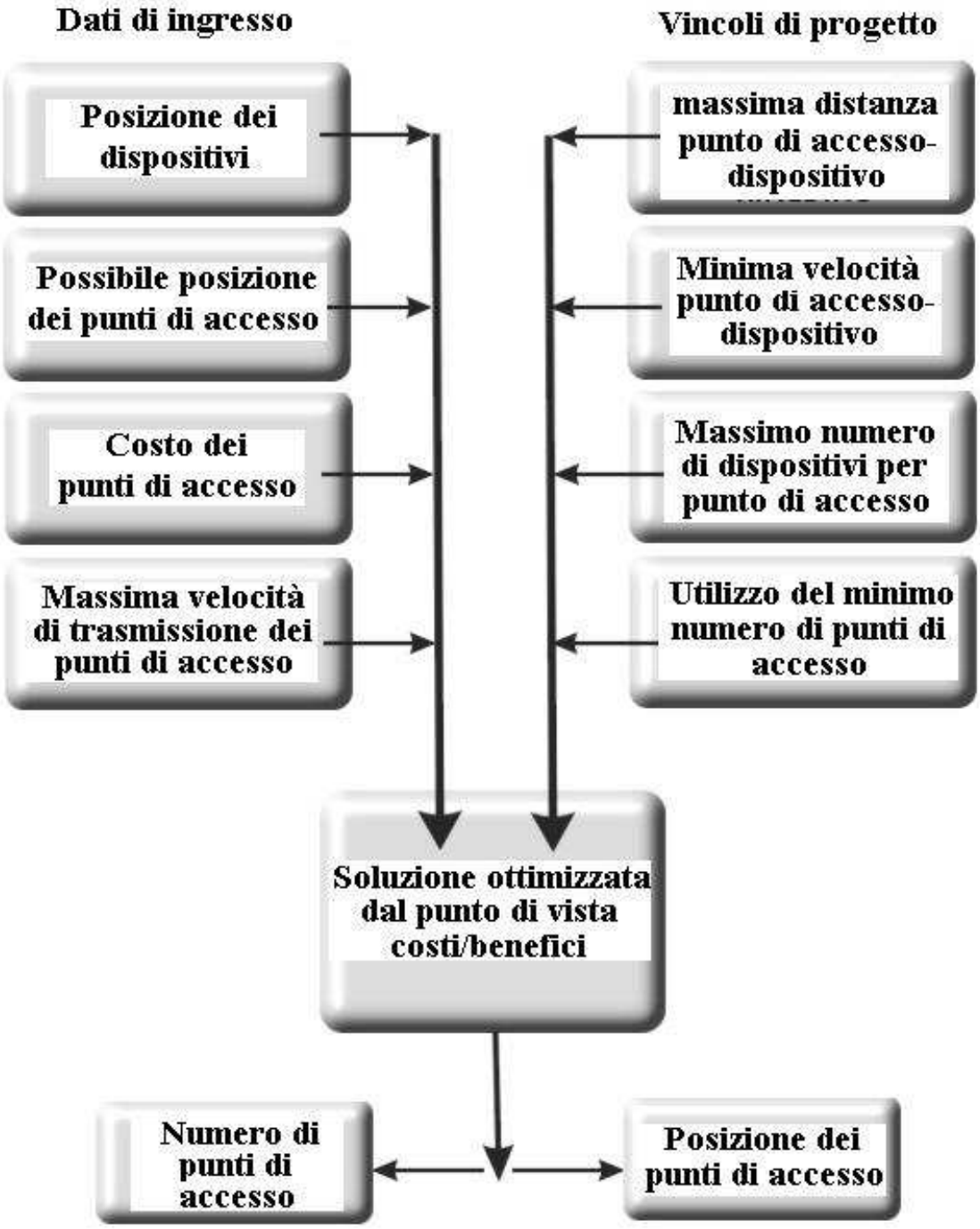

Fig.8 Schematizzazione del problema di progettazione ottimizzata.

Questo genere di problema multivariabile/multivincolo può essere efficacemente risolto utilizzando tecniche evoluzionistiche quali quelle offerte dagli algoritmi genetici.

5.1 Gli algoritmi genetici

Gli algoritmi genetici offrono il grande vantaggio di evolvere il loro comportamento per soddisfare le richieste dell'utente, utilizzando un meccanismo evolutivo che è molto simile a quello utilizzato in natura.

Algoritmi genetici differenti possono essere utilizzati per raggiungere scopi differenti, ciascuno caratterizzato da proprietà ben definite.
Gli algoritmi genetici sono dunque considerati metodi di ottimizzazione numerica ad ampio spettro che utilizzano i naturali processi di evoluzione e ricombinazione genetica. Grazie alla loro versatilità essi possono essere utilizzati in differenti ambiti.
Gli algoritmi genetici sono particolarmente utili quando lo scopo del problema consiste nel trovare un'approssimazione di un minimo globale di una funzione multi-modale, in un dominio pluridimensionale, in maniera quasi ottima. Al contrario della maggior parte dei metodi di ottimizzazione, essi possono trattare facilmente funzioni discontinue e non-differenziabili.
Tali algoritmi codificano ogni parametro del problema che deve essere ottimizzato in una sequenza opportuna (dove l'alfabeto utilizzato è generalmente binario) chiamata gene e combinano i differenti geni per costituire un cromosoma. Un opportuno insieme di cromosomi, denominato popolazione, viene sottoposto ad un processo Darwiniano di selezione naturale, con tanto di accoppiamento e mutazione, creando nuove generazioni fino a che non si raggiunga la soluzione ottima finale sotto la pressione selettiva della funzione di ottimizzazione desiderata.
Gli ottimizzatori genetici operano, dunque, secondo i 9 punti elencato di seguito:

1) codifica, sotto forma di geni, dei parametri della soluzione da ottimizzare;
2) creazione di cromosomi come stringhe di geni;
3) inizializzazione della popolazione iniziale;
4) valutazione ed assegnazione del valore di adeguatezza ad ogni individuo della popolazione;
5) riproduzione per mezzo della selezione degli individui migliori attraverso la funzione di obiettivo;
6) ricombinazione per la generazione di individui ricombinati;
7) mutazione degli individui ricombinati per produrre gli elementi della prossima generazione;
8) valutazione ed assegnazione del valore di adeguatezza ad ogni individuo della popolazione della prossima generazione;
9) controllo di convergenza dell'algoritmo.

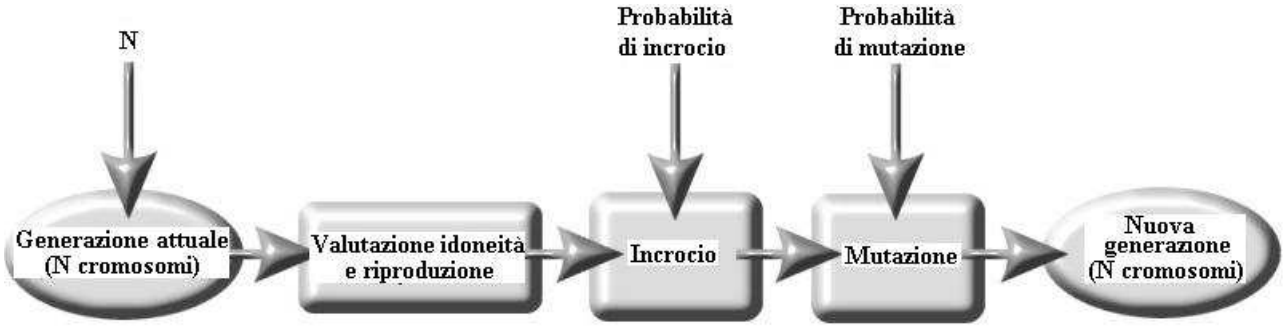

Fig.9 Ciclo base di un algoritmo genetico.

La codifica rappresenta la mappatura dallo spazio dei parametri allo spazio dei cromosomi, trasformando l'insieme dei parametri, che è generalmente composto da numeri reali, in una stringa caratterizzata da una lunghezza finite. I parametri vengono codificati in geni dei cromosomi che permettono all'algoritmo genetico di evolvere indipendentemente dai parametri stessi e quindi dallo spazio delle soluzioni.

Fig.10 Codifica dei parametri soluzione in termini di geni del cromosoma.

Una volta creato il cromosoma, è necessario scegliere il numero di essi che compone la popolazione iniziale. Tale numero influenza fortemente l'efficienza dell'algoritmo nel cercare la soluzione ottima: un numero elevato fornisce una migliore capacità di ricerca nello spazio delle soluzioni ma rallenta la convergenza. Un buon compromesso consiste nello scegliere un numero di cromosomi che varia tra 5 e 10 volte il numero di bit in un cromosoma, anche se nella maggior parte dei casi è sufficiente utilizzare una popolazione di 40-100 cromosomi e che non dipende dalla lunghezza stessa dei cromosomi. La popolazione iniziale può essere scelta casualmente o può essere pre-selezionata secondo caratteristiche specifiche del problema in oggetto.
La funzione obiettivo, o funzione costo, fornisce una misura della idoneità di un dato cromosoma e quindi della idoneità di un individuo all'interno di una popolazione. Poiché la funzione obiettivo opera sui parametri stessi, è necessario decodificare i geni che compongono un dato cromosoma per calcolare la funzione obiettivo di un dato individuo della popolazione.
La riproduzione avviene utilizzando un'opportuna strategia di selezione che utilizza la funzione obiettivo per selezionare un certo numero di candidati ottimali. A ciascun individuo viene assegnato una spazio, su di una ruota di roulette virtuale, che è proporzionale al suo livello di idoneità: più elevata è la sua idoneità e maggiore è lo spazio assegnato sulla roulette e conseguentemente la probabilità di essere selezionato, ad ogni giro di ruota, per far parte della generazione successiva. La roulette virtuale viene ruotata più volte sino ad ottenere una nuova generazione composta dallo stesso numero di individui della popolazione iniziale.
Il processo di ricombinazione seleziona casualmente 2 individui della popolazione riprodotta, detti genitori, incrociandoli per generare 2 nuovi individui, detti figli. La tecnica più semplice per ottenere ciò è denominata "incrocio a punto singolo", nella quale, se la probabilità di incrocio supera una certa soglia, viene selezionato casualmente un punto dei cromosomi genitori: la parte precedente tale punto nel cromosoma genitore A diventa la prima parte del cromosoma figlio A mentre la parte successiva del cromosoma genitore B diventa la parte successiva del cromosoma figlio A. Analogamente per il cromosoma figlio B.
Se la probabilità di incrocio è al di sotto di una soglia prefissata, l'intero cromosoma genitore A viene copiato nel cromosoma figlio A e lo stesso avviene per il genitore B e il figlio B. L'incrocio è utile per riorganizzare geni al fine di produrre combinazioni migliori degli stessi e quindi individui maggiormente idonei per il problema considerato. Il processo di ricombinazione si è dimostrato essere molto importante e si è trovato che lo stesso dovrebbe essere applicato con una probabilità variabile tra 0,6 e 0,8 per ottenere i risultati migliori.
La mutazione viene utilizzata per permettere il recupero di parti dello spazio delle soluzioni che non sono rappresentate dalla popolazione corrente. Se la probabilità di mutazione supera una soglia prefissata, un elemento della stringa che compone il cromosoma viene selezionato casualmente e viene cambiato da "1" a "0" o viceversa, in funzione del suo valore iniziale. Per ottenere i migliori risultati, è stato dimostrato che le mutazioni devono avvenire con probabilità ridotta e variabile tra 0,01 e 0,1.
Il controllo di convergenza può utilizzare criteri differenti come l'assenza di ulteriori miglioramenti della popolazione, il raggiungimento dello scopo desiderato o il raggiungimento di un numero massimo prefissato di generazioni.

Nel nostro caso è stato messo a punto un algoritmo genetico che assicura una riduzione dei costi che supera il 70%.
E' ora necessario codificare il problema in oggetto in un algoritmo genetico estremamente semplice ed efficiente.

5.2 Implementazione del problema

Una volta acquisiti i dati iniziali relativi a:
1) il numero e la posizione dei dispositivi da coprire e l'eventuale velocità richiesta alla connessione;
2) il massimo numero di dispositivi che possono accedere al singolo punto di accesso;
è necessario calcolare il numero iniziale minimo di punti di accesso da utilizzare nel processo di ottimizzazione.
Principalmente si possono verificare 2 situazioni:
1) i dispositivi da coprire sono uniformemente distribuiti in tutta l'area considerata;
2) i dispositivi sono concentrati in poche zone.
Nel primo caso è necessario utilizzare almeno un numero minimo di punti di accesso $N^{PA}_{ST\,min}$ la cui somma delle aree di copertura sia pari all'intera area da coprire (purché il numero di dispositivi da coprire non sia superiore alla somma degli accessi permessi dai punti di accesso, poiché in tal caso il numero dei punti di accesso dovrà essere superiore). Nel secondo caso è necessario utilizzare un numero minimo di punti di accesso $N^{PA}_{ND\,min}$ pari al rapporto tra il massimo numero di accessi sostenibili dal singolo PA e il numero totale di dispositivi da coprire, arrotondando all'intero superiore. E' ovvio che raramente si riuscirà a raggiungere tale situazione poiché i dispositivi sono generalmente distribuiti in maniera tale da non riuscire ad utilizzare, al massimo, gli accessi consentiti dai singoli PA.
In funzione della situazione dominante, uno dei 2 numeri di cui sopra sarà superiore all'altro: il numero iniziale di PA sarà uguale al più grande tra i 2, cioè: $N^{PA}_{\ min} = \max\left(N^{PA}_{ST\,min}, N^{PA}_{ND\,min}\right)$.

Per calcolare $N^{PA}_{ST\,min}$, nota la zona da coprire, la cui superficie è pari a S_T, e nota l'area di copertura (circolare) del punto di accesso (riducendola opportunamente rispetto alla massima portata raggiungibile, al fine di tenere conto delle inevitabili attenuazioni che si manifestano all'interno di luoghi chiusi), la cui superficie è pari a S_{PA}, il numero minimo N^{PA}_{min} di punti di accesso è pari a:

$$N^{PA}_{min} = \text{int}\,(S_T / S_{PA}),$$

dove int () rappresenta l'operazione di arrotondamento, per eccesso, all'intero più vicino.
Il numero così ottenuto è ovviamente ideale, giacché esso può essere raggiunto se i punti di accesso possono essere installati ovunque nell'area di interesse e se il diagramma di copertura dei punti di accesso è caratterizzato da una forma regolare (quadrata, ecc), in maniera tale da poterlo congiungere con la copertura dei punti di accesso vicini evitando sovrapposizioni. In condizioni reali tale numero può diminuire (se i dispositivi che devono utilizzare i punti di accesso non sono equamente distribuiti ma sono concentrati in zone) o può aumentare (se i dispositivi che devono utilizzare i punti di accesso non solo sono distribuiti in tutta la zona considerata ma sono, in uno o più punti, in numero superiore al massimo che può essere gestito dal singolo punto di accesso, richiedendone l'utilizzo di più di uno).
Per tenere quindi conto di eventuali fattori peggiorativi al contorno, data una certa zona da coprire con il servizio wireless, si considera un numero iniziale di punti di accesso pari a $n*N^{PA}_{min}$, (dove n è un parametro maggiore di 1) maggiore del minimo numero N^{PA}_{min} di punti di accesso considerato, lasciando all'algoritmo genetico l'onere di ottimizzare ed eventualmente ridurre il loro numero, in funzione della disponibilità di punti di installazione e del numero di dispositivi da servire.
Una volta definito il numero iniziale $n*N^{PA}_{min}$ di punti di accesso, è necessario definire i parametri che devono essere ottimizzati per ogni punto di accesso, rappresentati principalmente dalla sua posizione cioè dalle sue coordinate.

Poiché non tutti i punti di accesso vengono utilizzati per coprire la zona in considerazione, è necessario aggiungere, per ogni punto di accesso, un'informazione che indica se esso è presente o meno nel punto in considerazione.
Tali considerazioni ci portano a considerare 3 parametri, per ogni punto di accesso, che sono:
1) coordinata x;
2) coordinata y;
3) presenza del punto di accesso.
E' a questo punto necessario definire l'intervallo di variabilità dei parametri in considerazione e la relativa accuratezza per rappresentarli in termini di stringhe binarie.
Per quanto riguarda le coordinate x e y, se si considera una risoluzione di 1 metro e si considera una estensione verosimile per una copertura wireless in un edificio (≈ 1-2 km in strutture molto estese), 11 bit sono sufficienti per rappresentare distanze variabili tra 0 e 2048 metri. Se è necessario considerare un'area più estesa, è sufficiente aggiungere degli altri bit, considerando che ogni bit raddoppia la distanza rappresentabile.
La presenza di ogni punto di accesso nella posizione indicata viene codificata utilizzando un solo bit, dove un "1" binario sta ad indicare che il punto di accesso è presente mentre uno "0" binario indica che il punto di accesso non è presente nella posizione (x,y) considerata.
Vengono quindi utilizzati 3 geni per codificare i parametri di ogni punto di accesso, la cui lunghezza totale è pari a 23 bit. Tali caratteristiche sono riassunte nella tabella seguente.

Parametri del punto di accesso			
Gene	**Caratteristiche**	**Numero di bit**	**Variabilità**
1	Coordinata x	11	0 ÷ 2.048 metri
2	Coordinata y	11	0 ÷ 2.048 metri
3	Presenza del punto di accesso	1	0 ÷ 1

Tavola 1. Parametri del punto di accesso

Ogni cromosoma, o individuo, che rappresenta una soluzione del problema, è composto da una stringa binaria che rappresenta tutti i $n*N^{PA}_{min}$ punti di accesso e i relativi 3 parametri da ottimizzare. La lunghezza totale di ogni cromosoma è quindi uguale a $23* n*N^{PA}_{min}$ bit.
E' a questo punto necessario definire la funzione di ottimizzazione.
Tale funzione deve considerare tutti quelli che sono gli scopi dell'ottimizzazione, rappresentati da:
1) copertura di tutti i N^D dispositivi presenti;
2) riduzione al minimo della sovrapposizione delle aree di copertura dei punti di accesso;
3) posizionamento dei punti di accesso solo nelle zona consentite;
4) non superamento del numero di dispositivi presenti per ogni punto di accesso;
5) rispetto della velocità di trasmissione richiesta da ogni dispositivo.
I primi 2 punti vengono sintetizzati in una funzione opportuna mentre i punti seguenti vengono considerati mediante matrici opportune.
La funzione di ottimizzazione del generico cromosoma C può essere scritta come:

$$f(C) = \frac{\frac{N^D(C)}{N^D}}{\frac{\text{area di sovrapposizione totale}(C)}{S_T} + 1} \tag{6}$$

dove N^D (C) rappresenta il numero di dispositivi coperti dall'attuale soluzione prevista dal cromosoma C, N^{PA}(C) il numero di punti di accesso previsti dal cromosoma C.
La funzione in oggetto tiene in considerazione le prestazioni del cromosoma C (che rappresenta una possibile distribuzione di punti di accesso nell'area in considerazione) in termini di dispositivi

coperti (numeratore), di numero minimo di punti di accesso (primo termine a denominatore) e di minima area di sovrapposizione tra punti di accesso (secondo termine a denominatore). Il termine unitario presente al denominatore è stato aggiunto per evitare possibili divergenze all'infinito quando la funzione di ottimizzazione viene utilizzata per valutare un cromosoma C che distribuisce i PA in maniera tale da non presentare aree di copertura in sovrapposizione.
L'informazione relativa alle zone di installazione consentite (punto 3) viene memorizzata in un opportuna matrice binaria, caratterizzata dalle stesse dimensioni e risoluzione delle coordinate (x,y) dei punti di accesso (cioè 2^{11} x 2^{11}). Ogni elemento della matrice, rappresentante una zona di dimensioni 1 m x 1 m dell'area in oggetto che può essere utilizzata per l'installazione di un punto di accesso viene contrassegnata con un 1 binario, diversamente viene contrassegnata con uno zero binario.
Poiché nella maggior parte dei casi l'area in considerazione è caratterizzata da un'estensione senz'altro inferiore al massimo previsto (2.048 m x 2.048 m), utilizzando tale rappresentazione è possibile disegnare con precisione il confine dell'area in oggetto.
L'informazione relativa al numero di dispositivi presenti nelle varie zone dell'area in oggetto e sulla relativa velocità richiesta viene memorizzata in un opportuna matrice binaria, caratterizzata dalle stesse dimensioni e risoluzione delle coordinate (x,y) dei punti di accesso (cioè 2^{11} x 2^{11} metri). Ogni elemento della matrice, rappresentante una zona di dimensioni 1 m x 1 m dell'area in oggetto, contiene una serie di valori relativi alla velocità richiesta il cui numero è pari quello dei dispositivi wireless da coprire e che sono presenti nella zona in oggetto.
Il controllo sul corretto posizionamento dei punti di accesso viene eseguito ad ogni operazione genetica (riproduzione, incrocio, mutazione), controllando nella matrice delle zone di installazione consentite se le coordinate di ogni punto di accesso del cromosoma oggetto della valutazione sono contrassegnate con un "1" o con uno "0": se ciò avviene il cromosoma viene eliminato.
Il controllo sulla corretta copertura dei dispositivi presenti (in termine di non superamento del massimo numero di dispositivi supportabili dal singolo punto di accesso e in termini di rispetto della velocità richiesta da ogni dispositivo, che diminuisce all'aumentare della distanza del dispositivo stesso dal punto di accesso) viene eseguito ad ogni operazione genetica (riproduzione, incrocio, mutazione), controllando i parametri contenuti nella matrice di copertura siano rispettati dalla disposizione dei punti di accesso prevista dal cromosoma oggetto della valutazione: se ciò non avviene il cromosoma viene eliminato.
Una volta generata la popolazione iniziale in maniera casuale, i cromosomi caratterizzati da punti di accesso che non rispettano le condizioni contenute nelle matrici in oggetto vengono eliminati e la selezione viene eseguita solo sugli individui rimanenti, fino ad ottenere una popolazione caratterizzata dallo stesso numero di individui della popolazione iniziale.
Poiché la popolazione viene inizializzata in maniera casuale, una parte di essa viene solitamente eliminata fin dall'inizio e dopo qualche iterazione si vengono a generare individui maggiormente prestanti che non è più necessario eliminare.
Una volta ricombinata e mutata la popolazione, la funzione di ottimizzazione viene calcolata di nuovo con lo stesso criterio illustrato. Il test di convergenza viene eseguito controllando se la differenza tra il valor medio delle funzioni di ottimizzazione della generazione attuale e il valor medio delle ultime N_G generazioni è inferiore ad una certa percentuale p_{stop}.
Dei buoni risultati, unitamente ad una rapida convergenza, sono stati ottenuti con popolazioni composte 50-70 individui, con parametri di convergenza N_G and p_{stop} uguali rispettivamente a 30 e 0,2.

5.3 Risultati ottenuti

L'algoritmo genetico proposto si è dimostrato essere estremamente versatile nella progettazione ottimizzata delle rete wireless.

Le soluzioni ottimali si ottengono, in genere, dopo un numero limitato di generazioni e che generalmente non supera le 50-70 iterazioni. Il tempo di calcolo dipende fortemente dal numero di punti di accesso poiché ciascuno di essi aggiunge 23 bit ad ogni cromosoma e quindi 23 bit di informazione che deve essere elaborata dall'algoritmo genetico. Il numero di punti di accesso aumenta non solo con le dimensioni della zona considerata ma anche con la riduzione dell'area in cui è richiesta la copertura: maggiore è tale area e maggiore è il numero di punti di accesso e quindi il tempo necessario a raggiungere la soluzione finale ottimale.
Un esempio applicativo è stato sviluppato considerando una zona di 800 x 800 metri e punti di accesso in grado di coprire un'area circolare di diametro pari a 100 metri e in grado di permettere l'accesso, in contemporanea, di 60 utenti al massimo. Per semplificare il problema si considerano punti accesso che consentono la massima velocità di trasmissione delle informazioni a prescindere dalla distanza dagli stessi dispositivi periferici, potendo comunque l'algoritmo considerare anche tale aspetto.
La matrice di distribuzione dei dispositivi è mostrata in figura 11, laddove in ogni quadrato del reticolo (dimensioni grafiche 20 x 20 m, dimensioni di calcolo 1 x 1 m) viene riportato il numero di dispositivi presenti (non riportando la velocità di trasmissione richiesta in quanto considerata costante per tutti).

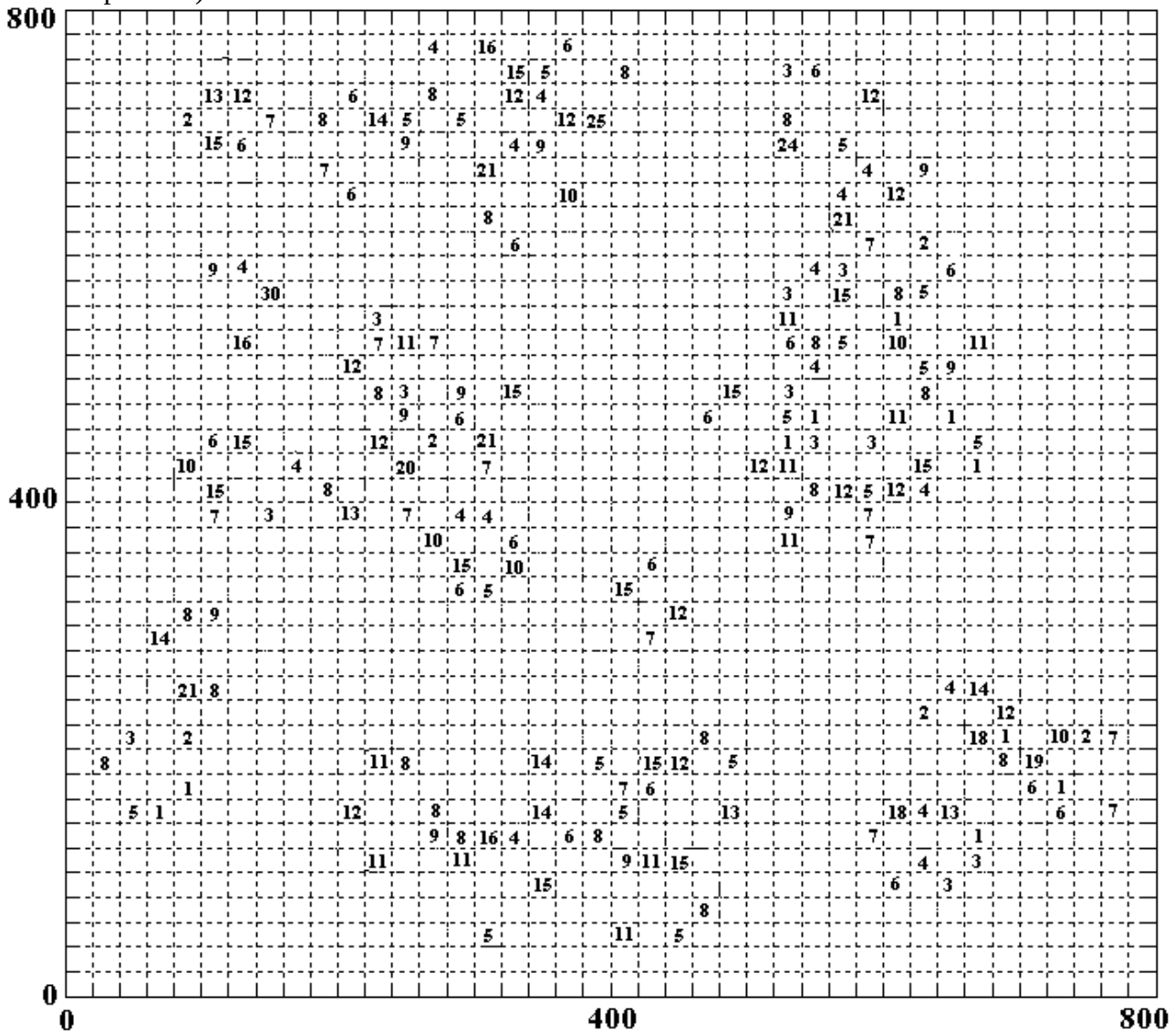

Fig.11 Esempio di matrice di distribuzione dei 1645 dispositivi da coprire. In ogni quadrato, di dimensioni 20 m x 20 m (l'ottimizzazione viene condotta su quadrati di dimensioni 1 m x 1m), è riportato il numero di dispositivi da coprire con punti di accesso che, nel caso in oggetto, può garantire sino a 60 accessi contemporaneamente.

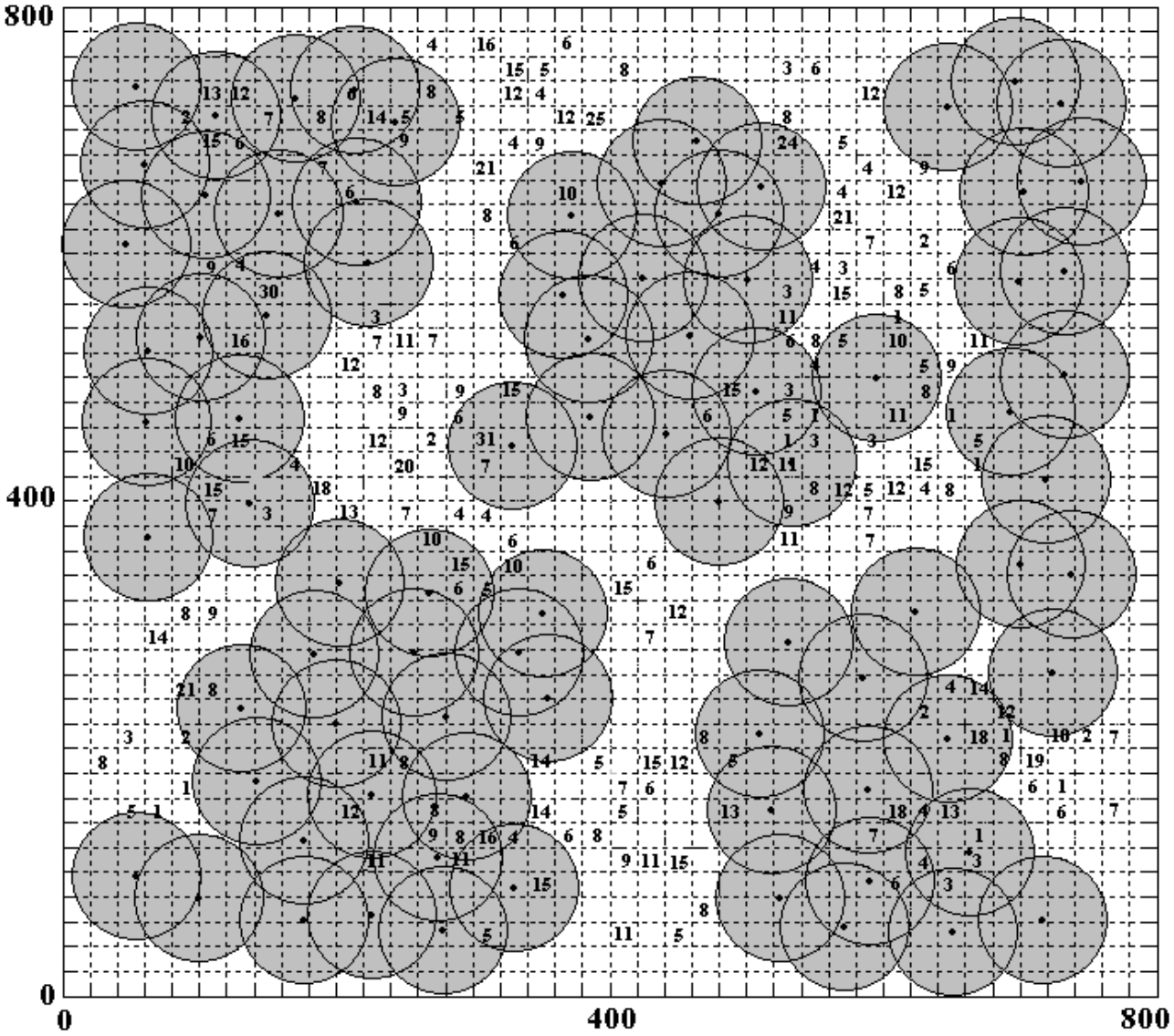

Fig.12 Esempio di distribuzione casuale iniziale del punti di accesso (82, calcolati in base all'intera superficie da coprire) relativamente alla situazione indicata nella figura precedente. Ogni PA può coprire un'area circolare di 100 metri di diametro.

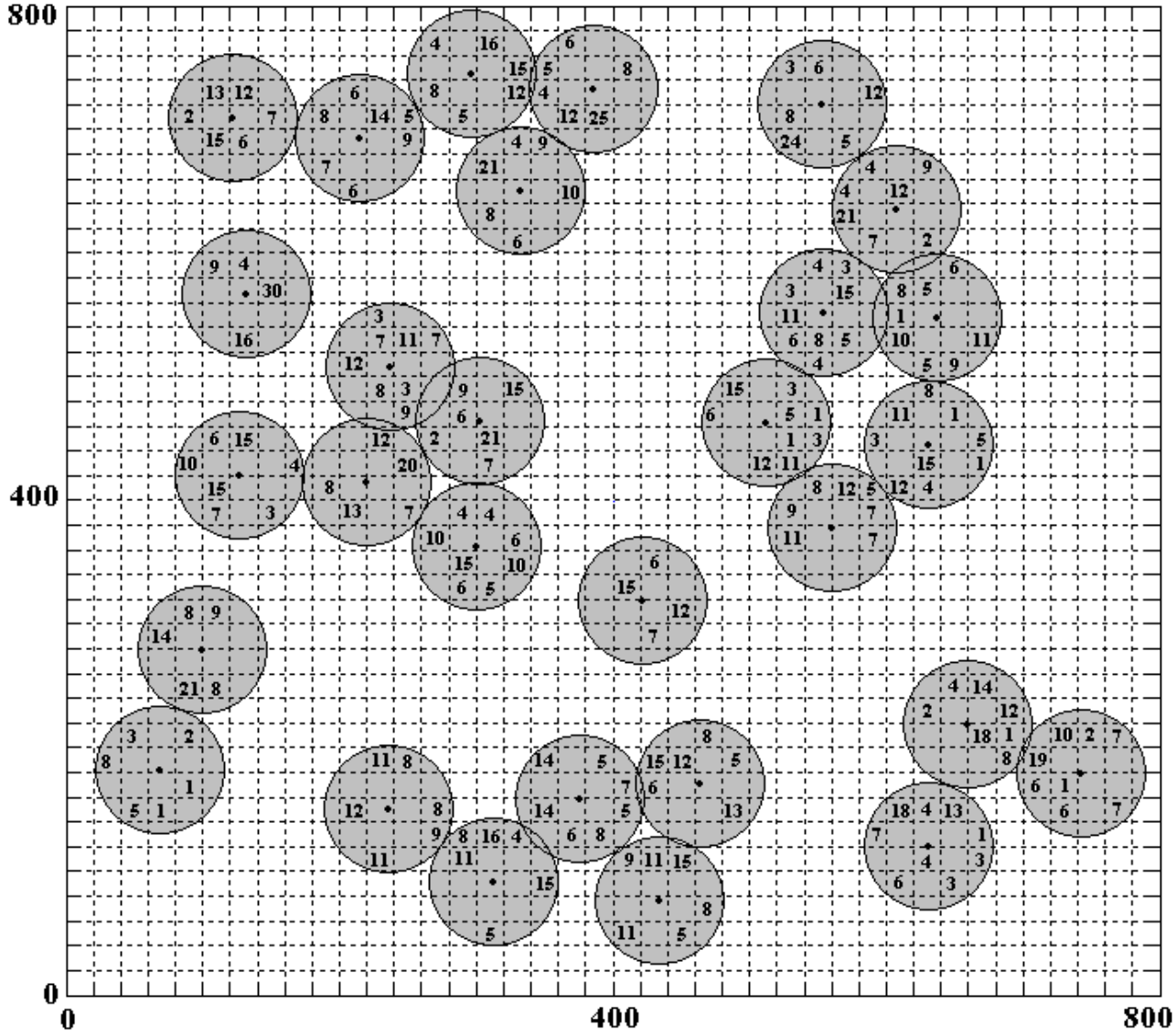

Fig.13 Esempio di distribuzione ottimizzata dei punti di accesso. In questa soluzione ne sono stati ottenuti 29. Le soluzioni ottimizzate sono state ottenute, per il problema in oggetto, dopo 50-70 generazioni. Il numero ottimizzato di PA è pari a 29, prossimo al valore teorico di 28, ottenuto presumendo che ogni PA riuscisse a coprire un numero di dispositivi pari alla sua massima capacità (situazione mai raggiungibile in pratica a causa della distribuzione varia e casuale dei dispositivi all'interno dell'area da coprire).

Tenendo conto della copertura integrale della superficie, si ottiene un numero minimo iniziale $N_{ST\ min}^{PA}$ di punti di accesso pari a 82 mentre tenendo conto del numero di dispositivi da coprire, si ottiene un numero minimo iniziale $N_{ND\ min}^{PA}$ di punti di accesso pari a 28, per cui il numero minimo di punti di accesso è dunque pari a 82 (il maggiore tra i due).
I risultati ottenuti sono mostrati nelle figure 12 e 13.
Come si può vedere, l'algoritmo è riuscito ad ottenere un livello di ottimizzazione tale (solo 29 PA), partendo da un numero minimo di 82 PA necessario a coprire teoricamente l'intera superficie, da arrivare molto vicino al limite teorico di 28 PA (praticamente irraggiungibile poiché la distribuzione dei dispositivi in genere è tale da non riuscire a utilizzare al massimo le possibilità di accesso di ogni singolo PA).

In generale, al fine di valutare le capacità di ottimizzazione dell'algoritmo genetico proposto, sono state simulate varie configurazioni iniziali variando tutti i possibili parametri (numero di dispositivi, area da coprire, massimo numero di accessi al singolo PA, velocità di trasmissione richiesta, ecc.) in maniera casuale al fine di affrontare praticamente tutte le casistiche. In figura 14 è riportato un grafico di sintesi in cui viene indicata la riduzione dei punti di accesso, e quindi dei costi, in funzione del numero di dispositivi da coprire utilizzando PA caratterizzati da differenti valori del massimo numero di dispositivi che possono accedere in contemporanea. Come si può vedere, all'aumentare del numero di dispositivi aumenta la riduzione del numero di PA, poiché l'algoritmo può contare su un maggior numero di PA su cui poter effettuare il processo di ottimizzazione sull'ampia casistica distributiva dei dispositivi nell'area in oggetto. Inoltre, a parità di numero di dispositivi da coprire, si ottengono riduzioni maggiori quando si utilizzano PA che servono un numero inferiore di dispositivi: tale andamento è giustificato dal fatto che, servendo un numero ridotto di dispositivi, i PA possono essere distribuiti sull'area con vincoli meno stringenti e quindi con maggiore precisione, aumentando le prestazioni del processo di ottimizzazione.

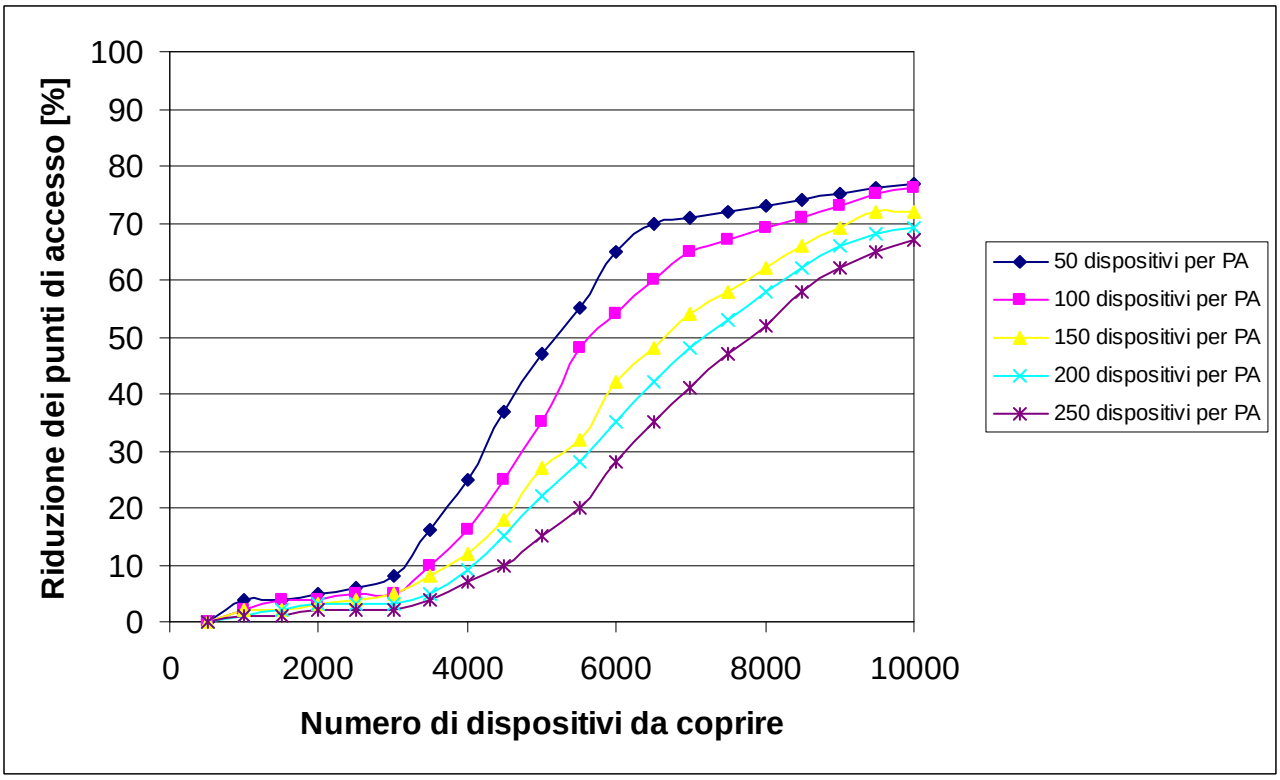

Fig.14 Riduzione percentuale del numero di punti di accesso in funzione del numero di dispositivi da coprire per vari valori del massimo numero di dispositivi per punto di accesso.

6. CONCLUSIONI

Le reti wireless, grazie alle loro caratteristiche, stanno avendo uno sviluppo sempre più rapido e permetteranno di realizzare funzionalità e servizi estremamente innovativi.
Come tutti i sistemi di elaborazione e trasmissione dei dati, esse richiedono una serie di precauzioni ed accorgimenti da adottare al fine di garantire la sicurezza dei dati e delle persone.
Nella progettazione di una rete wireless, soprattutto quando si è in presenza di una rete di una certa consistenza in termini di estensione e di numero di dispositivi che vi accedono, si può ricorrere a tecniche di ottimizzazione genetiche, quale quella che è stata illustrata nel presente lavoro, che permettono di ridurre notevolmente i costi della rete unitamente ad un elevato livello delle prestazioni della stessa.

7. BIBLIOGRAFIA

[1] F.Garzia, G.M.Veca, *L'inquinamento elettromagnetico: fondamenti tecnici e principi normativi*,
[2] T.Bucciarelli, F.Garzia, G.M.Poscetti, *Sicurezza delle Telecomunicazioni*, Il Sole 24 Ore, Milano, in preparazione.
Carocci Faber, Roma, 2002.
[3] Randall K. Nichols, Panos C. Lekkas, *WIRELESS SECURITY – Model, Threats, and Solutions*, Mc Graw Hill Telecom, New York, 2003.
[4] Hitchcock R.T., Patterson R.M., *Radio-Frequency and ELF Electromagnetic Energies: A Handbook for Health Professionals*, John Wiley & Sons, New York (USA), 1995
[5] AA.VV., *ICNIRP, Guidelines for limiting exposure to time-varying electric, magnetic, and electromagnetic fields (up to 300 GHz)*, Health Physics, Vol. 74, n. 4, pp. 494-522 (1998)
[6] AA.VV., *CEI 211-5 (CEI ES 59005), Considerazioni per la valutazione dell'esposizione umana ai campi elettromagnetici (EMF) derivanti da apparecchi di telecomunicazione mobile (MTE) nel campo di frequenza 30 MHz – 6 GHz*, CEI Comitato Elettrotecnico Italiano, Milano, 1999
[7] AA.VV., *CEI 211-7, Guida per la misura e per la valutazione dei campi elettrici e magnetici nell'intervallo di frequenza 10 kHz – 300 GHz, con riferimento all'esposizione umana*, CEI Comitato Elettrotecnico Italiano, Milano, 2001
[8] Legge 22 febbraio 2001, n.36 - Legge quadro sulla protezione dalle esposizioni a campi elettrici, magnetici ed elettromagnetici. (G.U. del 7 marzo 2001, n.55).
[9] Decreto del Presidente del Consiglio dei Ministri 8 luglio 2003 - Fissazione dei limiti di esposizione, dei valori di attenzione e degli obiettivi di qualità per la protezione della popolazione dalle esposizioni a campi elettrici, magnetici ed elettromagnetici generati a frequenze comprese tra 100 kHz e 300 GHz . (G.U. n. 199 del 28-8-2003).
[10] Decreto del Presidente del Consiglio dei Ministri 8 luglio 2003 - Fissazione dei limiti di esposizione, dei valori di attenzione e degli obiettivi di qualità per la protezione della popolazione dalle esposizioni ai campi elettrici e magnetici alla frequenza di rete (50 Hz) generati dagli elettrodotti. (G.U. n. 200 del 29-8-2003).
[11] Raccomandazione del Consiglio dell'unione Europea relativa alla limitazione dell'esposizione della popolazione ai campi elettromagnetici con frequenza da 0 Hz a 300 GHz. (G.U. Comunità Europee 30 luglio 1999, L 199/62).
[12] Direttiva 2004/40/EC del Parlamento Europeo e del Consiglio, del 29 Aprile 2004, sulle norme minime per la salute e sicurezza in relazione all'esposizione dei lavoratori ai rischi derivanti dagli agenti fisici (campi elettromagnetici) (diciottesima Direttiva particolare ai sensi dell'articolo 16(1) della Direttiva 391/89/EEC). (G.U. UE L184 del 24 maggio 2004).