2. OVERVIEW DEL PROTOCOLLO IEEE 802.11 E DEL PROTOCOLLO DI ROUTING USATO

2.1 LE RETI WIRELESS

La rapida evoluzione della tecnologia di trasmissione "via etere" ha dato un nuovo impulso allo sviluppo dei sistemi *wireless* (senza fili), dettato anche dai diversi vantaggi che essi possono avere rispetto alle reti cablate: flessibilità nel posizionamento delle stazioni, facilità di installazione e riconfigurazione, possibilità di avere stazioni mobili.
Si cerca, quindi, di sviluppare sistemi con prestazioni analoghe alle reti *wired* (cablate) e con i vantaggi delle wireless, cercando di risolvere i problemi di efficienza, sicurezza e robustezza della trasmissione, che l'assenza del "filo" inevitabilmente porta.
Le reti wireless possono essere classificate in base alla copertura geografica ed alla tecnologia su cui sono basate.

a) In base all'ambiente
Le reti wireless possono operare in quattro distinti ambienti: *in-building, ambiente di campus, MAN (metropolitan area networks), WAN (wide area networks).*
Quando la collocazione delle stazioni all'interno di un edificio varia molto raramente, si parla di ambiente *in-building tethered.* Questo segmento di mercato copre, ad esempio, i vecchi edifici dove è difficile o troppo costoso installare nuove reti cablate. Nell'ambiente *in-building non-tethered,* invece, viene sfruttata la caratteristica di mobilità delle reti wireless. Si fornisce cioè una connessione tra un computer portatile e i servizi di una LAN, mentre l'utente si può spostare liberamente nell'edificio.
Si parla di *ambiente di campus* quando vi sono più edifici vicini compresi in un'area limitata. Anche in questo caso le reti wireless rispondono alle esigenze di connessione fra gli edifici e di mobilità delle singole stazioni all'interno del campus.
Le reti wireless a largo raggio (MAN e WAN) sono in grado di trasmettere dati in un'area metropolitana o in un'intera nazione. I principali tipi di reti wireless "wide-

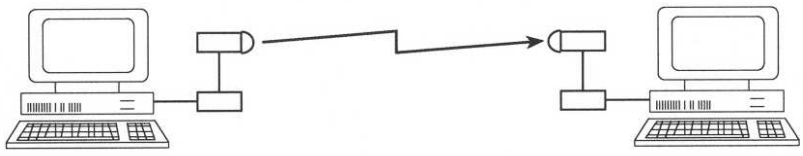
area" si basano sulle reti radio pubbliche e private a commutazione di pacchetto e sulle reti cellulari a commutazione di circuito.

b) In base alla tecnologia

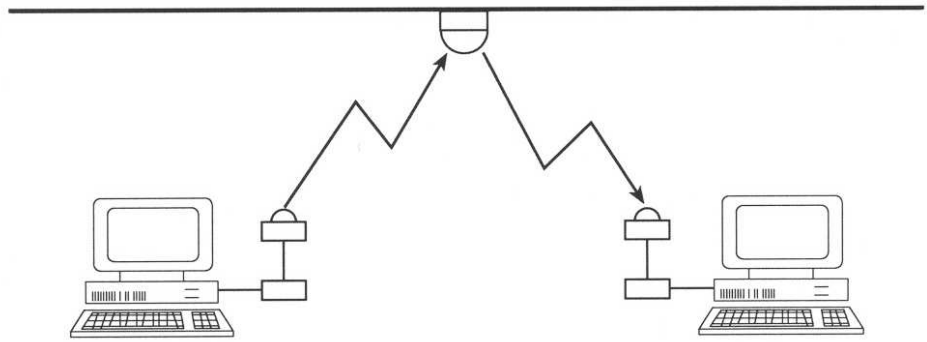
La scelta della tecnologia per la realizzazione di una rete wireless è ovviamente strettamente legata alla topologia ed alla tipologia della rete stessa.
Attualmente le tecnologie wireless sono: *powerline, ottica, radiofrequenze, microonde, cellulare e satellitare.*

Tecnologia powerline. La tecnologia *"powerline*" fa uso dei comuni fili della corrente all' interno di un edificio per trasmettere il segnale. In assenza di interruzioni (ad esempio trasformatori) nella rete elettrica, è possibile stabilire un link di comunicazione tra chiamante e ricevente mediante onde convogliate. A causa della gran quantità di rumore presente sui fili e del tipo di mezzo usato per trasmettere la corrente, la velocità di trasmissione è generalmente bassa, tra 1.2 e 38.4 Kb/s. Il pregio maggiore di questa tecnologia è la relativa ecomicità.

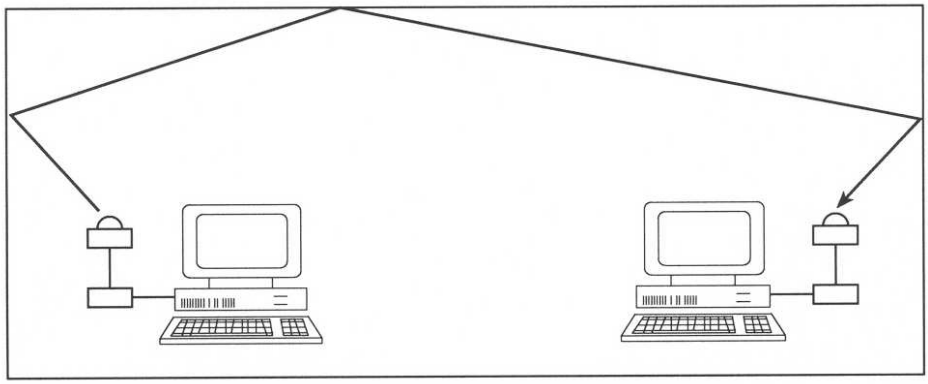
Tecnologia ottica. La tecnologia *"ottica"* utilizza le lunghezze d' onda nell' infrarosso per trasmettere l' informazione. In una wireless LAN a raggi infrarossi (IR), ogni stazione è equipaggiata con un *transceiver* dotato per la trasmissione di un LED *(Light Emitting Diode)* che emette luce a raggi infrarossi e, per la ricezione, di un fotodiodo, operanti alla medesima lunghezza d' onda. Si hanno a disposizione tre modi di radiazione degli IR per l' interscambio di dati tra le stazioni: *punto-punto, semi-diffusione* e *diffusione totale*. Nella modalità punto-punto, due transceiver devono essere perfettamente allineati per potersi illuminare reciprocamente con un fascio di luce IR. Lo scambio di dati tra le stazioni avviene modulando il fascio di infrarossi. Questa tecnica va bene per la realizzazione di LAN di tipo Token Ring, realizzando l' anello fisico mediante una sequenza circolare di link punto-punto. Con trasmissione laser-IR unidirezionale si possono coprire distanze anche di alcuni Km (fig. 2.1 a). Nella modalità di radiazione per semi-diffusione (fig. 2.1 b), il segnale ottico emesso da una stazione viene captato da tutte le altre, realizzando così delle connessioni punto-multipunto o broadcast.



a) Propagazione Punto-Punto



b) Propagazione per Semi-diffusione (con satellite)



c) Propagazione per diffusione totale

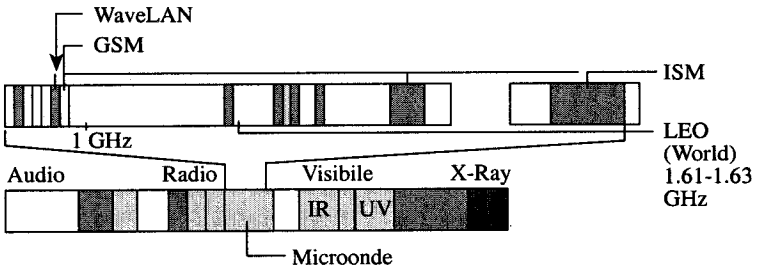
Figura 2.1 Modalità di radiazione dei raggi infrarossi.

Si sfrutta una superficie riflettente sulla quale vanno a collimare i fasci IR provenienti dai transceiver di tutte le stazioni: con questa configurazione, per il principio di diffusione della radiazione luminosa, il raggio proveniente da una stazione verrà riflesso verso tutte le altre rendendo così possibile una comunicazione di tipo broadcast.
La superficie riflettente può essere passiva, di solito il soffitto della stanza ove ha sede la LAN, oppure attiva, cioè realizzata mediante un dispositivo, detto *satellite*, che serve ad amplificare e rigenerare il segnale ottico prima di effettuarne il broadcast (funziona praticamente come un repeater). La diffusione passiva richiede più potenza nei transceiver delle stazioni, ma consente una più facile installazione della rete dal momento che non occorre il posizionamento del satellite.
Nella radiazione per diffusione totale (fig. 2.1 c) la potenza ottica emessa da un transceiver deve essere tale da consentire al raggio di diffondersi per tutto il volume della stanza dopo una serie di riflessioni multiple sui muri. Questo segnale verrà captato da qualunque altra stazione all' interno dello stesso spazio, senza la necessità di alcun particolare orientamento di quest' ultima. La presenza di riflessioni, tuttavia,

limita la massima velocità di trasmissione a causa dell' interferenza dovuta al fenomeno del *multipath* (per cui un segnale può essere ricevuto attraverso più cammini caratterizzati da differenti ritardi).
Le modalità di radiazione per semi-diffusione e diffusione, dal momento che consentono una comunicazione broadcast, sono adatte all'implementazione di reti di tipo Ethernet. In particolare, la prima permette la realizzazione di reti con stazioni fisse, la seconda con stazioni mobili.
Le reti wireless ad IR possono essere installate solo nell' ambito di un' unica stanza, in quanto le stazioni devono trovarsi in linea ottica nel caso di link punto-punto, oppure avere una superficie riflettente comune, nel caso dei link punto-multipunto ottenuti per semi-diffusione, oppure devono essere situate tutte nello stesso volume, se si usa la diffusione totale. È inoltre difficile garantire la compresenza di più network isolate poiché, anche se si possono utilizzare nella trasmissione diverse frequenze portanti, la possibilità di passare da una frequenza ottica ad un' altra è difficile e costosa da ottenere. Nonostante queste limitazioni, gli IR offrono notevoli vantaggi come, ad esempio, l' immunità alle interferenze elettromagnetiche (EMI), l' intrinseca sicurezza della trasmissione (perché in ambiente molto limitato) e l' assenza di licenze da parte delle PTT (in Italia, il Ministero delle Poste e Telecomunicazioni) per le installazioni.
La tecnologia dei raggi infrarossi è sicuramente la più matura tra quelle utilizzate nell' ambito delle reti wireless in quanto è da una ventina d' anni che la trasmissione dati mediante IR è realizzata mediante apparecchiature commerciali.

Tecnologia delle radio frequenze. L' utilizzo delle *"radiofrequenze"* è ostacolato dal fatto che la complessità dei *radio-transceíver* cresce con il crescere della frequenza di trasmissione, ed il costo è, in generale, più elevato del corrispettivo IR, anche se può essere in parte abbattuto sfruttando la componentistica ad alta diffusione (ad esempio la telefonia cellulare). Uno dei vantaggi di questa tecnologia risiede nella possibilità di coprire aree estese, che superano i limiti di un singolo ambiente. Con una trasmissione a bassa potenza (<1W) si possono coprire distanze di circa 1 Km all' aperto e 50-100 m al chiuso, a seconda del numero di pareti da attraversare. Un ulteriore vantaggio della trasmissione RF consiste nella possibilità di permettere la compresenza di più network isolate, mediante la variazione della frequenza della portante trasmissiva.
La scelta delle frequenze e della modalità di trasmissione è strettamente legata alle esigenze di progetto e alla regolamentazione presente nei diversi Paesi.
Nel 1985 il Federal Communication Commitee (FCC) assegnò tre bande di frequenza, nel campo delle microonde, alle trasmissioni senza licenza con potenza massima di 1 W. Queste bande, 902 - 928 MHz, 2400 - 2483 MHz e 5725 - 5850 MHz, erano precedentemente disponibili per applicazioni Industriali, Scientifiche e Mediche, da ciò il nome *bande ISM* (figura 2.2). Dal 1985, avendo a disposizione le bande ISM, alcuni costruttori di prodotti di networking iniziarono a progettare dei dispositivi per wireless LAN operanti a tali frequenze. Essendo bande piuttosto strette e, non necessitando di licenza, aperte a chiunque volesse utilizzarle (con il solo vincolo della potenza massima di 1 W), si arrivò ben presto ad un livello di interferenza inammissibile e ciò portò ITCC a imporre l' utilizzo della tecnica di modulazione *Spread Spectrum (SS)* per la trasmissione in banda ISM.

La tecnica di modulazione Spread Spectrum è nata alla fine della Seconda Guerra Mondiale per scopi militari: serviva per prevenire l' interferenza durante il controllo di armi telecomandate. Consiste nel distribuire l' energia di un segnale a banda limitata su di una banda molto più ampia al fine di abbassarne notevolmente la densità spettrale di energia. L' idea è quella di ottenere un segnale con un livello energetico al di sotto di quello del rumore ambientale, che, come è noto, è costante e a banda pressoché illimitata, per renderlo non intercettabile. In ambito civile lo scopo è quello di minimizzare le interferenze che inevitabilmente si hanno tra più segnali che condividono la stessa banda.



Servizio	Frequenze
Radio AM	535-1605 KHz
Telefono Cordless	46-47 48-49 MHz
Radio FM	88-108 MHz
TV USA	54-88 174-216 470-806 MHz
ARDIS	855-865 MHz
Telefono Cellulare USA	826-849 860-894 MHz
Telefono Cellulare Europa	872-905 917-950 MHz
RAM (Mobitex)	896-902 MHz
NCR (WaveLAN)	902-928 MHz
GSM (Telefono Digitale)	890-915 935-960 MHz
LEO (satellite)	1.97-1.98 GHz
Banda ISM	902-928 2400-2480 5150-5250 MHz
California Microvawe	2.40-2.48 GHz
Forni a microonde	2.43-2.46 GHz
Motorola (Altair)	18.8-19.2 GHz

Figura 2.2 Utilizzo dello spettro elettromagnetico per le telecomunicazioni.

Esistono due tecniche per ottenere un segnale Spread Spectrum da uno a banda limitata: *Direct Sequence Spread Spectrum (DSSS), e Frequency Hopping Spread S*pectrum (FHSS).

1) DSSS: il segnale trasmesso è modulato con una sequenza pseudo-casuale binaria *(chipping sequence*, figura 2.3). Per trasmettere un 1 si invia la sequenza di chipping positiva, per trasmettere uno zero la sequenza negativa. La velocità relativa tra frequenza pseudo-casuale e trasmissione (cioè la lunghezza della sequenza di chipping) è, nel caso commerciale, compresa tra 10 e 100, mentre in quello militare tra 1000 e 10000. Il ricevitore per ricostruire l' informazione esegue l' EXOR tra segnale e sequenza pseudo-casuale: se sono in fase, il risultato è il segnale trasmesso.

Mediante tale tecnica si trasmette ancora con una singola portante a frequenza fissa, come nelle trasmissioni tradizionali, ma, grazie alla sequenza di cipher e allo schema di modulazione usato, la potenza del segnale si distribuisce su uno spettro più ampio.

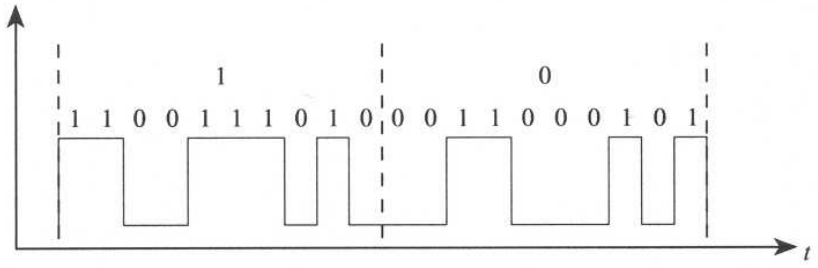


Figura 2.3 Esempio di trasmissione DSSS.

2) FHSS: tutta la banda disponibile è divisa in un insieme di canali di uguale larghezza. La trasmissione avviene per un certo periodo di tempo *(dwell t*ime) su un canale poi passa su un altro seguendo una precisa sequenza *(hopping sequence, figura* 2.4). Tale sequenza può essere predeterminata o trasmessa anch'essa insieme ai dati, comunque deve essere tale da garantire un ugual uso di tutti i canali di trasmissione.

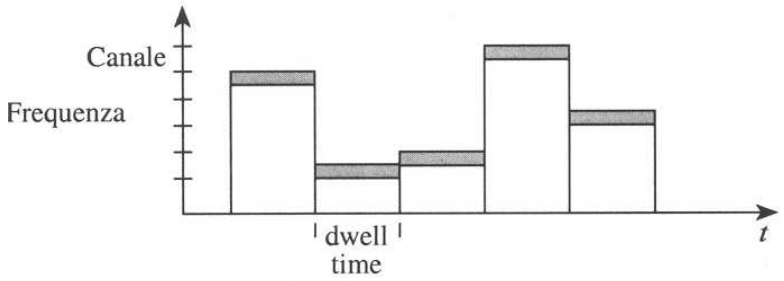


Figura 2.4 Esempio di trasmissione FHSS.

Quando il dwell time è minore del tempo di bit si parla di *fast-frequency hopping*, mentre quando il dwell time è (molto) maggiore del tempo di bit si parla di *slow-frequency hopping.* I sistemi basati sul primo tipo sono più costosi e ad alto consumo ma, dal momento che ogni bit viene trasmesso su molti canali, offrono il vantaggio di una maggiore tolleranza alla distorsione selettiva in frequenza. Lo slow-frequency hopping, invece, permette una maggiore facilità nel sincronismo dell' hop.

La scelta della banda in cui operare dipende dalle esigenze di lavoro. In tabella 2.1 è riportato un confronto fra le caratteristiche delle bande ISM. Attualmente la più utilizzata ed affollata è la seconda (2.4-2.483 GHz), che presenta vantaggi di ampiezza, di universalità (è utilizzabile senza licenza in tutto il mondo) e di costo (la componentistica può in parte sfruttare la tecnologia al silicio, di basso costo).

	I	II	III
Frequenze	902-928	2.4-2.4835	5.725-5.850
Larghezza di banda	26 MHz	83.5 MHz	125 MHz
Necessità di licenza FCC	No	No	No
Utilizzabilità	USA/Canada	Ovunque	USA/Canada
Costo tecnologia	Basso (Si)	Basso/medio (Si, GAAs)	Alto (GaAs)
Dimensione canali FH	0.5 MHz	1 MHz	1MHz
Numero canali F11 (USA)	Elevato	Basso	Quasi nullo
Sorgenti di interferenza (USA)	Utilizzatoti primari-molte LAN-molti non-Spread Spectrum	Utilizzatori primari poche LAN- pochi non-SS- forni a microonde	Utilizzatoti primari pochissime LAN pochissimi non-SS
Sorgenti di interferenza	Telefoni cellulari		Alcuni radar

Tabella 2.1 Confronto fra le bande ISM.

Tecnologia delle microonde. Alcuni costruttori hanno realizzato dei dispositivi per wireless LAN operanti in bande a loro licenziate. Uno dei più importanti è Motorola, che ha introdotto il sistema Altair, una rete Ethernet a "*microonde"* operante a 10 Mb/s. Esso si compone di *Altair* Plus II, per applicazioni wireless in-bulding, e *Altair VistaPoint*, bridge wireless per collegare LAN distinte. Entrambi i prodotti sfruttano la speciale tecnologia in radiofrequenza di Motorola che funziona a 18 GHz a basso consumo. Inoltre, Altair Plús Il offre capacità di network management con *l'Altair ExtendedMIB* (Management Information Base), che permette il pieno controllo remoto della rete (wireless e non) da una singola stazione. Il sistema Altair Plus II fornisce un throughput massimo di 5.7 Mb/s. L' Altair VistaPoint è un bridge wireless per collegare LAN cablate o wireless anche tra piani o edifici diversi purché non troppo distanti: permette la comunicazione di segmenti di LAN a una distanza di 15 m oppure, nella versione "1ong-range", fino a 1.2 Km negli USA e 2.1 Km nella maggior parte degli altri paesi. Entrambi i bridge VistaPoint offrono una capacità trasmissiva massima di 5.3 Mb/s. In Europa è stata presentato da Olivetti Systems & Networks una wireless LAN basata sullo standard Digital European Cordless Telecommunications (DECT), analoga al sistema Altair: si tratta di un hub collegato in topologia stellare con dei satelliti mediante link a microonde in modulazione di frequenza. Le frequenze usate sono nell' intorno dei 18 GHz con potenze molto ridotte.

Tecnologia cellulare. Dal momento che le frequenze trasmissive sono una risorsa limitata, è meglio riutilizzarle il più possibile. È questa la filosofia che sta alla base della tecnologia *"cellulare"*. In pratica si fa in modo che aree geografiche adiacenti (celle) usino insiemi di frequenze disgiunti. Le celle non adiacenti possono quindi

riutilizzare le stesse frequenze senza interferenza. Quando ci si sposta *(roaming)* da una cella ad un' altra, automaticamente, in modo trasparente, viene garantito il passaggio all' insieme di frequenze della nuova cella (funzione di*handover).* Vi possono essere sistemi di trasmissione cellulare dedicati alla trasmissione dati oppure condivisi con la telefonia.
Un esempio di sistema misto è CDPD *(Cellular Digital Packet Data),* sviluppato da IBM, McCaw Cellular Data, Baby Bells ed altri. Esso permette di trasmettere pacchetti di dati saltando da un canale cellulare ad un altro per sfruttare i vuoti in mezzo al traffico vocale. Infatti tutte le chiamate cellulari devono avere un periodo di silenzio di 5÷10 secondi dopo la sconnessione per il reset della linea stessa; in questo intervallo i dati possono essere inviati a una stazione di base e poi al ricevitore. CDPD offre velocità fino a 19.2 Kb/s.
Nel caso di trasferimenti di file lunghi può essere invece utile acquisire un canale cellulare fino al completamento della trasmissione: è questa la via seguita da CSC *(Circuit Switched Data)* di McCaw Cellular Communications.

Tecnologia satellitare. Le caratteristiche principali delle trasmissioni mediante *"satellite"* sono l' estensione della copertura geografica ed il funzionamento intrinsecamente *broadcast.* I satelliti sono classificati in tre grosse categorie: *geosincroni* (GEO), *Medium Earth Orbit (MEO), e Low Earth Orbit* (LEO).

I sistemi geosincroni sono posizionati in orbita equatoriale geostazionaria, a 36.000 Km di quota. La distanza dalla terra determina il ritardo di trasmissione, che nei GEO e' di circa 255 ms (round trip time) e la potenza di trasmissione, che, essendo molto alta, impedisce il loro utilizzo con trasmettitori portatili. Tre satelliti GEO sono sufficienti per la copertaura globale della terra (poli esclusi). Un satellite GEO e' sempre in visione per un utente terrestre.
I satelliti MEO sono posizionati a circa 10000 Km di altezza ed il ritardo di trasmissione a loro associato e' di circa 110-130 ms. La copertura globale della terra si ottiene con una constellazione di 10-15 satelliti.

I satelliti LEO sono posizionati in una fascia che va dai 500 ai 2000 Km di altezza. Al di sotto dei 500 Km di altezza, i satelliti sarebbero fortemente danneggiati dal pulviscolo atmosferico; al di sopra dei 2000 Km la fascia di radiazioni di Van Allen impedirebbe l'utilizzo dei satelliti. A seconda della quota della costellazione, dai 50 ai 200 satelliti sono necessari per la copertura globale della terra. Ogni satellite LEO rimane in visione di un utente terrestre per pochi minuti, per cui e' necessario a terra un sistema di tracking per seguire il movimento del satellite.

La tabella 2.2 a pagina seguente riassume le principali caratteristiche delle tecnologie analizzate.

Tipo di WLNA	***Velocità***	***Estensione***	***Vantaggi***	***Svantaggi***
Powerline	da 1.2 a 38,4 Kb/s	da 5 m ad alcuni Km	Economicità	Elevato rumore nella trasmissione
Infrarossi	da 230 Kb/s a 16 Mb/s	da 30 m a200 m	-Flessibilità di installazione riconfigurazione e manutenzione -Tecnologia consolidata e sicura -Velocità al pari delle reti cablate -Immunità alla interferenze EMI -Assenza di licenza FCC -Buona mobilità	-In alcune implementazioni è indispensabile il perfettoallineamento delle stazioni -LAN confinate in un unico volume -Problemi di interferenza con luce ambientale forte -Difficile comprensenza di network isolate
Radio frequenza	2 Mb/s	da 250 m a3 Km	-Flessibilità di installazione, riconfigurazione manutenzione -Penetrazione dei muri portanti -Assenza di licenza FCC -Possibilità di compresenza di network isolate	-Suscettibilità alle interferenze EMI -Velocità ridotta rispetto alla e LAN cabalte -Esposizione utenti a radiazioni elettromagnetiche -Scarsa mobilità
Microonde	10 Mb/s	80 m	-Flessibilità di installazione, riconfigurazione manutenzione -Velocità al pari delle reti cablate -Immunità alla interferenze EMI	-Propagazione del segnale limitata -Esposizione utenti a radiazioni elettromagnetiche -Licenza FCC
Cellulare	fino a 19.2 Kb/s	Rete cellulare	-Uso della rete cellulare telefonica preesistente -Tecnologia ad alta diffusione	-Possibili interferenze in radiofrequenza -Ritardi elevati
Satellitare		Migliaia di Km	-Trasmissione broadcast -Ampia copertura del territorio	-Costi iniziali elevati -Ritardo di trasmissione -Sensibile all'attenuazione del segnale dalla banda Ku in su.

Tabella 2.2 WLAN - Analisi comparata.

Le bande più popolare per la comunicazione satellitare sono:
a) la "banda C": 6 GHz per l' uplink (Terra-satellite) e 4 GHz per il downlink (satellite-Terra);
b) la "banda Ku": 12 GHz per l' uplink (Terra-satellite) e 14 GHz per il downlink (satellite-Terra).
La banda Ka (20-30 GHz) e' per adesso usata solo sperimentalmente. Da queste frequenze in poi la qualita' del segnale trasmesso e' fortemente influenzata dalle condizioni atmosferiche che, se non buone, provocano un forte attenuazione del segnale. Tale attenuazione del segnale (*fade*) deve essere controbilanciata con speciali contromisure (tecniche di *fade countermeasure*).

2.2 STANDARDIZZAZIONE DELLE WLAN

Esistono molteplici organizzazioni che si stanno occupando dello sviluppo di standard sulle wireless LAN (WLAN). Sono coinvolte in tali attività entità nazionali, continentali e mondiali. Quella che segue è una panoramica sui lavori svolti dai vari enti di standardizzazione.

A livello mondiale
Il Taskgroup 811 del Comité Consultatif International *des R*adiocomunications (CCIR), che è una parte dell' International Communication Union (ITU), è al lavoro su un progetto denominato *Future Publie Land Mobile Telecommunication System* (FPLMTS), il cui scopo è di ottenere una distribuzione valida a livello mondiale delle frequenze per le comunicazioni numeriche radiomobili, sia per fonia sia per i dati, fino a 20 Mb/s.
Nel 1992, durante la Worldwide Administrative Radio Conference (WARC 92), sono state assegnate al progetto FPLMTS due bande di frequenza, 1885-2025 MHz e 2110-2200 MHz, ed è inoltre stata approvata una risoluzione che stabilisce le linee guida per l' implementazione di sistemi FPLMTS ed invita il CCITT ad implementare tale tecnologia sfruttando le reti attualmente esistenti.

Europa
Nel marzo del 1992, il *Technical Committeefor Radio Equipment andSystems* (TC RES), una componente dell' European Telecommunications *Standard I*nstitute (ETSI), ha approvato la versione definitiva del Digital *European C*ordless Telecommunications Standard (DECT). Questo standard è mirato alla telefonia e supporta dieci canali multiplati in frequenza (FDM) sui quali sono instradati 12 canali bidirezionali multiplati nel tempo (TDM) da 32 Kb/s. I canali possono essere usati separatamente per veicolare il traffico vocale, oppure in modo combinato ottenendo un unico canale numerico avente una banda aggregata di 7.68 Mb/s.
Due sottocomitati tecnici dell' ETSI hanno inoltre cominciato a lavorare su progetti concernenti le wireless LAN:

1) il comitato RES2 si occupa di uno standard per sistemi di medie prestazioni operanti nella banda ISM intorno ai 2.4 GHz con tecnica di modulazione Spread Spectrum;
2) il comitato RES10 si occupa invece di uno standard per HighPerformance European Radio Local Area Network (HIPERLAN), una wireless LAN ad elevate prestazioni, tra i 10 ed i 20 Mb/s, operante in una banda di 150 MHz allocata nell' intorno dei 5.2 GHz.

Giappone
Il *Telecommunications Technology Group* (TTG), un comitato consultivo del *Ministry for Post and Telecommunications* (MPT), che si occupa della regolamentazione e dell' assegnazione delle frequenze, ha raccomandato l' utilizzo delle bande 1215-3400 MHz e 17.7 - 21.1 GHz per le applicazioni di tipo wireless LAN. Basandosi sugli orientamenti offerti dal TTG, il *Research and Development Centerfor Radio Systems* (RCR), un altro organismo del MPT, fra gli obiettivi del quale c' è lo studio delle architetture dei sistemi per le wireless LAN, nel 1992 ha redatto una specifica per LAN a medie prestazioni operanti nella banda 2.4-2.5 GHz con modulazione Spread Spectrum. RCR è anche al lavoro su una specifica per LAN ad elevate prestazioni, 10 Mb/s, nella banda 18-19 GHz.

Stati Uniti
Negli Stati Uniti l' organizzazione che si occupa della standardizzazione delle wireless LAN è lo FIEEE Working Group for wireless LAN, denominato IEEE 802.11. Al lavoro di questo gruppo è dedicato il paragrafo successivo.

2.3 LO STANDARD IEEE 802.11

L'architettura della rete *wireless* 802.11 è costituita da diversi componenti interagenti che supportano la mobilità delle stazioni in maniera trasparente ai livelli superiori dello stack protocollare.
Il blocco fondamentale della WLAN è il ***Basic Service Set*** (**BSS**), definito come un gruppo di stazioni, fisse o mobili, collocate geograficamente all'interno di una cella, che possono stabilire connessioni dirette o con l'ausilio di strutture intermedie.
Nel primo caso, nel quale le stazioni comunicano direttamente l'una con l'altra, si parla di ***Independent*** **BSS** (**IBSS**): la rete *Ad Hoc* ne è un esempio (fig. 2.5).
Nel secondo caso, ovvero in una rete con infrastruttura, il BSS comprende, oltre alle stazioni, anche un ***access point*** (AP) che permette di connettere le stazioni all'interno della medesima cella.

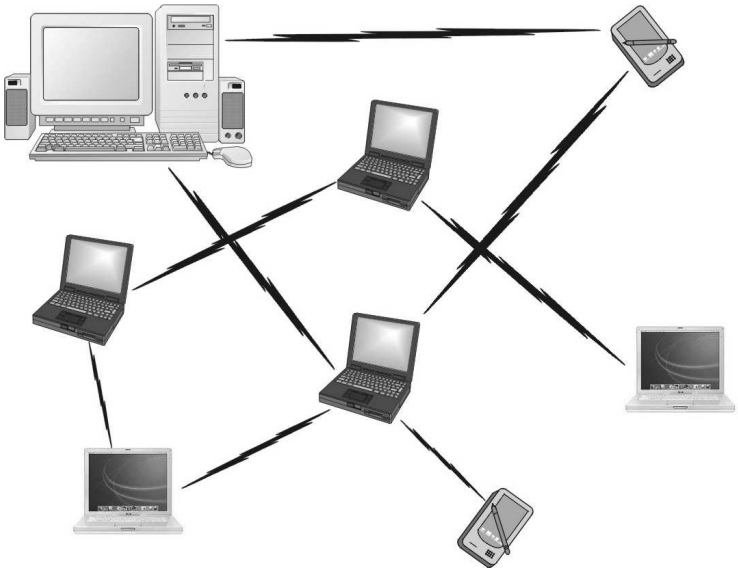
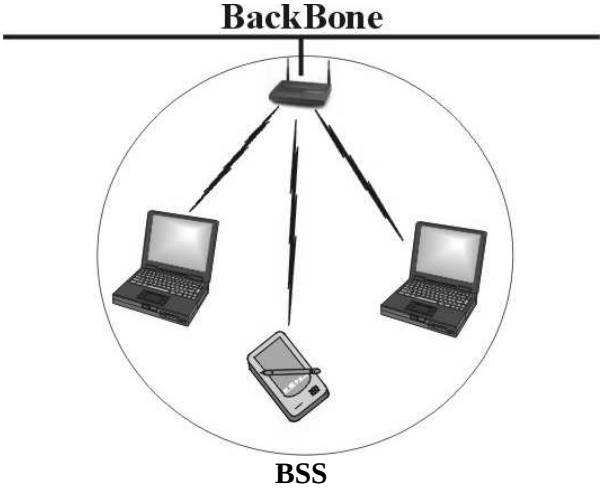


Figura 2.5 Schema di una rete Ad Hoc

Normalmente, una Infrastructure Network è formata da diverse celle e l'architettura di interconnessione tra i diversi BSS è il **Distribuition System** (**DS**)**,** una sorta di backbone network responsabile del trasporto a livello MAC di un MAC Service Data Unit (MSDU). Il DS è indipendente dall'architettura della rete 802.11 e pertanto può essere indifferentemente una rete Wired; Ethernet, Token Ring, FDDI, o un'altra rete Wireless. L'intera WLAN, comprendente le varie celle, i loro rispettivi Access Points ed il Distribuition System, è vista come un'unica rete 802 che va sotto il nome di **Extended Service Set** (**ESS**) (fig. 2.6).



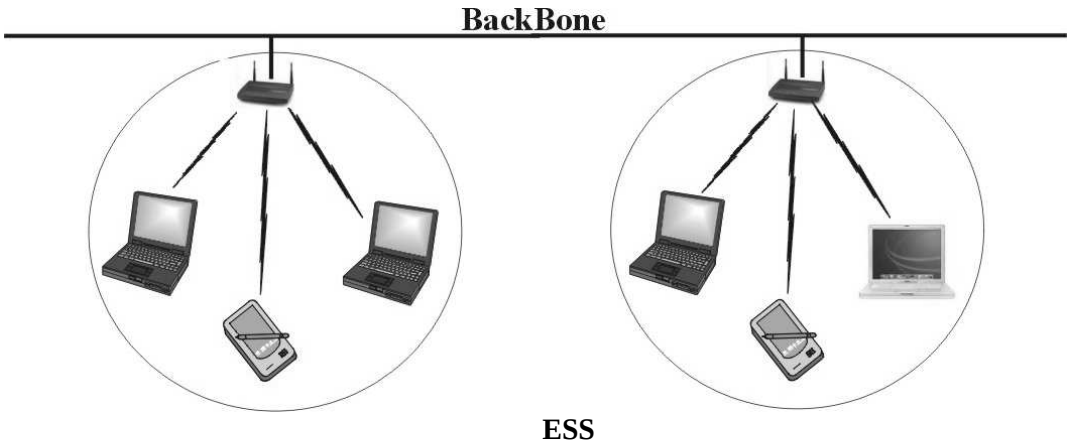
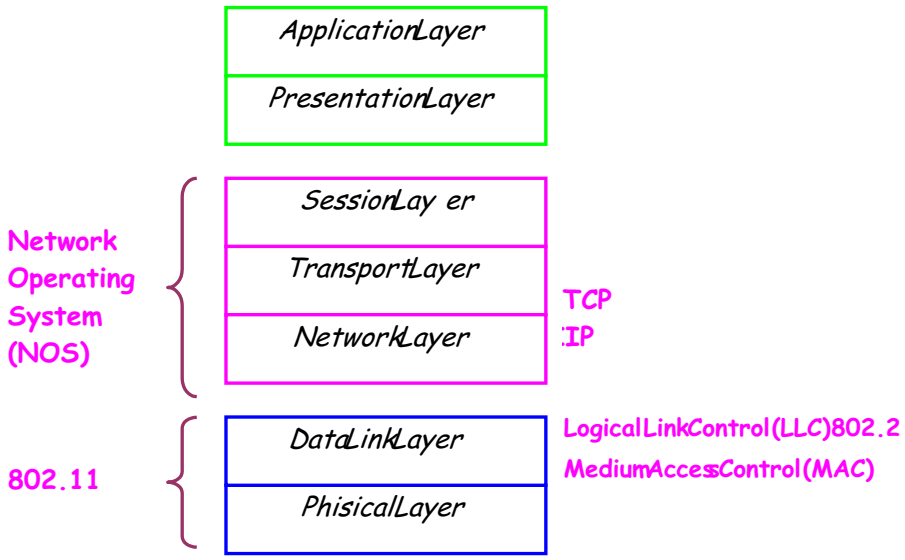


Figura 2.6 Schema di una Infrastructure Network. BSS e ESS

2.3.1 Descrizione dello standard IEEE 802.11

Come tutti i protocolli della famiglia 802.x, anche lo standard IEEE 802.11 definisce i due livelli logici più bassi del modello OSI (Open System Interconnection): il livello fisico (Physical Layer - PHY) e il livello Data Link (Medium Access Control - MAC).

Livello Fisico
La convergenza tra MAC e lo specifico mezzo fisico è realizzata mediante la *Physical Layer Convergence Procedure* (PLCP). Essa si occupa di tradurre la MPDU (MAC Protocol Data Unit) nel formato opportuno per la trasmissione; ad esempio, inserisce all' inizio del frame il preambolo fisico occorrente.
Il sottolivello *Physical Medium Dependent* (PMD) realizza i meccanismi per l' individuazione del *clear channel* (mezzo trasmissivo libero), per la trasmissione e per la ricezione.



Già dal luglio 1992 il working group ha deciso di standardizzare tre tipi di trasmissione: infrarossi, radiofrequenza Frequency Hopping Spread Spectrum (FHSS) e radiofrequenza Direct Sequence Spread Spectrum (DSSS), nelle bande ISM (2.4-2.4835 GHz).
In questa tesi tralasceremo di occuparci della trasmissione a infrarossi.

Radiofrequenza DSSS PHY
Per il DS-PHY sono specificati un *Basic Access Rate* di 1 Mb/s, ottenuto con modulazione DBPSK (Differential Binary Phase Shift Keying), e un *enhanced access rate* di 2 Mb/s ottenuto con modulazione DQPSK *(Differential Quaternary Phase Shift Keying).* La sequenza di chipping è lunga 11 chip.
Come banda di trasmissione è stata scelta la banda ISM a 2.4 GHz in cui sono stati definiti 7 canali. Uno è specifico per il Giappone, mentre gli altri, per USA ed Europa, sono raggruppati in 3 coppie di canali, sebbene per l' Europa uno dei canali della prima coppia non possa essere utilizzato. I canali di una coppia possono operare senza interferenza. I canali di tutte e tre le coppie possono essere usati simultaneamente in un sistema tipo cellulare. La potenza massima di trasmissione è fissata a 1 W in USA e 100 mW in Europa, mentre quella minima non deve essere inferiore ai 10 mW.
Nelle figure seguenti sono mostrati le due forme nello standard 802.11b: con preambolo lungo o con preambolo corto. Quest'ultimo serve ad assicurare l'aumento

del *throughput* di una rete nel momento in cui si trasmettono dati speciali come voce, *Voice-over IP* (VoIP) e *streaming video*.

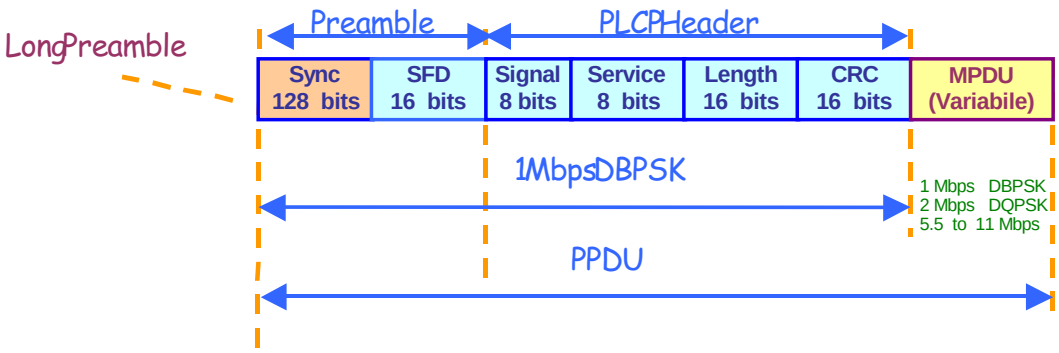


Figura 2.7 Formato del frame 802.11b con preambolo lungo

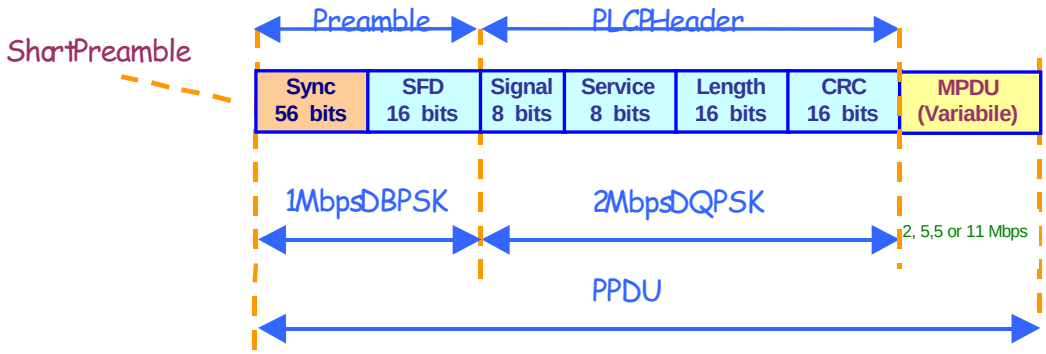


Figura 2.8 Formato del frame 802.11b con preambolo corto

Radiofrequenza FHSS PHY

Il Frequency Hopping Spread Spectrum ha un data rate di 1 Mb/s con modulazione 2 level GFSK *(Gaussian Frequeney Shift Keying)* e di 2 Mb/s con modulazione 4 level GFSK. In USA e in Europa il range di frequenze utilizzabili, scelto sempre nella seconda banda ISM (2.4 GHz), va dai 2.402 GHz ai 2.482 GHz, ed in esso sono individuati 79 canali per il frequency hopping di 1 MHz di ampiezza. La trasmissione deve essere tale da concentrare il 99% dell' energia all' interno del canale, ed avere la "20 dB bandwidth" inferiore a 1 MHz (figura 2.9).

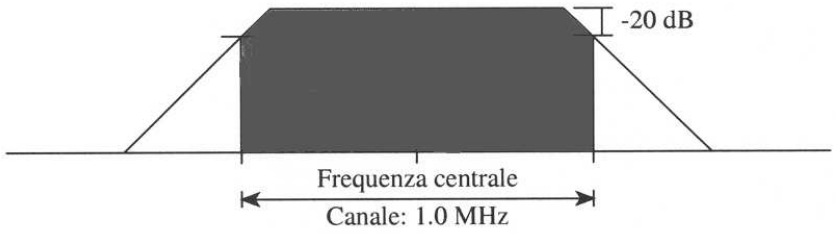


Figura 2.9 Occupazione della banda del singolo canale frequency hopping.

La sequenza di *hop* viene scelta in modo tale da poter collocare diverse reti simili nella stessa area geografica e per migliorare l' efficienza totale e il throughput di ciascuna rete. Sono definiti 3 insiemi di 22 sequenze di hop ciascuno, che rispettano il criterio di un solo canale adiacente che interferisce su ciascun lato del canale desiderato.
La frequenza dell' hop è controllata dai livelli superiori al PMD: dal momento che si deve poter massimizzare l' uso di ogni intervallo di hop e lo sfruttamento dell' intera banda di trasmissione, i livelli superiori devono dire al PMD quando saltare, definendo in questo modo l' hop rate del sistema. Questo preclude la nozione di un hop rate massimo. L' hop rate minimo, invece, è controllato dalle regolamentazioni ufficiali ed è definito dal numero di canali visitati diviso il tempo totale impiegato per completare la sequenza. Per gli USA, ITCC stabilisce che un PMD deve visitare almeno 75 canali in un periodo di 30 secondi: 75/30 = 2.5 hop/s minimi.
A livello PLCP, nel formato del frame viene aggiunto un *preamble* e un *header*. *Il* primo contiene 80 bit di sincronizzazione e 16 bit di Start Frame Delimiter. Il secondo ècostituito da 3 campi: 6 bit di segnalazione per usi futuri, 16 bit di indicazione del numero di ottetti della MPDU e 16 bit di CRC (figura 2.10).

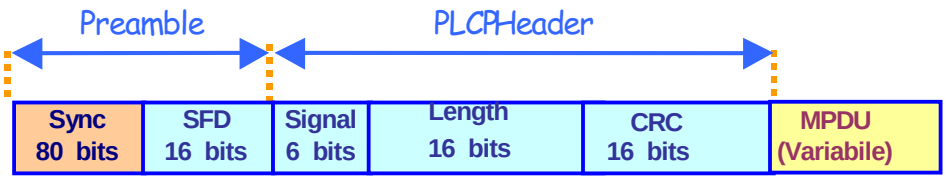


Figura 2.10 FHSS: PLCP Frame Format.

Per ulteriori specifiche del livello fisico si veda le references [1]-[2]-[3].

Livello MAC

Lo scopo del MAC group dell' IEEE 802.11 è quello di creare un singolo Medium Access Control per i diversi livelli fisici visti in precedenza. Nasce così il wireless LAN MAC, che pone il suo fondamento nel DFWMAC *(Distributed Foundation Wireless MAC)*, una proposta congiunta di NCR/Symbol e XIRCOM. Esso si presenta come supporto a due tipi di reti: *ad hoc LAN*, (piccola) rete di stazioni paritetiche, normalmente distribuite su una zona tale da permettere la trasmissione reciproca senza la presenza di una infrastruttura; *infrastructure network*, rete, anche vasta, caratterizzata dalla presenza di un *Distribution System* (DS), a sua volta wireless o wired. Al distribution system si accede mediante stazioni apposite dette *Access Point* (AP, figura 2.11).

Ogni insieme di stazioni associate a formare un gruppo in cui comunicano direttamente fra di loro è detto *Basic Service Set* (BSS) caratterizzato da un identificatore, *BSS-ID.* L' insieme di più BSS, interconnessi mediante access point e un distribution system, forma un *Extended Service Set* (ESS), caratterizzato da un identificatore *ESS-ID.*

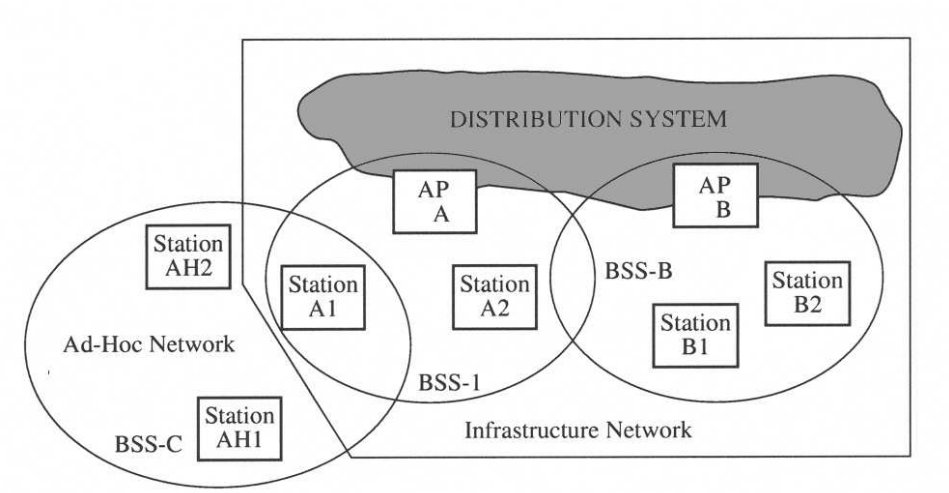


Figura 2.11 Rete *ad hoc* ed infrastructure.

Lo standard 802. 11 specifica una serie di servizi propri di ciascuna stazione ed una serie di servizi propri del Distribution System. La tabella 2.3 illustra tali servizi. Il principale metodo di accesso dell' 802.11 MAC è una funzione di coordinamento distribuita (DCF): il *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA). Esso è utilizzato per la trasmissione asincrona, e può essere affiancato da una funzione di coordinamento centralizzata (PCF) a maggior priorità per servizi limitati nel tempo.

Categoria di servizi	*Servizio*	*Scopo*
Servizi forniti da ogni stazione	Autenticazione	Utilizzato per verificare l' identità delle stazioni ch vogliono stabilire fra loro un link diretto di comunicazione. Non si tratta di autenticazione user-to-user o end-to end. L' 802. 11 fornisce il supporto lascia la possibilità di implementare protocolli di autenticazione diversi.
	Associazione	Servizio mediante il quale una stazione entra a far parte di un BSS (deve essere preceduto dall' autenticazione). Nel caso di infrastructur network tale servizio è fornito unicamente dall' Access Point. In tale maniera il Distributio System sa a quale AP far riferimento per trasmettere un frame alla stazione.
	Disassociazione	Servizio mediante il quale si termina una precedente associazione.Non è una richiesta ma è una notifica, quindi non può essere rifiutata.
	Privacy	Utilizzato per stabilire un opportuno algoritmo per criptare i messaggi.
Servizi	Distribuzione	Servizio mediante il quale, utilizzando le informazioni di associazione, le MSDU vengono distribuite all' interno di un DS. Se ad es. la stazion Al (figura 2.11) deve trasmettere un messaggio a B 1, il percorso seguito è: da Al all' AP-A, dall' AP-A DS, dal DS all' AP-B, dall' AP-B a B l. L' AP passa il messaggio dal BSS al DS viene detto "input AP". L' AP che passa il messaggio dal DS al BS viene detto "output AP". Se Al deve trasmettere ad A2, "input AP" e "output AP" coincidono e corrispondono ad A. L' 802. Il non specifica l modalità di trasmissione nel DS.
	Integrazione	Permette lo scambio di MSDU tra DS ed una rete esistente. Viene svolto da una stazione particolare detta portal. L' 802. Il non ne specific l' implementazione.
	Riassociazione	Permette il trasferimento di una stazione da un BSS ad un altro (all' intemo di un medesimo ESS) mediante il passaggio dall' associazione dell stazione con l' AP del vecchio BSS a quella con l' A del nuovo. Il servizio di riassociazione è quindi necessario per permettere la mobilità delle stazioni al di fuori dei BSS.

Tabella 2.3 Specifiche dei servizi.

Distribuited Coordination Function

Il mezzo fisico wireless a differenza di quello wired non permette un facile Carrier Sense ed una facile Collision Detection. È possibile ad esempio che due stazioni facenti parte di una medesima rete con infrastruttura riescano a comunicare con l' AP senza "sentirsi" fra di loro (problema del terminale nascosto). Il metodo di accesso scelto, il CSMA/CA, cerca una soluzione per tali problemi.

Una qualunque stazione che vuole trasmettere, per prima cosa deve verificare se un'altra stazione sta trasmettendo (Carrier Sense), e, se riconosce la presenza di trasmissioni, si mette in attesa. Quando il mezzo si libera attende che rimanga tale per un intervallo di tempo minimo *(Distributed InterFrame Space:* DIFS), dopo di che inizia una fase di contesa per l'utilizzo del mezzo *(contention window)*: la stazione sceglie un'intervallo casuale *(backoff)* al termine del quale, se il mezzo è ancora libero, inizia la trasmissione. L' intervallo di backoff serve a ridurre la probabilità di collisione quando, alla fine di una trasmissione, ci sono molte stazioni in attesa che il mezzo si liberi. L' intervallo di backoff è scelto tenendo conto di un parametro che oscilla tra un valore massimo ed uno minimo, raddoppiando ogni volta che si deve ripetere la trasmissione di un frame. In questo modo si allunga la finestra di contesa riducendo la probabilità di collisione nel caso di carico elevato della rete.

Quando una stazione, in attesa che termini l' intervallo di backoff, sente che il mezzo non è più libero, congela il tempo di backoff rimasto. Quando poi rileva il mezzo libero per un tempo pari ad un DIFS, non sceglie un nuovo intervallo di attesa, ma termina il precedente (figura 2.12).

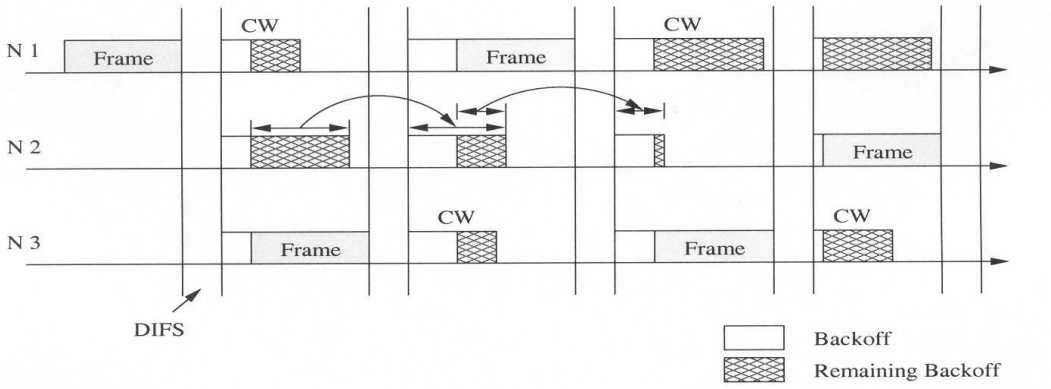


Figura 2.12 Procedura di backoff.

Comunque, il mecccanismo di backoff non esclude la possibilità di trasmissioni contemporanee, e quindi di collisioni. Per realizzare la "ollision avoidace" lo standard prevede un protocollo Request To Send (RTS) – Clear To Send (CTS). Quando una stazione trova libero il mezzo allo scadere del tempo di backoff, non invia subito il dato, bensì un frame di RTS. Se riceve dal destinatario un frame di risposta CTS allora procede all' invio del messaggio, altrimenti suppone che si sia verificata una collisione e si mette in attesa per riprovare. Per evitare che durante i messaggi di protocollo si entri nuovamente in una contention window, il tempo di attesa per i messaggi di risposta e

per l' invio dei dati dopo il CTS è più corto del DIFS; tale tempo è detto*Short InterFrame Space* (SIFS). La stazione destinataria, se la trasmissione ha successo, invia poi un messaggio di ACK. La figura 2.13 illustra la relazione tra DIFS e SIFS in corrisDondenza di un ACK.

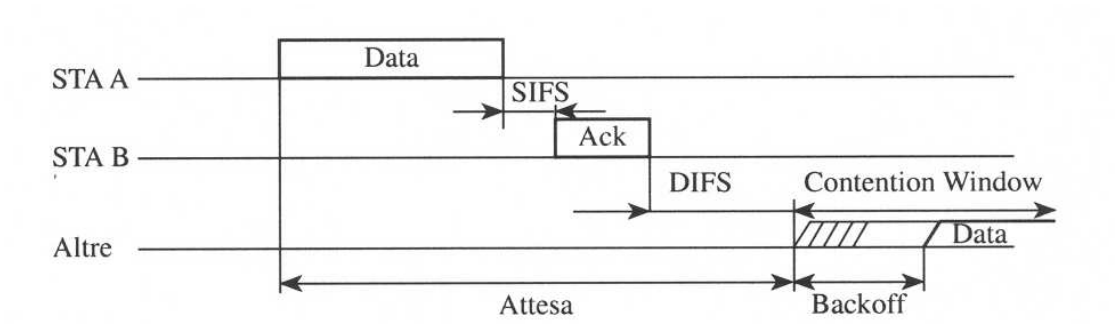


Figura 2.13 SIFS e DIFS in una trasmissione DATA-ACK.

Quando è in corso una trasmissione secondo il protocollo RTS/CTS, tutte le stazioni non interessate dovrebbero "sentire" il mezzo occupato. Tuttavia, a causa della bassa affidabilità della trasmissione, una stazione potrebbe non ricevere i messaggi e iniziare una trasmissione generando collisione. Per prevenire questa eventualità, il protocollo realizza anche un "carrier sense virtuale". I messaggi RTS e CTS contengono informazioni sulla durata della trasmissione successiva, che le stazioni non interessate alla ricezione caricano, in un registro detto *Net Allocation Vector* (NAV). Tale registro viene via via decrementato e ogni stazione ne attenderà l' azzeramento prima di cominciare la procedura di trasmissione (figura 2.14). Dal momento che il CTS è trasmesso dalla stazione di destinazione, le informazioni sulla durata della trasmissione raggiungono sia le stazioni vicine alla destinazione che quelle vicine alla sorgente.

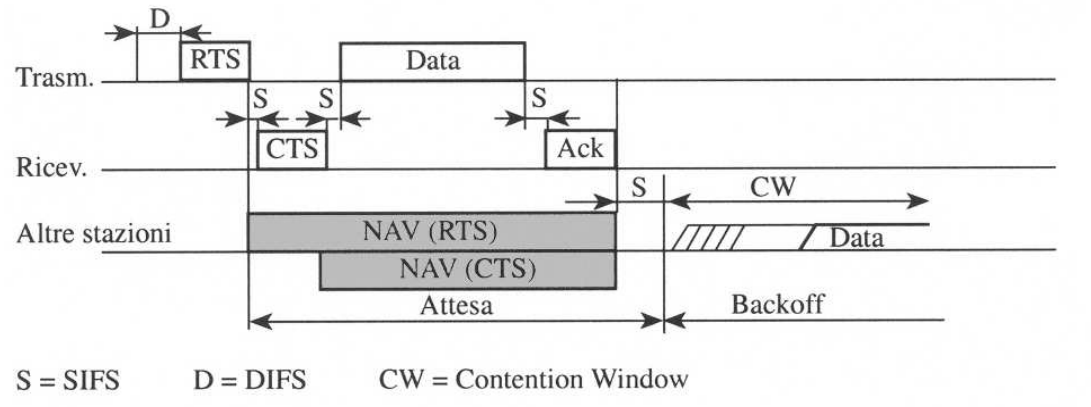


Figura 2.14 Net Allocation Vector (NAV).

L' utilizzo del protocollo RTS/CTS ha due controindicazioni: innanzi tutto, se il pacchetto di dati è corto, l'overhead introdotto può essere eccessivo; inoltre, non è applicabile nel caso dei pacchetti multicast e broadcast (in quanto più di una stazione potrebbe rispondere al RTS). Esiste pertanto la possibilità (obbligatoria per pacchetti al di sotto di una certa dimensione definibile a priori) di effettuare la trasmissione dei dati immediatamente allo scadere del tempo di backoff, se il mezzo è ancora libero. In questo caso è naturalmente possibile che una collisione impedisca la corretta trasmissione dei dati. Nel caso di pacchetti singlecast un messaggio di ACK segnala al mittente l' avvenuta ricezione, mentre per i pacchetti multicast e broadcast non c' è modo di sapere se la trasmissione è andata a buon fine. Se la stazione trasmittente non riceve l' acknowledge entro un tempo limite, ritrasmette il frame dopo aver partecipato nuovamente alla contesa del mezzo. La mancata ricezione dell' acknowledge, tuttavia, non esclude che il frame di dati sia in realtà arrivato correttamente. Pertanto, ogni frame ritrasmesso ha un opportuno bit *(retry bit)* settato. L' eventuale ricezione di frame duplicati viene controllata mediante il confronto dell' MPDU-ID, un campo di 16 bit ottenuto con funzione di hash dal *network identifier (2* ottetti), dal *source address* (6 ottetti) e dal *sequence number (1* ottetto). Ogni stazione mantiene l' MPDU-ID degli ultimi frame ricevuti. Viene scartato il frame con il retry bit settato e MPDU-ID uguale ad uno dei precedenti.

Point Coordination Function

Il wireless MAC di *802.11* prevede anche una funzione di coordinamento centralizzata (PCF: *Point Coordination Function).* Essa può essere gestita solo da alcune stazioni *(Point Coordination),* come ad esempio gli AP delle reti infrastructure. Una PCF non è in grado di sovrapporsi con un' altra PCF sul medesimo canale trasmissivo. La PCF usa una struttura a *Superframe* (SF), dove si alternano il periodo di contesa, in cui è attiva la DCF, e il periodo senza contesa *(contentino free),* in cui è attiva la PCF (figura 2.15). La lunghezza del Superframe è un parametro che può dipendere dai servizi supportati e dal livello fisico; nel caso di frequency hopping, ad esempio, deve essere un sottomultiplo intero del dwell time. La massima durata del periodo contention free è pari alla lunghezza del Superfiame meno la lunghezza minima del contention period, che è pari a quella massima di un frame. La PCF coesiste con la DCF disabilitandola temporaneamente grazie ad una scelta opportuna dei tempi per cui si deve attendere che il mezzo sia libero per poter trasmettere.

Il point coordinator (PC) dà inizio al periodo di trasmissione senza contesa. Il traffico diretto dal PC ad una stazione associata viene detto *CF-Down* mentre il traffico in direzione opposta viene detto *CF-Up. Il PC* diventa padrone del mezzo trasmissivo mediante un accesso prioritario. Infatti, all' inizio del Superframe, prima di iniziare una trasmissione *CF-Down,* attende che il mezzo sia libero per un periodo pari a un *Point InterFrame Space* (PIFS), più grande di un Short IFS ma minore del Distributed IFS. In tale maniera anticipa la normale trasmissione delle stazioni.

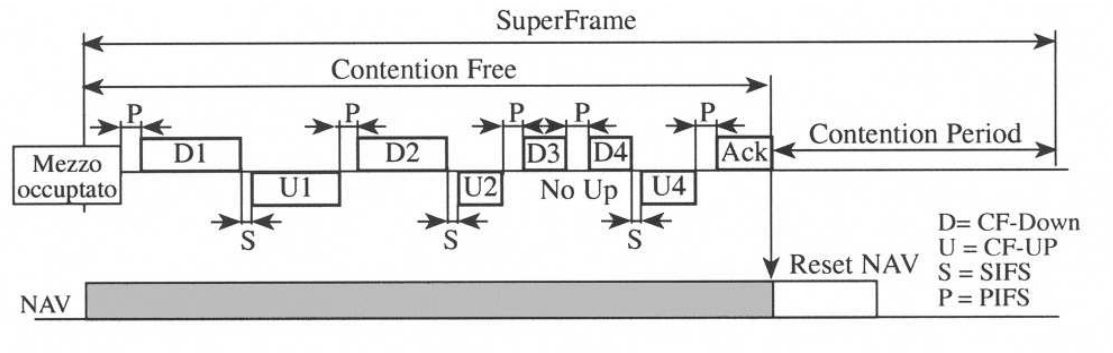


Figura 2.15 Struttura a Superframe e protocollo PCF.

Il PC coordina l' accesso al mezzo mediante il *polling*, mantenendo una tabella di quante stazioni ad esso associate hanno fatto richiesta del servizio contention free. Per ognuna di esse esegue un poll ed attende la trasmissione, che deve avvenire dopo un Short IFS altrimenti esegue il poll di un' altra stazione. Quando una stazione non trasmette per un lungo periodo viene cancellata dalla polling list. Nel periodo contention free non vi sono frame di acknowledge. L' acknowledge è trasmesso settando un bit opportuno nel frame successivo. Ad esempio in figura 2.15 U 1 contiene l' ack per D 1 e così via.
Per diminuire il rischio di collisione, ad ogni inizio di Superfiame ogni stazione carica nel Net Allocation Vector la lunghezza massima del periodo Contention Free. Al termine di questo il Point Coordination resetta il NAV di tutte le stazioni con la trasmissione di un frame opportuno.

Sincronizzazione e power management
È importante che le stazioni di un medesimo BSS siano sincronizzate per permettere operazioni di power management, temporizzazione del Superframe, sincronizzazione nel frequency hopping.
Ogni stazione ha un timer interno che conta in microsecondi con modulo pari al valore del parametro TSFTIMERMOD; il timer delle stazioni di uno stesso BSS viene mantenuto sincronizzato mediante la Time Synchronization Function (TSF).
Questo non è in contrasto con il metodo di accesso CSMA in quanto non si tratta di protocollo sincrono. La temporizzazione di determinati eventi non implica, in questo caso, lo stabilire il tempo preciso in cui essi avvengono, ma il tempo minimo, in quanto ci possono essere dei ritardi.
Nel caso di reti con infrastuttura l' Access Point ha il controllo della tempificazione. Esso invia periodicamente un frame opportuno di sincronizzazione detto *beacon*. Ogni beacon contiene, oltre all' ESS-ID e al BSS-ID, il timestamp (31 bit) dell' AP all' esatto momento dell' inizio della trasmissione, e la lunghezza dell' intervallo tra due beacon (24 bit). Tale intervallo è fisso, ossia non è misurato relativamente alla trasmissione del beacon precedente: se la trasmissione di un beacon è ritardata perché il mezzo è occupato, quelli successivi non ne risentono (figura 2.16).

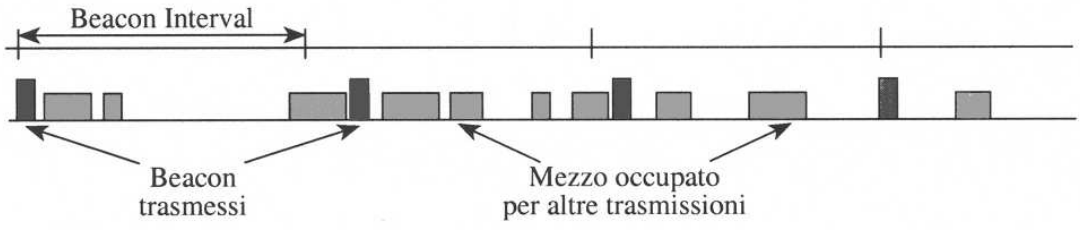


Figura 2.16 Trasmissione di beacon.

Ogni stazione che riceve un beacon assume come proprio il valore del timer dell' AP. Nel caso di reti "ad hoc", le stazioni di un medesimo BSS che sono sincronizzate hanno un opportuno flag settato. Ogni stazione sincronizzata concorre alla trasmissione dei beacon periodici. La procedura seguita è simile a quella di backoff: in pratica il beacon viene trasmesso dalla stazione che ha scelto casualmente l' intervallo di attesa di trasmissione più breve.
Nel beacon, oltre al timestamp della stazione trasmittente e alla lunghezza dell'intervallo di beacon, è contenuto un campo indicante il "peso" della stazione *(weight).* Hanno peso maggiore le stazioni che fanno parte da più tempo del BSS, e sono in grado di sentire un maggior numero di stazioni. Quando una stazione non ancora sincronizzata riceve un beacon, si sincronizza copiando il timestamp. Invece quando una stazione già sincronizzata riceve un beacon calcola la differenza tra il timestamp e il proprio timer. Se è maggiore di una certa soglia allora vuol dire che all' interno del BSS si sono formati due gruppi sincronizzati diversamente ed è, quindi, necessario iniziare una opportuna procedura di riunificazione; altrimenti aggiusta il proprio timer di più o di meno a seconda del peso della stazione che ha trasmesso il beacon.
Una stazione che vuole entrare a far parte di un certo BSS deve sintonizzarsi sul canale opportuno e sincronizzarsi con le altre stazioni appartenenti a quel BSS. Questo è ottenuto mediante lo *scanning* di tutti i canali per un certo periodo di tempo fino a quando non vengono ricevuti messaggi da parte dell' AP o delle altre stazioni. Sono possibili due tipi di scanning: *passive scanning* e *active scanning.*
Nel *passive scanning* le reti vengono individuate semplicemente mediante l' ascolto. La stazione scandisce tutti i diversi canali rimanendo in ascolto un certo periodo di tempo in ciascuno di essi, in attesa di un beacon. Nel beacon sono contenute le informazioni di BSS-ID e *timestamp* necessarie alla sincronizzazione. Questo metodo di scanning è efficiente se il BEACON-INTERVAL è relativamente breve ed il PHY supporta pochi canali di trasmissione.
Nell' *active scanning* la stazione manda una *probe request,* cioè un frame broadcast contenente l' identificatore della rete cercata, ossia ESS-ID e uno specifico o un qualunque BSS-ID. Rimane poi in attesa per un certo periodo di tempo di un *probe response.* Se non ha avuto risposta passa al canale successivo e così via. È possibile che in un canale siano ricevuti più probe response.

Nel caso delle reti infrastructure, è l' AP incaricato di rispondere al probe request. Se su un medesimo canale sono in ascolto più AP interessati alla richiesta, tutti manderanno il proprio probe response (figura 2.17).
Nel caso di reti "ad hoc" ci si comporta come nella trasmissione del beacon: una sola stazione manderà il probe response.
Particolarmente curato nel wireless MAC è l' aspetto riguardante il *power management:* è importante che in una rete wireless, dove molte stazioni possono essere costituite da in computer portatili, i consumi possano essere ridotti. L' idea, è quella di permettere di spegnere i transceiver il più a lungo possibile, bufferizzando i frame prima di trasmetterli e avvisando la stazione ricevente della presenza di traffico in attesa mediante brevi messaggi periodici (Traffic Indication Map: TIM). Ai ricevitori è sufficiente ascoltare i TIM fino a che non viene annunciata una trasmissione a loro indirizzata.

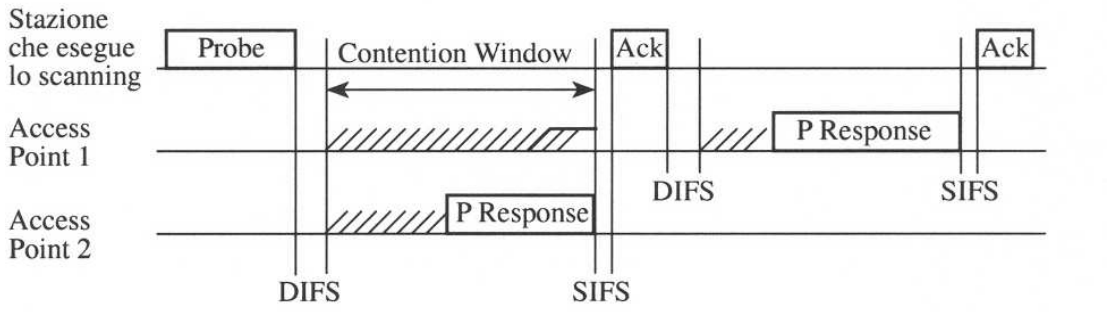


Figura 2.17 Active Scanning.

I transceiver delle stazioni possono essere in tre stati differenti: transmit (in trasmissione), awake (ricevitore in attesa), doze (trasmettitore e ricevitore spenti: consumo minimo). Il passaggio tra tali stati è regolato in maniera differente a seconda della modalità di power management scelta dalla stazione.
Nel caso di reti infrastructure particolari funzioni di power management sono svolte dall' AP. Esso mantiene lo stato delle stazioni ad esso associate, invia i TIM e bufferizza i frame diretti alle stazioni in power-save mode, o tutti i frame broadcast e multicast nel caso in cui nel BSS vi siano stazioni in power save mode.
Le stazioni possono essere in quattro power management mode:
- CAM (Continuous Active Mode): transceiver sempre attivo; la stazione può trasmettere e ricevere in ogni momento.
- TAM (Temporary Active Mode): come CAM solo per certi periodi.
- PSP (Power Save Polling): la stazione ascolta i TIM, se vi è indicazione di traffico ad essa indirizzato esegue il polling dell' AP per ricevere i frame. Non è necessario che ascolti tutti i TIM.
- PSNP (Power Save Non Polling): la stazione ascolta TIM particolari detti Delivery TIM, a seguito dei quali l' AP trasmette tutti i frame diretti alle stazioni PSNP senza bisogno del polling. Non e'quindi necessario che la stazione ascolti tutti i TIM.

I TIM vengono trasmessi ad interavalli fissi in maniera che sia sufficiente alle stazioni in power save mode di passare solo periodicamente dallo stato doze a quello awake (figura 2.18). I TIM sono trasmessi ogni 20-50 ms, mentre i DTIM ogni 50-200 ms.

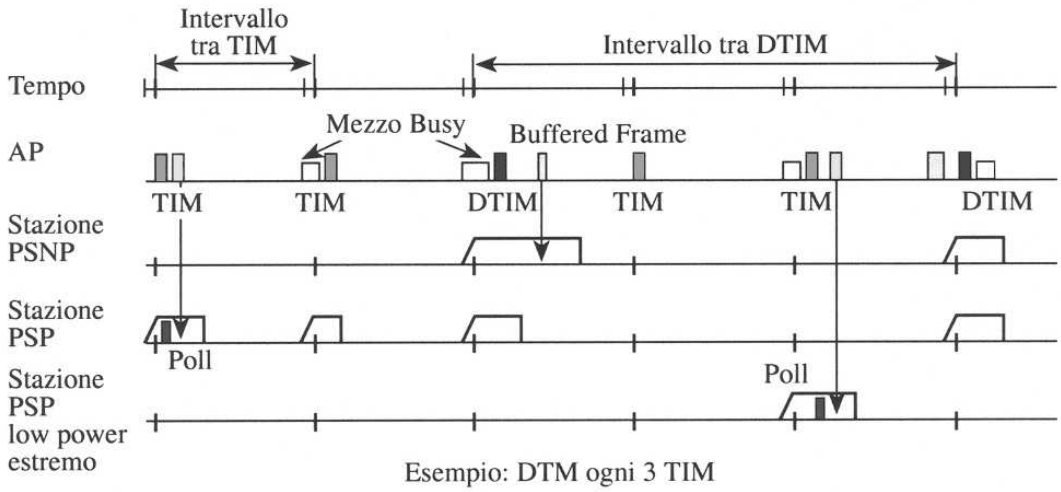


Figura 2.18 Power management in una rete infrastructure.

I frame broadcast e multicast sono trasmessi dall' AP immediatamente dopo aver avvisato le stazioni nei DTIM. Se una stazione non vuole perdere la trasmissione broad/multicast è necessario che ascolti tutti i DTIM.
Nel caso di reti "ad hoc" sono possibili solo il Continuous Active Mode e il Power Save Non Polling. Ogni stazione monitorizza lo stato delle altre stazioni. Quando una stazione deve trasmettere ad un' altra in power save mode, la avvisa mediante un *"ad hoc" TIM*. Gli "ad hoc" TIM vengono trasmessi in un intervallo detto *wake-up window*, in cui tutte le stazioni sono *awake*. La wake-up window si ripete ogni intervallo di beacon (figura 2.19).

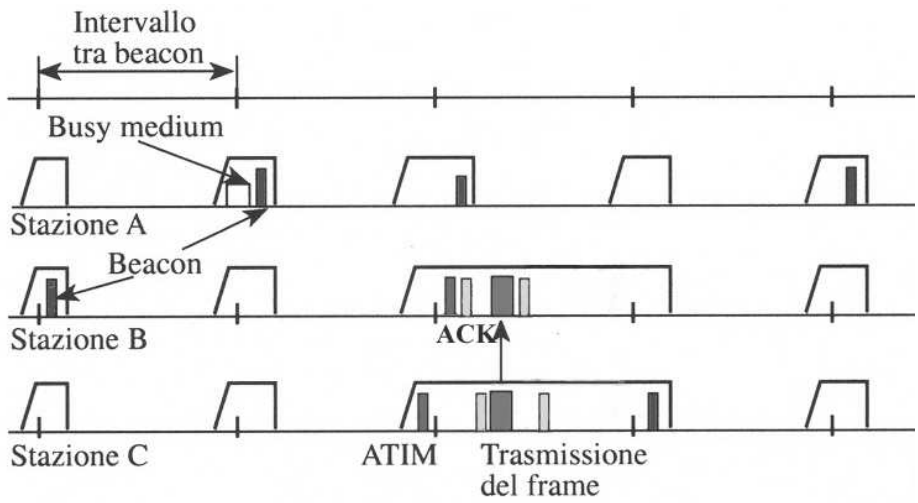


Figura 2.19 Power Management in una rete "ad hoc".

2.4 IL PROTOCOLLO AODV

Gli algoritmi di instradamento per una rete Ad Hoc devono essere in grado di fornire il corretto percorso che un pacchetto deve seguire adattandosi, allo stesso tempo, ai frequenti e impredicibili mutamenti della topologia della rete. Questo fa sì che l' ammontare del traffico di segnalazione, necessario ad un algoritmo di instradamento distribuito, sia molto elevato, in contrasto con la necessità delle reti wireless di minimizzare l' utilizzo delle risorse di comunicazione. La maggior parte degli studi svolti sugli algoritmi di instradamento per reti ad hoc mirano quindi a trovare il modo di diminuire il traffico di segnalazione prodotto dal livello di routing.
Gli algoritmi di instradamento esistenti possono essere classificati in tre categorie: algoritmi proactive, reactive e hybrid.
Gli algoritmi di tipo ***proactive*** mantengono costantemente aggiornate le informazioni di instradamento tramite scambi di pacchetti a intervalli temporali fissi. Questo permette di avere l' instradamento immediatamente disponibile ad ogni richiesta di routing. Lo svantaggio è che gli algoritmi proactive producono traffico di segnalazione anche quando non viene trasmesso nessun pacchetto dati; ciò può causare problemi di sovraccarico nella rete, specie se i nodi si spostano velocemente.
Nei protocolli di tipo ***reactive*** viene invocata una procedura per determinare il corretto instradamento solo nel momento in cui il pacchetto deve essere trasmesso. In questo modo si riduce il traffico di segnalazione a scapito di un aumento dei tempi di consegna.
Il terzo tipo di protocolli, ***hybrid,*** cerca, come dice il nome, di unire i vantaggi di entrambi i protocolli precedenti, restringendo l' applicazione di algoritmi proactive ai soli vicini del nodo che vuole trasmettere il pacchetto.

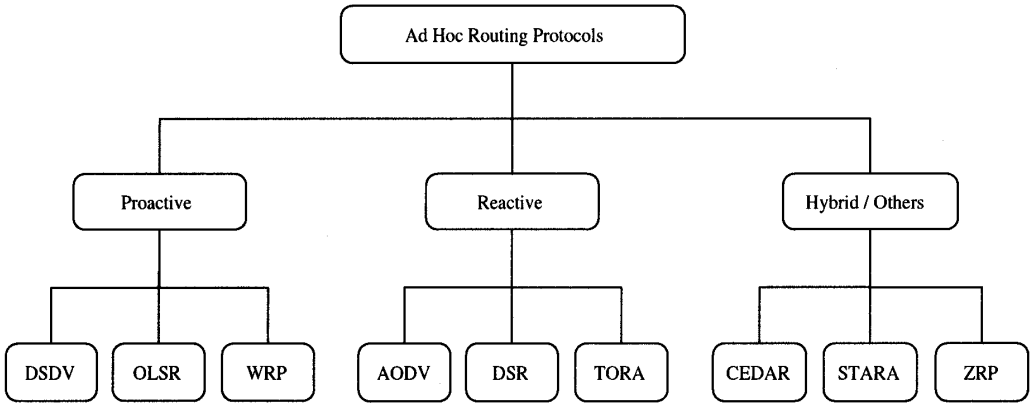


Figura 2.20 Classificazione dei protocolli di routing ad hoc

Una suddivisione alternativa alla precedente può essere fatta in base alla topologia della rete, che può essere "gerarchica" (hierarchical) o "piatta" (flat). In una rete "gerarchica" i nodi sono partizionati in gruppi detti cluster.Per ogni cluster è selezionato un "cluster head" attraverso i quali passa il traffico della rete.
In una rete ad hoc "piatta" non è prevista nessuna centralizzazione. Due nodi sono connessi se le condizioni radio sono tali da permettere al nodo destinazione di sentire la trasmissione del vicino (ovvero se due nodi sono in copertura radio).
Un vantaggio della rete "piatta" è la possibilità di stabilire più di un percorso tra nodo sorgente e destinazione; questo permette di valutare in modi diversi quale collegamento è da preferire, a seconda delle richieste e dell' utilizzo della rete. Il vantaggio della rete "gerarchica" è invece quello di minimizzare il numero dei pacchetti di routing che vengono scambiati tra i nodi di uno stesso cluster e tra i cluster head.
Di seguito viene fornita una descrizione della struttura del protocollo di routing AODV (di tipo reactive).

2.4.1 Specifiche del protocollo AODV

Il protocollo Ad hoc On-demand Distance Vector (AODV) [4] è un protocollo di routing di tipo reactive basato sull' algoritmo Distance Vector. Una caratteristica fondamentale del protocollo è quella di utilizzare "numeri di sequenza", i quali forniscono ai nodi uno strumento per valutare quanto sia aggiornato un determinato percorso. Un terminale che si trovi a dover scegliere tra più percorsi verso una certa destinazione sceglierà quello caratterizzato dal numero di sequenza maggiore, corrispondente ad un informazione di routing più recente. Inoltre il protocollo supporta l' instradamento multicast, ovvero consente la creazione di gruppi di utenti nella rete, i cui membri possono comunque cambiare in qualunque momento.

Ogni nodo mantiene le informazioni di instradamento per una destinazione all' interno di una *routing table* strutturata nel seguente modo:
Destination IP Address L' indirizzo IP della destinazione;
Next Hop Il nodo, nel raggio di trasmissione, a cui inviare il pacchetto per raggiungere la destinazione stessa;
Hop Count Il peso dell' intero percorso, rappresentato dal numero complessivo di salti;
Lifetime Il tempo di validità delle informazioni di routing;
Destination Sequence Number È un valore di riferimento che rappresenta la "versione" più aggiornata del percorso che deve essere preso in considerazione. Consente quindi ad un nodo di poter eliminare eventuali informazioni di routing obsolete;
List of Precursors Una lista di quei terminali (vicini) che, dovendo trasmettere pacchetti dati verso la destinazione, di indirizzo *Destination IP Address*, utilizzano questo percorso, sfruttando il nodo come relay.

2.4.2 Generazione di una richiesta

Se un nodo si trova nella condizione di dover trasmettere verso una destinazione per cui non ha informazioni di routing, esso provvede ad inviare un pacchetto broadcast denominato "Route Request" (fig. 2.21). I campi più significativi sono i seguenti:
Source IP Address Indirizzo del nodo richiedente (che da ora in poi, per semplicità di notazione, verrà indicato come "Source node");
Destination IP Address Indirizzo del nodo per cui si cercano informazioni di routing ("Destination node");
Hop Count Il costo associato al percorso, incrementato progressivamente da ogni nodo attraversato dal pacchetto;
Broadcast ID Un numero identificativo della richiesta broadcast;
Destination Sequence Number L' ultimo numero di sequenza che è stato associato, in passato, al percorso verso il nodo Destination. Qualsiasi informazione di Routing caratterizzata da un numero di sequenza più basso deve essere considerata obsoleta;
Source Sequence Number Il numero di sequenza che dovrà essere associato al Reverse Route dai nodi che riceveranno questo Request.

Figura 2.21 Pacchetto di Route Request

Quando un nodo riceve un Route Request ne sfrutta il contenuto per effettuare un "refresh" delle informazioni nella propria routing table. Il pacchetto infatti fornisce

indirettamente informazioni su come raggiungere il mittente della richiesta, sul numero di hop necessari, e sull' indirizzo del Next Hop (l' ultimo nodo ad aver inviato il pacchetto). Il nodo aggiunge una entry nella propria routing table e crea un "Reverse Route", ovvero diretto in senso opposto rispetto a quello in cui viaggiano i pacchetti Request. La sua funzione principale è quella di fornire un percorso ai pacchetti di risposta Route Reply di ritorno verso la sorgente, ma potrà essere utilizzato anche per inviare eventuali pacchetti dati.
Viceversa, se nella tabella esiste già una entry, allora il nodo valuta se sia il caso o meno di fare un aggiornamento: se il numero di sequenza associato al percorso è inferiore al Source Sequence Number che compare nel pacchetto Request ciò significa che il percorso in tabella ormai non è più valido.
Nel caso in cui il nodo non possieda alcuna informazione sulla destinazione provvede a ripetere a sua volta il Route Request, non prima di aver incrementato di una unità il campo Hop Count del pacchetto (per tenere conto del nuovo salto), e aver modificato il campo Source nell' header IP[1] del pacchetto. Quest' ultima operazione è necessaria per consentire al nodo successivo di sapere quale nodo ha inviato per ultimo il pacchetto.
Se, d' altro canto, il nodo ha informazioni di routing verifica se il valore del campo Destination Sequence Number associato al percorso posseduto è inferiore al valore che compare all' interno del Request. In tale caso significa che l' informazione in possesso del nodo è ormai obsoleta, ed anche in tale caso il pacchetto viene reinviato. In caso contrario l' informazione è sufficientemente aggiornata, e può quindi procedere all' invio di una risposta verso il nodo Source.

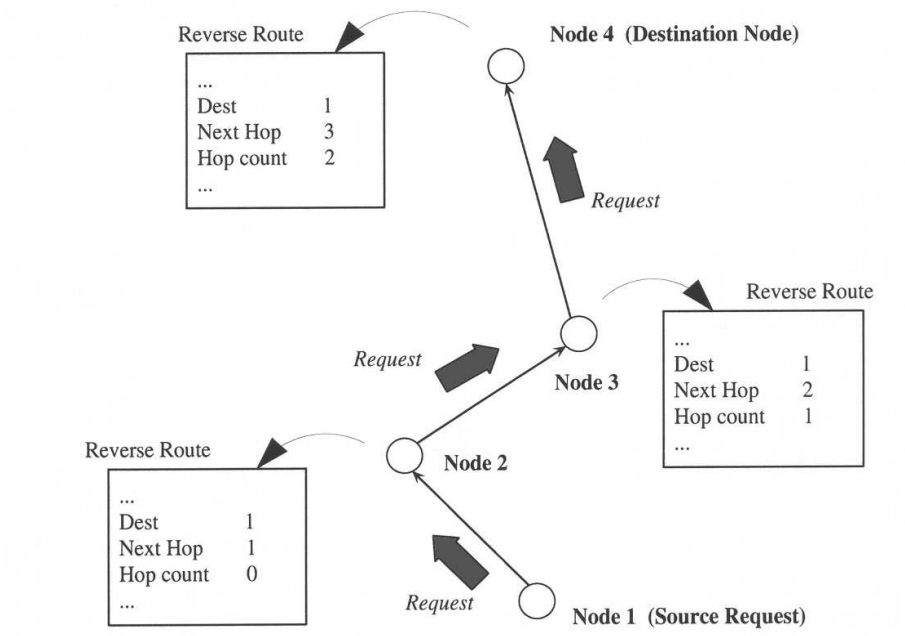


Figura 2.22 Creazione del reverse route al momento della ricezione di un Request

[1] Da non confondere con il campo Source IP Address del Route Request.

2.4.3 Expanding ring search

Per ridurre al minimo il numero di pacchetti Route Request utilizzati in questa fase di route discovery è stata introdotta una ottimizzazione, che coinvolge il Time-To-Live dei pacchetti. Il nodo Source genera dapprima un pacchetto con un TTL_START (valore iniziale del Time-To-Live), tipicamente molto basso. Se, dopo un certo tempo, il nodo non riceve nessuna risposta può ritenere che la richiesta non sia andata a buon fine e provvede ad inviare un nuovo Route Request con un TTL incrementato, rispetto al precedente, di una quantità TTL_INCREMENT, e così via. I valori dei tempi di attesa oltre i quali il nodo genera una nuova richiesta sono proporzionali al TTL stesso, e sono definiti nel seguente modo:

Timeout = 2*TTL*NODE_TRAVERSAL_TIME

Il parametro NODE_TRAVERSAL_TIME è una stima del tempo impiegato da un pacchetto di segnalazione ad attraversare un nodo, comprensivo anche della procedura *"four way handshake"* a livello MAC. Il valore del timeout si riferisce al caso in cui il nodo con informazioni di routing si trovi ad una distanza pari a TTL salti, la massima raggiungibile dal pacchetto di richiesta, e tiene conto anche del tempo di ritorno delle informazioni (moltiplicando per un fattore 2).Tale procedura è chiamata *expanding ring search* e la scelta di questo nome è abbastanza ovvia: la ricerca viene fatta su parti della rete delimitate da anelli di dimensioni i sempre maggiori, centrati sul nodo sorgente. Lo standard AODV fissa i valori TTL-START=1, e TTL_INCREMENT=2.

2.4.4 Generazione di una risposta

La risposta ad una richiesta di informazioni avviene generando un pacchetto dati unicast chiamato Route Reply, ed inviandolo verso il nodo Source. Viene quindi sfruttato proprio il Reverse Route che ciascun nodo ha provveduto a creare al passaggio del Route Request. I campi di maggior interesse sono i seguenti:

Destination IP Address L' indirizzo del nodo che ha richiesto l' informazione, ovvero il Source;
Hop Count Il costo associato al percorso;
Destination Sequence Number Il numero di sequenza da associare a questo percorso.
Ancora una volta, al passaggio del Route Reply, ogni nodo può sfruttarne le informazioni per aggiornare la propria tabella di routing.

2.4.5 Eliminazione selettiva dei Route Request

Quando un nodo riceve un Request ma non è in grado di rispondere al mittente, è costretto a procedere egli stesso ad un nuovo invio broadcast. Per evitare che si crei una situazione di loop, cioè che il Request continui a rimpallare tra due nodi, è indispensabile introdurre un meccanismo di limitazione. Ad ogni Route Request viene attribuito un indice progressivo, inserito nel campo Broadcast ID del pacchetto stesso. Tale valore, considerato in associazione con l' indirizzo IP del nodo Source, caratterizza univocamente una richiesta. Quando un nodo riceve un pacchetto Route Request è quindi in grado, dall' osservazione di questi due campi, di stabilire se ha già ricevuto, nel "recente" passato, una richiesta analoga[2]; in tale caso provvede a scartare il pacchetto. Questo comporta che i percorsi compiuti dai pacchetti Request non possono mai incrociarsi. Il meccanismo di selezione viene applicato anche da un nodo che sia in possesso di informazioni di routing aggiornate (che può essere o non essere la destinazione stessa). La conseguenza più rilevante è che questo nodo genera un pacchetto di risposta solo in corrispondenza della prima richiesta ricevuta, essendo quelle successive tutte scartate (Figura.2.23). Alla fine quindi avrà un peso rilevante, nella scelta del percorso, anche il livello di traffico incontrato dai Request e verrà preferito il tragitto meno congestionato.

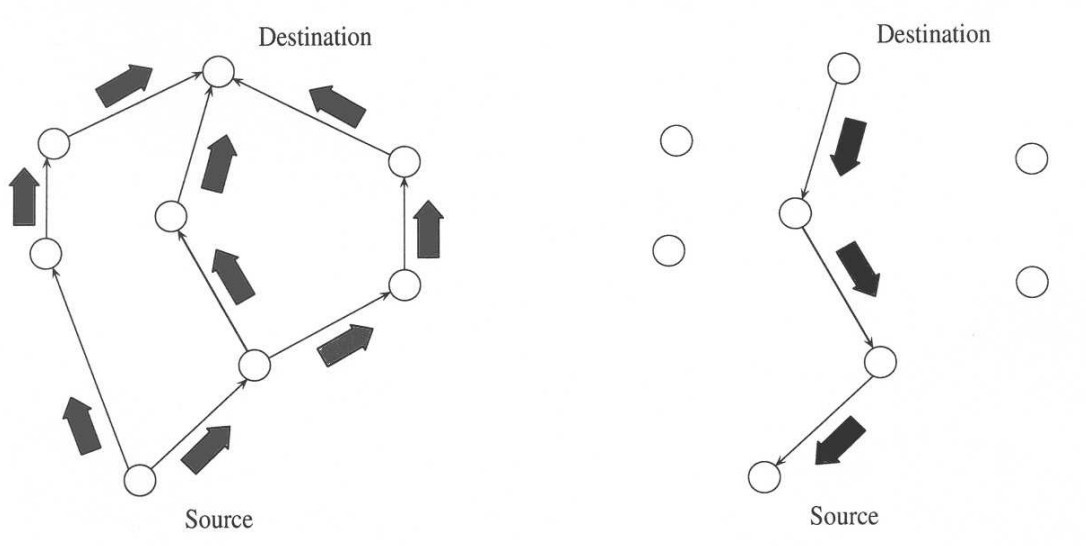


Figura 2.23 A sinistra: i percorsi compiuti dai Route Request. A destra: percorso compiuto dal Route Reply

[2] tempo di validità di questa informazione corrisponde al parametro ID_SAVE, fissato dallo standard in 30 secondi.

L' eliminazione selettiva dei request ha, da un lato, il vantaggio di ridurre il numero dei pacchetti di segnalazione allo stretto indispensabile, ma dall' altro lato limita spesso la scelta del Source ad un unico percorso possibile. La questione sarà ripresa in seguito.

2.4.6 Pacchetti Hello

Il protocollo prevede la possibilità che i nodi scambino periodicamente, con i vicini, brevi pacchetti di segnalazione broadcast (con TTL=1) chiamati "Hello messages". Tali pacchetti vengono utilizzati per la gestione delle connessioni da parte dei nodi stessi. Anche se consentito dallo standard l' utilizzo dei pacchetti di Hello non è comunque obbligatorio.

2.4.7 Link breakage

Con tale espressione si indica la situazione in cui un nodo è impossibilitato a trasmettere ad un nodo vicino. Ciò può avvenire per una congestione del link, oppure semplicemente perché il nodo vicino, se in mobilità, si è spostato al di fuori del raggio di trasmissione massimo, e non è raggiungibile. Il protocollo prevede più di un modo per la gestione della rottura di un collegamento.

Hello messages Un nodo può determinare lo stato del collegamento dall' ascolto dei pacchetti di Hello. Se un nodo non riceve, per un certo tempo, nessun pacchetto di Hello da parte di un vicino assume la rottura di tale collegamento.

Link layer detection La verifica dello stato del collegamento è eseguita dal livello MAC ogni volta che un pacchetto dati viene inviato ad un nodo vicino. Questa modalità è prevista, ad esempio, dallo standard IEEE 802.11, in cui la mancata ricezione di un ACK dopo un certo numero di ritrasmissioni, o il fallimento di una negoziazione tramite scambio di pacchetti RTS/CTS sono sintomo di un problema. In questo caso il pacchetto dati viene scartato, ma viene anche inviato un segnale, a livello di Routing, che provvede a gestire la condizione d' errore.

Passive Acknoledgement Dopo l' invio di un pacchetto dati verso una destinazione, un nodo può mettersi in ascolto per verificare se il Next Hop svolge correttamente il suo compito, ovvero se il vicino provvede effettivamente ad instradare il pacchetto appena ricevuto. Se tale operazione non viene eseguita entro un certo tempo il nodo assume la rottura del link con il Next Hop. [vedi Nota in fondo al capitolo]

2.4.8 Link breakage management

Nel caso in cui un nodo verifichi la rottura di un link, indipendentemente dalla strategia seguita, esso provvede a generare un pacchetto unicast chiamato Triggered Reply che informa del problema tutti i precursori. Ogni nodo che riceve tale pacchetto aggiorna quindi la propria tabella di routing, marcando il Route come inutilizzabile, e provvede a sua volta a ripetere il pacchetto ai propri precursori. L' informazione riguarda quindi solo l' insieme di nodi che stavano sfruttando quel link (Figura 2.24). A questo punto quindi è necessaria una nuova fase di route discovery allo scopo di trovare un percorso alternativo per la medesima destinazione.

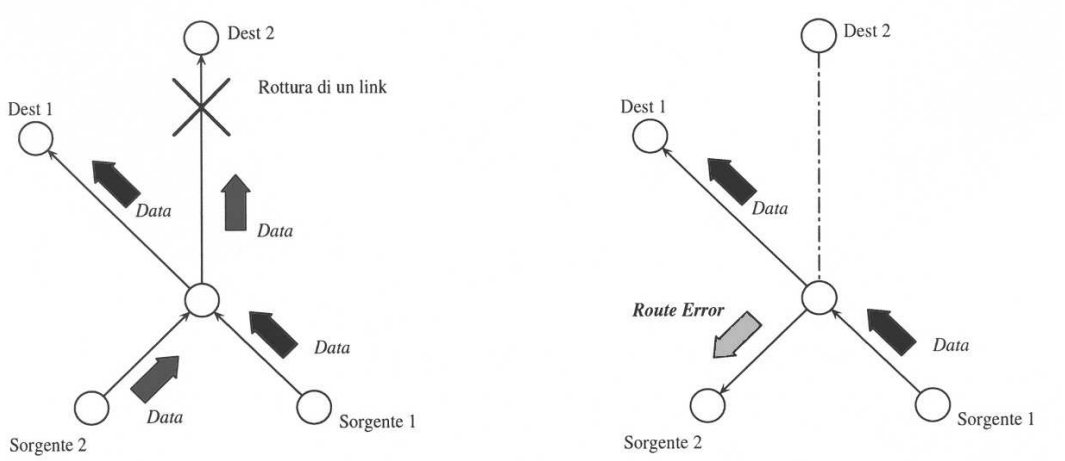


Figura 2.24 La rottura di un link (sinistra) provoca l' invio di un Route Error a tutti (e soli) i nodi che lo stavano utilizzando (destra)

2.5 AODV POWER CONTROL

È possibile inoltre effettuare delle modifiche al protocollo AODV Standard, per realizzare un protocollo di routing mirato alla minimizzazione della spesa energetica per le trasmissioni. Tale protocollo, per differenziarlo dalla versione non modificata, verrà nel seguito denominato "AODV Power Control".

È stato dapprima necessario introdurre una modifica generale alla struttura di un pacchetto. Ciò per consentire ai nodi di avere uno strumento per lo scambio di informazioni sulla potenza utilizzata nelle trasmissioni.

In ogni pacchetto sono stati introdotti due campi supplementari, denominati P_{tx} e P_{rx}.

Il primo specifica con quale potenza è effettuata una data trasmissione: il valore viene fissato dal modulo di routing al momento dell' invio del pacchetto stesso. Il livello fisico provvederà a modulare la potenza di trasmissione basandosi sul valore letto in tale campo. Il ricevente è quindi in grado di stabilire con quale potenza un pacchetto è stato trasmesso, e anche con quale potenza è stato ricevuto grazie ad un hardware

preposto a tale funzione. Tale valore viene comunicato al modulo di routing del nodo ricevente inserendolo nel secondo campo del pacchetto (P_{rx}). Il protocollo di instradamento, dall' analisi dei valori dei due campi, è quindi in grado di stimare la potenza minima necessaria che dovrebbe essere utilizzata per comunicare verso il nodo che ha inviato il pacchetto. Tale stima si ricava effettuando un semplice bilancio di potenza:

$$P_t = \frac{P_{tx}}{P_{rx}} \times R_{th}$$

in cui:

P_t è la potenza necessaria per comunicare verso il nodo che ha inviato il pacchetto;

R_{th} è la soglia di sensibilità del ricevitore (cioè la potenza minima per una corretta ricezione);

P_{tx} è la potenza con cui è stato trasmesso il pacchetto;

P_{rx} è la potenza con cui è stato ricevuto il pacchetto.

Per tenere conto degli inevitabili disturbi che si verificano durante le trasmissioni (interferenze con trasmissioni di altri terminali, fading ...) è necessaria una maggiorazione di tale valore di potenza, al fine di rendere più affidabile la comunicazione. Si introduce allora una soglia di sicurezza S_T *(Security Threshold).* La potenza utilizzata per raggiungere un nodo diventa quindi

$$P_t = \frac{P_{tx}}{P_{rx}} \times R_{th} \times S_T$$

e rappresenta la nuova metrica che verrà presa in considerazione per attribuire un peso numerico ad un collegamento.
Il controllo di potenza viene applicato anche ai pacchetti di livello MAC che precedono e seguono l' invio del pacchetto dati. Il valore con cui devono essere trasmessi i pacchetti dati viene deciso dal modulo di routing, che fissa il valore del campo P_{tx} in base al valore contenuto in una propria tabella di instradamento. Il valore della potenza con cui devono essere inviati i pacchetti RTS/CTS/ACK viene fissato dal livello MAC, basandosi proprio sul valore letto nel campo P_{tx} del pacchetto dati, al momento della ricezione del medesimo dal livello di instradamento superiore.

Struttura dei pacchetti

Nei pacchetti Route Request e Route Reply il campo "Hop count" tiene traccia del numero di salti compiuto dal pacchetto di segnalazione durante il percorso. Questo fornisce quindi ai moduli di routing dei vari nodi un mezzo per valutare il costo del percorso. Prendendo in considerazione una metrica di tipo diverso, basata sulla potenza

di trasmissione, è stato allora inserito un campo ulteriore "Power" che, analogamente, consente di attribuire al percorso un peso in termini di potenza.

Route Table
La tabella di routing è stata modificata introducendo due nuovi campi
Pwr-cost Il costo associato al percorso;
Pwr-next La potenza che deve essere utilizzata per trasmettere al Next Hop;

Modifiche apportate al protocollo
Nel paragrafo 2.4 è stato descritta la modalità con cui il protocollo AODV limita il numero dei pacchetti Route Request nella rete tramite un criterio selettivo. Ogni nodo, alla ricezione di un Route Request verifica se lo ha già ricevuto precedentemente, ed in tal caso provvede a scartarlo. Questo ha un senso nell' ottica di minimizzare la lunghezza del percorso (intesa come "numero totale di hop") ma nel momento in cui l' obiettivo diventa quello di minimizzare l' energia spesa, un tale meccanismo deve essere necessariamente modificato.
Supponiamo (Esempio in figura 2.25) che il nodo 1 voglia stabilire una connessione con il nodo 4, e che il percorso energeticamente più favorevole sia quello che passa per i nodi 1-2-3-4. Inizialmente il nodo 1 invia dunque un Route Request broadcast, che viene ricevuto, dai nodi 2 e 3. Se nessuno dei due nodi è in grado di fornire al nodo 1 informazioni di routing entrambi inviano nuovamente il pacchetto. A questo punto però il pacchetto Route Request che il nodo 2 provvede a reinviare non verrà preso in considerazione dal nodo 3, ed il percorso finale utilizzato per la trasmissione sarà dunque quello formato dai nodi 1-3-4 (tragitto di lunghezza minima).

Per evitare che percorsi potenzialmente vantaggiosi vengano scartati si deve intervenire sul meccanismo di limitazione dei Request. È necessario che un nodo abbia la possibilità di rispondere a più richieste in successione, non solo alla prima (che non è detto sia la migliore). Naturalmente non è pensabile di eliminare tout court perché l' aumento incontrollato di pacchetti di segnalazione finirebbe ben presto con l' avere il sopravvento sul traffico dati della rete, portandola rapidamente al collasso.

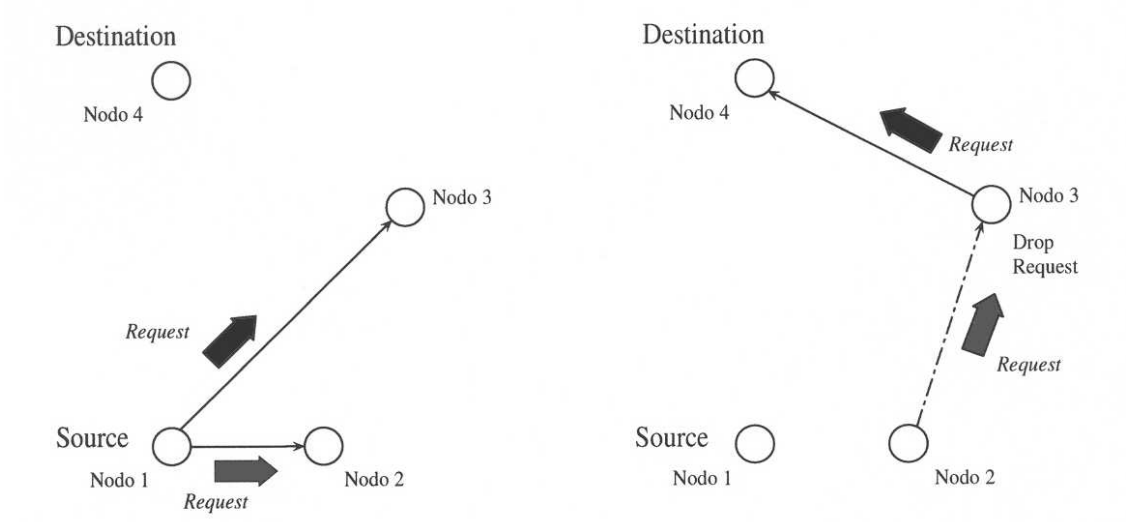


Figura 2.25 Protocollo AODV: percorsi potenzialmente ottimi non sono presi in considerazione

Il nodo mantiene una lista dei Request ricevuti, e del costo associato al tragitto compiuto dal pacchetto fino a quel momento, ottenibile direttamente dal campo *Power*.

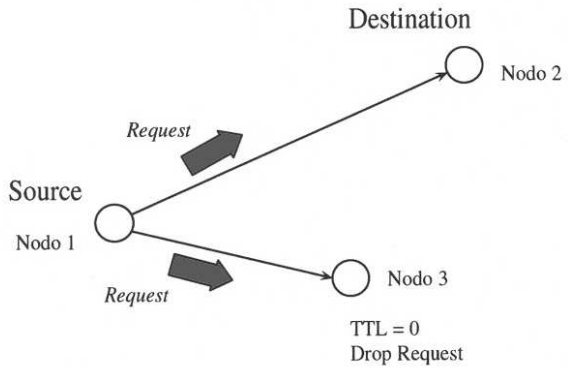


Figura 2.26 Expanding Ring Search preclude l' uso di un percorso potenzialmente ottimo

Al momento della ricezione di un identico Request, il nodo verifica se il costo è inferiore a quello presente in lista. In tal caso significa che il pacchetto successivo ha percorso un tragitto più vantaggioso, e quindi il nodo effettua un forward del pacchetto. Il costo di tale pacchetto viene memorizzato, e diventa quindi il nuovo "minimo" di riferimento. In caso contrario viene semplicemente scartato.

Un altro aspetto importante da considerare è legato alla strategia *expanding ring search* (descritta nel paragrafo 2.4.3) utilizzata durante la fase di route discovery. Lo scopo è quello di ottimizzare l' invio dei Request utilizzando TTL progressivamente crescenti. Nell' esempio di figura 2.26 si supponga che il tragitto migliore sia quello di destra, in cui si sfrutta un nodo intermedio (percorso 1-3-2). Il nodo Source invia un primo Request, con il campo TTL fissato ad l. In questo caso la richiesta va a buon fine: il nodo Destination riceve il Request, e può rispondere. Anche il nodo intermedio (3) riceve il medesimo Request, ma non può effettuare un forward, poiché il TTL ha raggiunto zero. In definitiva il percorso scelto sarà inevitabilmente subottimo (percorso 1-2 anziché 1-3-2); il protocollo tendenzialmente preferisce percorsi composti da un numero minore di salti.

Nota:

In uno studio simulativo [5] sono state confrontate le diverse strategie *Link Layer Detection* e *Hello messages.* In trasmissioni basate su protocollo di trasporto UDP, per quanto riguarda il numero di pacchetti consegnati, la prima procedura fornisce migliori risultati rispetto all' uso di pacchetti di Hello, specialmente in condizioni di mobilità dei nodi. Questo si spiega tenendo conto che la rottura del collegamento tra due terminali che si muovono è un evento molto frequente. Tuttavia, utilizzando messaggi periodici, tale rottura non può essere verificata tempestivamente, ma solo al momento della mancata ricezione del successivo messaggio di Hello. Il nodo può trovarsi nella condizione di continuare a trasmettere pacchetti dati verso un nodo vicino ritenendo il link ancora valido. Tali pacchetti verrebbero irrimediabilmente perduti. L' intervallo di invio dei pacchetti di Hello diventa quindi un parametro cruciale per le prestazioni della rete. Occorre tenere comunque presente che una sua semplice riduzione porterebbe ad un aumento della frequenza di "refresh" delle informazioni, ma anche ad un aumento del numero di pacchetti di segnalazione per secondo, e quindi ad un maggiore overhead. Dal medesimo studio risulta invece una significativa diminuzione dei ritardi di consegna nel caso si utilizzino i pacchetti di Hello. Tale risultato positivo va comunque considerato in relazione al minor numero di pacchetti consegnati. La mancanza di un aggiornamento rapido delle informazioni di routing rende di fatto le connessioni più "fragili". Per questo motivo i pacchetti che devono compiere percorsi lunghi (impiegando quindi più tempo) hanno una probabilità maggiore di non arrivare a destinazione, ed il loro contributo al calcolo dei ritardi è quindi minimo
Prendendo in considerazione trasmissioni con protocollo di trasporto TCP, e andando a studiare l' efficienza misurando il throughput, lo studio mostra risultati sostanzialmente analoghi.
Nel seguito si dimostrerà come la modifica del protocollo AODV, per introdurre il controllo di potenza, porti ad un sostanziale aumento del traffico di segnalazione.