

Guida alle Wireless Sensor Network

di Teodoro Ambrogio, Daniela D'Aloisi, Giuseppe Fierro, Susanna Ragazzini (FUB)

1. Applicazioni

Il modo più efficiente per trasmettere dati nelle reti di sensori è la tecnica multi-hop (rimbalzi multipli), che consente di avere meno perdita di segnale che non in una trasmissione diretta a lunga distanza. In altre parole, invece di instaurare la comunicazione fino ad un'antenna si utilizzano una serie di piccoli salti che necessitano di meno energia e garantiscono una maggiore affidabilità. Infatti, se uno dei nodi è inattivo, perché ad esempio gli si sono scaricate le batterie, la rete è capace di riconfigurarsi e trovare comunque una via per far comunicare tra loro i vari nodi.

Ogni sensore si comporta come un nodo capace di far rimbalzare automaticamente le informazioni verso un altro nodo che si trova più vicino alla destinazione prescelta. Le informazioni rimbalzano attraverso diversi nodi, con una serie di cammini multipli a un obiettivo che può essere anche molto lontano.

Invece di avere un sistema centralizzato che si occupa di raccogliere, trasportare e portare a destinazione le informazioni, abbiamo una rete distribuita formata da nodi tutti uguali che si auto-organizzano in modo da creare un efficiente sistema di comunicazione. Indichiamo questo tipo di reti con la sigla C1WSN.

Un secondo tipo di rete (C2WSN), più semplice, usa la tecnica single-hop (balzo singolo), in cui i sensori non trasmettono dati ai nodi vicini, ma ad un nodo detto wireless router preposto ad inviare i dati del gruppo di sensori al router, senza alcun processamento dei dati ricevuti. La topologia di questo tipo di rete è generalmente punto-punto.

Questo tipo di rete è poco costoso e largamente utilizzato nel campo del monitoraggio industriale, medico e degli edifici. Molte applicazioni di questo tipo impiegano la soluzione standard IEEE 802.15.4 (ZigBee), protocollo che minimizza il tempo di attività del radiotrasmettitore, così da ridurre il consumo di energia. ZigBee opera nelle frequenze radio assegnate per scopi industriali, scientifici e medici che corrisponde a 868 MHz in Europa, 915 MHz negli Stati Uniti e 2,4 GHz nella maggior parte del resto del mondo.

Il protocollo ZigBee è sostanzialmente diverso da quello Bluetooth: ZigBee colloquia con un elevato numero di nodi attivi in condizioni statiche e dinamiche, con una capacità di rimanere in uno stato di inattività (latenza) per lungo tempo senza dovere colloquiare con la rete, bassissimo consumo; Bluetooth invece viene utilizzato per reti quasi statiche con un basso numero di dispositivi connessi, ha una latenza bassa, e ha un elevato consumo.

Le reti C2WSN hanno molte applicazioni nel campo della domotica:

- gestione dell'illuminazione, del riscaldamento e della refrigerazione della singola casa;
- controllo dei consumi di gas, acqua e elettricità;
- notifica del rilevamento di un evento inusuale (intrusione);
- installazione e aggiornamento dei sistemi di controllo della casa;
- automazione di più case per il monitoraggio dei guasti, per la sicurezza domestica.

Applicazioni analoghe sono state sviluppate per l'automazione di interi edifici. Il controllo wireless dei consumi energetici di un edificio può essere fatta in modo semplice con una rete con tecnologia ZigBee; per esempio, la gestione centralizzata del condizionamento delle stanze di un hotel permette all'operatore di essere certo che le stanze vuote non siano condizionate, con un conseguente risparmio sui costi di gestione.

Un analogo discorso è valido anche per l'illuminazione dei vari ambienti, consentendo di illuminare in modo differenziato le varie zone, anche a seconda dell'illuminazione esterna e se una postazione di lettura (per esempio) sia occupata o no.

Le C2WSN possono essere utilizzate anche nell'automazione industriale, sia nei processi di produzione per ridurre l'intervento umano, sia per monitorare emissioni nocive e per aumentare la sicurezza degli operatori, sia per la gestione del magazzino merci e per il controllo generale dei consumi energetici dell'edificio.

In campo medico è possibile utilizzare le WNS sia nella medicina di routine (come seguire la riabilitazione di un paziente colpito da ictus o, a domicilio, monitorare lo stato di salute di un paziente cronico) che in quella di emergenza (come il rilevamento dei parametri vitali di tutti i pazienti del triage di un pronto soccorso).

Le reti di tipo C1WSN suscitano maggiore interesse nel campo della ricerca, soprattutto relativamente alla gestione dei disastri, al campo militare e alla sicurezza degli edifici.

Nella gestione dei disastri, uno scenario può essere un terremoto di grave entità. Un gran numero di sensori può essere gettato da un elicottero che sorvoli il luogo del disastro: la rete di sensori può assistere le operazioni di salvataggio, individuare i sopravvissuti, identificare le aree di rischio per i soccorritori, facilitando le operazioni e nel contempo rendendole più sicure.

Alcune reti hanno sensori dotati di videocamera a colori, altre ad infrarossi e possono quindi essere utilizzate anche in assenza di luce e sotto le macerie di un edificio. Anche nel campo dell'ingegneria civile, le WNS consentono il monitoraggio di strutture (edifici, ponti e viadotti) inserendo i sensori nelle posizioni critiche, per esempio dopo un

terremoto di media intensità, autodiagnosticando cedimenti strutturali anche nascosti che sono particolarmente insidiosi perché non rilevabili se non procedendo a costosi sondaggi sulle strutture. Oltre all'aspetto economico, è particolarmente rilevante quello dell'aumento della sicurezza degli edifici in zone sismiche: infatti i cedimenti nascosti potrebbero fare crollare la struttura durante un successivo terremoto, anche lieve. In campo militare possono essere utilizzate per la rilevazione di intrusione del nemico nel territorio, per il rilevare attacchi chimici, biologici e nucleari, per la sorveglianza di luoghi "sensibili" come i confini territoriali. I nodi delle reti di sensori sono più piccoli, più potenti e meno costosi dei sensori utilizzati in passato; il fatto che le WSN siano robuste, auto-organizzanti e che non richiedano la presenza di personale specializzato nel posizionamento dei sensori le rende essenziali in condizioni difficili e sui teatri di battaglia.

I sensori, per questo tipo di applicazione, devono essere in grado di rilevare vibrazioni del terreno, eventi impulsivi (come uno sparo o passi) o veicolari (un'auto, un camion o un cingolato).

L'utilizzo di sensori multipli su uno stesso nodo consente utilizzare algoritmi che fondono dati sismici, acustici, magnetici, etc. in modo da ridurre la possibilità dei falsi allarmi.

2. Tecnologie di base dei sensori wireless

Una Wireless Sensor Network (WSN) è una rete di piccoli nodi (o motes) capaci di ospitare sensori con capacità di comunicazione wireless, di eseguire delle elaborazioni sullo stesso nodo e di comunicare attraverso protocolli di rete ad-hoc.

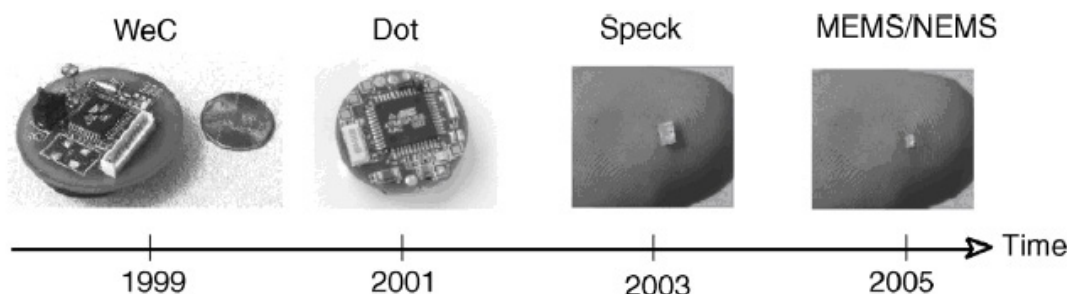


Figura 1

La Figura 1 mostra il progresso della tecnologia dei sensori nel tempo.

Le funzionalità di base di una rete di sensori dipendono tipicamente dal contesto delle applicazioni, ma alcuni requisiti sono tipici:

1. determinare il valore di un parametro in un certo luogo. Ad esempio, si ha bisogno di conoscere i valori di temperatura, pressione atmosferica, umidità;
2. determinare l'occorrenza di eventi di interesse, stimando i parametri relativi. Ad esempio, in una rete orientata al traffico stradale, si dovrebbe poter osservare il movimento di un veicolo, stimandone velocità, direzione;
3. classificare un oggetto individuato. Ad esempio, capire se il veicolo in questione è un'automobile, un pullman, un autobus;
4. tracciare un oggetto. Ad esempio, in campo militare, tracciare gli spostamenti del nemico all'interno dell'area geografica coperta.

Naturalmente, i dati raccolti devono essere trasmessi in un tempo relativamente rapido in modo che si possano intraprendere tempestivamente le azioni dovute.

Fra i *sensori passivi* distinguiamo quelli che costituiscono un singolo elemento (usati per misure termometriche, sismiche, acustiche e di umidità) e quelli ottici e di misurazione biochimica. I sensori passivi tendono ad essere dispositivi a bassa energia.

I *sensori attivi* tendono invece ad essere sistemi ad alta energia e includono radar e sonar.

In generale, le reti wireless di sensori possono essere esposte ad ambienti ostili, con elevate temperature, alte vibrazioni o livelli di rumorosità. Possono essere incorporate in unità mobili e robot o in sistemi manifatturieri. I sensori sono pertanto piccoli, di basso costo e robusti. I nodi di sensori hanno diverse configurazioni: dai nodi connessi a una LAN e collegati permanentemente all'energia elettrica, a nodi che comunicano con tecnologia wireless alimentati da piccole batterie.

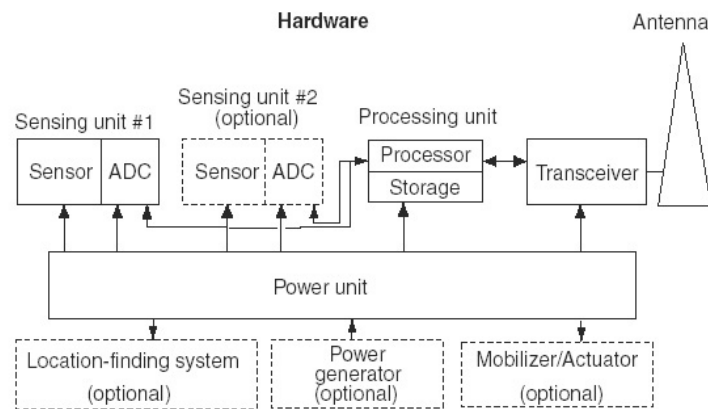
Una rete di sensori deve consentire particolari funzionalità sui nodi: il processamento del segnale digitale, la compressione dello stesso, la gestione degli errori, la codifica delle informazioni. È necessario, perciò, che i componenti hardware siano costruiti ad hoc.

Gli *Smart Dust* (polveri intelligenti) sono costituiti da una serie di computer microscopici di un millimetro cubo (come

un granello di sabbia) ed incorporano sensori, processori, radiotrasmettitori, software e un sistema di alimentazione. Gli elementi di base della costruzione della polvere intelligente sono i *Mems* (micro-electro-mechanical systems), cioè micro-computer che integrano insieme capacità di calcolo, parti meccaniche e sensori elettronici. I sensori come gli Smart Dust possiedono quattro sottosistemi hardware base:

1. *Power*: un'adeguata energia "di scorta" è necessaria per supportare le operazioni da poche ore, a mesi, ad anni, a seconda dell'applicazione.
2. *Logica computazionale e memoria*: per gestire la crittazione dei dati, gli errori con FEC, la modulazione digitale e la trasmissione. I microcontrollori variano da 8-bit fino a 64-bit, mentre i supporti di memoria arrivano fino a 100GB.
3. *Sensori trasduttori*: i sensori in generale.
4. *Comunicazione*: le reti wireless devono avere la capacità di comunicare sia con C1WSN che con C2WSN.

Nelle Figure 2 e 3 rispettivamente i componenti hardware e software di un sensore.



ADC = Analog-to-Digital Converter

Figura 2

I sensori tipicamente hanno cinque sottosistemi base:

1. *Middleware*. Microcodice del Sistema Operativo, usato dalle applicazioni ad alto livello per supportare varie funzioni. (per esempio TinyOS).
2. *Driver dei sensori*: sono i moduli software che gestiscono le funzioni base dei sensori.
3. *Codice di comunicazione*: questo codice gestisce le funzioni di comunicazione, incluso il routing, il forwarding dei pacchetti, la topologia della rete, il MAC, il FEC.
4. *Drivers di comunicazione*: gestiscono lo strato di radio link, la sincronizzazione e il clocking, l'encoding del segnale e la modulazione.

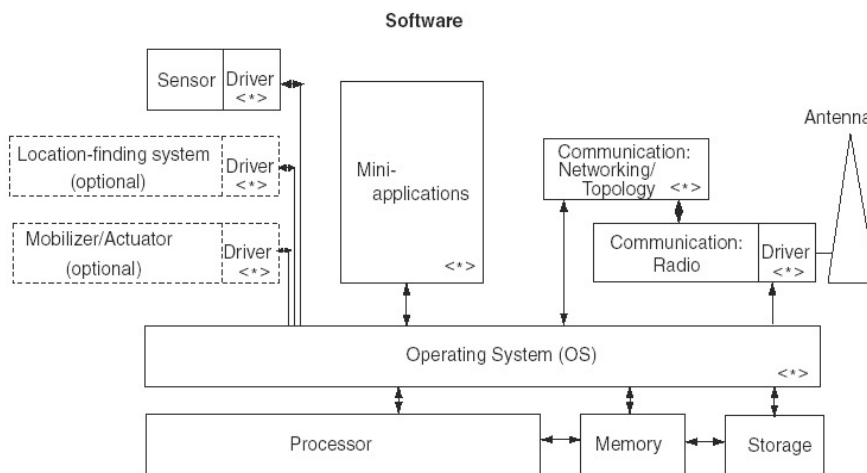


Figura 3

3. Protocolli MAC per le WSN

Le straordinarie potenzialità delle reti di sensori senza fili sono dovute non tanto ad elevate capacità elaborative locali dei singoli nodi, che sono invece relativamente modeste, quanto alla possibilità che hanno i nodi, nel loro complesso, di coordinarsi fra loro e quindi di auto-organizzarsi.

Perché tale coordinamento sia possibile è necessario che fra i nodi venga attivato un efficace sistema di comunicazione. D'altro canto una rete wireless, per propria natura, è esente da un collegamento fisico del tipo punto-punto fra nodi contigui ed essi, essendo praticamente tutti connessi fra loro, sono costretti a condividere un unico canale.

Tale vincolo impone l'implementazione di un opportuno protocollo di tipo MAC (Medium Access Control) che regoli l'accesso dei vari nodi alle informazioni di proprio interesse.

Facendo riferimento al modello ISO-OSI il MAC rappresenta il sottolivello inferiore del livello Data Link e comunica col livello fisico assumendosi il compito di sintetizzare (in trasmissione) e di analizzare (in ricezione) pacchetti in cui siano stati inseriti, in testa e in coda, opportuni dati aggiuntivi relativi all'indirizzamento ed al controllo degli errori. La scelta di un metodo MAC è determinante per le prestazioni di una rete WSN. Ci sono molti metodi classici per risolvere il problema dell'accesso, classificabili in tre maggiori categorie: assegnazione fissa delle risorse del canale, assegnazione a richiesta delle risorse del canale, assegnazione random delle risorse del canale.

3.1. Assegnazione fissa delle risorse del canale

- *Accesso multiplo a divisione di frequenza (FDMA)*: è una tecnica che consiste nel suddividere la banda disponibile in sottobande che sono assegnate ai vari nodi. Un opportuno filtraggio effettuato in ricezione permetterà di estrarre l'informazione inviata da ciascun nodo.
- *Accesso multiplo a ripartizione nel tempo (TDMA)*: a ciascun nodo è assegnato un intervallo di tempo in cui gli è consentito trasmettere.
- *Accesso multiplo a divisione di codice (CDMA)*: all'informazione trasmessa è associato un codice che identifica la sorgente. Il sistema utilizza tecniche di espansione dello spettro (Spread Spectrum) sia del tipo *frequency hopping* (FHSS) sia del tipo *direct sequence* (DSSS).

3.2. Assegnazione a richiesta delle risorse del canale

- *Polling*: questo sistema prevede che un dispositivo di controllo (Master) interroghi ciclicamente ciascun nodo (Slave) assegnando di volta in volta le risorse a quei nodi che hanno qualcosa da trasmettere.
- *Prenotazione*: in questo schema una frazione del canale viene utilizzata dai nodi per effettuare una richiesta di trasmissione.

3.3. Assegnazione random delle risorse del canale

- *ALOHA*: è uno schema che lascia a ciascun nodo la facoltà di decidere se e quando trasmettere in base a vincoli prestabiliti. A seconda dell'entità di tali vincoli esistono tre casi possibili.
 - **a. Aloha puro**: Assenza totale di vincoli. Ciascun nodo trasmette quando ha dati da trasmettere. L'efficienza massima asintotica di questo protocollo, intesa come probabilità massima che in una rete di infiniti nodi un nodo trasmetta senza dar luogo a collisioni, è pari a $1/(2e) \approx 18.4\%$.
 - **b. Aloha Slotted**: Il tempo viene suddiviso in intervalli uguali detti slot. Ogni nodo è vincolato ad iniziare la propria trasmissione nell'istante iniziale di tali intervalli. Rispetto allo schema precedente l'efficienza massima asintotica si raddoppia.
 - **c. Aloha Framed slotted**: Gli intervalli temporali vengono a loro volta raggruppati in trame. Ciascun nodo non può trasmettere più di una volta per ogni trama. Il sovraccarico computazionale di questo protocollo è dello stesso ordine di grandezza del precedente mentre l'ulteriore vincolo imposto riduce notevolmente la probabilità di collisione.
- *Accesso multiplo con rilevamento della portante (CSMA)*: Ogni nodo prima di trasmettere verifica se sul canale è già attiva una trasmissione rilevandone la portante. Se il canale risulta libero trasmette, altrimenti si mette in uno stato atteso. A seconda delle modalità di attesa si distinguono vari tipi di CSMA. Si parla di CSMA persistente se il tentativo di ritrasmissione viene effettuato non appena si libera il canale. Se invece il tentativo viene effettuato dopo un tempo casuale il CSMA viene chiamato non persistente. Sono previste anche modalità di attesa miste. Poiché tale protocollo non è in grado di evitare che si verificano collisioni esso viene di solito arricchito con sistemi di rilevamento delle collisioni (CD) o di prevenzione delle collisioni (CA).

Tra i requisiti di cui bisogna tradizionalmente tener conto quando si progetta un protocollo MAC (come l'entità dei ritardi, il *throughput*, la robustezza, la scalabilità, etc.) ve ne sono alcuni che nel caso specifico delle reti di sensori wireless rivestono un'importanza particolare.

Tali reti sono costituite da sensori di solito alimentati da batterie di bassa capacità e spesso situati in posti non presidiati e/o difficilmente raggiungibili per consentirne una frequente sostituzione o ricarica. Ne consegue che l'efficienza energetica del protocollo diventa un parametro di primaria importanza e costringe il progettista alla ricerca

di opportuni compromessi tra questo parametro ed altri requisiti più tipicamente trasmissivi. I principali fattori che possono determinare un eccessivo consumo di energia sono nell'ordine:

- *frequenza delle collisioni*: troppe collisioni costringono infatti ad una frequente ritrasmissione dei pacchetti persi;
- *ascolto inattivo*: tempo in cui il nodo resta in ascolto di dati non trasmessi (idle listening);
- *frequenza di overhearing*: numero di volte in cui il nodo riceve dati destinati ad altri nodi;
- *eccesso di pacchetti di controllo*: percentuale di pacchetti utilizzati dal protocollo per regolare l'accesso al canale rispetto al numero di pacchetti totale.

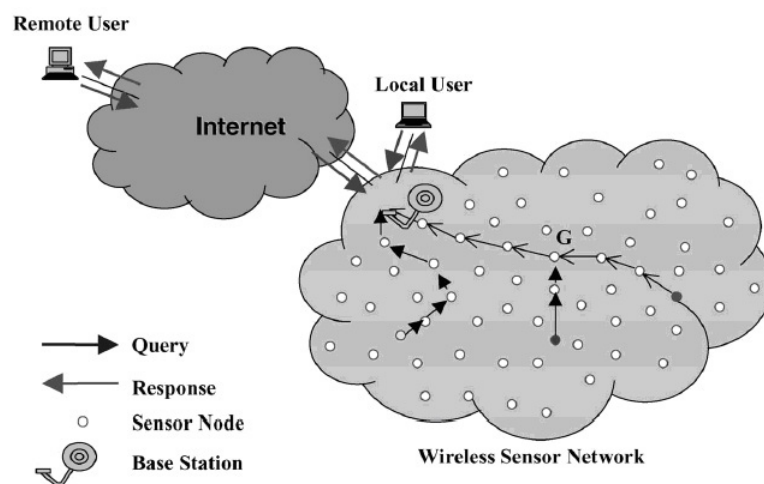
Un altro parametro che non va trascurato, perché può avere un notevole impatto sul consumo energetico, è la troppo frequente commutazione fra diverse modalità di funzionamento.

La maggior parte dei protocolli MAC che tengono conto delle suddette specifiche possono essere classificati in due principali categorie:

- *Schedule-based*. La maggior parte dei protocolli appartenenti a questa categoria sono delle opportune varianti del sistema TDMA in cui gli *slot* temporali vengono organizzati in trame (*logical frames*). Solo un sottoinsieme degli intervalli temporali della trama è assegnato a ciascun nodo. Sia il numero di *slot per frame* che gli algoritmi di *scheduling* sono parametri di progetto predeterminati. Il risparmio energetico legato a questa tecnica è dovuto principalmente al fatto che ciascun nodo—quando non deve né trasmettere né ricevere—si pone in uno stato di inattività (*sleep mode*). Tipici protocolli appartenenti a questa categoria sono lo SMACS (Self-Organizing Medium Access Control for Sensornets), il Bluetooth ed il LEACH (Low-Energy Adaptive Clustering Hierarchy).
- *Content-based*. Questi protocolli, conosciuti anche come *Random Access-Based Protocols*, non richiedono alcun coordinamento fra i nodi che condividono il canale. La risoluzione dei conflitti viene affidata a meccanismi di sincronizzazione del tipo RTS (*Request-To-Send*) e CTS (*Clear-To-Send*) che rendono il protocollo più robusto, ma non riducono in maniera significativa il dispendio di energia. Alcuni di essi come il PAMAS (Power Aware MultiAccess protocol with Signaling) riescono a ridurre il consumo dovuto all'*overhearing*, ma non quello causato dall'*idle listening*. Altri come lo STEM (*Sparse Topology and Energy Management*), utilizzando canali distinti per trasmettere dati e segnali di *wake-up*, riescono a ridurre notevolmente i consumi energetici a patto però che il sistema non richiede troppo frequenti commutazioni dei nodi fra lo stato dormiente e quello di veglia. Appartengono a questa categoria anche i protocolli T-MAC (*Timeout-MAC*) e B-MAC (*Berkeley-MAC*).

4. Protocolli di routing

Il modo con cui i dati viaggiano tra la stazione base e le locazioni dove i fenomeni sono osservati costituisce un importante aspetto per queste reti. Nella maggior parte dei casi, i dati effettuano tanti salti (hop) attraverso i quali i pacchetti viaggiano con brevi raggi di comunicazione.



Multihop data and query forwarding.

Figura 4

Compito principale di un algoritmo di routing è determinare il set di nodi intermedi allo scopo di trovare un cammino tra il nodo sorgente e quello destinazione. In una WSN, è importante contenere l'utilizzo della banda e il consumo di energia, processi richiesti ai nodi mobili. Trovare una strategia che bilanci questi fattori è un obiettivo primario. Gli algoritmi di routing per le reti *ad hoc* possono essere classificati in base al modo in cui l'informazione è acquisita e mantenuta e in base a cui questa è usata per trovare i cammini fra i nodi.

Generalmente ogni nodo annuncia la sua presenza nella rete ed ascolta la comunicazione tra gli altri nodi, che diventano conosciuti. Col passare del tempo ogni nodo acquisisce la conoscenza di tutti i nodi della rete e di uno o più modi per comunicare con loro.

Gli algoritmi di routing devono:

- assicurarsi che le dimensioni delle tabelle di routing siano ragionevolmente piccole, anche alla luce delle risorse ridotte delle quali spesso dispongono i nodi in una rete ad hoc;
- riuscire a scegliere il miglior percorso per raggiungere gli altri nodi (in base a vari parametri, come velocità, affidabilità e assenza di congestione);
- tenere le proprie tabelle di routing aggiornate nel caso la topologia di rete cambi;
- raggiungere il funzionamento ottimale in poco tempo e inviando un numero esiguo di pacchetti.

I protocolli per le reti ad hoc possono essere generalmente classificati a seconda delle strategie seguita in proattivi, reattivi e ibridi:

- *proattivi* (o *table-driven*): basati su una diffusione di informazioni di routing per mantenere le tabelle consistenti e accurate per tutti i nodi della rete. Nel caso di struttura di rete "piatta", queste strategie hanno la potenzialità per calcolare il percorso ottimo. L'overhead richiesto per determinare questi percorsi può essere proibitivo nel caso di cambiamenti dinamici dell'ambiente. Il routing gerarchico è maggiormente adatto nel caso di reti ad hoc di grandi dimensioni.
- *reattivi*: stabiliscono su richiesta percorsi solo per un insieme limitato di nodi destinazione. Queste strategie tipicamente non mantengono informazioni globali su tutti i nodi della rete. Tuttavia fanno affidamento su una ricerca dinamica per stabilire un percorso tra una sorgente e una destinazione.
- *ibridi*: si basano sull'esistenza di una struttura di rete per ottenere stabilità e scalabilità in grandi reti. La rete è organizzata in cluster mutuamente adiacenti, a cui dinamicamente sono aggiunti e sottratti nodi. Il punto critico è quello di ridurre l'overhead necessario a mantenere i cluster.
- *altri*: altri protocolli di routing possono essere progettati in modo tale da organizzare la rete in modo gerarchico o geografico, possono essere ottimizzati per permettere il multicasting dei pacchetti o possono anche porre particolare riguardo sulla quantità di energia residua sui singoli nodi ("Energy-aware routing").

Per tenere conto delle esigenze particolari delle WSN, sono state proposte diverse strategie di routing.

Una prima classe di protocolli adotta una topologia di rete "piatta" (flat) nella quale tutti i singoli nodi sono considerati pari (*peer*). Un'architettura piatta presenta diversi vantaggi, incluso il minimo overhead per mantenere l'infrastruttura e la possibilità di trovare percorsi multipli tra i nodi per prevenire i guasti (*fault tolerance*).

Una seconda classe impone una struttura di rete che assicuri efficienza energetica, stabilità e scalabilità. I nodi sono organizzati in clusters nei quali un nodo con certe caratteristiche—per esempio, la più alta energia residua—assume il ruolo di *cluster head* che diventa il coordinatore delle attività all'interno del cluster e responsabile di fare girare le informazioni tra i cluster. Il *clustering* riduce notevolmente il consumo di energia ed estende l'arco di vita di una rete.

Una terza classe di protocolli usa un approccio data-centrico per disseminare interesse all'interno della rete. I nodi sono caratterizzati da attributi (approccio detto *attributo-based naming*): un nodo sorgente effettua una query cercando un attributo piuttosto che uno specifico nodo sensore a cui sono assegnati dei *task*.

Una quarta classe è detta *location-based*, utile in applicazioni in cui la copertura geografica delle rete è importante ed è rilevante sapere cosa accade intorno ad un nodo specifico.

Esaminiamo alcuni algoritmi di routine specifici per le WSN: *flooding* e sue varianti, *Sensor Protocol for Information via Negotiation (SPIN)*, *Low-Energy Adaptive Clustering Hierarchy (LEACH)* e *geographical routing*.

Il *flooding* è una tecnica comune usata frequentemente per la ricerca di cammini e per la disseminazione delle informazioni nelle reti ad hoc wireless e wired. Il *flooding* usa un approccio reattivo dove ogni nodo che riceve un pacchetto di controllo lo rinvia a tutti i suoi vicini. Il *flooding* presenta l'inconveniente di generare un numero enorme (teoricamente infinito) di pacchetti.

Si possono applicare delle tecniche per limitare il traffico generato:

- inserire in ogni pacchetto un contatore che viene decrementato ad ogni hop. Quando il contatore arriva a zero, il pacchetto viene scartato. Un appropriato valore iniziale può essere il diametro della sottorete;
- inserire una coppia (source router ID, sequence number) in ogni pacchetto. Ogni router esamina tali informazioni e ne tiene traccia, e quando le vede per la seconda volta scarta il pacchetto;
- *selective flooding*: i pacchetti vengono duplicati solo sulle linee che vanno all'incirca nella giusta direzione (per questo si devono mantenere apposite tabelle a bordo).

Il *flooding* non è utilizzabile in generale come algoritmo di routing, ma è utile in campo militare (offre la massima affidabilità e robustezza), è utile per l'aggiornamento contemporaneo di informazioni distribuite e come strumento di paragone per altri algoritmi, visto che trova sempre, fra gli altri, il cammino minimo.

Il *gossiping* è una variante del *flooding*: in questo caso, i nodi qui non usano il broadcast ma inviano i pacchetti ad un solo nodo selezionato in modo random tra i vicini.

Il *Sensor Protocol for Information via Negotiation (SPIN)* è un protocollo basato sulla disseminazione di informazioni che evita il *flooding* inviando metadati sul sensore, anziché i dati stessi. Poiché solo i nodi interessati rispondono e la dimensione dei metadati è inferiore a quella dei dati, risulta meno oneroso del *flooding*. Un ricevitore che esprime interesse nel dato può richiedere l'invio completo del dato stesso. Nella comunicazione vengono utilizzati tre tipi di messaggi:

- ADV, *advertise data*;
- REQ, *request for data*;
- DATA, *data message* (contiene il valore vero e proprio fornito dal sensore).

È possibile introdurre anche vincoli sui consumi energetici (es. approccio euristico). Questa forma di negoziazione assicura che i dati vengano inviati solo ai nodi interessati, eliminando il traffico e riducendo significativamente la trasmissione ridondante dei dati nella rete. Inoltre, si riduce fortemente il consumo di energia.

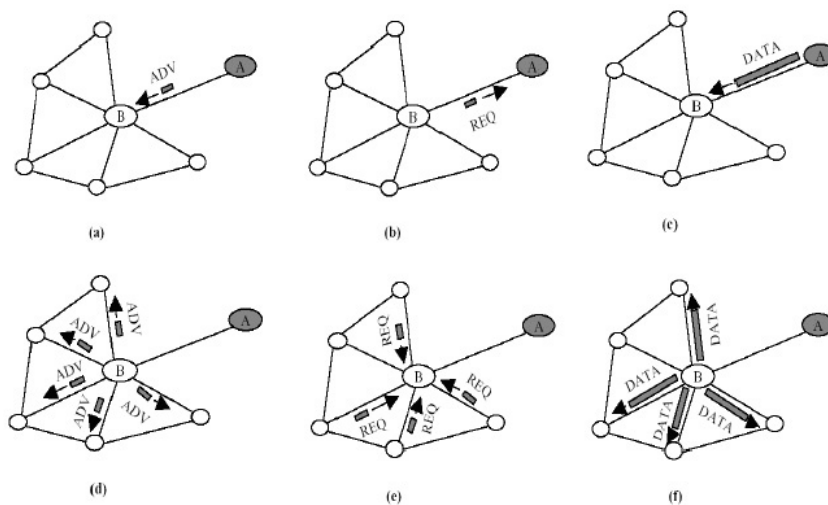


Figura 5: funzionamento di base del protocollo SPIN

L'algoritmo di tipo *LEACH (Low-Energy Adaptive Clustering Hierarchy)* è progettato per raccogliere dati e inviarli al nodo ricevente (data sink), tipicamente una stazione base. LEACH adotta una topologia in cui i nodi si auto-organizzano in cluster ed eleggono un nodo capo-cluster (Figura 6). Questi ultimi comunicano con i capo-cluster vicini costituendo così una struttura gerarchica fino alla stazione base. Il protocollo minimizza la dissipazione di energia, in quanto il capo-cluster riceve ed aggrega i dati dei nodi appartenenti al cluster prima di inviarli alla stazione base. Dopo un certo periodo di tempo la rete entra nuovamente in fase di setup e inizia nuovamente la fase di selezione dei capo-cluster.

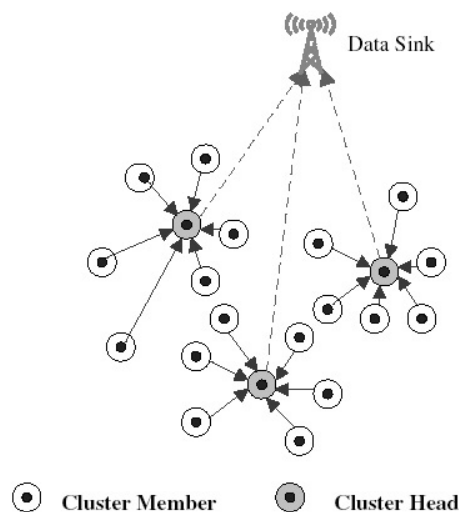


Figura 6: Modello LEACH

L'obiettivo principale degli algoritmi geografici di routine (geographical routine) è usare informazioni sulla locazione dei nodi per formulare un'efficiente ricerca fino alla destinazione. Un algoritmo di questo tipo è molto comodo nelle reti di sensori perché minimizza il numero di trasmissioni attraverso la stazione base eliminando ridondanza di dati trasmessi.

5. Protocolli di trasporto

L'architettura dei computer e delle reti di comunicazione è strutturata in livelli (o layer) in cui ogni livello agisce come *service provider* del livello immediatamente superiore, che agisce come utente del servizio. Le interazioni tra livelli contigui avvengono attraverso dei punti detti *service access point (SAP)*.

Il livello di rete (L3) fornisce servizi di indirizzamento e instradamento (*routing*) al livello superiore, il livello di trasporto (L4), che a sua volta fornisce servizi di trasporto messaggi al livello superiore (L5, livello sessione).

In questo modello i tre livelli inferiori (L1-fisico, L2-datalink e L3-rete) sono presenti in tutti i nodi, mentre il livello di trasporto e quello di sessione esistono solo negli end-point (o host) e agiscono come parte di funzioni di protocollo end-to-end.

Il livello di trasporto è responsabile anche della segmentazione dei dati provenienti dal livello superiore: alla sorgente i messaggi sono trasformati in una catena di segmenti e sono riassemblati nel messaggio originale una volta arrivati a destinazione.

I protocolli di trasporto più noti sono il *transport control protocol (TCP)* e lo *user datagram protocol (UDP)*, comunemente usati in Internet ma non adatti per le WSN.

Le ragioni sono molte: una delle principali è l'assenza d'interazione tra TCP e UDP e i protocolli dei livelli più bassi. Nelle WSN, tali livelli portano informazioni molto utili al livello di trasporto e al miglioramento delle prestazioni di sistema.

Nel definire un protocollo di trasporto per le WSN dobbiamo tenere in considerazione molti fattori. Le WSN dovrebbero essere progettate considerando alcuni fattori critici, quali conservazione dell'energia, controllo della congestione, affidabilità nel trasporto dei dati, sicurezza e gestione. Queste condizioni spesso coinvolgono uno o più livelli dei protocolli gerarchici. Per esempio, il controllo della congestione può riguardare solo il livello di trasporto, mentre la conservazione dell'energia può essere collegata almeno ai livelli fisico, data link e rete.

Il progetto di un protocollo di trasporto per le WSN deve considerare diversi aspetti:

1. Il protocollo dovrebbe garantire il controllo della congestione e il trasporto dei dati in modo affidabile. Le congestioni possono avere luogo nel nodo *sink* dove arriva la maggior parte dei dati che partono dai nodi sensori. Sebbene il protocollo MAC possa recuperare pacchetti persi per *bit error*, non è però in grado di trattare perdite dovute a *buffer overflow*. Le WSN necessiterebbero di un meccanismo simile a quelli usati da TCP, come ad esempio ACK, anche se bisognerebbe tenere conto del fatto che le problematiche nelle reti di sensori sono diverse che in Internet. Infatti in certe applicazioni, i nodi potrebbero avere bisogno di ricevere pacchetti solo da alcuni nodi in una certa area e non da ogni singolo nodo in quell'area. Inoltre, i due problemi potrebbero essere efficacemente risolti con un approccio *hop-by-hop* che potrebbe anche minimizzare la dimensione dei buffer nei nodi intermedi.
2. Il protocollo dovrebbe garantire la semplificazione del processo di connessione iniziale oppure potrebbe essere del tipo *connectionless* (senza connessione, come UDP, in cui lo scambio di dati tra la sorgente e il/i destinatario/i non richiede l'operazione preliminare di creare tra di essi un circuito, fisico o virtuale, su cui instradare l'intero flusso di dati in modo predeterminato e ordinato nel tempo) per accelerare il processo, aumentare il *throughput* e abbassare il ritardo di trasmissione. La maggior parte delle applicazioni in WSN sono reattive, quindi i nodi monitorano e aspettano un evento per inviare dati al *sink*: i pacchetti da inviare possono essere anche pochi.
3. Il protocollo di trasporto dovrebbe evitare perdite di pacchetto quanto più possibile poiché le perdite si traducono in spreco di energia. Per evitare tali perdite, il protocollo dovrebbe usare un controllo di congestione attiva (Active Congestion Control, ACC): il controllo va attivato prima che la congestione abbia effettivamente luogo. Per esempio, il nodo che invia o un nodo intermedio può ridurre la velocità quando la dimensione del buffer raggiunge una certa soglia.
4. Il protocollo dovrebbe garantire un comportamento corretto per tutti i tipi di nodi sensori, riservando lo stesso trattamento a sensori con differente distanza dal *sink*.
5. Se possibile, il protocollo dovrebbe essere progettato tenendo in mente criteri di ottimizzazione cross-layer per aumentare le prestazioni. Per esempio, se un algoritmo di instradamento informasse il protocollo di trasporto di un buco nel percorso, il protocollo dovrebbe essere in grado di dedurre che il problema è causato dal percorso e non da una congestione. In questo caso, non sarebbe necessario cambiare la velocità di trasferimento.

Attributes	CODA	ESRT	RMST	PSPQ	GARUDA
Direction	Upstream	Upstream	Upstream	Downstream	Downstream
Congestion					
<i>Support</i>	Yes	Passive	No	No	No
<i>Congestion detection</i>	Buffer	Buffer	—	—	—
	occupancy	occupancy			
	channel condition				
<i>Open- or close-loop congestion control</i>	Both	No	—	—	—
Reliability					
<i>Support</i>	No	Yes	Yes	Yes	Yes
<i>Packet or application reliability</i>	—	Application	Packet	Packet	Packet
<i>Loss detection</i>	—	No	Yes	Yes	Yes
<i>End-to-end (E2E) or hop-by-hop (HbH)</i>	—	E2E	HbH	HbH	HbH
<i>Cache</i>	—	No	Option	Yes	Yes
<i>In- or out-sequence</i>	—	N/A	In-sequence	Out-of-sequence	Out-of-sequence
<i>NACK</i>	—	ACK	NACK	NACK	NACK
<i>ACK or NACK</i>	—	ACK	NACK	NACK	NACK
Energy conversation	Good	Fair	—	—	Yes

Tabella 1- Protocolli di trasporto per WSN

In Tabella 1 sono riportate le caratteristiche di alcuni protocolli esistenti.

CODA (*Congestion Detection and Avoidance*) è una tecnica di controllo della congestione in upstream. Rileva le congestioni monitorando l'occupazione del buffer e il carico sul canale wireless. Se questi eccedono una soglia prefissata, vuole dire che si è in presenza di congestione.

ESRT (*Event-to-Sink Reliable Transport*) calcola periodicamente il tasso di pacchetti ricevuti con successo in un dato intervallo di tempo attraverso un valore d'affidabilità (*reliability*). Lavora principalmente sul *sink*.

RMST (*Reliable Multisegment Transport*) garantisce il successo della trasmissione di pacchetti in upstream.

PSPQ (*Pump Slowly. Fetch Quickly*) distribuisce dati dal *sink* ai sensori con una cadenza relativamente lenta permettendo a quest'ultimi di recuperare segmenti persi dai nodi immediatamente vicini.

GARUDA garantisce il successo della trasmissione di pacchetti in downstream.

Un protocollo di trasporto per le WSN dovrebbe tenere conto di tutti i fattori critici, mentre i protocolli esistenti, tra cui quelli riportati in Tabella 1, affrontano solo alcuni aspetti e spesso in una sola direzione (o upstream o downstream). Molte applicazioni, per esempio operazioni di sorveglianza, richiedono protocolli che lavorino in entrambi i sensi.

Un altro problema con i protocolli esistenti è che controllano le congestioni o *end-by-end* o *hop-by-hop*. In CODA sono presenti entrambi i controlli, ma sono usati simultaneamente piuttosto che adattivamente. Un controllo adattivo che integri entrambi i meccanismi può essere più vantaggioso per reti di sensori wireless con diverse applicazioni e utile grazie alla conservazione dell'energia e alla semplificazione delle operazioni dei sensori.

I protocolli studiati finora sono affidabili o a livello di pacchetto o a livello di applicazione. Se una rete di sensori supportasse due applicazioni, di cui una affidabile a livello di pacchetto e l'altra a livello di applicazione, i protocolli attuali avrebbero difficoltà a trattarle. La soluzione sarebbe un meccanismo di ripristino adattivo in grado di garantire affidabilità in entrambi i livelli e anche di assicurare efficienza energetica.

Nessuno dei protocolli esistenti assicura inoltre ottimizzazione cross-layer.

6. Gestione di rete

Una rete di comunicazione di computer generalmente consiste di tre componenti: device fisici—inclusi i link sia wireless che wired, nodi di rete (hub, bridge, switch, router), terminali e server—protocolli, dati e applicazioni.

I protocolli sono usati per trasportare informazioni in modo efficiente, preferibilmente in modo corretto, sicuro, affidabile e comprensibile. Sono insieme di software residenti nei device fisici. La collaborazione tra device fisici e protocolli di rete costituisce un solido supporto per le applicazioni.

Tuttavia, i device e i protocolli non sono sufficienti per supportare in modo efficace le operazioni di una rete di comunicazione: sono anche richiesti strumenti e tecniche di gestione della rete (NM, Network Management) per i servizi e per assicurare la cooperazione delle varie entità.

Algoritmi di gestione della rete sono fondamentali in varie situazioni:

- Molti elementi ed entità software che formano la rete che possono presentare dei guasti e dei malfunzionamenti. Una apposita funzionalità di gestione deve essere in grado di determinare quando, dove e perché si manifesta il malfunzionamento e come ripristinare lo stato corretto.
- L'ottimizzazione delle prestazioni di un sistema distribuito richiede che la gestione della rete collabori al processo.

- Per la maggior parte delle reti, le funzioni di NM possono essere usate per raccogliere e analizzare il comportamento dell'interazione dell'utente durante l'interfacciamento con la rete, fattore molto importante per pianificare l'evoluzione a lungo termine della capacità di rete e le sue prestazioni.

Progettare degli algoritmi per la gestione di rete consiste nel determinare un insieme di funzioni per:

- monitorare lo stato della rete;
- riconoscere errori e anomalie nella rete;
- amministrare, controllare e configurare componenti di rete;
- provvedere alle normali operazioni;
- migliorare l'efficienza della rete e le prestazioni delle applicazioni.

Per effettuare tutte queste operazioni, un NM necessita di collezionare in tempo reale informazioni dagli elementi di rete, analizzarle e applicare controlli basati su queste informazioni. Spesso ogni elemento di rete organizza e gestisce le sue informazioni (Management Information Base, MIB). Generalmente c'è un agente in ogni elemento che raccoglie i dati e riferisce ad un centro di gestione che ha visione dell'intera rete di informazioni.

Tra i modelli tradizionali di Network Management possiamo annoverare SNMP (*Simple Network Management Protocol*) e TOM (*Telecom Operation Map*).

SNMP è il protocollo più usato. Comprende tre componenti: un sistema di gestione della rete (NMS, Network Management System), gli elementi da gestire (router, switch, server e host) e gli agenti. Lo NMS è costituito da un insieme d'applicazioni che monitora e/o controlla gli elementi da gestire, ed in grado di espletare diversi compiti. Ciascun elemento è gestito da un agente. Lo SNMP è un protocollo semplice e di larga applicazione, ma ha il problema di richiedere troppa banda.

TOM è basato su modelli di gestione servizi e di gestione di rete. TOM fornisce solo un framework per la gestione dei servizi strutturati in livelli su due dimensioni.

Nessuno dei due è adatto a trattare con le WSN, anche se l'architettura a livelli di TOM e la semplicità di SNMP sono caratteristiche da considerare nella progettazione di protocolli per le reti di sensori wireless.

Le WSN hanno generalmente una struttura ad hoc e risorse limitate che influiscono sulla progettazione dei protocolli di rete, del modello applicativo e del sistema operativo.

La gestione di rete deve usare le risorse in modo efficiente e efficace e gioca un ruolo più cruciale che nelle reti tradizionali perché molta della conoscenza e informazione è "sparsa" su tutta la rete e solo un algoritmo di gestione può essere in grado di "raccogliere" tale informazione per definire il comportamento dell'intera rete: il livello di varie risorse, l'area di copertura, l'organizzazione dei nodi e il livello di cooperazione tra i nodi.

Nonostante la criticità, il problema non è stato finora studiato con la dovuta attenzione e sono state applicate le soluzioni già esistenti (SNMP e TOM) anche se con soluzioni insoddisfacenti.

Sono molte le caratteristiche rilevanti che un sistema di gestione rete dovrebbe possedere:

- ridotto consumo energetico e ridotto uso di banda considerando che le comunicazioni richiedono molta energia;
- soluzioni scalabili, tenendo conto del fatto che i nodi di una rete possono essere da decine a migliaia;
- soluzioni semplici e pratiche, poiché le WSN sono sistemi distribuiti vincolati alle risorse;
- il modello informativo per i nodi sensori, le caratteristiche e le applicazioni della WSN dovrebbero essere contenuti nel MIB;
- interfaccia verso le applicazioni.

Ci sono altri elementi che concorrono ad una buona gestione di rete, come l'etichettatura dei nodi (*naming*), la localizzazione, la manutenzione e la tolleranza ai guasti (*fault tolerance*). *Naming* è lo schema usato per identificare i nodi sensori: può abbassare i costi di computazione e rendere più efficiente dal punto di vista energetico il protocollo di routing.

La localizzazione permette di individuare dove è un nodo: è un servizio utile a molte applicazioni.

L'attività di manutenzione coinvolge molti aspetti, quali cambio di batterie, configurazione dei nodi sensori, etc.

Una rete di sensori può essere soggetta a diversi guasti e/o problemi, sia hardware che software. I meccanismi di recupero richiesti sono quindi di tipo differente a seconda del tipo di emergenza. Proprio per queste ragioni, dovrebbero essere presenti funzionalità di fault tolerance.