SAPIENZA
UNIVERSITÀ DI ROMA

Facoltà di Ingegneria

Corso di laurea in Ingegneria delle Telecomunicazioni

Reti wireless multihop per applicazioni in ambito industriale

Candidato
Simone Allemanini
801145

Relatore
Maria Gabriella Di Benedetto

Correlatore
Luca De Nardis

A/A 2009/2010

INDICE

1. INDUSTRIAL ETHERNET

1.1 I SISTEMI DI COMUNICAZIONE IN AMBIENTE INDUSTRIALE

Solitamente troviamo almeno quattro livelli gerarchici in un sistema di comunicazione in ambito industriale.

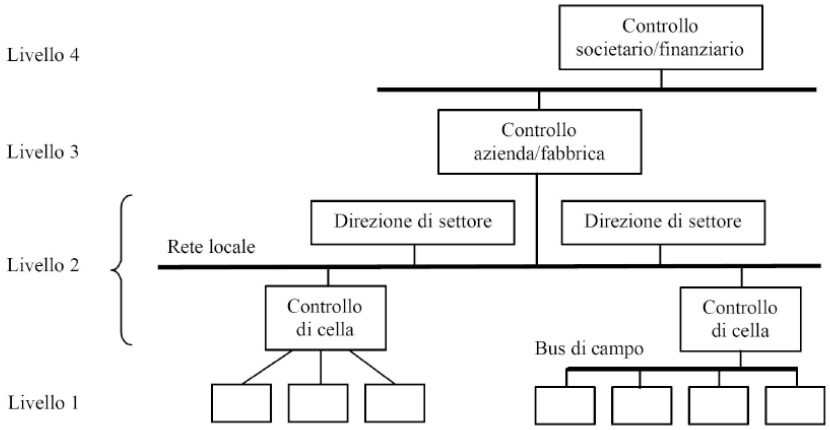


Figura 1 - Livelli in un sistema di comunicazione in ambito industriale

Nel caso si analizzi l'organizzazione del solo reparto di produzione di una azienda, è possibile individuare la tipica struttura visibile nella seguente figura.

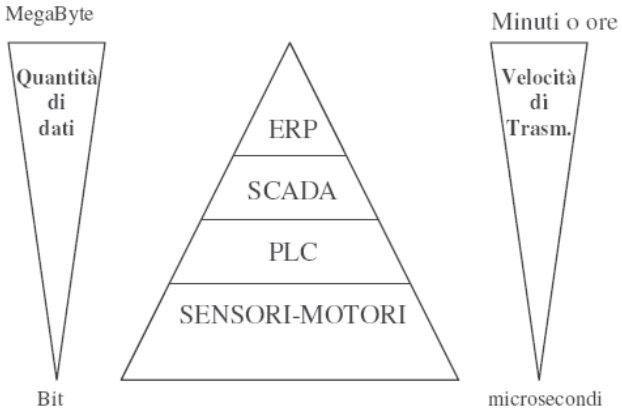


Figura 2

Tipicamente in questo ambito il livello 1 è costituito dai trasduttori (finecorsa, sensori, encoder,…) e attuatori (relè, motori, elettrovalvole, spie di segnalazione,…) posti sull'impianto di produzione; a livello 2 ci sono i controllori di cella (PLC,

CNC) che controllano sensori e trasduttori ai quali sono collegati direttamente o tramite bus di campo. Tutti i PLC che coordinano le varie celle di un reparto di produzione sono collegati fra loro tramite rete locale alla quale si connette anche un sistema SCADA (Supervisory Control And Data Acquisition, Sistema centralizzato di supervisione e controllo di sistemi distribuiti) di supervisione (livello 3). Il livello 3 viene anche detto livello di sistema e i sistemi di comunicazione vengono detti bus di processo o di cella. A livello 4, detto anche livello di controllo e di servizio, ci sono i sistemi CAD/CAM. Tali sistemi elaborano i dati di produzione e li presentano in una forma adeguata al management, prelevandoli da tutti i sistemi SCADA della fabbrica ai quali sono connessi, sempre tramite LAN.
Salendo nella piramide aumenta la quantità di dati e diminuiscono i requisiti relativi alla velocità del collegamento.

1.1.1 IL CONCETTO DI REAL-TIME

Con il termine **determinismo** si indica la rapidità del sistema a reagire *entro un intervallo di tempo prevedibile* (<100 msec).
Il **tempo reale**, nel contesto dei bus di campo, è legato al concetto di determinismo. Un sistema tempo reale reagisce in un *arco di tempo definito più ristretto* (< 10 msec). In una **rete isocrona** il trasferimento dati avviene in tempo reale ad intervalli di tempo equidistanti. Tale rete:

- garantisce il trasferimento di dati tra diverse stazioni entro un intervallo di tempo definito
- consente un'esatta determinazione (previsione) del momento del trasferimento dei dati

1.1.2 LA SINCRONIZZAZIONE E I BUS DI CAMPO

La decentralizzazione diventa sempre più importante nella realizzazione di moderni impianti di automazione.
Questo trend è motivato soprattutto dal prezzo e da una installazione più facile. Oggi gli utenti richiedono soluzioni decentrate anche per il comando di macchine veloci. I processi di produzione e di lavorazione diventano sempre più veloci. Contemporaneamente crescono anche le esigenze relative alla precisione della produzione.
In quest'ottica vengono richiesti tempi di reazione di processo brevi, definiti e riproducibili.
Applicazioni che necessitano di queste esigenze sono:

- Motion Control
- Sincronismo
- Regolazioni
- Programmatori a camme a base software
- Misure multiple
- Misura del numero di giri e di portata

E’ possibile soddisfare quest'esigenza realizzando un accoppiamento diretto tra il ciclo equidistante, le unità di periferia ed il programma applicativo.
L'accoppiamento sincrono di una soluzione di automazione viene definita "**isocronismo**". L’isocronismo è molto adatto per applicazioni in cui i sensori e gli attuatori sono distribuiti sulla macchina.

1.2 ETHERNET A LIVELLO INDUSTRIALE

Nel settore dell’automazione industriale si sta cercando di introdurre la rete Ethernet anche a livello di campo. La rete Ethernet è molto diffusa a livello mondiale e l’introduzione di Ethernet a livello industriale può portare diversi vantaggi. Oltre ai vantaggi economici, un altro vantaggio consiste nella possibilità di utilizzare internet a livello industriale. Ethernet esisteva già a livello industriale, ma solo fino a pochi anni fa era concentrata solo a livello amministrativo. Era la rete che collegava i vari uffici dell’amministrazione oppure collegava gli impianti di produzione a livello di area, non era la rete su cui viaggiavano i dati critici dell’automazione, con cui vengono, ad esempio, controllati gli azionamenti. Con il termine Industrial Ethernet ci si riferisce in genere a quelle applicazioni che utilizzano Ethernet per le comunicazioni a livello di campo, ossia di PLC e periferia. Per capire come è stato possibile utilizzare Ethernet a livello di bus di campo, si deve analizzare il suo funzionamento.

1.2.1 LA COMUNICAZIONE CSMA/CD

IEEE 802.3 si basa su un metodo di accesso multiplo **CSMA - Carrier Sense Multiple Access**. Ogni nodo gestisce in modo autonomo l’accesso al bus e tutti i nodi sono in “ascolto” continuo (Carrier Sensing) sul bus. Un nodo è in grado di riconoscere quando il bus è libero attraverso l’assenza del segnale portante (Carrier) ed di rilevare una collisione. Se il bus è libero, un nodo può tentare di accedervi rispettando l’inizio del time slot successivo. Uno slot time definisce il tempo massimo di ritardo di propogazione fisica del segnale sull’intera rete (**Collision Domain** = diametro massimo della rete). Nel CSMA/CD quando un nodo che sta trasmettendo rileva una collisione, sospende la sua trasmissione ed invia un segnale di avvenuta collisione.
Dopo una collisione un nodo rinnova il tentativo di trasmissione. Il suo tempo di attesa viene incrementato secondo un algoritmo detto di “back-off” in cui il tempo di attesa per ciascun nodo è funzione del numero di collisioni consecutive rilevate e del numero stimato di altri nodi. Al crescere del numero delle collisioni, il tempo di attesa cresce in modo esponenziale (algoritmo di back-off); maggiore è il tempo di attesa, minori sono le possibilità per un nodo di acquisire il canale di trasmissione.

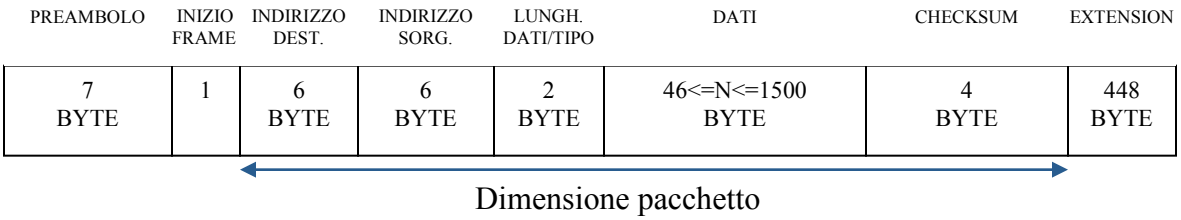
1.2.2 ETHERNET COME BUS DI CAMPO

La connessione tra le stazioni di comunicazione avviene in Ethernet attraverso la tecnica a “**commutazione di pacchetto**”. Ogni singolo pacchetto di dati può seguire un diverso percorso per raggiungere la destinazione finale. Il sistema ricevente

riceve quindi spesso i dati in ordine sparso. Ciò determina l'esigenza, da parte del sistema trasmittente, di etichettare ciascun pacchetto di dati con un numero che ne identifica la posizione all'interno della sequenza di trasmissione. Il sistema di ricezione può così utilizzare tali valori per ricostruire la sequenza originale dei dati. Il vantaggio della tecnica di commutazione a pacchetto è che non necessita di una grande larghezza di banda. Essa è particolarmente utile quando occorre trasmettere i tradizionali dati di una rete (es. file di database) mentre si rivela inadeguata per la trasmissione di dati audio e video e in generale per le comunicazioni real-time. Un pacchetto di dati Ethernet è un insieme di impulsi digitali trasmessi attraverso il mezzo trasmissivo.
Esso può essere di dimensione variabile (da 64 a 1518 byte) ed è composto da 4 parti
principali :

- Preambolo: Le informazioni sono trasmesse in modo asincrono in forma di pacchetti. Non avendo una linea di clock, ma solo una linea dati è necessaria una fase di sincronizzazione. In questa fase si utilizzano i 7 byte del preambolo, byte composti da bit 0 e 1 alternati che servono per sincronizzare il ricevitore.
- Inizio del Frame: Byte che delimita l'inizio del frame, uguale a 10101011
- Indirizzo destinatario: Contiene informazioni che riguardano il mittente del pacchetto (6 byte).
- Indirizzo sorgente: Contiene informazioni che riguardano il destinatario del pacchetto (6 byte). I valori, detti anche indirizzi MAC (Media Access Control) rappresentano gli indirizzi dei due sistemi collegati e rappresentano dei numeri univoci che identificano ciascun singolo dispositivo di rete.
- Lunghezza dei dati: indica il numero di byte presenti nel pacchetto dati (2 byte).
- Dati: Effettive informazioni che devono essere trasmesse (da 46 a 1500 byte).
- Checksum: Sequenza utilizzata per verificare la correttezza dei dati ricevuti. Il sistema trasmittente elabora questi byte mediante un algoritmo chiamato CRC(Cyclic Redundancy Check) (4 byte).
- Extension: L'estensione dei pacchetti viene effettuata sui pacchetti corti per garantire uno slot time di almeno 4,096µs (512 byte =448 + 64).

In figura è visibile il tipico messaggio ETHERNET. Ethernet è standardizzata tramite la norma IEEE 802.3.
Le specifiche coprono per esempio la tecnologia d'accesso, i metodi di trasmissione e i mezzi di trasmissione per Ethernet classica, per Gigabit Ethernet (1000 Mbit/s). Gigabit Ethernet 1000 Mbit/s è un'estensione compatibile di Ethernet di 10 Mbit/s ed Ethernet 100Mbit/s. Questa è la versione più adatta per la comunicazione a livello di campo coniugando velocità e basso costo di componenti e infrastrutture.



Ipotizzando una rete 1000 Base-X, si osserva che per sensori o attuatori semplici, quale ad esempio un sensore di umidità che si limita a trasmettere due bytes (1 dato = 2 bytes = percentuale di umidità), Ethernet risulta poco efficiente. Infatti, il tempo *Teth* per trasmettere l'informazione risulta pari a 4,256 μs con una efficienza ηeth risultante inferiore al 10%.

Dimensione minima pacchetto Ethernet = 14 + 46 + 4 = 64 byte
Dimensione Extension = 448 byte
Dimensione Inter packet gap = 12 byte

$$Teth = (64 + 8 + 448 + 12) \times 8 \times Tbit = \mathbf{4{,}256\ \mu s} \quad \text{con } Tbit = 1/1000 \text{ Mb/s}$$

$$\eta eth = (d \times 8 \times Tbit) / (64 + 8 + 448 + 12) \times 8 \times Tbit \approx \mathbf{2{,}4\ \%} \quad \text{con } d=2$$
$$\eta eth = (d \times 8 \times Tbit) / (64 + 8 + 448 + 12) \times 8 \times Tbit \approx \mathbf{9{,}5\ \%} \quad \text{con } d=8$$

Ovviamente se si considerano i protocolli a livello superiore, come IP o TCP, l'efficienza tende a peggiorare, pur considerando l'header (H) minimo, e la rete libera (il data-rate può essere notevolmente ridotto in caso di rete affollata). Storicamente l'impiego di Ethernet come bus di campo è risultato penalizzato dal non-determinismo e, per quanto concerne la scarna messaggistica dei sensori e degli attuatori, dalla bassa efficienza, dato che **il numero di byte trasmessi è elevato rispetto al numero di byte che contengono effettivamente informazione**. Oggi, la diffusa presenza di switch, che inoltrano il messaggio solo al destinatario, e l'aumento della velocità di trasmissione (10MHz, 100MHz, 1GHz) riducono notevolmente la probabilità di collisione, per cui Ethernet diventa una soluzione sempre più interessante anche per le applicazioni veloci quali i bus di campo. Il non determinismo di Ethernet non sembra particolarmente penalizzante rispetto ai bus di campo nei sistemi a bassa dinamica, in quanto una rete in ambiente industriale viene progettata con un ridotto numero di utenti e, in genere, segmentata su più reti locali. Anche la bassa efficienza, aggravata dalla presenza di protocolli di una certa complessità quali UDP-IP o TCP-IP, risulta meno penalizzante grazie alle elevate velocità di trasmissione, e in generale è un argomento meno valido rispetto alla presenza delle infrastrutture. Ethernet ha la sua naturale evoluzione in Internet, che consente una diagnostica decentrata di semplice implementazione. E' per questo motivo che anche a livello industriale vanno affermandosi protocolli standard, quali quelli utilizzati dai comuni browser, come Internet Explorer o Netscape Navigator (IP, TCP, HTTP) e cominciano a comparire sul mercato i primi web-sensors, ossia sensori direttamente interfacciati su Internet e consultabili mediante un comune browser anche se non pienamente compatibili con i protocolli in questione.

1.2.2.1 IL COLLEGAMENTO DEI DISPOSITIVI TRAMITE SWITCH

La rete Ethernet che funziona utilizzando il protocollo CSMA/CD è adatta per un bus di campo?
L'utilizzo di CSMA/CD può generare delle collisioni fra i pacchetti, quindi sembrerebbe non adatta per applicazioni industriali a livello di campo. Il problema delle collisioni è stato risolto connettendo i vari dispositivi tramite uno switch. Gli switch inoltrano il messaggio solo al destinatario. In questo caso non abbiamo più dispositivi connessi su uno stesso bus. Ogni dispositivo è connesso ad una porta dello switch. Se la stazione A vuole parlare con la stazione B e la stazione C vuole parlare con la stazione D si creano all'interno dello switch dei circuiti per cui le informazioni passano direttamente da C e D e da A a B. Cosa succede se la stazione A sta parlando con la stazione B, ma anche D vuole parlare con B? Non abbiamo collisione perché lo switch è un elemento con memoria. Può memorizzare quello che la stazione D voleva dire alla stazione B e spedirlo quando la stazione B ha finito di parlare con A. All'interno dello switch ci sono dei buffer che permettono di memorizzare i vari pacchetti nel caso la destinazione sia occupata. Questo permette, fino a quando non si satura il buffer, di non perdere nessun pacchetto. Il costo di uno switch è in genere proporzionale alla dimensione di questi buffer.

1.2.2.2 INCAPSULAMENTO

L'idea più semplice per utilizzare ethernet con i protocolli di bus di campo esistenti è stata quella di incapsulare i protocolli esistenti all'interno del campo dati del pacchetto ethernet. Un esempio di incapsulamento è **Ethernet /Ip** (Ethernet Industrial Protocoll). Si è incapsulato all'interno del pacchetto ethernet un bus di campo quale DeviceNet.
DeviceNet in questo caso diventa uno dei tanti protocolli applicativi oltre a Http e Ftp. Sotto il livello applicativo ci si avvale ancora del protocollo TCP/IP. EtherNet/IP mantiene invariati il livello fisico ed il metodo di accesso CSMA/CD Standard Ethernet IEEE, utilizza i servizi offerti dai protocolli TCP/IP e integra tutte le funzioni del protocollo applicativo CIP - Control and Information Protocol, cuore della tecnologia di comunicazione NetLinx di Rockwell Automation.
L'impiego di EtherNet/IP permette in pratica di realizzare soluzioni di controllo distribuite con prestazioni paragonabili a quelle di ControlNet. Un altro degli standard più diffusi, grazie alla sua semplicità è **Modbus** over TCP. In tutti questi standard si tende a preservare il livello di applicazione rispetto al bus di campo adottato. Si tratta di protocolli in genere poco adatti ad applicazioni di "motion control" e i tempi di ciclo sono nell'ordine della decina di ms. Un approccio di questo tipo presenta i seguenti svantaggi. Il passaggio attraverso l'incapsulamento e poi attraverso TCP/IP ,crea dei ritardi che oltretutto non sono costanti. Sono quindi stati sviluppati altri protocolli per applicazioni in tempo reale, i cosiddetti protocolli isocroni real-time.

1.3 METODOLOGIE DI APPROCCIO PER L'IMPIEGO DELL'INDUSTRIAL ETHERNET

Ethernet come tecnologia 'pura' occupa solo i livelli più bassi della pila ISO OSI. I diversi dialetti parlati tutt'oggi nel mondo dell'Ethernet Industriale si differenziano nei livelli compresi tra 3 (livello di rete) e 7 (livello di applicazione). Una

linea comune, almeno in parte, a tutte le implementazioni è rappresentata dalla presenza dei protocolli di secondo e terzo livello resi celebri dalla diffusione di Internet e generalmente noti sotto il nome di stack TCP/IP.

In linea di massima è possibile identificare tre diversi modi di utilizzare Ethernet nell'industria:

1. **ENCAPSULATE TRAMITE TCP-UDP**

2. **HYBRID**

3. **RTPS (Real-Time Publish Subscribe)**

Prima di passare a descrivere alcune di queste implementazioni, è utile fare una breve digressione sull'ultimo dei grandi ostacoli che è necessario superare per potersi affacciare sul campo: il determinismo. L'impiego di una topologia a stella commutata con tratte full-duplex ha ridimensionato considerevolmente questo problema e la separazione dei domini di collisione ha contribuito a renderlo ancora più marginale. Le applicazioni di controllo sono tuttavia molto esigenti da questo punto di vista ma sono state sviluppate varianti in grado di gestire informazioni in tempo reale con latenze comparabili a quelle dei bus di campo.

1.3.1 ENCAPSULATE TRAMITE TCP-UDP

I vantaggi di impiegare dei protocolli giù rodati e di incapsulare i loro messaggi all'interno dei datagrammi TCP o UDP sono abbastanza chiari: la curva di apprendimento è ridotta, dato che è possibile riciclare il know-how maturato in anni di utilizzo del bus di campo prescelto; si possono utilizzare gli stessi dispositivi a fronte di poche modifiche; le comunicazioni da e verso la rete gestionale e il software di supervisione sono praticamente trasparenti, dato che tutto quello che serve è estrarre dai pacchetti IP ricevuti le informazioni inserite dai dispositivi sul campo. Esistono diversi approcci di incapsulamento che seguono a grandi linee questo tipo di schema. Ethernet/IP (in breve EIP) è la trasfigurazione su Ethernet dei bus di campo DeviceNet e ControlNet; ModBus/TCP rappresenta sostanzialmente un'implementazione del diffuso bus ModBus su stack TCP/IP; recentemente ModBus è stato reso disponibile anche per l'implementazione IDA di cui tratteremo tra poco; la Fieldbus Foundation ha messo a punto uno standard denominato HSE (High Speed Ethernet) che porta i vantaggi del bus di campo H1.
La figura 4 mostra l'architettura di una parte dei protocolli impiegati da Ethernet/IP: un protocollo di incapsulamento interfaccia TCP e UDP con il Control and Information Protocol (CIP) utilizzato anche da DeviceNet e ControlNet. Il sistema utilizza un modello a oggetti per distinguere i dati provenienti da questi due bus da quelli giunti da Ethernet. Il protocollo TCP viene impiegato per veicolare le informazioni di tipo non deterministico, mentre per i dati critici che devono essere resi disponibili in tempo reale o quasi ci si appoggia al più leggero UDP. Lo schema di scambio delle informazioni è di tipo editore-abbonato e in quanto tale offre una trasmissione multicast molto efficiente.

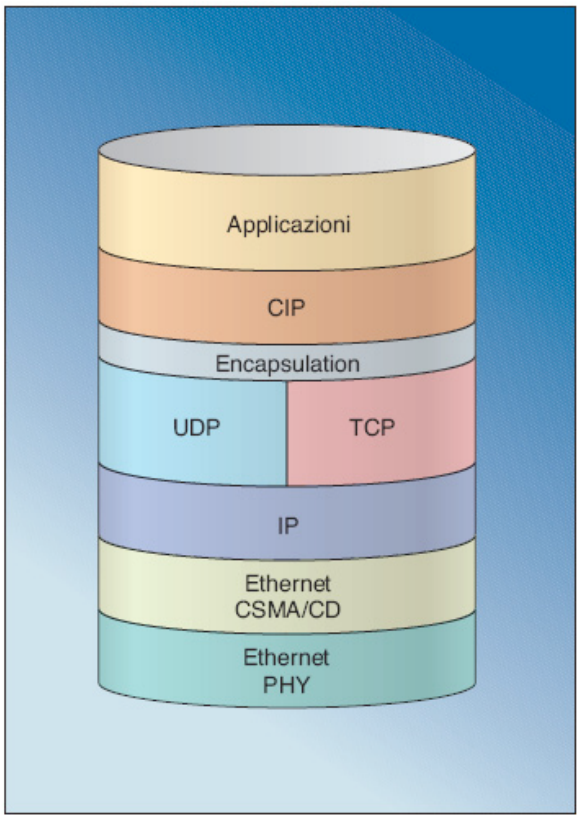


Figura 3 - Rappresentazione semplificata dell'architettura Ethernet/IP, che sfrutta i concetti sviluppati con DeviceNet e ControlNet

1.3.2 HYBRID TECHNIC

Come esempio del secondo approccio all'Ethernet industriale, citiamo brevemente gli standard Profinet e Ethernet Powerlink (figura 5).

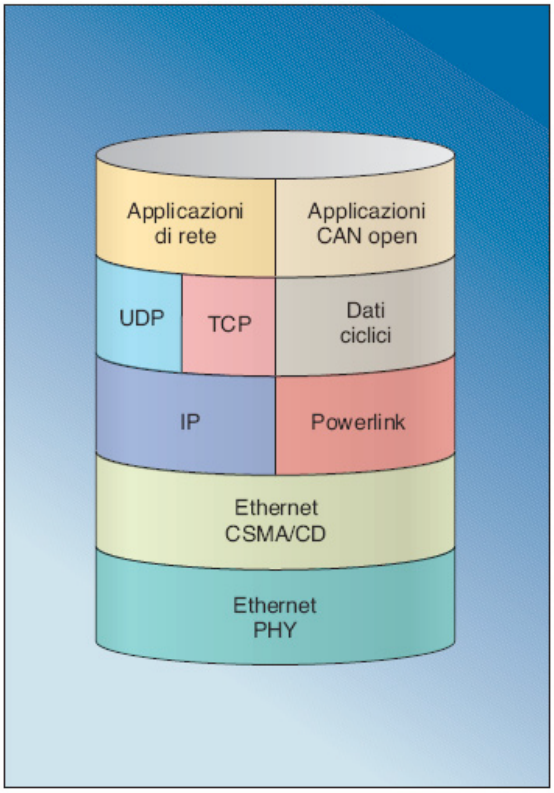


Figura 4 - Schema dell'architettura Ethernet PowerLink

Si tratta di due implementazioni per certi aspetti simili che separano il mondo strettamente deterministico associato agli I/O e al campo da quello più 'rilassato' della rete Ethernet tradizionale ai livelli superiori. Powerlink utilizza una topologia ad albero con dei tradizionali hub Fast Ethernet e sfrutta un'architettura di tipo master-slave con interrogazione (polling) dei dispositivi. La separazione tra i componenti in tempo e i dispositivi tradizionali che non richiedono un determinismo spinto è di fatto fisica, in quanto le sottoreti in tempo reale dialogano con la rete Ethernet tradizionale attraverso opportuni ponti. I messaggi provenienti dai dispositivi critici hanno la precedenza sui comuni pacchetti TCP/IP che viaggiano in rete. Profinet è un'implementazione basata su tecnologia Ethernet che utilizza la tecnologia DCOM (Distribute Component Object Module) per interfacciare il mondo di Ethernet TCP/IP a quello dei dispositivi Profibus dislocati sul campo. In questo caso il 'ponte' tra i due mondi è rappresentato dal software che provvede a traslare in una lingua franca le informazioni provenienti dai dispositivi compatibili con il sistema. La descrizione dei dispositivi viene effettuata in XML e risulta indipendente dal particolare produttore o sistema operativo utilizzato. Ovviamente tutti i dispositivi della rete che si affacciano sul campo devono essere compatibili con la modellazione DCOM. Come per altri standard precedentemente illustrati, anche Profinet permette di utilizzare i protocolli di tipo più consono alle informazioni da trasferire: bus di campo per gli I/O in tempo reale deterministiche, UDP/IP per i sistemi di controllo e supervisione senza pretese di determinismo e il classico connubio TCP/IP per le informazioni non critiche.

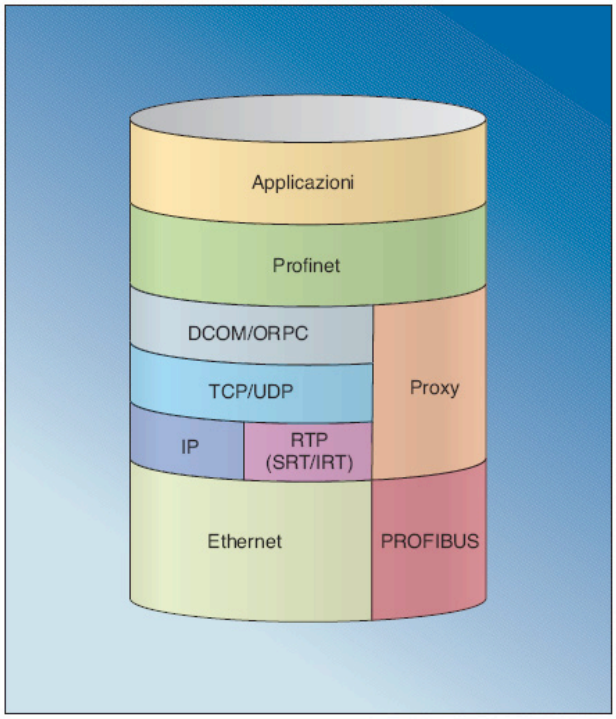


Figura 5 - Schema dell'architettura Profinet

1.3.3 RTPS (Real-Time Publish Subscribe) TECHNIC

A differenza della precedente implementazione, IDA (Interface for Distributed Automation) non si appoggia ad alcuna soluzione fieldbus preesistente. Per implementare le comunicazioni in tempo reale viene impiegato un protocollo di tipo editore-abbonato, RTPS (Real-Time Publish Subscribe) che si appoggia a sua volta alla coppia UDP/IP (figura 7). IDA permette di realizzare sistemi di automazione distribuita su un sistema di comunicazione orientato agli oggetti. I metodi associati a questi oggetti permettono il trasferimento di dati in tempo reale o di informazioni non critiche.
La gestione dei dispositivi tramite Web avviene tramite il tradizionale protocollo Http e la descrizione XML dei profili di periferica. Il middleware provvede a verificare l'ingresso o la terminazione di applicazioni consentendo il passaggio dei messaggi ai dispositivi secondari quando quelli primari vengono a mancare; in breve, consente la sostituzione a caldo (hot-swap) dei dispositivi. EtherCAT (Ethernet for Control Automation Technology) è una soluzione proprietaria basata su Ethernet le cui caratteristiche di determinismo si riassumono nei 30 microsecondi sufficienti, secondo il produttore, a elaborare 1.000 punti di I/O.

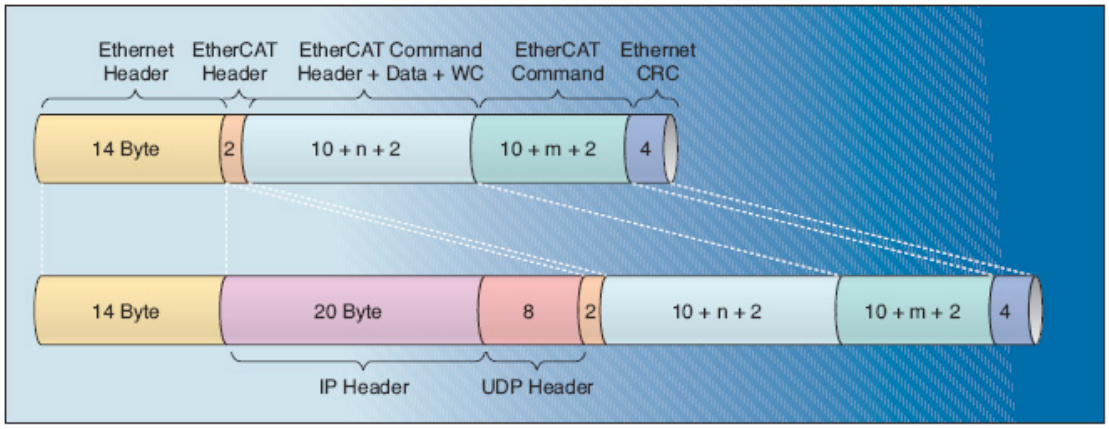


Figura 6 - EtherCAT è una soluzione proprietaria altamente scalabile

Il segreto di queste prestazioni risiede nella realizzazione di una sottorete dedicata che provvede a raccogliere i dati da tutti i dispositivi sul campo e a creare un unico messaggio con le informazioni collettive. Gli I/O sono connessi in una configurazione ad anello aperto a una stazione host per mezzo di un bus proprietario (E-bus). Il pacchetto Ethernet viene convertito nel formato E-bus, viaggia nella sottorete, passa per tutti i dispositivi e ritorna, opportunamente aggiornato, all'host. Durante il passaggio da un I/O all'altro esso viene infatti letto dall'unità FMMU (Fieldbus Memory Management Unit) integrata su ciascun dispositivo e, se richiesto, viene anche modificato nel giro di una frazione di microsecondo. Il risultato è che i telegrammi subiscono un ritardo minimo e possono indirizzare migliaia di dispositivi in ciascuna sottorete. Il sistema risulta estremamente scalabile (migliaia di nodi per un'estensione di chilometri) e, visto che il contenuto di informazioni del pacchetto Ethernet non viene alterato, quest'ultimo può essere riconvertito nel momento in cui dovesse essere richiesta un'informazione critica.

1.4 APPROFONDIMENTO SULLE PRINCIPALI SOLUZIONI INDUSTRIAL ETHERNET

1.4.1 ETHERNET / IP

Ethernet/IP, conosciuto anche con l'acronimo di EIP, si sta evolvendo verso un livello applicativo standard grazie agli sforzi di Odva (Open DeviceNet Vendor Association), Ioana (The Industrial Open Ethernet Association), CI (Control Net International) e IEA (Industrial Ethernet Association). Lo scopo è diffondere EIP e renderlo a tutti gli effetti uno standard

certificato e adattabile al maggior numero possibile di dispositivi di automazione. Ethernet/IP, infatti, utilizza tutti i protocolli di trasporto e di controllo già presenti in Ethernet, inclusi il Transport Control Protocol (TCP), l'Internet Protocol (IP) e le tecnologie di cui sono dotate le schede di rete. Progettare basandosi su queste tecnologie standard significa quindi operare in modo trasparente rispetto a tutti i dispositivi Ethernet presenti oggi sul mercato. Inoltre, dal momento che EIP è fondato su una piattaforma con tecnologia standard, è assicurato l'allineamento di Ethernet/IP con l'evolversi di questa tecnologia.

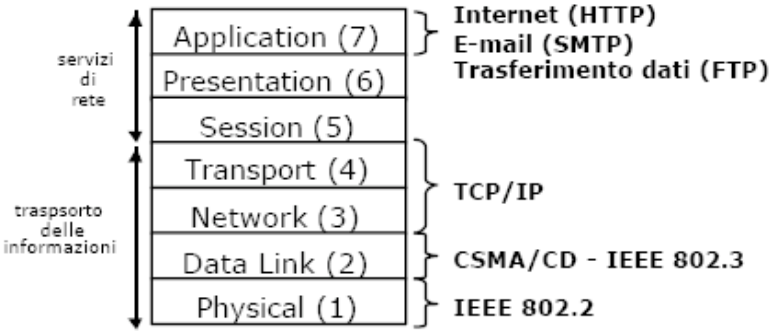


Figura 7 – Modello ISO-OSI

1.4.1.1 CIP (CONTROL AND INFORMATION PROTOCOL)

L'utilizzo del TCP/UDP/IP e le specifiche IEEE 802.2 e 802.3 non garantiscono che due nodi Ethernet possano comunicare fra loro; devono essere condivisi anche gli "Application Layer". La larghezza di banda permette a Ethernet di supportare differenti protocolli applicativi. In ambito "Office Automation" si sono imposti da tempo per Ethernet TCP/IP applicativi standard (p.e. FTP, SMTP, HTTP), viceversa, in ambito industriale, pur utilizzando Ethernet TCP/IP, molti dispositivi implementano di fatto applicativi proprietari.
Basato su Ethernet TCP/IP, EtherNet/IP utilizza un applicativo di fatto "Open" (CIP - Control and Information Protocol).

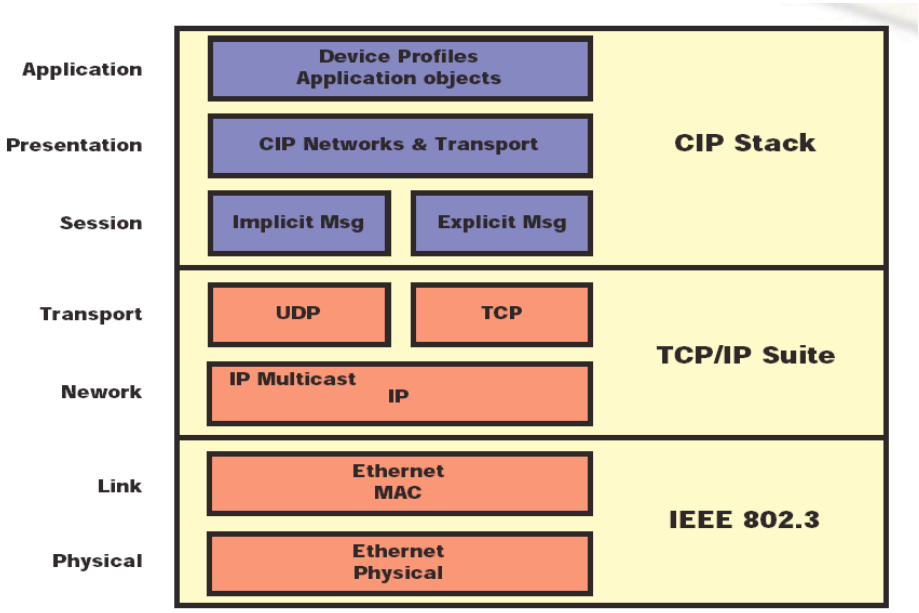


Figura 9 – Suite protocol

Il protocollo CIP (Common Industrial Protocol) gioca un ruolo fondamentale in Ethernet/IP: questo standard, infatti, organizza i dispositivi in rete come un insieme di oggetti definendone gli accessi, il comportamento e le estensioni in modo tale da avere un meccanismo comune di interfaccia con ogni dispositivo.

È promosso attivamente da ODVA e ControlNet International e le specifiche sono liberamente accessibili.

L'Application Layer di EtherNet/IP richiede che una "sessione di contatto" (Connessione) fra nodo trasmettitore e nodo ricevitore sia SEMPRE stabilita prima dell'invio del messaggio. Una Connessione(**Connection ID**) è una relazione logica fra un messaggio (**Message ID**) ed un indirizzo di nodo (**MAC ID**). Ogni nodo gestisce autonomamente l'associazione dei Message ID con il proprio MAC ID.

In un dispositivo "Client" (Sender) una Connessione "produce"una richiesta di dati, mentre, in un dispositivo "Server" (Target) una Connessione "produce" i dati richiesti dal dispositivo "Client"

Il protocollo CIP definisce due tipi di messaggi:

- **Explicit Message**
- **I/O (Implicit) Message**

I Messaggi di tipo **Explicit Message** utilizzano servizi di accesso ai singoli dispositivi di tipo: "Occasionali" (**UnConnected)**, "Ciclici" (**Connected).** Inoltre gli explicit message, sono messaggi autodescrittivi; in ognuno vengono definiti formato e tipo di dati, indirizzi degli attributi di destinazione, ecc …

Gli explicit message inoltre utilizzano una tecnica di indirizzamento **Point to Point** e comunicazioni di tipo **Peer to Peer.** Questo tipo di messaggi sono incapsulati nel Frame TCP/IP.

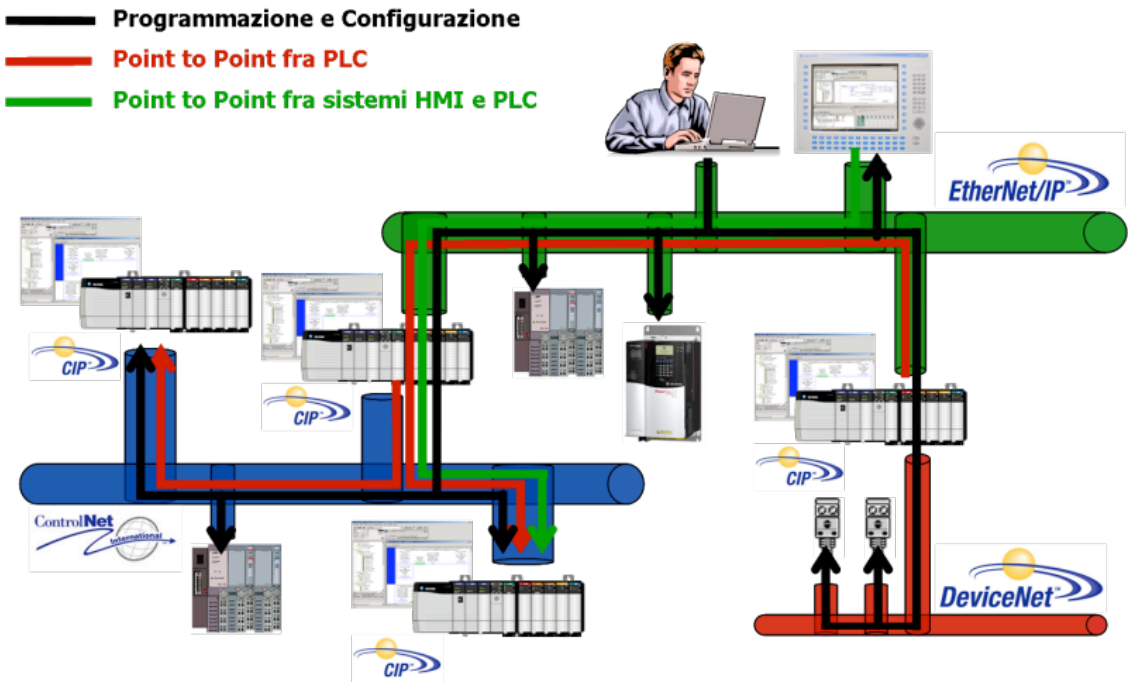


Figura 10 - CIP - Explicit Message

I messaggi di tipo **I/O (Implicit) Message** utilizzano SOLO servizi di tipo "Ciclici" (**Connected**) per applicazioni Time-Critical I/O (Change of State, Cyclic, Polling, ecc …). Il contenuto di questi messaggi (formato e tipo dei dati, attributi di destinazione e Comandi) sono stabiliti tramite il tool di configurazione (il Frame contiene solo i dati ed il Connection ID). La tecnica di indirizzamento utilizzata è di tipo **Point to Point, Multicast e Broadcast** ed le Comunicazioni sono di tipo **Peer to Peer e MultiMaster/Slave.**

Questo tipo di messaggi sono incapsulati nel Frame UDP/IP.

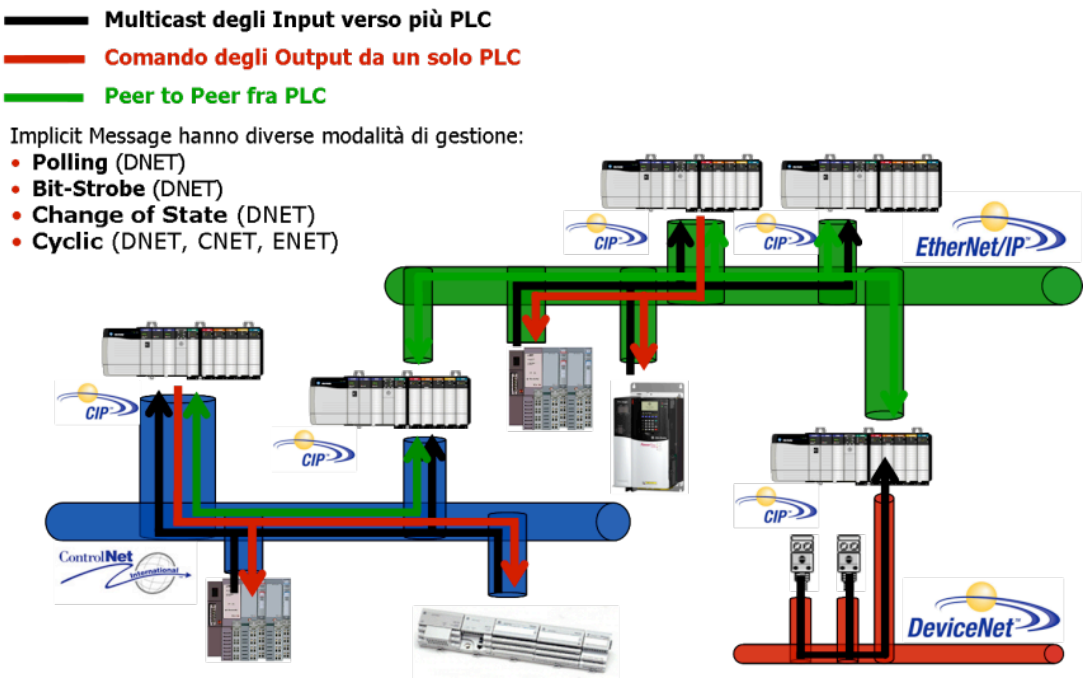


Figura 11 - CIP - Implicit Message

I Dati di **tipo Real Time I/O** sono generati con modalità differenti:

- **Poll Messaging**
  – Modalità Master/Slave
  – Inter Scan Delay (ISD)(Tempo minimo di attesa che consente a tutti i nodi Slave di rispondere all'interrogazione ciclica del Master. Il Master non inizierà un nuovo Ciclo di Scansione prima che questo tempo sia terminato
- **Cyclic Messaging**
  – Generazione delle informazioni su basi temporali predefinite
- **Change of State Messaging**
  – Un'informazione viene generata solo quando il suo contenuto è variato (cambio di stato)
- Sono permessi sistemi ibridi (CoS, Cyclic & Polling).

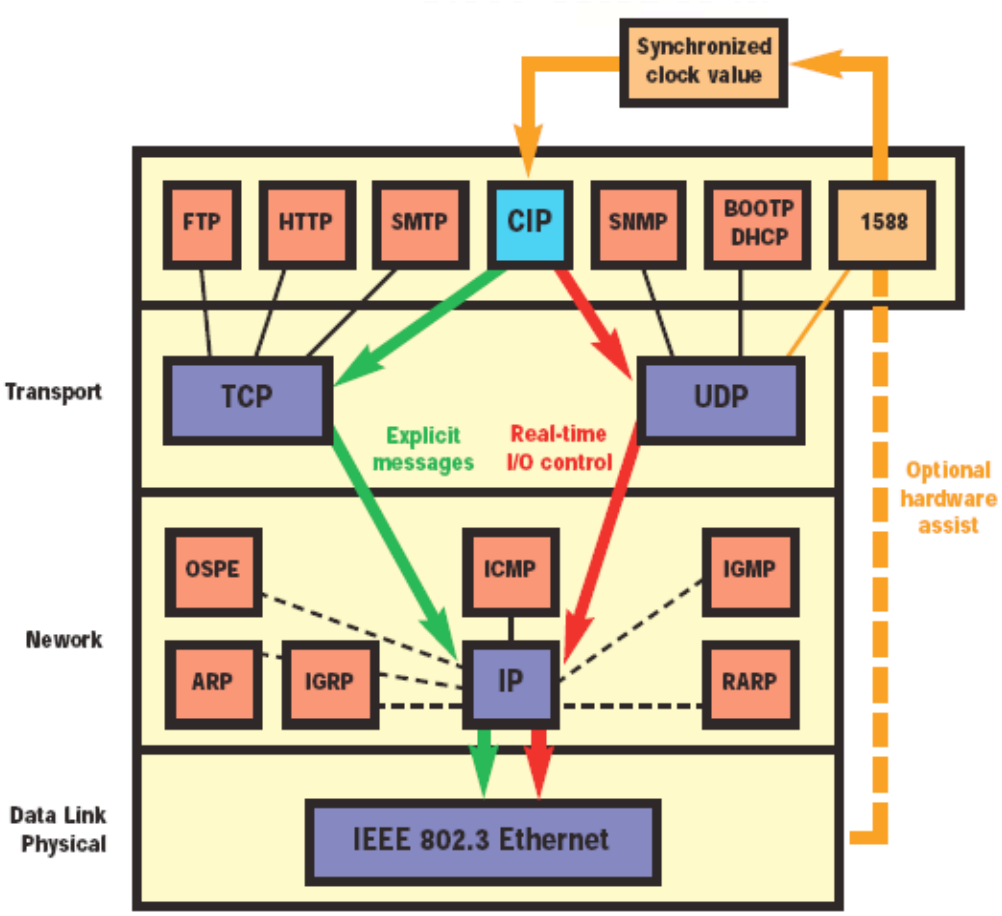
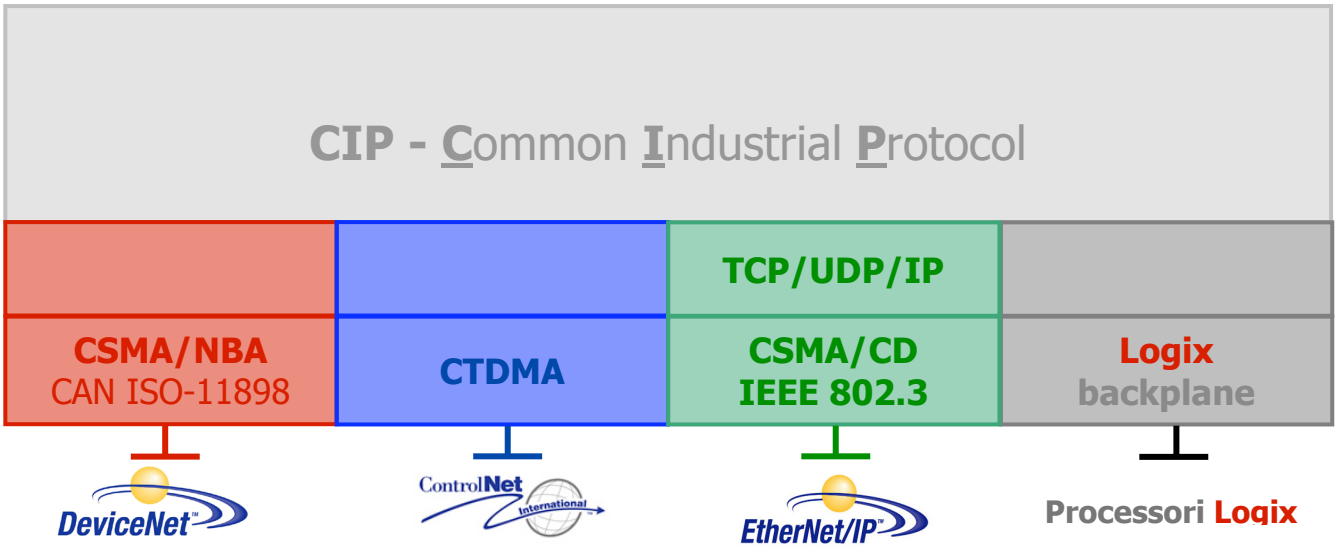


Figura 12 - CIP nel modello ISO/OSI

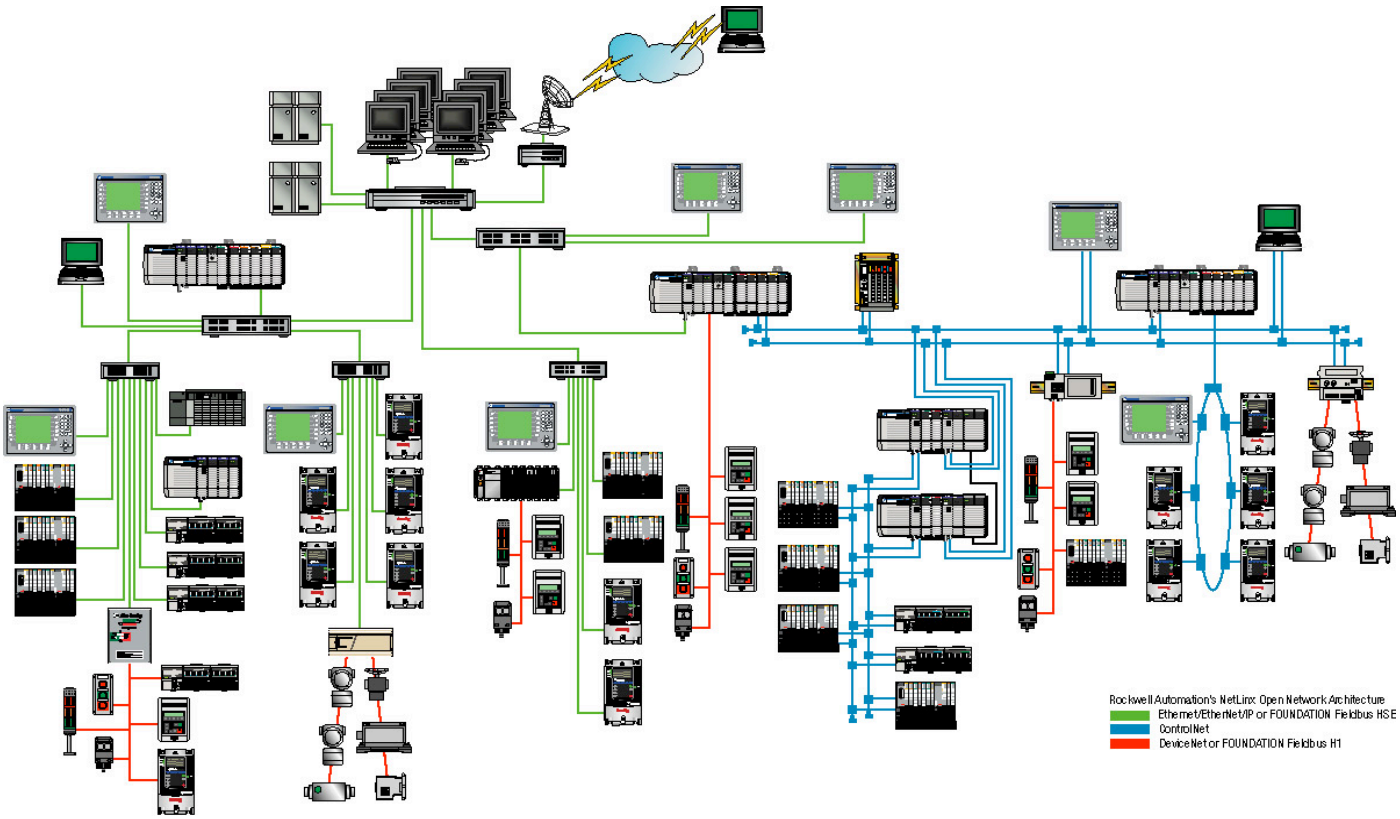
NetLink è un'architettura di comunicazione integrata per configurare, programmare, controllare e visualizzare informazioni e dati in modo efficiente e trasparente. NetLink si basa su tecnologie standard e su un solo applicativo.



CSMA/NBA Carrier Sense Multiple Access/Non-Destructive Bitwise Arbitration
CTDMA Concurrent Time Domain Multiple Access
CSMA/CD Carrier Sense Multiple Access with Collision Detection

Le specifiche delle tre reti sono gestite da due consorzi indipendenti:

- **ODVA** - Open DeviceNet Vendor Association
- **ControlNet International**



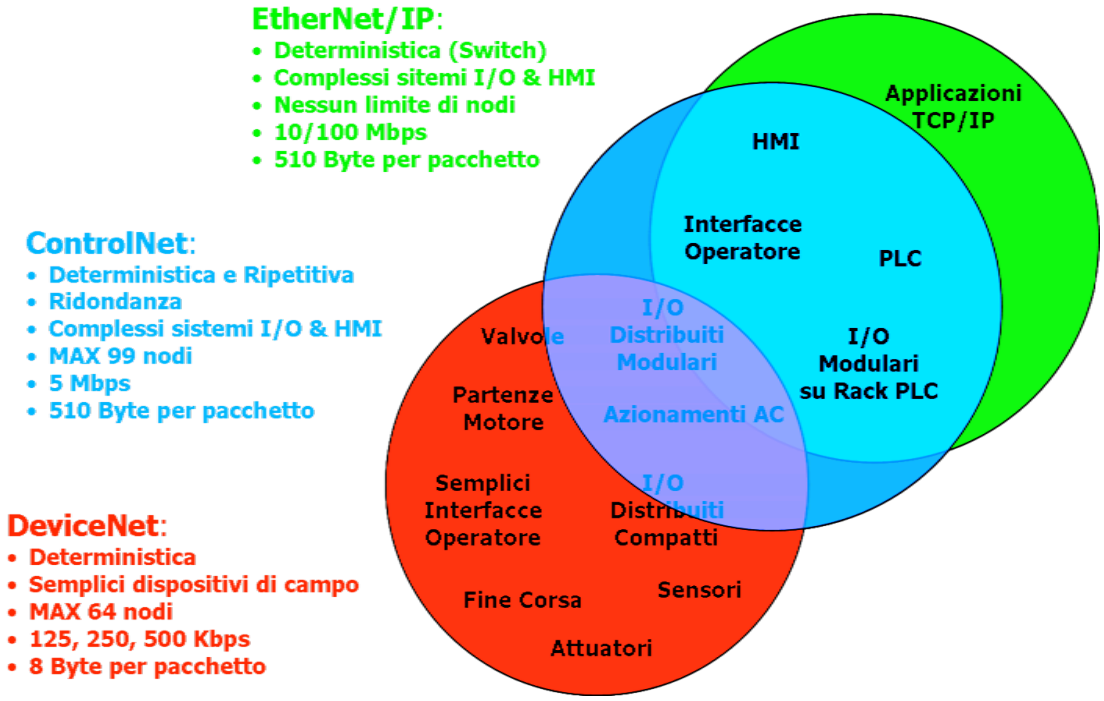


Figura 13 - Differenze applicative DeviceNet, ControlNet, EtherNet/IP

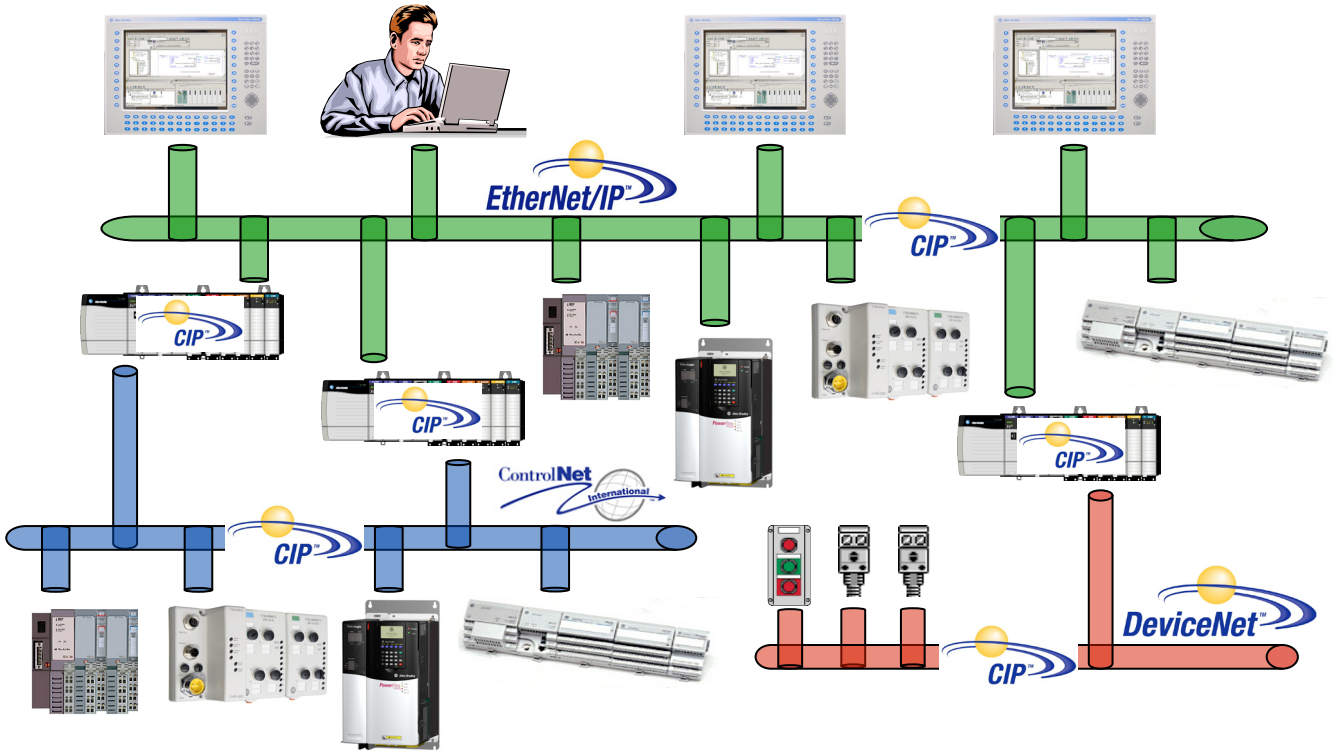


Figura 14 - CIP: UN SOLO protocollo per TRE reti

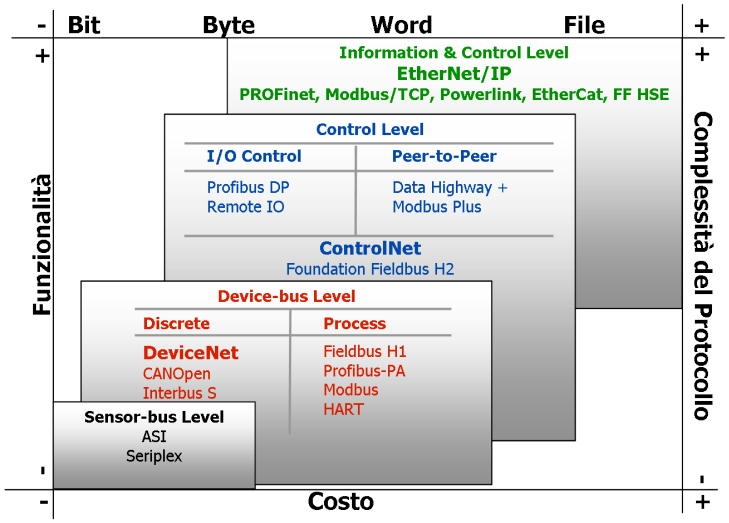


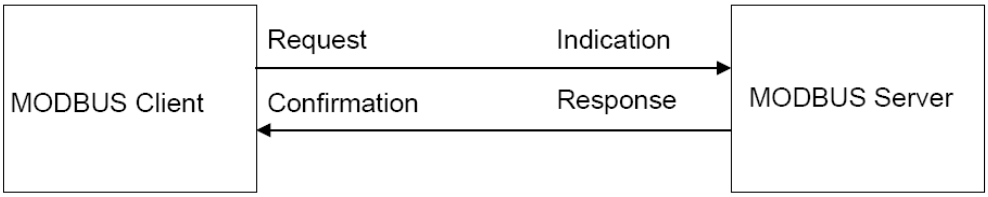
Figura 15 - Come si posizionano DeviceNet, ControlNet, EtherNet/IP

1.4.2 MODBUS TCP

1.4.2.1 GENERAL COMMUNICATION ARCHITECTURE

Il MODBUS messaging service fornisce una comunicazione client/server tra device connessi su rete Ethernet TCP/IP. Il modello client/server è basato su quattro tipi di messaggi

- **MODBUS Request**
- **MODBUS Confirmation**
- **MODBUS Indication**
- **MODBUS Response**



- Un **MODBUS Request** è il messaggio inviato sulla rete attraverso il Client per inizializzare una transazione
- Un **MODBUS Indication** è il Request message ricevuto su lato Server

- Un **MODBUS Response** è il Response message inviato dal Server
- Un **MODBUS Confirmation** è il Response Message ricevuto su lato Client

I MODBUS messaging services (Client / Server Model) sono usati per lo scambio di informazioni real time:

- tra due device applications
- tra device application e altri device
- tra HMI/SCADA applications e devices
- tra un PC e un device program provvedendo su servizi di linea

Un sistema di comunicazione su MODBUS TCP/IP può includere differenti tipi di device:

- Un MODBUS TCP/IP Client e Server devices connessi alla rete TCP/IP
- L'interconnessione tra device come bridge, router or gateway per collegamenti tra la rete TCP/IP e una linea di sottoreti seriali, la quale permette connessioni tra MODBUS Serial line Client e Server e devices.

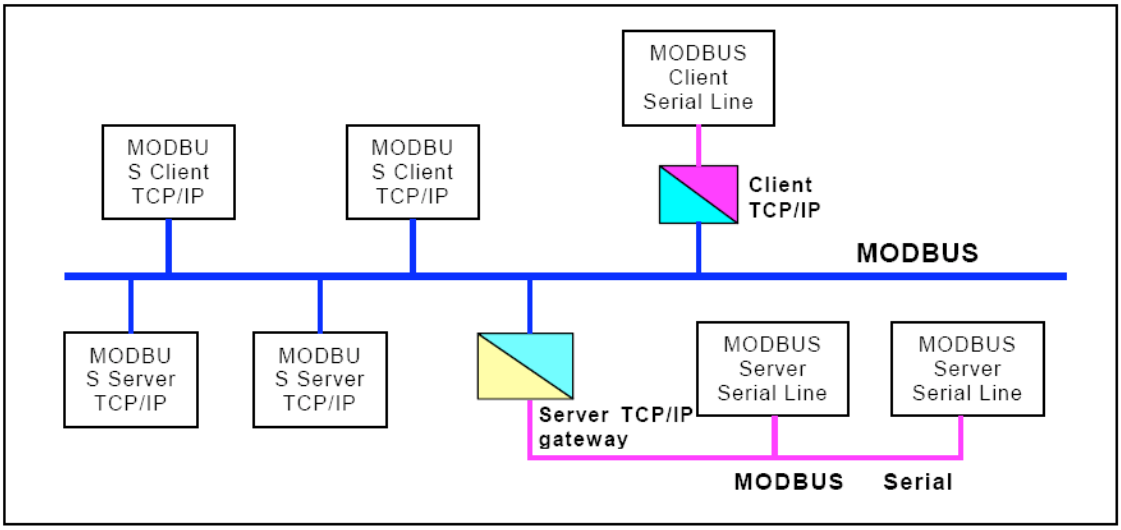


Figura 16 - MODBUS TCP/IP communication architecture

Il MODBUS protocol definisce un semplice Protocol Data Unit (PDU) indipendentemente dal fondamentale layer di comunicazione. Il mapping tra il MODBUS protocol su specifici bus o reti può introdurre qualche campo aggiuntivo su l'Application Data Unit (ADU).

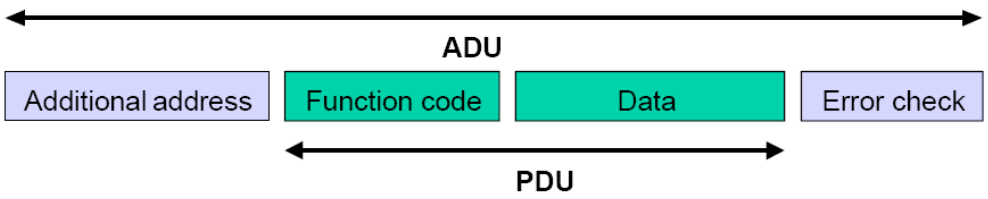


Figure 17 - General MODBUS frame

Il client che inizializza una transazione MODBUS costruisce la MODBUS Application Data Unit. La function code indica al server quale tipo di azione deve essere compiuta.

1.4.2.2 MODBUS COMPONENT ARCHITECTURE MODEL

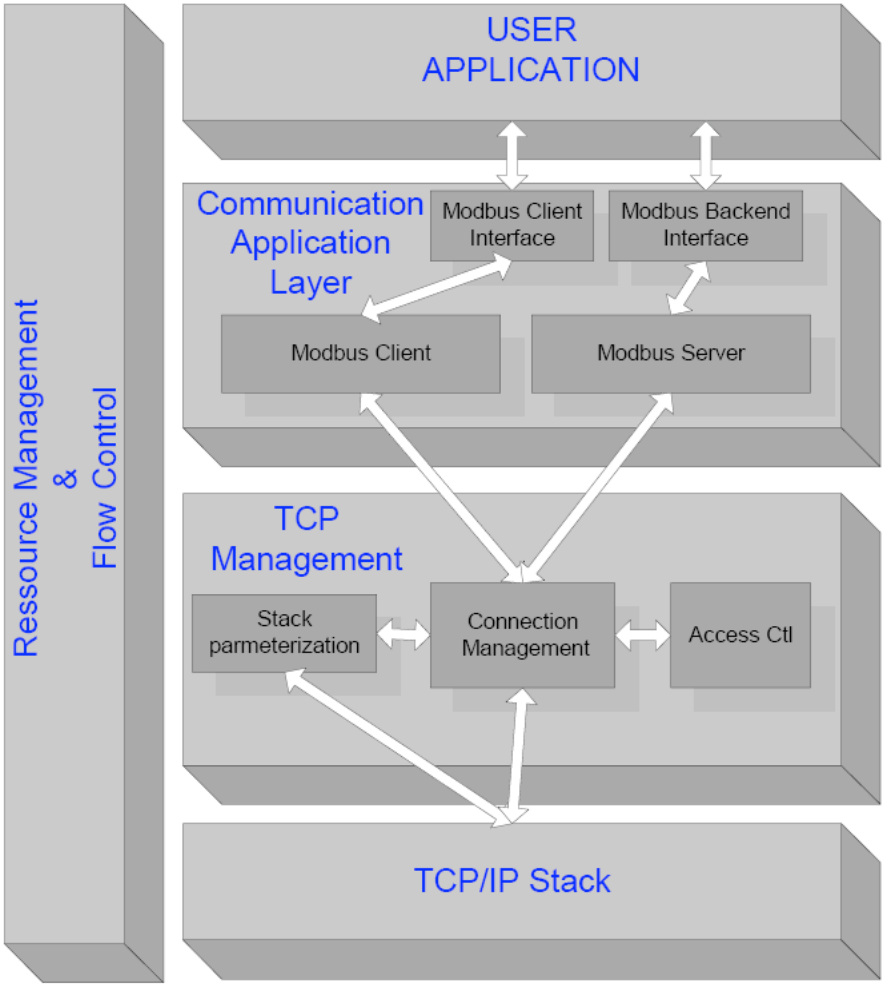


Figure 18 - MODBUS Messaging Service Conceptual Architecture

1.4.2.2.1 COMMUNICATION APPLICATION LAYER

Un MODBUS device può fornire un client and/or un server MODBUS interface.

MODBUS Client:

- Il MODBUS Client permette alle applicazioni utente di scambiare informazioni di controllo con un remote device. Il MODBUS Client costruisce un MODBUS request da I parametric contenuti in una richiesta trasmessa attraverso l'applicazione utente al MODBUS Client Interface.

MODBUS Client Interface:

- The MODBUS Client Interface fornisce una interfaccia per autorizzare il user application a costruire le richieste per vari MODBUS services, includendo l'accesso al MODBUS application objects

MODBUS Server:

- Sulla ricezione di un MODBUS request questo modulo attiva una azione locale a leggere, a scrivere o ad ottenere altre azioni.

MODBUS Backend Interface:

- Il MODBUS Backend Interface è una interfaccia del MODBUS Server per le user application, nella quale le applicazioni sono definite.

1.4.2.2.2 TCP MAGEMENT LAYER

Una delle principali funzioni del messaging service è gestire le comunicazioni stabilite e quelle terminate ed a gestire il data flow su connessioni TCP .
Connection Management

- Una comunicazione tra un client e un server MODBUS Module richiede l'uso di un modulo di gestione della connessione TCP. Questo è necessario per gestire globalmente i messaggi delle connessioni TCP.

Access Control Module

- In certi contesti critici, l'accessibilità a dati interni di devices deve essere negata per alcuni host. Quindi una modalità di sicurezza deve essere implementata se richiesta.

1.4.2.2.3 TCP/IP STACK LAYER

Il TCP/IP stack può essere parametrizzato per adattare il data flow control, la gestione dell'indirizzo e la gestione della connessione per differenti specifiche di restrizione. In genere il BSD socket interface è utilizzato per gestire le connessioni TCP.

1.4.3 PROFINET

PROFINET è uno standard innovativo e aperto sviluppato da PROFIBUS International per l'automazione industriale basato su Industrial Ethernet. Diventato standard internazionale con la normativa IEC 61158, supporta attraverso la comunicazione Ethernet l'integrazione di dispositivi di campo per automazione e applicazioni critiche dal punto di vista delle temporizzazioni.

PROFINET è composto da due differenti protocolli: un protocollo **PROFINET CBA** (descritto in appendice C) poco adatto al tempo reale ma basato su standard di accesso molto diffusi quali RPC/DCOM/OPC, e un protocollo pensato per il campo e il tempo reale **PROFINET IO**.

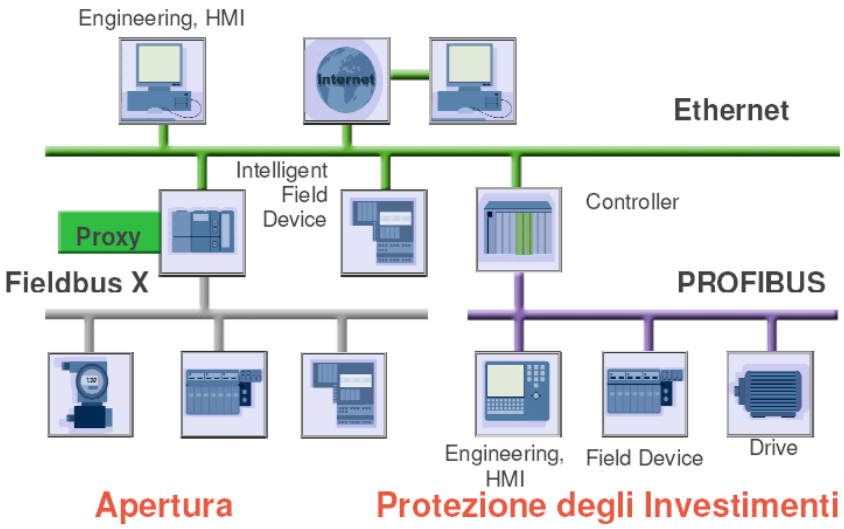


Figura 19 - PROFINET offre apertura e protezione degli investimenti

1.4.3.1 COMUNICAZIONE IN PROFINET

La comunicazione in PROFINET presenta tre livelli di prestazioni:

1. TCP, UDP e IP per dati non critici rispetto al tempo, come assegnamento di parametri e configurazione
2. Soft Real Time (SRT) per dati di processo critici rispetto al tempo; utilizzata nel campo dell'automazione aziendale
3. Isochronous Real Time (IRT) per particolari applicazioni, come per applicazioni di Motion Control.

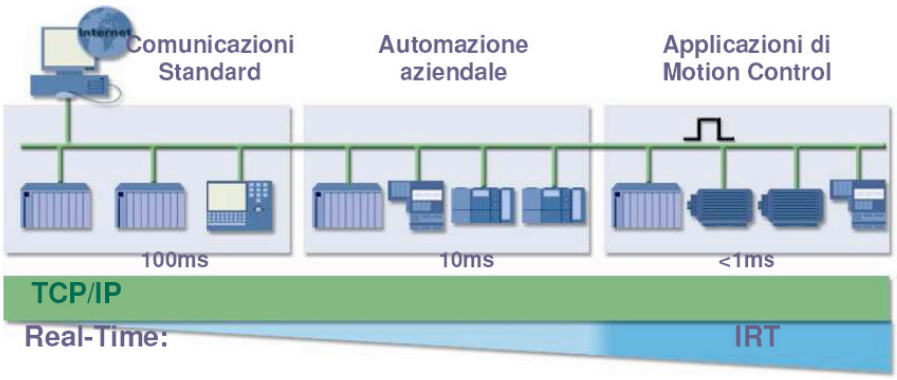


Figura 20 – I tre livelli della comunicazione PROFINET

Il grafico sottostante (fig. 30) evidenzia la distribuzione dei tempi di risposta dei tre diversi approcci PROFINET alla comunicazione.

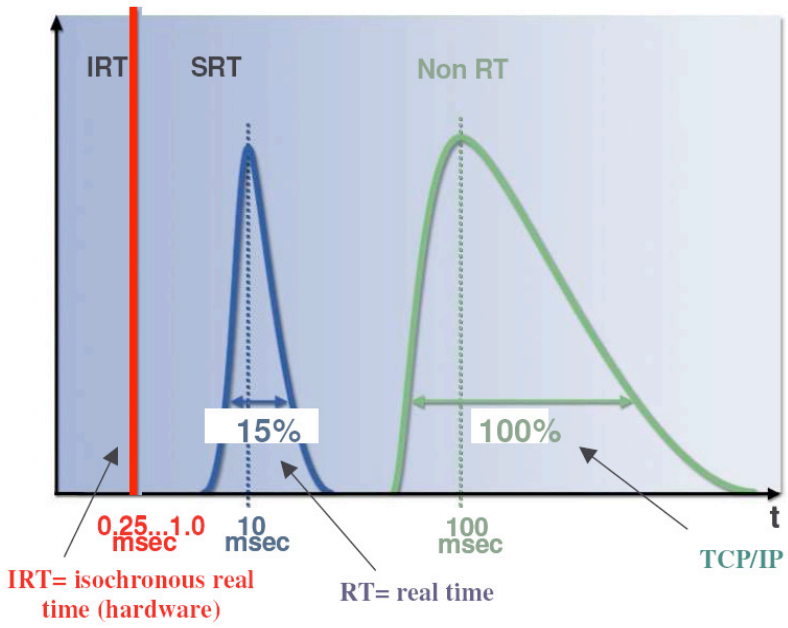


Figura 21 - Distribuzione dei tempi di risposta dei tre approcci PROFINET alla comunicazione

La comunicazione standard attraverso il protocollo TCP/IP impiega tempi di risposta medi attorno ai 100 ms. La comunicazione tramite SRT Chanel evidenzia un miglioramento dei tempi di trasmissione di un fattore 10, i tempi di risposta si attestano infatti attorno ai 10 ms. Anche la varianza subisce una riduzione che si attesta attorno ad un fattore che oscilla tra le 5 e le 8 volte quello della comunicazione standard. Pertanto i tre livelli di prestazioni di PROFINET coprono l'intero campo delle applicazioni per l'automazione e di conseguenza le caratteristiche fondamentali dello standard PROFINET sono le seguenti:

- Uso in contemporanea di comunicazioni basate su TCP e comunicazioni real Time
- Protocollo di comunicazione real time standardizzato per tutte le applicazioni, sia per comunicazioni tra componenti in sistemi distribuiti, sia per comunicazioni tra i controllori e periferiche decentrate
- Comunicazione real time scalabile

1.4.3.1.1 LA COMUNICAZIONE IN TEMPO REALE

PROFINET usa Ethernet e TCP/IP come base per la comunicazione.
Con Ethernet, non è possibile definire un tempo all'interno del quale i dati devono essere trasmessi attendibilmente.
L'utilizzo del protocollo TCP/IP ha rivelato che sono necessari tempi considerevoli utilizzando questo stack di comunicazione, oltre a questo l'elaborazione dello stack TCP/IP produce un ritardo non costante.
L'esperienza indica inoltre che la velocità della trasmissione seguendo la linea in Ethernet di 100 Mbit è trascurabile rispetto all'elaborazione nei dispositivi. Ciò significa che tutti i miglioramenti nel tasso d'aggiornamento e quindi nella risposta in tempo reale devono essere realizzati soprattutto attraverso ottimizzazioni dello stack di comunicazione nel Provider e nel Consumer. Si definisce **tempo di aggiornamento** il tempo che passa da quando una variabile è generata in un'applicazione del dispositivo a quando è trasmessa ad un altro dispositivo attraverso i sistemi di comunicazione e successivamente è messa a disposizione dell'applicazione.

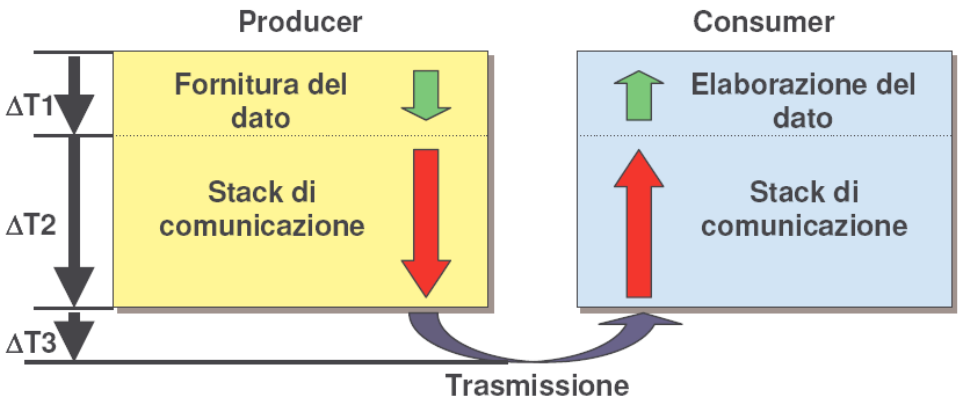


Figura 22 – Tempo di aggiornamento

Il tempo ΔT1 è determinato dall'architettura hardware del dispositivo e difficilmente dipende dal protocollo. Il tempo ΔT3 dipende dal sistema di trasmissione. Il tempo ΔT2 è dovuto allo stack di comunicazione.
In PROFINET i dispositivi con funzionalità altamente tempo-critiche possono, quando stabiliscono il collegamento, negoziare protocolli di comunicazione con capacità real-time che riducono il tempo ΔT2.

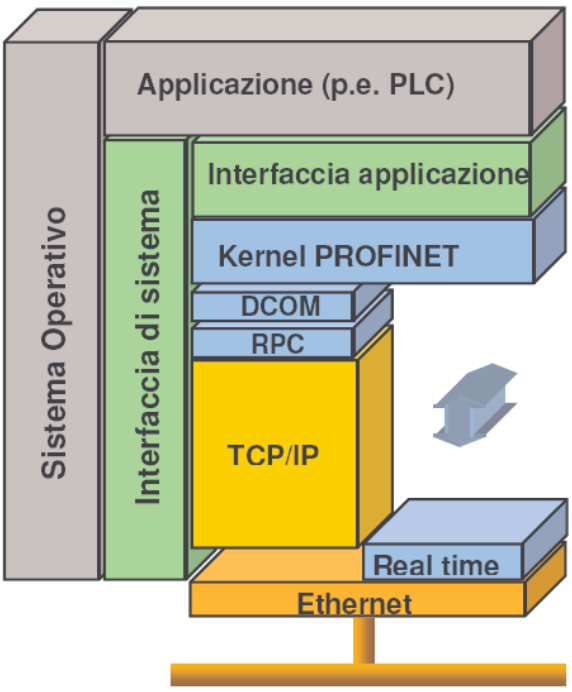


Figura 23 - stack di comunicazione PROFINET

In questo modo, PROFINET soddisfa le elevate richieste real-time disposte sul sistema di comunicazione. La soluzione proposta minimizza notevolmente i tempi dello stack di comunicazione e i risultati nelle prestazioni aumentano in termini di tasso d'aggiornamento dei dati di automazione. L'eliminazione di parecchi livelli di protocollo riduce la lunghezza di messaggio e meno tempo è richiesto prima che i dati da trasmettere siano pronti per la trasmissione e l'applicazione sia pronta per procedere. Un'ulteriore beneficio si ha considerando che la potenza del processore necessario nel dispositivo per la comunicazione è notevolmente ridotto. PROFINET distingue diverse classi realtime che si differenziano in funzione delle performance richieste: *RT (chiamato anche SRT) e IRT*. Viene utilizzata anche la seguente terminologia: *Real-time locale* per la comunicazione RT e *Real-time sincronizzato* per la comunicazione IRT.

1.4.3.2 PROFINET IO

Con PROFINET IO, l'integrazione di dispositivi di campo decentralizzati è implementata direttamente su Ethernet. Per questo scopo, la metodologia di accesso Master-Slave di PROFIBUS DP è stata convertita al modello provider-consumer. PROFINET prevede tre tipi di dispositivi:

- **IO-Controller:** dispositivo controllore sul quale gira il programma di automazione
- **IO-Device:** dispositivo di bus di campo remoto, che viene assegnato a un IOController
- **IO-Supervisor:** dispositivo/PC di programmazione con funzioni di configurazione e di diagnostica

Dal punto di vista della comunicazione, tutti i dispositivi su Ethernet sono trattati allo stesso modo. Tuttavia, durante il processo di configurazione i vari dispositivi sono assegnati ad un controllore centralizzato (IO-Controller). Per la configurazione viene utilizzata la stessa interfaccia di PROFIBUS. Durante il funzionamento, i dispositivi periferici (IO-Device) trasferiscono le informazioni di input al controller; il controller elabora le informazioni e trasferisce l'output ai dispositivi periferici. Le varie informazioni possono essere trasferite tra gli IO-Controller e gli IO-Device attraverso i seguenti canali:

- **Dati ciclici di IO**. Questi dati sono trasferiti sul canale real time
- **Allarmi.** Sono trasferiti sul canale real time
- **Parametrizzazione, configurazione, lettura delle informazioni diagnostiche.** Questi dati sono trasferiti attraverso canali standard sulla basedi UDP/IP

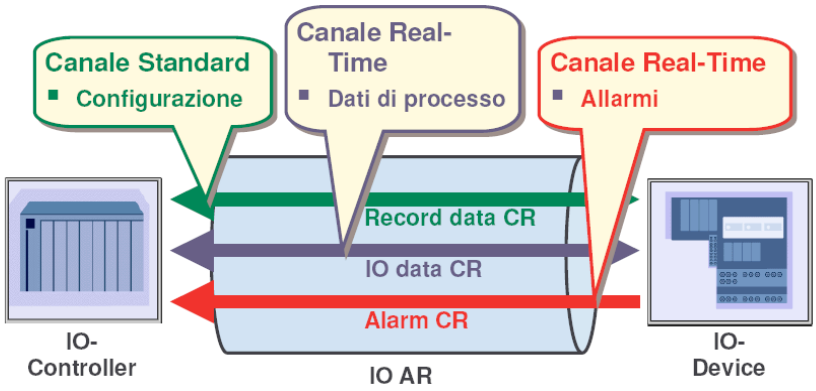


Figura 24 – I canali di comunicazione

Alla partenza, vengono stabilite le istanze di relazione (IO-AR) tra gli IO-Controller e gli IO-Device attraverso un canale UDP/IP. L'istanza di relazione IO-AR contiene diverse relazioni di comunicazione (CR) attraverso le quali sono trasferite la configurazione, i dati di processo e gli allarmi. Il dispositivo IO-Controller trasferisce i dati di parametrizzazione e di configurazione del dispositivo IO-Device assegnato sulla "Record data CR". La trasmissione ciclica dei dati di ingresso e di uscita è implementata sulla "IO CR" . Gli eventi aciclici sono trasmessi sulla "Alarm CR" al IO-Controller. In PROFINET esistono diversi tipi di allarme: unplug, plug in, diagnostici, di stato e allarmi di aggiornamento, inoltre sono comunque possibili allarmi specifici inseriti dal produttore del dispositivo. E' possibile assegnare una priorità alta o bassa agli allarmi.

2 WIRELESS TECHNOLOGY IN INDUSTRIAL NETWORK

2.1 INTRODUZIONE

Con il successo delle tecnologie wireless nell'elettronica di consumo, le tecnologie wireless standard sono state previste per la distribuzione anche negli ambienti industriali. Le applicazioni industriali che coinvolgono sotto sistemi mobili, o il solo desiderio di risparmiare il cablaggio, rendono le tecnologie wireless un'attrazione. Nonostante tutto, tali applicazioni spesso hanno richieste urgenti di attendibilità e sul tempo. In ambienti wired (cablati), il tempo e l'attendibilità sono ben serviti dai sistemi fieldbus (che sono una tecnologia matura progettata per facilitare la comunicazione tra i controllori digitali e i sensori e gli attuatori che si interfacciano con il processo fisico). Quando sono inclusi links wireless, le richieste di tempo e attendibilità sono significativamente più difficili da incontrare, a causa delle proprietà avverse dei canali radio.

In questo capitolo, discutiamo, quindi, alcuni problemi chiave che emergono nei sistemi di comunicazione industriali wireless: 1) problemi fondamentali, come raggiungere la trasmissione tempestivamente ed in modo affidabile, nonostante errori di canale; 2) l'utilizzo di tecnologie wireless esistenti per questo campo specifico di applicazioni; 3) la creazione di sistemi ibridi nei quali le stazioni wireless siano incluse nei sistemi wired esistenti.

La vera convenienza dell'essere in grado di connettere apparecchi senza l'uso del cablato, ha portato al successo, senza precedenti, di tecnologie wireless nell'industria di beni di consumo. In base a tale successo, le applicazioni che usano tali tecnologie stanno iniziando ad apparire anche in vari altri ambiti. Nell'ambiente industriale o commerciale, ad esempio, i benefici dell'utilizzo delle tecnologie wireless sono molteplici. Prima di tutto, il costo ed il tempo necessari per l'istallazione e la manutenzione dei cavi, normalmente richiesti in tale ambito, possono essere sostanzialmente ridotti, quindi rendendo più facili l'installazione dell'impianto e la riconfigurazione. Ciò è molto importante negli ambienti HARSH, dove esistono parti chimiche, vibrazioni o parti mobili che possono, potenzialmente, danneggiare qualsiasi tipo di cavo. In termini di flessibilità di installazione, i sistemi stazionari possono essere associati, in modo wireless, a qualsiasi sotto sistema mobile, o robot mobile, che può esistere per raggiungere una connettività che, altrimenti, sarebbe impossibile. Inoltre, il compito dell'accesso temporaneo di qualsiasi macchinario nell'istallazione, a scopo diagnostico o di programmazione, può essere enormemente semplificato mediante l'uso di queste tecnologie wireless.

Essendosi semplificato l'accesso al macchinario, vi sono molte applicazioni industriali che possono beneficiare dall'uso delle tecnologie wireless. La localizzazione e il monitoraggio di parti non finite, la coordinazione di veicoli di trasporto autonomi e robot mobili, così come le applicazioni che coinvolgono il controllo distribuito, sono tutte aree nelle quali le tecnologie wireless possono essere usate, in ambito industriale.

Molte di tali applicazioni industriali sono servite da sistemi fieldbus come PROFIBUS, CAN ecc.. , che sono wired. I sistemi fieldbus sono stati progettati, specificatamente, per svolgere compiti antonomi, o di controllo che fanno affidamento sull'interconnessione di controllori digitali con altri controllori digitali, così come sensori e/o attuatori. Lo scopo primario di tali sistemi è di fornire servizi di comunicazione in tempo reale, che risultino sia prevedibili, sia affidabili, cioè, che diano garanzie sull'eventuale consegna di packets e sul tempo di consegna. Alcune caratteristiche importanti del traffico fieldbus sono: 1) la presenza del traffico ciclico (cioè ricorrente), o anche del traffico periodico (jitter limitato tra packets successivi richiesti), soggetto a deadlines; 2)la presenza di importanti packets aciclici come gli allarmi, che hanno bisogno di essere trasmessi in modo affidabile con latenze delimitate; 3) la maggior parte dei packets è breve, dell'ordine di pochi byte.

L'architettura del protocollo, della maggior parte dei sistemi fieldbus, copre solo il layer fisico, il layer del link dei dati che include il sub layer di controllo di accesso medio (MAC) ed il layer dell'applicazione del modello di riferimento OSI.
I vantaggi della tecnologia wireless hanno portato ad un certo numero di soluzioni. Tali soluzioni vanno dalle reti, voice-oriented, cellulari a larga scala come UMTS, alle soluzioni data-oriented, come le LAN wireless (WLAN), le reti wireless personal area (WPAN) come le reti di sensori wireless. I sistemi WLAN, come la famiglia degli standard IEEE 802.11, sono progettati per fornire agli utilizzatori alta velocità di dati (decine di megabit al secondo) su aree di decine di centinaia di metri. I sistemi WPAN, come il Bluetooth (BT), e l'IEEE 802.15.4, sono stati progettati per connettere apparecchi in modo wireless, prendendo in considerazione il parametro relativo all'energia consumata. Essi supportano le velocità medie di dati nell'ordine di centinaia di kbit al secondo, fino a pochi megabit a secondo ed hanno aree dell'ordine di pochi metri. Molti distributori offrono attrezzature conformi a questi standard.
Utilizzare il wireless su applicazioni basate sul fieldbus comporterebbe la progettazione di sistemi aventi un esigente complessità strutturale. Poiché i canali wireless sono inclini a possibili errori di trasmissione, dovuti sia a interruzioni del canale (che avvengono quando la forza del segnale ricevuto cade sotto una soglia critica) e/o a interferenza, le richieste di affidabilità e di rispettare il real-time risultano maggiormente compromesse rispetto all'utilizzo di un canale wired. Questo è uno dei problemi chiave da risolvere nei sistemi fieldbus wireless, o in generale nell'uso di tecnologie wireless nelle applicazioni industriali.
Lo scopo del capitolo è di dare una visione generale sui problemi e sulle conclusioni che sorgono, quando si considera l'uso delle tecnologie wireless standardizzate, come IEEE 802.11, BT, o IEEE 802.15. in una rete industriale controllata in modo fieldbus.

2.2 PRINCIPALI PROBLEMI DI REAL-TIME E FIELDBUS COMMUNICATION

Dato che c'è un certo numero di sistemi fieldbus (wired) maturi e disponibili commercialmente, la questione è se vi sono maggiori difficoltà nell'uso di questi con il wireless. Alcuni esempi discussi in questa sezione mostrano che alcuni protocolli hanno difficoltà. Un problema, particolarmente importante, è l'errore di canale; gli errori di canale, ad esempio, possono far mancare al packet le loro deadlines. Di conseguenza, non interessano solo le ripercussioni degli errori, ma anche i meccanismi che permettono di trattare gli uni con gli altri. Verranno discussi alcuni di questi meccanismi, che sono stati proposti proprio per i sistemi fieldbus.

2.2.1 PROPRIETA' DEI WIRELESS CHANNELS E TRANSCEIVER

1. Path Loss:

La forza del segnale, di un segnale radio, diminuisce con la distanza tra un trasmettitore ed un ricevitore. Tale diminuzione è conosciuta come path-loss. La grandezza del path-loss dipende da diversi parametri, tra i quali la tecnologia dell'antenna, le frequenze usate e le condizioni ambientali presenti. Un'approssimazione molto usata è il modello a log-distance. In tale modello, la forza del segnale ricevuto $\mathbf{P_r}$ ad una distanza d si comporta come $\mathbf{P_r(d) \sim P_t \cdot (d_0/d)^{\gamma}}$ per distanze d maggiori di una distanza di riferimento $\mathbf{d_0}$ ed una radiated signal strenght $\mathbf{P_t}$. La

distanza di riferimento dipende dalla tecnologia dell'antenna. Il cosiddetto esponente di perdita di path γ assume, di solito, valori tra due (free-space path loss) e sei, in relazione all'ambiente. Negli ambienti industriali sono stati osservati esponenti di perdita di path tra due e tre, ma a volte capita anche che i valori siano più piccoli di due.

2. Half-Duplex Operation of Transceiver:

I transceivers wireless non sono capaci di trasmettere e ricevere simultaneamente sullo stesso canale. A causa di questo, la maggior parte dei transceivers wireless sono half-duplex. Essi inibiscono le operazioni di trasmissione e ricezione simultanee. Il primo svantaggio di tale approccio è la perdita di tempo sperimentata dalla distinta rotazione ricezione- trasmissione.

3. Physical Layer Overhead:

Per far acquisire, da un ricevitore, una sincronizzazione, la maggior parte dei sistemi wireless usa sequenze di istruzione *(training sequenze)* extra di simboli ben conosciuti. Quando vi è una sequenza di istruzione all'inizio di un packet, è detta preambolo *(preamble)*. Ad esempio, il layer fisico di IEEE 802.11 con sequenza diretta spread-spectrum (DSSS) richiede preamboli di lunghezza 128-μs, trasmessi con tutti i packet.

4. Channel Error:

Un trasmettitore wireless propaga waveforms in multiple direzioni spaziali allo stesso tempo. Tali waveforms possono essere soggette a riflessione, diffrazione o dispersione. Come risultato, multiple copie della stessa waveform possono raggiungere il ricevitore, dopo aver seguito diversi path, con diverse lunghezze relative e diversi tempi di viaggio (dispersione di tempo). Una misura comune per tale dispersione di tempo è *rms delay spread* (root mean square), o semplicemente diffusione del ritardo. La dispersione nel tempo ha due importanti conseguenze:

- con small-scale o multipath-fading, multiple copie possono interferire in modo costruttivo, o distruttivo sul ricevitore. Se una stazione (trasmettitore/ricevitore), o parti dell'ambiente hanno modo di muoversi, il segnale composito al ricevitore si alterna tra interferenze costruttive e distruttive, portando a, fluttuazioni veloci nella lunghezza del segnale ricevuto (variazione del tempo). Nel caso di interferenza distruttiva, il canale è spesso detto essere in deep fade (dissolvenza profonda) e molti errori avvengono durante la decodificazione dei simboli del canale. Quando la durata del deep fade abbraccia diversi simboli del canale consecutivi, gli errori di simbolo/bit inizieranno ad apparire in bursts.
- Interferenza intersimbolo (ISI): quando la dispersione di tempo è larga, può succedere che le waveforms, che appartengono a diversi simboli, si sovrappongono al ricevitore. Nel caso di tale ISI, è necessario un particolare sforzo per ricostruire il simbolo originale.

Vi sono altre distorsioni alle waveforms wireless, incluse l'interferenza co-canale e l'interferenza del canale adiacente da sistemi di comunicazione wireless co-localizzati, da rumore termico o fatto dall'uomo, così come i Doppler shifts (i cambiamenti). Negli ambienti industriali si può creare il rumore significativo, così come la distorsione dell'elettronica del transceiver, anche, tramite motori forti, da commutatori di frequenze statiche, da apparecchi elettrici di scarico ed altro.

Misurazioni di alcune caratteristiche chiave del canale wireless, negli ambienti industriali, hanno dimostrato che la diffusione di ritardo può raggiungere valori maggiori di 200 ns.

Tali fenomeni si tramutano in errori di bit e perdite di packet, con possibili ritardi se i packet hanno bisogno di essere ritrasmessi. Le perdite di packet avvengono quando, ad esempio, il ricevitore di un packet fallisce ad acquisire una sincronizzazione di carrier, o di bit, mentre gli errori di bit si riferiscono ad errori causati da bit capovolti (flipped), dopo che la sincronizzazione è già stata raggiunta con successo. Le caratteristiche dell'errore, dimostrate dal canale wireless, dipendono dall'ambiente di propagazione, dallo schema di modulazione scelto, dalla potenza di trasmissione, dalla frequenza in uso, così come da molti altri parametri.

La descrizione successiva ci dà un esempio di come può essere grave una tale situazione. Le misurazioni in un ambiente industriale, con un chipset conforme a IEEE 802.11b hanno mostrato che velocità di errore di bit di breve termine, nell'ordine di 10^{-4} ...10^{-2} possono essere raggiunte per una modulazione shift-keying [schema di modulazione digitale che trasmette i dati cambiando, o modulando la fase di un segnale di riferimento (the carrier wave)] a fase quaternaria 2-Mb/s (QPSK). Inoltre, vi sono periodi lunghi un minuto in cui sono state osservate velocità di perdita di path di almeno del 10% (e a volte fino all'80%). Errori di bit e perdite di packet, poi, sono bursty, cioè avvengono in cluster con periodi liberi da errore ("runs") tra i cluster. Naturalmente, tali risultati sono specifici per quel chipset e quell'ambiente, ma simili trend sono stati osservati anche in altri studi di misurazioni wireless.

2.2.2 PROBLEMI E CONSEGUENZE RELATIVE ALLE PROPRIETA' DEI WIRELESS CHANNELS

1. Problemi di consistenza:

quando un sistema usa il modello di comunicazione produttore-distributore-consumatore, come fanno alcuni protocolli fieldbus, la comunicazione è basata su trasmissioni di identificatori-dati in broadcast senza acknowledged. Quando il produttore riceve l'identificatore-dati ritrasmette in broadcast i relativi dati. Tutti i consumatori interessati a tali dati possono copiare il valore ricevuto nel buffer interno per le loro applicazioni. Per raggiungere la *coerenza spaziale* tra un insieme di consumatori k, è richiesto che ognuno di questi consumatori k riceva il valore dei dati. La coerenza spaziale è richiesta, ad esempio, quando un distinto k controlla il lavoro sullo stesso processo fisico. Non raggiungere la coerenza spaziale potrebbe portare a decisioni di controllo inconsistenti tra i controllori. Tale inconsistenza spaziale potrebbe avvenire, ad esempio, se i packet vengono persi.

Come esempio, presumiamo che il canale wireless è tale che per ogni coppia di trasmettitore-ricevitore un packet è corrotto con una certa probabilità p. Quando il produttore ha ricevuto l'identificatore e trasmette il valore dei dati, raggiungendo la coerenza spaziale, richiede che tutti i consumatori k ricevano il packet di dati, che avviene con probabilità $(1-p)^k$. Come esempio numerico: con $p = 0.2$, la coerenza spaziale tra $k = 4$ consumatori è raggiunta solo con ≈41% della probabilità.

Un altro requisito fondamentale è la *coerenza temporale relativa*. Consideriamo, ad esempio, un insieme di sensori k che campionano un processo fisico. Per raggiungere la coerenza temporale relativa, tutti i sensori devono campionare il processo nella stessa finestra di tempo pre-specificata.

2. Problemi per i Token-Passing Protocols:

Token passing è un metodo di accesso al canale in cui un segnale, detto token, viene passato tra i nodi i quali autorizzano il nodo a comunicare.

I sistemi fieldbus, come PROFIBUS, si affidano a token passing per far circolare il token al fine di iniziare le trasmissioni tra un numero di controllori (detti stazioni master nel PROFIBUS). Le stazioni master sono organizzate in un anello logico sulla sommità di un mezzo broadcast. È dimostrato che ripetute perdite di packet token sono un problema grave per la stabilità dell'anello logico (stabilità dell'anello). Quando fallisce una prova per passare il token da *x* a *y*, x deve passare immediatamente alla successiva prova. Nel caso di canali bursty, tuttavia, può anche avvenire che il canale tra *x* e *y* si trovi in deep fade e ci starà per diverso tempo. Tale deep fade potrebbe, potenzialmente, rendere tutte le successivi prove per passare il token inutili, facendo perdere *y* all'anello. Una stazione master *y* che è stata persa dall'anello, non deve trasmettere fino a che non venga re-inclusa, esplicitamente, da un'altra master. Tale re-inclusione può impegnare multiple circolazioni di token ed i packet, che arrivano alla stazione master *y* nel frattempo, incorreranno in ritardi corrispondenti. Tali problemi di ritardo sono molto meno frequenti quando sono considerati canali non bursty, che hanno la stessa velocità media di errore di packet. I protocolli token passing, quindi, servono da esempio, per il fatto che spesso è importante non solo la presenza di errori di bit, ma anche le caratteristiche (bursty contro non bursty) degli errori.

Un altro problema con i protocolli token passing riguarda l'ordinamento delle stazione lungo l'anello. Tale condizione essenziale non può essere sempre garantita, quando le stazioni sono mobili. I protocolli fieldbus, basati sul token passing, non sono attrezzati per trattare con la mobilità e devono essere aggiunti meccanismi appropriati.

3. Problemi per il Carrier-Sense Multiple Access (CSMA) protocols:

I sistemi fieldbus come CAN, usano i protocolli basati su CSMA dove sono possibili collisioni.

In generale, i protocolli basati su CSMA lavorano in un modo distribuito, dove una stazione A che vuole trasmettere, prima ha bisogno di rilevare il mezzo di trasmissione. Se il mezzo risulta libero, la stazione inizia a trasmettere. Le molte varianti di CSMA che esistono, differiscono in ciò che avviene quando si rileva il mezzo occupato. Nell'opzione scelta per fieldbus CAN, una stazione A che vuole trasmettere, aspetta la fine della trasmissione entrante ed inizia il proprio packet immediatamente dopo. Poiché un'altra stazione B potrebbe fare ugualmente, può avvenire una collisione. Il protocollo CAN (wired) è basato sul meccanismo deterministico di risolvere il contenzioso. Tale meccanismo è difficile da usare nel wireless. Si basa sull'abilità della stazione di trasmettere e ricevere simultaneamente sullo stesso canale, che è impossibile con transceivers wireless half-duplex. I ricevitori hanno bisogno di una forza minima, del segnale ricevuto, per decodificare, con successo, i packet, o determinare che un'altra stazione stia correntemente trasmettendo (carrier sensing). A causa di una perdita di path, il livello minimo del segnale richiesto può non essere raggiunto, una volta che la distanza tra il trasmettitore ed il ricevitore aumenta. Di conseguenza, le operazioni carrier-sensing possono fallire, dando vita ad un problema del "terminale nascosto", di cui soffrono tutti i protocolli basati su CSMA. Consideriamo tre stazioni, A, B e C, organizzate in modo che A e C non possono rilevare le trasmissioni l'una dell'altra, ma la stazione B può ricevere i segnali sia da A, sia da C. La stazione A trasmette un packet a B. La stazione C vuole fare lo stesso, esegue un rilevamento della portate e trova un canale inattivo, perché è fuori dall'area di A. Di conseguenza, la stazione C inizia a trasmettere ed i packet di A e di C collidono in B.

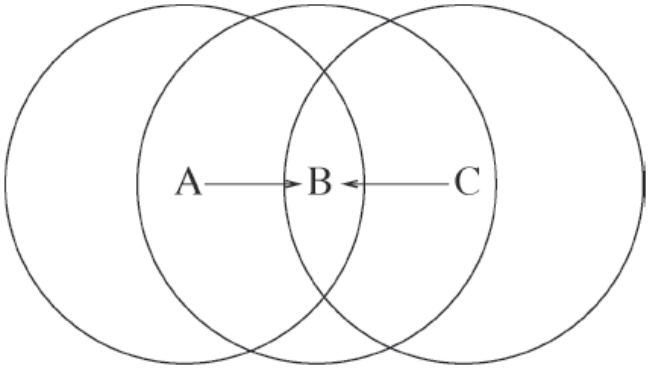


Figura 25 – scenario d'esempio di un problema terminale nascosto; i cerchi indicano l'area della trasmissione/rilevamento

Sono state suggerite diverse soluzioni, come il busy tone (tono di occupato), per risolvere il problema terminale nascosto. L'approccio più usato oggi, tuttavia, è l'handshake RTS/CTS adottato da IEEE 802.11 standard. In questo schema, la stazione A inizia il suo scambio di packet con B, usando un packet di controllo breve detto request-to-send (RTS). La stazione B risponde con un packet clear-to-send (CTS). Solo dopo la ricezione del RTS la stazione A continua con l'invio del packet di dati. Qualsiasi altra stazione che riceve un packet RTS o un CTS non destinato ad essa, deve rimanere ferma per il tempo indicato nei packet RTS/CTS, per evitare la distorsione di scambi di packet in corso.

Il problema con l'handshake RTS/CTS nel contesto di sistemi fieldbus è che la maggior parte di tutti i packet è molto piccola. La maggioranza di packet è dell'ordine di pochi byte e i packet stessi sono di poco maggiori dei packet RTS o CTS. Quindi, l'handshake RTS/CTS crea un overhead significativo. A volte può essere possibile evitare situazioni terminali nascoste (e handshake RTS/CTS) mediante una accurata riconsiderazione della disposizione delle stazioni. Un altro approccio è il non utilizzo di RTS/CTS e prendersi il rischio di avere situazioni terminali nascoste, mentre si riduce la probabilità tagliando il tempo necessario per trasmettere un packet, ma in tal modo ci vuole un aumento nella velocità dei bit. Tale approccio è attuabile in certe condizioni. Le applicazioni industriali spesso richiedono non solo moderate velocità di bit, nell'ordine di centinaia di kilobit al secondo, o pochi megabit al secondo (CAN ha 1 Mb/s come velocità massima).

2.2.3 TECNICHE DI RISOLUZIONE DEL CHANNEL ERROR

Anche quando i problemi, come quello dei terminali nascosti, non avvengono, o in qualche modo vengono elusi, i problemi creati dagli errori di canale rimangono. Molti meccanismi sono stati sviluppati, in passato, per fare trasmissioni di dati su canali wireless più robusti. Ciò dipende dal sistema fieldbus e dal modello di comunicazione al quale tali meccanismi sono applicabili.

I sistemi fieldbus, che lavorano in accordo con il modello produttore-distributore-consumatore, fanno uso esteso di broadcasting. Non vi sono ritrasmissioni e, in generale, il trasmettitore non ha modo di verificare che le deadlines si sono rispettate. Le tecniche nelle quali non vi è feedback dal ricevitore al trasmettitore, sono conosciute come tecniche open-loop. Un approccio utile è la codificazione dell'avanzamento della correzione di errore (FEC). Negli schemi FEC, il trasmettitore aggiunge bit doppi al packet, che permettono al ricevitore di correggere gli errori di bit, se non ve ne sono molti. La ratio dei bit dell'utilizzatore nei confronti del numero globale di bit, dopo la codifica (i bit dell'utilizzatore più i bit dell'overhead) è detta velocità del codice. Approssimativamente, minore è la velocità del codice, maggiore è l'overhead e migliore è la capacità di correzione dell'errore. Un esempio è fornito da BT.

Vi sono molte altre opzioni per aumentare la robustezza che non richiede feedback (meccanismi open-loop). Prendiamo un esempio: 1- usando schemi di modulazione multipath e resistenti alle interferenze, come la moltiplicazione della divisione di frequenza ortogonale (OFDM), o la modulazione spread-spectrum; 2- trasmettendo un packet non solo una volta, ma multiple volte; 3- ottimizzando la disposizione dell'unità e il numero di infrastrutture richieste.

Alcuni sistemi fieldbus, come PROFIBUS, usano ritrasmissioni e possono dare, ad un trasmettitore parte del controllo, per sapere se le deadlines si sono incontrate o no. I protocolli nei quali il trasmettitore riceve feedback dal ricevitore ed esegue ritrasmissioni, se necessarie, sono comunemente detti protocolli di richiesta ripetuta automaticamente (ARQ) . Poiché il ricevitore fornisce feedback, essi possono essere anche classificati come tecniche closed-loop. Le ritrasmissioni sono utili, quando richieste urgenti di affidabilità, che devono essere incontrate, non possono essere raggiunte solo tramite tecniche open-loop (esempio: importanti packet di allarme). Inoltre, in contrasto con la codifica FEC open-loop, i protocolli ARQ producono overhead solo quando è necessario combattere gli errori.. Il numero disponibile di ritrasmissioni, tuttavia, è naturalmente limitato dalle deadlines del packet. Tutto il tempo che il trasmettitore impiega per la ritrasmissione di un packet è sottratto dalle deadlines di altri packet che aspettano di essere trasmessi. Il problema nel progetto del protocollo è, quindi, trovare uno schema buono che migliori l'attendibilità della consegna in una data deadline.

Nella sezione seguente, discutiamo i meccanismi di protocollo open-loop e closed-loop selezionati. Tali meccanismi sono stati proposti nel contesto dei sistemi fieldbus wireless e nelle comunicazioni in tempo reale wireless.

1. **Utilizzo della diversità spaziale:**

   come è stato spiegato, a causa del fading multipath, la forza del segnale ricevuto, probabilmente, va a cambiare tra i ricevitori situati in diverse postazioni. Consideriamo due ricevitori, *r* e *s*, che sono alla stessa distanza da un trasmettitore. Se *r* e *s* sono relativamente vicino l'un l'altro, la probabilità che *r* e *s* sperimentino una deep fade allo stesso momento è più alta, se la loro distanza è maggiore della cosiddetta distanza di coerenza. Il funzionamento del canale è, quindi, spazio dipendente e la diversità spaziale può essere utilizzata in un certo numero di modi.

   La diversità di ricezione è una tecnica open-loop in cui il ricevitore è equipaggiato con antenne multiple. La distanza di tali antenne dovrebbe comprendere la distanza di coerenza anticipata presa in considerazione. Quando il segnale ricevuto da un'antenna è in deep fade, può succedere che il segnale è buono abbastanza per una ricezione propria in un'altra antenna, se la distanza di antenna è abbastanza grande. Il ricevitore è capace di commutare (switch) tra le antenne e può, ad esempio, scegliere a chi dare il segnale più forte.

   Negli schemi di diversità di trasmissione, il trasmettitore usa multiple antenne. Ci sono schemi di diversità di trasmissione che lavorano a livello di simboli di canale individuale. Quando devono essere usati adattatori di rete

wireless, disponibili in commercio, gli schemi di diversità di trasmissione, che lavorano a livello di interi packet, diventano più interessanti.

Nello schema closed-loop discusso, il trasmettitore commuta le antenne di trasmissione, solo nel caso di ritrasmissioni di packet. La prima prova di una trasmissione di packet è sull'antenna uno, la prima ritrasmissione sull'antenna due, la seconda ritrasmissione sull'antenna tre e così via, in modo round-robin (cioè l'alternarsi in modo circolare). Tale approccio è basato sull'assunto che, per gli errori di canali bursty, è meglio commutare verso un canale, spazialmente diverso, che ritrasmettere sullo stesso canale e incontrare, probabilmente, lo stesso errore burst che ha colpito il packet originale.

A volte, per ragioni di costo, o in piccole aziende, non è possibile equipaggiare le stazioni con antenne multiple. Un approccio alternativo per raggiungere la diversità spaziale, nel processo di trasmissione, è di lasciare che le altre stazioni aiutino con ritrasmissioni di packet. Quando una stazione A fallisce la trasmissione di un packet verso la stazione C, un'altra stazione B può aver preso il packet ed eseguito una ritrasmissione al posto di A. Per evitare la coordinazione, richiesta tra diversi possibili aiutanti B1, B2…, il ruolo di B può essere confinato ad una dedicata stazione. Tali schemi forniscono un tipo di diversità di cooperazione.

Gli approcci per utilizzare la diversità spaziale nelle ritrasmissioni sono risultati essere efficienti nella riduzione della probabilità che le deadlines vengano mancate. Essi lavorano meglio, tuttavia, quando i canali spaziali sono indipendenti/non correlati. Questo è un assunto ragionevole da fare, quando la dissolvenza multipath è la fonte dominante degli errori di canale. Quando un nodo ricevente è posto vicino ad una fonte di interferenza, tuttavia, le antenne di trasmissione che commutano non sono tanto utili perché tutti i canali spaziali saranno influenzati.

2. **Schemi ARQ ibridi:**

negli schemi ARQ ibridi, le ritrasmissioni e la codifica della correzione dell'errore (FEC) possono essere combinate in diversi modi. Nel semplice ARQ ibrido di tipo1, tutti i packet sono codificati in modo FEC e usano sempre lo stesso codice. Quando il ricevitore non può correggere tutti gli errori di bit, esso lascia il packet e richiede una ritrasmissione (fino ad un massimo di prove per packet). Nell'ARQ ibrido di tipo 2, il ricevitore non lascia, semplicemente, i packet errati, ma cerca di usare l'informazione contenuta in tali copie errate per aiutare nella decodifica di ulteriori ritrasmissioni.

Un esempio semplice dello schema ARQ di tipo 2 è il bit-by-bit majority voting (votazione/voto a maggioranza bit-a-bit): una volta che il ricevitore ha ricevuto almeno tre versioni errate dello stesso packet, può indovinare quale packet ricevuto dovrebbe essere, applicando, successivamente, una procedura di majority voting a tutti i bit provenienti dalle precedenti prove. Tale metodo è variato, includendo la deadline e la probabilità di consegna desiderata nella scelta degli schemi di codifica attuali. Majority voting è l'ultima risorsa quando una copia non corretta è stata ricevuta prima della deadline.

In uno schema ARQ di tipo 2 con deadline (codifica dipendente da deadline), il trasmettitore mappa la deadline per un packet e la sua probabilità di consegna desiderata verso uno dei metodi di codifica FEC, creando un numero di bit overhead per i dati. Nell'occasione in cui debba essere fatta una ritrasmissione, il trasmettitore non ripete i dati dell'utilizzatore, ma piuttosto invia più bit overhead. Tale approccio è detto ridondanza incrementale.

3. **Application Lsyer Mechanism:**

a volte può non essere possibile, per i layer più bassi, correggere tutti gli errori di canale. Per eventi asincroni importanti, come gli allarmi, questa restrizione è intollerabile. Per il campionamento di dati periodici di un

processo continuo e lentamente variabile, si può, semplicemente, accettare perdite occasionali, o cercare di nasconderle. Si può, ad esempio, sostituire i campioni mancanti al ricevitore, mediante un valore stimato.

2.3 TECNOLOGIE WIRELESS PER L'INDUSTRIAL AUTOMATION

Per varie ragioni, citate all'inizio dell'introduzione, le tecnologie wireless possono essere vantaggiose per gli ambienti industriali. A causa della tendenza generale verso la standardizzazione e del fatto che sono disponibili tecnologie wireless economiche, commercial-of-the-shelf (COTS), sembrerebbe logico solo investigare queste per la loro convenienza nell'impiego industriale. Di particolare interesse, per gli ambienti industriali, sono le tecnologie che non richiedono alcun tipo di concessione della licenza della frequenza. Queste tecnologie includono le tecnologie WPAN, come IEEE 802.15.1/BT e IEEE 802.15.4, così come le tecnologie WLAN dalla famiglia di IEEE 802.11.
Nonostante i vantaggi che una singola rete wireless potrebbe offrire sul piano industriale, vengono spesso richieste reti WLAN/WPAN multiple in parallelo, in regioni dell'impianto diverse o in sovrapposizione. A causa di questo fatto, la coesistenza delle reti multiple dello stesso tipo, o di diverso tipo, ha bisogno di essere studiata. Consideriamo come certi modelli di comunicazione, propri di quelli dei sistemi fieldbus, possono essere impiegati in tali reti in sovrapposizione.

2.3.1 BT TECHNOLOGY/IEEE 802.15.1

Per permettere l'impiego quasi mondiale, il BT special interest group SIG (gruppo di interesse speciale verso BT), ha posto la tecnologia in una banda industriale, scientifica e medica senza licenza (ISM) a 2.4 GHz.
Progettando un sistema semplice, gli inventori di BT lo hanno creato per avere un uso diffuso.
Le reti BT sono organizzate in "piconets" nelle quali un'unità master coordina il traffico tra sette unità slave attive. L'unità master origina la richiesta per una connessione. In un singolo piconet, le varie unità slave possono solo comunicare le une con le altre mediante il master. Nonostante tutto, ogni unità BT può essere membro fino a 4 diversi piconet, simultaneamente (sebbene possa essere master in solo uno di essi). Una formazione in cui diverse piconets sono interconnesse in tale maniera, è detta scatternet (un tipo di rete ad hoc che consiste di due o più piconet). Finora, il ruolo delle scatternet è rimasto relativamente limitato.
Il traffico piconet è strettamente organizzato in un accesso multiplo su divisione di tempo (TDMA/duplex). In questo schema, il master può solo iniziare a trasmettere in slot di tempo dispari (ciascuna slot è lunga 625 μs), mentre le slave possono solo rispondere in slot pari, dopo essere state sondate dal packet del master.
Poiché non c'è coordinazione tra diverse piconets, possono avvenire collisioni di packet, se due piconets sono localizzate una vicino all'altra. Per minimizzare l'effetto di tale collisione, così come per far fronte al fatto che le frequenze, usate da altri apparecchi sul canale radio, possono variare significativamente sulla bandwidth della banda ISM a 2.4 GHz, ogni piconet esegue uno schema di hopping (passaggio) di frequenza piuttosto rapido (FH) su 79 portanti di bandwidth da 1 MHz ciascuno. La frequenza di hopping massima di questo schema è posta a 1.6 kHz (corrispondente alla lunghezza di slot di 625 μs) e la sequenza di hop, usata dalla piconet individuale, viene trovata dall'indirizzo unico del suo master, mediante un algoritmo specifico. Per ciascun packet BT inviato, è scelta una nuova frequenza per inviarlo. Nella versione BT 1.2, è stato introdotto uno schema FH adattivo (AFH), che permette l'esclusione di certe portanti una volta che è stata notata la

corruzione di un packet, avvenuta nella frequenza di un carrier. Bisogna notare che, tuttavia, AFH è usato più come mezzo per migliorare la performance di una piconet BT, in presenza di altri sistemi non hopping nella banda ISM a 2.4 GHz, che come modo per migliorare la performance tra le piconet BT coesistenti.

Sul layer fisico (PHY), i dati sono modulati in modo shift keying della frequenza Gaussian (GFSK) a 1 M/s e trasmessi con una potenza di 0 dBm (1 mW). Con una tale potenza di trasmissione, ci si può aspettare, dagli apparecchi BT, che abbiano fino a un'area nominale di circa 10 m. BT può anche essere usato con una potenza di trasmissione fino a 20-dBm. La trasmissione, a tale potenza, risulta in una più vasta area, ma richiede l'impiego di un controllo di potenza per riempire i ruoli della banda ISM.

Sul layer di link dei dati, viene fatta una distinzione tra i packet senza connessione asincronica (ACL) e quelli orientati con una connessione sincronica (SCO): i link ACL assicurano una trasmissione di dati attendibile con uno schema ARQ che inizia la ritrasmissione di un packet, in caso in cui la valutazione, del controllo della ridondanza ciclica inclusa (CRC), mostri inconsistenze. Esistono dei diversi tipi di ACL e possono occupare sia una, sia tre, sia cinque slot di tempo ACL, in relazione a quale tipo è usato. Tre dei tipi di packet ACL includono payloads (carichi utili) non codificati, mentre gli altri tre hanno payloads che sono protetti da FEC a velocità-2/3 (velocità di codice) che usa un codice di blocco Hamming abbreviato di lunghezza 15 o 10 senza alcun interleaving (è un modo per organizzare i dati in maniera non contigua per aumentare la performance). I tipi di packet ACL non codificati sono conosciuti come DH1, DH2 e DH3, mentre i tre codificati sono conosciuti come DM1, DM3 e DM5. Usando packet del tipo DH5, per i dati e DH1, per conferma, si ha il throughput massimo possibile (unidirezionale) per BT a 723 kb/s.

I link SCO, al contrario, supportano il traffico in tempo reale, ri-servendo gli slot del tempo a intervalli periodici. Le ritrasmissioni non sono permesse con questi tipi di link, ma nella versione BT 1.2/2.0, i link SCO "estesi" sono stati introdotti, dove può essere fatto un numero limitato di ritrasmissioni. I tre differenti tipi di packet SCO hanno tutti la stessa lunghezza e richiedono un tempo di 366 μs per trasmissione. Essi trasportano, di solito, 64kb/s di parole codificate con il metodo "continuously variable slope delta modulation" (CVSD) e sono differenziate dall'avere o i payloads non protetti, i payloads codificati FEC velocità-2/3, o i payloads codificati FEC velocità-1/3. Tali tipi di packet sono conosciuti come HV3, HV2 e HV1, rispettivamente. Il link SCO esteso è molto flessibile, supportando le varie velocità di trasmissione. I packet SCO persi possono essere sostituiti da un modello di cancellazione.

A causa della breve area di BT e del piccolo numero di slave che sono attive, a qualsiasi momento, diversi piconets BT indipendenti coesisteranno in ambito industriale.

Quando due piconets, che si sovrappongono, operano su diverse frequenze, la qualità del segnale è buona, ma quando essi passano (hop) alla stessa frequenza, i packet possono essere distrutti oltre la ricognizione. Quando si usa un metodo senza codifica, la potenza consumata dalla rete, così come il carico globale della rete, è ridotta. Per ottenere un buon throughput ed avere una bassa interferenza, è svantaggioso usare tipi di packet brevi. Tale fatto è sfortunato, perché i packet brevi sono, di solito, usati nelle applicazioni industriali.

La sicurezza è supportata in BT dalla specificazione dell'autenticazione e dalla codifica.

Lo sviluppo più recente per BT è la versione BT 2.0. La versione BT 2.0 ha aumentato le velocità dei dati, usando gli schemi di modulazione π/4-DQPSK e 8DPSK oltre a quello tradizionale GFSK. La velocità della trasmissione, che risulta da questi miglioramenti, è circa tre volte più alta rispetto alle versioni precedenti di BT.

2.3.2 IEEE 802.15.4

IEEE 802.15.4 definisce le specifiche riguardanti lo strato fisico e MAC per low-rate wireless personal area network (LR-WPAN). A differenza della wireless local area network (WLAN), la quale racchiude la famiglia IEEE 802.11, LR-WPAN enfatizza le operazioni short-range, low-data-rate, energy-efficency, e low-cost. Di conseguenza LR-WPAN è diventato uno delle più probabili tecnologie per le wireless sensor network (WSN).
Caratteristiche principali della rete di comunicazione:

- Data rate di 250 kb/s, 40kb/s e 20 kb/s
- Operabilità in configurazione a stella o mesh
- 16 bit o 64 bit di indirizzo allocati
- Accesso al canale in modalità CSMA-CA
- Completa definizione del protocollo per il trasferimento dei dati
- Basso consumo di potenza
- Indicazione della qualità del canale
- 16 canali nella banda attorno a 2.45 GHz, 10 canali nella banda attorno a 915 MHz, un canale ad 868 MHz

2.3.2.1 TOPOLOGIE DI RETE

Una rete LR-WPAN può essere composta da due diversi tipi di dispositivi: FFD (Full Function Device) e RFD (Reduced Function Device).
Un dispositivo FFD può dialogare con entrambi i dispositivi a differenza di un RFD che può dialogare soltanto con un FFD.
Il dispositivo FFD può operare all'interno di una rete secondo tre modalità:

- Funzionando da coordinatore della rete
- Funzionando da coordinatore semplice
- Funzionando, semplicemente, da terminale di comunicazione

Una rete LR-WPAN, a seconda della specifica applicazione, può essere configurata considerando una particolare topologia.
Due possibili topologie possono essere utilizzate: a stella o mesh.
Mentre in una topologia a stella i dispositivi possono comunicare soltanto con il coordinatore, in una topologia mesh ogni dispositivo può comunicare con tutti i dispositivi vicini..
Di conseguenza, in una topologia a stella, il centro stella controlla e gestisce ogni tipo di comunicazione ed è tipicamente collegato ad alimentazione fissa.
Una topologia mesh è principalmente rivolta ad applicazione come il controllo e monitoraggio industriale, reti di sensori wireless e sicurezza ambientale, mentre, una topologia a stella è rivolta ad applicazioni tipiche come l'home automation o il collegamento di periferiche al pc.

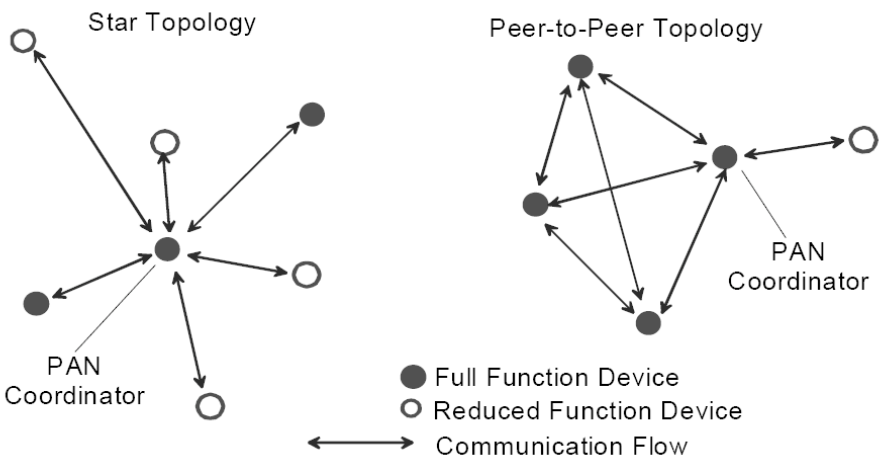


Figura 26 - Topologie di rete previste dallo standard IEEE 802.15.4

2.3.2.2 DEFINIZIONE DEI LAYERS

L'architettura di una LR-WPAN è conforme al modello ISO-OSI, di conseguenza è strutturata a strati (layers). Ogni strato è responsabile di una parte dello standard e gli corrispondono specifiche funzioni.
Lo standard 802.15.4 pone le specifiche relative ai due strati più bassi non preoccupandosi degli strati superiori.
Al physical level avviene l'attivazione o la disattivazione del ricetrasmettitore, la selezione ed il controllo del canale, la trasmissione e la ricezione dei pacchetti attraverso il mezzo fisico.
Al MAC level avviene il controllo dell'accesso al mezzo fisico, viene gestita la connessione o disconnessione alla rete, viene attuata la tecnica CSMA-CA (Carrier Sense Multiple Access with Collision Avoidance) per l'accesso al canale, con la possibilità di utilizare dei GTS (Guaranteed Time Slot) che garantiscono l'accesso al canale su base priorità.
Lo strato superiore è costituito dal network level e provvede alla gestione ed indirizzamento dei messaggi all'interno della rete.

2.3.2.3 TRASFERIMENTO DATI

Il trasferimento di dati comprende 3 diverse modalità.

- Trasmissione dal dispositivo al coordinatore
- Ricezione dei dati dal coordinatore al dispositivo
- Trasmissione e ricezione dei dati tra due dispositivi (rete mesh)

Se la rete supporta i beacon, quando un dispositivo deve trasferire dati al coordinatore attende prima il network beacon.

La ricezione del beacon, di conseguenza, porta il dispositivo a sincronizzarsi con il superframe e inviare i suoi pacchetti di dati (data frame) in modalità slotted CSMA-CA per la gestione delle collisioni.
Di conseguenza il coordinatore comunica al dispositivo l'avvenuta ricezione dei dati mediante un frame di "acknowledgment", con cui si completa la transazione.

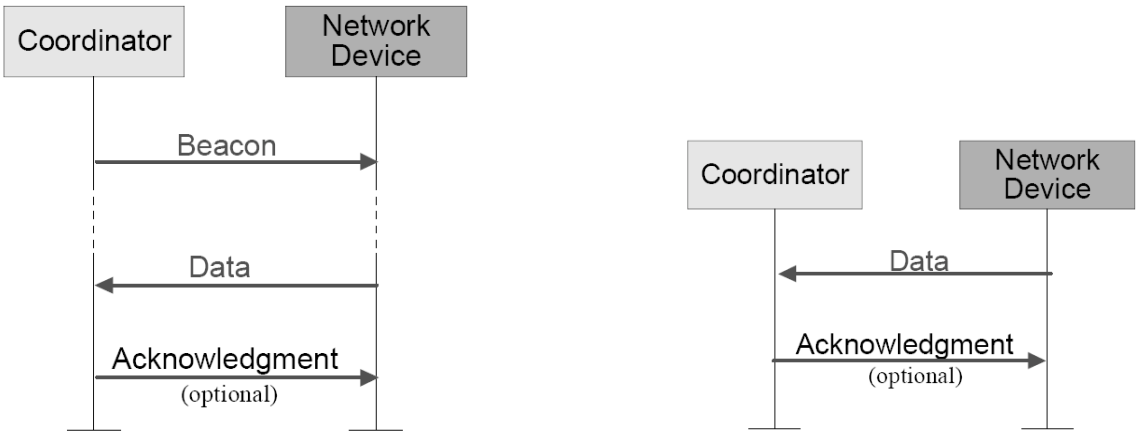


Figura 27 - Protocollo per il trasferimento dei dati al coordinatore in modalitá "beacon" e non

Se la rete non supporta i beacon, il dispositivo trasmette il suo data frame usando però, un "unslotted CSMA-CA", in quanto la rete non è ora sincronizzata.
Anche in questo caso, un messaggio opzionale di "acknowledgment" dal coordinatore completa il trasferimento.

Per quanto riguarda il trasferimento dei dati dal coordinatore, se la rete supporta i beacon, il coordinatore indica nel beacon la presenza di un messaggio in attesa.
Il dispositivo ascolta periodicamente il segnale ed in questo caso trasmette un comando di "data request" in modalità CSMA-CA.
Il coordinatore segnala l'avvenuta ricezione della richiesta mediante un frame di "acknowledgement", quindi il data frame pendente viene inviato sempre in modalità CSMA-CA.

In una rete che supporta i beacon, il coordinatore indica nel network beacon la presenza di un messaggio di attesa.
Il dispositivo ascolta periodicamente il segnale ed in questo caso trasmette un comando di "data request" in modalità CSMA-CA.
Il coordinatore segnala l'avvenuta ricezione della richiesta mediante un frame di "acknowledgement", quindi il data frame pendente viene inviato sempre in modalità CSMA-CA.
Il dispositivo segnala l'avvenuta ricezione dei dati trasmettendo a sua volta un frame di acknowledgment.
Il messaggio viene così rimosso dalla lista dei dati in attesa all'interno del beacon.
Se la rete non supporta i beacon, il coordinatore mette da parte i dati per uno specifico dispositivo, attendendo il suo data request; questo viene inviato dal dispositivo in questione in modalità unslotted CSMA-CA.
Il coordinatore segnala l'avvenuta ricezione della richiesta con un acknoledgment di ritorno, cui segue, nel caso vi siano effettivamente messaggi pendenti, l'invio del data frame.
Se non vi sono messaggi pendenti, il coordinatore trasmette un data frame con un payload di lunghezza nulla ad indicare l'assenza di messaggi. La transazione si completa quindi, con l'invio di un frame di acknoledgment al coordinatore.

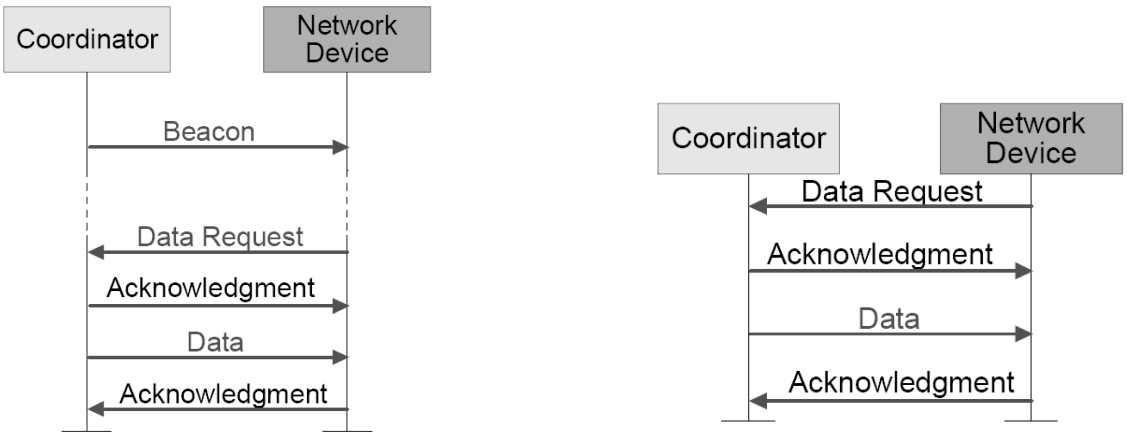


Figura 28 - Modalità di trasferimento dei dati dal coordinatore in entrambe le direzioni

In una rete mesh infine, un dispositivo deve essere in grado di comunicare con ogni altro presente nella propria sfera di copertura.
Per fare ciò, i dispositivi che vogliono comunicare possono rimanere costantemente in ascolto oppure sincronizzarsi.

2.3.2.4 RETI LOCALI WIRELESS SPREAD SPECTRUM

Le reti locali wireless utilizzano tecniche di modulazione a dispersione dello spettro (spread-spectrum) e funzionano nelle bande dei 900MHz, 2.4GHz e 5.8GHz.
La seguente figura confronta gli intervalli di trasmissione in queste bande che sono compresi fra 902 e 928MHz, fra 2.400 e 2.483GHz e fra 5.725 e 5.850GHz.

Si tratta di bande cosiddette ISM (Industrial, Scientific and Medical) *senza licenza*.

Una rete locale wireless, come una rete telefonica cellulare, deve avere *capacità di accesso multiplo*, ovvero più utenti devono avere la possibilità di condividere un determinato insieme di frequenze.

Questa condivisione è necessaria in quanto l'ampiezza di banda disponibile non è sufficiente per stabilire un canale permanente per ciascun utente.

La tecnica di accesso deve essere esente da disturbi, deve essere sufficientemente robusta per supportare le interferenze e deve avere una bassa probabilità di intercettazione, in modo da garantire la privacy degli utenti.

Queste funzionalità sono offerte dalle tecniche a *dispersione dello spettro spread-spectrum*.

Queste tecniche forniscono quindi a più utenti un accesso simultaneo ad un ampia gamma di bande di frequenza, tramite metodi CDMA (Code Division Multiple Access).

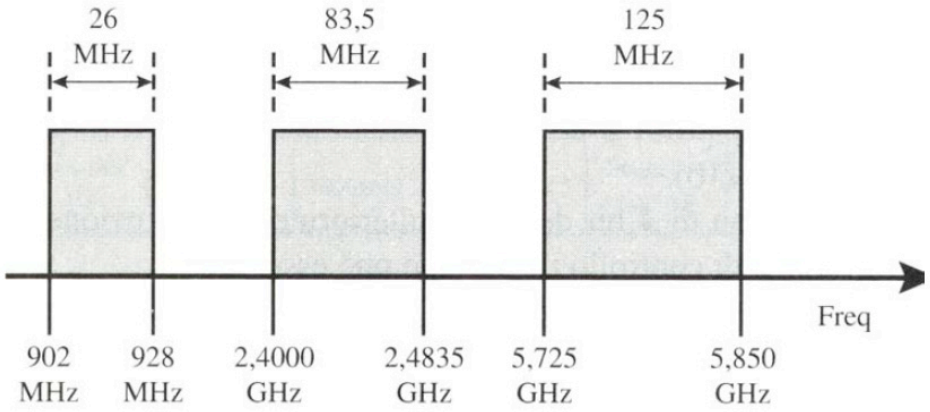


Figura 29 – Le tre bande ISM utilizzate per le reti locali wireless

Lo scopo della dispersione di spettro è quello di distribuire la potenza del segnale su un'ampiezza di banda W molto maggiore rispetto alla velocità di trasmissione R in bit/s.

Questo significa che il fattore di espansione dell'ampiezza di banda W/R è molto maggiore di 1.

Introducendo delle forme d'onda codificate per sfruttare la ridondanza disponibile in questa ampiezza di banda espansa, i sistemi di comunicazione a dispersione dello spettro, risolvono gli elevati livelli di interferenza che possono verificarsi nei canali wireless.

L'utilizzo di *sequenze pseudocasuali* è un altro fattore importante dei sistemi a dispersione di spettro, in quanto si fa in modo che il segnale assuma l'aspetto di rumore casuale.

Questo complica le intercettazioni da parte di ricevitori non autorizzati.

La seguente figura mostra gli elementi chiave del sistema di comunicazione digitale a dispersione di spettro.

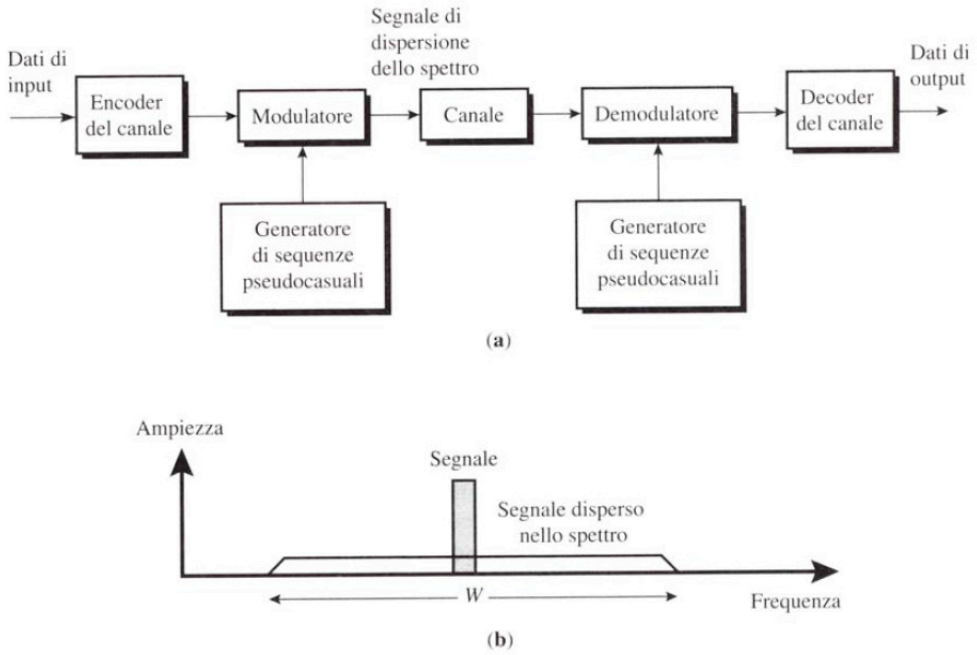


Figura 30 – La tecnica di dispersione dello spettro

All'estremità trasmittente le informazioni entrano in un encoder ad una velocità di R bit/s per produrre un segnale analogico con un'ampiezza di banda relativamente stretta, su una determinata frequenza centrale. Un generatore di sequenze produce una sequenza pseudocasuale di valori binari che viene sovrapposta al segnale trasmesso in un modulatore.
La sequenza pseudocasuale binaria è costituita da una serie di cifre casuali, che si ripete dopo un determinato periodo.
Questa modulazione del segnale con una sequenza pseudocasuale, ha lo scopo di aumentare significativamente l'ampiezza di banda del segnale trasmesso.
All'estremità ricevente, per demodulare il segnale viene impiegato un generatore di sequenze pseudocasuali identico.
Infine il decoder di canale ripristina il flusso di dati originario.
Nelle reti locali wireless, si utilizzano principalmente 2 metodi di dispersione dello spettro:

- FHSS (Frequency Hopping Spread Spectrum)
- DSSS (Direct Sequence Spread Spectrum)

Si tratta sostanzialmente di tecniche di segnalazione differenti e non interoperabili.

2.3.3 IEEE 802.11 TECHNOLOGIES

IEEE 802.11 è composto da un numero di specifiche che, principalmente, definiscono i layer MAC e fisici dei sistemi WLAN. Al pari di altri standard dalle serie IEEE 802.x, i IEEE 802.11 MAC indicano il logical link control (LLC) (letteralmente controllo di link logico) IEEE 802.2 come interfaccia standard verso layer più elevati. Poiché IEEE 802.11 è

uno standard WLAN, la sua funzione principale è quella di fornire un throughput elevato ed una continua connessione di rete. A causa dell'attenzione sulle tecnologie COTS per connessioni wireless nell'industria, saranno trattate, qui, soltanto le più comuni variazioni ed estensioni dei sistemi IEEE 802.11. Tali variazioni ed estensioni comprendono 802.11 MAC, IEEE 802.11a, IEEE 802.11b, e IEEE 802.11g per layer fisici, così come estensioni pertinenti, rispetto alla pianificazione di rete e QoS. I parametri principali di IEEE 802.11 a/b/g sono i seguenti.

- IEEE 802.11a si trova nelle bande dei 5-GHz che sono esenti da licenza in Europa (5.15–5.35 GHz e 5.47–5.725 GHz) e senza licenza negli Stati Uniti (bande UNII, 5.15–5.35 GHz and 5.725–5.825 GHz). Sull'intero spettro, questo consente, a 21 sistemi, di funzionare in parallelo in Europa ed a 8 di funzionare negli USA. Il layer fisico IEEE 802.11 (PHY) si basa sul multicarrier system orthogonal frequency-division multiplexing (OFDM). Vi sono sette modalità, dalla modulazione BPSK con velocità-1/2 FEC e 6-Mb/s di velocità dati alla modulazione a 64-QAM con velocità -3/4 FEC e 54-Mb/s di velocità dati. Le velocità massime, visibili all'utente, dipendono dalle dimensioni dei packet trasmessi. Nella modalità a 54-Mb/s, la trasmissione dei packet di Ethernet, lunghi 1500 B, risulta in una velocità massima, per utente, di circa 30 Mb/s, mentre trasmettere packet con payloads dell'utente di appena 60 B, risulta in un throughput di 2.6 Mb/s. Quest'ultimo valore di throughput è quello che interessa nelle applicazioni industriali, dal momento che le dimensioni piccole dei packet sono dominanti nelle reti fieldbus.

- IEEE 802.11b è un'estensione ad alta velocità dell'originale IEEE 802.11 a modalità DSSS e per questo usa la banda 2.4-GHz ISM. Anche se in teoria 11 o 13 diverse frequenze centrali possono essere usate per DSSS (a seconda che ci si trovi negli USA o in Europa), solo tre sistemi possono in realtà operare in parallelo. Oltre a supportare le velocità della modulazione 1- e 2-Mb/s del sistema basico IEEE 802.1, il payload del IEEE 802.11b PHY permette una modulazione con 5.5- e 11-Mb/s complementary code keying (CCK). Le velocità massime dei dati per utente sono 7.11 Mb/s nel caso di packet di Ethernet e 0.75 Mb/s nel caso di packet con payload a carico dell'utente di 60 B in lunghezza.

- IEEE 802.11g è un'estensione alla specifica IEEE 802.11b e, perciò, è posta nella banda a 2.4-GHz. Supporta quattro distinti layer fisici, di cui due sono vincolanti: il PHY che è identico a IEEE 802.11b e un OFDM PHY che usa la stessa modulazione e le combinazione di codici del IEEE 802.11a. A causa della diversa banda di frequenza, le velocità massime di trasmissione dell'utente sono circa 26 Mb/s per i packet di Ethernet e circa 2 Mb/s per i packet, con payload a carico dell'utente, di 60 B, quando si usa lo schema di modulazione 54-Mb/s.

Si può vedere che, quando si trasmettono packet che contengono piccoli payloads (come nel caso della maggior parte dei sistemi fieldbus), i valori del throughput sono notevolmente ridotti. Questa riduzione è dovuta al grande overhead dei packet IEEE 802.11 ed ai differenti parametri presenti nel protocollo CSMA. A differenza di BT, o IEEE 802.15.4, IEEE 802.11 è stato appositamente ottimizzato per trasmettere grandi file di dati, mostrando, perciò, una performance al di sotto dell'ottimale, quando la maggior parte dei dati è costituita da packet a controllo corto. E' da notare che i valori del throughput possono diminuire ancora di più, quando, in aggiunta, si usano protocolli di layer più elevati. Misurazioni per il throughput

del traffico TCP/IP in packet di Ethernet per la specifica IEEE 802.11b, ad esempio, hanno dato risultati di un throughput massimo di 5-Mb/s. IEEE 802.11 impiega un meccanismo di ritrasmissione dei pacchetti.

In teoria, è possibile avere reti IEEE 802.11 ad hoc, che consistono, soltanto, di stazioni mobili (MS). Tuttavia è più probabile che l'IEEE 802.11 venga usato in una modalità di infrastruttura, in cui un AP trasmette tutte le comunicazioni fra stazioni e altri reti. Per organizzare il traffico nel link radio, IEEE 802.11 MAC fornisce due funzioni di coordinazione. La prima, la *funzione di coordinazione distribuita* (DCF), è obbligatoria e richiede che tutte le stazioni competino per il canale, in accordo con il protocollo CSMA-CA. Quando il meccanismo carrier-sense determina che il canale è libero, una stazione può iniziare a trasmettere. Se il canale viene trovato occupato (busy), la stazione aspetta che la trasmissione in corso finisca, fino a quando il canale torna libero. In quell'istante, inizia un conto alla rovescia casuale. Se il canale diventa occupato prima che il conto termini, il conto si ferma e ricomincia una volta che il canale torna libero. Se il conto termina e nessun'altra stazione ha iniziato una trasmissione nel frattempo, la stazione inizia la trasmissione. La finestra di contesa *(contention window),* dalla quale i valori del conto alla rovescia vengono scelti, aumenta, esponenzialmente, dopo ogni tentativo fallito di trasmettere un packet.
Il metodo base CSMA-CA può essere migliorato con un opzionale handshake RTS/CTS, per evitare situazioni terminali nascosti. L'utente può controllare se l'handshake viene, o non viene, usato configurando una soglia per le dimensioni della struttura. Se la dimensione di una struttura supera la soglia, allora si userà il RTS/CTS, altrimenti no. La seconda funzione di coordinamento, *point coordination function* (PCF), non è obbligatoria ed è pensata per fornire servizi a tempo limitato (time-bounded), suddividendo il tempo in una superstruttura a lunghezza variabile (variable-length), che a loro volta sono suddivisi in un *contention-free period* (CFP) e un *contention period* (CP). All'interno del CFP, viene usato uno schema di votazione/interrogazione in sequenza (polling), mentre l'accesso è regolato secondo DCF durante CP.
A causa dell'esistenza di ostacoli (metallo) e della potenza di trasmissione di 20 dBm, bisogna guardare alla diffusione del ritardo (delay spread) dell'ambiente commerciale, se vi si vuole utilizzare IEEE 802.11. Mentre la diffusione del ritardo, nelle case e negli uffici, è presunta essere <50 e <100, rispettivamente, assume valori di 200-300 ns nell'ambiente commerciale (la diffusione del ritardo è molto meno grave in BT a causa delle sue potenze e velocità di trasmissione, molto più piccole). Nel caso di IEEE 802.11.b, un ricevitore RAKE supporta (solo) circa 60-ns di diffusione di ritardo in modalità 11 Mb/s e 200 ns in modalità 5.5 Mb/s.
Nel caso di IEEE 802.11a o g, la situazione è migliore. A causa dell'intervallo di guardia, tra i simboli del canale inerenti nella tecnologia OFDM, la diffusione di ritardo di diverse centinaia di nanosecondi, può essere supportata, facilmente, senza porre attenzione agli algoritmi del ricevitore impiegati.
Quando si considera la performance della rete globale e non solo la performance del link individuale, il numero delle pubblicazioni che presentato risultati ben fondati è limitato. Quelli esistenti, tuttavia, mostrano che la capacità è, anzi, un problema.

2.4 STANDARD INDUSTRIALI PER WIRELESS SENSOR NETWORK

Gli standard industriali per wireless sensor network presenti nel mercato sono: ZigBee, WirelessHART, ISA100.11a. Tutti questi standards utilizzano IEEE802.15.4 per il phisycal layer ed operano nella banda dei 2.4GHz ISM (Industrial, Scientific and Medical).

2.4.1 ZigBee

Lo ZigBee è specifico per comunicazioni wireless a breve distanza ed a basso consumo di potenza. La velocità di trasmissione massima è di 250 kbps e risulta più bassa rispetto a quella riscontrata per il Bluetooth e UWB. Di conseguenza lo Zig Bee è indirizzato per tutte quelle applicazioni per le quali il traffico dati è basso e c'è la necessità di una elevato numero di device.
I moduli radio con queste specifiche vengono forniti da molti venditori nell'ambito di reti di sensori wireless per applicazioni di monitoraggio e controllo, in scenari come l'home automation e l'industrial automation.

2.4.2 WirelessHART

WirelessHART è una specifica per la comunicazione in HART protocols. Questa specifica, emanata dall'HART Communication Foundation (HFC), si riferisce ad uno dei possibili metodi di trasmissione digitale in ambito wireless. Questo protocollo utilizza una tecnica di modulazione di tipo Direct Sequence Spread Spectrum (DSSS) ed una tecnica di accesso multiplo al canale di tipo CDMA. Vengono inoltre utilizzati il Channel hopping e il mesh networking per ridurre l'interferenza radio e il rumore elettromagnetico. L'appication layer adotta HART protocol con lo scopo di assicurare robustezza, sicurezza e semplicità nella comunicazione. I primi test su campo della specifica Wireless HART hanno riguardato applicazioni di diagnosi dei device e monitoraggio dei processi.

2.4.3 ISA100.11a

L'international society of automation (ISA) si riserva lo scopo di studiare problemi tecnici e standards legati al mondo dell'automazione industriale.
Il comitato ISA SP100 si occupa dello standard wireless industriale chiamato ISA100. L'ISA100 si riferisce ad una famiglia di standard che coprono diverse applicazioni. ISA100.11a, approvata nell'Aprile del 2009 è una specifica per l'automazione dei processi. Lo scopo del comitato ISA100 è aperto e democratico verso utenti e fornitori che vogliono cooperare e sviluppare standards insieme. L'obbiettivo dell'ISA100.11a è una comunicazione sicura e robusta tra le applicazioni riferite all'automazione dei processi. Di conseguenza si occupa della realizzazione ed integrazione di nuovi ed esistenti sistemi di reti wireless. Le specifiche tecniche dell'ISA100.11a comprendono un elevato numero di applicazioni e provvedono alla connessione con differenti tipi di reti.
Il physical layer adottato, come per il WirelessHART, è lo IEEE 802.15.4. Il Data link layer adotta un protocollo ibrido tra un TDMA e un CSMA. Nel network layer la cooperazione tra protocooli come il fielbus, profibus e il modbus può essere effettuata attraverso tunneling o object mapping.

ISA100.12 (WirelessHART convergence) è stato fondato come un sotto-comitato avente lo scopo di esaminare la convergenza tra ISA100.11a e il WirelessHart. In questo comitato, viene studiato un metodo concreto per risolvere il problema di coesistenza di entrambe le tecnologie. La seguente tabella mostra una comparazione tra entrambi gli standard.

Table 1: Comparison table between WirelessHART and ISA100.11a

Item	WirelessHART (HART 7.2)	ISA100.11a
Organization	HART Communication Foundation	ISA SP100 committee
Features	Wireless extension of HART specification	Industrial wireless system specification ISA100 family standard Standards for relational technologies are under consideration such as Factory automation, Backbone network, power source, RFID, Trustworthy wireless, etc.
PHY, MAC Layer	IEEE 802.15.4, 2.4GHz-band DSSS (Direct-Sequence Spread Spectrum) Channel hopping, TDMA, Channel Blacklisting	IEEE 802.15.4, 2.4GHz-band DSSS (Direct-Sequence Spread Spectrum) Channel hopping, TDMA, CSMA, Hybrid Channel Blacklisting
Network Layer	Extended HART address Mesh network	IPv6 addressing (6LowPAN) Mesh network
Upper Layer	HART protocol - Command & response - Burst mode	ISA100.11a Native protocol - Publishing / Subscribe, Client / Server, Bulk, Alert (event notification) Object Mapping, Tunneling protocol (Available existing protocol: HART, FOUNDATION Fieldbus, Profibus, Modbus, etc.)
Security	Encryption: AES128bit public symmetric key Join Key, Network ID, End to end security	Encryption: AES128bit public symmetric key Join Key, Network ID, End to end security Public key cryptosystem (option)

2.4.4 REGOLAZIONE RADIO

Gli standard wireless menzionati precedentemente operano nella frequenza dei 2.4 Ghz (2400-2483,5 MHz) con una banda di 2 Mhz per canale. Il numero di canali disponibili nella banda dei 2.4 Ghz è di 16. Lo IEEE802 è uno standard indirizzato per device low-power e la potenza in trasmissione dipende dalle regolamentazioni regionali (US up to 1W, Europe up to 100mW, Japan up to 10mW/Mhz).
Inoltre può essere utilizzata la frequenza dei 915 MHz (902-928 MHz) con 10 canali a disposizione. Questa frequenza radio possiede una buona diffrazione ed un'alta permeabilità.

2.4.5 APPLICAZIONI WIRELESS PER L'AUTOMAZIONE DI PROCESSO

Esistono due principali soluzioni wireless nell'automazione di processo nell'impianto: field network e plant network. Per field network si intende una rete wireless di sensori aventi funzionalità di diagnosi, monitoraggio dei processi e in futuro, anche di controllo dei processi. Viceversa, per plant network, si intende una rete (Wi-Fi 802.11a/b/g) di dispositivi utilizzati per il mobile monitoring, la video sorveglianza, l'asset, l'human tracking e l'RFID. L'utilizzo del wireless permette all'utente di ridurre i costi relativi all'acquisto di nuovi field sensor. Inoltre attraverso soluzioni mesh è possibile sviluppare (senza costi aggiuntivi) sistemi ridondanti per aumentare l'affidabilità dell'intera rete. L'integrazione con una plant network permette

inoltre un aumento dell'efficienza del lavoratore in termini di semplicità e mobilità per quanto riguarda il monitoraggio ed il controllo dei processi.

2.4.6 LA TECNOLOGIA WIRELESS PER L'INDUSTRIA

ISA100.11a ed il WirelessHart sono stati proposti come standards wireless industriale ed entrambi utilizzano l'IEEE802.15.4 nella frequenza dei 2.4 Ghz come lo ZigBee. Parallelamente anche il Wi-Fi (802.11a/b/g) sfrutta la frequenza dei 2.4 Ghz per le proprie comunicazioni. Il relativo problema di coesistenza di entrambi gli standard viene attenuato dalla possibilità di effettuare un channel hopping. In entrambi gli standard è inoltre possibile utilizzare una star topology o una mesh topology. Il trade-off nel proporre una topologia di rete al posto dell'altra, risiede nel rapporto tra flessibilità e prestazioni. Di conseguenza ottenere una maggiore flessibilità dei device su uno specifico scenario di riferimento, porterebbe a dover scegliere una soluzione mesh a discapito di una a star. Viceversa una soluzione star apporterebbe una minor latenza nel trasferimento dei dati a differenza di una soluzione mesh. Una conseguente visione globale riguardante le esigenze reali dell'impianto risulta perciò indispensabile nella scelta della topologia di rete.

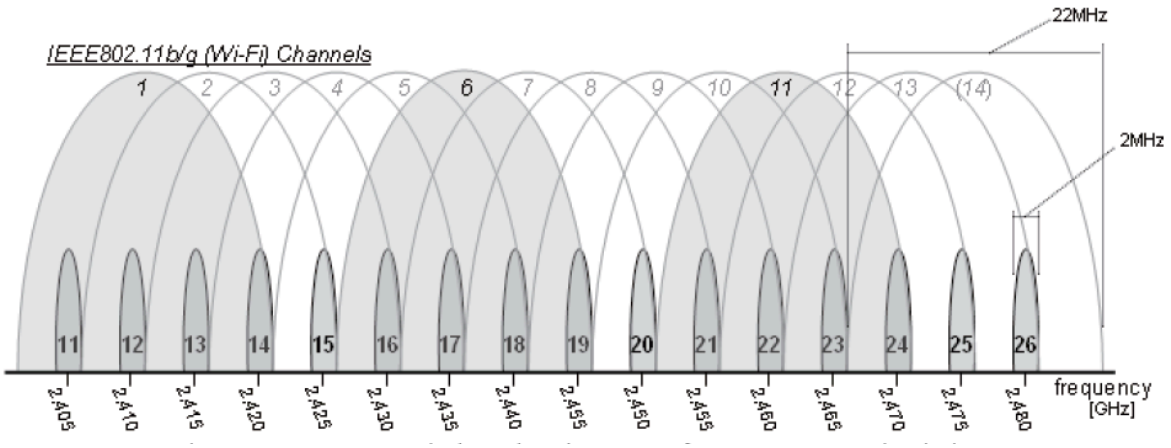


Figura 31 – Assegnazione delle frequenze e delle bande nello IEEE802.15.4 e Wi-Fi

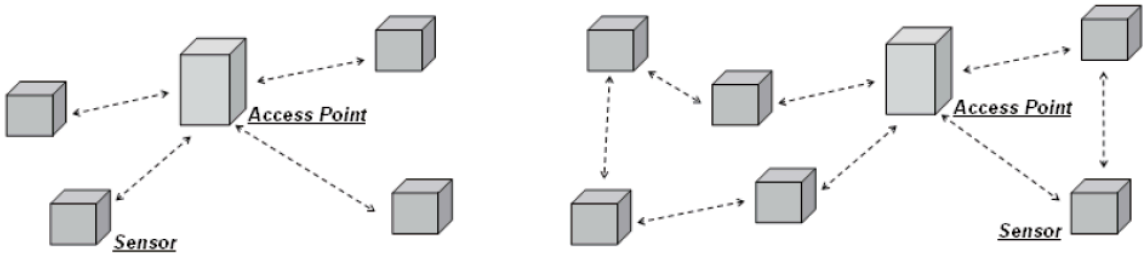


Figura 32 – Star e Mesh topology network

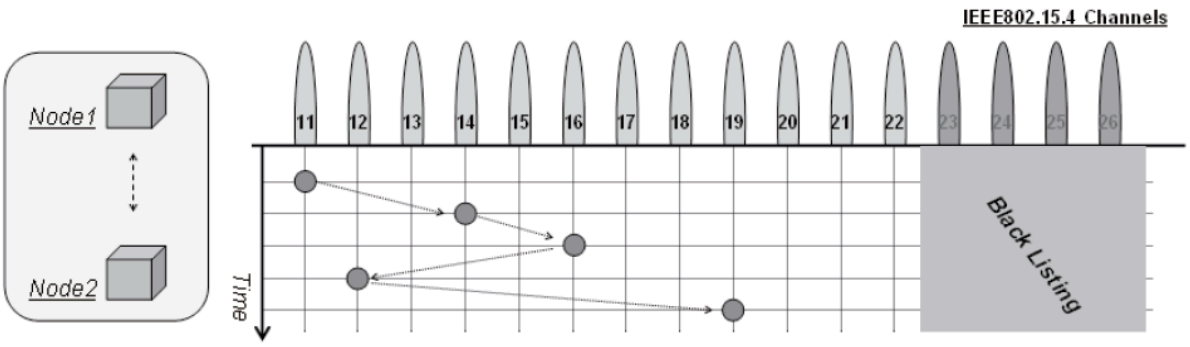


Figura 33 – Frequency hopping

3 ROUTING IN WIRELESS SENSOR NETWORK

3.1 INTRODUZIONE

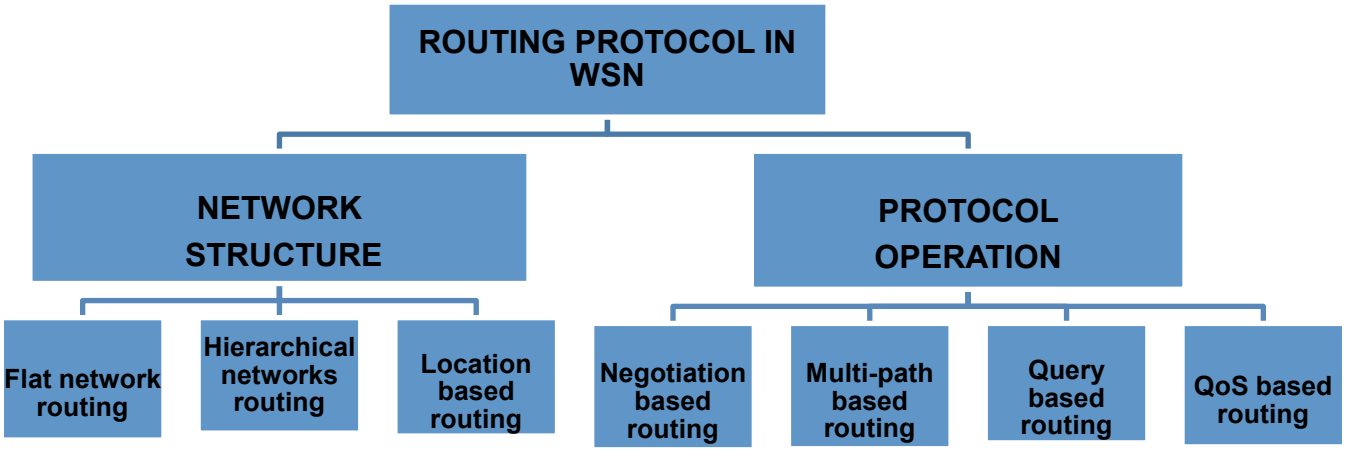
Una rete di sensori è un sistema di sensori auto-aggreganti, a basso costo, basso consumo energetico e facilmente accessibili da postazioni remote per il controllo e la raccolta dei dati. Tali sistemi, imponendo una fitta rete di sistemi di monitoraggio e controllo, hanno l'obiettivo di ridurre l'impiego umano direttamente sul campo.
I nodi della rete sono caratterizzati da un'architettura molto semplice e potenza di calcolo/trasmissione moderata. Sono tipicamente usati per il monitoraggio di parametri relativi alla temperatura, umidità, pressione, vibrazioni ecc…
Particolare attenzione è concentrata su tecniche di trasmissione/ricezione che consentano la riduzione dei consumi di energia e quindi l'aumento del tempo di autonomia della rete. In particolare: strategie cooperative per l'instradamento ottimale e la trasmissione efficiente di dati in reti ad-hoc tecniche per l'ottimizzazione del consumo energetico (batterie) o per la massimizzazione della capacità di trasmissione.

3.2 CLASSIFICATION ROUTING PROTOCOLS

Le principali limitazioni dei routing protocol sono:

- High power consumption
- Low bandwidth
- High error rates
- High delay

Una classificazione dei diversi routing protocol per sensor networks è riportata nella seguente figura:



Network Structure:

- Flat network routing: uguali funzioni per tutti i nodi
- Hierarchical networks routing: differenti funzioni per un insieme di nodi
- Location based routing: i dati vengono instradati tenendo presento la posizione dei nodi

Protocol Operation:

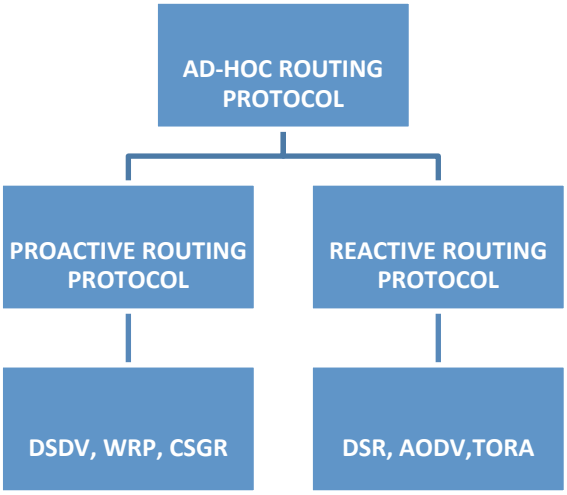
- Negotiation based routing: utilizza la descrizione dei dati per eliminare la duplicazione
- Multi-path based routing: vengono utilizzati più path per aumentare la ridondanza dei dati ed aumentare il fault tollerance
- Query based routing: utilizza un meccanismo su base query per l'istradamento dei dati
- QoS based routing: viene utilizzato un compromesso tra bandwidth, Energy, etc…

3.3 AD-HOC ROUTING PROTOCOLS

Ad-hoc routing rappresenta un insieme di standards che descrivono il routing dei packets tra i diversi devices.
I routing protocols sono classificati in tre tipi:

- Proactive/table-driven routing protocols: nella tabella di routing vengono riportati i diversi path per le diverse destinazioni
- Reactive/On-Demanding routing protocols: un meccanisco di route discovering è utilizzato per trovare il best path

- Hybrid routing protocols: è una combinazione tra il Proactive e Reactive routing protocols



AODV e DSDV sono i principali protocolli di routing che vengono maggiormente utilizzati.

3.3.1 DSDV (DESTINATION-SEQUENCE DISTANCE-VECTOR)

Il protocollo si basa sul'algoritmo bellman-ford per trovare il best path. Questo algoritmo è molto simile al più popolare Dijkstra's algorithm con l'aggiunta di pesi negativi. Ogni nodo mantiene una tabella contenente tutte le destinazioni disponibili, il numero di hops necessari, e un sequence number. L'utilizzo del sequence number ha lo scopo di distinguere vecchie e nuove route. Per tenere traccia dei cambiamenti, un messaggio periodico contenete la routing table viene trasmesso da ciascun nodo ai suoi vicini.
L'update della routing table è time-driven ed event-driven.

3.4 AODV (Ad-hoc On-demand Distance Vector)

3.4.1 INTRODUZIONE

L'Ad-hoc On-demand Distance Vector è un protocollo di routing di tipo *reactive*. Di conseguenza vengono ricercati i percorsi nella rete solo su richiesta, al contrario dei protocolli più comuni in Internet e nelle reti cablate che individuano tutti i nodi ed i percorsi possibili della rete indipendentemente dal loro utilizzo (protocolli di tipo *proactive*). Come suggerisce il nome, AODV è un derivato per reti ad-hoc del protocollo Distance Vector (basato sul vettore delle distanze secondo una metrica che può includere vari fattori). Ogni nodo possiede un numero di sequenza (sequence number, monotamente crescente) per una determinata destinazione e viene utilizzato per assicurare l'assenza di cicli nei percorsi.

I pacchetti definiti dal protocollo AODV nel caso in cui si ha la necessità di un "discovering root" per una determinata destinazione, sono:

- **Route request** (RREQ)
- **Route reply** (RREP)
- **Route error** (RERR)

Tutti questi messaggi possono essere implementati come semplici pacchetti UDP, di conseguenza il routing si basa comunque sul Internet Protocol (IP).
Tali tipi di messaggio sono ricevuti tramite UDP, di conseguenza potrebbe essere applicata una normale procedura di tipo IP header. Ad esempio, il nodo richiedente potrebbe utilizzare il suo indirizzo IP per la trasmissione dei messaggi DATA, mentre utilizzare l'indirizzo IP (255.255.255.255) per tutti i messaggi di broadcast.
Inizialmente, quando un nodo sorgente vuole comunicare con un nodo destinazione, controlla nella propria routing table se esiste una rotta verso la relativa destinazione. Se la rotta è conosciuta ed è valida, l'AODV non gioca alcun ruolo. Al contrario, per una rotta non conosciuta o non valida, il nodo sorgente trasmette un RREQ per trovare una rotta verso la destinazione. Una rotta può essere determinata quando il RREQ raggiunge il nodo destinazione o un nodo intermediario con una rotta 'fresh enough' verso la destinazione. Una rotta è 'fresh enough' quando il sequence number associato è maggiore o uguale al sequence number contenuto nel RREQ. La rotta è resa disponibile, inviando (mediante modalità unicast) indietro un RREP verso il nodo RREQ originator. Ciascun nodo, che riceve la richiesta, possiede una rotta verso l'RREQ originator. Di conseguenza, il REEP può essere trasmesso, in modo unicast, verso il RREQ originator.

I nodi controllano lo stato del link dei next-hops delle rotte attive. Quando viene scoperta la caduta di un link su una rotta attiva, viene utilizzato un messaggio RERR, per notificare ad un altro nodo, l'avvenuta perdita del link. Il messaggio RERR indica le destinazioni che non sono più raggiungibili, tramite il link corrotto. Per realizzare questo meccanismo di comunicazione, ciascun nodo possiede una "precursor list" che contiene l'indirizzo IP, per ciascuno dei suoi vicini, che forse lo utilizzano come next-hop, verso ciascuna destinazione. L'informazione nelle precursor lists è acquisita, durante la procedura di generazione del messaggio RREP, che per definizione deve essere inviato ad un nodo in una precursor list.
Può essere ricevuto anche un RREQ per un indirizzo IP multicast. In questa tesi, non viene specificato e né realizzato il processo per tali messaggi.
AODV è un protocollo di routing che tratta la gestione della routing table. L'informazione contenuta nella routing table deve essere mantenuta anche per rotte di breve durata, come quelle create per immagazzinare, in modo temporaneo, percorsi inversi verso nodi che originano RREQ. AODV utilizza i seguenti campi per ciascuna rotta immagazzinata nella tabella di routing:

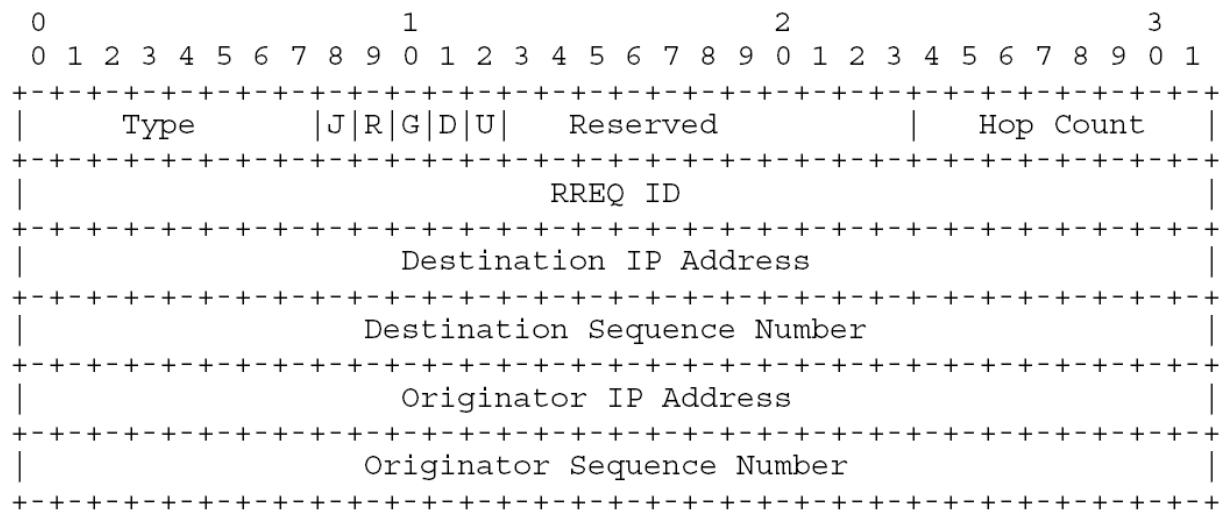
- Indirizzo IP di destinazione
- Sequence number
- Flags di routing (valido, non valido)
- Hop count (numero di hop necessari per raggiungere la destinazione)
- Next-hop
- Lists of precursors

- Lifetime (tempo di decadenza o cancellazione della route)

La gestione del numero di sequenza è essenziale per evitare loops di routing
Il protocollo di routing AODV è progettato per reti ad hoc con numero di nodi da 10 a 1000. L'AODV è stato progettato per ridurre il flooding del traffico di controllo e per eliminare l'overhead sul traffico dati, al fine di aumentare la scalabilità e la performance.

3.4.2 FORMATO DEI MESSAGGI

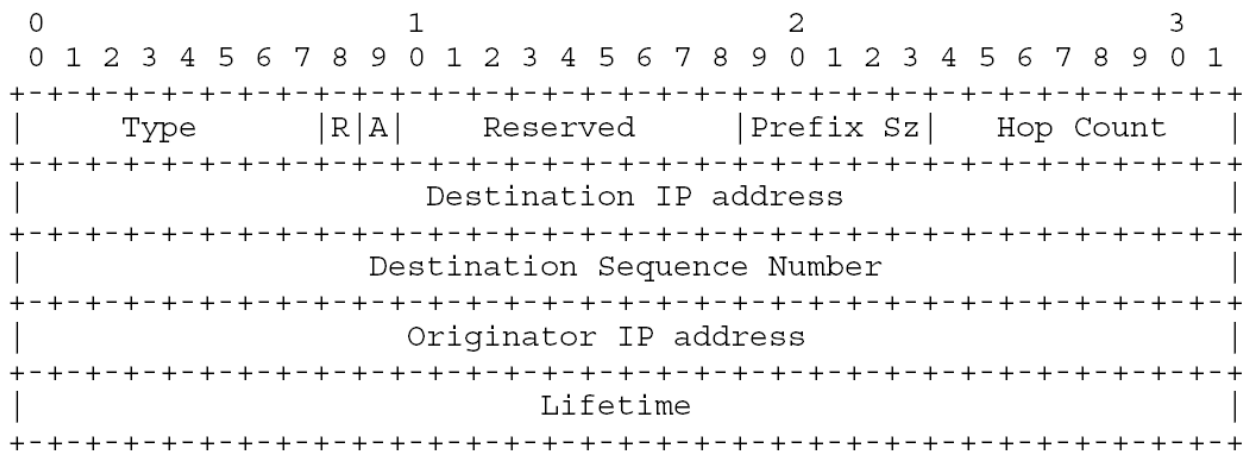
3.4.2.1 FORMATO DEL MESSAGGIO DI RICHIESTA ROTTA (RREQ)



Il formato del RREQ contiene i seguenti campi:

- Type 1
- J Join flag, riservato per multicast(non implementato)
- R repair flag, riservato per multi cast(non implemaentato)
- G flag RREP gratuitous
- D flag di destinazione
- U numero di sequenza sconosciuto
- RESERVED riservato, inviato come 0, ignorato in ricezione(non implementato)
- Hop Count numero di hop dall'originator node al nodo che gestisce la Richiesta
- RREQ ID un numero di sequenza che identifica solo il RREQ
- Destination IP Address indirizzo IP della destinazione;
- Destination Sequence Number ultimo numero di sequenza ricevuto;
- Originator IP Address indirizzo IP del nodo che ha originato la richiesta di rotta;
- Originator Sequence Number il numero di sequenza attuale

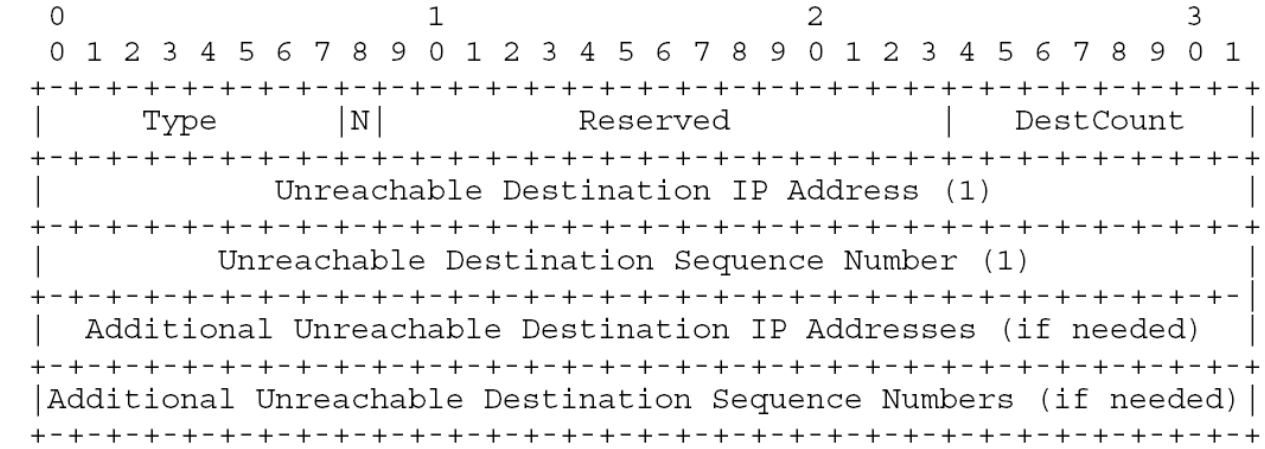
3.4.2.2 FORMATO DEL MESSAGGIO RREP



Il formato del RREP contiene i seguenti campi:

- Type 2
- R repair flag, usato per multi cast(non implementato)
- A (non implementato)
- Reserved Prefix Size spedito come 0, ignorato in ricezione(non implementato)
- Hop Count numero di hop dall'indirizzo IP di origine all'indirizzo IP di destinazione
- Destination IP Address indirizzo IP della destinazione
- Destination Sequence Number il numero di sequenza della destinazione associato alla rotta
- Originator IP Address indirizzo IP del nodo che ha originato il RREP
- Lifetime il tempo (millisecondi) entro il quale i nodi che hanno ricevuto un RREP considerano valida la rotta.

3.4.2.3 FORMATO DEL MESSAGGIO DI ERRORE DI ROUTE (RERR)



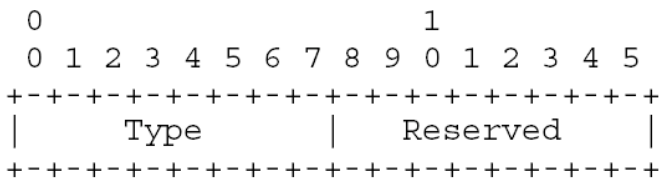
Il formato del messaggio di errore di route illustrato sopra e contiene i seguenti campi:

- Type 3
- N flag no delete(non implementato)
- Reserved inviato come 0, ignorato in ricezione(non implementato)
- Destcount numero di destinazioni non raggiungibili
- Unreacheable Destination IP Address l'indirizzo IP della destinazione che è divenuto irraggiungibile a causa della caduta di link;
- Unreacheable Destination Sequence Number il sequence number della rotta relativa alla destinazione irraggiungibile

Il messaggio RRER è inviato se la caduta di un link rende una o più destinazioni irraggiungibili da parte di uno o più nodi vicini.

3.4.2.4 FORMATO DEL RREP-ACK

Il messaggio RREP-ACK DEVE essere inviato in risposta ad un messaggio RREP.



- Type 4
- Riserved inviato come 0, ignorato in ricezione

3.4.3 MANTENIMENTO DEI SEQUENCE NUMBER

Ogni rotta contenuta nella routing table DEVE includere l'ultima informazione disponibile sul sequence number per l'indirizzo IP del nodo di destinazione.
Il sequnce number è aggiornato ogni volta che un nodo riceve nuove informazioni sul numero di sequenza da parte dei messaggi RREQ, RREP o RERR che possono essere ricevuti in relazione a quella destinazione. Un nodo di destinazione incrementa il proprio SN in due circostanze:

- Immediatamente prima che un nodo origini un RREQ, DEVE incrementare il proprio numero di sequenza.
- Immediatamente prima che un nodo di destinazione origini un RREP in risposta a un RREQ, DEVE aggiornare il proprio numero di sequenza.

Per accertarsi che l'informazione riguardante una destinazione non sia scaduta, il nodo compara SN presente in routing table con quello ottenuto dal messaggio AODV in entrata.
L'unica altra circostanza in cui un nodo può cambiare il numero di sequenza della destinazione, in una delle rotte della routing table, è in risposta alla caduta di un link verso quella destinazione. Nella propria routing table, il nodo determina quali destinazioni utilizzano il link corrotto come next-hop. In questo caso, per ciascuna destinazione che utilizza il nodo corrotto come next-hop, viene incrementato il numero di sequenza e marcata la rotta come invalida. Ogni volta che una qualsiasi informazione (routing 'fresh enough') per una determinata destinazione (cioè, contenente un numero di sequenza almeno uguale al numero di sequenza registrato)viene ricevuta da un nodo che ha marcato quella rotta della propria routing table come invalida, il nodo DOVREBBE aggiornare la sua informazione della routing table, in accordo con l'informazione contenuta nell'aggiornamento.

3.4.4 ROTTE DELLA ROUTING TABLE E PRECURSOR LISTS

Quando un nodo riceve un pacchetto di controllo AODV da un vicino, crea o aggiorna una rotta per una particolare destinazione, controllando se la rotta è già presente nella routing table. Nel caso in cui non vi sia una rotta corrispondente per quella destinazione ne viene creata una nuova. Al contrario la rotta viene aggiornata, se il nuovo sequence number è:

- Più alto del numero di sequenza della destinazione presente nella tabella di routing
- I numeri di sequenza sono uguali, ma il conteggio degli hops (della nuova informazione) più uno, è più piccolo del conteggio degli hops esistente nella tabella di route
- Il numero di sequenza è sconosciuto

Il campo Lifetime della rotta presente nella tabella di routing può essere determinato dal pacchetto di controllo oppure inizializzato all'ACTIVE_ROUTE_TIMEOUT. Di conseguenza tale rotta può essere utilizzata per inviare qualsiasi pacchetto di dati.
In ogni istante di tempo in cui una rotta viene utilizzata per inoltrare un pacchetto di dati, il campo di Active Route Lifetime è aggiornato per essere uguale al tempo corrente più l'ACTIVE_ROUTE_TIMEOUT.
Per ciascuna rotta (valida) mantenuta da un nodo nella propria routing table, il nodo mantiene anche una lista di precursori che possono inoltrare pacchetti su questa rotta. Tali precursori riceveranno notificazioni dal nodo nel caso di individuazione di una perdita del link. La lista dei precursori in una rotta della tabella di routing contiene i nodi (vicini) verso i quali una risposta di route è stata generata o inoltrata.

3.4.5 CREAZIONE DI RICHIESTE ROUTE (RREQ)

Un nodo inoltra un RREQ quando determina che ha bisogno di una rotta verso una destinazione e la rotta non è presente nella propria routing table. Questo può accadere se la destinazione è sconosciuta al nodo, o se una rotta, precedentemente valida verso la destinazione, decade o viene classificata come invalida. All'interno del RREQ, il campo sequence number della

destinazione viene posto uguale all'ultimo sequence number conosciuto per tale destinazione. Di conseguenza viene copiato dal campo sequence number della destinazione presente nella tabella di routing. Nel RREQ, l'originator sequence number è posto uguale al sequence number del nodo stesso, e viene incrementato prima dell'inserimento nel RREQ. Il campo ID del RREQ è incrementato di uno dall'ultimo ID del RREQ utilizzato dal nodo corrente. Ciascun nodo mantiene solo un ID di RREQ. Il campo del conteggio di hop è posto uguale a zero.
Prima di trasmettere un RREQ, l'originator node memorizza temporaneamente l'ID del RREQ e l'indirizzo IP dell'originator del RREQ per un PATH_DISCOVERY_TIME. In tal modo, quando l'originator riceve il pacchetto dai suoi vicini, non rielabora e non re-inoltra il pacchetto.
Dopo la trasmissione di un RREQ, un nodo attende un RREP (o un altro messaggio di controllo con informazioni correnti che riguardano una rotta verso la destinazione appropriata). Se una rotta non è ricevuta all'interno del NET_TRAVERSAL_TIME millisecondi, il nodo PUO' cercare ancora di scoprire una rotta, trasmettendo un altro RREQ fino ad un massimo di RREQ_RETRIES volte, ad un valore massimo di TTL. Per ogni nuovo tentativo DEVE aumentare ed aggiornare l'ID del RREQ.
I pacchetti di dati che attendono una rotta (cioè, in attesa di un RREP, dopo che è stato inviato un RREQ) DOVREBBERO essere memorizzati temporaneamente (buffered). Il buffering (memorizzazione temporanea) DOVREBBE essere "first-in, first-out" (FIFO). Se al raggiungimento del RREQ_RETRIES, al massimo TTL, non è stato ancora ricevuto nessun RREP, tutti i pacchetti di dati destinati per quella destinazione corrispondente, DOVREBBERO essere lasciati dal buffer e DOVREBBE essere consegnato all'applicazione un messaggio di destinazione non raggiungibile.
Per ridurre la congestione in una rete, le prove ripetute da un nodo sorgente, alla ricerca di una rotta per una singola destinazione, DEVONO utilizzare un backoff esponenziale binario. La prima volta che un nodo sorgente trasmette un RREQ, attende NET_TRASVERSAL_TIME millisecondi per la ricezione di un RREP. Se non viene ricevuto un RREP in quel tempo, il nodo sorgente invia un nuovo RREQ. Mentre calcola il tempo di attesa per un RREP, dopo aver spedito il secondo RREQ, il nodo sorgente DEVE usare un backoff esponenziale binario. Quindi, il tempo di attesa per il RREP corrispondente al secondo RREQ è 2 * NET_TRAVERSAL_TIME millisecondi. Se non viene ricevuto nessun RREP in quel periodo di tempo, può essere inviato un altro RREQ, fino ad un massimo di RREQ_RETRIES volte dopo il primo RREQ. Per ciascun tentativo in più, il tempo di attesa per RREP è moltiplicato per 2, così che il tempo si conformi al backoff esponenziale binario.

3.4.6 ELABORAZIONE ED INVIO DEI RREQ

Quando un nodo riceve un RREQ, crea o aggiorna, per prima cosa, una rotta verso il precedente hop, poi controlla per determinare se è stato ricevuto un RREQ con lo stesso indirizzo IP originator e ID RREQ in, almeno, l'ultimo PATH_DISCOVERY_TIME. Se tale RREQ è stato ricevuto, il nodo abbandona, il RREQ nuovamente ricevuto.
Per prima cosa, si incrementa di "uno" il valore del conteggio di hop nel RREQ, per conteggiare il nuovo hop mediante il nodo intermedio. Poi il nodo cerca una rotta inversa verso originator node. Se necessario, viene creata o aggiornata la rotta, utilizzando il sequence number del RREQ. Quando la rotta inversa è creata o aggiornata, anche le seguenti azioni sulla rotta sono espletate:

1. Il sequence number presente all'interno del RREQ è comparato al sequence number della rotta presente presente nella routing table e copiato se risulta maggiore;
2. Il conteggio degli hop è copiato dal conteggio degli hop del messaggio RREQ.

Se un messaggio RREQ è ricevuto, il Lifetime della rotta inversa, per l'indirizzo IP originante, è fissato come il maggiore tra (ExistingLifetime, MinimalLifetime), in cui
MinimalLifetime = (current time + 2 * NET_TRASVERSAL_TIME – 2*HopCount* NODE_TRASVERSAL_TIME).
Il nodo corrente può usare la rotta inversa per inoltrare i pacchetti di dati nello stesso modo di qualsiasi altra rotta nella tabella di routing.
Se un nodo non crea un RREP e se l'entrante IP header ha un TTL maggiore di 1, il nodo aggiorna e trasmette il RREQ all'indirizzo 255.255.255.255 su ciascuna delle sue interfacce configurate. Per aggiornare il RREQ, il campo TTL, è diminuito di uno ed il campo di conteggio degli hops nel messaggio RREQ è incrementato di uno, per contare il successivo hop mediante il nodo intermedio. In oltre, il SN della destinazione, per la destinazione richiesta, è fissato come il massimo tra il valore corrispondente ricevuto ed il valore della sequenza di destinazione correntemente mantenuto dal nodo per la destinazione richiesta.

3.4.7 GENERAZIONE DELLE RISPOSTE DI ROUTE (RREP)

Un nodo genera il RREP se:

1. È la destinazione
2. Ha una rotta attiva verso la destinazione; il sequence number della destinazione, nella tabella di routing, è valido e maggiore, o uguale, a quello del numero di sequenza della destinazione nel RREQ

Quando è generato un messaggio RREP, un nodo copia l'indirizzo IP della destinazione e il numero di sequenza dell'originator dal RREQ al RREP.
Una volta creato, il RREP è trasmesso in modo unicast al successivo hop verso l'originator del RREQ. Mentre il RREP è inoltrato verso il nodo che ha creato il messaggio RREQ, il campo del conteggio degli hops è aumentato di "uno" per ciascun hop. Quindi, quando il RREP raggiunge l'origine, il conteggio degli hops rappresenta la distanza, in hops, della destinazione dall'origine.

3.4.7.1 GENERAZIONE DEL RREP DALLA DESTINAZIONE

Se il nodo generante è esso stesso la destinazione, DEVE incrementare il proprio numero di sequenza di "uno" se il numero di sequenza nel pacchetto RREQ è uguale al valore incrementato. Altrimenti, la destinazione non cambia il suo numero di sequenza, prima di generare il RREP. Il nodo di destinazione pone il suo numero di sequenza (forse nuovamente incrementato) nel campo del numero di sequenza della destinazione del RREP ed inserisce il valore zero nel campo di conteggio degli hops del RREP.

Il nodo di destinazione copia il valore MY_ROUTE_TIMEOUT nel campo Lifetime del RREP.

3.4.7.2 GENERAZIONE DEL RREP DA UN NODO INTERMEDIO

Se il nodo generante il RREP non è il nodo di destinazione, ma è un hop intermedio lungo il percorso dall'origine alla destinazione, esso copia il proprio numero di sequenza, conosciuto per la destinazione, nel campo del numero di sequenza della destinazione nel messaggio RREP.
Il nodo intermedio aggiorna la rotta, ponendo il nodo da cui ha ricevuto il RREQ nella precursor list
Il nodo intermedio pone la sua distanza in hop dalla destinazione (indicata dal conteggio di hop nella tabella di routing) nel RREP.

3.4.7.3 GENERAZIONE DEL RREP GRATUITOUS

Dopo che un nodo riceve un RREQ se il nodo intermedio invia un RREP all'originator node, esso DEVE trasmettere, in modo unicast, un RREP gratuitous al nodo di destinazione. Un RREP gratuitous che deve essere inviato alla destinazione desiderata, contiene i seguenti valori nei campi del messaggio RREP:

- Hop count — il numero degli hop come indicato nella rotta (verso l'originator) presente nella routing table
- Indirizzo IP della destinazione — l'indirizzo IP del RREQ originator;
- SN della destinazione
- Lifetime — il rimanente Lifetime della rotta verso il RREQ originator

Un RREP gratuitous è poi inviato al successivo hop lungo il path verso il nodo di destinazione, proprio come se il nodo di destinazione avesse già emesso un RREQ per l'originator node e questo RREP sia stato prodotto in risposta a quel RREQ.

3.4.8 RICEZIONE ED INOLTRO DEI RREP

Quando un nodo riceve un messaggio RREP, esso cerca una rotta verso l'hop precedente. Se è necessario, una rotta viene creata per l'hop precedente. Di conseguenza, il nodo incrementa il valore del conteggio di hops nel RREP di uno. La rotta, per la destinazione, menzionata nel RREP, viene creata se essa non è presente nella routing table. In caso contrario, il nodo compara il numero di sequenza della destinazione presente nella routing table con il numero di sequenza della destinazione immagazzinato nel RREP. Su base comparazione, la rotta esistente è aggiornata solo nelle seguenti circostanze:

- Il numero di sequenza della destinazione nel RREP è maggiore del sequence number della destinazione presente nella routing table
- I SN sono gli stessi, ma la rotta è classificata come inattiva
- I numeri di sequenza sono gli stessi e il nuovo conteggio hop è più piccolo del conteggio di hop presente nella routing table

Se la rotta nella routing table verso la destinazione è creata o aggiornata, allora avvengono le seguenti azioni:

- la rotta è classificata come attiva
- il numero di sequenza della destinazione è marcato come valido
- il successivo hop della rotta è assegnato per essere il nodo da cui il RREP è stato ricevuto
- il conteggio hop è posto come valore del nuovo conteggio hop
- il tempo di decadenza è posto al tempo corrente più il valore del Lifetime nel messaggio RREP
- il numero di sequenza della destinazione è il numero di sequenza della destinazione nel messaggio RREP

Successivamente il nodo corrente può utilizzare questa rotta per inoltrare pacchetti di dati verso la destinazione.
Se il nodo corrente non è il nodo indicato dall'indirizzo IP originante nel messaggio RREP, il nodo consulta la sua rotta della routing table per l'originator node, per determinare il successivo hop per il pacchetto RREP e poi inoltra il RREP verso l'origine. Se un nodo inoltra un RREP su un link che è unidirezionale, il nodo DOVREBBE richiedere che il destinatario di RREP confermi la ricezione di RREP, inviando indietro un messaggio RREP-ACK.
Quando qualsiasi nodo trasmette un RREP, la precursor list per il nodo di destinazione corrispondente è aggiornata, aggiungendo ad esso il next-hop verso il quale RREP è inoltrato. Inoltre, a ciascun nodo la rotta (inversa), ha il suo Lifetime cambiato, per essere il massimo tra (Lifetime-esistente, (tempo-current + ACTIVE_ROUTE_TIMEOUT). Infine, la precursor list per il successivo hop, verso la destinazione, è aggiornata per contenere il successivo hop.

3.4.9 OPERAZIONE SU LINK UNIDIREZIONALI

È possibile che una trasmissione RREP possa fallire. Per ovviare a tale problema, quando un nodo trova che la sua trasmissione di un messaggio RREP è fallita, esso memorizza il next-hop ,del fallito RREP, in una lista nera. Tali fallimenti possono essere trovati mediante l'assenza di una conferma (ad esempio, RREP-ACK). Un nodo ignora tutti i RREQ ricevuti da qualsiasi nodo nella sua lista nera. I nodi sono rimossi dalla lista nera, dopo un periodo di BLACKLIST_TIMEOUT. Tale periodo dovrebbe essere posto ad un limite superiore di tempo impiegato per eseguire il numero permesso di tentativi di richiesta di rotta.
Il pacchetto RREP-ACK non contiene alcuna informazione su quale RREP sta trasmettendo la conferma.

3.4.10 MESSAGGIO DI HELLO

Un nodo PUO' offrire un'informazione di connessione, trasmettendo messaggi locali di Hello. Un nodo DOVREBBE usare solo messaggi di Hello se è parte di una rotta attiva. Ogni HELLO_INTERVAL millisecondi, il nodo controlla se ha inviato un broadcast (ad esempio, un RREQ) nell'ultimo HELLO_INTERVAL. Se non l'ha fatto, PUO' trasmettere un RREP con TTL = 1, detto messaggio di Hello, con i campi del messaggio RREP posti come segue:

- Indirizzo IP di destinazione l'indirizzo IP del nodo

- Numero di sequenza della destinazione l'ultimo SN
- Numero hop 0
- Lifetime ALLOWED_HELLO_LOSS * HELLO_INTERVAL

Ogni volta che un nodo riceve un messaggio di Hello da un vicino, il nodo DOVREBBE essere sicuro che ha una rotta attiva verso il vicino e crearne una se è necessario. Se una rotta esiste, allora il Lifetime per la rotta dovrebbe essere incrementato, se necessario, per essere almeno ALLOWED_HELLO_LOSS * HELLO_INTERVAL. La rotta verso il vicino, se esiste, DEVE successivamente contenere l'ultimo numero di sequenza della destinazione dal messaggio di Hello.

3.4.11 MESSAGGI DI ROUTE ERROR (RERR)

Di solito, le procedure di errore di rotta e la rottura del link richiedono i seguenti passi:

- invalidazione delle rotte esistenti
- elenco delle destinazioni colpite
- determinazione dei possibili vicini che possono essere colpiti
- consegna di un appropriato RERR per tali vicini

Un messaggio di errore di rotta (RERR) PUO' essere trasmesso sia in modo broadcast (se vi sono molti precursors), sia unicast (se c'è un solo precursore), o iterativamente unicast verso tutti i precursori (se la modalità broadcast non è utilizzata). Un nodo inizia la procedura per un messaggio RERR in tre situazioni:

1. se individua la caduta di un link per un next-hop relativo ad una rotta attiva memorizzata nella routing table
2. se riceve un pacchetto di dati destinato ad un nodo per il quale non si ha una rotta
3. se riceve un RERR da un vicino per una o più rotte attive.

Per il primo caso, inizialmente, il nodo crea una lista delle destinazioni non più raggiungibili a causa del vicino (next-hop verso la destinazione desiderata) non raggiungibile.
Per il secondo caso, c'è solo una destinazione non raggiungibile, che è la destinazione del pacchetto di dati che non può essere consegnato.
Per il terzo caso, la lista dovrebbe comprendere tutte quelle destinazioni per le quali esiste una rotta che utilizza come next-hop il nodo che ha trasmesso il RRER.
Alcune delle destinazioni irraggiungibili nella lista potrebbero essere usate dai nodi vicini e può essere, quindi, necessario inviare un (nuovo) RERR. Il RERR dovrebbe contenere quelle destinazioni, che sono parte della lista, creata, di destinazioni irraggiungibili ed hanno una lista di precursori non vuota.
Il nodo vicino o i nodi vicini che dovrebbero ricevere il RERR sono tutti quelli che appartengono alla lista di precursori di almeno una delle destinazioni non raggiungibili nel RERR nuovamente creato. In caso vi sia solo un unico vicino che ha bisogno di ricevere il RERR, un RERR DOVREBBE essere unicast verso quel vicino. Altrimenti, RERR è di solito inviato

all'indirizzo broadcast locale (IP di destinazione == 255.255.255.255, TTL == 1). Il campo DestCount del pacchetto RERR indica il numero di destinazioni irraggiungibili.
Poco prima di trasmettere il RERR, vengono effettuati aggiornamenti sulla routing table che possono influenzare i SN della destinazione per le destinazioni irraggiungibili. Per ciascuna di queste destinazioni, la corrispondente routing table è aggiornata come segue:

1. il numero di sequenza della destinazione non più raggiungibile presente nella routing table viene incrementato nei i casi 1 e 2 descritti precedentemente oppure copiato dal RERR entrante nel caso 3;
2. la rotta viene invalidata;
3. il campo Lifetime è aggiornato al tempo corrente più il DELETE_PERIOD. Prima di questo tempo, l'entrata NON DOVREBBE essere cancellata.

Si può notare che il campo Lifetime nella tabella di routing gioca un doppio ruolo – per una rotta attiva è il tempo di decadenza e per una rotta invalida è il tempo di cancellazione. Se un pacchetto di dati è ricevuto per una rotta invalida, il campo Lifetime è aggiornato al tempo corrente più il DELETE_PERIOD.

3.4.12 AODV ADAPTIVE FLOODING (AODV-AF)

L'AODV adaptive-floading è stato sviluppato con lo scopo di ridurre il flooding dei messaggi di controllo nella rete con l'aspettativa di ottenere un aumento del packets-rate RX/TX ed un aumento della durata media della batteria in ciascun nodo. Di conseguenza, a differenza di quanto avviene nel semplice AODV, il nodo non ritrasmetterà sempre il pacchetto RREQ. L'AODV AF si basa sul concetto di probabilità e sul ruolo (passato) assunto da ciascun nodo nelle trasmissioni precedenti di RREQ tra una determinata coppia sorgente-destinazione.
Durante la simulazione ogni nodo memorizza il numero di pacchetti RREP e RREQ relativi alla coppia originator-destination.
Ogni volta che un nodo riceve un pacchetto di RREQ, se la rotta per la destinazione non è conosciuta, esso ritrasmetterà il pacchetto di RREQ con una probabilità:

$$P_{ToT}(t) = P_N(t) * P_S(t) *\ldots* P_O(t)$$

N : id del host corrente
S : id del host sorgente
O : id del host originator

La probabilità $P_N(t)$ è legata al prodotto delle probabilità $P_S(t-1)$ ed $P_N(t-1)$:

$$P_N(t) = P_S(t-1) * P_N(t-1)$$

- $P_S(t-1)$ è riferita al nodo **sorgente** dal quale è arrivato il pacchetto di RREQ e deriva dall'inverso del rapporto tra il numero di RREP ed RREQ memorizzati fino a quel momento e relativi alla specifica coppia originator-destination
- $P_N(t-1)$ è riferita al nodo **ricevente** il pacchetto di RREQ e deriva dall'inverso del rapporto tra il numero di RREP ed RREQ memorizzati fino a quel momento e relativi alla specifica coppia originator-destination

La tecnica descritta prende il nome di AODV-AF con probabilità doppia.

Di conseguenza, la probabilità $P_N(t)$ originerà un sottoinsieme di nodi costituito da tutti quelli con la più alta probabilità di ritrasmissione del RREQ's packet. La dimensione del sottoinsieme varierà dinamicamente all'aumentare del tempo di simulazione.

In sistemi "high reliability" è possibile ridurre l'espressione precedente ed esplicarla con la seguente formula:

$$P_N(t) = P_S(t-1)$$

Questa tecnica prende il nome di AODV-AF con probabilità singola.

Teoricamente, il trade-off tra le due differenti tecniche comporta un aumento del "ratio RX/TX" ad una diminuzione della "fault tollerance" del sistema, secondo una logica di proporzionalità inversa.

In un contesto nel quale il risparmio energetico risulta essere il vincolo primario per una WSN, è stata apportata una modifica all' AODV-AF con lo scopo di ridurre la varianza del livello di batteria residuo di ciascun nodo rispetto alla media di tutti i nodi.
Di conseguenza la formula adottata per la ritrasmissione dei RREQ è stata rielaborata per un utilizzo più efficiente della batteria di ogni singolo nodo.

$$P_N(t) = P_S(t-1) * P_N(t-1) * P_B(t)$$

Dove $P_B(t)$ rappresenta il rapporto tra il livello di batteria residua ed il livello di batteria iniziale.

4 OMNeT++

OMNeT++ è un framework di simulazione ad eventi discreti orientato alle reti. OMNeT++ è scritto in c++ ed è public-source. Di conseguenza, grazie anche alla sua struttura modulare, è particolarmente adatto per la simulazione di reti di sensori wireless. Una relativa facilità nell'utilizzo di OMNeT++ viene raggiunta attraverso l'ausilio di un linguaggio addizionale NED mirato alla configurazione della simulazione.
In questa tesi viene proposto un modello di simulazione inerente allo standard IEEE802.15.4 con protocollo di routing AODV (Ad-hoc On-demand Distance Vector). Di conseguenza, mentre l'implementazione dello strato fisico e MAC comporta l'osservanza delle specifiche descritte nello standard IEEE802.15.4, l'implementazione dello strato di rete porta a considerare le specifiche apportate nel draft ufficiale della NOKIA riguardante il protocollo di routing AODV.
Per la costruzione dell'intera rete si è utilizzato il modello IEEE 802.15.4 sviluppato dal Department of Computer Science 7 presso the University of Erlangen-Nürnberg to Germany.
Questo modello è stato sviluppato nell'INET framework di OMNeT++. L'architettura del modello è mostrata nella seguente figura.

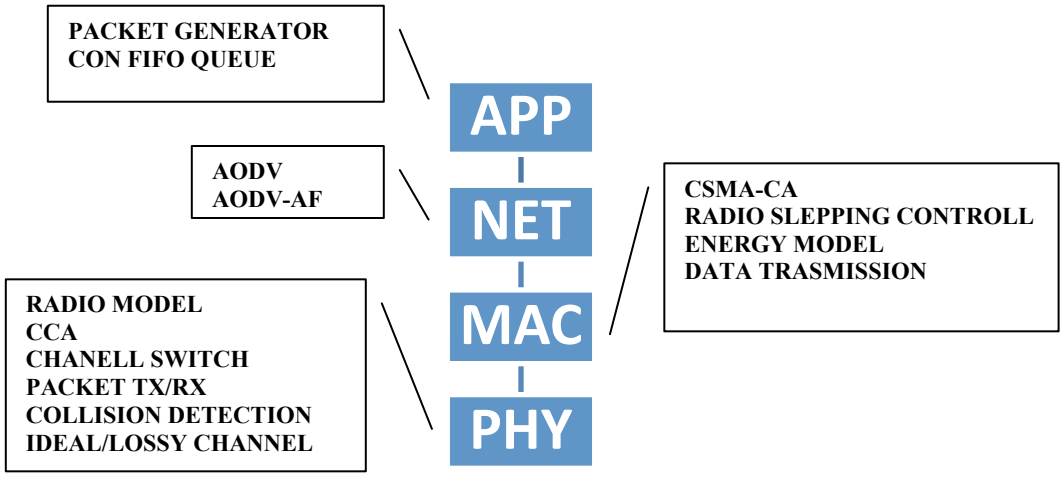


Figure 34 – Struttura e componenti del OMNET++ model

La struttura è composta da 3 sub modeles (c++) indipendenti: traffic, MAC e PHY. Il sub module "traffic" è stato re-implementato per contenere il protocollo di routing AODV. I moduli sono connessi tra loro via gates e comunicano tramite messaggi. La seguente figura mostra uno snapshot del modello nell'interfaccia grafica di OMNeT++ chiamata Tkenv.

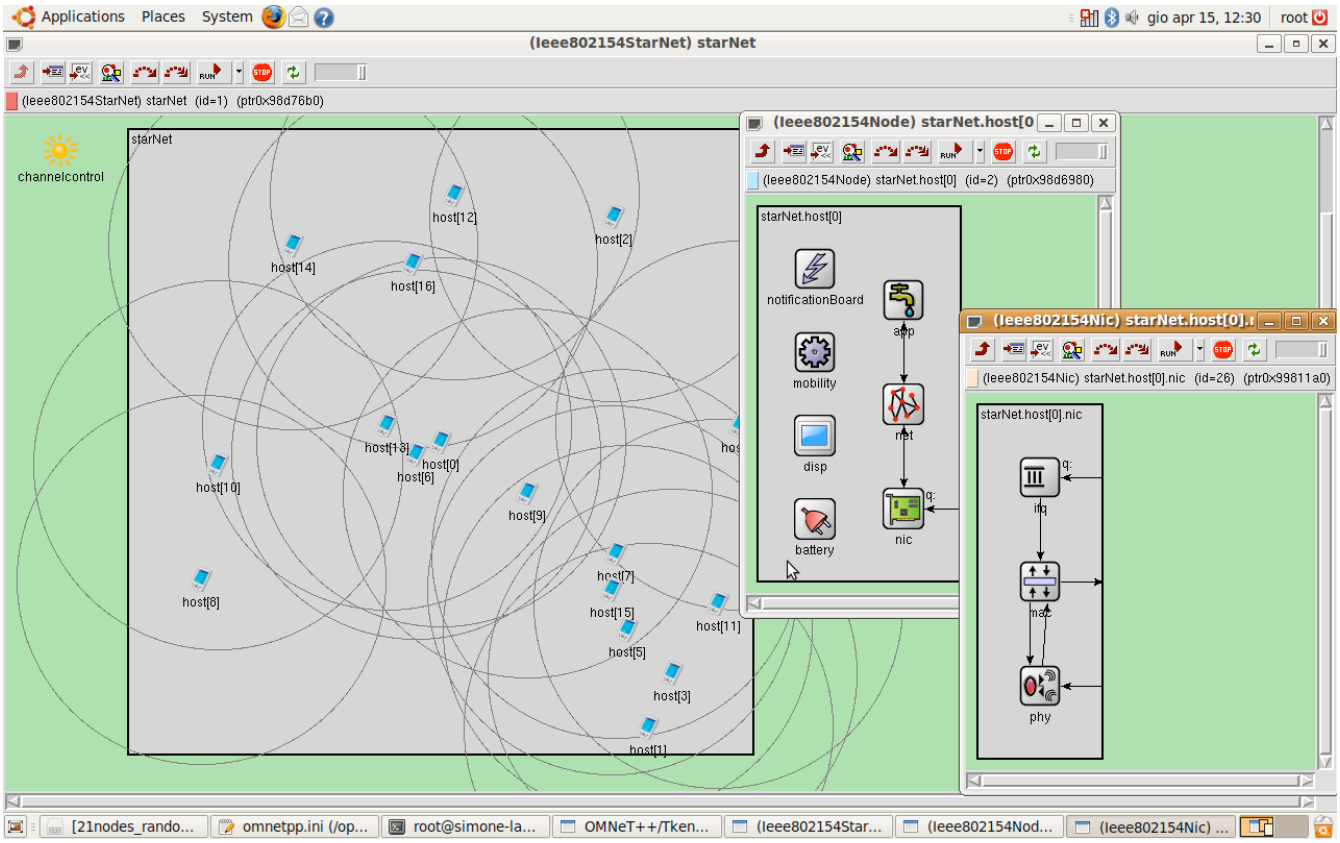


Figure 35 – OMNET++ MODEL

Di conseguenza il lavoro consiste nell'implementazione del protocollo di routing AODV (network level) e dell'integrazione di esso con gli strati inferiori. La riuscita del funzionamento dell'intera rete ha permesso, in un secondo momento, di studiare e sviluppare una modifica adaptive-flooding da apportare all'algoritmo di routing (AODV) sviluppato in precedenza. Gli indicatori presi in considerazione per lo studio dell'AODV-AF riguardano il rapporto RX packet su TX packet ed il valore del livello della batteria residua relativa ai diversi nodi. Per ottenere una visione complessiva su un possibile aumento delle performance sull'intera rete sono state ottenute diverse istanze di simulazione al variare del numero di nodi della rete.

4.1 PHY MODULE

Nell'INET framework, un general radio module chiamato AbstractRadio implementa le comuni funzioni della radio: packet trasmission, peacket reception con collision detection, channel switch, etc… Questo modello è stato modificato per creare un modello di radio conforme allo standard IEEE802.15.4 attraverso la modifica o l'aggiunta dei seguenti contenuti:

- Ridefinizione degli stati radio:
  in accordo alle specifiche, la radio è stata modellata con 3 stati: trasceiver disabile (TRX_OFF), trasmitter enabled (TX_ON) e receiver enabled (RX_ON). Il MAC module interagisce con il PHY module ed opera il rapid-changing

tra i diversi stati attraverso delle primitive di richiesta. Il PHY module riporta il risultato del setting al MAC attraverso delle primitive di conferma

- Clear channel access (CCA):
  Il MAC module richiede un CCA al PHY attraverso la primitiva di richiesta PLME-CCA. Lo stato del canale (occupato o libero) viene controllato attraverso la lettura di due flags: isRxing e isTxing. Questi flags indicano se la radio si trova nello stato di ricezione o trasmissione. Il PHY riporta il risultato del CCA al MAC attraverso una primitiva di conferma.

4.2 MAC MODULE

Il modulo MAC contiene due parti principali: channel access e Energy model.

4.2.1 CHANNEL ACCESS

Il channel access rappresenta la parte principale di ogni protocollo MAC. Nel channel access sono state implementate la maggior parte delle funzioni e primitive definite nelle specifiche. La funzione principale riguarda l'implementazione del CSMA-CA (Carrier Sensing Multiple Access con Collision Avoidance).

4.2.2 ENERGY MODEL

Il consumo di energia ha un ruolo fondamentale nello standard IEEE802.15.4. In questo modello viene misurata la sola energia consumata dalla radio. Per ottenere le misurazioni viene tenuta traccia del corrente stato della radio nel PHY module attraverso un inter-module aggiuntivo chiamato NotificationBoard. Di conseguenza viene calcolato l'intervallo di tempo per il quale la radio mantiene un certo stato.

4.3 NET MODULE

Il net module non rappresenta una specifica del'IEEE802.15.4 ed inizialmente era stato fornito di un semplice star routing (con coordinator). Successivamente è stato eliminato lo star routing ed è stato implementato un mesh routing con protocollo AODV. Anche in questo sono state implementate la maggior parte delle funzioni specificate nel draft ufficiale. Una successiva modifica adaptive-flooding è stata apportata al protocollo AODV.

4.4 TRAFFIC MODULE

Il traffic module è stato implementato da Dietrich Isabel e supporta diversi tipi di generazione di traffico. La tipologia di traffico apportata a questo modello rispecchia una distribuzione uniforme.

4.5 AODV ANALYSIS

Lo studio delle performance dell'AODV-AF è stato condotto attraverso i seguenti test :

- Packet delivery ratio (RX/TX)
- Residual battery
- Media hops

Tutte le simulazioni sono state impostate con i seguenti parametri:

- Map size: 600m x 600m
- Host's number: 17-22-27
- Inter-departure time: 5 s
- Lenght-data: 10 byte
- Destination: uniform

PHY layer parameters:

- Trasmitter Power: 1.0 mW
- Sensitivity: -85 dBm
- Path loss alpha ($P(d) = P(d0) - 10\alpha \log10(d/d0)$ [dBm]): 2 (senza fading)
- Thermal Noise: -110 dBm
- Signal-to-Noise and Interference Ratio (SNIR): 4 dB
- Carrier frequency: 2.4 Ghz
- Channel number: 11 (channel 0: 20 Kb/s, channel 1-10: 40 Kb/s, channel 11-26 : 250 Kb/s)

Battery parameters:

- Battery capacity: 25 mAh
- Usage radio idle: 1.38 mA
- Usage radio transmitter: 9.6 mA
- Usage radio sleep: 0.06 mA

Ogni simulazione è stata eseguita per tre differenti scenari: 17 nodi, 22 nodi, 27 nodi. Di conseguenza è stato fatto variare il numero di nodi mantenendo costante la map-size.

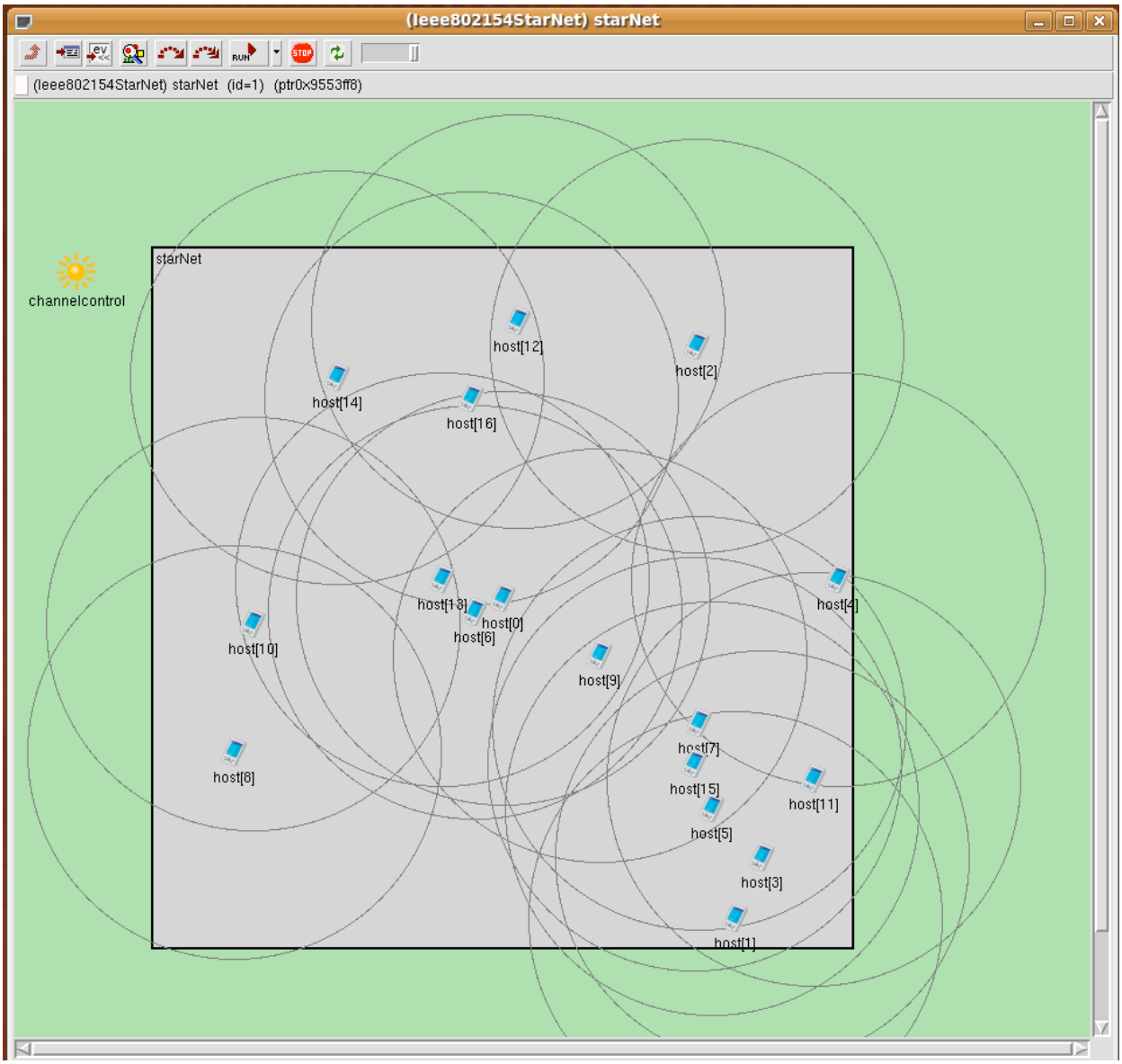


Figure 36 – SCENARIO CON 17 NODI

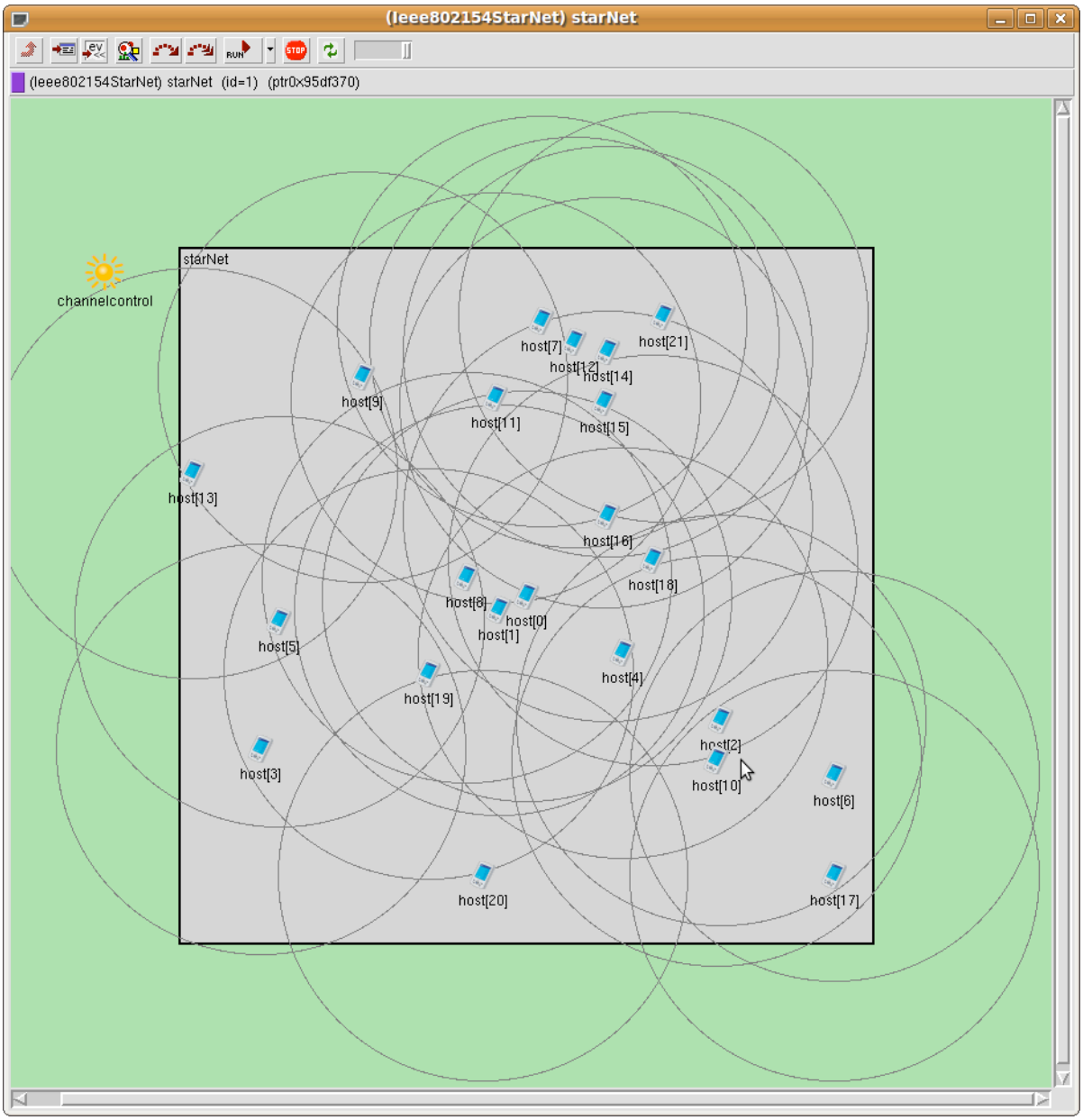


Figure 37 – SCENARIO CON 22 NODI

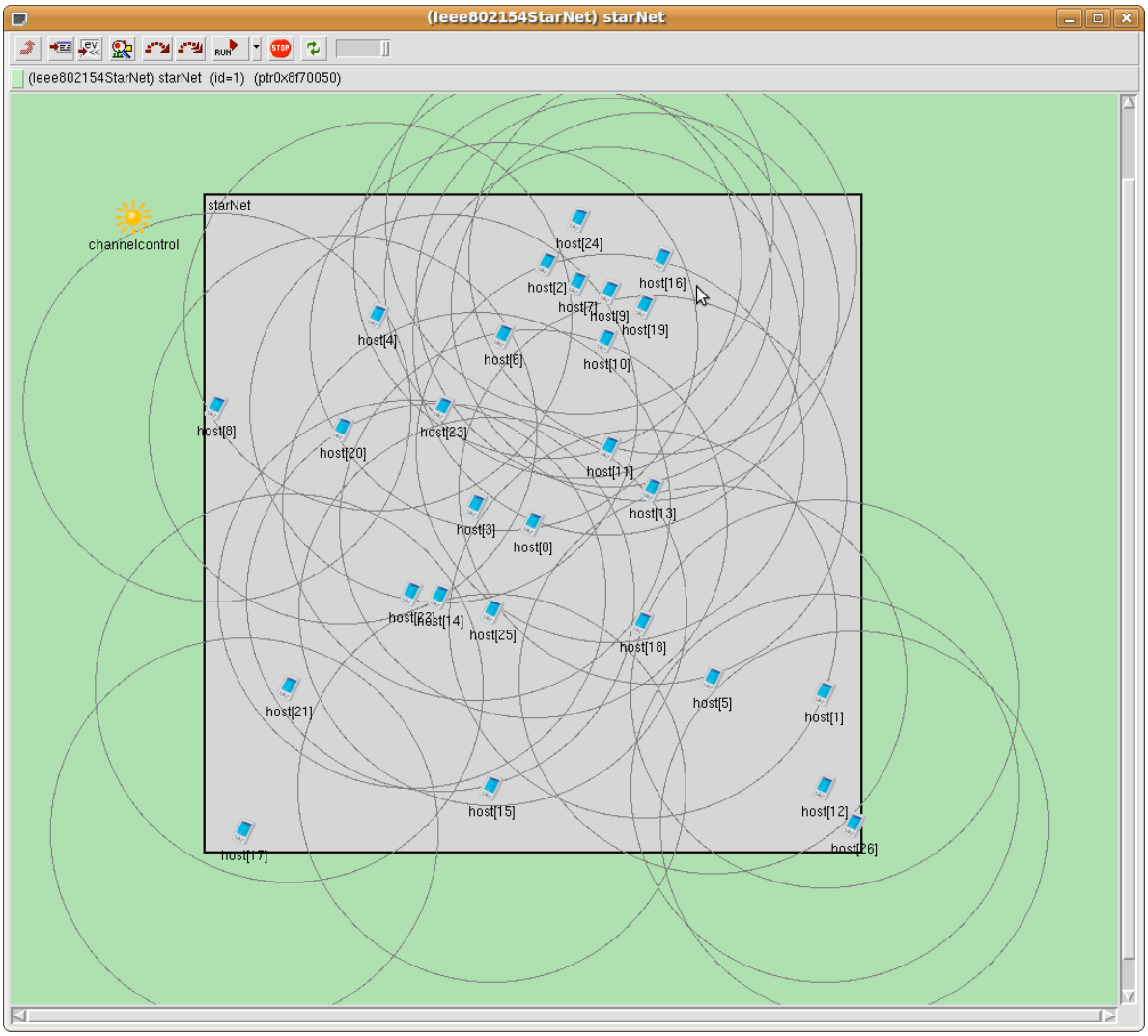


Figure 38 – SCENARIO CON 27 NODI

4.5.1 PACKET DELIVERY RATIO (RX/TX) E RESIDUAL BATTERY IN AODV E AODV-AF CON DESTINAZIONI UNIFORMI

Il Packet delivery ratio è il rapporto tra il numero di pacchetti dati ricevuti e il numero di pacchetti dati trasmessi.
I grafici sottostanti riportano il packet delivery ratio al variare del tempo di simulazione per le diverse tipologie di rete. Di seguito vengono riportati i due grafici inerenti alle due diverse tipologie di routing: AODV e AODV-AF.

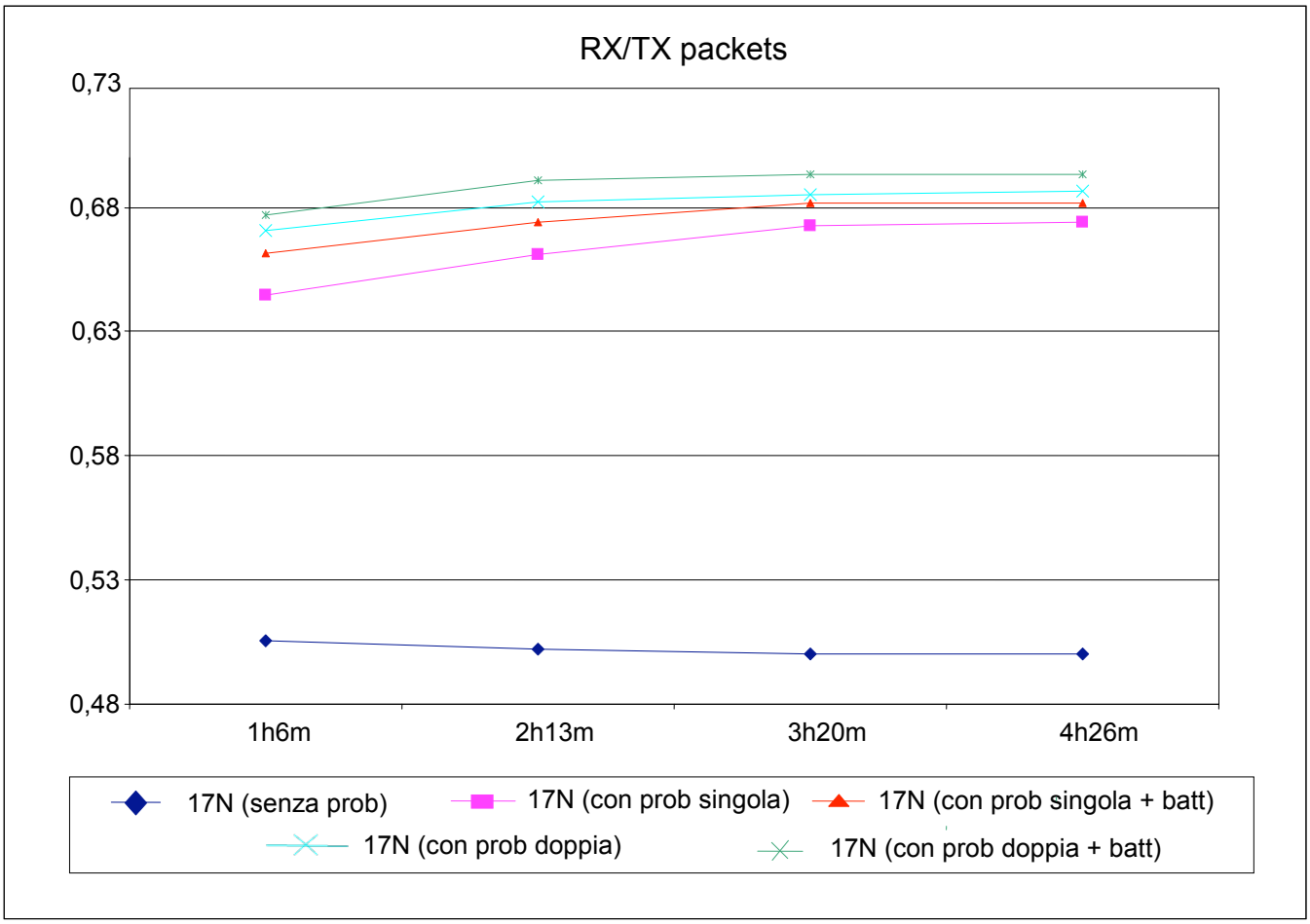


Figure 39 – 17 Nodi (dest uniform)

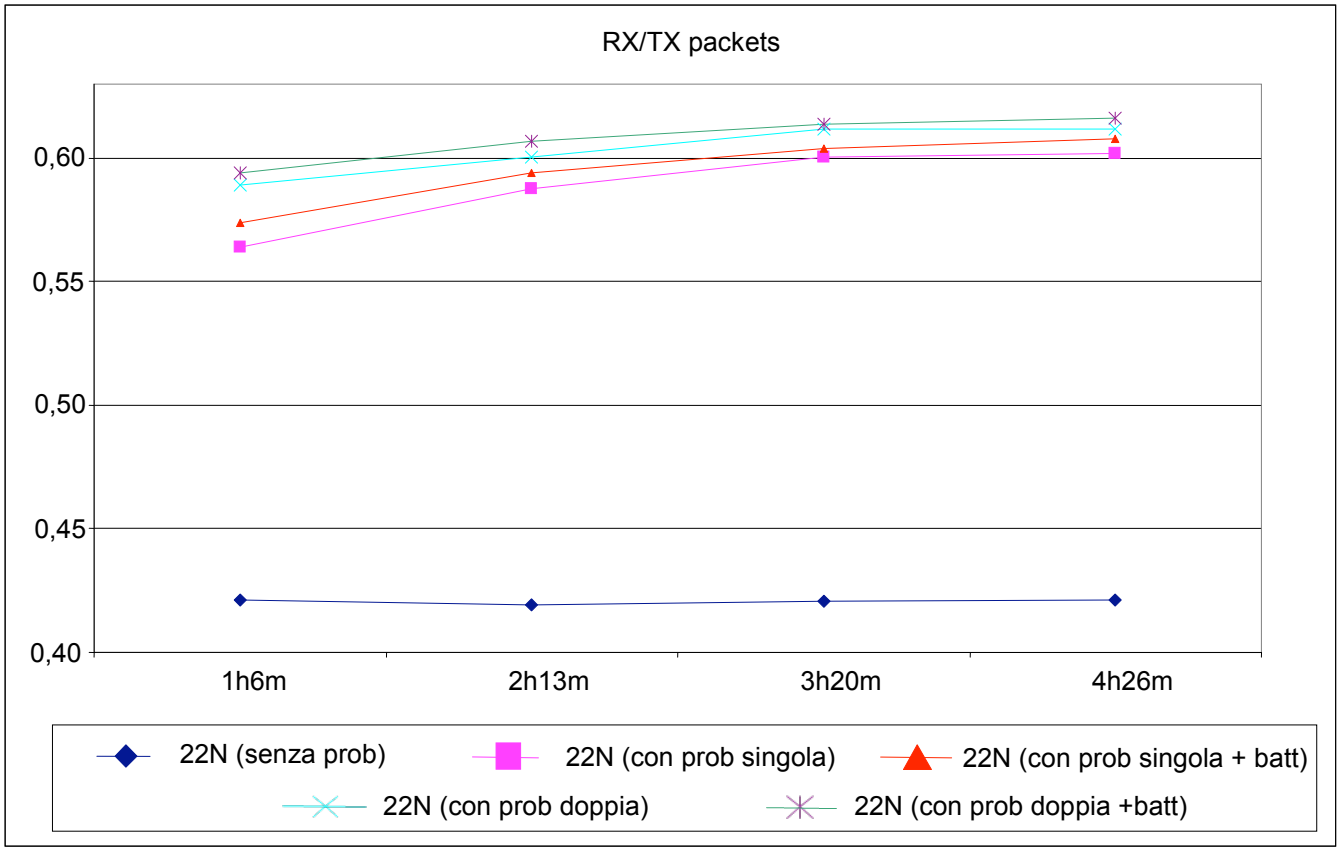


Figure 40 – 22 Nodi (dest uniform)

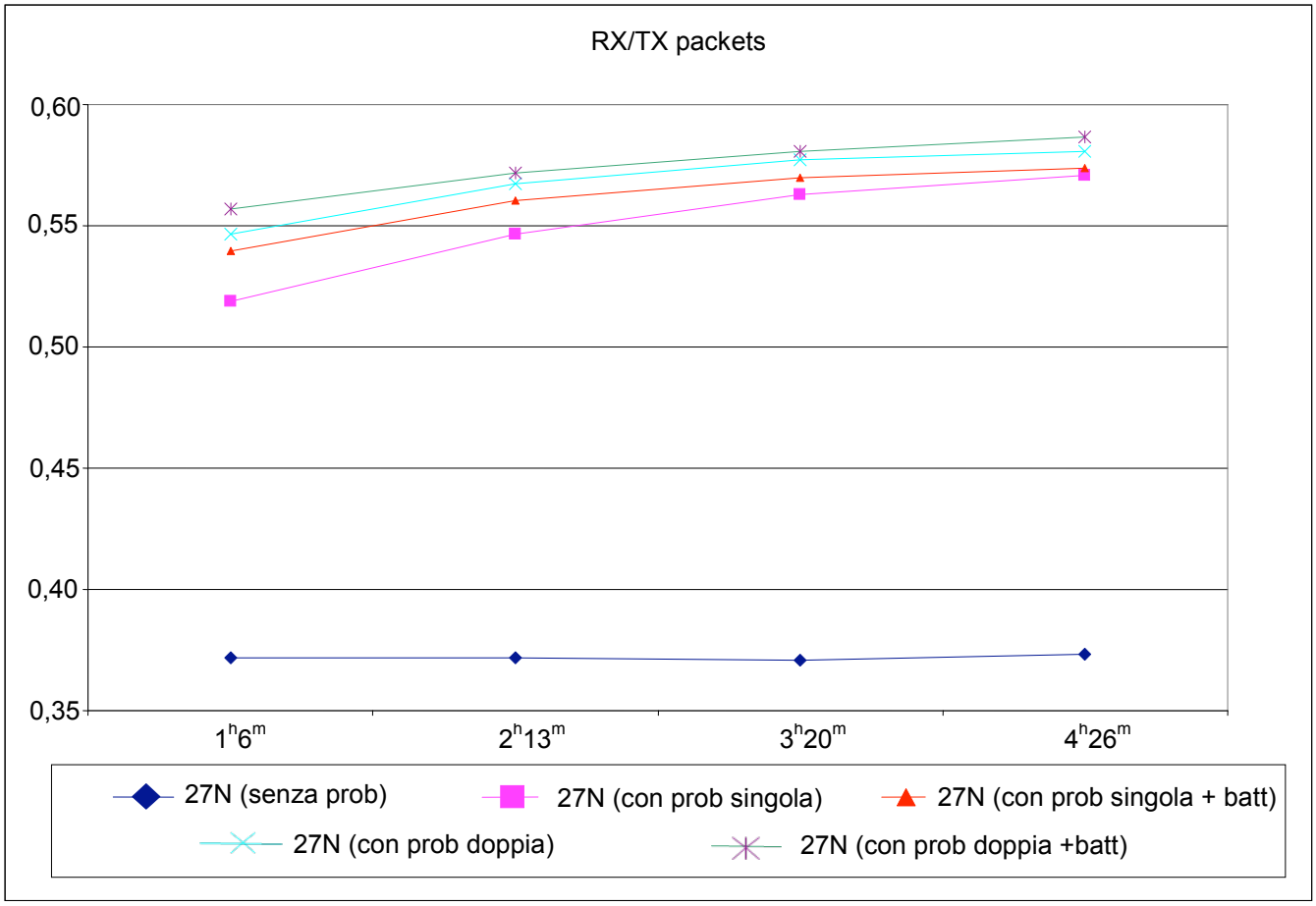


Figure 41 – 27 Nodi (dest uniform)

Il residual battery rispecchia il relativo decremento del livello della batteria al variare del tempo di simulazione per diverse tipologie di rete.

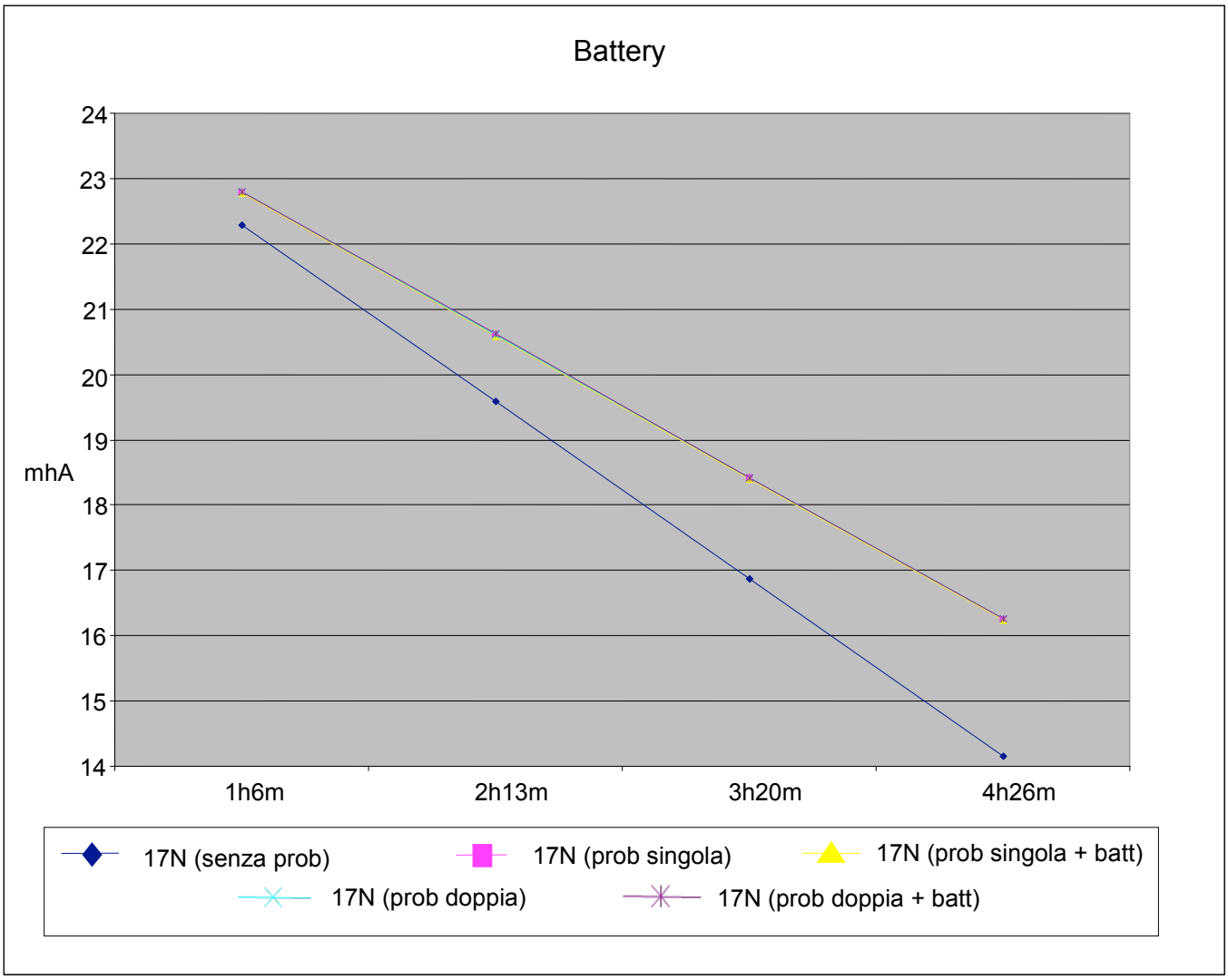


Figure 42 – 17 Nodi (dest uniform)

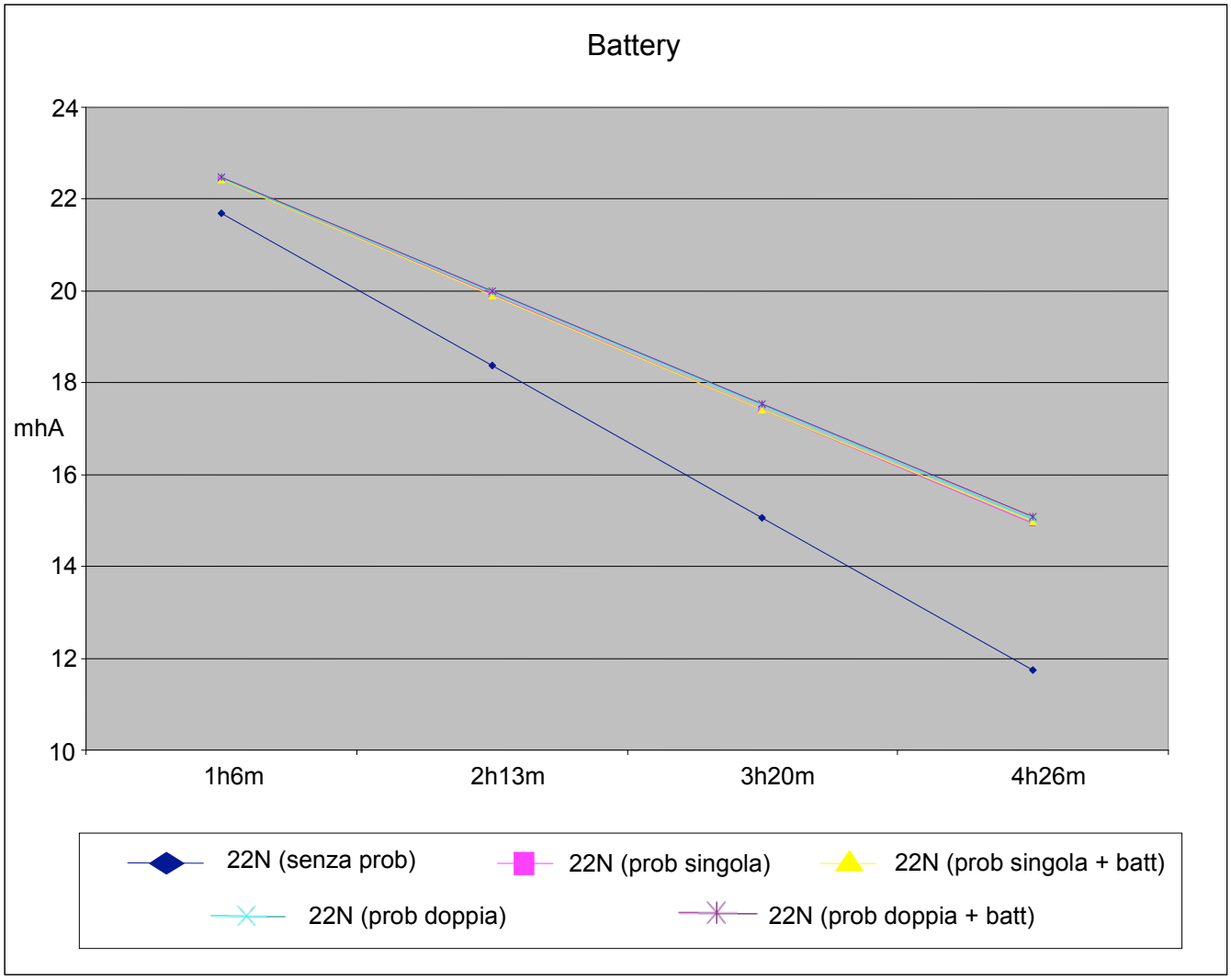


Figure 43 – 22 Nodi (dest uniform)

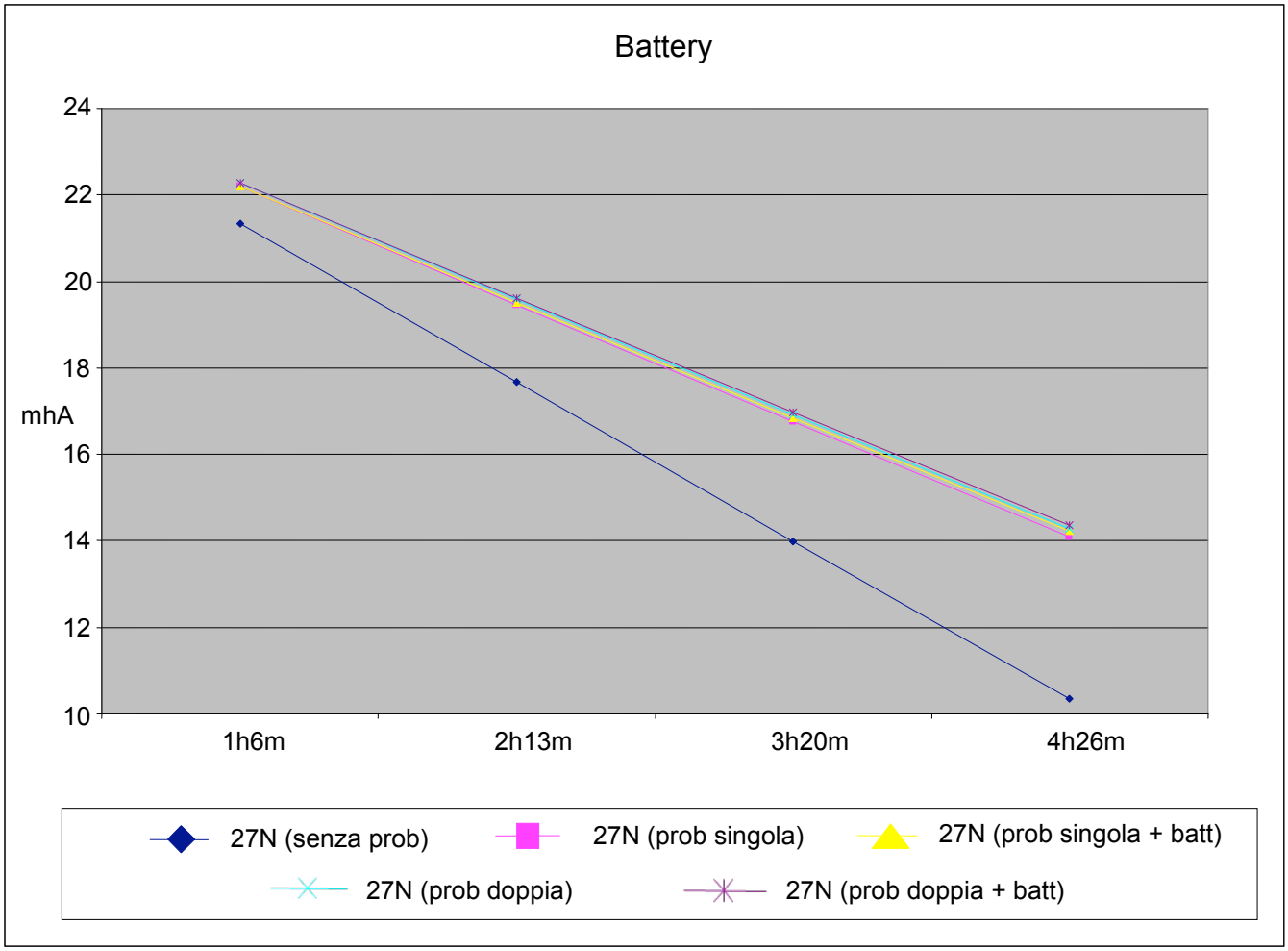


Figure 44 – 27 Nodi (dest uniform)

4.5.2 PACKET DELIVERY RATIO (RX/TX) E RESIDUAL BATTERY IN AODV E AODV-AF CON SINGOLA DESTINAZIONE

Le simulazioni eseguite con destinazioni uniformi sono state replicate con una singola destinazione per ricreare la situazione in cui ci sia un gateway nella rete.

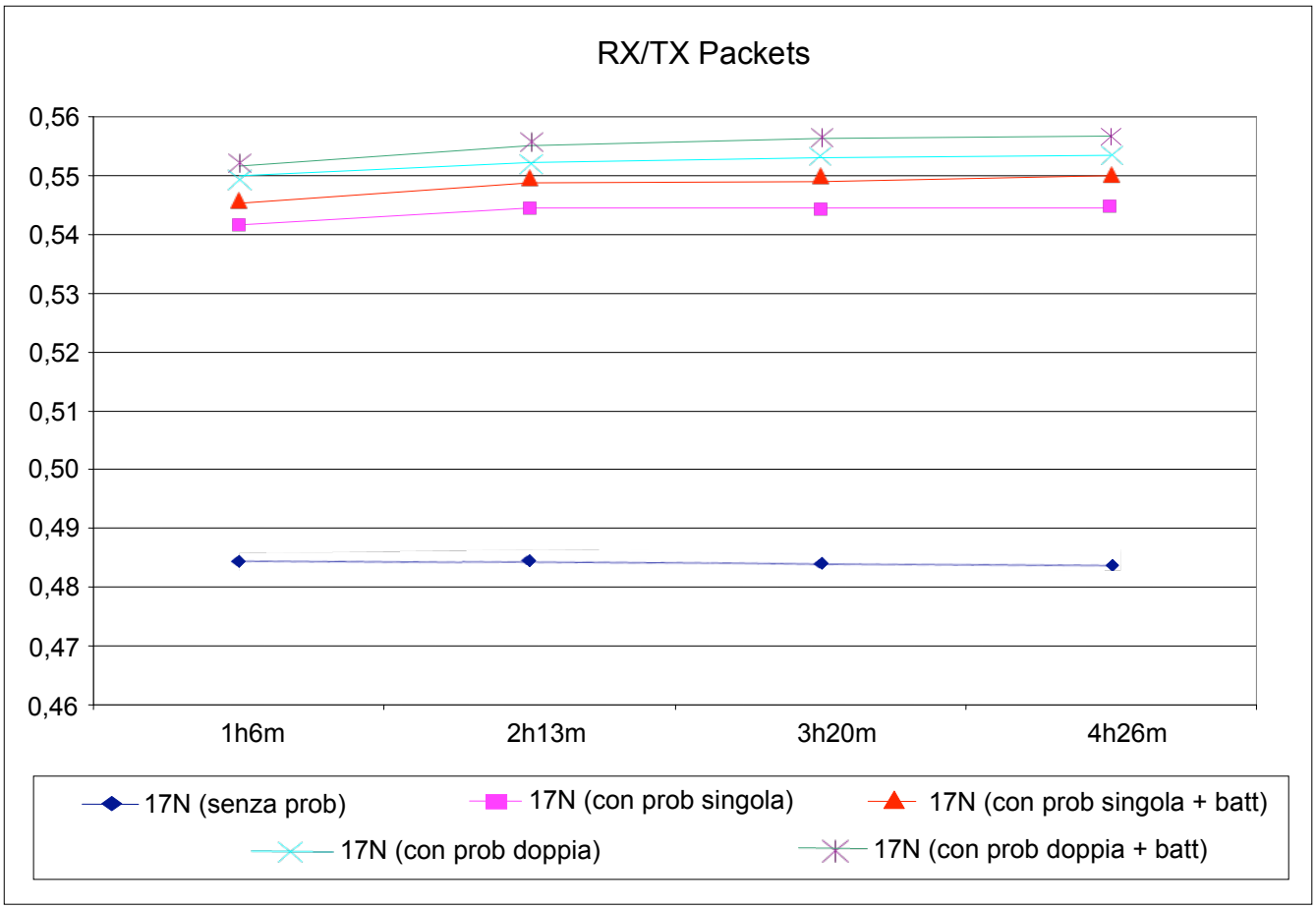


Figure 45 – 17 Nodi (dest singola)

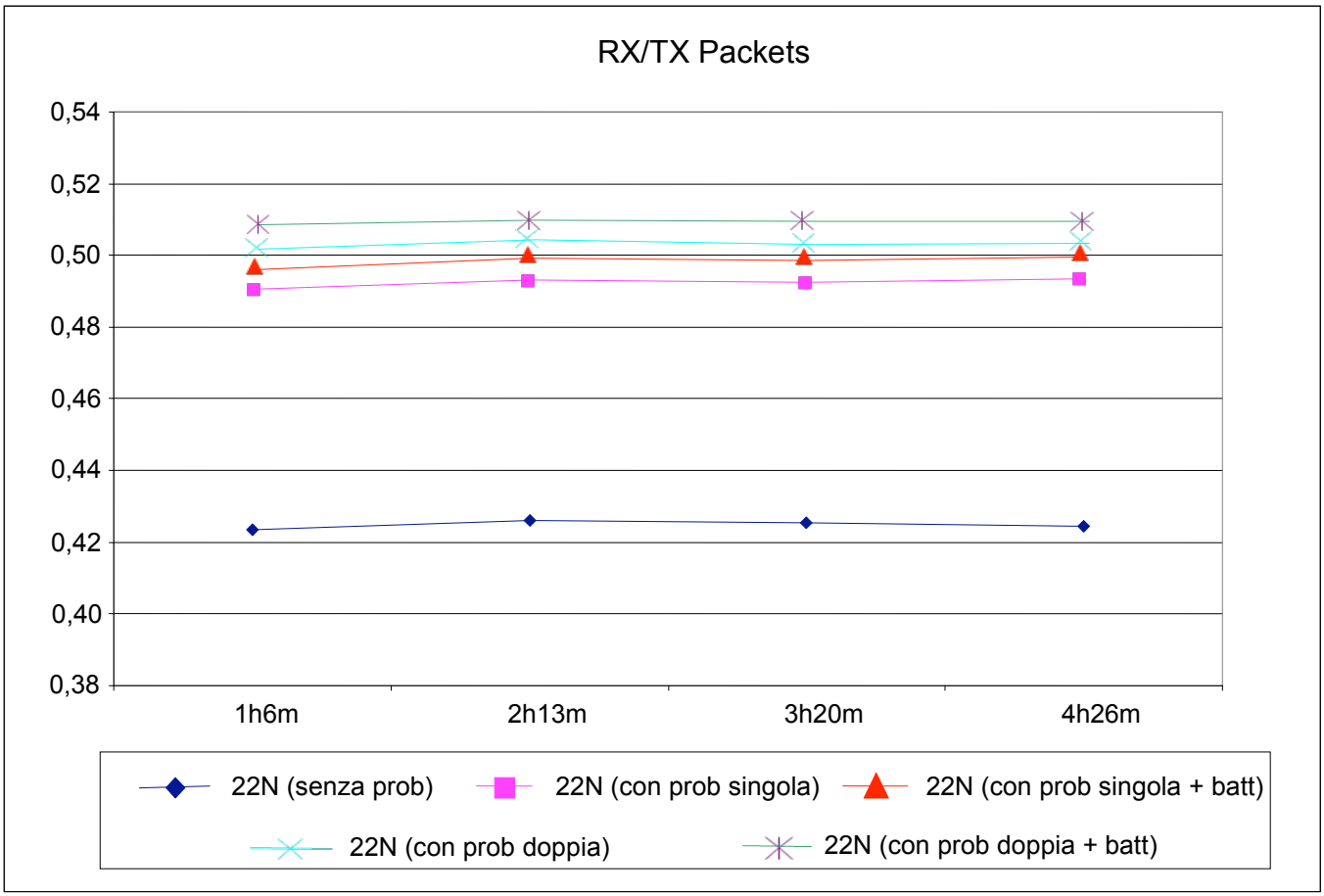


Figure 46 – 22 Nodi (dest singola)

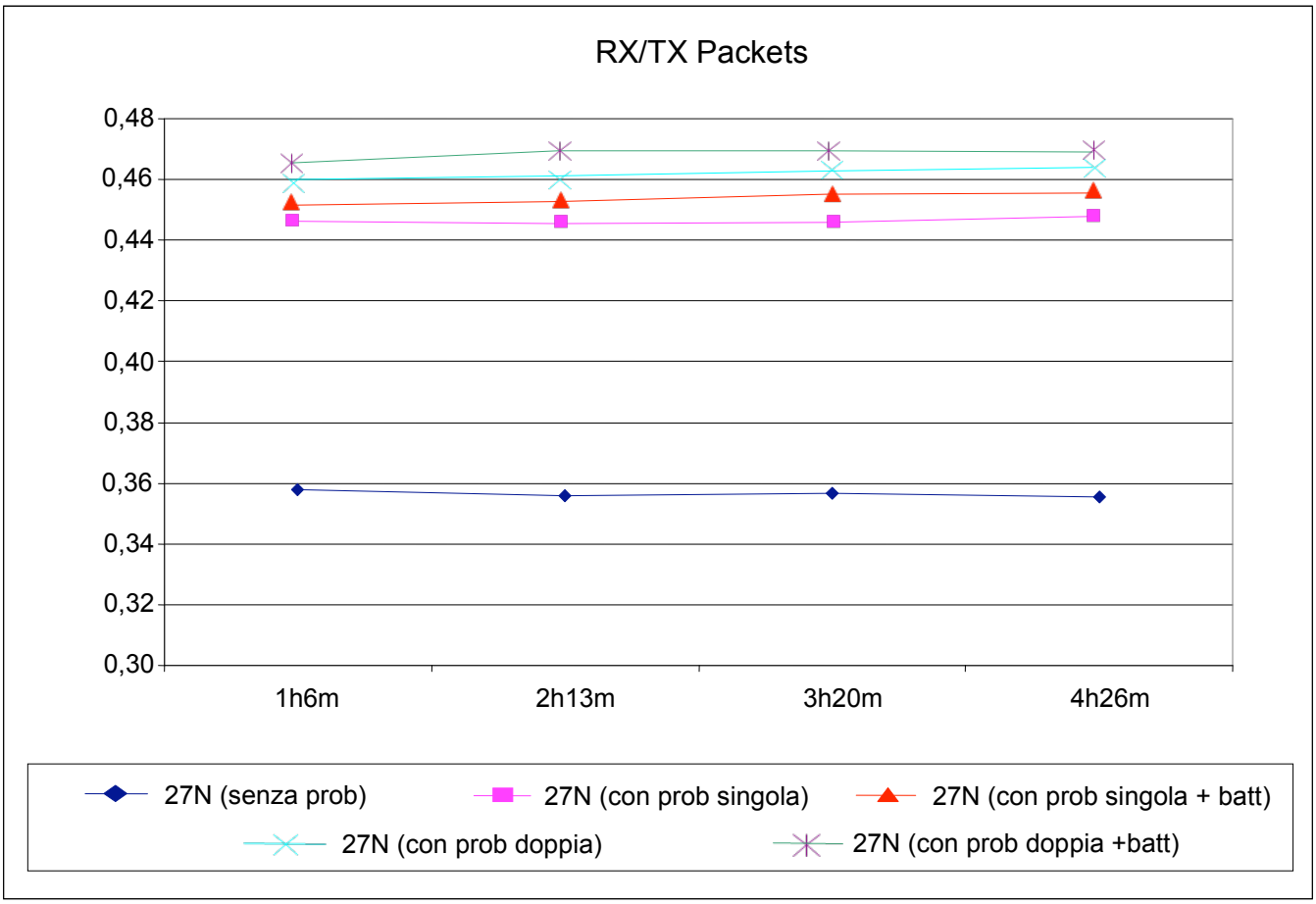


Figure 47 – 27 Nodi (dest singola)

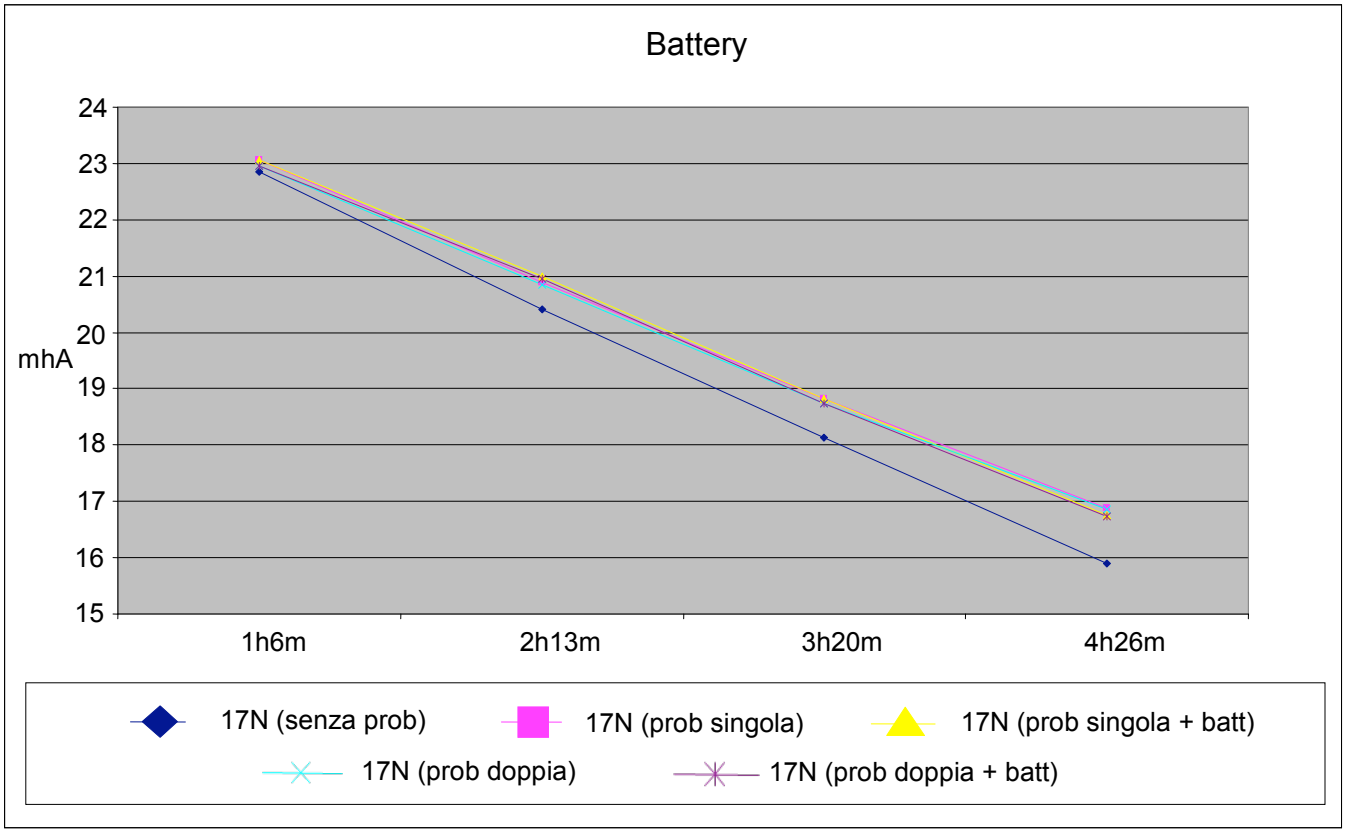


Figure 48 – 17 Nodi (dest singola)

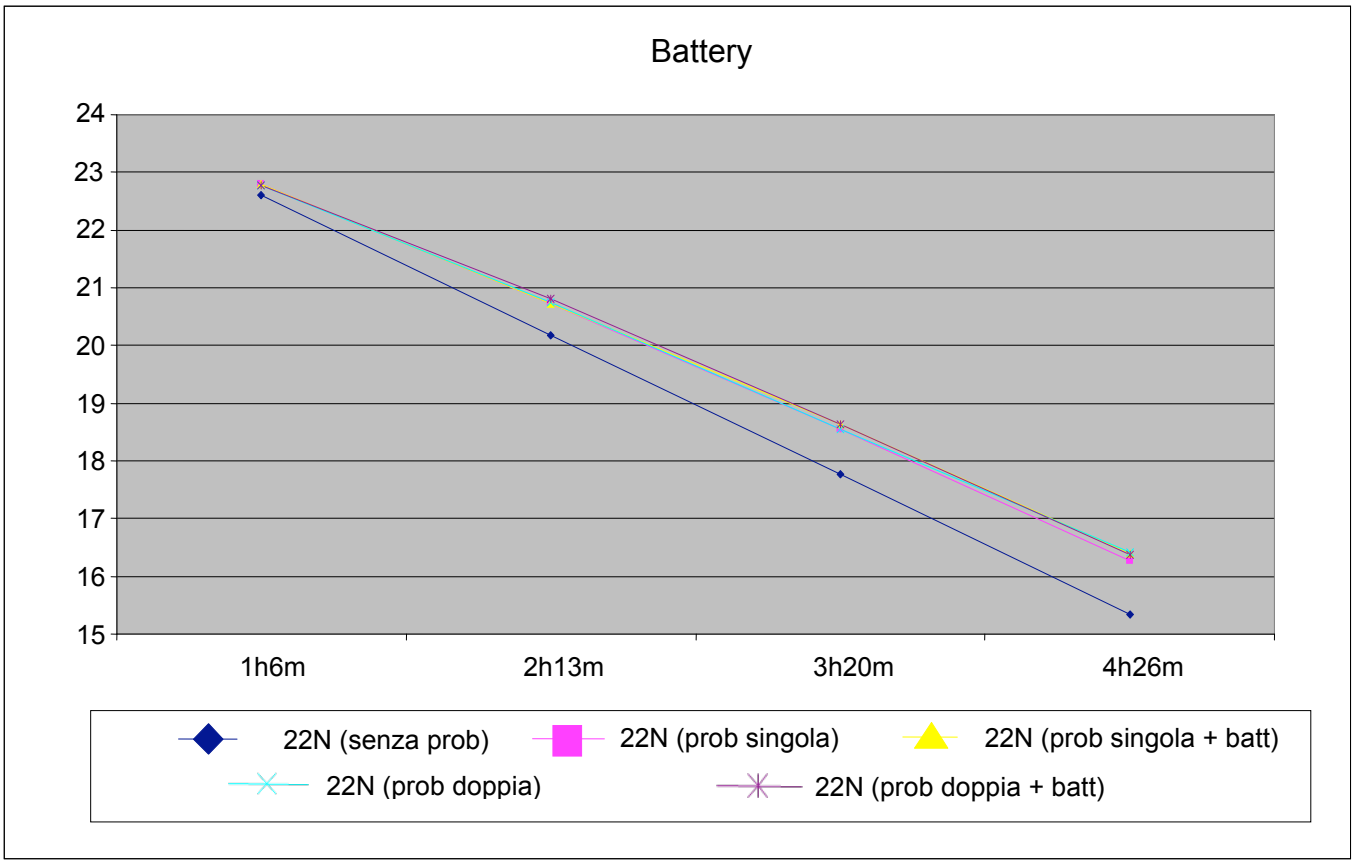


Figure 49 – 22 Nodi (dest singola)

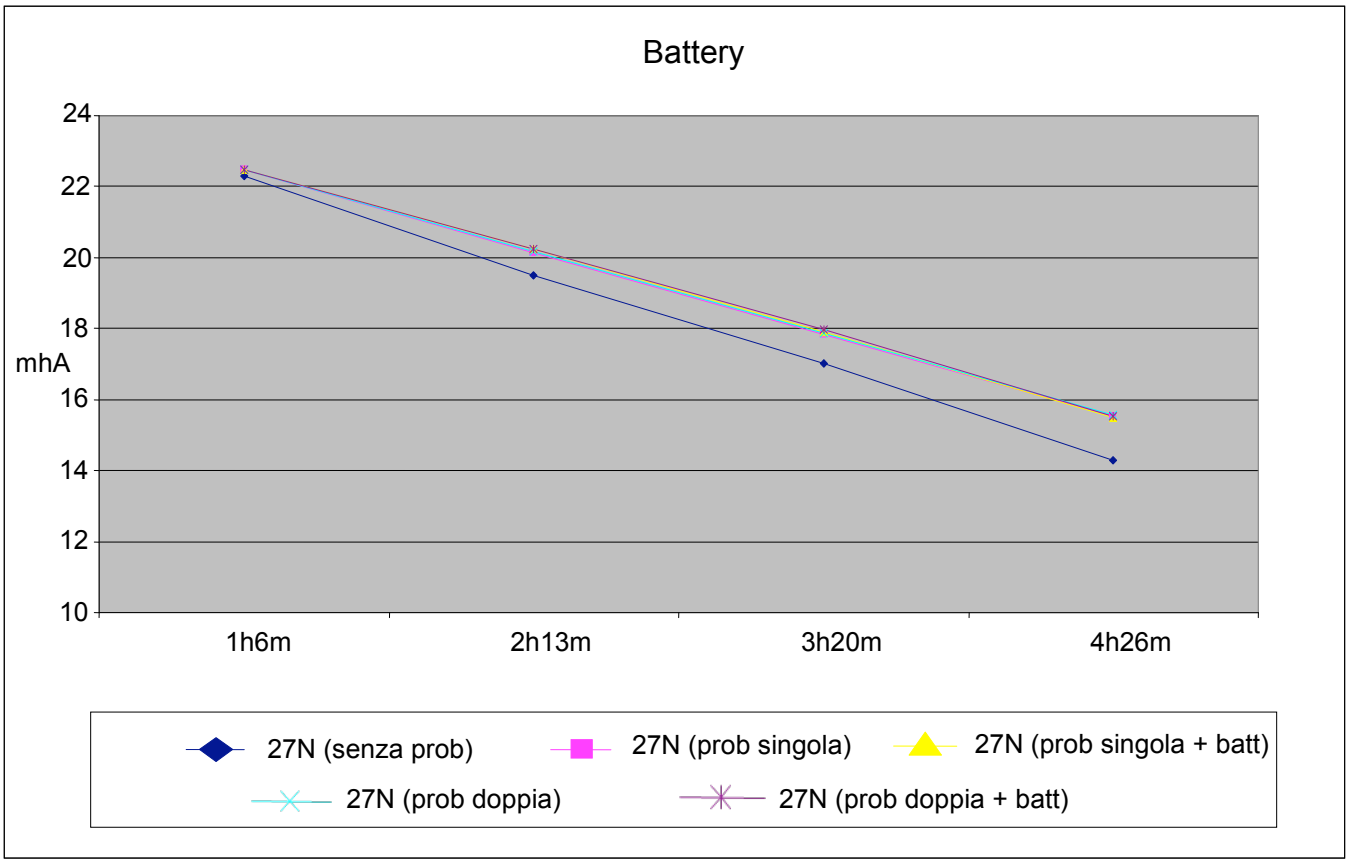


Figure 50 – 27 Nodi (dest singola)

4.5.3 DIFFERENTI TECNICHE AODV

Questa ulteriore analisi ha lo scopo di osservare le differenze tra le due tecniche AODV-AF con e senza contributo della batteria. Per effettuare questa analisi è stato fissato un istante di tempo a $4^{h}26^{m}$ ed è stata considerata una singola destinazione.

Le analisi sono state effettuate osservando il grafico raffigurante la media degli hops ed il grafico rappresentativo del livello di batteria di ogni host. I valori riportati in entrambi i grafici si riferiscono alle differenti tecniche AODV-AF(con e senza contributo della batteria) per ogni scenario di riferimento(17N, 22N, 27N) .

In questi termini, a parità del numero di hops, si rileva un miglioramento delle prestazioni in termini di varianza per le configurazioni che utilizzano una tecnica AODV-AF con contributo della batteria.

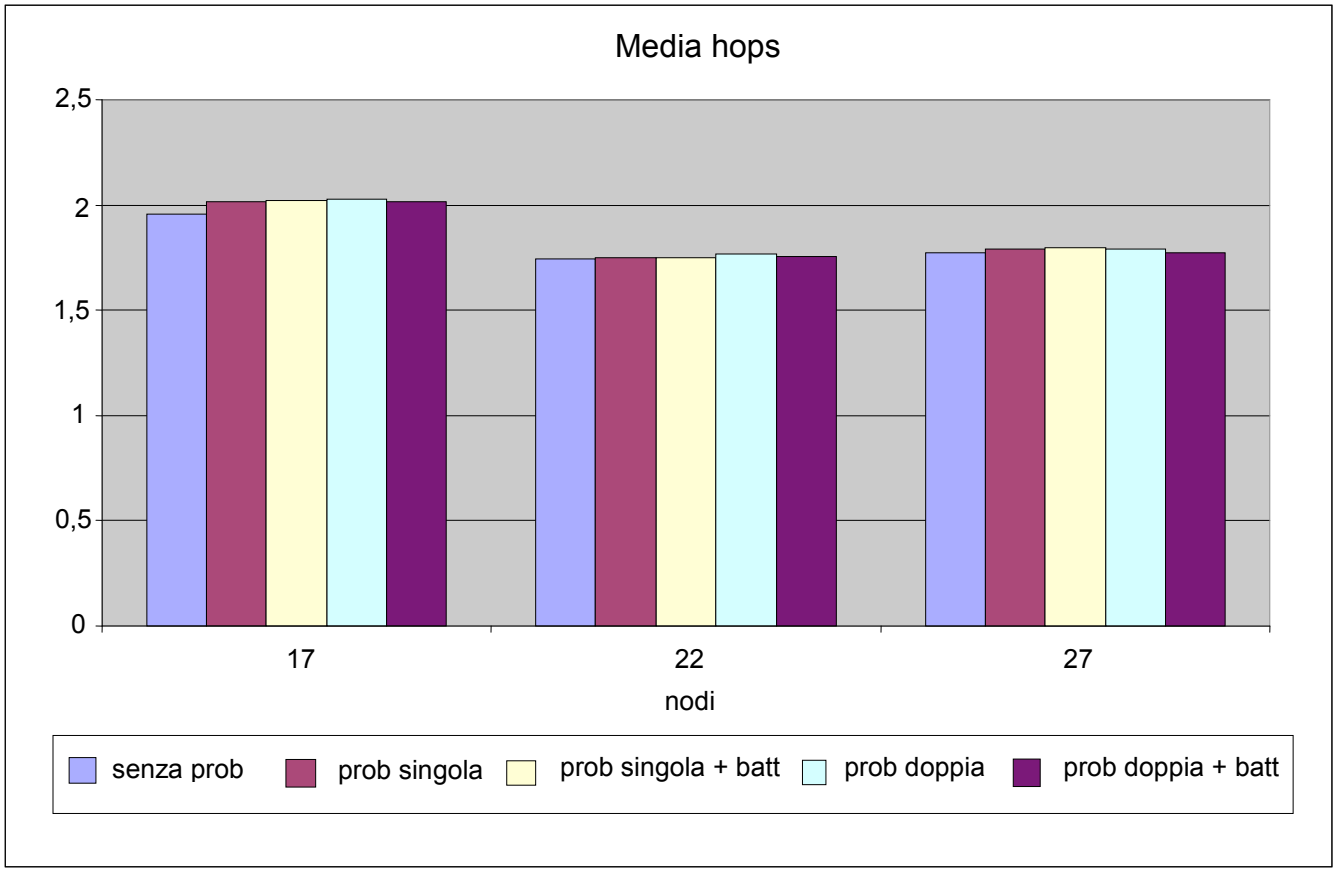


Figure 51 – Media hops (dest singola)

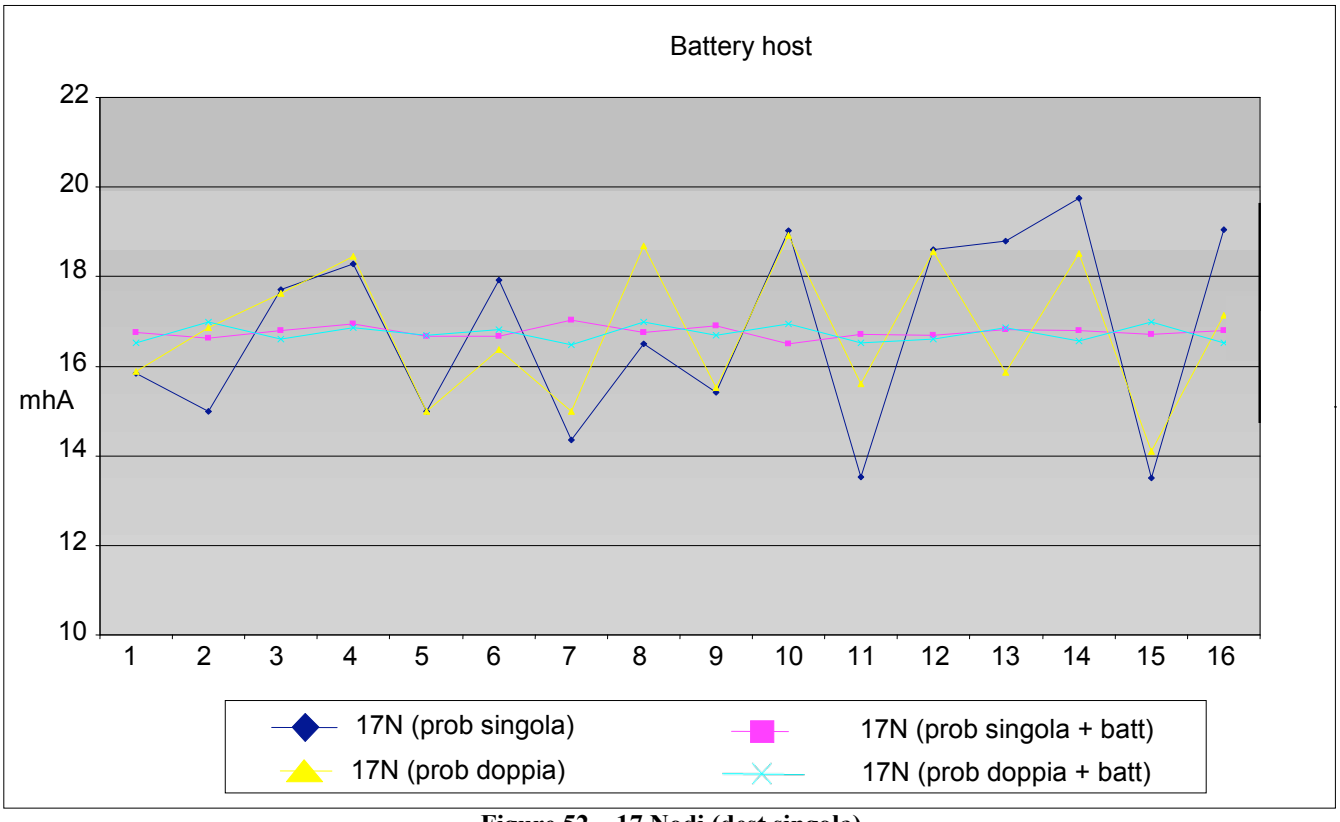


Figure 52 – 17 Nodi (dest singola)

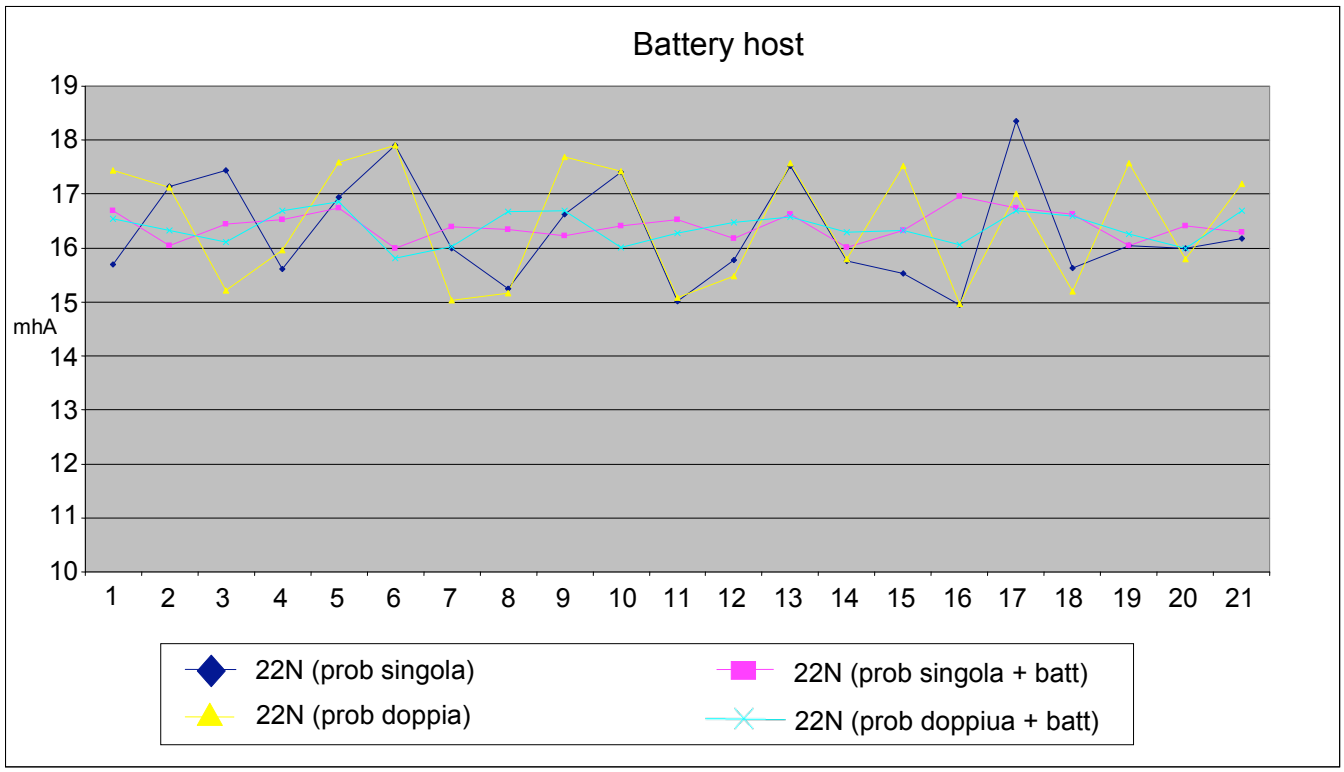


Figure 53 – 22 Nodi (dest singola)

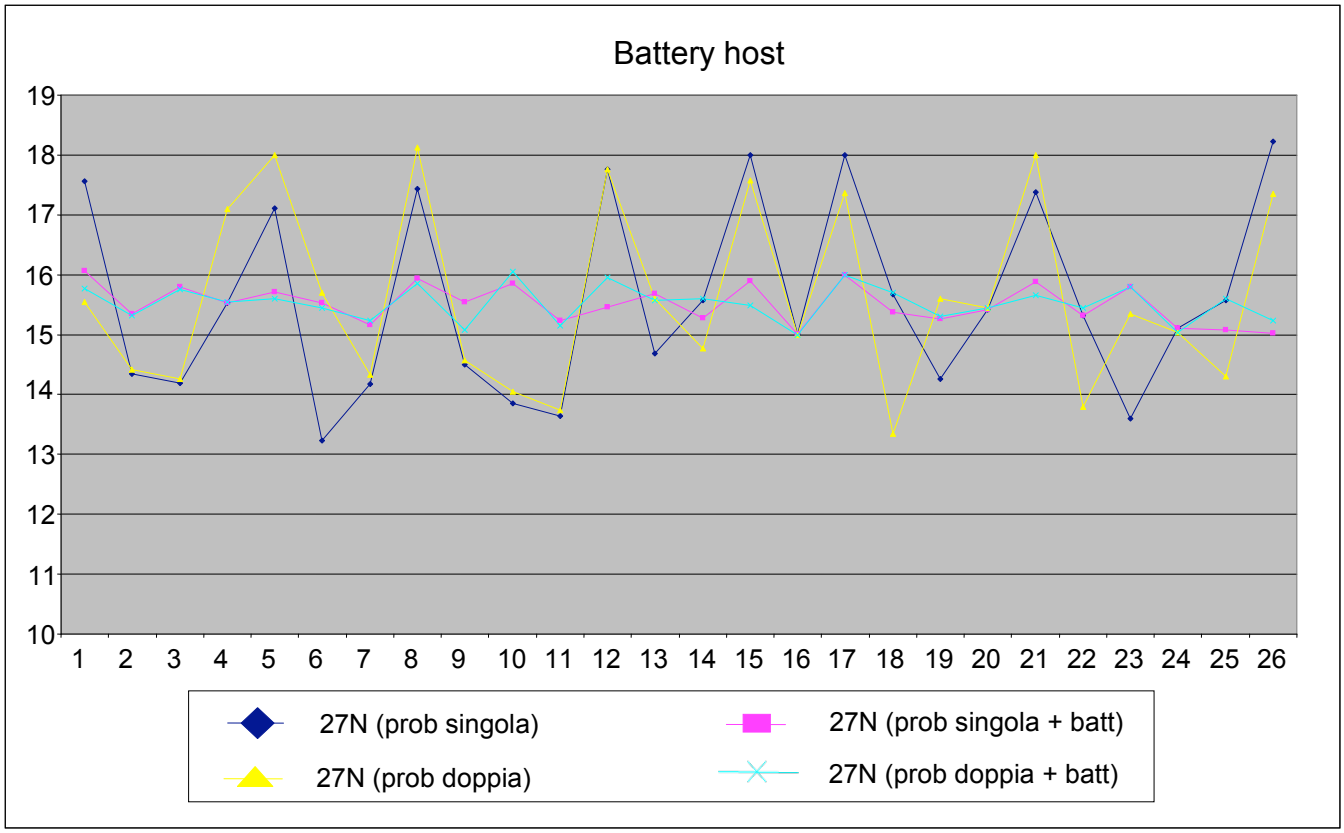


Figure 54 – 27 Nodi (dest singola)

4.6 REALIZZAZIONE “WIRELESS SENSORS NETWORK” IN GAETA’S PLANT

Questo progetto nasce dall’esigenza di testare la tecnologia “wireless sensors network” in ambito industriale. A partire da questa esigenza è stato proposto come scenario di riferimento l’impianto industriale di Gaeta.

La soluzione wireless è stata progettata per garantire gli attuali standard di sicurezza dell’impianto.

Lo standard preso in considerazione per la realizzazione della intera rete è il WirelessHART.

I livelli di affidabilità e performance, rispetto ad un collegamento FastEthernet, sono limitati dalla stessa tecnologia Wireless in termini di riduzione dei costi infrastrutturali.

Lo studio proposto è stato realizzato attraverso sopralluoghi necessari per verificare la reale copertura, le eventuali barriere e il conseguente numero di sensori wireless necessari per il test.

Per tutte le area interessate si è deciso di utilizzare 7 sensori wireless, e un gatway.

Il numero ed il tipo di sensori wireless sono stati scelti per venire incontro alle reali esigenze dell’impianto ed per realizzare una “mesh network” indispensabile per testare la tecnologia.

Di conseguenza, per l’effettiva realizzazione della rete sono state definite due differenti soluzioni:

1. utilizzare degli adapter wireless su alcuni sensori (non wireless) già presenti nell’impianto
2. utilizzare sensori wireless nuovi.

L’infrastruttura permetterà:

1. monitoraggio e acquisizione dei dati trasmessi dai differenti wireless sensors
2. confronto prestazioni (throughput, delay) tra soluzioni cablate già esistenti e nuove soluzioni wireless
3. verifica affidabilità dell’intera “wireless sensors network”

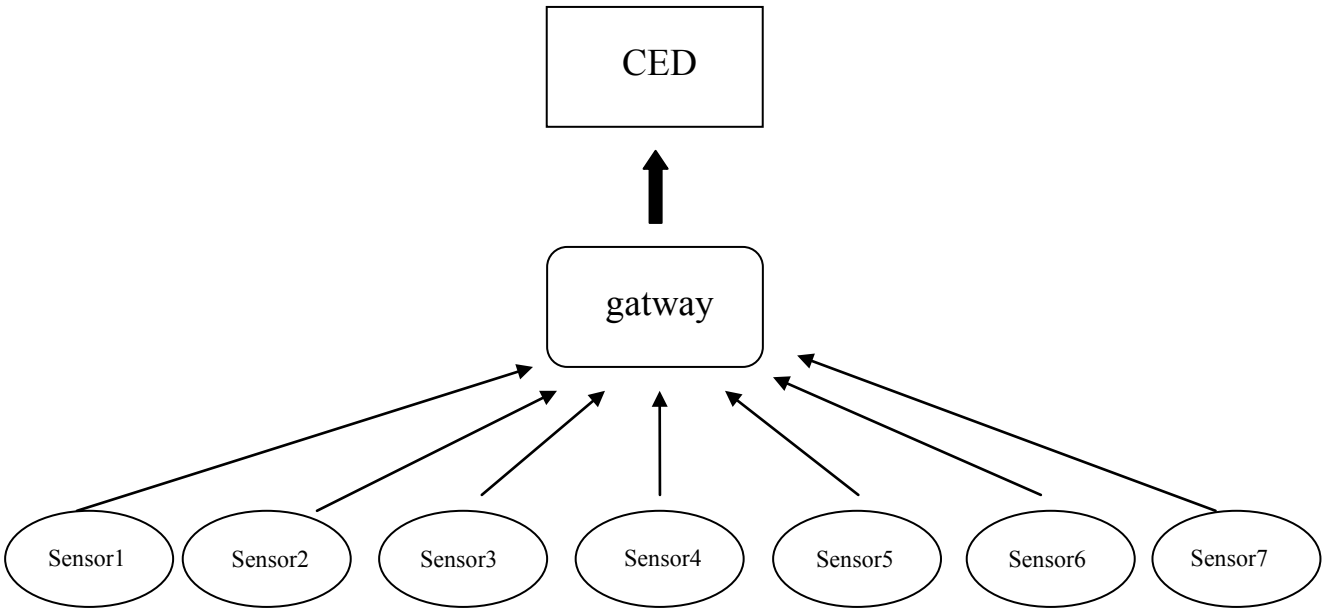


Figure 55 – Disegno architetturale

In seguito viene riportata la mappa dell'impianto di Gaeta con il posizionamento dei relativi sensori.

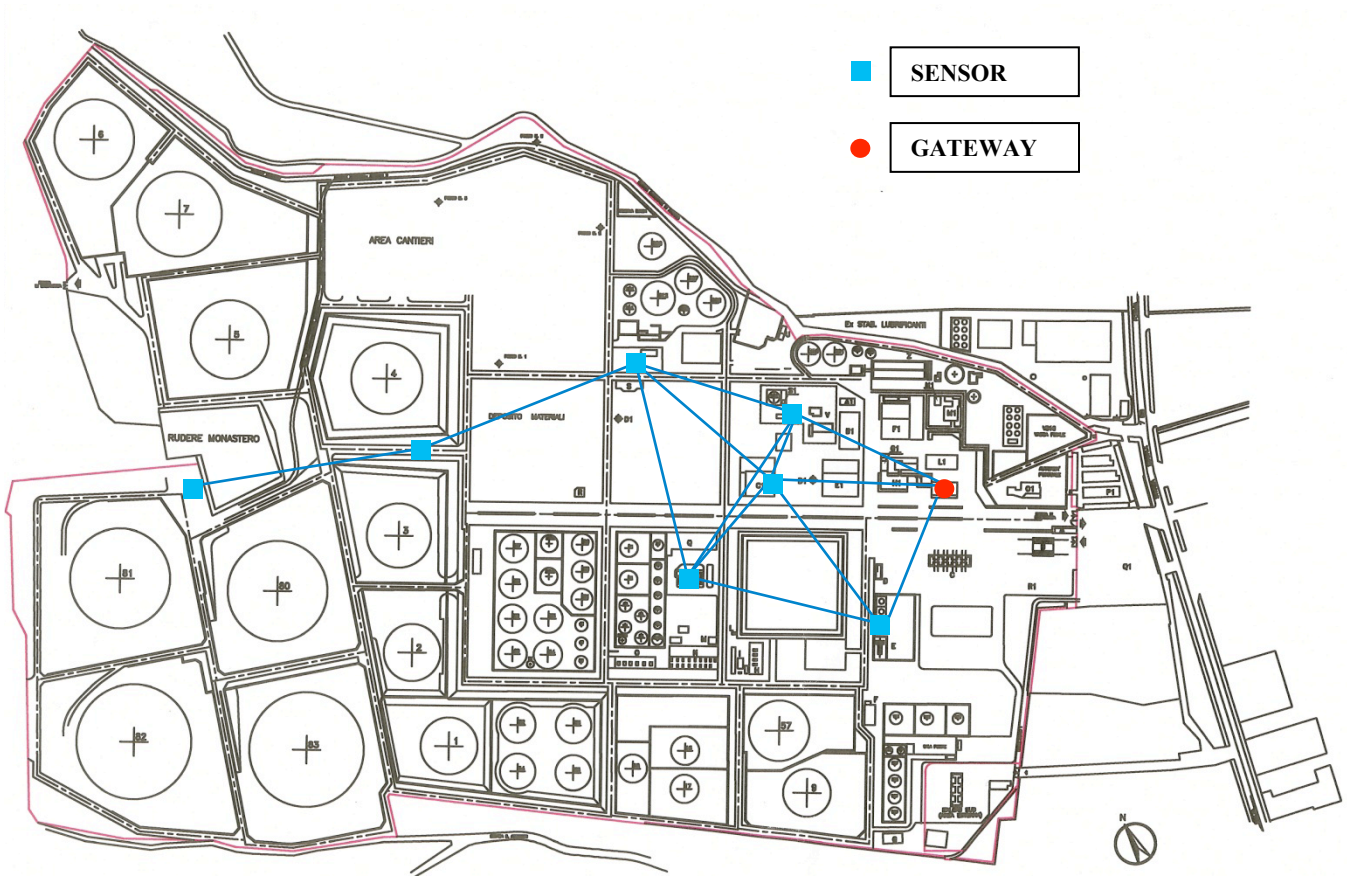


Figure 56 – mappa Gaeta

Utilizzando l'impianto di Gaeta come scenario "reale" di riferimento ed il modello in Omnet+ sviluppato in precedenza sono state effettuate delle simulazioni per testare le differenti tecniche di routing AODV-AF.

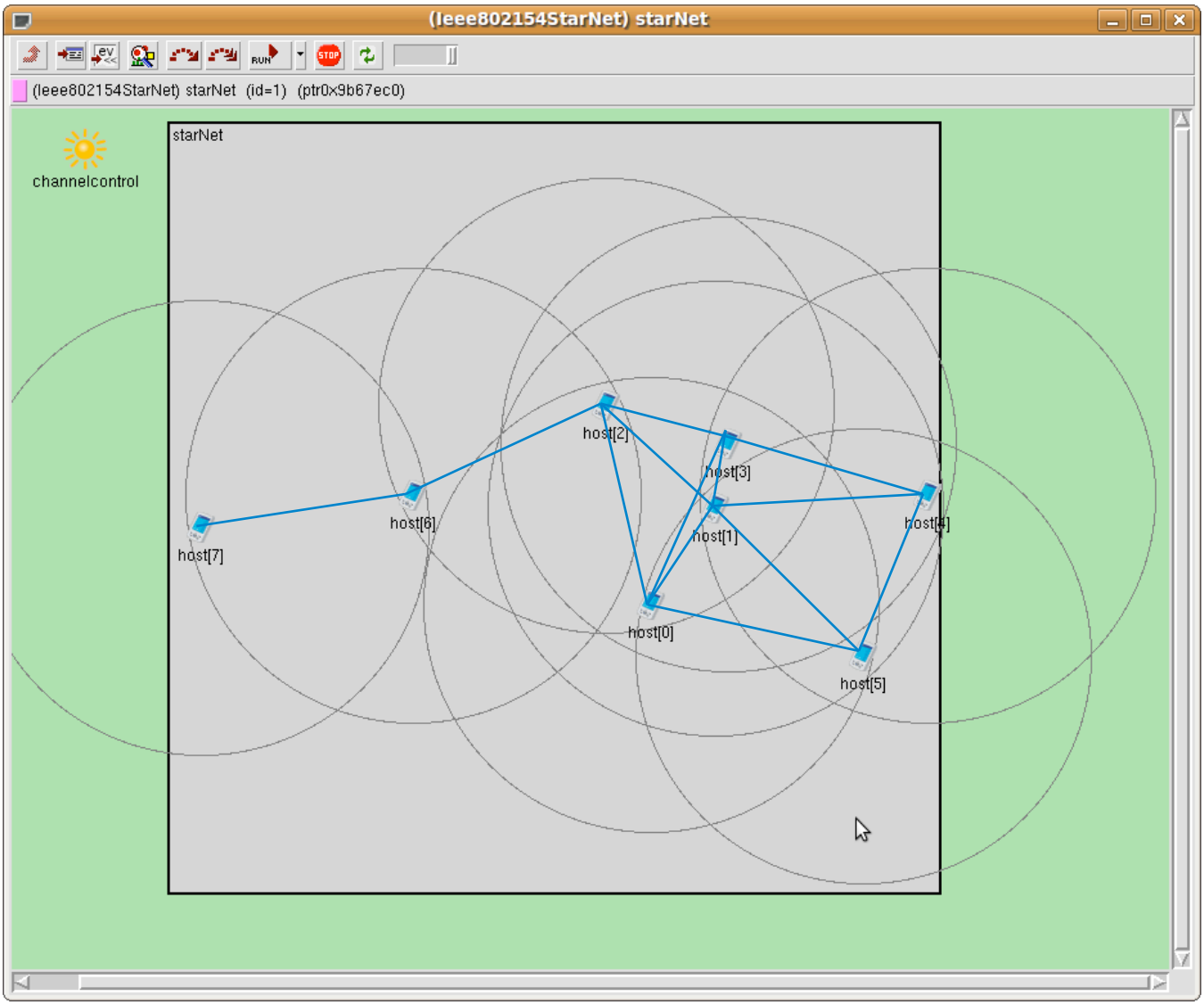


Figure 57 – Simulazione Omnet+ 8 nodi

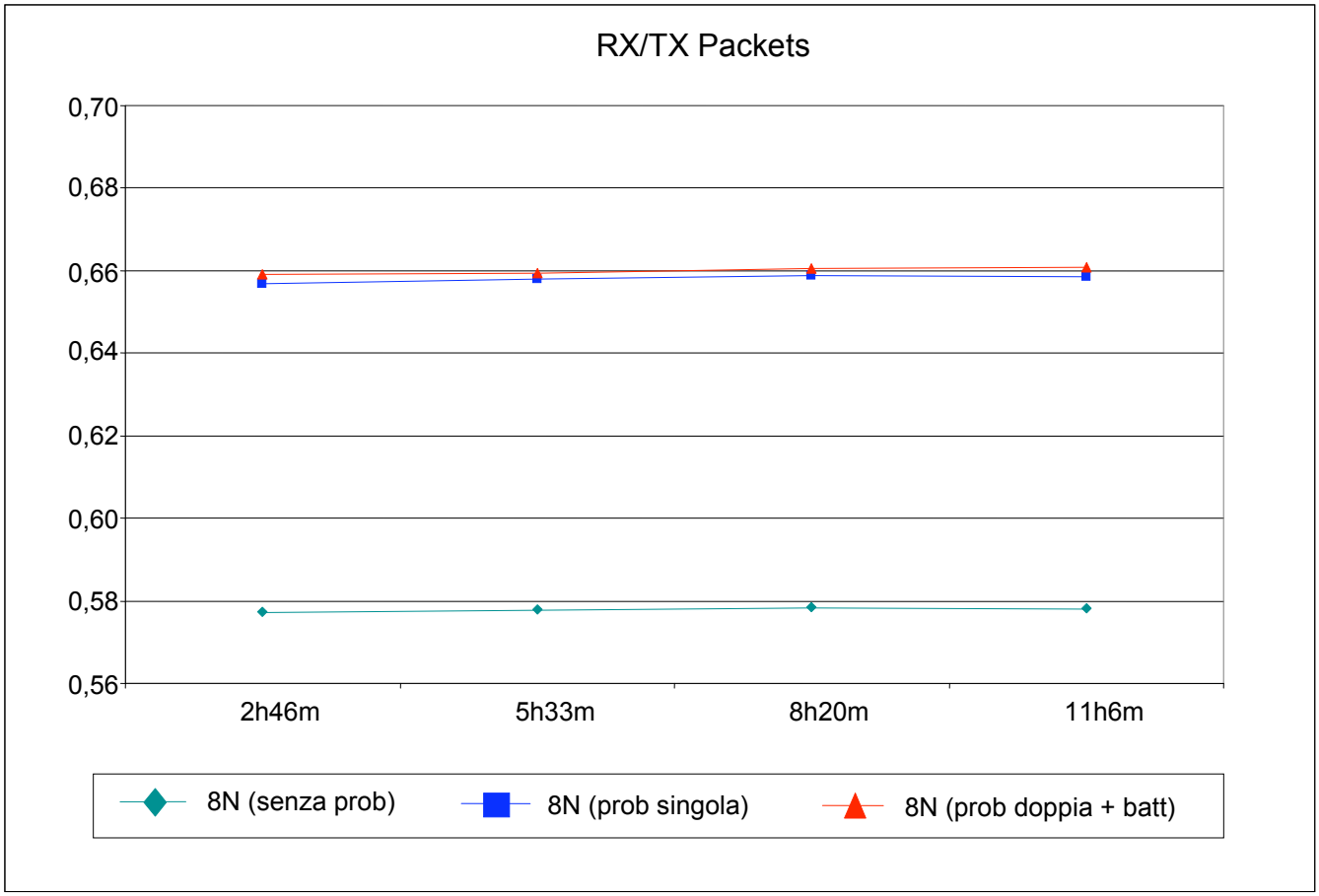


Figure 58 – RX/TX Packets

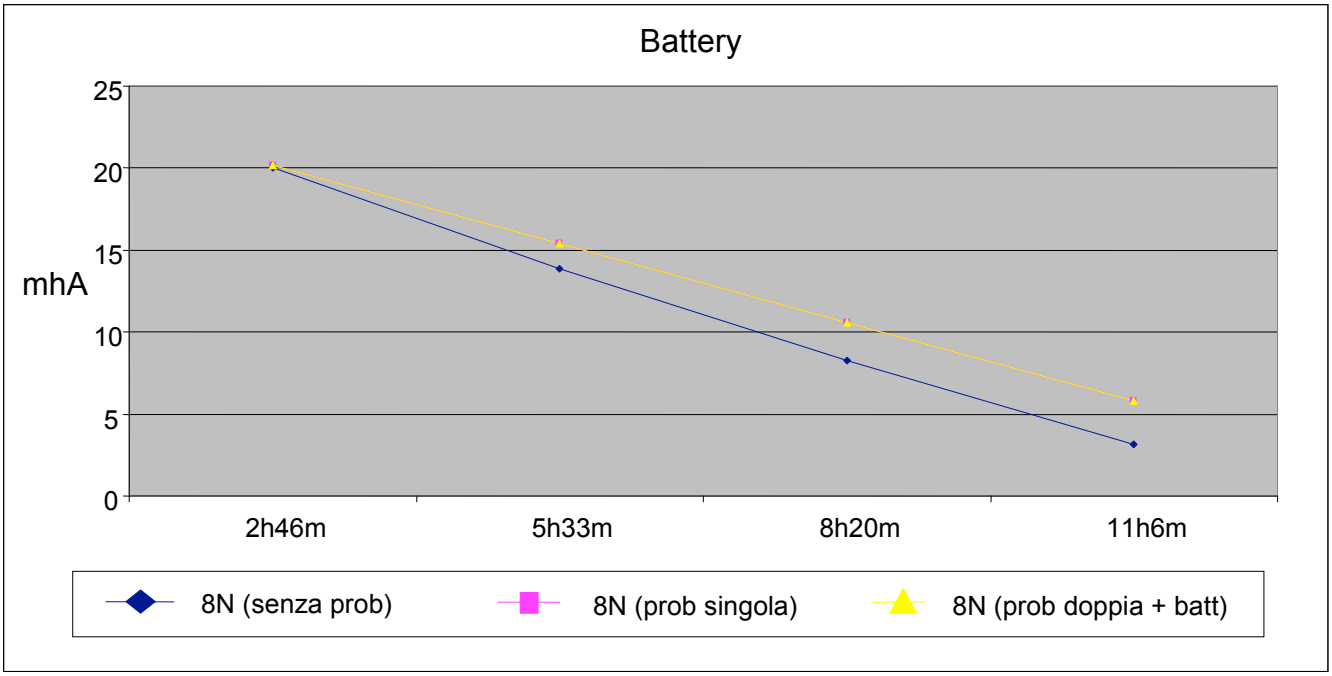


Figure 59 – Batteria network

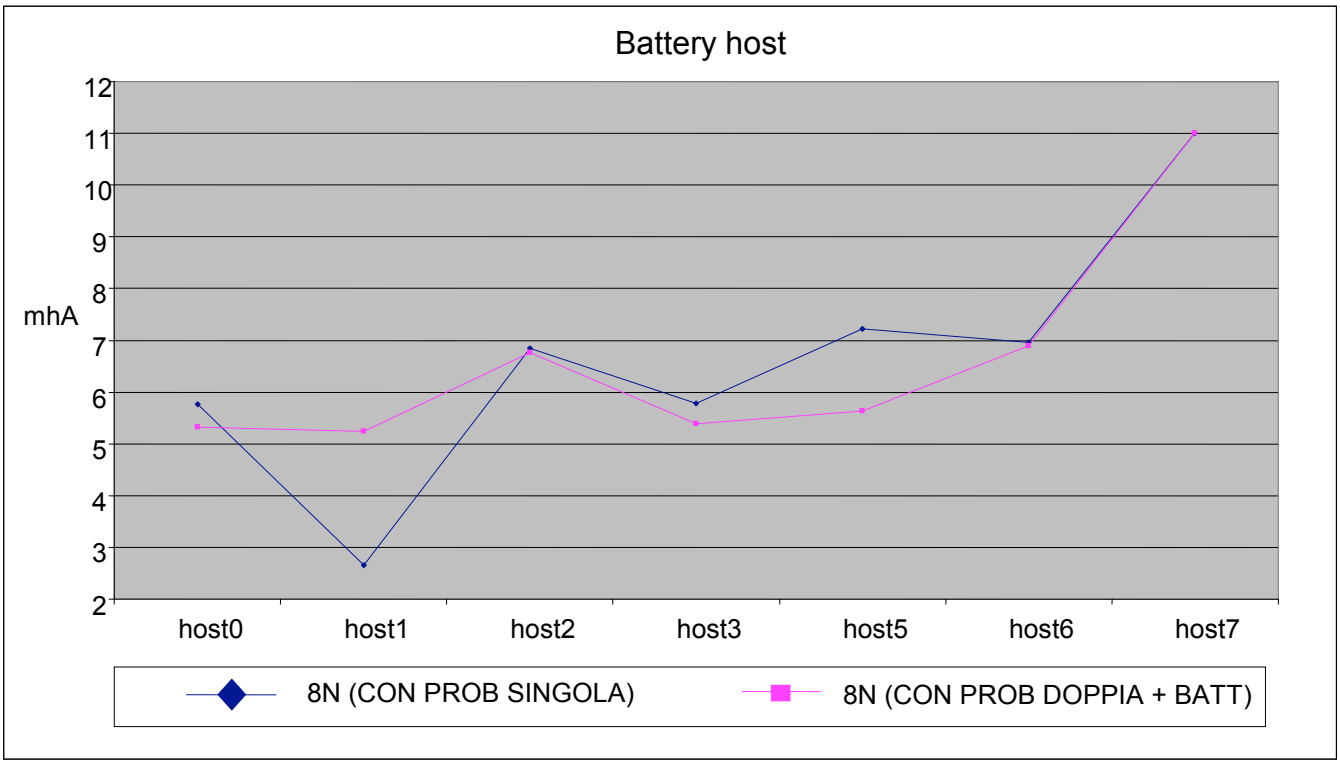


Figure 60 – Batteria host

Osservando un numero di hops che rimane inalterato per entrambe le configurazioni (grafico successivo), il grafico precedente mostra una diminuzione della varianza nella configurazione con probabilità doppia con contributo della batteria.

Partendo da queste osservazioni, per entrambe le configurazioni, è stato preso in considerazione l'host con il livello più basso di batteria per calcolare l'autonomia residua.

La differenza temporale tra l'autonomia residua di entrambe è risultata essere di circa 1^h44^m .

Di conseguenza, nello scenario reale di Gaeta, l'utilizzo di una configurazione con probabilità doppia e contributo della batteria, aumenta l'autonomia della rete di 1^h44^m.

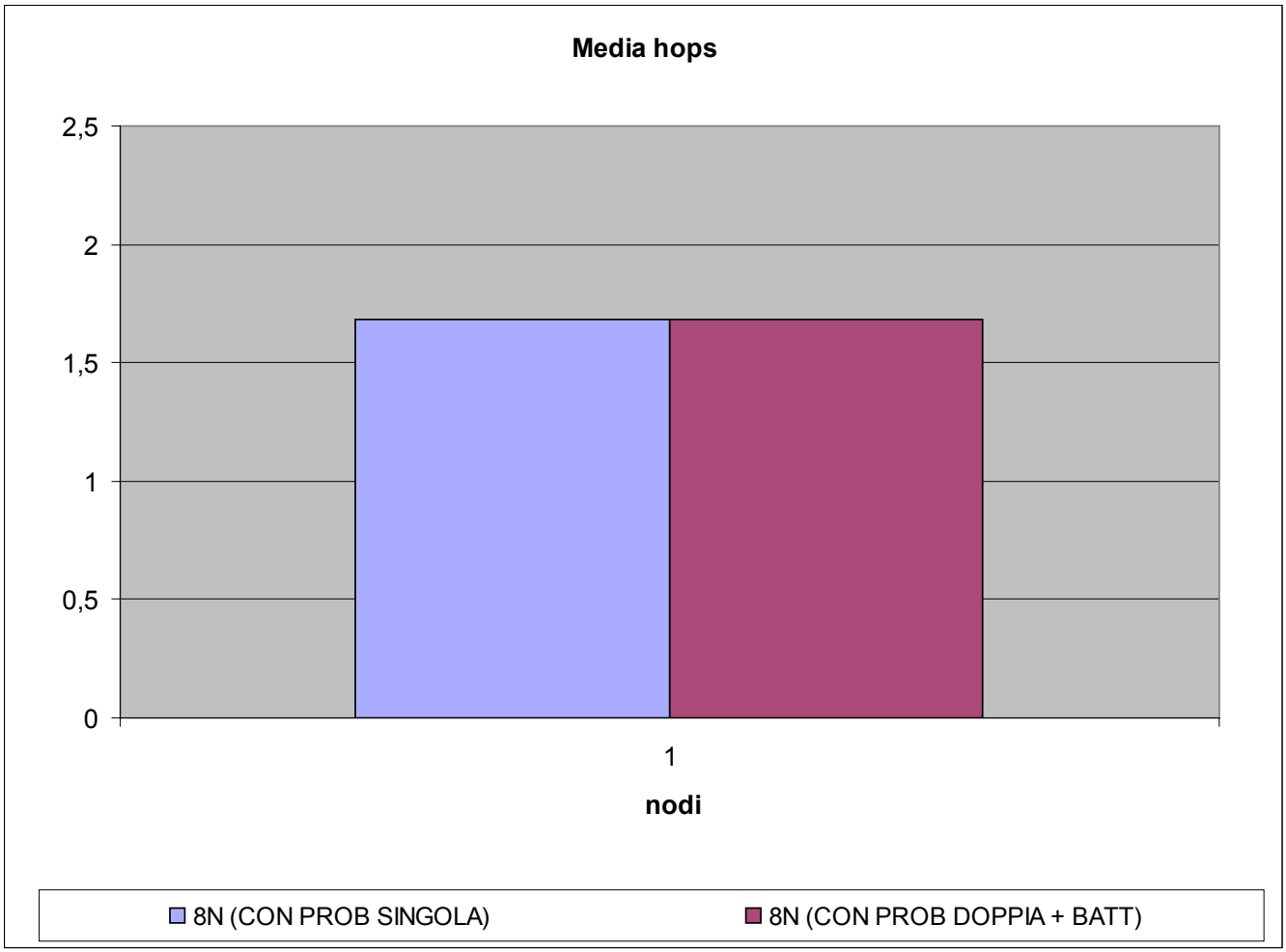


Figure 61 – N° Hops

5 CONCLUSIONI

Le argomentazioni trattate nella tesi collocate in un contesto “reale” industriale hanno permesso di sviluppare, simulare ed analizzare i dati ottenuti con Omnet+ contemporaneamente alla realizzazione di un progetto di rete di sensori wireless presso l’impianto di Gaeta di ENI s.p.a.

Lo scenario di Gaeta è stato utilizzato come riferimento per le simulazioni in Omnet+.

Il contesto industriale insieme alle specifiche di progetto hanno portato a sviluppare la tesi sull’analisi delle prestazioni di un particolare algoritmo di routing : AODV.

In questo contesto è stato scelto il protocolo di routing AODV poiché risulta essere lo standard utilizzato dalle principali tecnologie di mercato come: ZigBee, WirelessHart, ecc..

I risultati ottenuti con Omnet+ hanno evidenziato il trade-off esistente tra sistemi con semplice AODV e sistemi con AODV_AF e AODV_AF con contributo della batteria.

Il trade-off concerne sistemi ad alta reliability con un inefficiente utilizzo delle risorse ed sistemi a bassa reliability con un efficente utilizzo delle risorse.

BIBLIOGRAFIA:

[1] Xavier Carcelle, Tuan Dang, Catherin Devic. Industrial Wireless Technologies: application for electrical utilities

[2] Feng Chen, Nan Wang, reinhard German, Falko Dressler, Siemens AG. Performance Evalutation of IEEE 802.15.4 LR-WPAN for industrial Applications

[3] Wang hui. The Application and Research of Wireless Technology in Industrial Network

[4] Jianping Song, Song Han, Aloysius K. Mok, Deje Chen, Mike Lucas, Mark Nixon. WirelessHART: Applyng Wireless Technology in Real-Time Industrial Process Control

[5] Josè A. Gutierrez, Marco Naeve, Eaton Corporation Ed Callaway, Monique Bourgeois, Vinay Mitter, Bob Heile. IEEE 802.15.4: A Developing Standard for Low-Power Low-Cost Wireless Personal Area Network.

[6] Feng Chen, Falko Dresser. A Simulation Model of IEEE 802.15.4 in OMNet++

[7] Andreas Willig, Kirsten Matheus, Adam Wolisz. Wireless Technology in Industrial Network

[8] Shizhuang Lin, Jingyu Liu, Yanjun Fang. ZigBee Based Wireless Sensor Networks and its Applications in Industrial

[9] Hisanori Hayashi, Toshi Hasegawa, Koji Demachi. Wireless Technology for Process Automation

[10] Tomas Lennvall, Stefan Svensson. A Comparison of Wireless HART and for Industrial Application