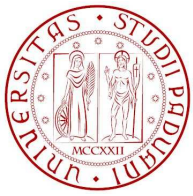


Università degli Studi di Padova

Dipartimento di Ingegneria dell'Informazione
Corso di Laurea in Ingegneria delle Telecomunicazioni

Tesi di Laurea

SMART GRIDS, STATO DELL'ARTE E PRINCIPALI PROBLEMATICHE

Laureando:
Francesco GRASSO

Relatore:
Dr. Stefano TOMASIN

Anno accademico 2010/2011

Indice

Introduzione

Le *smart grid* si pongono come evoluzione delle attuali reti di distribuzione elettrica relativamente alla crescente domanda di energia, all'espansione nell'utilizzo di fonti d'energia rinnovabile e all'evoluzione nelle tecnologie informative. Esse sono un'efficiente soluzione dal punto di vista energetico e soprattutto dal punto di vista economico.
L'obbiettivo di questa tesi è presentare un quadro generale sulla situazione energetica, su cosa siano le *smart grid* e le comunicazioni su linee di potenza, per poi presentarne le principali problematiche e relative soluzioni.
Nel primo capitolo verranno quindi descritti i principali svantaggi delle reti elettriche attuali, sottolineando la loro inadeguatezza nell'integrazione delle fonti d'energia rinnovabile. Si presenteranno in seguito le *smart grid* e le loro principali caratteristiche, come l'utilizzo di generazione distribuita, passando poi all'elenco delle principali problematiche e delle principali direzioni di ricerca per lo sviluppo delle stesse.
Il secondo capitolo si focalizzerà in particolare sul problema del controllo delle tensioni, presentando prima il modello di rete per poi esporre il metodo dell'analisi di sensibilità delle tensioni relativamente alla potenza reattiva. Si introdurranno quindi gli algoritmi di raggruppamento delle tensioni per la classificazione in base alla sensibilità, facilitando in tal modo l'organizzazione del controllo (tramite inserimenti di potenza reattiva). Verrà poi affrontato il problema della *Cyber Security* relativamente allo scambio d'informazioni nelle *smart grid*, considerando in particolare la crittografia relativamente all'implementazione dei protocolli d'autenticazione e descrivendo la struttura di un *frame* relativamente a tali comunicazioni nelle reti di potenza.
Nel terzo capitolo verranno considerati i protocolli di comunicazione *powerline*, in particolare il protocollo G3-PLC. Si partirà dalla descrizione del modello di canale utilizzato, descrivendone le caratteristiche in relazione alla variabilità dei carichi e quindi al relativo comportamento in frequenza passando poi al modello statistico. In seguito si passerà alla descrizione vera e propria dello standard G3-PLC considerando lo strato fisico, quindi descrivendo il trasmettitore e i relativi blocchi, la struttura del *frame* di comunicazione e le modulazioni utilizzate.

Capitolo 1

Contesto

1.1 I problemi dell'attuale rete elettrica

Il panorama energetico globale annovera la presenza di un numero limitato di industrie che concentrano la produzione elettrica in megacentrali a combustibili fossili e nucleari. L'elettricità prodotta viene immessa in grandi dorsali ad alta tensione, da cui si dipartono le reti che arrivano fino alle utenze. Si tratta ancora di un modello unidirezionale e passivo. L'infrastruttura, che è complessa e costosa, incide in maniera significativa sul costo finale dell'energia e presenta una certa cristallizzazione: il flusso di energia viaggia in maniera unidirezionale, dal luogo di produzione a quello di consumo e, in tale contesto, l'utente finale costituisce solo ed esclusivamente un carico passivo della rete. Tale impostazione presenta molti svantaggi:

1) Elevate perdite per effetto Joule subite lungo la linea di collegamento dalle grosse centrali alle utenze;

2) Impossibilità di gestire in modo efficace i flussi di energia per convogliarla dove necessario a causa dalla mancanza di protocolli nella gestione dinamica dei flussi energetici;

3) Difficoltà nello sfruttare a pieno fonti di energia rinnovabile come eolico e fotovoltaico;

4) Tempi di risposta troppo lunghi in caso di black-out di grandi dimensioni, con impossibilità di arginare gli effetti valanga nelle cadute di tensione e conseguenti interruzioni di flusso energetico.

1.2 Le fonti d'energia rinnovabile

La più rapida espansione nell'utilizzazione delle fonti d'energia rinnovabile è attesa maggiormente nel campo eolico e solare. Negli Stati Uniti si stima che il settore eolico cresca da 31TWh nel 2008 (ovvero l'1,3% del fabbisogno) fino a 1160TWh nel 2030, il che equivarrebbe ad ottenere un supporto pari al 20% della produzione totale (pari a circa 5800TWh) [1]. La causa che rende imprevedibili le fonti eoliche è la capacità produttiva che risulta molto inferiore rispetto a quella dei generatori convenzionali. La forte variabilità e incostanza nella produzione eolica è causata dal progetto delle attrezzature produttive e dalla loro distribuzione geografica. Quest'ultima risulta essere non lineare in quanto le fonti eoliche su larga scala sono tipicamente distribuite a grande distanza dai carichi comportando limitazioni trasmissive di tipo termico, voltaico e soprattutto, a problemi di instabilità. Per quanto riguarda le fonti solari, esse si presentano come la più abbondante fonte di energia rinnovabile. L'energia solare totale che in un anno raggiunge la superficie terrestre è pari a circa 1000 volte il consumo mondiale di combustibile fossile in un anno [2]. Le due prevalenti tecnologie che sfruttano l'energia solare sono la termica e la fotovoltaica. La causa della variabilità di tale fonte rinnovabile è dovuta alla "disponibilità" della luce solare. I fattori di capacità infatti, oscillano tra il 10% e il 20% che può essere innalzato fino al 70% utilizzando mezzi di stoccaggio (per fattore di capacità si intende il rapporto tra la produzione di energia elettrica effettiva fornita da un impianto di potenza durante un periodo di tempo e la fornitura teorica di energia che avrebbe potuto offrire se avesse operato alla piena potenza operativa massima). Come nel campo eolico, anche il campo solare presenta problemi di limitazione trasmissiva a causa della lontananza delle fonti dai carichi. In definitiva, le fonti d'energia rinnovabile costituiscono un'importante risorsa energetica, ma il loro utilizzo richiede un'elasticità e una capacità d'adattamento a fattori di variabilità che le attuali reti elettriche non sono in grado di ottenere.

1.3 Le *smart grid*

La crescente domanda di energia ha stimolato la formulazione di piani di ampliamento e potenziamento delle attuali reti elettriche nei paesi industrializzati e in quelli in via di sviluppo sollevando il problema dei crescenti costi economici ed ambientali che rendono difficoltoso l'uso dei vecchi paradigmi per tali ampliamenti e potenziamenti. Parallelamente, i continui progressi nelle ICT (*Information & Communications Technology*) hanno creato una convergenza di interessi scientifici e industriali sull'utilizzazione di tali tecnologie per attuare un processo di trasformazione strutturale di ogni fase del ciclo energetico: dalla produzione, all'accumulo, al trasporto, alla distribuzione, alla vendita e al consumo intelligente di energia. Vengono quindi attivate o migliorate nuove funzionalità nella gestione della rete elettrica trasportando attraverso la sua attuale infrastruttura flussi informativi necessari per specifici compiti, rendendo i nodi della rete dei nodi attivi. Tale connubio tra ICT ed energia viene comunemente identificato col termine di *Smart Grid*.

1.4 Principali vantaggi e caratteristiche delle *smart grid*

Uno dei maggiori vantaggi introdotti dalle *Smart Grid* è l'abilità di integrare efficientemente e semplicemente fonti di energia rinnovabili che risultano essere intermittenti a causa della loro dipendenza da fenomeni non costanti, ma che costituiscono un'importante approvvigionamento d'energia se adeguatamente sfruttate. I soggetti interessati dalle *smart grid* sono tutte le utenze, che spaziano dal semplice utilizzatore e dai produttori di energia fino ai provider di trasmissione e alle comunità finanziarie. La funzionalità base delle *smart grid* si incentra sull'integrazione delle risorse energetiche distribuite (DER - *Distribuited Energy Resources*) nell'attuale sistema, dove per DER si fa riferimento a generatori, accumulatori e carichi controllabili connessi alla distribuzione elettrica.

Caratteristica fondamentale delle *smart grid* è inoltre la capacità di gestire, tramite protocolli e flussi informativi, generatori e carichi attivi disponibili nella rete, coordinandoli per compiere determinate funzioni in tempo reale come, per esempio, far fronte ad un picco, bilanciare il carico di un alimentatore oppure sopperire ad un improvviso calo di tensione attingendo da più distretti in cui è presente un surplus. Viene quindi applicato alla rete elettrica un protocollo simile al P2P (*Peer to peer*) di gestione delle informazioni utilizzato nelle reti informatiche. In una tale rete il rapporto gerarchico tra i nodi viene

praticamente annullato, ottenendo quindi tutti nodi paritari, compresi i nodi *end-user* della rete di distribuzione che non fungono da semplici utilizzatori delle risorse di rete, ma costituiscono essi stessi nodi che condividono e scambiano informazioni.

I dispositivi della rete elettrica, in questo modo, diventano parte attiva di un ciclo di controllo esteso alle grandi centrali di generazione così come ai componenti dei singoli utenti. Passando inoltre a un sistema di generazione distribuito di questo tipo vengono fortemente ridotte le perdite di trasmissione essendo l'energia elettrica prodotta in buona parte lì dove viene consumata grazie all'utilizzazione di fonti di energia rinnovabili come generatori connessi direttamente all'utente finale. Conseguenza fondamentale dell'utilizzo di flussi informativi attraverso l'attuale infrastruttura della rete è la possibilità di gestire i picchi di massima richiesta con uno *scheduling* sui carichi in modo da evitare che essi siano attivati tutti nello stesso momento. Uno degli aspetti critici nella distribuzione energetica è il verificarsi di picchi di massima richiesta. Durante tali picchi, per garantire un flusso energetico costante senza interruzioni, si utilizzano generatori ausiliari in standby che vengono messi in funzione per ovviare al calo di tensione dovuto ai numerosi carichi della rete che si presentano nella stessa finestra temporale. È chiaro che generatori di questo tipo costituiscono una risorsa economica gravosa che, se eliminata, aumenterebbe notevolmente l'efficienza generale del sistema. È possibile ridurre questi picchi di massima richiesta attuando una regolazione dei consumi con l'uso congiunto di *smart meter* (contatori digitali in grado di comunicare col resto della rete) e di sistemi di gestione automatizzata dei carichi al livello *end-user*.

Considerando l'utenza domestica, la gestione intelligente dei carichi come gli elettrodomestici, che possono essere avviati in un qualsiasi momento della giornata senza particolari ripercussioni sulle dinamiche casalinghe, avviene grazie alla comunicazione dello *smart meter* con la rete. Quest'ultima, infatti, utilizzando segnali di controllo e informazione, comunica, su richiesta del contatore digitale, se si è in presenza della fascia oraria di picco energetico. Lo *smart meter* a questo punto, agisce di conseguenza avviando i carichi solo dopo l'avvenuta conferma di assenza di picchi. In situazioni del genere non solo si appiattisce il picco di massima richiesta, ma avviene anche un risparmio sull'utilizzo di generatori di stand by o persino una limitazione del numero di nuove centrali da costruire per sopperire al fabbisogno energetico. Avviene oltretutto un notevole risparmio economico dell'utente visto che la fascia oraria di picco risulta il momento in cui l'elettricità costa di più.

1.5 Fondamento dell'infrastruttura informatica per le *smart grid*

La realizzazione di una *smart grid* richiede maggiori requisiti di sicurezza e affidabilità, data l'esposizione di sistemi critici al sistema informativo. Una tale infrastruttura dovrebbe essere in grado di gestire comunicazioni bidirezionali quasi istantanee tra ogni nodo della rete. Tutto ciò coinvolge la gestione di enormi flussi di dati sia d'analisi che di controllo, richiedendo una struttura capace di gestire risposte informative intelligenti in brevissimo tempo, coordinate con un alto livello di analisi globale per prevenire o contenere l'evolversi di problematiche. È chiaro che adottare un sistema centralizzato per un simile scopo risulterebbe troppo lento, sia a causa della stessa topologia di rete, per ovvi problemi di accodamento dei flussi informativi, sia per la problematica dei tempi di elaborazione degli stessi.
Un'architettura di rete distribuita invece, costituirebbe un sistema molto più efficiente basandosi su:

- Dispositivi di controllo automatizzati per la gestione rapida e intelligente dei flussi di potenza e per il controllo sia in trasmissione che in ricezione della tensione;

- Dispositivi integrati per il controllo adattativo sulle informazioni trasmesse, come diagnosi su flussi dati corrotti o ripetuti e identificazione degli *header*;

- Comunicazioni sicure tra i nodi integrate nella struttura base della rete, con elevati gradi di distribuzione basate su *standard* per consentire flessibilità alla configurazione di rete e assicurare monitoraggio e comunicazione tra i nodi e i dispositivi di controllo;

- Elevate capacità di elaborazione per consentire analisi affidabili in grado di dare supporto agli operatori e ai dispositivi di controllo distribuiti secondo una gerarchia geografica;

- Tecnologie internet tramite l'utilizzo di protocolli per facilitare lo scambio e l'elaborazione dei dati e la sicurezza, implementando un'architettura basata su *standard* con dispositivi *Plug and Play* e componenti *Service Oriented.*

1.6 Ambiti di ricerca e problematiche principali per le *smart grid*

I principali settori di sviluppo per le *smart grid* si incentrano sulle principali problematiche di modellamento e sviluppo dei mezzi e delle tecnologie necessarie per costruire un'infrastruttura sicura ed affidabile. Lo sviluppo si pone secondo delle aree funzionali:

a) Creazione di modelli:

- Stilare un catalogo di componenti, strategie di controllo operative e casi test per le *smart grid*;
- Sviluppare modelli di reti e risorse rinnovabili basate su progetti pilota per *smart grid*;
- Creare delle funzioni test per la rilevazione dei comportamenti principali in determinate dinamiche;
- Creare delle linee guida per i dispositivi delle *smart grid* in modo da attuare compatibilità e scambio;
- Integrare i progetti di *smart grid* con i sistemi provider già esistenti.

b) Sviluppo delle tecnologie:

- Sistemi affidabili di test e misura sulle prestazioni;
- Bande di trasmissione incrementate, comunicazioni sicure e affidabili;
- Ricerca mista sia sulla corrente alternata che continua per la distribuzione;
- Sviluppo di metodi per il controllo delle DER e il controllo delle tensioni;
- Elettronica di potenza per la trasformazione e lo stoccaggio dell'energia, per la ricarica e la gestione della potenza reattiva.

c) Dimostrazione e valutazione:

- Verifica delle prestazioni delle tecnologie *smart grid* inclusi metodi di controllo e interoperabilità;
- Accumulo di dati di analisi e modellamento;
- Costruzione di processi e infrastrutture per i test e il supporto.

d) Standardizzazione:

- Sviluppo di test per incrementare interoperabilità, integrazione e *upgrade*;
- Identificazione di lacune negli *standard* della *cyber security* e progetto di procedure comuni per lo scambio di informazioni entro i limiti stabiliti per la sicurezza.

1.7 La copertura di aree remote: le *microgrid*

La problematica della copertura elettrica di aree remote come zone rurali e isole, trova la sua soluzione nell'utilizzazione di piccole reti di potenza locali per l'approvvigionamento energetico basato su un'autosufficienza quasi totale. Le *microgrid* sono appunto delle reti di potenza ridotta che si appoggiano a generatori di piccola portata. Tali generatori operano come un unico sistema il cui scopo è la fornitura di energia elettrica al livello locale ad un gruppo di utenze.
È chiaro che una rete siffatta può comunque operare connessioni con reti di livello superiore e scambiare energia con esse. Trovando la sua applicazione soprattutto per aree remote, la *microgrid* adotta una modalità di funzionamento "ad isola". Ciò significa che manterrà autonomamente il suo equilibrio generazione/carico usando solamente le risorse locali disponibili come generatori diesel, pannelli fotovoltaici e generazione idroelettrica.
Per questioni economiche e conseguente impossibilità di ampliamenti di grande portata, le *microgrid* operano sempre vicino ai limiti della propria capacità generativa, tendendo spesso al sovraccarico. A differenza delle reti di grandi dimensioni le quali, per abbattere un carico eccessivo disconnettono intere zone di carico della rete senza una precisa classificazione di priorità in base alla tipologia di carico, nelle *microgrid* una tale procedura risulta molto più difficile e si tende ad adottare un metodo di minor impatto. Il metodo

consiste nella disconnessione dei soli carichi che risulteranno non essenziali secondo una scala di priorità.
Si vanno a costituire in tal modo degli *smart system* basati sulla gestione automatizzata della domanda (DSM-*Demand Side Management*) che sono in grado di disconnettere i nodi della rete in modo selettivo secondo una modalità stabilita a priori con l'utilizzatore interessato.
I livelli di automazione nella DSM possono essere così definiti:

- Manual DSM: Utilizza un approccio in cui si effettua la disconnessione manualmente per ogni carico in questione;

- Semi-Automated DSM: Utilizza una strategia di gestione del carico pre-programmata inizializzata manualmente tramite un sistema di controllo centralizzato;

- Fully-Automated DSM: Non necessita di intervento umano, ma il controllo è inizializzato tramite la ricezione di un segnale di comunicazione esterno il quale inizializza una strategia pre-programmata di gestione dei carichi.

La configurazione del DSM è relativamente complessa. Considerando che le operazioni della *microgrid* siano controllate da un MGCC (*MicroGrid Central Controller)* il quale livella generazione e carico, tale controllore ha di solito accesso diretto alle unità generative in modo da controllare la potenza prodotta in accordo con la situazione di carico. Esso però non avrà accesso diretto ad ogni carico, bensì ne vedrà uno solo dato dalla somma di tutti gli utilizzatori.
Nella *microgrid* sarà quindi richiesta l'aggiunta di nuovi dispositivi quali *switch* e *power meter* che supportino il controllo remoto (le comunicazioni tra il MGCC e i dispositivi di controllo possono essere realizzati ad esempio tramite comunicazioni *wireless hop-to-hop* o tramite comunicazioni *powerline*). Usando questi dispositivi di controllo, l'MGCC è in grado di classificare la tipologia dei carichi e, in una situazione di sovraccarico, di decidere quali possano essere disconnessi e quali no. Il rilevamento automatico dei dispositivi nella *microgrid* è denominato *"self configuration"* [3].

Capitolo 2

Controllo delle tensioni: carichi attivi e generazione distribuita

2.1 Introduzione

Alcuni dispositivi già installati nella rete elettrica sono in grado di generare/assorbire potenza reattiva. Tali dispositivi sono generalmente denominati FACTS (*Flexible AC Trasmission System Devices*) e ne sono un esempio gli invertitori come i pannelli solari e i veicoli elettrici ibridi (*PHEVs – Pluggable Hybrid Electric Vehicles*). Anche i condensatori sincroni (realizzati mediante componenti meccanici) possono essere classificati come FACTS. Tali dispositivi reattivi non sono utilizzati dall'attuale sistema di potenza.
Come noto infatti, la potenza reattiva non dà luogo a un consumo energetico giacché rappresenta l'energia che viene alternativamente assorbita e restituita dal campo magnetico (circuiti induttivi) o dal campo elettrico (circuiti capacitivi). E' una componente che tende ad essere ridotta, visto che in tal modo diminuisce anche la corrente e quindi si attenuano le perdite per effetto Joule. E' possibile però effettuare un'integrazione dei dispositivi reattivi al livello *end-user* nella rete di distribuzione. In tal modo, appoggiandosi a un'infrastruttura di comunicazione sicura, si potrebbe fornire supporto di tensione alla rete, operando un controllo sui voltaggi tramite tali dispositivi. E' infatti noto che i dispositivi reattivi (risorse reattive) disponibili possono essere usati per incrementare i voltaggi, rendendo il sistema meno vulnerabile all'instabilità di tensione e permettendo il ripristino di quest'ultimo dopo una destabilizzazione avvenuta a causa di interferenze.
Per riportare il sistema ad un punto di equilibrio, si operano dei controlli detti appunto controlli correttivi. Azioni che possono essere classificate come controlli correttivi sono, ad esempio, la ridistribuzione dei generatori o la dispersione del carico di rete che però risultano dispendiosi o con tempi di risposta troppo lunghi. La commutazione delle linee

di trasmissione invece presenta il vantaggio di cambiare lo stato del sistema, sopperendo ai problemi di tensione e presentando sia tempi di risposta brevi sia costi limitati.
Si mostrerà come determinare, dal punto di vista topologico, le posizioni nell'infrastruttura di comunicazione dalle quali eseguire il controllo reattivo e si discuteranno i metodi per costituire dei "gruppi di supporto reattivo". In generale, verrà mostrato come le *Smart Grid* permettano l'utilizzo dei dispositivi *end-user* già disponibili nella rete come mezzi per sopperire ai problemi del sistema di potenza (ad es. collasso di tensione).

2.2 Sensibilità delle tensioni alla potenza reattiva

Modello di rete

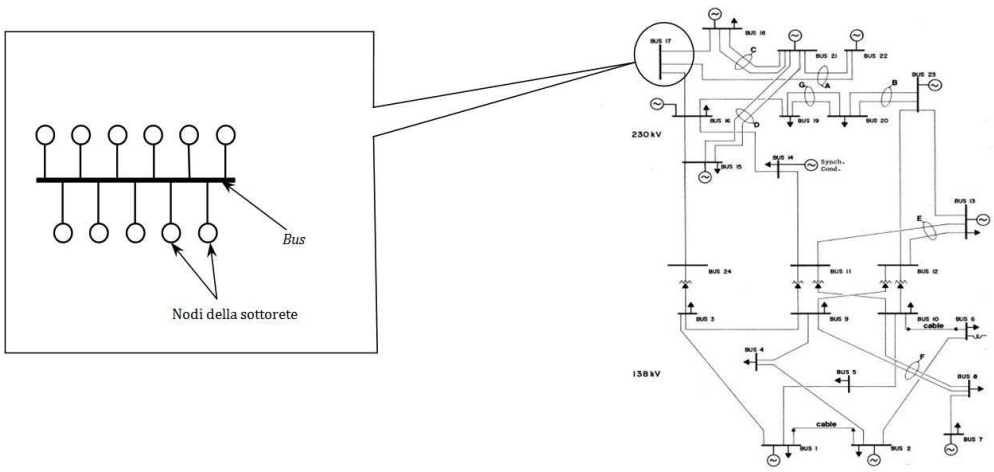


Figura 2.1: Particolare di un modello mediante bus (24 bus)

La rete verrà considerata come modello mediante *bus* (figura 2.1). In tale modello, le sottoreti della rete globale sono organizzate tramite una topologia architettata secondo un'unica linea (detta appunto *bus*) alla quale sono connessi tutti i nodi della stessa.
Essa è quindi una visione riassuntiva dove le varie sottoreti sono viste come un'unica linea (*bus*) rappresentante il carico totale di quel distretto.
I *bus* che presentano caratteristiche reattive, ovvero quelli di cui si cercherà di controllare l'uscita di potenza reattiva (Q, espressa *in MVAr – Mega VoltAmpere reactive*), saranno indicati come *Q-C buses* (*Q-Controlled buses*).

L'analisi della sensibilità

Il metodo dell'analisi di sensibilità della tensione alla potenza viene usato per determinare analiticamente il cambiamento per unità di tensione dovuto ad ogni variazione per unità di potenza attiva e reattiva. È semplicemente la misura di quanto è sensibile la tensione di un particolare *bus* rispetto ai cambiamenti di potenza attiva e reattiva in un altro *bus* in particolari condizioni di carico. Tale analisi è basata sulla matrice sensibilità che è ricavata dalla matrice Jacobiana delle equazioni di flusso del metodo Newton-Raphson (che trova le soluzioni al flusso di potenza usando la matrice ammettenza del sistema)[4].

Usando un approccio vettoriale, detti $\boldsymbol{V}, \boldsymbol{\vartheta}$ rispettivamente il vettore riga delle ampiezze di tensione del *bus* e il vettore riga degli angoli di tali fasori, si considerino le equazioni non lineari del flusso di potenza attiva (P) e reattiva (Q) a un *bus* generico

$$\boldsymbol{P}(\boldsymbol{\theta}, \boldsymbol{V}) = \mathbf{0}$$
$$\boldsymbol{Q}(\boldsymbol{\theta}, \boldsymbol{V}) = \mathbf{0}$$

Il metodo Newton-Raphson risolve le equazioni sopra citate usando l'espansione in serie di Taylor rispetto alle ampiezze di tensione e agli angoli di sfasamento delle stesse (Esprimendola in forma matrice/vettore), ottenendo

$$\begin{bmatrix} \frac{d\boldsymbol{P}}{d\boldsymbol{Q}} \end{bmatrix} = \underbrace{\begin{bmatrix} \frac{\partial \boldsymbol{P}}{\partial \boldsymbol{\theta}} & \frac{\partial \boldsymbol{P}}{\partial |\boldsymbol{V}|} \\ \frac{\partial \boldsymbol{Q}}{\partial \boldsymbol{\theta}} & \frac{\partial \boldsymbol{Q}}{\partial |\boldsymbol{V}|} \end{bmatrix}}_{\mathbf{J}} \begin{bmatrix} \frac{d\theta}{d|\boldsymbol{V}|} \end{bmatrix} \quad \Rightarrow \quad \begin{bmatrix} \frac{d\theta}{d|\boldsymbol{V}|} \end{bmatrix} = \begin{bmatrix} \frac{\partial \boldsymbol{P}}{\partial \boldsymbol{\theta}} & \frac{\partial \boldsymbol{P}}{\partial |\boldsymbol{V}|} \\ \frac{\partial \boldsymbol{Q}}{\partial \boldsymbol{\theta}} & \frac{\partial \boldsymbol{Q}}{\partial |\boldsymbol{V}|} \end{bmatrix}^{-1} \begin{bmatrix} \frac{d\boldsymbol{P}}{d\boldsymbol{Q}} \end{bmatrix}$$

I cambiamenti delle tensioni e delle loro fasi in relazione alle variazioni di potenza (attiva e reattiva) sono quindi date dalla matrice Jacobiana $[\mathbf{J}]^{-1}$ [5].

Notazioni ed equazioni di flusso per la potenza

Si consideri una rete con n bus. Sia il vettore $\boldsymbol{S}_{(\boldsymbol{\theta},\boldsymbol{V})} = [\boldsymbol{\theta}, \boldsymbol{V}]^{\boldsymbol{T}}$, il vettore colonna delle ampiezze e degli angoli dei *bus* (gli angoli rappresentano gli sfasamenti tensione-corrente nella rappresentazione fasoriale). La matrice delle ammettenze del sistema è $\mathbf{G}+\mathrm{j}\mathbf{B}$. Le sensibilità delle tensioni rispetto alla potenza reattiva sono derivate dalle equazioni di flusso di potenza reale e potenza reattiva al *bus* i-esimo date da

$$P_{i,calc} = V_i \sum_{j=1}^{n} V_j \left[G_{ij} \cos\left(\theta_i - \theta_j\right) + B_{ij} \text{sen}\left(\theta_i - \theta_j\right) \right]$$

$$Q_{i,calc} = V_i \sum_{j=1}^{n} V_j \left[G_{ij} \text{sen}\left(\theta_i - \theta_j\right) - B_{ij} \cos\left(\theta_i - \theta_j\right) \right]$$

Considerando

$$\Delta p_i = P_{i,calc} - (P_{i,gen}, P_{i,load})$$

$$\Delta q_i = P_{i,calc} - (Q_{i,gen}, Q_{i,load})$$

Il bilancio di potenza viene espresso dal vettore $\boldsymbol{f}_{(p,q)} = [\Delta \boldsymbol{p}, \Delta \boldsymbol{q}]^T$.

Variabili di stato delle sensibilità

Calcolando la matrice Jacobiana del flusso di potenza e ricavandone il negativo del suo inverso, si ottiene una matrice che descrive come cambiano le variabili di stato θ, V in relazione allo sfasamento introdotto dagli inserimenti di potenza nel *bus*

$$\Delta \boldsymbol{s}_{(\theta,V)} = [-\boldsymbol{J}]^{-1} \boldsymbol{f}_{p,q}$$

Sia $\boldsymbol{Q_s}$ il vettore riga degli inserimenti di potenza reattiva di una certa rete in ogni bus ($Q_{s,i} = Q_{i,gen} - Q_{i,load}$).
La sensibilità del vettore riga ampiezze di tensione $\boldsymbol{V}$ rispetto al vettore riga $\boldsymbol{Q_s}$ è data dalla matrice blocco $\boldsymbol{\Lambda_{VQ}}$ di $\boldsymbol{J^{-1}}$ ($\text{con } \Lambda_{ij} = \frac{\partial i}{\partial j}$)

$$[\boldsymbol{J}]^{-1} = \begin{bmatrix} \frac{\partial \boldsymbol{\theta}}{\partial \boldsymbol{P_s}} & \frac{\partial \boldsymbol{\theta}}{\partial \boldsymbol{Q_s}} \\ \frac{\partial \boldsymbol{V}}{\partial \boldsymbol{P_s}} & \frac{\partial \boldsymbol{V}}{\partial \boldsymbol{Q_s}} \end{bmatrix} = \begin{bmatrix} \boldsymbol{\Lambda_{\theta P}} & \boldsymbol{\Lambda_{\theta Q}} \\ \boldsymbol{\Lambda_{VP}} & \boldsymbol{\Lambda_{VQ}} \end{bmatrix}$$

La matrice $[\boldsymbol{J}]^{-1}$ descrive come le variabili di stato convergano ad una soluzione delle equazioni di flusso a causa di un cambiamento anche piccolo nell'inserimento di potenza reattiva in un *bus*.

2.3 Un metodo per il controllo delle tensioni

La problematica del controllo di tensione

Detto M il numero di tensioni dei carichi di un *bus* e usando la rappresentazione fasoriale (ogni tensione viene rappresentata col suo vettore $\boldsymbol{V}$ che indica ampiezza e fase della stessa), la funzione che esprime la somma delle differenze tra le tensioni assunte effettivamente dai carichi del *bus* e le tensioni nominali di tali carichi è data da (qui nel caso del *bus* 1)

$$\boldsymbol{f_1} = \sum_{i=1}^{M} [\boldsymbol{V} - \boldsymbol{V}_{nom}]_i^2 = \sum_{i=1}^{M} [\boldsymbol{\eta}_i]^2$$

La problematica del controllo delle tensioni si incentra sulla minimizzazione di $\boldsymbol{f_1}$in base alle limitazioni del flusso di potenza imposti dal sistema utilizzato. In tal modo l'obbiettivo è quello di configurare un *bus Q-C* in modo tale che abbia un profilo di tensione il più vicino possibile al profilo nominale dichiarato. Il metodo che verrà qui utilizzato per tale ottimizzazione è lo "*steepest descent approach*".

Il metodo del gradiente (*steepest descent*)

Il metodo del gradiente è il più semplice dei metodi *line search* anche se risulta il più lento dal punto di vista computazionale.
Data una generica funzione $f: \mathbb{R}^n \rightarrow \mathbb{R}$, il gradiente di quest'ultima è

$$\nabla f(x_k) = \left(\frac{\partial f}{\partial \xi_1}(x_k), \dots, \frac{\partial f}{\partial \xi_n}(x_k)\right)$$

ξ_i è inteso come l'i-esimo componente di *f*. Si ha che al passo k-esimo i metodi *line-search* hanno un'iterazione definita come

$$x_{k+1} = x_k + \alpha_k e_k$$

$$f(x_k + \alpha_k e_k) = \min_{\alpha \geq 0} f(x_k + \alpha_k e_k)$$

Siccome il gradiente definisce la massima variazione positiva della funzione, si ha che la massima discesa della stessa è data da $-\nabla f(x_k)$.
Detta ora $g_k := \nabla f(x_k)$, il metodo definisce $e_k = -g_k$ e quindi si ottiene

$$\frac{df}{de_k}(x_k) = \nabla f(x_k) e_k$$

In pratica tale metodo, preso un punto x_k, esegue una ricerca nella funzione inversa del gradiente $-g_k = -\nabla f(x_k)$.

Determinazione dei *Q-C buses*

Le sensibilità delle tensioni rispetto alla potenza reattiva possono essere usate per identificare i *bus* le cui iniezioni di potenza reattiva hanno una notevole influenza sulle tensioni di interesse. Tali *bus* identificati dalle sensibilità sono candidati ad essere appunto dei *Q-C buses.* Utilizzando il *steepest descent approach* per l'ottimizzazione di f_1, le sensibilità alla potenza reattiva di tale funzione sono date dal vettore riga sensibilità

$$\nabla \boldsymbol{f}_1 = 2\boldsymbol{\eta}\boldsymbol{\Lambda}_{\mathbf{VQ}} \qquad \text{dove} \quad \boldsymbol{\eta} = \boldsymbol{V} - \boldsymbol{V}_{\boldsymbol{nom}}$$

E' chiaro che i *bus* con sensibilità maggiore consentiranno un miglior controllo sulle tensioni.
I candidati ad essere dei *Q-C buses* vengono determinati scegliendo i *bus* che hanno la maggiore ampiezza di sensibilità per la funzione $\boldsymbol{f_1}$ considerata. Corrispondono quindi alle k posizioni più efficaci corrispondenti ai k elementi del vettore sensibilità $\nabla \boldsymbol{f_1}$ che sono più lontane dallo zero.

Classificazione dei carichi

E' possibile operare una classificazione dei carichi della rete in base alle loro componenti reattive. Visto che i sistemi di potenza hanno molti bus di carichi, una tale classificazione agevola la schematizzazione in differenti livelli di capacità di controllo reattivo agevolando l'identificazione dei *Q-C buses.* Verrà indicata come CAT1 la categoria più controllabile (quindi con una maggior componente reattiva) e CATN la categoria non controllabile affatto. I carichi con categoria più bassa (quindi i più controllabili) avranno un'attribuzione prioritaria maggiore nell'analisi per la selezione dei *Q-C buses.* Una tale

categorizzazione dei carichi sarà però dinamica, ovvero se, ad esempio, un carico di CAT1 comincia a lambire i limiti di potenza reattiva che è in grado di assorbire/fornire, passerà ad una categoria superiore.

2.4 I gruppi di supporto reattivo

Controllare le tensioni operando comandi correttivi su carichi e sorgenti richiede l'uso di comunicazioni efficienti e sicure. Risulterebbe più efficiente operare tale rete di comunicazione organizzandola in sottoinsiemi. Piuttosto che considerare ogni dispositivo della rete come una possibile destinazione per un comando reattivo, è più conveniente suddividere i dispositivi in gruppi di supporto reattivi. Tali gruppi sono composti da dispositivi scelti in modo da controllare il più possibile la tensione del nodo considerato. Si ha quindi che per ogni voltaggio viene identificato un bus di supporto. Esistono diversi algoritmi per operare tali raggruppamenti.

Identificazione dei *bus* di supporto per ogni voltaggio

Per determinare i *bus* di supporto bisogna identificare il valore con modulo maggiore (che verrà chiamato w) nella riga di $\boldsymbol{\Lambda_{VQ}}$ corrispondente ad ogni tensione. Siccome ogni riga rappresenta una tensione di *bus* e ogni colonna rappresenta un inserimento di potenza reattiva, le colonne col valore più alto per una riga danno i migliori supporti *Q-C* (*Q-C supporter*) per quelle tensioni di *bus*.

Algoritmo gerarchico di raggruppamento

Per identificare le tensioni che sono similmente influenzate dagli inserimenti di potenza reattiva, si possono raggruppare le righe di $\boldsymbol{\Lambda_{VQ}}$. Il raggruppamento gerarchico è un possibile approccio derivante dagli schemi agglomerativi. Tali schemi iniziano dal livello più basso dove ogni elemento costituisce un singolo gruppo (*cluster*) e in seguito, ad ogni avanzamento di livello, i *cluster* più vicini vengono fusi in uno solo. In tal modo, ogni livello rappresenta un grado differente di granularità tra i *cluster* e quindi più alto è il livello, più grossolano sarà il raggruppamento.
Questo algoritmo fa uso della matrice distanza $\boldsymbol{D}$ e gli elementi D_{ij} rappresentano la distanza euclidea tra la riga i e la riga j della matrice $\boldsymbol{\Lambda_{VQ}}$. Ad ogni livello vengono identificati e fusi insieme i due *cluster* più simili r e s (trovando il minimo valore $\boldsymbol{D_{rs}}$). A questo punto si cancellano le righe e le colonne corrispondenti ad r e s nella matrice distanza e si

aggiunge una nuova riga per il nuovo *cluster* (r,s). La metrica usata per determinare la distanza tra il *cluster* derivante dalla fusione di $\boldsymbol{r}$ e $\boldsymbol{s}$ e qualsiasi altro *cluster* $\boldsymbol{w}$ è

$$D_{(r,s)l} = min\left(D_{r,l}, D_{s,l}\right).$$

Algoritmo di raggruppamento Q-T (*Quality threshold*)

Anche questo metodo utilizza la matrice distanza ***D.*** Viene inizialmente specificato un limite massimo di diametro per i *cluster*. Per ogni riga di $\boldsymbol{\Lambda_{VQ}}$ si forma un cluster candidato che conterrà tutte le altre righe di $\boldsymbol{\Lambda_{VQ}}$ che sono più vicine in termini di distanza finché il diametro del cluster non raggiunge la soglia dichiarata. I cluster classificati come candidati che siano composti da un maggior numero di elementi diventeranno dei *true clusters*. Chiaramente tutti gli elementi dei *true cluster* non saranno soggetti ad altre considerazioni di selezione e il processo continuerà ad iterare finché tutti i punti non appartengano a tali *cluster*, ottenendo così un raggruppamento completo.

Algoritmo VCI (voltage coupling index)

L'algoritmo VCI opera un raggruppamento delle tensioni che reagiscono allo stesso modo alle variazioni di potenza reattiva, basato sulla metrica di similarità del coseno. In questo caso, la metrica, applicata ai vettori riga della matrice blocco delle sensibilità rispetto alla potenza reattiva, prende il nome di indice di accoppiamento della tensione (VCI). Considerando due vettori riga $\boldsymbol{\lambda_i}$,$\boldsymbol{\lambda_j}$ della matrice blocco $\boldsymbol{\Lambda_{VQ}}$ e l'angolo ϑ tra tali due vettori, il VCI è dato da

$$cos\theta_{\lambda_i\lambda_j} = \frac{\boldsymbol{\lambda_i}\boldsymbol{\lambda_j}}{\|\boldsymbol{\lambda_i}\|\|\boldsymbol{\lambda_j}\|}$$

Tale indice ha valori compresi tra -1 e 1. Quando assume valore assoluto 1, significa che l'angolo tra i due vettori è zero, e quindi c'è una correlazione totale tra i due modi in cui le due tensioni di *bus* reagiscono agli inserimenti di potenza reattiva (similarità pari a 1). Quando invece il VCI assume valore assoluto pari a zero, significa che i due vettori riga sono ortogonali tra loro e quindi non si ha alcuna correlazione tra i modi in cui le due tensioni di *bus* reagiscono agli inserimenti di potenza reattiva (similarità pari a zero).
Indichiamo con $\boldsymbol{K}$ una matrice**,** dove K_{ij} fornisce il VCI tra le righe i e j. L'algoritmo identifica per ogni linea di $\boldsymbol{K}$ tutte le tensioni che sono accoppiate da un VCI con ampiez-

za maggiore di una soglia stabilita. Il *cluster* così formato (che chiameremo A_i) verrà denotato come *cluster* debole. In seguito, si identificheranno le tensioni nelle righe di $\boldsymbol{K}$ date dagli elementi di A_i che siano inferiori al limite dichiarato in precedenza e si porranno in un cluster che chiameremo A_j. Gli elementi in comune tra A_i e A_j verranno raggruppati in un *cluster* detto *cluster* forte (è ovviamente possibile che un bus non appartenga a nessun *cluster* forte e saranno quindi considerati come *cluster* deboli con un solo elemento). Dopo tali raggruppamenti si avrà quindi che le tensioni nei *cluster* forti saranno degli ottimi candidati per i gruppi di supporto reattivi.

Approccio ibrido

E' chiaro che il modo più preciso e ottimale per scegliere i gruppi di controllo delle tensioni è una combinazione degli algoritmi sopra elencati. Ad esempio l'algoritmo VCI può essere applicato in principio per determinare i candidati ottimali da sottoporre poi all'algoritmo gerarchico di raggruppamento [6].

2.5 Casi test per il controllo della potenza reattiva

Verranno di seguito mostrati degli esempi applicativi sulle metodologie viste sopra, in particolare sulla scelta dei *Q-C buses* e su come possano essere controllati per incrementare il profilo di tensione (inclusa quindi la costruzione dei gruppi di supporto reattivo).

Test di sistema sull'affidabilità della linea (*IEEE 24-BUS RTS-Reliability Test System*)

Verrà preso come modello il sistema di trasmissione IEEE 24-Bus. Tale modello fornisce i valori di carico per ogni ora con una durata totale di un anno. Il sistema di generazione contiene 32 unità con una potenza generata nell'intervallo 12-400MW. Il sistema di trasmissione in questione contiene 24 bus di carico/generazione interconnessi da 38 linee alimentate da due voltaggi di 138 e 200kV [7]. L'RTS ha bassa tensione nei bus. Supponendo che la controllabilità dei carichi possa essere suddivisa in categorie, considero solo due categorie: CAT1 (carichi completamente controllabili) e CAT3 (carichi non affatto controllabili). Come già enunciato, tali categorie possono essere modificate. I carichi di CAT1 possono chiaramente essere considerati candidati ad essere dei *Q-C Buses* e saranno selezionati in base alle funzioni sensibilità discusse in precedenza. Va notato che i ca-

richi CAT2 sarebbero quei carichi parzialmente controllabili, ma per semplicità, livelli intermedi di controllabilità non verranno considerati.
Si prendono in considerazione le 4 posizioni di CAT1 più rilevanti come effettivi *Q-C Buses* per innalzare le 5 tensioni più basse ad un profilo di tensione di 1 su unità. Vengono in seguito determinate le uscite di potenza reattiva Q_{net} (in MVAr) della rete richieste per ottenere tale controllo (un $Q_{net} < 0$ indicherà la presenza di un carico reattivo, mentre $Q_{net} > 0$ indicherà una sorgente).
Una correzione sulla potenza reattiva di un numero limitato di bus può causare anche un incremento sostanziale del profilo di tensione della rete. L'uso dei soli controlli reattivi pone come principale vantaggio che quest'ultimi possono essere subito usati grazie al fatto che i dispositivi reattivi sono già presenti e installati nella rete prevenendo inoltre l'uso della dispersione dei carichi come controllo correttivo.
Nell'esempio qui considerato, si avrebbe che i 5 voltaggi più bassi si sovrapporrebbero alle 4 locazioni più controllabili. Più il sistema viene caricato e meno avverrà tale sovrapposizione visto che i bus con la tensione più bassa non saranno più di CAT1 a causa della mancanza di riserve). Ad alti livelli di carico la risposta non sarà più lineare rendendo più arduo determinare la corretta dimensione per effettuare la correzione. Ciononostante, l'approccio identificherà il supporto più efficiente da selezionare e potrebbero essere fatti aggiustamenti di tensione ulteriori, se necessari, prima che i livelli di tensione desiderati siano raggiunti.

Stima di controllo lineare

Invece di determinare come sopra i valori di Q necessari a raggiungere il profilo di tensione desiderato entro una soglia di tolleranza, è possibile usare direttamente la sensibilità per approssimare i controlli necessari, il che non richiederebbe iterazione.
L'errore sul controllo dipenderebbe dalla relazione lineare tra la potenza reattiva dei *Q-C buses* e le tensioni interessate. Portando su di un grafico le tensioni dei *bus*, si possono evidenziare le differenze tra i valori di tensione prima e dopo il controllo correttivo. Si nota come con il controllo correttivo il profilo sia sostanzialmente incrementato, ma come l'errore sia maggiore che con un'approssimazione lineare. Usando una regressione lineare infatti, l'approssimazione può essere meglio calcolata ottenendo così delle discrepanze tollerabili nella tensione finale.

Gruppi di supporto reattivo

QT	VCI- clusters forti	VCI cluster deboli
[3],[4],[5],[8],[9],[24]	[9],[11],[12]	[4][5][8]
[10],[12],[11],[17],[20]	[15],[16],[17]	[3,24],[3,15,24]
[15],[16],[19]	[16],[17],[19]	[9,10,11,12]
	[19],[20]	[15,16,17,24]
	[3],[24]	[15,16,17,19],[19,20]

Tabella 2.1: *Clusters* RTS classificati a seconda dell'algoritmo usato

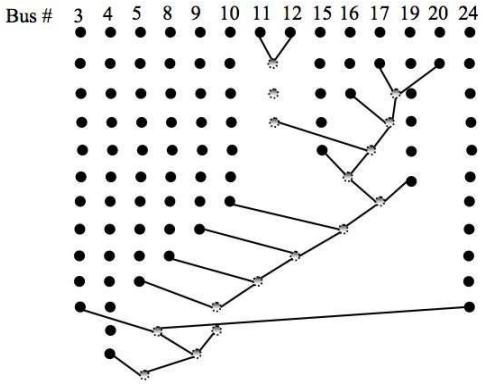


Figura 2.2: Formazione cluster secondo algoritmo gerarchico

Voltage-Coupled groups	Supporter Buses
4	[4,9,3,8,24]
5	[5,10,8,9,4]
8	[8,9,10,4,3]
10	[12,15,11,17,3]
[9,11,12]	[9,4,10,3,8]
[15,16,17]	[15,16,19,24,3]
[16,17,19]	[16,19,15,24,3]
[19,20]	[19,20,16,15,24]
[3,24]	[3,24,9,15,4]

Tabella 2.2: Bus di supporto per i gruppi di tensione

Per quanto riguarda gli schemi agglomerativi applicati alla rete a 24 *bus*, la forma dei *cluster* è quella mostrata in figura 2.2. L'algoritmo gerarchico inizialmente forma *cluster* contenenti i *bus* 11,12 ; 17,20 ecc..

Per l'algoritmo QT, posto un limite di 0,04 e un diametro massimo dei *cluster* di 5, essi risulteranno composti come in tabella 2.1.

L'algoritmo QT mostra quindi risultati simili a quello gerarchico. I bus che per ultimi si aggregano ad un cluster nel metodo gerarchico sono mostrati dall'algoritmo QT come aventi i loro personali cluster, mentre il resto dei *bus* sono divisi in 2 gruppi.

Usando l'algoritmo VCI, *cluster* forti e deboli sono mostrati nelle ultime due colonne della tabella 2.1. E' possibile che gli stessi *bus* appartengano a più cluster forti comportando una sovrapposizione delle regioni interessate. Le tensioni che non sono accoppiate sono automaticamente indicate come *cluster* deboli a sé stanti. A questo punto, basandosi sui *cluster* forti identificati con l'algoritmo VCI, si possono identificare $\boldsymbol{l}$ *bus* di supporto i quali possono essere solo di categoria CAT1. Supponendo $\boldsymbol{l}$=**5**, i migliori *bus* di supporto

per ogni regione sono identificati nella colonna 2 della tabella 2.2, ordinati secondo una scala decrescente di efficienza.

2.6 Un'infrastruttura informatica di comunicazione sicura

L'utilizzo del controllo distribuito per la potenza reattiva, richiede che lo scambio di informazioni avvenga in modo sicuro e senza ritardi. La velocità è richiesta in quanto la mole di dati da gestire è ingente, considerato che vanno supportate molte tensioni, mentre la sicurezza è chiaramente necessaria visto che i dispositivi in questione fanno parte di sistemi critici.
Due aspetti fondamentali della sicurezza in una rete informativa sono l'integrità e l'autenticità delle informazioni. Ci si riferisce quindi non solo al fatto che i messaggi inviati siano privi di errori e che non siano intercettati prima dell'effettivo recapito, ma anche che siano autentici ed effettivamente provenienti dal mittente dichiarato.
Per ottenere tali caratteristiche, è necessario l'utilizzo dei protocolli di autenticazione che definiscano standard procedurali nella verifica delle informazioni ricevute e l'istituzione di primitive di crittografia. Altro aspetto chiave è la disponibilità, intesa come reperibilità dal punto di vista comunicativo, che ogni dispositivo deve avere nei confronti dei mezzi di controllo. In tal modo si assicura che i comandi di controllo arrivino ai dispositivi interessati con i corrispettivi *feedback* come il riscontro di recapito del messaggio o verifica della integrità dello stesso. In questa sezione verranno discussi i vari approcci per l'autenticazione e la disponibilità identificando i vantaggi che essi introducono nella rete.
Verrà utilizzata una visione semplificata della rete, ovvero essa sarà schematizzata come una semplice connessione tra dispositivo di controllo e dispositivo controllato tramite connessione con nodi di commutazione intermedi (Figura 2.3). Tali nodi possono essere router (*wireless/wired*) o altri dispositivi che dispongono di tecniche di instradamento e commutazione. L'obbiettivo di un'infrastruttura siffatta è quindi quello di garantire un'autenticazione al livello *end to end* tra i dispositivi di controllo e gli elementi della rete da controllare anche nel caso in cui i nodi intermedi non siano completamente affidabili.

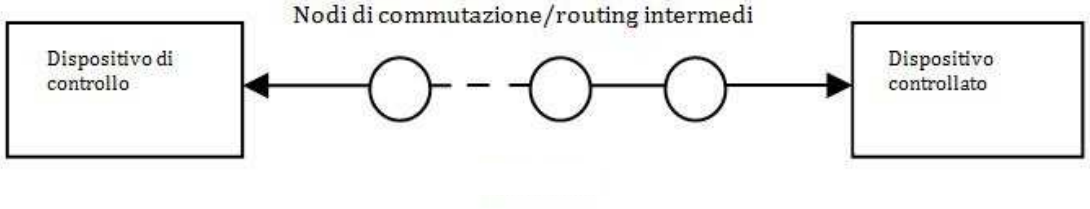


Figura 2.3: Schema connessione tra dispositivo di controllo e dispositivo controllato

Autenticazione

I meccanismi di autenticazione sono utilizzati per accertarsi che un'entità informatica sia effettivamente ciò che dichiara di essere. Tali meccanismi vengono progettati e realizzati in base agli standard internazionali ISO-IEC 9798-1 [8].

Vengono realizzati tramite mezzi crittografici come la cifratura, i sistemi crittografici simmetrici/asimmetrici e i codici di autenticazione dei messaggi. Sono mezzi studiati per fronteggiare attacchi informatici come "*man-in-the middle*" , impersonificazioni ecc.

Tali meccanismi oltretutto, provvedono a conferire utili proprietà al protocollo tramite il quale sono implementate. Un esempio di tali proprietà sono la prevenzione dalle repliche, l'aggiornamento delle informazioni e la facilitata capacità di gestione dello stato del sistema. In generale, spinti da necessità di efficienza e specifiche di sicurezza, i protocolli di autenticazione vengono principalmente costruiti sulla base di sistemi di crittografia simmetrici o asimmetrici.

Crittografia simmetrica e asimmetrica

È possibile operare una distinzione fra le varie tecniche di crittografia esistenti, basandosi sul tipo di chiave utilizzato. Si individuano, così, due categorie di sistemi crittografici: quelli a repertorio, che sostituiscono a ciascuna parola una determinata serie di lettere e numeri e quelli a cifratura letterale, che provvedono alla sostituzione di lettere (sistemi a sostituzione monoalfabetica), di gruppi di lettere (sistemi a sostituzione poligrammica), o di frazioni di lettere (sistemi tomogrammici). Sempre sulla base del tipo di chiave utilizzato, si distinguono due diversi tipi di tecniche crittografiche: quelle che richiedono l'uso di una sola chiave segreta per criptare e decriptare il messaggio, e perciò dette "simmetriche" , e quelle che utilizzano una coppia di chiavi, diverse per chiudere ed aprire il documento, di cui una viene resa pubblica, e dette allora "asimmetriche".

I sistemi di crittografia simmetrica funzionano partendo da una medesima chiave, nota solo dai suoi due utilizzatori, posseduta dall'emittente e dal destinatario di un messaggio, e che serve allo stesso tempo per la cifratura e la decifrazione del messaggio elettronico. Tale metodo è adatto soprattutto per soddisfare l'esigenza di genuinità del documento nel momento della sua conservazione nelle memorie del computer.
Nella crittografia asimmetrica invece, come detto sopra, ogni utente ha a disposizione due chiavi per proteggere il contenuto del documento che intende trasmettere: una chiave segreta, che custodisce e che gli permettere di procedere alla cifratura, seguendo dei criteri esclusivi (grazie ai quali è possibile identificare l'autore), e una chiave pubblica che egli distribuisce a tutti coloro ai quali desidera comunicare i propri messaggi cifrati. Non è necessario che le parti si scambino informazioni riservate relative al metodo di protezione del documento (e quindi la chiave simmetrica che permette l'operazione): la chiave privata infatti è destinata a rimanere segreta ed è utilizzabile dal solo legittimo titolare; l'altra chiave deve invece essere resa pubblica, con i mezzi più diversi, associandola al nome di un titolare (associazione che sarà garantita da un apposito soggetto, il cosiddetto certificatore) [9].
In definitiva, si nota come i sistemi a chiave crittografica simmetrica siano più efficienti in termini di complessità computazionale.

L'attacco M.I.T.M. (*Man In The Middle*)

La tipologia di attacco che va sotto il nome di man in the middle consiste nel dirottare il traffico generato durante la comunicazione tra due *host* verso un terzo *host* (attaccante). Durante l'attacco è necessario far credere ad entrambi gli *end-point* della comunicazione che l'*host* attaccante è in realtà il loro interlocutore legittimo. L'*host* attaccante riceve quindi tutto il traffico generato dai nodi comunicanti e si preoccupa di inoltrare correttamente il traffico verso l'effettiva destinazione dei pacchetti ricevuti. A seconda della capacità di riuscire a dirottare solo uno o entrambi i versi della connessione l'attacco verrà chiamato MITM *half duplex* o *full duplex*. Il risultato più importante però, ottenibile con la tecnica del man in the middle, è la capacità da parte di un attaccante di modificare il flusso di dati della connessione con diverse tipologie d'attacco (*sniffing, hijacking, injecting...*) [10].

L'attacco "Replay"

Uno degli attacchi più pericolosi che i protocolli di autenticazione devono fronteggiare, è il "*replay attack*". Consiste nella capacità dell'entità intrusa di catturare i messaggi e replicarli ai dispositivi interessati nella comunicazione in un successivo momento. Un tale attacco può essere prevenuto incrementando la frequenza di "rinfresco" e aggiornamento della gestione dei messaggi. Tale incremento può essere ottenuto se nel protocollo è supportata la nozione del tempo (presenza di un segnale di *clock*), attivando così la sincronizzazione dell'orologio in modo tale che i marcatori temporali (lo standard più usato è detto *UNIX Timestamp*. Esso è un numero rappresentante i secondi trascorsi dalle 00.00.00 dell'1 Gennaio 1970 fino ad un certa data. Supponendo che oggi sia il 16 luglio 2005, ore 12:42:22, il *timestamp* in questo istante è 1121510542. Questo significa che sono passati 1121510542 secondi dalla mezzanotte del 1 gennaio 1970) possano provvedere all'aggiornamento.
Altra opzione per prevenire tale attacco è l'uso di numeri sequenziali (per la determinazione di una sequenza di messaggistica precisa che eviti oltretutto la ripetizione di invio).

Disponibilità

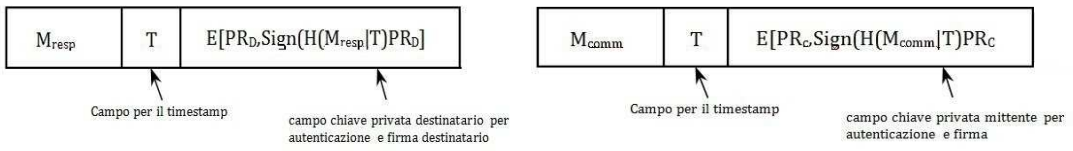
La disponibilità di sistema è un aspetto chiave da mantenere prioritario in sistemi critici quali le *Smart Grid*. In primo luogo, il sistema deve essere efficiente nell'uso dei suoi mezzi di elaborazione e comunicazione in modo che tali mezzi non arrivino ad essere sovraccaricati cosicché si possano gestire tutte le richieste provenienti dai dispositivi della rete. In secondo luogo, il sistema deve avere una buona gestione intrinseca dell'errore per assicurare una capacità di gestione dei fallimenti (ad es. messaggi corrotti).
Il sistema deve anche possedere un'adeguata ridondanza in modo tale che, se dei sottosistemi incorrono in errori o vengono compromessi, non crolla l'intera architettura. Infine, è anche necessaria la capacità di supporto di funzioni di sicurezza ausiliarie che possano essere rilasciate nel sistema informatico della rete per rilevare e rispondere a minacce come gli attacchi informatici.

Un esempio di scambio d'informazioni

Quando la tensione di un nodo comincia a lambire i limiti, i supporti reattivi devono intervenire per correggere tale deviazione. Si consideri a titolo d'esempio il sistema di figura 2.3. Tale sistema usa una chiave pubblica per quanto riguarda l'autenticazione, un marcatore temporale (*timestamp*) per ottenere un riferimento cronologico e una funzione di ripartizione per la verifica di integrità del messaggio. Il dispositivo di controllo, invia un

messaggio ad un qualsiasi nodo all'interno del gruppo di supporto reattivo del nodo con la tensione oltre i limiti prestabiliti. Il controllore intraprenderà questa comunicazione con ogni nodo di tale gruppo di supporto reattivo. Il nodo di controllo ha una sua chiave privata e una pubblica che verranno indicate rispettivamente con PR_C e PU_C e inoltre esso mantiene una lista delle chiavi pubbliche dei nodi del gruppo di supporto reattivo in questione (si suppone quindi che il sistema operi con un'architettura crittografica di tipo asimmetrico). Saranno denotate con PR_D e PU_D rispettivamente le chiavi private e pubbliche di ogni dispositivo del gruppo. Secondo l'architettura asimmetrica quindi, ogni nodo del gruppo conoscerà la chiave crittografica pubblica PU_C del nodo di controllo. È chiaro che le chiavi vengono stabilite e distribuite a priori tra i soli nodi che formano la rete di comunicazione.

Nel momento in cui il nodo controllore necessita di mandare uno specifico comando di controllo di tensione, che verrà detto M_{comm}, lo manderà tramite un testo in chiaro marcato con un *timestamp* in modo da prevenire il *replay*. Marcherà inoltre il messaggio con la sua autenticazione e manderà la "firma" al dispositivo interessato. La firma viene usata per prevenire l'attacco "man in the middle" visto che solo la chiave pubblica del controllore è in grado di decifrare il messaggio in modo appropriato e visto che la firma può essere composta solo tramite la chiave privata dello stesso nodo controllore. Inoltre il nodo destinatario del messaggio sarà in grado di decrittare il messaggio con la chiave pubblica del controllore e confrontare il messaggio così decrittato con l'*hash* $H(M_{comm}|T)$ che esso elaborerà. Se l'*hash* coinciderà con il messaggio decrittato, allora il nodo destinatario saprà che soltanto il nodo controllore può aver inviato tale messaggio e che non può essere stato né intercettato né alterato. In definitiva i campi del messaggio di richiesta comando in trasmissione e ricezione saranno così suddivisi:



Come già detto, i *timestamps* servono per assicurarsi che i messaggi non vengano inviati più volte. Quando un controllore manda il comando M_{comm} al dispositivo da controllare, manda nel campo *timestamp* il tempo registrato al momento dell'invio. Il mittente quindi memorizzerà il tempo inviato in un certa lista L_{req} di *tracker* temporali per invii in attesa di conferma. Tale lista aiuta il controllore a monitorare di quante e quali siano le richieste di comunicazione accettate ed elaborate. Quando il nodo destinatario riceve il coman-

do e il *timestamp*, risponde al comando e in seguito, comunica al controllore la sua risposta inviando lo stesso *timestamp* e registrando quest'ultimo in una lista L_{proc} di *tracker* temporali relativi a richieste già elaborate. A questo punto, quando il controllore riceve la risposta dal nodo destinatario con il relativo *timestamp* T, esso lo rimuove dalla lista L_{req}. Se il nodo destinatario in seguito, dovesse ricevere una richiesta di comando con un *timestamp* risultante già nella lista L_{proc}, esso lo ignorerà completamente [11].

Capitolo 3

Trasmissione dati nelle *Smart Grid: Powerline Communication*

3.1 Introduzione

L'implementazione delle *Smart Grid* prevede l'utilizzo di un'ingente quantità di informazioni di controllo e aggiornamento. L'efficienza, la sicurezza e l'affidabilità della rete possono essere incrementate trasformando l'attuale infrastruttura di distribuzione elettrica in un servizio interattivo tra operatori e clienti. Il maggior vantaggio nella costruzione di un sistema di comunicazione all'interno di un sistema di potenza (*powerline communication*), consiste nel fatto che l'infrastruttura fisica è già presente e vanno solo aggiunti dispositivi di controllo e comunicazione, implementando i protocolli necessari.
L'AMI (*Advanced Metering Infrastructure*) è un semplice esempio di un sistema nel quale tutti i dispositivi di rilevamento/controllo (*meter*) forniscono le informazioni necessarie al "*master head end*" entro un breve intervallo di tempo (frazioni di secondo). Le tecnologie di comunicazione nelle *smart grid* devono permettere la comunicazione interattiva e veloce del centro di controllo della rete di potenza con tutti i *meter* connessi alla rete, offrendo una visione dinamica del sistema di potenza. Implementazioni di una tale infrastruttura sono state effettuate tramite tecnologie *wireless.* Tale comunicazione *multi-user* in un sistema di potenza a basso voltaggio deve però render conto di problemi come l'elevato numero di sensori, i comportamenti tempo-varianti dei circuiti, l'alto rumore di fondo e la variazione delle topologie di rete.
Verrà prima presentato il modello di canale adottato, ovvero un modello rappresentante la variazione statistica del tempo e la selettività in frequenza dei canali. Questo modello adopererà una visione del canale secondo le configurazioni MIMO/MISO (*Multiple Input Multiple Output – Multiple Input Single Output).* In seguito verrà presentato il protocollo di comunicazione G3-PLC per le reti *powerline* che utilizza l'OFDMA (*Orthogonal Frequency Division Multiplexing)* [12].

3.2 Modello del canale

Le bande CENELEC (*Committee European de Normalization Electrotechnique*)

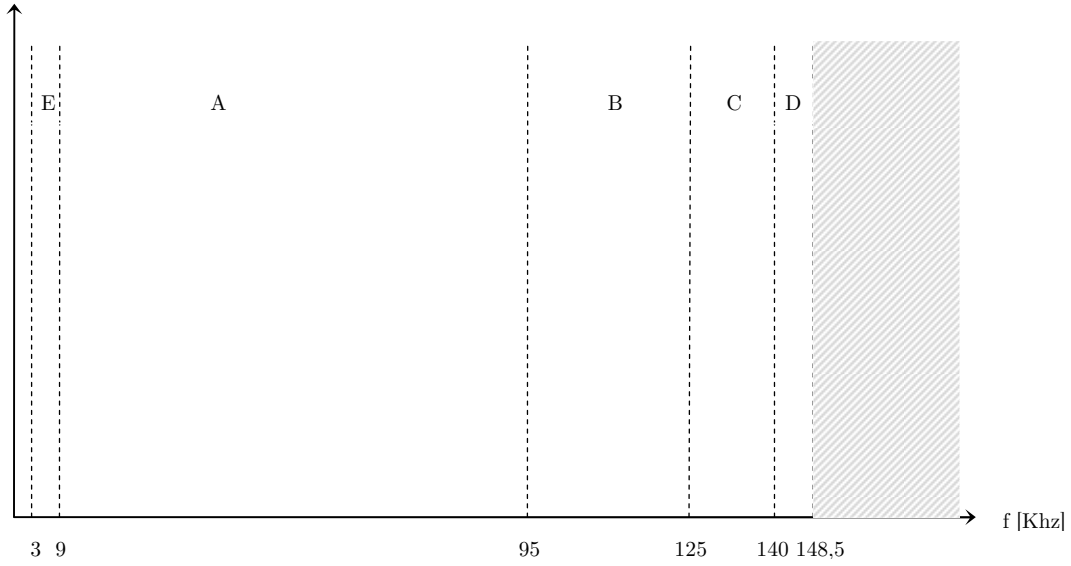


Figura 3.1: Le bande dello standard CENELEC

In Europa, gli slot frequenziali a disposizione per eventuali sistemi di comunicazione su linee elettriche a bassa tensione, sono quelli stabiliti dal CENELEC (Comitato Europeo di normalizzazione elettrotecnica, fondato nel 1973 senza scopi di lucro con sede a Bruxelles) nella normativa EN 50065-1 del 1991. Questa consiste nell'uso di un *range* di frequenze che va da 3kHz a 148,5kHz, suddiviso in 5 sottobande ognuna con scopo diverso:

1. Banda A (da 9kHz a 95kHz) ad uso esclusivo delle industrie fornitrici di energia elettrica;
2. Banda B (da 95kHz a 125kHz) per sistemi che richiedono presenza continua di canale disponibile, occasionalmente può essere utilizzata per inviare altri tipi di segnalazioni. In questa banda non è definito un protocollo di accesso;
3. Banda C (da 125kHz a 140kHz) per sistemi che funzionano a *time sharing* o a *burst,* e che quindi non occupano continuativamente il canale;
4. Banda D (da 140kHz a 148,5kHz) per sistemi di sicurezza e antincendio;
5. Banda E (da 3kHz a 8,5kHz) ancora per sistemi che usano continuativamente il canale.

Modello di canale utilizzato

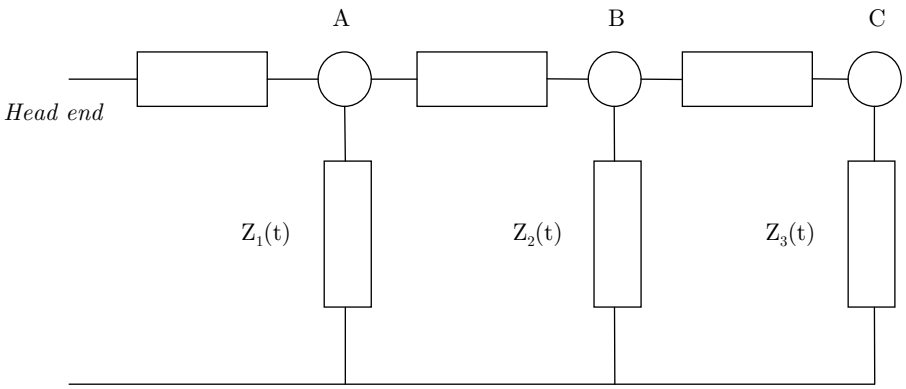


Figura 3.2 : *Bus* di rete tempo-variante (MISO)

Nella comunicazione *full duplex* di una rete, il problema chiave consiste nella tempo-varianza dei carichi. Considerando un *bus* di rete come in figura 3.2, la tempo-varianza dei carichi $Z_1(t)$, $Z_2(t)$ e $Z_3(t)$ è rappresentata denotandoli come delle variabili aleatorie.
Si supporrà che i *meter*/sensori siano in tali carichi e che quindi la loro impedenza sia compresa nell'impedenza rappresentata.
Le risposte del canale ad *A, B, C* saranno rispettivamente $H_A(f)$, $H_B(f)$ e $H_C(f)$ e si mostrerà come esse siano correlate tra loro, tempo-varianti e come mostrino in generale un *fading* non secondo *Rayleigh*.
La struttura dei *bus* avrà una topologia ad albero e l'analisi tratterà il canale sul modello MISO di comunicazione tra la radice e i nodi. Siccome ogni nodo in un albero può essere trattato come radice, la stessa analisi può essere applicata ad un canale MIMO nel quale i *meters*/sensori comunicano tra loro simultaneamente.
Si considererà anche la presenza del rumore di fondo e dei rumori d'impulso (rumore granulare) nel dominio sia del tempo sia della frequenza [13].

Il *Fading*

Il *fading* è un fenomeno in base al quale un segnale elettromagnetico, viaggiando via etere lungo percorsi continuamente variabili, giunge al ricevitore con intensità e fase discontinua. In alcuni tipi di collegamento infatti, può avvenire che tra il trasmettitore e il ricevitore sussistano contemporaneamente più percorsi elettromagnetici possibili (*multipath*), per cui il campo e.m. complessivo sul ricevitore risulta dalla somma di quelli relativi a più onde e.m., localmente piane. Sul ricevente ha quindi luogo un fenomeno di interferenza i cui effetti vanno appunto sotto il nome di *fading* (affievolimenti). Esso può dar luo-

go ad un'elevata attenuazione del segnale ricevuto rispetto al caso di normale propagazione.

Può essere determinato, ad esempio, dal continuo e lento variare delle condizioni di temperatura, umidità e pressione entro la quale avviene la propagazione. Tale fatto determina, attraverso fenomeni di riflessione, rifrazione e diffusione delle onde, la ricezione di un segnale con ampiezza e fase continuamente variabili.

Comportamento selettivo in frequenza del canale

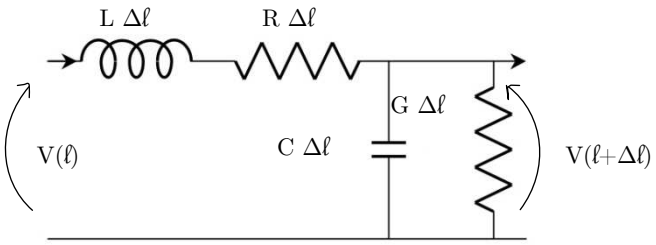


Figura 3.3: Circuito equivalente di un tratto infinitesimo di linea

Si consideri un tratto infinitesimo di una linea di trasmissione. Il modello circuitale equivalente per descrivere la propagazione dell'onda di tensione e di corrente attraverso l'elemento infinitesimo $\Delta\ell$ della linea di trasmissione è quello dato in figura 3.3. Siano *R, G, L* e *C*, rispettivamente, resistenza, conduttanza, induttanza e capacità per unità di lunghezza. Posto $\omega=2\pi f$, dove f è la frequenza, la costante di propagazione di una tale linea sarà (considerando il modello tramite impedenze con $Z_1 = R + j\omega L$ e $Z_2 = \frac{G}{1+j\omega GC}$)

$$\gamma = \sqrt{Z_1 Y_2} = \sqrt{(R + j\omega L)(G + j\omega C)} = \sqrt{RG - \omega^2 LC + j\omega(LG + CR)} = \alpha + j\beta$$

Mentre l'impedenza caratteristica Z_C sarà data dal rapporto

$$Z_c = \frac{Z_1}{Y_2} = \sqrt{\frac{R + j\omega L}{G + j\omega C}}$$

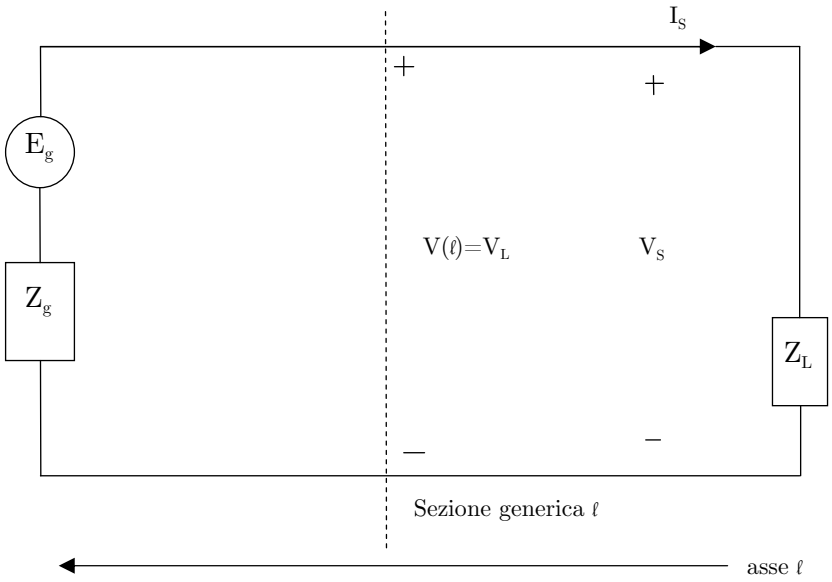


Figura 3.4: circuito equivalente rappresentante tutta la linea di trasmissione con carico e generatore ai capi

Considerando ora la linea di trasmissione nel suo complesso, essa potrà essere rappresentata dal circuito equivalente di figura 3.4.
Dalla teoria delle linee di trasmissione [14] quindi, considero il sistema di equazioni

$$\begin{cases} V_L = V_s \cosh(\gamma l) + Z_C I_S \text{senh}(\gamma l) \\ I_L = \dfrac{V_S}{Z_C} \text{senh}(\gamma l) + I_S \cosh(\gamma l) \end{cases}$$

che in forma matriciale (matrice di propagazione) è dato da

$$\begin{bmatrix} V_L \\ I_L \end{bmatrix} = \begin{bmatrix} \cosh(\gamma l) & Z_C \text{senh}(\gamma l) \\ \frac{1}{Z_C} \text{senh}(\gamma l) & \cosh(\gamma l) \end{bmatrix} \begin{bmatrix} V_S \\ I_S \end{bmatrix} .$$

L'impedenza d'ingresso risulterà quindi

$$\mathrm{Z_{in}} = \frac{\mathrm{V_L}}{\mathrm{I_L}} = \frac{\mathrm{V_s} \cosh(\gamma \mathrm{l}) + \mathrm{Z_C I_S} \text{senh}(\gamma \mathrm{l})}{\frac{\mathrm{V_S}}{\mathrm{Z_C}} \text{senh}(\gamma \mathrm{l}) + \mathrm{I_S} \cosh(\gamma \mathrm{l})} .$$

Moltiplicando e dividendo il denominatore per Z_C e dividendo ambo i membri dell'uguaglianza per I_S si otterrà la seguente espressione per l'impedenza d'ingresso

$$Z_{in} = \frac{V_L}{I_L} = Z_C \frac{\frac{V_S}{I_S}\cosh(\gamma l) + Z_C \operatorname{senh}(\gamma l)}{\frac{V_S}{I_S}\operatorname{senh}(\gamma l) + Z_C \cosh(\gamma l)} = Z_C \frac{Z_L \cosh(\gamma l) + Z_C \operatorname{senh}(\gamma l)}{Z_L \operatorname{senh}(\gamma l) + Z_C \cosh(\gamma l)} .$$

La propagazione nelle reti con topologia ad albero può essere analizzata tramite la matrice di propagazione sopra citata. In tal modo si può "propagare" con un procedimento ricorsivo l'impedenza del nodo foglia fino alla sorgente. Viceversa, i segnali dalla sorgente fino ai nodi foglia possono essere "propagati" usando la divisione tensione/corrente che verrà mostrata in seguito.

Comportamenti statistici del canale

La connessione/disconnessione dei carichi è causa del *fading* che risulta essere non di *Rayleigh* a causa della tempo-varianza degli elementi circuitali. Tale natura tempo-variante provoca comportamenti non lineari e conseguentemente, l'analisi di Fourier risulta non applicabile.

Ciononostante, se i cambiamenti non lineari sono lenti rispetto alla frequenza di interesse, è possibile un'approssimazione ad una situazione statica potendo così applicare l'analisi di Fourier.

Si consideri la propagazione del segnale attraverso un generico nodo i-esimo (con i=1, 2, ...) di un ramo della rete con topologia ad albero.

La funzione di trasferimento (complessa) $H^i(f)$ dall'*head-end* al nodo i-esimo, e l'impedenza equivalente $Z_i^{eq}(f,t)$ possono essere ricavate usando la matrice di propagazione e l'espressione per l'impedenza d'ingresso calcolata sopra.

Le relazioni tensione/corrente al nodo i-esimo (dove V^i e I^i sono appunto tensione e corrente al nodo i-esimo) sono date da

$$V^i(f) = Z_L^i(f,t) I^i(f) .$$

Sotto le ipotesi di "quasi - staticità" adottate, le impedenze saranno modellate come campione di un insieme di impedenze tempo-invarianti con una distribuzione aleatoria appropriata. Tale variabile aleatoria verrà indicata con $Z_L^{i+1}(f)$. Usando le equazioni di relazione corrente/tensione al nodo i-esimo insieme alla matrice di propagazione e

all'impedenza d'ingresso, si ha che $H^i(f)$ è data ricorsivamente in termini di funzione di trasferimento del nodo i-1esimo

$$Z_{in}^{i}(f) = \left[\frac{Z_{eq}^{i+1}(f)\cosh(\gamma l)+Z_C \operatorname{senh}(\gamma l)}{Z_C \cosh(\gamma l)+Z_{eq}^{i+1}(f)\operatorname{senh}(\gamma l)}\right]$$

$$\Rightarrow \quad H^i(f) = H^{i-1}\frac{Z_{eq}^{i}(f)}{\left(Z_{eq}^{i}(f)\cosh(\gamma l)+Z_C \operatorname{senh}(\gamma l)\right)}$$

$$Z_{eq}^{i}(f) = \frac{Z_L Z_{in}^{i}(f)}{\left(Z_L^{i}(f)+Z_{in}^{i}(f)\right)}$$

Dove $Z_{eq}^{i+1}(f)$ è l'impedenza equivalente vista verso i nodi foglia dal nodo i+1esimo (vista l'approssimazione quasi – statica tutte le impedenze usate sono tempo-varianti). L'impedenza $Z_i^{eq}(f)$ è una variabile aleatoria e di conseguenza lo è anche la funzione di trasferimento $H^i(f)$. Oltretutto, a causa della ricorsione, la risposta del canale a differenti distanze è correlata e tale correlazione dipende dalla frequenza, i canali MIMO sono quindi caratterizzati da una correlazione tra le funzioni di trasferimento di differenti rami.

Rumore del canale

La misura del rumore sulle *power lines* ha mostrato che il rumore di fondo su queste linee è colorato (detti colorati a causa del fatto che alcune componenti dello spettro sono prevalenti su altre) e che la sua PSD (*Power Spectral Density*) diminuisce con l'aumentare della frequenza. La PSD del rumore di fondo può essere approssimata con

$$N(f) = 10^{\left(K-3.95x10^{-5}\, f/Hz\right)}\left[\frac{W}{kHz}\right]$$

Dove K ha una distribuzione gaussiana con media -5.4 e deviazione standard 0,5 [15].

3.3 Sistemi OFDMA (*Orthogonal Frequency Division Multiple Access*)

OFDM - *Orthogonal Frequency Division Multiplexing*

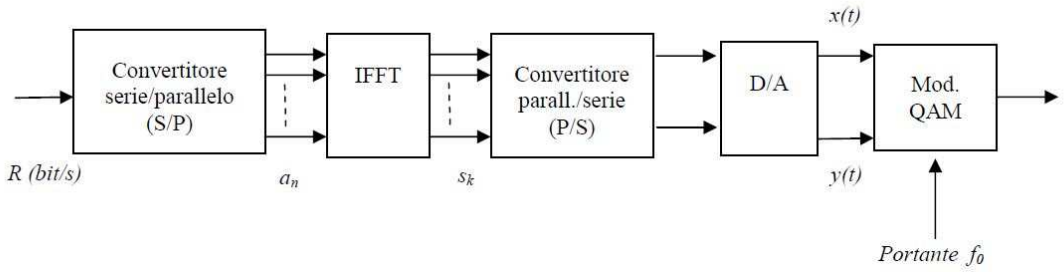


Figura 3.5: Modulatore OFDM

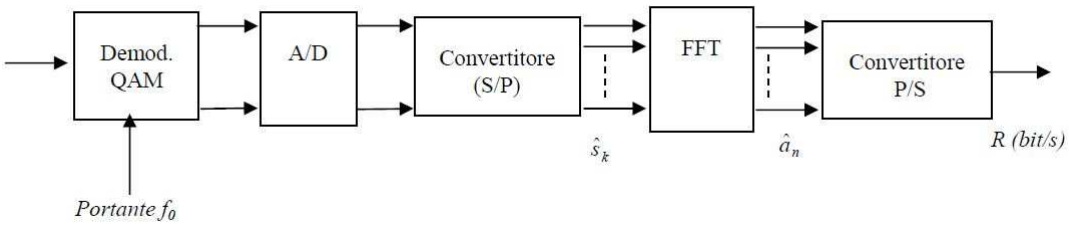


Figura 3.6: Demodulatore OFDM

La modulazione OFDM è una tecnica per trasmettere dati in parallelo utilizzando un certo numero di portanti, con una spaziatura scelta opportunamente in modo da garantire l'ortogonalità. Questa tecnica consente la trasmissione attraverso canali fortemente distorcenti di tipo *multipath*. Un segnale OFDM consiste in N sottoportanti equispaziate in frequenza di una quantità Δf. La banda portante B è quindi suddivisa in N sottocanali che vengono resi ortogonali. Se si trasmettesse l'intero flusso R su un'unica portante occupando una banda B, si avrebbe forte interferenza intersimbolica e quindi necessità di una complessa equalizzazione di canale. Trasmettendo invece N flussi ciascuno a velocità R/N in N sottobande di larghezza $\Delta f = B/N$, si può dire in prima approssimazione che la funzione di trasferimento di canale per ciascuna sottobanda può essere considerata in pratica non distorcente (se Δf è sufficientemente piccola). In un intervallo di durata T_S quindi, detta A_C l'ampiezza della portante e a_n il generico elemento del vettore dei dati $\boldsymbol{a}=[a_0, a_1, \ldots, a_{N-1}]$, l'inviluppo complesso del segnale OFDM è

$$s(t) = A_c \sum_{n=0}^{N-1} a_n \varphi_n(t)$$

Dove le portanti ortogonali sono $\varphi_n(t) = e^{j2\pi f_n t}$ con

$$0 \leq t \leq T_s \quad , \quad f_n = \frac{n}{T_s} \quad , \quad 0 \leq n \leq N-1$$

Un aspetto essenziale che rende spesso vantaggioso questo tipo di trasmissione è che può essere realizzato con grande efficienza ricorrendo a tecniche di elaborazione numerica (la trasformata di Fourier veloce FFT), che consentono notevoli riduzioni di complessità.
Nel tempo i campioni del segnale *s(t)* ad intervalli T_S/N sono:

$$s_k = s\left(k\frac{T_S}{N}\right) = \sum_{n=0}^{N-1} a_n e^{j2\pi\frac{nk}{N}}$$

In figura 3.5, l'inviluppo complesso è rappresentato dalle componenti I e Q (rispettivamente *x(t)* e *y(t)*) e i dati d'ingresso hanno un intervallo di segnalazione pari a T_S. Il convertitore serie-parallelo legge blocchi di N simboli per volta e ne mantiene il valore in uscita su N linee in parallelo (vettore $\boldsymbol{a}$) per un periodo pari a $T=NT_S$. Il blocco IFFT, il cui ingresso è il vettore $\boldsymbol{a}$, fornisce in uscita un vettore complesso **s**, contenente gli N campioni spaziati di T_S dell'inviluppo complesso del segnale modulato. Il convertitore parallelo-serie riorganizza infine tali campioni in un flusso seriale. Le componenti I e Q dell'inviluppo complesso del segnale OFDM, e cioè i segnali *x(t)* e *y(t)*, sono generate convertendo in analogico rispettivamente la parte reale e quella immaginaria di ogni campione mediante convertitore *D/A*. Il segnale OFDM è quindi ottenuto mediante un modulatore QAM, si modulano cioè in ampiezza (modulazione di ampiezza in quadratura) N sottoportanti a frequenza f_n rispettivamente con i simboli $a_0\ a_1\ .\ .\ .\ a_{N-1}$. Poiché le sottoportanti, essendo $\Delta f = 1/T_S$, sono ortogonali sull'intervallo di tempo T_S, i simboli a_n possono essere estratti senza interferenza mutua tra gli N canali in parallelo. Il segnale *s(t)* costruito con le N sottoportanti andrà poi traslato in frequenza nella banda del canale trasmissivo, mediante conversione (modulazione) su una conveniente portante di trasmissione f_0.
In ricezione la demodulazione avviene secondo i passi seguenti: si demodula la portante f_0 estraendo i segnali *x(t)* e *y(t)* (blocco demodulatore QAM); i campioni di questi, prelevati

con periodo *Ts/N* (blocco *A/D*-Analogico/Digitale) e convertiti in un flusso seriale (blocco *S/P*), determinano i valori (complessi) $\{\hat{s}_k\}$, a meno naturalmente dei disturbi; il calcolo della trasformata di Fourier FFT del blocco $\{\hat{s}_k\}$ ricostruisce i valori dei simboli d'informazione $\{\hat{a}_n\}$ (blocco FFT). Per la presenza del rumore, occorrerà effettuare un'operazione di decisione per ottenere i valori più probabili dei simboli a_n.

La tecnica OFDM consente quindi di frazionare un canale distorcente in un insieme di sottocanali paralleli non distorcenti. Si pensi, come tipico canale distorcente, al caso di presenza sul collegamento radio di "cammini" multipli quindi alla presenza in ricezione di "echi" ritardati tra loro nel tempo. La durata del simbolo OFDM (blocco di N simboli d'informazione) verrà scelta molto maggiore del ritardo relativo tra gli echi. In tal modo gli echi in pratica verranno a sovrapporsi, potendosi trascurare il ritardo relativo, e in pratica non si avrà distorsione. Per assicurare la non interferenza tra i simboli OFDM e l'ortogonalità delle sottoportanti in presenza di dispersione temporale sul canale, si inserisce tra un simbolo ed il successivo un intervallo di guardia di durata Δ pari almeno alla dispersione temporale (durata della risposta impulsiva di canale). Più precisamente, nell'intervallo di guardia si trasmette un'estensione ciclica del simbolo OFDM. Si premette cioè al blocco dei valori $\{s_k\}$ di durata $(0, T_S)$, che rappresenta l'intero gruppo di sottoportanti modulate, la copia del segmento finale di durata Δ del suddetto blocco, e si trasmette il blocco ($-\Delta$, Ts) costituito dai valori $\{s_k\}$ con l'aggiunta dell'estensione ciclica. In ricezione si utilizzano i campioni $r\left(k\frac{T_S}{N}\right)$ nell'intervallo $(0, T_S)$ ignorando il prefisso in ($-\Delta$, 0), e da essi si possono ricostruire a meno dei disturbi, mediante FFT, i valori $\{H_k a_k\}$, essendo H_k il valore della funzione di trasferimento di canale alla frequenza f_k. Si ha infatti, per la presenza del prefisso la convoluzione del segnale trasmesso *s(t)* e della risposta impulsiva di canale H è circolare e si ha quindi

$$r(t) = \sum_n H_n a_n \, e^{j2\pi f_n t} + n(t)$$

$$r\left(k\frac{T_S}{N}\right) = \sum_n H_n a_n \, e^{j2\pi\frac{nk}{N}} + n_k \ .$$

Le tecniche di accesso multiplo OFDMA

L'OFDMA (*Orthogonal Frequency Division Multiple Access*) è una tecnica di modulazione dei sistemi BWA (*Broadband Wireless Access*) ed è parte dei principali sistemi radiomobili di generazione successiva alla terza. Costituisce un caso particolare dell'FDMA (*Frequency Division Multiple Access*), quindi la separazione avviene nel dominio della

frequenza. A differenza dei tradizionali schemi di modulazione multi portante, diversi trasmettitori dell'OFDMA modulano simultaneamente diverse sottoportanti. In pratica, agli utenti non sono assegnate bande non sovrapposte in frequenza, separate da un tempo di guardia, ma vengono assegnate delle sottoportanti ortogonali. Come descritto nello standard 802.16a-2003, tale sistema offre un guadagno di 12dB nel *link-budget* del *down link* (dalla stazione base agli utenti) e di 18dB in *uplink* (dagli utenti alla stazione base), rispetto a tecniche tradizionali di accesso multiplo.
L'OFDMA rende possibile la messa in atto di *suscriber unit* (SU) con accesso a banda larga. In definitiva l'OFDMA assomiglia ad una modulazione OFDM con accesso multiplo che combina TDMA e FDMA. A differenza della modulazione OFDM la quale trasmette tutte le portanti in parallelo con la stessa ampiezza, nell'OFDMA tutte le portanti sono divise in m sottogruppi ognuno dei quali raggruppa n sottoportanti.
È adottata in vari sistemi *wireless* come *WiMax* e 3GPP per l'ottimizzazione dei diversi usi (in contemporanea) della banda disponibile e per la trasmissione dei dati da stazioni mobili alle stazioni base.
Gli schemi più usati a riguardo sono gli *interleaved OFDMA* e i *sub-band based OFDMA*.

3.4 *Standard* per le comunicazioni *powerline*: G3-PLC

L'utilizzo di una rete *powerline* per lo scambio di informazioni presenta un'agevolazione notevole: l'infrastruttura fisica già presente e funzionante. Trasmettere informazioni attraverso un canale di potenza non costituisce una dinamica ideale in quanto un canale *powerline* ha caratteristiche e parametri che variano sia col tempo che con la frequenza. Mentre le regioni ad alta frequenza presentano un *multipath-fading* significativo affiancato da ingenti attenuazioni su distanza (anche sotto i 35m), le regioni a frequenza più bassa da 20KHz a 500KHz sono particolarmente sensibili alle interferenze su banda stretta e al rumore d'impulso. Il canale *powerline* è quindi molto selettivo in frequenza. La modulazione OFDM utilizza efficientemente la banda limitata CENELEC permettendo tecniche di codifica avanzate rendendo in tal modo la comunicazione su *powerline* molto robusta.
Si è creato un largo interesse nel'utilizzo delle basse frequenze 20KHz-500KHz per le comunicazioni su *powerline* e sono stati messi in atto *standard* per la regolamentazione

dell'uso di tali frequenze. Un esempio è costituito dallo *standard* Europeo CENELEC 500065-1 citato nel paragrafo 3.2, che ha diviso lo spettro 3KHz-148,5KHz a bassa frequenza per *powerline,* in 4 differenti bande di frequenza da *A* a *D.* Negli Stati Uniti invece, l'FCC (*Federal Communications Commission*) ha allocato tutto lo spettro tra 14KHz e 480KHz ad un'unica larga banda comunemente denominata *FCC band.*
All'inizio sono stati sviluppati diversi *standard* per diversi strati fisici della rete dedicati alle comunicazioni su *powerline* basati su bande ad alta frequenza che si estendono fino a diversi MHz. Attualmente invece, sono state disposte alcune configurazioni su 3 strati fisici per l'utilizzo di comunicazioni su basse frequenze:

1. *Prime:* intese per i *modem* operanti nel *range* 42KHz-88KHz;
2. *Homeplug Command and Control:* opera a frequenze superiori ai 400KHz;
3. *G3*-PLC: intese per i *modem* operanti nel *range* 35,9KHz-90,6KHz (dove è previsto di estendere il limite superiore a 480KHz).

Caratteristiche principali del G3-PLC: Trasmettitore

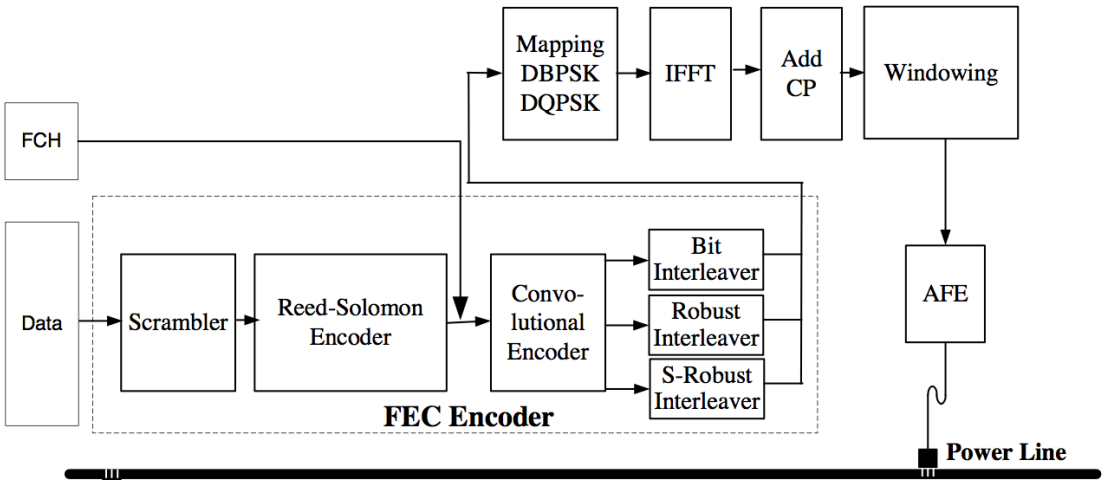


Figura 3.7: Schema a blocchi di un trasmettitore G3-PLC

Come detto sopra, lo *standard* G3-PLC supporta comunicazioni nello spettro tra 35,9kHz fino a 90,6kHz, quindi nella banda CENELEC-A con l'opzione di estendere il limite superiore a 180kHz.

Di conseguenza, la frequenza di campionamento risulta essere 400kHz in modo da avere un certo margine sotto la frequenza di Nyquist ($f_s \geq 2B$, con f_s frequenza di campionamento e B la banda del segnale) per il filtraggio dei segnali nel trasmettitore e nel ricevitore.

Viene usato il *multiplexing* OFDM con modulazione DBPSK (*Differential Binary Phase Shift Keying)* e DQPSK (*Differential Quadrature Phase Shift Keying)* rispettivamente per velocità di 1Mbps e 2Mbps. Tali schemi di modulazione vengono applicati ad ogni portante per supportare fino a 31,1Kbps di flusso dati in condizioni normali. L'uso di questi schemi di modulazione semplifica notevolmente il progetto del ricevitore visto che non è necessario un circuito di tracciamento per il rilevamento coerente della fase di ogni portante. Infatti, le fasi delle portanti nel simbolo adiacente sono usate come riferimento per il rilevamento della fase delle portanti nel simbolo corrente. Viene inoltre utilizzato un prefisso ciclico (*CP-Cyclic Prefix*) per l'intervallo di guardia in frequenza prima del blocco *AFE* (*Analog Front End*).

Il massimo numero di portati che possono essere usate è fissato a 128, con conseguente dimensione di 256 per la IFFT (*Inverse Fast Fourier Transform*), in riferimento al calcolo veloce della trasformata di Fourier discreta effettuato tramite l'algoritmo FFT appunto. Tali algoritmi di calcolo usano la tecnica *divide-et-impera* che consiste nella decomposizione ricorsiva della trasformata discreta in trasformate di dimensioni ridotte ogni volta della metà riducendo in tal modo la complessità in tempo per il calcolo.

L'utilizzo di una dimensione di 256 porta ad una spaziatura in frequenza tra le portanti OFDM pari a 1,5625kHz (f_s/N) dove N è la dimensione dell'IFFT. Di conseguenza, per ogni simbolo sono utilizzate 36 portanti.

Struttura del *frame*

Lo strato fisico (*PHYsical*) supporta due tipi di *frame* (struttura informativa):

1) ACK (*ACKnowledge) frame*

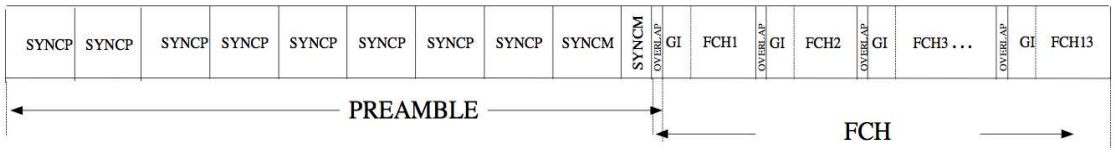


Figura 3.8: Schema campi dati *dell'ACK/NACK frame*

2) *Data frame*

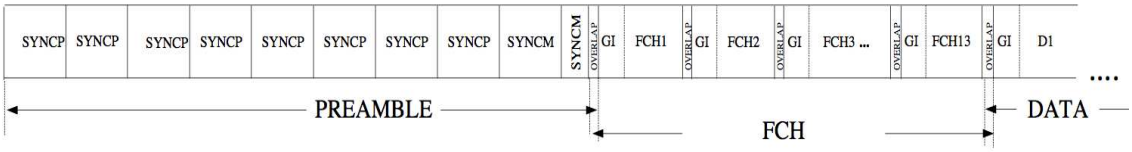


Figura 3.9: Schema campi dati del *data frame*

Preambolo

c	ϕ_c	c	ϕ_c	c	ϕ_c
0	2(π/8)	12	1(π/8)	24	13(π/8)
1	1(π/8)	13	11(π/8)	25	2(π/8)
2	0(π/8)	14	5(π/8)	26	6(π/8)
3	15(π/8)	15	14(π/8)	27	10(π/8)
4	14(π/8)	16	7(π/8)	28	13(π/8)
5	12(π/8)	17	15(π/8)	29	0
6	10(π/8)	18	7((π/8)	30	2(π/8)
7	7(π/8)	19	15(π/8)	31	3(π/8)
8	3(π/8)	20	6(π/8)	32	5(π/8)
9	15(π/8)	21	13(π/8)	33	6(π/8)
10	11(π/8)	22	2(π/8)	34	7(π/8)
11	6(π/8)	23	8(π/8)	35	7(π/8)

Tabella 3.1: Definizione del vettore di fase

Ogni *frame* inizia con un preambolo che è usato per la sincronizzazione di trama, per la localizzazione e per l'adattamento AGC (*Automatic Gain Control)*. Quest'ultimo è una proceduta automatica che consente di regolare il fattore di amplificazione in base a parametri specificati a priori. In generale viene usato per fare in modo che il segnale abbia sempre una determinata ampiezza.

SYNCP si riferisce ai simboli che sono moltiplicati per +1 nella funzione segno [16] e SYNCM invece a quelli che sono moltiplicati per -1.

Il preambolo è composto da 8 *P-symbols*, identici seguiti da 1,5 *M-symbols*. Ognuno dei simboli P e M sono di 256 campioni generati da una sequenza PN (*Pseudo Noise*). Tale sequenza è una sequenza periodica di 0 e di 1 ed è usata come mezzo per l'allargamento della sequenza di banda. I simboli P e M vengono memorizzati nel trasmettitore e trasmessi subito prima dei simboli del campo dati.

I simboli P sono usati per l'adattamento AGC, sincronizzazione dei simboli e la stima della fase iniziale di riferimento. I simboli M sono identici ai simboli P tranne per il fatto che le portanti sono sfasate di π. Al ricevitore, la distanza di fase tra i simboli P e i simboli M viene utilizzata per la sincronizzazione di trama.
Un simbolo P è generato creando 36 portanti ugualmente distanziate, con la fase di ogni portante data da Φ_C come mostrato in tabella 3.1.
Un modo per generare tale segnale è di partire nel dominio della frequenza e creare 36 portanti complesse con fase iniziale Φ_C.

Sincronizzazione

Si assuma il preambolo come un segnale periodico di periodo P e si considerino gli 1,5 M-*symbols* come un *flag* di inizio del *data stream*. Per la sincronizzazione sul preambolo si userà l'algoritmo *SC* (*Schmidl-Cox*) [17] che effettua il calcolo dell'autocorrelazione del segnale ricevuto *r(n)* (nel dominio del tempo) con traslazione di una costante *P*. Detta W la lunghezza della finestra di correlazione, l'autocorrelazione è data da

$$N(n) = \frac{1}{W}\sum_{d=0}^{W-1} r(n+d)r^*(n+d+P)$$

Ne segue che la potenza del segnale ricevuto contenuto nella finestra di correlazione W è

$$D(n) = \frac{1}{W}\sum_{d=0}^{W-1} |r(n+d+P)|^2 \ .$$

Si ricava quindi la metrica

$$M_{SC}(n) = \frac{|N(n)|^2}{\big(D(n)\big)^2} \in [0,1] \ .$$

Se tale metrica eccede un certo limite prestabilito $p^2 \in [0,1]$, viene eseguita una ricerca sul massimo di $M_{SC}(n)$ che porterà ad una stima dell'indice n_0 che andrà a rappresentare l'inizio del preambolo.
Per un $W>>P$, si può affermare che

$$\frac{|N(n)|^2}{\big(D(n)\big)^2} > p^2 \quad \Leftrightarrow \quad |N(n)| > p\, D(n) \, .$$

Al momento in cui si verifica tale disuguaglianza, quindi al superamento del limite, si può assumere di essere vicini a n_0. Per la ricerca del punto di massimo di M_{SC} è sufficiente considerare

$$\tilde{n}_0 = \arg\max_n |C(n)|.$$

Una volta determinato l'indice temporale corretto, l'*offset* di frequenza della portante $\tilde{\omega}$ può essere ottenuto dalla fase $\hat{\varphi}$ della corrispondente correlazione $C(n_0)$

$$\hat{\varphi} = \arg\big(C(n_0)\big) = \arctan\frac{\Im\{C(n_0)\}}{\Re\{C(n_0)\}}\ .$$

Attraverso la relazione

$$\tilde{\omega} = \frac{\hat{\varphi}N}{2\pi P}.$$

In definitiva, attraverso l'individuazione di picchi di massimo nell'autocorrelazione si è in grado di effettuare la sincronizzazione di tempo e di frequenza sull'inizio del simbolo di SYNCP del *preamble*, individuando poi l'inizio del campo dati grazie al *flag* di segnalazione costituito dagli 1,5 *M-symbol.*

L'FCH

Il preambolo è seguito da 13 simboli di dati allocati all'FCH (*Frame Control Header*) il quale contiene le informazioni di controllo per la demodulazione dei dati contenuti nel campo *Data*. Contiene inoltre informazioni sul tipo di *frame*, lunghezza del *frame* ecc... Negli schemi delle figure 3.8 e 3.9, il campo GI sta per *Guard Interval* che è l'intervallo contenente il prefisso ciclico che serve per diminuire la velocità di trasmissione ed aumentare la banda necessaria. Il campo FCH è protetto da un codice ridondante (*Cyclic Redundancy Check*) a 5bit CRC5 che è calcolato utilizzano un generatore polinomiale di grado 5, ovvero $G(x)=x^5+x^2+1$.

DBPSK e DQPSK

Ricordando che la forma d'onda trasmessa in una modulazione *2-PSK* è una forma d'onda del tipo

$$s_{TX}(t) = [\sum_n a[n]p(t-nT)]cos(2\pi f_0 t + \pi) \;\; \text{con} \;\; 0 < t < T$$

per evitare l'impiego di un demodulatore coerente nel ricevitore, in modo da renderlo più semplice ed economico, è possibile usare la *Differential 2-PSK (DBPSK)*. Consiste nel trasmettere (mediante una modulazione *2-PSK*), invece che la sequenza originaria di bit $\mathbf{u}_T = (u_T[n])$, una sequenza $\mathbf{u}_T' = (u_T'[n])$ ottenuta tramite un *differential precoder* il quale effettua la somma in modulo due

$$\mathbf{u}_T'[n] = u_T[n] \oplus u_T'[n-1].$$

Al ricevitore, viene recuperata la portante con un algoritmo che può introdurre un'ambiguità di fase di π. Viene in seguito effettuata la demodulazione e si ottiene la sequenza binaria ricevuta $\mathbf{u}'_R = (u_R'[n])$. Poi, invertendo la trasformazione effettuata al trasmettitore con un *differential postcoder* si ottiene la vera sequenza binaria d'informazione ricevuta

$$\mathbf{u}_R[n] = u_R'[n] \oplus u_R'[n-1].$$

La verifica del rumore consiste nell'uguaglianza $u_R'[n] = u_T'[n]$. La modulazione *DBPSK* altro non è che la modulazione *4-PSK* differenziale, ovvero la coppia di bit non codifica la fase della portante, ma la differenza di fase rispetto alla portante che codificava i due bit precedenti.

Modalità di funzionamento del sistema

Il sistema opera in tre modalità differenti: *Normal DBPSK mode, Normal DQPSK mode* e *ROBUST mode*. Nei due modi normali, la correzione dell'errore FEC (*Forward Error Correction*) è composta con un codificatore *Reed Solomon* (I codici *Reed Solomon* verranno esposti più avanti) e un codificatore convoluzionale. Nella modalità *ROBUST* invece, la FEC è composta come i *normal mode* tranne per l'aggiunta di un *Repetition Coder (RC)* che introduce 3bit di ridondanza per ogni bit di dati. È presente inoltre

un'opzione per una *Super ROBUST mode* usata per la trasmissione di FCH, che usa il codice convoluzionale combinato con RC che introduce 5bit di ridondanza per ogni bit di dati.
Il codificatore convoluzionale è un codificatore con un polinomio generatore *G=[133,171]* e una lunghezza fissa di 7. Vengono aggiunti sei zeri al campo dati per indicare la fine di trama.
Successivamente al codificatore convoluzionale è posizionato un *interleaver* che gestisce la protezione verso due tipi di errori:

- *Burst Error:* che può corrompere diversi simboli consecutivi dell'OFDM.
- Un *fade* che può compromettere alcune frequenze adiacenti per un numero abbastanza grande di simboli OFDM.

Per correggere entrambi i tipi di errori, viene applicato uno schema di *interleaving* a due dimensioni (figura 3.7) di cui una dimensione esegue *l'interleaving* dei bit nel dominio del tempo e il secondo lo esegue nel dominio della frequenza. In tal modo si previene la corruzione dei dati a causa del *fading* dipendente dalla frequenza e del rumore impulsivo.
In seguito al modulatore infine, è applicato un blocco per l'IFFT che esegue una IFFT a 256 punti e genera 256 campioni nel dominio del tempo che sono seguiti da 30 campioni di un prefisso ciclico.

Lo *scrambler*

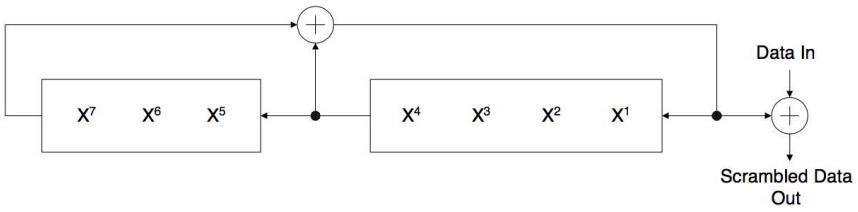


Figura 3.11: Schema a blocchi dello *scrambler*

Il blocco dati *scrambler* dà al flusso dati una distribuzione aleatoria. Viene effettuato uno XOR dello *stream* dati con una sequenza ripetuta PN la quale utilizza il generatore polinomiale $S(x)=x^7 \oplus x^4 \oplus 1$

Il blocco di *windowing*

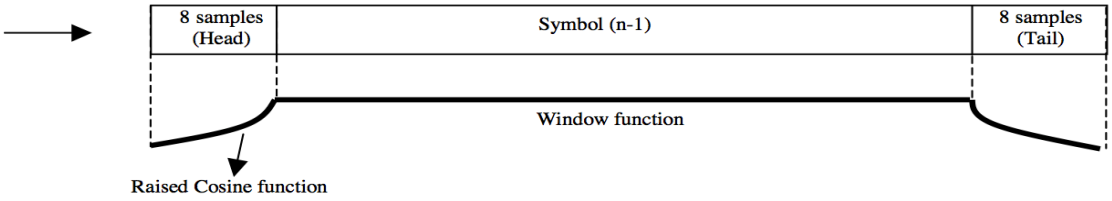


Figura 3.12: Simboli del flusso dati sagomati in base alla funzione coseno rialzato

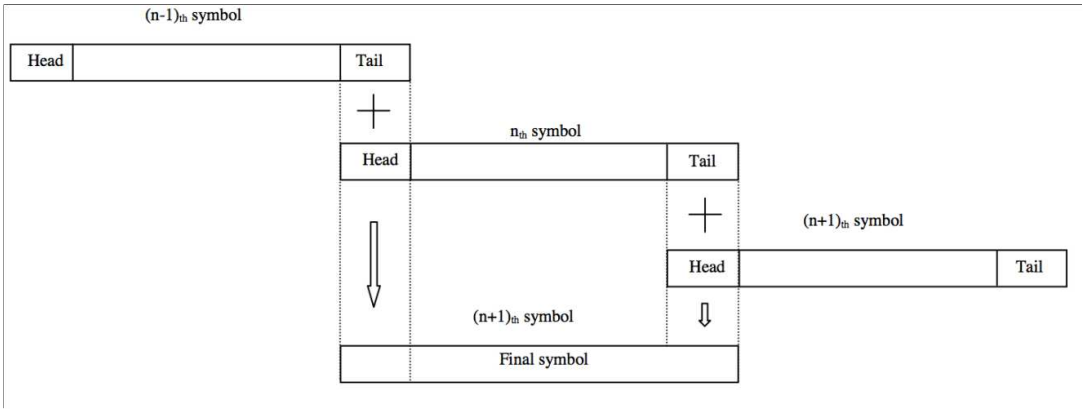


Figura 3.13: Sovrapposizione e fusione

Per ridurre le emissioni fuori banda, tutti i simboli del flusso dati vengono sagomati sul coseno rialzato. In tal modo, la testa e la coda di simboli adiacenti, vengono sovrapposte e sommate.

Ogni lato di ogni simbolo viene prima modellato sul coseno rialzato come mostrato in figura 3.12. Per costruire il simbolo n-esimo, gli 8 campioni della sua coda vengono sovrapposti agli 8 campioni della testa del simbolo successivo (n+1)-esimo ed infine i due campi sovrapposti vengono fusi insieme (figura 3.13).

Codici *Reed Solomon*

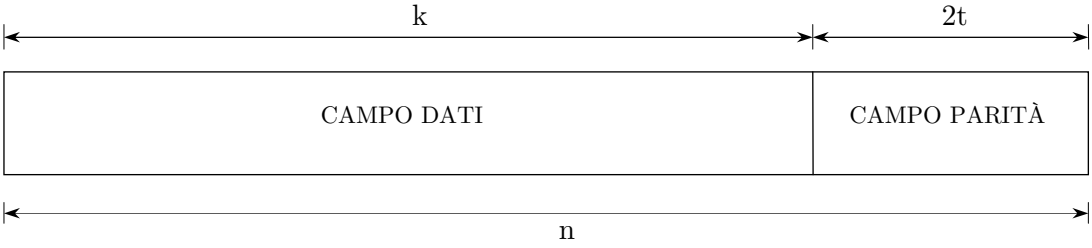


Figura 3.14: Esempio parola di codice

I *Reed Solomon (RS)* sono codici a correzione d'errore basati su codici a blocco. Un codificatore *Reed Solomon* aggiunge bit di ridondanza a un blocco dati, processando quindi ogni blocco e cercando di correggerne gli errori il cui rilevamento e correzione dipendono dalle caratteristiche del codice. Si consideri un gruppo di simboli di s bit. I dati vengono quindi suddivisi in gruppi di k bit ed a ogni blocco si aggiungono $2t$ simboli per formare una parola di codice di n bit. Dato un simbolo di dimensione s, la parola di codice può essere al massimo lunga n=2^s-1 bit.
Un decodificatore *Reed Solomon* può correggere fino a t simboli che contengono errori. Se si considera come esempio un codice RS(225,223), con s=8, significa n=255 e k=223. Il numero di bit/simbolo è pari a 8. In tal caso il decodificatore riesce a correggere fino a t=16 simboli ricevuti errati, ovvero 16 byte (ogni simbolo è rappresentato con 8bit) ovunque allocati nella parola di codice vengono corretti (in decodifica il codice riesce a correggere fino a t errori e $2t$ cancellature. Le cancellature sono i valori ritenuti non intellegibili a priori. In un sistema di comunicazione sono spesso disponibili informazioni sulla qualità del segnale in ricezione. In particolare può essere possibile sapere a priori, prima di iniziare la decodifica vera e propria dei messaggi, che alcuni simboli ricevuti sono sicuramente non affidabili. Questo corrisponde concretamente ad avere informazioni su alcune posizioni d'errore, anche se non si hanno dati su quale sia il valore effettivo che sarebbe dovuto essere ricevuto). Quando la parola viene decodificata, si possono verificare tre dinamiche:

1. Se $2s+r<2t$ (s errori e t cancellature) allora la parola di codice viene decodificata correttamente;
2. Il decodificatore riconosce che non può decifrare la parola e lo segnala;
3. Il decodificatore decodifica la parola in modo errato.

Codifica convoluzionale

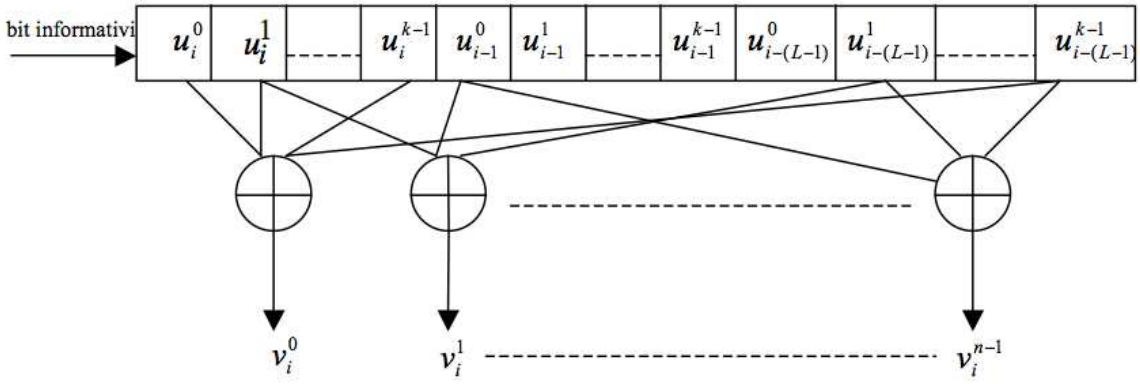


Figura 3.15: Schema generico di un codificatore convoluzionale

I codici convoluzionali sono codici a correzione d'errore che operano una specie di convoluzione sulla stringa binaria da trasmettere. Sono dotati di memoria in quanto l'influenza di un blocco di bit in ingresso si protrae sulla codifica dei blocchi successivi. La codifica consiste nel prelevare una serie di valori ottenuti da particolari operazioni effettuate su un registro a scorrimento (*shift-register*) ovvero un dispositivo elettronico formato da un clock e da n celle numerate collegate in serie. Ogni cella è in grado di memorizzare un solo bit di informazione, di avere un *input* e un *output*; il *clock* controlla il movimento del contenuto delle celle. Ad ogni impulso di *clock* il registro consente lo scorrimento dei bit da una cella a quella immediatamente adiacente (lo scorrimento può avvenire verso destra o verso sinistra a seconda del registro).

Tale codifica non necessita quindi l'uso di un sincronismo di blocco e di conseguenza è in grado di codificare messaggi molto lunghi.

I bit del codice quindi sono dati dalla somma in modulo due (dove il numero di sommatori sarà pari al numero di bit di codice) tra alcune celle dello *shift register*. I gruppi di celle che si sommeranno e il numero di bit di codice per ogni bit del messaggio, saranno dati dalla definizione a priori della funzione del codice.

La lunghezza del messaggio codificato è data dalla somma della lunghezza del messaggio originario con la lunghezza dello *shift register*.

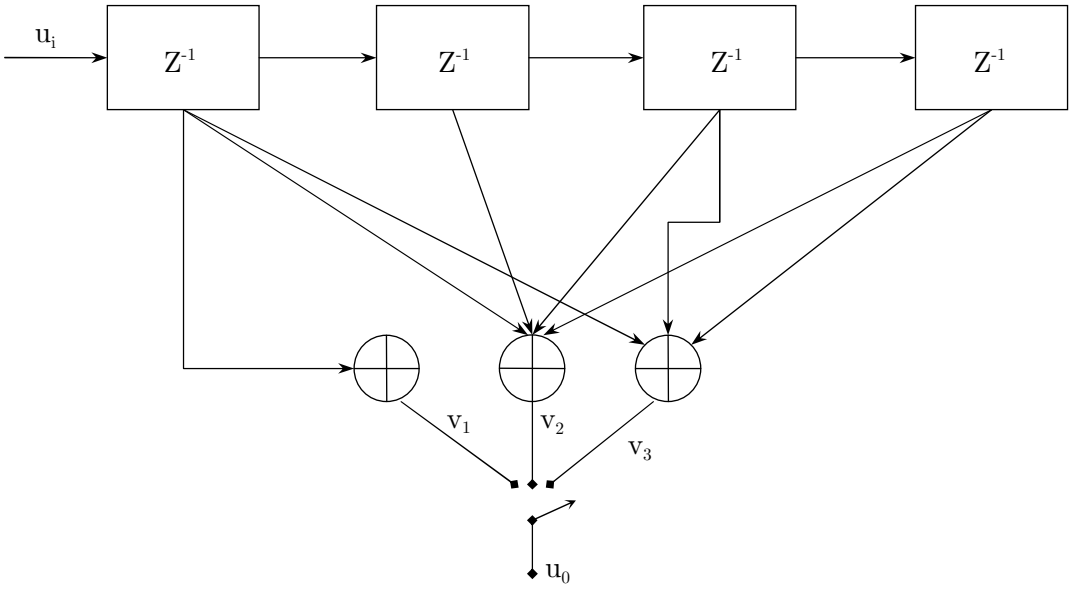
ESEMPIO: *Shift Register* a 4 stadi verso destra con prelevamento di 3 uscite (ogni bit del messaggio originario corrisponderà a 3 bit del messaggio codificato)

Specificazione:

$v_1 = s_1$

$v_2 = s_1 + s_2 + s_3 + s_4$

$v_3 = s_1 + s_3 + s_4$



Considerando come messaggio in ingresso il vettore dati **u**=[1,0,1,1,0], si ottiene:

MESSAGGIO (l=5) *SHIFT REGISTER (k=4)*

u_1	u_2	u_3	u_4	u_5	s_1	s_2	s_3	s_4					
1	0	1	1	0	0	0	0	0					
	1	0	1	1	0	0	0	0					
		1	0	1	1	0	0	0					
			1	0	1	1	0	0					
				1	0	1	1	0					
					1	0	1	1	0				
					0	1	0	1	1	0			
					0	0	1	0	1	1	0		
					0	0	0	1	0	1	1	0	
					0	0	0	0	1	0	1	1	0

Partendo dal basso e con inizializzazione dello *shift register* a zero (quindi partendo dalla penultima riga), si ottiene la codifica di 3 bit per ogni bit del messaggio (la lunghezza in bit del messaggio codificato sarà pari a $h=l+k=9$). Il vettore $\boldsymbol{c}=[c_1,c_2,c_3,c_4,c_5,c_6,c_7,c_8,c_9]$ del messaggio codificato sarà quindi ($\oplus$ indica la somma in modulo due)

$$\mathbf{c_1=(1),(1\oplus 0\oplus 0\oplus 0),(1\oplus 0\oplus 0)=111}$$
$$\mathbf{c_2=(0),(0\oplus 1\oplus 0\oplus 0),(0\oplus 0\oplus 0)=010}$$
$$\mathbf{c_3=(1),(1\oplus 0\oplus 1\oplus 0),(1\oplus 1\oplus 0)=100}$$
$$\mathbf{c_4=(1),(1\oplus 1\oplus 0\oplus 1),(1\oplus 0\oplus 1)=110}$$
$$\mathbf{c_5=(0),(0\oplus 1\oplus 1\oplus 0),(0\oplus 1\oplus 0)=001}$$
$$\mathbf{c_6=(0),(0\oplus 0\oplus 1\oplus 1),(0\oplus 1\oplus 1)=000}$$
$$\mathbf{c_7=(0),(0\oplus 0\oplus 0\oplus 1),(0\oplus 0\oplus 1)=011}$$
$$\mathbf{c_8=(0),(0\oplus 0\oplus 0\oplus 0),(0\oplus 0\oplus 0)=000}$$
$$\mathbf{c_9=(0),(0\oplus 0\oplus 0\oplus 0),(0\oplus 0\oplus 0)=000}$$

Conclusioni

Le principali problematiche da affrontare nell'implementazione delle *smart grid* sono il controllo delle tensioni, la *cyber security* e la gestione del flusso d'informazione e di controllo all'interno della rete (quindi i protocolli da adottare nelle comunicazioni su linea di potenza).

È stato visto come gli algoritmi di raggruppamento gerarchico basati sull'analisi delle sensibilità delle tensioni alla potenza reattiva siano un mezzo efficace per determinare le posizioni di controllo (inserimenti di potenza reattiva) ottimali. In questo modo è possibile selezionare i punti e la topologia più efficiente per l'inserimento della potenza reattiva coinvolgendo gruppi di *bus* che reagiscono nel medesimo modo.

Per quanto riguarda il problema della sicurezza, si è visto come si rende necessaria una crittografia sui segnali di comunicazione e controllo adoperati nelle *smart grid* vista l'esposizione informatica di strutture critiche. In particolare la crittografia asimmetrica è da preferire grazie al fatto che la chiave privata rimane nota al solo legittimo titolare nonostante la minore efficienza computazionale rispetto alla crittografia simmetrica. Quindi si è visto come si compongono i campi dei messaggi di inizio trasmissione e la metodologia sull'utilizzazione delle chiavi crittografiche.

Relativamente ai protocolli di comunicazione su linee di potenza, dopo aver presentato un modello di canale sulla base delle caratteristiche statistiche (in particolare sulla variabilità dei carichi), si è preso in esame il protocollo G3-PLC, presentandone lo schema a blocchi e passando alla descrizione di ognuno di essi. Esso utilizza una OFDM con modulazione DBPSK e DQPSK nella banda CENELEC-A, il che semplifica notevolmente la complessità del ricevitore. Quindi tale protocollo riduce il costo dell'infrastruttura necessaria, risulta robusto (grazie appunto allo strato fisico basato sull'OFDM e alla modalità ROBUST) e soprattutto sicuro, grazie al blocco FEC che utilizza una codifica *Reed Solomon* e un codificatore convoluzionale incorporando efficientemente i tre aspetti principali per le comunicazioni su linee di potenza: la *Cyber Security*, la robustezza e l'efficienza realizzativa.

BIBLIOGRAFIA

[1] "Annual Report on US Wind Power Installation, Cost and Performance Trends: 2007", May 2008, published by Energy Efficiency and Renewable Energy, Department of Energy, USA.

[2] "Forecast perspectives on U.S. Solar Market Trajectory Solar Energy Industry", U.s. DOE Solar Energy Technologies Program May 30, 2008.

[3] "Automatic Electric Load Identification in Self-Configuring Microgrids", IEEE Africon 2009, 23-25 September 2009.

[4] "Newton Raphson Power Flow Solution Employing Sistematically Constructed Jacobian Matrix" ,2nd IEEE international conference on Power and energy (PECon 08), December 1-3 2008, Johor Baharu, Malaysia.

[5] "Voltage Stability Indices for stressed power systems", IEEE transaction on power systems, Vol 8, No.1, pp. 326-335, February 1993.

[6] Rogers, K.M.; Klump, R.; Khurana, H.; Overbye, T.J., "Smart Gris, enabled load and distribuited generation as a reactive resource", Sect. II-IV, Innovative Smart Grid Technologies (ISGT), 2010. Publication Year: 2010.

[7] P.M. Subcommittee, "IEEE Realiability Test System", IEEE Transactions on power Apparatus and Systems, vol. PAS-98, no. 6, pp. 2047-2054, Nov. 1979.

[8] International Standards Organization and International Electrotechnical Commission. ISO/IEC 9798-1:1997 Information technology –Security techniques-Entity authentication-Parts.

[9] "Crittografia e Diritto" G.Ziccardi, 2003.

[10] "Man in the middle attacks", ITBH Technical white paper #2 , sept. 2002.

[11] Rogers, K.M.; Klump, R.; Khurana, H.; Overbye, T.J., "Smart Gris, enabled load and distribuited generation as a reactive resource", Sect. VI, Innovative Smart Grid Technologies (ISGT), 2010. Publication Year: 2010.

[12] G.N. Srinivasa Prasanna, Amrita Lakshmi,Sumanth. S, Vijiaya Simha, Jyotsna Bapat, and George Koomulli, "Data communication over the Smart Grid", Department of Information Technology, III TB,Corporate Innovation & Technology, NXP Semiconductors India Pvt Ltd. – Sect. I.

[13] G.N. Srinivasa Prasanna, Amrita Lakshmi,Sumanth. S, Vijiaya Simha, Jyotsna Bapat, and George Koomulli, "Data communication over the Smart Grid", Department of Information Technology, III TB,Corporate Innovation & Technology, NXP Semiconductors India Pvt Ltd. – Sect. II.

[14] M.Midrio , "Propagazione guidata".

[15] G.N. Srinivasa Prasanna, Amrita Lakshmi,Sumanth. S, Vijiaya Simha, Jyotsna Bapat, and George Koomulli, "Data communication over the Smart Grid", Department of Information Technology, III TB,Corporate Innovation & Technology, NXP Semiconductors India Pvt Ltd. – Sect. IV.

[16] "G3-PLC physical layer specifications", Electricite Reaseau Distribution France, Aug. 2009.

[17] T.M. Schmidl and D.C. Cox, "Robust frequency and timing synchronization for OFDM", IEEE Trans. Commun., vol.42, no.10, pp 2908-2914, Oct. 1994.