School of Industrial and Information Engineering

Master of Science in Nuclear Engineering

POLITECNICO
MILANO 1863

Cyber risk assessment of cyber-physical system for renewable energy application

Candidate:

Gregorio Cova
ID number: 864187

Advisor:	*Co-Advisors:*
Prof. Enrico **Zio**	Prof. Wei **Wang**

Academic Year: 2020/2021

Acknowledgements

- Voglio ringraziare il professore Enrico Zio del Politecnico di Milano, senza la cui attenzione e consigli questo lavoro non sarebbe stato possibile. Grazie per avermi incoraggiato e dato fiducia e per avermi dato la possibilità di lavorare con il Dr. Wei Wang, ricercatore e professore presso la City University of Hong Kong, ormai affezionato collaboratore.
- I would like to express my sincere thanks to Wei, a collaborator and a friend, thank you for your incredible availability and your priceless suggestions.
- Grazie alla mia famiglia, il cui affetto, vicinanza e sopportazione in periodi complicati sono stati fondamentali per il raggiungimento di questo traguardo. Siete stati la mia forza e la mia resistenza, porterò sempre nel cuore quanto avete desiderato con me questo giorno.
- Infine un sincero grazie a tutti i miei amici, solo voi sapete quanto siete stati importanti.

Abstract

Cyber-Physical Power System (CPS) coordinate the physical systems by interconnections via the cyber domain, enabling functionalities of real-time monitoring, dynamic control, and decision support. Specifically to renewable energy generation, advanced control techniques are required to support and enhance controllability and responsiveness of renewable resources – wind and solar – within electric power systems. CPS also gives rise to the new challenge that the system integrity can be compromised by accidental or intentional cyber breaches, which can lead to impacts on the supply of power, customer satisfaction, economic loss, etc. In this thesis, we propose a simulation-based framework for cyber risk assessment of CPSs for renewable energy generation, aimed at exploring the effect of cyber threats on the CPS functionality, and identifying the risk-important elements. A cost-benefit analysis, based on the Mixed Integer Linear Programming (MILP) model, is first performed to prioritize and choose the optimal time of attack, taking into account uncertainties related to the primary renewable resource availability and to the customer demand of power. Then, different operational scenario are presented to attacker choice. With respect to False Data Injection Attacks (FDIA) to the state estimators of the CPSs, attack at the assumed preferred days is simulated. Base on the Value-at-Risk measures of the system important objective functions, critical elements are identified. The proposed framework can be of help in enhancing the risk and resilience management of CPSs for renewable energy application against induced failures. For demonstration purpose, we apply the proposed framework to IEEE 30-bus test system considering both solar photovoltaic and wind turbine distributed generations. The power grid control process is considered to be compromised by specific False Data Injection Attack bypassing the bad data detection to cause catastrophic consequences of the system.

Keywords: Cyber-Physical System; Renewable energy generation; Uncertainty; FDI; Cyber Security; Mixed Integer Linear Programming; Monte Carlo; Value-at-Risk.

Sommario

Cyber-physical Power System (CPS) coordinano i sistemi di potenza grazie alla interconnessione con il cominio informatico, abilitando funzionalità come il monitoraggio in tempo reale, il controllo dinamico e supporto decisionale. Specificatamente alla produzione di energia da rinnovabili, avanzate tecniche di controllo sono richieste per supportare e migliorare la controllabilità e la reattività delle risorse rinnovabili - eolico e solare - all'interno di sistemi di potenza elettrica. CPS fa emergere nuove sfide poichè l'integrità del sistema può essere compromessa da violazioni di sicurezza o errori accidentali, che possono avere un impatto sulla produzione di potenza, soddisfazione dei clienti, perdite economiche, ecc. In questa tesi, proponiamo una procedura di simulazioni per la valutazione del rischio informatico del CPSs nella produzione di energia rinnovabile, volta a investigare gli effetti dei pericoli informatici sulle funzionalità del CPS, e identificare gli elementi importanti dal punto di vista del rischio. Un' analisi costi benefici , basata su un modello di Programmazione Linear a variabili intere miste (MILP) , è svolta in primo luogo per prioritizzare e scegliere i migliori tempi di attacco informatico, tenendo in considerazione le incertezze relative alla disponibilità di risorse primarie rinnovabili e le richieste di energia dei clienti. Successivamente sono creati scenari di attacco informatico durante i tempi preferiti calcolati, attraverso attacchi di iniezione di dati falsi (FDIA) nello stimatore di stato del CPS. Basandoci sulle misure Value-at-Risk delle funzioni di performance del sistema, vengono identifica gli elementi critici. Lo schema di lavoro proposto può essere di aiuto nel migliorare la gestione del rischio e della resilienza dei sistemi CPS nella applicazioni di energia rinnovabile contro guasti indotti. A titolo di esempio, abbiamo applicato il procedimento proposto alla rete di test IEEE 30-bus considerando produzione di energia distribuita sia da solare fotovoltaico sia da turbine eoliche. Viene così simulata la compromissione dei sistemi di controllo dei processi della rete elettrica da specifici FDIA che sorpassano il rilevatore di dati falsi per causare conseguenze catastrofiche sul sistema.

Parole chiave: Sistemi di potenza cyber-fisici ; generazione di potenza da rinnovabili ; incertezza; sicurezza informatica ; programmazione lineare a variabili intere miste; Monte Carlo ; valori di rischio.

Estratto

Motivazioni e Problema

Le reti elettriche sono sistemi complessi che devono perseguire diversi obiettivi. L'energia deve essere instradata e distribuita in modo efficiente a tutte le sottostazioni di distribuzione e tutto il processo deve essere eseguito con prestazioni elevate, rispettando il livello di affidabilità sicurezza e protezione desiderato. Per monitorare lo stato di funzionamento delle reti elettriche, dal 1970 quando è stato introdotto e viene da allora impiegato lo SCADA, "Supervisory Control and Data Acquisition" un'architettura di comunicazione e controllo di sistemi. Indispensabile per il monitoraggio e la supervisione di sistemi fisici, basata sulla comunicazione tramite sensori, dispositivi elettronici, server e computer. La rete SCADA è illustrata oltre che nella figura, dove è rappresentata la gerarchia principale di comunicazione. Il fondo è occupato dai dispositivi di campo suddivisi in sensori / attuatori e in RTU / PLC (Remote Terminal Unit e Programmable Logic Control), per i dettagli [13]. Le comunicazioni avvengono con protocolli crittografati e non crittografati, tramite cavo o wireless. Dalle sottostazioni vengono generate le informazioni che sono poi disponibili presso il Centro di Controllo per gli Operatori di Sistema grazie allo SCADA. Queste nuove funzionalità hanno aperto la strada a possibili pericoli derivanti dalla forte interconnesione informatica delle strutture, fra di loro e quando connesse a internet. Il sistema che si verrà ad analizzare in qusto lavoro è fisico ma anche interconnesso, chiamato quindi CPS, "Cyber Physical System". In questo lavoro si è voluto fare una analisi di valutazione della componenti più vulnerabili all'interno della sensoristica della rete elettrica, e l'obiettivo è creare un framework per identificare le criticità di questi componenti a causa degli effetti emergenti dell'accoppiamento del cyber-dominio con una struttura di rete ad alta penetrazione di risorse rinnovabili, in modo da evidenziare pro e contro della generazione distribuita di impianti eolici e pannelli fotovoltaici, considerando inoltre la variabilità stagionale, a fronte di scenari di attacco al sistema informatico.

Tramite *false data injection attack* FDIA, che è l'attacco che si analizzerà in questa discussione un malintenzionato potrebbe prendere il controllo dei dispositivi elettronici per sostituire i dati affidabili, relativi al sistema, con quelli adeguatamente modellati da lui stesso. Ad esempio nella figura sono indicati tre principali punti vulnerabili del CPS

relativi all'infrastruttura della rete elettrica. Un malintenzionato può manipolare il flusso di dati violando le RTU (A1), lanciando il cosiddetto attacco Man-In-The-Middle (MITM) ai collegamenti di comunicazione (A2) o accedendo direttamente al master SCADA del Control Center (A3) . Per qualsiasi punto di accesso, in questa discussione, si presume che l'autore dell'attacco ottenga il privilegio di modificare i valori di misurazione. È ragionevole considerare un attacco da A1 ad A3 in ordine crescente di difficoltà. A1, ad esempio, permette all'attaccante la modifica di poche letture dei sensori, mentre con A3 potrebbe essere molto più complicato fare breccia nel sistema a causa dei firewall e dei sistemi di rilevamento delle intrusioni (IDS) ma l'attaccante potrà finalmente cambiare la maggior parte dei dati generati z in z_a, $z_a = z + a$, essendo a il *vettore di attacco*. Il monitoraggio del sistema è fornito da un insieme di valori z presi da vari dispositivi (come RTU, menzionato sopra) posto sui componenti fondamentali della rete, come sottostazioni e linee elettriche. Lo scambio di informazioni comprende le tensioni del bus, le iniezioni di potenza reale e reattiva del bus e i flussi di potenza in entrambe le direzioni. I dati vengono trasferiti a un centro di controllo, che ha la capacità di monitorare e attuare i comandi. Le misurazioni sono così raccolte dallo *State Estimator*. Questo modulo consente il calcolo delle variabili di stato del sistema, quindi la situazione reale della rete. Va sottolineato che, una pratica ben nota nei sistemi ingegneristici è la ridondanza dei componenti per evitare il completo guasto del sistema, in questo senso solitamente sulle reti elettriche i contatori sono ridondanti. Avere ridondanza permette al modulo *State Estimation* di calcolare la *migliore stima*. La ridondanza consente il calcolo degli stati più simili allo stato reale fisico, non conoscibili dai sensori. Le misurazioni generate dai dispositivi potrebbero contenere rumore o potrebbero essere completamente sbagliate, come un guasto del sensore, quindi SE e Bad Data Detector (BDD) hanno lo scopo di trovare il **valore difettoso** e rimuoverlo. Qui viene analizzata la situazione in cui un malintenzionato vuole iniettare dati falsi nel sistema rimanendo nel frattempo inosservato.

State estimation

Le variabili di sistema sono rappresentate con il vettore colonna di *variabili di stato* $\mathbf{x} = (x_1, x_2, ..., x_n)$ e il vettore colonna delle *misurazioni*, (flusso di potenza del ramo, alimentazione del bus, angoli di tensione ecc.) $\mathbf{z}=(z_1, , z_2, ..., z_m)$, con n il numero di variabili di stato e m il numero di sensori. Questi due vettori sono fisicamente correlati e possono essere modellati da una funzione non lineare *h(...)* più un vettore di rumore che imita gli errori o l'imprecisione del sensore $\mathbf{e} = (e_1, e_3, ..., e_m)$, come segue:

$$z(\mathbf{x}) = (h_1(\mathbf{x}), h_2(\mathbf{x}), ..., h_m(\mathbf{x})) + e \tag{1}$$

Con $h_i(\mathbf{x})$ una funzione di $\mathbf{x}$. La discussione farà riferimento a un'ipotesi DC, *modello di misurazione* utilizzando l'assunzione DC è modellata da un modello di regressione lineare:

$$z(\mathbf{x}) = H(\mathbf{x}) + e \tag{2}$$

$$\min_x J(x) = [z^{meas} - H(x)]^T [R^{-1}][z^{meas} - H(x)] \tag{3}$$

Uso comune di trovare il minimo di una funzione oggetto è il porre uguale a 0 la derivata della funzione stessa, $\nabla J(\mathbf{x}) = 0$, sviluppando poi 2.6 si può ottenere ciò che segue:

$$x^{est} = [H^T R^{-1} H]^{-1} H^T R^{-1} \mathbf{z}^{meas} \tag{4}$$

Si deve notare che questa formula vale solo se $N_m > N_n$, quando le misure sono ridondanti e superano i numero di variabili di stato. Quindi x^{est} è la migliore approssimazione della stima dello stato del sistema,e può essere usate per ulteriori calcoli. Per esempio per stimare il relativo vettore delle misure più probabile $\hat{z}^{meas}$. Ora se si avvera la seguente relazione, vuol dire che misura grossolane sono state rivelate :

$$\|z - H\hat{x}\|^2 > \tau \tag{5}$$

. Una volta creato il vettore attacco esso viene inserito nel flusso di informazioni, viene elaborato dallo stimatore di stato ed infini viede dato o meno l'allarme.

OPF

Una volta che le misure corrotte hanno sorpassato il rilevatore di misure erronee, e che è stato calcolato lo stato del sistema, questo viene inviato ad un algoritmo chiamato OPF. L'algoritmo viene calcolato dallo Centro di controllo per controllare che il sistema stia effettivamente funzionando nel migliore dei modi, altrimenti darebbe il comando agli attuatori per modificare lo stato di esercizio. In realtà OPF riceve come input la potenza netta scambiata con l'esterno dalle sottostazioni, che a sua volta viene calcolata a partire dallo stato del sistema. OPF quindi calcola quale dovrebbe essere il migliore programma di produzione energetica e da comando che questo venga eseguito. Il profilo dei carichi però è diverso da quello ricevuto dal modulo che esegue l'OPF, quindi ci sara un disaccoppiamento tra domanda e generazione. Questo disaccoppiamento darà luogo ad un aumento di energia non servita ai clienti, riassunta nel parametro di performance ENS.

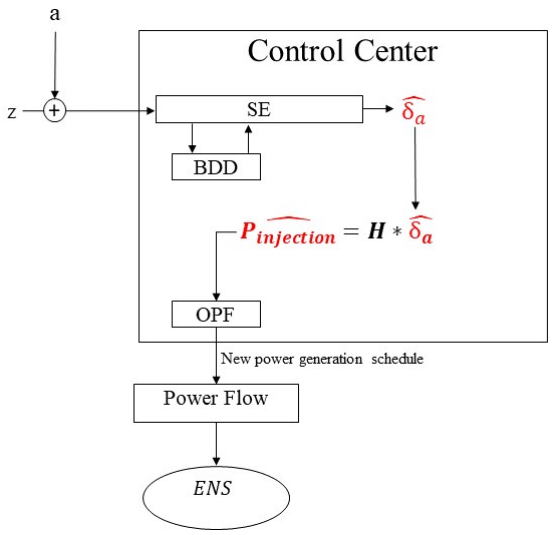


Figure 1: Effect of FDIA on power grid system.

k-Clustering and simulation

Attraverso modelli stocastici per predire l'andamento e le fluttuazione di :

- Richiesta elettrica
- Generatori tradizionali di potenza
- Potenza generata dai pannelli fotovoltaici
- Potenza generata dalle turbine eoliche
- Temperatura ambiente

con il metodo della trasformata inversa MC, vengono campionati i valori per un periodo totale di 100 anni. Ovviamente analizzare il comportamento della reta su una quantità di dati così elevata risulta troppo oneroso anche dai processori più potenti. Allora si è pensato di prendere ispirazione dall'algoritmo k-MILP, che ha l'obiettivo di raggruppare in cluster i giorni più simili tra di loro e di selezionare per ogni gruppo un rappresentante. Successivamente vengono identificati i giorni in cui si sono campionate le situazioni ambientali estreme, un giorno estremo per ogni attributo. Gli attributi sono stati selezionati con criteri di ragionevolezza su quali potessero essere i parametri più influenti sulla rete elettrica. Quindi essi sono :

- Profilo richiesta di energia.
- Irraggiamento solare.
- Velocità vento.

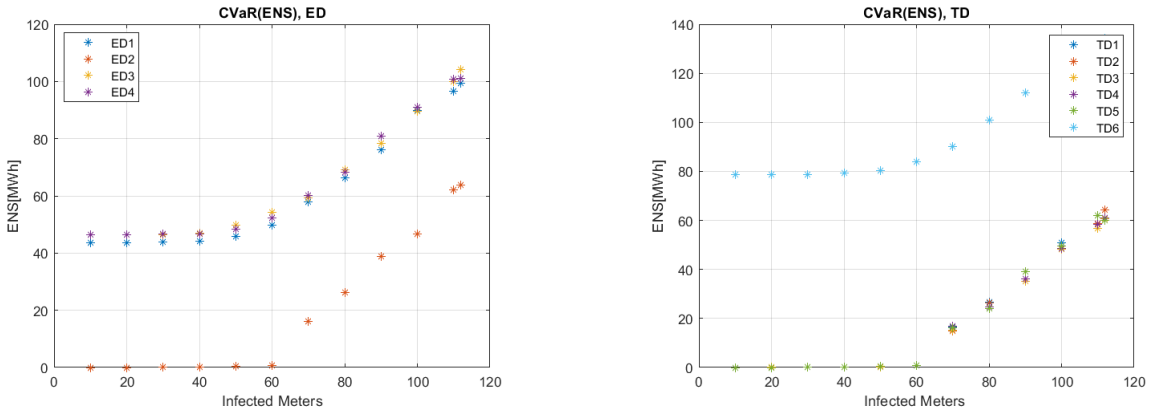


Figure 2: Risk measure CVaR trends

- Temperatura ambiente.

L'approccio tenuto in questa trattazione però prende la clusterizzazione dal punto di vista dell'attaccante. In quanto si è provato a pensare quali giorni un attaccante avrebbe provato più probabilmente ad attaccare. Non potendo asserire nessuna regola, si è pensato di sottoporre ad attacco sia i giorni molto comuni sia i giorni con condizioi estreme , per simulare attaccanti che preferisco attaccare una rete già stressata dalle condizioni atmosferiche e pure una rete in condizione nominali, in sicurezza. Per eseguire le simulazioni è stato inoltre assunto un numero di sensori controllati dall' attaccante, variabile, in modo da poter valutare la distribuizione della funzione ENS al variare della potenza dell'attaccante. Per la valutazione ci si è avvalso dell'uso di funzioni di rischio chiamate CVaR e DCVaR, spesso utilizzate nella valutazione dei portafolgi finanziari, ma applicata oggi giorno anche agli studi di ottimizzaione ingegneristici. Ecco i primi risultati : Da cui si evince che al crescere oltre i 50 sensori controllati dalla forza dell'attaccante, la funzione di Rischio CVaR inizia a salire, indicando che la media di taglio di carico, sapendo che sono nello scenario di rischio più estremo, inizia a salire. Lo scenario di rischio più estremo è stato settato sul 10% dei valori più estremi, infatti l'ulteriore funzione di rischio utilizzata qui è VaR_α, in cui $\alpha = 90\%$. Successivamente si è focalizzata l'attenzione sull'identificazione dei sensori più critici. Allora andando ad analizzare meglio l'attacco a soglia con 50 sensori, si è calcolata la frequenza con cui venivano corrotti quei sensori che portavano il valore della funzione ENS sopra il rispettivo valore CVaR. Gli istogrammi relativi a questi risultati sono mostrati qui sotto. Per una veloce visione della significatività delle frequenze di attacco sui singoli sensori, questi sono stati riassunti qui sotto, andando ad isolare i 10 maggiormente colpiti, in rosso nella figura sopra ed enumerati nella tabella seguente:

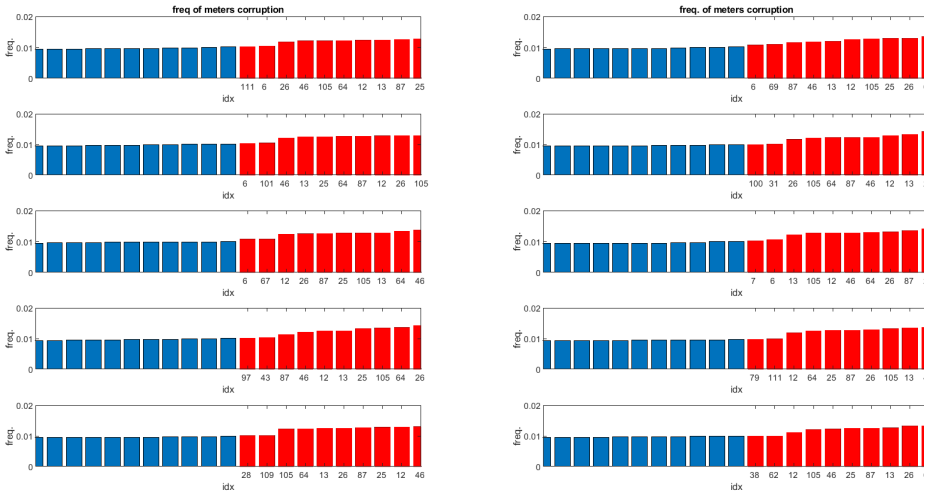


Figure 3: Histogram of the frequency of corruption for meters index

Day type	♯1	♯2	♯3	♯4	♯5	♯6	♯7	♯8	♯9	♯10
TD1)	6	12	13	25	26	46	64	87	105	111
TD2)	6	12	13	25	26	46	64	69	87	105
TD3)	6	12	13	25	26	46	64	87	101	105
TD4)	12	13	25	26	31	46	64	87	100	105
TD5)	6	12	13	25	26	46	64	67	87	105
TD6)	6	7	12	13	25	26	46	64	87	105
ED1)	12	13	25	26	43	46	64	87	97	105
ED2)	12	13	25	26	46	64	79	87	105	111
ED3)	12	13	25	26	27	28	46	64	87	105
ED4)	12	13	25	26	27	46	62	64	87	105

Contents

List of Figures

List of Tables

1

Introduction

In recent years we have seen fast development of power grids towards autonomous and intelligent systems. This is a reaction to the necessity of overtaking new challenges and needs, appeared with the development of modern society, and the availability of new advanced technology. Thanks continuous updating of the state of the art, is straighforward to understand that power system are becoming more and more complex infrastructure. The so called Cyber-Physical System (CPS) is the natural response to this transformation. New challanges like climate change and the consequent energy transition to low carbon-emission resources, the encreasing in power demand, high utilization of interconnected systems and so on, raise more requirements for the side of reiability angainst faults and security from malicious or criminal attack. With the term CPS it is outlined the tide and entwined relationship between the *physical layer* and the *cyber layer* of complex system.

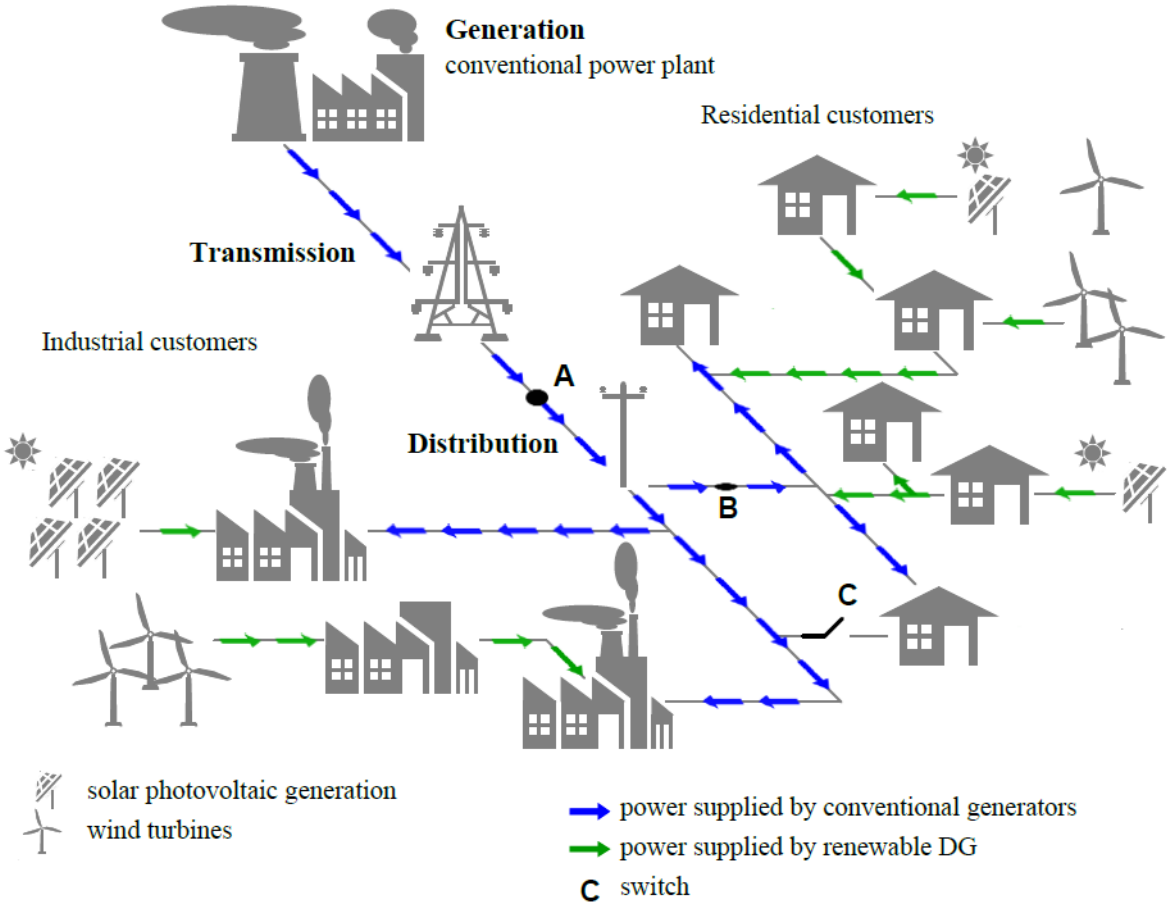
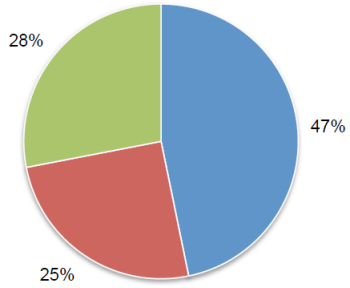


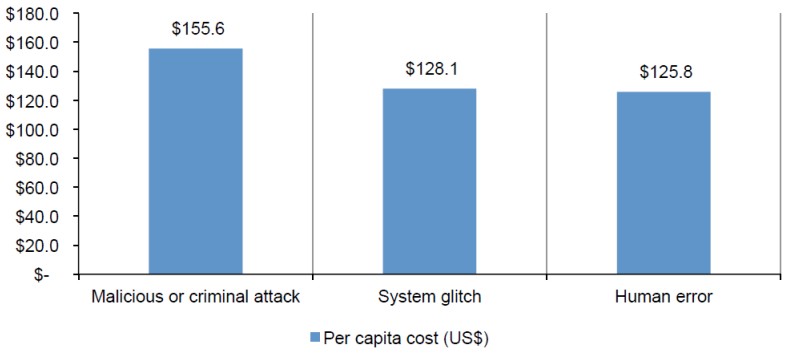
Figure 1.1: Electric Grid Area Network

Improving the communications and the interconnections of these layers improve the management of high performances and can help to address the key drivers of modern power grids, as for example the augmentation of renewables penetration. The worst scenario depicted by climate change experts is a major security challenge of the 21st century. While inaction would lead to catastrophic consequences (with implications for energy security), action also involves radical transformations affecting the global energy landscape, and the global awareness is pushing governments and energy facilities owners and stakeholders towards progressive decarbonization, reducing fossil fuel share and the reliance of global economy on them. Electricity production so is shifting from traditional generators, like gas turbine and combined Rankine cycles, to renewable resources with less environmental impact, see 1.1. Many researches have demonstrated that distributed renewable generation – e.g. wind farm and photovoltaic panels – can achieve higher performances than bulk

supply with traditional generators, and the new efficiency of renewable technology have lead local Systems Operators (SO) to augment renewables penetration and renewables investments in their design optimization projects for the portion of transmission/distribution networks under their competence. Thou implementing small distributed power generators (DGs) among the grid rise many physical problems, like voltage quality, phase angle deviation, reliable electricity provision etc. Solutions have been investigated from different works that concentrate on portfolio optimization from the point of view of DGs optimal size selection and location. The most critical factor to be addressed when talking about primary resources is the inherent uncertainty, specifically wind speed and solar irradiance, which are volatile and not regular in magnitudes. Is subsequent that the fluctuation in the power provision needs inevitably to be coped with traditional suppliers, which are constant and more reliable. Moreover, seasonal variability needs to be properly modelled to take in account peak values of seasons (heat waves or extreme cold), cumulative unreliable situation and so on, worsen by greenhouse effects. So, renewables greatly augment the importance of digitalization and the wider adoption of interconnected electroni devices have already started to affect the very notion of energy system security, with new risks and opportunities emerging. In fact, critical-infrastructure security is of most importance, weaknesses in cyber security threaten the physical side due to the deep integration of the two layers. For example the interruption of critical infrastructures system functionality , like the provision of electricity to end users in case of electric grids, can have catastrophic economic and social consequences. Real-time monitoring on field and coordination by Control Center and Corporate office is strongly required but also augment the exposure to the cyber domain which is an adjoint threat and pose new vulnerabilities to power systems. The Ponemon institute produce a detailed teport about cybersecurity concerns for organizations each year, and here to highlight the importance of cyber-intrusion are presented two results of the report from 2017, pointing out the relevance with respect to other cause of failure and the capital cost of breaches,1.2a and 1.2b. We are witness of the evolution into a smart world everywhere connected and the related risk of cyber breaches are no more negligible compared to other traditional issues. “Given the probability of a cyber breach



(a) Pie Chart 2 provides a summary of the main root causes of data breaches.



(b) Per capita cost of data breach for three root causes of the breach incidents

is nearly 100 percent, the question for executives and security professionals becomes not whether to act, but how? ...", says the Ponemon Institute and Siemens in the collaboration report 2017. SOs have to enforce the system in cybersecurity, this must be done through a combination of risk analysis and cost-benefit analyses, based on suitable models of the distribution network, but also of the conditions at the boundaries affecting the grid's components (e.g. weather phenomena). In the literature, many works focus on how to strenghten the reliability of a network through the support of local flexibility resources. In some cases, also the possibility of an islanded operation of the network is considered, in order to avoid power supply interruptions. Power plants, transmission and distribution grids, substations and consumers are able to communicate; all these agents are interconnected in LANs or WANs and can interact with each others and internet with encrypted or more often non-encrypted protocols. A common use among digitalized systems is the adoption of SCADA architecture which increase controllability and performances by supervisory controlling the operativity in time. The so-called Cyber-attack are capable of undermining or even totally disrupting the chain process in the flowstream of SCADA. Cyber-attack has resulted in many security problems in recent years and have become a critical concern for both industrial control system users and vendors. For example, in 2000, the Supervisory Control and Data acquisition (SCADA) system of the sewage control system in Maroochy Shire, Australia was compromised. In 2003, a cyber-attack penetrated a computer network at the Davis-Besse nuclear power plant in the U.S. In 2008, the public transport system in Poland was hacker remotely, while in 2010 the Stuxnet worm attacked Iran's Natanza

nuclear fuel-enrichment facility and in 2016 malware BlackEnergy intrude in Ukraine's electricity infrastructures and cause blackouts for several hours. Among these many types of attacks, we focus on the injection of false data in the system process. This is False Data Injection Attack (FDIA) against SCADA which aims at changing the values collected by control processes. By injecting false measurements in the communication network of the SCADA architecture, the Control Center is forced to believe in wrong values and so guided to take wrong decisions. Control Center usually comprehend different tasks: like Contingency Analysis and Optimal Power Flow (OPF), because of this is such a critical part. OPF, is usually run by Control Center at different time scale, 5 minuts, 15 minuts or every hour depending on the adjustment required. Control Center thanks to SCADA gathers the measurements of power loads along with energy prices, then by applying optimization algorithm is able to find the most efficent solution of generation dispatch and energy shedding in terms of economical and service reliability aspects. OPF computes the aggregated cost of running the grid, taking in consideration cost of energy production, revenues from selling power and the penalty cost for not having satisfied the demand. Furthermore the algorithm impose Energy shedding to adjust the supply-demand balance, and routing the energy in the most efficent manner. So finally an FDIA can change the power load profile and the result of Optimal Power Flow might not be correct, this is reflected in the objectives values. To exacerbate the consequences under cyber-attack, the uncertainty in the physical parameters and variables of a DG-integrated network could propagate into the operational response and raise risk of incurring in non-desirable outcomes or non-satisfactory performance. This issues demands a framework of evaluation and control both focusing on grid operation and cyber-attack side. Global Cost (GC) and Energy Not Supplied (ENS) are used here as two risk metric which aid us to understand the consequences of attacked, and their distribution are sinthetized with Risk Importance Measures. In several works various deviation and risk measures have been introduced into the DG optimization planning frameworks, framing the problem as a portfolio optimization in which the different types of DG technologies are treated analogously to financial assets. Similarly, to mean-variance approaches, and likewise derived from portfolio optimization theory direct risk base frame-

works have been formulated and applied to tackle cyber-attack problems under uncertain conditions. In particularly we state a framework for risk assessment of an electric power grid to identify most vulnerable sensors susceptible to FDIA in a context of long-term operation of the power grid using three different Risk Measures: VaR(value-at-risk), CVaR (Conditional Value-at-Risk) and DCVaR (Conditional Value-at-Risk Deviation), thanks to these index characteristics the present analysis is leaded. In this thesis work Monte Carlo base method has been used for exploring all possible scenarios for the long-term operation. Firstly, using Monte Carlo based simulation it is created a sample of 100 years of grid operation, then thanks to the k-MILP algorithm, which is a customization of the well-known k-modoids clustering thecnique, for each year we select 10 different days, 6 vey typical days and 4 for extreme weather days. It results in 1000 days to be analyzed. This allows the synthetizetion of the most salient features of the day of operation of the network and to focus our attention with false data injection attack against only the meaningful days without applying it to the overall sample space of 100 years. Moreover, by analyzing the changing in the important metrics we want to point out the critical sensors needed to launch an effective FDIA and which components are most likely be compromised, and so which components are vulnerable by the point of view of attacker. In the final part of the thesis work is the identification of the minimum set-combination of sensors that an attacker should compromise to make the grid operation unreliable. In doing so, we propose an analysis scheme to target cybersecurity efforts and strengthen defenses against cyber attacks. For demonstration purpose we apply our research to IEEE 30-bus test feeder, representing sub-transmission and distribution portion of a power grid, whose important variables can be compromised by properly shaped FDIA attacks bypassing detection and cause catastrophic consequences for the system. It is worth considering that, with the evolution of users' habits and the increasing dependence of household appliances on the electric energy dispatch, today also household customers are asking for a highly reliable power supply as well as industrial and commercial utilities. Therefore, SOs must ensure an adequate resilience of the network, with the goal to minimize the impact of cyber-attack in terms of faults occurrence and support the rapid recovery of power supply in the case of outages. To

target this aspect here it is considered different penalty-cost values, related to which consumer is not been served. Moreover, in the very end of the work for each attack magnitude included in the Risk analysis, a Interruption Risk Index (IRI) is computed. It is defined as the ratio between the number of costumers not served or not satisfied involved in the service interruption, (NUD) and the Return Time (TR) of the fault event. The index is usefull to define a merit order among grid substaions to measure their criticality with respect to the service, and also to guide investments on resilience towards right direction.

The remainder of the thesis is organized as follows:

- In Chapter 2 Introduction to FDIA and preliminary concepts adopted throughout the thesis are presented.
- In Chapter 3 Basic functioning of power grid and how a cyber attack can worsen the operations and performances.
- In Chapter 4 The algorithm of k-MILP is presented , focusing also on the Monte Carlo inverse transform to explore possible scenarios.
- In Chapter 5 the main simulation scheme and the case study are detailed.
- In Chapter 6 Some Results.
- In Chapter 7 Conclusions and future steps.

2

Problem Statement and Motivation

Power grids are complex systems which must pursue various objectives. Energy must be routed and efficently distribuited to all substations and all the process must be run with high performances, meeting the desired level of reliability safety and security. To monitor the status of operation in electric grids, since 1970 when it's been introduced, is employed SCADA, a distributed Information and Technologies (ICT) system architecture for monitoring and supervising physical systems based on communication throu sensors, electronic devices, servers and computers. SCADA network is illustrated beyonde in figure 2.1, where is represented the main hierarchy of the coomunication tree. The bottom is occupied by field devices divided in sensor/actuators and in RTU/PLC (Remote Terminal Unit and Programmable Logic Control), see for details [13]. Communications are used with encrypted and non-encrypted protocols, via wired or wireless. From substations (Remote stations)

the informations are so available at the Control Center for the System Operators, at the top of the figure, and for many other applications. It is a technology in constant evolution, hand

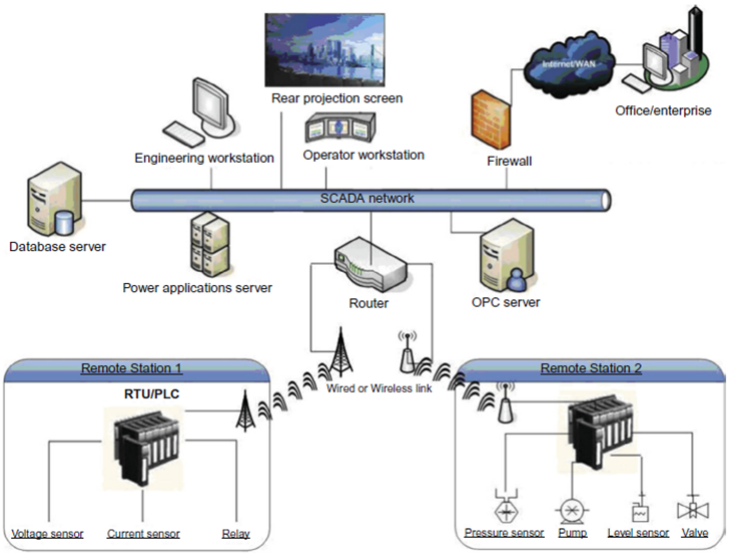


Figure 2.1: SCADA network

in hand with the progress of electronics, information technology and telecommunications networks, mainly used in the industrial and infrastructural fields. In this paper the focus is directed on the vulnerability of SCADA to cybersecurity attack and how they potentially threats the power system. Cybersecurity threats affect the capability of the Electrical Power System Operators to guarantee resilience, reliability, stability, security of supply, and power quality to the final users of electricity. Foundamentals system service at risk of cyber-attacks include:

- electricity supply;
- electricity transmission stability and reliability;
- communication between systems or equipment;
- information of the operating conditions of generation and transmission equipment ;

Moreover, some cyber-threats examples may be represented by :

- smart meters can be the access point into the power system
- trip a generator unit and change its schedule

- disrupt the proper function of the system
- cause a blackout in a big area of the grid
- attack on the electricity market
- unauthorized interference on the measurement of electricity consumption (end-users)
- attacks through the power system on civil infrastructure.

In order to identify the threats, it is important to understand the structure of the cyber domain, integrated within the power system. For such a large-scale infrastructure as power grid, the loss of pocket data via communication and faults of sensors are very frequent. Generated measurements are directed to *state estimator* which provides to the Energy Management System (EMS) and Human Operator at Control Center information that may not be correct. With the encrease of connections between SCADA and Control Center or enterprise LANs, various access points have emerged and critical grid components are potentially vulnerable from internet intrusions. The attack method here discussed is the so called *False Data Injection Attack*. It belongs to the general group of integrity attack, tampering measurements. Specifically it will be considered the most general attack, the injection of *random* values into the system. In this work it is targeted the assessment of the most vulnerable component inside the power grid structure, and the overall aim is creating a framework to identify the emerging effects of the coupling of cyber-domain with a grid structure with high penetration of renewable resources, so to highlight pro and cons of having a distributed generation system with wind turbine and photovoltaic panels, considering seasonal variability, against attack scenarios.

2.1 Cyber-Attack: FDIA

Let's introduce the Cyber Attack in analysis. With FDIA an attacker wants to take over electronics devices to start an attack of substituting reliable data,related to the system, whith properly shaped ones. For istance in the picture 2.2 are indicated three main vulnerable point of the CPPS related to power grid infrastructure. An attacker can manipulate the

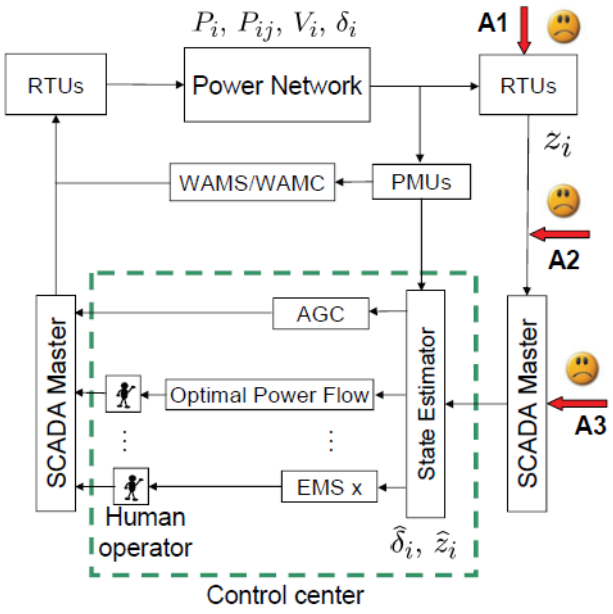


Figure 2.2: Block-diagram of Power grid CPPS

flow of data by breaching RTUs (A1), launching the so called Man-In-The-Middle attack (MITM) to communication links (A2) or by directly accessing the SCADA master of the Control Center (A3). For any access point, in this discussion, it is assumed that attacker gains the privilege to modify measurement values. It is reasonable to consider A1 to A3 attack in ascending order of difficulty. A1 for example make the attacker able to modify few sensors readings meanwhile intruding with A3 could be much more complicated due to firewalls and Intrusion Detection Systems (IDS) but he/she can finnally change most of the data available z in z_a, $z_a = z + a$, being a the *attack vector*. System monitoring is provided by set of readings z from various devices (like RTU, mentioned above) placed on the foundamentals component of the grid, such as substations and power lines. The information exchange comprehend bus voltages, bus real and reactive power injections, and power flows forward and backward. The data are transferred to a control center, which has the ability of monitoring and attuating commands. The measurements are so collected by the *State Estimator*. This module enable the computation of system state variables, hence the actual situation of the grid. It must be pointed out that , a well-know practise in engineered systems is the redundancy of components in order do avoid complete failure of the system, in this sense usually on power grids meters are redundant. Having some redun-

dancy allow *State Estimation* module to look for the *best estimate*. Redundancy allow the computation of the states most similar to the physical true state, not-knowable by sensors. Measurements generated by devices could contain noyse or could be completly wrong, like a sensor failure, thus SE and Bad Data Detector (BDD) have the scope to find the **faulty value** out and remove it. Here it is analysed the situation in which an attacker wants to inject false data in the system meanwhile remaining undetected. If the datas computed by the *State Estimation* affect negatively the output of the *SE* the resulting misinformation can hinder the *SOs* decisional capability. In fact the control center use the *SE* outcome to perform further analysis, such as Optimal Power Flow, Contingency analysis and AGC , figure 2.2. Many research have built models to detect this type of *bad measurements*, looking for methods to process and get rid of them, for example in ref. [3],[4],[6],[5]. These work focus mainly on interacting bad measurements. So if a malicious agent currupts sensors values they should be recognized by BDD in the SE, but is demonstrated that *FDIA* can bypass most of the more common detection methods.

2.2 State Estimation

To ensure the reliable operation of the grid, even in the scenario of failures, power engineers apply meters on power system to monitor important components. Considering on field meters, installed on branches or on bus connections, they control in real-time the power network. The readings taken from the field are sent to Remote Terminal Unit which are components installed at substations, able to compute several commands over the reporting of measurements to SCADA master. RTU can communicate with Control Center through wire-less channels. Based on the analysis result Control center can decide whether or not the power system is operating in fault condition. The State Estimation problem is related to the calculation of power system state variables using sensors readings. Hereafter we define and detail the process of the best state estimation. System variables are represented with the column vector of *state variables* $\mathbf{x}=(x_1, x_2, ..., x_n)$ and the column vector of *measurements* (branch power flow,bus power injection, voltage angles etc.) $\mathbf{z}=(z_1, , z_2, ..., z_m)$, with n the

number of state variables and m the number of sensors measurements. These two vectors are physically related and can be modelled by a non-linear function *h(...)* plus a noise vector which mimick the sensor errors or inaccuracy **e**=$(e_1, e_3, ..., e_m)$, as follows :

$$z(\mathbf{x}) = (h_1(\mathbf{x}), h_2(\mathbf{x}), ..., h_m(\mathbf{x})) + e \tag{2.1}$$

With $h_i(\mathbf{x})$ a function of **x**. The discussion will refer to a DC assumption,*measurement model* using DC assumption is modelled by a linear regression model :

$$z(\mathbf{x}) = H(\mathbf{x}) + e \tag{2.2}$$

Here **H** is the Jacobian matrix of the non-linear systems of equations and is a full rank matrix mxn. The purpose of the state estimation is the computation of the vector $\hat{\mathbf{x}}$, that in this case is the best estimate of the not knowable true state vector **x**, according to the model. The best estimate of the values in **x** is achieved with three different methods, which are described in the section below ,*maximum likelihood criterio,the weighted least square criterion and the minimum variance criterion*, but more detailed in ref.[7].

2.2.1 Weighted Least Square Estimation

Here it is formulated the problem of optimal *state estimation*, that is , as already mentioned, a statistical problem which aims to evaluate one or more unknown parameters starting from the observable variables. The data are always inexact, because of low accuracy or because of random noise affecting monitoring devices, hence *SE* output is also not perfect, this guide the problem in analysis. The statistical criterion are:

1. Maximum likelihood : maximize the probability that $\hat{\mathbf{x}}$ is as close as possible to the true value **x**.

2. Weighted least-square : minimize the sum of the squares of the weighted deviations of the estimated measurement $\hat{z}$ from the real measurements z.

3. Minimum variance : minimize the mean value of the sum of the squares of the devia-

tions of the estimated components of the state variable vector from the corresponding components of the true state variable vector.

When we assume meters errors normally distributed and unbiased, $e \sim N(0, \sigma^2)$, each of these criteria converge in the same formula. It is worth to say that in the physical DC-model, *true* value of z is a linear function of state variables, to modelize the reality it is added the error vector, 2.2. So the estimator look for the solution x^{est} which maximize the probability that the readings z^{meas} would occur.Referring to [7] for more details, for N_n unkown parameters using N_m measurements

$$\min_{(x_1,x_2,...,x_n)} J(x_1,x_2,...,x_n) = \sum_{i=1}^{N_m} \frac{[z_i^{meas} - h_i(x_1,x_2,...,x_n)]^2}{\sigma_i^2} \tag{2.3}$$

h_i = functional dependence of value i from state variables.

σ_i^2 = variance of the measurement index i.

J(x) = measurement residual, the objective function to be minimized.

N_m = number of indipendent measurements.

z_i^{meas} = sensor readings of index i.

The last formula 2.3 is the already mentioned *weighted least-squares estimator*. Therefore to simplify, the notation, linearizing the problem it is assumed that $h_i(\mathbf{x})$ is a linear equation and so is guaranteed a closed- form solution, hence it can be introduced the matrix formulation as:

$$\mathbf{h}(\mathbf{x}) = \begin{bmatrix} h_1(x) \\ h_2(x) \\ . \\ . \\ . \\ h_m(x) \end{bmatrix} = [H]\mathbf{x} \qquad \mathbf{z}^{meas} = \begin{bmatrix} z_1^{meas} \\ z_2^{meas} \\ . \\ . \\ . \\ z_m^{meas} \end{bmatrix} \tag{2.4}$$

on the left is the vector of the equations of linear combination of H and x, the state variable vector **x**; on the right is the vector of z^{meas}.

Moreover :

$$[R] = \begin{bmatrix} \sigma_1^2 & & & & \\ & \sigma_2^2 & & & \\ & & . & & \\ & & & . & \\ & & & & . \\ & & & & \sigma_m^2 \end{bmatrix} \tag{2.5}$$

is the covariance matrix of the measurements model. Now it can be written the following minimization problem with linear combination of matrix:

$$\min_x J(x) = [z^{meas} - H(x)]^T [R^{-1}][z^{meas} - H(x)] \tag{2.6}$$

Common use to solve a minimization problem is to impose to zero the gradient of the argument, $\nabla J(\mathbf{x}) = 0$, developing the 2.6 it can be obatained as follow:

$$x^{est} = [H^T R^{-1} H]^{-1} H^T R^{-1} \mathbf{z}^{meas} \tag{2.7}$$

It must be pointed out that this formula can hold only in the case of $N_m > N_n$, when measurements are redundant and exceed the number of state variables. So x^{est} is the best approximization of system's state, it can be used for further computation. For example it can be estimated the most probable measurements values $\hat{z}^{meas}$.

2.2.2 Bad Data Detection: Hypotheses Testing

When *State Estimator* fails to yield values compatible with the standard deviation described in[2.5], the matrix [R],it must be concluded that the set of measurement contains bad data. Bad Data Detector is a module subsequent to the State Estimator. Bad Data can be referred to gross data caused by low accuracy of field sensors, by packet loss of communication channels or malicious injection. Malicious agent aim to inject wrong values in the SCADA

system. The detector relies on a comparative criterion where a threshold τ is identified with respect to the desired level of *false rate alarm* . The test run by the module *BDD* make use of the outcome of state estimation, the vector $\hat{x}$ and the objective function of the minimization above in 2.6, J. It is considered now the performace indicator $J(\hat{x})$ which is

$$J(\hat{x}) = \sum_{i=1}^{N_m} \left(\frac{z_i^{meas} - \hat{z}_i}{\sigma_i^2} \right)^2 \tag{2.8}$$

if the error $e_i$is indipendent and normally distributed, $e_i \sim N(0,1)$, with zero mean and unit variance, then the objective function **J(x)** follows a Chi-square distribution with $N_m - N_n = \nu$ degree of fredom of the system. The *SE* outcome is one realization of the random variable J(**x**), it has to be evaluated with respect to a threshold if the observation comes actually from the χ^2-distribution. More concisely, the hypotheses test consider the null hypothesis $H_\circ$ and the alternative hypothesis H_1. The former require the expected value to be $\mathbb{E}(J) == N_m - N_n$, and the latter $\mathbb{E}(J) > N_m - N_n$ so the test is basically executed as:

- if $J(\hat{x}) > \tau$ $H_\circ$ is rejected, bad measurement identified in the last set of data.
- if $J(\hat{x}) \leq \tau$ H_1 is rejected, and $H_\circ$ is confirmed, datas are accurate .

At the basis of the decision is *rate of false allarm*, which is a parameter of monitoring systems that need to be balanced between the probability of giving the allarm when measurements belongs to a normale behaviour and the probability of not giving the allarm when the measurement vector actually contains gross errors. The significance level of the test is identified with α, if the constant value τ is required so :

$$\tau = \chi^2_{\nu,1-\alpha} \tag{2.9}$$

it is equal to state that $\mathbb{P}(J(\hat{x})) > \tau = \alpha$. In sinthesys, BDD is based on the computation of measurement residual for each unit time of collection $\hat{r} = z - \hat{z} = z - H\hat{x}$, the difference of the vector of observations and the vector of estimated measurements, then is been applied

the L_2*norm* and bad measurement is inferred if:

$$\|z - H\hat{x}\|^2 > \tau \tag{2.10}$$

.

2.3 Attack vector

FDIA is one of possible cyber-attacks that electric power system engineer need to adress during design process and during the whole life of network operation. Is been demonstrated that by exploiting the readings taken at meters, the enemy can act sthealtily , as it is stated in the theorem :

Theorem 1 *Suppose the original measurements* $\mathbf{z}$ *can pass the bad measurement detection. The malicious measurement* $z_a = z + a$ *can bypass the bad measurement detection if* $\boldsymbol{a}$ *is a linear combination of the column vectors of* $\boldsymbol{H}$*, that is,* $a = Hc$*.*

The theorem and its demonstration can be found in ref.[10] and in ref.[11], the main result is the followging:

$$\|z_a - H\hat{x}_{bad}\| = \|z - H\hat{x}\| \leq \tau \tag{2.11}$$

The aspect which pose more concern is that if vector a is a linear combination of columns vector of the Jacobian matrix **H**, which is only dependent on the power network topology and a vector **c** choosen by the attacker, the attack is totally *undetectable*.

$$\mathbf{a}^{m\times 1} = H^{m\times n} \cdot c^{n\times 1} \tag{2.12}$$

The attacker only need matrix **H**. As explained in 2.2.2, the common detectors rely on the study of L_2*-norm* of measurements residual ($\|\hat{r} = z^{meas} - \hat{z}\|$), if bad datas don't affect this quantity also the allarm it will not be triggered, and so they bypass succesfully the *Bad Data Detection*. False Data vector can be easily constructed, and to properly compute it , the malicious agent needs to start from the knowledge of the topology matrix **H**, recovering

grid topology information: connectivity and branches characteristics (length, resistance and reactance). Achieving these information is not trivial, first of all connectivity isn't published by transmission company, as well as lines parameters. Moreover the access to important physical point from where it is conceivable to gain worthy information is most of the time denied to non-employees. If the attacker is motivated and succesfully gains the required information he/she will compute the attack vector as follow. Let's assume the attacker to have taken control over k meters, $I_{meter} = \{i_1, ..., i_k\}$ the set of indices of controlled sensors, consequentely he/she can use these meters to send wrong pocket of data to Control Systems. Only the readings z_i can be manipulated, where $i \in I_{meters}$. Is straightforward to say that attack vector $\mathbf{a} = (a_1, a_2, ..., a_m)$ requires to have zero entry $a_j = 0$ where the element's index $j \notin I_{meter}$, because he/she have no influence on it. Hence there are double constrictions : zeroed entry value for not controlled measurement and the need to compute $\mathbf{a}$ as a linear combination not to be reveiled from the allarm, as in the formula 2.12. Here is presented the case in which the injected error has random values, called *Random False Data Injection Attack*, still requiring to satisfy the above conditions. The formula to obtain the attack vector is reported here below, it is been used $a^{'}$ to indicate the attack vector restricted to the indexes in $I_{meter} = \{i_1, ..., i_k\}$:

$$\mathbf{a}^{'} = (I - B^{'-} \cdot B^{'}) \cdot d \tag{2.13}$$

where vector d has random entry values and is functional to define attack magnitude, while matrix $\mathbf{B}$ is the difference of projection matrix P of H and the identity matrix:

$$P = H(H^T H)^{-1} H^T \rightarrow B = (P - I) = H(H^T H)^{-1} H^T \tag{2.14}$$

and moreover matrix $B^{'-}$ is the matrix 1-invers of $B^{'}$, which is the matrix related only to the k measurement index controlled by attacker. Finally $a^{'}$ must be nested in the complete vector $\mathbf{a}$:

$$\mathbf{a} = (..., 0..., a_1^{'}, ..., 0, ..., a_i^{'}, ..., 0, ..., a_k^{'}, ...) \tag{2.15}$$

For a better explanation the authors refer to the discussion in [11].

3

Power Grid Model

This chapter is dedicated to describe in a comprehensive manner the physical behaviour of electric power grid, so for a better understanding of how a properly built cyber-attack is able to interact with the operativity of the network and disrupt the reliability and availability and resilience of the the nominal performances.

3.1 Power Grid model and DC assumption

Firstly it is reviewed the steady-state power network modeling, in which power flows is considered. A *power transmisssion system* is the coupling of electricity generators and constumers on a geographycal area, togheter with transformers and tranmission lines are the main components of an eletrical network, interconnected throu **nodes**, called *bus* or *substations*. It is necessary for reliability requirements that power network also involve

redundant paths so that the current can be delivered from any generator to any costumers, especially under fault condition of any of the components, on the basis of the most economical path and cost of power. A really simple representation of a two bus system is depicted in picture 3.1, where is available one Power Generator and one Loads connected thanks to one eletrical line $\{i, j\}$. This system can be formulated in terms of non-linear algebric

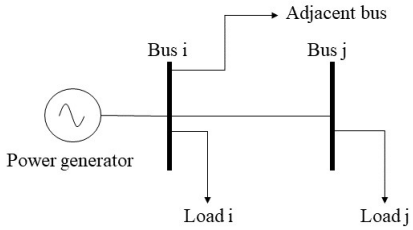


Figure 3.1: Simple two-bus system model

equations bounding the nodes parameters. Each bus i can be represented by four variables : V_i voltage magnitude,δ_i voltage angle,P_i active power injection,Q_i reactive power injection. Thou it is considered only DC-formulation so it must be introduced some further assumption:

- Only consider active power; all shunt elements, bus and branch reactive power flow are discarded.
- Resistance value of transmission lines is negligible, branches are considered lossless. $R_{i,j} \to 0$.
- Voltage magnitude is always equal to 1 p.u.
- Voltage angle δ_i are small enough to let this approximation : $\sin(\delta_i - \delta_j) \approx \delta_i - \delta_j$

The system model is described by nodal formulation : the net current injection at bus i is related by Kirchoff's Current Law (KCL) to the flows in branches incident to the bus. So

$$P_i = \sum_{j \in N_i} P_{i,j} \tag{3.1}$$

detailed procedure is well described in [7], here it is just presented the expression for active power injections:

$$P_i = V_i \sum_{j \in N_i} V_j (G_{i,j} \cos\theta_{i,j} + B_{i,j} \sin\theta_{i,j}) \tag{3.2}$$

Being $\theta_{i,j} = \delta_i - \delta_j$ the voltage angle difference of the two bus, and considering $R_{i,j} \to 0$ the conductance will be $G_{i,j} = \frac{R_{i,j}}{R_{i,j}^2 + X_{i,j}^2} \approx 0$ and the susceptance $B_{i,j} = -\frac{X_{i,j}^2}{X_{i,j}^2 + R_{i,j}^2} \approx -\frac{1}{X_{i,j}}$, with $R_{i,j}$ and $X_{i,j}$ the branch resistance and the reactance value considering only from bus i to j, the previous formula yield :

$$P_{i,j} = \frac{V_i \cdot V_j}{X_{i,j}} \sin(\delta_i - \delta_j) \tag{3.3}$$

Moreover it can be further approximated in :

$$P_{i,j} = \frac{\delta_i - \delta_j}{X_{i,j}} \tag{3.4}$$

The total number of equation will be the sum of the number of bus and the number of branches minus the reference bus. Assuming the reference value for δ_1, the other bus voltage angles are taken as *state variables*, while the *bus power injections* are the observable values :$P_{G,i} - Load_i$, see the example in the figure 3.2. Thus the state estimation described

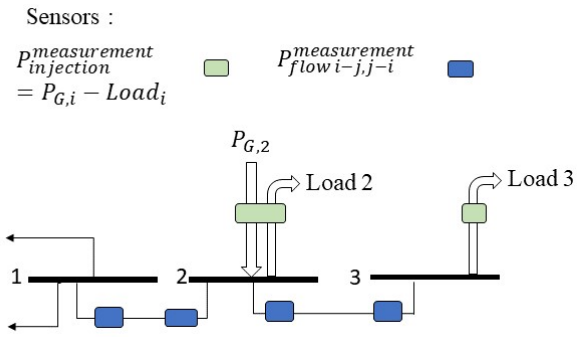


Figure 3.2: section of three bus, sensors set on power branch and on bus power injection.

above with eq. 2.1, can be re-formulated with a linear model, as in eq. 2.2. In power system the values monitored by control center are mainly power flows which are dependent variable on the bus voltage angles $P_i = \sum_{j \in N_i} h_{i,j}(\delta_i, \delta_j)$, accordingly to that bus voltage angles are considered the *state variable* of the system. The DC measurement model from here on

is $z(\mathbf{x}) = H(\mathbf{x}) + e$ and the matrix $\mathbf{H}^{m \times n}$ is a costant *Jacobian* matrix whose element are the coefficent of the linear relation between Power Injection or Power Flow and state variables $\mathbf{x} = (\delta_1, \delta_2, ..., \delta_n)$. Is noteworthy to say that usually bus number 1 is adopted as *slack* bus, and so it is used voltage angle of bus 1 a a reference value, arbitrarily chosen apriori, most common practise is to set $\delta_1 = 0$. It is necessary because the system of linear equazion is now solvable, thanks to the slack variable.

3.2 OPF - Optimal Power Flow

Optimal Power Flow algorithm is used in modern grid Control Center to assess many parameters among the grid and to take under control severals variables. Here the interest is just on the optimal point of operation (commitment of every generators), operative cost for running the network and the amount of demand not satisfied for each substations. OPF is a difficult mathematical programming problem, three main method have been commonly adopted to solve it :

- Lambda-iteration method.
- The gradient method.
- Newton's method.

Now by using one of these methods there exist programming codes which can solve reliably the formulation. Rougly speaking, OPF is a minimization problem which aims to find the minimum of the objective function, (frequently the aggregated cost of operation) constrained by power flow equations, power available and power branch limits. Following is shown the formulation used in the thesis.

OPF:

$$\min_{P_{G,i}, LS_i, \Delta\delta_{(i,j)}} CO = \sum_{i \in N} \sum_{G \in GDG} (COv_{G,i} - EP) \cdot P_{G,i} + (C_{LS,i} + EP) \cdot \sum_{i \in N} LS_i \tag{3.5}$$

$$s.t. \qquad L_i - \sum_{G \in GDG} P_{G,i} - S_{ref} \sum_{j \in N} B_{i,j}(\delta_i - \delta_j) - LS_i = 0 \tag{3.6}$$

$$0 \leq P_{G,i} \leq P_{av,i} \tag{3.7}$$

$$S_{ref}|B_{i,j}(\delta_i - \delta_j)| \leq P_{max,i,j} \tag{3.8}$$

Constraints must be considered for all $i \in N$, where N is the numerosity of substations. Then G is a specific generator and GDG is the set of traditional and renewable generators togheter. Decision variables $P_{G,i}$,LS_i,$\Delta\delta_{i,j}$ are respectively the power generated at bus i, Load disconnected at bus i, difference in bus voltage angles. $COv_{G,i}$,$P_{av,i}$ is the variable cost of production of generator at bus i and the power available, $C_{LS,i}$ is the penalty cost of shedding demand at bus i, L_i is load demand at bus i, S_{ref},EP is the per unit reference power and the electricity price, $P_{max,i,j}$ is the maximum power bearable by electric lines, and $B_{i,j}$ is the inverse of the reactance between bus i and j

3.3 FDIA against SE embedded into CPS

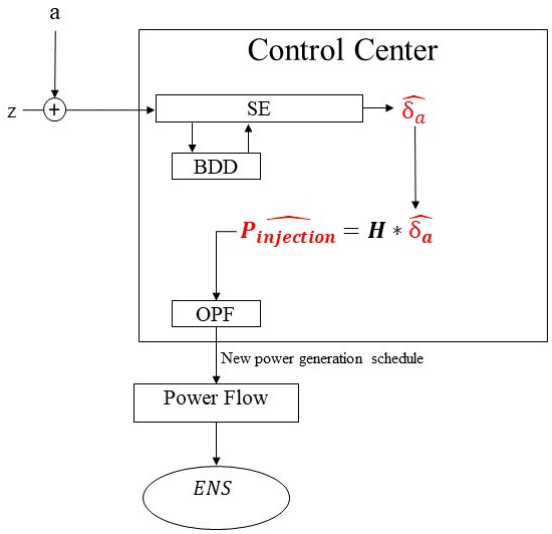


Figure 3.3: Effect of FDIA on power grid system.

By looking at the picture above it can be seen the flow of measuremnts data. Once the set of data is sent to Control Center the attacker launch the malicious vector. So SE receive corrupted information, compute a wrong estimate of the system and deliver it to the

subsequent OPF, whose aim is to adjust grid operativity by correcting unbalanced supply-demand profile throu the regulation of Power production schedule. Actually the OPF it is consiedered here receive as input the *power injection*. A further assumption must be made, information regarding energy actually produced are totally secure, because the company of the power generator can share this information. The only unknown/not observable value so is the Load Profile, hidden by the FDIA.

$$\hat{Power}_{injection,i} = P_{G,i} - P_{load,i} \tag{3.9}$$

Simply it is calculated the resultant $P_{load,i}$ for each bus i. With the false profile of load demand OPF is forced to output non-optimal generation schedule, as well as forcing some bus to shed the load to save the energy balance. Further it is calculated the effective Load shedding, by applying the new generation schedule and the real load profile(computed during the scenario generation) to a PowerFlow algorithm. Power Flow only receive in input power injection of each bus, then it try to calculate the power routing till every cunsumers. The load shedding in the node i, is defined as the amount of load disconnected in node i to alleviate overloaded feeders and/or balance the demand of power with just the available power supply. The outcome of this further step is essentially the flow of power in all the net and the performance function called *ENS*.

$$ENS = \sum_{i \in N} P_{shedding,i} \cdot t \tag{3.10}$$

The variable t is the time scale on which is calculated the duration of the disservice, set here $t = 1hour$.

4

k-MILP clustering with Monte Carlo engine embedded

In many application of power grid system, the design process have to address the daily and seasonal variations due to dependancy with weather conditions of several parameters and futures. This fact encrease the required level of details needed for a comprehensive description of the system to study, in terms of local, temporal and the uncertainty of input data. Most common practise in power grid system study is the extension of time horizon to one or several years simulations, and the adoption of the minimum time resolution of one hour enable to take under control phenomenon both in large and short scale. The advantage of this detailed description of the system hinder the tractability of the problem. Many works, for istance in ref. [1] and ref. [2] , the authors have considered the limited tractability and

have solved it by sinthetizing the sistem in a lower dimension. The clustering method proposed can automatically identify among the data set the few periods which are both more usual and more atypical. The 'representative' periods can be used at the place of common huge historical data archive involving lots of parameters and variables varying in time. This thesis work take inspiration from the clustering method described in the work [1], it is adopted here the algorithm k-MILP and used to diversify the scenarios that an attacker could find when he/she is looking for intruding in the system, the purpose of chosing a few representative periods is seen from the point of view of a clever attacker, which take advatage of ambient condition to properly choose the correct attack timing. Taking in consideration attacker interest, or better, attacker possible choice of grid condition, FDIA is so computed in our assumption on a limited set of typical and atypical periods. In our risk assessment the selection of these periods plays an important role, because the selection and computation of false data injection is carried out on the basis of representative days characteristics profile. Drawbacks of this metodology is the loss of chronological sequence of grid operation, so it is definetly not suitable for projects with storage system and or dynamic constraints. The periods here considered are on a daily basis, the selection of both the most representative days profiles and the days with extreme profiles could also be the most interesting choice from the point of view of a malicious agent. Extreme days, as it is common usage, are selected both as days in which the peak values are reached, and as "atypical" periods that differs to much from the others, so that they cannot be clustered with the others. It is also presented here a procedure to create a pool of days to be fed to tha k-MILP. Using a Monte Carlo approach inverse tranform method [12], it is investigated all the possible realization of a day time, considering seasonal,weekly and daily variability of the parameters, using as unit time scale 1 hour.

4.1 Monte Carlo Engine

MC-simulation is foundamental to address and model the many types of source of variability and to study the response of the network to an extensive representative combination of

possible conditions. Very suitable to finally evaluate performance functions of engineering systems, by the time it permit the computation of the function distribution, and so lead a risk analysis considering the level of likelihood desidered. In fact, insted of analytically calculate the performance functions, with MC it can be simulated. Many stochastic model are thus presented related to the uncertainties here taken in consideration.

4.1.1 Power Demand

The procedure to evaluate power load demand variation along one year is based on data taken from [16], there it is archived the peak annual load value of the 30bus IEEE test system, and also the distribution along the substations of the overall demand. The peak value in the reference is 283.4 MW, in this work by the time it's been introduced more generators than previously exist, the value is raised at 450MW. Moreover, from here [17] are also the tables which describe in percentage terms the behaviour of demand, on daily weekly and seasonality basis. So from the load profile in percent of substations and from the annual peak is been inferred the values of the whole year frame. Is been also assumed that these computed values, are actually distributed with a normal *pdf*, so the values have been taken as average with variance $\sigma^2 = 0.1\mu$, this happens because consumers don't require energy simultaneously so the demand may fluctuate around an average value. As it is described in reference [20], energy price is a fuction of the annual peak and the load demand profile, reproducing the characteristic of the net to be a 'price taker'. The relation it is used here to compute for each unit time the energy price is :

$$EP(Load_i|EP_{max}, Load_{max}) = EP_{max} \sum_{i \in N} \frac{Load_i}{Load_{max}} \left(-0.38 \sum_{i \in N} \frac{Load_i}{Load_{max}} + 1.38 \right) \quad (4.1)$$

EP is expressed in $\$/MWh$ and $EP_{max} = 100\$/MWh$ is taken as reference value associated to the maximum aggregated power load.

4.1.2 Traditional power generators

As it will be detailed in the next chapter, in the case study presented here two bulk power supply are considered. The first is related to a conventional enery production plan, the second is related to hydropower plant. To consider the uncertainty derived also from these traditional resources it is considered to be normally distributed. Numerical value can be seen on the table 5.1.

4.1.3 Photovoltaic generation

Each photovoltaic module (PV) consist of pannels composed with a number of solar cells set at $n_c = 20000$. Cells involve the photochemistry reaction to produce voltage difference and so current, thanks to incident photons. The solar irradiation function is expressed in kWh/m^2 can be simulated from a Beta function [19]. Actually the solar irradiance probability density function is bimodal, and so two functions beta must be merged togheter. Parameters to find the best fitting Beta have been computed by archive data , taken from [22]. Extrapolating important parameters α and β from historical recordings in a determined geographical area then it is possible to construct irradiance function, it follows:

$$f(s) = \begin{cases} \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} \cdot s^{\alpha-1} \cdot (1-s)^{\beta-1} & 0 \leq s \leq 1 \\ 0 & otherwise \end{cases} \tag{4.2}$$

The maximum solar irradiance is been set at $1kw/m^2$, s is the irradiance variable. The functional relations throu the parameters for the energy production from PV cells are listed below togheter with the power output:

$$P(s) = \begin{cases} P^{'}(s) & if \quad 0 \leq P^{'}(s) \leq P_{max} \\ P_{max} & if \quad P_{max} < P^{'}(s) \end{cases} \tag{4.3}$$

$$P^{'}(s) = n_c \cdot FF \cdot V(s) \cdot I(s) \times 10^{-6}$$

$$T_C(s) = T_{amb} + s(T_{no} + 20)/0.8$$

$$I(T_C) = s(I_{SC} + k_I(T_C - 25))$$

$$V(T_C) = V_{OC} + k_V \cdot T_C$$

$$FF = (V_{MPP} \cdot I_{MPP})/(V_{OC} \cdot I_{SC})$$

4.1.4 Wind Turbines generation

The modelization of wind speed, which is needed to compute power generated by the wind turbine, is been assumed to be a weibull distribution, as explained in if the time frame of collection is long enough, wind speed value can be hourly approximiated by weibull with parameters taken from :. It's been studied that weibull reproduce quite good the observed values at higher speed rate, while for low wind speed overestimate the realistic behaviour, but it is not affecting the framework presented. To assess the deterministic profile of energy production is been used the formula :

$$P(ws) = \begin{cases} 0 & 0 \leq ws \leq ws_{ci} \\ (A + B \cdot ws + C \cdot ws^2) \cdot P_r & ws_{ci} \leq ws \leq ws_r \\ P_r & ws_r \leq ws \leq ws_{co} \\ 0 & sw \geq ws_{co} \end{cases} \tag{4.4}$$

The coefficent values appearing in the formula are here described:

$$\begin{aligned} A &= \frac{1}{(ws_{ci} - ws_r)^2}\left\{ws_{ci}(ws_{ci} + ws_r) - 4ws_{ci}ws_r\left[\frac{ws_c + ws_r}{2ws_r}\right]^3\right\} \\ B &= \frac{1}{(ws_{ci} - ws_r)^2}\left\{4(ws_{ci} + ws_r) - 4ws_{ci}ws_r\left[\frac{ws_c + ws_r}{2ws_r}\right]^3 - (3ws_{ci} + ws_r)\right\} \\ C &= \frac{1}{(ws_{ci} - ws_r)^2}\left\{2 - 4\left[\frac{ws_c + ws_r}{2ws_r}\right]^3\right\} \end{aligned} \tag{4.5}$$

Thi formula from bound the wind speed and the power production throu three parameters on wind velocity and the rated power. Finally it is added a random noise to simulate

realistic deviation from the deterministic values :

$$P_{output}(ws) = P(ws) + \varepsilon \tag{4.6}$$

ε is normally distribute with $\mu = 0, \sigma^2 = 0.1P_r$

4.1.5 Ambient Temperature

Ambient temperature data have been retrivied from ref. [18], the data archive contains historical records of the maximum and minimum temperature daily related to 1 years, (average value over 30 years). By computing the linear equation from the minimum to the maxium value respectively at 5a.m. and 4p.m., the hourly value of temperature is assessed for the entire year. Considered the stochastic deviation, it is assumed a normal distribution.

Table 4.1: Parameter for each generator type.

Gen.Type	Technical parameters				
G1	$P_{max,1}(MW)$	Normal μ_1	Normal σ_1		
	340	300	18.5		
G2	$P_{max,2}(MW)$	Normal μ_2	Normal σ_2		
	50	42.5	5		
PV	$P_{average}(MW)$	$P_{max}(MW)$	$V_{OC}(V)$	$I_{SC}(A)$	$V_{MPP}(V)$
	1.07	75	21.98	5.32	17.32
	$I_{MPP}(A)$	$k_V(mV/^\circ C)$	$k_I(mA/^\circ C)$	$T_{NO}(^\circ C)$	$Tamb(^\circ C)$
	4.76	14.4	1.22	43	30
WT	$P_{average}(MW)$	$P_r(MW)$	$ws_{ci}(m/s)$	$ws_r(m/s)$	$ws_{co}(m/s)$
	0.93	1.5	5	15	25

4.2 Clustering techniques

The requirement of the algorithm is to be able to select days which could be representative of the original time series constrained to the fact that operational feasibility must

be preserved and the costs are the closest to the actual ones. For these purpose extreme days are added for the first istance and clustering techniques for the second istance, enablig us to use all the spectre of possible attack scenarios. The object of the aggregation method is to gather a set of periods $j \in \{1,..,N_d\}$, in our case N_d is equal to 365 which are days of the year, each ones containing the same number of time steps $N_h = 24$ hours with $h \in \{1,...,N_h\}$ and N_a attributes, clustering in a pre-determined number of N_k of groups in a way that group members are as similar as possible. So finally the group can be represented by a single element.

Basically in our method the clustering is led by the minimization of a distance measure based on the attributes of the periods to be clustered. Here we have chosen 4 attributes for clustering:

- Load profile
- Solar Irradiance
- Wind Speed
- Ambient Temperature.

The periodicy of these attributes, phisical phenomena and energy demand, make it strainghtforward to use 24h for time steps basis: *typical days*. The model can be formulated as a Mixed Integer Linear Programming (MILP),[2]. In k-MILP clustering instead of using statistical well-known *first order moment* as representative period, a real period, called *the medoid* is selected among the elements of the group. In this way we can preserve the seasonal and the daily correlation between the many attributes.

4.2.1 Dissimilarity Matrix and Distance Matrix

How to define the distance between two days. We start from the input data about ambient temperature, load profile solar irradiance and wind speed, arranging them in a $N_d - by - N_h * N_a$matrix (L) as is shown in 4.7, so that each row is the object to be classified, and the columns are related to the objects attributes at each time steps. Hence, for each day,

columns from 1 to 24 are load demand, from 25 to 48 are solar irradiance, from 49 to 72 are wind speed and from 73 to 96 are ambient temperatures.

$$L = \begin{bmatrix} x_{1,1,1} & \dots & x_{1,24,1} & \dots & x_{1,1,2} & \dots & x_{1,24,2} & \dots & x_{1,24,4} \\ . & & . & & . & & . & & . \\ . & & . & & . & & . & & . \\ . & & . & & . & & . & & . \\ x_{i,1,1} & \dots & x_{i,24,1} & \dots & x_{i,1,2} & \dots & x_{i,24,2} & \dots & x_{i,24,4} \\ . & & . & & . & & . & & . \\ . & & . & & . & & . & & . \\ . & & . & & . & & . & & . \\ x_{365,1,1} & \dots & x_{365,24,1} & \dots & x_{365,1,2} & \dots & x_{365,24,2} & \dots & x_{365,24,4} \end{bmatrix} \tag{4.7}$$

The distance measure mentioned above is the *Euclidean Distance*, and aims at computing the value of the distance between each couple of elements, in this case, each couple of days.

It is calculated as follow, Eq.(4.8)

$$d_{i,j} = \sqrt{\sum_{h=1}^{N_h} \sum_{a=1}^{N_a} (x_{a,h,i} - x_{a,h,j})^2} \quad \forall i, j \in \{1, ..., N_d\} \tag{4.8}$$

Here below matrix representation (4.9)

$$d_{i,j} = \begin{bmatrix} 0 & d_{1,2} & . & . & . & d_{1,365} \\ & & & & & . \\ & 0 & & & & . \\ & & & . & & . \\ & & & & . & d_{364,365} \\ sim & & & & & 0 \end{bmatrix} \tag{4.9}$$

In the figure above 4.9, we can see the values of distances of each element to each other; when day i and j are very close, components of 4.9 are almost zero, instead when the value

of $d_{i,j}$ becomes larger they are very different. So is obvious that diagonal elements are zero because each day is equal to itself. All the information needed to run k-MILP clustering algorithm are contained in this matrix 4.9.

4.2.2 Clustering algorithm

Firstly is needed to choose the number of group in which it is needed to divide data set, k cluster, then it can be stated the MILP problem. The MILP problem can be formulated as the minimization of the Euclidean Distance subjected to constraints, as follow 4.10:

$$\min \sum_{i=1}^{N_d} \sum_{j=1}^{N_d} d_{i,j} * z_{i,j} \tag{4.10}$$

Subject to :

$$\sum_{j=1}^{N_d} z_{i,j} \leq 1 \quad \forall i \in \{1,...,N_d\} \tag{4.11}$$

$$z_{i,j} \leq y_i \quad \forall i,j \in \{1,...,N_d\} \tag{4.12}$$

$$\sum_{i=1}^{N_d} y_i = N_k \tag{4.13}$$

$$\sum_{i=1}^{N_d} \sum_{j=1}^{N_d} z_{i,j} = N_d - N_{ED} \tag{4.14}$$

$$\sum_{i=1}^{N_d} \sum_{j=1}^{N_d} \sum_{h=1}^{N_h} \|x_{a,h,j} - x_{a,h,i}\| * z_{i,j} \leq \lambda_a^{LDC} * \sum_{j=1}^{N_d} \sum_{h=1}^{N_h} x_{a,h,j} \quad \forall a \in A^{LDC} \tag{4.15}$$

$$\sum_{j=1}^{N_d} m_{a,j} * \max_h x_{a,h,j} \leq \lambda_a^{PEAK} * \max_{d,h} x_{a,h,d} \quad \forall a \in A^{PEAK} \tag{4.16}$$

$$\sum_{j=1}^{N_d} m_{a,j} = 1 \quad \forall a \tag{4.17}$$

$$m_{a,j} \leq 1 - \sum_{i}^{N_d} z_{i,j} \quad \forall a, \forall j \tag{4.18}$$

where $z_{i,j}$ is equal to 1 if day j is represented by day i, and 0 otherwise. The variable y_i label the candidates, 1 if the candidate represent a cluster, 0 otherwise. Contrains 4.11 imposes that each day of the year is assigned to a representative day, meanwhile also allowing the

model to automatically exluding particular days from the clustering. Constrain 4.12 imply that the assignation is possible only for days selected as typical. Constrain 4.13 limit the clusters number by determining the number of TD. 4.14 is needed to get rid of the trivial solution that wants all days are classified as extreme (N_{ED} is the extreme days number, chosen by the author).The algorithm is so able to detemine which days is more "atypical" of the year, candidates that are not well represented from the representative TD. In order to mantain a realistic value of the aggregation of the Load Demand Curve (LDC),for some $a \in A^{LDC}$ constrain 4.15 impose that the difference between the sum of original data set and the sum of the repetition of the representative periods is limited by a tolerance, and so the LDC aggregated must be a percetage of the original time series (λ_a^{LDC} assumed to be 5%, it can also be less, like 2%). Moreover the relation in eq. 4.16 force for some pre-selected attributes $a \in A^{PEAK}$, a least one of the chosen extreme day by the algorithm contains the highest peak value (or similar) from the data set. It should be noted that $h \in \{1,...,N_h\}$ and $d \in \{1,...,N_d\}$ and λ_a^{PEAK} is a real value which is used to bound the quantity of the *PEAK* to be represented by extreme days, it may be set to e.g. 10-100%. The remaining 2 constraints, 4.17 and 4.18 support the computation by the optimization algorithm of the binary variale $m_{a,j}$, which is equal to 1 if the day candidate j is selected te be *ED* for candidate a, 0 otherwise. The proposed k-MILP problem can be solved by commercially available solver in less than 10 minuts.

4.3 k-MILP model for the automatic identification of extreme and typical days

4.3.1 Normalization of values

One year time-series of Load Demand, solar irradiance, wind speed and ambient temperature are been used to run the model, which need the data sets to be all on the same time-scale. So the time-series are normalized before been given to the algorithm. Let be $x_{a,h,i}$ the normalized data, $\tilde{x}_{a,h,i}$ the original value, the normalization of data sets is then be

realized by taking in consideration the maximum and the minimum value of the series, for each attribute a, as :

$$x_{a,h,i} = \frac{\tilde{x}_{a,h,i} - \min \tilde{x}_{a,h,i}}{\max \tilde{x}_{a,h,i} - \min \tilde{x}_{a,h,i}} \tag{4.19}$$

As already stated the number of *typical days*(TD) and the number of *extreme days*(ED) are previously determined, 6 for the former and 4 for the last.

For semplicity of writing the mixed integer linear programming on matlab, we have used the toolbox YALMIP, which enable easily to construct the objective function and the various constraints. It has been also used among the various standard optional optimization solver the software Gurobi,the most powerfull mathematical optimization solver.

5

Search for vulnerability threshold and critical components

5.1 Case study

The system under analysis here is the IEEE 30 bus test power system, reffering to both sub-transmission and distribution network, from the research [20]. It is refferred to a portion of an old U.S. electric power grid, around 1969, frequently used for research purpose because of the availability of data about connectivity, loads and lines parameters. In the picture the distribution side is depicted with blu branch lines at 33kV nominal voltage value, meanwhile black routes are representative of the sub-transmission area at 132kV. Due to DC assumption already detailed above, synchronous condenser have been discarded form the

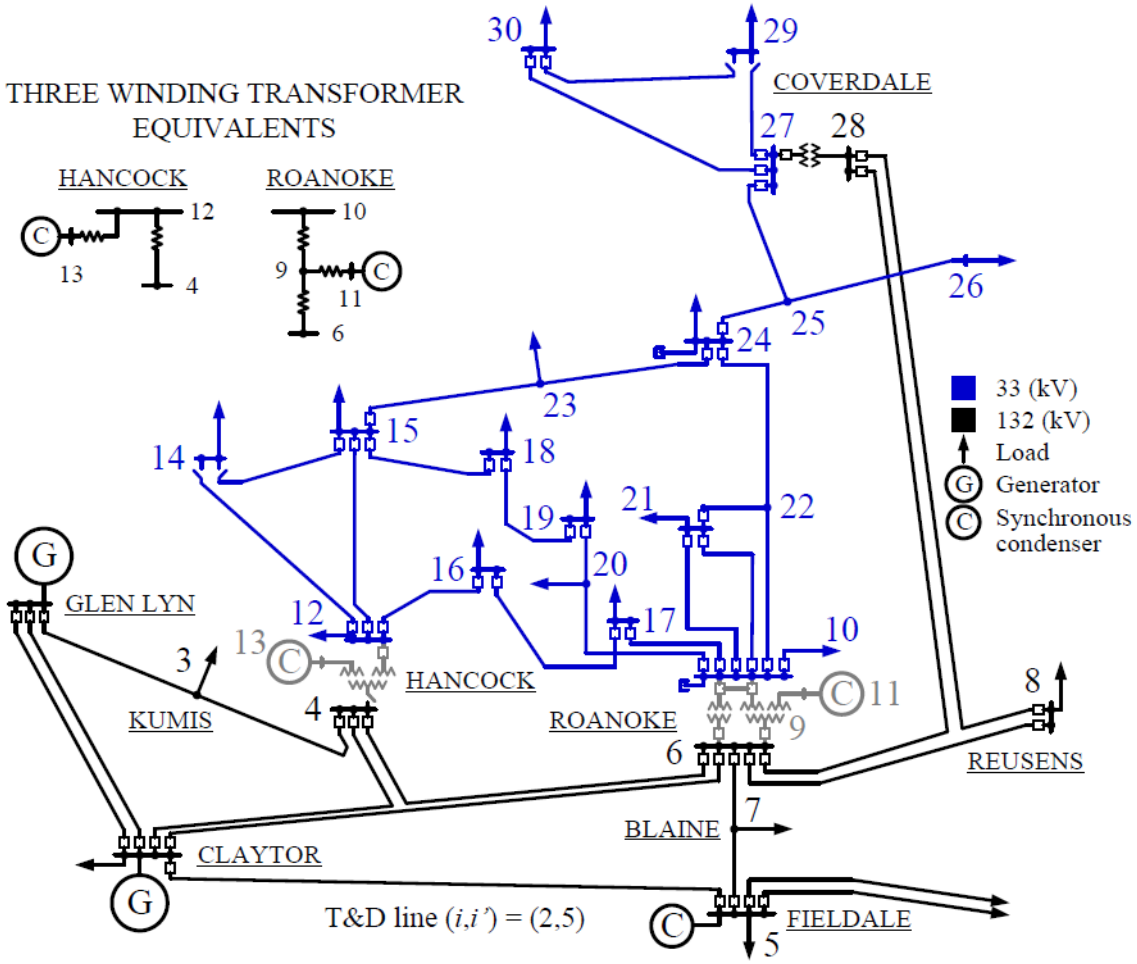


Figure 5.1: Power Network 30-bus, Subtransmission Transmission system

work. Thus the two areas at different voltage level communicate throu three main transofmers substations pair (4:12),(6:10) and (27:28). This system is a usual test bed for assessment studies thanks to interesting features. First of all is quite big system so that can involve at the same time the issues related to higly interconnected power network and the computational simplicity of a handable structure of just 30 nodes; also IEEE30bus is equipped with two bulk-power supply, the first one is a traditional dense power generator (e.g. Gas Turbine) attached to bus 1, the second is hydropower station attached at bus number 2,with less specific energy and less overall power. Moreover the test system is characterized by high variation in loads along substaions, so there are bus with a demand close to 100MW for example bus 4 and others around 3MW, as it is bus 16. The authors of this thesis aribitrarely chose the susbstaions at which the renewables generators should be attached, basing the choice on voltage of the different network areas. Usually wind

turbine farm are connected to medium voltage grid or low voltage, so it is assumed here that wind farm only can be at substations at 132kV, meanwhile PV pannels are usually connected to household portion of the network and so it is more reasonable to connect only the substations at 33kV. Details in the table below:

Renewable allocation		
Bus	Gen.	Quantity
2	WT	25
5	WT	25
8	WT	25
14	PV	30
21	PV	10
30	PV	20

WT stands for wind turbine, as it can be seen wind farm are composed of 25WT each, while photovoltaic pannels vary from 10 to 30. These values are in accordance of the considered share of renewable plants connected to the grid, computed from the formula :

$$\sum_{i \in N} \sum_{G \in DG} \frac{G_i \cdot P_{av,G,i}}{Load_{max}} = PF \tag{5.1}$$

With G representing the matrix of quantity and location of generators, DG is the submatrix of G containing only renewables generators, $P_{av,G,i}$ is the rated power that generator G at substation i can deliver. PF is the *penetration factor*, setted at 30%.

5.2 Risk Measure

At the conclusion of one loop of the work-flow che simulator have obtained the Energy Not Supplied distribution respect to substations. Thus to evaluate the level of risk and uncertainty related to the performance function ENS, are adopted here a two main risk measures:

- *Conditional value at risk* (CVaR).
- *Deviations of Conditional Value at Risk* (DCVaR).

The latter is a function of the former. These Risk measures are frequently encountered in finantial portfolio optimization and then also they have been used in engineering applications, such as design optimization plannig. It must be introduced the *Value at Risk* from which DCVaR and CVaR are derived:

$$VaR_\alpha(x) = inf\{z : F_x(z) > \alpha\} \tag{5.2}$$

For a discrete approximation of the performance function, VaR is the minimim quantity of the function for which the probability to exceed that value is greater or equal to α. So now :

$$CVaR_\alpha(x) = \mathbb{E}(x/x \geq VaR_\alpha(x)) \tag{5.3}$$

is the definition of the CVaR, it represents the average value of performance loss given that the performance loss is greater or equal to VaR(x). Basically it provides a measure of the extent of the frequency of occurrence of non desired scenarios. Meanwhile the formulation of its deviation is:

$$DVaR_\alpha(x) = CVaR_\alpha(x - \mathbb{E}(x)) \tag{5.4}$$

and this last focus on the uncertainty of performance loss by the time it exceed the average value. Is strightforward that the two quantity are bounded in the relation following :

$$DCVaR_\alpha(x) = CVaR_\alpha(x) - \mathbb{E}(x) \tag{5.5}$$

. For a better description and understandings of the risk measure here utilized, detailed discussion are covered in[14],[15]. The value for α considered in the simulation is discretional and has been chosen whithin a conservative aspect, so it is $\alpha = 90\%$.

5.3 Simulation

The thesis in object propose a framework to assess risk in cyber domain and moreover , trough an analysis of the impact of cyber attack on the costumer satisfaction, try to infer guidelines to protect efficently the grid with the updated knowledge of the map of the most vulnerable sensors installed. It has been assumed as case study a DC-renewables integrated network, well described in the following section, in which have been choosen by discretion of the authors which substations is connected to renewables. Two different kind of renewable power generators are here taken in consideration, Photovoltaic Pannel and Wind Turbine, leaving the possibilities of further study and simulations about battery and cars connected to grid for the future researches. First step is the selection of the quantity and location of the distributed resources by the formulation of the matrix G(for traditional generator) and DG(renewables generator) to be fed in the matlab simulator. After having assessed all the required statistical distribution of frquency related to the grid and ambient parameters, all the possible scenarios are investigated by MC-sampling with 1h as unit time scale. It has been implemented in the framework the Monte Carlo inverse trasnform method ,[12]. The several variables identifying the operative condition have been randomly sampled different times according to their assumed distribution based on this method, to fed finally a pool of days composing a total of 100 years.. The simulation proceed by applying to these 100 years the k-MILP algorithm. The clustering program as already explained identify 6 typical days and 4 extreme days in which one year can be summarised. A total of 1000 foundamentals days are so selected to efficently conduct the sequent risk analysis. OPF program compute the grid operation for all of this days , and after having calculated all the measuremnts of the network area they are altereted by an attac vector. Thus the falsified measuremnt are sent to *state estimation* to be controlled and used to assess the actual state of the power system. The output will be corrupted, of course, and the perceived load demand of substations altereted. The new load profile are the new input for a second round of OPF, which will assess how to adjust the grid in presence of the new condition. It will result a power production schedule not effectively optimized , and this can lead to serious consequencies :

- not fullfill the total demand.
- excessive production of energy.
- bottleneck in power transmission.

Hence the simulator is fed with 1000 different days and output a distribution of ENS.

It's been crucial for the proposed procedure to take advantage of the MATLAB toolbox MATPOWER [21], from where it has been exploited the Optimal Power Flow algorithm, coherently adjusted for the case study in object.

The flow chart represent the steps to compute ENS probability density function , and by applying risk measure the procedure can provide detailed information about the consequence of intrusion. For every attacked day the algorithm look for an attack vector to stealthily inject random false data. It is assumed that rarely the malicious agent can decide wich sensor to corrupt, so it is decided to randomly extract the location of the infected components. With this method by comparing the risk measures of the ENS distribution versus the number of manipulated meters, it can be inferred the threshold value of meters to be compromised to significantly affect network efficency. It remain to assess the intra-day timing of FDIA, for simplicity and by referring to cybersecurity reports, the following assumption are taken:

1. Attack duration is extracted from a Uniform distribution with parameters $\alpha = 4$and $\beta = 10$.
2. Starting time of attack is randomly selected from 4 values : 4a.m. / 10a.m. / 4p.m. / 10p.m.

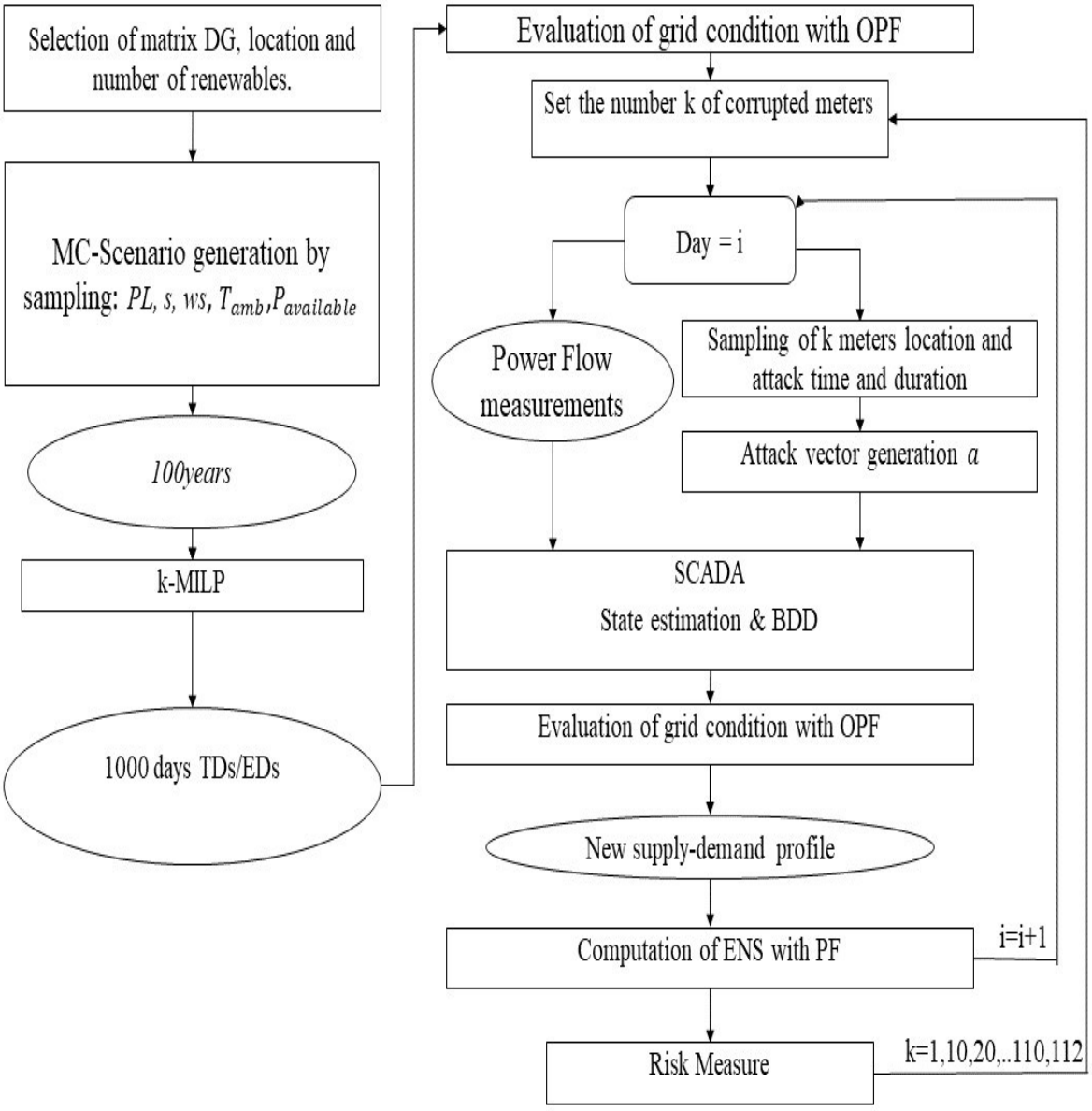


Figure 5.2: Flow-chart of the first proposed framework

6

Results

The simulation take several hours with a laptop Dell equipped with intel core i5 2.3GHz. First of all it is pursued the identification of the thresold number of sensors that an attacker need to have under his/her control. In fact from the view point of SO, this is a foundamental value on which further investment of cybersecurity can be based. FDIA specifically is based on the combinatorial search for an attack vector that must satisfy the condition described in 2.12, and is not trivial. It is considered the formula 2.13 forcing the computation of the vector, resulting in a zero-vector when the FDIA construction fail. The failure is due to the impossibility of injecting false data without triggering the allarm, that mean without encreasing the value of the $L_2 norm$ of the residual, and finally this is because the location of corrupted meters don't allow the insertion of data deviated from the physical values. If meters infected are related to all the interacting measurements that have no influence on

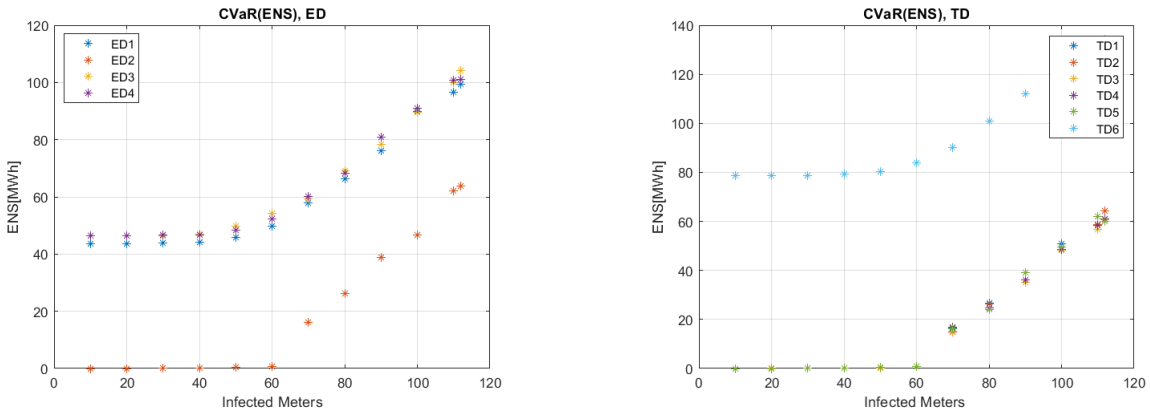


Figure 6.1: Risk measure CVaR trends

other values, the attack vector can be computed. By running the simulation with different number of compromised sensors, it is found that 50 is the critical number of measurements that the SO have to simultaneously make sure not to be compromised in order to avoid effective attack. The risk measure related to the performance funcion ENS suggest that after 50 corrupted measurements, the unsatisfaction of consumers start rising from the non-attacked values. Is interesting also that the fake quantity injected in the grid by the attack : the vector shaped by the component d in the formula 2.13, steeply rise in magnitude after 50/60 corrupted measurements, from 0MW till 6MW. This effect is due to the probability of finding a suitable vector very low before 50 corruptions and very probable after 60. From the CVaR computation it can be seen in picture that if we encrease the entity of the attack after 50/60 infected components the average value of consumer unsatisfaction , given that the ENS is greater then the Value at Risk 90% rise. The risk measure enlight the average loss if we incurr in a scenario of risk of loss that is 10% probable. As we can see extreme days related to peak load, peak wind speed and peak ambient temperature are already affected by high CVaR values also without attack,mostly because of physical reasons related to the network under different ambient conditions.

- ED1 is related to high values of load demand.
- ED2 is related to high values of solare irradiance.
- ED3 is related to high values of wind speed.
- ED4 is related to high Tamb values.

Figure 6.2: On the same line are represented the distribution with encreasing attack magnitude. Column represent the attack to different representative days

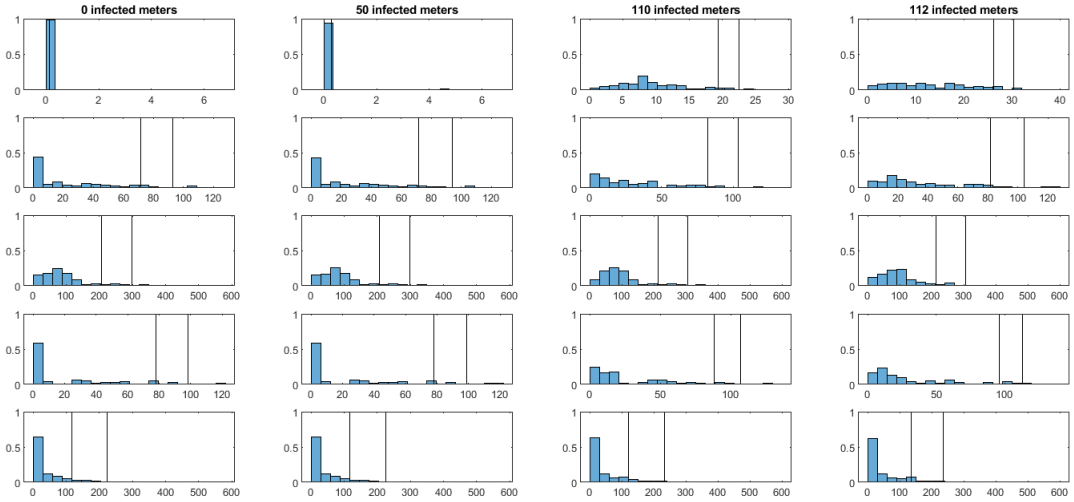
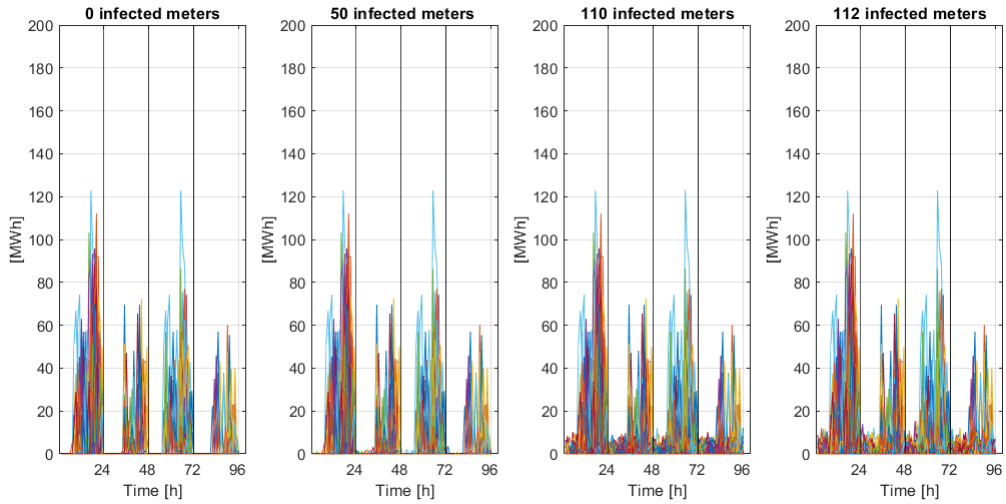


Figure 6.3: Extreme days and Energy not supplied



The typical days instead are randomly clusterized based on similarities. It can be inferred that TD6 represent days with loss due to low value of production of wind power and solar power. The other 5 TD are more similar unrisky scenarios. For typical days the attack clearly affecft the distribution, while for TD6 and the other extreme days it smooth a little the distribution but not in a sensible manner, it is further explained in the sequent plots. As it can be seen from the subsequent plots FDIA encrease the little loss for all the representative days, so basically the corruption with false data lead to more frequent loss smaller in magnitude with respect to the ENS normally occurring durig grid operations. This is due to the combination of low demand and high power availability characterizing these days.

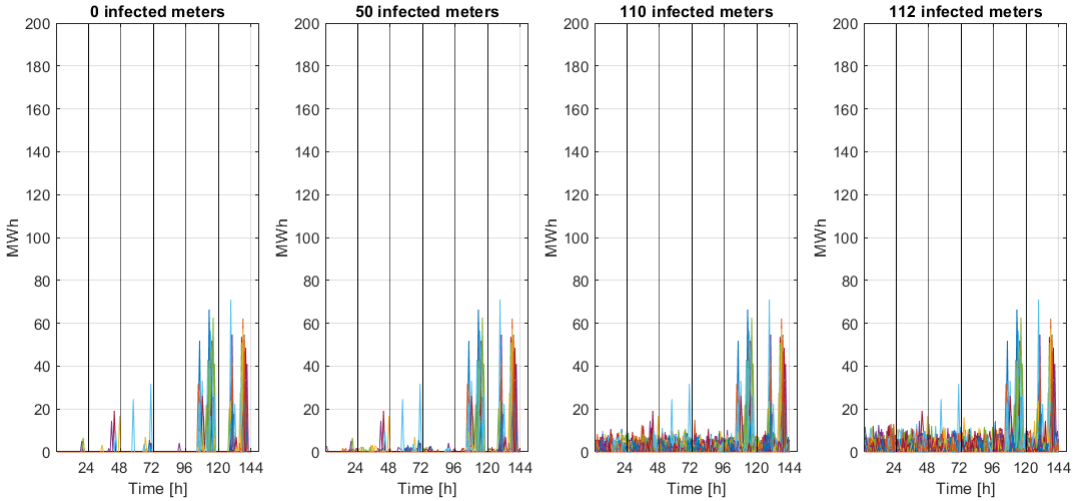


Figure 6.4: Typical days and Energy not supplied

In this case also if cyber attack mislead the profile of the electricity request, the power generation schedule can adjust easily to the new demand. Moreover, due to the soft condition of the power flow pre-attack, the entire net (thanks to the maximum power bearable by branches), can adapt perfectly to the more stressed condition due to cyber-attack. For typical days, except for the TD6, FDIA induce an encrease in the amount of ENS registered, so consequently the DCVaR encrease as it can be seen in the picture above.

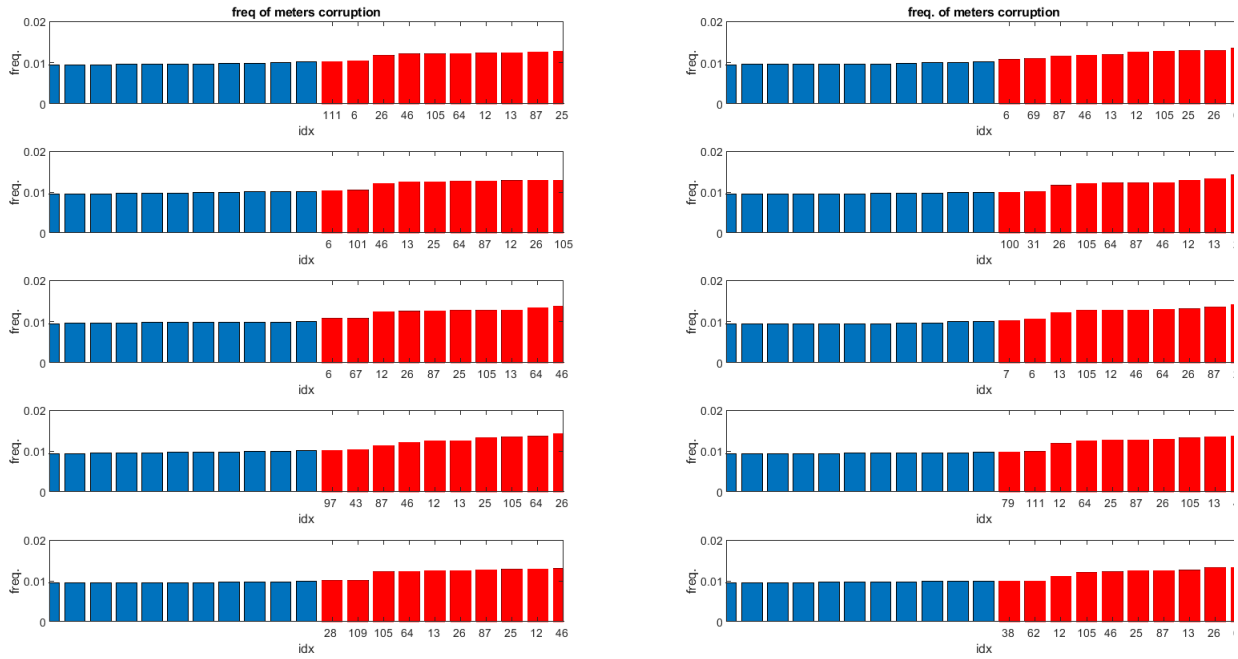


Figure 6.5: Histogram of the frequency of corruption for meters index.

Previously we underline the specific quantity of 50 meters as an important treshold that

divide negligible variation in Risk Measures related to Energy delivered to costumers, and significant variation which means induced loss of grid efficiency. So, now we have propose the combination sets of 10 sensors which, if hijacked by attacker, they can lead to values of ENS higher then the threshold of CVaR. The CVaR represent the threshold for the severe consequencies in the case of the minimum number of accessible sensors underlined before (=50). When the attacker select a proper set of sensors, the grid becomes unobservable, and he/she can inject whatever error he/she want while not affecting the residuals of the measurements (most of the anomaly detectors are based on residuals). It can be reasonable to think that 50 corrupted sensors can lead to a non negligible probability of using some of the minimal combination set for the most severe consequencies. Result are plotted in picture above, and then they are sinthetized in the table 6.1.

Table 6.1: Critical sensors for each representative day.

Day type	♯1	♯2	♯3	♯4	♯5	♯6	♯7	♯8	♯9	♯10
TD1)	6	12	13	25	26	46	64	87	105	111
TD2)	6	12	13	25	26	46	64	69	87	105
TD3)	6	12	13	25	26	46	64	87	101	105
TD4)	12	13	25	26	31	46	64	87	100	105
TD5)	6	12	13	25	26	46	64	67	87	105
TD6)	6	7	12	13	25	26	46	64	87	105
ED1)	12	13	25	26	43	46	64	87	97	105
ED2)	12	13	25	26	46	64	79	87	105	111
ED3)	12	13	25	26	27	28	46	64	87	105
ED4)	12	13	25	26	27	46	62	64	87	105

As we can see, there are some measurement index which always occur when the FDIA has been able to encrease the Ens value above the CVaR. So they reasonably can be pointed out as the most critical components among the network. It is noteworthy also that index measuremnt from 0 to 30 are related to power injection, in table depcted in green, the other are related to branch power flow.

7

Conclusion and Future Works

7.1 Conclusion

From this work it can be enforce the resilience of electricity grids by following the guideline of vulnerabilities and critical component anlysed here, according to two aspects: on the one hand, increasing network robustness by rising, where economically sustainable the design limits that identify the infrastructural capability to withstand extreme stresses (e.g., by rising, to an economically sustainable level, design limits of electrical lines); on the other hand, improving the effectiveness and promptness of service recovery, i.e. the system's capability to return to acceptable working condition, even by means of temporary measures (e.g. the temporary repowering of unsupplied electrical substations). From the work emerge the potential adjoint threat when a power network already stressed by power

condition or environmental condition is also attacked by malicious agent.

7.2 Future Works

The sector is changing rapidly, as well as new findings and new method of analysis. This thesis work can be taken in consideration for further development of the research, investigating the dynamics of the system, on a lower time scale, and discard the DC assumption to explore the AC-power network operation. Moreover two different kind of renewable power generator are here taken in consideration, Photovoltaic Pannel and Wind Turbine, leaving the possibilities of further study and simulations about battery and cars for the future.

Bibliography

[1] Matteo Zatti,Marco Gabba, Marco Freschini,Michele Rossi,Agostino Gambarotta,Mirko Morini, Emanuele Martelli,k-MILP: A novel clustering approach to select typical and extreme days for multi-energy systems design optimization

[2] Fernando Domínguez-Mu~noz,José M. Cejudo-López,Antonio Carrillo-Andrés,Manuel Gallardo-Salazar,Selection of typical demand days for CHP optimization

[3] Monticelli,A. 1999. State Estimation in Electric Power System, A generalized approach. Kluwer, Amsterdam.

[4] Mili,L.,Custem,T.V.,and Pavella M.R. 1985. Bad data identification methods in power system state estimation, a comparative study.IEEE Trans. Power Appar.Syst.103,11,3037-3049.

[5] Monticelli,A. and Garcia,A. 1983.Reliable bad data processing for real-time state estimation.IEEE Trans.Power Appar.Sys.102,5,1126-1139.

[6] Monticelli,A.,Wu,F.F., and Multiple,M.Y.1986. Bad data identification for state estimation by combinatorial optimization. IEEE Trans. Power Delivery 1,3,361-369.

[7] Wood, A. and Wollenberg, B. 1996 Power Generation, Operation, and Control (2nd ed.), Wiley, New York

[8] Yanling Yuan, Zuyi Li and Kui Ren. 2011. Modelling Load redistribution attacks in Power systems. IEEE Transaction on smart grid, vol.2, NO.2.

[9] Yanling Yuan,Zuyi Li,Kui Ren, 2012 Quantitavie analysis of load redistribution attacks in Power systems. IEEE Transaction on Parallele and distributed system, vol. 23, NO.9.

[10] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," presented at the 1stWorkshop Secure Control Syst. (CPSWEEK), Stockholm, Sweden, Apr. 2010.

[11] Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," in Proc. 16th ACM Conf. Comput. Commun. Security, Nov. 2009, pp. 21–32.

[12] Zio E., The Monte Carlo simulation method for system reliability and risk analysis. Springer Series in Reliability Engineering. Springer London; 2013.

[13] Sayed K, Gabbar HA. Chapter 18 - SCADA and smart energy grid control automation. Smart Energy Grid Eng 2017:481–514.

[14] R. Rockafellar, S. Uryasev, and M. Zabarankin, "Generalized deviations in risk analysis," Finance and Stochastics, vol. 10, no. 1, pp. 51–74, 2006.

[15] R. Rockafellar and S. Uryasev, "Conditional value-at-risk for general loss distributions," Journal of Banking and Finance, vol. 26, no. 7, pp.1443 – 1471, 2002.

[16] University of Washington, College of Engineering, Department of Electrical Engineering, Available at: http://www.ee.washington.edu/research/pstca.

[17] The IEEE reliability test system – 1996 . A report prepared by the reliability test system task force of the application of probability methods subcommettee.

[18] Ambient temperature data taken from: ftp://ftp.ncdc.noaa.gov/pub/data/normals/1981-2010/

[19] Atwa Y, El-Saadany E, Salama M, Seethapathy R. Optimal renewable resourcesmix for distribution system energy loss minimization. Power Syst IEEE TransFeb 2010;25:360e70

[20] Mena R, Hennebel M, Li Y, Zio E. A multi-objective optimization framework for risk-controlled integration of renewable generation into electric power system. Energy 106 (2016) 712-727.

[21] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "MATPOWER: Steady-State Operations, Planning and Analysis Tools for Power Systems Research and Education," Power Systems, IEEE Transactions on, vol. 26, no. 1, pp. 12–19, Feb. 2011. DOI

[22] Irradiation data it's been downloaded from the website $https://rredc.nrel.gov/solar/old_data/nsrdb/$