QATAR UNIVERSITY

COLLEGE OF ENGINEERING

CYBER-ATTACKS AGAINST VOLTAGE PROFILE IN SMART DISTRIBUTION GRIDS WITH HIGHLY-DISPERSED PV GENERATORS: DETECTION AND PROTECTION

BY

NOUR GHALIB ABU AYSHEH

A Thesis Submitted to

the Faculty of the College of Engineering

in Partial Fulfillment of the Requirements for the Degree of

Masters of Science in Electrical Engineering

January 2021

COMMITTEE PAGE

The members of the Committee approve the Thesis of
Nour defended on 28/10/2020.

Tamer Khattab
Thesis/Dissertation Supervisor

Ahmed Massoud
Thesis/Dissertation Co-Supervisor

Walaa Hamouda
External Examiner

Nizar Zorba
Internal Examiner

Mohsen Guizani
Dean's Representative

Approved:

Khalid Kamal Naji, Dean, College of Engineering

ABSTRACT

ABU AYSHEH, NOUR, GHALIB., Masters : January : 2021,

Masters of Science in Electrical Engineering

Title: Cyber-Attacks Against Voltage Profile in Smart Distribution Grids with Highly-Dispersed PV Generators: Detection and Protection.

Supervisor of Thesis: Dr. Tamer Khattab.

In this work, we study the effect of cyber-attacks on voltage regulation in smart grids with highly dispersed photovoltaic (PV) power generators. We picture how the cyber-attacks in the distribution network with the existence of PV generators can cause induced voltage violations of overvoltage or undervoltage. It is demonstrated that if an attacker falsifies measurements, voltage violations may occur in the system. A proposed algorithm using a PV perturbation method to check the response of the nodes in the network is applied to detect the cyber-attacks and protect against destructive reactions as a second detection and protection layer in addition to classical cyber protection at the communication network layer. We establish a primary distribution network model that incorporates the effects of attacks that penetrate the communication network and inject falsified data. We project the proposed basic model into a distribution network example to show the effect of such attacks. We further use the extended model to evaluate the proposed algorithms' ability to detect and hence protect from these attacks.

ACKNOWLEDGMENT

First, I would like to express my sincere gratitude and deep gratitude to Allah Almighty as with Allah blessing I have successfully completed this Thesis. I would like to express my appreciation to Prof. Tamer Khattab and Prof. Ahmed Massoud for their professional support, patience, guidance, motivation, and encouragement. Besides, I would like to express my special thanks to my family for their support, inspiration, and motivation.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

1.1 Motivation

The evolution of electric power distribution systems into the smart grid (SG) system mandates the transformation from one-way communication and electromechanical power grid into an advanced decentralized digital infrastructure, as shown in Figure 1. SGs functionalities include two-way communication, equipment control, and energy distribution. SGs provide flexible operation for consumers' interface and can integrate various types of energy sources. Although the two-way communication network is the basic structure of an SG, it increases the network's complexity and adds new challenges by increasing its vulnerability to cyber-attacks. As a result, a cybersecurity strategy with new approaches to secure the network and save privacy is needed for SGs. Developing practical approaches for securing the computation and communication networks of the electric power infrastructure is the way to secure and defend the SG data's privacy.

According to the National Institute of Standards and Technology (NIST), there are two main characteristics for the SG; the increase of using digital information and control technologies to improve overall electric grid operations, and the need for dynamic optimization of the grid operation with full cybersecurity [24].

Cybersecurity for the power industry addresses a wide range of topics, including (i) automation and communications that concern the operation of electric power systems, (ii) the functionality of the utilities that manage them, and (iii) the business operations relating to customers and financial transactions (billing and charging). More attention has been given to the equipment implementation in the power industry, which directly improves the power system reliability. A substantial degree of coordination can be achieved with communication networks linking this equipment. On the other hand, the communication network's existence affects the reliability of the power system and increases the probability of security threats as the system becomes more vulnerable to cyber-attacks. In particular, if the attackers can penetrate a network, get access to control software, and modify the power system settings to destabilize the grid, large scale damages might be introduced.

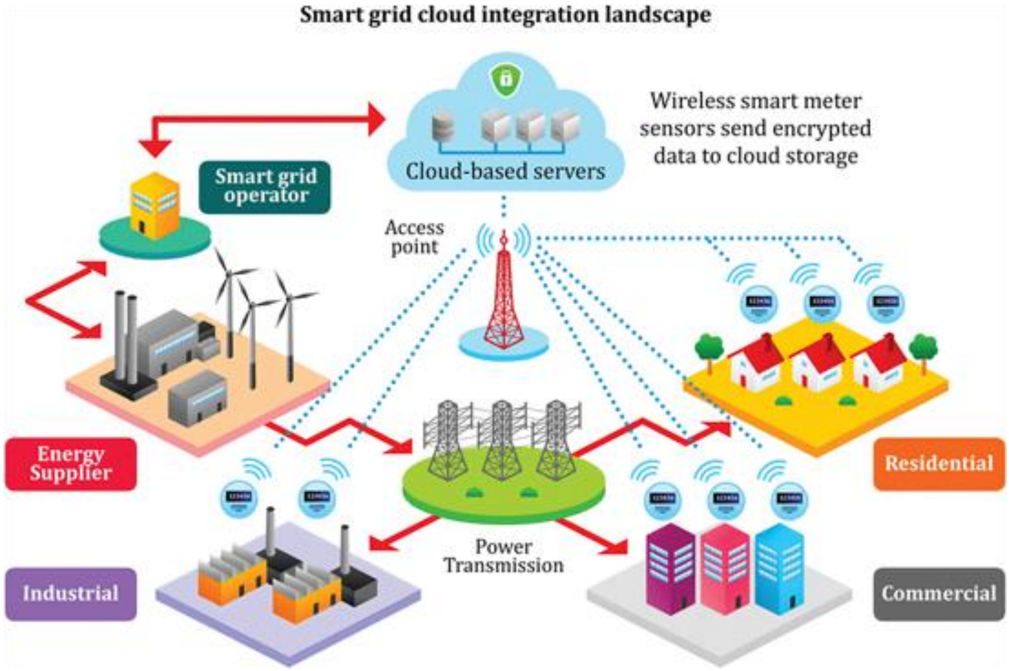


Figure 1.Smart grid evolution.

Therefore, addressing critical cybersecurity scenarios of the SG to detect attacks and protect against their potential undesired effects help in understanding and improving the existing technologies and potentially may introduce new ones.

1.2 Electric Distribution Network Background

The electric distribution system covers all parts of the electric system from the sub-transmission to the customers. It includes distribution substations, primary distribution feeders, distribution transformers, voltage regulators, and protective devices. The sub-transmission usually distributes electric power from the power source to the distribution substations. The distribution substation consists of power transformers with the appropriate voltage regulators, bus bars, and switchgear to reduce the transmitted voltage to a lower voltage.

Historically, electricity was not transmitted but preferably generated at the same place of usage (loads). European and US cities had the first power distribution systems established at the same time to supply lighting where the former used arc lightings running on nearly 3000 V AC or DC, and the latter used light bulbs running on a low voltage of 100 V DC [37].

In the case of high voltages needed in the arc lighting, one station can generate enough power for a long line of lights reaching 11 km. Doubling the voltage would allow transmitting the same amount of power four times the distance for a given power loss using the same cable dimensions. In low voltage light bulbs, some modifications in the Edison Pearl Street Station installed in 1882 enabled supplying customers after 1 mile. Adding thick copper conductor cables and photovoltaic generators (PV) within 1.5 miles supports such systems [37].

Electric power systems have been traditionally based on sizeable centralized generation stations at a relatively small number of locations where the power flow is unidirectional (from the generation stations to the loads). However, in SGs with distribution generators (DGs), electrical power systems have decentralized generation stations located at distribution sites and communicating with each other. The DGs' addition to the conventional distribution system introduces some challenges to the voltage profile, network protection, transient stability, power flow, and fault current.

1.3 Development of Smart Grids in Distribution Networks

The new system joins electric power generators with customers within a wide range area using distribution networks called the SG. This new system needs monitoring schemes to guarantee the system's reliability; the state estimation technique offers an estimation of the power grid state during the analysis and modeling time [64]. SG initiatives yield a highly reliant grid on its cyberinfrastructure to ensure the significant number of power applications needed to deliver better monitor and control abilities to the SG. The conventional power grid is used to transmit power from central generators to several customers. However, the SG uses bidirectional flows of electricity and information to distribute power in more effective ways.

1.4 Voltage Regulation in Smart Grid Distribution Network

A significant increase in the dispersion of renewable energy generators such as PV, wind turbines, and fuel cells in distribution networks occurred to cover the increasing electricity demands. These renewable energy sources are expected to reach 19% of the total power produced between 2007-2030, and the PV generators bear the most substantial portion of this trend [26]. Distribution networks with such large dispersion of PVs encounter many challenges. On a typical day, the characteristic load curve has a high demand load-interval that coincides with an interval of small or zero PV power production on a typical PV source power profile. This leads to a considerable voltage drop and network overloading.

Moreover, reverse power flow may happen due to the excess power generated by the PV at the maximum power point while the load is at the off-peak interval, which may cause power quality problems. Voltage violations (overvoltage or undervoltage) and overloading in the network increases the challenge in SGs [27]. The mentioned problems may harm appliances and sensitive electronic devices. Depending on the connected PV generation level, many resources can be utilized to compensate for the voltage problems. The primary compensation resources suitable for low voltage (LV) networks on the customer side include PV inverter active power, PV inverter reactive power, and distributed energy storage unit (DESU).

Regarding voltage regulation, the electric utility goal is to deliver electricity to clients at a predefined standardized voltage level (e.g., 220 V or 240 V). Though, due to the distribution feeder, the voltage magnitude to customers fluctuates. According to regulations, the supplied voltage must lie within an allowable range of ±5% [72]. Under varying load conditions, the following types of devices are usually employed to sustain the supplied voltage level within this tolerance band:

- Load tap changer (LTC) at the substation transformer, which adjusts the voltage supplied to the feeder by changing the turns ratio.
- Capacitors to reduce the current flow to loads that consume reactive power, which decreases the voltage drop.

1.5 Thesis Scope

Promising future comes with green energy usage worldwide using PV generators, which decreases the need for fossil fuel, reduces the emission of unwanted gases, and has financial benefits. The inclusion of green (renewable) energy sources into the grid mandates the transformation into SG systems. In this respect, an intensive study on voltage stability support and coordinated control contribution are crucial elements to having a robust power system.

Communication infrastructure that guarantees two-way information between different SG assets is needed to provide online voltage stability support from renewable generation plants. Attacking this communication system brings threats on the grid with overvoltage or undervoltage, economic problems, and, in the worst case, a complete blackout. Recently, the threats on SGs exhibited an apparent growth through cyber-attacks directing the attacks towards the electric grid and its critical infrastructure. The field of cybersecurity in SGs emerged as a result of this trend.

This thesis addresses the impact of cyber-attacks on voltage regulation in distribution systems with highly penetrating PV systems and proposes a novel approach based on perturb and observe at the power system level to detect cyberattacks on the SGs. It assumes that the cyber-attack has managed to penetrate the communication network cybersecurity defense and has already injected falsified readings into the network control. Accordingly, the thesis studies the potential undesired effects of such a scenario, how to detect them at the power network level, and how to minimize/prevent their undesired effects.

1.6 Thesis Contribution

Since the start of cyber-attack threats on the SG voltage profile, the primary studies have focused on detecting and preventing cyber-attacks at the communication network level using classical data/context anomaly detection methods. The work in this thesis addresses attack detection and prevention using active power grid equipment and techniques, which introduces a second layer of cyber defense to the SG and the classical communication network defense layer.

The main contributions of this thesis can be summarized as follows.

1. Study the potential effects of cyber-attacks (that penetrate the communication network cyber defense layer) on a smart distribution system's voltage profile with a high penetration of PVs through highlighted different scenarios.
2. Propose an active power grid layer approach using perturb and observe technique to detect and protect the distribution network against cyber-attacks on voltage regulation.

1.7 Thesis Objectives

Within the scope of the thesis and its main target contributions listed in the previous section, the overarching objective of this thesis can be stated as follows: Study the effect of overvoltages and propose a second layer of cyber defense in SGs through devising a power grid layer algorithm capable of detecting and preventing induced overvoltage attack scenarios in LV distribution networks with high penetration of PV sources.

In this thesis, the overvoltage problem due to high PV penetration in LV distribution networks is addressed and analyzed. Besides, a review of the cyber-attacks in the SG is conducted to realize their types and highlight the cyber-attacks that consider voltage profiles in the LV distribution networks. The algorithm for protecting from the overvoltage cyber-attacks in LV distribution networks is presented with simulation results to validate the proposed method.

The thesis objectives can be summarized as follows:

- Review literature on voltage regulation and the voltage violations in the SG. Moreover, cybersecurity and corresponding cyber-attacks on the SG with high penetration of PV are reviewed.
- Study the effect of adding renewable energy sources on a radial feeder distribution network on the voltage profile.
- Study the cyber-attacks that penetrate the communication network layer security defenses effects on the distribution transformer of distribution networks.

- Propose a power grid-based algorithm for detection and protection against cyber-attacks in smart distribution networks with highly dispersed PV generators as a second layer cyber defense mechanism for SGs.

1.8 Thesis Flow

In this thesis, we present six chapters, where Chapter 1 shows the work's motivation and the main contribution along with the objectives as laid out in the previous sections. In Chapter 2, a literature survey covering the work related to the scope of voltage violation problems and cyberattacks with the cybersecurity defense is presented. Chapter 3 highlights the voltage violation in the low voltage distribution network and discusses the effect of the PV penetration on the network's voltage profile. Chapter 4 discusses modeling the cyber-attacks on a simple distribution network to highlight the voltage violation effect resulting from these attacks. In Chapter 5, a modified distribution network is introduced with a detailed voltage mathematical analysis. A sensitivity and behavior analysis is applied to the network using the same attack models presented in Chapter 4. Two proposed algorithms for detection and protection using PV perturbation and observation methods were introduced and applied to the network. Results under different case studies were deduced and discussed. Finally, Chapter 6 presents the conclusions along with future work.

CHAPTER 2: BACKGROUND AND LITERATURE SURVEY

With the increased penetration of distributed generation (DG) in power systems, the move towards SG systems is accelerating. Accordingly, the need for using communication networks in power systems has increased. Due to the deployment of communication networks in the power systems, the number of attacks is expected to increase, which may cause a severe problem. Recently, the volume of research and studies conducted on cybersecurity technologies in the SG and their role in improving the quality of monitoring and decision making has been steadily increasing. A review of the state-of-the-art research in this area is conducted in the following sections, along with a description of the main concepts involved.

2.1 Smart Grids

The U.S Department of Energy defined the conventional grid, *the electric grid*, as the network of transmission lines, substations, and transformers that work together to distribute electricity from the power generator to the customers. The current electric grid was built in the 1890s and enhanced over time. Today, it contains more than 9,200 electric generation units and more than 1 million megawatts of generation capacity and distributing feeding with more than 300,000 miles of transmission lines [66]. To move forward, we need a new kind of electric grid that can systematize and control the increasing difficulty and electricity requirements in the 21st century.

This National Institute of Standards and Technology (NIST) describes SGs with more technical oriented terminologies: "*Advanced power grid for the 21st century includes the addition and integration of many varieties of digital computing and communication technologies and services into the power delivery infrastructure. Bidirectional flows of energy and two-way communication and control capabilities enable an array of new functionalities and applications that go well beyond 'smart' meters for homes and businesses.*" [25].

The digital technology that permits two-way communication between the generator and its customers in addition to sensing along the transmission lines is what makes the grid smart. The SG consists of controls, computers, automation, and new techniques and equipment working together. These components work with the electrical grid to respond digitally to the fast variation in the electric demand.

The SG is anticipated to upgrade the energy industry to new levels of reliability, availability, and efficiency, which are needed for modern electric systems' proper operation. The SG has several benefits, according to [68], including:

- Higher efficiency in the transmission of electricity.
- Faster response to the power disturbances.
- Lower cost for both utilities and consumers.
- The decrease in peak demand decreases electricity rates.
- Allow high penetration of large-scale renewable energy systems.

- Better integration of customer-owner power generation systems, including renewable energy systems.
- Improved security.

SGs collect and maintain the electric grid data and provides the techniques and technologies required to utilize the data to make efficient decisions about the energy utilization over the network.

The characteristics of SGs are typically discussed in terms of their economic benefits, security advantages and challenges, and their ability to support renewable energy sources. However, SGs have benefits to end-users as well by allowing a unique level of customer involvement. For instance, there is no need to wait for the monthly usage report to know the user's electricity consumption profile. Smart meters and other mechanisms allow monitoring the availability, usage, and cost of electricity. Joint with real-time dynamic pricing, it permits saving money by consuming less power when electricity is most expensive.

SGs come with their set of challenges as well. The work in [39] defines the Advanced Metering Infrastructure (AMI) as an architecture for automatic, two-way communication between a smart utility meter and a utility company. A smart meter typically tracks power consumption in a more detailed way than a conventional meter and transfers the information back to the utility for monitoring and billing purposes. Moreover, customers can be up-to-date on how much power they consume, which helps them in making decisions on how to modify their power consumption profile to minimize energy costs. Moreover, by managing the peak load through consumer participation as well as distributed energy generation and storage, the utility is likely to provide electricity at lower rates for all. Such heavy dependence on information networking increases the possibility of vulnerabilities associated with communications and networking systems in SGs. Indeed, the heavy dependence on communication networks increases the risk of compromising the reliability and security of power systems operation, which is, ironically, the ultimate objective of SGs. Network intrusions by adversaries may lead to a variety of severe consequences in the SG, ranging from customer information leakage to a cascade of failures, such as massive blackouts and destruction of infrastructures as well as user's equipment.

2.2 Cyber-attacks

In general, an attack on a network is any effort to change, disable, damage, steal, or have illegal entree to a network. A cyber-attack is any kind of violent or undesired behavior that goals computer information systems, infrastructures, computer networks, or personal computer devices. Depending on the attack's situation, these attacks can be either cyberwarfare or cyberterrorism [69]. These attacks can be hired by nation-states, individuals, groups, society or organizations.

A cyber-attack may affect a specific target by hacking into a vulnerable system. Attacks may happen personally as installing spyware on a personal computer or at a higher level, like destroying nations' infrastructure. There is a significant national and international effort to bound these attacks and try to detect and prevent them. Meanwhile, cyber-attacks are becoming increasingly sophisticated and dangerous.

Government and infrastructure targets have a severe effect on people’s lives and are considered critical targets for cyber-attacks. Examples of such targets are industrial control systems, energy resource management systems, financial institutions, telecommunications infrastructures, transportation systems, defense and security entities, and water facilities [66]. Figure 2 shows different cyber-attacks in the last ten years around the world.

As a single example, the work in [40] established an industrial control system testbed and examined two operative cases, namely, water level control and air pollution control. They proposed an automatic-learning based method for malicious intrusion detection, which is used to conduct various tests on the developed testbed. Their results show that their method can effectively detect various kinds of network attacks.

In December 2015, SANS institute [65], in cooperation with the Electricity Information Sharing and Analysis Center (E-ISAC), published a report about the Ukraine’s Power system's cyber-attack incident in which the system experienced a wide-area power outage affected 225,000 customers.

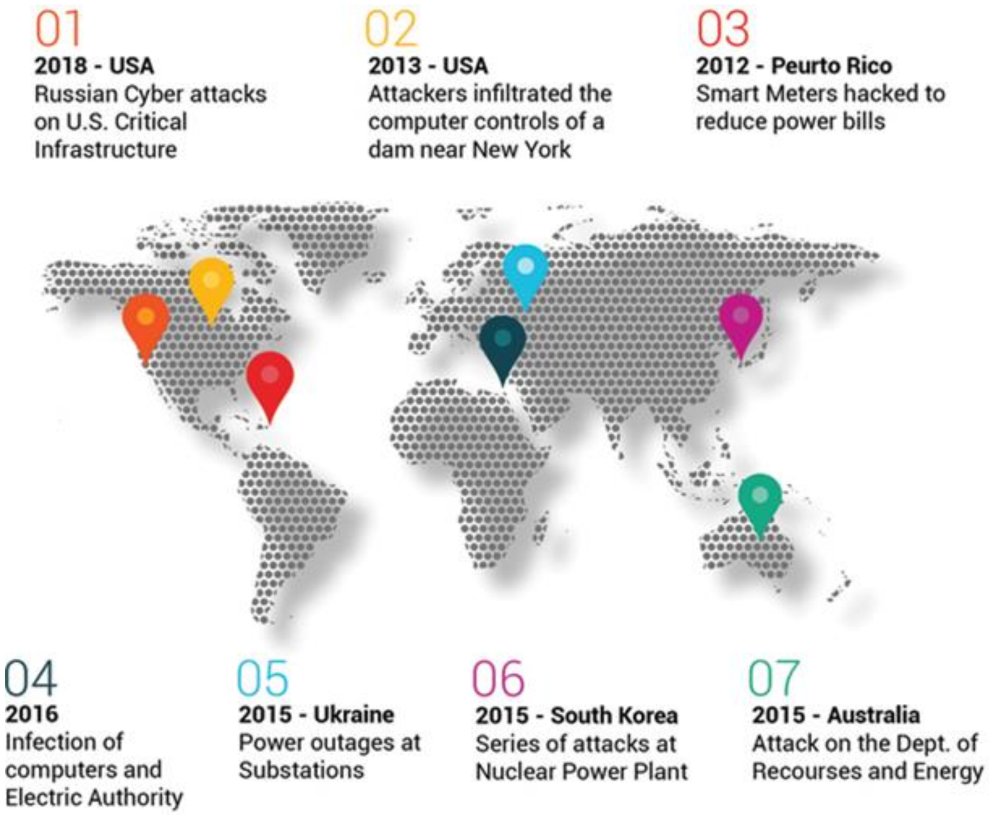

01
2018 - USA
Russian Cyber attacks on U.S. Critical Infrastructure
02
2013 - USA
Attackers infiltrated the computer controls of a dam near New York
03
2012 - Peurto Rico
Smart Meters hacked to reduce power bills
04
2016
Infection of computers and Electric Authority
05
2015 - Ukraine
Power outages at Substations
06
2015 - South Korea
Series of attacks at Nuclear Power Plant
07
2015 - Australia
Attack on the Dept. of Recourses and Energy

Figure 2. Different cyber-attacks on the substations around the world.

2.3 Cybersecurity

Researchers have studied cybersecurity in power systems to assess cybersecurity risks and find solutions to improve power grids' security [41].

The threat due to cyber-attacks has become a fundamental challenge to address to achieve the safe operation of an SG. More than 46 cyber-attack incidents were identified in the energy area during 2015 [44]. The majority of these attacks targeted the information technology (IT) subsystem of the SG. The U.S. Department of Energy (DoE) suspects that the actual number of cyber-attack is higher than reported [42]. To recognize, detect, and prevent cyber vulnerabilities in an SG, approaches should be developed to detect cyber disturbances and reduce their effects.

Security for industrial control systems, including control systems distributed and SCADA systems, always attracted researchers and industry parties' attention equally, particularly the security issue in systems related to critical infrastructures like electricity, water and sewage water, oil and gas, chemical, etc. In history, industrial control systems are considered exclusively, unlike the typical information technology (IT) systems as the traditional system were disconnected from the bigger enterprise systems and use exclusive components [59]. In reference to NIST Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security," when mainstream solutions became available at a lower cost with conventional technology and the Internet of Things (IoT), this began to change.

ICS depends on widely existing computers, networks, and operating systems, that offer better elasticity in the design of the system and system integration, at the same time that generating higher risks and difficulties for the ones who in charge of engineering, construction, maintenance, and operating these systems. By transferring to the use of widely integrated technology, the system designers and control operators experience the challenge of platform security, which may have illegal access by attackers.

Currently, worldwide compliance commands, like the European Union’s General Data Protection Regulation (GDPR), are obliging companies to have extra practical actions to prevent cyber-attacks. with these challenges and possible exposures, many safety measures could be used to reduce risks at the same time have the benefits of the recently integrated systems.

CISCO defined cybersecurity as the way of protecting systems, networks, and programs from digital attacks. These attacks are generally intended to access, alter, or destroy important information, stealing money, or disrupting processes. Cybersecurity combines a set of tools, technologies, risk management methods, and best practices to protect networks, programs, and/or data from any risk of unauthorized/undesired access.

Due to the heavy dependence on information networking, SGs have more potential vulnerabilities related to communications and networking systems. Accordingly, the risk of compromising reliable and secure power system operations in SGs has increased. As a result, more investigations in the SG cybersecurity issues are carried, and cybersecurity has evolved into an essential aspect in the design of information networks in SGs [5].

The SG communication network is a very critical infrastructure tool for information exchange. To guarantee a secure and reliable operation, it is vital to identify what are the cybersecurity objectives and requirements for this network. There are three main objectives for SG security that need to be addressed [6]:

- Availability: Ensuring timely and reliable access to information is the most critical objective in the SG. Because any loss of accessibility may cause an interruption of access to the information, which weakens the power transfer.
- Data Integrity: Defensive against inappropriate data alteration, which can lead to incorrect decisions regarding power management.

- Confidentiality: Conserving authorized restrictions on information access, mainly to protect personal privacy and proprietary information.

In addition to these high-level objectives, the National Institute of Standards Technology NIST report [6] defines two security requirements for the SG, including cybersecurity and physical security. The cybersecurity part agrees particular matters and requirements associated to SG security, in the other hand the part that agrees necessities relating to physical part and environment safety known as physical security.

2.4 Cyber-Attacks in Smart Grids

To guarantee the privacy and integrity of the grid data, cryptographic protection approaches of communication are applied. Many conventional protocols and devices used in the power systems' communications networks; such as MODBUS protocol, Distributed Network Protocol 3.0 (DNP3) used in supervisory control and data acquisition (SCADA), communication standard for Substation Automation System (SAS), Phasor Measurement Unit (PMU) and Distributed Energy Resources (DER); were developed before cybersecurity grew into a serious concern. New developments and upgrades have been proposed on their authentication frameworks [45]-[49] to secure these communication protocols.

Vulnerability assessment helps protect SGs by studying cyber-attack events in detail and incorporating the relations between the cyber system and the physical system. Many attackers target SCADA as it is a fundamental component in control systems. The authors in [53] illustrate how the exchange of information between several power units through wide area networks (WANs) is the primary source of vulnerabilities. SCADA links the different SG subsystems, like the Advanced Metering Infrastructure (AMI), DER, and Distribution Automation (DA) systems. Once attackers can access the SCADA network, they can inflict severe damages. A high number of smart meters convey benefits to the distribution system's operation, but it may bring cybersecurity worries, such as confidentiality, data alteration attacks, and illegal load control remotely. The attacker could access the AMI network through any public node. Such issues show that one layer of cybersecurity defense cannot deliver enough SG security and protection.

AMI cyber-attacks have been discussed in the literature, like power theft, false data injection (FDI), and customer information access [54]–[57]. Many standards and guidelines were issued and published to ensure the SG proper operation along with high cybersecurity. Ref [58] suggests fundamental guidelines for power grids data communication systems. A “Roadmap to Achieve Energy Delivery System Cybersecurity” is issued by the Energy Sector Control Systems Working Group (ESCSWG) for the same purpose [56], and another SG cybersecurity guideline, NISTIR 7628, was issued by NIST [57].

The work in [13] presents the importance of using a distributed security system through peer-to-peer communications, reputation-based trust, and data retransmission schemes to prevent undesirable attacks. The concerns of using Internet-like communication have been investigated and summarizing in two points. First, the power system's dependency on communication systems may make it breakable while unprotected from cyber-attacks on the communication network or system deficiency. Second, the reliance on the communication systems to protect and control the power grid creates an attractive target for the attackers and increases the risk of Byzantine failures.

The authors in [14] assessed and compared several robust state estimation methods in different configurations of attacks. They focused on the likely attacks on the Jacobian matrix through state estimation (SE) and the effect on robust estimators like the least trimmed squares estimator (LTS). It is shown that the attacks on the Jacobian matrix man introduce an increase to leverage points that are difficult to manage in practice even if randomly generated. Also, they generated an untraceable stealthy corruption scenario that poses dangers to strong SE. These attacks were generated theoretically for this context. The authors also well-defined masked attacks and studied the detection abilities of the common approaches in power systems, theoretically and numerically.

In [12], the effect of compromising the measurements of the network on the electricity cost was studied. The attacker is assumed to cause a variation in the prices by changing the tariffs. The condition is designed as a zero-sum game among the protector and the attacker. The model expresses the times proportion in which both defender and attacker may defend and attack several measurements, correspondingly. The outcome of simulations on the PJM 5-Bus test system presents the strong ability to attack the electricity charges on actual markets.

The work in [15] proposed a bilevel mixed-integer linear programming (MILP) designed to find out the least number of readings to be secured to reduce the risk of cyber-attacks. A decomposition technique to find a partially optimal solution has been introduced.

The work suggested separating the power grid into subnetworks using the MILP approach to reduce the computation complexity further.

Smart grids are exposed to a growing amount of cyber-attack actions due to the high IT integration and discovered that attackers could significantly raise the charge of the power system operation by FDI attacks. The attack vector can be found by computing a bi-level linear programming (LP) problem and solve it, which becomes complicated for big systems [12].

The work in [16] proposed a primary technique to determine an efficient attack vector, which may generate an essential raise in operating charges. The approach uses the solution of an LP formulation. The modeling outcomes on the IEEE testing systems prove the efficiency of the mentioned approach.

In [17], FDI attacks on state estimation in smart grids were inspected. The authors showed that an attacker could exploit a power system's configuration to launch such attacks by generating random faults into confident state variables and avoiding the existing bad data detection techniques. The work investigates two realistic attack scenarios: (i) the invader is controlled by some specific meters because of the meter protection, or (ii) the attacker has limited resources that can be used to compromise meters. It was shown that the attacker could efficiently build attack vectors in these two scenarios that could alter the state estimation outcomes and adjust these outcomes randomly. The work demonstrated the accomplishment of such attacks using IEEE testing systems. The conclusion was that the smart grid security should be rechecked with possibly malicious attacks.

The authors in [18] presented a security-oriented cyber-physical contingency analysis (SOCCA) model that finds contingencies probable from attacks, with existing cybersecurity in the power system's control network. SOCCA offers smart grid security operators with abilities for evaluating the effect of such malicious behavior on the power grid. Therefore, it allows operators to choose upon the proper assignment of solutions to prevent any proactive intrusion. Their outcomes present that SOCCA uses conventional power contingency analysis techniques that assume actual power component failures from accidental failures and other normal reasons.

[19] presented a survey on cybersecurity in the SG. The work highlights many methods of cyber-attacks against the SG. The discussed attacks cover jamming in substations, Address Resolution Protocol (ARP) spoofing, buffer flooding, and traffic flooding. The authors present a detailed study of cyber-security problems for the SG. They mainly focus on studying and analyzing security needs, network vulnerabilities, secure communication procedures, and architectures in the SG.

The work in [20] discusses the physical cyber-security of Wide-Area Monitoring, Protection, and Control (WAMPAC) from a specific cyber-attack viewpoint and presents a game-theoretic method to solve the issue. Then it defines how physical cyber-security testbeds could be utilized to estimate the security study and accomplish accurate attack-defense research for SG conditions.

In [21], the authors focused on cyber-attacks that aim to use data integrity in SG networks. They investigated the effect of FDI attacks on SM control systems. They focused on the parametric feedback linearization (PFL) controller and derived closed-form terms for the faults in rotors’ speed and angle because of cyber-attacks on data integrity. Additionally, they investigated adaptive control approaches to remove or mitigate the effect of FDI attacks on system dynamics.

[22] discussed four detailed attack cases for cyber elements in SCADA systems networks, which can disconnect breakers of actual parts. Two Bayesian attack diagram models are constructed to explain the cyber-attack methods and estimate the chances of significant cyber-attacks. The load loss possibilities in the IEEE reliability test system RTS79 is assessed, with more breaker disconnections caused by the cyber-attacks. The modeling outcomes reveal that the SG reliability decrease as the rate of significant attacks on the cyber components rises and the ability level of attackers grow.

A study in [63] showed that the detection probability of attacks increases when the error on parameter estimation increases. According to the detection probability and attack impact metrics, the attack depends on the system model's knowledge in the first place. An attacker with full knowledge and limited attack resources causes more damage than an attacker with limited knowledge and enough attack resources.

The research in [64] addressed detecting successive unobservable cyber data attacks on PMU measurements by formulating the identification problem as a matrix decomposition problem of a low-rank matrix and a transformed column-sparse matrix. It proposes a convex-optimization-based solution method and provides its theoretical guarantee. The resulting matrix decomposition approach can be applied to other scenarios.

In contrast to the previous methods which focus mainly on data and network methods for attack detection, the study in [65] proposed an algorithm that checks the sensor measurements and determines whether the current values are normal or not. This approach is considered a power system layer approach; however, it is a passive algorithm as it uses calculated and measured reading for the voltages.

2.5 The Voltage Violation Problem

2.5.1 Voltage Regulation in Distribution Networks with PVs

Consistent growth in load demand has led to new plans for maximizing electricity production, including renewable energy sources such as wind, PV, tidal, etc. With the increasing penetration of DGs, the distribution networks are expected to experience a significant change ranging from structure perspective to mode of operation perspective. Distribution networks are transforming from passive to Active Distribution Networks (ADNs), including the role of energy collection, transmission, storage, and distribution [1].

Also, the addition of DGs may have negative consequences on the distribution system, mainly that the network has been classically operating in the top-down approach mode, where the flow of electricity is predictable since the power is transmitted from the higher voltage (generation) side to the lower voltage (load) side. However, this is changing due to DG sources' penetration, which leads to bidirectional power flow and a non-uniform voltage profile [2].

High dispersion of PV generators in LV distribution networks raised additional new challenges in terms of power quality. The work in [67] explores power quality issues using practical field tests with two different sizes of PVs; 1.5 MW and 3.3 MW. The authors estimate the probability of voltage flicker severity in the network. The authors in [30] present an analysis of several techniques and approaches. These approaches avoid overvoltage in the distribution system in the LV side connected to the PV and discuss the full effects of each of these techniques. The proposed explanation contain grid reinforcement, batteries and others. The authors show that collaboration between the techniques of overvoltage regulation and organization between voltage control units improves the PV hosting size of LV feeders in the grid.

In [31], the authors propose a control approach that allows high dispersion of distributed energy sources in a low-voltage grid. Four control approaches were reviewed and compared to develop a modified technique called a three-phase damping control technique. This technique was shown to have the most effective benefit on the other control techniques' voltage profile.

The authors in [32] tried to predict any disturbance in the network, such as overvoltage, caused by the high penetration of PVs. The article studied seven training approaches utilized in artificial neural networks for time-based estimate of the produced active power and the distribution network state. The results are compared to the classical Support Vector Machine (SVM) technique, to conclude that the Bayesian Regularization and the Artificial Neural Network have better performance and are more suitable for addressing this problem compared to SVM.

In [33], the authors proposed an approach based on the coordination of multiple battery energy storage systems (BESSs) for voltage control in low-voltage distribution networks (LVDNs). This method aims to solve overvoltage problems using a real-time digital simulator and a MATLAB model of a real UK LVDN with a high dispersion of PVs. It was shown that the proposed coordinated control has a more robust and efficient role in preventing voltage rise problems in LVDNs. The advantage of this method is that it reduces the costs of battery replacement to the storage operator.

The work in [34] underlines the use of solar inverters with reactive power control to increase the dispersion level of PV power production. The sensitivity analysis shows that the solar inverter's location plays a fundamental role in the efficiency of the reactive power for the grid voltage support. For example, locating the solar inverter at the radial feeder gives more efficiency for the same amount of reactive power. With this essential knowledge, a location-dependent power factor set value can be allocated to each inverter, and the grid voltage support can be accomplished with lower reactive power consumption. A new approach was proposed to avoid pointless reactive power absorption from the grid through an acceptable voltage range or to enhance reactive power contribution from the inverters closest to the transformer during a grid overvoltage condition. The new method was presented in terms of the injected active power and the local grid voltage-dependent reactive power.

In [35], a new approach is used for reactive power control, which considers the inverter’s capacity. This approach controls the overvoltage by selective var injection based on the inverter position, capacity, and minimum power factor. This approach improves both the voltage regulation and the inverter's reactive power capacity.

The work in [36] explores how shortages in both reactive power control (RPC) and active power control (APC) as separate approaches can be mitigated by combining them.

Strategies with a combination of two RPCs, as well as a combination of one RPC with APC, are proposed as two coordination algorithms using the instantaneous measurement of node voltage and active power. These coordination algorithms are fixed in all the rooftop PV DG grid-tied inverters (GTIs), where the GTIs coordinate among themselves for voltage support without exceeding individual inverter volt-ampere rating. The resultant strategy gives a significant enhancement in voltage management.

2.5.2 Cyber-Attacks Induced Voltage Violation

In distribution networks, voltage regulation is essential for sustaining the power quality at the consumer’s side. Online Load Tap Changer (OLTC) is used for controlling the voltage to maintain an allowable range. Different voltage control schemes are applied in different parts of the power system to maintain voltage levels within limits. Excitation control and voltage regulators; transformers OLTCs; shunt capacitors; static shunt compensation and thyristorized control for step-less control of reactive power; and synchronous condensers in receiving end substations for reactive power compensation are examples of such schemes.

Conventional control methods are based on the line drop compensator (LDC). The principle of these methods is based on estimating the voltage at a particular remote point in the network via local measurements at the substation.

The voltage profile of the feeder depends on the feeder layout. If no DG is connected in LV radial feeders, the voltage profile is uniform and decreases when moving from the feeder upstream to downstream. However, when DGs are connected to the feeder, the DG injection of active power may cause a steady-state voltage rise in the feeder. This changes the profile characteristics to a non-predictable and complex voltage profile, limiting the applicability of LDC. This may be avoided by sectionalization and employment of IT switches (switches with sensors) in the feeders. These IT switches are equipped with sensors for phase, voltages, and currents. They also have voltage and current transformers. The IT switches are connected to the voltage regulator using optical fiber cables to send their voltage measurements with certain sampling periods [64].

The voltage regulator is added to obtain a more precise voltage profile across the feeder in real-time. It determines the required output voltage level of the transformer LRT and hence, its tap position. The use of voltage measurements needs real-time data exchange via communication networks. This may increase the risk of cyber-attacks by increasing the chances of hacking the data and injecting falsified information, affecting the voltage regulation. The conventional LDC mostly uses local information; therefore, it might be more robust to cyber-attacks. On the other hand, and with DGs' penetration, it might fail to regulate the voltage correctly. The attacks may occur through the Internet, hacking into the communication network, hacking into the substation, or even hacking into the control center [64].

2.6 Remarks on literature

Different cyber-attack approaches in SG systems were introduced, emphasizing cyber-attacks targeting the voltage regulation component of the power grid. Some of the proposed methods, models, modified protocols, and algorithms to detect and protect SG's power distribution system were discussed. It is noticed that the existing literature lacks (does not adequately address) two key aspects of cybersecurity in SG systems: (i) the high penetration of DG (particularly PV sources) and (ii) actively utilizing the physical properties of the power distribution layer to achieve cybersecurity detection and protection mechanisms in addition to the conventional communications network layer based detection methods.

The proposed mechanisms in this thesis can be classified as active detection and protection algorithms. The thesis introduces a new approach to mitigate cyber-attacks on power distribution systems by using a second layer (the power distribution layer) of detection and protection against voltage violation attacks targeting SGs with high penetration of PV-based DG. The utilized perturbation and observation idea to detect and prevent cyber-attacks is considered a cybersecurity approach implemented at the SG power distribution layer.

CHAPTER 3: MODELING CYBER-ATTACK INDUCED VOLTAGE VIOLATIONS

This thesis focuses on voltage regulation cyber-attacks in low voltage distribution systems with high penetration of PV-based DG systems. We start our work in this chapter by describing the proposed system assumptions, characteristics, behavior, model, and mathematical representation.

3.1 Low Voltage Distribution Networks with High Penetration of PV-based DG

Electricity consumption is expected to increase by about 25% by 2040 [70]. A vast evolution of electricity generation capacity is necessary to match the electricity demand in the future. There are many ways to generate electricity, like traditional thermal plants and distributed generating units. The most significant part of the electricity generation is from fossil fuel, but it has significant drawbacks in our global environment. Recently, for mitigating global warming and supporting sustainable energy development, renewable energies such as wind generation and PV generation have attracted attention worldwide. Therefore, this revolution of using renewable energy in the form of (DGs) is rapidly increasing.

A DG could be dispatchable or non-dispatchable. Dispatchable generation means electricity sources that could be utilized on-demand and dispatched whenever needed by power grid operators, depending on the customer’s needs. These generators could be switched on or off or could alter their power output depending on a specific demand [1], which is the opposite of non-dispatchable renewable energy sources, uncontrollable by the operators. The renewable energy source types that are dispatchable and operate without separating the energy storage are biomass, geothermal, and ocean thermal. Solar PV and wind act as a non-dispatchable source, highly dependent on the amount of energy generated by its prime source, depending on solar radiation and wind speed. The location of DGs at very close to consumers has advantages and disadvantages. First, it decreases transmission and distribution losses and has a low investment risk; it also has a short construction and easy maintenance time. The system operating condition and DGs characteristics, size, and location determine its impact on the distribution system (DS).

Due to the non-continuous characteristics of the renewable generations (RGs), new challenges were added to the distribution system. Although the integration of these RGs in the distribution systems near the customers decreases the transmission cost and power loss, it also affects the power system efficiency, reliability, and quality. The RGs changes the traditional power flow from one-directional flow to a bi-directional flow. Accordingly, an imbalance in energy production and consumption occur. The load voltage fluctuation that happens in the DS produces a problem for the distribution network operator (DNO) in matching demand with energy supplied. The entire network operating system should be revised and controlled in the advanced control system to avoid that. This came up with the SG concept, which offers reliability and optimal utilization of the RGs.

The main problem of the high dispersion of RGs is voltage control and management. It is necessary to keep the voltage within the allowable range to ensure the electrical system's reliability. The intermittency and uncertainty of solar and wind energies are the main problems that should be addressed.

3.2 Effect of PV on the Voltage Profile

The challenges associated with DGs' penetration span different aspects such as voltage levels and power flow, equipment thermal ratings, fault current levels, protection issues, etc. Voltage profile is a common constraint when deploying DGs such as PV generators. The other constraint on the capacity of the installed DG is the thermal limitation due to high current flow through electrical devices such as transformers. Moreover, the bidirectional power flow may affect the protection devices. Also, high penetration of DGs may elevate the fault current levels beyond the permissible limit, which may harm the network protection and power system infrastructure. Increasing the number of connected DGs may cause a rise in the voltage above its allowable level [3], particularly with light loading. Variations of active power injected into the feeder should be compensated to decrease these voltage variations. This can be done with energy storage devices such as flywheels, supercapacitors, or batteries. Considering the aforementioned challenges pertinent to DGs' penetration, an Active Network Management (ANM) scheme is crucial that it deliver synchronization for the operation of the power system. Relating to the work in [4], this scheme ANM was well-defined as using the actual control with the IT systems to deliver better integrations of the renewable generators; it measures or estimates the demand of the several feeders, joined with measurements of the power obtained from DG units.

The voltage rise effect due to DG's connection is illustrated using a simple circuit shown in Figure 3. In this distribution network, the PV generator (including the power electronics converter), with P_{PV}, Q_{PV} together with local load, P_L, $Q_{L,}$ and a STATCOM as a reactive compensator with $Q_{STAT,}$ which is connected to the distribution transformer through a feeder with impedance Z. The transformer is equipped with an OLTC to enable voltage regulation by varying the transformer ratio under load without interruption.

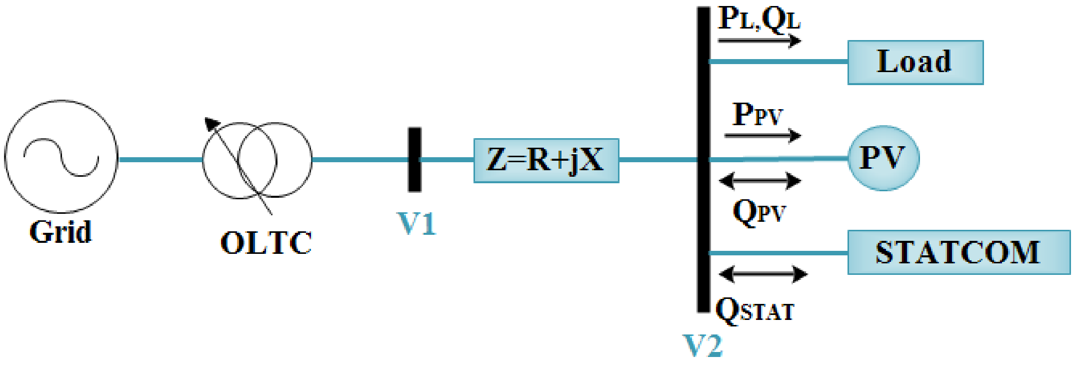


Figure 3. Simple distribution network with distributed generators (e.g., PV)[71].

In Figure 3, the voltage (V_2) at bus bar number 2 can be approximately calculated as in (1).

$$V_2 \approx V_1 + R\,(P_{PV} - P_L) + X(\pm Q_{PV} - Q_L \pm Q_{STAT}), \qquad (1)$$

such that $$V_{min} < V_2 < V_{max}.$$

The PV generators distribute active power (+P_{PV}) and may inject capacitive or inductive power (±Q_G). The load consumes active (−P_L) and injects reactive (−Q_L) power assuming inductive loads at the customer's side. STATCOM exports or absorbs reactive power (±Q_{STAT}). We can use (1) to analyze the relationship between the voltage and the amount of generation that can be connected and the impact of the alternative control actions to manage voltage rise [4].

In LV radial feeders considered in the distribution network, the R/X ratio is relatively high. Then neglecting the factor X in (1) and considering only R, the equation can be written as follows:

$$V_2 \approx V_1 + R\,(P_{PV} - P_L). \tag{2}$$

In (2), we can notice how the insertion of PV generators can directly cause voltage fluctuations due to the variation in their power output and reverse power flow in the highly dispersed distributed generators. On the other hand, these PV generators can be used as a method to mitigate this problem. PV generators usually connected to different types of converters to perform different functions as Maximum Power Point Tracking (MPPT) (DC-DC converter) and grid integration (inverter). These converters can also control the injected power from the PV to the network, which permits to maintain the voltage level in the allowable range. This approach is called active power curtailment. This is merely clear in the relation between the voltage at the second bus V_2 in (2), which is directly proportional to the active injected Power from the PV. The inverter first checks the voltage level at a particular node. If it is in the allowable range, then no action is taken, but if the voltage lies out of this range, the inverter will control the power injected in the network accordingly to compensate for the voltage level.

Maintaining proper voltage regulation in the distribution system is essential to keep proper operating conditions. Voltage variations above the allowable levels may lead to undesirable operation in the distribution system, harm in the utility equipment and customer appliances/devices.

A long radial feeder with the existence of the DG has two critical cases that should be considered:

1. The burdensome loading at a long radial feeder causes undervoltage for users downstream of the network.
2. The light loading and maximum DG power injection may cause overvoltage for users downstream of the network.

3.3 System Modeling

To model the effect of integrated PV on the distribution network, a basic model has been implemented. Figure 4 presents a distribution network with a single feeder to incorporate the effect of PV generators on the voltage variations. This enables an understanding of how the attacks may occur on the network. PV and load profiles are based on data from [23]. The feeder is an LV cable of 0.164+j0.074 Ohm/km [73].

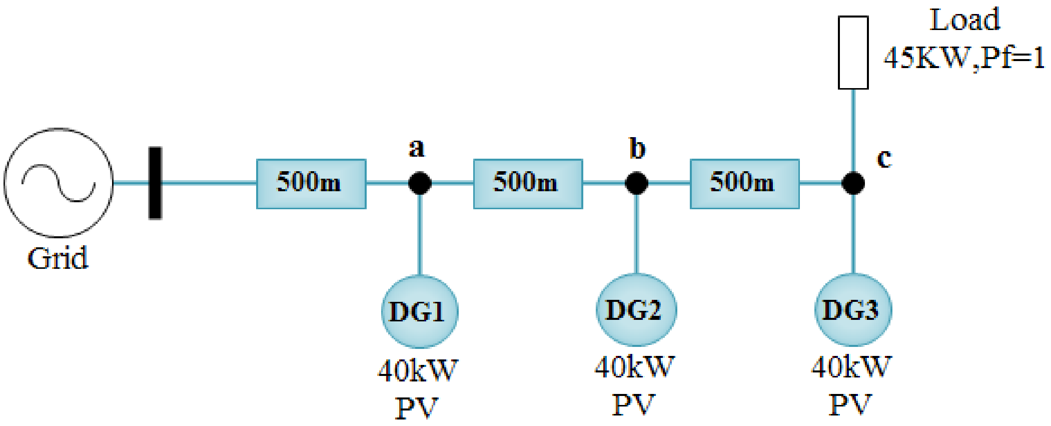


Figure 4. A low voltage radial feeder distribution system.

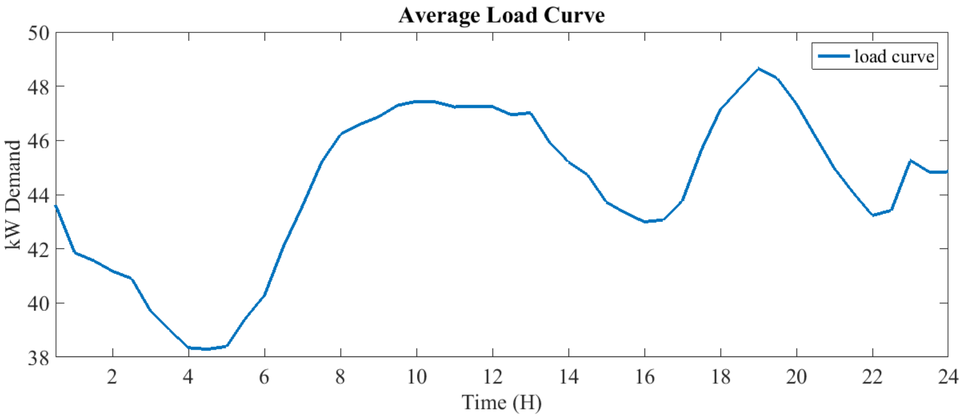


Figure 5. Average load curve of 45 kW for a distribution network [23].

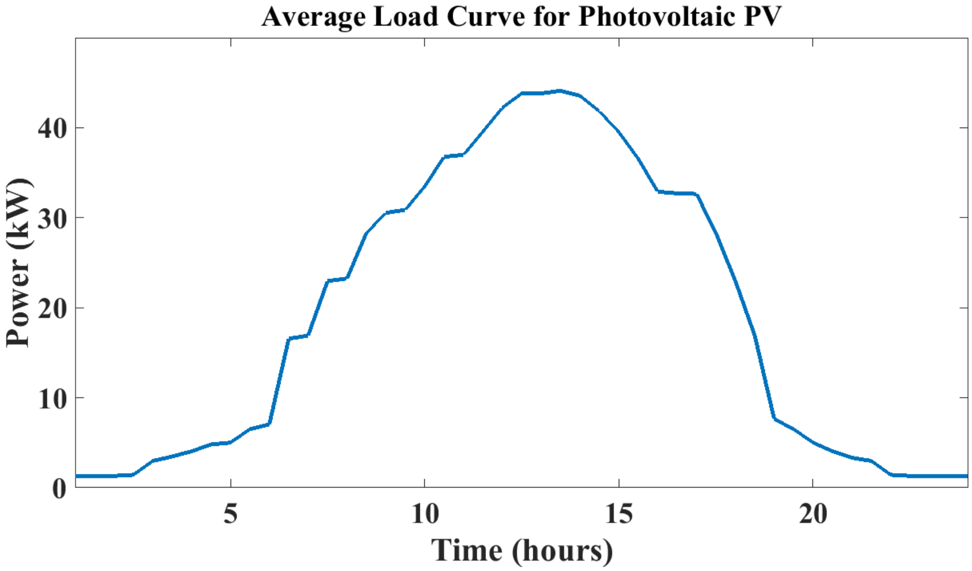


Figure 6. PV load curve.

The PV generator used in the network provides mainly active power. The PV generators are modeled using a controlled current source in Matlab/Simulink. The PV generator is assumed to have a rated power of 40kW with an average load curve shown in Figure 6. This controlled current source is driven by raw data that presents the output power of a PV, as listed in Appendix A.

Using MATLAB, the network shown in Figure 4 was built and simulated to study the network's behavior under different scenarios. The effect of having PVs on the voltage profile in the network is investigated. As shown in Figure 5, an average load curve is used in the network in the simulation to show the variation in the voltage according to the load demands during the 24 hours. To have a clear picture of the relation between the parameters in the distribution system in Figure 4, a system of equations can be derived. The active powers at nodes *c*, *b*, and *a* are expressed as

$$P_c = P_{pv(c)} - P_{l(c)} \tag{2}$$

$$P_b = P_{pv(b)} \tag{3}$$

$$P_a = P_{pv(a)}, \tag{4}$$

where P_c, P_b and P_a are the powers at nodes *c*, *b*, and *a* simultaneously.

The voltage differences $\Delta V_b$and ΔV_a are given by

$$\Delta V_b = Z_c I_c = V_b - V_c \tag{5}$$

$$\Delta V_a = Z_b I_b = V_a - V_b, \tag{6}$$

where the currents in the branches equal to

$$I_c = \frac{P_c}{V_c} \tag{7}$$

$$I_b = \frac{P_b}{V_b} + I_c \tag{8}$$

$$I_a = \frac{P_a}{V_a} + I_b. \tag{9}$$

P_n is the power of node n, $\Delta V_b\ and\ \Delta V_a$ are the voltage differences between nodes (*c* and *b*) and (*b* and *a*) and $I_n$is the current through resistance R_n assuming unity power factor and taking into consideration that these are per-phase equations.

3.4 Problem Definition and Considered Scenarios

This section defines the considered problem of overvoltage and undervoltage at one node by defining the scope of the different possible attack scenarios. We portray these scenarios by mimicking the attacker's role, who induces changes on the source data (i.e., voltage readings) to enforce the PV generators to generate less or more power. The scenarios are illustrated and simulated using Matlab/Simulink platform. All the considered scenarios here assume the single feeder network with PV generators, shown in Figure 4.

A. Attacker modeling

As discussed previously, cyber-attacks have different strategies, such as cyber campaign, cyberwarfare or cyberterrorism. These attacks have two main potential effects: voltage violation in the feeder; and output power loss at PV systems. Regardless of the attacker's target, these attacks cause interruption and falsify the measurements. The attacker falsifies the received measurements at the transformer according to the required objective of the attack. This, in turn, may induce an incorrect and undesired OLTC reaction.

In the simulation model, this has been considered through a control signal. The control signal is used to affect the OLTC by introducing either an undervoltage (i.e., to mimic an undervoltage attack) or an overvoltage (i.e., to mimic an overvoltage attack).

B. Normal operation (no attack) scenario

In this case, the normal operation of the network is presented, which shows in Figure 7 shows the profile of the voltage at nodes (a, b & c) over 24 hours with the peak consumption occurring in the interval from 7 am to 7 pm. It can be seen that it follows the same behavior of the PV profile in Figure 6.

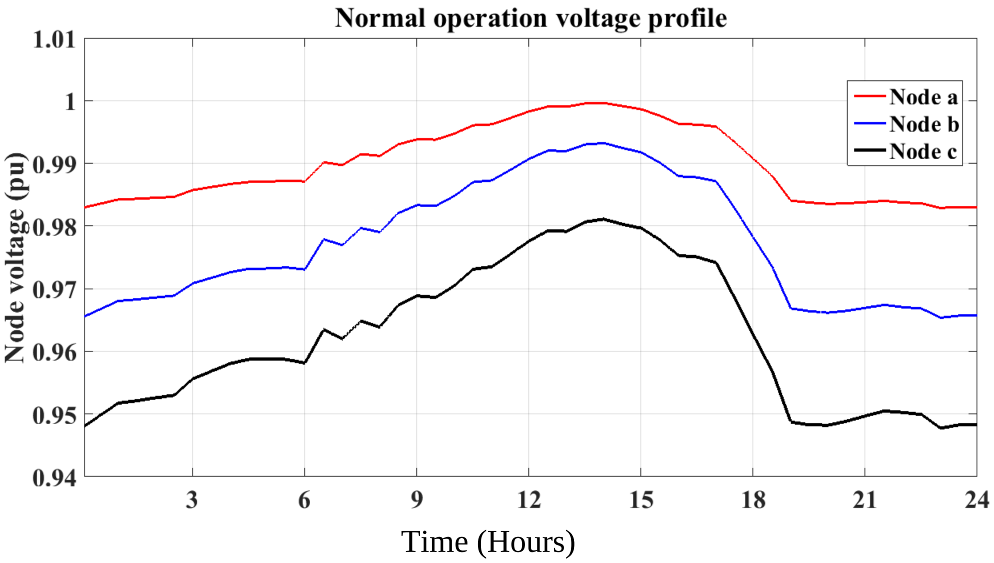


Figure 7. Voltage profile at nodes a, b and c at normal operation.

Figure 7 shows that the node voltages in Figure 4 are within the $0.95 - 1$ PU in the network's normal operation and almost follow the shape of the PV load curve due to the power injection from the PV. The figure also shows that the nodes' voltages decrease as the measurement point moves closer to the load. Nevertheless, this profile may change under many factors, including issues related to the PV itself caused by the weather and the load demands changing during the day. On the other hand, having a more complex network makes the behavior of the voltage profile unpredictable and increases the need for controllers and communication networks in the system to coordinate between the transformer side and the distribution side. This raises the possibility of having attacks and complicates the process of detecting attacks at the same time.

C. Overvoltage attacks

Figure 8 mimics the attacker's role that falsifies the data by changing the measurement of the node voltage to 95% of the actual reading. This falsified data is transmitted to the OLTC of the transformer. Therefore the OLTC will act incorrectly to step up the voltage of the network. A delay may be incurred in a real network between the action, its reception at the OLTC, and the response reaction. However, in this work, we ignore such delays to focus on the power system operation itself. Figure 8 shows the response of the network nodes voltages due to having false data injection at one node. This false data causes an overvoltage, causing damage to the appliances, especially at the heavy loading times.

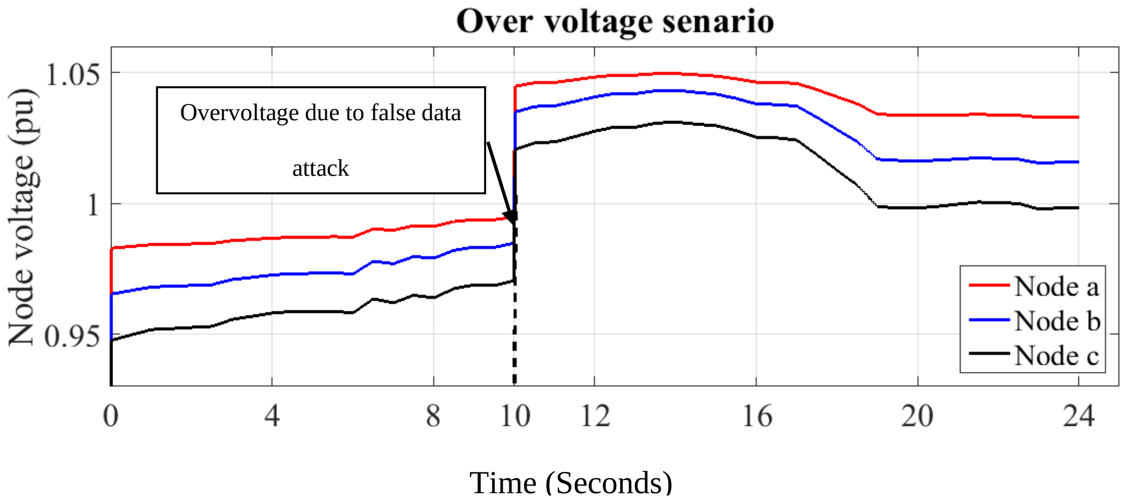


Figure 8. Voltage profiles of nodes a, b, and c with voltage stepping up to 1.05pu due to falsified data injection (i.e., changing the measurement of the node voltage to 95% of the actual reading) at t = 10 seconds.

D. Undervoltage attacks

In this attack, the attacker falsifies the data by changing the measurement of the node voltage to 105% of the actual reading. This falsified data is transmitted to the OLTC of the transformer. Therefore the OLTC will act incorrectly to step down the voltage of the network. This will lead to under-voltage at the nodes, which appears in Figure 9. This undervoltage may harm the network at the light loading time.

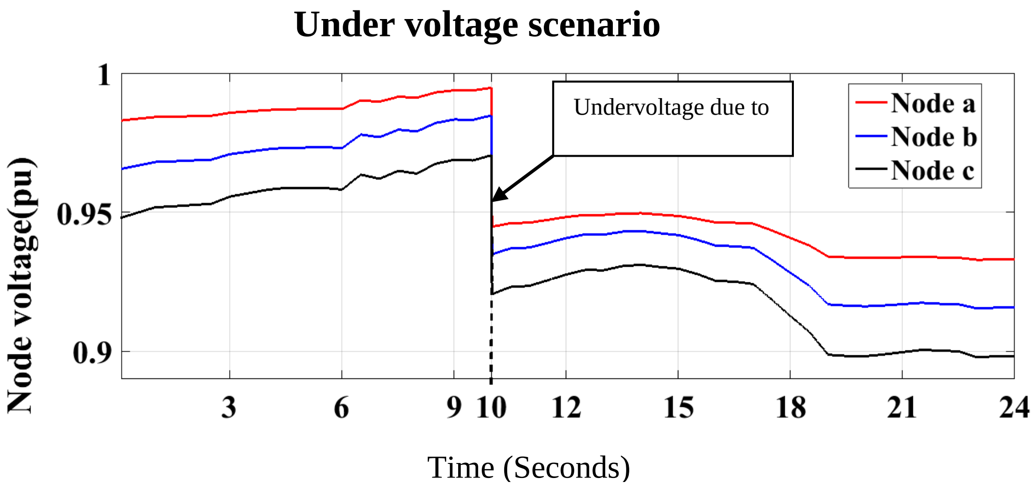


Figure 9. Voltage profiles of nodes a, b, and c with voltage stepping down to 1.05pu due to falsified data injection (i.e., changing the measurement of the node voltage to 105% of the actual reading) at t = 10 seconds.

Simulating the different cases of attacks shows the network operation and response to the attacks. Furthermore, this clarifies the network's behavior under-voltage level changes, which may cause overvoltage or undervoltage in the distribution network.

CHAPTER 4: DETECTION AND PROTECTION AGAINST CYBER-ATTACK INDUCED VOLTAGE VIOLATIONS

This chapter introduces our proposed approaches for detection and protection against cyber-attacks induced voltage violations. The proposed attack detection and protection algorithms are presented in light of the considered system attack scenarios introduced in Chapter 3.

4.1 Extending the System Model

We start by introducing an extended detailed general system model of a one feeder distribution network with different connected loads and PVs. The network shown in Figure 10 consists of n nodes with $n-1$ loads and $n-1$ PVs. We further provide a mathematical analysis of the considered system network.

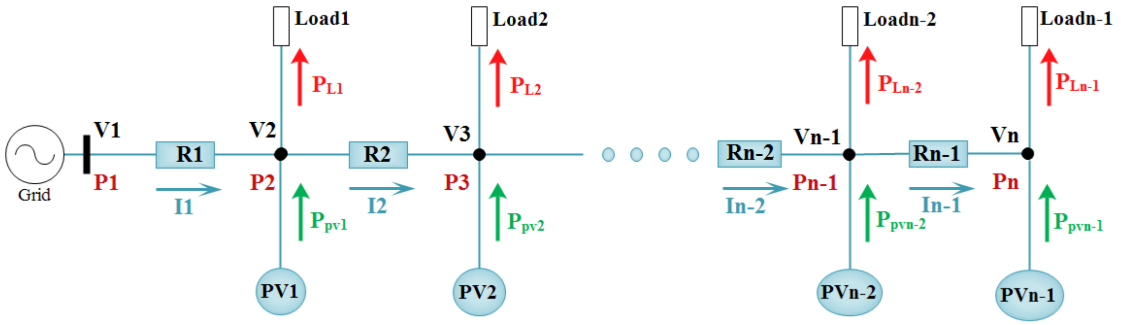


Figure 10. A general single feeder distribution network.[71]

Consider the distribution network model in Figure 10. Voltage regulation is essential to ensure the power quality measured by the feeder's voltage levels, which should always stay within the allowable range. When there is no power injection from PV generators at any node in the feeder which means $P_{pvi} \ = 0\ , for\ i = 1 \dots n - 1$, the voltage profile for the feeder is a decreasing function of distance from the grid. This network's analysis can be carried out using the voltage and the current measurements, the topology information, and past load data. In this case, the introduction of falsified readings at any single point is easily detectable through comparing it with the list of voltage readings on the same feeder. Nevertheless, when PVs are connected, a voltage rise may occur in any node through the feeder. This changes the profile characteristics of the feeder. Starting with the last two nodes n & $n - 1$, the equations which express the voltage drop and feeder currents can be written as follows

$$P_n = P_{pv(n-1)} - P_{l(n-1)} \tag{10}$$

$$\Delta V_{n-1} = Z_{n-1}\ I_{n-1} \tag{11}$$

$$V_{n-1} = V_n + \Delta V_{n-1} \tag{12}$$

$$I_{n-1} = \frac{P_n}{V_n} + I_n, \tag{13}$$

where P_n is the power at node n, ΔV_{n-1} is the voltage difference between node n and node $n-1$, I_{n-1} is the current flowing from node $n-1$ to node n, and $Z_{n-1} = R_{n-1} + jX_{n-1} \approx R_{n-1}$ is the impedance of the line that links node $n-1$ with node n, assuming a high R/X ratio in the LV distribution lines and unity power factor. Applying these equations on each node from node 1 to node n results in a set of simultaneous equations that can be expressed in a matrix form as follows

$$\begin{bmatrix} P_n \\ \vdots \\ P_2 \end{bmatrix}_{(n-1)\times 1} = \begin{bmatrix} P_{pv(n-1)} \\ \vdots \\ P_{pv1} \end{bmatrix}_{(n-1)\times 1} - \begin{bmatrix} P_{l(n-1)} \\ \vdots \\ P_{l1} \end{bmatrix}_{(n-1)\times 1} \tag{14}$$

$$\begin{bmatrix} V_{n-1} \\ \vdots \\ V_1 \end{bmatrix}_{(n-1)\times 1} = \begin{bmatrix} V_n \\ \vdots \\ V_2 \end{bmatrix}_{(n-1)\times 1} + \begin{bmatrix} \Delta V_{n-1} \\ \vdots \\ \Delta V_1 \end{bmatrix}_{(n-1)\times 1} \tag{15}$$

$$\begin{bmatrix} I_{n-1} \\ \vdots \\ I_1 \end{bmatrix}_{(n-1)\times 1} = \begin{bmatrix} \frac{P_n}{V_n} \\ \vdots \\ \frac{P_2}{V_2} \end{bmatrix}_{(n-1)\times 1} + \begin{bmatrix} I_n \\ \vdots \\ I_2 \end{bmatrix}_{(n-1)\times 1} \tag{16}$$

$$\begin{bmatrix} \Delta V_{n-1} \\ \vdots \\ \Delta V_1 \end{bmatrix}_{(n-1)\times 1} = \begin{bmatrix} R_{n-1} & 0 & \cdots & 0 & 0 \\ 0 & R_{n-2} & 0 & \ldots & 0 \\ \vdots & 0 & \ddots & 0 & \vdots \\ 0 & \ldots & 0 & R_2 & 0 \\ 0 & 0 & \cdots & 0 & R_1 \end{bmatrix}_{(n\_1)\times(n-1)} \begin{bmatrix} I_{n-1} \\ \vdots \\ I_1 \end{bmatrix}_{(n-1)\times 1} . \tag{17}$$

These represent the general system equations employed for the analysis of the distribution network. These equations represent a single-phase of the depicted three-phase distribution system.

4.2 Overall Proposed Framework

Our proposed approach for voltage violation attack detection and mitigation at the power-grid layer utilizes the above-discussed network analysis to learn key characteristics and voltage behavioral aspects of the underlying network configuration. Accordingly, it utilizes the learned characteristics and behavior to strategically apply a perturbation approach to detect and mitigate the voltage violation attack scenarios discussed previously in Chapter 3.

The proposed framework has three phases of action, which can be summarized as follows:

Phase 1: Off-line network analysis

In this phase, the network operator utilizes the known network parameters (such as loads and ratings of installed PVs) to perform a detailed network analysis using the model discussed in Section 4.2 to provide governing equations that represent the relations between voltages and currents across the different feeders connected to the OLTC.

Phase 2: Off-line critical PV identification

In this phase, the network operator uses simulation tools along with the governing equations defined in Phase 1 to detect the location along the feeder that has the PV with the most critical effect on voltages (critical PV).

Phase 3: Online active perturbation

In this phase, the OLTC performs voltage perturbations at the critical PV and based on these perturbations' measured responses. It can detect and mitigate voltage violation attacks.

In the following sections, we will have a detailed analysis and discussion about these phases and how they are carried out in our sample single feeder network.

4.3 Off-line Network Analysis

The single feeder network shown in Figure 11 can be analyzed using the general form equations presented in (14)-(17). The network consists of 3 loads; Load 1&2 with a connected load of $50\ kW$ and Load 3 with $25\ kW$ power absorption. The network includes

3 PV power generators, each with 45 kW generated power and a $500 - meter$ low voltage cable of $185\,mm^2$ with impedance of $(0.082 + j1.1777e - 4)\,\Omega/km$. Power flow analysis can be conducted analytically or using one of the available software such as MATLAB/SIMULINK or ETAP.

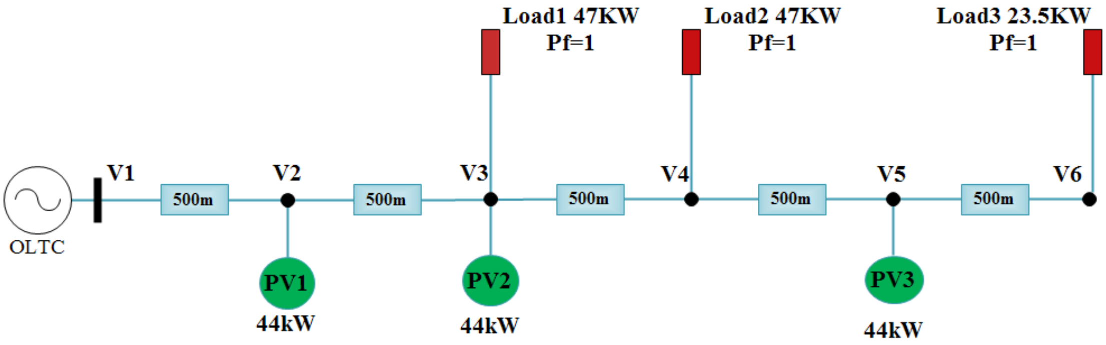


Figure 11. A single line diagram for a radial feeder distribution network.

The extended network is shown in Figure 12 With currents and voltages labeled in detail. The power at each node can be calculated using known load consumption parameters and PV power generators at each node. Where $P2 = P_{pv1} = 45kW,$ $P3 = P_{pv2} - P_{L1} = 45 - 50 = -5kW,$ $P4 = P_{L2} = -50kW,$ $P5 = P_{pv3} = 45kW$ and $P6 = P_{L3} = -25kW.$

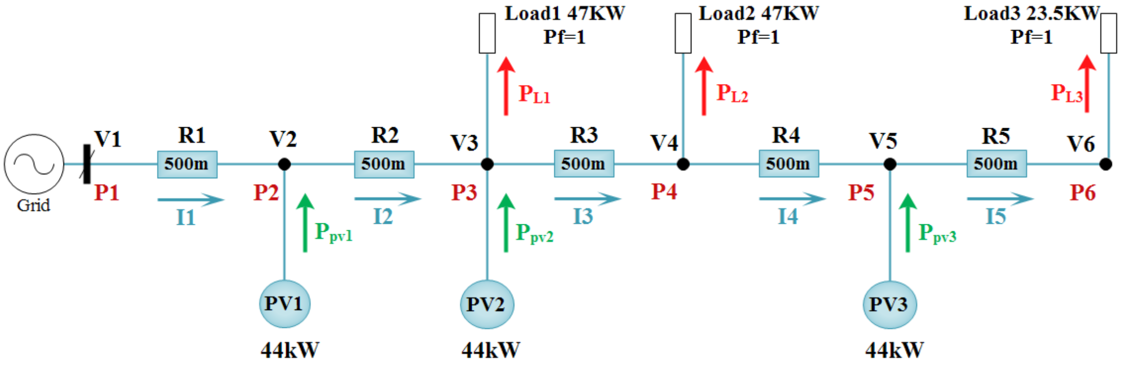


Figure 12. A single line diagram of the extended single feeder distribution network.

The distribution line has an impedance of $0.082 + \mathrm{j}1.1777\mathrm{e} - 4\ \Omega/\mathrm{km}$, but X is neglected as the ratio R/X is high, resulting in a resistive impedance with $0.082\ \Omega/\mathrm{km}$. Therefore, the impedance for the length of 500m in the network distribution lines equals 0.041Ω. Then substituting the parameters in the general form of the system equations presented in (15)-(17), resulting in the following:

The relation between the voltages of the nodes is

$$\begin{bmatrix} V_5 \\ V_4 \\ V_3 \\ V_2 \\ V_1 \end{bmatrix} = \begin{bmatrix} V_6 \\ V_5 \\ V_4 \\ V_3 \\ V_2 \end{bmatrix} + \begin{bmatrix} \Delta V_5 \\ \Delta V_4 \\ \Delta V_3 \\ \Delta V_2 \\ \Delta V_1 \end{bmatrix}. \tag{18}$$

The currents in the distribution line flowing through the different nodes are

$$\begin{bmatrix} I_5 \\ I_4 \\ I_3 \\ I_2 \\ I_1 \end{bmatrix} = \begin{bmatrix} \frac{P_6}{V_6} \\ \frac{P_5}{V_5} \\ \frac{P_4}{V_4} \\ \frac{P_3}{V_3} \\ \frac{P_2}{V_2} \end{bmatrix} + \begin{bmatrix} I_6 \\ I_5 \\ I_4 \\ I_3 \\ I_2 \end{bmatrix} = \begin{bmatrix} \frac{-25k}{V_6} \\ \frac{45k}{V_5} \\ \frac{-50k}{V_4} \\ \frac{-3k}{V_3} \\ \frac{45k}{V_2} \end{bmatrix} + \begin{bmatrix} I_6 \\ I_5 \\ I_4 \\ I_3 \\ I_2 \end{bmatrix}, \tag{19}$$

and finally, the voltage differences between any two nodes can be written as

$$\begin{bmatrix} \Delta V_5 \\ \Delta V_4 \\ \Delta V_3 \\ \Delta V_2 \\ \Delta V_1 \end{bmatrix} = \begin{bmatrix} R_5 & 0 & 0 & 0 & 0 \\ 0 & R_4 & 0 & 0 & 0 \\ 0 & 0 & R_3 & 0 & 0 \\ 0 & 0 & 0 & R_2 & 0 \\ 0 & 0 & 0 & 0 & R_1 \end{bmatrix} \begin{bmatrix} I_5 \\ I_4 \\ I_3 \\ I_2 \\ I_1 \end{bmatrix} \tag{20}$$

$$\begin{bmatrix} \Delta V_5 \\ \Delta V_4 \\ \Delta V_3 \\ \Delta V_2 \\ \Delta V_1 \end{bmatrix} = \begin{bmatrix} 0.041\Omega & 0 & 0 & 0 & 0 \\ 0 & 0.041\Omega & 0 & 0 & 0 \\ 0 & 0 & 0.041\Omega & 0 & 0 \\ 0 & 0 & 0 & 0.041\Omega & 0 \\ 0 & 0 & 0 & 0 & 0.041\Omega \end{bmatrix} \begin{bmatrix} I_5 \\ I_4 \\ I_3 \\ I_2 \\ I_1 \end{bmatrix}. \tag{21}$$

These single-phase equations can be solved using MATLAB. This analysis shows the proper work at the network and ensures the voltage level of the nodes within the allowable range in normal operation under no attack. This will help to study the network with a clear vision and reasonable results as if this network presents a real distribution network.

4.4 Off-line Critical PV Identification

To carry this task, sensitivity and behavioral analysis are carried using the model built in Phase 1. The network is modeled to present a distribution network highly penetrated with PV generators. The network illustrated in Figure 11. consists of different loads spread along a single feeder distribution network, provided with three PV power generators. An average load curve for realistic distribution areas in France [23] was used as the load. The nodes may be classified according to their voltage sensitivity to power variations. The PV that has the most significant effect on the voltage profile across the radial feeder distribution network is the one with the highest power rating and/or at the farthest end of the distribution transformer. Identifying this PV helps in the next section that addresses the proposed detection algorithm. In Figure 12 It is clear that PV3 will have the highest effect on the feeder nodes. In order to prove this systematically, the sensitivity of the nodes is studied using the following procedures. The procedures start with increasing each PV generator power level gradually from 10% to 90% from their rated power, then recording the nodes' voltage levels on the network to check their effects on the nodes. The resulting data is used to draw the relation of each PV power level and the node voltages. Figure 13 represents the graph that shows the response of node 2 voltage due to a change in the power of PV1, PV2, and PV3. The x-axis shows the percentage of the increase in each PV's power, while the y-axis shows the voltage level in Pu. As apparent in the graph, the PV’s power increase has a profound effect on node 2.

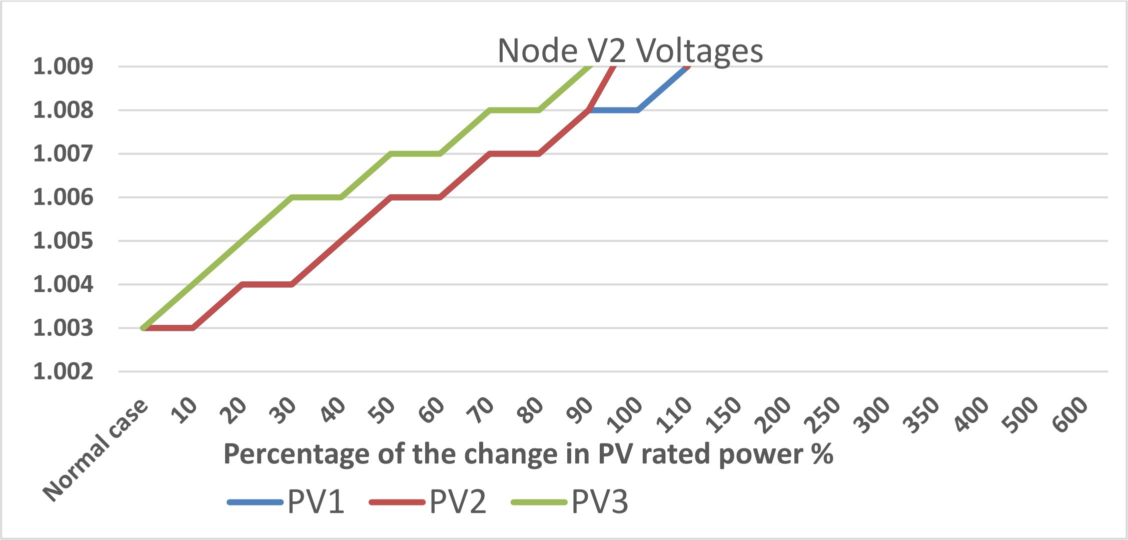


Figure 13. Per unit voltage response at node 2 with percentage changing in the PVs rated power (PV1 line is the same as PV2 line).

The graph in Figure 14 for node 3 shows the response of node 3 voltage to changes in the power of PV1, PV2, and PV3. The x-axis shows the percentage of the increase in each PV's power, while the y-axis shows the voltage level in Pu. The graph shows that the effect of the PV1, PV2, and PV3 power changes on the voltage is almost the same, and these changes are less likely to cause dangerous overvoltage.

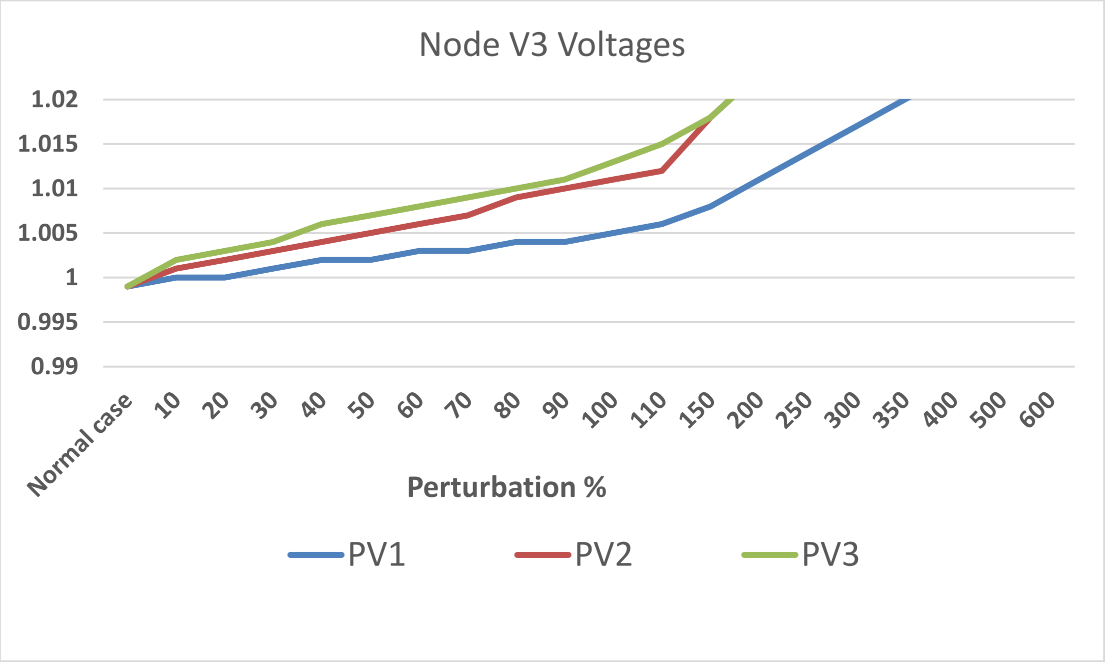


Figure 14. Per unit voltage response at node 3 with PVs perturbations.

The graph in Figure 15 shows the response of node 4 voltage due to the change in the power of PV1, PV2, and PV3. The x-axis shows the percentage of the increase in the power of each PV, where the y-axis shows the voltage level in Pu. The readings of the voltage at node 4 while increasing the PV's power show that PV3 has a higher effect on the voltage rise.

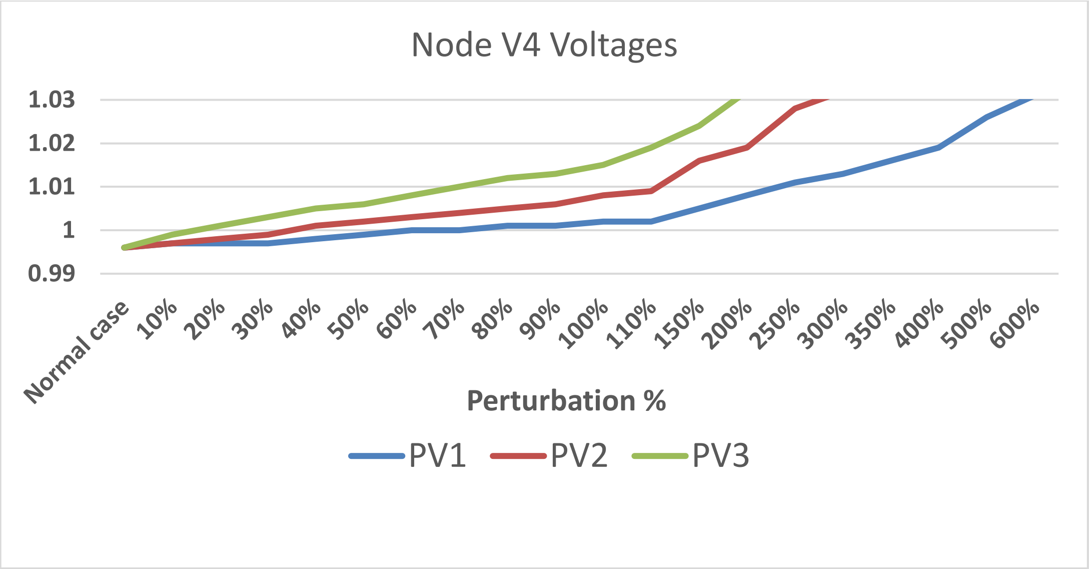


Figure 15. Per unit voltage response at node 4 with PVs perturbations.

For node 5, Figure 16 represents the graph that shows the response of node 5 voltage due to changes in the power of PV1, PV2, and PV3. The x-axis shows the percentage of the increase in each PV's power, while the y-axis shows the voltage level in Pu. It is evident from the graph that PV3 affects the voltage faster and with a larger amount, which means that PV3 power and node 5 voltage have a high dependency.

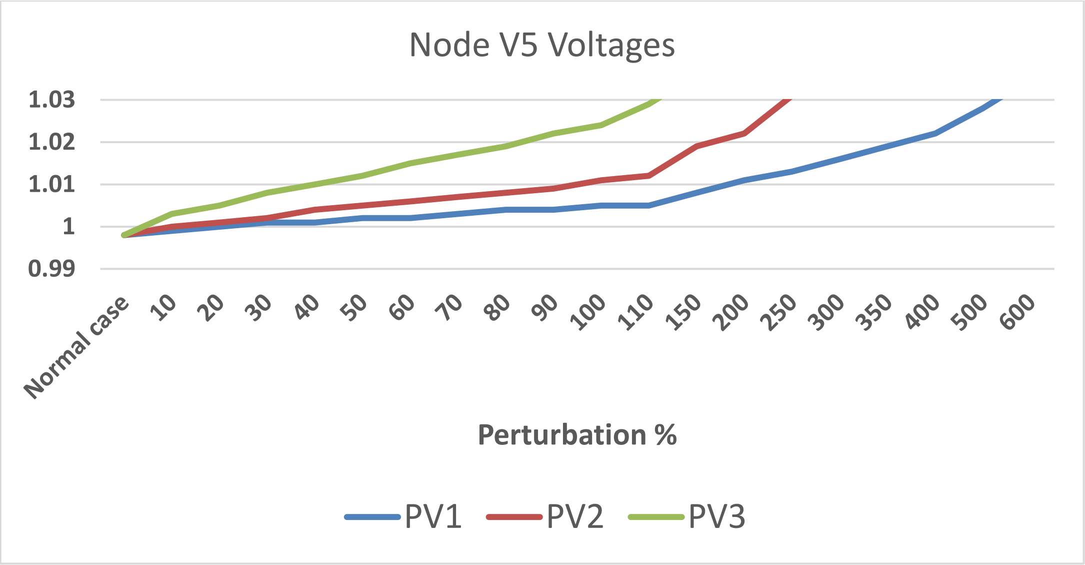


Figure 16. Per Unit voltage response at node 5 with PVs perturbations.

Figure 17 represents the graph that shows the response of node 6 voltage due to a change in the power of PV1, PV2, and PV3. The x-axis shows the percentage of the increase in each PV's power, while the y-axis shows the voltage level in Pu. As evident from the graph, there is a high dependency between V6 and PV3 power.

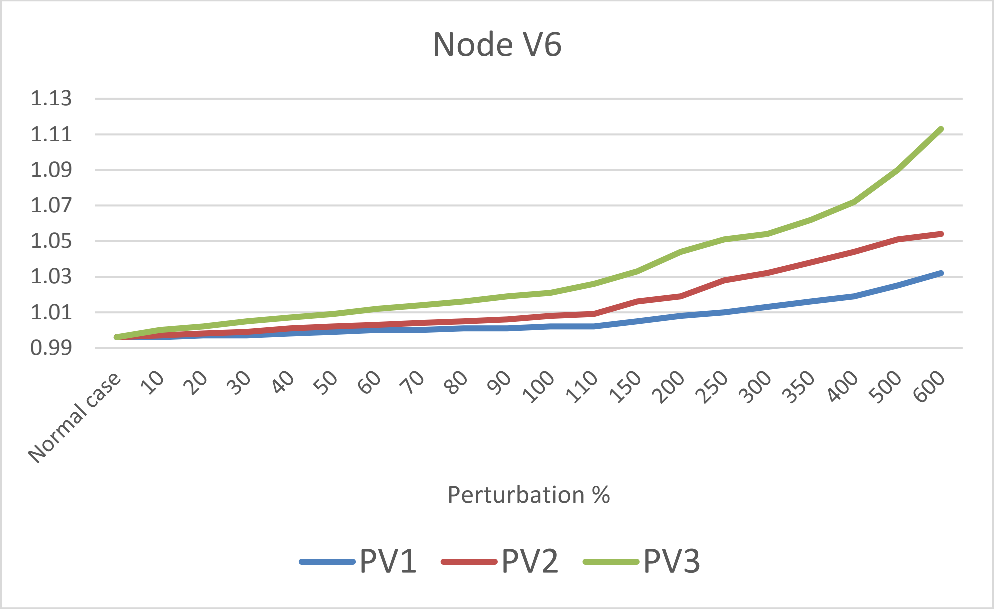


Figure 17. Per unit voltage response at node 6 with PVs perturbations.

After comparing all node responses to the three PV perturbations, it is clear that PV3 power has the highest effect on the voltage profile compared to other PVs.

Therefore, PV perturbation at this node (marked as the highest sensitive node) may be used to ensure the detection and protection against cyber-attacks. Accordingly, the OLTC will have to introduce the correct action even with received falsified data.

4.5 Online Active Perturbation (Attack Detection Algorithms)

A cyber-attack on the power network may target any of the network nodes. False data injection attacks are achieved by injecting false values to the OLTC received voltage and current measurements of the nodes. Accordingly, the OLTC responds incorrectly to compensate for the network's voltage causing undesired voltage violations over the network.

4.5.1 General proposed algorithms

Two detection algorithm approaches are proposed to detect and mitigate the false data injection in the distribution network.

1) The first algorithm, named as (Act then Check). This algorithm starts whenever there is a variation in the voltage readings at any node. Then the OLTC responds to compensate for this variation. A PV perturbation is then introduced; this perturbation can be increasing or decreasing in the PV power according to the network loading and PV power generating. The value of such perturbation (ΔP) is considered 10% of the PV rated power to provide a sufficient response in the network voltage level. If all nodes responded to the perturbation similarly, then there is no attack. On the other hand, if one or more nodes have a different response, they are under attack. In this case, the OLTC returns to its voltage level.

2) The second algorithm, named as (Check then Act). This approach starts with checking the validity of any variation in any node's voltage by making a PV perturbation first. This PV perturbation checks the response of all nodes in the network. If all nodes have the same response, then there is no attack, and the OLTC needs to act and compensate for the variation in the voltage level, but if one or more nodes responded differently than

these nodes considered to be under attack and no need for any action from the OLTC. Except for nodeX that has the attack, this indicates an attack on the network, particularly on nodeX, then no need to step up the voltage. This step saves the network from unnecessary changes in the voltage. This algorithm can also discover if this is a real undervoltage problem at nodeX, that if the response of the nodeX to the perturbation was the same as the others, then OLTC needs to introduce an increase in the voltage. This type ensures the proper operation of all nodes to detect the attacker before any increase in the voltage, and thus avoid the unnecessary overvoltage problem that may harm the critical and sensitive devices. The next two sections show the validation of the discussed algorithms on detecting over voltage and under voltage attacks.

4.5.2 Detection of overvoltage attacks

In the overvoltage attack, false data injected into the network by the attacker (i.e., alters the real readings by reducing its value at nodeX). If the new reading for nodeX is not within the allowable voltage range, there are two proposed algorithms to follow.

(i) Act then Check algorithm illustrated in the flowchart shown in Figure 18. The OLTC starts to respond to the low voltage reading at nodeX and increases the voltage by 0.05 PU. Accordingly, the voltage increases on the entire network nodes. Then the PV power is perturbed by ΔP, the network response to this perturbation is monitored and shows that nodeX has a different response to the perturbation; this leads that nodeX is under attack. In this case, the OLTC reduces the voltage back. This type of algorithm took the action of changing the voltage before checking to ensure proper work of the network, which may cause an overvoltage if there is an attack.

(ii) Check then Act algorithm illustrated in the flowchart shown in Figure 19. It starts with introducing a perturbation in the PV power to check all nodes' response to this perturbation. All nodes will have a voltage increase except node X. This indicates there is an attack on the network, particularly on nodeX, then no need for stepping up the voltage at the OLTC. This step saves the network from unnecessary changes in the voltage. This type ensures all nodes' proper operation to detect the attacker before any increase in the voltage, thus avoiding the unnecessary overvoltage problem that may harm the critical and sensitive devices.

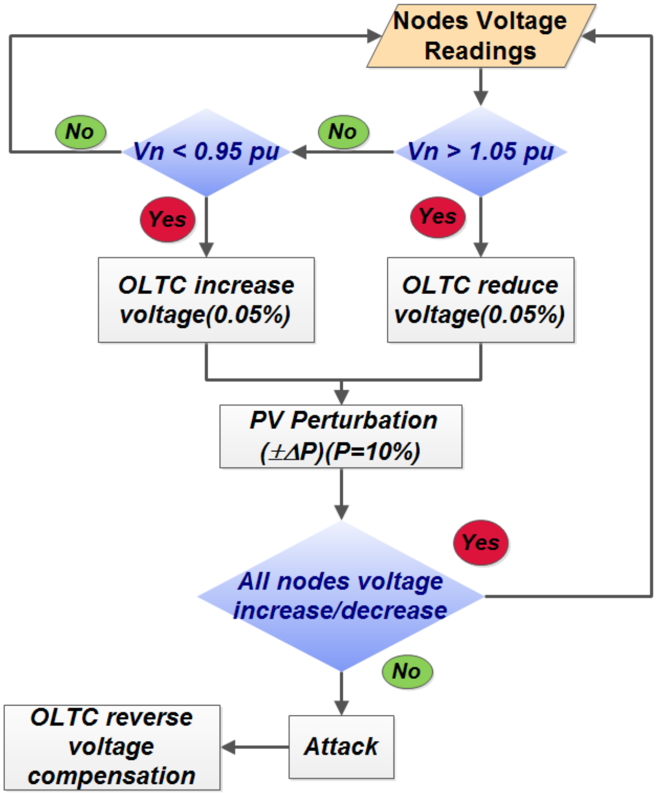

Nodes Voltage Readings
No
Vn < 0.95 pu
No
Vn > 1.05 pu
Yes
Yes
OLTC increase voltage(0.05%)
OLTC reduce voltage(0.05%)
PV Perturbation (±ΔP)(P=10%)
Yes
All nodes voltage increase/decrease
No
OLTC reverse voltage compensation
Attack

Figure 18. Perturbation and detection algorithm I (Act then Check).

4.5.3 Detection of undervoltage attacks

For the case of an undervoltage attack, the attacker may send false data at one node, nodeX, which lies above the allowable voltage range. In this case, the two proposed algorithms can be followed;

(i) With the Act then Check algorithm illustrated in the flowchart shown in Figure 18, the OLTC will respond to this high reading at nodeX and decreases the voltage. A PV perturbation checks the response of the entire network and finds out that nodeX has false data. Then the OLTC will increase the voltage back.

(ii) Check then Act algorithm illustrated in the flowchart shown in Figure 19, checks the validity of this data first by making an extra step, this step starts with making a perturbation in the PV power, and check the response of all nodes to this perturbation. In this case, we can make positive perturbation and check the nodes voltages; if all nodes are increased in their voltages that means there is no attack on the network, and the node with high reading may suffer from overvoltage, and the OLTC needs to decrease the voltage. Nevertheless, if all nodes have higher voltages except nodeX, that means that this nodeX is under attack, and there is no need to decrease the voltage in the network. This algorithm detects the existence of the attack before taking any action in the OLTC.

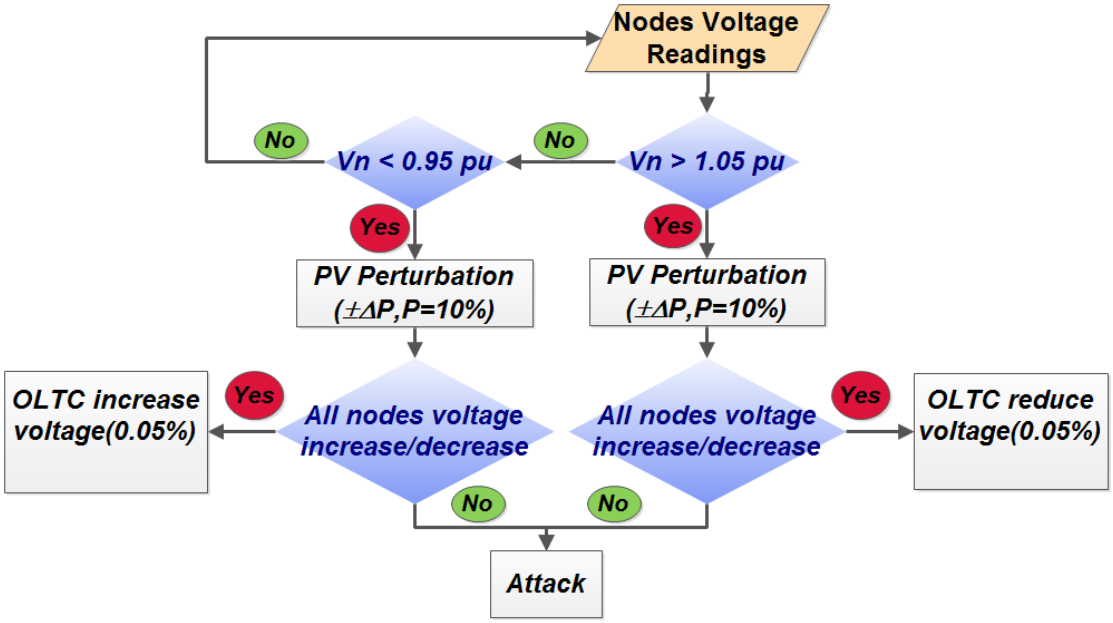

Nodes Voltage Readings
Vn < 0.95 pu
Vn > 1.05 pu
No
No
Yes
Yes
PV Perturbation (±ΔP,P=10%)
PV Perturbation (±ΔP,P=10%)
OLTC increase voltage(0.05%)
Yes
All nodes voltage increase/decrease
All nodes voltage increase/decrease
Yes
OLTC reduce voltage(0.05%)
No
No
Attack

Figure 19. Perturbation and detection algorithm II (Check then Act).

4.6 Algorithms Discussion

Applying the Act then Check algorithm on the network, the OLTC starts to increase or decrease voltage according to the data received from the attacked node. There may be a risk of having overvoltage or undervoltage issues in the network. However, by applying the Check then Act algorithm, this risk can be avoided by the additional step of checking the status of the nodes, by applying a known perturbation and explore the result to decide the correct action. Nevertheless, having more steps to do before taking action adds the risk of having overvoltage in on node for a longer time, causing damages to that node’s appliances.

4.7 Case Studies and Results

In this section, the network studied and analyzed, under different scenarios of undervoltage and overvoltage levels, to present the effect of cyber-attacks on such distribution networks, with high penetration of PVs. At the same time, the proposed two algorithms were performed to detect these attacks. We introduced two types of algorithms: (i) Act then Check and (ii) Check then Act, but the decision of which one to follow depends on different factors, including network appliances type, the media of the network, and the type of the attack itself.

Referring to the previously detailed algorithms in Figure 18 and Figure 19, we applied the two types on the extended network in Figure 11, on the simulation, in different scenarios of attacks illustrated in Flowchart below, then studied the validity of this algorithm. In each case, one node has a voltage level, which is not in the allowable range, and according to this reading, we apply the two types of algorithms and then discuss the preferred type for each case. We investigate the following case studies:

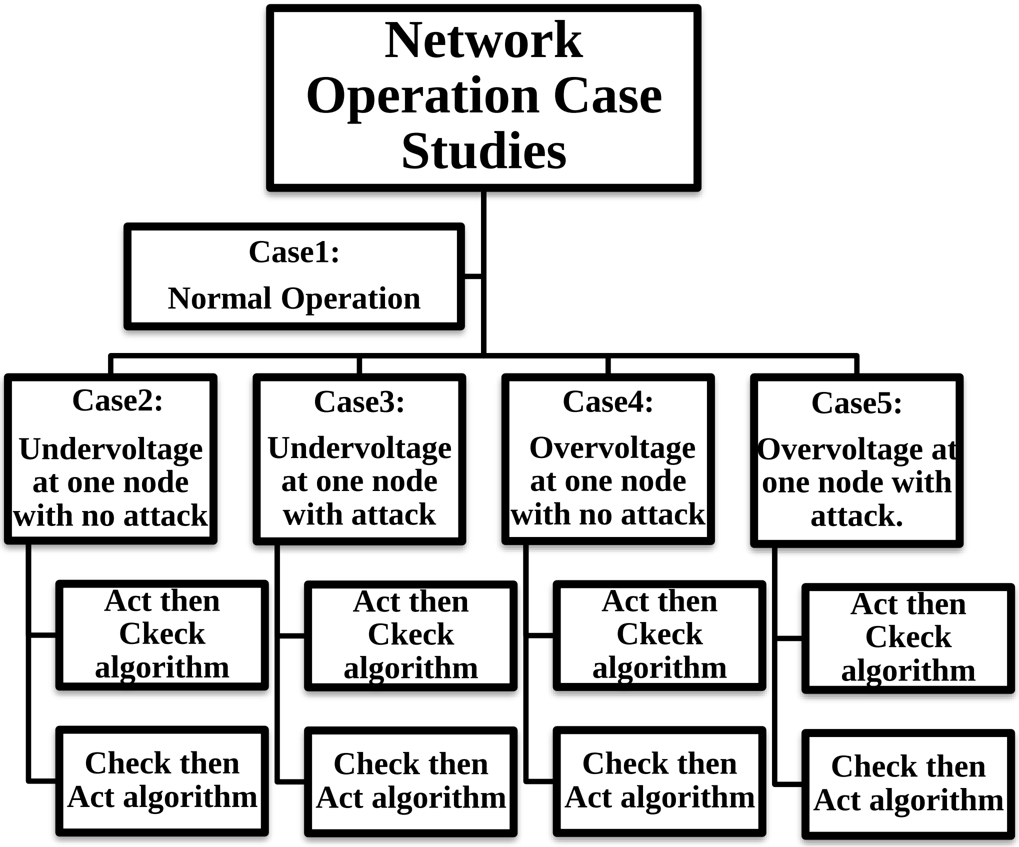
A. *Normal Operation.*

B. *Undervoltage at one node with no attack.*

C. *Undervoltage at one node with attack.*

D. *Overvoltage at one node with no attack.*

E. *Overvoltage at one node with attack.*



A. Case1: Normal Operation

At normal operation, all nodes have voltage within the allowable range. Figure 20 presents the typical voltage profile for each node during the day with the PV generators' existence.

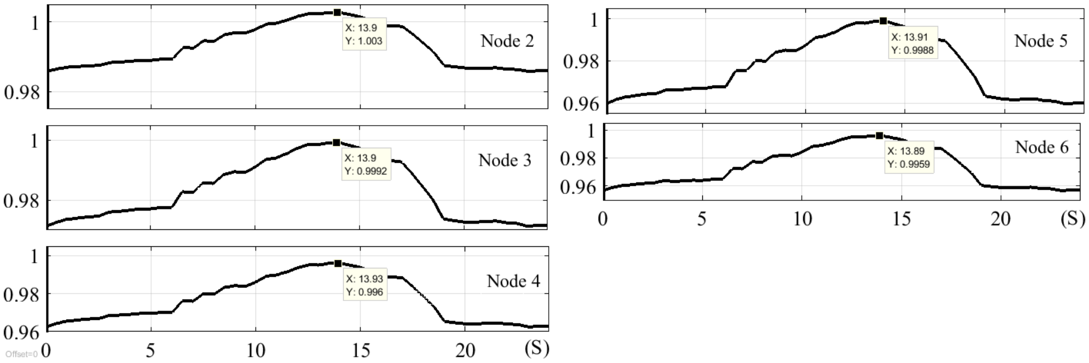


Figure 20. Per unit voltages of the nodes in the normal operation of the network.

The voltage level for the nodes lies within the allowable range (0.95pu to 1.05pu) according to the standards of ±5% allowable variation [72].

The nodes from 2 to 6 are arranged from nearest to farthest from the source. It is expected to have a decrease in the voltage levels going farther from the source. Nevertheless, having PV generators injecting power causes unexpected voltage levels. This is evident in Figure 20.

*B. Case2**:** Undervoltage without attack*

1. Act then check Algorithm

We study the case when node6 has and actual undervoltage. First, all nodes' voltages data measurements are sent to the OLTC from IT switches at each node when such undervoltage is sensed. The OLTC takes action to compensate for the voltage at node6.

Then PV3 has a perturbation in the injected power to check the nodes' response to ensure that all nodes respond correctly and no node is under attack.

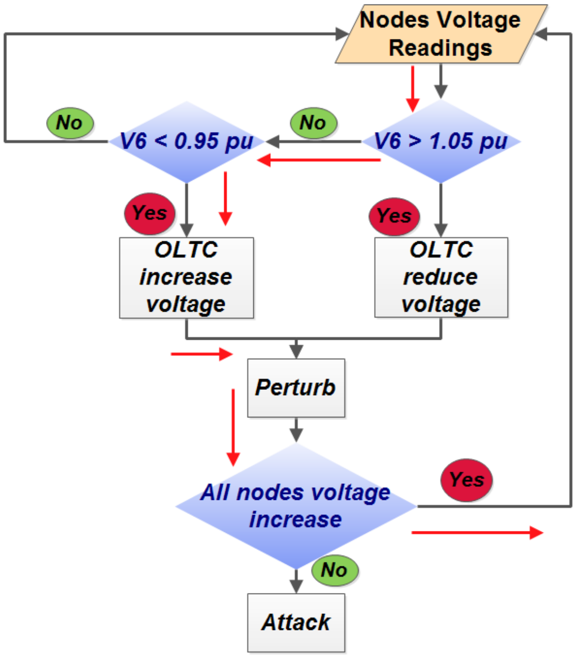


Figure 21. Case2 using perturbation and detection algorithm I (Act then Check).

We consider the algorithm in the flowchart in Figure 21, and follow the red arrows illustrated, and apply it in the simulation network. First, the OLTC senses the undervoltage at node6 and takes the action of increasing the voltage level; then, the PV3 makes a perturbation to check the validity of the node’s measurements.

The graphs in Figure *22* show the nodes' output voltage level at the time of 2 seconds. The undervoltage occurred at node6, from 0.96 per unit to 0.91per unit. Comparing the measurements received from the IT switches at the nodes, the OLTC steps up the voltage by 0.05per unit step to become 1.05 per unit, to make up the undervoltage at node6. Then PV3 increases the injected power to the network at time 2.5s for a short time to check the response of node6, which has the undervoltage. Accordingly, the voltage level at all nodes increases.

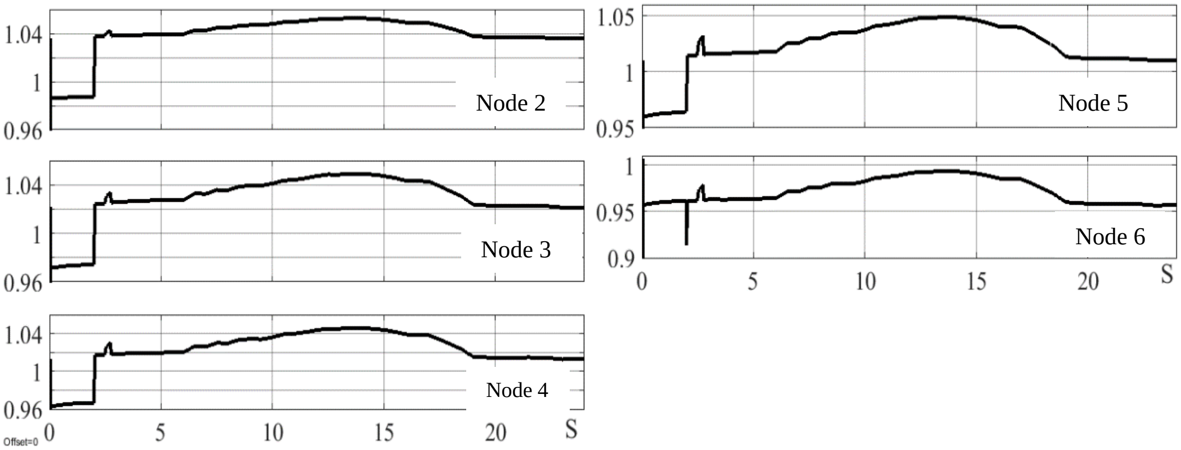


Figure 22. Per unit voltages of the nodes in case2 of undervoltage case without attack - Act then Check algorithm I.

The problem of undervoltage at node6 is solved. Nonetheless, voltages at the other nodes increase due to the step-up introduced by the OLTC. However, all nodes' response, due to the perturb in the power of PV3, shows that all nodes have real readings without any attack, which means all nodes are in normal operation.

This shows how the algorithm can compensate for the voltage variation, but the problem is: sometimes, the step-up voltage by the transformer may cause a real overvoltage at the nodes. In this case, the Check then Act algorithm will perform better, which will check and detect the attack with the perturbation step before increasing the voltage.

2. *Check then Act Algorithm*

The same case of node6 is studied using the second type of the algorithm. First, each node's voltage data measurement is sent to the OLTC from IT switches at each node. When such undervoltage is sensed, PV3 makes a perturbation in the injected power to the network, checks the nodes' response, and ensures that all nodes respond correctly and no node is under attack. Then the OLTC takes action to compensate for the voltage at node6.

In the SIMULINK, our network was tested to have undervoltage at node6. We consider the algorithm II Check the Act, the flow chart in Figure 23, and follow the red arrows.

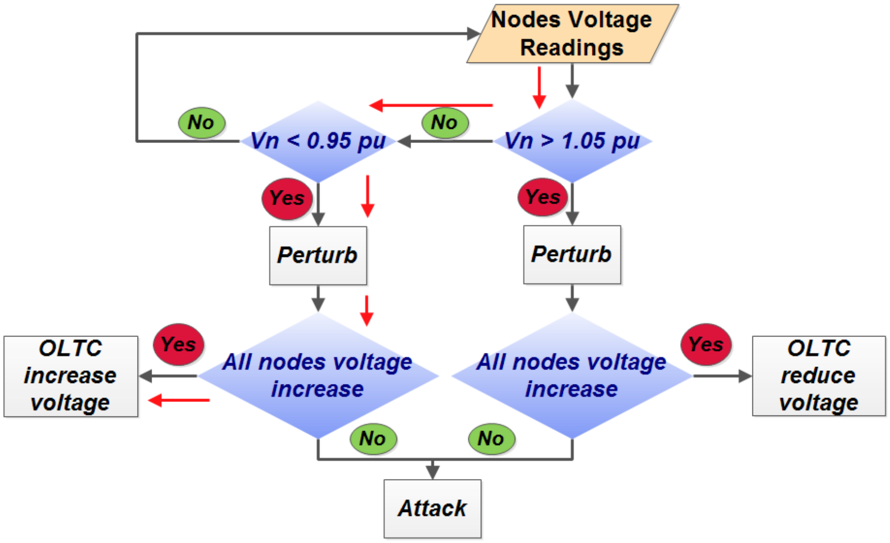


Figure 23. Case2 using perturbation and detection algorithm II (Check then Act).

First, the OLTC senses the undervoltage. The OLTC performs the checking by requesting PV3 to perturb the power injection and check the node’s measurements' validity. After that, the OLTC takes the action of increasing the voltage level to compensate for the voltage level at node6.

Graphs in Figure 24 show the voltage levels at the nodes at the time of 2 second. The undervoltage occurred at node6, from 0.96 per unit to 0.91per unit. Comparing the measurements coming from the IT switches at the nodes, PV3 makes a short perturb in the network by increasing the generated power to the network to check the response of node6, which has the undervoltage. All nodes responded to the perturb similarly by a small increase in their voltage, which indicates that all nodes are not under attack. At that time, the OLTC step up the voltage by 0.05per unit step, to become 1.05 per unit, to make up the undervoltage at node6. Accordingly, the voltage level at all nodes increases, and the undervoltage problem is solved.

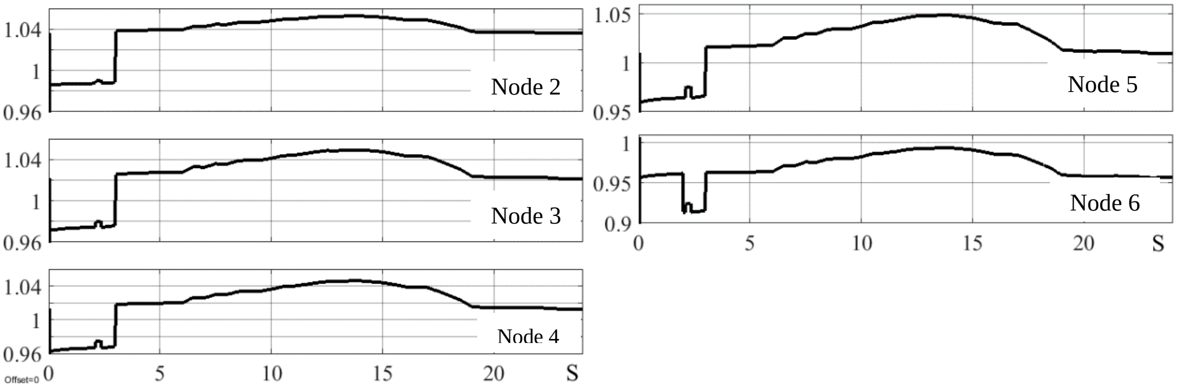


Figure 24. Per unit voltages of the nodes in case2 undervoltage case without attack -Check then Act algorithm II.

This algorithm has an extra step before taking the action of stepping up the voltage to compensate for the voltage. The step of perturbing the PV power gives a good indicator of all nodes' operation and illustrates if any node has false data. This enables detecting the case of having falsified readings attack on the node readings.

C. Case3: Undervoltage at one node with an attack

1. Act then Check Algorithm

Case three presents the scenario of having an attack on node6, and it shows how the attacker can fake the reading of node6 and affect the whole network at the same time. In this case, we apply the algorithm type I to detect the attacker. The algorithm shown in the flow chart in Figure 23 is followed in the simulation network.

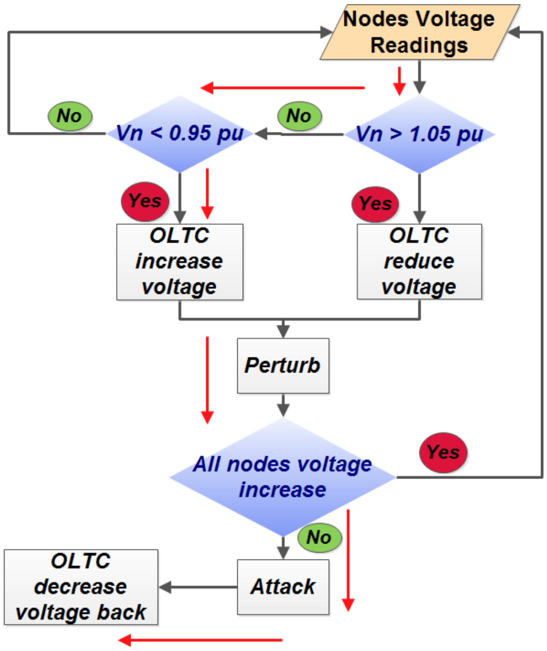


Figure 25. Case3 using perturbation and detection algorithm I (Act then Check).

Following the red arrows in the flowchart in Figure 23, the readings of the node's voltages are checked to find node6 voltage $V_6 < 0.95$. Then the OLTC steps up the voltage level in the network to adapt the voltage level at node6. After that, PV3 perturbs the power injected to check the nodes' response, according to this increment. If any node has a different response, that means it is under attack.

Figure 26 shows the result of the simulation network in the case of having an attack on node6. The attack occurred at second 2 on node6. The attacker altered the voltage reading of the node from 0.97 Per Unit to 0.91 Per Unit, which results in an under-voltage in node6. Then the OLTC at second 3 steps up the network's voltage level by 0.05 to compensate for the variation in the voltage at node6. As a result of this step up, all nodes have voltage levels increased except node6. After that, PV3 is perturbed, where power injected to the network is increased for a fixed time at second 3.5, to check the nodes' response. Similarly, all nodes react by having a small increase in their voltages except node6, with no response. This no response or false response of node6 reading indicates the existence of the attack.

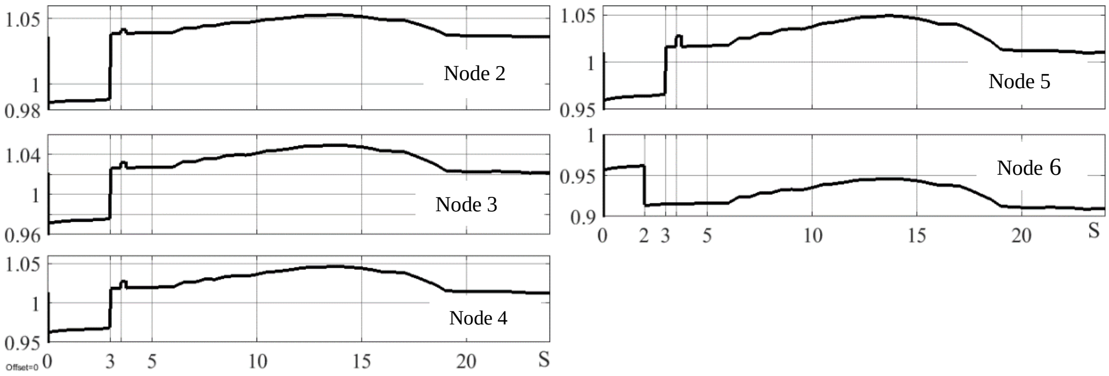


Figure 26. Per unit voltages of the nodes in case3 undervoltage case with an attack - Act then Check algorithm I.

2. *Check then Act Algorithm*

We apply the algorithm Check then Act in the same case of having undervoltage reading because of the attack. The algorithm starts with the check step by perturbing the PV3 power and monitoring the nodes' response, then takes the correct action. The flow chart in Figure 27 shows the algorithm followed. It first checks the nodes' voltage, then having V6 < 0.95 makes PV3 start the perturbation step and check the response of all nodes. However, node6 does not respond to power increment. This means the node6 is under attack, and no need to step up the voltage in the OLTC. In this case, the Check then Act algorithm performs better by detecting the attack and reducing one step.

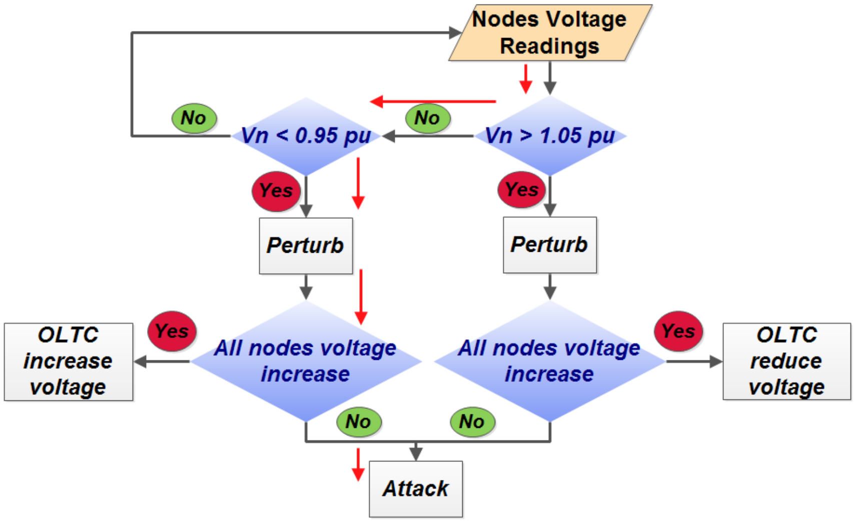


Figure 27. Case3 using perturbation and detection algorithm II (Check then Act).

Figure 28 shows the per-unit voltage for the 5 nodes, at time 2 seconds the attack occurs, then at time 2.5 seconds, the PV makes the perturbation for 1% of the 24 seconds, the nodes2,3,4 and 5 have increased in their voltages as expected, but node6 has no response, and this means that node6 is under attack.

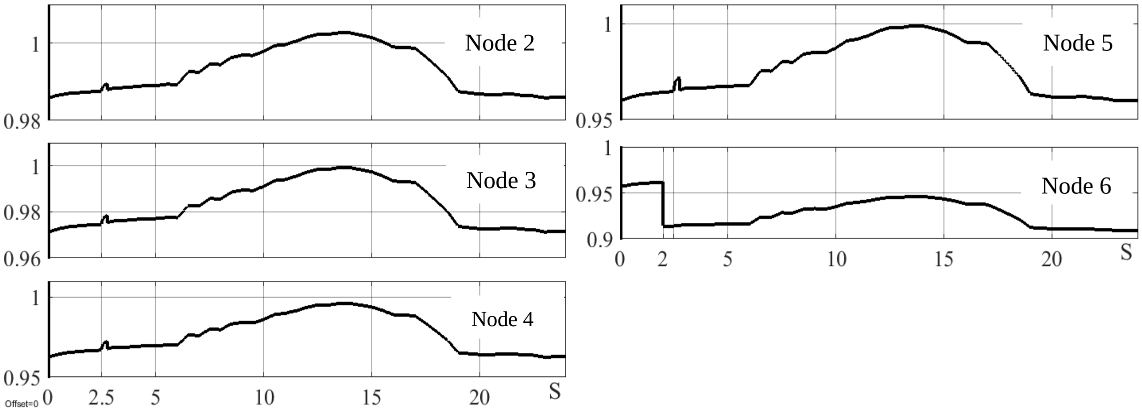


Figure 28. Per unit voltages of the nodes in case3 undervoltage case with attack-Check then Act algorithm II.

As evident in case3 of having an attack with an undervoltage, Check then Act algorithm performs better by reducing one unnecessary step, where the step of perturbation helps to detect the attacker.

The next cases explain these two algorithms in the overvoltage scenarios of having a real overvoltage problem or having a false data injection attack that causes overvoltage at the node.

D. Case4: Overvoltage at one node without attack

1. Act then Check Algorithm

The case of having overvoltage at node6 is performed in the network. Then the algorithm type I is tested. Red arrows in the flowchart in Figure 29 show the steps followed in this case. As the voltage at node6 is sensed to have a voltage higher than the allowable limit, the OLTC steps the voltage level down to avoid such high voltage and protect node6. After that, PV3 makes the perturbing step in the injected power to ensure the nodes' response. The voltage at node6 is increased due to this perturbation as the rest of the node voltages increased, then there is a real overvoltage at node6.

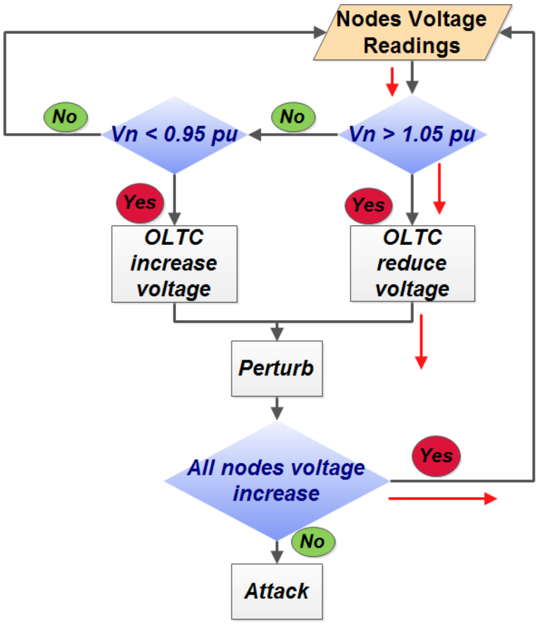


Figure 29. Case4 using perturbation and detection algorithm I (Act then Check).

The result of simulation for this case shown in *Figure 30*, normal operation in all nodes till second 13, where node6 suffered from increasing in the voltage, the OLTC act and step-down the voltage level, from compensating this increase at the same time, then PV3 make the check step by perturbing the power injection to the network, all nodes have a response including node6 which means that it has real overvoltage. Furthermore, the action of the OLTC saves node6 from the overvoltage immediately.

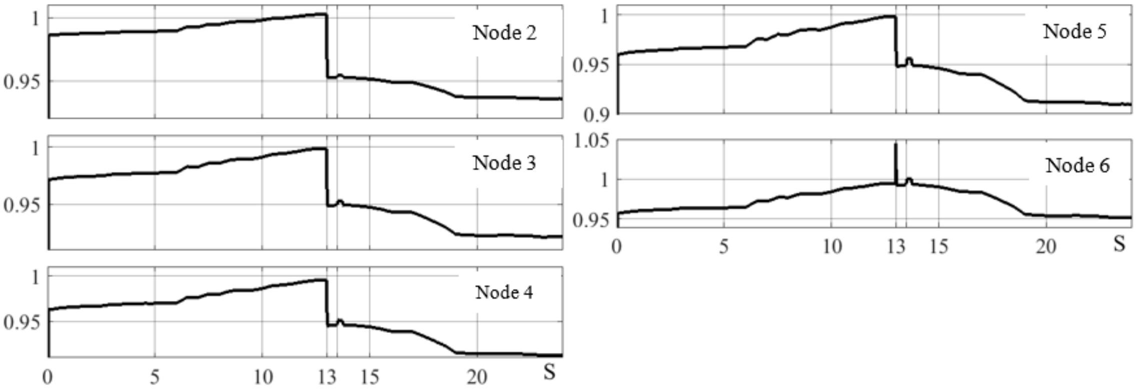


Figure 30. Per unit voltages of the nodes in Case4 overvoltage case without attack-Act, then Check algorithm I.

2. *Check then Act Algorithm*

Algorithm of Check then Act applied in the network, following the red arrows in the flowchart in Figure 29, the PV3 apply perturbation on the network, before the OLTC takes the action of stepping the voltage down, then check the nodes' response to decide.

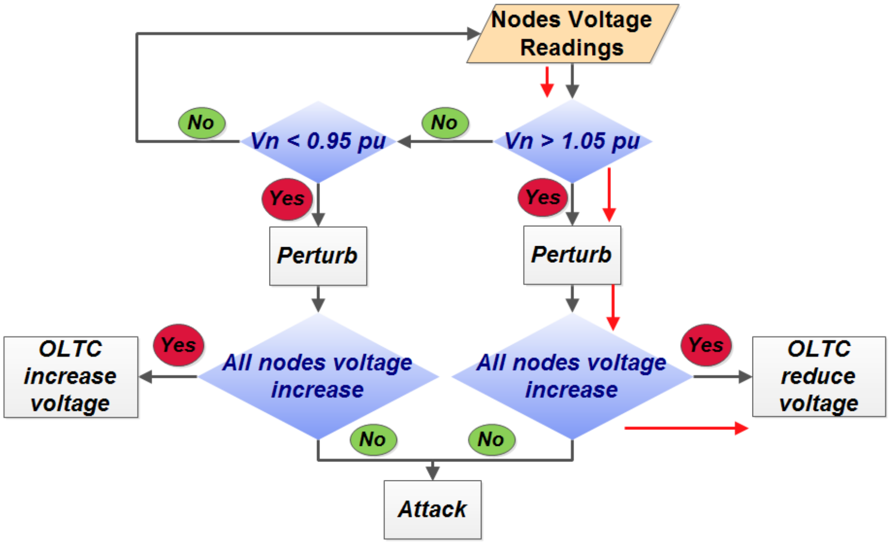


Figure 31. Case4 using perturbation and detection algorithm II (Check then Act).

The results of applying the algorithm in the network are shown in Figure 32. At second 13, node6 suffered from high voltage, then PV3 make a perturbation at second 13.5, all nodes have the response of increasing in voltage, which means no node is under attack, which leads that node6 has real overvoltage, so the OLTC step-down the voltage level at second 14.5, to compensate the voltage level at node6.

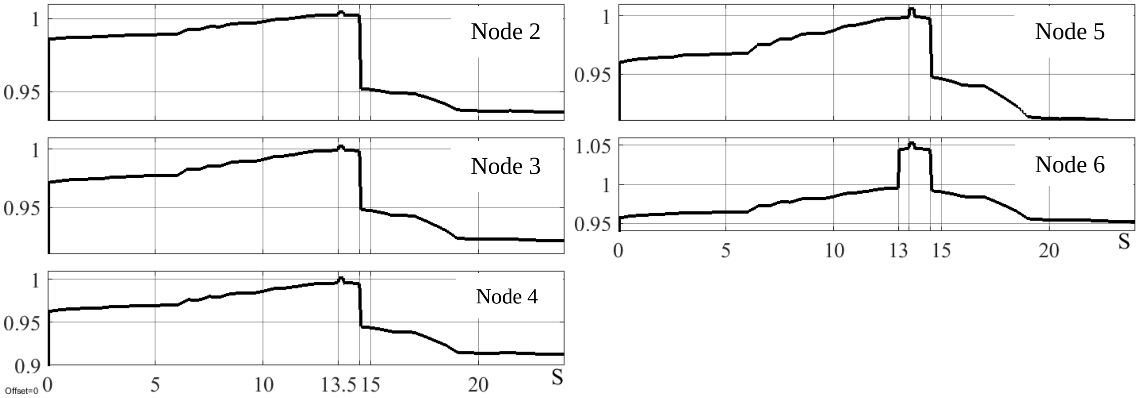


Figure 32. Per unit voltages of the nodes in case 4 overvoltage case without attack-Check then Act algorithm II.

E. Case5: Overvoltage at one node with attack

1. Act then Check Algorithm

In the case of an overvoltage attack, the algorithm can detect the attacker by following the red arrows in the flowchart in Figure 33. When detecting the overvoltage at node6, the OLTC reduces the voltage, then the PV3 makes a small perturbation in the network, and checks the nodes response if node6 does not respond, that means that the data of overvoltage is fake and altered by an attacker.

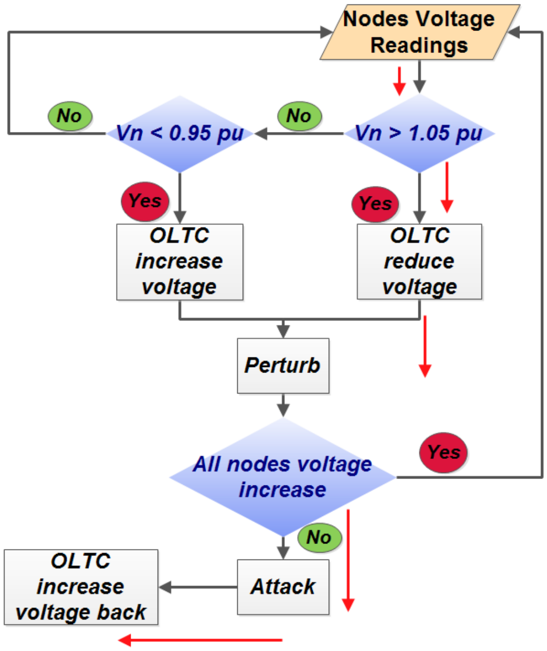


Figure 33. Case5 using perturbation and detection algorithm I (Act then Check).

Figure 34 shows the result of applying the algorithm in the simulation network. At second 13 node6 experience an attack, and have a false data of high voltage reading, at the same time the OLTC increase the voltage level of the network, after that at second 14 PV3 perturb the network for a short time, but no response from node6 is presented, this leads that node6 is under attack.

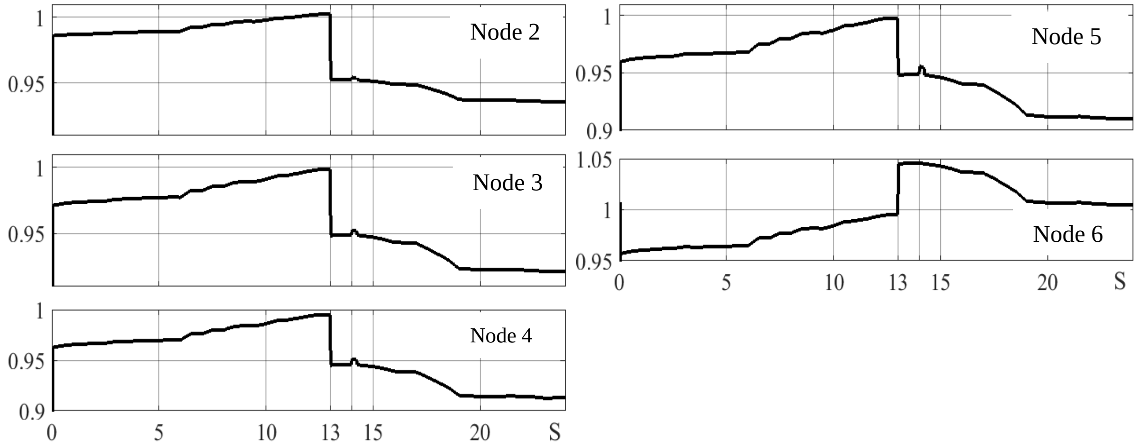


Figure 34 . Per unit voltages of the nodes in case 5 overvoltage case with attack-Act the Check algorithm II.

2. *Check then Act Algorithm*

The algorithm of Check then Act shows a better result in this case than Act then Check. It reduces the time of detection of the attacker. As the reading of the overvoltage at node6 is sensed, the PV makes the perturbation to have a quick check on the nodes' response. Then node6 does not respond, which means it is under attack, as illustrated in the flowchart in Figure 35.

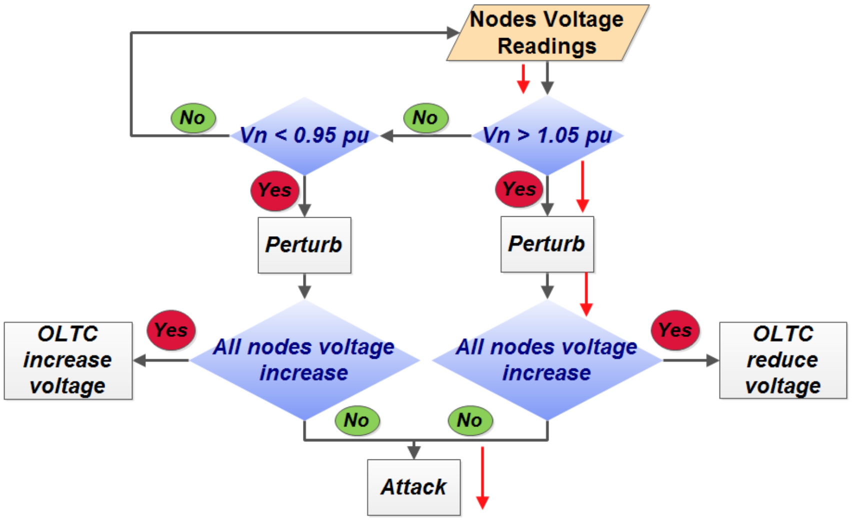


Figure 35. Case5 using perturbation and detection algorithm II (Check then Act).

The output of applying this algorithm in the network is shown in Figure 36 below. At the second 13 node6 experience an attack that results in an overvoltage in the node reading, following the algorithm Check then act, the PV3 make a perturbation at second 13.5, the nodes react to this perturbation similarly except node6 has no response, and this is clear in the figure below, which means node6 is under attack.

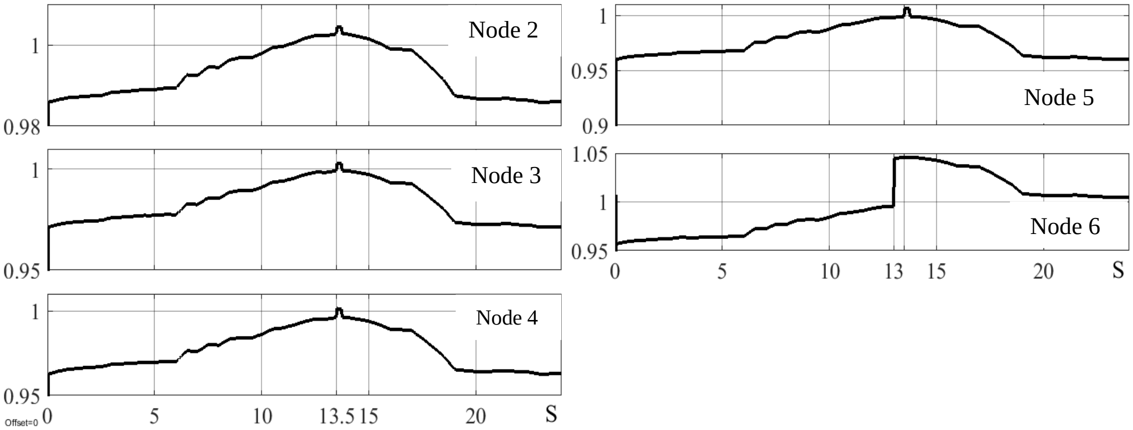


Figure 36. Per unit voltages of the nodes in case5 overvoltage case with attack-Check then Act algorithm II.

4.8 Multi-node attack detection

Previously in this chapter, the two algorithms introduced as i) Act then Check, ii) Check then Act, were applied to detect one node attack. In this section, these two algorithms will be applied to detect a multi-node attack. Applying the algorithms to have two or more attacks on the network will work to detect these attacks. This depends on the response of each node to the perturbation of the PV. A five-node attack will be presented to elucidate that.

i) Algorithm Act then Check for multi-node attack represented in Figure *37*. Assuming having attacks on all nodes (node2, node3, node4, node5, and node6), following the flow chart, the voltages' reading will indicate to have undervoltage or overvoltage in all nodes. Then the OLTC will act according to this information. After that, the PV will perturb and check the nodes' response. If they all react correctly according to the perturbation sign, then there is no attack, but if there were no response, they all have an attack.

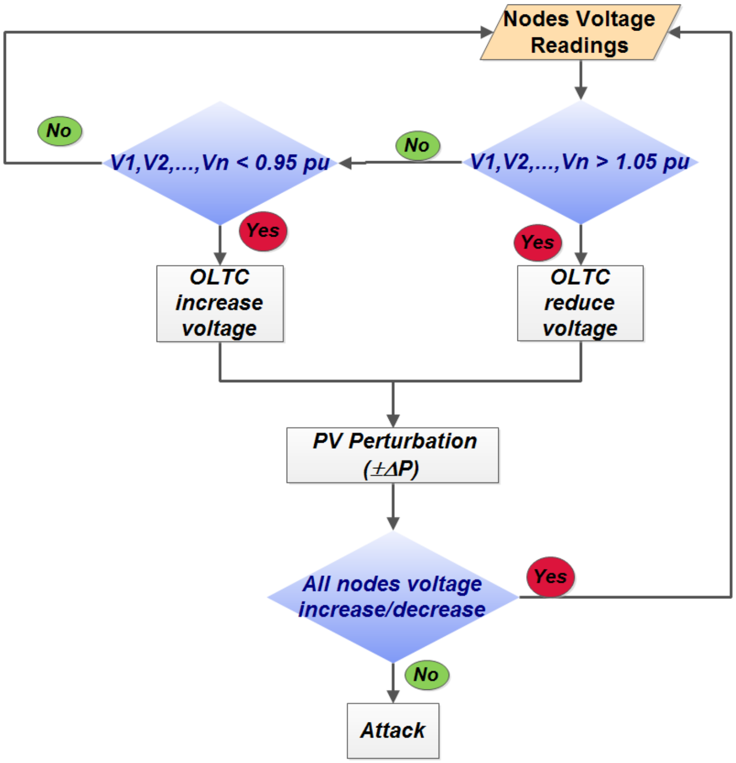


Figure 37. Multi-node perturbation and detection algorithm I (Act then Check).

ii) Algorithm Check then Act for multi-node attack represented in Figure 38. Applying this algorithm to detect the five nodes' attack as follows: first sensing the voltage of the nodes to have overvoltage or undervoltage. Then applying the PV perturbation and monitoring the response of all nodes. If they have the correct response, then there is no attack, and the OLTC will act accordingly to compensate for the voltage variation. However, if they do not have a response, then they are all under attack.

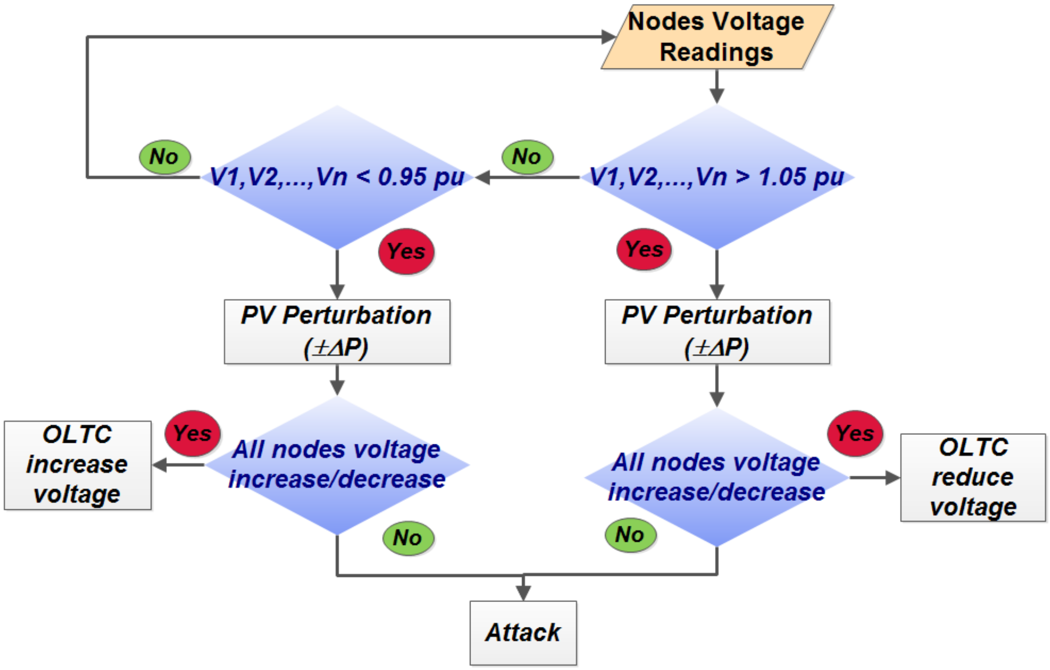


Figure 38. Multi-node perturbation and detection algorithm II (Check then Act).

This section shows that the PV perturbation has the main role of the detecting part, that the node that does not react correctly to the PV perturbation indicates to have an attack. Table 1 shows a comparison between the two algorithm approaches.

Table 1. Algorithm comparison.

Properties	Act then check algorithm	Check then act algorithm
Detection method	PV power perturbation.	PV power perturbation.
Attack detection	Detect one or more attacks.	Detect one or more attacks.
Overvoltage	Occurs due to low voltage attack.	Occurs due to actual overvoltage.
Undervoltage	Occurs due to a high voltage attack.	Occurs due to actual undervoltage.
Speed of the detection	Has a delay	No delay
Speed of the action	No delay	Has a delay

Refer to Table 1, the PV power perturbation used as a key detection tool in the network in both algorithms. Both approaches succeeded in detecting more than one attack occur in the network. Check then Act may cause a delay in the action of the OLTC but not overvoltage/undervoltage. Act then check may cause overvoltage/undervoltage, but it has fast action when having a real problem in the network node voltages.

Discussion

Based on the analysis and results achieved for the different scenarios and using both proposed algorithms, we notice the following general observations:

- The one feeder distribution network used for testing the suggested algorithm has been selected and configured to highlight the main points in the system, including the incorporation of distributed loads and distributed generation and the sensitivity aspects that play a crucial role in optimizing the proposed detection algorithms. The network has been simulated on Simulink® using standard bus parameters, real load profiles, and real PV generation profile to achieve more realistic results.

- The two proposed perturb and observe detection and protection algorithms (Act then Check, Check, then Act) have been shown to perform the required attack detection and mitigation functionality but with different advantages and disadvantages depending on the scenario.

- The Act then Check algorithm compensates the voltage violation immediately. Therefore, it protects the appliances against actual voltage violations. On the other side, a falsified attack will cause a short duration of voltage violation due to the instantaneous response to the falsified data and the delay in the detection process until the response is corrected.

- The Check then Act algorithm checks the legitimacy of the voltage violation readings before taking response actions. This will protect the system against attack induced voltage violations. In the case of actual voltage violations, the delayed voltage regulation response due to delays in the check process will cause short durations of voltage violations to be sustained on the network before corrective actions are taken.

- The main disadvantages of both proposed algorithms in the different scenarios stem from the check delay problem. This delay depends on the communication media used to transfer measurement from the IT switches to the OLTC. Different media like Fiber optics, separate data copper lines, power line communications, and wireless have different properties such as propagation delays, causing different communication time delays.

- The algorithm proposed has been applied in the network on node 6. Node 6 has been chosen according to the sensitivity analysis, which found that node 6 has the most critical relation with the variation of the PV's power injected. This can be considered as a worst-case scenario, yet it presents an excellent description of the overall system responses and the percentages of the perturbation used

- The proposed perturb and observe algorithms are limited in the sense that perturbations cannot be applied during the time of sunrise and sunset unless the PV system is provided with storage. This point does not represent a significant problem because all the industry now is headed to use storage systems with any PV.

- Both algorithms can have short durations of overvoltage/undervoltage either due to delayed response to actual violations in the case of Check then Act algorithm or due to immediate unverified response to attacks in the case of Act then Check algorithm.

- The performance of the two proposed algorithms depends on the probability of voltage violation falsification attacks, the probability of actual voltage violations, the relative costs of overvoltage and undervoltage durations, and the system communication delays.

- One can envision an adaptive approach that takes historical measures of the network to estimate the above-mentioned parameters and accordingly decide which algorithm to use such that the total cost is minimized.

CHAPTER 5: CONCLUSIONS AND FUTURE WORKS

5.1 Conclusions

This thesis highlighted cybersecurity problems in distributed systems and studied the effect of cyber-attacks on voltage profile in a single feeder distribution network with highly dispersed PV penetration and distributed loads. The high penetration of the PV in the distribution network results in new SGs that are more vulnerable to cyber-attacks. This raises the importance of cybersecurity on SGs to detect these attacks and protect the system against their adverse effects.

Mathematical network analysis has been done to study the node voltage and current responses to known perturbations on each PV in the network. Network analysis has been done on the network nodes and PVs. The most critical response comes from the PV3 side. This idea is used as the starting point of the proposed algorithms, where the perturbation has been done to have the maximum response from the rest of the network. Two simple and efficient attack detection algorithms based on perturb and observe checks were introduced. The algorithms perform the check at the actual power distribution layer, which introduces a second layer of protection in addition to classical communication network security measures. The two algorithms were simulated on a system model incorporating load and PV generation profiles. The results show that the proposed algorithms have complementary performance in terms of possibilities of voltage violations on the system. Voltage violations can still occur either due to delayed regulation response to actual violations on the system in the case of the Check then Act algorithm or due to instantaneous response to falsified attacks in the case of Act the Check algorithm.

5.2 Future Work

The results and models achieved in this work provided the basis for more future work as follows:

- Study the algorithm in more sophisticated distribution systems with multiple feeder lines and consider a storage system with each PV to help in the perturbation procedure.
- Study the effect of the different communication mediums of the network on the performance of the proposed algorithm.
- Combining both algorithms in an adaptive system that switches between the two algorithms based on the distribution network statistics and the attack statistics to optimize the overall network performance (minimize the probability of voltage violations).
- Detection performance analysis can be done to find the probability of attack detection of the proposed algorithms under different attack scenarios and network parameters.

REFERENCES

[1] P. Li *et al*., "Coordinated Control Method of Voltage and Reactive Power for Active Distribution Networks Based on Soft Open Point," in *IEEE Transactions on Sustainable Energy*, vol. 8, no. 4, pp. 1430-1442, Oct. 2017.

[2] R. Tonkoski, D. Turcotte, and T. H. M. EL-Fouly, "Impact of High PV Penetration on Voltage Profiles in Residential Neighborhoods," in *IEEE Transactions on Sustainable Energy*, vol. 3, no. 3, pp. 518-527, July 2012.

[3] C. L. Masters, "Voltage Rise: The Big Issue When Connecting Embedded Generation to Long 11 Kv Overhead Lines," in *Power Engineering Journal*, vol. 16, no. 1, pp. 5-12, Feb. 2002.

[4] T. Sansawatt, L. F. Ochoa and G. P. Harrison, "Integrating Distributed Generation Using Decentralised Voltage Regulation," *IEEE PES General Meeting*, Providence, RI, 2010, pp. 1-6.

[5] Strbac G., Jenkins N., Hird M. Wierzbowski and B. Olek, "Integration of the embedded generation into distribution systems at the competitive markets," *ISGT 2014*, Washington, DC, 2014, pp. 1-5.

[6] The Smart Grid Interoperability Panel – Cyber Security Working Group, “Guidelines for smart grid cyber security,” *NISTIR 7628*, Rev.1, September(2010)

[7] T. Wu, C. Chang, Z. Liu, and T. Yu, "Single-Stage Converters for Photovoltaic Powered Lighting Systems with MPPT and Charging Features," *APEC '98 Thirteenth*

Annual Applied Power Electronics Conference and Exposition, Anaheim, CA, USA, 1998, pp. 1149-1155 vol.2.

[8] A. M. De Broe, S. Drouilhet, and V. Gevorgian, "A Peak Power Tracker for Small Wind Turbines in Battery Charging Applications," in *IEEE Transactions on Energy Conversion*, vol. 14, no. 4, pp. 1630-1635, Dec. 1999.

[9] B. M. Omar, H. Samir, Z. S. Ahmed, and D. K. Y. Islam, "A Comparative Investigation of Maximum Power Point Tracking Techniques for Grid Connected PV System Under Various Weather Conditions," *2017 5th International Conference on Electrical Engineering - Boumerdes (ICEE-B)*, Boumerdes, 2017, pp. 1-5.

[10] Salas V, Olıas E, Barrado A. A La zaro., “Review Of The Maximum Power Point Tracking Algorithms for Stand-Alone Photo Voltaic Systems,” *Solar Energy Materials & Solar Cells*,2006;90:1555–78

[11] T. Esram and P. L. Chapman, "Comparison of Photovoltaic Array Maximum Power Point Tracking Techniques," in *IEEE Transactions on Energy Conversion*, vol. 22, no. 2, pp. 439-449, June 2007.

[12] M. Esmalifalak, G. Shi, Z. Han and L. Song, "Bad Data Injection Attack and Defense in Electricity Market Using Game Theory Study," in *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 160-169, March 2013.

[13] K. J. Ross, K. M. Hopkinson, and M. Pachter, "Using a Distributed Agent-Based Communication Enabled Special Protection System to Enhance Smart Grid Security," in *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp.

[14] Y. Chakhchoukh and H. Ishii, "Coordinated Cyber-Attacks on the Measurement Function in Hybrid State Estimation," in *IEEE Transactions on Power Systems*, vol. 30, no. 5, pp. 2487-2497, Sept. 2015.

[15] X. Liu, Z. Li and Z. Li, "Optimal Protection Strategy Against False Data Injection Attacks in Power Systems," in *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1802-1810, July 2017.

[16] X. Liu, Z. Li, Z. Shuai, and Y. Wen, "Cyber Attacks Against the Economic Operation of Power Systems: A Fast Solution," *in IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 1023-1025, March 2017

[17] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online Detection of Stealthy False Data Injection Attacks in Power System State Estimation," *in IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1-1.

[18] S. Zonouz, C. M. Davis, K. R. Davis, R. Berthier, R. B. Bobba, and W. H. Sanders, "SOCCA: A Security-Oriented Cyber-Physical Contingency Analysis in Power Infrastructures," *in* IEEE *Transactions on Smart Grid*, vol. 5, no. 1, pp. 3-13, Jan. 2014.

[19] W. Wang and Z. Lu, “Survey Cyber Security in the Smart Grid: Survey and Challenges,” *Computer Networks: The International Journal of Computer and Telecommunications Networking.*, vol. 57, no. 5, pp. 1344–1371, Apr. 2013.

[20] Aditya Ashok, Adam Hahn, and Manimaran Govindarasu,”Cyber-Physical Security of Wide-Area Monitoring, Protection and Control in a smart grid environment,” *Journal of Advanced Research*, Volume 5, Issue 4, Pages 481-489,2014, ISSN 2090-1232A.

[21] Farraj, E. Hammad, and D. Kundur, "On the Impact of Cyber Attacks on Data Integrity in Storage-Based Transient Stability Control," *in IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3322-3333, Dec. 2017.

[22] Y. Zhang, L. Wang, Y. Xiang, and C. W. Ten, "Power System Reliability Evaluation with SCADA Cybersecurity Considerations*," in IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1707-1721, July 2015.

[23] http://clients.rte-france.com/lang/an/visiteurs/vie/vie_stats_conso_inst.jsp

[24] The Smart Grid Interoperability, "Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security," *Panel Cyber Security Working Group*, September 2010.

[25] Chih-Che Sun, Adam Hahn, Chen-Ching Liu, "Cyber Security of A Power Grid: State-of-The-Art," *International Journal of Electrical Power & Energy Systems*, Volume 99,2018, Pages 45-56, ISSN 0142-0615.

[26] G. Tsengenes and G. Adamidis, "Investigation of The Behavior of A Three Phase Grid-Connected Photovoltaic System to Control Active and Reactive Power," *Electric Power Systems Research*, vol. 81, pp. 177-184, 2011

[27] M. Salvador and S. Grieu, "Methodology for The Design of Energy Production and Storage Systems in Buildings: Minimization of The Energy Impact on The Electricity Grid," *Energy and Buildings*, vol. 47, pp. 659-673, 2012.

[28] International Organization for Standardization (ISO). "*Publicly Available Standards". standards.iso.org.*

[29] S. Pukhrem, M. Basu, and M. F. Conlon, "Probabilistic Risk Assessment of Power Quality Variations and Events Under Temporal and Spatial Characteristic of Increased PV

Integration in Low-Voltage Distribution Networks," *in IEEE Transactions on Power Systems*, vol. 33, no. 3, pp. 3246-3254, May 2018

[30] S. Hashemi and J. Østergaard, "Methods and Strategies for Overvoltage Prevention in Low Voltage Distribution Systems With PV," *in IET Renewable Power Generation*, vol. 11, no. 2, pp. 205-214, 2 8 2017.

[31] D. V. Bozalakov, T. L. Vandoorn, B. Meersman, G. K. Papagiannis, A. I. Chrysochos, and L. Vandevelde, "Damping-Based Droop Control Strategy Allowing an Increased Penetration of Renewable Energy Resources in Low-Voltage Grids," *in IEEE Transactions on Power Delivery*, vol. 31, no. 4, pp. 1447-1455, Aug. 2016.

[32] T. Vieira da Silva, R. Vitor Arantes Monteiro, F. A. M. Moura, M. R. M. C. Albertini, M. A. Tamashiro, and G. Caixeta Guimaraes, "Performance Analysis of Neural Network Training Algorithms and Support Vector Machine for Power Generation Forecast of Photovoltaic Panel," *in IEEE Latin America Transactions*, vol. 15, no. 6, pp. 1091-1100, June 2017.

[33] L. Wang, D. H. Liang, A. F. Crossland, P. C. Taylor, D. Jones, and N. S. Wade, "Coordination of Multiple Energy Storage Units in a Low-Voltage Distribution Network," *in IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 2906-2918, Nov. 2015.

[34] E. Demirok, P. C. González, K. H. B. Frederiksen, D. Sera, P. Rodriguez, and R. Teodorescu, "Local Reactive Power Control Methods for Overvoltage Prevention of Distributed Solar Inverters in Low-Voltage Grids," in *IEEE Journal of Photovoltaics*, vol. 1, no. 2, pp. 174-182, Oct. 2011.

[35] Safayet, P. Fajri, and I. Husain, "Reactive Power Management for Overvoltage Prevention at High PV Penetration in a Low-Voltage Distribution System," *in IEEE Transactions on Industry Applications,* vol. 53, no. 6, pp. 5786-5794, Nov.-Dec. 2017.

[36] S. Pukhrem, M. Basu, M. F. Conlon, and K. Sunderland, "Enhanced Network Voltage Management Techniques Under the Proliferation of Rooftop Solar PV Installation in Low-Voltage Distribution Network," *in IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 5, no. 2, pp. 681-694, June 2017.

[37] Price, Elizabeth Lamond. "The 100 Most Significant Events in American Business: *An Encyclopedia*." (2013), page 86.

[38] F. Halim, S. Yussof, and M. E. Rusli. "Cyber Security Issues in Smart Meter and Their Solutions," *IJCSNS International Journal of Computer Science and Network Security*, VOL.18 No.3, March 2018.

[39] A. Aggarwal, S. Kunta, and P. K. Verma, "A Proposed Communications Infrastructure For The Smart Grid," *2010 Innovative Smart Grid Technologies (ISGT)*, Gothenburg, 2010, pp. 1-5.

[40] C. Lin, S. Wu, and M. Lee, "Cyber Attack and Defense on Industry Control Systems," *2017 IEEE Conference on Dependable and Secure Computing*, Taipei, 2017, pp. 524-526.

[41] Chih-Che Sun, Adam Hahn, Chen-Ching Liu, "Cyber Security Of A Power Grid: State-Of-The-Art," *International Journal of Electrical Power & Energy Systems*, Volume 99,2018, Pages 45-56, ISSN 0142-0615.

[42] National Cybersecurity and Communications Integration Center/ Industrial Control Systems Cyber Emergency Response Team NCCIC and ICS-CERT. NCCIC/ICS-CERT 2015 year, Apr. 19, 2016

[43] G.Colleen, S.Dane, and W.Aaron. Tue. "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector." *United States*. doi:10.2172/1337873.

[44] Chih-Che Sun, Adam Hahn, and Chen-Ching Liu, "Cyber Security of A Power Grid: State-of-The-Art," *International Journal of Electrical Power & Energy Systems*, Volume 99, Pages 45-56,2018.

[45] E. Padilla, K. Agbossou, and A. Cardenas, "Towards Smart Integration of Distributed Energy Resources Using Distributed Network Protocol Over Ethernet," in *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1686-1695, July 2014.

[46] R. C. -. Phan, "Authenticated Modbus Protocol for Critical Infrastructure Protection," in *IEEE Transactions on Power Delivery*, vol. 27, no. 3, pp. 1687-1689, July 2012.

[47] G. Hayes and K. El-Khatib, "Securing Modbus Transactions Using Hash-Based Message Authentication Codes And Stream Transmission Control Protocol," *2013 Third International Conference on Communications and Information Technology (ICCIT)*, Beirut, 2013, pp. 179-184.

[48] G. Gilchrist, "Secure authentication for DNP3," *2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, Pittsburgh, PA, 2008, pp. 1-3.

[49] R. Amoah, S. Camtepe and E. Foo, "Securing DNP3 Broadcast Communications in SCADA Systems," in *IEEE Transactions on Industrial Informatics*, vol. 12, no. 4, pp. 1474-1485, Aug. 2016.

[50] K. Song, K. Yu, and D. Lim, "Secure frame format for avoiding replay attack in Distributed Network Protocol (DNP3)," *2015 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, 2015, pp. 344-349.

[51] G. N. Ericsson, "Toward a Framework for Managing Information Security for an Electric Power Utility—CIGRÉ Experiences," in *IEEE Transactions on Power Delivery*, vol. 22, no. 3, pp. 1461-1469, July 2007.

[52] V. Namboodiri, V. Aravinthan, S. N. Mohapatra, B. Karimi, and W. Jewell, "Toward a Secure Wireless-Based Home Area Network for Metering in Smart Grids," in *IEEE Systems Journal*, vol. 8, no. 2, pp. 509-520, June 2014.

[53] X. Liang, X. Li, R. Lu, X. Lin, and X. Shen, "UDP: Usage-Based Dynamic Pricing With Privacy Preservation for Smart Grid," in *IEEE Transactions on Smart Grid,* vol. 4, no. 1, pp. 141-150, March 2013.

[54] D. E. Bakken, A. Bose, C. H. Hauser, D. E. Whitehead, and G. C. Zweigle, "Smart Generation and Transmission with Coherent, Real-Time Data," in *Proceedings of the IEEE*, vol. 99, no. 6, pp. 928-951, June 2011.

[55] North American Electric Reliability Corporation (NERC). CIP standard.

[56] Energy Sector Control Systems Working Group (ESCSWG)," Roadmap to Achieve Energy Delivery System Cyber Security," *The U.S. Department of Energy*.

[57] The Smart Grid Interoperability, " Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security*," Panel Cyber Security Working Group*, September 2010.

[58] NISTIR 7628.*;* " Guidelines for Smart Grid Cyber Security"*; National Institute of Standards and Technology; U.S. Department of Commerce: Gaithersburg, MD* (31 August 2010).

[59] SP 800-82 Rev.1.; " Guide to Industrial Control Systems (ICS) Security"; *National Institute of Standards and Technology; U.S. Department of Commerce: Gaithersburg, MD* (14 May 2013).

[60] R. Deng, P. Zhuang, and H. Liang, "False Data Injection Attacks Against State Estimation in Power Distribution Systems," *in IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2871-2881, May 2019.

[61] P. Gao *et al*., "Identification of Successive "Unobservable" Cyber Data Attacks in Power Systems Through Matrix Decomposition," in *IEEE Transactions on Signal Processing*, vol. 64, no. 21, pp. 5557-5570, 1 Nov.1, 2016.

[62] J.O.Petinrin and M. Shaaban, "Impact of renewable generation on voltage control in distribution systems" *Renewable and Sustainable Energy Reviews,* Volume 65, Pages 770-783, November 2016.

[63] Xuan Liu; Zuyi Li; Zhikang Shuai; Yunfeng Wen "Cyber Attacks Against the Economic Operation of Power Systems: A Fast Solution*" IEEE Transactions on Smart Grid*, Volume 8, Issue, 2, March 2017.

[64] Yao Liu, Peng Ning, and Michael K. Reiter. 2009. "False data injection attacks against state estimation in electric power grids." *In Proceedings of the 16th ACM*

conference on Computer and communications security (CCS '09). ACM, New York, NY, USA, 21-32.

[65] Y. Isozaki et al., "Detection of Cyber Attacks Against Voltage Control in Distribution Power Grids With PVs," *in IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1824-1835, July 2016.

[66] (ISO) International Organization for Standardization. "*Publicly Available Standards*".

[67] Tapan Kumar Saha, Mithulananthan N., "Field Investigation of Voltage Quality Issues in Distribution Network with PV Penetration", *IEEE PES Asia-Pacific Power and Energy Engineering Conference, Brisbane, QLD, Australia*, 15-18 Nov. 2015, pp. 1-5.

[68] Rahman, Md & Bin, M & Chowdhury, Ramim & Abdulla, Md & Mamun, Al & Hasan, Md & Mahfuz, Sayeed, (2013), "Summary of Smart Grid: Benefits and Issues", *International Journal of Scientific and Engineering Research*, Volume 4.

[69] Judy McKay (Chair), Matthias Hamburg (Vice-Chair), "Standard Glossary of Terms Used in Software Testing, Version 3.1" *International Software Testing Qualifications Board Glossary ISTQB,* 18. March 2016.

[70] Matthaios Santamouris, "Energy Consumption and Environmental Quality of the Building Sector", *Minimizing Energy Consumption, Energy Poverty and Global and Local Climate Change in the Built Environment: Innovating to Zero*, Chapter 2, 2019.

[71] M. A. Mahmud, M. J. Hossain, H. R. Pota, and A. B. M. Nasiruzzaman, "Voltage control of distribution networks with distributed generation using reactive power

compensation," *IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*, Melbourne, VIC, 2011, pp. 985-990, doi: 10.1109/IECON.2011.6119329.

[72] American National Standards Institute, C84.1-2011: American National Standard for Electric Power Systems and Equipment—Voltage Ratings (60 Hertz), 2011.

[73] Cipcigan L, Taylor P, Lyons P. "A dynamic virtual power station model comprising small-scale energy zones", *International Journal of Renewable Energy Technology*, 2009, 1(2), 173-191.

APPENDIX:

APPENDIX 1: PV OUTPUT POWER

Time	PV power(kW)
0.5	1.289812
1.0	1.278751
1.5	1.300872
2.0	1.311933
2.5	1.433600
3.0	2.978105
3.5	3.470370
4.0	4.049088
4.5	4.810380
5.0	5.011572
5.5	6.508548
6.0	7.037196
6.5	16.556280
7.0	16.910069
7.5	22.964977
8.0	23.247828

8.5	28.294299
9.0	30.540289
9.5	30.870757
10.0	33.470371
10.5	36.766500
11.0	36.990640
11.5	39.564956
12.0	42.220380
12.5	43.818488
13.0	43.818488
13.5	44.099217
14.0	43.552646
14.5	41.815808
15.0	39.517699
15.5	36.544767
16.0	32.895930
16.5	32.705610
17.0	32.643714
17.5	28.294299
18.0	22.964977
18.5	16.910069

19.0	7.637340
19.5	6.508548
20.0	5.011572
20.5	4.049088
21.0	3.335220
21.5	2.978105
22.0	1.433600
22.5	1.311933
23.0	1.300872
23.5	1.278751
24.0	1.289812