12-4-2018

Exploring Cyber Security Issues and Solutions for Various Components of DC Microgrid System

Sultana Razia Akhter

EXPLORING CYBER SECURITY ISSUES AND SOLUTIONS FOR VARIOUS COMPONENTS OF DC MICROGRID SYSTEM

By

Sultana Razia Akhter

A Thesis

Submitted in Partial Fulfilment of the

Requirements for the Degree of

Master of Science

Major: Electrical and Computer Engineering

The University of Memphis

December 2018

This thesis is dedicated to my parents A M Rezaul Karim Talukder & Tahura Akhter Khatun, dear family members, and people who made this abroad like home away from home.

ACKNOWLEDGEMENT

To start with, I would like to thank Dr. Mohd. Hasan Ali, my honorable thesis supervisor, for his immense support, encouragement, supervision throughout my graduate study at University of Memphis. I heartfully appreciate his effort and time for me to explain things and concepts related to my research. I am thankful to almighty for blessing me with such good advisor who helped me learn new things and has been a good philosopher and guide.

I would also like to thank Dr. Chrysanthe Preza and Dr. Sajjan Shiva for their support and consent to be in my thesis committee and providing me with their valuable suggestions and time to present my work in front of them.

I would like to mention special thanks to the current members of Electric Power and Energy Systems (EPES) laboratory for their knowledgeable discussion and suggestions as well as providing friendly and joyful environment to carry on daily work.

Finally, my special thanks will go for my dear parents and family who have always motivated, supported, loved me, and thereby strengthened me up throughout my life.

ABSTRACT

Nowadays, considering the growing demand for the DC loads and simplified interface with renewable power generation sources, DC microgrids (DCMG) could be cost-effective solutions for the power supply in a small-scale area. The supervisory control and data acquisition (SCADA) system maintains the bidirectional power communication through the internet connectivity with the microgrid. However, this intelligent and interactive feature may pose a cyber-security threat to the power grid. This work aims at exploring cyber-security issues and their solutions for the DC-microgrid system. To mitigate the adverse effects of various cyber-attacks such as the False Data Injection (FDI) attack, Distributed Denial of Service (DDoS) attack, etc., two new techniques based on non-linear and proportional-integral (PI) controllers have been proposed. Simulations results obtained from the MATLAB/Simulink software demonstrate the effectiveness of the proposed methods in mitigating the adverse effects of cyber-attacks on the DCMG system performance.

PREFACE

Two papers resulting of this work have been used as the manuscript of this thesis. The methods and results from those papers have been used in a combined way in Chapters 2 and 3. One paper has been submitted and is currently under review at the *IEEE Innovative Smart Grid Technologies (ISGT) conference 2019.* Another paper is ready for submission at the *IEEE Transactions on Smart Grid.*

Following is the list of articles used in this thesis:

- S. R. Akhter and M. H. Ali, “Cyber Security Issues and Solutions for Photovoltaic (PV) System Connected to DC Microgrid”, *IEEE PES Innovative Smart Grid Technologies (ISGT) conference,* Washington DC, USA, February 18-21, 2019. (Under Review)
- S. R. Akhter and M. H. Ali, “A Novel Solution to Mitigate Adverse Effects of Single, Repeated and Simultaneous Cyber-Attacks on DC Microgrid System”, in *IEEE Transaction on Smart Grid.* (Under Review)

TABLE OF CONENTS

Chapter 3

Chapter 4

LIST OF FIGURES

LIST OF ACRONYMS

AC	Alternating Current
BES	Battery Energy Storage
DC	Direct Current
DCMG	DC Microgrid
DDoS	Distributed Denial of Service
DER	Distributed Energy Resources
DG	Distributed Generator
ESS	Energy Storage System
FC	Fuel Cell
FDI	False Data Injection
IGBT	Insulated Gate Bipolar Transistor
MG	Microgrid
MPPT	Maximum Power Point Tracker
N-L	Non-Linear
PCC	Point of Common Coupling

PI	Proportional Integral
PMSG	Permanent Magnet Synchronous Generator
PMU	Phasor Measurement Unit
PV	Photovoltaic
RES	Renewable Energy Resources
SCADA	Supervisory Control And Data Acquisition
WPS	Wind Power System

CHAPTER-1

INTRODUCTION

It’s been more than 150 years, the electric power has been commercialized and since then it has always been a topic of argument on what form of electric power we should choose for generation, transmission and distribution. Is that alternating current (AC) or direct current (DC)? At that time Thomas Edison lost the great technological battle known as “The war of currents” against George Westinghouse and Nikola Tesla, and also he failed to establish the efficient DC power network model in front of AC power network due to having a shortcoming of high distance transmission losses.

In recent times, the concept of localized, autonomous and resilient microgrid (MG) power system has gained wider popularity [1], [2], [3], [4], [5], [6], [7]. Considering the increasing demand for the DC-loads, simplified interface with the renewable power generation, reduction in the usage and losses associated with the power-converters, the perception of DC Microgrid (DCMG) could be a cheaper and more efficient alternative for the power supply in small-scale areas like residential areas, university campuses, offices, shopping malls, military bases, aircrafts, etc.

Furthermore, integrating the intelligence and internet connectivity, this microgrid system will allow the consumers to engage with the main grid through smart metering and ultimately that will result in dynamic demand-management. This publicized feature makes the whole system into cyber-physical system, and ultimately that causes the issue of cyber security. So, to ensure the reliable and resilient power supply, cyber security issues should be acknowledged and resolved. In this section, we will have a look at the state-of-the-art of the DC Microgrid system and the cyber security aspect of it.

1.1 Background and Literature Review

1.1.1 DC Microgrid and its Control

DC MICROGRID:

The Microgrid (MG) concept considers a bunch of loads and micro-sources, in terms of the production capability (50-100MW), functioning as a single controllable system that provides power to its local area, both in stand-alone mode or the interconnected mode with the conventional grid system. For the distributed generation systems with the renewable resources, this microgrid concept is providing a new architype for the future power industry, while depleting fossil fuels, increasing energy demand, and need for high-reliable power supply have become some burning questions. These microgrid systems allow bidirectional flow of power and also incorporate communication channels along with the power network that provides better controllability and introduces the active consumer participation.

Microgrids can be of two types, namely the AC microgrid that provides AC power and the DC microgrid that provides DC power. In recent times, the renewable energy resources are the main concerns, and Photovoltaic system, Fuel cell system, Battery energy system all produce DC currents. Moreover, for capturing the maximum power from the wind and to provide better quality of power, in wind power generation system the AC power is first converted into DC, then converted into AC again. Thus, the introduction of DC microgrid system will eventually minimize both the cost and the complexity of the power network in terms of the reduced number of power converters. From the load side, nowadays, the number of DC loads are increasing such as mobiles phones, computers, the data centers that require DC supply, etc. In addition, the following features such as

- Simple power regulation
- Absence of reactive power and frequency control
- Decentralized planning and distributing
- Low cost and high reliability

ensure better power quality with less power loss. Thus, the DC microgrid system can be a good option for the data center, residential area, portable military bases, etc. [8], [9], [1], [10], Fig. 1 clearly specifies the motivation for using the DCMG as future grid system.

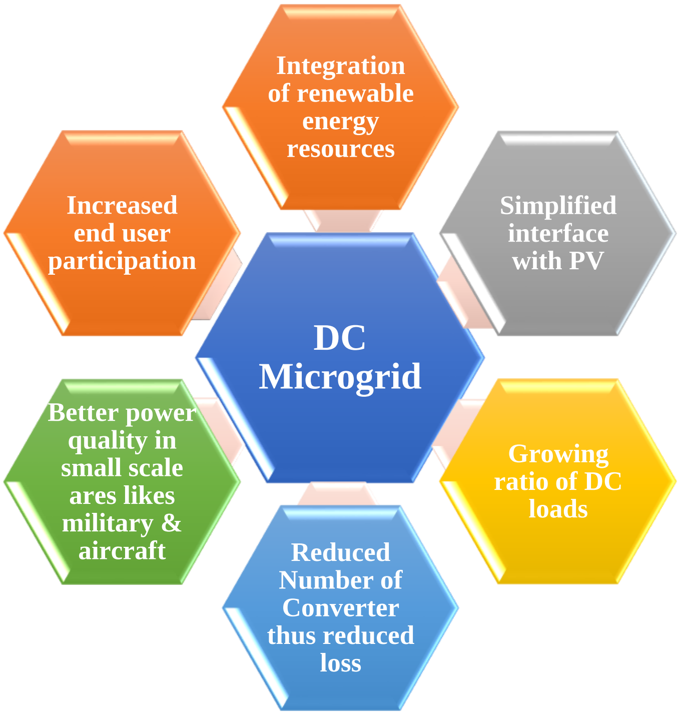

Integration of renewable energy resources
Increased end user participation
Simplified interface with PV
DC Microgrid
Better power quality in small scale ares likes military & aircraft
Growing ratio of DC loads
Reduced Number of Converter thus reduced loss

Fig. 1: Motivation towards DC Microgrid System.

A general structure of the DC MG has been shown in Fig. 2. There are some generation units, AC load, DC load, and ESS. Those are connected in parallel with the DC bus through the corresponding AC-DC rectifier for the AC generation system such as wind power system, DC-AC inverters for the AC loads, and DC-DC converters for the DC loads and generation systems. The designed DC bus is connected with the main grid system through a switching mechanism, so that the bidirectional power flow to and from both the grids can be obtained. The total system is being monitored by the supervisory control and data acquisition (SCADA) system that necessitates multilevel control schemes for the DC MG system.

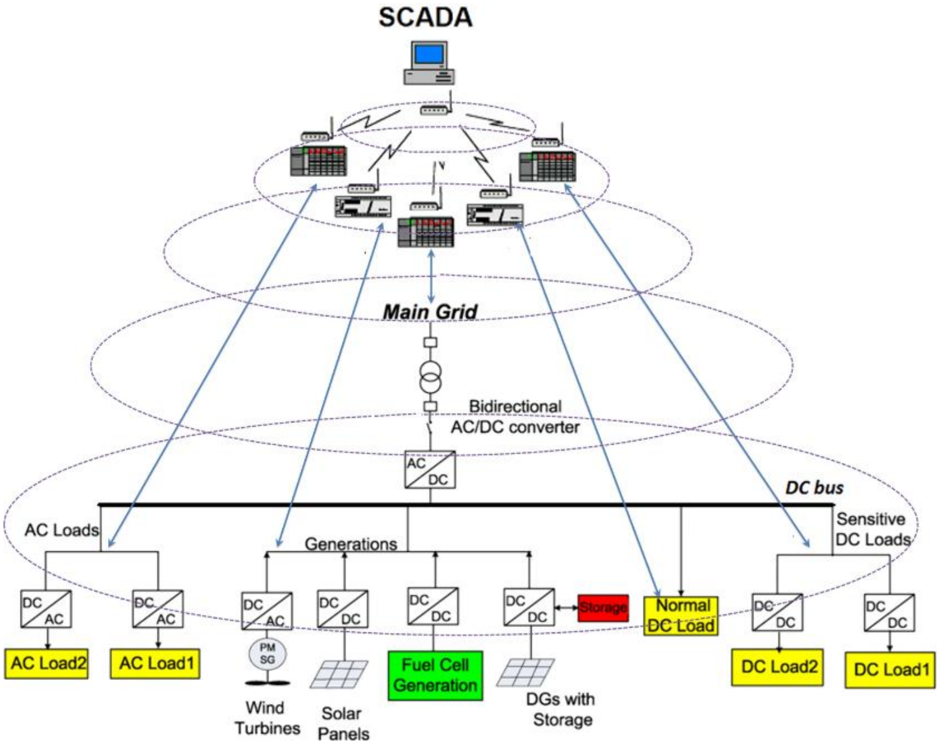


Fig. 2: DC MG System incorporated with the SCADA system.

DC MG CONTROL SCHEME:

The wider usage of the renewable energy resources, power electronics devices for rectifier and converter, intelligent control among the DGs, proper voltage and current sharing, power flow control, mode of operation with reliability and dynamic response all make the management and control of DC MG system more multi-objective tasks, which cover different methodological aspects, technicality, time scales and physical levels. These domains necessitate the multilevel control scheme for the robust and reliable operation of DC MG system. That includes the three principal control levels [5], [11], [12] as follows:

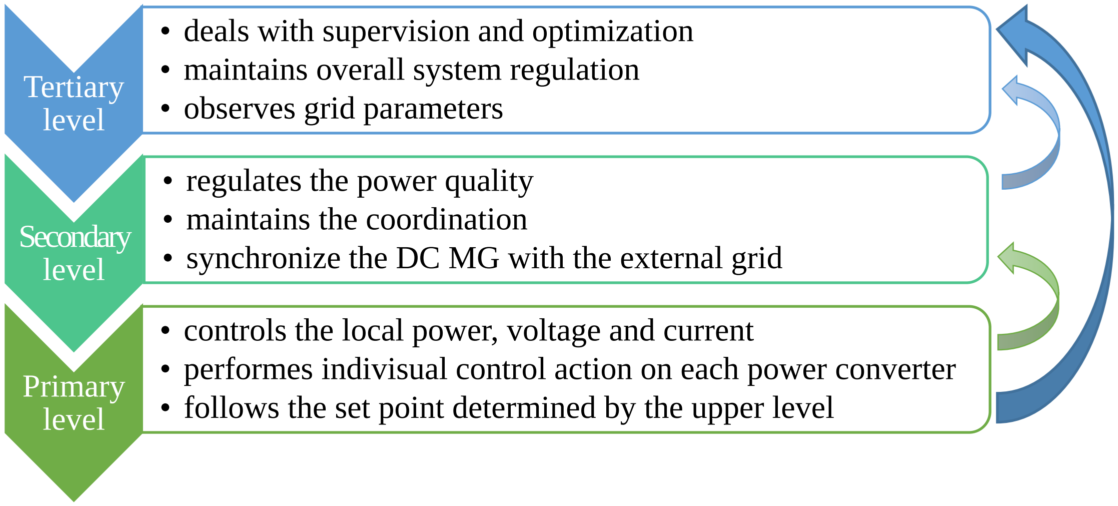

Tertiary level
• deals with supervision and optimization
• maintains overall system regulation
• observes grid parameters
Secondary level
• regulates the power quality
• maintains the coordination
• synchronize the DC MG with the external grid
Primary level
• controls the local power, voltage and current
• performes indivisual control action on each power converter
• follows the set point determined by the upper level

Fig. 3: Control levels for DC MG.

Depending upon this multilevel control characteristics and the communication links among the controllers, the total DC MG control system can be divided into four major schemes. The Table 1 shows the basic conception and the scope of operation for different control schemes:

TABLE 1. ANALYZING DIFFERENT CONTROL SCHEMES OF DCMG

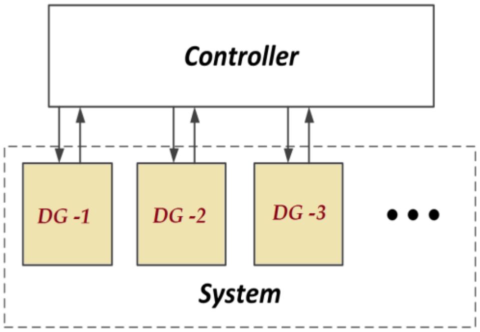
Control Scheme	**Features**	**Description**
Centralized control scheme [13], [14],	Conception	Collects and transmits information from and to local DGs respectively.  Fig. 4: *Centralized Control.*
	Advantage	▪ Include strong observability ▪ Straight forward implementation ▪ Overall controllability ▪ Suitable for localized and small size of MGs, where the amount of information to be exchanged is limited. ▪ Require less communication among the DG units, so time delay issue can be minimized. ▪ Cost economic, as it uses only one central controller

TABLE. 1 (Continued)

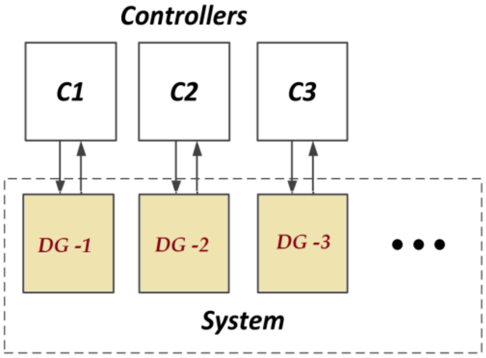
Control Scheme	**Features**	**Description**
	Disadvantage	▪ Single point failure issue, i.e., as only one controller is being used, any breakdown of the controller will affect the total system. ▪ Reduced flexibility and expandability ▪ Considerable amount of computational resources is necessary.
Decentralized control scheme [15], [16], [17]	Conception	Performs regulation based on the information from the local measurement.  Controllers C1 C2 C3 DG -1 DG -2 DG -3 • • • System Fig. 5: *Decentralized Control*
	Advantage	▪ Independent control; does not require information from other part of the system ▪ Controls respective unit relying on the local information ▪ Real time communication is not required, thus reduces the time delay.

TABLE. 1 (Continued)

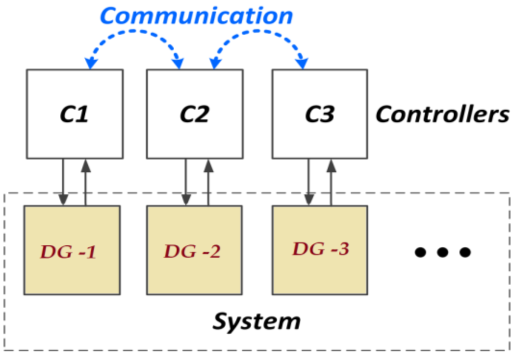
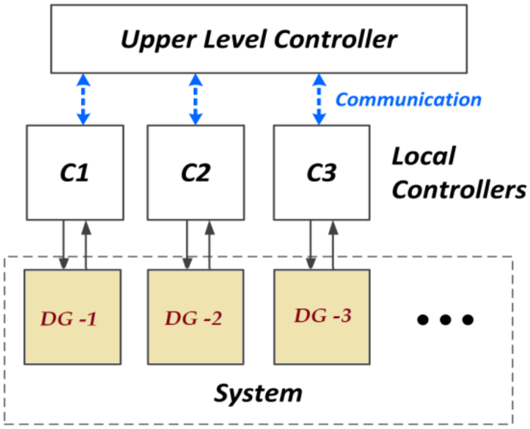
Control Scheme	**Control Scheme**	**Control Scheme**
		▪ Reduces computational complexity.
	Disadvantage	▪ Global coordination is not possible due to lack of communication among individual converters. Incurs the cost as the number of controllers are increasing
Distributed control scheme [18], [12], [19]	Conception	Modern communication technologies (like- WiFi, Zigbee etc.) and Information Exchange Algorithm (P2P, Gossip, Consensus) motivate to go with this control scheme. It performs regulation based on local measurements as well as the neighboring communication.  Communication C1 C2 C3 Controllers DG -1 DG -2 DG -3 System Fig. 6: Distributed Control
	Advantage	▪ Allows the distributed controllers to communicate with each other.

TABLE. 1 (Continued)

Control Scheme	**Control Scheme**	**Control Scheme**
		▪ The information exchange algorithms allow the parameters to come to a covenant quantity by exchanging the information among the neighboring controllers. ▪ A coordinated control can be achieved. ▪ Allows global measurement technique. Moderate computational complexity.
	Disadvantage	▪ Proper communication and information channel is needed. ▪ Any of the controller's discoordination may affect the other's performance. ▪ Time delay can be a major issue. Increases the cost.
Hierarchical control scheme [17], [20], [21], [22], [23]	Conception	▪ Due to increasing complexity of the energy management system and required intelligence for the controllers, the idea of this controller has been developed. It performs the regulation using different levels (upper and lower) by distributing the control functions among all the levels.

TABLE. 1 (Continued)

Control Scheme	**Control Scheme**	**Control Scheme**
		 Upper Level Controller Communication C1 C2 C3 Local Controllers DG -1 DG -2 DG -3 • • • System Fig. 7: Hierarchical Control
	Advantage	▪ Functions provided by the centralized controller and can be realized in a distributed way by the primary controllers. ▪ Simple function can be provided to primary controllers, that control basic voltage/current control and power sharing. Advanced control and management function can be provided for the secondary controller, that co-ordinates the total system.
	Disadvantage	▪ Involves high level of computational and intellectual controller design. ▪ Global information is required, that may cause serious time delay issue.

1.1.2 Cyber Security Issues and Solutions in Power System

The SCADA system necessitates multilevel control for providing reliability and dynamic response for the DC MG system. This multilevel monitoring and control requires the two-way communication among the main grid, DC MG and the SCADA system, thus makes the total structure to a cyber-physical system. By introducing the communication channels with computerized control system, the functionality and the efficiency of the smart power network can be enhanced with dynamic demand management system. But this potentiality can introduce the security vulnerability to such cyber-physical system. Several types of cyber-attack [3] can take place in the DCMG based power network, such as:

- **Masquerading -** Attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for.
- **Message Replay Attacks -** Repeating the same outcome or making the constant image of a data.
- **Eavesdropping -** Capturing small packets from the network transmitted by other computers and analyzing those data searching for information.
- **False Data Injection Attack (FDIA) -** Attacker aims to attack and find any data as long as it can result in a wrong estimation for the state variables of a system.
- **Distributed Denial of Service (DDoS) -** Exhaust system resources by sending flood request to prevent legitimate user from accessing the system.
- **Privacy Leakage on Meters -** Utility usage information of the meter broadcast via wireless network can be hacked.
- **Malware and Software Flaws -** Inserting any malware or software, the system can be vulnerable.

In recent time, prognosticating the vulnerabilities in terms of security threats on the modern cyber-physical power, lots of researches are going on for detecting and managing the risk of cyber-attacks in the power systems. The work in [3] describes the security vulnerabilities of smart power system specially on the DC microgrid and discusses some possible forms of attacks such as Masquerading, Message Reply Attack, Eavesdropping, False Data Injection (FDI), Distributed Denial of Services (DDOS), privacy leakage on the smart meters. Beg et al. propose a method of FDI Attack (FDIA) detection technique in DC microgrid system [24]. In this work, the DCMG properties are referred from the Simulink/Stateflow to the Daikon tool, with the HYbrid iNvariant GEneratoR (Hynger) interface that infers the candidate invariance, and using the SpaceEx, the tool actual invariants are obtained. Any mismatch within those invariants indicates the presence of FDIA. They carried on their research [25] and proposed another FDIA detection technique using the Signal Temporal Logic (STL) that monitors the DC bus voltage and current of the DCMG against specified data. This work also detects the DDOS attack and provides a quantification of the attack impact demonstration for the whole system in a hardware-in-the-loop environment. To justify the efficiency of the literature based cyber-attack detection techniques, a realistic platform based on 13.8KV DC and hybrid microgrid security testbed has been proposed in [26]. The performance of the testbed has been evaluated from both software and hardware-based attack scenarios.

Very few works have been done on cyber-security issues considering the photovoltaic system-based power model. The work in [27] represents a cyber-attack risk assessment framework using the Markov Chain Process to provide the detection ability for the microgrid control system and analyze the monitory impact of cyber-attack using the Monte-Carlo approach. Another risk assessment framework has been developed in [28] for commercial photovoltaic plant in Spain called SOL-PV1 with 20MW capacity examining the vulnerabilities and the attack vectors of the PV grid and categorizes some unique features that will differ from system to systems in case of industrial control strategy. A probabilistic approach for quantifying the uncertainties in the solar PV farms using bootstrap Confidence Interval (BCI) has been proposed in [29] for the optimal management and successful integration of PV farms with the main grid. Isozaki et al. [30] focused on the effect of cyber-attack on voltage regulation at the distribution level when the PV system is connected. They developed an algorithm for detecting the attack through falsifying the measurement data of the sensor that enables the sectionalizing switches. The constraint of the work is that it performs effectively only for limited range of malfunctioned sensor data.

Among all the patterns of cyber-attack, considering the threat and their feasibility in practical arena, the most common form of attack considered for research is the False/Bad Data Injection where an intruder aims to attack any data as long as it can result in a wrong estimation for the state variables of a system, and Distributed Denial of Service that exhausts system resources by sending flood request to prevent legitimate user from accessing the system. As this is the emerging field of power research, most of the work till now explore in defining the possible adverse effects of cyber-attack at different points of power system [31], [32], [33], [34] and determining the detection technique of such kind of susceptibilities. For the FDIA, a data-driven approach to distinguish between cyber-attack and physical fault using Sequential Minimal Optimization (SMO) based support vector machine has been used in [35]. Different dynamic sate estimation based detection methods have been broadly discussed in several literatures using deep learning [36], Phasor Measurement Unit (PMU) data [37], Chi-Square method and Euclidean distance detector [38], Markov Model for determining the state space decision [39], Anomaly detection algorithm [40], and harmony search algorithm using the K-nearest neighbor (KNN) [41]. Some other techniques such as the Diagnostic Robust Generalized Potential (DRGP) technique [42], distributed block chain-based protection framework against DDOS attack through the communicating channel [43], Parametric Feedback Linearization (PFL) based control scheme for the delay minimization due to DDOS attack [44] show effective responses for the power grids.

1.2 Motivation

Based on the thorough literature search, all the works that have been carried out till now for the DC Microgrid system or any other power system can be categorize into three parts such as i) analyzing the risk and effect of cyber-attack on the power network from the technical point of view, ii) quantifying the economic impact of such kind of attack on the power system, and iii) detecting the cyber-attack on the power system. But very few works have been done in distinguishing the attack from the other disturbances and faults occurred in the power network. Specially in the DC microgrid concentration very few works are available. More importantly, different studies considered only the IEEE bus systems rather than modelling full-fledged microgrid platforms. Moreover, the mitigation technique of the instability caused by cyber-attack has not properly been studied yet.

1.3 Objectives of the Thesis

The overall goal of this thesis is to explore new and effective control means to mitigate the adverse effects of cyber-attacks on various components of the DCMG. To achieve these goals, this thesis proposes to conduct the following specific research.

- A DCMG model consisting of PV system, fuel cell, battery energy storage and PMSG based wind generator system has been developed.
- New solutions in the forms of non-linear controller as well as PI controller have been developed to alleviate the adverse effects of various cyber-attacks on the controller performance of the DCMG.

1.4 Novelty

The novelty of this work stands on the following facts.

- The cyber security issues and solutions for the DCMG have not been explored yet in detail for the DC Microgrid system.
- This work proposes new control means and solutions to mitigate the adverse effects of cyber-attacks on various components of the DCMG system.

1.5 Organization of the Thesis

The organization of the thesis is as follows.

- Chapter - 2 describes the DCMG system modelling for the analysis of the cyber security issues and solution techniques. It also provides detailed description on the proposed controllers.

- Chapter - 3 shows and describes the simulation results and represents the index-based performance evaluation measure for the proposed controllers.
- Chapter - 4 provides the conclusions for this work and proposes some future scope of it.

CHAPTER-2

DC MICROGRID SYSTEM DESCRIPTION AND CONTROL METHODOLOGY

From the concept of the DCMG system, it is clear that the presence of the communication infrastructure makes the whole system cyber-physical. This chapter describes the system modelling of the DC MG system and control, possible types of cyber threats, their impacts and also control methodologies that have been implemented for this research work.

2.1 Cyber Physical DC Microgrid Model

For the simulation, the system as shown in Fig. 8 has been considered, where there is a solar panel with the Maximum Power Point Tracking (MPPT) system that produces the duty cycle for the boost convert and provides power to the DC grid. A battery energy storage system (BESS) is also equipped to minimize the power fluctuation due to the temperature and the solar irradiation change. Moreover, a Fuel Cell (FC) connected with a DC-DC Converter, a Permanent Magnet Synchronous Machine (PMSG) based Wind Generation (WG) system equipped with a AC-DC inverter and a DC load are connected with the DC bus that consume 5.112MW of power at 400V. The power capacity of the PV, FC and WG are 3MW, 112.5KW and 2MW, respectively. The designed DC bus is connected with the main grid via an inverter through a switching mechanism that ensures the bidirectional power flow to and from the both grids. The whole DC microgrid is controlled and monitored through the centralized control system, i.e., the SCADA, in different layers. Cyber-attacks may happen at any points of the supervisory control. The different components of the DCMG system are explained below.

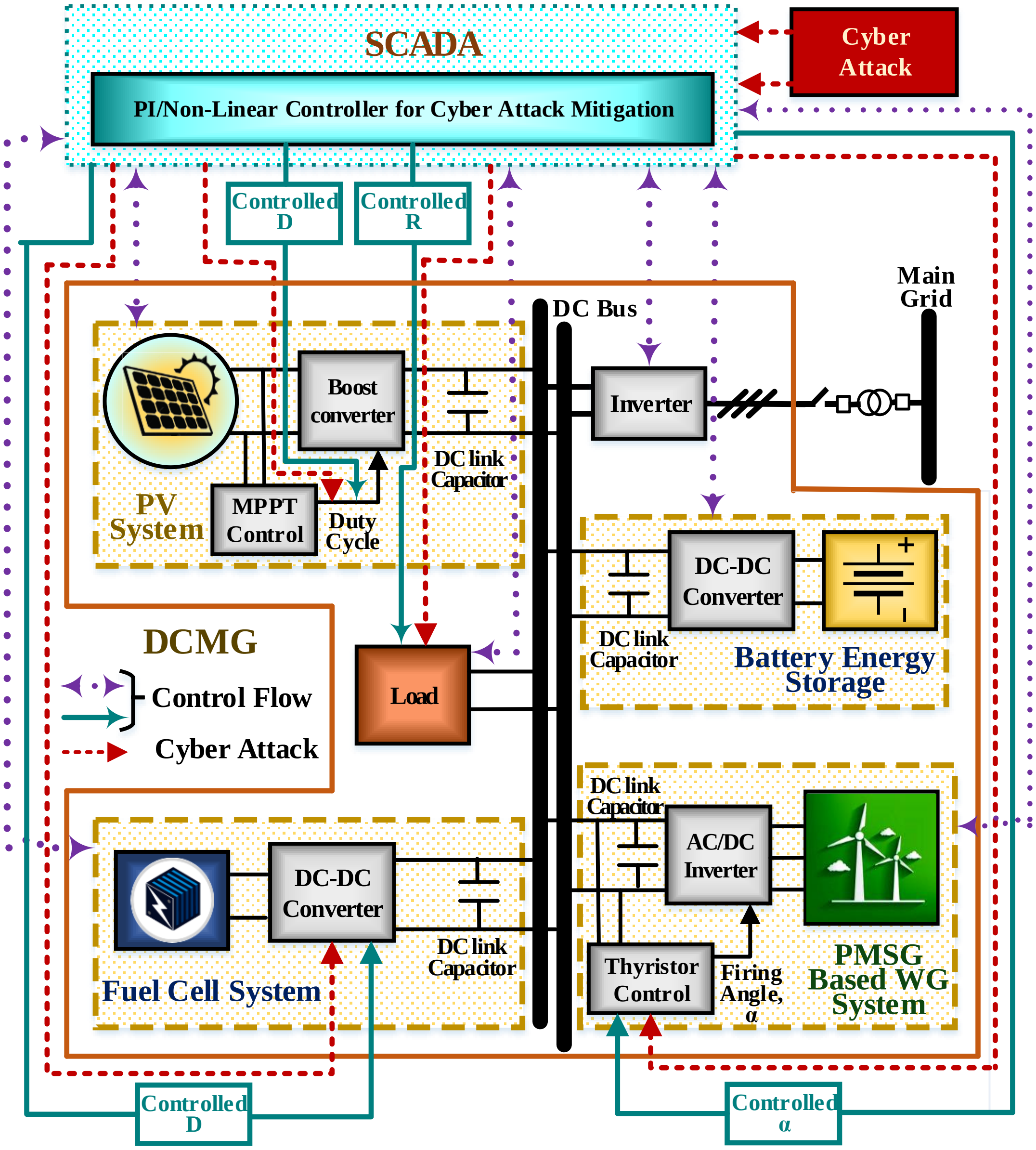


Fig. 8: DC microgrid system supervised by SCADA system.

PHOTOVOLTAIC (PV) SYSTEM:

Among many other renewable resources like hydro, geothermal, wind, biomass, etc., nowadays the solar system or more commonly known as the photovoltaic (PV) system has engrossed the considerable amount of attention of the power engineers [45], [46]. According to the US Department of Energy, the installation of solar power system has grown seventeen-fold from 1.2 gigawatts (GW) in 2008 to an estimated 30 GW today. This amount capacitates to deliver the power almost at 5.7 million regular American homes. Again, the cost of solar panels and the price of the solar power have been dropped by about 60% and 50%, respectively [47].

The photovoltaic system model used in this research is exemplified in Fig. 8, where the system consists of solar module that produces the Direct Current (DC) due to the solar irradiance penetration on the solar cell surface, a DC-DC boost converter to match up the voltage at the terminal of DC microgrid, the MPPT system to regulate the PV voltage and current as well as the power. The DC link capacitor is coupled before the DC bus.

Fig. 9 shows the equivalent circuit of individual PV cell that includes one diode, one shunt resistance, R_{sh} (with high value in KΩ range) representing the leakage current loss, and the series resistance, R_s (very small value) that represents the losses due to metallic contacts (grid contacts, current collecting bus, etc.).

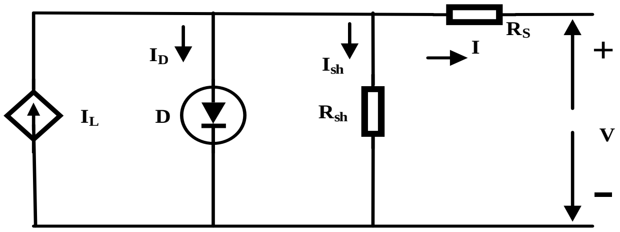


Fig. 9: Equivalent circuit of solar cell.

The current produced by the PV can be represented by the following equations [7], [31]:

$$I = I_L - I_D - I_{sh} \tag{1}$$

$$I_D = I_0 \left\{ exp \left[\frac{qV_D}{nkT} \right] - 1 \right\} \tag{2}$$

$$I = I_L - I_0 \left\{ exp \left[\frac{qV_D}{nkT} \right] - 1 \right\} - \frac{V_D}{R_{sh}} \tag{3}$$

where I_L is the photo generated current, I_D is the current across the diode, I_{sh} is the shunt current, I_0 is the reverse saturation current, n is the diode ideality factor (1 for an ideal diode), q is elementary charge, k is Boltzmann's constant ($1.38*10^{-23}$ J/K), T is absolute temperature, and V_D is the diode voltage.

The voltage produced at the terminal of the PV cell can be represented by:

$$V = V_D - IR_S \tag{4}$$

$$V = n\frac{kT}{q} ln\left(\frac{I_L - I}{I_0} + 1\right) - IR_S \tag{5}$$

As the power produced by the solar cell is very low, the series-parallel combination of the solar string helps achieve the desired power level. In this work, the

Helios USA 9T6 420W solar module has been used [48]. The 1800 parallel stings with 4 series strings are used to obtain the 3MW power at required 400V DC considering the solar irradiance and the temperature of 1000 W/m^2 and 25°C, respectively. The Perturb & Observe MPPT algorithm [49], which produces the duty cycle, D, for the DC-DC boost converter has been used. In this work, the optimal value of D is considered as 0.5 with the upper and lower bound at 0.58 and 0.38, respectively.

The DC link voltage V_{DC}, i.e., the voltage output of the boost converter is obtained depending upon the duty cycle, D, and the PV terminal voltage, V_{PV}, as represented by the following equation [45]:

$$V_{DC} = \frac{V_{PV}}{1 - D} \tag{6}$$

BATTERY ENERGY STORAGE SYSTEM (BESS):

The Battery Energy Storage System used in this work and shown in Fig. 10 comprises the battery, DC-DC Buck/Boost converter, and DC link Capacitor.

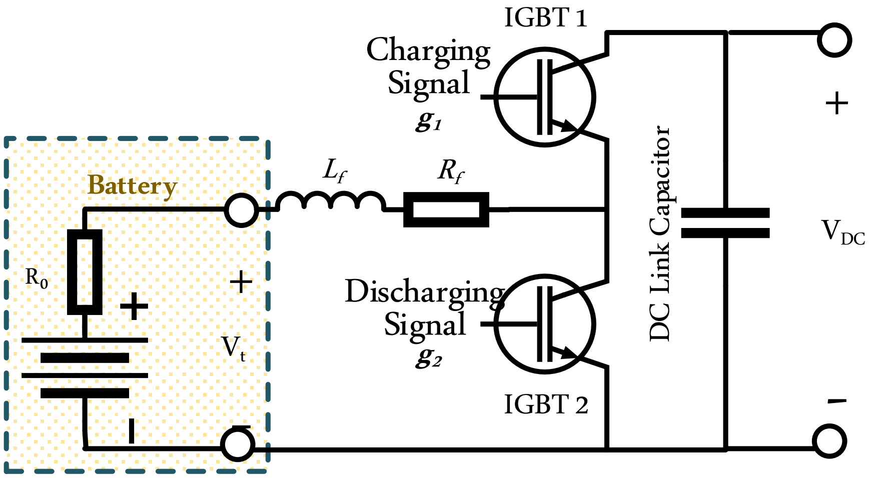


Fig. 10: Equivalent circuit of Battery Energy Storage System.

The output voltage of the battery is dependent upon the State of Charge (SOC) and has the following relationship:

$$V_t = V_0 \left[\frac{SOC}{1 - \beta(1 - SOC)} \right] \tag{7}$$

Where, V_0 is the voltage when the battery is fully charged at no load, as defined by the Nominal voltage parameter and β is the parameter that determines the charge and discharge characteristics of the battery.

The DC-DC Buck/Boost converter using the insulated-gate-bipolar-transistor (IGBT) switches has the main purpose to control the DC link voltage by properly charging and discharging the battery. In this BESS modelling, a proportional-Integral (PI) controller has been used to determine the switching frequency, the gate signal (g_1 and g_2) for the IGBTs depending upon the difference of load power and the generated power. When the load power is less than the generated one, the converter works in the boost mode, and when the load power is greater, then it switches to the buck mode. The operation of the BESS can successfully handle the impact of temperature and solar irradiance variation on the PV system and enhance the PV power quality as shown in Fig. 11. In this work, the battery energy storage system works for energy management purpose during the solar irradiance variation in the PV system.

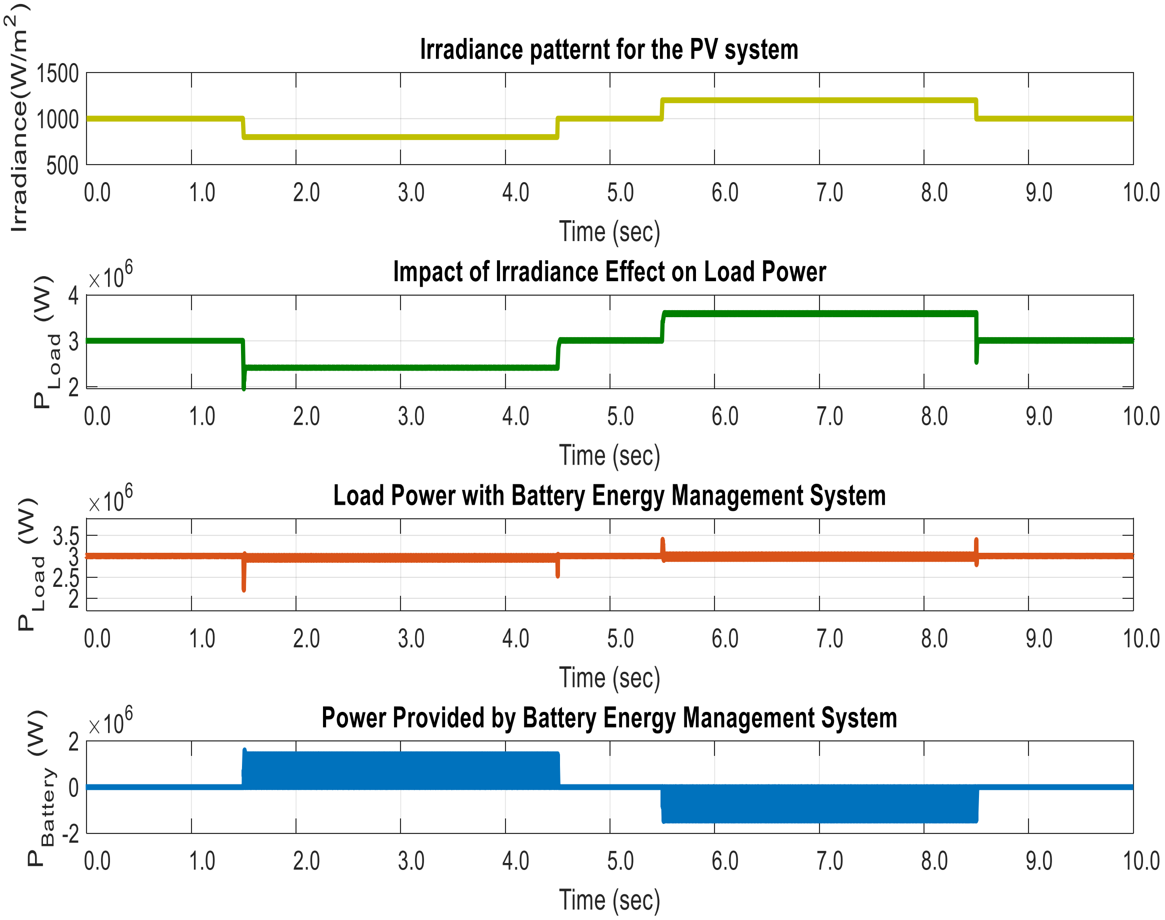


Fig. 11: Performance of Battery Energy Storage during solar irradiance variation.

FUEL CELL (FC):

Fuel cells are power generation devices that convert chemical energy directly into the electrical energy. In the basic construction of the fuel cell there are two electrodes named anode and cathode, an electrolyte substance that carries electrically charged particles from anode to cathode and also catalyst that speeds the reaction at the electrodes. Hydrogen is the main input for the fuel cell and this power generation process is very environment friendly as the byproduct of this chemical reaction is only the water. There are different kinds of Fuel cell, the most commons are proton exchange membrane fuel cell (PEMFC), direct methanol fuel cell (DMFC), alkaline fuel cell (AFC), phosphoric acid fuel cell (PAFC), molten carbonate fuel cell (MCFC) and solid oxide fuel cells (SOFC) [50], [51], [52]. In this research work, the PEMFC has been used. Though the working principle of the FC varies for different types, but the basic is to ionizing the hydrogen atom at the anode then allowing the electrons to pass through the cathode that completes a full path thus produces direct current (DC) [53]. And the protons are passed through the electrolyte mix up with the oxygen of the air and produces water. In Fig. 12, the basic operation of the fuel cell has been shown. Here the electrolyte plays the important role as they control the right path for electrons and protons and permit the electrons only to flow toward the cathode. Though the fuel cells are the environment friendly source of power, but it is highly expensive due to cost of hydrogen as well as the electrolyte. Moreover, it produces a good amount of heat when the hydrogen gets ionized.

PMSG BASED WIND POWER SYSTEM:

The basic principle of the wind power system is to convert the wind energy into mechanical energy by rotating the turbine with force of the wind and finally this rotation of turbine produces the electrical energy. The power captured by the wind turbine can be expressed as [54],

$$P_m = \frac{1}{2}\rho\pi R^2 {V_w}^3 C_p(\lambda, \beta) \tag{8}$$

Where,

P_m : extracted power from wind [W]

P : air density [kg/m3]

R : blade radius [m]

V_w : wind velocity [m/s]

λ : tip speed ratio

β : blade pitch angle [deg]

C_p : power coefficient which is a function of both λ and β.

In this work, the Type-4 wind turbine [55] i.e., the permanent magnet synchronous generator type variable speed wind power system has been used. The main reason of using the PMSG is to avoid the separate excitation system for the field and the power electronic inverter/converter system allows the variable speed of the wind, and thus the maximum wind power can be captured. As the power production from a wind turbine is a function of wind speed, most wind turbines begin to produce power at wind speeds of about 4 m/s (9 mph), achieve rated power at approximately 13 m/s (29 mph), and stop power production at 25 m/s (56 mph). There is a pitch control system in WG system that usually maintains the pitch angle to uphold a constant output power at the terminal of the generator when the wind speed is over the rated speed. In this work, a constant wind speed of 15m/s has been considered and the system generates 2MW of power.

2.2 Possible Cyber Threats

As shown in Fig. 8, the DC microgrid is connected with the main grid system and the total cyber physical system is being monitored by the SCADA system in different layers. The SCADA is a kind of centralized control system architecture for any power grid that stores, monitors and process all the data available to the power network. SCADA includes the usage of computers, programmable logic controllers, data communication channels, graphical user interface (GUI) system, high level of network observatory system, etc. As all the controller set points are handled through the SCADA, it is possible to tamper any kinds of data from there or destroy the interface with the grid that may result in an unexpected unbalanced situation. For example, an intruder can change the value of duty cycle, which is the input to the boost converter of the PV system, abruptly to any value. The information of duty cycle can be missing from the boost converter. Again, an attacker can attack on the load profile that will cause the change in the load value at the SCADA, whereas the physical load value will remain unchanged. In all of these cases, the physical system will receive misleading information from the SCADA and will result in deviation of PV array terminal voltage, the voltage and power at the DC microgrid terminal.

Moreover, since every controller has some reference values, an intruder can easily change that set point, and thus can hamper the performance of the controller. For example, in the battery energy storage system, an intruder can change the reference value of the power. In that case, the controller will not be able to provide the optimum power required for the system at that moment, and that will hamper the performance of the power system, and also the consumers will be affected with the high or low voltage causing from the variable nature of the solar or wind. If such situation continues for longer time, the equipment attached to the power system will be damaged and the whole system may be shut down.

DISTINGUISHING CYBER ATTACKS FROM OTHER DISTURBANCES:

As already mentioned, to consider the cyber-attack scenario, in this work four parameters have been chosen, i.e., the duty cycle of the DC-DC boost converter of the photovoltaic system, reference value of the firing-angle controller of the AC-DC inverter of the PMSG based variable speed wind power generation system, reference value of the battery energy management system controller and load profile. All these quantities are independent of the fault or any other transient instability scenario in the grid. The duty cycle usually varies with the change in solar irradiance and the temperature in case of the PV system or with the fuel cell dynamic in case of the FC system. This type of variation is time dependent and does not change instantly or abruptly. Again, during a faulty condition, the reference values of the controller never be changed, it only happens if somebody manipulate those values intentionally. Similarly, in case of load, its value never varies with the fault. The only parameters that can vary are the voltage that may go very low and the current that may become very high. The value of the load may vary with respect to the demand throughout the day, but this will not happen abruptly or enormously, as load profile is always maintained and monitored according to the grid code by the SCADA. Whereas in case of FDI cyber-attack, the parameters can be changed to very sudden and unusual values, or in case of DDoS attack, due to the flood of data suddenly some delayed response may occur. Therefore, by recognizing the pattern of the duty cycle and load profile at the SCADA, the cyber-attack scenarios can possibly be recognized. In this work, the main concentration is to show the cyber-attack mitigation effects using the proposed controllers.

2.3 Proposed Control Methodology

PROPOSED CONTROLLERS FOR MITIGATION OF ADVERSE EFFECTS OF CYBER-ATTACKS:

In this work, two types of controllers, such as a simple non-linear controller and the PI controller have been used to mitigate the adverse effects of cyber-attacks on the PV system performance. The control algorithm and the controller description are provided in the following.

A. Control Algorithm:

All kinds of vulnerabilities in a power system have direct impact on the terminal voltage. So, the main objective is to regain the voltage at its required level within the shortest possible time. Thus, the DC link voltage, VDC, has been used as the controller input. This voltage is compared with the reference voltage of VDC (400V) to get the error function ΔVDC. These voltage values are converted into per unit quantities with the base value of 400V. Fig. 12 Shows the basic algorithm of the proposed cyber-attack mitigation techniques.

In case of normal situation, the error value is zero. The controller continuously monitors the voltage deviation at the DC bus. In case of any deviation in ΔV_{DC}, the controller will first check whether there is any cyber-attack in the system or any other disturbances. In that case, all the set point values will be checked. If the set point values are unchanged, then the system will detect other disturbances and accordingly suitable controller will be activated. But if any of the set point value is changed, then the cyber-attack will be detected. In this work, as the focus is to mitigate the cyber-attack effect, the controller will check for the location of the cyber-attack depending upon the manipulated parameter. This can be detected by monitoring the performances of the individual distributed energy resources (DER), because the cyber-attack impact will be higher on that specific DER where the attack has occurred. Again, if there is any deviation in load value, R, then the controller for the R value correction will be enabled and will ensure the voltage deviation at zero. When the system will be stable, the controller will get disconnected immediately and the system will resume its original connections.

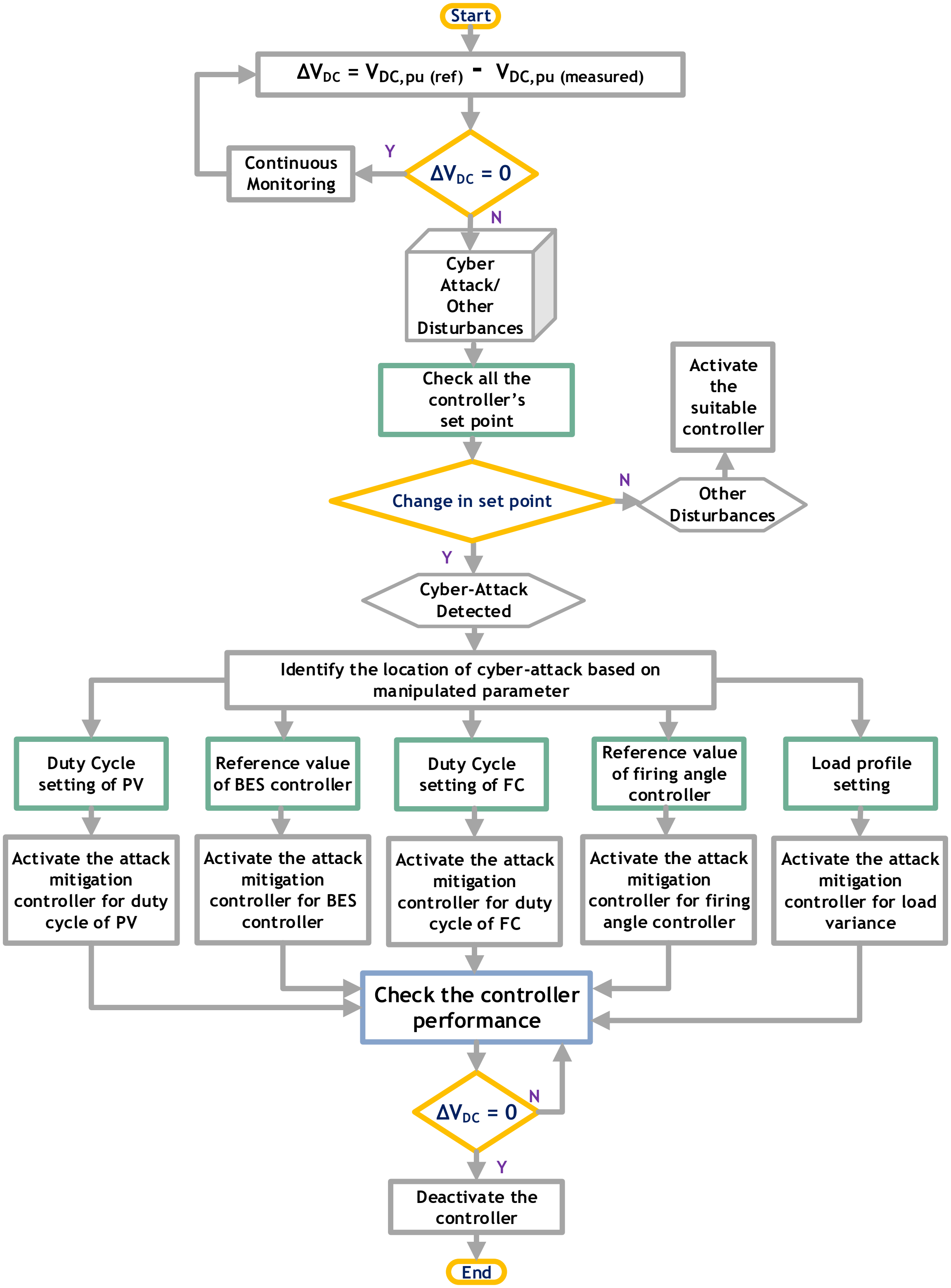

Start
ΔV_DC = V_DC,pu (ref) - V_DC,pu (measured)
ΔV_DC = 0
Y
Continuous Monitoring
N
Cyber Attack/ Other Disturbances
Check all the controller's set point
Activate the suitable controller
Change in set point
N
Other Disturbances
Y
Cyber-Attack Detected
Identify the location of cyber-attack based on manipulated parameter
Duty Cycle setting of PV
Reference value of BES controller
Duty Cycle setting of FC
Reference value of firing angle controller
Load profile setting
Activate the attack mitigation controller for duty cycle of PV
Activate the attack mitigation controller for BES controller
Activate the attack mitigation controller for duty cycle of FC
Activate the attack mitigation controller for firing angle controller
Activate the attack mitigation controller for load variance
Check the controller performance
ΔV_DC = 0
N
Y
Deactivate the controller
End

Fig. 12: Proposed control algorithm.

It is to be noted here that, the controller will be secured in a black box/ hidden box that will generally remain out of data cloud of the SCADA so that no intruder effect can hamper this controller. This will come into action only when it is required for a short period of time, suppose for 2-3 seconds, and once the system comes back, the controller will again be disconnected and out of the communication channel. This very small action time of the controller will not be enough for the intruder to understand the control system and thus the controller will be secure.

B. Non-linear Controller

As the power grid is highly non-linear, application of non-linear controllers in power grid is highly preferred. This control action can be governed by any nonlinear differential equations or any other mathematical model. In this work, two simple exponential equations have been used as the nonlinear function shown in the following:

$$1 - K_2 e^{-|\Delta V_{DC}|K_1} \tag{9}$$

$$K_2 e^{-|\Delta V_{DC}|K_1} \tag{10}$$

$$K_2 e^{-|\Delta P_{Load}|K_1} \tag{11}$$

Where K_1 and K_2 are the constant values and ΔV_{DC} is the input to the controller. By tuning the values of K_1 and K_2, the required controller values of the manipulated signal are obtained. Equation 9 is used for the cyber-attack mitigation in case of load and the duty cycle, D, in case of PV and FC with different values of K_1 and K_2. Similarly, equation 10 is used for regaining the reference values of the AC-DC converter in case of the WG system and equation 11 is for the battery energy management system. The parameters have been set in a way so that the controller can handle any kind of voltage deviation from very high to very low. The parameters of the controller have been shown in TABLE 2.

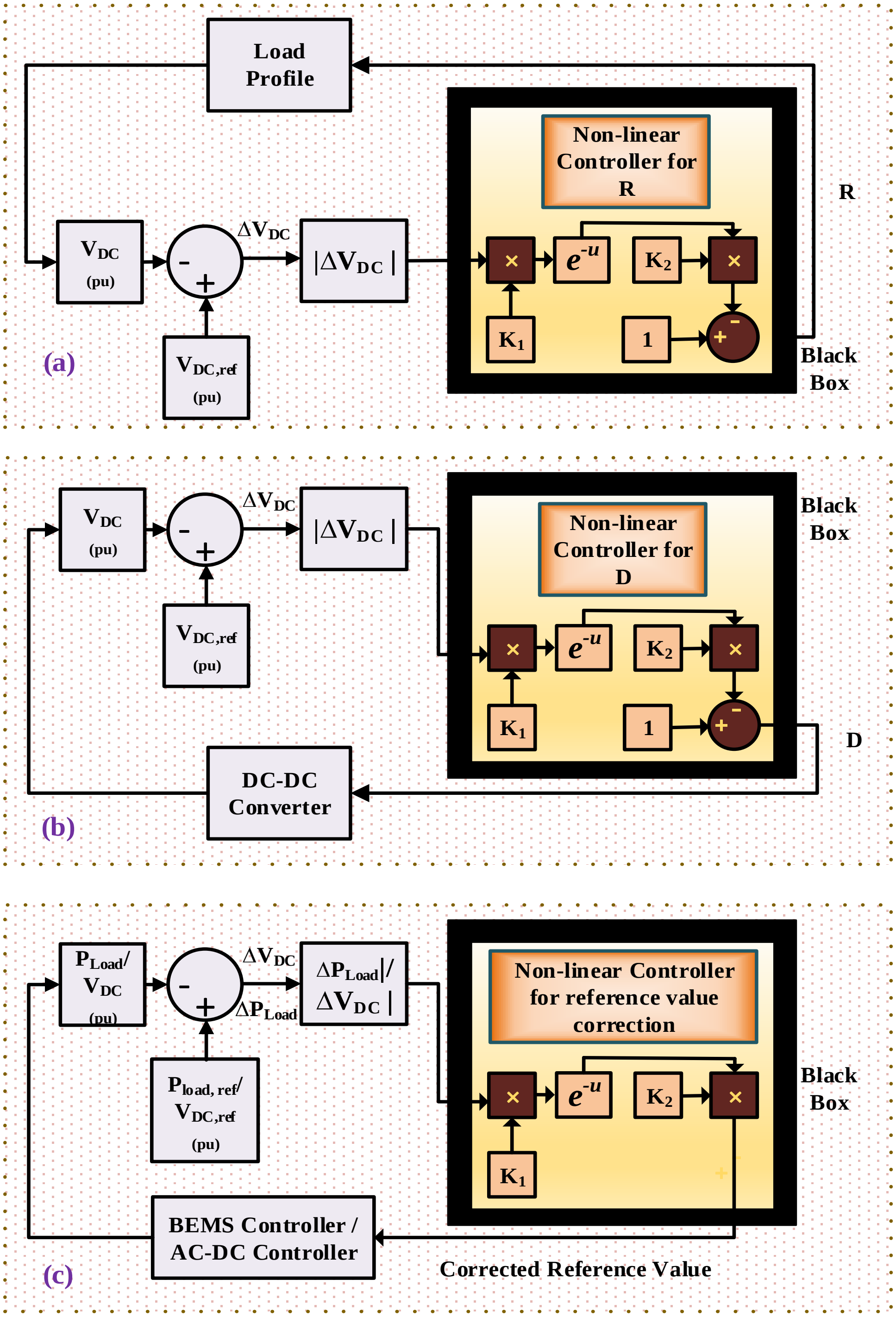


Fig. 13: Proposed Non-linear controller.

Fig. 13 represents the block diagram of the nonlinear controller. One controller is for the duty cycle correction that can handle both the FDI and DDOS attacks with the same parameter value, and another one is for the load correction.

C. Proportion-Integral (PI) Controller

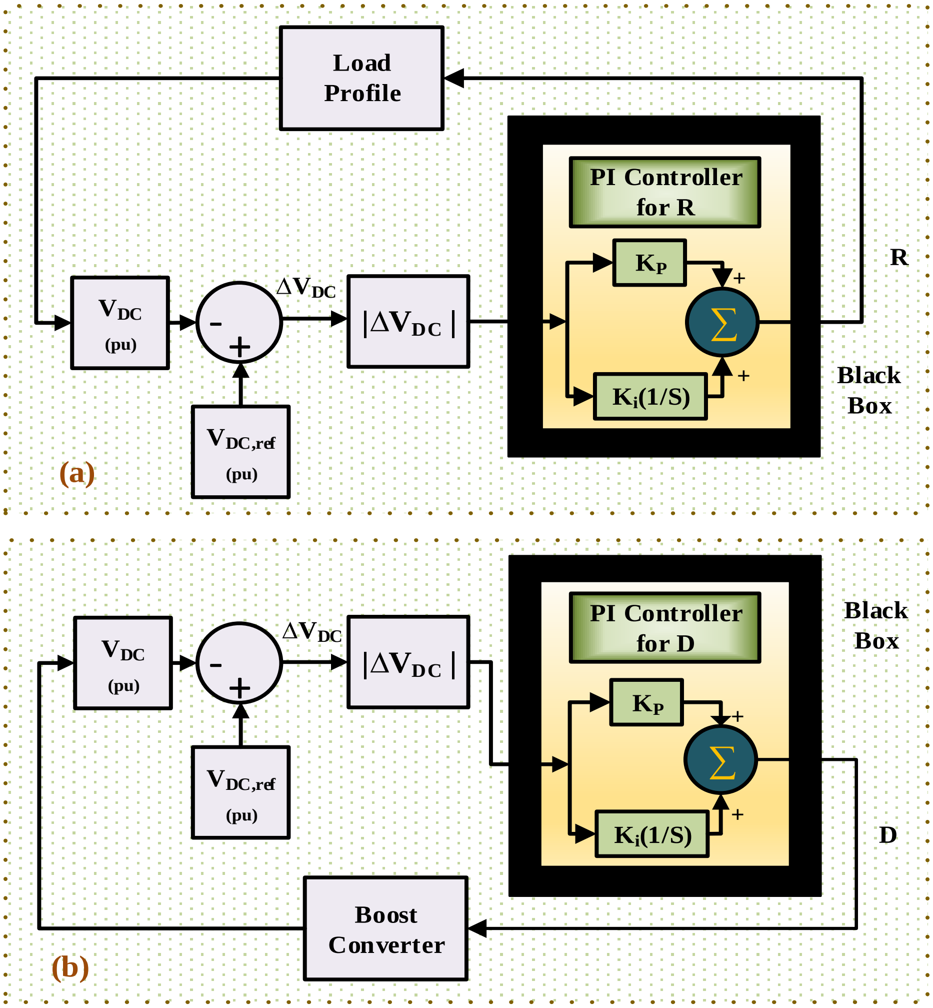


Fig. 14. Proposed PI controller.

The PI controller is one of the popular controllers that is being extensively used in industrial control. Fig. 14 shows the block diagram for the PI controller. This also works the same way as the nonlinear controller in two parts for duty cycle and load variation.

The transfer function that has been used for the PI controller in Laplace domain (s) is as follows:

$$D = |\Delta V_{DC}| \left[K_p + \frac{1}{s} K_i \right] \tag{12}$$

Where K_p and K_i are the proportional and integral gain of the PI controller, respectively. ΔV_{DC} and D are the input and output variable of the controller, respectively, and bear the same meaning as mentioned in the previous subsection. The values of the parameters K_p and K_i are shown in TABLE 2, in the next page. These values have been obtained by trial and error and it can handle any abrupt change in the input from high to low.

The attack scenario cases mentioned in the following table are described in the Table-3 in Chapter-3.

TABLE 2. PARAMETER VALUES OF THE CONTROLLER FOR CYBER-ATTACK

Attack Scenerio	Attack Point	Non-linear Controller		PI Controller	
		K_1	K_2	K_p	K_i
Case -I	D of PV	0.735	0.5	0.9972	0.896
Case-II	R	0.0215	0.9468	0.34	0.09
Case-III	D of PV	0.735	0.5	-	-
	R	0.0215	0.9468	-	-
Case-IV	P_{ref}	0.0735	$3e^6$	-	-
Case-V	D of FC	0.735	0.36	-	-
Case-VI	V_{ref}	0.0735	400	-	-

2.4 Conclusion

This chapter describes the modelling of the DC Microgrid system used for the analysis of the cyber security issues and solution techniques. It also explains the cyber security threats towards the power system, especially in PV connected DC Microgrid system. And finally, this chapter provides detailed description on the proposed controllers along with parameter values.

CHAPTER-3

EFFECTIVENESS TESTING OF PROPOSED CONTROLLERS FOR MITIGATING ADVERSE EFFECTS OF CYBER-ATTACKS

In this chapter, the effectiveness of the proposed controller in the DC microgrid system has been evaluated. The evaluation has been shown through some graphical images obtained from the real time simulation and also mathematically by calculating the percentage improvement from the voltage index value. The details are described in the following subsections.

3.1 Simulation Condition

The simulations are performed through the MATLAB/Simulink Software. In the simulation study, constant irradiance and temperature in case of PV system and constant wind speed in case of wind power system have been considered. Since these parameters vary gradually with time and any cyber-attack may happen within few seconds, these changes will not impact much. In all cyber-attack cases, the mitigation controller has been activated after 0.1 sec of the occurrence of attack. This 0.1sec time has been considered as time delay to allow the sensor to choose the right type of controller based on the location of attack to mitigate the adverse effects of cyber-attacks. The time step of the simulation is 5µsec for all cases.

The scenarios that have been considered in this work are briefly listed in the following table based on the pattern, type and location of the attack.

Table 3. CYBER-ATTACK SCENARIO

Case of study	***Scenario***	***Pattern of Attack***	***Type of Attack***	***Location of Attack***
Case-I Attack on Photovoltaic System	1	Single Attack	FDI	Duty Cycle of the PV Boost Converter
	2		DDoS	
	3	Random Attack	FDI	
	4	Repetitive Attack	DDoS	
	5		FDI	
Case-II Attack on Load Profile	1	Single Attack	FDI	Load Profile
	2	Repetitive Attack		
Case-III Simultaneous Attack	1	Single Attack	FDI	Duty Cycle of the PV Boost Converter and Load Profile simultaneously
	2	Repetitive Attack		Duty Cycle of the PV Boost Converter and Load Profile simultaneously
Case-IV Attack on Battery Energy Storage (BES)	1	Single Attack	FDI	Reference value of the BES control scheme
Case-V Attack on Fuel Cell System	1	Single Attack	FDI	Duty Cycle of the DC-DC Converter of the Fuel Cell
Case-VI Attack on PMSG based Wind Power System	1	Single Attack	FDI	Reference value of the Firing angle (Alpha value) controller of the AC-DC converter in WG system

3.2 Cyber Security Issues and Solution for DC Microgrid System

3.2.1 Cyber Attack on PV System

A. CASE-I; SCENARIO-1

Effects and Solution of FDI Attack on Duty Cycle of The PV Boost Converter:

In case of the false data injection attack scenario, it has been considered that, at 0.5 sec of simulation, the intruder attacks on the duty cycle at the input of the DC-DC boost converter. Figs. 15-18 show the responses of four parameters, such as the duty cycle, PV array voltage, DC grid Voltage, and output power respectively. As shown from the responses, the duty cycle increases to its 90% value which is a very high value as it's range typically varies from 0-1 only. Also, the terminal voltage of the PV array goes close to zero, and the DC grid voltage and the power at the grid become very low.

In that situation, to recover the steadiness of the grid, the controller has been activated at 0.6 sec. For the PI controller case, the duty cycle comes back to 0.5 value within almost 6 sec. Comparing to that in case of the nonlinear controller the duty cycle comes back at the desired value immediately within 1 sec. As the D value is recovered, both the voltages at the terminal of PV array and the DC grid gradually come back to the 400V level. Following the voltage, the output power is also improved. It is quite certain that in all four cases the performance of the nonlinear controller is much better that that of PI controller.

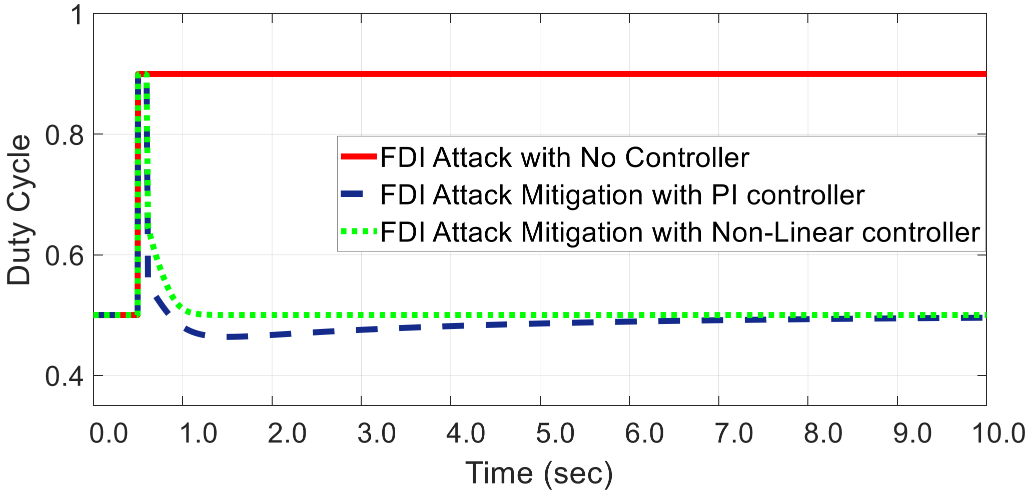


Fig. 15: False Data Injection (FDI) attack on duty cycle of the PV boost converter scenario and mitigation effect on the duty cycle.

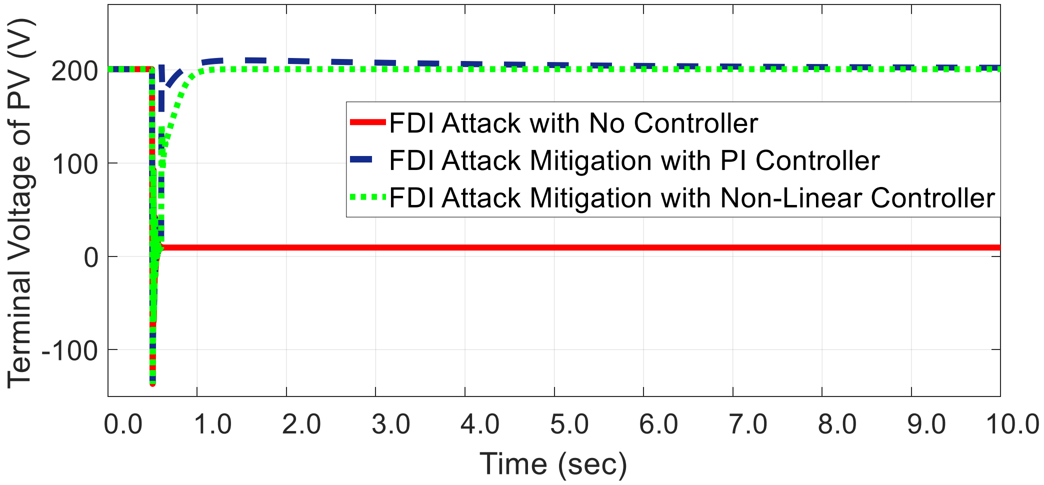


Fig. 16: False Data Injection (FDI) attack on duty cycle of the PV boost converter scenario and mitigation effect on the PV array terminal voltage.

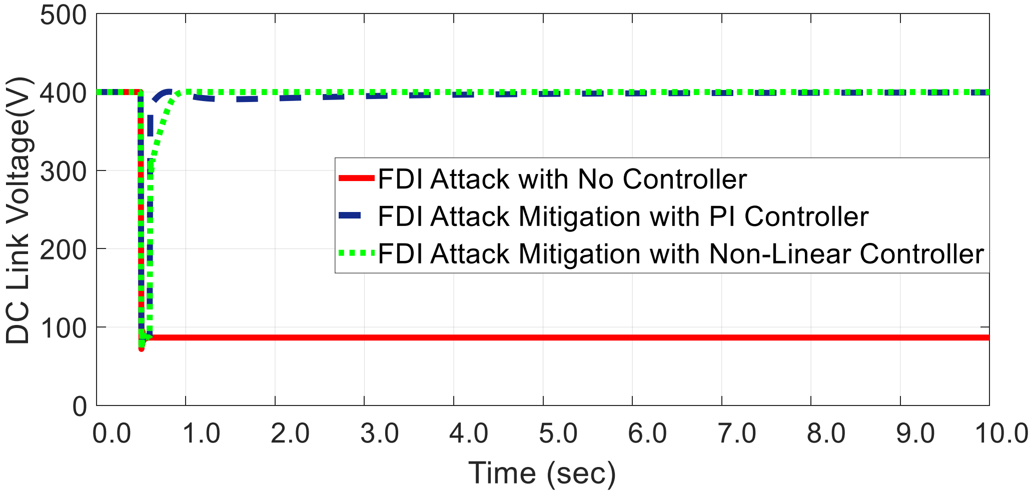


Fig. 17: False Data Injection (FDI) attack on duty cycle of the PV boost converter scenario and mitigation effect on the DC microgrid terminal voltage.

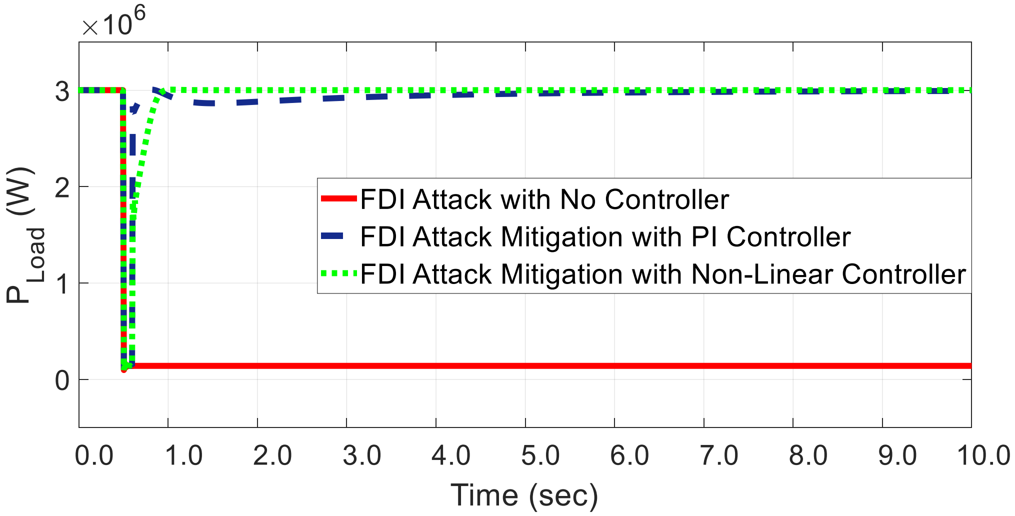


Fig. 18: False Data Injection (FDI) attack on duty cycle of the PV boost converter scenario and mitigation effect on the Power at DC microgrid.

B. CASE-I; SCENARIO-2

Effects and Solution of DDOS Attack on Duty Cycle of the PV Boost Converter:

The DDoS is another very frequent type of cyber-attack. It causes flood data that prohibits the normal data flow through the communication channel. So, the system will get no signal for few moments or longer period of time. In the case of the DDoS attack, the scenario has been simulated such as the intruder attacks the duty cycle by making it zero in the boost converter input at 0.5sec. Figs. 19-22 show the responses of the duty cycle, voltage at both the terminal of PV array and the DC grid, and the load power, respectively. From these figures, it is clear that the sudden absence of duty cycle in the DC-DC Boost converter makes the system vulnerable. To handle such situation, the controller has been activated at 0.6sec, and both the controllers attempt to make the duty cycle value at 0.5 at the terminal of boost converter. From the results it is visible that the performance of the non-linear controller and the PI controller is significantly different. For every case, the non-linear controller performs almost instantly after the activation and helps the duty cycle and DC grid voltage come back instantly at their rated values of 0.5 and 400V, respectively. But in case of PI controller, the duty cycle value restored almost after 7 secs, and the PV array voltage took long time to get stable, although the DC grid terminal voltage and the output power came back after 5 seconds.

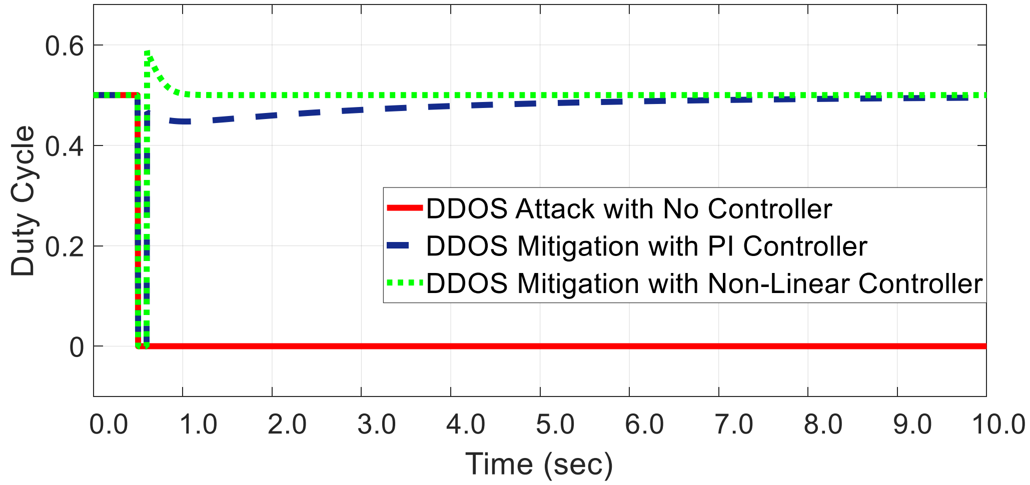


Fig. 19: Distributed Denial of Service (DDoS) attack on duty cycle of the PV boost converter scenario and mitigation effect on the duty cycle.

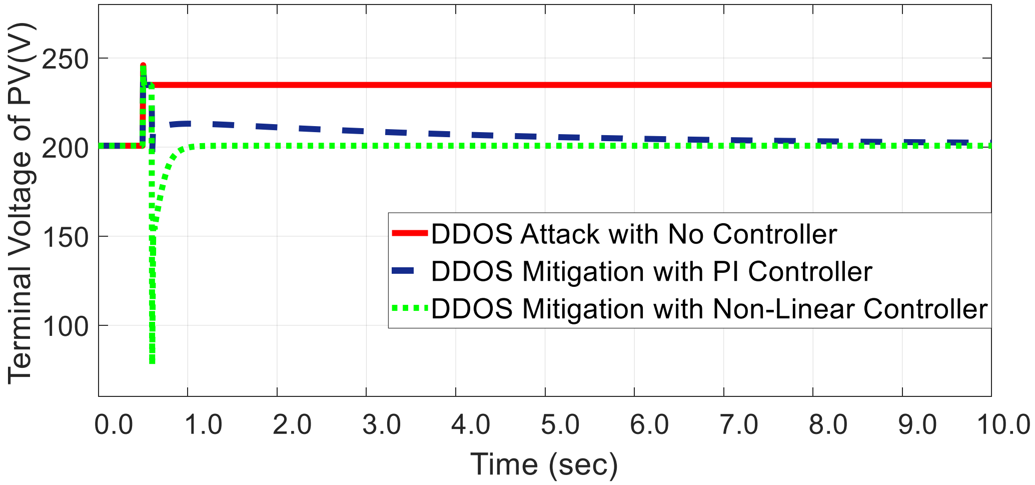


Fig. 20: Distributed Denial of Service (DDoS) attack on duty cycle of the PV boost converter scenario and mitigation effect on the PV array terminal voltage.

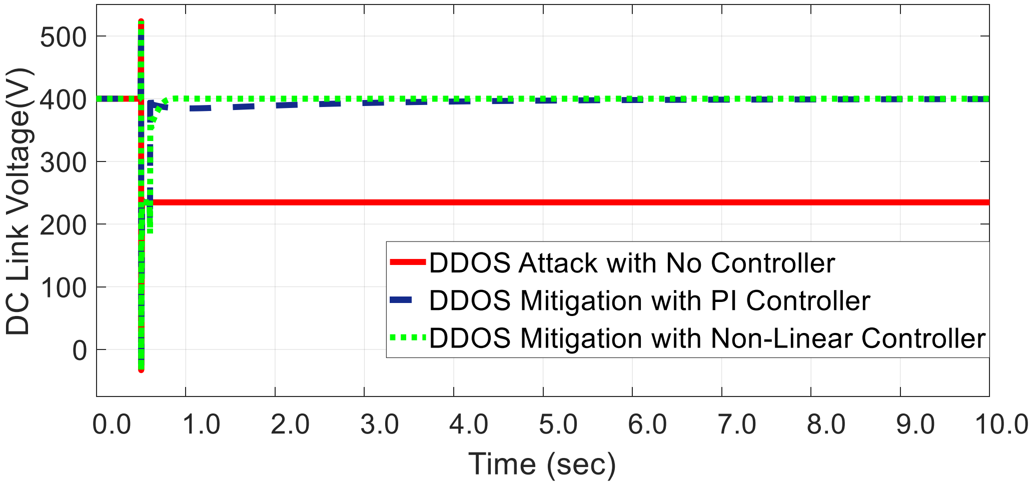


Fig. 21: Distributed Denial of Service (DDoS) attack on duty cycle of the PV boost converter scenario and mitigation effect on the DC microgrid terminal voltage.

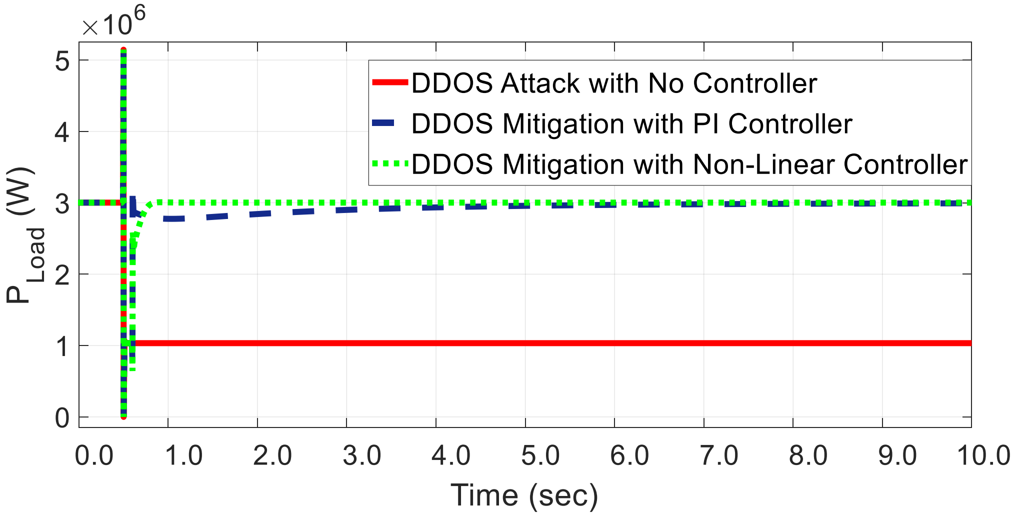


Fig. 22: Distributed Denial of Service (DDoS) attack on duty cycle of the PV boost converter scenario and mitigation effect on the Power at DC microgrid.

C. CASE-I; SCENARIO-3

Effects and Solution of Random FDI Attack on Duty Cycle of the PV Boost Converter:

In case of the random false data injection attack scenario, it has been considered that, at 0.5 sec of simulation the intruder attacks with random change in value of the duty cycle at the input of the DC-DC boost converter of the PV system. Figs. 23-26 show the responses of four parameters, such as the duty cycle, PV array voltage, DC grid Voltage, and output power. As shown from the responses, the duty cycle varies randomly within 10-90% value. Also, the terminal voltage of the PV array, the DC grid voltage and the power at the grid varies randomly from very low to high values in an inversely proportional manner with the duty cycle change.

In that situation, to recover the stability of the grid, the controller has been activated at 0.6 sec. For the PI controller case, the duty cycle comes back to 0.5 value within almost 6 sec. Comparing to that in case of the nonlinear (N-L) controller the duty cycle comes back at the desired value immediately within 1 sec. As the D value is recovered, both the voltages at the terminal of PV array and the DC grid gradually come back to the 400V level. Following the voltage, the output power is also improved. It is quite certain that in all four cases the performance of the nonlinear (N-L) controller is much better that that of PI controller. This proves the robustness of the controllers, that means they can handle any abrupt changes properly within very short period time.

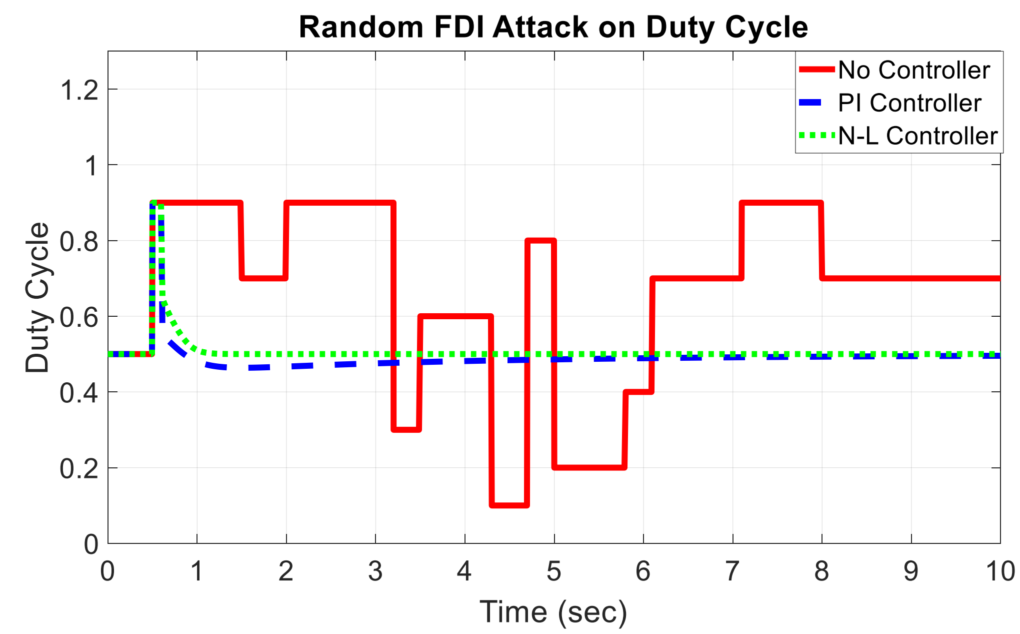


Fig. 23: Random FDI attack on duty cycle of the PV boost converter scenario and mitigation effect on the duty cycle.

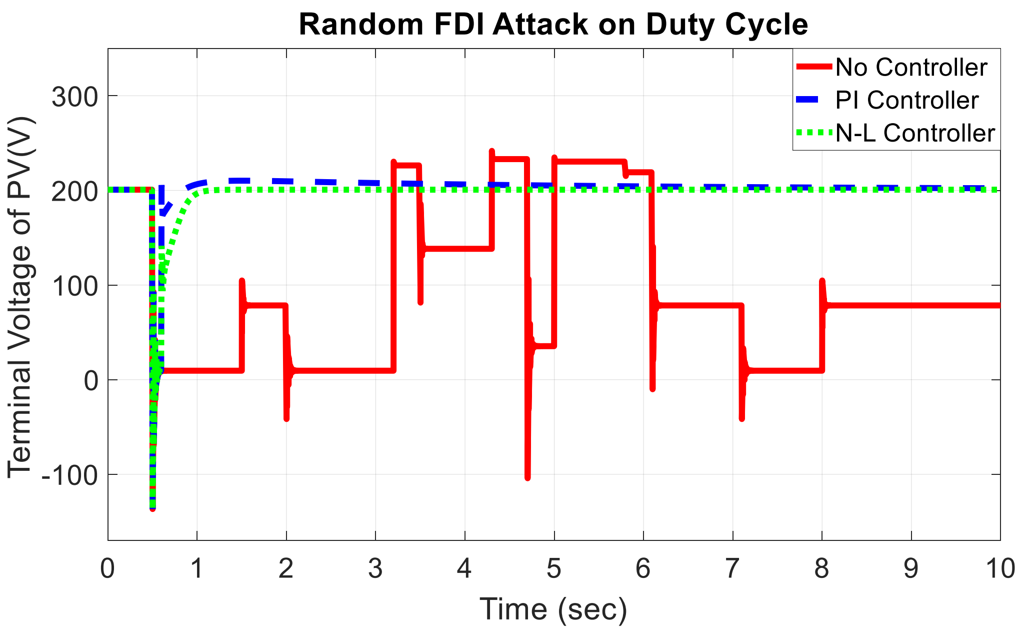


Fig. 24: Random FDI attack on duty cycle of the PV boost converter scenario and mitigation effect on the terminal voltage of PV array.

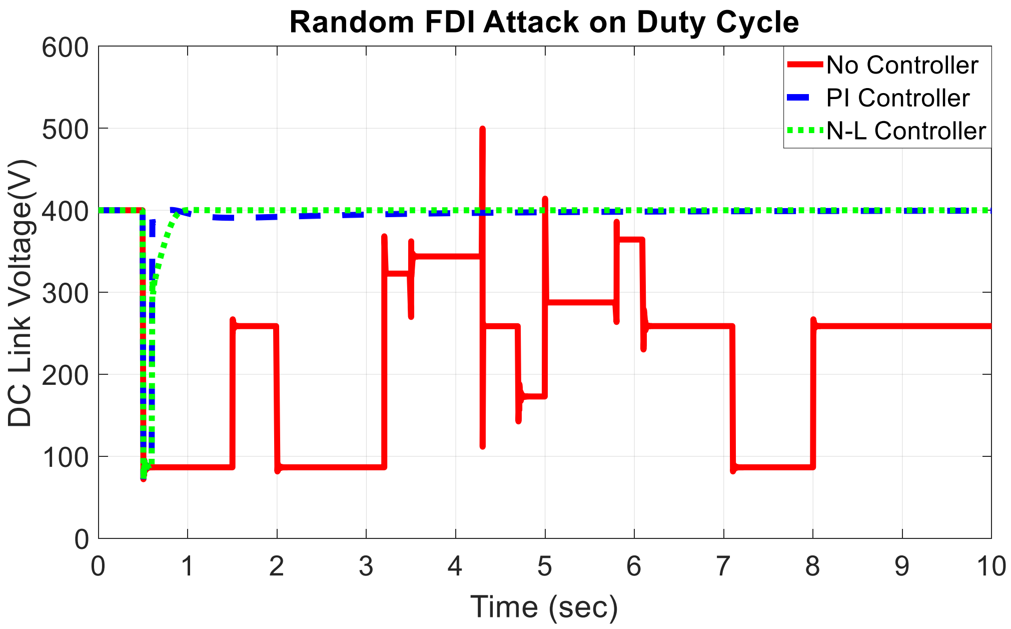


Fig. 25: Random FDI attack on duty cycle of the PV boost converter scenario and mitigation effect on the voltage at DC link.

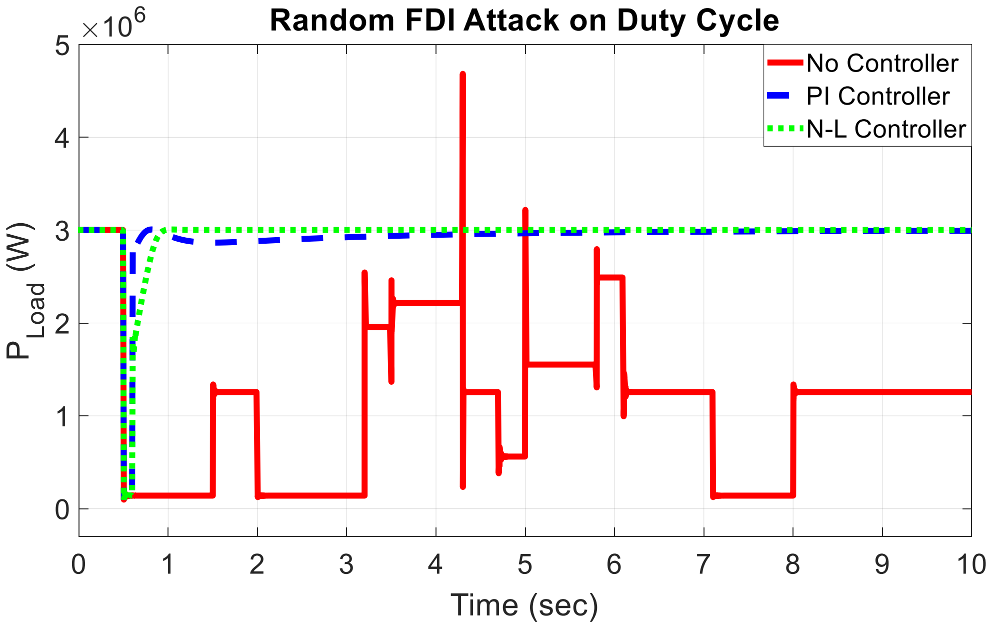


Fig. 26: Random FDI attack on duty cycle of the PV boost converter scenario and mitigation effect on the load power.

D. CASE-I; SCENARIO-4

Repeated Attack

Till now the cyber-attacks that occurs once in a system have been discussed. Now the aim is to explore more worst scenarios by imposing the repetitive attack. That means, once an attack has been mitigated, another attack will affect the system one more time. It may continue for a longer time so that the whole power system may exhaust and fail. This can be considered as one of the severest case of cyber-attacks.

In this situation, the aim is to control such repetitive attack scenario using controller. As from the above cases, both single attack and random attack, it is clearly visible that the non-linear controller outperforms the PI controller. For that reason, in the following works, only the non-linear controller for the cyber-attack mitigation purpose has been considered.

Effects and Solution of Repeated DDoS Attack on Duty Cycle of The PV Boost Converter:

In the case of the repeated DDoS attack, the scenario has been simulated such as the intruder attacks the duty cycle by making it zero in the boost converter input at 0.5sec. After one second (1.5 sec) the attack has been removed, but again after two seconds (3.5 sec), the intruder imposes the manipulation for one more second and the attacker follows the similar pattern of repeated DDoS attack for rest of the time. Figs. 27-30 show the responses of the duty cycle, voltage at both the terminal of PV array and the DC grid, and the load power, respectively. From these figures, it is clear that sudden absence of duty cycle in the DC-DC Boost converter makes the system vulnerable. To handle such situation, in each time of attack the controller has been activated after 0.1 sec of attack time considering the delay and when the intruder removes the attack, the controller again gets deactivated ensuring the stability. Suppose, for the 1st attempt, the attack happens at 0.5 sec and the controller gets activated at 0.6sec. The non-linear controller attempts to make the duty cycle value at 0.5 at the terminal of boost converter. From the results it is clear that the non-linear controller performs rapidly and within 0.3sec the optimal value is regained in all of the cases.

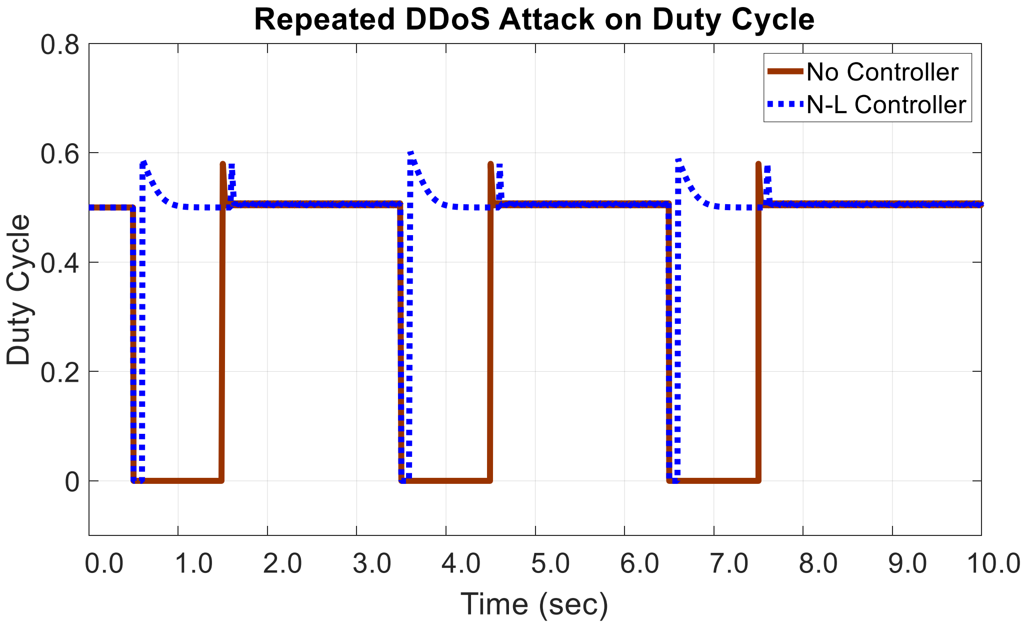


Fig. 27: Repeated DDoS attack on duty cycle of the PV boost converter scenario and mitigation effect on the duty cycle.

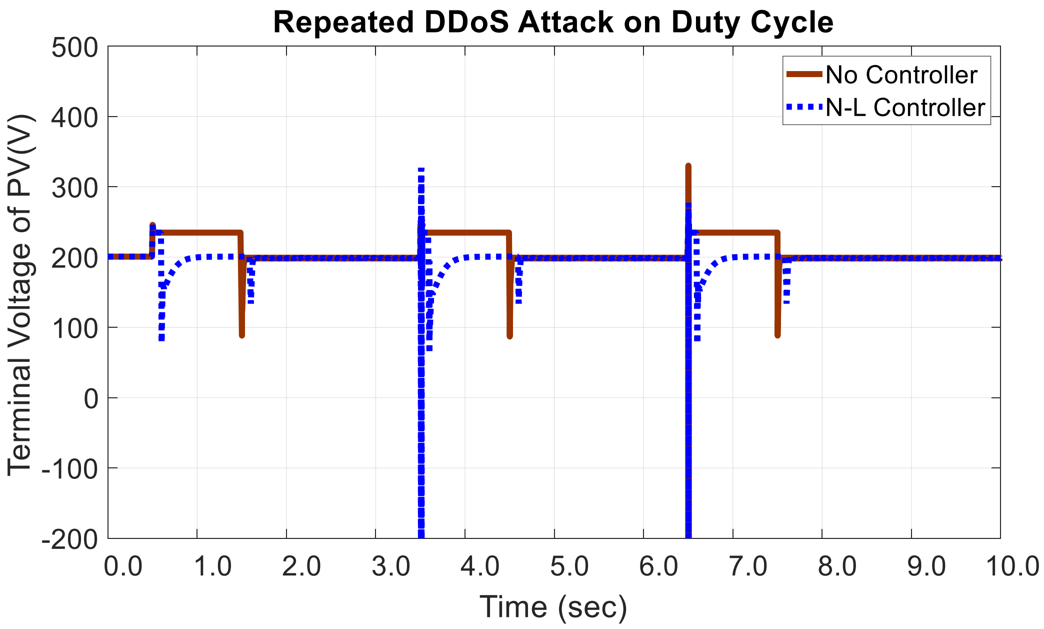


Fig. 28: Repeated DDoS attack on duty cycle of the PV boost converter scenario and mitigation effect on the PV array terminal voltage.

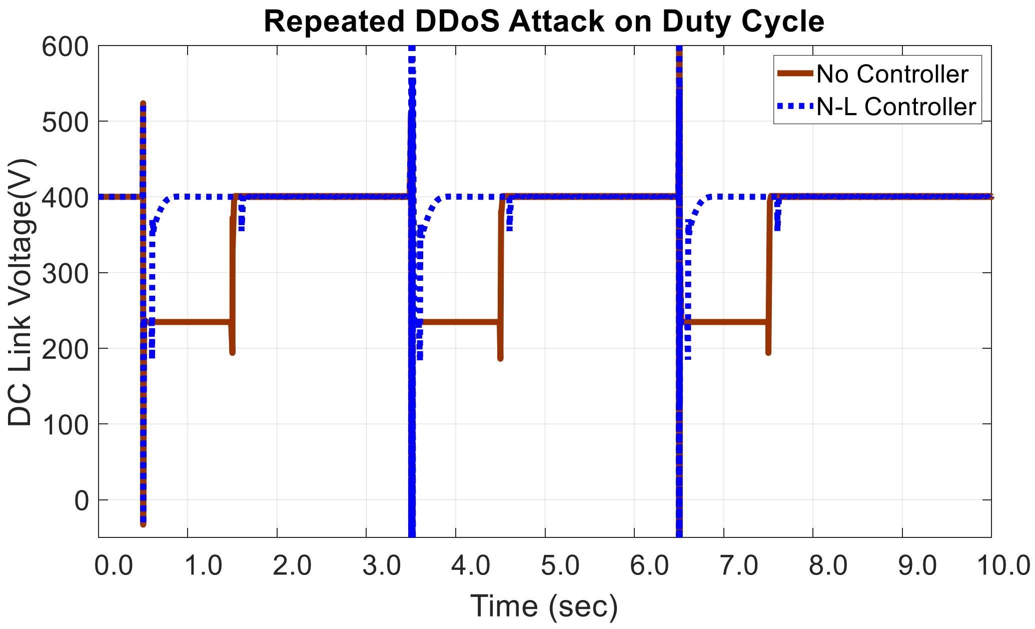


Fig. 29: Repeated DDoS attack on duty cycle of the PV boost converter scenario and mitigation effect on the DC link voltage.

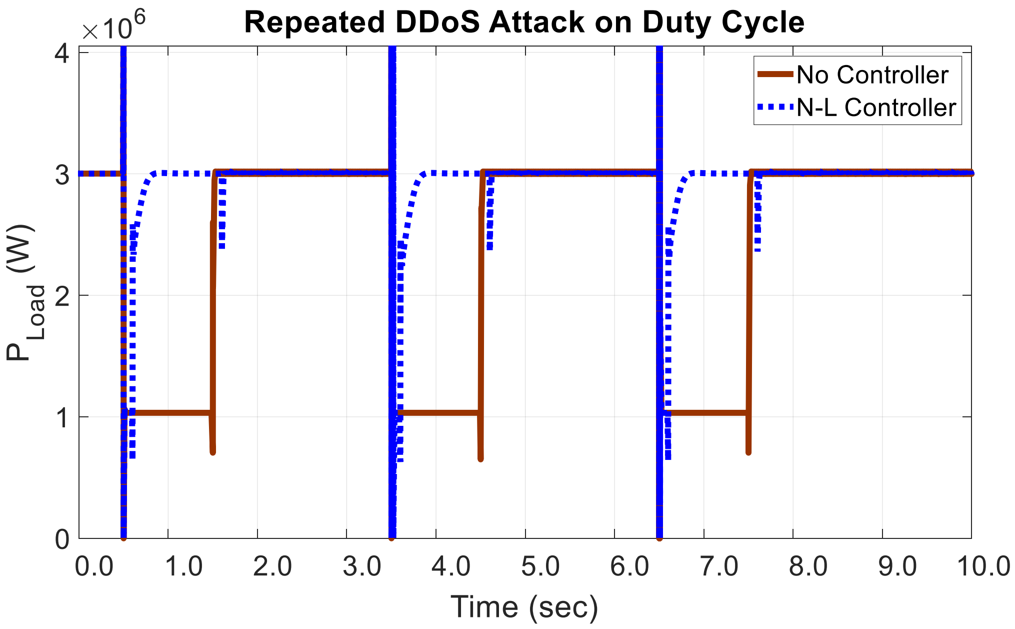


Fig. 30: Repeated DDoS attack on duty cycle of the PV boost converter scenario and mitigation effect on the load power.

E. CASE-I; SCENARIO-5

Effects and Solution of Repeated FDI Attack on Duty Cycle of The PV Boost Converter:

In the case of the repeated false data injection attack scenario, it has been considered that, at 0.5 sec of simulation the intruder attacks on the duty cycle at the input of the DC-DC boost converter. After one second (1.5 sec) the false data has been removed, but again after two seconds (3.5 sec), the intruder imposes the false data for one more second and the attacker follows the similar pattern of repeated attack for rest of the time. Figs. 31-34 show the responses of four parameters, such as the duty cycle, PV array voltage, DC grid Voltage, and output power. As shown from the responses, the duty cycle increases to its 90% value which is a very high value. Also, the terminal voltage of the PV array goes close to zero, and the DC grid voltage and the power at the grid become very low.

In that situation, to recover the imbalance situation of the grid, allowing the signal delay the controller has been activated after 0.1sec of the attack in every repeated stage at 0.6 sec, 3.6 sec, and 6.6 sec, respectively. For the nonlinear controller, the duty cycle comes back at the desired value properly within very short time (0.4 sec). As the D value is recovered, both the voltages at the terminal of PV array and the DC grid gradually come back to the 400V level. Following the voltage, the output power is also improved.

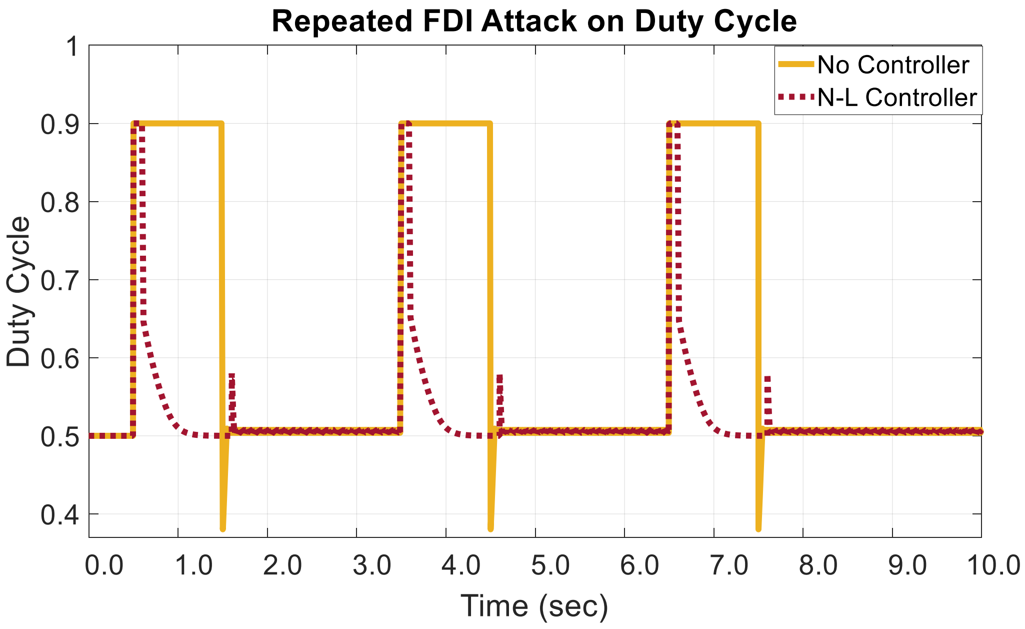


Fig. 31: Repeated FDI attack on duty cycle of the PV boost converter scenario and mitigation effect on the duty cycle.

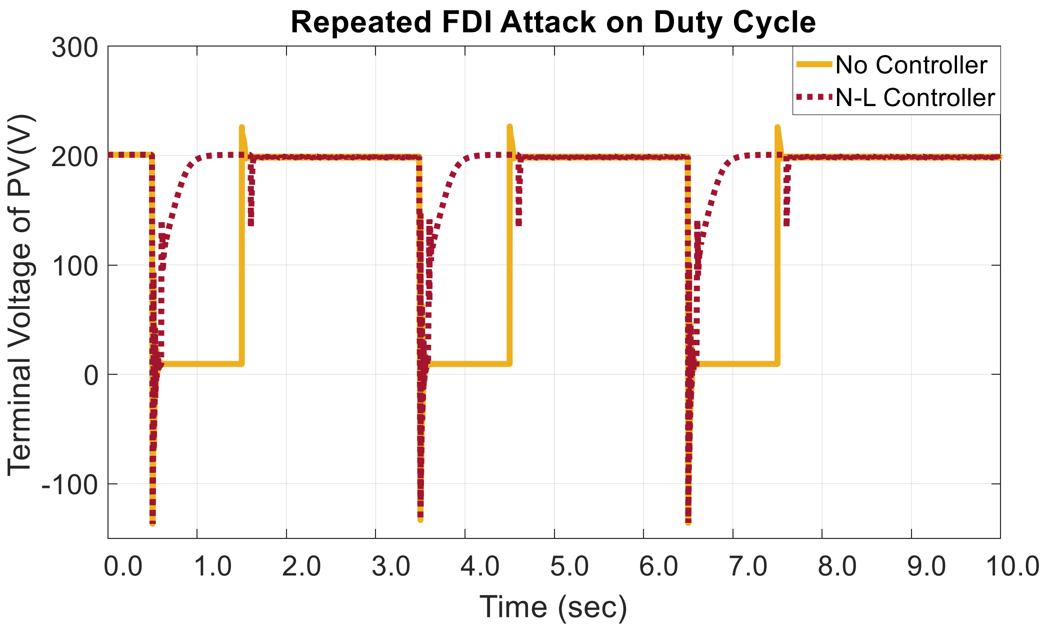


Fig. 32: Repeated FDI attack on duty cycle of the PV boost converter scenario and mitigation effect on the terminal voltage of PV array.

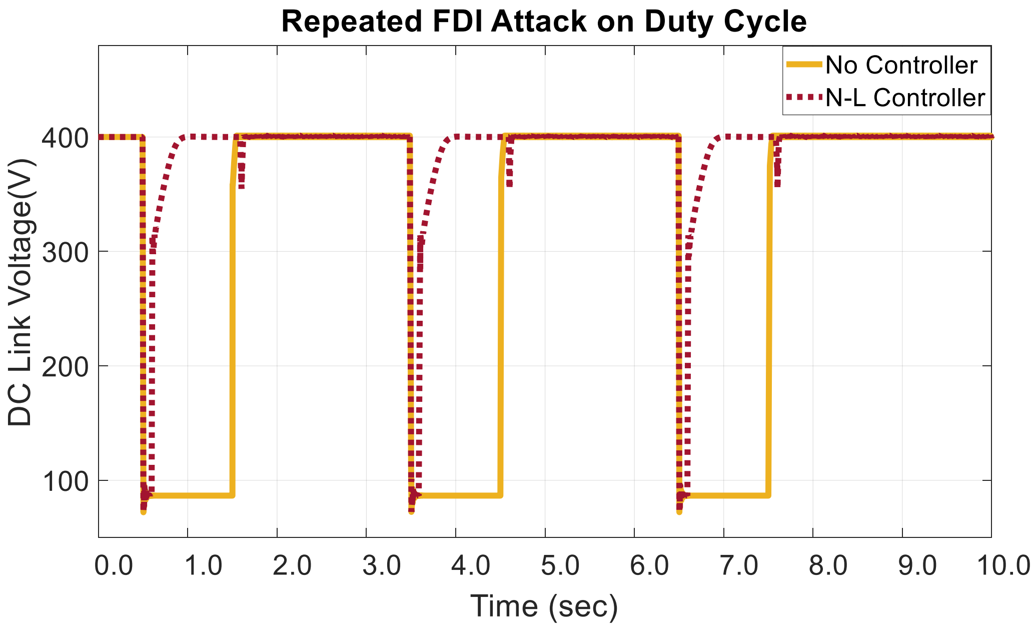


Fig. 33: Repeated FDI attack on duty cycle of the PV boost converter scenario and mitigation effect on the DC link voltage.

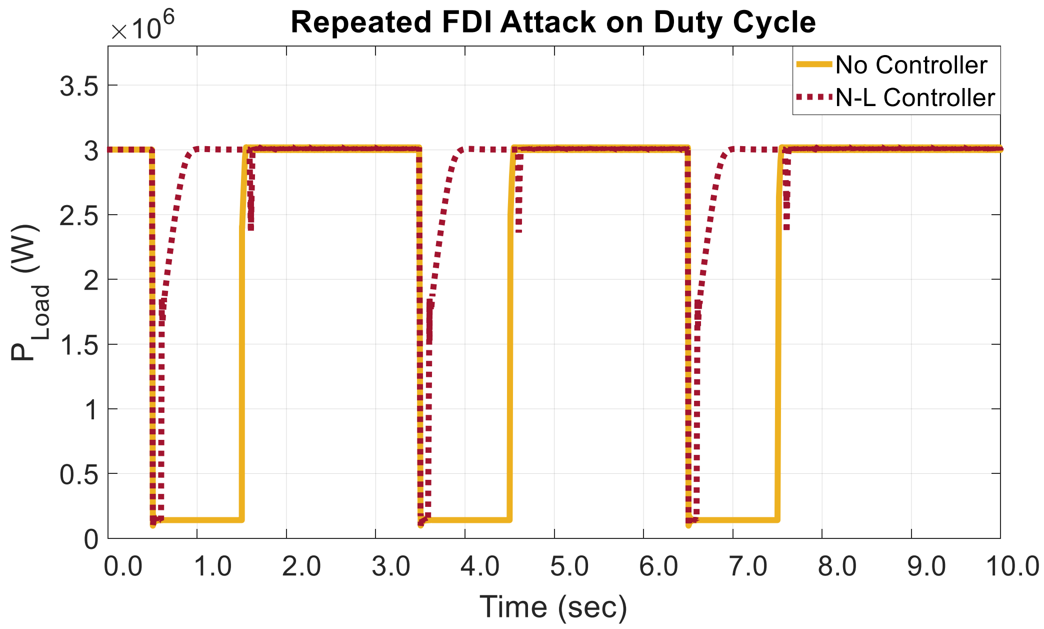


Fig. 34: Repeated FDI attack on duty cycle of the PV boost converter scenario and mitigation effect on the load power.

3.2.2 Cyber Attack on Load Profile

A. CASE-II; SCENARIO-1

Effects and Solution of FDI Attack on Load:

In this case, the attack has been simulated in a way that at 0.5sec the intruder changes the value of the load from the original set value of 0.0533Ω to a high value of 0.3Ω. For such high value of load, the terminal voltage of the DC grid rises up to 558.4V. As a result, the maximum power point condition gets diverged and the power goes very low. And the system becomes unstable. In this situation, at 0.6sec the controllers have been activated to stabilize the system by setting back the load. Figs. 35-38 show the responses of the duty cycle, voltage at both the terminal of PV array and the DC grid, and the load power, respectively.

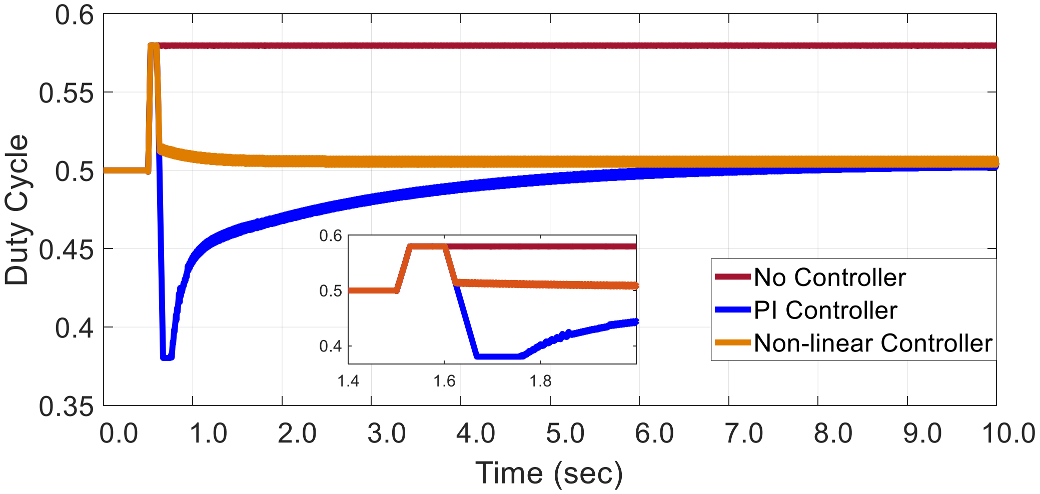


Fig. 35: False Data Injection (FDI) attack on load scenario and mitigation effect on the Duty Cycle.

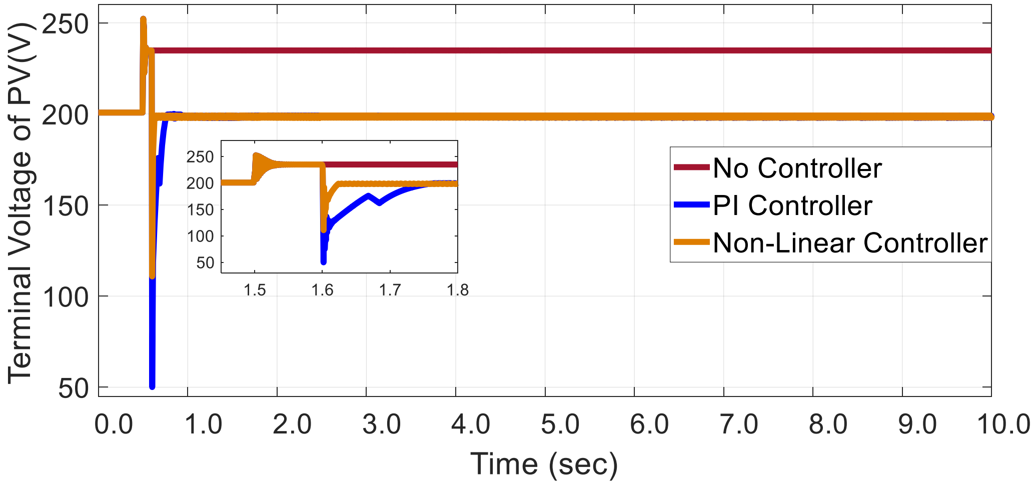


Fig. 36: False Data Injection (FDI) attack on load scenario and mitigation effect on the PV array terminal voltage.

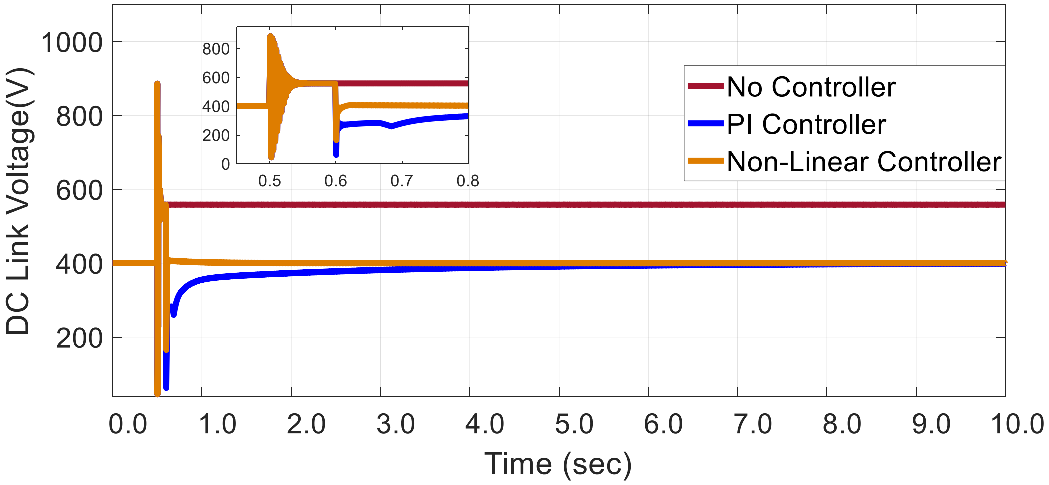


Fig. 37: False Data Injection (FDI) attack on load scenario and mitigation effect on the DC microgrid terminal voltage.

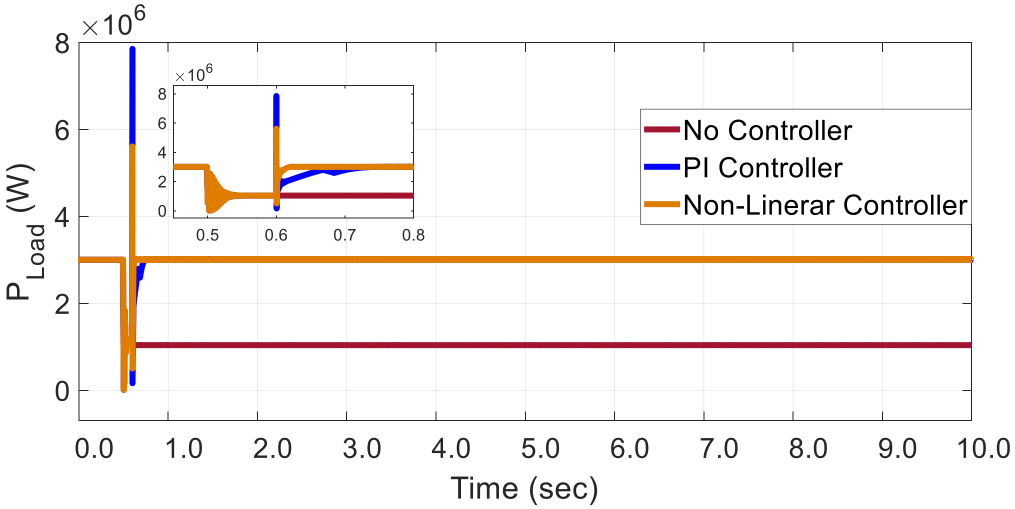


Fig. 38: False Data Injection (FDI) attack on load scenario and mitigation effect on the power at DC microgrid.

B. CASE-II; SCENARIO-2

Effects and Solution of Repeated FDI Attack on Load:

In this case, the similar attack pattern has been followed as the repeated FDI attack on duty cycle. At 00.5sec the intruder changes the value of the load from the original set value of 0.0533Ω to a high value of 0.3Ω. For such high value of load, the terminal voltage of the DC grid rises up to 558.4V. As a result, the maximum power point condition gets diverged and the power goes very low. After one second (1.5 sec) the false data has been removed, but again after two seconds (3.5 sec), the intruder imposes the false data for one more second and the attacker follows the similar pattern of repeated attack for rest of the time. In that situation, to recover the vulnerable situation of the grid, the controller has been activated allowing the signal delay after 0.1sec of the attack in every repeated stage at 0.6 sec, 3.6 sec, and 6.6 sec, respectively. In this situation, at 0.6sec the controllers have been activated to stabilize the system by setting back the load. Figs. 39-42 show the responses of the duty cycle, voltage at both the terminal of PV array and the DC grid, and the load power, respectively.

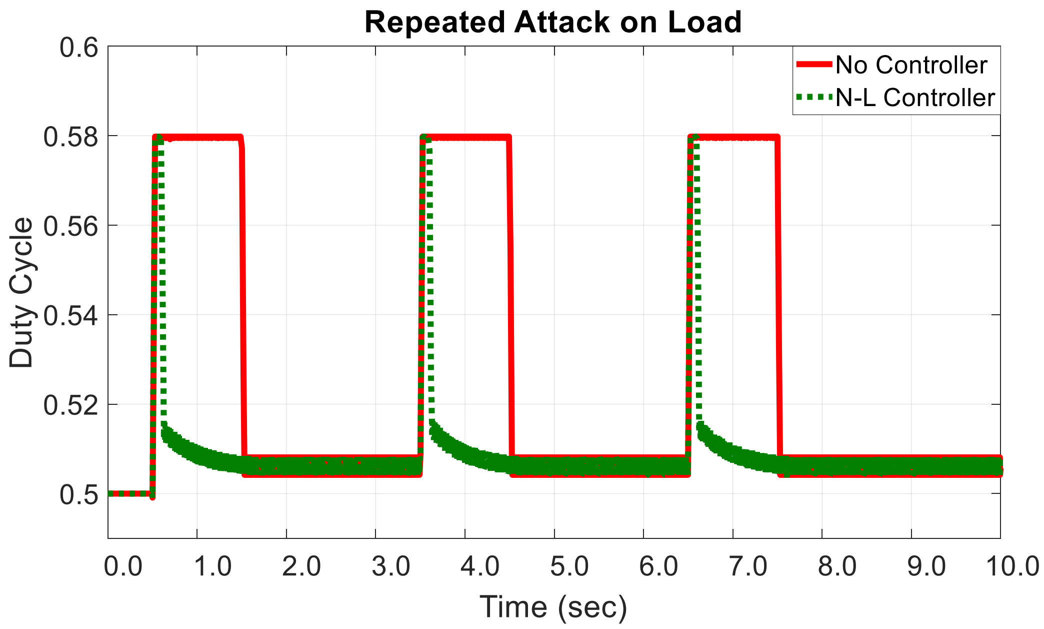


Fig. 39: Repeated False Data Injection (FDI) attack on load scenario and mitigation effect on the duty cycle.

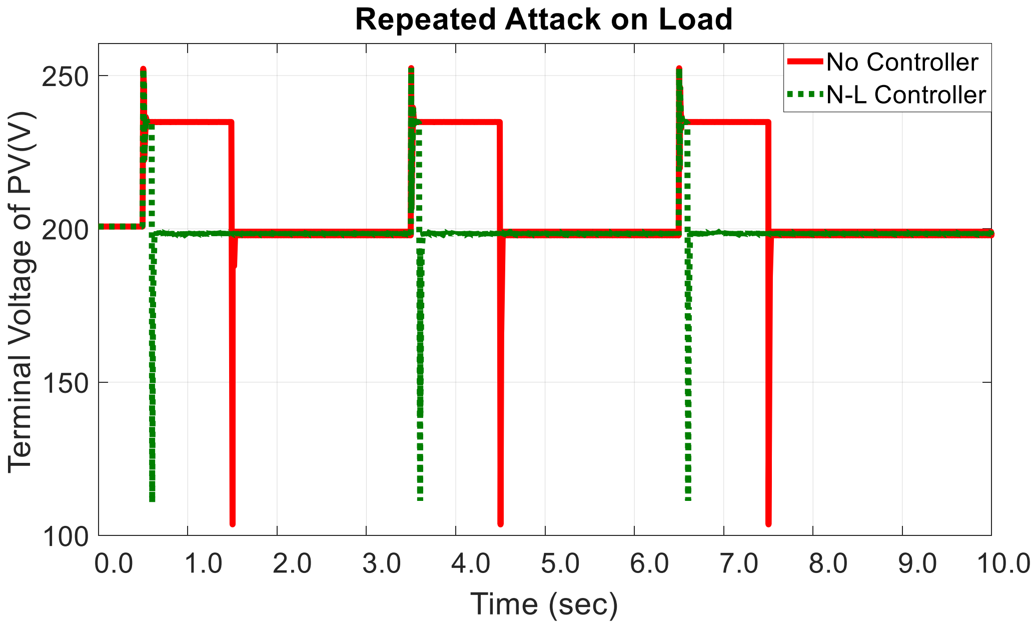


Fig. 40: Repeated False Data Injection (FDI) attack on load scenario and mitigation effect on the terminal voltage of PV array.

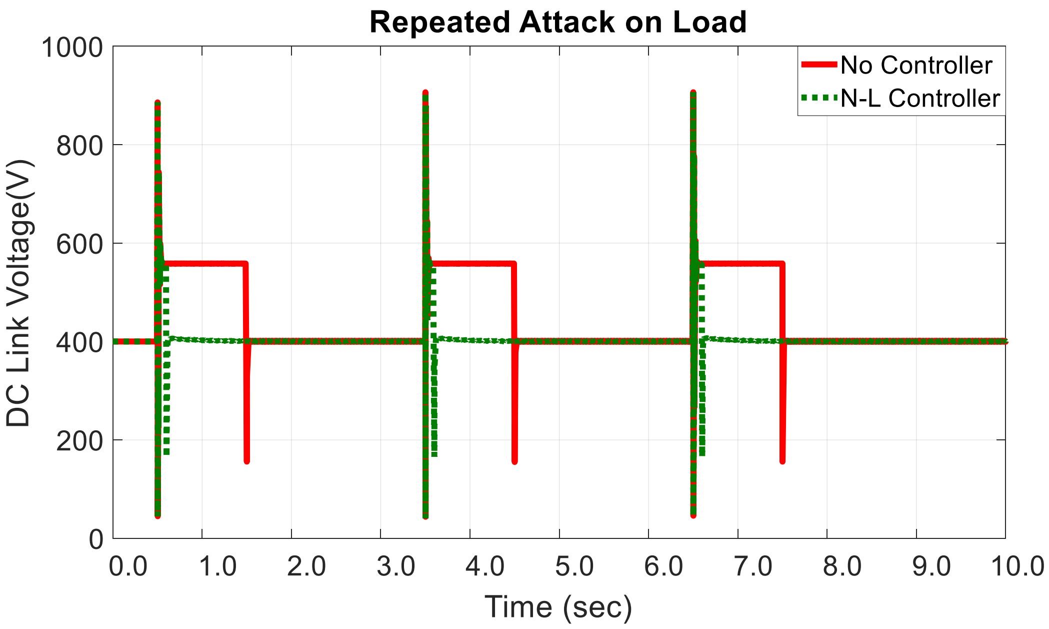


Fig. 41: Repeated False Data Injection (FDI) attack on load scenario and mitigation effect on DC link voltage.

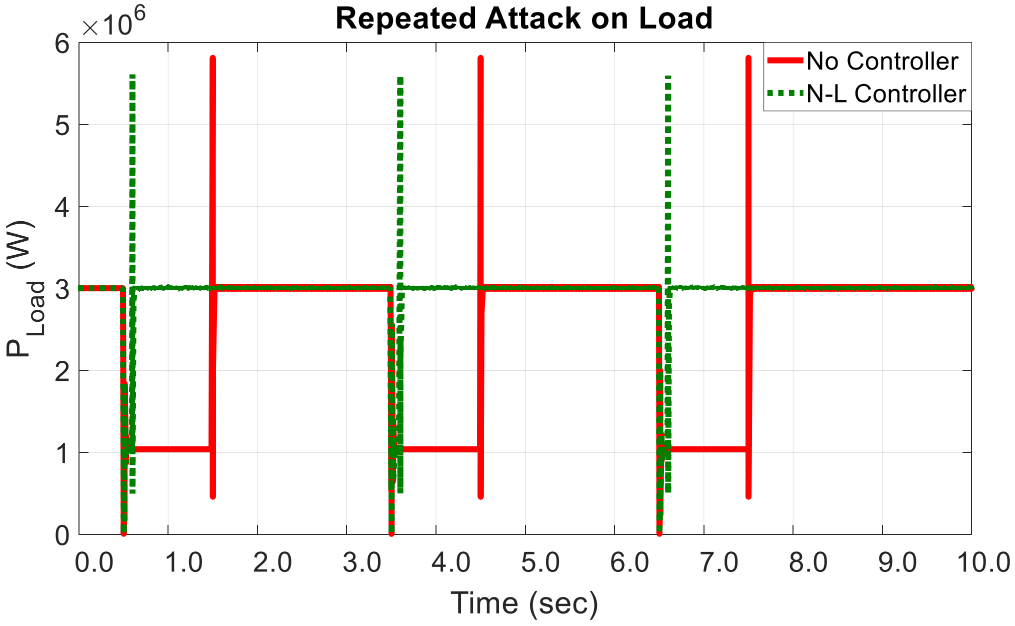


Fig. 42: Repeated False Data Injection (FDI) attack on load scenario and mitigation effect on load power.

3.2.3 Simultaneous Cyber Attack

A. CASE-III; SCENARIO-1

Simultaneous Attack on the Multiple components of DCMG:

Cyber-attack can happen at many locations of a power system. An intruder can target more than one location at a time. If happens so, then it will be very challenging to mitigate such vulnerabilities, because the attack in various location at the same time will have devastation effect on the system. In this section, it has been considered that the intruder attacks through false data injection both at the DC-DC boost converter of the PV system as well as the load profile. Again, in this case, the effect of single attack scenario and the repeated attack scenario will be observed. Then the performance of the existing controller will be observed whether it can withstand in such extreme situation or not.

Effects and Solution of Simultaneous FDI Attack on Both Duty Cycle of the PV Boost Converter and Load:

In case of the false data injection attack scenario, it has been considered that, at 0.5 sec of simulation the intruder attacks both on the duty cycle at the input of the DC-DC boost converter and the load profile. The intruder increases the duty cycle value and make it 90% and simultaneously change the load value from 0.0533Ω to a high value of 0.3Ω. Figs. 43-46 show the responses of four parameters, such as the duty cycle, PV array voltage, DC grid Voltage, and output power, respectively. As shown from the responses, the duty cycle increases to its

90% value, the terminal voltage of the PV array goes close to zero near around 50V, the power at the grid become very low (almost 800KW) and the DC grid voltage become higher (approximately 480V instead of 400V).

In that situation, to recover such instability of the grid, the controller has been activated at 0.6 sec. As a result, the duty cycle comes back to 0.5 value almost immediately within 0.25 sec. and the load value is resumed. As a result, both the voltages at the terminal of PV array and the DC grid gradually come back to their desired level. Following the voltage, the output power is also improved. It is quite certain that in all four cases the performance of the nonlinear controller is compatible.

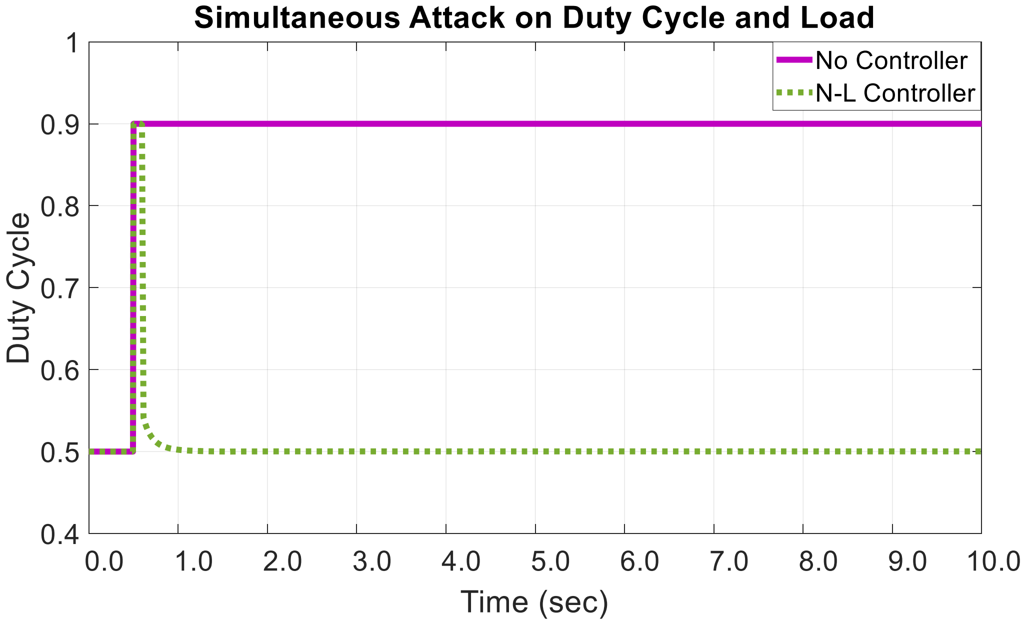


Fig. 43: Simultaneous False Data Injection (FDI) attack on Both Duty Cycle of the PV boost converter and load scenario and mitigation effect on Duty Cycle.

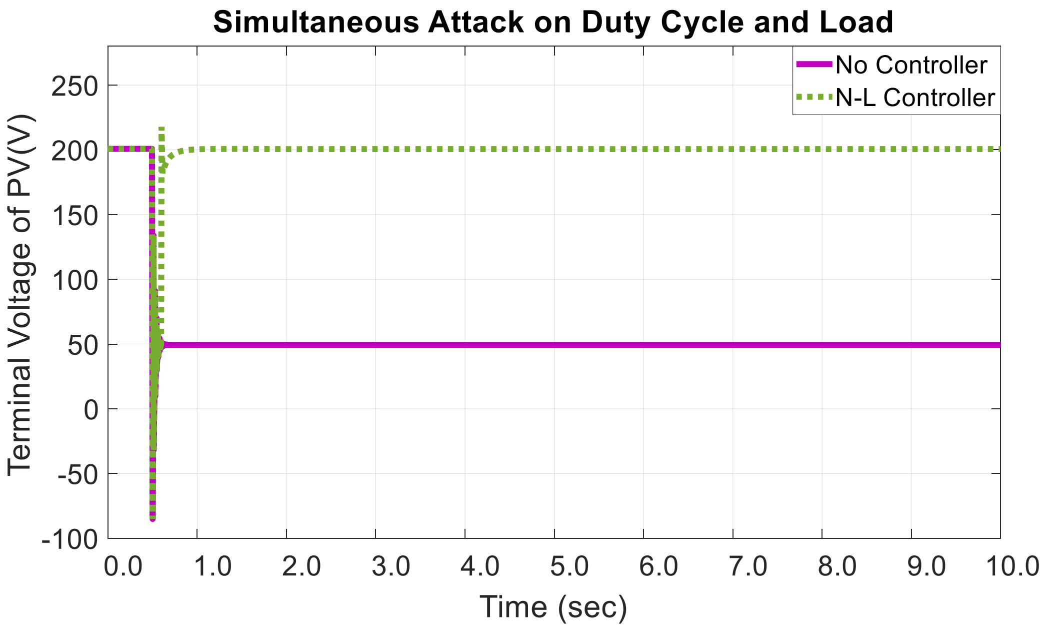


Fig. 44: Simultaneous False Data Injection (FDI) attack on Both Duty Cycle of the PV boost converter and load scenario and mitigation effect on terminal voltage of PV array.

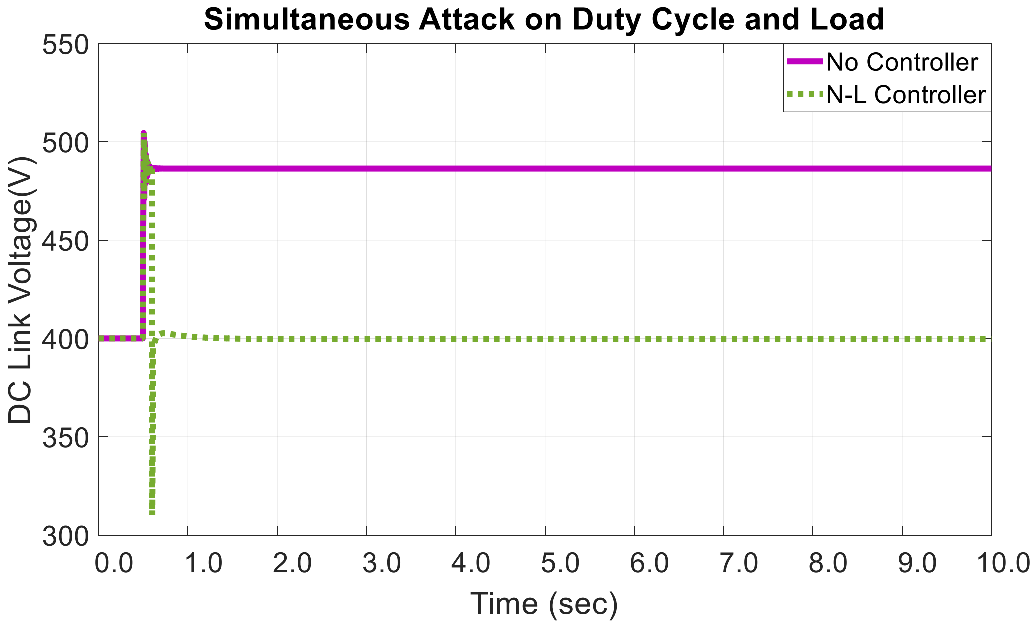


Fig. 45: Simultaneous False Data Injection (FDI) attack on Both Duty Cycle of the PV boost converter and load scenario and mitigation effect on the DC link voltage.

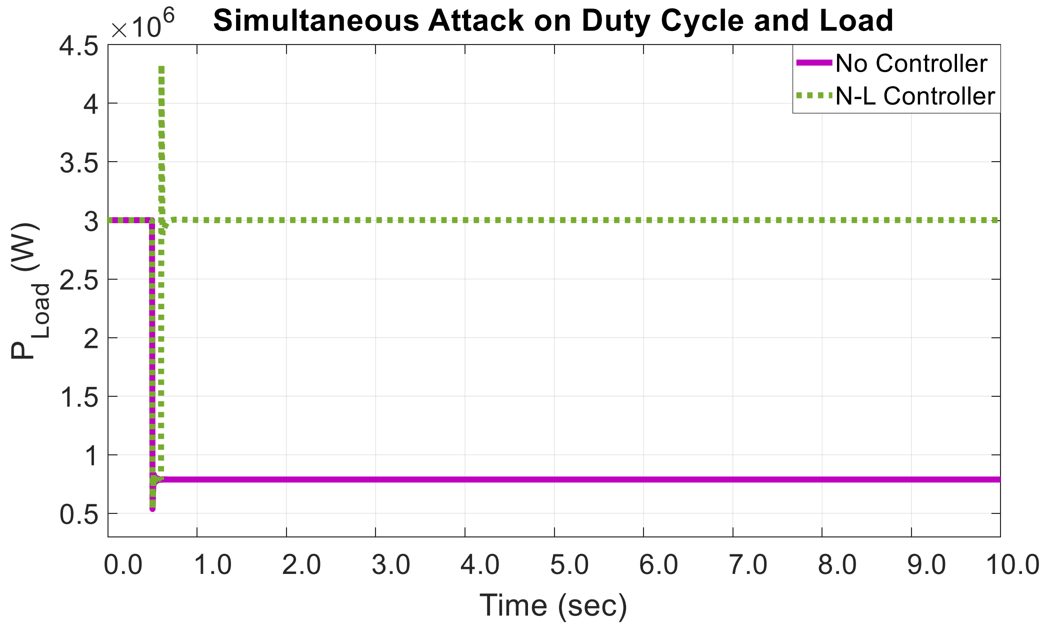


Fig. 46: Simultaneous False Data Injection (FDI) attack on Both Duty Cycle of the PV boost converter and load scenario and mitigation effect on load power.

B. CASE-III; SCENARIO-2

Effects and Solution of Repetitive Simultaneous FDI Attack on Both Duty Cycle of the PV Boost Converter and Load:

For the repetitive simultaneous false data injection attack scenario, it has been considered that, at 0.5 sec of simulation the intruder attacks both on the duty cycle at the input of the DC-DC boost converter and the load profile. The intruder increases the duty cycle value and makes it 90% and simultaneously changes the load value from 0.0533Ω to a high value of 0.3Ω. Then after one second both of the attacks have been removed and imposed 2 second later. This pattern follows for the rest of the time. In every case, for the mitigation, nonlinear controller is activated after 0.1second allowing the delay, thus the system stability is regained properly. Figs. 47-50 show the responses of four parameters, such as the duty cycle, PV array voltage, DC grid Voltage, and output power, respectively.

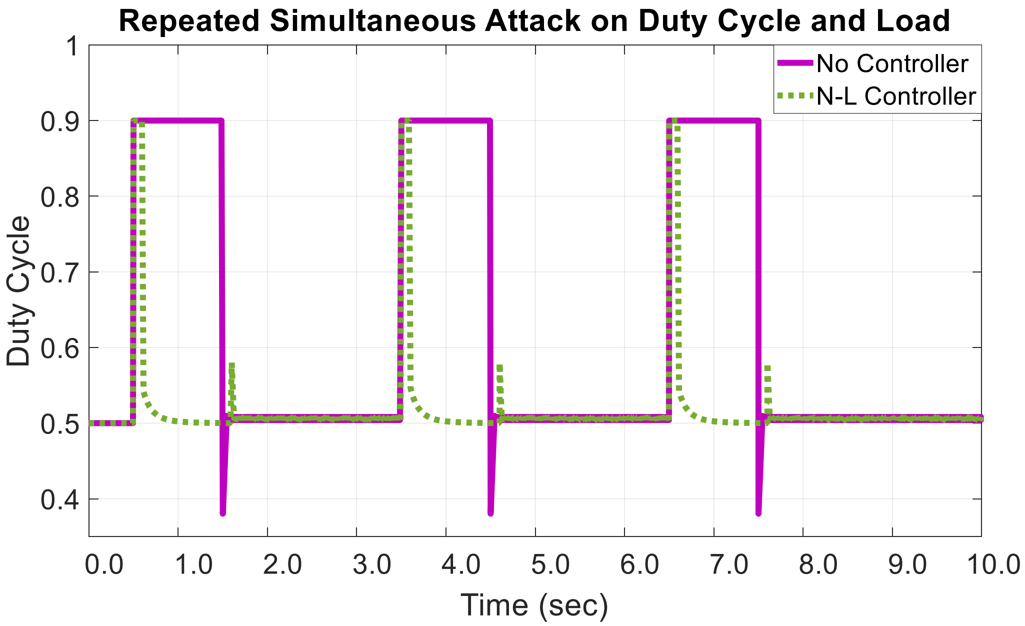


Fig. 47: Repeated simultaneous False Data Injection (FDI) attack on Both Duty Cycle of the PV boost converter and load scenario and mitigation effect on Duty Cycle.

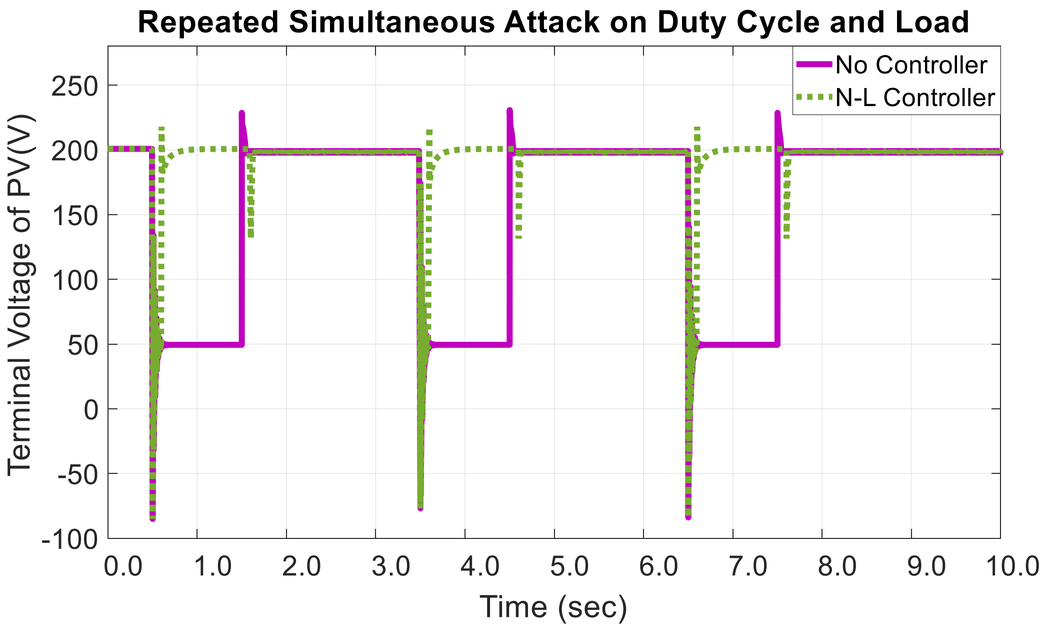


Fig. 48: Repeated simultaneous False Data Injection (FDI) attack on Both Duty Cycle of the PV boost converter and load scenario and mitigation effect on terminal voltage of PV array.

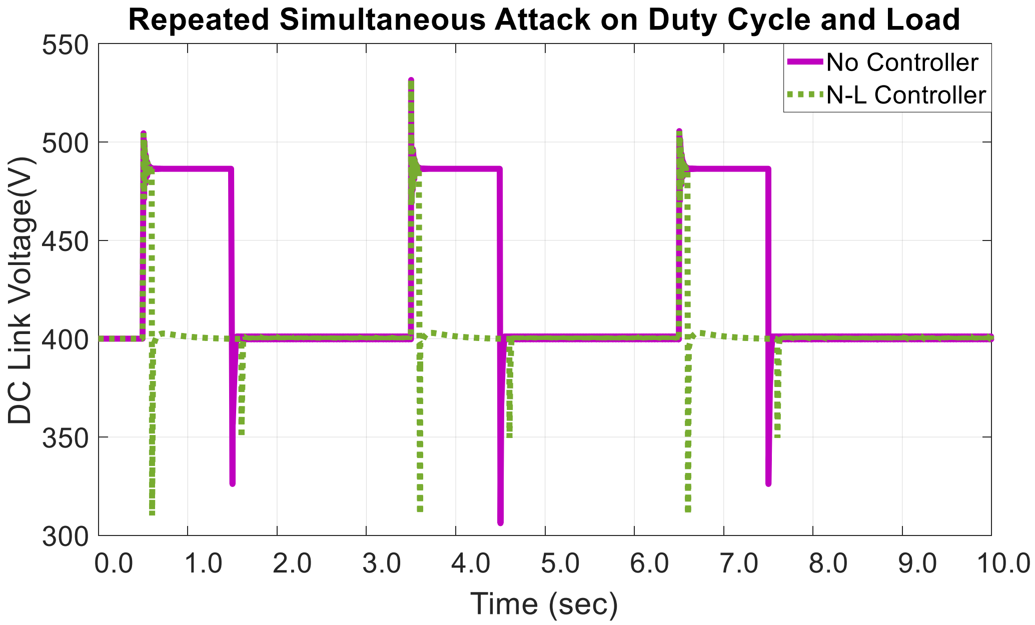


Fig. 49: Repeated simultaneous False Data Injection (FDI) attack on Both Duty Cycle of the PV boost converter and load scenario and mitigation effect on DC link voltage.

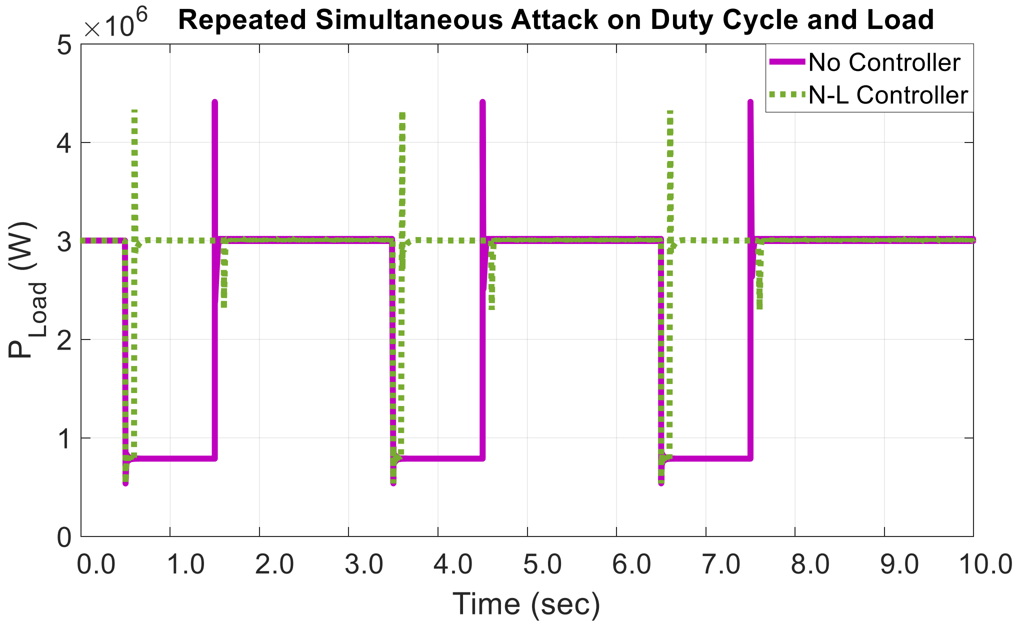


Fig. 50: Repeated simultaneous False Data Injection (FDI) attack on Both Duty Cycle of the PV boost converter and load scenario and mitigation effect on load power.

3.2.4 Cyber Attack on the Battery Energy Storage

A. CASE-IV; SCENARIO-1

Effects and Solution of FDI Attack on the Refence Value of Battery Energy Storage Control System

In case of the false data injection attack scenario on the Battery Energy System (BES), it has been considered that, at 0.5 sec of simulation the solar irradiance goes down to the value of 800 W/m^2. As a result, the load power goes low as well, and the BES starts providing power to the grid to minimize the power fluctuation. In that situation at 1.5 sec, the intruder changes the reference value of the BES management controller from 3MW to 4.5MW, and consequently the performance of the BES is hampered and the load power drops to 2.4MW and the voltage also go down at 360V instead of 400V. Fig. 51 shows the BES performance during the irradiation change before the occurrence of FDI attack and Figs. 52-54 show the responses of three parameters, such as the DC grid Voltage, output power at the load and power provided by the battery, respectively.

In that situation, to mitigate the adverse effect of the cyber-attack at 1.6 second, the nonlinear controller gets activated and tries to regain the reference value to its original set point. Within less than one second the BES starts providing optimum power and thus grid power is recovered.

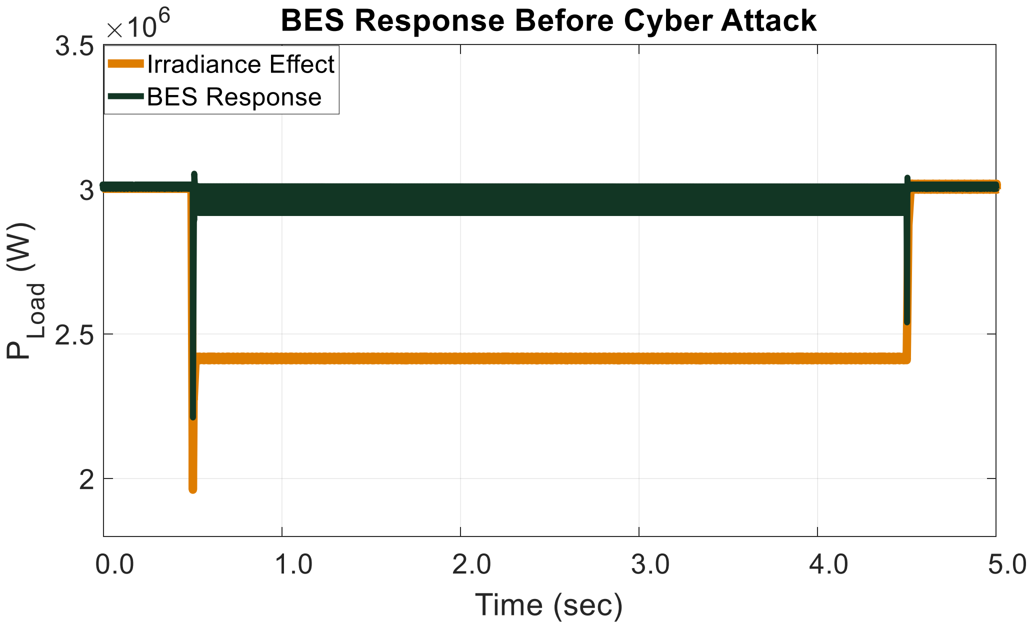


Fig. 51: Battery Energy Storage Performance during the irradiation change before the occurrence of FDI attack.

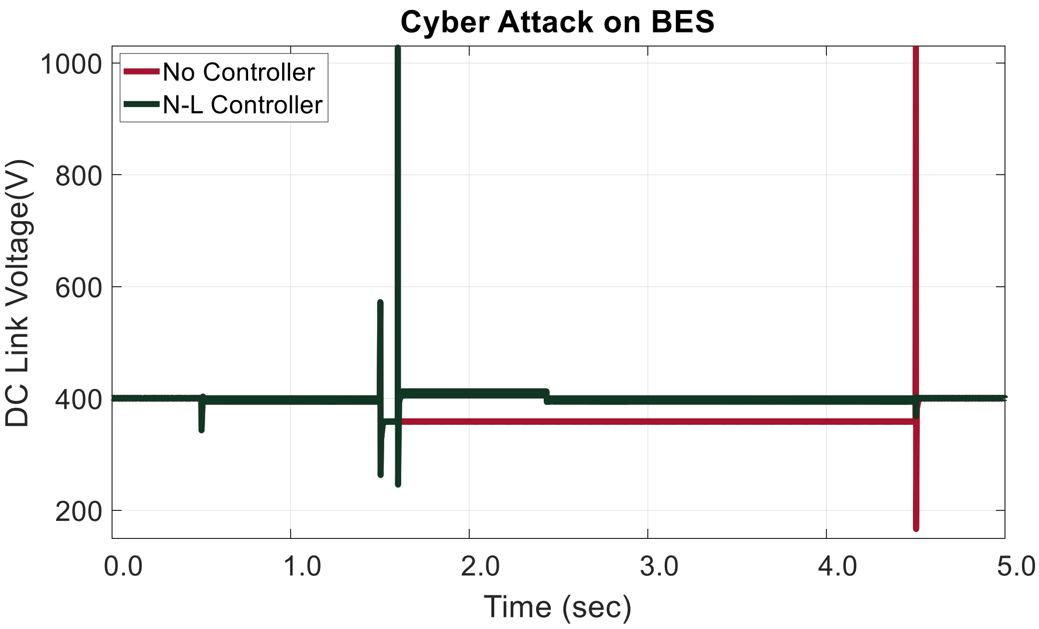


Fig. 52: False Data Injection (FDI) attack on the Battery Energy Storage scenario and mitigation effect on the DC link Voltage.

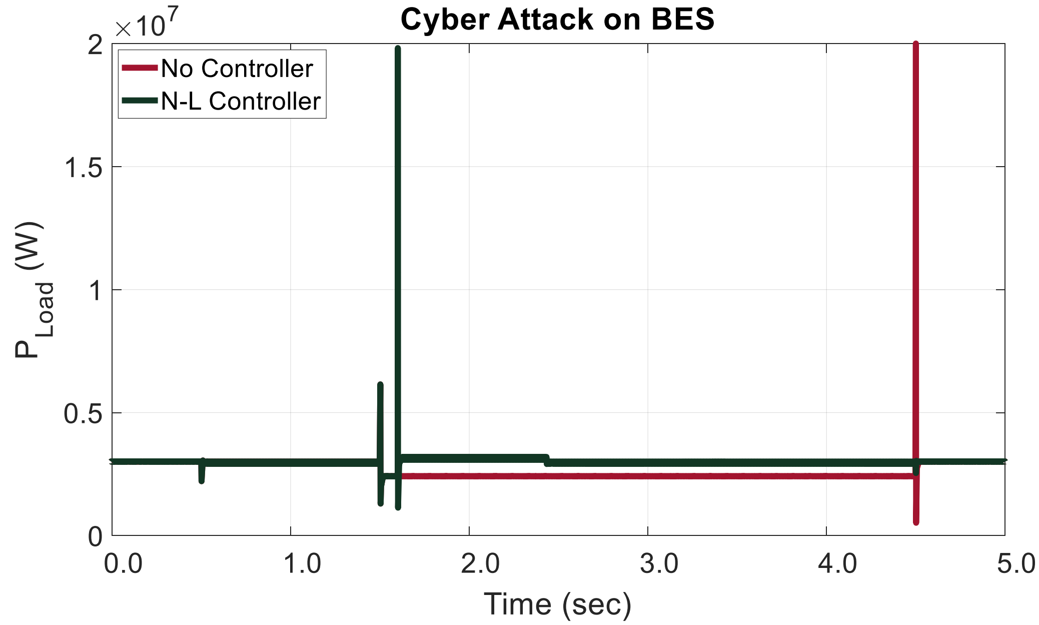


Fig. 53: False Data Injection (FDI) attack on the Battery Energy Storage scenario and mitigation effect on the load power.

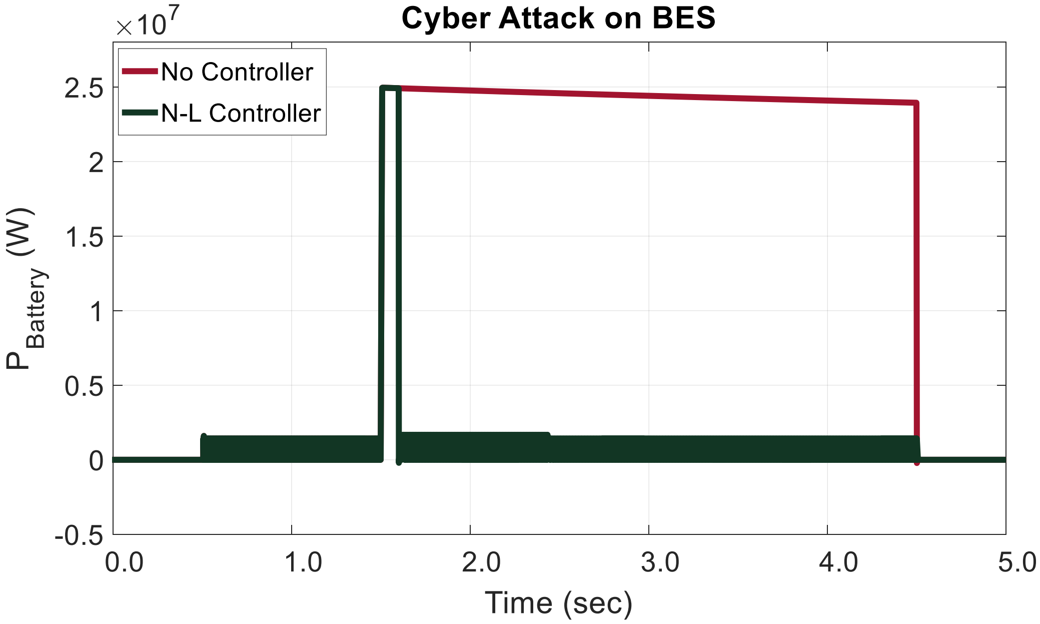


Fig. 54: False Data Injection (FDI) attack on the Battery Energy Storage scenario and mitigation effect on power provided by the battery.

3.2.5 Cyber Attack on the Fuel Cell System

B. CASE-V; SCENARIO-1

Effects and Solution of FDI Attack on the Duty Cycle of the DC-DC Converter of Fuel Cell System

In case of the false data injection attack scenario on the Duty Cycle of the DC-DC Converter of Fuel Cell System, it has been considered that, at 1.00 sec of simulation the intruder changes the value of the duty cycle of the DC-DC converter of the fuel cell from 0.64 to 0.15. As the value goes very low, the FC power also drops down from 115.2KW to 2.1KW. Figs. 55 and 56 show the responses of the Duty Cycle and the output power of FC, respectively.

In that situation, to mitigate the adverse effect of the cyber-attack, at 1.1 second the nonlinear controller gets activated and almost immediately it regains the duty cycle value to its original set point, as well as the power also comes back.

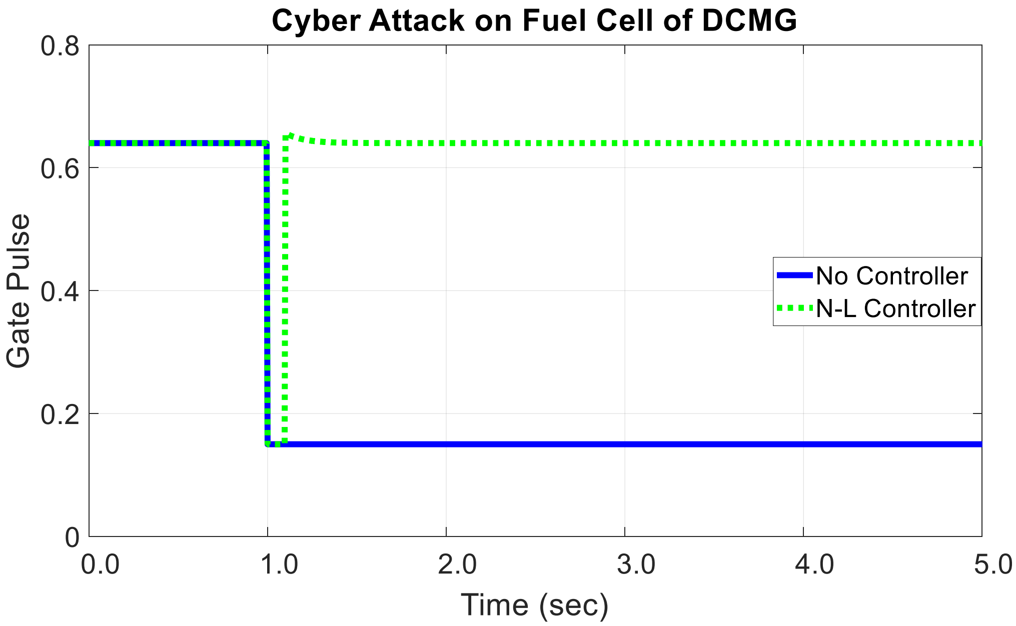


Fig. 55: False Data Injection (FDI) attack on the duty cycle of the DC-DC converter of fuel cell system scenario and mitigation effect on the Duty Cycle of FC.

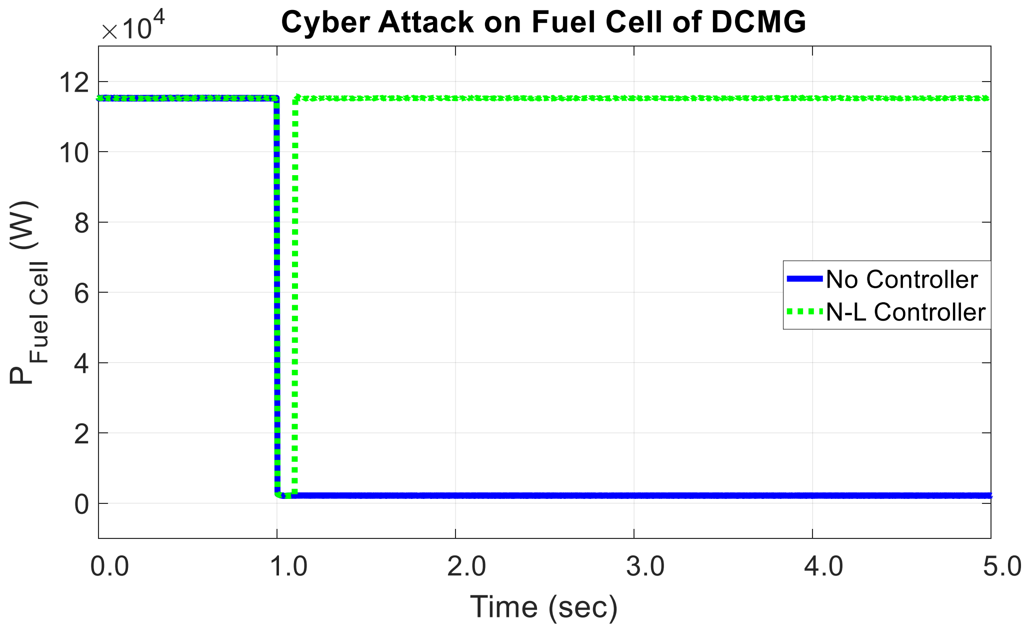


Fig. 56: False Data Injection (FDI) attack on the duty cycle of the DC-DC converter of fuel cell system scenario and mitigation effect on the power provided by the FC.

3.2.6 Cyber Attack on the Wind Power System

C. CASE-VI; SCENARIO-1

Effects and Solution of FDI Attack on the Voltage Reference Value of the Firing Angle Controller of AC-DC Converter of PMSG based Wind Power System

In case of the False Data Injection (FDI) attack scenario on the voltage reference value of the firing angle controller of AC-DC converter in PMSG based wind power system, it has been considered that, at 0.5 sec of simulation the intruder changes the voltage reference value of the firing angle controller from 400 to 100. This firing angle controller takes the DC link voltage as input of the controller to produce the required firing angle, α. Thus, with the change of the reference value it generates inappropriate angle value that hampers the conduction of the AC-DC converter. As a result, the DC link voltage as well as the load power goes low from 400V to 370.5V and from 5.115MW to 4.388MW respectively, as shown in Figs. 57-59.

In that situation, to mitigate the adverse effect of the cyber-attack, at 0.6 sec the nonlinear controller gets activated and within 0.7 second it regains the reference value of the voltage. As a result, the alpha value comes back to its required value to produce the 5.112MW of power at 400V value at the DC grid.

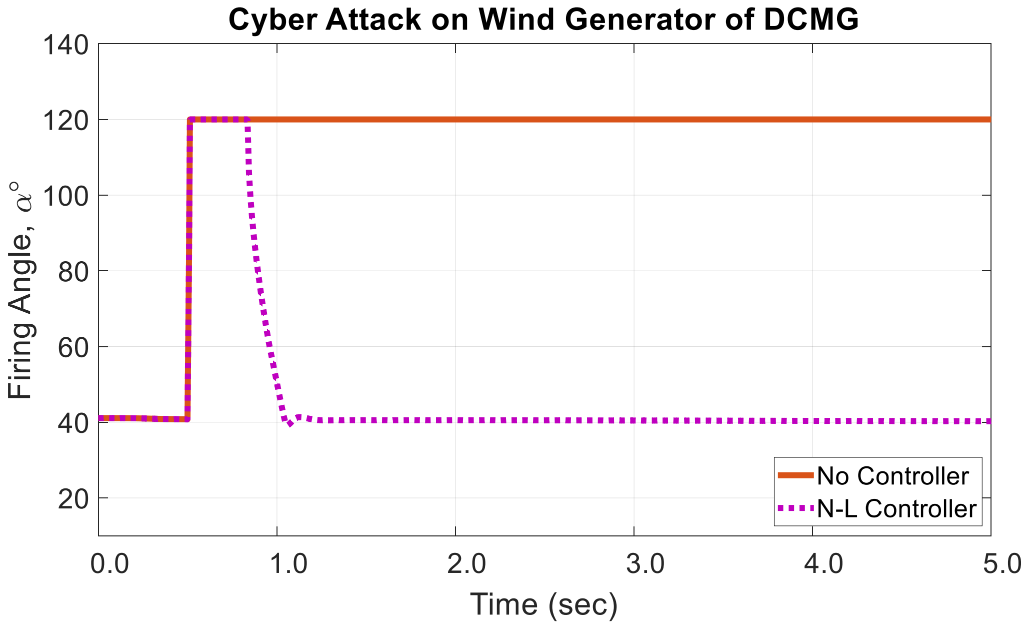


Fig. 57: False Data Injection (FDI) attack on the voltage reference value of the firing angle controller of AC-DC converter in PMSG based wind power system scenario and mitigation effect on the firing angle.

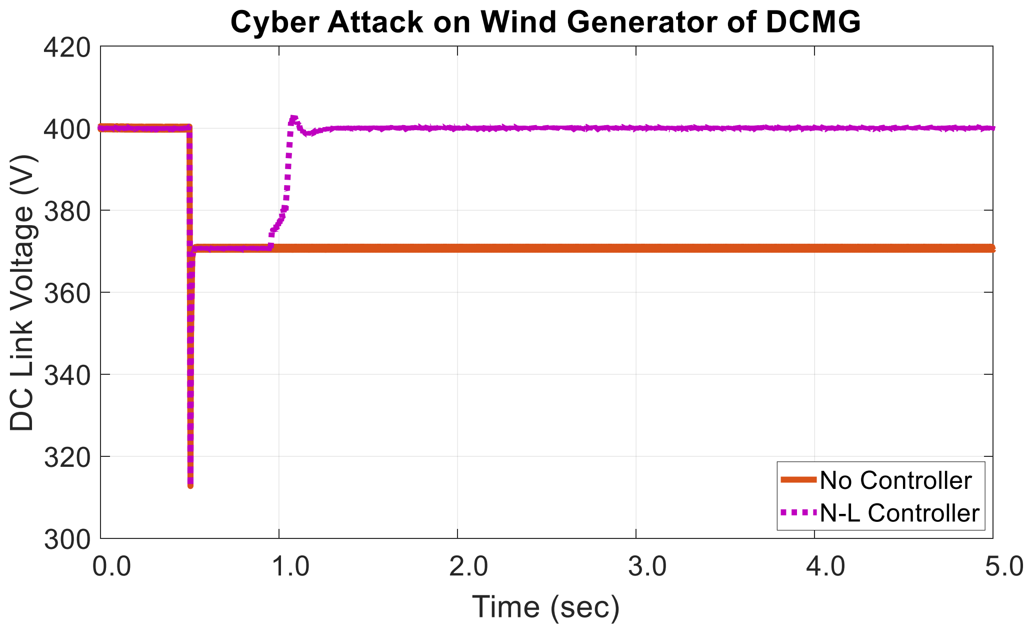


Fig. 58: False Data Injection (FDI) attack on the voltage reference value of the firing angle controller of AC-DC converter in PMSG based wind power system scenario and mitigation effect on the DC grid voltage.

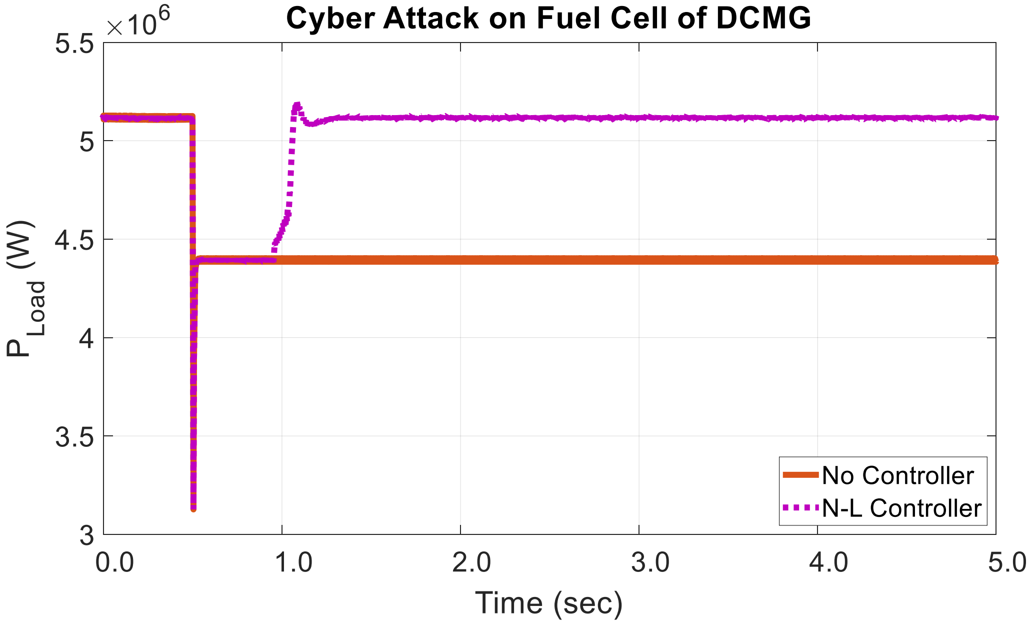


Fig. 59: False Data Injection (FDI) attack on the voltage reference value of the firing angle controller of AC-DC converter in PMSG based wind power system scenario and mitigation effect on the load power.

3.3 Index based performance evaluation of the proposed controllers

The performance of the proposed cyber security mitigation techniques has been evaluated through the voltage index calculation using the following equation:

$$Voltage\ Index = \int_0^T |\Delta V_{DC}|\, dt \tag{13}$$

Where, T is the simulation time for different cases. The lower the value of voltage index, the better the system performance. In other words, the less deviation of the DC grid terminal voltage with respect to time ensures the system stability. For obvious understanding of the controller performance, the percentage improvement has been calculated following the equation below:

$$\frac{V_{index_{No\ controller}} - V_{index_{With\ controller}}}{V_{index_{No\ controller}}} \times 100 \tag{14}$$

The Table 4 shows the voltage index values for all the scenarios that have been considered in this study. In that table for some of the cases of PI controller there is no index values, because on those cases only non-linear controller has been used. From these index values it is evident that the cyber-attack makes the DC microgrid system very much insecure, as the voltage index values without the controller are large. Using the proposed controllers, the system performance improved greatly. However, in all cases, where both the controllers are used, it is clear from the percentage improvement data that the non-linear controller is slightly better than the PI controller.

TABLE 4: VOTAGE INDEX VALUES FOR CYBER-ATTACK

Attack Scenario	Voltage Index				
	No Controller	Non-Linear Controller		PI Controller	
	Index	Index	Percentage Improvement (%)	Index	Percentage Improvement (%)
Case-I Scenario-1	7.442	0.1104	98.517	0.1518	96.961
Scenario-2	3.927	0.0517	98.684	0.1511	96.152
Scenario-3	4.398	0.1140	97.41	0.1518	96.55
Scenario-4	1.261	0.1713	86.42	-	-
Scenario-5	2.362	0.3382	85.68	-	-
Case-II Scenario-1	3.763	0.0534	98.58	0.3772	89.976
Scenario-2	1.203	0.1512	87.43	-	-
Case-III Scenario-1	2.052	0.0295	98.56	-	-
Scenario-2	0.6604	0.0817	87.63	-	-
Case-IV Scenario-1	0.3191	0.0511	83.99	-	-
Case-V Scenario-1	4.414	0.996	97.74	-	-
Case-VI Scenario-1	0.3311	0.0418	87.74	-	-

3.4 Conclusion

This chapter provides the detailed illustration of the different case studies of cyber-attack on the DC microgrid system. Through the graphical representation, the impact of cyber-attack on different components of microgrid system has been shown, that helps determine the severity of the different cases. Along with this, those plots also affirm the effectiveness of the proposed controllers for mitigation of adverse effects of cyber-attacks. In addition, the voltage index measurement and the percentage improvement calculation clearly show the improved performance and reliability of the proposed controllers.

CHAPTER-4

CONCLUSION AND FUTURE WORK

4.1 Conclusion

This work explores the effect of different type of cyber-attacks at different locations and components of the DC microgrid system. This thesis can be concluded as follows.

- This work provides a detail modelling of the DC microgrid system considering the distributed energy resources like PV, fuel cell, PMSG baser wind power system and most importantly the BES system which is the essential part of any microgrid system.
- Two types of mitigation controller, non-linear controller and the PI controller have been designed and proposed for the mitigation of the cyber-attack in the DCMG system.
- The proposed controllers can handle the cyber-attacks properly whether it is single attack, random attack, repetitive attack or simultaneous attack on the multiple locations of the DCMG system.

4.2 Contribution of this work

- This research proposes completely new scope of work on the DCMG system, as till now nobody has worked on the cyber-attack mitigation techniques on the DCMG system.

- This thesis proposed the design of the non-linear controller that can handle any type of set point change scenarios, thereby making the controller robust.
- The multiple attack locations in terms of real components of DCMG system has been considered in this work.
- The implementation of the proposed concept will ensure the stability, reliability and power quality of local area power system by ensuring the usage of everlasting energy resources with proper control of energy storage.

BROADER IMPACT OF THIS WORK

This research will provide a new approach to the conventional power generation system and it will have some intellectual, industrial as well as social benefits, as described below.

- Most of the industries, data centers, university campuses, hospitals, etc., use their individual power generation system or the subsystem to meet the power demand. Again, military bases need mobile means of power so that they can move anywhere with the power source. A regulated DCMG System can be a good option for the high-quality source of power.
- At any means consumers expect uninterrupted power, which can get hampered by the cyber-attacks. The outcome of this research can be helpful in increasing the reliability of such DCMG.
- The university campuses, hospitals, apartments, etc., can build the prototype based on the outcome of this research.
- This research can be added to the academic syllabus for any course that relates to smart grid or advanced power systems study.

4.3 Future scope of the work

This work can be extended to perform the following research tasks.

- A robust cyber-attack detection technique by recognizing the patterns of cyber-attack can be investigated.
- Other robust solutions to mitigate the adverse effects of cyber-attacks on the DCMG performance can be explored.
- As energy storage is an inseparable part of any MG system, more robust energy storage system using adaptive controllers can be designed for the DCMG system.

REFERENCES

[1] H. Lotfi and A. Khodaei, “AC versus DC microgrid planning,” *IEEE Trans. Smart Grid*, vol. 8, no. 1, pp. 296–304, 2017.

[2] J. Liu, W. Zhang, and G. Rizzoni, “Robust stability analysis of DC microgrids with constant power loads,” vol. 8950, no. c, pp. 1–9, 2017.

[3] X. Zhong, L. Yu, and R. Brooks, “Cyber security in smart DC microgrid operations,” *DC Microgrids (ICDCM*, pp. 86–91, 2015.

[4] F. Li, Z., Shahidehpour, M., and Aminifar, “Cybersecurity in Distributed Power Systems,” *Proc. IEEE*, vol. 105, no. 7, pp. 1367–1388, 2017.

[5] M. Kumar, S. C. Srivastava, and S. N. Singh, “Control Strategies of a DC Microgrid for Grid Connected and Islanded Operations,” *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 1588–1601, 2015.

[6] M. Adly and K. Strunz, “Irradiance-Adaptive PV Module Integrated Converter for High Efficiency and Power Quality in Standalone and DC Microgrid Applications,” *IEEE Trans. Ind. Electron.*, vol. 65, no. 1, pp. 436–446, 2018.

[7] C. S. Karavas, K. G. Arvanitis, G. Kyriakarakos, D. D. Piromalis, and G. Papadakis, “A novel autonomous PV powered desalination system based on a DC microgrid concept incorporating short-term energy storage,” *Sol. Energy*, vol. 159, no. November 2017, pp. 947–961, 2018.

[8] L. Xu and D. Chen, “Control and operation of a DC microgrid with variable generation and energy storage,” *IEEE Trans. Power Deliv.*, vol. 26, no. 4, pp. 2513–2522, 2011.

[9] C. D., X. L., and Y. L., “DC voltage variation based autonomous control of DC microgrids,” *IEEE Trans. Power Deliv.*, vol. 28, no. 2, pp. 637–648, 2013.

[10] S. Dhar, R. K. Patnaik, and P. K. Dash, “Fault Detection and Location of Photovoltaic Based DC Microgrid Using Differential Protection Strategy,” *IEEE Trans. Smart Grid*, vol. 3053, no. c, pp. 1–1, 2017.

[11] J. M. Guerrero, P. C. Loh, T. L. Lee, and M. Chandorkar, “Advanced control architectures for intelligent microgridsPart II: Power quality, energy storage, and AC/DC microgrids,” *IEEE Trans. Ind. Electron.*, vol. 60, no. 4, pp. 1263–1270, 2013.

[12] S. Anand, B. G. Fernandes, and J. M. Guerrero, “Distributed control to ensure proportional load sharing and improve voltage regulation in low-voltage DC microgrids,” *IEEE Trans. Power Electron.*, vol. 28, no. 4, pp. 1900–1913, 2013.

[13] T. Dragicevic, X. Lu, J. C. Vasquez, and J. M. Guerrero, “DC Microgrids - Part I: A Review of Control Strategies and Stabilization Techniques,” *IEEE Trans. Power Electron.*, vol. 31, no. 7, pp. 4876–4891, 2016.

[14] A. G. Tsikalakis and N. D. Hatziargyriou, “Centralized control for optimizing microgrids operation,” *IEEE Trans. Energy Convers.*, vol. 23, no. 1, pp. 241–248, 2008.

[15] M. D. Cook, G. G. Parker, R. D. Robinett, and W. W. Weaver, “Decentralized Mode-Adaptive Guidance and Control for DC Microgrid,” *IEEE Trans. Power Deliv.*, vol. 32, no. 1, pp. 263–271, 2017.

[16] A. Khorsandi, M. Ashourloo, and H. Mokhtari, “A decentralized control method for a low-voltage dc microgrid,” *IEEE Trans. Energy Convers.*, vol. 29, no. 4, pp. 793–801, 2014.

[17] J. M. Guerrero, M. Chandorkar, T. Lee, and P. C. Loh, “Advanced Control Architectures for Intelligent Microgrids; Part I: Decentralized and Hierarchical Control,” *Ind. Electron. IEEE Trans.*, vol. 60, no. 4, pp. 1254–1262, 2013.

[18] T. V. Vu, S. Paran, F. Diaz Franco, T. El-Mezyani, and C. S. Edrington, “An Alternative Distributed Control Architecture for Improvement in the Transient Response of DC Microgrids,” *IEEE Trans. Ind. Electron.*, vol. PP, no. 99, pp. 574–584, 2016.

[19] X. Lu, K. Sun, J. M. Guerrero, J. C. Vasquez, and L. Huang, “State-of-charge balance using adaptive droop control for distributed energy storage systems in DC microgrid applications,” *IEEE Trans. Ind. Electron.*, vol. 61, no. 6, pp. 2804–2815, 2014.

[20] C. Dong *et al.*, “Time-delay Stability Analysis for Hybrid Energy Storage System

with Hierarchical Control in DC Microgrids," *IEEE Trans. Smart Grid*, vol. 3053, no. c, 2017.

[21] C. Jin, P. Wang, J. Xiao, Y. Tang, and F. H. Choo, "Implementation of hierarchical control in DC microgrids," *IEEE Trans. Ind. Electron.*, vol. 61, no. 8, pp. 4032–4042, 2014.

[22] A. Bidram and A. Davoudi, "Hierarchical structure of microgrids control system," *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 1963–1976, 2012.

[23] J. Ma, L. Yuan, Z. Zhao, and F. He, "Transmission Loss Optimization Based Optimal Power Flow Strategy by Hierarchical Control for DC Micro-grids," *IEEE Trans. Power Electron.*, vol. 8993, no. c, pp. 1–1, 2016.

[24] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of False-Data Injection Attacks in Cyber-Physical DC Microgrids," *IEEE Trans. Ind. Informatics*, vol. 13, no. 5, pp. 2693–2703, 2017.

[25] O. A. Beg, L. V. Nguyen, T. T. Johnson, and A. Davoudi, "Signal Temporal Logic-based Attack Detection in DC Microgrids," *IEEE Trans. Smart Grid*, vol. 3053, no. c, pp. 1–11, 2018.

[26] Q. L. and J. Di H. A. Mantooth, Y. Liu, C. Farnell, F. Zhang, "Securing DC and hybrid microgrids," in *2015 IEEE First International Conference on DC Microgrids (ICDCM)*, 2015, p. 285–286c.

[27] X. Liu, M. Shahidehpour, Y. Cao, L. Wu, W. Wei, and X. Liu, "Microgrid Risk Analysis Considering the Impact of Cyber Attacks on Solar PV and ESS Control Systems," *IEEE Trans. Smart Grid*, vol. 8, no. 3, pp. 1330–1339, 2017.

[28] A. W. Miranda and S. Goldsmith, "Cyber-physical risk management for PV photovoltaic plants," *Proc. - Int. Carnahan Conf. Secur. Technol.*, vol. 2017–Octob, pp. 1–8, 2017.

[29] W. B. Solar *et al.*, "A New Strategy to Quantify Uncertainties of Forecasts Using Bootstrap Confidence Intervals," pp. 0–4, 2015.

[30] and Y. H. Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, "Detection of cyber attacks against voltage control in distribution power grids,"

2014 IEEE Int. Conf. Smart Grid Commun., vol. 7, no. 4, pp. 842–847, 2014.

[31] P. Li, Y. Liu, H. Xin, and X. Jiang, “A Robust Distributed Economic Dispatch Strategy of Virtual Power Plant Under Cyber-Attacks,” *IEEE Trans. Ind. Informatics*, vol. 3203, no. c, 2017.

[32] H. Zhang, W. Meng, J. Qi, X. Wang, and W. X. Zheng, “Distributed Load Sharing under False Data Injection Attack in Inverter-Based Microgrid,” *IEEE Trans. Ind. Electron.*, vol. 0046, no. c, pp. 1–1, 2018.

[33] S. Liu, B. Chen, T. Zourntos, D. Kundur, and K. Butler-Purry, “A coordinated multi-switch attack for cascading failures in smart grid,” *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1183–1195, 2014.

[34] L. Langer, P. Smith, M. Hutle, and A. Schaeffer-Filho, “Analysing cyber-physical attacks to a Smart Grid: A voltage control use case,” *2016 Power Syst. Comput. Conf.*, pp. 1–7, 2016.

[35] A. Anwar, A. N. Mahmood, and Z. Shah, “A Data-Driven Approach to Distinguish Cyber-Attacks from Physical Faults in a Smart Grid,” *Proc. 24th ACM Int. Conf. Inf. Knowl. Manag. - CIKM ’15*, no. November, pp. 1811–1814, 2015.

[36] H. Wang *et al.*, “Deep Learning Based Interval State Estimation of AC Smart Grids against Sparse Cyber Attacks,” *IEEE Trans. Ind. Informatics*, vol. 3203, no. c, pp. 1–12, 2018.

[37] A. F. Taha, J. Qi, J. Wang, and J. H. Panchal, “Risk Mitigation for Dynamic State Estimation Against Cyber Attacks and Unknown Inputs,” vol. 9, no. 2, pp. 886–899, 2015.

[38] Y. Zhou and Z. Miao, “Cyber attacks, detection and protection in smart grid state estimation,” *NAPS 2016 - 48th North Am. Power Symp. Proc.*, pp. 1–6, 2016.

[39] M. H. Kapourchali, S. Member, M. Sepehry, and S. Member, “Fault Detector and Switch Placement in Cyber- Enabled Power Distribution Network,” *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 1–12, 2018.

[40] A. Ashok, M. Govindarasu, and V. Ajjarapu, “Online Detection of Stealthy False Data Injection Attacks in Power System State Estimation,” *IEEE Trans. Smart*

Grid, vol. 9, no. 3, pp. 1–1, 2018.

[41] T. S. Abdelgayed, W. G. Morsi, and T. S. Sidhu, “A new harmony search approach for optimal wavelets applied to fault classification,” *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 521–529, 2018.

[42] A. Majumdar and B. C. Pal, “Bad Data Detection in the Context of Leverage Point Attacks in Modern Power Networks,” *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 2042–2054, 2018.

[43] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, “Distributed Blockchain-Based Data Protection Framework for Modern Power Systems against Cyber Attacks,” *IEEE Trans. Smart Grid*, vol. 3053, no. c, pp. 1–1, 2018.

[44] A. Farraj, E. Hammad, and D. Kundur, “A cyber-physical control framework for transient stability in smart grids,” *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 1205–1215, 2018.

[45] U. Yilmaz, A. Kircay, and S. Borekci, “PV system fuzzy logic MPPT method and PI control as a charge controller,” *Renew. Sustain. Energy Rev.*, vol. 81, no. August 2017, pp. 994–1001, 2018.

[46] L. B. G. Campanhol, S. A. O. Da Silva, A. A. De Oliveira, and V. D. Bacon, “Dynamic Performance Improvement of a Grid-Tied PV System Using a Feed-Forward Control Loop Acting on the NPC Inverter Currents,” *IEEE Trans. Ind. Electron.*, vol. 64, no. 3, pp. 2092–2101, 2017.

[47] Department of Energy, “Solar Energy in the United States,” 2018. [Online]. Available: https://energy.gov/eere/solarpoweringamerica/solar-energy-united-states. [Accessed: 16-Oct-2018].

[48] Ecodirect, “Helios 9T6-420 > 420 Watt Solar Panel,” 2018. [Online]. Available: https://www.ecodirect.com/Helios-9T6-420-420W-49V-PV-Panel-p/helios-9t6-420.htm. [Accessed: 14-Mar-2018].

[49] T. P. Sahu and T. V. Dixit, “Modelling and analysis of perturb and observe and incremental conductance MPPT algorithm for PV array using Ċuk converter,” *2014 IEEE Students’ Conf. Electr. Electron. Comput. Sci. SCEECS 2014*, vol. 4, no. 2, pp. 213–224, 2014.

[50] F. G. P. Plant, W. Yang, S. Member, K. Y. Lee, S. T. Junker, and H. Ghezel-ayagh, “Fuzzy Fault Diagnosis and Accommodation System,” *Energy*, vol. 25, no. 4, pp. 1187–1194, 2010.

[51] H. Van Heemst, “The Future Is Present in California: Delivering on the Promise of Fuel Cell-Powered Transportation,” no. February, pp. 75–77, 2001.

[52] F. I. S. ; S. ; Y. P. H. ; I. M. N. ; H. Devianto, “Effect of start-stop cycles and hydrogen temperature on the performance of Proton Exchange Membrane Fuel Cell (PEMFC),” in *2014 International Conference on Electrical Engineering and Computer Science (ICEECS).*

[53] B. Woo and J. Chang, “Hydrogen Production via Water Electrolysis: The Benefits of a Solar Cell-Powered Process,” *IEEE Electrif. Mag.*, pp. 19–25, 2018.

[54] M. F. M. Arani and Y. A. R. I. Mohamed, “Assessment and Enhancement of a Full-Scale PMSG-Based Wind Power Generator Performance under Faults,” *IEEE Trans. Energy Convers.*, vol. 31, no. 2, pp. 728–739, 2016.

[55] X. Zeng, J. Yao, Z. Chen, W. Hu, Z. Chen, and T. Zhou, “Co-Ordinated control strategy for hybrid wind farms with PMSG and FSIG under unbalanced grid voltage condition,” *IEEE Trans. Sustain. Energy*, vol. 7, no. 3, pp. 1100–1110, 2016.