B.Thej/Afr.J.Bio.Sc.6(10) 4009-4015

ISSN: 2663-2187

https://doi.org/10.33472/AFJBS.6.10.2024 4009-4015

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

A CYBER SECURITY IN DC MICROGRIDS FOR DETECTING FALSE DATA INJECTION BY FUZZY CONTROLLER

Mr. B Theja
PG Scholar
Department of Electrical and Electronics Engineering,
Kuppam Engineering College,
KES Nagar, Kuppam, Andhra Pradesh 517425 India
Email:thejutheju026@gmail.com

Dr.Velappagari Sekhar
Associate Professor & HOD
Department of Electrical and Electronics Engineering,
Kuppam Engineering College,
KES Nagar, Kuppam, Andhra Pradesh 517425 India
Email: velappagarisekhar@gmail.com

Mr. V.Niranjan
Lecturer
Department of Electrical and Electronics Engineering,
Dr.Y.C. James Yen Government Polytechnic,
Kuppam, Andhra Pradesh 517425 India
Email: *niranjan.vaidhyam@gmail.com*

Mr. M Komal Kumar
PG Scholar
Department of Electrical and Electronics Engineering,
Kuppam Engineering College,
KES Nagar, Kuppam, Andhra Pradesh 517425 India
Email: komalkumarreddy15@gmail.com

***Abstract*— The increasing incorporation of digital technologies into power networks has raised serious concerns about the susceptibility to cyberattacks. The dependable functioning of DC micro grid clusters is seriously threatened, especially by false data injection assaults. The detection of cyberattacks using bogus data injection in the control systems of several DC micro grid clusters is the focus of this study. To control the micro grid clusters, the current system uses a Proportional-Integral-Derivative (PID) controller in the control block. Nevertheless, conventional controllers such as PID are vulnerable to malevolent manipulations via fake data injection assaults, jeopardizing the micro grid clusters' stability and efficacy. A suggested system is presented in response to this vulnerability, and the control block of the system includes a fuzzy controller. Fuzzy logic controllers are more resistant to cyberattacks because of their resilience and adaptability. By strengthening the system's defenses against false data injection assaults, the integration of the fuzzy controller seeks to improve the cyber-physical security of the DC micro grid clusters. The performance of the suggested fuzzy controller-based system and the current PID-based system are compared in the study both in the presence of simulated fake data injection assaults and under typical operating conditions. In order to demonstrate the benefits of the fuzzy controller in terms of identifying and countering cyberattacks while preserving the intended stability and functionality of the DC micro grid clusters, comparative studies are carried out.**

Keywords*— *DC Microgrid, PID Controller, fuzzy controller, cyber security etc.

I. INTRODUCTION

The capacity of DC microgrids (MGs), often referred to as next-generation power systems, to transmit power from renewable energy sources and energy storage devices to a variety of loads more reliably and efficiently than the AC grid has drawn a lot of interest in recent years. The DC MG is a distributed power supply that can be linked to the electric grid or used independently. Power generation [1], smart homes [2], transportation systems [3], and other fields are examples of such applications. Owing to the Industry 4.0 paradigm's quick development, information technology-based solutions are now frequently employed in industrial operations.

Cyber-physical systems have emerged as a result of the revolutionary advances, allowing for the real-time

transmission of massive volumes of data between several devices [4]. As a result, the DC MG framework has a tendency to be more intelligent, dispersed, and closely network connected.However, DC MGs are more susceptible to security risks [5] and are at a larger risk of being penetrated by malevolent attackers because of their heavy reliance on communication technologies. Generally speaking, the accuracy of the data that the measuring devices or sensors collect has a significant impact on how well a possible microgrid controller functions.

For instance, in the event that an attacker compromises the sensors or communication links, the controllers can get inaccurate data and, as a result, make poor control decisions [6], which could result in unfavorable power-sharing [7], frequency oscillation [8], and stability problems [9]. Because of this, energy storage devices might not be able to supply the necessary amount of power or run at the best possible economic dispatch, and renewable energy generating units might not be able to capture the maximum amount of power from nature or meet the proper power sharing between microgrids [10].

More dangerously, in the absence of sufficient hardware or software regulations, attackers might be able to interfere with the system and cause substantial societal harm. A few instances are the nuclear plant that was infected with Stuxnet malware [11], the power outage that occurred [12, 13], and the nuclear plant blackout disaster [14]. Given the significant damage that cyberattacks can do to microgrid systems, it is essential to have a reliable detection mechanism in place to stave them off. The landscape of power distribution networks has changed dramatically in recent years due to the emergence of DC microgrids, which provide several benefits like increased efficiency, dependability, and integration of renewable energy sources. However, since digital control and communication technologies are used more frequently, cyber attacks have become a serious worry. These threats present hazards like data breaches, system manipulations..

Particularly, false data injection attacks have drawn attention since they can jeopardize the dependability and integrity of microgrid operations. In these attacks, hostile actors introduce fake data into the system, which causes control algorithms to make incorrect judgments and thereby impair grid performance. It is critical to identify and stop these attacks in order to guarantee the safe and dependable operation of DC microgrids.It is therefore essential to use cutting edge control methods in conjunction with strong cyber security protocols. With its reputation for managing intricate and unpredictable systems, fuzzy logic control presents a viable method for identifying and countering fake data injection assaults in DC microgrids. Fuzzy inference systems are integrated into the control framework to enable the system to adapt to dynamic operations

Our goal in this research is to use MATLAB to create and implement a strong cyber security system for DC microgrids. The methodology we employ entails the creation and incorporation of a fuzzy controller with the ability to identify irregularities in data streams and differentiate between reputable and malevolent inputs. We can model, simulate, and validate the efficacy of our suggested solution under a variety of operational and attack situations by utilizing MATLAB's flexibility and computing capability.

II. CYBER SECURITY ATTACKS

The utilization of a mathematical model of the system is the only prerequisite for the model-based attack detection technique. Consequently, the detection performance improves with the quality of the model used to describe the dynamics of the system. While many assault detection techniques have been created recently, very little research has included modeling uncertainty in the detection strategy design. Traditional observer-based approaches may not be able to produce accurate detection performance because of parameter fluctuations. As far as we are aware, no studies have been conducted to provide guidance on how to develop and use reliable detection methods for distributed DC microgrids. Therefore, robust cyber-attack detection remains a valuable area for research. To address the above challenges, this paper proposes a parity-based cyber-attack detection scheme for a DC MG cluster. The main contributions of this work are listed as follows.

A. Attack Detection Framework For Dc Microgrids

This research presents a real-time framework for cyber-attack detection that may be implemented on a wide scale, including threshold computation and residual generation. When taking into account the modeling uncertainties of DC microgrids, the limitations of observer-based detection techniques are explored. The system may be efficiently monitored by the suggested attack detection approach even in the presence of unknown load and voltage change situations.

B. Robust Detection Design

In contrast to current detection methods, the suggested residual generation allows for trustworthy attack identification even when there are fluctuations in the parameters. Additionally, a novel multi-objective optimization problem is formulated to improve the sensitivity to attacks. Additionally, an analytical solution using the singular value decomposition approach is offered.

C. Suitable for multiple applications

The suggested attack detection technique can be used in both grid-forming and grid-feeding converters since it is based on the converter model. In addition, keep in mind that converters in a microgrid cluster also facilitate energy conversion and interaction between distinct microgrids.

Therefore, a multiple DC microgrid cluster can likewise use the attack detection technique described in this study.

D. CYBER–PHYSICAL DC MICROGRIDS

This section explains the distributed control and proposed robust detection framework for a DC microgrid.

1) Electrical model of DC microgrids

Considering a microgrid composed of a renewable energy source (RES), a Buck converter and loads, the DC MG cluster can be obtained by interconnecting microgird through power lines, as shown in Fig. 1.

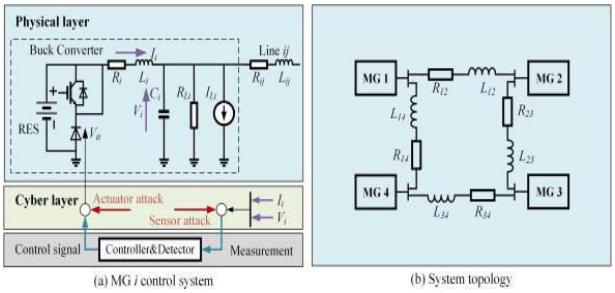

Fig. 1. DC Microgrid Control System

Typically, a ZIP load consisting of a constant power load (P), constant current load (I), and constant impedance load (Z) is assumed for every microgird. As stated in [40], an equivalent impedance load and an equivalent current load can be used to represent the ZIP load following the linearization of the constant power load around the rated voltage point. Fig. 4.11 also shows the local generation unit's structure. Since the suggested detecting method is resistant to unknown loads, the linearization of a constant power load actually has no effect on the detector that is being shown.

E. Attack Detection Design

The design procedure for a DC microgrid detection method is covered in this section. Fig. 1 depicts the suggested detection scheme's organizational structure. The suggested detector consists of residual generation based on parity relations and an appropriate threshold for each MG. In that case, an attack is presumed. It will be demonstrated that the suggested assault detection is resistant to changes in parameters as well as unknown disruptions. For the sake of brevity, the subscript is removed since it has no bearing on the explanation of detection design.

III. EXISTING METHOD

As said, the insufficient data make it unreliable to develop an attack detection system that is resistant to both unknown disturbances and parameter fluctuations. The parity relations of the DC MG, where the historical measurements of previous steps are stored, are examined in order to create an ideal robust detection design. It is possible to construct the parity relation of the DC MG system (2) under discussion by gathering data with a window length of s.

.

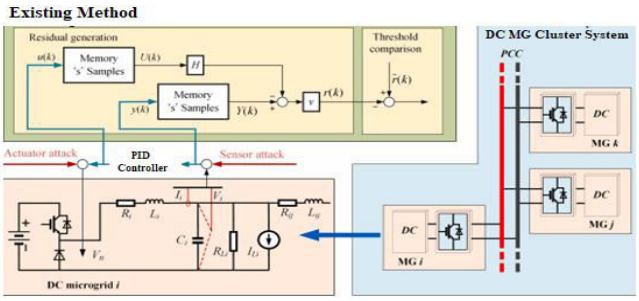

Fig. 2. Existing Parity- Based Attack detection approach

A. PI Controller Based Speed Control

Generally, one of the three approaches—trial and error, evolutionary strategies based on searching, Cohen Coon, Lambda tuning, and Ziegler Nichols—is used to develop the PI based controller. The trial and error method is recommended for PI controller tuning when comparing different approaches since it offers multiple advantages in terms of identifying gain settings and superior performance in motor drive applications. Two crucial factors were the primary focus of the trial-and-error approach for determining the proportional and integral gain for motor driving applications.

Kp and Ki, which were determined through trial and error, have numerical values of 50 and 2, respectively. Reducing error is the PI controller's goal in order to improve drive efficiency. When regulating an induction motor's speed at a constant torque, the closed loop PI controller's goal is to perform better. These PI controller limitations are mostly associated with variable operating conditions. FLC gets around this PI controller constraint.

IV. PROPOSED METHOD

DC microgrids have become a key player in the quickly changing energy distribution environment, offering improved efficiency, more dependability, and greater integration of renewable energy sources. The integrity and stability of microgrid operations are threatened by cyber security risks, which are a major concern because to the growing dependence on digital control and communication technologies. False data injection attacks are one of these risks that can seriously affect power distribution and manipulate control choices.

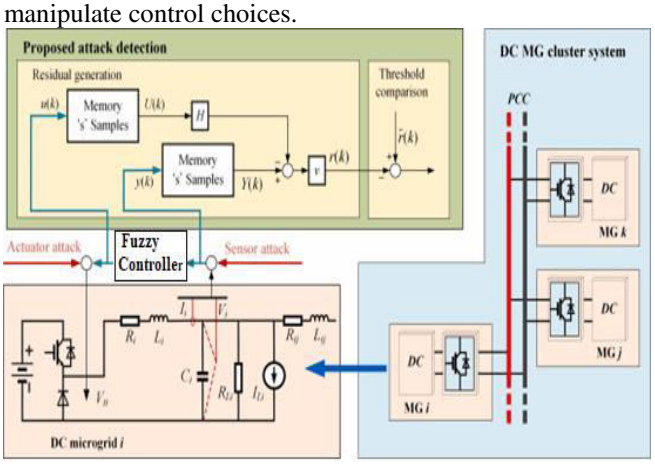

Fig. 3. Proposed system

Advanced cyber security protocols tailored to the unique characteristics of DC microgrids are required to address these challenges. In this case, a mix of state-of-the-art control techniques and strong defense strategies becomes essential. The purpose of this work is to improve the resilience of DC microgrids against fake data injection attacks by combining fuzzy logic control and residual attack detection.

.

A. Operation

1) DC Microgrids:

These localized energy distribution networks operate independently or in conjunction with the main grid, serving critical loads and optimizing power flow. Their decentralized nature makes them susceptible to cyber attacks, necessitating robust security measures to ensure uninterrupted operation.

2) False Data Injection Attacks:

These attacks involve adversaries injecting falsified data into the microgrid's measurement or control systems. By distorting sensor readings or command signals, attackers can manipulate system behavior, compromise stability, and cause financial losses or service disruptions.

3) Fuzzy Controller:

Fuzzy logic control offers a flexible and adaptive approach to managing complex and uncertain systems. By incorporating linguistic variables and fuzzy inference systems, fuzzy controllers can effectively model nonlinear relationships and adapt to dynamic operating conditions, making them well-suited for microgrid control.

4) Residual Attack Detection:

Residual analysis techniques involve comparing measured and estimated system behaviors to detect discrepancies indicative of cyber-attacks. By monitoring residual signals, deviations caused by false data injection attacks can be identified, enabling timely mitigation measures.

B. Methodology

1) System Modeling and Simulation Setup:

Develop a comprehensive model of the DC microgrid system using MATLAB/Simulink, incorporating components such as renewable energy sources, energy storage systems, converters, loads, and communication interfaces.Define the dynamics of the system components, including power generation, energy storage, voltage regulation, and control algorithms.

Establish communication channels between sensors, controllers, and actuators within the microgrid architecture.

2) Fuzzy Controller Design:

Design a fuzzy logic-based controller to regulate power flow, voltage, and frequency within the DC microgrid. Define linguistic variables and membership functions representing system inputs (e.g., voltage, current) and outputs (e.g., control signals). Develop fuzzy inference rules and membership function parameters based on system dynamics and operational requirements. Implement the fuzzy controller within the microgrid model and validate its performance under normal operating conditions.

3) Residual Generation and Attack Detection:

Design algorithms for residual generation based on system observability and state estimation techniques. Define metrics for residual analysis to detect discrepancies between measured and estimated system behaviors.

4) Integration and Cyber Security Framework Development:

Integrate the fuzzy controller with the residual attack detection system within the microgrid simulation environment. Establish communication protocols and data exchange mechanisms between the controller, sensors, actuators, and the attack detection module. Implement cyber security measures, such as encryption, authentication, and intrusion detection, to safeguard communication channels and prevent unauthorized access.

5) Simulation and Evaluation:

Conduct extensive simulations using MATLAB/Simulink to evaluate the performance of the integrated cyber security framework under various operating conditions and attack scenarios. Assess the ability of the fuzzy controller to maintain stable operation and mitigate the impact of false data injection attacks on microgrid performance.

C. Fuzzy Logic Controller

One of the most effective tools for improving electrical equipment is its ability to assess speed controllers quickly while integrating rule-based protocols and human reasoning. Generally speaking, there are three ways to control induction motors: (1) the voltage/frequency approach

(2) regulation of flow Technique
(3) The vector control approach.
The suggested FL controller aims to address two primary tasks: (1) determining the speed of an induction motor and (2) decreasing speed error by utilizing a rules-based system while simultaneously degrading harmonics.

There are two inputs and one output in the FL controller's design. The modulating signal is regarded as the output, and the error and change in error speed as the input. FL controller primarily adheres to the four prerequisite actions, including:

(1) Analog fuzzifier transforms input into fuzzy variables; (2) Fuzzy rules are stored; (3) Inference and related rules are applied; and (4) Fuzzy variables are transformed into actual targets by Defuzzifier.

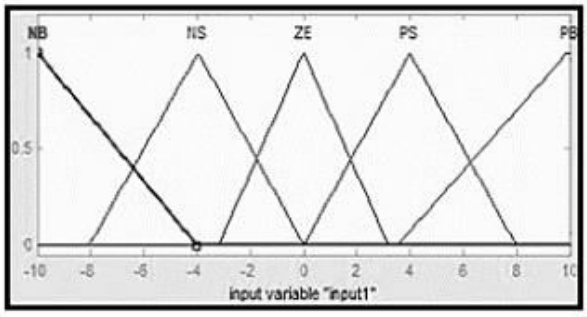

Fig. 4. Proposed system Allocation of range for subsets

e/ce	NB	NS	ZE	PS	PB
NB	ZE	NS	NB	NB	NB
NS	ZE	NS	NB	NS	NB
ZE	PB	PS	ZE	NS	NB
PS	PB	PS	PS	ZE	NS
PB	PB	PB	PB	PS	ZE

Fig. 5. Fuzzy Rules

Two or more relationship values from the fuzzifier input variables make up the fuzzy operator's input. One truth value is the result. If input 1 is stated to represent a mistake, then input 2 represents a changing error. Eight fuzzy subsets make up the linguistic variables; five of these subsets are employed and are explained as follows: Positive error speed Small (PS), Positive error speed Big (PB), Negative error speed Big (NB), Negative error speed Small (NS), and (5) Zero mistake rate (ZE) If the output, let's say, is NS, then all rule-based membership functions will function with it if its value is up to 0.3416.

.

V. Simulation Results

The simulation findings are probably showing the efficacy of two alternative control strategies for identifying fake data injection attacks in cyber security in DC microgrids: one using a fuzzy controller (a proposed way) and the other using a PID controller (an existing method). Simulation outcomes recorded in MATLAB 2013a.

A. Existing Method

With the help of a PID controller, figure 6 most likely depicts the voltage profile of the DC microgrid over time. It could show how constant the voltage is throughout operation or how erratic it gets.

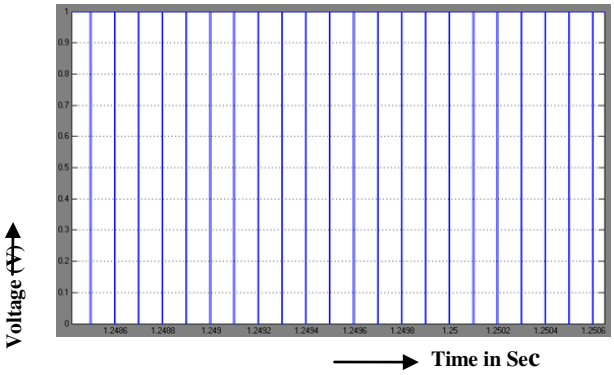

Fig. 6. DC Microgrid Voltage

Figure 7 most likely shows the microgrid's voltage and current waveforms. It might demonstrate how they change over time and reveal any unusual oscillations or disruptions.

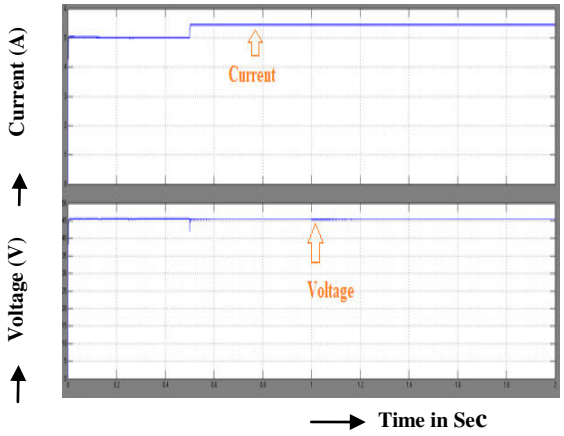

Fig. 7. Current and Voltage wveform

The output voltage waveform in figure 8 is probably the major focus here. It illustrates how the controller reacts to variations in load or disturbances and how effectively it keeps the output voltage steady.

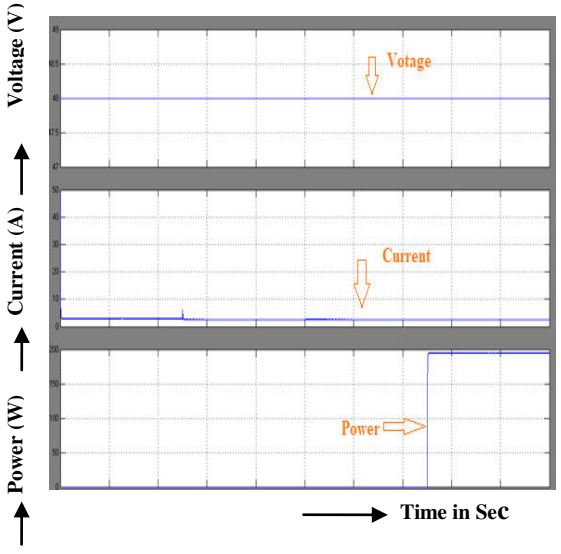

Fig. 8. Output voltage waveform

B. Proposed Method

In proposed method use fuzzy control to improve the performance. The figure 9 shows the fuzzy rules.

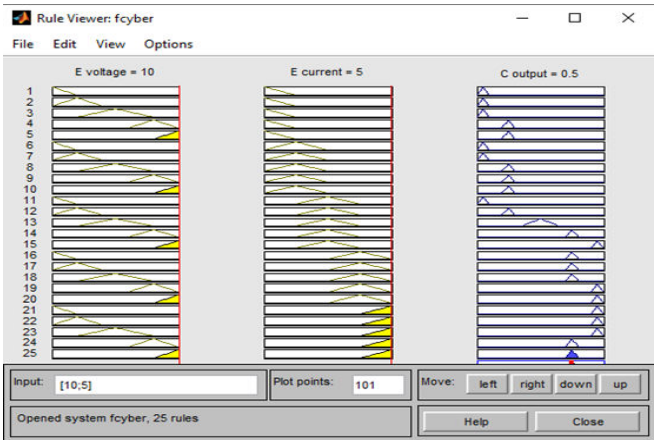

Fig. 9. Fuzzy Rules

Figure 10, which is similar to Fig. 6, most likely depicts the DC microgrid's voltage profile when it is controlled by a fuzzy controller. It enables comparison of the fuzzy controller's performance in sustaining steady voltage levels with that of the current PID controller.

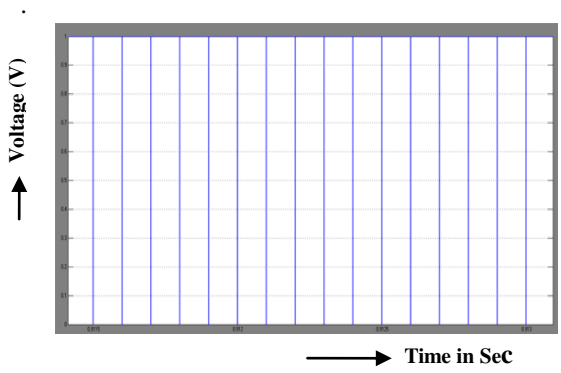

Fig. 10. DC Microgrid Voltage

This figure 11 may provide a combined view of current and voltage waveforms, offering insights into how they interact and whether the fuzzy controller effectively regulates both.

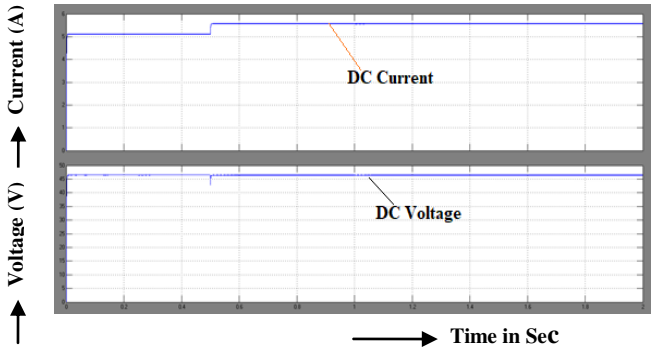

Fig. 11. DC Microgrid Current and Voltage

This figure might be more comprehensive, showing not only voltage and current but also the speed of a motor connected to the microgrid. It allows for assessing the overall performance of the system under the fuzzy controller.

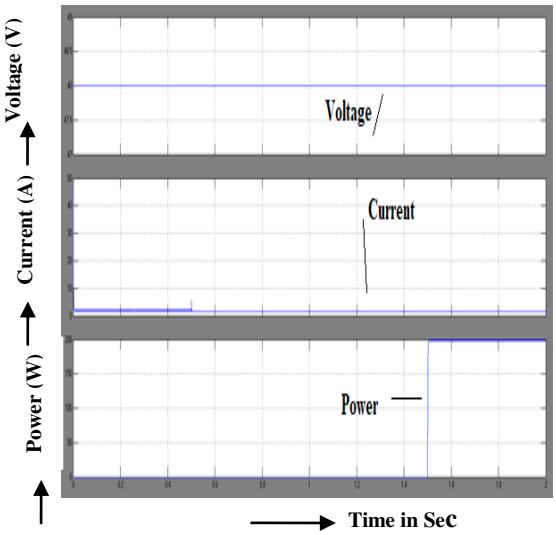

Fig. 12. Voltage ,Current and Speed of Motor

In both cases, the simulation results likely aim to demonstrate the effectiveness of the proposed fuzzy controller in detecting false data injection attacks compared to the traditional PID controller. Metrics such as stability, response time, and robustness against attacks may be evaluated through these figures to justify the adoption of the fuzzy controller for enhancing cyber security in DC microgrids.

VI. CONCLUSION

The development and implementation of a cyber-security framework for DC microgrids using a combination of fuzzy control and residual attack detection represent a significant step towards ensuring the reliability, resilience, and security of modern energy distribution systems. By leveraging fuzzy logic-based controllers and advanced anomaly detection

techniques, we have demonstrated the ability to detect and mitigate false data injection attacks in real-time, thereby safeguarding critical infrastructure and enhancing the trustworthiness of DC microgrid operations.The integration of fuzzy control enables efficient regulation of power flow, voltage, and frequency within microgrids, while residual attack detection provides a robust defense mechanism against cyber threats. Through extensive simulations and evaluations, we have validated the effectiveness of the proposed framework under various operating conditions and attack scenarios, highlighting its ability to maintain stable microgrid operation and mitigate the impact of malicious activities.

Future Scope

Explore and integrate more advanced cyber security techniques such as machine learning-based anomaly detection, deep learning for intrusion detection, and blockchain-based authentication and data integrity verification to enhance the resilience of DC microgrids against cyber threats.

REFERENCES

[1] Lu S-y, Wang L, Lo T-M, Prokhorov AV. Integration of wind power and wave power generation systems using a DC microgrid. IEEE Trans Ind Appl 2014;51(4):2753–61.

[2] Chub A, Vinnikov D, Liivik E, Jalakas T. Multiphase quasi-z-source DC–DC converters for residential distributed generation systems. IEEE Trans Ind Electron 2018;65(10):8361–71.

[3] Mardani MM, Khooban MH, Masoudian A, Dragičević T. Model predictive control of DC–DC converters to mitigate the effects of pulsed power loads in naval DC microgrids. IEEE Trans Ind Electron 2018;66(7):5676–85.

[4] Villalonga A, Beruvides G, Castaño F, Haber R. Cloud-based industrial cyberphysical system for data-driven reasoning. a review and use case on an industry 4.0 pilot line. Statistics 2020;34:35.

[5] Tan S, Wu Y, Xie P, Guerrero JM, Vasquez JC, Abusorrah A. New challenges in the design of microgrid system. IEEE Electrif Mag 2020;8(4):98–106.

[6] Hug G, Giampapa JA. Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. IEEE Trans Smart Grid 2012;3(3):1362–70.

[7] Zhao J, Mili L, Wang M. A generalized false data injection attacks against power system nonlinear state estimator and countermeasures. IEEE Trans Power Syst 2018;33(5):4868–77.

[8] Zuo S, Beg OA, Lewis FL, Davoudi A. Resilient networked AC microgrids under unbounded cyber attacks. IEEE Trans Smart Grid 2020;11(5):3785–94.

[9] Liu S, Hu Z, Wang X, Wu L. Stochastic stability analysis and control of secondary frequency regulation for islanded microgrids under random denial of service attacks. IEEE Trans Ind Inf 2018;15(7):4066–75.

[10] Tan S, Xie P, Guerrero JM, Vasquez JC, Han R. Cyberattack detection for converter-based distributed dc microgrids: Observer-based approaches. IEEE Ind Electron Mag 2021;2–12. http://dx.doi.org/10.1109/MIE.2021.3059996.

[11] Farwell JP, Rohozinski R. Stuxnet and the future of cyber war. Survival 2011;53(1):23–40.

[12] Conti JP. The day the samba stopped [power blackouts]. Eng Technol 2010;5(4):46–7.

[13] [Case DU. Analysis of the cyber attack on the ukrainian power grid. Electr Inf Shar Anal Cent (E-ISAC) 2016;388.

[14] Lee C-H, Chen B-K, Chen N-M, Liu C-W. Lessons learned from the blackoutaccident at a nuclear power plant in Taiwan. IEEE Trans Power Deliv2010;25(4):2726–33.

[15] Peng C, Sun H, Yang M, Wang Y. A survey on security communication and control for smart grids under malicious cyber attacks. IEEE Trans Syst Man Cybern: Syst 2019;49(8):1554–69. http://dx.doi.org/10.1109/TSMC.2018.2884952.

[16] Tan S, Guerrero JM, Xie P, Han R, Vasquez JC. Brief survey on attack detection methods for cyber-physical systems. IEEE Syst J 2020.

ABOUT AUTHORS

1. Mr. B Theja, studying M.Tech II Year., (PE), Department of Electrical and Electronics Engineering, Kuppam Engineering College, KES Nagar, Kuppam, Andhra Pradesh 517425 India.

2. Dr. Velappagari Sekhar, Associate Professor & HOD, Department of Electrical and Electronics Engineering, Kuppam Engineering College, KES Nagar, Kuppam, Andhra Pradesh 517425 India
.

3. Mr**.** V.Niranjan, Lecturer, Department of Electrical and Electronics Engineering, Dr. Y.C. James Yen Government Polytechnic, Kuppam, Andhra Pradesh 517425 India

4. Mr. M Komal Kumar, studying M.Tech II Year., (PE), Department of Electrical and Electronics Engineering, Kuppam Engineering College, KES Nagar, Kuppam, Andhra Pradesh 517425 India.