CHAPTER 1

INTRODUCTION

A microgrid is a group of interconnected loads and distributed energy resources with defined electrical boundaries that constitute a local electric power system at distribution voltage levels and can operate in either grid-connected or island mode [7]. Micro-grids can run independently and locally by disconnecting from the traditional grid. Microgrids are self-contained energy systems that may function autonomously while servicing a specific area or community. They improve grid resilience by allowing them to separate from the main grid while continuing to operate during outages. Micro-grids make it easier to integrate renewable energy sources such as solar farms and electric vehicles, while also minimizing energy losses during transmission and distribution. There are three types of microgrid topologies: alternating current (AC), direct current (DC), and hybrid. AC micro-grids use converters to connect AC power sources to an AC bus, whereas DC micro-grids connect DC power sources directly to a DC bus. Hybrid microgrids integrate both alternating current and direct current power sources, allowing bidirectional power transfer between AC and DC buses. These various topologies provide flexibility in managing energy flow and enable the efficient use of diverse power sources inside micro-grids.[7][8]

1.1 BACKGROUND

The grid internet link exposes the grid to several types of threats, including Advanced Persistent Threats (APT), Distributed Denial-of-Service (DDoS), botnets, and zero-days. Only a few instances are Stuxnet, Duqu, Red October, and Black Energy. Since 2010, there has been an increase in the number of incidents involving industrial security. Bias injection attacks, zero dynamics assaults, denial of service (DoS) attacks, eavesdropping attacks, replay attacks, stealthy attacks, covert attacks, and dynamic false data injection attacks are all examples of cyber intrusions into cyber-physical systems (CPSs). These attacks assaults can still be categorised based on the one or more security criteria they jeopardise.[1]

Replay attacks, which entail an attacker recording data delivered via a communication network and replaying it later, are another type of DC microgrid attack. Because they exhibit the same statistical behaviour as normal communication, these attacks are difficult to detect using standard monitoring techniques. Many techniques inspired by watermarking in the multimedia industry have been proposed. One method involves adding a time-varying watermark to a system's input signal, which

changes the steady-state characteristic statistics. This change allows the monitoring system to recognise the presence of an assault.

Another technique is to directly add a watermark signal to the sensor measurements sent to the monitoring scheme and controller. Along with replay attacks, stealthy data injection assaults are being studied. To prevent unauthorised data injection, one technique for countering these attacks is to encode sensor measurements using a coding matrix that is presumed to be unknown to the attacker. All existing methods for detecting replay assaults, however, assume a centralised monitoring scheme, which is inefficient for distributed control microgrids (DCmGs) due to increasing communication costs. As a result, in this exploratory work, the distributed watermarking technique for monitoring microgrids is used. The distributed approach eliminates the requirement for all distributed generation units (DGUs) to communicate with a single location.[2]

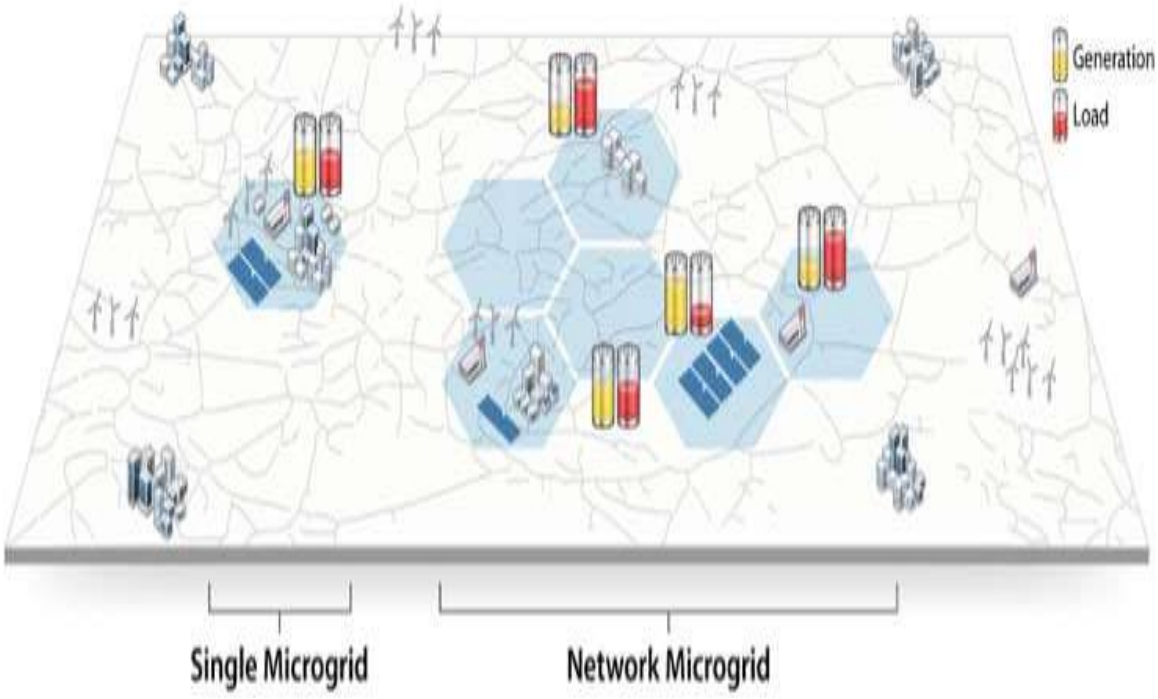

Figure 1: MICROGRID

A single DC microgrid is a localized electrical system that operates on direct current (DC) instead of alternating current (AC). It consists of a collection of energy sources (such as solar panels, wind turbines, or batteries), energy storage devices, and loads (consumers) that are connected together in a small-scale power grid. The DC microgrid can operate independently or be connected to the main AC grid.

A networked DC grid, also known as a DC power system, refers to a collection of interconnected DC microgrids or DC-based power sources and loads that are connected together in a larger-scale power distribution network. In a networked DC grid, multiple DC microgrids or DC-based systems are linked together to form a larger and more complex electrical network. The concept of a networked DC grid is gaining attention as a potential solution for efficient power distribution and integration of renewable energy sources.[11]

1.2 OBJECTIVE

The main objectives are as follows:

- To create a simulation model for DC microgrid for the analysis of replay attack scenarios using MATLAB.
- To compare between the normal operation and attack scenarios for dc microgrid.
- To monitor the impact of Replay attack that can only be detect using Dynamic watermarking algorithm

1.3 PROBLEM STATEMENT

- Utilities lack a comprehensive set of indicators and evaluation tools for measuring the security features of smart grid infrastructures.
- The number of cyber-attacks against the grid system has increased.
- Cyber-attacks has a variety of effects, including blackouts, the loss of secret information, and even physical harm to power devices.
- Security threats and network performance have a significant impact on smart grid applications.

CHAPTER 2.

LITERATURE SURVEY

[1] A basic framework for detecting cyber-attacks on cyber-physical DC microgrids, by Subham Sahoo, Sukumar Mishra, Jimmy Chih-Hsien Peng and Tomislav Dragicevic.

The vulnerability of typical cooperative approaches in DC microgrids to fake data injection is thoroughly examined. Furthermore, the modelling of stealth assaults that confuse distributed observers is performed utilizing necessary and sufficient conditions. To overcome this issue, a cooperative vulnerability factor technique is developed that uses the PI output of the voltage observer to track changes for each agent and provides an accurate identification approach for the attacked agent(s). To improve fidelity, it is cross-coupled with the secondary current sublayer, allowing it to work in the worst-case scenario of an attack. Its resilience is assessed by comparing simulation and experimental findings for fake data injection and stealth assaults on numerous sensors or links.

[2] A distributed watermarking approach that can be used to support a monitoring scheme for validating information exchanged between DGUs in a DcmG, by Alexander J. Gallo, Mustafa S. Turan, Francesca Boem, Giancarlo Ferrari-Trecate and Thomas Parisini.

The problem of replay attacks in the communication network between Distributed Generation Units (DGUs) of a DC microgrid is examined. The DGUs are regulated through a hierarchical control architecture, and are networked to achieve secondary control objectives The analysis of the monitoring method under replay attack without the additive watermark reveals that the assault is undetectable as long as data is recorded in steady state. In order to detect the action of an attacker, a distributed attack detection scheme based on multiple Unknown Input Observers (UIOs) has been introduced (Gallo et al., 2018). This monitoring strategy is capable of detecting whether the communication is subject to an attack, based on limited knowledge of the neighbors' dynamics, and on information regarding the bounds on the disturbance. The watermark is then introduced, and a condition on the watermark is derived to ensure detection. The paper suggests a basic watermark signal design and demonstrate its usefulness via simulation. In the future, we intend to investigate non-ideal communication networks and offer a more refined watermarking signal.

[3] A stealth Cyber Attack Detection Strategy for DC Microgrids by Sahoo, Subham & Mishra, Sukumar & Peng, Jimmy & Dragicevic, Tomislav, (2018).

This paper proposes a cooperative mechanism for detecting potentially deceptive cyber-attacks that attempt to disregard average voltage regulation & current sharing in cyber-physical DC microgrids. Considering a set of conventional cyber-attacks, the detection becomes fairly easy for distributed observer-based techniques. However, a well-planned set of balanced attacks, termed as the stealth attack, can bypass the conventional observer-based detection theory as the control objectives are met without any physical error involved. In this paper, we discuss the formulation & associated scope of instability from stealth attacks to deceive distributed observers realizing the necessary & sufficient conditions to model such attacks. To address this issue, a novel cooperative vulnerability factor (CVF) framework for each agent is introduced, which accurately identifies the attacked agent(s) under various scenarios. To facilitate detection under worst cases, the CVFs from the secondary voltage control sublayer is strategically cross-coupled to the current sublayer, which ultimately disorients the control objectives in the presence of stealth attacks and provides a clear norm for triggering defense mechanisms. Finally, the performance of the proposed detection strategy is simulated in MATLAB/SIMULINK environment and experimentally validated for FDI & stealth attacks on sensors and communication links.

[4] Grid attack analyzer, a framework for smart grid cyber- attack analysis, by Tan Duy Le, Mengmeng Ge, Adnan Anwar, Seng W Loke, Razvan Beuran, Robin Doss and Yasuo Tan.

Grid attack analyzer—Cyber Attack Analysis for Smart Grids is built on the analytical modelling method used in general smart grid cybersecurity training. Grid Attack Analyzer receives as input the smart grid model, security parameters, and database. Grid attack analyzer— Cyber-attack analysis for Smart Grids is built on the analytical modelling method used in general smart grid cybersecurity training.

Grid Attack Analyzer uses the smart grid model, security settings, and database as input to prepare the environment for the analysis session and calculates security metrics using the preprocessing components to enable the analysis of various attack types. During the vulnerability analysis process, Grid Attack Analyzer is strengthened by capturing all possible attack vectors and computing the values of specified security metrics. Furthermore, the attack graph can be automatically constructed to capture assault paths.

[5] Grid attack sim, framework for smart grid attack co-simulation. 2020 A paper by Tan Duy Le, Adnan Anwar, Seng W. Loke, Razvan Beuran and Yasuo Tan.

This paper suggests cybersecurity experiences that can be achieved by conducting training using a smart grid co-simulation, which is the integration of at least two simulation models. However, there has been little effort to research attack simulation tools for smart grids. In this research, this paper first review the existing research in the field, and then propose a smart grid attack co-simulation framework called GridAttackSim based on the combination of GridLAB-D, ns-3, and FNCS. The proposed architecture allows us to simulate smart grid infrastructure features with various cybersecurity attacks and then visualize their consequences automatically. Furthermore, the simulator not only features a set of built-in attack profiles but also enables scientists and electric utilities interested in improving smart grid security to design new ones. Case studies were conducted to validate the key functionalities of the proposed framework. The simulation results are supported by relevant works in the field, and the system can potentially be deployed for cybersecurity training and research. It delivers a detailed review of previous initiatives in the field before presenting Grid attack sim, our framework for smart grid attack co-simulation. A comprehensive smart grid attack co-simulation tool, a user-friendly GUI, an extended attack pattern library with attack schedule, and result visualization functions are included in the framework. Case studies with the simple test feeder and IEEE 13 Node models were also performed to validate our system.

[6] ASTORIA: A framework for attack simulation and evaluation in smart grids 2018, by Alexandre Gustavo Wermann; Marcelo Cardoso Bortolozzo; Eduardo Germanoda Silva; Alberto Schaeffer-Filho.

ASTORIA: A framework for attack simulation and evaluation in smart grids.

This paper proposes ASTORIA, a framework developed to allow the simulation of attacks and the evaluation of their impact on Smart Grid infrastructures, using closely-related real devices and real topologies comprising both power gridelements as well as ICT and networking equipment. ASTORIA can be used by Smart Grid operators not only to analyze the impact of malicious attacks and other security threats in different components, but also to permit the development and evaluation of anomaly detection techniques in a simulation environment. Further, It creates evaluation scenarios illustrating customizable Smart Grid topologies, comprising sensors, master and remote stations, and using an extensible set of attack profiles.

CHAPTER 3.

COMPONENTS REQUIRED

MATLAB (acronym for "MATrix LABoratory") is a proprietary multi-paradigm programming language and numeric computing environment developed by mathworks. MATLAB supports matrix manipulation, function and data visualisation, algorithm implementation, user interface building, and interfacing with programmes written in other languages. Although MATLAB is primarily designed for numerical computation, an optional toolbox that employs the MuPAD symbolic engine provides access to symbolic computing capabilities. Simulink, a separate software, includes graphical multi-domain simulation and model-based design for dynamic and embedded systems. MATLAB will have over 4 million users worldwide by 2020.[13] They have backgrounds in engineering, physics, and economics. In 2017, over 5000 colleges and institutions around the world used MATLAB to support education and research.[14]

Simulink is a MATLAB-integrated simulation and model-based design environment for embedded and dynamic systems. Simulink is a data flow graphical programming language tool for modelling, modelling, and analysing multi-domain dynamic systems. Simulink was also created by MathWorks. It functions primarily as a graphical block diagramming tool with a collection of block libraries that are customisable. It enables to import MATLAB algorithms into models and export simulation data for additional analysis into MATLAB. Simulink is capable of design simulation, autonomous code generation, testing and verification of embedded systems at the system level. It can be used with a number of additional MathWorks add-on products as well as hardware and software from other companies. Simulink may use analysis of model coverage, requirements traceability, and modelling style to systematically verify and validate models.With the help of Simulink Design Verifier, you may find design flaws and create test case scenarios for model checking.[13]

3.1COMPONENTS REQUIRED

1.Distribution Generation Unit:

The circuit contains average value DC-DC converter which acts as a Distribution generation unit. A DC-to-DC converter is an electronic circuit or electromechanical device that converts a source of direct current (DC) from one voltage level to another. It is a type of electric power converter. Power levels range from very low (small batteries) to very high (high-voltage power transmission).

a) Voltage controller unit: It is used to control the voltage level. This block consists of pid controller, Vin, Duty cycle block, resistor, capacitor and many more.

b) Current controller unit: It operates by utilizing feedback mechanisms. This means they continually measure the actual current flowing in a circuit, compare it to the desired current (set- point), and then adjust the power device's operation to eliminate any difference.

c) V ref: It is used to create a reference voltage that can be compared to the actual value.

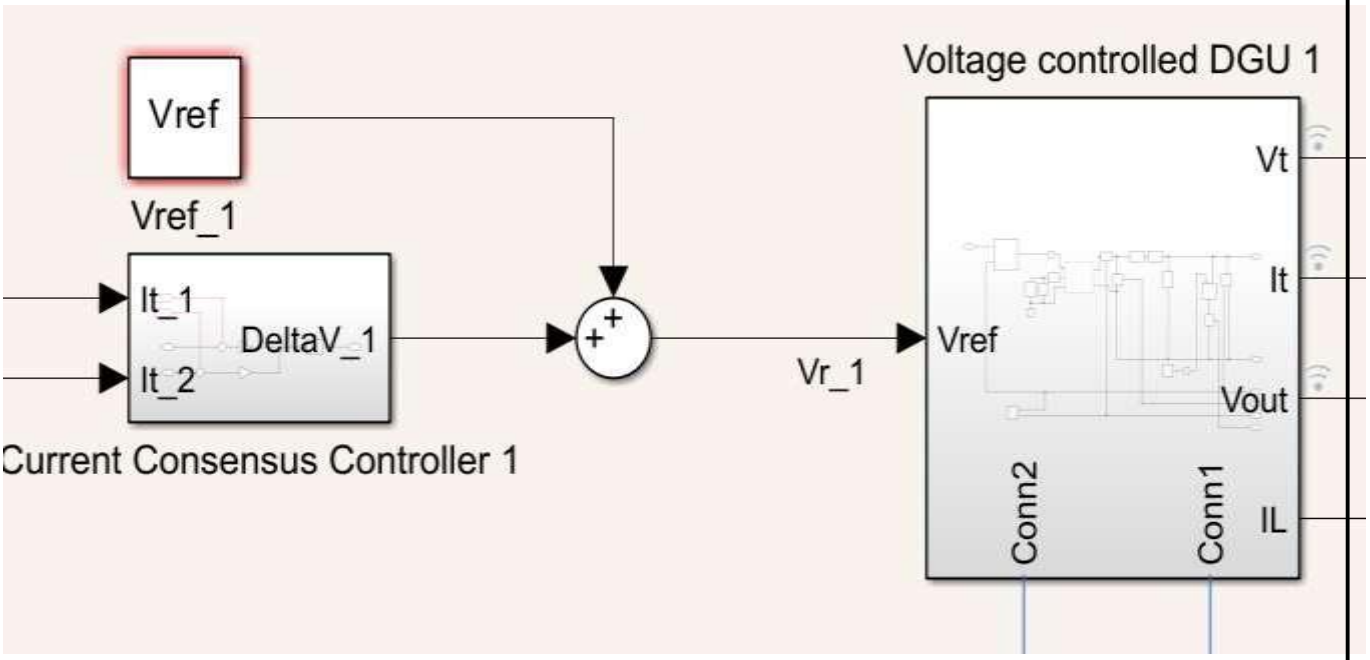

Figure 2: Distribution Generation unit

2. Watermark Add Block:

The model injects watermarks into voltage and current measurements communicated to the current consensus controller. A time-varying signal, unknown to the attacker, as a watermark and use the residuals generated by an observer to detect any modifications or false data injections to the signals in the communication channel. The watermark signal is a periodic sawtooth wave, which the add Watermark subsystems in the model inject into the voltage and current measurements communicated to the current consensus controller.

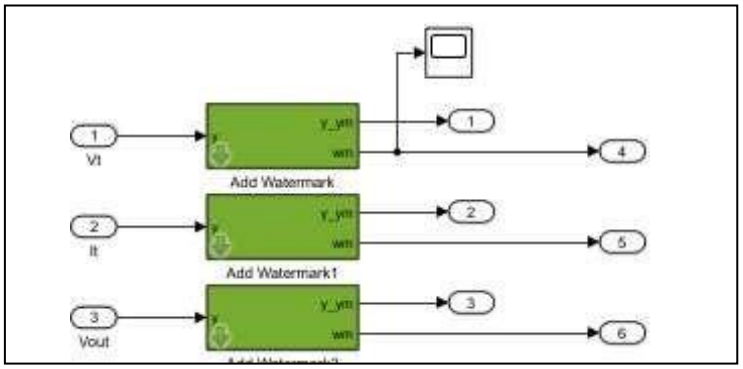

Figure 3: Watermark Add Block

3. Watermark removal block:

This subsystem subtracts the watermark signal from the feedback before the subsystems compute the reference voltage adjustment and construct the observer residuals.

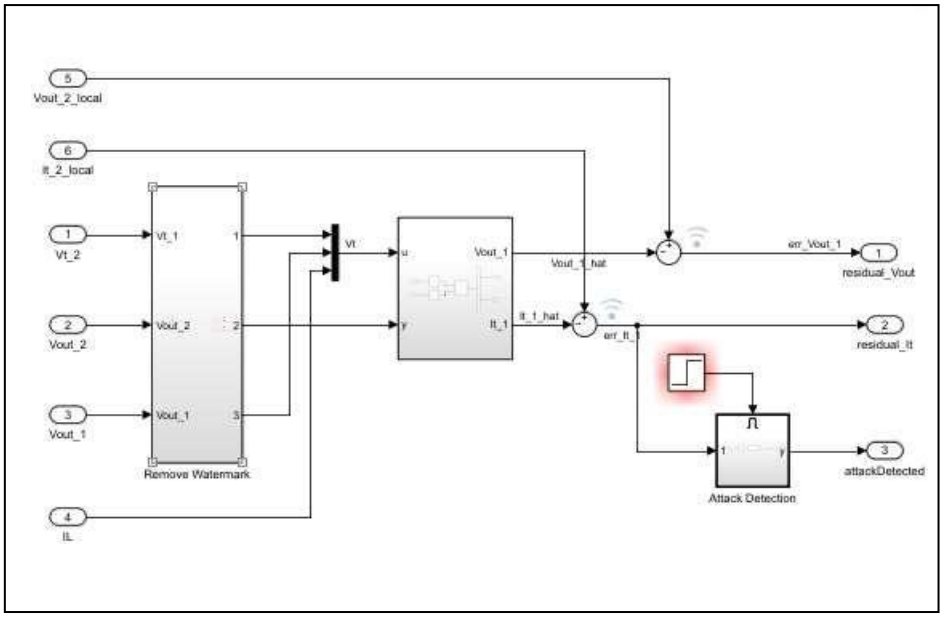

Figure 4: Watermark Remover Block

4. Line system:

This block is used to connect between different DGU and consist of resistors, inductors, reference and solvers.

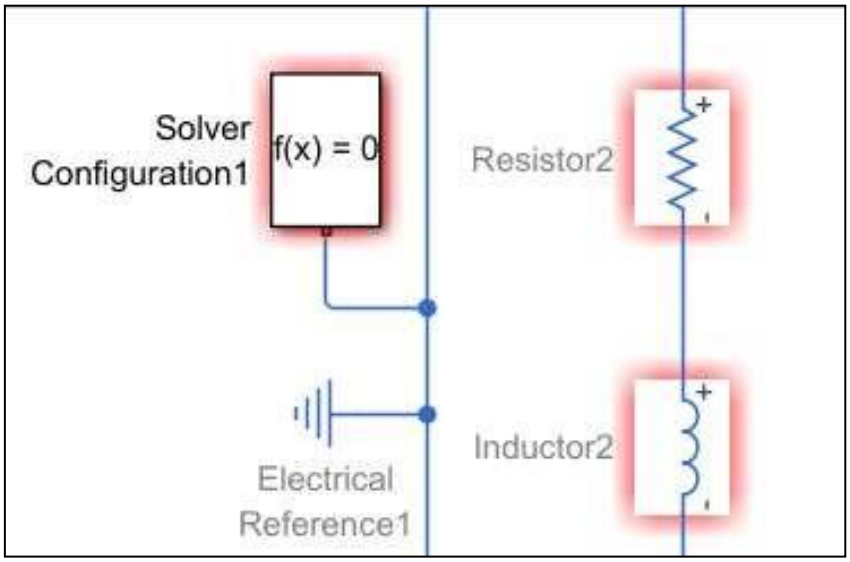

Figure 5: Line System block

5. Controller block:

This serves as a communication link between the two dc-dc converters. This is vulnerable to a fake data injection attack.

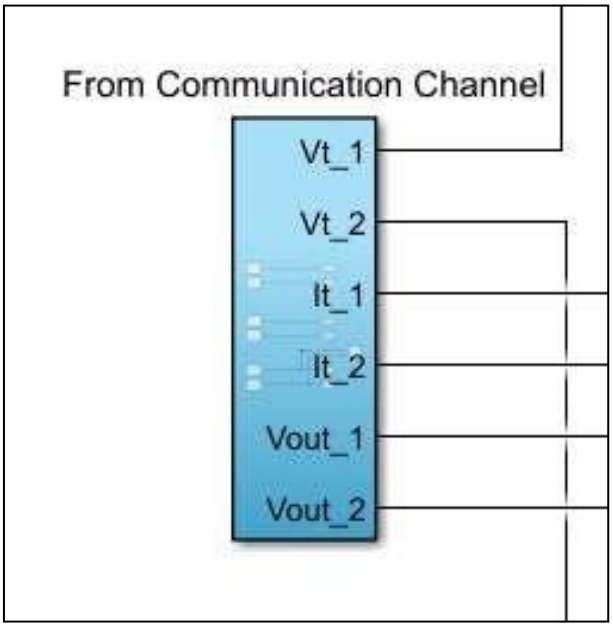

Figure 6: Contoller Block

6.Kalman filter:

The Kalman Filter block to estimate states of a state-space plant model given process and measurement noise covariance data. The state-space model can be time-varying. A steady-state Kalman filter implementation is used if the state-space model and noise covariance matrices are all time-invariant, and a time-varying Kalman filter is used otherwise. A Kalman filter provides the optimal solution to the continuous or discrete estimation problems in Continuous-Time Estimation (System Identification Toolbox) and Discrete-Time Estimation (System Identification Toolbox).[13]

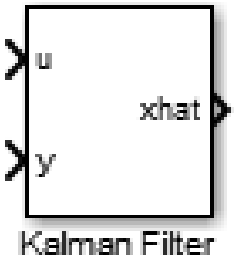

Figure 7: Kalman's Filter

7.Replay Attack Block:

A replay attack is when a malicious agent can observe the signals in the communication channel and then replace current transmitted measurements with delayed recorded observations. This attack delays the signals in the communication channel. It is particularly deceptive when the system is at steady state.

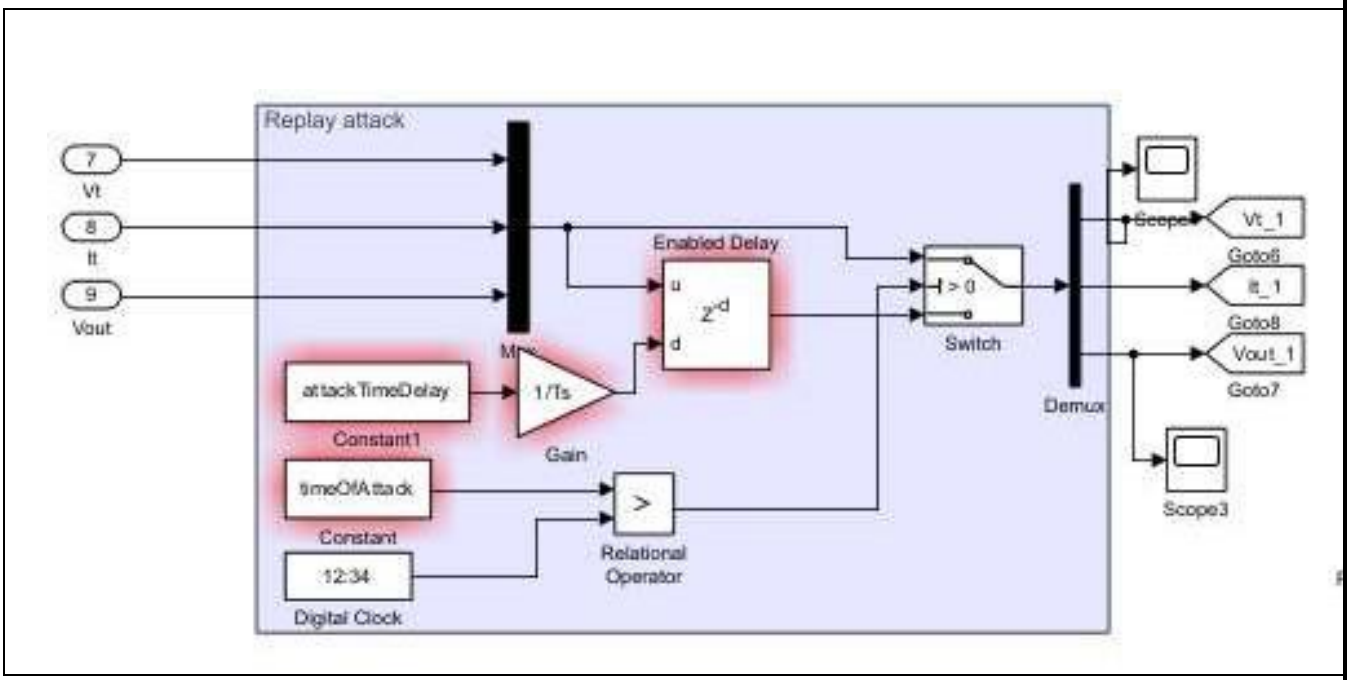

Figure 8: Replay Attack Block

CHAPTER 4.
METHODOLOGY

4.1 BLOCK DIAGRAM

The block diagram shows the working flow of our system. The physical units act as the distribution generation unit for the DC microgrid. The system forms a closed loop where the feedback can be compared

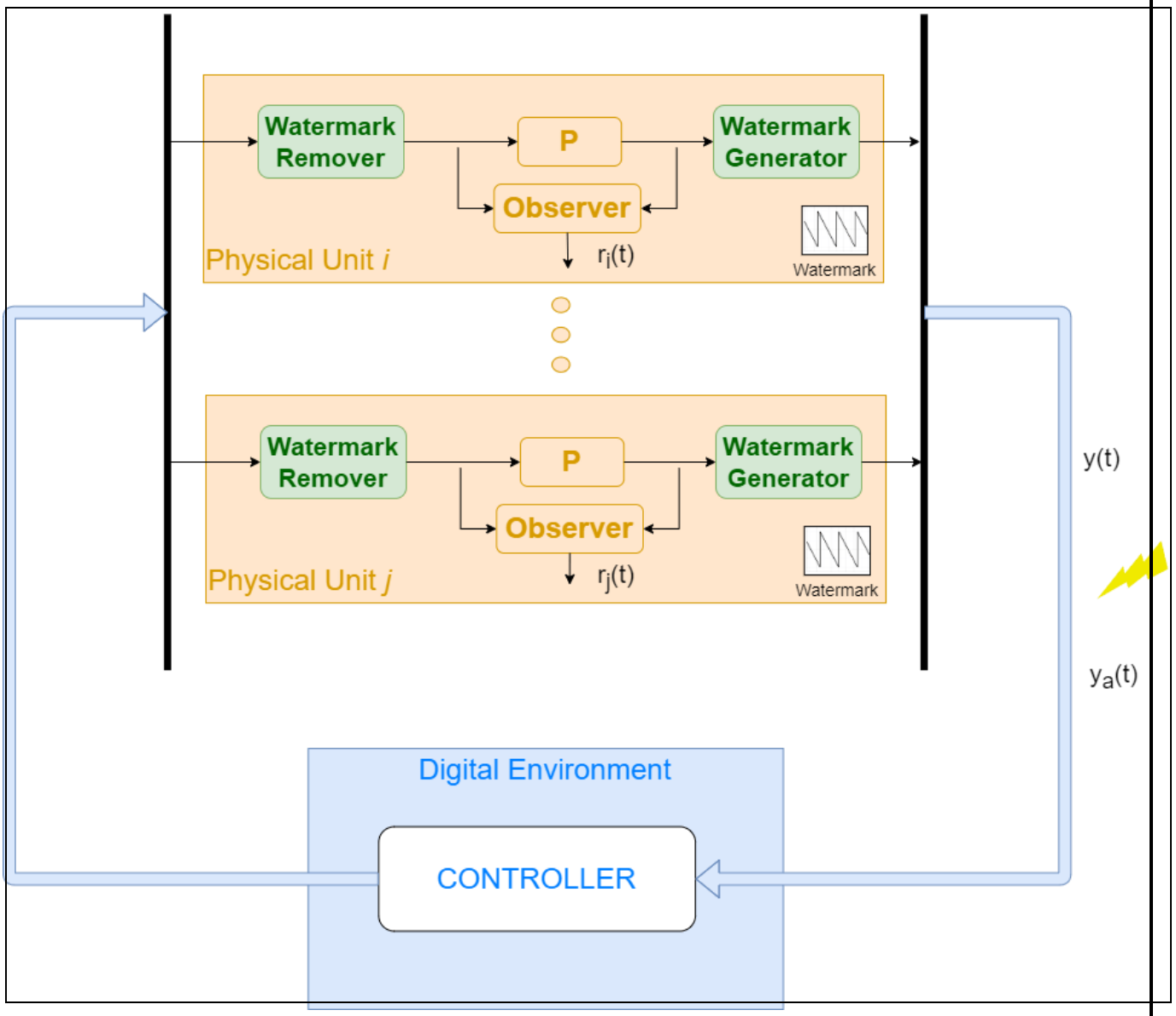

Figure 9: Block Diagram for proposed architecture

In a cyber-physical system (CPS), they utilise distributed watermarking to identify replay assaults. A DC Microgrid (DCmG) is a linked network of distributed generation units (DGU) that reflect physical

systems and are controlled by current consensus loops that are responsible for load sharing across several grids. This architecture necessitates communication between the line currents of each DGU.

The communication channel is vulnerable to attacks that can introduce misleading information and cause the central current consensus loop to behave abnormally. A replay attack, for example, delays the signals in the communication channel. The watermark block generates a time-varying signal that is unknown to the attacker as a watermark and uses the residuals generated by an observer to detect any alterations or fake data injections into the communication channel signals.

An attacker can use replay attacks to record data carried over a communication network and then replay it, substituting actual communication signals with delayed data. To identify an attack, a time-varying watermark is added to a system's input signal in order to change the steady-state characteristic statistics, allowing the monitoring scheme to detect the presence of an attack.[2]

4.1 CIRCUIT DIAGRAM

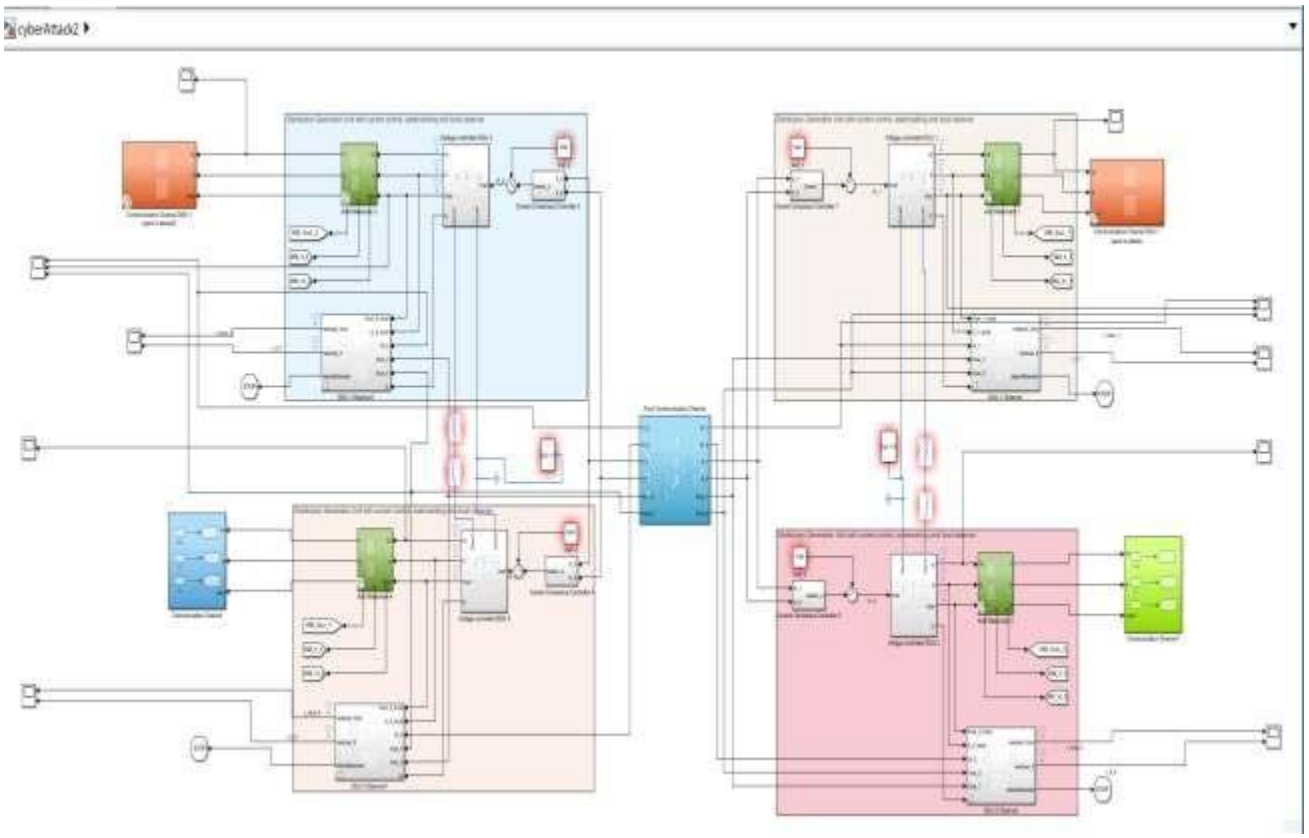

Figure 10 : Circuit Diagram of the model

Figure 10 depicts the Simulink model consisting of 4 DGU's which are interconnected with each other. DGU 1 and DGU3 have replay attack module for the attack on the communication module.

4.2 WORKING PRINCIPLE

Replay assaults are typically undetectable. To identify a replay attack, we add a time-varying signal [i, j] (t) to the data transferred from DGU i to DGU j, similar to the idea behind sensor watermarking (Ferrari and Teixeira, 2017). The preliminary work the following is presumed to be free of bias in the consensus scheme's performance. Watermark [i, j] (t) applied to y [I, j] (t) is known exactly for all t by both DGU i and DGU j. △ [2].

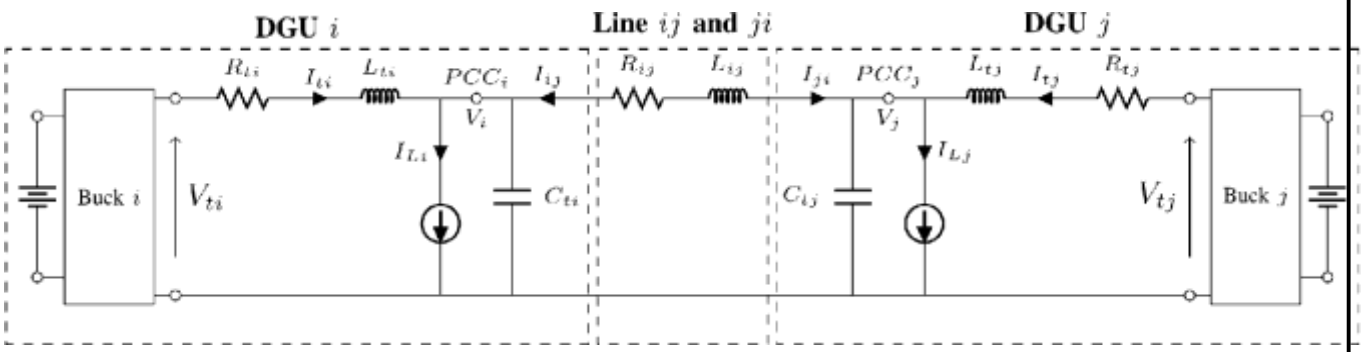

Figure 11: Circuit Diagram of Distribution Generation unit

A distributed generation microgrid (DCmG) is an interconnected system of distributed generating units (DGU) that reflect physical systems and are governed by current consensus loops that are responsible for load sharing across numerous units. The Figure 11 shows the connection between two DGUs architecture necessitates communication between the line currents of each DGU. The communication channel is vulnerable to attacks that can introduce misleading information and cause the central current consensus loop to behave abnormally. A replay attack, for example, delays the signals in the communication channel. The DCmG is made up of two linked distributed generation units that are modelled using the Average-Value DC-DC Converter.

The proposed system has three modes: Attack mode, Observer mode, and Watermarking mode. First, we disable all modes, then define the DGU parameters, power line parameters, and vary the load current for the first unit to show the voltage and line current transients, as both units share the changed load and PID controller parameters. After all specifications have been applied, the usual state of the circuit is displayed. A replay attack occurs when a hostile agent observes the signals in the communication channel and then replaces the current sent measurements with delayed recorded data. This assault causes the signals in the communication channel to be delayed. It is especially deceiving when the system is at rest.

$$y\ a(t)=y(t)+\beta(t-Ta)\ [-y(t)+y(t-t0)] \quad \text{---------- eq(1)}$$

here,

β(t-Ta) denotes an activation function that begins at time Ta and delays the signal y(t) by t0, and y a(t) denotes the modified signal.

When the load fluctuates, the attack causes undesirable behavior. The existing consensus control does not detect variations in line current caused by the communication channel delay.

As a watermark, employ a time-varying signal that is unknown to the attacker and use the residuals generated by an observer to identify any alterations or fraudulent data injections to the signals in the communication channel.

The watermark signal is a periodic saw-tooth wave that is injected into the voltage and current measurements communicated to the current consensus controller by the Add Watermark subsystems in the model.

The Remove Watermark subsystems delete this signal from the feedback before computing the reference voltage adjustment and generating the observer residuals.

The model calculates the model states by employing a linear Kalman filter and the following model[14]

$$Vi(t)=(1/C_{ti})I_{ti}(t)-(1/C_{ti}R_{ij})V_i(t)+(1/C_{ti}R_{ij})V_j(t)-(1/C_{ti}I_{Li}(t)\cdot \quad \text{----------eq(2)}$$

$$Iti(t)=-1/L_{ti}Vi(t)-R_{ti}/L_{ti}I_{ti}(t)+1/L_{ti}V_{ti}(t) \quad \text{---------- eq(3)}$$

The watermark signal converts the delay introduced by the attack in the signals into a disturbance. As a result, the system detects an assault when the observer produces a nonzero residual. The watermark signal's amplitude must be properly adjusted to allow detection of a repeat attack while not allowing currents to surpass the rated capacity prior to detection.[2]

CHAPTER 5
RESULT AND DISCUSSION

5.1 OUTPUT WAVEFORM

5.1.1 NORMAL CONDITION

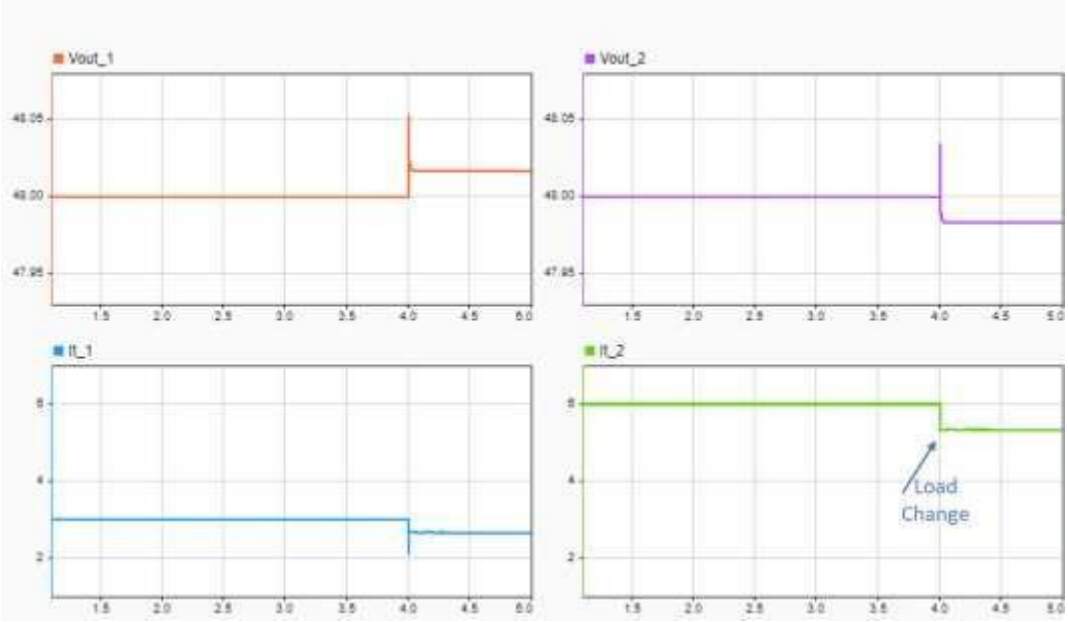

Figure 12: Normal condition waveform

5.1.2 ATTACK CONDITION

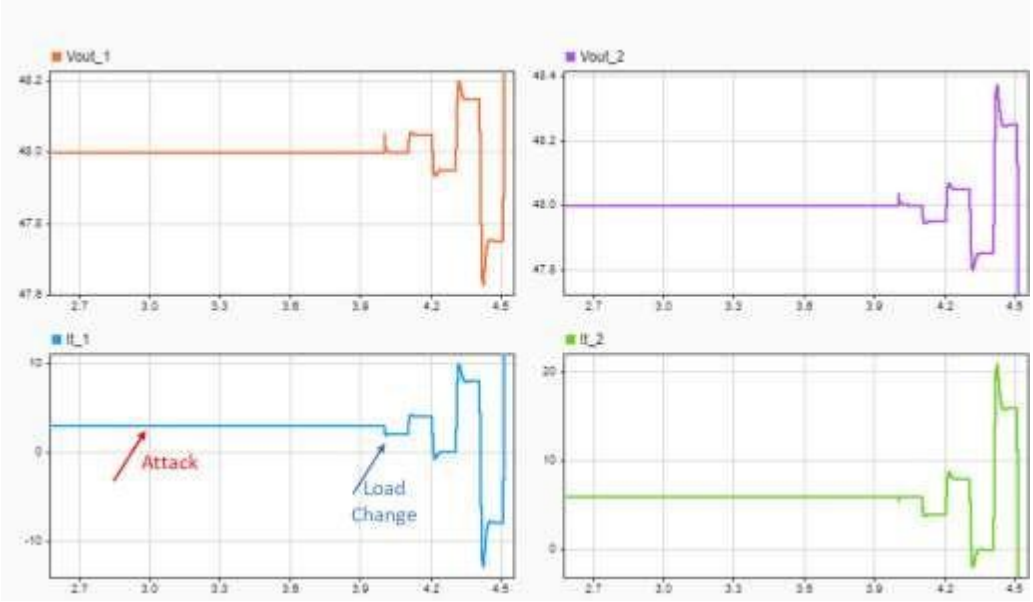

Figure 13: Attack condition waveform

5.1.3 DETECTION CONDITION

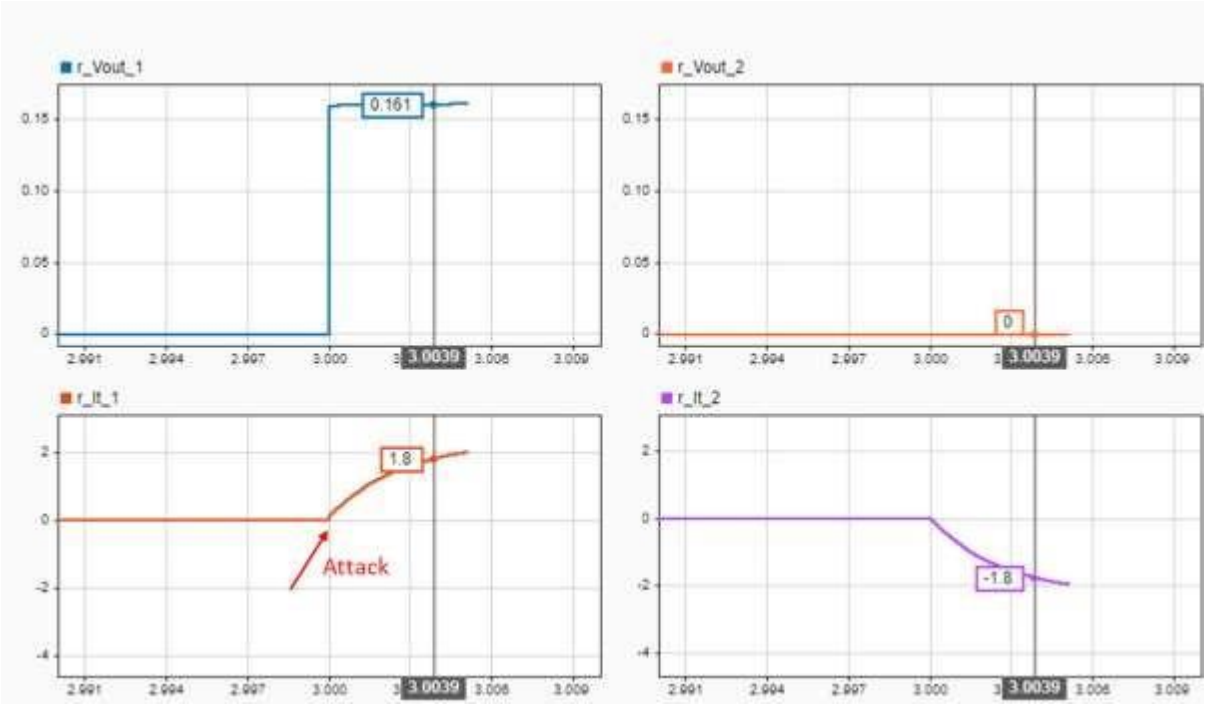

Figure 14: Detected condition waveform

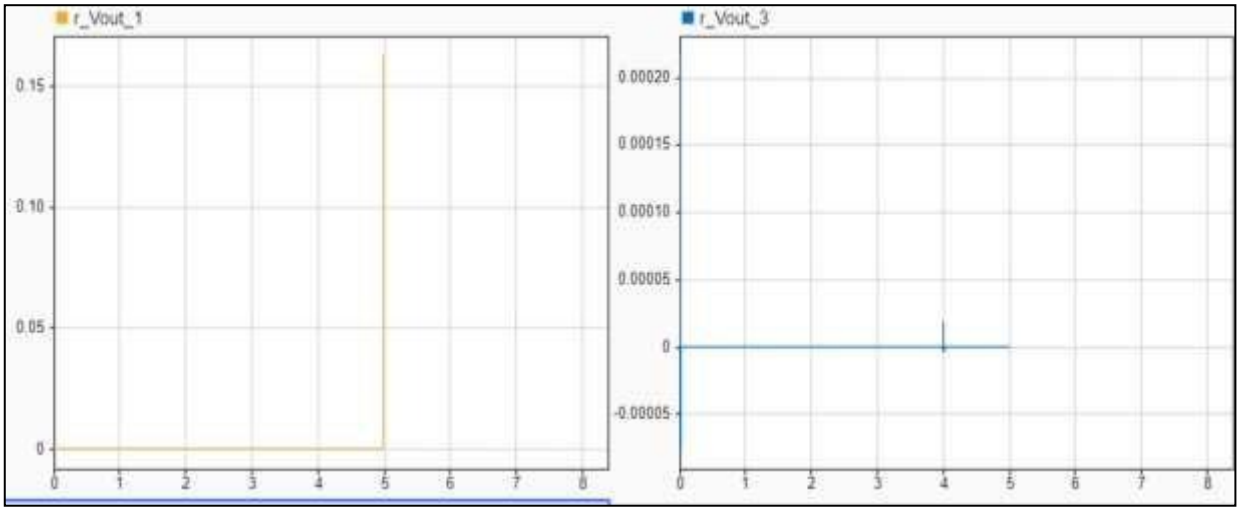

Figure 15: Detected condition waveform before DGU 3 attack time

5.2 RESULT

In a normal operating condition, the four interconnected systems work seamlessly without any errors. They are designed to function together, as illustrated in Figure 12. However, to demonstrate that a load is connected at t=4 seconds, a change in the load can be observed within the system.At this stage, the attack mode is not activated, meaning the system is secure and unaffected by any malicious activities. The system operates in a steady state, and any potential attacks go unnoticed.

However, when the attack mode is enabled to a high level, an attack is initiated at t=3 seconds, as shown in Figure 13. Initially, this attack remains undetected while the system is in a steady state. However, at t=4 seconds, the load shifts, and inaccurate measurements at the consensus controller led to an unstable system. As a result, the uncontrolled line currents exceed the rated capacity, as depicted in the bottom row of the plot. Within 300 milliseconds of the load change, the local Distributed Generation Unit (DGU) is damaged due to the attack. The timing of the attack can be altered to target the DGUs simultaneously or at different times. Since the watermark mode is not enabled, the attack remains invisible to the system.

When the watermark mode is enabled, a watermark signal is introduced, converting the delay caused by the attack into a disturbance. The residual plots in Figure 14 illustrate the response to the attack at t=3 seconds. The voltage difference measured in DGU 1 (top left) and the line currents observed in both DGUs (bottom row) are non-zero and exceed predetermined thresholds within 4 milliseconds. The voltage difference in DGU 2 (top right) remains at 0, indicating that the attack was directed at the signals from DGU 1.

If both DGU 1 and DGU 3 are attacked simultaneously, the presence of a residual output voltage (Vout) suggests that the signals from both DGU 1 and DGU 2 have been attacked. In the case of attacks occurring at different times, the Kalman filter is utilized to detect the DGU with the least attacked time. The filter then mitigates the attack, filtering out the malicious signals and halting the operation of the affected DGU as shown in Figure 1

CHAPTER 6.

CONCLUSION.

The research described here focuses on developing a distributed watermarking approach to address the problem of replay assaults in a distributed control microgrid (DCmG). The primary goal aims to improve the monitoring system used to verify the data sent back and forth within the microgrid between Distributed Generation Units (DGUs).

In the beginning, a study is done to comprehend how the monitoring system behaves when replay assaults are used against it without the use of a watermark. As long as the recorded data is inside the steady state, it is discovered that these attacks are undetectable. Therefore, the necessity for an additional technique to efficiently detect and stop replay attacks is evident. A watermark is added to the system to help with this problem.

A requirement that the watermark must meet in order to successfully identify replay attacks is derived. The system's steady-state characteristic statistics are changed by integrating the watermark, allowing the monitoring system to differentiate between genuine communication signals and data that has been replayed.

REFERENCES

[1] Helem Sabina Sánchez, Damiano Rotondo, Teresa Escobet, Vicenç Puig, Jordi Saludes, Joseba Quevedo, Journal of the Franklin Institute, "*Detection of replay attacks in cyber-physical systems using a frequency-based signature*". Issue 5, 2019, https://doi.org/10.1016/j.jfranklin.2019.01.005.

[2] Alexander J.Gallo ,Mustafa S.Turan Francesca Boem, Giancarlo Ferrari-Trecate , Thomas Parisini, "*Distributed watermarking for secure control of microgrids under replay attacks*" ,2018, DOI https://doi.org/10.1016/j.ifacol.2018.12.032.

[3] Sahoo, Subham & Mishra, Sukumar & Peng, Jimmy & Dragicevic, Tomislav. (2018), "*A Stealth Cyber Attack Detection Strategy for DC Microgrids*", IEEE Transactions on Power Electronics. PP. 1-1. 10.1109/TPEL.2018.2879886.

[4] Le TD, Ge M, Anwar A, Loke SW, Beuran R, Doss R, Tan Y, "*Grid Attack Analyzer: A Cyber Attack Analysis Framework for Smart Grids*". Sensors (Basel). Jun 24;22(13):4795. doi: 10.3390/s22134795. PMID: 35808292; PMCID: PMC9268941.

[5] Grids Tan, Le & Anwar, Adnan & Loke, Seng & Beuran, Razvan & Tan, Yasuo. (2020), "*Grid Attack Sim: A Cyber Attack Simulation Framework for Smart, Electronics*". 9.21 https://doi.org/10.3390/electronics9081218

[6] A.G. Wermann, M.C. Bortolozzo, E. Germano da Silva, A. Schaeffer-Filho, L. Paschoal Gaspary and M. Barcellos, "*ASTORIA: A framework for attack simulation and evaluation in smart grids*". NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium, Istanbul, Turkey, 2016, pp. 273-280, doi: 10.1109/NOMS.2016.7502822.

[7] Moslem Dehghani, Taher Niknam, Mohammad Ghiasi, Navid Bayati, Mehdi Savaghebi . "*Cyber-Attack Detection in DC Microgrids Based on Deep Machine Learning and Wavelet Singular Values Approach"*. Electronics 2021, 10(16), 1914; https://doi.org/10.3390/electronics10161914

[8] Jiang, Jing & Qian, Yi. (2017). "*Defense Mechanisms against Data Injection Attacks in Smart Grid Networks*". IEEE Communications Magazine. 55. 76-82. 10.1109/MCOM.2017.1700180.

[9] A. J. Gallo, M. S. Turan, P. Nahata, F. Boem, T. Parisini and G. Ferrari-Trecate, "*Distributed Cyber-Attack Detection in the Secondary Control of DC Microgrids,"* 2018 European Control Conference *(ECC)*, Limassol, Cyprus, 2018, pp. 344-349, doi: 10.23919/ECC.2018.8550549.

[10] X. Zhong, L. Yu, R. Brooks and G. K. Venayagamoorthy, "*Cyber security in smart DC microgrid operations,"* 2015 IEEE First International Conference on DC Microgrids *(ICDCM)*, Atlanta, GA, USA, 2015, pp. 86-91, doi: 10.1109/ICDCM.2015.7152015.

[11] "Microgrid", Electropedia International Electrotechnical Commission. 2017-12-15.

[12] “Grid System”, Office of electricity. Url: https://www.energy.gov/oe/grid-systems

[13] Mathworks

[14] H. Neema, H. Vardhan, C. Barreto and X. Koutsoukos, *"Web-Based Platform for Evaluation of Resilient and Transactive Smart-Grids*," 2019 7th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), Montreal, QC, Canada, 2019, pp. 1-6, doi: 10.1109/MSCPES.2019.8738796.

[15] T. Duy Le, A. Anwar, R. Beuran and S. W. Loke, "*Smart Grid Co-Simulation Tools: Review and Cybersecurity Case Study*," *2019* 7th International Conference on Smart Grid (icSmartGrid), Newcastle, NSW, Australia, 2019, pp. 39-45, doi: 10.1109/icSmartGrid48354.2019.8990712.