2024 IEEE International Conference on Environment and Electrical Engineering and 2024 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&amp;CPS Europe) | 979-8-3503-5518-5/24/$31.00 ©2024 IEEE | DOI: 10.1109/EEEIC/ICPSEUROPE61470.2024.10751374

Cyber-Physical Testbed for Distributed Consensus Control Amid Denial of Service Attacks

Ibtissam Kharchouf
Energy Systems Research Laboratory
Florida International University
Miami, FL, USA
ikhar002@fiu.edu

Hossam M. Hussein
Energy Systems Research Laboratory
Florida International University
Miami, FL, USA
hhuss013@fiu.edu

Mahmoud S. Abdelrahman
Energy Systems Research Laboratory
Florida International University
Miami, FL, USA
mabde046@fiu.edu

S M Sajjad Hossain Rafin
Energy Systems Research Laboratory
Florida International University
Miami, FL, USA
srafi010@fiu.edu

Osama A. Mohammed
Energy Systems Research Laboratory
Florida International University
Miami, FL, USA
mohammed@fiu.edu

***Abstract*—AC microgrids (MGs) are exposed to communication disturbances and malicious cyber-attacks due to the sparse communication network. In this work, a controller hardware-in-the-loop (C-HIL) setup is designed to test the effect of communication disturbances and different types of cyber-attacks by proposing a secondary controller utilizing distributed consensus scheme for a multi-agent system (MAS). The proposed MG cyber-physical system (CPS) includes, an islanded AC MG modeled and run in OPAL-RT, secondary agents implemented on external controllers, and an attacker agent. UDP/IP communication protocol is used to facilitate communication between OPAL-RT and the controller agents, as well as neighboring agents. The study highlights the risk AC MGs are exposed to under denial-of-service (DoS) cyber-attacks. The impacts of DoS attacks on the closed-loop stability of the AC MG are analyzed comprehensively. The experiments emphasize the severe impact of DoS attacks on the controlled system and the necessity to implement detection and mitigation measures to ensure the stability and reliability of microgrids.**

Keywords*— Consensus algorithm, cyber-physical system (CPS), denial of service attack (DoS), distributed secondary control, microgrids, multi-agent system (MAS), OPAL-RT, real-time simulation.

NOMENCLATURE

V_{od}, V_{oq}	Direct and quadrature output voltage
I_{od}, I_{oq}	Direct and quadrature output current
ω_n, V_n	Frequency and voltage nominal setpoints
ω_c	Cutoff frequency
m_p, n_q	Droop coefficients
ω_{ref}, V_{ref}	Frequency reference and voltage reference
$u_{\omega i}, u_{Voi}$	Auxiliary controls
u_{pi}, u_{qi}	Auxiliary controls
C_P, C_q	Control coefficients
C_ω, C_{Vo}	Control coefficients
a_{ij}	Elements of the adjacent matrix A
τ_a	DoS attack duration

I. INTRODUCTION

Microgrids (MGs) enhance power quality/reliability and supply power to individual end-user sites. The term "Microgrid" denotes a cluster of Distributed Energy Resources (DERs) and loads interconnected within determined electrical boundaries. A microgrid can function in both islanded and grid-connected modes, where the microgrid connection and disconnection to the grid are performed following economic and technical constraints. Modern microgrids are considered a complex Cyber-Physical System (CPS) due to cyber communication's key role by enabling fast measurement and control of DERs.

Control is a critical enabler technology for the deployment of MG systems. Like the traditional power grid, MGs have a multi-layered hierarchical control technique. Advanced control techniques need to be effectively used at all MG levels. The controllers must guarantee a secure operation of MGs in both functioning modes and the effective disconnection or reconnection processes. MGs' conventional hierarchical control structure is divided into three levels, i.e., Primary, Secondary, and Tertiary Control, with different time scales. The primary control (PC), also called local control of distributed generators (DGs), is designed to maintain voltage and frequency stability while managing the sharing of active and reactive power through local measurements.

This control level includes internal voltage and current control loops and droop control, and it is decentralized to ensure that the system's stability is not reliant on the communication network. The secondary control (SC) level compensates for the imprecise voltage and frequency regulation caused by the primary control and helps in proportional power sharing. At the high level, the tertiary control (TC) is implemented for optimal dispatch operations and to control the power flow.

The current secondary control strategies can be categorized into three types: decentralized, centralized, and distributed. The centralized control method presents many problems, such as poor plug-and-play capability, high computational and bandwidth demand, and the risk of a single point of failure, which may affect the system's reliability [1]. To overcome these issues, the distributed multi-agent system (MAS) control is becoming more popular for its scalability, flexibility, and plug-and-play ability. In the distributed secondary control, the

This work was partially supported by grants from the Office of Naval Research, National Science Foundation, and the US Department of Energy. The authors are with the Energy Systems Research Laboratory, Department of Electrical and Computer Engineering, Florida International University, Miami, FL, USA. (e-mail: mohammed@fu.edu).

979-8-3503-5518-5/24/$31.00 ©2024 IEEE

communication network is set so that each agent only communicates with its neighboring agents. All agents work cooperatively towards a global objective [2]. Different distributed algorithms have been implemented in the literature to optimize and control AC MGs.

With the increasing role of communication networks in microgrids, the communication turbulences impact such as transmission delay, limited bandwidth, data loss, channel interruption, , and physical defects of communication equipment should be fully analyzed. The communication delay effect is one practical challenge affecting the microgrid performance [3]. In practice, the exchange of information between neighboring agents is not instantaneous, and many factors affect the communication delay, such as network traffic, communication protocols, bandwidth, etc. Communication delays can directly or indirectly affect control commands execution of microgrids, resulting in the system malfunction, and in severe events, may cause cascading failures. As a consequence, in the CPS research, more focus is being directed towards the interaction between the communication network and the physical system.

This intricate connection between physical and cyber systems makes them vulnerable to cyber threats. Thus, it is crucial to identify potential vulnerabilities, evaluate their impact, and provide solutions to these security issues. To accurately simulate the physical system and the communication network interaction, a C-HIL must be provided to study the effect of communication network disturbances and cyber-attacks on the control. Hardware testbeds are best for testing controls, communication networks, and the impact of cyber-attacks. However, factors related to costs and risks limit the researcher's ability to conduct tests on fully hardware testbeds. As a solution, hardware and software platforms (HIL) offer a more practical approach than pure digital simulation platforms. Researchers in the literature widely use hardware-in-the-loop (HIL) simulation, and it's named C-HIL when the hardware involved consists only of controllers. In our study, we built a C-HIL simulation platform in the Energy Systems Research Laboratory (ESRL) using OPAL-RT and external controllers. This setup is best for examining the effects of communication networks disruptions on microgrid performance, as well as the effect of attacks on CPSs [4].

Data integrity attacks, such as False Data Injection (FDIA) and Replay attacks, can be performed by injecting data at the sensor, actuator, or communication link [5]. Attacks such as DoS and Distributed-DoS prevent users from accessing system resources, causing significant disruption. Confidentiality attacks such as eavesdropping have no direct impact on the operation. However, the revealed information can be used to perform attacks that aim to impact the CPS control objectives.

This paper aims to study the impact caused by DoS cyber-attacks with different packet rates and attack durations on the closed-loop stability of an islanded AC microgrid. This paper first introduces a new cyber-physical testbench to overcome the limitations of fully hardware testbeds. The proposed platform consists of: (i) a real-time microgrid model implemented on RT-LAB, (ii) a secondary controller utilizing distributed consensus implemented on external controllers, (iii) an attacker agent implemented on a separate R-Pi to perform different types of attacks. This proposed C-HIL is mainly developed to test controls, communication network disturbances, and the impact of cyber-attacks, as well as to further test detection and mitigation techniques to overcome these issues. The setup consists of an OPAL-RT simulator and external controllers deployed on Raspberry Pis. All communications, both between the OPAL-RT and the secondary controllers and among the secondary controllers, are conducted via the UDP/IP protocol.

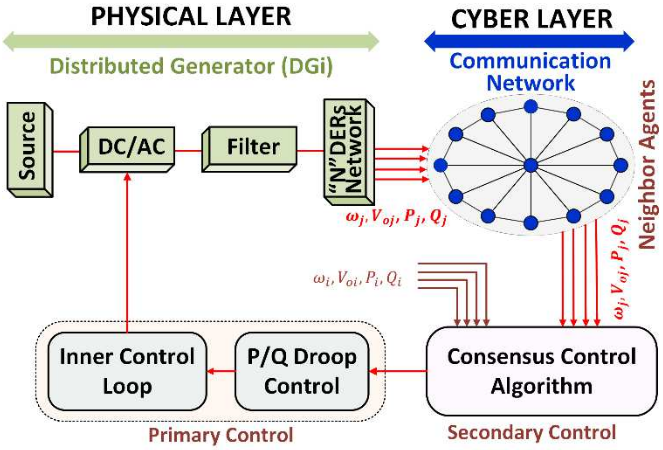


Fig. 1. DG control scheme

The reminder of this paper is organized as: An overview of the primary and secondary control mechanisms and the communication network is given in Section II. Section III details the testbed setup. Section IV presents study cases results and discussions that confirm the setup and demonstrate the consequences of DoS attacks on the studied system. Finally, conclusions are provided in Section V.

II. Fundamentals

A. Primary Control

The primary controller of the DG inverter is composed of three control loops: a current control loop, a voltage control loop, and a power control loop.

External power control loop responsible for regulating the frequency and voltage magnitude of the fundamental component of the inverter output voltage. This regulation is based on droop characteristics linked to real and reactive power as depicted in Fig. 2. The principle of droop control aims to replicate the response of a synchronous generator. In traditional power systems, rotating machines adjust their frequency downwards in response to increased demand, following their governor's droop characteristics [6], [7]. Likewise, inverters implemented this concept by lowering the reference frequency as the demand rises. Additionally, droop characteristics are used in voltage magnitude for reactive power sharing.

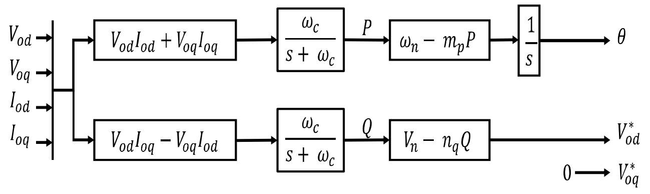

V_{od}
V_{oq}
I_{od}
I_{oq}
$V_{od}I_{od} + V_{oq}I_{oq}$
$\frac{\omega_c}{s+\omega_c}$
P
$\omega_n - m_pP$
$\frac{1}{s}$
θ
$V_{od}I_{oq} - V_{oq}I_{od}$
$\frac{\omega_c}{s+\omega_c}$
Q
$V_n - n_qQ$
V^*_{od}
0
V^*_{oq}

Fig. 2. Power control loop block diagram

The active (P) and reactive (Q) power are computed using the measured output current and output voltage. Subsequently, they undergo low-pass filtering, as described in (1), where ω_c represents cutoff frequency of the filters.

$$\begin{cases} P = \frac{\omega_c}{s+\omega_c}(V_{od}I_{od} + V_{oq}I_{oq}) \\ Q = \frac{\omega_c}{s+\omega_c}(V_{od}I_{oq} - V_{oq}I_{od}) \end{cases} \tag{1}$$

For power sharing purpose, an artificial droop is incorporated into both voltage and frequency magnitude, as described in (2). Here, V_n and ω_n represent the voltage amplitude and nominal frequency, respectively.

$$\begin{cases} \omega = \omega_n - m_pP \\ V_o = V_n - n_qQ \end{cases} \tag{2}$$

The droop coefficients (m_p and n_q) are calculated corresponding to (3) and vary with the output power rating. The voltage reference (V^{ref}) is determined from the power control loop. It's important to note that V^{ref} is applied along the (d) axis. Meanwhile, the reference for the (q) axis is maintained null.

$$m_p = \frac{\Delta\omega}{P_{max}} \quad , \quad n_q = \frac{\Delta V_o}{Q_{max}} \tag{3}$$

Current and voltage control loops: They generate the reference for output current I^{ref}_{inv} and input voltage V^{ref}_{inv}. Fig.3.a and Fig.3.b depict the internal current and voltage loops.

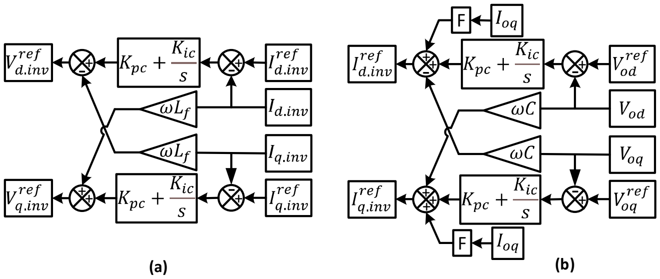


Fig. 3. (a) PI current control loop, (b) voltage control loop

B. Preliminaries and Communication Network

Before introducing the distributed secondary control, a brief about some properties of graph theory should be investigated.

The system under study is an islanded AC MG comprising multiple DGs. In our analysis, the communication network between these DGs is modeled as an undirected graph, considering it from the viewpoint of control methods. The graph's nodes and edges denote the DGs and their communication link. The MG under consideration is characterized by the model shown in Fig. 4.a, and its equivalent weighted graph is depicted in Fig. 4.b. Node DGi represents the DG and the edge lines indicate the communication link among DG units. The digraph is commonly represented as $\mathcal{G} = (\mathcal{V}, E, A)$, where $\mathcal{V} = \{v_1, v_2, \dots, v_N\}$ denotes a set of $\mathcal{N}$ nodes, $E \subseteq \mathcal{V} \times \mathcal{V}$ is a set of edges, $A = (a_{ij})_{N\times N}, (i, j \in V)$ is a weighted adjacency matrix. Fig.4.c shows the corresponding adjacency matrix of the studied system. Each DG is considered as a node of the communication digraph, and the communication network edges are denoted by the communication links. The edge (v_j, v_i) signifies that node j (at the tail of the edge) transmits information to node i (at the head of the edge). The edge's weight is greater than zero if $(v_j, v_i) \in E$, otherwise $a_{ij} = 0$. $N_i = \{j | (v_j, v_i) \in E\}$ denotes the set of neighbors of the ith node, where j is termed as neighbor of i if $(v_j, v_i) \in E$. Each node in the graph possesses in-degree matrix D, defined as $D = diag\{d_1, d_2, \dots, d_N\}$ where $d_i = \sum_{j=1}^{N_i} a_{ij}$. The Laplacian matrix is defined as $L = D - A$ [8], [9].

C. Secondary Control

The Frequency and voltage restoration and efficient power sharing among the distributed sources are the secondary controller objectives [10]. Each DG in the distributed control exchanges information with neighboring DGs. Differentiating both terms in (2) gives:

$$\begin{cases} \dot{\omega}_i = \dot{\omega}_{ni} - m_{pi}\dot{P}_i \equiv u_{\omega i} \\ \dot{V}_{oi} = \dot{V}_{ni} - n_{qi}\dot{Q}_i \equiv u_{Voi} \end{cases} \tag{4}$$

The nominal setpoints ω_{ni} and V_{ni} are set by SC as follows:

$$\omega_{ni} = \int(\dot{\omega}_i + m_{pi}\dot{P}_i)dt = \int(u_{\omega i} + u_{Pi})dt \tag{5}$$

$$V_{ni} = \int(\dot{V}_{oi} + n_{qi}\dot{Q}_i)dt = \int(u_{Voi} + u_{Qi})dt \tag{6}$$

The accurate power sharing challenge can be formulated as follows: $u_{Pi} = m_{pi}\dot{P}_i$ and $u_{Qi} = n_{qi}\dot{Q}_i$. Here, ω_{ni} has $u_{\omega i}$ and u_{Pi} as secondary control inputs, while V_{ni} has u_{Voi} and u_{Qi} as secondary control inputs. $u_{\omega i}$ and u_{Voi} serve as auxiliary controls.

The objectives of the secondary controller are:

- *Regulation of Frequency and voltage objective:*

$$\lim_{t\to\infty} |\omega_i(t) - \omega_{ref}| = 0 \quad \forall i = 1,2,\dots,N. \tag{7}$$

$$\lim_{t\to\infty} |V_{oi}(t) - V_{ref}| = 0 \quad \forall i = 1,2,\dots,N. \tag{8}$$

- *Power Sharing objective:*

$$\lim_{t\to\infty} |m_{pi}P_i(t) - m_{pj}P_j(t)| = 0 \quad \forall i \neq j. \tag{9}$$

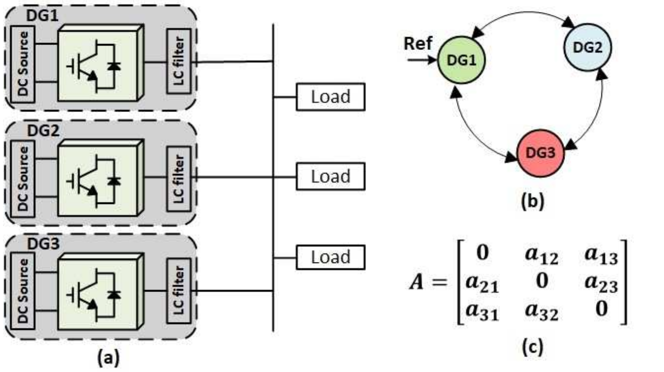
$$\lim_{t\to\infty} |n_{qi}Q_i(t) - n_{qj}Q_j(t)| = 0 \quad \forall i \neq j. \tag{10}$$

These control objectives can be fulfilled by regulating the control inputs of every agent: $u_{\omega i}$, u_{Voi}, u_{Pi}, and u_{Qi}.

1) Frequency and voltage control

As previously explained, the DGs connect with each other via the specified communication digraph illustrated in Fig. 4.b. The control signals $u_{\omega i}$ and u_{Voi} are determined using information from both the DGs themselves and their neighboring units, as follows:

$$u_{\omega i} = C_\omega\left[\sum_{j=1}^{N} a_{ij}(\omega_j - \omega_i) + g_i(\omega^{ref} - \omega_i)\right] \tag{11}$$



$$A = \begin{bmatrix} 0 & a_{12} & a_{13} \\ a_{21} & 0 & a_{23} \\ a_{31} & a_{32} & 0 \end{bmatrix}$$

Fig. 4. (a) MG model, (b) corrsponding weighted graph, (c) adjacency matrix

$$u_{Voi} = C_{Vo}\left[\sum_{j=1}^{N} a_{ij}\left(V_{oj} - V_{oi}\right) + g_i\left(V^{ref} - V_{oi}\right)\right] \quad (12)$$

C_{ω} and C_{Vo} represent the control gains, both of which are positive. The pinning gain g_i is configured to 1 if the DG can directly receive set points; otherwise, it is set to 0.

2) *Active and Reactive power sharing*

The auxiliary controls u_{Pi} and u_{Qi} are selected based on the DGs' own information as well as the information from their neighbors, as follows:

$$u_{Pi} = C_P\left[\sum_{j=1}^{N} a_{ij}\left(m_{pj}P_j - m_{pi}P_i\right)\right] \quad (13)$$

$$u_{Qi} = C_Q\left[\sum_{j=1}^{N} a_{ij}\left(n_{qj}Q_j - n_{qi}Q_i\right)\right] \quad (14)$$

III. Testbed Setup

This part outlines an assessment setup for the designed agents using the consensus control. It provides details of the studied islanded MG and the setup elements, including the physical layer, cyber layer, and DoS attack.

As shown in Fig.5, the C-HIL experimental testbed of the cyber-physical microgrid consists of two primary connected components: (i) the physical system, which includes the AC MG components and primary controllers, simulated in real-time using OPAL-RT. (ii) the cyber layer, consists of hardware agents operating on Raspberry Pis. Primarily, real-time measurements are sent from the OPAL-RT simulator to respective external secondary controllers (agents) via the UDP/IP protocol. These measurements are then shared with neighboring agents through UDP/IP.

A. *Physical Layer*

The MG model is created using MATLAB/Simulink and simulated on OPAL-RT. This model includes the MG system along with the corresponding local controllers. The latter are composed of inner and outer control loops. In each control iteration, local measurement packets ($[\omega_i, V_{oi}, m_{pi}P_i, n_{qi}Q_i]$) are sent to the corresponding secondary controllers through UDP/IP. The secondary controllers then send control input packets ($[u_{\omega i}, u_{Voi}, u_{Pi}, u_{Qi}]$) back to the OPAL-RT via UDP/IP to compute the ω_{ni} and V_{ni} setpoints. The external secondary controllers exchange data with the primary controllers and neighboring agents within the local area network (LAN).

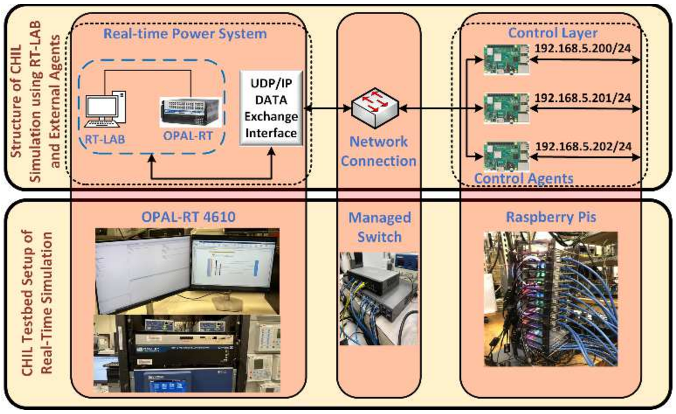


Fig. 5. C-HIL testbed setup

B. *Cyber Layer*

The designed secondary control agents can receive measurements, update the states, handle calculations, and return control signals. Every agent represents a DG that runs the consensus control according to the specified control objectives. Every agent receives local measurement packets (ω, V, P, Q), and transmits control signals back. The communication topology between the R-Pis agents is shown in Fig. 4.b.

In this test-setup, Raspberry Pi 3 Model B+ devices were used. Secondary controllers are programmed using a Python script into each Raspberry Pi, and each agent is assigned a static IP address. Each agent starts a communication channel to enable data exchange between the agents and starts a client socket connection with the OPAL-RT simulator. Commands are sent to the runtime once the connection is established.

The control pseudo-code is given as follows:

Consensus Secondary Control Pseudo Code

```
// Initialization
Define Adjacency, Diagonal, and Laplacian matrices.
Initialize agent details.
Initialize UDP socket with OPAL-RT.
// Neighbors Initialization
Get the number of neighbor agents.
Initialize neighbor agents' details.
Initialize UDP socket with agents.
// Main Loop
While True:
    Get local measurements from OPAL-RT.
    For each neighboring agent in range (Num_Neighbors):
        Send local measurements to neighboring agents.
    For each neighboring agent in range (Num_Neighbors):
        Receive local measurements from neighbors.
    Calculate control signals.
    Send control signals to OPAL-RT.
```

C. *DoS Attack*

1) *DoS Attack Model*

DoS attacks are also known as jamming attacks. They aim to overload communication links, devices, routers, servers, etc., to delay or prevent legitimate users from timely access to data. They can lead to total data loss or to data replacement with prior transmitted/received data. Different approaches can be used to perform a DoS attack, for instance data packet loss, zero input, network flooding, etc.

Consider the communication between DGi and DGj during the interval $[t_1, t_2] \subset [0, \infty)$. The states communicated from OPAL-RT to the agents and between the agents are $x_i \in [\omega_i, V_{oi}, m_{pi}P_i, n_{qi}Q_i]$, and the states communicated from the agents to OPAL-RT are$y_i \in [u_{\omega i}, u_{Voi}, u_{Pi}, u_{Qi}]$. Let m_μ be the DoS attacks number during the interval $[t_1, t_2] \subset [0, \infty)$. Define $I_k = [t_a\, ,\ t_a + \tau_a]$ as the k^{th} interval during which a DoS attack occurs, where $t_a\, , t_a + \tau_a$, and τ_a represent the start, end, and DoS length, respectively. The overall DoS time between two agents can be described as [11].

$$\Gamma_{DoS}^{(i,j)} = (t_1, t_2) \cap \left(\cup_{a=1}^{m_\mu} I_k^{(i,j)} \right) \tag{15}$$

Intruders may introduce other constraints, such as those on τ_a to achieve stealthiness; a characteristic where attacks go undetected.

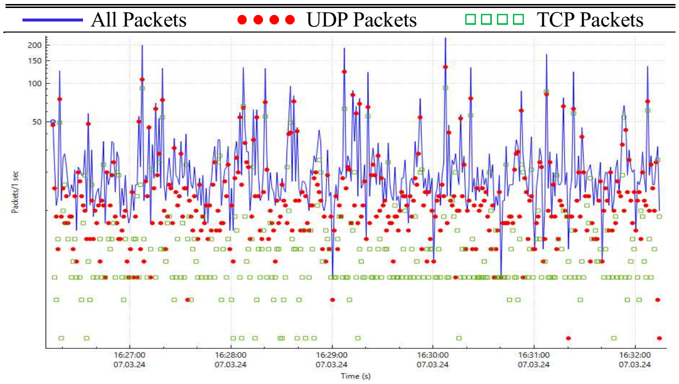


Fig. 6. Normal Network traffic

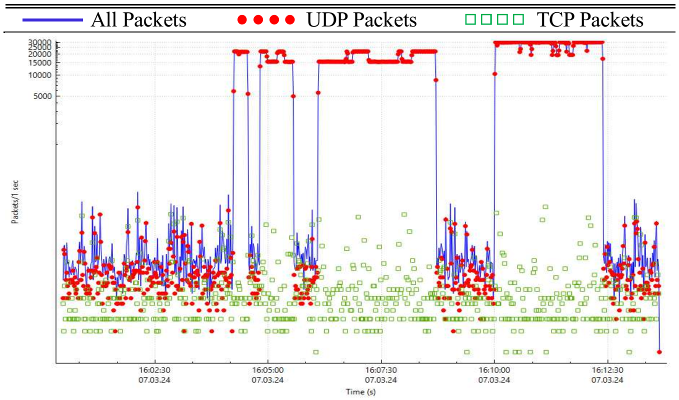


Fig. 7. Ubnormal Network traffic (during DoS attacks)

2) *DoS Attack Agent*

The DoS attacks were initiated from a separate agent. An agent can be overwhelmed by high traffic volume to devastate its capacity to respond to legitimate requests. This flood can be performed using different techniques, such as sending large number of packets/s (pps) or using multiple sources to amplify the attack. Additionally, communication links can be targeted, resulting in changes to the communication topology. Some common types of DoS attacks include, SYN flood, Ping flood, HTTP flood, and UDP flood. The proposed C-HIL setup demonstrates the effects of UDP flood attacks on the physical system. Fig. 6 shows a normal network traffic, while Fig. 7 shows network profile throughout a series of DoS attacks, showcasing deferent durations and UDP packet frequencies. The success of these attacks depends on both the magnitude of generated traffic and the target system or network's capacity to withstand it.

IV. Results and Discussion

This section has carried out a real-time performance assessment of the C-HIL testbed under DoS attacks, where attacks with varying packet lengths and rates target the agents. An AC MG structured by three parallel inverters at power ratings of 500KW, 300KW, and 200 KW, respectively, all connected to the PCC bus. This MG model is developed using MATLAB/Simulink 2022a and loaded into the target (OPAL-RT) through RT-LAB software. The consensus controllers are configured as: $C_\omega = 0.2$, $C_{Vo} = 0.1$, $C_P = 4$, and $C_Q = 100$. The droop coefficients are all set to $m_p = 0.01$ and $n_q = 0.04$.

A. *Real time C-HIL simulation performance*

The implemented distributed consensus secondary control is verified using the developed C-HIL setup. In this test, the droop start is at t=20s, followed by load increase at t=40s. The secondary controller is then activated around t=60s, the load decreased at t=80s, then slightly increased at t=100, and a final load increase at t=120s. Note that the load profile is the same in all studied cases. As shown in Fig. 8, at the time of droop activation, the objective of power sharing was achieved. However, the F and V dropped from their reference values (60 Hz and 600 V). The increase of load at t=40s emphasizes the previously observed droop behavior. To restore the system F and V, the secondary control is activated around t=60s. V and F were restored to 600V and 60Hz while maintaining equal power sharing. At t=80s, t=100s, and t=120s, the load was increased and decreased to emphasize the ability of the secondary control to achieve the objectives specified in (7), (8), (9), and (10).

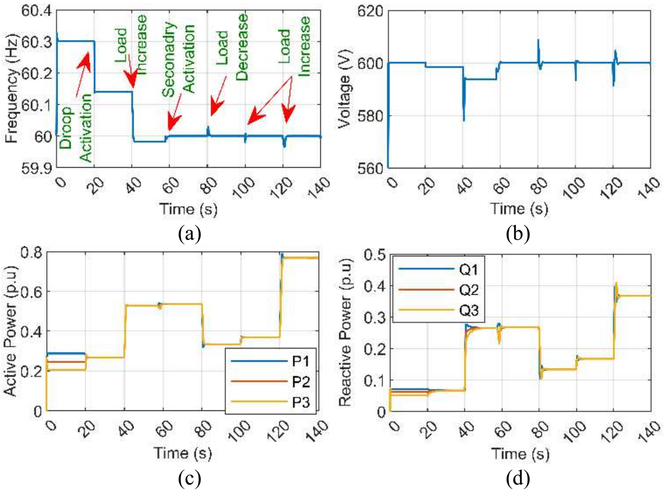
B. *DoS attack on agent 2 (DG2)*

1) *Case 1:*

The DoS attack occurs at t=40s, stops at t=80s, and occurs again at t=120s. The attack lengths are $\tau_{a1} = 40s$ and $\tau_{a2} = 20s$. The frequency, voltage, active, and reactive power performance are shown in Fig. 9. Due to the signal reference from DG1 and the droop control, the system voltage and frequency were restored to 600V and 60Hz, respectively. However, the observed power-sharing performance during the attacks is due to its high dependence on the network topology. The results showed that the DoS could deteriorate the consensus power-sharing objectives while a limited influence on MG stability was observed.

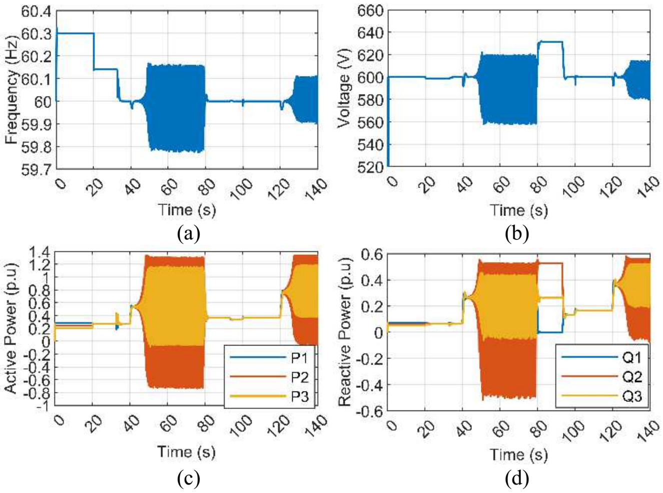
2) *Case 2:*

In this case, the DoS attacks occurred at t=20s, t=65s, t=80s, and t=100s. The frequency, voltage, active, and reactive power performance are shown in Fig. 10. The attack lengths in this case are shorter compared to the previous case (around. $\tau_a = 5s$) except for the last attack ($\tau_{a4} > 10s$). However, the attacker floods the targeted DG with a higher volume of traffic compared with the first case. Here, it can also be noticed that the system voltage and frequency can still be reinstated to 600V and 60Hz. However, the DoS attack in this case directly affected the MG stability when ($\tau_a > 5s$).



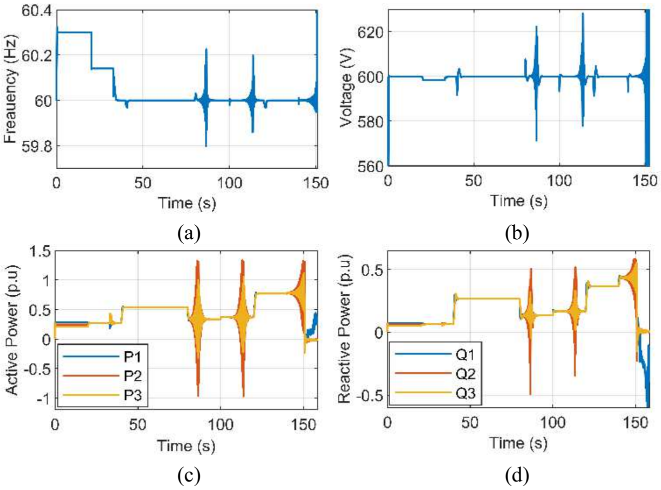
(a) (b) (c) (d)

Fig. 8. MG operation: (a) Frequency, (b) Voltage, (c) Active power, (d) Reactive power



(a) (b) (c) (d)

Fig. 9. MG operation under DoS attack on agent 2: (a) Frequency, (b) Voltage, (c) Active power, (d) Reactive power



(a) (b) (c) (d)

Fig. 10. MG operation under DoS attack on agent 2: (a) Frequency, (b) Voltage, (c) Active power, (d) Reactive power

The success of these attacks frequently relies on the amount of traffic generated by the attack and the ability of the target system to manage the incoming traffic. Depending on the attackers' resources and the capabilities of the target system, packet rates can be adjusted.

V. Conclusion

This work presented a C-HIL setup to assess the effects of cyber-attacks on MG CPSs. A distributed consensus secondary control-based MG is implemented using a real UDP/IP communication network. The proposed CPS testbed includes three main parts: real-time MG model implemented on RT-LAB, (ii) a secondary controller utilizing distributed consensus implemented on external controllers, (iii) an attacker agent implemented on a separate R-Pi to perform different types of attacks. The experimental results validated the proposed control's performance and showed the impact of DoS attacks on such systems. In the performed test cases, attackers can adjust the packet rate and length to maximize the impact of the attack while minimizing their own resources and detection risk. This work is a building stone for future research focused on developing detection and mitigation techniques.

References

[1] Y. Han, X. Ning, P. Yang, and L. Xu, "Review of Power Sharing, Voltage Restoration and Stabilization Techniques in Hierarchical Controlled DC Microgrids," IEEE Access, vol. 7, pp. 149202–149223, 2019, doi: 10.1109/ACCESS.2019.2946706.

[2] F. Doost Mohammadi, H. Keshtkar Vanashi, and A. Feliachi, "State-Space Modeling, Analysis, and Distributed Secondary Frequency Control of Isolated Microgrids," IEEE Trans. Energy Convers., vol. 33, no. 1, pp. 155–165, Mar. 2018, doi: 10.1109/TEC.2017.2757012.

[3] H. Fan, H. Wang, S. Xia, X. Li, P. Xu, and Y. Gao, "Review of Modeling and Simulation Methods for Cyber Physical Power System," Front. Energy Res., vol. 9, p. 642997, May 2021, doi: 10.3389/fenrg.2021.642997.

[4] I. Kharchouf and O. A. Mohammed, "Controller Hardware-in-the-Loop Testbed of a Distributed Consensus Multi-Agent System Control under Deception and Disruption Cyber-Attacks," Energies, vol. 17, no. 7, p. 1669, Mar. 2024, doi: 10.3390/en17071669.

[5] P. K. Reddy Shabad, A. Alrashide, and O. Mohammed, "Anomaly Detection in Smart Grids using Machine Learning," in IECON 2021 – 47th Annual Conference of the IEEE Industrial Electronics Society, Toronto, ON, Canada: IEEE, Oct. 2021, pp. 1–8. doi: 10.1109/IECON48115.2021.9589851.

[6] J. Lai, H. Zhou, X. Lu, X. Yu, and W. Hu, "Droop-Based Distributed Cooperative Control for Microgrids With Time-Varying Delays," IEEE Trans. Smart Grid, vol. 7, no. 4, pp. 1775–1789, Jul. 2016, doi: 10.1109/TSG.2016.2557813.

[7] N. Pogaku, M. Prodanovic, and T. C. Green, "Modeling, Analysis and Testing of Autonomous Operation of an Inverter-Based Microgrid," IEEE Trans. Power Electron., vol. 22, no. 2, pp. 613–625, Mar. 2007, doi: 10.1109/TPEL.2006.890003.

[8] A. Bidram, A. Davoudi, and F. L. Lewis, "A Multiobjective Distributed Control Framework for Islanded AC Microgrids," IEEE Trans. Ind. Inform., vol. 10, no. 3, pp. 1785–1798, Aug. 2014, doi: 10.1109/TII.2014.2326917.

[9] Y. Han, H. Li, P. Shen, E. A. A. Coelho, and J. M. Guerrero, "Review of Active and Reactive Power Sharing Strategies in Hierarchical Controlled Microgrids," IEEE Trans. Power Electron., vol. 32, no. 3, pp. 2427–2451, Mar. 2017, doi: 10.1109/TPEL.2016.2569597.

[10] I. Kharchouf, M. S. Abdelrahman, and O. A. Mohammed, "ANN-Based Secure Control of Islanded Microgrid Under False Data Injection Cyber-Attack," in 2023 IEEE Industry Applications Society Annual Meeting (IAS), Nashville, TN, USA: IEEE, Oct. 2023, pp. 1–6. doi: 10.1109/IAS54024.2023.10406659.

[11] P. S. Tadepalli and D. Pullaguram, "Distributed Control Microgrids: Cyber-Attack Models, Impacts and Remedial Strategies," IEEE Trans. Signal Inf. Process. Netw., vol. 8, pp. 1008–1023, 2022, doi: 10.1109/TSIPN.2022.3230562.