2024 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT) | 979-8-3503-1360-4/24/$31.00 ©2024 IEEE | DOI: 10.1109/ISGT59692.2024.10454181

Mitigating False Data Injection Attacks on Inverter Set Points in a 100% Inverter-Based Microgrid

Milad Beikbabaei, *Graduate Student Member, IEEE*, Mario Montano, Ali Mehrizi-Sani, *Senior Member, IEEE*,
and Chen-Ching Liu, *Life Fellow, IEEE*
The Bradley Department of Electrical and Computer Engineering
Virginia Polytechnic Institute and State University, Blacksburg, VA 24061
e-mails: {miladb, mariom, mehrizi, ccliu}@vt.edu

***Abstract*—The increasing number of 100% inverter-based microgrids is introducing new challenges in their control and cybersecurity. Previous work has studied the cyber vulnerabilities of microgrids; however, very few work has studied methods to mitigate and detect cyberattacks in a 100% inverter-based microgrid. Attackers can utilize communication-based devices in a microgrid to launch false data injection (FDI) attacks and cause voltage and frequency instability. This paper studies the effects of FDI attacks on the real and reactive power set points of inverter-based resources (IBR) in a 100% inverter-based microgrid. This work co-simulates a power system using PSCAD and a communication system using Python to study FDI attacks. The communication system is modeled as a first in first out (FIFO) queue model. A long short-term memory (LSTM)-based method is used to mitigate and detect ramp and bias FDI attacks. The proposed strategy is tested on a microgrid with four IBRs subject to different FDI attacks.**

***Index Terms*—Cyberattack, detection, false data injection (FDI), inverter-based resources (IBR), long short-term memory (LSTM), microgrid, photovoltaic (PV).**

I. Introduction

The U.S. has the goal of reaching 100% clean electricity by 2035 [1]. As a result, more photovoltaic (PV) and wind generation are being installed in the grid. PV, type III wind turbines, and type IV wind turbines are connected to the grid via an inverter. Therefore, the number of installed 100% inverter-based microgrids is increasing, introducing new challenges in control and cybersecurity. It is necessary to study the cybersecurity of microgrids since attackers can utilize communication-based devices installed in the microgrid to launch cyberattacks. These devices enable sending and receiving measurements and commands. Remote terminal units (RTU) send voltage and current measurements to the control center, and operators send control commands such as generation set points and opening breakers to RTUs.

Several successful cyberattacks have been reported. In 2015, a successful cyberattack on the Ukrainian power system left 225,000 Ukrainians without electricity [2]. The U.S. Department of Energy has reported 36 disturbances to the power system from cyber events or vandalism in the first three months of 2023 [3]. As a result, numerous research has been conducted to study the effects of cyberattacks on the grid and ways to mitigate and detect them. Moreover, attackers use false data injection (FDI) and denial of service (DoS) attacks. In FDI attacks, attackers falsify the data and commands being sent to RTUs to cause disturbances in the power system. In DoS attacks, attackers stop data from being sent to the RTU. Attackers can launch FDI on solar PV units and SCADA systems of a wind farm [4], [5]. Both FDI and DoS attacks can be detected and mitigated.

Previous work has studied the cybersecurity of microgrids; however, very few have studied methods to mitigate and detect cyberattacks in 100% inverter-based microgrids. Reference [6] uses a long short-term memory (LSTM)-based system to monitor the cybersecurity of microgrid networks; however, it only detects the cyberattack. Machine learning–based and observer-based methods can be used to mitigate and detect FDI attacks. Luenberger and augmented Kalman filter can estimate the signal value under FDI attacks [7]. An artificial neural network (ANN) detects and mitigates DoS and FDI on the Volt-VAr control system [8]. ANN detects and mitigates FDI on a DC microgrid inverter control [9]. In [10], LSTM detects power measurement anomalies with high accuracy and estimates them. Stacked autoencoders with LSTM architectures can detect electricity theft [11]. An LSTM network detects cyberattacks on a PV farm [12].

This work simulates a 100% inverter-based microgrid, where it has four inverter-based resources (IBR). Two of them are in the grid-following mode, and the rest are in the grid-forming mode. IBR acts as a current source in the grid-following mode. IBR acts as a voltage source where Q-V droop control helps to keep the voltage within the nominal range, and P-f droop control helps to keep the frequency within the nominal range in the grid-forming mode [13]. A certain number of inverters are set to grid-forming mode to control the frequency and voltage of the 100% inverter-based microgrid. A co-simulation platform is needed to study the cybersecurity of a grid. This work studies FDI attacks on a 100% inverter-based microgrid and proposes a detection and mitigation method using LSTM. The LSTM-based method is tested using the co-simulation platform for various FDI

This work is supported in part by the National Science Foundation (NSF) under award ECCS-1953213, in part by the State of Virginia's Commonwealth Cyber Initiative (www.cyberinitiative.org), in part by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) under the Solar Energy Technologies Office Award Number 38637 (UNIFI Consortium led by NREL), and in part by Manitoba Hydro International. The views expressed herein do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

979-8-3503-1360-4/24/$31.00 ©2024 IEEE

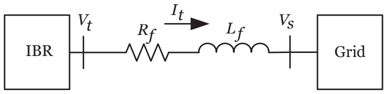

Fig. 1. Single-line diagram of an IBR connected to the grid through an RL filter.

attacks, which provides the following advantages:

- The LSTM-based method detects and mitigates both ramp and bias FDI attacks.
- The LSTM-based method prevents voltage instability.
- The LSTM-based method uses data packets to detect a cyberattack.
- The co-simulation platform enables studying FDI attacks on the power set points of an IBR in a 100% inverter-based microgrid.

Inverter control is discussed in the next section. Section III discusses the implementation of the cyber-physical system. First, the physical layer is described; then, the cyber layer and the co-simulation platform are discussed. Section IV describes the detection and mitigation method. Section V shows the simulation results, and Section VI concludes the paper.

II. Inverter Control

This section introduces inverter controls.

A. Grid-Following Mode

This subsection describes the IBR model in grid-following mode, where it operates as a voltage-sourced converter. A single-line diagram of an IBR connected to the grid through an RL filter is shown in Fig. 1. The phase angle of the voltage is estimated using a phase-locked loop (PLL), which is used in abc-frame to dq-frame transformation. The KVL equation in dq-frame is shown in the following [14]:

$$\begin{aligned}\frac{di_d}{dt} &= -\frac{R_f}{L_f} i_{t,d} + \frac{1}{L_f}(v_{t,d} + \omega L_f i_{t,q} - v_{s,d}),\\ \frac{di_q}{dt} &= -\frac{R_f}{L_f} i_{t,q} + \frac{1}{L_f}(v_{t,q} - \omega L_f i_{t,d} - v_{s,q}),\end{aligned} \tag{1}$$

where i_t is the IBR output currents, V_t is the IBR terminal voltage, and V_s is the voltage after the RL filter. Auxiliary variables are defined and shown in the following:

$$\begin{aligned}U_d &= \frac{1}{L_f}(v_{t,d} + \omega L_f i_{t,q} - v_{s,d}),\\ U_q &= \frac{1}{L_f}(v_{t,q} - \omega L_f i_{t,d} - v_{s,q}).\end{aligned} \tag{2}$$

Substituting (2) in (1) results is (3):

$$\begin{aligned}\frac{di_d}{dt} &= -\frac{R_f}{L_f} i_{t,d} + U_d,\\ \frac{di_q}{dt} &= -\frac{R_f}{L_f} i_{t,q} + U_q,\end{aligned} \tag{3}$$

where d- and q-axes are decoupled as shown in (3), and a PI controller can be used to control the system. Fig. 2 shows the conventional decoupled current control loop [14].

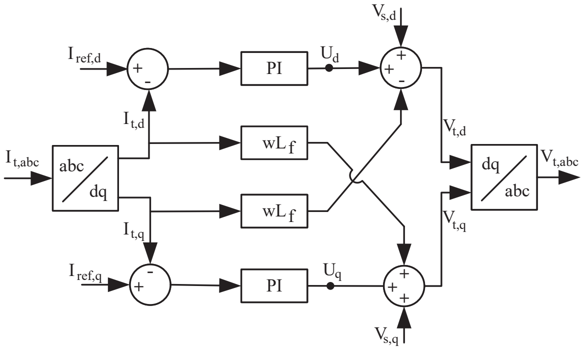

Fig. 2. Decoupled current control for d- and q-axes.

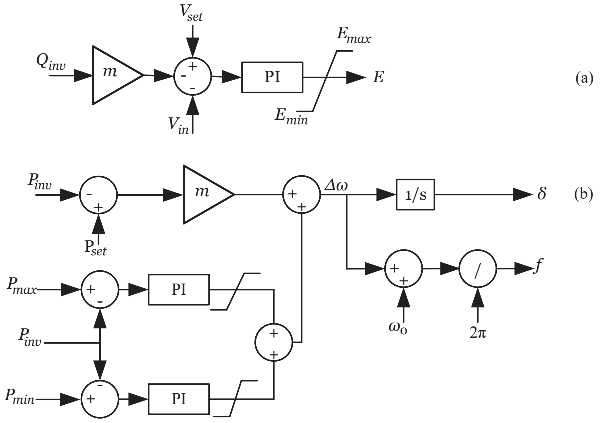

Fig. 3. Droop control for a grid-forming IBR: (a) Q-V (b) P-f.

B. Grid-Forming Mode

Droop control helps maintain the frequency and voltage of the grid within their nominal values in the grid-forming mode. Fig. 3(a) shows the Q-V droop control, which can change the reactive power of an IBR. If the grid voltage deviates from 1 pu, the reactive power will change to keep the grid voltage within the nominal range. Fig. 3(b) shows the P-f droop control, which can change the real power of an IBR. If the grid frequency deviates from 1 pu, the real power will change to keep the grid frequency within the nominal range [13]. Fig. 3 shows PI controllers in P-f and Q-V droop controls.

III. Cyber-Physical System

This section describes the physical layer, the cyber layer, and the co-simulation platform.

A. Physical Layer

A physical layer represents a power system. This work uses PSCAD to simulate the physical layer since it is the de facto industry standard tool for IBR modeling and simulation. Fig. 4 shows the single-line diagram of a microgrid with four IBRs, where the base power and voltage are 1 MVA and 12.47 kV. IBRs are connected to the grid via a transformer, where the primary and secondary voltages are 480 V and 12.47 kV. The DC bus voltage of the IBR is 1.2 kV, the output voltage of the IBR is 480 V, and the IBR maximum output power is 1 MVA. The IBR filter resistance is $2\,\text{m}\Omega$, and the IBR filter reactance is 30 μH. IBR 1 and IBR 2 are grid-forming, and

979-8-3503-1360-4/24/$31.00 ©2024 IEEE

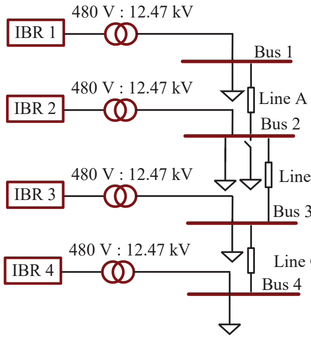

Fig. 4. Single-line diagram of the 100% inverter-based microgrid.

IBR 3 and IBR 4 are grid-following. For the grid-following mode, gains of the PI block are $k_P = 1.5$, $k_I = 0.003$. For the grid-forming mode, gains of the PI block in P-f droop control are $k_P = 0.5$, $k_I = 0.002$, and in Q-V droop control are $k_P = 0.5$, $k_I = 0.003$.

Line A connects bus 1 and bus 2, line B connects bus 2 and bus 3, and line C connects bus 3 and bus 4 together. Line A resistance and inductance are 1.4 Ω and 5.4 mH. Line B resistance and inductance are 2.2 Ω and 8.4 mH. Line C resistance and inductance are 0.6 Ω and 2.5 mH. A three-phase load is connected to each bus where its real power is 0.3 pu, and its reactive power is 0.03 pu. A dispatchable load is connected to bus 2, where its real power is 0.3 pu, and its reactive power is 0.03 pu.

B. Cyber Layer

A cyber layer represents a communication layer and can be simulated using Python. Communication links are modeled as first in first out (FIFO) queues. Fig. 5 shows the cyber layer, where each IBR has an RTU that sends the root mean square (RMS) value of the terminal voltage and current, the IBR real power, and the IBR reactive power to the control center. The control center receives measurements and sends reactive power set points to the IBR RTU; however, attackers can falsify the set points being sent to the IBR RTU. Fig. 5 shows the implementation of FDI attacks in the cyber layer, where the FDI block falsifies the set points received from the control center. A detection algorithm block is added between the FDI attacks block and the IBR RTU to enable detecting and mitigating the FDI attacks. Each inverter has a detection algorithm block, which is described in Section IV.

C. Co-Simulation Platform

In a cyber-physical system, a cyber and a physical system are simulated simultaneously, enabling the study of the cyber vulnerability of the grid. In this work, PSCAD simulates the physical layer. PSCAD can exchange data with other software, [15] studies PSCAD interface with MATLAB. In this work, the Python co-simulation block in PSCAD v5 is used to enable the exchange of data between the PSCAD and Python code. The cyber layer is added to the Python code. Fig. 6 shows how data is exchanged between the physical and the cyber layer.

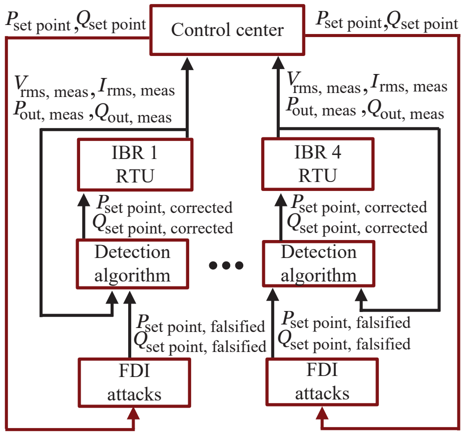
$P_{\text{set point}}, Q_{\text{set point}}$
Control center
$P_{\text{set point}}, Q_{\text{set point}}$
$V_{\text{rms, meas}}, I_{\text{rms, meas}}$
$P_{\text{out, meas}}, Q_{\text{out, meas}}$
$V_{\text{rms, meas}}, I_{\text{rms, meas}}$
$P_{\text{out, meas}}, Q_{\text{out, meas}}$
IBR 1 RTU
IBR 4 RTU
$P_{\text{set point, corrected}}$
$Q_{\text{set point, corrected}}$
$P_{\text{set point, corrected}}$
$Q_{\text{set point, corrected}}$
Detection algorithm
Detection algorithm
$P_{\text{set point, falsified}}$
$Q_{\text{set point, falsified}}$
$P_{\text{set point, falsified}}$
$Q_{\text{set point, falsified}}$
FDI attacks
FDI attacks

Fig. 5. Cyber layer of the microgrid.

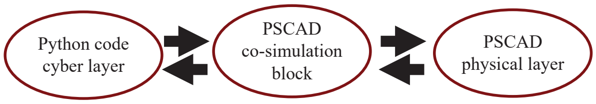

Fig. 6. Data exchange path of the co-simulation platform.

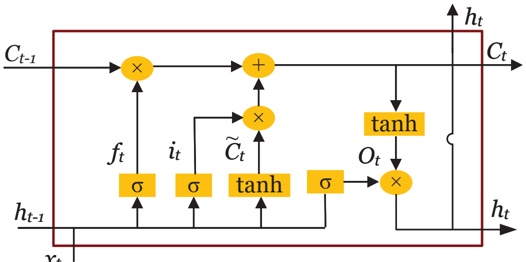

Fig. 7. Gates mechanism of an LSTM unit.

IV. Cyberattack Detection and Mitigation

This section introduces LSTM and then describes cyberattack detection and mitigation method.

A. Long Short-Term Memory

LSTM is widely used in time series prediction. LSTM uses gating mechanisms. Fig. 7 shows a unit of LSTM where C_{t-1} represents the previous cell states unit, x_t considers the input current signal, h_t is the current LSTM unit output, h_{t-1} is the previous LSTM unit output, i_t is the input gate, f_t is the forget gate, and O_t represents the output gate [16].

LSTM equations are shown as follows:

$$\begin{aligned}
f_t &= \sigma(W_f\,[h_{t-1}, x_t] + b_f),\\
i_t &= \sigma(W_i\,[h_{t-1}, x_t] + b_i),\\
\tilde{C}_t &= \tanh(W_C\,[h_{t-1}, x_t] + b_C),\\
C_t &= f_t\, C_{t-1} + i_t\, \tilde{C}_t\\
O_t &= \sigma(W_O\,[h_{t-1}, x_t] + b_O),\\
h_t &= O_t\, \tanh(C_t),\\
\sigma_x &= \frac{1}{1+e^{-x}},
\end{aligned} \tag{4}$$

where the forget gate selects the portion of data that will be used in the next steps. Once the input data decides which information should be added to the input state, the output

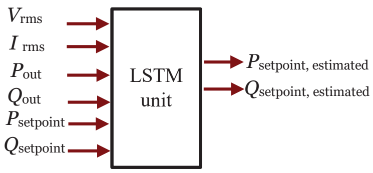

Fig. 8. Inputs and outputs of the LSTM block.

gate calculates the next hidden state [16]. The LSTM gate coefficients are set during the training process. LSTM uses a dataset, and the LSTM gate coefficients are updated at each training epoch to increase the LSTM prediction accuracy.

B. Proposed Method

Each IBR has an LSTM block to mitigate and detect FDI attacks on the real and reactive power set points. The RMS value of the current and voltage, the real power output of the IBR, the reactive power output of the IBR, the real power set point of the IBR, and the reactive power set point of the IBR are the LSTM block inputs as shown in Fig. 8. The estimated real and reactive power set points are the LSTM block outputs as shown in Fig. 8. Each LSTM unit uses 6 inputs, which helps keep the mitigation accuracy high even if one of the measurements is noisy due to sensor malfunction. The LSTM block estimates the power set points, and if the difference between the estimated and received set points is more than a threshold, the estimated set points are sent to the IBR FRTU instead of the received set points. The threshold is set based on the accuracy of LSTM under FDI attacks, and it is set to 7% in this work since the accuracy of the trained LSTM under various ramp and bias attacks is 94.1%.

C. LSTM Training and Parameters

The microgrid is simulated in PSCAD. For LSTM training, a data set is generated by simulating the ramp and bias attacks on the real and reactive power set points that cause voltage and frequency violations. The voltage and frequency violations happen if the bus voltage increases over 1.05 pu or decreases below 0.95 pu, and the frequency increases over 62 Hz or decreases below 58 Hz. 70% of the dataset is used for training, and the rest is used for testing the algorithm.

The LSTM is trained using the Keras library in Python 3.8, and its hyperparameters are set using trial and error. The LSTM has 3 hidden layers, where each hidden layer has 6 neurons the output of each layer is the input of the next hidden layer. LSTM algorithm is trained for 100 epochs, the activation function is $\tanh$, the optimizer is Adam, the optimizer learning rate is 0.001, and the loss function is MSE [17].

V. SIMULATION RESULTS

Attackers use positive bias attacks, negative bias attacks, positive ramp attacks, and negative ramp attacks on the reactive power set point of IBR 3 to cause overvoltage or undervoltage in the microgrid. The value of the bias and ramp FDI attacks are selected in a way that the voltage increases over 1.1 pu or decreases below 0.9 pu. Four cases are simulated. In all cases, the reactive power of IBR 3 is 0.03 pu before applying FDI attacks.

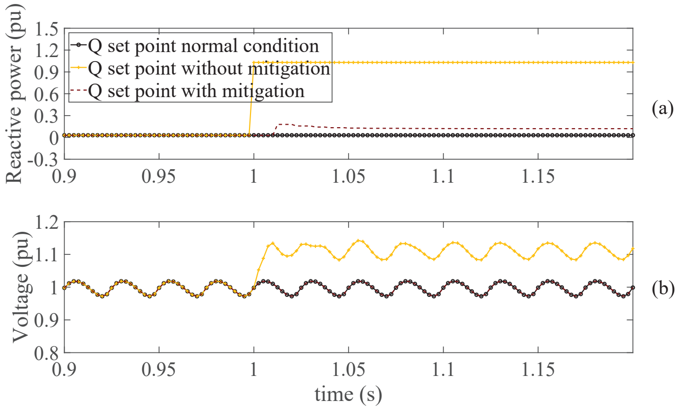

Fig. 9. Simulation results for the positive bias attack: (a) IBR 3 reactive power set point, (b) voltage of bus 3.

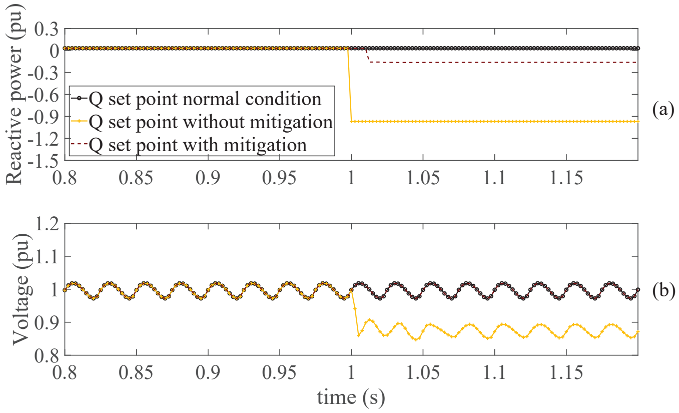

Fig. 10. Simulation results for the negative bias attack: (a) IBR 3 reactive power set point, (b) voltage of bus 3.

A. Case 1: Positive Bias Cyberattacks

Attackers launch an FDI cyberattack at $t = 1$ s and increase the reactive power set point of IBR 3 to 1 pu. Fig. 9(a) shows the reactive power set point under cyberattacks with and without the mitigation method and under normal conditions. Fig. 9(b) shows bus 3 voltage, where it increases from 1 pu to 1.11 pu when no detection and mitigation method is implemented in the microgrid. However, using the proposed method, the grid voltage does not change.

B. Case 2: Negative Bias Cyberattacks

Attackers launch an FDI cyberattack at $t = 1$ s and decrease the reactive power set point of IBR 3 to -1 pu. Fig. 10(a) shows the reactive power set point under cyberattacks with and without the mitigation method and under normal conditions. Fig. 10(b) shows bus 3 voltage, where it decreases from 1 pu to 0.88 pu when no detection and mitigation method is implemented in the microgrid. However, using the proposed method, the grid voltage does not change.

C. Case 3: Positive Ramp Cyberattacks

Attackers launch an FDI cyberattack at $t = 1$ s and increase the reactive power set point of IBR 3 to 1 pu using a ramp. Fig. 11(a) shows the reactive power set point under cyberattacks with and without the mitigation method and under normal conditions. Fig. 11(b) shows bus 3 voltage, where

979-8-3503-1360-4/24/$31.00 ©2024 IEEE

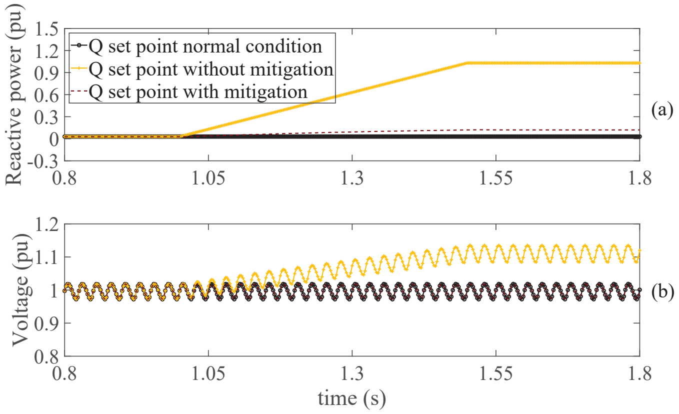

Fig. 11. Simulation results for the positive ramp attack: (a) IBR 3 reactive power set point, (b) voltage of bus 3.

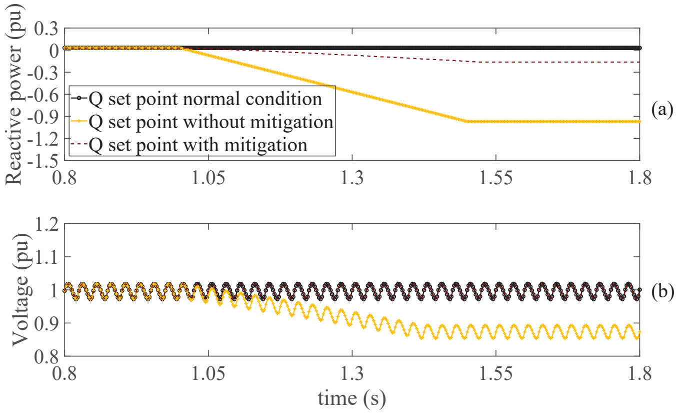

Fig. 12. Simulation results for the negative ramp attack: (a) IBR 3 reactive power set point, (b) voltage of bus 3.

it increases from 1 pu to 1.11 pu when no detection and mitigation method is implemented in the microgrid. However, using the proposed method, the grid voltage does not change.

D. Case 4: Negative Ramp Cyberattacks

Attackers launch an FDI cyberattack at $t = 1$ s and decrease the reactive power set point of IBR 3 to -1 pu using a ramp. Fig. 12(a) shows the reactive power set point with and without mitigation method and under normal conditions. Fig. 12(b) shows bus 3 voltage, where it decreases from 1 pu to 0.88 pu when no detection and mitigation method is implemented in the microgrid. However, using the proposed method, the grid voltage does not change.

VI. Conclusion

This work studies FDI attacks on the real and reactive power set points of IBRs in a 100% inverter-based microgrid. Ramp and bias FDI attacks on IBR set points can cause voltage instability. This work uses an LSTM-based method to mitigate and detect FDI attacks in a 100% inverter-based microgrid with four IBRs. Each IBR has an LSTM block, which uses the RMS current, RMS voltage, real and reactive power output, and real and reactive power set points of the IBR to estimate the real and reactive power set points of the IBR. If the difference between the estimated and the received set points is larger than the threshold, the estimated set points will be sent instead of the received set points to the IBR RTU. The microgrid is tested under four FDI attacks. A successful FDI attack changes the grid voltage by more than 0.11 pu; however, the grid voltage does not change under cyberattacks using the proposed detection method. Moreover, the implemented system in this work facilitates studying other types of cyberattacks such as DoS, delay, and replay attacks.

References

[1] U.S. Department of Energy (DoE), “On the path to 100% clean electricity,” Aug. 2023. [Online]. Available: https://www.energy.gov/policy/articles/path-100-clean-electricity

[2] T. Nguyen, S. Wang, M. Alhazmi, M. Nazemi, A. Estebsari, and P. Dehghanian, “Electric power grid resilience to cyber adversaries: State of the art,” *IEEE Access*, vol. 8, May 2020.

[3] U.S. Department of Energy (DoE), “Electric disturbance events annual summaries[online],” Aug. 2023. [Online]. Available: https://www.oe.netl.doe.gov/OE417_annual_summary.aspx

[4] A. Teymouri, A. Mehrizi-Sani, and C.-C. Liu, “Cyber security risk assessment of solar PV units with reactive power capability,” *IECON - 44th Annual Conference of the IEEE Industrial Electronics Society*, Oct. 2018.

[5] A. Zabetian-Hosseini, A. Mehrizi-Sani, and C.-C. Liu, “Cyberattack to cyber-physical model of wind farm SCADA,” *IECON - 44th Annual Conference of the IEEE Industrial Electronics Society*, Oct. 2018.

[6] M. Karanfil, D. E. Rebbah, M. Debbabi, M. Kassouf, M. Ghafouri, E.-N. S. Youssef, and A. Hanna, “Detection of microgrid cyberattacks using network and system management,” *IEEE Transactions on Smart Grid*, vol. 14, no. 3, Nov. 2022.

[7] K. Xiahou, Y. Liu, and Q. H. Wu, “Decentralized detection and mitigation of multiple false data injection attacks in multiarea power systems,” *IEEE Journal of Emerging and Selected Topics in Industrial Electronics*, vol. 3, no. 1, Jan. 2022.

[8] M. Beikbabaei and A. Mehrizi-Sani, “Detection and mitigation of cyberattacks on Volt-Var control,” *CIGRE Symposium Australia*, Sep. 2023.

[9] M. R. Habibi, H. R. Baghaee, F. Blaabjerg, and T. Dragicevic, “Secure control of DC microgrids for instant detection and mitigation of cyber-attacks based on artificial intelligence,” *IEEE Systems Journal*, vol. 16, no. 2, Jun. 2022.

[10] M. Wilson, H. Mahmood, and J. Giordano, “Detection and mitigation of cyberattacks against power measurement channels using LSTM neural networks,” *IEEE Energy Conversion Congress and Exposition (ECCE)*, Oct. 2021.

[11] A. Takiddin, M. Ismail, U. Zafar, and E. Serpedin, “Deep autoencoder-based anomaly detection of electricity theft cyberattacks in smart grids,” *IEEE Systems Journal*, vol. 16, no. 3, Jan. 2022.

[12] F. Li, Q. Li, J. Zhang, J. Kou, J. Ye, W. Song, and H. A. Mantooth, “Detection and diagnosis of data integrity attacks in solar farms based on multilayer long short-term memory network,” *IEEE Transactions on Power Electronics*, vol. 36, no. 3, Mar. 2021.

[13] W. Du, F. K. Tuffner, K. P. Schneider, R. H. Lasseter, J. Xie, Z. Chen, and B. Bhattarai, “Modeling of grid-forming and grid-following inverters for dynamic simulation of large-scale distribution systems,” *IEEE Transactions on Power Delivery*, vol. 36, no. 4, Aug. 2021.

[14] M. Yazdanian and A. Mehrizi-Sani, “Internal model-based current control of the RL filter-based voltage-sourced converter,” *IEEE Transactions on Energy Conversion*, vol. 29, no. 4, Sep. 2014.

[15] S. Filizadeh, M. Heidari, A. Mehrizi-Sani, J. Jatskevich, and J. A. Martinez, “Techniques for interfacing electromagnetic transient simulation programs with general mathematical tools IEEE taskforce on interfacing techniques for simulation tools,” *IEEE Transactions on Power Delivery*, vol. 23, no. 4, Oct. 2008.

[16] F. A. Gers, N. N. Schraudolph, and J. Schmidhuber, “Learning precise timing with LSTM recurrent networks,” *Journal of Machine Learning Research*, vol. 3, Aug. 2002.

[17] Tensorflow API notebook, “Notebooks for keras lstm [online],” Oct. 2023. [Online]. Available: https://www.tensorflow.org/api_docs/python/tf/keras/layers/LSTM

979-8-3503-1360-4/24/$31.00 ©2024 IEEE