# Cyber Vulnerability Assessment of Microgrids with 5G-Enabled Distributed Control

Ardavan Mohammadhassani, Yousef Akbar, Ali Mehrizi-Sani, and Haining Wang
The Bradley Department of Electrical and Computer Engineering
Virginia Polytechnic Institute and State University, Blacksburg, VA 24061
Emails:{ardavanmh93,akbary,mehrizi,hnw}@vt.edu

***Abstract*—Enabling communication between the individual controllers of inverter-based resources (IBR) in a microgrid can result in improved system-wide response. However, it increases the vulnerability of microgrids to cyberattacks. This paper investigates the effects of cyberattacks on microgrids with 5G-enabled coordinated set point modulation (5GCSPM). A modified CIGRE North American MV distribution benchmark system with 28 IBRs equipped with 5GCSPM is built in PSCAD/EMTDC as the physical layer. A cyber-physical system is created by enabling TCP/IP communication between PSCAD/EMTDC and Raspberry Pi4. Different cyberattacks are carried out on the TCP/IP connection while running time-domain simulation studies to evaluate the performance of 5GCSPM.**

***Index Terms*—5G mobile communication, cyberattack, cyber-physical systems, distributed control, distributed power generation, microgrids, renewable energy sources.**

## I. Introduction

The power distribution system is experiencing an increasing growth in the interconnection of inverter-based resources (IBR) in the form of microgrids [1], [2]. Operating in either grid-connected or islanded mode, microgrids have enough generation capacity to supply loads in their own domain. Therefore, they can maintain power supply in case of faults in the main grid. They can also provide restoration assistance to the main grid if they have excess generation. Currently, the most common microgrid control technology is centralized control [3]. However, centralized control may not function properly when the number of IBRs is large. Several reasons can explain this, including:

1) Increased computational burden;
2) Frequent redesign requirements as a change in one unit affects the central controller;
3) Reliability and security issues due to the central controller being a single point of failure.

Thus, noncentralized control methods might be a more suitable choice for microgrids with a large number of IBRs [4]–[6]. Noncentralized methods can be classified into two groups: decentralized and distributed methods. Decentralized methods assume that the interactions between the subsystems is negligible and no communications are required. However, this assumption is not always true and results in a poor system-wide response. Contrarily, distributed control methods do consider communication between the subsystems. However, the need for a distributed control method becomes more significant in secondary and tertiary control as the need for high reliability, security, and situational awareness arises. Meanwhile, choosing the right communication technology for distributed control is a complicated task [7], [8]. Currently, the optical fiber technology is commonly used in power systems because of its high reliability and speed. However, this technology requires a large capital investment and expensive maintenance. It also does not scale well when more IBRs are added to the microgrid. Wireless technologies such as Wi-Fi and ZigBee are less costly than optical fiber and also scale well. However, they are susceptible to interference and offer lower speeds. On the other hand, 5G offers superior performance due to its several features, including ultra reliable low latency communication (URLLC), massive machine type communication (mMTC), and enhanced mobile broadband (eMBB) [9]. This make 5G a suitable choice for enabling communications in distributed control methodologies.

5G builds up on existing advanced technologies using innovative new techniques. However, this also makes 5G networks an attractive target for cybercriminals. Security challenges rise from different reasons, including the IP-based open architecture of 5G, the diversity of 5G access network technologies, and non-security-professional device operators [9]–[12]. In case of 5G-enabled distributed control, cyberattacks can target both control and communication entities of a microgrid, ranging from tampering with sensory information, corrupting control signals by false data injection (FDI), and blocking data transmission on the communication links through denial-of-service (DoS) attacks [13]. Depending on the skill set of an attacker and the degree of information available to them, the severity of the consequences of an attack on a microgrid can vary from stopping ancillary services and power flow management systems to immediate system shutdown. Therefore, the performance of the microgrid with 5G-enabled distributed control should be studied under cyberattack scenarios to outline its vulnerabilities for future resilient and cybersecure designs.

This paper studies the performance of an inverter-based microgrid with 5G-enabled coordinated set point modulation (5GCSPM) under different cyberattack scenarios. 5GC-

This work was supported in part by the National Science Foundation (NSF) under awards ECCS-1953198 and EECS-1953213, in part by Manitoba Hydro International, and in part by the Commonwealth Cyber Initiative (CCI), an investment by the Commonwealth of Virginia in the advancement of cyber R&D, innovation, and workforce development.

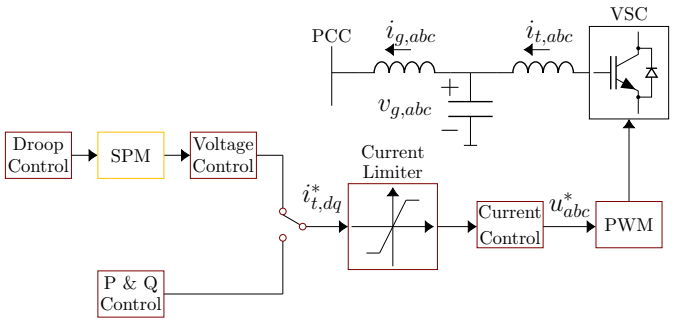


Fig. 1. Block diagram representation of a conventional IBR control system equipped with SPM.

SPM is implemented on a modified CIGRE North American MV distribution benchmark system with 28 IBRs in PSCAD/EMTDC software to construct the physical layer. The cyber-physical system is created using the cosimulation tool in PSCAD to establish a TCP/IP connection with a Raspberry Pi4. Time-domain simulation case studies are carried out in PSCAD/EMTDC software to evaluate the performance of 5GCSPM under different cyberattack scenarios conducted on the TCP/IP connection using pcap and scapy modules in Python.

The rest of this paper is structured as follows. Section II presents a brief overview of 5GCSPM. Section III outlines the cyber vulnerabilities of 5GCSPM. Performance evaluation of the 5GCSPM under different cyberattacks is presented in Section IV. Finally, conclusions are provided in Section V.

## II. Overview of Coordinated Set Point Modulation

### A. A Brief Introduction on Online Set Point Modulation

Fig. 1 shows the conventional control method for IBRs with LCL filters equipped with set point modulation (SPM) [14]. During grid-connected mode of operation, the output current references of the voltage-sourced converter (VSC) $i^*_{t,dq}$ are generated by the P&Q control block. On the other hand, the droop control and voltage control blocks generate $i^*_{t,dq}$ during islanded mode of operation. The islanded mode of operation is considered in this paper. The SPM block generates the modulated set points for the voltage control block using

$$v^{'*}_{t,d} = v^*_{t,d} + m e_{t,d}\,(t)\,, \tag{1}$$

where $e_{t,d}\,(t)$ is the tracking error and $m$ is a design parameter. SPM utilizes predicted error $\hat{e}_{\text{pred}}\,(t)$ to improve its dynamic response. Therefore, (1) becomes

$$v^{'*}_{t,d} = v^*_{t,d} + m\hat{e}_{\text{pred}}\,(t)\,. \tag{2}$$

Communications should be enabled between IBRs to improve system-wide response.

### B. Overview of Coordinated Set Point Modulation

Fig. 2 shows a sample radial microgrid with $N$ IBRs equipped with 5GCSPM [15]. This microgrid can be represented using a complex-weighted graph $\chi = (\nu_\chi, \varepsilon_\chi)$, where the vertices $\nu_\chi = \{\nu_1, \nu_2, \ldots, \nu_N\}$ are the IBR buses and the edges $\varepsilon_\chi \subseteq \nu_\chi \times \nu_\chi$ are the electrical interconnections.

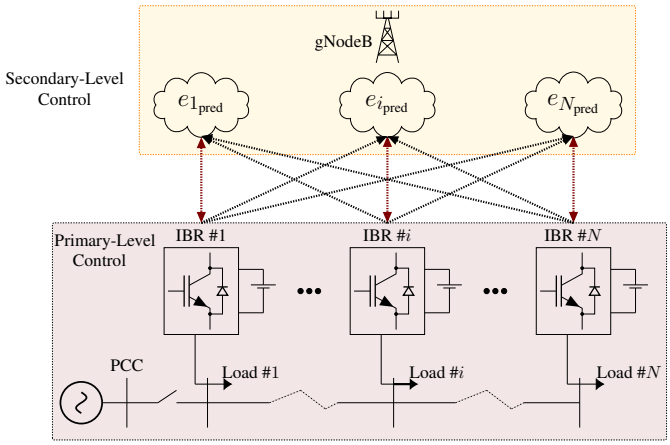


Fig. 2. A radial microgrid with $N$ IBRs equipped with 5GCSPM.

In CSPM, it is assumed that the $N$ IBRs have the capability to communicate with each other over an undirected communication graph $\varrho = (\nu_\varrho, \varepsilon_\varrho)$, where the vertices $\nu_\varrho = \{\nu_1, \nu_2, \ldots, \nu_N\}$ correspond to the vertices in $\chi$ and the edges $\varepsilon_\varrho \subseteq \nu_\varrho \times \nu_\varrho$ represent the communication links for the IBRs, which are not necessarily the same as their electrical interconnections. The adjacency matrix for the communications network is defined as $A = [a_{ij}] \subseteq \mathbb{R}^{n\times n}$, where $a_{ij} = 1$ defines an active communication link between IBRs $i$ and $j$ via the connected edge $(\nu_i, \nu_j) \in \varepsilon_\varrho$ and $a_{ij} = 0$ defines no connectivity.

Primary-level control for the sample radial microgrid in Fig. 2 uses SPM for each IBR in standalone mode. Therefore, no communication is used at this level of control. The modulated set point for the $i$th IBR is found using (3) by using linear error prediction as

$$\hat{e}_{i_{\text{pred}}}\,(t_0 + T_{\text{pred}}) = e_i\,(t_0) + r\,(t_0)\,T_{\text{pred}}, \tag{3}$$

where $T_{\text{pred}}$ is the prediction horizon and $r$ is the average rate of change calculated over previous measurements using the least squares method. Secondary-level control, however, is the level of control that enables coordination among the $N$ IBRs and requires exchange of information between the IBRs. Therefore, the set point for the $i$th IBR is modulated using

$$v^{''*}_{ti,d} = v^*_{ti,d} + m_i\hat{e}_{i_{\text{pred}}}\,(t) + m_i \sum_{j=1, j\neq i}^{N} a_{ij}\hat{e}_{j_{\text{pred}}}\,(t)\,, \tag{4}$$

where $\hat{e}_{j_{\text{pred}}}$ is the predicted error of the $j$th IBR.

Communication between the IBRs is enabled using 5G wireless communication technology designed in [16]. The packet generated by the $i$th IBR is first uploaded to the gNodeB. Then, the uploaded packet is downloaded by the $j$th IBR. The gNodeB is in charge of scheduling which IBRs are allowed to upload and download packets using the MAD algorithm. The IBRs generate packets at will, which means they generate a fresh packet whenever they are selected by the gNodeB. This means that the 5G numerology $\mu = 0$ and the transmission time interval (TTI) is 1 ms, which is justified because IBRs generate packets at a much faster rate than TTI.

## III. Cyber-Threat Analysis of 5GCSPM

### A. Overview of Security Challenges in 5G

5G aims to provide 1–10 Gbps data rates and almost 100% coverage by installing multiple base stations to provide improved quality of service (QoS) and extremely low latency [17]. On the other hand, the inheritance of IP-based communication technology from 4G and the large number of user-end devices significantly extends the range of cyber threats in 5G. 5G is proposed to connect critical infrastructure, such as the power system, that require tight security measures to ensure their safety. Therefore, its vulnerabilities should be outlined for future resilient designs.

The three main vulnerable points in 5G security are the mobile cloud computing, software-defined networking (SDN), and communication channels. Cloud computing shares a number of services among multiple users. Therefore, it is possible for an adversary to attack cloud computing resources through different ways such as targeting physical devices, application-based threats, and attacking the cloud server via denial-of-service (DoS) attacks. The central nature of SDN introduces several ways for cybercriminals to attack the SDN. The controller traffic in SDN can be easily identified, which makes it a favorable choice for DoS attacks. Moreover, installation of malicious software can cause chaos across the network as almost every network function is implemented through software. Pre-5G mobile networks utilized GTP and IPSec tunnels to secure their communication channels. Mobile network communication interfaces such as X2, S1, S6, and S7 are significantly complex to attack. However, SDN-based 5G networks offer only common SDN interfaces. These interfaces are commonly protected with transport layer security (TLS) or secure socket layer (SSL). However, TLS or SSL sessions are highly vulnerable to IP layer attacks and SDN scanner attacks.

### B. Overview of Cyber Vulnerabilities in 5GCSPM

An adversary can target both measurement and control entities of a microgrid, including tampering with current and voltage transformer and phasor measurement unit measurements and manipulating control systems to change system dynamics and create instability. The IBR control algorithms, such as the one shown in Fig. 1, are implemented on real-time processors. Intrusion into the processor will allow access only to reference setpoints, i.e. $v^*_{t,d}$ and $v^{'*}_{t,d}$. An attacker can change $v^*_{t,d}$ and $v^{'*}_{t,d}$ to create a disturbance and cause instability by activating the protection apparatus. Moreover, in a 5GCSPM framework, the IBRs exchange their $\hat{e}_{i_{\text{pred}}}$ signals via communication links. Manipulation of $\hat{e}_{i_{\text{pred}}}$ values via false data injection (FDI) attacks can change system dynamics to a point that the IBRs lose concensus and the microgrid becomes unstable. DoS attacks on IBRs can lead to their disconnection from the microgrid and cause system-wide disturbances.

Microgrids have a smaller size than the power system and thus are more vulnerable to disturbances. Therefore, cyber-attacks can put the stability of the microgrid at risk. Some common attack scenarios for microgrids are summarized as below:

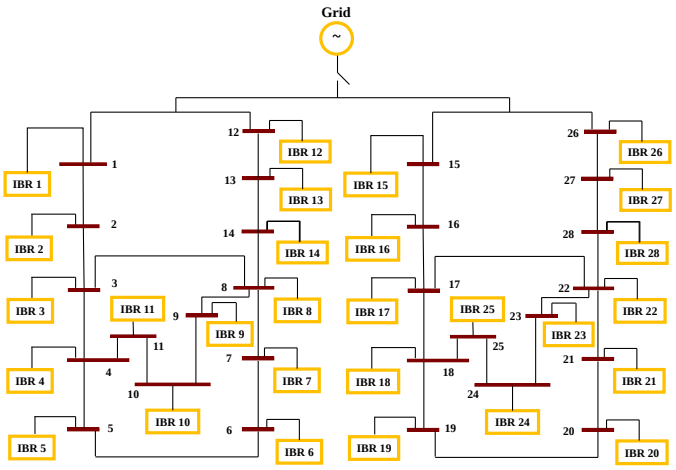


Fig. 3. Modified CIGRE North American MV distribution benchmark system with 28 IBRs (loads are not shown).

- **Sensor Malfunction:** Corrupting sensory information is usually done by an attacker from inside an organization. Trojan horse malware program can be used to control the data acquisition system as a remote host. Adding a bias in the reported data through changing sensor gains is a common attack on sensory information.
- **Communication Link Intrusion:** Attacks on communications are usually done via FDI or DoS. FDI attacks can occur on data either inside in the controller or inside networking apparatus. Packets can be manipulated in several ways including authroization violation, illegitimate log access, and replaying past data.
- **Controller Manipulation:** The reference inputs of the real-time controller can be changed using a trojan horse malware.

## IV. Performance Evaluation

In this paper, the modified CIGRE North American MV distribution benchmark system with 28 IBRs, also shown in Fig. 3, is modeled in PSCAD/EMTDC software as the physical layer. The communication graph between the IBRs is constructed as follows:

- IBR 1 communicates with IBRs 2 and 14.
- IBR 14 communicates with IBRs 1 and 13.
- IBR 15 communicates with IBRs 16 and 29.
- IBR 28 communicates with IBRs 27 and 15.
- For $i \neq 1, 14, 15, 28$: IBR i communicates with IBR $i-1$ and IBR $i+1$.

The cyber layer is created by establishing a TCP/IP connection between PSCAD/EMTDC and Raspberry Pi4. Various cyber-attack scenarios are carried out on the TCP/IP connection during time-domain simulation case studies to evaluate the performance of the 5GCSPM.

### A. Case 1: DoS Attack on a Single IBR

Fig. 4 shows the simulation results for Case 1. Prior to $t = 100$ ms, the microgrid is in the steady state. At $t = 100$ ms, the load at bus 1 disconnects. A TCP/IP packet with a reset flag is injected to communication link to simulate a DoS

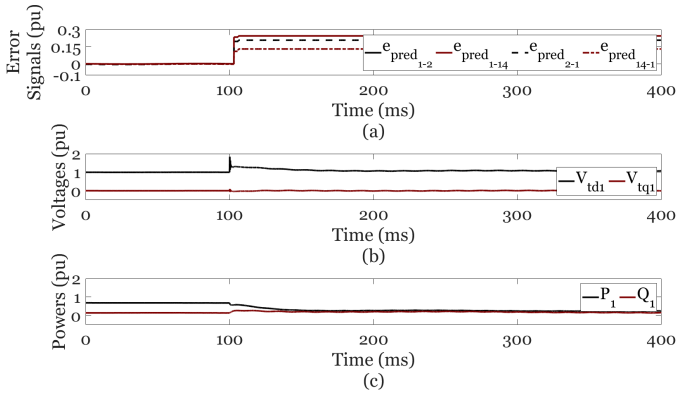


Fig. 4. Simulation results for Case 1: (a) exchanged error signals, (b) output voltages of IBR1, and (c) output power of IBR1.

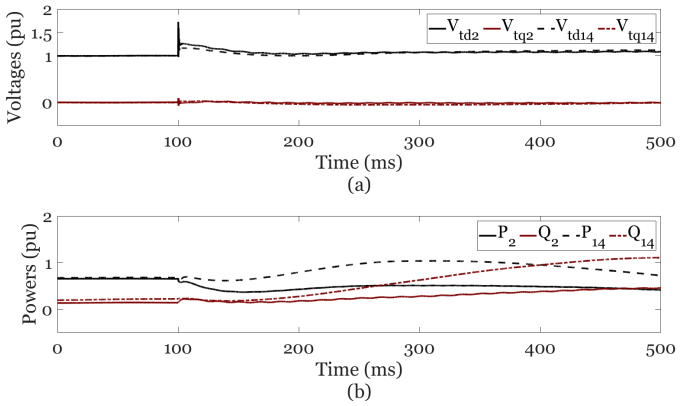


Fig. 5. Simulation results for Case 2: (a) output voltages of IBR2 and IBR14 and (b) output powers of IBR2 and IBR14.

attack on IBR1. Fig. 4(a) shows that after the DoS attack, the error signals to and from IBR1 become constant. Fig. 4(b) shows that $V_{td1}$ overshoots to 1.84 pu and settles at 1.08 pu after 200 ms. Fig. 4(c) shows the output powers of IBR1. This figure shows that active power decreases while reactive power increases. This is because the DoS attack causes IBR1 to increase its output voltage and thus increase $Q_1$.

### *B. Case 2: DoS Attacks on Multiple IBRs*

Fig. 5 shows the simulation results for Case 2. Prior to $t =$ 100 ms, the microgrid is in the steady state. At $t = 100$ ms, the load at bus 1 disconnects. A TCP/IP packet with a reset flag is injected to communication link to simulate DoS attacks on IBR1, IBR2, and IBR14. Fig. 5(a) shows that $V_{td2}$ overshoots to 1.72 pu, while $V_{td14}$ overshoots to 1.2 pu. Both voltages settle at 1.1 pu after 200 ms. Fig. 5(b) shows the oscillatory output powers of IBR2 and IBR14 with the output powers of IBR14 surpassing 1 pu.

### *C. Case 3: False Data Injection into a Single IBR*

Fig. 6 shows the simulation results for Case 3. Prior to $t = 100$ ms, the microgrid is in the steady state. At $t =$ 100 ms, the error signals received by IBR1 are manipulated by injecting a sinusoidal signal $u = \sin(60 \times 2\pi t)$. Fig. 6(a) shows that the error signals received by IBR1 are turned into sine waves. This causes the output voltages of IBR1 to have a

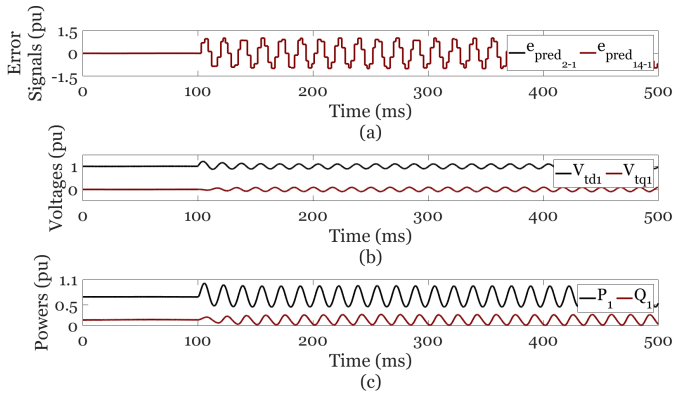


Fig. 6. Simulation results for Case 3: (a) error signals from IBR1, (b) output voltages of IBR1, and (c) output powers of IBR1.

sinusoidal shape as well, as shown in Fig. 6(b). Therefore, the three-phase output voltages will become distorted. Fig. 6(c) shows the output power injected by IBR1. This figure shows that the real and reactive powers become oscillatory with large variations. Since the IBRs communicate with each other via the underlying communication graph, the sinusoidal variation appears in all IBRs.

## V. Conclusions

Enabling 5G communication between IBRs in a microgrid can result in improved performance of CSPM. However, this also opens the gateway to cyberthreats. This paper evaluates the performance of 5GCSPM under different cyberattack scenarios to outline its vulnerabilities for future cybersecure designs. The modified CIGRE North American MV distribution benchmark system with 28 IBRs is built in PSCAD/EMTDC software to construct the physical layer. The cyber layer is created by enabling TCP/IP communications between PSCAD/EMTDC and Raspberry Pi4. DoS and FDI attacks are conducted on the TCP/IP connection to evaluate the performance of 5GCSPM during time-domain simulations. Simulation results demonstrate that cyberattacks can have a adverse effect on the stability of 5GCSPM by changing the output voltage and power of IBRs.

## References


[1] "Renewables became the second-most prevalent U.S. electricity source in 2020," *U.S. Energy Information Administration*, Jul. 2021. [Online]. Available: https://www.eia.gov/todayinenergy/detail.php?id=48896#

[2] B. Mohandes, M. S. E. Moursi, N. Hatziargyriou, and S. E. Khatib, "A review of power system flexibility with high penetration of renewables," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 3140–3155, Jul. 2019.

[3] D. E. Olivares, A. Mehrizi-Sani, A. H. Etemadi, C. A. Cañizares, R. Iravani, M. Kazerani, A. H. Hajimiragha, O. Gomis-Bellmunt, M. Saeedifard, R. Palma-Behnke, G. A. Jiménez-Estévez, and N. D. Hatziargyriou, "Trends in microgrid control," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1905–1919, Jul. 2014.

[4] M. Yazdanian and A. Mehrizi-Sani, "Distributed control techniques in microgrids," *IEEE Trans. Smart Grid*, vol. 5, no. 6, pp. 2901–2909, Nov. 2014.

[5] Q. Zhou, M. Shahidehpour, A. Paaso, S. Bahramirad, A. Alabdulwahab, and A. Abusorrah, "Distributed control and communication strategies in networked microgrids," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2586–2633, Fourthquarter 2020.

[6] E. Espina, J. Llanos, C. Burgos-Mellado, R. Cárdenas-Dobson, M. Martínez-Gómez, and D. Sáez, "Distributed control strategies for microgrids: An overview," *IEEE Access*, vol. 8, pp. 193 412–193 448, Oct. 2020.
[7] I. Serban, S. Céspedes, C. Marinescu, C. A. Azurdia-Meza, J. S. Gómez, and D. S. Hueichapan, "Communication requirements in microgrids: A practical survey," *IEEE Access*, vol. 8, pp. 47 694–47 712, Mar. 2020.
[8] S. Liu, X. Wang, and P. X. Liu, "Impact of communication delays on secondary frequency control in an islanded microgrid," *IEEE Trans. Ind. Electron.*, vol. 62, no. 4, pp. 2021–2031, Apr. 2015.
[9] J. Rodriguez, "Fundamentals of 5G mobile networks," *Wiley*, 2014.
[10] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3682–3722, Fourthquarter 2019.
[11] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, Dec. 2018.
[12] M. Wazid, A. K. Das, S. Shetty, P. Gope, and J. J. P. C. Rodrigues, "Security in 5G-enabled internet of things communication: Issues, challenges, and future research roadmap," *IEEE Access*, vol. 9, pp. 4466–4489, Dec. 2021.
[13] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Cyber security in control of grid-tied power electronic converters—challenges and vulnerabilities," *IEEE Trans. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 5, pp. 5326–5340, Oct. 2021.
[14] A. Mehrizi-Sani and R. Iravani, "Online set point modulation to enhance microgrid dynamic response: Theoretical foundation," *IEEE Trans. Power Syst.*, vol. 27, no. 4, pp. 2167–2174, Nov. 2012.
[15] H. Ghaffarzadeh and A. Mehrizi-Sani, "Adaptive set point modulation to mitigate transients in power systems," *IET Gener. Transm. Distrib.*, vol. 14, no. 23, p. 5463–5470, Dec. 2020.
[16] R. Iyer, B. Choudhury, V. K. Shah, and A. Mehrizi-Sani, "Power systems performance under 5G radio access network in a co-simulation environment," *2021 IEEE ISIE*, Dec. 2021.
[17] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1617–1655, thirdquarter 2016.