False Data Injection Attacks Against Synchronization Systems in Microgrids

Amr S. Mohamed, Mohammadreza F. M. Arani, *Member, IEEE*, Amir Abiri Jahromi, *Senior Member, IEEE*, and Deepa Kundur, *Fellow, IEEE*

***Abstract*—Synchronization systems play a vital role in the day-to-day operation of power systems and their restoration after cascading failures. Hence, their resilience to cyberattacks is imperative. In this paper, we demonstrate that a well-planned false data injection attack against the synchronization system of a generator is capable of causing tripping subsequently leading to instability and blackout. We present an analytical framework behind the design and implementation of the proposed cyberattack. Moreover, we derive and discuss the conditions for which a cyberattack interfering with a synchronizing signal can be successful. Effective physical mitigation strategies are then proposed to improve the cyber-resilience of synchronization systems. The proposed cyberattack model and mitigation strategies are verified for a microgrid test system using an OPAL-RT real-time simulator.**

***Index Terms*—Cyber-physical systems, resilience, cyberattack, power system restoration, synchronization systems, microgrids.**

I. Introduction

CONCERNS about the cybersecurity of power systems have been on the rise in recent years particularly following the cyberattacks against the Ukrainian electricity infrastructure [1]–[3]. The North American Electric Reliability Corporation (NERC) has taken initial steps towards addressing these concerns by mandating the critical infrastructure protection (CIP) standards. The CIP standards require the identification, categorization and protection of cyber assets that are essential to the reliable operation of the bulk electric system [4]. Yet, one of the main challenges facing the cybersecurity of power systems is their scale and complexity as well as their extensive reliance on information and communication technologies [5].

The cybersecurity of power systems control has been examined extensively in recent years at the generation, transmission and distribution levels [6]. Yet, most of the literature on the cybersecurity of generation control loops has been focused on automatic generation control (AGC) [7]–[9]. This is mainly because AGC relies on supervisory control and data acquisition (SCADA) systems. In contrast, the cybersecurity of automatic voltage regulation, governor and synchronization control has received little attention since they commonly rely on local control loops. Resilient synchrony of microgrids is another topic that has gained attention in recent years [10]–[14]. These papers are mostly focused on cyberattacks against the secondary frequency control of inverter-based microgrids during continuous islanded operation mode. These papers do not investigate the resilience of the reconnection process of islanded microgrids and the synchronization system used for this purpose which is investigated in this paper.

Synchronization systems play a vital role in the day-to-day operation of power systems as well as their restoration after cascading failures [15]. These systems have traditionally been used for bringing baseload, peaking or standby generators online and connecting them to the grid, as well as reconnecting two synchronous systems during black start or after system separation following a disturbance [16], [17]. Today, synchronization systems play additional roles such as connecting islanded microgrids to the main grid [18]–[20].

Synchronization systems bring the voltage, frequency, and phase angle differences between two spinning systems into tolerable thresholds before safely connecting them by closing the interconnecting circuit breaker (CB) [21], [22]. The synchronization system essentially adjusts the frequency and voltage of the spinning systems by sending control commands to the governor and exciter of a generator or a set of generators [23], [24] and can be managed manually by the system operator, by using auto-synchronization systems, or through some combination of both [16].

Correct synchronization is critical to prevent damage to generators or disturbance when connecting two or more power systems [25]. As such, synchronization systems typically include multiple levels of supervision including an automatic synchronization controller (ASC) and a human operator overseeing it. Synchronism-check and voltage relays may be employed as additional levels of supervision to prevent an interconnecting CB from closing during faulty synchronization conditions [26]–[28]. This is while no supervision exists on the synchronizing signal communicated from the ASC to the generator exciter and governor. Traditionally, the integrity of the synchronizing signal has not been of concern due to the absence of remote access to the synchronization system and the reliance on hardwired communication of signals from the synchronization panel to the control systems of the governor, exciter and interconnecting CB [28].

This characteristic has been changing rapidly in recent years

The authors wish to acknowledge the NSERC Discovery Grants Program and NSERC Strategic Partnerships for Projects Programs as well as Fonds de Recherche du Québec – Nature et Technologies (FRQNT) postdoctoral fellowship for providing funding for this work.

Amr S. Mohamed, and D. Kundur are with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada. (e-mails: amr.mohamed@mail.utoronto.ca, dkundur@ece.utoronto.ca)

Mohammadreza F. M. Arani is with the Department of Electrical, Computer & Biomedical Engineering, Ryerson University, Toronto, ON M5B 2K3, Canada. (e-mail:marani@ryerson.ca)

A. Abiri Jahromi is with the School of Electronic and Electrical Engineering, University of Leeds, Leeds, LS2 9JT, United Kingdom. (e-mail:a.abirijahromi@leeds.ac.uk)

due to the need for improved reliability, reduced installation costs, as well as the movement toward automation and remote synchronization, particularly in the case of microgrids [28]–[30]. Emerging synchronization systems provide remote access features and employ open data transmission protocols on fiber-optic or Ethernet based communication to send correction pulses to the generator governor and exciter to automatically adjust the frequency and voltage during synchronization [31], [32]. A cyberattacker may infiltrate such a system more easily and proceed to install malware on the ASC, or access the communication channel of the synchronization system by adding a new malicious communication device. Subsequently, the cyberattacker can send corrupted control commands to the generator governor or exciter to cause a generator trip, stability problems and/or a potential blackout.

The impact of attacks targeting automatic synchronization systems has been recently studied by Kandasamy in [33]. It is demonstrated in [33] that cyberattacks can delay the synchronization of a generator indefinitely. This paper expands on the work presented in [33] by considering how FDI attacks against synchronization systems can be executed in the context of microgrids. In this paper, we study a FDI attack model targeting automatic synchronization systems in microgrids which not only hinders the synchronization, but can also directly trip a generator potentially leading to microgrid blackout.

We present the analytical framework behind the design and implementation of the cyberattack. Sensitivity analyses of system parameters and how they may influence the success of the cyberattack are further performed and presented. Afterwards, we propose two physical mitigation strategies to enhance the cyber-resilience of synchronization systems.

The main contributions of this paper are as follows:

- For the first time, we investigate cyberattacks interfering with the microgrid synchronization process. We discuss how emerging synchronization systems in microgrids enable cyber vulnerabilities which allow a skilled attacker to execute FDI attacks with severe consequences. We demonstrate that the attacker is able to exploit system resonance and influence the microgrid frequency to rapidly trip a generator which may potentially lead to microgrid blackout.
- We present an analytical framework for designing novel attacks against synchronization systems. The framework incorporates understanding of the operation of industrial ASC devices and theoretical analysis of synchronization control. The framework highlights the threats of periodic FDI attacks, and yields success conditions for the attacks and design guidelines for the FDI attack signal. The framework also identifies the fastest attack for tripping a generator by attacking its synchronization system.
- We develop and implement two physical mitigation strategies to prevent the success of the attacks. Based on theoretical analysis of synchronization control, we derive equations to calculate the threshold for an anomaly detection based strategy, and the saturation value for a limiter-block based strategy.

We validate the FDI attacks and mitigation strategies via real-time simulations using a detailed microgrid model on OPAL-RT HyperSim simulator.

The remainder of this paper is organized as follows. In Section II, we present the attack model against synchronization systems. The analytical framework is established in Section III for designing a successful cyberattack. Moreover, sensitivity analyses are performed to examine how variations in the system parameters may affect the success of the attack against synchronization systems. In Section IV, the mitigation strategies are developed and their impact on synchronization process is assessed. Section V details empirical testing and verification of the proposed mitigation strategies on a microgrid test system using an OPAL-RT real-time simulator. We provide the concluding remarks in Section VI.

II. Attack Model

Despite the massive integration of inverter-interfaced distributed energy resources (DERs) such as wind and solar, synchronous generators continue to play the key role in the synchronization of bulk power systems and microgrids. This paper investigates the cybersecurity of the synchronization systems of synchronous generators in microgrids. Nevertheless, the findings are applicable more generally to the cybersecurity of generator synchronization in bulk power systems.

Fig. 1 illustrates the schematic representation of cyberattacks against the synchronization system of a microgrid. At the point of common coupling (PCC) of the microgrid and the main grid, an ASC monitors the voltage of the microgrid and the main grid and sends control signals to the governor of the synchronizing generator to adjust the frequency of the microgrid to the main grid by means of digital I/O pulses (e.g. ABB SYNCHROTACT [34]) or by interrogated contacts (e.g. SEL A25A [35]). To model the control signals, (+1) and (-1) pulses are considered when commanding the generator to respectively ramp up and down, and (0) is considered in the absence of control command or when communication is lost. The control signals are communicated over the microgrid network to the governor of the synchronizing generator.

Fig. 2 illustrates the signals and measurements which are involved in the synchronization of the microgrid. Voltage transformers are used to obtain local measurements of the voltage of the main-grid ($V_{Grid-side}$) and microgrid ($V_{Microgrid-side}$) at the PCC, and the circuit breaker at the PCC is closed when the voltage profiles are sufficiently close and synchronization criteria are met. The synchronization control signal ω_{cp} is communicated from the PCC local-area network (LAN) to the synchronizing generator LAN over the microgrid network typically using IEC61850 protocol. The synchronizing signal communication is illustrated in Fig. 3.

The objective of the attack is to trip the synchronizing generator by sending falsified synchronization control signals to the generator governor. Fig. 2 illustrates the protective relays of the generator including under-frequency (UF) (ANSI 81U), over-frequency (OF) (81O), and rate-of-change-of-frequency (ROCOF) (81R). To achieve the goal of the attack, the falsified synchronization control signal must trigger at least one of these protective relays.

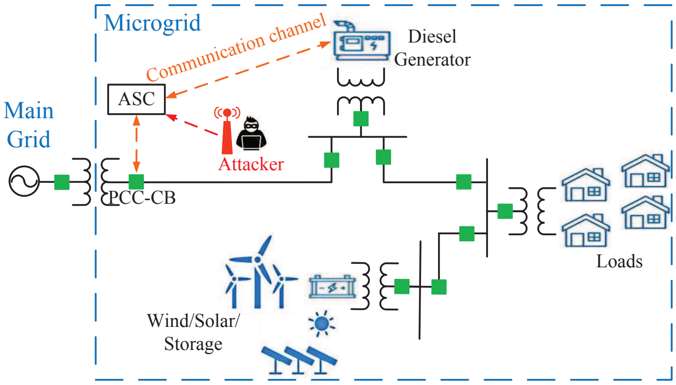

Fig. 1. Schematic representation of cyberattacks against the synchronization system of a microgrid.

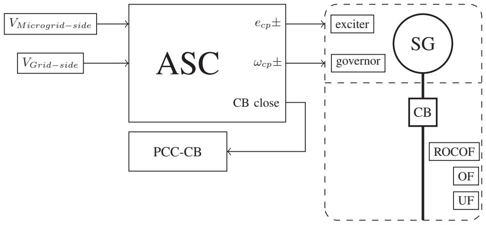

Fig. 2. Automatic synchronization control of a synchronous generator in a microgrid

Two attack models are considered in this paper. The first attack model is based on programmable logic controller rootkit attacks as discussed in [33]. The adaptation of this attack model to our work is illustrated by the dashed red arrows (1) and (2a) in Fig. 3. Arrow (1) represents the attacker gaining remote access to the Human-Machine Interface (HMI) at the PCC LAN. The reprogramming of the ASC via a rootkit attack is represented by arrow (2a). The second attack model takes advantage of the microgid communication network. The route of the synchronizing signal in the microgrid communication network is traced with solid red arrows from the ASC to the synchronizing generator governor in Fig. 3. This attack model exploits the vulnerabilities in the IEC 61850 protocol to capture and modify, or fabricate false signals, as discussed in [36], [37]. This attack is feasible due to lack of communication encryption. This approach is represented by (2b) in Fig. 3. It is worth noting that, in contrast to [33], the attacker does not need to spoof the HMI available to the system operator to hide suspicious activities. This is because the attack models considered in this paper can be executed very fast to prevent any corrective actions by the operator to thwart the attack. We discuss in Section III how knowledge of the resonance frequency of the system can enable the attacker to achieve this goal.

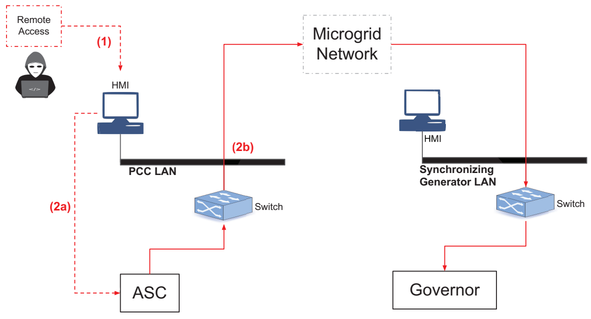

Fig. 3. Attack model diagram

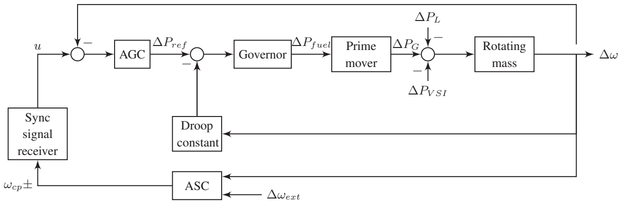

Fig. 4. Synchronous generator block diagram.

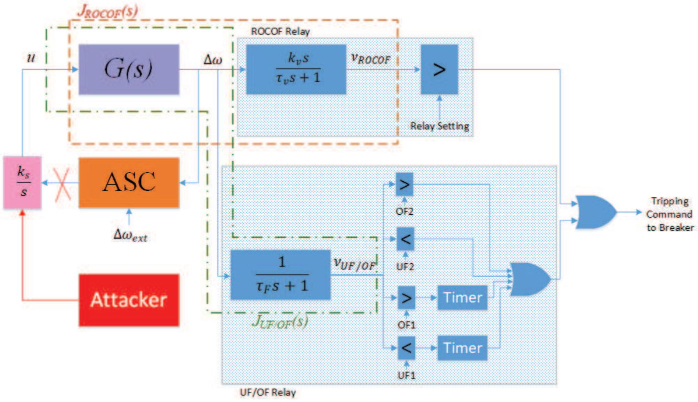

Fig. 5. The block diagram of the transfer functions involved in attacks against synchronization systems.

Tripping the synchronizing generator can have significant impacts as the loss of generation in the microgrid which can result in microgrid blackout. Exploring the potential of cyberattacks on synchronization systems requires a study of synchronous generator control and protection subsystems as detailed in the next section.

III. Analytical Model

This section presents the underlying analytical framework for designing cyberattacks against synchronization systems. We begin by describing the typical control architecture of a synchronous generator. The conditions for the successful implementation of a cyberattack against synchronization systems are subsequently derived and discussed.

A. Modeling of the Synchronization System of a Synchronous Generator

The typical small-signal block diagram of the control system of a synchronous generator is shown in Figure 3 [38]. The synchronous generator is modeled by a rotating mass driven by a combustion engine such as a gas turbine or a reciprocating diesel engine. The combustion engine is controlled by several control loops including speed-droop governor, automatic generation control (AGC) and ASC. The equations governing the dynamics of a synchronous generator are provided in (1)-(3) [38]:

$$\Delta\dot{P}_G = -\frac{1}{\tau_T}\Delta P_G + \frac{k_T}{\tau_T}\Delta P_{fuel} \tag{1}$$

$$\Delta\dot{P}_{fuel} = -\frac{1}{\tau_G}\Delta P_{fuel} + \frac{k_G}{\tau_G}(\Delta P_{ref} - k_d\Delta\omega) \tag{2}$$

$$\Delta\dot{P}_{ref} = k_c(u - \Delta\omega) \tag{3}$$

where Δ denotes deviation from the point of linearization, P_{fuel} represents the fuel intake of the synchronous generator,

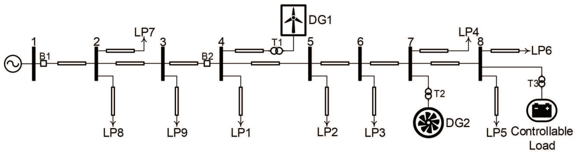

Fig. 6. Microgrid test system with the synchronous generator DG2 in charge of synchronization with the main grid.

P_{ref} denotes the AGC load reference, u is the time integral of the ASC synchronizing signal, ω denotes the system frequency, and τ and k denote the time-constants and gains in different control loops, respectively. Subscripts T and G refer to the prime-mover and governor, respectively.

The frequency at the synchronous generator bus is governed by the well-known swing equation given in (4):

$$\Delta\dot{\omega} = -\frac{D}{M}\Delta\omega + \frac{1}{M}(\Delta P_G - \Delta P_{VSI} - \Delta P_L) \qquad (4)$$

where M and D denote the inertia and load damping constants, P_G represents the output of the synchronous generator, P_{VSI} is the power output of voltage source inverter (VSI) interfaced DERs which provide frequency regulation, and P_L denotes the demand.

The state space representation of Equations (1)-(4) is given in (5):

$$\dot{x}_g = A_g x_g + B_{1g}u + B_{2g}\Delta P_L + B_{3g}\Delta P_{VSI} \qquad (5)$$

where the state vector is

$$x_g = [\Delta P_{ref} \quad \Delta P_{fuel} \quad \Delta P_G \quad \Delta\omega]^T$$

A_g represents the state matrix, and B_{1g}, B_{2g} and B_{3g} denote input matrices. The matrices are defined in the Appendix.

To investigate the possibility of tripping a synchronous generator using the synchronization signal, we model synchronous generator control and protection subsystems. The transfer function $G(s)$ relating the input signal u in Fig. 5 to the output signal $\Delta\omega$ can be derived from (5) as given in (6):

$$G(s) = \frac{\Delta\omega}{u} = [0 \quad 0 \quad 0 \quad 1]\,(sI - A_g)^{-1}B_{1g} \qquad (6)$$

Fig. 5 illustrates the subsystems relevant to the study of cyberattacks against the synchronization system. As illustrated in Fig. 5, the falsified synchronization signal passes through an integrator block which transforms it into signal u before entering the block with transfer function $G(s)$. In Fig. 5, the frequency deviation is denoted by $\Delta\omega$, the measured frequency deviation is denoted by $\nu_{_{UF/OF}}$, and the measured rate of change of frequency is denoted by $\nu_{_{ROCOF}}$. The under-frequency/over-frequency and ROCOF relays respectively are denoted by the subscripts UF/OF and ROCOF. The objective of the attacker is to trigger one of the ROCOF or under-frequency/over-frequency relays to trip the generator. To achieve this objective, the signal u has to be manipulated such that one of the relay measurements exceeds its corresponding relay setting.

B. Frequency Analysis of the Synchronization System

Considering the transfer functions of the under-frequency/over-frequency and ROCOF protective relays in combination with the transfer function $G(s)$, we respectively obtain the transfer functions $J_{_{UF/OF}}(s)$ and $J_{_{ROCOF}}(s)$ as illustrated in Fig. 5. These transfer functions relate the signal u directly to the frequency relay measurements. We restate that the objective of the attacker is to manipulate the signal u to trip the synchronous generator, and that the tripping is dictated by the frequency relays based on the relay measurements.

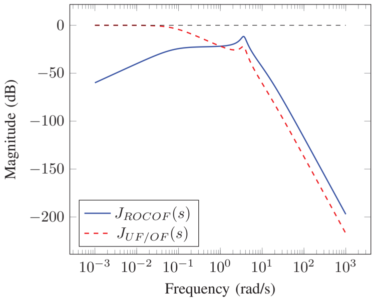

Fig. 7. Bode magnitude plots of the transfer functions $J_{_{ROCOF}}(s)$ and $J_{_{UF/OF}}(s)$.

For demonstration purposes, we consider the data of the synchronous generator DG2 in the microgrid test system shown in Fig. 6. The test system data is provided in the Appendix.

We begin by examining the characteristics of $J_{_{ROCOF}}(s)$ and $J_{_{UF/OF}}(s)$ for the synchronous generator DG2 which are shown in Fig. 7. The transfer function $J_{_{UF/OF}}(s)$, represented by the dashed red curve in Fig. 7, exhibits a low pass behavior with a low crossover frequency which is in accordance with synchronous generators typically showing a slow dynamic response behaviour. Therefore, any attack targeting the under-frequency/over-frequency relay will require a long attack duration and, hence, can be easily detected and mitigated.

In contrast, the transfer function $J_{_{ROCOF}}(s)$, represented by the blue solid curve in Fig. 7, exhibits a band-pass behavior. A periodic signal u with a frequency inside this band-pass can be used to trigger the ROCOF relay. The band-pass, as shown in Fig. 7, is at a relatively high frequency range in comparison with the $J_{_{UF/OF}}(s)$ case, which enables the periodic attack to be designed with higher frequencies and for the attacks to be executed faster.

Another important observation in Fig. 7 is the resonance frequency which occurs at $\omega = 3.60$ rad/s. As synchronous generators are more vulnerable to high oscillations at their resonance frequencies, information about the resonance frequency can be used by a cyberattacker to design a fast attack. The implications of this will be investigated further in the next subsection.

C. Conditions for Successful Attacks

Now, we explore the characteristics of the synchronizing signal to derive the conditions for a successful cyberattack. Industrial ASC devices offer a range of options to tailor the synchronization process to the requirements of generation plants. These options include the ability to choose between a fixed or proportional frequency mode to specify the width of each correction pulse, and the pulse interval defining the time between the rising edges of consecutive correction pulses in the synchronizing signal [34], [35]. The synchronizing signal consists of a stream of (+1) and (-1) pulses. Therefore, the attacker should devise a similar pattern to make the attack signal unrecognizable from the synchronizing signal by operators.

We posit that it is possible to ignore the harmonic frequencies of the periodic attack signal considering the small bandwidths of $J_{ROCOF}(s)$ and $J_{UF/OF}(s)$. Therefore, the attack signal u_{attack} can be approximated with a pure sinusoidal signal with a fundamental frequency ω_{attack} while deriving the conditions for a successful attack without loss of generality. As such, the signals ν_{ROCOF} and $\nu_{UF/OF}$ in Fig. 5 are also considered to be sinusoidal. The peak values of the signals ν_{ROCOF} and $\nu_{UF/OF}$ can be calculated as given in (7)-(8) for the attack signal u_{attack}:

$$\nu^{pk}_{ROCOF} = |J_{ROCOF}(\omega_{attack})| u^{pk}_{attack} \tag{7}$$

$$\nu^{pk}_{UF/OF} = \left|J_{UF/OF}(\omega_{attack})\right| u^{pk}_{attack} \tag{8}$$

where the magnitude of the transfer function $J(s)$ at the attack frequency ω_{attack} is denoted by $|J_{ROCOF}(\omega_{attack})|$ and $\left|J_{UF/OF}(\omega_{attack})\right|$ respectively for ROCOF and under-frequency/over-frequency relays.

The peak value of at least one of the measurements ν_{ROCOF} and $\nu_{UF,OF}$ should violate the setting of the corresponding protective relay for the attack to be successful. This means that either the peak value of ν_{ROCOF} should exceed the ROCOF relay setting, R, *i.e.,* $\nu^{pk}_{ROCOF} \geq R$ or the peak value of $\nu_{UF/OF}$ should exceed one of the under-frequency/over-frequency relay settings, $\min\{UF, OF\}$, *i.e.,* $\nu^{pk}_{UF/OF} \geq \min\{UF, OF\}$. Thus, the conditions for successful attacks can be derived from (7)-(8) as given in (9)-(10).

$$u^{pk}_{attack} \geq u^{pk,R}_{attack}(\omega_{attack}) = \frac{R}{|J_{ROCOF}(\omega_{attack})|} \tag{9}$$

$$u^{pk}_{attack} \geq u^{pk,F}_{attack}(\omega_{attack}) = \frac{\min\{UF, OF\}}{\left|J_{UF/OF}(\omega_{attack})\right|} \tag{10}$$

It is worth noting that the required peak values of the signal u_{attack} for triggering the ROCOF and under-frequency/over-frequency protective relays are dictated by the characteristics of the synchronous generator ($J_{ROCOF}(\omega_{attack})$, $J_{UF/OF}(\omega_{attack})$) and the settings of the protective relays (R, UF, OF) as indicated by (9)-(10). Moreover, the minimum value of $u^{pk,R}_{attack}$ which corresponds to the maximum value of $|J_{ROCOF}(\omega_{attack})|$ occurs at the resonance frequency. This underscores the importance of the resonance frequency while devising an attack against the synchronization system of a synchronous generator.

The ROCOF and under-frequency/over-frequency protective relays can be triggered through the synchronizing signal only if the peak value of the signal u_{attack} can satisfy the conditions in (9)-(10). Thus, we need to investigate the maximum realizable peak value of the signal u_{attack} in order to determine the feasibility of implementing a successful attack. As discussed previously, ASC control signal consists of a stream of (+1) and (-1) pulses. The maximum peak value of the fundamental component of the signal u occurs when the synchronizing signal is a square wave with only (+1) and (-1) amplitudes. The integrator k_s/s in Fig. 5 transforms the square wave signal with only (+1) and (-1) amplitudes to a triangular signal. The Fourier series of this triangular signal is given in (11):

$$u(t) = \frac{4k_s}{\pi\omega_{attack}} \sum_{n=1}^{\infty} \frac{(-1)^{(n-1)/2}}{n^2} \sin(\omega_{attack} n t) \tag{11}$$

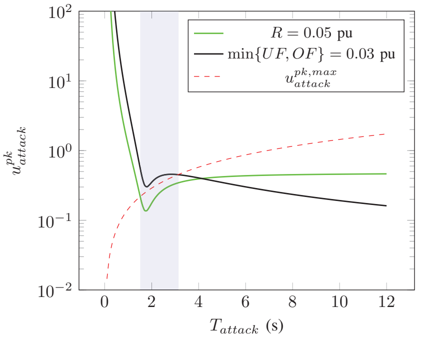

Fig. 8. The conditions on the required peak value of u^{pk}_{attack} for the successful implementation of an attack using falsified synchronizing signals.

The maximum peak value of u_{attack}, $u^{pk,max}_{attack} = 4k_s/\pi\omega_{attack}$ as indicated in (11), is a function of the integrator gain k_s and the frequency of the attack signal ω_{attack}. As such, the only parameter that can be controlled by the attacker in (9)-(11) to implement a successful attack is the frequency or time period, *i.e.,* $T_{attack} = 2\pi/\omega_{attack}$, of the falsified synchronizing signal. This is again because the other parameters, *i.e.,* $J_{ROCOF}(\omega_{attack})$, $J_{UF/OF}(\omega_{attack})$, R, UF, OF and k_s, are dictated by the characteristics of the synchronous generator and the settings of the protective relays.

The ultimate conditions for implementing a successful attack against the synchronization system are given in (12)-(13). The conditions indicate that the attack is feasible only when the maximum achievable peak value of the signal u_{attack} is larger than one of the minimum values required to trigger a frequency protective relay of the synchronous generator.

$$u^{pk,R}_{attack}(\omega_{attack}) \leq u^{pk,max}_{attack}(\omega_{attack}) \quad \text{OR} \tag{12}$$

$$u^{pk,F}_{attack}(\omega_{attack}) \leq u^{pk,max}_{attack}(\omega_{attack}) \tag{13}$$

The data of the synchronous generator DG2 is used again here to demonstrate the attack conditions. The required peak value of the signal u^{pk}_{attack} for triggering the ROCOF and under-frequency/over-frequency protective relays of the synchronous generator DG2 are illustrated in Fig. 8 as functions of T_{attack}, *i.e.,* the time period of the signal u^{pk}_{attack}. The required peak value of the signal u^{pk}_{attack} for triggering the ROCOF relay with a setting of $R = 0.05$ pu is illustrated by the curve in green. The required peak value of the signal u^{pk}_{attack} for triggering the under-frequency/over-frequency protective relay with a setting of $\min\{UF, OF\} = 0.03$ pu is illustrated by the curve in black. The relay settings are adopted from IEEE Std. 1547 [39] and provided in the Appendix. The green and black curves move up (down) as the corresponding relay setting is set to larger (smaller) values.

The curve in red in Fig. 8 shows the maximum achievable peak value of the signal u_{attack} as a function of T_{attack}.

In Fig. 8, the minimum value of $u^{pk,R}_{attack}$ occurs at T_{attack} approximately equal to 1.73 seconds. This time period corresponds to the resonance frequency of the synchronous generator which is equal to 3.6 rad/s.

As illustrated in Fig. 8, the attacker can successfully trigger the protective relays of a synchronous generator by manipulating the time period of the falsified synchronizing signal to the governor. The protective relay is triggered by the falsified synchronizing signal when the red curve is above the curve associated with the protective relay. For instance, the ROCOF relay with the setting of 0.05 pu can be triggered by the falsified synchronizing signals with time periods larger than 1.52 seconds. Moreover, the under-frequency/over-frequency relay can be triggered by falsified synchronizing signals with time periods larger than 3.15 seconds. Falsified synchronizing signals with time periods larger than 3.15 seconds may trigger both relays. Yet, the ROCOF relay still may be triggered first considering the slow behavior of $J_{_{UF/OF}}(s)$ for the under-frequency/over-frequency relay. Fig. 8 illustrates the vulnerability of the synchronization systems of the synchronous generator DG2 as well as the conditions for implementing a successful attack which is one of the main objectives of the present paper.

The observations in Fig. 8 are consistent with the observations in Fig. 7. As illustrated in Fig. 8 the under-frequency/over-frequency relay can be triggered by falsified synchronizing signals with time periods larger than 3.15 seconds. This range verifies the low-pass behavior of the under-frequency/over-frequency relay. Similarly, Fig. 8 verifies the band-pass behavior of the ROCOF relay considering that the falsified synchronizing signals with time periods less than 1.52 seconds would not trigger the ROCOF relay.

The remaining question to be answered is the accessibility of the required information for devising a successful attack to the attacker. The settings of the generator protective relays can be gathered from various standards and manufacturer manuals. The data about the generator transfer function $G(s)$ can be estimated using the approach presented in [40] by eavesdropping the system frequency $\Delta\omega$ during the system disturbances or by active probing. The attacker can also obtain information about the resonance frequency of the synchronous generator by passively monitoring the frequency response of the system during disturbances.

It is worth noting that the attacker does not necessarily need the aforementioned information to implement a successful attack. This is because, the attack success can be guaranteed by increasing the time period of the falsified synchronizing signal. Referring back to Fig. 8, this strategy can be visually explained by tracing the red curve representing $u_{_{attack}}^{pk,max}$ towards longer time periods where the curve ascends above the green or black curves; at which point, the frequency protective relays can be triggered.

D. Modeling of the Synchronization System of a Microgrid

The proposed analytical model for the synchronization system of a synchronous generator is extended here to microgrids. Inverter-interfaced DERs like storage, wind and solar do not commonly contribute to frequency regulation in traditional microgrids. The modeling of the synchronization system in microgrids in which inverter-interfaced DERs do not contribute to frequency regulation is similar to the modeling presented previously for a synchronous generator. Yet, there have been several initiatives in academia and industry in recent years to realize frequency regulation using inverter-interfaced DERs in microgrids. As such, we examine the impact of these resources on the attacks against the synchronization system of a microgrid.

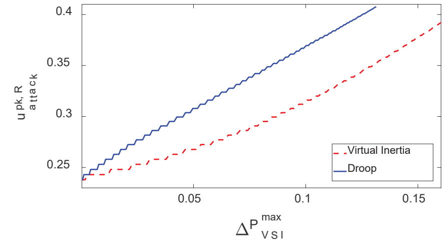

Fig. 9. The conditions on the required peak value of $u_{_{attack}}^{pk}$ for the successful implementation of an attack considering the contribution of the inverter-interfaced DERs.

The transfer function of an inverter-interfaced distributed energy resource in droop control and virtual inertia mode are given in (14)-(15), respectively:

$$\Delta P_{VSI(dr)} = \frac{K_{dr}}{\tau_v s + 1}\Delta\omega \tag{14}$$

$$\Delta P_{VSI(\nu i)} = \frac{K_{\nu i} s}{\tau_v s + 1}\Delta\omega \tag{15}$$

The microgrid test system in Fig. 6 is employed for the demonstration purposes. The required peak value of the signal $u_{_{attack}}^{pk}$ for triggering the ROCOF protective relay of the synchronous generator DG2 is illustrated in Fig. 9 as a function of the maximum power output of inverter-interfaced DERs, ΔP_{VSI}^{max}. The setting of the ROCOF protective relay R and the time period of the attack signal $T_{_{attack}}$ are respectively considered to be 0.05 pu and 2 seconds.

As illustrated in Fig. 9, the increase in ΔP_{VSI}^{max} due to the contribution of inverter-interfaced DERs increases the required $u_{_{attack}}^{pk}$ to trigger the ROCOF protective relay. The same trend exists for the under-frequency/over-frequency relay in the presence of droop control and virtual inertia from inverter-interfaced DERs. This indicates that it is more difficult to implement a successful attack against synchronization systems when interconnecting two systems with high inertia and frequency regulating mechanisms compared to interconnecting a weak grid with low inertia and weak frequency regulating mechanism like a microgrid to the main grid.

E. Sensitivity Analyses

Sensitivity analyses are performed in this section to show that the attacks are applicable to systems with a wide range of control system parameters. Specifically, we demonstrate the impact of varying the parameters in the transfer function $J_{_{ROCOF}}(s)$ such as AGC and droop gains on the required peak value of the signal $u_{_{attack}}$ to trigger the ROCOF protective relay. Moreover, the impact of the AGC and droop gains on the performance of the control loops of the synchronous generator is discussed.

Fig. 10 illustrates the impact of varying the AGC gain k_c on the required peak value of the signal $u_{_{attack}}$ to trigger the

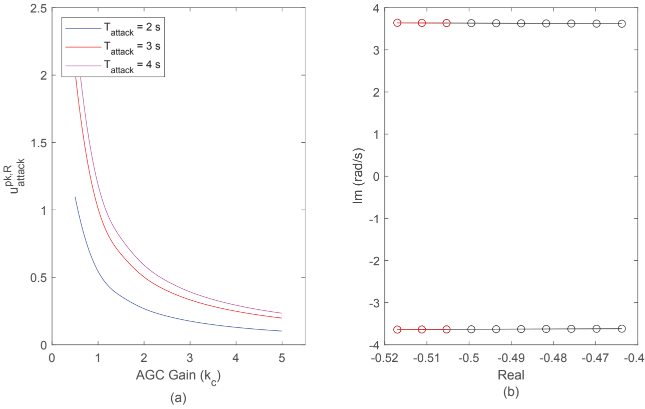

Fig. 10. Sensitivity analysis; (a) $u^{pk,R}_{attack}$ versus the AGC gain k_c, (b) Loci of the eigenvalues of the mechanical mode when k_c is changed from 0.5 to 5 with steps of 0.5. The increase is to the right.

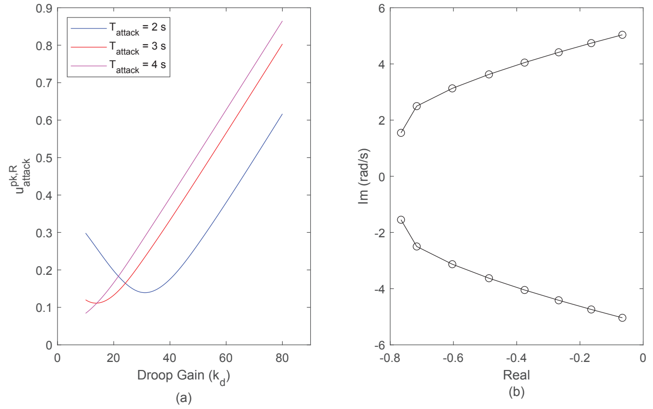

Fig. 11. Sensitivity analysis; (a) $u^{pk,R}_{attack}$ versus the droop gain k_d, (b) Loci of the eigenvalues of the mechanical mode when k_d is changed from 10 to 80 with steps of 10. The increase is to the right.

ROCOF relay and the performance of AGC. It can be observed in Fig. 10 (a) that decreasing the AGC gain increases the required peak value $u^{pk,R}_{attack}$. Fig. 10 (b) illustrates the impact of varying the AGC gain from 0.5 to 5 on the location of the dominant mechanical eigenmode of the system transfer function $G(s)$. The red points in Fig. 10 (b) show the low values of the AGC gain for which the attack is infeasible. Although small values of the AGC gain increase the required peak value $u^{pk,R}_{attack}$, these values are impractical as they also diminish the performance of AGC.

Fig. 11 illustrates the impact of varying the droop gain k_d on the required peak value of the signal u_{attack} to trigger the ROCOF relay and the performance of frequency-droop control. It can be observed in Fig. 11 (a) that increasing the droop gain increases the required peak value $u^{pk,R}_{attack}$. Although the large values of the droop gain k_d increase the required peak value $u^{pk,R}_{attack}$ to trigger the ROCOF relay, these values also decrease the internal stability of the system. This is illustrated by Fig. 11 (b) which shows the impact of varying the droop gain from 10 to 80 on the location of the dominant mechanical eigenmode of the system transfer function $G(s)$. Increasing the droop gain would eventually destabilize the system by moving the poles of $G(s)$ outside the stable left-half plane.

Thus, the attacks are applicable to systems with the considered values of AGC and droop gain, and when not, the gain values themselves are impractical for the system.

A similar sensitivity analysis as the one presented here can be performed to demonstrate the impact of the parameters in the transfer function $J_{UF/OF}(s)$ on the required peak value of the signal u to trigger the under-frequency/over-frequency relay; the results of this sensitivity analysis are not provided for the sake of brevity.

IV. Mitigation Strategy

Cyber and physical solutions can be used to mitigate the cyberattacks against synchronization systems. Cyber solutions either rely on the protection of cyber assets from intrusion or rely on encryption of data. This is while physical solutions entail physical modifications of the system. The deficiency of the cyber solutions is that skilled attackers with sufficient resources may still compromise the security measures. Here, we propose two physical mitigation strategies as the last line of defense against cyberattacks targeting synchronization systems. The first mitigation strategy is based on an anomaly detection system. The second mitigation strategy is based on incorporating a limiter block in the governor control logic of the synchronizing generator. We also verify that the mitigation strategies do not interfere with the normal synchronization process.

A. Anomaly Detection Based Mitigation Strategy

The generator frequency during a successful cyberattack has to change faster than during normal synchronization to prevent attack detection by operators. Hence, we propose an anomaly detection based mitigation strategy capable of detecting attacks by monitoring the rate-of-change of frequency of the system. The following equation can be used to identify anomalies and disable synchronization while alarming the operators.

$$1\left(\nu > \Lambda_A\right) \tag{16}$$

where $1(\cdot)$ is a function equal to 1 when the condition inside the brackets is true, indicating the presence of an anomaly, and 0 otherwise. ν indicates the rate-of-change of frequency which can be obtained by simple processing of the voltage measurements. The threshold Λ_A can be derived via theoretical analysis of the small-signal model presented in Section III or statistical analysis of system historical data.
Here, we use small-signal model to derive Λ_A. Let Γ denote the width of a normal synchronizing signal correction pulse. If the ASC is set to fixed frequency mode then the value of Γ will be fixed as discussed in Section III-C. If the ASC is in proportional frequency mode, then we will set Γ equal to the maximum pulse width. This pulse enters the integrator block k_s/s in Fig. 5 resulting in signal $u(t)$. The signal $u(t)$ increases or decreases linearly with time until it has seen a change of Γk_s. The governor control will react to adjust the frequency of the generator according to the signal $u(t)$. Λ_A can be computed as the maximum rate-of-change of frequency during a normal synchronization process. The mitigation strategy resets the integrator block output and disables the synchronization process when the measured rate-of-change of frequency is higher than Λ_A.

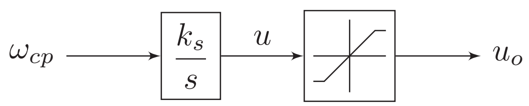

Fig. 12. Block diagram of the proposed mitigation strategy.

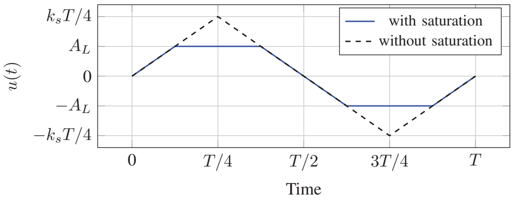

Fig. 13. The signal $u(t)$ with the maximum achievable peak value before and after using the limiter block.

Using the ROCOF relay measurement for ν, the above explanation can be condensed into the following equation to compute Λ_A.

$$\Lambda_A \geq \max_t \mathcal{L}^{-1}\left(\frac{k_s}{s^2}\left(1-e^{-\Gamma s}\right) J_{ROCOF}(s)\right)(t) \tag{17}$$

where $\mathcal{L}^{-1}$ is the inverse Laplace transform, and $J_{ROCOF}(s)$ is as introduced in Section III. B.

For example, the value of Λ_A for the testbed under study for a maximum pulse width of 10 milliseconds must be greater than or equal to 2.5×10^{-3} pu.

When an anomaly is detected, an alarm is sent to alert the operator. Moreover, a local signal is sent to the governor to disable the synchronization process temporarily until the rate-of-change of frequency of the system settles back to the normal range.

It is worth noting that the mitigation strategy relies on local measurements from voltage transformers to calculate the rate-of-change of frequency. Therefore, it is more difficult to compromise it by cyber intrusions.

B. Limiter Block Based Mitigation Strategy

As discussed in Section III. C, the successful implementation of attacks against synchronization systems depends on the maximum achievable peak value of the signal u_{attack}. Therefore, the conditions for preventing successful attacks against synchronization systems can be derived from (12)-(13) as given in (18)-(19):

$$u_{attack}^{pk,max}(\omega_{attack}) < u_{attack}^{pk,R}(\omega_{attack}) \quad \text{AND} \tag{18}$$

$$u_{attack}^{pk,max}(\omega_{attack}) < u_{attack}^{pk,F}(\omega_{attack}) \tag{19}$$

Hence, we propose to add a limiter block in the synchronization control loop after the integrator block k_s/s as illustrated in Fig. 12 in order to satisfy the conditions in (18)-(19). The triangular signal u is considered again here because it results in the maximum achievable peak value for the signal u as discussed in Section III. C. The conditions (18)-(19) transform the triangular signal u to a trapezoidal signal as illustrated in Fig. 13. The peak value of the fundamental component of the trapezoidal waveform is given in (20). This peak value is obtained from the Fourier series of trapezoidal waveform:

$$\frac{4}{\pi\omega}\sin(A_L\omega_{attack}/k_s). \tag{20}$$

The saturation value of the limiter to prevent attacks denoted by A_L in (20) can be computed using conditions (21)-(22):

$$\frac{4}{\pi\omega}\sin(A_L\omega_{attack}/k_s) < u_{attack}^{pk,R} \tag{21}$$

$$\frac{4}{\pi\omega}\sin(A_L\omega_{attack}/k_s) < u_{attack}^{pk,F} \tag{22}$$

As discussed in Section III. C, minimum values of $u_{attack}^{pk,R}$ and $u_{attack}^{pk,F}$ occur at the resonance frequency. Thus, the ultimate saturation value of the limiter can be obtained from (21)-(22) as given in (23):

$$A_L < \frac{k_s}{\omega_r}\arcsin\left(\frac{u^{pk,min}\pi\omega_r}{4}\right) \tag{23}$$

where ω_r denotes the resonance frequency, and $u^{pk,min}$ represents the minimum value of $u_{attack}^{pk,R}(\omega_r)$ and $u_{attack}^{pk,F}(\omega_r)$.

Limiting the signal $u(t)$ below the saturation value A_L prevents the success of periodic FDI attacks irrespective of the pattern of the attack. This mitigation strategy can be easily extended to other non-periodic FDI attacks such as saturated ramp and ramp attacks. In saturated ramp and ramp attacks, the attacker falsifies the synchronization control signal in order to shape the signal $u(t)$ as saturated ramp and unlimited ramp signals, respectively. To mitigate these attacks, the saturation value of the limiter, i.e., Λ_B, must be smaller than the minimum value of A_L, as well as the under-frequency/over-frequency relay settings as given in the following.

$$\Lambda_B < \min\{A_L, UF, OF\} \tag{24}$$

This mitigation strategy can be implemented via a small logic modification in the governor control IED. The proposed mitigation strategy does not have any impact on other control loops of a synchronous generator since it only modifies the synchronization control loop.

C. Impact on Normal Synchronization

We demonstrate that the proposed mitigation strategies do not have a tangible impact on the synchronization process in the absence of cyberattacks. It is assumed that the microgrid test system in Fig. 6 starts the synchronization process at $t = 2$ seconds when the frequency difference between the microgrid and the main grid is 0.6 Hz. In the testbed under study, A_L is equal to 0.15. Considering under-frequency and over-frequency relay settings of 0.058 pu and 0.033 pu, respectively, we implement a limiter block saturation value of 0.025 pu which satisfies equation (24). For the anomaly detection based mitigation strategy, we implement a threshold value equal to 3×10^{-3} pu which satisfies equation (17).

Fig. 14 illustrates the synchronization process for the cases with and without the mitigation in the absence of cyberattacks. The curves associated with the cases with and without the limiter block mitigation strategy are respectively shown in red and blue. The acceptable ranges of the frequency and phase angle for closing the PCC circuit breaker are shown by black dashed lines in Fig. 14 (b) and (c), respectively.

As illustrated in Fig. 14 (d), the rate-of-change of frequency does not exceed the anomaly detection threshold shown by red

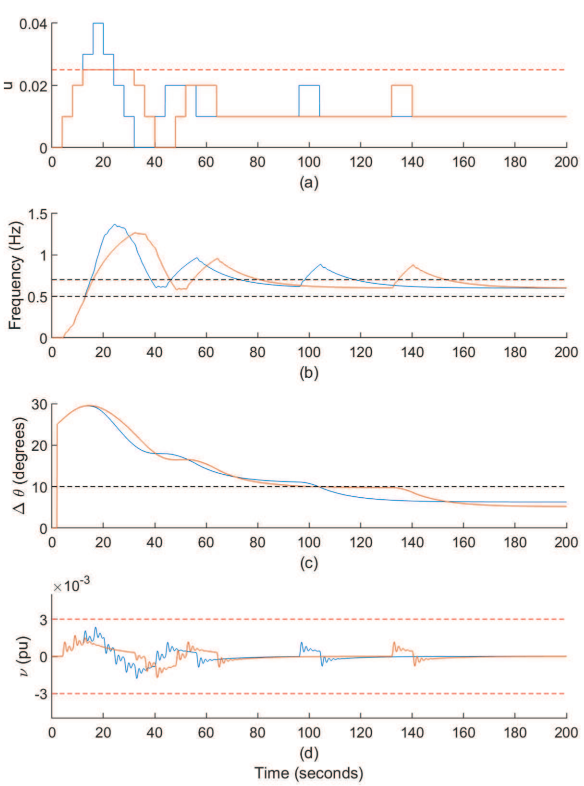

Fig. 14. Microgrid synchronization with (red) and without (blue) the proposed limiter block mitigation strategies in the absence of cyberattacks. (a) shows the signal u. (b) shows the microgrid frequency relative to the frequency of the main grid. (c) shows the microgrid phase angle relative to the phase angle of the main grid, (d) shows the microgrid rate-of-change of frequency.

dashed lines. This verifies that the mitigation strategy does not intervene with the normal synchronization process.

As for the limiter block strategy, the saturation value is shown by a red dashed line in Fig. 14 (a). The signal u cannot exceed this limit for the case with the limiter block mitigation strategy. The case without the mitigation strategy arrives at the acceptable range for closing the PCC circuit breaker in approximately 124 seconds. This is while it approximately takes 159 seconds for the case with the mitigation strategy to arrive at the acceptable range for closing the PCC circuit breaker. It can be observed that the results of both cases are satisfactory. Therefore, we conclude that microgrids would not bear tangible dynamic or economic consequences due to this short time delay.

It is noteworthy that both mitigation strategies do not impact generation frequency control, do not require intensive computation and do not rely on a cyber system offering a physical layer of security to improve the cyber-physical resilience of synchronization systems.

V. Real-time Simulation Results

The OPAL-RT real-time simulator is employed to test and verify the findings of the paper using the detailed model of the microgrid test system in Fig. 6. The microgrid test system in Fig. 6 replicates an existing medium-voltage rural distribution system in Ontario, Canada. Two distributed generators (DG) are connected to the microgrid. DG1 is a variable speed wind generator which is connected to the microgrid through a 2.5 MVA full-scale converter. DG2 is a 2.5 MVA synchronous generator which is in charge of synchronization process during the transition form islanded mode of operation to the grid connection mode of operation. An energy storage system with a 125 kWh capacity is further connected to the microgrid at bus 8 which is represented as a controllable load. Naming conventions are used such that B, T and LP respectively represent circuit breakers, transformers and loads in Fig. 6. The microgrid test system data are provided in the Appendix.

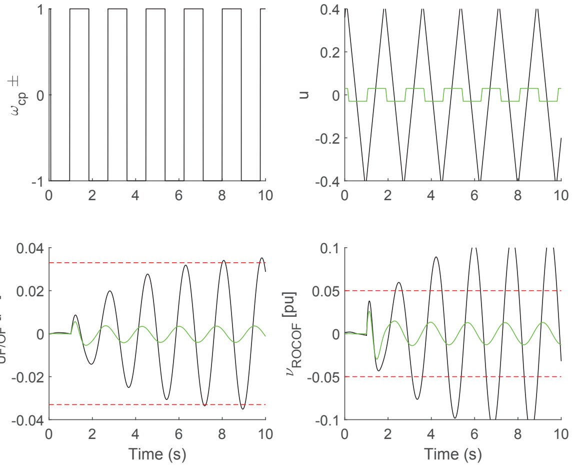

Fig. 15. Simulation results using OPAL-RT: An attack with the time period of the system resonance and a stream of (+1) and (-1) pulses.

The settings of the ROCOF and under-frequency/over-frequency relays respectively are considered to be equal to 0.05 pu and 0.033 pu in the studies, and are illustrated by horizontal dashed lines in Figs. 15–21. The ROCOF relay trips the synchronous generator once the measurement exceeds the relay setting. Yet, signals are shown after exceeding the setting of the protective relay for demonstration purposes. The signals $\omega_{cp}\pm$, u_{attack}, ν_{ROCOF} and $\nu_{UF,OF}$ are demonstrated in green and black in the case study figures respectively for the cases with and without implementing the mitigation strategy. We first validate the limiter block based mitigation strategy where the saturation value of the limiter block is set to 0.03. Afterwards, we validate the anomaly detection based strategy.

A. Limiter Block Based Mitigation Strategy

1) Case Study A1: The objective of the first case study is to demonstrate how fast the ROCOF protective relay of the synchronous generator in the microgrid test system can be triggered by attacks against the synchronization system. A fast attack prevents any corrective action by the operator to thwart the attack. As such, the time period of the falsified synchronizing signal is considered to be equal to the time period of the resonance frequency. Afterwards, the proposed mitigation strategy is employed to demonstrate its capability in preventing the attack. As illustrated in Fig. 15, the ROCOF relay is triggered just after 2 seconds in this study in the absence of the proposed mitigation strategy.

Yet, this attack results in large fluctuations in the frequency of the microgrid which is conveniently detectable by the microgrid operators.

2) Case Study A2: The objective of this case study is to reduce the microgrid frequency fluctuations observed in Case Study A1 to make the attack undetectable by operators

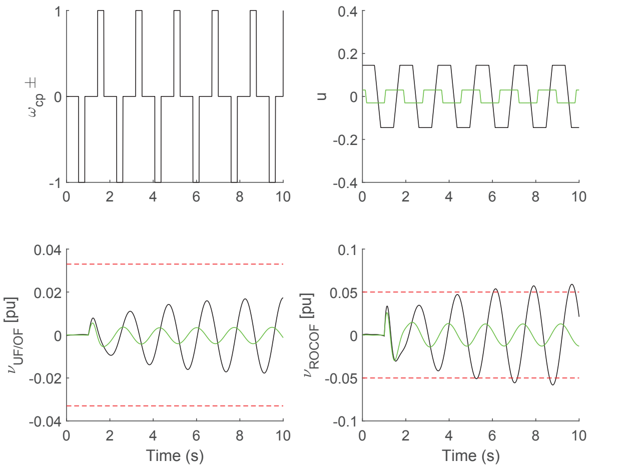

Fig. 16. Simulation results using OPAL-RT: An attack with the time period of the system resonance and a stream of (+1) and (-1) pulses with reduced duty cycle.

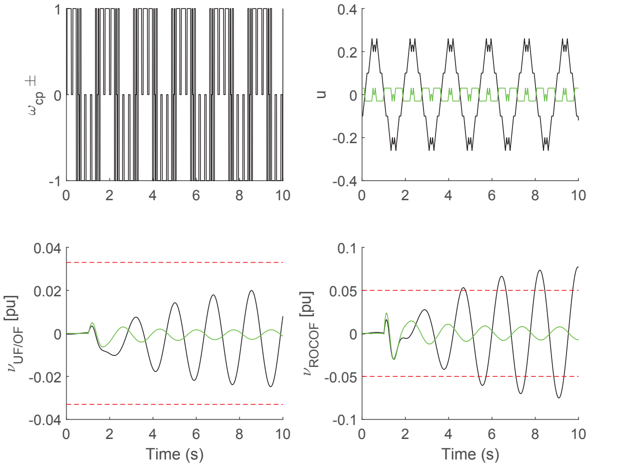

Fig. 17. Simulation results using OPAL-RT: An attack with time period of the system resonance and a complex pattern.

monitoring microgrid frequency. To achieve this objective, the duty cycle of (+1) and (-1) pulses is reduced. This results in reduced microgrid frequency fluctuations at the expense of longer time for triggering the ROCOF relay. The ROCOF relay is triggered in less than 8 seconds in this study in the absence of the mitigation strategy as illustrated in Fig. 16.

3) Case Study A3: The objective of this study is to demonstrate that more complex attack patterns can also be exploited to trigger the ROCOF relay. The time period of the falsified synchronization signal is considered to correspond to the resonance frequency. The falsified synchronization signal is designed to satisfy the attack success conditions in (9)-(10). Consequently, the ROCOF relay is triggered just after 3 seconds in this study in the absence of the mitigation strategy. Note that the fastest relay triggering time observed in Case Study A1 has increased by 150% in this case study. It confirms the analyses in the previous sections that triangular waveforms, despite their simplicity, can trigger the relays much faster compared to other attacks. The simulation results are shown in Fig. 17.

4) Case Study A4: The objective of this study is to demonstrate that it is possible to trigger the ROCOF relay by using the falsified synchronizing signal with time periods different from the time period of the resonance frequency. Moreover, this study verifies that an attacker does not need to have exact knowledge of the system to implement a successful attack. The time period of the falsified synchronizing signal in this study is selected to be different from the time period of the resonance frequency. The time period of the falsified synchronizing signal in this study is considered to be 1.52 seconds which results in $u^{pk,max}_{attack} = u^{pk,R}_{attack}$. The ROCOF relay is triggered in less than 5 seconds in this study in the absence of the mitigation strategy as illustrated in Fig. 18.

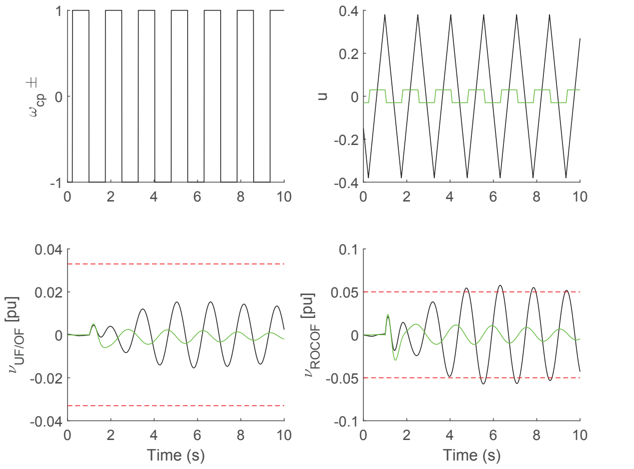

Fig. 18. Simulation results using OPAL-RT: An attack with a time period different from the time period of the system resonance.

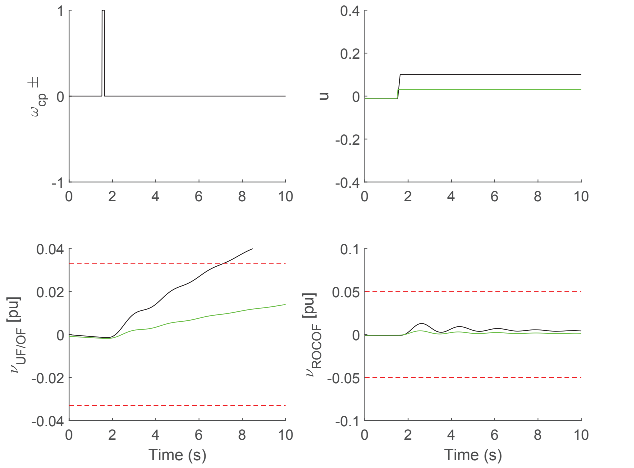

Fig. 19. Simulation results using OPAL-RT: Saturated ramp attack.

5) Case Study A5: The objective of this study is to demonstrate that the mitigation strategy based on the limiter block is capable of preventing non-periodic FDI attacks. In Fig. 19, we consider a saturated ramp attack. In this attack, the attacker's aim is to inject a falsified synchronization signal to raise the frequency of the generator beyond the relay setting of the over-frequency relay. Fig. 19 shows that this attack is able to trip the generator in approximately 6 seconds in the absence of the proposed mitigation strategy. The mitigation strategy successfully prevents the frequency from exceeding the over-frequency relay setting. Unlike the periodic attacks, the rate-of-change of frequency deviation is small and cannot trigger the ROCOF relay. The attack also takes a relatively longer time to trip a generator as compared to the periodic attack in Case Study A1.

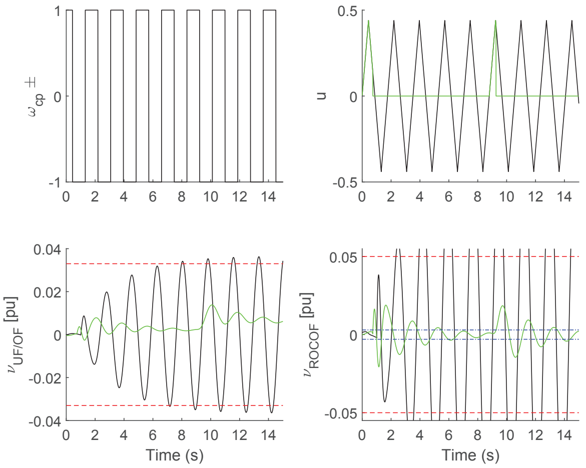

Fig. 20. Simulation results using OPAL-RT: Periodic attack with the anomaly detection based mitigation strategy.

B. Anomaly Detection Based Mitigation Strategy

The threshold value for the anomaly detection mitigation strategy is set to be equal to 3×10^{-3} pu. This threshold is shown with horizontal dashed blue lines in Figs. 20–21. When $\nu_{_{ROCOF}}$ exceeds this threshold, an anomaly is detected and a local signal is sent to the governor to disable the synchronization process temporarily until the rate-of-change of frequency of the system settles back to the normal range. For the system under study, the synchronization is re-enabled when $\nu_{_{ROCOF}}$ has stayed below the threshold for 3 seconds.

1) Case Study B1: In this case study, we reconsider the attack in Case Study A1 which has the shortest success time. Fig. 20 shows that the mitigation strategy disables the synchronizing signal in less than 1 second after the attack starts. Synchronization is re-enabled approximately after 8 seconds but promptly disabled again due to the detection of anomaly. Similar results are observed in the other periodic attack patterns. The simulation results obtained for the other periodic attacks are not provided here for the sake of brevity.

2) Case Study B2: In this case study, we consider a ramp attack to demonstrate that the anomaly detection mitigation strategy is capable of preventing non-periodic FDI attacks. Fig. 21 shows that the ramp attack is able to trip the generator in less than 6 seconds in the absence of the mitigation strategy. Yet, the mitigation strategy successfully prevents the attack.

The simulation results in Case Study A1-A5 and B1-B2 demonstrate that the proposed mitigation strategies successfully prevent all presented FDI attacks. This is evidenced by the measurements shown in green not exceeding their corresponding relay settings in Figs. 15–21.

VI. Conclusion

This paper presented an analytical framework for deriving conditions for the successful implementation of FDI cyberattacks against the synchronization systems of synchronous generators in microgrids. We show that an attacker can implement a fast successful attack by manipulating the time period of the synchronizing control signal to the governor of a synchronous generator. Moreover, we demonstrate that the time period associated with the resonance frequency of the targeted system results in the fastest attack. Yet, the attacker does not need to have exact knowledge of the resonance frequency to implement a successful attack.

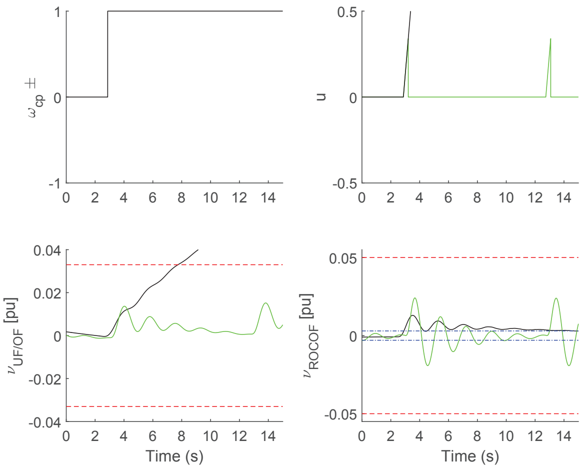

Fig. 21. Simulation results using OPAL-RT: Ramp attack with the anomaly detection based mitigation strategy.

The proposed analytical framework is further employed to devise effective physical mitigation strategies, one of which is based on incorporating a limiter into the synchronization control loop, and the other is based on detecting anomalies in the power system rate-of-change of frequency during the synchronization process. It is determined that the proposed mitigation strategies do not have a tangible impact on the synchronization process in the absence of cyberattacks. Moreover, the proposed mitigation strategies do not interfere with other control loops of the synchronous generator.

Lastly, sensitivity analyses are performed to explore the impact that parameters such as AGC and droop gains of a synchronous generator have on the successful implementation of the attack. The impact of the inverter-based DERs is further investigated for the successful implementation of cyberattacks against synchronization systems in microgrids. The simulation results illustrate that inverter-based DERs, whether operated in virtual inertia or droop control mode, make it more difficult to implement a successful attack against the synchronization system of a microgrid.

Appendix

State Space Representation Matrices

$$A = \begin{bmatrix} 0 & 0 & 0 & -k_c \\ k_G/\tau_G & -1/\tau_G & 0 & -k_d k_G/\tau_G \\ 0 & k_T/\tau_T & -1/\tau_T & 0 \\ 0 & 0 & 1/M & -D/M \end{bmatrix}$$

$$B_{1g} = \begin{bmatrix} k_c & 0 & 0 & 0 \end{bmatrix}^T$$

$$B_{2g} = B_{3g} = \begin{bmatrix} 0 & 0 & 0 & -1/M \end{bmatrix}^T$$

TABLE I
TEST SYSTEM DATA

A. Loads
$LP1$: 47 kW + j15.61 kVAr
$LP2$: 2565 kW + j843.06 kVAr
$LP3$: 289.75 kW + j95.24 kVAr
$LP4$: 152 kW + j49.96 kVAr
$LP5$: 517.8 kW + j170.18 kVAr
$LP6$: 194.8 kW + j64.01 kVAr
B. Energy Storage System
1.1 KV, 125 KWh
C. Generators
$DG1$: 2 MVA PMSG
$H_{gen} = 0.53$, $H_{tur} = 4.27$, $k_s = 1.6$, $D_{gen} = D_{tur} = 0$
P_p = 32, with 2 MW wind turbine, $T_\nu = 0.1$ s
$DG2$: 2.5 MVA SG
AVR parameters: $K_A = 400$, $T_A = 0.02$
Non-reheat thermal turbine: $\tau_T = 450$ ms, $\tau_G = 80$ ms
$k_T = k_G = 1$, $M = 6$, $D = 0.03$
Control and protection parameters: $k_c = 3$, $k_d = 40$
$\tau_\nu = 0.1$, $\tau_F = 1$, $k_\nu = k_s = 1$

TABLE II
DG2 RELAY SETTINGS - IEEE CATEGORY III PROTECTION RELAY STANDARDIZED SETTINGS AS IN [39]

Function	Default setting	Allowable setting limit
OF	62.0 Hz ($0.0\dot{3}$ pu)	66.0 Hz (0.100 pu)
UF	56.5 Hz (0.058 pu)	50.0 Hz (0.167 pu)
ROCOF	3 Hz/s (0.05 pu)	

REFERENCES

[1] S. K. Khaitan, J. D. McCalley, and C. C. Liu, Cyber physical systems approach to smart electric power grid. Springer, 2015.

[2] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317-3318, 2016.

[3] *Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Cyber-Attack Against Ukrainian Critical Infrastructure*, 2016 (accessed August 29, 2019).

[4] *North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards*, 2019 (accessed August 29, 2019). [Online]. Available: http://www.nerc.com

[5] G. N. Ericsson, "Cyber security and power system communication essential parts of a smart grid infrastructure," *IEEE Trans. Power Delivery*, vol. 25, no. 3, pp. 1501-1507, 2010.

[6] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyberphysical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210-224, 2011.

[7] P. Mohajerin Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "Cyber attack in a two-area power system: impact identification using reachability", *in Proc. Amer. Control Conf.*, pp. 962-967, July 2010.

[8] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 580-591, Mar. 2014.

[9] A. Ameli, A. Hooshyar, E. F. El-Saadany and A. M. Youssef, "Attack detection and identification for automatic generation control systems," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4760–4774, Sept. 2018.

[10] Sahoo, Y. Yang, and F. Blaabjerg, "Resilient synchronization strategy for ac microgrids under cyber attacks," *IEEE Trans. on Power Electronics*, vol. 36, no. 1, pp. 73-77, 2020.

[11] Y. Chen, D. Qi, H. Dong, C. Li, Z. Li, and J. Zhang, "A FDI attack-resilient distributed secondary control strategy for islanded microgrids," *IEEE Trans. on Smart Grid*, early access.

[12] S. Zuo, O. A. Beg, F. L. Lewis, and A. Davoudi, "Resilient networked AC microgrids under unbounded cyber attacks," *IEEE Trans. on Smart Grid*, vol. 11, no. 5, pp. 3785-3794, 2020.

[13] H. Zhang, W. Meng, J. Qi, X. Wang, and W. X. Zheng, "Distributed load sharing under false data injection attack in an inverter-based microgrid," *IEEE Trans. on Indust. Electronics*, vol. 66, no. 2, pp. 1543-1551, 2018.

[14] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi,"Synchrony in networked microgrids under attacks," *IEEE Trans. on Smart Grid*, vol. 9, no. 6, pp. 6731-6741, 2017.

[15] K. Koellner, C. Anderson, and R. Moxley, "Generator black start validation using synchronized phasor measurement," *in 2007 60th Annual Conference for Protective Relay Engineers*, pp. 498-504, 2007.

[16] W. Strang, C. Mozina, B. Beckwith, T. Beckwith, S. Chhak, E. Fennell, E. Kalkstein, K. Kozminski, A. Pierce, P. Powell *et al.*, "Generator synchronizing industry survey results", *IEEE Trans. Power Delivery*, vol. 11, no. 1, pp. 174-183, 1996.

[17] M. J. Thompson, "Fundamentals and advancements in generator synchronizing systems," *in 2012 65th Annual Conference for Protective Relay Engineers*, pp. 203-214, 2012.

[18] C. Cho, J.-H. Jeon, J.-Y. Kim, S. Kwon, K. Park, and S. Kim, "Active synchronizing control of a microgrid," *IEEE Trans. Power Electronics*, vol. 26, no. 12, pp. 3707-3719, 2011.

[19] D. Shi, Y. Luo, and R. K. Sharma, "Active synchronization control for microgrid reconnection after islanding," *in IEEE PES Innovative Smart Grid Technologies*, Europe, 2014, pp. 16.

[20] Y. Zhang, R. A. Dougal, and H. Zheng, "Tieline reconnection of microgrids using controllable variable reactors," *IEEE Trans. Industry Applications*, vol. 50, no. 4, pp. 2798-2806, 2013.

[21] "IEEE standard for salient-pole 50 hz and 60 hz SGs and generator/motors for hydraulic turbine applications rated 5 mva and above," IEEE Standard C50.12–2005, 2005.

[22] "IEEE standard for cylindrical-rotor 50 hz and 60 hz SGs rated 10 mva and above," IEEE Standard C50.13–2014, 2014.

[23] D. L. Ransom, "Get in step with synchronization," *IEEE Trans. on Industry Applications*, vol. 50, no. 6, pp. 4210-4215, 2014.

[24] S. M. Manson, A. Upreti, and M. J. Thompson, "Case study: Smart automatic synchronization in islanded power systems," in 2015 IEEEIAS 51st Industrial & Commercial Power Systems Technical Conference (I&CPS). IEEE, 2015, pp. 1-10.

[25] M. J. Thompson and K. G. Ravikumar, "New developments in generator synchronizing systems," *in Proceedings of the 13th Annual Western Power Delivery Automation Conference*, 2011.

[26] R. A. Evans, "A manual/automatic synchronization circuit for a 37.5 MVA steam-turbine-driven generator," *IEEE Trans. Industry Applications*, vol. 26, no. 6, pp. 1081-1085, 1990.

[27] L. C. Gross, L. S. Anderson, and R. C. Young, "Avoid generator and system damage due to a slow synchronizing breaker," Wisconsin Electric Power Company and Schweitzer Engineering Laboratories, USA, 1997.

[28] M. Thompson, "Advancements in synchronizing systems for microgrids and grid restoration," *in proceedings of the 13th International Conference on Developments in Power System Protection*, 2016.

[29] M. J. Thompson, A. Li, R. Luo, M. C. Tu, and I. Urdaneta, "Advanced synchronizing systems improve reliability and flexibility of offshore power systems", *in 2015 IEEE Petroleum and Chemical Industry Committee Conference (PCIC)*, 2015, pp. 19.

[30] T. Foxcroft and M. Thompson, "Advanced synchronising system provides flexibility for complex bus arrangement," 2015.

[31] T. M. L. Assis and G. N. Taranto, "Automatic reconnection from intentional islanding based on remote sensing of voltage and frequency signals," *IEEE Trans. on Smart Grid*, vol. 3, no. 4, pp. 1877-1884, 2012.

[32] R. J. Best, D. J. Morrow, D. M. Laverty, and P. A. Crossley, "Synchrophasor broadcast over internet protocol for distributed generator synchronization," *IEEE Trans. Power Delivery*, vol. 25, no. 4, pp. 2835-2841, 2010.

[33] N. K. Kandasamy, "An investigation on feasibility and security for cyberattacks on generator synchronization process," *IEEE Trans. on Indust. Informatics*, vol. 16, no. 9, pp. 5825-5834, 2019.

[34] ABB SYNCHROTACT 5 - synchronizing relays, 2019 (accessed August 30, 2019). [Online]. Available: https://new.abb.com/power-electronics/synchronizing-equipment/relays/synchrotact-5

[35] SEL-451 Protection, Automation, and Bay Control System, 2019 (accessed August 30, 2019). [Online]. Available: https://selinc.com/products/451/

[36] J. Hong, C.-C. Liu, and M. Govindarasu, "Detection of cyber intrusions using network-based multicast messages for substation automation," in ISGT 2014. IEEE, 2014, pp. 1-5.

[37] Y. M. Khaw, A. Abiri Jahromi, M. F. M. Arani, S. Sanner, D. Kundur and M. Kassouf, "A Deep Learning-Based Cyberattack Detection System for Transmission Protective Relays," *IEEE Trans. on Smart Grid*, early access.

[38] P. Kundur, N. J. Balu, and M. G. Lauby, Power system stability and control. McGraw-hill New York, 1994, vol. 7.

[39] "IEEE standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces," IEEE Std 1547-2018.

[40] R. Tan, H. H. Nguyen, E. Foo, X. Dong, D. K. Yau, Z. Kalbarczyk, R. K. Iyer, and H. B. Gooi, "Optimal false data injection attack againstautomatic generation control in power grids," in Proc. of the 7th Intern. Conf. on Cyber-Physical Systems, IEEE Press, 2016.

Amr S. Mohamed is a PhD candidate in the Department of Electrical and Computer Engineering at the University of Toronto. He received an MASc degree in Electrical and Computer Engineering from the University of Toronto in 2020 where his research focused on smart grid cyberphysical security. His research interests are in utilizing machine learning methods to enhance cyberphysical systems' security, resilience and control.

Mohammadreza Fakhari Moghaddam Arani received the M.Sc. from University of Waterloo, Waterloo, Canada, in 2012, in electrical engineering and the Ph.D. degree in Energy Systems in the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, Canada, in 2017. From 2012 to 2013, he worked as a research associate at the University of Waterloo. He was a NSERC post-doctoral fellow at the University of Toronto, from 2017 to 2019. He joined Ryerson University, Toronto, Canada, as an Assistant Professor in July 2019. His research interests include cyber-physical security of smart grids, renewable and distributed generation, plug-in hybrid electric vehicles, microgrids dynamics and control, power system stability. Dr. Arani is the holder of the Canada Research Chair in Smart Grid Cyber-Physical Security.

Amir Abiri Jahromi (M'16–SM'21) received the Ph.D. degree in Electrical and Computer Engineering from McGill University, Montréal, QC, Canada, in 2016. From January 2018 to December 2019, he was a Postdoctoral Fellow at the University of Toronto. In 2020, he was a Research Associate at the University of Toronto.

Currently, Amir Abiri Jahromi is a Lecturer at the School of Electronic and Electrical Engineering, University of Leeds. His research interests are in the fields of power system modeling, cyber-physical security, reliability, economics and optimization of power systems.

Deepa Kundur is Professor & Chair of The Edward S. Rogers Sr. Department of Electrical & Computer Engineering at the University of Toronto. A native of Toronto, Canada, she received the B.A.Sc., M.A.Sc., and Ph.D. degrees all in Electrical and Computer Engineering in 1993, 1995, and 1999, respectively, from the University of Toronto.

Professor Kundur's research interests lie at the interface of cybersecurity, signal processing and complex dynamical networks. She is an author of over 200 journal and conference papers and is also a recognized authority on cyber security issues. She has served in numerous conference executive organization roles including as Publicity Chair for ICASSP 2021, Track Chair for the 2020 IEEE International Conference on Autonomous Systems, General Chair of the 2018 GlobalSIP Symposium on Information Processing, Learning and Optimization for Smart Energy Infrastructures, TPC Co-Chair for IEEE SmartGridComm 2018. Symposium Co-Chair for the Communications for the Smart Grid Track of ICC 2017, General Chair for the Workshop on Communications, Computation and Control for Resilient Smart Energy Systems at ACM e-Energy 2016, General Chair for the Workshop on Cyber-Physical Smart Grid Security and Resilience at Globecom 2016, General Chair for the Symposium on Signal and Information Processing for Smart Grid Infrastructures at GlobalSIP 2016, General Chair for the 2015 International Conference on Smart Grids for Smart Cities, General Chair for the 2015 Smart Grid Resilience (SGR) Workshop at IEEE GLOBECOM 2015 and General Chair for the IEEE GlobalSIP15 Symposium on Signal and Information Processing for Optimizing Future Energy Systems. Professor Kundur currently serves on the Advisory Board of IEEE Spectrum.

Professor Kundur's research has received best paper recognitions at numerous venues including the 2015 IEEE Smart Grid Communications Conference, the 2015 IEEE Electrical Power and Energy Conference, the 2012 IEEE Canadian Conference on Electrical & Computer Engineering, the 2011 Cyber Security and Information Intelligence Research Workshop and the 2008 IEEE INFOCOM Workshop on Mission Critical Networks. She has also been the recipient of teaching awards at both the University of Toronto and Texas A&M University. She is a Fellow of the IEEE, a Fellow of the Canadian Academy of Engineering, and a Senior Fellow of Massey College.