Protection and Control of Modern Power Systems

ORIGINAL RESEARCH

Open Access

A novel hybrid cybersecurity scheme against false data injection attacks in automated power systems

Shahbaz Hussain[1,2], S. M. Suhail Hussain[3,4*], Marziyeh Hemmati[2], Atif Iqbal[1], Rashid Alammari[1], Stefano Zanero[2], Enrico Ragaini[2] and Giambattista Gruosso[2]

Abstract

The conventional power systems are evolving as smart grids. In recent times cyberattacks on smart grids have been increasing. Among different attacks, False Data Injection (FDI) is considered as an emerging threat that has significant impact. By exploiting the vulnerabilities of IEC 61850 Generic Object-Oriented Substation Events (GOOSE) and Sampled Values (SV) attackers can launch different FDI attacks. In this paper, a real-time set up capable of simulating FDI on GOOSE and SV protocols is developed to evaluate the impact of such attacks on power grid. IEC 62351 stipulates cybersecurity guidelines for GOOSE and SV, but only at communication or Information Technology (IT) level. Hence there is a need to develop a holistic security both at IT and Operation Technology (OT) level. In this regard, a novel sequence content resolver-based hybrid security scheme suitable to tackle FDI attacks on GOOSE and SV is proposed. Furthermore, the computational performance of the proposed hybrid security scheme is presented to demonstrate its applicability to the time critical GOOSE and SV protocols.

Keywords Cyberattacks, False data injection, Real time digital simulation, IEC 61850, Communication protocols, Control authority, Countermeasures

1 Introduction

The power systems of today are evolving into smart grids with the advent of information and communication technology (ICT) [1]. The introduction of ICT has led to increased automation in smart grids. IEC 61850 is emerging as the most popular automation standard in power utility systems [2]. The standard was designed to provide interoperability and standardized communication among different devices and components of power systems. It gives guidelines on the modelling of devices in an electrical system as a logical environment and communication through different protocols. The most significant protocols in the IEC 61850 standard are GOOSE, SV, Manufacturing Message Specification (MMS) and Simple Network Time Protocol (SNTP). The first two protocols are time critical and are used to transfer messages between Protection and Control (P&C) Intelligent Electronic Devices (IEDs), and Circuit Breaker (CB) IEDs via GOOSE and Merging Units (MUs) IEDs via SV.

The ease of operation in cyber physical systems and standardized semantics invites attackers to enter from the doors of cyberspace and exploit various vulnerabilities present in the communication protocols and the standard to achieve their malicious objectives [3]. The most vulnerable devices for attack in the automated

*Correspondence:
S. M. Suhail Hussain
suhail@ieee.org
[1] Department of Electrical Engineering, Qatar University, Doha, Qatar
[2] Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, Milan, Italy
[3] Department of Electrical Engineering, King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia
[4] Interdisciplinary Research Center for Renewable Energy and Power Systems (IRC-REPS), King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia

power systems are the P&C IEDs together with their associated communication [4]. The engineering workplace in control centers may have access to the internet, which opens an access for adversaries to infiltrate and gain a foothold in the power system communication network [5, 6]. An attacker who has gained access to the power system network can directly access the IEDs and launch different attacks. Among different attacks, FDI is considered as an emerging threat that has significant impact. Because of the inherent vulnerabilities, the attackers launch different FDI on GOOSE and SV protocols [7, 8]. With the former, attackers can directly control the protection devices in the field [9, 10], whereas with the latter, they can indirectly lead the IEDs to achieve the same objective as shown in Fig. 1. If the SV messages are tampered with and matched with fault conditions by the attackers, the IEDs will respond to the non-existent faults created in the form of cyberattack. To study the impact of FDI attacks on GOOSE and SV messages, a testbed is required. This paper develops a real-time digital simulator-based hardware-in-the-loop (HIL) testbed to demonstrate and evaluate the impact of FDI attacks on GOOSE and SV messages.

The IEC 61850 standard does not provide any guidelines for securing the GOOSE or SV messages against cyber-attacks, while the IEC 62351 standard complements the IEC 61850 standard by providing the cybersecurity strategies to protect the IEC 61850 communication messages [11]. The aims and objective of this standard are to list mandatory cybersecurity requirements for the attacks originating at IT level. IEC 62351 recommends different authentication and encryption algorithms to secure the channels between publisher and subscriber of GOOSE and SV messages [11]. For instance, references [12–15] provide IT-based solutions for securing GOOSE and SV messages. In [12, 13], light weight message authentication code (MAC) algorithms are proposed to secure the GOOSE messages, whereas [14, 15] introduce caching-based MAC and Less-online/More-offline MAC signatures with reduced computational complexities to secure GOOSE and SV messages. These cyber security algorithms do not however deal with the case of an attack on the end device itself (i.e., when the end devise is compromised). Furthermore, as MAC algorithms are symmetric they require a pre-shared secret key, managing the secret key is a challenging task.

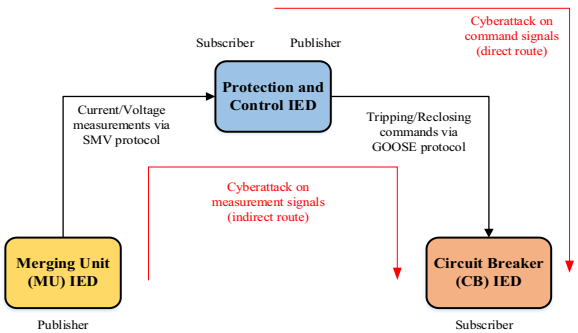

Fig. 1 Direct and indirect attack on CB IED via P&C IED and MU IED, respectively

To overcome these challenges, researchers have proposed different OT-based solutions for securing GOOSE and SV messages. The differences between IT and OT solutions are that IT solutions are based on the cyber/communication domain while OT solutions are based on the physical/power domain. The OT solutions for securing GOOSE and SV messages proposed in literature can be classified as rule-based methods [16, 17], Artificial Intelligence (AI) [18, 19] or Machine Learning (ML) methods [20–23]. Rule-based methods take into consideration the knowledge of communication packets and the possible attack types that can be carried out on them, based on which, various rules are then designed to investigate the packets and provide necessary countermeasures against different attacks. However, the rules should be updated continuously to tackle new types of attacks. The AI and ML learning methods, on the other hand, require large datasets for training which in turn requires large memory and high computational power. Table 1 summarizes the different types of cybersecurity solutions for securing GOOSE and SV messages. From Table 1, it is clear that current work focuses on either IT or OT levels, but a holistic solution including both electrical and communication aspects is still awaited.

It is important to create holistic and hybrid solutions providing security at IT and OT levels in cyber physical systems. This work is an initial effort in this direction to propose an IT + OT based cybersecurity solution that can be implemented at the end device for its security and take into consideration the unique identifiers from both the communication and electrical aspects. GOOSE and SV messages are time critical and have strict timing requirements. Hence, the security scheme must have very low computational complexity to ensure its applicability to GOOSE and SV messages. In this paper, performance evaluation in terms of computational complexity of the proposed hybrid IT + OT security scheme is presented to demonstrate its applicability to time critical GOOSE and SV messages. The main contributions of this paper are summarized as follows:

1. Developing a real-time cyber security testbed using a real-time digital simulator, IEC 61850 protocol emulators, and network tools for studying FDI attacks on GOOSE and SV messages.

Table 1 Cybersecurity solutions provided in the literature on GOOSE and SV Messages

References	Protocol	IT		OT (rule based, AI and ML)	IT + OT based deterministic
		Authentication	Encryption		
Rodríguez et al. [13]	GOOSE & SV	✓	✓	×	×
El Hariri et al. [18]	SV	×	×	✓	×
Ustun et al. [19]	SV	×	×	✓	×
Hussain et al. [12]	GOOSE	✓	×	×	×
Hong et al. [17]	GOOSE	×	×	✓	×
Esiner et al. [15]	GOOSE & SV	✓	×	×	×
Wang et al. [22]	GOOSE	×	×	✓	×
Yang et al. [23]	GOOSE	×	×	✓	×
This work	GOOSE & SV	×	×	×	✓

2. Evaluation and demonstration of the impact of FDI attacks on GOOSE and SV messages
3. Proposing a novel IT + OT cybersecurity solution for GOOSE and SV messages.
4. Performance evaluation in terms of computational complexity of the proposed IT + OT scheme to test its applicability to GOOSE and SV messages

The rest of the paper is organized as follows. Section 2 presents an overview on SV and GOOSE protocols. The methodology to validate cyberattacks in real-time is covered in Sect. 3 which explains the developed testbed for implementation of attacks, and the simulation and modification of GOOSE and SV packets. Section 4 demonstrates the impact of cyberattacks on GOOSE and SV on a simple electrical system and a standard microgrid, whereas Sect. 5 presents the proposed novel sequence content resolver-based cybersecurity solution. Section 6 concludes the work.

2 Overview of GOOSE and SV protocols

IEC 61850 is a popular automation standard initially proposed for substation automation but later extended to entire power utility automation including renewable energy sources. It provides standardized object-oriented models and semantics of different components of a power system and communication protocols for data exchange among different IEDs, controllers and Human Machine Interfaces (HMIs). The digitalized values of currents and voltages are communicated from MUs to P&C IEDs through the SV protocol. Based on these measurements, under different operating conditions such as during fault, maintenance or normal operation, the P&C IEDs send tripping/reclosing commands via the GOOSE protocol to CB IEDs. GOOSE and SV protocols are therefore of utmost importance because of their time-critical nature and protection associated functions. Hence, these protocols are often soft targets for attackers. The attackers target the CB IEDs to change their status either by attacking directly on the GOOSE protocol or indirectly on the SV protocol as shown in Fig. 1.

The GOOSE and SV layer 2 messages are directly mapped to the data link layer, and both protocols have similar packet structure with difference in Protocol

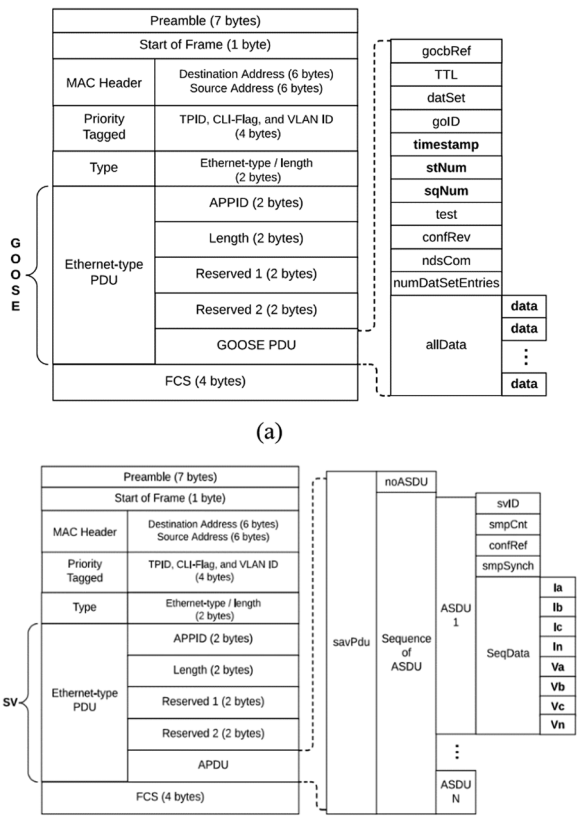

Fig. 2 Structure of **a** GOOSE and **b** SV message [5]

Data Unit (PDU) as shown in Fig. 2a and b. The PDU in both protocols consists of transmission associated counters and the valuable data being transmitted. In GOOSE, it is denoted by GOOSE PDU consisting of parameters such as 'timestamp', 'stNum', 'sqNum' and 'allData'. 'timestamp' denotes time the packet formed. 'stNum' and 'sqNum' are the two counters, with the former being the status number which is incremented whenever there is change in GOOSE data starting with 1, while the latter represents the sequence which keeps on incrementing with each repetition of the GOOSE packet until its maximum value is reached after which it is set to 0. 'allData' contains the data carried by the GOOSE messages. For example, it can be of a Boolean type representing trip/reclose commands for the circuit breakers.

Similarly, SV PDU contains parameters such as 'smpCnt' and 'seqData' or 'PhsMeas1' in each Application Specific Data Unit (ASDU). 'smpCnt' is the counter which increments from 0 to its maximum value depending upon the system frequency under consideration. 'seqData' contains the sampled values of currents and voltages and represent the sinusoidal nature of waveforms with each broadcasted packet. Inside an electrical substation, multiple IEDs communicate with CBs via the GOOSE protocol and with MUs via SV. An attacker can target any of these communication protocols to control the IEDs in general and CB IEDs in particular. GOOSE and SV are time critical protocols with a time limit of 3 ms.

In real scenarios, the attackers' first objective is to access the LAN network. This is achieved by one or a combination of the following vulnerabilities presented in the control center [24]:

1. Poorly configured gateways and firewalls
2. Weak passwords
3. Scanning of IP addresses, ports & services
4. Old OSs
5. USB flash drives
6. Shared internet
7. Weak network segmentation

Once the attackers get access to the network LAN by exploiting the aforementioned vulnerabilities, they can compromise one or multiple IEDs to achieve malicious goals. As there is no security provided in the SV & GOOSE protocols, it is simple for the attackers to compromise the MUs and P&C IEDs and feed false data to lead the P&C IEDs into unwanted operation of multiple CBs. The attacks should be addressed with sound and secure cybersecurity solutions.

3 Methodology to validate combined FDI cyberattacks

To avoid downtime and damage to equipment inside the power grid, a testbed with real-time digital simulators is developed to simulate the attacks and to investigate the effects and impact. Once the 'evaluation of impact' study is carried out in depth, appropriate countermeasures and mitigation methods that can effectively counter these attacks can be developed. Hence, there is a lot of research currently being carried out to develop testbeds using real-time digital simulation [25, 26]. On similar lines, in this paper a testbed is developed using Typhoon HIL and emulated IEDs (using Infotech tools) as shown in Fig. 3 to simulate power systems and later inject FDI attacks to evaluate the impact on power systems.

Two Typhoon HIL 404 devices are used to simulate the microgrid and publisher-subscriber setup for GOOSE and SV protocols. Infotech tools GOOSE Sender and SV Sender are used to inject counterfeit messages to the subscriber to evaluate the impact of attacks on the simulated microgrid. In Fig. 3, the two Typhoon HIL 404 are connected to two computers using USB ports. The central PC is to simulate the microgrid and contains the subscriber while the left laptop simulates the publisher and contains the Infotech tools for the FDI attack. HIL 404 devices and the left laptop are also connected by Ethernet through a switch placed on the right.

The GOOSE messages in Typhoon HIL are programmed to transmit in the form of a structure containing value (XCBR.Pos.stVal), quality (XCBR.Pos.q) and time (XCBR.Pos.t) information. The publisher sends this structure and it is received by the subscriber as shown in Fig. 4. The value contains the two-bit information as shown in Table 2 sent by the publisher and the same is received by the subscriber if there is no FDI attack.

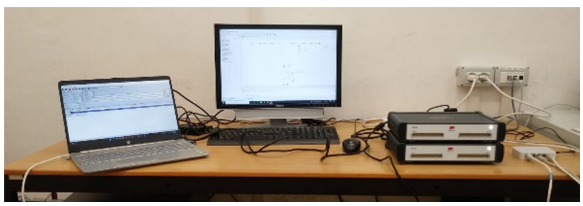

Fig. 3 Testbed with Typhoon HIL, Infotech tools and Wireshark

Fig. 4 GOOSE Publisher and Subscriber in Typhoon HIL Schematics

Table 2 GOOSE value equivalent in different environments

Binary	Hexadecimal	Typhoon	Infotech tools
00 000 000	00	0	00
10 000 000	80	1	10
01 000 000	40	2	01
11 000 000	c0	3	11

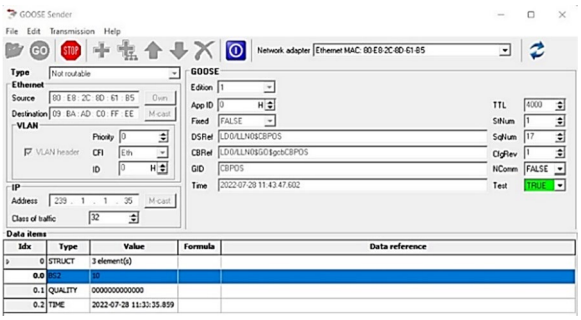

Fig. 5 Runtime of Infotech tools GOOSE Sender with two bit string set to 1

Fig. 6 Set and received GOOSE value in Typhoon SCADA HIL after attack

This is the case of an FDI attack launched from Infotech tools GOOSE Sender. It is set by inserting the gocbRef, datSet and goID parameters taken from the original Typhoon GOOSE packet captured in Wireshark, and by defining the structure by setting the intended value to be sent to the subscriber as shown in Fig. 5. For example, the GOOSE publisher sends value 0 and the same is received, but value 1 is injected by Infotech which will be received now as shown in Figs. 6 and 7. Consequently, it will unintentionally trip the corresponding CB IED inside the microgrid.

The same behavior can be observed in the case of SV packets. Three-phase sinusoidal waveforms of voltage (amplitude 10 V) and current (amplitude 5 A) are sent by the SV publisher in Typhoon HIL and the sampled waveforms are received by the SV subscriber. Now, the attack is carried out by Infotech tools SV Sender where waveforms are sent for voltages (amplitude 1000) and currents (amplitude 100) as shown in Fig. 8. These distort the received waveforms by the subscriber as shown in Fig. 9. The App ID parameter is set in Infotech tools

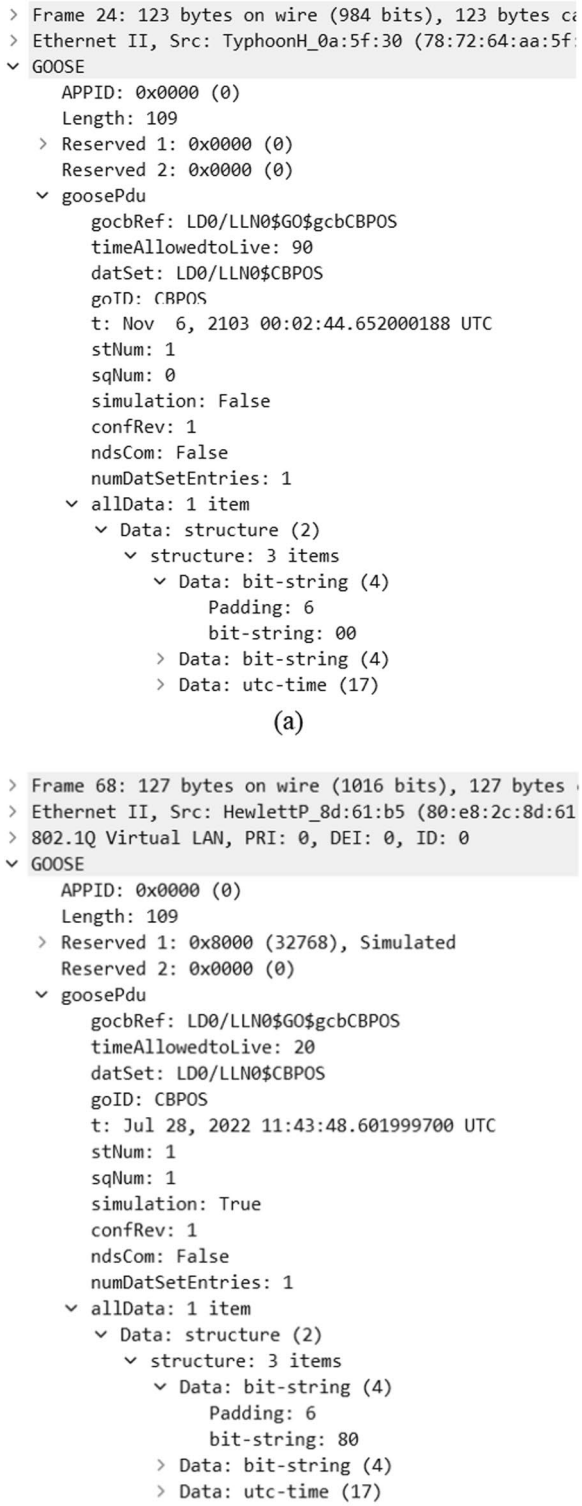

Fig. 7 Original and counterfeit GOOSE packets before **a** and after **b** masquerade attack

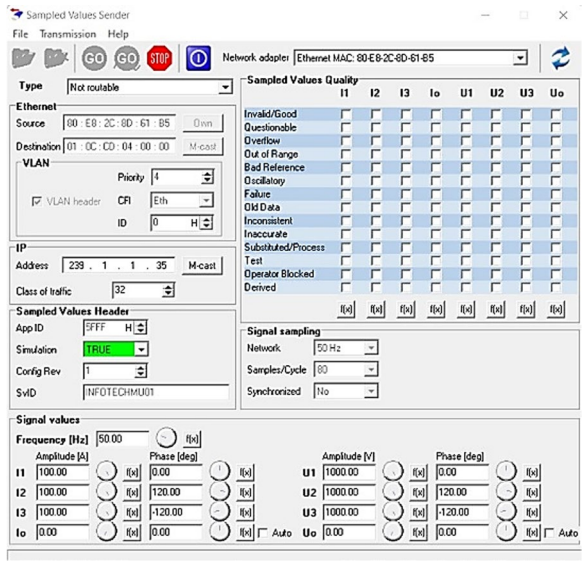

Fig. 8 Runtime of Infotech tools SV Sender with App ID set to 5FFF

SV Sender from the original SV packet of Typhoon captured in Wireshark. This distorted waveform can lead the P&C IEDs to issue tripping/reclosing commands to the CB IEDs.

4 Evaluation of impact on power system

In order to demonstrate the impact of cyberattacks, a test microgrid as shown in Fig. 10 [27] is simulated in Typhoon HIL with the set-up developed in Sect. 3. The microgrid has three load buses (2, 3 and 4), two generation buses (5 and 6) and the grid is connected to bus 13. The reference frequency is 50 Hz and the reference voltage is 400 kV. Buses 2 and 3 have constant impedance loads with active power of 250 MW and power factor 0.9, while bus 4 has constant power load with active power of 400 MW. Generator 1 at bus 6 is a constant power source with active power of 400 MW and is working at 1 per unit of the reference power. Generator 2 at bus 5 is working at 0.5 per unit of the reference power, i.e., 200 MW. The rest of the G2 parameters are shown in Table 3.

G2 has to be started manually after running the SCADA model in Typhoon HIL according to a sequence of controlling operations to avoid loss of synchronism by the grid as shown in Table 4.

A test scenario in which loads 3 and 4 are critical at respective buses 3 and 4 is considered. During the islanded mode of operation, CB_G (grid circuit breaker) is interlocked with CB_L2 (load 2 circuit breaker), such that if CB_G = 1 (open) then CB_L2 = 1 (open).

The GOOSE publisher from Typhoon HIL can transmit open or close commands which are subscribed by both

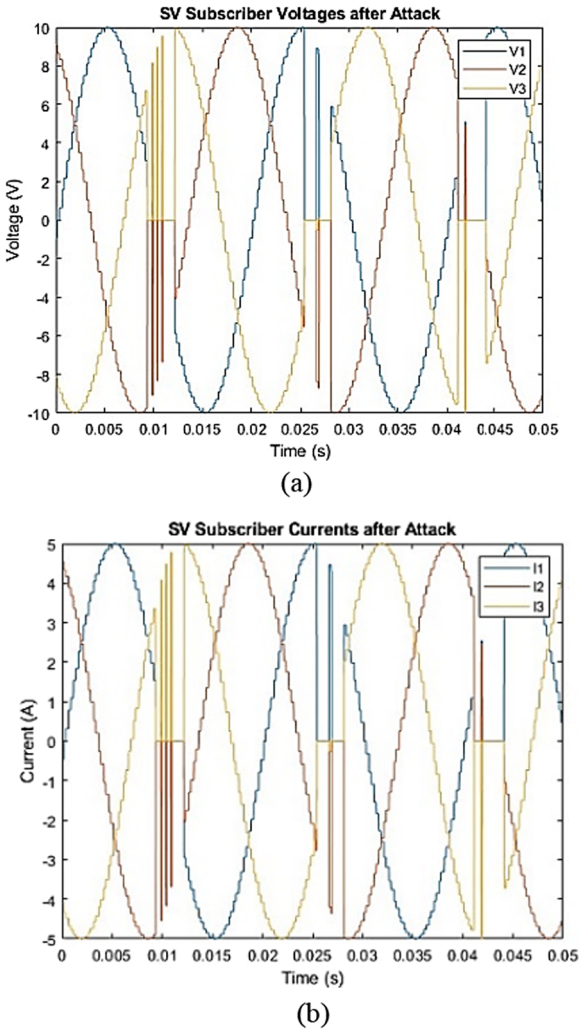

Fig. 9 SV subscriber **a** voltage waveform after the attack **b** current waveform after the attack

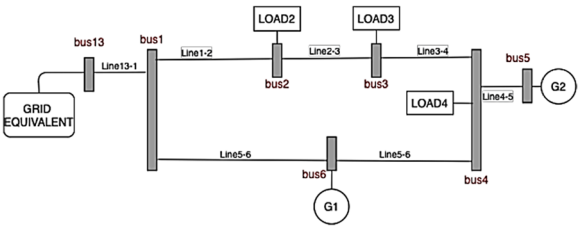

Fig. 10 Microgrid test system

the grid CB and load 2 CB to create grid-connected or islanded modes of operation. An FDI attack occurs when these modes are controlled by an attacker using Infotech tools GOOSE Sender as in this case. This malicious injection of GOOSE packets is subscribed by the grid CB and

Table 3 Parameters of generator G2 connected at bus 5

Nominal active power (P_n)	400 MW
Nominal apparent power (A_n)	444 MVA
Nominal generator line voltage (V_{1Ln})	40 kV
Nominal grid line voltage (V_{2Ln})	400 kV
Nominal frequency (F_n)	50 Hz
Nominal mechanical speed (N)	1500 rpm
Ratio of internal transformer	10

Table 4 Generator start button algorithm [27]

Set the genset in "droop control" operating mode
Enable the generator
Wait for the generator to synchronize with the grid
Change the operating mode to "grid following"

load 2 CB and its impact travels beyond buses 13 and 2 to all other buses. In the same way, the GOOSE publisher in Typhoon HIL can be influenced by injecting malicious SV packets which cause the GOOSE publisher to issue wrong commands. In both scenarios, the grid CB and load 2 CB will be affected and the impact should be observed when these two breakers are tripped, i.e., in the islanded mode of operation.

In order to observe the impact on the microgrid, malicious packets are injected to CB_G and CB_L2 to trip (open) them both, and the voltage and current profiles of all the buses are then discussed to evaluate the impact of this artificially created islanding. It is interesting to note that the grid CB is tripped at 0 s and load 2 is disconnected with a delay at 0.5 s.

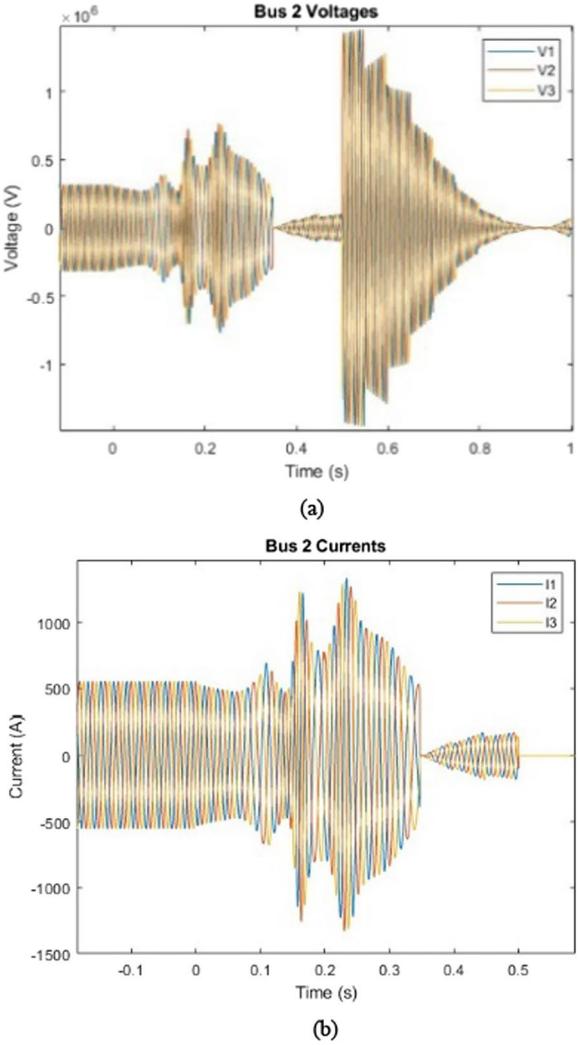

Fig. 11 Bus 2 **a** voltages **b** current with grid disconnected at 0 s and load 2 disconnected at 0.5 s

4.1 Buses 2 and 13 (circuit breaker buses)

These are the buses whose CBs are controlled by the attacker. The voltage and current profiles of buses 2 (load bus) and 13 (grid bus) are shown in Figs. 11 and 12, respectively.

In Fig. 11a, the voltage is sinusoidal before 0 s but gets disturbed at 0 s when the grid is disconnected. The spikes in the voltage rise at 0.5 s when load 2 is disconnected. The current in Fig. 11b shows a similar disturbance to the voltage waveforms from 0 s but stops at 0.5 s as load 2 is disconnected.

In Fig. 12a, the voltage at grid bus 13 follows the same pattern as that of bus 2 in Fig. 11a, i.e., the disturbance appears from 0 s and rises at 0.5 s while the current in Fig. 12b follows the true sinusoidal nature until the grid is disconnected at 0 s.

4.2 Buses 3 and 4 (load buses)

Buses 3 and 4 are the load buses, with constant impedance load (250 MW with pf = 0.9) at bus 3 and constant power load (400 MW) at bus 4. These will be reflected in their current waveforms on islanding by the attacker. The voltage and current profiles of buses 3 and 4 are shown in Figs. 13 and 14, respectively.

In Fig. 13a, the disturbance in voltage starts from 0 s and increases after certain period and the spike rises at 0.5 s. The current waveform in Fig. 13b follows the same behavior as that of voltage as the load is of a constant impedance type.

In Fig. 14a, the voltage at bus 4 replicates the pattern of voltage at bus 3. However, its current in Fig. 14b increases from 0 s and rests before 0.2 s as it is a constant

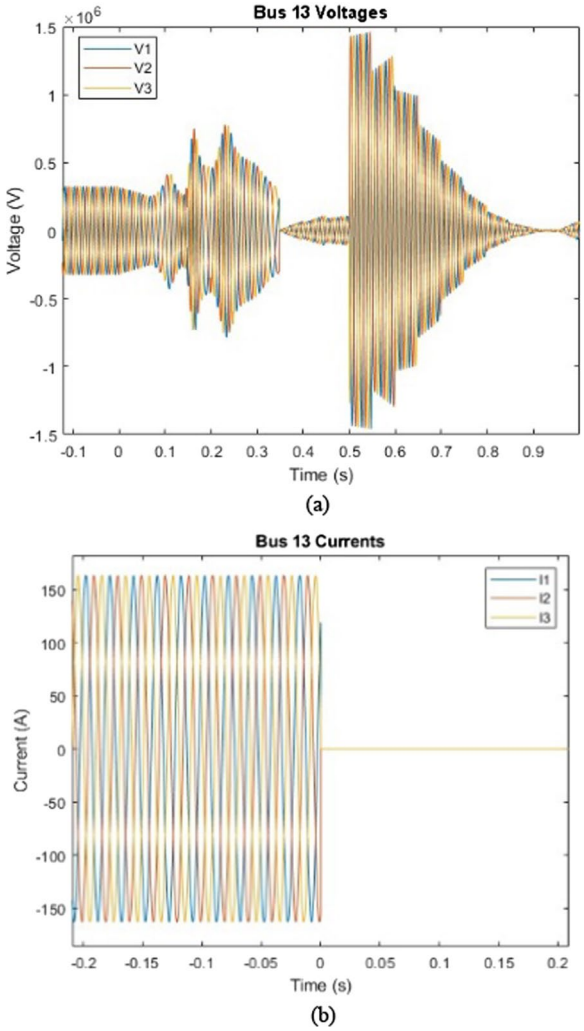

Fig. 12 Bus 13 **a** voltages and **b** currents with grid disconnected at 0 s and load 2 disconnected at 0.5 s

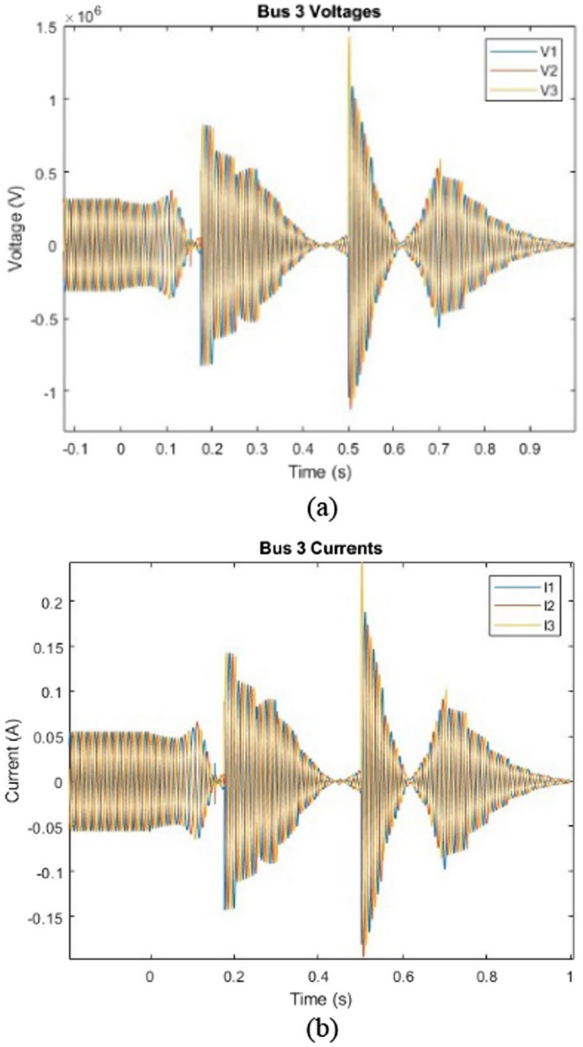

Fig. 13 Bus 3 **a** voltages and **b** currents with grid disconnected at 0 s and load 2 disconnected at 0.5 s

power load bus after which there are minor spikes on the way including the last one at t = 0.5 s.

4.3 Buses 5 and 6 (generation buses)

The generation bus 5 has a constant power source of 400 MW while bus 6 has generator of 200 MW. The impact of the attacker's islanding on these two buses is observed from their voltage and current profiles as shown in Figs. 15 and 16.

In Fig. 15a, the voltage is disturbed from 0 s with spikes at a delay of 0.21 s from 0 s and 0.5 s including the spike at 0.5 s. It matches the tri-spike voltage profiles of buses 3 and 4. As it is a constant power source, its current in Fig. 15b has disturbance from 0 s onwards and rests before 0.15 s with a minor spike at 0.5 s following minor disturbance.

In Fig. 16a, the voltage pattern matches exactly the voltage of bus 5 and the tri-spike pattern of voltages at buses 3 and 4. As it is a generator, its current in Fig. 16b rises initially from 0 s and then undergoes an exponential decay.

4.4 Discussion on waveforms and general impact on the microgrid

There are large spikes at buses 13, 2, 3, 4 at 0.5 s for voltages and currents of bus 3. Currents of buses 2 and 13 vanish after they are disconnected, while buses 5 and 6 voltages are similar with the largest spikes at 0.5 s and 0.71 s. A tri-spike pattern in voltages is observed in most cases, with the exception of currents at buses 4, 5 and 6. Currents disappear for constant power source or load but decay exponentially for the generator. Spikes or

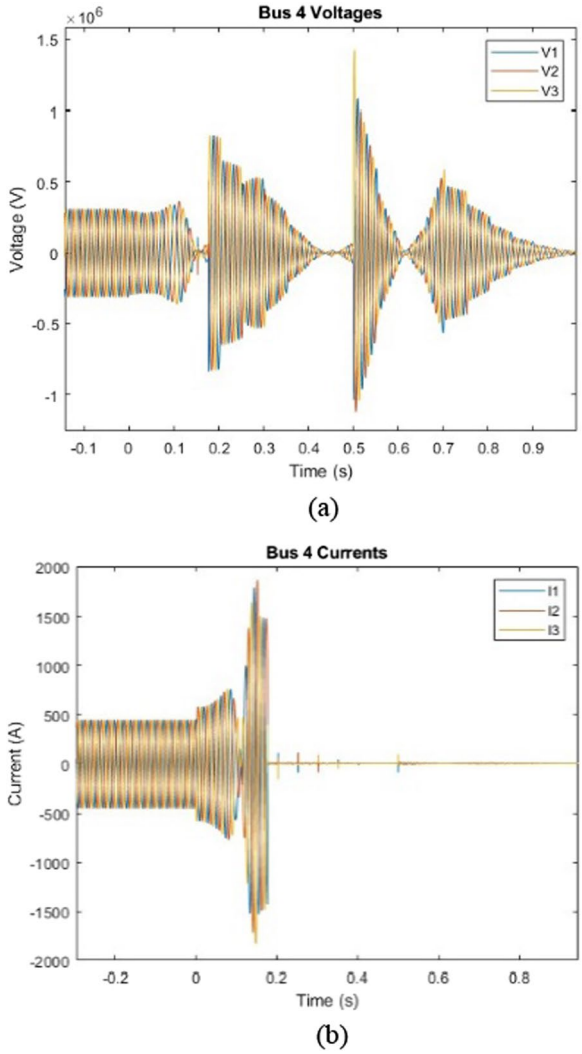

Fig. 14 Bus 4 **a** voltages and **b** currents with grid disconnected at 0 s and load 2 disconnected at 0.5 s

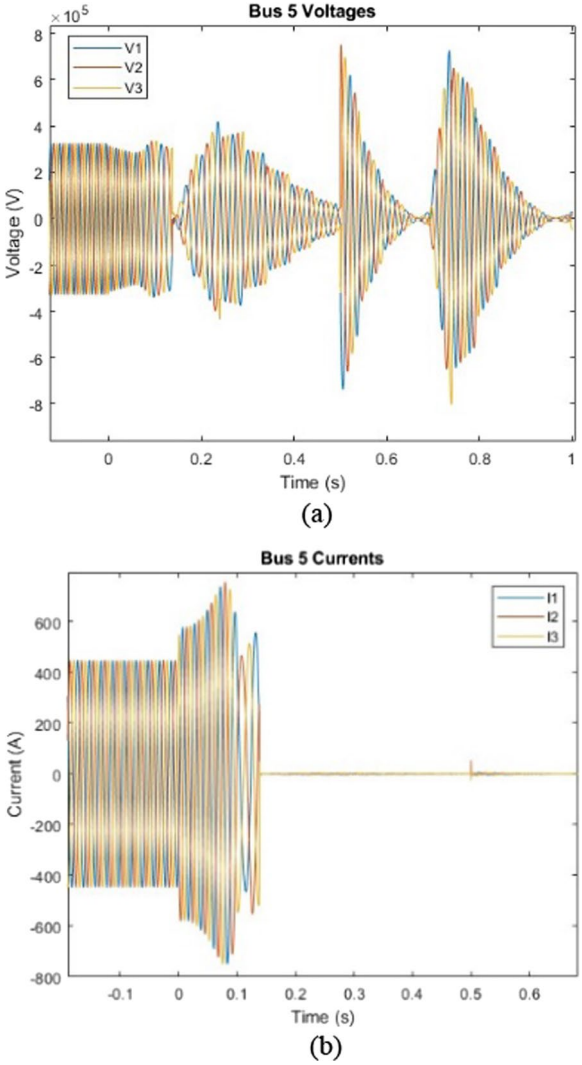

Fig. 15 Bus 5 **a** voltages and **b** currents with grid disconnected at 0 s and load 2 disconnected at 0.5 s

transients are dangerous for power systems, and are all triggered by a malicious GOOSE packet of value = 1 (trip) by the attacker on two interlocked CBs at buses 2 and 13. When the quantity of tripping CBs increases, the impact on the power system will become more severe.

5 Proposed IT + OT hybrid cybersecurity solution

5.1 GOOSE protocol

The block diagram of the sequence content resolver for the GOOSE protocol is shown in Fig. 17. As seen, the CB behaving as a subscriber IED receives GOOSE messages, which are then passed to the COMM module to check the sequence of packets based on transmission counters (stNum and sqNum) and drop the old sequence packets (packets with stNum = n coming after stNum = n + 1) to avoid replay attack. Hence at this stage, all the old sequence packets will be dropped and the traffic is then passed to the ELEC module which will check the data items containing the Boolean value of the tripping/reclosing command. The ELEC module will confer with the neighboring IEDs whether to issue the tripping/reclosing command. On confirmation, appropriate action of allowing or blocking the command will be taken inside the ELEC module. The detailed functional diagram of the novel sequence content resolver for the GOOSE protocol is shown in Fig. 18.

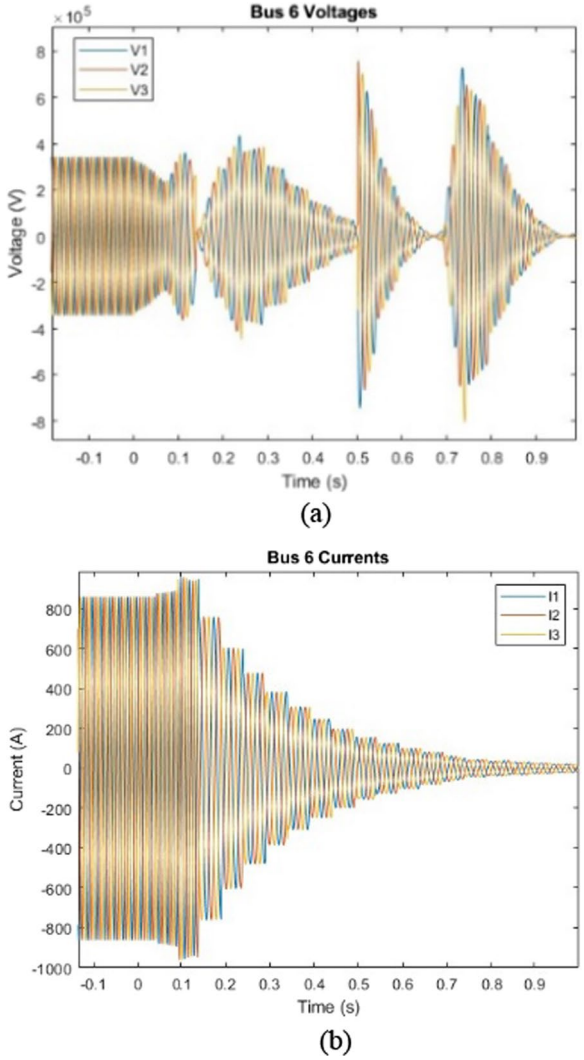

Fig. 16 Bus 6 **a** voltages and **b** currents with grid disconnected at 0 s and load 2 disconnected at 0.5 s

As shown in Fig. 18, in the COMM module, the MAC value is checked first and then the sequence is investigated with transmission counter stNum and sqNum. If the old packets are replayed with previous stNum or current sqNum, it means there is a replay attack and those packets are discarded. In the ELEC module, the status update (stNum++) is confirmed from the adjacent IEDs based on which decision for masquerade attack is made. The data content of GOOSE packets is severed in case of masquerade attack generally with increment of stNum to reflect the counterfeit status update. The packet X is then matched with the stored previous packet Y in the subscriber IED to check for the content and channel attack. Finally, the packet X is matched with packet Z which is obtained from the publisher IED via a dedicated path to check for the sender attack. At any point, if counterfeit messages are found, they will be blocked and proper alerts issued, while only the genuine packets broadcasted from the publisher IED will be passed.

5.2 SV protocol

The block diagram of the sequence content resolver for the SV protocol is shown in Fig. 19. As seen, the P&C IED is subscribing to the MU IED acting as publisher IED and sends the sampled waveforms of voltages and currents. There is a fault module to tackle the system faults before the sequence content resolver, as it handles only cyberattack. The traffic in the subscriber IED is first passed to the COMM module where the sequence of packets is checked and out-of-sequence packets, such as a packet with smpCnt = n coming after packet with smpCnt = n + 1, are dropped. As the smpCnt iterates from 0 to 4000 for 50 Hz and 4800 for 60 Hz, and resets for 80 samples/cycle, the MAC value and timestamps of packets are also checked to drop the out-of-sequence packets to avoid replay attacks. The streamlined version of traffic is then passed over to the ELEC module which checks the data content or values of PhsMeas1 to confirm the true representation of sinusoidal waveforms of voltages and currents. In the case of spikes, transients or disturbances in the waveforms, the instantaneous values of voltages or currents will be way beyond the threshold and these packets will be discarded. The detailed functional diagram of the sequence content resolver for the SV protocol is shown in Fig. 20.

In the subscriber IED, the MAC value is checked first for the integrity of packets in the COMM module. The sequence of packets is then investigated by smpCnt and timestamps to deter old sequence packets to avoid replay attacks. The traffic is then handed over to the ELEC module where content of PhsMeas1 is screened to be in limit. If the values of voltages or currents are in limits, they are passed, otherwise they are blocked and a content attack alert is issued. The packet X is then compared with previous stored packet Y in subscriber IED to again check out threshold values and channel attack. Finally, the packet X is matched with the packet Z which is stored in the publisher IED and transmitted via a dedicated path to the subscriber IED for out-of-limits values. In the case of values going beyond the thresholds, the packets are blocked with a sender attack alert, otherwise they are passed.

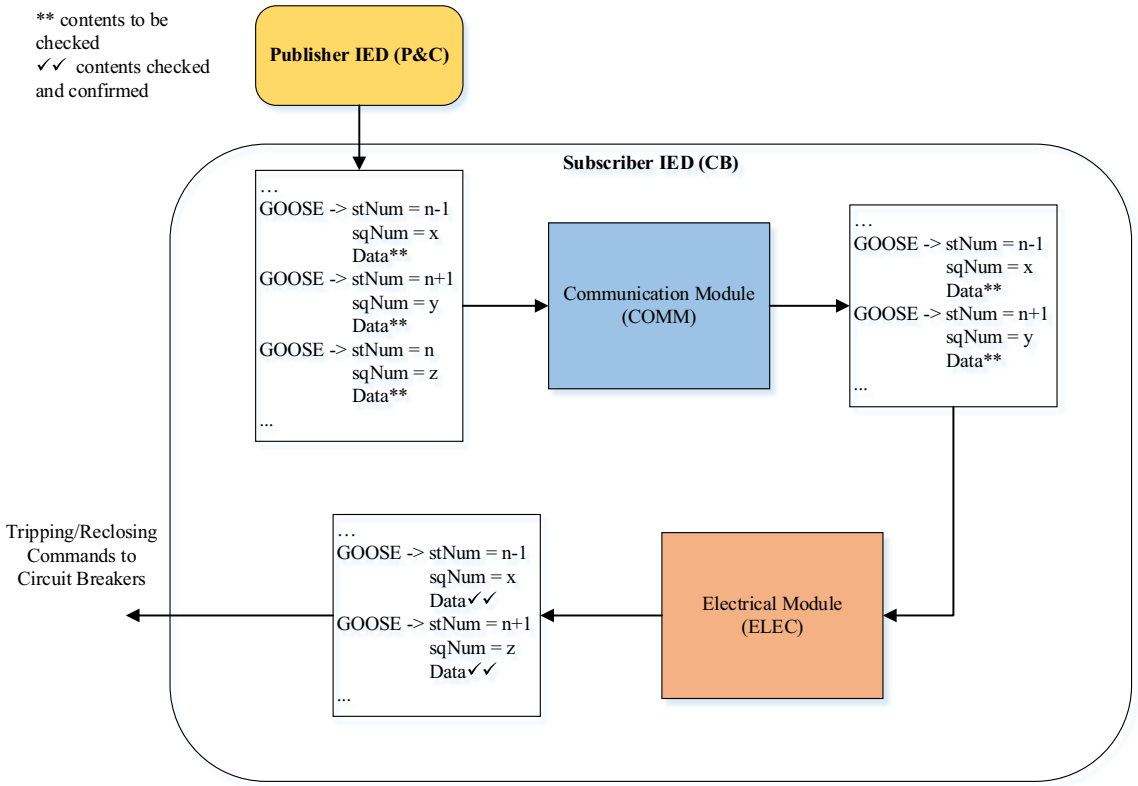

Fig. 17 Block diagram of sequence content resolver for GOOSE protocol

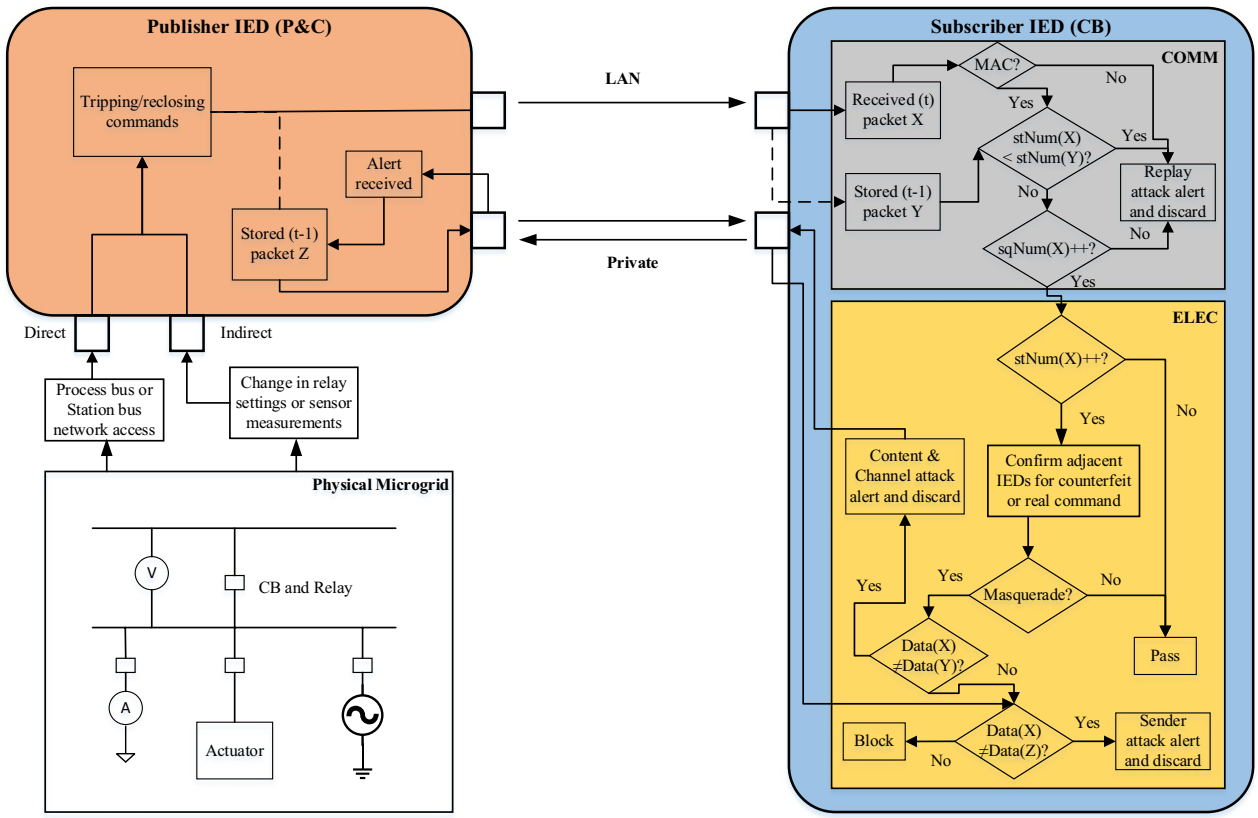

Fig. 18 Functional diagram of sequence content resolver for GOOSE protocol

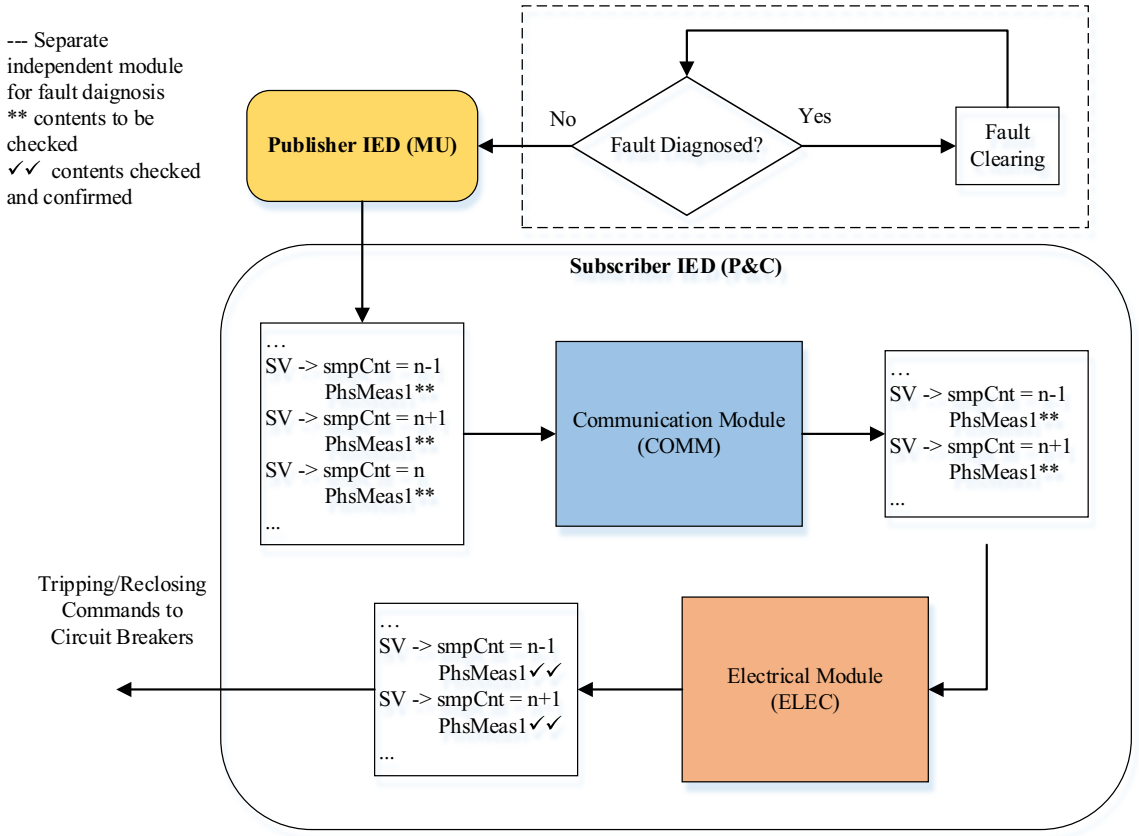

Fig. 19 Block diagram of sequence content resolver for the SV protocol

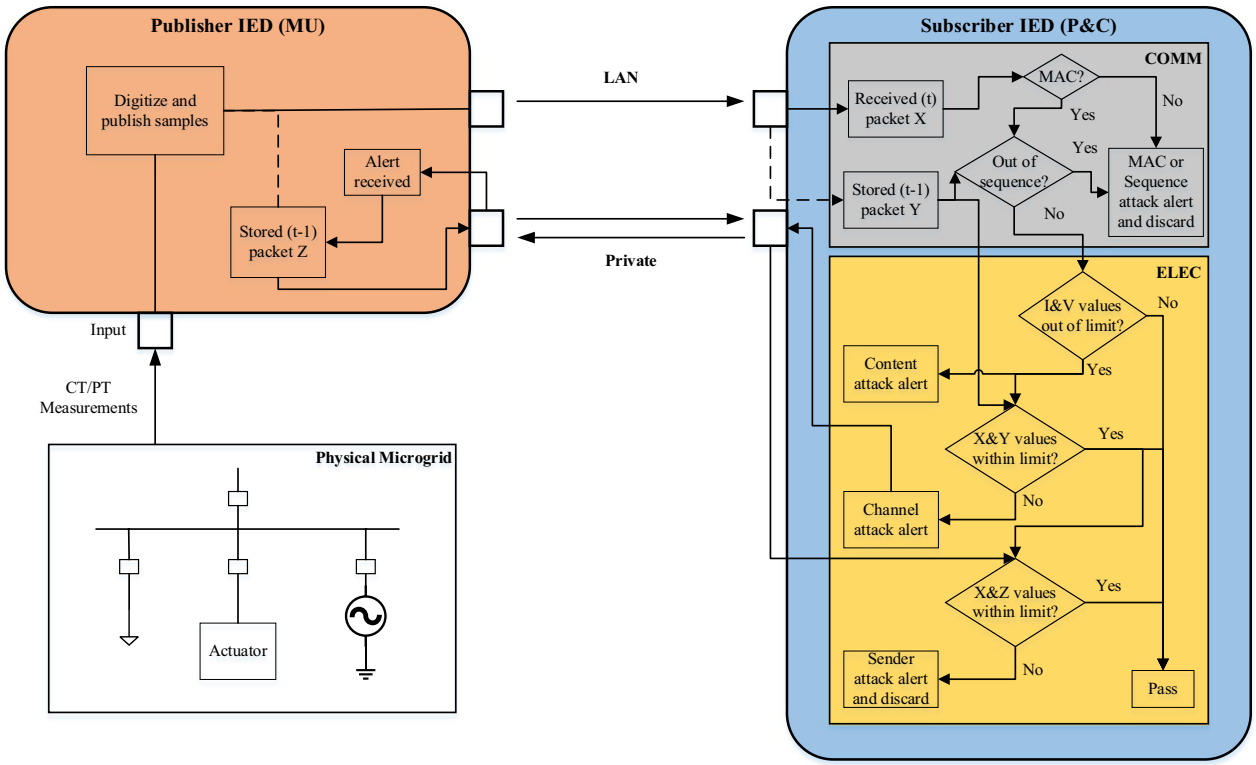

Fig. 20 Functional diagram of sequence content resolver for the SV protocol

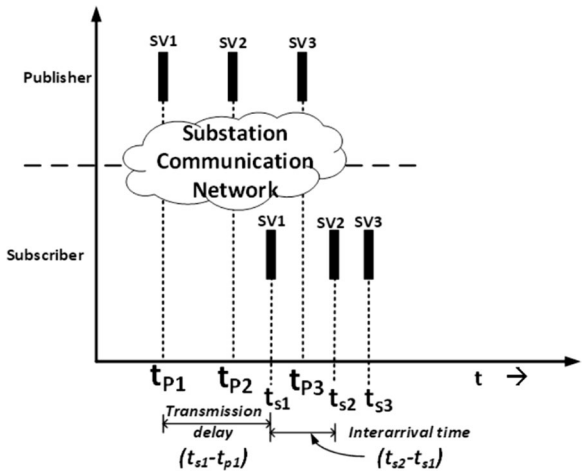

Fig. 21 SV message exchange between a publisher and a subscriber

5.3 Performance evaluation

GOOSE messages generally carry time critical messages and hence have a stringent timing requirement. The typical End-to-End delay requirements for critical GOOSE messages is 3 ms including the communication network transmission delay. The transmission delay is the duration from publishing of a GOOSE packet at the publisher to its arrival at the subscriber. SV messages have very high messaging rates resulting in high throughputs and very low inter-arrival times. Inter-arrival time is the duration between arrivals of two consecutive SV packets at the subscriber. Figure 21 illustrates the inter-arrival times and communication network transmission delays for SV messages. The typical SV messages rates, as per the IEC 61850 standards, is 4000 and 4800 packets per second for 50 Hz and 60 Hz systems, respectively, with the inter-arrival times of SV messages being 0.24 ms and 0.21 ms.

The performance will be sound if the time to probe the GOOSE / SV packet by the proposed IT + OT scheme is less than the transmission delays for GOOSE messages and the interarrival times for SV packets to avoid congestion. Hence, the computational performance evaluation of the proposed IT + OT solution is presented in this section. The proposed IT + OT solution has two main parts, i.e., implementation of MAC algorithms (IT) and sequence content resolver (OT). From [13], it was observed that the computational delays for MAC algorithms is 0.007 ms. The computational time for executing the sequence content resolver is calculated. The difference in the time stamps of the simulation before and after the execution of sequence content resolver code gives the computational time elapsed. The simulation is performed for 100 GOOSE and SV packets, respectively, and the average computational delay for executing sequence content resolver is found to be 0.006 ms. Hence, the total computational delay for the proposed IT + OT scheme is found to be 0.013 ms, which is well below the 0.21 ms limit. Hence, it can be concluded that the proposed security mechanism can be readily applied to time critical GOOSE and SV messages. Table 5 shows the comparative computational performance of different security schemes in the literature and the proposed security scheme for SV messages.

Table 5 Computational delays of cybersecurity mechanism for SV packets

Scheme	Computational time in ms	Platform utilized	Lower than Inter-arrival time
M. Rodríguez et al. [13]	0.006	Zynq 7020 FPGA	✓
M. El Hariri et al. [18]	0.29	ODROID C2 microcontroller	×
T. S. Ustun et al. [19]	0.049	Intel Core i7 @ 2.80 GHz 32 GB RAM	✓
This work	0.013	Intel Core i7 @ 1.80 GHz 16 GB RAM	✓

Typically, P&C IEDs perform multiple protection and control functions simultaneously. Hence, P&C IEDs are subscribed to multiple SV streams from different MU IEDs. When P&C IEDs are subscribed to multiple SV streams at the same time, the inter-arrival times of the packets decrease considerably. For successful operation, the incoming packets must be processed (including the security scheme processing) within the inter-arrival time. If the incoming packet is not processed within the inter-arrival time, it leads to buffer overflows and packet losses. Table 6 compares the computational delays for multiple SV streams supported by the proposed hybrid scheme and other existing schemes in the literature. From Table 6, it can also be seen that the proposed hybrid security scheme can support up to 15 SV streams.

Table 6 Computational delays for multiple SV streams

Scheme		M. Rodríguez et al. [13]	M. El Hariri et al. [18]	T. S. Ustun et al. [19]	This work
Processing time for each packet (ms)		0.006	0.29	0.049	0.013
No. of SV streams (inter-arrival time in ms)	1 (0.2)	✓	×	✓	✓
	2 (0.1)	✓	×	✓	✓
	3 (0.067)	✓	×	✓	✓
	5 (0.04)	✓	×	×	✓
	10 (0.02)	✓	×	×	✓
	15 (0.013)	✓	×	×	✓

× denotes processor is not capable to support processing of SV streams for given scheme. ✓ denotes processor can support the processing of SV streams for given scheme

6 Conclusions

In this work, a novel methodology to simulate and validate replay and masquerade attacks on GOOSE and SV protocols is developed using a testbed. The effect of these attacks on electrical systems is then studied and a novel cybersecurity solution called a 'sequence content resolver' is proposed. The structure of GOOSE and SV protocols with respect to their parameters for attack simulation and cybersecurity perspective is also investigated. Future work will focus on the implementation of cybersecurity solutions on lines of rule-based and artificial intelligence mitigation methods.

Abbreviation

AI	Artificial intelligence
ASDU	Application specific data unit
CB	Circuit breakers
FDI	False data injection
GOOSE	Generic object-oriented substation events
HMI	Human machine interface
IT	Information technology
IED	Intelligent electronic devices
MAC	Message authentication code (MAC)
MMS	Manufacturing message specification
ML	Machine learning
MU	Merging unit
OT	Operation technology
P&C	Protection and control
PDU	Protocol data unit
stNum	Status number
sqNum	Sequence number
SNTP	Simple network time protocol
SV	Sampled values
P_n	Nominal active power
A_n	Nominal apparent power
V_{1Ln}	Nominal generator line voltage
V_{2Ln}	Nominal grid line voltage
F_n	Nominal frequency
N	Nominal mechanical speed

Acknowledgements

Author at KFUPM acknowledge the support from Interdisciplinary Research Center for Renewable Energy and Power Systems under grant INRE2322.

Author contributions

S.H.: Writing—Original Draft, Methodology, Validation, Conceptualization, Software, Investigation; S.M.S.H.: Writing—Original Draft, Methodology, Validation, Conceptualization, Investigation, Supervision; M.H.: Writing—Review & Editing, Conceptualization, Software; A.I.: Writing—Review & Editing, Funding acquisition, Supervision, Conceptualization; R.A.: Writing—Review & Editing, Supervision; S.Z.: Writing—Review & Editing, Supervision; E.R.: Writing—Review & Editing, Supervision; G.G.: Writing—Review & Editing, Supervision.

Funding

No funding to declare.

Availability of data and materials

Not applicable.

Declarations

Competing interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Received: 29 January 2023 Accepted: 25 July 2023
Published online: 07 August 2023

References

1. Wang, K., Yu, J., Yu, Y., Qian, Y., Zeng, D., Guo, S., et al. (2017). A survey on energy internet: Architecture, approach, and emerging technologies. *IEEE Systems Journal, 12*, 2403–2416.
2. Aftab, M. A., Hussain, S. S., Ali, I., & Ustun, T. S. (2020). IEC 61850 based substation automation system: A survey. *International Journal of Electrical Power & Energy Systems, 120*, 106008.
3. Hussain, S., Fernandez, J.H., Al-Ali, A.K., & Shikfa, A. (2021). Vulnerabilities and countermeasures in electrical substations. *International Journal of Critical Infrastructure Protection*, 100406.
4. Hagman, K., Frisk, L., Menezes, J., & Saha, M.M. (2016). Cyber security measures in protection and control IEDs. *13th International Conference on Development in Power System Protection (DPSP)*, Edinburgh.
5. Wright, J.G., & Wolthusen, S.G. (2017). Access Control and Availability Vulnerabilities in the ISO/IEC 61850 Substation Automation Protocol. *Lecture Notes in Computer Science, Springer, Cham,* 10242.
6. Rashid, M.T.A., Yussof, S., Yusoff, Y., & Ismail, R. (2014). A review of security attacks on IEC61850 substation automation system network. *6th international conference on information technology and multimedia*.
7. Roomi, M.M., Hussain, S.M.S., Mashima, D., Chang, E.C., &. Ustun, T.S. (2023). Analysis of False Data Injection Attacks Against Automated Control for Parallel Generators in IEC 61850-Based Smart Grid Systems. *IEEE Systems Journal*.
8. Jahromi, A. A., Kemmeugne, A., Kundur, A., & Haddadi, A. (2021). Cyber-Physical Attacks Targeting Communication-Assisted Protection Schemes. *IEEE Transactions on Power Systems, 35*(1), 440–450.
9. Hussain, S., *et al.* (2021). A novel methodology to validate cyberattacks and evaluate their impact on power systems using real time digital simulation. *IEEE Texas Power and Energy Conference (TPEC)*
10. Hoyos, J., Dehus, M., & Brown, T.X., (2012). Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure. *2012 IEEE Globecom Workshops*.
11. Hussain, S. M. S., Ustun, T. S., & Kalam, A. (2020). A Review of IEC 62351 Security Mechanisms for IEC 61850 Message Exchanges. *IEEE Transactions on Industrial Informatics, 16*(9), 5643–5654.
12. Hussain, S. M. S., Farooq, S. M., & Ustun, T. S. (2019). Analysis and Implementation of Message Authentication Code (MAC) Algorithms for GOOSE Message Security. *IEEE Access, 7*, 80980–80984.
13. Rodríguez, M., Lázaro, J., Bidarte, U., Jiménez, J., & Astarloa, A. (2021). A Fixed-Latency Architecture to Secure GOOSE and Sampled Value Messages in Substation Systems. *IEEE Access, 9*, 51646–51658.
14. U. Tefek, E. Esiner, D. Mashima, B. Chen and Y. -C. Hu, (2022). Caching-based Multicast Message Authentication in Time-critical Industrial Control Systems. *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications*, 1039–1048.
15. Esiner, E., et al. (2022). LoMoS: Less-Online/More-Offline Signatures for Extremely Time-Critical Systems. *IEEE Transactions on Smart Grid., 13*(4), 3214–3226.
16. El Hariri, M., Faddel, S., & Mohammed, O. (2018). Physical-model-checking to detect switching-related attacks in power systems. *Sensors, 18*, 2478.
17. Hong, J., Nuqui, R. F., Kondabathini, A., Ishchenko, D., & Martin, A. (2018). Cyber attack resilient distance protection and circuit breaker control for digital substations. *IEEE Transactions on Industrial Informatics, 15*, 4332–4341.
18. El Hariri, M., Harmon, E., Youssef, T., Saleh, M., Habib, H., & Mohammed, O. (2019). The iec 61850 sampled measured values protocol: Analysis, threat identification, and feasibility of using nn forecasters to detect spoofed packets. *Energies, 12*, 3731.
19. Ustun, T. S., Hussain, S. S., Yavuz, L., & Onen, A. (2021). Artificial Intelligence Based Intrusion Detection System for IEC 61850 Sampled Values Under Symmetric and Asymmetric Faults. *IEEE Access, 9*, 56486–56495.
20. C. Feng, T. Li, and D. Chana, (2017). Multi-level anomaly detection in industrial control systems via package signatures and LSTM networks. *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 261–272.

21. V. K. Singh and M. Govindarasu, (2021). Cyber-Physical Anomaly Detection for Wide-Area Protection using Machine Learning. *IEEE Transactions on Smart Grid*.
22. Wang, X., Fidge, C., Nourbakhsh, G., Foo, E., Jadidi, Z., & Li, C. (2022). Anomaly Detection for Insider Attacks From Untrusted Intelligent Electronic Devices in Substation Automation Systems *IEEE*. *Access, 10*, 6629–6649.
23. Yang, L., Zhai, Y., Zhang, Y., Zhao, Y., Li, Z., & Xu, T. (2022). A new methodology for anomaly detection of attacks in IEC 61850-based substation system. *Journal of Information Security and Applications, 68*, 103262.
24. Quincozes, S. E., Albuquerque, C., Passos, D., & Mossé, D. (2021). A survey on intrusion detection and prevention systems in digital substations. *Computer Networks, 184*, 107679.
25. Cao, G., Gu, W., Gu, C., Sheng, W., Pan, J., Li, R., & Sun, L. (2019). Real-time cyber−physical system co-simulation testbed for microgrids control. *IET Cyber-Physical Systems: Theory & Applications, 4*, 38–45.
26. Montoya, J., Brandl, R., Vishwanath, K., Johnson, J., Darbali-Zamora, R., Summers, A., et al. (2020). Advanced laboratory testing methods using real-time simulation and hardware-in-the-loop techniques: A survey of smart grid international research facility network activities. *Energies, 13*, 3267.
27. M. Hemmati, H. Palahalli, G. Gruosso, and S. Grillo, (2021). Interoperability analysis of IEC61850 protocol using an emulated IED in a HIL microgrid testbed. *2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 152–157.