EasyChair Preprint

№ 3006

Cyber Attacks on Protective Relays in Digital Substations and Impact Analysis

Vetrivel Subramaniam Rajkumar, Marko Tealane,
Alexandru Stefanov and Peter Palensky

March 19, 2020

Cyber Attacks Against Protective Relays in Digital Substations and Impact Analysis

Vetrivel Subramaniam Rajkumar *, Marko Tealane†, Alexandru Ştefanov *, Peter Palensky *
*Department of Electrical Sustainable Energy
Delft University of Technology
Delft, The Netherlands
v.subramaniamrajkumar@tudelft.nl
†Department of Electrical Power Engineering and Mechatronics
Talinn University of Technology
Talinn, Estonia
marko.tealane@taltech.ee

***Abstract*—Power systems automation and communication standards are crucial for the transition of the conventional power system towards a smart grid. The IEC 61850 standard is widely used for substation automation and protection. It enables real-time communication and data exchange between critical substation automation devices. IEC 61850 serves as the foundation for open communication and data exchange for digital substations of the smart grid. However, IEC 61850 has cyber security vulnerabilities that can be exploited with a man-in-the-middle attack. Such coordinated cyber attacks against the protection system in digital substations can disconnect generation and transmission lines, causing cascading failures. In this paper, we demonstrate a cyber attack involving the Generic Object-Oriented Substation Event (GOOSE) protocol of IEC 61850. This is achieved by exploiting the cyber security vulnerabilities in the protocol and injecting spoofed GOOSE data frames into the substation communication network at the bay level. The cyber attack leads to tripping of multiple protective relays in the power grid, eventually resulting in a blackout. The attack model and impact on system dynamics are verified experimentally through hardware-in-the-loop simulations using commercial relays and Real-Time Digital Simulator (RTDS).**

***Index Terms*—cyber-physical systems; IEC 61850; cyber security; cyber attacks, cascading failures**

I. Introduction

The integration of renewable energy resources, driven by the energy transition calls for a paradigm shift in the makeup of the power system. Digitalization of the power grid and deployment of Information and Communication Technologies (ICTs) allow for increased inter-connectivity between different components and layers of the grid. This is realized through advanced power system automation and communication standards, which form the basis for a smart grid. Digitalization enables the possibility towards a more efficient, intelligent, resilient, and sustainable resource utilization. However, the increased digitalization brings newer challenges to cyber secure the operation of the smart grid [1], [2].

IEC 61850 is a modern power system communications standard that serves as the foundation for an open communication and data exchange within digital substations. These substations are an integral part of the smart grid. A digital substation offers a plethora of benefits, not limited to: improved measuring accuracy, ease of device configuration, and real-time performance. IEC 61850 standard defines a vendor agnostic data exchange architecture applied to substation automation and protection systems. This allows for the interoperability of devices from different vendors. IEC 61850 adopts existing standard communication protocol stacks and services [3]. Over the years, IEC 61850 has grown out of the substation boundaries to cover substation-to-substation and substation-to-control center applications. Furthermore, it enables information exchange through different communication protocols, one of which is covered extensively in this paper. The Generic Object-Oriented Substation Event (GOOSE) protocol is used for communicating critical events in real-time, e.g., tripping commands between two or more protective relays using Ethernet multi-cast [4].

On the flip side, IEC 61850 comes with its fair share of cyber security vulnerabilities. For example, it does not implement any encryption because of the real-time requirements imposed by the protection system to communicate trip signals. The additional computational burden to encrypt/decrypt the GOOSE messages may significantly impact the real-time performance of protective relays. The exploit of GOOSE vulnerabilities is demonstrated in [5]–[7]. It is a cause for concern that such cyber security loopholes maybe exploited by potential cyber attackers.

Cyber attacks against power grids are a real modern day threat. On December 23, 2015, cyber attacks were conducted on the power grid in Ukraine. Seven 110 kV and twenty-three 35 kV power substations were disconnected from the power grid for hours. These attacks were the first publicly acknowledged cyber incidents to result in power outages that affected about 225,000 customers. The attackers modified schedules for uninterruptible power supplies, opened circuit breakers, and used 'KillDisk' for wiping of workstations, servers, and remote terminal units [8]. On December 17, 2016, another cyber attack was launched in Ukraine. It affected the Supervisory Control And Data Acquisition (SCADA) system at the transmission level targeting a single 330 kV substation. This attack resulted in a power outage, in the distribution network wherein a total load of 200 MW was lost. This is the first publicly acknowledged malware that targeted power systems, leading to a power outage [9]. Consequently, cyber security of power systems has emerged as an important area of research [10], [11].

Previous work on cyber security of power systems, has shown how substation communication networks can be com-

promised in various ways [12]. The cyber attacks exploiting the vulnerabilities of TCP/IP-based substation communication networks are discussed in [10]. The various vulnerabilities present in the IEC 61850 standard, i.e., GOOSE protocol, and how they may be exploited are reported in [5]–[7], [13]. However, what is found missing in previous work is a generic cyber attack model applicable to all IEC 61850-compliant commercial relays. Furthermore, an experimental framework is needed to conduct cyber attacks on commercial protective relays. This facilitates the impact analysis of such cyber attacks on power system dynamics, and investigation of how they may lead to cascading failures in the grid and even a blackout.

In this paper, we propose a generic model of a man-in-the-middle cyber attack that exploits the security vulnerabilities of IEC 61850 GOOSE protocol. The objective is to highlight the dangerous implications of not securing IEC 61850 standard used for protection systems. The cyber attack injects spoofed GOOSE data frames into the substation communication network, at the bay level. This leads to tripping of multiple protective relays at various digital substations, resulting in the disconnection of multiple generation and transmission lines. By orchestrating a carefully coordinated cyber attack on one or more protective relays in digital substations, a cascading failure is induced, eventually culminating in a blackout. The attack model and impact on system dynamics are verified on the proposed experimental framework. This is realised through Hardware-in-the-Loop (HIL) simulations of commercial relays with a Real-Time Digital Simulator (RTDS).

The rest of this paper is organized as follows: Section II presents the nature and details of the cyber attack model developed in this paper to instigate abnormal system conditions. The case study and experimental framework are covered in Section III, while Section IV presents the simulation results. Conclusions and recommendations are discussed in Section V.

II. Cyber Attack Model on Protective Relays

A cyber attack in a digital substation is a malicious event where an adversary modifies, degrades or disables a service of at least one protection, automation or control device. This brings into question the paths and means through which cyber attacks are executed, i.e., attack vectors. To this end, physical access to the substation communication network is not always necessary [10]. The cyber attacks can be conducted remotely by exploiting backdoors to access the Local Operating Network (LON), e.g., infected station control systems or engineering workstations used for relay configuration. With the increasing adoption of IEC 61850, the traditional hardwiring of protective relays is replaced by digital communications implemented via Ethernet over fibre optics. IEC 61850 implements a publisher-subscriber communication mechanism for various protection schemes. In this context, the status and trip signals are communicated as GOOSE frames via the process bus between various Intelligent Electronic Devices (IEDs) at the bay level as represented in Fig.1. As IEC 61850 traffic is not encrypted, attackers can conduct a man-in-the-middle attack, which is the focus of this research. Such a cyber attack can be modelled in two stages as described below.

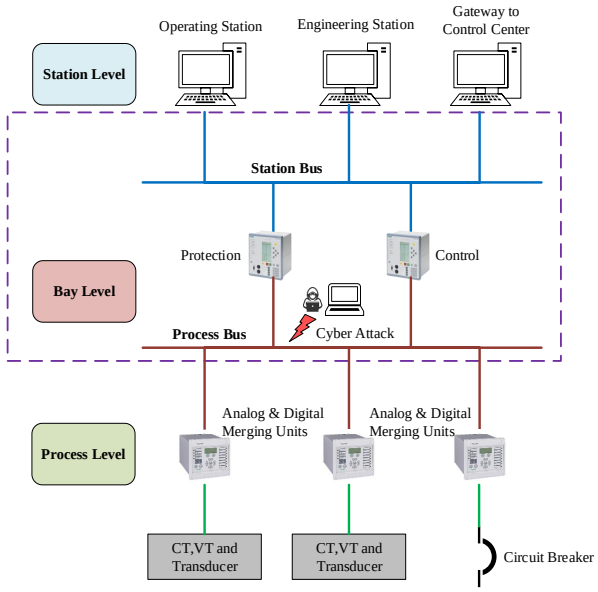


Fig. 1: Digital substation network layout.

A. Network Reconnaissance

The first stage is to monitor the substation communication traffic and identify GOOSE messages. The structure of a typical GOOSE frame is show in Fig.2. It includes the physical link destination and source addresses, i.e., Media Access Control (MAC), tag of the Virtual Local Area Network (VLAN), type header, length of the frame, and data payload. Under the data payload, the status and sequence number fields, i.e., stNum and sqNum, in the GOOSE message are often considered as basic security mechanisms. In the processing algorithm for GOOSE protocol, the sequence number updates incrementally during normal operation, while the status number remains fixed. In case of a power system event, e.g., relay trip, the status number is incremented by one and sequence number is reset to zero. Therefore, incoming GOOSE messages with a lower status number are not processed and the packet is discarded.

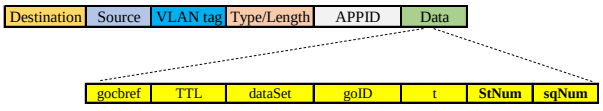


Fig. 2: Structure of a typical GOOSE data frame.

However, such measures are inadequate and do not guarantee cyber security, because any adversary can listen to the current status and sequence number and inject suitable values. Also, the source MAC address of the GOOSE packet can be spoofed easily by the attacker [5], [10], [11]. Keeping this in

mind, this paper seeks to formulate a generic model of a man-in-the-middle cyber attack to supply false GOOSE information to protective relays. The first stage of the attack is completed by monitoring the network for the Ethernet source, destination, VLAN, and GOOSE data payload. Most importantly, the status number and sequence number field within the data payload are noted. This information is used for weaponization in the second stage, to develop an appropriate attack vector to execute the man-in-the-middle cyber attack.

B. Cyber Attack Execution

An attack algorithm is developed to inject spoofed GOOSE frames by using information collected from the first stage. The spoofed GOOSE frames contain a modified data payload that issues a trip signal, i.e., goosepdu. This spoofed data frame also contains modified status and sequence number fields. By injecting this spoofed data in the process bus at a high rate, abnormal operation of protective relays is caused. The algorithm is summarized below.

Algorithm 1: Injection of spoofed GOOSE frames

```
Start;
Monitor network packets for GOOSE;
Get src, dst, VLAN tag, stNum, sqNum and goosepdu;
Set stNum=stNum+50, sqNum=0, n=0;
Modify goosepdu to trip;
while (n!=1000) do
    send packet(src, dest, VLAN, stNum, sqNum,
      goosepdu);
    n=n+1;
end
```

Under normal operating conditions, all GOOSE messages are communicated within a predefined time T. The normal range for T is 5-100 ms. When a substation event occurs, e.g., a trip signal, the update rate of the new GOOSE messages increases to statistically assure that the message is delivered. This event mode time t has a range of 0.5 to 5 ms. Also, the status number is incremented and sequence number is reset. Therefore, to conduct a successful attack the spoofed GOOSE packets containing the abnormal trip signals are maliciously sent at higher rate in comparison to the regular update rate, i.e., $t_{attack} << T$. This can be observed in Fig.3. The IED receiving these spoofed GOOSE frames has no other option than to react, as it contains the correct source MAC address, status, and sequence number. Thus, the subscribing IED is tricked into believing a substation event has taken place. This results in an undesirable protection operation.

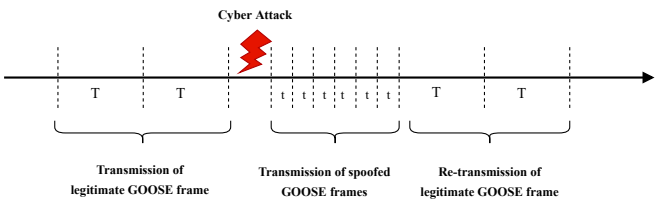


Fig. 3: Attack model to target GOOSE data frames.

If the power grid is in a stressed condition with a high load demand, then an unwanted or unforeseen trip, due to a cyber attack can lead to substation voltages going out of limits, for nominal system operation. In order to restore the system voltages to a normal condition, Under Voltage Load Shedding (UVLS) schemes are implemented. Once the voltage drops below what is an acceptable threshold, e.g., 0.92 p.u, this protection function is activated and results in some loads being disconnected from the grid. Therefore, in theory, the cyber attack on IEDs can result in load shedding. In addition, the power that was flowing in the line disconnected by the cyber attack is rerouted through other lines. This increases the loading on the remaining transmission lines in the system and can result in line overloads. This poses a more serious risk, especially in the case of cable networks, because cables have strict overloading limits. Although, overhead lines are less susceptible to overloads, a sustained overload will create more sag in the conductors. This can lead to a major fault in the line, causing it to trip. This can set off a chain of cascading failures, eventually resulting in a blackout [14], [15].

III. Experimental Framework

The proposed cyber attack model is implemented on an experimental framework for validation. The cyber attack described in this paper compromises GOOSE messages from commercial relays. This results in an unwanted trip of multiple circuit breakers that leads to cascading failures and a blackout in the power grid. The impact on system dynamics is assessed using a Real-Time Digital Simulator (RTDS).

A. HIL Setup

The hardware-in-the-loop setup used to carry out the cyber attack investigations is shown in Fig.4. The physical power system is modelled in real-time using the RTDS platform. The targeted IEDs are highlighted in the figure, i.e., IED 1 and 2. IED 1 is fully IEC 61850 compliant, meaning the relay has the capability for GOOSE messaging and uses Sampled Values (SV) for measurements. IEDs 2 and 3 are partially IEC 61850 compliant. They are hardwired and receive analogue signals from RTDS through power amplifiers. However, they send tripping commands through GOOSE messages. As shown in Fig.4, the relay data links are connected to a network switch which also has a connection to RTDS GTNET 2x card. The card provides the sampled values and acts as a subscribing IED to the GOOSE messages from the relays. The cyber attack on GOOSE messages of IEDs 1 and 2 is conducted via the same network switch connecting all equipment. This network layout is representative of a typical bay level communication network in a digital substation.

B. Implementation Details

The simulated power system on RTDS has a nominal voltage level of 400 kV and frequency of 50 Hz. The biggest load centre is located at bus 4, with a total demand of 1000 MW. The system has three generation units providing 415 MW of the total load of 1500 MW. The excess load is supplied from

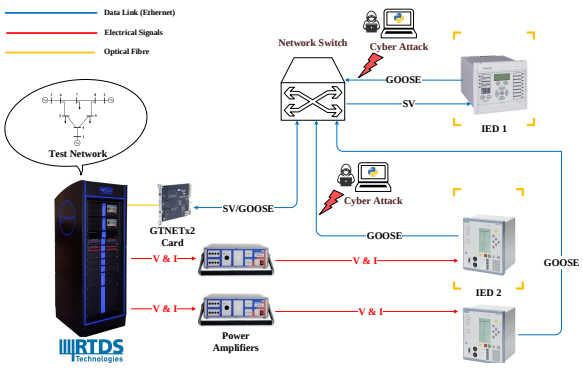


Fig. 4: Hardware-in-the-Loop test setup to analyse real-time impact of cyber attacks.

the grid equivalent at bus 13. The single line diagram of the simulated system is shown in 5. Bus 4 implements an under-voltage load shedding scheme to maintain system stability in case of under-voltages or faults. UVLS is set up according to [16], which sheds load in 5% increments of the total load demand with time delays of 4 to 10 s. In addition to this, transmission line 1-2 employs an overload protection scheme. As stated in [17], the overload protection for overhead lines is a topic for individual dispatch centers. Therefore, different areas may have different practices in applying overload protection on lines. For simplification, the overload protection has been modelled with a threshold of 1.1 p.u of the nominal line current and a time delay of 7 s. In this paper, we use a well-known communication network tool, i.e., Wireshark, to carry out network reconnaissance. The data collected from this stage is used in a python script for weaponization, based on the scapy library [18]. This script executes the cyber attack by injecting spoofed GOOSE frames into the substation communication network. Two cyber attacks are conducted and studied, i.e., single and coordinated man-in-the-middle. The single cyber attack targets only one relay, while the coordinated attack compromises two protective relays.

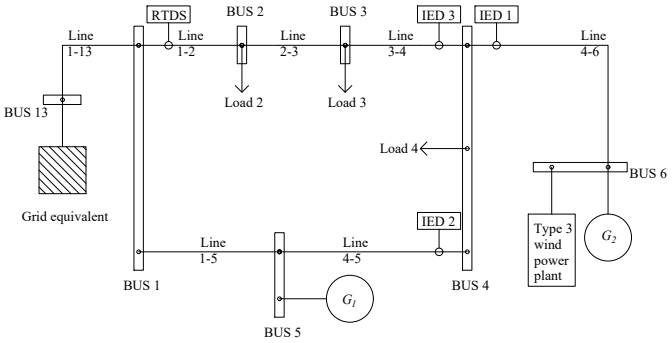


Fig. 5: Single line diagram of modelled power system.

IV. Simulation Results

A. Spoofing of GOOSE data frames

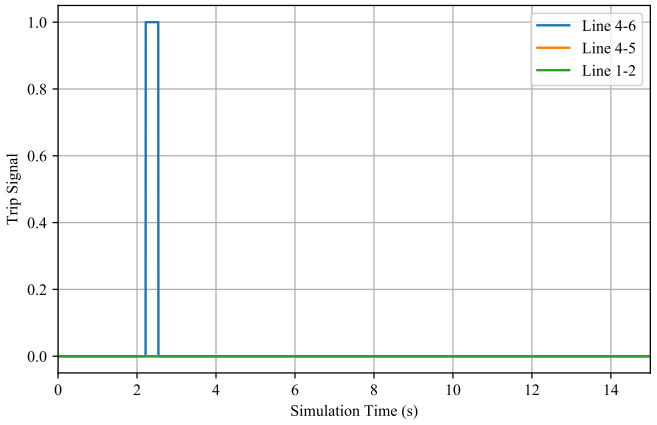
Table I depicts the successful manipulation of GOOSE data frames, that are processed by the subscribing IED. Column 1 shows the legitimate data frames published by the physical IED to the subscriber. The false value of the Boolean field refers to the current trip status of the IED, i.e., keep the circuit breaker closed. After carefully monitoring the network, a stream of spoofed data frames is then injected at a very high rate as described previously. This causes the subscribing IED to act upon them and open the associated circuit breaker contacts. By simply altering one Boolean bit from false to true along with the status and sequence number fields, an attacker can wreak havoc on the physical power grid, as explained subsequently in this section. It is interesting to note, the timestamp of the spoofed data frame is wrong as shown in the table, i.e., March 20, 1994. Yet, the subscribing IED is forced to act upon these false trip signals due to the higher status number field, i.e., stNum is set to 99.

TABLE I: Spoofing of GOOSE data frame.

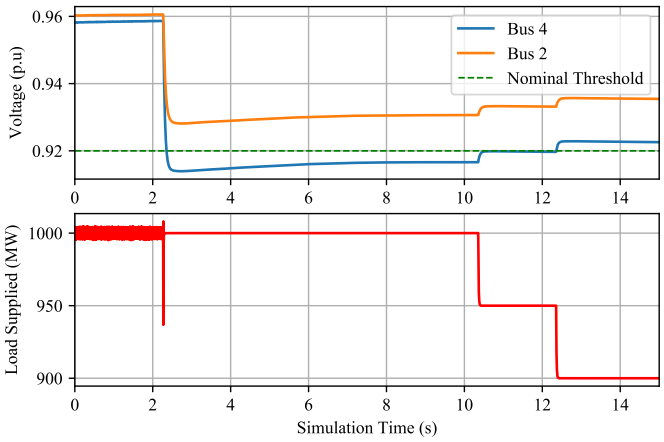
Normal operation GOOSE frame	**Cyber attack: False GOOSE frame**
gocbRef: P446_SVSystem/LLN0GOgcb01	gocbRef: P446_SVSystem/LLN0GOgcb01
timeAllowedtoLive: 2001	timeAllowedtoLive: 5
t: Mar 28, 1994 03:42:25.531999945 UTC	t: Mar 20, 1994 22:04:09.076999962 UTC
stNum: 95	**stNum: 99**
sqNum: 80850	sqNum: 0
numDatSetEntries: 10	numDatSetEntries: 10
allData: 10 items	allData: 10 items
Data: boolean (3)	Data: boolean (3)
boolean: False	**boolean: True**

B. Single Cyber Attack

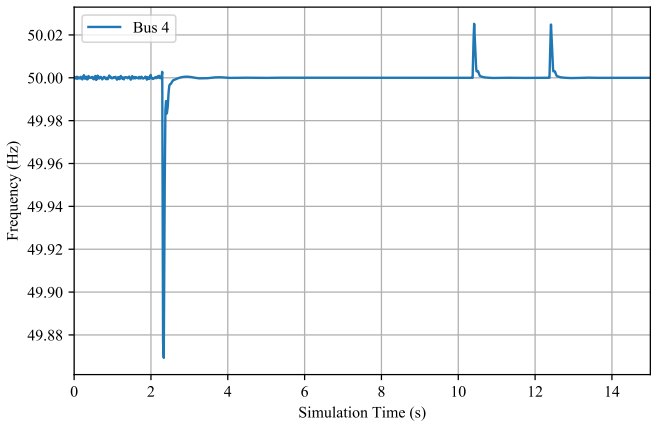
In the first cyber attack, only one IED's tripping command is compromised. This IED is located at bus 4 on transmission line 4-6. The attack results in a spoofed trip signal sent to RTDS by the attacker posing as the publishing IED. Consequently, this causes the circuit breaker contact of line 4-6 to open, as seen in Fig.6a. Due to this line disconnection, about 220 MW of generation is lost. Hence, the voltage at bus 4 drops below the nominal threshold of 0.92 p.u, as shown in Fig.6b. In order to restore the voltage back to acceptable levels, two steps of UVLS are activated. This results in 100 MW of load shed due to the attack as depicted in Fig.6b. When analysing the frequency variation in Fig.6c, it is seen that the frequency of the system drops below 49.88 Hz for a short amount of time. This is due to the disconnection of the wind power plant and one of the synchronous generators, which amount to about 10 % of the total generation of the system. The power deficit is accounted by the external grid. In the later stages, frequency rises by about 20 mHz when each step of load shedding is activated. Overall, the power system remains stable after the cyber attack on a single IED. Hence, in order to cause any sort of major damage to the power grid, a potential attacker needs to know the precise network topology and IEDs to target in the system. As per most national grid codes, it is crucial that the $N-1$ criterion is always satisfied. Thus, compromising only one IED may not adversely affect the power system stability.



(a) Trip signals

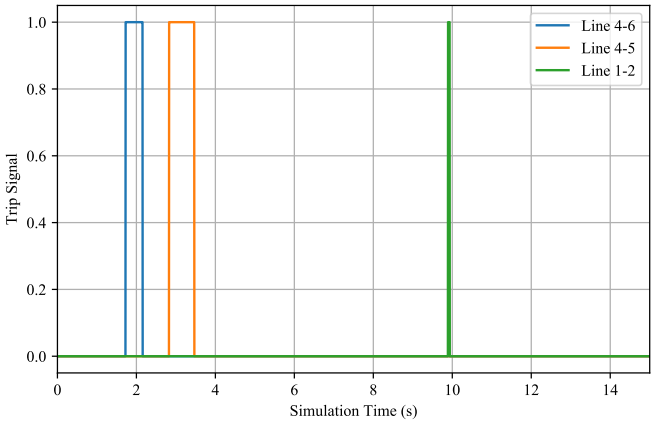


(b) Bus voltage and active power demand met

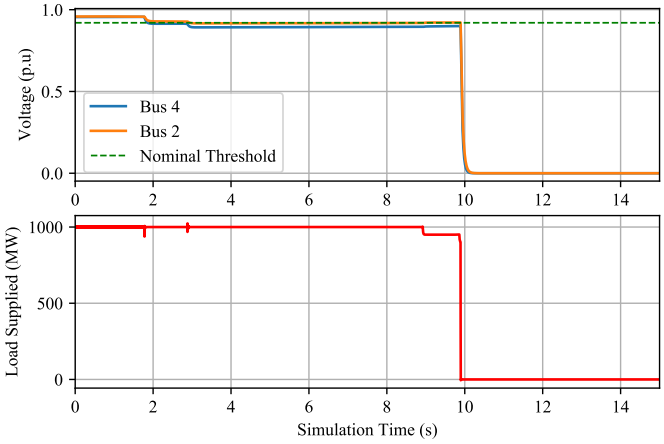


(c) Frequency at Bus 4

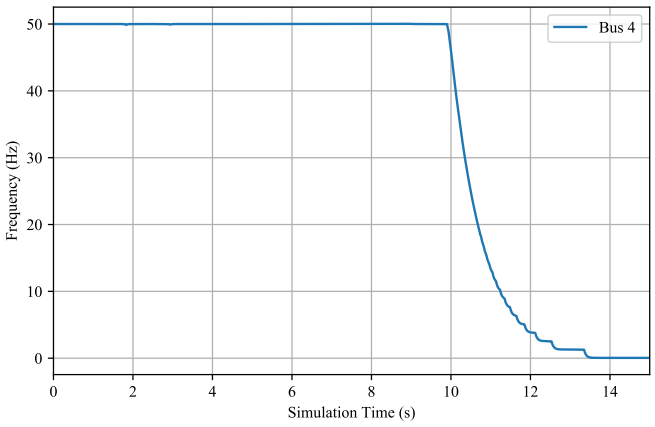
Fig. 6: Impact of cyber attack on one IED.



(a) Trip signals



(b) Bus voltage and active power demand met



(c) Frequency at Bus 4

Fig. 7: Impact of coordinated cyber attack on multiple IEDs.

C. *Coordinated Attack*

The second attack studied in this paper is a coordinated cyber attack that targets two IEDs, i.e., IED 1 and 2. To this end, two tripping signals are compromised that result in two lines being disconnected from bus 4, i.e., 4-5 and 4-6. The tripping signals due to the attack are shown in Fig.7a. The overload protection causes line 1-2 to trip at 10 s simulation

time. The resulting response of the power system to the attack is observed in Fig.7b. Immediately post the cyber attack, the voltage in substation drops below the acceptable nominal threshold of 0.92 p.u. Furthermore, around 8 seconds after the attack, some load is shed in order to restore voltage. However, a few seconds after this, the load supplied, voltage, and frequency drop to zero because of the tripping of line 1-2. Thus, the cyber attack results in a power system blackout.

V. Conclusions and Recommendations

This paper presents the attack model that manipulates GOOSE data in digital substations. Furthermore, it demonstrates the execution and impact of the man-in-the-middle attack, which exploits vulnerabilities in the GOOSE protocol used by protective relays. This causes cascading failures in the power grid resulting in a blackout. One measure to prevent such man-in-the-middle attacks is ensuring the authenticity and integrity of the message using authentication codes at the end of every GOOSE message, as standardized by IEC 62351-6. With this measure, the sending IED is clearly identified and it becomes impossible to manipulate the GOOSE message content. However, the usage of authentication keys for IEDs requires a key management infrastructure inside the digital substation. For this reason, these GOOSE security mechanisms have not yet gained widespread use. In future work, we will focus on the design of intrusion detection and prevention systems and special protection schemes that can mitigate the impact of such cyber attacks and prevent a blackout. With the increasing power grid digitalization and adoption of the IEC 61850 standard, greater attention needs to be paid to cyber security. It is an urgent need of the hour, to ensure the cyber security and resilience of future cyber-physical energy systems.

Acknowledgment

This work is part of the Designing Systems for Informed Resilience Engineering (DeSIRE) program of the 4TU Centre for Resilience Engineering (4TU.RE). DeSIRE is funded by the 4TU-program High Tech for a Sustainable Future (HTSF). 4TU is the federation of the four technical universities in The Netherlands (Delft University of Technology, TUD, Eindhoven University of Technology, TU/e, University of Twente, UT and Wageningen University and Research, WUR).

References

[1] C. C. Liu, A. Stefanov, J. Hong, and P. Panciatici, "Intruders in the grid," *IEEE Power and Energy Magazine*, vol. 10, no. 1, pp. 58–66, Jan 2012.

[2] G. Ericsson, "Cyber Security and Power System Communication," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, pp. 1501–1507, 2010.

[3] H. Zimmermann, "Osi reference model - the iso model of architecture for open systems interconnection," *IEEE Transactions on Communications*, vol. 28, no. 4, pp. 425–432, April 1980.

[4] M. G. Kanabar and T. S. Sidhu, "Performance of iec 61850-9-2 process bus and corrective measure for digital relaying," *IEEE Transactions on Power Delivery*, vol. 26, no. 2, pp. 725–735, April 2011.

[5] J. Hoyos, M. Dehus, and T. X. Brown, "Exploiting the goose protocol: A practical attack on cyber-infrastructure," in *2012 IEEE Globecom Workshops*, Dec 2012, pp. 1508–1513.

[6] M. E. Hariri, T. Youssef, and O. Mohammed, "On the implementation of the iec 61850 standard: Will different manufacturer devices behave similarly under identical conditions?" *Electronics*, vol. 5, no. 4, p. 85, May 2016.

[7] T. A. Youssef, M. E. Hariri, N. Bugay, and O. A. Mohammed, "Iec 61850: Technology standards and cyber-threats," in *2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC)*, June 2016, pp. 1–6.

[8] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," in *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, April 2017, pp. 1–8.

[9] D. U. Case, "Analysis of the cyber attack on the ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, 2016.

[10] A. Stefanov and C. C. Liu, "Cyber-power system security in a smart grid environment," in *2012 IEEE PES Innovative Smart Grid Technologies, ISGT 2012*, 2012.

[11] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the cyber-physical impact of cyber events on the power grid," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2444–2453, 2015.

[12] Junho Hong, Chen-Ching Liu, and M. Govindarasu, "Cyber-physical security in a substation." Institute of Electrical and Electronics Engineers (IEEE), nov 2012, pp. 1–1.

[13] N. Kush, E. Ahmed, M. Branagan, and E. Foo, "Poisoned goose: Exploiting the goose protocol," in *Proceedings of the Twelfth Australasian Information Security Conference - Volume 149*, ser. AISC '14. AUS: Australian Computer Society, Inc., 2014, p. 17–22.

[14] S. Corsi and C. Sabelli, "General blackout in italy sunday september 28, 2003, h. 03:28:00," in *IEEE Power Engineering Society General Meeting, 2004.*, June 2004, pp. 1691–1702.

[15] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, A. Stankovic, C. Taylor, and V. Vittal, "Causes of the 2003 major grid blackouts in north america and europe, and recommended means to improve system dynamic performance," *IEEE Transactions on Power Systems*, vol. 20, no. 4, pp. 1922–1928, Nov 2005.

[16] C. Mozina, "Undervoltage load shedding," in *2007 Power Systems Conference: Advanced Metering, Protection, Control, Communication, and Distributed Resources*, March 2007, pp. 39–54.

[17] ENTSO-E, *Best Protection Practices for HV and EHV AC-Transmission Systems of ENTSO-E Electrical Grids*, 2018.

[18] "Scapy," available online: https://pypi.org/project/scapy/.