Cyber System Recovery for IEC 61850 Substations

Ruoxi Zhu
Student Member, IEEE
Virginia Tech
Blacksburg, VA
ruoxi@vt.edu

Junho Hong
Member, IEEE
University of Michigan-Dearborn
Dearborn, MI
jhwr@umich.edu

Chen-Ching Liu
Life Fellow, IEEE
Virginia Tech
Blacksburg, VA
ccliu@vt.edu

Jiankang Wang
Member, IEEE
The Ohio State University
Columbus, OH
wang.6536@ osu.edu

***Abstract*— When a power system undergoes coordinated cyberattacks, the cascading events could result in a blackout. It is a complex process to restore the system after a cyberattack since both cyber and physical systems need to be restored. Traditionally power system restoration is focused on recovery of the physical power system. To extend the restoration methodology to a power grid as a cyber-physical system, this paper is concerned with the restoration of the cyber system based on detection and isolation of the attacked device and recovery of the functions through collaboration among multiple devices. To this end, at the first stage, the substation automation system (SAS) recovers independently of any untrusted remote control. This paper proposes a new strategy for cyber recovery at an IEC 61850 based SAS following a cyberattack. The compromised components are isolated at the substation Local Area Network (LAN) by dynamic network reconfiguration, which is implemented with the centralized controller of Software Defined Network (SDN). Furthermore, the proposed collaborative Intelligent Electronic Devices (IEDs) are deployed to recover the main functions of the compromised device. A cyber-power system testbed with the SDN controller and commercial grade IEC 61850 code has been developed for implementation and validation of the proposed strategy.**

Keywords—cyber security, substation automation, IED, SDN, cyber system recovery, resiliency

I. INTRODUCTION

With the integration of communication technologies and IEDs, an IEC 61850 based SAS increases the efficiency of power system monitoring, control, and protection. However, the expanded connectivity with a Wide Area Network (WAN) also exposes the system to new attack vectors. Substations are vulnerable targets for the cyber (and physical) attackers since most of them are unstaffed and some are located in remote locations. In fact, the cyberattacks on the Ukraine power grid in 2015 compromised 6 substations through remote access, resulting in large-scale outages for up to six hours [1]. Also, from the detailed survey of physical intrusions into substations in [2], intruders, who physically break into the substation control room, have various options to launch the cyberattacks inside the substation, e.g. connecting a host to substation LAN for accessing IEDs/Supervisory Control And Data Acquisition (SCADA) system or transmitting fabricated control commands to substation equipment by human interface. Those attacks, either from inside or outside the substations, is a powerful reminder of the vulnerabilities of a smart grid with respect to cyber intrusions. Traditionally, power system restoration deals mainly with the physical power system. As a cyber-physical system, however, the restoration of cyber systems must be incorporated to achieve a systematic strategy. The report [1] shows that even after the electrical service was restored, the impacted distribution systems continued to operate in an constrained mode due to cyber security concerns.

This work was supported by National Science Foundation under Grant No. ECCS-1824577 at Virginia Tech, a Collaborative Project with The Ohio State University.

To promptly recover the main functionality of the system operation and control, this paper proposes a new strategy of cyber recovery for IEC 61850 based SASs. As the post-mortem failure analysis for a cyberattack can be time-consuming, it is necessary to recover the main functions of the substation first to maintain critical operations of the power system. On the other hand, until the attack path is fully reconstructed, it is risky to expose the system to remote access. Thus, the proposed strategy relies on local recovery actions within the substation network.

Various studies have been reported on intrusion detection and mitigation at the substation level. The vulnerability assessment of SASs is proposed in [3]. The cyberattack scenarios are discussed in [4] based on the interaction between Information and Communications Technology (ICT) and the physical power system. A network-based Intrusion Detection System (IDS) is proposed using multicast messages in SAS[5]. With IDS integrated with each IED, the collaboration between the IEDs serves to enhance the monitoring and detection of cyberattacks [6, 7]. In the literature, few studies have been reported on power system restoration following outages caused by the cyberattacks. In [8], a complex optimization model is developed for the restoration of interdependent power system and communication system. A self-healing optimization problem is proposed to restore the observability of power system after a cyberattack [9]. Similarly, SHAP-NET platform developed in [10] mitigates the impact of cyberattacks on the PMU network via network reconfiguration. To optimize the reclosing time of Circuit Breakers (CBs) after the attack, a reinforcement learning based strategy is proposed for real-time decision making [11].

Research on mitigation and recovery of the cyber-power system following a cyberattack is in an early stage of development. Indeed, 1) existing research relies on a centralized approach for restoration of the physical grid, which may be manipulated through an unsecured communication network. 2) A systematic methodology is critically needed for fast recovery of the cyber system functions at substations following a cyberattack. This paper provides a new method for the cyber recovery at IEC 61850 based SASs. The main contributions of this paper are:

- Proposing a strategy to recover the main functions of a substation following cyberattacks.

- Developing a local recovery procedure which is solely based on the collaborative devices within the substation network.
- Implementing the proposed method with the cyber-physical testbed. Test results validate the feasibility of the proposed method at an IEC 61850 based SAS.

The remaining of this paper is organized as follows: Section II formulates the potential attack points at the substation; In Section III, the proposed procedure for cyber system recovery is described. Section IV discusses the testbed setup and the simulation results for two realistic scenarios. The conclusion and future work are given in Section V.

II. Problem Formulation

The ICT of substations includes remote functions for SCADA system, which potentially exposes the cyber-power system to cyber intrusions. An intended purpose of a substation cyberattack is to open CBs and trigger a cascaded sequence of events, leading to a blackout. To maliciously manipulate the operation of CB, four potential attack points at the substation level are illustrated in Fig.1. It is noted that the adversary can trigger the attack from inside or outside the substation LAN. Thus, the potential attack paths are classified into two categories as follows.

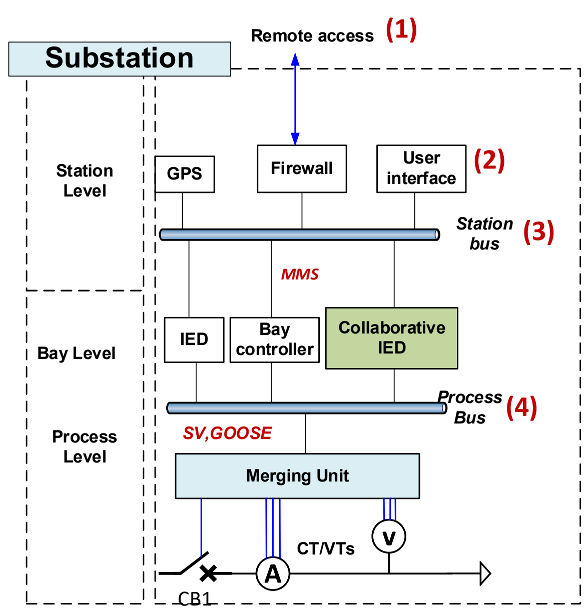


Fig. 1. Potential attack surface at substations

A. From Inside the Subsatation

As shown in Fig.1, from inside the substation, an adversary can intrude into the substation network by unauthorized access at attack points (2), (3) or (4). Once (2), (3) are accessed, the adversary can issue falsified control commands in Manufacturing Message Specification (MMS) messages to open the CBs. When the process bus ((4) in Fig.1) is compromised, the adversary can inject fabricated measurements with Sample Value (SV) packets to trigger a protective relay. Also, with the access of the process bus, the station equipment, e.g., protective IEDs, can be compromised. To open the CBs, the adversary can manipulate relay settings or directly issue malicious GOOSE messages. To disrupt services of the equipment at station/process bus, the adversary can launch a GOOSE/SV based Denial of Service (DoS) attack.

B. From Outside the Substation

If the adversary compromises remote access points, shown with (1) in Fig.1, the attack path leading to CBs will be: (1), (3), (4). For example, the attacker utilizes Virtual Private Network (VPN) as a backdoor to communicate with the Industrial Control System (ICS). Then the attacker accesses the substation from remote through the ICS to launch the attack by issuing malicious commands. Moreover, for the DoS attacks from outside the substation, the adversary can launch TCP syn flooding to shut down the communication link between the substation and SCADA system. As a result, data exchange between the substation and control center will be disrupted.

Using the proposed method, the compromised substation components will be isolated during cyber system recovery. By integrating the security information provided from IDS with the current system configuration, the proposed scheme is able to handle the cyber recovery from various attack types in SAS, such as false data injection, false command injection, replay, and DoS attacks.

III. Methodology for Cyber Recovey

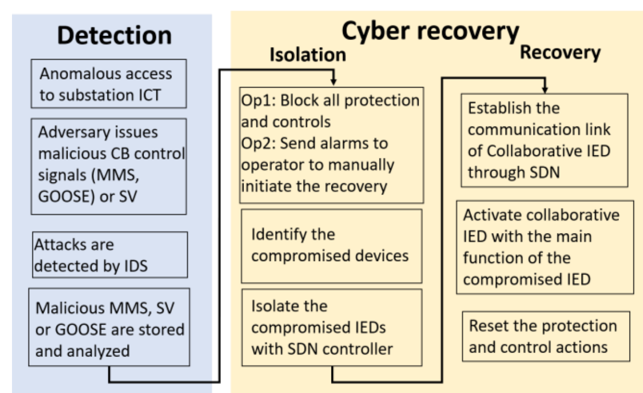


Fig. 2. Methodology of cyber recovery at a substation

In order to secure the digital substations, the concept of a collaborative IDS has been proposed [6, 7]. The author`s prior results in [6] validated the accuracy of the IDS in IEC 61850 based substations. Based on a specification-based detection algorithm, the IDS integrated IEDs parse the data traffic (i.e., MMS, SV and GOOSE) to detect the anomalies without disrupting the main IED functions. With the collaboration among the IEDs, the IDS can detect and mitigate simultaneous intrusions at multiple IEDs. Moreover, the collaborative IDS will save each IED`s security information with time stamps in the database, providing vital information for the procedure of cyber recovery. As shown in Fig. 2, detection of a cyber intrusion at the substation level will trigger the proposed cyber recovery. Following the detection step, the strategy for cyber system recovery is based on isolation and recovery.

A. Isolation

Once an attack is detected, there are two options to initiate the procedure of isolation at substation level.

- Option 1: Protection and control functions of all IEDs are blocked. The collaborative IDS [6] sends the security information within a GOOSE message to the neighboring IEDs so that the IEDs will switch to a blocking mode. By doing so, the subsequent attacks will not be able to interrupt normal operation of the power grid during the process of cyber recovery.

- Option 2: The operator manually initiates the process of recovery. With the attacks successfully detected by the IDS, the alarms and security information are sent to the operator, who will execute the isolation.

The security information generated by the IDS at each IED contains the security violations of the attack. Thus, the attack points at the substation level can be identified. For instance, the GOOSE intrusion detection provides useful information contained in the malicious packets: source/destination MAC address, sequence number, time stamp, etc. The source MAC address is tied to the compromised IED that sends out the fabricated control. Under this scenario, this particular IED will be isolated during the procedure.

To implement the isolation of the compromised components, SDN, with complete network visibility, increases the flexibility of control over the substation network [12]. The control plane that determines the packets forwarding is removed from the switches to the centralized SDN controller. OpenFlow as the common industrial standard is used to program the communication between the flow controller and network appliance (SDN switches). Based on the various attacks discussed in Section II, SDN controller implements the isolation by programming the flow tables of the correlative switches. Table I shows the relation between the security information from the IDS and correlative SDN switches that the compromised IED is connected to.

TABLE I. CORRELATIVE SDN SWITCHES FOR VARIOUS ATTACK SCENARIOS

Attack points	Detected malicious messages	Correlative SDN Switches
Remote Access	MMS, GOOSE	Station bus, process bus, firewall
Inside of subtaion	MMS	Station bus
	GOOSE, SV	Station bus, process bus

- *Attacks from outside of substation:* With the information of malicious MMS and GOOSE packets, the attack path described in Section II is traced. If the MMS is issued from remote access, the IP address of the user, who is falsely authenticated by the firewall, should be blocked. To secure the substation from unsecured remote access, the central controller of SDN will update the flow table of the firewall to block the connection outside of substation LAN. If a DoS attack discussed in Section II is launched from outside the substation, the network based IDS may detect the flooding traffic and filter the traffic through router firewalls[13]. Under the circumstance, the proposed isolation scheme, which is focused on communication inside the substation LAN, will not be triggered.
- *Attacks from inside of substation:* According to the attack points shown in Section II, if the IDS detects anomalies of GOOSE and SV packets, the flow table of the Ethernet switches (process bus and station bus) will be updated through the SDN controller. On the other hand, if the malicious MMS is detected containing the fabricated control from the compromised station IED, the SDN controller will send the flow entry to the Ethernet switch (station bus) to block the related MAC and IP address.

Note that, the performance of the isolation scheme is not affected even if the attacker uses a fabricated IP address or changing IP address frequently. The SDN controller, with full flexibility of control over the network, will block the new malicious IP address as soon as the malicious message is detected.

B. Recovery

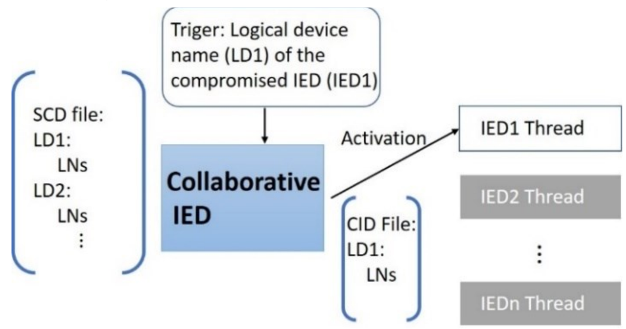


Fig. 3. Configuration of proposed collaborative IED

Based on the isolation of the compromised appliance at the SAS, it is necessary to promptly recover the basic protection actions and controls of the substation before the system is fully restored from the cyberattack. The collaborative IED is developed for the recovery of any type of IEDs present in the substation. Once the compromised IED is isolated, the SDN controller issues the flow entry to redirect the traffic to the collaborative IED. In other words, any packets sent to the compromised IED will be sent out of the Ethernet port connected to collaborative IED.

Meanwhile, the proposed collaborative IED will convert to the same logical device (LD) of the isolated IED and activate its main functions. Based on the design of backup IED for the faulty IED in [14], the configuration of the collaborative IED follows the System Configuration Language (SCL) engineering of IEC 61850 based system. SCL specifies a hierarchy of SCL files, which describe the multi-level of the system with a standardized format [15]. For instance, Substation Configuration Description (SCD) file contains the information of substation configuration, and Configured IED Description (CID) file contains full configuration of the IED.

As shown in Fig. 3, the proposed collaborative IED with SCD file has full information of substation configuration, providing the capability to convert to any type of IEDs. In normal operation, the collaborative IED is in a “waiting” mode acting as a hot standby. It will keep the connection alive to Substation LAN but does not carry out any action. As an IED with Ethernet connection, the collaborative IED is exposed to cyberattacks as well. To prevent the proposed IED from being attacked, network hardening [16] will be initiated once the collaborative IED is in service. This security measure is used to block all communication ports except for the change mode operation (hot-standby to active).

When isolation is triggered, the collaborative IED will be activated by the file with the LD name of the isolated IED. The corresponding thread will be executed by parsing the SCD file with the LD name. As the collaborative IED remains online all the time, it seamlessly takes over the main functions and data mapping information of the compromised IED without interruption. Once the attack is fully cleared, the SDN controller will end the recovery module and reset the network. The compromised components will be restored and the collaborative IED will remove the active threads and reset to the online waiting mode.

IV. Simulation Results

A. Testbed Setup

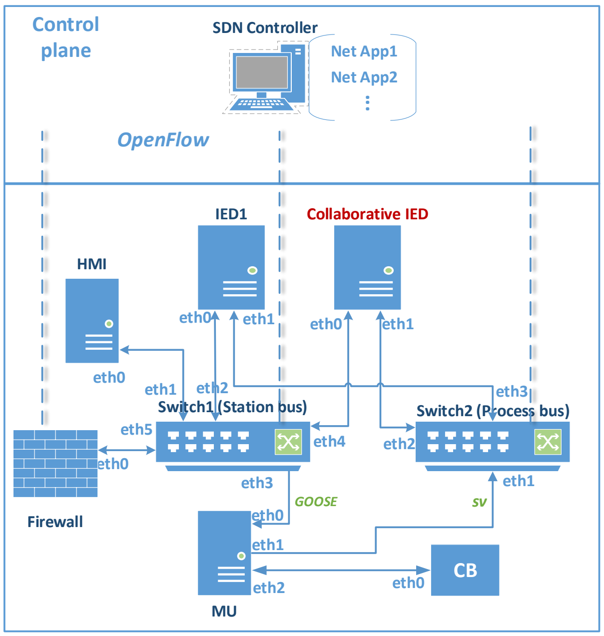


Fig. 4. SDN based substation network

A cyber-physical system testbed representing the IEC 61850 based substation in an SDN environment has been designed and implemented at Virginia Tech. Commercial grade IEC 61850 source code is embedded to generate the IEC 61850 based environment. A real time power system simulator is used for co-simulation of the physical layer. Mininet, as a network emulator, is used for implementation of SDN. To develop the centralized control of SDN, the extension "RECOVERY" is programmed in POX controller which is running on the same host as the remote SDN controller [17]. Simulations are performed on an embedded computer.

The topology of SDN based substation network has been established as shown in Fig. 4. In this simulated SDN based substation network, the controller is connected to two Ethernet switches (station bus and process bus) and one firewall with OpenFlow links. Some devices, such as IED1, collaborative IED, and Merging Unit (MU), have two Ethernet ports that are connected to both switches. Human Machine Interface (HMI) and the firewall are connected to the station bus only. Simulation results are presented for two realistic scenarios as follows.

B. Scenario1: Fabricated GOOSE from IED1

Based on the embedded IDS in the testbed, security information of the malicious GOOSE indicates the source MAC address of IED1. Therefore, the process of cyber recovery is triggered by isolating IED1. First, the SDN controller sends out one new flow entry to the station bus to block the traffic from the source MAC address (00:00:00:00:00:01), which is tied to IED1. Then, the controller issued an OpenFlow command about the flow table modification. The modified flow entry redirects the packets with the destination address of IED1 to the reconfigured collaborative IED as illustrated in Fig. 5. Note that the collaborative IED has subscribed to the Ethernet switch before the recovery starts. By doing so, it seamlessly converts to the isolated IED without interruption.

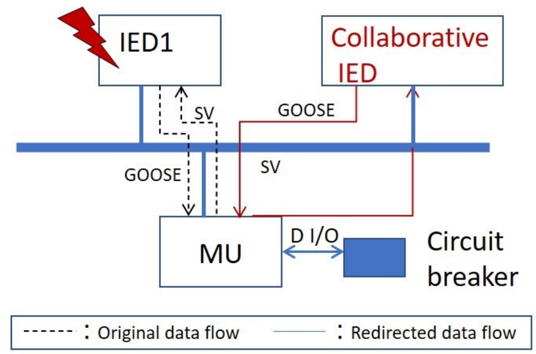
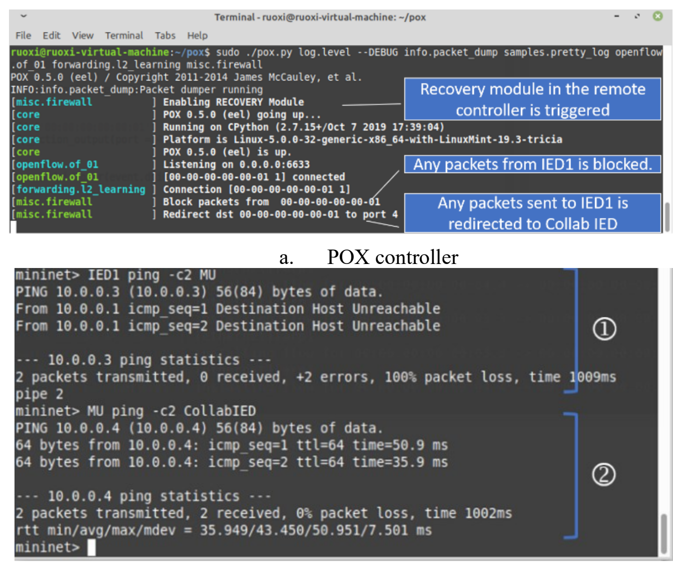


Fig. 5. Isolation of IED1



a. POX controller

b. Mininet console

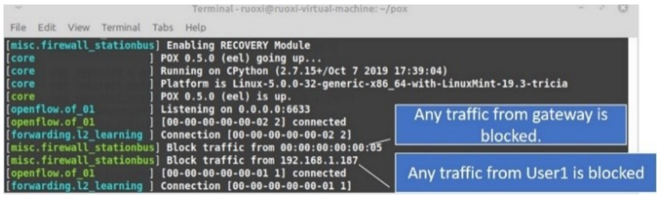
Fig. 6. Simulation results of SDN under Scenario 1

Fig. 6a shows the logs from actions of the controller. After the controller successfully activates the recovery module, the proposed flow entries are issued via OpenFlow link to Switch1 (Station bus). To verify the updated flow table, Fig. 6b shows the results of connectivity between the hosts in Mininet:
①: After isolation of IED1, IED1 is not able to ping Merging Unit (MU), as the packets from IED1 is blocked based on the flow table.

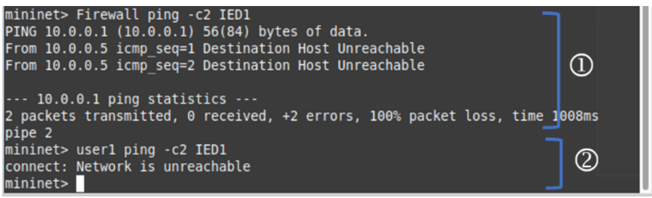
②: With the new entry in the flow table, the connection between MU and collaborative IED is established.

The proposed cyber recovery successfully isolated the compromised IED1 and reconfigured the communication link with the collaborative IED.

C. Scenario2: Attack from remote access



a. POX controller



b. Mininet console under Scenario 2

Fig. 7. Simulation results of SDN under Scenario 2

In this scenario, the attacker remotely accesses the station bus through the firewall and manipulates the LD using MMS communication. The MMS message tampers with the data attribute of the IED, which eventually triggers the GOOSE message with the tripping signal. Therefore, once the IDS detects the malicious GOOSE and corresponding MMS message. The source IP of MMS message indicates if the packet is from remote access or the local HMI. In this scenario, the malicious MMS packets contain source IP address from the remote host. As soon as the process of recovery is triggered, the SDN controller will send a new flow entry to the firewall to block the traffic from the particular source IP. Furthermore, to prevent further intrusions from the remote access point, the incoming traffic from the firewall is blocked during the cyber recovery.

Once the recovery module is activated, the connections between the switches and controller are established. Based on the detection results, the controller sends two OpenFlow messages to the firewall and the switch to isolate the connection tied to the remote access point as shown in Fig. 7a. In this scenario, since the local host of the PC, named User1, sends out the malicious commands to the station bus, the particular IP address of User1 is blocked.

To verify the updated flow table, Fig. 7b shows the results of connectivity of the hosts in Mininet:
①: After isolation of the firewall, it is not able to ping any other host in the network.
②: As the IP address of User1 is blocked by the updated flow entry, User1 cannot reach the substation network anymore.

The proposed recovery process successfully blocks the unauthorized user and isolated the firewall, preventing further attacks through remote access.

V. Conclusion

This paper provides a strategy of cyber system recovery for a substation following cyberattacks. Based on security information provided by the IDS, the proposed method is used to recover the functionality of the substation in two steps: isolation and recovery. The procedure has been validated with attack scenarios using the simulation of SDN based substation network. The test results indicate that the proposed method is promising for integration with the IEC 61850 based SAS. For the future work, the cyber system restoration needs to be expanded to the entire SCADA system. Based on the secured communication between the substations, the restoration process for the cyber system can be deployed in a distributed manner.

References

[1] D. U. Case, "Analysis of The Cyber Attack on the Ukrainian Power Grid," *Electricity Information Sharing and Analysis Center (E-ISAC),* vol. 388, 2016.

[2] J. Xie, C. C. Liu, M. Sforna, M. Bilek, and R. Hamza, "On-Line Physical Security Monitoring of Power Substations," *International Transactions on Electrical Energy Systems,* vol. 26, no. 6, pp. 1148-1170, 2016.

[3] G. Hug and J. A. Giampapa, "Vulnerability Assessment of AC State Estimation With Respect to False Data Injection Cyber-Attacks," *IEEE Transactions on Smart Grid,* vol. 3, no. 3, pp. 1362-1370, 2012, doi: 10.1109/TSG.2012.2195338.

[4] A. Stefanov and C. Liu, "Cyber-Power System Security in a Smart Grid Environment," in *2012 IEEE PES Innovative Smart Grid Technologies (ISGT)*, 16-20 Jan. 2012 2012, pp. 1-3, doi: 10.1109/ISGT.2012.6175560.

[5] J. Hong, C. C. Liu, and M. Govindarasu, "Detection of Cyber Intrusions Using Network-Based Multicast Messages for Substation Automation," in *2014 IEEE PES Innovative Smart Grid Technologies (ISGT)*, 19-22 Feb. 2014 2014, pp. 1-5, doi: 10.1109/ISGT.2014.6816375.

[6] J. Hong and C. C. Liu, "Intelligent Electronic Devices With Collaborative Intrusion Detection Systems," *IEEE Transactions on Smart Grid,* vol. 10, no. 1, pp. 271-281, 2019, doi: 10.1109/tsg.2017.2737826.

[7] J. Hong, R. F. Nuqui, A. Kondabathini, D. Ishchenko, and A. Martin, "Cyber Attack Resilient Distance Protection and Circuit Breaker Control for Digital Substations," *IEEE Transactions on Industrial Informatics,* vol. 15, no. 7, pp. 4332-4341, 2019, doi: 10.1109/tii.2018.2884728.

[8] P. M. Baidya and W. Sun, "Effective Restoration Strategies of Interdependent Power System and Communication Network," *The Journal of Engineering,* vol. 2017, no. 13, pp. 1760-1764, 2017, doi: 10.1049/joe.2017.0634.

[9] H. Lin, C. Chen, and J. Wang, "Self-Healing Attack-Resilient PMU Network for Power System Operation," *IEEE Transactions on Smart Grid,* vol. 9, no. 3, pp. 1551-1565, 2018, doi: 10.1109/TSG.2016.2593021.

[10] V. K. Singh, E. Vaughan, and J. Rivera, "SHARP-Net: Platform for Self-Healing and Attack Resilient PMU Networks," in *2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 17-20 Feb. 2020 2020, pp. 1-5, doi: 10.1109/ISGT45199.2020.9087796.

[11] F. Wei, Z. Wan, and H. He, "Cyber-Attack Recovery Strategy for Smart Grid Based on Deep Reinforcement Learning," *IEEE Transactions on Smart Grid,* vol. 11, no. 3, pp. 2476-2486, 2020.

[12] B. Genge and P. Haller, "A Hierarchical Control Plane for Software-Defined Networks-Based Industrial Control Systems," in *2016 IFIP Networking Conference (IFIP Networking) and Workshops*, 2016: IEEE, pp. 73-81.

[13] R. Deal, *Cisco Router Firewall Security*. Cisco Press, 2004.

[14] I. Lim and T. S. Sidhu, "Design of a Backup IED for IEC 61850-Based Substation," *IEEE Transactions on Power Delivery,* vol. 28, no. 4, pp. 2048-2055, 2013, doi: 10.1109/TPWRD.2013.2258686.

[15] Communication networks and systems in substations - Part 6: Configuration description language for communication in electrical substations related to IEDs, IEC 61850-6, IEC.

[16] S. Noel, J. Sushil, B. O. Berry, and M. Jacobs, "Efficient Minimum-Cost Network Hardening via Exploit Dependency Graphs," in *19th Annual Computer Security Applications Conference, 2003. Proceedings.*, 8-12 Dec. 2003 2003, pp. 86-95, doi: 10.1109/CSAC.2003.1254313.

[17] S. Kaur, J. Singh, and N. S. Ghumman, "Network Programmability Using POX Controller," in *International Conference on Communication, Computing & Systems (ICCCN'2014)*, 2014, pp. 134-138.