Intrusion Detection and Recovery of a Cyber-Power System

Ruoxi Zhu

Dissertation submitted to the Faculty of
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
in
Electrical Engineering

Chen-Ching Liu, Chair
Jiankang Wang
Vassilis Kekatos
Jin-Hee Cho
Paul K. Ampadu

April 12, 2024
Blacksburg, Virginia

Keywords: Intrusion Detection, Intrusion Mitigation, Cyber Resilience, Cyber-Physical System, Cyber System Recovery, SCADA, DNP3, Digital Substations, IEC 61850

Intrusion Detection and Recovery of a Cyber-Power System

Ruoxi Zhu

(ABSTRACT)

The advent of Information and Communications Technology (ICT) in power systems has revolutionized the monitoring, operation, and control mechanisms through advanced control and communication functions. However, this integration significantly elevates the vulnerability of modern power systems to cyber intrusions, posing severe risks to the integrity and reliability of the power grid. This dissertation presents the results of a comprehensive study into the detection of cyber intrusions and restoration of cyber-power systems post-attack with a focus on IEC 61850 based substations and recovery methodologies in the cyber-physical system framework.

The first step of this study is to develop a novel Intrusion Detection System (IDS) specifically designed for deployment in automated substations. The proposed IDS effectively identifies falsified measurements within Manufacturing Messaging Specification (MMS) messages by verifying the consistency of electric circuit laws. This distributed approach helps avoid the transfer of contaminated measurements from substations to the control center, ensuring the integrity of SCADA systems. Utilizing a cyber-physical system testbed and the IEEE 39-bus test system, the IDS demonstrates high detection accuracy and validates its efficacy in real-time operational environments.

Building upon the intrusion detection methodology, this dissertation advances into cyber system recovery strategies, which are designed to meet the challenges of restoring a power grid as a cyber-physical system following catastrophic cyberattacks. A novel restoration strategy is proposed, emphasizing the self-recovery of a substation automation system (SAS) within the substation through dynamic network reconfiguration and collaborative efforts among Intelligent Electronic Devices (IEDs). This strategy, validated through a cyber-power system testbed incorporating SDN technology and IEC 61850 protocol, highlights the critical role of cyber recovery in maintaining grid resilience.

Further, this research extends its methodology to include a cyber-physical system restoration strategy that integrates an optimization-based multi-system restoration approach with cyber-power system simulation for constraint checking. This innovative strategy developed and validated using

an Software Defined Networking (SDN) network for the IEEE 39-bus system, demonstrates the capability to efficiently restore the cyber-power system and maximize restoration capability following a large-scale cyberattack.

Overall, this dissertation makes original contributions to the field of power system security by developing and validating effective mechanisms for the detection of and recovery from cyber intrusions in the cyber-power system. Here are the main contributions of this dissertation:

1) This work develops a distributed IDS, specifically designed for the substation automation environment, capable of pinpointing the targets of cyberattacks, including sophisticated attacks involving multiple substations. The effectiveness of this IDS in a real-time operational context is validated to demonstrate its efficiency and potential for widespread deployment.

2) A novel recovery strategy is proposed to restore the critical functions of substations following cyberattacks. This strategy emphasizes local recovery procedures that leverage the collaboration of devices within the substation network, circumventing the need for external control during the initial recovery phase. The implementation and validation of this method through a cyber-physical system testbed—specifically, within an IEC 61850 based Substation Automation System (SAS)—underscores its practicality and effectiveness in real-world scenarios.

3) The dissertation results in a new co-restoration strategy that integrates mixed integer linear programming to sequentially optimize the restoration of generators, power components, and communication nodes. This approach ensures optimal restoration decisions within a limited time horizon, enhancing the recovery capabilities of the cyber-power system. The application of an SDN based network simulator facilitates accurate modeling of cyber-power system interactions, including communication constraints and dynamic restoration scenarios. The strategy's adaptability is further improved by real-time assessment of the feasibility of the restoration sequence incorporating power flow and communication network constraints to ensure an effective recovery process.

Intrusion Detection and Recovery of a Cyber-Power System

Ruoxi Zhu

(GENERAL AUDIENCE ABSTRACT)

Electricity is a critical service that supports the society and economy. Today, electric power systems are becoming smarter, using advanced Information and Communications Technology to manage and distribute electricity more efficiently. This new technology creates a smart grid, a network that not only delivers power but also uses computers and other tools to remotely monitor electricity flows and address any issues that may arise. However, these smart systems with high connectivity utilizing information and communication systems can be vulnerable to cyberattacks, which could disrupt the electricity supply.

To protect against these threats, this study is focused on creating systems that can detect when an abnormal condition is taking place in the cyber-power grid. These detection systems are designed to detect and identify signs of cyberattacks at key points in the power network, particularly at substations, which play a vital role in the delivery of electricity. Substations control the power grid operating conditions to make sure that electricity service is reliable and efficient for the consumers Just like traffic lights help manage the flow of vehicles, substations manage the flow of electricity to make sure electric energy is delivered to where it needed.

Once a cyberattack is detected, the next step is to stop the attack and mitigate the impact it may have made to ensure that the power grid returns to normal operations as quickly as possible. This dissertation is concerned with the development and validation of analytical and computational methods to quickly identify the cyberattacks and prevent the disruptions to the electricity service. Also, the focus of this work is also on a coordinated recovery of both the cyber system (digital controls and monitoring) and power system (physical infrastructure including transformers and transmission and distribution lines). This co-restoration approach is key to sustain the critical

electricity service and ensures that the grid is resilient against the cyber threats. By developing strategies that address both the cyber and physical aspects, the proposed methodology aims to minimize downtime and reduce the impact of large-scale cyberattacks on the electrical infrastructure. The impact of the results of this dissertation is the enhancement of security and resilience of the electric energy supply in an era where the risks of cyber threats are increasingly significantly.

Overall, by developing new methodologies to detect and respond to cyberattacks, the cyber-power system's capability to withstand and recover from cyberattacks is enhanced in the increasingly technology-dependent power grid environment.

Dedication

To my parents and to my husband, who saved me from myself

Acknowledgments

First and foremost, I extend my deepest gratitude to my academic advisor, Dr. Chen-Ching Liu, for his invaluable guidance, unwavering support, and profound wisdom throughout the duration of my Ph.D. journey. Dr. Liu's expertise in the field and his keen insights have not only shaped this research but have also profoundly influenced my growth as a person. I am truly honored to have had the opportunity to work under his mentorship, and I am immensely thankful for his contributions to my professional and personal development.

In addition, I would also like to express my sincere appreciation to the members of my dissertation committee: Dr. Jiankang Wang, Dr. Vassilis Kekatos, Dr. Jin-Hee Cho, and Dr. Paul Ampadu, for their invaluable feedback and insightful comments on my work. Each member has contributed uniquely to my research and personal development: Dr. Jiankang Wang's meticulousness and profound knowledge in the field have significantly enhanced the quality of my research; Dr. Vassilis Kekatos' expertise in optimization and systems analysis has been instrumental in shaping the analytical aspects of my dissertation; Dr. Jin-Hee Cho's vast experience in cyber-security has enriched my work with cutting-edge perspectives and methodologies; and Dr. Paul Ampadu's wisdom and encouragement have been vital in overcoming the challenges encountered during my studies.

My journey would not have been the same without the friendship and intellectual supportfrom my lab mates. To Jenny Appiah-Kubi, Nitasha Sahani, Lung-An Lee, Chensen Qi, Juan Carlos Bedoya, and Akshay Jain, your collaboration and endless discussions have been a source of motivation and inspiration. I am equally grateful to my colleagues at the Power and Energy Center, Manish Singh,

Mana Jalali, and Suchishmita Biswas, for creating an environment of enthusiasm. Your willingness to share knowledge and insights has enriched my academic experience. The pleasant and supportive atmosphere we shared has been instrumental in fostering my development as a researcher. Special thanks are extended to Victoria Deal, Lisa Burns, and Laura Villada Esquivel from the ECE administrative and support staff. The guidance and support provided by each of you have helpful in overcoming the administrative and logistical hurdles.

No word can fully express the gratitude I owe to my parents, Qin Zhang and Kuanjiang Zhu, for their unconditional love, unwavering support, and the sacrifice they have made to see me reach this point in my life. Their belief in my potential and their encouragement to pursue my passion have been the guidepost of my journey. To my husband, Le Chen, whose love, patience, and endless support have been my sanctuary. Your understanding and companionship have been my source of strength and joy throughout this challenging and rewarding journey. Thank you for being my rock. And to Marble, my faithful dog, who has provided unconditional love and countless moments of relief and happiness are a relief from the stress during the pandemic. Your joyful greetings and companionship have been a constant reminder of the simple pleasures in life.

Finally, I would like to acknowledge the financial support I have received: National Science Foundation (NSF under Grant No. ECCS-1824577 and No. CPS 1837359), Department of Energy, Commonwealth Cyber Initiative, the Bradley Department of Electrical and Computer Engineering, and Power and Energy Center.

Publications from this Dissertation

Journal Papers

[1] **R. Zhu**, C. -C. Liu, J. Hong and J. Wang, "Intrusion Detection Against MMS-Based Measurement Attacks at Digital Substations," in *IEEE Access*, vol. 9, pp. 1240-1249, 2021, doi: 10.1109/ACCESS.2020.3047341.

[2] N. Sahani, **R. Zhu**, J.-H. Cho, and C.-C. Liu, "Machine Learning-Based Intrusion Detection for Smart Grid Computing: A survey," *ACM Transactions on Cyber-Physical Systems*, vol. 7, no. 2, pp. 1-31, 2023.

[3] R. Zhu, C.-C. Liu, and j. Hong, "Cyber-Power System Restoration Planning under Large-scale Cyberattacks," To be submitted for publication.

Conference Papers

[1] C.-C. Sun, **R. Zhu**, and C. -C. Liu, "Cyber Attack and Defense for Smart Inverters in a Distribution System," in *CIGRE Study Committee D2 Colloquium, Helsinki, Finland*, 2019.

[2] **R. Zhu**, J. Hong, C.-C. Liu, and J. Wang, "Cyber System Recovery for IEC 61850 Substations," in *2021 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2021: IEEE, pp. 1-5.

Book

[1] C. -C. Liu, J. C. Bedoya, N. Sahani, A. Stefanov, J. Appiah-Kubi, C.-C. Sun, J. Y. Lee and **R. Zhu** (2021), "Cyber–Physical System Security of Distribution Systems", *Foundations and Trends® in Electric Energy Systems:* Vol. 4: No. 4, pp 346-410. http://dx.doi.org/10.1561/3100000026

Contents

List of Figures

List of Tables

Chapter 1

Introduction

An interconnected network, known as an electrical grid, comprising of substations, transformers, and transmission lines ensures the delivery of electricity from power plants to consumers including residential, industrial, or commercial load. However, as the need for centralized control and management increases along with communications between electric utility and consumers, the previously isolated power grid is connected through the (proprietary) computer and communication network. Additionally, digital technology also has sensors in the transmission lines with control capabilities. This control and automation capability in the power grid is known as the `smart grid' as it responds to rapidly changing electrical demand and reacts in a timely manner to any adverse deviations from regular operating conditions due to faults, attacks, or intrusions. A smart grid is intended to ensure system reliability, power availability, and electric energy efficiency during physical or network disturbances by integrating the physical power system with the cyber system.

Information and communications technology (ICT) in a smart grid leads to high connectivity for the power system infrastructure. The cyber system and power system together form a comprehensive cyber-physical system. However, the conventional communication infrastructure in power systems suffers from limited bandwidth and high latency, failing to meet the demands of future advanced applications. Additionally, ensuring security becomes crucial, especially with the increasing integration of third-party Distributed Energy Resources (DERs). This dissertation aims to enhance the cyber resilience of power transmission systems by addressing the constraints of the current communication infrastructure.

1.1 Motivation

An Intrusion Detection System (IDS) is a network security solution to monitor the data traffic flow, detect suspicious activities or threats in the system, identify a specific type of unauthorized

access or malicious intent, and raise a flag to notify an operator to block such security breaches. Two different IDS approaches to detect malicious activities are: an anomaly-based IDS in which a normal behavior is the base, and any deviation is considered a threat to detect unknown attacks, whereas a signature-based IDS compares the traffic flow with already determined attack patterns and any match raises an issue of system threat. An IDS screens a known attack's signatures or any variation from normal behavior to spot system attacks by evaluating the malicious data at the protocol and application layer. Depending on the placement of an IDS in the system, it can be host-based (i.e., software applications installed on individual client computers) or network-based (i.e., placed in the network at multiple points as hardware sensors or as installed system software connected to a network analyzing data packet flow) [1].

Smart grid network architecture includes Home Area Network (HAN), Neighborhood Area Network (NAN), and Wide Area Network (WAN). The HAN and NAN involve the metering structure, smart meters, and data concentrators, whereas the WAN involves applications like Supervisory Control and Data Acquisition (SCADA) [2]. As this arrangement involves the inter-dependency of communication technology at different network levels, the system becomes more susceptible to internal and/or external attacks. As efficient IDS deployment needs the understanding of the environment, for smart grid environments, the functional considerations need to be taken into account [3].

Conventional IDSs fall short in addressing the dynamic nature of the data flow in a smart grid which compromises the resiliency and reliability and limits the scalability of the system. An IDS in the smart grid should be scalable and adaptive to the changing network topology. In addition, it should support legacy protocols with confidentiality, integrity, availability, non-repudiation, and authentication as security goals. Further, the IDS also support hardware resource constraints and associated maintenance cycles in the system. Additionally, the IDS needs to address real-time dynamic traffic patterns with a deterministic approach. This can allow the smart grid's mission-critical nature to be ensured with a highly resilient and reliable IDS in the system.

The challenges of IDS deployment in the smart grid as compared to other environments are prevalent in terms of system security and its associated economic repercussions upon the systems being attacked or failed. Along with power system network security constraints, the sensor

networks, and the complex communication process between the utility and the consumers in the smart grid should ensure smooth and reliable power transfer and usage data. However, as the sensor network is part of the system, security challenges related to data integrity, availability, and connectivity are at stake. Furthermore, in terms of the hardware aspect of the system, the failure to detect such intrusions in the system can introduce a physical impact on the power system in terms of a major blackout, loss of control, or system collapse. As traditional IDSs are not capable of handling dynamic data flow, this dissertation is intended to detect cyber intrusions at the substation level in terms of specific protocols. Also, accordingly, the solutions to cyberattack recovery and restoration are also introduced.

1.2 Objectives and Contributions

As the potential risk of large scale cyberattacks targeting power system, the intrusion detection and recovery of cyber-power systems has become increasingly important. The contributions of this dissertation are as follows: (1) a comprehensive survey of the state of the art is introduced. The survey presents the security vulnerabilities of power transmission systems, general attack types for WAMS and digital substations, and the intrusion detection techniques and the existing cyberattack recovery approaches for power systems. With the survey, researchers will have an overall understanding of the intrusion detection and recovery of cyber-power systems. (2) In terms of measurement-based attacks at substations, an intrusion detection and mitigation method is proposed. (3) A fast recovery strategy for digital substation is proposed based SDN based technology. (4) In order to restore the cyber-power system against severe cyberattacks, a co-restoration strategy is introduced, and (5) A SDN based cyber-physical system simulation environment has been developed to test the performance of the proposed detection and recovery strategies against large scale cyberattacks.

1.3 Organization of the Dissertation

The remainder of the dissertation is organized as follows. Chapter 2 presents the survey of the state of the art of intrusion detection and recovery for cyber-power system. Chapter 3 introduces the solution for intrusion detection and mitigation against measurement-based attacks at substations.

Correspondingly, the cyber system recovery at digital substation is introduced at Chapter 4. In Chapter 5, the cyber-power system restoration strategy is introduced. Finally, the dissertation is concluded in Chapter 6 and the future work is also presented.

Chapter 2

Intrusion Detection and Recovery for Cyber-power system: A Survey

As complex cyber-physical systems, modern power grids utilize layers of ICT to maintain system reliability and efficiency. The fast-increasing connectivity through industrial control systems is known to be a source of vulnerabilities that can be exploited for potential cyber intrusions. With the integration of communication technologies and the 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 unmanned 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. This attack is a powerful reminder of the vulnerabilities of a smart grid with respect to cyber intrusions.

As this dissertation is focused on power transmission systems shown in Fig. 2.1, especially on substation level, the following survey will be mainly discussed on the state of the art of intrusion detection and recovery on transmission systems.

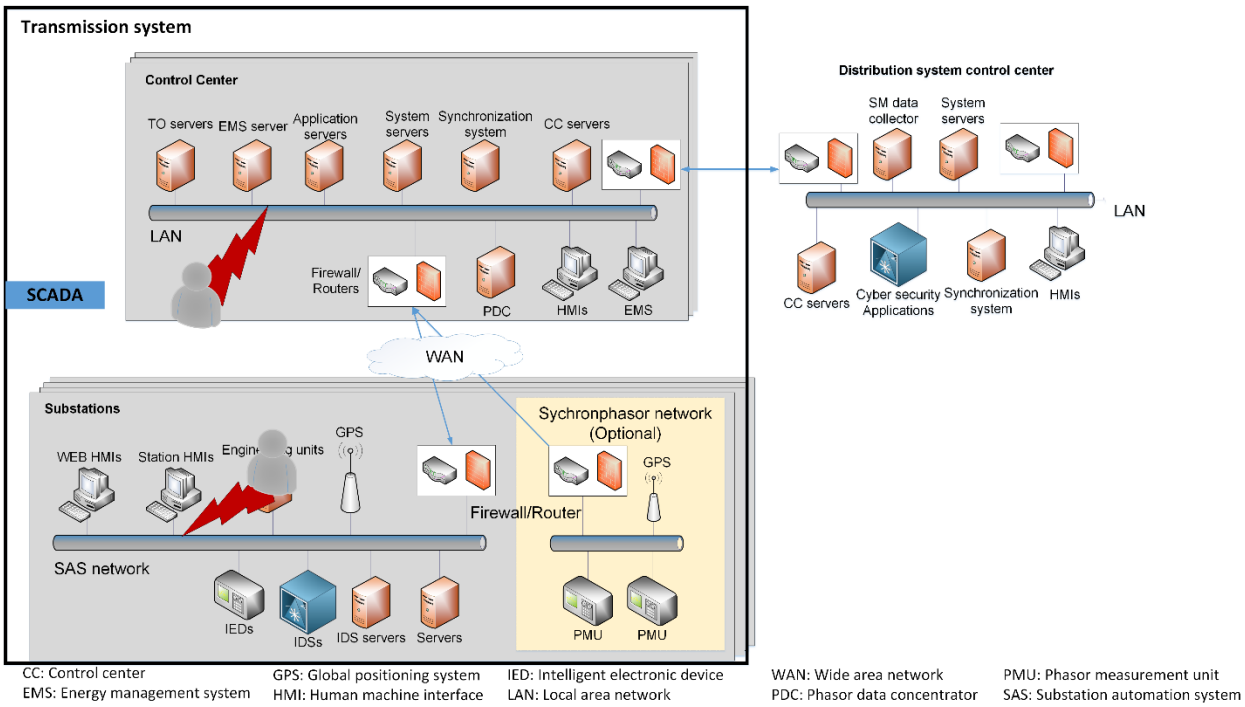


Figure 2.1 Cyber system of power transmission systems

2.1 Security Vulnerabilities in Power Transmission Systems

2.1.1 Security Vulnerabilities in Wide-Area Measurement Systems (WAMS)

WAMS leverage the high-speed wide area networks to poll power system measurements from field sensors. In this paper, we generalize the WAMS into two systems, synchrophasor systems, and traditional SCADA systems. As a conventional Industrial Control System (ICS) used in a power system, SCADA collects measurement data from Remote Terminal Units (RTU) or Intelligent Electronic Devices (IEDs) in substations and transmits the controlled or monitored data from the control center back to the grid. WAN can implement Distributed Network Protocol 3 (DNP3) [4] and Modbus [5] which are the specialized protocols for communications between the substations and control center in a SCADA system. Compared with the SCADA system, synchrophasor data are generated by physical devices, such as Phasor Measurement Units (PMU).

As the control and monitoring functions of SCADA and synchrophasor networks highly rely on cyber infrastructure, cybersecurity concerns within communication networks can negatively impact the normal operations of a power system. WAMS has the following security vulnerabilities:

- The existing SCADA in the power system still uses standardized technologies and protocols which expose vulnerabilities to attackers as they might have knowledge of the loophole of those technologies.

- A few companies developed an Energy Management System (EMS) integrated with WAMS. The widespread availability of technical information provides useful information to cyber adversaries to intrude into the WAMS based on known vulnerabilities.

- Due to a lack of security mechanisms embedded in the communication networks of WAMS, the data exchange can be highly vulnerable to False Data Injection (FDI) attacks.

2.1.2 Security Vulnerabilities in Substation Automation Systems (SAS)

A SAS provides protection, control, automation, monitoring, and communication capabilities as part of a comprehensive substation control and monitoring solution [6]. To take advantage of modern ICT, IEC 61850 is developed as a new global standard for substation automation. Even though IEC 62351 standard provides guidance on security measures for IEC 61850-based SAS, the deployment of security measures in the substation Local Area Network(LAN) is still in development. Therefore, it is critical to develop IDS that achieves the QoS requirements of cyber infrastructure in power systems.

The modern substations have the following security vulnerabilities:

- The protection and control functions at digital substations heavily depend on the Ethernet-based communication within a substation LAN. Once any device within the substation is under attack, the basic functions at the substation level can be manipulated.

- Most IEDs deployed at a SAS are from third-party vendors. The adversary may leverage the loophole of the firmware of the IEDs to launch the attacks which can make the IEDs malfunction.

- As some cyber infrastructures at the SAS has TCP/IP interface, they can be vulnerable to various network attacks, such as DoS or MITM attacks.
- Cybersecurity mechanisms are rarely considered when protocols, such as IEC 61850, DNP3, and Modbus, are developed. Even though some authentication mechanisms are proposed in IEC 62351 or DNP3-SA, their weaknesses are well known as discussed in [7, 8]. Therefore, the plain text traffic (e.g., Generic Object-Oriented Substation Event (GOOSE) or Sampled Values (SV)) can be easily modified by unauthorized access.

2.2 Cyberattacks in Power Transmission Systems

The following attacks have been researched in power transmission system:

1) Denial of service (DoS)

The DoS attack makes the system inaccessible for the authorized users due to the disruption created by an attacker by flooding requests or information traffic in the targeted host/network, preventing legitimate access and connection disruption [9-16].

SYN flood: An attacker may use an incomplete request of three-way handshake methods in a TCP/IP network to make the ports unavailable for additional requests. It saturates all ports by sending continuous incomplete requests to restrict legitimate client/server connections [17, 18].

Buffer overflow: An attacker may flood a network with more traffics than the capacity the network address is designed to handle[19].

Crash attack: This attack is less known where an attacker transmits bugs to exploit system vulnerabilities [20].

SYN flood and buffer overflow attacks are most commonly simulated in smart grid applications. These attacks can restrict the actual measurement packets to come through a control center to take further control actions. Additionally, a lack of timely delivery of power system measurements to the operator at the control center can have a tangible impact on the power grid like system failure, protective relay malfunction, and reduction in system observability.

2) False information attack

In the SCADA network, tampered, modified or false information can be injected into the system to compromise normal operations. This false information can be data that includes measurements of different system variables or commands from the control centers. The control centers can be compromised to jeopardize the line of preventive and protective actions for the system.

False data injection: An attacker can inject bad data which compromises measurements in the SCADA network from different base level grid sensors, such that undetected errors further contribute to faulty state variable estimations, such as bus voltage and line current measures. Furthermore, erroneous data injection in power system measurements can lead to faulty control command dispatch that causes grid-network states to fluctuate [21-31].

False command injection: False command injection attack executes random commands on the host system through a vulnerable application due to the lack of proper validation of the input commands. In smart grid and SCADA applications, false control command injection in the control center can have physical system impact, resulting in widespread outages or cascading failures [9, 15, 23, 24, 30-33].

3) Scanning attack

The scanning attacks (Port scanning, network scanning, etc.) are the most common attacks that the attackers use to discover the services that they can exploit to intrude into systems. To launch the port scan, the attackers will discover all the active ports of the system. Then by sending packets through the ports, the response will contain the information of the running services and potential vulnerabilities [27, 34-36].

4) Reconnaissance attack

In computer security, reconnaissance is a type of computer attack that the adversary intrude into the targeted system by using Trojan, phishing emails, etc. The purpose of the attack usually is to collect the information on the affected system before launching the harmful attacks to the target. The cyberattacks targeting Ukraine power grid are using this attack technique as the first step of the attack vector. With the results of reconnaissance, the attackers managed to navigate to the control workstation of the SCADA system [37, 38].

5) Man-in-the-middle attacks

Man-in-the-middle is a type of attack in which an intruder places itself in a communication channel between two or more systems as a relay or proxy. It being an eavesdropper exploits the real-time data exchange, noticing the network vulnerabilities and can also tap into the channel for sending modified data or commands [37]. There can be different types of man-in-the-middle attacks that are common in smart grid environments which are discussed below:

ARP (Address Resolution Protocol) spoofing: The attackers exploit the vulnerability of ARP by sending the ARP request to resolve the MAC address from the network layer to the data-link layer without any authentication strategy. ARP spoofing is a technique that an attacker sends the fake ARP reply to associate the malicious MAC address with the IP address of another host [35].

Replay attack: This is a network attack where the intruder intercepts the data and re-transmits it over and over to create disruption. In the replay attack, the adversary gets hold of valid data transmission done by an authorized user before and then sends it repeatedly with malicious intent so that the receiver does not understand that there is fraudulent activity happening in the network by masquerading information [39, 40].

6) Physical system attacks

The coordinated attacks which involve designing system faults, change in protective gears in the physical grid like relay setting change, disconnecting relay or frequent relay switching operations have major impacts on the power grid. The adversary can also gain access to original topology files and cause an attack on the system topology by modifying the SCADA topology while avoiding detections by the operator. Also, covert data attacks can be major repercussions of this kind of network topology attack in the smart grid. The intruder can alter data from certain smart meters, IEDs and network switches to mislead the control center with an incorrect network topology [21, 24, 30, 31, 33].

2.3 Intrusion Detection for Power Transmission System

Much of the literature on cyber security of power grids is concerned with the SCADA system in the transmission level. False data injection attacks (FDIAs) are well studied as a threat to cyber

security of a smart grid [41]. Under the assumption that the adversary has the knowledge of system configuration, malicious measurements may be able to bypass bad data detection [42]. Research has been conducted on the attack model of FDIAs, impact of FDIAs, and vulnerability assessment for state estimation with respect to FDIAs [43-45]. Phasor Measurement Units (PMUs) are used as countermeasures to defend against FDIAs [46-48]. By analyzing the behavior of FDIAs, data driven and machine learning methods are exploited to detect attacks in real-time [29, 49, 50]. However, the previous work is mostly centralized, which is not designed to detect FDIAs before falsified measurements arrive at the control center level. To prevent the malicious measurements from intrusion into software applications at the control center, e.g., the Energy Management System (EMS), it is important to detect and stop the falsified measurements before they are sent out of the substations.

IEC 62351 standard is developed to handle the security of multi-protocol messaging [51]. However, currently no industrialized solution is deployed in Substation Automation Systems (SASs). On the other hand, DNP3 Secure Authentication (DNP3-SA) [4] provides a security mechanism for communication between substations and the control center; however, it is not able to detect attacks in which falsified measurements are encapsulated in the payload of DNP3 packets before authentication and integrity checking. Hence, substations are vulnerable to such attacks on measurements.

Motivated by the critical need to detect measurement attacks at the substation level, this paper is concerned with the study of attack paths in SAS and defense actions. Various studies in the literature have explored the cyber defense of substation automation. The risk and vulnerability assessment is proposed for SCADA and IEC 61850 based substations [52, 53]. To counter the threats to an IEC 61850-based substation, a signature-based IDS is developed based on the data collected by simulating the attacks on IEDs [54]. In [55-58], a comprehensive IDS integrates protocol specification, and logical behaviors for detecting abnormal behaviors within the cyber-physical systems. Based on IEC 61850 standards, the collaborative intrusion detection system proposed in [59] monitors and detects cyberattacks by screening the characteristics of Generic Object Oriented Substation Events (GOOSE) and Sample Value (SV) packets at each IED. Game-theoretic techniques are used in [60] to optimize the security mechanism for a large number of substations against coordinated attacks. Since the ICT-based IDS has a limited impact on such

intrusions that bypass the cyber defense, some studies propose defense strategies according to physical nature of the power system. To detect intrusions against the protection system, context information based defense is proposed [61, 62]. By learning the pattern of attack data, an IDS is proposed [63] for IEEE 1815.1-based network at substations. Considering the upward trend in supply chain attacks, a concrete model for supply chain attacks in IEC 61850 substations is proposed with a new security metric [64].

2.4 Cyber System Recovery for Power Transmission System

Based on the timeframe, a cyberattack lifecycle follows the “cyber kill chain,” first introduced by Lockheed Martin [65], including reconnaissance, weaponize, deliver, exploit, control, execute, and maintain. Identifying the attack before the “execute” stage is no easy task. However, once the attacker successfully executes an attack on the ICT components of the power grid, the IDS should be able to detect anomalous behaviors. Therefore, based upon the information provided by the IDS, the focus of the proposed recovery strategy falls into the two stages of “execute” and “maintain,” The stage "execute" indicates that the adversary achieves the desired cyber effect. In other words, when the intruder successfully gains unauthorized access to any node in the cyber system, the following attack actions such as DoS, extract/alter/destroy/inject data, will likely be enabled. The last stage, "maintain," of the lifecycle suggests that the adversary manages to maintain long-term presence in the compromised system. For example, the attackers can distribute multiple backdoors or malicious insertions into the system during the stage of “deliver.” Once an attack action is detected by the IDS, other backdoors which have yet been detected will potentially be enabled for the future attack. Therefore, the recovery strategy for power system after cyberattacks includes two stages, “execute” and “maintain”.

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 [66] 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. Thus, once an intrusion detection system (IDS) identifies abnormal actions in the cyber system, it is critical to recover the information infrastructure and restore the functionality of the

power system as soon as possible. Without a real-time recovery strategy for the grid operation, the risk of cascading failures increases following the attack [67].

Various studies have been reported on intrusion detection and mitigation at the substation level. The vulnerability assessment of SASs is proposed in [44]. The cyber attack/mitigation scenarios are discussed in [68] based on the interaction between Information and Communications Technology (ICT) and the physical power system. To detect cyber intrusions in a SAS, a network-based detection system is proposed using multicast messages [69]. With the Intrusion Detection System (IDS) integrated with each IED, the collaboration between the IEDs serves to enhance the monitoring and detection of cyberattacks [59, 70]. In the literature, few studies have been reported on power system restoration following outages caused by the cyberattacks. In [71], a complex optimization model is developed for the restoration of interdependent power system and communication system. In order to restore the observability of the power system after a cyberattack, a self-healing optimization problem is proposed to reconnect the uncompromised PMUs [72]. Similarly, the SHAP-NET platform developed in [73] 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 [74].

For recover the power system from cyberattacks, several systematic strategies have been proposed. It is proposed to use a Bayesian Network to quantify the potential cyber risk and determine the mitigation techniques based on the types of cyberattacks [75]. A tri-level optimization model for optimal allocation of the defense resource is proposed to prevent cascading failures caused by coordinated attacks [76]. To support fast recovery of both cyber and physical systems, the SDN-based self-healing methods are proposed [77, 78] to recover the communication networks for Phasor Measurement Units (PMUs) and microgrids against cyber intrusions. A cyber resilient distributed control strategy for microgrids is developed to detect and isolate the compromised network against successive attacks [79]. To determine the optimal reclosing time of transmission lines following cyberattacks, a recovery scheme is developed based on a reinforcement learning framework [74]. The novel concept of cyber restoration for power systems is introduced in [80], emphasizing the importance of swift observability recovery after disruptions.

Existing research predominantly emphasizes prevention and initial response, often overlooking the complexities of restoring interdependent cyber and power functionalities. In [81], the authors have addressed the necessity of understanding the intricate dependencies between these domains to assess the potential consequences of cyber events on the power grid. The significance of cyber-physical systems (CPSs) [82] is highlighted in enhancing physical systems' capabilities through cyber elements, with applications across various sectors including power systems. However, the interaction between cyber and power system during the restoration process is not clearly analyzed.

Chapter 3

Intrusion Detection and Mitigation against Measurement Attacks

Attackers can gain access to the protected infrastructures of the grid and launch attacks to manipulate measurements at the substations. The fabricated measurements can mislead the operators in the control center to take undesirable actions. Therefore, these attacks targeting power system measurements such as voltage and current are defined as measurement attacks in this dissertation. The Intrusion Detection System (IDS) proposed in this paper is deployed in IEC 61850 based substations. Regarding the detection of measurement attacks, several issues are observed: 1) Existing methods identify false measurements based on state estimation and bad data detection in the control center level. In other words, the technology does not detect measurement-based attacks at the substations before malicious measurements arrive at the control centers. 2) The specification-based IDS at the substation level is not able to identify false measurements if the fabricated data is encapsulated with legitimate headers. 3) Cyberattacks targeting measurements at multiple substations cannot be detected by local substation IDSs without a system strategy. 4) Although IEC 62351-4 specifies the cyber security of MMS, it is not commonly applied.

The proposed IDS in this paper is able to identify falsified measurements in MMS messages. Based on the law of physics of the electrical network, a distributed IDS against measurement attacks in the substation is proposed.

3.1 Problem Formulation

IEC 61850 based SAS enables different devices to cooperatively maintain system properties in a modernized substation. Specifically, based on functionalities, the physical devices are organized in three levels: the process, bay, and station levels. To support communication properties in SAS,

IEC 61850 based protocols, e.g., GOOSE, SV and MMS, are used. SV messages are used for sharing measurements of Current Transformers (CTs)/Voltage Transformers (VTs) with protective IEDs. Since there is a built-in security mechanism in SV streams, e.g., Message Authentication Code (MAC) in IEC 62351-6, for ensuring integrity, the proposed method to detect and mitigate measurement-based attacks against MMS messages does not affect the substation protection scheme. As a new function for cyber security, the proposed IDS is focused on MMS messages to prevent falsified measurements from being sent out of the substations.

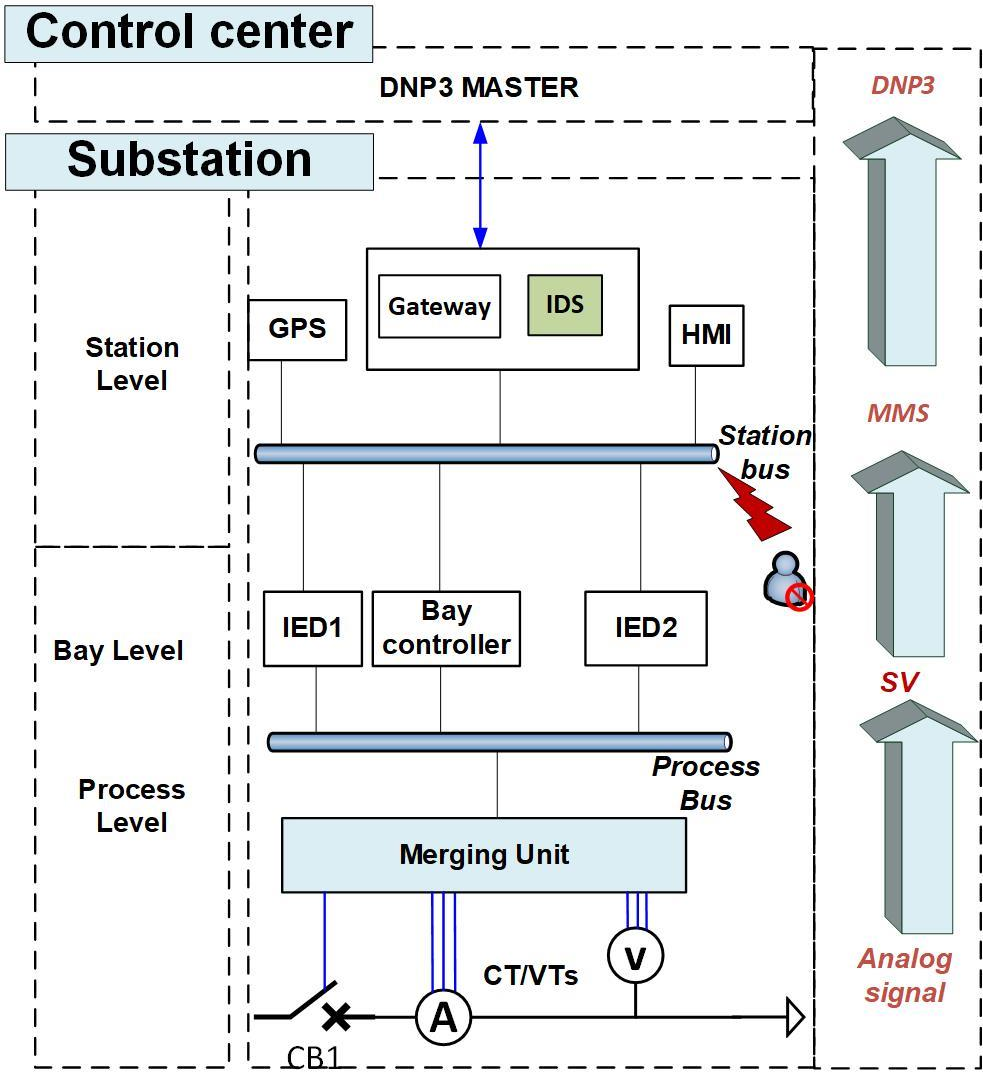


Figure 3.1 Attack path of measurement attacks at substations

In digital substations, MMS communication uses a client/server model for reporting, monitoring, and control between IEDs and the SCADA system. As shown in Fig. 3.1, in order to transmit the measurement data to the SCADA system, the gateway as MMS client sends “read-request” to access the information contained in the IED objects. Then, the corresponding IED, as MMS server, sends the response back with the measurement data encapsulated in MMS messages. As a line of defense to detect the measurement attack at SAS, the proposed IDS is configured to detect/mitigate the falsified measurements within MMS messages before they are sent to the control center through DNP3 communication.

In the cyberattack against Ukrainian power grid [83], the adversary takes control of servers in the substations through unauthorized remote access. Once the station network is compromised, the attackers will be capable of eavesdropping on MMS communication and injecting malicious packets. Without cyber security scanning at the substation level, fabricated measurements will be sequentially transmitted through DNP3 polling. The proposed defense action is a distributed IDS at the substation level. Falsified measurements are identified based on the law of physics of the power network: Kirchhoff’s Current Law (KCL), Kirchhoff’s Voltage Law (KVL) and Ohm`s law. The distributed nature of the proposed IDS enables each substation IDS to cross check the measurements with other substations.

3.2 Measurement Attack Model at IEC 61850 Substations

This section describes the potential measurement attack path on MMS messages and implementation of the proposed IDS at the substations.

3.2.1 Measurement Attack Path in SAS

Based on vulnerabilities with respect to measurement attacks, the attack path in the SAS is illustrated in Fig. 3.1.

1) Bay level and station level

The substation network is accessed from the remote access point or internal network. Once adversaries compromise the targeted substation through unauthorized access, they will gain access

to the bay level devices through the station network. Sequentially, the adversary executes the attacks against measured values through MMS communication between the IED and gateway.

As shown in Fig. 3.1, MMS messages are converted to DNP3 at the gateway according to IEEE Std 1815.1 [84], which defines the way data structures are mapped. The falsified measurements indicate a change in the system states, which creates the event data at the DNP3 outstation. Once an event polling is received, the DNP3 outstation at the substation will send the malicious data to the DNP3 master at the control center [4].

2) Control center level

Once the control center receives malicious DNP3 packets, system operators can be misled by fabricated measurements or triggered alarms and take undesirable actions. For example, multiple substations may send falsified high voltages at the substations. In response, operators may decide to switch off capacitor banks at these substations, leading to actual low voltage conditions in the power grid.

3.2.2 Implementation of Distributed IDS at Substations

1) Law of physics

Table 3.1 IDS Rules for measurement attacks

Measurements	IDS rules
Current	Kirchhoff`s Current Law (KCL): $\lvert\sum i_{exit} - \sum i_{enter}\rvert \leq k_{cer1}\lvert i_1\rvert + \cdots + k_{cern}\lvert i_n\rvert$
Voltage	Kirchhoff`s Voltage Law (KVL): $\lvert v_1 + \cdots + v_n\rvert \leq k_{ver1}\lvert v_1\rvert + \cdots + k_{vern}\lvert v_n\rvert$

Voltage and Current	Ohm`s Law: $\left\|v_j - v_k - i_{jk}Z_{line}\right\| \leq \max\{k_{verj}\left\|v_j\right\|, k_{verk}\left\|v_k\right\|, k_{cerjk}\left\|i_{jk}Z_{line}\right\| \}$

The proposed IDS applies the law of physics to detect anomalies in the measurements. The measurement system in IEC 61850 based substations includes sensing elements and IEDs. CT and VT (or Low-Power Voltage Transformers (LPVT) and Low–Power Current Transformers (LPCT)) are instrument transformers for current and voltage measurements. Note that CT/VT and the Merging Unit (MU) are subject to measurement errors, which may cause a violation of the detection rules, e.g., KCL, KVL or Ohm`s Law. The accuracy of CT/VT and MUs under a normal condition is expressed by the accuracy class of the instrument [85]. To distinguish between measurement errors and cyberattacks, rules of the proposed IDS shown in Table 3.1 include the coefficient k_{ceri}/k_{veri}, given for each instrument i , $i = 1,2, \dots, n$. They specify the tolerance in measurement errors. Current and voltage measurements are assumed to be synchronized phasors with time stamps.

KCL: The current, i_{exit} (i_{enter}), denotes current phasors exiting (entering) the substation. When applying KCL to line currents at different voltage levels, the effect of a transformer must be considered. The compensation includes the magnitude and phase-shift determined by the transformation ratio and connection of the windings [86]. As shown in Table 3.1, when the difference between the summation of i_{exit} and that of i_{enter} is within the error tolerance, KCL is considered satisfied.

KVL: For any loop in the circuit graph, KVL requires that the algebraic sum of voltage drops on all branches around the loop be zero. v_n denotes the voltage phasor at node n. Correspondingly, k_{vern} is the error coefficient of the voltage measurement. For each loop, one of the buses is assigned to be the responsible bus. Based on the inter-communication between substations, the responsible bus is tasked to verify KVL with measurements from other nodes in this loop. When the summation of branch voltages in the loop does not exceed the error tolerance, KVL holds.

Ohm`s Law: In Table 3.1, current phasor i_{jk} denotes the line current between two substations j, k, and z_{line} denotes the line impedance. v_j, v_k are the voltage phasors from substation j and k and k_{verj}, k_{verk} k_{cerjk} are the error coefficients of v_j, v_k and i_{jk}, respectively. Given the limit of the error tolerance, Ohm`s Law between v_j and v_k is verified with local measurement i_{jk} and voltage measurement v_k from substation k.

2) Deployment of the IDS in SAS

Since MMS messages are the attack targets, the proposed IDS, as a novel security feature, is integrated with the gateway as shown in Fig. 3.1. Based on the proposed IDS, synchronized measurements are needed for verification by the three rules. Therefore, IEDs with IEC/TR 61850-90-5 capability are needed to provide synchronized data at the substation [87].

3) Distributed architecture

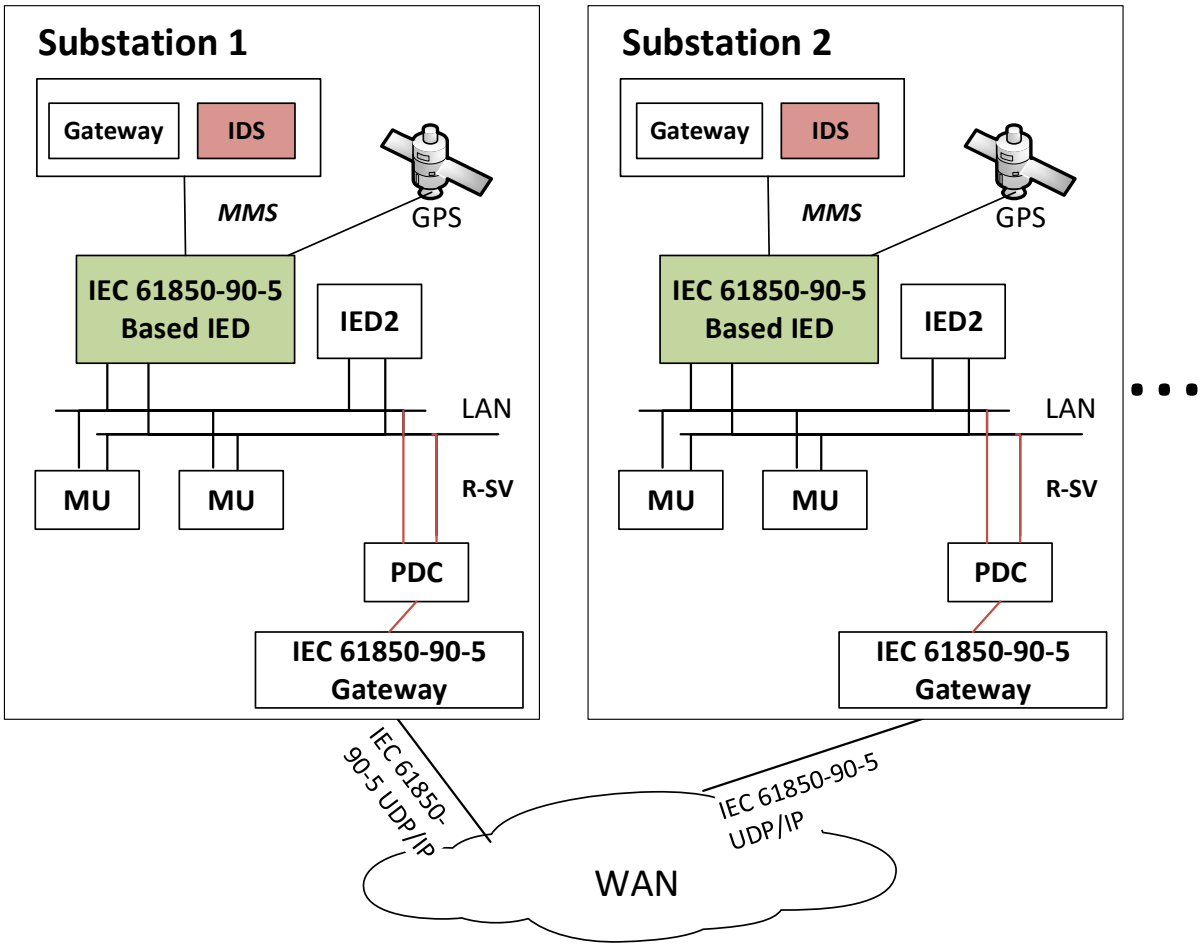


Figure 3.2 Communication mechanism between the substations

To cross check measurements with other substations, the enabling technology of the proposed algorithm is the wide-area communication of synchronized measurements. IEC/TR 61850-90-5 is developed for exchanging synchrophasor data between different LANs through WANs based on IEC 61850 standard [87]. To secure the communication over public network, IEC 61850-90-5 provides message authentication and integrity mechanisms, including Group Domain of Interpretation (GDOI) key distribution model, Hash based Message Authentication Code (HMAC), and Transport Layer Security (TLS). The proposed distributed IDS shown in Fig. 3.2 uses IEC 61850-90-5 for secure transmission of the synchronized data.

As shown in Fig. 3.2, the synchronized data will be sent from the IED to the substation Phasor Data Concentrator (PDC). IEC 61850-90-5 will map the measurement data onto the UDP/IP

protocol and then forward Routable-SV (R-SV) over WAN. Once the local PDC receives data from other substations, the real-time measurement will be transmitted to the proposed IDS, where the data stream is parsed with local measurements according to the proposed rules.

4) Time synchronization

To synchronize local measurements with the measurements from other substations, IED supporting IEC 61850-90-5 generates time stamps of the measurements to provide GPS synchronized time for the IDS. Once a substation PDC receives synchronized measurements from other substations, it will align the data according to the time stamps. Each substation, as a distributed node of the proposed IDS, analyzes the measurements based on time stamps of the packets. Therefore, the communication delay between substations does not impact the accuracy of the IDS.

3.2.3 Specification of IDS

Fig. 3.3 describes functions of the proposed IDS. First, the module of packet filtering filters out irrelevant traffic. Only MMS messages responding to the data access request will proceed to the packet parsing module. Synchronized data from other substations are transmitted from the substation PDC to the IDS as an input. At the module of packet parsing, measurement messages with time stamps are generated based on local sample values. Using synchronized measurements from local and other buses, circuit laws in Table are used to identify possible violations. After all rules are checked, the IDS triggers alarms if any violation is detected. For mitigation, the proposed IDS will discard malicious data once a violation is verified. Meanwhile, the IDS will transmit actual measurements with time stamps to the gateway. Hence, the control center is not impacted by measurement attacks that take place in the substations.

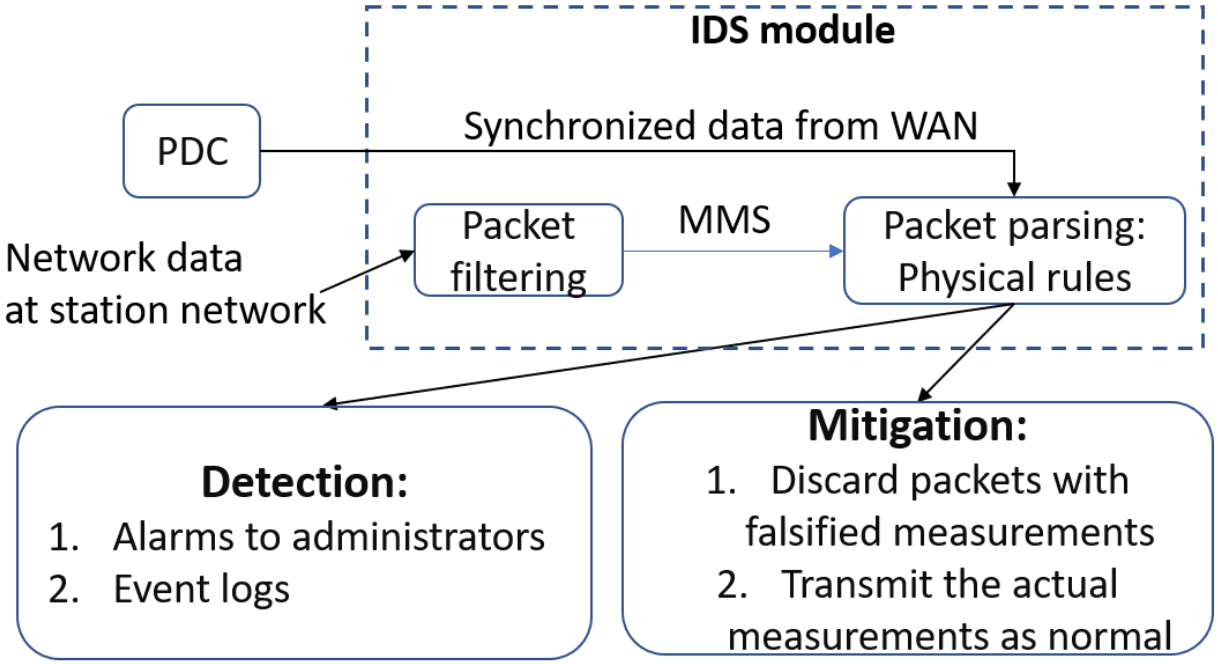


Figure 3.3 Specification of IDS

3.3 Computational Algorithms

This section shows that the law of physics used in the IDS can be used to detect false measurements under various attack scenarios. From the system topology, the adjacency matrix $\boldsymbol{A}$ of the graph-theoretic model of a power system is defined [88]. As shown in (1), the column with label nd and row with label br corresponds to each node and branch, respectively. Loads and generators are treated as branches connected to the ground node. Nonzero entries "1" and " -1" in each row represent the polarity of the connection.

$$A = \begin{array}{c} \\ br_1 \\ br_2 \\ \vdots \\ br_m \end{array} \begin{array}{c} \begin{array}{cccc} nd_1 & nd_2 & \dots & nd_n \end{array} \\ \begin{bmatrix} 1 & -1 & \dots & 0 \\ 0 & 1 & -1 & \dots \\ 0 & 1 & \dots & -1 \\ -1 & \dots & 0 & 1 \end{bmatrix} \end{array} \tag{1}$$

The branch voltage vector is a linear combination of the corresponding nodal voltages, i.e.,

$$V_b = AV_n \tag{2}$$

where V_b, V_n denotes the vector of branch voltages (voltage drops on branches) and nodal voltages, respectively.

According to KCL, the sum of all currents at each node equals 0, which is formulated by the matrix A^T in (3).

$$A^T I_b = 0 \tag{3}$$

where I_b is the vector of all branch currents.

3.3.1 Measurement Attacks at a Single Substation

Let $v'_{nj} = \epsilon v_{nj}$ represent the observed voltage measurement at bus j, where $\epsilon \neq 1$ means that the voltage measurement is falsified. Similarly, $i'_{jk} = \varepsilon_{jk} i_{jk}$, ε_{jk} denotes the attack model of current measurement. $\varepsilon_{jk} \neq 1$ means that the current measurement is falsified. Then $(\varepsilon_{jk} - 1) i_{jk}$ represents the value added to the original measurement.

Scenario 1: multiple branch currents at bus j are falsified:

a) If $\sum(\varepsilon_{exit} - 1) i_{exit} \neq \sum(\varepsilon_{enter} - 1) i_{enter}$:

$$\sum i'_{exit} = \sum i_{exit} + \sum(\varepsilon_{exit} - 1) i_{exit}$$

$$\neq \sum i_{enter} + \sum(\varepsilon_{enter} - 1) i_{enter} = \sum i'_{enter},$$

then KCL will be violated.

b) If $\sum(\varepsilon_{exit} - 1) i_{exit} = \sum(\varepsilon_{enter} - 1) i_{enter}$:

$$\sum i'_{exit} = \sum \varepsilon_{exit} i_{exit} = \sum \varepsilon_{enter} i_{enter} = \sum i'_{enter},$$

In this case, KCL will fail to detect the malicious current measurements. However, Ohm`s law will be violated by i'_{jk}: $i'_{jk} z_{line} = (\varepsilon_{jk} i_{jk}) z_{line} \neq i_{jk} z_{line} = v_{nj} - v_{nk}$.

Scenario 2: voltage measurement at bus j is falsified:

For any branch current i_{jk}, $i_{jk} z_{line} \neq v'_{nj} - v_{nk}$. Thus, Ohm` s law of the IDS will be violated at bus j.

Scenario 3: voltage and current measurements are attacked at bus j :

For any line at bus j, if $i'_{jk} z_{line} \neq v'_{nj} - v_{nk}$, the IDS will detect the attack by Ohm`s law.

3.3.2 Measurement Attacks at Multiple Substations

Let $\boldsymbol{V'_n} = \boldsymbol{T_{vol}} \boldsymbol{V_n}$ represent the vector of voltage measurements that may contain falsified data. $\boldsymbol{T_{vol}}$ defines the attack model, where $\boldsymbol{T_{vol}} = diag(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n)$. $\varepsilon_i \neq 1$ means that the ith voltage measurement is falsified. Similarly, $\boldsymbol{I'_b} = \boldsymbol{T_{cur}} \boldsymbol{I_b}$, $\boldsymbol{T_{cur}} = daig(\lambda_1, \lambda_2, \dots, \lambda_m)$. $\lambda_i \neq 1$ means that the ith branch current is falsified. The adversary can choose any $\boldsymbol{T_{cur}}, \boldsymbol{T_{vol}}$ to construct the malicious measurements. Thus, there are two attack scenarios:

Scenario1: Suppose voltage and current measurements are attacked at multiple substations, and $\boldsymbol{T_{cur}}, \boldsymbol{T_{vol}}$ are matrices and not scalar.

According to (3), the falsified current measurements are verified as follows:

$$\boldsymbol{A^T I'_b} = \boldsymbol{A^T}(\boldsymbol{T_{cur}} \boldsymbol{I_b}) \neq \boldsymbol{A^T I_b} = \boldsymbol{0} \tag{4}$$

Both voltage and current measurements are verified by Ohm`s law:

$$\boldsymbol{T_{cur}} diag(\boldsymbol{Z_{line}}) \boldsymbol{I_b} = \boldsymbol{T_{cur}} \boldsymbol{A} \boldsymbol{V_n} \neq \boldsymbol{A} \boldsymbol{T_{vol}} \boldsymbol{V_n} \tag{5}$$

Inequalities (4) and (5) show that this proposed attack will be detected by KCL and Ohm`s law.

Scenario 2: Suppose voltage and current measurements are attacked at multiple substations and $T_{vol} = \mu_1, T_{cur} = \mu_2,$ where μ_1, μ_2 are scalar.

a) If $\mu_1 \neq \mu_2$,

$$\boldsymbol{A^T}(\boldsymbol{T_{cur}} \boldsymbol{I_b}) = \mu_1 \boldsymbol{A^T I_b} = \boldsymbol{0} \tag{6}$$

Thus, KCL will fail to detect such attacks that all branch currents in the system are falsified by the factor μ_1. However, inequality (5) is satisfied, thus Ohm`s law will detect such attacks.

b) If $T_{vol} = T_{cur} = \mu$, measurements at all buses are multiplied by the same factor μ as follows:

$$\boldsymbol{T_{cur}} \boldsymbol{diag}(\boldsymbol{Z_{line}}) \boldsymbol{I_b} = \boldsymbol{T_{cur}} \boldsymbol{A} \boldsymbol{V_n} = \mu \boldsymbol{A} \boldsymbol{V_n} = \boldsymbol{A} \boldsymbol{T_{vol}} \boldsymbol{V_n} \tag{7}$$

Equations (6), (7) show that the attack targeting *all* buses in the system by the same factor can avoid being detected by the proposed IDS. However, it is unlikely that all of the large number of buses will be attacked at the same time.

3.3.3 KVL Detection

Measurement attacks that cannot be detected by Ohm`s law and KCL are analyzed based on the KVL detection. Under this specific scenario, the falsified voltage and current measurement $v_j'$, $i_{kj}'$ satisfy KCL and Ohm`s law at bus j:

$$v_k - v_j' = i_{kj}' z_{kj} \tag{8}$$

Normally, KVL is satisfied around each loop, i.e., $i_{12}z_{12} + \cdots + i_{n1}z_{n1} = 0$. However, under the attack given by (8), KVL for the related loop is expressed as:

$$\begin{aligned} &v_1 - v_2 + \cdots + v_k - v_j' + v_j - v_{j+1} + \cdots + v_n - v_1 \\ &\quad = i_{12}z_{12} + \cdots + i_{kj}' z_{kj} + \cdots + i_{n1}z_{n1} \neq 0 \end{aligned} \tag{9}$$

Inequality (9) indicates that KVL is able to uncover such attacks that cannot be detected by KCL and Ohm`s Law.

3.4 Testbed Setup

A cyber-physical system testbed is developed to simulate the measurement attacks and implement the proposed IDS at the substation level. Simulations are performed on an embedded computer. The IEEE 39-bus system is implemented in an industry level power system simulator. As the physical system layer in the co-simulation environment, the simulated voltage and current measurements are exported to a simulated substation automation system in real-time. A commercial grade IEC 61850 source code is embedded to implement the MMS communication. To detect measurement attacks, the proposed IDS will parse the data flow of local measurements and synchronized data from other substations. Fig. 3.4 illustrates the data flow of the proposed testbed.

Communication between the substations is needed to identify falsified measurements using KVL and Ohm`s Law. Industrial communication protocols (e.g., IEC 61850 and IEC 61850-90-5) are

used to establish the communication network among substations. Each of the 39 substations is assigned a unique address in LAN. Data packets with measurements are sent to the destination IP address of the corresponding substations. Since data streaming among substations is transmitted in a distributed manner [87], data exchange between substations is executed in parallel using multiprocessing on the proposed simulation environment.

For KCL validation, IDS in substation LAN will parse local current measurements. Moreover, using the proposed ICT network, every substation checks Ohm`s Law with local voltage measurements as well as those transmitted from other substations. For KVL validation, the loops in the IEEE 39 bus system are detected by the circuit analysis tool in Python. As shown in Fig. 3.5, there are 21 independent loops in the graph. The dashed lines in the figure represent the loops including ground node, generator nodes, and load nodes. For instance, the yellow dashed line between node 15 and node 16 indicates that the loads which are connected to ground form a loop in the circuit with the transmission line between bus 15 and bus 16. The blue dashed line between node 31 and node 32 shows that the two generators which are connected to ground form a circuit loop with the transmission line between node 31 and node 32.

For the IDS measurement checking, a responsible node (bus) is predefined for each loop. For instance, node 11, node 12 and node 13 in loop 1 send packets to the responsible node, node 10,

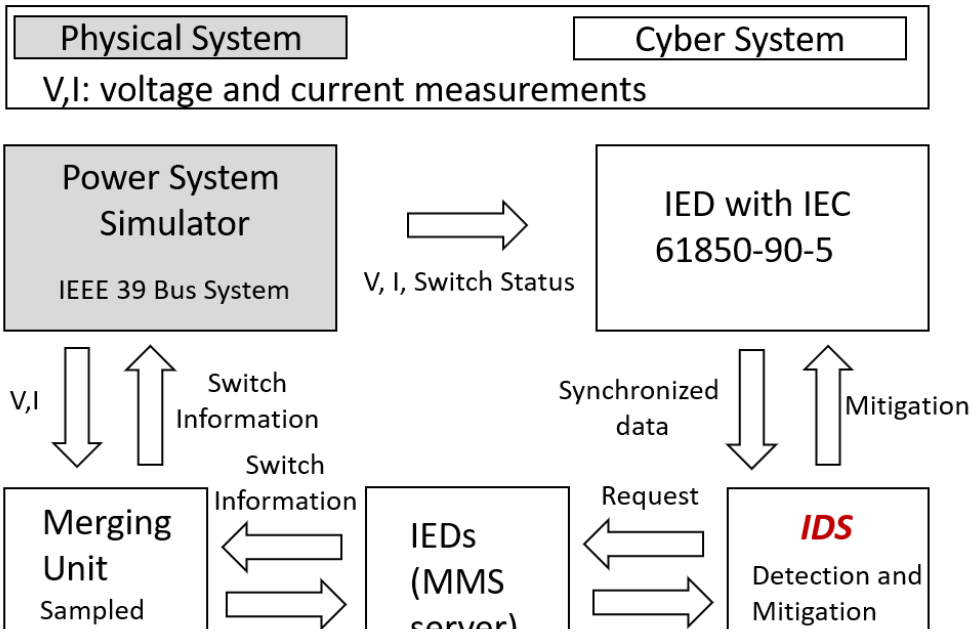


Figure 3.4 Data flow of cyber-physical system testbed

such that the current measurements from each node in loop 1 are extracted from the payload of the packets for KVL validation.

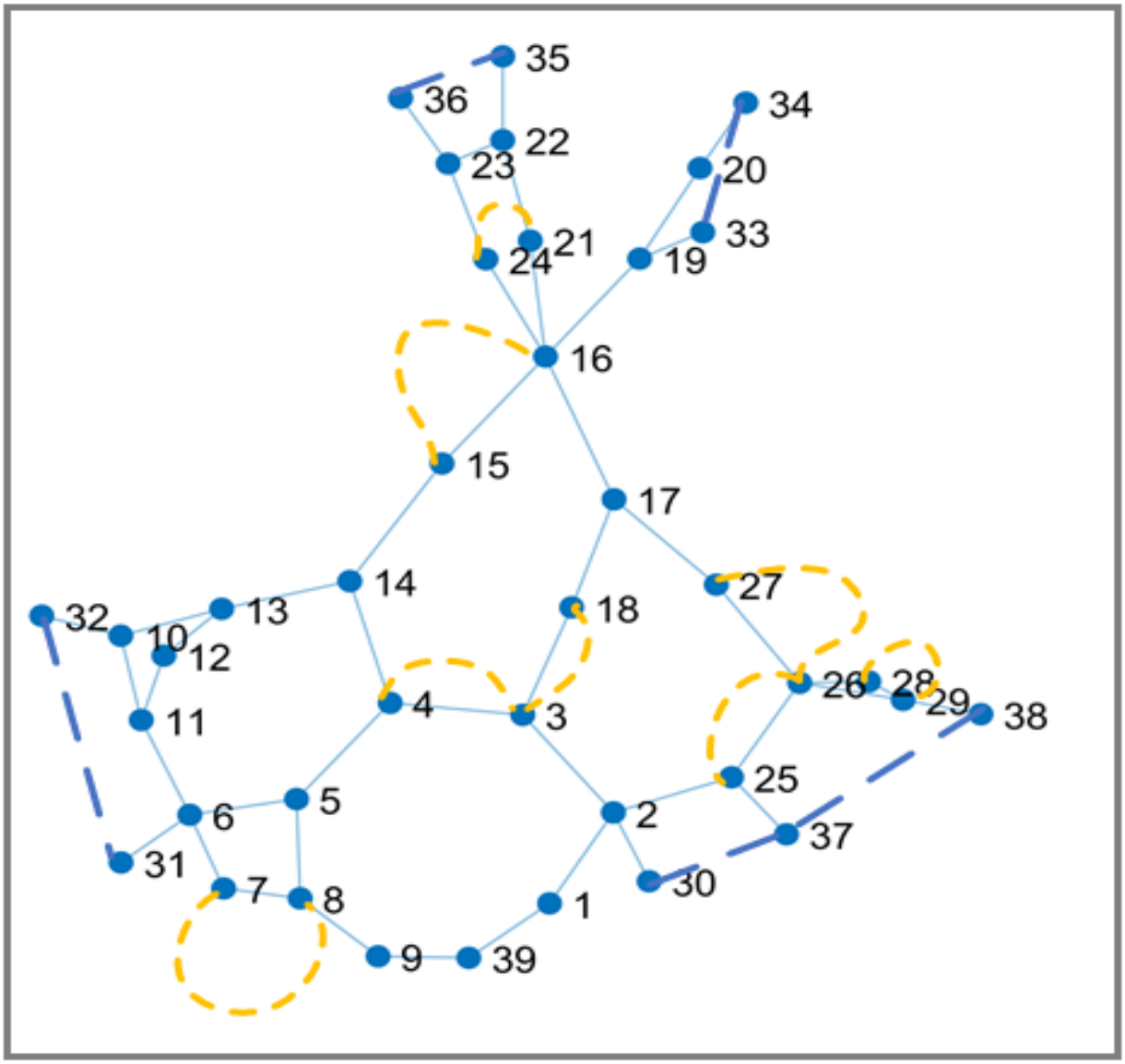


Figure 3.5 Independent circuit loops for IEEE 39 bus system

3.5 Experimentation & Evaluation

Measurement attacks targeting single or multiple substations are simulated. A stealth false data injection attack is simulated for comparison between the proposed substation level IDS and a control center EMS based IDS. Representative attack scenarios are developed for simulation and validation of the proposed IDS.

Based on the concept of "undetectable" malicious measurements, e.g., [41-45], a general attack model can be constructed by $z_{bad} = z + a$, where z denotes the original measurements and a is the attack vector. To bypass the bad data detection in state estimation, if the attacker uses an attack vector $a = Hc$, where H is the measurement matrix used in state estimation, and c is an arbitrary nonzero vector, the threshold of bad data detection will not be violated. However, the proposed stealth attack will undermine the results of state estimation.

In this attack scenario, the original measurements are generated by combining the power flow results with measurement errors. The measurements of voltage magnitudes at bus 11 and bus 13 are falsified with a constructed vector c. The injected error shown in Fig. 6 represents the difference between the voltage magnitudes of power flow results and manipulated results of state estimation. It is noted that the differences at bus 11 and bus 13 are significant.

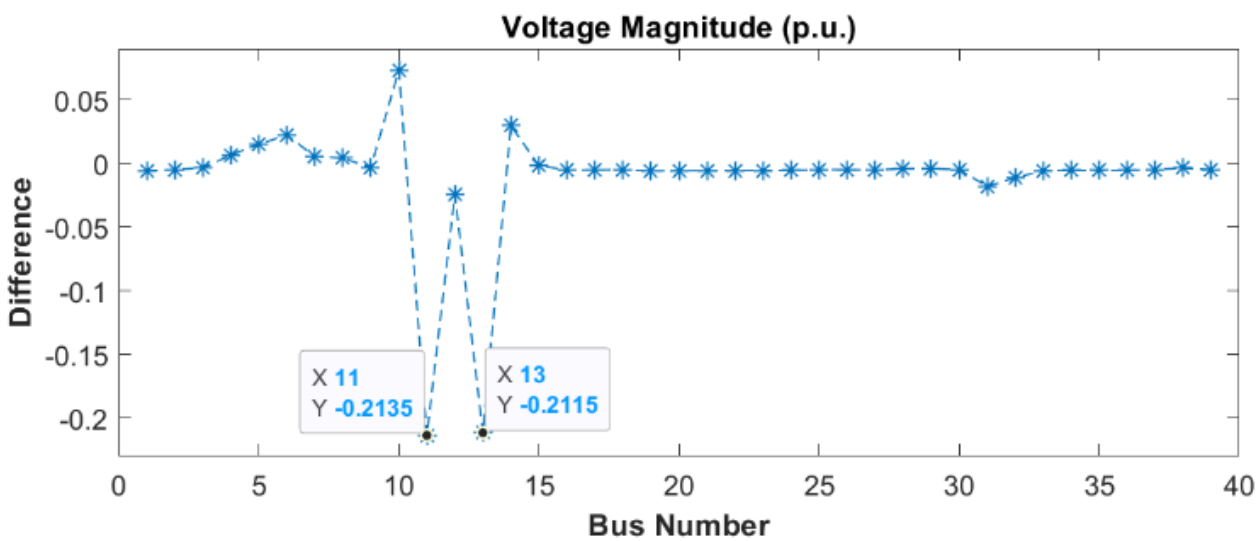


Figure 3.6 Difference between the original and estimated measurements after a stealth attack

Table 3.2 IDS rules for stealth attack

Stealth attack	**Attack targets**	**IDS alerts**	**Bad data detection results**
$\boldsymbol{z_{bad}} = \boldsymbol{z} + \boldsymbol{Hc}$	Bus 11, Bus 13	t = 0.078s, 0.095s: Ohm`s Law alert triggered at buses 11,13	$\lVert z_{bad} - X_{est} \rVert < \tau$

Table 3.2 shows the detection results of the stealth attack. According to the IDS, the malicious voltage measurements violate Ohm`s law at bus 11 and 13, which triggers the alerts at 0.078 and 0.095 seconds at each substation. However, the norm of measurement residuals, $\lVert z_{bad} - X_{est} \rVert$, is less than the threshold, referred to the Chi-squares table. Thus, without the proposed substation IDS, this attack can successfully inject malicious errors and bypass bad data detection. Much research has been concerned with the detection of stealth attacks targeting state estimation. Usually, it is assumed that attackers have full/partial knowledge of the current system configuration. However, the proposed substation IDS is able to detect and mitigate the falsified measurements before they are sent out of the substation, whether the attacks are independent or coordinated.

Table 3.3 shows the detection results for different attack scenarios. For scenarios 1, the attacker falsified the voltage measurements by increasing the magnitude of measurements to 1.3 times. As current measurements are not fabricated, KCL and KVL are not violated according to the detection algorithms. From the detection results in Table 3.3, Ohm`s Law at bus 10 successfully detects the attack, IDS warning is triggered as a response.

For scenario 2, current measurements on the line between bus 10 and bus 13 are falsified at bus 10, causing a violation of KCL and Ohm`s Law at bus 10. The IDS warning at bus 10 is triggered. Since the falsified current violates KVL of Loop 1 (including buses 10,11, 12, 13), KVL alert is also triggered.

Table 3.3 IDS Performance for measurement attack scenarios

Attack Scenario	**Attack Target**	**IDS Alert with Detection Time (DT)**
1. Increase voltage magnitude to 1.3 times of the measurement	Bus 10	t = 0.072s: Ohm`s Law alert triggered at bus 10
2. Increase line current between bus 10 and bus 13 to 3 times of the measurement	Bus 10	t = 0.003s: KCL alert triggered at bus 10 t = 0.065s: Ohm`s Law alert triggered at bus 10 t = 0.093s: KVL alert triggered at bus 10 (Loop 1)
3. Increase all the current magnitude to 3 times of the measurement	Bus 11 and 13	t = 0.055s: Ohm`s Law alert triggered at bus 11 t = 0.065s: Ohm`s Law alert triggered at bus 13 t = 0.092s: KVL alert triggered at bus 10 (Loop 1) t = 0.103s: KVL alert triggered at bus 13 (Loop 2)
4. Increase voltage to 1.3 times, current to 3 times of the measurement	Bus 10	t = 0.063s: Ohm`s Law alert triggered at bus 10 t = 0.085s: KVL alert triggered at bus 10 (Loop 1)

5. Increase voltage to 1.3 times, current to 3 times of measurement	Bus 11 and 13	t = 0.059s: Ohm`s Law alert triggered at bus 11  t = 0.062s: Ohm`s Law alert triggered at bus 13 t = 0.086s: KVL alert triggered at bus 10 (Loop 1) t = 0.097s: KVL alert triggered at bus 13 (Loop 2)

For scenario 3, all current measurements at bus 11 and bus 13 are falsified by increasing the line current to 3 times of the measurements. KCL fails to detect this attack. However, Ohm`s Law successfully detects this measurement attack at buses 11 and 13. KVL alerts are triggered by Loop 1 and Loop 2. Thus, IDS warning at both buses is triggered.

Similarly, if both voltage and current measurements are falsified at scenarios 4 and 5, the proposed IDS is able to detect the measurement-based attack by checking IDS rules. As shown in Table 3.3, Detection Time (DT) is estimated by the time difference between the time stamp in the messages and the time when the scanned packet is detected by any rule. The detection of KVL usually takes more time to complete. Ohm`s Law detection is relatively fast since the time delay is based solely on the transmission delay of other buses. For KCL, the detection is the fastest as there is no need for communication with other substations. Once an alert is triggered by a violation, the IDS warning is triggered. Therefore, DT of a particular measurement attack is determined by the fastest alert.

3.5.1 Performance of the IDS

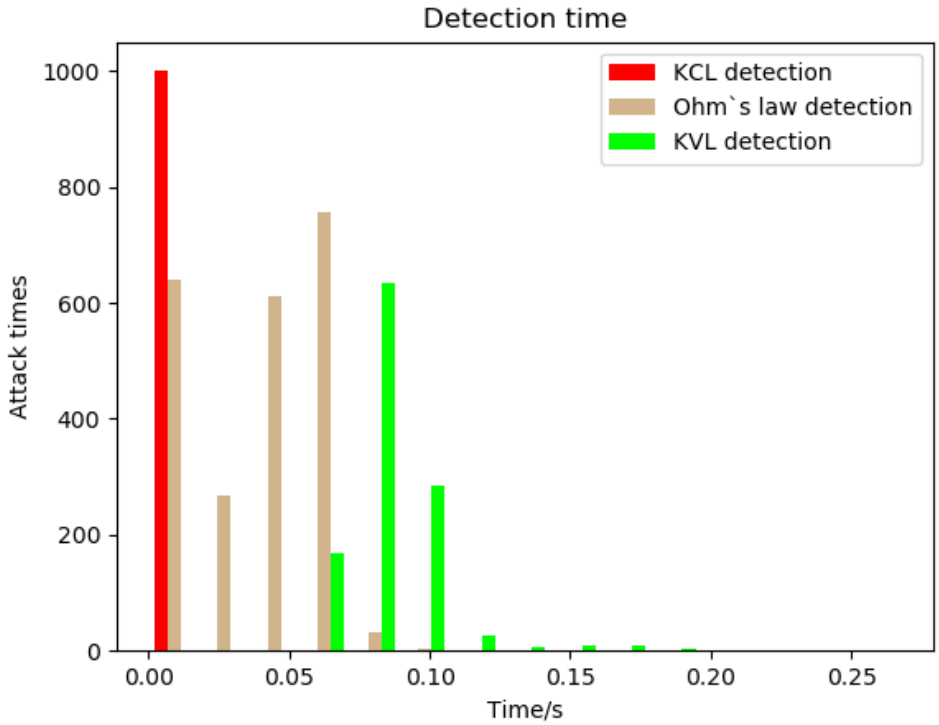
1) Detection time (DT)

Using Monte Carlo simulation, the measurement attacks targeting a random bus in IEEE 39 bus system are executed 1000 times on the proposed testbed. DT as a performance metric is measured for each attack.

Fig. 3.7 illustrates the distribution of DT under single-bus and two-bus attacks, respectively. The Y axis of the figure shows the number of attacks that have been detected during the simulation. From the distribution of the results, KVL detection requires more time to check the detection rule. As the responsible bus in the loop validates KVL by collecting the measurement packets from other buses in the loop, the latency is caused by the highest transmission delay over all buses in the loop. Specifically, the maximum DT observed from KVL detection reached 0.15 second, as this loop is the largest loop in the system with 8 substations. Communication between buses is efficient. Indeed, checking of the Ohm`s Law is completed within 0.1 second. As validation of KCL is processed at the local substation without any confirmation information from outer network, DT for KCL is around 0.01 second. In Fig. 3.7, the maximum DT is lower than 0.2 second, which is smaller than the cyclical time of DNP3 polling. Hence, the proposed IDS is able to identify falsified measurements before the measurement messages are sent out by DNP3 outstation.

A histogram comparing the results is shown in Fig. 3.7(a) and (b). It is noted that the DT distribution of single-bus attacks is close to that of two-bus attacks as expected. The reason is that the proposed IDS checks the consistency of measurements in a distributed manner at the substation level.

The general DT distribution for various attack scenarios in 39-bus system is given in Fig. 3.8. In order to evaluate the performance of the proposed IDS under multiple cyberattacks, substations are randomly selected by the measurement attack. The Y axis in Fig. 3.8 represents the number of substations that are attacked simultaneously. For each attack scenario, the detection time of the attack is the time when the first alert is triggered by the IDS. In Fig. 3.8, the band represented by the box gives the maximum, minimum, and median of the detection time over 100 experiments, respectively. The outliers are defined as red points located outside the box. By comparing the respective median of each box, all medians are close to each other, and fall under 0.025s. The results show that, for a broad range of attacks, the distributed IDS responds within a short time.



(a) Single-bus attacks

(b) Two-bus attacks

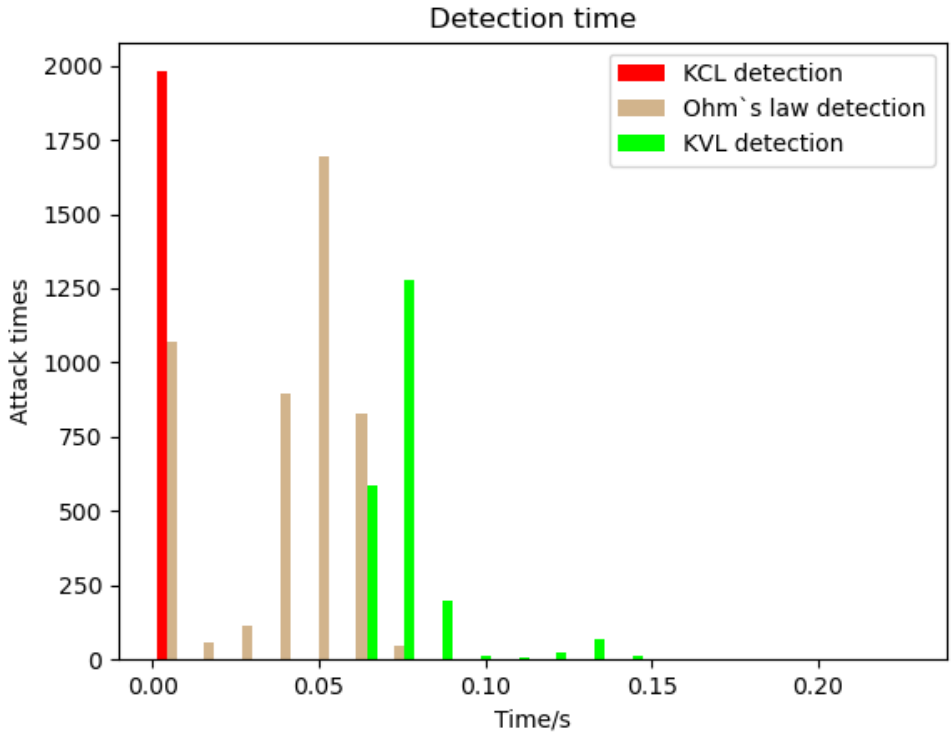


Figure 3.7 Distribution of detection time of each rule in IDS

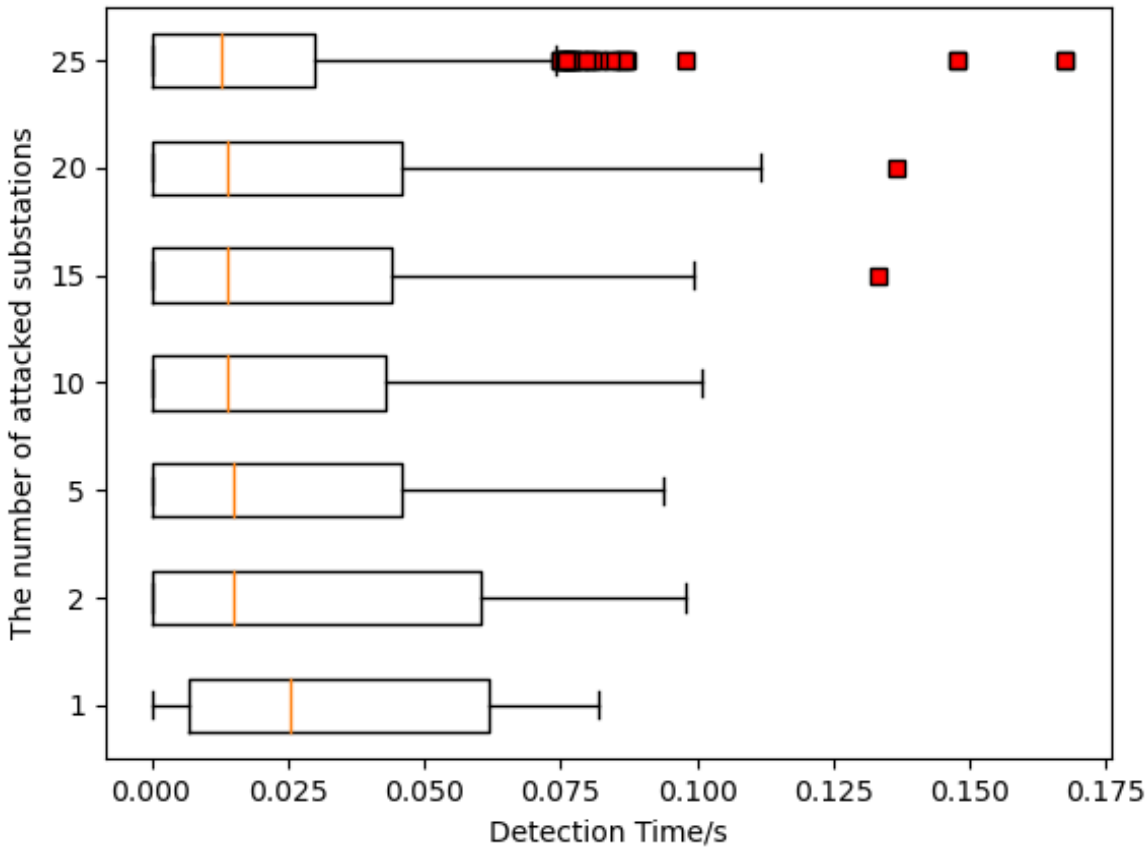


Figure 3.8 Distribution of detection time for attacks targeting multiple substations

2) Detection rate (DR)

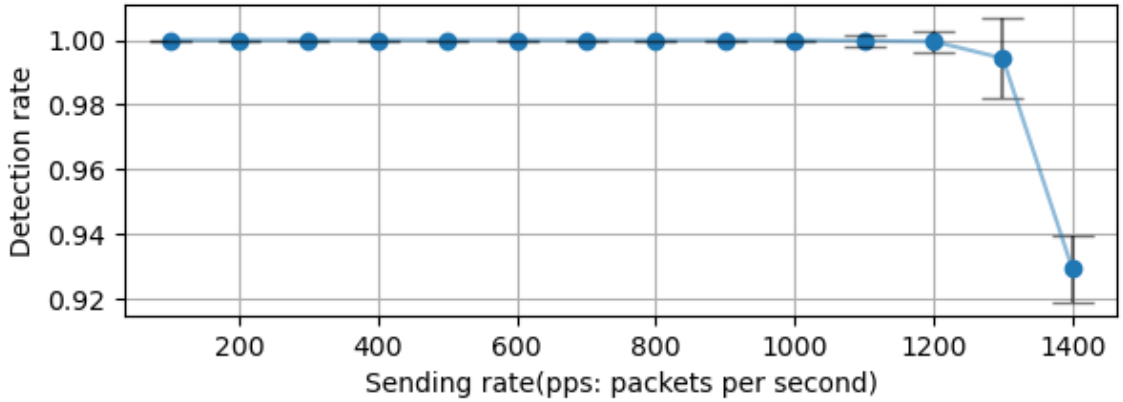


Figure 3.9 Detection rate with difference traffic rates

The accuracy of the proposed IDS is measured by DR, which is the ratio of TP (number of attacked instances IDS correctly detects) and $FN + TP$ (overall number of the attack instances).

$$DR = \frac{TP}{FN + TP} \tag{10}$$

Measurement packets mixed with the falsified measurements are sent in different rates. For a given rate, the experiments are repeated 100 times. The error bar is calculated based on the standard deviation of the results. Fig. 3.9 shows the impact of traffic rate for DR. The results show that the IDS is able to detect the falsified data in the mixed data stream. In other words, if the attacker floods the system with duplicate packets at a rate of 1000 packets per second, the alarms are triggered once the first fabricated measurement is captured. Therefore, the mitigation strategy is able to prevent the substation from further flooding. However, it is observed that DR declines from 100% to 93%, when the sending rate exceeds 1000 packets per second. The error bar indicates the low performance of the IDS when the data traffic is too fast. Along with the increase of traffic speed, the delay time between any two packets becomes too small. The IDS is not fast enough to identify each packet within the mixed data stream at such a high speed, causing the falsified measurements in the missing packets to be misclassified.

3.6 Conclusion

In this work, the potential attack path of measurement attacks at the substation level is established. The performance of the proposed IDS has been validated by simulation with realistic measurement attacks. The proposed method achieves a high level of detection accuracy under high speed traffic of measurement messages. By the proposed IDS, measurement attacks are detected within the substations, thereby avoiding the impact of falsified measurements on system operation in the control center. For the future work, collaborative IDSs with communication among the substations should be studied so that the distributed IDSs will be able to work as a team to detect various attack types targeting the digital substations.

Chapter 4

Cyber System Recovery at Digital Substations

With the integration of communication technologies and the 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 unmanned and some are located in remote locations.

To promptly recover the main functionality of the system operation and control, this dissertation 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.

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 proposed method are:

- Proposing a strategy to recover the main functions of a substation following cyberattacks.
- Presenting a novel application suitable for integration within the Software Defined Network (SDN) environment of digital substations.

- Developing a local recovery procedure which is solely based on 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.

4.1 Problem Formulation

The ICT of substations includes remote functions for the Supervisory Control And Data Acquisition (SCADA) system, which potentially exposes the cyber-power system to cyber intrusions. The 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 CB control signals, four potential attack points at the substation level are illustrated in Fig.4.1. It is noted that the adversary can trigger the attack from inside or outside the substation. Based on the analysis of different attack paths, the compromised components that will be isolated during the cyber recovery are discovered.

1) From inside the substation

From inside of the substation, an adversary can intrude into the substation network by accessing attack points (2), (3) or (4) as shown in Fig. 4.1.

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.4.1) 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.

2) By Remote Access

If the adversary gains access through (1) in Fig.4.1, 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.

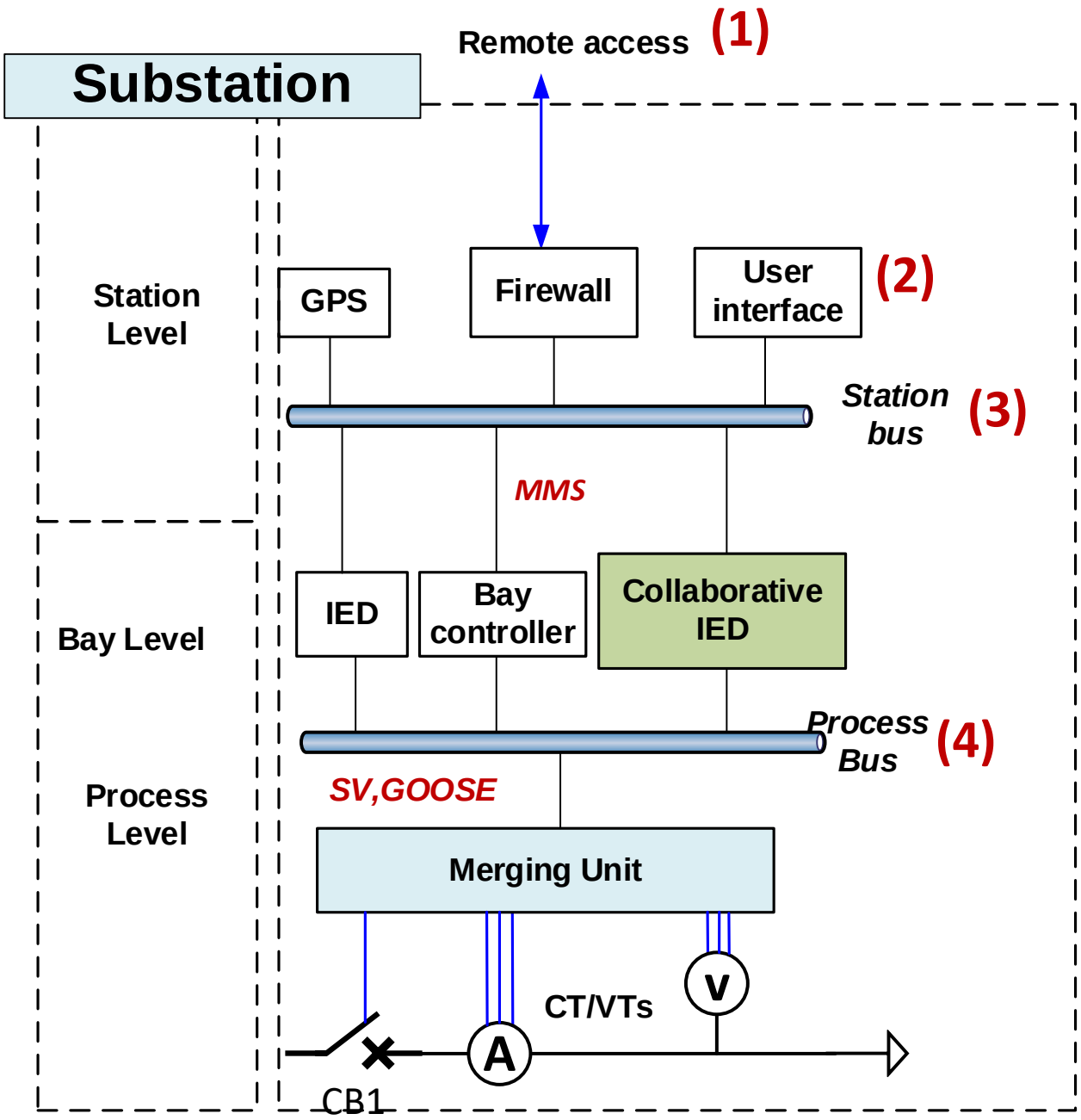


Figure 4.1 Potential attack surface at substations

4.2 Methodology for Cyber Recovery

In order to secure the digital substations, the concept of a collaborative Intrusion Detection Systems (IDS) has been proposed [59, 70]. 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. As shown in Fig. 4.2, 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.

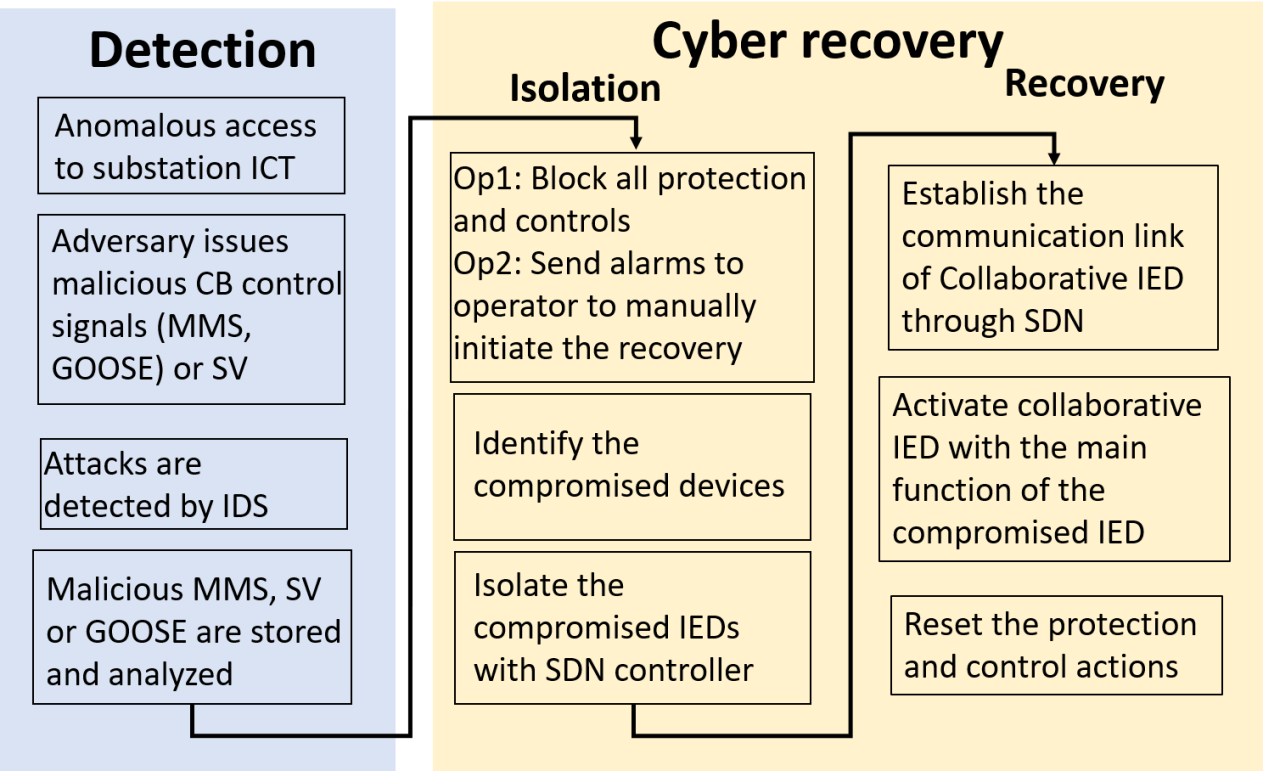


Figure 4.2 Methodology of cyber recovery at a substation

4.2.1 Isolation

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

- Option 1: Protection and control functions of all IEDs are blocked. The collaborative IDS [59] 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 component, SDN, with complete network visibility, increases the flexibility of control over the substation network [89]. 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). Note that in this case, the centralized SDN controller is trusted. Security measures for the SDN controller are assumed within the scope of this study.

Based on information of the various attacks in Section II, SDN controller implements the isolation by programming the flow tables of the correlative switches. Table 4.1 shows the relation between the security information from the IDS and correlative SDN switches that the compromised IED is connected to.

Table 4.1 Correlative SDN switched 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 remote access:* 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.
- *Attacks from inside of the substation:* Based on the attack points in Section II, both station bus and process bus can be compromised under cyber intrusions from inside of the substation LAN. 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 SDN controller. On the other hand, if the malicious MMS is detected containing the fabricated control from the compromised station IED, the SDN will send the flow entry to the Ethernet switch (station bus) to block the related MAC and IP address.

4.2.2 Recovery

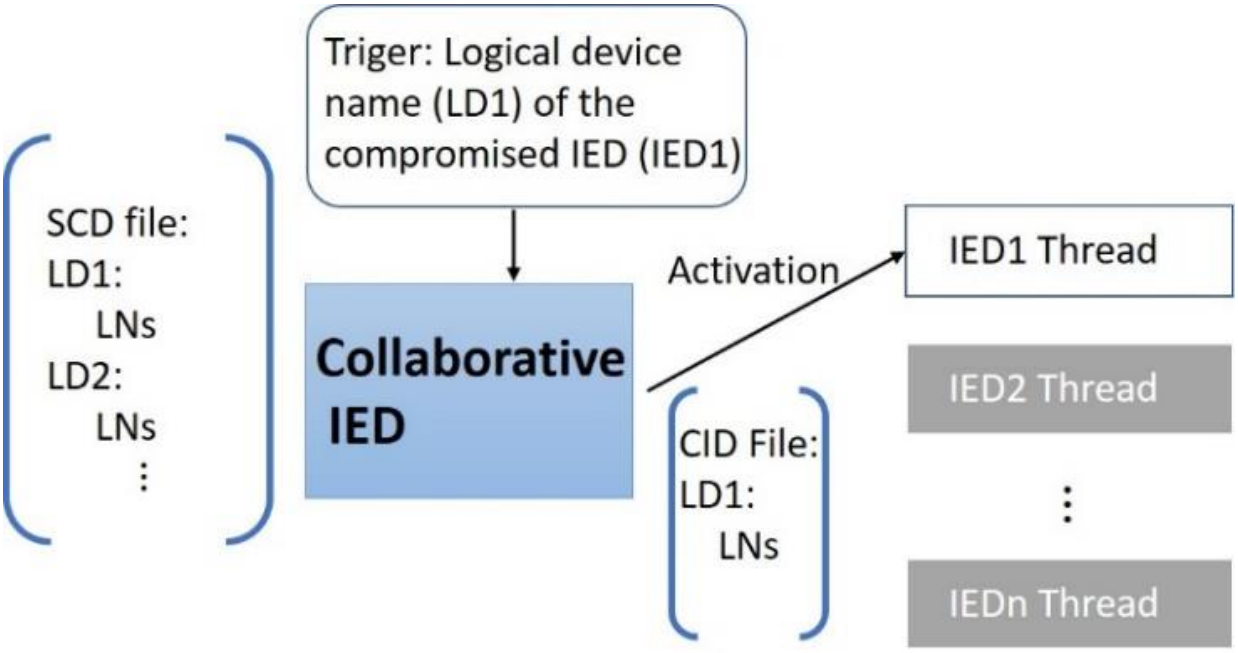


Figure 4.3 Configuration of proposed collaborative IED

Based on 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, 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 connecting with 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 [90], 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 [91]. 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. 4.3, the proposed collaborative IED with SCD file has full information of substation configuration, providing the capability to convert to any type of IEDs. 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, 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.

4.3 Simulation Results

4.3.1 Testbed Setup

A cyber-physical system testbed representing the IEC 61850 based substation with the 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 [92]. Simulations are performed on an embedded computer.

The topology of SDN based substation network has been established as shown in Fig. 4.4. 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 (IED1, collaborative IED, and 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.

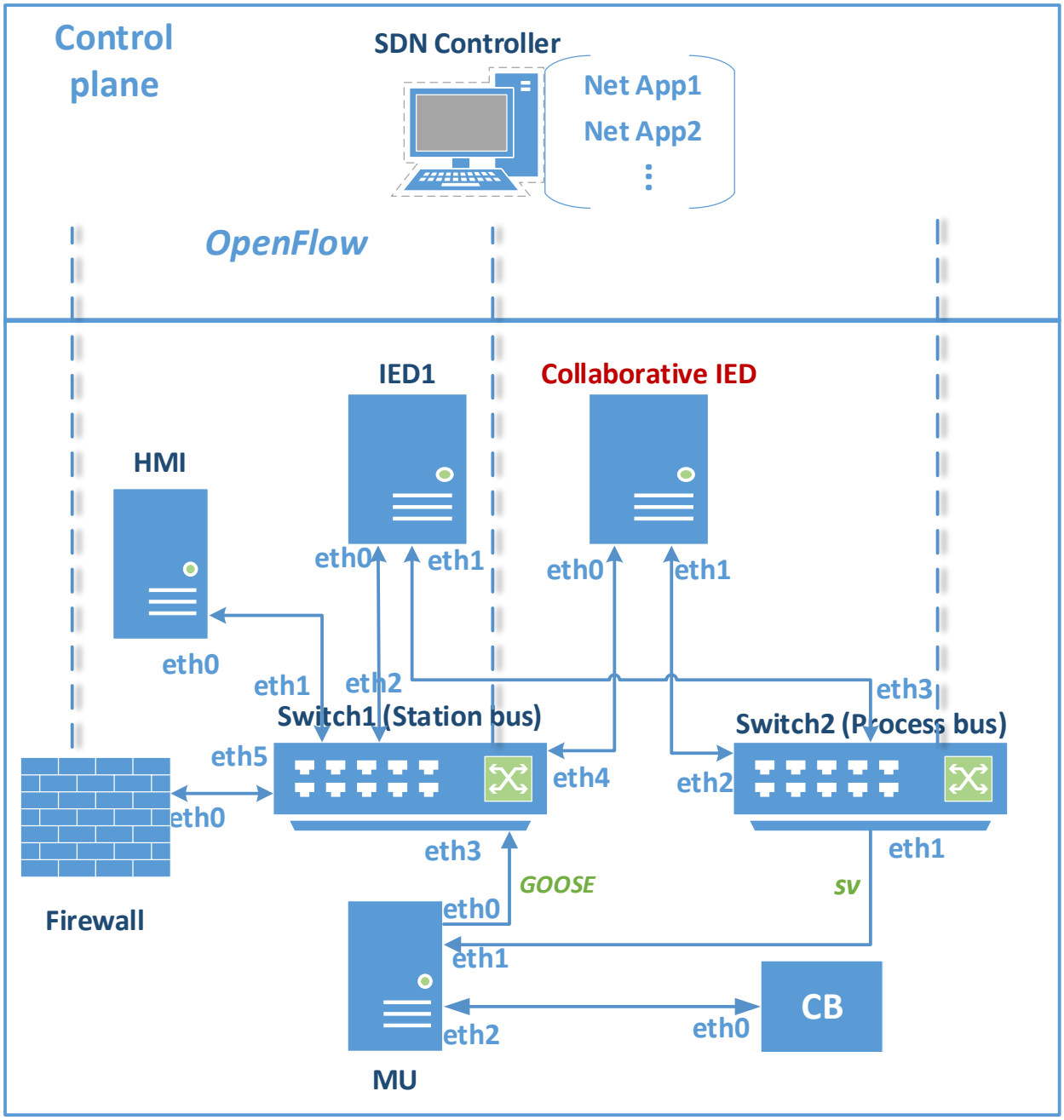


Figure 4.4 SDN based substation network

4.3.2 Scenario1: Fabricated GOOSE from IED1

Based on the embedded IDS in the testbed, security information of the malicious GOOSE indicates the source MAC 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. 4.5. 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.

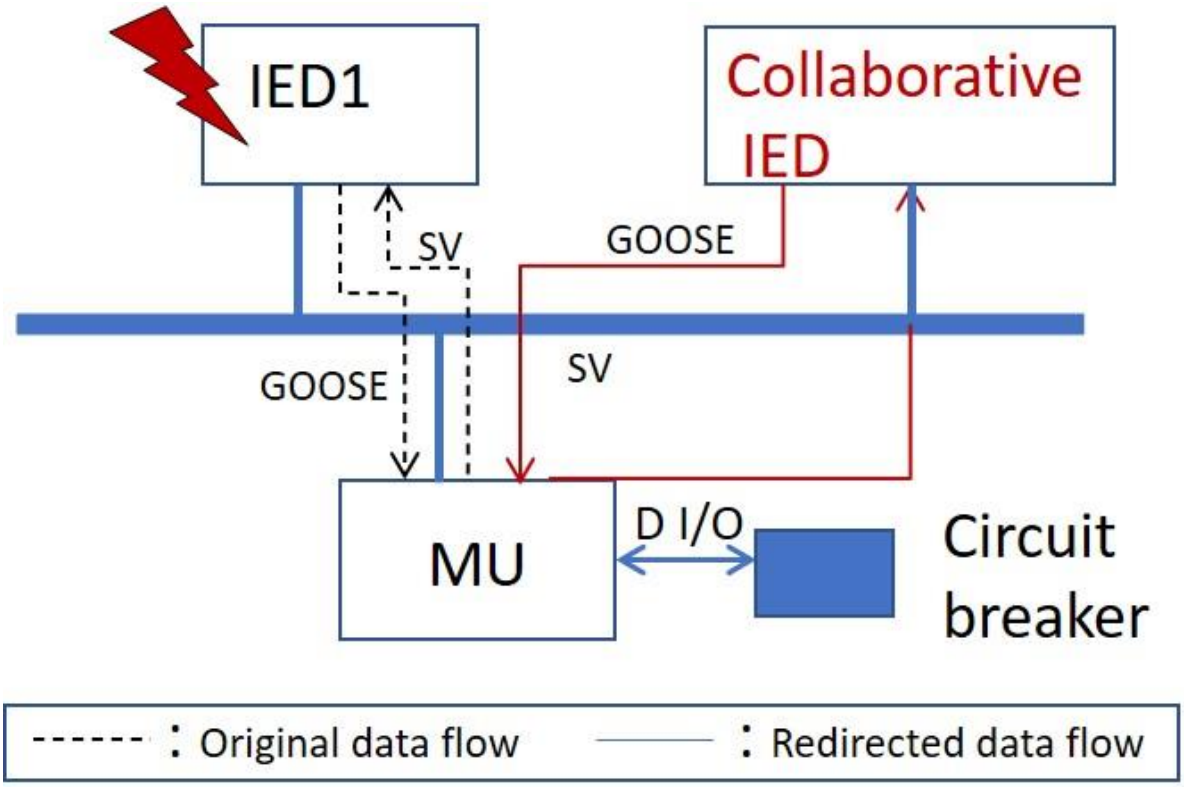
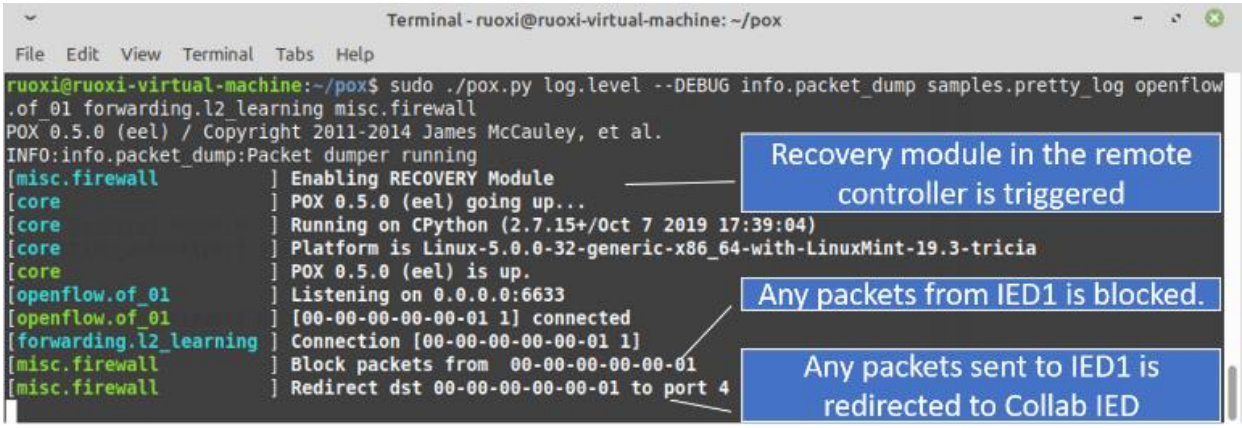
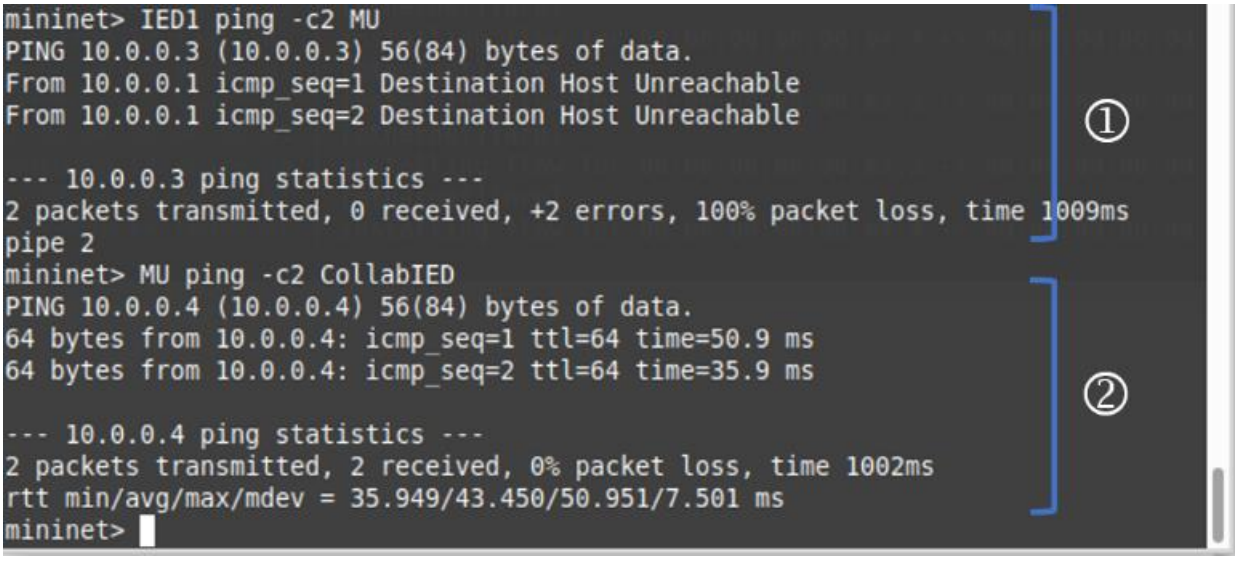


Figure 4.5 Isolation of IED1



a. POX controller



b. Mininet console

Figure 4.6 Simulation results of SDN under scenario 1

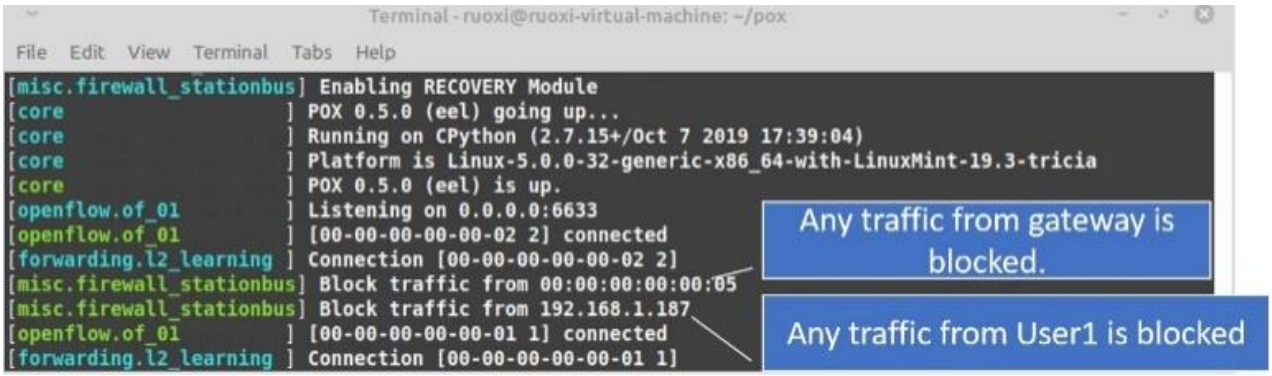
Fig. 4.6a shows the logs from actions of the controller. After the controller successfully activates the recovery module, the proposed flow entries are issued via OpenFlow link to Switch1 (Station bus). To verify the updated flow table, Fig. 4.6b shows the results of connectivity between the hosts in 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.

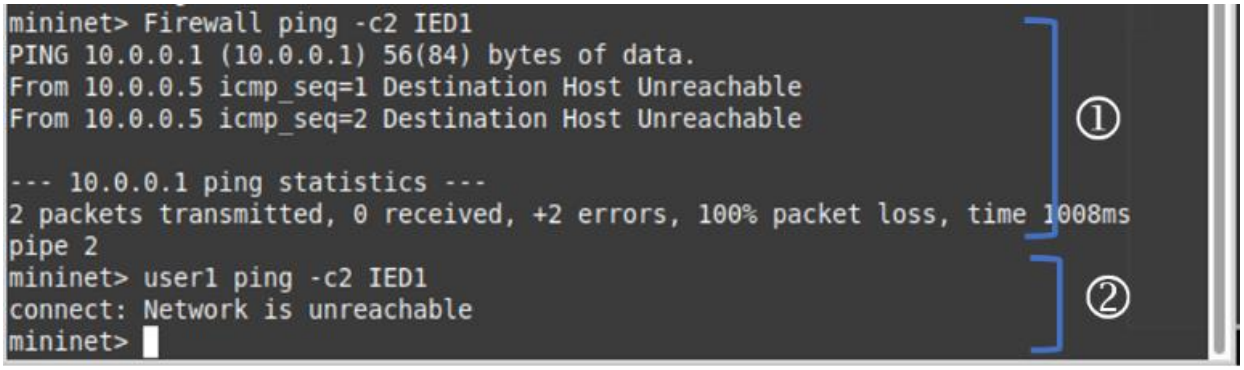
②: With the new entry in the flow table, the connection between MU and collaborative IED is established.

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

4.3.3 Scenario2: Attack from Remote Access



a. POX controller



b. Mininet console under Scenario 2

Figure 4.7 Simulation results of SDN under scenario 2

In this scenario, the attacker accesses from remote the station bus through the firewall and navigates 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 the 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, 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, 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. 4.7a. 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. 4.7b 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, which prevents further attacks through remote access.

4.4 Conclusion

This work 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 extended to multiple substations. Based on the secured communication between the substations, the restoration process for the cyber system can be deployed in a distributed manner.

Chapter 5

Cyber-Power System Restoration Planning under Large-scale Cyberattacks

On May 7, 2021, a U.S. pipeline system, Colonial Pipeline, suffered a ransomware attack that successfully compromised its billing system. The company halted the pipeline's operations to prevent further attacks on the Operational Technology (OT) system. It took more than one week to fully recover their network and restore operations after the attacks. This incident is the latest example of how the vulnerabilities in cyber systems can lead to large-scale attacks that require considerable effort to recover from. However, the post-cyberattack restoration strategy for power systems needs further study, despite its critical importance in mitigating economic losses and ensuring public safety.

The motivation for this research is to develop an effective strategy for post-cyberattack cyber-power restoration. Once an intrusion detection system (IDS) identifies abnormal actions in the cyber system, it is crucial to recover the information and communication technology (ICT) infrastructure and restore the functionality of the power system as soon as possible. To address these challenges, this paper proposes an integrated strategy for power grid restoration that accounts for the challenges posed by severe cyberattacks. This strategy emphasizes the interdependency between communication disruptions and manual intervention, leading to a comprehensive restoration approach validated by a cyber-power simulator. Considering that potential large-scale cyberattacks can compromise multiple distributed devices, the proposed cyber system restoration strategy should be capable of handling the limited capacity of the communication network of a power system. In this paper, an SDN-based solution for cyber-power system restoration is proposed for the flexible monitoring and control of the communication network.

5.1 Cyber-power System Restoration Algorithm

5.1.1 Interdependency between Cyber System and Power System

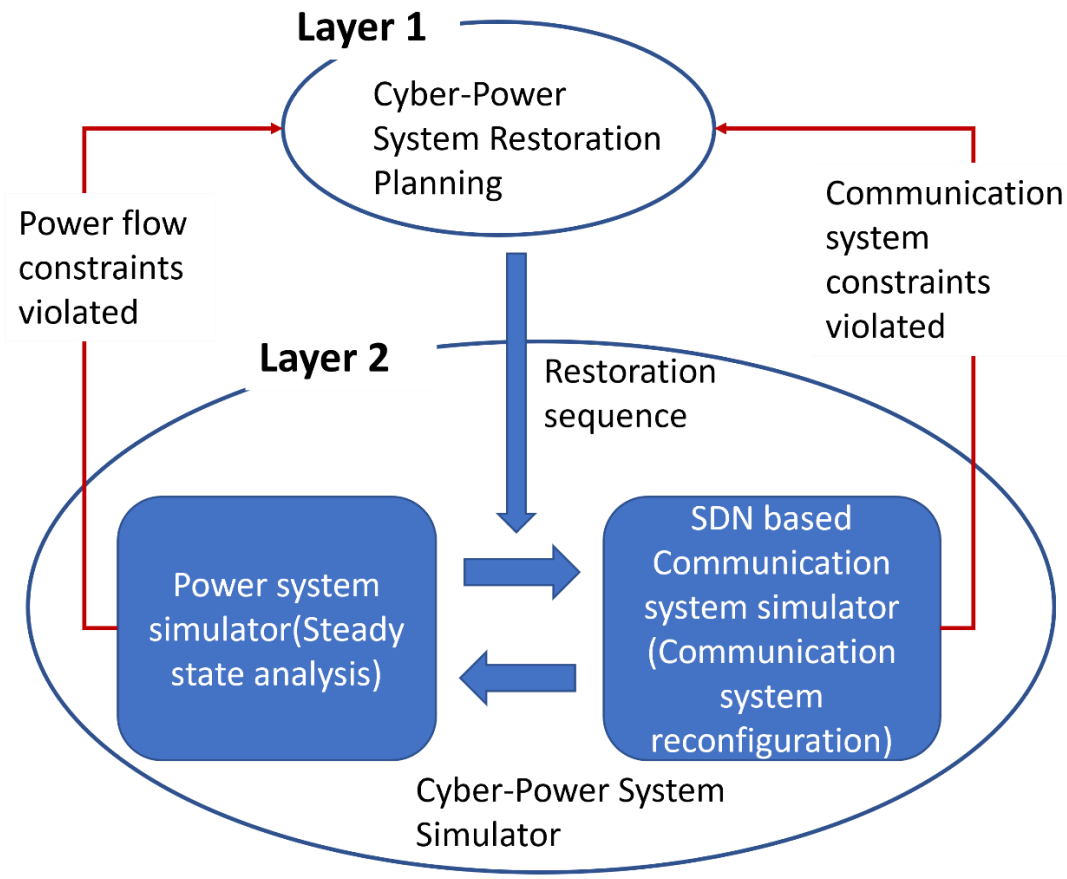


Figure 5.1 Cyber-power system restoration strategy

After a blackout in the power system, effective communication becomes pivotal for facilitating the restoration process. However, if a severe cyberattack compromises the supervisory control and data acquisition (SCADA) network, it leads to a disruption in the remote monitoring and control capabilities of the power system, resulting in a delay in power system restoration. When the cyber system is compromised, repair crews need to be dispatched to manually operate breakers at substations, further impeding power system restoration. Therefore, by considering the interdependency of both the power and cyber systems, the optimal restoration path for both can be identified and implemented.

In this paper, as shown in Fig. 5.1, the proposed cyber-power system restoration strategy is twofold. In Layer 1, the multi-network restoration is modeled using mixed integer linear programming. In Layer 2, a constraint check of both the power system and communication network is implemented using a cyber-power system simulator. The proposed optimization model provides an initial sequence for activating generators, power system buses, and communication nodes. Because the proposed objective function and constraints are a linear combination of binary decision variables, the global optimal solution is achieved at each time slot (10 minutes). By using the cyber-power system simulator, the power flow constraints and communication system constraints will be checked at each restoration step. If the constraints are violated, the restoration sequence will be recalculated. The new restoration steps will be checked by the co-simulation until the cyber-power system is feasible at each restoration step.

5.1.2 Optimization Model of Cyber-Power System Restoration

The cyber-power system is modeled as an integer linear programming problem. Binary variables serve to denote the operational state during the restoration process, either active or inactive, of power system buses, communication nodes, and associated communication links.

Considering the blackstart capabilities, generators are categorized into Non-Black Start Units (NBSUs) and Black-Start Units (BSUs). When a unit is energized, the output of the generator increases gradually to the maximum output. The ramp rate measures how quickly a unit can change its output. From the authors' previous work [93], the nonlinear gelnerator capability curve can be modeled by the binary decision variable u_{igen}^{t} as shown follows:

$$BSC_i = C_i\left(T - t_i^c - \frac{C_i}{K_i}\right) + \frac{(C_i)^2}{2K_i} - P_i^c T$$

$$-(C_i - P_i^c)t_i^{st} \tag{1}$$

$$t_i^{st} = \sum\left(1 - u_{igen}^{t}\right) + 1 \tag{2}$$

where $u_{igen}^{t}$is the binary decision variable representing the status of NBSU generator i at each time slot. $u_{igen}^{t} = 0$ indicated that $NBSU_i$ is not energized at time t. BSC_i represents the blackstart capability of generator i, C_i is the capacity of generator $i,\ T$ is the entire restoration time, t_i^c is the

cranking time of generator i to begin to ramp up, K_i is the ramping rate of generator i, and P_i^c is the cranking power requirement of generator i. As shown in (2), the start-up time t_i^{st} of generator i is expressed with u_{igen}^t. Noted that, it is assumed that the generator will not be shut down as long as it is energized. By doing so, the decision variable matrix of each generator of the proposed restoration algorithm is modeled by 1by T.

The optimization of the power network focuses on its topological constraints and overall online generation capacity, while the communication network aims to expedite the restoration of nodes and links. The improvement of the previous work[93] is the mutual reliance between power and communication links is taken into account as network constraints as shown in (3). The objective is:

$$\max \sum_{i \in S_{NBSU}} BSC_i + \sum_{t \in S_T, i \in S_{node,} j \in S_{link}} b_{nodei}^t + b_{linkj}^t \tag{3}$$

Here, $S_T = 1, \dots, T$ is the set of restoration time from 1 to T; S_{node} is the set of the communication nodes, S_{link} is the set of communication links. b_{nodei}^t is the binary variable of the $communication\ node_i$ at time t, 1 means the communication link is available, 0 means the opposite. Similarly, b_{linj}^t is the binary variable of communication link j at time t.

From (1) and (2), the BSC of a specific unit is determined by the status of u_{igen}^t of NBSUs. Therefore, the objective function is further simplified as:

$$\max \sum_{i \in S_{NBSU}} \sum_{t \in S_T} (C_i - P_i^c) u_{igen}^t + \sum_{t \in S_T, i \in S_{node,} j \in S_{link}} b_{nodei}^t + b_{linkj}^t \tag{4}$$

5.1.3 Constraints

1) Constraints for generator units

Considering the inherent properties of thermal generators, NBSU i exhibit a maximum allowable start-up time T_i^{max}. Furthermore, the unit must adhere to a minimum critical time period, T_i^{min} before initiating the cranking process.

$$t_i^{st} \leq T_i^{max} \qquad i \in S_g \tag{5}$$

$$t_i^{st} \geq T_i^{min} \tag{6}$$

Also, sufficient black-start capacity is necessary to fulfill the cranking power demands of NBSUs. S_{gen} is the set of generators.

$$\sum_{i \in S_{gen}} P_{igen}^t \geq 0 \qquad t \in S_T \tag{7}$$

2) Topological constraints for power system

The constraints (8)-(11) represent the transmission line and node energization constraints in a power system.

If a transmission line becomes energized at time t + 1, then a minimum of one connected bus must be energized at time t.

$$0 \leq u_{lineij}^{t+1} \leq u_{busi}^t + u_{busj}^t \quad t \in S_t,\ ij \in S_{line} \tag{8}$$

Where u_{lineij}^t means the the binary variable of power system line ij at time t, 1 means the line is energized, 0 means the opposite. Similarly, u_{busi}^t means the binary variable of power system bus i at time t, 1 means the bus is energized, 0 means the opposite.

If a non-black-start bus becomes energized at time t, then at least one of its connected transmission lines must be energized at the same time t.

$$u_{busi}^t \in \sum_{ij \in S_{line-busi}} u_{lineij}^t \tag{9}$$

A bus or a line will not be de-energized once it is energized.

$$u_{busi}^t \leq u_{busi}^{t+1} \tag{10}$$

$$u_{lineij}^t \leq u_{lineij}^{t+1} \tag{11}$$

3) Topological Constraints for Communication System

Likewise, the constraint of reestablishing communication links and nodes are characterized by the subsequent formulations. If a communication link is reconnected at time $t+1$, then a minimum of one connected communication node must be energized at time t.

$$b_{linkij}^{t+1} \leq b_{nodei}^{t} + b_{nodej}^{t} \tag{12}$$

In terms of the communication nodes that are not directedly connected with the power system bus, their availability at time t is contingent upon the presence of at least one operational network link connected to the node at time t.S_r is the set of communication nodes that are isolated from the power system bus. $S_{link-nodei}$ represents the set of the communication links that are connected to node i.

$$b_{nodei}^{t} \in \sum_{ij \in S_{link-nodei}} b_{linkij}^{t} \qquad i \in S_r \tag{13}$$

A communication node or link will not be disconnected once it is reenergized.

$$b_{nodei}^{t} \leq b_{nodei}^{t+1} \tag{14}$$

$$b_{linkij}^{t} \leq b_{linkij}^{t+1} \tag{15}$$

4) Interdependency constraints

The accessibility of the communication system is crucial for power system restoration, especially for power system buses located in remote areas. For the restoration of these buses, remotely controlling circuit breakers effectively minimizes delays by eliminating the need to dispatch crews to the field. In the proposed approach, generator buses do not require remote breaker operations, as on-site personnel are present. Constraints (16 and 17) illustrate the interdependence between the cyber system and the power system.

A non-generator bus is energized at t only if the communication node at that bus is available.

$$u_{ngi}^{t} \leq b_{nodei}^{t}, t \in [0, T] \tag{16}$$

In this paper, we assume that it takes time $T_{reconfig}$ for SDN controller to reconfigure the communication network infrastructure after a cyberattack. Here, $T_{reconfig}$ is predefined as a constant value.

$$\sum_{t \in S_t} b_{nodei}^{t} - \sum_{t \in S_t} u_{ngi}^{t} \geq T_{reconfig} \quad i \in S_{attack} \tag{17}$$

5.2 Cyber-power System Simulator for Constraint Check

The proposed optimization model generates an initial starting sequence for generators, power system buses, communication nodes, and links. However, the feasibility of the restoration sequence must be verified in both the cyber and power systems. If power flow constraints or communication network constraints are unmet, global optimality could be jeopardized. Consequently, a cyber-power system simulator, as depicted in Fig. 5.1, is deployed to assess feasibility for each time slot within the sequence.

5.2.1 Cyber-power System Simulator Set-up

The cyber-power system simulator consists of a power system simulator, SCADA simulator, and Open Platform Communications (OPC) server. In this paper, the IEEE 39-bus system is used to demonstrate the interaction between cyber and power systems. An SDN-based solution for cyber system recovery in the power grid is proposed. The proposed SDN-based communication network for IEEE 39 bus system is implemented in Mininet with limited bandwidth for each communication link. POX controller is utilized as SDN controller for the implementation of proposed cyber recovery applications. The network traffic analysis tool, sFlow, is built into Mininet to provide the real-time traffic visibility of the simulated network. Mininet, POX controller, and sFlow are installed on one virtual machine. The platform runs a 64-bit Ubuntu 19.3 with two virtual CPUs and 4GB of RAM. In order to analyze the interactions between the cyber system and power system, IEEE 39-bus power system is simulated in the power system simulator, DigSILENT 2018, which provides real-time responses from the physical system. The OPC server is used as the bridge between Mininet platform and DigSILENT for real-time data exchange. The power system simulator is installed in another virtual machine (2 virtual CPUs and 4 GB of RAM) that runs Windows 7.

5.2.2 SDN based SCADA Network

Currently, the smart grid communication network is built on various protocols and devices from different vendors, making network management a complex task. Thus, traditional approaches that

have been adopted to manage smart grid communications are not sufficient. As a programmable network infrastructure, an SDN based communication network can be integrated with a smart grid for flexible monitoring and control of the communication network. The motivation to utilize SDN based SCADA in terms of attack-resiliency includes [94]:

1) Based on the programmability of SDN WAN, the applications in a SCADA system can be customized to meet various communication requirements.

2) When the power system is under cyber threats, the centralized SDN controller with a global view enables attack detection and mitigation to be performed with a higher level of precision and visibility.

3) In case of a cyberattack or communication failure, a smart grid's capability to communicate and respond will be reduced. To restore the operations as soon as possible, the SDN based environment can adapt to the changing conditions of the communication network within a short period of time.

Note that in this case, the centralized SDN controller is trusted. Security measures for the SDN controller are assumed within the scope of this study.

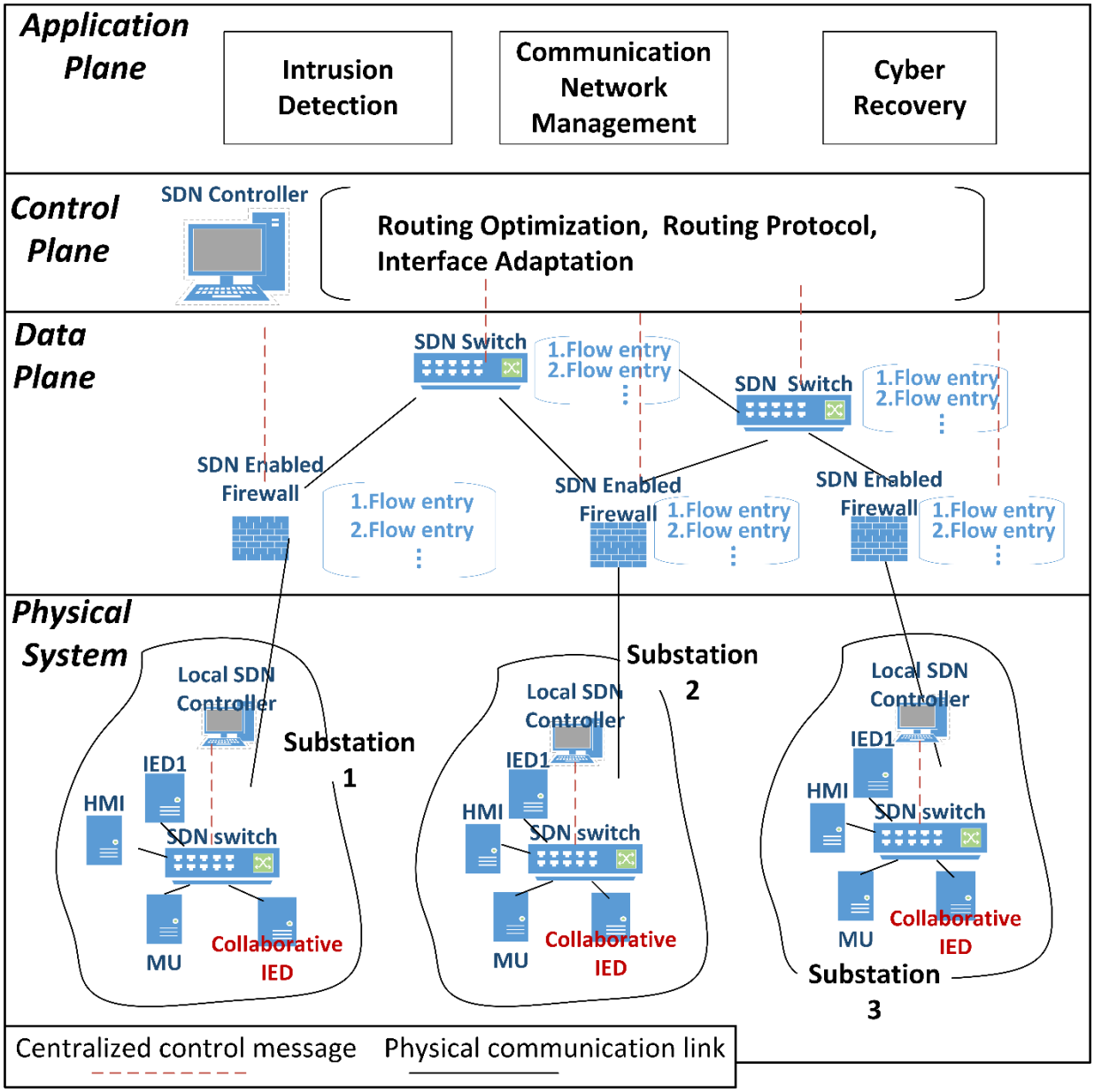


Figure 5.2 SDN based SCADA communication network

As depicted in Fig. 5.2, the proposed SDN-based SCADA system comprises four layers: the physical system layer, SDN data plane, SDN control plane, and SDN application plane. The SDN data plane, containing SDN-based network nodes, connects the physical power system to the SDN controller. Each substation or control center LAN in the power system is equipped with an SDN-enabled firewall, which uses a flow table to forward traffic to the next hop. At the SDN control plane, the centralized SDN controller connects the SDN-based nodes using the OpenFlow protocol [95]. The application plane is decoupled from the data plane through the SDN controller. In the

application layer, the centralized design of SDN enables complex and flexible applications, including Intrusion Detection Systems (IDS), network management, and cyber recovery. Additionally, as part of a hierarchical SDN-based communication infrastructure, there is a local SDN controller at each substation, which controls and monitors the IEC 61850-based substation LAN. The specific SDN scheme for the substation automation system is shown in [96].

Considering the communication demand of a modern power system, the proposed SCADA design for the IEEE 39 bus system is based on the network architecture illustrated in Fig. 5.3. In line with the existing utility network, the communication links between any two substations are sparse. However, in the near future, substations within the communication network will have direct connections with their neighboring substations. IEC 61850-90-5 has introduced a routable version of Sampled Values (SV)/Generic Object Oriented Substation Events (GOOSE) messages, termed R-SV/R-GOOSE, capable of supporting wide-area protection and control applications[97]. Therefore, in this paper, it is assumed that every substation can communicate with the neighboring substations using R-SV/R-GOOSE. As illustrated in Fig. 5.2, the access level includes an SDN-enabled firewall at each substation. At the core level, core nodes represent the sub-SCADA servers in the data center to which the edge switches are connected. It's important to note that the control center node in this communication network is represented by the t_2 core node.

A large-scale cyberattack targeting a power system can cause not only an outage but also corruption of the cyber system during the restoration of power systems. When the cyber system is compromised, communication capability can become a constraint for cyber-power system restoration. Therefore, to estimate the communication capacity of each link, an algorithm is deployed to construct the network according to the communication demands of a modern power system. The capacity of each communication link in the proposed network is determined based on the following optimization model. For a critical smart grid application, the communication demands of each substation are described in Table 5.1, which follows the requirements of QoS [98, 99]. In order to estimate the optimal capacity of the communication link, the objective of the algorithm is to minimize the cost in terms of the communication link capacity Y_e.

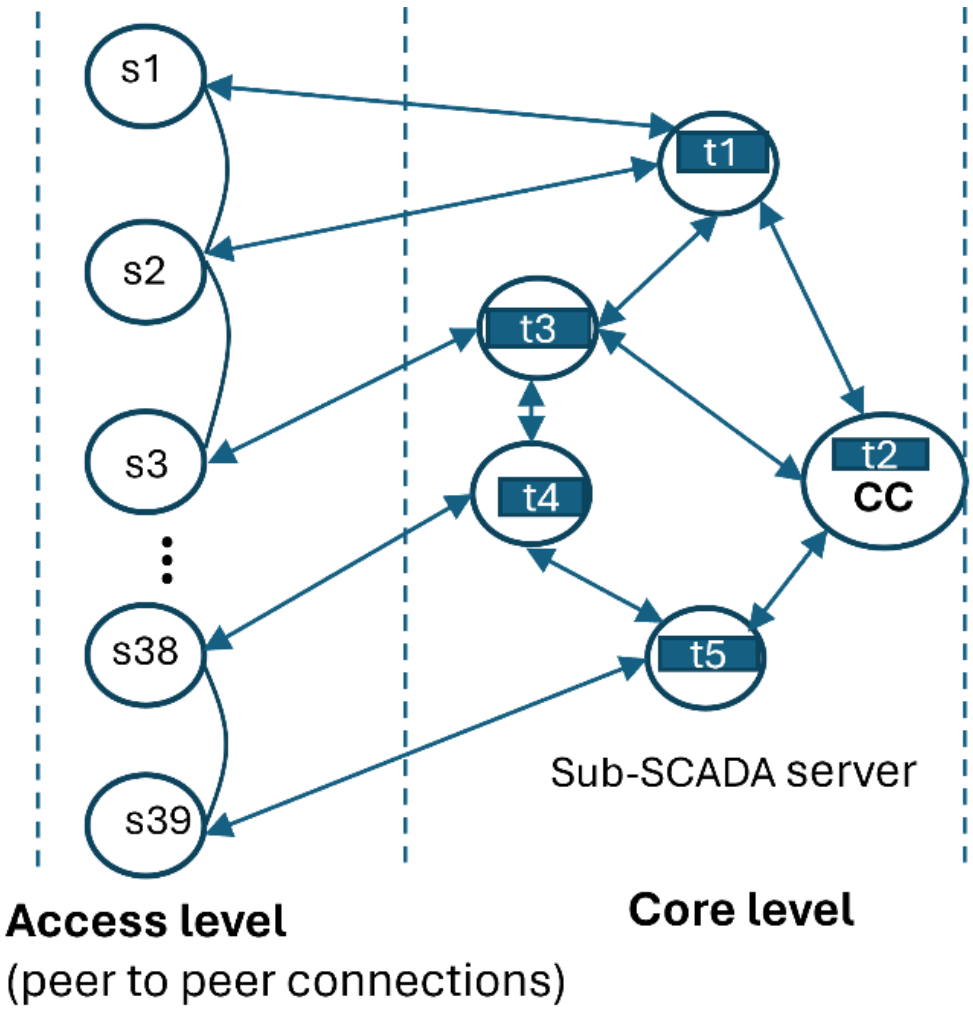


Figure 5.3 The proposed network architecture of IEEE 39-bus system

Objective: $\min \sum_{e \in E} Y_e$

$s.t.$

$$Y_e = C_e + y_e\,, \quad e \in E \tag{18}$$

$$\sum_{p \in Q_e} x_p \leq Y_e, \qquad e \in E \tag{19}$$

$$\sum_{p \in P_d} x_p = h_{d,} \qquad d \in D \tag{20}$$

$$x_p \in \{0, h_d\} \quad for\ all\ d \in D\ and\ p \in P_d \tag{21}$$

C_e is the pre-installed capacity, which is the average upstream bandwidth based on the daily traffic profile. D represents a set of point-to-point demands. For each demand $d \in D$, there is a set of candidate routes P_d between the end nodes.x_p is the traffic flow on route p. h_d is the traffic flow that has to be routed between the end nodes. In this case, h_d is assigned with the demand from each substation. Q_e denotes the set of routing paths traversing link $e \in E$ in the forward direction. Constraint (3) is the definition of communication link capacity Y_e. Constraint (4) limits the traffic flow on link e with line capacity Y_e. The demand between the end nodes h_d is defined by (5). Constraint (6) indicates that the traffic on each route is either 0 or the demand h_d. Based on the estimation of network capacity for IEEE 39-bus system, the proposed cyber-physical system restoration strategy is evaluated on the proposed network.

Table 5.1 Network requirements of smart grid applications

Application	**Data rate**
Protection	300kbps
SCADA	300kbps
Voice	1Mbps
Operational services (metering, fault reporting and event analysis)	10Mbps
Security (surveillance video)	25Mbps
PMU	3Mbps

5.2.3 Constraint Checking using Cyber-power System Simulator

Using the starting sequence from the optimization model, the on/off status of generators, buses, communication nodes, and links is determined for each time slot. Based on the status at each restoration step, the cyber-power system simulator can be reconfigured to perform constraint checks for both the power and cyber systems.

1) Power System Constraint Check

Based on the response from the power system simulator, the voltage status of the power system is determined through steady-state analysis. If the voltage constraint, e.g., 90% - 110%, is violated, the restoration planning will be adjusted using the following strategies: a) delaying the energization of specific buses connected to lengthy transmission lines; b) gradually restoring critical loads in accordance with generation capacity.

2) Cyber System Constraint Check

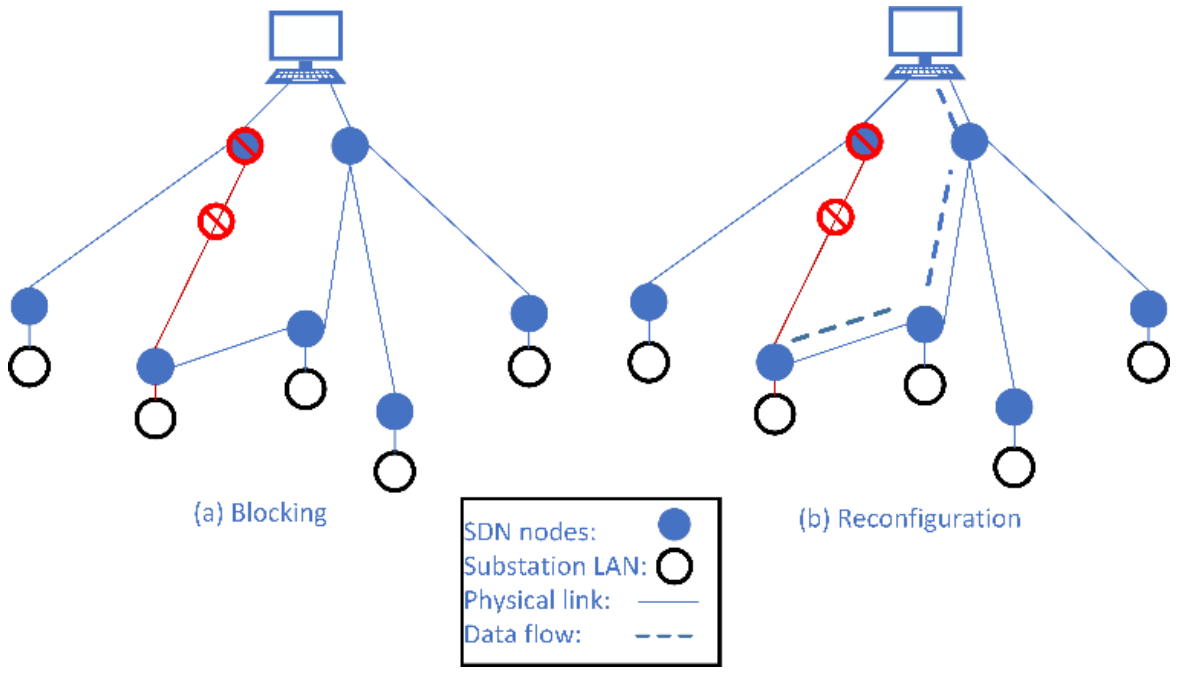


Figure 5.4 SDN based communication network recovery

With the status of communication nodes and links known, the SDN controller will reconfigure the communication network. First, the compromised communication link will be isolated to prevent any additional adverse impacts, as depicted in Fig. 5.4(a). Additionally, the source IP addresses of malicious traffic will be blocked through the SDN firewall. The containment strategy, which aims to drop incoming traffic from a specific port, can successfully reduce the chance of resource exhaustion.

The next stage of the proposed strategy involves recovering the communication network between the substations and the control center. SDN can significantly enhance network reconfiguration, especially in the context of recovering from a cyberattack and making changes to the network

infrastructure. Based on the ICT network topology, the adjacency matrix with network capacity will be updated by setting the capacity of the blocked edges to zero. The communication demand of each substation is estimated from the average hourly traffic, which varies depending on the time of day. It is important to note that if multiple substations are under a DDoS attack, the demands from these substations will saturate the capacity of some edges, as most communication links become unavailable during the isolation stage. Therefore, to recover the routing path for the substations, the problem can be formulated as a max flow problem with multiple sources and one sink as shown in Fig. 5.5.

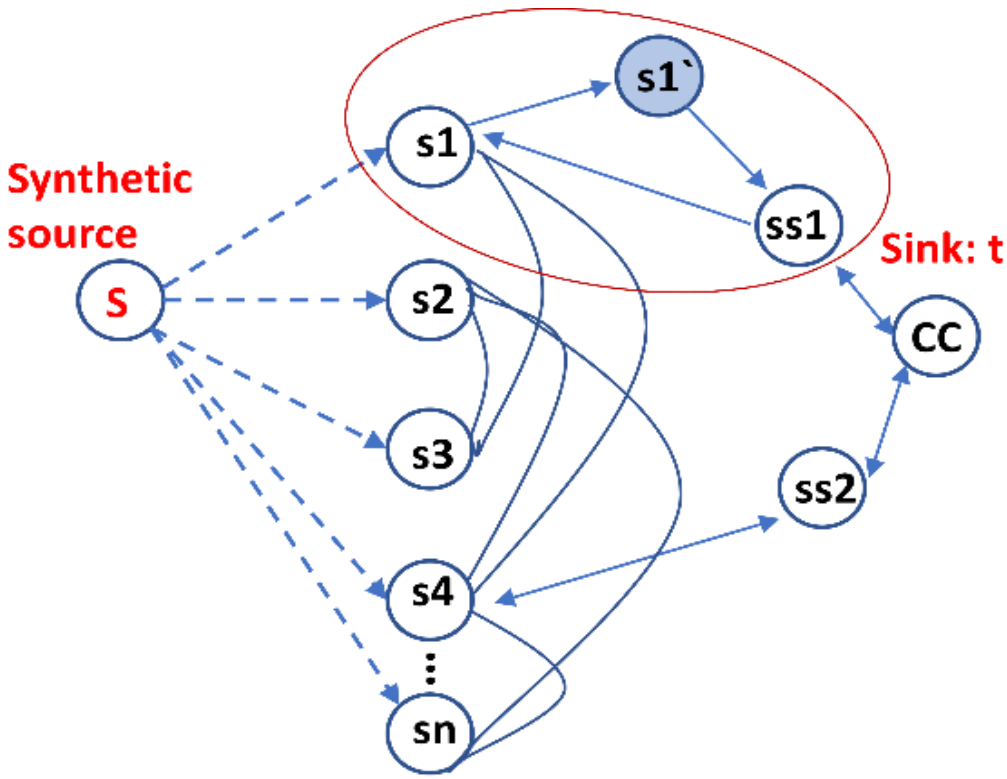


Figure 5.5 Max flow problem of proposed SDN

The communication demands of the substations from the SCADA system are represented by sources $s_1, s_2, \ldots, s_n$. The control center is the single sink cc in the network. To solve the max flow problem of the proposed network with multiple sources, a synthetic source s is added. The capacity between s and the real source is the demand of each substation. For instance, if the traffic from substation 1 to the control center is 9 Mbps at the present time, the capacity of the edge $s - s1$ is 9 Mbps. Some node pairs with a reversed edge (e.g., node s_1 and ss_1 in Fig. 5.5) are called anti-parallel edges. To eliminate anti-parallel edges, the pseudo node $s_1{}'$ shown in the red oval is

introduced. Note that the two edges $s_1 - s_1{}'$ and $s_1{}' - ss_1$ have the same capacity as the original $s_1 - ss_1$. By doing so, the problem is transformed to a single source single sink max flow problem of a directed capacitated network $G = (V, E, C)$, where V, E represents, respectively, the set of vertices and edges in the network. An element $e = (i, j)$ of E is an edge linking vertices i and j. An element c_{ij} of C represents the capacity of the edge.

Hence, the mathematical formulation of the problem is given:

$$\max \sum_{\{j|(s,j) \in E\}} x_{sj}$$

$$s.t \sum_{\{\, l|(l,i) \in E \,\}} x_{li} - \sum_{\{\, j|(i,j) \in E \,\}} x_{ij} = 0 \quad \forall\, i \neq s, t \tag{22}$$

$$0 \leq x_{ij} \leq c_{ij} \quad \forall\, (i,j) \in E \tag{23}$$

where x_{ij} represents the traffic throughput on edge $e(i,j)$. Here, the max flow problem is formulated as standard linear programming to maximize the flow from the source. Constraint

(1) shows that incoming traffic equals outgoing traffic at each vertex. Constraint (2) indicates that the edge traffic must not exceed the capacity. To reduce the computational time, an iterative algorithm is used to solve the problem in stages and output the traffic path for each substation. The algorithm of Edmonds and Karp [100] is implemented to search for the shortest augmenting path using Breadth-First Search (BFS). Different from the original BFS, the algorithm in this paper not only provides the maximum traffic flow from the substations to the control center, but also exports the optimal traffic for each source. As shown in Algorithm 1, with the calculated traffic path for each substation, the SDN controller is able to reconfigure the routing path from substations to the control center and show the maximum flow from the substation to the control center.

Algorithm1: Edmonds and Karp algorithm to determine the optimal path for each source

Input: graph, source, sink

Output: all paths from source to sink, max flow from source to sink
Initialize flow from source: max_flow = 0

Initialize a list to store all paths from source to sink: path_store = list()

```
Repeat
        BFS search of the graph
    Update the topological order of the vertices
        Initialize flow for current path: path_flow =∞
    Initialize stack to store vertex along the path in reverse      order: path_vertices = stack()
        for each vertex backtrack from sink to source
                Add the vertex to path_vertices
                Update path_flow
        end
        Update path_store using vertices in path_vertices
        Update max_flow using path_flow
    for each vertex backtrack from sink to source
                Update graph edge weight using path_flow
        end
Until no new path was found by BFS
```

Considering the limited bandwidth of the SCADA system and the severe impact of a DDoS attack targeting multiple substations, the upstream traffic from some substations needs to be split at certain SDN switches according to the traffic path derived from Algorithm 1. Consequently, SDN load balancing as a traffic forwarding application is deployed at each OpenFlow Switch to control the data path accordingly [101].

Note that if multiple substations are under a DDoS attack, the demands from these situations will saturate the capacity of some edges, as most communication links become unavailable during the isolation stage. The proposed method recovers the routing path for each substation by systematically maximizing the traffic flow from substations to the control center. If simulation results indicate that some substations cannot fully transmit their communication demands, this

signifies a violation of the communication system constraint. In such instances, the recovery time for the affected communication nodes should be postponed. Consequently, the energization of the corresponding power system buses should also be delayed.

5.3 Simulation Results

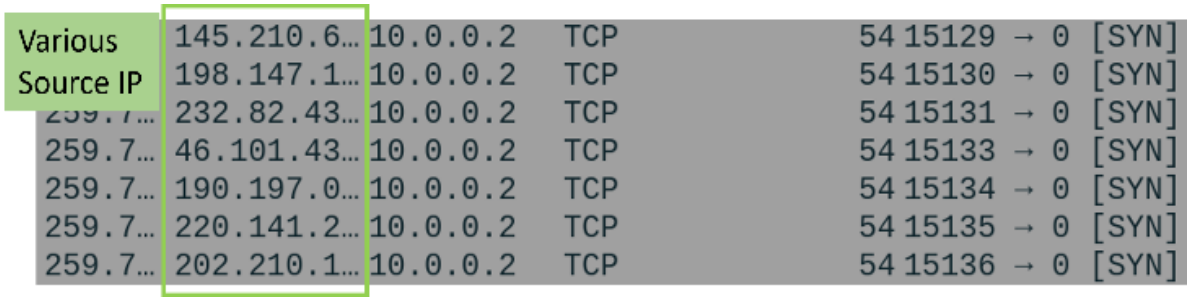


Figure 5.6 Traffic of the flooding attack against substation 2 (10.0.0.2)

During the cyberattack on the Ukrainian power grid, attackers utilized the BlackEnergy3 malware to maliciously intrude into the ICS network and inject false commands into multiple substations. Concurrently, a DoS attack was initiated on the telephone system, hindering power system restoration efforts [102]. In this study, a sophisticated attack similar to real-world incidents is simulated on the IEEE 39-Bus system using the proposed co-simulator to validate the efficacy of the suggested cyber-power system restoration strategy. In the simulation, falsified commands are sent to buses 3, 6, 15, 12, 19, and 26 to trip the circuit breakers via malicious access to the SCADA network. Simultaneously, DDoS attacks were executed using SYN flooding attacks aimed at Intelligent Electronic Devices (IEDs) utilizing the Distributed Network Protocol (DNP3) across several substations.

The screenshot from Wireshark shown in Fig. 5.6 depicts the malicious traffic during the attack. The traffic floods the IED at substation 2 with TCP SYN packets originating from millions of distinct source IP addresses, simulating a DDoS attack launched from multiple attack servers. In this case, the communication links with abnormal traffic include s2-t1, s4-t2, s5-t2, s6-t3, and s7-t3. Following the SDN strategy depicted in Fig. 5.4(a), the compromised communication links will be isolated to mitigate the impact of the cyberattacks as quickly as possible. Consequently, the state of the communication network after the blocking process serves as the initial condition for the proposed restoration algorithm. As the power system collapsed following the cyberattacks, the initial status of the power system in the proposed restoration plan is a complete blackout.

With the information provided in [103], there are 10 generators in the IEEE 39-bus system and G10 serves as BSU to crank the other 9 NBSUs in the restoration process. The starting time of BSU is designated as the beginning of the proposed restoration process, meaning G10 will be energized at $time = 0$. The restoration state is updated every 10 minutes; therefore, the time's per unit value is 10 minutes.

Iteration 1:

Table 5.2 The power system restoration schedule at Iteration 1

0	3	4	5	6
G10	B30	B2	B25,B1	B37,B39
7	8	9	10	11
G8,B3, B26, G1	B4,B18	B17,b15	B6, B16	B11, B31,B19, B24
12	13	14	15	
G2,B29,B10,B20,B33 B23	B38,B32, B34, G4, B22, B36	G3 ,G5, G7, B35, G9	G6	

The initial restoration sequence is shown as Iteration1 in Table 5.2. As the reconfiguration of the SDN-based firewall at the compromised substations takes 1 hour, bus 3 and 26 are energized at Step 7 which is after the router reconfiguration. By using the proposed cyber-physical system simulation, each restoration step is evaluated. At Step 4, the communication network is congested because of the limited bandwidth after the compromised communication links are blocked. As shown in the following figure, the optimal data paths are determined via the proposed algorithm, however, the total traffic from the substations to the control center is lower than the required demand, and only 2Mbps is sent out from substation 2 to the control center which is lower than

the normal communication traffic (9Mbps). Therefore, the energized time for bus 2 should be postponed by 1 hour. The restoration algorithm will be recalculated.

```
The maximum possible flow from source to sink is 107Mbpb
all stored paths:
('0->2->9->1->8', 2)
```

Figure 5.7 Routing path for substation 2

Iteration 2:

Table 5.3 The power system restoration sequence at Iteration 2

0	3	4	5	6
G10	B30			
7	8	9	10	11
B2	B25	B39,b37,b26	B3, G1	B4,B18
12	13	14	15	16
B17,b15	B6, B16	B11, B31,B19, B24	G2,B29,B10,B20,B33 B23, B38, G8	B32, B34, G4, B22, B36
17	18	19	20	
G3 ,G5, G7, B35, G9	G6	B39	G1	

The restoration sequence of power system buses at Iteration 2 is shown in Table 5.3. With the communication end points at Bus 3, 26, 15, 6, and 19 are recovered after t=6pu., the communication paths for those nodes are determined based on the proposed algorithm. By using

the cyber-physical system simulation for validating the criteria at each restoration step, the communication at b2 is reconfigured by SDN with no communication link saturated. At step 9, there is overvoltage at bus 26, therefore, loads at Bus 25 and 26 are picked up. At step 11, the simulation results shows there is overvoltage at bus 4 and 18, therefore, picking up loads at bus 4 and 18. At step 15, there is overvoltage at bus 29 and 38, therefore, the paralleling of G8 needs to be postponed. Therefore, adding additional constraint: $t_{G8} \geq 16$.

Iteration 3:

Table 5.4 The power system restoration sequence at Iteration 3

0	3	4	5	6
G10	B30			
7	8	9	10	11
B2	B25	B39,b37,b26	B3, G1	B4,B18
12	13	14	15	16
B17,b15	B6, B16	B11, B31,B19, B24	G2,B29,B10,B20,B33 B23, B38	B32, B34, G4, B22, B36, G8
17	18	19	20	
G3 ,G5, G7, B35, G9	G6	B39	G1	

The final restoration sequence is shown in Table 5.4. At this iteration, the communication system is fully restored except for the blocked communication links. With the restoration sequences in Table 5.4, all NBSUs are cranked, and the essential transmission paths are established in parallel.

As shown in Figure 5.8, under the same attack, the orange curve depicts the restoration of generation capability without the proposed co-restoration method. Should there be any rapid recovery for the communication at bus 2, a crew would need to be dispatched to the substation to manually operate the breakers, which would take 12 units of time. However, with the co-restoration strategy, the NBSUs can be activated earlier, as shown by the blue curve.

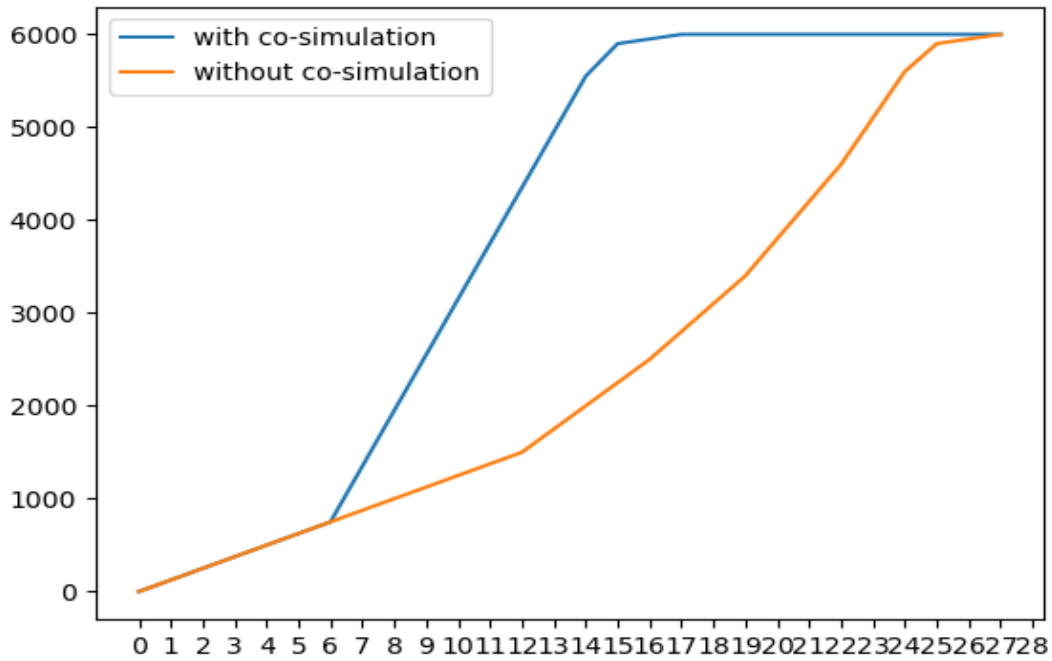


Figure 5.8 The restoration process under attack with/without the proposed co-restoration strategy

The proposed co-restoration strategy not only reduces restoration time for power system buses but also enhances transient stability during power system restoration. Further analysis can be done by comparing the dynamic response at each restoration step with and without the proposed strategy.

5.4 Conclusion

In this work, a cyber-power system restoration strategy under large-scale cyberattack is discussed. Considering the interaction between cyber and power systems, the co-restoration strategy is proposed with two layers of applications: optimization based cyber-power system restoration algorithm and cyber-power system simulation for constraint check. To validate the proposed strategy, the SDN-based communication network of the IEEE 39-bus system is designed and

implemented. The test results show the capabilities of the proposed restoration planning method, (a) cyber system and power system are restored parallelly, (b) by utilizing the cyber system recovery, the restoration time for power system is reduced, (c) With the mitigation methods, the impact of the large-scale cyberattack has been contained. For future work, battery storage should be considered in the proposed cyber-power system restoration strategy.

Chapter 6
Conclusion and Future Work

6.1 Conclusion

This dissertation is concerned with the intrusion detection and recovery of a cyber-power system, highlighting the critical interdependency between cybersecurity and the reliable operation of the physical power grid. Through analysis and the development of innovative detection and recovery strategies, this research makes important contributions to the understanding and enhancement of cyber-power system resilience.

The study began by outlining the theoretical framework for intrusion detection, which served as a foundation for the subsequent exploration of detection techniques and recovery mechanisms. The dissertation reports the results of a holistic exploration into intrusion detection and recovery of cyber-power systems, addressing critical vulnerabilities at the substation level and proposing effective strategies for system-wide recovery in the aftermath of cyberattacks. Through a methodical study, this research establishes a robust framework for securing power system against sophisticated cyber threats, thereby contributing significantly to the field of cyber-physical system security.

The initial phase of the research establishes the pathways for measurement attacks at the substation level, resulting in a novel IDS characterized by high detection accuracy under the conditions of low- and high-speed traffic of measurement messages. Proactive detection within substations is crucial, effectively mitigating the risk of falsified measurements impacting the broader system

operations at the control center. The validation of this IDS through simulation with realistic attack scenarios underscores its efficacy and practicality for deployment in existing substation networks. Subsequent investigations involve the development of cyber system recovery strategies, first at the substation level, then expanding to address large-scale cyberattacks on the power system. The dissertation outlines a two-step recovery process—isolation and recovery—based on IDS-generated security information. This process is demonstrated to effectively restore substation functionality with an emphasis on the compatibility with IEC 61850 based Substation Automation Systems (SAS) through SDN-based simulation tests.

In further extensions, the research then proposes a novel SDN-based recovery strategy aimed at minimizing the attack surface, restoring the cyber infrastructure of the power system, and preventing future attacks. This comprehensive approach is validated using the IEEE 39-bus system as a model to demonstrate the strategy's effectiveness in not only recovering from large-scale cyberattacks but also in bolstering the system's resilience against future threats.

This research culminates in a co-restoration strategy for cyber-power systems under the threat of large-scale cyberattacks. By considering the interdependencies between cyber and power systems, the dissertation proposes a two-layered approach that includes an optimization-based restoration algorithm and a simulation for constraint checking. This strategy is validated through the implementation of an SDN-based communication network for the IEEE 39-bus system that enables the parallel restoration of cyber and power systems, leading to reduce restoration time due to cyber system recovery and effective mitigation of the cyberattack.

6.2 Future Work

To improve the proposed work in this dissertation, here are recommendations for the next to enhance the security and resilience of cyber-power systems:

Collaborative IDS Across Substations:

Future research should look into the development and implementation of collaborative IDS frameworks that enable real-time communication and data sharing among substations. By leveraging distributed IDSs that operate collaboratively, the detection process can be significantly improved through the collective analysis of threat patterns and anomalies across the network. Studies can focus on developing algorithms for efficient data fusion and threat intelligence sharing to achieve privacy-preserving mechanisms while enhancing overall system security.

Distributed Cyber System Restoration for Multiple Substations:

Expanding the cyber system restoration process to encompass multiple substations is a critical area for the future work. This involves creating a robust framework for secured communication between substations, enabling a distributed and coordinated restoration effort. Research should focus on designing scalable protocols that can manage the restoration process across a wide network of substations to minimize the disruption to system operations.

Cyber Recovery Strategies for Other Critical Infrastructure:

The extension of cyber recovery strategies to other critical components of the power grid, such as distributed energy resources (DERs) and smart meters, is essential. Future investigations should explore the unique vulnerabilities and attack surfaces associated with these components and develop recovery strategies that can be integrated into the power grid recovery plan. This research should also consider the increasing DERs and the role of smart meters in grid management,

emphasizing the need for a resilient recovery approach that can adapt to the dynamic nature of the smart grid.

Incorporation of Battery Storage in Cyber-Power System Restoration:

Considering battery storage in the cyber-power system restoration strategy presents an innovative direction for the future work. Battery storage systems play a crucial role in providing backup power and facilitating the integration of renewable energy sources. Future research should investigate how battery storage can be leveraged during and after cyberattacks to support recovery efforts and minimize service disruption. This involves developing algorithms that dynamically manage battery storage resources in response to cyber incidents.

References

[1] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Computing Surveys (CSUR)*, vol. 41, no. 3, pp. 1-58, 2009.

[2] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 5-20, 2012.

[3] N. Kush, E. Foo, E. Ahmed, I. Ahmed, and A. Clark, "Gap analysis of intrusion detection in smart grids," 2011.

[4] *IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)*, IEEE Std 1815-2012, IEEE, 2012.

[5] A. Swales, "Open modbus/tcp specification," *Schneider Electric*, vol. 29, no. 3, p. 19, 1999.

[6] S. E. Quincozes, C. Albuquerque, D. Passos, and D. Mossé, "A survey on intrusion detection and prevention systems in digital substations," *Computer Networks*, vol. 184, p. 107679, 2021.

[7] R. Amoah, S. Camtepe, and E. Foo, "Securing DNP3 broadcast communications in SCADA systems," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 4, pp. 1474-1485, 2016.

[8] M. Strobel, N. Wiedermann, and C. Eckert, "Novel weaknesses in IEC 62351 protected smart grid control systems," in *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2016: IEEE, pp. 266-270.

[9] U. Adhikari, T. Morris, and S. Pan, "WAMS cyber-physical test bed for power system, cybersecurity study, and data mining," *IEEE Transactions on Smart Grid*, vol. 8, no. 6, pp. 2744-2753, 2016.

[10] A. Almalawi, A. Fahad, Z. Tari, A. Alamri, R. AlGhamdi, and A. Y. Zomaya, "An efficient data-driven clustering technique to detect attacks in SCADA systems," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 893-906, 2015.

[11] E. G. da Silva, A. S. da Silva, J. A. Wickboldt, P. Smith, L. Z. Granville, and A. Schaeffer-Filho, "A one-class NIDS for SDN-based SCADA systems," in *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, 2016, vol. 1: IEEE, pp. 303-312.

[12] M. N. Kurt, O. Ogundijo, C. Li, and X. Wang, "Online cyber-attack detection in smart grid: A reinforcement learning approach," *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5174-5185, 2018.

[13] L. A. Maglaras, J. Jiang, and T. J. Cruz, "Combining ensemble methods and social network metrics for improving accuracy of OCSVM on intrusion detection in SCADA systems," *Journal of Information Security and Applications*, vol. 30, pp. 15-26, 2016.

[14] R. Samdarshi, N. Sinha, and P. Tripathi, "A triple layer intrusion detection system for SCADA security of electric utility," in *2015 annual IEEE India conference (INDICON)*, 2015: IEEE, pp. 1-5.

[15] K. Stefanidis and A. G. Voyiatzis, "An HMM-based anomaly detection approach for SCADA systems," in *Information Security Theory and Practice: 10th IFIP WG 11.2 International Conference, WISTP 2016, Heraklion, Crete, Greece, September 26–27, 2016, Proceedings 10*, 2016: Springer, pp. 85-99.

[16] M. A. Teixeira, T. Salman, M. Zolanvari, R. Jain, N. Meskin, and M. Samaka, "SCADA system testbed for cybersecurity research using machine learning approach," *Future Internet*, vol. 10, no. 8, p. 76, 2018.

[17] K. Choi, X. Chen, S. Li, M. Kim, K. Chae, and J. Na, "Intrusion detection of NSM based DoS attacks using data mining in smart grid," *Energies*, vol. 5, no. 10, pp. 4091-4109, 2012.

[18] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 847-855, 2013.

[19] A. G. Wermann, M. C. Bortolozzo, E. G. da Silva, A. Schaeffer-Filho, L. P. Gaspary, and M. Barcellos, "ASTORIA: A framework for attack simulation and evaluation in smart grids," in *NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium*, 2016: IEEE, pp. 273-280.

[20] S. Ghosh and M. H. Ali, "Impact of crash override and tampering communication data cyber-attacks on the power quality of the hybrid system," in *2018 IEEE International Conference on Power Electronics, Drives and Energy Systems (PEDES)*, 2018: IEEE, pp. 1-5.

[21] D. An, Q. Yang, W. Liu, and Y. Zhang, "Defending against data integrity attacks in smart grid: A deep reinforcement learning-based approach," *IEEE Access*, vol. 7, pp. 110835-110845, 2019.

[22] A. Anwar, A. N. Mahmood, and Z. Tari, "Identification of vulnerable node clusters against false data injection attack in an AMI based smart grid," *Information Systems*, vol. 53, pp. 201-212, 2015.

[23] J. M. Beaver, R. C. Borges-Hink, and M. A. Buckner, "An evaluation of machine learning methods to detect malicious SCADA communications," in *2013 12th International Conference on Machine Learning and Applications*, 2013, vol. 2: IEEE, pp. 54-59.

[24] K. Demertzis and L. Iliadis, "A computational intelligence system identifying cyber-attacks on smart energy grids," *Modern Discrete Mathematics and Analysis: with Applications in Cryptography, Information Systems and Modeling*, pp. 97-116, 2018.

[25] H. do Nascimento Alves, N. G. Bretas, A. S. Bretas, and B.-H. Matthews, "Smart grids false data injection identification: a deep learning approach," in *2019 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, 2019: IEEE, pp. 1-5.

[26] D. I. Dogaru and I. Dumitrache, "Cyber security of smart grids in the context of big data and machine learning," in *2019 22nd International Conference on Control Systems and Computer Science (CSCS)*, 2019: IEEE, pp. 61-67.

[27] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Systems Journal*, vol. 11, no. 3, pp. 1644-1652, 2014.

[28] S. A. Foroutan and F. R. Salmasi, "Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method," *IET Cyber‐Physical Systems: Theory & Applications*, vol. 2, no. 4, pp. 161-171, 2017.

[29] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2505-2516, 9/2017, doi: 10.1109/TSG.2017.2703842.

[30] R. C. B. Hink, J. M. Beaver, M. A. Buckner, T. Morris, U. Adhikari, and S. Pan, "Machine learning for power system disturbance and cyber-attack discrimination," in *2014 7th International Symposium on Resilient Control Systems (ISRCS)*, 2014: IEEE, pp. 1-8.

[31] M. Keshk, N. Moustafa, E. Sitnikova, and G. Creech, "Privacy preservation intrusion detection technique for SCADA systems," in *2017 Military Communications and Information Systems Conference (MilCIS)*, 2017: IEEE, pp. 1-6.

[32] L. A. Maglaras and J. Jiang, "Intrusion detection in SCADA systems using machine learning techniques," in *2014 Science and Information Conference*, 2014: IEEE, pp. 626-631.

[33] S. Pan, T. Morris, and U. Adhikari, "Developing a hybrid intrusion detection system using data mining for power systems," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 3104-3113, 2015.

[34] R. Berthier and W. H. Sanders, "Specification-based intrusion detection for advanced metering infrastructures," in *2011 IEEE 17th Pacific Rim International Symposium on Dependable Computing*, 2011: IEEE, pp. 184-193.

[35] O. Linda, M. Manic, T. Vollmer, and J. Wright, "Fuzzy logic based anomaly detection for embedded network security cyber sensor," in *2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS)*, 2011: IEEE, pp. 202-209.

[36] S. Shin, T. Kwon, G.-Y. Jo, Y. Park, and H. Rhy, "An experimental study of hierarchical intrusion detection for wireless industrial sensor networks," *IEEE Transactions On Industrial Informatics*, vol. 6, no. 4, pp. 744-757, 2010.

[37] Y. Yang *et al.*, "Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid SCADA systems," *International Conference on Sustainable*

Power Generation and Supply (SUPERGEN 2012), Hangzhou, 2012, pp. 1-8, doi: 10.1049/cp.2012.1831. 2012.

[38] R. Vijayanand, D. Devaraj, and B. Kannapiran, "Support vector machine based intrusion detection system with reduced input features for advanced metering infrastructure of smart grid," in *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2017: IEEE, pp. 1-7.

[39] M. Ma, P. Zhou, D. Du, C. Peng, M. Fei, and H. M. AlBuflasa, "Detecting replay attacks in power systems: A data-driven approach," in *Advanced Computational Methods in Energy, Power, Electric Vehicles, and Their Integration: International Conference on Life System Modeling and Simulation, LSMS 2017 and International Conference on Intelligent Computing for Sustainable Energy and Environment, ICSEE 2017, Nanjing, China, September 22-24, 2017, Proceedings, Part III*, 2017: Springer, pp. 450-457.

[40] T.-T. Tran, O.-S. Shin, and J.-H. Lee, "Detection of replay attacks in smart grid systems," in *2013 International Conference on Computing, Management and Telecommunications (ComManTel)*, 2013: IEEE, pp. 298-302.

[41] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 411-423, 2017, doi: 10.1109/TII.2016.2614396.

[42] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," (in en), *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 1-33, 05/2011 2011, doi: 10.1145/1952982.1952995.

[43] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Transactions on Smart Grid,* vol. 2, no. 4, pp. 645-658, 2011, doi: 10.1109/TSG.2011.2163807.

[44] 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.

[45] B. Chen, H. Li, and B. Zhou, "Real-time identification of false data injection attacks: A novel dynamic-static parallel state estimation based mechanism," *IEEE Access,* vol. 7, pp. 95812-95824, 2019, doi: 10.1109/ACCESS.2019.2929785.

[46] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Transactions on Smart Grid,* vol. 2, no. 2, pp. 326-333, 6/2011 2011, doi: 10.1109/TSG.2011.2119336.

[47] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks," *IEEE Transactions on Smart Grid,* vol. 4, no. 3, pp. 1244-1253, 9/2013 2013, doi: 10.1109/TSG.2013.2245155.

[48] J. Zhao, G. Zhang, and R. A. Jabr, "Robust detection of cyber attacks on state estimators using phasor measurements," *IEEE Transactions on Power Systems,* vol. 32, no. 3, pp. 2468-2470, 5/2017 2017, doi: 10.1109/TPWRS.2016.2603447.

[49] Y. Wang, M. M. Amin, J. Fu, and H. B. Moussa, "A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids," *IEEE Access,* vol. 5, pp. 26022-26033, 2017 2017, doi: 10.1109/ACCESS.2017.2769099.

[50] Z. Wang, Y. Chen, F. Liu, Y. Xia, and X. Zhang, "Power system security under false data injection attacks with exploitation and exploration based on reinforcement learning," *IEEE Access,* vol. 6, pp. 48785-48796, 2018 2018, doi: 10.1109/ACCESS.2018.2856520.

[51] *Power Systems Management and Associated Information Exchange -Data and Communications Security - Part 6: Security for IEC 61850, 1.0.*, IEC 62351-6, 2007.

[52] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Transactions on Power Systems,* vol. 23, no. 4, pp. 1836-1846, 11/2008 2008, doi: 10.1109/TPWRS.2008.2002298.

[53] N. Liu, J. Zhang, and X. Wu, "Asset analysis of risk assessment for IEC 61850-based power control systems—Part I: Methodology," *IEEE Transactions on Power Delivery,* vol. 26, no. 2, pp. 869-875, 04/2011 2011, doi: 10.1109/TPWRD.2010.2090950.

[54] U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh, and J.-C. Tan, "An intrusion detection system for IEC61850 automated substations," *IEEE Transactions on Power Delivery,* vol. 25, no. 4, pp. 2376-2383, 10/2010 2010, doi: 10.1109/TPWRD.2010.2050076.

[55] Y. Yang, H.-Q. Xu, L. Gao, Y.-B. Yuan, K. McLaughlin, and S. Sezer, "Multidimensional intrusion detection system for IEC 61850-based SCADA networks," *IEEE Transactions on Power Delivery,* vol. 32, no. 2, pp. 1068-1078, 4/2017 2017, doi: 10.1109/TPWRD.2016.2603339.

[56] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. Nai Fovino, and A. Trombetta, "A multidimensional critical state analysis for detecting intrusions in SCADA systems," *IEEE Transactions on Industrial Informatics,* vol. 7, no. 2, pp. 179-186, 05/2011 2011, doi: 10.1109/TII.2010.2099234.

[57] C.-W. Ten, J. Hong, and C.-C. Liu, "Anomaly detection for cybersecurity of the substations," *IEEE Transactions on Smart Grid,* vol. 2, no. 4, pp. 865-873, 12/2011 2011, doi: 10.1109/TSG.2011.2159406.

[58] J. Hong, C.-C. Liu, and M. Govindarasu, "Integrated anomaly detection for cyber security of the substations," *IEEE Transactions on Smart Grid,* vol. 5, no. 4, pp. 1643-1653, 7/2014 2014, doi: 10.1109/TSG.2013.2294473.

[59] 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.

[60] M. Touhiduzzaman, A. Hahn, and A. K. Srivastava, "A Diversity-based substation cyber defense strategy utilizing coloring games," *IEEE Transactions on Smart Grid,* vol. 10, no. 5, pp. 5405-5415, 9/2019 2019, doi: 10.1109/TSG.2018.2881672.

[61] R. Macwan *et al.*, "Collaborative defense against data injection attack in IEC61850 based smart sbstations," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*, 7/2016 2016, Boston, MA, USA: IEEE, pp. 1-5, doi: 10.1109/PESGM.2016.7741376.

[62] S. Sheng, W. L. Chan, K. K. Li, D. Xianzhong, and Z. Xiangjun, "Context information-based cyber security defense of protection system," *IEEE Transactions on Power Delivery,* vol. 22, no. 3, pp. 1477-1481, 07/2007 2007, doi: 10.1109/TPWRD.2006.886775.

[63] S. Kwon, H. Yoo, and T. Shon, "IEEE 1815.1-based power system security with bidirectional RNN-based network anomalous attack detection for cyber-physical system," *IEEE Access,* vol. 8, pp. 77572-77586, 2020 2020, doi: 10.1109/ACCESS.2020.2989770.

[64] O. Duman, M. Ghafouri, M. Kassouf, R. Atallah, L. Wang, and M. Debbabi, "Modeling supply chain attacks in IEC 61850 substations," in *2019 IEEE International Conference on*

Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), 2019: IEEE, pp. 1-6.

[65] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues in Information Warfare & Security Research*, vol. 1, no. 1, p. 80, 2011.

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

[67] J. Guo, F. Liu, J. Wang, J. Lin, and S. Mei, "Toward efficient cascading outage simulation and probability analysis in power systems," *IEEE Transactions on Power Systems*, vol. 33, no. 3, pp. 2370-2382, 2018.

[68] 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.

[69] J. Hong, C. Liu, and M. Govindarasu, "Detection of cyber intrusions using network-based multicast messages for substation automation," in *ISGT 2014*, 19-22 Feb. 2014 2014, pp. 1-5, doi: 10.1109/ISGT.2014.6816375.

[70] 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.

[71] 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.

[72] 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.

[73] 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.

[74] 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.

[75] N. U. Ibne Hossain, M. Nagahi, R. Jaradat, C. Shah, R. Buchanan, and M. Hamilton, "Modeling and assessing cyber resilience of smart grid using Bayesian network-based approach: a system of systems problem," *Journal of Computational Design and Engineering,* vol. 7, no. 3, pp. 352-366, 2020, doi: 10.1093/jcde/qwaa029.

[76] K. Lai, M. Illindala, and K. Subramaniam, "A tri-level optimization model to mitigate coordinated attacks on electric power systems in a cyber-physical environment," *Applied Energy,* vol. 235, pp. 204-218, 2019.

[77] D. Jin *et al.*, "Toward a cyber resilient and secure microgrid using software-defined networking," *IEEE Transactions on Smart Grid,* vol. 8, no. 5, pp. 2494-2504, 2017.

[78] H. Lin *et al.*, "Self-healing attack-resilient PMU network for power system operation," *IEEE Transactions on Smart Grid,* vol. 9, no. 3, pp. 1551-1565, 2016.

[79] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "A cyber-attack resilient distributed control strategy in islanded microgrids," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 3690-3701, 2020.

[80] S. N. Edib, Y. Lin, V. M. Vokkarane, F. Qiu, R. Yao, and B. Chen, "Cyber restoration of power systems: Concept and methodology for resilient observability," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2023.

[81] 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.

[82] J. Li, H. Li, H. Wang, and Q. Su, "Actuator attack detection and power balance for cyber physical power systems," *IET Control Theory & Applications*, vol. 17, no. 6, pp. 776-787, 2023.

[83] J. Slowik, "CRASHOVERRIDE: Reassessing the 2016 Ukraine electric power event as a protection-focused attack," *Dragos, Washington, DC, USA, Tech. Rep., Aug*, 2019.

[84] "IEEE standard for exchanging information between networks implementing IEC 61850 and IEEE Std 1815(TM) [Distributed Network Protocol (DNP3)]," IEEE 1815.1-2015 2015.

[85] R. Minkner and E. O. Schweitzer, "Low power voltage and current transducers for protecting and measuring medium and high voltage systems," in *Western Protective Relay Conference, Spokane, WA*, 1999.

[86] L. Sevov, Z. Zhang, I. Voloh, and J. Cardenas, "Differential protection for power transformers with non-standard phase shifts," in *2011 64th Annual Conference for*

Protective Relay Engineers, 11-14 April 2011 2011, pp. 301-309, doi: 10.1109/CPRE.2011.6035631.

[87] "Communication networks and systems for power utility automation - Part 90-5: Use of IEC 61850 to Transmit Synchrophasor Information According to IEEE C37.118," IEC TR 61850-90-5:2012 2012.

[88] F. H. Branin, "Computer methods of network analysis," *Proceedings of the IEEE*, vol. 55, no. 11, pp. 1787-1801, 1967, doi: 10.1109/PROC.1967.6010.

[89] 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.

[90] 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.

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

[92] 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.

[93] Y. Jiang *et al.*, "Blackstart capability planning for power system restoration," *International Journal of Electrical Power & Energy Systems*, vol. 86, pp. 127-137, 2017/03/01/ 2017, doi: https://doi.org/10.1016/j.ijepes.2016.10.008.

[94] D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: a comprehensive survey," *Proceedings of the IEEE,* vol. 103, no. 1, pp. 14-76, 2014.

[95] O. N. Foundation. "OpenFlow switch specification." https://opennetworking.org/wp-content/uploads/2014/10/openflow-switch-v1.5.1.pdf (accessed.

[96] R. Zhu, J. Hong, C. C. Liu, and J. Wang, "Cyber system recovery for IEC 61850 substations," in *2021 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2021: IEEE, pp. 1-5.

[97] S. S. Hussain, M. M. Roomi, D. Mashima, and E.-C. Chang, "End-to-end performance evaluation of r-sv/r-goose messages for wide area protection and control applications," in *2023 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2023: IEEE, pp. 1-5.

[98] W. Luan, D. Sharp, and S. Lancashire, *Smart Grid Communication Network Capacity Planning for Power Utilities*. 2010, pp. 1-4.

[99] Y.-H. Jeon, "QoS requirements for the smart grid communications system," *International Journal of Computer Science and Network Security,* vol. 11, no. 3, pp. 86-94, 2011.

[100] J. Edmonds and R. M. Karp, "Theoretical improvements in algorithmic efficiency for network flow problems," *Journal of the ACM (JACM),* vol. 19, no. 2, pp. 248-264, 1972.

[101] M. Alsaeedi, M. M. Mohamad, and A. A. Al-Roubaiey, "Toward adaptive and scalable OpenFlow-SDN flow control: A survey," *IEEE Access,* vol. 7, pp. 107346-107379, 2019.

[102] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," Electricity Information Sharing and Analysis Center (E-ISAC),2016, vol. 388.

[103] W. Sun and C.-C. Liu, "Optimal transmission path search in power system restoration," in *2013 IREP Symposium Bulk Power System Dynamics and Control-IX Optimization, Security and Control of the Emerging Power Grid*, 2013: IEEE, pp. 1-5.