Article:

Kemmeugne, A, Abiri Jahromi, A and Kundur, D (2022) Resilience Enhancement of Pilot Protection in Power Systems. IEEE Transactions on Power Delivery, 37 (6). pp. 5255-5266. ISSN 0885-8977

https://doi.org/10.1109/tpwrd.2022.3175148

Resilience Enhancement of Pilot Protection in Power Systems

Anthony Kemmeugne *Student Member, IEEE*, Amir Abiri Jahromi, *Senior Member, IEEE*, Deepa Kundur, *Fellow, IEEE*

***Abstract*—Concerns about the cybersecurity and resilience of power systems have heightened in electric utilities and regulatory agencies over the past decade mainly because of the unpredictable target, location and scale of cyberattacks and the potential severity of consequences. The cybersecurity of pilot protection is paramount in bulk power systems considering their prevalence and the crucial role they play in protecting critical assets and preventing large system disturbances and major blackouts. This paper investigates the resilience of pilot protection using a co-simulation platform based on OPAL-RT simulator and Riverbed Modeler. It is demonstrated that software-defined networking for operational technology (OT SDN) significantly improves the resilience of pilot protection to false data injection (FDI) attacks compared to traditional networks. Moreover, the resilience of OT SDN based pilot protection to denial of service (DoS) attack against the SDN controller is investigated both in the proactive and reactive modes of operation. The simulation results verified the resilience of OT SDN controller in OT SDN based pilot protection to DoS attacks in the proactive mode of operation.**

***Index Terms*—Cyber-physical security, power system resilience, pilot protection, software-defined networking, co-simulation.**

I. Introduction

THE electric power system represents a critical infrastructure upon which other critical infrastructures including telecommunications, transportation, and financial systems depend, thus forming a backbone for the security and welfare of modern societies. Given the evolving landscape of threats and adverse events against power systems, it is imperative that we assess and enhance their resilience. The notion of power system resilience is defined by the National Academies as “the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events” [1], [2].

Adverse events against power systems can be classified as intentional and unintentional. The impact of unintentional factors, including natural disasters, accidental failures, involuntary human error and design flaws, can be managed and mitigated, in part, by targeted resilience investment, power system restoration drills, high-quality human resource training, and improved engineering designs. This is while the impact of intentional events such as cyber-physical attacks are more challenging to mitigate due to their often targeted and stealthy nature and scale [3].

Concerns about the cyber-physical security of power systems have been on the rise in recent years, in particular, after the physical attacks on substation transformers in California [4] and cyberattacks on the Ukrainian power grid in 2016 and 2017 [5], [6]. To address these and other growing concerns, the North American Electric Reliability Corporation (NERC) has established and mandated the critical infrastructure protection (CIP) standards [7]. As indicated in the CIP standards, the resilience of power systems is dependent on the resilience of its associated cyber networks. The emergence of interoperable communication protocols such as IEC 61850, deployment of smart grid technologies, and adoption of Internet of Things (IoT) devices and cloud services only heightens concern of this dependence [8]. Despite the unquestionable benefits of this transformation in reducing costs, improving reliability, and automating and streamlining protection, control and asset management, it introduces complex cybersecurity concerns that must be appropriately addressed.

The cybersecurity of protection systems has been at the forefront of concerns in regulatory agencies and utilities in recent years [9], [10]. This is mainly because protection systems form the most critical and fastest line of defence against power system faults and disturbances. Moreover, various studies have indicated that misoperation of protective relays have played a role in major disturbances and widespread blackouts in power systems [11], [12]. Misoperation or delayed operation of protection systems during fault or large disturbances has serious consequences for power system security and stability. In addition, sustained faults can damage and even destroy critical assets including transformers. The replacement of damaged assets often take weeks or months significantly hampering electric power restoration. Moreover, sustained faults increase the risk of wildfires [13], [14]. Thus, it is imperative to improve the cyber-resilience of protective relays against cyberattacks particularly during critical faults and major disturbances.

Existing research on the cybersecurity of protection systems mainly focuses on cyberattack impact analysis, developing novel cyber-resilient protection logics, or proposing intrusion and anomaly detection systems. This is while little or no attention has been given to the cyber-resilience of the associated communication networks that represent an integral part of protection systems, in particular pilot protection. The impact of cyberattacks against protection systems has been investigated in [15] from reliability aspect. In [16], a distributed multi-agent scheme has been proposed to detect and identify cyberattacks against protection systems. Methods for detecting false data injection (FDI) attacks against transmission line differential

This project was funded through the NSERC Discovery Grant and Strategic Partnership Grants for Projects programs.

A. Kemmeugne, and D. Kundur are with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada. (e-mails: Anthony.kemmeugne@mail.utoronto.ca, dkundur@ece.utoronto.ca)

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

protection have been proposed in [17], [18]. In [19], domain-based cyber-physical security solutions have been proposed for distance protection and circuit breaker control. The impact of cyberattacks against pilot protection has been investigated in [14] while considering potential physical solutions. Rule-based anomaly and intrusion detection systems have been proposed in [20]–[23] for cybersecurity enhancement of protection systems. In [24]–[27], machine learning-based anomaly detection systems have been proposed for protection systems.

As the protection systems move away from copper wires and power-line carriers toward local area network (LAN)-based and Internet protocol (IP)-related communication technologies, it is important to examine the resilience of these communication technologies due to the stringent communication requirements of protection systems. The design and application of legacy Ethernet LAN and IP-based communication networks to protection systems is an arduous task and may not necessarily satisfy the performance requirements. This is because network devices that forward packets in traditional communication networks also determine the network path for packets through using spanning tree algorithms (STA) and associated protocols that need to communicate continuously and negotiate forwarding paths, which adds jitter and degrades performance particularly in the event of a topology change or failure.

Although the network architecture is known in legacy communications, lack of monitoring capabilities of network traffic results in low network visibility. Moreover, power and telecommunication engineers must individually configure each individual network device separately using vendor specific and low-level commands to ensure that strict real-time requirements would not be violated. In addition, legacy communication networks function based on plug-and-play model which allows devices to communicate immediately after connection without human intervention. This results in a communication network architecture that lacks global visibility, cybersecurity and resilience requirements for managing time-critical and secure operation of protection systems.

In contrast, software-defined networking is a programmable architecture for communication networks that decouples the decision-making functions from packet forwarding functions in network devices and hands them to a centralized controller. With the separation of decision-making from packet forwarding, network devices become simple forwarding devices that focus solely on forwarding packets based on flow tables. The architecture of software-defined networking brings about numerous benefits including; 1) on-demand resource allocation and dynamic monitoring 2) simpler and less error-prone configuration of network devices through software, 3) improved cybersecurity by deny-by-default model and whitelisting of communication packets, and 4) better network visibility and situational awareness.

Software-defined networking (SDN) has been extensively investigated in the literature in the context of microgrids and smart grids for monitoring and control purposes [28]–[30]. Nevertheless, SDN has received little attention in the literature for power system protection applications. The main difference between monitoring/control and protection applications in power systems is in the importance of communication network latency in protection applications. The potential benefits of applying software-defined networking to protective relays have been highlighted in a recent research and development project on cybersecurity of energy delivery systems by Department of Energy [13]. To the best of our knowledge, no prior research work has investigated the specific risks and benefits that SDN may bring to the resilience of pilot protection against cyberattacks. As such, in this paper, we investigate the resilience of pilot protection. The resilience of legacy communication networks and software-defined networking for pilot protection is investigated using a co-simulation platform based on the OPAL-RT and Riverbed Modeler platforms. It is demonstrated that software-defined networking for operational technology (OT SDN) significantly improves the cybersecurity of pilot protection compared to legacy communication networks.

The main contributions of this paper are as follows:

- The notion of cyber-resilience of pilot protection is proposed, for the first time, and investigated for both SDN and legacy Ethernet-based communication networks. We characterize the resistance of employing OT SDN to FDI attacks, as well as the improved resilience of OT SDN controller in proactive mode to DoS attacks.
- We demonstrate how software-defined networking can be integrated and implemented for pilot protection in substation environments. Despite the extensive research on the application of SDN to microgrids and smart grids for monitoring and control purposes, to the best of the authors' knowledge, no prior research work has investigated the application of SDN to protection and in particular pilot protection.
- A co-simulation platform based on OPAL-RT and Riverbed Modeler is employed to empirically test and validate the benefits of software-defined networking for improving the cyber-resilience of pilot protection.

The remainder of the paper is organized as follows. Section II provides the necessary background about pilot protection in bulk power systems and its resilience. Moreover, the key questions concerning the resilience of SDN for pilot protection are discussed. In addition, the attack model against pilot protection is presented. In Section III, we first present the principles of software-defined networking. Afterwards, we highlight IT SDN shortcomings and OT SDN benefits for operational technology. Moreover, we discuss the specific risks and benefits of IT SDN in reactive mode of operation and OT SDN in proactive mode of operation for operational technology. The co-simulation platform employed to investigate the resilience of the legacy communication networks and software-defined networking for pilot protection is presented in Section IV. Simulation results are provided in Section V. A discussion about the impact of cyberattacks on the dependability and security of pilot protection schemes is provided in Section VI before concluding the paper in Section VII.

II. Cybersecurity of Pilot Protection

Transmission lines in bulk power systems are protected by primary/main and back-up protection using the principles of distance, overcurrent and differential relaying [31]. The primary/main protection of transmission lines is commonly based on pilot protection. This is mainly because overcurrent and distance protection relays are unable to meet the need for high-speed fault clearing.

A. Pilot Protection in Bulk Power Systems

High-speed fault clearing is essential in bulk power systems to maintain system stability, reduce damage to critical assets, improve power quality, and simplify protective relay coordination. Pilot protection achieves high-speed fault clearing for the entire line segment by using a communication channel to compare information from the transmission line terminals. Pilot protection can be classified into directional comparison protection and current-based protection. Directional comparison protection includes: 1) direct transfer trip (DTT), 2) direct underreaching transfer trip (DUTT), 3) permissive underreaching transfer trip (PUTT), 4) permissive overreaching transfer trip (POTT), 5) directional comparison blocking (DCB), and 6) directional comparison unblocking (DCUB). Current-based protection includes: 1) phase comparison protection, and 2) differential protection [32], [33].

Directional comparison protection uses a communication channel to exchange information about the direction of the fault in relation to the protection device. If the fault direction is *into* the line at all line terminals, the fault is *internal* and a trip signal is issued. Otherwise, the fault is *external* and the tripping signal is blocked. Directional comparison protection can be classified as: 1) transfer tripping schemes and 2) blocking schemes. In transfer tripping schemes, the communication channel is used to transmit a permissive tripping instruction to the remote relay. This is while in the blocking schemes, the communication channel is used to transmit a blocking instruction to the remote relay.

An important distinction between transfer tripping schemes and blocking schemes is the dependence of their reliability to the availability of the communication channel. The reliability of protection systems is separated into two aspects; 1) dependability and 2) security. Dependability is concerned with the ability of the protection scheme to operate correctly for faults within its intended zone of protection. Security is concerned with the ability of the protection scheme not to misoperate for external faults and unfaulted operating conditions [32], [33].

In the absence of cyberattacks, the transfer tripping schemes are very secure since they do not trip for external faults if the communication channel is inoperative. Conversely, these schemes lack dependability because they will not operate for internal faults if the communication channel is inoperative. In the absence of cyberattacks, the blocking schemes are very dependable because they will operate for internal faults even if the communication channel is unavailable. On the contrary, they are less secure than transfer tripping schemes because they will trip for external faults within reach of the tripping functions if the communication channel is inoperative [32], [33].

In current-based approaches, phase comparison protection assesses the phase angles of the currents at the transmission line terminals. The angle difference between the local current and the current at the remote ends determines the existence of a fault on the line. On the other hand, differential protection compares the sum of the local and remote current value at each terminal with an operation threshold value. Ideally, in a no-fault scenario, the line current entering at one end would be the same as that leaving at the other end, resulting in an actual differential current value close to zero such that protection remains inactive. In the presence of a fault, the differential current value will exceed the threshold activating protection. The dependability and security of current-based protection is highly dependent on the availability of the communication system.

B. Cyber-Resilience of Pilot Protection

Historically, two security strategies including the perimeter defense and security-by-obscurity have been applied to protect substations and protective devices. The perimeter defence strategy uses firewalls at the boundary of substations and works based on the idea that all devices inside the substations are trustworthy. The security-by-obscurity strategy works based on the idea that cyberattackers knowledge about the proprietary information and communication technologies (ICT) inside the substations is limited. The emergence of standardized and interoperable communication protocols such as IEC 61850 with remote access as well as applications like industrial internet of things (IIOT) renders both the security-by-obscurity and the perimeter defense strategies obsolete.

In order to address the cybersecurity concerns associated with the IEC 61850 protocols, the IEC 62351 standard has been proposed by WG15 of TC57 [34]. Various measures like message level authentications, encryption mechanisms and role-based access controls that restrict unnecessary permissions are recommended by the IEC 62351 standard to enhance the overall cybersecurity of the substation automation. Yet, no encryption mechanism was specified in the IEC 62351 standard for generic object oriented substation event (GOOSE) and sampled value (SV) messages used by pilot protection because of the time critical nature of these messages [35]. As such, a breach on the substation local area network is sufficient to compromise pilot protection schemes.

Layered firewalls with deny-by-default approach and intrusion detection systems (IDS) have been considered in the literature to address the cybersecurity concerns of protection and control systems in substations [27], [36]. Nevertheless, firewalls and intrusion detection systems have their own shortcomings. For example, remote management access to firewalls is considered as a security concern [36]. Signature-based and anomaly-based intrusion detection systems also suffer from shortcomings like limitations in detecting previously unseen attacks and high false positive rates [27]. In contrast to firewalls, SDN provides unparalleled cybersecurity benefits by its ability to monitor and control communication packets at all layers of the substation communications network. Moreover, SDN control plane communications to configure SDN switches are encrypted and authenticated which reduces the attack surface compared to firewall management systems. Additionally, SDN can be programmed to only send packets that do not match approved flow entries to intrusion detection systems which eliminates IDS false positives.

In this paper, we investigate the role that software-defined networking can play in implementing layered cybersecurity measures in substations and improving the cyber resilience of pilot protection. In particular, we address the following three key questions.

1) *What are the main resilience benefits of employing SDN for pilot protection?* We study how communication traffic between protective relays can be pre-engineered using SDN in the same manner that power system automation and control systems are pre-engineered. This feature significantly reduces the possibility of engineering errors and design flaws. Second, we examine the deny-by-default model and whitelisting feature of SDN for pilot protection. The deny-by-default model provides the ability to drop all unknown communication packets and devices, while the whitelisting feature allows examination of communication packet features including packet ingress and egress ports, Ether-type, source and destination MAC addresses and dropping un-authorized traffic. In contrast to firewalls which are located at the boundary of substations, SDN provides layered cybersecurity throughout the substation communication network.

2) *What are the most significant cybersecurity vulnerabilities associated with SDN and its implications for pilot protection?* The main risk associated with SDN is the vulnerability of SDN central controller to DoS attacks. We examine both reactive and proactive modes of operation to assess the seriousness of this vulnerability for pilot protection.

3) *How can we feasibly test and assess the cyber-resilience of SDN for pilot protection?* Given the critical nature of power grids, cybersecurity studies typically warrant isolated conditions for testing. Pilot testbeds and empirical prototyping are commonly used for analyzing the performance of protocols and communication network technologies in power system applications [37]. As such, we employ a co-simulator based on OPAL-RT simulator and Riverbed Modeler for analyzing the cyber-resilience of SDN and legacy communication networks in pilot protection. The co-simulator provides the capability to replicate both cyber and physical parts of pilot protection enabling a more comprehensive assessment.

C. Attack Model

Cyberattackers target confidentiality, integrity and availability of data. Confidentiality ensures that data is only known to authorized parties and systems, integrity safeguards that data is authentic and accurate, and availability assures data is accessible to people and systems when it is needed. Integrity and availability of data are paramount for pilot protection. Hence, we consider false data injection (FDI) and denial of service (DoS) attacks, the most well-known attacks against data integrity and availability.

We assume, in this paper, that opponents have remote access to the substation communication network as illustrated in Fig. 1 to perform a cyberattack against Pilot protection. Cyberattackers can access the substation network by recruiting a substation employee or a contractor who has authority to access communication devices in the substation. They can also steal legitimate credentials using malware similarly to the 2015 Ukraine attack. The stolen or leaked substation operator credentials may also be used by opponents for network discovery, and then remote connection to the substation communication network to finally perform a cyberattack.

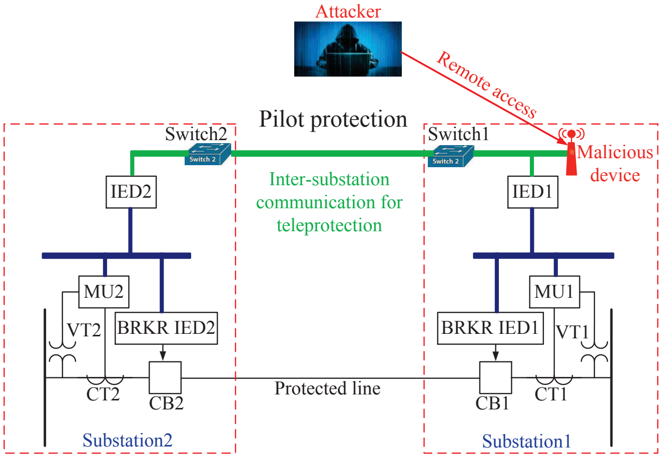


Fig. 1. Schematic representation of the attack model against pilot protection.

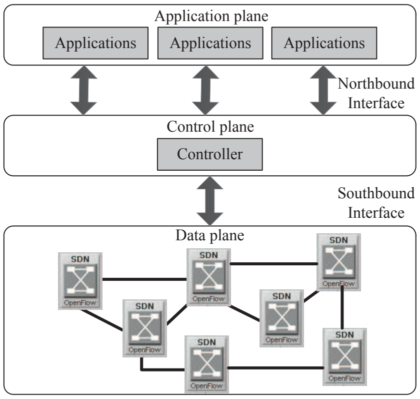


Fig. 2. Overview of SDN architecture.

III. Software-Defined Networking

SDN is a programmable architecture for communication networks that decouples the packet forwarding functions in network devices from the decision-making functions [38], [39]. SDN consists of an application plane, control plane and data plane as illustrated in Fig. 2. The SDN application plane consists of a range of applications that make requests to the control plane for network functions/resources. The SDN control plane consists of a centralized SDN controller that is responsible for controlling and managing the entire network. The control plane supervises the network behaviour through open interfaces and performs two tasks; 1) translates the needs of the application plane into flow rules for the forwarding devices in the data plane, and 2) provides information about the network state in the data plane to the application plane. The SDN data plane consists of forwarding devices such as OpenFlow switches that execute the flow rules directed by the SDN controller through flow tables. The northbound interface provides communication between SDN application plane and SDN control plane. The southbound interface provides communication between SDN control plane and SDN data plane. The OpenFlow protocol is commonly employed in the southbound interface. The OpenFlow protocol is an open standard that is managed by the Open Networking Foundation [38].

The OpenFlow protocol employs three functions – matches, actions and counters – to make decisions concerning the communication packets in the forwarding devices. The flow tables in forwarding devices consist of combinations of matches and associated actions. The match function examines the packets for specified match criteria like ingress port, Ethernet source or destination medium access control (MAC) address, and Ethertype. The action function then defines a specific action or set of actions that is applied to all packets that meet the specified match criteria. The SDN controller uses counters to monitor traffic and collect statistics such as the number of dropped packets and total byte count for a flow table [40].

SDN was originally developed for coordinating and managing large IT networks with dynamic and unpredictable traffic. SDN for IT networks operates in a reactive mode such that the forwarding devices send any packet that does not match their flow table to the SDN controller. The SDN controller then sends the packet to the application plane that then accordingly programs the flow tables of the forwarding devices through the SDN controller such that the packet reaches intended destinations. In a reactive mode of operation, the application plane may also instruct the controller to delete rules for a flow after a period of inactivity to reduce the flow table size in forwarding devices enabling performance improvement. The application plane may also modify or add flow rules to the SDN switches based on the statistics collected from the network to improve performance. This functionality is one of the major benefits of IT SDN known as on-demand resource allocation. Yet, reactive mode of operation in IT SDN suffers from the vulnerability that an attacker can flood an SDN controller by sending a large number of new packets unrecognizable to SDN switches. Various solutions such as the use of multiple controllers have been suggested to address this weakness of SDN controllers in IT networks.

In contrast to IT networks, OT networks are responsible for critical processes and high-speed decision-making which are characterized by deterministic and predictable traffic. As such, the reactive mode of operation is not appropriate for OT networks, which resulted in the introduction of OT SDN that works based on a proactive mode of operation. In proactive mode, all traffic is considered to be known and pre-engineered by the SDN controller. Therefore, forwarding devices do not react to unknown traffic by sending it to the control plane for decision-making. Instead, proactive mode locks down the flow tables in forwarding devices such that only pre-engineered traffic can be forwarded. Thus, the controller solely will be used to monitor port activity of forwarding devices and baseline OT network traffic for identifying potential malicious activities. Other techniques such as SNMP further can be used for monitoring purposes of OT SDN and remove the SDN controller to prevent any potential attack surface.

The principles of OT SDN bring important cybersecurity benefits to the communication networks for operational technology including pilot protection. OT SDN enhances the cybersecurity of communication networks by a deny-by-default model; OT SDN drops any packets that do not match the pre-engineered flow tables in the forwarding devices. In this model, devices are not allowed to connect and communicate with the network without prior approval. A recording of any device connections can be logged and reported to the SDN controller for further investigation. Thus, approved devices cannot communicate before defining flow rules for them in flow tables of forwarding devices. This is important because the legitimate traffic coming from a wrong port/device will be dropped which deters FDI from compromised ports/devices.

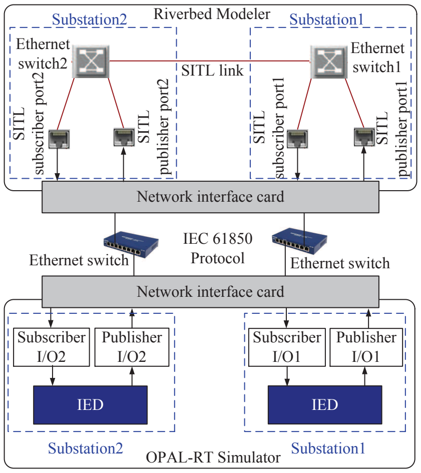


Fig. 3. Implementation of pilot protection based on legacy networks in the co-simulator.

Another benefit of SDN related to cybersecurity is enhanced situational awareness and high network visibility. In SDN, it is possible to centrally observe forwarding devices and monitor every communication between them. This enables early detection of malicious activities by baselining the communication traffic and monitoring the port activity of forwarding devices.

IV. Co-Simulation Platform

Traditionally, cyber and physical aspects of power systems have been modelled and simulated separately using event-based and continuous-time simulators, respectively. Yet, the rapid integration of communication networks and software entities with physical equipment that are responsible for controlling and monitoring power systems has created the need for coupled simulation of cyber-physical components. In particular, the need for the analysis of the complex interactions between the cyber and physical parts has expedited the emergence of co-simulators. Co-simulators are comprised of two or more domain-specific simulators that are tethered to model the interactions amongst different domains. They provide a cost-effective, safe and practical alternative to prototype or real systems for conducting various experiments including cyber-physical security analysis especially in the context of modern power systems.

A real-time co-simulator based on OPAL-RT and Riverbed Modeler is employed in this paper to investigate the cyber-resilience of pilot protection in the context of both legacy communication networks and OT SDN. The implementations of pilot protection based on legacy communication networks and OT SDN in the co-simulator are illustrated in Figs. 3 and 4, respectively. OPAL-RT simulator is a real-time simulator that provides interfaces to other simulators or hardware through its input/output (I/O) modules and Ethernet ports. OPAL-RT simulator conveniently supports various communication protocols in power systems such as IEC 61850 protocols and DNP3. Riverbed Modeler is a flexible communication network simulator that supports real-time simulations through a system-in-the-loop module and provides a development environment supporting a variety of protocols, technologies and network types.

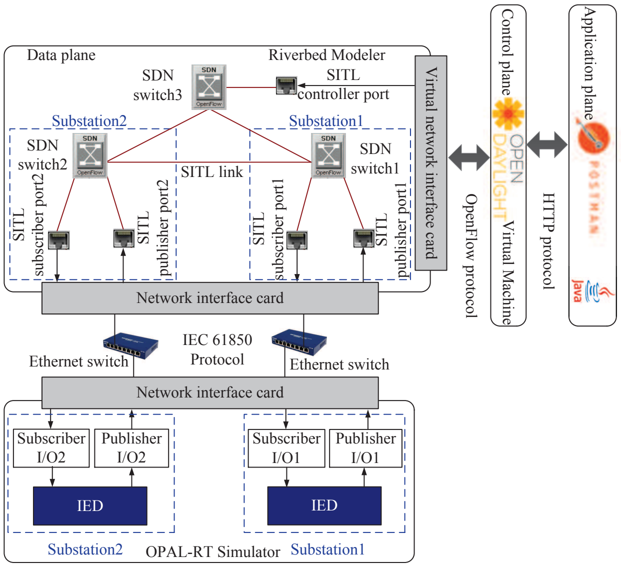


Fig. 4. Implementation of pilot protection based on SDN for operational technology in the co-simulator.

The IEC 61850 protocol, common to modern pilot protection systems, is employed in the co-simulator to communicate information between OPAL-RT simulator and Riverbed Modeler, and network interface cards enable the data transfer between OPAL-RT simulator and Riverbed Modeler. The system-in-the-loop (SITL) publisher and subscriber ports in the Riverbed Modeler perform the conversion of the real IEC 61850 packets to simulated packets and vice versa, respectively. It is worth noting that the publisher and subscriber traffic between the two simulators is separated using two Ethernet switches and cables as illustrated in Figs. 3 and 4.

The legacy communication network is implemented in Riverbed Modeler as illustrated in Fig. 3. The communication channel between substations is modelled by a SITL link that connects Ethernet switches in substations. Each Ethernet switch receives communication packets through a SITL link from a SITL publisher and sends communication packets to the Ethernet switch in the other substation through a SITL link. Moreover, each Ethernet switch delivers communication packets received from the Ethernet switch in the other substation to a SITL subscriber through a SITL link.

The OT SDN communication network consists of application plane, control plane and data plane as illustrated in Fig. 4. The SDN application plane is implemented using Postman. Postman is a popular application programming interface (API) that allows interaction with SDN controller using the HTTP protocol. The forwarding rules in SDN switches are programmed in extensible markup language (XML) format in Postman. Postman then sends a POST request to the SDN controller with payload in XML format through HTTP protocol. SDN controller is implemented using OpenDaylight. OpenDaylight is a modular open platform for customizing and automating networks. OpenDaylight is installed on an Oracle virtual machine. OpenDaylight controller runs as a service which enables communication between applications in the SDN application plane and the SDN data plane. OpenDaylight interacts with the data plane using Openflow protocol. The SDN data plane is implemented in Riverbed Modeler. OpenDaylight communicates with Riverbed Modeler through a SITL port, *i.e.*, SITL controller port as illustrated in Fig. 4.

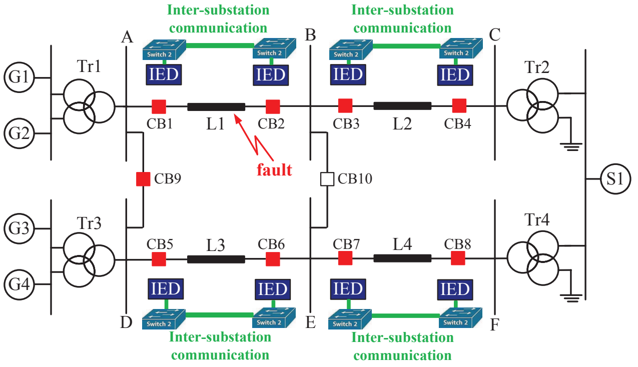

Inter-substation communication
Inter-substation communication
A
B
C
G1
G2
Tr1
Tr2
Switch 2
IED
CB1
L1
CB2
CB3
L2
CB4
fault
CB9
CB10
S1
G3
G4
Tr3
Tr4
CB5
L3
CB6
CB7
L4
CB8
D
E
F
Inter-substation communication
Inter-substation communication

Fig. 5. The IEEE PSRC D6 benchmark test system..

Similar to the legacy communication network, the communication channel between substations is modelled by a SITL link. The difference here is that SDN switches are used in substations instead of Ethernet switches. Each SDN switch receives packets through a SITL link from a SITL publisher and sends packets to the SDN switch in the other substation through a SITL link based on flow rules in its flow table. Moreover, each SDN switch delivers packets received from the SDN switch in the other substation to a SITL subscriber through a SITL link.

V. Case Studies and Empirical Tests

Seven case studies are conducted in this section to investigate the benefits of OT SDN in improving the cyber-resilience of pilot protection. In the first study, a directional comparison protection *i.e.*, permissive overreaching transfer trip (POTT) is implemented in the co-simulation platform using both legacy communication networks and SDN. The POTT protection trips the circuit breaker at each end of a protected line immediately after receiving the overreaching zone 2 signals from both terminals of the protected line. In the second study, it is demonstrated that pilot protection like POTT using legacy communication networks is vulnerable to FDI attack. In the third study, OT SDN which uses proactive mode of operation is implemented to demonstrate how OT SDN can successfully prevent FDI attacks against pilot protection like POTT.

In the fourth study, it is demonstrated that direct underreaching transfer trip (DUTT) protection using legacy communication networks is vulnerable to FDI attacks. In the fifth study, OT SDN in proactive mode of operation is implemented in the co-simulation platform similar to the third study to demonstrate how OT SDN can successfully prevent FDI attacks against DUTT protection. In the sixth and seventh studies, we demonstrate how SDN is vulnerable to DoS attacks in the reactive mode of operation while being resilient to DoS attacks in the proactive mode, respectively. The POTT protection scheme is considered in the sixth and seventh studies. The same approach can be used to investigate DoS attacks against OT SDN in the other pilot protection schemes.

The IEEE power system relaying committee (PSRC) D6 benchmark test system [41], [42] is used in the case studies. The benchmark test system connects a power plant with four 250 MVA generators to a 230 kV transmission network through two parallel 500 kV transmission lines. The 230 kV transmission network is modelled as an infinite bus. All the

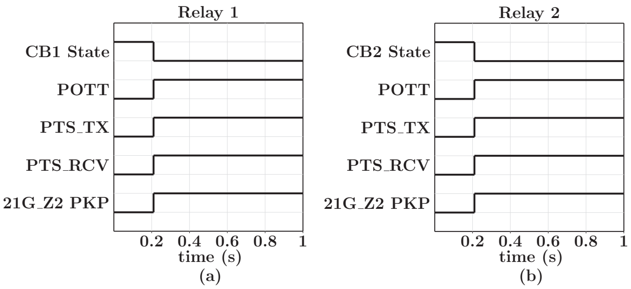


Fig. 6. POTT protection signals and circuit breakers state of (a) Relay 1 and CB1 and (b) Relay 2 and CB2.

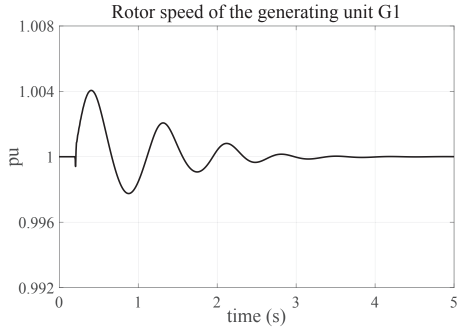


Fig. 7. The rotor speed of the generating unit G1 when the permanent three-phase-to-ground fault at 82% of the line L1 is cleared instantaneously.

circuit breakers in the benchmark test system except the circuit breaker CB10 are initially closed as illustrated in Fig. 5. In the case studies, a permanent three-phase-to-ground midline fault occurs at t = 0.2 s on line L1 of the benchmark test system as illustrated in Fig. 5. The location of the fault is at 82% of the transmission line from bus A.

A. Case Study I: Simulating the IEEE PSRC D6 Test System for Legacy Communication Networks and OT SDN

POTT protection is implemented in this case study using distance relays. Moreover, for comparison, the communication network between the substations is implemented using both legacy communication networks (Fig. 3) and OT SDN (Fig. 4). A permanent three-phase-to-ground midline fault on the transmission line L1 of the benchmark test system is simulated in OPAL-RT simulator as discussed previously. The simulation results for legacy Ethernet-based communication networks and OT SDN are essentially identical in the absence of cyberattacks which are presented collectively in Figs. 6 and 7.

As illustrated in Fig. 6, in the absence of cyberattacks, the zone 2 elements of distance protective relays in both substations observes the fault and issue the permissive trip signal (PTS TX). Thus, POTT protection operates and instantaneously trips the circuit breakers CB1 and CB2. The opening of the circuit breakers CB1 and CB2 isolates the faulty transmission line L1 and preserves the stability of the generators in the power plant as illustrated in Fig. 7.

B. Case Study II: Simulating False Data Injection Attacks Against Legacy Communication Networks for POTT Scheme

The implementation of the FDI attack against pilot protection based on legacy communication network in Riverbed Modeler is illustrated in Fig. 8. The GOOSE packets containing false permissive transfer trip signals are first generated using OPAL-RT simulator and saved using the Wireshark tool; Wireshark is an open-source software that is able to monitor, and save communication packets. The GOOSE packets containing false permissive transfer trip signals are then injected into the communication network via the Wireshark tool through a SITL port as illustrated in Fig. 8. The FDI attack, here, takes advantage of the plug-and-play model of the legacy communication networks. The attacker can simply perform the FDI attack by connecting the attack device to the communication network of the substations as illustrated in Fig. 8.

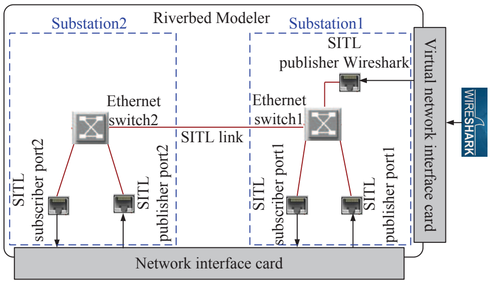


Fig. 8. Implementation of false data injection attack against legacy communication network in Riverbed Modeler.

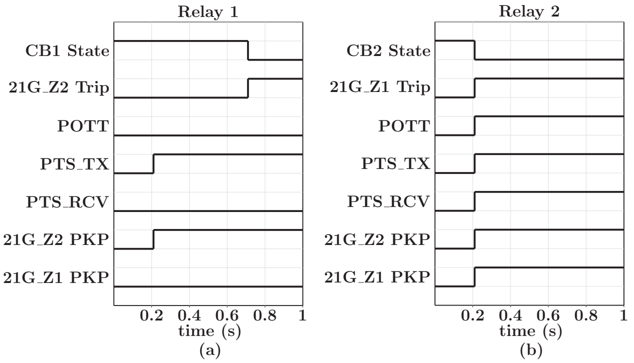


Fig. 9. Step-distance relay signals and circuit breakers state of (a) Relay 1 and CB1 and (b) Relay 2 and CB2.

Similar to Case Study I, a permanent three-phase-to-ground midline fault is simulated in OPAL-RT simulator on the transmission line L1 of the benchmark test system at 82% of the transmission line from bus A. The protective relay and circuit breaker signals are illustrated in Fig. 9. In Fig. 9, PTS_TX denotes transmitted transfer trip signal. PTS_RCV denotes received transfer trip signal. 21G_Z1 PKP and 21G_Z2 PKP respectively denote zone 1 and zone 2 pick-up signals of distance relays. 21G_Z1 Trip and 21G_Z2 Trip respectively denote zone 1 and zone 2 trip signals of distance relays. CB1

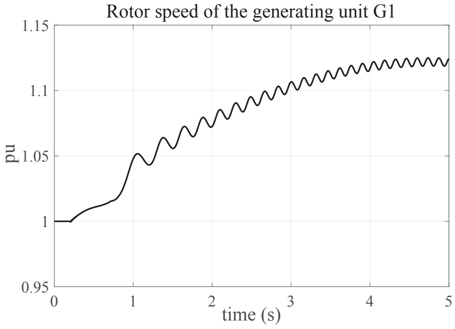
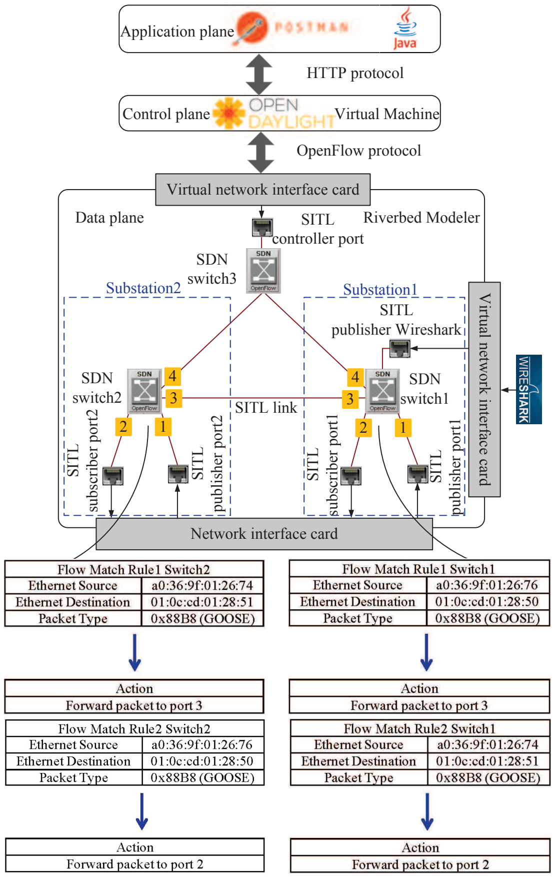


Fig. 10. The rotor speed of the generating unit G1 when the permanent three-phase-to-ground fault at 82% of the line L1 is cleared after 30 cycles.



Flow Match Rule1 Switch2	
Ethernet Source	a0:36:9f:01:26:74
Ethernet Destination	01:0c:cd:01:28:51
Packet Type	0x88B8 (GOOSE)

Action
Forward packet to port 3

Flow Match Rule2 Switch2	
Ethernet Source	a0:36:9f:01:26:76
Ethernet Destination	01:0c:cd:01:28:50
Packet Type	0x88B8 (GOOSE)

Action
Forward packet to port 2

Flow Match Rule1 Switch1	
Ethernet Source	a0:36:9f:01:26:76
Ethernet Destination	01:0c:cd:01:28:50
Packet Type	0x88B8 (GOOSE)

Action
Forward packet to port 3

Flow Match Rule2 Switch1	
Ethernet Source	a0:36:9f:01:26:74
Ethernet Destination	01:0c:cd:01:28:51
Packet Type	0x88B8 (GOOSE)

Action
Forward packet to port 2

Fig. 11. Implementation of false data injection attack against SDN network in Riverbed Modeler.

State and CB2 state respectively denote the status of the circuit breakers CB1 and CB2.

As illustrated in Fig. 9 (a) and (b) both relays see the fault in zone 2 (21G_Z2 PKP) and send the permissive trip signals (PTS_TX) to the remote relay. Nevertheless, the attacker replaces the original GOOSE packets containing the permissive trip signals from substation 2 to substation 1 with false GOOSE packets indicating no permissive trip signals (PTS_RCV). Therefore, the POTT protection does not operate in substation 1 as illustrated in Fig. 9 (a). The distance relay 2 sees the fault in zone 1 (21G_Z1 PKP) and instantaneously issues 21G_Z1 trip signal to the circuit breaker CB2 as illustrated in Fig. 9 (b). This is while the distance relay 1 waits for 30 cycles before issuing the 21G_Z2 trip signal to the circuit breaker CB1 as illustrated in Fig. 9 (a). As a result, the transmission line L1 remains connected to the bus A despite the fault and the generators continue to feed the fault current. Thus, the generators lose synchronism as illustrated in Fig. 10 demonstrating the vulnerability of legacy communication networks to FDI attacks.

C. Case Study III: Simulating False Data Injection Attacks Against OT SDN for POTT Scheme

Implementation of the FDI attack against pilot protection based on OT SDN is illustrated in Fig. 11. The legitimate traffic between substations is pre-engineered in SDN switches by Postman through OpenDaylight. The pre-engineered forwarding rules programmed in Postman for a SDN switch contains the name of the switch. Moreover, the header information is defined which include source MAC address, destination MAC address, and the type of the packet, *i.e.*, GOOSE packet. The action that should be taken by the SDN switch is further defined to send the packet to a pre-determined port as illustrated in Fig. 11.

Similar to Case Study II, the POTT protection is implemented and communication packets containing false data is again injected to the communication network using Wireshark tool through a SITL port as illustrated in Fig. 11. It is assumed that the cyberattacker knows the destination MAC address and the type of legitimate packets *i.e.*, GOOSE. Moreover, it is assumed that the attacker is able to gain access to an approved port of the SDN switch to inject the packets containing false data. It is worth noting that a cyberattacker without access to an approved port cannot inject false data since the SDN switches work based on a deny-by-default model in contrast to legacy switches which work based on a plug-and-play model. Nevertheless, the attacker cannot obtain information about the source MAC address of the legitimate packets since the attacker does not have access to the information about the protective relay in the remote substation. The packets containing false GOOSE messages coming through the approved port are dropped in this Case Study by SDN switches since the source address of the packets was not correct.

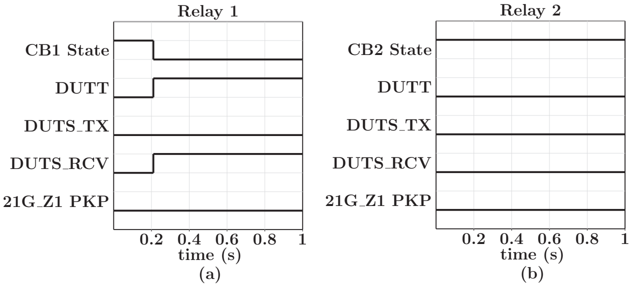


Fig. 12. Step-distance relay signals and circuit breakers state of (a) Relay 1 and CB1 and (b) Relay 2 and CB2.

As a result, the permissive trip signals (PTS TX) are received by POTT protection similar to Case Study 1 (Fig. 6) and the faulty line L1 is isolated immediately. Therefore, the stability of the generators in the power plant is preserved similar to Case Study 1 (Fig. 7) despite the FDI cyberattack.

D. Case Study IV: Simulating False Data Injection Attacks Against Legacy Communication Networks for DUTT Scheme

The implementation of the FDI attack against DUTT scheme based on legacy communication network in Riverbed Modeler is similar to case study II (Fig. 8). The GOOSE packets containing false direct underreaching transfer trip signals are first generated using OPAL-RT simulator and saved using the Wireshark tool. The GOOSE packets containing false direct underreaching transfer trip signals are then injected into the communication network via the Wireshark tool through a SITL port similar to case study II (Fig. 8). The difference to case study II is that the benchmark test system is working under normal conditions in this case study. The cyberattacker injects GOOSE packets containing false direct underreaching transfer trip signals at t = 0.2 s with the objective of opening the circuit breaker CB1 and tripping the transmission line L1.

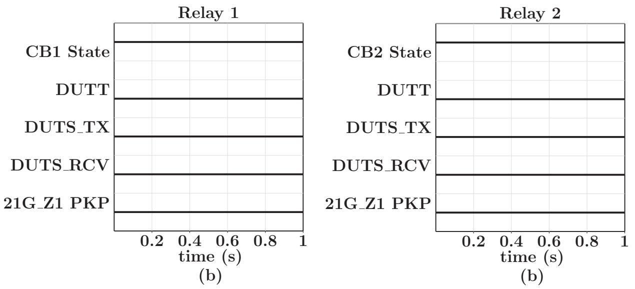


Fig. 13. Step-distance relay signals and circuit breakers state of (a) Relay 1 and CB1 and (b) Relay 2 and CB2.

The protective relay and circuit breaker signals for this case study are illustrated in Fig. 12. In Fig. 12, DUTS_TX denotes transmitted direct underreaching transfer trip signal. DUTS_RCV denotes received direct underreaching transfer trip signal. 21G_Z1 PKP denotes zone 1 pick-up signal of distance relays. CB1 State and CB2 state respectively denote the status of the circuit breakers CB1 and CB2.

As illustrated in Fig. 12 (a) and (b), there is no fault in the system and distance relays do not see any faults in zone 1 (21G_Z1 PKP). The cyberattacker sends GOOSE packets containing false direct underreaching transfer trip signals at t = 0.2 s to the circuit breaker CB1. Therefore, the circuit breaker CB1 opens as illustrated in Fig. 12 (a) and trips the transmission line L1. The outage of the transmission line L1 causes a disturbance in the system but the generators do not lose synchronism due to this cyberattack. The rotor speed of the generator G1 in this case study is similar to Case Study I (Fig. 7).

E. Case Study V: Simulating False Data Injection Attacks Against OT SDN for DUTT Scheme

The implementation of the FDI attack against DUTT scheme based on OT SDN is similar to case study III (Fig. 11). The legitimate traffic between substations is pre-engineered in SDN switches by Postman through OpenDaylight. The pre-engineered forwarding rules programmed in Postman for a SDN switch contains the name of the switch. Moreover, the header information is defined which include source MAC address, destination MAC address, and the type of the packet, *i.e.*, GOOSE packet. The action that should be taken by the SDN switch is further defined to send the packet to a predetermined port as illustrated in Fig. 11.

Similar to Case Study IV, the communication packets containing false direct underreaching transfer trip signals are again injected to the communication network using Wireshark tool through a SITL port as illustrated in Fig. 11. It is assumed that the cyberattacker knows the destination MAC address and the type of legitimate packets *i.e.*, GOOSE. Moreover, it is assumed that the attacker is able to gain access to an approved port of the SDN switch to inject the packets containing false direct underreaching transfer trip signals. The packets containing false direct underreaching transfer trip signals coming through the approved port are dropped in this case study by SDN switches since the source address of the packets was not correct. As illustrated in Fig. 13 (a) and (b), the cyberattack is unsuccessful and the circuit breaker CB1 remains closed. Thus, the power system continues to operate under normal conditions.

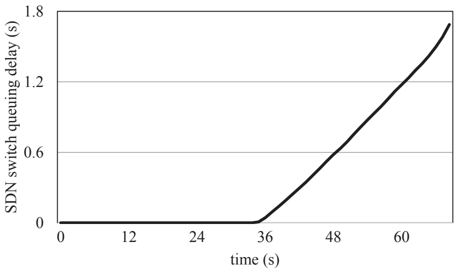


Fig. 14. The queuing delay of a SDN switch under a DoS attack in the reactive mode of operation.

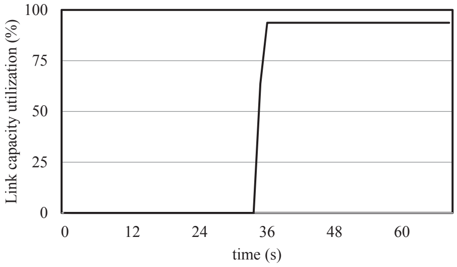


Fig. 15. Communication statistics of the link between data plane and control plane after a DoS attack in the reactive mode of operation.

F. Case Study VI: Simulating DoS attacks against SDN in the Reactive Mode of Operation

The vulnerability of SDN in reactive mode to DoS attacks is examined in this study. The communication traffic between substations is pre-engineered in SDN switches by the SDN controller similar to study III. The difference, here, is that SDN switches are programmed to forward unknown communication packets to the SDN controller based on the reactive mode of operation.

We consider a scenario where an attacker has access to an approved port in an SDN switch to inject communication packets. The objective of the attacker is to disable the communication network by injecting a large number of unknown packets. The TCP replay command in Wireshark tool is used to implement the DoS attack. The number of packets injected by the attacker in this study is forty thousand times larger than the number of packets in study III to realize a DoS attack.

In this study, SDN switches forward a copy of the unknown packets to the SDN controller based on the reactive mode of operation. As illustrated in Fig. 14, the computational resources of the SDN switch under attack are entirely consumed by the DoS attack. As a result, the queuing delay of the SDN switch begins to increase to more than 1 s. Moreover, the DoS attack consumes the available communication capacity between the data plane and control plane as illustrated in Fig. 15. As such, the SDN controller is unable to take any corrective action to mitigate the DoS attack consequences, for example, by updating the flow tables of SDN switches. Any attempt to update the flow tables of SDN switches resulted in the error message 501 which indicates the SDN controller request failure. Thus, DoS attacks in the reactive mode of operation are successful.

As illustrated in Fig. 16 (a), relay 1 sees the fault in zone 2 (21G_Z2 PKP) and sends the permissive trip signal (PTS_TX)

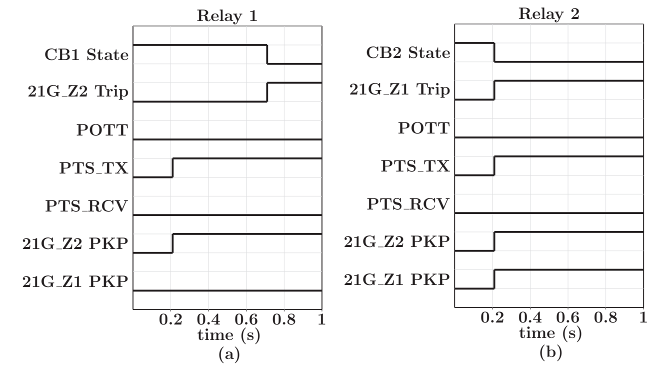


Fig. 16. Step-distance relay signals and circuit breakers state of (a) Relay 1 and CB1 and (b) Relay 2 and CB2.

to relay 2. Moreover, relay 2 sees the fault both in zone 1 and 2 (21G_Z1 PKP and 21G_Z2 PKP) and sends the permissive trip signal (PTS_TX) to the relay 1 as illustrated in Fig. 16 (b). Nevertheless, the permissive trip signals get delayed by the DoS attack and do not reach the respective remote relay in a timely fashion. The relay 2 (R2) instantaneously issues 21G_Z1 trip signal to the circuit breaker CB2 as illustrated in Fig. 16 (b) because it sees the fault in zone 1 (21G_Z1 PKP). This is while the relay 1 (R1) waits for 30 cycles before issuing the 21G_Z2 trip signal to the circuit breaker CB1 as illustrated in Fig. 16 (a). This is because relay 1 does not receive the permissive trip signal (PTS_RCV) from the relay 2. Thus, the generators lose synchronism similar to Case Study II (Fig. 10) demonstrating the vulnerability of pilot protection based on SDN in reactive mode to DoS attacks.

G. Case Study VII: Simulating DoS Attacks against SDN in the Proactive Mode of Operation

The vulnerability of SDN to DoS attacks in the proactive mode of operation is examined in this study. To lock down the flow tables, the SDN controller is removed after initializing the switches in the data plane. A scenario similar to study IV is considered where an attacker has access to an approved port in an SDN switch to inject communication packets, the TCP replay command in Wireshark tool is used to implement the DoS attack, and the number of packets injected by the attacker in this study is also on the same scale.

As evident, the unknown packets are dropped by the SDN switches without sending a copy to the SDN controller. As such, the queuing delay caused by the DoS attack in proactive mode of operation remains under a millisecond as illustrated in Fig. 17. This is because the computational resources of the SDN switch under attack are not consumed to send a replica of the unknown packets to the SDN controller. Thus, the DoS attack is unsuccessful in SDN proactive mode of operation.

In this study, the permissive trip signals (PTS TX) are received by POTT protection similar to Case Study 1 (Fig. 6) and the faulty line L1 is isolated immediately. Therefore, the stability of the generators in the power plant is preserved similar to Case Study 1 (Fig. 7) despite the DoS cyberattack. This demonstrates the resilience of pilot protection based on SDN to DoS attacks in proactive mode compared to reactive.

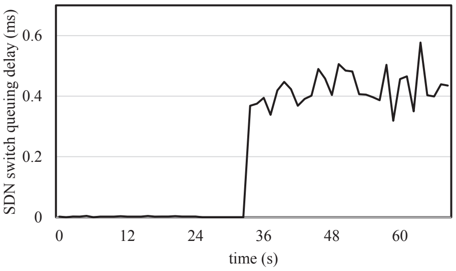


Fig. 17. The queuing delay of a SDN switch under a DoS attack in the proactive mode of operation.

VI. Discussion

Cyberattackers can produce both security and dependability failures for pilot protection. Nevertheless, there is a distinction between the number of signals that should be compromised by cyberattackers to cause dependability and security failures depending on the type of the pilot protection scheme.

For example, FDI attacks can produce both dependability and security failures for POTT protection scheme when there is a fault within the zone 2 protection reach of the relay. The dependability failure for POTT protection scheme occurs when the fault is on the line and the compromised transfer trip signal by the FDI attack indicates that there is no fault on the line. Conversely, the security failure for POTT protection scheme occurs when the fault is on the adjacent line and within the zone 2 protection reach of the relay but the compromised transfer trip signal by the FDI attack indicates that the fault is on the line. A cyberattacker cannot produce security failures for POTT protection scheme just by compromising the transfer trip signal by FDI attack when there is no fault in the system. This is while a cyberattacker can produce dependability and security failures for DUTT and DTT schemes just by compromising the transfer trip signal under all conditions.

Cyberattackers also can produce dependability and security failures for DCB protection scheme when there is a fault within the zone 2 protection reach of the relay. The dependability failure for DCB protection scheme occurs when the fault is on the line and the compromised blocking signal by the FDI attack indicates that there is no fault on the line. Conversely, the security failure for DCB protection scheme occurs when the fault is on the adjacent line and within the zone 2 protection reach of the relay but the compromised blocking signal by the FDI attack indicates that the fault is on the line. A cyberattacker cannot produce security failures for DCB protection scheme just by compromising the blocking signal by FDI attack when there is no fault in the system. The same discussions can be provided for other pilot protection. Nevertheless, we do not discuss all the pilot protection for brevity.

Pilot protection failures have more serious consequences when there is a fault in the system compared to when the system is operating under normal conditions. This is because pilot protection failures during faults can result in more severe stability problems and larger disturbances. As such, we mostly focused on the cases when there is a fault in the system in this paper.

VII. Conclusion

This paper proposed and investigated the notion of cyber-resilience for pilot protection. It is demonstrated that software-defined networking for operational technology brings key resilience benefits to pilot protection compared to legacy Ethernet-based communication networks. This includes improved cybersecurity by a deny-by-default model and whitelisting of communication packets as well as better network visibility and situational awareness. It is further illustrated how OT SDN in a proactive mode of operation is resilient to DoS attacks in contrast to IT SDN in reactive mode. Future research will focus on investigating the failure recovery and self-healing benefits of OT SDN compared to legacy communication networks for pilot protection. It is further worth noting that despite the unquestionable benefits of OT SDN for pilot protection, OT SDN might be vulnerable to FDI attacks against telecontrol commands from control centers like Ukrainian attack. We will investigate the risks and benefits of OT SDN for telecontrol commands from control centers in our future research.

References

[1] National Research Council, Disaster Resilience: A National Imperative, National Academics Press, Washington, DC, 2012.

[2] National Academics of Sciences, Engineering, Medicine, Enhancing the Resilience of the Nation's Electricity System, National Academics Press, 2017.

[3] Congressional Research Service, Electric Grid Cybersecurity, R45312, 2018.

[4] R. Smith "Assault on California Power Station Raises Alarm on Potential for Terrorism," *The Wall Street Journal*, 2014.

[5] R. M. Lee, M. J. Assante, and T. Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case*, Elect. Inf. Sharing Anal. Center, Washington, DC, USA, Mar. 2016.

[6] J. Slowik, "Anatomy of an attack: Detecting and defeating CRASHOVERRIDE," Hanover, MD, USA, Dragos Inc., White Paper, Oct. 2018.

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

[8] National Academies of Sciences, Engineering, and Medicine, Communications, Cyber Resilience, and the Future of the U.S. Electric Power System: Proceedings of a Workshop, The National Academies Press, Washington DC, 2020.

[9] "Cyber resilience and response, 2018 public-private analytic exchange program," Department of Homeland Security, Tech. Rep., 2018. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/2018 AEP Cyber Resilience and Response.pdf

[10] S. Ward *et al.*, "Cyber security issues for protective relays; c1 working group members of power system relaying committee," *In Proc. IEEE Power Eng. Soc. Gen. Meet.*, June 2007, pp. 1-8.

[11] R. Baldick *et al.*, "Initial review of methods for cascading failure analysis in electric power transmission systems IEEE PES CAMS task force on understanding, prediction, mitigation and restoration of cascading failures," *2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, Pittsburgh, PA, 2008, pp. 1-8.

[12] P. Kundur, C. Taylor, and P. Pourbeik "Blackout experiences and lessons, best practices for system dynamic performance, and role of new technologies," *IEEE Special Publ.* 07TP190, July 2007.

[13] Pacific Northwest National Laboratory, Cybersecurity for Distance Relay Protection, Tech. Rep., PNNL–29663 Feb. 2020.

[14] A. Abiri-Jahromi, A. Kemmeugne, D. Kundur and A. Haddadi, "Cyber-physical attacks targeting communication-assisted protection schemes," *IEEE Trans. Power Syst.*, vol. 35, no. 1, pp. 440–450, Jan. 2020.

[15] M. Bahrami, M. Fotuhi-Firuzabad and H. Farzin, "Reliability evaluation of power grids considering integrity attacks against substation protective IEDs," *IEEE Trans. Ind. Informat.*, *early access*.

[16] M. S. Rahman, M. A. Mahmud, A. M. T. Oo, and H. R. Pota, "Multi-agent approach for enhancing security of protection schemes in cyber-physical energy systems," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 436-447, Apr. 2017.

[17] A. Ameli, A. Hooshyar, and E. F. El-Saadany, "Development of a cyber-resilient line current differential relay," *IEEE Trans. Ind. Informat.*, vol. 15, no. 1, pp. 305–318, Jan. 2019.

[18] A. Ameli, A. Hooshyar, E. F. El-Saadany, and A. M. Youssef, "An intrusion detection method for line current differential relays," *IEEE Trans. Information Forensics and Security*, vol. 15, pp. 329-344, 2020.

[19] J. Hong *et al.*, "Cyber attack resilient distance protection and circuit breaker control for digital substations," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4332–4341, July 2019.

[20] U. K. Premaratne, J. Samarabandu, and T. S. Sidhu, "An intrusion detection system for IEC61850 automated substations," *IEEE Trans. Power Del.*, vol. 25, pp. 2376–2383, Oct. 2010.

[21] C. W. Ten, J. Hong, and C. C. Liu, "Anomaly detection for cybersecurity of the substations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 865-873, Dec. 2011.

[22] J. Hong, C. C. Liu, and M. Govindarasu, "Integrated anomaly detection for cyber security of the substations," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1643-1653, April 2014.

[23] J. Hong, and C. C. Liu,"Intelligent electronic devices with collaborative intrusion detection systems" *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 271–281, Jan. 2019.

[24] S. Sheng, W. L. Chan, K. K. Li, D. Xianzhong, and Z. Xiangjun, "Context information-based cyber security defense of protection system," *IEEE Trans. Power Del.*, vol. 22, no. 3, pp. 1477-1481, July 2007.

[25] A. Ahmed, V. V. G. Krishnan, S. A. Foroutan, M. Touhiduzzaman, A. Srivastava, Y. Wu, A. Hahn, and S. Sindhu "Cyberphysical security analytics for anomalies in transmission protection systems," *IEEE Trans. Ind. Appl.*, vol. 55, no. 6, pp. 6313-6323, Nov. 2019.

[26] A. Ameli, A. Ayad, E. El-Saadany, M. Salama and A. Youssef, "A learning-based framework for detecting cyber-attacks against line current differential relays," *IEEE Trans. Power Del.*, *early access*.

[27] Y. M. Khaw, A. A. Jahromi, M. F. M. Arani, S. Sanner, D. Kundur and M. Kassouf, "A Deep learning-based cyberattack detection system for transmission protective relays," in *IEEE Trans. Smart Grid early access*.

[28] L. Ren, Y. Qin, B. Wang, P. Zhang, P. B. Luh and R. Jin, "Enabling resilient microgrid through programmable network," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 2826–2836, Nov. 2017

[29] D. Ibdah, M. Kanani, N. Lachtar, N. Allan and B. Al-Duwairi, "On the security of SDN-enabled smart grid systems," *2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, Ras Al Khaimah, United Arab Emirates, 2017, pp. 1–5.

[30] M. H. Rehmani, A. Davy, B. Jennings and C. Assi, "Software defined networks-based smart grid communication: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2637–2670, 2019.

[31] J. L. Blackburn and and T. J. Domin, Protective Relaying - Principles and Applications, 3rd ed., *CRC Press*, 2007.

[32] IEEE std. C37.113-2015, IEEE Guide for Protective Relay Applications to Transmission Lines, Dec. 2015.

[33] JWG 34/35.11, Protection Using Telecommunications, Technical Brochure, CIGRÉ, 2001.

[34] International Electrotechnical Commission (IEC), "IEC TS 62351–1 Power systems management and associated information exchange Data and communications security. Part 1: Communication network and system security Introduction to security issues," 2007.

[35] International Electrotechnical Commission (IEC), "IEC TS 62351–6 Power systems management and associated information exchange Data and communications security. Part 6: Security for IEC 61850," 2007.

[36] D. Anderson and N. Kipp, "Implementing firewalls for modern substation cybersecurity", *In Proc. 12th Annual Western Power Delivery Automation Conference*, April, 2010, pp. 1–7.

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

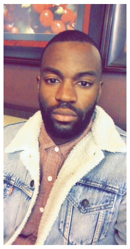
[38] Open Networking Foundation, "Software-defined networking: The new norm for networks," ONF White Paper, 2012.

[39] OpenFlow, Open Networking Foundation. [Online]. Available: http://www.opennetworking.org/

[40] P. Robertson, "Software-defined networking for mission-critical operations," Industrial Ethernet Book, Issue 98, February 2017. [Online]. Available: http://www.iebmedia.com.

[41] IEEE PSRC WG D6, "Power swing and out-of-step considerations on transmission lines," Jul. 2005.

[42] H. Gras, J. Mahseredjian, E. Rutovic, U. Karaagac, A. Haddadi, O. Saad, I. Kocar, and A. El-Akoum, "A new hierarchical approach for modeling protection systems in EMTtype software," *in Proc. Intern. Conf. Power Syst. Transients*, Seoul, South Korea, Jun. 2017, pp. 1-6.



Anthony Kemmeugne (Student Member, IEEE) received the Engineering degree in telecommunication and electronics from Telecom Saint–Etienne, Saint–Etienne, France, in 2018, and the M.Sc. degree in electrical and computer engineering from the Universite du Quebec a Chicoutimi, Chicoutimi, QC, Canada, in 2018. He is currently working toward the Ph.D. degree at the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON, Canada.

From 2017 to 2018, he was a Research Engineer with the Research Institute of Hydro Quebec, Montreal, QC, Canada. His research interests include communication systems, and advanced simulation methods including programmable networks, power systems co-simulation, and smart grid cybersecurity.

Amir Abiri Jahromi (Senior Member, IEEE) received the Ph.D. degree in Electrical and Computer Engineering from McGill University, Montreal, QC, Canada, in 2016. From January 2018 to December 2019, he was a Postdoctoral Fellow at the University of Toronto. In 2020, he was a Research Associate at the University of Toronto.

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

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

Professor Kundur's research interests lie at the interface of cybersecurity, signal processing and complex dynamical networks. She is an author of over 200 journal and conference papers and is a recognized authority on cybersecurity issues. She has served as Honorary Chair of the 2021 IEEE Electric Power and Energy Conference, Publicity Chair for ICASSP 2021, General Chair of the 2018 GlobalSIP Symposium on Information Processing, Learning and Optimization for Smart Energy Infrastructures, TPC Co–Chair for IEEE SmartGridComm 2018, and Symposium Co–Chair for the Communications for the Smart Grid Track of ICC 2017, amongst other roles. Professor Kundur currently serves on the Advisory Board of IEEE Spectrum and, from 2013 to 2020.

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